Citrix SD-WAN Orchestrator pour les locaux 14.4

Contents

Notes de publication de SD-WAN Orchestrator pour la version sur site 14.4

December 10, 2024

Ce document de notes de version décrit les améliorations et les modifications, ainsi que les problèmes résolus et connus qui existent pour la version Build 14.4 de Citrix SD-WAN Orchestrator for On-premises.

Remarques

Ce document de notes de version n'inclut pas de correctifs liés à la sécurité. Pour obtenir une liste des correctifs et avis liés à la sécurité, consultez le bulletin de sécurité Citrix.

Problèmes connus

Les problèmes qui existent dans la version 14.4.

La publication du logiciel SD-WAN dans Citrix SD-WAN Orchestrator for On-premises peut échouer avec l'erreur suivante :

`Failed to fetch software details from Citrix cloud.`

Solution de contournement: déconnectez-vous et reconnectez-vous à Citrix Cloud via Citrix SD-WAN Orchestrator for On-premises, puis publiez le logiciel SD-WAN.

[SDW-24980]

Notes de mise à jour pour la version 14.3 de SD-WAN Orchestrator pour locaux

October 21, 2022

Ce document de notes de mise à jour décrit les améliorations et les modifications, ainsi que les problèmes résolus et connus qui existent pour la version 14.3 de Citrix SD-WAN Orchestrator for On-premises.

Remarques

Ce document de notes de publication n'inclut pas les correctifs liés à la sécurité. Pour obtenir la liste des correctifs et des conseils liés à la sécurité, consultez le bulletin de sécurité Citrix.

Nouveautés

Les améliorations et modifications disponibles dans la version 14.3.

Configuration et gestion

Stratégies QoS

La page des politiques de QoS est remaniée pour améliorer l'expérience utilisateur. Les options telles que les règles d'application personnalisées, les règles d'application, les règles HDX, les règles de groupe d'applications, les règles IP et les règles de protocole IP par défaut sont améliorées avec une nouvelle présentation.

[SDW-11029]

Plateforme et systèmes

Améliorations apportées à la gestion de l'adresse IP/IP

Les colonnes **IP de gestion** et **Accès aux appareils** des écrans d'interface utilisateur suivants sont améliorées pour afficher l'adresse IP intrabande ou l'adresse IP de gestion en fonction du type d'adresse IP que l'appareil utilise pour communiquer avec Citrix SD-WAN Orchestrator for On-premises :

- Fournisseur > Rapports > Inventaire > Détails
- Client > Configuration > Accueil du réseau > Actions > Afficher les détails
- Client > Rapports > Inventaire > Détails
- Site > Tableau de bord > Appareils

[SDW-23353]

Exporter le rapport au format CSV

Grâce à la fonctionnalité **Exporter au format CSV**, vous pouvez télécharger les points du graphique du chemin (chemin virtuel/membre) pour n'importe quelle série chronologique (horaire, hebdomadaire, etc.) sous forme de fichier Excel de valeurs séparées par des virgules (CSV) et être en mesure de tracer tous les points de données distincts pour un rapport de site particulier.

[SDW-20988]

Authentification du certificat

Citrix SD-WAN Orchestrator pour locaux prend en charge l'authentification des appliances pour les chemins virtuels statiques et dynamiques à l'aide de l'infrastructure à clé publique (PKI) en tant que fonctionnalité de sécurité supplémentaire. L'activation de la fonctionnalité étend le mécanisme d'authentification de chemin virtuel existant en distribuant les certificats PKI sur le chemin de données, par l'appliance initiant l'échange. L'amélioration de l'ICP prend également en charge la gestion des listes de révocation de certificats (CRL) pour la révocation centralisée des certificats compromis.

[SDW-19295]

SD-WAN Orchestrator

Afficher la configuration (aperçu)

Citrix SD-WAN Orchestrator pour locaux présente la page **Afficher la configuration** au niveau du site. Cette page fournit un résumé détaillé de la configuration d'un site sur plusieurs sous-systèmes.

[SDW-22284]

Statistiques entemps réel au niveau du réseau, statistiquesen temps réel au niveau du site

La **connexion au pare-feu** est désormais renommée **Firewall Statistics**. Les politiques NAT et de filtre ont récemment été ajoutées dans la liste déroulante des types de statistiques. De plus, les options de statistiques en temps réel sont restructurées et réparties dans les catégories suivantes :

- Statistiques du réseau
- Statistiques relatives aux applications
- Statistiques d'itinéraire

[SDW-20966]

Paramètres du haut débit mobile et état du haut débit mobile

Vous pouvez désormais connecter l'appliance Citrix SD-WAN de votre site à un réseau via une connexion Internet haut débit. Cet état du haut débit mobile et cette prise en charge de la configuration sont disponibles pour les modems internes. Vous pouvez également consulter l'état de la configuration haut débit de votre appareil et de la carte SIM active.

[SDW-10907]

Problèmes résolus

Les problèmes résolus dans la version 14.3.

Configuration et gestion

Le certificat PKI n'était pas affiché sur l'interface utilisateur Citrix SD-WAN Orchestrator for On-premises. Ce problème s'est produit car le champ **Unité organisationnelle** était obligatoire sur le certificat PKI.

[SDW-23726]

Divers

Certains sites ne peuvent pas se connecter à Citrix SD-WAN Orchestrator pour l'interface utilisateur locale.

[SDWANHELP-2601]

Problèmes connus

Les problèmes qui existent dans la version 14.3.

Les graphiques des applications et des catégories d'applications sont vides sur la page **Rapports** > **Utilisation** > **Applications** de l'interface utilisateur Citrix SD-WAN Orchestrator for On-premises.

[SDW-23817]

La version logicielle précédemment sélectionnée sur la page **Déploiement** > **Paramètres** > **Mise à niveau partielle du site** > **Version logicielle** de l'interface utilisateur n'est pas conservée lorsque les utilisateurs reviennent sur cette page.

Solution : sélectionnez manuellement la version partielle du logiciel de mise à niveau du site pour chaque site en cliquant sur **Déploiement** > **Sélectionner les sites**.

[SDW-22374]

Parfois, l'interface utilisateur affiche une erreur après la configuration des paramètres de l'interface de gestion. Toutefois, la configuration est réussie et une actualisation est requise pour que les paramètres mis à jour apparaissent sur l'interface utilisateur.

[SDW-22139]

Dans une configuration gérée par un fournisseur, les annonces ajoutées par les administrateurs du fournisseur ne sont pas affichées aux clients lors de leur connexion.

[SDW-18491]

Notes de mise à jour pour la version 13.2.1 de SD-WAN Orchestrator pour locaux

October 21, 2022

Ce document de notes de mise à jour décrit les améliorations et les modifications, ainsi que les problèmes résolus et connus qui existent pour la version 13.2.1 de Citrix SD-WAN Orchestrator for On-premises.

Remarques

Ce document de notes de publication n'inclut pas les correctifs liés à la sécurité. Pour obtenir la liste des correctifs et des conseils liés à la sécurité, consultez le bulletin de sécurité Citrix.

Problèmes résolus

Les problèmes résolus dans la version 13.2.1.

Plateforme et systèmes

Citrix SD-WAN Orchestrator pour locaux envoie des paquets de synchronisation TCP au point de terminaison AWS.

[SDW-23477]

Problèmes connus

Les problèmes qui existent dans la version 13.2.1.

Divers

Certains sites ne peuvent pas se connecter à Citrix SD-WAN Orchestrator pour l'interface utilisateur locale.

Solution : utilisez un sous-réseau différent du sous-réseau 172.17.x.x.

[SDWANHELP-2601]

Dans certains scénarios, après avoir déployé Cloud Direct pour les sites et poussé les configurations (préparation et activation), le service Cloud Direct ne s'affiche pas.

Solution : activez le service Cloud Direct manuellement pour chaque site.

[SDW-22493]

La version logicielle précédemment sélectionnée sur la page **Déploiement** > **Paramètres** > **Mise à niveau partielle du site** > **Version logicielle** de l'interface utilisateur n'est pas conservée lorsque les utilisateurs reviennent sur cette page.

Solution : sélectionnez manuellement la version partielle du logiciel de mise à niveau du site pour chaque site en accédant à **Déploiement** > **Sélectionner des sites**.

[SDW-22374]

Parfois, l'interface utilisateur affiche une erreur après la configuration des paramètres de l'interface de gestion. Toutefois, la configuration est réussie et une actualisation est requise pour que les paramètres mis à jour apparaissent sur l'interface utilisateur.

[SDW-22139]

Dans une configuration gérée par un fournisseur, les annonces ajoutées par les administrateurs du fournisseur ne sont pas affichées aux clients lors de leur connexion.

[SDW-18491]

Plateforme et systèmes

L'interface utilisateur de l'une des appliances Citrix SD-WAN n'est pas accessible car le fournisseur de statistiques réseau réutilise une session, ce qui a entraîné un comportement incorrect du processus HTTPD (dans de rares cas).

[SDW-23392]

Sur l'appliance Citrix SD-WAN 210, si vous supprimez la licence complémentaire SE, les services sont désactivés.

Solution : avant de supprimer une licence complémentaire SE (ou) de passer d'une licence AE à une licence SE, supprimez les politiques de pare-feu associées au profil de sécurité, configurez l'appliance en tant que gestion hors bande (si la gestion intrabande est configurée), puis passez à l'étape et au processus d'activation pour convertir l'appliance en édition standard.

[SDW-18031]

Notes de mise à jour pour la version 13.2 de SD-WAN Orchestrator pour locaux

October 21, 2022

Ce document de notes de mise à jour décrit les améliorations et les modifications, ainsi que les problèmes résolus et connus qui existent pour la version 13.2 de Citrix SD-WAN Orchestrator for On-premises.

Remarques

Ce document de notes de publication n'inclut pas les correctifs liés à la sécurité. Pour obtenir la liste des correctifs et des conseils liés à la sécurité, consultez le bulletin de sécurité Citrix.

Nouveautés

Les améliorations et modifications disponibles dans la version 13.2.

Configuration et gestion

Restaurer la version précédente

Citrix SD-WAN Orchestrator pour locaux introduit la fonctionnalité de restauration de la version précédente. Lorsque l'option **Restaurer la version précédente** est sélectionnée, Citrix SD-WAN Orchestrator pour locaux lance une activation à l'échelle du réseau de la configuration précédente et restaure la configuration (/le logiciel) précédemment activée sur votre réseau.

[SDW-22042]

Améliorations apportées

Une fois les licences récupérées et mises à niveau vers la production, l'étiquette du bouton **Mettre à niveau vers la production** devient Mise à **niveau vers la production**, indiquant que la mise à niveau de la licence est déjà effectuée.

[SDW-20674]

API - Résolution de l'adresse du site :

Lorsqu'un site est créé à l'aide d'une API, son adresse est automatiquement obtenue à l'aide des valeurs de latitude et de longitude, transmises lors de la création du site, à l'aide de l'API Google Maps.

[SDW-20654]

Restructuration du menu réseau

Le menu Citrix SD-WAN Orchestrator pour la configuration globale sur site a été restructuré afin de permettre une meilleure catégorisation et une meilleure découvrabilité des fonctions clés de Citrix SD-WAN. De plus, chaque service de livraison est désormais disponible à la fois dans les canaux de

distribution et dans chaque page de fonctions clés afin de répondre à la configuration administrative à partir d'un contexte global ou par fonction. Par exemple, un administrateur peut configurer le service Citrix SIA globalement via un canal de distribution le jour 0 et peut également exécuter les fonctions Day N sous Sécurité sous Cloud Security Services pour apporter des modifications.

Les pages de configuration au niveau du réseau sont améliorées comme suit :

- **Network Config Home** est renommé **Network Home**.
- **Les services de livraison** sous **Configuration > Canaux de distribution** sont désormais renommés en **Définitions de services**.
- Sous **Configuration > Sécurité**, la page **Chiffrement réseau** est renommée **Sécurité réseau**.
- Les pages situées sous **Configuration > Sécurité** sont regroupées de manière logique comme suit pour faciliter leur découverte :

Groupe	Options du menu
Sécurité de superposition SD-WAN	Sécurité du réseau
	Chemin virtuel IPsec
Firewall de base	Zone de pare-feu
	Paramètres par défaut du pare-feu
	Stratégies de pare-feu
IPsec et GRE	Certificats
	Profils de chiffrement IPSec
	Service IPsec
	Service GRE
Sécurité Wi-Fi	Profils RADIUS
	Profils SSID

- Vous pouvez configurer les services suivants depuis **Configuration > Canaux de distribution > Définition du service** ou depuis **Configuration > Sécurité** :
  - IPSec
  - GRE
- La page **Groupes ECMP** est déplacée sous **Configuration > Routage**.
- Vous pouvez configurer le **BGP, l'OSPF, les groupes de multidiffusion et le VRRP** au niveau du réseau sous **Configuration > Routage**. Vous pouvez sélectionner un site et cliquer sur **OK**. Il

vous amène à la page de configuration spécifique au niveau du site. Auparavant, ces configurations n'étaient disponibles qu'au niveau du site.

- Vous pouvez configurer le service Cloud Direct depuis **Configuration > Canaux de diffusion > Définition du service** ou depuis **Configuration > Routage > SaaS et Cloud On Ramp**
- La page des **paramètres de l'application et du DNS** est renommée en **Paramètres de l'application et des groupes**.
- Les paramètres relatifs au DPI qui se trouvaient précédemment sous **Configuration > Paramètres de l'application et du DNS > Paramètres de l'application** sont déplacés sous **Configuration > Paramètres de l'application et groupes > Paramètres DPI**.
- La page**Service de localisation réseau** qui se trouvait sous **Configuration > Services de livraison** est placée directement sous **Configuration.**

[SDW-14698]

Annulation en cas d'erreur

Lors du déploiement réseau (activation), les sites qui ne parviennent pas à se connecter à Citrix SD-WAN Orchestrator for On-premises sont restaurés vers la version précédente pour tenter de restaurer la connectivité. La restauration sur ces sites est initiée lorsque la publication est hors ligne pendant un certain temps (actuellement 30 minutes).

Si l'un des sites du réseau tente de revenir en arrière, une fenêtre contextuelle apparaît avec deux options permettant de restaurer l'ensemble du réseau ou d'ignorer ces sites et de mettre fin au déploiement.

La fonction Rollback on Error doit être activée avant de lancer un déploiement réseau.

[SDW-11153]

Divers

Règles IP

L'option Override Service est ajoutée dans la section **Règles IP > Politique de trafic de chemin virtuel** . Lorsque la **politique de trafic** est sélectionnée en tant que **service de remplacement**, vous pouvez sélectionner le type de service Intranet, Internet, relais ou Discard auquel le service de chemin virtuel remplace.

[SDW-22213]

Différence de configuration

Une fonctionnalité **Config Diff** vient d'être ajoutée au niveau du réseau sous **Configuration**. La fonctionnalité **Config Diff** vous permet de vérifier la différence entre deux versions de points de contrôle

de configuration. Vous pouvez également consulter les configurations à la fois au niveau global et au niveau du site.

[SDW-4563]

Paramètres de l'appliance

Citrix SD-WAN Orchestrator pour locaux introduit une option permettant de configurer la priorité du réseau de gestion. Vous pouvez sélectionner In-Band ou Out-of-band comme interface de gestion pour votre réseau. Cette option n'est disponible que si l'appliance SD-WAN exécute une version logicielle de la version 11.4.2 ou ultérieure.

[NSSDW-35774]

Plateforme et systèmes

Authentification du certificat

Citrix SD-WAN Orchestrator pour locaux prend en charge l'authentification des appliances pour les chemins virtuels statiques et dynamiques à l'aide de l'infrastructure à clé publique (PKI) en tant que fonctionnalité de sécurité supplémentaire. L'activation de la fonctionnalité étend le mécanisme d'authentification de chemin virtuel existant en distribuant les certificats PKI sur le chemin de données, par l'appliance initiant l'échange. L'amélioration de l'ICP prend également en charge la gestion des listes de révocation de certificats (CRL) pour la révocation centralisée des certificats compromis.

[SDW-19295]

Améliorations apportées aujournal d'audit des fournisseurset au journal

Les pages **Journaux d'audit des fournisseurs** et **Journaux d'audit du réseau** sont améliorées avec les options suivantes :

- **IP source** : ce champ affiche l'adresse IP du point de terminaison à partir duquel une fonctionnalité SD-WAN est configurée. Ce champ s'affiche sur la page **Journaux d'audit** et sur la page **Informations d'audit** .
- **Exporter au format CSV** : cette option vous permet d'exporter les journaux d'audit au format CSV.
- **Ce qui a changé** : cette section affiche les journaux de toutes les modifications apportées aux fonctionnalités via l'interface utilisateur. Activez le bouton **Log Payloads** pour afficher cette section sur la page **Informations d'audit** . Cette section est actuellement disponible sur la page Informations sur l'audit du réseau.

[SDW-19219]

Ports personnalisés, configuration du protocole pour les applications basées sur des noms de domaine

Les applications basées sur les noms de domaine prennent désormais en charge les ports et le protocole configurables dans Citrix SD-WAN Orchestrator for On-premises. Lorsque vous activez la case à cocher **Configurer le port**, vous pouvez modifier, ajouter ou supprimer n'importe quel port ou la plage de ports selon vos besoins. Vous pouvez également modifier/sélectionner le protocole en tant que TCP, UDP ou N'importe lequel. Auparavant (et avec la case à cocher Configurer le port désactivée), seuls les ports 80 et 443 et le protocole **Any** étaient pris en charge pour les domaines regroupés sous une application.

[NSSDW-29930]

Problèmes résolus

Les problèmes résolus dans la version 13.2.

Divers

L'interface utilisateur Citrix SD-WAN Orchestrator pour site est inaccessible. Ce problème se produit lorsque les services exécutés dans {page.productname}} ne répondent pas aux demandes de pulsation et que la limite de redémarrage est dépassée.

[SDWANHELP-254]

Le téléchargement du package de mise à niveau logicielle échoue sur Citrix SD-WAN Orchestrator for On-premises. Ce problème se produit lorsqu'un utilisateur quitte la page de téléchargement alors que le téléchargement du package logiciel est en cours.

[SDWANHELP-2495]

Plateforme et systèmes

Une appliance SD-WAN exécutant une version logicielle de la version 11.4.1 passe en mode Grace lorsque des licences sont attribuées à l'appliance par Citrix SD-WAN Orchestrator for On-premises.

[SDW-23171]

Problèmes connus

Les problèmes qui existent dans la version 13.2.

Configuration et gestion

Sur une instance Citrix SD-WAN Orchestrator for On-premises récemment importée, le staging est bloqué dans l'état **Préparation du package** . Ce problème se produit lorsque le processus de transfert est lancé peu de temps après la création d'une nouvelle machine virtuelle.

Solution : réessayez le processus de mise en scène.

[SDW-20863]

Divers

L'état de service d'une appliance SD-WAN exécutant une version logicielle de la version 11.4.2 est affiché comme **BAD** sur l'interface utilisateur Citrix SD-WAN Orchestrator for On-premises. Le message d'erreur affiché est « **Aucune réponse de l'URL d'Orchestrator »**. Ce problème se produit lorsqu'un domaine personnalisé est configuré dans Citrix SD-WAN Orchestrator pour locaux.

Solution : redémarrez l'appliance SD-WAN.

[SDW-23322]

L'opération de **restauration de la version précédente** échoue avec le message d'erreur **Échec de l'activation (ER101)** pour les sites sur PSU lorsque la liste de mise à niveau partielle des sites est modifiée et qu'une gestion des modifications (étape et activation) est effectuée sur un réseau.

Solution : effectuez un nouveau cycle de gestion des modifications avant d'appliquer l'action **Restaurer la version précédente** .

[SDW-23227]

Dans certains scénarios, après avoir déployé Cloud Direct pour les sites et poussé les configurations (étape et activation), le service Cloud Direct ne s'affiche pas.

Solution : activez le service Cloud Direct manuellement pour chaque site.

[SDW-22493]

La version logicielle précédemment sélectionnée sur la page **Déploiement** > **Paramètres** > **Mise à niveau partielle du site** > **Version logicielle** de l'interface utilisateur n'est pas conservée lorsque les utilisateurs reviennent sur cette page.

Solution : sélectionnez manuellement la version partielle du logiciel de mise à niveau du site pour chaque site en cliquant sur **Déploiement** > **Sélectionner les sites**.

[SDW-22374]

Parfois, l'interface utilisateur affiche une erreur après la configuration des paramètres de l'interface de gestion. Toutefois, la configuration est réussie et une actualisation est requise pour que les paramètres mis à jour apparaissent sur l'interface utilisateur.

[SDW-22139]

Dans une configuration gérée par un fournisseur, les annonces ajoutées par les administrateurs du fournisseur ne sont pas affichées aux clients lors de leur connexion.

[SDW-18491]

Plateforme et systèmes

Le client n'est pas en mesure d'envoyer une notification push à son propre serveur HTTP.

[SDW-23134]

Notes de mise à jour pour la version 12.3 de SD-WAN Orchestrator pour locaux

July 14, 2023

Ce document de notes de mise à jour décrit les améliorations et les modifications, ainsi que les problèmes résolus et connus qui existent pour la version 12.3 de Citrix SD-WAN Orchestrator for On-premises.

Remarque

Ce document de notes de publication n'inclut pas les correctifs liés à la sécurité. Pour obtenir la liste des correctifs et des conseils liés à la sécurité, consultez le bulletin de sécurité Citrix.

Nouveautés

Les améliorations et modifications disponibles dans la version 12.3.

Divers

Paramètres de purge

Citrix SD-WAN Orchestrator pour locaux vous permet d'effacer les données historiques antérieures à l'intervalle des statistiques de purge (30 jours par défaut). Lorsque les données sont effacées, les données historiques antérieures au nombre de jours sélectionné sont supprimées et ne sont plus disponibles. Le processus de purge a lieu vers 0h48 tous les jours en fonction du fuseau horaire défini sur votre appliance SD-WAN.

[SDW-20402]

Interface de déploiement sans contact

Vous pouvez activer une interface Zero Touch Deployment (ZTD) sur Citrix SD-WAN Orchestrator pour les applications locales. L'interface ZTD sécurisée par une authentification bidirectionnelle fournit une interface de communication sécurisée pour les appliances SD-WAN et Citrix SD-WAN Orchestrator pour les applications sur site.

[SDW-19152]

Paramètres du chemin virtuel pour le lien

Vous pouvez personnaliser les largeurs de bande pour les chemins virtuels et les chemins virtuels dynamiques associés à une liaison WAN. Cette fonctionnalité est utile lorsque certains sites affichent des signes de dégradation des performances en raison de problèmes de bande passante.

[SDW-9760]

SD-WAN Orchestrator

Paramètres du serveur Syslog

Citrix SD-WAN Orchestrator pour locaux prend en charge la configuration des paramètres du serveur Syslog pour les appliances SD-WAN. En activant les paramètres Syslog, vous pouvez envoyer des alertes système et les détails des événements des appliances SD-WAN à un serveur Syslog externe.

[SDW-13990]

Problèmes résolus

Les problèmes résolus dans la version 12.3.

Divers

Dans certaines conditions, l'appliance SD-WAN ne parvient pas à communiquer avec Citrix SD-WAN Orchestrator pour la gestion sur site via intrabande lorsque la gestion intrabande est activée et que la gestion hors bande est connectée.

[SDWANHELP-2368]

L'interface utilisateur affiche incorrectement une erreur lorsque la valeur des chemins virtuels dynamiques est définie sur plus de 8, alors que la limite maximale autorisée est de 32. Ce problème est observé sur les appliances VPXL et 4100 SE.

[SDWANHELP-2354]

La liste déroulante des **versions du logiciel** située sous les paramètres de mise à niveau partielle du site affiche toutes les versions logicielles prises en charge au lieu d'afficher uniquement les versions publiées sous **Infrastructure** > **Administration de l'orchestrateur** > **Images logicielles** > **Appareil.

Si une version logicielle répertoriée dans Mise à niveau partielle du site n'est pas disponible pour publication sous **Infrastructure** > **Administration de l'orchestrateur** > **Images logicielles** > **Appliance**, la mise à niveau partielle du site ne peut pas être effectuée pour cette version.

[SDW-20992]

Problèmes connus

Les problèmes qui existent dans la version 12.3.

Configuration et gestion

Sur une instance Citrix SD-WAN Orchestrator for On-premises récemment importée, le staging est bloqué dans l'état **Préparation du package** . Ce problème se produit lorsque le processus de transfert est lancé peu de temps après la création d'une nouvelle machine virtuelle.

Solution : réessayez le processus de mise en scène.

[SDW-20863]

Divers

Citrix SD-WAN Orchestrator pour l'exécution locale de VMware ESXi 13 ne parvient pas à redémarrer et tombe en mauvais état.

Solution : utilisez VMware ESXi version 9.

[SDWANHELP-2182]

Dans certains scénarios, après avoir déployé Cloud Direct pour les sites et poussé les configurations (étape et activation), le service Cloud Direct ne s'affiche pas.

Solution : activez le service Cloud Direct manuellement pour chaque site.

[SDW-22493]

Le processus de mise en œuvre échoue par intermittence lorsque les utilisateurs effectuent une mise à niveau partielle du site. L'interface utilisateur affiche le message d'erreur **Staging failure due à une exception**.

Solution : réessayez le processus de mise en scène.

[SDW-22398]

La version logicielle précédemment sélectionnée sur la page **Déploiement** > **Paramètres** > **Mise à niveau partielle du site** > **Version logicielle** de l'interface utilisateur n'est pas conservée lorsque les utilisateurs reviennent sur cette page.

Solution : sélectionnez manuellement la version partielle du logiciel de mise à niveau du site pour chaque site en cliquant sur **Déploiement** > **Sélectionner les sites**.

[SDW-22374]

Parfois, l'interface utilisateur affiche une erreur après la configuration des paramètres de l'interface de gestion. Toutefois, la configuration est réussie et une actualisation est requise pour que les paramètres mis à jour apparaissent sur l'interface utilisateur.

[SDW-22139]

Les utilisateurs ne peuvent pas supprimer le fichier image Citrix SD-WAN Orchestrator for On-premises **tar.gz** chargé sur la page **Infrastructure** > **Administration de l'orchestrateur** > **Images logicielles** de l'interface utilisateur. Le message d'erreur affiché est **Une erreur s'est produite lors de la suppression du package logiciel**.

Solution : chargez un nouveau package logiciel. Le fichier précédemment chargé est automatiquement supprimé.

[SDW-22137]

Sur la page d'**accueil**Configuration > Configuration**réseau** de l'interface utilisateur, l'état de connectivité d'Orchestrator pour une appliance SD-WAN secondaire apparaît en ligne immédiatement après le téléchargement du fichier de configuration. Toutefois, l'état correct s'affiche une fois la configuration enregistrée pour le site.

[SDW-20913]

Dans une configuration gérée par un fournisseur, les annonces ajoutées par les administrateurs du fournisseur ne sont pas affichées aux clients lors de leur connexion.

[SDW-18491]

Lorsque la sauvegarde de la base de données d'une appliance est restaurée sur une autre appliance utilisant la même version de Citrix SD-WAN Orchestrator for On-premises, les détails de l'utilisateur ne sont pas restaurés. Sur l'appliance restaurée, si vous créez un utilisateur avec le même nom d'utilisateur que dans la base de données sauvegardée, l'erreur suivante s'affiche :

`User has a role already assigned`.

Solution : créez un utilisateur avec un nom d'utilisateur différent qui n'existait pas dans la base de données sauvegardée.

[SDW-15984]

Plateforme et systèmes

Dans l'appliance Citrix SD-WAN 210, si vous supprimez la licence complémentaire, les services sont désactivés.

Solution : supprimez la politique de pare-feu comportant un profil de sécurité, organisez et activez les modifications pour convertir l'appliance en édition standard.

[SDW-18031]

Notes de mise à jour pour la version 11.4.0a de SD-WAN Orchestrator pour locaux

July 14, 2023

Ce document de notes de mise à jour décrit les améliorations et les modifications, ainsi que les problèmes résolus et connus qui existent pour la version 11.4.0a de Citrix SD-WAN Orchestrator for On-premises.

Remarques

- Citrix SD-WAN Orchestrator pour locaux 11.4.0a résout le problème décrit dans SDWANHELP-2317 et remplace la version 11.4.
- Ce document de notes de publication n'inclut pas les correctifs liés à la sécurité. Pour obtenir la liste des correctifs et des conseils liés à la sécurité, consultez le bulletin de sécurité Citrix.

Nouveautés

Les améliorations et les modifications disponibles dans la version 11.4.0a.

Configuration et gestion

Proxy HTTP

Vous pouvez configurer les paramètres du proxy HTTP sur Citrix SD-WAN Orchestrator pour les applications locales. Cette fonctionnalité centralise la gestion de toutes les demandes sortantes adressées à Citrix Cloud. Les administrateurs peuvent acheminer les demandes sortantes depuis Citrix SD-WAN Orchestrator pour site local vers Citrix Cloud via un serveur proxy HTTP.

[SDW-20247]

Service Cloud Direct

Citrix SD-WAN Orchestrator pour locaux prend en charge le service Cloud Direct.

Le service Cloud Direct fournit des fonctionnalités SD-WAN en tant que service cloud grâce à une distribution fiable et sécurisée de tout le trafic lié à Internet, quel que soit l'environnement hôte (centre de données, cloud et Internet).

Le service Cloud Direct améliore la visibilité et la gestion du réseau. Il permet aux partenaires d'offrir à leurs clients finaux des services SD-WAN gérés pour les applications SaaS critiques.

[SDW-16396]

Gestion du stockage - Disponibilité générale

La fonctionnalité de gestion du stockage prend désormais en charge la disponibilité générale.

Citrix SD-WAN Orchestrator pour locaux prend en charge la migration de la configuration et des données d'un disque vers un autre. Vous pouvez effectuer une migration de disque pour augmenter l'espace disque ou pour une reprise après sinistre.

- **Ajouter un nouveau disque** : vous pouvez ajouter un nouveau disque dont la taille de stockage est au moins deux fois supérieure à celle des données actuelles consommées par Citrix SD-WAN Orchestrator pour locaux.
- **Reprise après sinistre** : en cas de sinistre, vous pouvez joindre le disque contenant le Citrix SD-WAN Orchestrator pour la configuration et les données sur site à une nouvelle instance de Citrix SD-WAN Orchestrator pour machine virtuelle locale.

[SDW-21316]

Déploiement Zero Touch négocié dans le cloud - Disponibilité générale

La fonctionnalité de déploiement Zero Touch, négociée dans le cloud, prend désormais en charge la disponibilité générale.

Le déploiement Zero Touch, négocié dans le cloud, est un processus automatisé qui implique Citrix SD-WAN Orchestrator for On-premises en tant que broker pour établir la connectivité entre Citrix SD-WAN Orchestrator pour locaux et les appliances Citrix SD-WAN.

[SDW-21312]

Version 11.4.1 de Citrix SD-WAN

La version 11.4.1 de Citrix SD-WAN est prise en charge sur Citrix SD-WAN Orchestrator pour locaux 11.4.

[SDW-21082]

Plateforme et systèmes

Sondage ICMP

Citrix SD-WAN Orchestrator pour locaux prend en charge le sondage ICMP. Il permet aux administrateurs de déterminer l'accessibilité à Internet vers/depuis l'appliance SD-WAN et l'hôte de destination. Les services ICMP suivants sont introduits dans l'interface utilisateur :

- Déterminer l'accessibilité à Internet à partir d'une liaison à l'aide de sondes ICMP
- Adresse du point de terminaison ICMP IPv4
- Intervalle entre les sondes (en secondes)
- Retries

[SDW-19292]

Annuler les paramètres du nœud de transit global

Vous pouvez désormais annuler les paramètres des nœuds de transit globaux et choisir d'activer ou de désactiver le transfert en étoile et l'exportation d'itinéraires uniquement sur les nœuds de transit de contrôle sélectionnés.

[SDW-19276]

API de statistiques sur les parcours des membres (version préliminaire) :

L'API de statistiques sur les chemins des membres est modifiée pour permettre au client de l'API de spécifier les champs d'intérêt. Les champs spécifiés sont renvoyés dans la charge utile de réponse.

[SDW-18903]

Rapports du site : VRRP

Le rapport VRRP fournit un rapport en temps réel sur les groupes VRRP configurés.

[SDW-12082]

Rapports du site : IGMP

Le tableau des rapports IGMP fournit un rapport en temps réel sur les statistiques IGMP et les groupes de proxy IGMP.

[SDW-12077]

Rapports du site : IPsec

Les rapports IPsec fournissent un rapport en temps réel sur les configurations des tunnels IPsec sur votre réseau.

[SDW-12076]

Rapports de site : protocoles de routage

Le rapport sur **les protocoles de routage** fournit les détails des paramètres associés aux protocoles de routage. Vous pouvez choisir le protocole dans la liste déroulante **Afficher** un domaine de routage dans la liste déroulante **Domaine de routage** selon vos besoins. Pour afficher les données actuelles, cliquez sur **Récupérer les dernières données**.

[SDW-12075]

Journaux d'audit des fournisseurs, journaux d'audit réseau

Les pages du journal d'audit au niveau du fournisseur et au niveau du réseau ont été améliorées avec les fonctionnalités suivantes :

- **Recherche** : Possibilité de rechercher une activité d'audit en fonction d'un mot clé.
- **Filtrage** : exécutez une recherche dans le journal d'audit en filtrant en fonction de l'utilisateur, de la fonctionnalité et de la plage horaire. Pour les journaux au niveau du réseau, vous pouvez également filtrer par site.
- **Informations d'audit** : sélectionnez l'icône d'informations dans la colonne **Action** pour accéder à la section **Informations sur l'audit** . Cette section fournit les informations suivantes :
- **Méthode : méthode**de requête HTTP de l'API invoquée.
- **État** : résultat de la demande d'API. Un message d'erreur s'affiche lorsque la demande d'API échoue.
- **Message de charge utile** : corps du message de demande envoyé via l'API.
- **URL** : URL HTTP de l'API révoquée.
- **Enregistrer les charges utiles** : par défaut, cette option est désactivée. Lorsque cette option est activée, le corps de requête du message d'API s'affiche dans la section **Informations d'audit** .

[SDW-18937]

Élément de sélection du site

La facilité d'utilisation du composant de sélection de sites dans les configurations suivantes est améliorée du point de vue de sa facilité d'utilisation :

1. Mise à niveau partielle du
2. Service de localisation du réseau
3. Règles de routage
4. Politiques de QoS
5. Filtres d'itinéraire d'importation
6. Exporter les filtres d'
7. Config automatique du proxy
8. Prévention des intrusions
9. Stratégies pare-feu
10. Paramètres de l'application

[SDW-16895]

Problèmes résolus

Les problèmes résolus dans la version 11.4.

Divers

La fonctionnalité ZTD négociée dans le cloud dépend du service SD-WAN Orchestrator pour fonctionner. Ce problème sera résolu dans une prochaine version de SD-WAN Orchestrator. Toutefois, les clients n'ont pas besoin de mettre à niveau leur Citrix SD-WAN Orchestrator pour les applications locales.

[SDW-20307]

La configuration ZTD du cloud SD-WAN ne fonctionne pas pour les sites HA si le ZTD cloud est déjà configuré sur un site principal.

[SDW-20208]

Citrix SD-WAN Orchestrator pour locaux affiche l'état **Non connecté** bien que l'appliance SD-WAN soit connectée à Citrix SD-WAN Orchestrator pour locaux.

[SDW-18280]

Problèmes connus

Les problèmes qui existent dans la version 11.4.

Configuration et gestion

Sur une instance Citrix SD-WAN Orchestrator for On-premises récemment importée, le staging est bloqué dans l'état **Préparation du package** . Ce problème se produit lorsque le processus de transfert est lancé peu de temps après la création d'une nouvelle machine virtuelle.

Solution : réessayez le processus de mise en scène.

[SDW-20863]

Divers

Le processus de mise en œuvre échoue lorsque les utilisateurs exécutant Citrix SD-WAN Orchestrator for On-premises 11.4 mettent à niveau leurs appliances Citrix SD-WAN vers la version 11.4.1. L'interface utilisateur affiche l'état **Échec de la mise en scène (échec du téléchargement des fichiers de script)**. Ce problème se produit lorsque la bande passante entre l'appliance Citrix SD-WAN et Citrix SD-WAN Orchestrator pour locaux est inférieure.

[SDWANHELP-2317]

Citrix SD-WAN Orchestrator pour l'exécution locale de VMware ESXi 13 ne parvient pas à redémarrer et tombe en mauvais état.

Solution : utilisez VMware ESXi version 9.

[SDWANHELP-2182]

L'interface utilisateur affiche une version logicielle de l'appliance SD-WAN incorrecte sur les pages **Configuration > Configurationréseau > Accueil**et**Configuration**>**Déploiement** . Ce problème se produit sur Citrix SD-WAN Orchestrator pour les instances locales récemment installées et avant que les utilisateurs n'effectuent une gestion des modifications.

[SDW-21018]

L'interface utilisateur n'affiche pas de message d'erreur lorsque le fonctionnement du site Cloud Direct échoue.

[SDW-21009]

La liste déroulante des **versions du logiciel** située sous les paramètres de mise à niveau partielle du site affiche toutes les versions logicielles prises en charge au lieu d'afficher uniquement les versions publiées sous **Infrastructure** > **Administration de l'orchestrateur** > **Images logicielles** > **Appareil.

Si une version logicielle répertoriée dans Mise à niveau partielle du site n'est pas disponible pour publication sous **Infrastructure** > **Administration de l'orchestrateur** > **Images logicielles** > **Appliance**, la mise à niveau partielle du site ne peut pas être effectuée pour cette version.

[SDW-20992]

Sur la page d'**accueil**Configuration > Configuration**réseau** de l'interface utilisateur, l'état de connectivité d'Orchestrator pour une appliance SD-WAN secondaire apparaît en ligne immédiatement après le téléchargement du fichier de configuration. Toutefois, l'état correct s'affiche une fois la configuration enregistrée pour le site.

[SDW-20913]

Dans une configuration gérée par un fournisseur, les annonces ajoutées par les administrateurs du fournisseur ne sont pas affichées aux clients lors de leur connexion.

[SDW-18491]

Lorsque la sauvegarde de la base de données d'une appliance est restaurée sur une autre appliance utilisant la même version de Citrix SD-WAN Orchestrator for On-premises, les détails de l'utilisateur ne sont pas restaurés. Sur l'appliance restaurée, si vous créez un utilisateur avec le même nom d'utilisateur que dans la base de données sauvegardée, l'erreur suivante s'affiche :

```
User has a role already assigned
```

Solution : créez un utilisateur avec un nom d'utilisateur différent qui n'existait pas dans la base de données sauvegardée.

[SDW-15984]

Notes de mise à jour pour la version 11.1 de Citrix SD-WAN Orchestrator pour locaux

July 14, 2023

Ce document de notes de mise à jour décrit les améliorations et les modifications, ainsi que les problèmes résolus et connus qui existent pour la version 11.1 de Citrix SD-WAN Orchestrator pour locaux.

Remarques

Ce document de notes de publication n'inclut pas les correctifs liés à la sécurité. Pour obtenir la liste des correctifs et des conseils liés à la sécurité, consultez le bulletin de sécurité Citrix.

Nouveautés

Améliorations et modifications disponibles dans la version 11.1.

Version 11.4.0a de Citrix SD-WAN

La version 11.4.0a de Citrix SD-WAN est prise en charge dans Citrix SD-WAN Orchestrator pour locaux.

[SDW-19785]

Version 11.3.2 de Citrix SD-WAN

La version 11.3.2 de Citrix SD-WAN est prise en charge dans Citrix SD-WAN Orchestrator pour locaux.

[SDW-19038]

Synthèse des itinéraires

Citrix SD-WAN Orchestrator pour locaux apporte une amélioration à la fonctionnalité de synthèse des itinéraires. Grâce à cette amélioration, vous pouvez ajouter des itinéraires récapitulatifs sans spécifier l'adresse IP de la passerelle.

[SDW-19404]

Équilibrage de charge ECMP

Les groupes ECMP (Equal Cost Multi-Path) vous permettent de regrouper plusieurs itinéraires, avec le même coût, la destination et le même type de service. L'équilibrage de charge ECMP garantit :

- Répartition du trafic sur plusieurs connexions à coût égal.
- Utilisation optimale de la bande passante disponible.
- Transfert dynamique du trafic vers un autre itinéraire membre ECMP, si un itinéraire devient inaccessible.
- Les groupes ECMP peuvent être formés via des chemins virtuels et des services Intranet.

[SDW-17452]

Gestion du stockage (version préliminaire)

Citrix SD-WAN Orchestrator pour locaux prend en charge la migration de la configuration et des données d'un disque vers un autre. Vous pouvez effectuer une migration de disque pour augmenter l'espace disque ou pour une reprise après sinistre.

- **Ajouter un nouveau disque** : vous pouvez ajouter un nouveau disque dont la taille de stockage est au moins deux fois supérieure à celle des données actuelles consommées par Citrix SD-WAN Orchestrator pour locaux.
- **Reprise après sinistre** : en cas de sinistre, vous pouvez joindre le disque contenant le Citrix SD-WAN Orchestrator pour la configuration et les données sur site à une nouvelle instance de Citrix SD-WAN Orchestrator pour machine virtuelle locale.

[SDW-16404]

Déploiement Zero Touch négocié dans le cloud (version préliminaire)

Le déploiement Zero Touch, négocié dans le cloud, est un processus automatisé qui implique Citrix SD-WAN Orchestrator for On-premises en tant que broker pour établir la connectivité entre Citrix SD-WAN Orchestrator pour locaux et les appliances Citrix SD-WAN.

[SDW-11614]

Améliorations des nœuds

L'activation de la communication hub-and-spoke dans le cadre des paramètres globaux permet à tous les sites d'utiliser les nœuds de contrôle comme nœuds de transit, par défaut, pour la communication de site à site. Les préférences spécifiques au site pour les nœuds de transit de superposition virtuels vous permettent de remplacer les paramètres globaux des nœuds de transit virtuels de superposition

pour tous les sites de votre réseau. Vous pouvez également choisir un nœud autre que le contrôle comme nœud de transit principal d'un site.

[SDW-12443]

Support du plan de données IPv6

Citrix SD-WAN Orchestrator pour locaux prend en charge les adresses IPv6 pour les configurations d'appliance Citrix SD-WAN suivantes avec le logiciel Citrix SD-WAN version 11.3.1 ou supérieure :

- Serveur DNS
- Flux
- Connexions pare-feu
- Groupes IP
- Régions
- Client DHCP
- Règles IP et règles d'application
- Traduction d'adresses réseau
- Service GRE
- Interfaces
- Service Internet
- Protocole de découverte de voisins
- Groupe de délégation de préfixe
- Service IPSec
- Paramètres HA
- Routes IP
- Gestion intrabande
- Paramètres DNS
- Ensemble d'options de serveur DHCP, de relais DHCP et de DHCP

[SDW-19194]

Problèmes résolus

Les problèmes qui sont résolus dans la version 11.1.

Les versions d'appliance SD-WAN inférieures à 11.2.0 ne peuvent pas se connecter à Citrix SD-WAN Orchestrator pour les versions locales inférieures à 11.1. Citrix SD-WAN Orchestrator pour locaux 11.1 est la version recommandée si les utilisateurs souhaitent connecter leurs appliances SD-WAN exécutant une version logicielle inférieure à la version 11.2.0.

[SDW-20220]

En cas d'échec de la mise à niveau du compte d'un client vers un compte de production, l'interface utilisateur n'affiche pas le message d'échec.

[SDW-19574]

La mise à niveau vers la production échoue dans Citrix SD-WAN Orchestrator pour locaux, pour les clients prépayés ne disposant que de licences perpétuelles.

[SDW-19558]

L'attribution de licences perpétuelles à des sites échoue dans Citrix SD-WAN Orchestrator pour les sites locaux.

[SDW-19556]

En cas d'échec lors de l'attribution de licences, l'interface utilisateur n'affiche pas le message d'échec sous **Administration** > **Licences**.

[SDW-19238]

Même si l'administrateur du client n'a pas accès à la suppression des serveurs d'authentification distants, l'interface utilisateur affiche l'icône de suppression. Toutefois, lorsque l'administrateur du client tente d'effectuer l'opération de suppression, l'erreur suivante s'affiche :

```
User is not authorized to perform this operation.
```

[SDW-18945]

Sur la page **Administration** > **Annonces** au niveau du fournisseur, si vous choisissez un client dans la barre de menu supérieure, une page blanche avec **Administration du réseau** comme titre s'affiche.

[SDW-18944]

Après avoir importé des droits de production valides, l'option de **mise à niveau vers la production** est disponible sous **Licences** avant même d'attribuer la licence à l'appliance.

[SDW-18721]

Problèmes connus

Les problèmes qui existent dans la version 11.1.

La fonctionnalité ZTD négociée dans le cloud dépend du service SD-WAN Orchestrator pour fonctionner. Ce problème sera résolu dans une prochaine version du service SD-WAN Orchestrator. Toutefois, les clients n'ont pas besoin de mettre à niveau leur Citrix SD-WAN Orchestrator pour les applications locales.

[SDW-20307]

Lorsque Citrix SD-WAN Orchestrator pour locaux est mis à niveau vers la version 11.1, les journaux d'audit collectés lors des versions précédentes affichent **sdwan-onprem-sp** en tant qu'utilisateur et le bouton de basculement des charges utiles du journal est activé sur l'interface utilisateur. Ces journaux sont effacés au bout de 92 jours.

[SDW-20305]

La configuration ZTD du cloud SD-WAN ne fonctionne pas pour les sites HA si le ZTD cloud est déjà configuré sur un site principal.

Solution :

1. Supprimez la configuration ZTD du cloud du site principal en accédant à **Administration** > **Paramètres ZTD** > **Cloud Brokered ZTD**.
2. Reconfigurez le site cloud ZTD pour les sites principaux et secondaires en même temps.

[SDW-20208]

La fonctionnalité de licence n'est pas prise en charge dans la configuration gérée par le fournisseur de Citrix SD-WAN Orchestrator pour locaux. Les fournisseurs peuvent continuer à utiliser les licences d'essai. Un délai de grâce de 60 jours est prévu.

[SDW-18831]

Lorsqu'une appliance perd sa connectivité à Citrix SD-WAN Orchestrator for On-premises pendant plus de 20 minutes et passe en phase de réenregistrement, elle envoie un numéro de série incorrect dans la demande d'enregistrement.

Solution : redémarrez l'appliance.

[SDW-18781]

Dans une configuration gérée par un fournisseur, les annonces ajoutées par les administrateurs du fournisseur ne sont pas affichées aux clients lors de leur connexion.

[SDW-18491]

Citrix SD-WAN Orchestrator pour locaux affiche l'état **Non connecté** bien que l'appliance SD-WAN soit connectée à Citrix SD-WAN Orchestrator pour locaux.

Solution : accédez à **Configuration** > **Network Config Home** et vérifiez l'état de connectivité de l'appliance sur l'interface utilisateur Citrix SD-WAN Orchestrator for On-premises.

[SDW-18280]

Lorsque la sauvegarde de la base de données d'une appliance est restaurée sur une autre appliance utilisant la même version de Citrix SD-WAN Orchestrator for On-premises, les détails de l'utilisateur ne sont pas restaurés. Sur l'appliance restaurée, si vous créez un utilisateur avec le même nom d'utilisateur que dans la base de données sauvegardée, l'erreur suivante s'affiche :

```
User has a role already assigned
```

Solution : créez un utilisateur avec un nom d'utilisateur différent qui n'existait pas dans la base de données sauvegardée.

[SDW-15984]

Citrix SD-WAN Orchestrator pour l'exécution locale de VMware ESXi 13 ne parvient pas à redémarrer et tombe en mauvais état.

Solution : utilisez VMware ESXi version 9.

[SDWANHELP-2182]

Notes de mise à jour pour la version 10.3 de Citrix SD-WAN Orchestrator pour locaux

October 21, 2022

Ce document de notes de mise à jour décrit les améliorations et les modifications, ainsi que les problèmes résolus et connus qui existent pour la version 10.3 de Citrix SD-WAN Orchestrator for On-premises.

Remarques

Ce document de notes de publication n'inclut pas les correctifs liés à la sécurité. Pour obtenir la liste des correctifs et des conseils liés à la sécurité, consultez le bulletin de sécurité Citrix.

Nouveautés

Améliorations et modifications disponibles dans la version 10.3.

Configuration et gestion

Routage dynamique

À partir de la version 11.3.1 de Citrix SD-WAN, vous pouvez configurer un ID de routeur pour l'ensemble du protocole et également un ID de routeur par domaine de routage. Grâce à cette amélioration, vous pouvez activer un routage dynamique stable sur plusieurs instances avec différents ID de routeur convergeant de manière stable.

[SDW-17097]

Réessayez la mise en scène

L'option Retry staging est désormais disponible pour relancer le transfert sur les sites où le processus de transfert a échoué.

[SDW-16538]

Application personnalisée

La case à cocher **Activer les rapports** vient d'être ajoutée pour les applications personnalisées basées sur le protocole IP. Vous pouvez désormais également consulter le trafic personnalisé défini par l'application basé sur le protocole IP et le nom de domaine sur la page **Rapports Utilisation** . L'option d'application personnalisée est également ajoutée en tant que type sur la page de **configuration de la qualité de l'application** .

[SDW-10862]

Divers

Configuration de secours

La configuration de secours garantit que l'appliance reste connectée au service de déploiement zéro contact en cas de panne de liaison, d'incompatibilité de configuration ou d'incompatibilité logicielle. La configuration de secours est activée par défaut sur les appliances disposant d'un profil de configuration par défaut. Si la configuration de secours est désactivée sur un site, vous pouvez l'activer via Citrix SD-WAN Orchestrator for On-premises.

[SDW-13978]

Flux

Vous pouvez désormais utiliser la section **Flux des** paramètres de l'appliance pour effectuer l'action suivante :

- Activer/désactiver le service Citrix Virtual WAN
- Redémarrer le routage dynamique
- Activer/désactiver les chemins virtuels
- Activer/désactiver les liens WAN

[SDW-13977]

Rôles d'administrateur réseau et d'administrateur de sécurité (version préliminaire)

Citrix SD-WAN Orchestrator pour locaux prend en charge les rôles suivants :

- **Provide-Network-Admin** : administrateur qui peut uniquement afficher et modifier les informations relatives au réseau.
- **Provider-Security-Admin** : administrateur qui peut uniquement consulter et modifier les informations relatives à la sécurité.
- **Customer-Network-Admin** : administrateur client qui peut uniquement consulter et modifier les informations relatives au réseau.
- **Customer-Security-Admin** : administrateur client qui peut uniquement consulter et modifier les informations relatives à la sécurité.

[SDW-13845]

Paramètres de l'appliance

Vous pouvez désormais configurer la date et l'heure, au niveau du site, via Citrix SD-WAN Orchestrator pour les applications locales. Vous pouvez configurer la date et l'heure manuellement ou via un serveur NTP et également définir le fuseau horaire.

[SDW-13321]

Support au niveau du fournisseur

Citrix SD-WAN Orchestrator pour locaux prend en charge la mutualisation. Grâce à la fonctionnalité d'hébergement mutualisé, plusieurs comptes clients peuvent être gérés à l'aide d'une seule instance Citrix SD-WAN Orchestrator pour une instance sur site. Vous pouvez utiliser l'un des types de configuration suivants.

- **Configuration gérée par le fournisseur** : les clients utilisent un Citrix SD-WAN Orchestrator pour un service sur site géré par des partenaires Citrix à l'aide de la fonctionnalité mutualisée.
- **Configuration gérée par le client** : les clients gèrent leur Citrix SD-WAN Orchestrator pour locaux en tant que service autogéré pour leur entreprise.

Dans le cadre de la prise en charge de la configuration gérée par le fournisseur, les fonctionnalités suivantes sont introduites :

- **Rôles** : Les rôles de niveau fournisseur suivants sont ajoutés :
  - Provider-Master-Admin-All
  - Provider-Master-Admin-Tenant
  - Provider-Master-ReadOnly-All
- **Tableau de bord** : une nouvelle page d'interface utilisateur est ajoutée qui fournit une vue d'ensemble de tous les clients SD-WAN gérés par un fournisseur.
- **Connectivité avec les appliances SD-WAN** : dans une configuration gérée par un fournisseur, seuls les fournisseurs ont la possibilité d'activer le type d'authentification et de régénérer le certificat Citrix SD-WAN Orchestrator for On-premises. Les clients ont la possibilité de télécharger le certificat de l'appliance.
- **Modèles de profil de site et modèles de liens WAN** : Les modèles permettent de créer des **profils de site** et des **profils de liens WAN** au niveau du client.
- **Publier le logiciel** : Citrix SD-WAN Orchestrator pour locaux permet aux administrateurs du fournisseur de télécharger la version du logiciel de l'appliance Citrix SD-WAN requise pour toutes les appliances de votre réseau. Les fournisseurs peuvent publier la version logicielle téléchargée. Le logiciel publié est téléchargé et stocké dans Citrix SD-WAN Orchestrator for On-premises. Les administrateurs clients peuvent déployer le logiciel publié sur toutes les appliances gérées par Citrix SD-WAN Orchestrator pour les applications sur site.

- **Administration** : Les administrateurs des fournisseurs peuvent configurer l'adresse IP de gestion, le DNS, les serveurs NTP et les serveurs d'authentification à distance.
- **Annonces** : les fournisseurs peuvent utiliser l'option **Annonces** pour envoyer des annonces ou des notifications à leurs clients.
- **Rapports** : Les **rapports sur les fournisseurs** fournissent une visibilité sur les alertes, les tendances d'utilisation et l'inventaire agrégé de tous les clients gérés par un fournisseur.

[SDW-12589]

Déploiement Zero Touch - Batch

Vous pouvez désormais importer un fichier CSV pour ajouter plusieurs sites simultanément pour Zero Touch Deployment. Un exemple de modèle téléchargeable est disponible dans l'interface utilisateur, téléchargez-le et fournissez tous les détails du site.

[SDW-12249]

Plateforme et systèmes

Rapports du site : Comptage des liens WAN

Les rapports de **mesure des liaisons WAN** fournissent des détails sur l'utilisation mesurée des liaisons WAN. Vous pouvez consulter les rapports pour obtenir des informations sur la consommation de données des liaisons WAN mesurées.

[SDW-8892]

Problèmes connus

Les problèmes qui existent dans la version 10.3.

Configuration et gestion

Pour la haute disponibilité intrabande, l'interface graphique ne dispose pas d'une option permettant de sélectionner la direction de la règle de destination avec le type de service Any, ce qui entraîne l'échec des règles sortantes. Le message d'erreur [EC818] Sur le nom du site : le type de service « any » ne peut pas être utilisé lorsque la direction est sortante.

[SDW-16968]

Divers

Même si l'administrateur du client n'a pas accès à la suppression des serveurs d'authentification distants, l'interface graphique affiche l'icône de suppression. Toutefois, lorsque vous essayez d'effectuer l'opération de suppression, l'erreur suivante s'affiche :

```
User is not authorized to perform this operation
```

[SDW-18945]

Sur la page **Administration > Annonces** au niveau du fournisseur, si vous choisissez un client dans la barre de menu supérieure, une page blanche avec **Administration du réseau** comme titre s'affiche.

[SDW-18944]

Vous ne pouvez pas restaurer la sauvegarde de base de données effectuée dans une configuration gérée par le fournisseur sur une configuration gérée par le client. De même, vous ne pouvez pas restaurer la sauvegarde de base de données effectuée dans une configuration gérée par le client sur une configuration gérée par le fournisseur.

[SDW-18904]

Lorsque le rôle customer-security-admin disposant d'un accès en lecture seule à la configuration du site tente de modifier la configuration, au lieu d'afficher un accès non autorisé, une bannière rouge avec un message d'erreur s'affiche.

[SDW-18840]

La fonctionnalité de licence n'est pas prise en charge dans la configuration gérée par le fournisseur de Citrix SD-WAN Orchestrator pour locaux. Les fournisseurs peuvent continuer à utiliser les licences d'essai. Un délai de grâce de 60 jours sera accordé.

[SDW-18831]

Lorsqu'une appliance perd sa connectivité à Citrix SD-WAN Orchestrator for On-premises pendant plus de 20 minutes et passe en phase de réenregistrement, elle envoie un numéro de série incorrect dans la demande d'enregistrement.

Solution : redémarrez l'appliance.

[SDW-18781]

Après avoir importé des droits de production valides, l'option **de mise à niveau vers la production** est disponible sous Licences avant même d'attribuer la licence à l'appliance.

Solution : cliquez sur **Mettre à niveau vers la production** uniquement une fois que la licence est attribuée à l'appliance.

[SDW-18721]

La traduction d'adresses réseau (NAT) n'est pas prise en charge entre Citrix SD-WAN Orchestrator for On-premises et l'appliance.

[SDW-18703]

Dans une configuration gérée par un fournisseur, les annonces ajoutées par les administrateurs du fournisseur ne sont pas affichées aux clients lors de leur connexion.

[SDW-18491]

La CLI permet aux utilisateurs de créer un mot de passe dont la longueur est comprise entre 8 et 128, mais la connexion à l'interface graphique échoue si la longueur du mot de passe est hors de la plage autorisée.

Solution : lors de la connexion à l'interface graphique, l'utilisateur est obligé de modifier la longueur du mot de passe pour qu'elle soit conforme à la plage autorisée.

[SDW-16068]

Lorsqu'un utilisateur essaie de se connecter, une bannière rouge peut s'afficher en haut de la page pendant une fraction de seconde avant d'afficher la page de connexion.

[SDW-16024]

Lorsque la sauvegarde de la base de données d'une appliance est restaurée sur une autre appliance utilisant la même version de Citrix SD-WAN Orchestrator for On-premises, les détails de l'utilisateur ne sont pas restaurés. Sur l'appliance restaurée, si vous créez un utilisateur avec le même nom d'utilisateur que dans la base de données sauvegardée, l'erreur suivante s'affiche :

```
User has a role already assigned
```

Solution : créez un utilisateur avec un nom d'utilisateur différent qui n'existait pas dans la base de données sauvegardée.

[SDW-15984]

Notes de mise à jour pour la version 9.6 de Citrix SD-WAN Orchestrator pour locaux

July 14, 2023

Ce document de notes de mise à jour décrit les améliorations et les modifications, ainsi que les problèmes résolus et connus qui existent pour la version 9.6 de Citrix SD-WAN Orchestrator for On-premises.

> **Remarque**
>
> Ce document de notes de mise à jour n'inclut pas les correctifs liés à la sécurité. Pour obtenir la liste des correctifs et des conseils liés à la sécurité, consultez le bulletin de sécurité Citrix.

Nouveautés

Améliorations et modifications disponibles dans la version 9.6.

Configuration et gestion

Routage dynamique

À partir de la version 11.3.1 de Citrix SD-WAN, vous pouvez configurer un ID de routeur pour l'ensemble du protocole et également un ID de routeur par domaine de routage. Grâce à cette amélioration, vous pouvez activer un routage dynamique stable sur plusieurs instances avec différents ID de routeur convergeant de manière stable.

[SDW-17097]

Divers

Certificat HTTPS

Un certificat HTTPS est requis pour établir une connexion HTTPS de gestion sécurisée à Citrix SD-WAN Orchestrator for On-premises. Vous pouvez utiliser le certificat par défaut disponible sur l'interface utilisateur graphique Citrix SD-WAN Orchestrator for On-premises ou télécharger un certificat HTTPS personnalisé généré à partir de tout autre framework tel qu'OpenSSL. Le certificat HTTPS personnalisé vous permet de contrôler la sécurité et les autres paramètres du sujet liés au certificat.

[SDW-16359]

Interfaces

À partir de la version 11.3.1 de Citrix SD-WAN, vous pouvez activer ou désactiver une interface virtuelle en cochant la case **Activé** .

[SDW-15993]

Problèmes résolus

Les problèmes qui sont résolus dans la version 9.6.

Configuration et gestion

Pour l'appliance Citrix SD-WAN 6100 SE, l'interface utilisateur n'affiche pas la page **LAG** sous **Configuration > Paramètres avancés**.

[SDWANHELP-1895]

Divers

L'interface graphique Citrix SD-WAN Orchestrator pour site Web invite les utilisateurs à se connecter toutes les heures, même lorsque l'interface graphique est utilisée en continu et qu'elle n'est pas laissée inactive.

[SDWANHELP-1902]

Lorsque vous créez un site en clonant un site existant, le **déploiement de la configuration/du logiciel > Vérifier la configuration** échoue.

[SDW-16103]

Problèmes connus

Les problèmes qui existent dans la version 9.6.

Divers

Si vous ouvrez l'interface utilisateur de Citrix SD-WAN Orchestrator pour site dans un nouvel onglet alors que l'actualisation du jeton d'authentification est en cours, toutes les sessions existantes dans le navigateur sont déconnectées.

[SDW-17719]

Si le disque est redimensionné à plus de 1,8 To, il n'est pas possible de le redimensionner.

[SDW-16404]

L'interface de ligne de commande permet aux utilisateurs de créer un mot de passe dont la longueur est comprise entre 8 et 128. Toutefois, la connexion à l'interface graphique échoue si la longueur du mot de passe est hors de la plage autorisée.

Solution : lors de la connexion à l'interface graphique, l'utilisateur est obligé de modifier la longueur du mot de passe pour qu'elle soit conforme à la plage autorisée.

[SDW-16068]

Lorsqu'un utilisateur essaie de se connecter, une bannière rouge peut s'afficher en haut de la page pendant une fraction de seconde avant d'afficher la page de connexion.

[SDW-16024]

Lorsque la sauvegarde de la base de données d'une appliance est restaurée sur une autre appliance utilisant la même version de Citrix SD-WAN Orchestrator for On-premises, les détails de l'utilisateur ne sont pas restaurés. Sur l'appliance restaurée, si vous créez un utilisateur avec le même nom d'utilisateur que dans la base de données sauvegardée, l'erreur suivante s'affiche :

```
User has a role already assigned
```

Solution : créez un utilisateur avec un nom d'utilisateur différent qui n'existait pas dans la base de données sauvegardée.

[SDW-15984]

Notes de mise à jour pour la version 1.0 de Citrix SD-WAN Orchestrator pour locaux

October 21, 2022

Citrix SD-WAN Orchestrator for On-premise est un service de gestion auto-hébergé disponible en tant qu'instance distincte pour chaque client. Il fournit une plate-forme de gestion de verre unique qui vous permet de configurer, de surveiller et d'analyser toutes les appliances SD-WAN de votre réseau SD-WAN.

Citrix SD-WAN Orchestrator for On-premise est recommandé pour les clients ayant des exigences réglementaires strictes en matière de souveraineté et de confidentialité des données.

Voici certaines des fonctionnalités clés :

- **Authentification** : prend en charge l'authentification locale et RADIUS/TACACS+.
- **Configuration centralisée : configuration**centralisée des réseaux SD-WAN, avec des flux de travail guidés, des aides visuelles et des profils.
- **Approvisionnement sans contact** : mise en service fluide du réseau et des connexions.
- **Politiques centrées sur les applications** : gestion du trafic basée sur les applications, qualité de service (QoS) et politiques de pare-feu, configurables globalement ou par site.
- **Synthèse hiérarchique de l'état de santé** : capacité à surveiller de manière centralisée l'état, l'utilisation, la qualité et les performances d'un réseau dans son ensemble, avec la possibilité d'explorer les sites individuels et les connexions associées.
- **Résolution des problèmes** : journaux des appareils et des audits, utilitaires de diagnostic tels que Ping, Traceroute, Packet Capture pour résoudre les problèmes de connectivité réseau.

Conditions préalables

- **Appareils électroménagers** : Au moins deux appareils. Une adresse IP doit être configurée pour chaque appliance SD-WAN ou instance virtuelle.
- **Compte de service Citrix SD-WAN Orchestrator** : pour utiliser Citrix SD-WAN Orchestrator sur site, vous devez disposer d'un compte dans le service Citrix SD-WAN Orchestrator. Pour plus d'informations, consultez la section Intégration du service Citrix SD-WAN Orchestrator.

Citrix SD-WAN Orchestrator pour site 1.0.1

Problèmes résolus

- **SDW-16456** : Tous les domaines de routage ne sont pas pris en charge dans Citrix SD-WAN Orchestrator pour locaux.
- **SDW-16063** : Au niveau du réseau, les rapports récapitulatifs Wi-Fi ne sont pas disponibles.
- **SDW-16054** : Si un compte client est créé en dehors de la région des États-Unis sur le service Citrix SD-WAN Orchestrator, le jeton d'API obtenu par la page Identity and Management (IDAM) de Citrix Cloud ne fonctionne pas. La connexion du client à Citrix SD-WAN Orchestrator for On-premises échoue avec le message d'erreur suivant : « ID client, ID client ou secret client non valide ».

  Vous pouvez désormais sélectionner le **POP** dans lequel votre compte cloud a été intégré, lors du premier démarrage de Citrix SD-WAN Orchestrator pour locaux.

Problèmes connus

- **SDW-16068** : La CLI permet aux utilisateurs de créer un mot de passe dont la longueur est comprise entre 8 et 128, mais la connexion à l'interface graphique échoue si la longueur du mot de passe dépasse la plage autorisée.
  - **Solution** : lors de la connexion à l'interface graphique, l'utilisateur est obligé de modifier la longueur du mot de passe pour qu'elle soit conforme à la plage autorisée.
- **SDW-16024** : Lorsqu'un utilisateur se connecte à l'interface utilisateur, une bannière rouge peut s'afficher en haut de la page pendant une fraction de seconde avant d'afficher la page de connexion.
- **SDW-15984** : Lorsque la sauvegarde de la base de données d'une appliance est restaurée sur une autre appliance utilisant la même version de Citrix SD-WAN Orchestrator for On-premises,

les détails de l'utilisateur ne sont pas restaurés. Sur l'appliance restaurée, si vous créez un utilisateur avec le même nom d'utilisateur que dans la base de données sauvegardée, l'erreur suivante s'affiche :

Un rôle a déjà été attribué à l'utilisateur

  - **Solution** : créez un utilisateur avec un nom d'utilisateur différent qui n'existait pas dans la base de données sauvegardée.

- **SDW-16103** : Lorsque vous créez un site en clonant un site existant, **Déployer la configuration/le logiciel > Vérifier la configuration** échoue.

  - **Solution** : ne créez pas de site en clonant un site existant.

- **SDW-16404** : Si le disque est redimensionné à plus de 1,8 To, le redimensionnement du disque n'a pas lieu.

Configuration système requise et installation

October 21, 2022

Avant d'installer Citrix SD-WAN Orchestrator pour locaux sur une machine virtuelle (VM), assurez-vous de comprendre la configuration matérielle et logicielle requise et d'avoir satisfait aux prérequis.

> **Remarque**
>
> La configuration système requise est commune à la fois au réseau à région unique et au réseau multirégional.

Configuration matérielle requise

Voici la configuration matérielle requise pour que Citrix SD-WAN Orchestrator for On-premises puisse stocker des données d'un mois ou des statistiques pour deux liaisons WAN par site en moyenne :

Nombre de sites	Processeur	RAM	Stockage
2000	256 vCPU 3 GHz ou supérieur	512 GO	2 C. À
1000	128 vCPU 3 GHz ou supérieur	256 GO	1 CUILLÈRE
500	64 processeurs virtuels à 3 GHz ou plus	128 GO	500 Go

Nombre de sites	Processeur	RAM	Stockage
256	32 vCPU 3 GHz ou supérieur	64 GO	256 GO
128	8 processeurs virtuels à 3 GHz ou plus	16 GO	256 GO

Logiciel

Citrix SD-WAN Orchestrator pour VPX sur site peut être configuré sur les plateformes suivantes :

Hyperviseur

- Mise à jour 1 de VMware ESXi 7.0.
- Serveur VMware ESXi, version 6.5.
- Citrix XenServer 6.5 ou version ultérieure.

Les cookies doivent être activés dans les navigateurs et JavaScript doivent être installés et activés.

Citrix SD-WAN Orchestrator pour interface Web sur site est pris en charge sur les navigateurs suivants :

- Google Chrome 40.0+
- Microsoft Internet Explorer 11+
- Mozilla Firefox 41.0+

Conditions préalables

Les conditions préalables à l'installation et au déploiement de Citrix SD-WAN Orchestrator pour locaux sont les suivantes :

- Le nœud de contrôle principal (MCN) du SD-WAN et les nœuds clients existants doivent être mis à niveau vers la dernière version du logiciel Citrix SD-WAN.
- Il est recommandé de disposer d'un serveur DHCP et de le configurer sur le réseau SD-WAN.
- Vous devez disposer du Citrix SD-WAN Orchestrator pour les fichiers d'installation locaux.

> **Remarque**
>
> Vous ne pouvez pas personnaliser ni installer de logiciel tiers sur Citrix SD-WAN Orchestrator pour locaux. Vous pouvez toutefois modifier les paramètres du processeur virtuel, de la mémoire et du stockage.

Téléchargez Citrix SD-WAN Orchestrator pour le logiciel local

Téléchargez les fichiers d'installation du logiciel Citrix SD-WAN Orchestrator for On-premises Management Console, pour la version et la plate-forme requises, depuis la page Téléchargements .

Les fichiers d'installation de Citrix SD-WAN Orchestrator pour locaux utilisent la convention de dénomination suivante :

- extension ctx-sdw-onprem-build
- extension ctx-onprem-build.build
- extension ctx-onprem-build.build

Plateforme	Extension
Citrix XenServer	.xva
VMware ESXi	-vmware.ova

Checklist d'installation et de configuration

Cette section fournit une liste de contrôle des informations dont vous avez besoin pour terminer l'installation et le déploiement de Citrix SD-WAN Orchestrator sur site.

Recueillez ou déterminez les informations suivantes :

- Adresse IP du serveur ESXi et du serveur XenServer qui héberge le Citrix SD-WAN Orchestrator pour la machine virtuelle (VM) sur site.
- Nom unique à attribuer au Citrix SD-WAN Orchestrator pour la machine virtuelle sur site.
- La quantité de mémoire à allouer au Citrix SD-WAN Orchestrator pour la machine virtuelle sur site.
- La quantité de capacité de disque à allouer au disque virtuel de la machine virtuelle.
- L'adresse IP de la passerelle Citrix SD-WAN Orchestrator à utiliser sur site pour communiquer avec des réseaux externes.
- Le masque de sous-réseau du réseau sur lequel Citrix SD-WAN Orchestrator for On-premises VM est installé.

> **Remarque**
>
> Citrix recommande de prendre régulièrement des instantanés des configurations des machines virtuelles et du SD-WAN.

Différence entre le service SD-WAN Orchestrator pour site et le service Citrix SD-WAN Orchestrator

October 21, 2022

Fonctionnalités

Fonctionnalités	Service Citrix SD-WAN Orchestrator	Citrix SD-WAN Orchestrator pour locaux
Plateforme d'édition avancée	Oui	Non
Plateforme Premium Edition	Oui	Non
Service de scaler	Oui	Non
Service Azure Virtual WAN	Oui	Non
Service d'Citrix Secure Internet Access	Oui	Non
Pare-feu hébergé	Oui	Non
Routage des applications sur des applications DPI prédéfinies et des applications personnalisées (basées sur le FQDN ou IP	Oui	Oui
Routage des applications sur les applications qui nécessitent des mises à jour de signature dynamiques (comme Office 365, Citrix Cloud et les applications récemment prises en charge).	Oui	Non
Orchestrator - Haute disponibilité	Oui	Non

Exigences

Exigences	Service Citrix SD-WAN Orchestrator	SD-WAN Orchestrator pour local
Image d'usine SD-WAN requise	Tout (version Factory Shipping)	Citrix SD-WAN 10.2.7, 11.1.1, 11.2.0, 11.2.2, 11.3.0 et versions ultérieures. *
Appliance déployée sur le réseau	Tous	Citrix SD-WAN 11.2.2, 11.3.0 et versions ultérieures. *
Connectivité Internet de l'appliance SD-WAN	Requis	Non requis
Ports de pare-feu à ouvrir	443	443, 22, ICMP
Gestion des licences	Modèles postpayés et prépayés	Modèle prépayé uniquement

- La version du logiciel Citrix SD-WAN prise en charge dépend de la version du logiciel SD-WAN Orchestrator for On-premises.

Installation et configuration de l'SD-WAN Orchestrator pour les applications locales sur un serveur ESXi

October 21, 2022

Installation du client VMware vSphere

Vous trouverez ci-dessous les instructions de base pour télécharger et installer le client VMware vSphere que vous utilisez pour créer et déployer Citrix SD-WAN Orchestrator pour machine virtuelle (VM) sur site.

Pour télécharger et installer le client VMware vSphere, procédez comme suit :

1. Ouvrez un navigateur et accédez au serveur ESXi qui héberge votre instance de machine virtuelle vSphere Client et Citrix SD-WAN Orchestrator pour une instance de machine virtuelle sur site. La page d'accueil de VMware ESXi s'affiche.
2. Cliquez sur le lien **Télécharger vSphere Client** pour télécharger le fichier d'installation de vSphere Client.
3. Installez vSphere Client.

   Exécutez le fichier d'installation de vSphere Client que vous avez téléchargé et acceptez chacune des options par défaut lorsque vous y êtes invité.

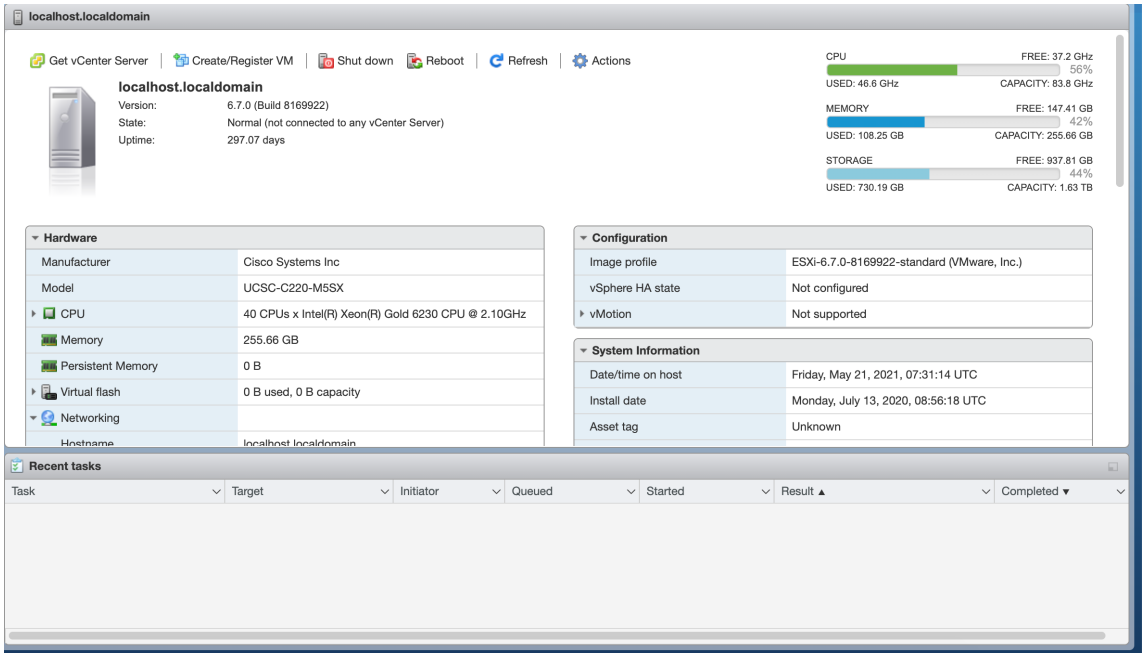
4. Une fois l'installation terminée, démarrez le programme vSphere Client.

   La page de connexion de VMware vSphere Client s'affiche et vous invite à saisir les informations d'identification du serveur ESXi.

5. Entrez les informations de connexion au serveur ESXi :

   - **Adresse IP/nom** : Entrez l'adresse IP ou le nom de domaine complet (FQDN) du serveur ESXi qui héberge votre instance de machine virtuelle Citrix SD-WAN Orchestrator pour une instance de machine virtuelle sur site.
   - **Nom d'utilisateur** : entrez le nom du compte administrateur du serveur. La valeur par défaut est racine.
   - **Mot de passe** : Entrez le mot de passe associé à ce compte administrateur.

6. Cliquez sur **Connexion**.
   La page principale de vSphere Client s'affiche.



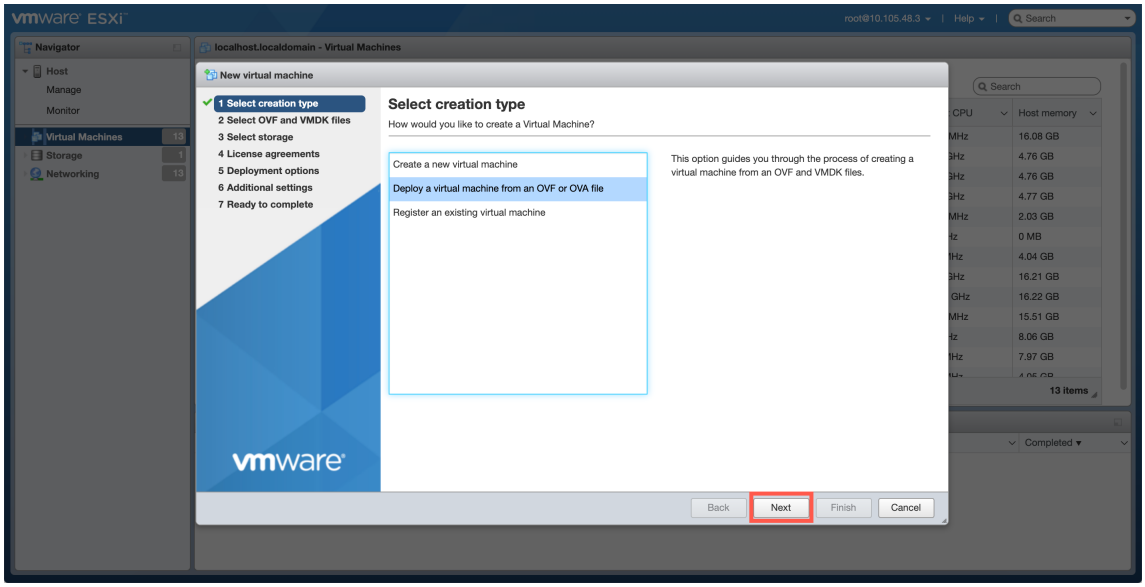
Création du Citrix SD-WAN Orchestrator pour machine virtuelle locale à l'aide du modèle OVF

Après avoir installé le client VMware vSphere, créez le Citrix SD-WAN Orchestrator pour la machine virtuelle sur site.

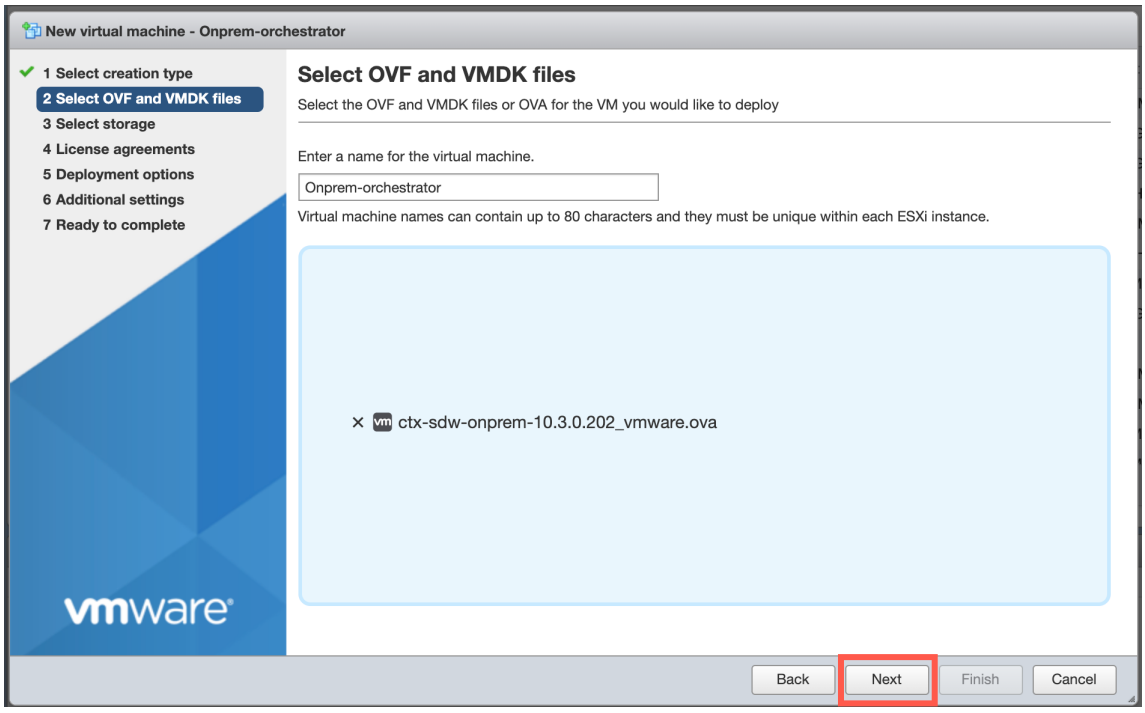
1. Si vous ne l'avez pas déjà fait, téléchargez le fichier modèle OVF Citrix SD-WAN Orchestrator for On-premises (fichier .ova) sur le PC local.

   Pour plus d'informations, consultez la section Configuration système requise et installation.

2. Dans vSphere Client, cliquez sur **Créer/enregistrer une machine virtuelle**, puis sélectionnez **Déployer une machine virtuelle à partir d'un fichier OVF ou OVA** dans la liste. Cliquez sur **Suivant**.



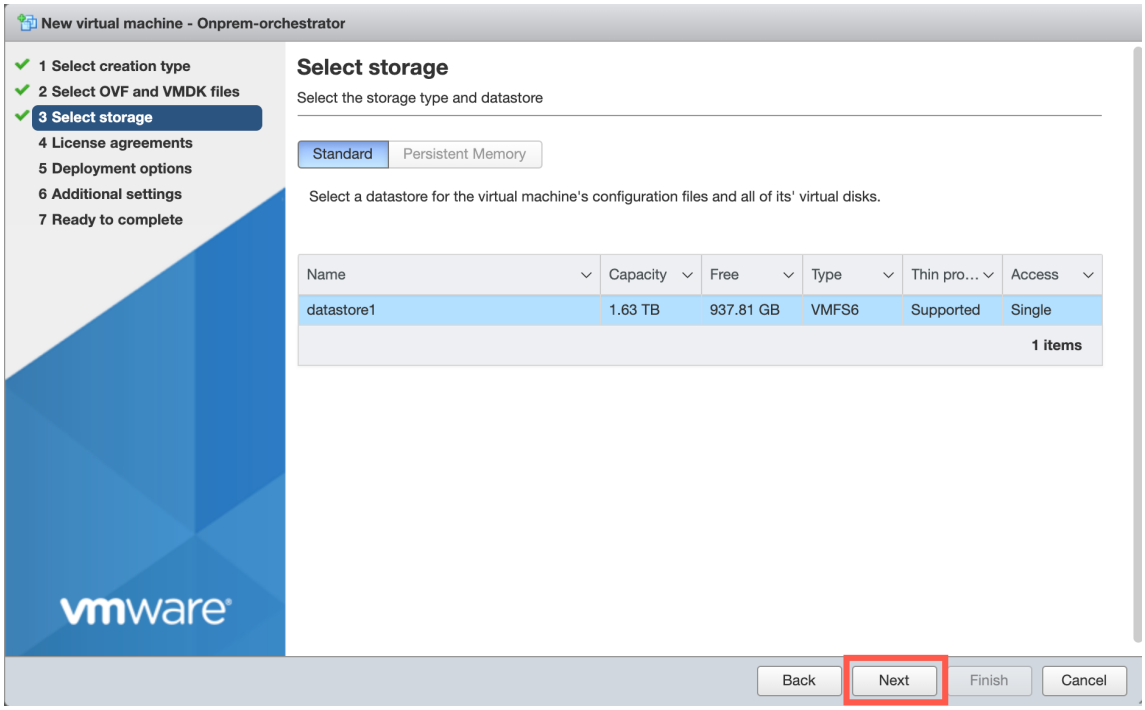
3. Entrez un nom unique pour la nouvelle machine virtuelle.
4. Cliquez dans la zone et sélectionnez le modèle Citrix SD-WAN Orchestrator for On-premises OVF (fichier .ova) que vous souhaitez installer ou vous pouvez faire glisser le fichier à l'intérieur de la zone.
5. Cliquez sur **Suivant**.



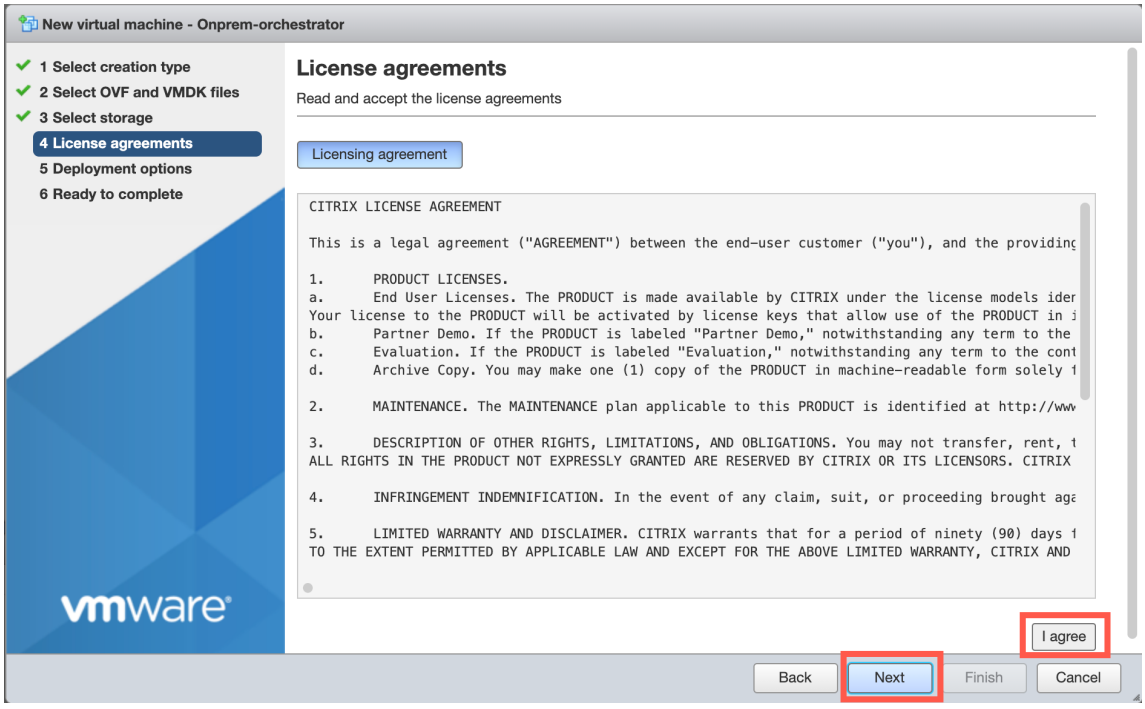
6. Cliquez sur **Suivant**.

   La page Stockage s'affiche.

7. Acceptez la ressource de stockage par défaut en cliquant sur **Suivant**.

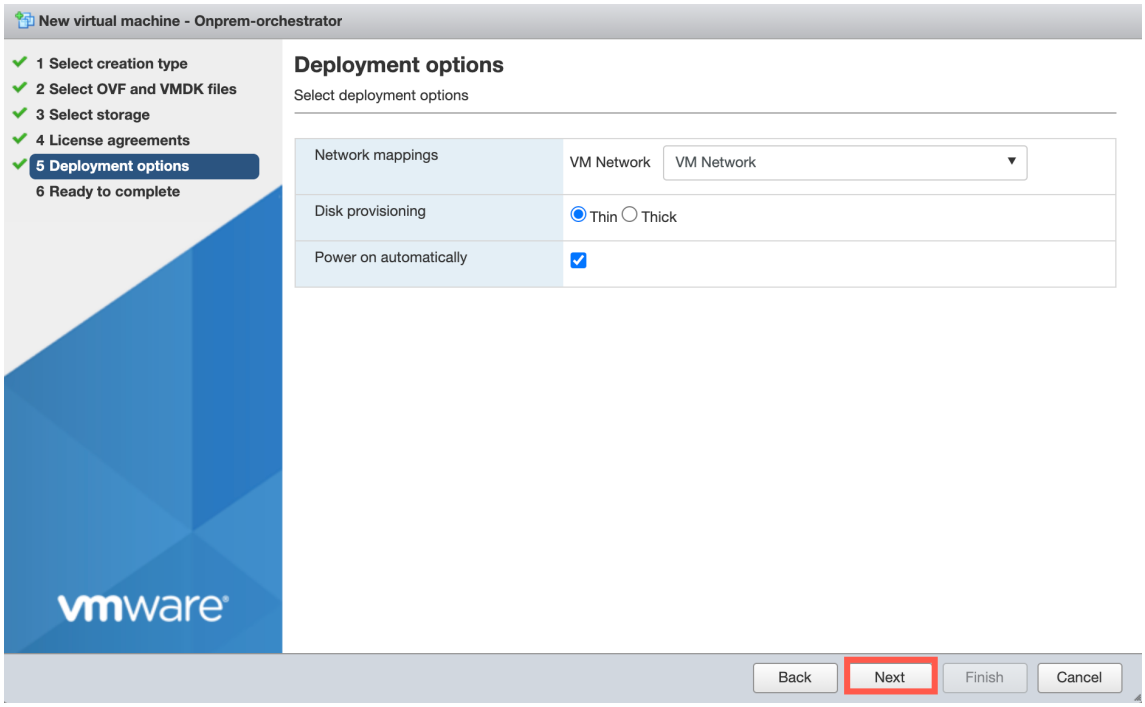


8. Sur la page EULA, cliquez sur **J'accepte**, puis sur **Suivant**.



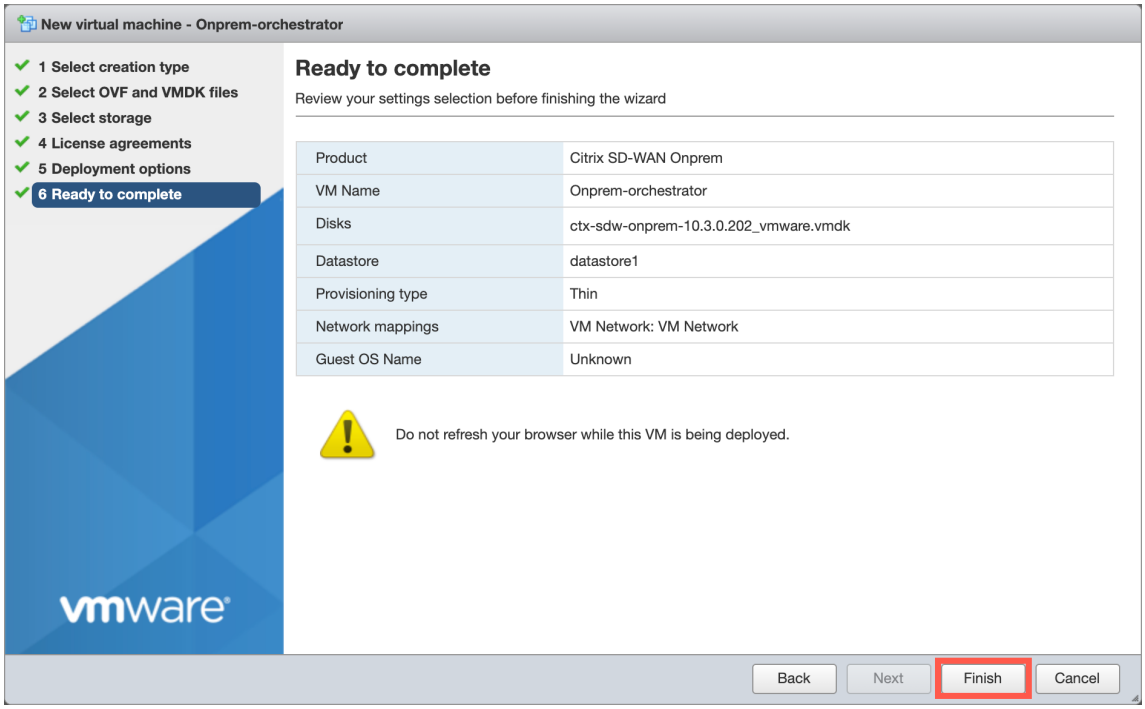
9. Sur la page des options de déploiement, sélectionnez le réseau de machines virtuelles dans

la liste déroulante et acceptez les paramètres par défaut pour les autres champs. Cliquez sur **Suivant**.



10. Sur la page Prêt à terminer, cliquez sur **Terminer** pour créer la machine virtuelle.

> **Remarque**
>
> La décompression de l'image disque sur le serveur peut prendre plusieurs minutes.

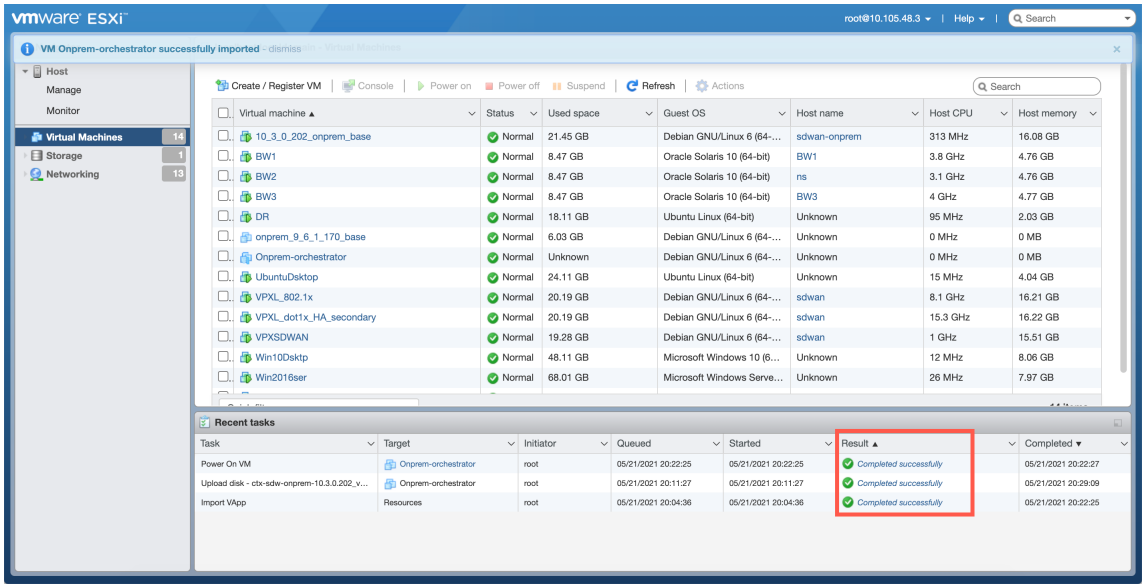


Afficher et enregistrer l'adresse IP de gestion sur le serveur ESXi

L'adresse IP de gestion est l'adresse IP de Citrix SD-WAN Orchestrator pour machine virtuelle sur site. Utilisez cette adresse IP pour vous connecter à l'interface utilisateur Web Citrix SD-WAN Orchestrator pour locaux.

Pour afficher l'adresse IP de gestion, procédez comme suit :

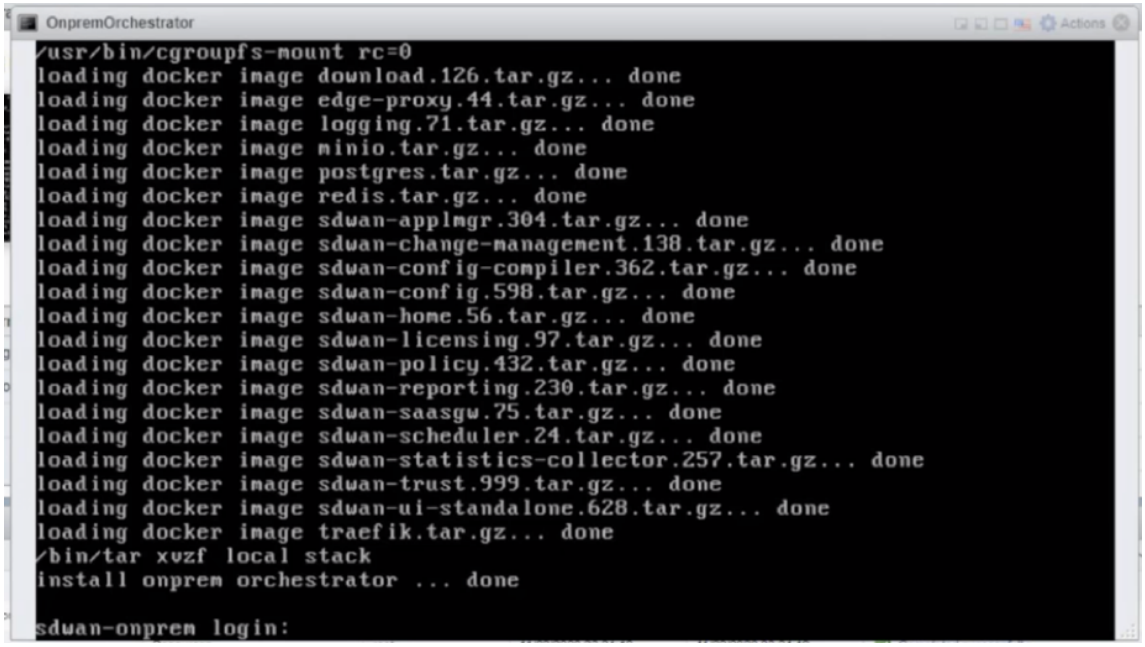
1. Sur la page Inventaire des clients vSphere, sélectionnez le nouveau Citrix SD-WAN Orchestrator pour machine virtuelle sur site.
2. Sur la page Citrix SD-WAN Orchestrator pour locaux, sous Tâches récentes, attendez que le résultat soit terminé.



3. Sélectionnez l'onglet **Console**, puis cliquez n'importe où dans la zone de la console pour passer en mode console.

   > **Remarque**
   >
   > Pour libérer le contrôle de votre curseur par la console, appuyez simultanément sur <Alt> les touches <Ctrl> et.

4. Appuyez sur **Entrée** pour afficher l'invite de connexion à la console.

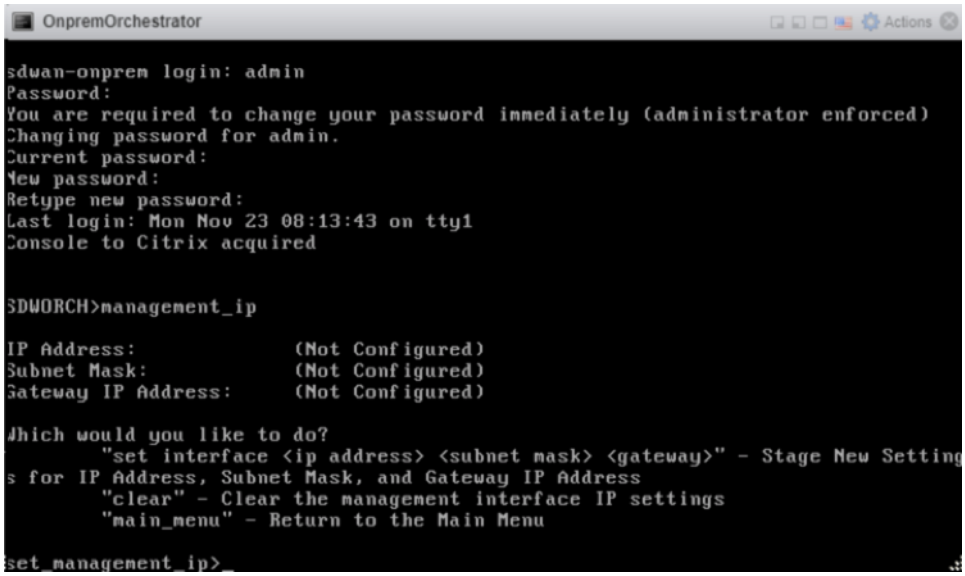


5. Connectez-vous à la console de la machine virtuelle.

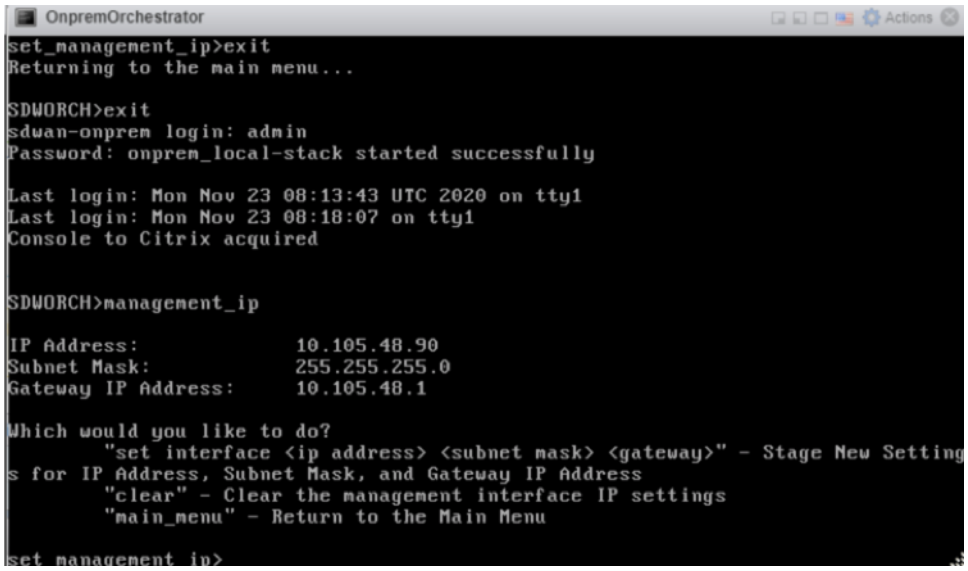
   Les informations de connexion par défaut pour le nouveau Citrix SD-WAN Orchestrator pour machine virtuelle locale sont les suivantes :

   - **Identifiant** : admin
   - **Mot de passe** : password

   > **Remarque**
   >
   > Il est obligatoire de modifier le mot de passe du compte administrateur par défaut lors de la première connexion. Cette modification est appliquée en utilisant l'interface de ligne de commande et l'interface utilisateur.



6. Enregistrez l'adresse IP de gestion de la machine virtuelle Citrix SD-WAN Orchestrator for On-premises, qui s'affiche sous la forme d'adresse IP de l'hôte dans un message de bienvenue qui apparaît lorsque vous vous connectez.



> **Remarque**
>
> - Le serveur DHCP doit être présent et disponible sur le réseau SD-WAN, sinon cette étape ne peut pas être terminée.
> - Dans la console, entrez la commande CLI `set_dns` pour confirmer le paramètre actuel du serveur DNS et reconfigurer le serveur DNS si le serveur DNS existant n'est pas en mesure de fournir le service DNS. Pour plus d'informations sur l'utilisation de la `set_dns` commande, consultez Citrix SD-WAN Orchestrator pour la connexion sur site.

Si le serveur DHCP n'est pas configuré sur le réseau SD-WAN, vous devez saisir manuellement une adresse IP statique.

Pour configurer une adresse IP statique comme adresse IP de gestion :

1. Lorsque la machine virtuelle est démarrée, cliquez sur l'onglet **Console** .
2. Connectez-vous à la machine virtuelle. Les informations de connexion par défaut pour le nouveau Citrix SD-WAN Orchestrator pour machine virtuelle locale sont les suivantes :
   - **Identifiant** : admin
   - **Mot de passe** : password
3. Dans la console, entrez la commande CLI `management_ip`.
4. Entrez la commande `set interface <ipaddress> <subnetmask> <gateway>` pour configurer l'adresse IP de gestion.
5. Êtes-vous sûr de vouloir modifier les paramètres IP de votre interface de gestion ?

   Vous risquez de perdre la connexion à l'appliance. <y/n>?

   Appuyez sur « y » pour modifier l'adresse IP et accéder à la nouvelle adresse IP de gestion configurée après environ 6 à 7 minutes.

Installation et configuration de l'SD-WAN Orchestrator pour les applications locales sur XenServer

October 21, 2022

Avant d'installer Citrix SD-WAN Orchestrator pour machine virtuelle locale sur un serveur XenServer, collectez les informations nécessaires comme décrit dans la liste de contrôle d'installation et de configuration.

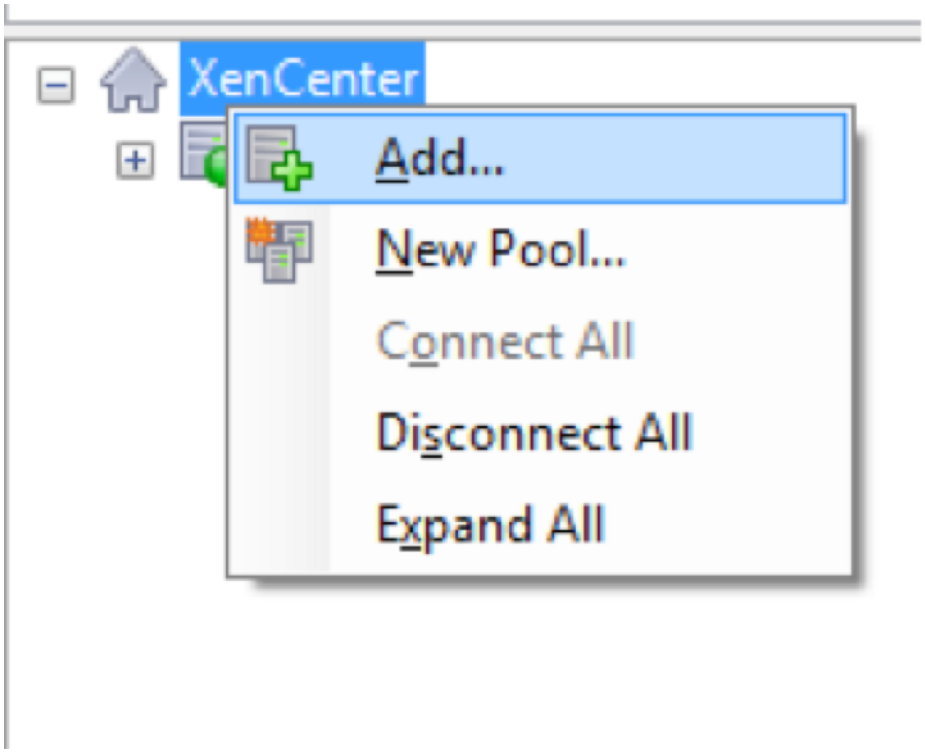
Installez le serveur XenServer

Pour installer le serveur Citrix XenServer sur lequel vous déployez Citrix SD-WAN Orchestrator pour machine virtuelle locale, XenCenter doit être installé sur votre ordinateur. Si vous ne l'avez pas déjà fait, téléchargez et installez XenCenter.

Pour installer un serveur XenServer :

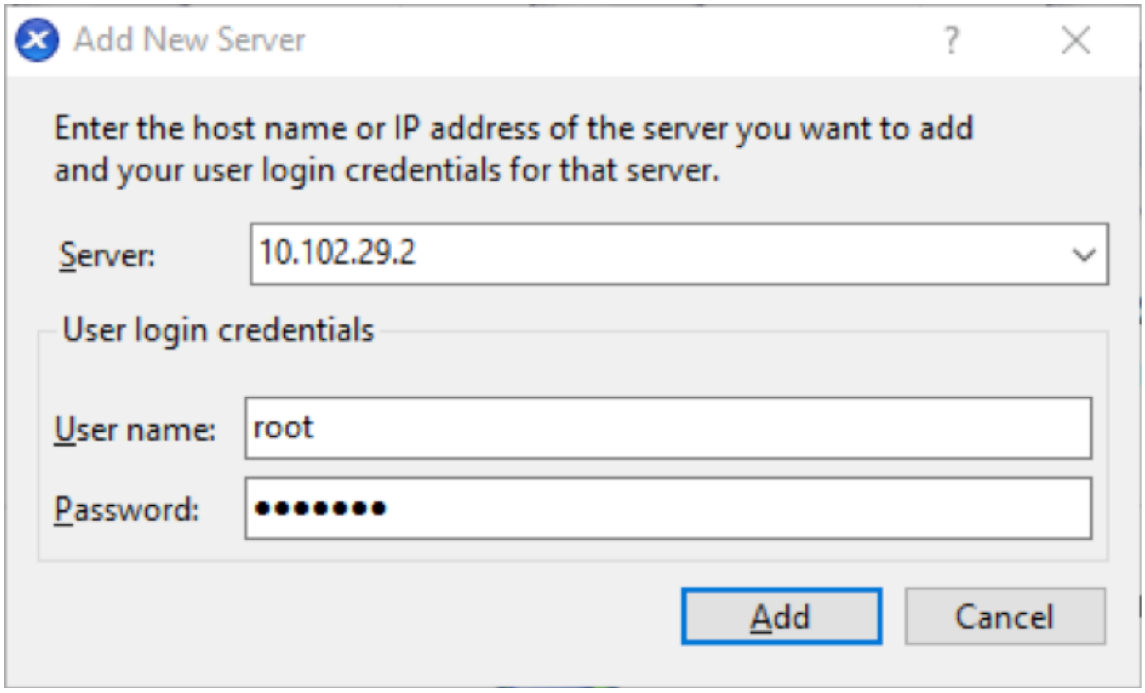
1. Ouvrez l'application XenCenter sur votre ordinateur.

2. Dans l'arborescence de gauche, cliquez avec le bouton droit sur **XenCenter** et sélectionnez **Ajouter**.



3. Dans la fenêtre **Ajouter un nouveau serveur**, entrez les informations requises dans les champs suivants :

   - **Serveur** : Entrez l'adresse IP ou le nom de domaine complet (FQDN) du serveur XenServer qui héberge votre instance de machine virtuelle Citrix SD-WAN Orchestrator pour une instance de machine virtuelle sur site.
   - **Nom d'utilisateur** : entrez le nom du compte administrateur du serveur. La valeur par défaut est racine.
   - **Mot de passe** : Entrez le mot de passe associé à ce compte administrateur.



4. Cliquez sur **Ajouter**.

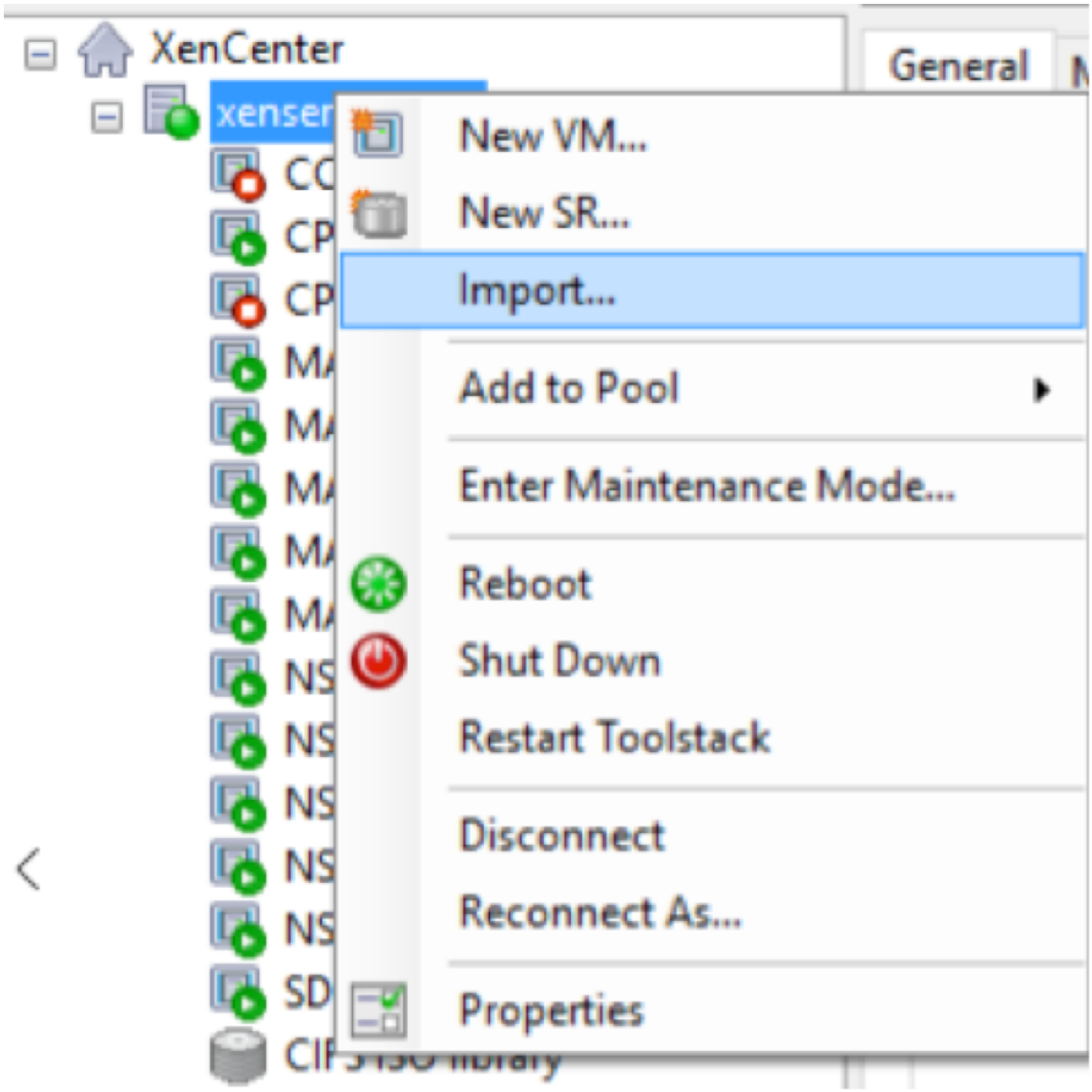
L'adresse IP du nouveau serveur apparaît dans le volet de gauche.

Créez le Citrix SD-WAN Orchestrator pour machine virtuelle locale à l'aide du fichier XVA

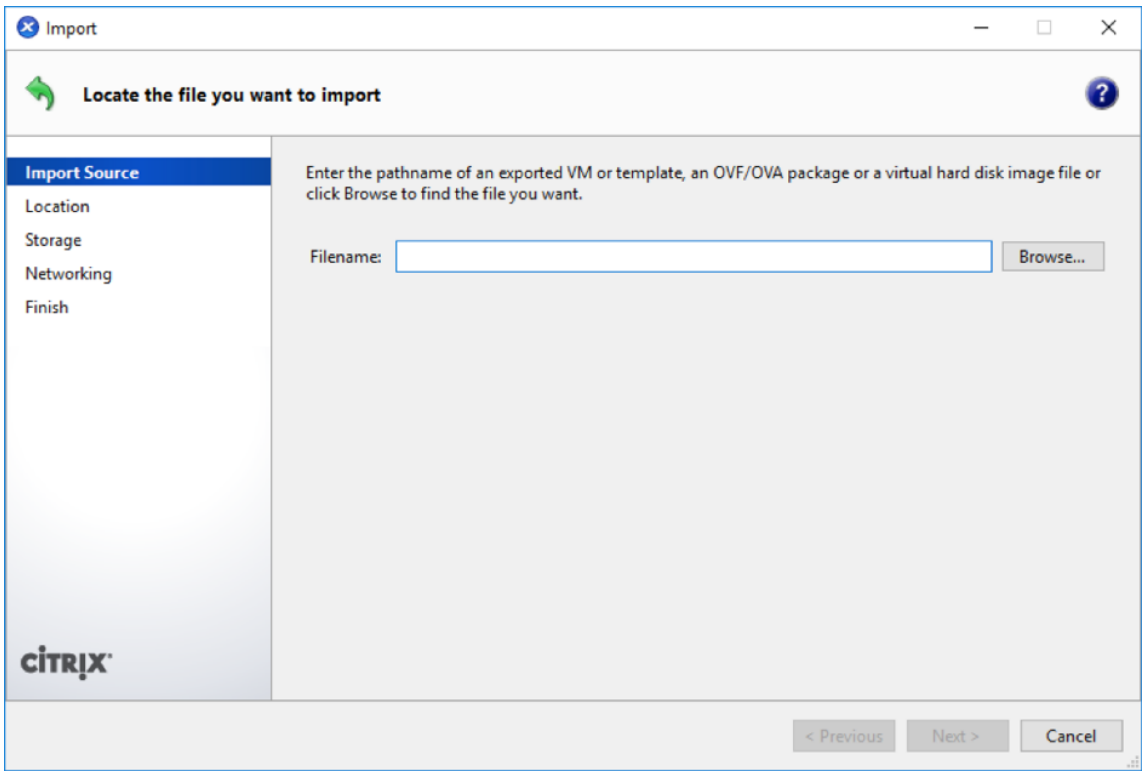
Le logiciel Citrix SD-WAN Orchestrator pour machines virtuelles sur site est distribué sous forme de fichier XVA. Si vous ne l'avez pas déjà fait, téléchargez le fichier .xva. Pour plus d'informations, consultez la section Configuration système requise et installation.

Pour créer le Citrix SD-WAN Orchestrator pour machine virtuelle locale, procédez comme suit :

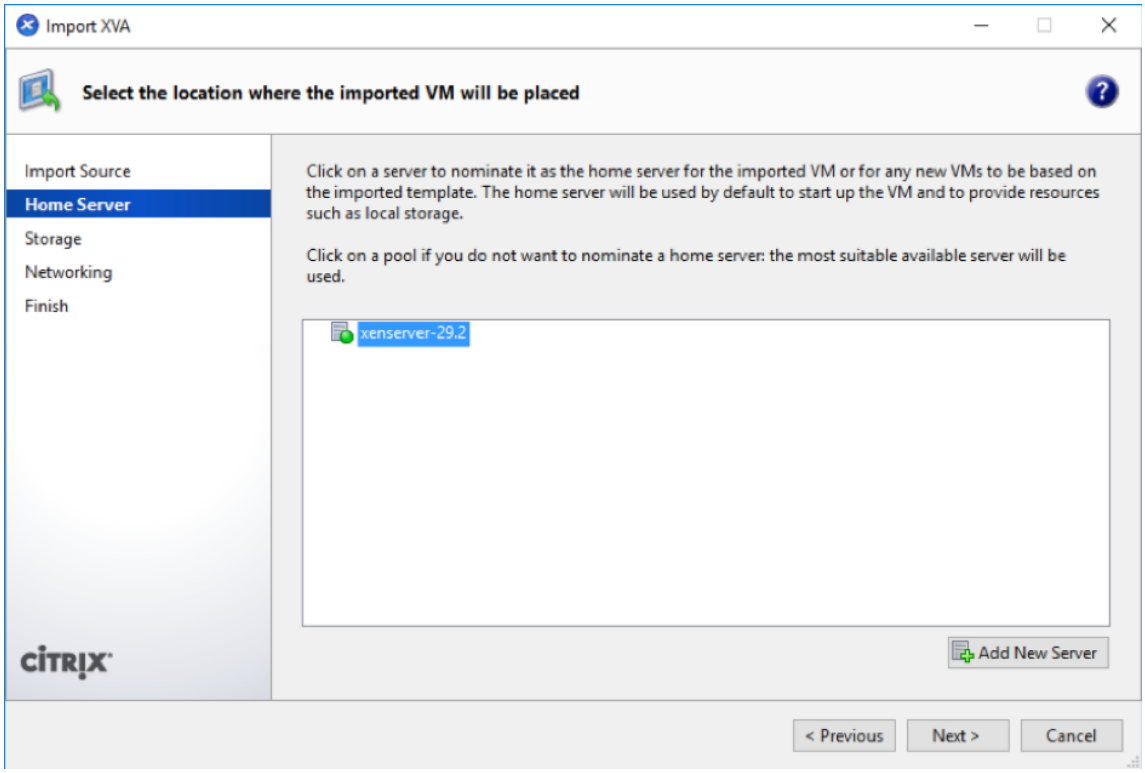
1. Dans XenCenter, cliquez avec le bouton droit sur **XenServer,**puis cliquez



2. Accédez au fichier .xva téléchargé, sélectionnez-le et cliquez sur **Suivant**.



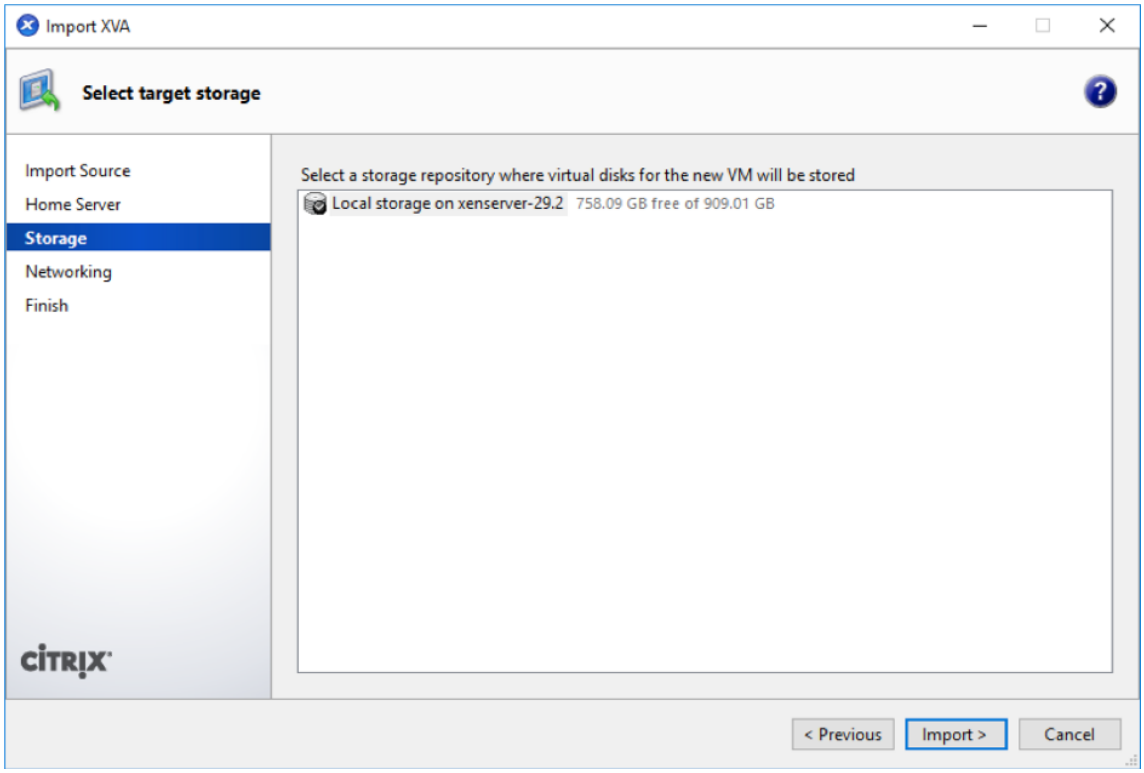
3. Sélectionnez un serveur XenServer créé précédemment comme emplacement vers lequel importer la machine virtuelle, puis cliquez sur **Suivant**.



4. Sélectionnez un référentiel de stockage dans lequel le disque virtuel de la nouvelle machine

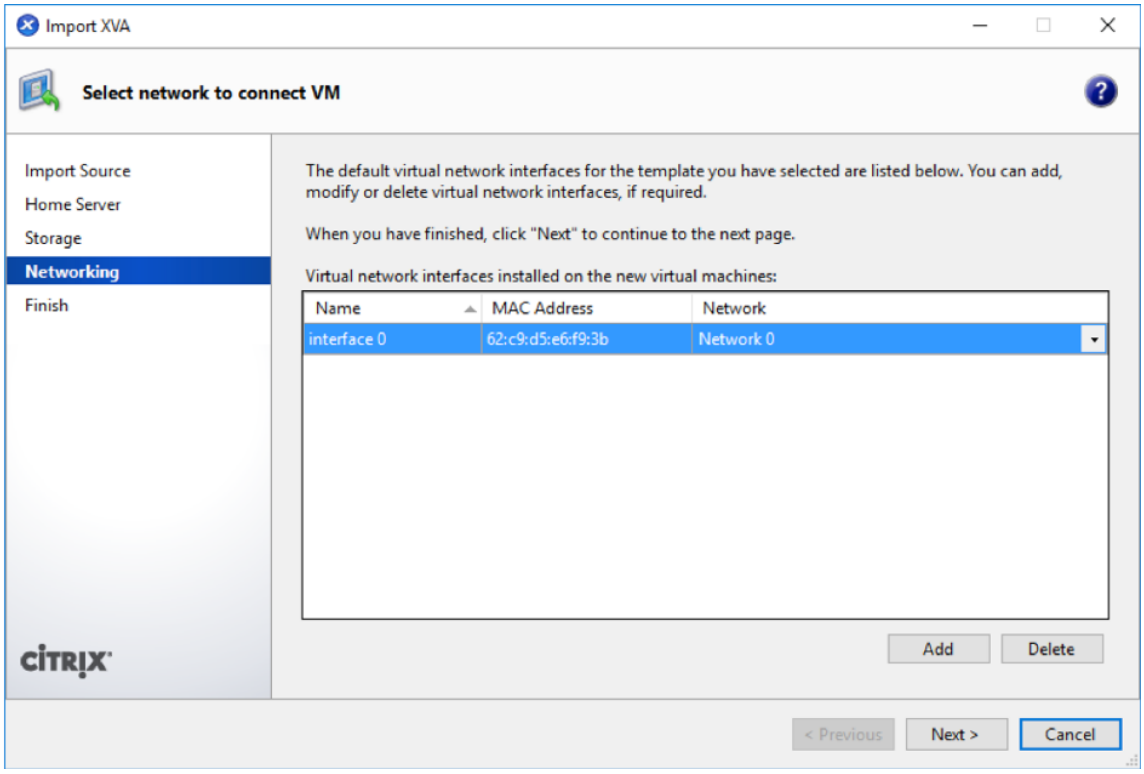
virtuelle est stocké, puis cliquez sur **Importer**.

Pour l'instant, vous pouvez accepter la ressource de stockage par défaut. Vous pouvez également configurer la banque de données.



Le Citrix SD-WAN Orchestrator pour machine virtuelle locale importé apparaît dans le volet de gauche.

5. Sélectionnez le réseau auquel vous souhaitez connecter la machine virtuelle, puis cliquez sur **Suivant**.



6. Cliquez sur **Terminer**.

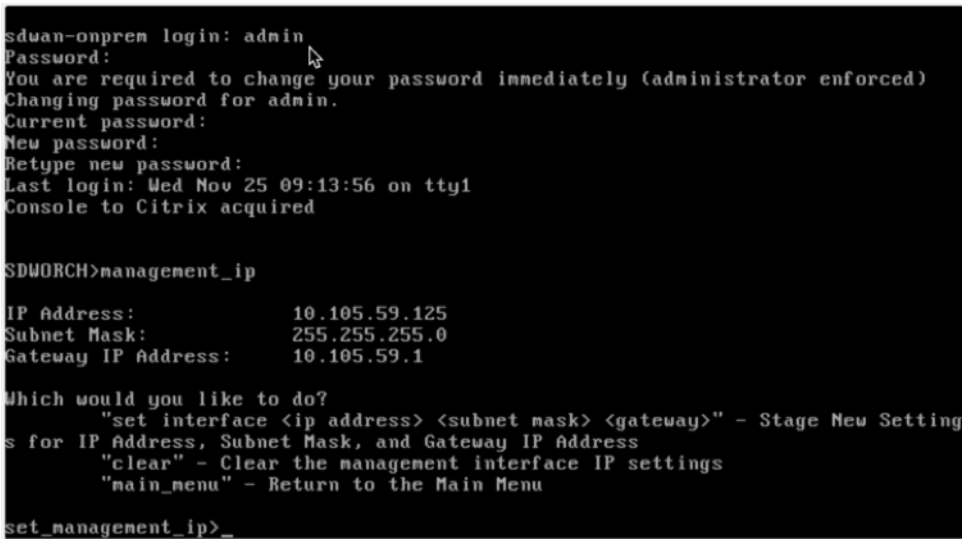
Afficher et enregistrer l'adresse IP de gestion sur XenServer

L'adresse IP de gestion est l'adresse IP de Citrix SD-WAN Orchestrator pour machine virtuelle sur site. Utilisez cette adresse IP pour vous connecter à l'interface utilisateur Web Citrix SD-WAN Orchestrator pour locaux.

> **Remarque**
>
> Le serveur DHCP doit être présent et disponible sur le réseau SD-WAN.

Pour afficher l'adresse IP de gestion :

1. Dans l'interface XenCenter, dans le volet de gauche, cliquez avec le bouton droit sur le nouveau Citrix SD-WAN Orchestrator pour machine virtuelle locale et sélectionnez **Démarrer**.
2. Lorsque la machine virtuelle est démarrée, cliquez sur l'onglet **Console** .



3. Prenez note de l'adresse IP de gestion.

   > **Remarque**
   >
   > Le serveur DHCP doit être présent et disponible sur le réseau SD-WAN, sinon cette étape ne peut pas être terminée.

4. Connectez-vous à la machine virtuelle. Les informations de connexion par défaut pour le nouveau Citrix SD-WAN Orchestrator pour machine virtuelle locale sont les suivantes :

   Identifiant : admin

   Mot de passe : password

   > **Remarque :**
   >
   > Il est obligatoire de modifier le mot de passe du compte administrateur par défaut lors de la première connexion. Cette modification est appliquée en utilisant l'interface de ligne de commande et l'interface utilisateur.

   Si le serveur DHCP n'est pas configuré sur le réseau Citrix SD-WAN, vous devez saisir manuellement une adresse IP statique.

Pour configurer une adresse IP statique comme adresse IP de gestion :

1. Lorsque la machine virtuelle est démarrée, cliquez sur l'onglet Console.
2. Connectez-vous à la machine virtuelle. Les informations de connexion par défaut pour le nouveau Citrix SD-WAN Orchestrator pour machine virtuelle locale sont les suivantes :

   Identifiant : admin

   Mot de passe : password

3. Dans la console, entrez la commande CLI `management_ip`.
4. Entrez la commande `set interface <ipaddress> <subnetmask> <gateway>` pour configurer l'adresse IP de gestion.
5. Êtes-vous sûr de vouloir modifier les paramètres IP de votre interface de gestion ?

   Vous risquez de perdre la connexion à l'appliance. <y/n>?

   Appuyez sur « y » pour modifier l'adresse IP et accéder à l'adresse IP de gestion configurée après environ 6 à 7 minutes.

Intégration de SD-WAN Orchestrator pour les applications sur site

October 21, 2022

Voici un aperçu du processus d'intégration de Citrix SD-WAN Orchestrator for On-premises :

- Intégration des fournisseurs et des locataires : Nos clients peuvent utiliser un service SD-WAN géré auprès de partenaires Citrix, activé par le service Citrix SD-WAN Orchestrator mutualisé.
- Intégration des entreprises « Do It Yourself » (DIY) : le service Citrix SD-WAN Orchestrator est également disponible en tant que service autogéré pour les entreprises.

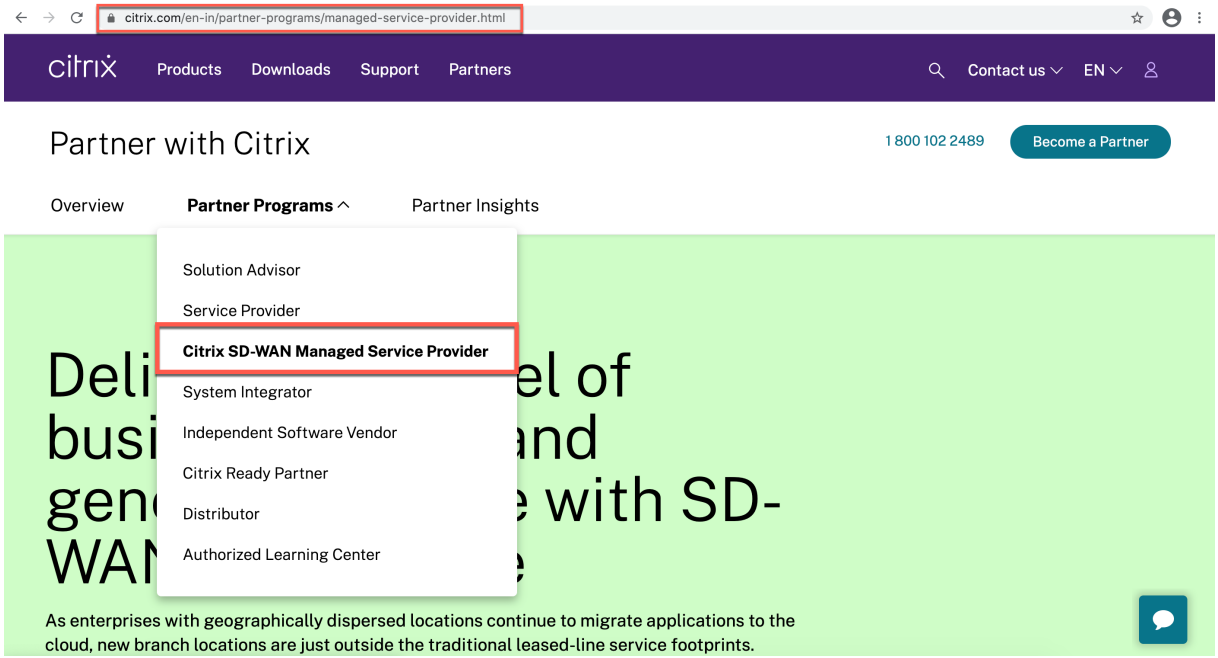
Fournisseur d'intégration et locataires

Cette section décrit le processus d'intégration des partenaires Citrix et de leurs locataires.
Voici un résumé du processus d'intégration :

1. Un partenaire potentiel s'inscrit en tant que Citrix Partner.
2. Citrix Partner s'enregistre en tant que revendeur Citrix SD-WAN.

Partenaire s'inscrit à un programme de partenariat Citrix

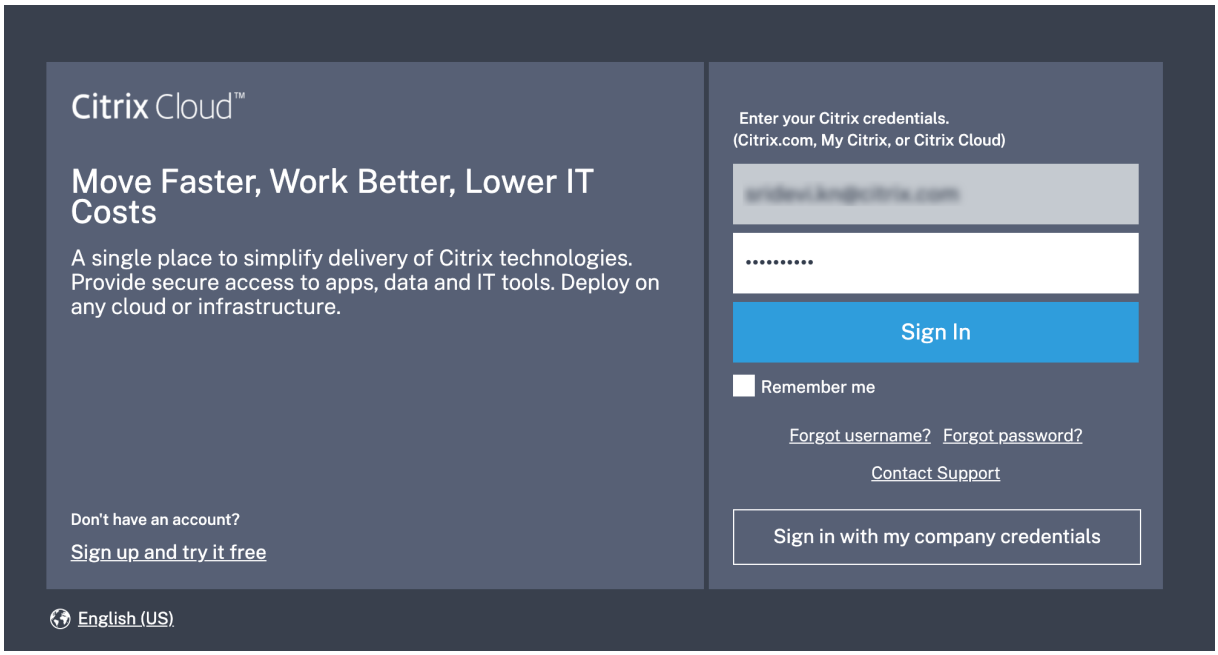
Un partenaire potentiel doit s'inscrire au Citrix Service Provider Program (CSP) - Inscription CSP.
Un partenaire peut également s'inscrire au programme Citrix SD-WAN Managed Service Provider, spécialement conçu pour les partenaires Citrix SD-WAN : SD-WAN MSP Sign Up.



Un compte Citrix Cloud (CC) est créé pour le partenaire dans le cadre du processus d'inscription. Pour plus d'informations, consultez la section Inscription à Citrix Cloud.

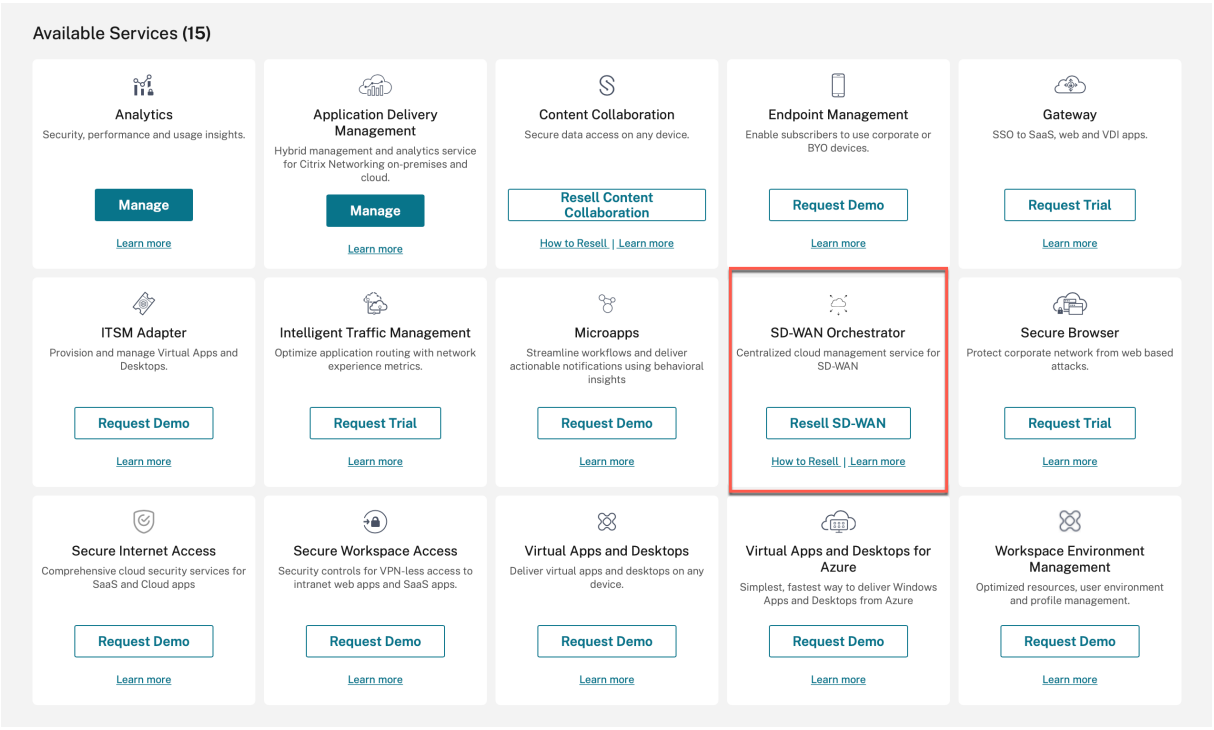
Le partenaire s'inscrit en tant que revendeur Citrix SD-WAN

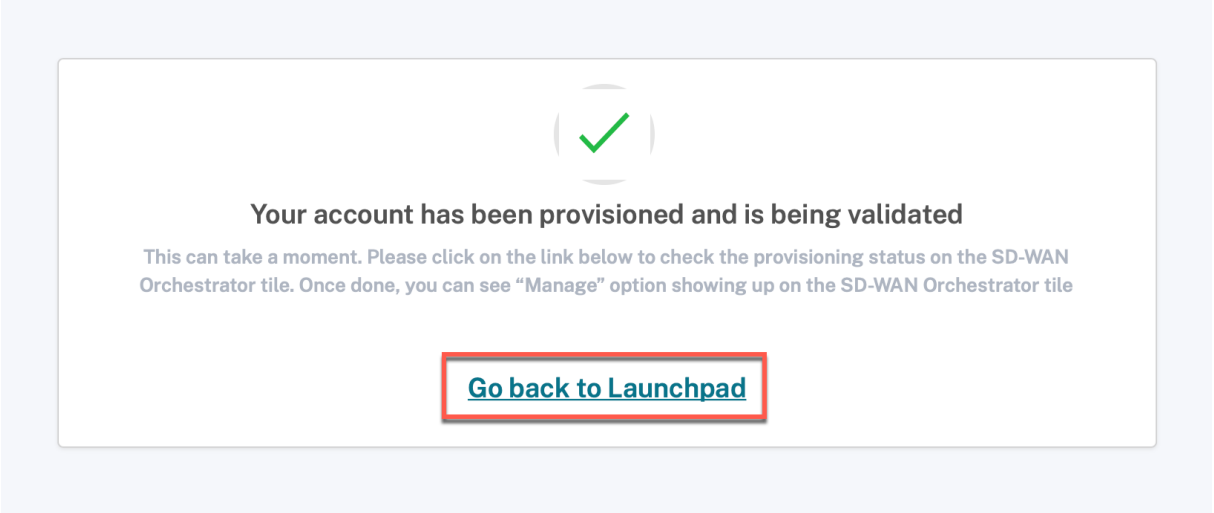
Le partenaire se connecte au compte Citrix Cloud.



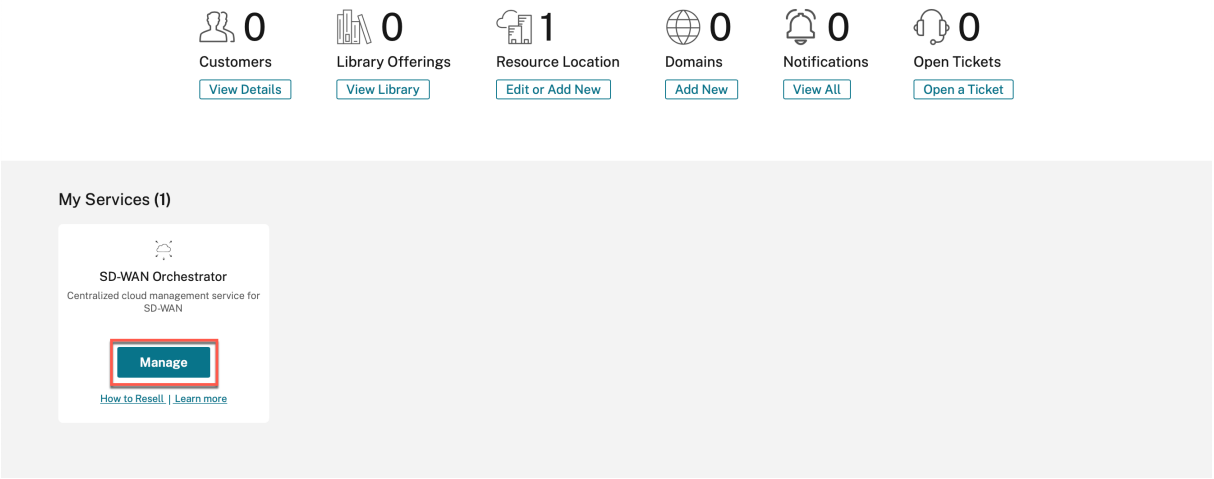
Un menu de tous les services disponibles sur Citrix Cloud s'affiche sur la page d'accueil. La vignette de **service Citrix SD-WAN Orchestrator** se trouve dans la section **Services disponibles** . Le partenaire

clique sur **Resell SD-WAN** sur la vignette pour s'enregistrer en tant que revendeur ou fournisseur de services Citrix SD-WAN.





La vignette du **service Citrix SD-WAN Orchestrator** s'affiche désormais sous **Mes services**.

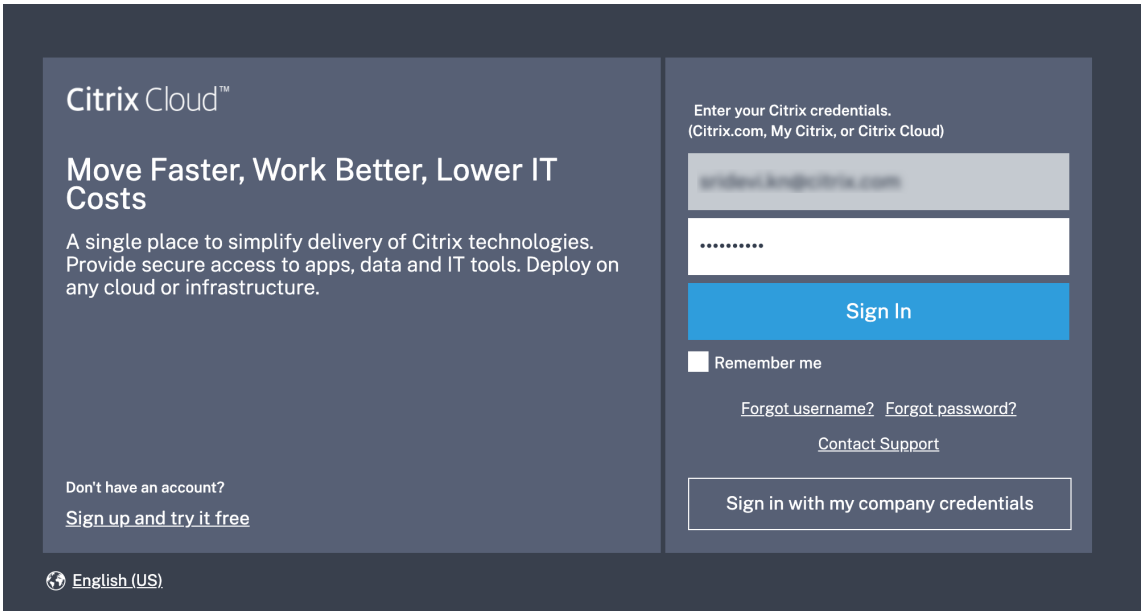


Intégration des clients DIY Enterprise

Cette section décrit le processus d'embarquement des clients d'entreprise DIY et la procédure à suivre pour inviter les administrateurs à gérer leur réseau SD-WAN.

Intégration des clients DIY

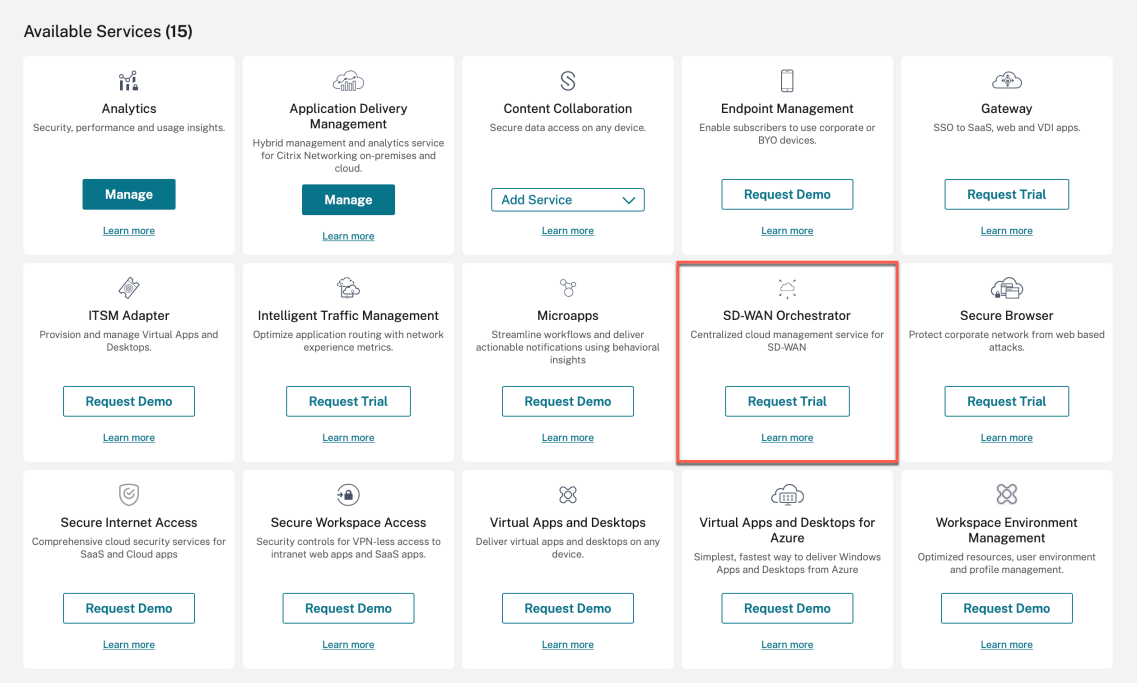
1. Le client se connecte au compte Citrix Cloud.



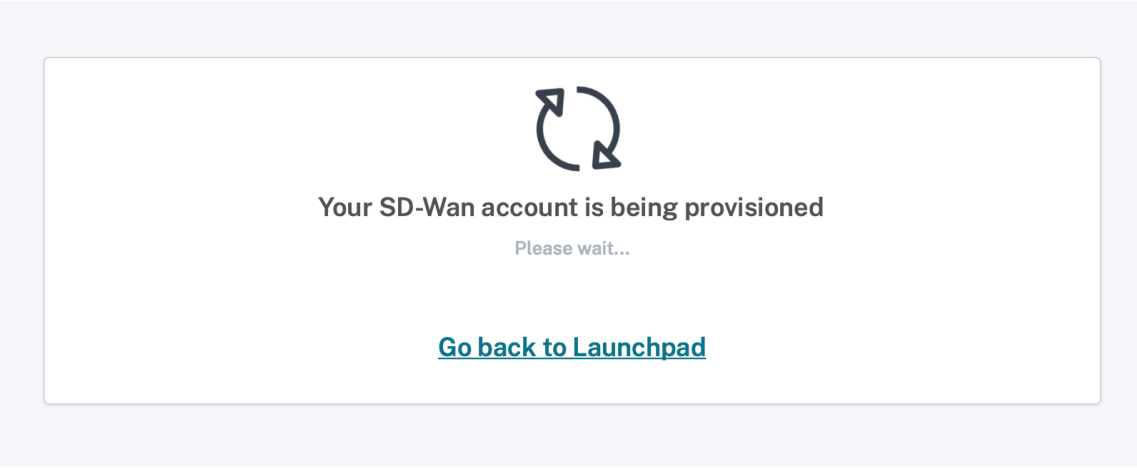
   Un menu de tous les services disponibles sur Citrix Cloud s'affiche sur la page d'accueil. La vignette de **service Citrix SD-WAN Orchestrator** se trouve dans la section **Services disponibles** .

> **Remarque**
>
> Assurez-vous de vous inscrire à Citrix Cloud à l'aide d'un seul compte officiel. Le nom de l'entreprise et l'identifiant d'e-mail utilisés doivent être associés à un seul compte Citrix Cloud.

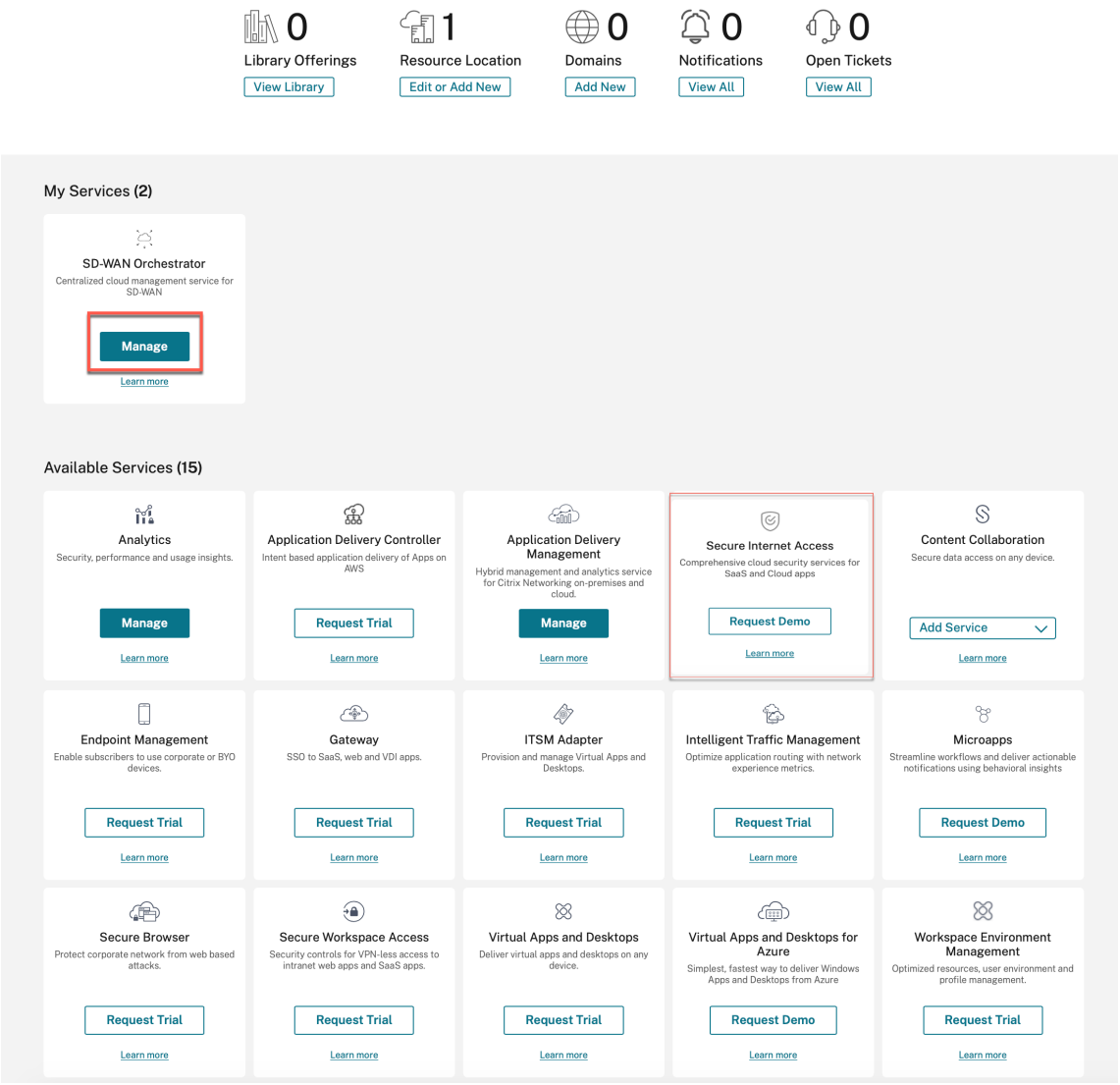
2. Le client clique sur **Demander un essai**.



Le compte SD-WAN du client est provisionné.



3. La vignette du **service Citrix SD-WAN Orchestrator** s'affiche désormais sous **Mes services**.



Citrix SD-WAN Orchestrator pour la connexion sur site

July 14, 2023

Cet article explique comment un client peut se connecter pour la première fois à Citrix SD-WAN Orchestrator pour locaux.

Voici les conditions préalables que vous devez remplir avant de vous connecter à Citrix SD-WAN Orchestrator pour les applications locales :

- Vous devez disposer d'un compte Citrix Cloud. Pour plus d'informations, voir Le client accède à SD-WAN Orchestrator.

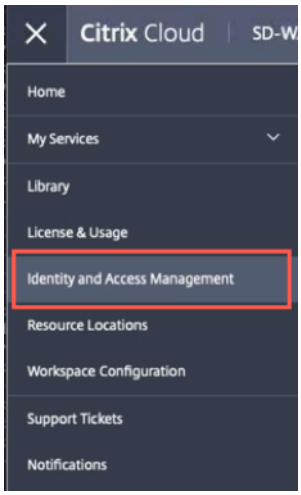
- Pour utiliser Citrix SD-WAN Orchestrator pour locaux, vous devez disposer d'un compte dans le service Citrix SD-WAN Orchestrator. Pour plus d'informations, consultez la section Intégration du service Citrix SD-WAN Orchestrator.
- Créez un administrateur doté de privilèges personnalisés.
- Créez un client à partir de la page d'accès à l'API pour obtenir l'identifiant, l'ID et les détails du secret du client. Ces informations sont nécessaires lors de la connexion à Citrix SD-WAN Orchestrator pour locaux

> **Remarque :**
>
> Sans la connexion au Cloud, vous ne pouvez pas passer à la connexion locale.

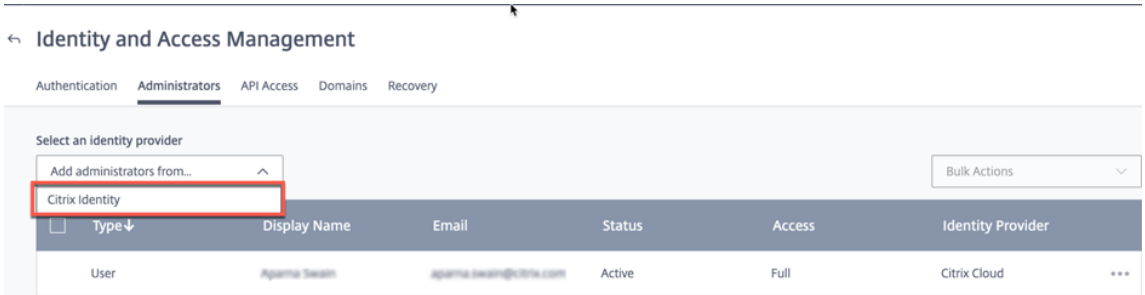
Créer un administrateur

Un fournisseur ou une entreprise cliente peut inviter un administrateur à gérer son réseau SD-WAN. Procédez comme suit pour inviter un administrateur :

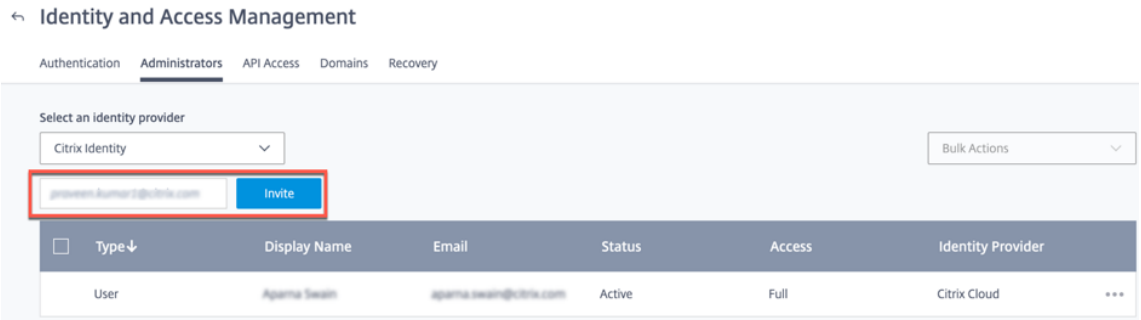
1. Connectez-vous au Citrix Cloud et accédez à **Gestion des identités et des accès**.



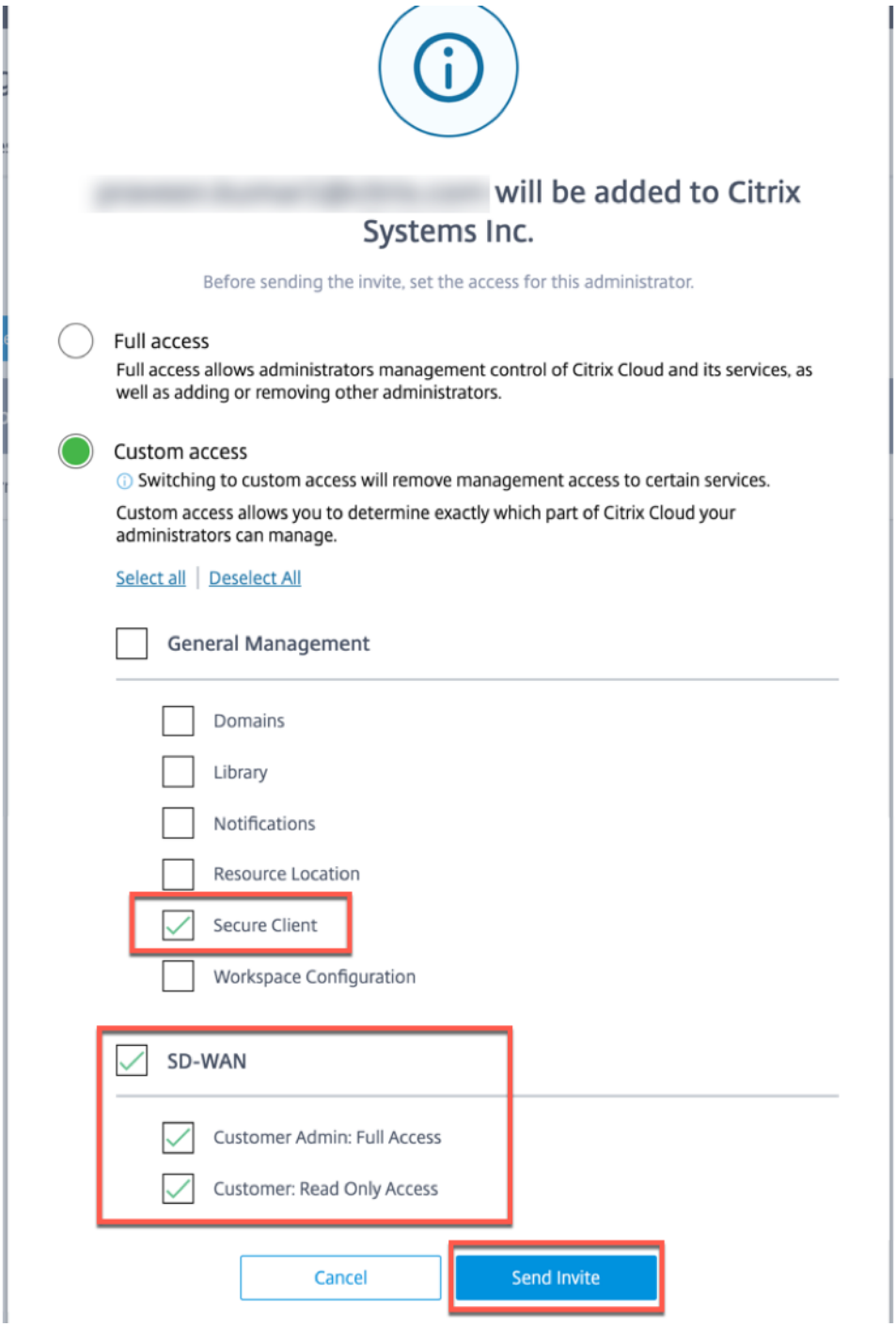
2. Accédez à la page **Administrateurs** et sélectionnez **Citrix Identity** dans la liste déroulante des fournisseurs d'identité.



3. Entrez le nouvel identifiant e-mail de l'administrateur et cliquez sur **Inviter**.



4. Vous pouvez choisir un **accès complet** ou un **accès personnalisé**. Il est recommandé de définir l'accès personnalisé pour l'administrateur qui gère uniquement les services SD-WAN. Lorsque le bouton radio **Accès personnalisé** est sélectionné, vous devez également cocher la case **Secure Client** dans la section **Gestion générale** et la case **SD-WAN** .



5. Cliquez sur **Envoyer invitation**.

Une fois que vous avez créé le compte administrateur, connectez-vous via le compte administrateur pour générer les clés d'**API** .

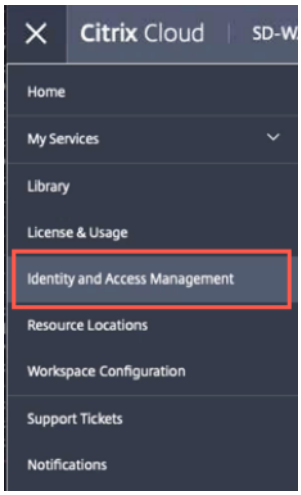
> **Remarque**
>
> Si vous avez déjà un rôle d'administrateur personnalisé, vous pouvez l'utiliser pour créer le jeton

> d'API.

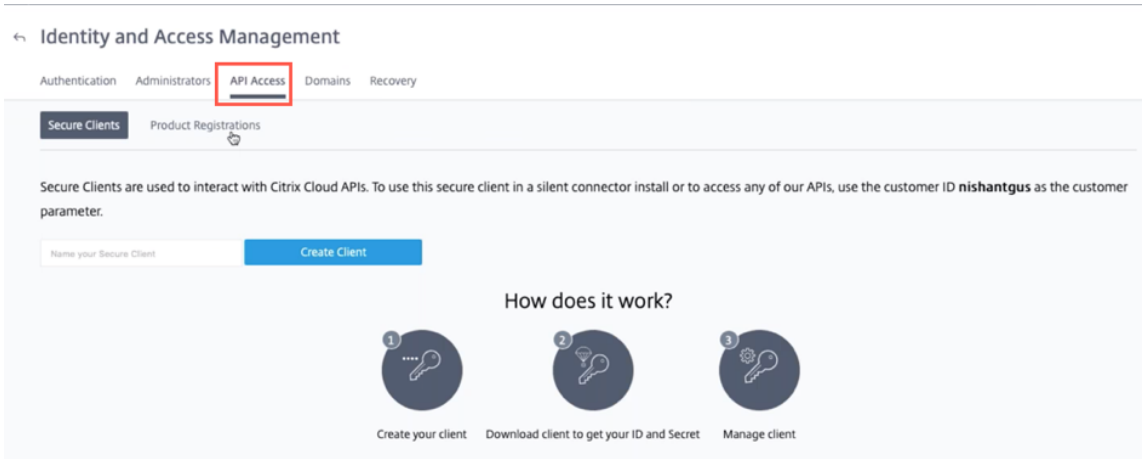
Générer un jeton API

Effectuez les étapes suivantes pour vous connecter à Citrix SD-WAN Orchestrator for On-premises.

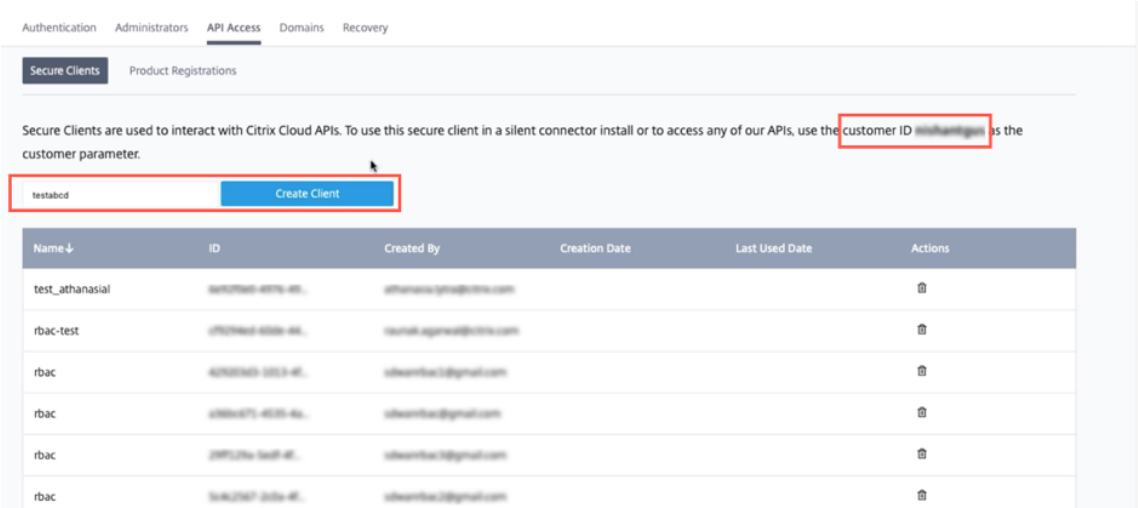
1. Connectez-vous au Citrix Cloud et accédez à **Gestion des identités et des accès**.



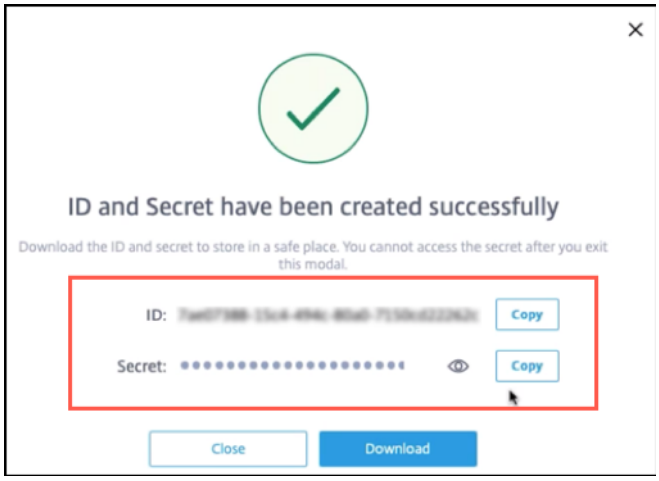
2. Accédez à la page **d'accès aux API** .



3. Créez un client. Notez l'**ID client** dont vous aurez besoin ultérieurement pour vous connecter à Citrix SD-WAN Orchestrator for On-premises.



4. Lorsque vous cliquez sur **Créer un client**, il vous fournit l'**identifiant** et une **clé secrète** que vous pouvez copier et enregistrer, ou télécharger.



5. Accédez à votre Citrix Hypervisor (XenServer/VMware) et démarrez Citrix SD-WAN Orchestrator pour les applications locales.
6. Une fois le Citrix SD-WAN Orchestrator pour site démarré, fournissez le nom d'utilisateur (admin) et le mot de passe (mot de passe) par défaut.

   > **Remarque :**
   >
   > Il est obligatoire de modifier le mot de passe du compte administrateur par défaut lors de la première connexion. Cette modification est appliquée en utilisant l'interface de ligne de commande et l'interface utilisateur.

7. Si le serveur DHCP n'est pas configuré sur le réseau SD-WAN, vous devez saisir manuellement une adresse IP statique. Pour configurer une adresse IP statique comme adresse IP de gestion :

   - Dans la console, entrez la commande CLI `management_ip`.

- Entrez la commande `set interface <ipaddress> <subnetmask> <gateway>`.

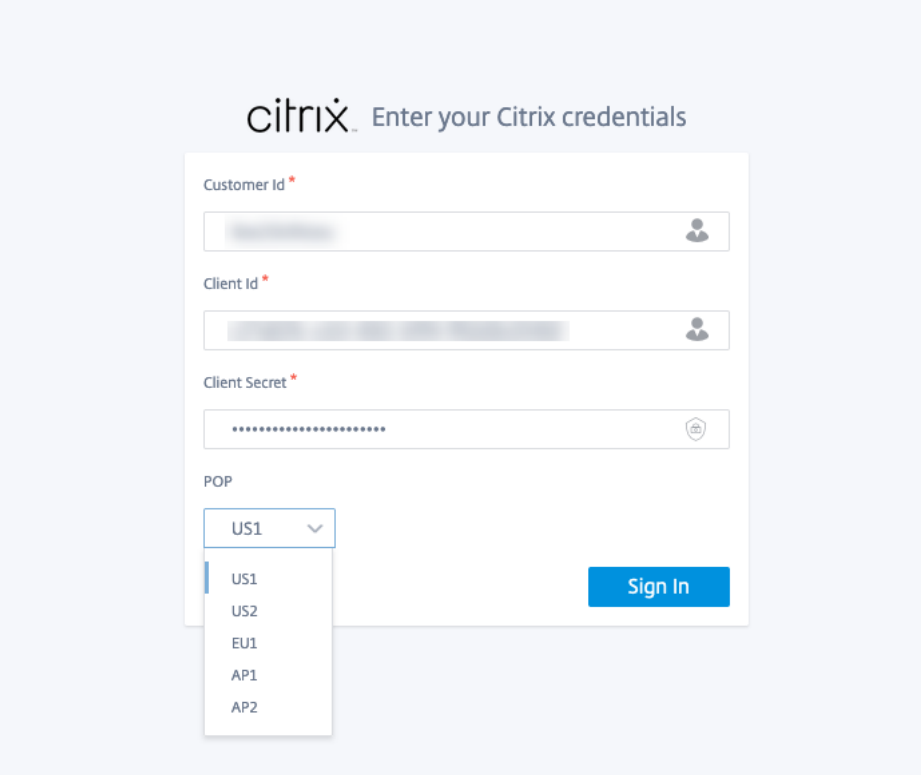
> **Remarque**
>
> - L'adresse IP de gestion est l'adresse IP de Citrix SD-WAN Orchestrator pour machine virtuelle sur site. Utilisez cette adresse IP pour vous connecter à l'interface utilisateur Web Citrix SD-WAN Orchestrator pour locaux.
> - L'interface de gestion peut être configurée via les deux méthodes : CLI et DHCP.

8. Une fois que Citrix SD-WAN Orchestrator for On-premises est démarré, il est configuré par défaut avec les serveurs DNS 9.9.9.9 et 149.112.112.112 comme serveurs principaux et secondaires respectivement. Si nécessaire, vous pouvez modifier l'adresse IP du serveur DNS à l'aide des commandes suivantes :

   - Dans la console, entrez la commande CLI `set_dns`.
   - Entrez la commande, `set primary <ipaddress>` puis entrez `y` pour confirmer la modification.
   - Entrez la commande `set secondary <ipaddress>` et entrez `y` pour confirmer la modification.

```
SDWORCH>set_dns

Primary :               nameserver 9.9.9.9
Seconday :              nameserver 149.112.112.112

Which would you like to do?
        "set primary <ip address>" - Stage New Primary DNS IP Address
        "set secondary <ip address>" - Stage New Primary DNS IP Address
        "clear" - Clear all DNS IP Address
        "main_menu" - Return to the Main Menu

set_dns>set primary 8.8.8.8

Are you sure you want to change your Domain Name Server IP settings? <y/n>?
y

Primary :               nameserver 8.8.8.8
Seconday :              nameserver 149.112.112.112

Which would you like to do?
        "set primary <ip address>" - Stage New Primary DNS IP Address
        "set secondary <ip address>" - Stage New Primary DNS IP Address
        "clear" - Clear all DNS IP Address
        "main_menu" - Return to the Main Menu

set_dns>set secondary 9.9.9.9

Are you sure you want to change your Domain Name Server IP settings? <y/n>?
y

Primary :               nameserver 8.8.8.8
Seconday :              nameserver 9.9.9.9

Which would you like to do?
        "set primary <ip address>" - Stage New Primary DNS IP Address
        "set secondary <ip address>" - Stage New Primary DNS IP Address
        "clear" - Clear all DNS IP Address
        "main_menu" - Return to the Main Menu
```

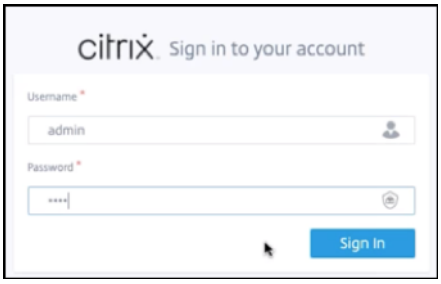
9. Ouvrez un nouveau navigateur à l'aide de l'adresse IP de gestion. L'écran suivant s'affiche :



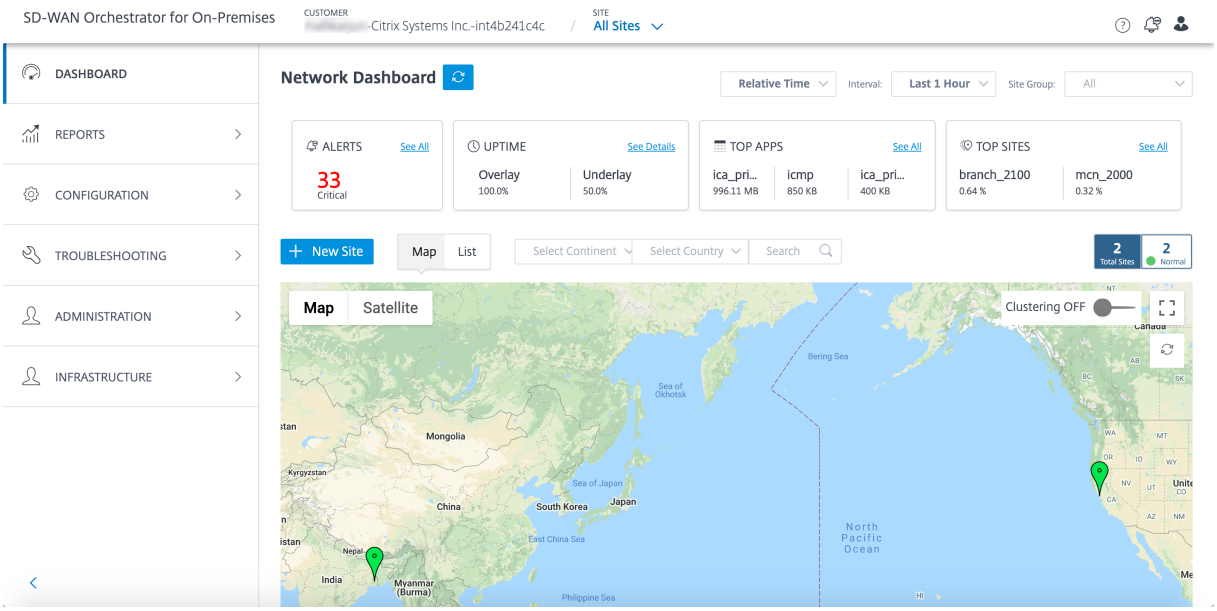
10. Fournissez l'**ID client, l'ID client** et le **secret client** que vous avez enregistrés ou téléchargés précédemment lors de la création du client à partir du cloud Orchestrator. Sélectionnez le POP dans lequel votre compte cloud a été intégré. Vous ne pouvez pas modifier le POP après une connexion réussie.

    > **Remarque**
    >
    > Cet écran s'affiche une fois tous les 15 jours. Pour la connexion/déconnexion suivante, seule la page de connexion locale s'affiche.

11. Indiquez le nom d'utilisateur et le mot de passe par défaut sur la page de connexion locale.



Vous pouvez voir que la page Citrix SD-WAN Orchestrator for On-premises Dashboard s'affiche.



Citrix SD-WAN Orchestrator pour les licences locales

October 21, 2022

Citrix SD-WAN Orchestrator pour les licences sur site s'applique aux clients Do It Yourself (DIY) et aux clients Direct Enterprise.

Comme condition préalable à Citrix SD-WAN Orchestrator pour les licences locales, assurez-vous d'être connecté au Citrix Cloud. Pour plus d'informations, consultez Citrix SD-WAN Orchestrator pour la connexion sur site.

Citrix SD-WAN Orchestrator pour le déploiement sur site est disponible gratuitement, mais le client doit prendre en charge les coûts de l'infrastructure et de la maintenance du serveur de gestion.

Mode d'essai

Le compte Citrix SD-WAN Orchestrator for On-premises du client est provisionné en mode d'essai. Le mode d'essai se poursuit pendant une période par défaut de 60 jours.

À l'expiration de la période d'essai, les chemins de données du client sont fermés. Les modifications supplémentaires ne peuvent pas être déployées tant que des licences valides n'ont pas été téléchargées. Le droit du client à Citrix Cloud pour Citrix SD-WAN Orchestrator pour site passe de la version d'essai à la version de production lorsque la première licence valide y est hébergée. En fonction du nombre et du type de licences téléchargées, un nombre équivalent de sites peut proposer les droits de bande passante appropriés. Un message persistant **Votre période d'essai a expiré.**

Passez à la version Production en récupérant au moins un droit de licence valide sur l'orchestrateur afin de restaurer les fonctionnalités du réseau et de continuer à l'utiliser. s'affiche pour les clients prépayés. Pour plus d'informations, voir Récupérer et attribuer des droits pour le modèle de facturation prépayé.

Modèle de facturation prépayée

Un modèle de facturation prépayé est fourni pour Citrix SD-WAN Orchestrator pour les clients sur site. Les trois types de modèles de facturation prépayée suivants sont disponibles :

- **Abonnement annuel prépayé** : L'abonnement prépayé comprend un plan d'un an et un plan de 3 ans. L'abonnement expire à la date d'expiration. Tous les appareils du réseau client disposent d'un abonnement annuel prépayé. Les licences de maintenance sont incluses dans le package d'abonnement et permettent de mettre à niveau les appliances vers des versions logicielles plus récentes.
- **Perpétuel prépayé** : Avec le mode perpétuel prépayé, les licences n'ont aucune limite de temps, aucune durée limitée ou aucune expiration. Toutefois, la licence de maintenance matérielle est disponible sous forme de module complémentaire payant et doit être achetée séparément. Tous les appareils du réseau client disposent d'un abonnement perpétuel prépayé.

Pour consulter le modèle de facturation dans Citrix SD-WAN Orchestrator pour locaux, au niveau du réseau, accédez à **Administration** > **Licences** > **Sélectionner le modèle de facturation**. Le modèle de facturation est affiché sous forme de **prépayé annuel et perpétuel**.

Téléchargez les licences sur tous les sites des clients. Pour plus d'informations, voir Récupérer et attribuer des droits pour le modèle de facturation prépayé.

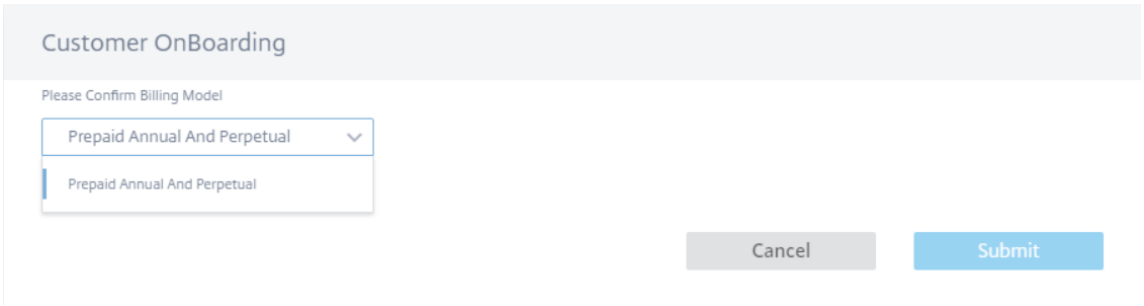
Récupérer et affecter des droits pour le modèle de facturation prépayée

Vous pouvez récupérer les droits de licence à l'aide du code d'accès fourni par Citrix par e-mail. Le client peut également consulter le code d'accès sur le portail de gestion des licences de Citrix Cloud. Le client peut avoir un modèle de facturation **prépayé perpétuel**ou un modèle de facturation par **abonnement annuel prépayé** sur le réseau.

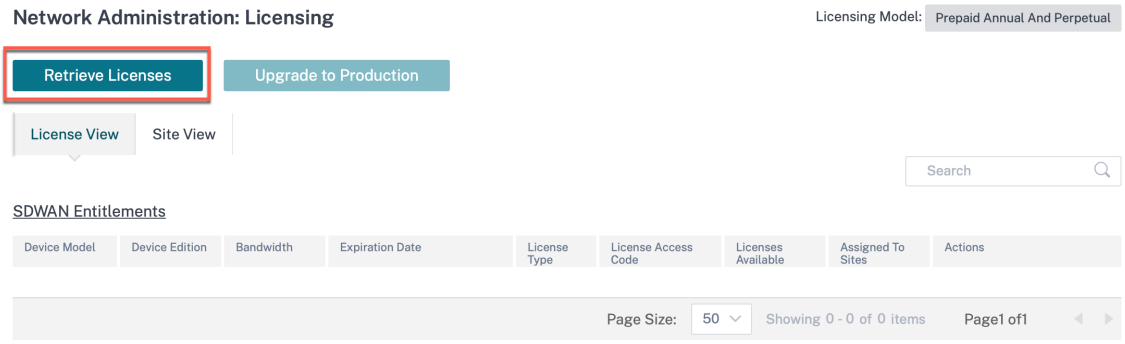
Prérequis : Assurez-vous que les licences Citrix SD-WAN Orchestrator pour les licences locales ne sont pas allouées en vous connectant au portail de gestion des licences. Si les licences sont allouées, libérez/désallouez les licences avant d'utiliser les codes d'accès aux licences dans le produit Citrix SD-WAN Orchestrator for On-premises.

1. Dans l'interface utilisateur de Citrix SD-WAN Orchestrator pour locaux, accédez à **Administration** > **Licences** et cliquez sur **Sélectionner le modèle de facturation**. Sélectionnez un modèle

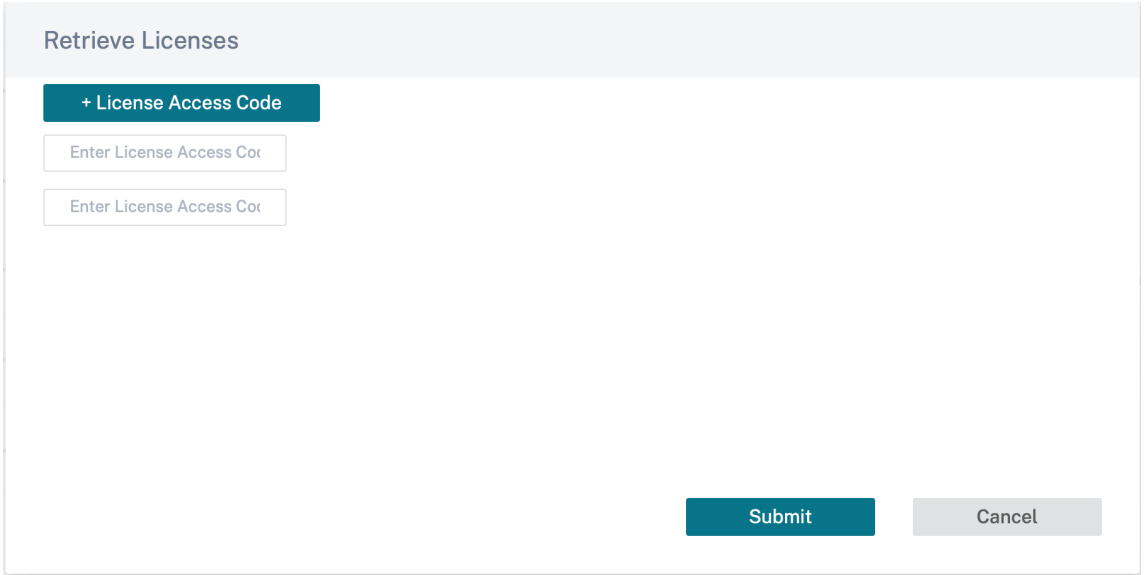
de facturation et cliquez sur **Soumettre**.



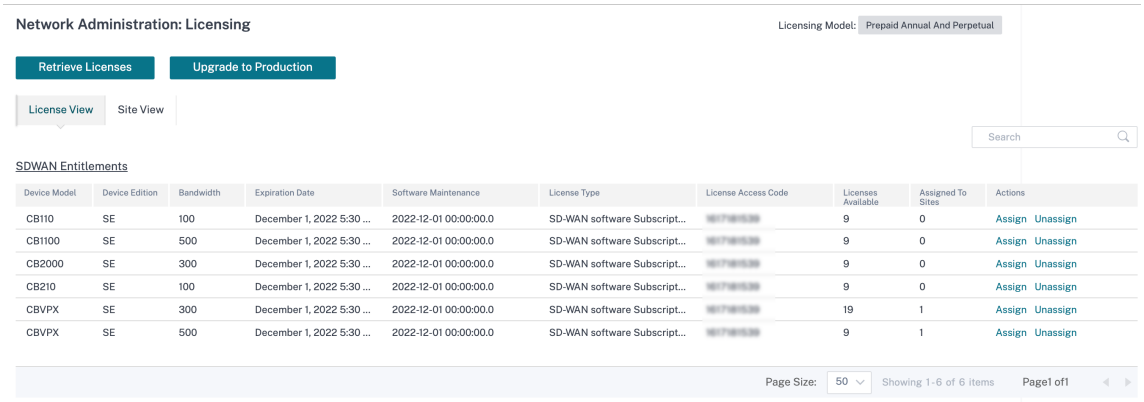
2. Cliquez sur **Récupérer les licences**.



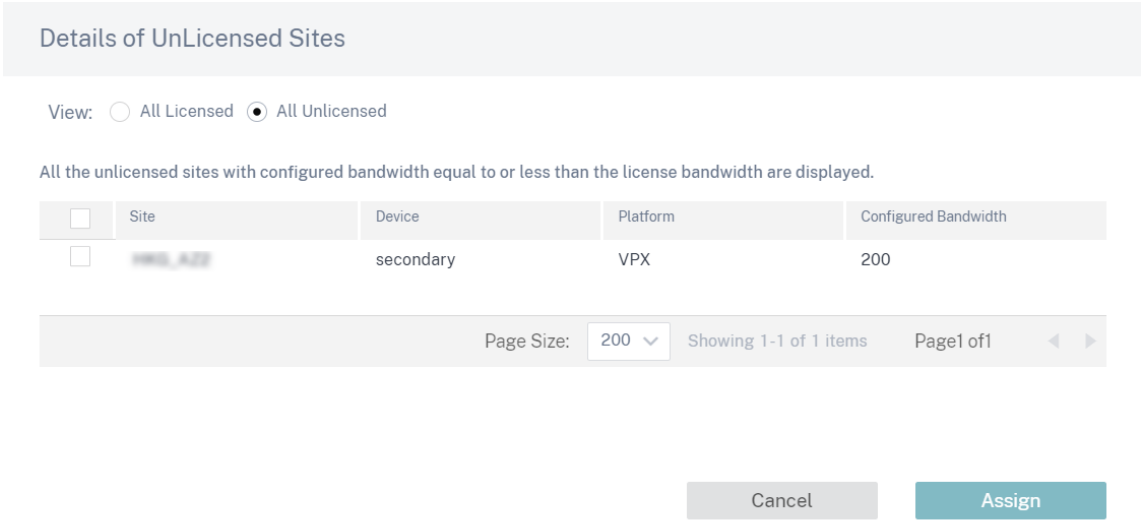
3. Cliquez sur **+ Code d'accès à la licence**, entrez le nombre de codes d'accès requis pour récupérer les droits et cliquez sur **Soumettre**.



Le Citrix SD-WAN Orchestrator pour locaux récupère les droits et renseigne le tableau des licences.

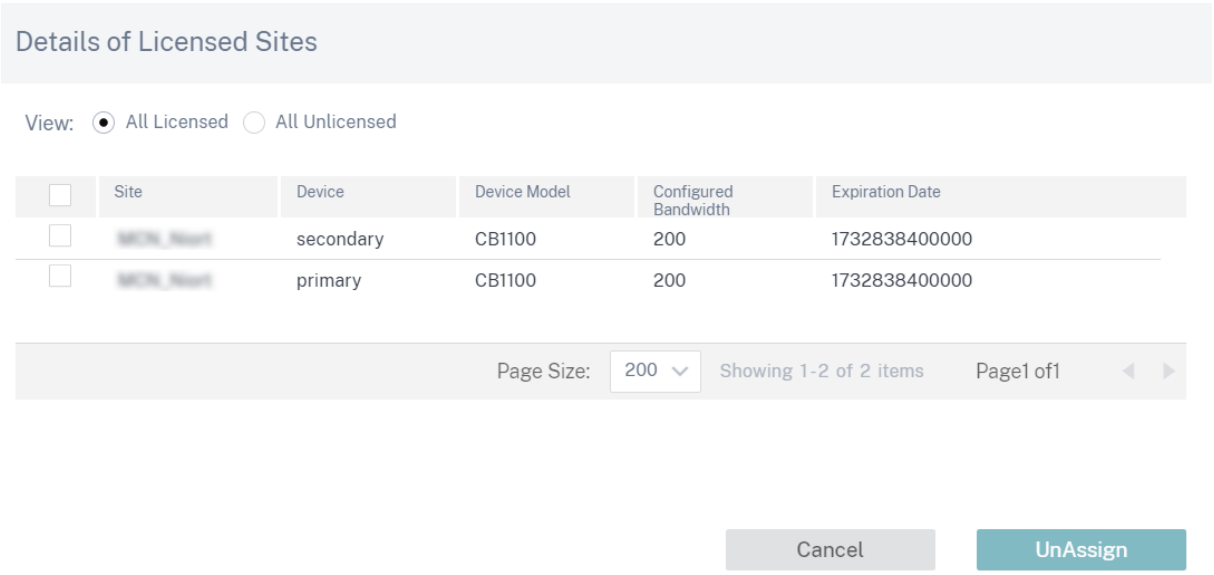


4. Cliquez sur **Affecter/Désattribuer** et sélectionnez **Tout sans licence**. Tous les sites sans licence dont la bande passante configurée est égale ou inférieure à la bande passante de licence s'affichent.



5. Sélectionnez les sites, cliquez sur **Attribuer**, puis sur **Mettre à niveau vers la production**.

Dans la vue **Toutes les licences**, la liste des sites sous licence s'affiche. Vous pouvez choisir de désaffecter les licences et de les libérer dans le pool.



Dans **Site View**, les sites sont automatiquement associés à des licences en fonction de la bande passante et de la bande passante de licence configurées, ce qui vous permet d'allouer rapidement les licences.

> **Remarque**
>
> Pour attribuer une licence à l'appliance, elle doit avoir un numéro de série vérifié.

Expiration de licence

À l'expiration de la licence, un délai de grâce de 30 jours est accordé. Le partenaire/client est censé renouveler ses licences pendant cette période. Une fois la période de grâce expirée, les chemins de données réseau du client sont désactivés et les modifications supplémentaires ne peuvent pas être déployées tant que les licences ne sont pas renouvelées.

Connectivité avec les appliances Citrix SD-WAN

October 21, 2022

Après avoir configuré les sites sur Citrix SD-WAN Orchestrator pour locaux, établissez la connectivité entre les appliances Citrix SD-WAN sur les sites à l'aide de Citrix SD-WAN Orchestrator pour locaux. Vous pouvez établir la connectivité de l'une des manières suivantes :

- **Authentification unidirectionnelle** : l'appliance SD-WAN authentifie Citrix SD-WAN Orchestrator pour les applications locales. Lorsque vous activez l'authentification unidirectionnelle, vous devez télécharger le certificat Citrix SD-WAN Orchestrator for On-premises et le télécharger sur l'appliance SD-WAN.
- **Authentification bidirectionnelle** : Le SD-WAN s'authentifie mutuellement à l'aide des certificats échangés. Lors de l'activation de l'authentification bidirectionnelle, vous devez télécharger le certificat de l'appliance SD-WAN sur Citrix SD-WAN Orchestrator pour site et également le certificat Citrix SD-WAN Orchestrator pour site sur l'appliance SD-WAN.
- **Aucune authentification** : La connectivité est établie entre le Citrix SD-WAN Orchestrator pour locaux et les appliances SD-WAN sans authentification. Vous n'avez pas besoin d'utiliser l'appliance SD-WAN ou Citrix SD-WAN Orchestrator pour le certificat sur site. Vous pouvez utiliser l'option Aucune authentification lorsque vous disposez d'un réseau sécurisé tel que MPLS.

> **Remarque**
>
> Il est recommandé de n'utiliser que l'authentification **unidirectionnelle ou l'** authentification bidirectionnelle. En l'absence d'authentification, vous devez choisir le serveur DNS sécurisé.

Vous pouvez configurer la connectivité avec chaque site manuellement ou utiliser le déploiement automatique sans intervention.

> **Remarque**
>
> Citrix SD-WAN 11.3.0 est la version logicielle minimale requise pour qu'une appliance se connecte à Citrix SD-WAN Orchestrator pour les applications locales.

Déploiement sans contact

Le déploiement sans intervention est un processus automatisé qui permet de configurer la connectivité entre les appliances et Citrix SD-WAN Orchestrator pour les applications sur site. Vous pouvez établir la connectivité automatiquement à l'aide de paramètres de déploiement Zero Touch non cloud ou de déploiements Zero Touch négociés dans le cloud.

Déploiement sans intervention sur le cloud

Les paramètres de déploiement sans intervention sur le cloud vous permettent de configurer Citrix SD-WAN Orchestrator pour obtenir des informations sur site sur les appliances SD-WAN. L'API NITRO

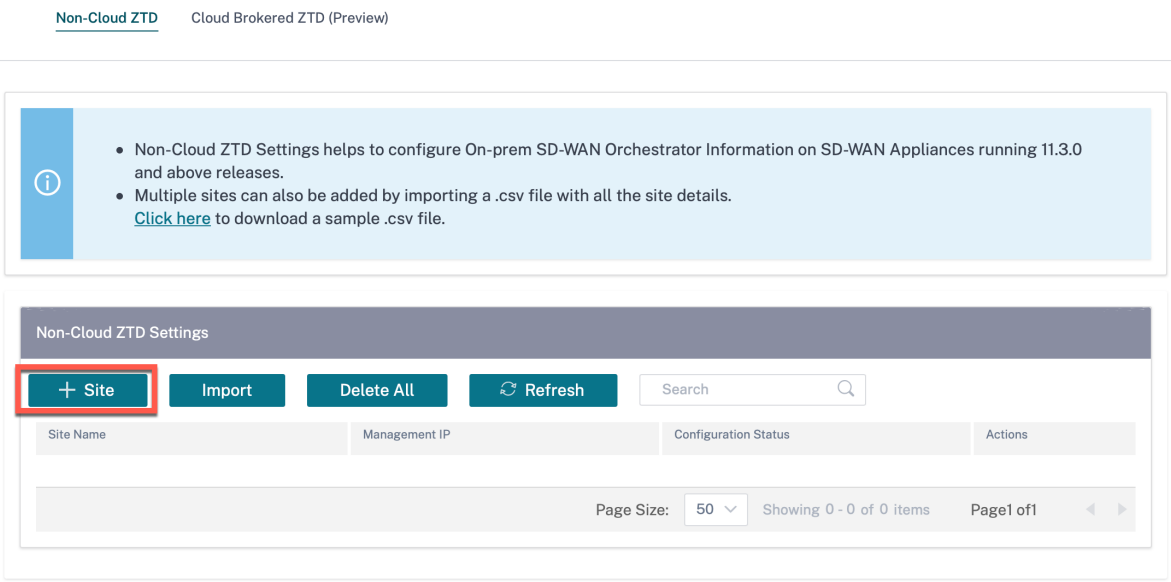
exécutée dans le back-end gère le téléchargement et le chargement des certificats. Il télécharge le certificat depuis Citrix SD-WAN Orchestrator pour locaux, se connecte à l'appliance SD-WAN et télécharge le certificat. Il télécharge également le certificat de l'appliance SD-WAN et le télécharge sur Citrix SD-WAN Orchestrator pour les applications locales.

> **Remarque**
>
> Le déploiement sans intervention sur le cloud est pris en charge sur les appliances SD-WAN fonctionnant avec la version 11.3.0 ou ultérieure.

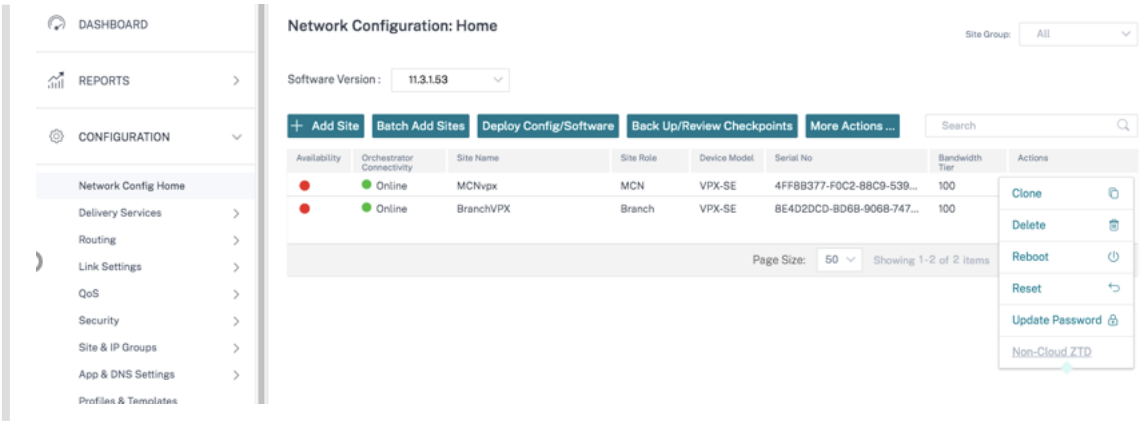
Le déploiement sans contact prend uniquement en charge l'authentification **unidirectionnelle et l'authentification bidirectionnelle**.**Aucune authentification n'**est prise en charge. Si le**type d'authentification**est activé sur la page**Administration > Authentification par certificat**, l'authentification bidirectionnelle est établie. Si le**type d'authentification** est désactivé, l'authentification unidirectionnelle est établie.

Vous pouvez ajouter des sites manuellement ou importer un fichier CSV pour ajouter plusieurs sites simultanément.

Pour configurer les paramètres de déploiement sans contact sur le cloud, accédez à **Administration** > **Paramètres ZTD** > **ZTD non cloud**, puis cliquez sur **+ Site**.



> **Remarque**
>
> Vous pouvez également accéder aux paramètres de déploiement sans intervention sur le cloud pour chaque site à partir de la page d'**accueil de la configuration réseau** . Cliquez sur l'icône d'action du site et sélectionnez **ZTD non cloud**.



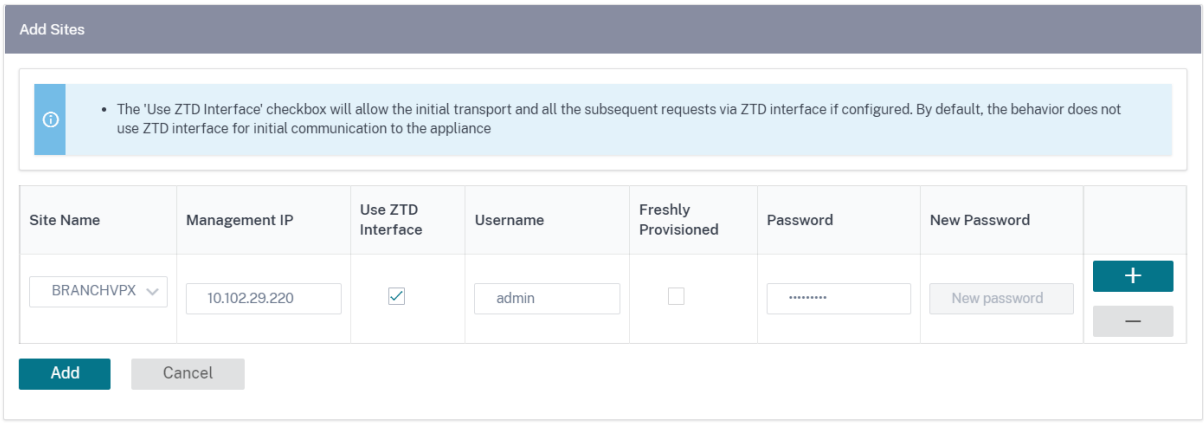
Sélectionnez un site dans la liste déroulante **Nom du site** et entrez l'adresse **IP de gestion** de l'appliance Citrix SD-WAN.

L'activation de l'option **Utiliser l'interface ZTD** garantit que l'interface ZTD est utilisée pour les ZTD non cloud, si l'interface ZTD est activée sur SD-WAN Orchestrator for On-premises.

> **Remarque**
>
> - Ignorez l'option **Utiliser l'interface ZTD**, si l'interface ZTD n'est pas activée sur SD-WAN Orchestrator for On-premises.
> - Activez l'option **Utiliser l'interface ZTD** lorsque l'appliance SD-WAN peut accéder à l'adresse IP de l'interface ZTD mais ne peut pas accéder à l'adresse IP de gestion.
> - Ne pas sélectionner l'option **Utiliser l'interface ZTD** après avoir activé l'interface ZTD ne signifie pas que l'adresse IP de l'interface de gestion est utilisée pour la communication entre l'appliance SD-WAN et le SD-WAN Orchestrator for On-premises. L'option **Utiliser l'interface ZTD** est utilisée uniquement pour la configuration initiale de l'appliance à l'aide de ZTD non cloud.

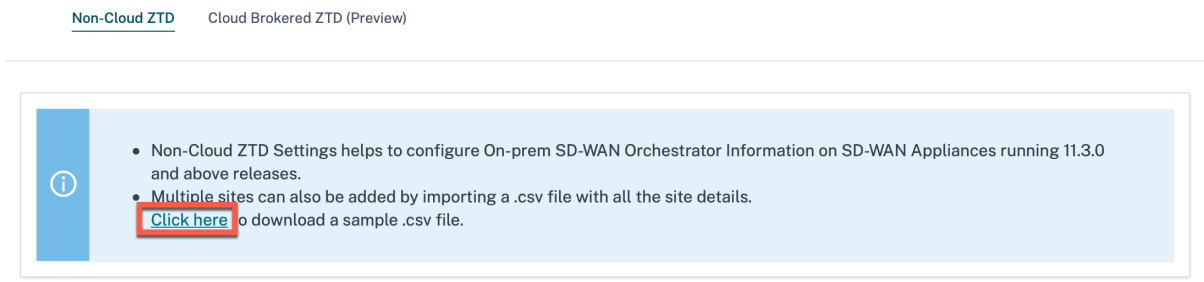
Entrez le nom d'utilisateur et le mot de passe du dispositif. Cochez la case **Freshly Provisioned** si vous ajoutez un site récemment approvisionné sur lequel le mot de passe par défaut n'a pas été modifié. Entrez le **nouveau mot de passe**. Le mot de passe par défaut est remplacé par le nouveau mot de passe au cours de ce processus de déploiement sans intervention.

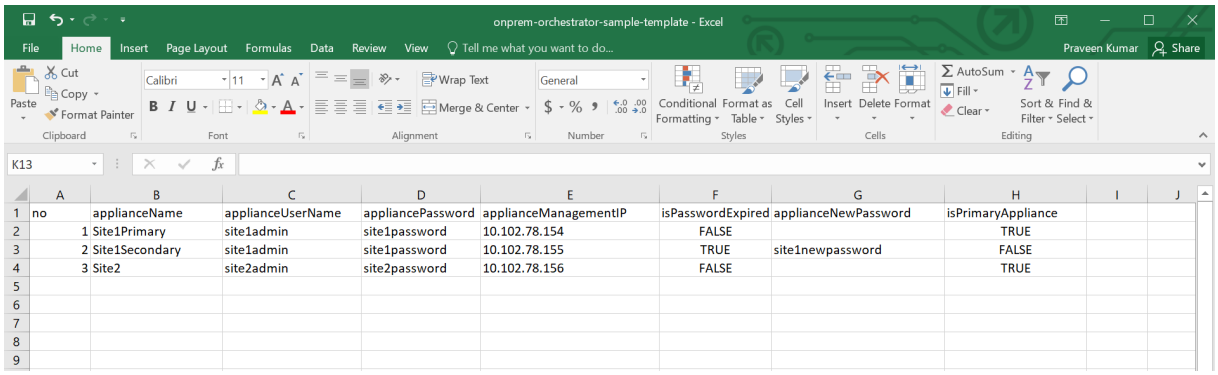
> **Remarque**
>
> Pour un site nouvellement approvisionné, il est obligatoire de modifier le mot de passe par défaut lors de la première connexion.



Cliquez sur **+** pour continuer à ajouter d'autres sites.

Vous pouvez également importer un fichier CSV pour ajouter plusieurs sites simultanément. Un exemple de modèle téléchargeable est disponible dans l'interface utilisateur. Téléchargez-le et fournissez les détails du site.



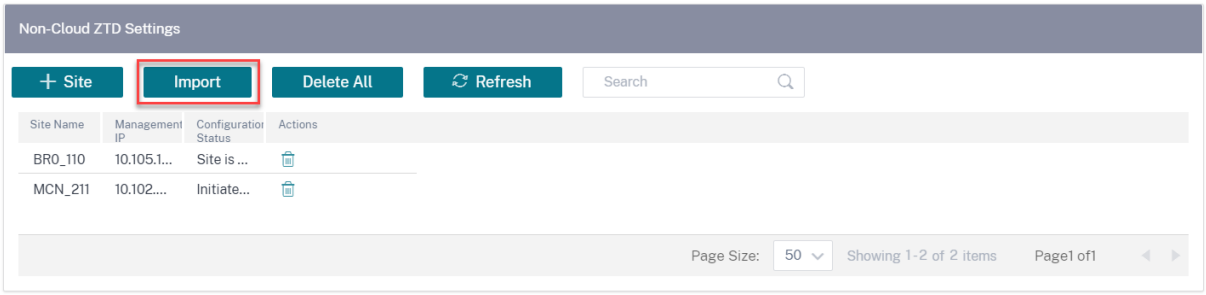


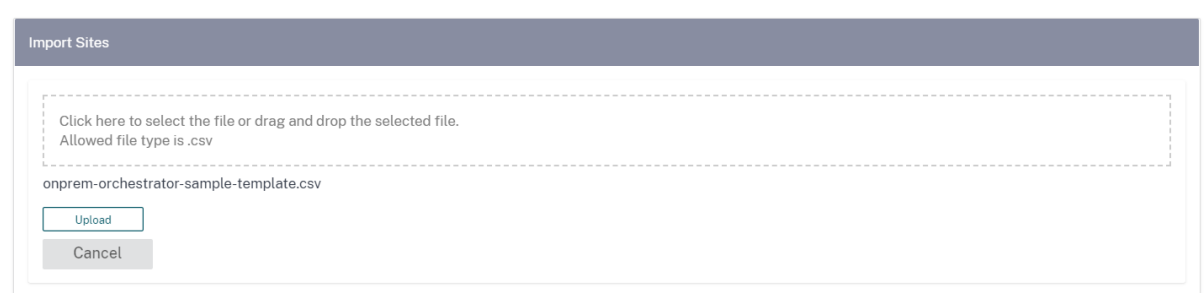
- **Nom de l'appliance** : nom du site configuré lors de la configuration du site. Pour plus d'informations, consultez la section Configuration du site.
- **Nom d'utilisateur de l'appliance** : nom d'utilisateur configuré sur l'appliance du site.
- **Mot de passe de l'appliance** : mot de passe correspondant à l'appliance du site.
- **Le mot de passe a-t-il expiré** ? Détermine si l'appliance vient d'être approvisionnée. Si la valeur est **True, entrez**le **nouveau mot de passe de l'appliance**.
- **Nouveau mot de passe de l'appliance** : mot de passe pour les appliances fraîchement approvisionnées. Si la valeur Le **mot de passe est-il expiré** est **True**, entrez le **nouveau mot de passe**

de l'appliance.

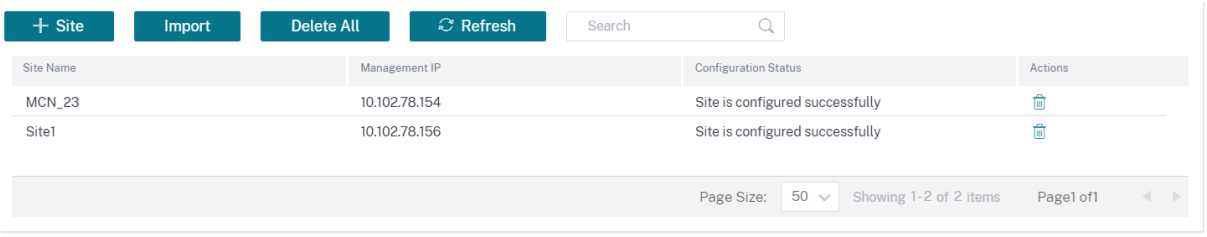
- **Est une appliance principale** : si la haute disponibilité (HA) est configurée, l'appliance active doit avoir la valeur True et l'appliance de secours doit avoir la valeur False. Si HA n'est pas configuré, la valeur doit être True.

Cliquez sur **Importer**, sélectionnez le fichier CSV et cliquez sur **Télécharger**.





L'état de configuration des sites s'affiche. Vous pouvez choisir de supprimer les sites individuellement ou de tout supprimer si les sites ne sont pas nécessaires pour un déploiement sans intervention.



Déploiement Zero Touch négocié dans le cloud

Le déploiement Zero Touch négocié dans le cloud utilise le service Citrix SD-WAN Orchestrator comme intermédiaire entre Citrix SD-WAN Orchestrator pour locaux et les appliances Citrix SD-WAN. Citrix SD-WAN Orchestrator pour locaux envoie un package de configuration de déploiement sans intervention dans le cloud au service Citrix SD-WAN Orchestrator. Le package de configuration du déploiement cloud Zero-Touch comprend les informations suivantes :

- Informations d'identité sur site
- Type d'authentification

- Certificat sur site
- Détails de l'appareil (liste des numéros de série)

Le service Citrix SD-WAN Orchestrator stocke les informations reçues de Citrix SD-WAN Orchestrator pour les applications locales. Lorsqu'une appliance contacte le service Citrix SD-WAN Orchestrator avec son numéro de série, l'intelligence acquise par le service Citrix SD-WAN Orchestrator détermine que l'appliance doit être gérée par Citrix SD-WAN Orchestrator for On-premises. Le service Citrix SD-WAN Orchestrator transmet le Citrix SD-WAN Orchestrator pour les informations sur site à l'appliance. L'appliance Citrix SD-WAN envoie son certificat au service Orchestrator. Le service Citrix SD-WAN Orchestrator reçoit et stocke le certificat de l'appliance.

Citrix SD-WAN Orchestrator pour locaux récupère régulièrement le certificat de l'appliance auprès du service Citrix SD-WAN Orchestrator. Une fois qu'une connexion sécurisée est établie entre Citrix SD-WAN Orchestrator pour locaux et l'appliance, le Citrix SD-WAN Orchestrator pour locaux transmet la configuration et les fichiers pertinents aux appliances.

Les paramètres de déploiement Zero Touch négociés dans le cloud ne sont disponibles que pour les clients dans une configuration gérée par le client. La configuration gérée par le fournisseur ne prend pas en charge les paramètres de déploiement Zero Touch négociés dans le cloud.

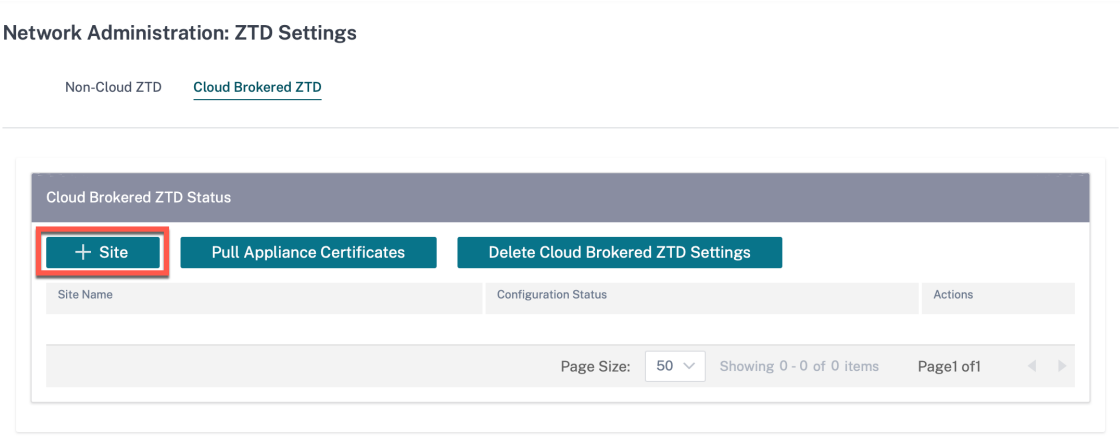
Conditions préalables

- Les appliances doivent accéder aux noms de domaine suivants pour établir une connexion avec le service Citrix SD-WAN Orchestrator :
  - sdwanzt.citrixnetworkapi.net
  - download.citrixnetworkapi.net
  - trust.citrixnetworkapi.net
  - sdwan-home.citrixnetworkapi.net
- Assurez-vous que Citrix SD-WAN Orchestrator pour locaux dispose toujours d'une connectivité au service Citrix SD-WAN Orchestrator pour les appliances SD-WAN intégrées.
- Assurez-vous que l'appliance Citrix SD-WAN est connectée au service SD-WAN Orchestrator lors du processus d'intégration initial et si la réinitialisation d'usine est effectuée sur l'appliance SD-WAN.

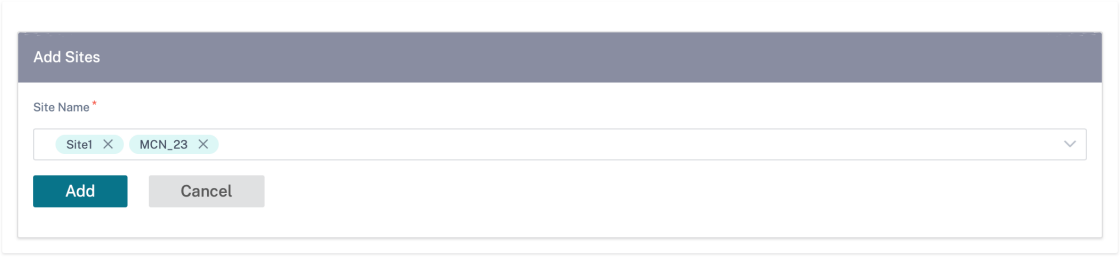
Pour configurer les paramètres de déploiement Zero Touch proposés par Cloud, procédez comme suit :

1. Dans Citrix SD-WAN Orchestrator pour locaux, créez et définissez des sites à l'aide du flux de travail guidé. Pour plus d'informations, voir Configuration du site.
2. Vérifiez et compilez la configuration à l'aide du suivi de déploiement. Pour plus d'informations, consultez la section Deployment Tracker dans la rubrique Configuration réseau .

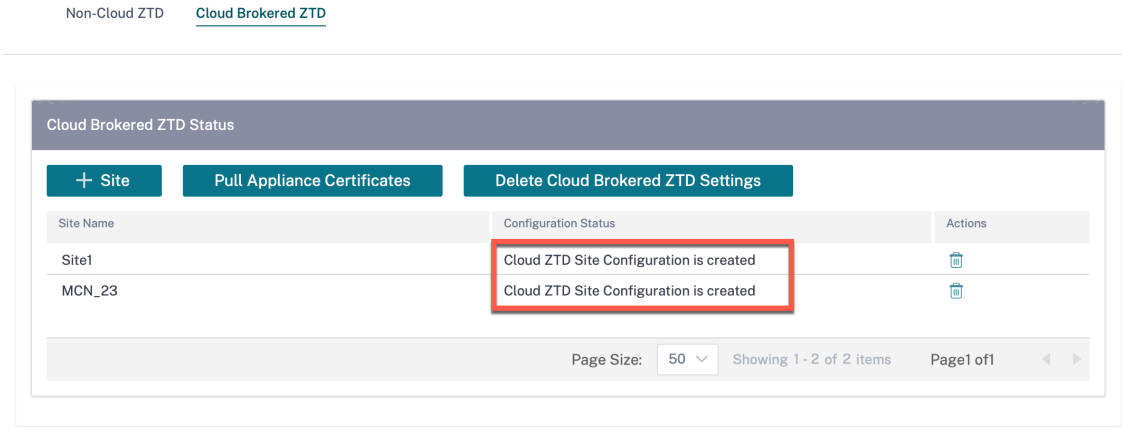
3. Accédez à **Administration > Paramètres ZTD > Cloud Brokered ZTD** et cliquez sur **+ Site**.



4. Dans la liste déroulante, sélectionnez un nom de site et cliquez sur **Ajouter**. Les sites sont répertoriés en fonction de votre configuration. Vous pouvez sélectionner un seul site ou plusieurs sites.



5. La configuration de déploiement sans contact dans le cloud est créée et envoyée au service Citrix SD-WAN Orchestrator.

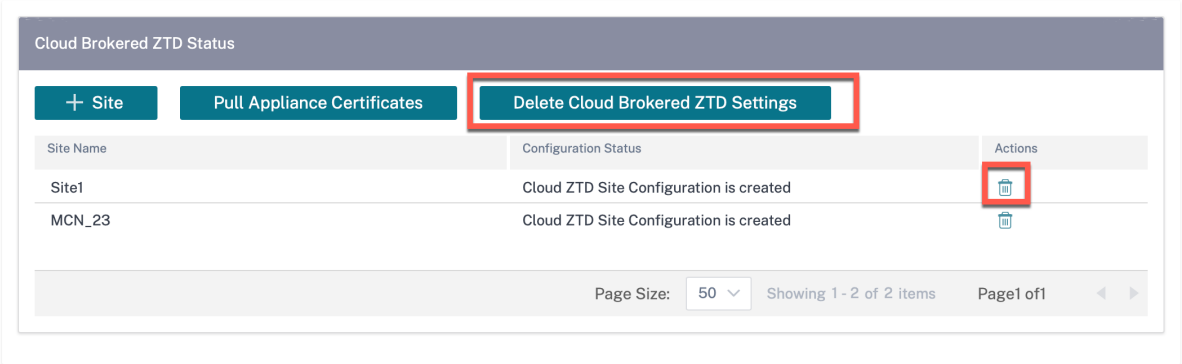


6. Branchez et allumez les appliances SD-WAN du centre de données et des succursales.
7. Les appliances contactent le service Citrix SD-WAN Orchestrator avec leur numéro de série.

8. Le service Citrix SD-WAN Orchestrator agit en tant que courtier entre Citrix SD-WAN Orchestrator for On-premises et les appliances. Il permet l'échange de certificats et l'appliance Citrix SD-WAN établit une connexion sécurisée avec Citrix SD-WAN Orchestrator pour les environnements locaux. Une fois le déploiement sans intervention réussi, le site configuré est mis en ligne et s'affiche dans la colonne **Orchestrator Connectivity** sous **Configuration > Network Config Home**.
9. **Activez** et **organisez** la configuration pour transférer la configuration et le logiciel aux appliances.
10. Une fois la configuration/le logiciel appliqué, les chemins virtuels sont établis et la colonne **Disponibilité** sous **Configuration > Network Config Home** est mise à jour avec l'état du chemin virtuel approprié.

> **REMARQUE :**
>
> Citrix SD-WAN Orchestrator pour locaux prend environ 30 minutes pour récupérer le certificat de l'appliance et intégrer complètement les appliances. Pour extraire les certificats de l'appliance immédiatement (sans attendre 30 minutes), cliquez sur **Extraire les certificats de l'appliance**.

Si nécessaire, vous pouvez choisir de cliquer sur **Supprimer les paramètres ZTD de Cloud Brokered**. Il supprime les informations relatives à tous les sites. Si vous devez supprimer les informations d'un site en particulier, cliquez sur l'icône de suppression correspondant à ce site.



Limitations

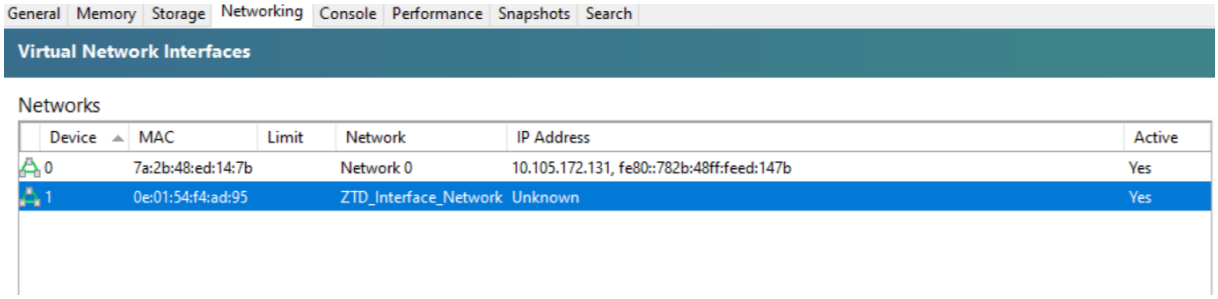
- Les appliances SD-WAN ne peuvent pas se connecter à plusieurs instances de Citrix SD-WAN Orchestrator pour locaux qui partagent des informations de connexion au cloud. Par exemple, une appliance SD-WAN reste connectée à Citrix SD-WAN Orchestrator for On-premises configuré pour la première fois. Le Citrix SD-WAN Orchestrator pour les détails locaux qui sont configurés ensuite ne sont pas transmis à l'appliance SD-WAN.
- Les appliances SD-WAN connectées via LTE ne peuvent pas établir de connexion avec Citrix SD-WAN Orchestrator pour les solutions locales hébergées sur un réseau privé.

Paramètres de l'interface ZTD

Vous pouvez activer une interface Zero Touch Deployment (ZTD) sur SD-WAN Orchestrator pour les applications sur site. L'interface ZTD sécurisée par une authentification bidirectionnelle fournit une interface de communication sécurisée pour les appliances SD-WAN et l'SD-WAN Orchestrator pour les applications sur site.

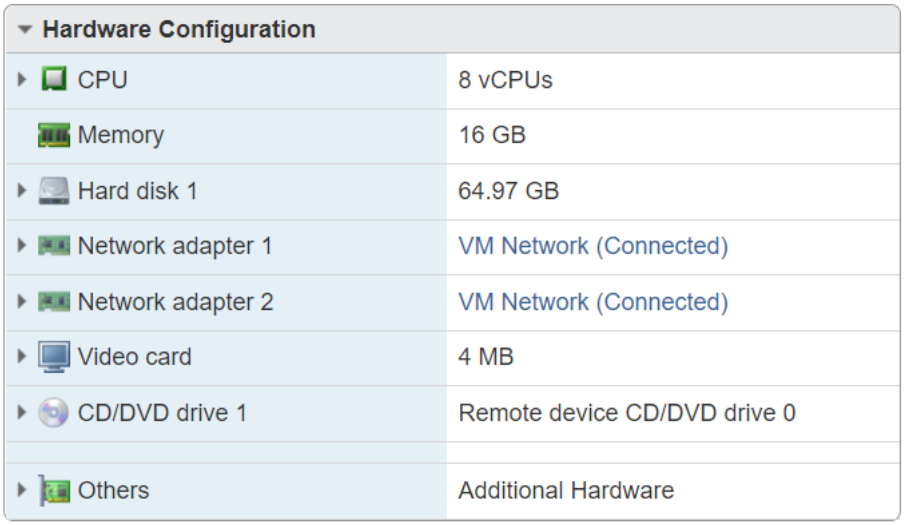
Après avoir activé l'interface ZTD, les nouvelles appliances D-WAN déployées via la technologie ZTD non cloud et la technologie ZTD négociée dans le cloud utilisent l'adresse IP de l'interface ZTD pour communiquer avec SD-WAN Orchestrator pour les applications sur site.

Comme condition préalable, assurez-vous que SD-WAN Orchestrator pour machine virtuelle sur site dispose d'une interface supplémentaire, en plus de l'interface de gestion.



Remarque

Pour la machine virtuelle VMware ESXi, assurez-vous que la machine virtuelle est redémarrée après avoir ajouté une interface supplémentaire pour ZTD.

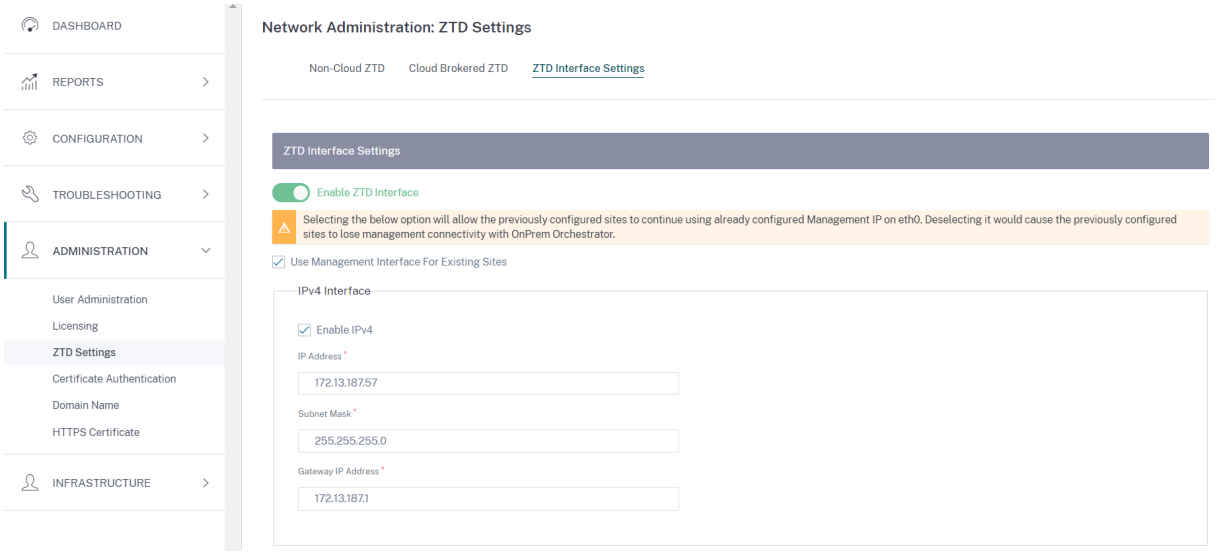


Activation de l'interface ZTD

Dans l'interface utilisateur graphique locale de SD-WAN Orchestrator, accédez à **Administration** > **Paramètres ZTD** et sélectionnez **Activer l'interface ZTD** pour activer l'interface ZTD. Fournissez l'adresse IP de l'interface ZTD, le masque de sous-réseau et l'adresse IP de la passerelle.

Sélectionnez **Utiliser l'interface de gestion pour les sites existants pour** vous assurer que les appliances SD-WAN déjà déployées via le ZTD non-Cloud ou le Cloud Brokered-ZTD continuent à se connecter à SD-WAN Orchestrator pour les sites locaux à l'aide de l'adresse IP de l'interface de gestion.

> **Avertissement**
>
> Si l'option **Utiliser l'interface de gestion pour les sites existants** n'est pas sélectionnée, les appliances SD-WAN déjà déployées via le ZTD non-Cloud ou le Cloud Brokered-ZTD perdent la connexion au SD-WAN Orchestrator for On-premises.



Configuration de ZTD non cloud à l'aide de l'interface ZTD Si l'option **Utiliser l'interface de gestion pour les sites existants** est sélectionnée, les appliances déjà déployées à l'aide de Non-Cloud ZTD continuent d'utiliser l'adresse IP de l'interface de gestion pour se connecter à SD-WAN Orchestrator for On-premises. Initiez un ZTD non cloud sur les appliances afin d'établir une connexion avec SD-WAN Orchestrator for On-premises à l'aide de l'adresse IP de l'interface ZTD.

> **Remarque**
>
> Vous pouvez désactiver l'option Utiliser l'interface de gestion pour les sites existants une fois que toutes les appliances SD-WAN ont établi une connexion avec SD-WAN Orchestrator for On-premises via l'adresse IP de l'interface ZTD.

Si l'option **Utiliser l'interface de gestion pour les sites existants** n'est pas sélectionnée, les appliances SD-WAN déjà déployées à l'aide de Non-Cloud ZTD perdent la connexion à SD-WAN Orchestrator for On-premises. Lancez la technologie ZTD non cloud sur les appliances SD-WAN afin de rétablir la connexion avec SD-WAN Orchestrator pour les applications sur site à l'aide de l'adresse IP de l'interface ZTD.

Configuration de Cloud Brokerd ZTD à l'aide de l'interface ZTD Si l'option **Utiliser l'interface de gestion pour les sites existants** est sélectionnée, les appliances déjà déployées à l'aide de Cloud Brokered ZTD continuent d'utiliser l'adresse IP de l'interface de gestion pour se connecter à SD-WAN Orchestrator pour les sites locaux. Pour établir une connexion avec SD-WAN Orchestrator for On-premises à l'aide de l'adresse IP de l'interface ZTD, effectuez l'une des opérations suivantes :

- Sur les appliances SD-WAN, mettez à jour l'adresse IP et le certificat du SD-WAN Orchestrator for On-premises.

  > **Remarque**
  >
  > Mettez à jour le certificat uniquement si les certificats sont régénérés manuellement ; vous n'avez pas besoin de mettre à jour le certificat si les appliances possèdent déjà les certificats.

- Effectuez une réinitialisation d'usine et lancez Cloud Brokered-ZTD sur les appliances, afin d'établir une connexion avec SD-WAN Orchestrator for On-premises à l'aide de l'adresse IP de l'interface ZTD.

> **Remarque**
>
> Vous pouvez désactiver l'option **Utiliser l'interface de gestion pour les sites existants** une fois que toutes les appliances SD-WAN ont établi une connexion avec SD-WAN Orchestrator for On-premises via l'adresse IP de l'interface ZTD.

Si l'option **Utiliser l'interface de gestion pour les sites existants** n'est pas sélectionnée, les appliances SD-WAN déjà déployées à l'aide de la technologie ZTD négociée dans le cloud perdent la connexion à SD-WAN Orchestrator for On-premises. Pour rétablir la connexion avec SD-WAN Orchestrator for On-premises à l'aide de l'adresse IP de l'interface ZTD, effectuez l'une des opérations suivantes :

- Sur les appliances SD-WAN, mettez à jour l'adresse IP et le certificat du SD-WAN Orchestrator for On-premises.
- Effectuez une réinitialisation d'usine et lancez Cloud Brokered-ZTD sur les appliances, afin d'établir une connexion avec SD-WAN Orchestrator for On-premises à l'aide de l'adresse IP de l'interface ZTD.

Configuration manuelle de la connectivité

Lors de la configuration manuelle de la connectivité, vous devez télécharger le certificat Citrix SD-WAN Orchestrator for On-premises et le charger sur chaque appliance du réseau. Cela implique de se connecter manuellement à chaque appliance pour télécharger les certificats.

Pour configurer la connectivité manuellement :

1. Accédez à **Administration > Authentification par certificat** et activez le **type d'authentification**.

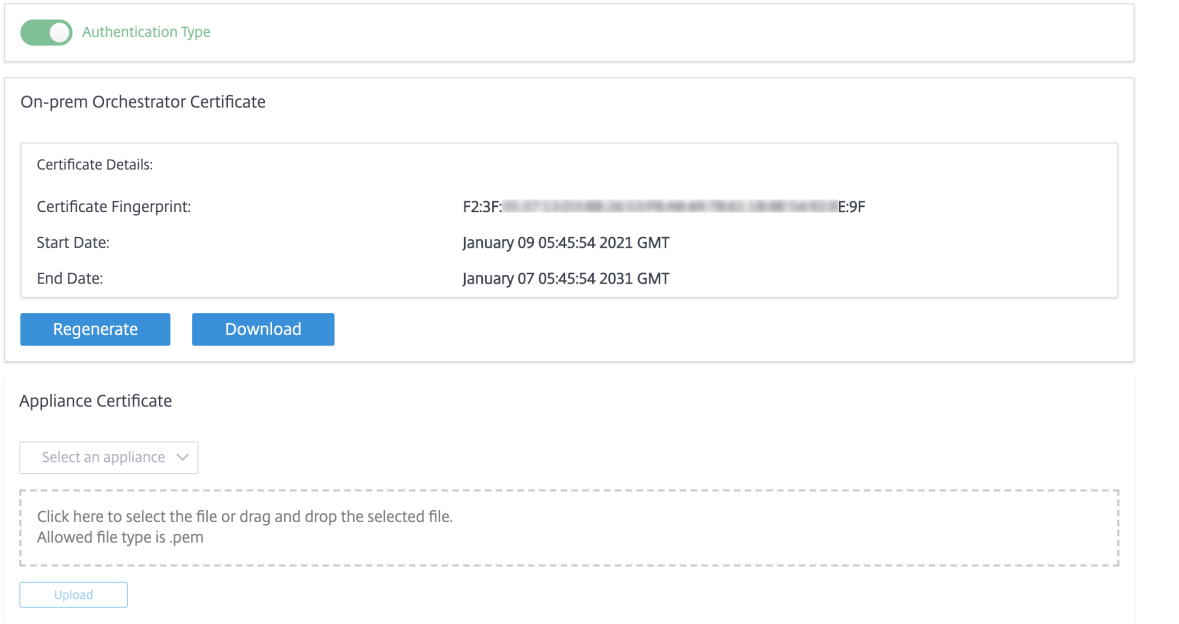
   Lorsque le type d'authentification est activé, l'appliance SD-WAN peut se connecter à Citrix SD-WAN Orchestrator pour les applications locales uniquement via une authentification bidirectionnelle. Lorsque le type d'authentification est désactivé, l'appliance SD-WAN peut se connecter à Citrix SD-WAN Orchestrator pour les applications locales via une authentification sans authentification, une authentification unidirectionnelle ou une authentification bidirectionnelle.

   > **Remarque :**
   >
   > Dans une configuration gérée par un fournisseur, seuls les fournisseurs peuvent activer le type d'authentification et régénérer le certificat Citrix SD-WAN Orchestrator for On-premises.

2. Cliquez sur **Régénérer** et **téléchargez** le certificat Citrix SD-WAN Orchestrator pour site.
3. Choisissez une appliance dans la section **Certificat de l'appliance** et téléchargez le certificat correspondant téléchargé depuis l'appliance SD-WAN. Pour des informations détaillées sur le téléchargement du certificat de l'appliance, consultez la section Configuration locale de Citrix SD-WAN Orchestrator sur l'appliance SD-WAN.

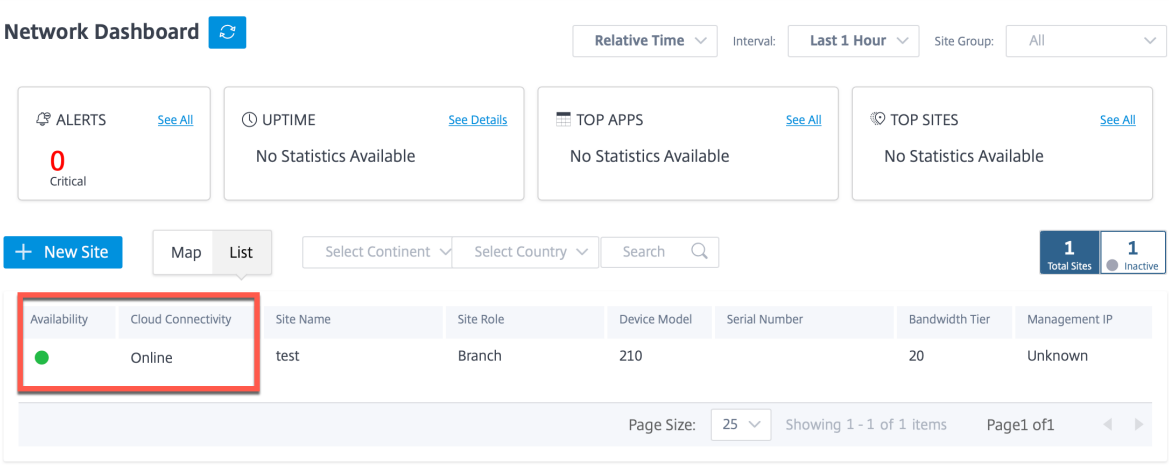
   > **REMARQUE**
   >
   > - Seul le type de fichier .pem est pris en charge.
   > - Seuls les administrateurs du client peuvent télécharger le certificat de l'appliance.

4. Connectez-vous à l'interface utilisateur de l'appliance SD-WAN, accédez à **Configuration > Réseau étendu virtuel > SD-WAN Orchestrator**sur site. Téléchargez le certificat téléchargé depuis Citrix SD-WAN Orchestrator pour les applications locales. Pour des informations détaillées, consultez Citrix SD-WAN Orchestrator pour la configuration sur site sur une appliance SD-WAN.



Vérifier la connectivité

Pour vérifier l'état de connectivité de l'appliance, accédez à **Configuration > Page d'accueil de la configuration réseau**et vérifiez la colonne **Cloud Connectivity** correspondant à votre site.

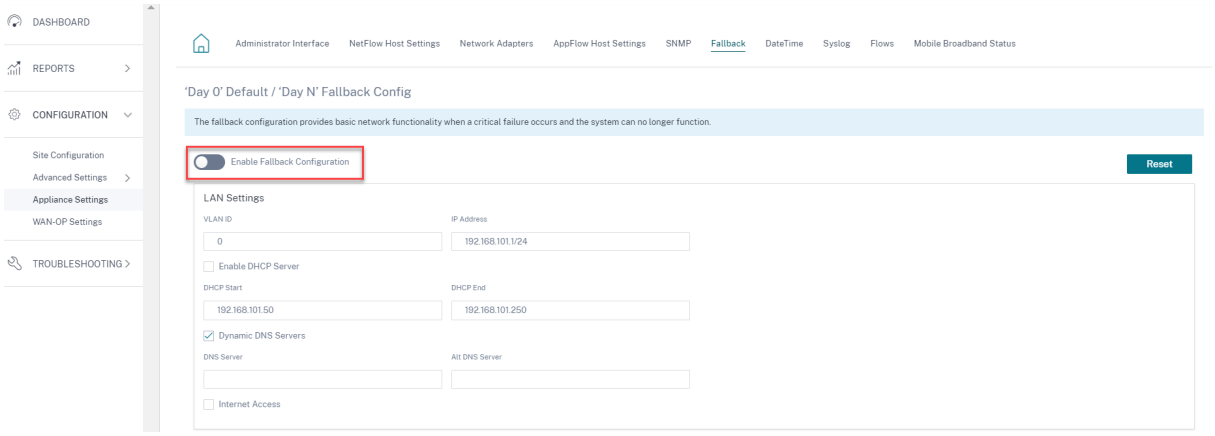


> **Remarque**
>
> Vous pouvez publier le logiciel souhaité pour mettre à niveau les dispositifs sous **Infrastructure > Administration de l'orchestrateur > Images logicielles > Appliance**. Pour plus d'informations, voir Publier un logiciel.

Configuration de secours

La configuration de secours garantit que le Citrix SD-WAN Orchestrator pour la connectivité sur site que vous avez établi avec l'appliance Citrix SD-WAN est conservé via l'adresse IP de gestion intra-bande de l'appliance.

Vous pouvez activer la configuration de secours sur Citrix SD-WAN Orchestrator for On-premises au niveau du site en accédant à **Configuration** > **Paramètres de l'appliance** > **Fallback** et en cliquant sur **Activer la configuration de secours**.

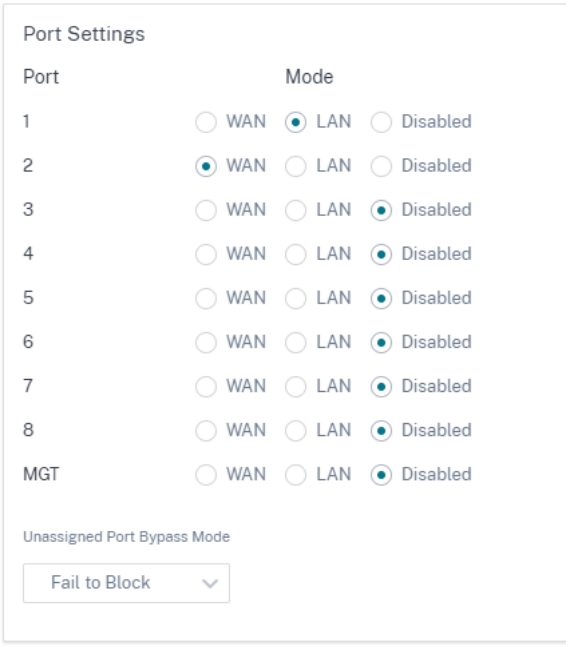


Pour des informations détaillées sur la configuration de secours, consultez la section Gestion intra-bande.

> **Remarque**
>
> Si vous utilisez une appliance autre que Citrix SD-WAN 110 SE, assurez-vous d'exécuter SD-WAN 11.2 ou une version ultérieure pour activer la configuration de secours par défaut.

Le tableau suivant fournit les détails des ports WAN et LAN prédésignés pour la configuration de secours sur différentes plates-formes :

Plateforme	Ports WAN	Ports LAN
110	1/2	1/1
110-LTE	1/2, LTE-1	1/1
210	1/4, 1/5	1/3
210-LTE	1/4, 1/5, LTE-1	1/3
VPX	2	1
410	1/4, 1/5, 1/6	1/3 (FTB)
1100	1/4, 1/5, 1/6	1/3 (FTB)



Configuration au niveau du fournisseur

November 12, 2020

Profils

Un profil est un **modèle de configuration en direct**. Un modèle régulier est destiné à faciliter la création d'une nouvelle entité. Mais une fois le modèle créé, les modifications ultérieures du modèle ne s'appliquent pas aux nouvelles entités créées à l'aide du modèle de base. Un profil sert d'entité principale centrale en direct, dont toutes les entités enfants héritent, non seulement lors de la création mais aussi tout au long de la vie d'un profil. Toutes les entités enfants associées au profil héritent automatiquement des modifications apportées à un profil.

Par exemple, Un administrateur crée un profil de configuration de site appelé **le petit magasin de détail** et l'applique à tous les petits magasins de détail appartenant à une entreprise. Maintenant, toute modification apportée au profil des petits magasins de détail à un moment donné serait appliquée automatiquement à tous les magasins héritant de ce profil. En fonction de ce qui est commun à toutes les entités et de ce qui ne l'est pas, certains paramètres de la configuration du profil peuvent être laissés indéfinis. Ces paramètres seraient personnalisables et peuvent varier selon les entités héritant du même profil.

Modèles de profil pour les fournisseurs de services

Les partenaires peuvent créer des modèles de profil que leurs clients peuvent utiliser lors de la création de profils.

Par exemple, un fournisseur peut créer quatre modèles de profil de site : Small Branch, Medium Branch, Grande succursale et Data Center. Ces modèles sont automatiquement mis à la disposition des comptes clients associés au partenaire. Les clients peuvent utiliser ces modèles lors de la création de profils.

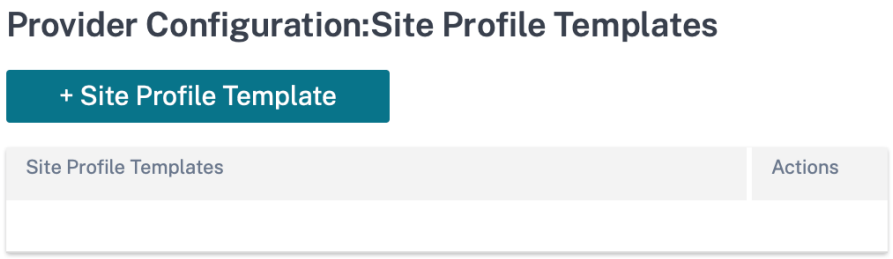
Par exemple, disons qu'un client décide de créer un profil pour la configuration de petites succursales. Le client peut sélectionner l'un des modèles partagés par le partenaire, mis à disposition via une liste déroulante dans le cadre de la configuration du profil. Le client peut le personnaliser en fonction de ses besoins réseau avant d'enregistrer le profil. Le modèle de profil n'est pas une entité dynamique. Il facilite simplement la création de profils au niveau du client. Les profils ne peuvent être créés qu'au niveau client et sont conçus pour être des entités actives servant d'enregistrements de configuration maître.

Le fournisseur peut créer des profils de configuration, qui peuvent être partagés avec certains ou tous les clients, selon les besoins. Les profils de site et WAN sont actuellement pris en charge.

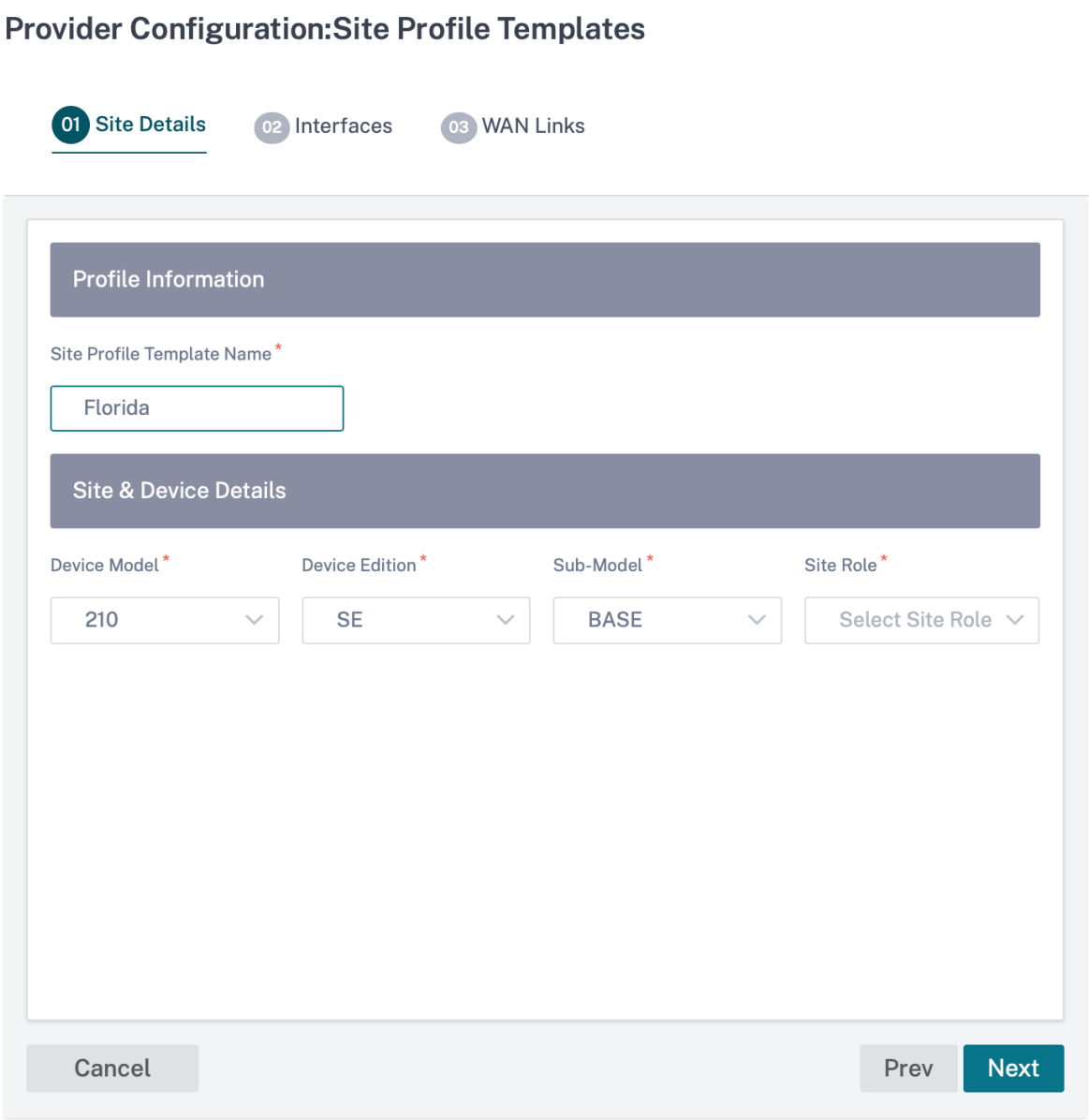
Modèles de profil de site

Les modèles de profil de site sont des modèles de configuration de site créés par des fournisseurs de services pour permettre la création de profils de site au niveau client.

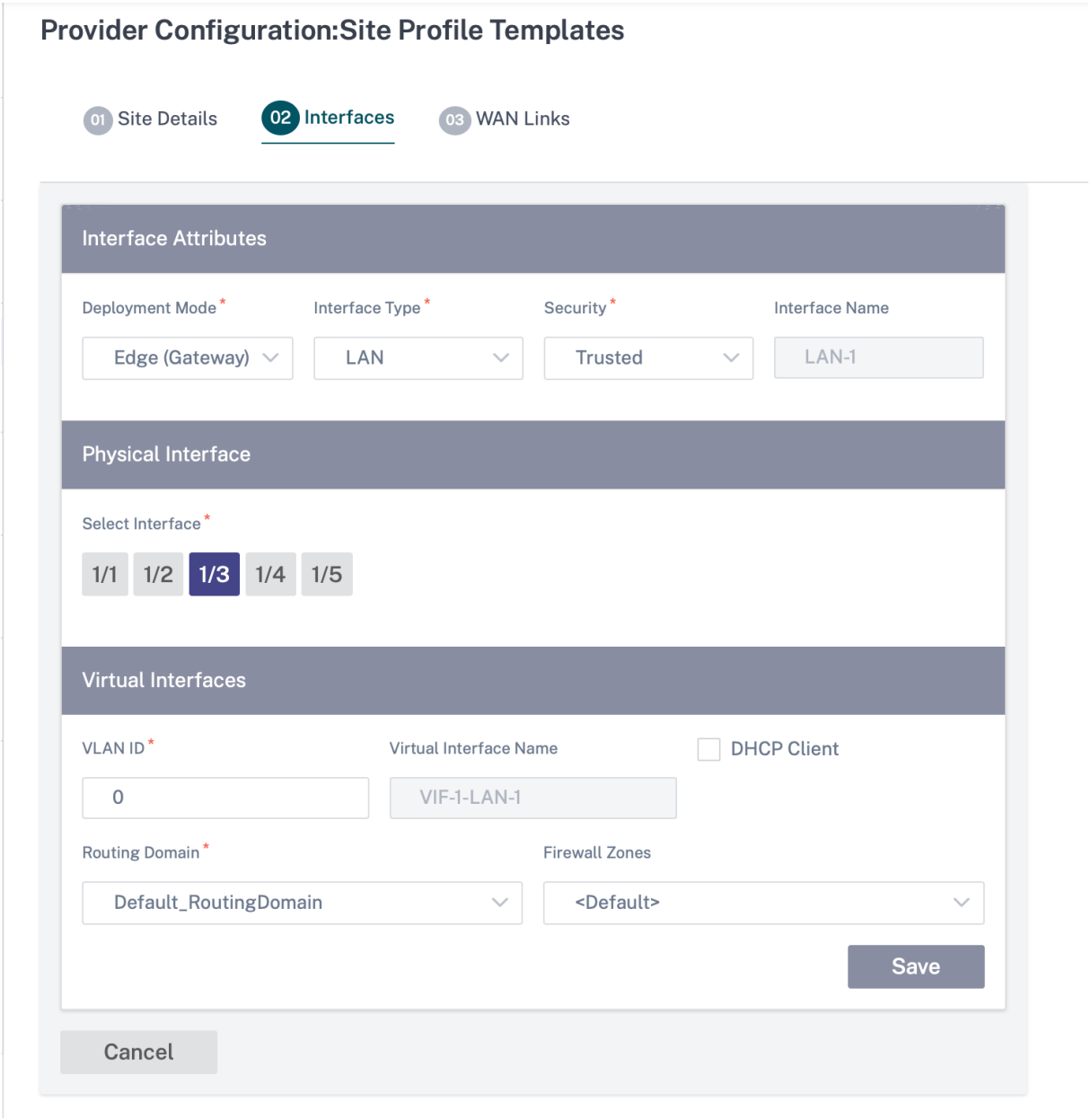
Pour créer des modèles de profil, accédez à **Configuration** > **Modèles de profil de site** et cliquez sur **+ Modèle de profil de site**.



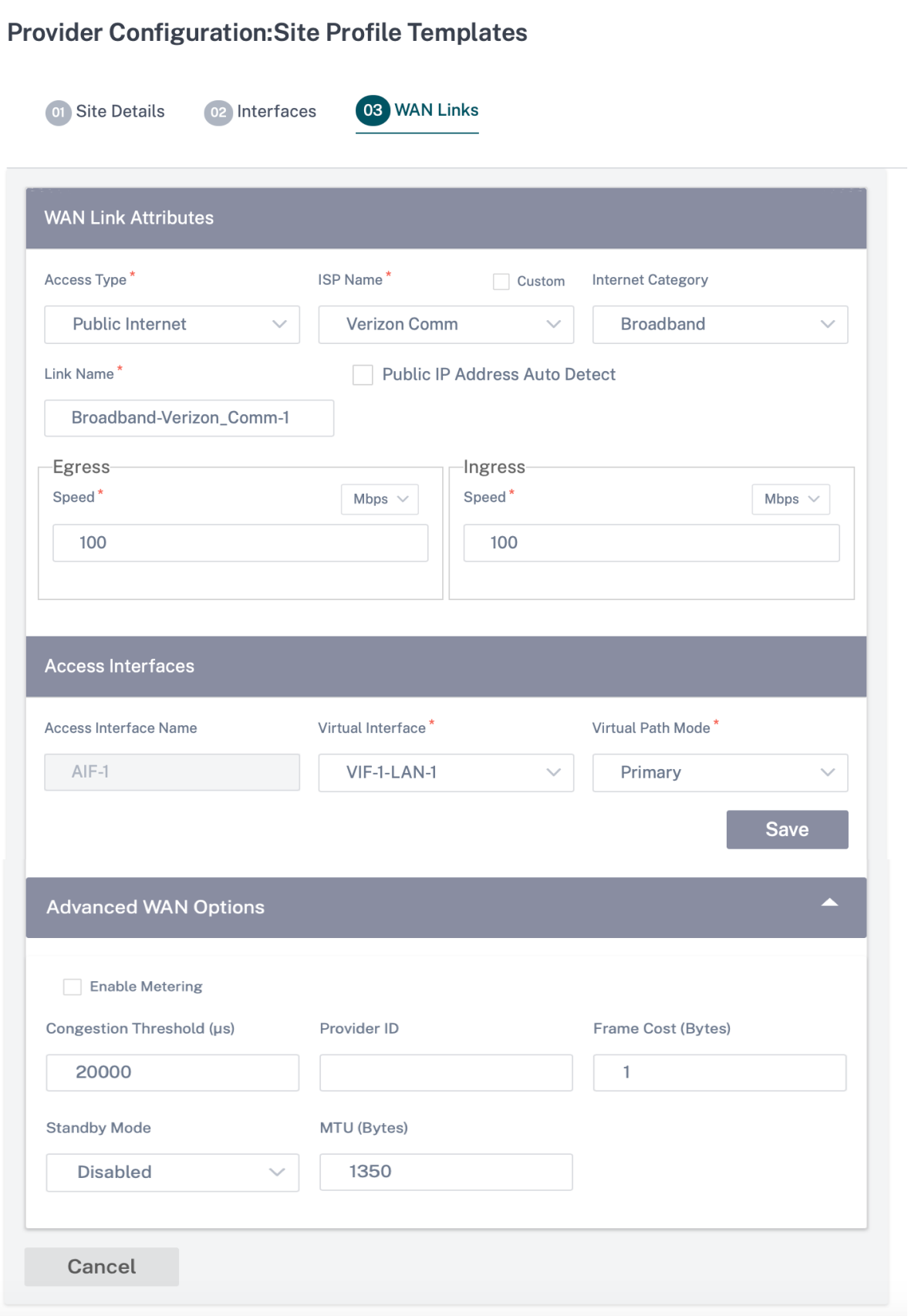
Pour créer un modèle de profil de site, vous devez configurer les **détails du site**, les **interfaces** et les **liens WAN**. Pour une description détaillée de la configuration des sites, voir Détails du site.



Affectez une interface pour le site en cliquant sur l'option **+ Interface**. Pour ajouter une interface, vous devez remplir les champs **Attributs d'interface**, **Interface physique** et **Interfaces virtuelles**. Pour une description détaillée de la configuration des interfaces, reportez-vous à la section Interfaces.

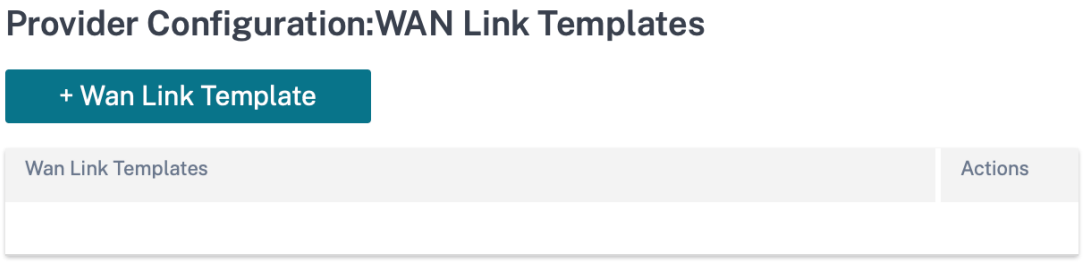


Fournissez des **attributs de liaison WAN**, des **interfaces d'accès** et des **services** avec des **options avancées**. Pour une description détaillée de la configuration des liaisons WAN, voir Liens WAN.



Modèles de liaison WAN

Les modèles de profil WAN sont des modèles de configuration de liaison WAN créés par les fournisseurs de services, pour permettre la création de profils de liaison WAN au niveau du client.



Pour créer un modèle de lien WAN, cliquez sur **+ Modèle de lien WAN**. Vous devez remplir les informations de lien WAN telles que le **nom du profil**, le **type d'accès**, la **catégorie Internet**, le **taux LAN à WAN** et ainsi de suite. Pour une description détaillée de la configuration des liaisons WAN, voir Liens WAN.

Réseau d'accueil

October 21, 2022

La page d'**accueil du réseau** sert de point d'ancrage pour la configuration du réseau, offre des fonctionnalités de configuration au niveau du réseau d'entreprise et sert de point de départ pour configurer le réseau SD-WAN d'une entreprise.

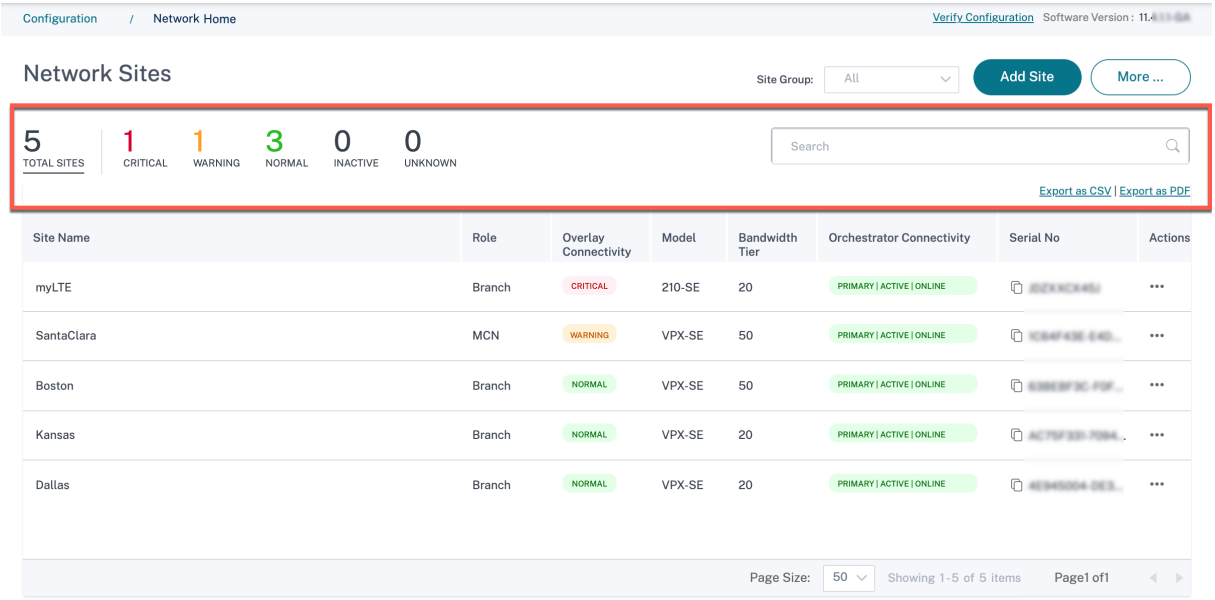
La page d'**accueil du réseau** affiche le nombre total de sites du réseau et sépare les sites en fonction de leur état de connectivité. Sélectionnez les liens numérotés pour afficher les sites en fonction des catégories de statut suivantes :

- **Critique** : sites dont tous les chemins virtuels associés sont inactifs.
- **Avertissement** : sites qui possèdent au moins un chemin virtuel vers le bas.
- **Normal** : tous les chemins virtuels et les chemins des membres associés du site sont actifs.
- **Inactif** : les sites sont à l'état non déployé et inactif.
- **Inconnu** - L'état du site est inconnu.

Le fait de cliquer sur le statut permet de filtrer les sites en fonction de leur statut et d'afficher les détails. Vous pouvez également utiliser la barre **de recherche** pour afficher les détails d'un site en fonction

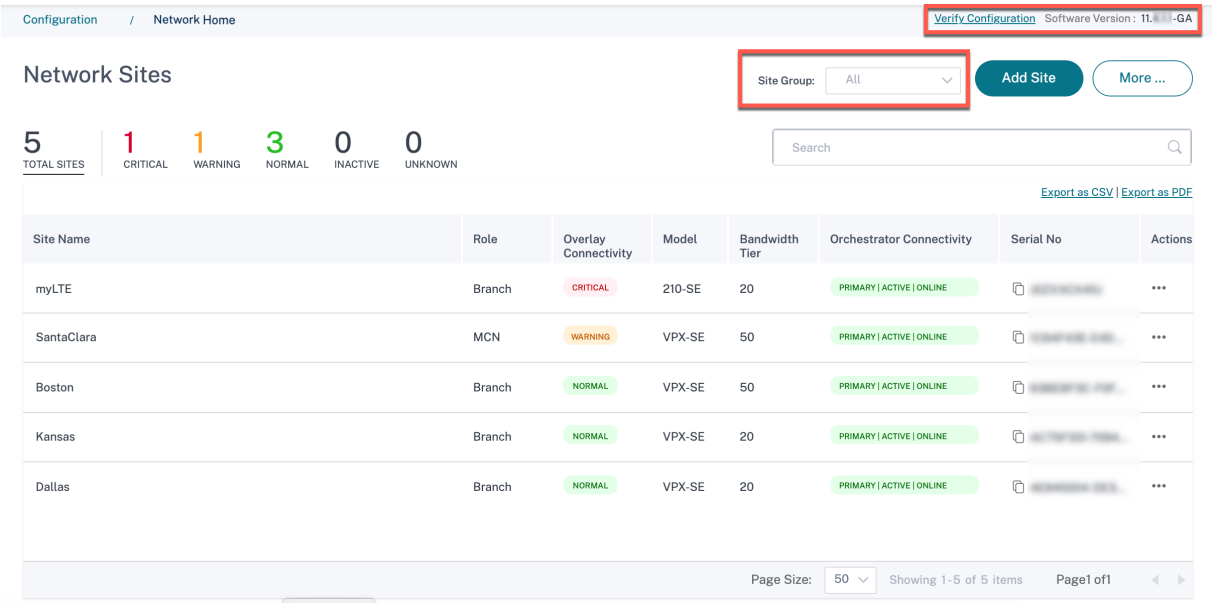
du nom du site, du rôle, de la connectivité de superposition, du modèle, du niveau de bande passante et des paramètres du numéro de série.

Vous pouvez exporter les résultats filtrés vers un fichier CSV ou PDF à l'aide des options **Exporter au format CSV** et **Exporter au format PDF** . Le nom du fichier CSV et PDF est préfixé par **SiteList** suivi de la date et de l'heure d'exportation du fichier.



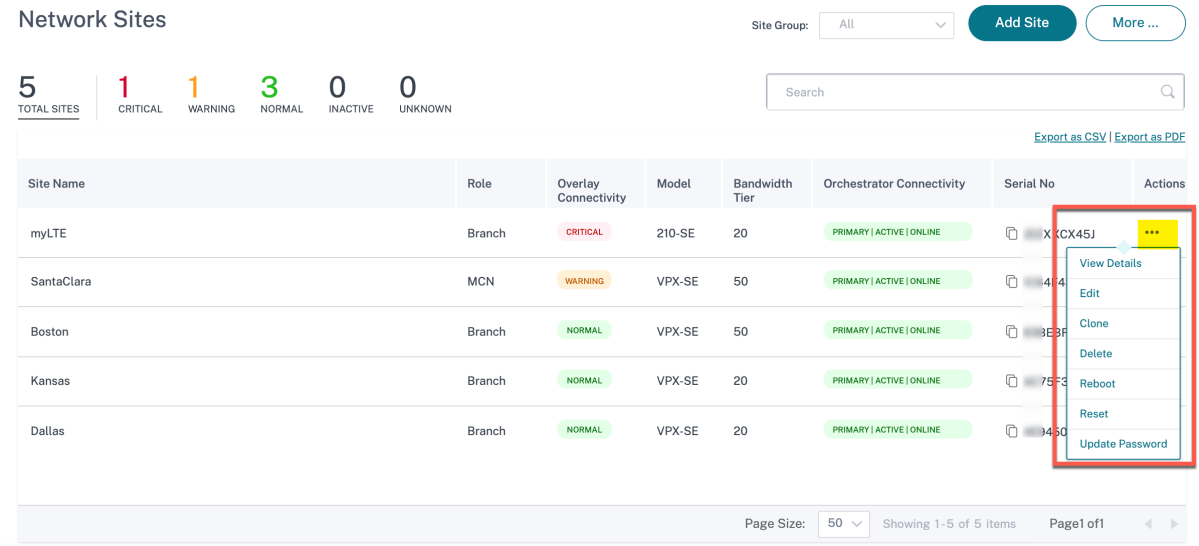
Dans le coin supérieur droit de l'écran, vous pouvez voir la version actuelle du logiciel. Cliquez sur **Vérifier la configuration** pour valider toute erreur d'audit. Pour plus de détails, voir Vérifier la configuration.

Vous pouvez filtrer les sites en fonction du groupe/de la région auquel ils appartiennent à l'aide de la liste déroulante **Groupe de sites** .

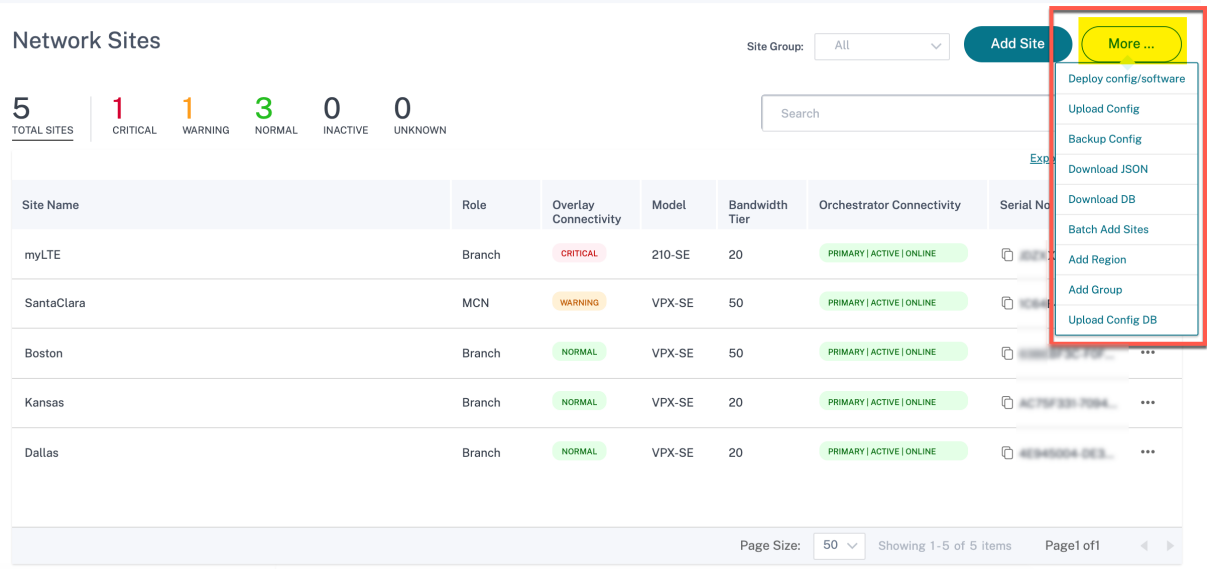


Cliquez sur le nom du site dans le résultat filtré pour accéder à l'écran **de configuration du site** . Si le site est configuré en haute disponibilité, la colonne **Orchestrator Connectivity** affiche l'état des appliances principales et secondaires. La colonne **Numéro de série** affiche le numéro de série de l'appliance. Dans une configuration à haute disponibilité, les numéros de série des appareils principaux et secondaires sont affichés. Vous pouvez copier le numéro de série de l'appliance à l'aide de l'icône de copie.

À l'aide de la colonne **Actions**, vous pouvez afficher les détails, modifier, cloner, supprimer, réinitialiser et mettre à jour le mot de passe du site. Vous pouvez également redémarrer les périphériques associés à un site.



Vous pouvez effectuer d'autres actions telles que la configuration du téléchargement, l'ajout de sites par lots, le téléchargement de fichiers JSON, etc. à l'aide de l'option **Plus...**



Ajouter un site

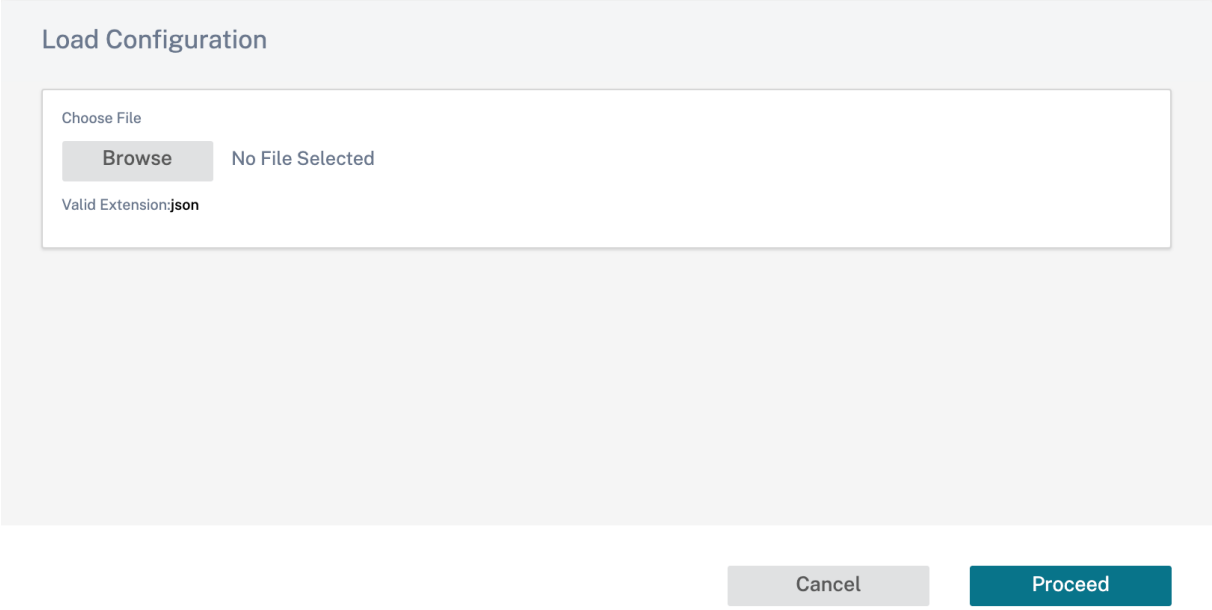
Utilisez l'option **+ Ajouter un site** pour ajouter un nouveau site. Pour plus d'informations sur le flux de travail de configuration du site, voir Configuration du site.

Déploiement de la configuration

L'option **Plus > Déployer la configuration/le logiciel** vous amène à la section **Déploiement** qui permet de vérifier, d'organiser et d'activer la configuration sur le réseau. Pour plus d'informations sur le déploiement de la configuration et du logiciel, voir Déploiement

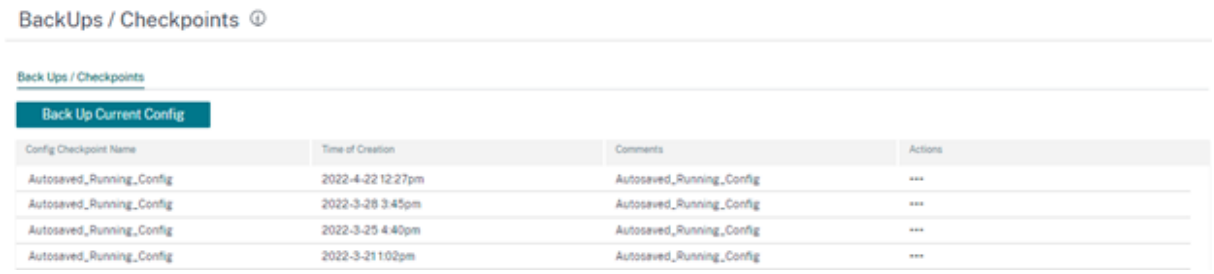
Configuration du téléchargement

L'option **Plus > Télécharger la configuration** vous permet de parcourir et de télécharger l'une des configurations précédemment enregistrées. La configuration récemment téléchargée sert de configuration active pour le réseau.



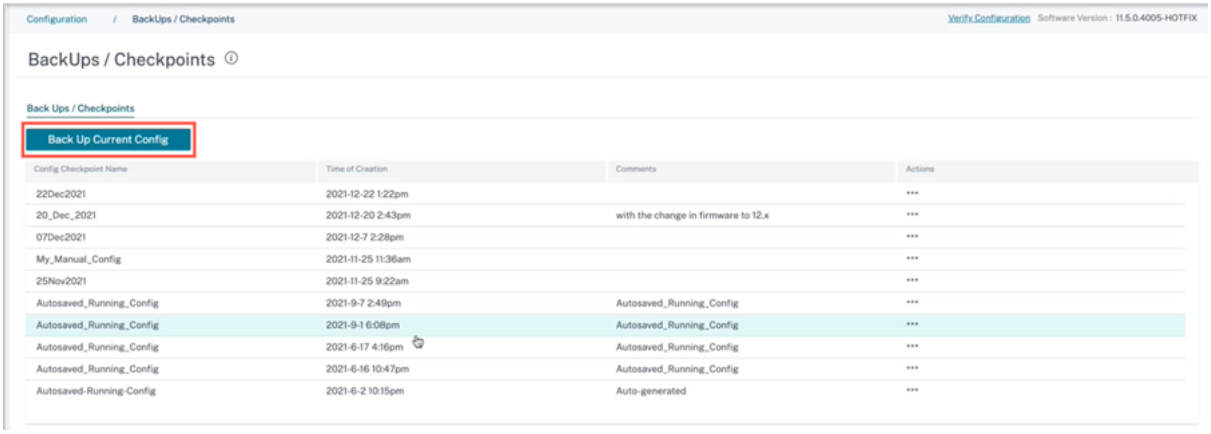
Sauvegardes/Points de contrôle

L'option **Plus > Configuration de sauvegarde** vous amène à la page **Sauvegardes/Points de contrôle** et permet de sauvegarder et de restaurer la configuration, ou de consulter les points de contrôle enregistrés.

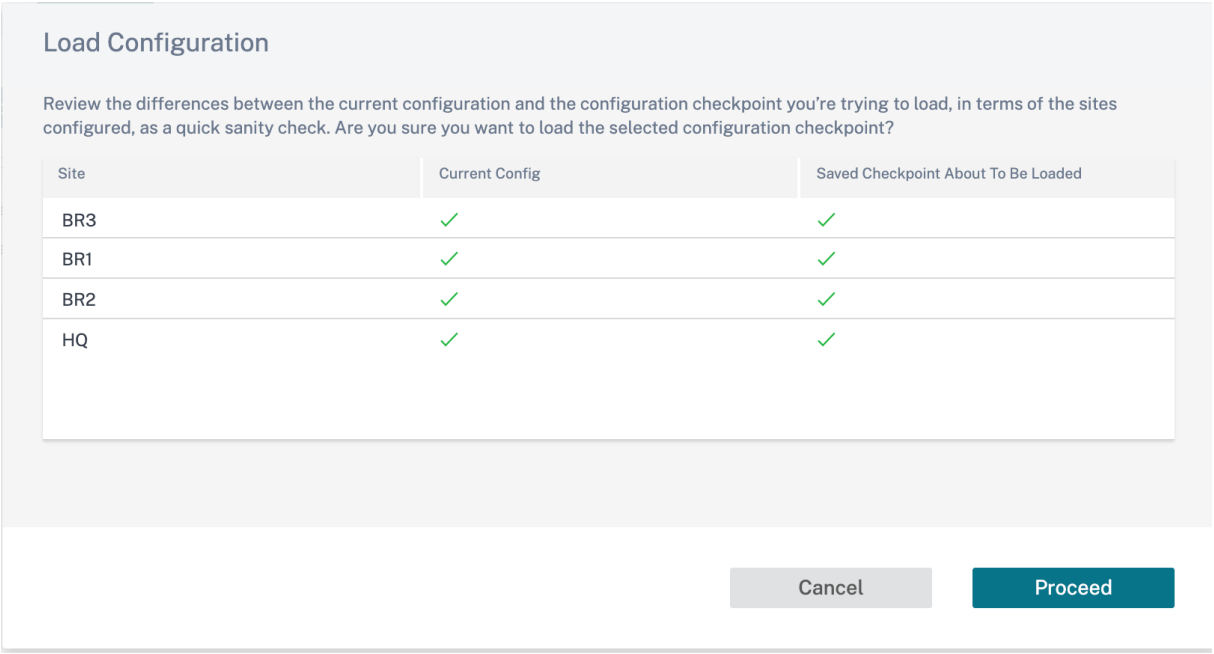


Cliquez sur **Vérifier la configuration** pour valider toute erreur d'audit.

Cliquez sur **Sauvegarder la configuration actuelle** pour sauvegarder la configuration actuelle en tant que point de contrôle pour une utilisation future.



Cliquez sur **Charger la configuration** (sous **Actions**) pour charger une configuration enregistrée. Cliquez sur **Continuer**.



Cliquez sur **Copier** (sous **Actions**) pour créer une copie similaire d'une configuration existante. Vous

pouvez également télécharger, modifier et supprimer les points de contrôle de configuration enregistrés. Ces opérations sont disponibles sous **Actions**.

Télécharger JSON

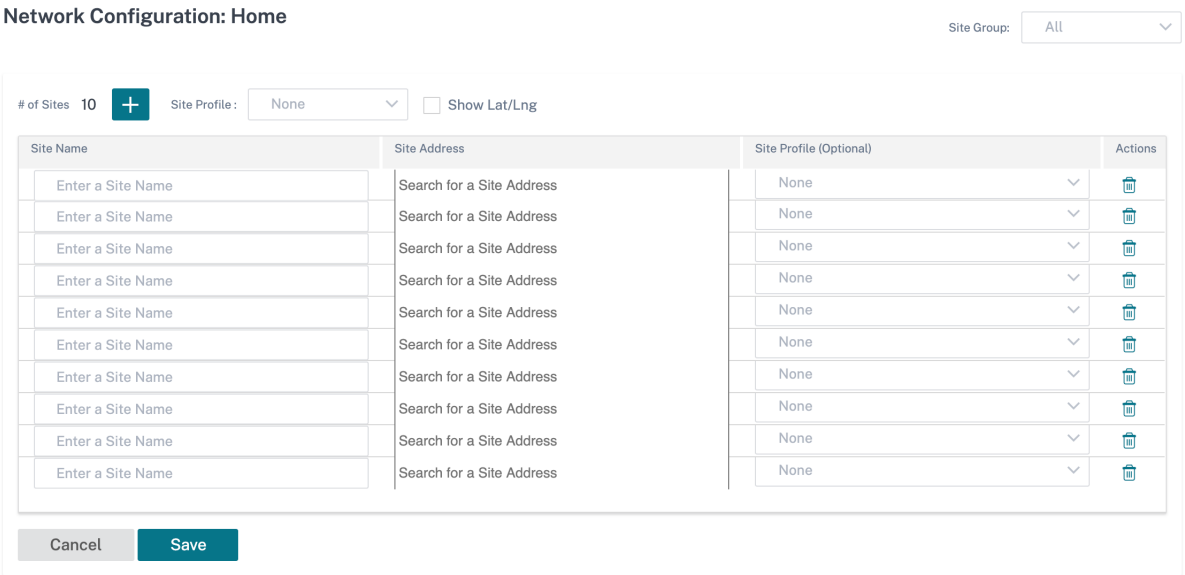
L'option **Plus > Télécharger JSON** vous permet de télécharger et d'exporter la configuration actuelle au format JSON, pour une révision hors ligne.

Télécharger DB

L'option **Plus > Télécharger la base** de données vous permet de télécharger et d'exporter la configuration actuelle au format de base de données.

Ajouter des sites par lots

L'option **Plus > Ajouter des sites par lots** vous permet d'ajouter rapidement plusieurs sites par lot. Vous pouvez également sélectionner un profil de site à utiliser pour chaque site, en vous laissant uniquement avec des paramètres uniques tels que les adresses IP qui restent à configurer pour chaque site.



Ajouter une région

L'option **Plus > Ajouter une région** vous permet de créer une région et vous amène à la page **Sites et groupes IP > Régions** . Pour plus d'informations, voir Régions.

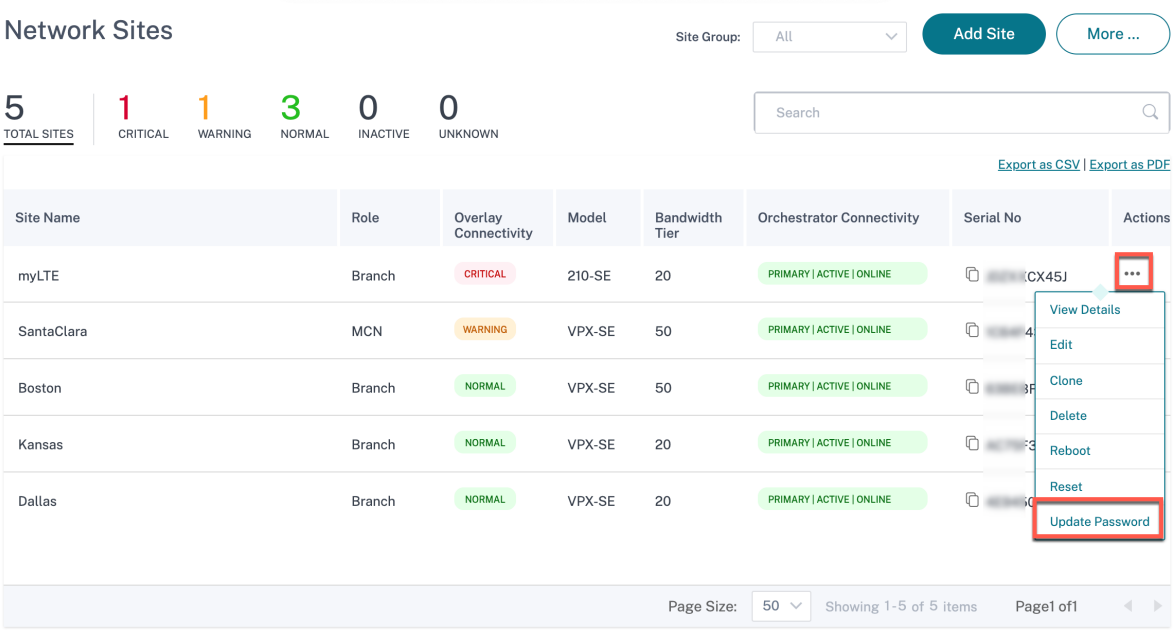
Ajouter un groupe

L'option **Plus > Ajouter un groupe** vous amène à la page **Sites et groupes IP > Groupes personnalisés** où vous pouvez créer une région. Pour plus d'informations, consultez la section Groupes personnalisés.

Mot de passe

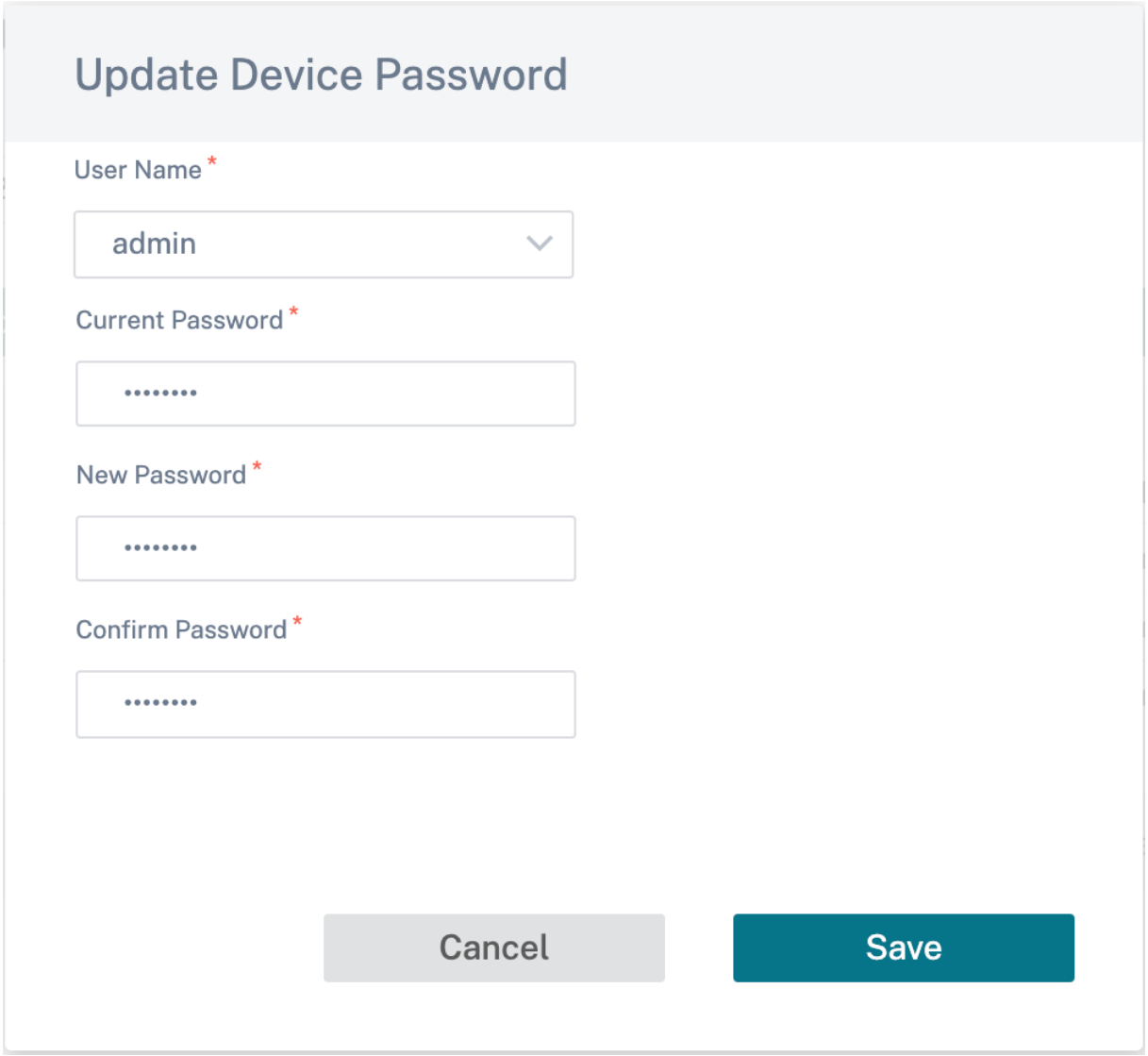
Vous pouvez modifier le mot de passe des appliances SD-WAN sur différents sites, sur le réseau, via Citrix SD-WAN Orchestrator for On-premises.

Pour modifier le mot de passe, pour un appareil en ligne, cliquez sur l'icône Plus et sélectionnez **Mettre à jour le mot de passe**.



Fournissez les valeurs pour les champs suivants :

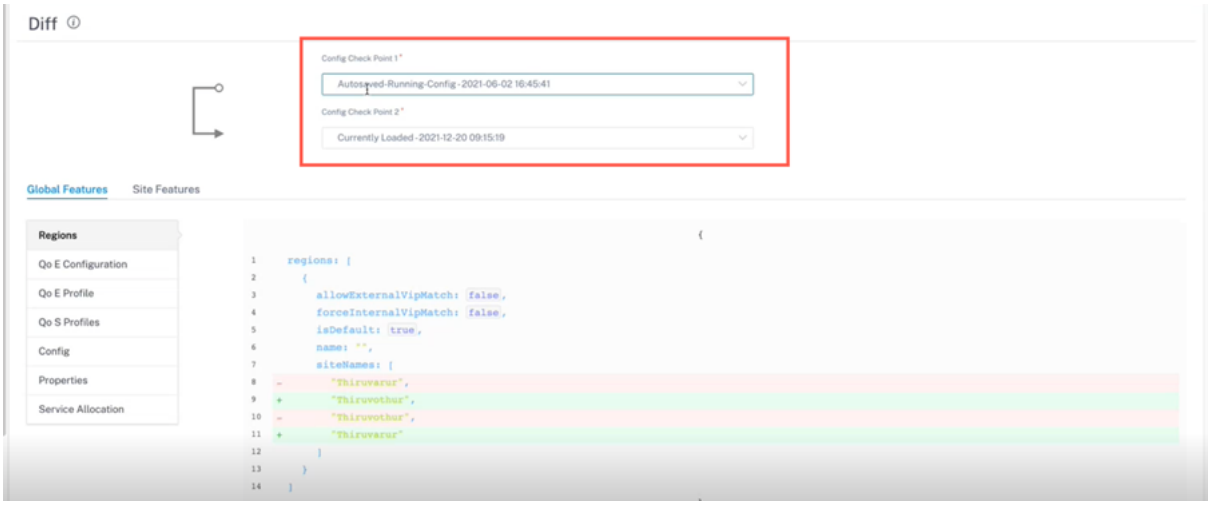
- **Nom d'utilisateur** : sélectionnez un nom d'utilisateur pour lequel vous souhaitez modifier le mot de passe dans la liste des utilisateurs configurés sur le site.
- **Mot de passe actuel** : Entrez le mot de passe actuel. Ce champ est facultatif pour les utilisateurs administrateurs.
- **Nouveau mot de passe** : Entrez le nouveau mot de passe de votre choix.
- **Confirmer le mot de passe** : Entrez à nouveau le mot de passe pour confirmation



La différence de configuration

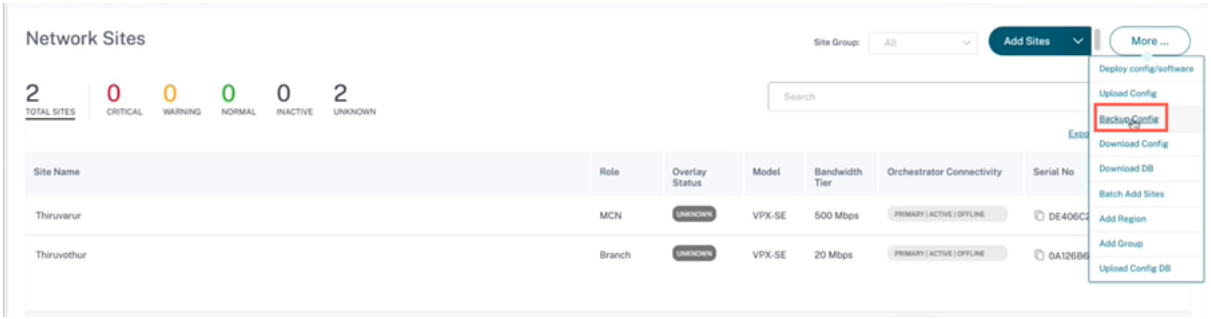
October 21, 2022

La fonctionnalité **Config Diff** vous permet de vérifier la différence entre deux versions de points de contrôle de configuration. L'option **Config Diff** est disponible au niveau du réseau, sous **Configuration** > **Config Diff**.

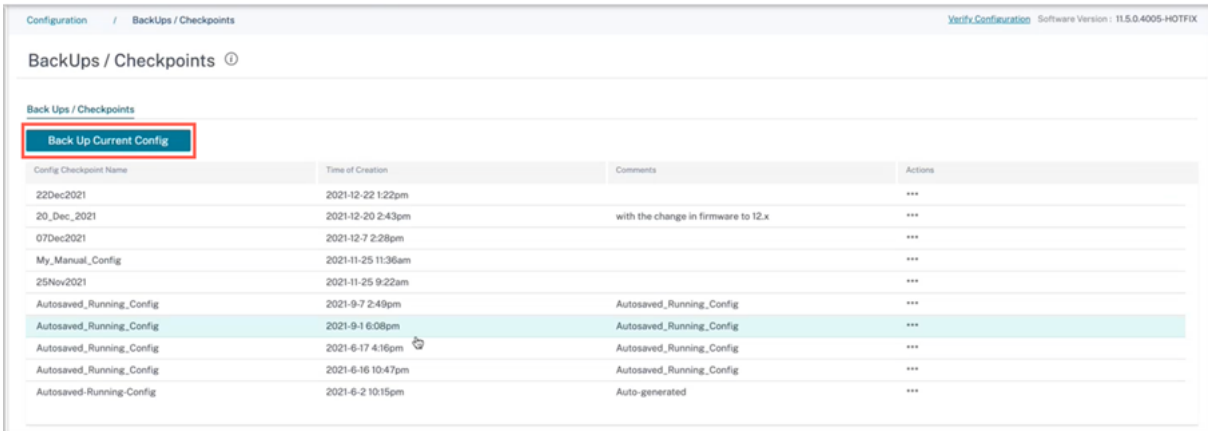


Pendant le déploiement, vous pouvez enregistrer une configuration sous un nom approprié. Les configurations enregistrées sont appelées points de contrôle. Lorsque vous comparez la différence entre les deux configurations, vous devez sélectionner les configurations requises dans les listes déroulantes **Config Check Point 1/2** .

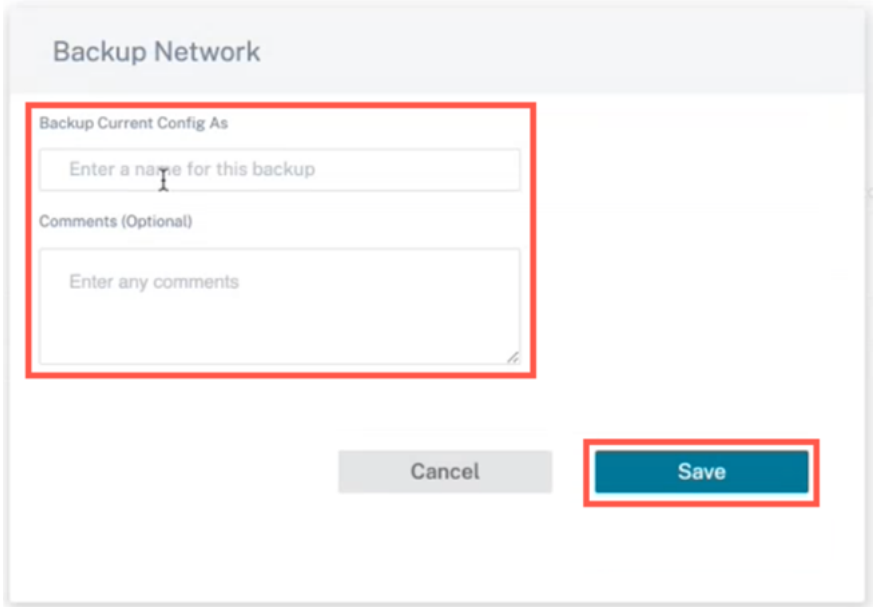
Vous pouvez consulter la liste des sauvegardes et des points de contrôle des configurations enregistrées sous **Configuration** > **Accueil du réseau** > sélectionnez **Sauvegarder la configuration** dans la liste déroulante **Plus** .



Lors d'un déploiement, la configuration est sauvegardée automatiquement à chaque fois. Vous pouvez également sauvegarder la configuration actuelle manuellement. Pour ce faire, cliquez sur l'option **Sauvegarder la configuration actuelle** .



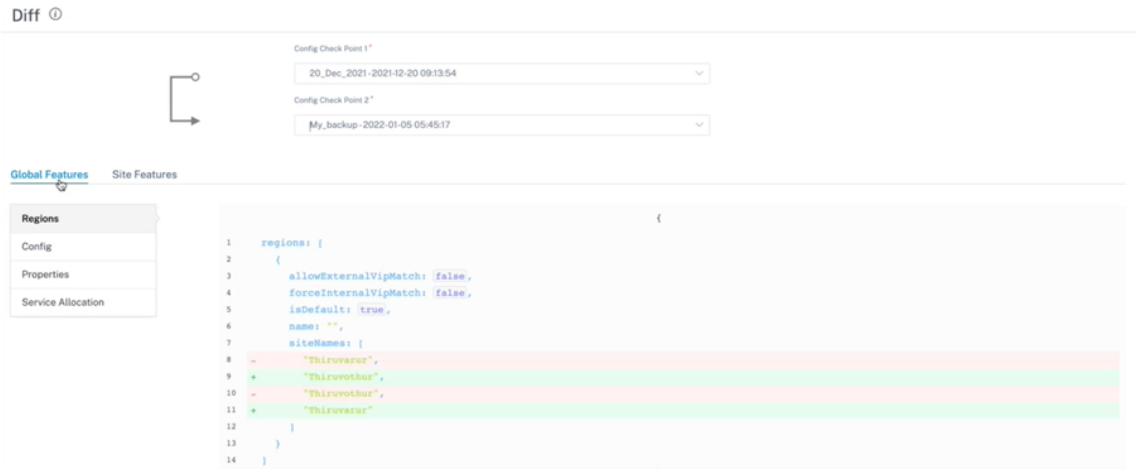
Fournissez un nom pour enregistrer votre configuration ainsi que des commentaires (facultatif). Cliquez sur **Enregistrer**.



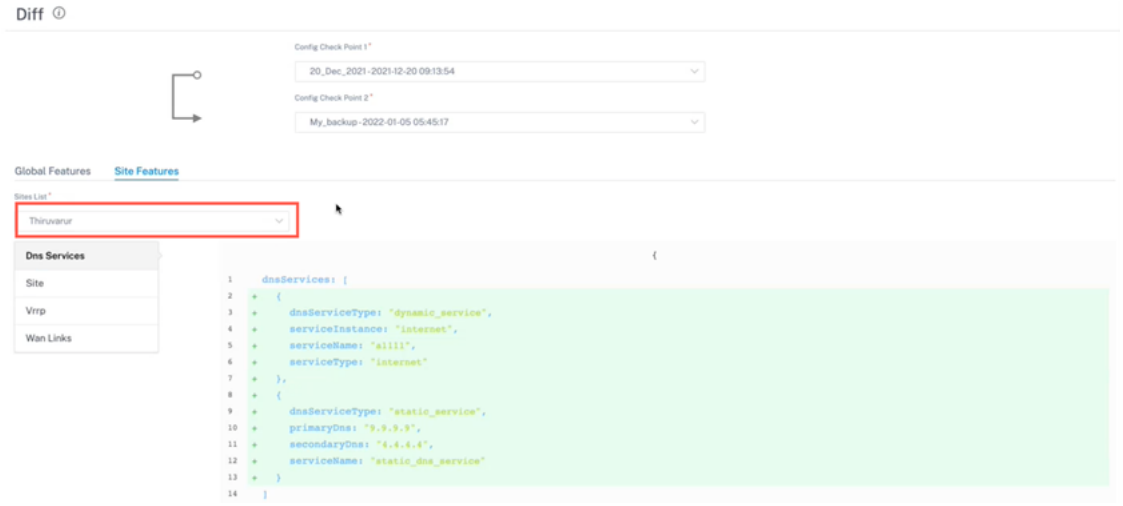
> **Remarque**
>
> Vous pouvez enregistrer/créer un maximum de cinq sauvegardes de configuration. La création d'une nouvelle sauvegarde supprime automatiquement la configuration de sauvegarde la plus ancienne.

Deux types de configurations sont disponibles :

- **Niveau global** : Dans la catégorie globale, vous pouvez consulter la liste des fonctionnalités globales mises à jour, telles que les régions, les propriétés et la configuration.



- **Niveau du site** : dans la catégorie du site, vous pouvez sélectionner le site dans la liste déroulante et afficher les détails modifiés tels que le site, les liens WAN et les services DNS.



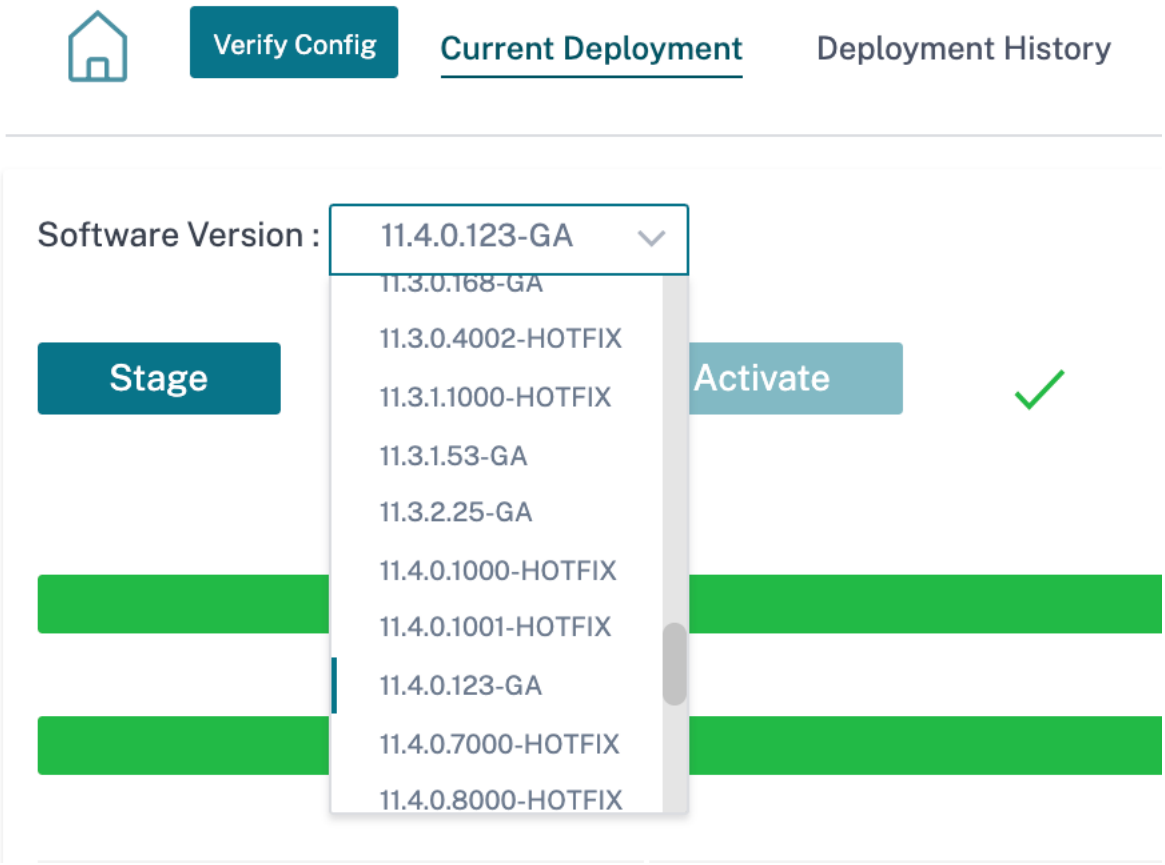
Une valeur supprimée apparaît sur fond rouge avec le symbole moins et la valeur actualisée/ajoutée apparaît sur fond vert avec le symbole plus.

Déploiement

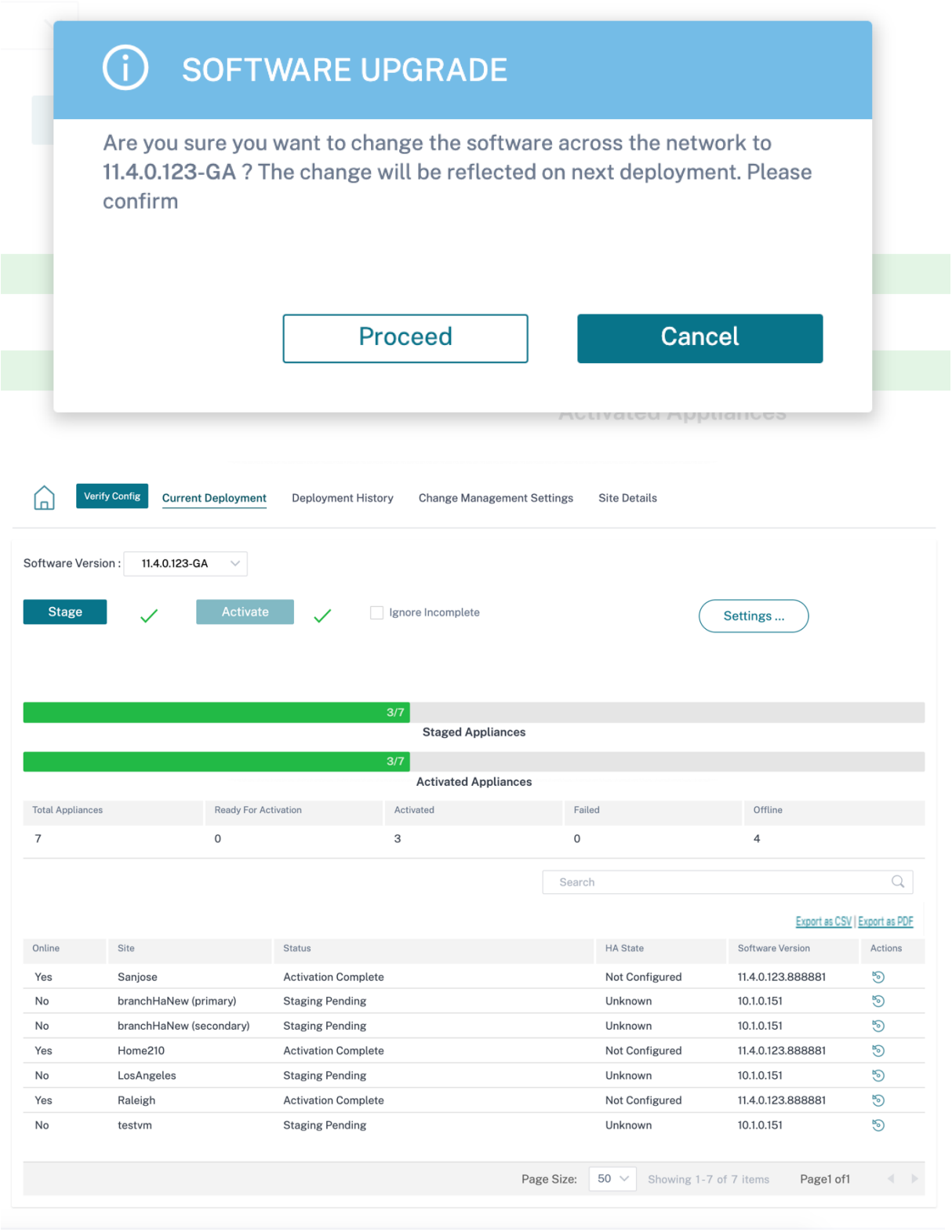
October 21, 2022

Une fois les sites configurés, la page **Déploiement** vous permet de modifier la version du logiciel, de mettre en place et de déployer la configuration sur le réseau.

Vous pouvez mettre à niveau le logiciel SD-WAN sur toutes les appliances du réseau, en sélectionnant la version du logiciel de l'appliance dans le champ **Version du logiciel** .



Un message de confirmation s'affiche. Cliquez sur **Continuer**.



Annulation en cas d'erreur

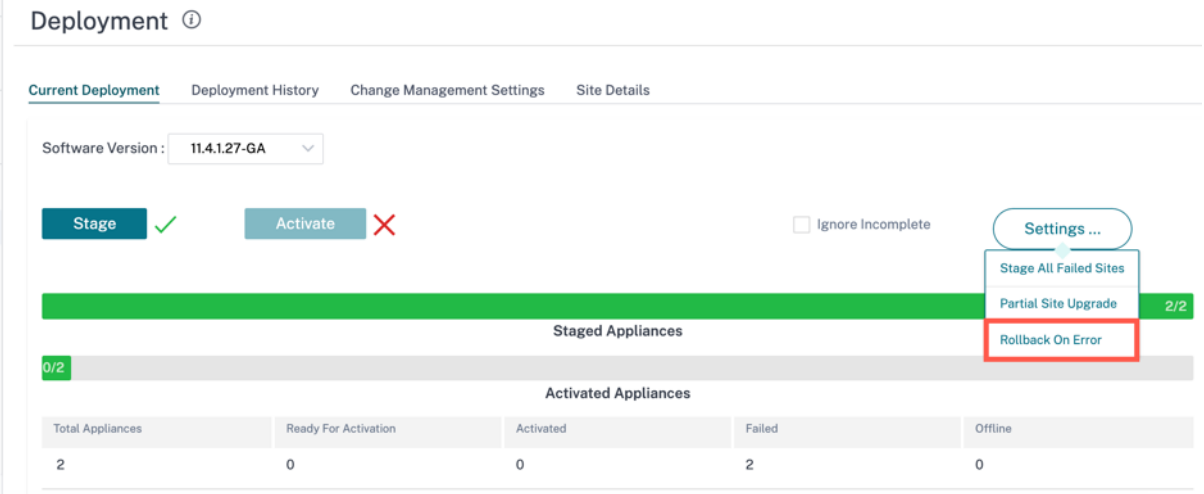
Lorsque la fonctionnalité **Rollback on Error** est activée, les sites qui ne parviennent pas à se connecter au service Citrix SD-WAN Orchestrator après avoir effectué une activation du réseau (dans le cadre du déploiement) déclenchent un retour automatique à la version précédente (package de dernière étape) pour tenter de restaurer la connectivité.

> **Remarque**
> La restauration automatique concerne uniquement le site qui n'a pas réussi à se connecter au service Citrix SD-WAN Orchestrator et non l'ensemble du réseau.

La restauration ne se déclenche que si l'appliance perd la connectivité du service Citrix SD-WAN Orchestrator, et non dans d'autres scénarios tels que la baisse de l'état du chemin virtuel, etc.

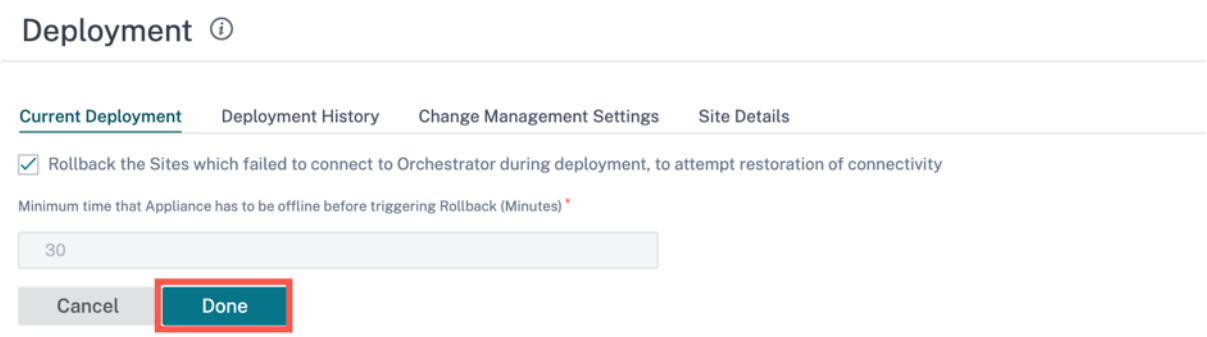
Si au moins un site du réseau initie une restauration, un message d'avertissement affiche la liste des sites qui tentent de revenir en arrière et une option permettant de lancer une restauration à l'échelle du réseau pour tous les sites en ligne. Vous pouvez vérifier la progression de ces sites et choisir l'action appropriée.

Pour activer la fonctionnalité de restauration en cas d'erreur, accédez à **Configuration > Déploiement > Paramètres > Annulation en cas d'erreur**.



Vous pouvez cocher la case **Restaurer en cas d'erreur** pour activer la restauration automatique des sites qui n'ont pas réussi à se connecter au service Citrix SD-WAN Orchestrator après l'activation. La fonctionnalité **Rollback on Error** doit être activée avant de commencer le déploiement pour activer sa fonctionnalité.

Pour qu'un site déclenche une restauration automatique, il doit rester hors ligne pendant au moins 30 minutes (actuellement non modifiable) après l'activation. Si le site peut se connecter au service Citrix SD-WAN Orchestrator dans les 30 minutes, la restauration n'est pas déclenchée.

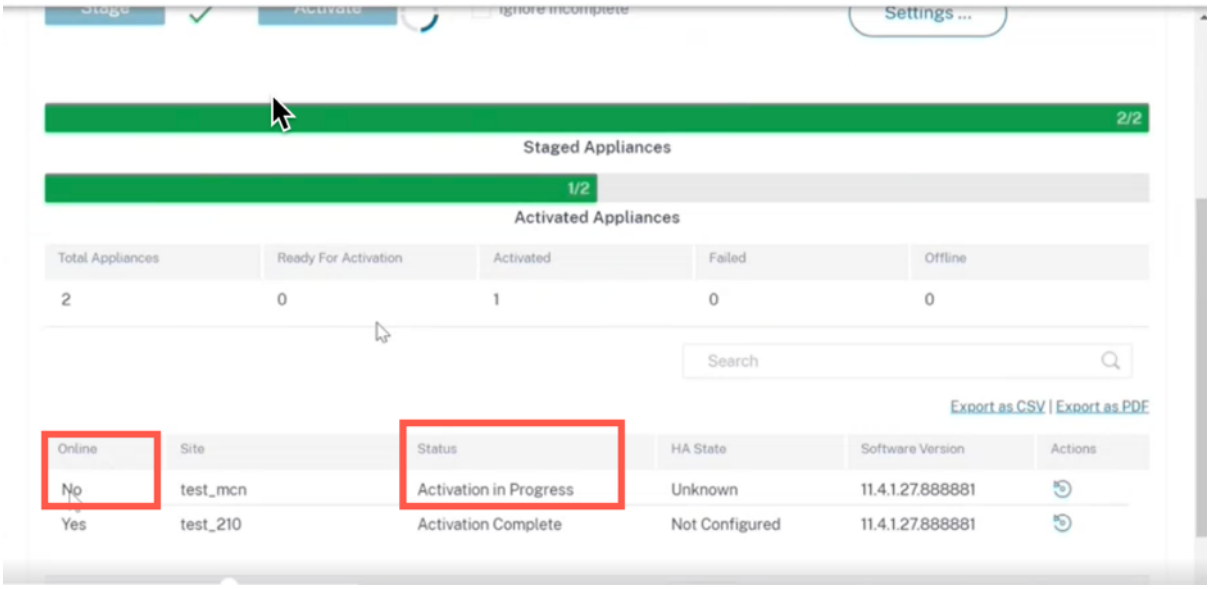


> **Remarque**
> La restauration sur les sites n'est effectuée que lorsque le site perd sa connectivité après l'activation. La restauration n'est pas déclenchée dans les cas où le site est en ligne et que l'activation a échoué.

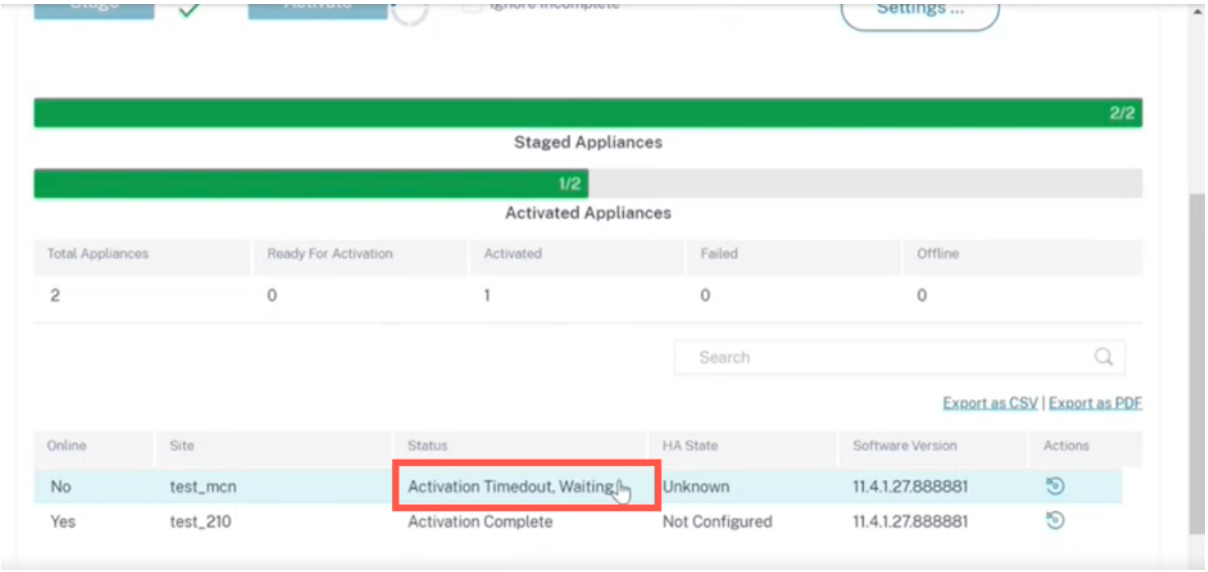
Cliquez sur **Terminé** une fois que vous avez activé la **restauration en cas d'erreur** .

Cas d'utilisation 1 : mise à niveau sans succès

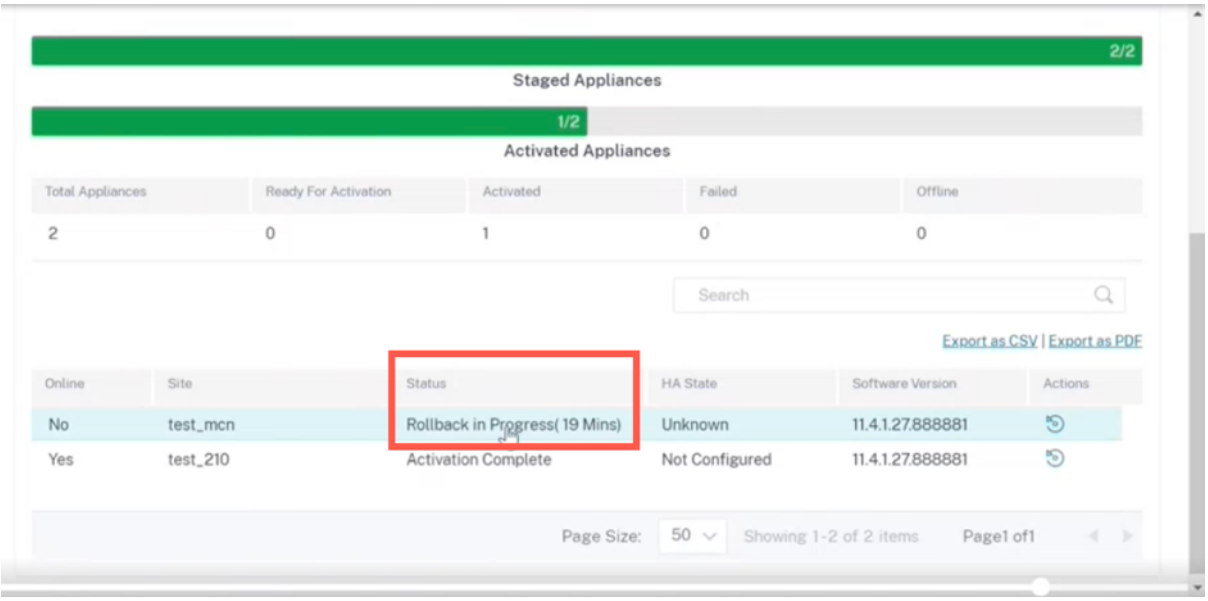
Un site attend la fin de l'activation pendant une durée spécifiée avec le statut **Activation en cours**.



Après ce délai d'expiration, si le site est toujours hors ligne, le service Citrix SD-WAN Orchestrator attend 30 minutes supplémentaires (délai d'initialisation du rollback) pour permettre au site de se reconnecter. À ce stade, l'état indique que le **délai d'activation est dépassé, en attente du lancement de la restauration (temps restant en minutes)**.

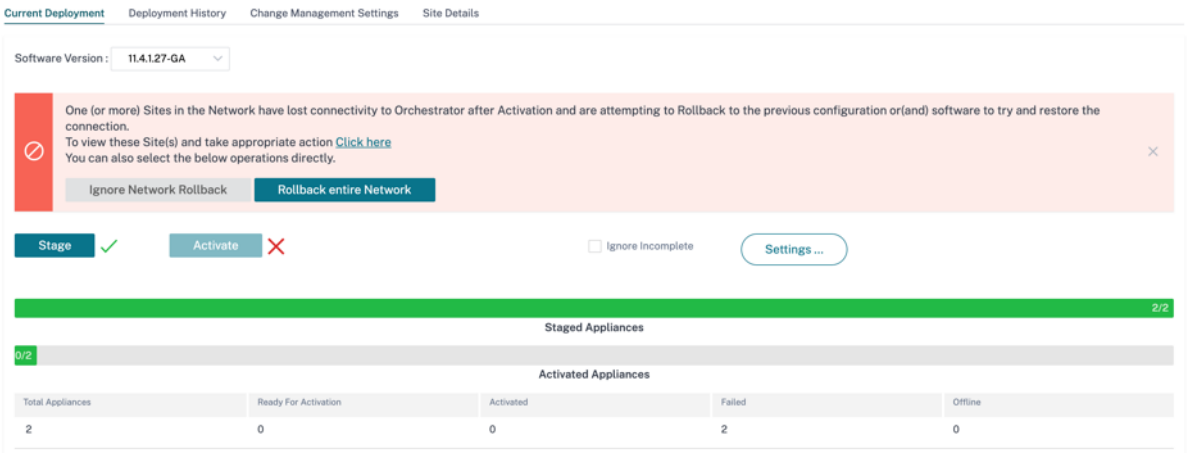


Après le délai d'attente de 30 minutes, l'appliance déclenche un retour automatique à la configuration précédente ou (et) au logiciel pour tenter de restaurer la connectivité du service Citrix SD-WAN Orchestrator. Le service Citrix SD-WAN Orchestrator attend 20 minutes (paramètre non configurable) pour que l'appliance se connecte au service Citrix SD-WAN Orchestrator et pendant cette période, l'état est indiqué comme **Rollback en cours (temps restant en minutes)**.



Si l'appliance ne parvient pas à se reconnecter, au cours de ces 20 minutes, le service Citrix SD-WAN Orchestrator marque l'opération de restauration comme ayant échoué et l'état est indiqué comme **Device Rollback Failed**.

Sur le réseau, si au moins un appareil a lancé le rollback automatique, une bannière est présentée à l'utilisateur comme suit :

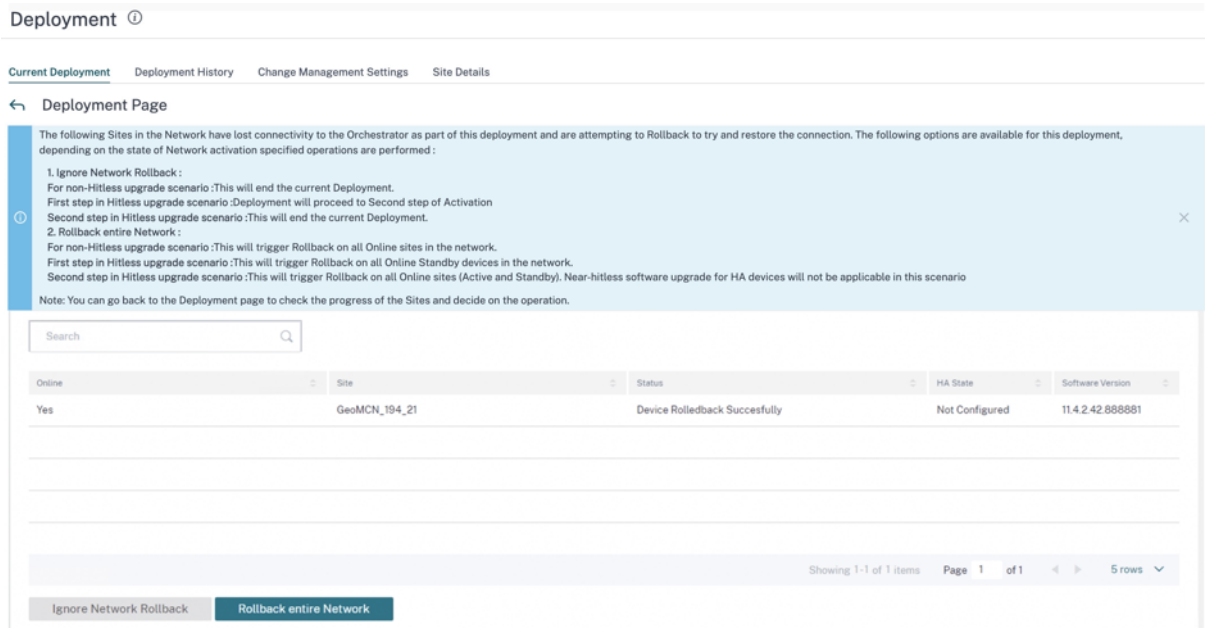


En fonction de l'étape de l'activation du réseau, les options affichées effectuent les opérations suivantes :

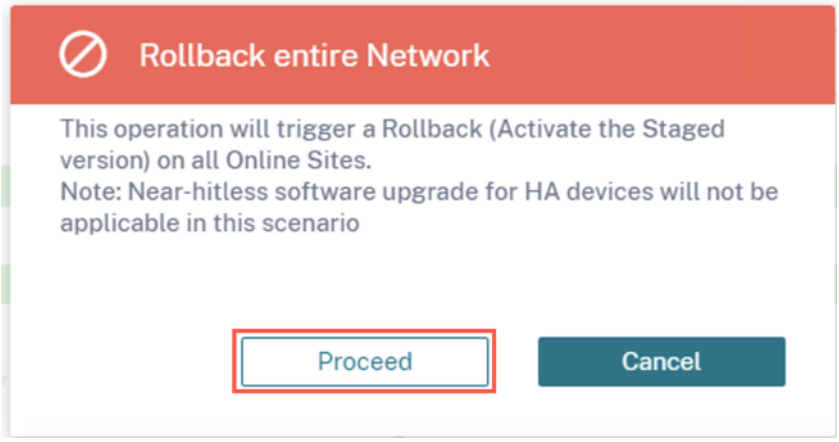
- Ignorer la restauration du réseau :
  - **Pour un scénario de mise à niveau sans succès** : mettez fin au déploiement en cours.
  - **Première étape du scénario de mise à niveau de Hitless** : le déploiement passe à la deuxième étape de l'activation.
  - **Deuxième étape du scénario de mise à niveau de Hitless** : mettre fin au déploiement en cours.
- Annulation de l'ensemble du réseau :
  - **Pour un scénario de mise à niveau sans**accès direct : déclenchez la restauration sur tous les sites en ligne du réseau.
  - **Première étape du scénario de mise à niveau de Hitless** : déclenchez le rollback sur tous les appareils en veille en ligne du réseau.
  - **Deuxième étape du scénario de mise à niveau de Hitless** : déclenchez le rollback sur tous les sites en ligne (actifs et en veille). La mise à niveau logicielle quasi automatique pour les appareils à haute disponibilité n'est pas applicable dans ce scénario.

Vous pouvez cliquer sur le lien hypertexte Plus **Cliquez ici** pour afficher la liste des sites pour lesquels la restauration est en cours ou terminée et effectuer les actions ci-dessus pour cette page.

Vous pouvez également attendre que les sites qui ont déclenché la restauration réussissent ou échouent avant de décider de déclencher la restauration à l'échelle du réseau.



Si vous sélectionnez l'option **Rétrograder l'ensemble du réseau**, la boîte de dialogue suivante s'affiche.



> **Remarque :**
> La mise à niveau logicielle quasi automatique pour une appliance haute disponibilité n'est pas applicable dans ce scénario, c'est-à-dire que s'il existe des sites de haute disponibilité sur le réseau, le déclenchement d'une restauration à l'échelle du réseau active les deux appliances de haute disponibilité de ce site en même temps, ce qui peut entraîner interruption du réseau.

Cliquez sur **Procéder** pour démarrer la restauration à l'échelle du réseau sur tous les sites en ligne.

Cas d'utilisation 2 : Hitless Upgrade

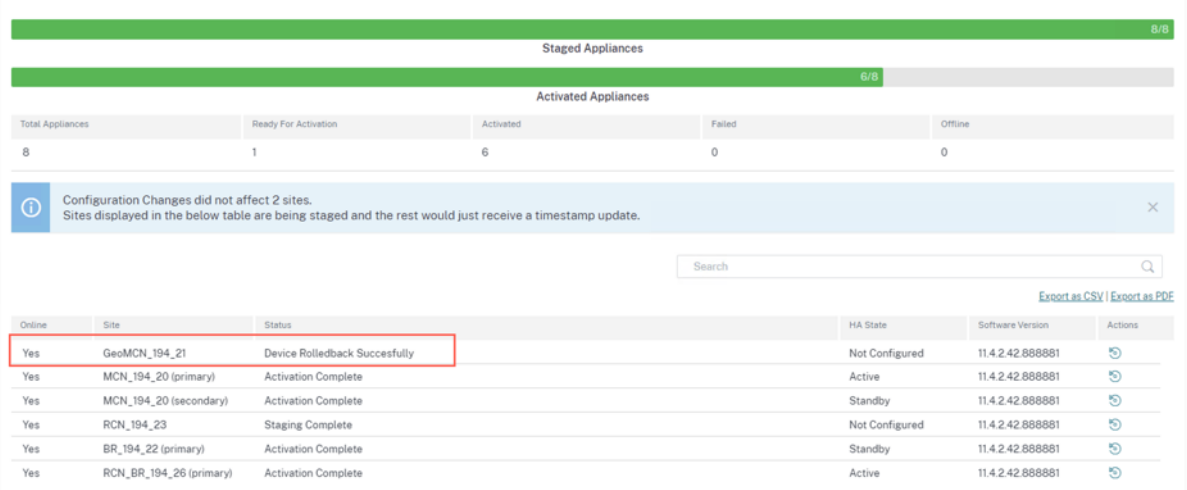
Dans le cas de la mise à niveau par Hitless, les appareils de secours seraient activés en premier, suivis des appareils actifs et non à haute disponibilité. Dans un premier temps, si l'appliance de secours se

déconnecte après l'activation et initie une restauration, les options suivantes sont disponibles :

- **Ignorer la restauration du réseau** : ignorez les appliances en veille qui sont hors ligne et procédez à l'activation des appliances actives.
- **Rétrograder l'ensemble du réseau** : annulez toutes les appliances de secours en ligne qui ont terminé l'activation et mettez fin au déploiement en cours. Aucune activation de l'appliance active et non à haute disponibilité n'est effectuée dans ce cas.

L'étape suivante de la mise à niveau automatique, à savoir l'activation d'un dispositif actif et non à haute disponibilité, consiste à suivre le même processus de restauration des erreurs, comme indiqué dans la section de mise à niveau sans incident ci-dessus. Dans ce scénario, si vous choisissez **Rollback entire Network**, le rollback se déclenche pour tous les dispositifs (actifs et en veille).

Une fois que le site a terminé la restauration et se reconnecte au service Citrix SD-WAN Orchestrator, l'état de ce site indique **Device Rollback Successful** et les sites sont en ligne.



Limitations

La correction automatique pour les appareils et le réseau rétrogradés ou restaurés n'est pas prise en charge.

> **Remarque**
> La restauration automatique du site n'est qu'un mécanisme de sauvegarde pour tenter de restaurer la connectivité perdue au service Citrix SD-WAN Orchestrator. Si l'appliance ne parvient toujours pas à se connecter au service Citrix SD-WAN Orchestrator, vérifiez la configuration réseau de cette appliance.

Vous pouvez exporter les résultats filtrés vers un fichier CSV ou PDF à l'aide des options **Exporter au format CSV** et **Exporter au format PDF** . Le nom du fichier CSV et PDF est précédé de la **liste des sites de déploiement**, suivie de la date et de l'heure d'exportation du fichier.

- **Étape** : Une fois la vérification de la configuration réussie, cliquez sur **Stage** pour distribuer les fichiers de configuration à toutes les appliances de votre réseau. Par défaut, le service Citrix SD-WAN Orchestrator attend que tous les nœuds de contrôle (MCN, RCN, Geo MCN, Geo RCN) et les appliances des succursales en ligne soient mis en place avant de permettre à l'utilisateur de procéder à l'activation.

  Si le processus de transfert échoue sur n'importe quel site, utilisez l'option **Retry Staging**, dans la colonne **Actions**, pour relancer le processus de préparation.

- **Activer** : cliquez sur **Activer** pour activer la configuration par étapes sur tous les sites du réseau.
- **Ignorer les éléments incomplets** : lorsque cette case est sélectionnée, la case **Activer** n'est activée qu'une fois que tous les nœuds de contrôle en ligne (MCN, RCN, Geo MCN, Geo RCN) ont été transférés. Vous pouvez choisir de l'activer même si certains appareils de la succursale en ligne ne sont pas intermédiaires. Les appliances des succursales en ligne qui ne parviennent pas à être transférées sont ignorées.
- **Paramètre de mise à niveaupartielle du site : L'option de mise à niveau**partielle du site est ajoutée pour mettre à niveau ou rétrograder les sites sélectionnés avec une version différente. La fonctionnalité de**mise à niveau partielle du site** permet de tester une nouvelle version avant de la déployer sur l'ensemble du réseau.

Grâce à la fonctionnalité de **mise à niveau partielle du site**, les mises à niveau peuvent être échelonnées, réduisant ainsi l'impact des mises à niveau logicielles pendant les heures de bureau.

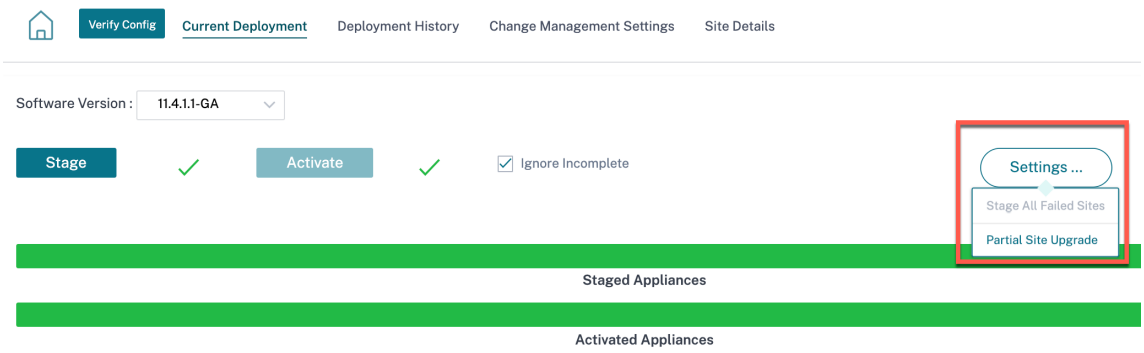
> **Remarque**
>
> La mise à niveau partielle du site ne peut être effectuée que lorsque tous les sites du réseau exécutent le logiciel Citrix SD-WAN version 11.2.2 ou supérieure.

Toute modification de configuration pour la **mise à niveau partielle du site** nécessite une gestion des modifications pour que les modifications prennent effet. La **mise à niveau partielle du site** sélectionne la version inférieure et génère la configuration correspondante. Aucune nouvelle fonctionnalité ne peut être testée lorsque le réseau est en mode de **mise à niveau partielle du site** .

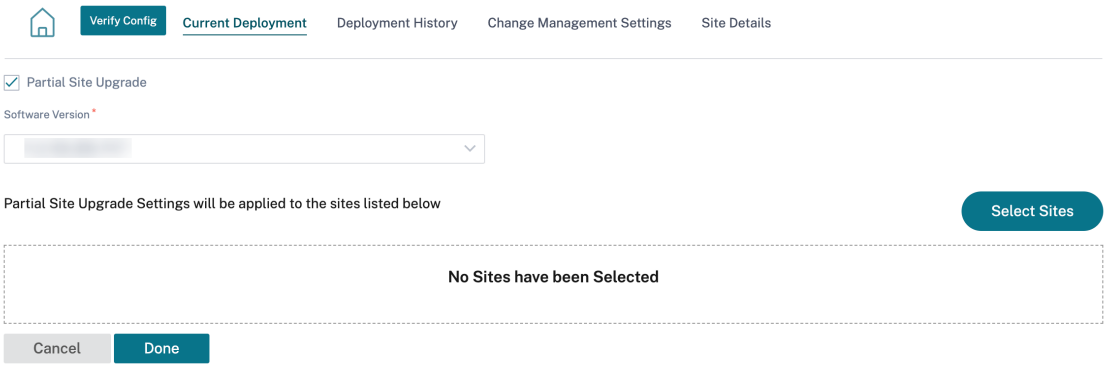
Lorsque vous passez d'une version plus récente à une version plus ancienne à l'aide de la **mise à niveau partielle du site**, si une fonctionnalité n'est prise en charge que dans la nouvelle version (avec une configuration similaire présente à la fois dans la nouvelle et dans l'ancienne version), des erreurs d'audit se produisent. Par exemple, si une nouvelle plate-forme est sélectionnée, qui n'est prise en charge que sur la nouvelle version, cela provoquera des erreurs d'audit.

Pour effectuer la mise à niveau partielle du site :

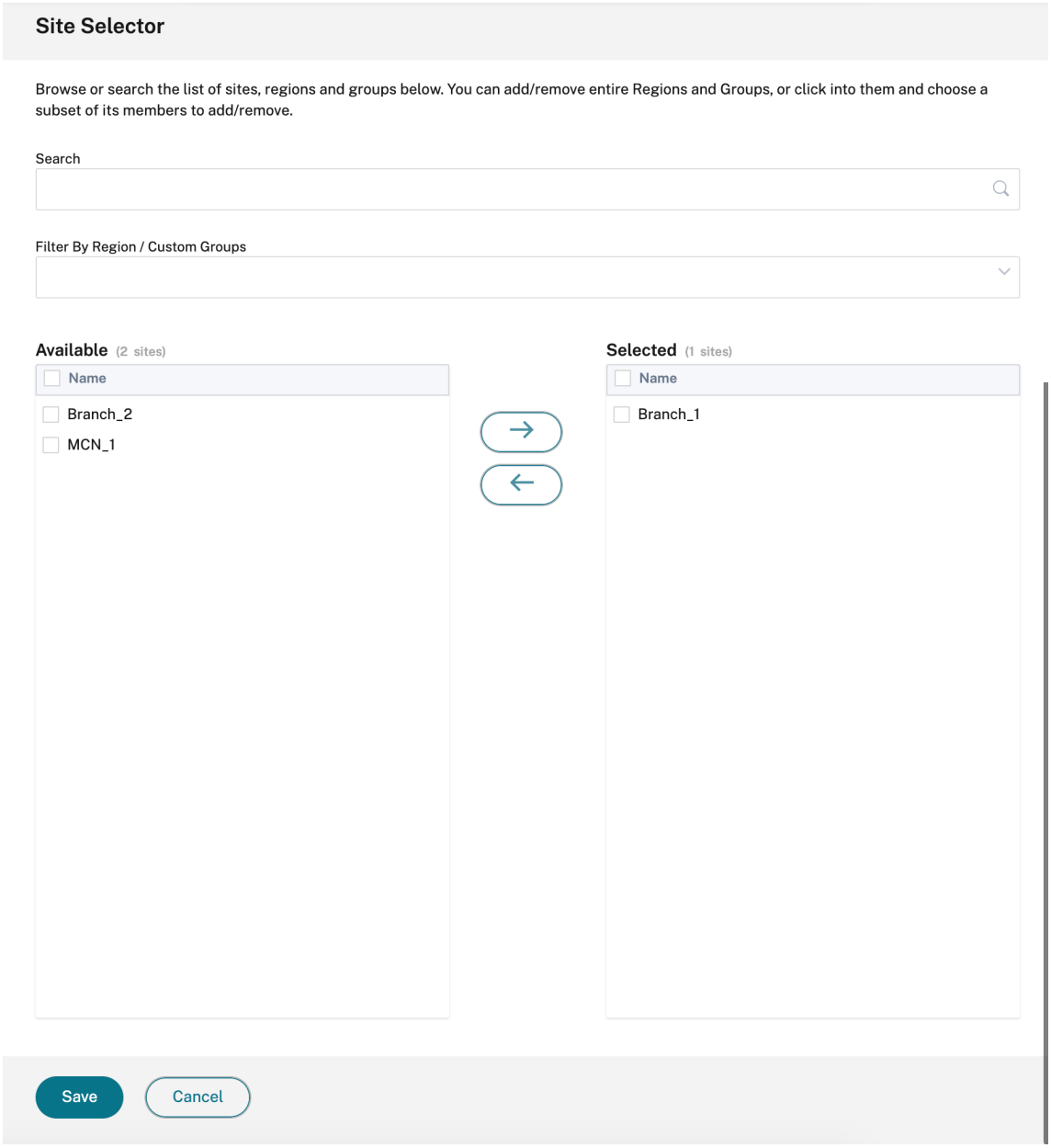
1. Cliquez sur le **paramètre…** et sélectionnez l'option de **mise à niveau partielle du site** .

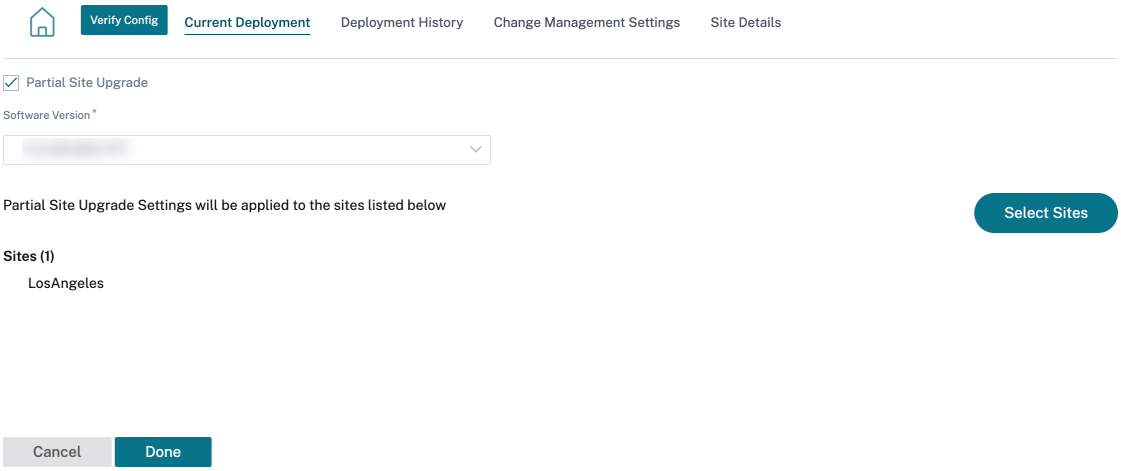


2. Cochez la case Mise à niveau partielle du site, choisissez la version du logiciel et cliquez sur **Sélectionner des sites** pour ajouter de nouveaux sites.



3. Sélectionnez les sites et cliquez sur **Enregistrer**.

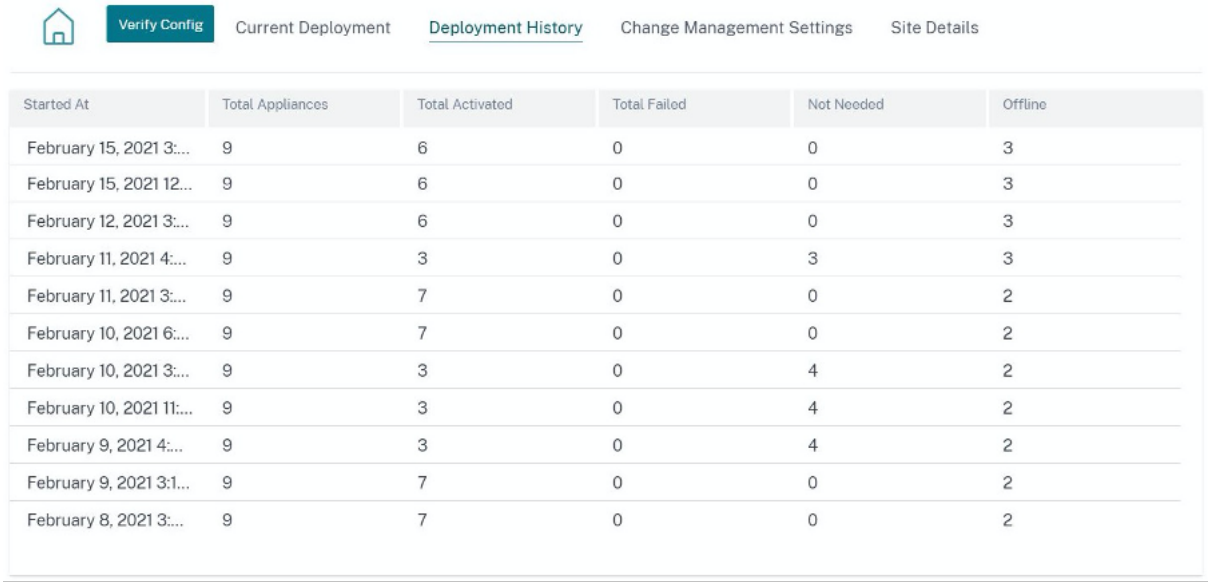




Dans le cas d'une mise à jour portant uniquement sur la configuration, seuls les sites dont la configuration a été modifiée sont transférés et activés. Pour les autres sites, l'horodatage est mis à jour et traité.

Si la version du logiciel est modifiée, la configuration et le package logiciel sont organisés et activés sur tous les sites du réseau.

La section **Historique des déploiements** permet de passer en revue les opérations de déploiement précédentes et leurs résultats.



Started At	Total Appliances	Total Activated	Total Failed	Not Needed	Offline
February 15, 2021 3:...	9	6	0	0	3
February 15, 2021 12...	9	6	0	0	3
February 12, 2021 3:...	9	6	0	0	3
February 11, 2021 4:...	9	3	0	3	3
February 11, 2021 3:...	9	7	0	0	2
February 10, 2021 6:...	9	7	0	0	2
February 10, 2021 3:...	9	3	0	4	2
February 10, 2021 11:...	9	3	0	4	2
February 9, 2021 4:...	9	3	0	4	2
February 9, 2021 3:1...	9	7	0	0	2
February 8, 2021 3:...	9	7	0	0	2

Mise à niveau logicielle HA quasi sans perturbations

Lors de la mise à niveau logicielle (versions 11.0.x et antérieures), la préparation et l'activation de toutes les appliances du réseau sont effectuées en même temps. Cela inclut la paire High Availability

(HA), ce qui entraîne des temps d'arrêt du réseau. Grâce à la fonctionnalité de mise à niveau logicielle rapide et rapide, le service Citrix SD-WAN Orchestrator garantit que le temps d'arrêt pendant le processus de mise à niveau logicielle (11.1.x et versions ultérieures) ne dépasse pas celui du switch HA au fil du temps.

> **Remarque**
>
> La mise à niveau logicielle HA quasi sans perturbations est applicable pour les éléments suivants :
>
> - Les sites qui sont déployés en mode haute disponibilité (HA). Elle ne s'applique pas aux sites autres que la HA.
> - Déploiements basés sur le service Citrix SD-WAN Orchestrator uniquement et non pour les réseaux gérés à l'aide du SD-WAN Center ou du MCN.
> - Mise à niveau logicielle uniquement et non mises à jour de configuration. S'il y a un changement de configuration en même temps que le logiciel dans le cadre de la mise à niveau, le service Citrix SD-WAN Orchestrator n'effectue pas de mise à niveau logicielle en haute disponibilité quasi automatique et poursuit la mise à niveau de la manière antérieure (mise à niveau en une seule étape).

Résumé de la séquence de mise à niveau :

1. Le service Citrix SD-WAN Orchestrator vérifie l'état HA de toutes les appliances du réseau.
2. Met à niveau toutes les appliances secondaires qui sont en **mode veille** .
3. Le basculement HA est déclenché et l'état des appareils **actifs** et **en veille** est modifié.
4. Met à niveau les appliances principales qui sont actuellement en **mode veille** .

La mise à niveau logicielle haute disponibilité quasi sans perturbations est un processus de mise à niveau en deux étapes :

Étape 1 : Lors de la mise à niveau logicielle, après la version 11.1, le service Citrix SD-WAN Orchestrator effectue d'abord la mise à niveau logicielle sur toutes les appliances en état de **veille** sur le réseau. Le réseau est toujours opérationnel avec les **appareils actifs** en place.

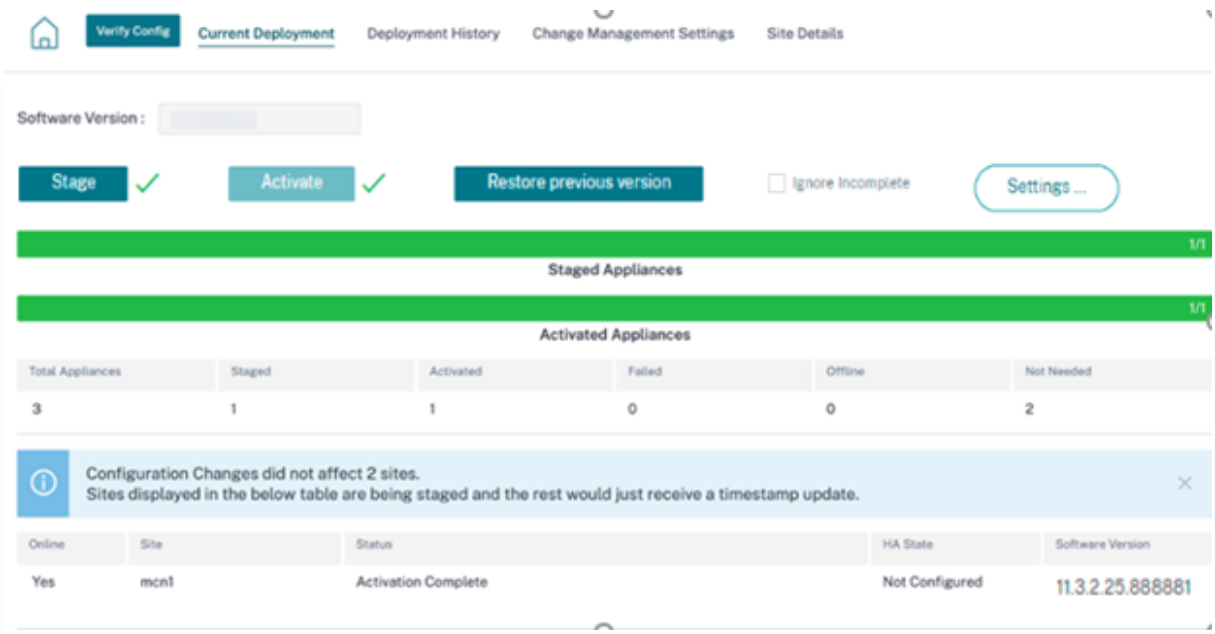
Une fois que tous les appareils **Standby** ont été mis à niveau vers la dernière version logicielle, le basculement HA est déclenché sur le réseau. Les appareils **Standby** (dotés du logiciel le plus récent) deviennent **actifs**.

Étape 2 : Les appareils **Standby** actuels dotés d'une ancienne version logicielle sont mis à niveau vers la dernière version logicielle et continueront à fonctionner en mode **veille** .

Au cours de ce processus de mise à niveau du logiciel, tous les autres sites non HA seront également activés avec les logiciels les plus récents.

Pour plus d'informations, consultez la FAQ.

Vous pouvez consulter l'état de la mise à niveau en accédant à **Deployment Tracker** > **Deployment actuel**.



- **Étape** : Cliquez sur **Stage** pour distribuer les fichiers de configuration à toutes les appliances de votre réseau. Par défaut, le service Citrix SD-WAN Orchestrator attend que tous les nœuds de contrôle (MCN, RCN, Geo MCN, Geo RCN) et les appliances de succursale en ligne soient mis en place avant de permettre à l'utilisateur de procéder à l'activation.
- **Activer** : cliquez sur **Activer** pour activer la configuration par étapes sur tous les sites du réseau.
- **Restaurer la version précédente** : Cliquez sur **Restaurer la version précédente** pour revenir à la configuration précédemment activée sur votre réseau. La mise à niveau logicielle rapide à haute disponibilité est applicable lorsque vous restaurez la version précédente si la version précédemment active est simplement une modification de version du logiciel et non une modification de configuration. Pour plus d'informations sur cette fonctionnalité, voir Restaurer la version précédente.
- **Ignorer les éléments incomplets** : lorsque cette case est sélectionnée, la case **Activer** n'est activée qu'une fois que tous les nœuds de contrôle en ligne (MCN, RCN, Geo MCN, Geo RCN) ont été transférés. Vous pouvez choisir de l'activer même si certains appareils de la succursale en ligne ne sont pas intermédiaires. Les appliances des succursales en ligne qui ne parviennent pas à être transférées sont ignorées.

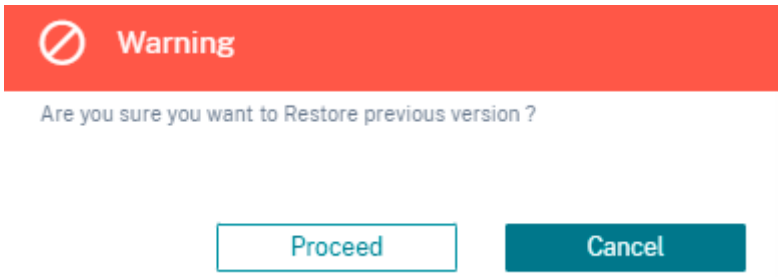
Dans le cas d'une mise à jour portant uniquement sur la configuration, seuls les sites dont la configuration a été modifiée sont transférés et activés. Pour les autres sites, l'horodatage est mis à jour et traité. La colonne **Non nécessaire** répertorie le nombre de sites pour lesquels aucune modification de configuration n'a été apportée.

Si la version du logiciel est modifiée, la configuration et le package logiciel sont organisés et activés sur tous les sites du réseau.

Restaurer la version précédente

Dans la fonctionnalité de restauration de la version précédente, le service Citrix SD-WAN Orchestrator lance une activation à l'échelle du réseau de la configuration précédente et restaure la configuration (et/ou le logiciel) précédemment activée sur votre réseau.

Lorsque vous sélectionnez l'option **Restaurer la version précédente**, le message de confirmation suivant s'affiche :



> **Remarque**
>
> L'action Restaurer la version précédente peut être effectuée lorsque le réseau n'est pas à l'état intermédiaire. Cette option est désactivée pour les réseaux intermédiaires.

Correction automatique pour la configuration et la mise à niveau logicielle

Dans le service Citrix SD-WAN Orchestrator, la fonctionnalité de correction automatique est mise en œuvre dans le flux de travail de gestion des modifications.

Lorsque le transfert a échoué pour un site et si le site qui a échoué de la mise en attente est un nœud de contrôle, vous devez redémarrer après avoir reçu le message d'échec de la mise en attente. Le bouton **Activer** ne sera pas activé si la mise en scène échoue pour les nœuds de contrôle. Si le site dont le transfert a échoué est un nœud de branche, vous êtes toujours autorisé à procéder à l'activation. Mais pour synchroniser cette succursale avec le réseau, effectuez une autre série de gestion du changement.

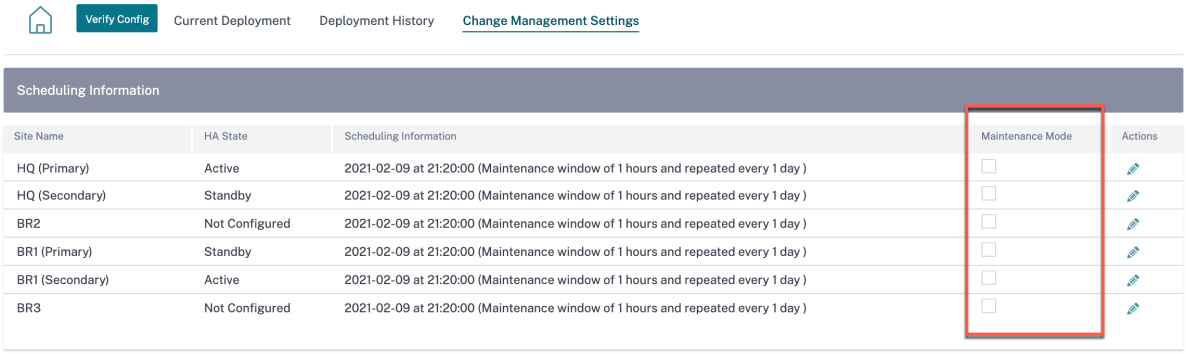
> **Remarque**
>
> - La vérification de correction automatique ne commence qu'après avoir cliqué sur le bouton **Activer** et s'arrête lorsque l'étape suivante est émise depuis l'interface utilisateur du service Citrix SD-WAN Orchestrator.
> - La fonctionnalité du mode maintenance ne s'applique qu'à la fonction de correction automatique. Si vous lancez une **étape et uneactivation**, l'appliance dont le mode de maintenance est activé est également mise à jour avec les modifications apportées au logiciel et à la configuration.

Avec l'amélioration de la fonction de correction automatique, lorsqu'une panne de transit se produit, le mécanisme de correction automatique pousse le logiciel et la version de configuration attendue vers la succursale défaillante et tente de la synchroniser avec le réseau actuel. La fonction de correction automatique est applicable en cas d'échec de transfert sur le nœud de succursale et d'échec d'activation sur n'importe quel nœud.

Les deux points de déclenchement suivants sont les deux points de déclenchement de la correction automatique :

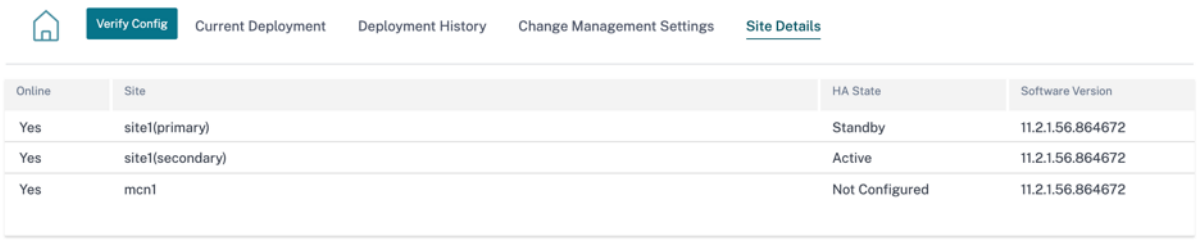
- Dans l'interface utilisateur du suivi du déploiement du service Citrix SD-WAN Orchestrator, une fois que vous recevez un message **d'échec de l'étape** ou **d'échec de l'activation**, la correction automatique commence à s'exécuter en arrière-plan. La vérification de correction automatique démarre une fois l'activation terminée.
- En cas de non-concordance entre le logiciel et la configuration, lorsque l'appliance n'a pas fourni le logiciel et la version de configuration attendus, le service Citrix SD-WAN Orchestrator commence à transférer le logiciel et la copie de configuration réellement requis vers l'appliance pour activation.

Pour dépanner un dispositif manuellement, cochez la case Mode maintenance sous les **paramètres de gestion des modifications**. Cette case à cocher permet de contrôler si le périphérique doit être coché pour une correction automatique ou non. Une fois que la case à cocher Mode de maintenance est désactivée, la correction automatique permet à l'appliance de se synchroniser avec le logiciel réseau et la version de configuration.



Détails du site

L'onglet **Détails du site** situé sous le Deployment Tracker fournit des informations sur tous les appareils du réseau. Le tableau contient le nom de l'appliance, la connectivité du service Citrix SD-WAN Orchestrator, l'état de haute disponibilité (HA) et la version du logiciel en cours d'exécution.



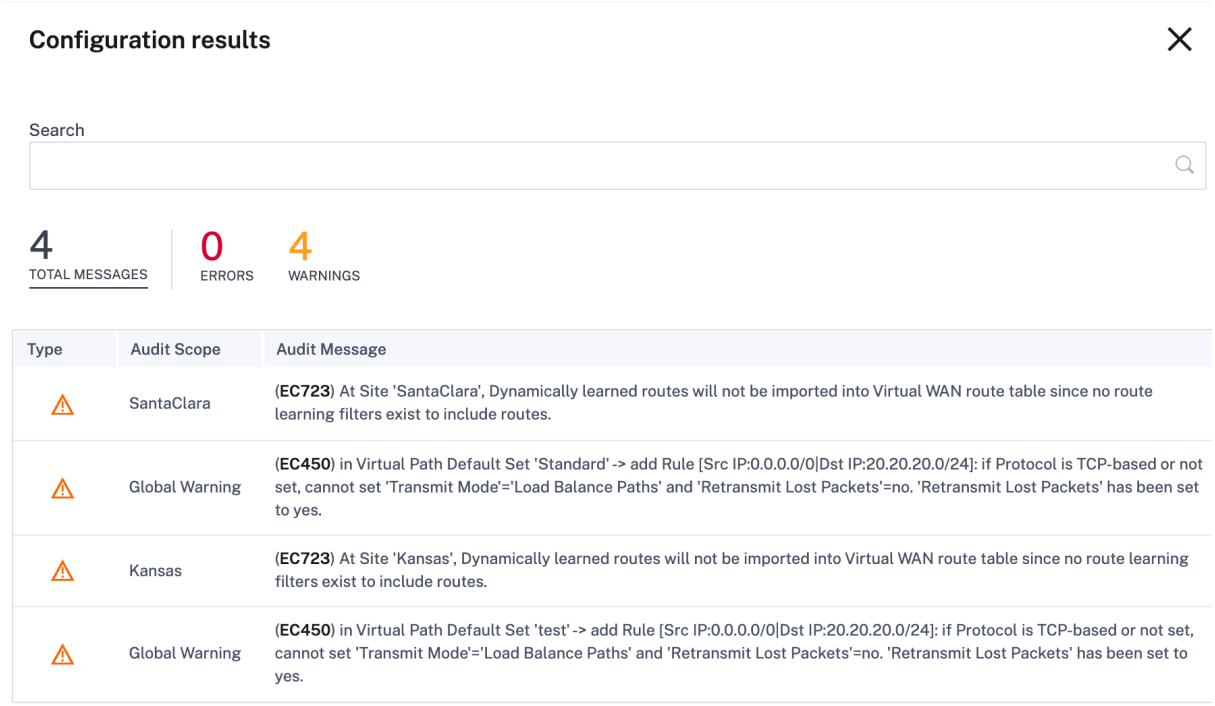
Vérifier la configuration

Vous pouvez cliquer sur **Vérifier la configuration** pour valider la configuration réseau et vérifier l'absence d'erreur ou d'avertissement d'audit. Lorsque vous cliquez sur **Vérifier la configuration, la page des résultats** de configuration s'affiche. Cette page contient des informations détaillées sur les erreurs d'audit et les avertissements.

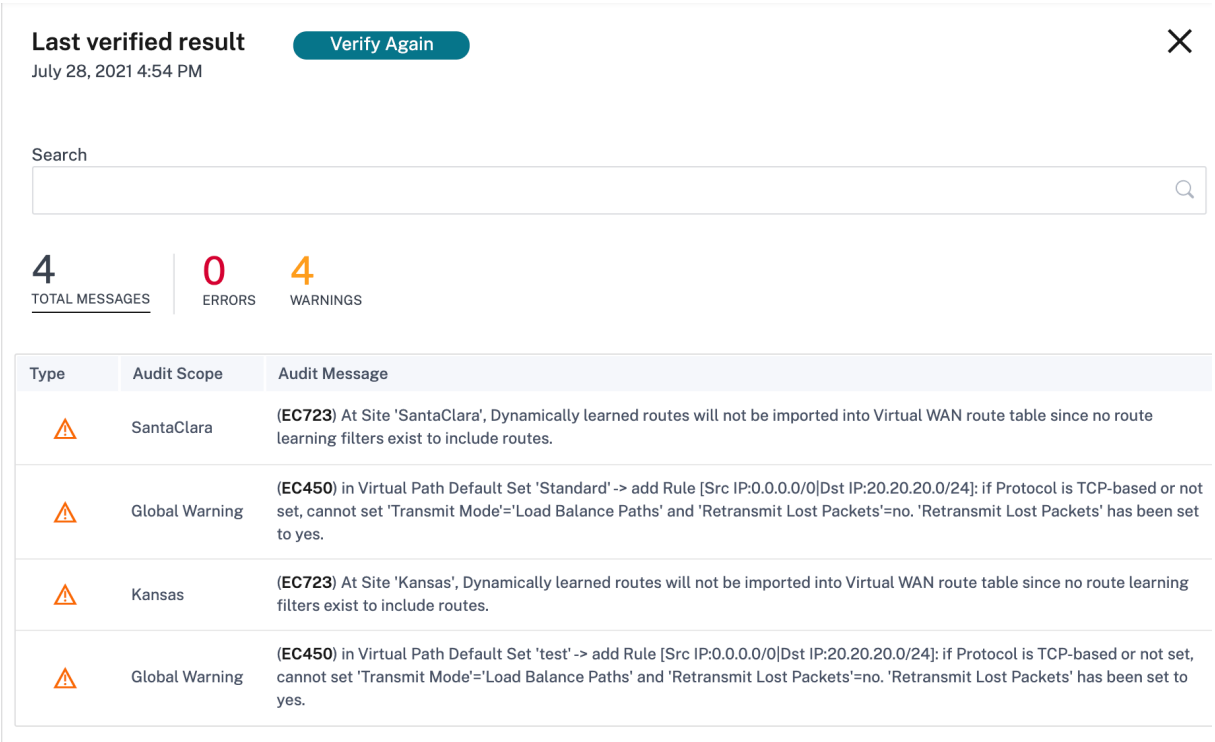
Les résultats de configuration affichent le nombre total d'erreurs d'audit et d'avertissements. Les résultats sont également filtrés en fonction du type d'audit (erreur ou avertissement) et affichés avec différents codes de couleur. Vous pouvez cliquer sur les liens numériques pour afficher les résultats filtrés.

La colonne **Type** affiche une icône pour indiquer s'il s'agit d'une erreur ou d'un avertissement. La colonne **Étendue de l'audit** indique si l'erreur ou l'avertissement concerne un site ou au niveau du réseau. Si l'erreur ou l'avertissement est spécifique à un site, le nom du site s'affiche. Si l'erreur ou l'avertissement se situe au niveau global, l'**erreur globale** ou l'**avertissement global** s'affichent respectivement. La colonne **Message d'audit** contient le code d'erreur et le message d'erreur.

Vous pouvez utiliser la barre de recherche pour rechercher des erreurs ou des avertissements spécifiques en fonction du type, du code d'erreur, du nom du site ou du message d'erreur.



Lorsque vous cliquez sur **Vérifier la configuration** pour la deuxième fois, la page des **résultats de la configuration** s'ouvre et affiche les mêmes résultats que lors de la dernière vérification de la configuration, ainsi que la date et l'heure. Si nécessaire, vous pouvez cliquer sur **Vérifier à nouveau** pour relancer la validation.



Définitions des services

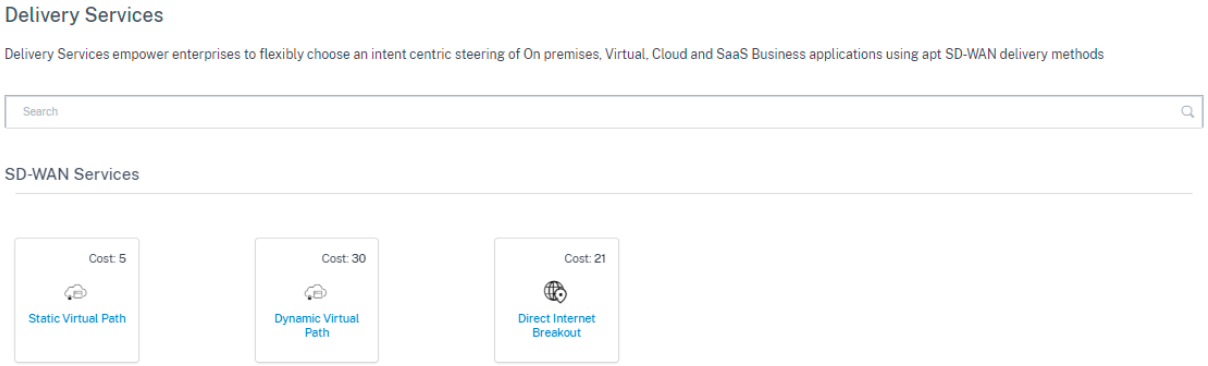
October 21, 2022

Les canaux de distribution sont généralement classés selon les définitions des services et l'allocation de bande passante.

Les services de diffusion sont des mécanismes de mise à disposition disponibles sur Citrix SD-WAN pour piloter différentes applications ou profils de trafic à l'aide des méthodes de diffusion appropriées en fonction des objectifs commerciaux. Vous pouvez configurer des services de diffusion tels qu'Internet, Intranet, Virtual Paths, IPsec et LAN GRE. Les services de livraison sont définis globalement et s'appliquent aux liaisons WAN sur des sites individuels, le cas échéant.

Chaque liaison WAN peut appliquer la totalité ou un sous-ensemble des services concernés et configurer des parts relatives de bande passante (%) entre tous les services de distribution.

Le service Virtual Path est disponible sur tous les liens par défaut. Les autres services peuvent être ajoutés au besoin.
Pour configurer les services de livraison, au niveau du client, accédez à **Configuration** > **Canaux de distribution** > **Définitions des services**.



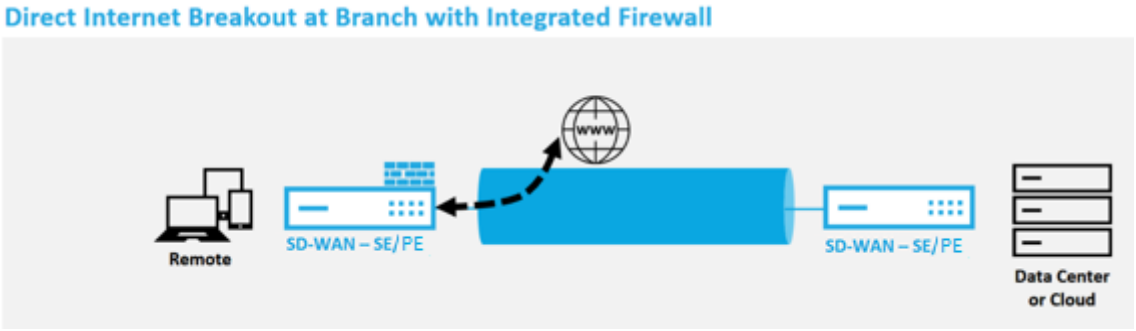
Les services de prestation peuvent être classés de façon générale comme suit :

- **Service de chemin virtuel** : tunnel SD-WAN superposé à double extrémité qui offre une connectivité sécurisée, fiable et de haute qualité entre deux sites hébergeant des appliances SD-WAN ou des instances virtuelles. Définissez la bande passante minimale réservée pour chaque chemin virtuel en Kbits/s. Ce paramètre est appliqué à toutes les liaisons WAN sur tous les sites du réseau.
- **Service Internet** : canal direct entre un site SD-WAN et Internet public, sans encapsulation SD-WAN. Citrix SD-WAN prend en charge la fonctionnalité d'équilibrage de charge de session pour le trafic Internet via plusieurs liens Internet.
- **Service intranet** : connectivité basée sur des liens sous-jacents entre un site SD-WAN et tout

site non SD-WAN. Le trafic est non encapsulé ou peut utiliser n'importe quelle encapsulation de chemin non virtuel telle que IPSec, GRE. Vous pouvez configurer plusieurs services Intranet.

Service Internet

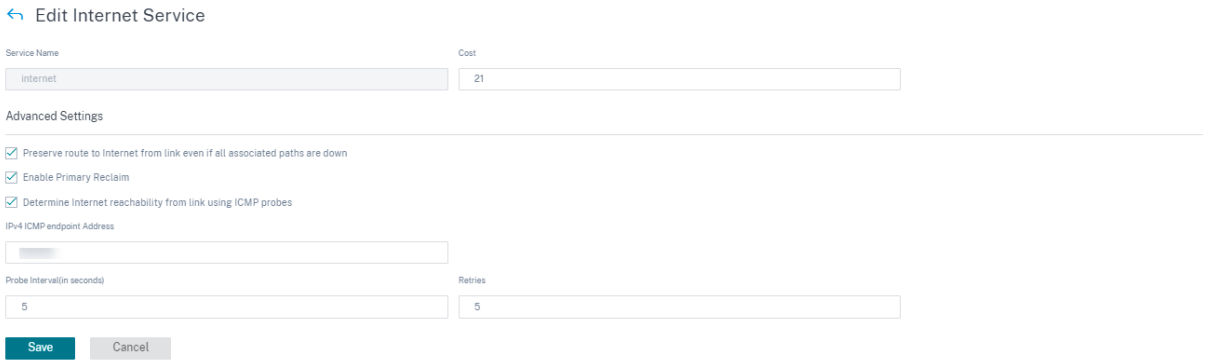
Le**service Internet** est disponible par défaut dans le cadre des services de livraison. Pour configurer un service Internet, au niveau du client, accédez à **Configuration** > **Canaux de distribution** > **Définitions des services**. Dans la section **Services SD-WAN**, sélectionnez la vignette **Direct Internet Breakout**, puis cliquez sur **Ajouter**.



Vous pouvez configurer les services Internet suivants :

- **Préserver l'itinéraire vers Internet à partir du lien même si tous les chemins associés sont inactifs** : vous pouvez configurer le coût de l'itinéraire du service Internet par rapport à d'autres services de distribution. Avec ce service, vous pouvez conserver l'itinéraire vers Internet à partir du lien, même si tous les chemins associés sont inactifs. Si tous les chemins associés à une liaison WAN sont inactifs, l'appliance SD-WAN utilise cette route pour envoyer/recevoir du trafic Internet.
- **Déterminez l'accessibilité à Internet à partir d'une liaison à l'aide de sondes**ICMP : vous pouvez activer les sondes ICMP pour des liens WAN Internet spécifiques vers un serveur explicite sur Internet. Avec le réglage de la sonde ICMP, l'appliance SD-WAN traite la liaison Internet comme étant active lorsque les chemins membres de la liaison sont actifs ou lorsque la réponse de la sonde ICMP est reçue du serveur.
- Adresse du point de**terminaison ICMP IPv4 : adresse**IPv4 de destination ou adresse du serveur.

- **Intervalle entre les sondes (en secondes)** : intervalle de temps pendant lequel l'appliance SD-WAN envoie des sondes sur les liaisons WAN configurées sur Internet. Par défaut, l'appliance SD-WAN envoie des sondes sur les liaisons WAN configurées toutes les 5 secondes.
- **Réessais** : nombre de nouvelles tentatives que vous pouvez tenter avant de déterminer si la liaison WAN est active ou non. Après 3 pannes de sonde consécutives, la liaison WAN est considérée comme morte. Le nombre maximum de nouvelles tentatives autorisées est de 10.



Modes de déploiement pris en charge

Le service Internet peut être utilisé dans les modes de déploiement suivants :

- Mode de déploiement en ligne (superposition SD-WAN)

Citrix SD-WAN peut être déployé en tant que solution de superposition sur n'importe quel réseau. En tant que solution de superposition, le SD-WAN est généralement déployé derrière des routeurs périphériques et/ou des pare-feu existants. Si le SD-WAN est déployé derrière un pare-feu réseau, l'interface peut être configurée comme fiable et le trafic Internet peut être acheminé vers le pare-feu en tant que passerelle Internet.

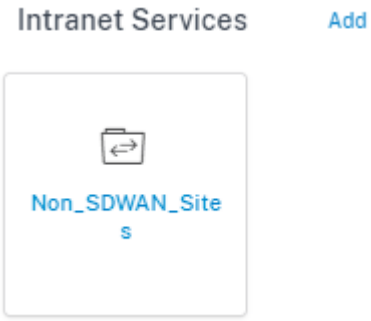
- Mode Edge ou passerelle

Citrix SD-WAN peut être déployé en tant que périphérique périphérique périphérique, en remplacement des périphériques de routeur Edge et/ou pare-feu existants. La fonctionnalité de pare-feu intégré permet au SD-WAN de protéger le réseau de la connectivité Internet directe. Dans ce mode, l'interface connectée à la liaison Internet publique est configurée comme non fiable, ce qui oblige le chiffrement à être activé, et les fonctionnalités de pare-feu et NAT dynamique sont activées pour sécuriser le réseau.

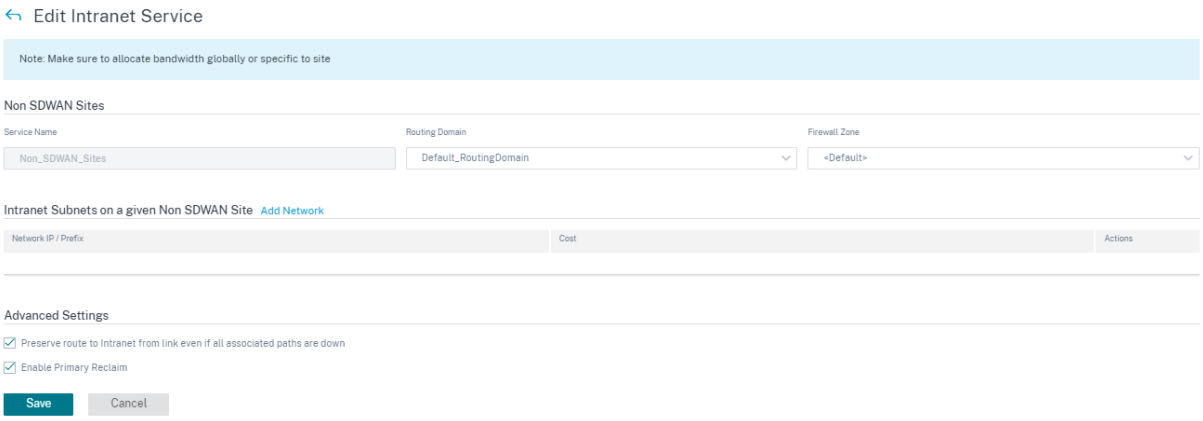
Service Intranet

Vous pouvez créer plusieurs services intranet. Pour ajouter un service Intranet, au niveau du client, accédez à **Configuration** > **Canaux de distribution** > **Définitions des services**. Dans la section **Ser-**

vices intranet, cliquez sur **Ajouter**.



Une fois le service intranet créé au niveau global, vous pouvez le référencer au niveau WAN Link. Fournissez un **nom de service**, sélectionnez le **domaine de routage** et la **zone de pare-feu**souhaités. Ajoutez toutes les adresses IP intranet sur le réseau, que d'autres sites du réseau peuvent interagir. Vous pouvez également conserver l'itinéraire vers l'intranet à partir du lien même si tous les chemins associés sont en panne.

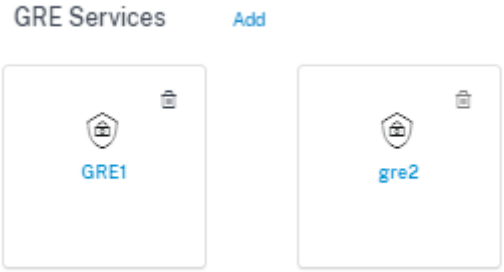


Service GRE

Vous pouvez configurer les appliances SD-WAN pour mettre fin aux tunnels GRE sur le réseau local.

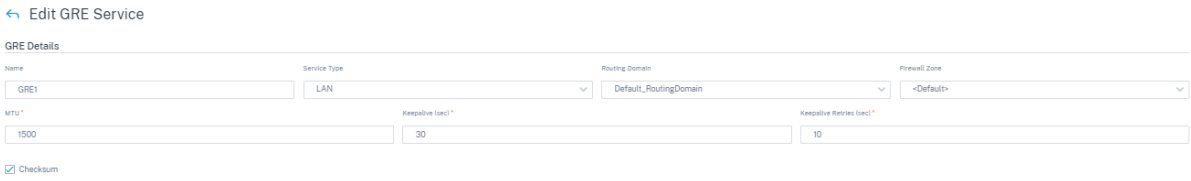
Pour ajouter un service GRE, au niveau du client, accédez à **Configuration** > **Canaux de distribution** > **Définitions des services**. Vous pouvez également accéder à la page de configuration **des services GRE** depuis **Configuration > Sécurité**.

Dans la section **IPsec et GRE**, accédez aux **services IPsec** et cliquez sur **Ajouter**.



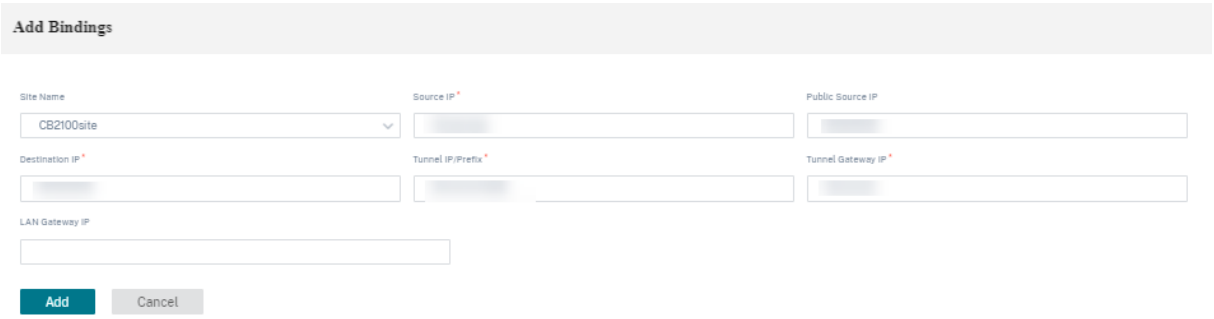
Détails du GRE :

- **Type de service** : Sélectionnez le service utilisé par le tunnel GRE.
- **Nom** : Nom du service LAN GRE.
- **Domaine de routage** : Domaine de routage pour le tunnel GRE.
- **Zone de pare-feu** : zone de pare-feu choisie pour le tunnel. Par défaut, le tunnel est placé dans Default_LAN_Zone.
- **MTU** : unité de transmission maximale : taille du plus grand datagramme IP pouvant être transféré via un lien spécifique. La gamme est de 576 à 1500. La valeur par défaut est 1500.
- **Keep alive** : Période entre l'envoi de messages de conservation de connexion active. S'il est configuré sur 0, aucun paquet « keep alive » n'est envoyé, mais le tunnel reste en place.
- **Réessais Keep Alive** : nombre de fois que l'appliance Citrix SD-WAN envoie des paquets Keep Alive sans réponse avant de fermer le tunnel.
- **Checksum** : active ou désactive Checksum pour l'en-tête GRE du tunnel.



Liaisons du site :

- **Nom du site** : Site permettant de cartographier le tunnel du GRE.
- **IP source** : adresse IP source du tunnel. Il s'agit de l'une des interfaces virtuelles configurées sur ce site. Le domaine de routage sélectionné détermine les adresses IP source disponibles.
- **IP source publique** : IP source si le trafic du tunnel passe par NAT.
- **IP de destination** : adresse IP de destination du tunnel.
- **IP/Préfixe du tunnel** : adresse IP et préfixe du tunnel GRE.
- **IP de la passerelle du tunnel** : adresse IP du prochain saut pour acheminer le trafic du tunnel.
- **IP de la passerelle LAN** : Adresse IP du saut suivant pour acheminer le trafic LAN.



Service IPSec

Les appliances Citrix SD-WAN peuvent négocier des tunnels IPsec fixes avec des homologues tiers du côté LAN ou WAN. Vous pouvez définir les points d'extrémité du tunnel et mapper les sites aux points d'extrémité du tunnel.

Vous pouvez également sélectionner et appliquer un profil de sécurité IPSec qui définit le protocole de sécurité et les paramètres IPSec.

Pour configurer les paramètres IPSec du chemin virtuel :

- Activez les tunnels IPSec de chemin virtuel pour tous les chemins virtuels pour lesquels la conformité FIPS est requise.
- Configurez l'authentification des messages en changeant le mode IPsec en AH ou ESP+Auth et en utilisant une fonction de hachage approuvée FIPS. SHA1 est accepté par la FIPS, mais SHA256 est fortement recommandé.
- La durée de vie IPSec ne doit pas être configurée plus de 8 heures (28 800 secondes).

Citrix SD-WAN utilise la version 2 de l'IKE avec des clés pré-partagées pour négocier des tunnels IPsec via le chemin virtuel en utilisant les paramètres suivants :

- DH Group 19 : ECP256 (courbe elliptique de 256 bits) pour la négociation de clés
- Chiffrement AES-CBC 256 bits
- Hachage SHA256 pour l'authentification des messages
- Hachage SHA256 pour l'intégrité des messages
- DH Group 2 : MODP-1024 pour un secret direct parfait

Pour configurer le tunnel IPsec pour un tiers, procédez comme suit :

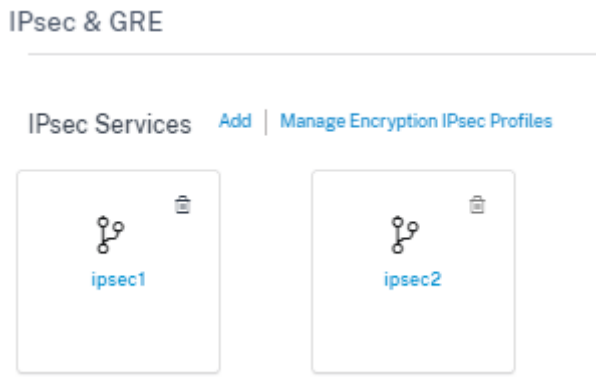
- Configurer le groupe DH approuvé FIPS. Les groupes 2 et 5 sont autorisés dans le cadre de la FIPS, mais les groupes 14 et plus sont fortement recommandés.
- Configurer la fonction de hachage approuvée FIPS. SHA1 est accepté par FIPS, mais SHA256 est fortement recommandé.

- Si vous utilisez iKev2, configurez une fonction d'intégrité approuvée par FIPS. SHA1 est accepté par FIPS, mais SHA256 est fortement recommandé.
- Configurez une durée de vie IKE et une durée de vie maximale ne dépassant pas 24 heures (86 400 secondes).
- Configurez l'authentification des messages IPsec en changeant le mode IPsec en AH ou ESP+Auth et en utilisant une fonction de hachage approuvée FIPS. SHA1 est accepté par la FIPS, mais SHA256 est fortement recommandé.
- Configurez une durée de vie IPSec et une durée de vie maximale de huit heures maximum (28 800 secondes).

Configuration d'un tunnel IPSec

Au niveau du client, accédez à **Configuration** > **Canaux de distribution** > **Définitions des services**. Vous pouvez également accéder à la page **des services IPsec** depuis **Configuration > Sécurité**.

Dans la section **IPsec et GRE** > **Services IPsec**, cliquez sur **Ajouter**. La page **Modifier le service IPSec** s'affiche.



1. Spécifiez les détails du service.
    - **Nom du service** : nom du service IPsec.
    - **Type de service** : Sélectionnez le service utilisé par le tunnel IPsec.
    - **Domaine de routage** : pour les tunnels IPsec via LAN, sélectionnez un domaine de routage. Si le tunnel IPsec utilise un service intranet, le service intranet détermine le domaine de routage.
    - **Zone de pare-feu** : zone de pare-feu pour le tunnel. Par défaut, le tunnel est placé dans Default_LAN_Zone.
    - **Activer l'ECMP** : lorsque la case **Activer l'ECMP** est cochée, l'équilibrage de charge ECMP est activé pour le tunnel IPSec.
    - **Type ECMP** : Sélectionnez le type de mécanisme d'équilibrage de charge ECMP selon les besoins. Pour plus de détails sur les types d'ECMP, consultez la section Équilibrage de charge ECMP.

2. Ajoutez le point de terminaison du tunnel.

    - **Nom** : Lorsque le **type de service** est Intranet, choisissez un service intranet que le tunnel protège. Sinon, entrez un nom pour le service.
    - **IP homologue** : adresse IP de l'homologue distant.
    - Profil**IPsec : profil**de sécurité IPsec qui définit le protocole de sécurité et les paramètres IPsec.
    - Clé**pré-partagée : clé**pré-partagée utilisée pour l'authentification IKE.
    - **Clé pré-partagée homologue : clé**pré-partagée utilisée pour l'authentification IKEv2.
    - **Données d'identité** : données à utiliser comme identité locale, lors de l'utilisation d'une identité manuelle ou d'un type de nom de domaine complet utilisateur.
    - **Données d'identité homologue** : données à utiliser comme identité homologue, lors de l'utilisation d'identité manuelle ou de type FQDN utilisateur.
    - **Certificat** : Si vous choisissez Certificat comme authentification IKE, faites votre choix parmi les certificats configurés.

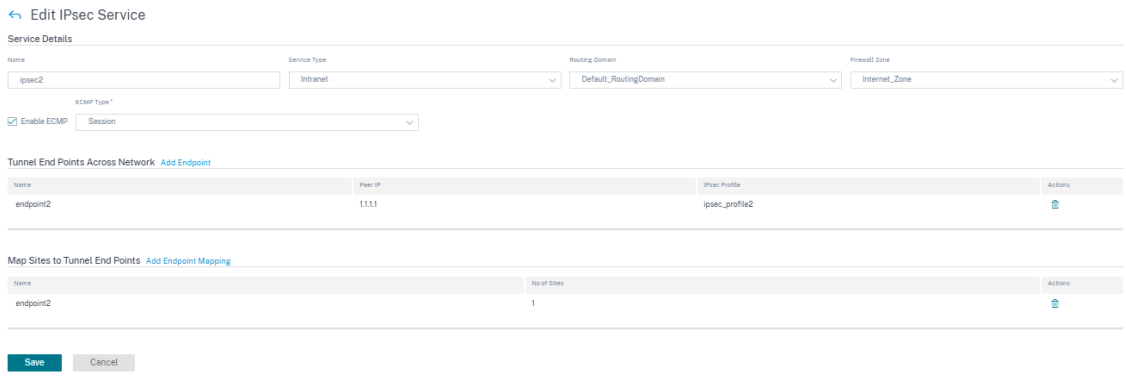
3. Mapper les sites aux points d'extrémité du tunnel.

    - **Choisissez Endpoint** : point de terminaison à mapper sur un site.
    - **Nom du site** : site à mapper au point de terminaison.
    - **Nom de l'interface virtuelle** : Interface virtuelle sur le site à utiliser comme point de terminaison.
    - **IP locale** : adresse IP virtuelle locale à utiliser comme point de terminaison du tunnel local.
    - **IP de la passerelle** : adresse IP du saut suivant.

4. Créez le réseau protégé.

    - **IP du réseau source/préfixe** : l'adresse IP source et le préfixe du trafic réseau que le tunnel IPsec protège.
    - **IP/préfixe du réseau**de destination : adresse IP de destination et préfixe du trafic réseau que le tunnel IPsec protège.

5. Assurez-vous que les configurations IPSec sont mises en miroir sur l'appliance homologue.



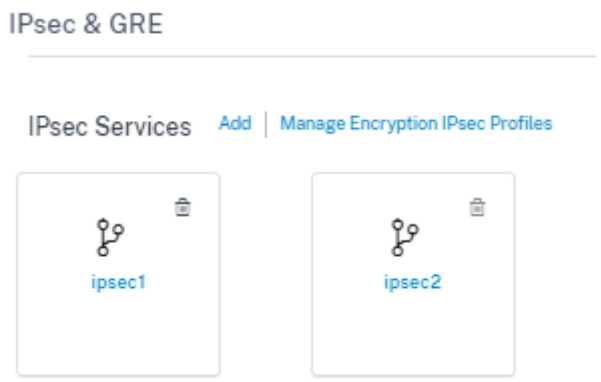
Pour plus d'informations sur la conformité à la norme FIPS, voir Sécurité du réseau.

> **Remarque**
>
> Citrix SD-WAN Orchestrator pour locaux prend en charge la connectivité à Oracle Cloud Infrastructure (OCI) via IPsec.

Profils de chiffrement IPsec

Pour ajouter un profil de chiffrement IPSec, au niveau du client, accédez à **Configuration** > **Canaux de distribution** > **Définitions des services**. Vous pouvez également accéder à la page de configuration **des profils de chiffrement IPSec** depuis **Configuration > Sécurité**.

Dans la section **IPsec et GRE**, sélectionnez **Gérer les profils IPsec de chiffrement**.



IPsec fournit des tunnels sécurisés. Citrix SD-WAN prend en charge les chemins virtuels IPSec, permettant aux périphériques tiers de mettre fin aux tunnels VPN IPsec du côté LAN ou WAN d'une appliance Citrix SD-WAN. Vous pouvez sécuriser les tunnels IPSec de site à site se terminant sur une appliance SD-WAN à l'aide d'un binaire cryptographique IPsec certifié FIPS 140-2 Niveau 1.

Citrix SD-WAN prend également en charge le tunnel IPsec résilient à l'aide d'un mécanisme de tunnel de chemin virtuel différencié.

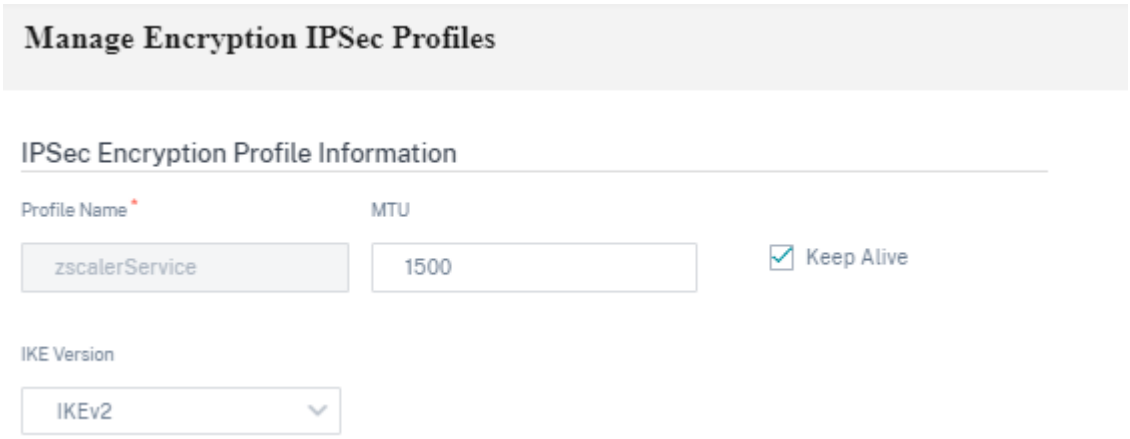
Les profils IPSec sont utilisés lors de la configuration des services IPSec en tant qu'ensembles de services de livraison. Sur la page du profil de sécurité IPsec, entrez les valeurs requises pour le **profil de chiffrement IPSec, les paramètres IKE** et les **paramètres IPsec**suivants.

Cliquez sur **Vérifier la configuration** pour valider toute erreur d'audit.

Informations sur le profil de chiffrement IPSec :

- **Nom du profil** : Entrez un nom de profil.
- **MTU** : Entrez la taille maximale des paquets IKE ou IPSec en octets.
- **Keep Alive** : cochez la case pour maintenir le tunnel actif et activer l'éligibilité des itinéraires.

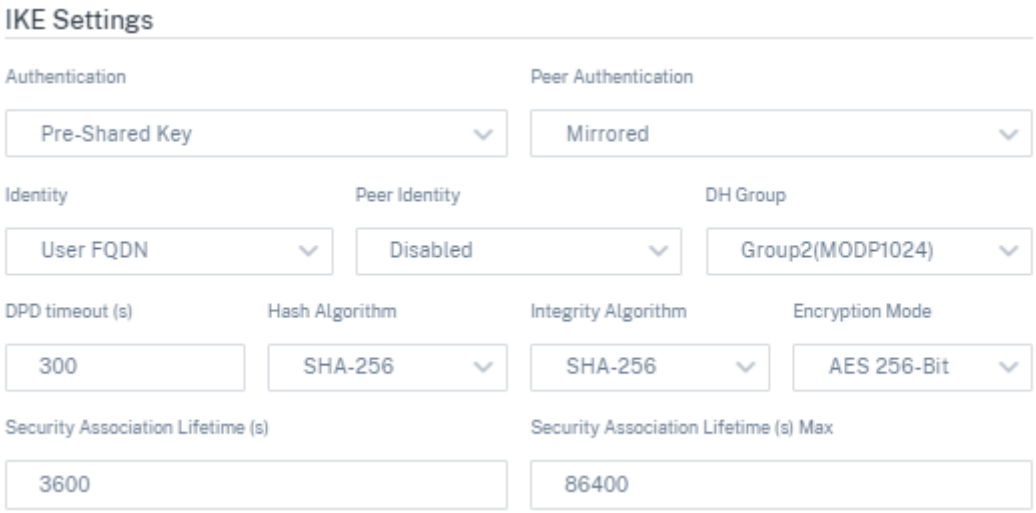
- **Version IKE** : Sélectionnez une version du protocole IKE dans la liste déroulante.



Paramètres IKE

- **Mode** : sélectionnez le mode principal ou le mode agressif dans la liste déroulante du mode de négociation IKE Phase 1.
  - **Main** : Aucune information n'est exposée aux attaquants potentiels pendant la négociation, mais elle est plus lente que le mode agressif. **Le mode principal** est conforme à la norme FIPS.
  - **Agressive** : Certaines informations (par exemple, l'identité des pairs qui négocient) sont exposées aux attaquants potentiels pendant la négociation, mais sont plus rapides que le mode principal. Le mode**agressif** n'est pas conforme à la norme FIPS.
- **Authentification** : Choisissez le type d'authentification comme certificat ou clé pré-partagée dans le menu déroulant.
- **Authentification par**les pairs : choisissez le type d'authentification par les pairs dans la liste déroulante.
- **Identité** : sélectionnez la méthode d'identité dans la liste déroulante.
- **Identité homologue** : sélectionnez la méthode d'identité homologue dans la liste déroulante.
- **Groupe DH** : sélectionnez le groupe Diffie-Hellman (DH) disponible pour la génération de clés IKE.
- **Délai (s) d'expiration du DPD** : Entrez le délai d'expiration de la détection des pairs morts (en secondes) pour les connexions VPN.
- **Algorithme de hachage** : choisissez un algorithme de hachage dans la liste déroulante pour authentifier les messages IKE.
- **Algorithme d'intégrité** : Choisissez l'algorithme de hachage IKEv2 à utiliser pour la vérification HMAC.
- **Mode de cryptage** : choisissez le mode de cryptage pour les messages IKE dans la liste déroulante.

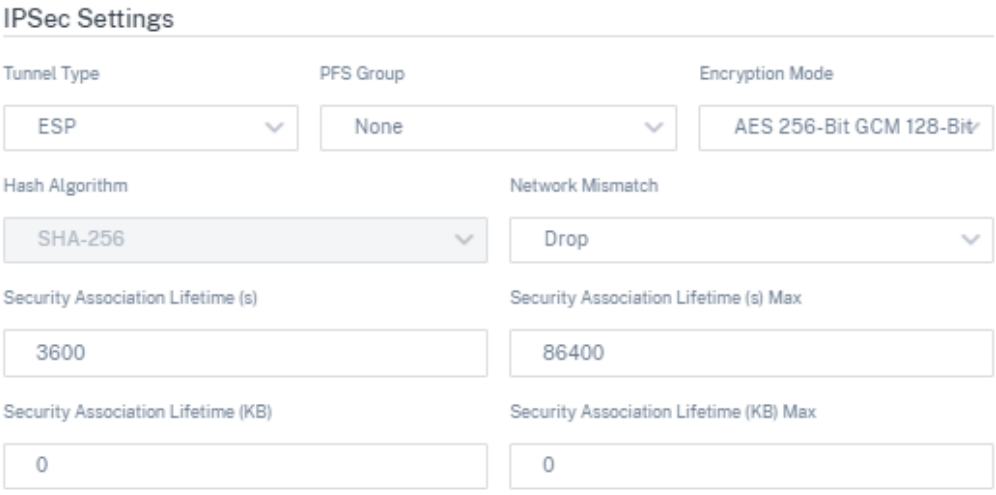
- **Durée (s) de vie des associations de sécurité** : Entrez la durée, en secondes, pendant laquelle une association de sécurité IKE doit exister.
- Durée (s)**maximale (s) de vie des associations de sécurité** : Entrez la durée maximale, en secondes, pendant laquelle une association de sécurité IKE doit exister.



Paramètres IPsec

- **Type de tunnel** : choisissez **ESP**, **ESP+Auth**, **ESP+NULL**ou **AH** comme type d'encapsulation du tunnel dans la liste déroulante. Celles-ci sont regroupées dans des catégories conformes à la norme FIPS et non conformes au FIPS.
  - **ESP** : chiffre uniquement les données utilisateur
  - **ESP+Auth** : crypte les données utilisateur et inclut un HMAC
  - **ESP+NULL** : Les paquets sont authentifiés mais non cryptés
  - **AH** : Comprend uniquement un HMAC
- **Groupe PFS** : choisissez le groupe Diffie-Hellman à utiliser pour une génération de clés de confidentialité directe parfaite dans le menu déroulant.
- **Mode de cryptage** : choisissez le mode de cryptage pour les messages IPsec dans le menu déroulant.
- **Algorithme de hachage : Les algorithmes**de hachage MD5, SHA1 et SHA-256 sont disponibles pour la vérification HMAC.
- **Incompatibilité réseau** : choisissez une action à effectuer si un paquet ne correspond pas aux réseaux protégés du tunnel IPSec dans le menu déroulant.
- **Durée (s) de vie des associations de sécurité** : Entrez la durée (en secondes) d'existence d'une association de sécurité IPsec.

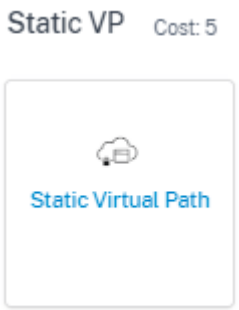
- Durée (s)**maximale (s) de vie des associations de sécurité** : Entrez la durée maximale (en secondes) pendant laquelle une association de sécurité IPsec doit exister.
- Durée de**vie de l'association de sécurité (Ko)** : entrez la quantité de données (en kilo-octets) nécessaire à l'existence d'une association de sécurité IPsec.
- Durée de**vie maximale de l'association de sécurité (Ko)** : Entrez la quantité maximale de données (en kilo-octets) pour autoriser l'existence d'une association de sécurité IPsec.



Chemin virtuel statique

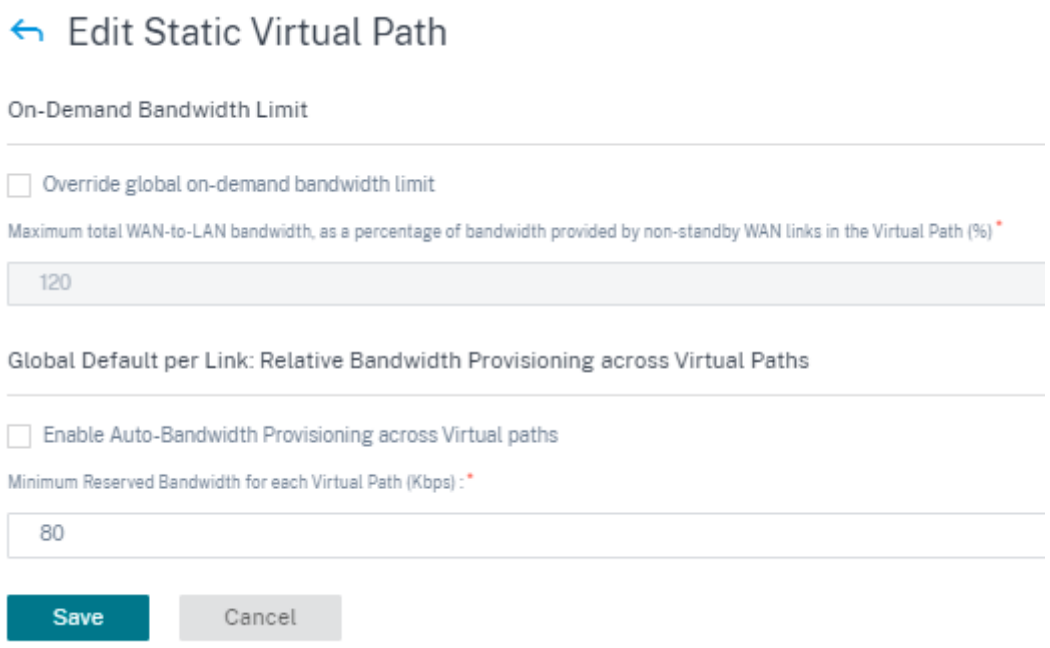
Les paramètres de chemin virtuel sont hérités des paramètres de chemin automatique de liaison WAN global. Vous pouvez remplacer ces configurations et ajouter ou supprimer le chemin d'accès du membre. Vous pouvez également filtrer les chemins virtuels en fonction du site et du profil QoS appliqué. Spécifiez une adresse IP de suivi pour la liaison WAN qui peut être pingée pour déterminer l'état de la liaison WAN. Vous pouvez également spécifier une adresse IP de suivi inverse pour le chemin inverse qui peut être pingé pour déterminer l'état du chemin inverse.

Pour configurer des chemins virtuels statiques, au niveau du client, accédez à **Configuration** > **Canaux de distribution**, puis cliquez sur la vignette **Chemin virtuel statique** .



Voici quelques-uns des paramètres pris en charge :

- **Liste de bande passante sur demande** :
  - Annuler la**limite globale de bande passante à la demande** : lorsque cette option est activée, les valeurs limites de bande passante globales sont remplacées par des valeurs spécifiques au site.
  - **Bande passante WAN-LAN totale maximale, en pourcentage de la bande passante fournie par les liaisons WAN non en veille dans le chemin virtuel (%)** : mettez à jour la limite de bande passante maximale, en %.
- **Valeur par défaut globale par lien : Provisioning de bande passante relative sur des chemins virtuels** :
  - **Activer le Provisioning automatique de la bande passante sur les chemins virtuels** : lorsque cette option est activée, la bande passante de tous les services est automatiquement calculée et appliquée en fonction de l'ampleur de la bande passante consommée par les sites distants.
  - **Bande passante réservée minimale pour chaque chemin virtuel (Kbits/s)** : bande passante maximale à réserver exclusivement pour chaque service sur chaque liaison WAN.

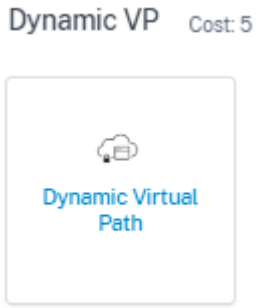


Paramètres du chemin virtuel dynamique

Les paramètres de chemin virtuel dynamique global permettent aux administrateurs de configurer les valeurs par défaut des chemins virtuels dynamiques sur l'ensemble du réseau.

Un chemin virtuel dynamique est instancié dynamiquement entre deux sites pour permettre une communication directe, sans sauts de noeuds SD-WAN intermédiaires. De même, la connexion de chemin virtuel dynamique est également supprimée dynamiquement. La création et la suppression de chemins virtuels dynamiques sont déclenchées en fonction des seuils de bande passante et des paramètres de temps.

Pour configurer des chemins virtuels dynamiques, au niveau du client, accédez à **Configuration** > **Canaux de distribution** > **Définitions de services**, puis cliquez sur la vignette **Chemin virtuel dynamique** .



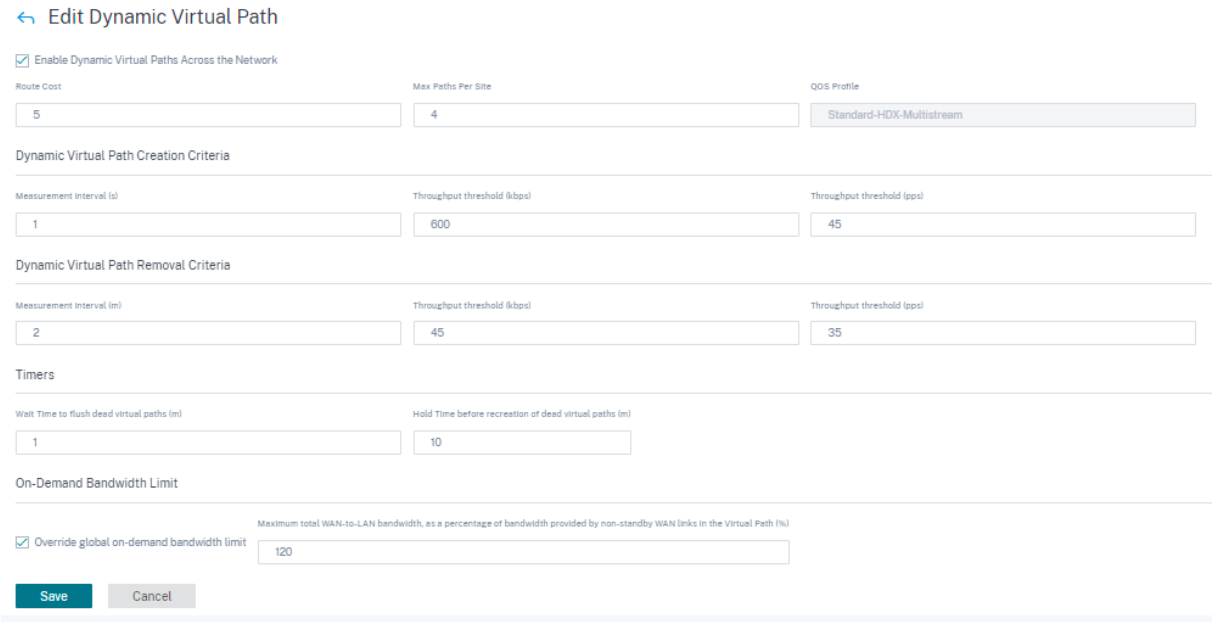
Voici quelques-uns des paramètres pris en charge :

- Provisionnement pour activer ou désactiver les chemins virtuels dynamiques sur le réseau
- Le coût de l'itinéraire pour les chemins virtuels dynamiques
- Le profil QoS à utiliser —**Standard** par défaut.
- Critères de création de chemins virtuels dynamiques :
  - **Intervalle de mesure (secondes)** : durée pendant laquelle le nombre de paquets et la bande passante sont mesurés afin de déterminer si le chemin virtuel dynamique doit être créé entre deux sites, dans ce cas, entre une branche donnée et le nœud de contrôle.
  - **Seuil de débit (kbps)** : seuil de débit total entre deux sites, mesuré sur l'**intervalle de mesure**, auquel le chemin virtuel dynamique est déclenché. Dans ce cas, le seuil s'applique au nœud de contrôle.
  - **Seuil de débit (pps)** : seuil de débit total entre deux sites, mesuré sur l'**intervalle de mesure**, auquel le chemin virtuel dynamique est déclenché.
- Critères de suppression de chemin virtuel dynamique :
  - **Intervalle de mesure (minutes)** : durée pendant laquelle le nombre de paquets et la bande passante sont mesurés afin de déterminer si un chemin virtuel dynamique doit être supprimé entre deux sites, dans ce cas, entre une branche donnée et le nœud de contrôle.
  - **Seuil de débit (kbps)** : seuil de débit total entre deux sites, mesuré sur l'**intervalle de mesure**, auquel le chemin virtuel dynamique est supprimé.

  - **Seuil de débit (pps)** : seuil de débit total entre deux sites, mesuré sur l'**intervalle de mesure**, auquel le chemin virtuel dynamique est supprimé.

- Minuteries
  - **Temps d'attente pour vider les chemins virtuels morts (m)** : temps après lequel un chemin virtuel dynamique mort est supprimé.
  - **Temps de maintien avant la recréation de chemins virtuels morts (m)** : temps après lequel un chemin virtuel dynamique supprimé parce qu'il était MORT peut être recréé.

- Liste de bande passante à
  - Annuler la**limite globale de bande passante à la demande** : lorsque cette option est activée, les valeurs limites de bande passante globales sont remplacées par des valeurs spécifiques au site.
  - **Bande passante WAN-LAN totale maximale, en pourcentage de la bande passante fournie par les liaisons WAN non en veille dans le chemin virtuel (%)** : mettez à jour la limite de bande passante maximale, en %.



Cliquez sur **Vérifier la configuration** pour valider toute erreur d'audit.

Routage

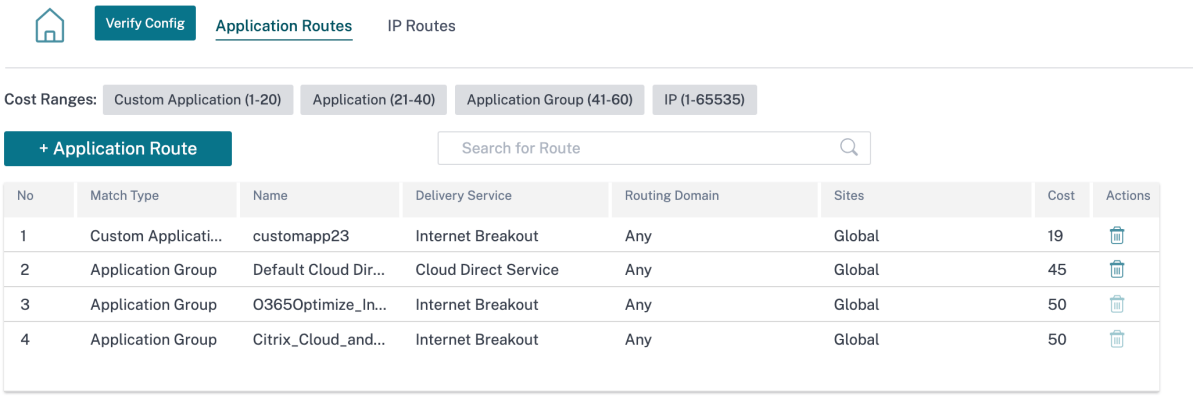
October 21, 2022

La section **Routage** propose les options suivantes :

- Règles de routage
- Récapitulatif des itinéraires
- Domaines de routage
- Importer des profils d'itinéraire
- Exporter les profils d'itinéraire
- nœuds de transit

Règles de routage

Les stratégies de routage aident à activer la direction du trafic. En fonction de la sélection (Itinéraires d'application et routes IP), vous pouvez utiliser différentes façons de diriger le trafic.

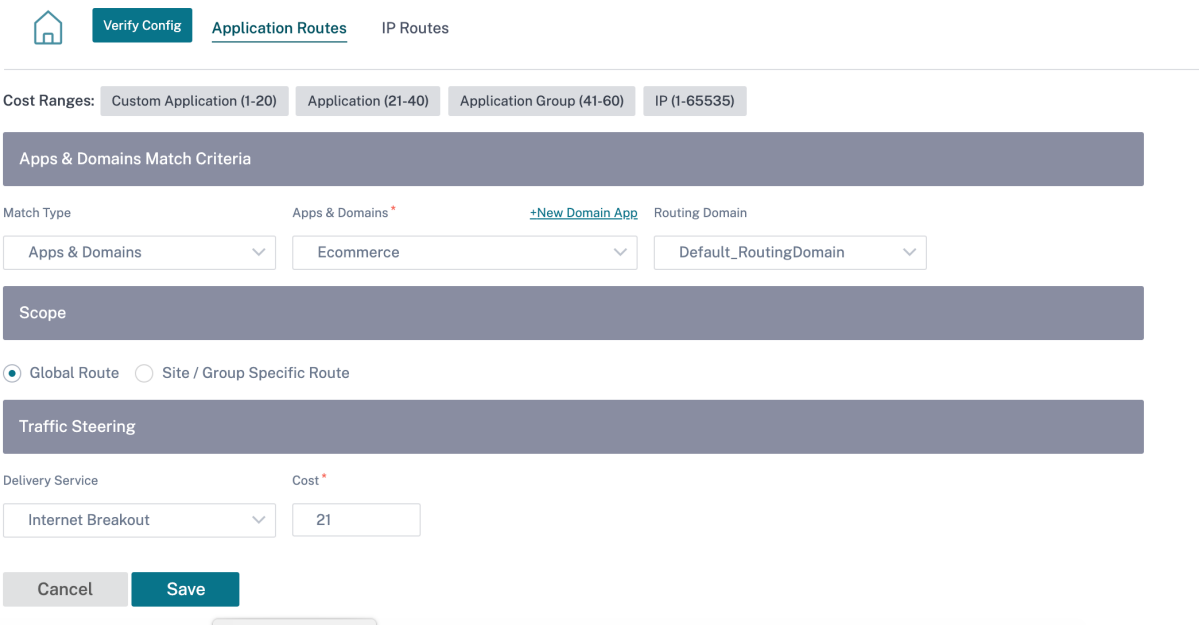


Itinéraires d'application

Cliquez sur **+ Route de l'application** pour créer un itinéraire d'application.

- **Critères de correspondance des applications personnalisés** :
  - **Type de correspondance** : Sélectionnez le type de correspondance **Application/Application personnalisée/Groupe** d'applications dans la liste déroulante.
  - **Application** : Choisissez une application dans la liste.
  - **Domaine de routage** : sélectionnez un domaine de routage.
- **Champ d'**application : Vous pouvez définir la portée de l'application au niveau global ou au niveau spécifique du site et du groupe.
- **Pilotage du trafic** ;
  - **Service de livraison** : Choisissez un service de livraison dans la liste.
  - **Coût** : reflète la priorité relative de chaque itinéraire. Réduisez le coût, plus la priorité est élevée.

- **Éligibilité basée sur le parcours** :
  - **Ajouter un chemin** : choisissez un site et des liens WAN. Si le chemin choisi descend, la route de l'application ne reçoit aucun trafic.

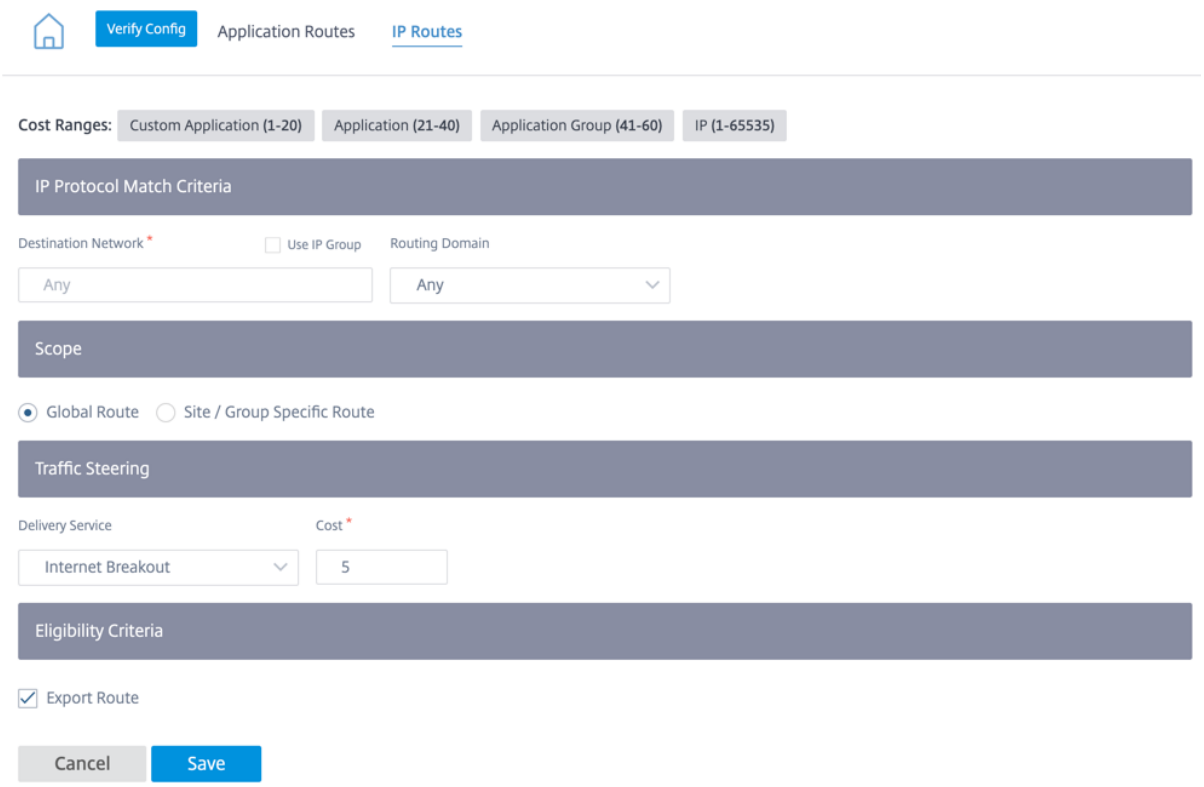


Si une nouvelle route d'application est ajoutée, le coût de l'itinéraire doit se situer dans la plage suivante :

- **Application personnalisée** : 1 à 20
- Nombre de**demandes** : 21 à 40
- **Groupe d'applications** : 41—60

Routes IP

Accédez à l'onglet **Routes IP** et cliquez sur **+** Politique d'itinéraire IP vers IP pour orienter le trafic.



- **Critères de correspondance du protocole IP** :
  - **Réseau de destination** : Ajoutez le réseau de destination qui permet de transférer les paquets.
  - **Utiliser un groupe IP** : vous pouvez ajouter un réseau de destination ou activer la case à cocher **Utiliser un groupe IP** pour sélectionner n'importe quel groupe IP dans la liste déroulante.
  - **Domaine de routage** : sélectionnez un domaine de routage dans la liste déroulante.
- **Étendue** : Vous pouvez définir le périmètre de la route IP au niveau global ou au niveau spécifique du site et du groupe.
- **Pilotage du trafic** :
  - **Service de livraison** : Choisissez un service de livraison dans la liste déroulante.
  - **Coût** : reflète la priorité relative de chaque itinéraire. Réduisez le coût, plus la priorité est élevée.

  Si une nouvelle route IP est ajoutée, le coût de l'itinéraire doit être compris entre 1 et 20.
- **Critères d'éligibilité** :
  - **Exporter l'itinéraire** : si la case **Exporter** l'itinéraire est cochée et si l'itinéraire est un itinéraire local, l'itinéraire peut être exporté par défaut. Si l'itinéraire est un itinéraire basé

sur INTRANET/INTERNET, alors pour que l'exportation fonctionne, le transfert WAN vers WAN doit être activé. Si la case **Exporter l'itinéraire** est décochée, l'itinéraire local ne peut pas être exporté vers un autre SD-WAN et a une importance locale.

- **Éligibilité basée sur le parcours** :
  - **Ajouter un chemin** : choisissez un site et des liens WAN. Si le chemin ajouté tombe en panne, la route IP ne reçoit aucun trafic.

Cliquez sur **Vérifier la configuration** pour valider toute erreur d'audit.

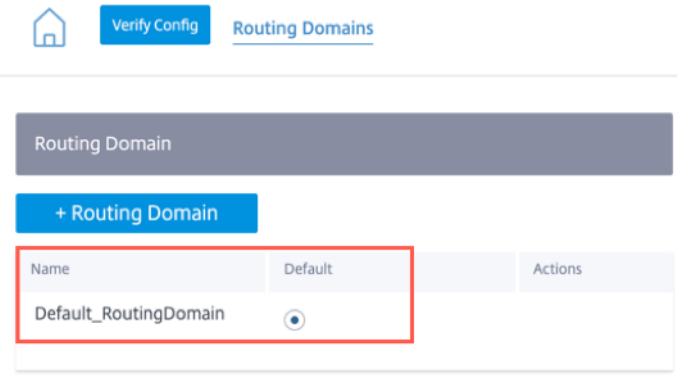
Récapitulatif des itinéraires

La synthèse des itinéraires réduit le nombre de routes qu'un routeur doit maintenir. Un itinéraire récapitulatif est un itinéraire unique qui est utilisé pour représenter plusieurs itinéraires. Il permet d'économiser la bande passante en envoyant une annonce de route unique, réduisant ainsi le nombre de liens entre les routeurs. Il économise de la mémoire car une seule adresse de route est conservée. Les ressources CPU sont utilisées plus efficacement en évitant les recherches récursives. Vous pouvez ajouter des itinéraires récapitulatifs sans spécifier l'adresse IP de la passerelle.

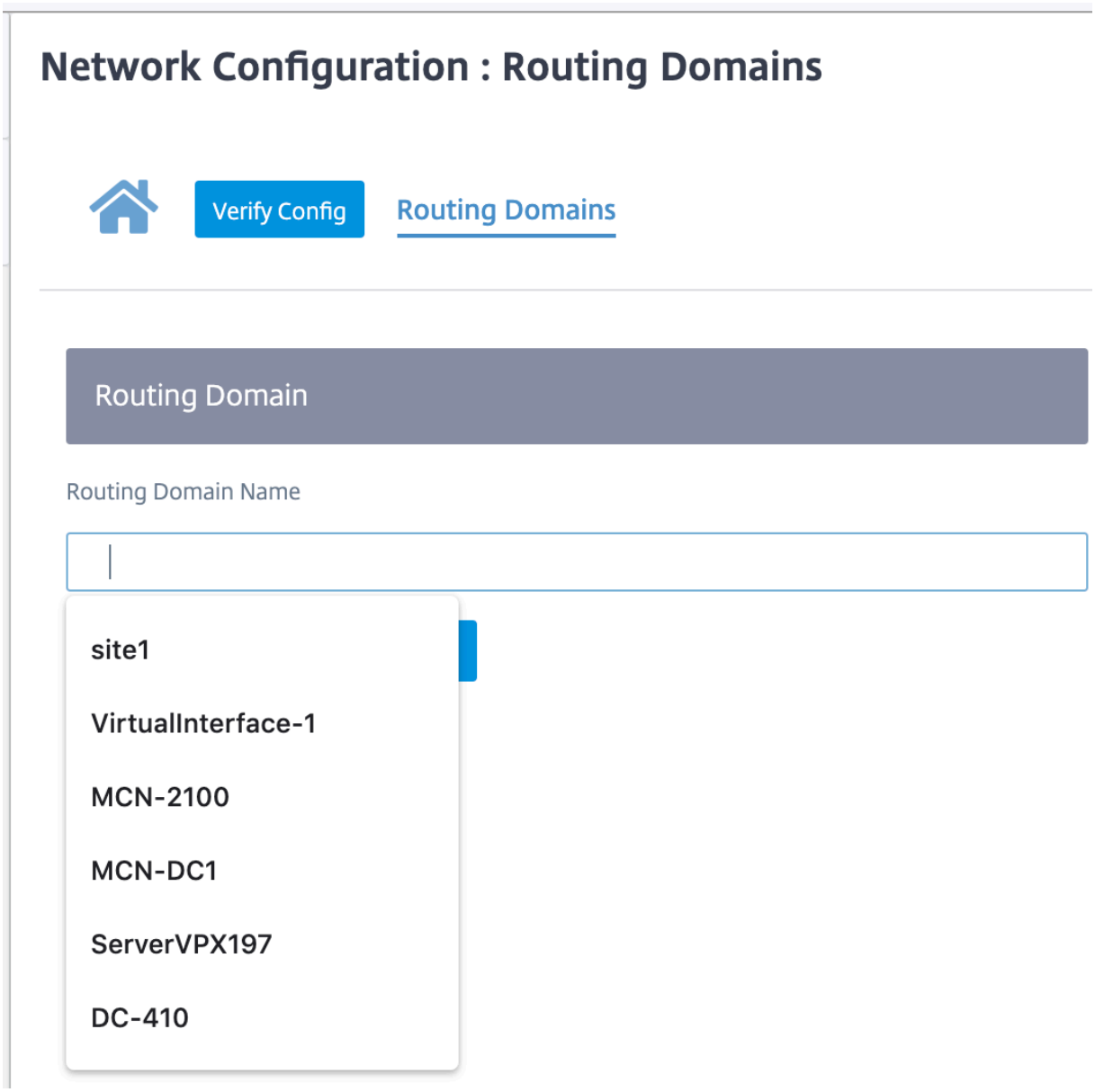
Domaine de routage

Les**domaines de routage** sont utilisés pour séparer le trafic via le VLAN. Une fois les domaines de routage créés, vous pouvez les référencer au niveau global (pour les services Intranet) ou au niveau de l'interface.

Vous pouvez également sélectionner le domaine de routage par défaut qui s'applique à tous les sites.



Pour faire correspondre les itinéraires d'un domaine de routage spécifique, cliquez sur **+ Domaine de routage** et choisissez l'un des domaines de routage configurés dans la liste déroulante. Cliquez sur **Enregistrer**.



Cliquez sur **Vérifier la configuration** pour valider toute erreur d'audit.

Pour plus d'informations, consultez la section Domaine de routage.

Service de domaine d'interroutage

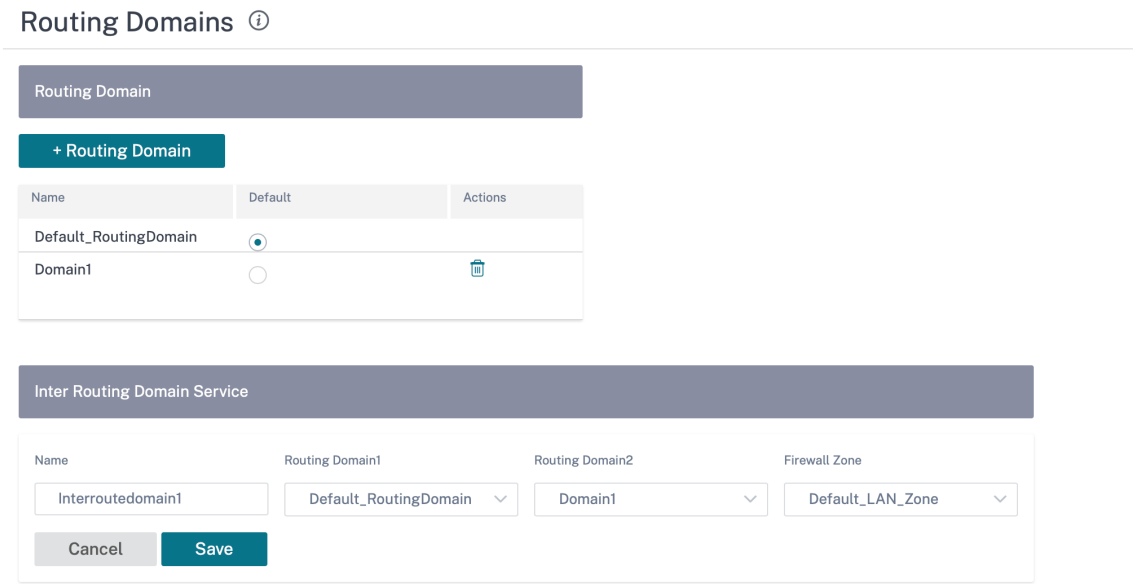
Citrix SD-WAN Orchestrator pour locaux fournit un service de domaine d'interroutage statique, permettant la fuite d'itinéraires entre les domaines de routage au sein d'un site ou entre différents sites. Cela élimine le besoin d'un routeur de bord pour gérer les fuites de route. Le service de routage inter-VRF peut également être utilisé pour configurer des routes, des stratégies de pare-feu et des règles NAT.

Pour plus d'informations, voir Service d'interroutage de domaines.

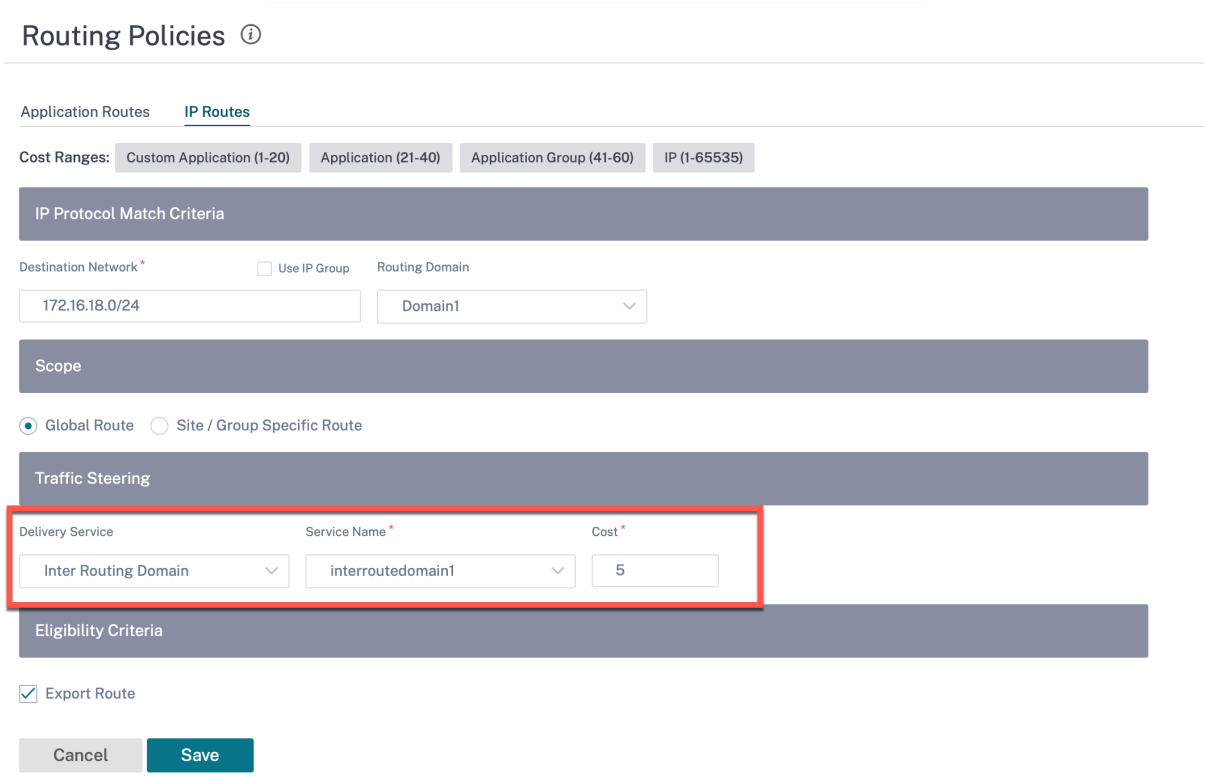
Pour configurer le service Inter-Routing Domain via Citrix SD-WAN Orchestrator pour locaux, procédez comme suit :

1. Au niveau du réseau, accédez à **Configuration** > **Routage** > Domaines de **routage > Service d'inter-domainesde routage**.
2. Cliquez sur **+ Domaine d'interroutage** et entrez des valeurs pour les paramètres suivants :

- **Nom** : Nom du service de domaine inter-routage.
- **Domaine de routage 1** : premier domaine de routage de la paire.
- **Domaine de routage 2** : deuxième domaine de routage de la paire.
- **Zone de pare-feu** : Zone de pare-feu du service.
  - **Par défaut** : La zone de pare-feu **Inter_Routing_Domain_Zone** est attribuée.
  - **Aucune** : Le service se comporte comme un conduit, qui n'a pas de zone et conserve la zone d'origine du paquet.
  - Toutes les zones configurées dans le réseau peuvent être sélectionnées.

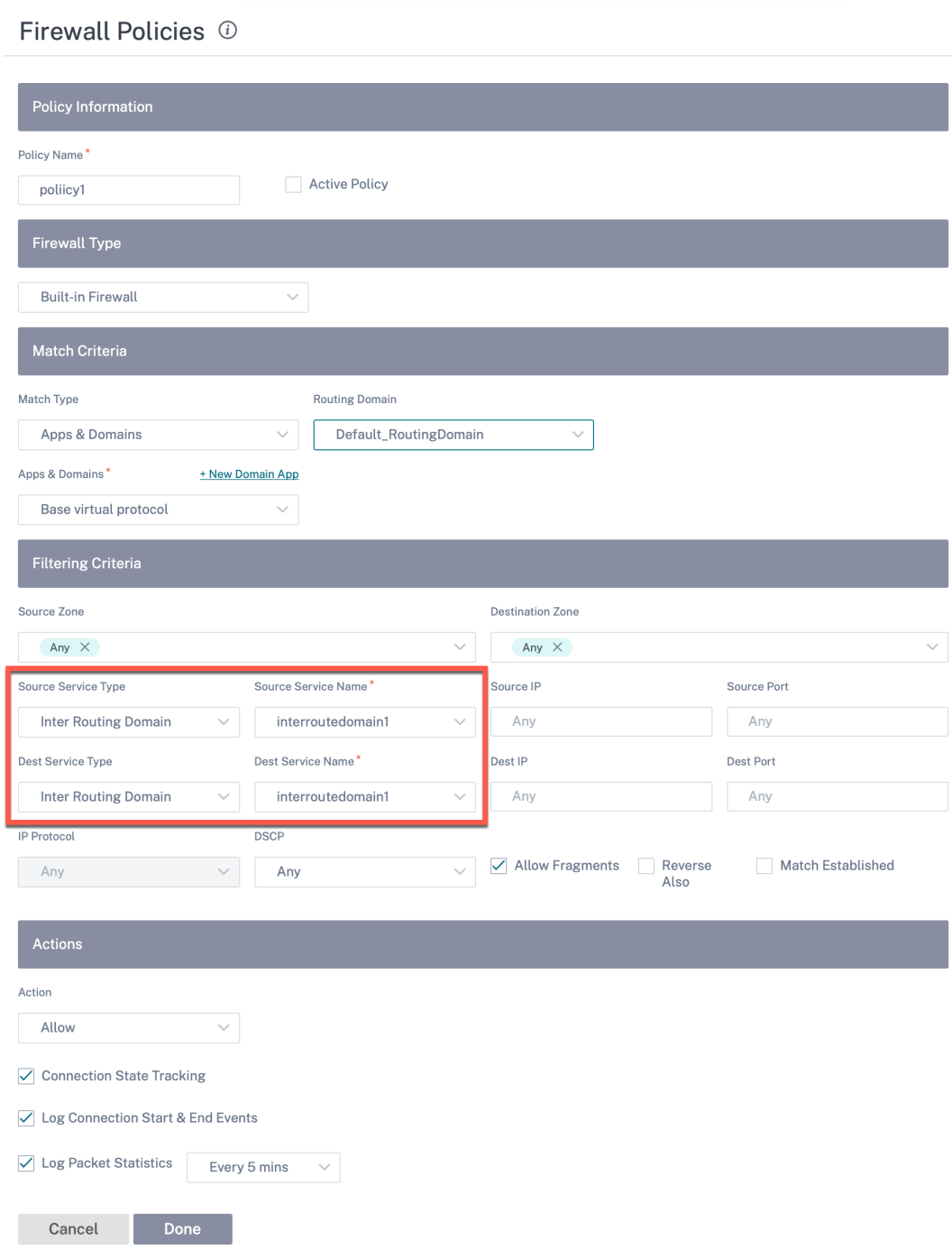


Pour créer des itinéraires à l'aide du service de domaine inter-routage, créez un itinéraire avec le type de service en tant que service de domaine inter-routage et sélectionnez le service de domaine inter-routage. Pour plus d'informations sur la configuration des itinéraires, consultez la section Politiques de routage.



Ajoutez également une route à partir de l'autre paire de domaines de routage, pour établir une connexion entre les deux domaines de routage.

Vous pouvez également configurer des stratégies de pare-feu pour contrôler le flux de trafic entre les domaines de routage. Dans les stratégies de pare-feu, sélectionnez Service de domaine Inter-routage pour les services source et de destination et sélectionnez l'action de pare-feu requise. Pour plus d'informations sur la configuration des politiques de pare-feu, voir Politiques de pare-feu.

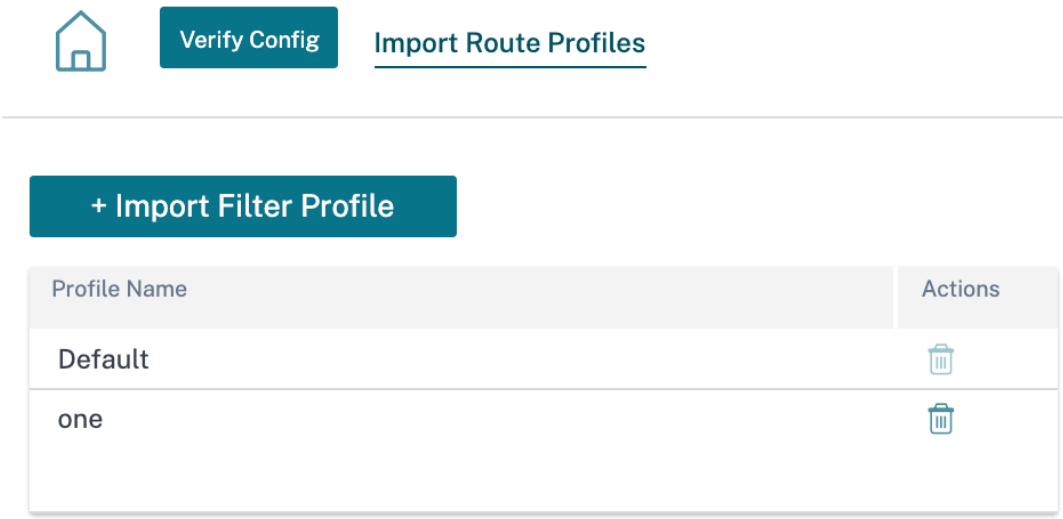


Vous pouvez également choisir le type de service Intranet pour configurer les stratégies NAT statiques et dynamiques. Pour plus d'informations sur la configuration des politiques NAT, voir Traduction d'adresses réseau.

Importer des profils d'itinéraire

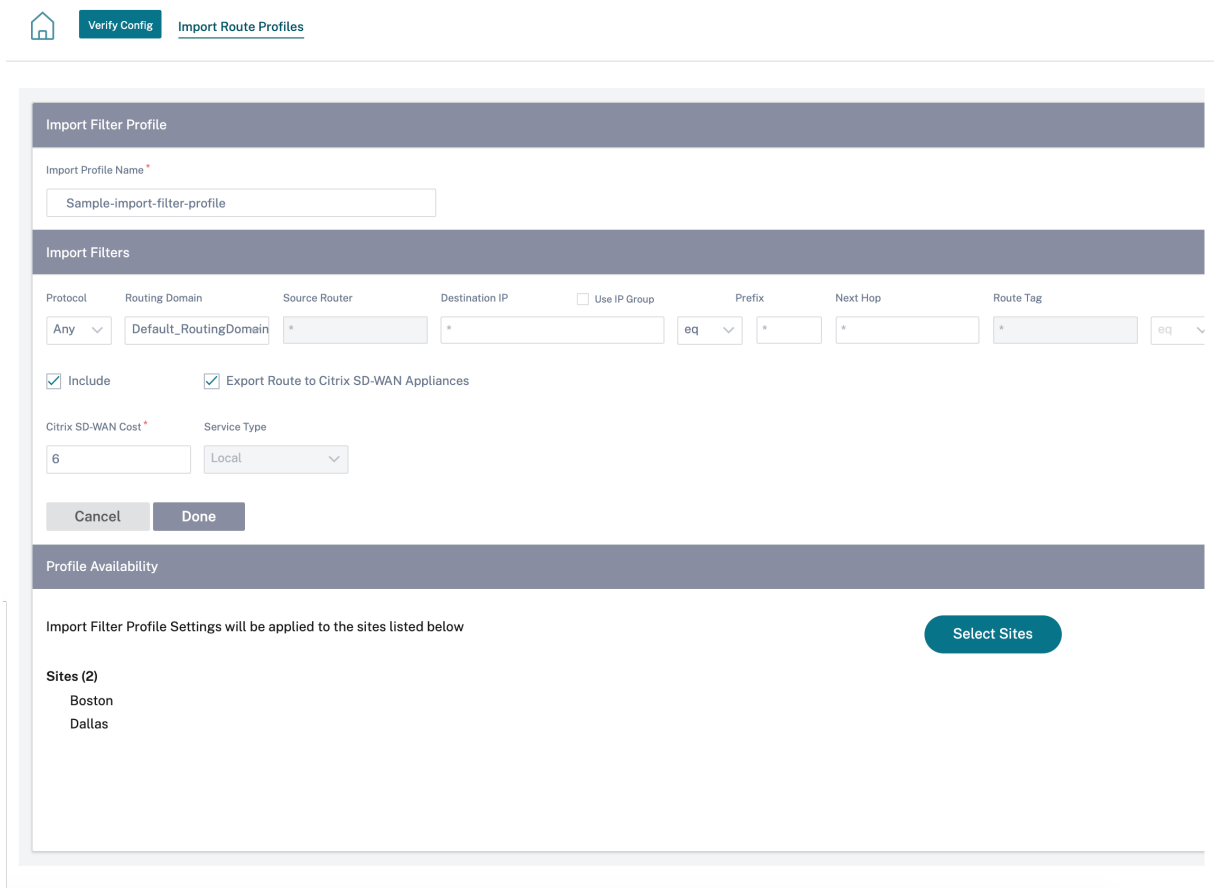
Vous pouvez configurer des filtres pour affiner la manière dont se déroule l'apprentissage par route.

Les règles de filtre d'importation sont des règles qui doivent être respectées avant d'importer des itinéraires dynamiques dans la base de données de routage SD-WAN. Par défaut, aucun itinéraire n'est importé.



Ajoutez un **profil de filtre d'importation** avec le **nom du profil d'importation, la disponibilité du profil** et **les filtres d'importation**, ainsi que les champs suivants :

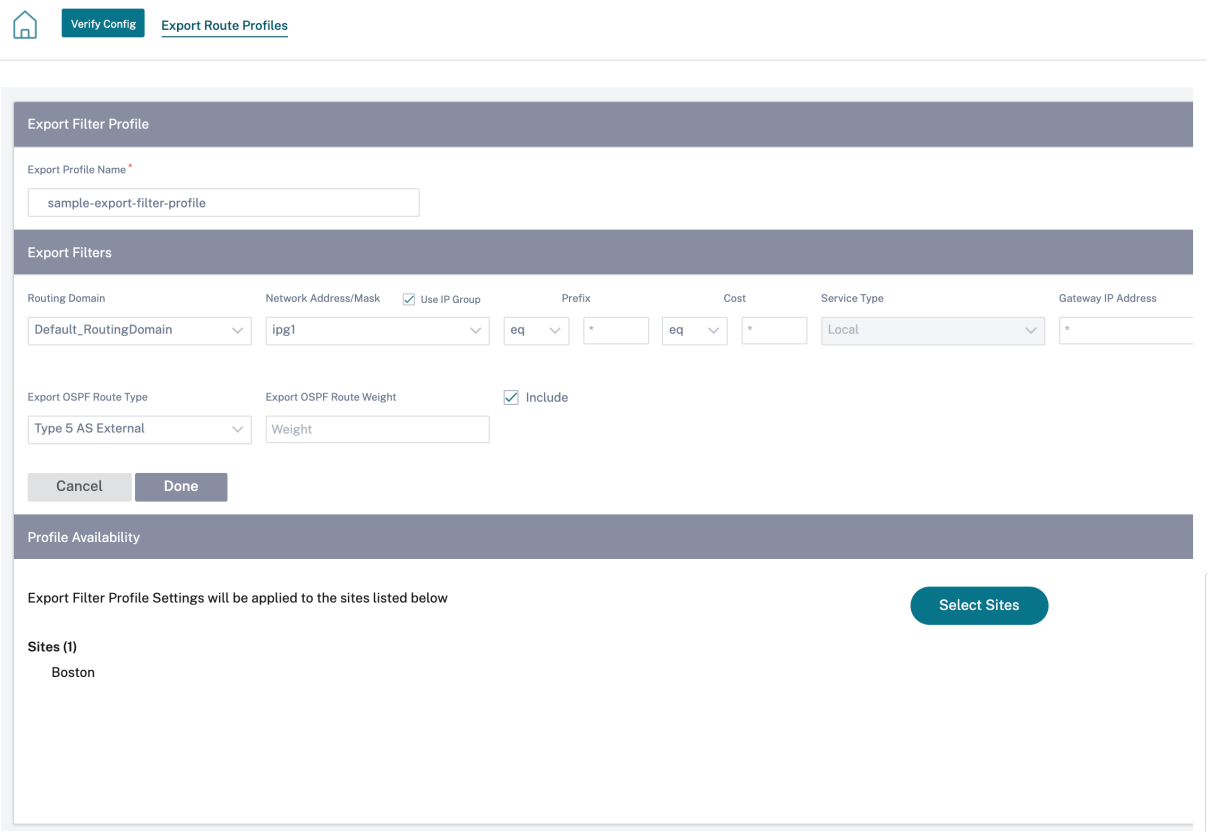
- **Protocole** : sélectionnez le protocole dans la liste.
- **Domaine de routage :** pour faire correspondre les itinéraires d'un domaine de routage spécifique, choisissez l'un des domaines de routage configurés dans la liste.
- **Routeur source** : entrez l'adresse IP et le masque de réseau de l'objet réseau configuré qui décrit le réseau de l'itinéraire.
- **IP de destination** : entrez l'adresse IP de destination.
- **Préfixe** : pour faire correspondre les itinéraires par préfixe, choisissez un prédicat de correspondance dans la liste et entrez un préfixe d'itinéraire dans le champ adjacent.
- **Saut suivant** : entrez la destination du saut suivant.
- **Tag d'itinéraire** : renseignez le tag d'itinéraire.
- **Coût** : méthode (prédicat) et coût d'itinéraire SD-WAN utilisés pour affiner la sélection des itinéraires exportés.



Cliquez sur **Vérifier la configuration** pour valider toute erreur d'audit.

Exporter des profils d'itinéraire

Définissez les règles à respecter lors de la publicité de routes SD-WAN via des protocoles de routage dynamiques. Par défaut, tous les itinéraires sont annoncés aux pairs.



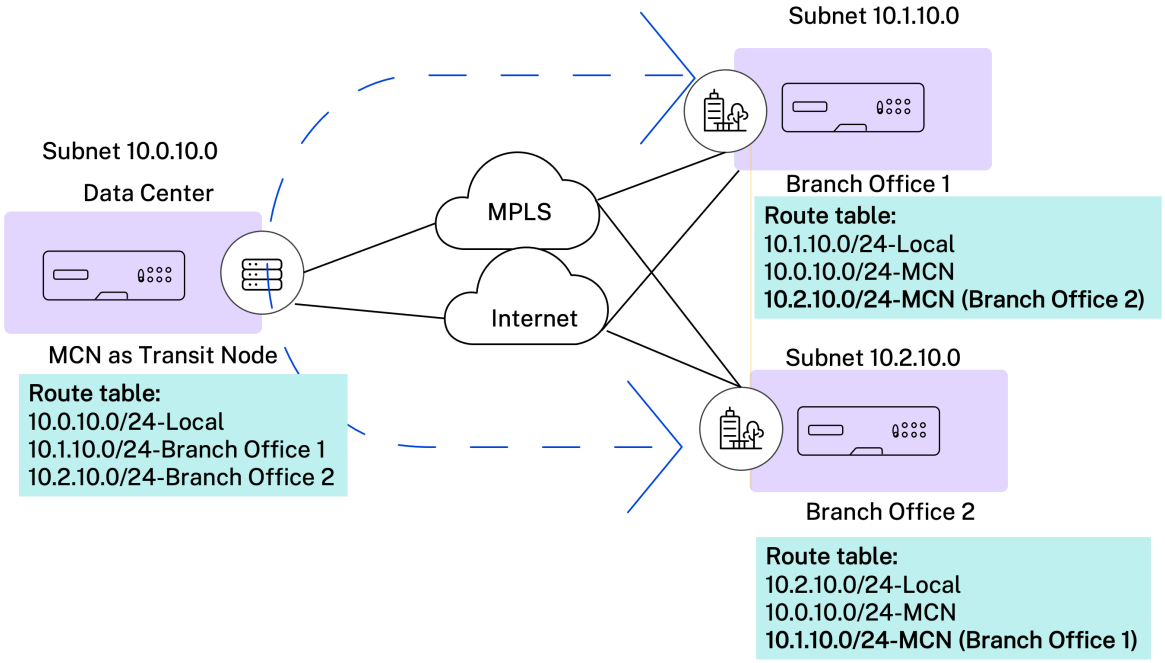
Cliquez sur **Vérifier la configuration** pour valider toute erreur d'audit.

nœuds de transit

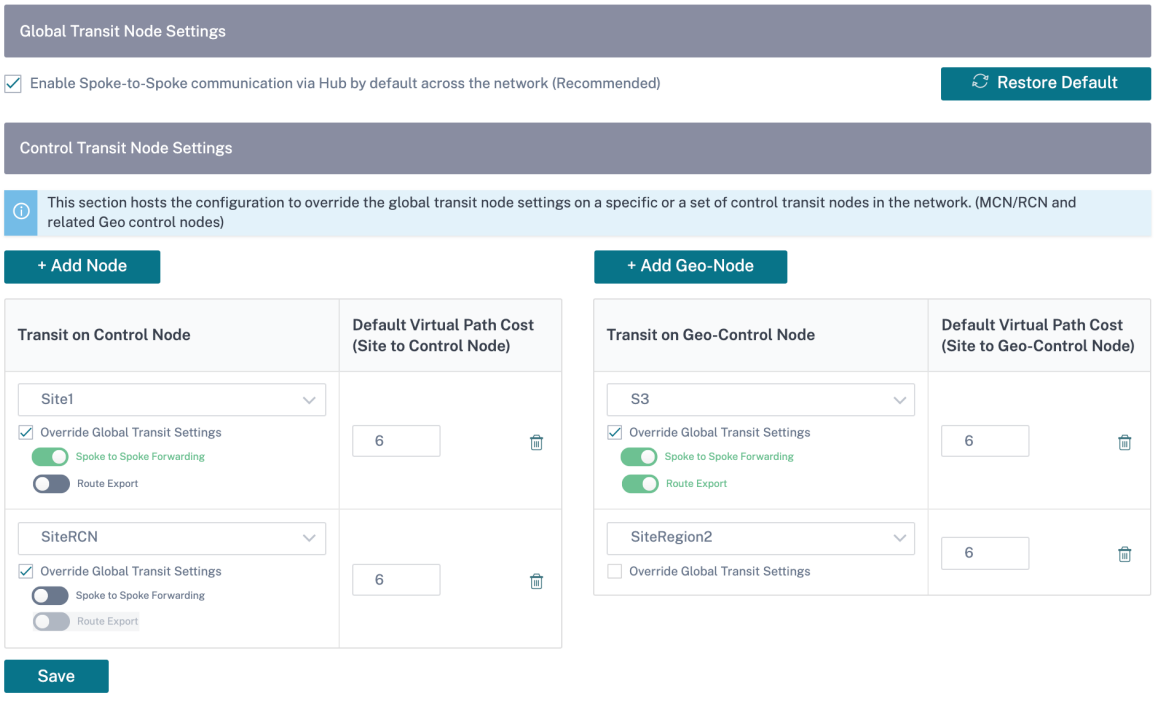
Nœud de transit de superposition virtuelle

Les nœuds de transit sont les sites capables de transférer le trafic entre une ou plusieurs succursales au sein d'une région.

Le trafic entre deux nœuds peut être influencé pour choisir un nœud de transit comme saut intermédiaire en ajustant le coût de l'itinéraire. Les nœuds de transit sont utilisés pour acheminer les données vers des nœuds non adjacents. Par exemple, si trois nœuds sont connectés dans la série A-B-C, les données de A à C peuvent être acheminées via B. Vous pouvez spécifier le nœud de transit et les sites à acheminer via le nœud de transit dans le service Citrix SD-WAN Orchestrator. Les chemins virtuels sont choisis dans l'ordre croissant du coût. Réduisez le coût, plus la priorité.



Nœuds de transit virtuels globaux par défaut Vous pouvez spécifier les nœuds de contrôle (MCN/RCN) et les nœuds de contrôle géographique (Geo-MCN/RCN) comme nœuds de transit par superposition virtuelle globale par défaut dans un réseau. L'activation de la communication en étoile via Hub dans le cadre des paramètres globaux permet à tous les sites d'utiliser les nœuds de contrôle configurés comme nœuds de transit, par défaut, pour la communication de site à site.



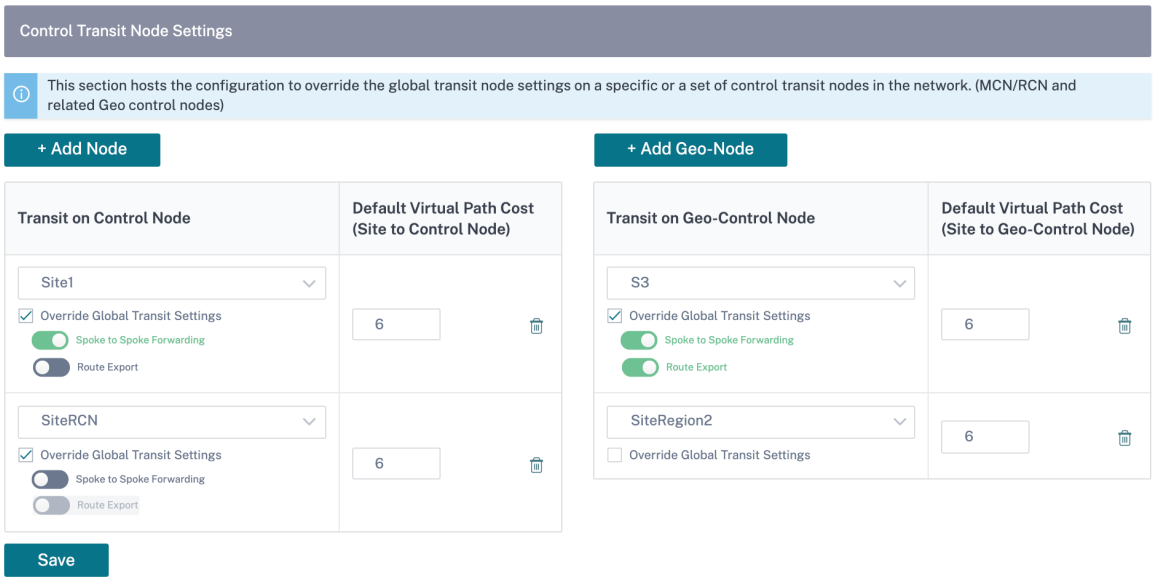
Ajoutez le nœud de contrôle et les nœuds de géo-contrôle que vous souhaitez utiliser comme nœuds de transit de superposition virtuels et spécifiez le coût du chemin virtuel. Les nœuds de contrôle et les nœuds de géo-contrôle ont 6 et 7 comme coûts de chemin virtuel par défaut respectifs. Vous pouvez choisir de modifier le coût du chemin virtuel en fonction de vos besoins réseau. Cliquez sur **Restaurer les paramètres par défaut** pour restaurer les coûts des chemins virtuels par défaut pour les nœuds de transit par défaut.

> **Remarque**
>
> Vous pouvez ajouter au maximum 3 nœuds de contrôle et 3 nœuds de géo-contrôle en tant que nœuds de transit.

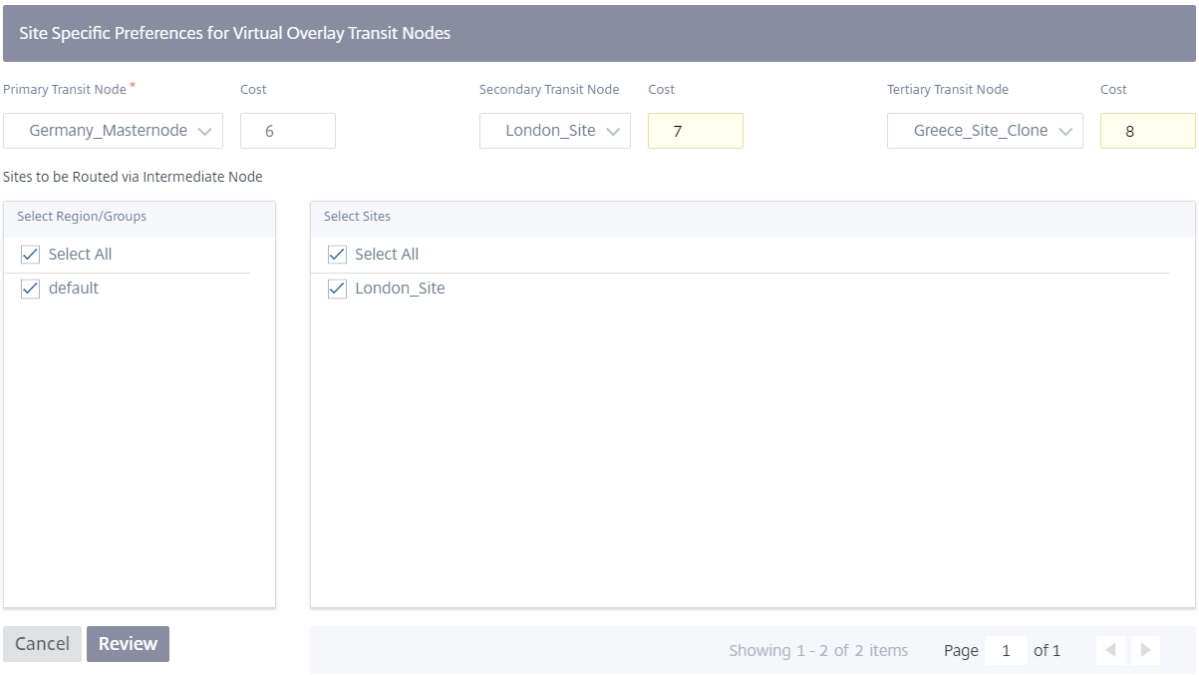
Par défaut, le transfert WAN vers WAN est activé sur tous les chemins associés aux nœuds de contrôle et de géo-contrôle sélectionnés. Le transfert Wan-WAN permet à un site d'agir comme un saut intermédiaire entre deux sites adjacents pour n'importe quel trafic de site à site, Internet ou intranet et d'agir comme médiateur pour les chemins virtuels dynamiques.

Vous pouvez annuler les paramètres du nœud de transit global et choisir d'activer ou de désactiver le transfert de point à point uniquement sur les nœuds de transit de contrôle sélectionnés. Lorsque le **transfert Spoke to Spoke** est activé, le nœud de contrôle de transit exporte les itinéraires sur les sites qui lui sont connectés. La communication de site à site et le chemin virtuel dynamique entre les sites connectés au nœud de transit sont seuls activés.

L'activation de **l'exportation d'itinéraires** permet le transfert de chemin virtuel vers un chemin virtuel et l'exportation d'itinéraires (transfert WAN vers WAN) sur tous les chemins de site. La désactivation du bouton active uniquement le transfert d'un chemin virtuel vers un chemin virtuel et désactive l'exportation d'itinéraires sur tous les chemins du site. L'exportation d'itinéraires ne peut être activée que lorsque le **transfert Spoke to Spoke** est activé.



Préférences spécifiques au site pour les nœuds de transit de superposition virtuelle Les préférences spécifiques au site pour les nœuds de transit de superposition virtuels vous permettent de remplacer les paramètres globaux des nœuds de transit virtuels de superposition pour tous les sites de votre réseau. Vous pouvez également choisir un nœud autre que le contrôle comme nœud de transit principal d'un site. Choisissez un nœud de contrôle ou un nœud de contrôle géo-contrôle comme nœuds de transit secondaire et tertiaire. Si le nœud de transit principal est en panne, les sites utilisent le nœud de transit secondaire. Si les nœuds de transit primaires et secondaires sont en panne, les sites utilisent le nœud de transit tertiaire. Spécifiez le coût des nœuds de transit et sélectionnez les sites auxquels les paramètres de nœud de transit virtuel de superposition spécifique au site sont appliqués.



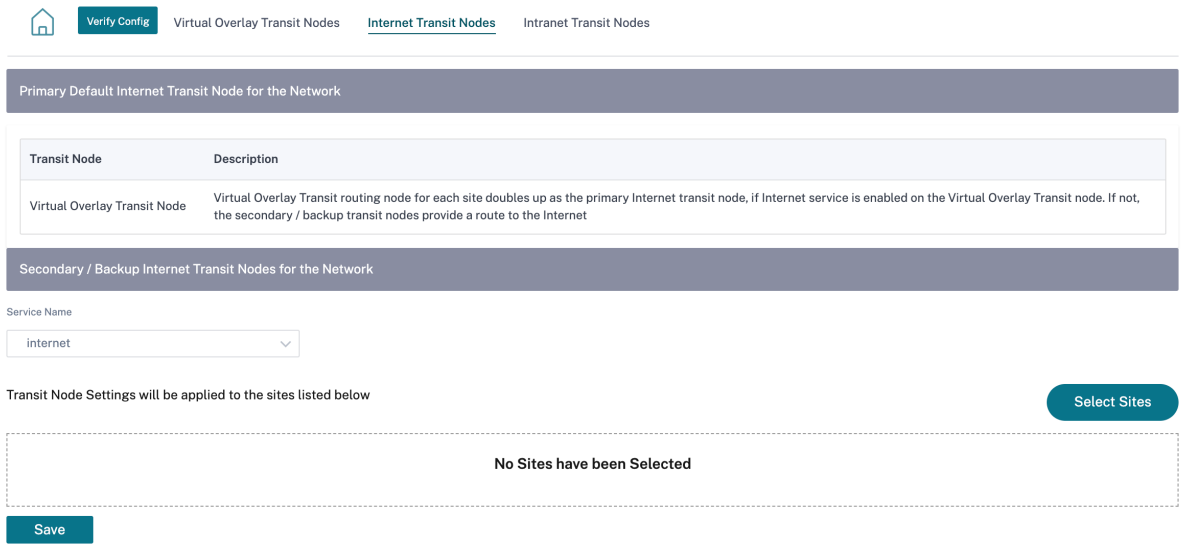
Nœud de transit Internet

Vous pouvez ajouter des sites en tant que sites de transit Internet pour permettre l'accès Internet aux sites. Les sites qui ont besoin d'une connexion Internet directe doivent avoir au moins un lien avec le service Internet activé. Cela signifie qu'au moins une liaison est définie sur un partage de bande passante non nul.

Un coût de trajet peut être attribué à chaque site de transit. Les sites dont le service Internet est disponible accèdent directement à Internet puisque l'itinéraire direct serait le chemin de routage le moins coûteux. Les sites sans service Internet peuvent acheminer vers Internet via les sites de transit configurés. Lorsque les sites de transit Internet sont configurés, les routes vers Internet via ces sites de transit sont automatiquement transmises à tous les sites. Les sites de transit Internet sont les sites dont le service Internet est activé.

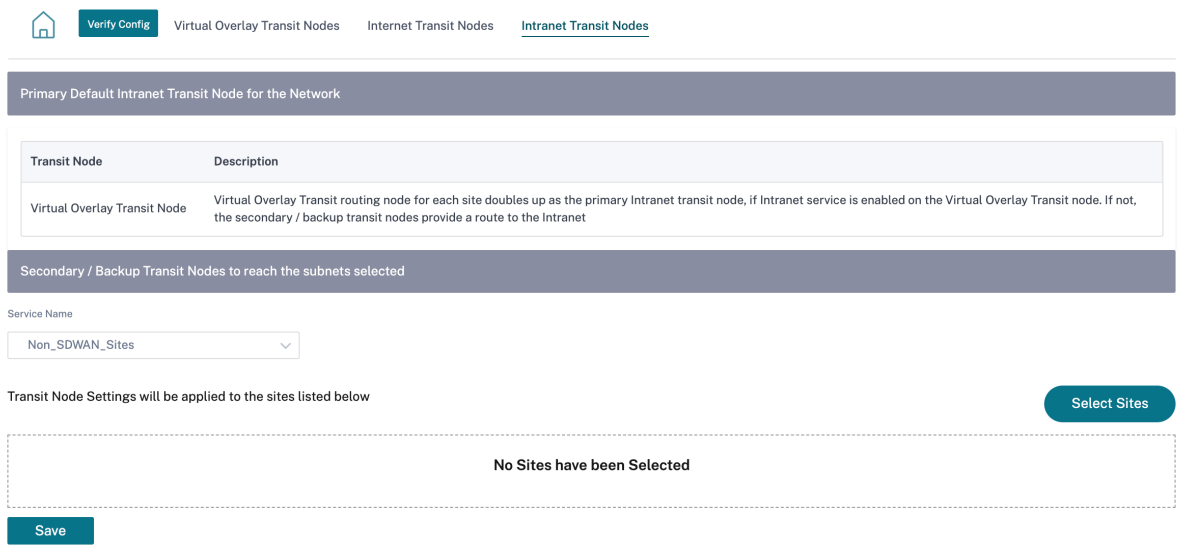
Par exemple, si San Francisco et New York sont configurés en tant que sites de transit Internet. Les itinéraires vers Internet via San Francisco et New York sont automatiquement poussés vers tous les sites.

Le nœud de transit virtuel superposé avec le service Internet activé agit comme le nœud de transit Internet principal. Si le service Internet n'est pas activé sur le nœud de transit virtuel de superposition, le nœud de transit Internet secondaire/de sauvegarde fournit un itinéraire vers Internet.



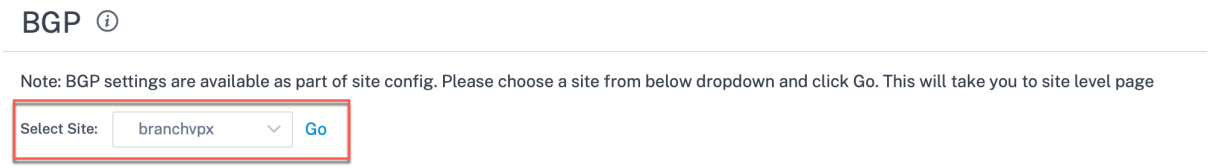
Nœud de transit intranet

Le nœud de transit intranet permet à tous les sites non intranet d'accéder aux réseaux intranet configurés. Un coût de trajet peut être attribué à chaque site de transit. Les sites disponibles avec le service intranet accèdent directement aux réseaux intranet puisque l'itinéraire direct serait le chemin de routage le plus bas coût. Les sites sans service intranet peuvent acheminer vers les réseaux intranet via les sites de transit configurés. Lorsque les sites de transit sont configurés, les itinéraires vers les réseaux intranet via ces sites de transit sont automatiquement acheminés vers tous les sites.
Par exemple, si 10.2.1.0/24 est un réseau intranet et qu'Austin et Dallas sont les sites de transit configurés. Les itinéraires vers cette adresse réseau via Austin et Dallas sont automatiquement poussés vers tous les sites.
Le nœud de transit virtuel superposé avec le service Intranet activé agit comme le nœud de transit intranet principal. Si le service intranet n'est pas activé sur le nœud de transit virtuel de superposition, le nœud de transit intranet secondaire de sauvegarde fournit un itinéraire vers l'intranet.



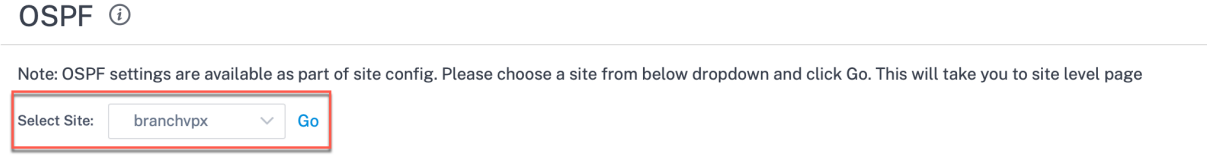
BGP

Vous pouvez configurer les paramètres BGP pour un site en sélectionnant le site requis dans la liste déroulante et en cliquant sur **OK**. Cela vous amène à la page de configuration BGP au niveau du site. Pour des informations détaillées sur la configuration de BGP, voir BGP.



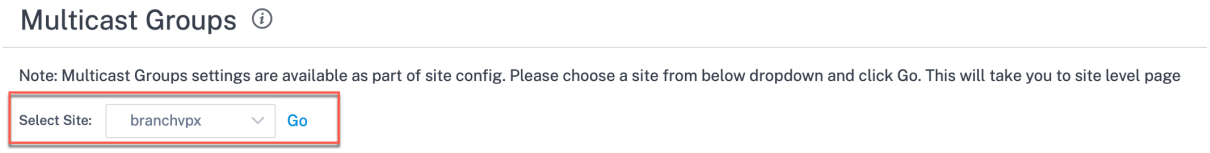
OSPF

Vous pouvez configurer les paramètres OSPF pour un site en sélectionnant le site requis dans la liste déroulante et en cliquant sur **OK**. Cela vous amène à la page de configuration OSPF au niveau du site. Pour des informations détaillées sur la configuration de l'OSPF, voir OSPF.



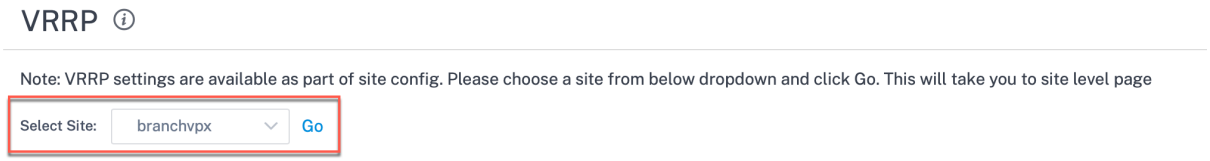
Groupes de multidiffusion

Vous pouvez configurer le routage de multidiffusion pour un site en sélectionnant le site requis dans la liste déroulante et en cliquant sur **OK**. Cela vous amène à la page de configuration des groupes de multidiffusion au niveau du site. Pour des informations détaillées sur la configuration du routage de multidiffusion, consultez la section Groupes de multidiffusion.



VRRP

Vous pouvez configurer le protocole de redondance du routeur virtuel (VRRP) pour un site en sélectionnant le site requis dans la liste déroulante et en cliquant sur **OK**. Cela vous amène à la page de configuration du VRRP au niveau du site. Pour des informations détaillées sur la configuration du routage de multidiffusion, voir VRRP.



Communication inter-liaison

October 21, 2022

Les paramètres de communication inter-liaison sont utilisés pour la création de chemins automatiques entre des liaisons WAN compatibles. Vous pouvez remplacer ces paramètres dans **Configuration du site** et **chemins virtuels**, où vous pouvez sélectionner ou désélectionner des chemins de membres individuels pour un chemin virtuel donné.

Actuellement, les deux paramètres suivants sont disponibles :

- Règles pour automatiser la création de chemins entre les liaisons WAN compatibles.
- Paramètres globaux par défaut pour les chemins virtuels dynamiques

Ces paramètres sont hérités par toutes les liaisons WAN du réseau client.

Cliquez sur **Vérifier la configuration** pour valider toute erreur d'audit.

Groupes de communication entre liens par défaut

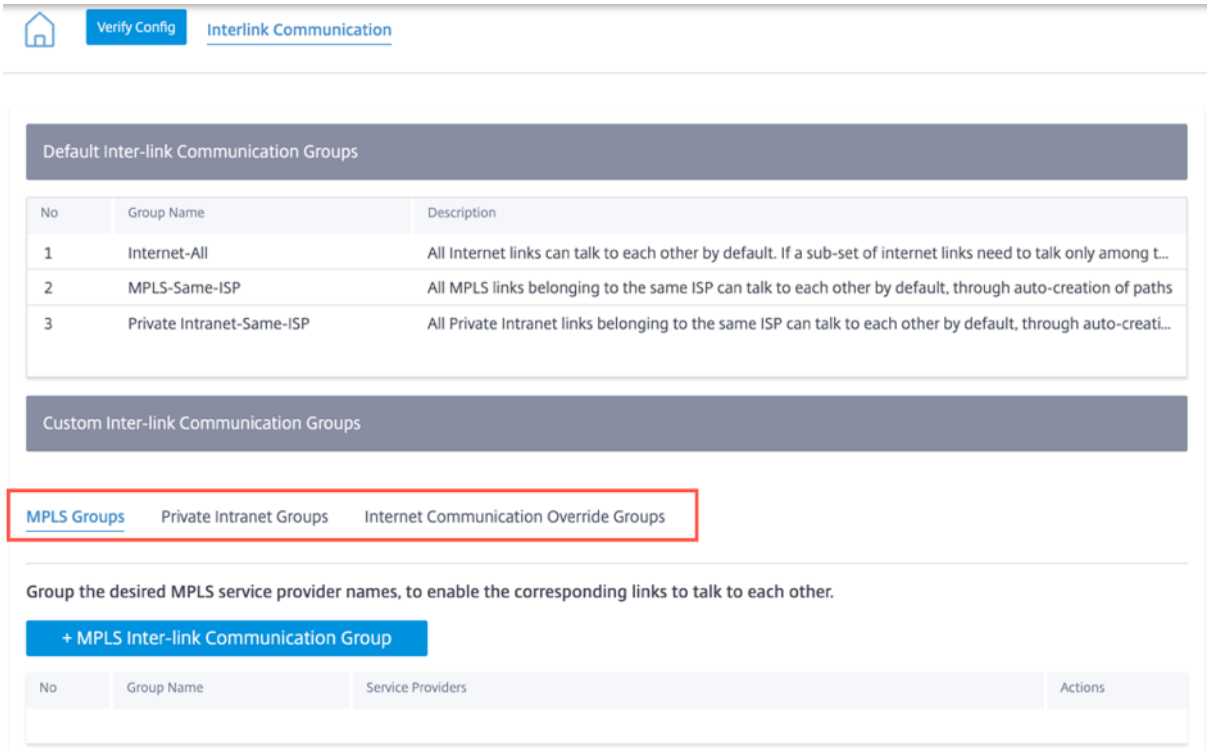
Les groupes de communication inter-liens par défaut sont destinés à automatiser la création de chemins entre :

- Deux liens Internet
- Deux liens MPLS qui partagent un fournisseur de services, et
- Deux liens intranet privés qui partagent un fournisseur de services

Groupes de communication inter-liens personnalisés

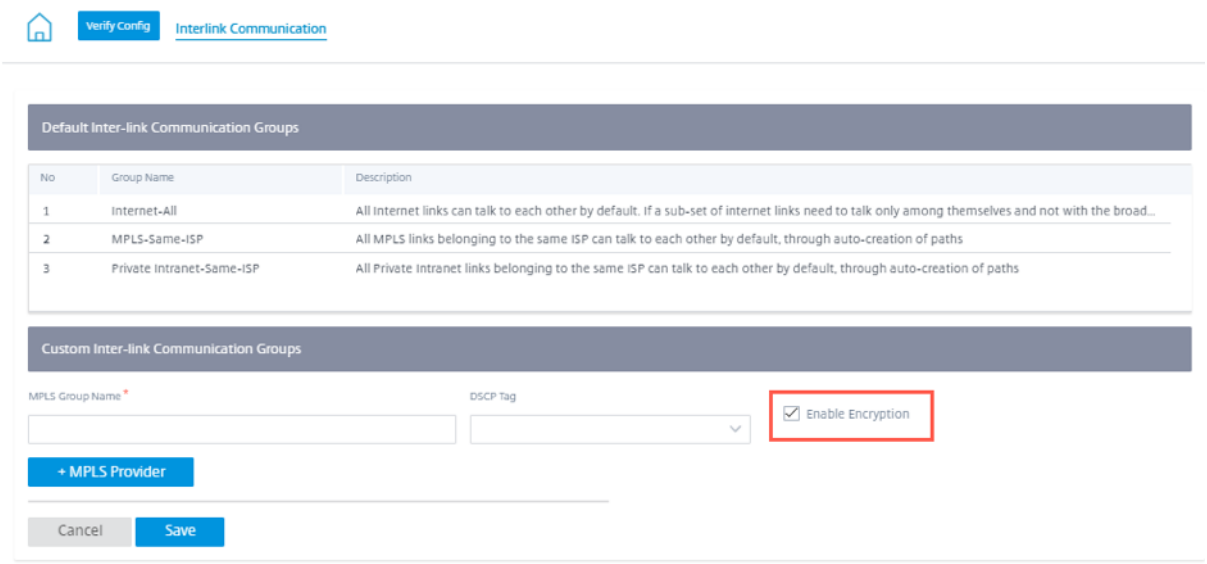
Les groupes de communication inter-liens personnalisés permettent aux liens Intranet privé, Internet public ou MPLS de créer automatiquement des chemins avec d'autres liens Intranet privé, Internet public ou MPLS entre différents fournisseurs de services.

Par exemple, considérez ce scénario - Une entreprise a des bureaux aux États-Unis et en Inde. Les bureaux américains utilisent les liaisons AT&T MPLS, tandis que les bureaux indiens utilisent les liaisons MPLS Airtel. Supposons que les liens MPLS AT&T et Airtel soient compatibles en termes de balises DSCP et de paramètres associés et se prêtent à la création de chemins entre eux. Les règles de communication inter-liens personnalisées vous permettent de sélectionner une paire de FAI (par exemple ATT —Airtel dans ce cas) et d'activer la création automatique de chemins parmi les liens appartenant à ces FAI.



- **Groupes MPLS** : Vous pouvez regrouper les noms des fournisseurs de services MPLS souhaités pour permettre aux liens correspondants de communiquer entre eux. Cliquez sur **+ MPLS Inter-Link Communication Group** et saisissez un nom de groupe MPLS. Sélectionnez la balise DSCP dans la liste déroulante. Vous pouvez également ajouter le fournisseur MPLS en sélectionnant le nom du fournisseur de services Internet dans la liste déroulante. La case à cocher **Activer le chiffrement** permet d'activer le chiffrement pour chaque groupe de communication MPLS inter-liens personnalisé. Dans de rares cas, pour éliminer la surcharge liée au chiffrement, vous pouvez désactiver cette option.
- **Groupes Intranet privés** : Vous pouvez regrouper les noms des fournisseurs de services Intranet de votre choix pour permettre aux liens correspondants de communiquer entre eux. Cliquez sur **+ Groupe de communication inter-liens pour l'intranet privé** et indiquez le nom du groupe intranet privé. Sélectionnez la balise DSCP dans la liste déroulante. Vous pouvez également ajouter le fournisseur intranet privé en sélectionnant le nom du fournisseur de services Internet dans la liste déroulante. La case à cocher **Activer le chiffrement** permet d'activer/désactiver le chiffrement pour chaque groupe de communication inter-liens Intranet privé personnalisé.
- **Groupes de remplacement des communications Internet** : si un sous-ensemble de liens Internet doit communiquer uniquement entre eux et non avec le reste des liens Internet, vous pouvez regrouper les noms de fournisseurs de services Internet correspondants pour permettre l'exclusion du groupe par défaut.

Le reste des liens Internet peut encore communiquer entre eux. Cliquez sur **+ Public Internet Inter-Link Communication Group** et saisissez un nom de groupe Internet public. Sélectionnez la balise DSCP dans la liste déroulante. Vous pouvez également ajouter le fournisseur Internet public en sélectionnant le nom du fournisseur de services Internet dans la liste déroulante. L'option **Activer le chiffrement** garantit que les paquets du groupe de communication inter-liens qui sont envoyés sur les chemins virtuels sont cryptés.



Sécurité

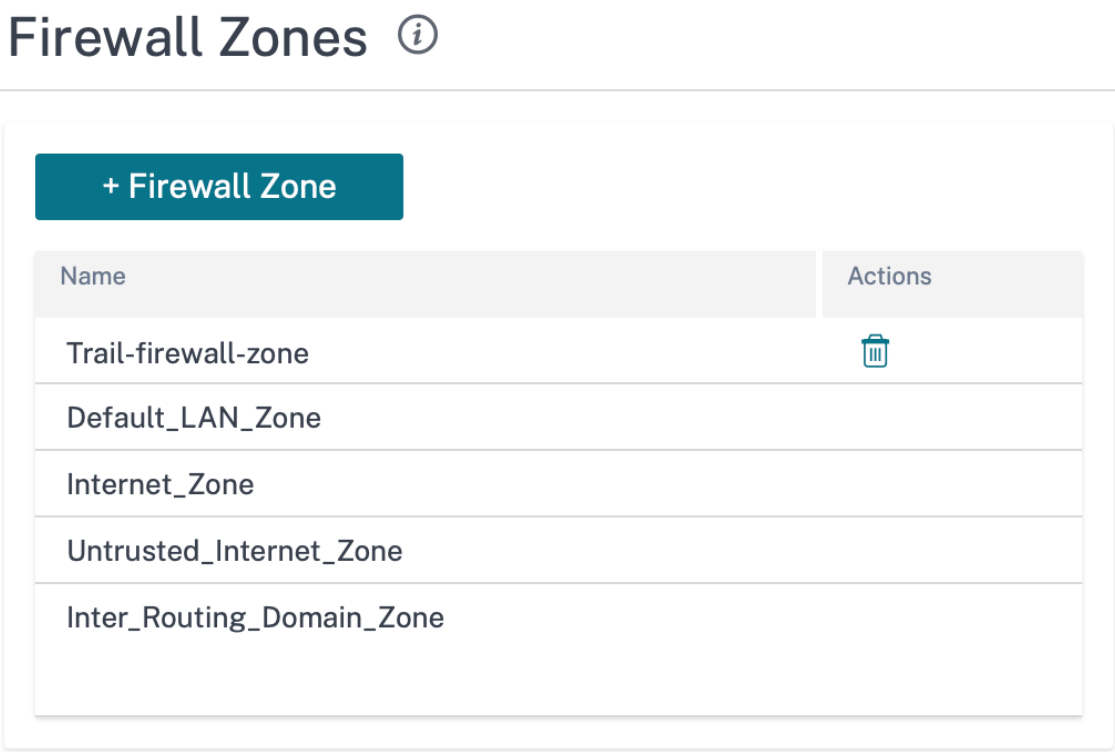
October 21, 2022

Vous pouvez configurer les paramètres de sécurité tels que la sécurité du réseau, le chemin virtuel IPsec, le pare-feu et les certificats applicables à toutes les appliances du réseau.

Zones pare-feu

Vous pouvez configurer des zones dans le réseau et définir des stratégies pour contrôler la manière dont le trafic entre et quitte les zones. Les zones suivantes sont disponibles par défaut :

- **Default_LAN_ZONE** : S'applique au trafic à destination ou en provenance d'un objet avec une zone configurable, lorsque la zone n'a pas été définie.
- **Internet_Zone** : s'applique au trafic à destination ou en provenance d'un service Internet via une interface sécurisée.
- **Untrusted_Internet_Zone** : s'applique au trafic à destination ou en provenance d'un service Internet via une interface non fiable.



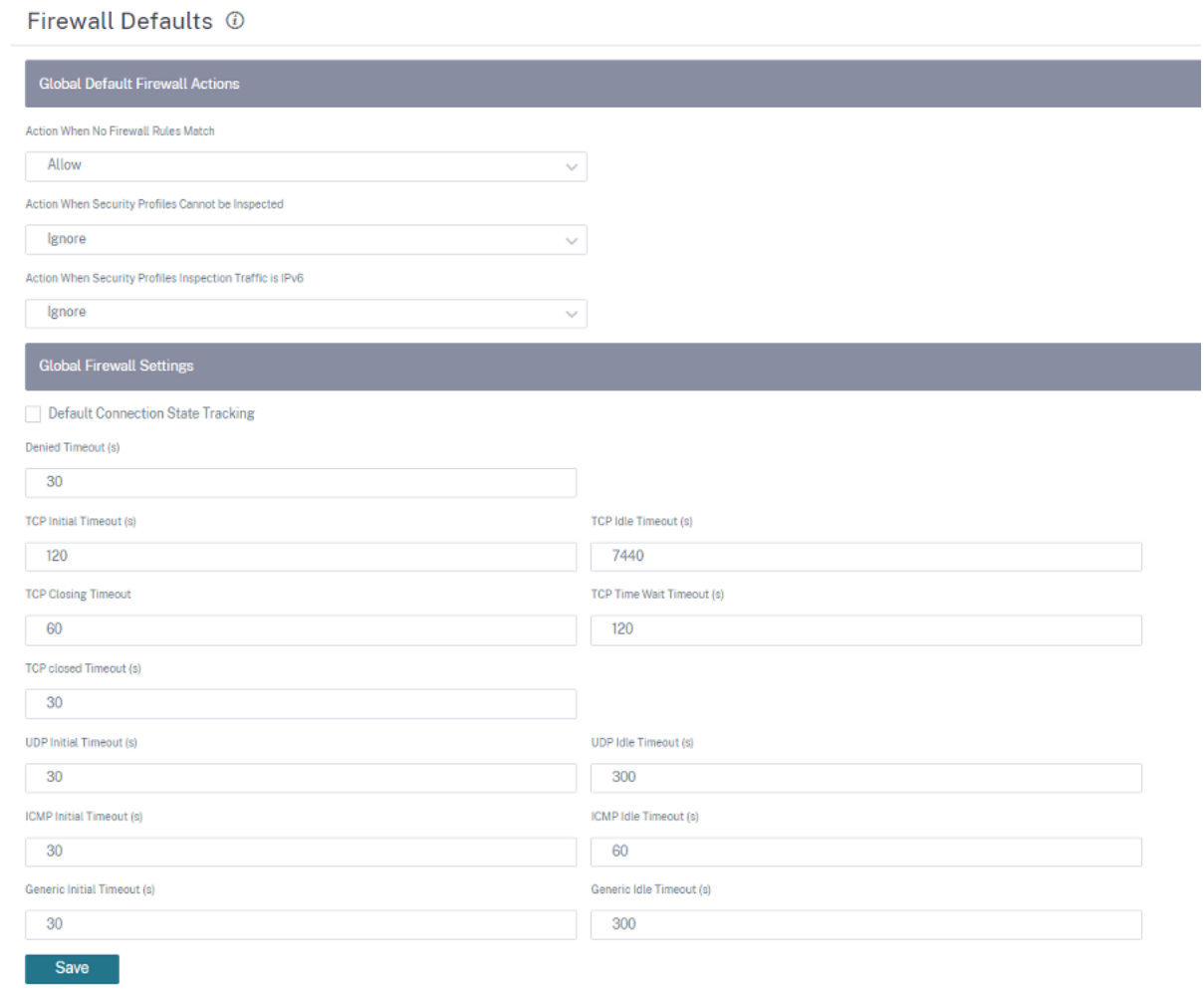
Vous pouvez également créer vos propres zones et les affecter aux types d'objets suivants :

- Interfaces réseau virtuelles
- Services Intranet
- Tunnels GRE
- Tunnels IPSec LAN

Cliquez sur **Vérifier la configuration** pour valider toute erreur d'audit.

Paramètres par défaut du pare-feu

Vous pouvez configurer les actions de pare-feu par défaut globales et les paramètres de pare-feu globaux qui peuvent être appliqués à toutes les appliances du réseau SD-WAN. Les paramètres peuvent également être définis au niveau du site, ce qui remplace le paramètre global.



- **Action lorsqu'aucune règle de pare-feu ne correspond** : Sélectionnez une action (Autoriser ou Supprimer) dans la liste pour les paquets qui ne correspondent pas à une politique de pare-feu.
- **Action lorsque les profils de sécurité ne peuvent pas être inspectés** : Sélectionnez une action (Ignorer ou Supprimer) pour les paquets qui correspondent à une règle de pare-feu et qui engagent un profil de sécurité mais qui ne peuvent temporairement pas être inspectés par le sous-système Edge Security. Si vous sélectionnez **Ignorer**, la règle de pare-feu correspondante est traitée comme non appariée et la règle de pare-feu suivante dans l'ordre est évaluée. Si vous sélectionnez **Drop**, les paquets correspondant à la règle de pare-feu correspondante sont supprimés.
- **Action de pare-feu par défaut** : sélectionnez une action (Autoriser/Supprimer) dans la liste pour les paquets qui ne correspondent pas à une politique.
- **Suivi de l'état de connexion par défaut** : active le suivi directionnel de l'état de connexion pour les flux TCP, UDP et ICMP qui ne correspondent pas à une politique de filtrage ou à une règle NAT.

> **Remarque**
>
> Les flux asymétriques sont bloqués lorsque le **suivi de l'état de connexion par défaut** est activé, même lorsqu'aucune politique de pare-feu n'est définie. S'il existe une possibilité de flux asymétriques sur un site, il est recommandé de l'activer au niveau du site ou de la politique et non globalement.

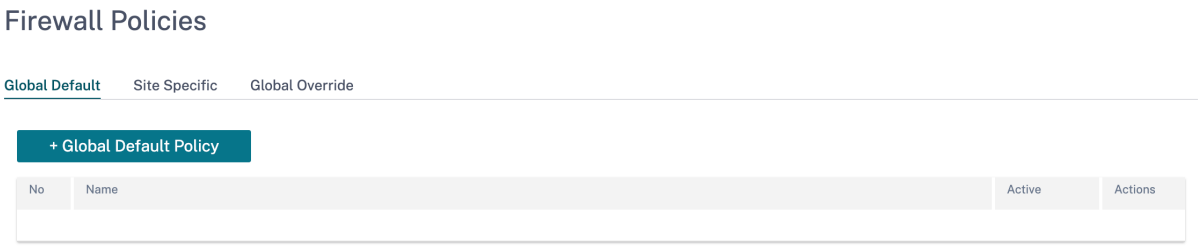
- **Délai (s) refusé (s)** : délai (en secondes) d'attente de nouveaux paquets avant de fermer les connexions refusées.
- **Délai (s) d'expiration initial (s) TCP** : temps (en secondes) d'attente de nouveaux paquets avant de fermer une session TCP incomplète.
- **Délai (s) d'inactivité TCP** : délai (en secondes) d'attente de nouveaux paquets avant de fermer une session TCP active.
- **Délai de fermeture du protocole TCP** : délai (en secondes) nécessaire pour attendre de nouveaux paquets avant de fermer une session TCP après une demande de fin.
- **Délai (s) d'attente TCP** : délai (en secondes) d'attente de nouveaux paquets avant de fermer une session TCP terminée.
- **Délai (s) de fermeture du protocole TCP** : temps (en secondes) nécessaire pour attendre de nouveaux paquets avant de fermer une session TCP abandonnée.
- **Délai (s) d'expiration initial (s) UDP** : temps (en secondes) nécessaire pour attendre de nouveaux paquets avant de fermer la session UDP qui n'a pas vu de trafic dans les deux sens.
- **Délai (s) d'inactivité UDP** : durée (en secondes) d'attente de nouveaux paquets avant de fermer une session UDP active.
- **Délai d'expiration initial (s) ICMP** : temps (en secondes) d'attente de nouveaux paquets avant de fermer une session ICMP qui n'a pas vu de trafic dans les deux sens
- **Délai (s) d'inactivité ICMP** : temps (en secondes) d'attente de nouveaux paquets avant de fermer une session ICMP active.
- **Délai (s) d'expiration initial générique** : temps (en secondes) nécessaire pour attendre de nouveaux paquets avant de fermer une session générique qui n'a pas vu de trafic dans les deux sens.
- **Délai (s) d'inactivité générique** : temps (en secondes) nécessaire pour attendre de nouveaux paquets avant de fermer une session générique active.

Cliquez sur **Vérifier la configuration** pour valider toute erreur d'audit.

Stratégies pare-feu

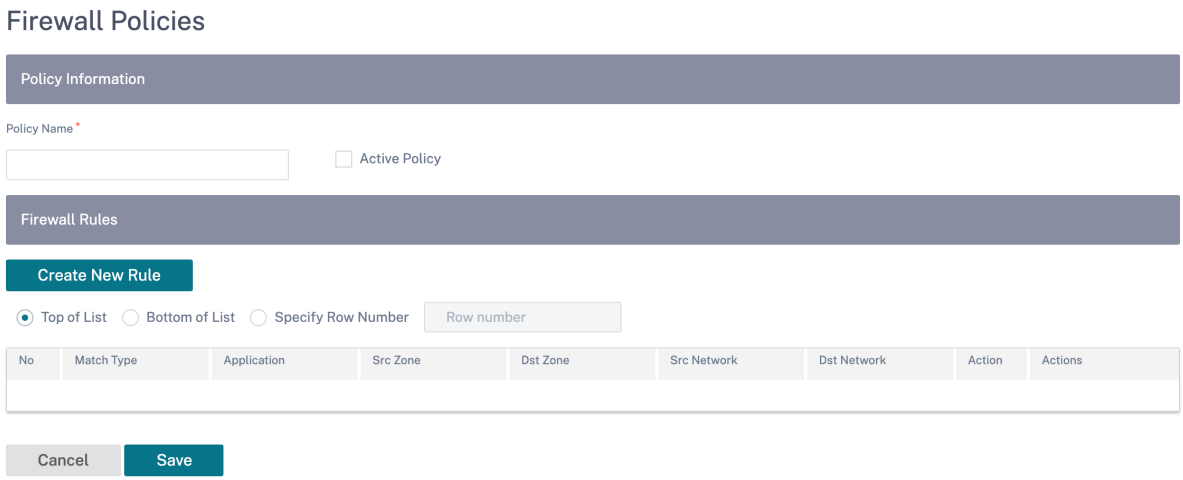
Les profils de pare-feu assurent la sécurité en garantissant que le trafic réseau est limité uniquement à une règle de pare-feu spécifique en fonction des critères de correspondance et en appliquant des actions spécifiques. Les **politiques de pare-feu** contiennent trois sections.

- **Valeur par défaut globale** —La politique globale par défaut est une agrégation de quelques règles de pare-feu. La politique que vous créez dans la section **Global Default** est appliquée à tous les sites du réseau.
- **Spécifique au site** : vous pouvez appliquer les règles de pare-feu définies sur certains sites spécifiques.
- **Remplacement global** : vous pouvez annuler les politiques globales et spécifiques au site à l'aide de la **politique de remplacement globale**.

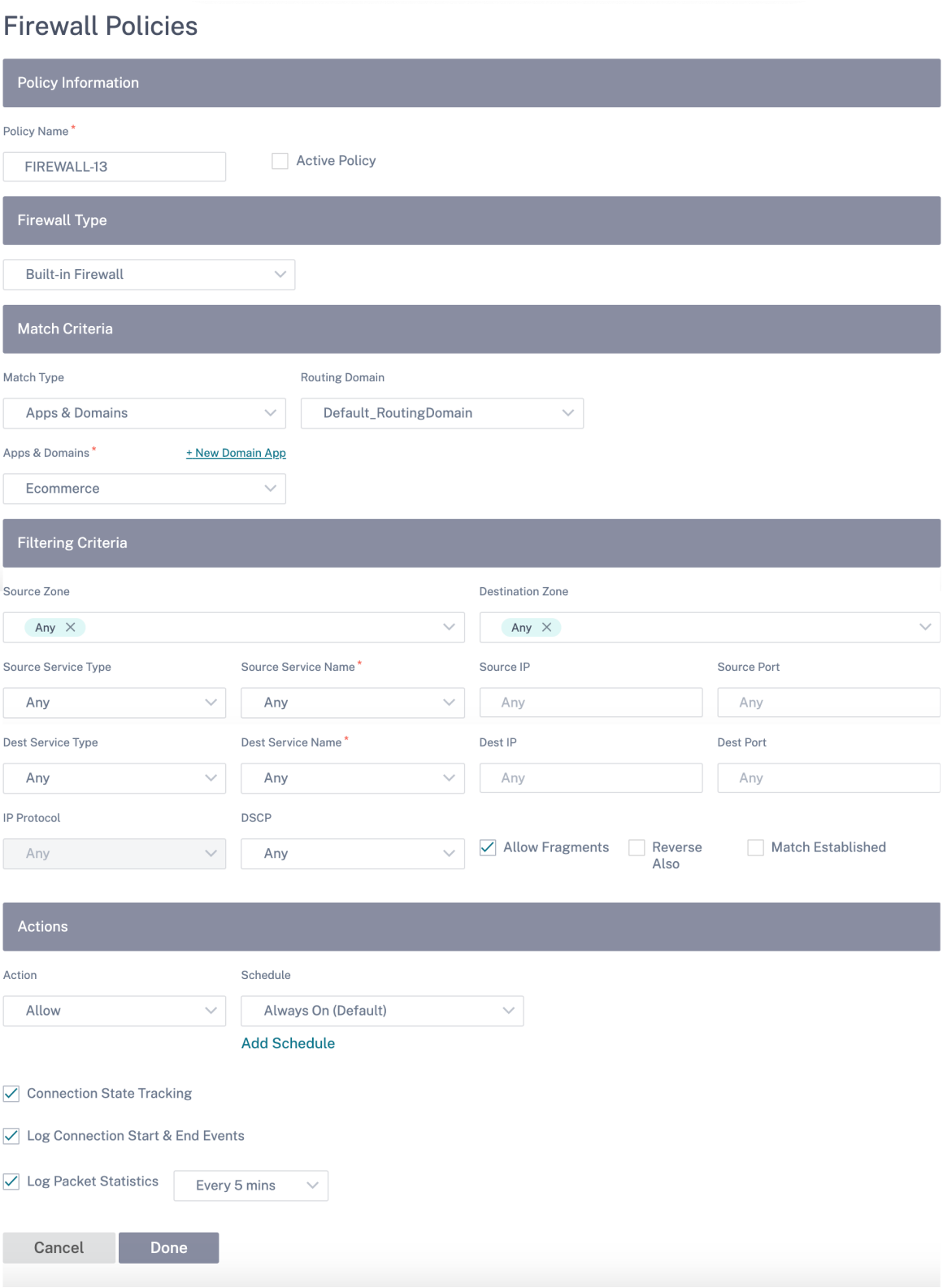


Vous pouvez définir des règles de pare-feu et les placer en fonction de la priorité. Vous pouvez choisir l'ordre de priorité à partir du haut de la liste, du bas de la liste ou d'une ligne spécifique.

Il est recommandé d'avoir des règles plus spécifiques pour les applications ou les sous-applications en haut, suivies de règles moins spécifiques pour celles qui représentent un trafic plus large.



Pour créer une règle de pare-feu, cliquez sur **Créer une nouvelle règle**.



- Entrez un nom de stratégie et cochez la case **Active Policy** si vous souhaitez appliquer toutes les règles de pare-feu.

- Les critères de correspondance définissent le trafic de la règle, par exemple, une application, une application définie personnalisée, un groupe d'applications, une famille d'applications ou un protocole IP.
- Critères de filtrage :
  - **Zone source : zone**de pare-feu source.
  - **Zone de destination : zone**de pare-feu de destination.
  - **Type de service source** : Le type de service SD-WAN source (local, chemin virtuel, intranet, hôte IP ou Internet) sont des exemples de types de services.
  - **Nom du service source** : nom d'un service lié au type de service. Par exemple, si le chemin virtuel est sélectionné pour le type de service source, il s'agit du nom du chemin virtuel spécifique. Cela n'est pas toujours obligatoire et dépend du type de service sélectionné.
  - **IP source** : adresse IP et masque de sous-réseau que la règle utilise pour faire correspondre.
  - **Port source** : port source utilisé par l'application spécifique.
  - **Type de service Dest** : le type de service SD-WAN de destination (local, chemin virtuel, intranet, hôte IP ou Internet) sont des exemples de types de services.
  - **Nom du service Dest** : nom d'un service lié au type de service. Cela n'est pas toujours obligatoire et dépend du type de service sélectionné.
  - **IP Dest** : L'adresse IP et le sous-réseau masquent le filtre à utiliser pour faire correspondre.
  - **Port Dest** : port de destination utilisé par l'application spécifique (c'est-à-dire le port de destination HTTP 80 pour le protocole TCP).
  - **Protocole IP** : Si ce type de correspondance est sélectionné, sélectionnez le protocole IP auquel la règle correspond. Les options incluent ANY, TCP, UDP ICMP et ainsi de suite.
  - **DSCP** : autorise l'utilisateur à faire correspondre un paramètre de balise DSCP.
  - **Autoriser les fragments** : autorise les fragments IP qui correspondent à cette règle.
  - **Inverser aussi** : ajoutez automatiquement une copie de cette politique de filtrage en inversant les paramètres de source et de destination.
  - **Correspondance établie** : met en correspondance les paquets entrants pour une connexion à laquelle les paquets sortants étaient autorisés.
- Les actions suivantes peuvent être exécutées sur un flux apparié :
  - **Autoriser** : autorisez le flux à travers le pare-feu.
  - **Supprimer** : empêchez le flux de traverser le pare-feu en supprimant les paquets.

- **Refuser** : bloquez le flux à travers le pare-feu et envoyez une réponse spécifique au protocole. TCP envoie une réinitialisation, ICMP envoie un message d'erreur.
- **Compter et continuer** : comptez le nombre de paquets et d'octets pour ce flux, puis continuez dans la liste des politiques.

Outre la définition de l'action à effectuer, vous pouvez également sélectionner les journaux à capturer.

Sécurité du réseau

Sélectionnez le mécanisme de chiffrement à utiliser sur le réseau. Vous pouvez configurer les paramètres de sécurité globaux qui sécurisent l'ensemble du réseau SD-WAN.

Le mode de chiffrement réseau définit l'algorithme utilisé pour tous les chemins chiffrés du réseau SD-WAN. Elle ne s'applique pas aux chemins non chiffrés. Vous pouvez définir le chiffrement comme AES-128 ou AES-256.

Conformité FIPS

Le mode FIPS oblige les utilisateurs à configurer des paramètres conformes à la norme FIPS pour leurs tunnels IPSec et des paramètres IPsec pour les chemins virtuels.

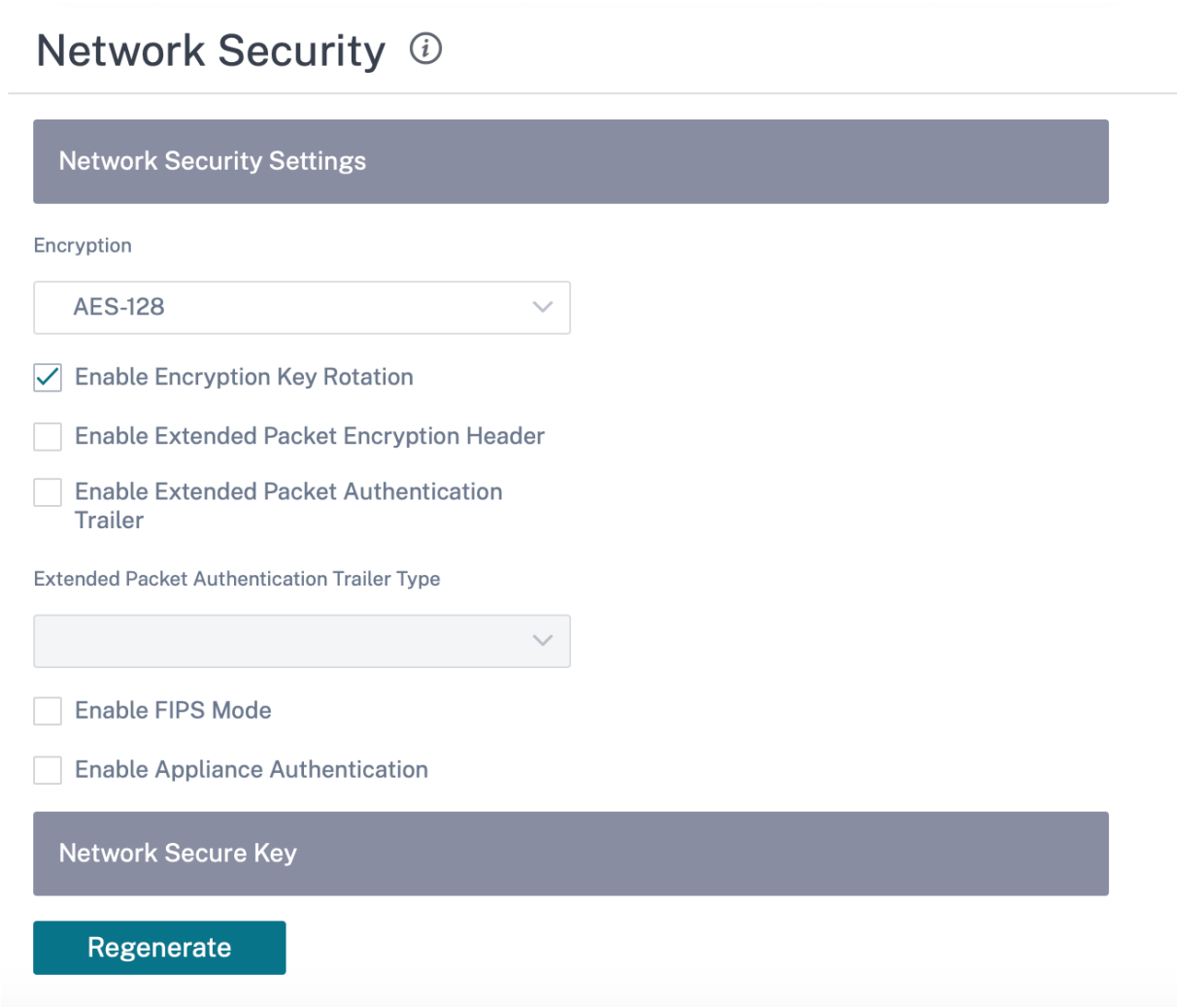
L'activation du mode FIPS offre les fonctionnalités suivantes :

- Affiche le mode IKE conforme à la norme FIPS.
- Affiche un groupe IKE DH conforme à FIPS dans lequel les utilisateurs peuvent sélectionner les paramètres requis pour configurer l'appliance en mode FIPS (2,5,14 —21).
- Affiche le type de tunnel IPSec conforme à FIPS dans les paramètres IPSec pour les chemins virtuels
- Mode Hash IKE et intégrité (IKEV2), mode Auth IPSec.
- Effectue des erreurs d'audit pour les paramètres de durée de vie basés sur la

Pour activer la conformité FIPS sur le service Citrix SD-WAN Orchestrator :

1. Accédez à **Configuration** > **Sécurité** > **Sécurité réseau**.
2. Dans la section **Paramètres de sécurité réseau**, cochez la case **Activer le mode FIPS** .

L'activation du mode FIPS permet d'appliquer des vérifications pendant la configuration afin de s'assurer que tous les paramètres de configuration liés à IPSec respectent les normes FIPS. Vous êtes invité par des erreurs d'audit et des avertissements à configurer IPSec.



Si la configuration IPsec n'est pas conforme aux normes FIPS lorsqu'elle est activée, une erreur d'audit peut se déclencher. Vous trouverez ci-dessous les types d'erreurs d'audit qui s'affichent lorsque vous cliquez sur **Verify Config** sur l'interface utilisateur Citrix SD-WAN Orchestrator for On-premises.

- Lorsque le mode FIPS est activé et que l'option non conforme à la norme FIPS est sélectionnée.
- Lorsque le mode FIPS est activé et qu'une valeur de durée de vie incorrecte est saisie.
- Lorsque le mode FIPS est activé et que les paramètres IPsec pour le chemin virtuel par défaut sont également activés, et que le mode Tunnel incorrect est sélectionné (ESP vs ESP_Auth/AH).
- Lorsque le mode FIPS est activé, les paramètres IPsec définis par défaut pour le chemin virtuel sont également activés et une valeur de durée de vie incorrecte est saisie.

Activer la rotation des clés de chiffrement : lorsque cette option est activée, les clés de chiffrement sont pivotées à des intervalles de 10 à 15 minutes.

Activer l'en-tête Extended Packet Encryption : Lorsque cette option est activée, un compteur chiffré de 16 octets est ajouté au début du trafic chiffré pour servir de vecteur d'initialisation, et le chiffrement

des paquets est aléatoire.

Enable Extended Packet Authentication Trailer : Lorsque cette option est activée, un code d'authentification est ajouté au contenu du trafic chiffré pour vérifier que le message est livré sans modification.

Extended Packet Authentication Trailer Type : Il s'agit du type de fin utilisé pour valider le contenu des paquets. Sélectionnez l'une des options suivantes dans le menu déroulant : **Somme de contrôle 32 bits** ou **SHA-256**.

Inspection SSL

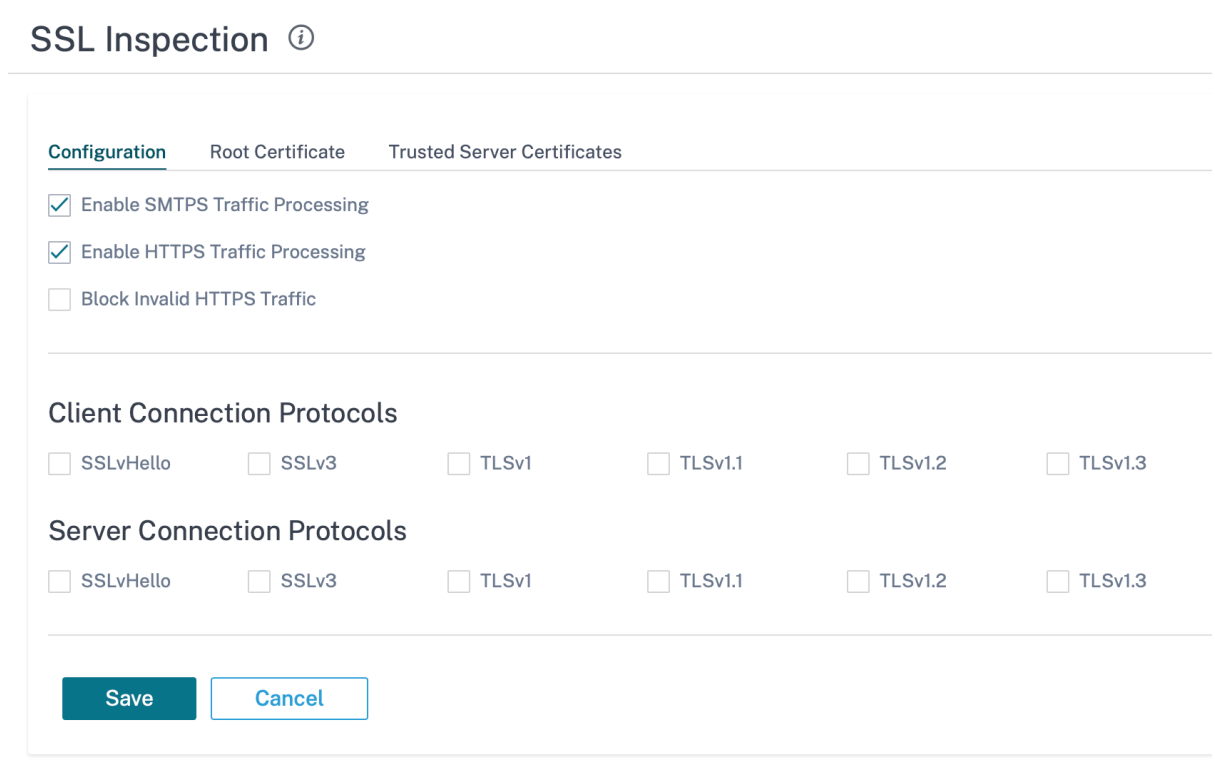
L'inspection SSL (Secure Sockets Layer) est un processus d'interception, de déchiffrement et d'analyse du trafic HTTPS et SMTP sécurisé pour détecter tout contenu malveillant. L'inspection SSL assure la sécurité du trafic entrant et sortant de votre organisation. Vous pouvez générer et télécharger le certificat de l'autorité de certification racine de votre organisation et effectuer l'inspection intermédiaire du trafic.

> **REMARQUE :**
>
> L'inspection SSL est prise en charge à partir de la version 11.3.0 de Citrix SD-WAN.

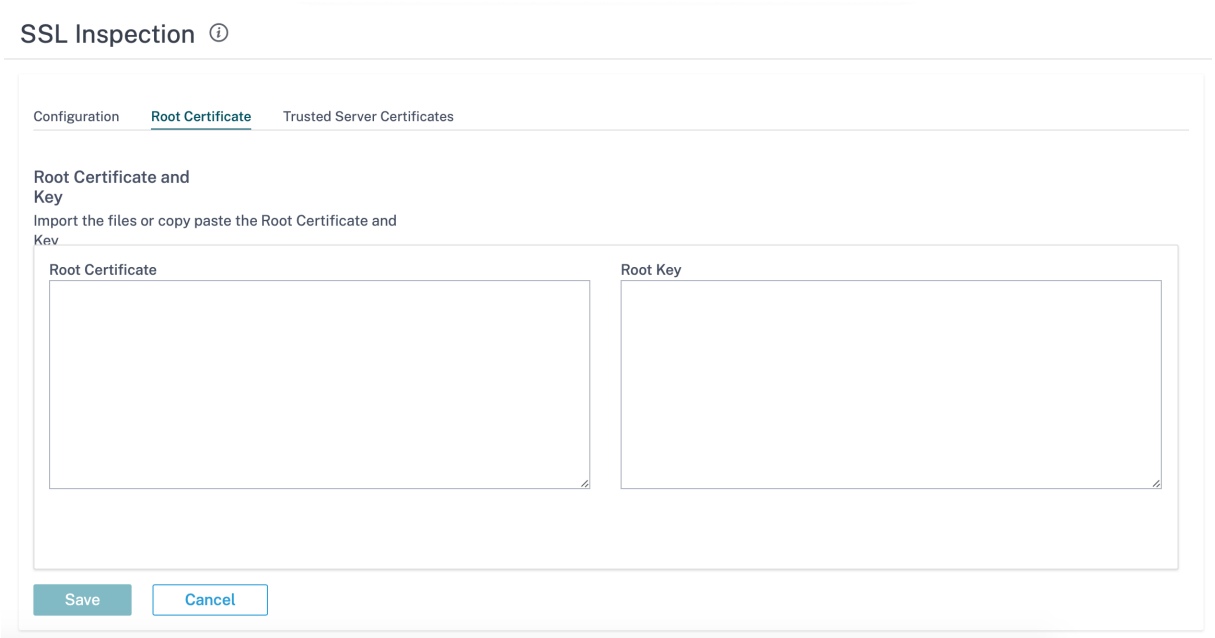
Pour activer l'inspection SSL, au niveau du réseau, accédez à **Configuration > Sécurité > Inspection SSL > Configuration** et définissez les paramètres de configuration SSL suivants.

- **Activer le traitement du trafic SMTPS** : Le trafic SMTP sécurisé est soumis à une inspection SSL.
- **Activer le traitement du trafic HTTPS** : Le trafic HTTPS est soumis à une inspection SSL.
- **Bloquer le trafic HTTPS non valide** : par défaut, lorsque la case **Bloquer le trafic HTTPS non valide** est décochée, le trafic non HTTPS sur le port 443 est ignoré et autorisé à circuler librement. Lorsque l'option **Bloquer le trafic HTTPS non valide** est sélectionnée, le trafic non HTTPS est bloqué pour inspection SSL. L'activation de cette option peut entraîner le blocage du trafic par ailleurs légitime, c'est-à-dire du trafic HTTP sur le port 443 ou du trafic HTTPS provenant de sites dont le certificat a expiré.
- **Protocoles de connexion client** : sélectionnez les protocoles clients requis. Les protocoles disponibles sont SSLvHello, SSLv3, TLSv1, TSLv1.1, TLSv1.2 et TLSv1.3.
- **Protocoles de connexion au serveur** : sélectionnez les protocoles de serveur requis. Les protocoles disponibles sont SSLvHello, SSLv3, TLSv1, TSLv1.1, TLSv1.2 et TLSv1.3.

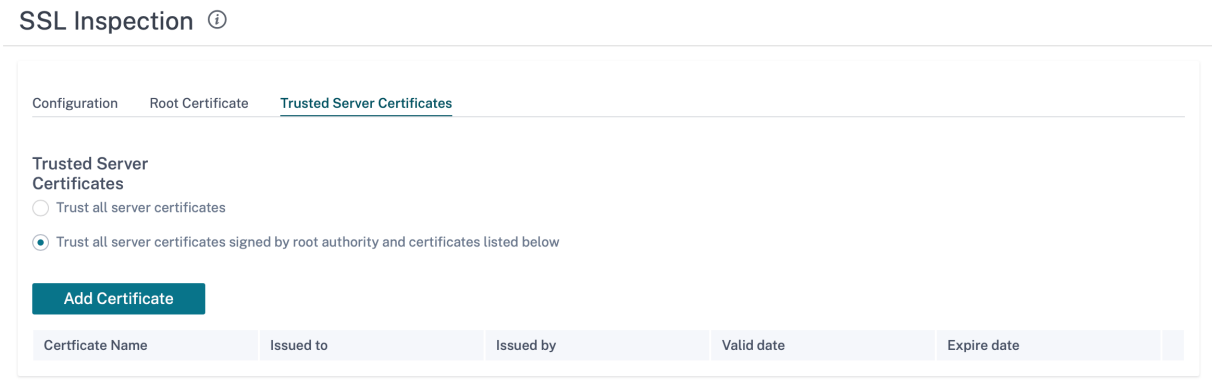
> **REMARQUE**
>
> Les versions antérieures à TLSv1.2 sont considérées comme vulnérables et ne doivent pas être activées, sauf si la rétrocompatibilité est importante.



Dans l'onglet **Certificat racine**, copiez et collez le certificat racine et la clé de l'autorité de certification racine (CA) de votre organisation. L'autorité de certification racine est utilisée pour créer et signer une copie falsifiée des certificats des sites d'origine, afin que l'inspection SSL puisse être effectuée. Il est implicitement supposé que le certificat de l'autorité de certification racine est installé sur tous les postes de travail et appareils clients dont le trafic SSL peut être inspecté.



L'option par défaut, **Faire confiance à tous les certificats de serveur signés par l'autorité racine et aux certificats répertoriés ci-dessous**, permet au SD-WAN de valider tous les certificats de serveur par rapport à la liste standard des autorités de certification racines et à l'autorité de certification racine précédemment configurées. Il supprime également les serveurs dont le certificat n'est pas valide. Pour contourner ce comportement, téléchargez le certificat SSL auto-signé des serveurs internes dans l'onglet **Certificats de serveur de confiance** . Cliquez sur **Ajouter un certificat** et saisissez un nom, recherchez le certificat et téléchargez-le. Sinon, si vous sélectionnez Faire **confiance à tous les certificats de serveur**, tous les serveurs sont considérés comme approuvés par Citrix SD-WAN, quel que soit leur statut de validation des certificats.



Dans le cadre des profils de sécurité, vous pouvez créer des règles SSL et les activer pour l'inspection SSL. Pour plus d'informations sur la création de règles SSL pour un profil de sécurité, consultez la section Sécurité Edge.

Prévention des intrusions

Le système de prévention des intrusions (IPS) détecte et empêche les activités malveillantes d'entrer sur votre réseau. L'IPS inspecte le trafic réseau et prend des mesures automatisées sur tous les flux de trafic entrants. Il inclut une base de données de plus de 34 000 détections de signatures et de signatures heuristiques pour les scans de ports, vous permettant de surveiller et de bloquer efficacement la plupart des requêtes suspectes.

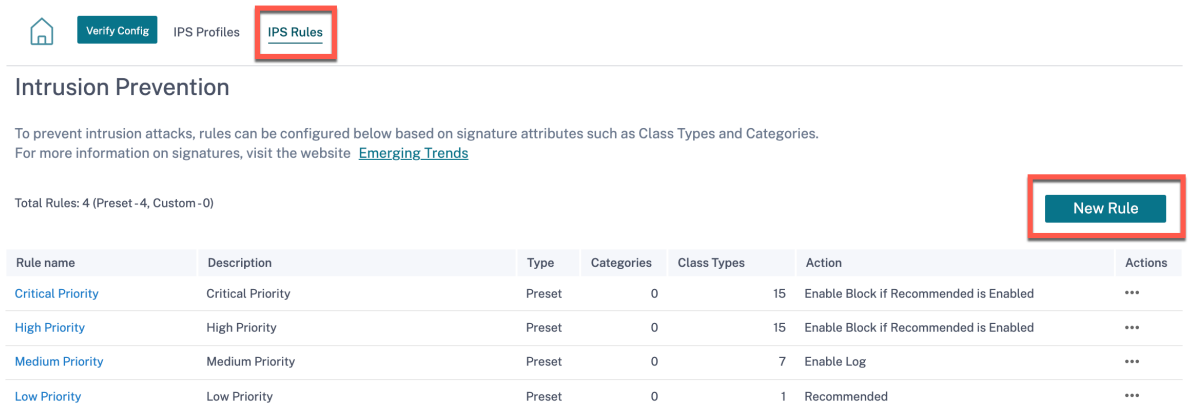
IPS utilise la détection basée sur la signature, qui fait correspondre les paquets entrants à une base de données de modèles d'exploits et d'attaques identifiables de manière unique. La base de données des signatures est automatiquement mise à jour quotidiennement. Comme il y a des milliers de signatures, les signatures sont regroupées en types Catégorie et Classe.

Vous pouvez créer des règles IPS et activer uniquement les catégories de signatures ou les types de classes requis par votre réseau. La prévention des intrusions étant un processus sensible au calcul, utilisez uniquement l'ensemble minimal de catégories de signatures ou de types de classes pertinents pour votre réseau.

Vous pouvez créer un profil IPS et activer une combinaison de règles IPS. Ces profils IPS peuvent ensuite être associés globalement à l'ensemble du réseau ou uniquement à des sites spécifiques.

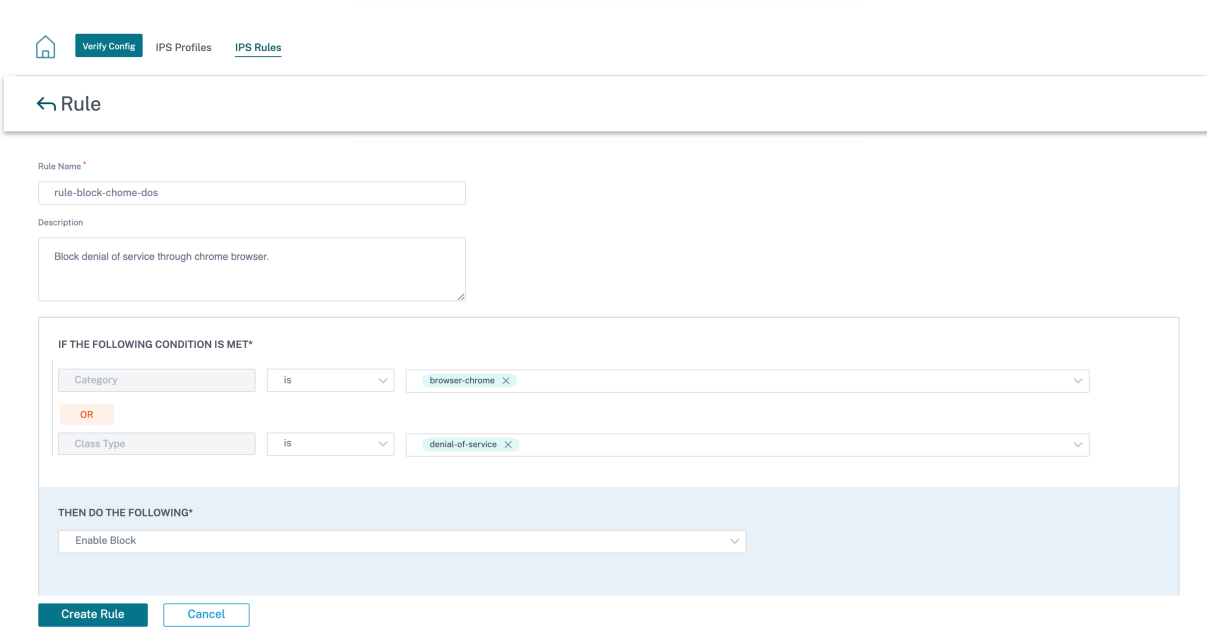
Chaque règle peut être associée à plusieurs profils IPS et chaque profil IPS peut être associé à plusieurs sites. Lorsqu'un profil IPS est activé, il inspecte le trafic réseau pour les sites auxquels le profil IPS est associé et pour les règles IPS activées dans ce profil.

Pour créer des règles IPS, au niveau du réseau, accédez à **Configuration > Sécurité > Prévention des intrusions > Règles IPS** et cliquez sur **Nouvelle règle**.



Fournissez un nom et une description de la règle. Sélectionnez les attributs de signature de catégorie de correspondance ou de type de classe, sélectionnez une action pour la règle et activez-la. Vous pouvez choisir parmi les actions de règle suivantes :

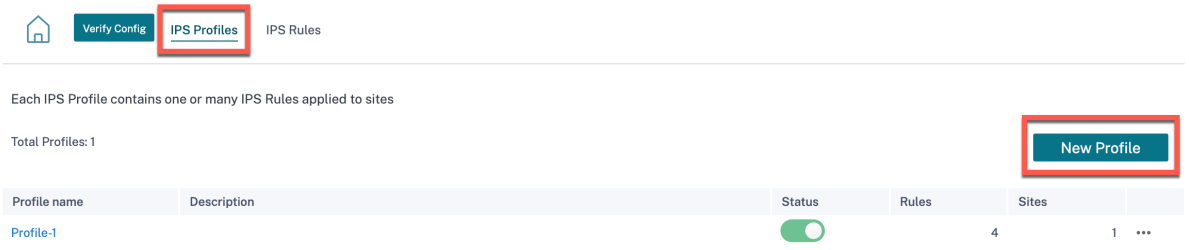
Action de règle	Fonction
Recommandé	Des actions recommandées sont définies pour chaque signature. Effectuez l'action recommandée pour les signatures.
Activer le journal	Autoriser et consigner le trafic correspondant à l'une des signatures de la règle.
Activer le bloc si recommandé est activé	Si l'action de la règle est **Recommandée** et que l'action recommandée pour la signature est **Activer le journal**, supprimez le trafic correspondant à l'une des signatures de la règle.
Activer le bloc	Suppriment le trafic correspondant à l'une des signatures de la règle.



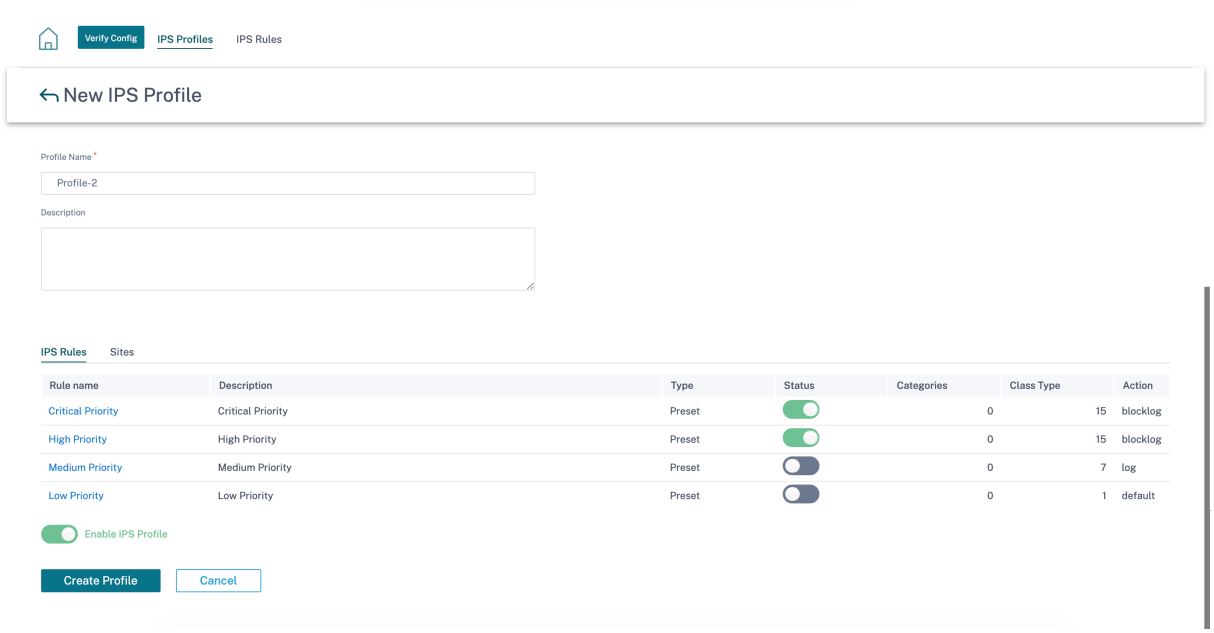
Remarque

- Étant donné que la prévention des intrusions est un processus sensible au calcul, utilisez uniquement l'ensemble minimal de catégories de signatures pertinentes pour vos déploiements de sécurité Edge.
- Le pare-feu SD-WAN supprime le trafic sur tous les ports WAN L4 qui ne sont pas transférés par port et ne sont pas visibles dans le moteur IPS. Cela fournit une couche de sécurité supplémentaire contre les attaques DOS et scan triviales.

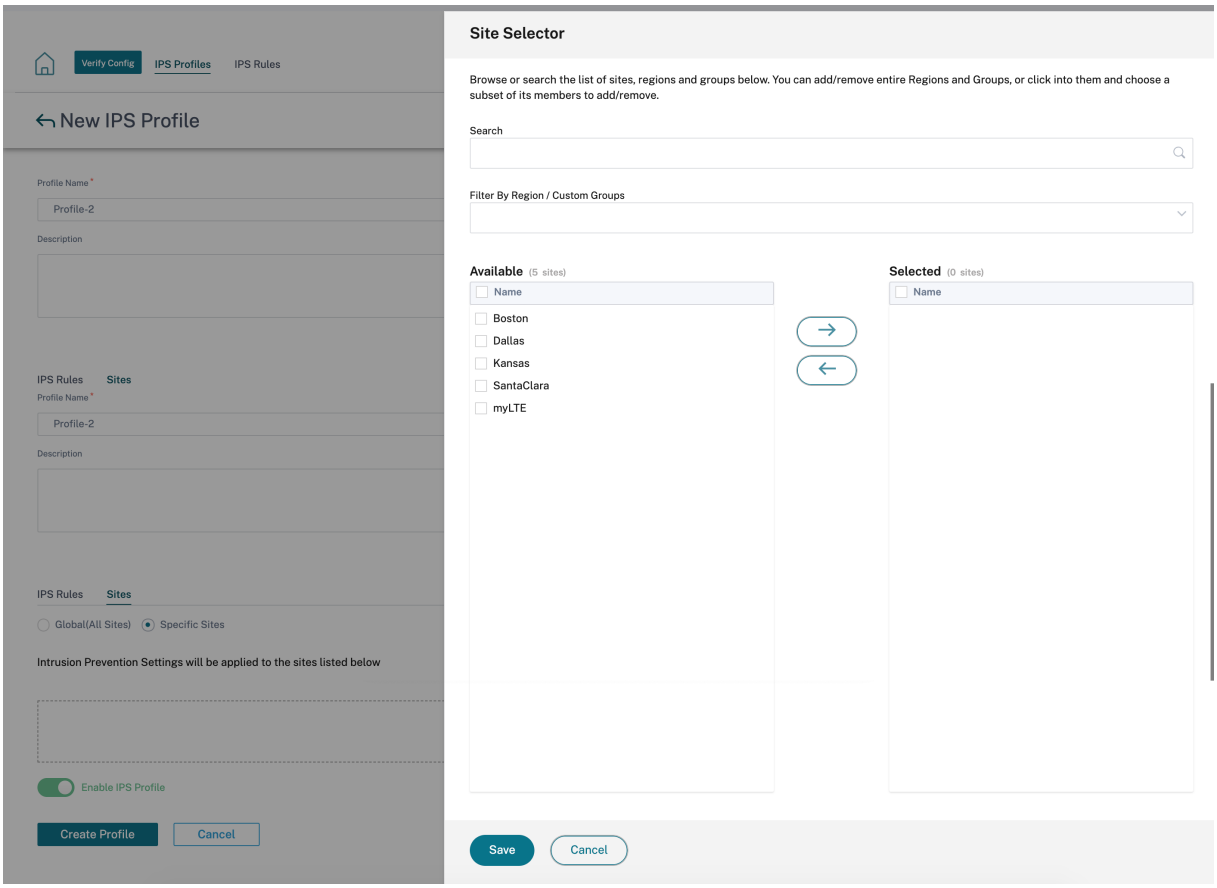
Pour créer des profils IPS, au niveau du réseau, accédez à **Configuration > Sécurité > Prévention des intrusions > Profils IPS** et cliquez sur **Nouveau profil**.



Fournissez un nom et une description pour le profil IPS. Dans l'onglet **Règles IPS**, activez les **règles IPS** requises et activez **Activer les profils IPS**.



Dans l'onglet **Sites**, cliquez sur **Sélectionner des sites**. Sélectionnez les sites et cliquez sur **Enregistrer**. Cliquez sur **Créer un profil**.



Vous pouvez activer ou désactiver ces profils IPS lors de la création de profils de sécurité. Les profils

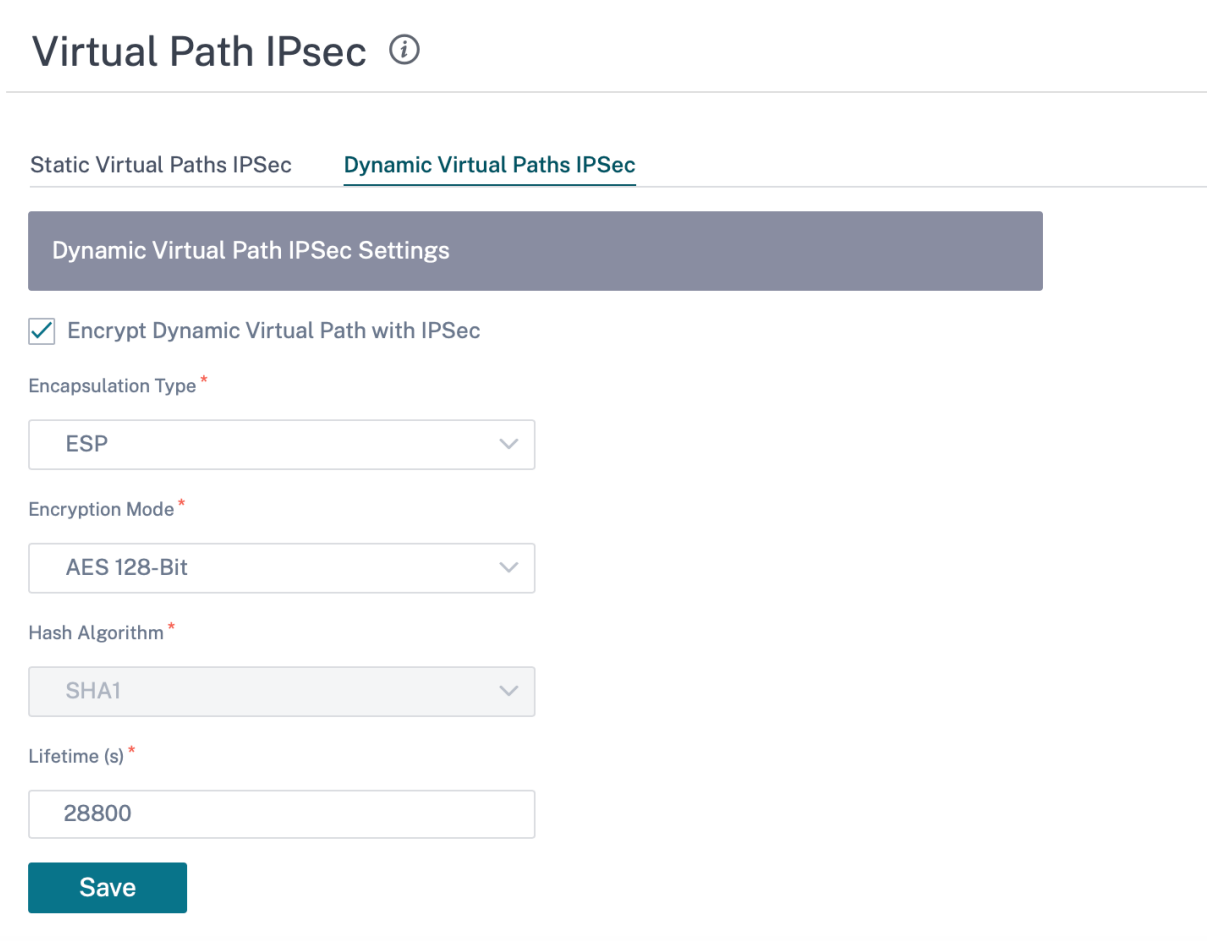
de sécurité sont utilisés pour créer des règles de pare-feu. Pour plus d'informations, voir Profil de sécurité —Prévention des intrusions.

Chemin virtuel IPsec

Le**chemin virtuel IPsec** définit les paramètres du tunnel IPsec afin de garantir la transmission sécurisée des données via les chemins virtuels statiques et les chemins virtuels dynamiques. Sélectionnez l'onglet **Chemins virtuels statiques IPsec** ou **Chemins virtuels dynamiques IPsec** pour définir les paramètres du tunnel IPSec.

- **Type d'encapsulation** : Choisissez l'un des types de sécurité suivants :
  - **ESP** : Les données sont encapsulées et cryptées.
  - **ESP+Auth** : les données sont encapsulées, cryptées et validées avec un HMAC.
  - **AH** : Les données sont validées avec un HMAC.
- **Mode de chiffrement** : algorithme de chiffrement utilisé lorsque l'ESP est activé.
- **Algorithme**de hachage : algorithme de hachage utilisé pour générer un HMAC.
- Durée de**vie (s)** : durée préférée, en secondes, pour qu'une association de sécurité IPsec existe. Entrez 0 pour illimité.

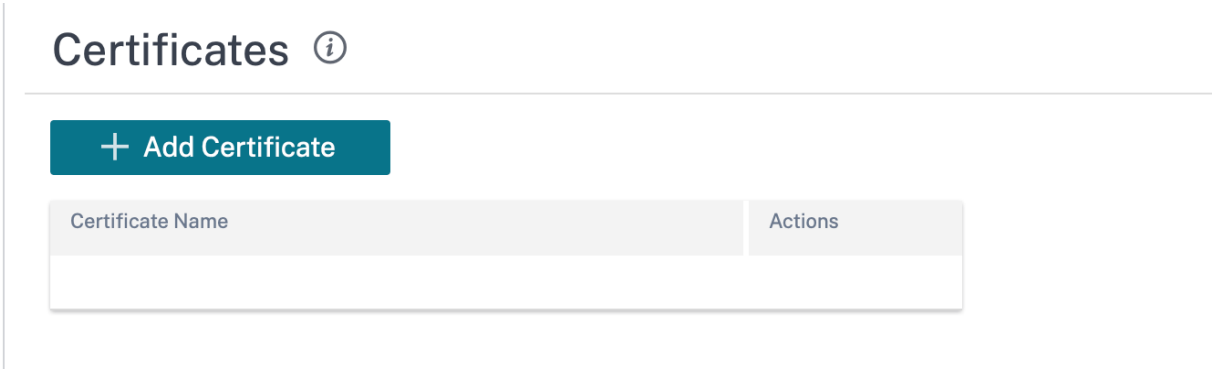
Pour plus d'informations sur la configuration du service IPsec, consultez la section Service IPSec.



Cliquez sur **Vérifier la configuration** pour valider toute erreur d'audit

Certificats

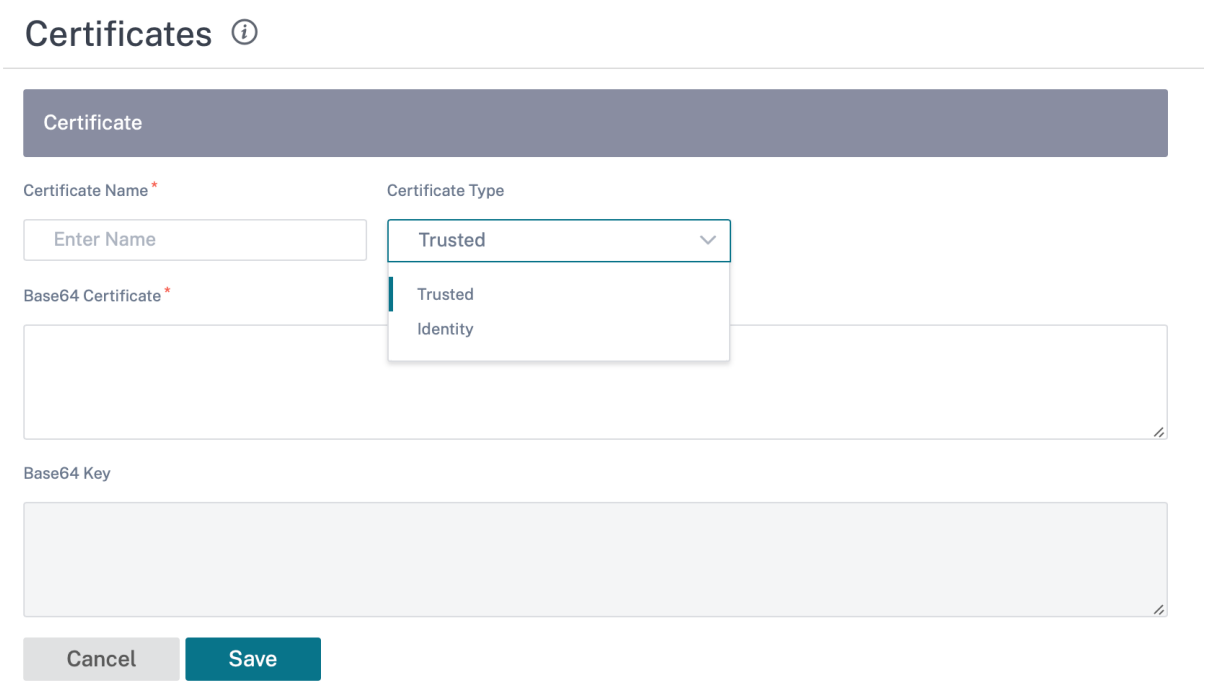
Il existe deux types de certificats : Identité et Certificat de confiance. Les certificats d'identité sont utilisés pour signer ou chiffrer des données afin de valider le contenu d'un message et l'identité de l'expéditeur. Les certificats approuvés sont utilisés pour vérifier les signatures de message. Les appliances Citrix SD-WAN acceptent à la fois les certificats d'identité et les certificats approuvés. Les administrateurs peuvent gérer les certificats dans l'Éditeur de configuration.



Cliquez sur **Vérifier la configuration** pour valider toute erreur d'audit

Pour ajouter un certificat, cliquez sur **Ajouter un certificat**.

- **Nom du certificat** : Entrez le nom du certificat.
- **Type de certificat** : Sélectionnez le type de certificat dans la liste déroulante.
  - **Certificats d'**identité : les certificats d'identité nécessitent que la clé privée du certificat soit mise à la disposition du signataire. Certificats d'identité ou leurs chaînes de certificats qui sont approuvés par un homologue pour valider le contenu et l'identité de l'expéditeur. Les certificats d'identité configurés et leurs empreintes digitales respectives sont affichés dans l'éditeur de configuration.
  - **Certificats**de confiance : Les certificats de confiance sont des certificats d'autorité de certification intermédiaire (CA) ou d'autorité de certification racine auto-signés utilisés pour valider l'identité d'un homologue. Aucune clé privée n'est requise pour un certificat de confiance. Les certificats approuvés configurés et leurs empreintes digitales respectives sont répertoriés ici.

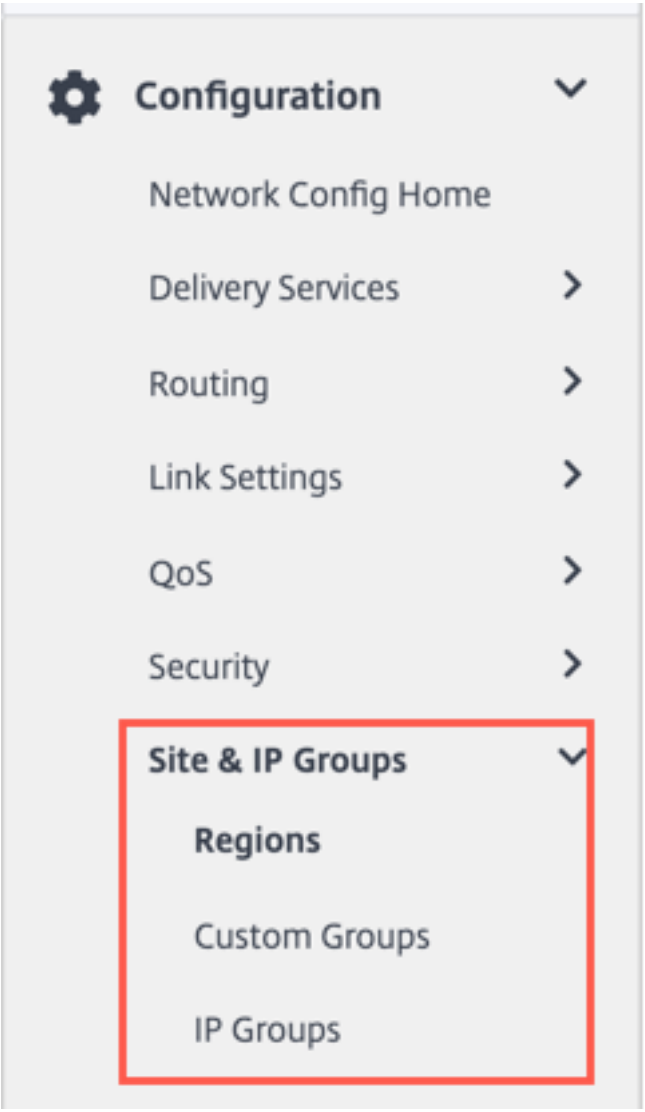


Groupes de sites et d'IP

October 21, 2022

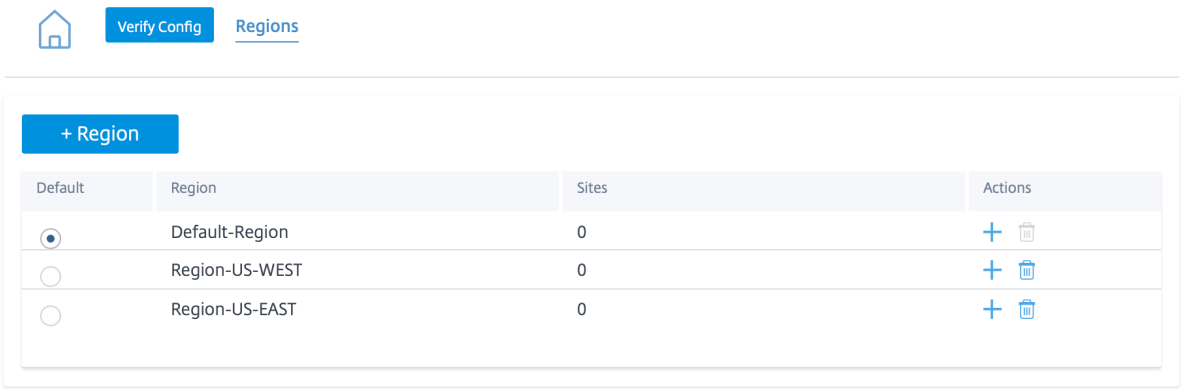
Les administrateurs peuvent regrouper des sites ou des adresses IP pour simplifier les stratégies d'application communes sur plusieurs sites ou adresses réseau, et servir de filtres pour les rapports.

Pour afficher les régions, les sites et les groupes d'adresses IP, accédez à **Configuration** > **Groupes de sites et d'adresses IP**.



Régions

Les régions aident à créer des limites administratives au sein de grands réseaux couvrant des centaines à des milliers de sites. Si votre organisation dispose d'un réseau étendu couvrant plusieurs limites administratives (ou géographiques), vous pouvez envisager de créer des régions pour segmenter le réseau.



Actuellement, un maximum de 1000 sites sont pris en charge par région. Chaque région devrait avoir un nœud de contrôle régional (RCN), qui sert de hub et de Controller pour la région. Par conséquent, vous envisageriez généralement un déploiement multi-région si votre réseau compte plus de 500 sites. Par défaut, tous les réseaux sont des réseaux à une seule région, où le nœud de contrôle maître (MCN) sert de concentrateur et de nœud de contrôle pour tous les sites. En ajoutant une ou plusieurs régions, le réseau devient un réseau multi-régions. La région associée au MCN est appelée **région par défaut**.

Un réseau multi-région prend en charge une architecture hiérarchique avec un MCN contrôlant plusieurs RCN. Chaque RCN, à son tour, contrôle plusieurs sites de succursales. Même dans un déploiement multi-région, vous pouvez faire doubler le MCN en tant que nœud concentrateur direct pour un sous-ensemble des sites tout en demandant au reste des sites d'utiliser leurs RCN respectifs en tant que nœuds hub.

Les sites gérés directement par le MCN, c'est-à-dire les RCN, et potentiellement certains autres sites gérés directement par le MCN sont considérés comme se trouvant dans la région **par défaut** . La **région par défaut** serait la seule région d'un réseau avant que d'autres régions ne soient ajoutées. Après avoir ajouté d'autres régions, vous pouvez sélectionner l'option **Par défaut** pour utiliser la région souhaitée comme région par défaut.

Pour créer une région :

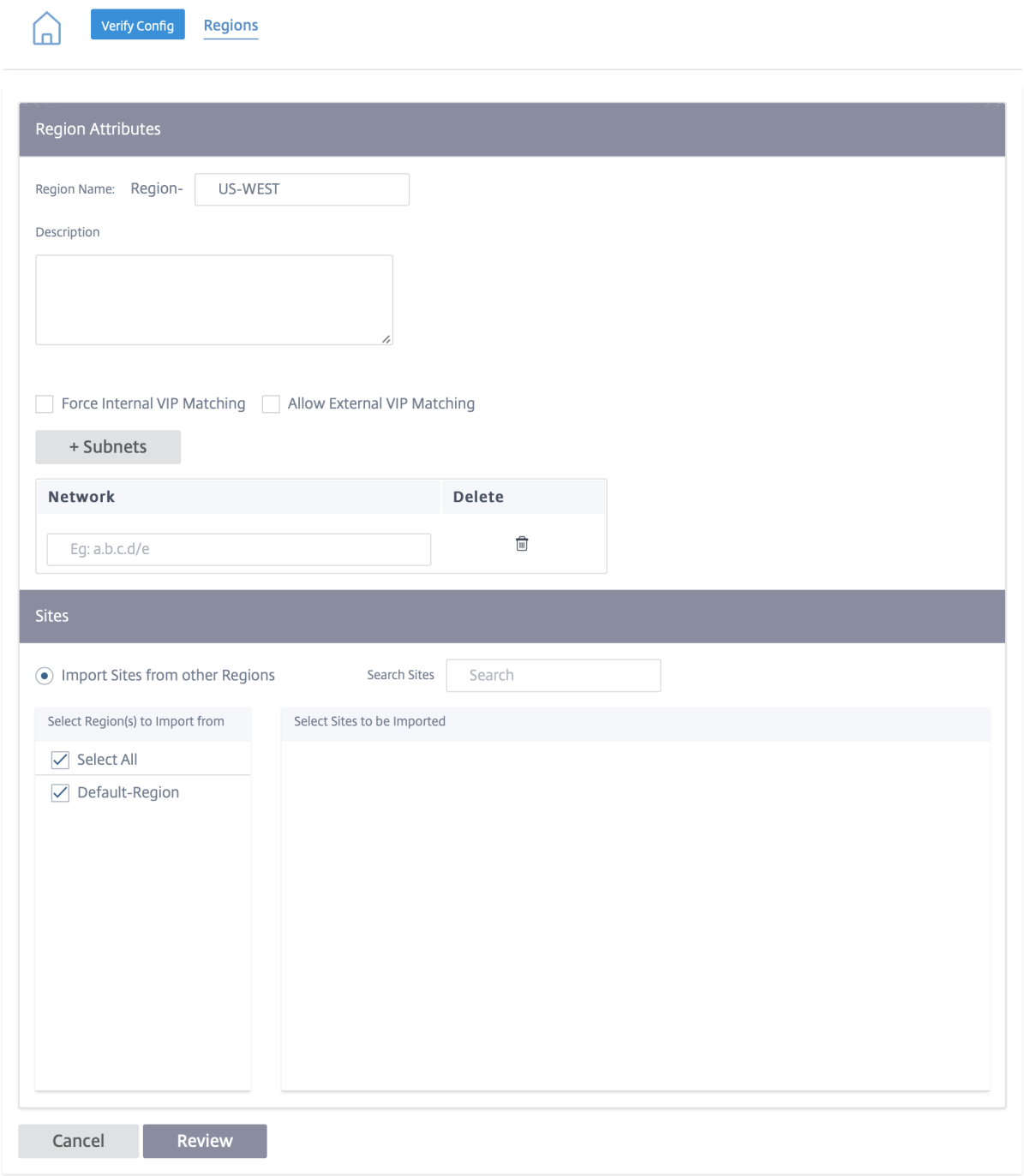
1. Cliquez sur **+ Région**. Fournissez un nom de région et une description.
2. Activez la correspondance VIP d'intervalle selon que vous souhaitez que la **correspondance VIP interne forcée** ou **Autoriser la correspondance VIP externe** .

    - Correspondance VIP interne forcée : Lorsque cette option est activée, toutes les adresses IP virtuelles non privées de la Région sont forcées de correspondre aux sous-réseaux configurés.
    - Correspondance VIP externe autorisée : Lorsque cette option est activée, les adresses IP virtuelles non privées provenant d'autres régions sont autorisées à correspondre aux sous-

réseaux configurés.

3. Cliquez sur **+ Sous-réseaux** pour ajouter des sous-réseaux. Entrez une adresse **réseau** . L'adresse réseau est l'adresse IP et le masque du sous-réseau.
4. Sélectionnez les sites.
5. Cliquez sur **Vérifier**, puis sur **Enregistrer**. La région nouvellement créée est ajoutée à la liste existante des régions.

> **Remarque**
>
> Un client ne peut disposer que de chemins virtuels statiques ou dynamiques au sein d'une région.



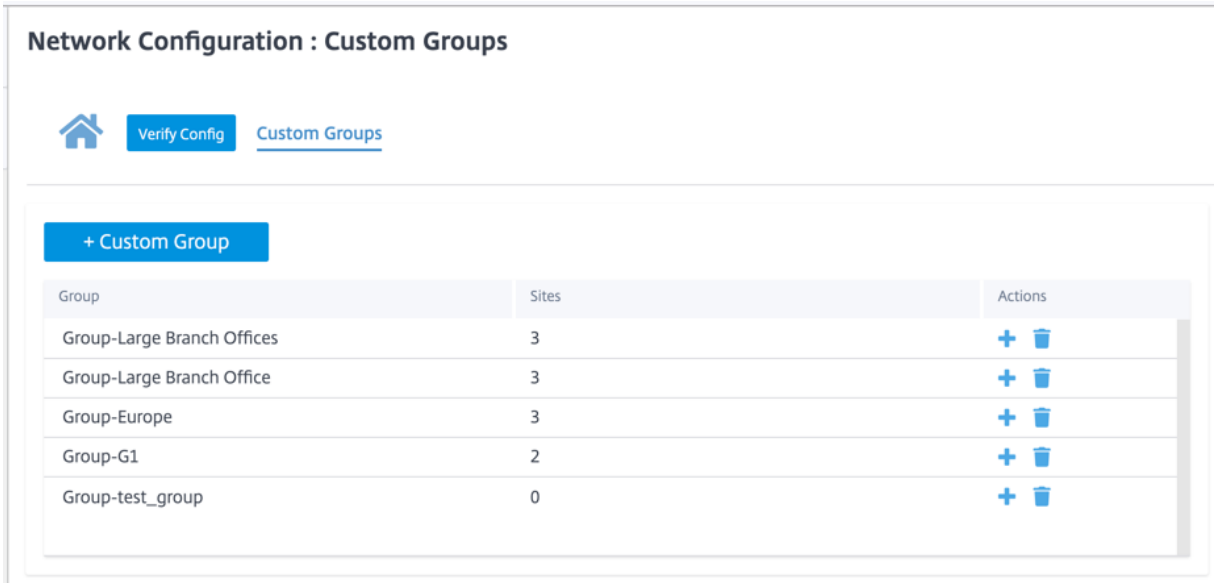
Vous pouvez placer des sites sous la région une fois qu'une région est créée avec succès.

> **Remarque**
>
> Les chemins virtuels dynamiques ne peuvent pas être établis entre des branches situées dans des régions différentes.

Cliquez sur **Vérifier la configuration** pour valider toute erreur d'audit.

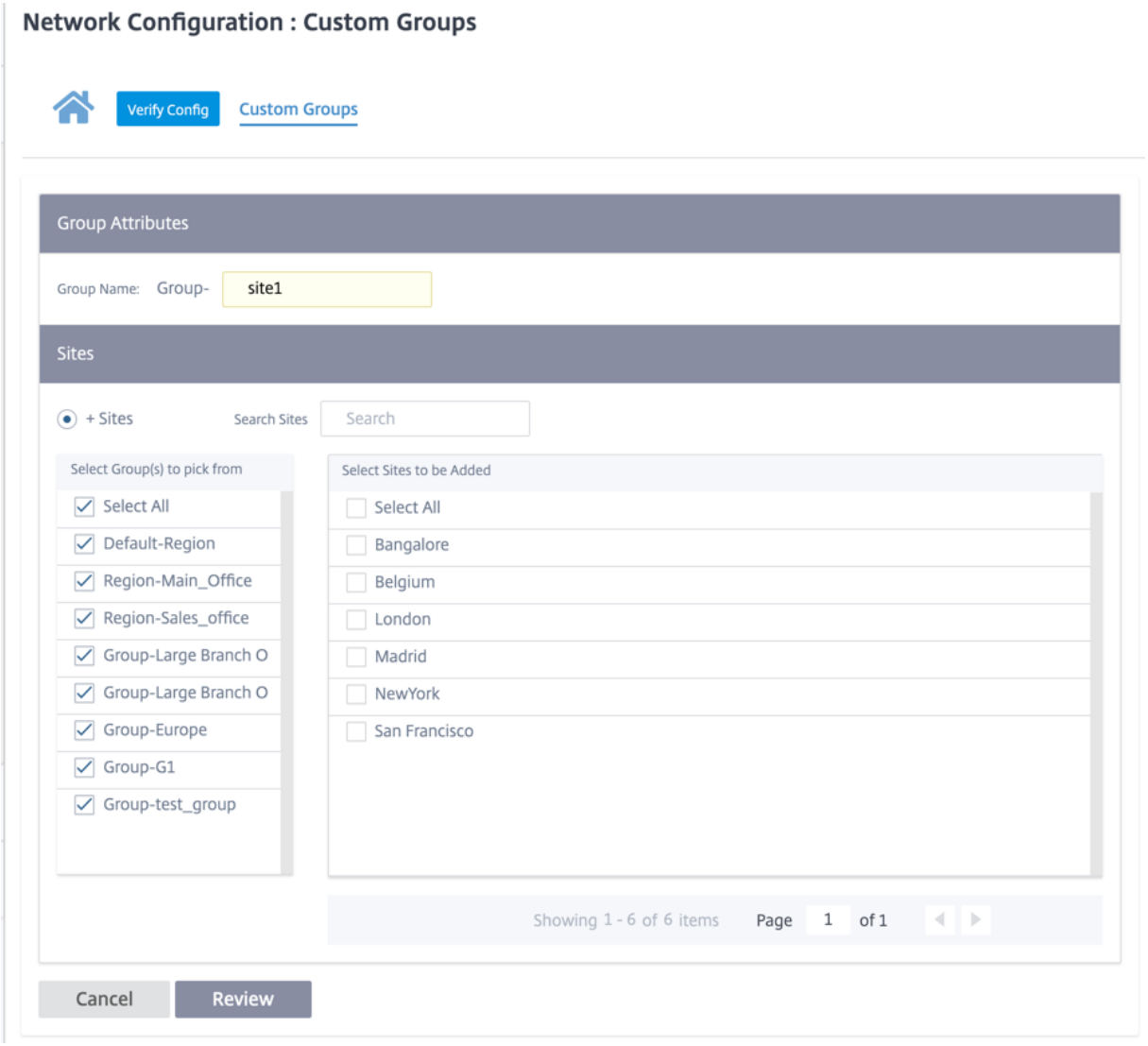
Groupes personnalisés

Les**groupes personnalisés** offrent aux utilisateurs la possibilité de regrouper des sites selon leurs besoins. Les utilisateurs peuvent appliquer des stratégies pour des groupes de sites à la fois, sans nécessairement avoir à traiter chaque site individuellement. Les groupes peuvent également servir de filtres pour les tableaux de bord, les rapports ou la configuration réseau. Contrairement aux régions, les groupes peuvent se chevaucher en termes de sites. En d'autres termes, les mêmes sites peuvent faire partie de plusieurs groupes.



Par exemple, un utilisateur peut créer un groupe nommé **Business Critical Sites** afin de configurer des politiques communes pour tous vos sites critiques. L'utilisateur peut également surveiller leur santé et leurs performances séparément en tant que groupe. Certains de ces sites peuvent également faire partie d'un groupe de **grandes succursales**, par exemple.

Les**groupes de sites personnalisés** permettent de regrouper logiquement des sites à des fins de création de rapports. Vous pouvez créer des groupes personnalisés et ajouter des sites à chaque groupe personnalisé. Pour créer un groupe personnalisé, cliquez sur **+ Groupe personnalisé**. Indiquez un nom de groupe et sélectionnez ou ajoutez des sites. Cliquez sur **Vérifier**, puis sur **Enregistrer**.

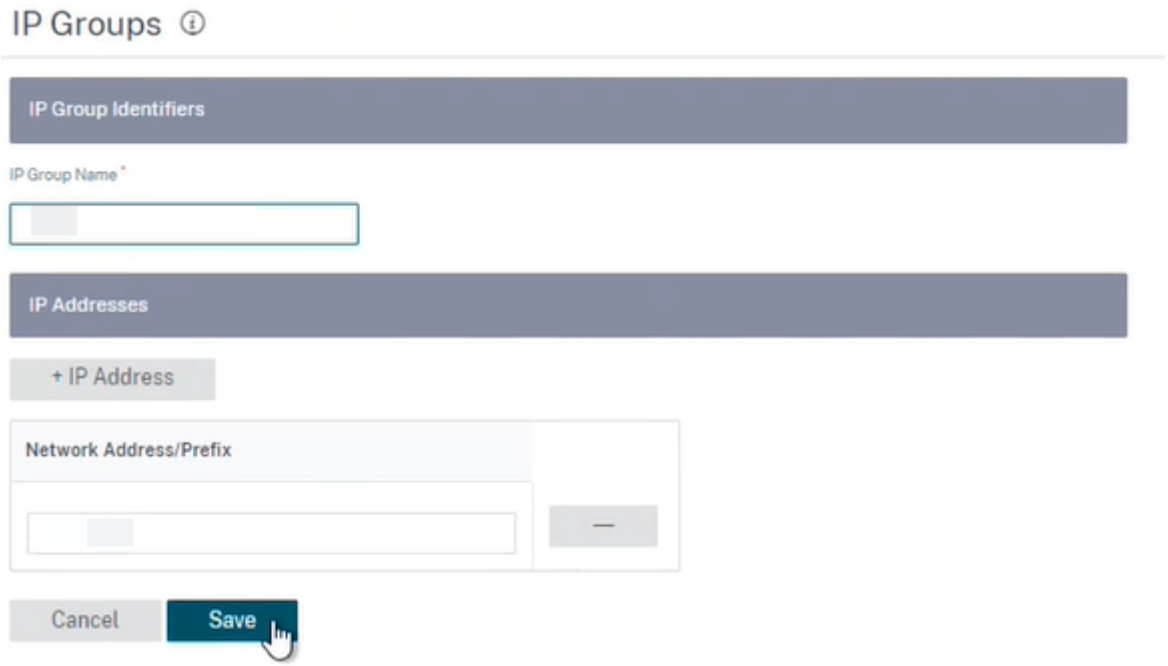


Cliquez sur **Vérifier la configuration** pour valider toute erreur d'audit.

Groupes IP

Le service Citrix SD-WAN Orchestrator introduit la possibilité d'ajouter des groupes IP (objets réseau). Avec cette option, vous pouvez regrouper des adresses IP et réseau à l'aide de **groupes IP** tout en définissant un filtre de routage plutôt que de créer un filtre pour chaque sous-réseau. Ces groupes peuvent être utilisés dans la configuration et les stratégies selon les besoins, sans nécessairement avoir à enfoncer chaque fois des adresses IP individuelles.

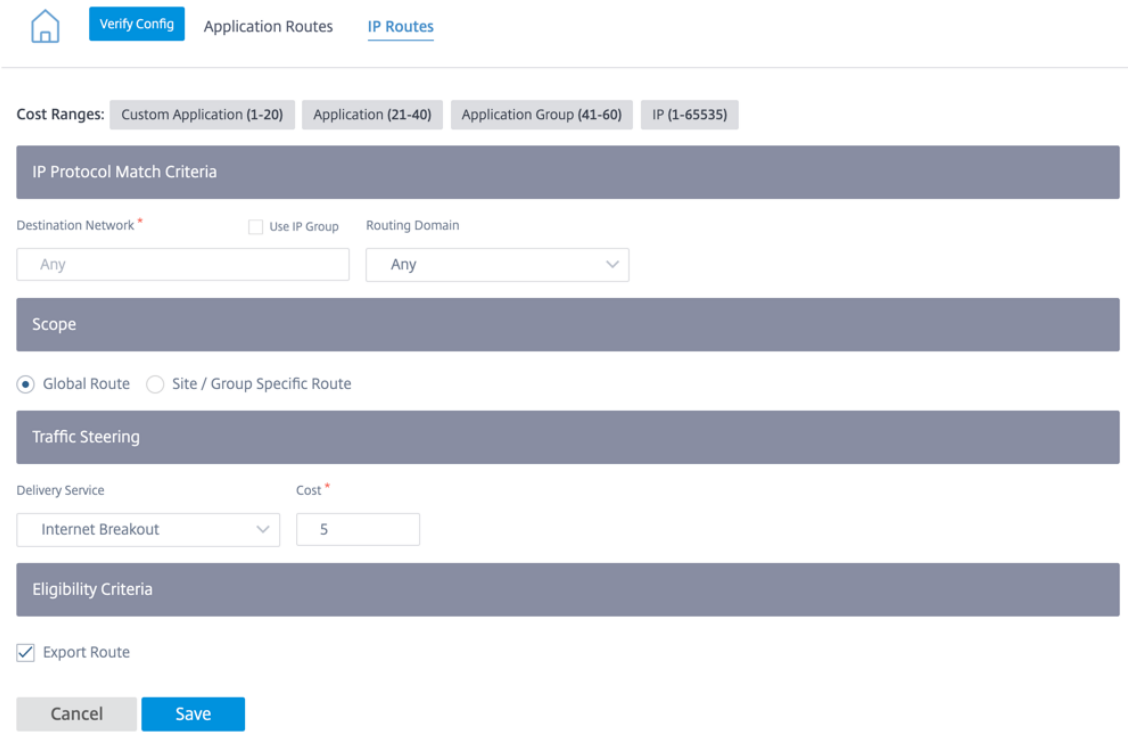
Vous pouvez créer des groupes IP et ajouter des adresses réseau et des préfixes. Pour créer un groupe IP, sélectionnez **Groupes IP** et cliquez sur **+ Groupe IP**. Indiquez un nom de groupe. Cliquez sur **+ Adresse IP** et entrez **les adresses IP** à ajouter au groupe IP.



Cliquez sur **Vérifier la configuration** pour valider toute erreur d'audit

Les fonctionnalités suivantes utilisent les groupes IP :

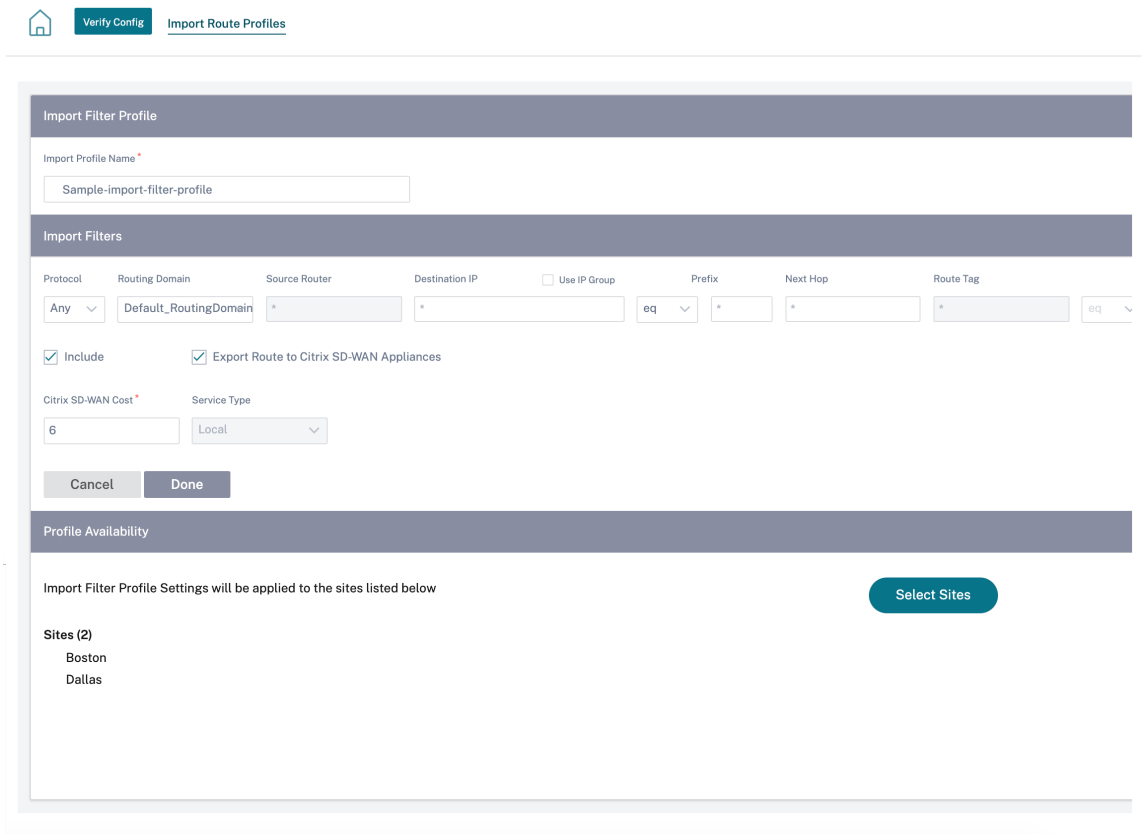
- **Création d'une route IP** : vous pouvez ajouter un réseau de destination ou activer la case à cocher **Utiliser un groupe IP** pour sélectionner un groupe IP existant. Pour plus d'informations, consultez la section Groupes d'adresses IP.



- **Importer des profils de route** : lors de la création d'un profil de filtre d'importation, vous pouvez choisir parmi la liste des groupes IP disponibles sur votre réseau.

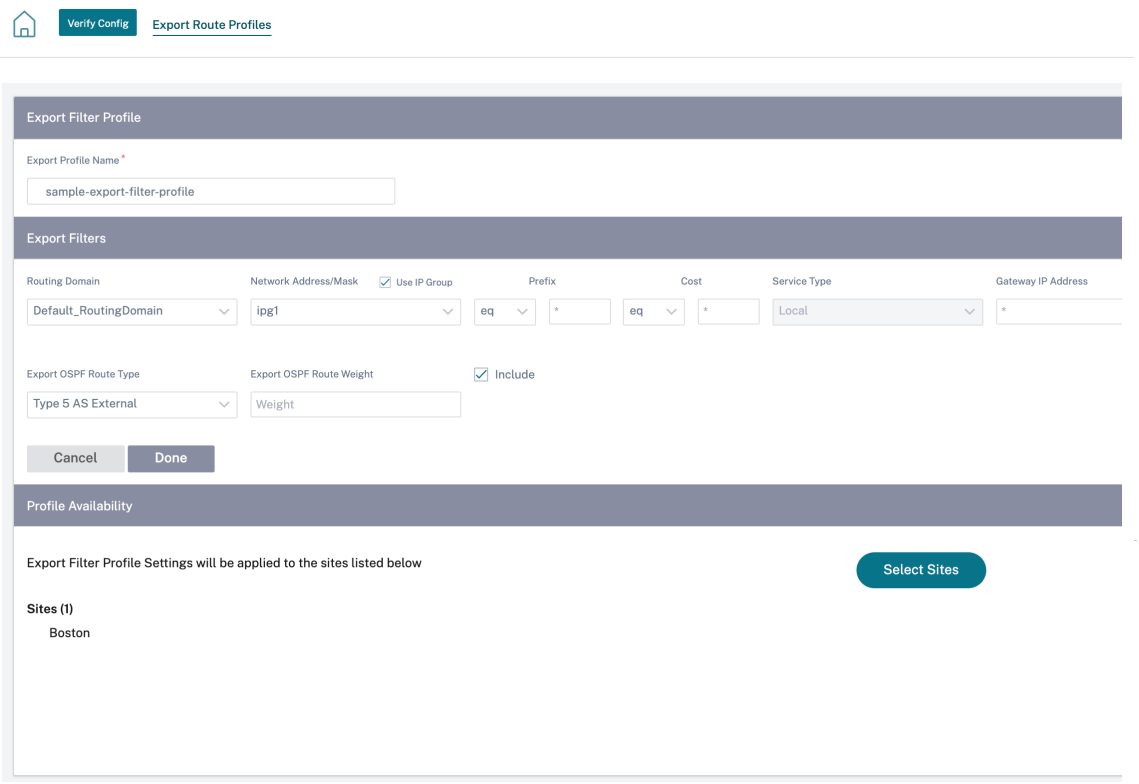
  Vous pouvez ajouter un réseau de destination ou activer la case à cocher **Utiliser un groupe IP** pour sélectionner un groupe IP existant.

  Pour plus d'informations, voir Importer des profils d'itinéraires.



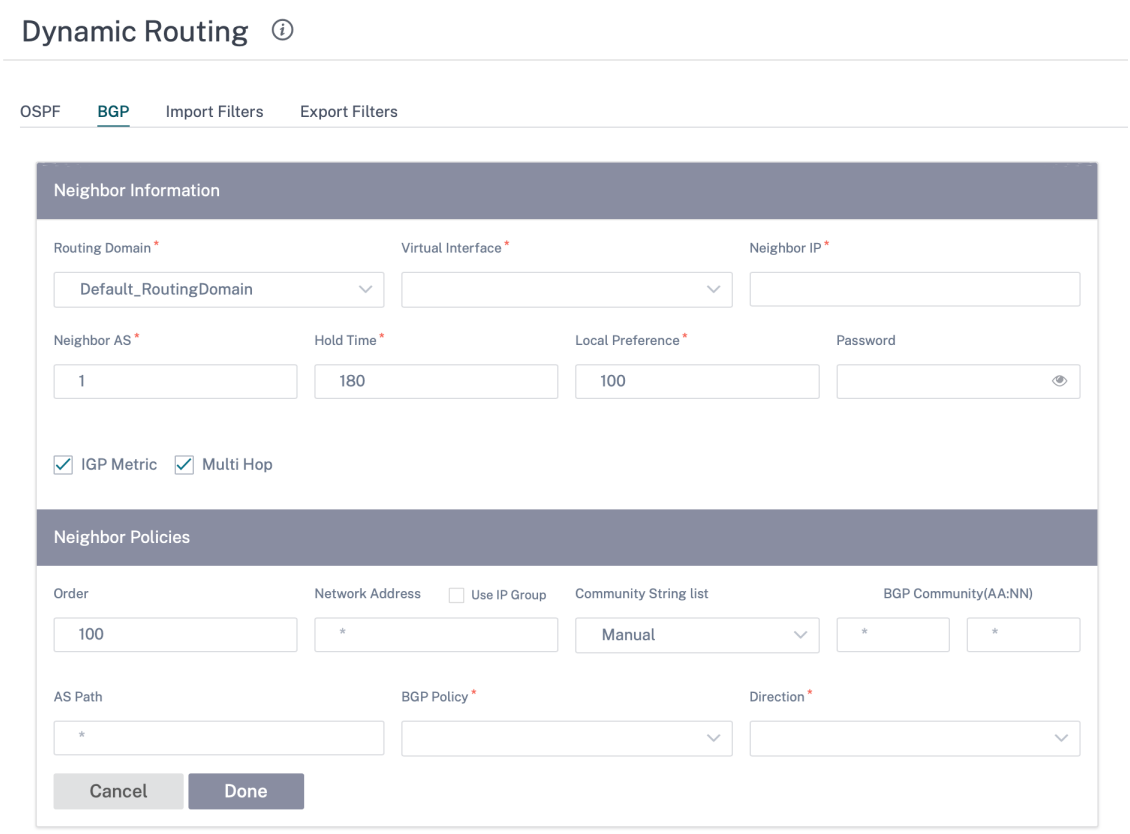
- **Exporter les profils de route** : lors de la création d'un profil de filtre d'exportation, vous pouvez ajouter un masque d'adresse réseau ou activer la case à cocher **Utiliser un groupe IP** pour sélectionner un groupe IP existant.

  Pour plus d'informations, voir Exporter des profils d'itinéraires.



- **Politiques de voisinage BGP** : lors de l'ajout d'une politique BGP configurée pour les routeurs voisins, vous pouvez ajouter une adresse réseau ou activer la case à cocher **Utiliser un groupe IP** pour sélectionner un groupe IP existant.

  Pour plus d'informations, voir BGP.



Paramètres et groupes de l'application

October 21, 2022

Cette section permet aux utilisateurs de définir des applications personnalisées, de regrouper des applications à utiliser dans des stratégies, des profils QoS et des paramètres DNS.

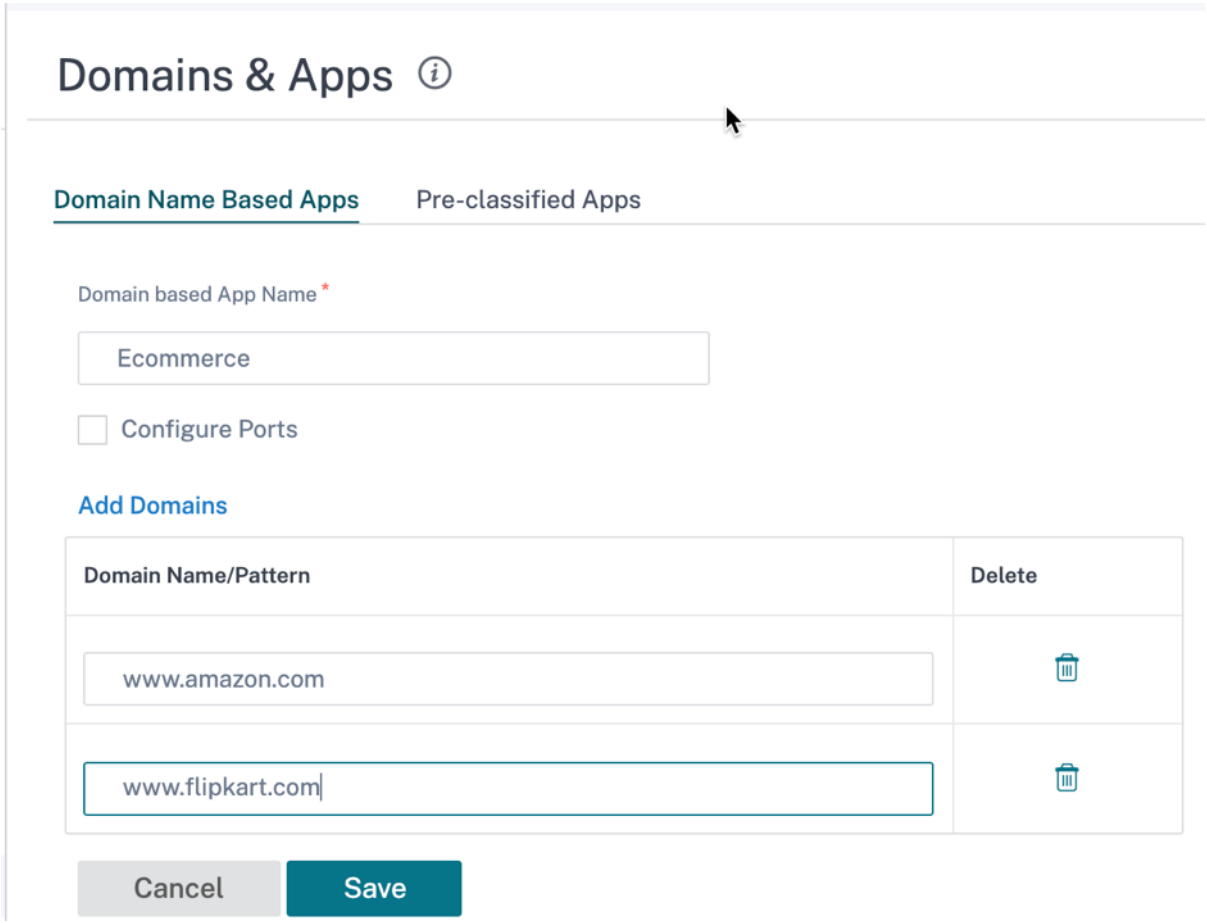
Vous pouvez définir un **groupe d'applications** pour les applications prédéfinies et personnalisées. Un **groupe** d'applications contient des applications qui nécessitent un traitement similaire lors de la définition d'une politique de sécurité.

Vous pouvez réutiliser fréquemment les **groupes d'applications** lorsque vous définissez des politiques telles que le pilotage des applications ou les règles de pare-feu. Il élimine le besoin de créer plusieurs entrées pour chaque application individuelle. De même, lors de l'utilisation de tous les services d'application, Groupes d'applications prend en charge les applications courantes avec un nom unique pour une réutilisation simplifiée et cohérente.

Pour afficher les **groupes d'applications**, accédez à **Configuration > Paramètres et groupes de l'application**.

Domaines et applications

Vous pouvez créer des applications internes basées sur des noms de domaine qui ne figurent pas dans la liste des applications publiées sur la page **Domaines et applications** . Pour créer des applications basées sur un nom de domaine, au niveau du réseau, accédez à **Paramètres et groupes de l'application > Domaines et applications > onglet Applications basées sur un nom de domaine**, puis cliquez sur **Nouvelle application basée sur un nom de domaine**. Entrez le nom de l'application et ajoutez les noms de domaine ou les modèles. Vous pouvez entrer le nom de domaine complet ou utiliser des caractères génériques au début.



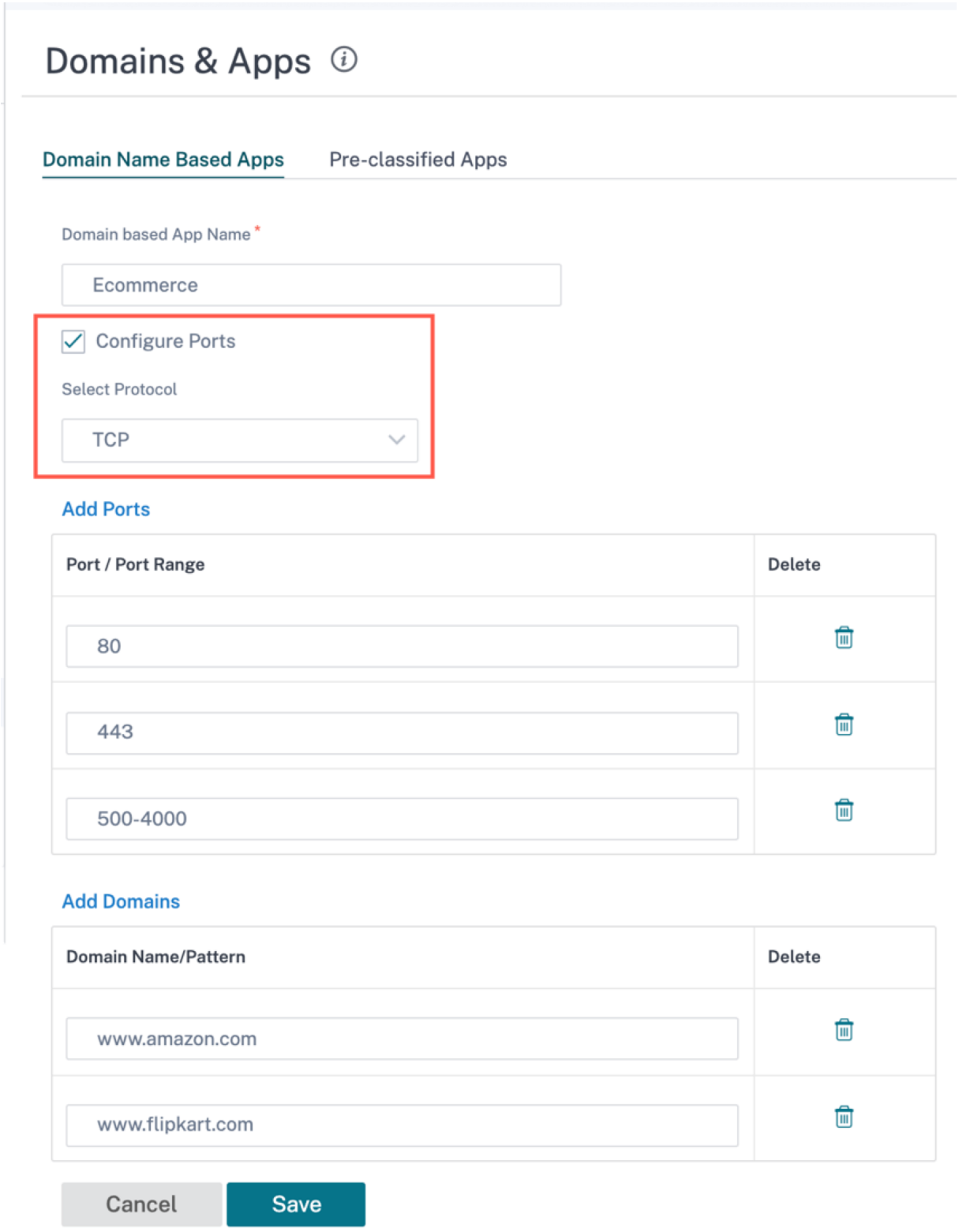
Toutes les applications basées sur des noms de domaine sont visibles dans le **routage des applications**, les **règles d'application**et **les politiques de pare-feu**.

À partir de la version 11.4.2 de Citrix SD-WAN, l'option **Configurer les ports** est disponible sous **Applications basées sur des noms de domaine**. Lorsque la case **Configurer les ports** est cochée, elle permet de configurer un groupe de plusieurs ports, plages de ports et un protocole (TCP/UDP/Any) pour l'application basée sur le domaine.

Auparavant, les ports **80** et **443**et le protocole **Any** étaient pris en charge pour les domaines regroupés dans une application. Vous pouvez voir le même comportement si la case **Configurer les ports** est

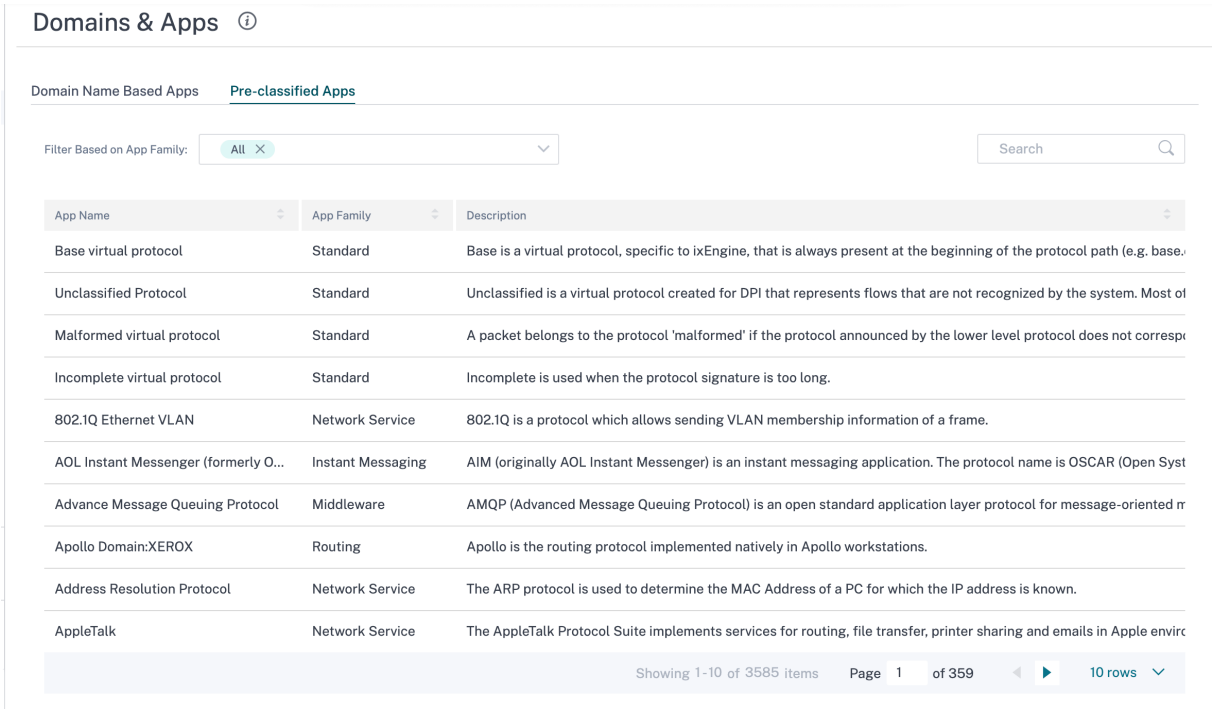
désactivée. Par défaut, la case à cocher **Configurer les ports** est désactivée.

Lorsque vous cochez la case **Configurer le port**, vous pouvez modifier, ajouter ou supprimer n'importe quel port ou la plage de ports selon les besoins, tout en sélectionnant le protocole TCP, UDP ou N'importe quel. Par défaut, la valeur du protocole est définie sur **Any** et les ports sont définis sur **80** et **443**.



Vous pouvez également consulter la liste des applications prédéfinies sous l'onglet **Applications pré-**

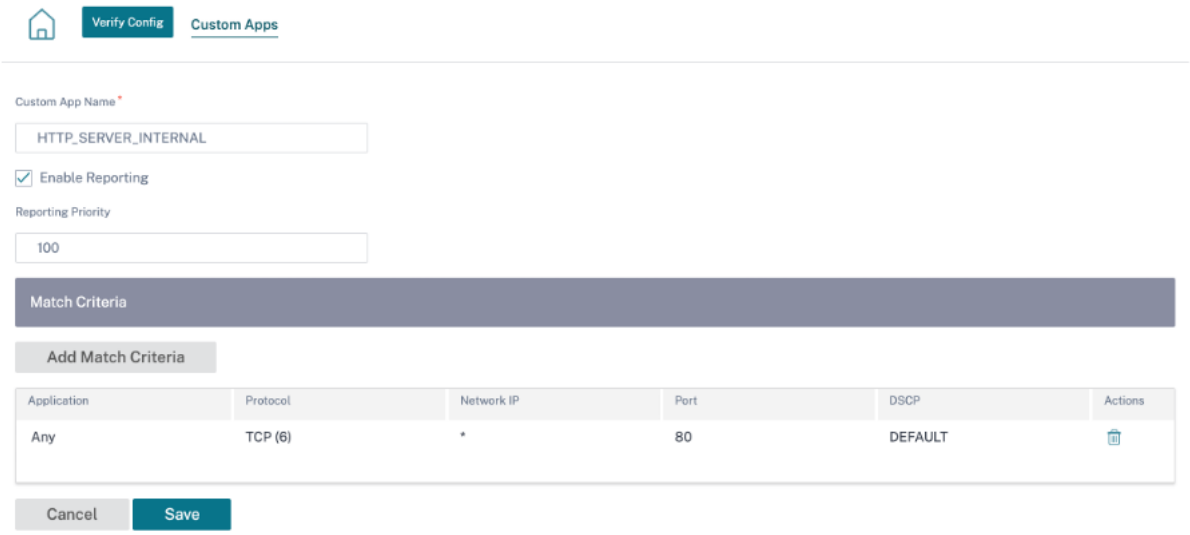
classées . Vous pouvez rechercher une application spécifique à l'aide de la barre **de recherche** ou filtrer la liste en fonction de la famille d'applications.



Application personnalisée

Les **applications personnalisées** sont utilisées pour créer des applications internes ou des combinaisons de ports IP qui ne sont pas disponibles dans la liste des applications publiées. L'administrateur doit définir une application personnalisée basée sur le protocole IP qui peut être utilisée dans plusieurs politiques selon les besoins, sans se référer à chaque fois aux détails de l'adresse IP et du numéro de port.

Pour créer une application personnalisée, au niveau du réseau, accédez à **Paramètres et groupes de l'application > Applications personnalisées**, cliquez sur **+ Application personnalisée** et entrez un nom pour l'application personnalisée. Spécifiez les critères de correspondance tels que le protocole IP, l'adresse IP réseau, le numéro de port et la balise DSCP. Le flux de données correspondant à ce critère est regroupé en tant qu'application personnalisée.

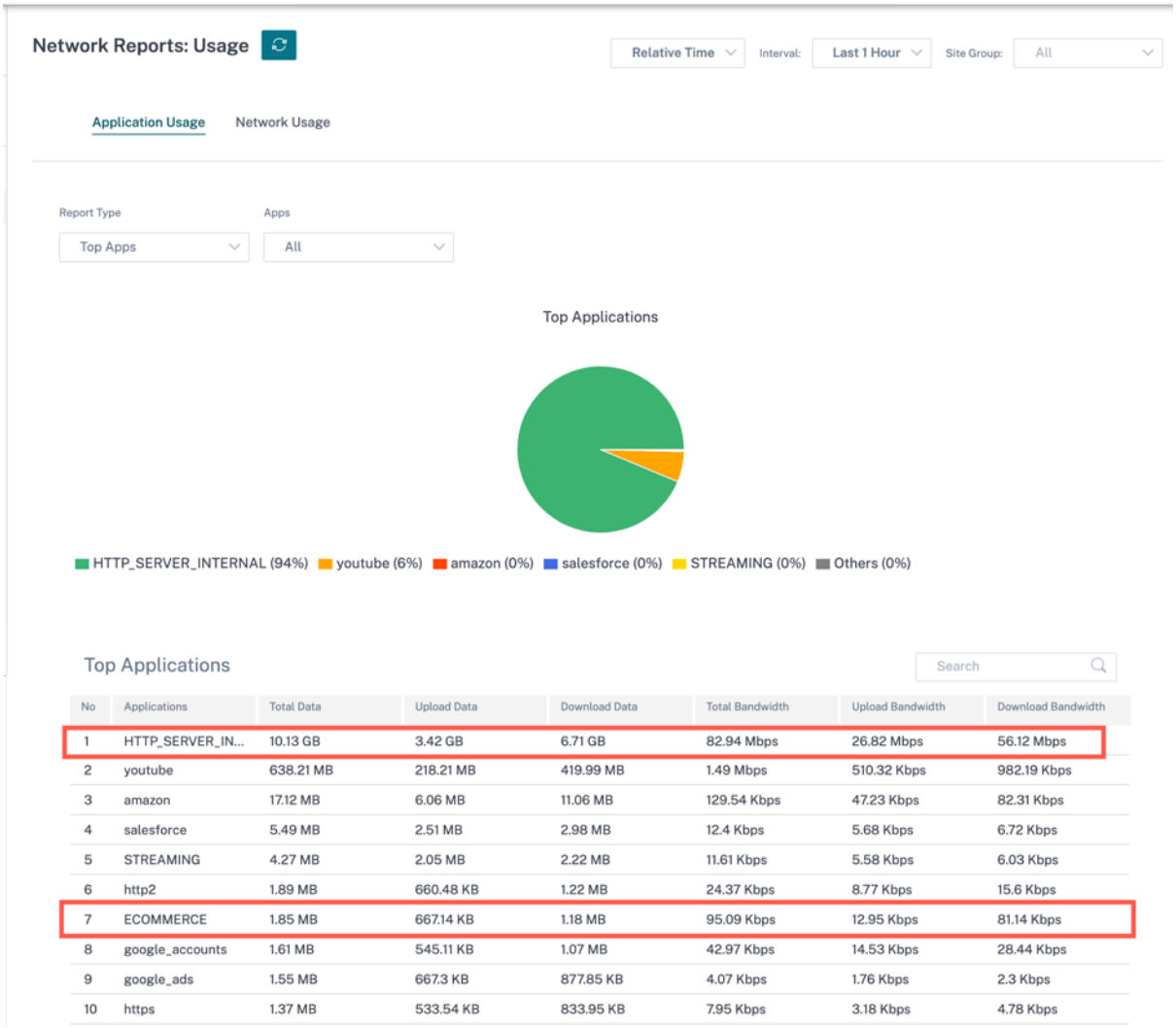


Une fois enregistrées, les applications personnalisées apparaissent dans une liste et peuvent être modifiées ou supprimées, selon les besoins.

La case à cocher **Activer les rapports** est ajoutée pour les applications personnalisées et les groupes d'applications basés sur le protocole IP. Vous devez cocher la case **Activer les rapports** et indiquer la priorité des rapports.

Lorsque la case **Activer les rapports** est cochée, vous pouvez consulter le trafic des applications personnalisées IP sous **Rapports** > **Utilisation**.

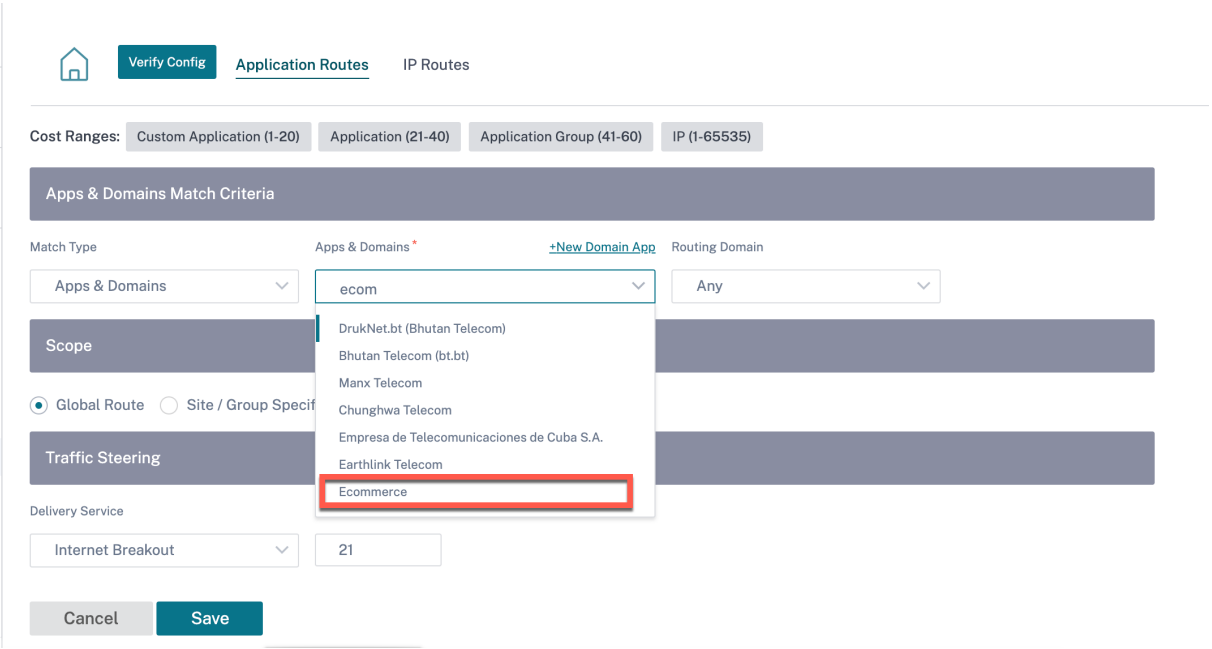
La priorité des rapports est l'ordre dans lequel les applications personnalisées ou les groupes d'applications basés sur le protocole IP sont sélectionnés pour les rapports. Il est utile de choisir l'application personnalisée ou le groupe d'applications à priorité élevée pour les rapports, lorsqu'il existe plusieurs correspondances lorsque la génération de rapports est activée. Par exemple, si la priorité de génération de rapports d'une application personnalisée est définie sur 1, cela signifie que l'application personnalisée obtient la priorité la plus élevée dans les rapports. Alors que si la priorité de reporting est définie sur 100, l'application personnalisée prend une priorité bien moindre en matière de reporting.



Remarque

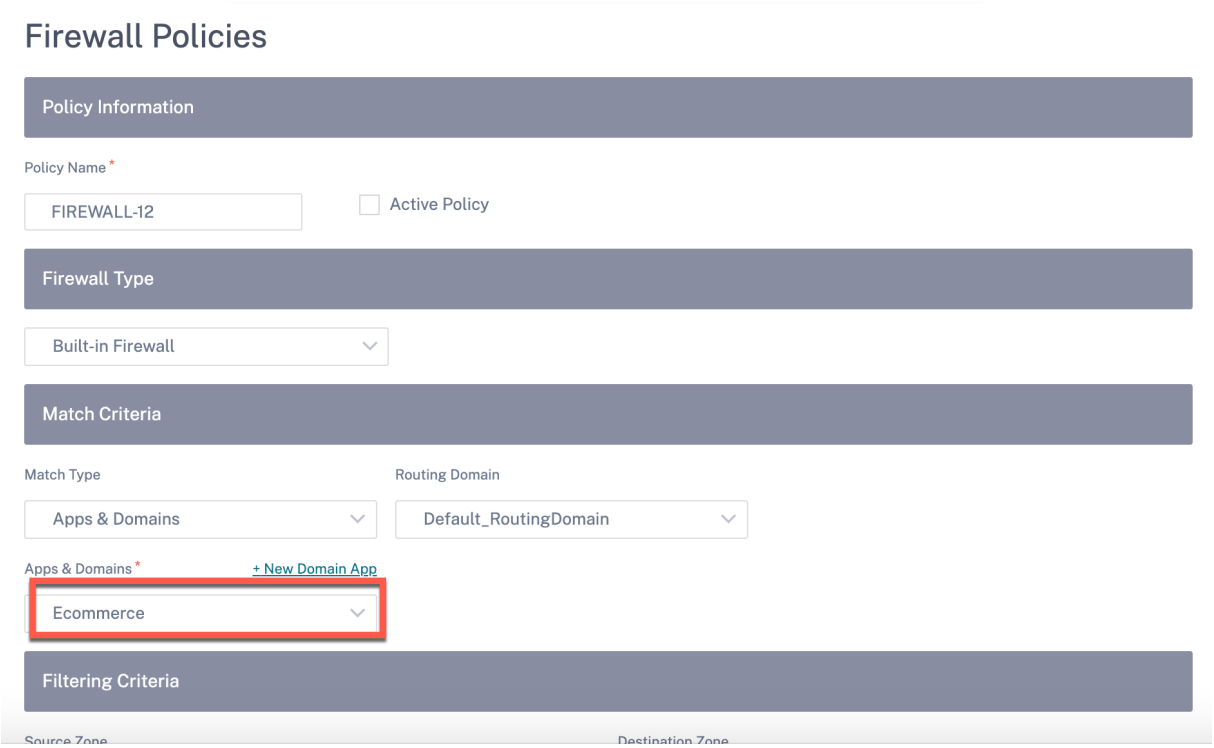
- Pour que vous puissiez utiliser une application basée sur un nom de domaine, **les applications et les domaines** doivent être répertoriés comme critères de correspondance lors de la création de l'itinéraire des applications, de la politique de qualité de service et de la politique de pare-feu.
- Pour que vous puissiez utiliser une application personnalisée, l'**application personnalisée** doit être répertoriée comme critère de correspondance lors de la création de l'itinéraire de l'application, de la politique de QoS et de la politique de pare-feu.

Une fois que vous avez créé l'application personnalisée, pour effectuer le routage de l'application, accédez à **Routage > Politiques de routage > + Route de l'application**, sélectionnez **Application personnalisée** dans la liste déroulante **Type de correspondance** . De même, pour l'application basée sur un nom de domaine, sélectionnez **Applications et domaines** dans la liste déroulante **Type de correspondance** .

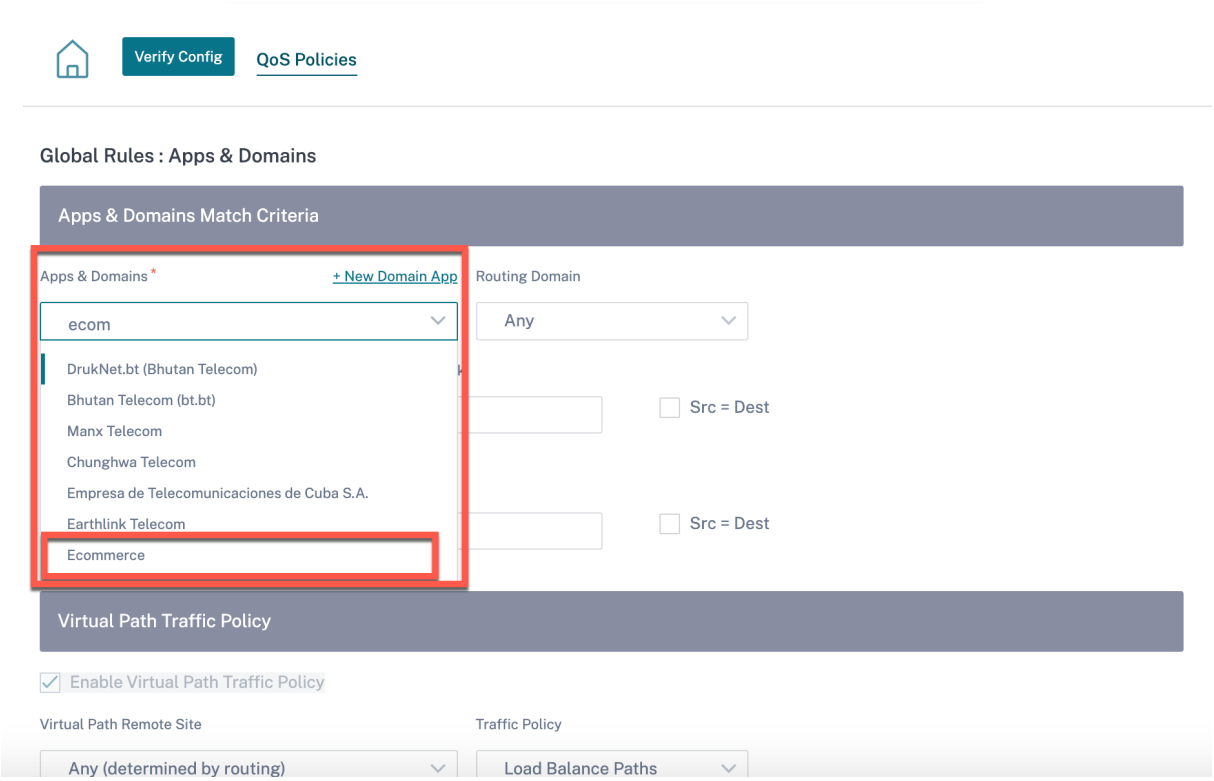


Vous pouvez également sélectionner une application basée sur un nom de domaine selon les critères de correspondance lors de la création d'une application personnalisée de **protocole IP** .

De même, pour afficher l'application personnalisée sous les **politiques de pare-feu**, accédez à **Sécurité > Stratégies de pare-feu**. L'application peut être utilisée pour tout type de politique (remplacement global/spécifique au site/politiques globales). Cliquez sur **Créer une nouvelle règle** et, sous **Critères de correspondance**, sélectionnez **Application personnalisée** dans la liste déroulante **Type de correspondance** . Pour afficher l'application basée sur un nom de domaine, sélectionnez **Applications et domaines** dans la liste déroulante **Type de correspondance** .



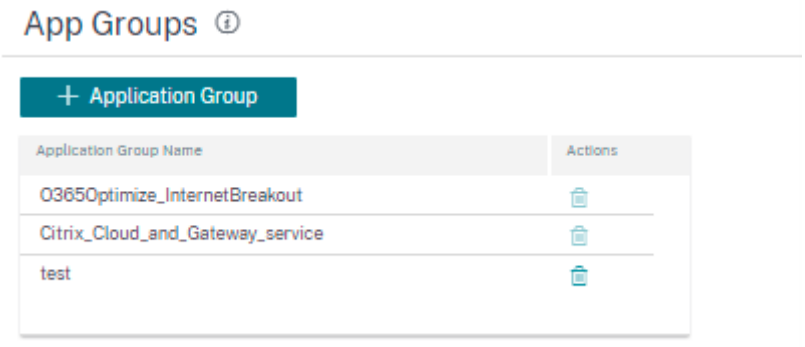
Vous pouvez consulter les applications personnalisées basées sur des noms de domaine à la fois sous Règle **globale ou Règle spécifique au site/au groupe**. Pour afficher les applications basées sur des noms de domaine, accédez à **QoS > Politiques de QoS > Règles globales > Règle d'application > + Règle**d'application, puis sélectionnez l'application basée sur le nom de domaine requise dans la liste déroulante **Applications et domaines** . Pour afficher les applications personnalisées, accédez à **QoS > Politiques de QoS > Règles globales > Règles d'application personnalisées > + Règle d'application personnalisée**, puis sélectionnez l'application personnalisée requise dans la liste déroulante des **applications personnalisées** .



Cliquez sur **Vérifier la configuration** pour valider toute erreur d'audit.

Groupes d'applications

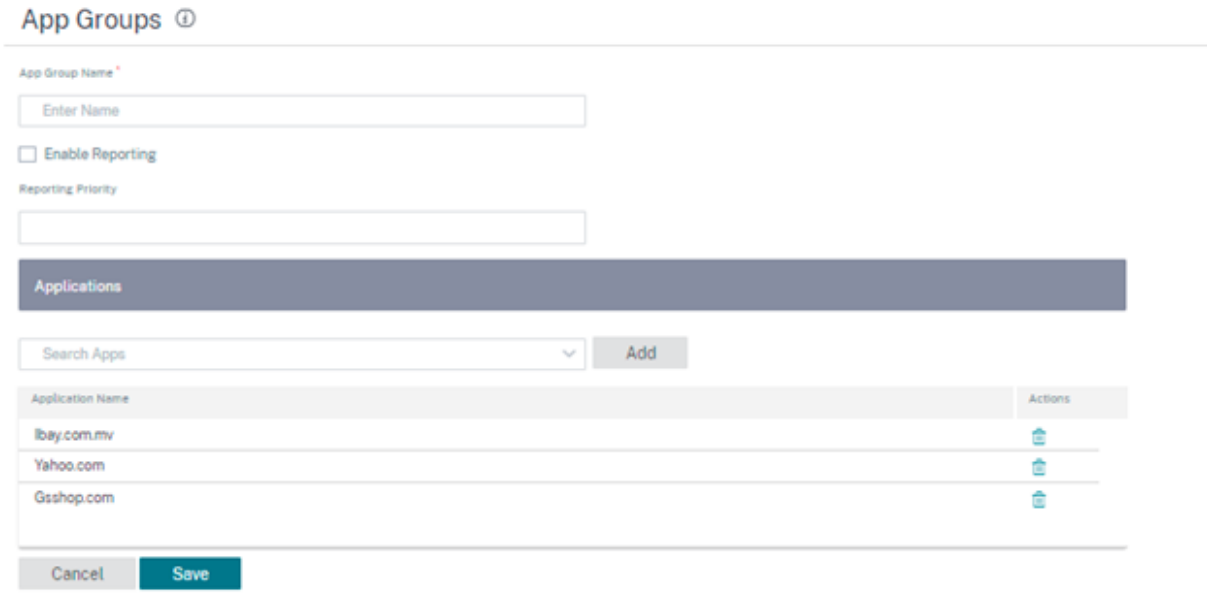
Un **groupe d'applications** permet aux administrateurs de regrouper des applications similaires afin de les utiliser dans des politiques communes, sans nécessairement avoir à créer une politique pour chaque application individuelle.



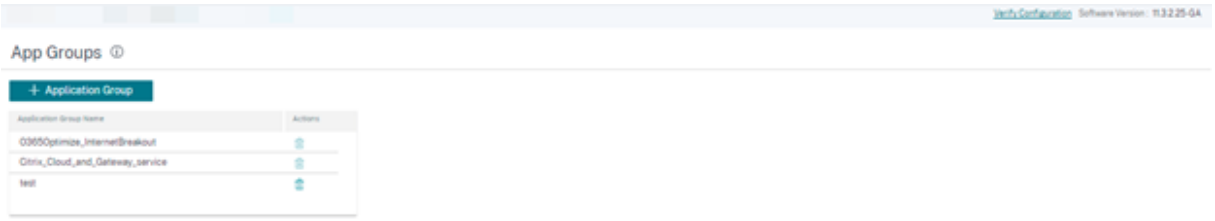
Vous pouvez créer un **groupe d'applications** à l'aide de l'option **Ajouter des groupes d'applications** . Vous pouvez référer le même groupe d'applications lors de la création d'une stratégie conformément au rôle d'application. La stratégie définie pour le groupe particulier est appliquée à chaque application correspondant à la catégorie spécifique.

Par exemple, vous pouvez créer un **groupe d'applications** en tant que **réseau social** et ajouter des réseaux sociaux tels que Facebook, LinkedIn et Twitter au groupe afin de définir certaines politiques pour les applications de réseaux sociaux.

Pour créer un **groupe d'applications**, spécifiez un nom de groupe, recherchez et ajoutez des applications dans la liste des **applications** .
Vous pouvez toujours revenir en arrière et modifier vos paramètres ou supprimer le **groupe d'applications** selon vos besoins.

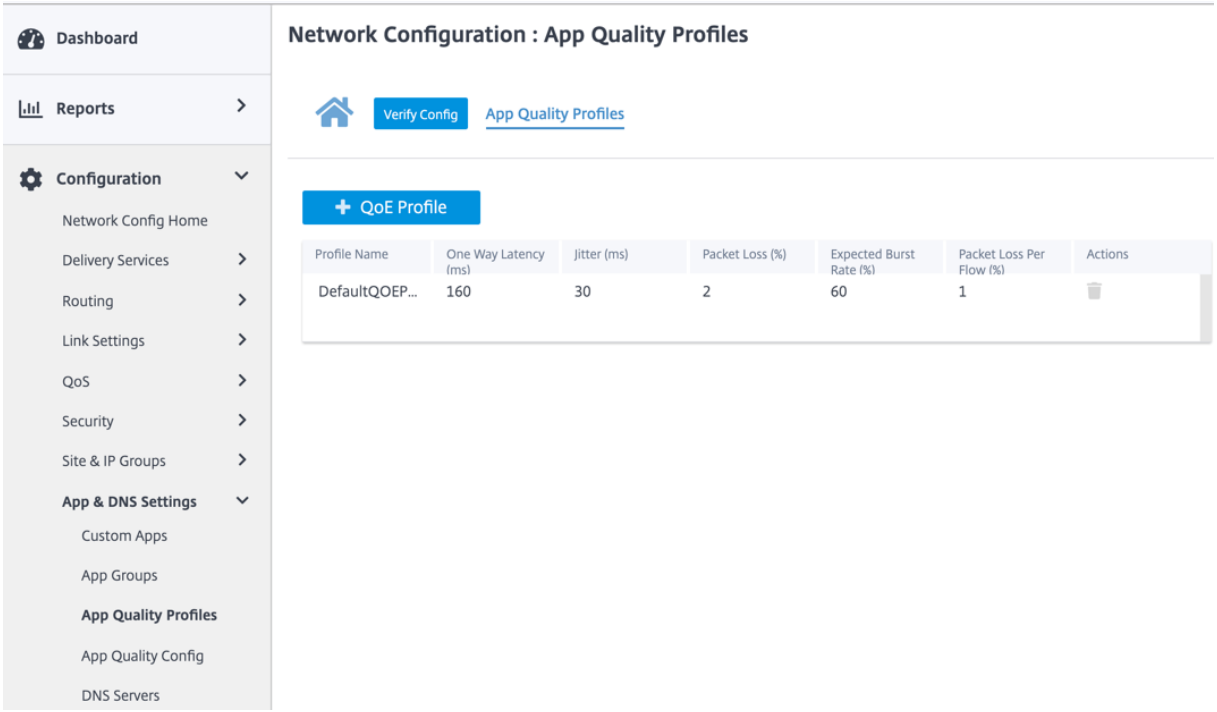


Cliquez sur **Vérifier la configuration** sur la page **Configuration** > **Paramètres et groupes** d'**applications > Groupes** d'applications pour valider toute erreur d'audit.



Profils de qualité des applications

Cette section vous permet d'afficher et de créer des profils de qualité d'application.



La**QoE des applications** est une mesure de la qualité d'expérience des applications dans le réseau SD-WAN. Il mesure la qualité des applications qui circulent à travers les chemins virtuels entre deux appliances SD-WAN.

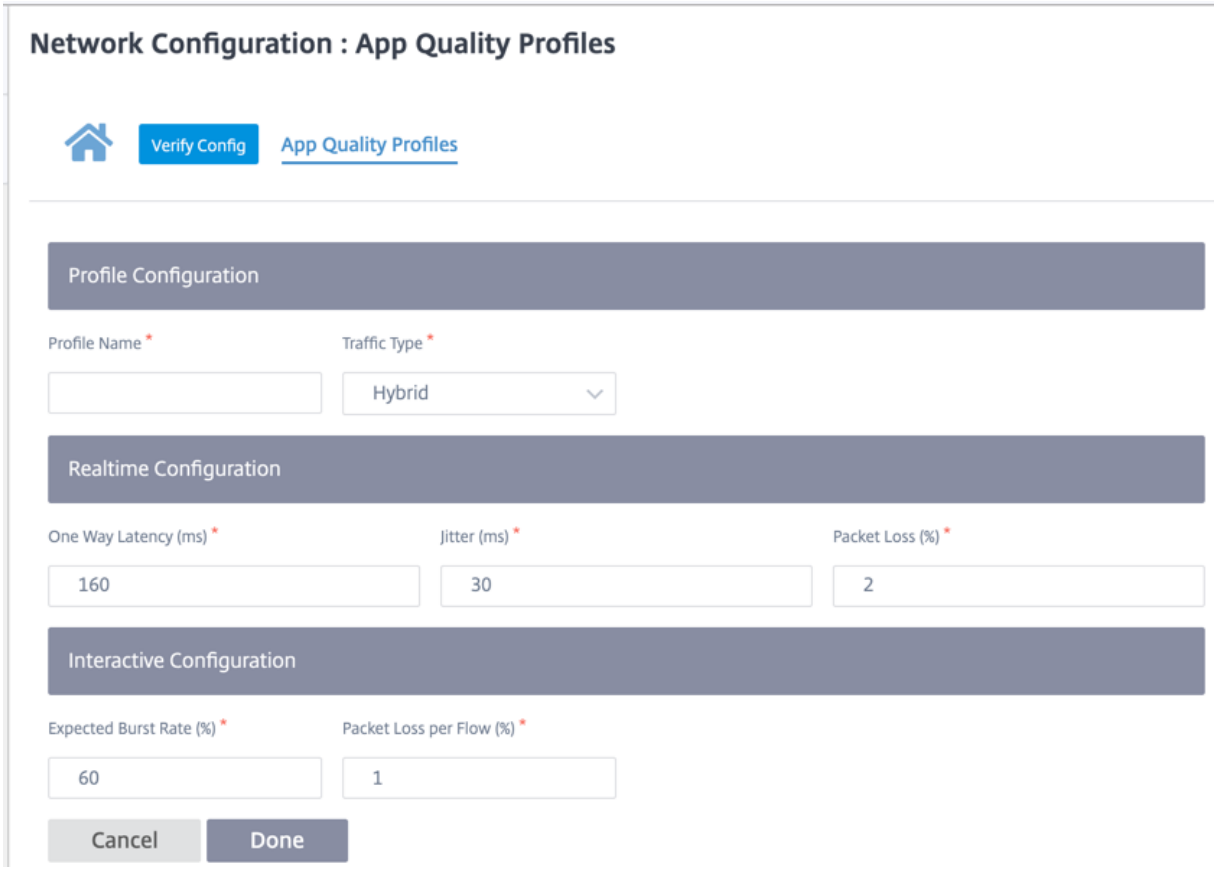
Le score QoE de l'application est une valeur comprise entre 0 et 10. La plage de score dans laquelle elle se trouve détermine la qualité d'une application.

Qualité	Gamme
Good	8–10
Fair	4–8
Poor	0–4

Le score QoE de l'application peut être utilisé pour mesurer la qualité des applications et identifier les tendances problématiques.

Configuration du profil

Cliquez sur **+ Profil QoE** pour créer un profil QoE, spécifier un nom de profil et sélectionner un type de trafic dans la liste déroulante.



Configuration en temps réel

Vous pouvez définir les seuils de qualité pour les appliances interactives et en temps réel à l'aide de profils QoE, et mapper ces profils avec des applications ou des objets d'applications.

Le calcul de QoE d'application pour les applications en temps réel utilise une technique innovante Citrix, qui est dérivée du score MOS.

Les valeurs de seuil par défaut sont les suivantes :

- Seuil de latence (ms) : 160
- Seuil de gigue (ms) : 30
- Seuil de perte de paquets (%) : 2

Un flux d'une application en temps réel qui respecte les seuils de latence, de perte et de gigue est considéré comme de bonne qualité.

La QoE pour les applications en temps réel est déterminée à partir du pourcentage de flux qui atteignent le seuil divisé par le nombre total d'échantillons de flux.

QoE pour temps réel = (Nombre d'échantillons de débit qui atteignent le seuil/Nombre total d'échantillons de débit) * 100

Il est représenté par un score QoE allant de 0 à 10.

Configuration interactive

La QoE des applications pour les applications interactives utilise une technique innovante Citrix basée sur les seuils de perte de paquets et de taux de rafale.

Les applications interactives sont sensibles à la perte de paquets et au débit. Par conséquent, nous mesurons le pourcentage de perte de paquets et le taux d'éclatement du trafic d'entrée et de sortie dans un flux.

Les seuils configurables sont :

- Pourcentage de perte de paquets.
- Pourcentage du taux d'éclatement prévu par rapport au taux d'éclatement d'entrée.

Les valeurs de seuil par défaut sont les suivantes :

- Seuil de perte de paquets : 1%
- Taux d'éclatement : 60%

Un flux est de bonne qualité si les conditions suivantes sont remplies :

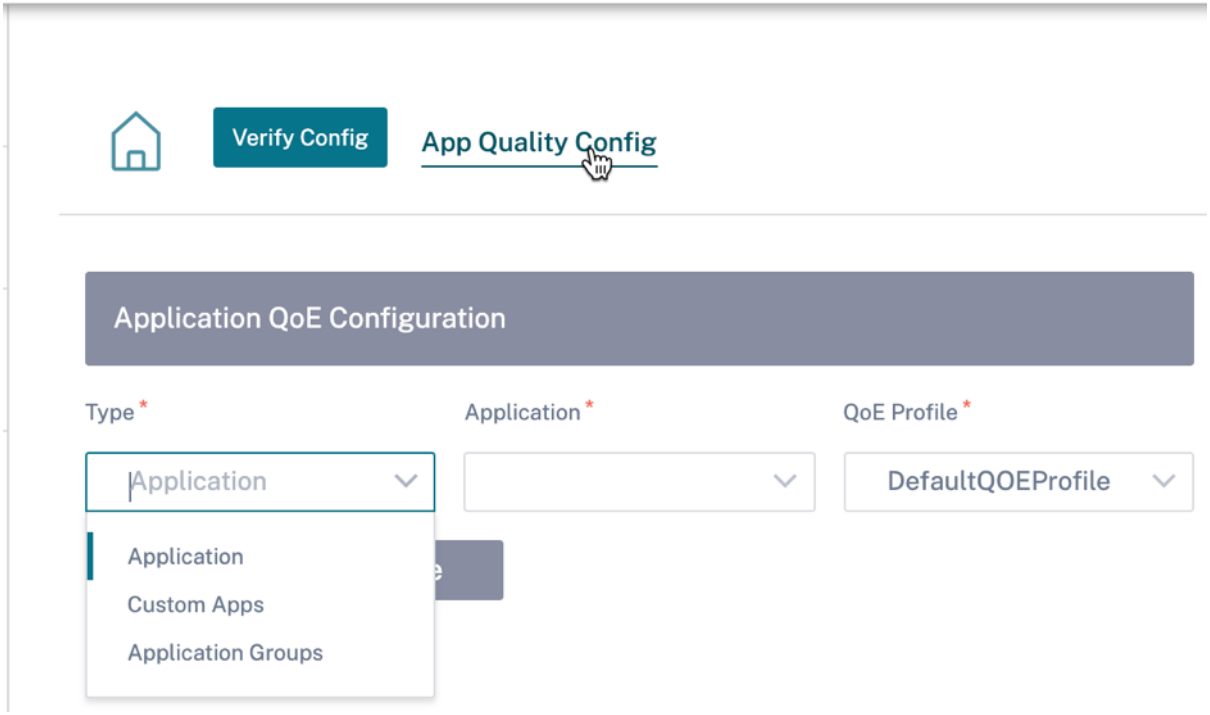
- Le pourcentage de perte pour un flux est inférieur au seuil configuré.
- Le taux de rafale de sortie est au moins le pourcentage configuré du taux de rafale d'entrée.

Configuration de la qualité des applications

Mappez des objets d'application ou d'application à des profils QoE par défaut ou personnalisés. Vous pouvez créer des profils QoE personnalisés pour un trafic interactif et en temps réel.

Cliquez sur **+Configuration QoE** pour créer des profils QoE personnalisés :

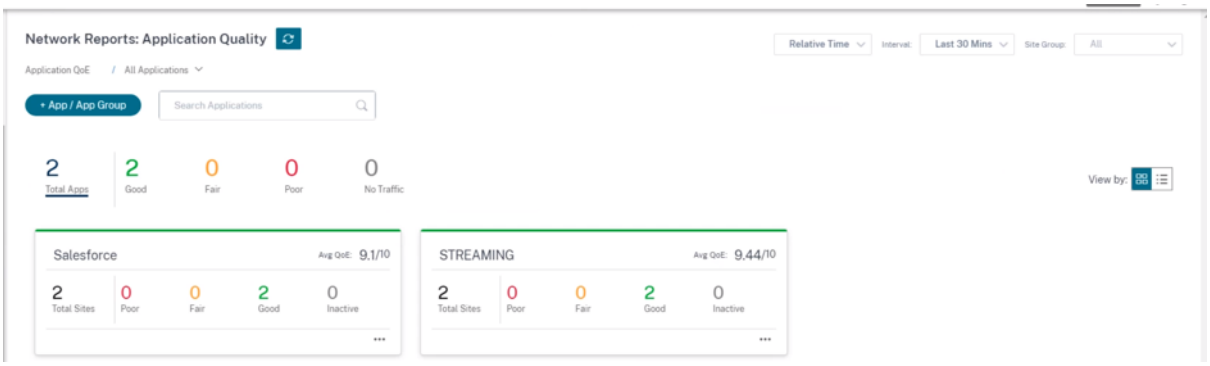
- **Type** : Sélectionnez l'application DPI ou un objet d'application (application, applications personnalisées et groupes d'applications).
- **Application** : recherchez et sélectionnez une application ou un objet d'application en fonction du type sélectionné.
- **Profil QoE** : sélectionnez un profil QoE à mapper à l'application ou à l'objet d'application.



Cliquez sur **Terminé**.

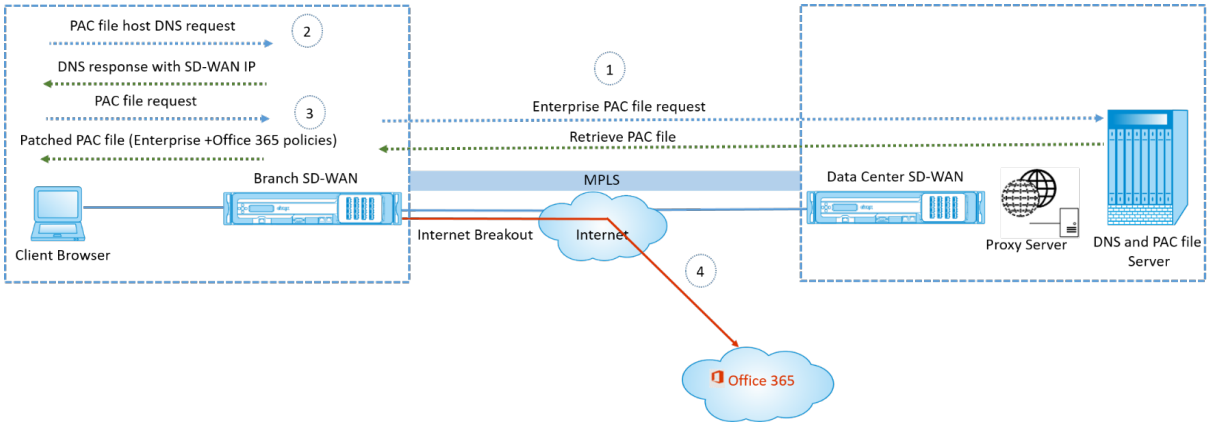
Cliquez sur **Vérifier la configuration** pour valider toute erreur d'audit.

Une fois que vous avez configuré la QoE de l'application avec le type d'application personnalisé, une vignette de rapport d'application pertinente est automatiquement générée sous **Rapports > Qualité de l'application**. Tout trafic correspondant à l'application sélectionnée passe par le chemin virtuel de l'application personnalisée.



Fonctionnement de la personnalisation des fichiers PAC

Idéalement, le fichier PAC hôte réseau d'entreprise sur le serveur Web interne, ces paramètres proxy sont distribués via la stratégie de groupe. Le navigateur client demande des fichiers PAC du serveur Web d'entreprise. L'appliance Citrix SD-WAN sert les fichiers PAC personnalisés pour les sites où la panne Office 365 est activée.



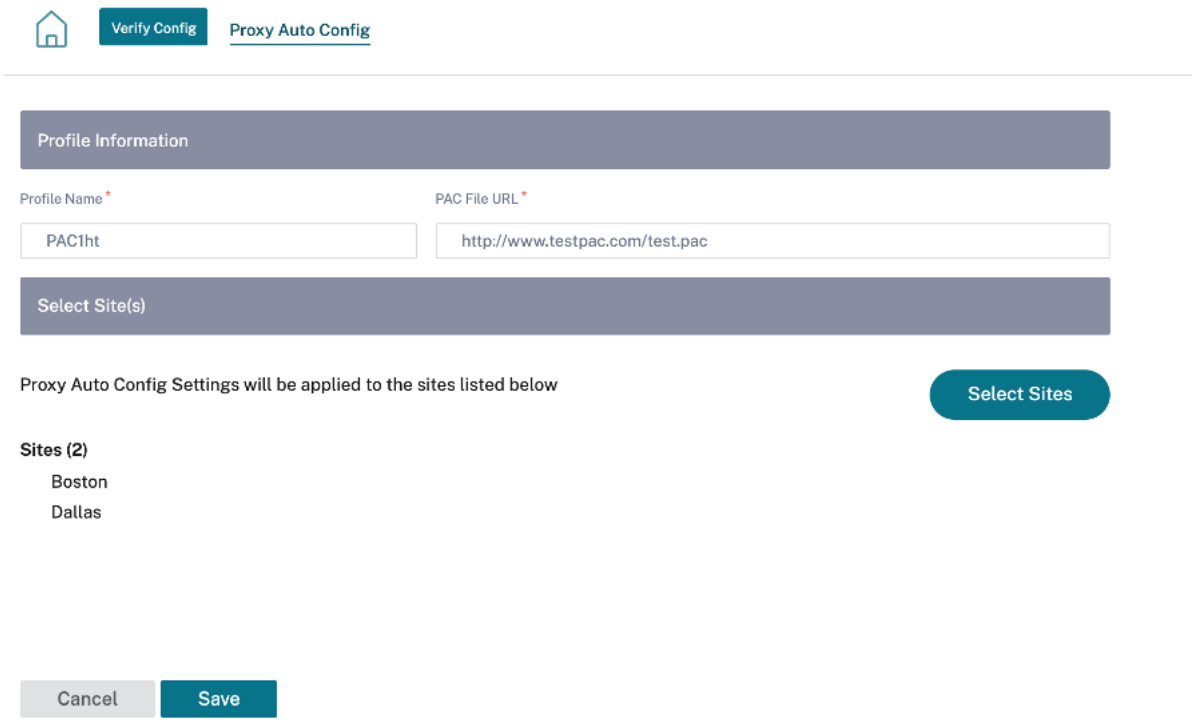
1. Citrix SD-WAN demande et récupère périodiquement la dernière copie du fichier PAC d'entreprise à partir du serveur Web d'entreprise. L'appliance Citrix SD-WAN corrige les URL Office 365 vers le fichier PAC d'entreprise. Le fichier PAC d'entreprise devrait avoir un espace réservé (balise spécifique au SD-WAN) dans lequel les URL Office 365 sont corrigées de façon transparente.
2. Le navigateur client déclenche une demande DNS pour l'hôte de fichier PAC d'entreprise. Citrix SD-WAN intercepte la demande pour le fichier de configuration du proxy FQDN et répond avec le VIP Citrix SD-WAN.
3. Le navigateur client demande le fichier PAC. L'appliance Citrix SD-WAN sert le fichier PAC corrigé localement. Le fichier PAC inclut la configuration du proxy d'entreprise et les stratégies d'exclusion d'URL Office 365.
4. À la réception d'une demande pour l'application Office 365, l'appliance Citrix SD-WAN effectue une sortie Internet directe.

Conditions préalables

1. Les entreprises doivent disposer d'un fichier PAC hébergé.
2. Le fichier PAC doit comporter un espace réservé *SDWAN_TAG* ou une occurrence de la `findproxyforurl` fonction permettant de patcher les URL d'Office 365.
3. L'URL du fichier PAC doit être basée sur le domaine et non sur IP.
4. Le fichier PAC est servi uniquement sur les VIP d'identité approuvés.
5. L'appliance Citrix SD-WAN doit pouvoir télécharger le fichier PAC d'entreprise via son interface de gestion.

Configurer la configuration automatique du proxy

Dans l'interface utilisateur du SD-WAN Orchestrartor, au niveau du réseau, accédez à **Configuration > Paramètreset groupes de l'application**>**Configuration automatique du proxy**et cliquez sur**+ profil de fichier PAC**.



Entrez un nom pour le profil de fichier PAC, indiquez l'URL du serveur de fichiers PAC d'entreprise. Les règles de présentation d'Office 365 sont appliquées dynamiquement au fichier PAC d'entreprise.

Sélectionnez les sites auxquels le profil de fichier PAC est appliqué. S'il existe différentes URL pour chaque site, créez un profil différent par site.

Limitations

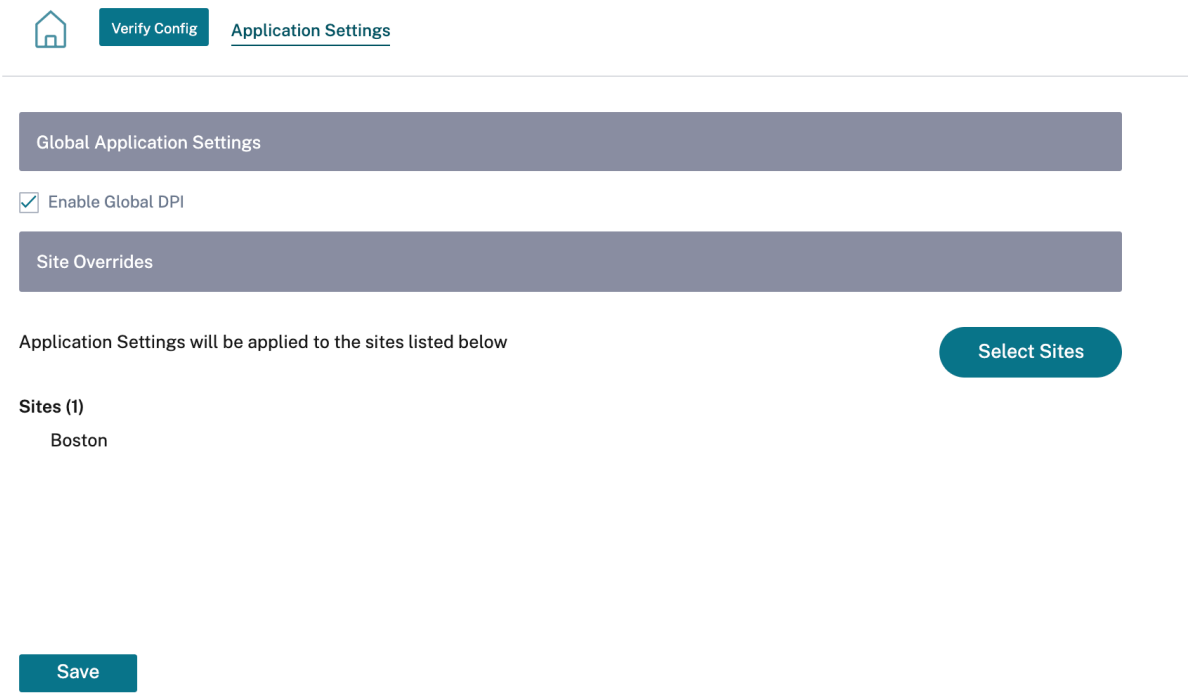
- Les requêtes du serveur de fichiers PAC HTTPS ne sont pas prises en charge.
- Plusieurs fichiers PAC dans un réseau ne sont pas pris en charge, y compris les fichiers PAC pour les domaines de routage ou les zones de sécurité.
- La génération d'un fichier PAC sur Citrix SD-WAN à partir de zéro n'est pas prise en charge.
- WPAD via DHCP n'est pas pris en charge.

Paramètres DPI

Les appliances Citrix SD-WAN effectuent une inspection approfondie des paquets (DPI) pour identifier et classer les applications. La bibliothèque DPI reconnaît des milliers d'applications commerciales. Il permet la découverte et la classification en temps réel des applications. À l'aide de la technologie DPI, l'appliance SD-WAN analyse les paquets entrants et classe le trafic comme appartenant à une application ou à une famille d'applications particulière.

DPI est activé globalement, par défaut, pour tous les sites de votre réseau. La désactivation de DPI arrête la capacité de classification PPP sur l'appliance. Vous ne pouvez plus utiliser les catégories d'application/applications classées PPP pour configurer des stratégies de pare-feu, de QoS et de routage. Vous ne pourrez pas non plus afficher le rapport sur les applications et les catégories d'applications les plus populaires.

Pour désactiver le DPI global, au niveau du réseau, accédez à **Configuration > Paramètres et groupes de l'application > Paramètres DPI** et désactivez la case à cocher **Activer le DPI global** .



Vous pouvez également choisir de désactiver les PPP pour certains sites uniquement en écrasant les paramètres DPI globaux. Pour désactiver le DPI pour les sites sélectionnés, ajoutez les sites à la liste des **remplacements** de sites.

Profils et modèles

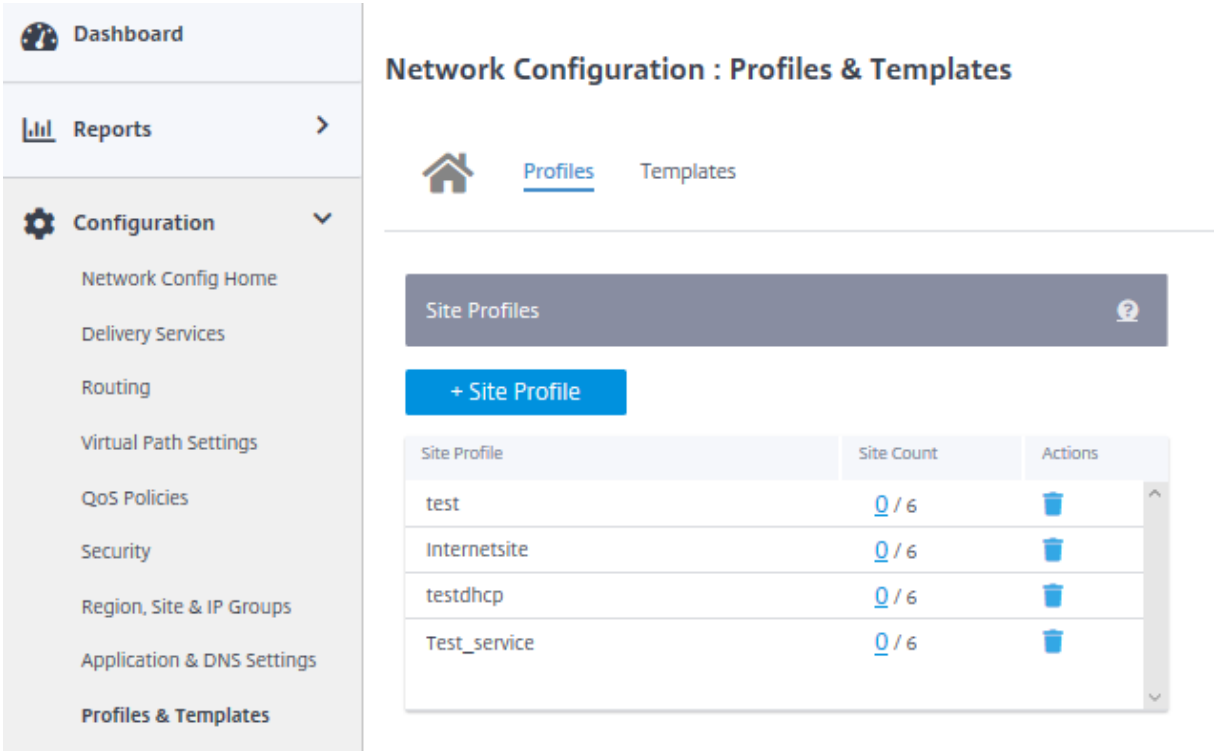
October 21, 2022

Un profil est un modèle de configuration en direct. Un modèle standard facilite la création d'une nouvelle entité. Mais une fois le modèle créé, les modifications ultérieures apportées au modèle ne s'appliquent pas aux entités existantes créées à l'aide du modèle de base. Un profil sert d'entité principale centrale en direct. Toutes les entités enfants héritent du profil, non seulement lors de la création mais aussi tout au long de la durée de vie d'un profil. Toutes les entités enfants associées au profil héritent automatiquement des modifications apportées à un profil.

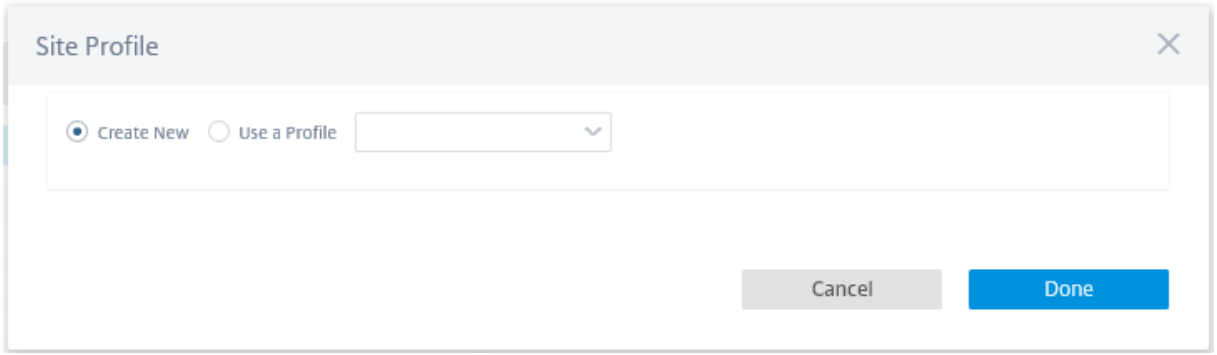
Par exemple, un administrateur crée un profil de configuration de site appelé le petit magasin de détail et l'applique à tous les petits magasins de détail appartenant à une entreprise. Maintenant, toute modification apportée au profil des petits magasins de détail à un moment donné serait appliquée automatiquement à tous les magasins héritant de ce profil. En fonction de ce qui est commun à toutes les entités et de ce qui ne l'est pas, certains paramètres de la configuration du profil peuvent être laissés indéfinis. Ces paramètres seraient personnalisables et peuvent varier selon les entités héritant du même profil.

Profils du site

Les profils de site vous aident à configurer facilement et rapidement des sites. Vous pouvez créer un profil de site une fois et le réutiliser plusieurs fois lors de la création de sites.

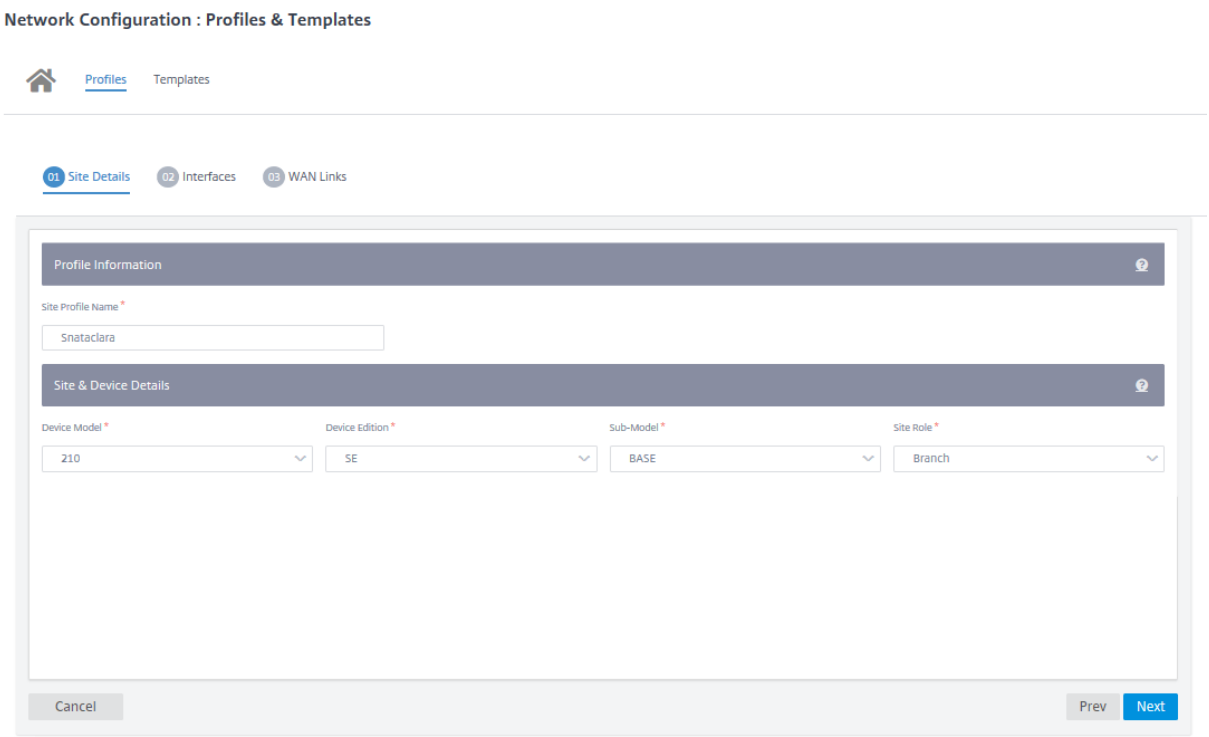


Pour créer un profil de site, cliquez sur **+ Profil du site**. Vous pouvez créer un profil à partir de zéro ou modifier un profil de site existant et l'enregistrer en tant que nouveau profil.

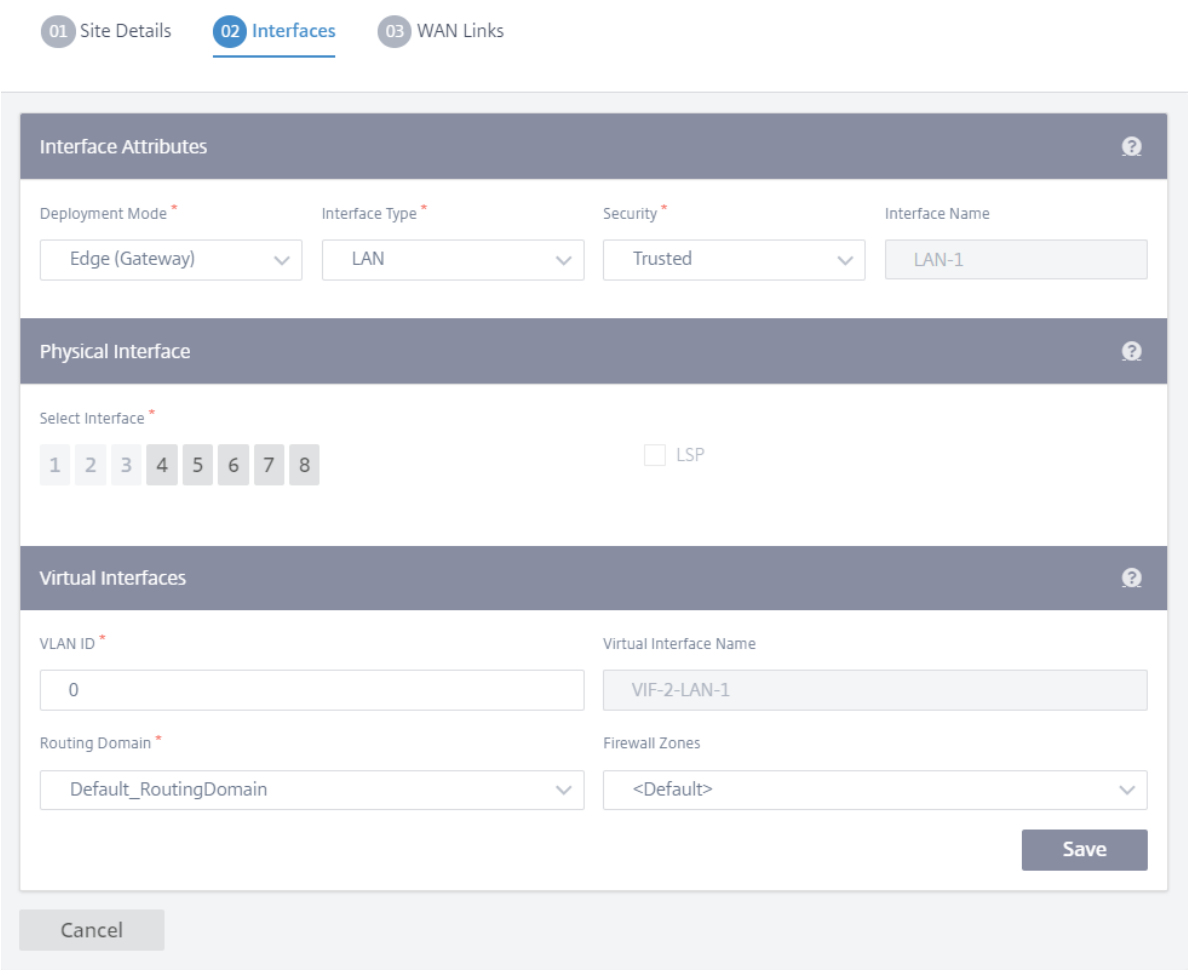


Pour créer un profil de site, vous devez configurer les **détails du site**, **les interfaces**et les **liens WAN**. Pour une description détaillée de la configuration des sites, voir Détails du site .

Fournissez les détails de l'appareil.

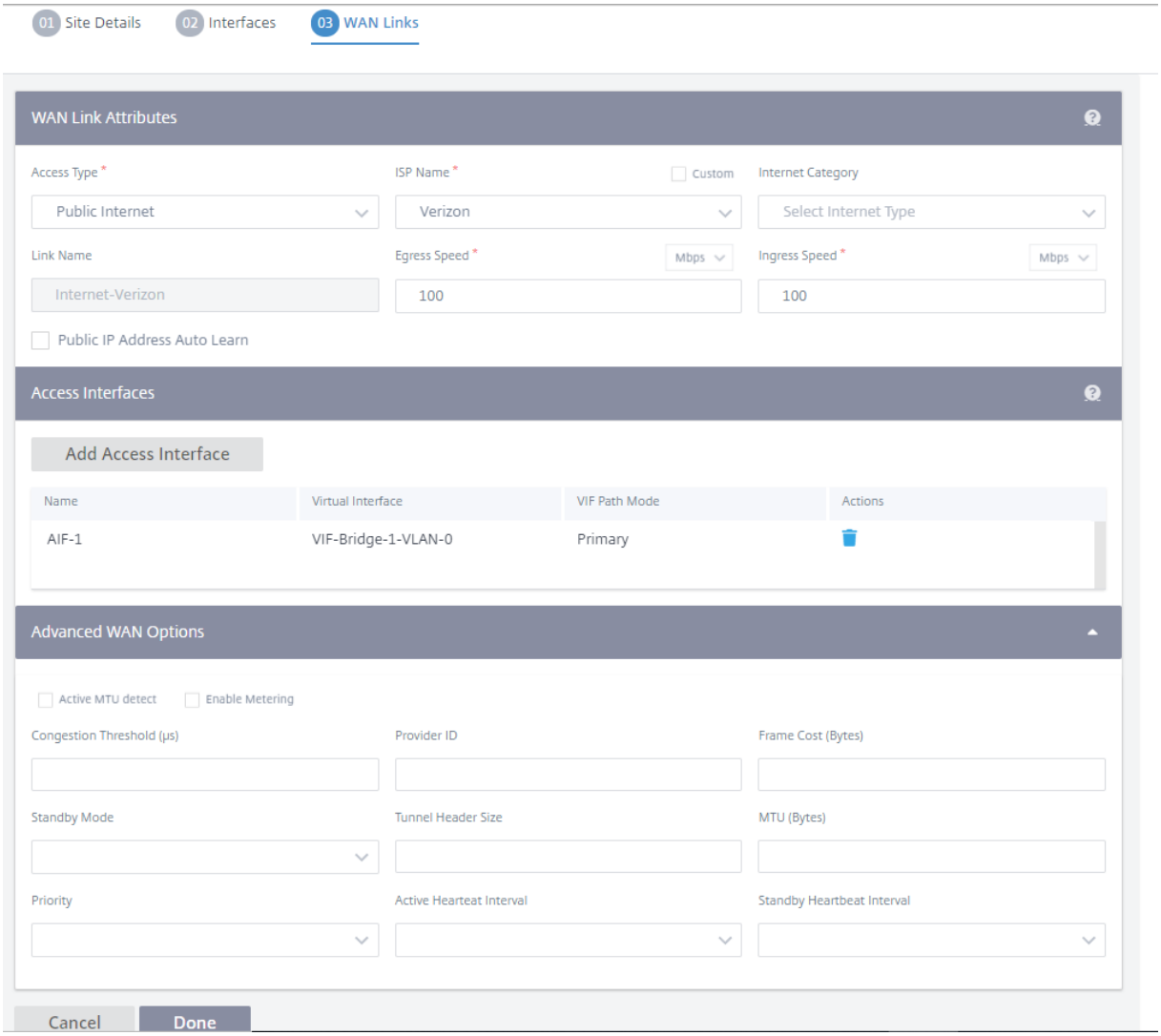


Attribuez une interface au site en cliquant sur l'option **+ Interface** . Pour ajouter une interface, vous devez remplir les champs **Attributs**d'**interface, Interface physique**et **Interfaces virtuelles** . Pour une description détaillée de la configuration des interfaces, voir Interfaces.



Remplissez **les attributs des liens WAN, lesinterfaces d'accès**et les**services**avec des**options avancées**.

Pour une description détaillée de la configuration des liaisons WAN, consultez la section Liaisons WAN.



Modèles

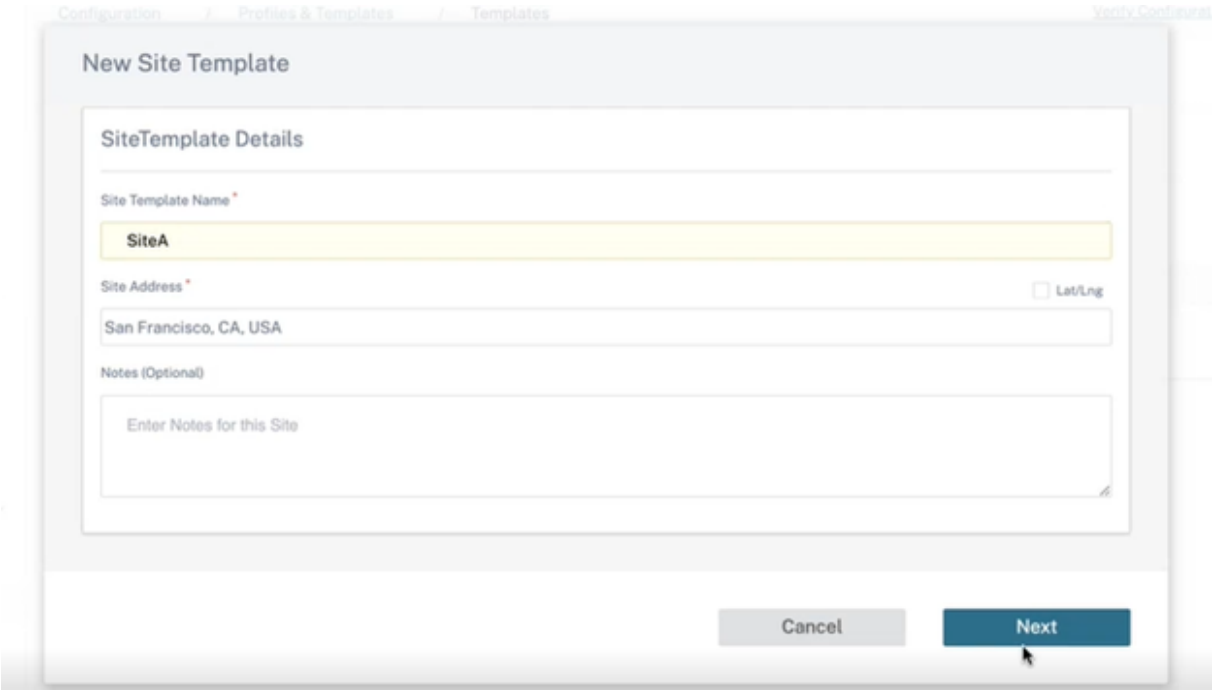
Le service Citrix SD-WAN Orchestrator vous permet d'utiliser des modèles sous la forme d'un ensemble prédéfini de champs pour configurer un nouveau site ou une liaison WAN.

Modèle de site

Un modèle de site est un modèle prédéfini utilisé pour la création de sites. Pour configurer un site à l'aide d'un modèle de site prédéfini, au niveau du client, accédez à **Configuration** > **Profils et modèles** > **Modèles**. Dans la section **Modèle de site**, cliquez sur **Ajouter un modèle de site**.

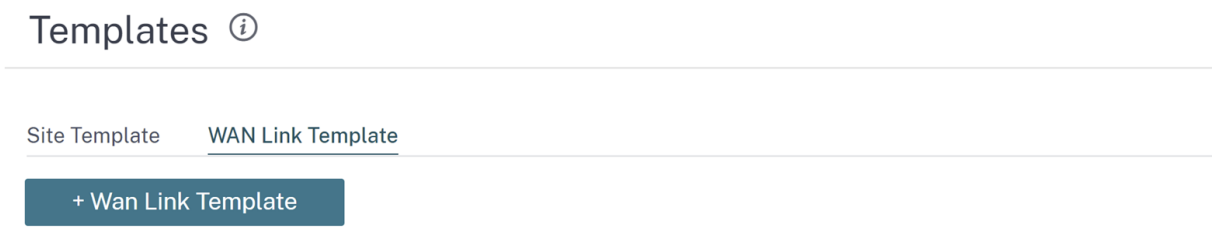
Sur l'écran **Nouveau modèle de site** qui s'affiche, fournissez les informations requises et cliquez sur **Suivant**.

> **Remarque**
>
> Lorsque vous clonez un site ou que vous créez un site à l'aide d'un modèle de site et que le Wi-Fi est configuré sur la source, les paramètres Wi-Fi ne sont pas copiés sur le nouveau site.

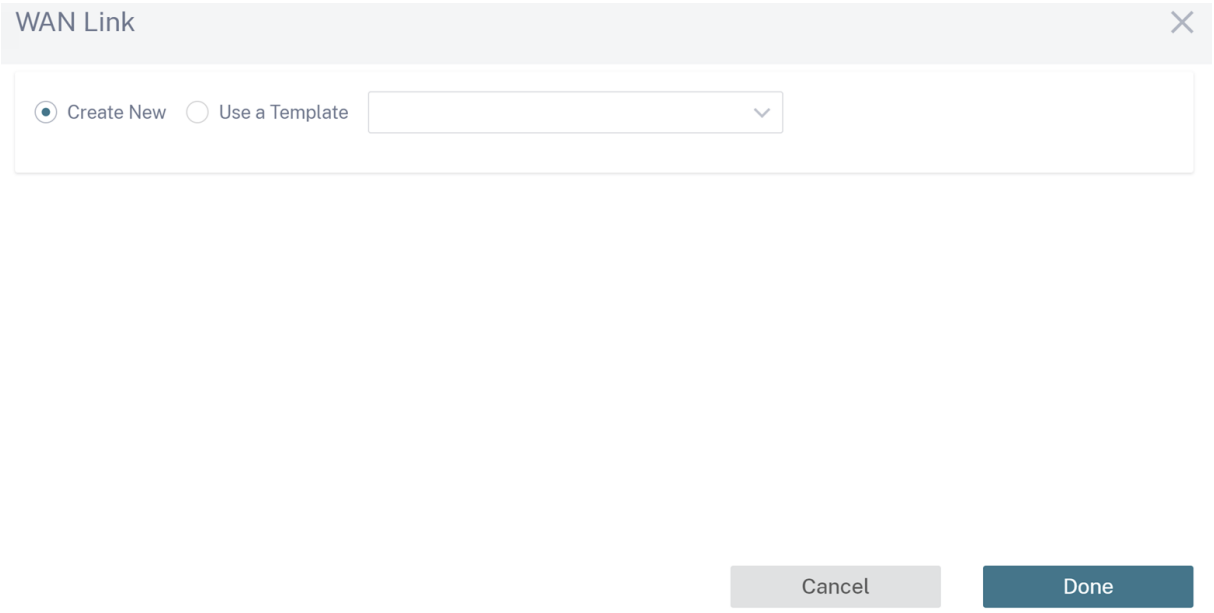


Modèle de lien WAN

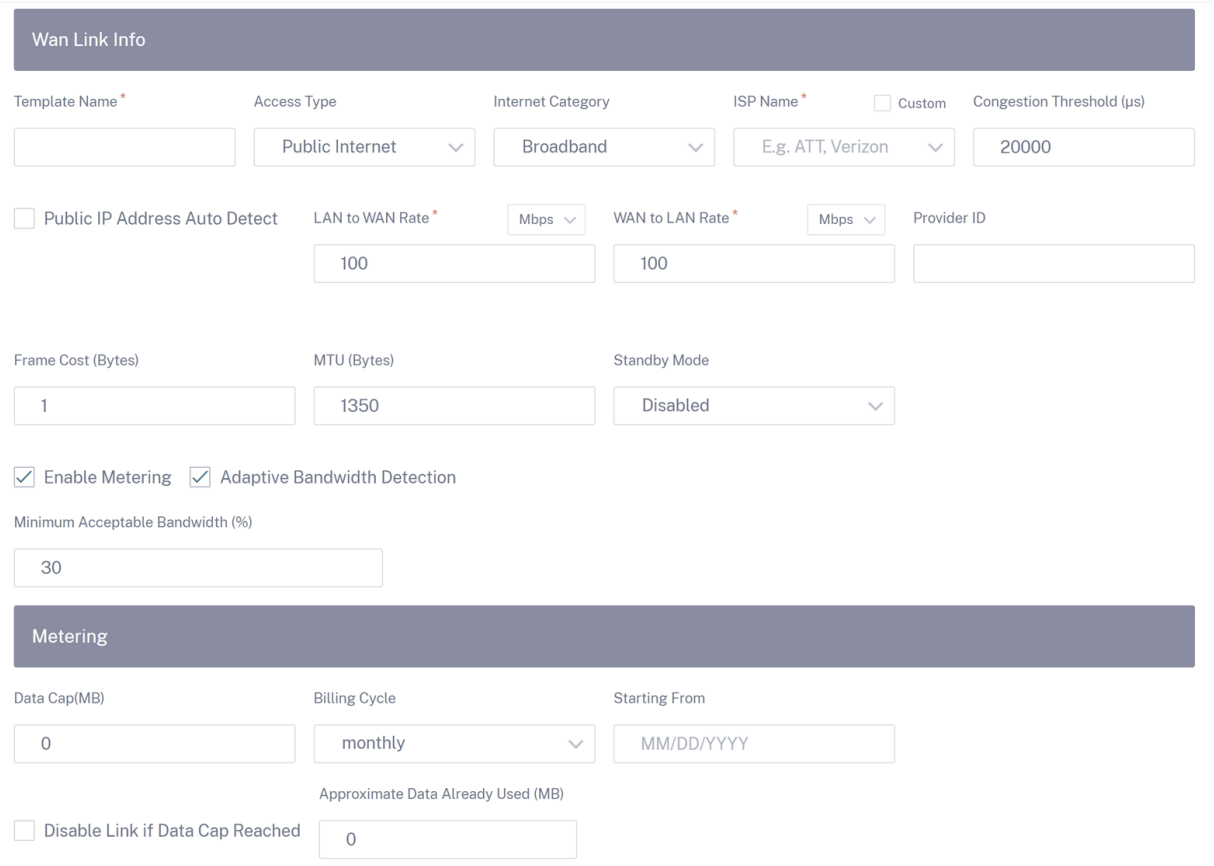
Les modèles de liens WAN vous aident à configurer les liens WAN facilement et rapidement. Vous pouvez créer un modèle de liaison WAN une fois et le réutiliser plusieurs fois lors de la configuration des liens WAN. Vous pouvez même copier les configurations du modèle de lien WAN modifié vers les configurations de lien WAN du site créées à l'aide du modèle de lien WAN.



Pour créer un modèle de lien WAN, cliquez sur **+ Modèle de lien WAN**. Vous pouvez créer un modèle à partir de zéro ou modifier un modèle de lien WAN existant et l'enregistrer en tant que nouveau modèle.



Fournissez les informations relatives à la liaison WAN, telles que le **nom du profil**, le **type d'accès**, la **catégorie Internet**, le **débit LAN/WAN** (Mbits/s), etc. pour créer un profil WAN. Pour une description détaillée de la configuration des liaisons WAN, consultez la section Liaisons WAN.

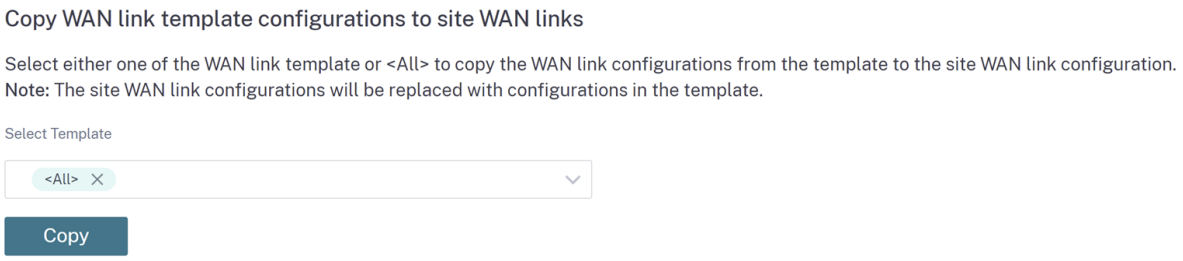


Auparavant, l'option permettant de copier les configurations du modèle de lien WAN modifié vers les

configurations de liens WAN du site n'était pas disponible. Par exemple, si un utilisateur avait déjà créé plusieurs liens WAN de site à l'aide d'un modèle de lien WAN et avait dû modifier une configuration particulière (par exemple, le réglage du seuil de congestion), il devait le faire sur chaque lien WAN du site individuellement. Désormais, l'utilisateur peut mettre à jour le modèle de lien WAN avec le nouveau paramètre de seuil de congestion et copier les dernières configurations du modèle de lien WAN sur tous les liens WAN du site créés à l'aide du modèle de lien WAN.

Lorsque vous sélectionnez un ou plusieurs modèles de liens WAN et que vous cliquez sur Copier, les mises à jour que vous apportez au modèle de lien WAN sont copiées dans la configuration de lien WAN du site créée à l'aide des modèles sélectionnés.

> **Remarque :**
>
> Les configurations de sites de liaison WAN créées à l'aide de la fonctionnalité de profil de site ne sont pas mises à jour.



Service de localisation du réseau

July 10, 2024

> **Mise à jour importante :**
>
> Cette fonctionnalité est obsolète dans le déploiement du service Citrix SD-WAN Orchestrator. Cependant, vous pouvez toujours activer le NLS à l'aide de Citrix Cloud. Pour plus de détails, voir Optimiser la connectivité aux espaces de travail avec Direct Workload Connection.

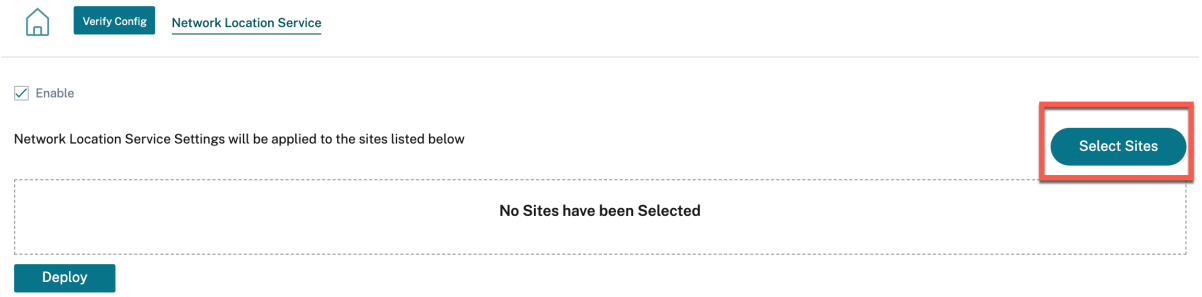
Le service de localisation du réseau (NLS) est un service Citrix Cloud qui détermine si l'utilisateur qui se connecte à Citrix Virtual Apps and Desktops provient du réseau interne. À l'aide du protocole NLS, vous pouvez éviter de configurer manuellement les adresses IP des emplacements déployés par Citrix SD-WAN via le script PowerShell. Pour des informations détaillées sur le NLS, consultez Citrix Workspace Network Location Service.

Vous pouvez activer le NLS pour tous les sites du réseau ou pour des sites spécifiques. Le site activé pour le NLS partage l'adresse IP publique de tous ses liens Internet WAN ainsi que d'autres détails du

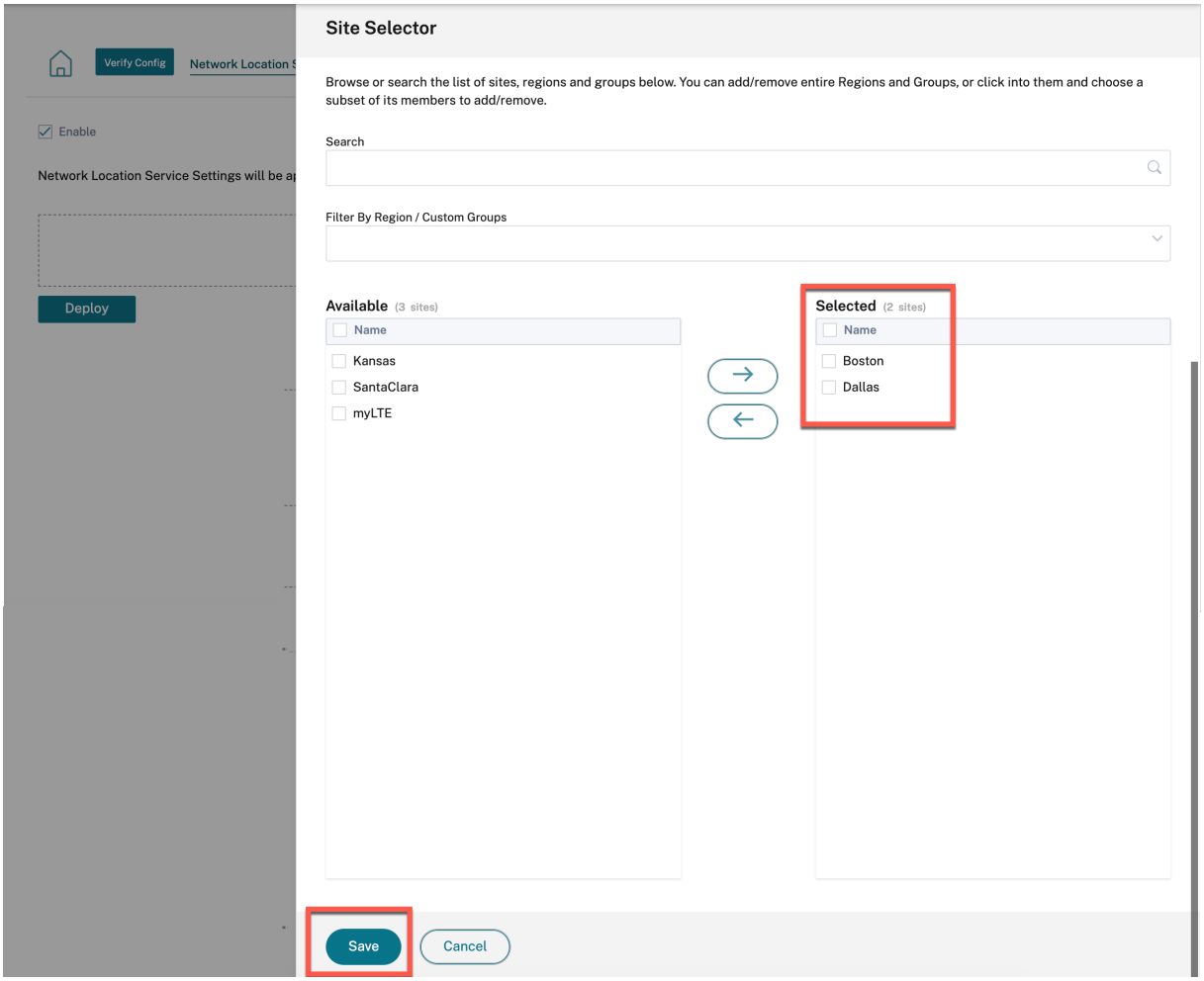
site tels que l'emplacement géographique et le fuseau horaire avec la base de données NLS. À l'aide de ces informations, le service de localisation réseau détermine si l'utilisateur qui se connecte à Citrix Virtual Apps and Desktops se trouve sur une interface réseau gérée par Citrix SD-WAN.

Si une demande utilisateur provient d'une interface réseau basée sur Citrix SD-WAN, l'utilisateur est connecté directement à Citrix Virtual Apps and Desktops Virtual Delivery Agent en contournant le service NetScaler Gateway.

Pour activer le NLS, au niveau du client, accédez à **Configuration > Service de localisation réseau**.



Sélectionnez **Activer** si vous souhaitez activer le NLS pour tous les sites du réseau. Pour activer le NLS pour des sites spécifiques, cliquez sur **Sélectionner des sites**. Choisissez la **région** et sélectionnez les sites en conséquence. Cliquez sur **Enregistrer**, puis sur **Déployer**.



Équilibrage de charge ECMP

October 21, 2022

Les groupes ECMP (Equal Cost Multi-Path) vous permettent de regrouper plusieurs chemins avec le même coût, la destination et le même service. La charge des connexions ou des données de session est équilibrée sur tous les chemins d'accès du groupe ECMP en fonction du type de groupe ECMP. Par exemple, considérez un réseau avec deux liaisons WAN entre une branche et un centre de données ayant le même coût d'itinéraire. Traditionnellement, l'une des liaisons WAN serait active et l'autre reste dormante agissant comme liaison de secours. Avec les groupes ECMP, vous pouvez regrouper ces liaisons WAN et permettre l'équilibrage de la charge du trafic via les deux liaisons WAN. L'équilibrage de charge ECMP garantit :

- Répartition du trafic sur plusieurs chemins à coût égal.
- Utilisation optimale de la bande passante disponible.

- Transfert dynamique du trafic vers un autre chemin membre de l'ECMP, si un itinéraire devient inaccessible.

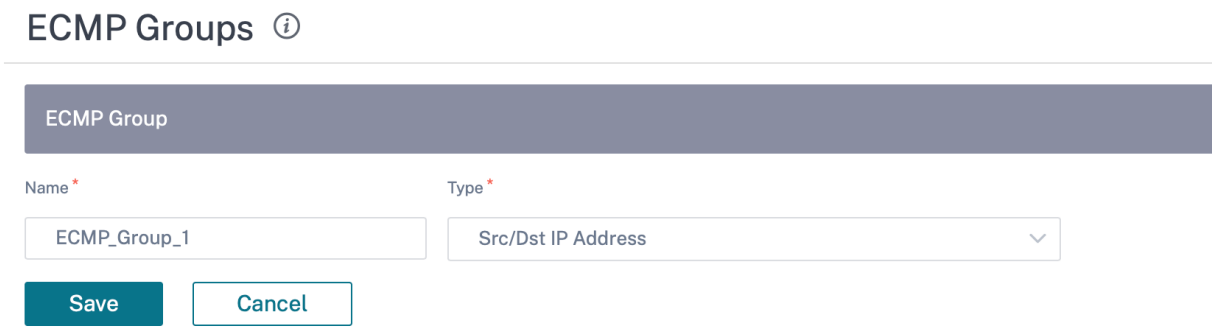
L'équilibrage de charge ECMP est pris en charge sur les services suivants :

- Chemins virtuels
- Citrix Secure Internet Access
- Zscaler
- IPSec
- GRE

Vous pouvez définir un maximum de 254 groupes ECMP dans votre réseau. Le nombre maximal de routes éligibles ECMP dans un groupe ECMP dépend de votre appliance et du type de licence. Les deux types de groupes ECMP suivants sont pris en charge sur Citrix SD-WAN :

- Adresse IP source/destination : Réseaux où plusieurs clients tentent de se connecter à la même destination, les connexions sont équilibrées en charge sur des liaisons WAN à coût égal.
- Session : Réseaux sur lesquels un seul client est connecté à une destination et où plusieurs sessions sont engendrées. Les données de session sont équilibrées en charge sur des liaisons WAN à coût égal.

Pour configurer un groupe ECMP, au niveau du réseau, accédez à **Configuration > Routage > Groupes ECMP**. Indiquez un nom pour le groupe ECMP et sélectionnez le type comme **adresse IP Src/Dest** ou **Session** selon les besoins.



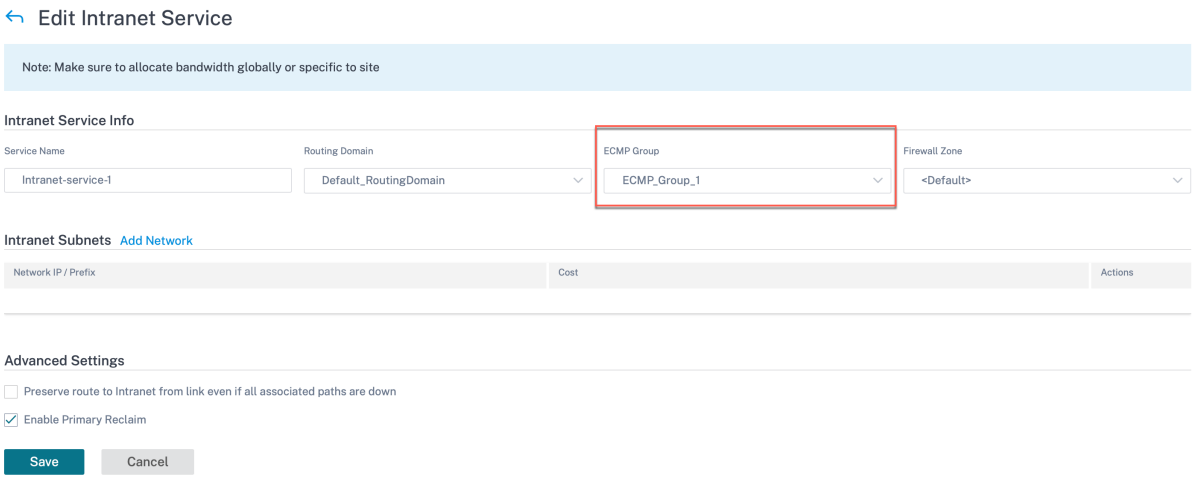
Vous pouvez associer les groupes ECMP aux services suivants :

- Chemins virtuels (au niveau du site)
- Citrix Secure Internet Access
- Zscaler
- IPSec
- GRE

Pour activer la configuration ECMP sur les services Intranet, au niveau du réseau*, accédez à **Configuration > Canaux de diffusion > Allocation de bande passante > Intranet + Service** et sélectionnez le

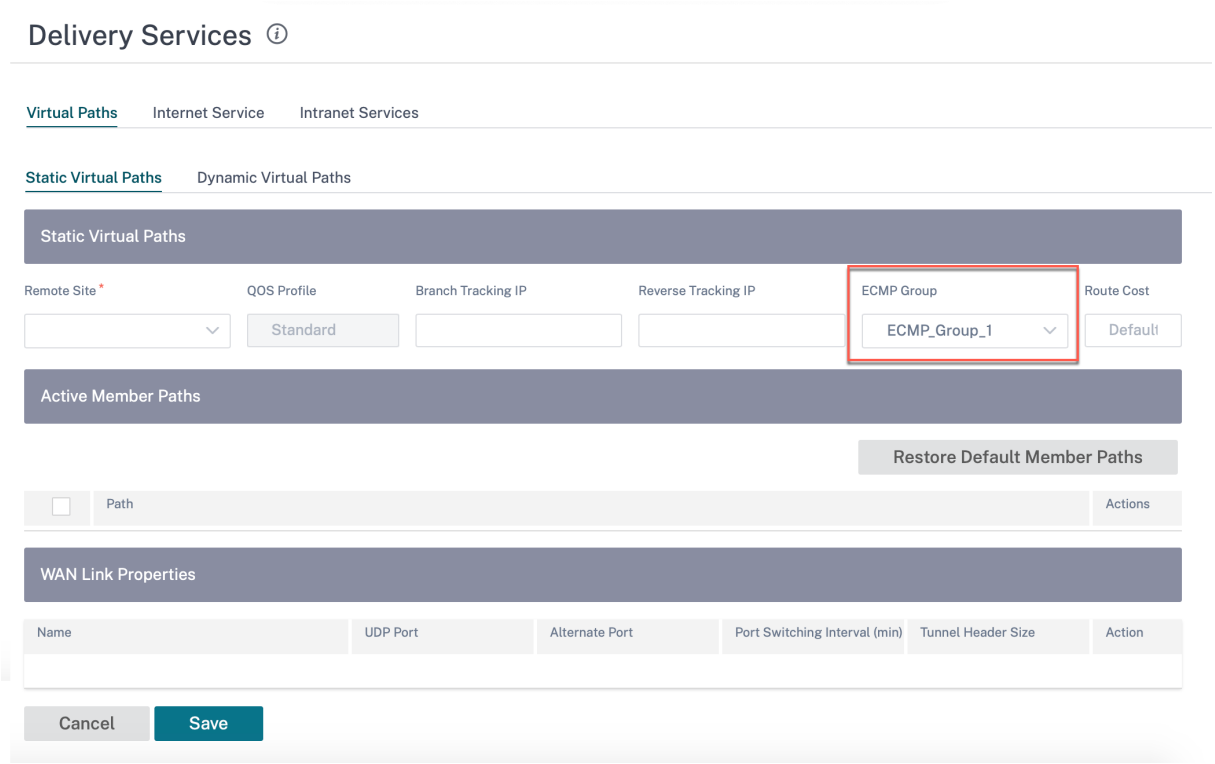
type de serviceIntranet. Sélectionnez le groupe ECMP lors de la configuration du service Intranet.

> **Remarque**
>
> Si vous sélectionnez **Aucun**, vous n'activerez pas la configuration ECMP sur le service.



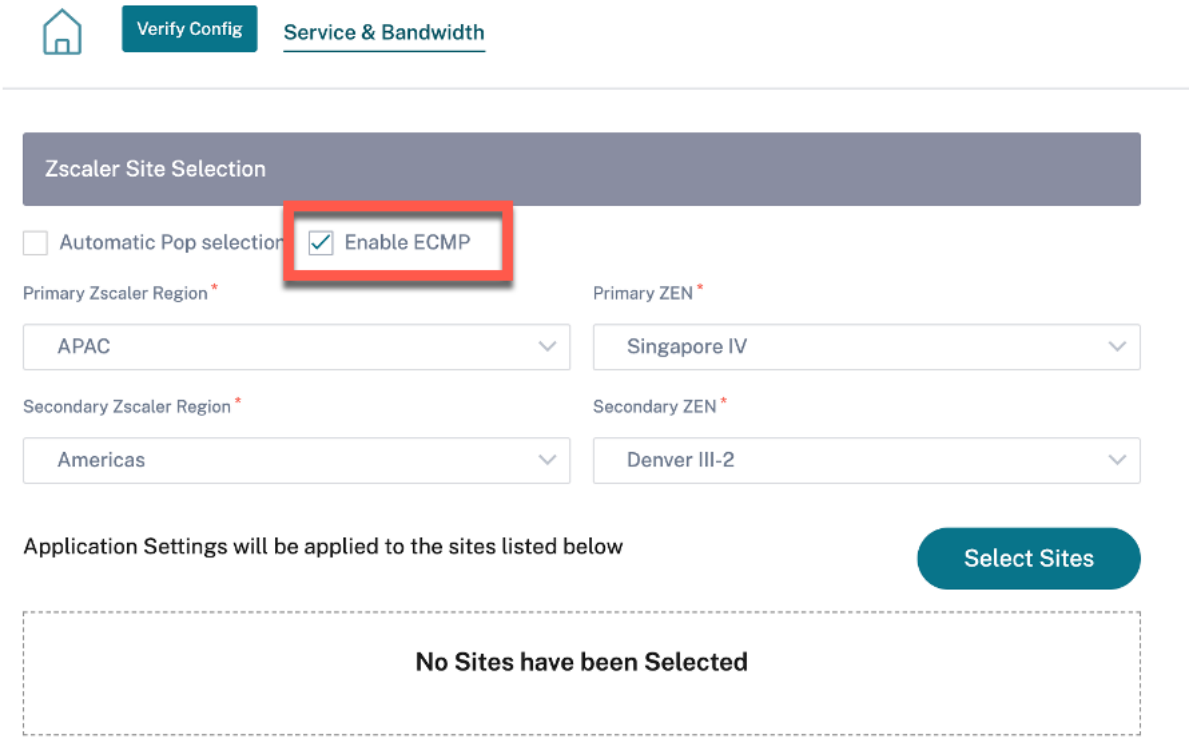
Pour activer la configuration ECMP sur les chemins virtuels, au niveau du site, accédez à **Configuration** > **Paramètres avancés** > **Services de mise** à disposition > **Chemins virtuels > Cheminsvirtuels statiques**>**+ Chemins virtuels**. Sélectionnez le groupe ECMP lors de la configuration des chemins virtuels statiques.

> **Remarque**
>
> Si vous sélectionnez **Aucun**, vous n'activerez pas la configuration ECMP sur le service.



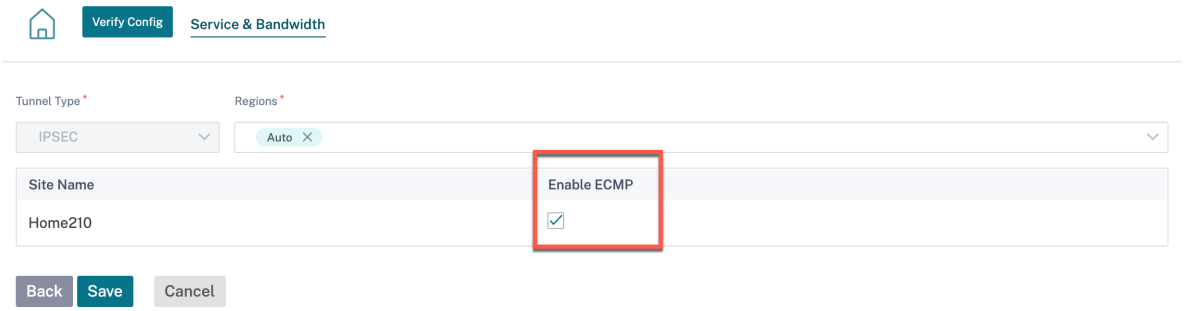
Pour activer la configuration ECMP sur les services Zscaler, au niveau du réseau, accédez à **Configuration > Services et bande passante**. Cliquez sur l'icône **Paramètres** à côté de Zscaler répertorié dans la colonne **Delivery Services** . Authentifiez-vous et cliquez sur **+ Site**. Cochez la case **Activer l'ECMP** lors de l'ajout de sites.

> **REMARQUE :**
>
> Le service Zscaler prend uniquement en charge l'équilibrage de charge ECMP basé sur les sessions.



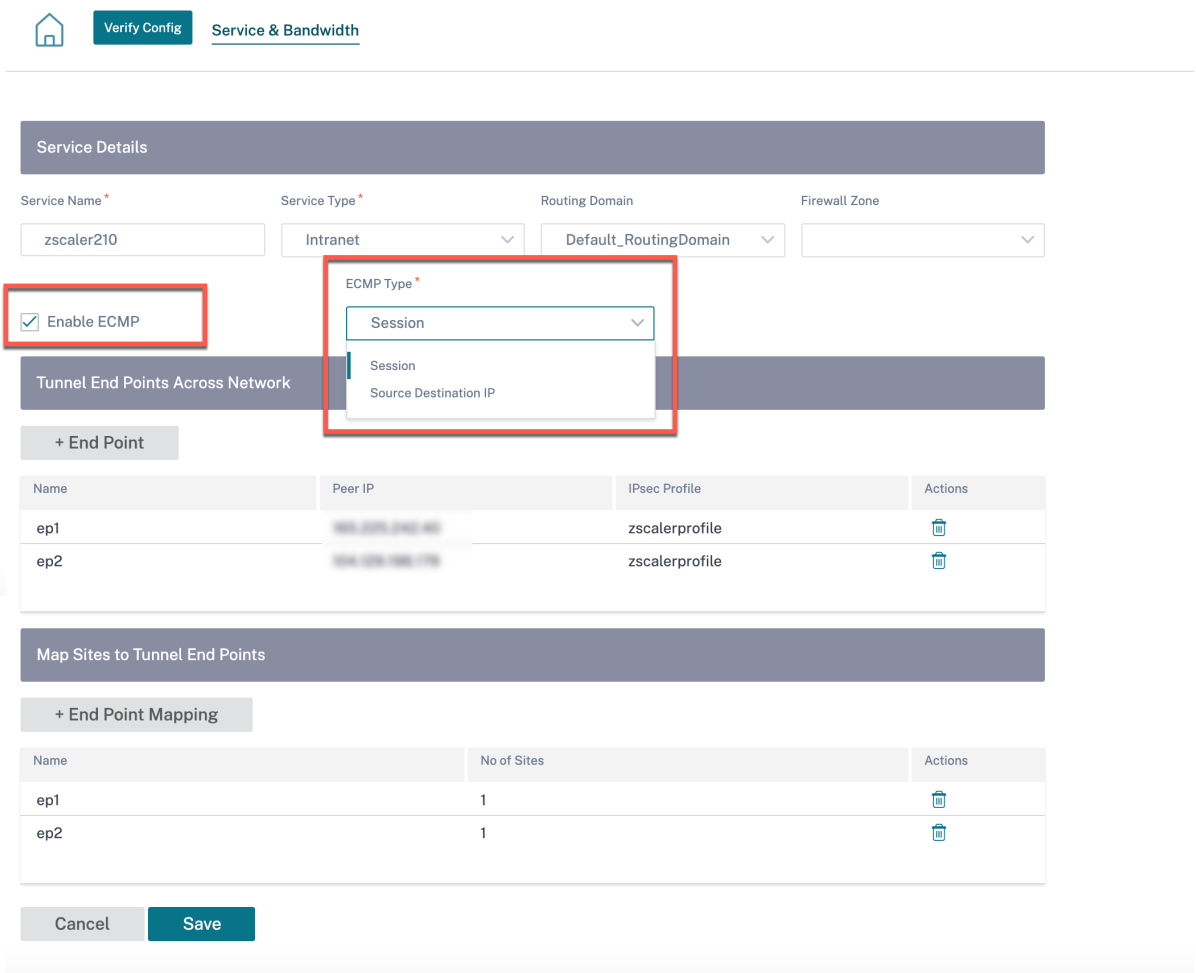
Pour activer la configuration ECMP sur le service Citrix Secure Internet Access, au niveau du réseau, accédez à **Configuration > Services et bande passante**. Cliquez sur l'icône **Paramètres** à côté de **Secure Internet Access Service** et cliquez sur **+ Site**. Cochez la case **Activer l'ECMP** après avoir sélectionné les sites.

> **REMARQUE :**
>
> Le service Citrix Secure Internet Access prend uniquement en charge l'équilibrage de charge ECMP basé sur les sessions.



Pour activer la configuration ECMP sur des tunnels IPsec fixes avec des homologues tiers côté LAN ou WAN, accédez à **Configuration > Services et bande passante > Intranet + Service** et sélectionnez le **type de serviceIPsec**. Cochez la case**Activer l'ECMP**et choisissez un type dans la

liste déroulante**Type ECMP** .



Règles d'application

October 21, 2022

Les règles d'application permettent à l'appliance Citrix SD-WAN d'analyser le trafic entrant et de le classer comme appartenant à une application ou à un groupe d'applications particulier. Cette classification améliore la qualité de service (QoS) d'applications individuelles ou de familles d'applications en créant et en appliquant des règles d'application.

Vous pouvez filtrer les flux de trafic en fonction des types de correspondance d'applications, de groupes d'applications ou d'objets d'application et leur appliquer des règles d'application. Les règles de l'application sont similaires aux règles du protocole Internet (IP). Pour plus d'informations sur les règles IP, voir Règles IP.

Pour chaque règle d'application, vous pouvez spécifier la politique de trafic. Les politiques de trafic disponibles sont les suivantes :

- **Chemin d'équilibrage de charge** : le trafic applicatif du flux est équilibré sur plusieurs chemins. Le trafic est envoyé par le meilleur chemin jusqu'à ce que ce chemin soit utilisé. Les paquets restants sont envoyés par le meilleur chemin suivant.
- **Chemin persistant** : le trafic de l'application reste sur le même chemin jusqu'à ce que le chemin d'accès ne soit plus disponible.
- **Dupliquer le chemin** : le trafic d'application est dupliqué sur plusieurs chemins, ce qui augmente la fiabilité.
  Les règles d'application sont associées aux classes.

Comment les règles d'application sont appliquées ?

Dans le réseau SD-WAN, lorsque les paquets entrants atteignent l'appliance SD-WAN, les quelques paquets initiaux ne subissent pas la classification DPI. À ce stade, les attributs de règle IP tels que Class, TCP terminaison sont appliqués aux paquets. Après la classification DPI, les attributs des règles d'application tels que Classe et politique de trafic remplacent les attributs de la règle IP.

Les règles IP ont plus d'attributs que les règles d'application. La règle d'application remplace uniquement certains attributs de la règle IP. Les autres attributs de la règle IP restent traités sur les paquets.

Par exemple, considérez que vous avez spécifié une règle d'application pour une application de messagerie Web telle que Google Mail qui utilise le protocole SMTP. La règle IP définie pour le protocole SMTP est appliquée initialement avant la classification DPI. Après avoir analysé les paquets et les avoir classés comme appartenant à l'application Google Mail, la règle d'application spécifiée pour l'application Google Mail est appliquée.

Création de règles d'application

Pour créer des règles d'application, accédez à **Configuration > QoS > Politiques de QoS** > **Règles d'application**. Sélectionnez l'onglet **Règles globales** pour créer des règles d'application au niveau global ou **Règles spécifiques au site/au groupe** pour créer des règles au niveau du site.

Cliquez sur **Nouvelle règle d'application** dans la section **Règles d'application** .

- Les applications et les domaines correspondent aux critères
  - **Applications et domaines** : choisissez une application ou un domaine dans la liste déroulante. Vous pouvez également créer une application de domaine en cliquant sur **+ Nouvelle application de domaine**. Entrez un nom et ajoutez des domaines.

  - **Domaine de routage** : sélectionnez un domaine de routage. Vous pouvez sélectionner le domaine de routage par défaut ou sélectionner **N'importe lequel**.
  - **Réseau source** : adresse IP source et masque de sous-réseau à comparer au trafic.
  - **Réseau**de destination : adresse IP de destination et masque de sous-réseau à comparer au trafic.
  - **Port source** : numéro de port source ou plage de ports à mettre en correspondance avec le trafic.
  - **Port de destination** : numéro de port de destination ou plage de ports à mettre en correspondance avec le trafic.
  - **Src = Dest** : si cette option est sélectionnée, le port source est également utilisé pour le port de destination.

- Politique de trafic sur Virtual Path

  Cochez la case **Activer la politique de trafic sur les chemins virtuels** .

  - **Site distant par chemin virtuel** : sélectionnez le chemin virtuel du site distant.
  - **Politique de trafic** : Choisissez l'une des politiques de trafic suivantes selon vos besoins.
    - **Chemins d'équilibrage**de charge : le trafic d'applications pour le flux est équilibré sur plusieurs chemins. Le trafic est envoyé par le meilleur chemin jusqu'à ce que ce chemin soit utilisé. Les paquets restants sont envoyés par le meilleur chemin suivant.
    - **Chemin persistant** : le trafic de l'application reste sur le même chemin jusqu'à ce que le chemin d'accès ne soit plus disponible. Sélectionnez l'une des **politiques de persistance**suivantes :
      - **Persister sur le lien d'origine** : le trafic de l'application reste sur le lien d'origine jusqu'à ce que le chemin ne soit plus disponible.
      - **Persister sur le lien MPLS si disponible, sinon sur le lien d'origine** : le trafic de l'application reste sur le lien MPLS. Si la liaison MPLS n'est pas disponible, le trafic reste sur la liaison d'origine.
      - **Persister sur le lien Internet si disponible, sinon sur le lien d'origine** : le trafic de l'application reste sur le lien Internet. Si le lien Internet n'est pas disponible, le trafic reste sur le lien d'origine.
      - **Poursuivre sur le lien intranet privé si disponible, sinon sur le lien d'origine** : le trafic de l'application reste sur le lien intranet privé. Si le lien intranet privé n'est pas disponible, le trafic reste sur le lien d'origine.

      L'**impédance de persistance** est le temps (en ms) pendant lequel le trafic de l'application reste sur le lien.
    - **Chemins dupliqués** : le trafic des applications est dupliqué sur plusieurs chemins, ce qui augmente la fiabilité

- Paramètres QoS (classe QoS)

- **Type de transfert** : Choisissez l'un des types de transfert suivants :
  - **Temps réel** : utilisé pour le trafic à faible latence, à faible bande passante et sensible au temps. Les applications en temps réel sont urgentes mais n'ont pas vraiment besoin d'une bande passante élevée (par exemple, la voix sur IP). Les applications en temps réel sont sensibles à la latence et à l'instabilité, mais peuvent tolérer certaines pertes.
  - **Interactif** : Utilisé pour le trafic interactif avec des exigences de latence faible à moyenne et des exigences de bande passante faible à moyenne. L'interaction se fait généralement entre un client et un serveur. La communication peut ne pas nécessiter de bande passante élevée, mais elle est sensible à la perte et à la latence.
  - **Vrac** : Utilisé pour le trafic à bande passante élevée et les applications pouvant tolérer une latence élevée. Les applications qui gèrent le transfert de fichiers et nécessitent une bande passante élevée sont classées dans la catégorie des applications groupées. Ces applications impliquent peu d'interférence humaine et sont principalement traitées par les systèmes eux-mêmes.
- **Priorité** : Choisissez une priorité pour le type de transfert sélectionné.

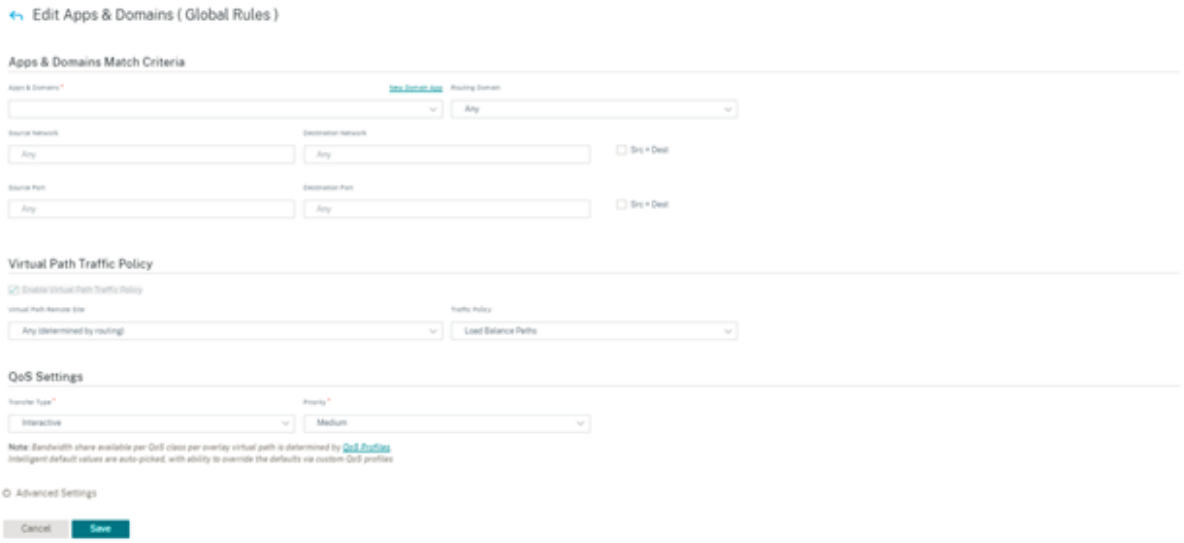
Paramètres avancés

- WAN en général
  - **Retransmettre les paquets perdus** : envoie le trafic correspondant à cette règle à l'appliance distante via un service fiable et retransmet les paquets perdus.
  - **Activer l'agrégation de paquets** : regroupe les petits paquets en paquets plus volumineux.
- LAN vers WAN
  - **Profondeur de dépôt (octets)** : seuil de profondeur de file d'attente au-delà duquel les paquets sont supprimés.
  - **Limite de suppression : délai**après lequel les paquets en attente dans le planificateur de classes sont supprimés. Ne s'applique pas à une classe en vrac.
  - **Activer RED** : Random Early Detection (RED) garantit un partage équitable des ressources de classe en rejetant les paquets en cas de congestion.
  - **Profondeur de désactivation des paquets dupliqués (octets)** : profondeur de file d'attente du planificateur de classes à laquelle les paquets dupliqués ne sont pas générés.
  - **Limite de désactivation des paquets dupliqués** : durée pendant laquelle la duplication peut être désactivée pour empêcher les doublons de consommer de la bande passante.
- WAN vers LAN
  - Balise**DSCP : étiquette**DSCP appliquée aux paquets qui répondent à cette règle sur le réseau WAN vers le réseau local, avant de les envoyer au réseau local.

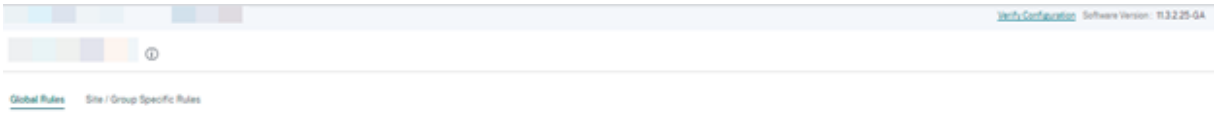
- **Activer le reséquençage des paquets** : Les flux de trafic qui correspondent à la règle sont balisés pour l'ordre des séquences, et les paquets sont réorganisés (si nécessaire) au niveau de l'appliance WAN vers LAN.
- **Hold Time** : Intervalle de temps pendant lequel les paquets sont conservés pour le reséquencement, après quoi les paquets sont envoyés au réseau local. Lorsque le temporisateur expire, les paquets sont envoyés au réseau local sans attendre plus longtemps les numéros de séquence prédéfinis.

  Si la règle a une politique de trafic en tant que chemin dupliqué, le temps de maintien par défaut est de 80 ms. Sinon, la valeur par défaut est de 900 ms pour les règles TCP et de 250 ms pour les règles non TCP.
- **Supprimer les paquets de reséquençage en retard** : élimine les paquets hors ordre arrivés après l'envoi des paquets nécessaires au reséquençage au réseau local.

Cliquez sur **Enregistrer** pour enregistrer les paramètres de configuration.



Cliquez sur **Vérifier la configuration** sur la page **Configuration** > **QoS> Politiques de QoS** pour valider toute erreur d'audit. Pour valider toute erreur d'audit.



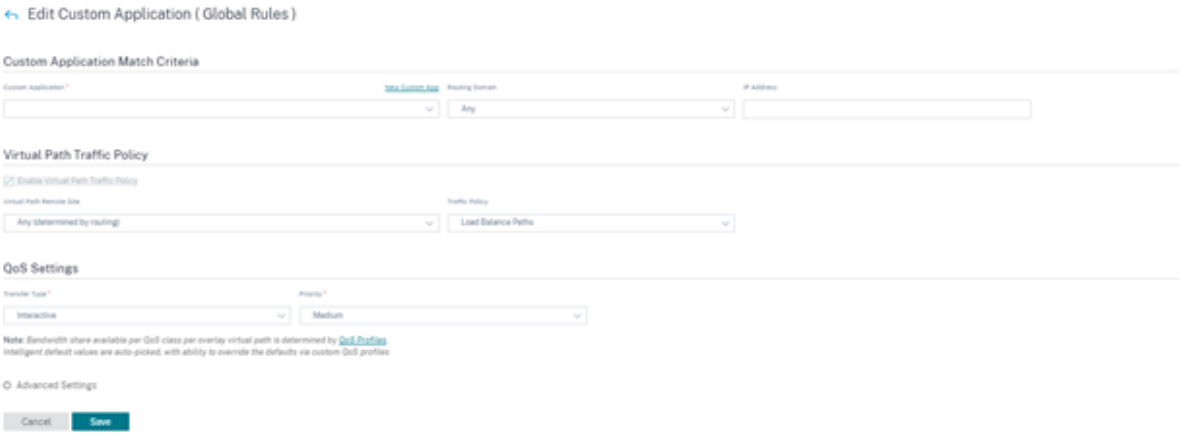
Création de règles d'application personnalisées

Vous pouvez également créer des règles d'application personnalisées. Pour créer une règle d'application personnalisée, accédez à **Configuration > QoS > Politiques de QoS** > **Règles d'application**

personnalisées. Sélectionnez l'onglet **Règles globales** pour créer des règles d'application personnalisées au niveau global ou **Règles spécifiques au site/au groupe** pour créer des règles au niveau du site.

Cliquez sur **Nouvelle règle d'application personnaliséedans la section Règles d'application personnalisées**. Cliquez sur**Nouvelle application personnalisée**à côté du nom du champ**Application personnalisée**. Entrez le nom de l'application personnalisée. Dans la section**Critères de correspondance**, sélectionnez l'application, le protocole, la balise DSCP et entrez l'adresse IP et le numéro de port du réseau. Cliquez sur**Enregistrer**.

Entrez les informations nécessaires dans les autres champs. Pour plus d'informations sur les descriptions des champs, voir Création de règles d'application.

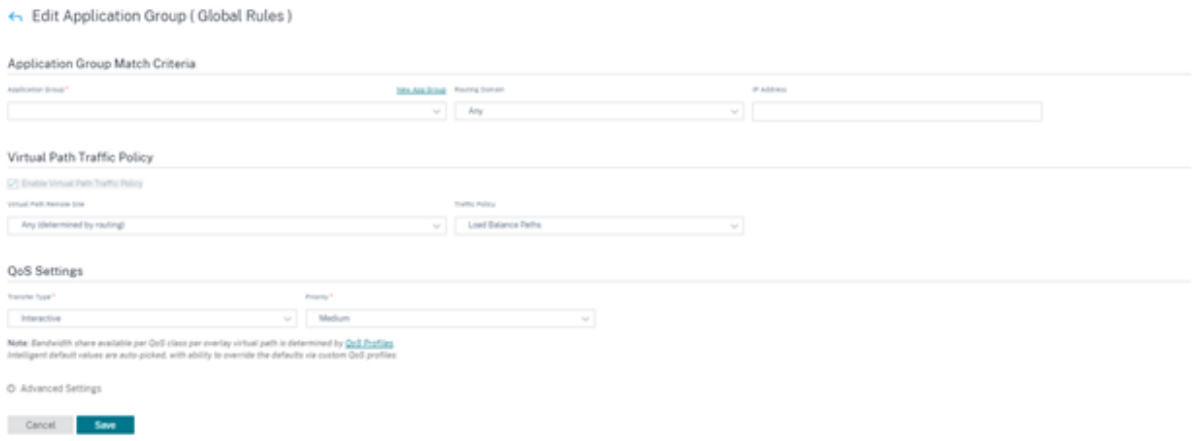


Création de règles de groupe d'applications

Vous pouvez créer des règles pour un groupe d'applications. Pour créer des règles de groupe d'applications, accédez à **Configuration > QoS > Politiques de QoS** > **Règles de groupe d'applications**. Sélectionnez l'onglet **Règles globales** pour créer des règles de groupe d'applications au niveau global ou **Règles spécifiques au site/au groupe** pour créer des règles au niveau du site.

Cliquez sur **Nouvelle règle de groupe** d'**applications dans la section Règles du groupe** d'applications. Cliquez sur **Nouveau groupe d'applications à côté dunom du champ du groupe**d'applications. Entrez un nom pour le groupe d'applications. Recherchez et ajoutez des applications selon vos besoins. Cliquez sur**Enregistrer**.

Entrez les informations nécessaires dans les autres champs. Pour plus d'informations sur les descriptions des champs, voir Création de règles d'application.



Vérifier les règles d'application

Pour vérifier les règles de l'application, accédez à **Rapports > Temps réel > Flux**. Sélectionnez le site pour lequel vous souhaitez consulter les informations sur les flux et le nombre de flux à afficher. Cliquez sur **Personnaliser les colonnes** et cochez les cases correspondant aux informations de flux que vous souhaitez afficher. Vérifiez si les informations de flux sont conformes aux règles configurées.

Accédez à **Rapports > Temps réel > Statistiques** et sélectionnez **Règles**. Choisissez le site et cliquez sur **Récupérer les dernières données**. Vérifiez les règles configurées.

Pour plus d'informations sur les rapports, voir Flows.

QoE HDX

October 21, 2022

Les paramètres réseau tels que la latence, la gigue et la perte de paquets affectent l'expérience utilisateur des utilisateurs HDX. La qualité de l'expérience (QoE) aide les utilisateurs à comprendre et à vérifier la qualité de leur expérience ICA. QoE est un indice calculé, qui indique les performances du trafic ICA. Les utilisateurs peuvent ajuster les règles et la stratégie pour améliorer la QoE.

La QoE est une valeur numérique comprise entre 0 et 100, plus la valeur est élevée, plus l'expérience utilisateur est bonne.

Les paramètres utilisés pour calculer la QoE sont mesurés entre les deux appliances Citrix SD-WAN situées côté client et côté serveur et non entre le client ou les appliances serveur elles-mêmes. La latence, la gigue et la chute de paquets sont mesurées au niveau du flux et elles peuvent être différentes

des statistiques au niveau du lien. L'application hôte final (client ou serveur) peut ne jamais savoir qu'il y a une perte de paquets sur le WAN. Si la retransmission réussit, le taux de perte de paquets au niveau du flux est inférieur à la perte de niveau de liaison. Cependant, par conséquent, cela peut augmenter un peu la latence et la gigue.

Vous pouvez afficher une représentation graphique de la qualité globale des applications HDX dans le tableau de bord HDX sur Citrix SD-WAN Orchestrator pour les applications locales. Les applications HDX sont classées dans les trois catégories de qualité suivantes :

Qualité	Gamme QoE
Good	71-100
Fair	51-70
Poor	0-50

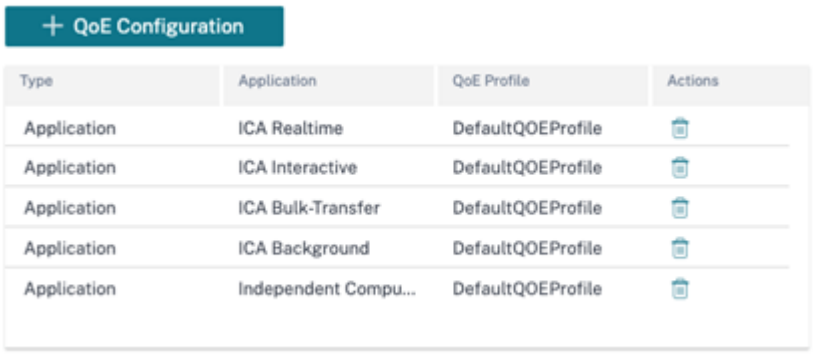
En fonction de la page d'interface utilisateur sélectionnée, une liste des cinq sites, des cinq utilisateurs, des cinq sessions les plus bas (moins de QoE) est affichée dans le tableau de bord HDX.

Une représentation graphique de la QoE pour différents intervalles de temps vous permet de surveiller les performances des applications HDX sur chaque site.

Configurer HDX QoE

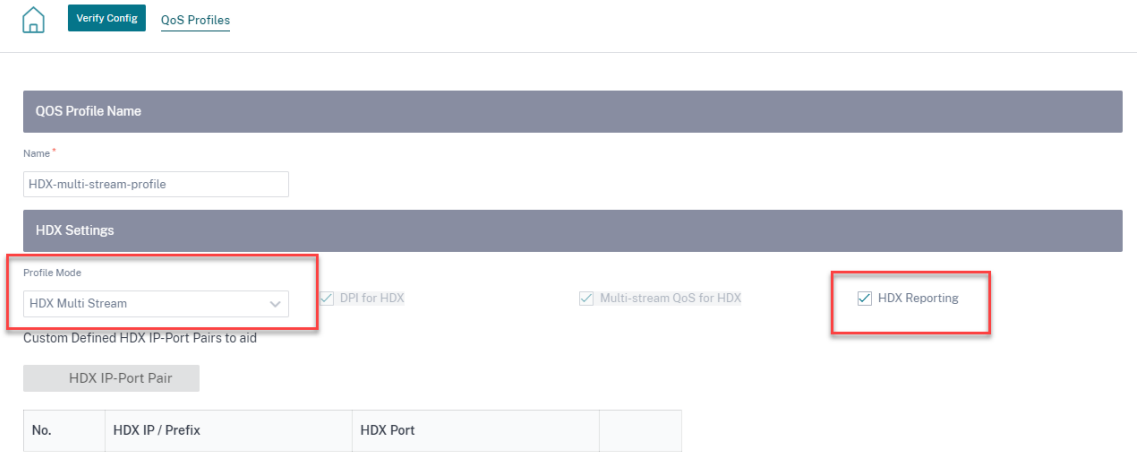
1. Au niveau du réseau, accédez à **Configuration > Paramètres et groupes de l'application > Configuration de la qualité de l'application** et cliquez sur **+ Configuration QoE**. Ajoutez les applications suivantes à l'aide du profil QoE que vous souhaitez utiliser pour le calcul du comportement HDX :

    - ICA en temps réel (ica_priority_0)
    - ICA Interactive (ica_priority_1)
    - Transfert en masse ICA (ica_priority_2)
    - Contexte ICA (ica_priority_3)
    - Architecture informatique indépendante (Citrix) (ICA)

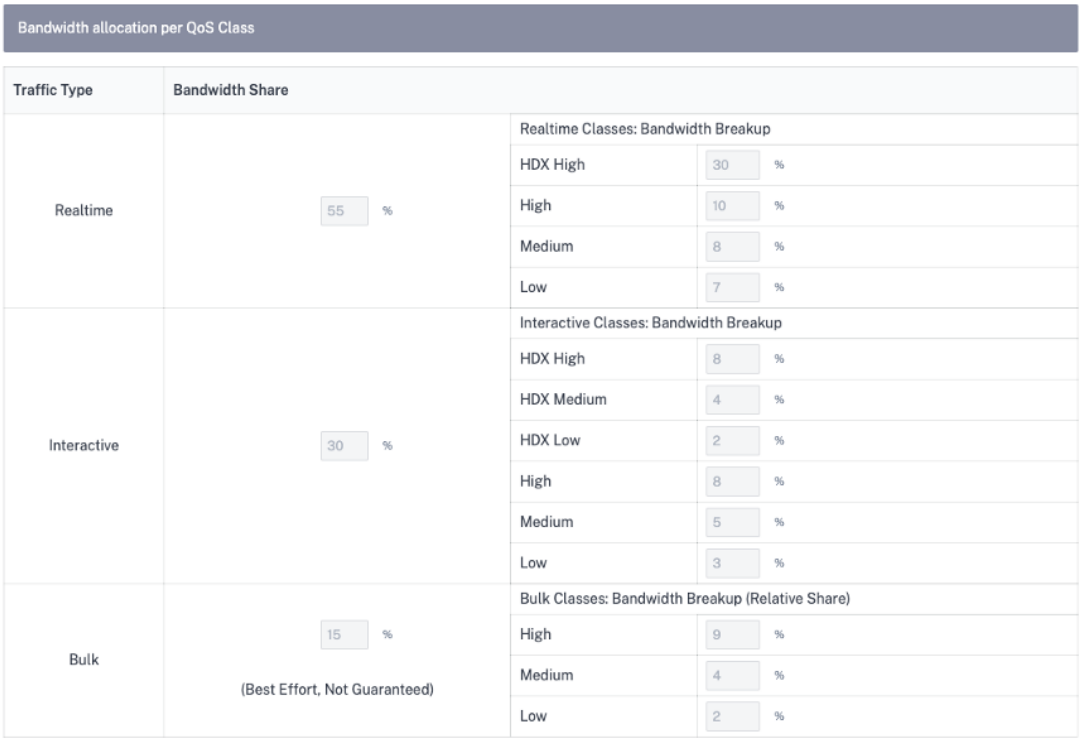


Ces configurations fournissent les paramètres permettant de mesurer les performances HDX utilisées dans le rapport HDX via le profil. La configuration d'ICA Real-time, d'ICA Interactive, d'ICA Bulk-Transfer et d'ICA Background est requise pour les connexions HDX Multi-Stream (MSI), tandis que l'architecture informatique indépendante (Citrix) est requise pour les connexions Single Stream (SSI).

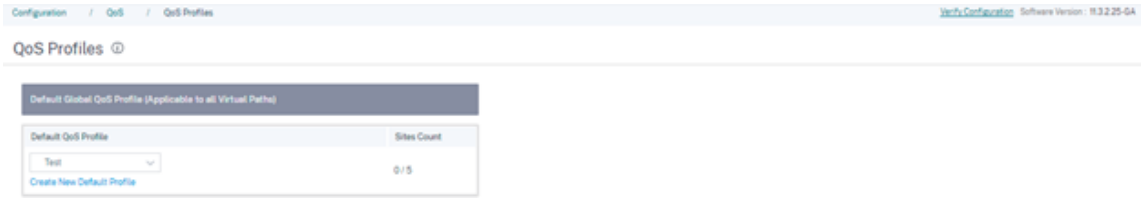
2. Accédez à **Configuration > QoS > Profils QoS**. Sélectionnez **Standard-HDX-MultiStream** comme profil QoS par défaut et cochez la case **HDX Reporting** . **Effacez le reporting HDX** si le reporting HDX n'est pas requis.



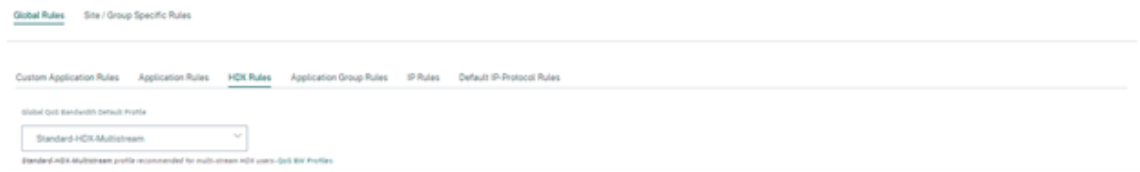
Dans chaque profil de QoS, il existe un pourcentage de bande passante prédéfini pour chaque classe. Ils sont configurables pour ajuster la bande passante attribuée aux classes utilisées par le trafic HDX.



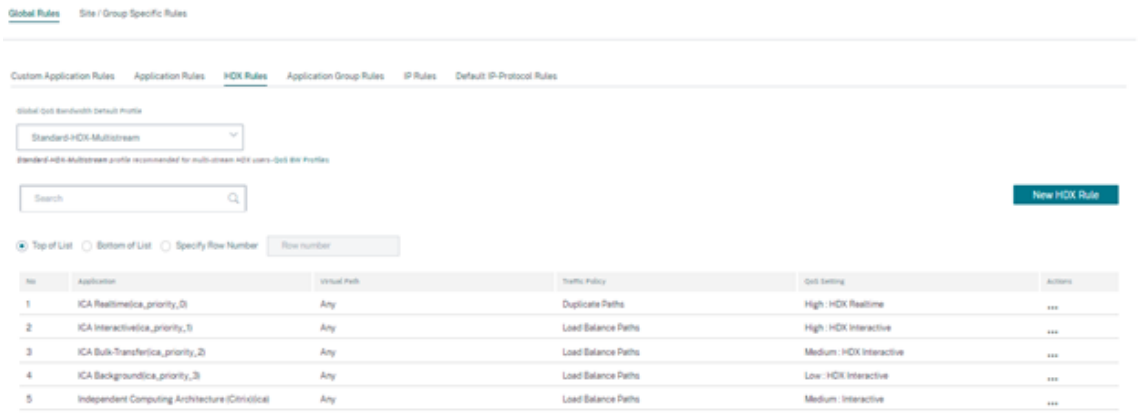
3. Assurez-vous que le nouveau profil QoS est activement utilisé en vérifiant l'indicateur **Nombre de sites** .



4. Accédez à **Configuration > QoS > Politiques de QoS** > **Règles HDX**et définissez le nouveau profil de QoS avec les rapports HDX activés en tant que **profil par défaut de bande passante QoS globale**.

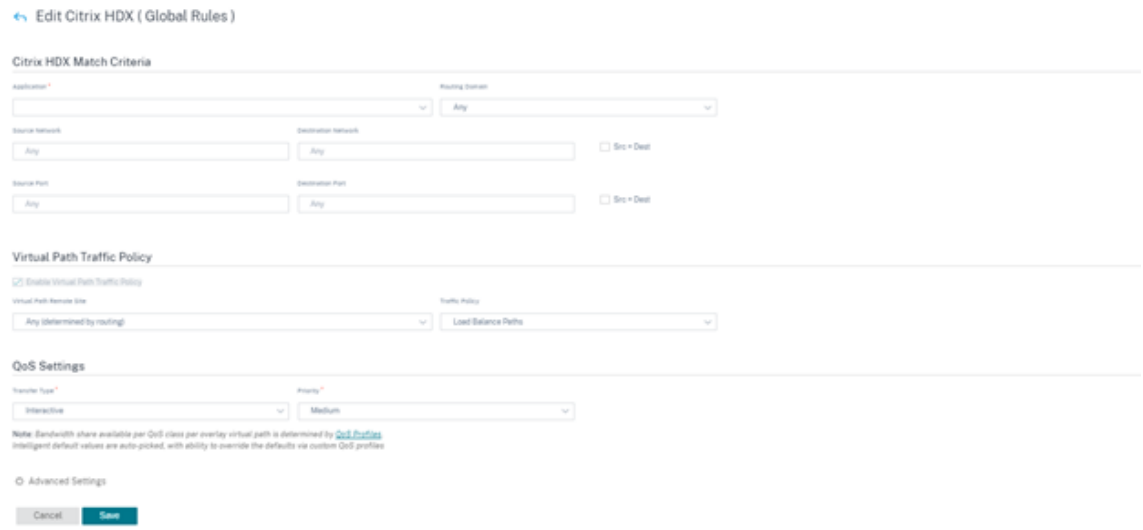


5. Ajoutez des règles HDX. Ces configurations attribuent des paramètres de QoS appropriés aux connexions HDX. Pour vérifier les détails des règles ou les modifier, accédez à la section inférieure de la page des **règles HDX** . Dans le tableau Règles, accédez à la colonne **Actions** et sélectionnez **Modifier**. Pour modifier le paramètre d'une règle par défaut, cliquez sur **Cloner** et apportez les modifications nécessaires.



Ces configurations peuvent être modifiées :

- Classe de QoS : temps réel, interactif, en masse
- Politique de circulation :
  - **Chemins dupliqués** : Le trafic sera dupliqué sur plusieurs chemins pour améliorer la fiabilité.
  - **Chemin persistant** : le trafic d'un flux restera sur le même chemin, sauf si le chemin devient indisponible.
  - **Chemins d'équilibrage**de charge : Le trafic d'un flux est équilibré sur plusieurs chemins.
  - **Paramètres avancés** : définissez les politiques de retransmission, de RED et de paquets en retard.



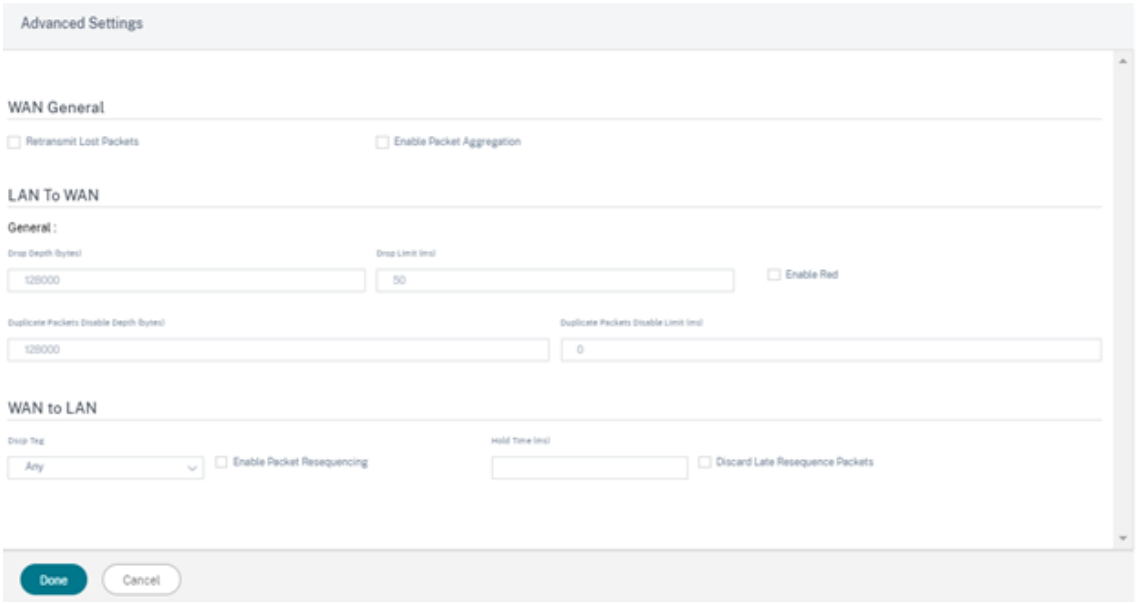


Tableau de bord et rapports HDX

Citrix SD-WAN Orchestrator pour locaux fournit le tableau de bord HDX pour des mesures détaillées et actualisées de l'expérience utilisateur de Citrix Virtual Applications and Desktops sur le réseau, pour chaque site, utilisateur et session.

Il existe deux types de sessions HDX : un seul flux et plusieurs flux. Une session à flux unique n'a qu'une seule connexion dans la session, alors qu'une session multi-flux en a quatre. Les sessions multi-flux permettent des QoS plus avancés. La connexion dans une session HDX à flux unique est par défaut la classe interactive, tandis que la connexion prioritaire d'une session HDX multi-flux par défaut est la classe en temps réel et les trois autres à la classe interactive. Ceci est configurable.

Le score de qualité d'expérience (QoE) est une valeur numérique comprise entre 0 et 100. Plus la valeur est élevée, meilleure est l'expérience utilisateur. Le trafic de classe en temps réel QoE est calculé en fonction de la gigue, de la latence et du taux de perte. La classe interactive QoE est calculée en fonction du taux d'éclatement et du taux de perte. Le QoE d'une session est la moyenne de toutes les connexions de la session. Le QoE d'un utilisateur est la moyenne de toutes les sessions lancées par cet utilisateur. Le QoE d'un site est la moyenne de toutes les sessions sur ce site.

Toutes les statistiques sont des mesures :

- Pour le trafic HDX sur ce site
- Expérimenté par cet utilisateur
- De toutes les connexions de cette session

Ils n'incluent pas les mesures d'autres types de trafic. Les mesures sont soit la moyenne sur la période sélectionnée, soit le total sur la période sélectionnée.

> **Remarque :**
>
> les rapports HDX nécessitent des versions logicielles minimales :
>
> - Citrix Virtual Apps and Desktops 7—1912 LTSR (ou version actuelle)
> - Application Citrix Workspace pour Windows 19.12 LTSR (ou version actuelle)
> - SD-WAN 11.2.0 (ou version actuelle)

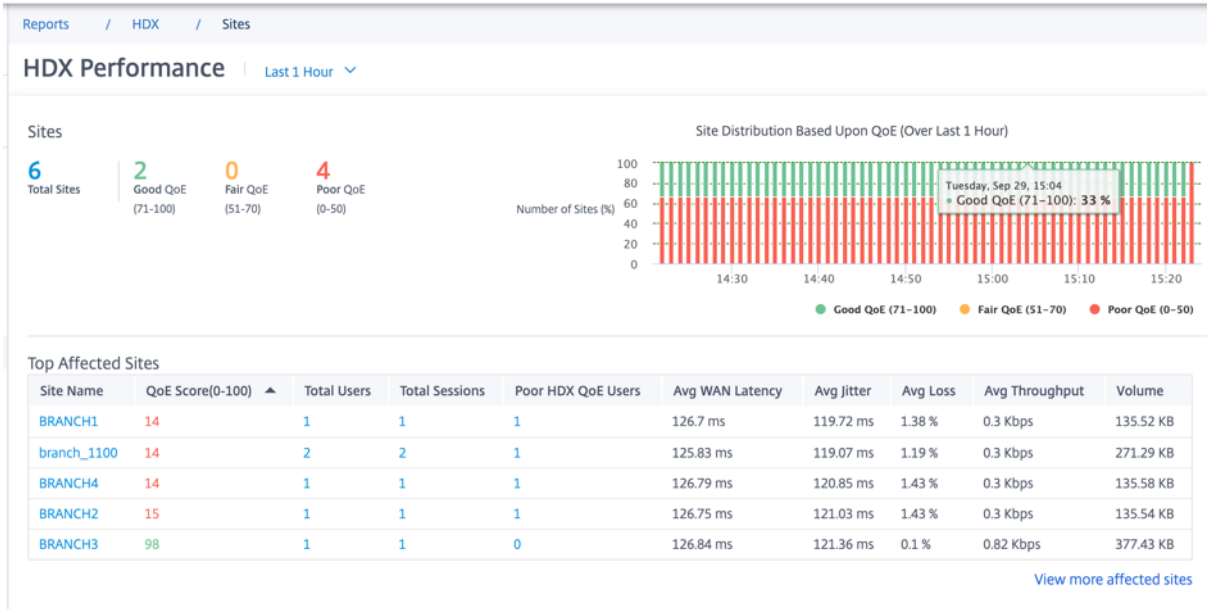
Citrix recommande toujours d'utiliser la dernière version du logiciel pour obtenir les dernières corrections de bogues et améliorations. Par exemple, le SD-WAN nécessite la version 11.2.3 ou 11.3.1 pour prendre en charge les nouvelles commandes EDT introduites dans les versions ultérieures de Citrix Virtual Apps and Desktops LTSR.

Les clients Mac et Linux ne bénéficient pas d'une prise en charge complète des rapports ICA et HDX multi-flux via Citrix SD-WAN. Par exemple, les clients Linux prennent en charge le multistream, mais manquent de détails tels que le temps d'aller-retour et le délai. La matrice des fonctionnalités CWA fournit des informations sur les systèmes d'exploitation qui prennent en charge les fonctionnalités **ICA multiport** et **HDX Insight avec NSAP VC** .

Les utilisateurs doivent accéder à HDX en dehors du chiffrement Citrix Gateway, soit via un accès direct à StoreFront, soit en utilisant des Beacon Points ou le service de localisation réseau.

Sites

Ce rapport HDX fournit des données HDX détaillées par site. Pour consulter les statistiques du site, accédez à **Rapports** > **HDX** > **Sites**.



Le tableau de bord indique sur site le trafic HDX en cours d'exécution pendant l'intervalle de temps sélectionné (par exemple, 5 dernières minutes, 30 dernières minutes, 1 dernier jour, 1 dernier mois, etc.). Les performances du site sont classées comme bonnes (71 à 100), passables (51-70) ou médiocres (0-50) en fonction du QoE du trafic HDX du site. La valeur de QoE dans la section récapitulative et **dans le tableau des sites les plus affectés** est la valeur moyenne sur la période sélectionnée. Le rapport graphique de séries chronologiques montre l'historique détaillé avec le temps écoulé. Chaque barre indique le pourcentage de bons, passables et mauvais sites QoE à ce moment-là.

Vous pouvez également consulter le nombre de sites en pourcentage présentant une QoE bonne, passable et mauvaise à ce moment-là dans le graphique de **distribution des sites basé sur la QoE** . Passez votre souris sur la barre de couleurs pour voir le pourcentage de sites dans un état bon/passé/mauvais.

> **REMARQUE**
>
> - Les statistiques sont collectées dans une direction, du côté distant vers le site actuel. Par exemple, pour une session entre le site-A et le site-B, le rapport du site-A est recueilli sur le trafic provenant du site-B vers le site-A, tandis que le rapport du site-B est recueilli sur le trafic provenant du site-A vers le site-B. Par conséquent, les statistiques de la même session sur le site a et le site-B peuvent être différentes.
> - Le **tableau des sites les plus touchés** ne reflète que les 5 sites les plus touchés. Par défaut, il affiche les 5 sites avec les scores QoE les plus faibles. Mais chaque colonne est triable, ascendante ou décroissante, et utilisée comme critère de requête. Par exemple, si vous cliquez sur le titre de la colonne **Avg Jitter**, vous pouvez afficher les 5 sites présentant la plus faible instabilité moyenne ou la plus élevée. Même chose pour les autres colonnes. Pour voir les détails de tous les sites avec du trafic HDX pendant la période sélectionnée, cliquez sur **Afficher plus de sites concernés**.

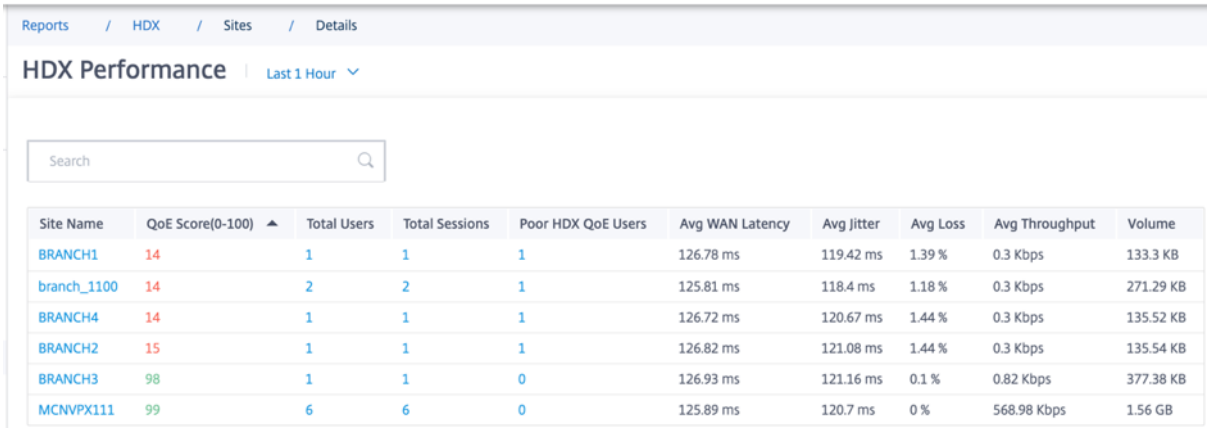
Voici les détails de chaque site :

- **Nom du site** : nom du site.
- **Score QoE (0-100)** : score QoE moyen de ce site.
- **Nombre total d'utilisateurs** : nombre total d'utilisateurs HDX actifs vus sur le site pendant la période sélectionnée.
- Nombre**total de sessions** : nombre total de sessions HDX consultées sur le site pendant la période sélectionnée, y compris les sessions à flux unique et à flux multiples.
- **Utilisateurs HDX QoE médiocres** : nombre d'utilisateurs HDX souffrant d'une mauvaise QoE (moins de 50).
- **Latence WAN**moyenne : latence moyenne sur le WAN, du site distant vers ce site.
- **Jitter moyen** : valeur de gigue moyenne pour la durée sélectionnée.
- **Perte moyenne** : valeur moyenne en pourcentage de perte de paquets pour la durée sélectionnée.

- **Débit moyen** : valeur moyenne du débit de données pour la durée sélectionnée.
- **Volume : volume**de trafic total vu sur ce site. L'interface graphique Citrix SD-WAN Orchestrator pour site Web peut ajuster et modifier l'unité en fonction de la valeur numérique.

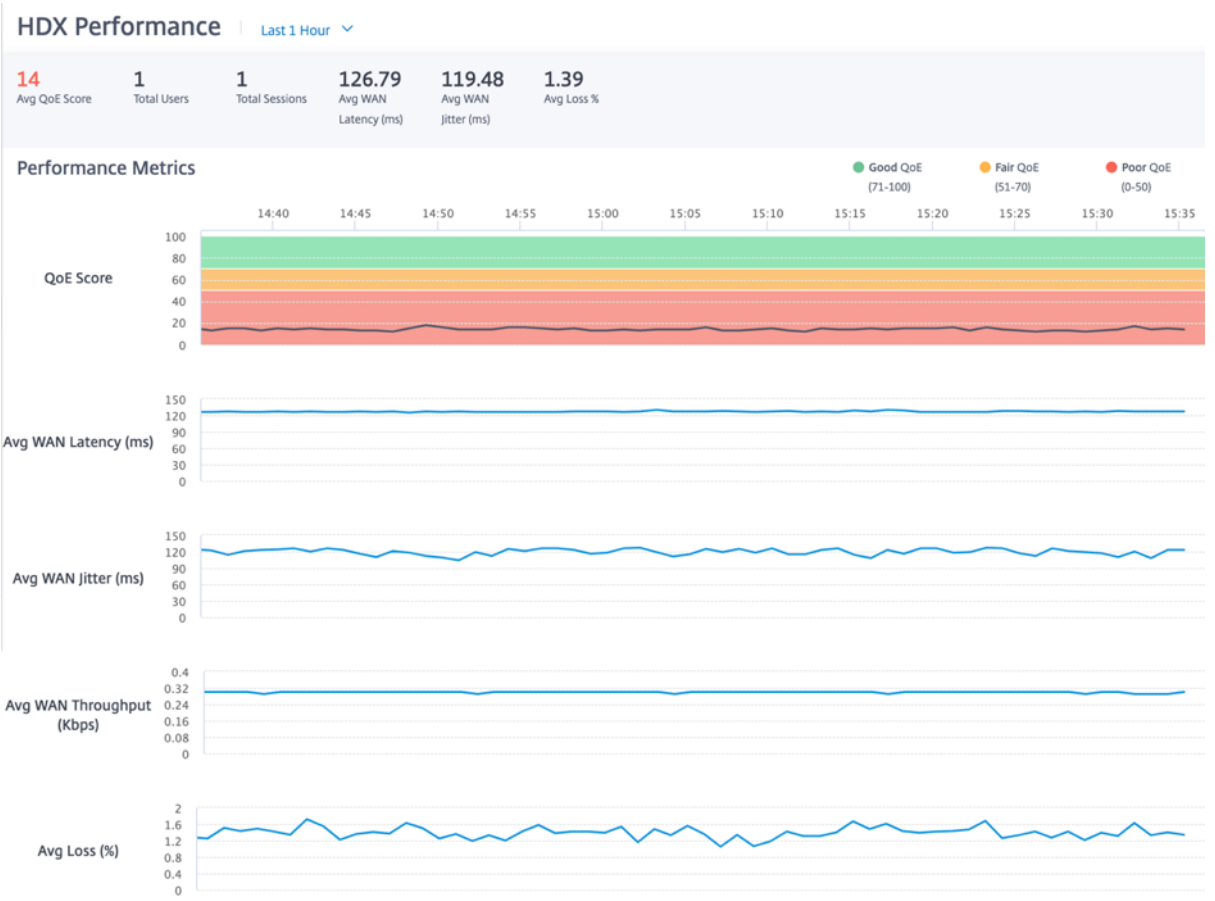
Cliquez sur un titre de colonne pour afficher le rapport trié sur cette colonne. Cliquez sur **Afficher plus de sites concernés** pour consulter les rapports de tous les sites. Cliquez sur une ligne unique pour afficher le rapport détaillé de ce site.

Le tableau de la capture d'écran suivante est un exemple de tableau de rapport présentant tous les sites. Il comporte les mêmes colonnes que le tableau des **sites les plus touchés** .



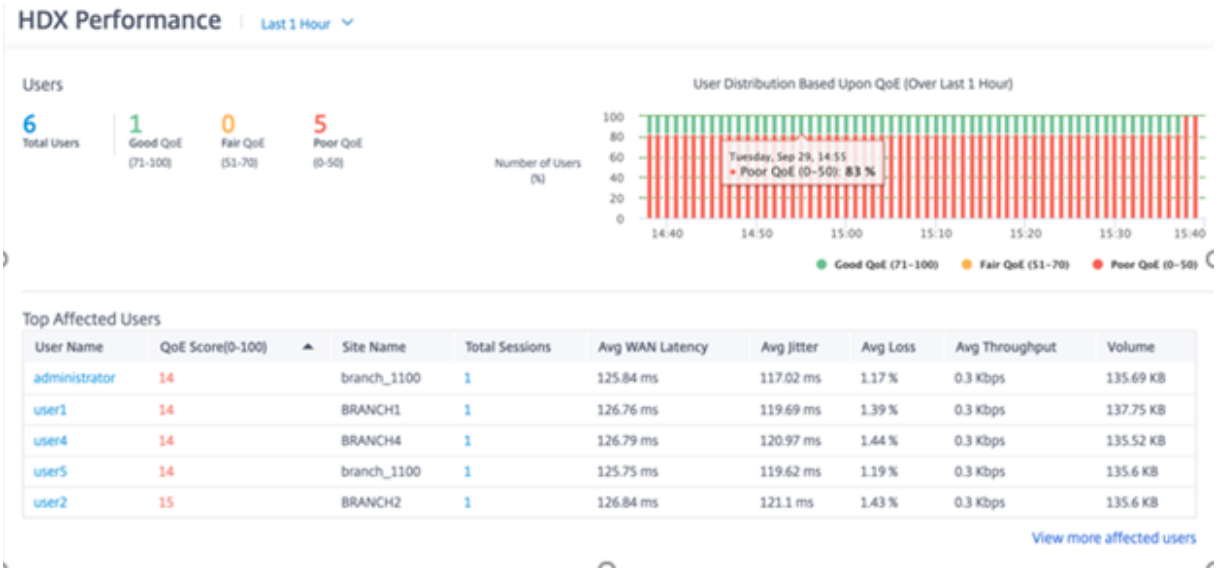
Site Name	QoE Score(0-100)	Total Users	Total Sessions	Poor HDX QoE Users	Avg WAN Latency	Avg Jitter	Avg Loss	Avg Throughput	Volume
BRANCH1	14	1	1	1	126.78 ms	119.42 ms	1.39 %	0.3 Kbps	133.3 KB
branch_1100	14	2	2	1	125.81 ms	118.4 ms	1.18 %	0.3 Kbps	271.29 KB
BRANCH4	14	1	1	1	126.72 ms	120.67 ms	1.44 %	0.3 Kbps	135.52 KB
BRANCH2	15	1	1	1	126.82 ms	121.08 ms	1.44 %	0.3 Kbps	135.54 KB
BRANCH3	98	1	1	0	126.93 ms	121.16 ms	0.1 %	0.82 Kbps	377.38 KB
MCNVPX111	99	6	6	0	125.89 ms	120.7 ms	0 %	568.98 Kbps	1.56 GB

Cliquez sur la ligne de site individuelle pour afficher une représentation graphique des mesures de performances. Passez la souris sur le graphique pour obtenir plus de détails.



Users

Pour consulter le rapport sur les utilisateurs HDX, accédez à **Rapports > HDX > Utilisateurs**.



Le rapport utilisateur indique les performances enregistrées par chaque utilisateur au cours de la péri-

ode sélectionnée (par exemple, les 5 dernières minutes, les 30 dernières minutes, le dernier jour, le dernier mois, etc.). Si l'utilisateur a été sur plusieurs sites au cours de la période sélectionnée, le dernier site à partir de lequel l'utilisateur s'est connecté est affiché dans le rapport. L'expérience utilisateur est classée comme bonne (71 à 100), passable (51-70) ou mauvaise (0-50) en fonction du score QoE de leur trafic HDX. Les valeurs de QoE figurant dans la section récapitulative et **dans le tableau des utilisateurs les plus affectés** sont les valeurs moyennes sur la période sélectionnée. Le rapport graphique de séries chronologiques montre l'historique détaillé avec le temps écoulé. Chaque barre indique le pourcentage d'utilisateurs ayant une QoE bonne, passable et médiocre à ce moment-là.

Vous pouvez également consulter le nombre d'utilisateurs en pourcentage ayant une QoE bonne, passable et médiocre à ce moment-là dans le graphique de **distribution des utilisateurs basée sur la QoE** . Passez votre souris sur la barre de couleurs pour voir le pourcentage d'utilisateurs en bon état, passé/mauvais.

Informations personnelles identifiables Actuellement, les rapports HDX QoE contiennent les deux champs d'informations personnelles (PII) suivants :

- **Nom d'utilisateur** : affiche le nom d'utilisateur.
- **Adresse IP** : affiche l'adresse IP du client.

> **REMARQUE**
>
> - Lorsque le nom d'utilisateur n'est pas disponible, l'adresse IP est affichée dans le champ **Nom d'utilisateur** .
> - Les rapports utilisateur HDX sont basés sur des statistiques provenant du SD-WAN côté client, et non du SD-WAN côté Virtual Delivery Agent (VDA). Cela reflète l'expérience HDX de l'utilisateur final.
> - Le **tableau des utilisateurs les plus touchés** ne reflète que les 5 utilisateurs les plus touchés. Par défaut, il affiche les 5 meilleurs utilisateurs ayant le QoE le plus bas. Mais chaque colonne est triable, ascendante ou décroissante, et utilisée comme critère de requête. Par exemple, si vous cliquez sur le titre de la colonne **Avg Jitter**, vous pouvez afficher les 5 utilisateurs présentant la gigue moyenne la plus faible ou la plus élevée. Pour voir les détails de tous les utilisateurs ayant reçu du trafic HDX au cours de la période sélectionnée, cliquez sur **Afficher plus d'utilisateurs concernés**.

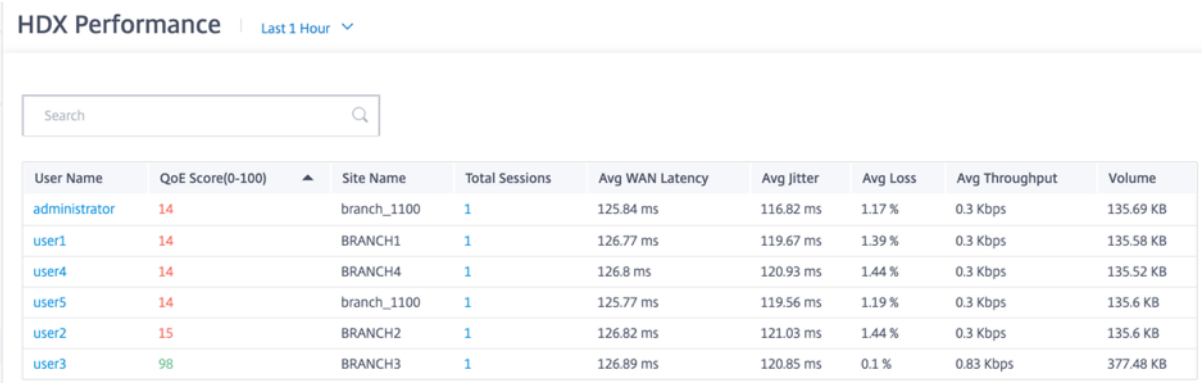
Voici les détails de chaque utilisateur :

- **Nom d'utilisateur** : nom d'utilisateur.
- **Score QoE (0-100)** : score QoE moyen de cet utilisateur.
- **Nom du site** : nom du site à partir duquel l'utilisateur s'est connecté.
- Nombre**total de sessions** : nombre total de sessions HDX actives de cet utilisateur, y compris les sessions à flux unique et à flux multiples.

- **Latence WAN**moyenne : latence moyenne sur le WAN, constatée côté client.
- **Jitter moyen** : valeur de gigue moyenne pour la durée sélectionnée.
- **Perte moyenne** : valeur moyenne en pourcentage de perte de paquets pour la durée sélectionnée.
- **Débit moyen** : valeur moyenne du débit de données pour la durée sélectionnée.
- **Volume : volume**de trafic total utilisé par cet utilisateur. L'interface graphique Citrix SD-WAN Orchestrator pour site Web peut ajuster et modifier l'unité en fonction de la valeur numérique.

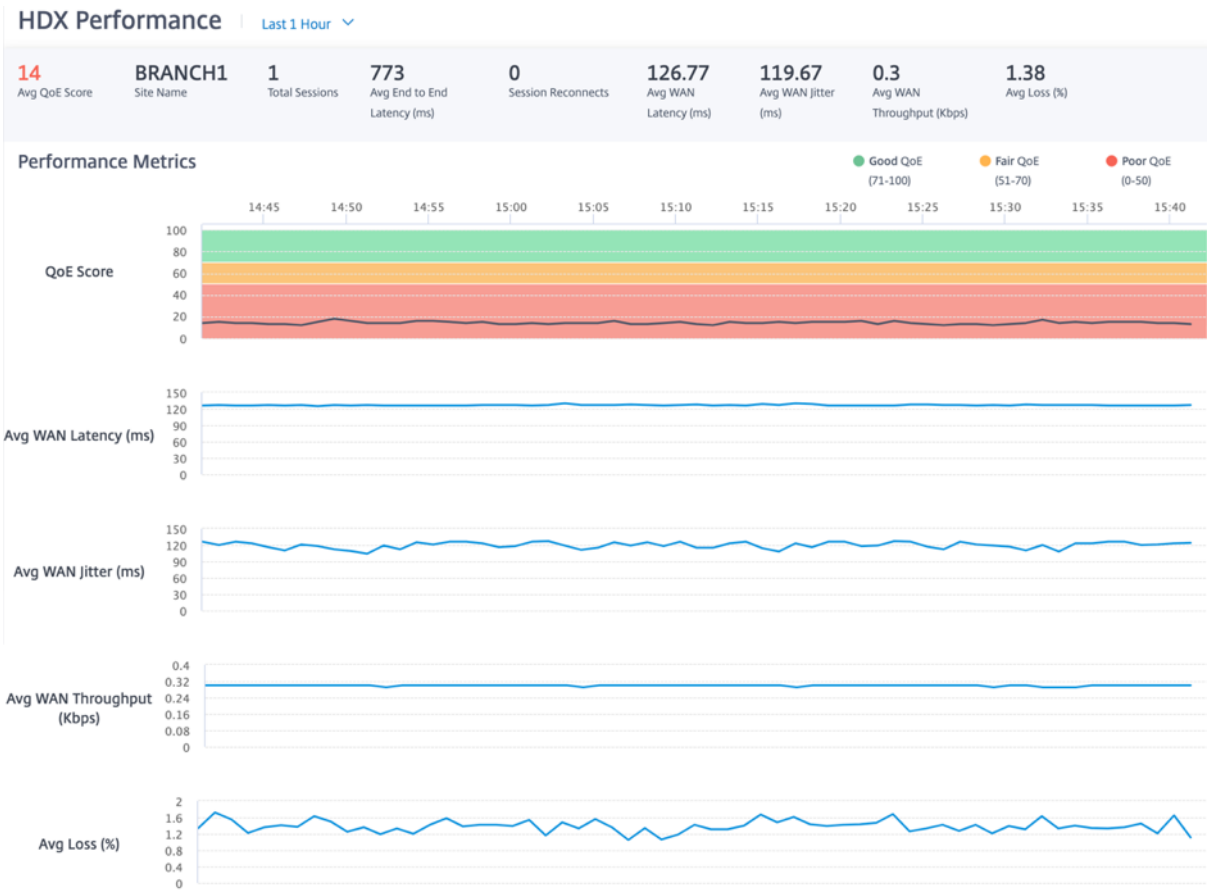
Cliquez sur un titre de colonne pour afficher le rapport trié sur cette colonne. Cliquez sur **Afficher plus d'utilisateurs concernés** pour consulter les rapports de tous les utilisateurs. Cliquez sur une ligne unique pour afficher le rapport détaillé de cet utilisateur.

La capture d'écran suivante est un exemple du rapport affichant tous les utilisateurs. Il comporte les mêmes colonnes que le tableau des **utilisateurs les plus touchés** .



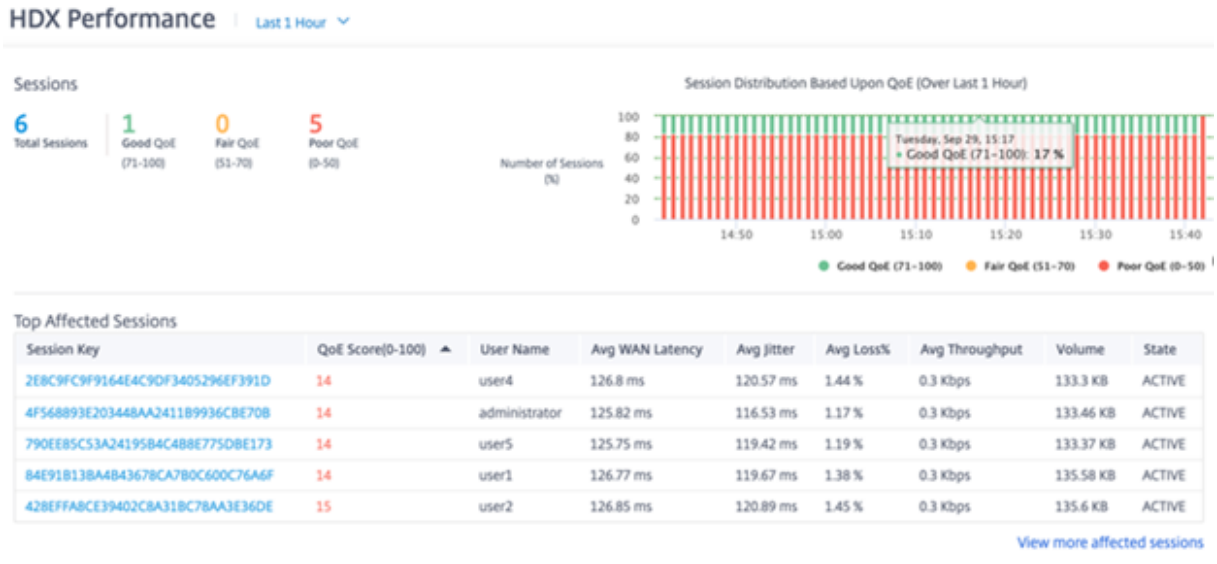
User Name	QoE Score(0-100)	Site Name	Total Sessions	Avg WAN Latency	Avg Jitter	Avg Loss	Avg Throughput	Volume
administrator	14	branch_1100	1	125.84 ms	116.82 ms	1.17 %	0.3 Kbps	135.69 KB
user1	14	BRANCH1	1	126.77 ms	119.67 ms	1.39 %	0.3 Kbps	135.58 KB
user4	14	BRANCH4	1	126.8 ms	120.93 ms	1.44 %	0.3 Kbps	135.52 KB
user5	14	branch_1100	1	125.77 ms	119.56 ms	1.19 %	0.3 Kbps	135.6 KB
user2	15	BRANCH2	1	126.82 ms	121.03 ms	1.44 %	0.3 Kbps	135.6 KB
user3	98	BRANCH3	1	126.89 ms	120.85 ms	0.1 %	0.83 Kbps	377.48 KB

Cliquez sur une ligne utilisateur individuelle pour afficher une représentation graphique des mesures de performances de cet utilisateur.



Sessions

Le rapport de session fournit des détails au niveau de la session. Pour consulter le rapport de session, accédez à **Rapports > HDX > Sessions**.



Le tableau de bord affiche les rapports des sessions HDX exécutées pendant la période sélectionnée (par exemple, les 5 dernières minutes, les 30 dernières minutes, le dernier jour, le dernier mois, etc.). Les séances sont classées comme bonnes (71 à 100), passables (51-70) ou médiocres (0-50) en fonction de la QoE de cette session. La valeur QoE dans la section récapitulative et la table des sessions les plus affectées est la valeur moyenne sur la période sélectionnée. Le rapport graphique de séries chronologiques montre l'historique détaillé avec le temps écoulé. Chaque barre indique le pourcentage de bonnes, passables et médiocres sessions QoE à ce moment-là.

Vous pouvez également consulter le nombre de sessions en pourcentage, avec une QoE bonne, passable et mauvaise à ce moment-là dans le graphique de **distribution des sessions basée sur la QoE** . Passez votre souris sur la barre de couleurs pour voir le pourcentage de sessions en bon état, passé/-mauvais.

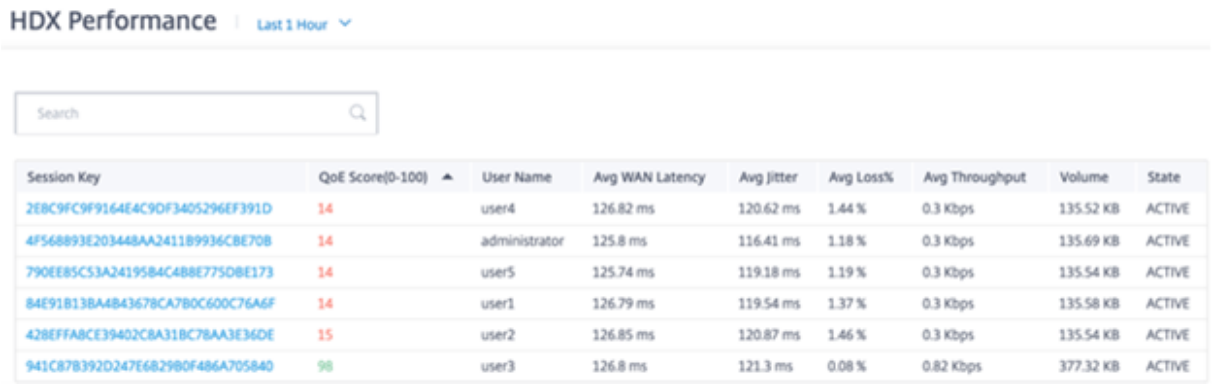
> **Remarque**
>
> - Les rapports de session HDX sont basés sur des statistiques provenant du SD-WAN côté client, et non du SD-WAN côté VDA. Cela reflète l'expérience HDX de l'utilisateur final.
> - Le **tableau des sessions les plus touchées** ne reflète que les 5 sessions les plus touchées. Par défaut, il affiche les 5 premières sessions avec la QoE la plus faible. Mais chaque colonne est triable, ascendante ou décroissante, et utilisée comme critère de requête. Par exemple, si vous cliquez sur le titre de la colonne **Avg Jitter**, vous pouvez afficher les 5 sessions présentant la gigue moyenne la plus faible ou la plus élevée. Pour voir les détails de toutes les sessions HDX pendant la période sélectionnée, cliquez sur **Afficher plus de sessions concernées**.

Voici le détail de la partie supérieure de chaque session :

- **Clé de session** : identité unique d'une session HDX.
- **Score QoE (0-100)** : la QoE moyenne de cette session.
- **Nom d'utilisateur** : nom d'utilisateur.
- **Latence WAN**moyenne : latence WAN moyenne de la session pendant la durée sélectionnée, mesurée côté client.
- **Jitter moyen** : valeur de gigue moyenne de la session pendant la durée sélectionnée.
- **% de perte moyenne** : valeur moyenne en pourcentage de perte de la session pour la durée sélectionnée.
- **Débit moyen** : valeur de débit moyenne de la session pour la durée sélectionnée.
- **Volume : volume**de trafic total utilisé par cette session. L'interface graphique Citrix SD-WAN Orchestrator pour site Web peut ajuster et modifier l'unité en fonction de la valeur numérique.
- **État : État**de la session.

Cliquez sur un titre de colonne pour afficher le rapport trié sur cette colonne. Cliquez sur **Afficher plus de sessions concernées** pour voir les rapports de toutes les sessions. Cliquez sur une ligne unique pour afficher le rapport détaillé de cette session.

La capture d'écran suivante est un exemple du tableau de rapport présentant toutes les sessions. Il comporte les mêmes colonnes que le tableau des **sessions les plus touchées** .



Cliquez sur la clé de session individuelle pour afficher une représentation graphique des mesures de performances ainsi que les détails sur toutes les variables affectant QoE.

- **Score QoE moyen** : la QoE moyenne sur la période sélectionnée.
- **Nom d'utilisateur** : utilisateur qui a lancé cette session.
- **Nom du VDA** : nom du VDA à partir duquel le poste de travail/l'application publié est fourni.
- **Durée de la session : durée**active de cette session au cours de la période sélectionnée.
- **Nom du site** : site client de l'utilisateur lorsque la session a été lancée.
- **VD/VA** : si cette session est une session de **bureau virtuel** ou une session d'**application virtuelle** .
- **État de la session** : État de la session à la fin de la période sélectionnée.

- **Type de session** : indique s'il s'agit d'une session multi-flux ou d'une session à flux unique lors du dernier lancement de la session.
- **Optimisé pour le WAN** : si cette session a été optimisée pour le WAN. Si le SD-WAN est une plate-forme PE, l'optimisation WAN est activée pour HDX et que cette session est optimisée, alors ce champ indique true.
- **Reconnexions de session** : si la session a été déconnectée et reconnectée automatiquement en raison d'un problème réseau, ce champ indique le nombre de ces occurrences.
- **Service réseau** : il s'agit du nom du service via lequel cette session est diffusée.
- **Latence HDX de bout**en bout : la moitié de la valeur du temps aller-retour entre le VDA et le client.
- **Latence WAN** : latence entre le SD-WAN côté VDA et le SD-WAN côté client.

Règles IP

October 21, 2022

Les règles IP vous aident à créer des règles pour votre réseau et à prendre certaines décisions en matière de qualité de service (QoS) en fonction de ces règles. Vous pouvez créer des règles personnalisées pour votre réseau. Par exemple, vous pouvez créer une règle comme suit : Si l'adresse IP source est 172.186.30.74 et l'adresse IP de destination est 172.186.10.89, définissez la **politique de trafic** sur **Chemin persistant et letype de trafic**sur**Temps réel**.

Vous pouvez créer des règles pour les flux de trafic et les associer à des applications et à des classes. Vous pouvez spécifier des critères pour filtrer le trafic d'un flux et appliquer un comportement général, un comportement LAN vers WAN, un comportement WAN vers LAN et des règles d'inspection de paquets.

Vous pouvez créer des règles IP globales et spécifiques au site au niveau du réseau. Si un site est associé à la règle créée globalement, vous pouvez créer des règles spécifiques au site. Dans de tels cas, les règles spécifiques au site prévalent et remplacent la règle créée globalement.

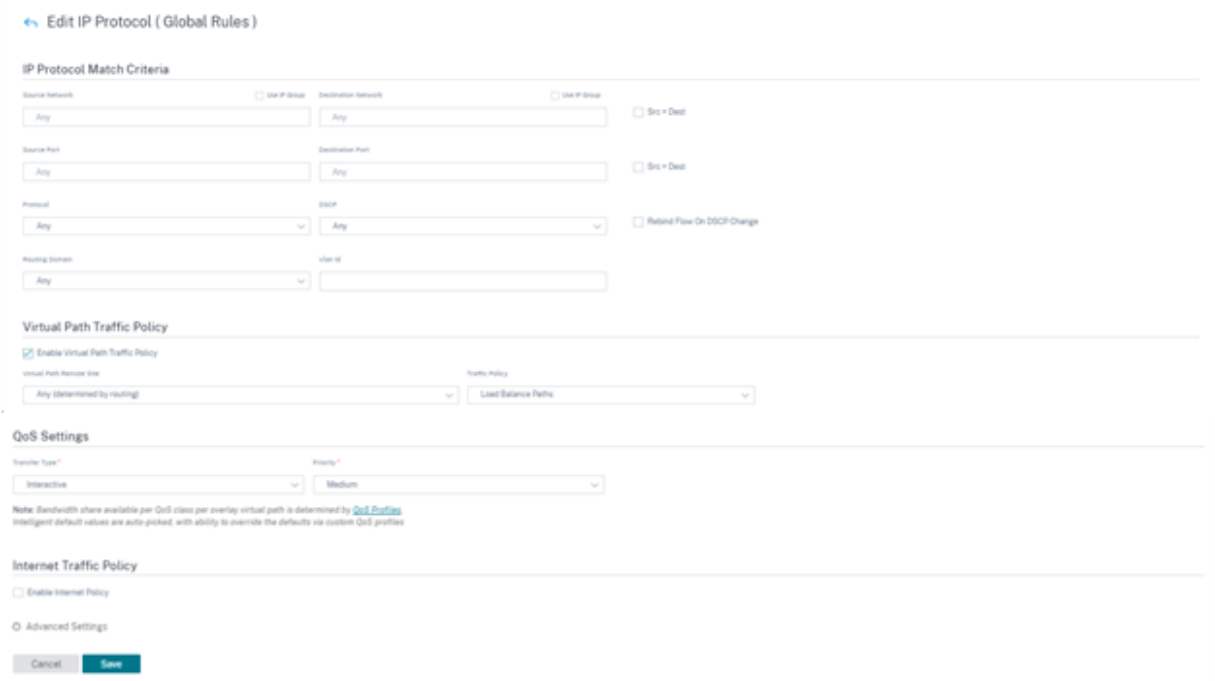
Les règles de protocole IP par défaut HTTP, HTTPS et ALTHTTPS apparaissent toujours en haut de la liste dans le tableau des règles. Toutefois, les règles IP spécifiques au site (une fois créées) apparaissent au-dessus des règles HTTP, HTTPS, ALTHTTPS et des règles IP globales dans le tableau des règles.

Création de règles IP

Pour créer des règles IP, accédez à **Configuration > QoS > Politiques de QoS** > **Règles IP**. Sélectionnez l'onglet **Règles globales** pour créer des règles IP au niveau global ou Règles **spécifiques au site/au**

groupe pour créer des règles au niveau du site.

Cliquez sur **Nouvelle règle IP** dans la section **Règles IP** .



- Critères de correspondance du protocole IP
  - **Ajouter/supprimer des sites** : (disponible uniquement lors de la création d'une règle IP spécifique au site) Sélectionnez les sites, cliquez sur **Vérifier**, puis sur **Terminé**.
  - **Réseau source** : adresse IP source et masque de sous-réseau auxquels la règle correspond.
  - **Réseau de destination** : adresse IP de destination et masque de sous-réseau auxquels la règle correspond.
  - **Utiliser un groupe IP** : cochez la case **Utiliser un groupe IP** pour sélectionner un groupe IP existant dans la liste déroulante.
  - **Src = Dst** : si cette option est sélectionnée, l'adresse IP source est également utilisée comme adresse IP de destination.
  - **Port source : port**source (ou plage de ports source) auquel la règle correspond.
  - **Port de destination** : port de destination (ou plage de ports de destination) auquel la règle correspond.
  - **Src = Dst** : si cette option est sélectionnée, le port source est également utilisé pour le port de destination.
  - **Protocole** : protocole auquel la règle correspond. Vous pouvez sélectionner l'un des protocoles prédéfinis, ou sélectionner **N'importe lequel**ou **Numéro**.
  - **Numéro de protocole** : Ce champ s'affiche uniquement lorsque vous sélectionnez **Numéro** dans la liste déroulante des **protocoles** . Lorsque vous sélectionnez un numéro

de protocole, l'entier associé au protocole est utilisé pour les configurations principales.
- **DSCP** : la balise DSCP dans l'en-tête IP à laquelle la règle correspond.
- **Domaine de routage** : domaine de routage auquel la règle correspond.
- **ID du VLAN** : Entrez l'ID du VLAN pour la règle. L'ID du VLAN identifie le trafic à destination et en provenance de l'interface virtuelle. Utilisez l'ID du VLAN comme 0 pour désigner le trafic natif ou non balisé.
- **Relier le flux lors d'une modification DSCP** : lorsque cette option est sélectionnée, les flux qui sont par ailleurs identiques en termes de critères de correspondance sont traités séparément si leurs champs DSCP diffèrent.

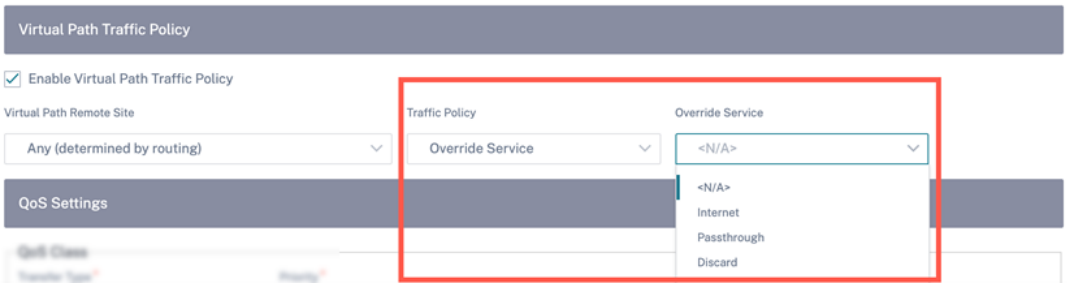
- Politique de trafic sur Virtual Path

  Cochez la case **Activer la politique de trafic sur les chemins virtuels** .

  - **Site distant par chemin virtuel** : sélectionnez le chemin virtuel du site distant.
  - **Politique de trafic** : Choisissez l'une des politiques de trafic suivantes selon vos besoins.
    - **Chemins d'équilibrage**de charge : le trafic d'applications pour le flux est équilibré sur plusieurs chemins. Le trafic est envoyé par le meilleur chemin jusqu'à ce que ce chemin soit utilisé. Les paquets restants sont envoyés par le meilleur chemin suivant.
    - **Chemin persistant** : le trafic de l'application reste sur le même chemin jusqu'à ce que le chemin d'accès ne soit plus disponible. Sélectionnez l'une des **politiques de persistance**suivantes :
      - **Persister sur le lien d'origine** : le trafic de l'application reste sur le lien d'origine jusqu'à ce que le chemin ne soit plus disponible.
      - **Persister sur le lien MPLS si disponible, sinon sur le lien d'origine** : le trafic de l'application reste sur le lien MPLS. Si la liaison MPLS n'est pas disponible, le trafic reste sur la liaison d'origine.
      - **Persister sur le lien Internet si disponible, sinon sur le lien d'origine** : le trafic de l'application reste sur le lien Internet. Si le lien Internet n'est pas disponible, le trafic reste sur le lien d'origine.
      - **Poursuivre sur le lien intranet privé si disponible, sinon sur le lien d'origine** : le trafic de l'application reste sur le lien intranet privé. Si le lien intranet privé n'est pas disponible, le trafic reste sur le lien d'origine.

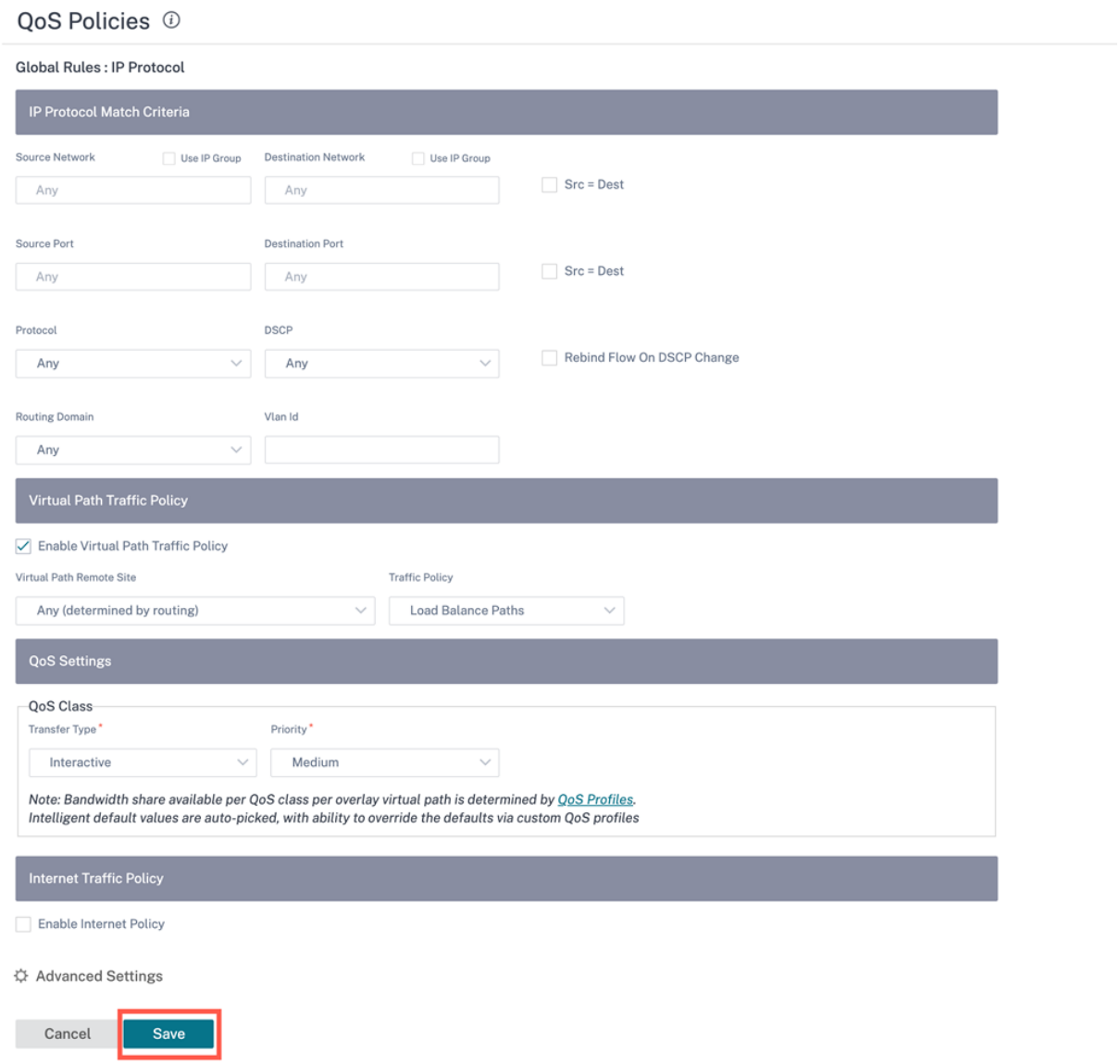
      L'**impédance de persistance** est le temps (en ms) pendant lequel le trafic de l'application reste sur le lien.
    - **Chemins dupliqués** : le trafic des applications est dupliqué sur plusieurs chemins, ce qui augmente la fiabilité
    - **Override Service** : Le trafic du flux est prioritaire vers un autre service. Sélectionnez le type de service Intranet, Internet, relais ou Discard auquel le service de chemin

virtuel remplace.

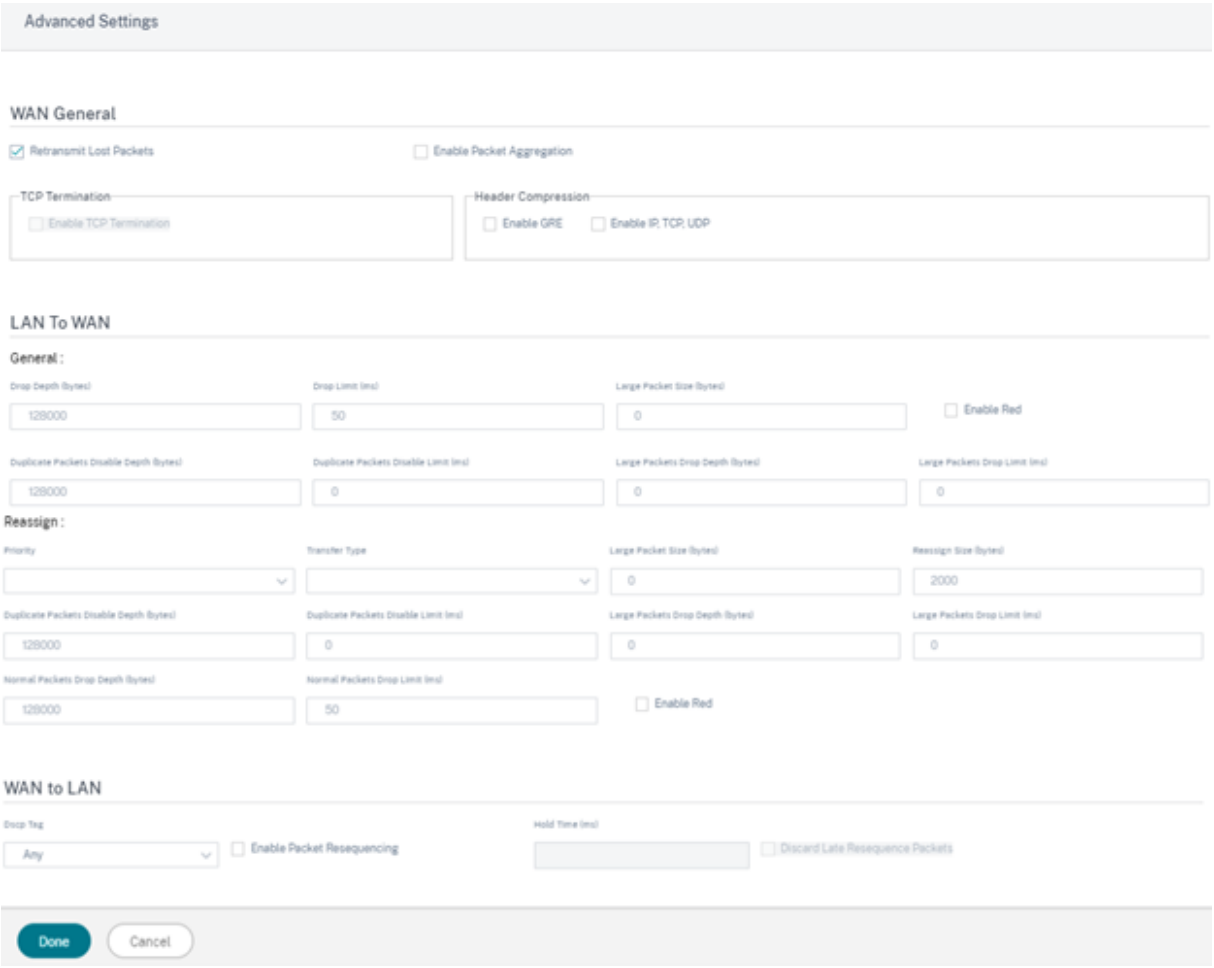


- Paramètres QoS (classe QoS)
  - **Type de transfert** : Choisissez l'un des types de transfert suivants :
    - **Temps réel** : utilisé pour le trafic à faible latence, à faible bande passante et sensible au temps. Les applications en temps réel sont urgentes mais n'ont pas vraiment besoin d'une bande passante élevée (par exemple, la voix sur IP). Les applications en temps réel sont sensibles à la latence et à l'instabilité, mais peuvent tolérer certaines pertes.
    - **Interactif** : Utilisé pour le trafic interactif avec des exigences de latence faible à moyenne et des exigences de bande passante faible à moyenne. L'interaction se fait généralement entre un client et un serveur. La communication peut ne pas nécessiter de bande passante élevée, mais elle est sensible à la perte et à la latence.
    - **Vrac** : Utilisé pour le trafic à bande passante élevée et les applications pouvant tolérer une latence élevée. Les applications qui gèrent le transfert de fichiers et nécessitent une bande passante élevée sont classées dans la catégorie des applications groupées. Ces applications impliquent peu d'interférence humaine et sont principalement traitées par les systèmes eux-mêmes.
  - **Priorité** : Choisissez une priorité pour le type de transfert sélectionné.
- Politique de trafic Internet
  - Cochez la case **Activer la politique Internet** pour configurer la politique de trafic Internet.
  - **Mode** : méthode de transmission et de réception de paquets pour les flux qui répondent à la règle. Vous pouvez choisir le **service de remplacement** ou **le lien WAN** selon vos besoins.
  - **Liaison WAN** : liaison WAN à utiliser par les flux correspondant à la règle lorsque l'équilibrage de charge Internet est activé.
  - **Override Service** : service de destination des flux correspondant à la règle.

> **Remarque**
>
> Un service de chemin virtuel ne peut pas remplacer un autre service de chemin virtuel.



Paramètres avancés



- WAN en général
  - **Retransmettre les paquets perdus** : envoie le trafic correspondant à cette règle à l'appliance distante via un service fiable et retransmet les paquets perdus.
  - **Activer l'agrégation de paquets** : regroupe les petits paquets en paquets plus volumineux.
  - **Activer la terminaison TCP** : Active la terminaison TCP du trafic pour ce flux. Le temps aller-retour pour l'accusé de réception des paquets est réduit, ce qui améliore le débit.
  - **Activer GRE** : compresse les en-têtes dans les paquets GRE.
  - **Activer IP, TCP et UDP** : compresse les en-têtes dans les paquets IP, TCP et UDP.

    > **Remarque :**
    >
    > les paquets IPv6 ne supportent pas la compression d'en-tête.

- LAN vers WAN

  Général

- **Profondeur de dépôt (octets)** : seuil de profondeur de file d'attente au-delà duquel les paquets sont supprimés.
- **Limite de suppression : délai**après lequel les paquets en attente dans le planificateur de classes sont supprimés. Ne s'applique pas à une classe en vrac.
- **Taille de paquets volumineux** : Les paquets inférieurs ou égaux à cette taille se voient attribuer les valeurs de limite de dépôt et de profondeur de dépôt spécifiées dans les champs **Profondeur de chute des grands paquets (octets)** et **Limite de chute des grands paquets (ms)** . Les paquets supérieurs à cette taille se voient attribuer les valeurs spécifiées dans les champs Drop Limit et Drop Depth par défaut.
- **Activer RED** : Random Early Detection (RED) garantit un partage équitable des ressources de classe en rejetant les paquets en cas de congestion.
- **Profondeur de désactivation des paquets dupliqués (octets)** : profondeur de file d'attente du planificateur de classes à laquelle les paquets dupliqués ne sont pas générés.
- **Limite de désactivation des paquets dupliqués** : durée pendant laquelle la duplication peut être désactivée pour empêcher les doublons de consommer de la bande passante.
- **Profondeur de dépôt des paquets importants (octets)** : si la profondeur de la file d'attente dépasse ce seuil, les paquets sont supprimés et les statistiques sont comptabilisées.
- **Limite de perte de paquets importants (ms)** : durée maximale estimée pendant laquelle les paquets supérieurs ou égaux à la taille des grands paquets doivent attendre dans le planificateur de classes. Si le temps estimé dépasse ce seuil, les paquets sont supprimés et les statistiques sont comptabilisées. Non valide pour les cours groupés.

Réaffecter

- **Priorité** : Vous pouvez définir la priorité de la liaison WAN de secours selon vos besoins. La priorité de la liaison WAN de secours indique l'ordre dans lequel une liaison WAN de secours devient active. Une liaison WAN de secours de haute priorité devient active en premier. Une liaison WAN de faible priorité devient active en dernier.
- **Type de transfert** : Sélectionnez un type de transfert auquel associer cette règle.
- **Profondeur de désactivation des paquets dupliqués (octets)** : profondeur de file d'attente du planificateur de classes à laquelle les paquets dupliqués ne sont pas générés.
- **Limite de désactivation des paquets dupliqués** : indique la durée pendant laquelle un paquet attend dans la file d'attente avant que la duplication ne soit effectuée, ce qui empêche les paquets dupliqués de consommer de la bande passante lorsque la bande passante est limitée.
- **Profondeur de dépôt des paquets importants (octets)** : si la profondeur de la file d'attente dépasse ce seuil, les paquets sont supprimés et les statistiques sont comptabilisées.
- **Limite de perte de paquets volumineux (ms)** : si le temps estimé dépasse ce seuil, les paquets sont supprimés et les statistiques sont comptabilisées. Non valide pour les cours groupés.
- **Profondeur de chute normale des paquets (octets)** : si la profondeur de la file d'attente

dépasse ce seuil, les paquets sont supprimés et les statistiques sont comptabilisées.
  - **Limite normale de perte de paquets (ms)** : si le temps estimé dépasse ce seuil, les paquets sont supprimés et les statistiques sont comptabilisées. Non valide pour les cours groupés.

- WAN vers LAN
  - Balise**DSCP : étiquette**DSCP appliquée aux paquets qui répondent à cette règle sur le réseau WAN vers le réseau local, avant de les envoyer au réseau local.
  - **Activer le reséquençage des paquets** : Les flux de trafic qui correspondent à la règle sont balisés pour l'ordre des séquences, et les paquets sont réorganisés (si nécessaire) au niveau de l'appliance WAN vers LAN.
  - **Hold Time** : Intervalle de temps pendant lequel les paquets sont conservés pour le reséquencement, après quoi les paquets sont envoyés au réseau local. Lorsque le temporisateur expire, les paquets sont envoyés au réseau local sans attendre plus longtemps les numéros de séquence prédéfinis.

    Si la règle a une politique de trafic en tant que chemin dupliqué, le temps de maintien par défaut est de 80 ms. Sinon, la valeur par défaut est de 900 ms pour les règles TCP et de 250 ms pour les règles non TCP.
  - **Supprimer les paquets de reséquençage en retard** : élimine les paquets hors ordre arrivés après l'envoi des paquets nécessaires au reséquençage au réseau local.

Cliquez sur **Enregistrer** pour enregistrer les paramètres de configuration. Cliquez sur **Vérifier la configuration** sur la page **Configuration** > **Politiques de QoS** pour valider toute erreur d'audit.

Vérifier les règles IP

Pour vérifier les règles IP, accédez à **Rapports > Temps réel > Flux**. Sélectionnez le site pour lequel vous souhaitez consulter les informations sur les flux et le nombre de flux à afficher. Cliquez sur **Personnaliser les colonnes** et cochez les cases correspondant aux informations de flux que vous souhaitez afficher. Vérifiez si les informations de flux sont conformes aux règles configurées.

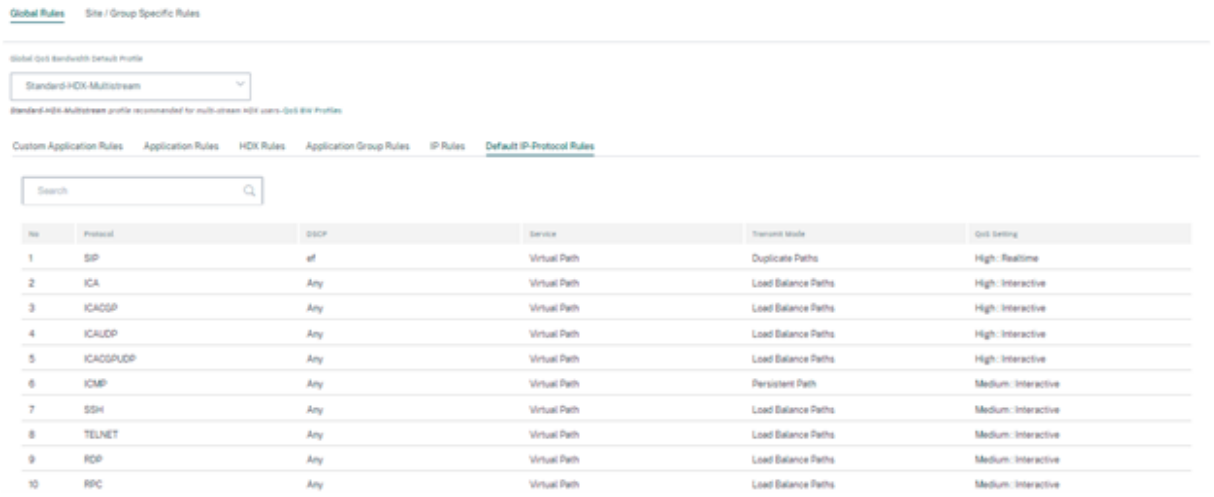
Accédez à **Rapports > Temps réel > Statistiques** et sélectionnez **Règles**. Choisissez le site et cliquez sur **Récupérer les dernières données**. Vérifiez les règles configurées. Pour plus d'informations, consultez la section Rapports du site.

Stratégies QoS

October 21, 2022

Un administrateur peut définir des stratégies d'application et de trafic. Ces stratégies aident à activer les fonctions de pilotage du trafic, de qualité de service (QoS) et de filtrage pour les applications. Indiquez si une règle définie peut être appliquée globalement sur tous les sites du réseau ou sur certains sites spécifiques.

Les stratégies sont définies sous la forme de plusieurs règles qui sont appliquées dans l'ordre défini par l'utilisateur.



Créer une nouvelle règle

Un administrateur doit placer la règle définie en fonction de la priorité. Les priorités sont classées en fonction de paramètres tels que le haut de la liste, le bas de la liste ou une ligne spécifique.

Il est recommandé d'avoir **des règles plus spécifiques** pour les applications ou les sous-applications en haut, suivies de règles **moins spécifiques** pour celles représentant un trafic plus large.

Par exemple, vous pouvez créer des règles spécifiques pour Facebook Messenger (sous-application) et Facebook (application). Placez une règle Facebook Messenger au-dessus de la règle Facebook afin que la règle Facebook Messenger soit sélectionnée. Si l'ordre est inversé, Facebook Messenger étant une sous-application de l'application Facebook, la règle de Facebook Messenger ne sera pas sélectionnée. Il est important d'obtenir la bonne commande.

Critères de

Sélectionnez le trafic pour une règle définie, telle que :

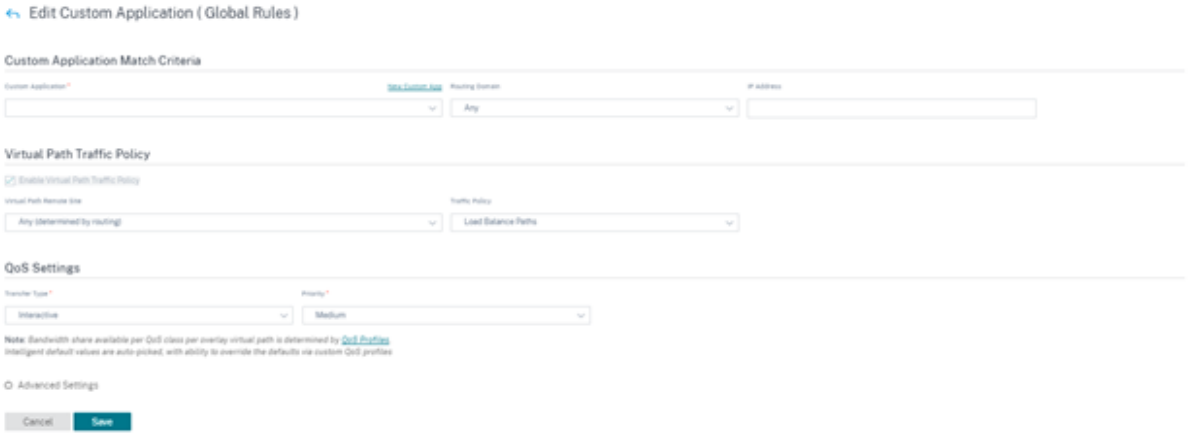
- Une demande
- Application définie sur mesure
- Groupe d'applications ou règle basée sur le protocole IP

Portée de règle

Indiquez si une règle définie peut être appliquée globalement sur tous les sites du réseau ou sur certains sites spécifiques.

Direction de l'application

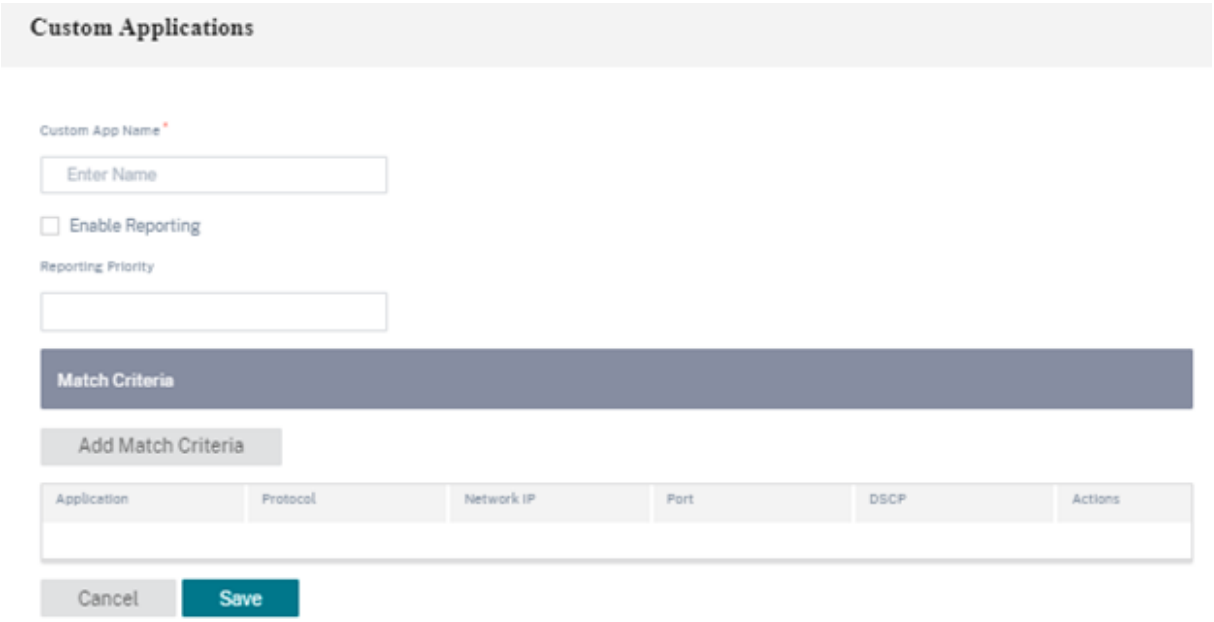
Accédez à **Configuration** > **QoS** > **Règles d'application personnalisées**. Spécifiez comment le trafic doit être dirigé.



Nouvelle application personnalisée : sélectionnez un critère de correspondance dans la liste. L'administrateur peut ajouter une nouvelle application personnalisée en donnant un nom à :

- Application personnalisée
- Protocole (TCP, UDP, ICMP)
- IP réseau/préfixe
- Port
- Balise DSCP

Vous pouvez également créer une application personnalisée basée sur un nom de domaine.

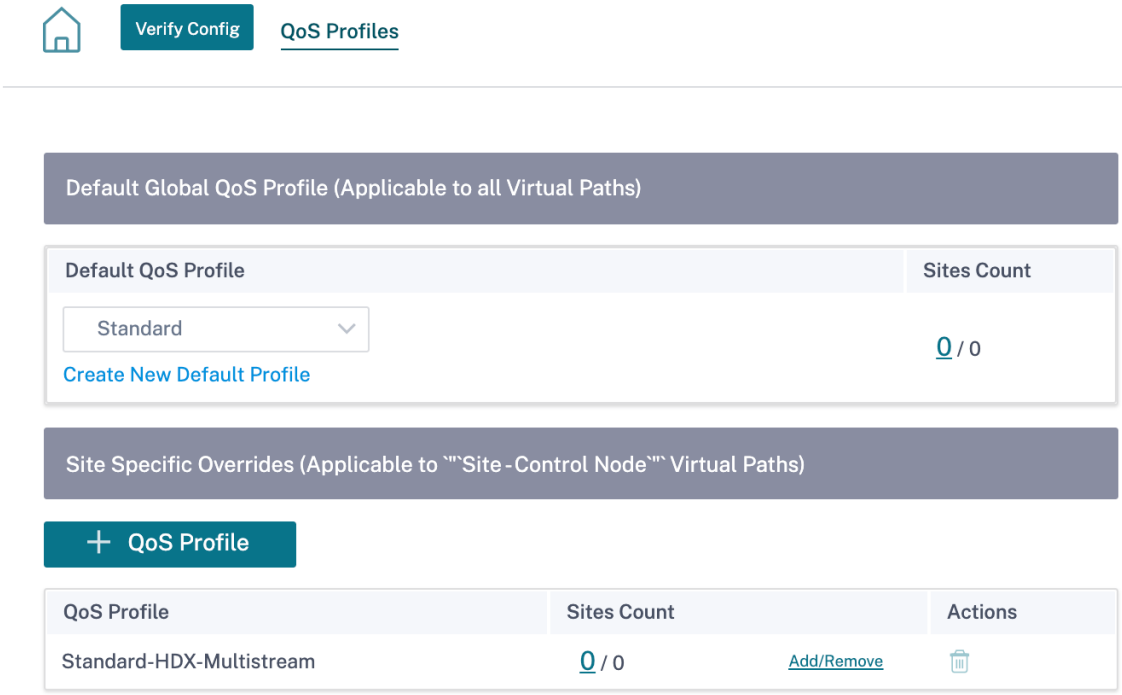


Cliquez sur **Vérifier la configuration** sur la page **Configuration** > **Politiques de QoS** pour valider toute erreur d'audit.

Règles IP **Les règles IP** vous aident à créer des règles pour votre réseau et à prendre certaines décisions en matière de qualité de service (QoS) en fonction de ces règles. Pour plus d'informations sur les règles IP, consultez la section Règles IP.

Profils QoS

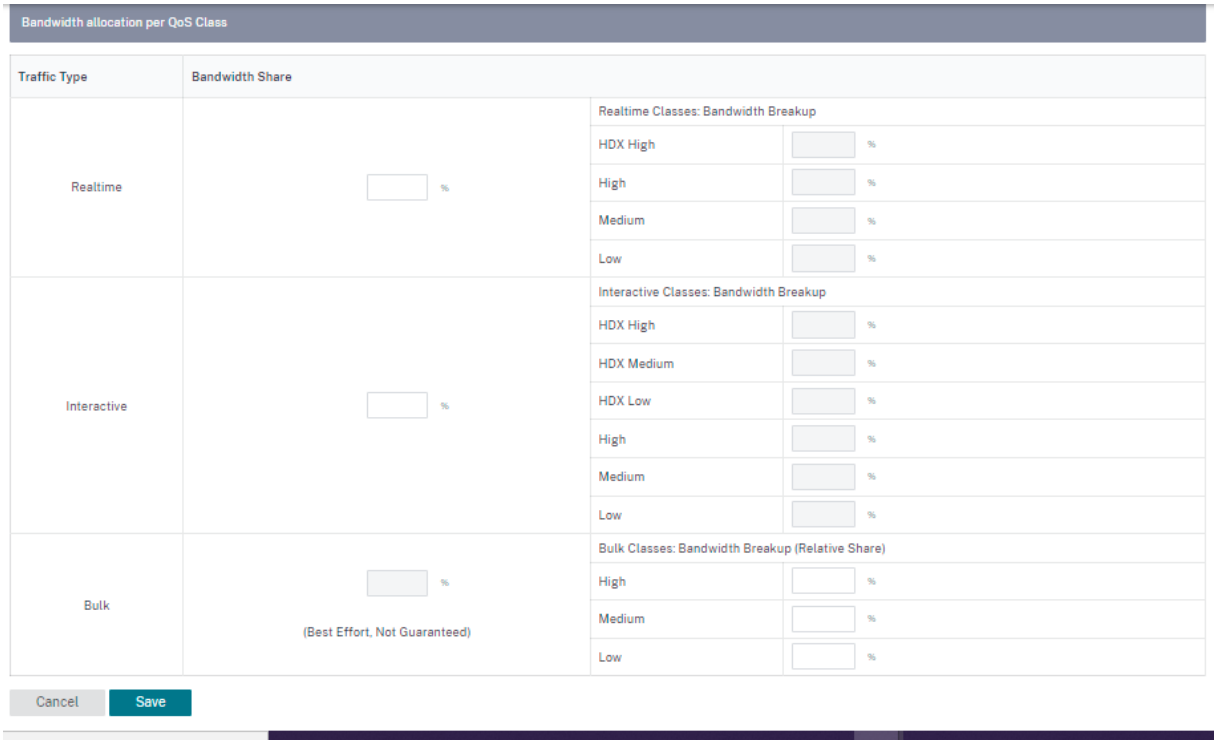
La section Qualité de service (QoS) permet de créer le profil QoS à l'aide de l'option **+ Profil QoS** . Le profil QoS fournit un service amélioré à certains trafic. L'objectif de la QoS est de fournir la priorité, y compris le type de trafic (classes en temps réel, interactif et groupé) et la bande passante dédiée. Les ruptures de bande passante sont disponibles en%. Cela a également amélioré les caractéristiques de perte.



Cliquez sur **Vérifier la configuration** sur la page **Configuration** > **Politiques de QoS** pour valider toute erreur d'audit.

Personnalisation des profils de QoS

Si les paramètres par défaut du chemin virtuel sont utilisés, les classes peuvent être modifiées sous **Configuration** > **QoS** > **Profils QoS**. Cliquez sur **Créer un nouveau profil par défaut**, entrez un nom pour l'ensemble par défaut, sélectionnez les sites et mettez à jour l'allocation de bande passante pour la classe QoS. Cliquez sur **Enregistrer**. Pour plus d'informations sur les classes, voir Classes.

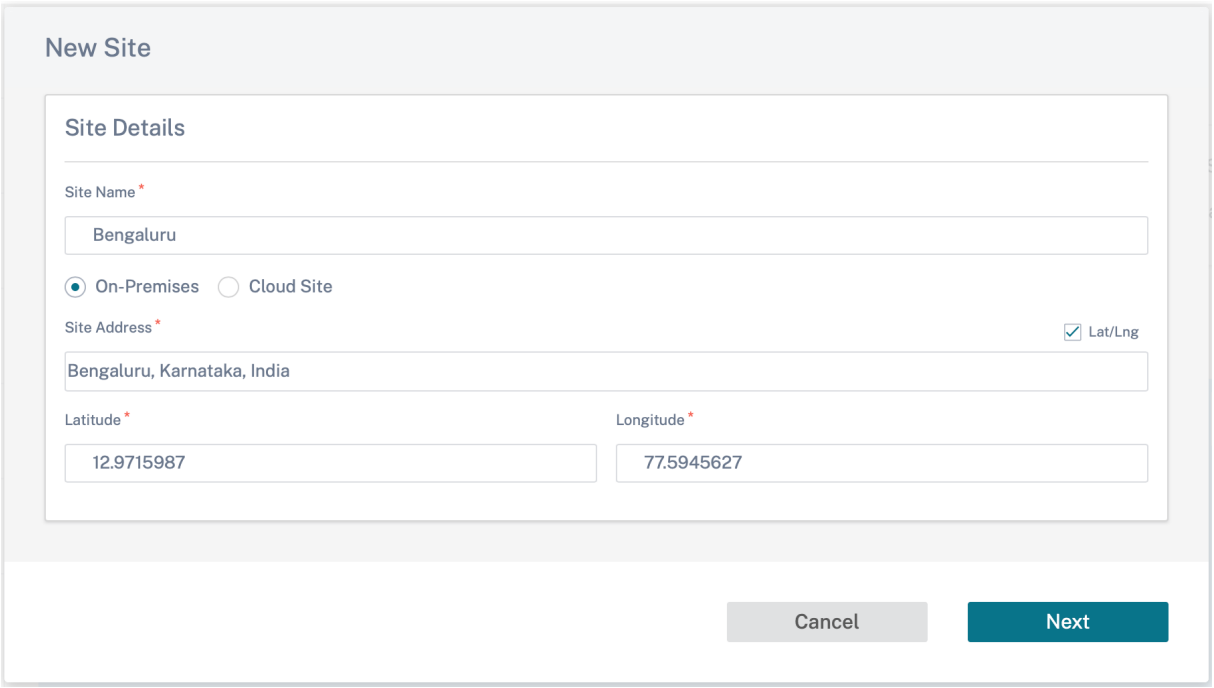


Configuration du site

October 21, 2022

Vous pouvez ajouter de nouveaux sites depuis la page d'**accueil du réseau** ou depuis la section **Profils et modèles** pour configurer votre réseau SD-WAN.

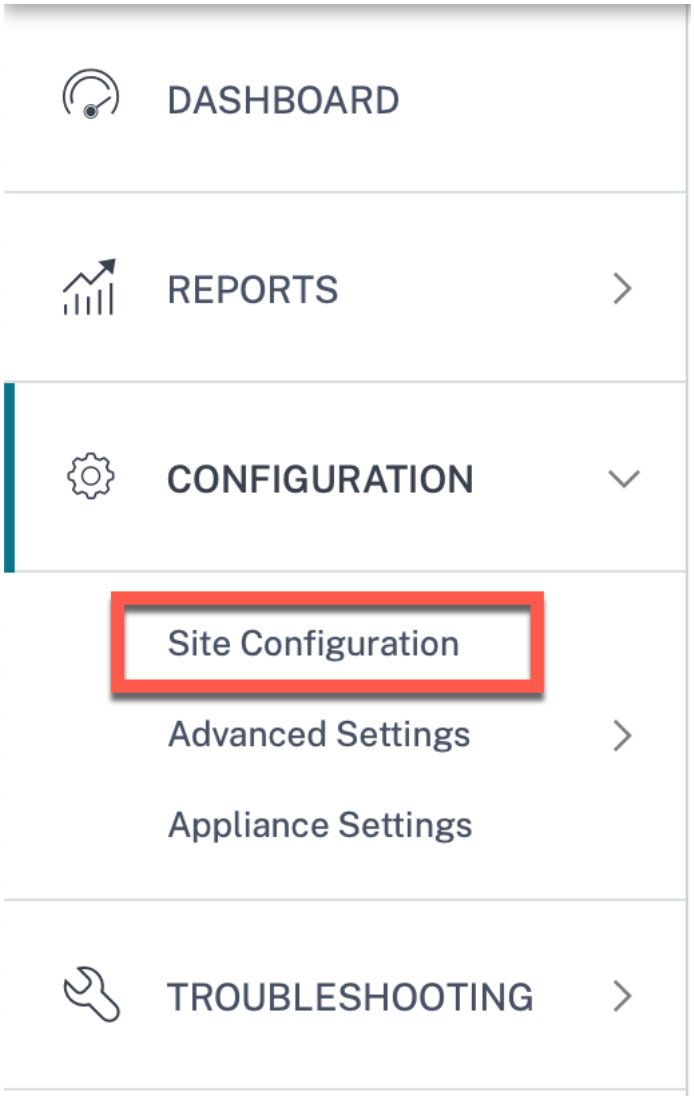
Pour créer un site, cliquez sur **+ Nouveau site** dans le tableau de bord du réseau. Indiquez un nom et un emplacement pour le site.



Vous pouvez créer un site à partir de zéro ou utiliser un profil de site pour configurer rapidement un site.

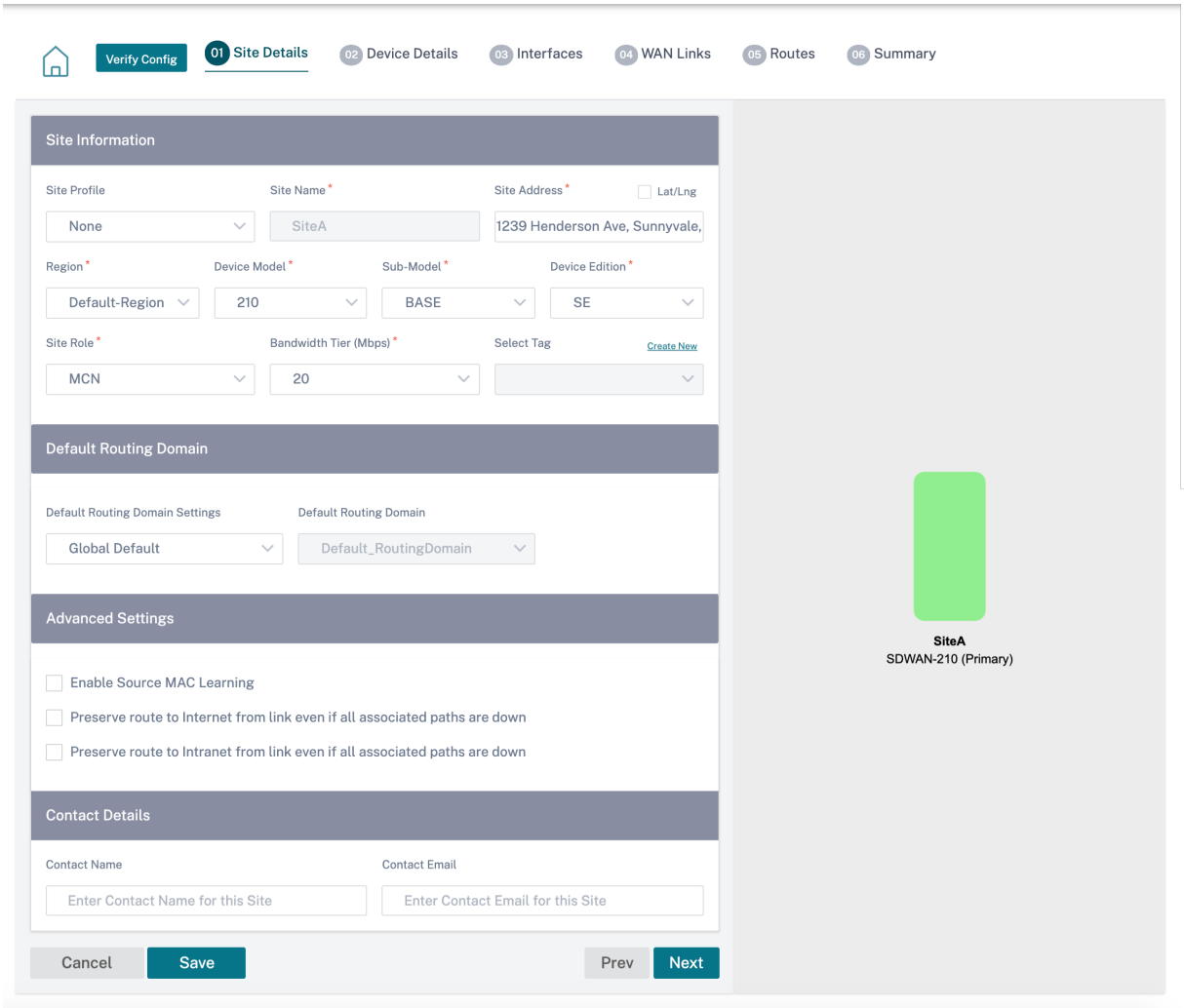
Un affichage graphique à droite de l'écran fournit un diagramme de topologie dynamique au fur et à mesure de la configuration.

Pour afficher la configuration du site, sélectionnez le site et accédez à **Configuration > Configuration du site**.

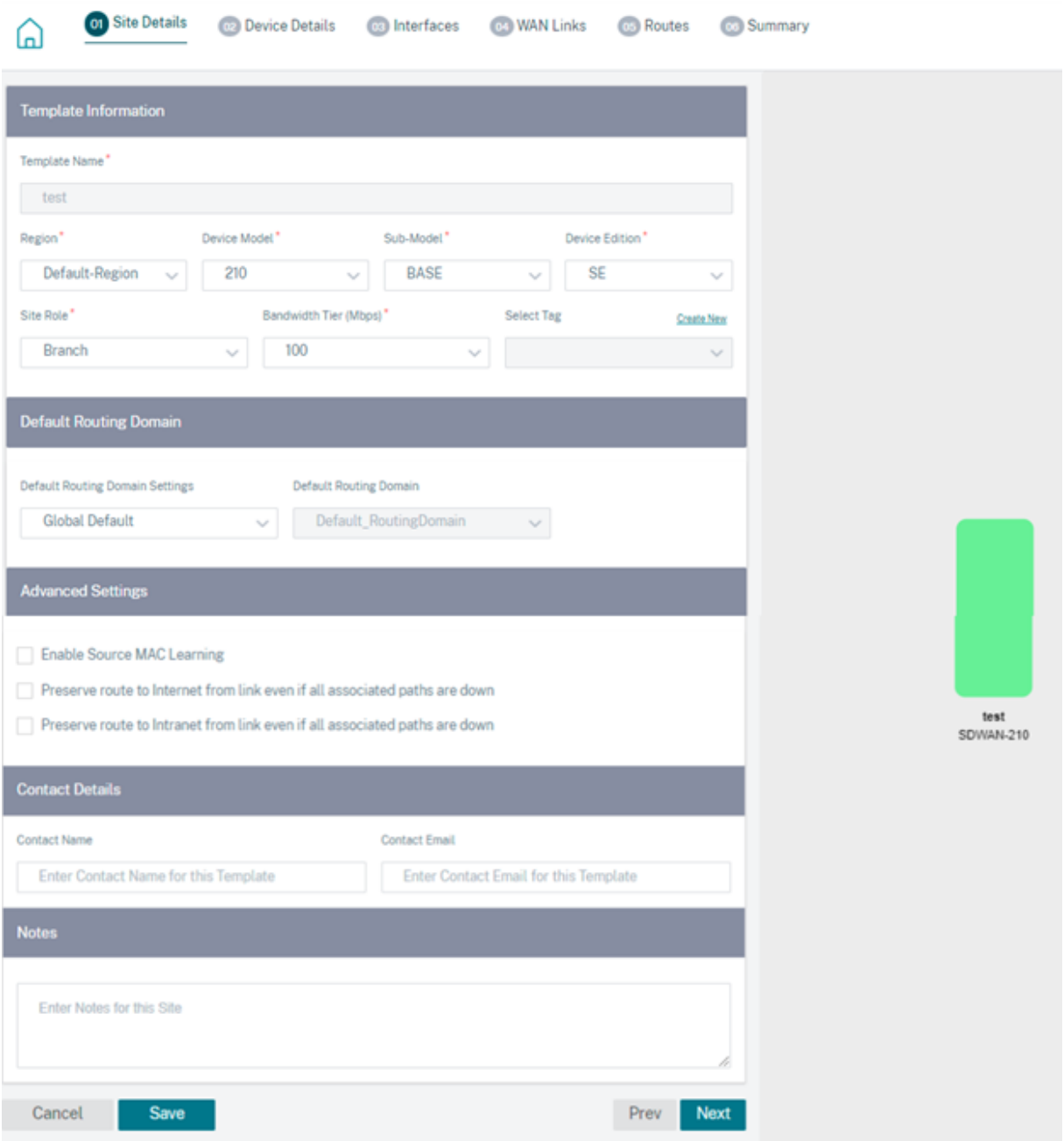


Détails du site

La première étape consiste à entrer le site, l'appareil, les paramètres avancés et les coordonnées du site.



Lorsque vous configurez des sites à l'aide d'un modèle de site, l'écran suivant s'affiche.



Informations sur le site/le modèle

- Le choix d'un **profil de site** renseigne automatiquement les paramètres du site, de l'interface et des liens WAN en fonction de la configuration du profil de site.
- **L'adresse** et **le nom du site** sont renseignés automatiquement en fonction des informations fournies à l'étape précédente.
- Cochez la case **Lat/Lng** pour obtenir la latitude et la longitude d'un site.

- Sélectionnez la **région** dans la liste déroulante.
- **Le modèle et le**sous-modèle**de l'appareil** peuvent être sélectionnés en fonction du modèle matériel ou de l'appliance virtuelle utilisé sur un site donné.
- **L'édition de l'appareil** se reflète automatiquement en fonction du modèle d'appareil sélectionné. Actuellement, l'édition Premium (PE), l'édition avancée (AE) et l'édition standard (SE) sont prises en charge. Le modèle PE est uniquement pris en charge sur les plateformes 1100, 2100, 5100 et 6100. Le modèle AE est pris en charge sur les plateformes 210 et 1100.

  > **Remarque**
  >
  > Le service Citrix SD-WAN Orchestrator ne prend pas en charge les plateformes Advanced Edition et Premium Edition.

- **Le rôle du site** définit le rôle de l'appareil. Vous pouvez attribuer l'un des rôles suivants à un site :
  - **MCN** : le nœud de contrôle principal (MCN) sert de contrôleur du réseau, et seul un périphérique actif d'un réseau peut être désigné comme MCN.
  - **Succursale** : Appliances installées sur les sites des succursales qui reçoivent la configuration du MCN et participent à la mise en place de fonctionnalités WAN virtuelles pour les succursales. Il peut y avoir plusieurs sites de succursales.
  - **RCN** : le nœud de contrôle régional (RCN) prend en charge l'architecture réseau hiérarchique, permettant ainsi le déploiement de réseaux multirégionaux. MCN contrôle plusieurs RCN et chaque RCN, à son tour, contrôle plusieurs sites de succursales.
  - **MCN géo-redondant** : site situé à un autre emplacement, qui prend en charge les fonctions de gestion du MCN, s'il n'est pas disponible, garantissant ainsi la reprise après sinistre. Le MCN géo-redondant ne fournit pas de fonctionnalités de haute disponibilité ou de basculement pour le MCN.
  - **RCN géo-redondant** : site situé à un autre endroit, qui prend en charge les fonctions de gestion du RCN, s'il n'est pas disponible, garantissant ainsi la reprise après sinistre. Le RCN géo-redondant ne fournit pas de fonctionnalités de haute disponibilité ou de basculement pour le RCN.
- Le**niveau de bande passante** est la capacité de bande passante facturable que vous pouvez configurer sur n'importe quel appareil, en fonction du modèle de l'appareil. Par exemple, l'appliance SD-WAN 410 Standard Edition (SE) prend en charge les niveaux de bande passante de 20, 50, 100, 150 et 200 Mbit/s. En fonction de vos besoins en bande passante pour un site donné, vous pouvez sélectionner le niveau souhaité. Chaque site est facturé pour le niveau de bande passante configuré.

Domaine de routage

La section **Domaine de routage** vous permet de sélectionner le domaine de routage par défaut pour le site. Les paramètres du**domaine de routage** peuvent être globaux ou spécifiques au site. Si vous sélectionnez **Global Defaults**, le domaine de routage par défaut applicable à l'échelle mondiale est automatiquement sélectionné. Si vous sélectionnez **Spécifique au site**, vous pouvez sélectionner le domaine de routage par défaut dans la liste déroulante **Domaine de routage** .

Prise en charge du routage pour la segmentation LAN

Les appliances SD-WAN Standard et Enterprise Edition (SE/PE) implémentent la segmentation du réseau local sur des sites distincts sur lesquels l'une ou l'autre appliance est déployée. Les appliances reconnaissent et conservent un enregistrement des VLAN côté LAN disponibles, et configurent des règles concernant les autres segments de réseau local (VLAN) auxquels les autres segments de réseau local (VLAN) peuvent se connecter sur un site distant avec une autre appliance SD-WAN SE/PE.

La fonctionnalité ci-dessus est mise en œuvre à l'aide d'une table de routage et de transfert virtuels (VRF) gérée dans l'appliance SD-WAN SE/PE, qui assure le suivi des plages d'adresses IP distantes accessibles à un segment de réseau local. Ce trafic VLAN vers VLAN traverserait toujours le WAN via le même chemin virtuel préétabli entre les deux appliances (aucun nouveau chemin n'a besoin d'être créé).

Un exemple d'utilisation de cette fonctionnalité est qu'un administrateur WAN peut segmenter l'environnement réseau des succursales locales via un VLAN et fournir à certains de ces segments (VLAN) un accès à des segments de réseau local côté DC ayant accès à Internet, tandis que d'autres peuvent ne pas obtenir un tel accès. La configuration des associations VLAN-VLAN est réalisée via l'interface Web du service Citrix SD-WAN Orchestrator.

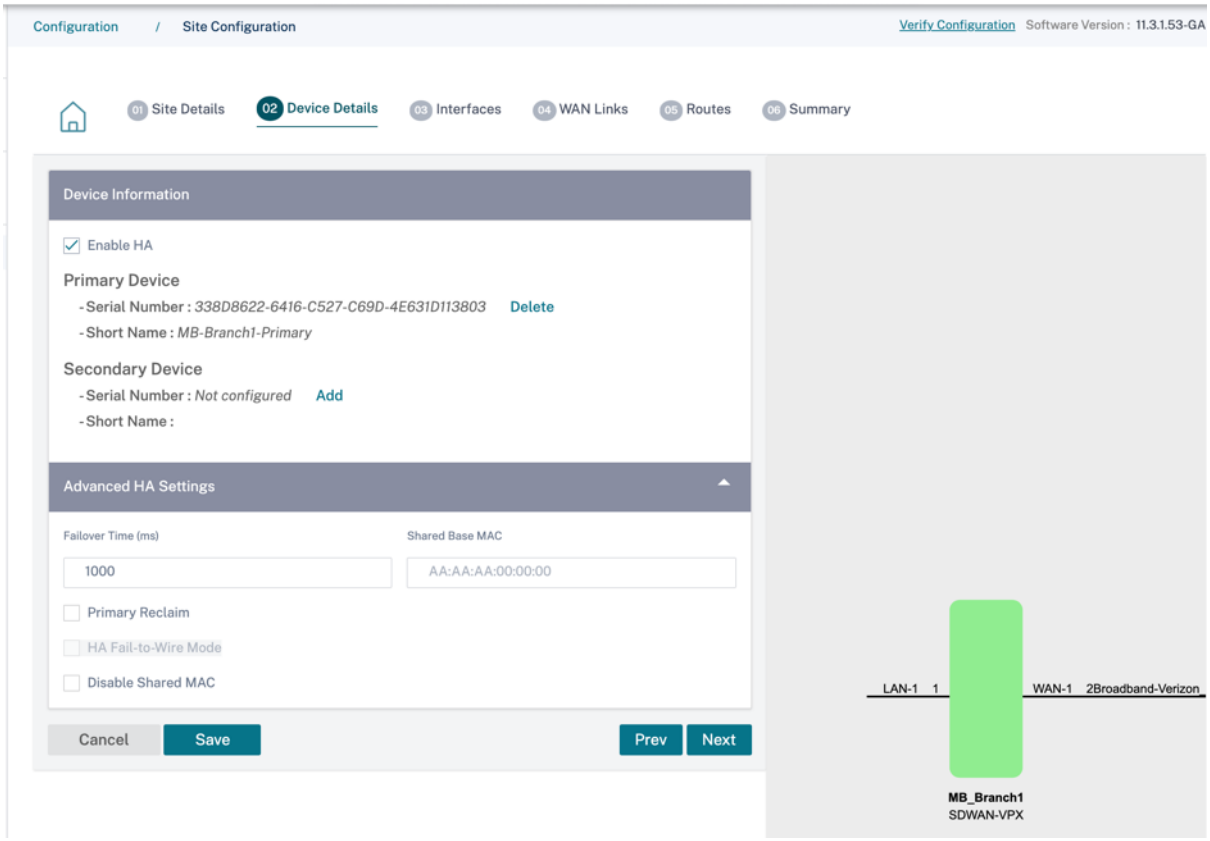
Paramètres avancés

- **Activer l'apprentissage du MAC source** : enregistre l'adresse MAC source des paquets reçus afin que les paquets sortants vers la même destination puissent être envoyés vers le même port.
- **Préserver l'itinéraire vers Internet à partir du lien même si tous les chemins associés sont inactifs** : lorsque cette option est activée, les paquets destinés au service Internet continuent de choisir le service Internet même si toutes les liaisons WAN du service Internet ne sont pas disponibles.
- **Préserver la route vers l'intranet à partir du lien même si tous les chemins associés sont inactifs** : lorsque cette option est activée, les paquets destinés au service intranet continuent de choisir le service intranet même si tous les liens WAN du service intranet ne sont pas disponibles.
- Coordonnées de l'administrateur disponible sur le site.

Un diagramme de réseau dynamique à droite du panneau de configuration fournit une rétroaction visuelle continue, au fur et à mesure que vous passez par le processus de configuration.

Détails de l'appareil

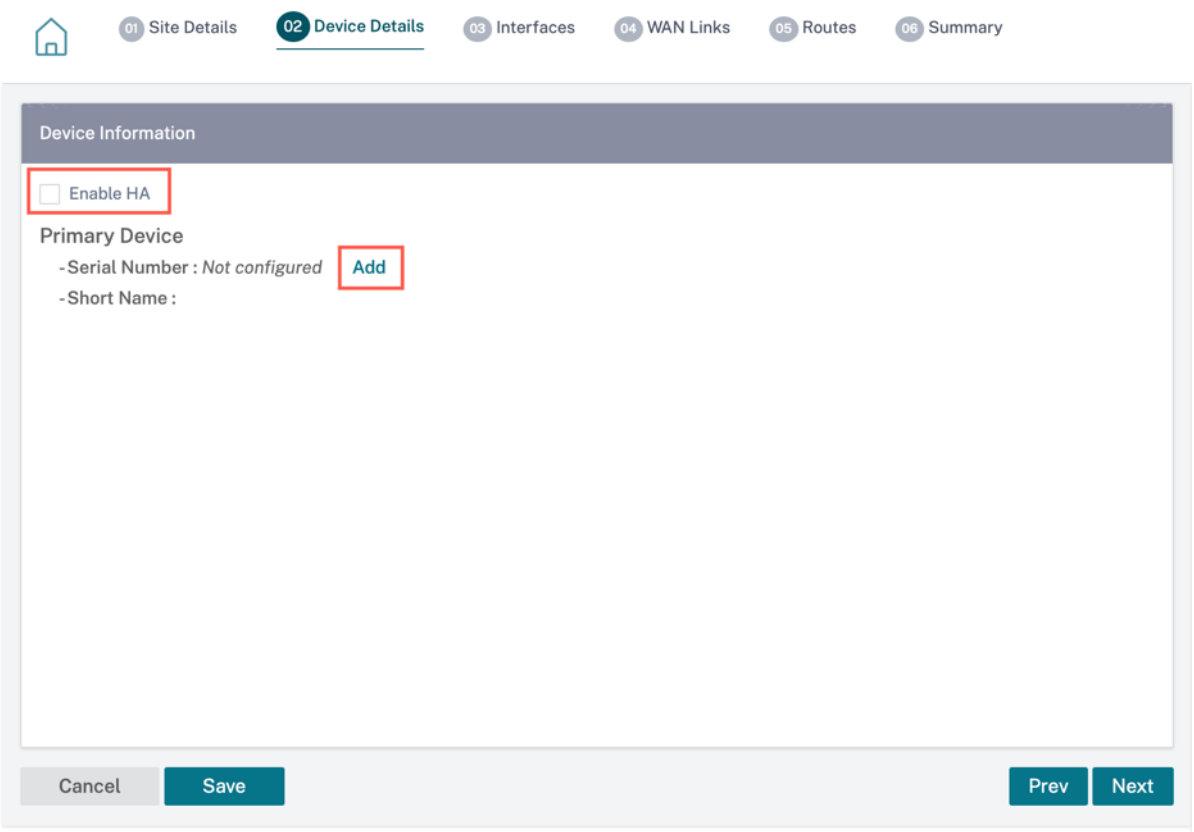
La section Détails de l'appareil vous permet de configurer et d'activer la haute disponibilité (HA) sur un site. Avec HA, deux appliances peuvent être déployées sur un site en tant que principal actif et secondaire passif. L'appliance secondaire prend le relais en cas de défaillance du principal. Pour plus d'informations, consultez la section Haute disponibilité.



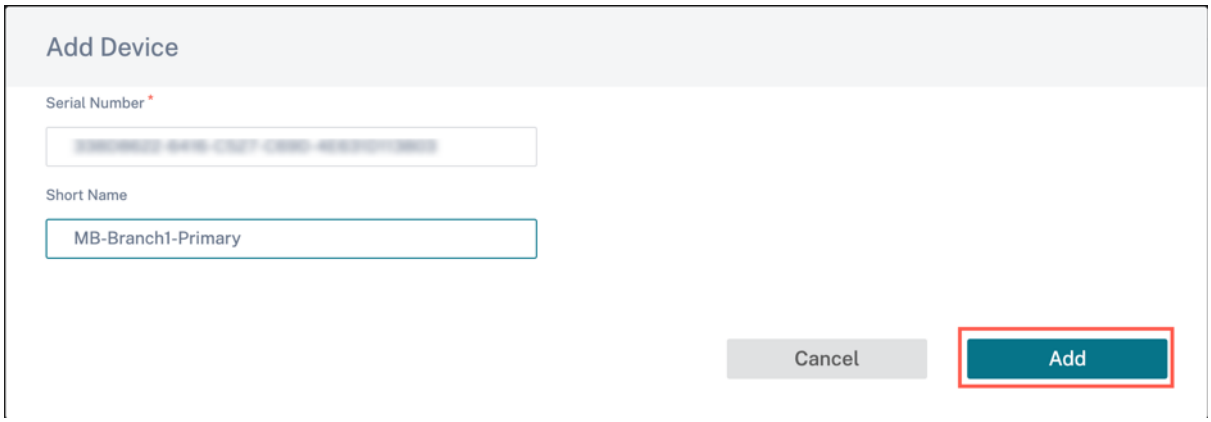
> **Remarque**
>
> Les numéros de série ne sont pas configurables à l'aide des modèles de sites

Informations sur l'appareil

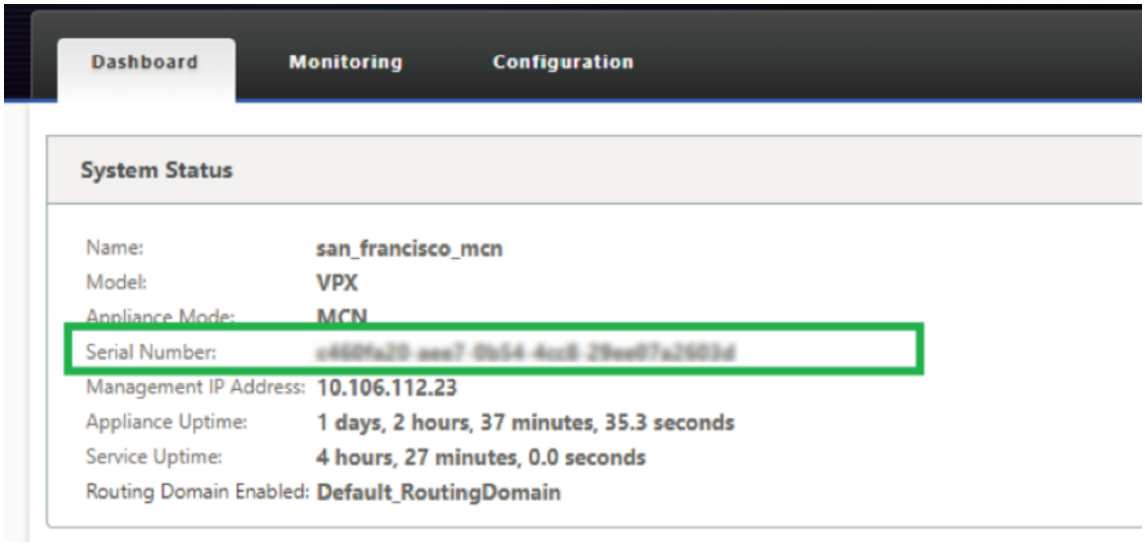
Activez HA et entrez le numéro de série et un nom abrégé pour les appliances principales et secondaires. Cliquez sur **Ajouter** et saisissez le numéro de série ainsi que le nom abrégé du site.



Cliquez sur **Ajouter**.



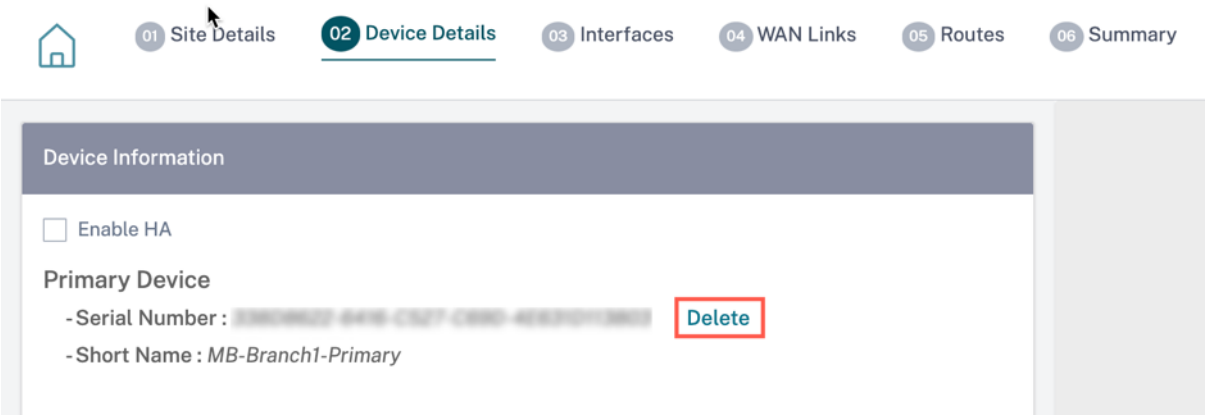
- **Numéro de série** : Le **numéro** de série d'une instance SD-WAN virtuelle (VPX) est accessible depuis la console Web VPX, comme indiqué dans la capture d'écran suivante. Un numéro de série d'une appliance matérielle se trouve également sur l'étiquette du périphérique.



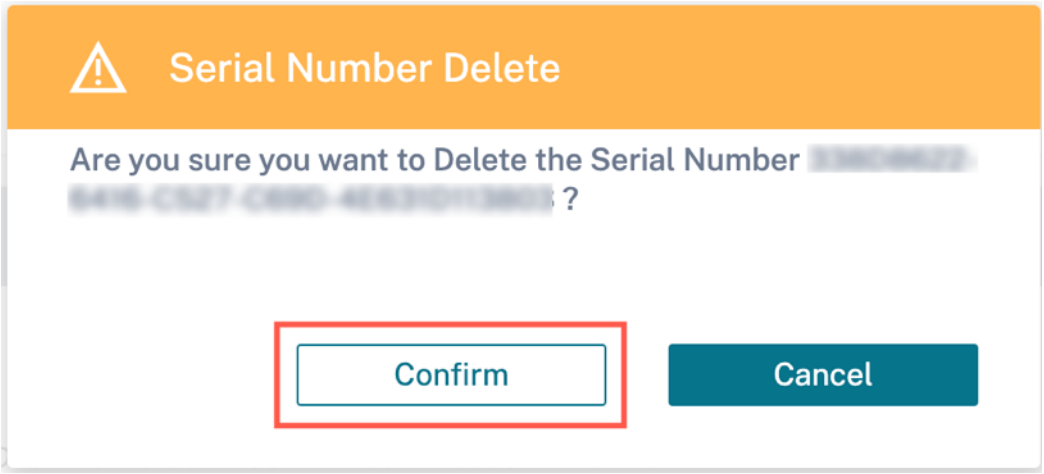
- **Nom abrégé** : Le champ **Nom abrégé** est utilisé pour spécifier un nom court facilement identifiable pour un site ou pour baliser un site si vous le souhaitez.

Cliquez sur l'option **Supprimer** si vous souhaitez supprimer le numéro de série.

> **Remarque**
> La mise à jour du numéro de série nécessite la suppression du numéro de série existant et la lecture d'un nouveau numéro.



Lorsque vous cliquez sur l'option **Supprimer**, une fenêtre contextuelle apparaît pour confirmer si vous souhaitez supprimer le numéro de série ou non.



Paramètres haute disponibilité avancés

- **Temps de basculement (ms)** : temps d'attente après la perte du contact avec l'appliance principale, avant que l'appliance de secours ne devienne active.
- **MAC de base partagé** : adresse MAC partagée pour les deux appliances à haute disponibilité. Lorsqu'un basculement se produit, le matériel secondaire possède les mêmes adresses MAC virtuelles que le matériel principal défaillant.
- **Désactiver Shared Base MAC** : Cette option n'est disponible que sur les hyperviseurs et les plateformes basées sur le cloud. Choisissez cette option pour désactiver l'adresse MAC virtuelle partagée.
- **Reprise principale** : L'appliance principale désignée reprend le contrôle lors du redémarrage après un événement de basculement.
- Mode**HA Fail-to-Wire : Le mode**HA Fail-to-Wire est activé. Pour plus de détails, consultez la section Modes de déploiement HA.
- **Activer la prise en charge du câble Y** : Les ports SFP (Small Form-Factor Pluggable) peuvent être utilisés avec un câble Y à fibre optique pour activer la fonctionnalité de haute disponibilité pour le déploiement en mode Edge. Cette option est disponible uniquement sur les appliances Citrix SD-WAN 1100 SE/PE. Pour plus d'informations, consultez Activer la haute disponibilité en mode Edge à l'aide d'un câble Y à fibre optique.

Informations sur le Wi-Fi

Vous pouvez configurer une appliance Citrix SD-WAN qui prend en charge le Wi-Fi en tant que point d'accès Wi-Fi.

Les deux variantes suivantes de la plate-forme Citrix SD-WAN 110 prennent en charge le Wi-Fi et peuvent être configurées en tant que point d'accès Wi-Fi :

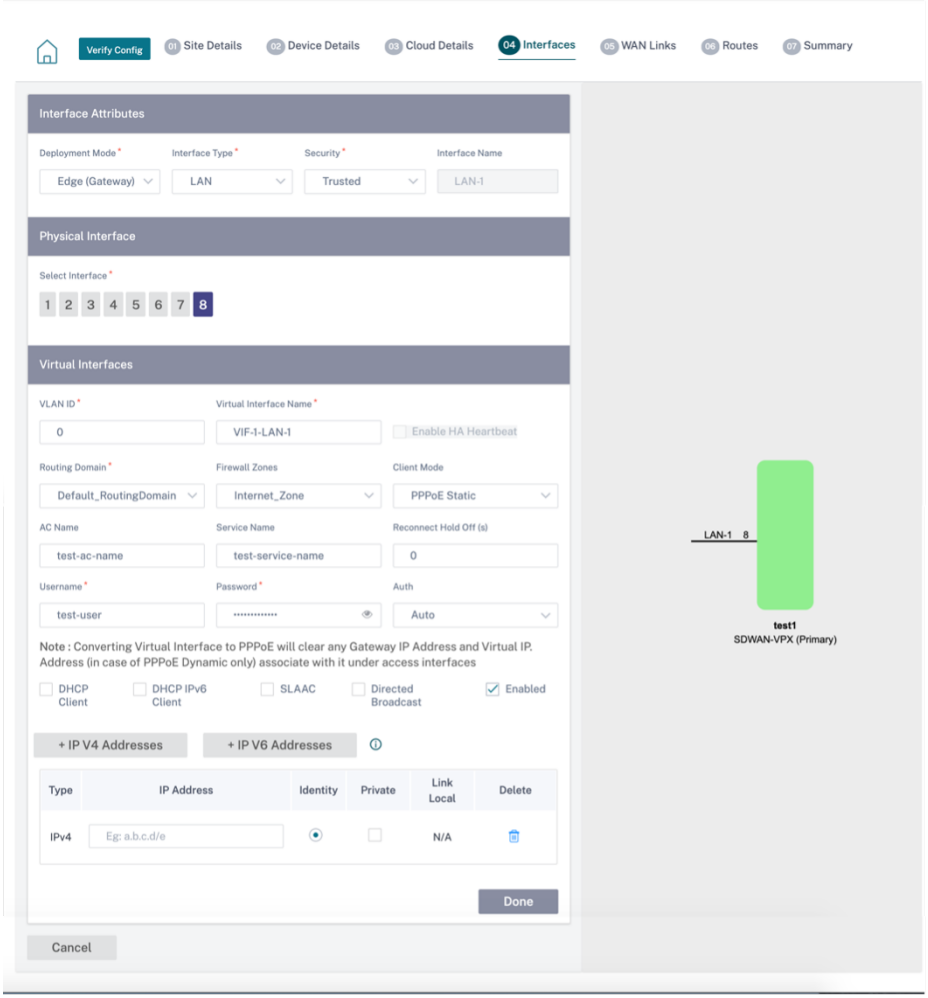
- Citrix SD-WAN 110-WiFi-SE
- Citrix SD-WAN 110-LTE-WiFi

Pour plus de détails sur la configuration Wi-Fi, voir Point d'accès Wi-Fi

Interfaces

L'étape suivante consiste à ajouter et configurer les interfaces. Cliquez sur **+ Interface** pour commencer à configurer l'interface. Cliquez sur **+ Interface HA** pour commencer à configurer l'interface HA. L'option **+ HA Interface** n'est disponible que si vous avez configuré un dispositif secondaire pour une haute disponibilité.

La configuration de l'interface implique la sélection du mode de déploiement et la définition des attributs de niveau d'interface. Cette configuration est applicable aux liaisons LAN et WAN.



Gestion intrabande

La gestion in-band vous permet d'utiliser les ports de données SD-WAN pour la gestion. Il transporte à la fois les données et le trafic de gestion, sans avoir à configurer un chemin de gestion supplémentaire. La gestion in-band permet aux adresses IP virtuelles de se connecter à des services de gestion tels que l'interface utilisateur Web et SSH. Vous pouvez accéder à l'interface utilisateur Web et SSH à l'aide de l'adresse IP de gestion et des adresses IP virtuelles in-band.

Pour activer la gestion intrabande, choisissez une adresse IPv4 dans la liste déroulante **IP de gestion intrabande** ou une adresse IPv6 dans la liste déroulante **IPv6 de gestion intrabande** . Sélectionnez le **proxy DNS** vers lequel toutes les requêtes DNS sur le plan de gestion intrabande et de sauvegarde sont transférées **dans la liste déroulante InBand Management DNS** ou **InBand Management DNS V6** .

Pour plus d'informations sur la gestion intrabande, voir Gestion intrabande.

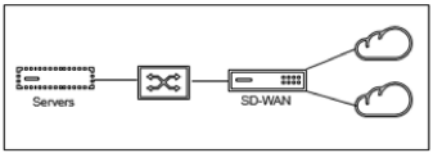
Les adresses IP configurées pour les interfaces sont répertoriées dans la liste déroulante **InBand Management IP** . Les services proxy DNS configurés sous **Paramètres avancés > DNS** sont répertoriés dans la liste déroulante **InBand Management DNS** .

Attributs interface

Les modes de déploiement suivants sont pris en charge :

1. Edge (passerelle)
2. Inline —Fail-to-Wire, Fail-to-Block et Virtual Inline.

- **Mode de déploiement** : sélectionnez l'un des modes de déploiement suivants.
  - **Edge (passerelle)** :

    Le mode passerelle implique que le SD-WAN sert de « passerelle » vers le WAN pour tout le trafic LAN. Le **mode Gateway** est le mode par défaut. Vous pouvez déployer l'appliance en tant que Gateway côté LAN ou WAN.
  - **En ligne** :

    Lorsque le SD-WAN est déployé en ligne entre un commutateur LAN et un routeur WAN, le SD-WAN est censé « relier » le LAN et le WAN.

    Toutes les appliances Citrix SD-WAN disposent d'interfaces appariées par pont prédéfinies. Lorsque l'option Bridge est activée, la sélection de n'importe quelle interface du côté

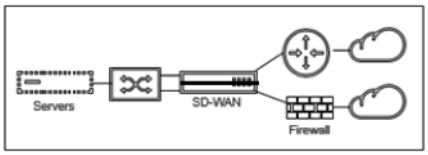
LAN met automatiquement en évidence l'interface jumelée réservée à l'extrémité WAN du pont. Par exemple, les interfaces physiques 1 et 2 sont une paire pontée.

* **Fail-To-Wire** : permet une connexion physique entre la paire d'interfaces pontée, permettant au trafic de contourner le SD-WAN et de traverser directement le pont en cas de redémarrage ou de panne de l'appliance.

Auparavant, le client DHCP n'était pris en charge que sur le port Fail-to-Block. Avec la version 11.2.0 de Citrix SD-WAN, la capacité du client DHCP est étendue sur le port Fail-to-Wire pour le site de la succursale avec des déploiements en série à haute disponibilité (HA). Cette amélioration :

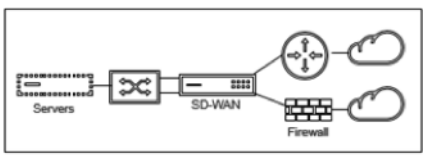
* Autorise la configuration du client DHCP sur un groupe d'interface non approuvé qui a des déploiements de paire de pont à fil et d'HA série.
* Permet de sélectionner les interfaces DHCP dans le cadre des liaisons WAN Intranet privé.

> **Remarques**
>
> * L'option Inline (Fail-to-Wire) est disponible uniquement sur les appliances matérielles et non sur les appliances virtuelles (VPX/VPXL).
> * Le client DHCP est désormais pris en charge sur le lien intranet privé.
> * Une interface LAN ne doit pas être connectée à la paire Fail-to-Wire car les paquets peuvent être pontés entre les interfaces.

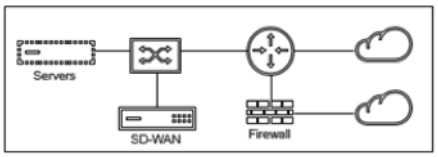


* **Fail-to-block** : cette option désactive la connexion physique entre la paire d'interfaces pontée sur les appliances matérielles, empêchant ainsi le trafic de traverser le pont en cas de redémarrage ou de panne de l'appliance.

> **Remarque**
>
> Inline (Fail-to-Block) est la seule option de mode pont disponible sur les appliances virtuelles (VPX/VPXL).



* **Virtuel en ligne (One-Arm)** :



Lorsque le SD-WAN est déployé dans ce mode, il dispose d'un **bras unique** le connectant au routeur WAN, au réseau local et au WAN partageant la même interface sur le SD-WAN. Par conséquent, les paramètres d'interface sont partagés entre les liaisons LAN et WAN.

- **Type d'interface :** sélectionnez le type d'interface dans la liste déroulante.
- **Sécurité (fiable/Non fiable)** : Spécifie le niveau de sécurité de l'interface. Les segments approuvés sont protégés par un pare-feu.
- **Nom de l'interface :** en fonction du mode de déploiement sélectionné, le champ **Nom de l'interface** est rempli automatiquement.

Interface physique

- **Sélectionnez l'interface :** sélectionnez le port Ethernet configurable disponible sur l'appliance.

Interface virtuelle

- ID du**VLAN : ID**permettant d'identifier et de marquer le trafic à destination et en provenance de l'interface.
- **Nom de l'interface virtuelle :** en fonction du mode de déploiement sélectionné, le champ **Nom de l'interface virtuelle** est rempli automatiquement.
- **Activer HA Heartbeat** : Activez la synchronisation des pulsations HA via cette interface. Cette option est activée si vous avez configuré une appliance secondaire pour HA. Sélectionnez cette option pour permettre aux appliances principales et secondaires de synchroniser les battements de cœur HA sur cette interface. Spécifiez l'adresse IP de l'appliance principale et secondaire.
- **Domaine de routage** : domaine de routage qui fournit un point d'administration unique du réseau de succursales ou d'un réseau de centre de données.
- **Zones** de pare-feu : zone de pare-feu à laquelle appartient l'interface. Les zones de pare-feu sécurisent et contrôlent les interfaces dans la zone logique.
- **Mode client :** sélectionnez **Mode client** dans la liste déroulante. Sur la sélection de PPPoE Static affiche plus de paramètres.

> **Remarque**
>
> Lorsque le mode Site (sous l'onglet Détails du site) est sélectionné comme **Branche** et que le **champ Sécurité** (sous l'onglet **Interface**) est sélectionné comme **Non fiable**, l'option **dynamique PPPoE** est disponible sous **Mode client**.

Citrix SD-WAN agit en tant que client PPPoE. Pour IPv4, le SD-WAN obtient l'adresse IPv4 dynamique ou utilise l'adresse IPv4 statique. Pour IPv6, il obtient l'adresse locale du lien auprès du serveur PPPoE. Pour l'adresse de monodiffusion IPv6, vous pouvez utiliser une adresse IP statique, DHCP ou SLAAC.

- **Client DHCP** : lorsqu'il est activé sur les interfaces virtuelles, le serveur DHCP attribue dynamiquement des adresses IPv4 au client connecté.
- **Client IPv6 DHCP** : lorsqu'il est activé sur les interfaces virtuelles, le serveur DHCP attribue dynamiquement des adresses IPv6 au client connecté.
- **SLAAC** : cette option n'est disponible que pour les adresses IPv6. Lorsque cette option est sélectionnée, l'interface obtient des adresses IPv6 via la configuration automatique des adresses sans état (SLAAC).
- **Diffusion dirigée** : lorsque la case **Diffusion dirigée** est cochée, les diffusions dirigées sont envoyées aux sous-réseaux IP virtuels de l'interface virtuelle.
- **Activé** : par défaut, la case **Activé** est cochée pour toutes les interfaces virtuelles. Si vous souhaitez désactiver l'interface virtuelle, désactivez la case à cocher **Activé** .

  > **Remarque**
  >
  > - La case à cocher **Activé** n'est disponible qu'à partir de Citrix SD-WAN version 11.3.1.
  > - L'option de désactivation d'une interface virtuelle n'est disponible que si elle n'est pas utilisée par une interface d'accès de liaison WAN. Si l'interface virtuelle est utilisée par une interface d'accès WAN, la case à cocher est en lecture seule et sélectionnée par défaut.
  > - Lors de la configuration d'autres fonctionnalités, ainsi que des interfaces virtuelles activées, les interfaces virtuelles désactivées sont également répertoriées, sauf sous **Interfaces d'accès** pour un **lien WAN**. Même si vous sélectionnez une interface virtuelle désactivée, l'interface virtuelle n'est pas prise en compte et n'a pas d'impact sur la configuration du réseau.

- **+ Adresse IPv4 : adresse**IPv4 virtuelle et masque réseau de l'interface.
- **+ Adresse IPv6 : adresse**IPv6 virtuelle et préfixe de l'interface.
- **Identité** : Choisissez une identité à utiliser pour les services IP. Par exemple, **l'identité** est utilisée comme adresse IP source pour communiquer avec les voisins BGP.

- **Privé** : lorsque cette option est activée, l'adresse IP virtuelle est uniquement routable sur l'appliance locale.

> **Remarque**
>
> - Les ports LTE ne prennent pas en charge les adresses IP statiques (IPv4 et IPv6).
> - Les ports LTE prennent en charge les protocoles DHCP et SLAAC. La configuration de DHCPv4 ou DHCPv6 est obligatoire. Le SLAAC est facultatif.
> - Dans les ports LTE, les adresses Link-Local peuvent être configurées pour IPv6 ou SLAAC.

Informations d'identification PPPoE

Le protocole PPPoE (Point-to-Point Protocol over Ethernet) connecte plusieurs utilisateurs d'ordinateurs sur un réseau local Ethernet à un site distant par l'intermédiaire d'appliances locales communes, par exemple, Citrix SD-WAN. PPPoE permet aux utilisateurs de partager une ligne d'abonné numérique (DSL), un modem câble ou une connexion sans fil commune à Internet. PPPoE combine le protocole PPP (Point-to-Point Protocol), couramment utilisé dans les connexions commutées, avec le protocole Ethernet, qui prend en charge plusieurs utilisateurs dans un réseau local. Les informations de protocole PPP sont encapsulées dans une trame Ethernet.

Les appliances Citrix SD-WAN utilisent le protocole PPPoE pour permettre aux FAI d'avoir des connexions DSL et modem câble continues et continues, contrairement aux connexions par modem câble. PPPoE fournit à chaque session de site utilisateur distant pour apprendre les adresses réseau de l'autre par le biais d'un échange initial appelé « découverte ». Une fois qu'une session est établie entre un utilisateur individuel et le site distant, par exemple un fournisseur d'accès Internet, la session peut être surveillée. Les entreprises utilisent un accès Internet partagé sur des lignes DSL à l'aide d'Ethernet et de PPPoE.

Citrix SD-WAN agit en tant que client PPPoE. Pour IPv4, le SD-WAN obtient l'adresse IPv4 dynamique ou utilise l'adresse IPv4 statique. Pour IPv6, il obtient l'adresse locale du lien auprès du serveur PPPoE. Pour l'adresse de monodiffusion IPv6, vous pouvez utiliser une adresse IP statique, DHCP ou SLAAC.

Les éléments suivants sont requis pour que les sessions PPPoE réussissent :

- Configurer l'interface réseau virtuel (VNI).
- Informations d'identification uniques pour créer une session PPPoE.
- Configurer le lien WAN. Chaque VNI ne peut avoir qu'un seul lien WAN configuré.
- Configurez l'adresse IP virtuelle. Chaque session obtient une adresse IP unique, dynamique ou statique, en fonction de la configuration fournie.
- Déployez l'appliance en mode pont pour utiliser PPPoE avec une adresse IP statique et configurez l'interface comme « fiable ». «

- Il est préférable que l'adresse IP statique ait une configuration pour forcer l'adresse IP proposée par le serveur ; si elle est différente de l'adresse IP statique configurée, une erreur peut se produire.
- Déployez l'appliance en tant que périphérique Edge pour utiliser le protocole PPPoE avec une adresse IP dynamique et configurez l'interface comme « non fiable ». «
- Les protocoles d'authentification pris en charge sont PAP, CHAP, EAP-MD5, EAP-SRP.
- Le nombre maximal de sessions multiples dépend du nombre de VNI configurés.
- Créez plusieurs VNI pour prendre en charge plusieurs sessions PPPoE par groupe d'interface.

> **Remarque**
>
> Plusieurs VNI peuvent être créés avec la même balise VLAN 802.1Q.

Limitations pour la configuration PPPoE :

- Le balisage VLAN 802.1q n'est pas pris en charge.
- L'authentification EAP-TLS n'est pas prise en charge.
- Compression d'adresse/de contrôle.
- Dégonfler la compression.
- Négociation de compression de champ de protocole
- Protocole de contrôle de compression.
- Compression BSD Compresser.
- Protocoles IPX.
- PPP Multi-Link.
- Compression d'en-tête TCP/IP de style Van Jacobson.
- Option de compression de l'ID de connexion dans la compression d'en-tête TCP/IP de style Van Jacobson.
- PPPoE n'est pas pris en charge sur les interfaces LTE.

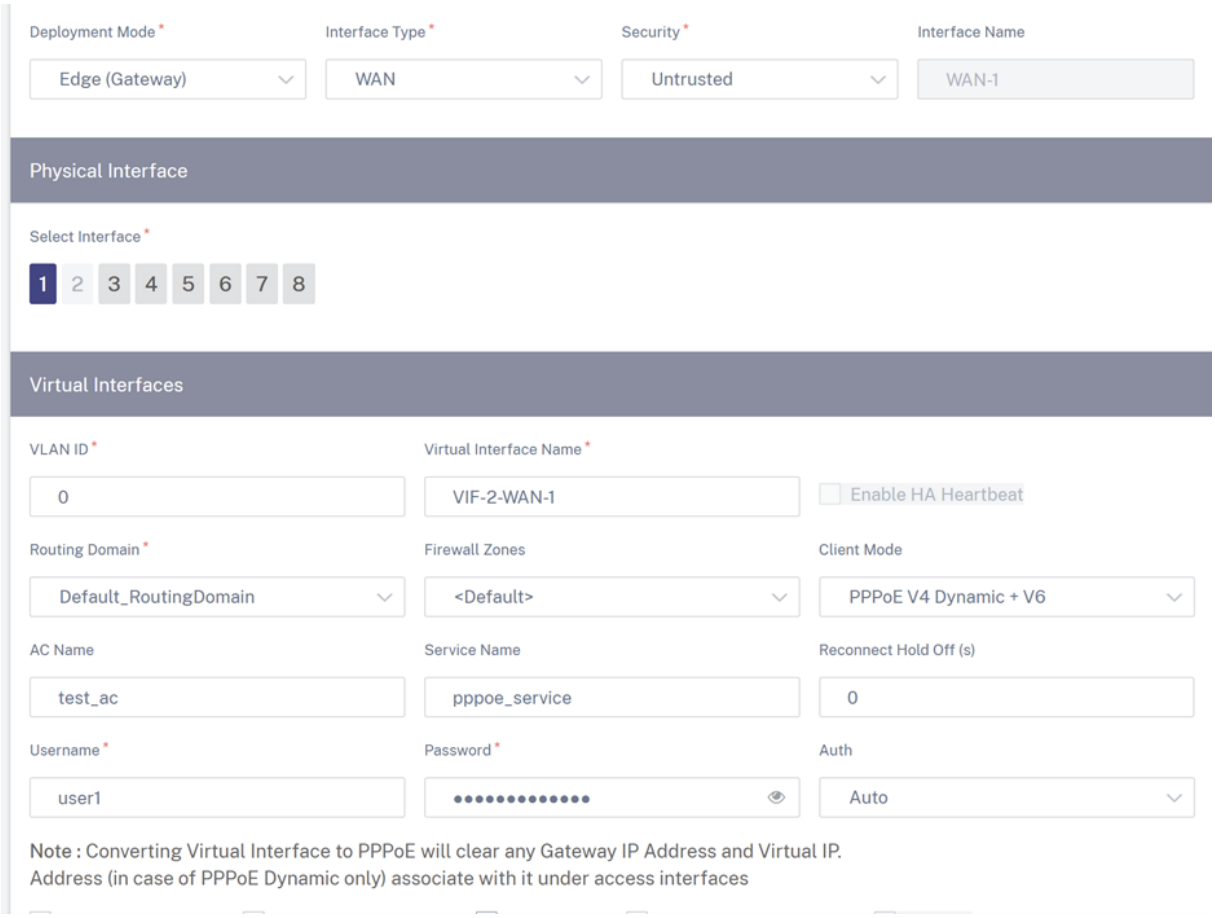
Dans la version 11.3.1 de Citrix SD-WAN, un en-tête PPPoE supplémentaire de 8 octets est envisagé pour ajuster la taille maximale du segment (MSS) de TCP. L'en-tête PPPoE supplémentaire de 8 octets ajuste le MSS dans les paquets de synchronisation en fonction du MTU. Le MTU pris en charge est compris entre 1 280 octets et 1 492 octets.

Configuration de PPPoE Sur un MCN, vous ne pouvez configurer que le PPPoE statique. Sur une branche, vous pouvez configurer le PPPoE statique ou le PPPoE dynamique.

Pour configurer PPPoE, au niveau du site, accédez à **Configuration > Configuration du site > onglet Interfaces** . Dans la section **Interfaces virtuelles**, sélectionnez l'option PPPoE appropriée dans la liste déroulante **Mode client** .

Remarque

- Un VNI configuré avec plusieurs interfaces ne peut avoir qu'une seule interface utilisée pour la connectivité PPPoE.
- Si un VNI configuré avec plusieurs interfaces et une connectivité PPPoE est remplacé par une autre interface, la page **Rapports > Temps réel > PPPoE** peut être utilisée pour arrêter la session existante et démarrer une nouvelle session. La nouvelle session peut ensuite être établie via la nouvelle interface.
- Si PPPoE Dynamic est sélectionné, le VNI doit être « Non approuvé. »



- **Nom AC :** Fournissez le nom du concentrateur d'accès (AC) pour la configuration PPPoE.
- **Nom du service :** Entrez un nom de service.
- **Suspendre (s) de reconnexion :** Entrez l'heure de suspension de la tentative de reconnexion.
- **Nom d'utilisateur :** Entrez le nom d'utilisateur pour la configuration PPPoE.
- **Mot de passe :** Entrez le mot de passe pour la configuration PPPoE.
- **Authentification :** sélectionnez le protocole d'autorisation dans la liste déroulante.
  - Lorsque l'option **Auth** est définie sur Auto, l'appliance SD-WAN honore la demande de protocole d'authentification prise en charge reçue du serveur.

- Lorsque l'option **Auth** est définie sur PAP/CHAP/EAP, seuls les protocoles d'authentification spécifiques sont respectés. Si PAP est dans la configuration et que le serveur envoie une demande d'authentification avec CHAP, la demande de connexion est rejetée. Si le serveur ne négocie pas avec PAP, un échec d'authentification se produit.

Une seule création de lien WAN est autorisée par VNI statique ou dynamique PPPoE. La configuration de liaison WAN varie en fonction de la sélection VNI du mode client.

Si le VNI est configuré avec le mode client dynamique PPPoE :

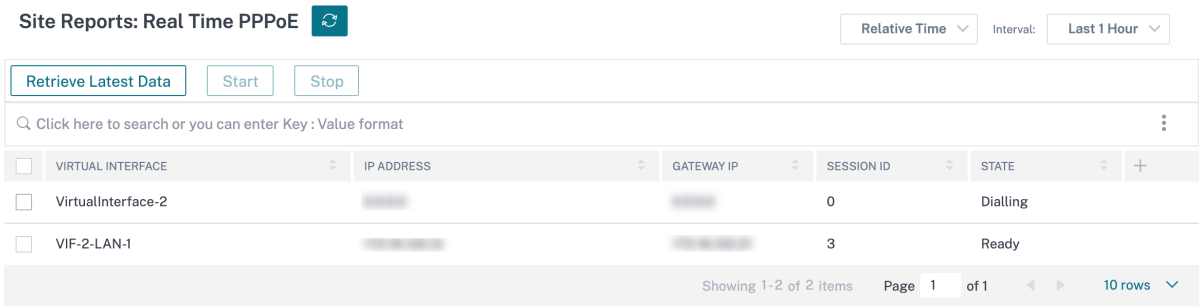
- Les champs d'adresse IP et d'adresse IP de passerelle deviennent inactifs.
- Le mode de chemin virtuel est défini sur « Primaire ».
- L'ARP proxy ne peut pas être configuré.

Par défaut, la liaison d'adresses MAC de passerelle est sélectionnée.

Si le VNI est configuré avec le mode client statique PPPoE, configurez l'adresse IP.

> **Remarque**
>
> Si le serveur ne respecte pas l'adresse IP statique configurée et propose une adresse IP différente, une erreur se produit. La session PPPoE tente de rétablir la connexion périodiquement, jusqu'à ce que le serveur accepte l'adresse IP configurée.

Surveillance et résolution des problèmes PPPoE Au niveau du site, naviguez dans la section **Rapports > Temps réel > PPPoE** pour afficher des informations sur les VNI configurés avec le mode client statique ou dynamique PPPoE. Il vous permet de démarrer ou d'arrêter manuellement les sessions à des fins de dépannage.



En cas de problème lors de l'établissement d'une session PPPoE :

- Lorsque vous passez la souris sur l'état d'échec, vous pouvez voir la raison de l'échec récent.
- Pour établir une nouvelle session ou pour dépanner une session PPPoE active, redémarrez la session.

- Si une session PPPoE est arrêtée manuellement, elle ne peut pas être démarrée tant qu'elle n'a pas été démarrée manuellement et qu'un changement de configuration n'est pas activé ou que le service n'a pas redémarré.

Une session PPPoE peut échouer pour les raisons suivantes :

- Lorsque le SD-WAN ne parvient pas à s'authentifier auprès de l'homologue en raison d'un nom d'utilisateur/mot de passe incorrect dans la configuration.
- La négociation PPP échoue - la négociation n'atteint pas le point où au moins un protocole réseau est en cours d'exécution.
- Problème de mémoire système ou de ressource système.
- Configuration invalide/incorrecte (nom d'AC ou nom de service incorrect).
- Échec de l'ouverture du port série en raison d'une erreur du système d'exploitation.
- Aucune réponse n'a été reçue pour les paquets d'écho (la liaison est défectueuse ou le serveur ne répond pas).
- Il y a eu plusieurs sessions de numérotation infructueuses continues avec en une minute.

Après 10 échecs consécutifs, la raison de l'échec est observée.

- Si l'échec est normal, il redémarre immédiatement.
- Si l'échec est une erreur, le redémarrage revient pendant 10 secondes.
- Si l'échec est fatal, le redémarrage revient pendant 30 secondes avant le redémarrage.

Les paquets de requête LCP Echo sont générés à partir du SD-WAN toutes les 60 secondes et le défaut de recevoir 5 réponses d'écho est considéré comme un échec de liaison et il rétablit la session.

- Si le VNI est opérationnel et prêt, les colonnes IP et IP de passerelle affichent les valeurs actuelles de la session. Il indique qu'il s'agit de valeurs récemment reçues.
- Si le VNI est arrêté ou est en état d'échec, les valeurs sont les dernières valeurs reçues.
- Passez la souris sur la colonne IP de la passerelle pour afficher l'adresse MAC du concentrateur d'accès PPPoE à partir duquel la session et l'adresse IP sont reçues.
- Passez la souris sur la valeur « État » pour afficher un message, ce qui est plus utile pour un état « Échec ».

Type de session PPPoE	Couleur du statut	Description
Configuré	Jaune	Un VNI est configuré avec PPPoE. C'est un état initial.

Type de session PPPoE	Couleur du statut	Description
Numérotation	Jaune	Une fois qu'un VNI est configuré, l'état de la session PPPoE passe à l'état de numérotation en démarrant la découverte PPPoE. Les informations sur les paquets sont capturées.
La	Jaune	Le VNI passe de l'état de découverte à l'état de session, en attendant de recevoir une adresse IP, s'il est dynamique, ou en attente d'un accusé de réception du serveur pour l' adresse IP annoncée, si elle est statique.
Prêt	Vert	Les paquets IP sont reçus et le VNI et la liaison WAN associée sont prêts à être utilisés.
Échec	Rouge	La session PPP/PPPoE est terminée. La raison de l'échec peut être due à une configuration non valide ou à une erreur fatale. La session tente de se reconnecter après 30 secondes.
Arrêté	Jaune	La session PPP/PPPoE est arrêtée manuellement.
Terminer	Jaune	Un état intermédiaire se terminant pour une raison. Cet état démarre automatiquement après une certaine durée (5 secondes pour une erreur normale ou 30 secondes pour une erreur fatale).
Désactivé	Jaune	Le service SD-WAN est désactivé.

Le fichier *SDWAN_ip_learned.log* contient des journaux liés à PPPoE. Accédez à **Résolution des problèmes > Journaux des périphériques** pour afficher ou télécharger le fichier *SDWAN_ip_learned.log* .

Configuration 802.1X filaire

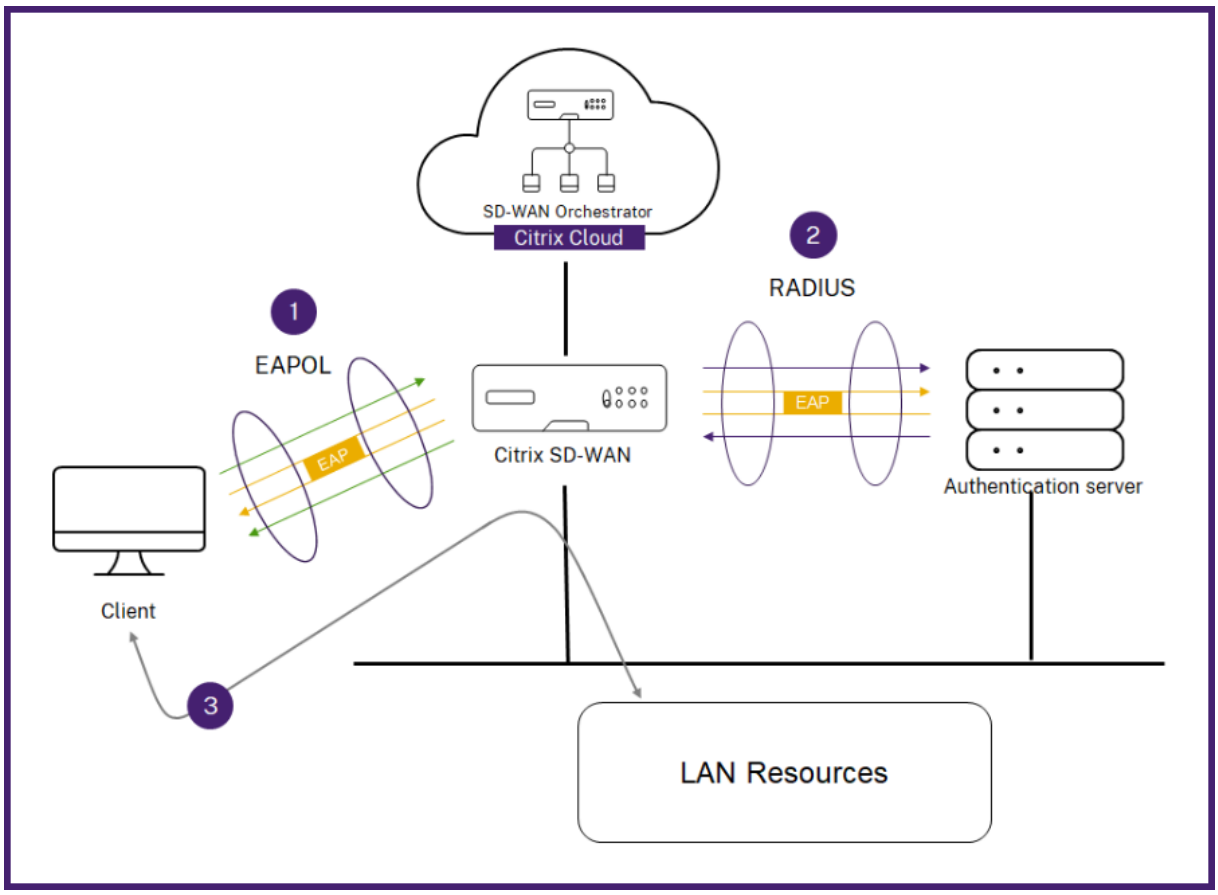
Le 802.1X filaire est un mécanisme d'authentification qui oblige les clients à s'authentifier avant de pouvoir accéder aux ressources du réseau local. Le service Citrix SD-WAN Orchestrator prend en charge la configuration de l'authentification 802.1X filaire sur les interfaces LAN.

Dans le réseau Citrix SD-WAN, les clients envoient des demandes d'authentification à l'appliance Citrix SD-WAN pour accéder aux ressources LAN. L'appliance Citrix SD-WAN agit en tant qu'authentificateur et envoie les demandes d'authentification au serveur d'authentification. Le service Citrix SD-WAN Orchestrator prend en charge uniquement les serveurs RADIUS à configurer en tant que serveurs d'authentification.

Lors de la première authentification, seuls les paquets EAPOL peuvent être traités ou les paquets DHCP capables d'initialiser l'authentification 802.1X à partir du réseau local virtuel par défaut. Un client nouvellement connecté doit être authentifié dans les 90 secondes. Si l'authentification est réussie, elle a accès aux ressources du réseau local.

Si l'authentification échoue, le client n'a pas accès au réseau et tous les paquets sont supprimés. Les clients directement connectés à l'appliance Citrix SD-WAN peuvent réessayer l'authentification en débranchant le câble Ethernet et en le réinsérant. Vous pouvez éventuellement définir un réseau local virtuel spécifique pour accorder l'accès à des ressources LAN limitées pour les demandes d'authentification ayant échoué. Dans de tels cas, les demandes d'authentification qui ont échoué ont accès au réseau local virtuel spécifié. Vous pouvez restreindre l'accès au trafic authentifié en utilisant différents domaines de routage ou zones de pare-feu lors de la création du réseau local virtuel.

> **Remarque**
>
> - La norme 802.1X doit toujours être activée sur le réseau local virtuel par défaut.
> - Les réseaux locaux virtuels dynamiques ne sont pas pris en charge.



L'appliance Citrix SD-WAN s'attend à recevoir des paquets sans balise 802.1Q (paquets non balisés). Si l'appliance Citrix SD-WAN reçoit un paquet avec une balise 802.1Q définie sur le réseau local virtuel attribué, tous les paquets provenant du MAC doivent être balisés. Si un paquet est reçu sans étiquette 802.1Q dans l'en-tête ou avec une étiquette autre que le réseau local virtuel auquel appartient l'adresse MAC, le paquet est supprimé.

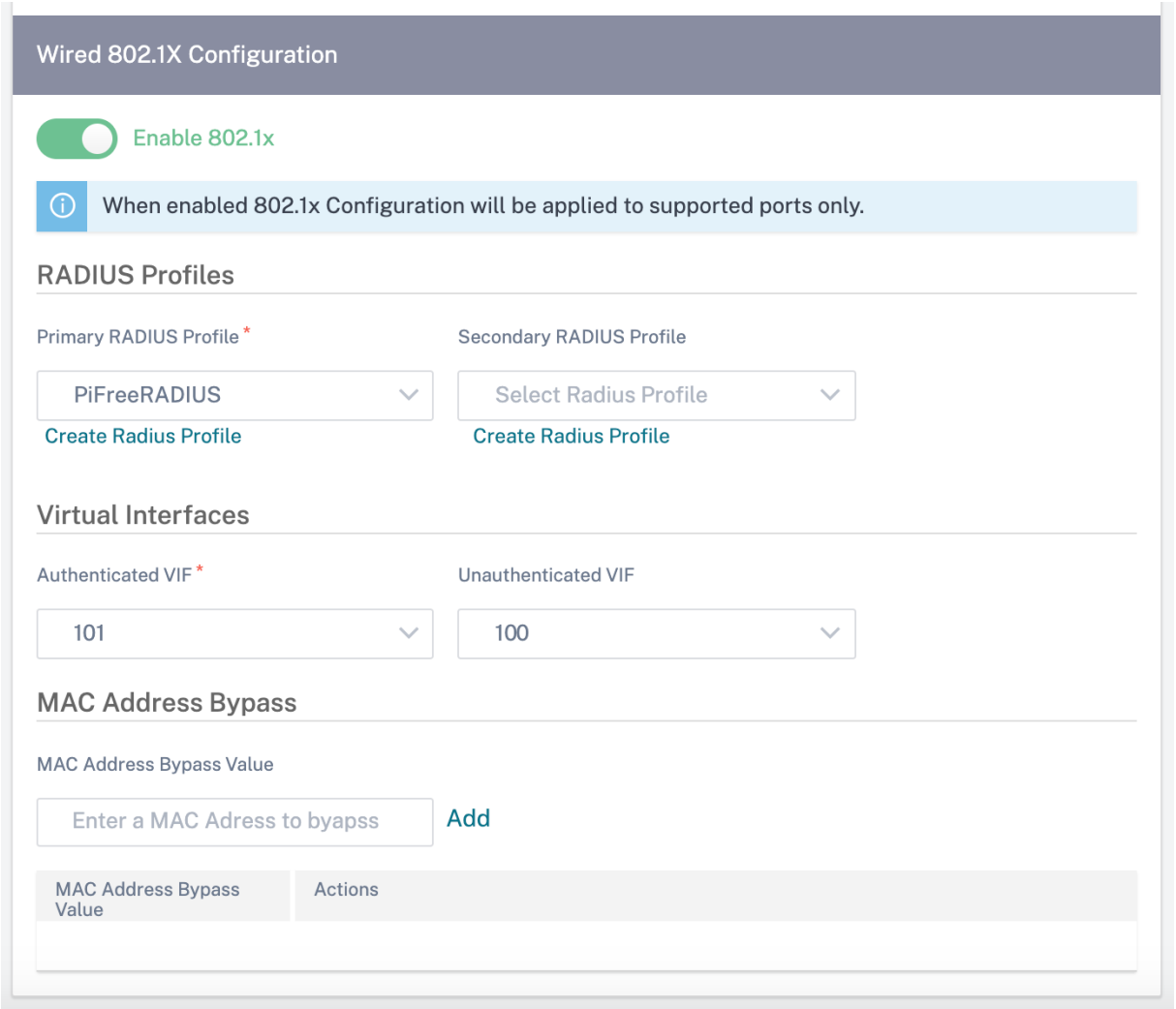
Lorsque plusieurs clients connectés à un commutateur tentent de s'authentifier en même temps sur un seul port, chaque client est authentifié individuellement, avant de pouvoir accéder aux ressources du réseau local. Les clients qui ne parviennent pas à s'authentifier peuvent recommencer l'authentification en débranchant le câble Ethernet, en attendant 3 minutes et en réinsérant le câble Ethernet. Les plateformes Citrix SD-WAN 110, 210 et 410 prennent en charge un maximum de 32 clients (authentifiés et non authentifiés). Toutes les autres plateformes prennent en charge un maximum de 64 clients (authentifiés et non authentifiés).

Pour configurer l'authentification 802.1X, accédez à **Configuration du site > Interfaces** et **activez le bouton Activer le 802.1x** . Sélectionnez un profil RADIUS existant ou cliquez sur **Créer un profil RADIUS** pour créer un profil RADIUS. Pour plus de détails sur la création d'un profil RADIUS, voir Profils de serveur RADIUS. Vous pouvez utiliser les mêmes profils RADIUS pour l'authentification filaire 802.1x et l'authentification WPA2-Enterprise sans fil, à condition que votre appliance prenne en charge le WPA2-Enterprise sans fil.

Sélectionnez une interface virtuelle dans la liste déroulante **VIF authentifiée** . L'interface virtuelle sélectionnée donne accès aux ressources du réseau local pour les demandes d'authentification réussies.

Vous pouvez éventuellement sélectionner une interface dans la liste déroulante **VIF non authentifiée** . L'interface virtuelle sélectionnée donne accès à une ressource LAN spécifique pour les demandes authentifiées ayant échoué.

Vous pouvez ajouter une liste d'adresses MAC qui contourne le processus d'authentification. Le trafic provenant de ces adresses MAC sera implicitement traité comme authentifié. Ces adresses MAC sont susceptibles de faire l'objet d'attaques malveillantes. Utilisez donc cette fonctionnalité uniquement dans des environnements physiquement sécurisés et pour le matériel existant qui ne prend pas en charge l'authentification 802.1x filaire.



Vous pouvez consulter les alertes associées aux demandes d'authentification 802.1x câblées sous **Rapports > Alertes**. Pour plus d'informations, voir Alertes.

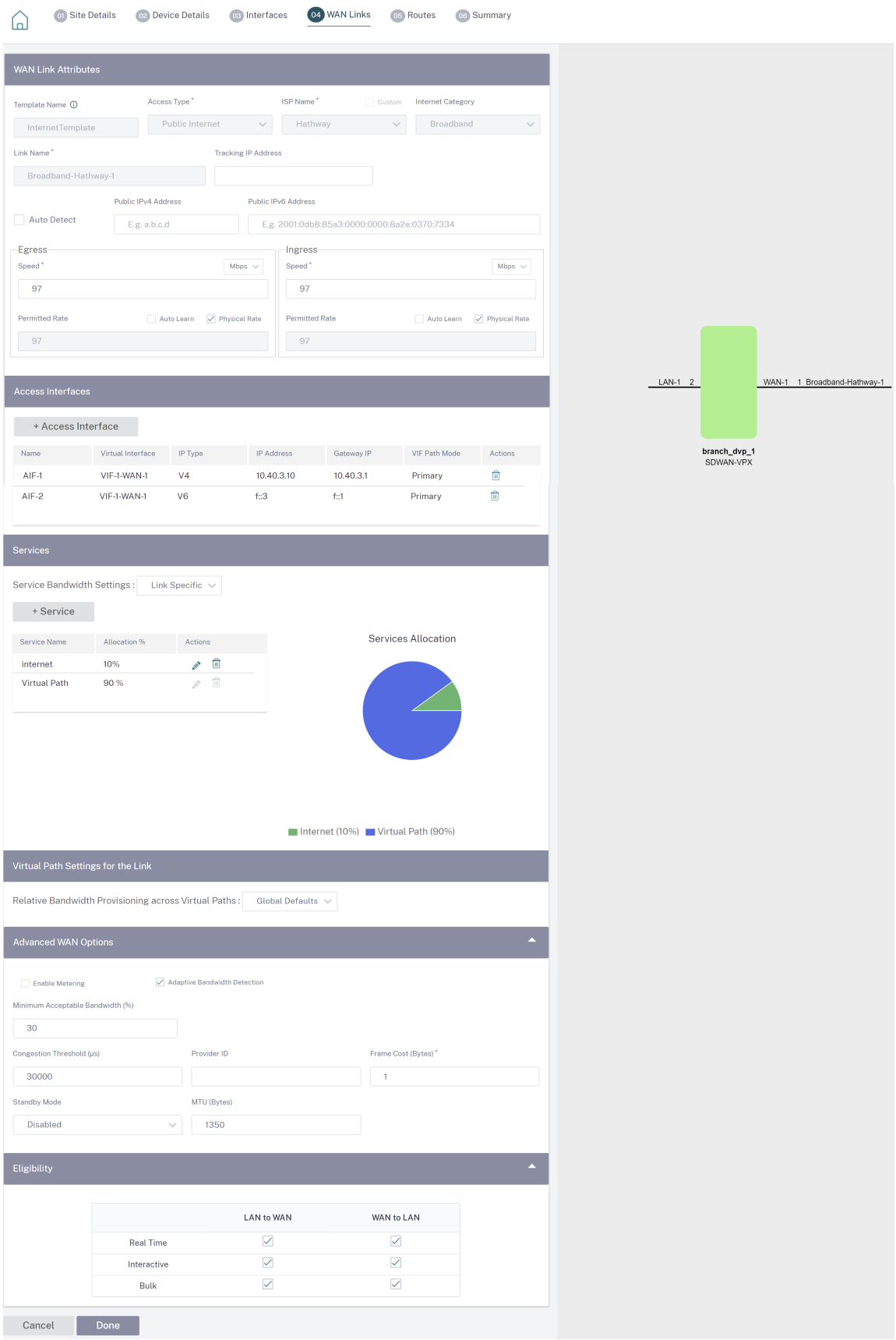
Liens WAN

L'étape suivante consiste à configurer les liens WAN. Cliquez sur **+ Lien WAN** pour commencer à configurer un lien WAN.

La configuration de la liaison WAN implique la configuration du type d'accès à la liaison WAN et des attributs d'interface d'accès.

Vous pouvez configurer l'attribut de **lien WAN** à partir de zéro ou utiliser un modèle de lien WAN pour configurer rapidement les attributs de lien WAN. Si vous avez déjà utilisé un profil de site, les attributs du **lien WAN** sont automatiquement renseignés.

Attributs de liaison WAN



- **Nom du modèle** : nom du modèle de lien WAN utilisé pour créer le lien WAN. Le nom du modèle de lien WAN ne peut pas être modifié après la création des liens WAN. Une fois les liens WAN créés à l'aide d'un modèle de lien WAN, vous ne pouvez pas modifier le type d'accès, le nom du fournisseur de services Internet ou la catégorie Internet.
- **Type d'accès** : Spécifie le type de connexion WAN de la liaison.
  - **Internet public** : indique que le lien est connecté à Internet via un fournisseur de services Internet.
  - **Intranet privé** : indique que le lien est connecté à un ou plusieurs sites au sein du réseau SD-WAN et ne peut pas se connecter à des emplacements situés en dehors du réseau SD-WAN.
  - **MPLS** : variante spécialisée de l'intranet privé. Indique que le lien utilise une ou plusieurs balises DSCP pour contrôler la qualité de service entre deux points ou plus sur un intranet et ne peut pas se connecter à des emplacements situés en dehors du réseau SD-WAN.
- **Nom du fournisseur**de services Internet : nom du fournisseur de services.
- **Catégorie Internet** : type de service technologique d'accès Internet par liaison WAN (haut débit, satellite, fibre, LTE, etc.) activé sur la liaison WAN.
- **Nom du lien** : renseigné automatiquement en fonction des entrées précédentes.
- **Adresse IP de suivi** : adresse IP virtuelle sur le chemin virtuel qui peut être envoyée par ping pour déterminer l'état du chemin.
- Adresse**IPv4 publique et adresseIPv6 publique** : adresse IP du serveur NAT ou DNS. Cette adresse est applicable et exposée, uniquement lorsque le type d'accès de liaison WAN est Public Internet ou Private Intranet dans le déploiement Serial HA. L'adresse IP publique peut être configurée manuellement ou auto-apprise à l'aide de l'option Auto Learn.
- **Détection automatique** : lorsqu'elle est activée, l'appliance SD-WAN détecte automatiquement l'adresse IP publique. Cette option n'est disponible que lorsque le rôle de l'appareil est une **branche** et non le **nœud de contrôle principal (MCN)**.
- Vitesse de**sortie : vitesse**du WAN au réseau local.
  - **Vitesse : vitesse**disponible ou autorisée du trafic WAN vers LAN en Kbits/s ou Mbits/s.
  - **Taux autorisé** : dans les cas où l'intégralité de la capacité de la liaison WAN n'est pas censée être utilisée par l'appliance SD-WAN, modifiez le débit autorisé en conséquence.
  - **Apprentissage automatique** : lorsque vous n'êtes pas sûr de la bande passante et que les liens ne sont pas fiables, vous pouvez activer la fonction d'apprentissage automatique. La fonction d'apprentissage automatique apprend uniquement la capacité de liaison sous-jacente et utilise la même valeur à l'avenir.
  - **Débit physique** : capacité de bande passante réelle de la liaison WAN.
- **Vitesse d'entrée : vitesse**du réseau local au réseau étendu.
  - **Vitesse : vitesse**disponible ou autorisée du trafic LAN vers WAN en Kbits/s ou Mbits/s.

- **Taux autorisé** : dans les cas où toute la capacité de la liaison LAN n'est pas censée être utilisée par l'appliance SD-WAN, modifiez le débit autorisé en conséquence.
- **Apprentissage automatique** : lorsque vous n'êtes pas sûr de la bande passante et que les liens ne sont pas fiables, vous pouvez activer la fonction d'apprentissage automatique. La fonction d'apprentissage automatique apprend uniquement la capacité de liaison sous-jacente et utilise la même valeur à l'avenir.
- **Débit physique** : capacité de bande passante réelle de la liaison LAN.

Files d'attente MPLS

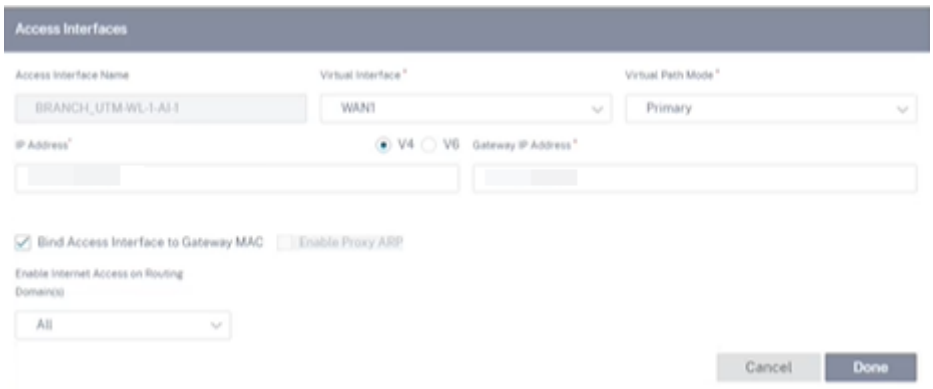
Les paramètres de **file d'attente MPLS** sont disponibles uniquement pour les accès à une liaison WAN de type MPLS. Cette option est destinée à activer la définition des files d'attente correspondant aux files d'attente MPLS du fournisseur de services, sur la liaison WAN MPLS MPLS. Pour plus d'informations sur l'ajout de files d'attente MPLS, voir Files d'attente MPLS.

Interface d'accès

Une interface d'accès définit l'adresse IP et l'adresse IP de passerelle d'une liaison WAN. Au moins une interface d'accès est requise pour chaque liaison WAN. Voici les paramètres de l'interface d'accès :

- **Nom de l'interface d'accès** : nom par lequel l'interface Access est référencée. La valeur par défaut utilise la convention de nommage suivante : WAN_link_name-AI-number : où WAN_LINK_Name est le nom du lien WAN que vous associez à cette interface, et le numéro est le nombre d'interfaces d'accès actuellement configurées pour ce lien, incrémenté de 1.
- **Interface virtuelle : interface**virtuelle utilisée par l'interface d'accès. Sélectionnez une entrée dans le menu déroulant des Interfaces virtuelles configurées pour le site de succursale actuel.
- **Mode chemin virtuel** : Spécifie la priorité du trafic du chemin virtuel sur la liaison WAN actuelle. Les options sont les suivantes : Primaire, Secondaireou Exclure. Si elle est définie sur Exclure, l'interface d'accès est utilisée uniquement pour le trafic Internet et Intranet.
- **Adresse IP : adresse**IP du point de terminaison de l'interface d'accès entre l'appliance et le WAN. Sélectionnez V4 (IPv4) ou V6 (IPv6) selon vos besoins.
- **Adresse IP de la passerelle** : adresse IP du routeur de passerelle.
- **Lier l'interface d'accès à la passerelle MAC** : si cette option est activée, l'adresse MAC source des paquets reçus sur les services Internet ou Intranet doit correspondre à l'adresse MAC de la passerelle (liens Wank > Options WAN avancées).
- **Activer le proxy ARP** : si cette option est activée, l'appliance Virtual WAN répond aux demandes ARP concernant l'adresse IP de la passerelle, lorsque la passerelle est inaccessible.
- **Activer l'accès à Internet sur le ou les domaines de routage** : crée automatiquement une route PAR DÉFAUT (0.0.0.0/0) dans toutes les tables de routage des domaines de routage respectifs. Vous pouvez activer pour TOUS les domaines de routage ou AUCUN. Il évite la nécessité de

créer une route statique exclusive sur tous les domaines de routage s'ils avaient besoin d'un accès Internet.



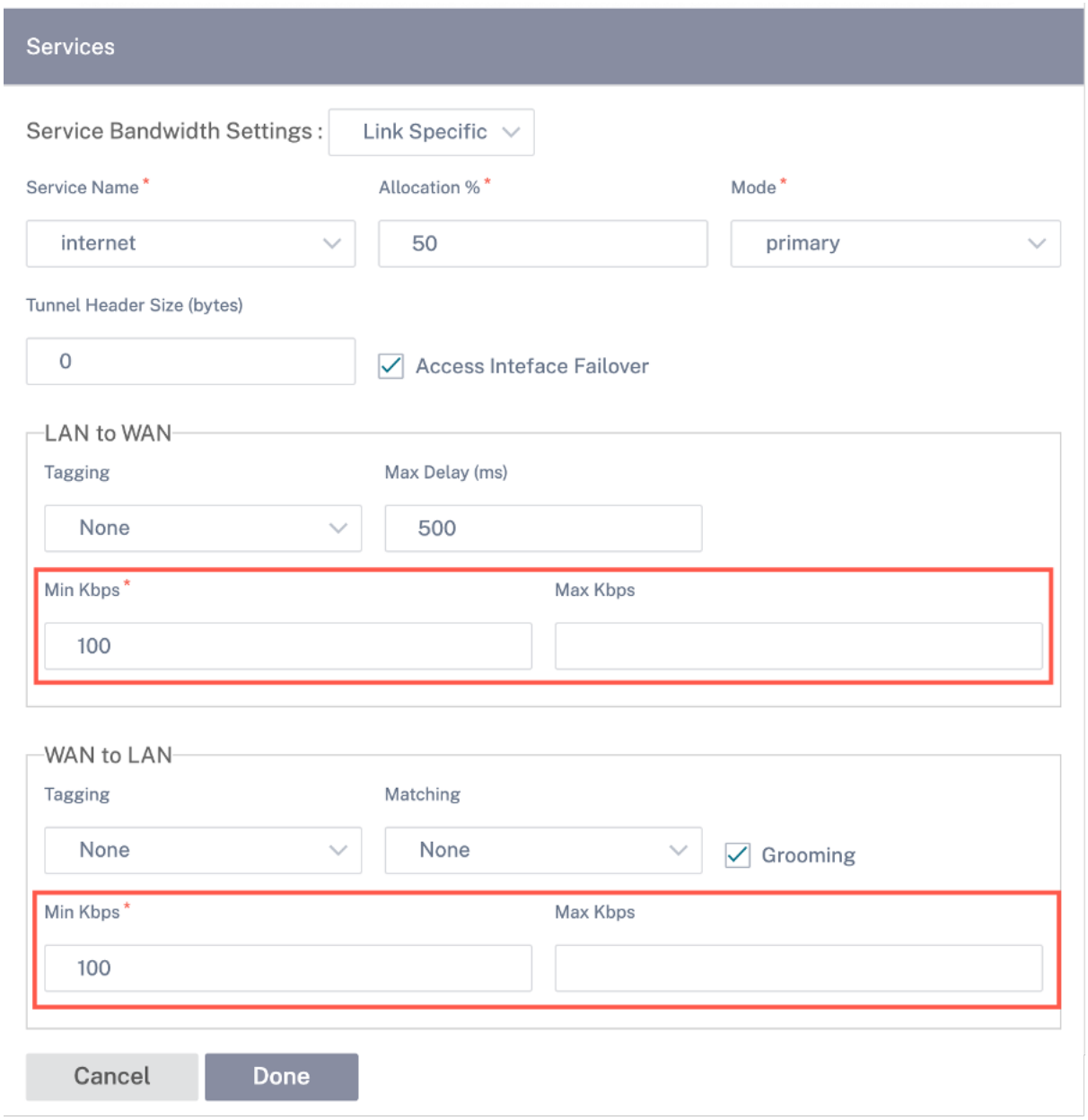
Services

La section **Services** vous permet d'ajouter des types de services et d'allouer le pourcentage de bande passante à utiliser pour chaque type de service. Vous pouvez définir les types de services et configurer leurs attributs dans la section Services de livraison . Vous pouvez choisir d'utiliser ces valeurs par défaut globales ou de configurer des paramètres de bande passante de service spécifiques à un lien dans la liste déroulante **Paramètres de bande passante du service** . Si vous choisissez un lien spécifique, entrez les détails suivants :

- **Nom du service** : nom du service de liaison WAN.
- **% d'allocation** : juste part garantie de bande passante allouée au service par rapport à la capacité totale de la liaison.
- **Mode : mode**de fonctionnement de la liaison WAN, en fonction du service sélectionné. Pour Internet, il y a un des services Primaire, Secondaire et Solde, et pour Intranet, il y a primaire et secondaire.
- **Taille de l'en-tête du tunnel** : taille de l'en-tête du tunnel, en octets.
- **Tag LAN vers WAN** : La balise DHCP à appliquer aux paquets LAN vers WAN sur le service.
- **Délai LAN vers WAN** : durée maximale de mise en mémoire tampon des paquets lorsque la bande passante des liaisons WAN est dépassée.
- **Minimum Kbits/s du réseau local vers le WAN** : valeur minimale de bande passante de téléchargement réservée au service. Le champ **Min Kbits/s** est obligatoire.
- **Kbits/s max. LAN vers WAN** : valeur de bande passante de téléchargement maximale réservée au service. Le champ **Max Kbits/s** est facultatif et la valeur ne peut pas être inférieure à la valeur de bande passante de téléchargement minimale configurée. La valeur doit être supérieure ou égale à la valeur de bande passante de téléchargement minimale.
- **Balise WAN vers LAN** : La balise DHCP à appliquer aux paquets WAN vers LAN du service.

- **Correspondance WAN vers LAN** : critères de correspondance pour les paquets Internet WAN vers LAN à attribuer au service.
- **Min. Kbits/s WAN vers LAN** : valeur minimale de bande passante de téléchargement réservée au service. Le champ **Min Kbits/s** est obligatoire.
- **Kbits/s max. du WAN au réseau local** : valeur maximale de bande passante de téléchargement réservée au service. Le champ **Max Kbits/s** est facultatif et la valeur ne peut pas être inférieure à la valeur de bande passante de téléchargement minimale configurée. La valeur doit être supérieure ou égale à la valeur de bande passante de téléchargement minimale.
- **Grooming WAN vers LAN** : si cette option est activée, les paquets sont supprimés de manière aléatoire pour éviter que le trafic WAN vers LAN ne dépasse la bande passante allouée au Service.

> **Remarque**
>
> Les champs minimum et maximum en Kbits/s ne sont pas disponibles pour le chemin virtuel.



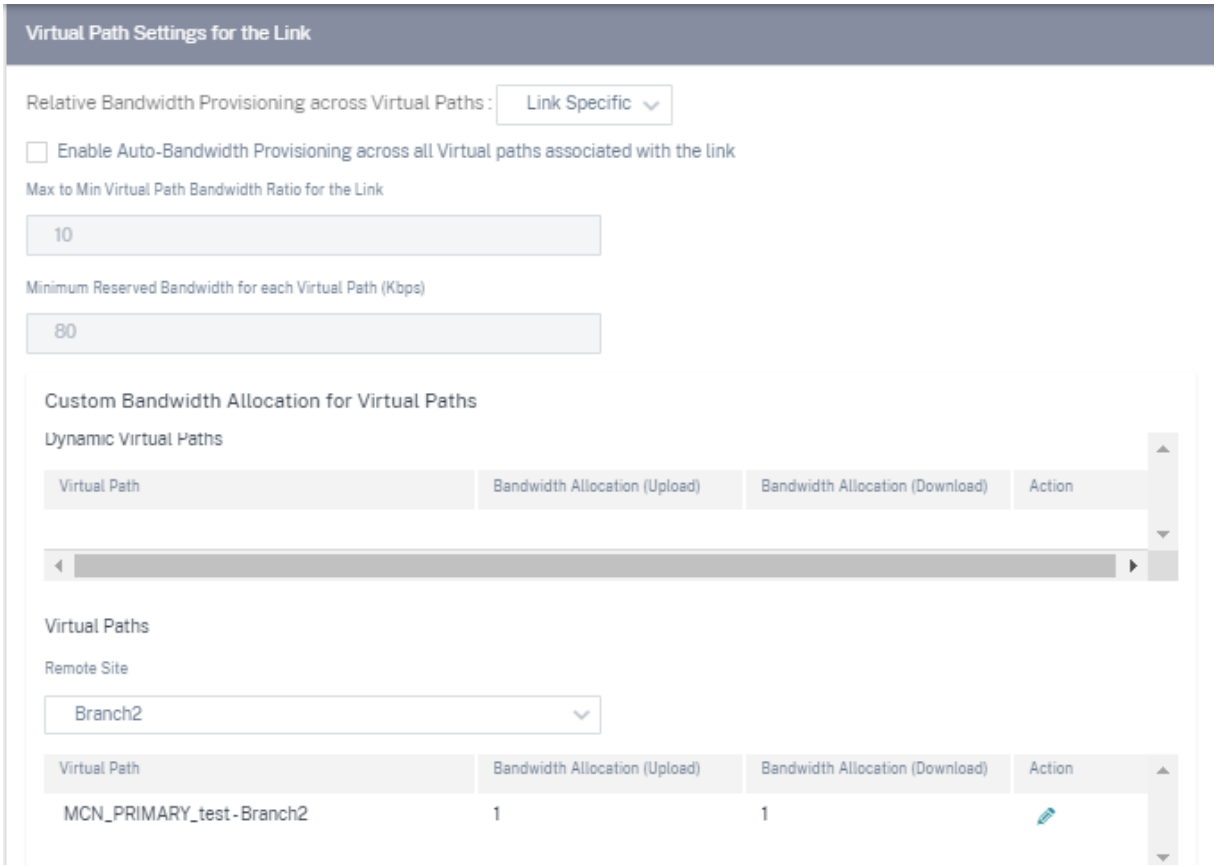
Paramètres du chemin virtuel pour le lien

Sélectionnez le provisionnement de bande passante relative sur les chemins virtuels comme étant **global par défaut** ou **spécifique au lien**, selon les besoins. Lorsque vous sélectionnez **Link Specific**, lorsque vous activez le provisionnement automatique de la bande passante, la part de bande passante du service de chemin virtuel est automatiquement calculée et appliquée en fonction de l'ampleur de la bande passante susceptible d'être consommée par les sites distants.

- **Rapport de bande passante max/minimum du chemin virtuel pour le lien** : vous pouvez définir le ratio de chemin virtuel maximal et minimum qui peut être appliqué à la liaison WAN

sélectionnée.

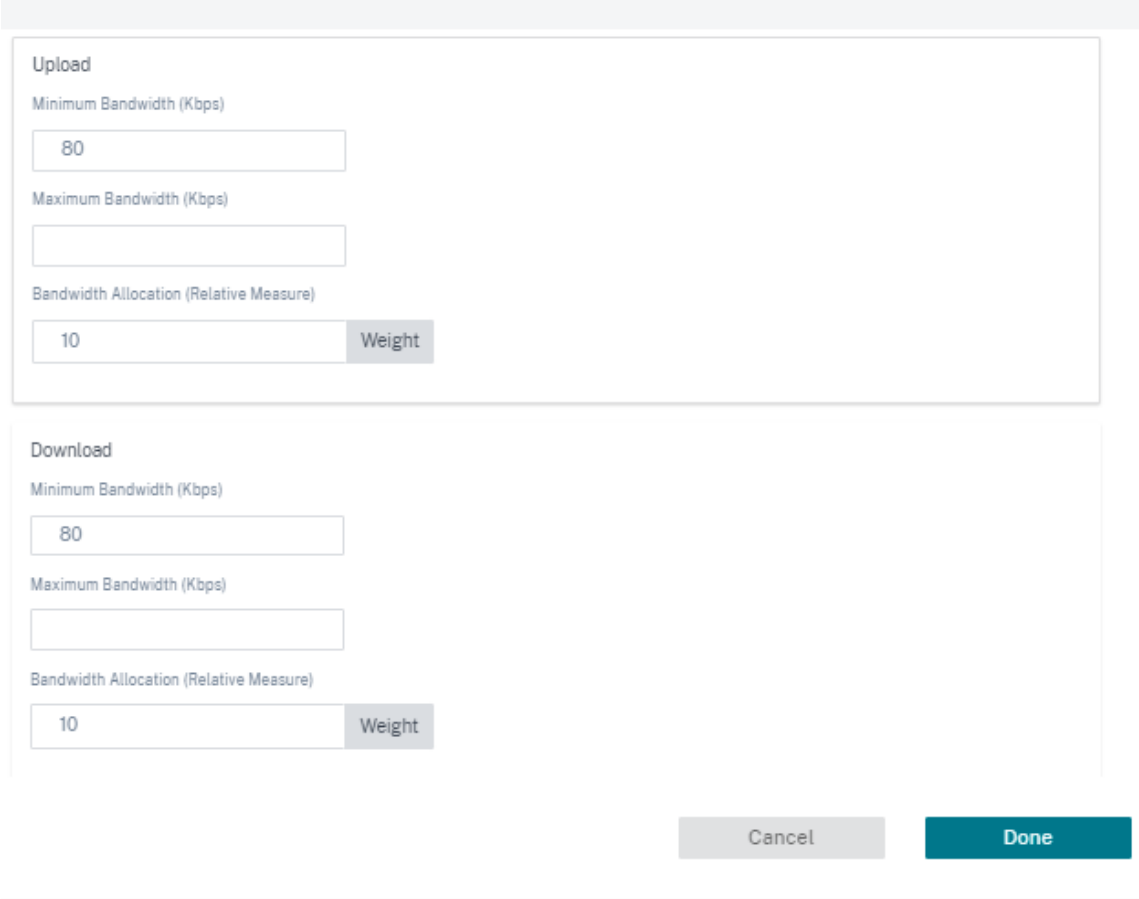
- **Bande passante réservée minimale pour chaque chemin virtuel (Kbits/s)** : Vous pouvez définir la valeur minimale de bande passante réservée en Kbit/s pour chaque chemin virtuel.



Pour personnaliser les bandes passantes des chemins virtuels associés à une liaison WAN :

1. Décochez la case **Activer le Provisioning automatique de la bande passante sur tous les chemins virtuels associés au lien** .
2. Dans la section **Allocation de bande passante personnalisée pour les chemins virtuels**, sélectionnez un site distant. Vous pouvez fournir des bandes passantes pour les chemins virtuels vers le site distant.
    - **Bande passante minimale (Kbit/s)** : bande passante minimale réservée au chemin virtuel. La bande passante minimale que vous pouvez définir pour un chemin virtuel est de 80 Kbits/s.
    - **Bande passante maximale (Kbits/s)** : bande passante maximale que le chemin virtuel peut utiliser à partir de la liaison WAN. Si la bande passante maximale n'est pas définie, le site utilise toute la bande passante disponible.
    - **Allocation de bande passante (mesure relative)** : part de bande passante allouée à un chemin virtuel en dehors de la bande passante éligible de son groupe. Par exemple, si un

groupe de liaisons WAN composé de 3 chemins virtuels est éligible à une bande passante de 30 Mbits/s et que vous souhaitez allouer une bande passante égale à chaque chemin virtuel, mettez à jour 10 comme allocation de bande passante sur le site distant.



3. Cliquez sur **Terminé**.

> **Remarque**
>
> Le service Citrix SD-WAN Orchestrator conserve les paramètres de bande passante personnalisés précédemment configurés, même après la désactivation des chemins virtuels dynamiques précédemment configurés entre deux sites. Veillez à mettre à jour les paramètres de bande passante personnalisés manuellement lorsque vous reconfigurez les chemins virtuels dynamiques.

Points à prendre en compte pour l'approvisionnement en bande passante

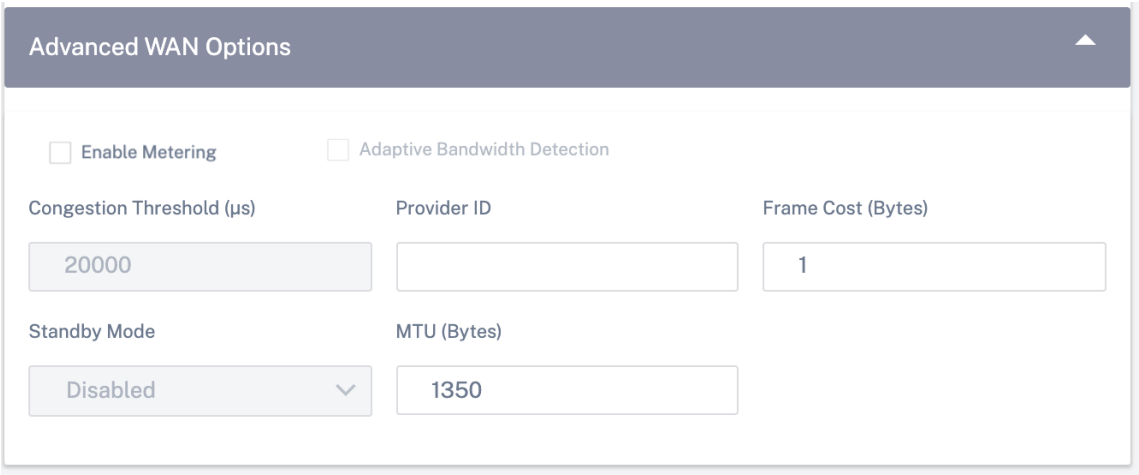
- Par défaut, toutes les succursales et tous les services WAN (chemin virtuel/Internet/Intranet) reçoivent une pondération de 1 chacun.
- La personnalisation de la bande passante est requise lorsqu'il existe une grande disparité en termes de besoins en bande passante.

- Lorsque des chemins virtuels dynamiques sont activés entre les sites disponibles, la capacité du lien WAN est partagée entre le chemin virtuel statique vers le centre de données et les chemins virtuels dynamiques.

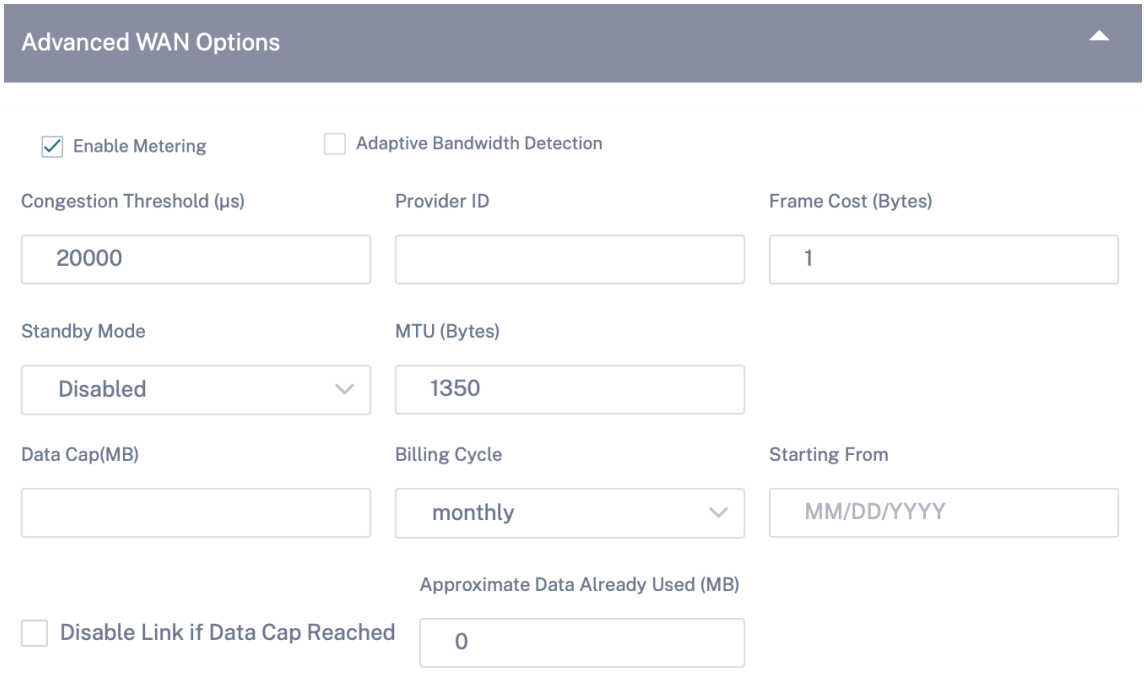
Options WAN avancées

Les paramètres avancés du lien WAN permettent de configurer les attributs **spécifiques du fournisseur de services** Internet.

- **Seuil de congestion : niveau**de congestion au-delà duquel la liaison WAN limite la transmission des paquets afin d'éviter une congestion supplémentaire.
- **ID du fournisseur** : identifiant unique permettant au fournisseur de différencier les chemins lors de l'envoi de paquets dupliqués.
- **Coût de trame (octets)** : octets d'en-tête/de bande supplémentaires ajoutés à chaque paquet, par exemple pour les remorques Ethernet IPG ou AAL5.
- **MTU (octets)** : la plus grande taille de paquet brute en octets, sans compter le coût de trame.
- **Mode veille** : Un lien de secours n'est pas utilisé pour transporter le trafic utilisateur à moins qu'il ne devienne actif. Le mode veille d'une liaison WAN est désactivé par défaut. Pour plus d'informations sur le mode veille, voir Mode veille.



- **Activer le comptage** : suit l'utilisation sur une liaison WAN et alerte l'utilisateur lorsque l'utilisation de la liaison dépasse le plafond de données configuré. Pour des informations détaillées sur le comptage, consultez la section Comptage et liaisons WAN de secours.



- **Détection adaptative de la bande passante** : utilise la liaison WAN à un débit de bande passante réduit lorsqu'une perte est détectée. Lorsque la bande passante disponible est inférieure à la **bande passante minimale acceptable**configurée, le chemin est marqué comme MAUVAIS. Utilisez la sensibilité aux pertes incorrecte personnalisée sous Path ou AutoPath avec Détection de bande passante adaptative.

  > **Remarque**
  >
  > La détection de bande passante adaptative est disponible uniquement pour le client et non pour MCN.

  - **Bande passante minimale acceptable** : lorsque le débit de bande passante varie, pourcentage de débit autorisé entre le WAN et le réseau local en dessous duquel le chemin est marqué comme MAUVAIS. Le nombre minimum de kbps est différent de chaque côté d'un chemin virtuel. La valeur peut être comprise entre 10 et 50 % et la valeur par défaut étant de 30 %.

Pour plus d'informations, voir Détection de bande passante adaptative

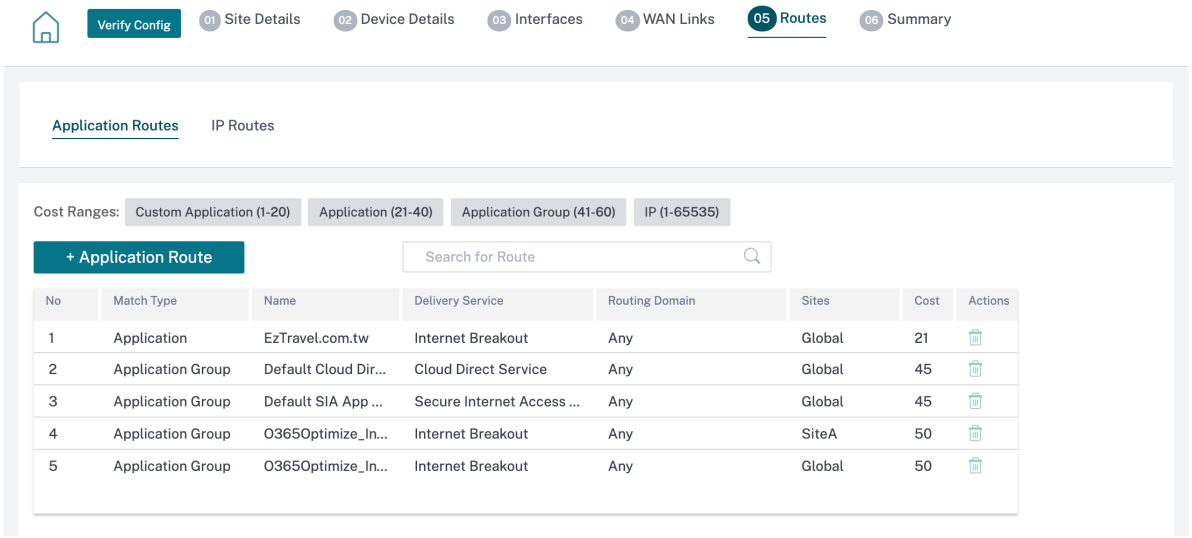
Itinéraires

L'étape suivante du workflow de configuration du site consiste à créer des itinéraires. Vous pouvez créer des itinéraires applicatifs et IP en fonction des exigences de votre site.

> **REMARQUE**
>
> Les itinéraires qui ont été ajoutés avant d'introduire les onglets **Route de l'application** et **Route IP** sont répertoriés sous l'onglet **Routes IP** avec **Delivery Service** en tant qu'Internet.

Les itinéraires globaux et les itinéraires spécifiques au site qui sont créés au niveau du réseau sont automatiquement répertoriés sous **les onglets Routes > Routes et itinéraires de l'application> Routes IP** . Vous ne pouvez afficher les itinéraires globaux qu'au niveau du site. Pour modifier ou supprimer un itinéraire global, accédez aux configurations au niveau du réseau.

Vous pouvez également créer, modifier ou supprimer des itinéraires au niveau du site.



Voies d'application

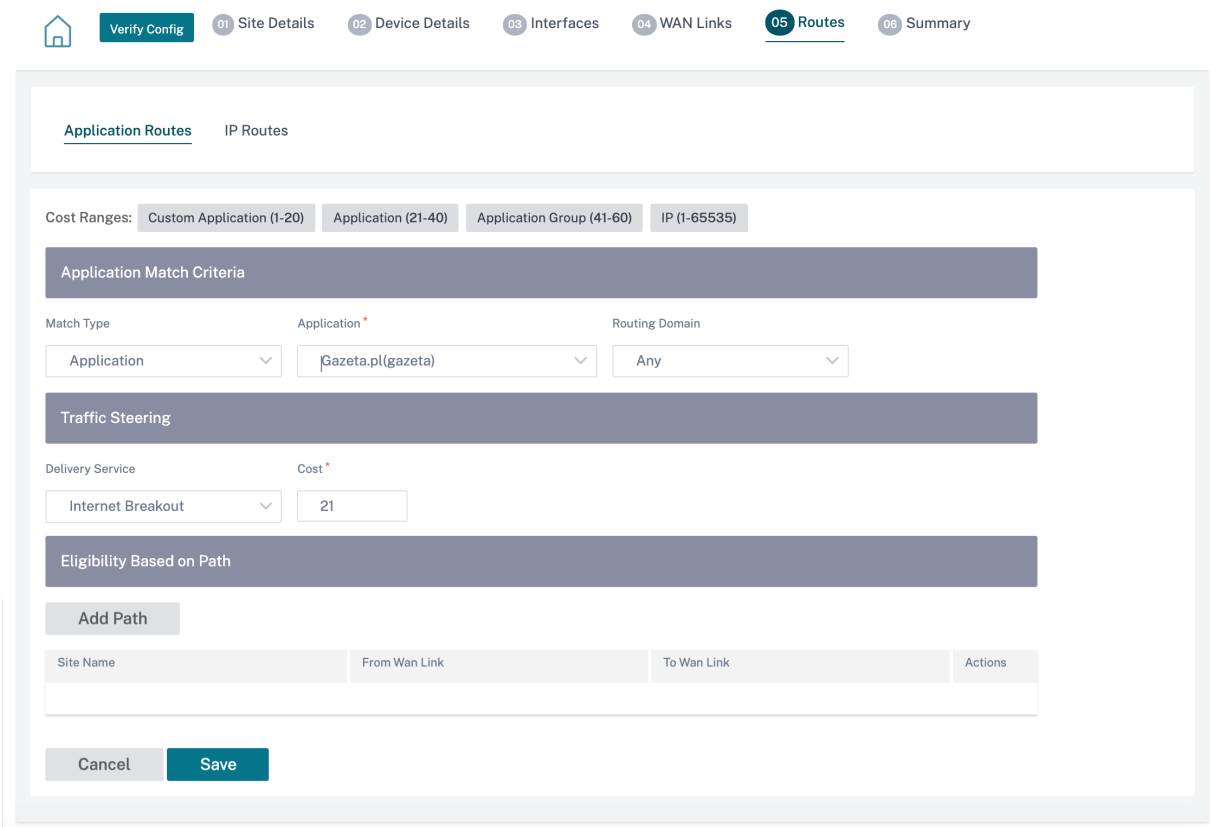
Cliquez sur **+ Route de l'application** pour créer un itinéraire d'application.

- **Critères de correspondance des applications personnalisés** :
  - **Type de correspondance** : sélectionnez le type de correspondance comme **Application/Application personnalisée/Groupe d'applications** dans la liste déroulante.
  - **Application** : Choisissez une application dans la liste déroulante.
  - **Domaine de routage** : sélectionnez un domaine de routage.
- **Direction du trafic**
  - **Service de livraison** : Choisissez un service de livraison dans la liste.
  - **Coût** : reflète la priorité relative de chaque itinéraire. Réduisez le coût, plus la priorité est élevée.
- **Éligibilité basée sur le parcours** :

- **Ajouter un chemin** : choisissez un site et des liens WAN, à la fois vers et depuis. Si le chemin ajouté tombe en panne, la route de l'application ne reçoit aucun trafic.

Si une nouvelle route d'application est ajoutée, le coût de l'itinéraire doit se situer dans la plage suivante :

- Application personnalisée : 1—20
- Application : 21—40
- Groupe d'application : 41—60



Routes IP

Accédez à l'onglet **Routes IP** et cliquez sur **+ Route IP** pour créer la politique d'itinéraire IP afin de piloter le trafic.

- **Critères de correspondance du protocole IP** :
  - **Réseau de destination** : Ajoutez le réseau de destination qui permet de transférer les paquets.
  - **Utiliser un groupe IP** : vous pouvez ajouter un réseau de destination ou activer la case à cocher Utiliser un groupe IP pour sélectionner n'importe quel groupe IP dans la liste déroulante.

  - **Domaine de routage** : sélectionnez un domaine de routage dans la liste déroulante.

- **Direction du trafic**

  - **Service de livraison** : Choisissez un service de livraison dans la liste déroulante.
  - **Coût** : reflète la priorité relative de chaque itinéraire. Réduisez le coût, plus la priorité est élevée.

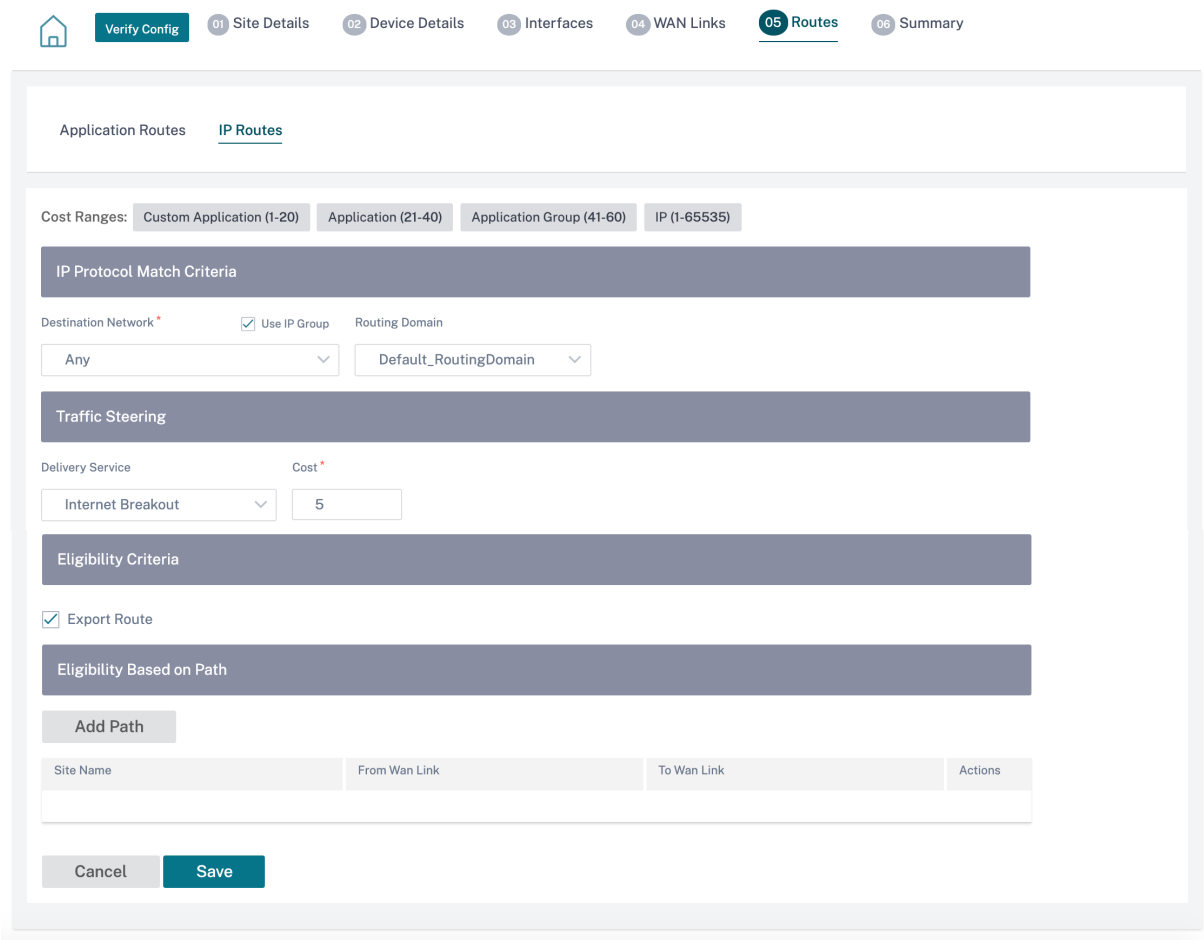
- **Critères d'éligibilité** :

  - **Exporter l'itinéraire** : si la case Exporter l'itinéraire est cochée et si l'itinéraire est un itinéraire local, l'itinéraire peut être exporté par défaut. Si l'itinéraire est un itinéraire basé sur INTRANET/INTERNET, alors pour que l'exportation fonctionne, le transfert WAN vers WAN doit être activé. Si la case à cocher Exporter l'itinéraire est désactivée, l'itinéraire local ne peut pas être exporté vers un autre SD-WAN et a une signification locale.

- **Éligibilité basée sur le parcours** :

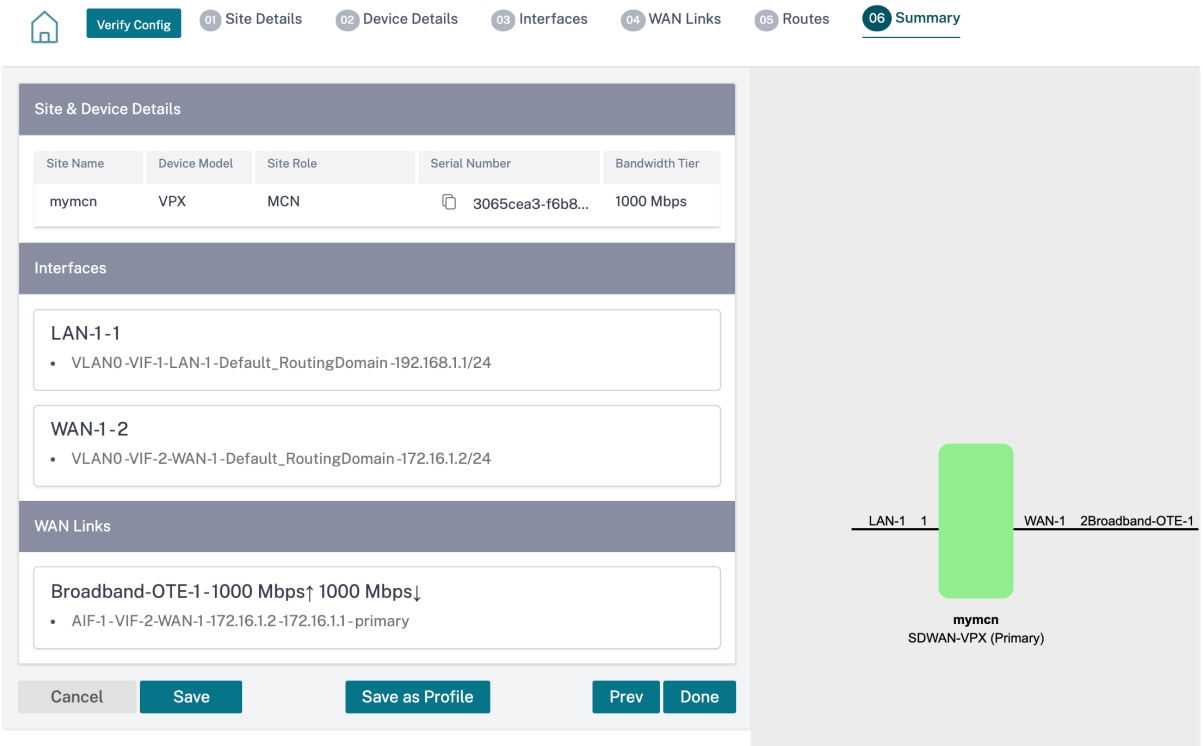
  - **Ajouter un chemin** : choisissez un site et des liens WAN, à la fois vers et depuis. Si le chemin ajouté tombe en panne, la route IP ne reçoit aucun trafic.

Si une nouvelle route IP est ajoutée, le coût de l'itinéraire doit être compris entre 1 et 20.



Résumé

Cette section fournit un résumé de la configuration du site pour permettre un examen rapide avant de soumettre la même configuration.



Utilisez l'option **Enregistrer en tant que modèle** pour enregistrer la configuration du site en tant que modèle à réutiliser sur d'autres sites. Cliquez sur **Terminer** pour marquer la fin de la configuration du site et vous rediriger vers la page d'**accueil Configuration réseau** pour passer en revue tous les sites configurés. Pour plus d'informations, voir Configuration réseau.

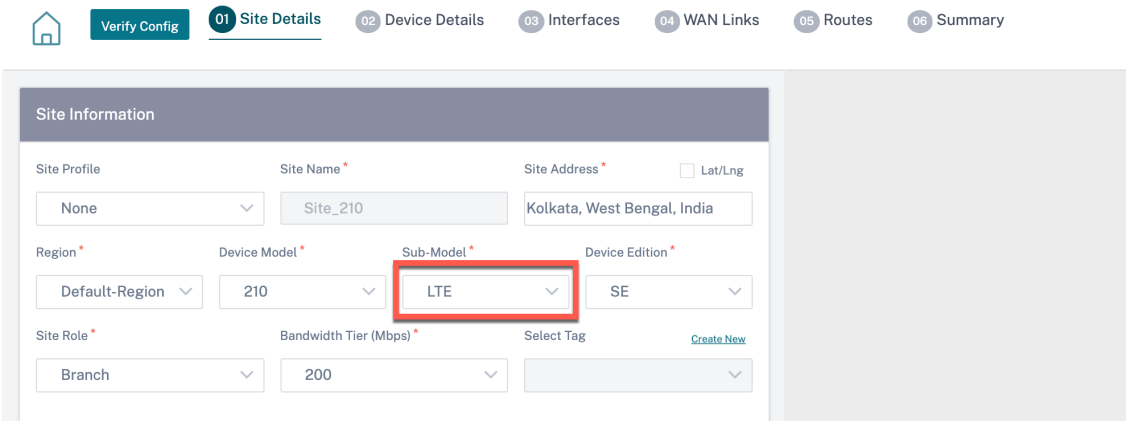
Mise à niveau du microprogramme LTE

October 21, 2022

Le service Citrix SD-WAN Orchestrator vous permet de configurer et de gérer tous les sites LTE de votre réseau. Il comprend des appareils connectés via un modem LTE interne ou un modem USB LTE externe.

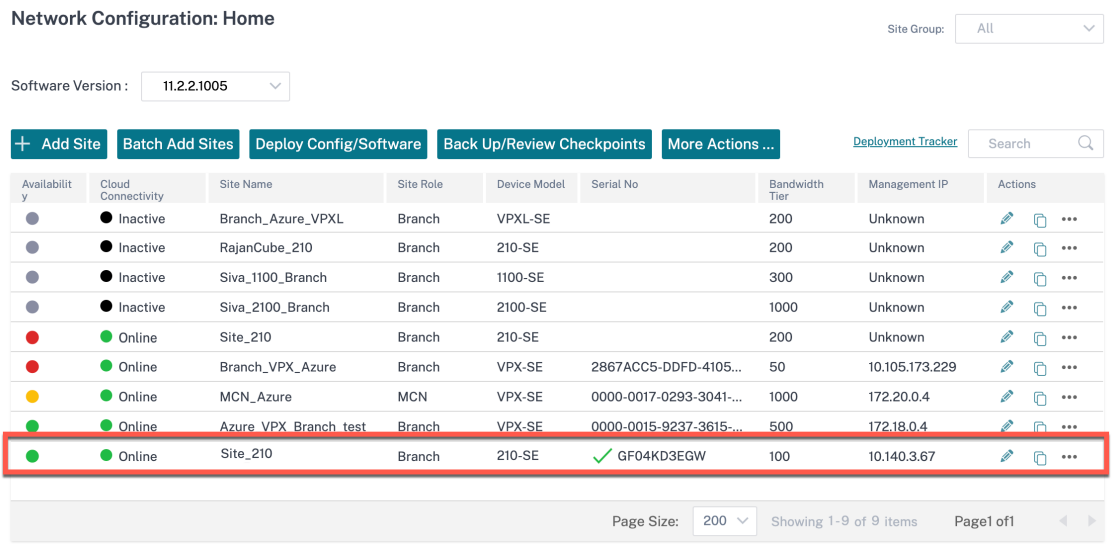
Pour configurer les sites LTE dans votre réseau :

1. Au niveau du site, accédez à **Configuration > Configuration du site**.



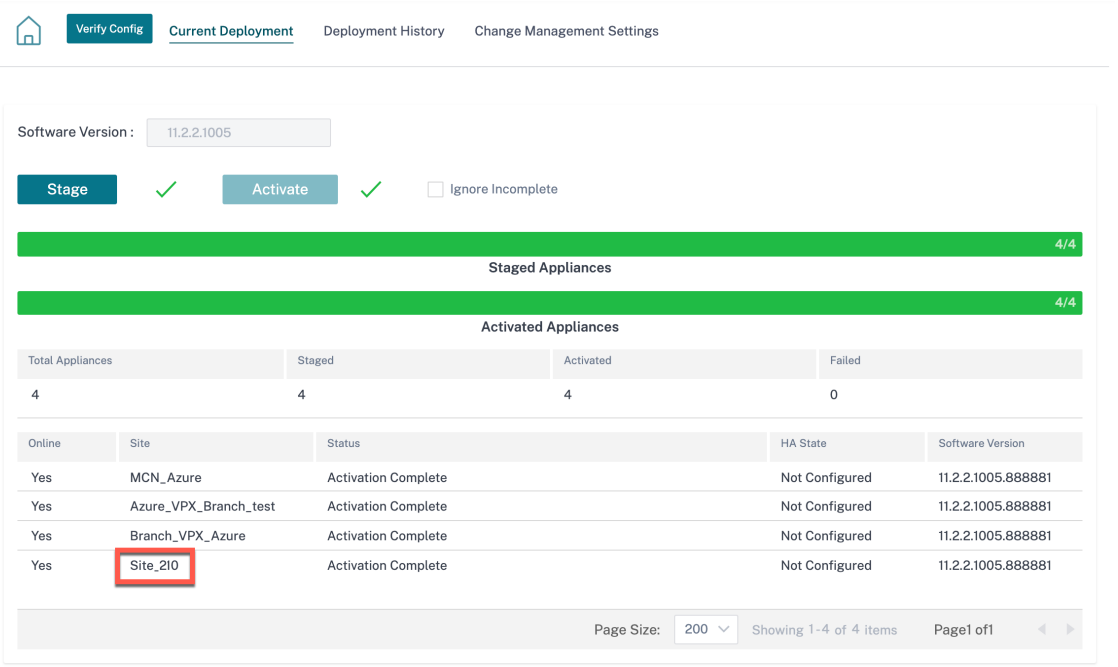
2. Sélectionnez le sous-modèle en tant que **LTE** avec les autres informations nécessaires, puis cliquez sur Enregistrer. Pour plus d'informations sur la configuration du site, voir Configuration du site.

3. Une fois le site créé, accédez à la page d'**accueil de la configuration réseau** et cliquez sur le bouton **Déployer la configuration/le logiciel** .



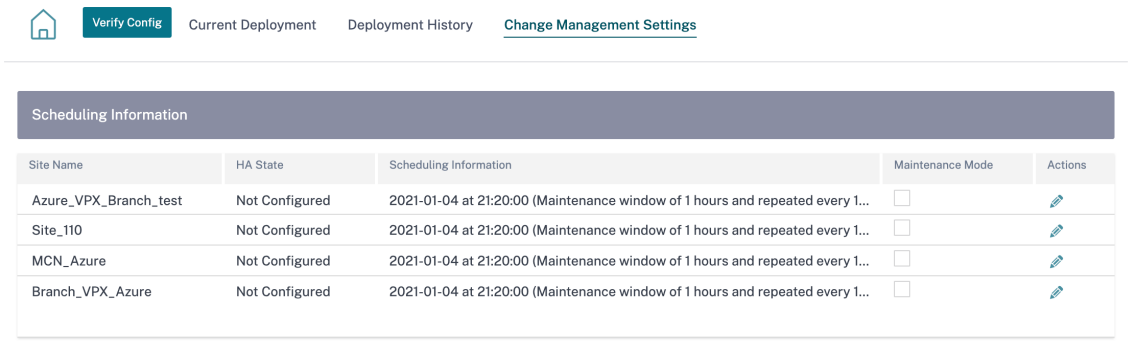
> C
>
> **Remarque**
>
> Actuellement, le support LTE est disponible sur les appliances Citrix SD-WAN 210.

4. Le champ **Version du logiciel** est automatiquement rempli avec le package de la dernière version du logiciel et le champ n'est pas modifiable. Une fois que vous avez cliqué sur **Stage**, il télécharge tous les microprogrammes LTE appropriés pour la version logicielle sélectionnée.



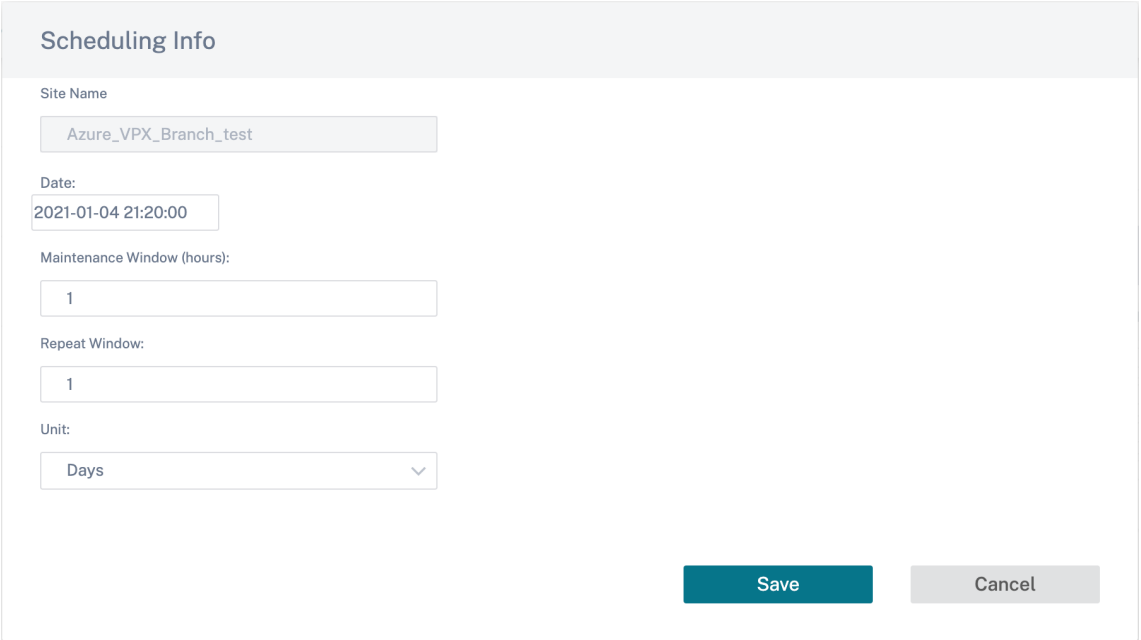
Il faut quelques minutes pour terminer la mise en scène. Vous pouvez afficher l'état pour suivre la progression du transit. Initialement, l'état indique **Staging Pending**, **Downloading Appliance Software**et enfin **Staging Complete**. Vous pouvez annuler la mise en scène à tout moment en cliquant sur le bouton **Annuler l'étape** .

5. Une fois la mise en scène terminée, cliquez sur le bouton **Activer** pour activer le logiciel.
6. L'activation du logiciel LTE fait partie de la fenêtre de planification. Pour mettre à niveau le logiciel LTE, accédez à l'onglet **Modifier les paramètres de gestion** . Vous pouvez voir une liste de noms de sites avec des informations de planification et une option d'action.



Dans la fenêtre de planification, une période spécifique est spécifiée pour terminer la mise à niveau du logiciel LTE.

7. Cliquez sur le symbole d'action et fournissez les informations de planification - date avec heure, durée de la fenêtre de maintenance en heures, répéter la fenêtre avec l'unité sous forme de jours/semaines/mois. Cliquez sur **Enregistrer**.



Une fois le timing défini, il propage les informations à l'appliance. Le microprogramme LTE est mis à niveau lorsque l'heure de l'appliance correspond à l'heure définie dans la fenêtre de planification. La fenêtre de planification vous permet de configurer une heure spécifique pour mettre à niveau le microprogramme LTE. La mise à niveau du microprogramme LTE ne démarre pas immédiatement lorsque vous définissez la fenêtre de planification.

> **Remarque**
>
> Pour toutes les appliances, les informations de planification par défaut déjà définies sont les suivantes :
>
> - **Fenêtre horaire** - 21:20:00
> - **Fenêtre de maintenance** - 1 heure
> - **Fenêtre répétée** - 1 jour
>
> Donc, si vous ne configurez pas les paramètres de gestion des modifications, la fenêtre de planification traite automatiquement la mise à jour. De plus, lorsque vous définissez la valeur de la **fenêtre de maintenance (heures)** sur **0**, la mise à niveau du microprogramme LTE se produit immédiatement.

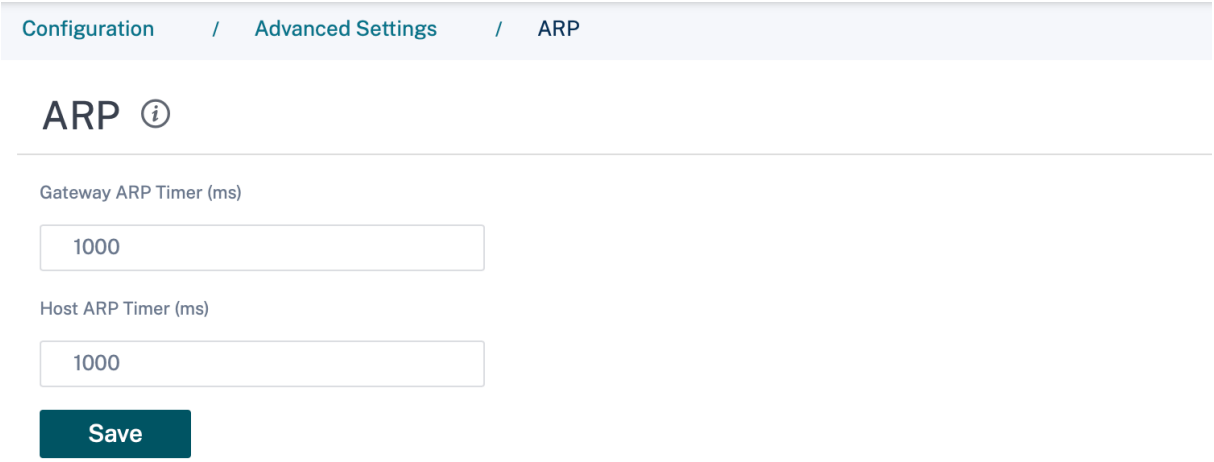
À partir de la version 11.1.0, un nouveau bouton de configuration est ajouté pour la configuration de la gestion in-band sur la page du groupe d'interface de site. Il s'agit d'une configuration obligatoire pour toute appliance devant être gérée via une adresse IP inband. L'absence de cette configuration dans le service Citrix SD-WAN Orchestrator peut entraîner la mise hors ligne de l'appliance (ce qui est particulièrement important lorsque les 210 et 110 s gérés via LTE passent à la version 11.1.0).

Protocole de résolution d'adresses

October 21, 2022

Dans les déploiements Citrix SD-WAN tels que Gateway et One-ARM, lorsque les demandes ARP (Address Resolution Protocol) sont reçues fréquemment, les points d'accès sont surchargés, ce qui affecte le flux de trafic. Pour surmonter la surcharge de trafic, vous pouvez configurer les temporisateurs ARP suivants pour envoyer les demandes ARP avec des intervalles de temps spécifiques.

- **Temporisateur ARP de passerelle (ms)** : temps (plage : 100 à 20 000 millisecondes) entre les requêtes ARP pour les adresses IP de passerelle configurées.
- **Minuteur ARP de l'hôte (ms)** : temps (plage : 1 000 à 180 000 millisecondes) entre les requêtes ARP pour les adresses IP hôtes configurées.



Protocole de découverte de voisins

October 21, 2022

Dans un réseau IPv6, les appliances Citrix SD-WAN diffusent régulièrement les messages publicitaires du routeur pour annoncer leur disponibilité et transmettre des informations aux appliances voisines du réseau SD-WAN. Les publicités du routeur incluent les informations de préfixe IPv6. Le protocole NDP (Neighbor Discovery Protocol) exécuté sur les appliances Citrix SD-WAN utilise ces publicités de routeur pour déterminer les périphériques voisins sur la même liaison. Le protocole NDP détermine également les adresses de couche de liaison de chacun, trouve les voisins et gère les informations d'accessibilité des voisins actifs.

Pour configurer la publicité du routeur NDP, accédez à **Configuration > Paramètres avancés > NDP** et cliquez sur **+ NDP**.

Choisissez l'une des interfaces virtuelles configurées dans la liste déroulante **Interface virtuelle** . Sélectionnez **Activer la publicité** pour permettre l'envoi de publicités périodiques sur le routeur et la réponse aux sollicitations du routeur pour l'interface virtuelle sélectionnée.

Spécifiez les intervalles de vie maximum, minimum et de durée de vie du routeur.

- **Intervalle**maximal : Durée maximale (en secondes) autorisée entre l'envoi périodique de publicités de routeur multidiffusion non sollicitées.
- **Intervalle min** : Temps minimum (en secondes) autorisé entre l'envoi d'annonces périodiques non sollicitées de routeurs multidiffusion.
- Durée de**vie du routeur : durée**(en secondes) pendant laquelle le routeur est considéré comme valide par les hôtes. 0 indique que le routeur ne peut pas être utilisé comme routeur par défaut

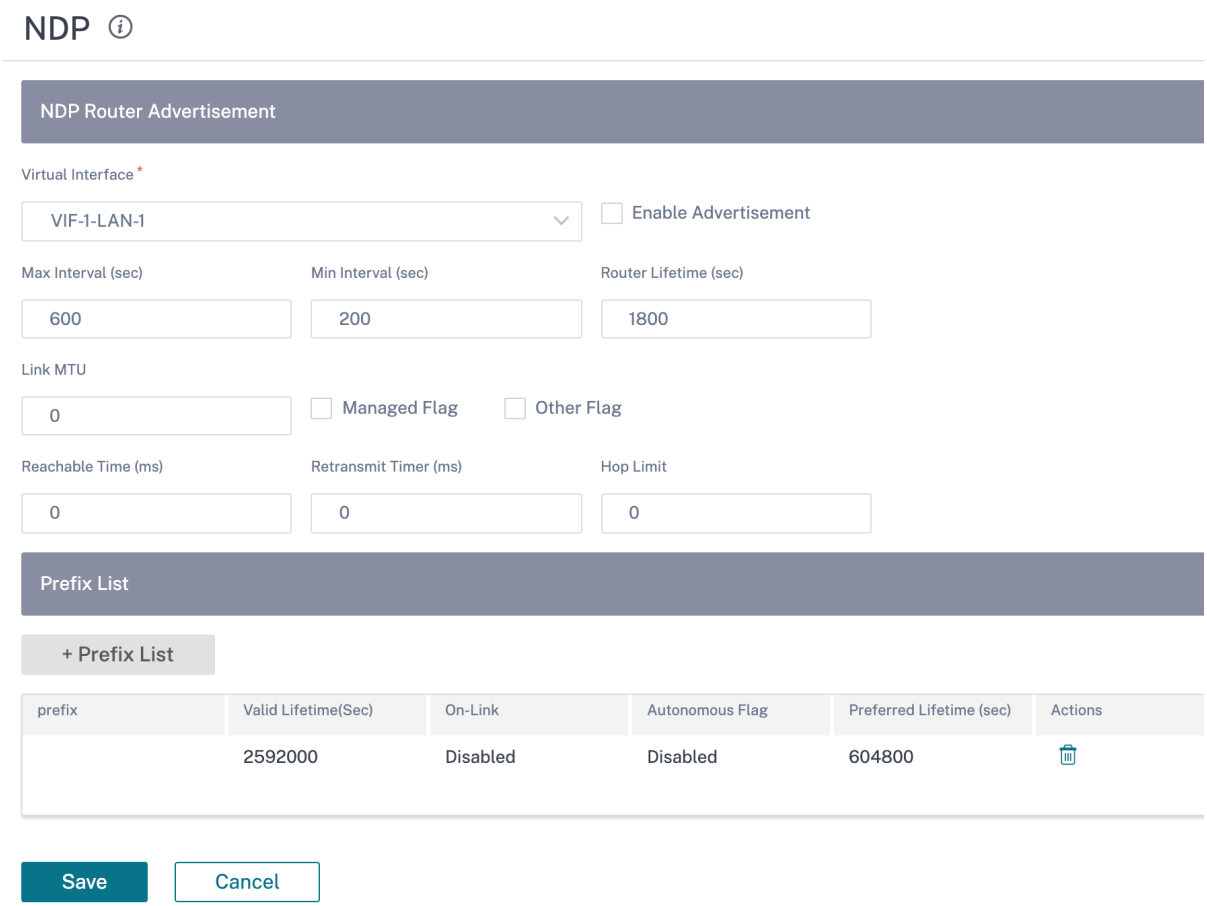
Sélectionnez **Managed Flag** si les adresses IP sont disponibles via le protocole DHCPv6. Sélectionnez **Autre indicateur** si les informations de configuration (autres que les adresses IP) sont disponibles via le protocole DHCPv6.

Spécifiez les valeurs suivantes pour l'interface sélectionnée.

- **Link MTU** : Unité de transmission maximale (MTU) recommandée pour l'interface.
- **Temps d'accès** : le temps (en millisecondes) pendant lequel le protocole NDP reste à l'état **Reachable** .
- **Minuterie de retransmission** : Temps (en millisecondes) entre la retransmission des messages de sollicitation de voisin lors de la résolution d'une adresse IP ou de l'exploration d'un voisin.
- **Limite de saut** : nombre maximal de sauts à inclure dans la publicité du routeur.

Cliquez sur +Liste des préfixes et entrez les valeurs suivantes :

- **Préfixe** : longueur du préfixe et du préfixe dans la notation CIDR (Classless Inter-Domain Routing).
- Durée de**vie valide : Durée**en secondes jusqu'à laquelle le préfixe est valide. -1 représente l'infini, ce qui signifie que le préfixe reste pour toujours.
- **On-link** : lorsqu'il est sélectionné, le préfixe est considéré comme local pour le réseau.
- **Indicateur autonome** : lorsqu'il est activé, le préfixe est utilisé par la configuration automatique d'adresse sans état (SLAAC) de l'hôte pour générer l'adresse IP.
- Durée de**vie du préfixe : Durée**(en secondes) jusqu'à laquelle le préfixe est considéré comme préféré.



Chemins virtuels

October 21, 2022

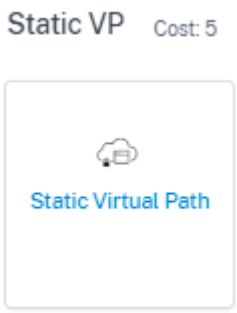
Un chemin virtuel est un lien logique entre deux liaisons WAN. Il comprend un ensemble de chemins WAN combinés pour fournir une communication de niveau de service élevé entre deux nœuds SD-WAN. Cela se fait en mesurant et en s'adaptant constamment à l'évolution de la demande des applications et des conditions WAN. Les appliances SD-WAN mesurent le réseau par chemin. Un chemin virtuel peut être statique (existe toujours) ou dynamique (existe uniquement lorsque le trafic entre deux appliances SD-WAN atteint un seuil configuré).

Chemins virtuels statiques

Les paramètres de chemin virtuel sont hérités des paramètres de chemin automatique de liaison WAN global. Vous pouvez remplacer ces configurations et ajouter ou supprimer le chemin d'accès du membre. Vous pouvez également filtrer les chemins virtuels en fonction du site et du profil QoS appliqué.

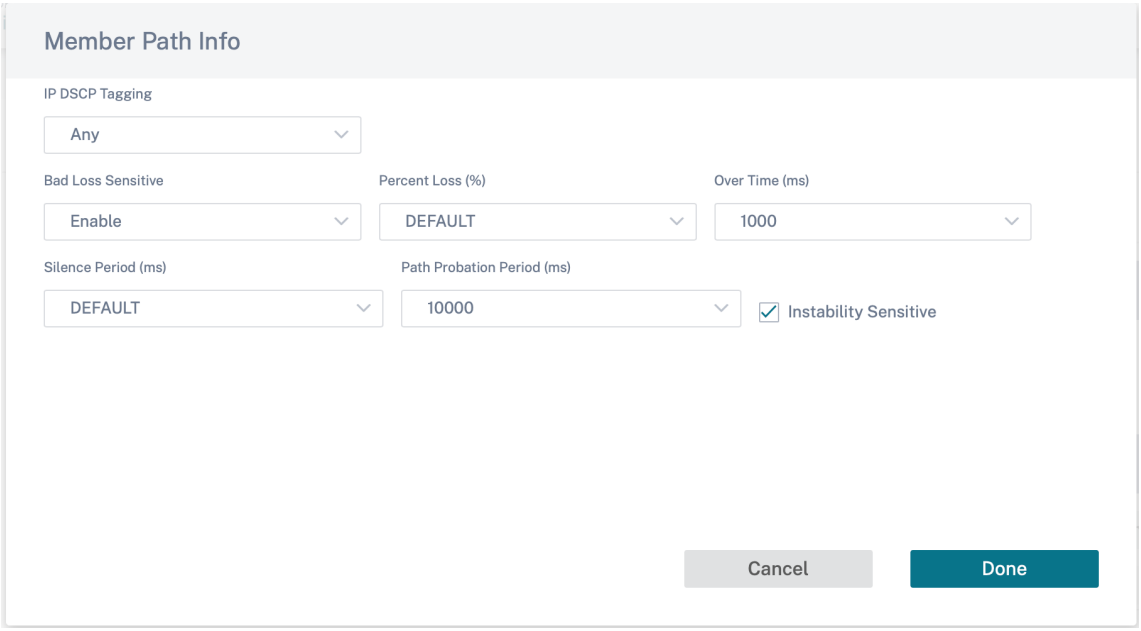
Spécifiez une adresse IP de suivi pour la liaison WAN qui peut être pingée pour déterminer l'état de la liaison WAN. Vous pouvez également spécifier une adresse IP de suivi inverse pour le chemin inverse qui peut être pingé pour déterminer l'état du chemin inverse.

Pour configurer des chemins virtuels statiques, à partir du niveau du site, accédez à **Configuration** > **Paramètres avancés** > **Chemins virtuels > Cheminsvirtuels statiques**.



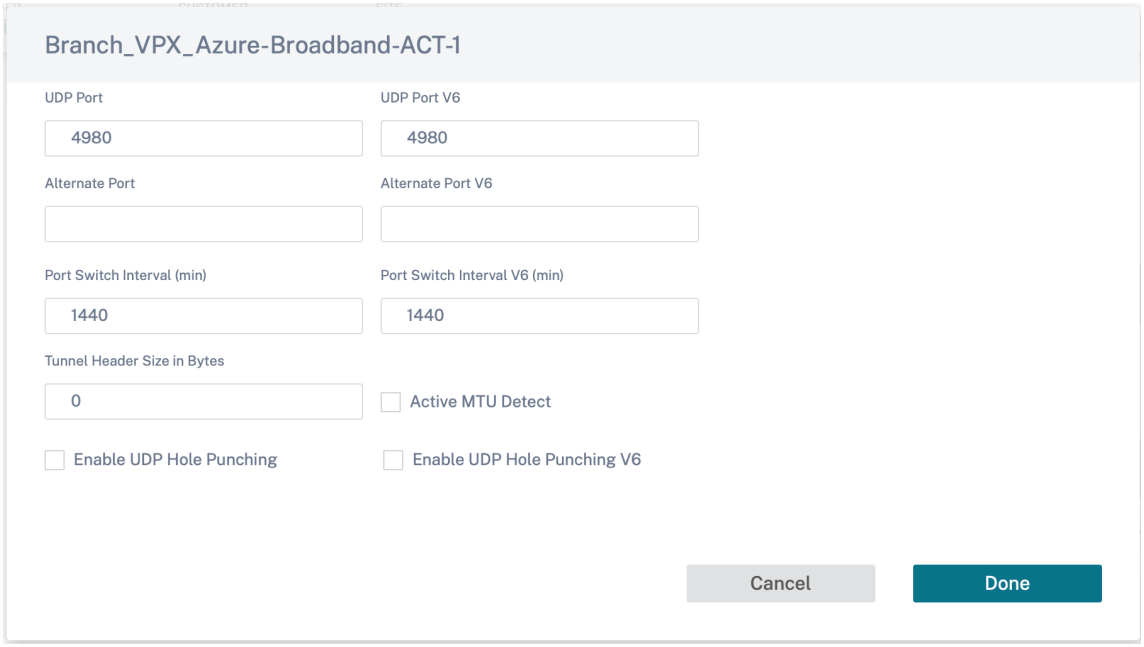
Les chemins des membres actifs sont répertoriés dans la section **Chemins des membres actifs**, vous pouvez consulter ou modifier les paramètres du chemin des membres.

- **Balisage IP DSCP** : balise pour l'en-tête IP externe de la trame du protocole VPCP (Virtual Path Control Protocol).
- **Sensible aux pertes** : si cette option est activée, un chemin peut être marqué comme MAUVAIS en raison d'une perte et entraîner une pénalité de latence sur le score du chemin. Définissez le pourcentage de perte sur le temps nécessaire pour marquer le chemin comme BAD. Désactivez cette option si la perte de bande passante est intolérable.
- **Pourcentage de perte** : si la perte de paquets dépasse le pourcentage défini au cours de la période configurée, l'état GOOD Path passe à BAD.
- **Au fil du temps** : si la perte de paquets dépasse le pourcentage défini pendant cette période configurée, l'état du chemin est marqué comme MAUVAIS.
- **Période de silence** : l'état du chemin passe de BON à MAUVAIS lorsqu'aucun paquet n'est reçu dans le délai spécifié.
- **Période de probation du parcours** : période d'attente avant de changer l'état du chemin de MAUVAIS à BON.
- **Sensible à l'instabilité** : les pénalités de latence dues à l'état BAD et à d'autres pics de latence sont prises en compte



Les détails du lien WAN pour les chemins d'accès actifs sélectionnés sont répertoriés, vous pouvez modifier les paramètres selon vos besoins. Les paramètres du **port UDP** peuvent être configurés pour IPv4 et IPv6.

- **Port UDP** : port utilisé pour le transfert de paquets LAN vers WAN et WAN vers LAN. Vous pouvez également spécifier.
- **Port alternatif : port**UDP alternatif à utiliser lorsque la commutation de port UDP est activée.
- **Intervalle entre les commutateurs de port** : intervalle, en minutes, pendant lequel la liaison WAN alterne son port UDP.
- **Taille de l'en-tête du tunnel en octets** : taille de l'en-tête du tunnel, en octets, le cas échéant.
- **Détection active de la MTU** : Les chemins LAN vers WAN pour les chemins virtuels dynamiques sont activement sondés pour détecter la MTU.
- **Activer la perforation UDP** : le MCN facilite la connectivité UDP entre les sites clients compatibles protégés par la technologie NAT.

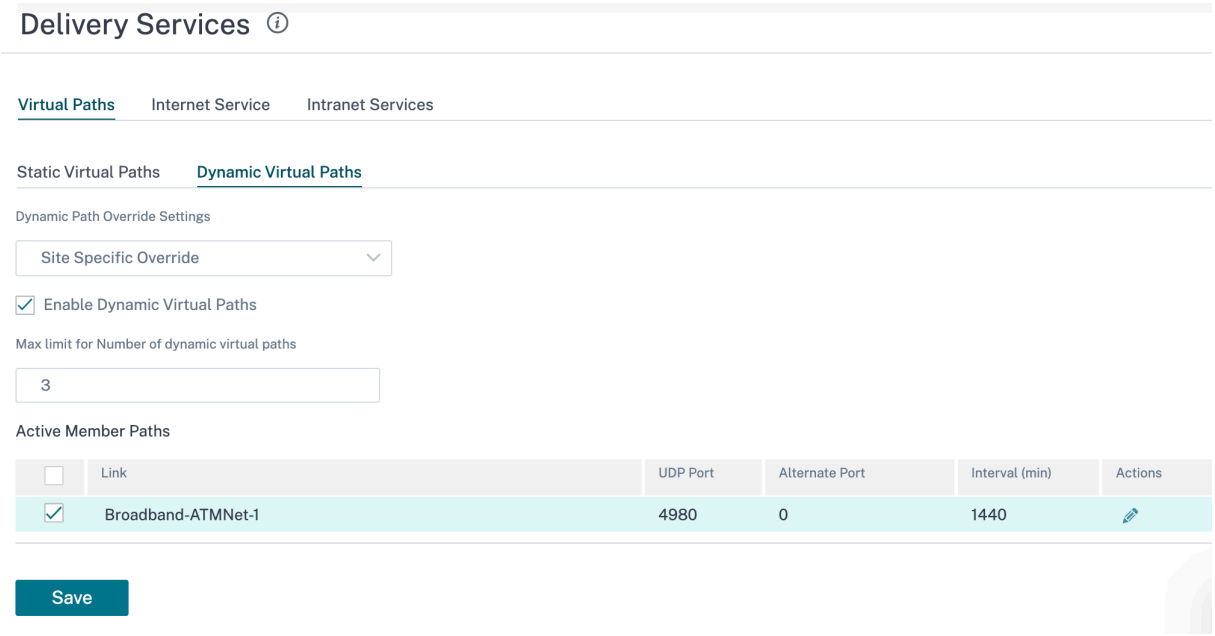


Chemins virtuels dynamiques

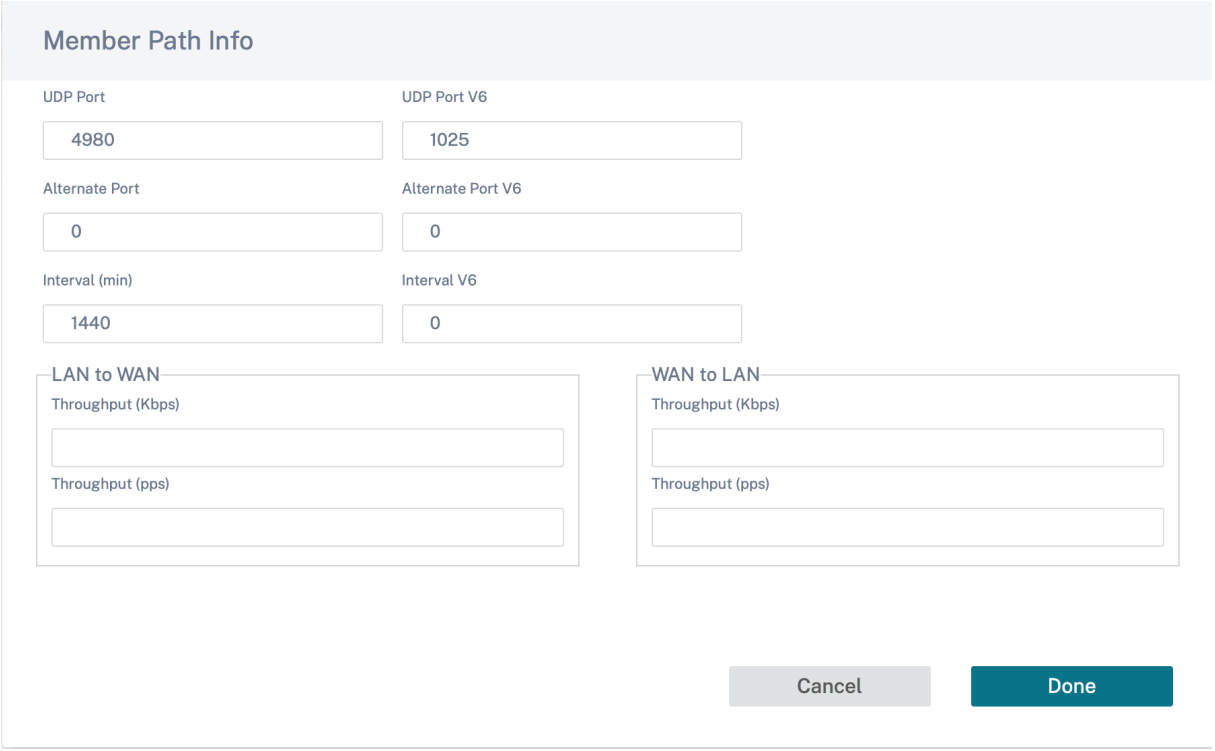
Avec la demande de VoIP et de visioconférence, le trafic entre les bureaux a augmenté. La configuration de connexions maillées complètes via des centres de données prend du temps et est inefficace. Avec Citrix SD-WAN, vous pouvez créer automatiquement des chemins entre les bureaux à la demande à l'aide de la fonctionnalité Chemin virtuel dynamique. La session utilise initialement un chemin fixe existant. Lorsque la bande passante et le seuil de temps sont atteints, un nouveau chemin est créé dynamiquement si ce nouveau chemin présente de meilleures caractéristiques de performance que le chemin fixe. Le trafic de session est transmis par le nouveau chemin d'accès, ce qui entraîne une utilisation efficace des ressources. Les chemins virtuels dynamiques n'existent que lorsqu'ils sont nécessaires et réduisent la quantité de trafic transmis vers et en provenance du centre de données.

Pour configurer des chemins virtuels dynamiques, à partir du niveau du site, accédez à **Configuration** > **Paramètres avancés** > **Chemins virtuels > Cheminsvirtuels dynamiques**.

Sélectionnez **Ignorer les valeurs par défaut globales** pour remplacer les paramètres de chemin virtuel hérités des paramètres de chemin automatique du lien WAN global. Sélectionnez **Activer les chemins virtuels dynamiques** pour autoriser les chemins virtuels dynamiques entre ce site et d'autres sites connectés via un nœud intermédiaire. Définissez les chemins virtuels dynamiques maximaux autorisés pour le site.



Définissez le port UDP et le seuil de chemin virtuel dynamique. Spécifiez le seuil de débit, en kbps ou en paquets par seconde, sur le site intermédiaire sur lequel les chemins virtuels dynamiques sont déclenchés sur LAN vers WAN ou WAN vers LAN.



Routage dynamique

October 21, 2022

Après la configuration et le déploiement des appliances SD-WAN dans le réseau et une fois les connexions établies, il est important de s'assurer que le trafic est correctement redirigé via le réseau SD-WAN superposé. Vous pouvez vérifier la redirection du trafic à l'aide des outils de diagnostic ping et traceroute. Si les tests ping et traceroute indiquent que la connectivité est établie via les chemins de sous-couche, la redirection du trafic peut être obtenue à l'aide des protocoles de routage dynamique suivants.

- **Open Shortest Path First (OSPF)** : Il s'agit d'un protocole de passerelle intérieure, utilisé pour rediriger le trafic au sein d'un système autonome, comme le réseau d'entreprise. L'OSPF utilise un algorithme de routage par état de liaison pour détecter les modifications de la topologie du réseau et rediriger les paquets en calculant d'abord le chemin le plus court pour chaque itinéraire. Utilisez ce protocole pour rediriger le trafic MPLS. Pour plus d'informations, consultez la section **OSPF** .
- **Border Gateway Protocol (BGP)** : Il s'agit d'un protocole de passerelle externe conçu pour rediriger le trafic et les informations d'accessibilité entre différents systèmes autonomes sur Internet. Il est capable de prendre des décisions de routage en fonction des chemins déterminés par les FAI. Utilisez ce protocole pour rediriger le trafic Internet. Pour plus d'informations, voir la section **Configurer le BGP** .

Auparavant, la fonctionnalité de routage dynamique n'était disponible que pour un seul identifiant de routeur. Vous avez pu configurer un identifiant de routeur unique soit globalement pour tous les domaines de routage configurés (un pour OSPF et BGP), soit ne fournir aucun identifiant de routeur. À partir de la version 11.3.1 de Citrix SD-WAN, vous pouvez non seulement configurer un ID de routeur pour l'ensemble du protocole, mais également configurer un ID de routeur pour chaque domaine de routage. Avec cette amélioration, vous pouvez activer le routage dynamique stable sur plusieurs instances avec différents ID de routeur convergeant de manière stable.

Si vous configurez un ID de routeur pour un domaine de routage spécifique, l'ID de routeur spécifique remplace le domaine de routage au niveau du protocole.

OSPF

Pour configurer OSFF, accédez à **Configuration > Paramètres avancés > Routage dynamique > OSPF**.

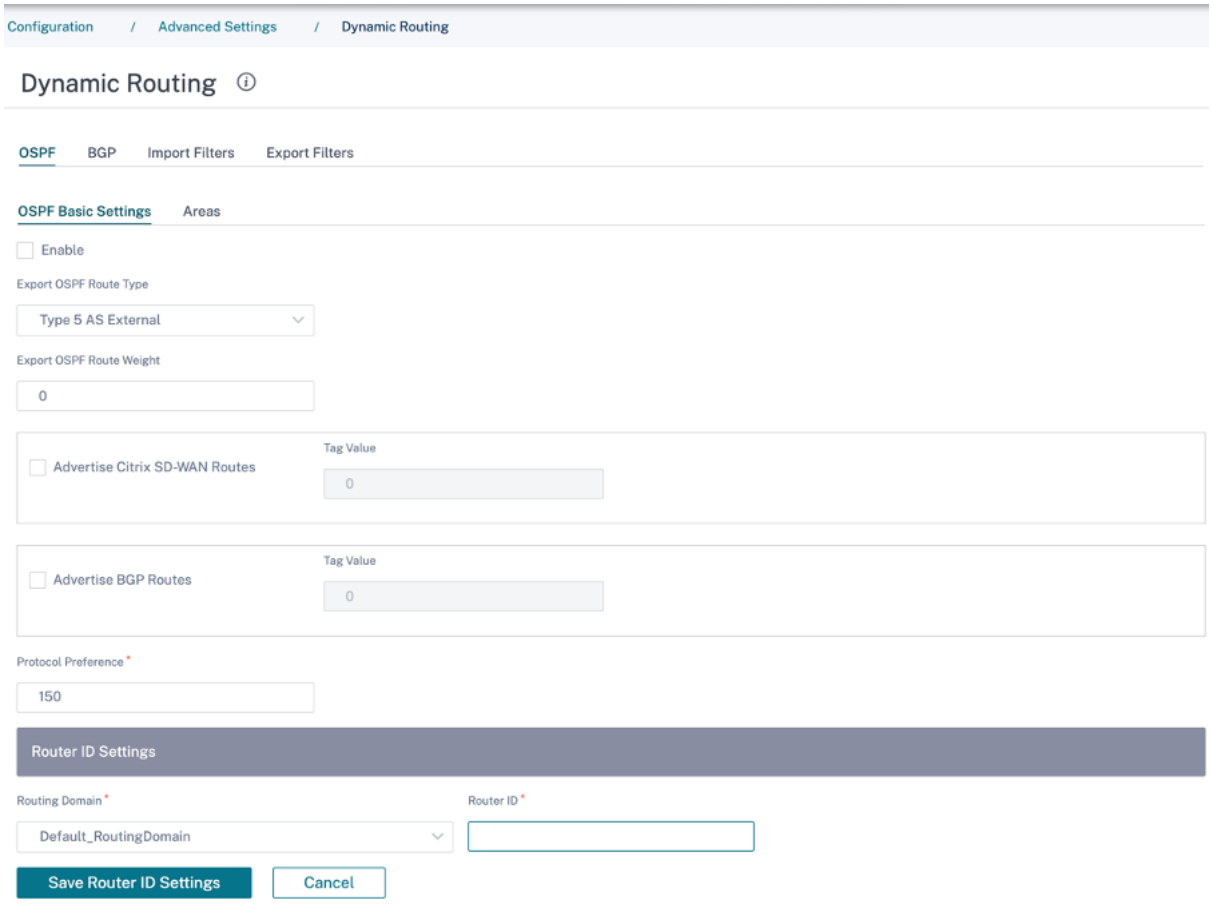
Paramètres de base OSPF

Voici les paramètres à configurer :

- **Activer** : autorisez le protocole de routage OSPF de l'appliance SD-WAN à commencer à échanger des paquets Hello entre des routeurs voisins.
- **ID du routeur** : adresse IPv4 utilisée pour les publicités OSPF. Ce champ est facultatif. Si elle n'est pas spécifiée, l'adresse IPv4 virtuelle la plus basse des interfaces virtuelles participant au routage est choisie. Pour l'interface IPv6, il est obligatoire de spécifier l'ID du routeur au format IPv4. Par exemple, 1.1.1.1.

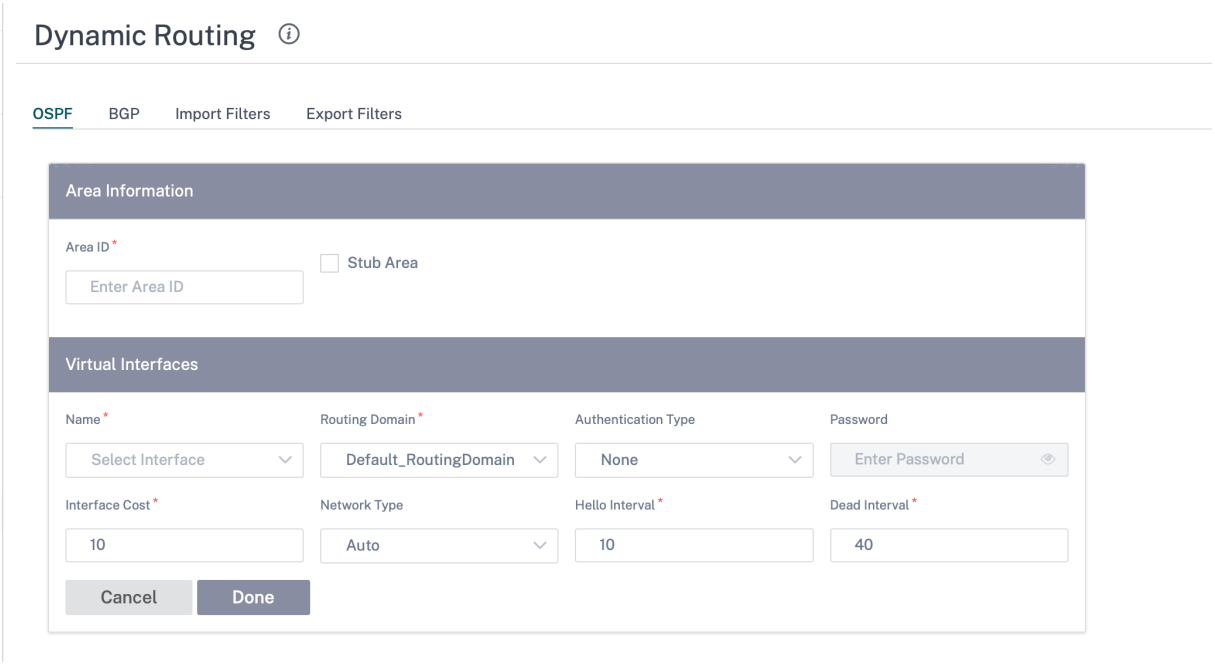
  > **Remarque**
  >
  > - La configuration de l'ID du routeur est facultative pour un réseau IPv4. Mais pour un réseau IPv6, la configuration de l'ID du routeur est obligatoire. L'ID du routeur pour un réseau IPv6 doit être configuré dans le même format IPv4 (notation 32 bits).
  >   * Vous devez créer un appairage IPv4 et IPv6 distinct vers le même routeur (le cas échéant) à des fins d'apprentissage et de publicité.

- **Exporter le type de route OSPF** : annoncez l'itinéraire SD-WAN aux voisins OSPF en tant que route intra-zone de type 1 ou route externe de type 5.
- **Exporter le poids de l'itinéraire OSPF** : Le coût annoncé aux voisins OSPF est le coût de l'itinéraire initial et le poids configuré ici.
- **Publicité des itinéraires SD-WAN** : Pour annoncer des itinéraires SD-WAN vers les éléments du réseau homologue.
- **Publicité des routes BGP** : pour permettre la redistribution des routes BGP dans le domaine OSPF.



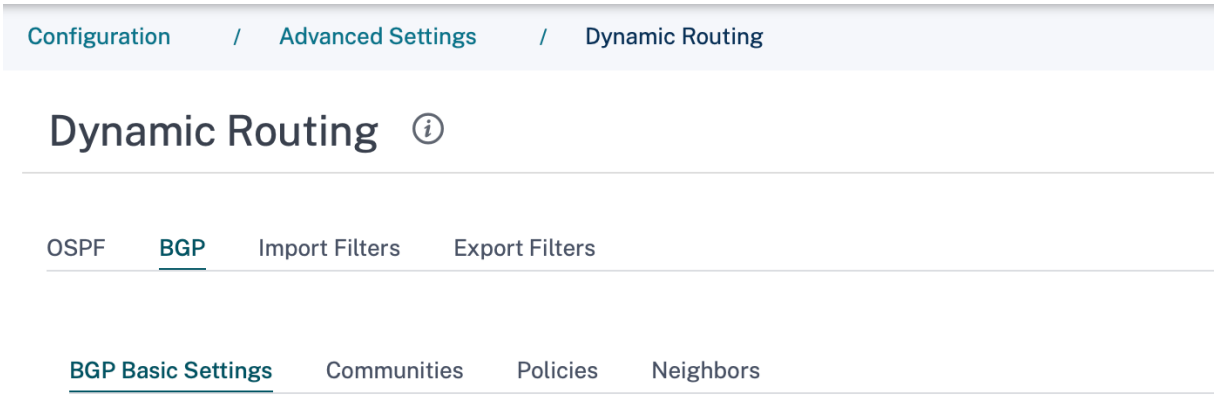
Zones

Cliquez sur **+ Zone** et fournissez l'ID de zone du réseau à partir duquel OSPF apprendra les itinéraires et annoncera les itinéraires. La zone du talon garantit que cette zone ne recevra pas de publicité sur les itinéraires provenant de l'extérieur du système autonome désigné. Configurez les paramètres de l'interface virtuelle.



BGP

Pour configurer BGP, accédez à **Configuration > Paramètres avancés > Routage dynamique > BGP**.



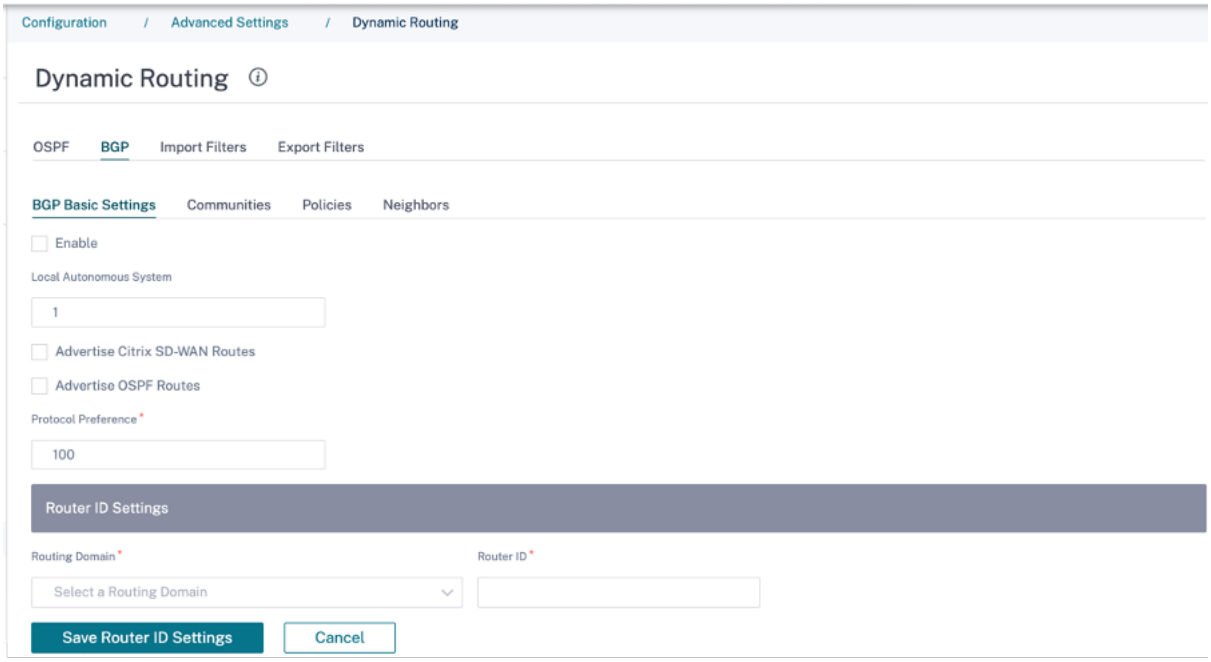
Paramètres de base BGP

Les paramètres à configurer sont les suivants :

- **Activer** : autorisez le protocole de routage BGP de l'appliance SD-WAN à commencer à envoyer un message ouvert dans le cadre de l'appairage BGP.
- **ID du routeur** : adresse IPv4 utilisée pour les publicités BGP. Si l'ID du routeur n'est pas spécifié, l'adresse IPv4 virtuelle la plus basse des interfaces virtuelles participant au routage est choisie.

> **Remarque**
>
> – La configuration de l'ID du routeur est facultative pour un réseau IPv4. Mais pour un réseau IPv6, la configuration de l'ID du routeur est obligatoire. L'ID du routeur pour un réseau IPv6 doit être configuré dans le même format IPv4 (notation 32 bits).
>
> * Vous devez créer un appairage IPv4 et IPv6 distinct vers le même routeur (le cas échéant) à des fins d'apprentissage et de publicité.

- **Système autonome local** : numéro du système autonome dans lequel s'exécute le protocole BGP.
- **Publicité des itinéraires SD-WAN** : Pour annoncer des itinéraires SD-WAN vers les éléments du réseau homologue.
- **Publicité des routes OSPF** : Pour permettre la redistribution des routes OSPF dans le domaine BGP.

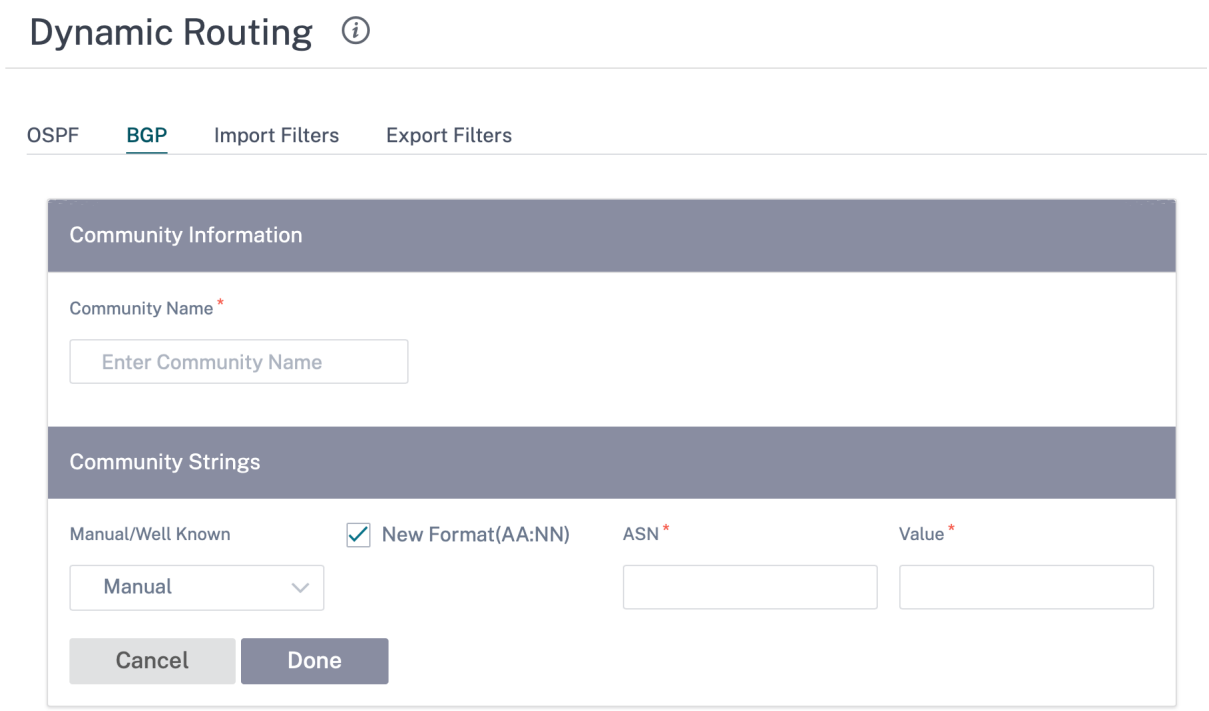


Communautés

Cliquez sur **+ Communauté** pour ajouter une communauté. Collection de communautés BGP qui peuvent être utilisées pour le filtrage des itinéraires. La liste des communautés peut également être utilisée pour définir ou modifier les communautés d'un itinéraire correspondant.

Pour chaque politique, les utilisateurs peuvent configurer plusieurs chaînes de communauté, l'attribut AS-PATH-PREPEND et l'attribut **MED** . Les utilisateurs peuvent configurer jusqu'à 10 attributs pour chaque stratégie.

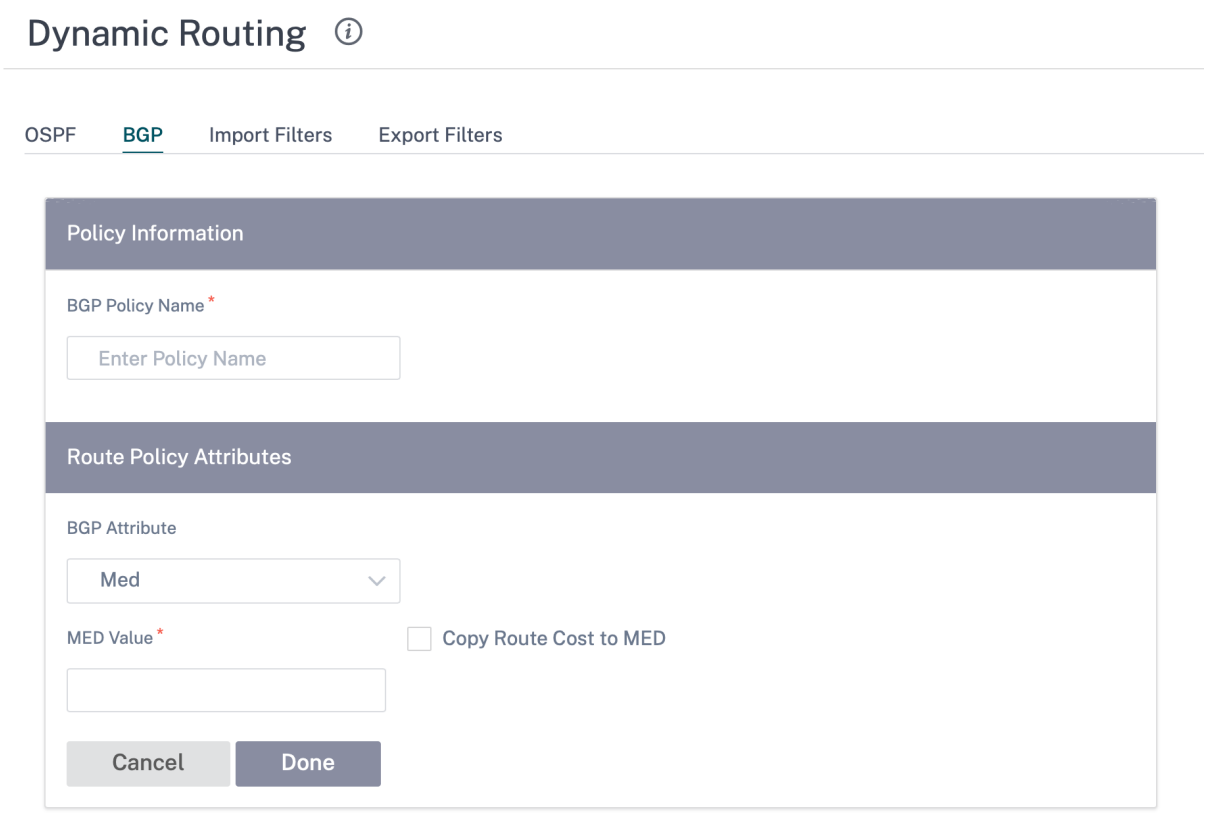
Spécifiez le nom de la communauté et entrez une chaîne de communauté à publier.



- **Nom de la communauté** : Entrez le nom de la communauté.
- **Manuel/Bien connu** : configurez la communauté BGP manuellement ou sélectionnez une communauté BGP standard bien connue dans la liste.
- **Nouveau format (AA:NN)** : Cochez la case pour utiliser le nouveau format pour configurer la communauté BGP.
- **ASN** : les 16 premiers chiffres de la communauté BGP lors de l'utilisation du nouveau format de configuration.
- **Valeur** : Entrez la valeur de la communauté BGP.

Stratégies

Collection d'attributs BGP qui peuvent être utilisés pour définir ou modifier les attributs d'itinéraire pour chaque homologue BGP. Créez des stratégies BGP à appliquer de manière sélective à un ensemble de réseaux par voisin, dans les deux sens (importation ou exportation). Une appliance SD-WAN prend en charge huit stratégies par site, avec jusqu'à huit objets réseau (ou huit réseaux) associés à une stratégie.

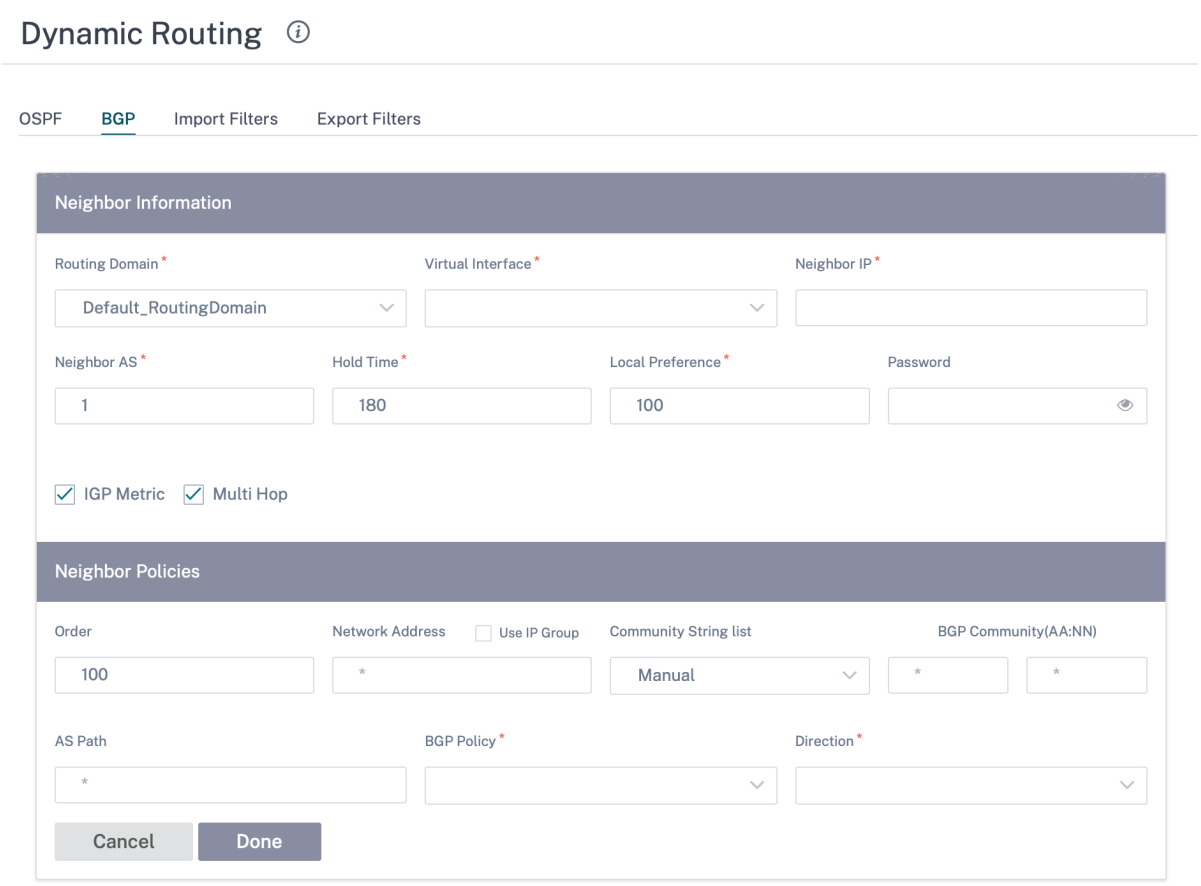


- **Nom de la stratégie BGP** : Entrez le nom de la stratégie BGP.
- **Attributs BGP** : Sélectionnez les attributs BGP dans la liste et fournissez les informations nécessaires.

Voisins

Les voisins sont tous les routeurs homologues BGP configurés qui sont vérifiés pour trouver les chemins les plus courts pour le routage. Tous les voisins doivent faire partie du même système autonome.

Cliquez sur **+ Voisin** pour ajouter une politique BGP configurée pour les routeurs voisins. Vous pouvez spécifier la direction pour indiquer si cette stratégie est appliquée aux itinéraires entrants ou sortants.



Filtrage d'itinéraire

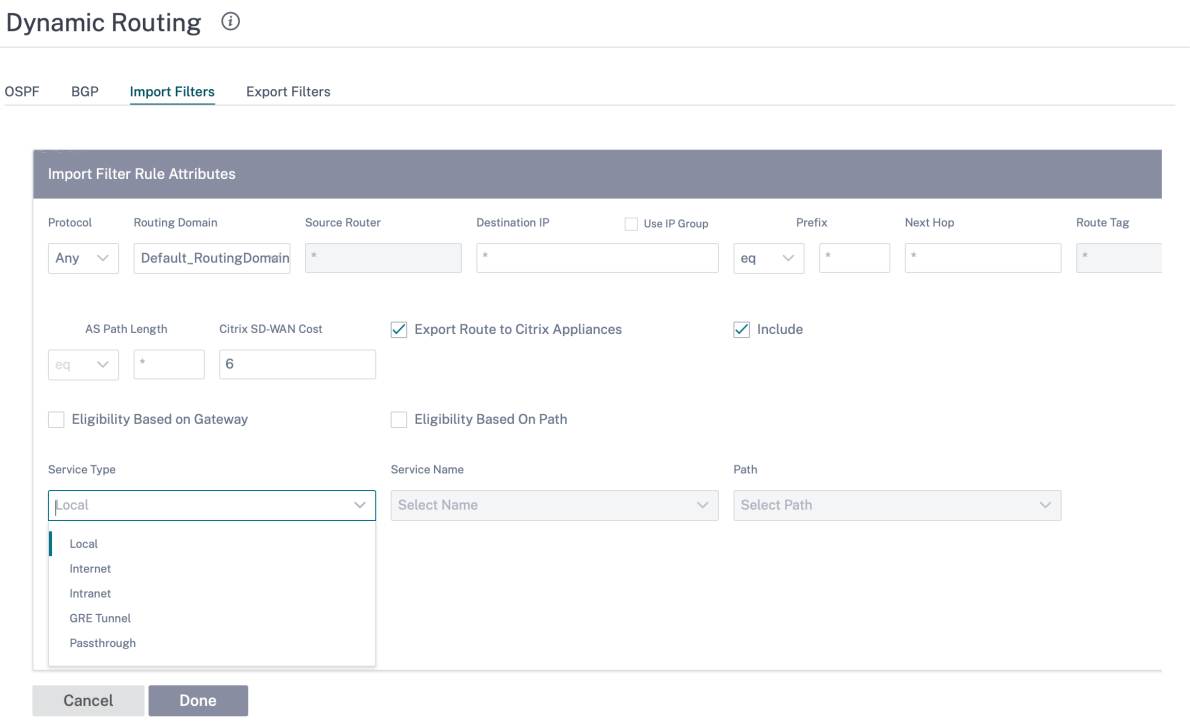
Pour les réseaux sur lesquels l'apprentissage des itinéraires est activé, Citrix SD-WAN Orchestrator permet de mieux contrôler quelles routes SD-WAN sont annoncées aux voisins de routage et quelles routes sont reçues des voisins de routage, plutôt que de faire de la publicité et d'accepter toutes les routes ou aucune route.

Filtres d'importation

Les filtres d'importation sont utilisés pour accepter ou ne pas accepter les itinéraires reçus à l'aide de voisins OSPF et BGP basés sur des critères de correspondance spécifiques. Les règles de filtre d'importation sont les règles qui doivent être respectées avant d'importer des itinéraires dynamiques dans la base de données d'itinéraires SD-WAN. Aucune route n'est importée par défaut.

Vous pouvez configurer des filtres pour affiner la manière dont se déroule l'apprentissage par route.

Cliquez sur **+ Importer une règle**.



Utilisez les critères suivants pour construire chaque filtre d'exportation que vous souhaitez créer.

Critères de	Description	Valeur
Protocol	Protocole de routage à l'aide duquel un itinéraire est appris. Sélectionnez le protocole dans la liste déroulante.	N'importe lequel, OSPF, BGP
Domaine de routage	Entrez le domaine de routage dans la liste déroulante.	• Nom de domaine de routage
Routeur source	Adresse IP du routeur source, elle est applicable uniquement pour iBGP	• Adresse IP
IP destination	L'adresse IP et le masque de sous-réseau de la destination d'un itinéraire	• Adresse IP
Utiliser un groupe IP	Cochez la case **Utiliser le groupe IP** selon vos besoins.	• Groupe IP

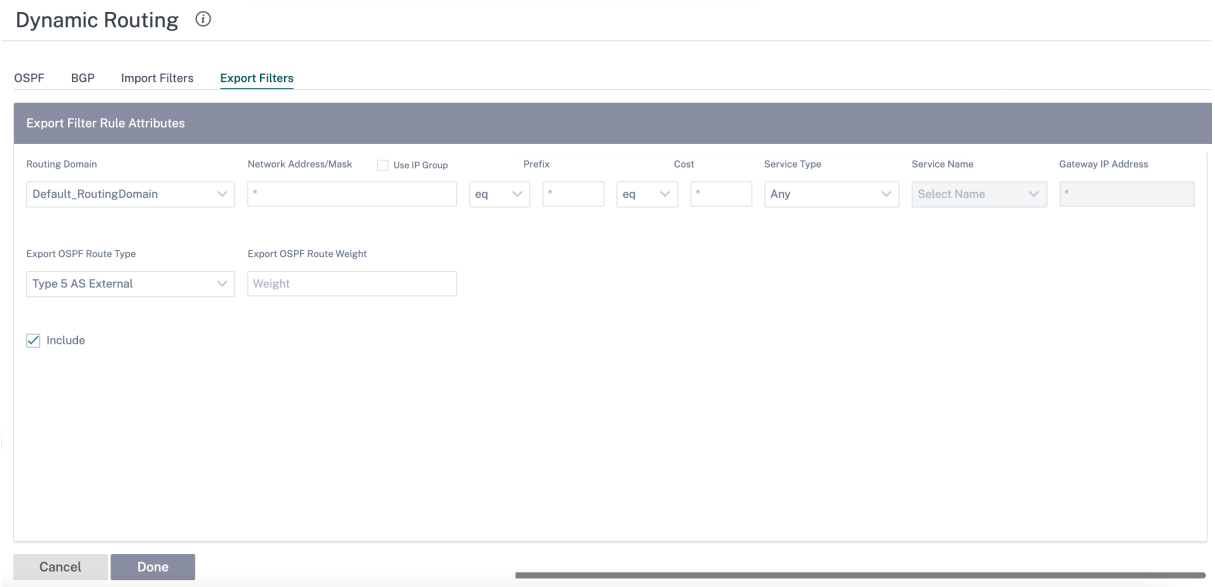
Critères de	Description	Valeur
Préfixe	Pour faire correspondre les itinéraires par préfixe, choisissez un prédicat de correspondance dans le menu et entrez un préfixe d'itinéraire dans le champ adjacent	• eq: Equal to, - lt: Less than, - le: Less than or equal to, - gt: Greater than, - ge: Greater than or equal to
Prochain saut	L'adresse IP du prochain saut	• Adresse IP
Balise d'itinéraire	La balise Route OSPF correspondant au filtre. Les balises de routage OSPF empêchent les boucles de routage lors de la redistribution mutuelle entre OSPF et d'autres protocoles	Valeur numérique
Coût	Coût d'itinéraire utilisé pour faire correspondre les routes OSPF pour l'importation	Valeur numérique
Longueur du chemin AS	Longueur du chemin AS utilisée pour faire correspondre les routes BGP pour l'importation	Valeur numérique
Exporter l'itinéraire vers les appliances Citrix	Cochez la case pour activer ce filtre. Sinon, le filtre est ignoré	Aucun
Inclure	Activez la case à cocher Inclure les itinéraires qui correspondent à ce filtre. Sinon, les routes correspondantes sont ignorées	Aucun
Éligibilité basée sur Gateway	Cochez cette case et indiquez le **type de service**, le **nom du service** et le **chemin** dans la liste déroulante.	Type de service (local, Internet, intranet, tunnel GRE, relais), nom du service et chemin
Éligibilité basée sur le parcours	Cochez cette case et indiquez le **type de service**, le **nom du service** et le **chemin** dans la liste déroulante.	Type de service (local, Internet, intranet, tunnel GRE, relais), nom du service et chemin

Cliquez sur **OK** pour enregistrer les paramètres.

Filtres d'exportation

Les filtres d'exportation sont utilisés pour inclure ou exclure des itinéraires pour la publicité à l'aide des protocoles OSPF et BGP basés sur des critères de correspondance spécifiques. Les règles de filtrage d'exportation sont les règles qui doivent être respectées lors de la publicité de routes SD-WAN via des protocoles de routage dynamiques. Toutes les routes sont annoncées aux pairs par défaut.

Cliquez sur **+ Exporter la règle**.



Utilisez les critères suivants pour construire chaque filtre d'exportation que vous souhaitez créer.

Critères de	Description	Valeur
Domaine de routage	Sélectionnez le domaine de routage dans la liste déroulante.	Domaine de routage
Adresse/masque réseau	Entrez l'**adresse IP** et le masque de sous-réseau de l'objet réseau configuré qui décrit le réseau de l'itinéraire	• Adresse IP
Utiliser un groupe IP	Cochez la case si nécessaire et entrez le groupe IP dans la liste déroulante.	• Groupe IP

Critères de	Description	Valeur
Préfixe	Pour faire correspondre les itinéraires par préfixe, choisissez un prédicat de correspondance dans le menu et entrez un préfixe d'itinéraire dans le champ adjacent	• eq: Equal to, - lt: Less than, - le: Less than or equal to, - gt: Greater than, - ge: Greater than or equal to
Coût	Méthode (prédicat) et coût d' itinéraire SD-WAN utilisés pour restreindre la sélection des itinéraires exportés	Valeur numérique
Type de service	Sélectionnez les types de service affectés aux itinéraires correspondants dans une liste de services Citrix SD-WAN	Tout, Local, Chemin Virtuel, Internet, Intranet, LAN GRE Tunnel, LAN IPSec Tunnel
Nom du site/service	Pour Intranet, LAN GRE Tunnel et LAN IPSec Tunnel, spécifiez le nom du type de service configuré à utiliser	Chaîne de texte
Adresse IP de la passerelle	Si vous choisissez LAN GRE Tunnel comme Type de service, entrez l'IP de la Gateway pour le tunnel	Adresse IP
Exporter le type de route OSP	Annoncez la route Citrix SD-WAN aux voisins OSPF comme une route intra-zone de type 1 ou une route externe de type 5. L'itinéraire par défaut est toujours annoncé comme étant de type 5 : route externe vers les zones normales et route récapitulative de type 3 vers les zones tronquées.	Type d'itinéraire
Exporter le poids de route OSP	Lors de l'exportation de routes Citrix SD-WAN vers OSPF, et le poids du coût Citrix SD-WAN de chaque itinéraire en tant que coût total.	Poids

Critères de	Description	Valeur
Inclure	Activez la case à cocher Inclure les itinéraires qui correspondent à ce filtre. Sinon, les routes correspondantes sont ignorées	Aucun

Le filtrage d'itinéraire est implémenté sur les routes LAN et les routes de chemin virtuel dans un réseau SD-WAN (datacenter ou branche) et est annoncé sur un réseau non-SD-WAN via BGP et OSPF.

Vous pouvez configurer jusqu'à 512 filtres d'exportation et 512 filtres d'importation. Il s'agit de la limite globale, et non de la limite de domaine de routage.

Traduction d'adresses réseau

October 21, 2022

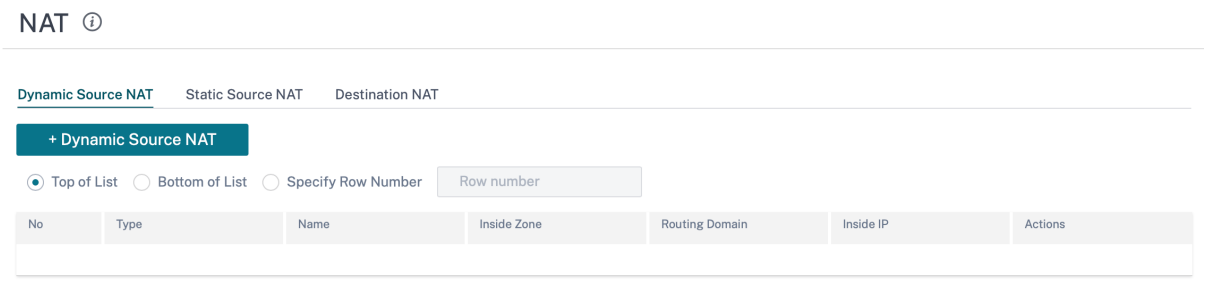
La traduction d'adresses réseau (NAT) sur l'appliance SD-WAN effectue la conservation des adresses IP afin de préserver le nombre limité d'adresses IP enregistrées. Il traduit les adresses privées du réseau interne en une adresse publique légale et connecte votre réseau SD-WAN privé à l'Internet public. L'adresse IP publique est utilisée pour la communication sur Internet. NAT assure également une sécurité supplémentaire en annonçant une seule adresse pour l'ensemble du réseau sur Internet, cachant l'ensemble du réseau interne.

Vous pouvez configurer les types de NAT suivants :

- NAT source dynamique
- NAT statique
- NAT de destination

> **Remarque**
>
> La fonctionnalité NAT ne peut être configurée qu'au niveau du site. Il n'y a pas de configuration globale (modèles) pour NAT.

Pour configurer la NAT pour un site à l'aide du service Citrix SD-WAN Orchestrator, à partir du niveau du site, accédez à **Configuration > Paramètres avancés > NAT**.



NAT entrant et sortant

La direction d'une connexion peut être de l'intérieur vers l'extérieur ou de l'extérieur vers l'intérieur. Lorsqu'une règle NAT est créée, vous pouvez définir la direction à l'aide de la case **à cocher On Receive** . Lorsque la case est cochée, la direction est configurée comme **entrante** et lorsque la case est décochée, la direction est configurée comme **sortante**.

- **Entrant** : l'adresse source est traduite pour les paquets reçus sur le service. L'adresse de destination est traduite pour les paquets transmis sur le service. Par exemple, service Internet au service LAN —Pour les paquets reçus (Internet vers LAN), l'adresse IP source est traduite. Pour les paquets transmis (LAN vers Internet), l'adresse IP de destination est traduite.
- **Sortant** : l'adresse de destination est traduite pour les paquets reçus sur le service. L'adresse source est traduite pour les paquets transmis sur le service. Par exemple, le service LAN au service Internet —pour les paquets transmis (LAN à Internet), l'adresse IP source est traduite. Pour les paquets reçus (Internet vers LAN), l'adresse IP de destination est traduite.

Dérivation de zone

Les zones de pare-feu source et de destination pour le trafic entrant ou sortant ne doivent pas être identiques. Si les zones de pare-feu source et de destination sont toutes les deux identiques, NAT n'est pas effectué sur le trafic.

Pour le NAT sortant, la zone extérieure est automatiquement dérivée du service. Chaque service sur SD-WAN est associé à une zone par défaut. Par exemple, le service Internet sur un lien Internet approuvé est associé à la zone Internet de confiance. De même, pour un NAT entrant, la zone interne est dérivée du service.

Pour un service de chemin virtuel, la dérivation de la zone NAT ne se produit pas automatiquement, vous devez entrer manuellement la zone intérieure et extérieure. Le NAT est effectué sur le trafic appartenant à ces zones uniquement. Les zones ne peuvent pas être dérivées pour les chemins virtuels car il peut y avoir plusieurs zones dans les sous-réseaux de chemins virtuels.

NAT source dynamique

La**NAT à source dynamique** est un mappage de plusieurs adresses IP privées ou de sous-réseaux au sein du réseau SD-WAN vers une adresse IP publique ou un sous-réseau extérieur au réseau SD-WAN. Il permet à plusieurs hôtes de faire traduire leurs adresses IP source en la même adresse IP publique avec des numéros de port différents. Le NAT restreint par port utilise le même port externe pour toutes les traductions liées à une adresse IP intérieure et une paire de ports. Le trafic provenant de différentes zones et sous-réseaux sur des adresses IP de confiance (internes) dans le segment LAN est envoyé sur une seule adresse IP publique (externe).

> **Remarque :**
>
> Les traductions NAT dynamiques autorisent tout le trafic réciproque pour une session initiée depuis le réseau interne. Pour filtrer ces connexions, ajoutez des politiques de filtrage pour le trafic sortant.

Traduction d'adresses de port

Dynamic NAT effectue la traduction d'adresses de port (PAT) ainsi que la traduction d'adresses IP. Les numéros de port sont utilisés pour distinguer quel trafic appartient à quelle adresse IP. Une seule adresse IP publique est utilisée pour toutes les adresses IP privées internes, mais un numéro de port différent est attribué à chaque adresse IP privée. PAT est un moyen économique d'autoriser plusieurs hôtes à se connecter à Internet à l'aide d'une seule adresse IP publique.

La case à cocher **Symétrique** définit la configuration PAT. Lors de la configuration des règles NAT, si la case est cochée, le NAT symétrique est configuré et, lorsqu'il est désactivé, le NAT à port restreint est configuré dans le back-end.

- **Port Restreint** : Port Restreint NAT utilise le même port externe pour toutes les traductions liées à une paire d'adresses IP internes et de ports. Ce mode est généralement utilisé pour autoriser les applications P2P Internet.
- **Symétrique** : le NAT symétrique utilise le même port externe pour toutes les traductions liées à une adresse IP intérieure, un port intérieur, une adresse IP extérieure et un tuple de port externe. Ce mode est généralement utilisé pour améliorer la sécurité ou augmenter le nombre maximal de sessions NAT.

Transfert de port

Le NAT dynamique avec redirection de port permet au trafic provenant d'un réseau externe d'accéder à des hôtes et à des ports spécifiques sur le réseau interne sans que la session ne soit initiée depuis l'intérieur. Ceci est généralement utilisé pour les hôtes internes tels que les serveurs Web.

Une fois le NAT dynamique configuré, vous pouvez définir les stratégies de transfert de port. Configurez NAT dynamique pour la traduction d'adresses IP et définissez la stratégie de transfert de port pour mapper un port externe à un port intérieur. Le transfert de port NAT dynamique est généralement utilisé pour permettre aux hôtes distants de se connecter à un hôte ou à un serveur sur votre réseau privé.

Configurer le NAT de source dynamique

Pour configurer la NAT dynamique pour un site à l'aide du service Citrix SD-WAN Orchestrator, à partir du niveau du site, accédez à **Configuration > Paramètres avancés > NAT > onglet NAT source dynamique** . Cliquez sur **+ Source dynamique NAT**.

- **Type** : types de services SD-WAN auxquels la politique NAT est appliquée. Pour le NAT statique, les types de services pris en charge sont les services locaux, les chemins virtuels, Internet, l'intranet et les services de domaine d'inter-routage.
- **Domaine de routage** : Sélectionnez le domaine de routage auquel s'applique la traduction sélectionnée.
- **Type d'adresse IP** : Sélectionnez le type d'adresse IPv4 ou IPv6 en fonction de vos préférences.
- **Service de destination** : entrez un nom pour le service qui correspond au type de service.
- **Zone intérieure** : Type de correspondance de zone de pare-feu intérieur à partir de laquelle le paquet doit être pour permettre la traduction.
- Adresse**IP intérieure/préfixe** : adresse IP interne et préfixe qui doivent être traduits si les critères de correspondance sont remplis.
- **IP externe** : adresse IP externe et préfixe vers lesquels l'adresse IP interne est traduite si les critères de correspondance sont remplis. Pour le trafic sortant utilisant les services Internet et Intranet, l'adresse IP de liaison WAN configurée est choisie dynamiquement comme adresse IP externe.
- **Parité de port** : Si cette option est activée, les ports externes pour les connexions NAT conservent la parité (même si le port intérieur est pair, impair si le port extérieur est impair).
- **Bind Responder Route** : garantit que le trafic de réponse est envoyé via le même service que celui sur lequel il est reçu, afin d'éviter un routage asymétrique.
- **Autoriser les données associées** : autorise le trafic lié au flux correspondant à la règle. Par exemple, la redirection ICMP liée au flux spécifique correspondant à la stratégie, s'il y avait un type d'erreur lié au flux.
- **Passthrough IPsec** : autorise la traduction d'une session IPsec (AH/ESP).
- **Passthrough GRE/PPTP** : garantit que le trafic de réponse est envoyé via le même service que celui sur lequel il est reçu, afin d'éviter un routage asymétrique.
- **À la réception** : lorsque cette case est cochée, le NAT entrant est configuré. Lorsque cette option est désactivée, le NAT sortant est configuré.

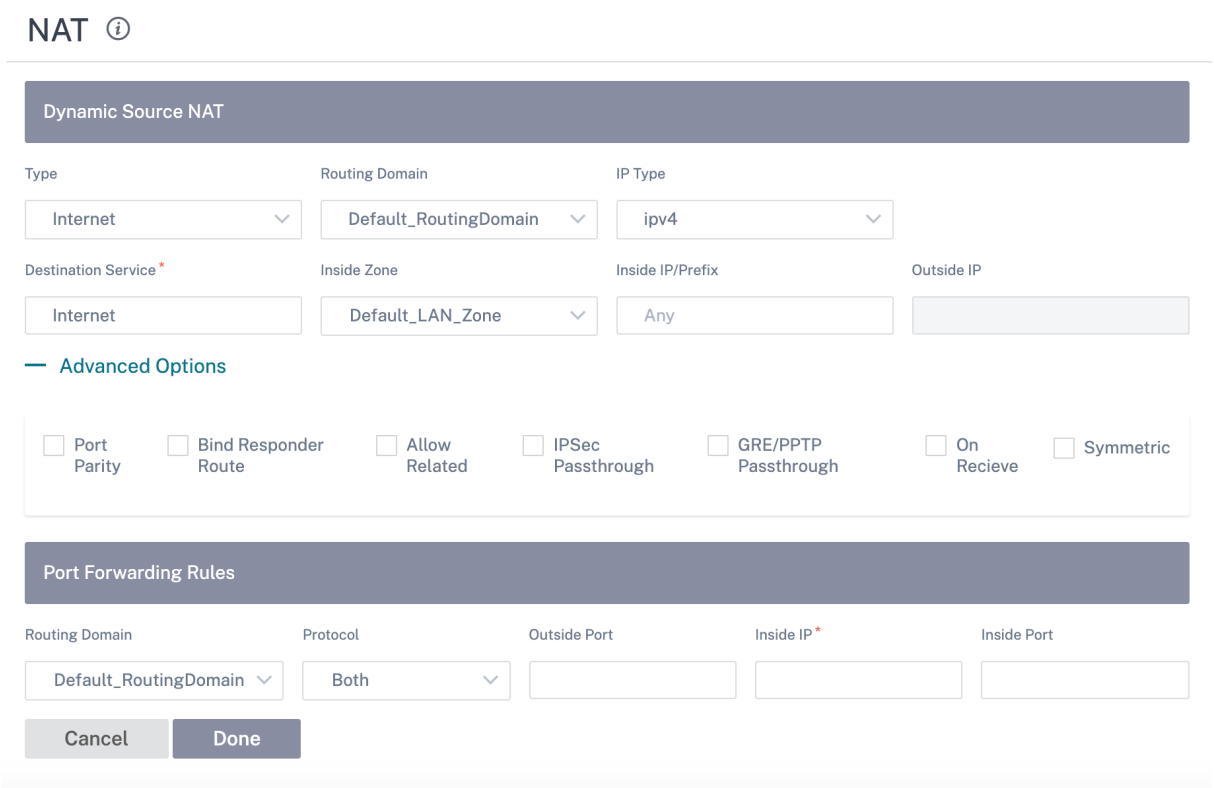
- **Symétrique** : lorsque cette case est cochée, le NAT symétrique est configuré. Lorsque cette option est désactivée, le NAT à port restreint est configuré

Règles de redirection de port :

- **Domaine de routage** : Sélectionnez le domaine de routage auquel s'applique la traduction sélectionnée.
- **Protocole** : TCP, UDP ou les deux.
- **Port extérieur** : Port externe qui est port avant vers le port intérieur.
- **IP interne** : adresse interne pour transférer les paquets correspondants.
- **Port intérieur** : Port intérieur dans lequel le port extérieur sera transféré.

Chaque règle de transfert de port a une règle NAT parent. L'adresse IP externe est tirée de la règle NAT parent.

> **Remarque**
>
> L'interface utilisateur du service Citrix SD-WAN Orchestrator affiche des règles NAT créées automatiquement lorsque les conditions suivantes sont remplies :
>
> - Le service Internet est activé sur le site.
> - La règle NAT de source dynamique Internet sortante IPv4 n'est pas configurée sur le site.
> - Au moins une liaison WAN se trouve sur une interface non fiable ou Internet est activé sur tous les domaines de routage.



Source statique NAT

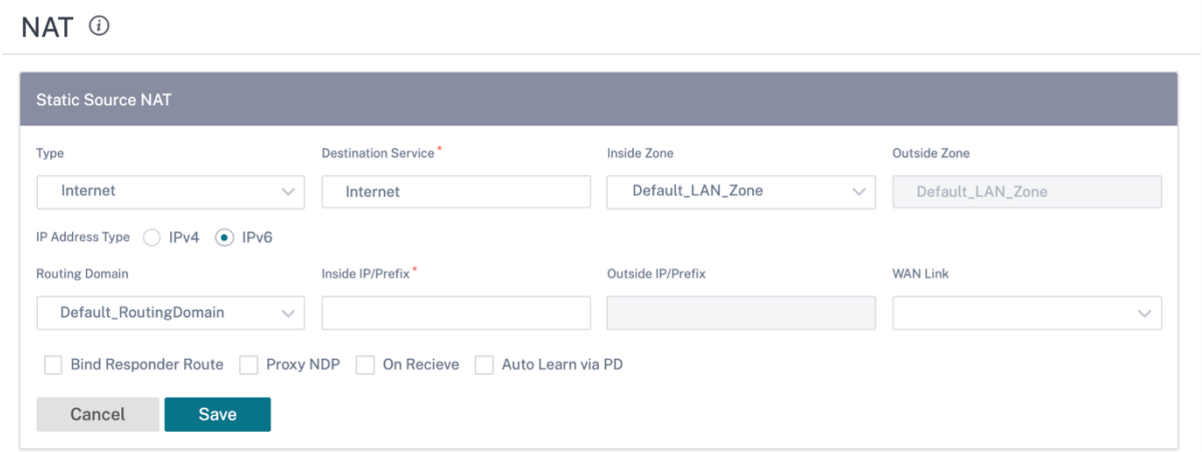
Le NAT statique est un mappage un-à-un d'une adresse IP privée ou d'un sous-réseau à l'intérieur du réseau SD-WAN vers une adresse IP publique ou un sous-réseau en dehors du réseau SD-WAN. Configurez le NAT statique en saisissant manuellement l'adresse IP interne et l'adresse IP externe vers laquelle il doit traduire. Vous pouvez configurer NAT statique pour les services de domaine Local, Virtual Paths, Internet, Intranet et Inter-routage.

Configurer le NAT de source statique

Pour configurer le NAT statique pour un site à l'aide du service Citrix SD-WAN Orchestrator, à partir du niveau du site, accédez à **Configuration > Paramètres avancés > NAT > onglet NAT source statique** . Cliquez sur **+ Source statique NAT**.

- **Type** : types de services SD-WAN auxquels la politique NAT est appliquée. Pour NAT statique, les types de service pris en charge sont les services de domaine Local, Virtual Paths, Internet, Intranet et Inter-routage
- **Service de destination** : entrez un nom pour le service qui correspond au type de service.
- **Zone intérieure** : Type de correspondance de zone de pare-feu intérieur à partir de laquelle le paquet doit être pour permettre la traduction.

- **Zone extérieure** : type de correspondance de zone de pare-feu extérieur à partir de laquelle le paquet doit être pour permettre la traduction.
- **Type d'adresse IP** : Sélectionnez le type d'adresse IPv4 ou IPv6 en fonction de vos préférences.
- **Domaine de routage** : Sélectionnez le domaine de routage auquel s'applique la traduction sélectionnée.
- Adresse**IP intérieure/préfixe** : adresse IP interne et préfixe qui doivent être traduits si les critères de correspondance sont remplis.
- Adresse**IP extérieure/préfixe** : adresse IP extérieure et préfixe vers lesquels l'adresse IP intérieure est traduite si les critères de correspondance sont remplis.
- **Bind Responder Route** : garantit que le trafic de réponse est envoyé via le même service que celui sur lequel il est reçu, afin d'éviter un routage asymétrique.
- **ARP proxy** : garantit que l'appliance répond aux demandes ARP locales pour l'adresse IP externe.
- **Proxy NDP** : garantit que l'appliance répond aux demandes NDP locales pour l'adresse IP externe.
- **À la réception** : lorsque cette case est cochée, le NAT entrant est configuré. Lorsque cette option est désactivée, le NAT sortant est configuré.
- **Apprentissage automatique via DP** : cette case à cocher est activée uniquement lorsque vous sélectionnez IPv6 comme **type d'adresse IP**. Lorsque cette option est sélectionnée, Citrix SD-WAN demande un préfixe au routeur délégant en amont et le routeur délégant répond par un préfixe à Citrix SD-WAN.



Stratégies NAT statiques pour le service Internet IPv6

Citrix SD-WAN prend en charge les politiques NAT statiques pour le service Internet IPv6 à partir de la version 11.4.0. Une politique NAT statique pour le service Internet IPv6 spécifie le mappage d'un préfixe réseau interne à un préfixe réseau externe. Le nombre de stratégies NAT statiques requises

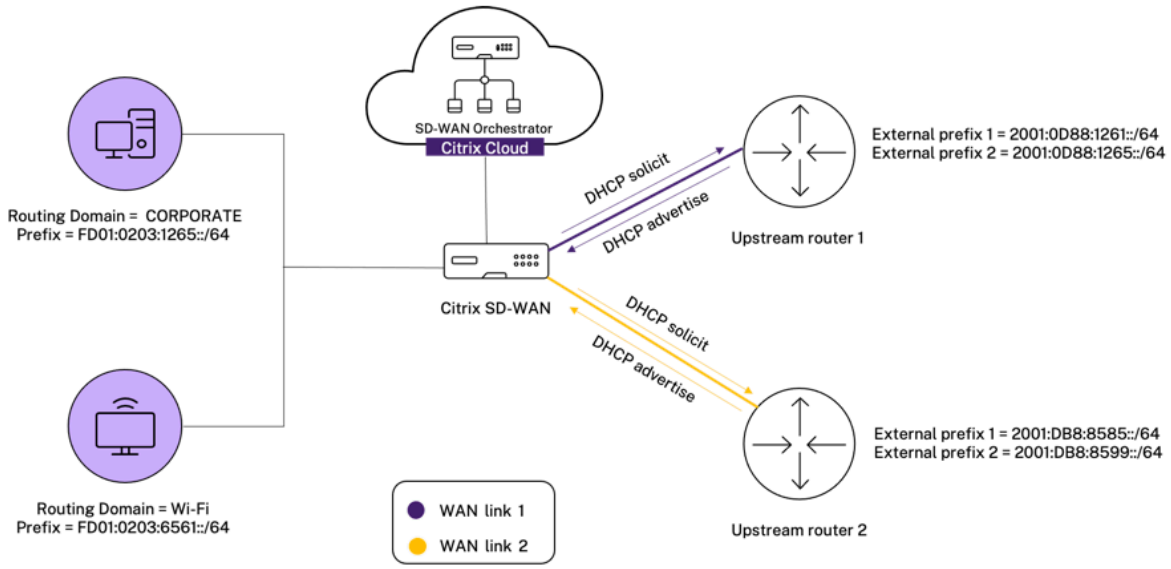
dépend du nombre de réseaux internes et du nombre de réseaux externes (liaisons WAN). S'il existe un nombre **M** de réseaux internes et un nombre **N** de liaisons WAN, le nombre de stratégies NAT statiques requises est **M x N.**

À partir de la version 11.4.0 de Citrix SD-WAN, lors de la création d'une politique NAT statique, vous pouvez soit saisir l'adresse IP externe manuellement, soit activer **Auto Learn via DP**. Lorsque **Auto Learn via DP** est activé, l'appliance SD-WAN reçoit des préfixes délégués du routeur délégué en amont via la délégation de préfixes DHCPv6. Avant Citrix SD-WAN version 11.4.0, l'adresse IP externe était dérivée automatiquement du service et il n'était pas possible de saisir manuellement l'adresse IP externe. Si vous mettez à niveau un dispositif vers la version 11.4.0 ou une version ultérieure et que des stratégies NAT statiques sont configurées pour le service Internet IPv6, vous devez mettre à jour manuellement les stratégies.

Exemple de configuration

Dans la topologie suivante, l'appliance Citrix SD-WAN est configurée avec 2 réseaux internes et 2 liaisons WAN :

- Le réseau interne 1 réside dans le domaine de routage CORPORATE avec le préfixe réseau FD01:0203:6561::/64
- Le réseau interne 2 réside dans le domaine de routage Wi-Fi avec le préfixe réseau FD01:0203:1265::/64
- Via la liaison WAN 1, l'appliance SD-WAN reçoit du routeur délégué amont via la délégation de préfixe DHCPv6, 2 préfixes délégués 2001:0D88:1261::/64 et 2001:0D88:1265::/64. Ces 2 préfixes délégués sont utilisés comme préfixes de réseau externe lorsque le trafic provenant des réseaux internes transite par la liaison WAN 1.
- Via la liaison WAN 2, l'appliance SD-WAN reçoit du routeur délégué amont via la délégation de préfixe DHCPv6, 2 préfixes délégués 2001:DB8:8585::/64 et 2001:DB8:8599::/64. Ces 2 préfixes délégués sont utilisés comme préfixes de réseau externe lorsque le trafic provenant des réseaux internes transite par la liaison WAN 2.



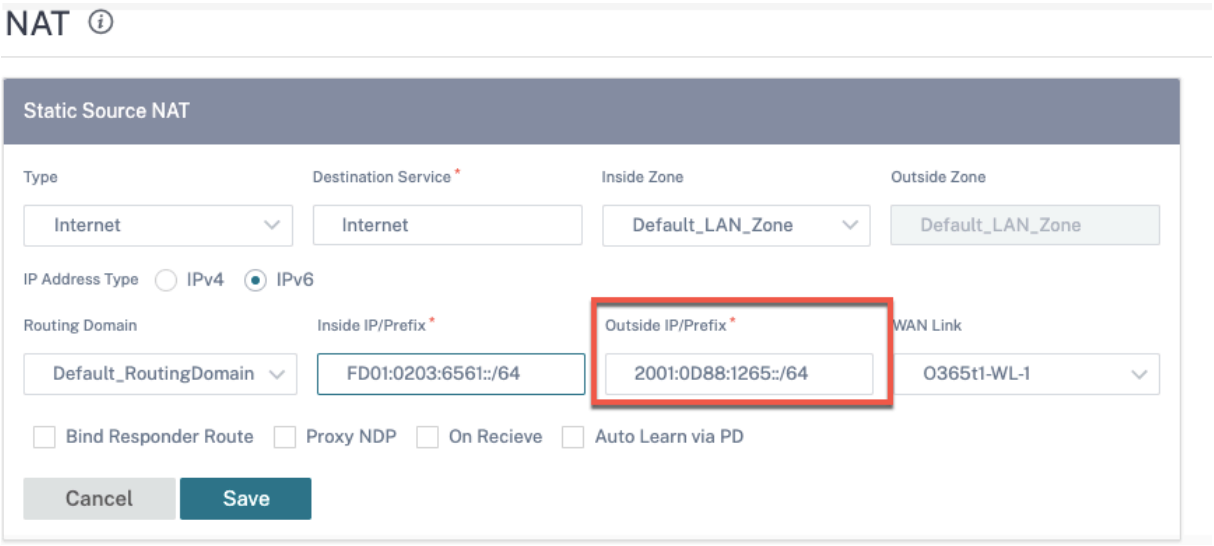
Dans ce scénario, il y a M=2 à l'intérieur des réseaux et des liaisons WAN N=2. Par conséquent, le nombre de politiques NAT statiques requises pour un déploiement correct du service Internet IPv6 est de 2 x 2 = 4. Ces 4 stratégies NAT statiques spécifient la traduction d'adresse pour :

- Réseau interne 1 via la liaison WAN 1
- Réseau interne 1 via la liaison WAN 2
- Réseau interne 2 via la liaison WAN 1
- Réseau interne 2 via la liaison WAN 2

Pour configurer ces politiques NAT statiques, à partir du niveau du site, accédez à **Configuration > Paramètres avancés > NAT > NAT source statique**. Cliquez sur **+ Source statique NAT**.

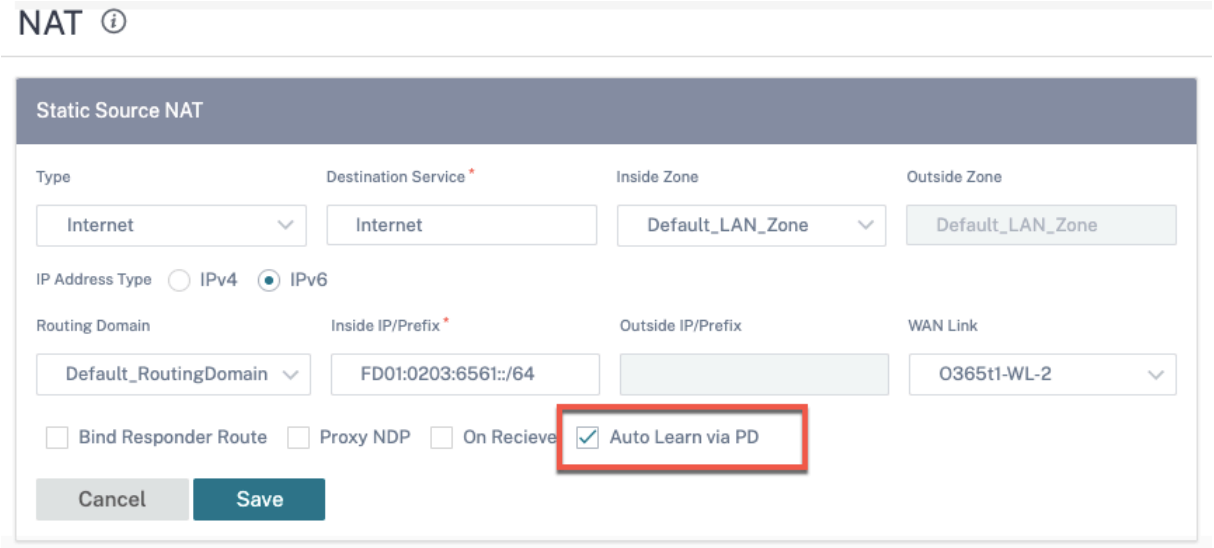
Lors de la création de politiques NAT, assurez-vous de sélectionner le **type** comme **Internet** et le **type d'adresse IP** comme **IPv6**. Sélectionnez le lien WAN et dans le champ **IP intérieur/Préfixe**, entrez le préfixe du réseau interne (seuls les préfixes /64 sont autorisés). Dans le champ **IP extérieur/Préfixe**, vous pouvez soit saisir manuellement le préfixe du réseau externe, soit sélectionner la case à cocher **Auto Learn via DP** .

Voici un exemple dans lequel l'adresse IP externe est entrée manuellement dans la stratégie NAT statique.



Si vous cochez la case **Auto Learn via DP**, assurez-vous que le routeur en amont prend en charge la délégation de préfixes DHCPv6. Citrix SD-WAN demande un préfixe au routeur délégué en amont et le routeur délégué répond par un préfixe à Citrix SD-WAN. Citrix SD-WAN utilise ce préfixe délégué pour traduire l'adresse IP interne en adresse IP externe.

Voici un exemple dans lequel l'**apprentissage automatique via DP** est activé, de sorte que le préfixe réseau externe est obtenu via la délégation de préfixe DHCPv6.



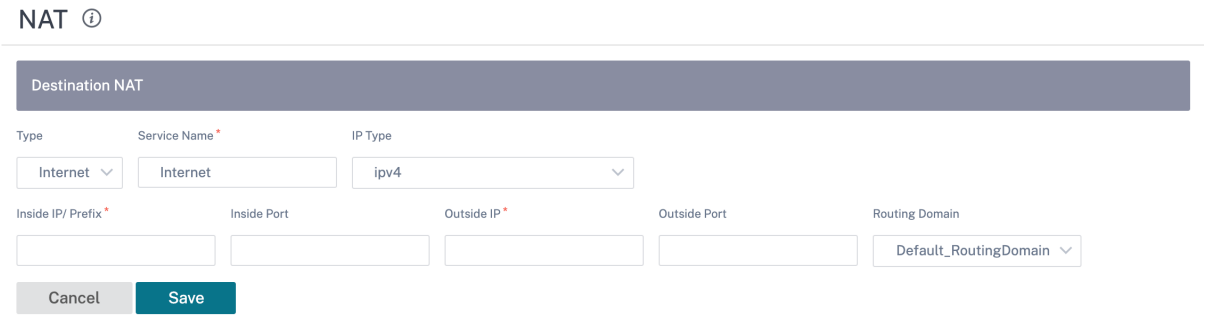
NAT de destination

Les politiques NAT de destination permettent de configurer des politiques de traduction d'adresses réseau entre des hôtes ou des sous-réseaux individuels.

> **Remarque**
>
> - Bien que les traductions entrantes et sortantes puissent être configurées simultanément pour un service, seule la première traduction correspondante sera utilisée. Plusieurs traductions peuvent avoir lieu si une règle existe sur le Service sur lequel un paquet est reçu et sur le Service sur lequel un paquet est envoyé.
> - Les traductions NAT de destination ne s'appliquent qu'au trafic provenant du service local.

Pour configurer ces politiques NAT de destination, à partir du niveau du site, accédez à **Configuration > Paramètres avancés > NAT > NAT de destination**. Cliquez sur **+ Destination NAT**.

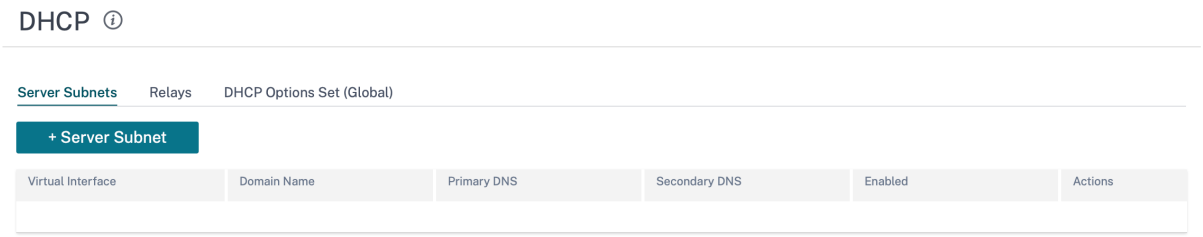
- **Type** : types de services SD-WAN auxquels la politique NAT est appliquée. Pour NAT statique, les types de service pris en charge sont les services de domaine Local, Virtual Paths, Internet, Intranet et Inter-routage
- **Nom du service** : entrez un nom pour le service qui correspond au type de service.
- **Type IP** : Sélectionnez le type d'adresse IPv4 ou IPv6 en fonction de vos préférences.
- **Port intérieur** : Port intérieur dans lequel le port extérieur sera transféré.
- **IP externe** : adresse IP externe et préfixe vers lesquels l'adresse IP interne est traduite si les critères de correspondance sont remplis. Pour le trafic sortant utilisant les services Internet et Intranet, l'adresse IP de liaison WAN configurée est choisie dynamiquement comme adresse IP externe.
- **Port extérieur** : Port externe qui est port avant vers le port intérieur.
- **Domaine de routage** : Sélectionnez le domaine de routage auquel s'applique la traduction sélectionnée.
- **À la réception** : lorsque cette case est cochée, le NAT entrant est configuré. Lorsque cette option est désactivée, le NAT sortant est configuré.



Protocole de configuration d'hôte dynamique

October 21, 2022

Vous pouvez configurer vos appliances SD-WAN en tant que **serveurs DHCP** ou en tant qu'**agent relais DHCP**. La fonctionnalité de serveur DHCP permet aux périphériques du même réseau que l'interface LAN/WAN de l'appliance SD-WAN d'obtenir leur configuration IP à partir de l'appliance SD-WAN. La fonction de relais DHCP permet à vos appliances SD-WAN de transférer des paquets DHCP entre le client DHCP et le serveur.



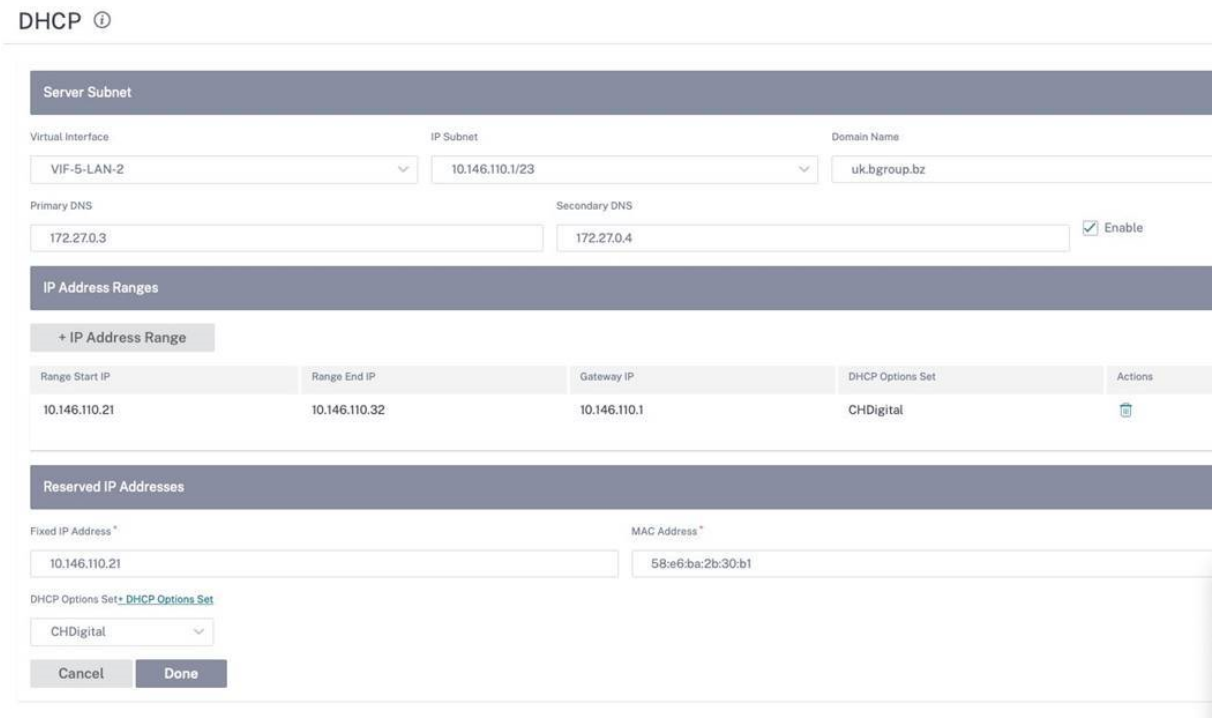
Serveur DHCP

Les appliances Citrix SD-WAN peuvent être configurées en tant que serveur DHCP. Il peut attribuer et gérer les adresses IP des pools d'adresses spécifiés du réseau aux clients DHCP.

Le serveur DHCP peut être configuré pour attribuer d'autres paramètres tels que l'adresse IP DNS et la Gateway par défaut. Le serveur DHCP accepte les demandes d'attribution d'adresse et les renouvellements. Le serveur DHCP accepte également les diffusions à partir de segments LAN connectés localement ou de requêtes DHCP transmises par d'autres agents relais DHCP au sein du réseau.

Pour configurer le serveur DHCP, dans la page Configuration du site, depuis le niveau du site, accédez à **Configuration > Paramètres avancés > DHCP > Sous-réseaux du serveur** > cliquez sur **+ Sous-réseau du serveur**.

Sélectionnez l'**interface virtuelle** à utiliser pour recevoir les demandes DHCP. Le sous-réseau IP auquel le serveur DHCP fournit les adresses IP est automatiquement renseigné.



Entrez le **nom de domaine**, le**DNS principal**et le **DNS secondaire**. Le serveur DHCP transmet ces informations aux clients DHCP.

Configurez des pools d'adresses IP dynamiques utilisés pour allouer des adresses IP aux clients. Spécifiez l'adresse IP de début et de fin de la plage et sélectionnez le **jeu d'options DHCP**.

> **Remarque**
>
> Le jeu d'options DHCP est constitué de groupes de paramètres DHCP qui peuvent être appliqués à des plages d'adresses IP individuelles. Pour plus d'informations, consultez la section Ensemble d'options DHCP.

Définissez l'adresse IP réservée en mappant les hôtes individuels qui nécessitent une adresse IP fixe à leur adresse MAC. Entrez l'**adresse IP fixe**, l'**adresse MAC**et sélectionnez un **ensemble d'options DHCP**.

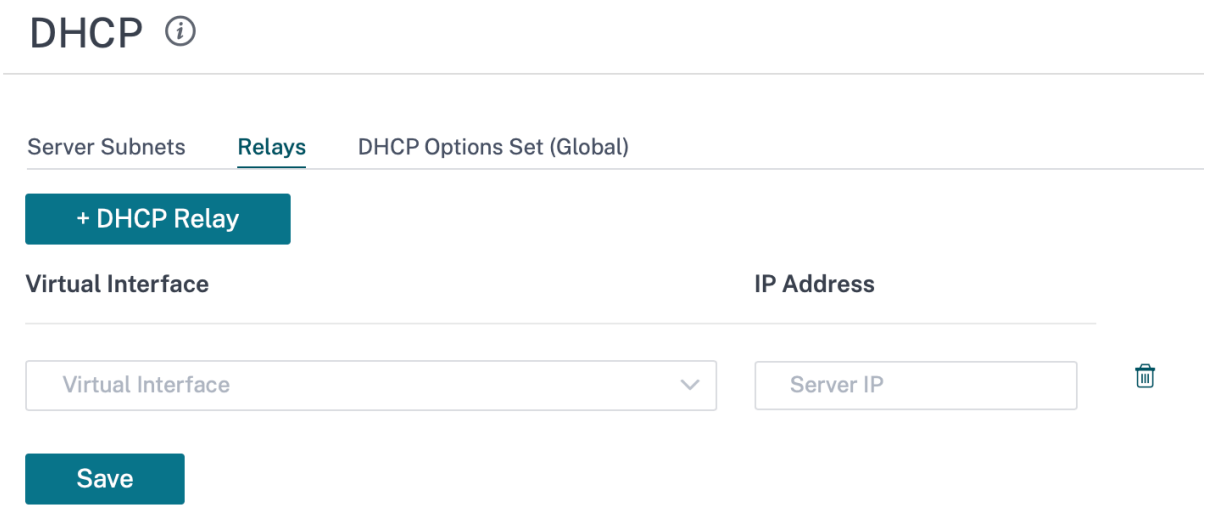
> **Remarque**
>
> Pour les adresses IP réservées, l'**adresse IP de la passerelle** est définie en configurant l'option **Router** dans le **jeu d'options DHCP**.

Relais DHCP

L'appliance Citrix SD-WAN peut être configurée en tant que relais DHCP. Il relaie les requêtes DHCP et les réponses entre les clients DHCP locaux et un serveur DHCP distant.

Il permet aux hôtes locaux d'acquérir des adresses IP dynamiques à partir du serveur DHCP distant. L'agent relais reçoit des messages DHCP et génère un nouveau message DHCP à envoyer sur une autre interface.

Pour configurer le serveur DHCP, dans la page Configuration du site, accédez à **Configuration > Paramètres avancés > DHCP > Relais** > cliquez sur **+ Relais DHCP**.



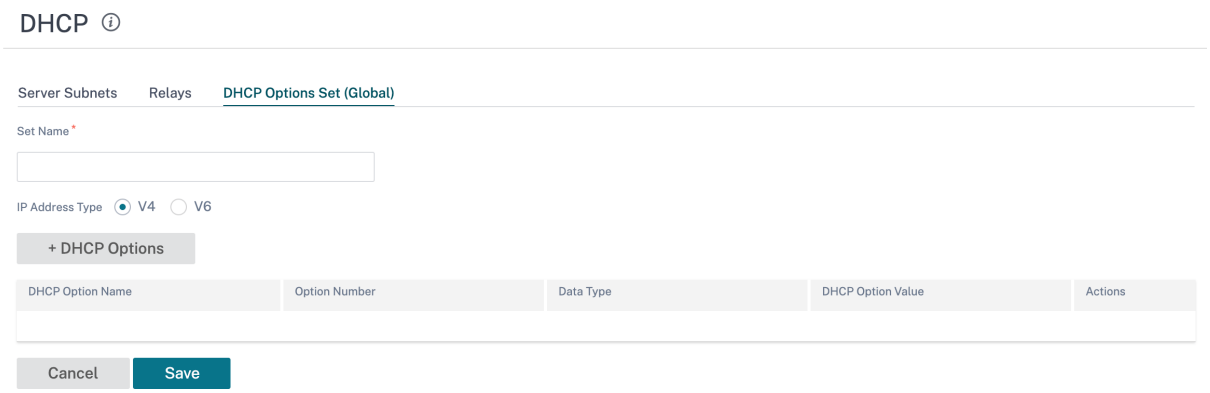
Sélectionnez une **interface virtuelle** qui communique avec un serveur DHCP distant. Entrez l'**adresse IP du serveur DHCP** que le relais utilise pour transférer la demande et la réponse des clients.

Vous pouvez configurer un seul **relais DHCP** à l'aide d'une interface réseau virtuelle commune et le diriger vers plusieurs serveurs DHCP.

Ensemble d'options DHCP

Les options DHCP sont un groupe de configurations DHCP qui peuvent être appliquées à des plages d'adresses IP individuelles ou à un seul hôte.

Définissez un nom pour le profil d'option DHCP et choisissez le **type d'adresse IP**. Cliquez sur **+ Définir les options DHCP** et sélectionnez le nom d'une option DHCP dans la liste. Le numéro d'option est préconfiguré. Pour les options personnalisées, la plage est de 224 à 254. Sélectionnez un **type de données** et entrez une **valeur** pour l'option.



Apprentissage des adresses IP de liaison WAN via le client DHCP

Les appliances Citrix SD-WAN prennent en charge l'apprentissage des adresses IP WAN Link via les clients DHCP. Cette fonctionnalité réduit la quantité de configuration manuelle requise pour déployer des appliances SD-WAN et réduit les coûts des FAI en éliminant le besoin d'acheter des adresses IP statiques. Les appliances SD-WAN peuvent obtenir des adresses IP dynamiques pour les liaisons WAN sur des interfaces non fiables. Cela élimine le besoin d'un routeur WAN intermédiaire pour effectuer cette fonction.

> **Remarques**
>
> - Le client DHCP ne peut être configuré que pour les interfaces non pontées non fiables configurées en tant que nœuds client.
> - Le client DHCP et le port de données peuvent être activés sur MCN/RCN uniquement si l'adresse IP publique est configurée.
> - Le déploiement à bras unique ou PBR (Policy Based Routing) n'est pas pris en charge sur le site avec la configuration du client DHCP.
> - Les événements DHCP sont enregistrés uniquement du point de vue du client et aucun journal du serveur DHCP n'est généré.

Pour plus d'informations sur la configuration du DHCP pour une interface virtuelle non fiable en mode fail-to-block et en mode fail-to-wire, voir Configuration au niveau du site.

Routage multidiffusion

October 21, 2022

Le routage multidiffusion permet une distribution efficace du trafic un-à-plusieurs. Une source de multidiffusion envoie le trafic de multidiffusion dans un seul flux vers un groupe de multidiffusion.

Le groupe de multidiffusion contient des récepteurs tels que des hôtes et des routeurs adjacents qui utilisent le protocole IGMP pour la communication multidiffusion. La voix sur IP, la vidéo à la demande, la télévision IP et la vidéoconférence sont quelques-unes des technologies courantes qui utilisent le routage multidiffusion. Lorsque vous activez le routage de multidiffusion sur l'appliance Citrix SD-WAN, l'appliance agit comme un routeur de multidiffusion.

Multidiffusion spécifique à la source

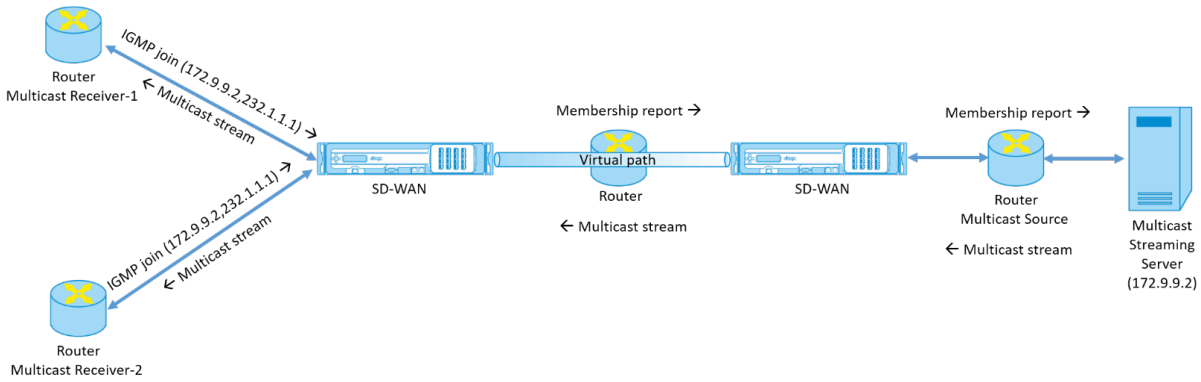
Les protocoles de multidiffusion permettent généralement aux récepteurs de multidiffusion de recevoir du trafic de multidiffusion à partir de n'importe quelle source.

Avec la multidiffusion spécifique à la source (SSM), vous pouvez spécifier la source à partir de laquelle les récepteurs reçoivent le trafic de multidiffusion. Il garantit que les récepteurs ne sont pas des écouteurs ouverts pour chaque source qui envoie des flux de multidiffusion, mais plutôt écouter une source de multidiffusion particulière.

Le SSM réduit le coût des ressources utilisées pour consommer du trafic provenant de toutes les sources possibles. Le SSM fournit également une couche de sécurité en veillant à ce que les récepteurs reçoivent le trafic d'un expéditeur connu.

La topologie suivante montre deux récepteurs de multidiffusion sur un site de succursale et un serveur de multidiffusion (172.9.9.2) dans le centre de données. Le serveur de multidiffusion diffuse le trafic sur un groupe particulier (232.1.1.1), les récepteurs rejoignent le groupe. Tout trafic diffusé sur le groupe de multidiffusion est relayé à tous les récepteurs qui ont rejoint le groupe.

> **Remarque**
>
> Pour que SSM fonctionne, l'IP du groupe de multidiffusion doit se situer dans la plage 232.0.0.0/8.



1. Les récepteurs de multidiffusion envoient une demande de jointure IGMP IP indiquant que les récepteurs souhaitent rejoindre le groupe de multidiffusion et recevoir le flux de multidiffusion à partir de la source.

La jointure IGMP comprend 2 attributs la source et le groupe de multidiffusion (S, G). IGMP Version 3 est utilisé pour SSM sur la source de multidiffusion et le récepteur pour relayer certaines adresses source spécifiques INCLUDE.

Le SSM permet aux récepteurs de recevoir explicitement des flux provenant de serveurs multidiffusion spécifiques, dont l'adresse source est explicitement fournie par les récepteurs dans le cadre de la requête JOIN. Dans cet exemple, une demande de jointure IGMP v3 est déclenchée avec une liste de sources d'inclusion explicite, qui contient la source 172.9.9.2, comme adresse qui envoie le flux de multidiffusion sur le groupe 232.1.1.1.

2. Le Citrix SD-WAN de la succursale écoute toutes les demandes IGMP de ces récepteurs et le convertit en rapport d'appartenance et l'envoie via le chemin virtuel à l'appliance SD-WAN du centre de données.
3. L'appliance Citrix SD-WAN du centre de données reçoit le rapport d'appartenance sur le chemin virtuel et le transfère à la source de multidiffusion, établissant ainsi un canal de contrôle.
4. La source de multidiffusion transmet le flux de multidiffusion sur le chemin virtuel aux récepteurs de multidiffusion.

Le trafic de canal de contrôle et le flux de multidiffusion traversent le chemin virtuel établi entre la succursale et le centre de données. Le chemin de superposition Citrix SD-WAN assure et isole le trafic multidiffusion contre la dégradation du WAN ou les suppositions de liaison.

Configuration de multidiffusion

Pour configurer la multidiffusion, effectuez les opérations suivantes sur le service SD-WAN Orchestrator à la fois à la source et à la destination.

1. Créer un groupe de multidiffusion : indiquez un nom et une adresse IP pour le groupe de multidiffusion. L'IP du groupe de multidiffusion doit se situer dans la plage 232.0.0.0/8 pour la multidiffusion spécifique à la source.
2. Activer le proxy IGMP —Vous pouvez configurer l'appliance Citrix SD-WAN en tant que proxy IGMP/MLD pour transporter les informations du canal de contrôle IGMP pour le routage de multidiffusion.
3. Définir les services en amont et en aval - Une interface en amont permet à l'IGMP PROXY de se connecter à l'appliance SD-WAN plus proche de la source de multidiffusion réelle qui diffuse le trafic. Une interface en aval permet au proxy IGMP de se connecter aux hôtes qui sont plus éloignés de la source de multidiffusion réelle qui diffuse le trafic.
   Les services en amont et en aval sont différents pour l'appliance à la source et l'appliance à la destination.

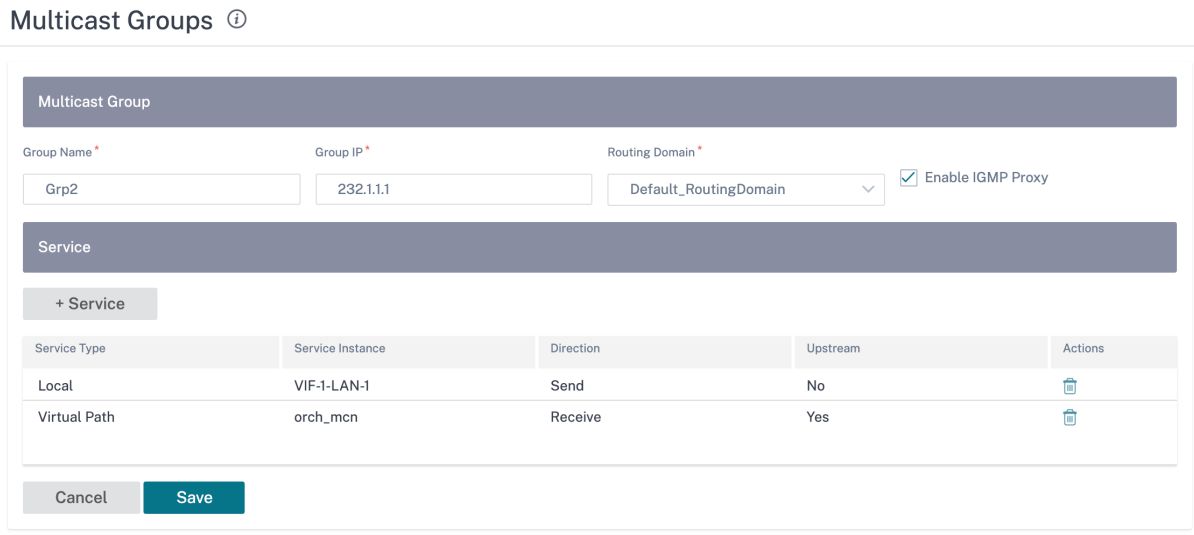
> **Remarque** :
>
> Une fois que la branche ou le MCN est configuré en amont, il doit également être configuré en amont pour les autres groupes.

Pour configurer la multidiffusion, au niveau du site, accédez à **Configuration** > **Paramètres avancés** > **Groupes de multidiffusion**. Créez un groupe de multidiffusion en fournissant un nom et une adresse IP (IPv4 ou IPv6) pour le groupe de multidiffusion. Cliquez sur **Activer le proxy IGMP**.

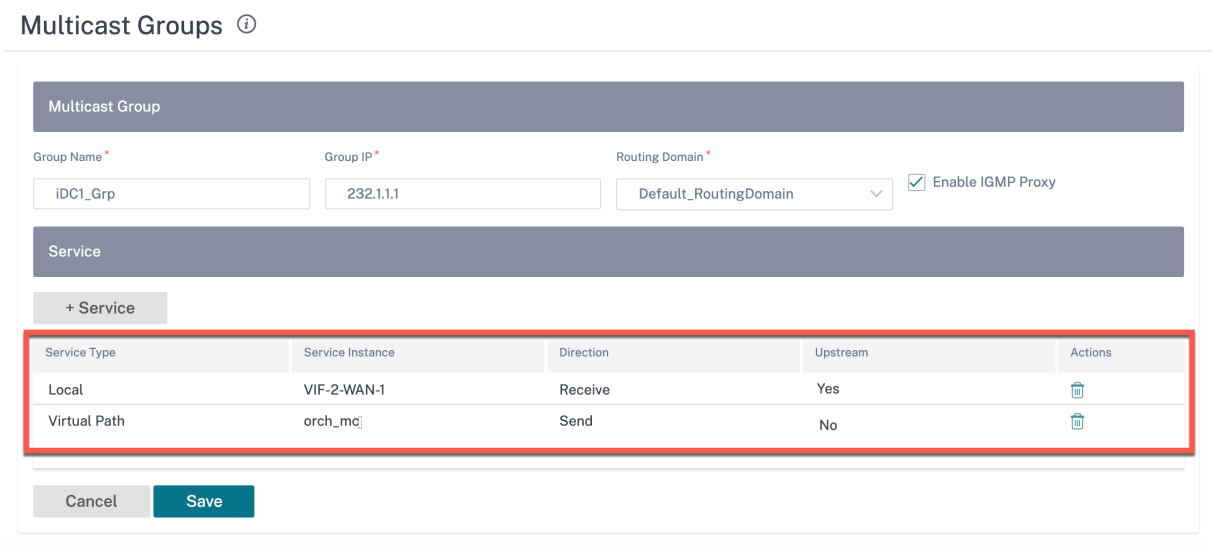
Configurez les chemins d'accès en amont et en aval pour les appliances de succursale et de centre de données.

Pour l'appliance plus proche du récepteur de multidiffusion (Branche), elle reçoit le trafic de multidiffusion sur l'interface Virtual Path Interface et envoie le trafic sur l'interface locale vers le récepteur.

> **Remarque** :
>
> - Lorsqu'une source de multidiffusion est configurée en tant que service Intranet, l'adresse IP source du flux de multidiffusion doit avoir une route mappée vers le service Intranet.
> - Assurez-vous de créer des politiques de pare-feu appropriées pour autoriser le trafic de multidiffusion sur l'appliance SD-WAN.



Pour l'appliance plus proche de la source de multidiffusion (centre de données), elle reçoit le trafic de multidiffusion sur l'interface locale et envoie le trafic sur l'interface Virtual Path Interface.

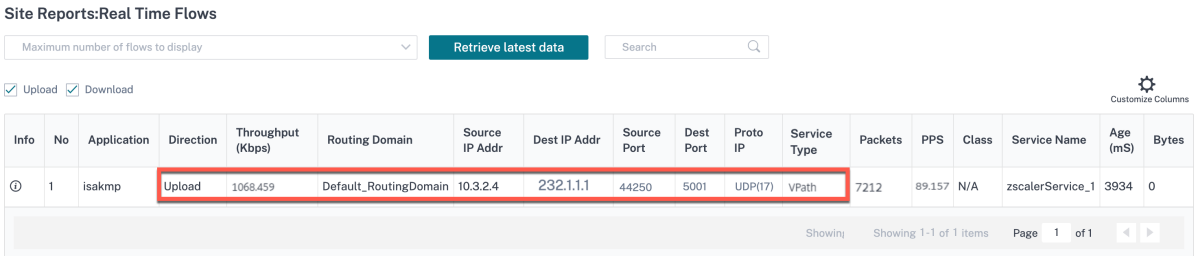


Surveillance

Statistiques sur les flux

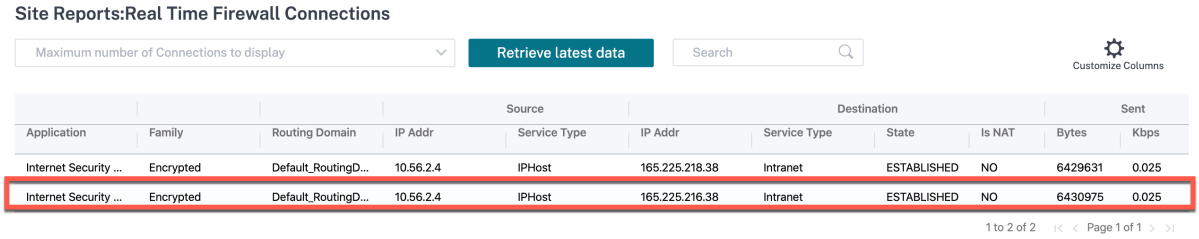
Une fois que le canal de contrôle de multidiffusion est établi et que la source de multidiffusion commence à diffuser, vous pouvez afficher les statistiques de flux de multidiffusion. Vous pouvez voir que le trafic UDP de multidiffusion a été envoyé sur le service de chemin virtuel d'un récepteur vers le groupe de multidiffusion 232.1.1.1.

> **Remarque** :
>
> Si SSM est activé et si le trafic provient d'un autre serveur qui ne fait pas partie de la liste attendue des expéditeurs source, l'appliance SD-WAN ne dispose pas de données de rapport.



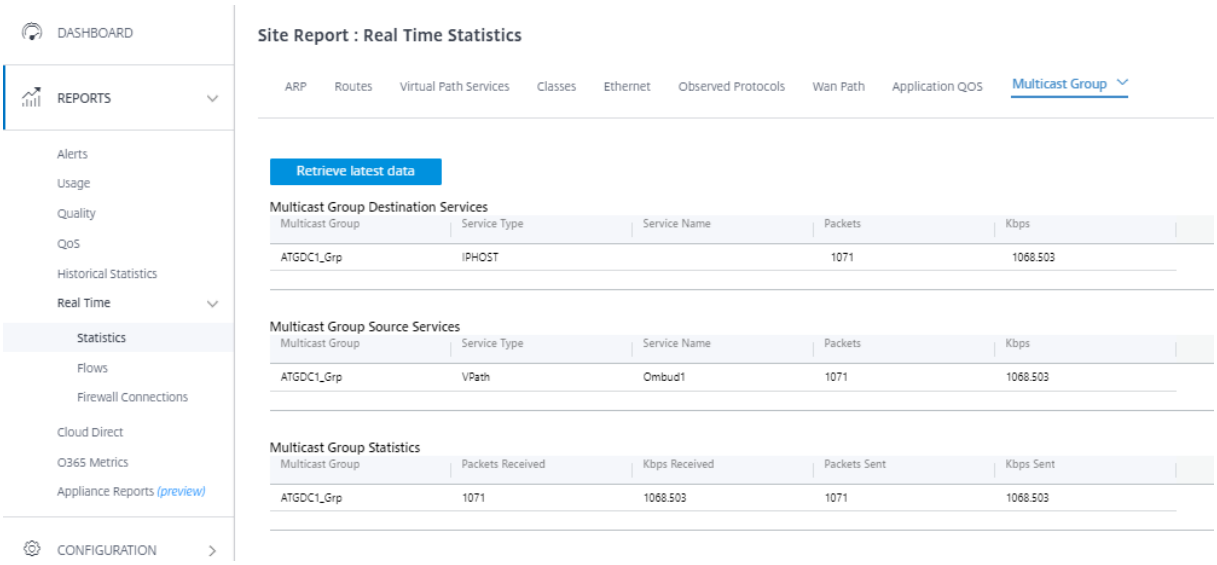
Statistiques de pare-feu

La table de pare-feu affiche le trafic de multidiffusion provenant de l'interface LAN sur l'adresse IP du groupe Multicast et est envoyé via le chemin virtuel.



Statistiques de groupe de multidiffusion

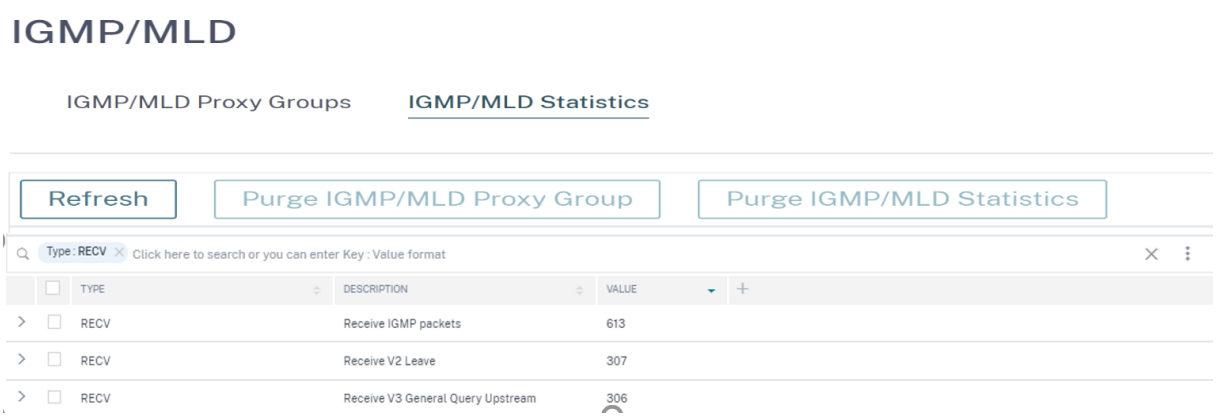
La table des groupes de multidiffusion fournit des détails sur le trafic de multidiffusion, tels que les paquets envoyés et reçus sur la source, la destination et l'agrégation des deux.



IGMP/MLD

Lorsque les récepteurs de multidiffusion lancent une demande de jointure de groupe, vous pouvez consulter les détails du récepteur sous **Rapports** > **Temps réel** > **IGMP/MLD** > **Statistiques IGMP/MLD**. Vous pouvez consulter ces informations à la fois à la source et à la destination. Cliquez sur **Actualiser** pour obtenir les données actuelles.

L'image suivante montre que les paquets IGMP/MLD reçus et que le type de filtre RECV est utilisé pour inclure les paquets de réception IGMP/MLD.



Pour afficher les détails des groupes proxy IGMP, accédez à **Rapports** > **Temps réel** > **IGMP/MLD** > **Groupes proxy IGMP/MLD**. Cliquez sur **Actualiser** pour obtenir les données actuelles.

Sélectionnez **Purger les statistiques IGMP/MLD** pour purger les données statistiques IGMP du tableau des statistiques IGMP.

Sélectionnez **Purger le groupe IGMP/MLD** pour purger les données du groupe IGMP dans le tableau des groupes IGMP.

Protocole de redondance de routeur virtuel

October 21, 2022

Le protocole VRRP (Virtual Router Redundancy Protocol) est un protocole largement utilisé qui fournit la redondance des appareils afin d'éliminer le point de défaillance unique inhérent à un environnement statique routé par défaut.

VRRP vous permet de configurer deux routeurs ou plus pour former un groupe. Ce groupe apparaît comme une passerelle par défaut unique avec une adresse IP virtuelle et une adresse MAC virtuelle.

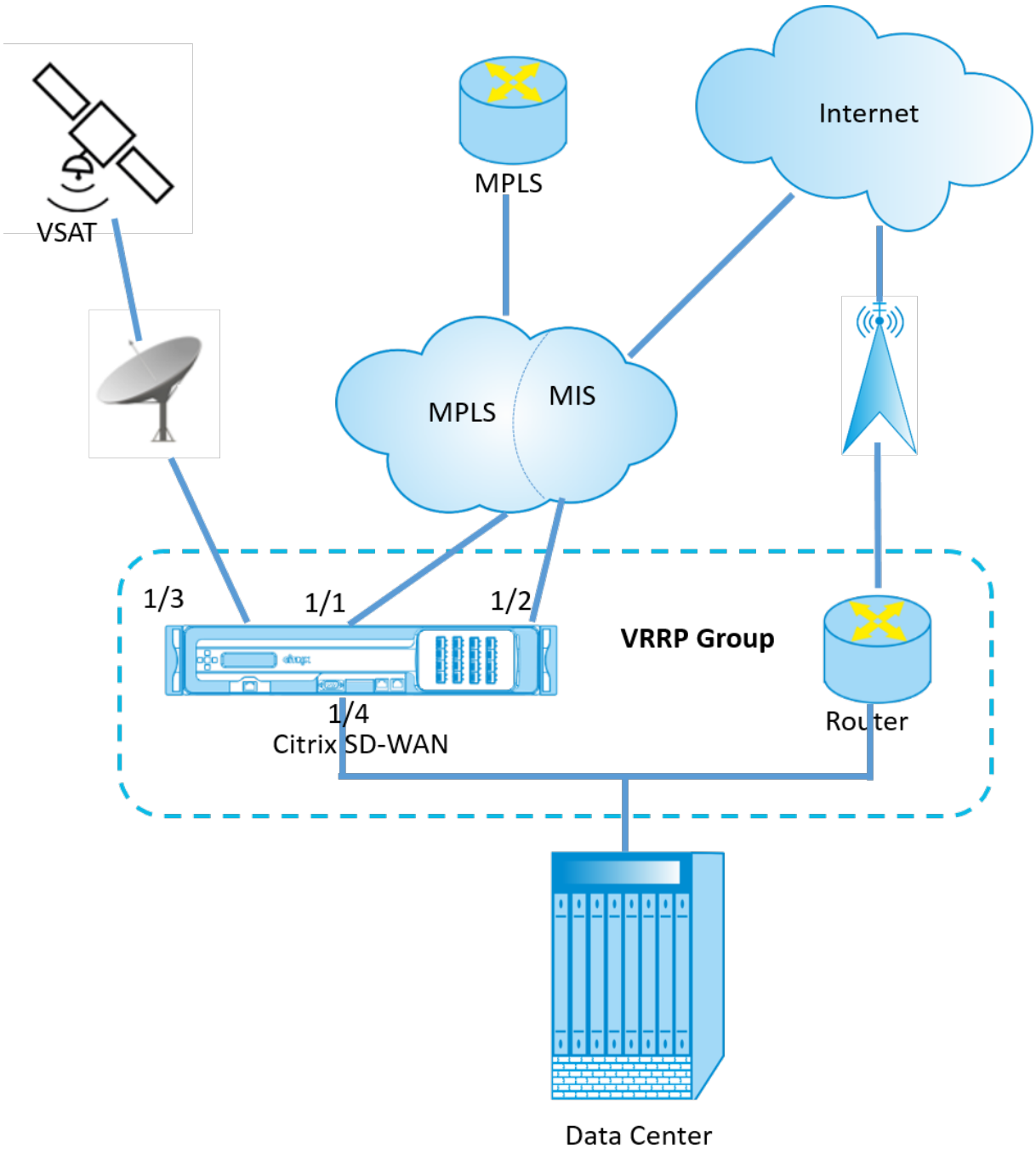
Un routeur de secours prend automatiquement le relais en cas de défaillance du routeur principal/principal. Dans une configuration VRRP, le routeur principal envoie un paquet VRRP connu sous le nom de publicité aux routeurs de secours. Lorsque le routeur principal arrête d'envoyer la publicité, le routeur de secours règle l'intervalle. Si aucune annonce n'est reçue pendant cette période d'attente, le routeur de secours lance la routine de basculement.

Le VRRP spécifie un processus d'élection dans lequel le routeur ayant la priorité la plus élevée devient le routeur principal. Si la priorité est la même entre les routeurs, le routeur avec l'adresse IP la plus élevée devient le routeur principal. Les autres routeurs sont en état de sauvegarde. Le processus d'élection est relancé si le routeur principal tombe en panne, si un nouveau routeur rejoint le groupe ou si un routeur existant quitte le groupe.

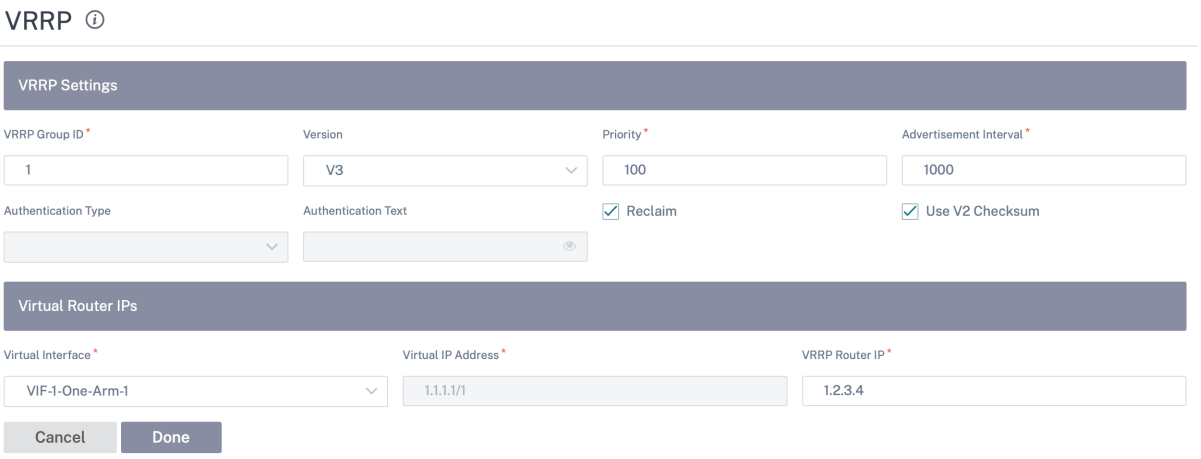
VRRP garantit un chemin par défaut haute disponibilité sans configurer les protocoles de routage dynamique ou de découverte de routeurs sur chaque hôte final.

Citrix SD-WAN version 10.1 prend en charge les versions 2 et 3 de VRRP pour interagir avec tous les routeurs tiers. La version 11.5 de Citrix SD-WAN prend en charge la version 6. L'appliance SD-WAN agit en tant que routeur principal et dirige le trafic vers l'utilisation du service de chemin virtuel entre les sites. Vous pouvez configurer l'appliance SD-WAN en tant que routeur principal VRRP en configurant l'adresse IP de l'interface virtuelle en tant qu'adresse IP VRRP et en définissant manuellement la priorité sur une valeur supérieure à celle des routeurs homologues. Vous pouvez configurer l'intervalle de publication et l'option preempt.

Le diagramme de réseau ci-dessous montre un dispositif Citrix SD-WAN et un routeur configuré en tant que groupe VRRP. L'appliance SD-WAN est configurée pour être le routeur principal. Si l'appliance SD-WAN tombe en panne, le routeur de sauvegarde prend le relais en quelques millisecondes, ce qui garantit qu'il n'y a pas de temps d'arrêt.



Pour configurer le VRRP, dans la page de configuration du site, accédez à **Configuration** > **Paramètres avancés** > **VRRP** > cliquez sur **+ Ajouter un VRRP**.



Vous pouvez modifier les paramètres de chemin d'accès de membre suivants :

- **ID du groupe VRRP : ID**du groupe VRRP. L'ID de groupe doit être une plage de valeurs comprise entre 1 et 255. Le même ID de groupe doit également être configuré sur les routeurs de sauvegarde.
- **Version : version**du protocole VRRP. Vous pouvez choisir entre le protocole VRRP V2 et V3.
- **Priorité** : priorité de l'appliance Citrix SD-WAN pour le groupe VRRP. La plage de priorité est de 1 à 254. Définissez cette valeur sur maximum (254) pour faire de l'appliance SD-WAN le routeur principal.

  > **Remarque**
  >
  > Si le routeur est le propriétaire de l'adresse IP VRRP, la priorité est définie sur 255 par défaut.

- **Intervalle de publicité** : fréquence en millisecondes, à laquelle les publicités VRRP sont envoyées lorsque l'appliance SD-WAN est le routeur principal. L'intervalle de publicité par défaut est d'une seconde.
- **Type d'authentification** : Vous pouvez choisir **Texte brut** pour saisir une chaîne d'authentification. La chaîne d'authentification est envoyée sous forme de texte brut sans aucun chiffrement dans les annonces VRRP. Sélectionnez **Aucun**si vous ne souhaitez pas configurer l'authentification.
- **Texte d'**authentification : chaîne d'authentification à envoyer dans la publicité VRRP. Cette option est activée si le **type d'authentification** est **Texte brut**.

  > **Remarque**
  >
  > Les paramètres **Type d'authentification et Texte d'authentification** sont activés uniquement pour la version 2 du protocole VRRP.

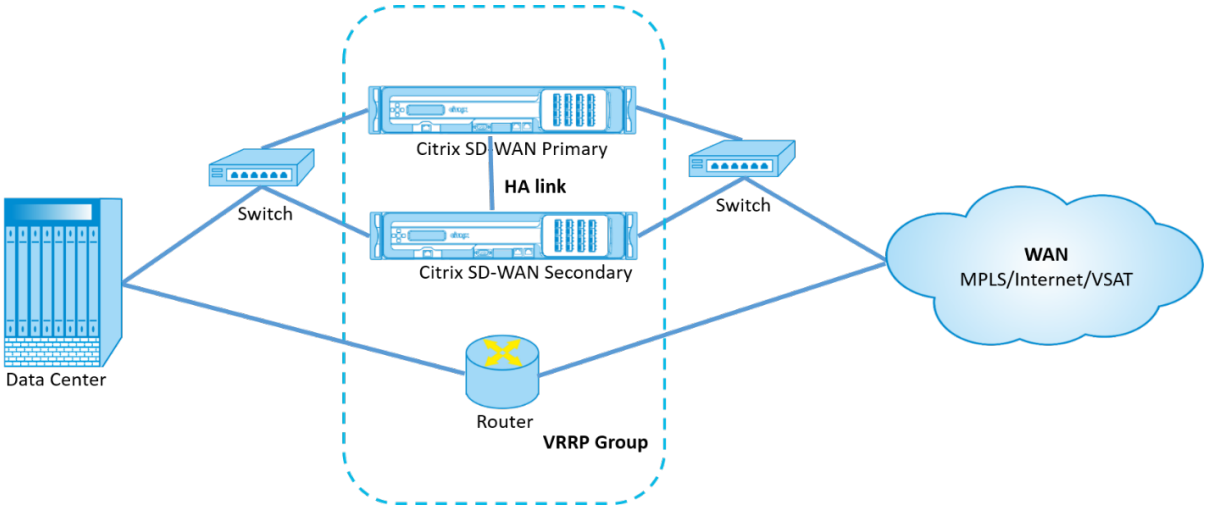
- **Utiliser la somme de contrôle V2** : permet la compatibilité avec les périphériques réseau tiers pour VRRPv3. Par défaut, VRRPv3 utilise la méthode de calcul de somme de contrôle v3. Certains périphériques tiers peuvent uniquement prendre en charge le calcul de la somme de contrôle vRRPV2. Dans de tels cas, activez cette option.
- **Interface virtuelle** : Interface virtuelle à utiliser pour le VRRP. Si IPv6 est utilisé, NDP RA sera activé par défaut sur l'interface virtuelle. Choisissez l'une des interfaces virtuelles configurées.
- **Adresse IP virtuelle : adresse**IP virtuelle attribuée à l'interface virtuelle. Choisissez l'une des adresses IP virtuelles configurées pour l'interface virtuelle. Vous pouvez spécifier l'adresse IPv4 ou IPv6.
- **IP du routeur VRRP** : adresse IP du routeur virtuel du groupe VRRP. Par défaut, l'adresse IP virtuelle de l'appliance SD-WAN est affectée en tant qu'adresse IP du routeur virtuel. L'adresse IP du routeur virtuel VRRP doit être une adresse IPv6 locale de liaison.

Limitations

- VRRP est pris en charge en mode passerelle uniquement.
- Vous pouvez configurer jusqu'à quatre ID VRRP (VRID).
- Jusqu'à 16 interfaces réseau virtuelles peuvent participer à VRID.

Haute disponibilité et VRRP

Vous pouvez réduire considérablement les temps d'arrêt du réseau et les perturbations du trafic en appliquant à la fois les fonctionnalités de haute disponibilité et de VRRP sur votre réseau SD-WAN. Déployez une paire d'appliances Citrix SD-WAN dans des rôles actif/de secours avec un routeur de secours pour former le groupe VRRP. Ce groupe apparaît comme une passerelle par défaut unique avec une adresse IP virtuelle et une adresse MAC virtuelle.



Voici deux cas de déploiement de la haute disponibilité et du VRRP :

1er cas : la minuterie de basculement haute disponibilité sur SD-WAN est égale à la minuterie de basculement VRRP.

Le comportement attendu est le basculement à haute disponibilité avant le basculement VRRP, c'est-à-dire que le trafic continue de circuler à travers la nouvelle appliance Active SD-WAN. Dans ce cas, SD-WAN continue avec le rôle maître VRRP.

2ème cas : minuteur de basculement haute disponibilité sur SD-WAN supérieur au minuteur de basculement VRRP.

Le comportement attendu est que le basculement VRRP vers le routeur se produit, c'est-à-dire que le routeur devient VRRP Master et le trafic peut momentanément circuler à travers le routeur, en contournant l'appliance SD-WAN.

Mais une fois le basculement à haute disponibilité effectué, le SD-WAN redevient VRRP Master, c'est-à-dire que le trafic passe désormais par la nouvelle appliance SD-WAN active.

Pour plus d'informations sur les modes de déploiement haute disponibilité, consultez la section Haute disponibilité.

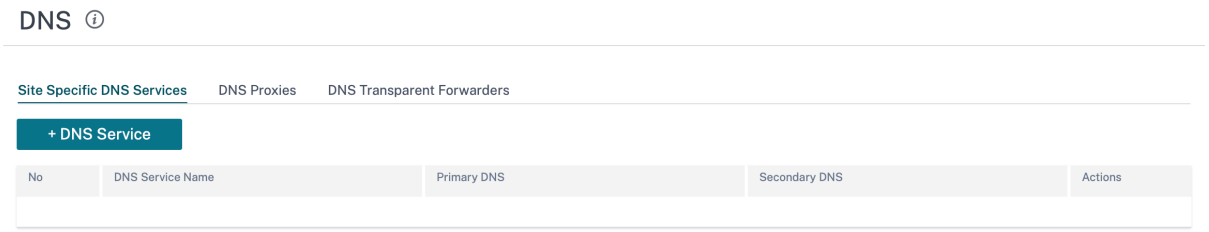
Paramètres du système de noms de domaine

October 21, 2022

Domain Name System (DNS) traduit les noms de domaine lisibles par l'homme en adresses IP lisibles par machine, et le sens inverse. Citrix SD-WAN fournit les fonctionnalités DNS suivantes :

- Proxy DNS
- Transfert transparent DNS

Pour configurer les paramètres DNS, sur la page Configuration du site, accédez à **Configuration > Paramètres avancés** > **Paramètres DNS**.



Serveurs DNS spécifiques au site

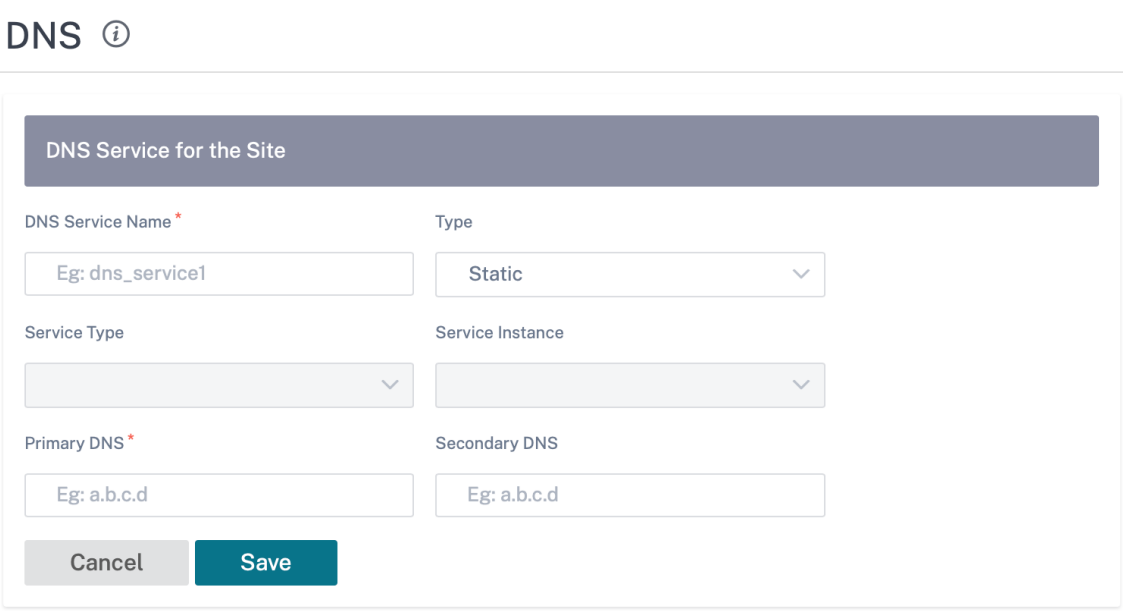
Dans l'onglet **Serveurs DNS spécifiques au site**, cliquez sur **+ Serveur DNS** pour configurer les serveurs DNS spécifiques au site vers lesquels les requêtes DNS sont acheminées. Indiquez un nom pour le serveur DNS. Choisissez l'un des types de service suivants :

- **Statique** : Intercepte les requêtes DNS destinées à l'adresse IP Citrix SD-WAN et les transmet aux serveurs DNS IPv4 spécifiés. Vous pouvez créer interne, FAI, google ou tout autre service DNS open source.
- **Dynamique** : intercepte les requêtes DNS destinées à l'adresse IP Citrix SD-WAN et la redirige vers l'un des serveurs DNS IPv4 appris à partir des liens WAN basés sur DHCP. Si la liaison WAN tombe en panne, un autre serveur DNS basé sur DHCP est choisi. Cette fonctionnalité est utile dans le déploiement où les FAI autorisent les requêtes DNS uniquement aux serveurs DNS hébergés par eux. Le service DNS dynamique peut être configuré uniquement au niveau du site. Un seul service DNS dynamique est autorisé par site.
- **StaticV6** : Intercepte les requêtes DNS destinées à l'adresse IP Citrix SD-WAN et les transmet aux serveurs DNS IPv6 spécifiés. Vous pouvez créer interne, FAI, google ou tout autre service DNS open source.
- **DynamicV6** : intercepte les requêtes DNS destinées à l'adresse IP Citrix SD-WAN et la redirige vers l'un des serveurs DNS IPv6 appris à partir des liens WAN basés sur DHCP. Si la liaison WAN tombe en panne, un autre serveur DNS basé sur DHCP est choisi. Cette fonctionnalité est utile dans le déploiement où les FAI autorisent les requêtes DNS uniquement aux serveurs DNS hébergés par eux. Le service DNS dynamique peut être configuré uniquement au niveau du site. Un seul service DNS dynamique est autorisé par site.

Pour configurer le service DNS statique, sélectionnez le **typeStatique**(pour une adresse IPv4) ou**Staticv6**(pour une adresse IPv6) et entrez une paire d'adresses IP du**DNS principal**et du serveur**DNS secondaire** .

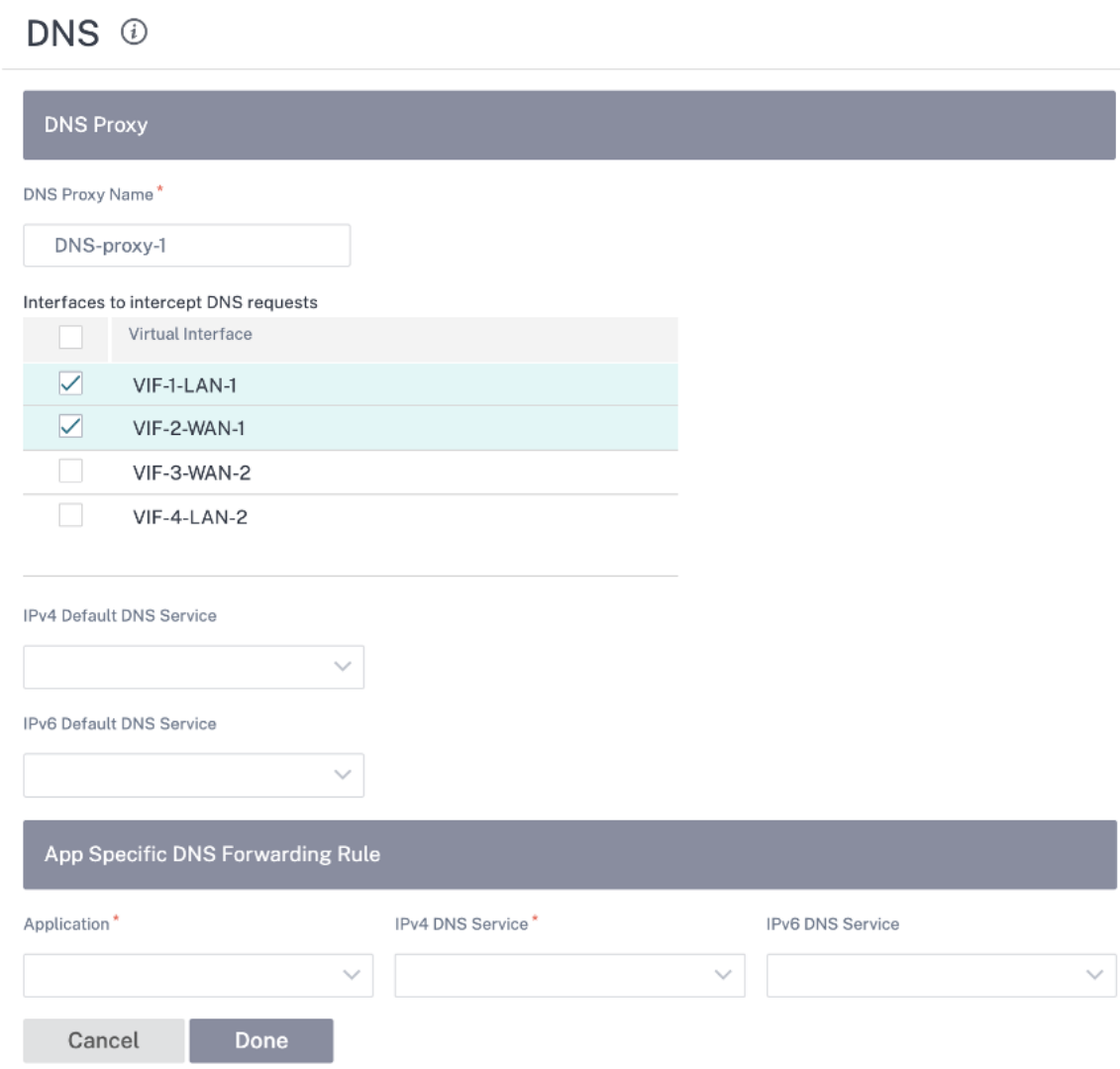
Pour configurer le service DNS dynamique, sélectionnez le **typeDynamic**(pour l'adresse IPv4) ou**DynamicV6**(pour l'adresse IPv6) et sélectionnez**Internet**pour le**type de service**et l'**instance de service**.

Les services proxy DNS correspondants sont répertoriés dans la liste déroulante **InBand Management DNS** sous **Configuration du site > Interfaces**.



Proxy DNS

Le proxy DNS intercepte les requêtes DNS destinées à l'adresse IP SD-WAN et les transmet aux serveurs DNS sélectionnés. Vous pouvez configurer un proxy avec plusieurs redirecteurs qui aide à diriger les demandes DNS en fonction des noms de domaine d'application.

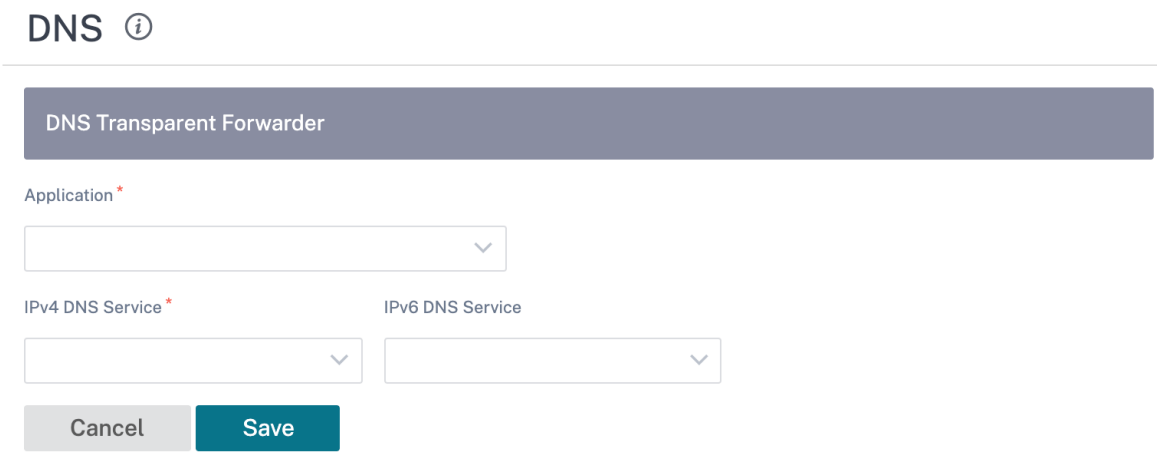


- Paramètres proxy DNS :
  - **Nom du proxy DNS** : nom du proxy DNS.
  - **Interfaces pour intercepter les requêtes DNS** : interfaces sur lesquelles les requêtes DNS sont interceptées. Seules les interfaces approuvées sont autorisées.
  - **Serveur DNS par défaut pour tout le trafic** : serveur DNS par défaut vers lequel les requêtes DNS sont transférées, si aucune des applications ne correspond dans la recherche du redirecteur DNS.
  - **Service DNS par défaut IPv4 : service**DNS IPv4 par défaut auquel les requêtes DNS sont transférées, si aucune des applications ne correspond dans la recherche du redirecteur DNS.
  - **Service DNS IPv6 par défaut : service**DNS IPv6 par défaut vers lequel les requêtes DNS sont transférées, si aucune des applications ne correspond dans la recherche du redirecteur DNS.

- Règles de transfert DNS spécifiques à l'application :
  - **Application** : Applications pour lesquelles les requêtes DNS doivent être transmises au serveur DNS sélectionné.
  - **Service DNS IPv4 : service**DNS IPv4 auquel la demande DNS est transmise pour l'application spécifiée.
  - **Service DNS IPv6** : service DNS IPv6 auquel la demande DNS est transmise pour l'application spécifiée.

Redirecteurs DNS transparents

Citrix SD-WAN peut être configuré en tant que redirecteur DNS transparent. Dans ce mode, le SD-WAN peut intercepter les requêtes DNS qui ne sont pas destinées à son adresse IP et les transmettre aux serveurs DNS spécifiés. Seules les requêtes DNS provenant du service local sur des interfaces de confiance sont interceptées. Si les requêtes DNS correspondent à des applications de la liste de redirection DNS, elles sont transférées au service DNS configuré.



- **Application** : Applications pour lesquelles les requêtes DNS doivent être transmises au serveur DNS sélectionné.
- **Service DNS IPv4 : service**DNS IPv4 auquel la demande DNS est transmise pour l'application spécifiée.
- **Service DNS IPv6** : service DNS IPv6 auquel la demande DNS est transmise pour l'application spécifiée.

Groupes de délégation de préfixes

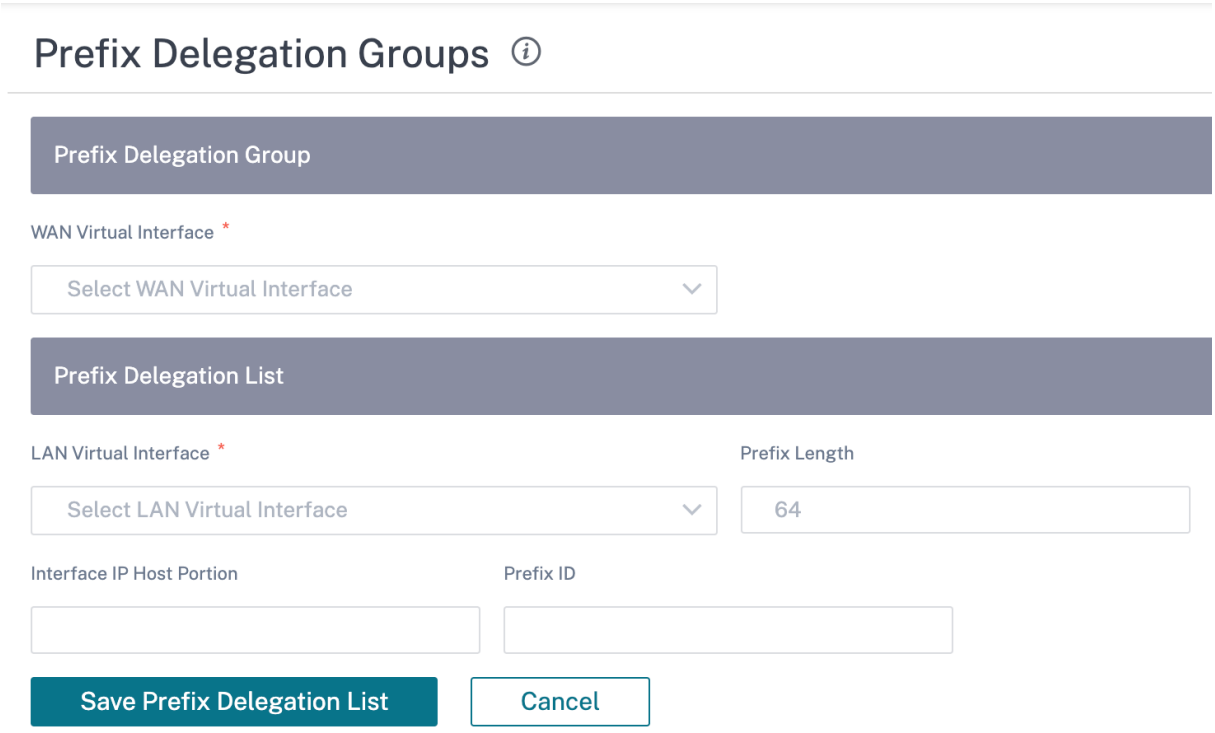
October 21, 2022

Les appliances Citrix SD-WAN peuvent être configurées en tant que client DHCPv6 pour demander un préfixe au fournisseur de services Internet à l'aide du port WAN configuré. Une fois que l'appliance Citrix SD-WAN reçoit le préfixe, elle l'utilise pour créer un pool d'adresses IP destinées aux clients du réseau local. L'appliance Citrix SD-WAN se comporte alors comme un serveur DHCP et annonce le préfixe sur les ports LAN aux clients côté LAN.

Pour configurer la délégation de préfixes, accédez à **Configuration > Paramètres avancés > Groupes de délégation de préfixes et cliquez sur + Groupesde délégation de préfixes**.

Choisissez une interface virtuelle WAN configurée sur laquelle le préfixe est demandé au fournisseur de services Internet et fournissez les informations suivantes :

- **Interface virtuelle LAN** : sélectionnez l'une des interfaces virtuelles LAN configurées pour lesquelles le préfixe est demandé.
- **Longueur du préfixe** : nombre de bits d'une adresse IPv6 monodiffusion globale qui font partie du préfixe.
- **Interface IP Host Portion** : Partie hôte à utiliser pour l'adresse IP de l'interface.
- **ID de préfixe** : identifiant unique permettant d'identifier les demandes de délégation de préfixe pour l'interface LAN.



Groupes d'agrégation de liens

October 21, 2022

La fonctionnalité de groupes d'agrégation de liens (LAG) vous permet de regrouper deux ports ou plus de votre appliance SD-WAN afin qu'ils fonctionnent ensemble comme un seul port. Cela garantit une disponibilité accrue, une redondance de liaison et des performances améliorées.

Citrix SD-WAN Orchestrator pour locaux prend en charge un groupe d'agrégation de liens simple (ACTIVE-BACKUP). Les négociations basées sur le protocole LACP 802.3ad ne sont pas prises en charge dans la version actuelle. À tout moment, un seul port est actif et les autres ports sont en mode de sauvegarde. Les supports actifs et de sauvegarde s'appuient sur le package Data Plane Development Kit (DPDK) pour la fonctionnalité LAG.

La fonctionnalité LAG n'est disponible que sur les plateformes suivantes :

- Citrix SD-WAN 110 SE
- Citrix SD-WAN 210 SE
- Citrix SD-WAN 410 SE
- Citrix SD-WAN 1100 SE/PE
- Citrix SD-WAN 2100 SE/PE
- Citrix SD-WAN 4100 SE
- Citrix SD-WAN 5100 SE/PE
- Citrix SD-WAN 6100 SE/PE

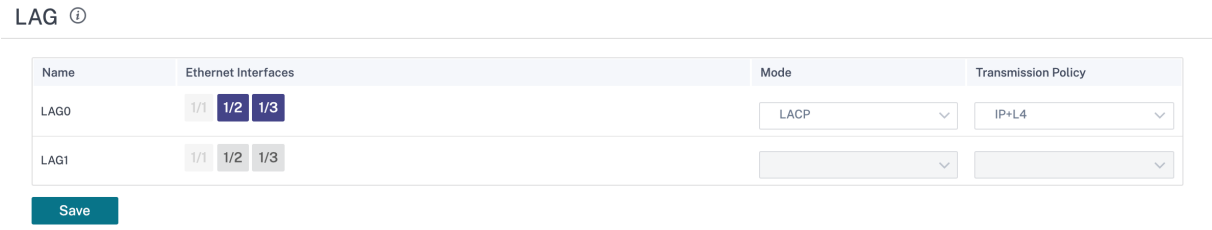
> Remarque
>
> - La fonctionnalité LAG n'est pas prise en charge sur les plates-formes VPX/VPXL.
> - Un minimum de deux ports et un maximum de quatre ports sont pris en charge par LAG.
> - Tous les membres du LAG doivent être du même type, par exemple 1/1 ou 1/2. Les configurations LAG 1/1 et 10/1 ne sont pas prises en charge.
> - La fonctionnalité LSP (Link State Propagation) n'est pas prise en charge si les LAG sont utilisés comme interfaces Ethernet dans les groupes d'interface.

Plateforme	Nombre maximum de LAG pris en charge	Ports compatibles LACP
110	1	1/1

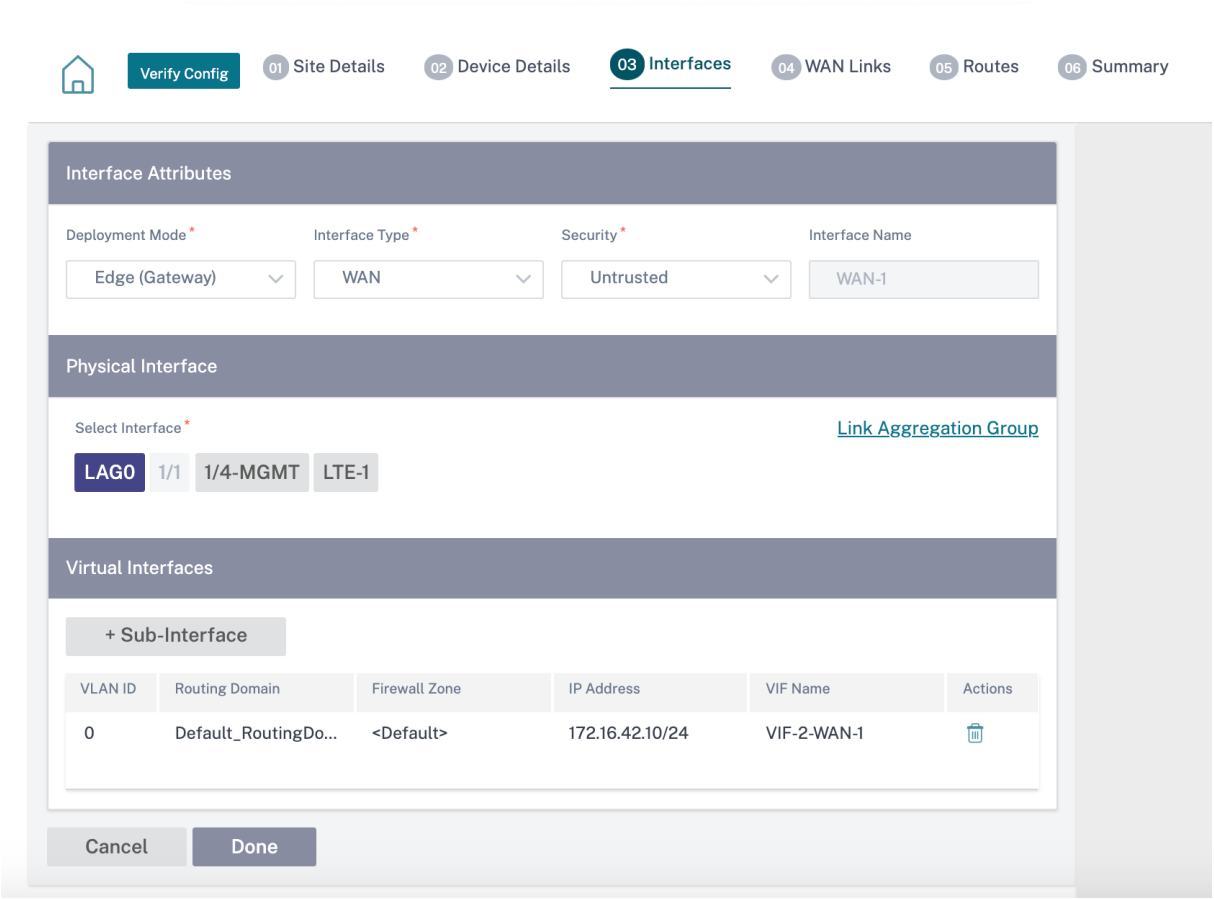
Plateforme	Nombre maximum de LAG pris en charge	Ports compatibles LACP
210	2	1/1 ou 1/2
410	1	1/1 ou 1/2
1100	3	1/1 ou 1/2
2100	3	1/1 ou 1/2
4100	4	1/1 ou 1/2
5100	3	10/1 ou 10/2

Plateforme	Nombre maximum de LAG pris en charge	Ports compatibles LACP
6100	4	1/1 ou 1/2

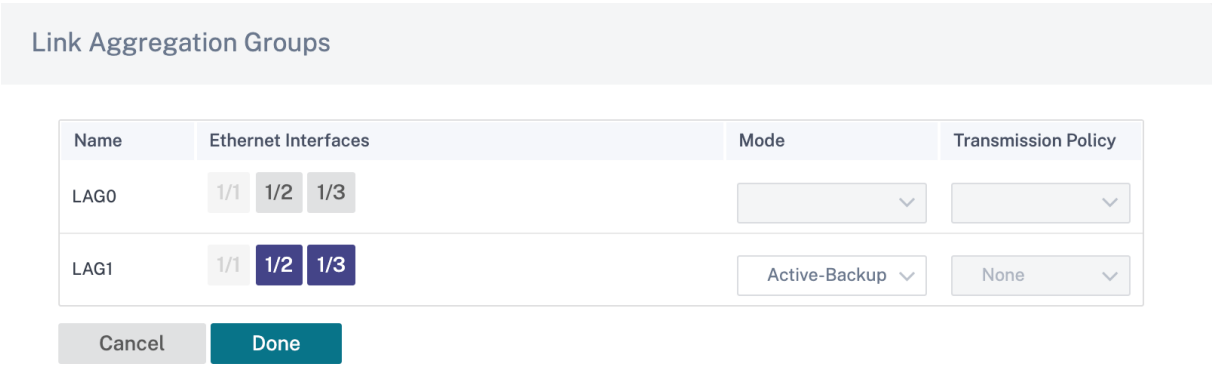
Pour configurer des groupes d'agrégation de liens, au niveau du site, accédez à **Configuration > Paramètres avancés > LAG** et sélectionnez les interfaces Ethernet membres pour former un groupe d'agrégation de liens.



Une fois les ports ajoutés au LAG, vous pouvez sélectionner les LAG pour configurer les interfaces sous **Configuration du site**. Ces interfaces sont également utilisées pour configurer les liaisons LAN/WAN et HA. Vous ne pouvez pas modifier les paramètres des ports membres individuels, les modifications de configuration apportées au LAG sont automatiquement répercutées sur les ports membres.



Dans la section **Interfaces**, cliquez sur **Groupe d'agrégation de liens** pour modifier rapidement la configuration du LAG si nécessaire.



Vous pouvez consulter les détails des interfaces configurées avec LAG et LACP sous **Rapports > Rapports sur les appliances > Groupe de LAG LACP**. Pour plus d'informations, consultez la section Rapports sur les appliances.

Paramètres de l'appliance

October 21, 2022

Le service Citrix SD-WAN Orchestrator vous permet de configurer les paramètres de l'appliance au niveau du site et de les transmettre aux appliances distantes.

Vous pouvez configurer les paramètres utilisateur, les adaptateurs réseau, NetFlow, AppFlow, SNMP, la configuration Fallback et les paramètres du flux de purge.

> **Remarque**
>
> L'option de configuration des paramètres de l'appliance n'est pas disponible lors de la création ou de la modification d'un modèle de site.

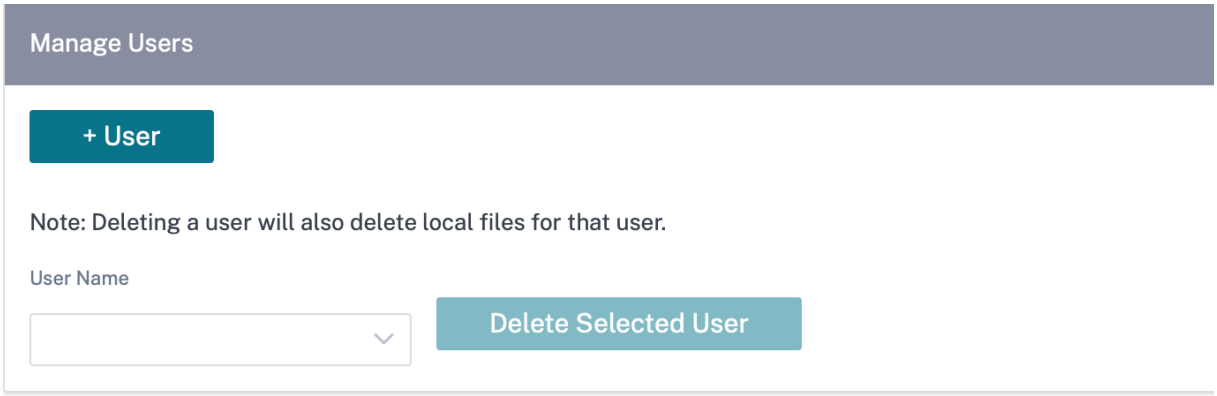
Si HA est configuré, sélectionnez l'appliance principale ou secondaire pour laquelle vous souhaitez modifier les paramètres de l'appliance.

Interface administrative

L'interface d'administration vous permet d'ajouter et de gérer les comptes d'utilisateurs locaux et distants. Les comptes d'utilisateur distant sont authentifiés via les serveurs d'authentification RADIUS ou TACACS+.

Gérer les utilisateurs

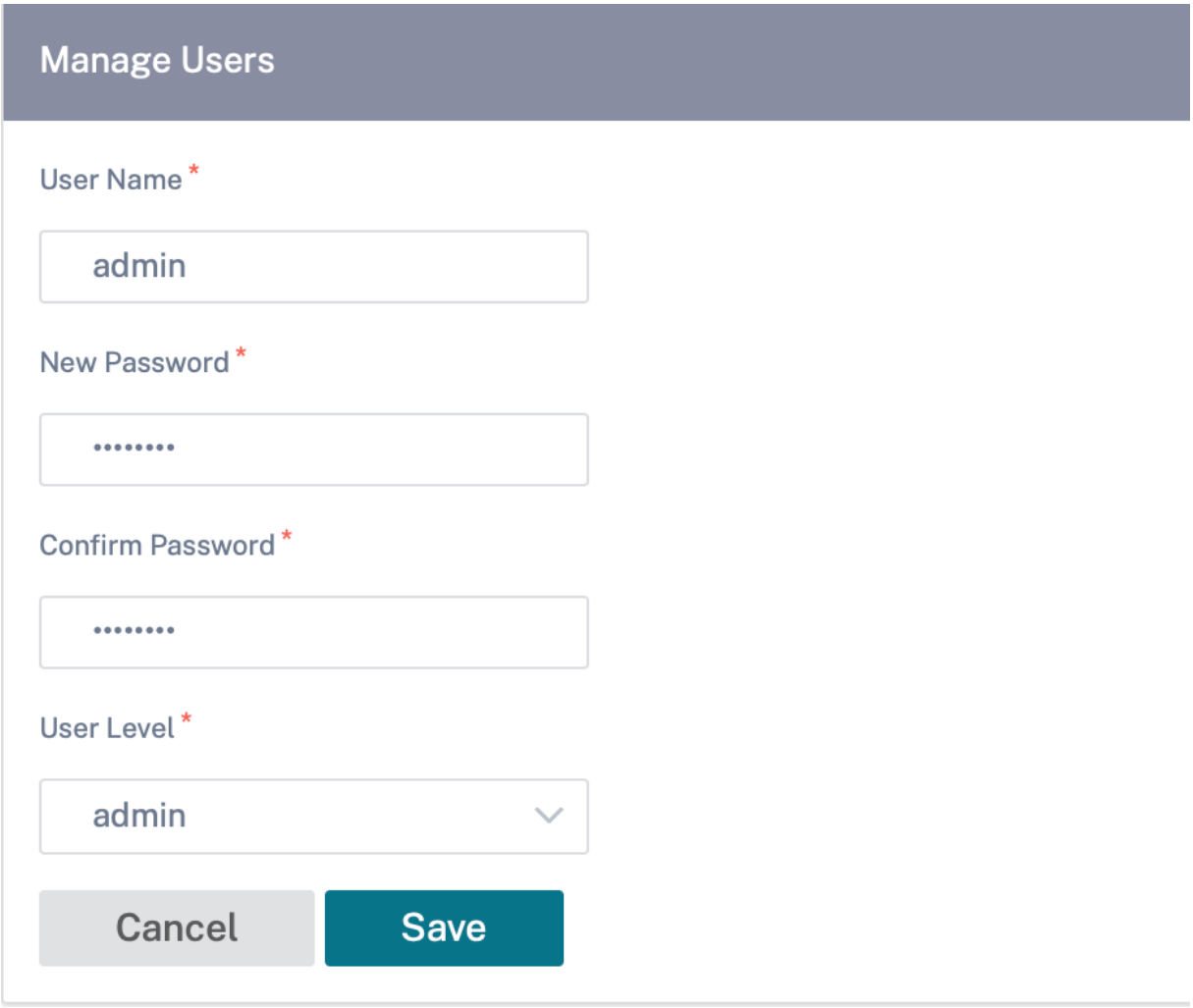
Vous pouvez ajouter de nouveaux comptes d'utilisateur pour le site. Pour ajouter un nouvel utilisateur, accédez à **Configuration** > **Paramètres de l'appliance** > **Interface administrateur** > **Gérer les utilisateurs**, puis cliquez sur **+Utilisateur**.



Fournissez les détails suivants :

- **Nom d'utilisateur** : nom d'utilisateur du compte utilisateur.
- **Nouveau mot de passe** : mot de passe du compte utilisateur.
- **Confirmer le mot de passe** : Entrez à nouveau le mot de passe pour le confirmer
- **Niveau utilisateur** : sélectionnez l'un des privilèges de compte suivants :
  - **Administrateur** : Un compte administrateur dispose d'un accès en lecture-écriture à tous les paramètres. Un administrateur peut effectuer la configuration et la mise à jour logicielle du réseau.
  - **Afficheur** : un compte Viewer est un compte en lecture seule qui permet d'accéder aux sections Tableau de bord, Rapports et Surveillance.
  - Administrateur**réseau** : un administrateur réseau dispose d'un accès en lecture-écriture aux paramètres réseau et d'un accès en lecture seule pour les autres paramètres.
  - Administrateur**de sécurité** : un administrateur de sécurité dispose d'un accès en lecture-écriture pour les paramètres liés au pare-feu/à la sécurité, d'un accès en lecture seule pour les autres paramètres.

    > **Remarque**
    >
    > L'administrateur de sécurité a le pouvoir de désactiver l'accès en écriture au pare-feu pour les autres utilisateurs (Administrateur/Viewer).

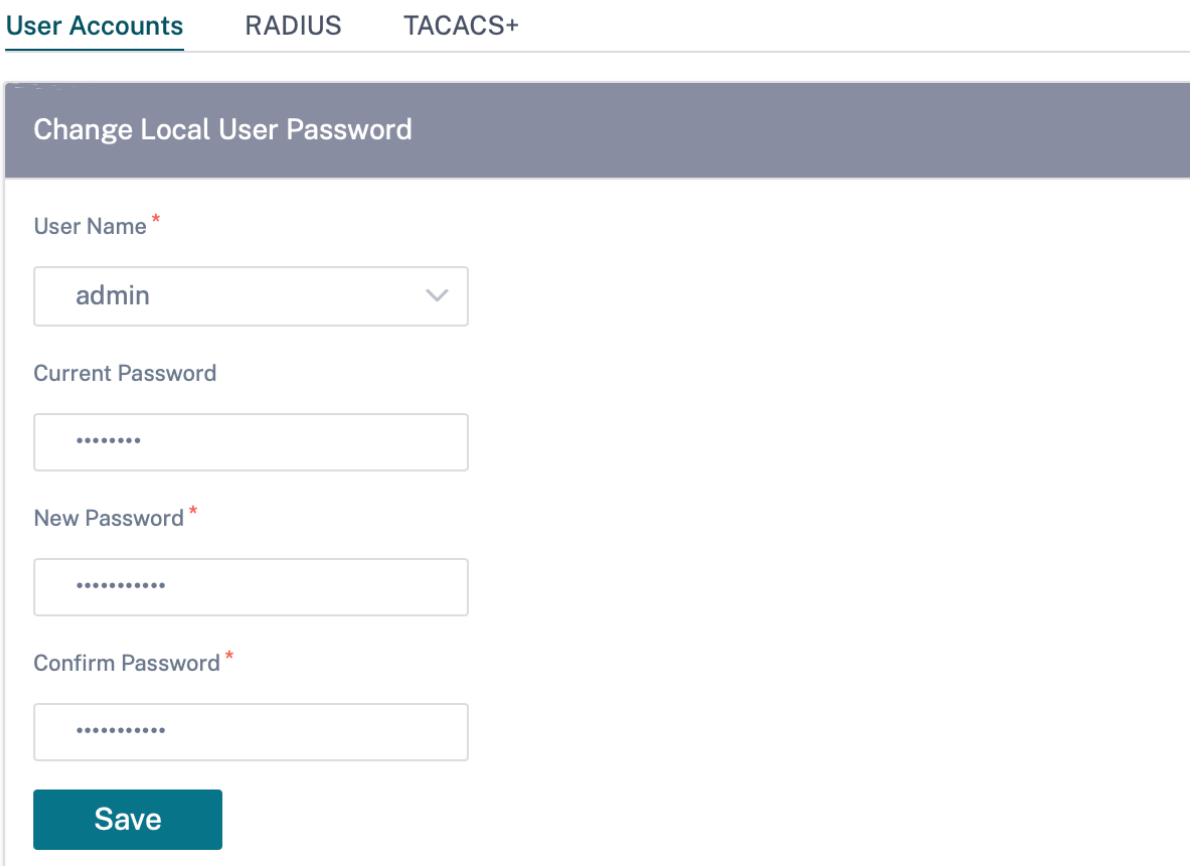


Pour supprimer un utilisateur, sélectionnez un nom d'utilisateur et cliquez sur **Supprimer l'utilisateur sélectionné**. Le compte d'utilisateur et les fichiers locaux sont supprimés.

Modifier le mot de passe utilisateur local

Pour modifier le mot de passe utilisateur local, accédez à **Configuration** > **Paramètres de l'appliance** > **Interface administrative** > **Comptes utilisateurs** > **Modifier le mot de passe utilisateur local** et entrez les valeurs suivantes :

- **Nom d'utilisateur** : sélectionnez un nom d'utilisateur pour lequel vous souhaitez modifier le mot de passe dans la liste des utilisateurs configurés sur le site.
- **Mot de passe actuel** : Entrez le mot de passe actuel. Ce champ est facultatif pour les utilisateurs administrateurs.
- **Nouveau mot de passe** : Entrez le nouveau mot de passe de votre choix.
- **Confirmer le mot de passe** : Entrez à nouveau le mot de passe pour le confirmer



Serveur d'authentification RADIUS

RADIUS active l'authentification des utilisateurs distants sur l'appliance. Pour utiliser l'authentification RADIUS, vous devez spécifier et configurer au moins un serveur RADIUS. Vous pouvez également configurer des serveurs RADIUS de sauvegarde redondants, jusqu'à un maximum de trois. Les serveurs sont vérifiés séquentiellement. Assurez-vous que les comptes d'utilisateur requis sont créés sur le serveur d'authentification RADIUS.

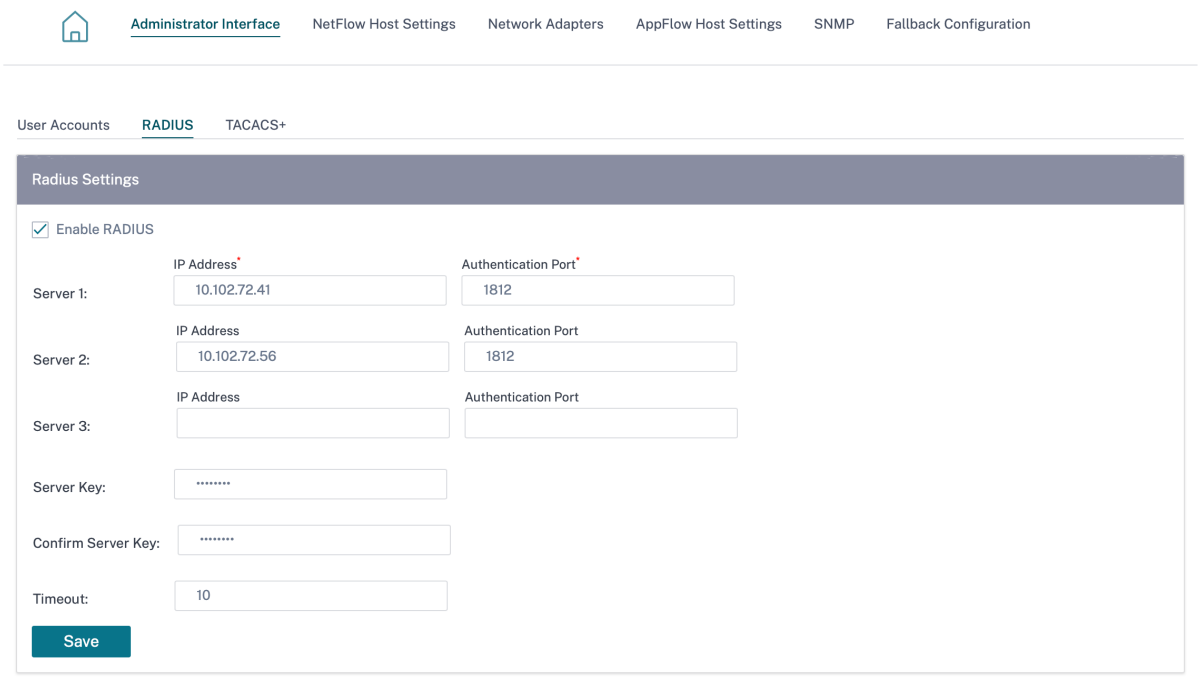
Pour configurer l'authentification RADIUS, accédez à **Configuration** > **Paramètres du dispositif** > **Interface administrative** > **RADIUS**, puis cliquez sur **Activer RADIUS**.

> **Remarque**
>
> Vous pouvez activer l'authentification RADIUS ou TACACS+ sur un site. Vous ne pouvez pas activer les deux en même temps.

Indiquez l'adresse IP de l'hôte du serveur RADIUS et le numéro de port d'authentification. Le numéro de port par défaut est 1812. Entrez une clé Serveur et confirmez-la, il s'agit d'une clé secrète utilisée pour se connecter au serveur RADIUS. Spécifiez l'intervalle de temps d'attente pour une réponse d'

authentification du serveur RADIUS. La valeur du délai d'attente doit être inférieure ou égale à 60 secondes.

> **Remarque**
>
> Les paramètres de **clé de serveur** et **de délai** d'expiration sont appliqués à tous les serveurs configurés.



Serveur d'authentification TACACS+

TACACS+ permet l'authentification des utilisateurs distants sur l'appliance. Pour utiliser l'authentification TACACS+, vous devez spécifier et configurer au moins un serveur TACACS+. Vous pouvez également configurer des serveurs TACACS+ de sauvegarde redondants, jusqu'à trois au maximum. Les serveurs sont vérifiés séquentiellement. Assurez-vous que les comptes utilisateur requis sont créés sur le serveur d'authentification TACACS+.

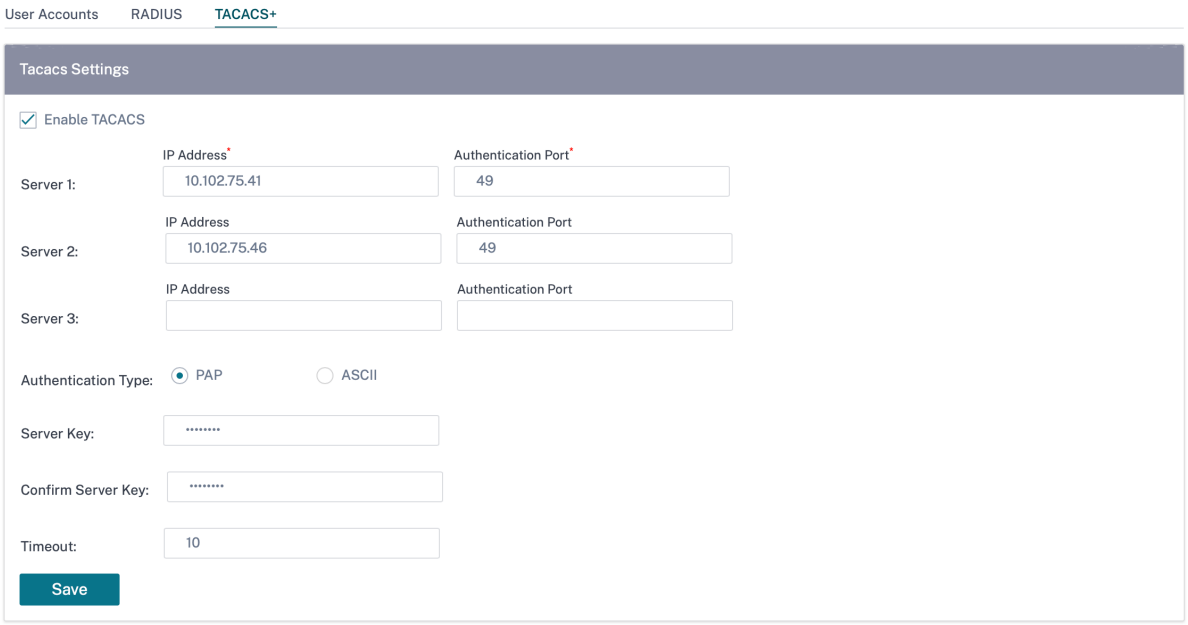
Pour configurer l'authentification TACACS+, accédez à **Configuration** > **Paramètres de l'appliance** > **Interface administrative** > **TACACS+** et cliquez sur **Activer TACACS+**.

> **Remarque**
>
> Vous pouvez activer l'authentification RADIUS ou TACACS+ sur un site. Vous ne pouvez pas activer les deux en même temps.

1. Sélectionnez la méthode de chiffrement pour envoyer le nom d'utilisateur et le mot de passe au serveur TACACS+.

2. Indiquez l'adresse IP de l'hôte du serveur TACACS+ et le numéro de port d'authentification. Le numéro de port par défaut est 49.
3. Entrez une clé de serveur et confirmez-la. Il s'agit d'une clé secrète utilisée pour se connecter au serveur TACACS+.
4. Spécifiez l'intervalle de temps d'attente pour une réponse d'authentification du serveur TACACS+. La valeur du délai d'attente doit être inférieure ou égale à 60 secondes.

> **Remarque**
>
> Les **paramètres du**type d'authentification**, de la**clé du serveur**et du délai** d'expiration sont appliqués à tous les serveurs configurés.



Paramètres de l'hôte NetFlow

Les collecteurs NetFlow collectent le trafic réseau IP lorsqu'il entre ou quitte une interface SD-WAN. Vous pouvez déterminer la source et la destination du trafic, la classe de service et les causes de la congestion du trafic à l'aide des données NetFlow. Pour plus d'informations, consultez Multiple NetFlow Collector.

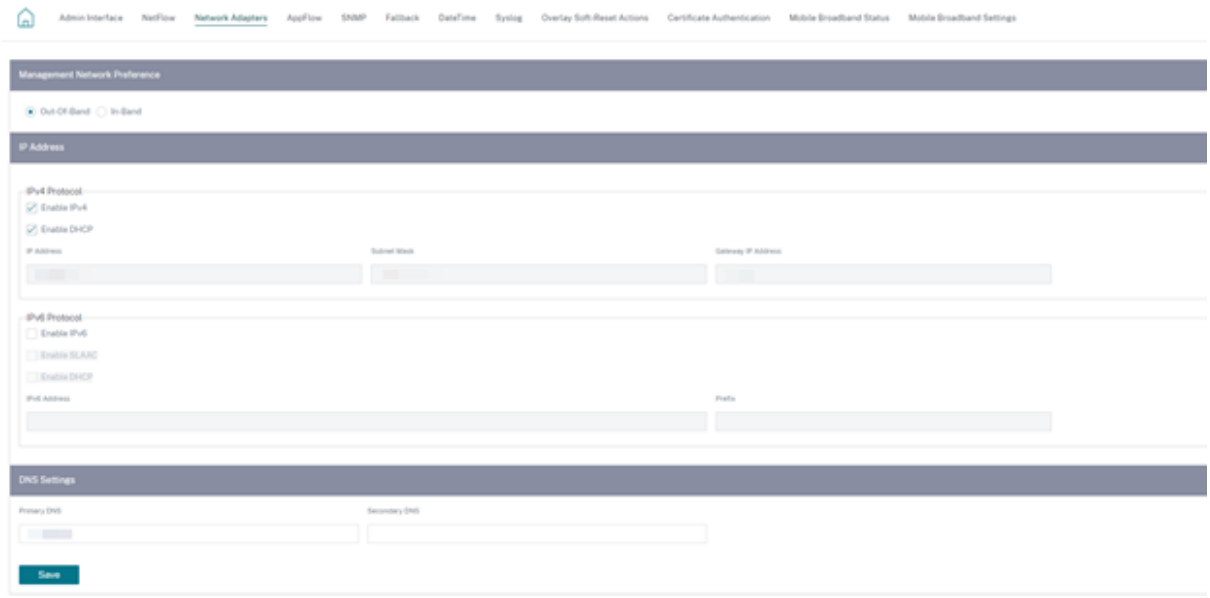
Vous pouvez configurer jusqu'à trois hôtes NetFlow. Pour configurer les paramètres d'hôte NetFlow, accédez à **Configuration** > Paramètres de **l'appliance > Paramètres** de l'**hôte NetFlow**. Sélectionnez **Activer NetFlow** et fournissez l'adresse IP et le numéro de port de l'hôte NetFlow.

Cartes réseau

Pour les appliances Citrix SD-WAN, vous pouvez modifier manuellement les préférences du réseau de gestion, l'adresse IP de gestion et d'autres paramètres réseau. Vous pouvez modifier l'adresse IPv4, le masque de sous-réseau, l'adresse IP de la passerelle, l'adresse IPv6 et le préfixe de l'appliance ou obtenir l'adresse IP automatiquement en activant DHCP ou SLAAC (uniquement pour les adresses IPv6). Pour plus d'informations, consultez la section Protocole de configuration dynamique de l'hôte.

> **Remarque**
>
> - Vous ne pouvez pas modifier l'adresse IP si l'interface est utilisée pour la gestion intrabande. Pour plus d'informations sur la gestion intrabande, voir Gestion intrabande.
> - L'option In-band ne fonctionne que si vous avez configuré un port de données en tant que port de gestion intrabande et si le service Internet est configuré. Assurez-vous que vous disposez de la configuration nécessaire pour prendre en charge la gestion intrabande pour l'appliance SD-WAN, avant de définir les préférences de gestion.
> - La section Préférences du réseau de gestion (intrabande et hors bande) est visible si l'appliance exécute une version logicielle de la version 11.4.2 ou ultérieure.

Pour configurer les paramètres de l'adaptateur réseau, accédez à **Configuration** > **Paramètres de l'appliance** > **Adaptateur réseau**.



Paramètres de l'hôte AppFlow

AppFlow et IPFIX sont des normes d'exportation de flux utilisées pour identifier et collecter des données d'application et de transaction dans l'infrastructure réseau. Ces données offrent une meilleure visibilité sur l'utilisation et les performances du trafic des applications.

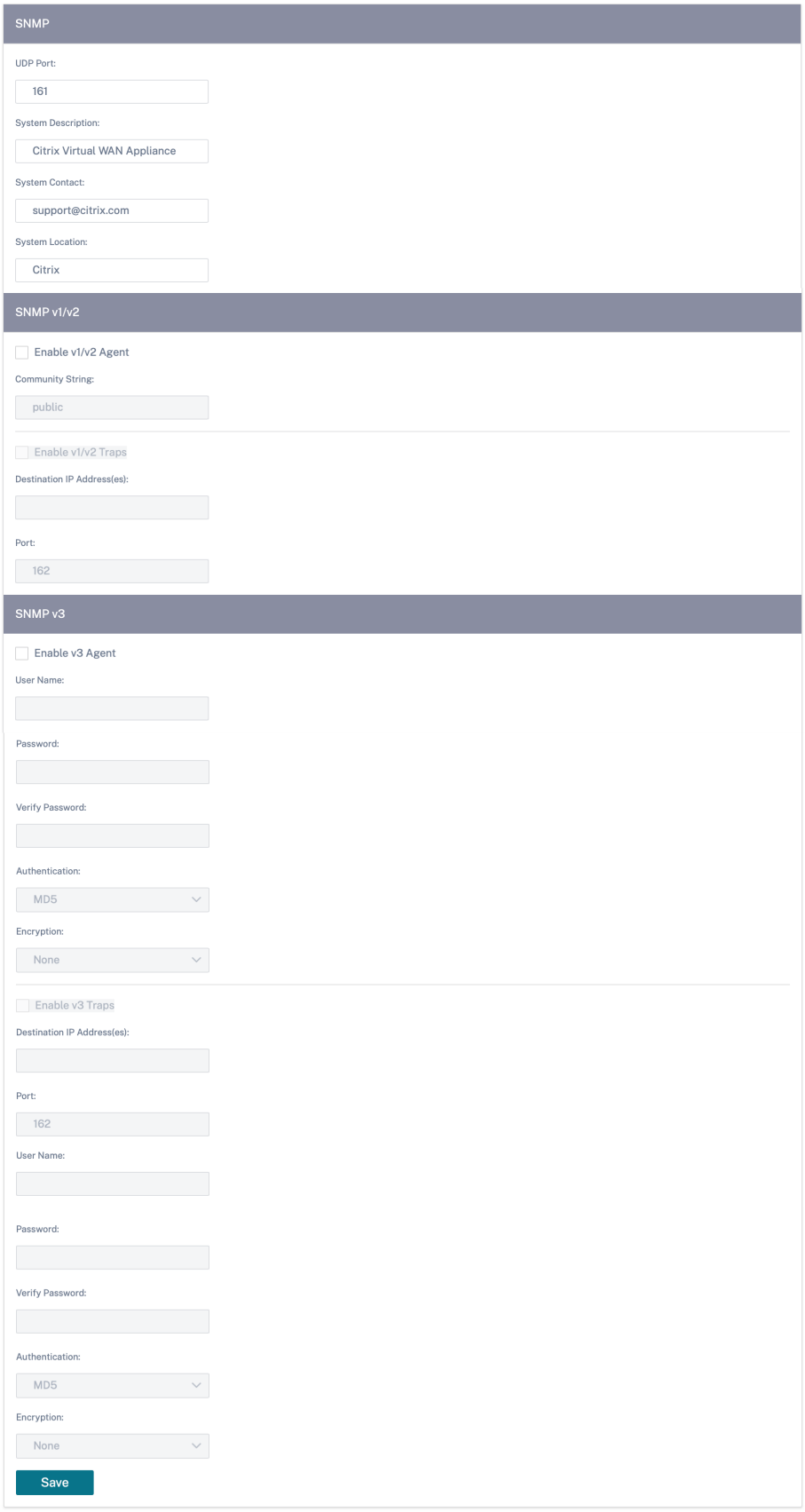
Les données collectées, appelées enregistrements de flux, sont transmises à un ou plusieurs collecteurs IPv4. Les collecteurs regroupent les enregistrements de flux et génèrent des rapports en temps réel ou historiques. Pour plus d'informations, consultez AppFlow et IPFIX.

SNMP

SNMP est utilisé pour échanger des informations de gestion entre les périphériques réseau. SNMPv1 est la première version du protocole SNMP. SNMPv2 est le protocole révisé, qui inclut des améliorations dans les types de paquets de protocole, les mappages de transport et les éléments de structure MIB. SNMPv3 définit la version sécurisée du SNMP. Le protocole SNMPv3 facilite également la configuration à distance des entités SNMP.

L'agent SNMP collecte localement les informations de gestion de l'appliance et les envoie au gestionnaire SNMP chaque fois qu'elles sont interrogées. Si l'agent détecte un événement d'urgence sur l'appliance, il envoie un message d'avertissement au gestionnaire sans attendre que les données soient interrogées. Ce message d'urgence s'appelle un piège. Activez les agents de version SNMP requis, les interruptions correspondantes et fournissez les informations requises. Pour plus de détails, reportez-vous à SNMP.

Pour configurer les paramètres SNMP, accédez à **Configuration** > **Paramètres de l'appliance** > **SNMP**

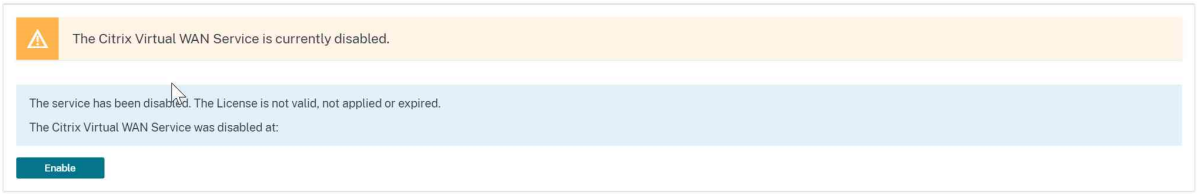


Configuration de secours

La configuration de secours garantit que l'appliance reste connectée au service de déploiement zéro contact en cas de panne de liaison, d'incompatibilité de configuration ou d'incompatibilité logicielle. La configuration de secours est activée par défaut sur les appliances disposant d'un profil de configuration par défaut. Vous pouvez également modifier la configuration de secours en fonction de vos paramètres réseau LAN existants. Pour plus d'informations, consultez la section Configuration de repli.

Flux

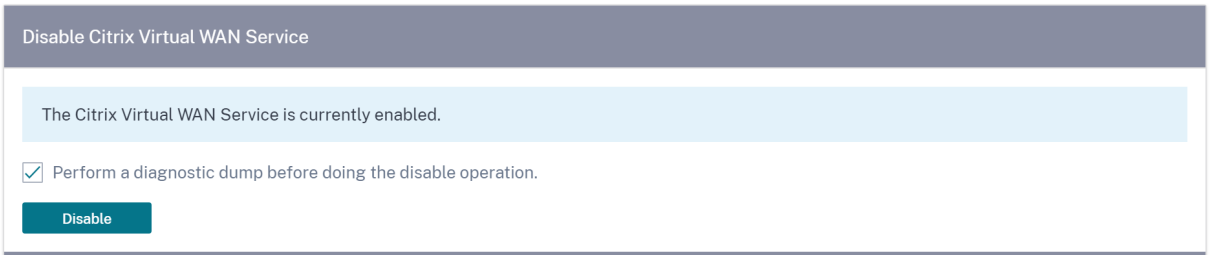
La section des flux vous permet d'activer ou de désactiver le service Citrix Virtual WAN sur l'appliance. L'activation du service active et démarre le démon Virtual WAN. Une option permettant d'activer le service Citrix Virtual Wan est disponible si le service est désactivé.



Désactiver le service Citrix Virtual WAN

L'option **Désactiver le service Citrix Virtual WAN** est disponible si le service est activé. La désactivation du service arrête le démon Virtual WAN sur l'appliance.

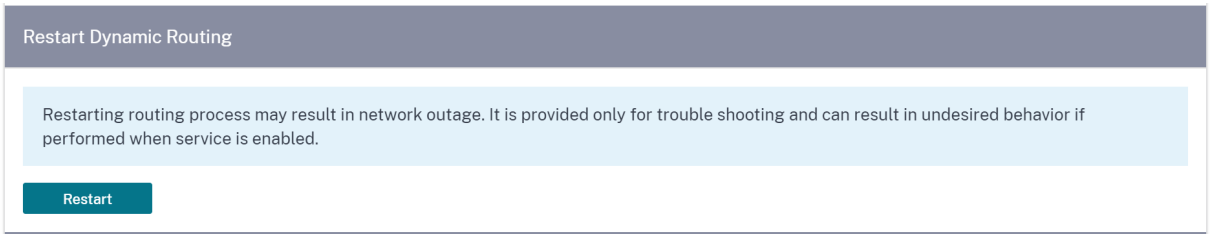
Vous pouvez choisir de collecter un fichier de diagnostic du réseau Virtual WAN avant de désactiver le service Citrix Virtual WAN.



Redémarrer le routage dynamique

Vous pouvez redémarrer le processus d'apprentissage dynamique des itinéraires via les protocoles de routage OSPF et BGP. L'option de redémarrage du routage dynamique est fournie à des fins de dépannage uniquement.

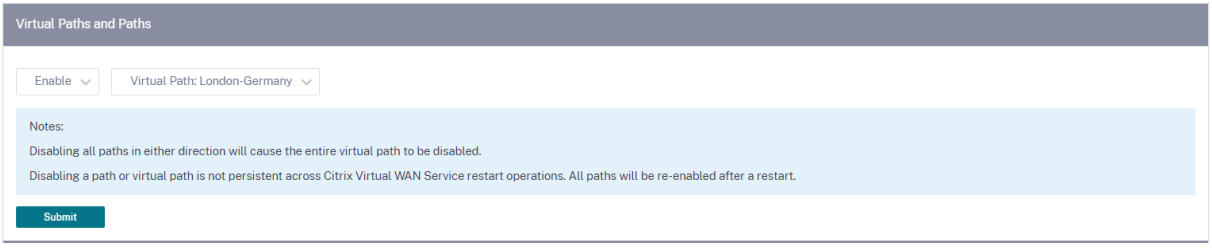
> **Avertissement**
>
> Le redémarrage du routage dynamique peut entraîner une panne du réseau.



Chemins virtuels

Vous pouvez choisir d'activer ou de désactiver le chemin virtuel entre deux sites. Vous pouvez choisir les chemins individuels sous-jacents, dans les deux sens, ou le chemin virtuel de superposition. La désactivation de chemins individuels désactive l'ensemble du chemin virtuel.

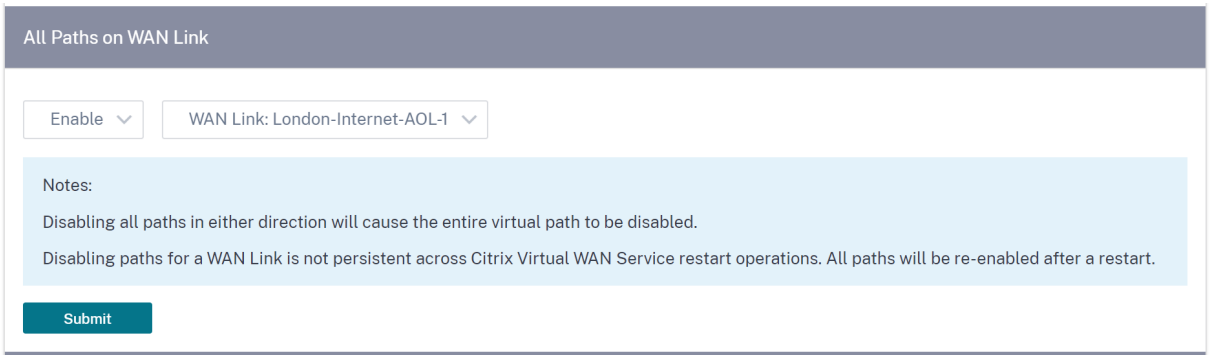
> **Remarque**
>
> Tous les chemins sont réactivés après le redémarrage du service Citrix Virtual WAN.



Tous les chemins sur la liaison WAN

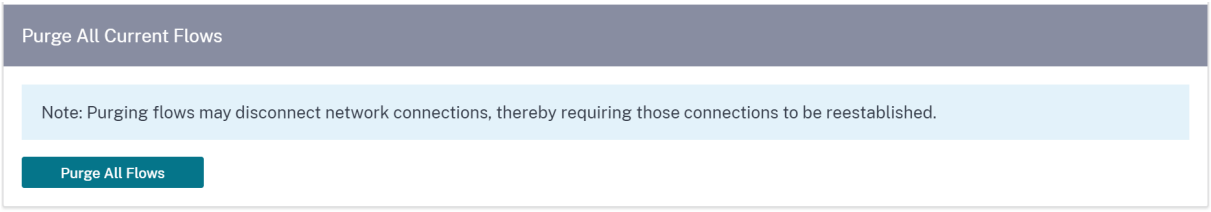
Vous pouvez choisir d'activer ou de désactiver les liaisons WAN entre 2 sites. Désactiver toutes les liaisons WAN, désactive le chemin virtuel.

> **Remarque**
>
> Toutes les liaisons WAN sont réactivées après le redémarrage du service Citrix Virtual WAN.



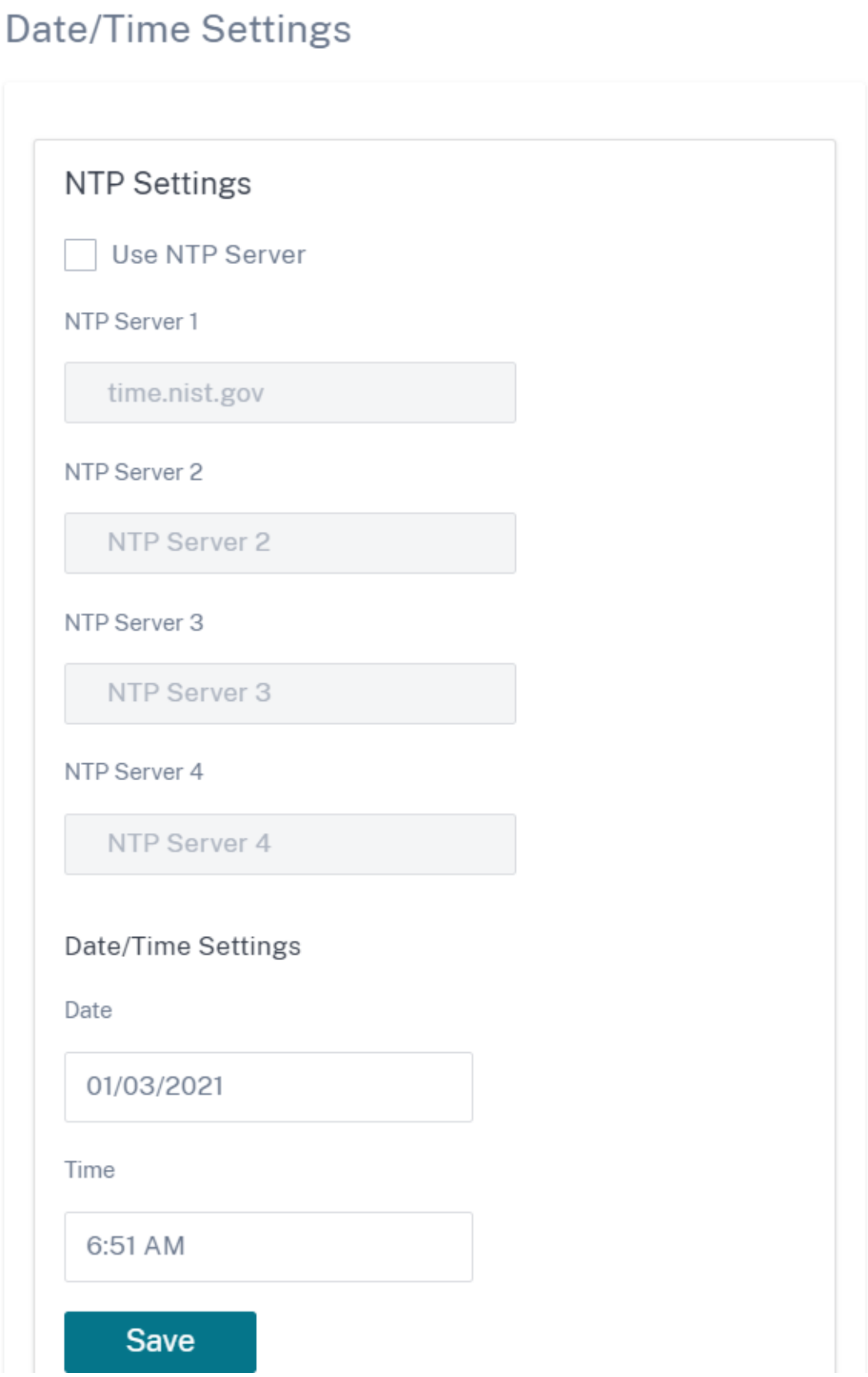
Purger tous les flux de courant

La purge des flux met fin à tous les flux de courant, efface les tables de flux, rétablit les connexions de flux et renseigne la table de flux.

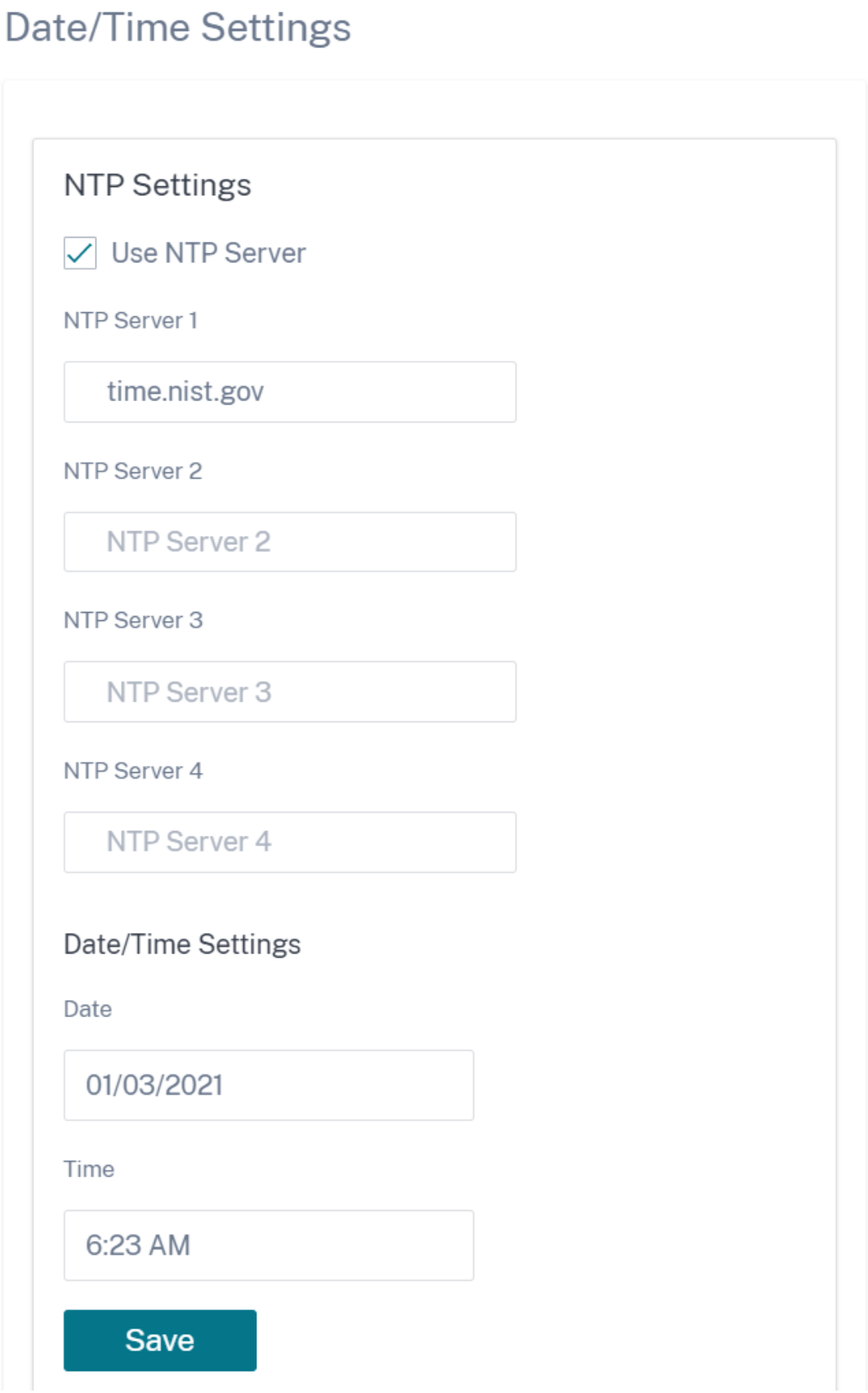


Date et heure

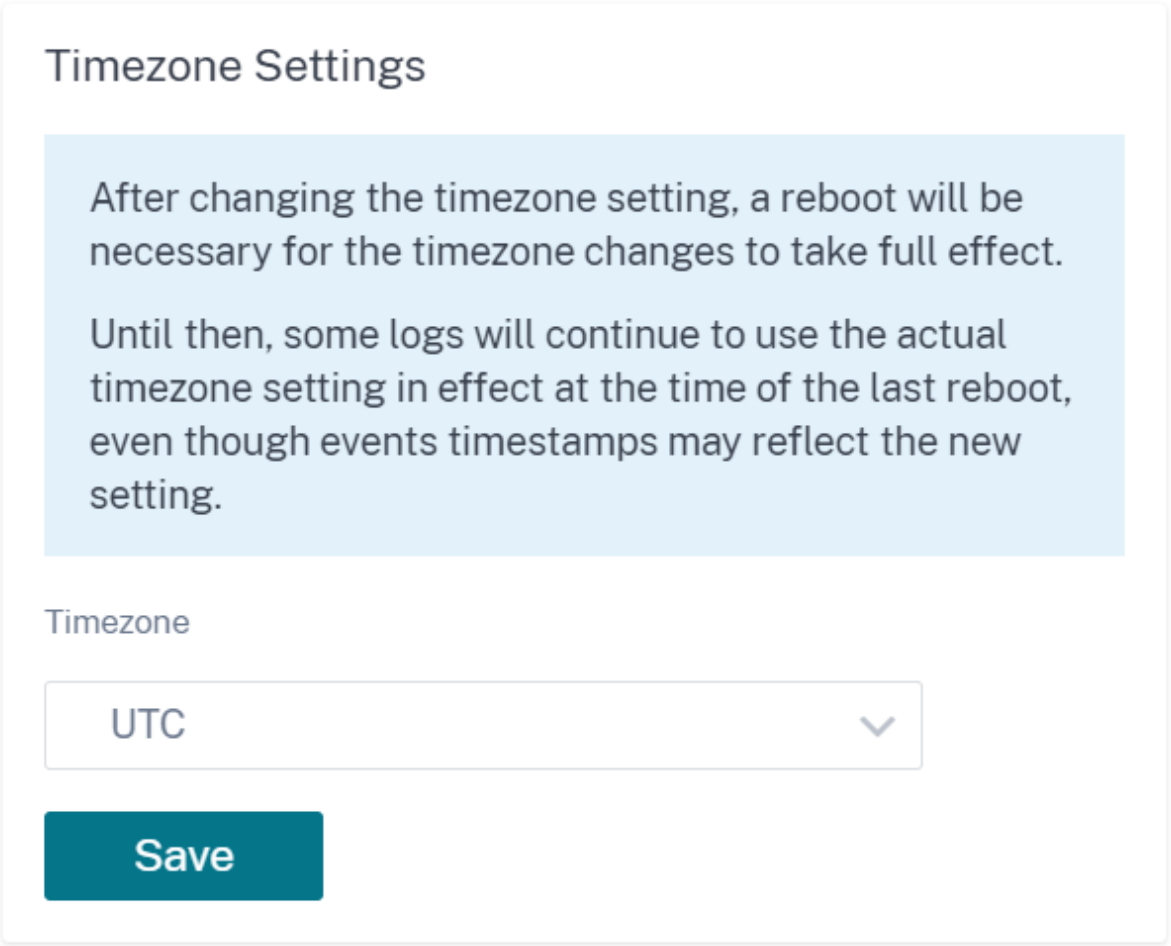
Vous pouvez modifier la date et l'heure de l'appliance manuellement ou à l'aide d'un serveur NTP. Pour configurer la date et l'heure manuellement, assurez-vous que l'option **Utiliser un serveur NTP** n'est pas sélectionnée et indiquez la date et l'heure.



Si vous sélectionnez l'option **Utiliser un serveur NTP**, vous ne pouvez pas saisir manuellement la date et l'heure actuelles. Vous pouvez spécifier jusqu'à 4 serveurs NTP, mais vous devez en spécifier au moins un. Ils agissent comme des serveurs NTP de sauvegarde. Si l'un des serveurs est en panne, l'appliance se synchronise automatiquement avec l'autre serveur NTP. Si vous spécifiez un nom de domaine pour un serveur NTP, vous devez également configurer un serveur DNS, sauf si vous l'avez déjà fait.

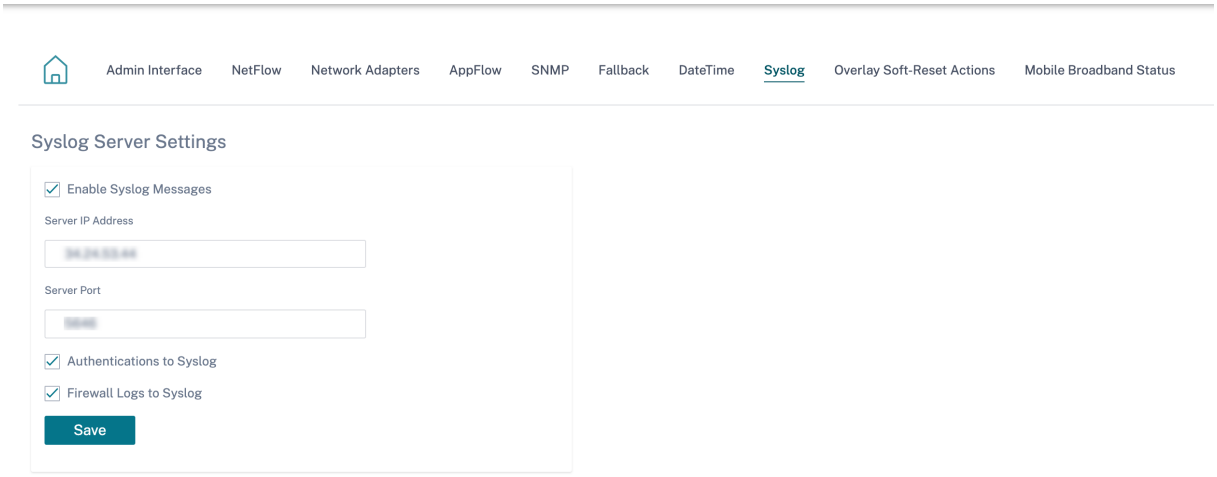


Si le fuseau horaire doit être modifié, modifiez-le avant de régler la date et l'heure, sinon vos paramètres ne seront pas conservés. Redémarrez l'appliance après avoir modifié le fuseau horaire.



Paramètres du serveur Syslog

Vous pouvez configurer les paramètres du serveur Syslog des appliances SD-WAN à l'aide du service Citrix SD-WAN Orchestrator. En activant les paramètres Syslog, vous pouvez envoyer des alertes système et les détails des événements des appliances SD-WAN à un serveur Syslog externe. Toutefois, vous devez sélectionner le type d'événement sur l'interface utilisateur de l'appliance SD-WAN en accédant à **Configuration** > **Paramètres de l'appliance** > **Journalisation/surveillance** > **Options d'alarme**. Pour plus d'informations, voir Configuration des alarmes.



Les paramètres de serveur Syslog suivants sont configurables via le service Citrix SD-WAN Orchestrator :

- **Activer les messages Syslog** : active ou désactive l'envoi de journaux ou de messages d'événements au serveur Syslog.
- **Adresse IP du serveur** : adresse IP du serveur Syslog.
- **Port du serveur** : numéro de port du serveur Syslog.
- **Authentification auprès de Syslog** : active ou désactive l'envoi de journaux d'authentification ou de messages d'événements au serveur Syslog.
- **Journaux de pare-feu vers Syslog** : activez ou désactivez l'envoi de journaux de pare-feu au serveur Syslog.

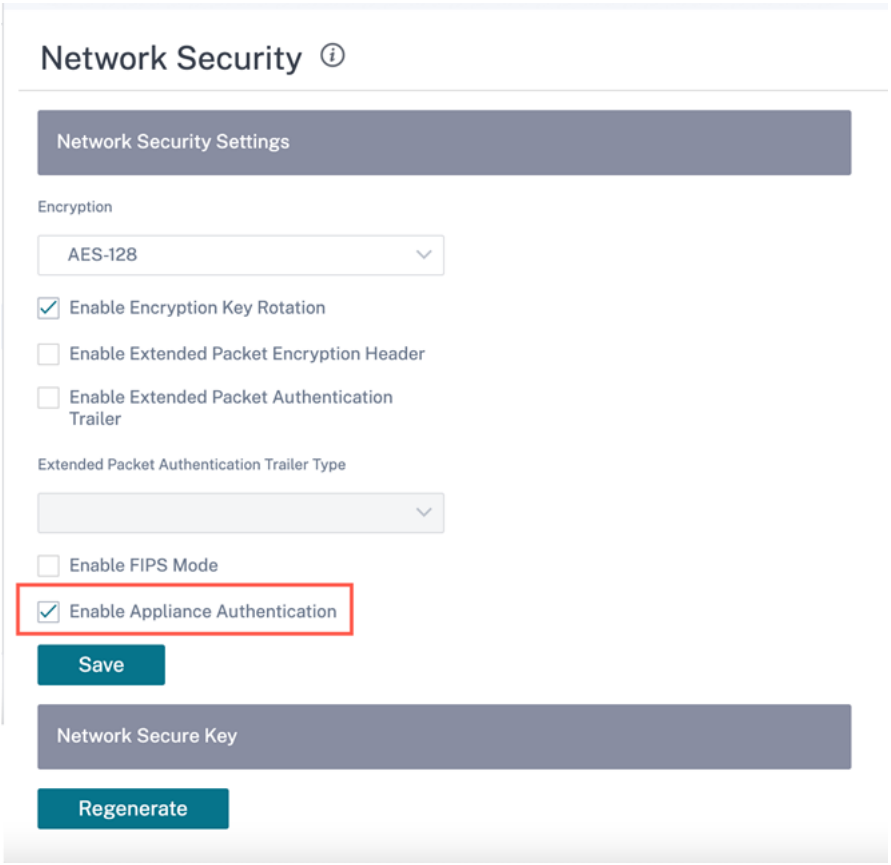
Authentification du certificat

Le service Citrix SD-WAN Orchestrator garantit que des chemins sécurisés sont établis entre les appliances du réseau SD-WAN à l'aide de techniques de sécurité telles que le chiffrement du réseau et les tunnels IPsec à chemin virtuel. Outre les mesures de sécurité existantes, l'authentification basée sur des certificats est introduite dans le service Citrix SD-WAN Orchestrator.

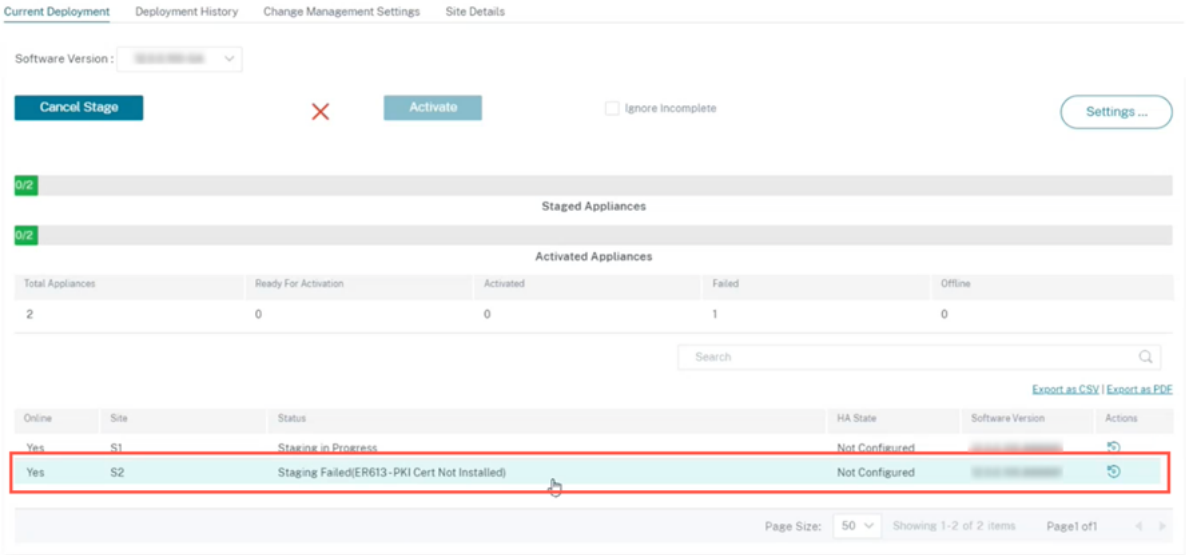
L'authentification par certificat permet aux organisations d'utiliser des certificats émis par leur autorité de certification (CA) privée pour authentifier les appliances. Les appliances sont authentifiées avant d'établir les chemins virtuels. Par exemple, si un dispositif de branche tente de se connecter au centre de données et que le certificat de la branche ne correspond pas au certificat attendu par le centre de données, le chemin d'accès virtuel n'est pas établi.

Le certificat émis par l'autorité de certification lie une clé publique au nom de l'appliance. La clé publique fonctionne avec la clé privée correspondante possédée par l'appliance identifiée par le certificat.

Pour activer l'authentification de l'appliance, au niveau du réseau, accédez à **Configuration** > **Sécurité > Sécuritéréseau**et sélectionnez**Activer l'authentification de l'appliance**. Cliquez sur**Enregistrer**.

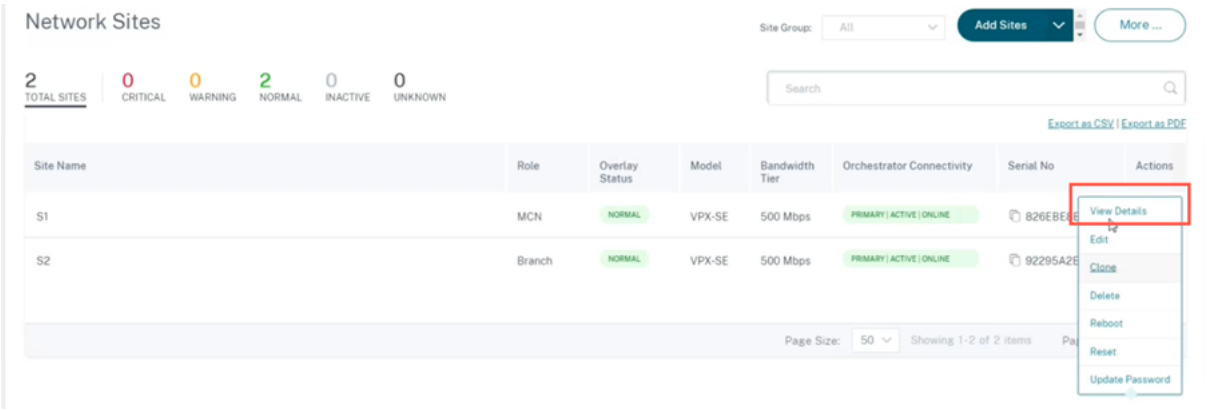


Pendant le déploiement, si l'authentification de l'appliance est activée mais qu'aucun certificat PKI n'est installé sur l'appliance, le test indique l'état d'échec.

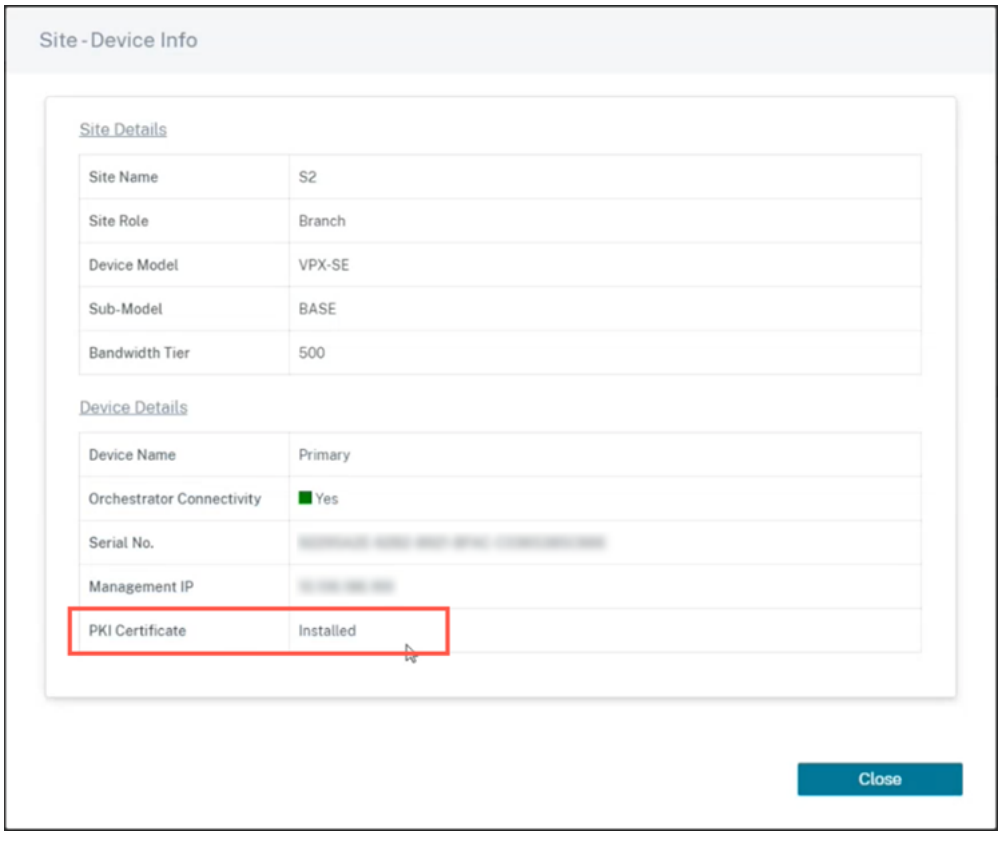


Voir le certificat

Vous pouvez accéder à la page détaillée de l'appareil pour vérifier si le certificat PKI est installé ou non. Pour ce faire, accédez à **Configuration** > **Accueil du réseau**, cliquez sur le symbole **d'action** correspondant au site sur lequel vous souhaitez vérifier le certificat, puis cliquez sur **Afficher les détails**.



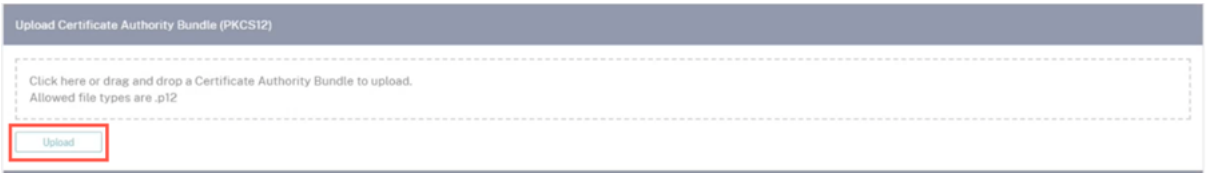
L'écran suivant affiche les détails du site et de l'appareil :



Dans la section **Détails du périphérique**, vous pouvez consulter l'état de l'installation du certificat PKI.

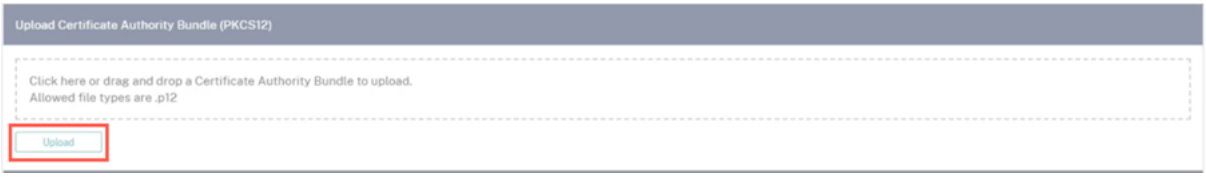
Charger le bundle d'identité

Le bundle Identity inclut une clé privée et le certificat associé à la clé privée. Vous pouvez télécharger le certificat de l'appliance émis par l'autorité de certification dans l'appliance. Le bundle de certificats est un fichier PKCS12, avec l'extension .p12. Vous pouvez choisir de le protéger avec un mot de passe. Glissez et déposez le fichier PKCS12, entrez un mot de passe et cliquez sur **Télécharger**. Si vous laissez le champ du mot de passe vide, il est considéré comme n'étant pas protégé par mot de passe.



Charger le bundle d'autorité de certification

Téléchargez le bundle PKCS12 qui correspond à l'autorité de signature du certificat. Le bundle d'autorités de certification inclut la chaîne complète de signatures, la racine et toutes les autorités de signature intermédiaires. Faites glisser le bundle PKCS12 et cliquez sur **Télécharger**.



Créer une demande de signature de certification

L'appliance peut générer un certificat non signé et créer une demande de signature de certificat (CSR). Pour créer un CSR pour un appareil, saisissez le nom de l'organisation, l'unité, la ville/la ville, la province/la région/le comté/la ville, le pays et l'adresse e-mail. Le nom commun de l'appliance est le nom du site qui est renseigné automatiquement et non modifiable. Cliquez sur **Créer un CSR**.

Gérer la demande de signature de certificat

Une fois le CSR généré avec succès à partir du back-end, vous devez le télécharger depuis l'appliance et le faire signer par son autorité de certification, puis le télécharger à nouveau sur l'appliance aux formats PEM ou DER. Il est utilisé comme certificat d'identité pour l'appliance. Téléchargez d'abord l'autorité de certification pour signer le certificat.

Une fois l'autorité de certification téléchargée, téléchargez le CSR signé.

Gestionnaire de liste de révocation de certificats

Une liste de révocation de certificats (LCR) est une liste publiée de numéros de série de certificats qui ne sont plus valides sur le réseau. Le fichier CRL est régulièrement téléchargé et stocké localement sur toute l'appliance. Lorsqu'un certificat est authentifié, le répondeur examine la liste de révocation pour voir si le certificat d'initiateurs a déjà été révoqué. Citrix SD-WAN prend actuellement en charge les LCR version 1 au format PEM et DER.

Pour activer la CRL, cochez la case CRL activée. Indiquez l'emplacement où le fichier de liste de révocation de révocation de révocation est Les emplacements HTTP, HTTPS et FTP sont pris en charge. Spécifiez l'intervalle de temps pour vérifier et télécharger le fichier CRL, la plage est de 1 à 1440 minutes. Cliquez sur **Paramètres de téléchargement**.

> **Remarque**
>
> La période de réauthentification pour un chemin virtua1 peut être comprise entre 10 et 15 minutes. Si l'intervalle de mise à jour des CRL est défini sur une durée plus courte, la liste des CRL mise à jour peut inclure un numéro de série actuellement actif. Mettez un certificat révoqué activement à disposition sur votre réseau pendant une courte durée.

Paramètres du haut débit mobile

Le service Citrix SD-WAN Orchestrator vous permet de connecter une appliance Citrix SD-WAN depuis votre site de succursale à un réseau via une connexion haut débit mobile.

Pour configurer les paramètres du haut débit mobile, au niveau du site, accédez à **Configuration** > Paramètres de **l'appliance > Paramètres** du **haut débit mobile**.

Actuellement, les paramètres du haut débit mobile peuvent être configurés sur les appliances Citrix SD-WAN 110 et Citrix SD-WAN-210.

Vous pouvez configurer les paramètres de haut débit mobile suivants sur le service Citrix SD-WAN Orchestrator.

État du code PIN de

Si vous avez inséré une carte SIM verrouillée par un code PIN, l'état de la carte SIM est **Activé**. Vous ne pouvez pas utiliser la carte SIM tant qu'elle n'est pas vérifiée à l'aide du code PIN SIM. Vous pouvez obtenir le code PIN de la carte SIM auprès du transporteur. Cliquez sur **Vérifier**.

Entrez le code PIN de la carte SIM fourni par le transporteur et cliquez sur **Vérifier**.

Désactiver le PIN SIM Vous pouvez désactiver la fonctionnalité de code PIN pour une carte SIM pour laquelle le code PIN de la carte SIM est activé et vérifié. Cliquez sur **Désactiver**. Entrez le code PIN de la carte SIM et cliquez sur **Désactiver**

Activer le PIN SIM Pour activer le code PIN de la carte SIM, cliquez sur **Activer**. Entrez le code PIN de la carte SIM fourni par le transporteur et cliquez sur **Activer**.

Si l'état du code PIN de la carte SIM passe à **Activé et Non vérifié**, cela signifie que le code PIN n'est pas vérifié et que vous ne pouvez effectuer aucune opération tant que le code PIN n'est pas vérifié.

Cliquez sur **Vérifier le code PIN**. Entrez le code PIN de la carte SIM fourni par l'opérateur et cliquez sur **Vérifier le code PIN**.

Modifier le code PIN SIM Une fois que le code PIN est **activé et vérifié**, vous pouvez choisir de le modifier.

Cliquez sur **Modifier**. Entrez le code PIN SIM fourni par le transporteur. Entrez le nouveau code PIN SIM et confirmez-le. Cliquez sur **Modifier**.

Débloquer la carte SIM Si vous oubliez le code PIN de la carte SIM, vous pouvez réinitialiser le code PIN de la carte SIM à l'aide de la carte SIM PUK obtenue auprès du transporteur.

Pour débloquer une carte SIM, cliquez sur **Débloquer**. Entrez le code PIN et le code PUK de la carte SIM obtenus auprès de l'opérateur et cliquez sur **Débloquer**.

> **Remarque**
>
> La carte SIM est bloquée de façon permanente avec 10 tentatives infructueuses de PUK, tout en débloquant la SIM. Contactez le fournisseur de services de l'opérateur pour obtenir une nouvelle carte SIM.

Paramètres APN

Pour configurer les paramètres APN, entrez l'APN, le nom d'utilisateur, le mot de passe et l'authentification fournis par l'opérateur. Vous pouvez choisir entre les protocoles d'authentification **PAP**, **CHAP**ou **PAPCHAP** . Si le transporteur n'a fourni aucun type d'authentification, définissez-le sur **Aucun**.

Paramètres réseau

Vous pouvez sélectionner le réseau mobile sur les appliances Citrix SD-WAN qui prennent en charge les modems internes.

Itinérant

L'option d'itinérance est activée par défaut sur vos appareils. Vous pouvez choisir de le désactiver.

Gérer le firmware

Chaque appliance sur laquelle LTE est activée dispose d'un ensemble de microprogrammes disponibles. Vous pouvez sélectionner dans la liste existante du firmware ou télécharger un firmware et l'appliquer. Si vous ne savez pas quel microprogramme utiliser, sélectionnez l'option AUTO-SIM pour permettre au modem LTE de choisir le microprogramme le plus adapté en fonction de la carte SIM insérée dans l'appliance.

> **Remarque**
>
> Actuellement, le firmware ne peut être appliqué que sur les appliances SD-WAN SE 210 LTE.

Activer/désactiver le modem

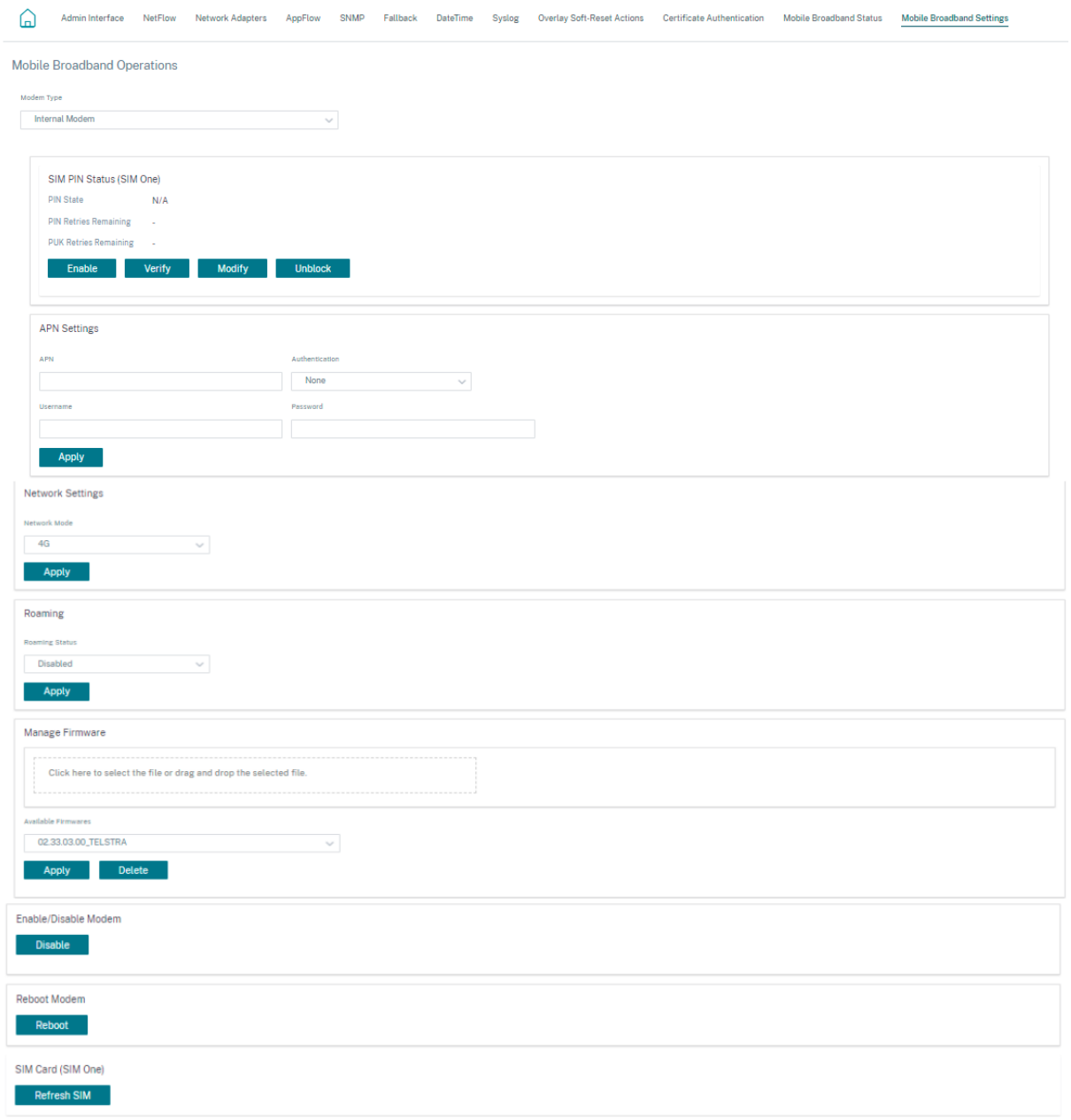
Activez ou désactivez le modem en fonction de votre intention d'utiliser la fonctionnalité haut débit. Par défaut, le modem est activé.

Redémarrer le modem

Redémarre le modem. Ce processus peut prendre jusqu'à 3 à 5 minutes pour terminer l'opération de redémarrage.

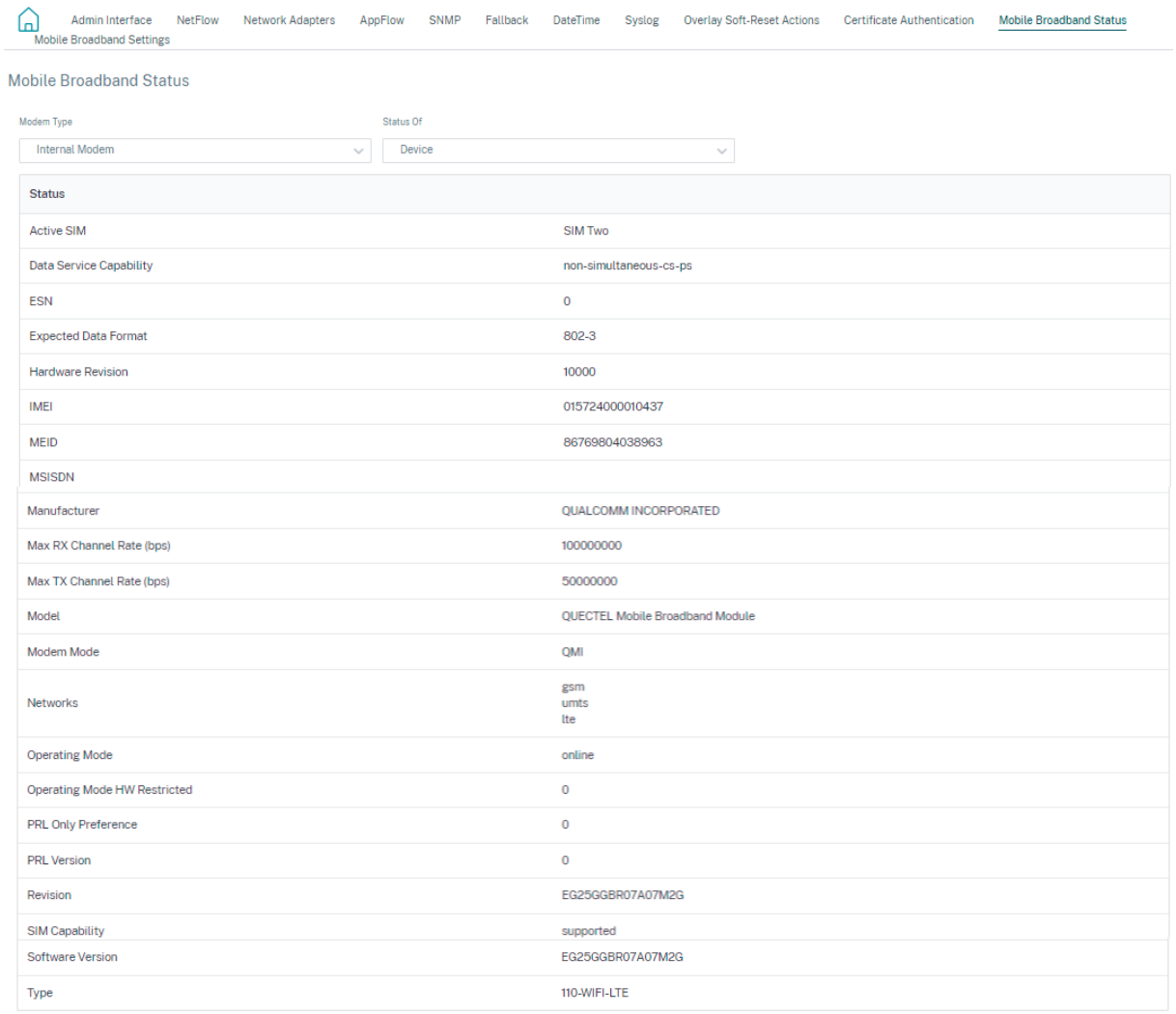
Actualiser la carte SIM

Utilisez cette option lorsque vous remplacez la carte SIM à chaud pour détecter une nouvelle carte SIM.



État du haut débit mobile

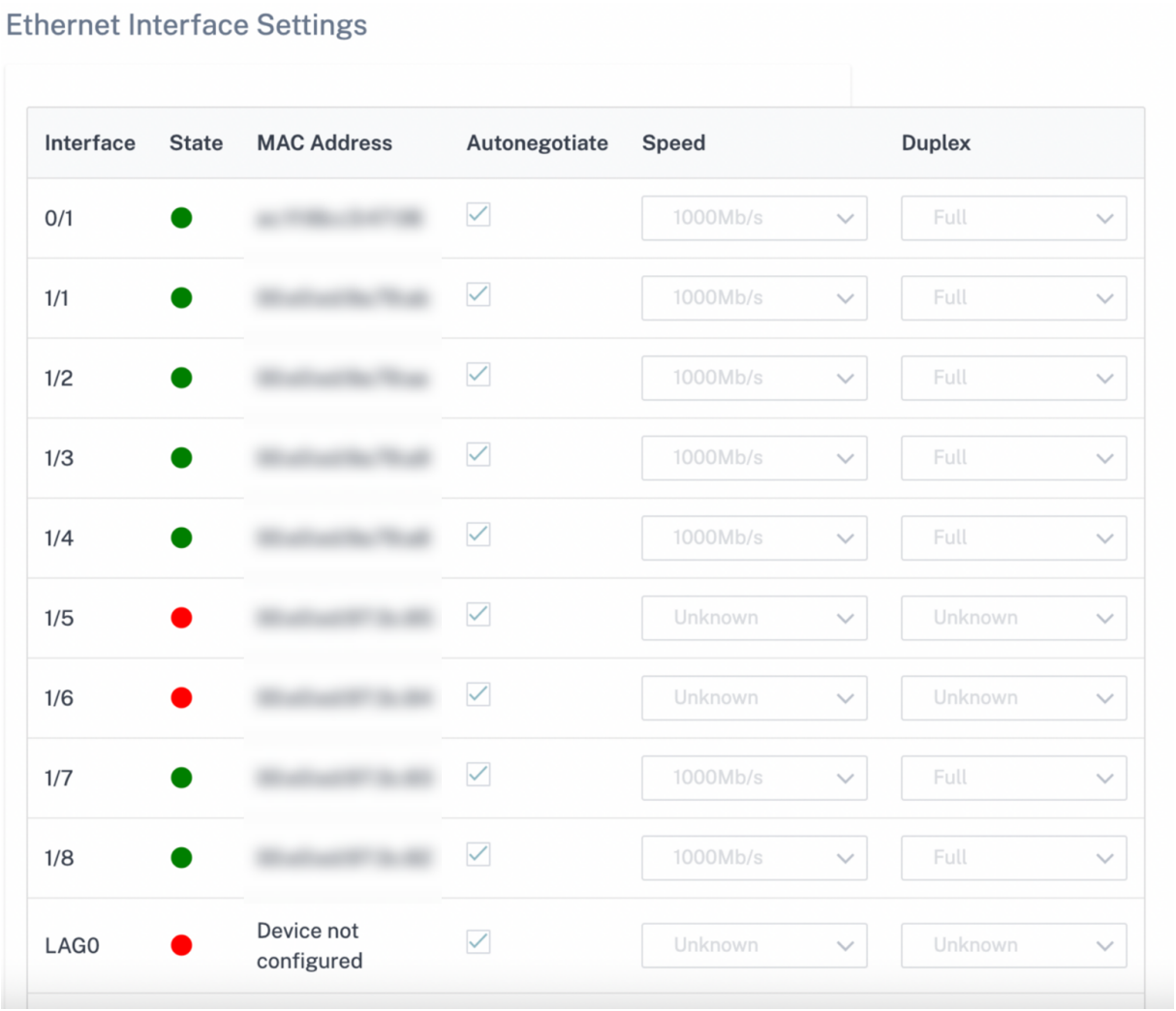
La section État du haut débit mobile affiche l'état de vos paramètres de configuration du haut débit. Pour consulter l'état du haut débit mobile, au niveau du site, accédez à **Configuration** > **Paramètres de l'appliance** > **État du haut débit mobile**. Vous pouvez consulter l'état de votre appareil et de la carte SIM active.



Paramètres de l'interface Ethernet

La section État de l'interface Ethernet affiche l'état de connectivité des ports Ethernet, le type d'interface, l'adresse MAC, la négociation automatique et les informations de configuration du duplex. Pour afficher les paramètres de l'interface Ethernet, au niveau du site, accédez à **Configuration** > Paramètres de **l'appliance > Paramètres** de **l'interface Ethernet**. Les ports qui sont inactifs administrativement sont indiqués en rouge.

> **Remarque**
>
> Ce paramètre est actuellement disponible en mode lecture seule sur l'interface utilisateur du service Citrix SD-WAN Orchestrator. Si vous souhaitez modifier les paramètres de l'interface Ethernet, vous pouvez le faire en utilisant la nouvelle interface utilisateur pour les appliances SD-WAN.



Gestion intrabande

October 21, 2022

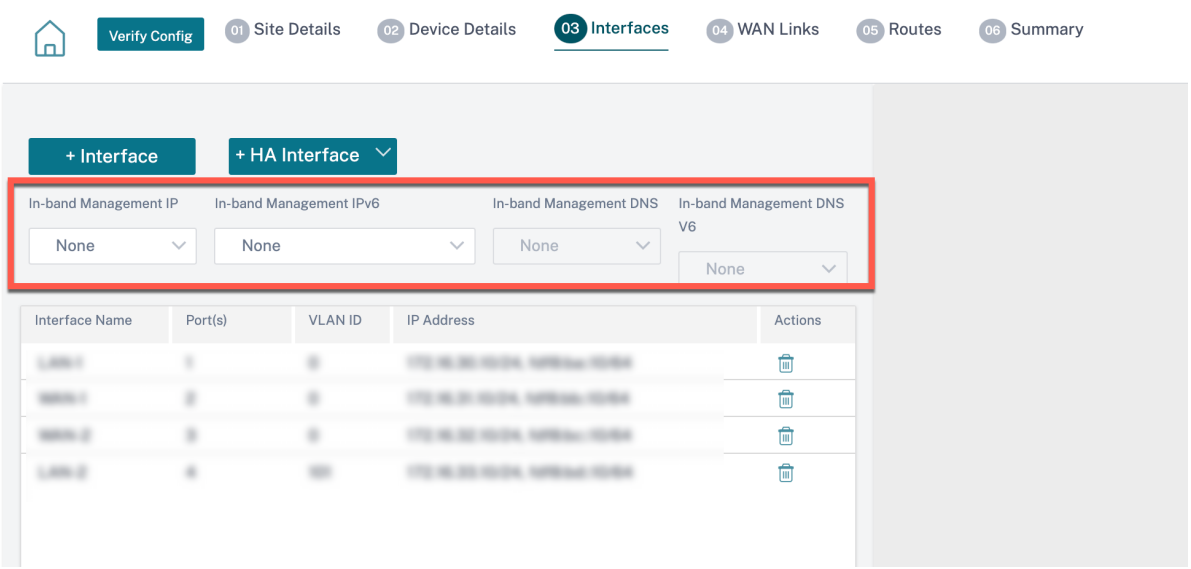
Le service Citrix SD-WAN Orchestrator vous permet de gérer l'appliance SD-WAN de deux manières : gestion hors bande et gestion intrabande. La gestion hors bande vous permet de créer une adresse IP de gestion à l'aide d'un port réservé à la gestion, qui transporte uniquement le trafic de gestion. La gestion in-band vous permet d'utiliser les ports de données SD-WAN pour la gestion. Il transporte à la fois le trafic de données et de gestion, sans avoir à configurer un chemin de gestion supplémentaire.

La gestion in-band permet aux adresses IP virtuelles de se connecter à des services de gestion tels que l'interface utilisateur Web et SSH. Vous pouvez activer la gestion in-band sur une interface approuvée qui est activée pour être utilisée pour les services IP. Vous pouvez accéder à l'interface utilisateur Web et SSH à l'aide de l'adresse IP de gestion et des adresses IP virtuelles in-band.

> **Remarque**
>
> La gestion intrabande dans le service Citrix SD-WAN Orchestrator est prise en charge pour Citrix SD-WAN 11.1.1 et versions ultérieures.

Pour activer la gestion intrabande sur une adresse IP virtuelle, au niveau du site, accédez à **Configuration > Configurationdu site**>**Interfaces**. Sélectionnez l'adresse IP virtuelle à utiliser comme port de gestion in-band. Vous pouvez utiliser l'**adresse IP de gestion InBand**ou la**gestion InBand IPv6** pour accéder à l'interface utilisateur Web et à SSH.

> **Remarque**
>
> La gestion in-band est prise en charge uniquement sur les ports LAN.



Pour une procédure détaillée sur la configuration d'une adresse IP virtuelle, voir Interfaces.

L'IP de gestion in-band agit également comme IP de gestion de sauvegarde. Il est utilisé comme adresse IP de gestion si le port de gestion n'est pas configuré avec une Gateway par défaut. Sélectionnez le **proxy DNS** vers lequel toutes les requêtes DNS sur le plan de gestion intrabande sont transférées. Pour plus d'informations sur la configuration du proxy DNS, voir Proxy DNS.

Pour les cas d'utilisation où la connectivité de l'appliance au service Citrix SD-WAN Orchestrator bascule entre les ports de gestion et les ports intrabande, configurez le DNS de **gestion intrabande ou le DNS** de **gestion intrabande V6** pour garantir une connectivité ininterrompue du service Citrix SD-WAN Orchestrator.

Provisioning intrabande

La nécessité de déployer des appliances SD-WAN dans des environnements plus simples, comme la maison ou les petites succursales, a considérablement augmenté. La configuration d'un accès de gestion distinct pour des déploiements plus simples est une surcharge supplémentaire. Le déploiement sans contact et la fonction de gestion in-band permettent le Provisioning et la gestion de la configuration via des ports de données désignés. Le déploiement sans contact est pris en charge sur les ports de données désignés et il n'est pas nécessaire d'utiliser un port de gestion distinct pour le déploiement sans contact.

Vous pouvez provisionner une appliance à l'état expédié en usine, qui prend en charge le Provisioning in-band en connectant le port de données ou de gestion à Internet. Les appliances prenant en charge le Provisioning in-band disposent de ports spécifiques pour le réseau local et le réseau étendu. L'appliance en état de réinitialisation d'usine dispose d'une configuration par défaut qui permet d'établir une connexion avec le service de déploiement zéro contact. Le port LAN agit en tant que serveur DHCP et attribue une IP dynamique au port WAN qui agit en tant que client DHCP. Les liaisons WAN surveillent le service DNS Quad 9 pour déterminer la connectivité WAN.

Une fois l'adresse IP obtenue et une connexion établie avec le service de déploiement zéro contact, les packages de configuration sont téléchargés et installés sur l'appliance. Pour plus d'informations sur le déploiement sans contact via le service Citrix SD-WAN Orchestrator, consultez Zero Touch Deployment.

> **Remarque**
>
> - Le Provisioning in-band est applicable à toutes les plates-formes. Toutefois, la configuration par défaut n'est activée que sur les plates-formes Citrix SD-WAN 110 et VPX car les autres plates-formes sont livrées avec une version logicielle plus ancienne.
> - Pour le Provisioning jour 0 des appliances SD-WAN via les ports de données, la version logicielle de l'appliance doit être Citrix SD-WAN 11.1.1 ou supérieure.

La configuration par défaut d'une appliance en état de réinitialisation d'usine comprend les configurations suivantes :

- Serveur DHCP sur port LAN
- Client DHCP sur port WAN
- Configuration QUAD9 pour DNS
- L'adresse IP LAN par défaut est 192.168.101.1/24 pour les appliances Citrix SD-WAN avec l'image d'usine 11.1.1.39.
- L'adresse IP LAN par défaut est 192.168.0.1/24 pour l'appliance Citrix SD-WAN 110 avec image d'usine 11.0.4.
- Licence Grace de 35 jours.

Une fois l'appliance provisionnée, la configuration par défaut est désactivée et remplacée par la configuration reçue du service de déploiement zéro contact. Si une licence d'appliance ou une licence de grâce expire, la configuration par défaut est activée, ce qui garantit que l'appliance reste connectée au service de déploiement zéro contact et reçoit le service géré par licence.

Configuration de secours

La configuration de secours garantit que l'appliance reste connectée au service de déploiement zéro contact en cas de panne de liaison, d'incompatibilité de configuration ou d'incompatibilité logicielle. La configuration de secours est activée par défaut sur les appliances disposant d'un profil de configuration par défaut. Vous pouvez également modifier la configuration de secours en fonction de vos paramètres réseau LAN existants.

La configuration de secours conserve la connectivité à l'appliance via l'adresse IP de gestion intrabande de l'appliance et le service Citrix SD-WAN Orchestrator dans les scénarios suivants :

- Où le t2_app se bloque
- vous essayez d'effectuer la réinitialisation de la configuration

Dans un scénario où la gestion intrabande d'une appliance est configurée et que vous effectuez une réinitialisation manuelle de la configuration ou que le t2_app se bloque plus de quatre fois en 120 secondes en raison de la configuration utilisateur. Dans ce cadre, le service est désactivé et vous perdez donc la connectivité au service Citrix SD-WAN Orchestrator et à l'appliance.

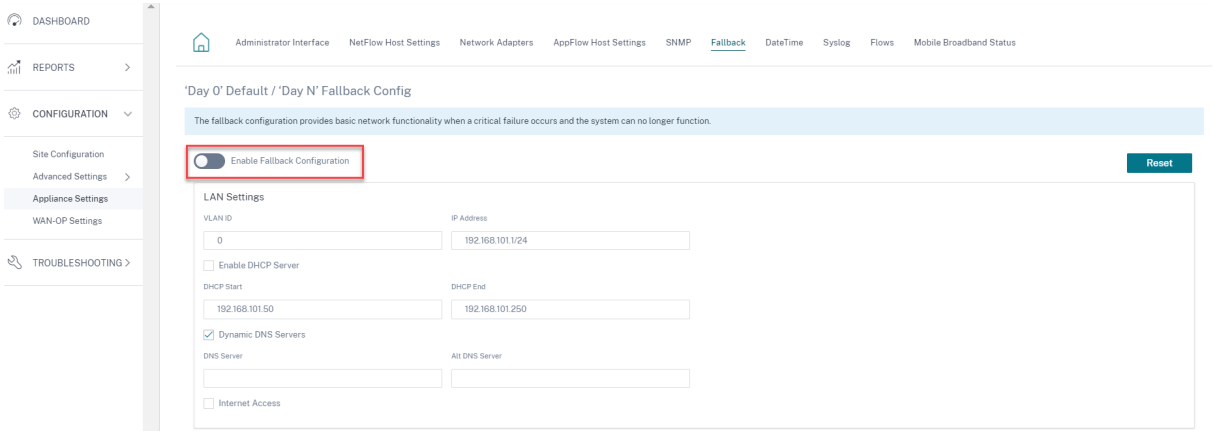
Mais si la configuration de secours était activée, vous obtiendrez les fonctionnalités ci-dessous :

- Accès intrabande de base aux fonctionnalités de gestion (interface utilisateur Web, SSH/SNMP)
- Possibilité pour l'appliance de se connecter à des services externes via un port intrabande (Citrix SD-WAN Orchestrator Service/ZTD)

Dans de tels scénarios, au lieu de désactiver, l'appliance de service revient avec une configuration de secours avec le service activé. La connectivité au service Citrix SD-WAN Orchestrator et à l'appliance via l'adresse IP de gestion intrabande reste intacte tant que la liaison est connectée à Internet.

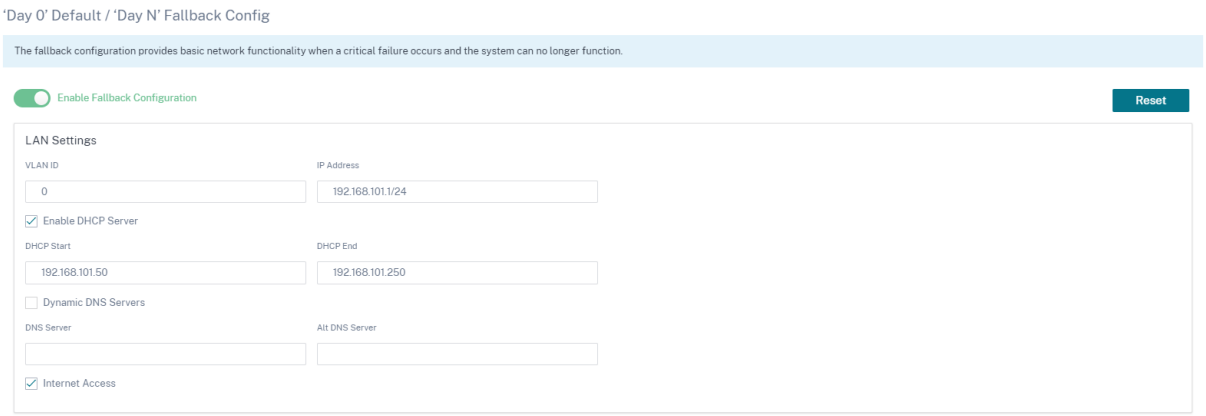
> **Remarque**
>
> Après le provisionnement initial de l'appliance, assurez-vous que la configuration de secours est activée pour une connectivité du service de déploiement sans intervention.

Si la configuration de secours est désactivée, vous pouvez l'activer via le service Citrix SD-WAN Orchestrator au niveau du site en accédant à **Configuration** > **Paramètres de l'appliance** > **Fallback** et en cliquant sur **Activer la configuration de secours** .



Pour personnaliser la configuration de secours en fonction de votre réseau local, modifiez les valeurs des paramètres LAN suivants conformément aux exigences de votre réseau. Il s'agit de la configuration minimale requise pour établir une connexion avec le service de déploiement zéro touche.

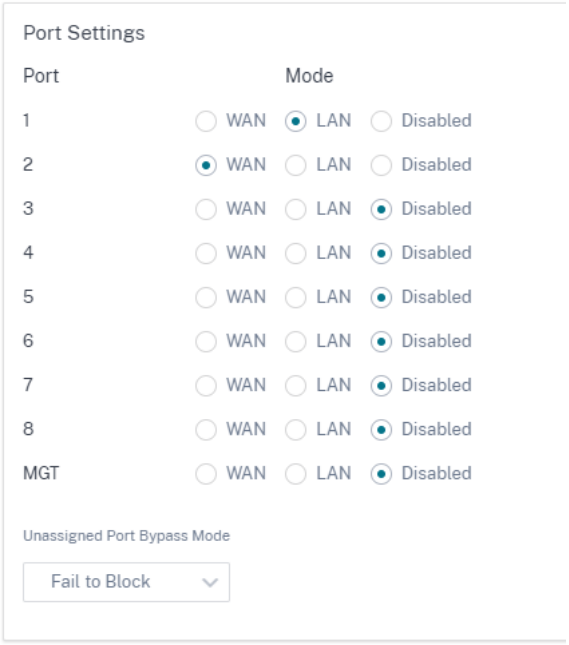
- **ID du VLAN** : ID du VLAN auquel le port LAN doit être groupé.
- **Adresse IP : Adresse**IP virtuelle affectée au port LAN.
- **Activer le serveur DHCP** : active le port LAN en tant que serveur DHCP. Le serveur DHCP attribue des adresses IP dynamiques au port WAN.
- **Début DHCP et fin DHCP** : plage d'adresses IP que DHCP utilise pour attribuer dynamiquement une adresse IP au port WAN.
- **Serveur DNS dynamique** : active le port LAN en tant que serveur de noms de domaine.
- **Serveur DNS** : adresse IP du serveur DNS principal.
- **Serveur DNS Alt** : Adresse IP du serveur DNS secondaire.
- **Accès Internet** : Autoriser l'accès Internet à tous les clients LAN sans autre filtrage.



Configurez le mode pour chaque port. Le port peut être un port LAN ou un port WAN ou peut être désactivé. Les ports affichés dépendent du modèle de l'appliance. En outre, définissez le mode de contournement de port sur **Fail-to-block** ou **Fail-to-Wire**.

Le tableau suivant fournit les détails des ports WAN et LAN prédésignés pour la configuration de secours sur différentes plates-formes :

Plateforme	Ports WAN	Ports LAN
110	1/2	1/1
110-LTE	1/2, LTE-1	1/1
210	1/4, 1/5	1/3
210-LTE	1/4, 1/5, LTE-1	1/3
VPX	2	1
410	1/4, 1/5, 1/6	1/3 (FTB)
1100	1/4, 1/5, 1/6	1/3 (FTB)

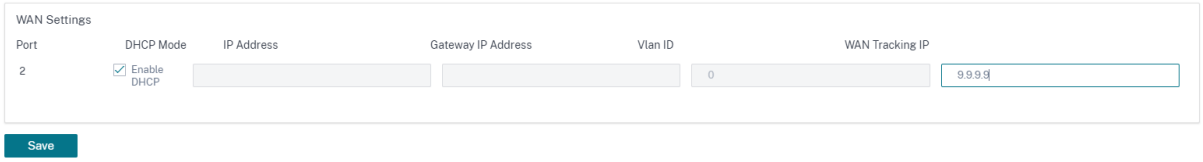


Les ports WAN peuvent être configurés en tant que liens WAN indépendants à l'aide du client DHCP et surveillent le service DNS Quad9 pour déterminer la connectivité WAN. Vous pouvez configurer les IP WAN ou IP statiques pour les ports WAN en l'absence de DHCP pour utiliser la gestion in-band pour le provisionnement initial.

> **Remarque**
>
> Vous ne pouvez configurer les ports Ethernet qu'avec les adresses IP statiques. Les IP statiques ne sont pas configurables avec les ports LTE-1 et LTE-E1. Bien que vous puissiez ajouter les ports LTE-1 et LTE-E1 en tant que WAN, les champs de configuration restent non modifiables.

Lorsque vous ajoutez un port WAN, il est ajouté dans la section **Paramètres WAN (Port : 2)** avec la case à cocher **Activer DHCP** sélectionnée par défaut. Si la case **Mode DHCP** est cochée, les champs

de texte **Adresse IP, Adresse IP de passerelle**et**ID du VLAN**sont grisés. Décochez la case**Activer le DHCP** si vous souhaitez configurer une adresse IP statique.



Par défaut, le champ **Adresse IP de suivi du WAN** est automatiquement rempli avec le 9.9.9.9. Vous pouvez modifier l'adresse au besoin.

> **Remarque**
>
> Si vous cochez la case **Serveurs DNS dynamiques**, veillez à ajouter/configurer au moins un port WAN avec le **mode DHCP** sélectionné.

Pour réinitialiser la configuration de secours à la configuration par défaut à tout moment, cliquez sur **Réinitialiser**.

> **Remarque**
>
> Il est recommandé d'activer la configuration de secours sur toutes les appliances connectées à Orchestrator via le port intraband/de gestion connecté au sous-réseau LAN. Assurez-vous que la configuration de secours par défaut est configurée conformément aux exigences de votre sous-réseau.

Basculement de port

Le service Citrix SD-WAN Orchestrator permet également de transférer le trafic de gestion de manière fluide vers le port de gestion lorsque le port de données tombe en panne et inversement. Si une appliance peut se connecter à Internet via les ports de gestion et in-band, le port de gestion est choisi pour un déploiement sans contact.

Au redémarrage de l'appliance, si Internet est disponible via le port intrabande et non le port de gestion, l'appliance est immédiatement connectée au service Citrix SD-WAN Orchestrator.

Une fois la connexion établie, un agent de service s'exécutant sur l'appliance envoie les informations de pulsation au service Citrix SD-WAN Orchestrator toutes les 10 secondes. Si le service Citrix SD-WAN Orchestrator ne reçoit pas le rythme cardiaque pendant 5 minutes, le basculement du port intrabande est activé. Le service Citrix SD-WAN Orchestrator indique que l'appliance est hors ligne pendant cette période.

Au redémarrage de l'appliance, si Internet n'est pas disponible sur le port de gestion et dans la bande et une fois la connexion Internet rétablie, l'agent de service prend environ 5 minutes pour redémarrer et établir une connexion.

Assurez-vous que l'option **Préserver l'itinéraire vers Internet à partir du lien même si tous les chemins associés sont inactifs** est activée au niveau du réseau, **Configuration** > **Delivery Services** > **Internet**. S'assurer que la connectivité au service Citrix SD-WAN Orchestrator est maintenue même si le chemin virtuel est en panne.

Port de gestion ou de données configurable

La gestion in-band permet aux ports de données de transporter à la fois les données et le trafic de gestion, éliminant ainsi le besoin d'un port de gestion dédié. Il laisse le port de gestion inutilisé sur les appliances bas de gamme, qui ont déjà une faible densité de port. Citrix SD-WAN vous permet de configurer le port de gestion pour qu'il fonctionne en tant que port de données ou port de gestion.

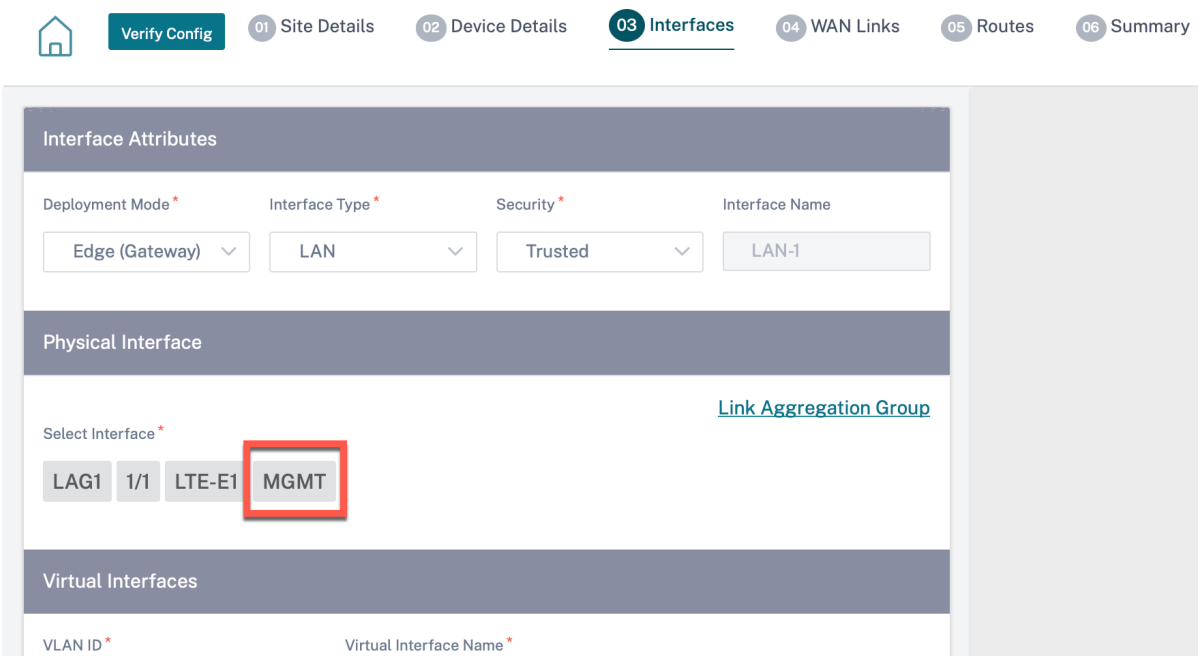
> **Remarque**
>
> Vous pouvez convertir le port de gestion en port de données uniquement sur les plates-formes suivantes.
>
> - Citrix SD-WAN 110 SE/LTE
> - Citrix SD-WAN 210 SE/LTE

Lors de la configuration d'un site, utilisez le port de gestion dans votre configuration. Une fois la configuration activée, le port de gestion est converti en port de données.

> **Remarque**
>
> Vous pouvez configurer un port de gestion uniquement lorsque la gestion intrabande est activée sur d'autres interfaces approuvées de l'appliance.

Pour configurer une interface de gestion, au niveau du site, accédez à **Configuration > Configura-**

tiondu site>**Interfaces** et sélectionnez l'interface MGMT. Pour plus d'informations sur la configuration des groupes d'interfaces, voir Interfaces.



Pour reconfigurer le port de gestion afin d'exécuter la fonctionnalité de gestion, supprimez la configuration. Créez une configuration sans utiliser le port de gestion et activez-la.

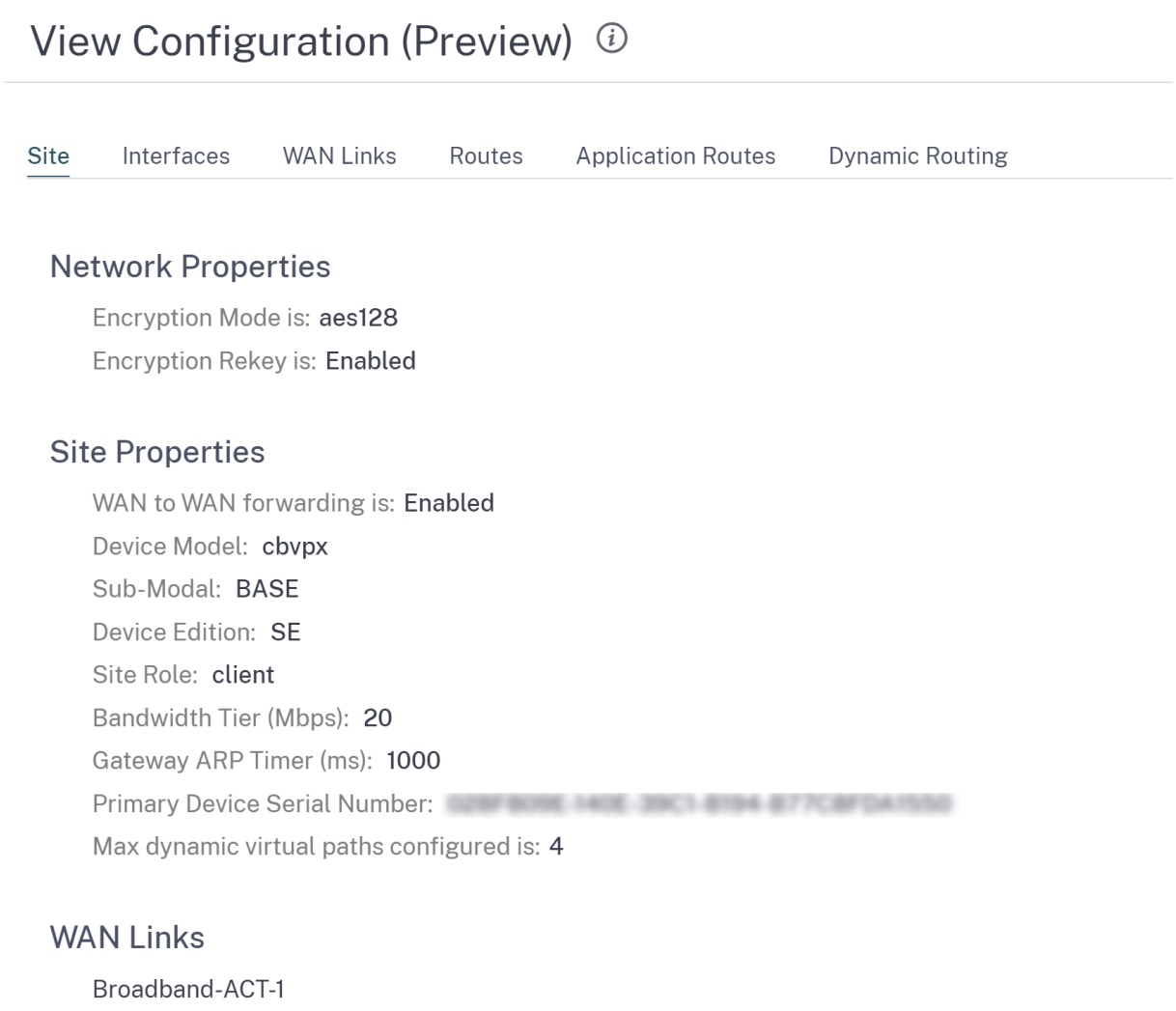
Afficher la configuration (aperçu)

October 21, 2022

La page **Afficher la configuration** fournit un résumé consolidé des paramètres de configuration d'un site. Pour afficher les configurations, au niveau du site, accédez à **Configuration** > **Afficher la configuration**. Pour plus d'informations sur la configuration du site, voir Configuration du site.

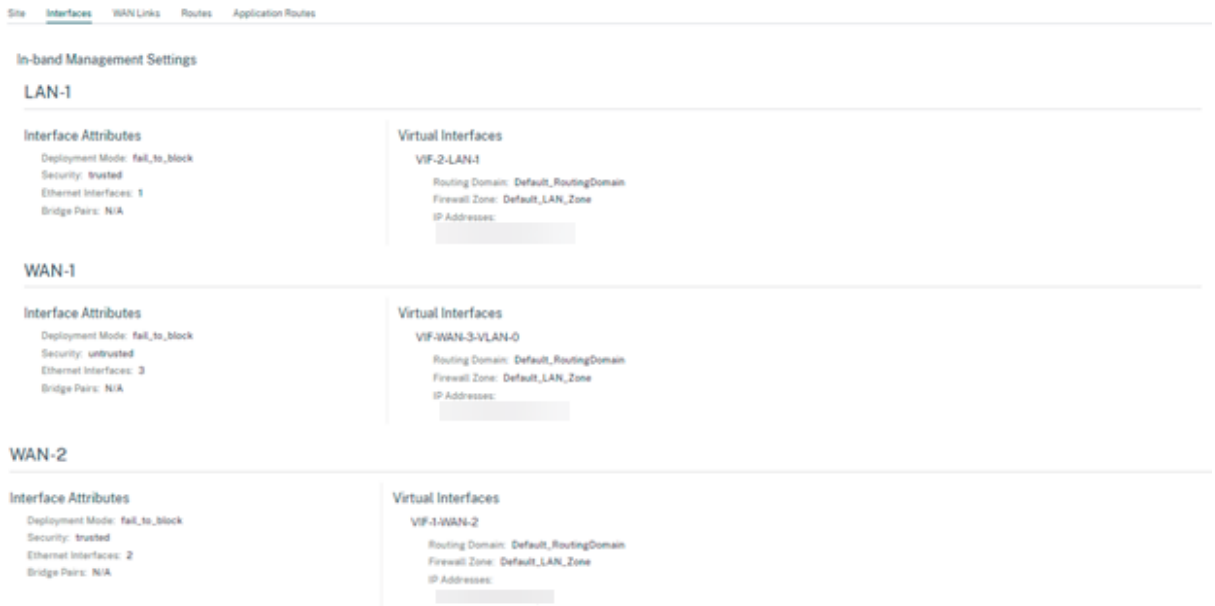
Sites

La page **Sites** affiche un résumé des détails du site. Le résumé du site inclut les propriétés du réseau, les propriétés du site et l'état des liens WAN. Pour consulter les détails de configuration du site, accédez à **Configuration** > **Afficher la configuration** > **Site**.



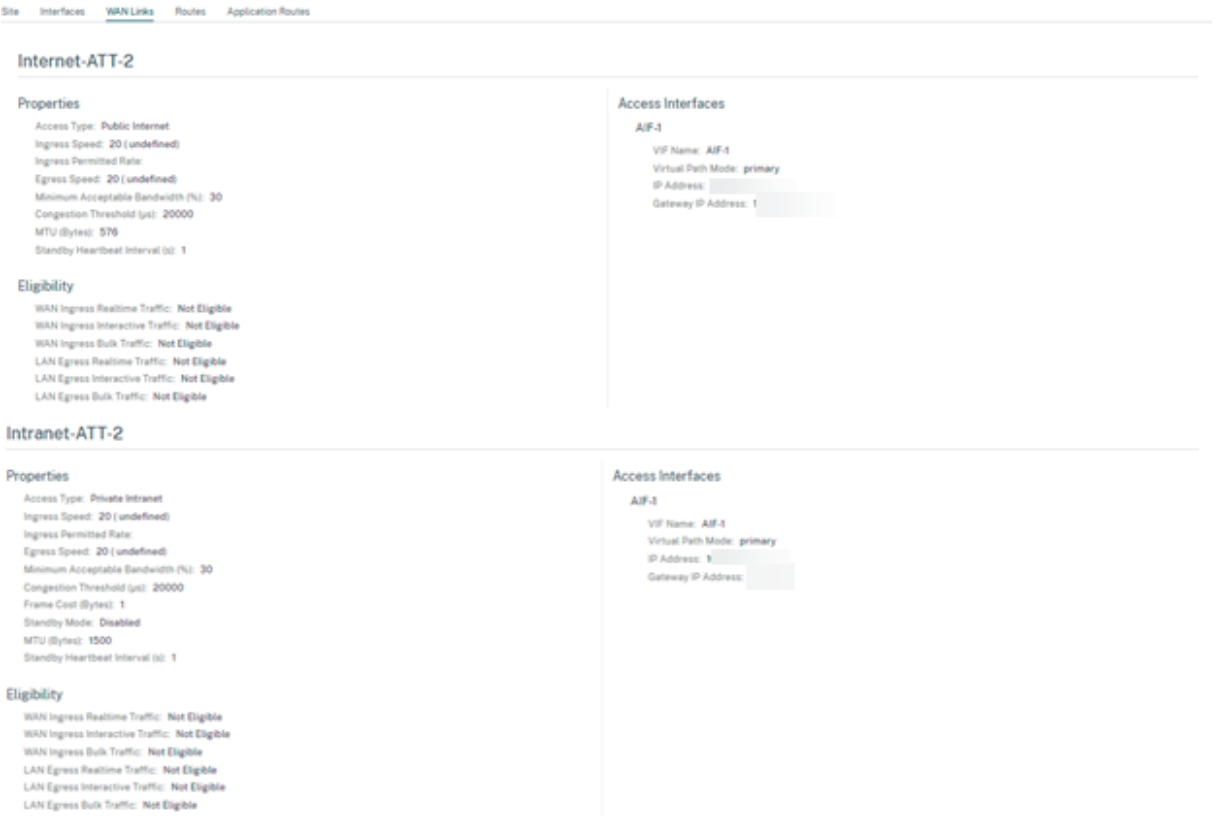
Interfaces

La page **Interfaces** affiche un résumé des interfaces configurées. Pour afficher les détails de configuration des interfaces virtuelles, accédez à **Configuration** > **Afficher la configuration** > **Interfaces**.



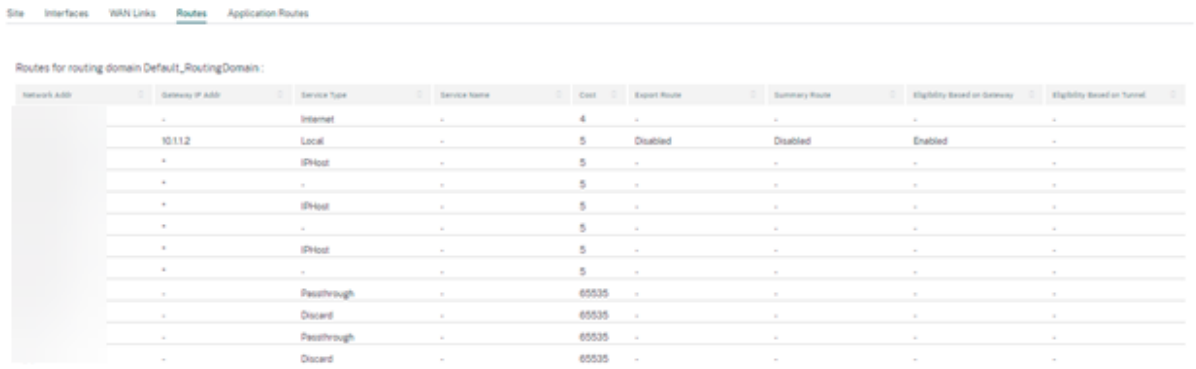
Liens WAN

Pour afficher les détails de configuration des liaisons WAN configurées, accédez à **Configuration** > **Afficher la configuration** > **Liens WAN**.



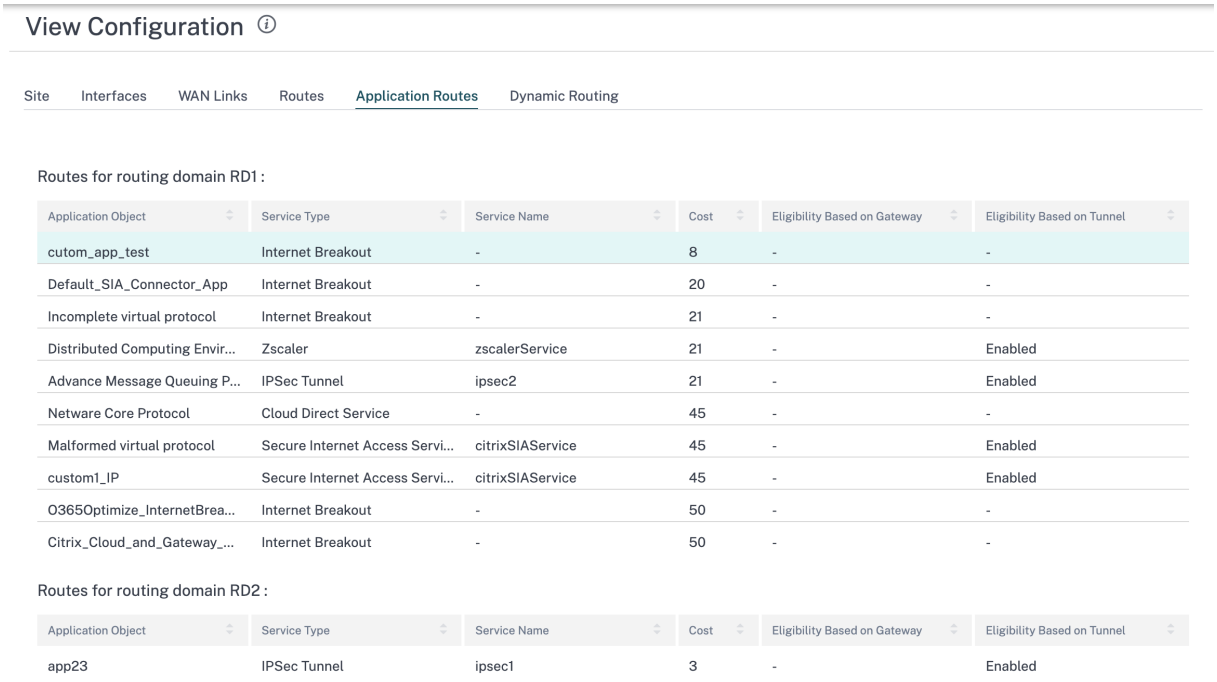
Itinéraires

Pour afficher les informations d'itinéraire des routes IP créées, accédez à **Configuration** > **Afficher la configuration** > **Routes**.



Voies d'application

Pour afficher un résumé des itinéraires d'application spécifiques, accédez à **Configuration** > **Afficher la configuration** > **Routes d'application**.



Routage dynamique

Pour consulter un résumé des configurations des filtres OSPF, BGP, des filtres d'importation et d'exportation, accédez à **Configuration** > **Afficher la configuration** > **Routage dynamique**.

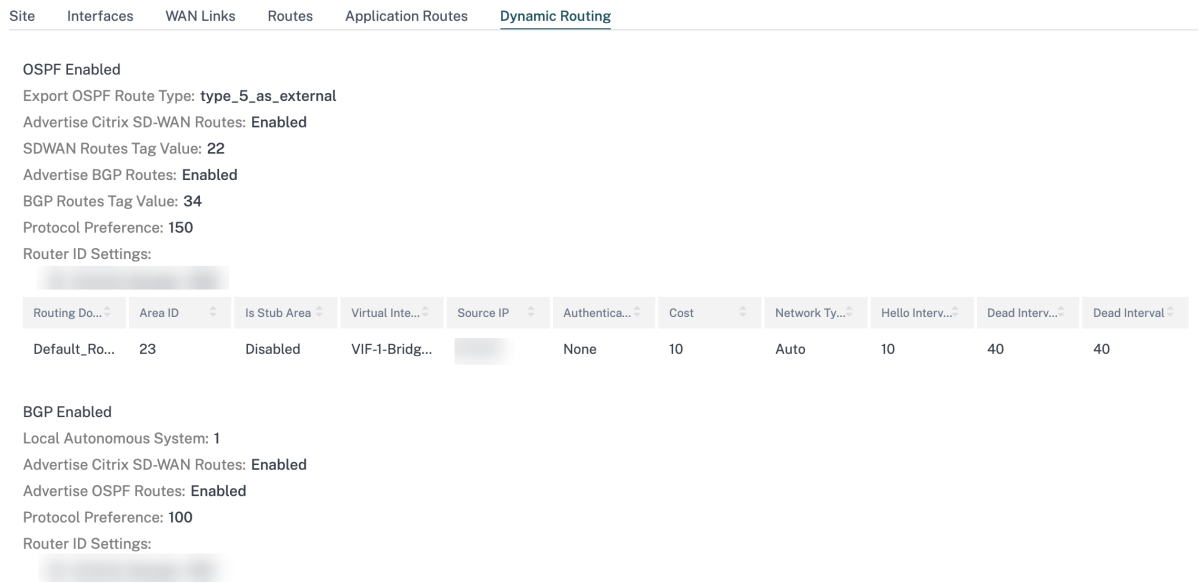
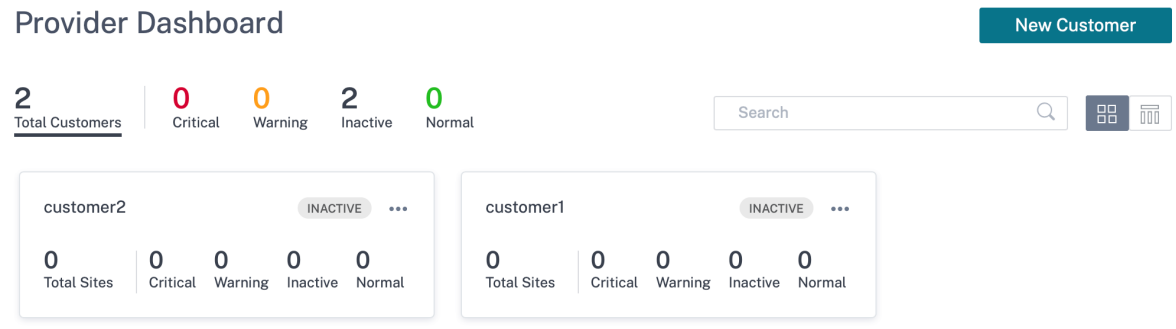


Tableau de bord fournisseur

November 12, 2020

Lorsque vous vous connectez en tant que partenaire Citrix, le **Tableau de bord du fournisseur** s'affiche. Il offre une vue d'ensemble des clients SD-WAN gérés par un fournisseur de services.



Un instantané de l'état de santé codé par couleur du réseau SD-WAN de chaque client est fourni, avec possibilité d'analyser en profondeur l'un d'entre eux pour obtenir des détails spécifiques au client. Le tableau de bord est disponible à la fois en mode **vignette** et en mode **Liste**.

Les critères de codage couleur utilisés pour le réseau du client sont les suivants :

- Critique (rouge) : un ou plusieurs sites sont en panne
- Avertissement (Orange) : Aucun site n'est en panne, mais il y a une ou plusieurs alertes critiques.
- Normal (vert) : Aucun site n'est en panne et il n'y a pas d'alerte critique.
- Inactif (gris) : le réseau est en cours de configuration, mais n'a pas encore été déployé.

Les critères de codage couleur permettent aux administrateurs de se concentrer sur les clients qui ont besoin de leur attention.

Tableau de bord Client/Réseau

July 10, 2024

Le tableau de bord du réseau fournit une vue d'ensemble du réseau SD-WAN d'une entreprise en termes de santé et d'utilisation sur tous les sites. Le tableau de bord capture un résumé des alertes à l'échelle du réseau, de la disponibilité des chemins de superposition et de sous-couche, met en évidence les tendances d'utilisation et fournit une vue globale du réseau.

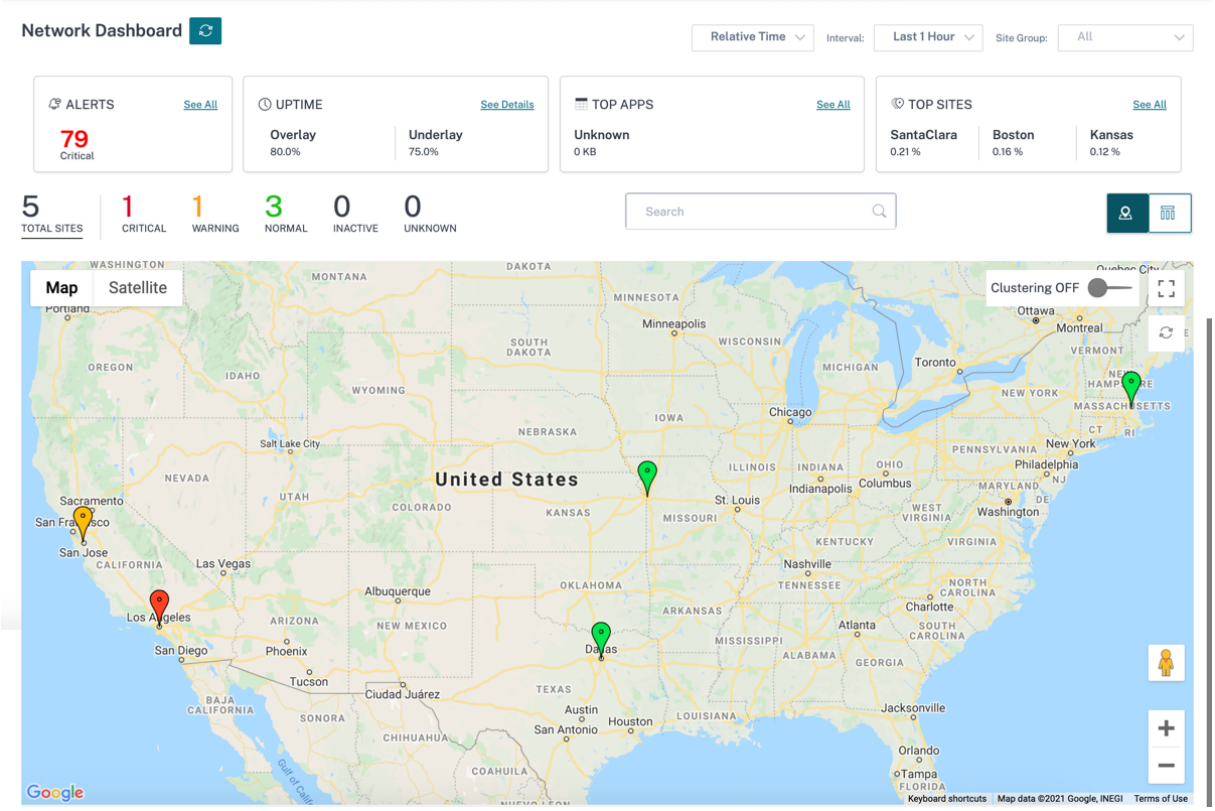
Le tableau de bord résume les aspects suivants d'un réseau, avec une disposition permettant une exploration plus approfondie pour plus de détails.

- **Alertes critiques** : nombre cumulé d'alertes de santé critiques, le cas échéant, qui apparaissent sur le réseau.
- **Disponibilité** : comparaison côte à côte du temps de disponibilité moyen offert par le réseau de superposition virtuel SD-WAN par rapport au réseau sous-jacent physique
- **Tendances d'utilisation** : meilleures applications, en fonction du volume de trafic, et meilleurs sites, en fonction de l'utilisation de la capacité.
- **Vue réseau** : représentation visuelle de tous les sites d'un réseau, disponible en mode carte et en mode liste.

Le tableau de bord répertorie le nombre total de sites du réseau et sépare les sites en fonction de leur état de connectivité. Sélectionnez les liens numérotés pour afficher les sites en fonction des catégories de statut suivantes :

- **Critique** : sites dont tous les chemins virtuels associés sont inactifs.
- **Avertissement** : sites qui possèdent au moins un chemin virtuel vers le bas.
- **Normal** : tous les chemins virtuels et les chemins des membres associés du site sont actifs.
- **Inactifs** : sites qui sont à l'état non déployé et inactif.
- **Inconnu** - L'état du site est inconnu.

Le fait de cliquer sur le statut permet de filtrer les sites en fonction de leur statut et d'afficher les détails. Vous pouvez également utiliser la barre **de recherche** pour afficher les détails d'un site en fonction du nom du site, du rôle, de la connectivité de superposition, du modèle, du niveau de bande passante et des paramètres du numéro de série.



La carte fournit une vue en temps réel du réseau mondial avec tous les sites de l'organisation représentés sur une carte du monde, en fonction de leur emplacement. La couleur de chaque site reflète sa santé actuelle.

Voici les critères de codage couleur utilisés pour chaque site :

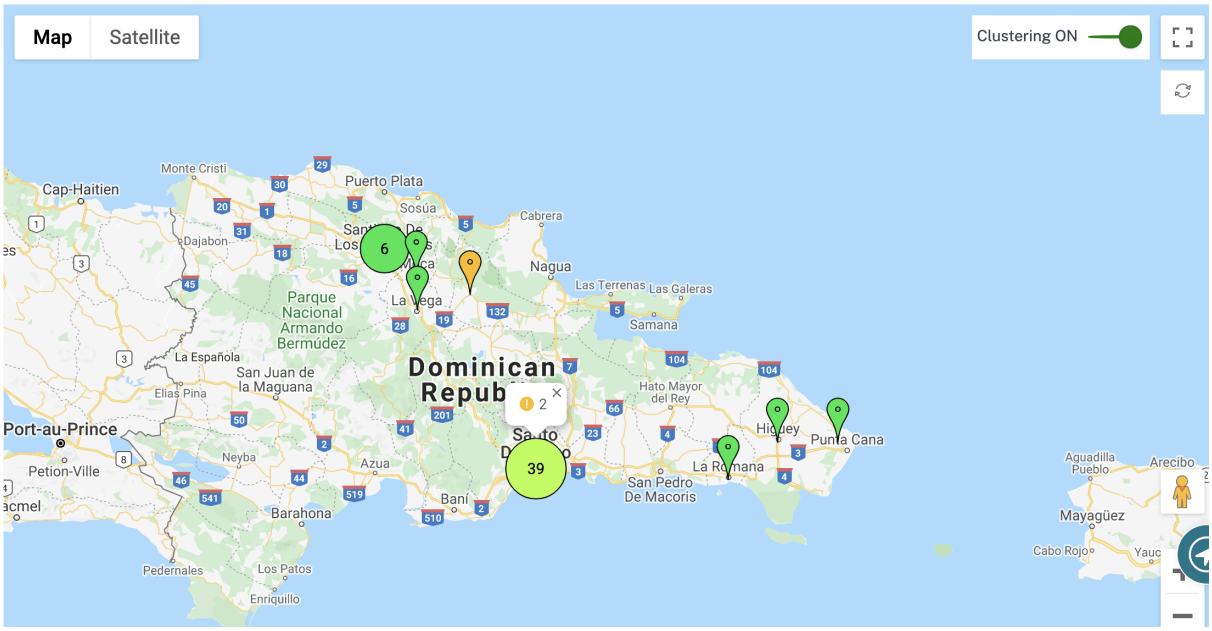
- **Critique (rouge)** : au moins un chemin virtuel de superposition associé à un site est INACTIF.
- **Avertissement (orange)** : Au moins un chemin de membre sous-jacent est INACTIF, mais tous les chemins virtuels de superposition sont en haut.
- **Normal (vert)** : tous les chemins virtuels de superposition et les chemins des membres sous-jacents associés sont en haut.
- **Inactif (gris)** : le site est en cours de configuration et n'a pas encore été déployé.

En survolant un site, certains détails clés spécifiques au site, tels que le rôle du site, le modèle de périphérique et le niveau de bande passante s'affichent. Les chemins virtuels associés à un site apparaissent avec des codes de couleur appropriés qui reflètent leur état de santé. La **vue de liste** fournit les mêmes informations pour chaque site, résumées sous forme d'entrées dans un tableau.

Mise en cluster

La fonctionnalité **Clustering ON** surveille la cohérence, l'état et la santé des différents sites d'un cluster ou d'une combinaison de clusters. Le service Clustering ON fournit une vue en temps réel des sites qui aident à surveiller le basculement et l'état actuel du site.

Cette fonctionnalité **Clustering ON** a été introduite pour gérer la haute densité de sites. Il n'est pas recommandé d'utiliser l'option de clustering off lorsqu'il y a des milliers de sites et cela réduit également les performances.



Le tableau suivant décrit la nuance de cinq couleurs utilisée pour les clusters pour représenter l'état des sites :

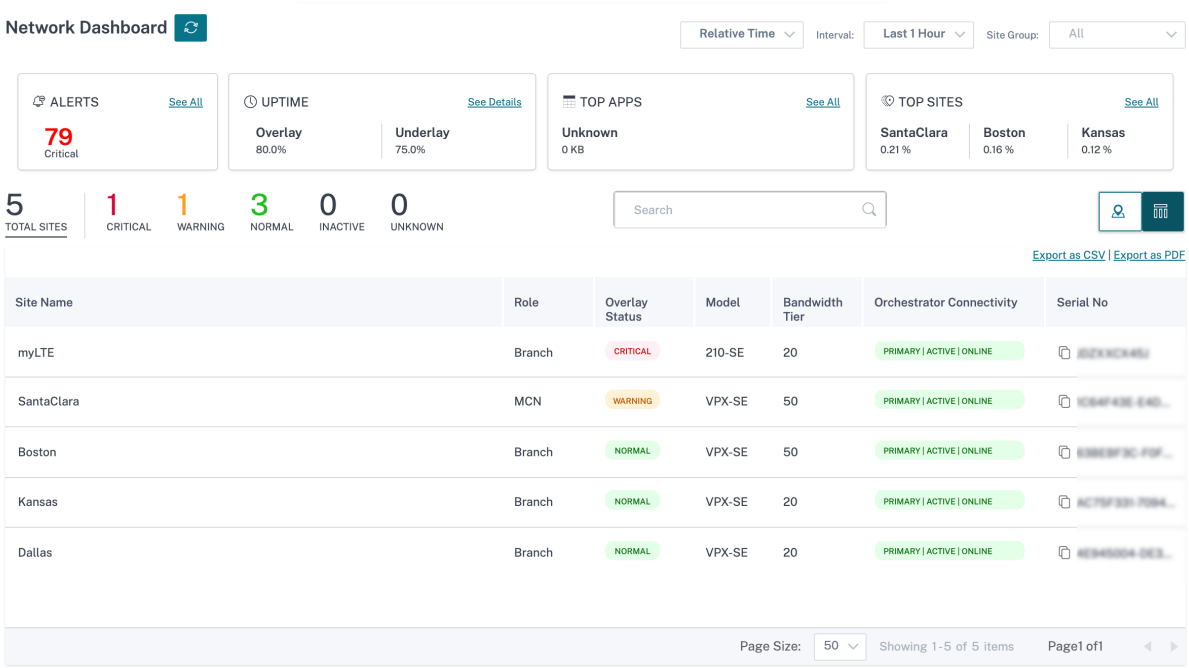
Légendes de couleur	Description
	Tous les sites du cluster sont verts. Cela signifie que chaque site possède tous les chemins virtuels et les chemins des membres associés (UP).
	Tous les sites du cluster sont orange. Cela signifie que chaque site possède au moins un chemin de membre DOWN, mais tous les chemins virtuels sont UP
	Tous les sites du cluster sont rouges. Cela signifie que chaque site possède au moins un chemin virtuel DOWN

Légendes de couleur	Description
	Le cluster a une combinaison de sites verts et oranges
	Le cluster a une combinaison de sites rouges et non rouges

Vous pouvez également vérifier l'aspect réseau en plaçant votre souris sur n'importe quel cluster. Les alertes critiques ou d'avertissement sont visibles au-dessus du cluster sous la forme d'une fenêtre contextuelle.

Si vous cliquez sur le cluster, il effectue un zoom sur ce cluster et affiche d'autres clusters. Vous pouvez voir une barre d'affichage avec le nombre de clusters. L'option flèche vous permet de revenir d'un pas en arrière. Cliquez sur le bouton **Fermer (X)** pour revenir à la page d'origine.

Vous pouvez également consulter le résumé du réseau dans la **vue par liste**.



- Cliquez sur un site « sous-configuré » inactif qui n'a pas encore été déployé pour accéder au flux de travail de configuration du site.
- Cliquez sur un site actif déjà déployé pour accéder au tableau de **bord du site**.

> **Remarque**
>
> Les tunnels de superposition Citrix SD-WAN sont appelés chemins virtuels. Vous disposez généralement d'un tunnel de chemin virtuel entre chaque site et le nœud de contrôle maître

> (MCN), et des chemins virtuels de site supplémentaires si nécessaire. Les chemins virtuels sont formés en liant ensemble les liens ou chemins WAN sous-couche. Ainsi, chaque chemin virtuel comprend plusieurs chemins de membres.
>
> Cela peut être affiché lorsqu'un utilisateur survole le terme chemin virtuel ou chemin de membre.

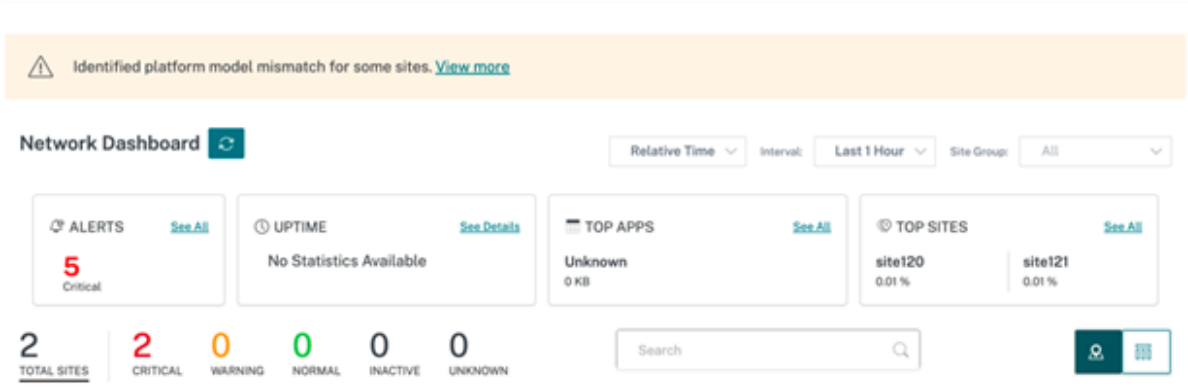
Vous pouvez faire glisser le **Pegman** sur la carte pour ouvrir la vue sur la rue.

Incompatibilité des appareils d'enregistrement

Le service Citrix SD-WAN Orchestrator signale une incompatibilité identifiée entre le modèle de plate-forme signalé par l'appliance et le modèle de plate-forme signalé par l'utilisateur.

Lorsque le modèle de plate-forme et le sous-modèle fournis par un utilisateur lors de la configuration du site ne correspondent pas au modèle de plate-forme et au sous-modèle fournis par l'appliance lors de l'enregistrement initial auprès du service Citrix SD-WAN Orchestrator, une notification concernant l'incompatibilité s'affiche sur le tableau de bord du réseau. Dans un tel scénario, veillez à configurer le modèle de plate-forme indiqué par l'appliance.

Cliquez sur **Afficher plus** pour obtenir une représentation tabulaire de l'inadéquation des modèles de plateforme pour chaque site.



Les informations relatives à l'**incompatibilité de plate-forme** fournissent des informations telles que le nom du site, le modèle et le sous-modèle de plate-forme signalés par l'appliance, et le modèle et sous-modèle de plate-forme signalés par l'utilisateur

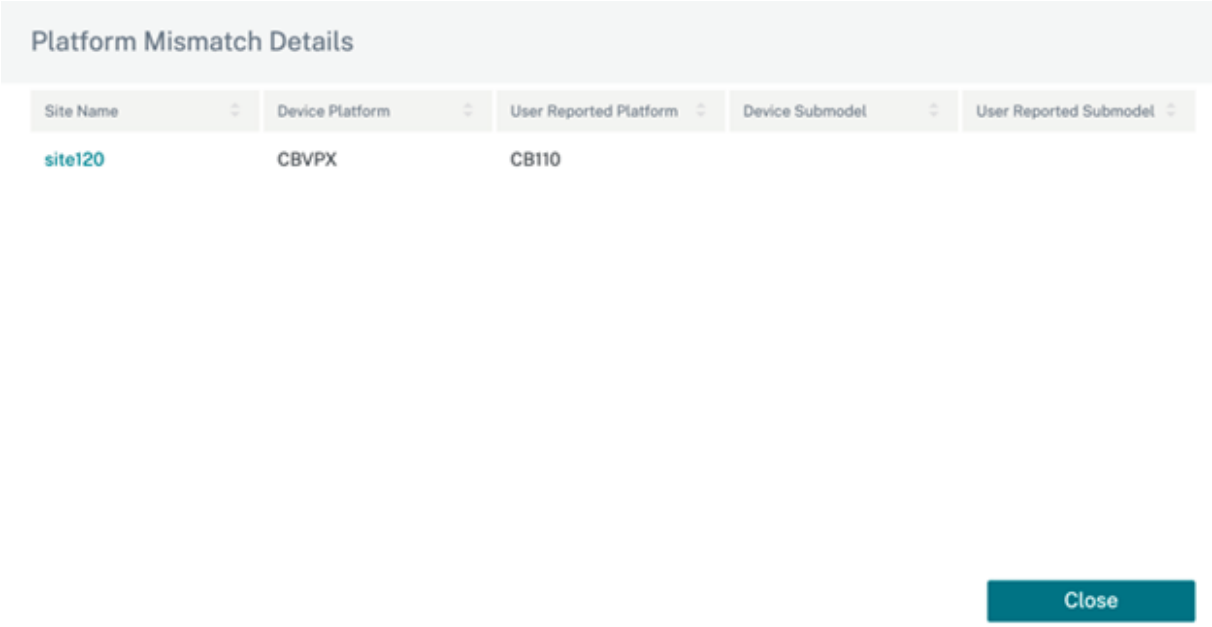


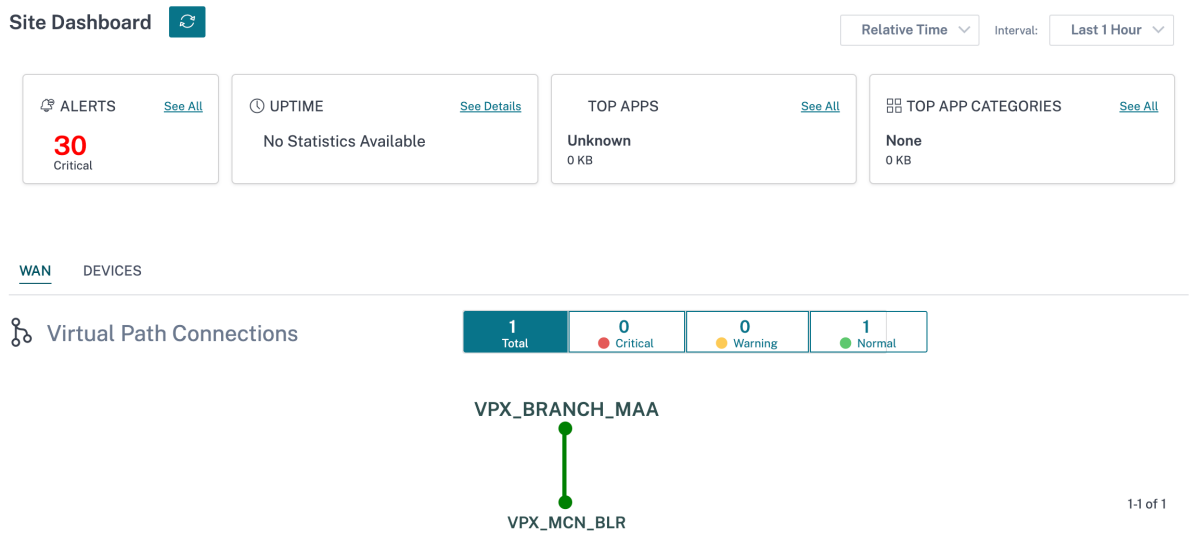
Tableau de bord site

October 21, 2022

Le Tableau de bord du site fournit une vue d'ensemble de l'état et des tendances d'utilisation d'un site.

Le tableau de bord résume les aspects suivants d'un site, avec une disposition permettant une exploration plus approfondie pour plus de détails.

- **Alertes critiques** : nombre cumulé d'alertes de santé critiques, le cas échéant, qui apparaissent sur le site.
- **Disponibilité** : comparaison côte à côte du temps de disponibilité moyen offert par les chemins de superposition virtuels du SD-WAN par rapport aux chemins sous-jacents physiques, associés à un site
- **Tendances d'utilisation** : principales applications et catégories d'applications associées à un site, en fonction du volume de trafic
- **Détails du site** : connexions WAN et appareils associés à un site



> **Conseil**
>
> Cliquez sur **Voir tout** ou **Voir les détails** pour afficher des statistiques plus détaillées.

Toutes les connexions de chemin virtuel de superposition associées à un site sont affichées avec un code couleur approprié pour refléter l'intégrité de chaque connexion.

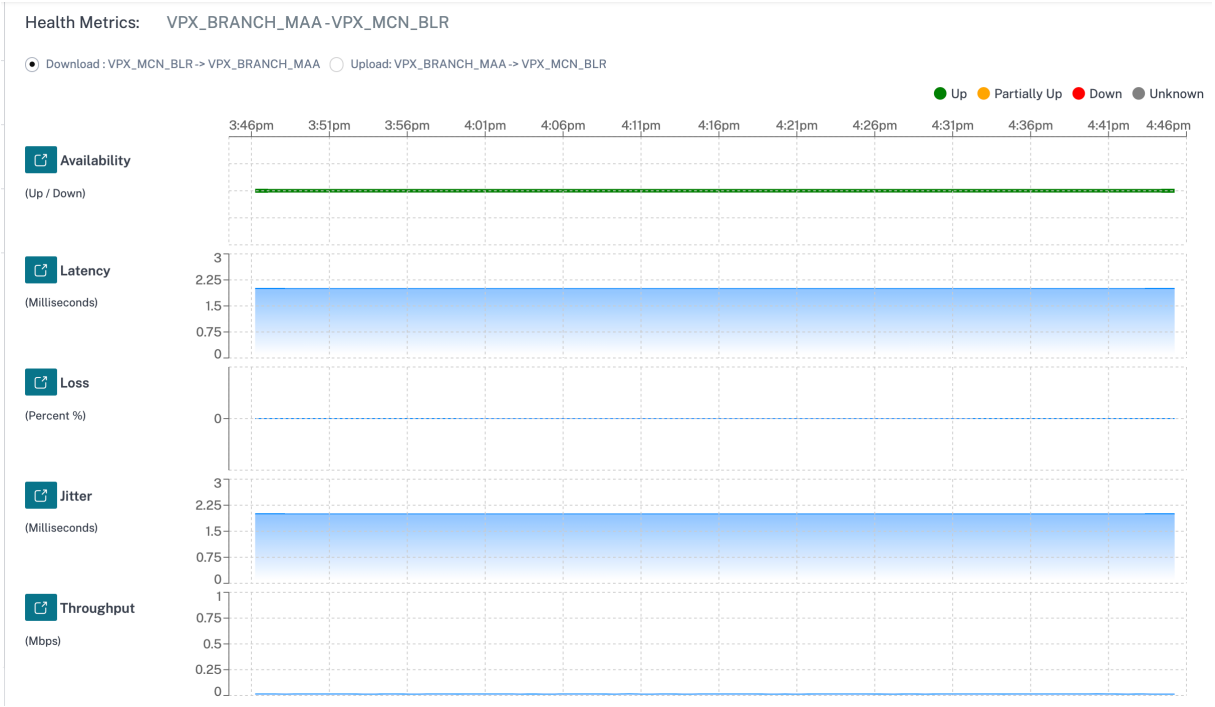
Vous pouvez sélectionner n'importe quelle connexion de chemin virtuel pour consulter les mesures d'intégrité et les tendances correspondantes.

Les critères de code couleur utilisés pour les connexions par chemin virtuel sont les suivants :

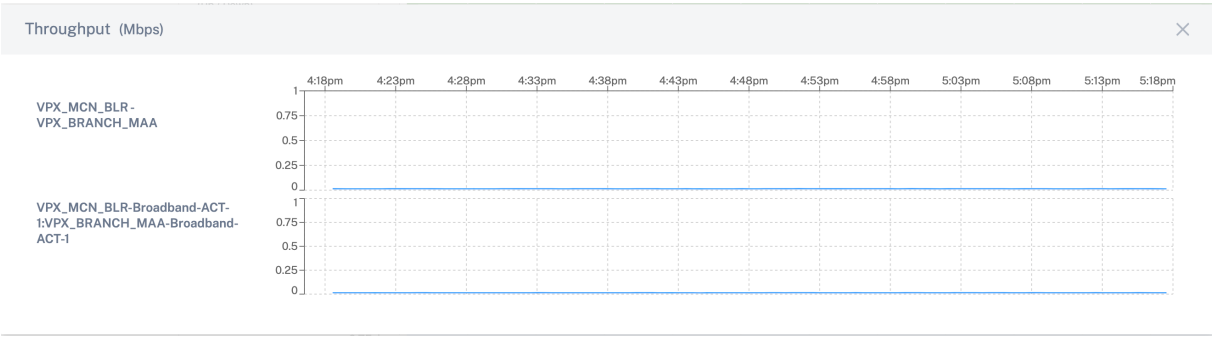
- **Critique (rouge)** : le chemin virtuel est inactif.
- **Avertissement (orange)** : Le chemin virtuel est en haut, mais au moins un chemin membre est INACTIF.
- **Normal (vert)** : chemin virtuel et tous les chemins des membres sont actifs.

Indicateurs de santé

Les mesures d'intégrité et les tendances graphiques concernant la disponibilité, la latence, la perte, la gigue et le débit sont affichées pour la connexion de chemin virtuel sélectionnée. Ces statistiques sont disponibles dans les deux sens : **WAN vers LAN** et **LAN vers WAN**. Toutes les mesures peuvent être passées en revue par rapport à une chronologie commune, afin de réduire rapidement le domaine problématique lors du dépannage.



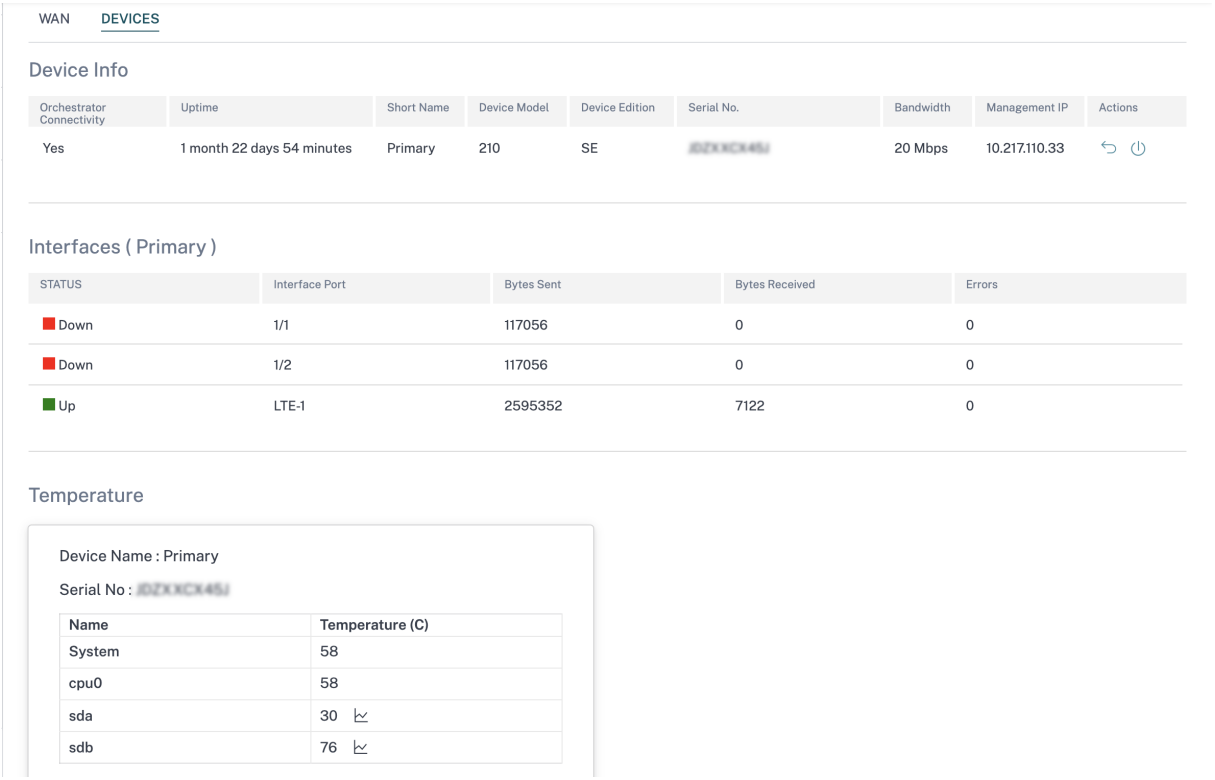
Vous pouvez approfondir chaque mesure d'intégrité pour obtenir une vue comparative du chemin virtuel de superposition et des chemins de membre de sous-couche pour la même mesure. Cela aiderait à résoudre les problèmes de superposition par rapport aux problèmes de sous-couche.



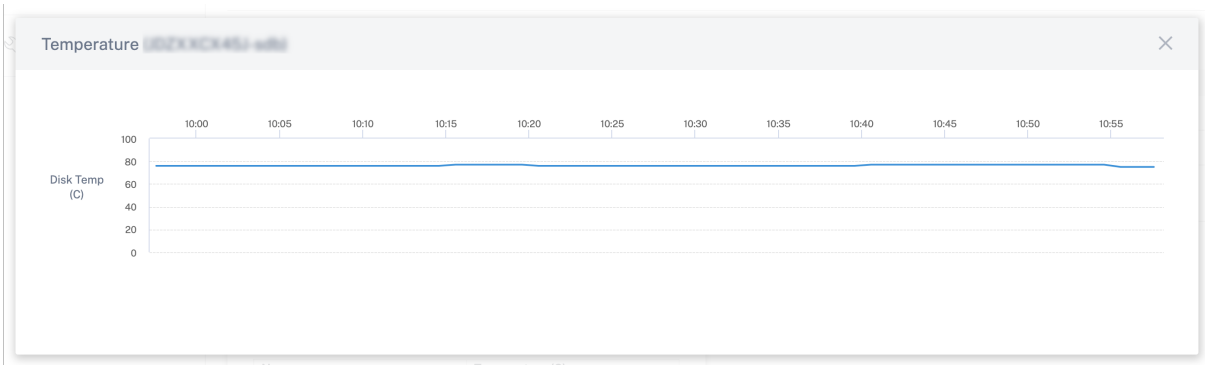
Devices

L'onglet **Appareils** affiche les détails associés aux appareils, aux interfaces et à la température du disque du site. Vous pouvez également redémarrer l'appliance, réinitialiser la configuration de l'appliance ou télécharger les journaux des périphériques.

La section **Température** affiche la température du système, du processeur et des disques en degrés Celsius.



Vous pouvez également cliquer sur l'icône graphique dans la colonne **Température (C)** et afficher les informations sous forme graphique.



Dépannage des fournisseurs

October 21, 2022

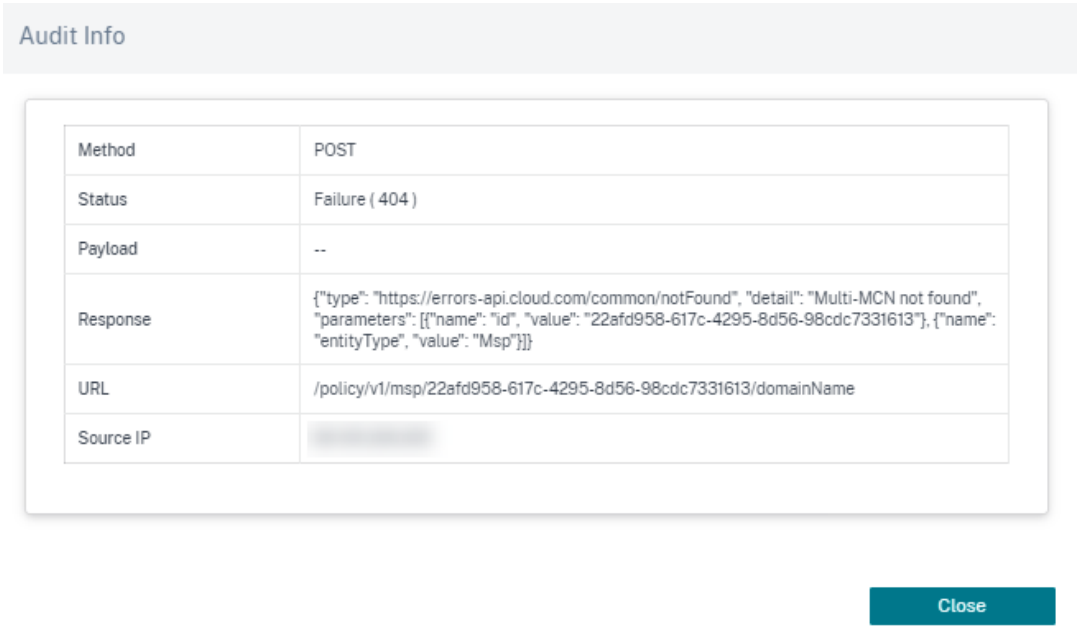
La page des journaux d'audit des fournisseurs affiche les journaux au niveau du fournisseur et les journaux des appareils, ce qui permet un dépannage rapide.

Journaux d'audit

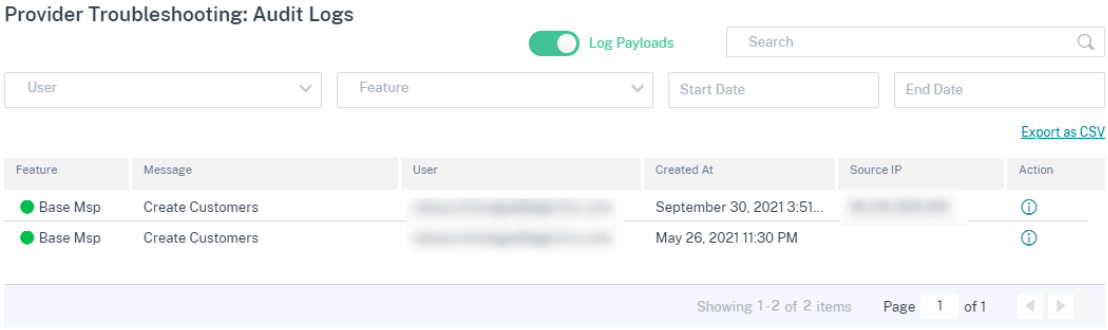
Les journaux d'audit enregistrent l'action, l'heure et le résultat de l'action effectuée par les fournisseurs. Accédez à **Résolution des problèmes** > **Journaux d'audit** pour afficher la page **Dépannage des fournisseurs : journaux d'audit** .

La page des journaux d'audit des fournisseurs affiche les informations suivantes :

- **Barre de recherche** : recherchez une activité d'audit en fonction d'un mot clé.
- **Options de filtrage** : exécutez une recherche dans le journal d'audit en filtrant selon les critères suivants :
  - Utilisateur
  - Fonctionnalité
  - Intervalle de temps
- **Exporter au format CSV** : lorsque vous cliquez sur cette option, les entrées du journal d'audit sont exportées vers un fichier CSV.
- **Informations d'audit** : sélectionnez l'icône dans la colonne **Action** pour accéder à la section **Informations d'audit** . Cette section fournit les informations suivantes :
  - **Méthode : méthode**de requête HTTP de l'API invoquée.
  - **État** : résultat de la demande d'API.
  - **Charge utile** : corps de la demande envoyée via l'API.
  - **Réponse : Réponse**d'erreur lorsque la demande d'API échoue. Ce champ s'affiche uniquement lorsque la demande d'API échoue.
  - **URL** : URL HTTP de l'API révoquée.
  - **IP source** : adresse IP du terminal à partir duquel la fonctionnalité a été configurée. Ce champ s'affiche sur la page Journaux d'audit et sur la page Informations d'audit.



- **Enregistrer les charges utiles** : par défaut, cette option est désactivée. Lorsque cette option est activée, le corps de requête du message d'API s'affiche dans la section **Informations d'audit** . Pour plus d'informations sur l'API, consultez le guide de l'API pour Citrix SD-WAN Orchestrator.



Dépannage réseau

October 21, 2022

Les clients peuvent consulter les journaux de toutes les appliances réseau, ce qui permet un dépannage rapide.

Journaux d'audit

Les journaux d'audit capturent l'action, l'heure et le résultat de l'action effectuée par les utilisateurs sur le réseau d'un client. Accédez à **Résolution des problèmes du SD-WAN** > **Journaux d'audit** pour afficher la page **Journaux d'audit de dépannage du SD-WAN** .

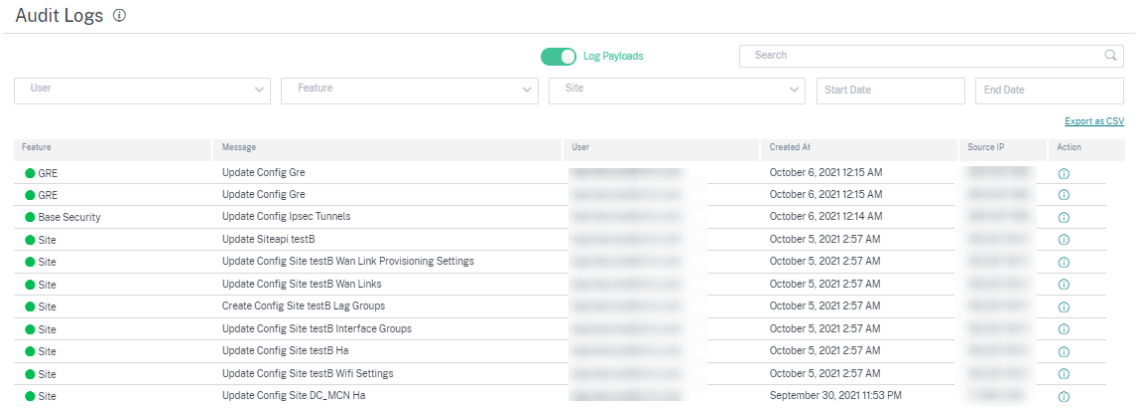
La page Journaux d'audit de dépannage du SD-WAN affiche les informations suivantes :

- **Barre de recherche** : recherchez une activité d'audit en fonction d'un mot clé.
- **Options de filtrage** : exécutez une recherche dans le journal d'audit en filtrant selon les critères suivants :
  - Utilisateur
  - Fonctionnalité
  - Site
  - Intervalle de temps
- **Exporter au format CSV** : lorsque vous cliquez sur cette option, les entrées du journal d'audit sont exportées vers un fichier CSV.
- **Informations d'audit** : sélectionnez l'icône dans la colonne **Action** pour accéder à la section **Informations d'audit** . Cette section fournit les informations suivantes :
  - **Méthode : méthode**de requête HTTP de l'API invoquée.
  - **État** : résultat de la demande d'API. La réponse d'erreur suivante s'affiche lorsque la demande d'API échoue.
  - **Charge utile** : corps de la demande envoyée via l'API.
  - **Réponse : Réponse**d'erreur lorsque la demande d'API échoue. Ce champ s'affiche uniquement lorsque la demande d'API échoue.
  - **URL** : URL HTTP de l'API révoquée.

- **IP source** : adresse IP du terminal à partir duquel la fonctionnalité a été configurée. Ce champ s'affiche sur la page Journaux d'audit et sur la page Informations d'audit.

- **Ce qui a changé** : cette section affiche les journaux de toutes les modifications apportées aux fonctionnalités via l'interface utilisateur. Activez le bouton Log Payloads pour afficher les modifications apportées à la section Informations d'audit.

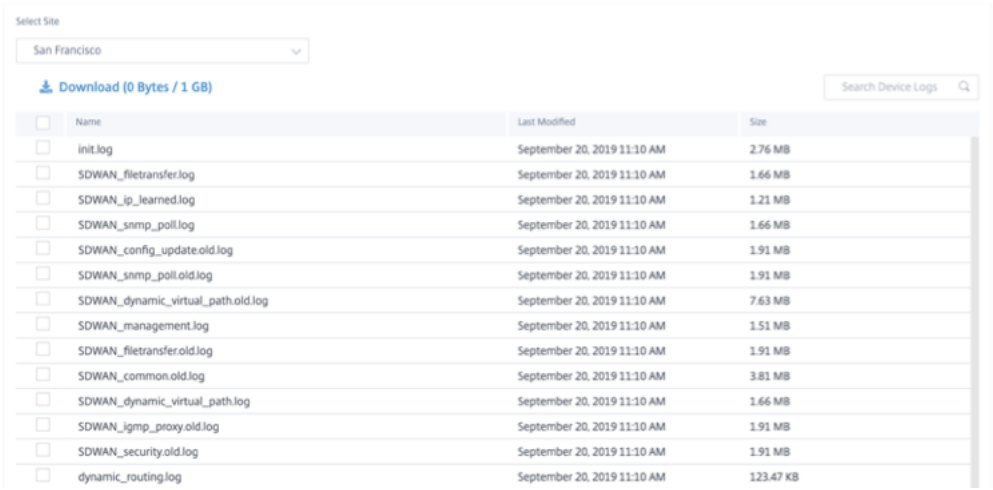
- **Enregistrer les charges utiles** : par défaut, cette option est désactivée. Lorsque cette option est activée, le corps de requête du message d'API s'affiche dans la section **Informations d'audit** . Pour plus d'informations sur l'API, consultez le guide de l'API pour Citrix SD-WAN Orchestrator.



Journaux périphériques

Les clients peuvent afficher les journaux des périphériques spécifiques aux sites.

Vous pouvez sélectionner des journaux de périphériques spécifiques, les télécharger et les partager avec les administrateurs du site si nécessaire.

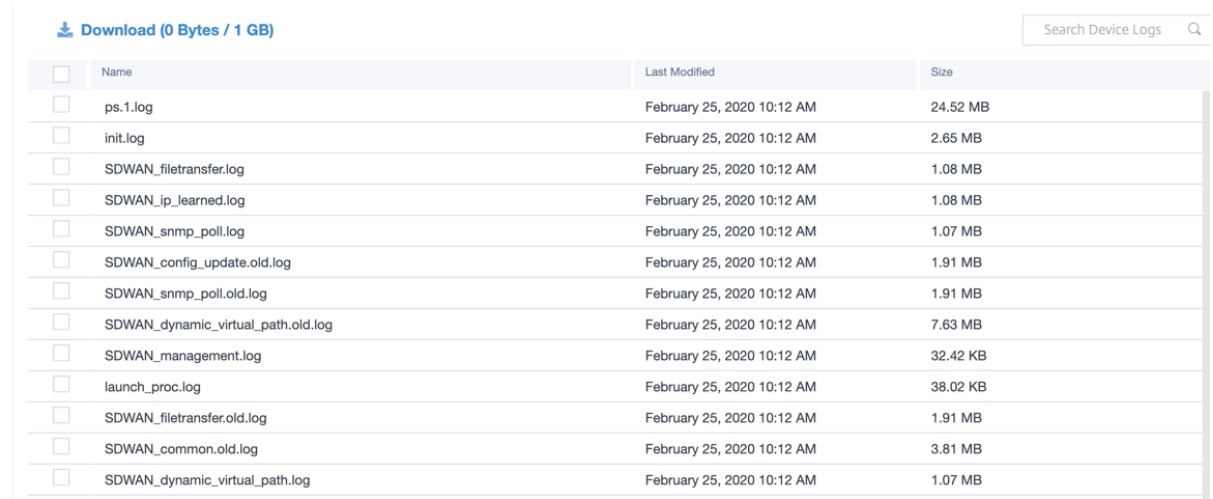


Dépannage du site

October 21, 2022

Journaux périphériques

Les journaux sont utiles pour résoudre les problèmes. L'administrateur du site peut afficher une liste de tous les journaux capturés sur tous les périphériques du site. Vous pouvez également télécharger des journaux pour une vérification ultérieure.

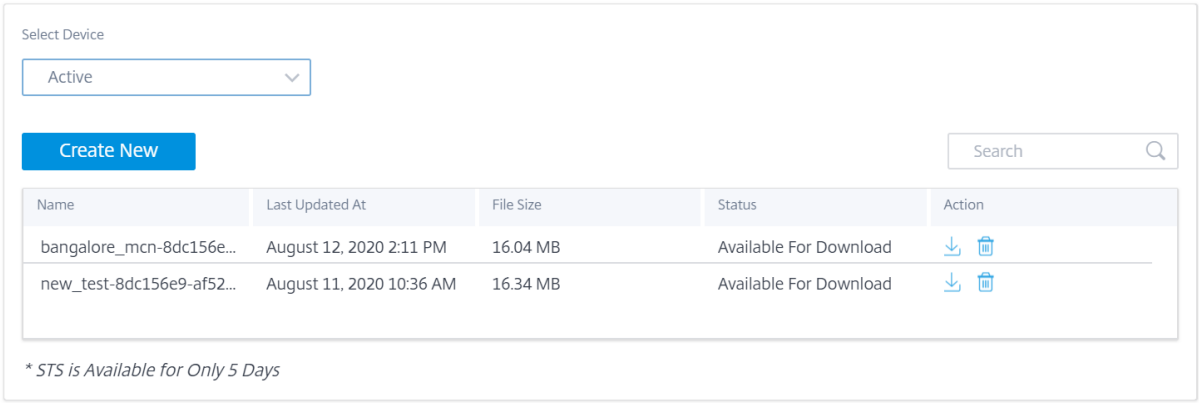


Afficher l'offre groupée de support technique

Le pack Show Tech Support (STS) contient des informations système importantes en temps réel telles que les journaux d'accès, les journaux de diagnostic, les journaux de pare-feu. Le bundle STS est utilisé pour résoudre les problèmes dans les appliances SD-WAN. Vous pouvez créer, télécharger l'offre groupée STS et le partager avec les représentants du support Citrix.

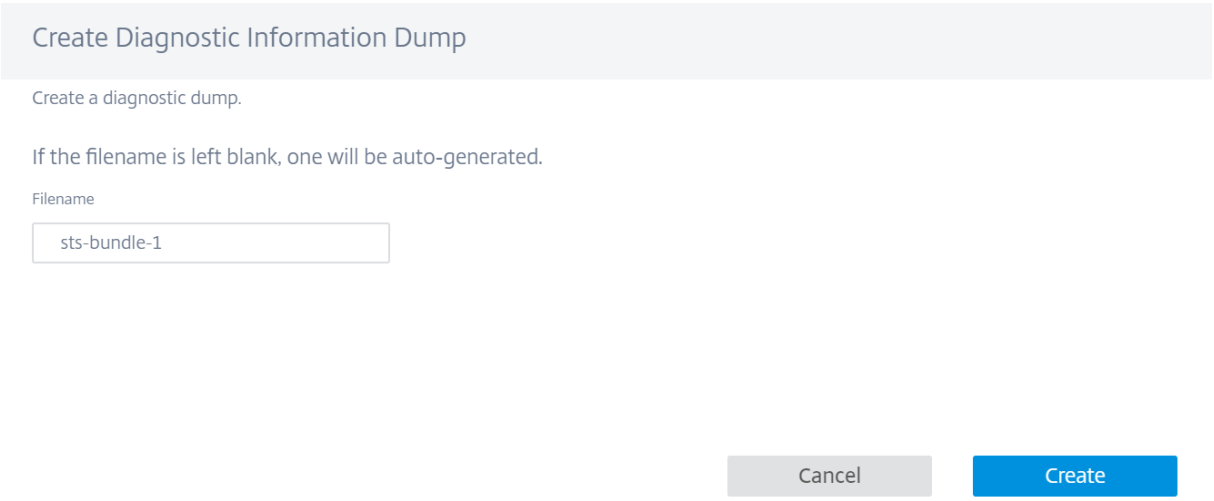
Si un site est configuré en mode de déploiement HA, vous pouvez sélectionner l'appliance active ou en veille pour laquelle vous souhaitez créer ou télécharger le bundle STS.

Pour créer un bundle STS pour une appliance de site, au niveau du site, accédez à **Résolution des problèmes** > **Bundle STS** et cliquez sur **Créer un nouveau**.



Indiquez un nom pour l'ensemble STS. Le nom doit commencer par une lettre et peut contenir des lettres, des chiffres, des tirets et des sous-scores. La longueur maximale autorisée du nom est de 32 caractères. Le nom fourni par l'utilisateur est utilisé comme préfixe dans le nom final. Pour garantir que les noms de fichiers sont uniques (horodatage) et pour aider à reconnaître le périphérique dans le package STS (numéro de série), le service génère un nom complet. Si aucun nom n'est fourni, un nom est généré automatiquement lors de la création du bundle.

Vous pouvez demander un nouveau STS uniquement lorsque l'appareil est en ligne et qu'aucun processus STS n'est actuellement en cours d'exécution sur l'appliance. Vous pouvez télécharger un STS déjà disponible à partir du service Citrix SD-WAN Orchestrator même si l'appareil est hors ligne.



À tout moment, le processus STS est dans l'un des états suivants :

Statut STS	Description
Demandé	Un nouveau forfait STS est demandé. Le traitement de la demande prend quelques minutes. Vous pouvez choisir d'annuler le processus de création STS, si nécessaire.
Chargement	Le package STS créé est téléchargé sur le service cloud. La durée dépend de la taille du colis. L'état est mis à jour toutes les 5 secondes. Vous ne pouvez pas annuler le processus de téléchargement STS.
Échec	Le processus STS a échoué lors de la création ou du téléchargement. Vous pouvez supprimer les entrées des opérations STS ayant échoué.
Disponible en téléchargement	Le processus de création et de téléchargement de STS est réussi. Vous pouvez maintenant télécharger ou supprimer les packages STS.

Une fois que le processus STS démarre sur l'appliance, la progression est mise à jour à intervalles réguliers dans la colonne d'état. Par exemple, **Requested (collecte de fichiers journaux)**.

Les packs STS et les dossiers d'échec sont conservés pendant 7 jours, après quoi ils sont automatiquement supprimés.

Rapports du fournisseur

October 21, 2022

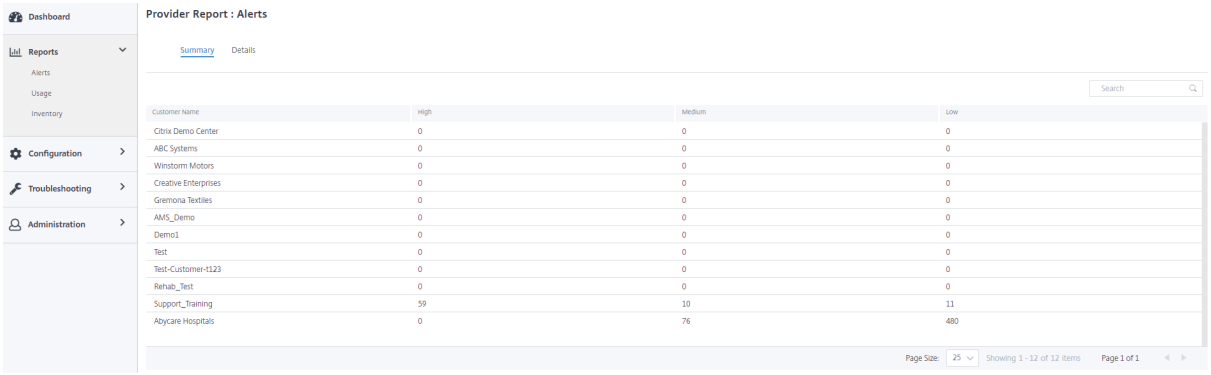
Les **rapports sur les fournisseurs** fournissent une visibilité sur les alertes, les tendances d'utilisation et l'inventaire agrégé de tous les clients gérés par un fournisseur.

Dans l'interface utilisateur de niveau fournisseur de services Citrix SD-WAN Orchestrator, accédez à **Reports**.

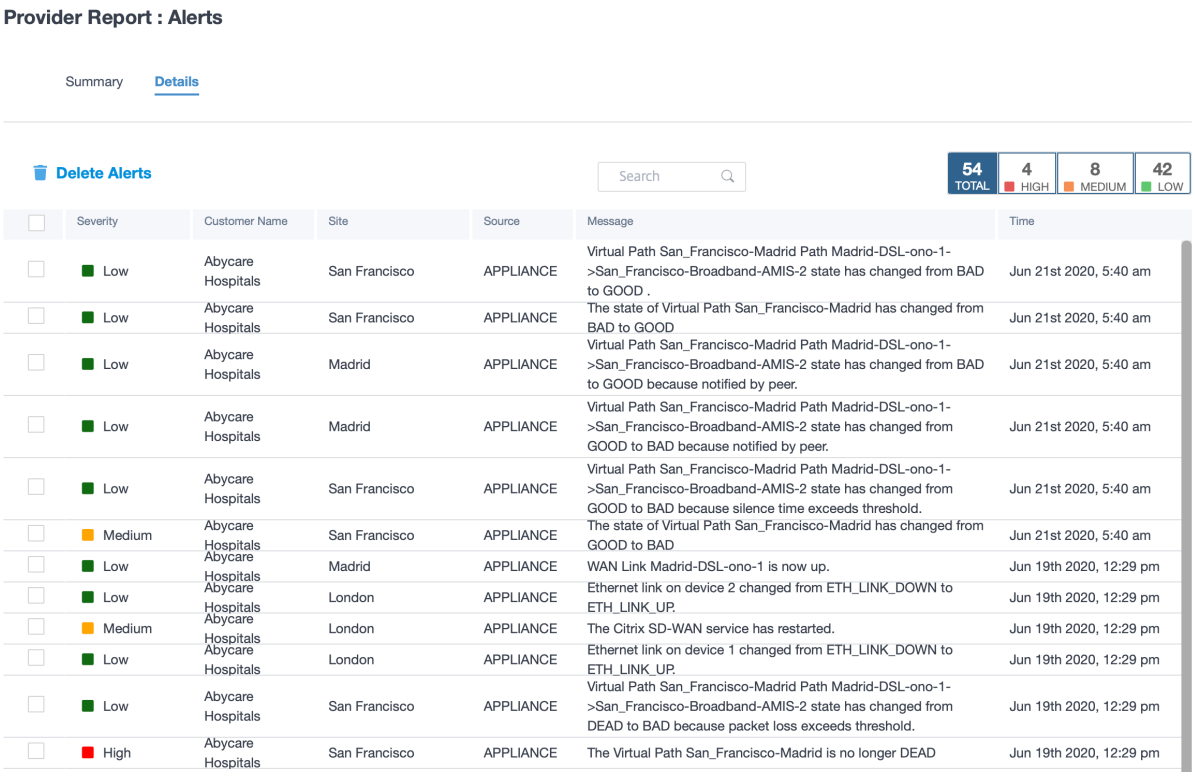
Alertes

Le fournisseur peut passer en revue tous les événements et alertes générés sur l'ensemble des réseaux clients.

La vue **récapitulative** affiche le nombre d'alertes élevées, moyennes et faibles pour chaque client.



Vous pouvez également consulter la gravité, le site d'origine de l'alerte, le message d'alerte, l'heure et d'autres informations sous **Détails**.



Severity	Customer Name	Site	Source	Message	Time
Low	Abycare Hospitals	San Francisco	APPLIANCE	Virtual Path San_Francisco-Madrid Path Madrid-DSL-ono-1->San_Francisco-Broadband-AMIS-2 state has changed from BAD to GOOD .	Jun 21st 2020, 5:40 am
Low	Abycare Hospitals	San Francisco	APPLIANCE	The state of Virtual Path San_Francisco-Madrid has changed from BAD to GOOD	Jun 21st 2020, 5:40 am
Low	Abycare Hospitals	Madrid	APPLIANCE	Virtual Path San_Francisco-Madrid Path Madrid-DSL-ono-1->San_Francisco-Broadband-AMIS-2 state has changed from BAD to GOOD because notified by peer.	Jun 21st 2020, 5:40 am
Low	Abycare Hospitals	Madrid	APPLIANCE	Virtual Path San_Francisco-Madrid Path Madrid-DSL-ono-1->San_Francisco-Broadband-AMIS-2 state has changed from GOOD to BAD because notified by peer.	Jun 21st 2020, 5:40 am
Low	Abycare Hospitals	San Francisco	APPLIANCE	Virtual Path San_Francisco-Madrid Path Madrid-DSL-ono-1->San_Francisco-Broadband-AMIS-2 state has changed from GOOD to BAD because silence time exceeds threshold.	Jun 21st 2020, 5:40 am
Medium	Abycare Hospitals	San Francisco	APPLIANCE	The state of Virtual Path San_Francisco-Madrid has changed from GOOD to BAD	Jun 21st 2020, 5:40 am
Low	Abycare Hospitals	Madrid	APPLIANCE	WAN Link Madrid-DSL-ono-1 is now up.	Jun 19th 2020, 12:29 pm
Low	Abycare Hospitals	London	APPLIANCE	Ethernet link on device 2 changed from ETH_LINK_DOWN to ETH_LINK_UP.	Jun 19th 2020, 12:29 pm
Medium	Abycare Hospitals	London	APPLIANCE	The Citrix SD-WAN service has restarted.	Jun 19th 2020, 12:29 pm
Low	Abycare Hospitals	London	APPLIANCE	Ethernet link on device 1 changed from ETH_LINK_DOWN to ETH_LINK_UP.	Jun 19th 2020, 12:29 pm
Low	Abycare Hospitals	San Francisco	APPLIANCE	Virtual Path San_Francisco-Madrid Path Madrid-DSL-ono-1->San_Francisco-Broadband-AMIS-2 state has changed from DEAD to BAD because packet loss exceeds threshold.	Jun 19th 2020, 12:29 pm
High	Abycare Hospitals	San Francisco	APPLIANCE	The Virtual Path San_Francisco-Madrid is no longer DEAD	Jun 19th 2020, 12:29 pm

Des options de filtrage appropriées peuvent être utilisées au besoin, par exemple : recherchez les alertes de gravité élevée pour tous les clients, ou les alertes pour un client donné, etc.

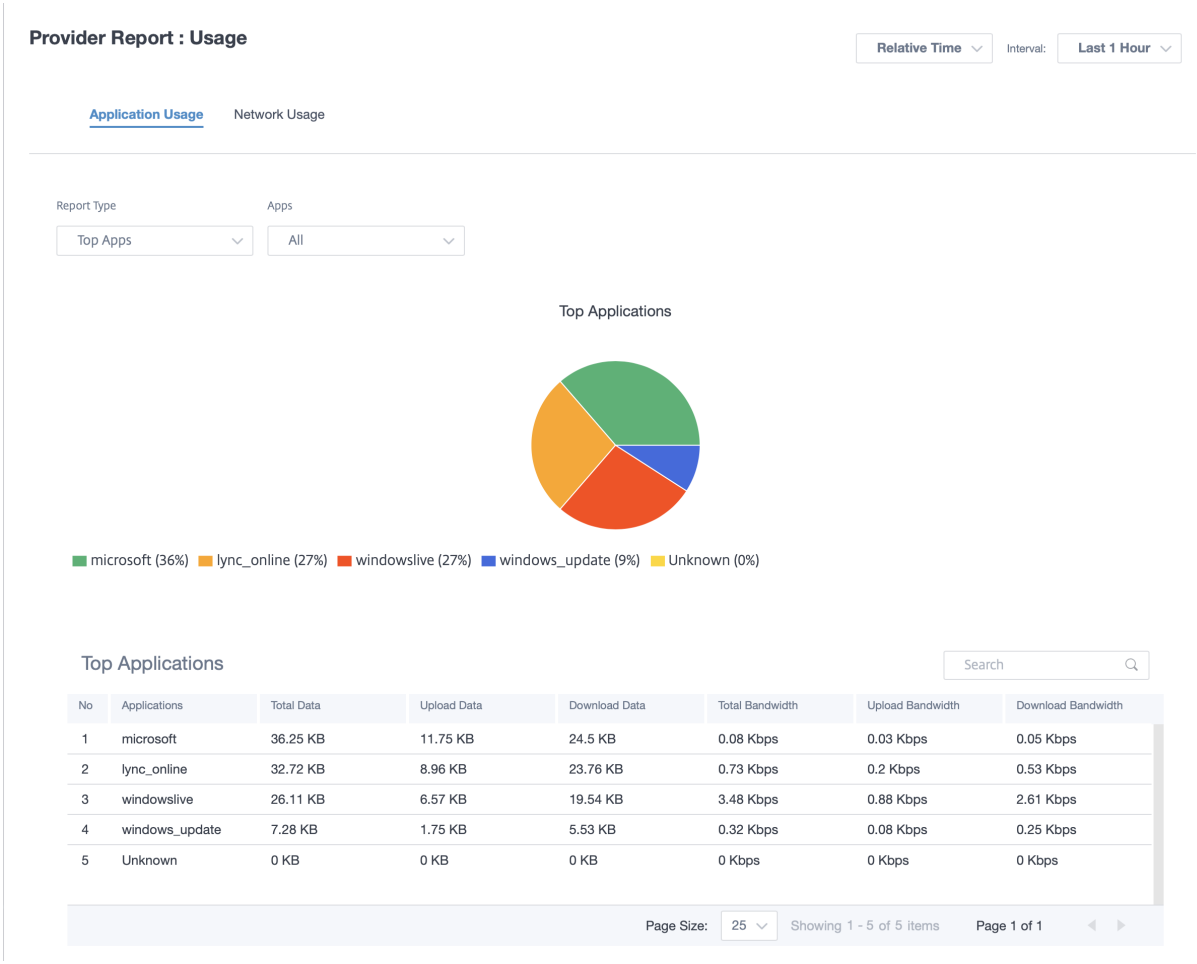
Vous pouvez également sélectionner et supprimer des alertes.

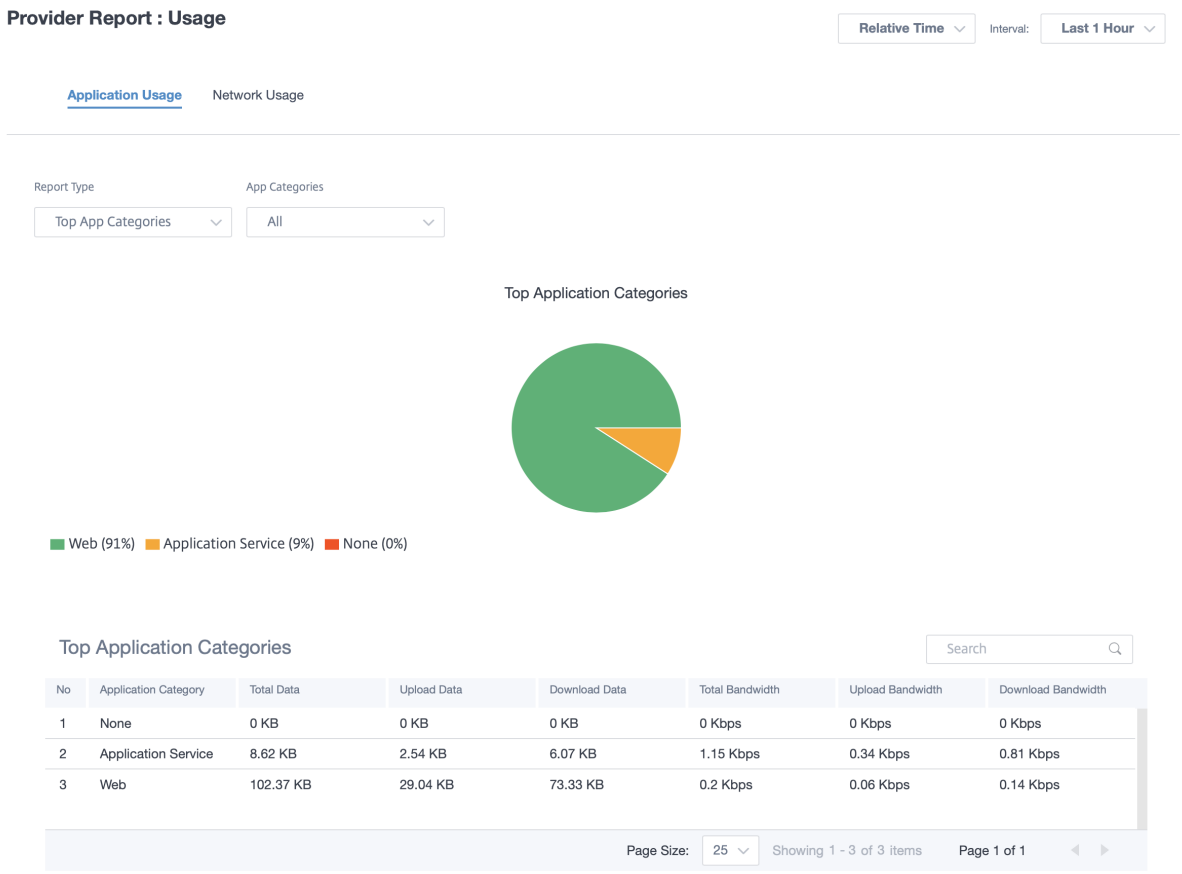
Utilisation

Le fournisseur peut examiner les tendances d'utilisation de plusieurs clients, telles que les **meilleures applications, lesprincipales catégories d'applications, la bande passante**des applications et les **meilleurs sites**.

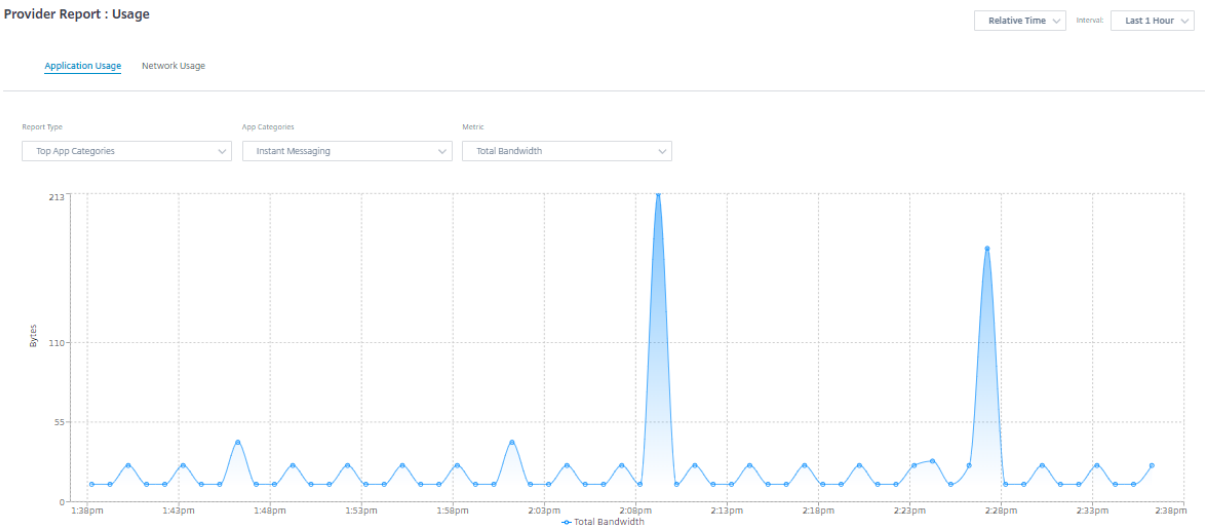
Principales catégories d'applications et d'applications

Le graphique **des principales applications** et des **principales catégories** d'applications montre les applications et les familles d'applications les plus utilisées sur l'ensemble des réseaux clients. Cela vous permet d'analyser le modèle de consommation de données et de réaffecter la limite de bande passante pour chaque classe de données, si nécessaire.





Vous pouvez afficher les statistiques d'utilisation de la bande passante. Les statistiques de bande passante sont collectées pour l'intervalle de temps sélectionné. Vous pouvez filtrer le rapport de statistiques en fonction du **type de rapport, des applications ou des catégories d'applications** et **des mesures**.



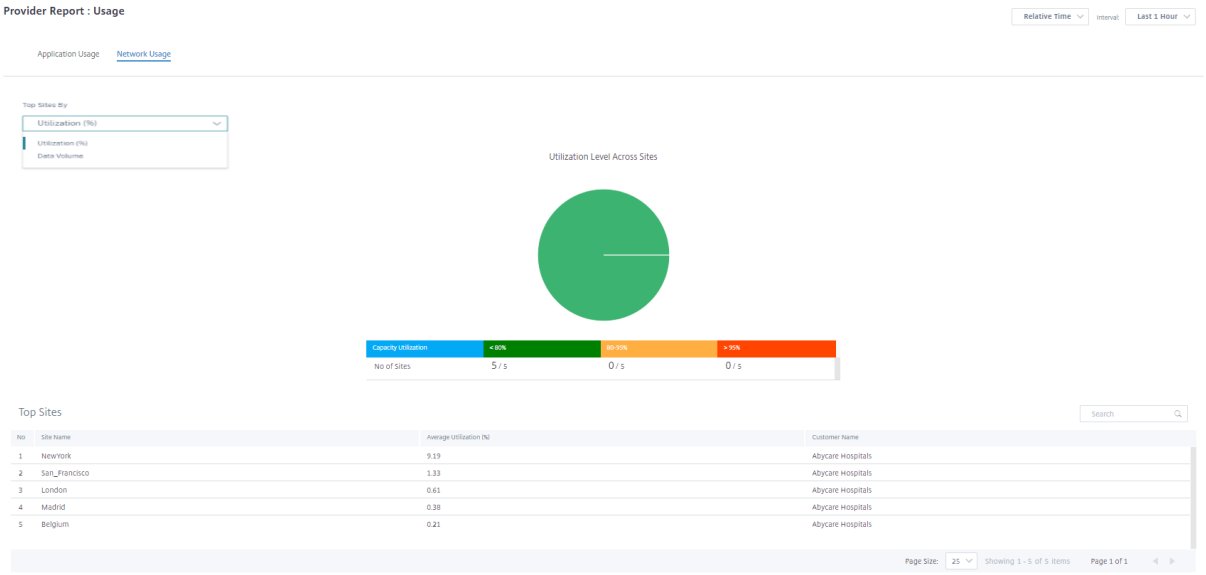
- **Type de rapport :** sélectionnez les **meilleures applications ou catégories** d'applications dans

la liste.

- **Applications/Catégories d'applications :** sélectionnez l'application ou les catégories les plus populaires dans la liste.
- **Mesure :** Sélectionnez la métrique de bande passante (telle que les données totales, les données entrantes, la bande passante totale) dans la liste.

Utilisation du réseau

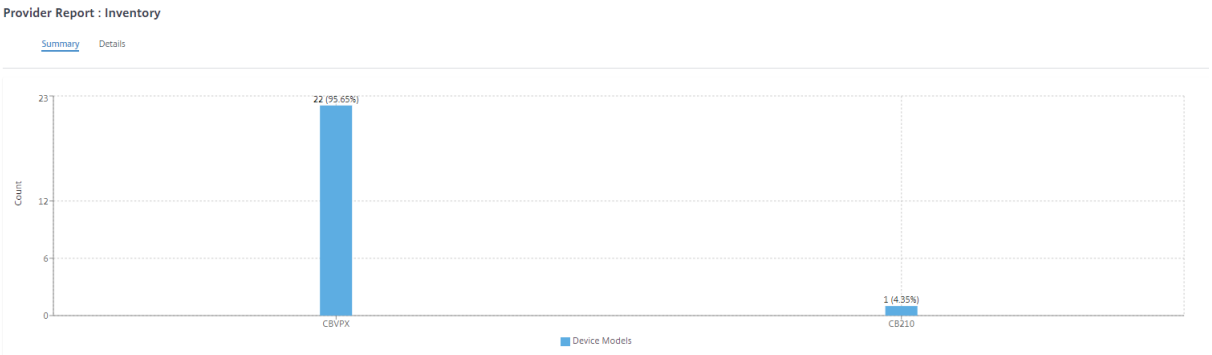
Le graphique d'utilisation du réseau représente les 10 principaux sites de tous les clients qui utilisent la bande passante la plus élevée. Vous pouvez afficher les sites par utilisation (%) ou par volume de données (Mo).



Inventory

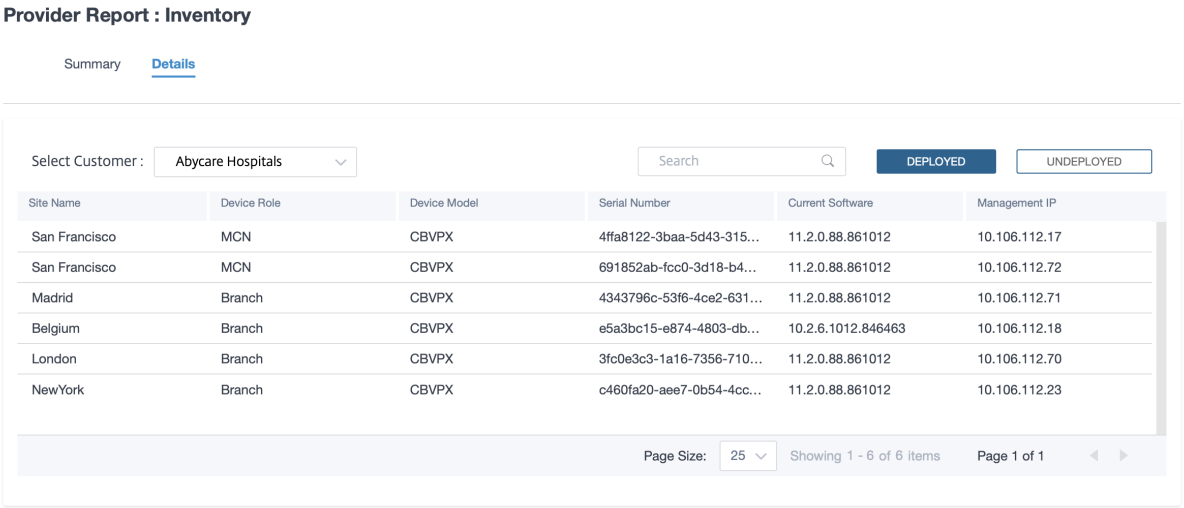
Le fournisseur peut afficher l'ensemble de l'inventaire des appareils pour tous les clients. Vous pouvez choisir d'afficher un résumé de l'inventaire ou une vue détaillée.

La vue récapitulative des stocks fournit un graphique de la répartition des stocks, décrivant les différents modèles d'appliance et le nombre de chaque type d'appliances utilisés sur les réseaux clients.



Des options de filtrage appropriées peuvent être utilisées au besoin, par exemple : recherchez tous les appareils appartenant à un client spécifique, ou tous les appareils avec un certain modèle d'appareil, etc.

La vue détaillée de l'inventaire fournit une liste de toutes les appliances déployées et celles qui sont configurées mais pas encore déployées. Choisissez un client dans la liste déroulante **Sélectionner un client** . Vous pouvez consulter le nom du site, le rôle de l'appareil, le modèle de l'appareil, le numéro de série de l'appareil, le logiciel actuel et l'adresse IP de gestion des appareils



Rapports client/réseau

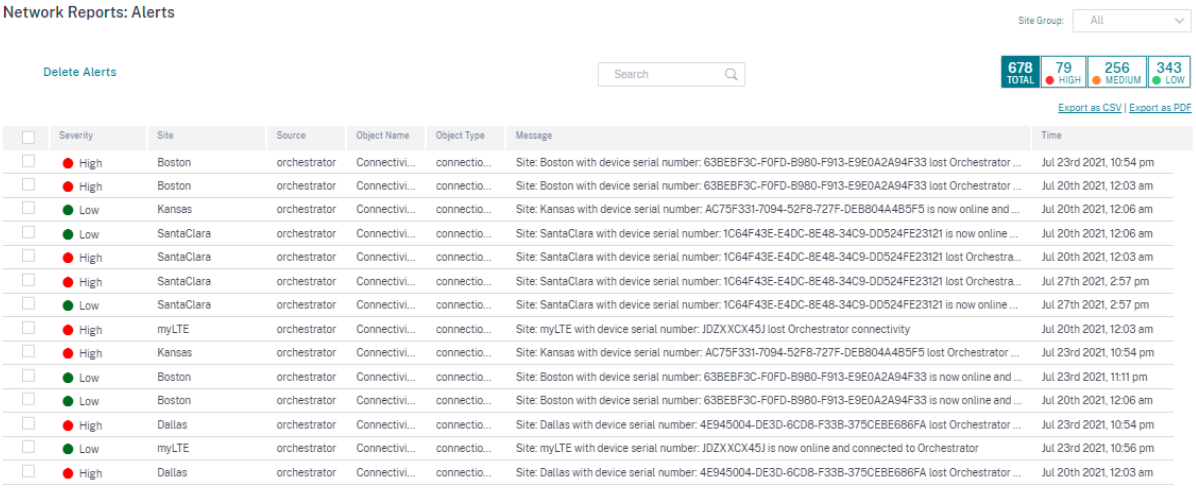
October 21, 2022

Les **rapports clients** fournissent une visibilité sur les alertes à l'échelle du réseau, les tendances d'utilisation, l'inventaire, la qualité, les diagnostics et l'état du pare-feu agrégés sur tous les sites d'un réseau client.

Alertes

Le client peut consulter un rapport détaillé de tous les événements et alertes générés sur tous les sites de ce réseau.

Il inclut la gravité, le site d'origine de l'alerte, le message d'alerte, l'heure et d'autres détails.



Severity	Site	Source	Object Name	Object Type	Message	Time
High	Boston	orchestrator	Connectivi...	connectio...	Site: Boston with device serial number: 63BEBF3C-F0FD-B980-F913-E9E0A2A94F33 lost Orchestrator ...	Jul 23rd 2021, 10:54 pm
High	Boston	orchestrator	Connectivi...	connectio...	Site: Boston with device serial number: 63BEBF3C-F0FD-B980-F913-E9E0A2A94F33 lost Orchestrator ...	Jul 20th 2021, 12:03 am
Low	Kansas	orchestrator	Connectivi...	connectio...	Site: Kansas with device serial number: AC75F331-7094-52F8-727F-DEB804A4B5F5 is now online and ...	Jul 20th 2021, 12:06 am
Low	SantaClara	orchestrator	Connectivi...	connectio...	Site: SantaClara with device serial number: 1C64F43E-E4DC-8E48-34C9-DD524FE23121 is now online ...	Jul 20th 2021, 12:06 am
High	SantaClara	orchestrator	Connectivi...	connectio...	Site: SantaClara with device serial number: 1C64F43E-E4DC-8E48-34C9-DD524FE23121 lost Orchestra...	Jul 20th 2021, 12:03 am
High	SantaClara	orchestrator	Connectivi...	connectio...	Site: SantaClara with device serial number: 1C64F43E-E4DC-8E48-34C9-DD524FE23121 lost Orchestra...	Jul 27th 2021, 2:57 pm
Low	SantaClara	orchestrator	Connectivi...	connectio...	Site: SantaClara with device serial number: 1C64F43E-E4DC-8E48-34C9-DD524FE23121 is now online ...	Jul 27th 2021, 2:57 pm
High	myLTE	orchestrator	Connectivi...	connectio...	Site: myLTE with device serial number: JDZXXCX45J lost Orchestrator connectivity	Jul 20th 2021, 12:03 am
High	Kansas	orchestrator	Connectivi...	connectio...	Site: Kansas with device serial number: AC75F331-7094-52F8-727F-DEB804A4B5F5 lost Orchestrator ...	Jul 23rd 2021, 10:54 pm
Low	Boston	orchestrator	Connectivi...	connectio...	Site: Boston with device serial number: 63BEBF3C-F0FD-B980-F913-E9E0A2A94F33 is now online and ...	Jul 23rd 2021, 11:11 pm
Low	Boston	orchestrator	Connectivi...	connectio...	Site: Boston with device serial number: 63BEBF3C-F0FD-B980-F913-E9E0A2A94F33 is now online and ...	Jul 20th 2021, 12:06 am
High	Dallas	orchestrator	Connectivi...	connectio...	Site: Dallas with device serial number: 4E945004-DE3D-6CD8-F33B-375CEBE686FA lost Orchestrator ...	Jul 23rd 2021, 10:54 pm
Low	myLTE	orchestrator	Connectivi...	connectio...	Site: myLTE with device serial number: JDZXXCX45J is now online and connected to Orchestrator	Jul 23rd 2021, 10:56 pm
High	Dallas	orchestrator	Connectivi...	connectio...	Site: Dallas with device serial number: 4E945004-DE3D-6CD8-F33B-375CEBE686FA lost Orchestrator ...	Jul 20th 2021, 12:03 am

Des options de filtrage appropriées peuvent être utilisées au besoin, par exemple : recherchez toutes les alertes de gravité élevée sur tous les sites, ou toutes les alertes pour un site particulier, etc.

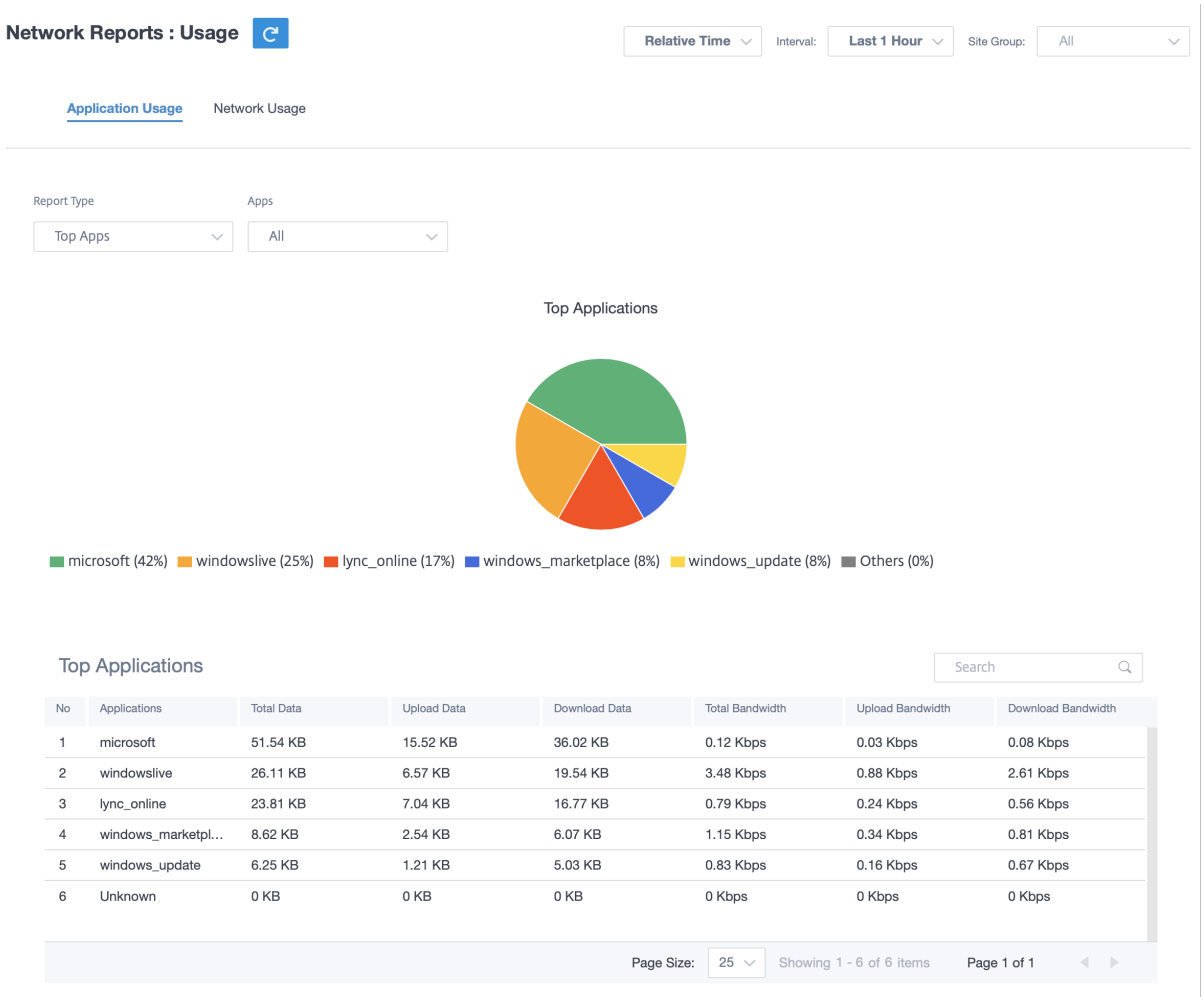
Vous pouvez également sélectionner et effacer les alertes.

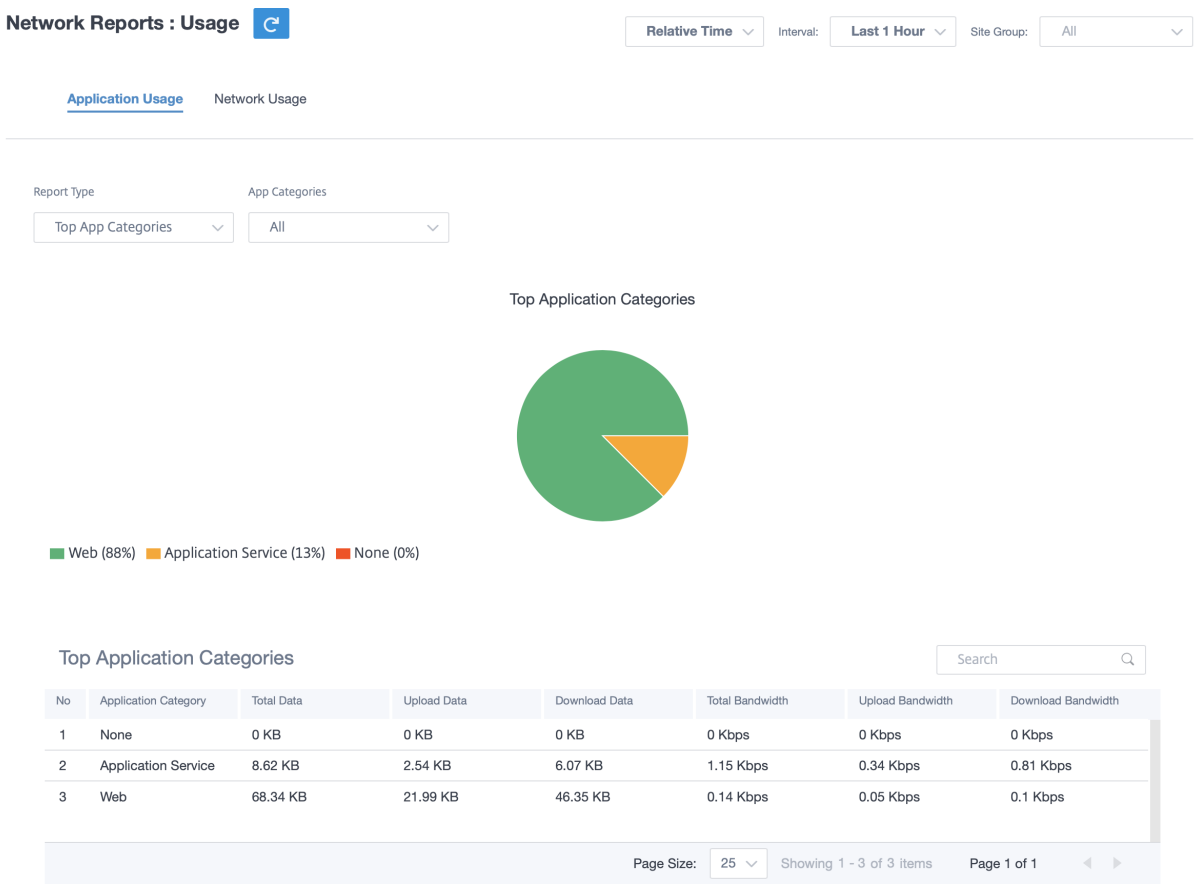
Utilisation

Les clients peuvent consulter les tendances d'utilisation, telles que **les meilleures applications, les principales catégories**d'**applications, la bande passante**des applications et les**meilleurs sites** sur tous les sites de leur réseau.

Principales catégories d'applications et d'applications

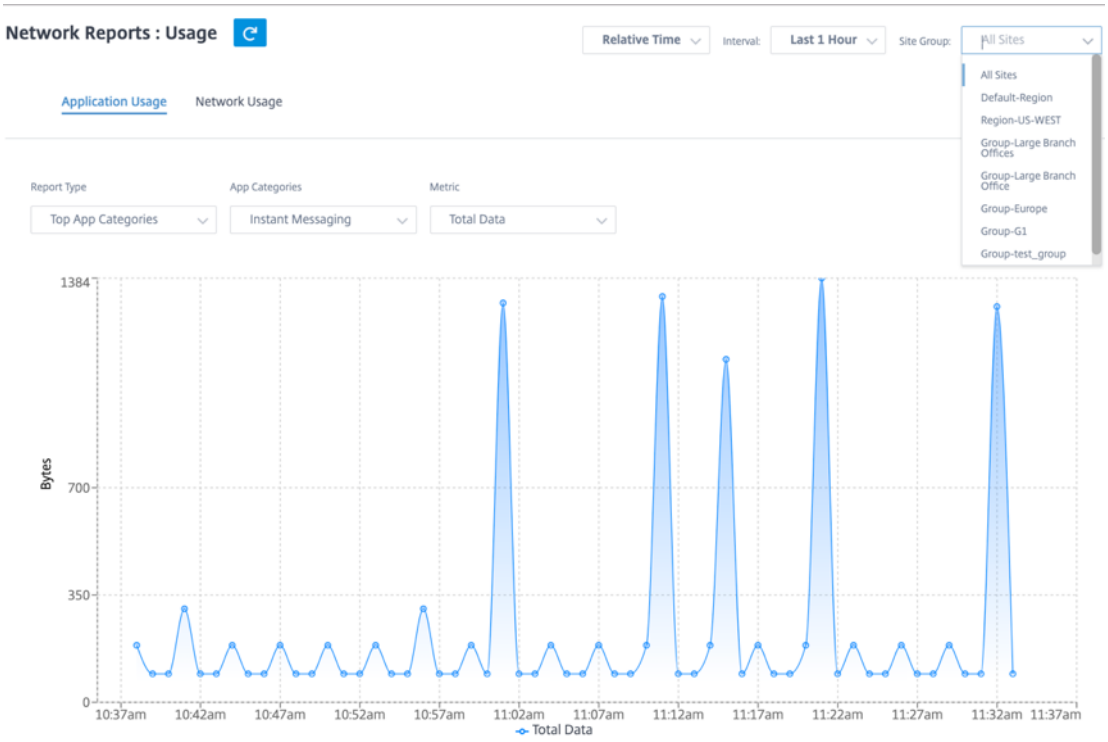
Le graphique **des principales applicationset des principales catégories** d'applications montre les principales applications et familles d'applications les plus utilisées sur tous les sites. Cela vous permet d'analyser le modèle de consommation de données et de réaffecter la limite de bande passante pour chaque classe de données du réseau.





Bande passante des applications

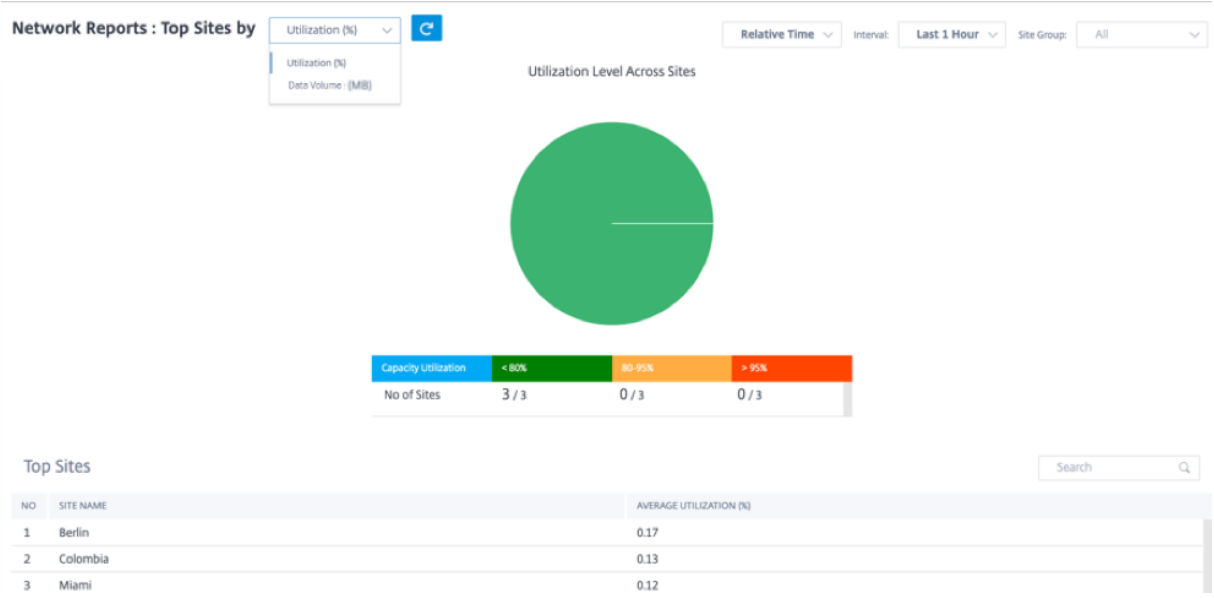
Vous pouvez afficher les statistiques d'utilisation de la bande passante pour le groupe de sites sélectionné ou pour tous les sites. Les statistiques de bande passante sont collectées pour l'intervalle de temps sélectionné. Vous pouvez filtrer le rapport de statistiques en fonction du **type de rapport, des applications ou des catégories d'applications** et **des mesures**.



- **Type de rapport :** sélectionnez les **meilleures applications ou catégories** d'applications dans la liste.
- **Applications/Catégories d'applications :** sélectionnez l'application ou les catégories les plus populaires (telles que le service réseau) dans la liste.
- **Mesure :** Sélectionnez la métrique de bande passante (telle que les données totales, les données entrantes, la bande passante totale) dans la liste.

Utilisation du réseau

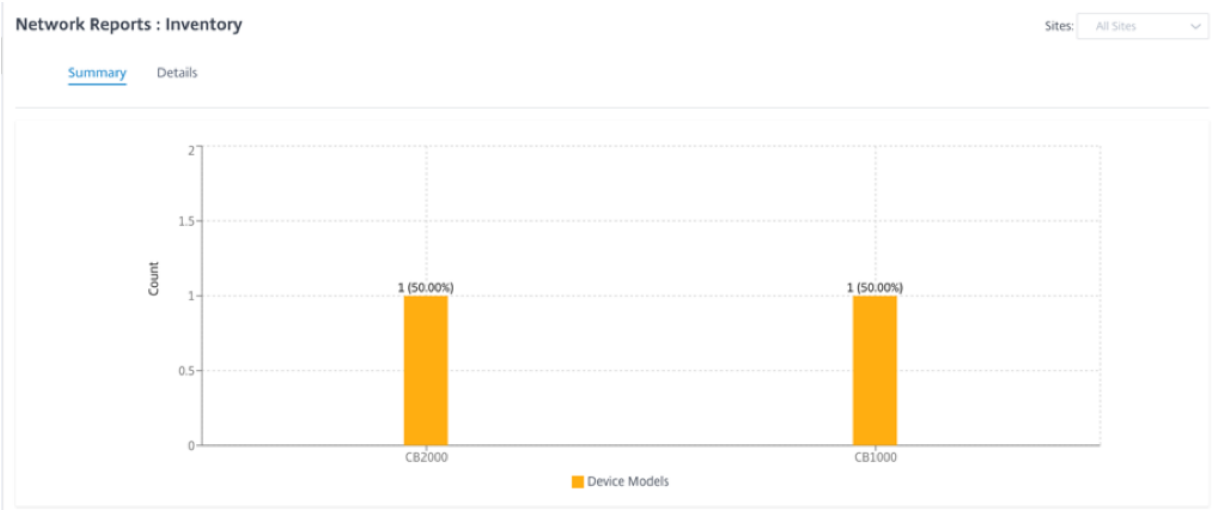
Le graphique **des meilleurs sites** présente les principaux sites du réseau client qui utilisent le plus de bande passante. Vous pouvez consulter les sites par utilisation (%) ou par volume de trafic (Mo).



Inventory

Le client peut consulter l'inventaire complet des appareils sur tous les sites du réseau. Vous pouvez choisir d'afficher un résumé de l'inventaire ou une vue détaillée.

La vue récapitulative des stocks fournit un graphique de la répartition des stocks, représentant les différents modèles d'appliance et le nombre de chaque type d'appliances utilisés sur tous les sites du réseau client.



Des options de filtrage appropriées peuvent être utilisées selon les besoins, par exemple : recherchez tous les appareils appartenant à un site spécifique, ou tous les appareils dotés d'un certain modèle d'appareil, etc.

La vue détaillée de l'inventaire fournit une liste de toutes les appliances déployées et celles qui sont

configurées mais pas encore déployées. Avec le client, le nom du site, le rôle de l'appareil, le numéro de série de l'appareil, le logiciel actuel et l'adresse IP de gestion des périphériques.

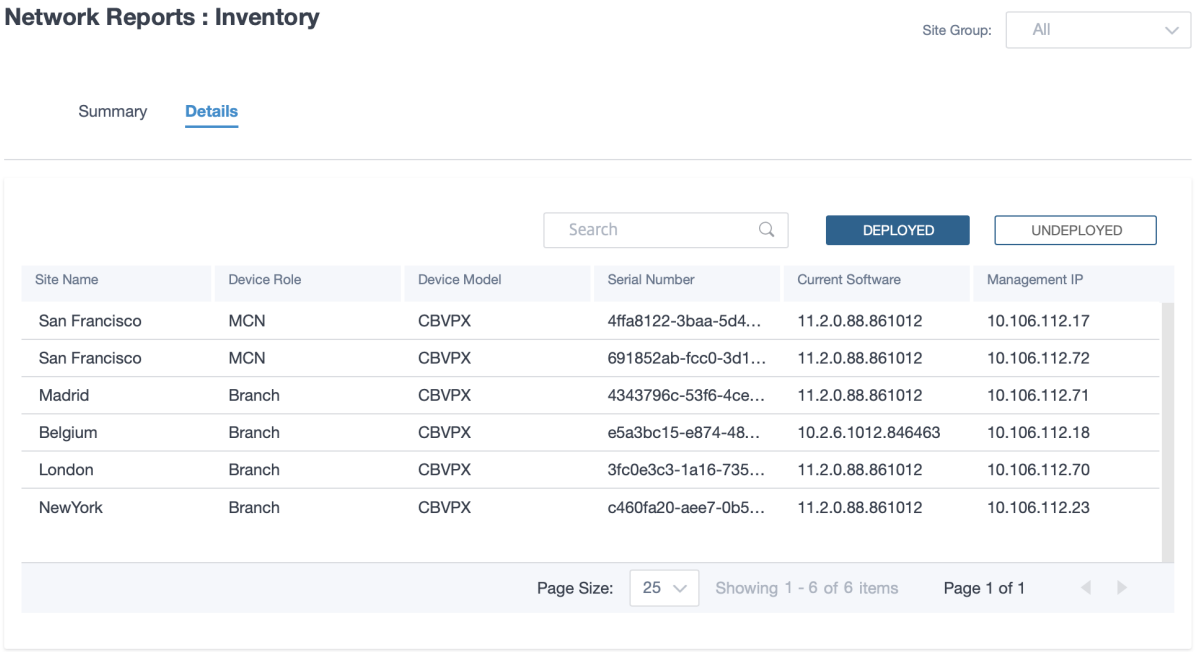
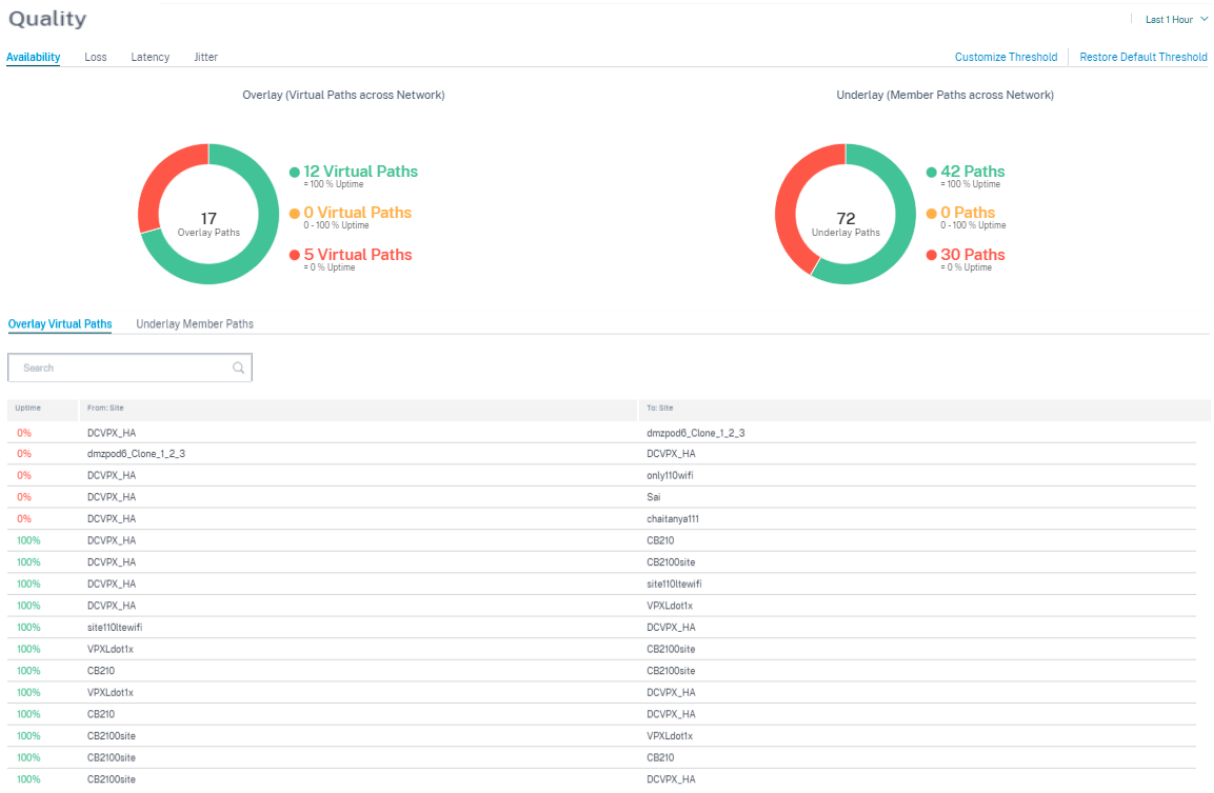


Tableau de bord et rapports HDX

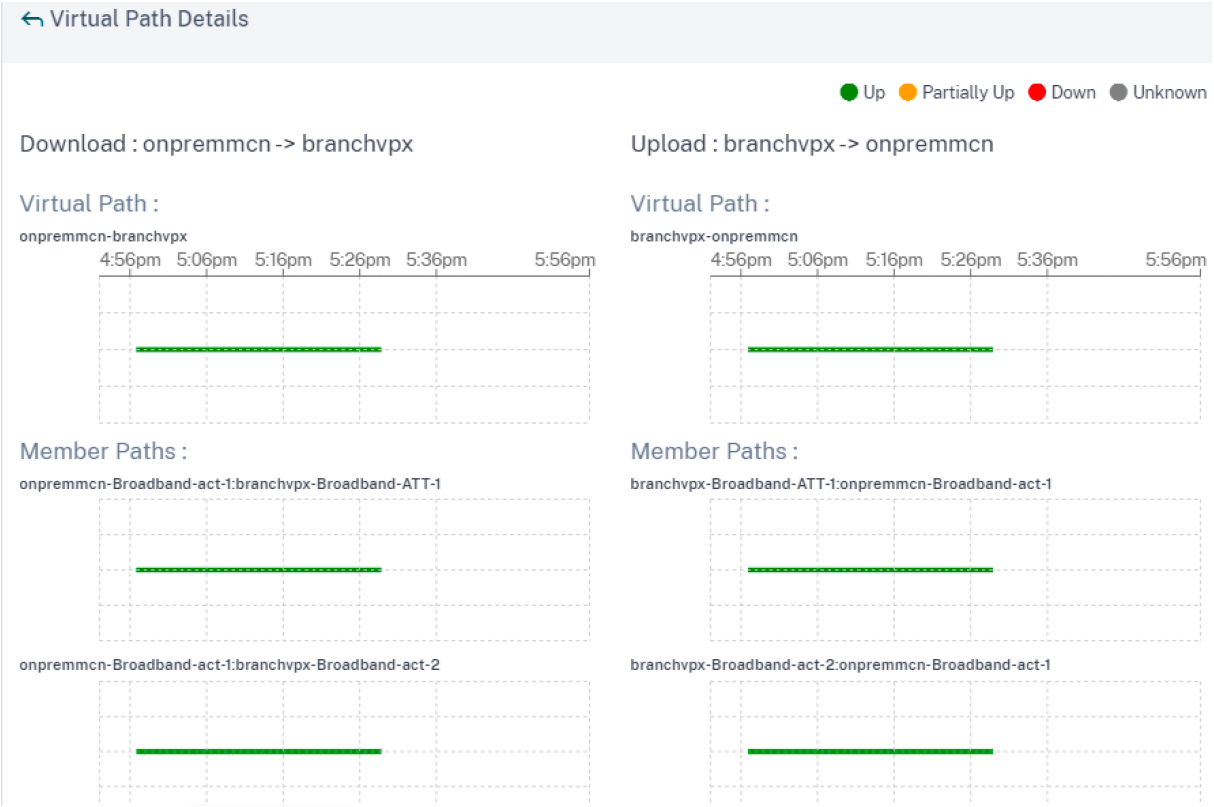
Pour plus de détails sur le tableau de bord et les rapports HDX, voir Tableau de bord et rapportsHDX.

Qualité

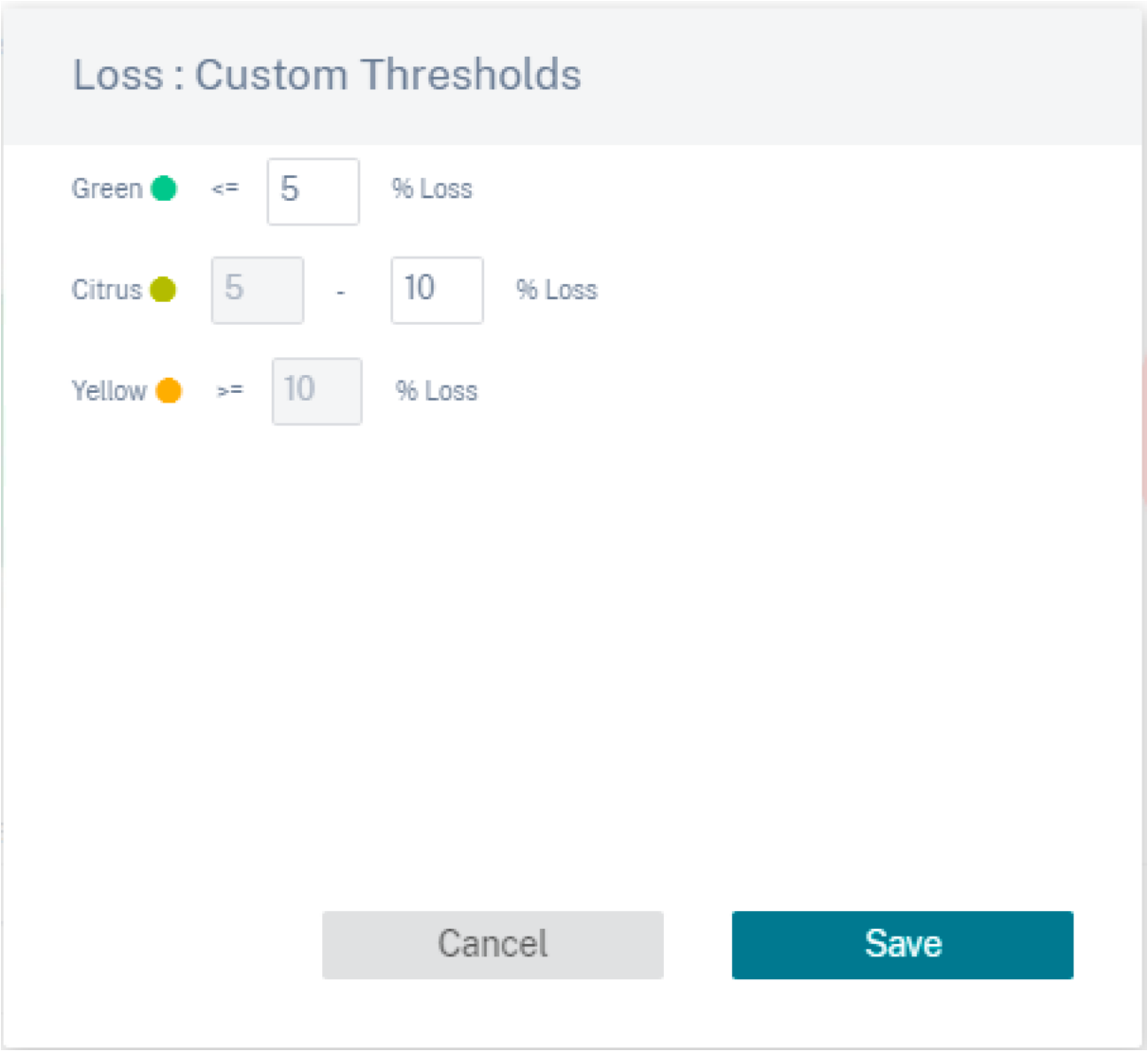
Le rapport sur la **qualité du réseau** permet une comparaison au niveau du réseau entre les chemins de superposition virtuelle et de sous-couche physique en termes de disponibilité et de perte, de latence et de gigue. Cela permet de surveiller efficacement l'évolution de la superposition par rapport au réseau sous-jacent et facilite également la résolution des problèmes. Pour Latency et Jitter, seuls les détails des chemins des membres sous-jacents sont affichés.



Cliquez sur l'entrée du tableau pour voir la vue détaillée.



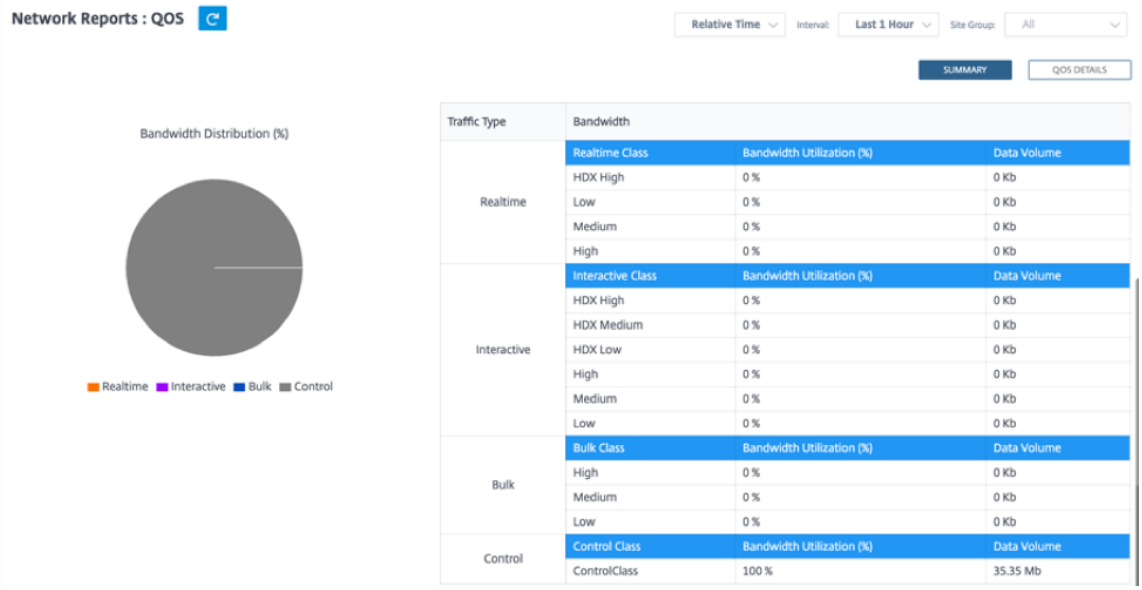
Vous pouvez personnaliser le seuil pour chaque paramètre de qualité du réseau.



Qualité du service

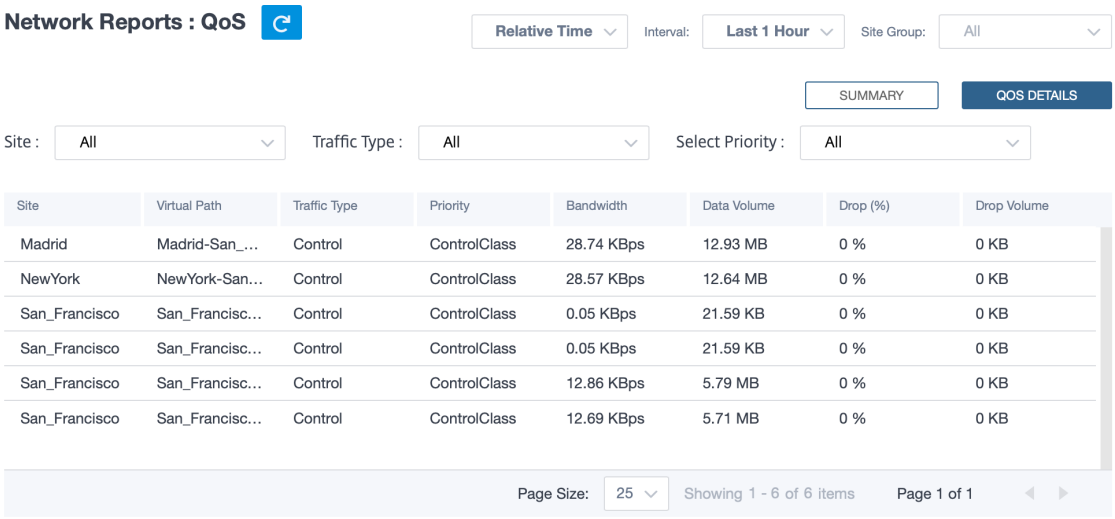
La qualité de service (QoS) gère le trafic de données afin de réduire la perte de paquets, la latence et la gigue sur le réseau. Pour plus d'informations, consultez la section Qualité de service. Voici deux façons d'afficher le rapport Qualité de service (QoS) :

- Vue**récapitulative :** La vue récapitulative fournit une vue d'ensemble de la consommation de bande passante pour tous les types de trafic : en temps réel, interactif, groupé et contrôlé sur le réseau et par site.



  - Temps**réel :** utilisé pour un trafic à faible latence, à faible bande passante et sensible au temps. Les applications en temps réel sont sensibles au temps, mais n'ont pas vraiment besoin d'une bande passante élevée (par exemple la voix sur IP). Les applications en temps réel sont sensibles à la latence et à la gigue, mais peuvent tolérer une certaine perte.
  - **Interactif :** utilisé pour le trafic interactif avec des exigences de latence faibles à moyennes et des exigences de bande passante faibles à moyennes. Les applications interactives impliquent une intervention humaine sous la forme de clics de souris ou de mouvements de curseur. L'interaction se fait généralement entre un client et un serveur. La communication peut ne pas nécessiter de bande passante élevée, mais elle est sensible à la perte et à la latence. Cependant, serveur à client a besoin d'une bande passante élevée pour transférer des informations graphiques, qui peuvent ne pas être sensibles à la perte.
  - **En masse :** Utilisé pour le trafic à bande passante élevée pouvant tolérer une latence élevée. Les applications qui gèrent le transfert de fichiers et qui ont besoin d'une bande passante élevée sont classées comme classe groupée. Ces applications impliquent peu d'interférence humaine et sont principalement traitées par les systèmes eux-mêmes.
  - **Contrôle :** Utilisé pour transférer des paquets de contrôle contenant des informations de routage, de planification et de statistiques de liens.

- **Vue détaillée : La vue** détaillée capture les tendances concernant la consommation de bande passante, le volume de trafic, les paquets abandonnés, etc. pour chaque classe de QoS associée à un chemin virtuel de superposition.



Ce rapport est disponible au niveau du site où l'utilisateur peut afficher les statistiques QoS en fonction du chemin virtuel entre les deux sites. Pour plus d'informations, consultez les rapports du site.

Statistiques historiques

Pour chaque site, vous pouvez afficher les statistiques sous forme de graphiques pour les paramètres réseau suivants :

- Sites
- Chemins virtuels
- Chemins
- Liens WAN
- Interfaces
- Classes
- Tunnels GRE
- Tunnels IPSec

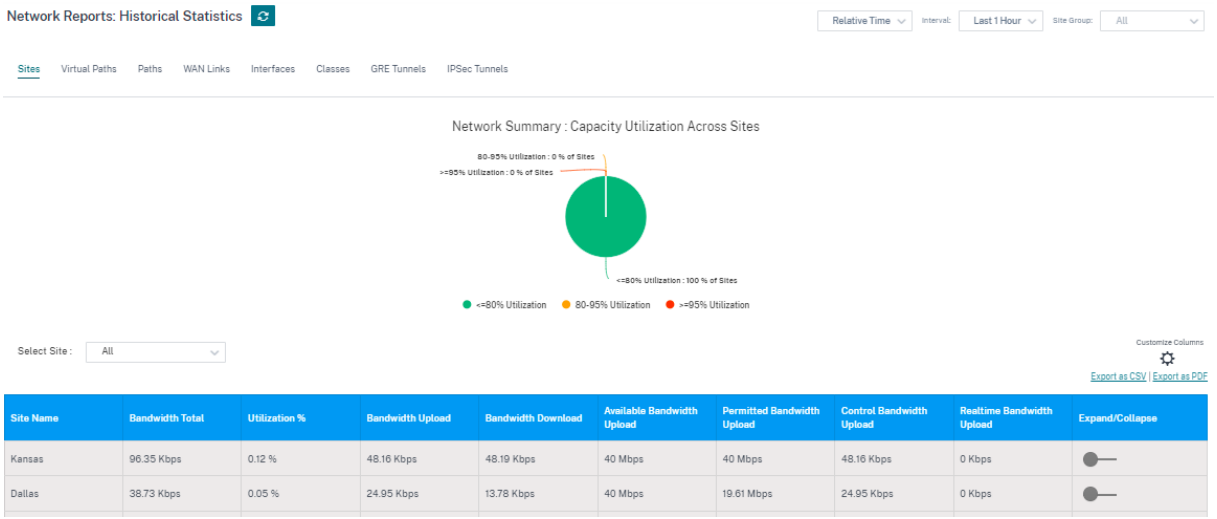
Les statistiques sont collectées sous forme de graphiques. Ces graphiques sont tracés en fonction de la chronologie par rapport à l'utilisation, ce qui vous permet de comprendre les tendances d'utilisation des différentes propriétés d'objets réseau. Vous pouvez afficher des graphiques pour les statistiques d'application à l'échelle du réseau.

Vous pouvez afficher ou masquer les graphiques et personnaliser les colonnes selon vos besoins.

Sites

Pour consulter les statistiques du site, accédez à **Rapports > Statistiques historiques > onglet Sites**
.

Sélectionnez le nom du site dans la liste.

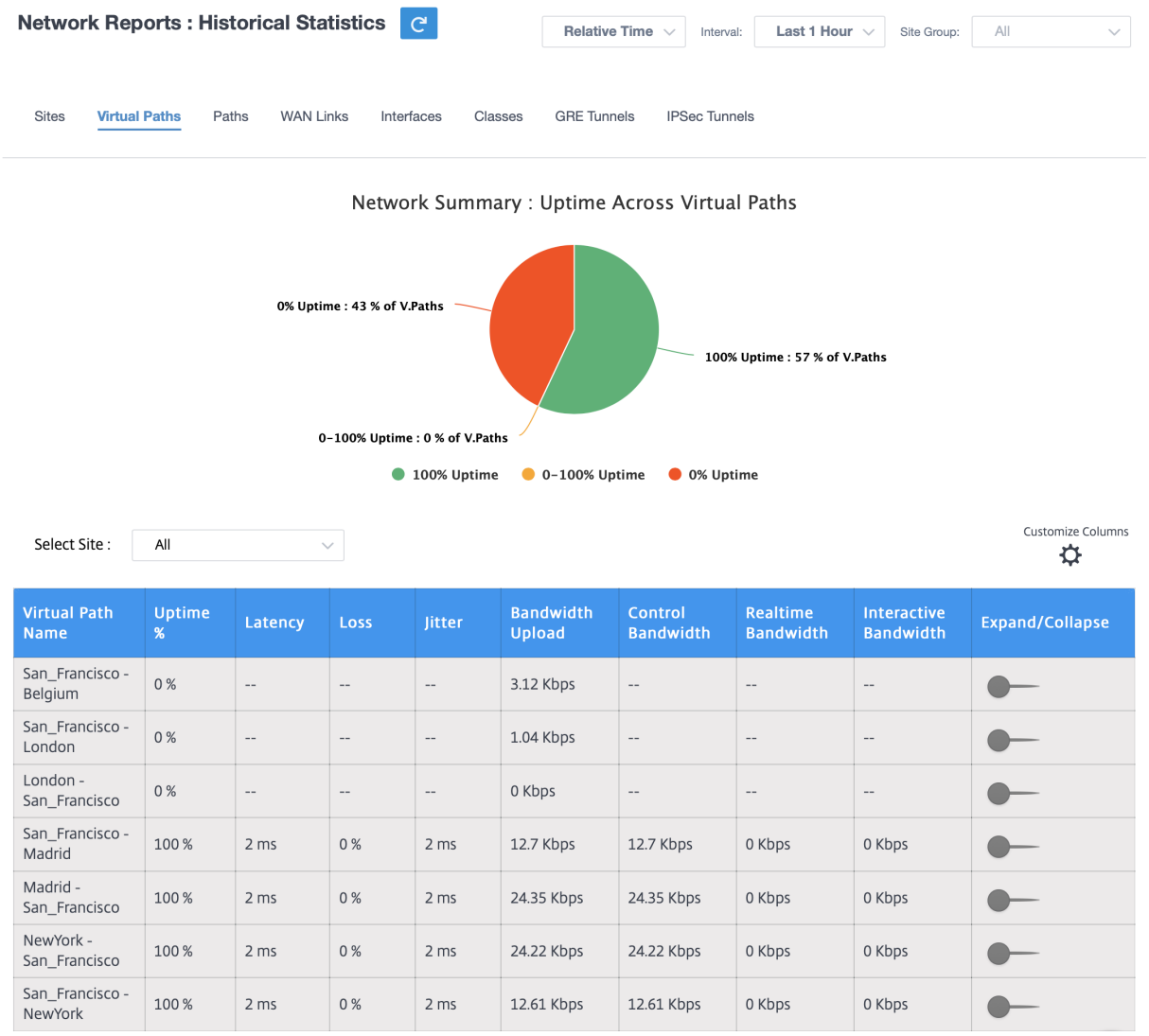


Vous pouvez afficher les mesures suivantes :

- **Nom du site** : nom du site.
- **Bande passante totale** : bande passante totale consommée par tous les types de paquets. Bande passante = Contrôle de la bande passante + bande passante en temps réel + bande passante interactive et bande passante en bloc.
- **Utilisation** : vous pouvez consulter les statistiques du site par utilisation (%).
- **Entrée de bande passante** : vitesse de téléchargement maximale et minimale via le port WAN.
- **Sortie de bande passante** : vitesse de téléchargement maximale et minimale via le port WAN.
- Entrée**de bande passante disponible** : bande passante totale allouée à tous les liens WAN d'un site.
- Entrée de**bande passante autorisée** : bande passante disponible pour la transmission d'informations.
- **Contrôle de l'entrée de**bande passante : bande passante utilisée pour transférer les paquets de contrôle contenant des informations de routage, de planification et de statistiques de liens.
- Entrée de**bande passante en temps réel** : bande passante consommée par les applications appartenant au type de classe en temps réel dans la configuration NetScaler SD-WAN. Les performances de ces applications dépendent en grande partie de la latence du réseau. Un paquet retardé est pire qu'un paquet perdu (par exemple, VoIP, Skype for Business).
- **Développer/Réduire** : Vous pouvez développer ou réduire les données selon vos besoins.

Chemins virtuels

Pour consulter les statistiques **des chemins virtuels**, accédez à **Rapports > Statistiques > onglet Chemins virtuels** .



Virtual Path Name	Uptime %	Latency	Loss	Jitter	Bandwidth Upload	Control Bandwidth	Realtime Bandwidth	Interactive Bandwidth	Expand/Collapse
San_Francisco - Belgium	0 %	--	--	--	3.12 Kbps	--	--	--	
San_Francisco - London	0 %	--	--	--	1.04 Kbps	--	--	--	
London - San_Francisco	0 %	--	--	--	0 Kbps	--	--	--	
San_Francisco - Madrid	100 %	2 ms	0 %	2 ms	12.7 Kbps	12.7 Kbps	0 Kbps	0 Kbps	
Madrid - San_Francisco	100 %	2 ms	0 %	2 ms	24.35 Kbps	24.35 Kbps	0 Kbps	0 Kbps	
NewYork - San_Francisco	100 %	2 ms	0 %	2 ms	24.22 Kbps	24.22 Kbps	0 Kbps	0 Kbps	
San_Francisco - NewYork	100 %	2 ms	0 %	2 ms	12.61 Kbps	12.61 Kbps	0 Kbps	0 Kbps	

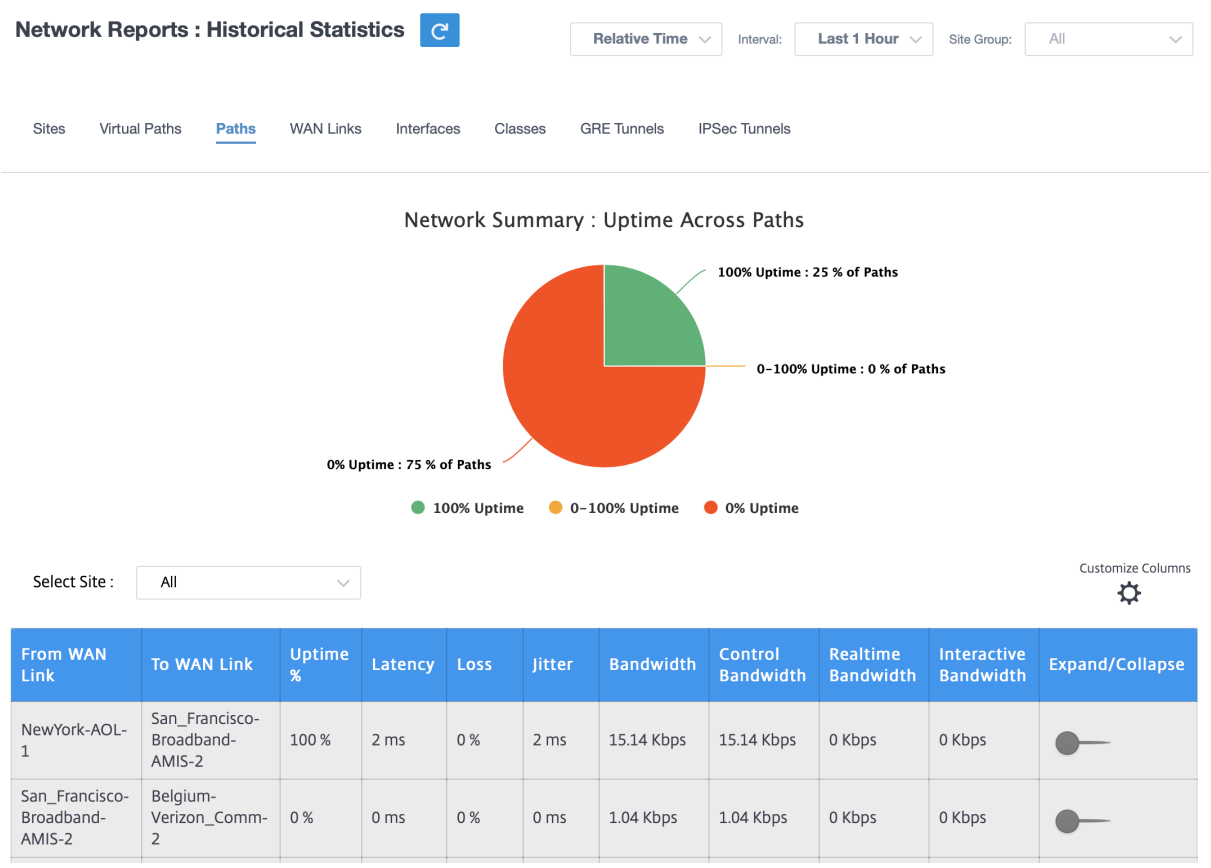
Vous pouvez afficher les mesures suivantes :

- **Nom du chemin virtuel : nom**du chemin virtuel.
- **Latence** : latence en millisecondes pour le trafic en temps réel.
- **Perte** : pourcentage de paquets perdus.
- **Jitter** : variation du délai de réception des paquets, en millisecondes.
- **Entrée de bande passante** : utilisation de la bande passante d'entrée (LAN vers WAN) pendant la période sélectionnée.
- **Bande passante de contrôle** : bande passante utilisée pour transférer des paquets de contrôle contenant des informations de routage, de planification et de statistiques de liens.
- **Bande passante en temps réel** : bande passante consommée par les applications appartenant au type de classe en temps réel dans la configuration SD-WAN. Les performances de ces applications dépendent en grande partie de la latence du réseau. Un paquet retardé est pire qu'un paquet perdu (par exemple, VoIP, Skype for Business).

- **Bande passante interactive** : bande passante consommée par les applications appartenant au type de classe interactive dans la configuration SD-WAN. Les performances de ces applications dépendent en grande partie de la latence du réseau et de la perte de paquets (par exemple, XenDesktop, XenApp).
- **Bande passante en masse** : bande passante consommée par les applications appartenant au type de classe de masse dans la configuration SD-WAN. Ces applications impliquent peu d'intervention humaine et sont gérées par les systèmes eux-mêmes (par exemple, FTP, opérations de sauvegarde).
- **Développer/Réduire** : Vous pouvez développer ou réduire les données selon vos besoins.

Chemins

Pour consulter les statistiques **des chemins**, accédez à **Rapports > Statistiques > onglet Chemins** .



From WAN Link	To WAN Link	Uptime %	Latency	Loss	Jitter	Bandwidth	Control Bandwidth	Realtime Bandwidth	Interactive Bandwidth	Expand/Collapse
NewYork-AOL-1	San_Francisco-Broadband-AMIS-2	100 %	2 ms	0 %	2 ms	15.14 Kbps	15.14 Kbps	0 Kbps	0 Kbps	
San_Francisco-Broadband-AMIS-2	Belgium-Verizon_Comm-2	0 %	0 ms	0 %	0 ms	1.04 Kbps	1.04 Kbps	0 Kbps	0 Kbps	

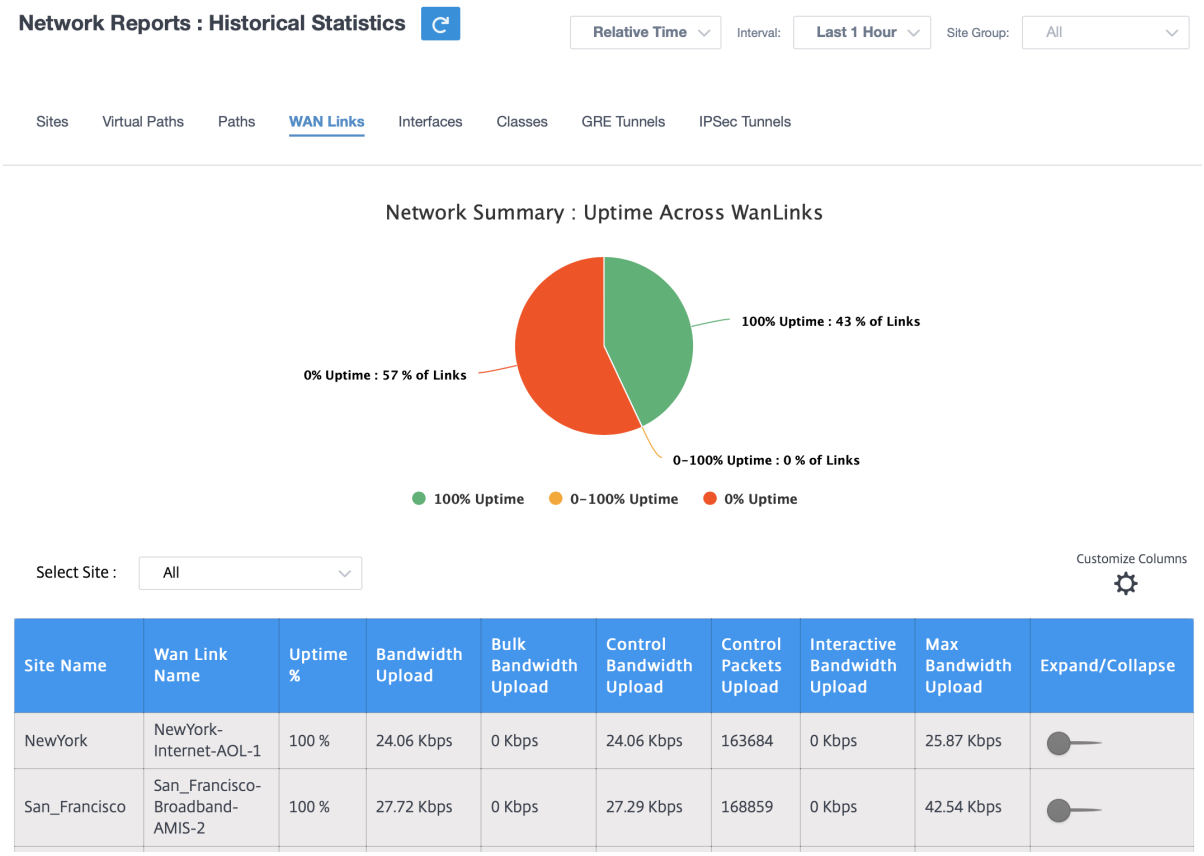
Vous pouvez afficher les mesures suivantes :

- **À partir du lien WAN** : le lien WAN source.
- **Vers le lien WAN** : le lien WAN de destination.
- **Latence** : latence en millisecondes pour le trafic en temps réel.

- **Perte** : pourcentage de paquets perdus.
- **Jitter** : variation du délai de réception des paquets, en millisecondes.
- **Bande passante** : bande passante totale consommée par tous les types de paquets. Bande passante = Contrôle de la bande passante + bande passante en temps réel + bande passante interactive et bande passante en bloc.
- **Bande passante de contrôle** : bande passante utilisée pour transférer des paquets de contrôle contenant des informations de routage, de planification et de statistiques de liens.
- **Bande passante en temps réel** : bande passante consommée par les applications appartenant au type de classe en temps réel dans la configuration SD-WAN. Les performances de ces applications dépendent en grande partie de la latence du réseau. Un paquet retardé est pire qu'un paquet perdu (par exemple, VoIP, Skype for Business).
- **Bande passante interactive** : bande passante consommée par les applications appartenant au type de classe interactive dans la configuration SD-WAN. Les performances de ces applications dépendent en grande partie de la latence du réseau et de la perte de paquets (par exemple, XenDesktop, XenApp).
- **Bande passante en masse** : bande passante consommée par les applications appartenant au type de classe de masse dans la configuration SD-WAN. Ces applications impliquent peu d'intervention humaine et sont gérées par les systèmes eux-mêmes (par exemple, FTP, opérations de sauvegarde).
- **Développer/Réduire** : Vous pouvez développer ou réduire les données selon vos besoins.

Liens WAN

Pour afficher les statistiques au niveau de la **liaison WAN**, accédez à **Rapports > Statistiques > onglet Liens WAN** .



Site Name	Wan Link Name	Uptime %	Bandwidth Upload	Bulk Bandwidth Upload	Control Bandwidth Upload	Control Packets Upload	Interactive Bandwidth Upload	Max Bandwidth Upload	Expand/Collapse
NewYork	NewYork-Internet-AOL-1	100 %	24.06 Kbps	0 Kbps	24.06 Kbps	163684	0 Kbps	25.87 Kbps	
San_Francisco	San_Francisco-Broadband-AMIS-2	100 %	27.72 Kbps	0 Kbps	27.29 Kbps	168859	0 Kbps	42.54 Kbps	

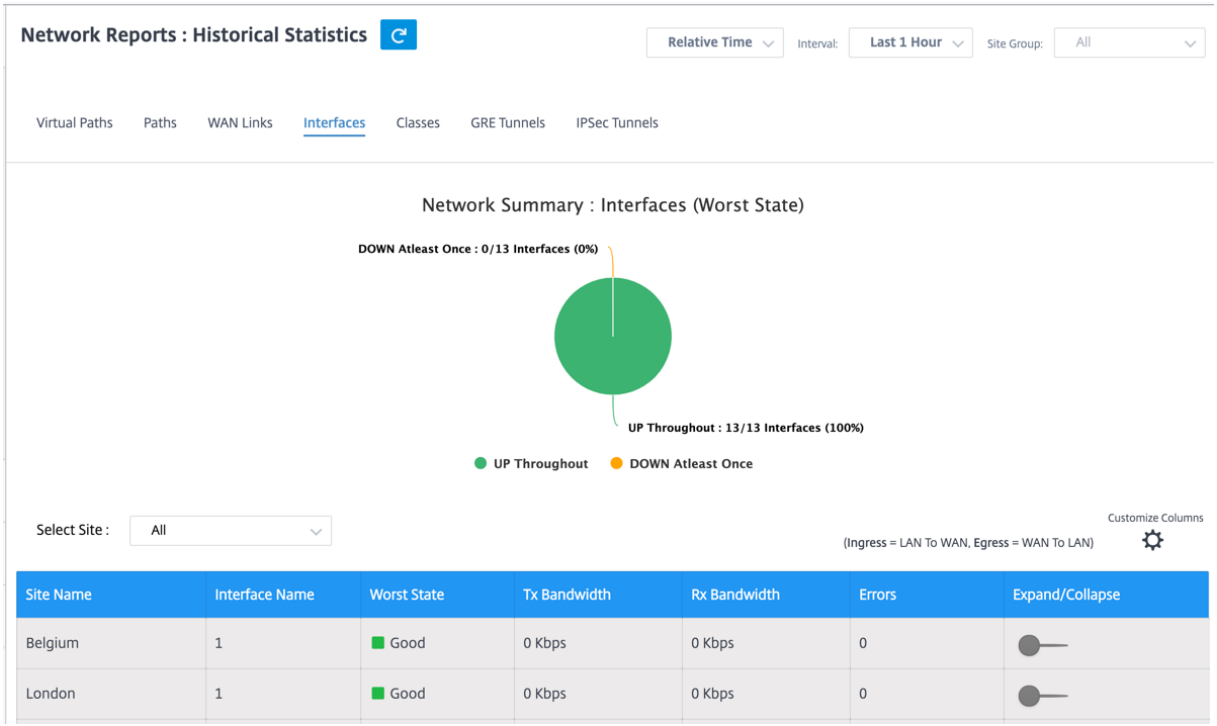
Vous pouvez afficher les mesures suivantes :

- **Nom du lien WAN** : nom du chemin.
- **Entrée de bande passante** : utilisation de la bande passante d'entrée (LAN vers WAN) pendant la période sélectionnée.
- Entrée de**bande passante en masse** : bande passante du chemin virtuel d'entrée (LAN vers WAN) utilisée par le trafic en masse pendant la période sélectionnée.
- **Entrée de bande passante de contrôle** : bande passante du chemin virtuel d'entrée (LAN vers WAN) utilisée par le trafic de contrôle pendant la période sélectionnée.
- **Entrée de paquets de contrôle** : paquets de contrôle de chemin virtuel entrants (LAN vers WAN) pour la période sélectionnée.
- Entrée de**bande passante interactive** : bande passante du chemin virtuel d'entrée (LAN vers WAN) utilisée par le trafic interactif pendant la période sélectionnée.
- Entrée**de bande passante maximale** : bande passante d'entrée maximale (LAN vers WAN) utilisée en une minute pendant la période sélectionnée.
- Entrée**de bande passante minimale** : bande passante d'entrée minimale (LAN vers WAN) utilisée en une minute pendant la période sélectionnée.
- **Développer/Réduire** : Vous pouvez développer ou réduire les données selon vos besoins.

Interfaces

Le rapport statistique Interfaces vous aide pendant le dépannage à voir rapidement si l'un des ports est en panne. Vous pouvez également afficher la bande passante transmise et reçue, ou les détails des paquets sur chaque port. Vous pouvez également afficher le nombre d'erreurs qui se sont produites sur ces interfaces pendant une certaine période.

Pour consulter les statistiques de **l'interface**, accédez à **Rapports > Statistiques > onglet Interfaces** .



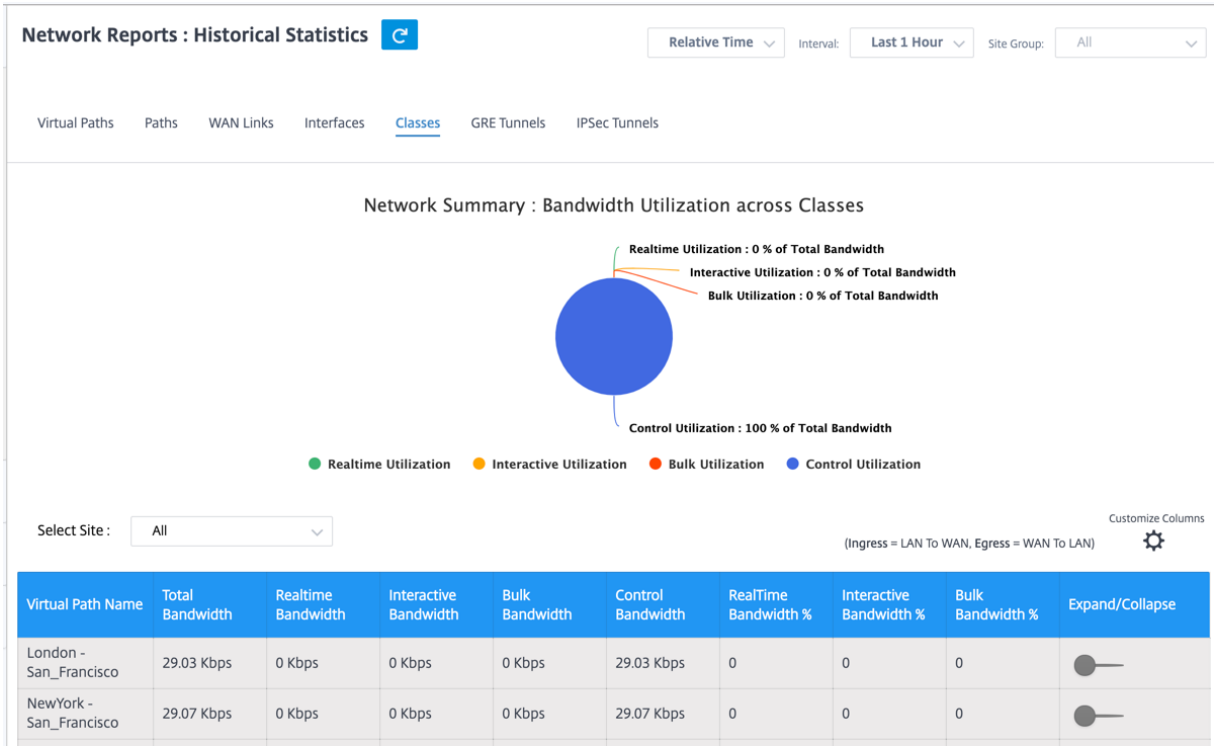
Vous pouvez afficher les mesures suivantes :

- **Nom de l'interface** : nom de l'interface Ethernet.
- **Bande passante Tx** : bande passante transmise.
- **Bande passante Rx** : Bande passante reçue.
- **Erreurs** : nombre d'erreurs observées au cours de la période sélectionnée.
- **Développer/Réduire** : Vous pouvez développer ou réduire les données selon vos besoins.

Classes

Les services virtuels peuvent être affectés à des classes QoS particulières, et différentes restrictions de bande passante peuvent être appliquées à différentes classes.

Pour consulter les statistiques des **cours**, accédez à **Rapports > Statistiques > onglet Classes** .



Vous pouvez afficher les mesures suivantes :

- **Classe QoS** : nom de la classe.
- **Bande passante** : bande passante transmise.
- **Volume de données** : données envoyées, en Kbits/s.
- **Volume de dépôt** : pourcentage de données supprimées.
- **Pourcentage de perte** : pourcentage de données supprimées.
- **Développer/Réduire** : Vous pouvez développer ou réduire les données selon vos besoins.

Tunnels GRE

Vous pouvez utiliser un mécanisme de tunnel pour transporter des paquets d'un protocole dans un autre protocole. Le protocole qui porte l'autre protocole est appelé le protocole de transport, et le protocole transporté est appelé le protocole passager. Generic Routing Encapsulation (GRE) est un mécanisme de tunnel qui utilise IP comme protocole de transport et peut transporter de nombreux protocoles passagers différents.

L'adresse source du tunnel et l'adresse de destination sont utilisées pour identifier les deux points de terminaison des liens virtuels point à point dans le tunnel. Pour plus d'informations sur la configuration des tunnels GRE sur les appliances Citrix SD-WAN, consultez Tunnel GRE.

Pour consulter les statistiques **du tunnel GRE**, accédez à **Rapports > Statistiques > onglet Tunnels GRE** .

Vous pouvez afficher les mesures suivantes :

- **Nom du site** : nom du site.
- **Bande passante Tx** : bande passante transmise.
- **Bande passante Rx** : Bande passante reçue.
- **Paquet abandonné** : nombre de paquets abandonnés en raison de la congestion du réseau.
- **Paquets fragmentés** : nombre de paquets fragmentés. Les paquets sont fragmentés pour créer des paquets plus petits qui peuvent passer par un lien avec un MTU plus petit que le datagramme d'origine. Les fragments sont réassemblés par l'hôte récepteur.
- **Développer/Réduire** : Vous pouvez développer ou réduire les données selon vos besoins.

Tunnels IPSec

Les protocoles de sécurité IP (IPsec) fournissent des services de sécurité tels que le chiffrement des données sensibles, l'authentification, la protection contre la réexécution et la confidentialité des données pour les paquets IP. Encapsulating Security Payload (ESP) et Authentication Header (AH) sont les deux protocoles de sécurité IPSec utilisés pour fournir ces services de sécurité.

En mode tunnel IPSec, l'ensemble du paquet IP d'origine est protégé par IPSec. Le paquet IP d'origine est enveloppé et chiffré, et un nouvel en-tête IP est ajouté avant de transmettre le paquet via le tunnel VPN.
Pour plus d'informations sur la configuration de tunnels IPsec sur les appliances Citrix SD-WAN, consultez Terminaison du tunnel IPSec.

Pour consulter les statistiques **du tunnel IPsec**, accédez à **Rapports > statistiques > onglet Tunnels IPSec** .

Vous pouvez afficher les mesures suivantes :

- **Nom du tunnel** : nom du tunnel.
- **État du tunnel : état**du tunnel IPsec.
- **MTU** : unité de transmission maximale : taille du plus grand datagramme IP pouvant être transféré via un lien spécifique.
- **Paquet reçu** : Nombre de paquets reçus.
- **Paquets envoyés** : Nombre de paquets envoyés.
- **Paquet abandonné** : nombre de paquets abandonnés en raison de la congestion du réseau.
- **Octets supprimés** : nombre d'octets supprimés.
- **Développer/Réduire** : Vous pouvez développer ou réduire les données selon vos besoins.

Statistiques en temps réel

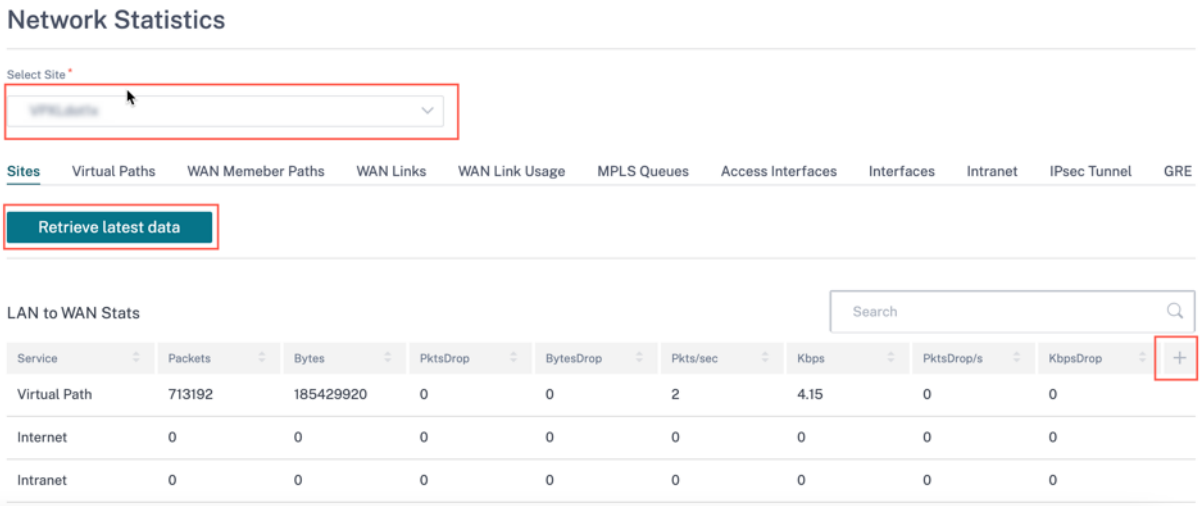
La page Statistiques en temps réel affiche les informations statistiques suivantes au niveau du client :

Statistiques du réseau

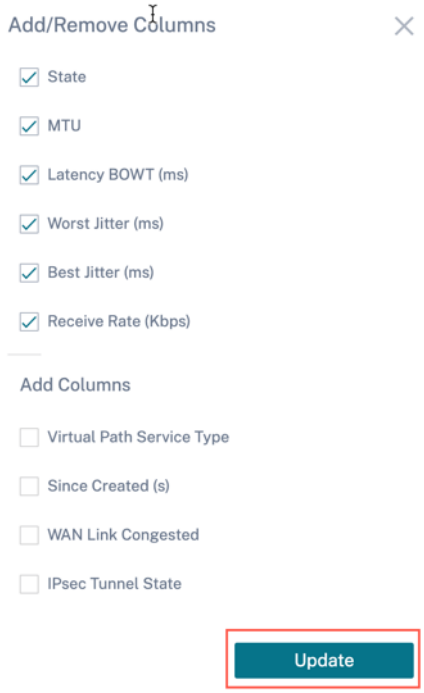
La page **Statistiques réseau** fournit les informations statistiques en temps réel suivantes sous **Rapports** > **Temps réel** > **Statistiques réseau** :

- Sites
- Chemins virtuels
- Chemins pour les membres
- Liens WAN
- Utilisation de la liaison WAN
- Files d'attente MPLS
- Interfaces d'accès
- Interfaces
- Intranet
- Tunnel IPSec
- GRE

Pour obtenir un rapport statistique en temps réel, accédez à l'onglet requis (sites, chemins virtuels, liens WAN), sélectionnez le site dans la liste déroulante, puis cliquez sur **Récupérer les dernières données**.



Cliquez sur le symbole plus (+) pour ajouter ou supprimer une colonne du tableau des statistiques, puis cliquez sur **Mettre à jour**.

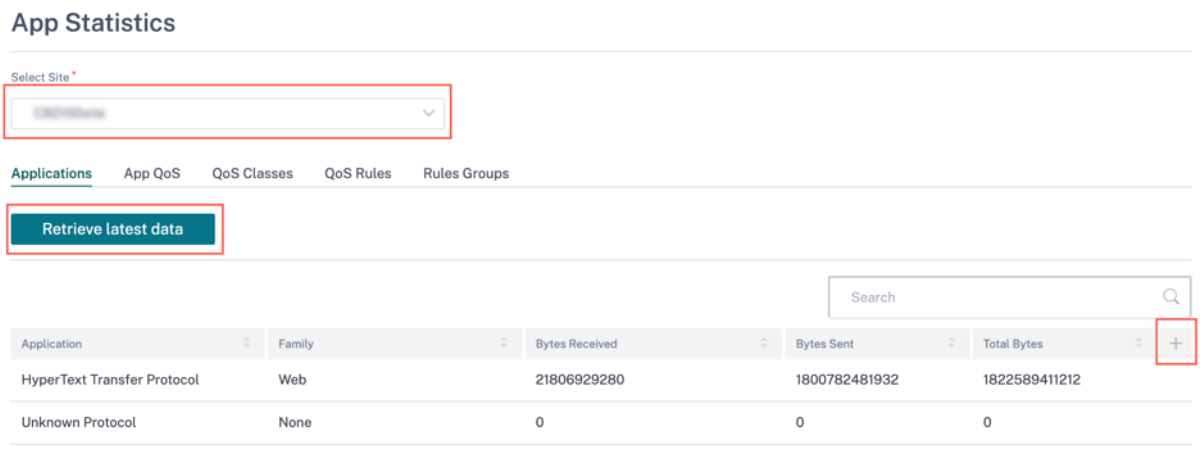


Statistiques de l'application

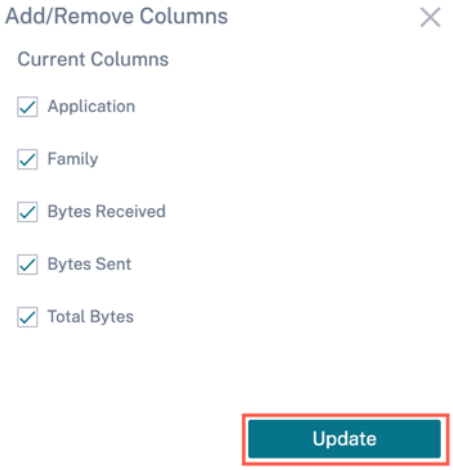
La page **Statistiques de l'application** fournit les informations statistiques en temps réel suivantes sous **Rapports > Temps réel > Statistiques de l'application** :

- Applications
- QoS des applications
- Cours de QoS
- Règles de QoS
- Groupes de règles

Pour obtenir un rapport statistique en temps réel, accédez à l'onglet requis (applications, règle QoS, classes de QoS), sélectionnez le site dans la liste déroulante et cliquez sur **Récupérer les dernières données**.



Cliquez sur le symbole plus (+) si vous souhaitez ajouter ou supprimer une colonne du tableau des statistiques, puis cliquez sur **Mettre à jour**.

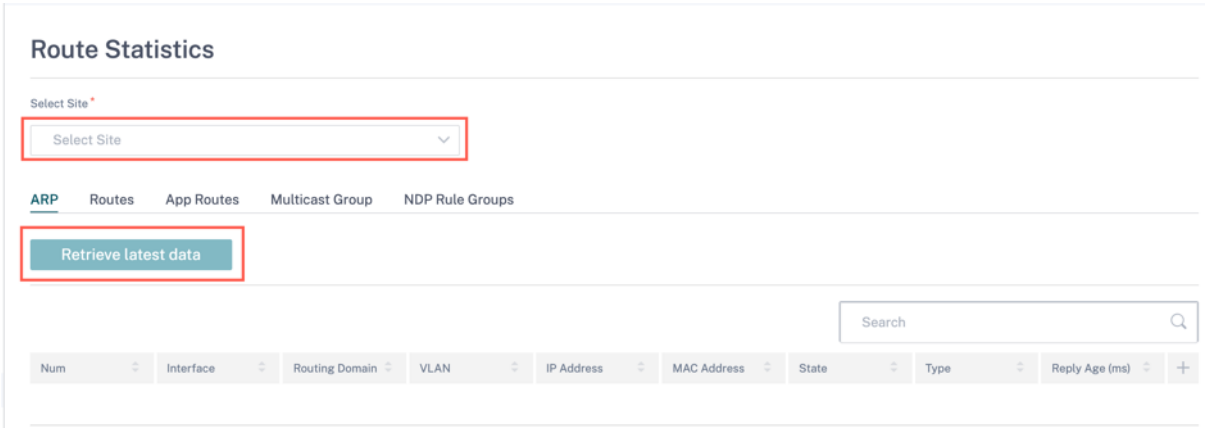


Statistiques d'itinéraire

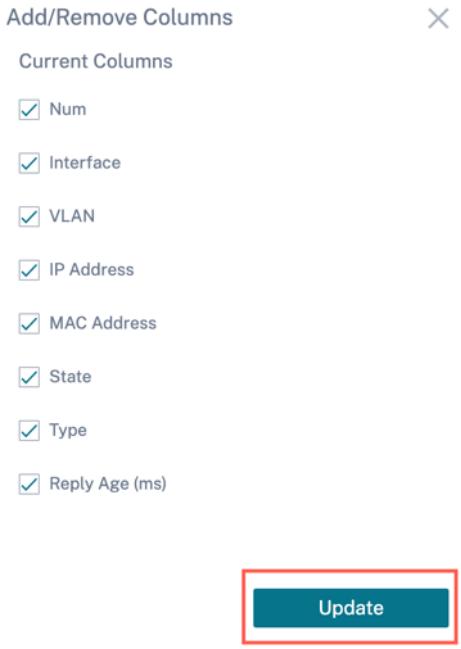
La page **Statistiques des itinéraires** fournit les informations statistiques en temps réel suivantes sous **Rapports > Temps réel > Statistiques d'itinéraires** :

- ARP
- Itinéraires
- Itinéraires d'application
- Protocoles observés
- Groupe Multicast
- Groupes de règles du NDP

Pour obtenir un rapport statistique en temps réel, accédez à l'onglet requis (tel que ARP, Routes, Applications Routes), sélectionnez le site dans la liste déroulante et cliquez sur **Récupérer les dernières données**.

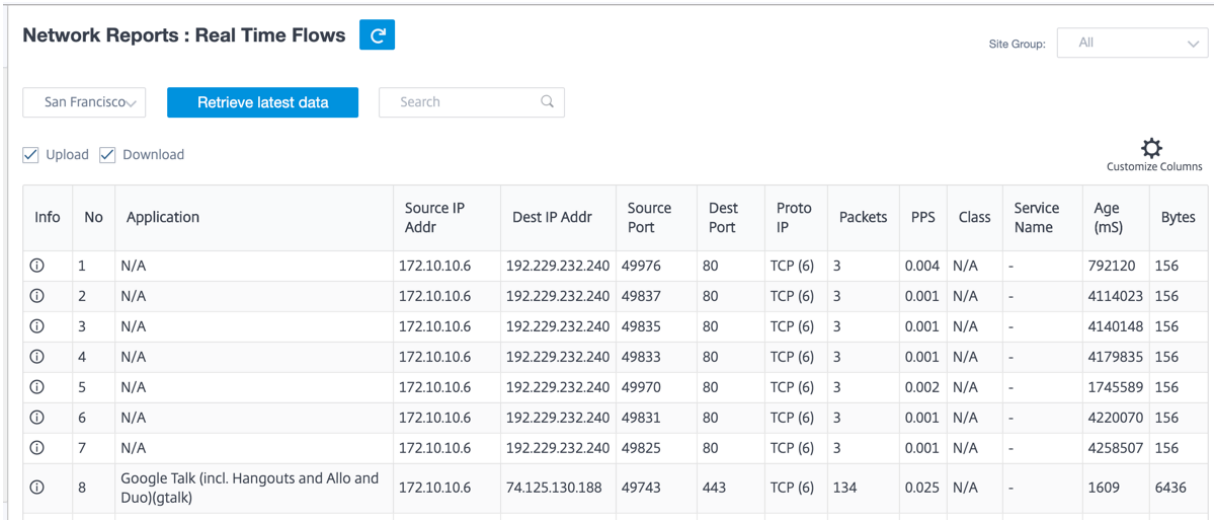


Cliquez sur le symbole plus (+) si vous souhaitez ajouter ou supprimer une colonne du tableau des statistiques, puis cliquez sur **Mettre à jour**.



Flux

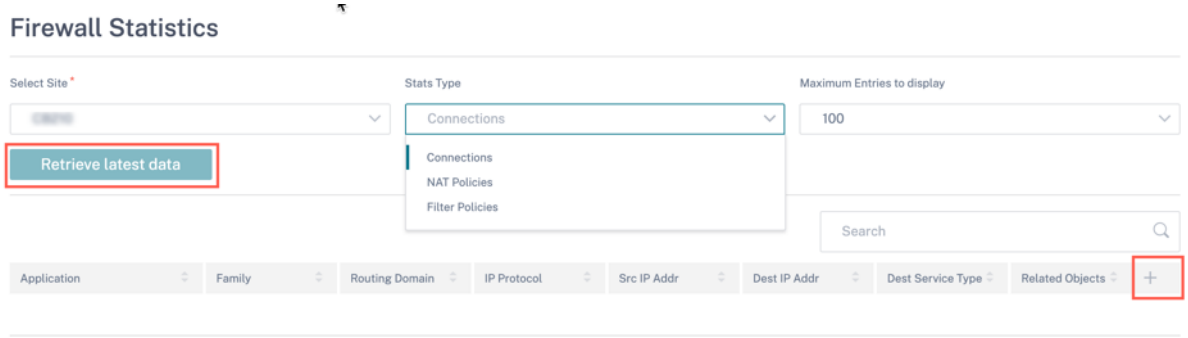
Au niveau du réseau, sélectionnez le site dans la liste déroulante avant de pouvoir récupérer les statistiques. La fonction **Flows** fournit des informations de flux unidirectionnelles relatives à une session particulière passant par l'appliance. Ceci fournit des informations sur le type de service de destination dans lequel se trouve le flux, ainsi que les informations relatives à la règle et au type de classe ainsi que sur le mode de transmission.



Info	No	Application	Source IP Addr	Dest IP Addr	Source Port	Dest Port	Proto IP	Packets	PPS	Class	Service Name	Age (mS)	Bytes
ⓘ	1	N/A	172.10.10.6	192.229.232.240	49976	80	TCP (6)	3	0.004	N/A	-	792120	156
ⓘ	2	N/A	172.10.10.6	192.229.232.240	49837	80	TCP (6)	3	0.001	N/A	-	4114023	156
ⓘ	3	N/A	172.10.10.6	192.229.232.240	49835	80	TCP (6)	3	0.001	N/A	-	4140148	156
ⓘ	4	N/A	172.10.10.6	192.229.232.240	49833	80	TCP (6)	3	0.001	N/A	-	4179835	156
ⓘ	5	N/A	172.10.10.6	192.229.232.240	49970	80	TCP (6)	3	0.002	N/A	-	1745589	156
ⓘ	6	N/A	172.10.10.6	192.229.232.240	49831	80	TCP (6)	3	0.001	N/A	-	4220070	156
ⓘ	7	N/A	172.10.10.6	192.229.232.240	49825	80	TCP (6)	3	0.001	N/A	-	4258507	156
ⓘ	8	Google Talk (incl. Hangouts and Allo and Duo)(gtalk)	172.10.10.6	74.125.130.188	49743	443	TCP (6)	134	0.025	N/A	-	1609	6436

Statistiques de pare-feu

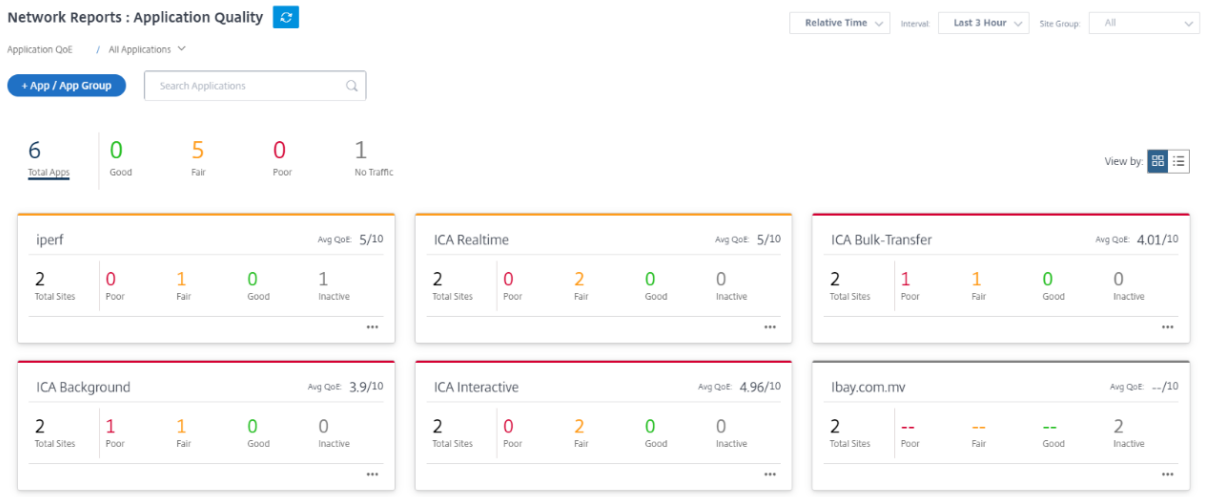
Au niveau du réseau, sélectionnez le site dans la liste déroulante avant de pouvoir récupérer les statistiques. Les **statistiques du pare-feu** fournissent l'état de la connexion associée à une session particulière en fonction de l'action de pare-feu configurée. Les connexions pare-feu fournissent également des détails complets sur la source et la destination de la connexion.



Qualité de l'application

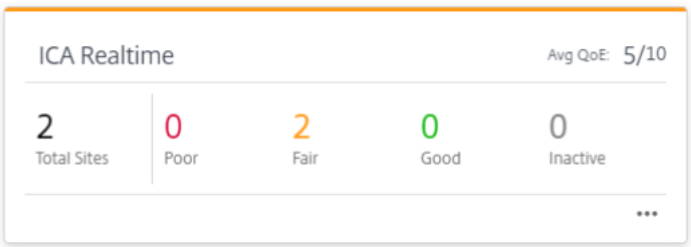
LaQoE des applications est une mesure de la qualité d'expérience des applications dans le réseau SD-WAN. Il mesure la qualité des applications qui circulent à travers les chemins virtuels entre deux appliances SD-WAN. Le score QoE de l'application est une valeur comprise entre 0 et 10. La plage de score dans laquelle elle se trouve détermine la qualité d'une application. Application QoE permet aux administrateurs réseau de vérifier la qualité de l'expérience des applications et de prendre des mesures proactives lorsque la qualité passe en dessous du seuil acceptable.

Qualité	Gamme	Codage couleur
Good	8–10	Vert
Fair	4–8	Orange
Poor	0–4	Rouge



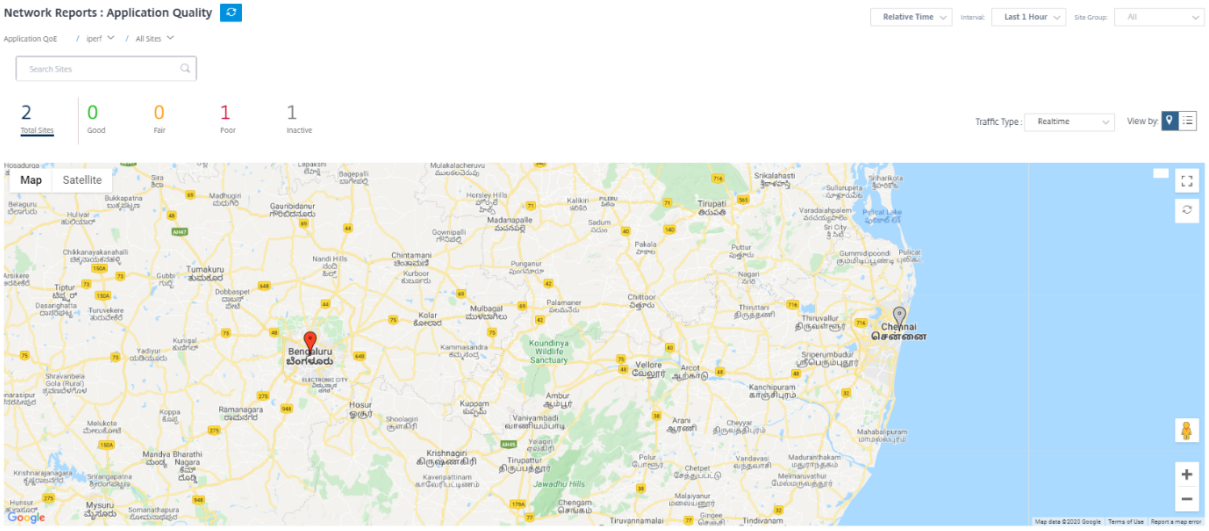
La partie supérieure du tableau de bord affiche le nombre total d'applications et le nombre d'applications dont la QoE d'application est bonne, équitable ou médiocre dans le réseau. Il affiche également le nombre d'applications qui n'ont aucun trafic.

La fiche d'application individuelle affiche le nombre de sites ayant une qualité d'application médiocre, passable ou correcte pour l'application spécifique. Il affiche également le nombre de sites qui n'utilisent pas activement l'application. Le QoE moyen est le score QoE moyen de l'application sur tous les sites du réseau.



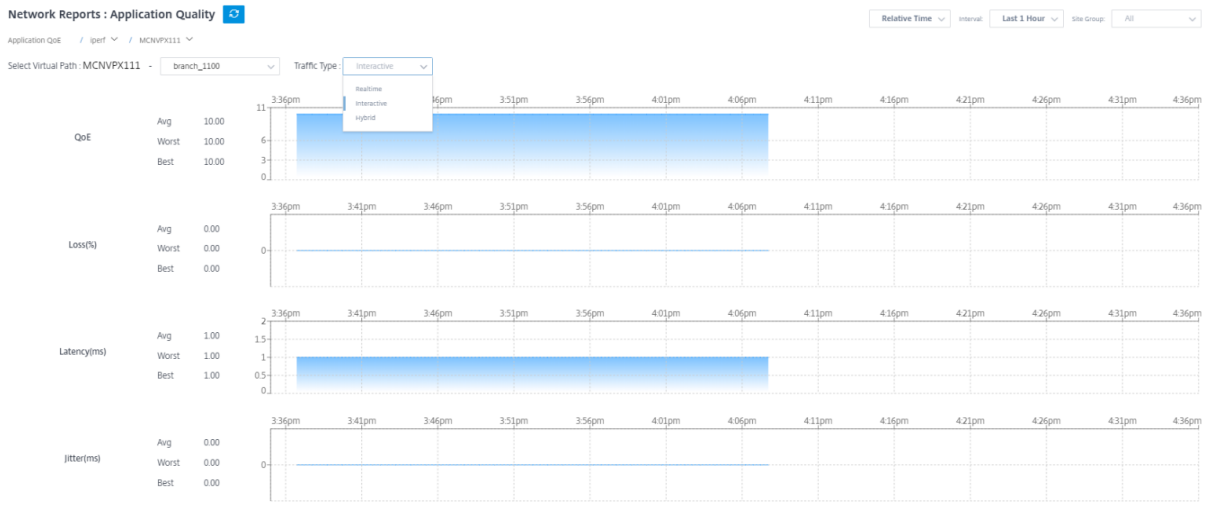
Cliquez sur une fiche d'application individuelle pour afficher les détails sur le nombre de sites dont la qualité d'application est bonne, passable ou médiocre pour l'application sélectionnée. Une vue

cartographique de tous les sites exécutant l'application sélectionnée s'affiche. Cliquez sur un site sur la carte pour approfondir l'exploration vers le bas et afficher les statistiques QoE de l'application des différents chemins virtuels sur le site.



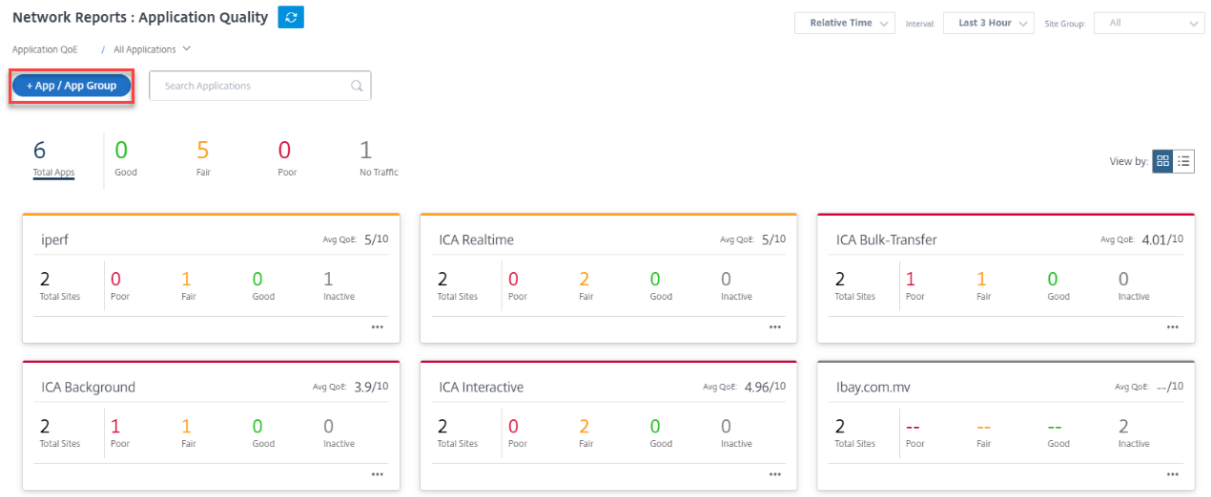
Vous pouvez afficher les mesures suivantes pour le trafic en temps réel, interactif et hybride pour la période sélectionnée :

- **QoE** : le score de QoE pour le trafic.
- **Perte** : pourcentage de perte pour le trafic.
- **Latence** : latence en millisecondes pour le trafic.
- **Instance** : Instance observée en millisecondes pour le trafic.

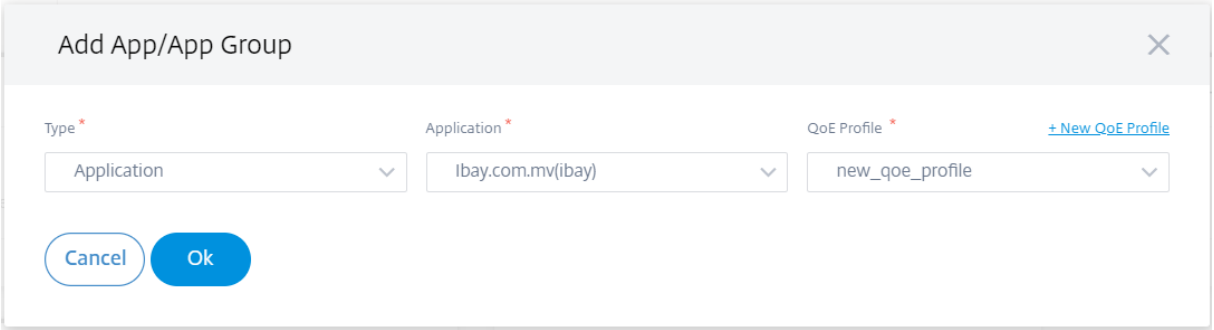


Profils QoE d'application

Cliquez sur **+ Application/Groupe d'applications** pour mapper les applications, les applications personnalisées ou les groupes d'applications aux profils QoE par défaut ou personnalisés.



Les profils QoE définissent le seuil du trafic en temps réel, interactif et hybride. Les seuils QoE selon les profils QoE sont appliqués à l'application ou au groupe d'applications sélectionné.



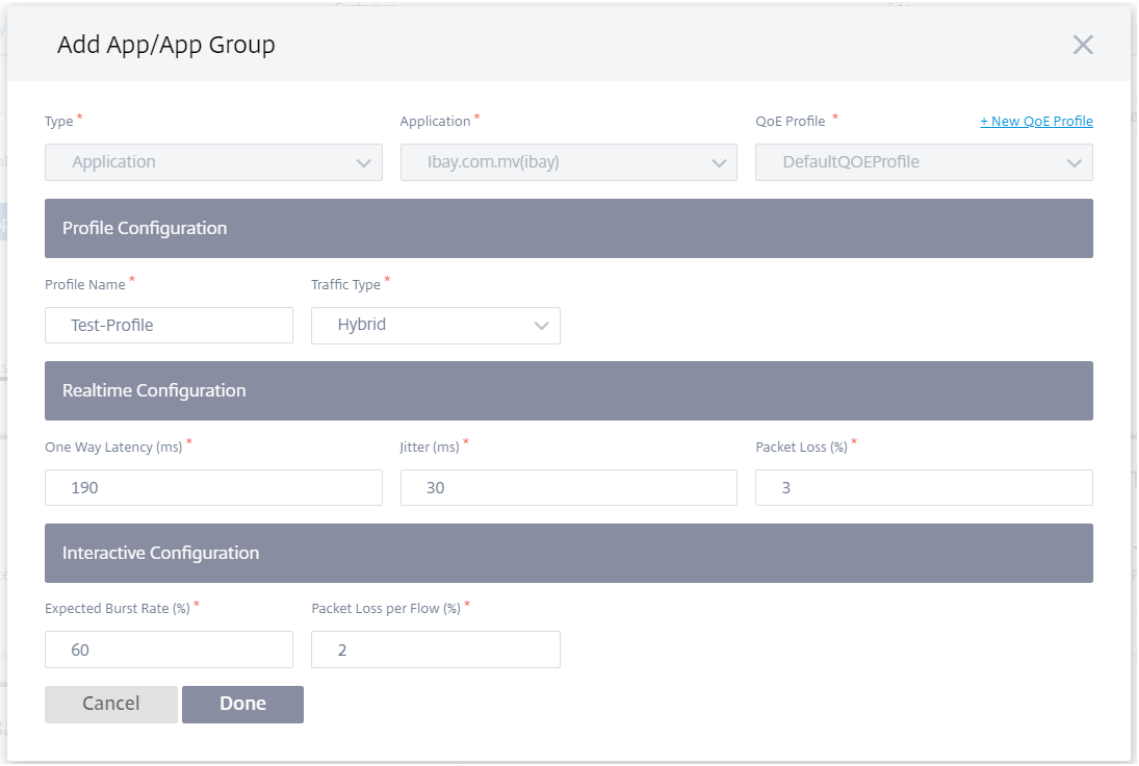
Cliquez sur **+ Nouveau profil QoE** pour créer un nouveau profil QoE d'application et entrez la valeur des paramètres suivants :

- **Nom du profil** : nom permettant d'identifier le profil qui définit des seuils pour le trafic interactif et en temps réel.
- **Type de trafic** : choisissez le type de trafic : en temps réel, interactif ou hybride. Si le type de trafic est hybride, vous pouvez configurer les seuils de profil QoE en temps réel et interactif.
- **Configuration en temps réel** : configurez des seuils pour les flux de trafic qui sélectionnent la politique de QoS en temps réel. Un flux d'application en temps réel qui répond aux seuils suivants pour la latence, la perte et la gigue est considéré comme de bonne qualité.
  - **Latence unidirectionnelle** : seuil de latence en millisecondes. La valeur de profil QoE par défaut est 160 ms.

  - **Jitter** : seuil de gigue en millisecondes. La valeur de profil QoE par défaut est de 30 ms.
  - **Perte de paquets** : pourcentage de perte de paquets. La valeur de profil QoE par défaut est 2%.

- **Configuration interactive** : configurez des seuils pour les flux de trafic qui sélectionnent la politique de QoS interactive. Un flux d'application interactive qui atteint le seuil suivant pour le rapport d'éclatement et la perte de paquets est considéré comme de bonne qualité.

  - **Taux de rafale attendu** : pourcentage du taux de rafale attendu. Le taux d'éclatement de sortie doit être au moins le pourcentage configuré du taux de rafale d'entrée. La valeur de profil QoE par défaut est 60 %.
  - **Perte de paquets par flux** : pourcentage de perte de paquets. La valeur de profil QoE par défaut est 1%.



L'application nouvellement ajoutée s'affiche dans le tableau de bord Qualité de l'application.

Vous pouvez également définir et configurer la QoE des applications à partir des paramètres de l'application et du DNS pour plus d'informations, voir Profils de qualité des applicationset Configuration de la qualitédes applications.

Rapports du site

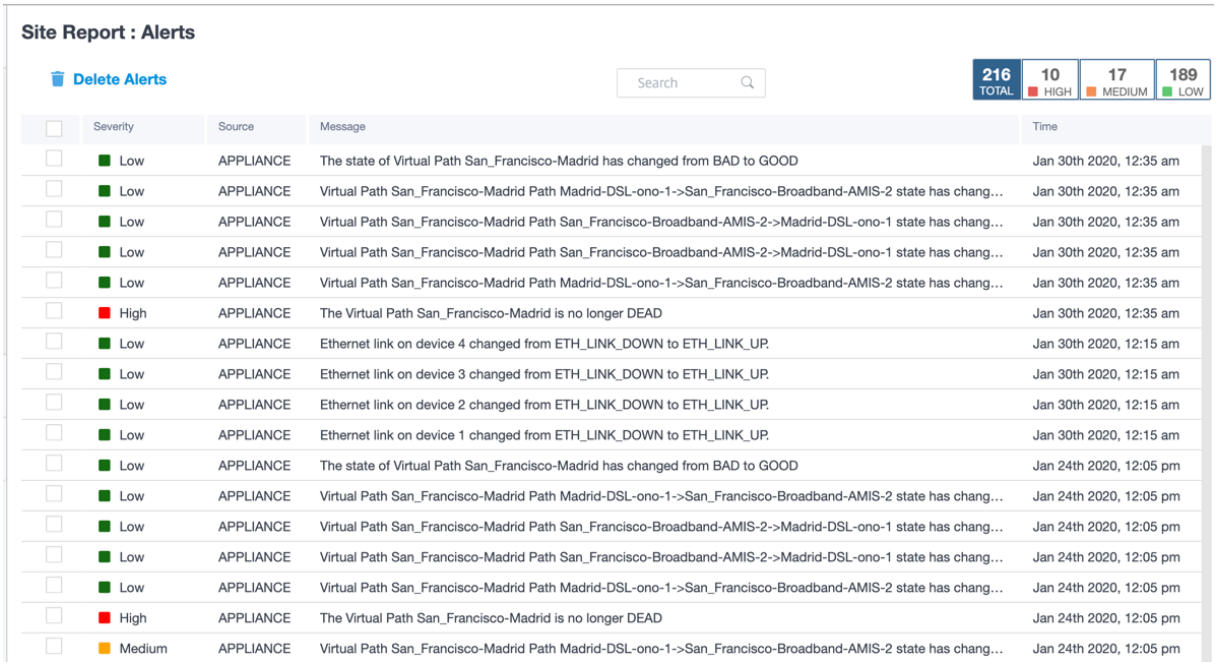
October 21, 2022

Les **rapports du site** fournissent une visibilité sur les alertes au niveau du site, les tendances d'utilisation, la qualité, les informations sur les appareils et les statistiques de pare-feu.

Alertes

L'administrateur du site peut consulter un rapport détaillé de tous les événements et alertes générés au niveau du site.

Il inclut la gravité, le site d'origine de l'alerte, le message d'alerte, l'heure et d'autres détails.



Severity	Source	Message	Time
Low	APPLIANCE	The state of Virtual Path San_Francisco-Madrid has changed from BAD to GOOD	Jan 30th 2020, 12:35 am
Low	APPLIANCE	Virtual Path San_Francisco-Madrid Path Madrid-DSL-ono-1->San_Francisco-Broadband-AMIS-2 state has chang...	Jan 30th 2020, 12:35 am
Low	APPLIANCE	Virtual Path San_Francisco-Madrid Path San_Francisco-Broadband-AMIS-2->Madrid-DSL-ono-1 state has chang...	Jan 30th 2020, 12:35 am
Low	APPLIANCE	Virtual Path San_Francisco-Madrid Path San_Francisco-Broadband-AMIS-2->Madrid-DSL-ono-1 state has chang...	Jan 30th 2020, 12:35 am
Low	APPLIANCE	Virtual Path San_Francisco-Madrid Path Madrid-DSL-ono-1->San_Francisco-Broadband-AMIS-2 state has chang...	Jan 30th 2020, 12:35 am
High	APPLIANCE	The Virtual Path San_Francisco-Madrid is no longer DEAD	Jan 30th 2020, 12:35 am
Low	APPLIANCE	Ethernet link on device 4 changed from ETH_LINK_DOWN to ETH_LINK_UP.	Jan 30th 2020, 12:15 am
Low	APPLIANCE	Ethernet link on device 3 changed from ETH_LINK_DOWN to ETH_LINK_UP.	Jan 30th 2020, 12:15 am
Low	APPLIANCE	Ethernet link on device 2 changed from ETH_LINK_DOWN to ETH_LINK_UP.	Jan 30th 2020, 12:15 am
Low	APPLIANCE	Ethernet link on device 1 changed from ETH_LINK_DOWN to ETH_LINK_UP.	Jan 30th 2020, 12:15 am
Low	APPLIANCE	The state of Virtual Path San_Francisco-Madrid has changed from BAD to GOOD	Jan 24th 2020, 12:05 pm
Low	APPLIANCE	Virtual Path San_Francisco-Madrid Path Madrid-DSL-ono-1->San_Francisco-Broadband-AMIS-2 state has chang...	Jan 24th 2020, 12:05 pm
Low	APPLIANCE	Virtual Path San_Francisco-Madrid Path San_Francisco-Broadband-AMIS-2->Madrid-DSL-ono-1 state has chang...	Jan 24th 2020, 12:05 pm
Low	APPLIANCE	Virtual Path San_Francisco-Madrid Path San_Francisco-Broadband-AMIS-2->Madrid-DSL-ono-1 state has chang...	Jan 24th 2020, 12:05 pm
Low	APPLIANCE	Virtual Path San_Francisco-Madrid Path Madrid-DSL-ono-1->San_Francisco-Broadband-AMIS-2 state has chang...	Jan 24th 2020, 12:05 pm
High	APPLIANCE	The Virtual Path San_Francisco-Madrid is no longer DEAD	Jan 24th 2020, 12:05 pm
Medium	APPLIANCE	Virtual Path San_Francisco-Madrid Path Madrid-DSL-ono-1->San_Francisco-Broadband-AMIS-2 state has chang...	Jan 24th 2020, 12:05 pm

Des options de filtrage appropriées peuvent être utilisées au besoin, par exemple : recherchez toutes les alertes de gravité élevée sur le site ou celles qui se sont produites au cours d'une période donnée.

Vous pouvez également sélectionner et effacer les alertes.

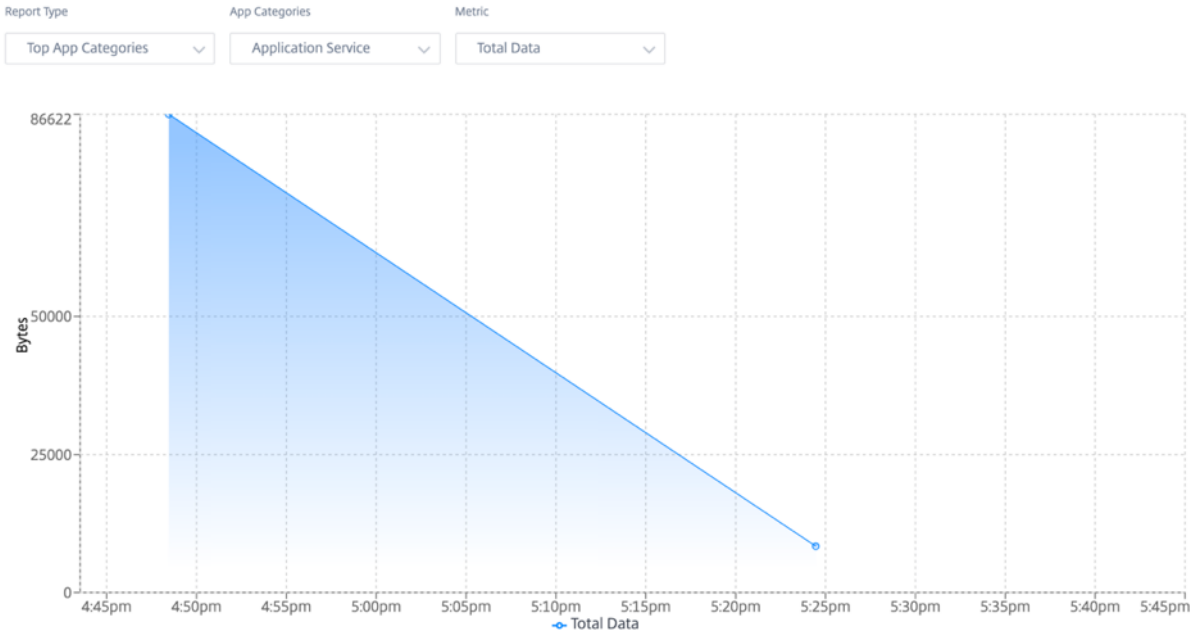
Utilisation

Les administrateurs du site peuvent examiner les tendances d'utilisation, telles que **les principales applications, les principales catégories**d'**applications et la bande passante** des applications sur un site donné.

Principales applications et catégories d'applications

Le graphique **des principales applicationset des principales catégories** d'applications montre les principales applications et familles d'applications les plus utilisées sur le site. Cela vous permet d'analyser le modèle de consommation de données et de réaffecter la limite de bande passante pour chaque classe de données du site.

Vous pouvez également afficher les statistiques d'utilisation de la bande passante. Les statistiques de bande passante sont collectées pour l'intervalle de temps sélectionné. Vous pouvez filtrer le rapport statistique en fonction du **type de rapport, des applications ou des catégories d'applications** et **des mesures**.

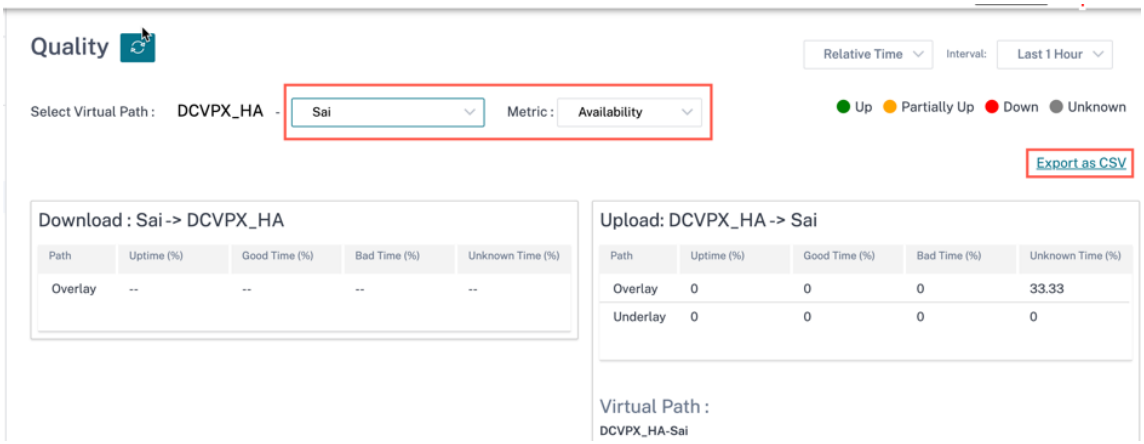


- **Type de rapport :** sélectionnez les **meilleures applications ou catégories** d'applications dans la liste.
- **Applications/Catégories d'applications :** sélectionnez l'application ou les catégories les plus populaires (telles que le service réseau) dans la liste.
- **Mesure :** Sélectionnez la métrique de bande passante (telle que les données totales, les données entrantes, la bande passante totale) dans la liste.

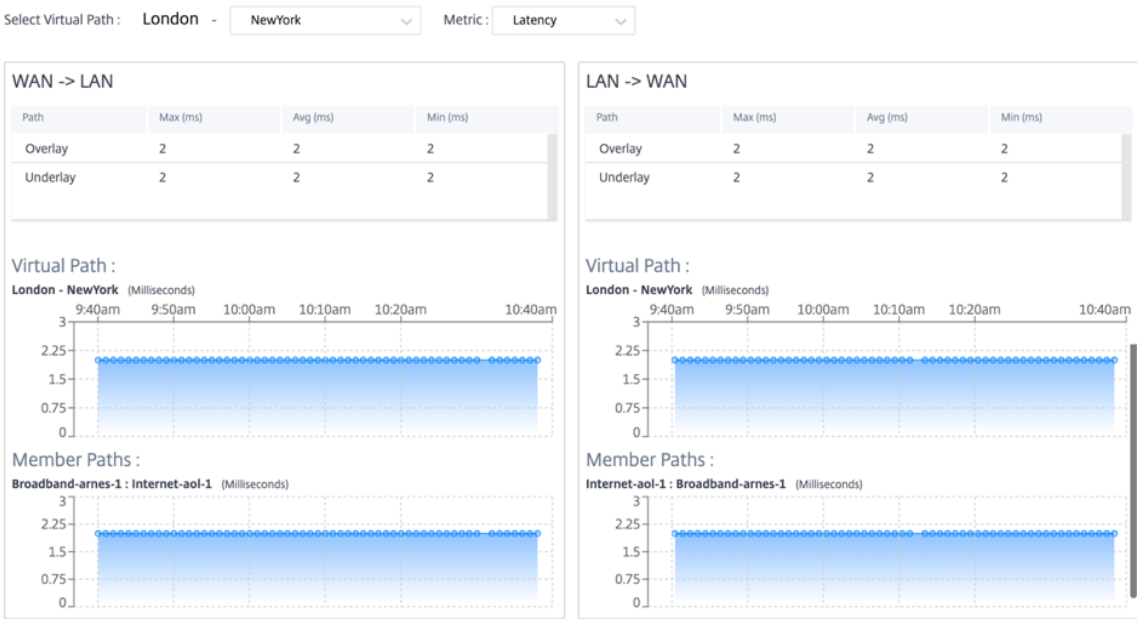
Qualité

Les administrateurs de site peuvent utiliser les rapports Qualité pour analyser la qualité d'expérience (QoE) sur le site pour chaque mesure QoS, telle que la disponibilité, la perte, la latence et la gigue. La mesure qualité est affichée pour les chemins virtuels de superposition et les chemins de membres sous-jacents.

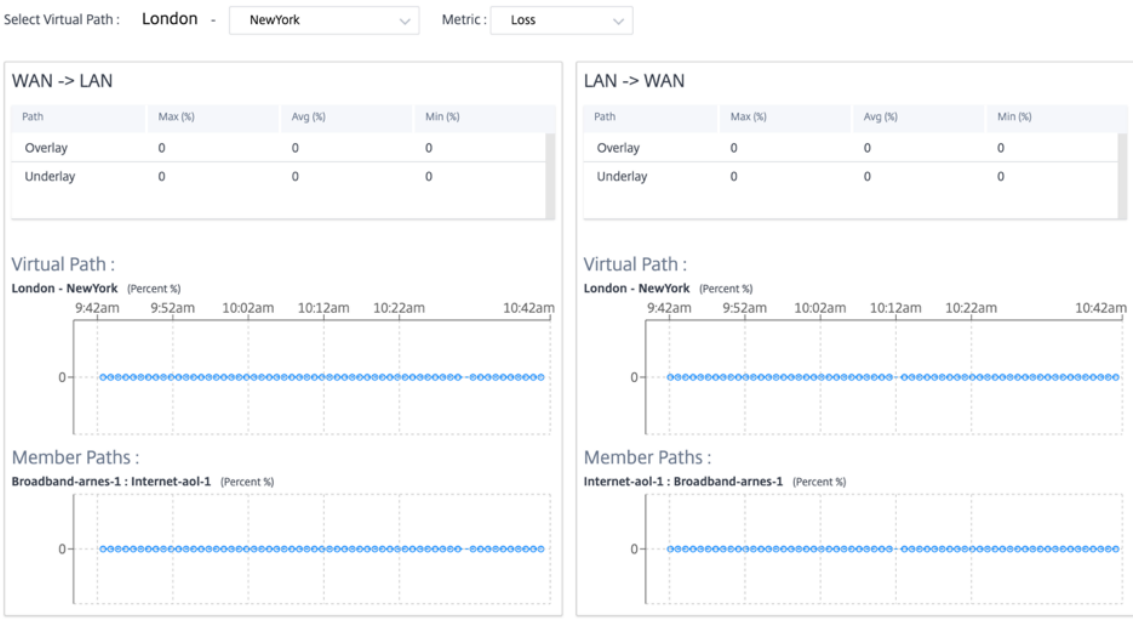
- **Disponibilité**



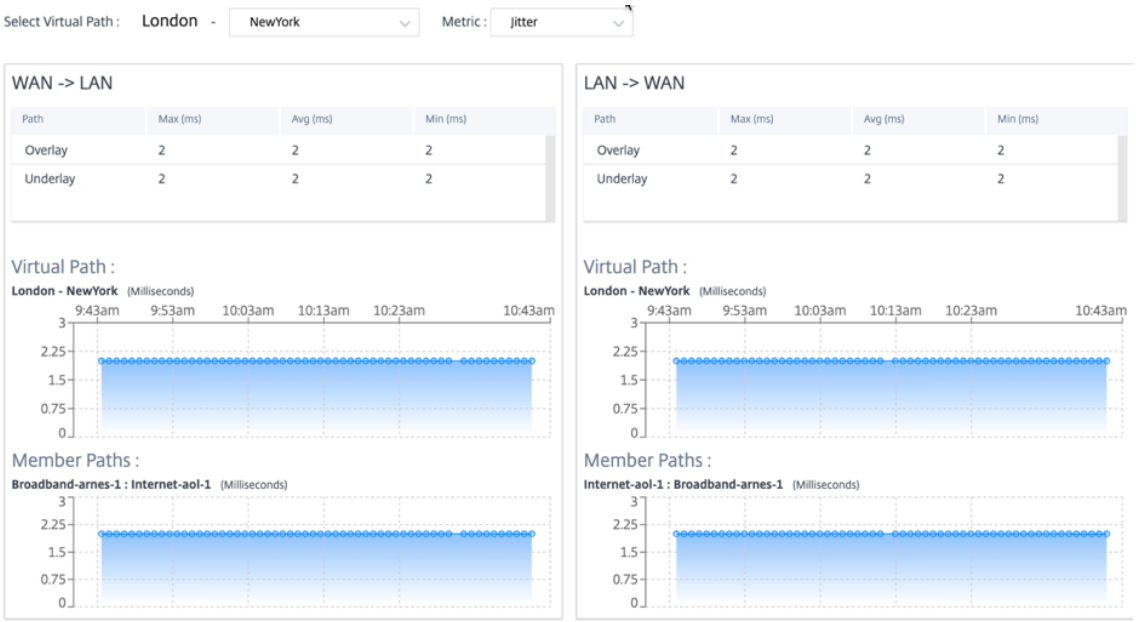
- **Latence**



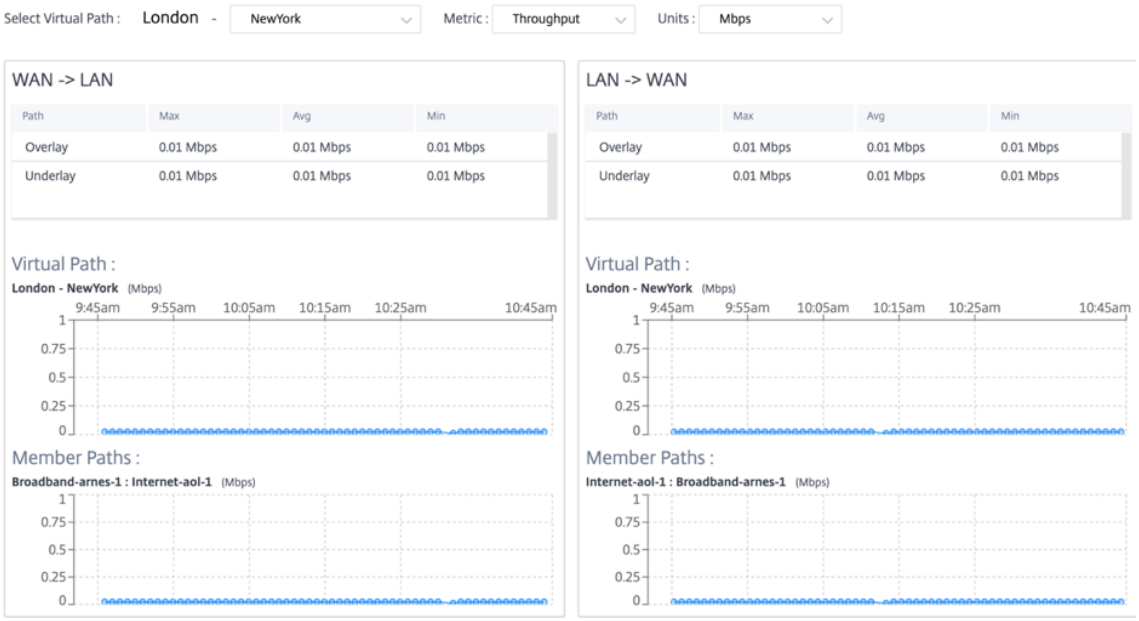
- **Perte**



- **Variation**



- **Débit**

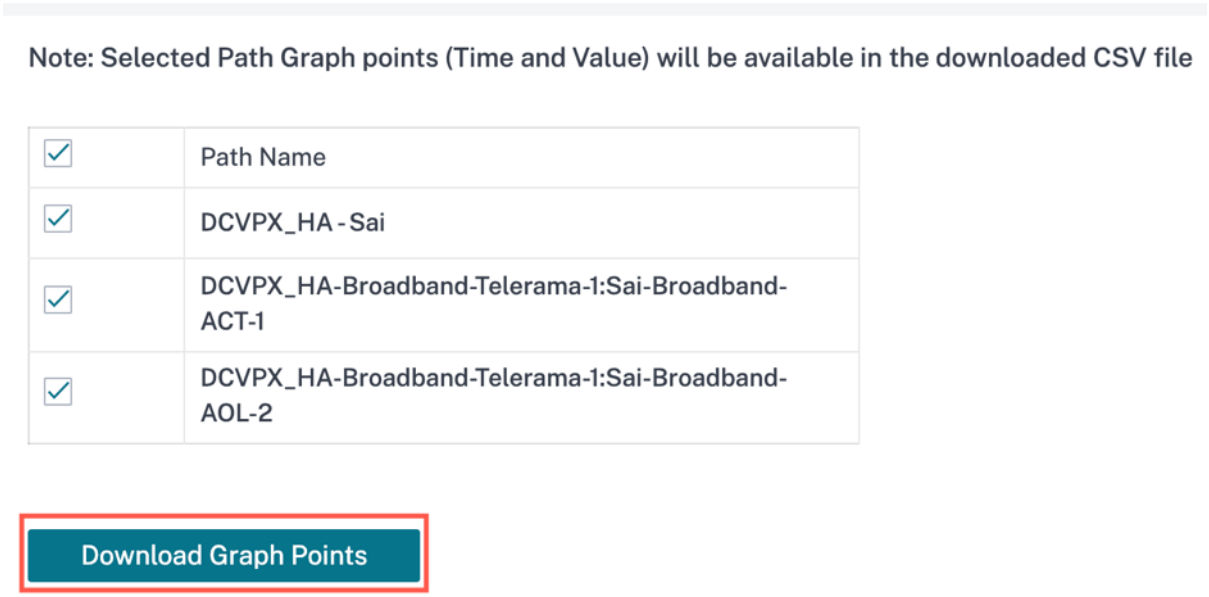


Exporter au format CSV

Grâce à la fonctionnalité **Exporter au format CSV**, vous pouvez télécharger les points du graphique du chemin (chemin virtuel/membre) pour n'importe quelle série chronologique (horaire, hebdomadaire, etc.) sous forme de fichier Excel de valeurs séparées par des virgules (CSV) et être en mesure de tracer tous les points de données distincts pour un rapport de site particulier.

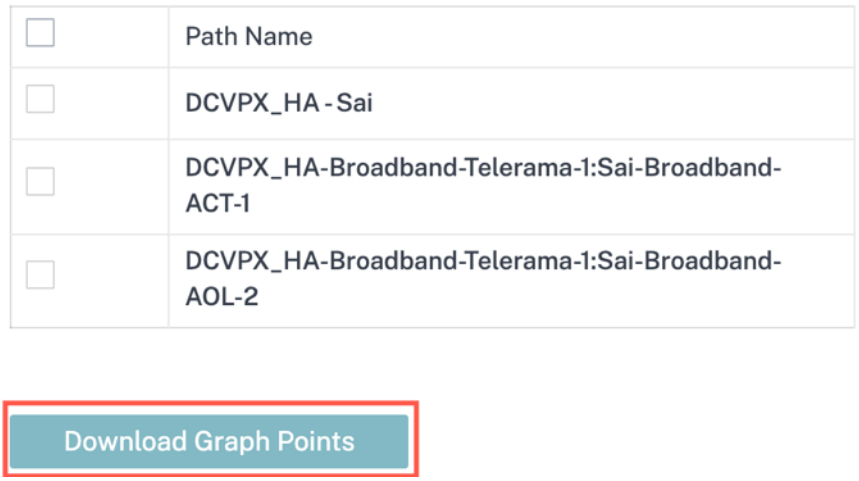
Pour télécharger/exporter le graphe de trajectoire au format CSV, accédez à **Rapports** > **Qualité** au niveau du site. Sélectionnez le site et la métrique dans la liste déroulante et cliquez sur le lien **Exporter au format CSV** .

Sélectionnez le chemin pour lequel vous souhaitez récupérer les données et cliquez sur **Télécharger les points du graphique**.

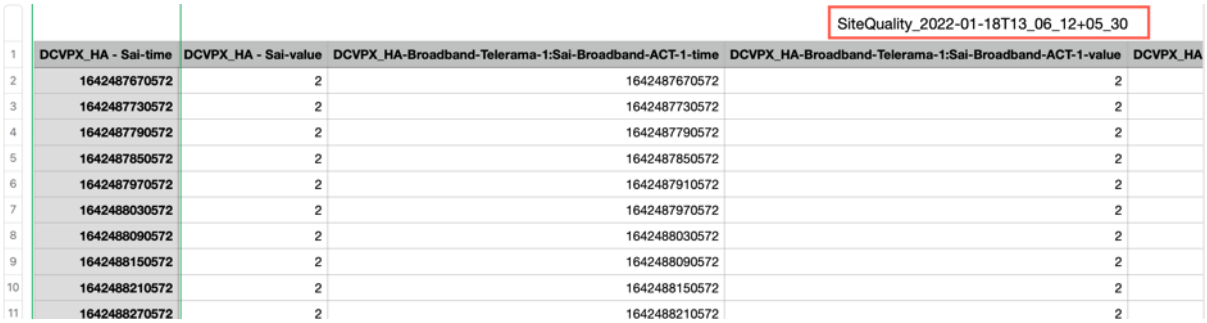


Par défaut, toutes les cases à cocher du chemin sont automatiquement sélectionnées. Vous pouvez le modifier selon vos besoins.

> **Remarque**
>
> Si aucun des chemins n'est sélectionné, le bouton **Télécharger les points du graphique** reste désactivé.



La convention de dénomination du fichier CSV téléchargé est **SiteQuality**, suivie d'un horodatage du téléchargement. Vous pouvez afficher chaque chemin avec une paire de temps et de valeur ainsi qu'un identifiant unique. Vous pouvez voir le temps en millisecondes et la valeur en unités.



			SiteQuality_2022-01-18T13_06_12+05_30		
1	DCVPX_HA - Sai-time	DCVPX_HA - Sai-value	DCVPX_HA-Broadband-Telerama-1:Sai-Broadband-ACT-1-time	DCVPX_HA-Broadband-Telerama-1:Sai-Broadband-ACT-1-value	DCVPX_HA
2	1642487670572	2	1642487670572	2	
3	1642487730572	2	1642487730572	2	
4	1642487790572	2	1642487790572	2	
5	1642487850572	2	1642487850572	2	
6	1642487970572	2	1642487910572	2	
7	1642488030572	2	1642487970572	2	
8	1642488090572	2	1642488030572	2	
9	1642488150572	2	1642488090572	2	
10	1642488210572	2	1642488150572	2	
11	1642488270572	2	1642488210572	2	

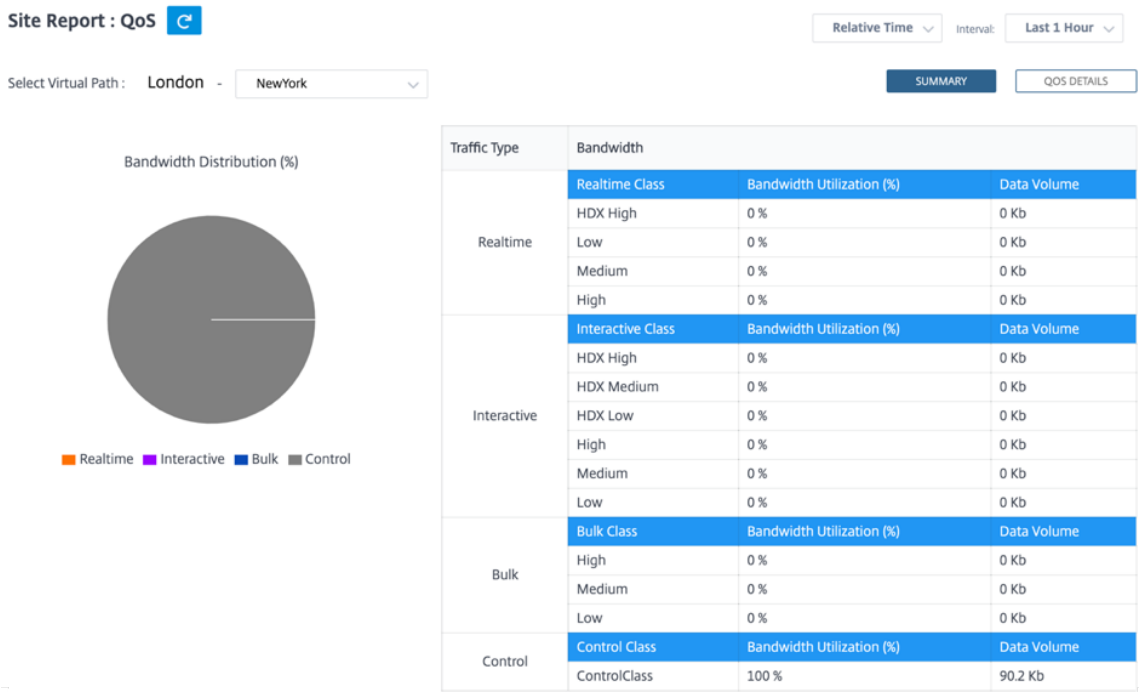
Sur la base de la sélection de mesures suivante, vous pouvez voir que différentes valeurs sont générées dans le fichier CSV :

- **Perte :** La valeur est exprimée en %.
- **Latence et instabilité :** la valeur s'affiche en millisecondes.
- **Débit :** La valeur est exprimée en Kbits/s.
- **Disponibilité :** affiche le chemin vers le haut, partiellement vers le haut, vers le bas et à une heure inconnue.
  - Si la valeur est 4, le chemin est à l'état Up.
  - Si la valeur est 3, le chemin est partiellement à l'état Up.
  - Si la valeur est inférieure à 3, le chemin est dans l'état Infaible/Inactif.

Qualité du service

La qualité de service (QoS) gère le trafic de données afin de réduire la perte de paquets, la latence et la gigue sur le réseau. Pour plus d'informations, consultez la section Qualité de service. Voici deux façons d'afficher le rapport Qualité de service (QoS) :

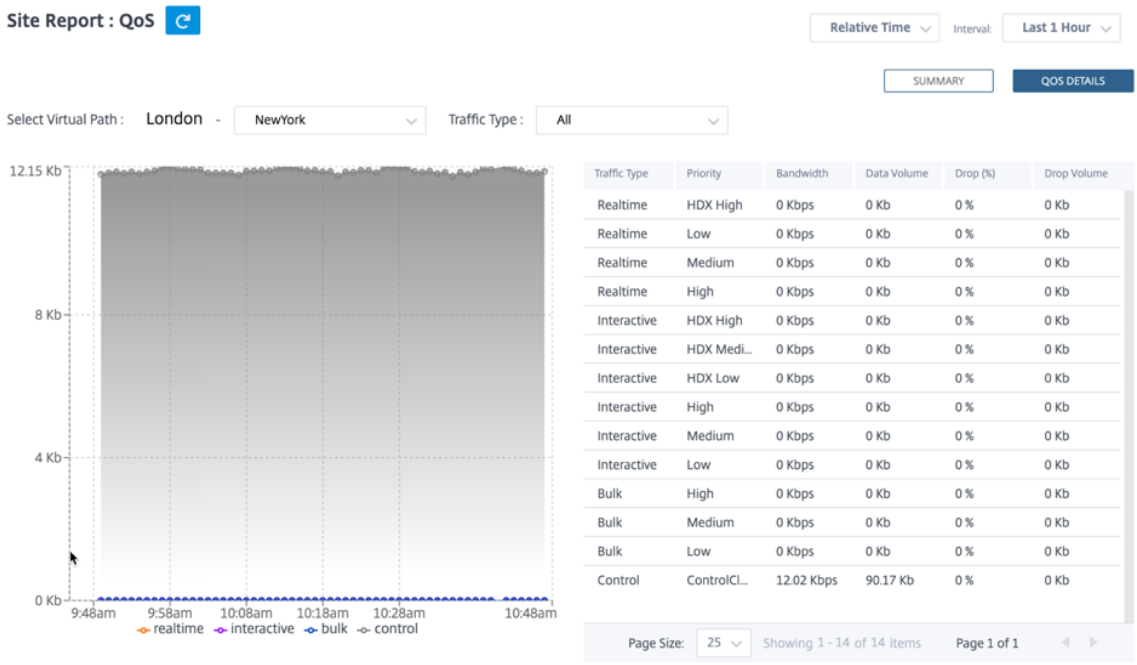
- Vue**récapitulative :** La vue récapitulative fournit une vue d'ensemble de la consommation de bande passante pour tous les types de trafic : en temps réel, interactif, groupé et contrôlé sur le réseau et par site.



Traffic Type	Bandwidth		
Realtime	Realtime Class	Bandwidth Utilization (%)	Data Volume
	HDX High	0 %	0 Kb
	Low	0 %	0 Kb
	Medium	0 %	0 Kb
	High	0 %	0 Kb
Interactive	Interactive Class	Bandwidth Utilization (%)	Data Volume
	HDX High	0 %	0 Kb
	HDX Medium	0 %	0 Kb
	HDX Low	0 %	0 Kb
	High	0 %	0 Kb
	Medium	0 %	0 Kb
	Low	0 %	0 Kb
Bulk	Bulk Class	Bandwidth Utilization (%)	Data Volume
	High	0 %	0 Kb
	Medium	0 %	0 Kb
	Low	0 %	0 Kb
Control	Control Class	Bandwidth Utilization (%)	Data Volume
	ControlClass	100 %	90.2 Kb

  - Temps**réel :** utilisé pour un trafic à faible latence, à faible bande passante et sensible au temps. Les applications en temps réel sont sensibles au temps mais n'ont pas vraiment besoin d'une bande passante élevée (par exemple, la voix sur IP). Les applications en temps réel sont sensibles à la latence et à la gigue, mais peuvent tolérer une certaine perte.
  - **Interactif :** utilisé pour le trafic interactif avec des exigences de latence faibles à moyennes et des exigences de bande passante faibles à moyennes. Les applications interactives impliquent une intervention humaine sous la forme de clics de souris ou de mouvements de curseur. L'interaction se fait généralement entre un client et un serveur. La communication peut ne pas nécessiter de bande passante élevée, mais elle est sensible à la perte et à la latence. Cependant, serveur à client a besoin d'une bande passante élevée pour transférer des informations graphiques, qui peuvent ne pas être sensibles à la perte.
  - **En masse :** Utilisé pour le trafic à bande passante élevée pouvant tolérer une latence élevée. Les applications qui gèrent le transfert de fichiers et qui ont besoin d'une bande passante élevée sont classées comme classe groupée. Ces applications impliquent peu d'interférence humaine et sont principalement traitées par les systèmes eux-mêmes.
  - **Contrôle :** Utilisé pour transférer des paquets de contrôle contenant des informations de routage, de planification et de statistiques de liens.

- **Vue détaillée : La vue** détaillée capture les tendances concernant la consommation de bande passante, le volume de trafic, les paquets abandonnés, etc. Pour chaque classe de QoS associée à un chemin virtuel de superposition. Vous pouvez afficher les statistiques QoS en fonction du chemin virtuel entre deux sites.



Statistiques historiques

Pour chaque site, vous pouvez afficher les statistiques sous forme de graphiques pour les paramètres réseau suivants :

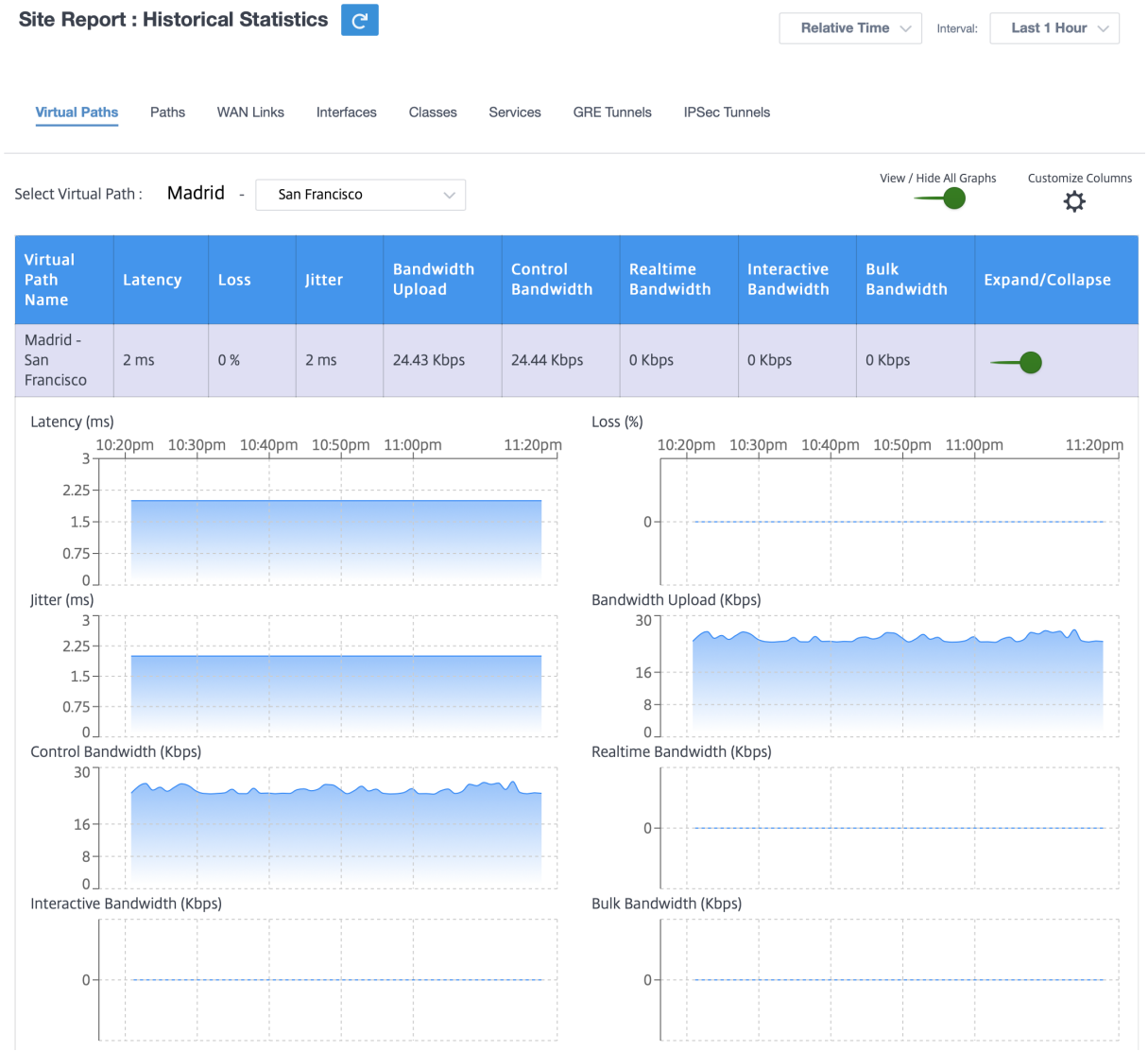
- Chemins virtuels
- Chemins
- Liens WAN
- Interfaces
- Classes
- Services
- Tunnels GRE
- Tunnels IPSec

Les statistiques sont collectées sous forme de graphiques. Ces graphiques sont tracés en fonction de la chronologie par rapport à l'utilisation, ce qui vous permet de comprendre les tendances d'utilisation des différentes propriétés d'objets réseau. Vous pouvez afficher des graphiques pour les statistiques d'application à l'échelle du réseau.

Vous pouvez afficher ou masquer les graphiques et personnaliser les colonnes selon vos besoins.

Chemins virtuels

Pour consulter les statistiques **des chemins virtuels**, accédez à **Rapports > Statistiques > onglet Chemins virtuels** .



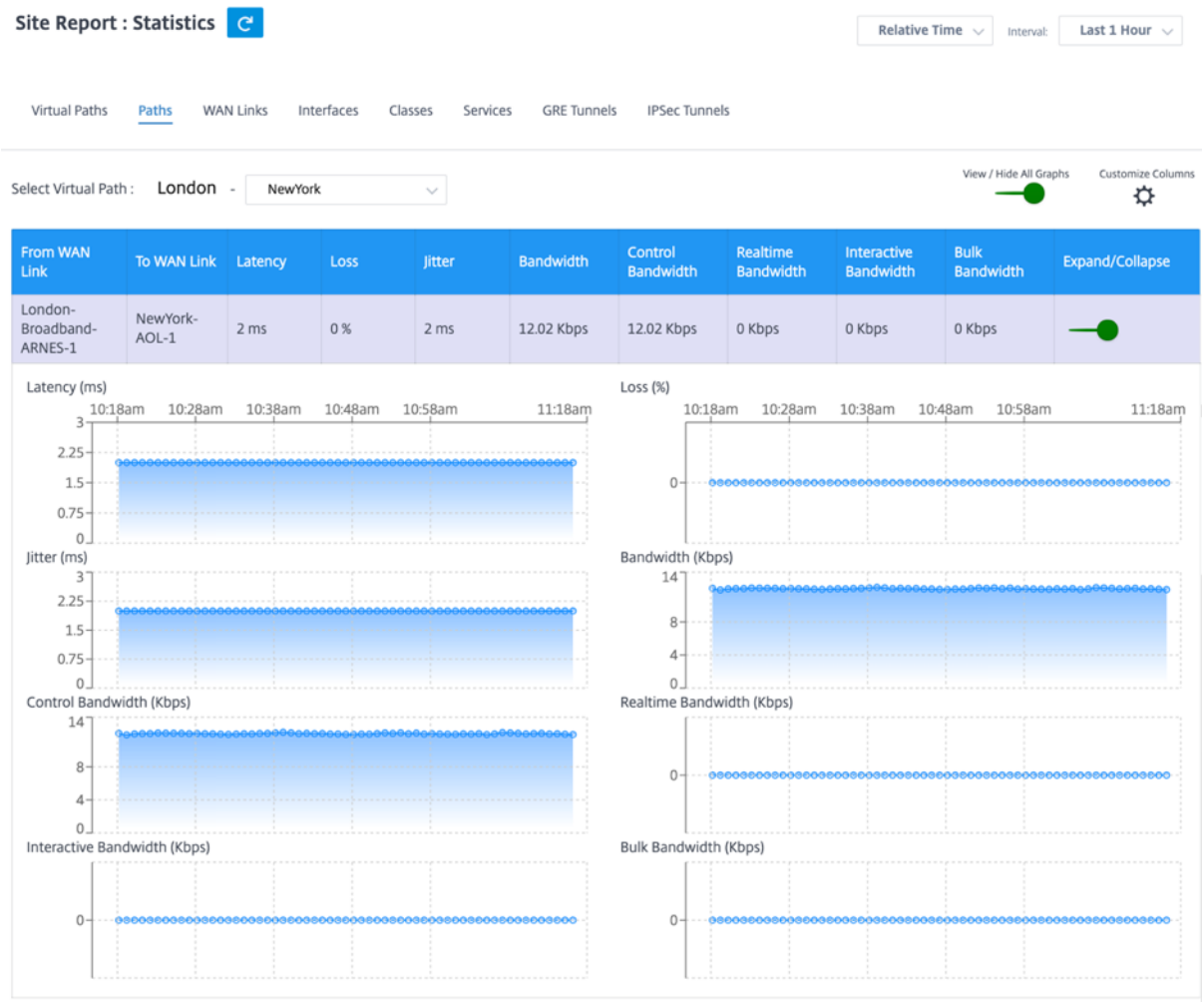
Vous pouvez afficher les mesures suivantes :

- **Nom du chemin virtuel : nom**du chemin virtuel.
- **Latence** : latence en millisecondes pour le trafic en temps réel.
- **Perte** : pourcentage de paquets perdus.
- **Jitter** : variation du délai de réception des paquets, en millisecondes.
- **Entrée de bande passante** : **utilisation de la bande passante d'entrée (LAN > WAN)** pour la période sélectionnée.
- **Bande passante de contrôle** : bande passante utilisée pour transférer des paquets de contrôle contenant des informations de routage, de planification et de statistiques de liens.

- **Bande passante en temps réel** : bande passante consommée par les applications appartenant au type de classe en temps réel dans la configuration SD-WAN. Les performances de ces applications dépendent en grande partie de la latence du réseau. Un paquet retardé est pire qu'un paquet perdu (par exemple, VoIP, Skype for Business).
- **Bande passante interactive** : bande passante consommée par les applications appartenant au type de classe interactive dans la configuration SD-WAN. Les performances de ces applications dépendent en grande partie de la latence du réseau et de la perte de paquets (par exemple, XenDesktop, XenApp).
- **Bande passante en masse** : bande passante consommée par les applications appartenant au type de classe de masse dans la configuration SD-WAN. Ces applications impliquent peu d'intervention humaine et sont principalement gérées par les systèmes eux-mêmes (par exemple, FTP, opérations de sauvegarde).
- **Développer/Réduire** : Vous pouvez développer ou réduire les données selon vos besoins.

Chemins

Pour consulter les statistiques **des chemins**, accédez à **Rapports > Statistiques > onglet Chemins** .



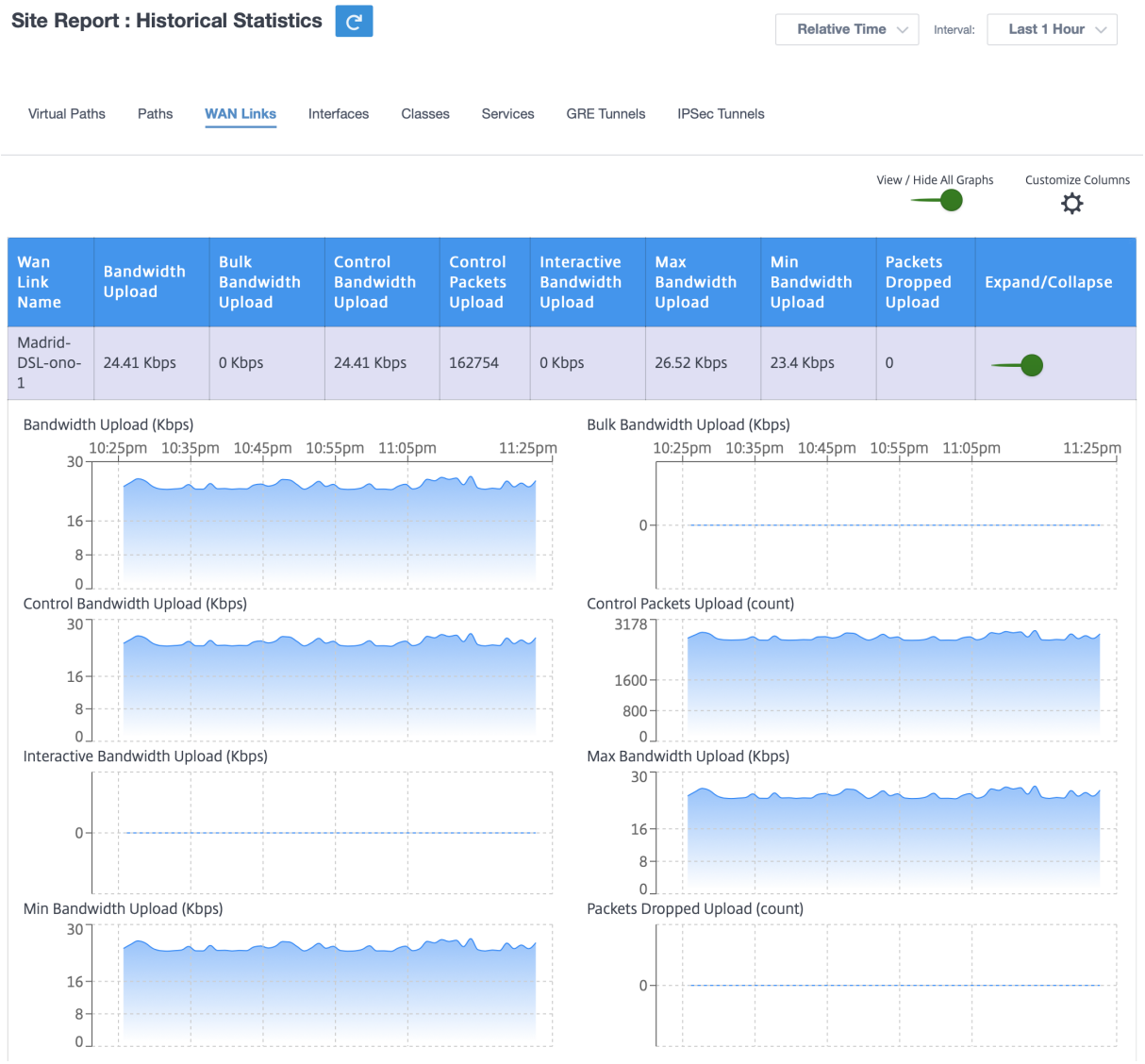
Vous pouvez afficher les mesures suivantes :

- **À partir du lien WAN** : le lien WAN source.
- **Vers le lien WAN** : le lien WAN de destination.
- **Latence** : latence en millisecondes pour le trafic en temps réel.
- **Perte** : pourcentage de paquets perdus.
- **Jitter** : variation du délai de réception des paquets, en millisecondes.
- **Bande passante** : bande passante totale consommée par tous les types de paquets. Bande passante = Contrôle de la bande passante + bande passante en temps réel + bande passante interactive et bande passante en bloc.
- **Bande passante de contrôle** : bande passante utilisée pour transférer des paquets de contrôle contenant des informations de routage, de planification et de statistiques de liens.
- **Bande passante en temps réel** : bande passante consommée par les applications appartenant au type de classe en temps réel dans la configuration SD-WAN. Les performances de ces applications dépendent en grande partie de la latence du réseau. Un paquet retardé est pire qu'un paquet perdu (par exemple, VoIP, Skype for Business).

- **Bande passante interactive** : bande passante consommée par les applications appartenant au type de classe interactive dans la configuration SD-WAN. Les performances de ces applications dépendent en grande partie de la latence du réseau et de la perte de paquets (par exemple, XenDesktop, XenApp).
- **Bande passante en masse** : bande passante consommée par les applications appartenant au type de classe de masse dans la configuration SD-WAN. Ces applications impliquent peu d'intervention humaine et sont principalement gérées par les systèmes eux-mêmes (par exemple, FTP, opérations de sauvegarde).
- **Développer/Réduire** : Vous pouvez développer ou réduire les données selon vos besoins.

Liens WAN

Pour afficher les statistiques au niveau de la **liaison WAN**, accédez à **Rapports > Statistiques > onglet Liens WAN** .



Vous pouvez afficher les mesures suivantes :

- **Nom du lien WAN** : nom du chemin.
- **Entrée de bande passante** : **utilisation de la bande passante d'entrée (LAN > WAN)** pour la période sélectionnée.
- Entrée de**bande passante en masse : bande passante du chemin virtuel d'entrée (LAN > WAN)** utilisée par le trafic en masse pendant la période sélectionnée.
- **Entrée de bande passante de contrôle : bande passante du chemin virtuel d'entrée (LAN > WAN)** utilisée par le trafic de contrôle pendant la période sélectionnée.
- **Entrée de paquets de contrôle** : **paquets de contrôle de chemin virtuel d'entrée (LAN > WAN)** pour la période sélectionnée.
- Entrée de**bande passante interactive** : **bande passante du chemin virtuel d'entrée (LAN > WAN)** utilisée par le trafic interactif pendant la période sélectionnée.

- Entrée**de bande passante maximale : bande passante d'entrée maximale (LAN > WAN)** utilisée en une minute pendant la période sélectionnée.
- Entrée**de bande passante minimale : bande passante d'entrée minimale (LAN > WAN)** utilisée en une minute pour la période sélectionnée.
- **Développer/Réduire** : Vous pouvez développer ou réduire les données selon vos besoins.

Interfaces

Le rapport statistique sur les interfaces vous aide, lors du dépannage, à déterminer rapidement si l'un des ports est en panne. Vous pouvez également afficher la bande passante transmise et reçue, ou les détails des paquets sur chaque port. Vous pouvez également afficher le nombre d'erreurs qui se sont produites sur ces interfaces pendant une certaine période.

Pour consulter les statistiques de **l'interface**, accédez à **Rapports > Statistiques > onglet Interfaces** .

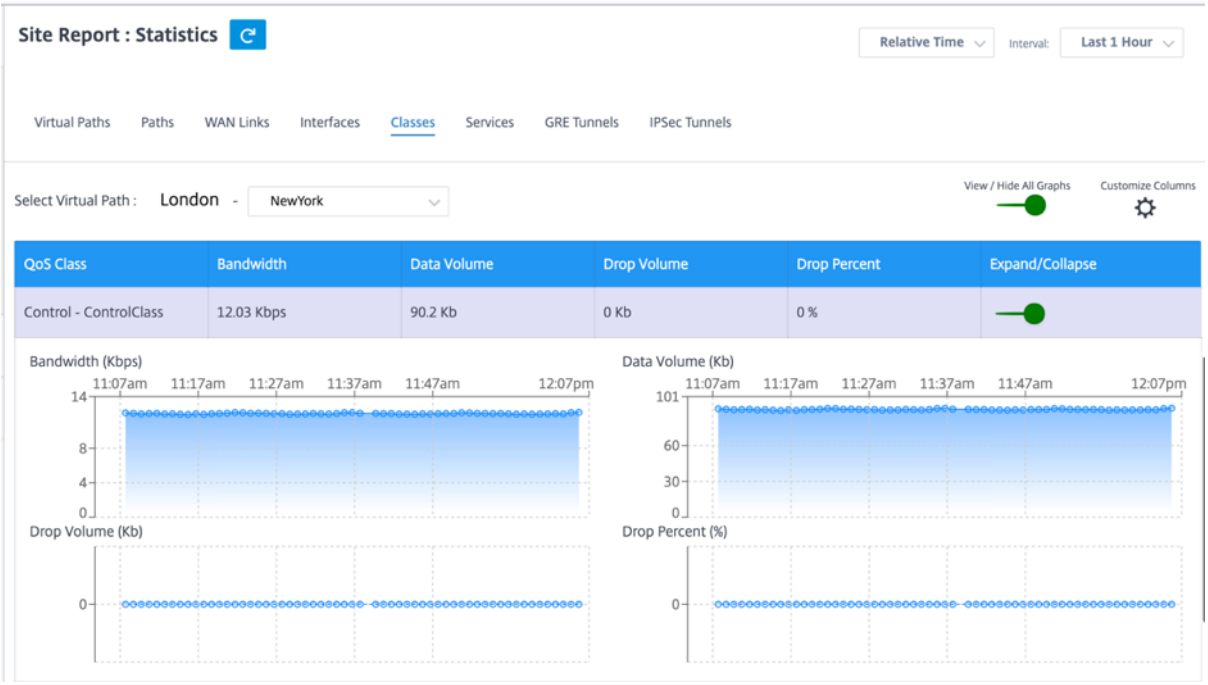
Vous pouvez afficher les mesures suivantes :

- **Nom de l'interface** : nom de l'interface Ethernet.
- **Bande passante Tx** : bande passante transmise.
- **Bande passante Rx** : Bande passante reçue.
- **Erreurs** : nombre d'erreurs observées au cours de la période sélectionnée.
- **Développer/Réduire** : Vous pouvez développer ou réduire les données selon vos besoins.

Classes

Les services virtuels peuvent être affectés à des classes QoS particulières, et différentes restrictions de bande passante peuvent être appliquées à différentes classes.

Pour consulter les statistiques des **cours**, accédez à **Rapports > Statistiques > onglet Classes** .



Vous pouvez afficher les mesures suivantes :

- **Classe QoS** : nom de la classe.
- **Bande passante** : bande passante transmise.
- **Volume de données** : données envoyées, en Kbits/s.
- **Volume de dépôt** : pourcentage de données supprimées.
- **Pourcentage de perte** : pourcentage de données supprimées.
- **Développer/Réduire** : Vous pouvez développer ou réduire les données selon vos besoins.

Services

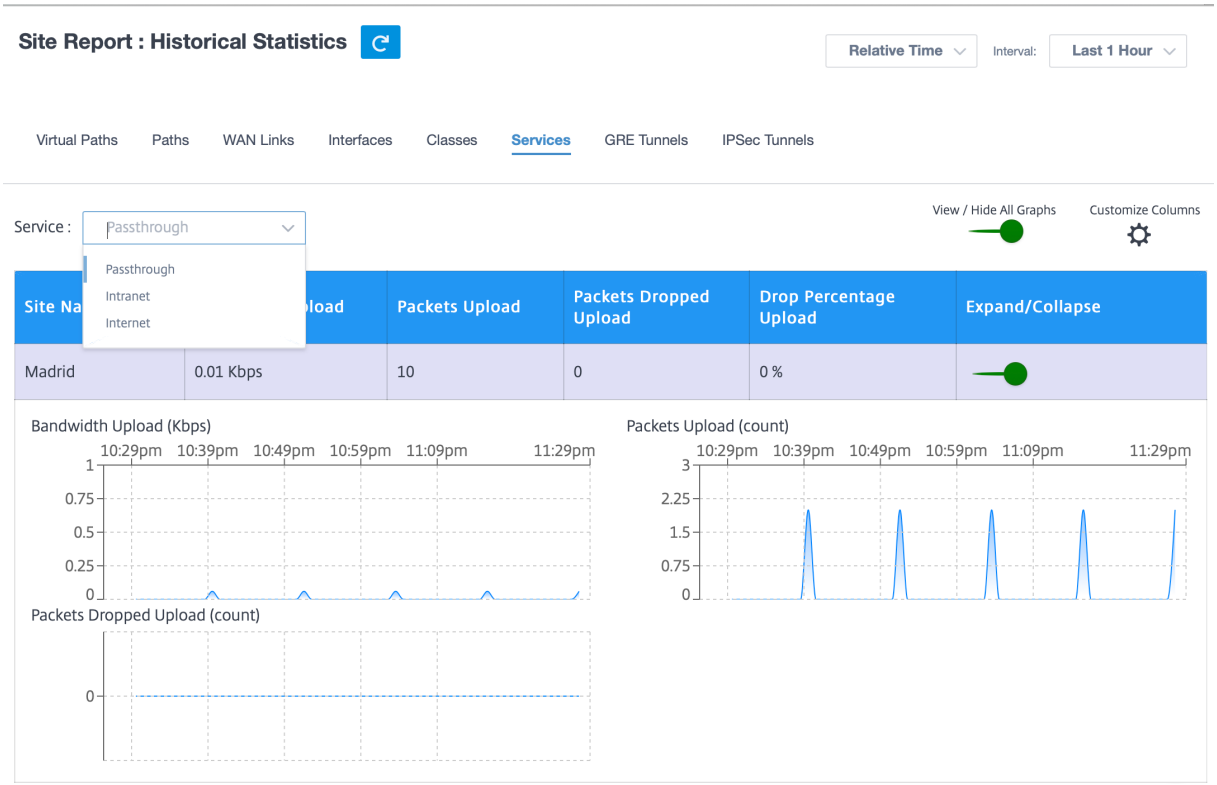
Pour consulter les statistiques **des services**, accédez à **Rapports > Statistiques > onglet Services** .

Sélectionnez le type de service dans la liste. Les options sont les suivantes :

- **Passthrough** —Ce service gère le trafic qui n'est pas intercepté, retardé, façonné ou modifié par le SD-WAN. Le trafic dirigé vers le service relais comprend les diffusions, les ARP et tout autre trafic non IPv4, ainsi que le trafic sur le sous-réseau local de Virtual WAN Appliance, les sous-réseaux configurés ou les règles appliquées par l'administrateur réseau. Ce trafic n'est pas retardé, façonné ou modifié par le SD-WAN. Par conséquent, vous devez vous assurer que le trafic Passthrough ne consomme pas de ressources importantes sur les liaisons WAN que l'appliance SD-WAN est configurée pour utiliser pour d'autres services.
- **Intranet** : ce service gère le trafic Intranet d'entreprise qui n'a pas été défini pour la transmission via un chemin virtuel. Comme pour le trafic Internet, il n'est pas encapsulé, et le SD-WAN

gère la bande passante en limitant ce trafic par rapport aux autres types de services en période de congestion. Dans certaines conditions, et s'il est configuré pour Intranet Fallback sur le chemin virtuel, le trafic qui se déplace habituellement avec un chemin virtuel peut plutôt être traité comme du trafic Intranet, afin de maintenir la fiabilité du réseau.

- **Internet** : ce service gère le trafic entre un site Enterprise et des sites sur l'Internet public. Le trafic de ce type n'est pas encapsulé. En période de congestion, le SD-WAN gère activement la bande passante en limitant le trafic Internet par rapport au chemin virtuel, et le trafic intranet selon la configuration SD-WAN établie par l'administrateur.



Vous pouvez afficher les mesures suivantes :

- **Nom du site** : nom du site.
- **Entrée de bande passante** : **utilisation de la bande passante d'entrée (LAN > WAN)** pour la période sélectionnée.
- **Entrée de paquets** : **(LAN > WAN) Paquets** envoyés pendant l'intervalle de temps sélectionné.
- **Développer/Réduire** : Vous pouvez développer ou réduire les données selon vos besoins.

Tunnels GRE

Vous pouvez utiliser un mécanisme de tunnel pour transporter des paquets d'un protocole dans un autre protocole. Le protocole qui porte l'autre protocole est appelé le protocole de transport, et le

protocole transporté est appelé le protocole passager. Generic Routing Encapsulation (GRE) est un mécanisme de tunnel qui utilise IP comme protocole de transport et peut transporter de nombreux protocoles passagers différents.

L'adresse source du tunnel et l'adresse de destination sont utilisées pour identifier les deux points de terminaison des liens virtuels point à point dans le tunnel. Pour plus d'informations sur la configuration des tunnels GRE sur les appliances Citrix SD-WAN, consultez Tunnel GRE.

Pour consulter les statistiques **du tunnel GRE**, accédez à **Rapports > Statistiques > onglet Tunnels GRE** .

Vous pouvez afficher les mesures suivantes :

- **Nom du site** : nom du site.
- **Bande passante Tx** : bande passante transmise.
- **Bande passante Rx** : Bande passante reçue.
- **Paquet abandonné** : nombre de paquets abandonnés en raison de la congestion du réseau.
- **Paquets fragmentés** : nombre de paquets fragmentés. Les paquets sont fragmentés pour créer des paquets plus petits qui peuvent passer par un lien avec un MTU plus petit que le datagramme d'origine. Les fragments sont réassemblés par l'hôte récepteur.
- **Développer/Réduire** : Vous pouvez développer ou réduire les données selon vos besoins.

Tunnels IPSec

Les protocoles de sécurité IP (IPsec) fournissent des services de sécurité tels que le chiffrement des données sensibles, l'authentification, la protection contre la réexécution et la confidentialité des données pour les paquets IP. Encapsulating Security Payload (ESP) et Authentication Header (AH) sont les deux protocoles de sécurité IPSec utilisés pour fournir ces services de sécurité.

En mode tunnel IPSec, l'ensemble du paquet IP d'origine est protégé par IPSec. Le paquet IP d'origine est enveloppé et chiffré, et un nouvel en-tête IP est ajouté avant de transmettre le paquet via le tunnel VPN.
Pour plus d'informations sur la configuration de tunnels IPsec sur les appliances Citrix SD-WAN, consultez Terminaison du tunnel IPSec.

Pour consulter les statistiques **du tunnel IPsec**, accédez à **Rapports > statistiques > onglet Tunnels IPSec** .

Vous pouvez afficher les mesures suivantes :

- **Nom du tunnel** : nom du tunnel.
- **État du tunnel : état**du tunnel IPsec.
- **MTU** : unité de transmission maximale : taille du plus grand datagramme IP pouvant être transféré via un lien spécifique.

- **Paquet reçu** : Nombre de paquets reçus.
- **Paquets envoyés** : Nombre de paquets envoyés.
- **Paquet abandonné** : nombre de paquets abandonnés en raison de la congestion du réseau.
- **Octets supprimés** : nombre d'octets supprimés.
- **Développer/Réduire** : Vous pouvez développer ou réduire les données selon vos besoins.

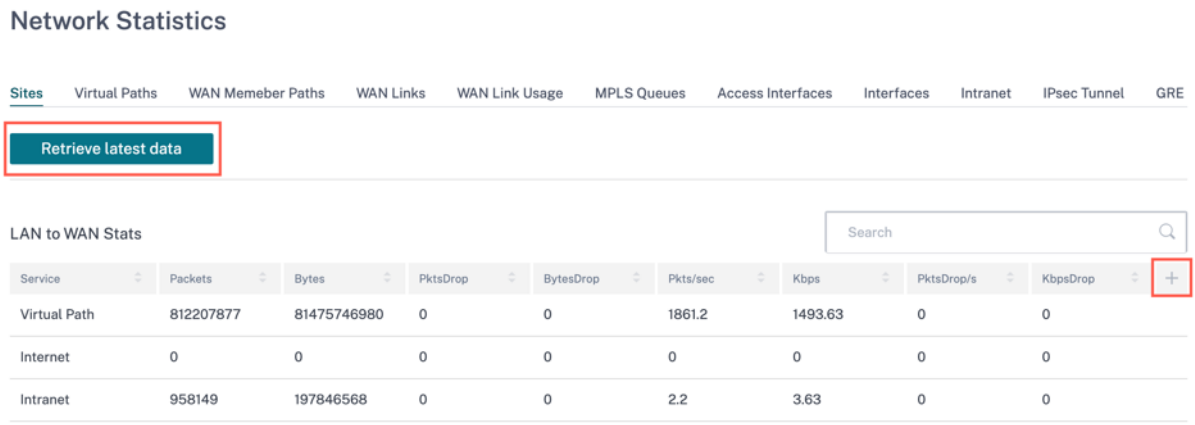
Statistiques en temps réel

Statistiques du réseau

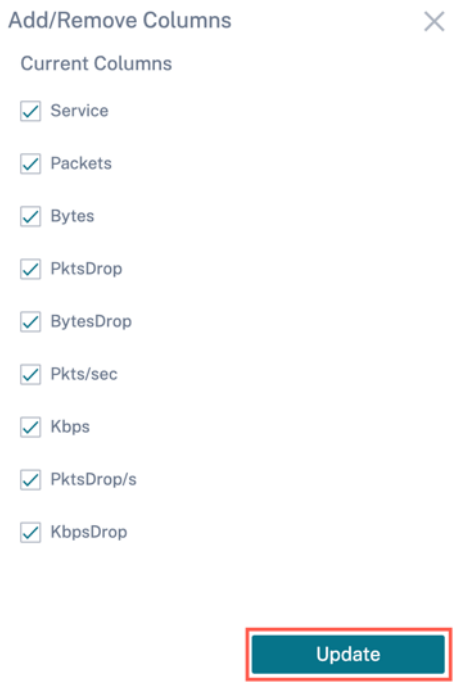
Vous pouvez obtenir les informations statistiques en temps réel suivantes sous **Rapports > Temps réel > Statistiques du réseau** :

- Site
- Chemins virtuels
- Chemins pour les membres
- Liens WAN
- Utilisation de la liaison WAN
- Files d'attente MPLS
- Interfaces d'accès
- Interfaces
- Intranet
- Tunnel IPSec
- GRE

Pour obtenir le rapport statistique en temps réel, accédez à l'onglet requis (site, chemins virtuels, liens WAN) et cliquez sur **Récupérer les dernières données**.



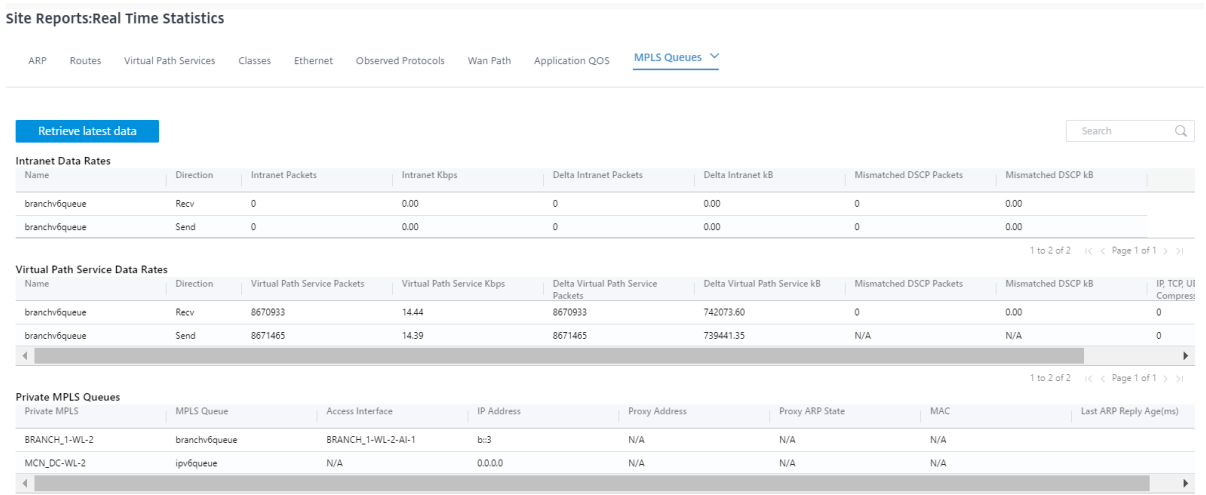
Cliquez sur le symbole plus (+) si vous souhaitez ajouter ou supprimer une colonne du tableau des statistiques, puis cliquez sur **Mettre à jour**.



Files d'attente MPLS Les files d'attente MPLS vous permettent de définir les files d'attente correspondant aux files d'attente MPLS du fournisseur de services, sur les liens WAN MPLS MPLS. Pour plus d'informations sur la configuration des files d'attente MPLS, voir Files d'attente MPLS.

Pour consulter les statistiques des files d'attente MPLS, au niveau du site, accédez à **Rapports** > **Temps réel** > **Statistiques réseau**. Cliquez sur **Files d'attente MPLS**, puis sur **Récupérer les dernières données**. Les données les plus récentes des files d'attente MPLS sont extraites de l'appliance et affichées dans Citrix SD-WAN Orchestrator for On-premises.

Vous pouvez afficher la direction, le nombre de paquets, les paquets delta et les paquets DSCP incompatibles pour les services Intranet et Virtual path.



Pour les files d'attente MPLS privées, vous pouvez afficher les détails suivants :

- **MPLS**privé : liaison WAN MPLS privée.
- **File d'attente MPLS** : file d'attente MPLS associée à la liaison WAN MPLS.
- **Interface d'accès : interface**d'accès associée à la file d'attente MPLS.
- **Adresse IP : adresse**IP associée à la file d'attente MPLS.
- **Adresse du proxy : adresse**IP du proxy associée à la file d'attente MPLS.
- État**ARP du proxy : état**du protocole de résolution d'adresses proxy. Activé, désactivé ou N/A
- **MAC** : adresse MAC de l'interface associée à la file d'attente MPLS.
- **Age de la dernière réponse ARP** : heure en millisecondes à laquelle la dernière réponse ARP a été reçue.

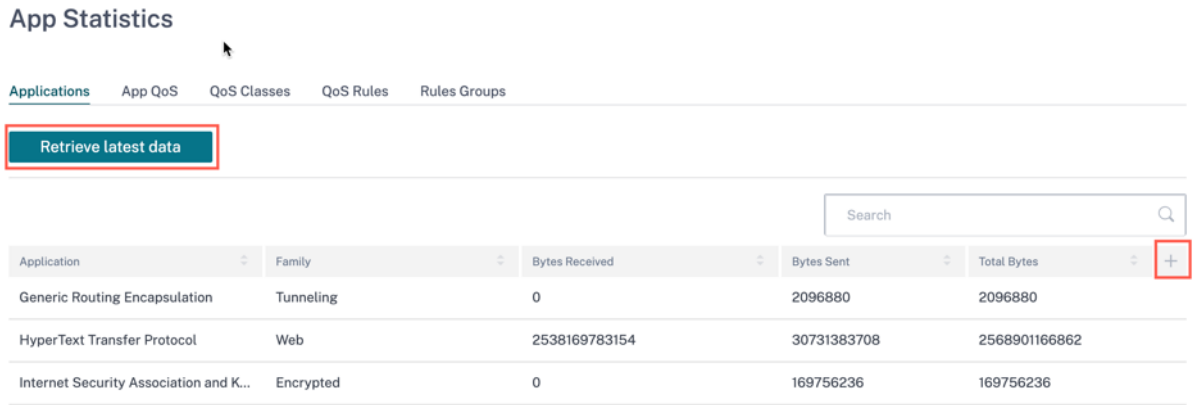
Pour plus de détails sur la résolution des problèmes, voir Résolution des files d'attente MPLS.

Statistiques de l'application

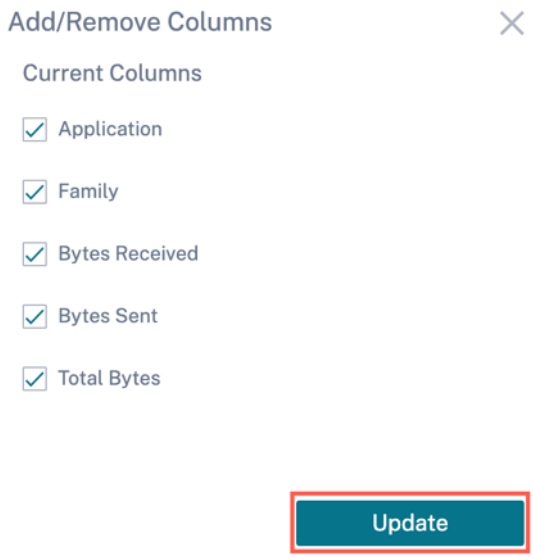
Vous pouvez obtenir les informations statistiques en temps réel suivantes sous **Rapports > Temps réel > Statistiques des applications** :

- Applications
- Protocoles observés
- QoS des applications
- Cours de QoS
- Règles de QoS
- Groupes de règles

Pour obtenir le rapport statistique en temps réel, accédez à l'onglet requis (applications, QoS des applications, règle de QoS) et cliquez sur **Récupérer les dernières données**.



Cliquez sur le symbole plus (+) si vous souhaitez ajouter ou supprimer une colonne du tableau des statistiques, puis cliquez sur **Mettre à jour**.

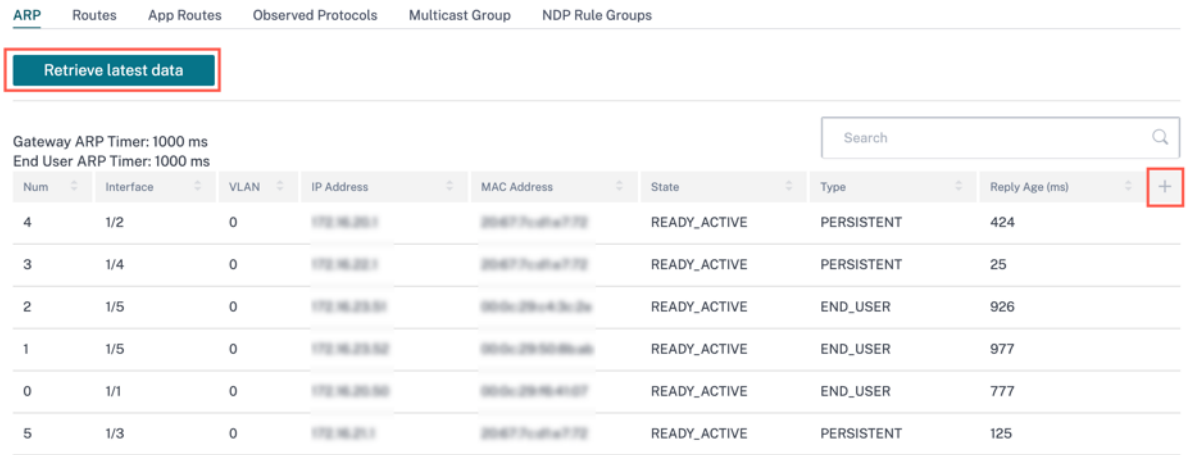


Statistiques d'itinéraire

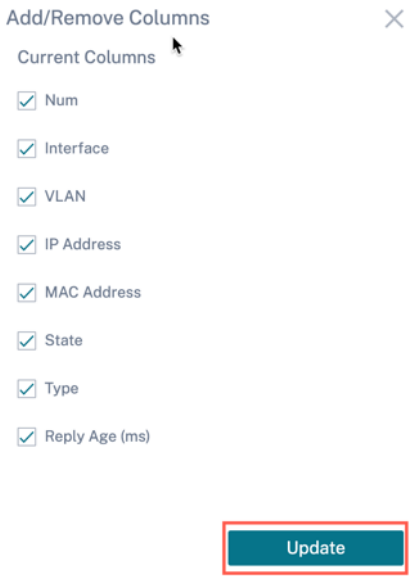
Vous pouvez obtenir les informations statistiques d'itinéraire en temps réel suivantes sous **Rapports > Temps réel > Statistiques d'itinéraires** :

- ARP (Protocole de résolution d'adresses)
- Itinéraires
- Itinéraires de l'
- Protocoles observés
- Groupe de multidiffusion
- Groupes de règles du NDP

Pour obtenir le rapport statistique en temps réel, accédez à l'onglet requis (tel que ARP, Routes, App Routes) et cliquez sur **Récupérer les dernières données**.



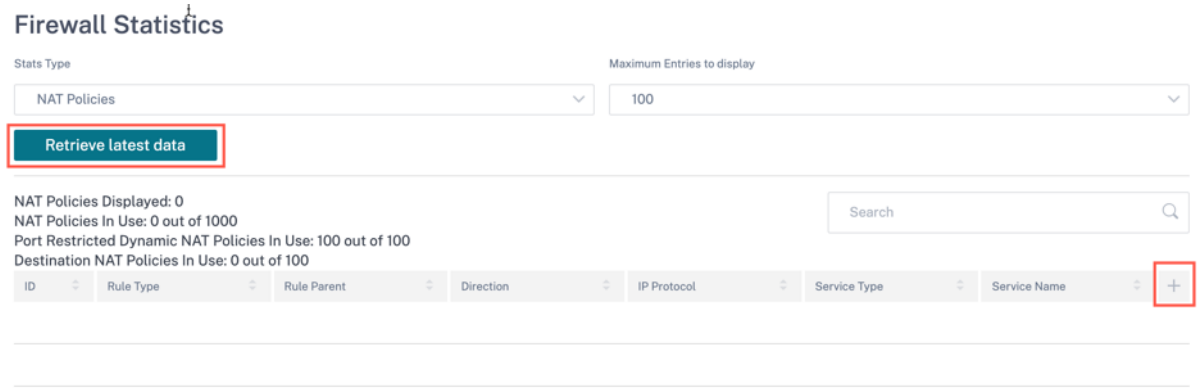
Cliquez sur le symbole plus (+) si vous souhaitez ajouter ou supprimer une colonne du tableau des statistiques, puis cliquez sur **Mettre à jour**.



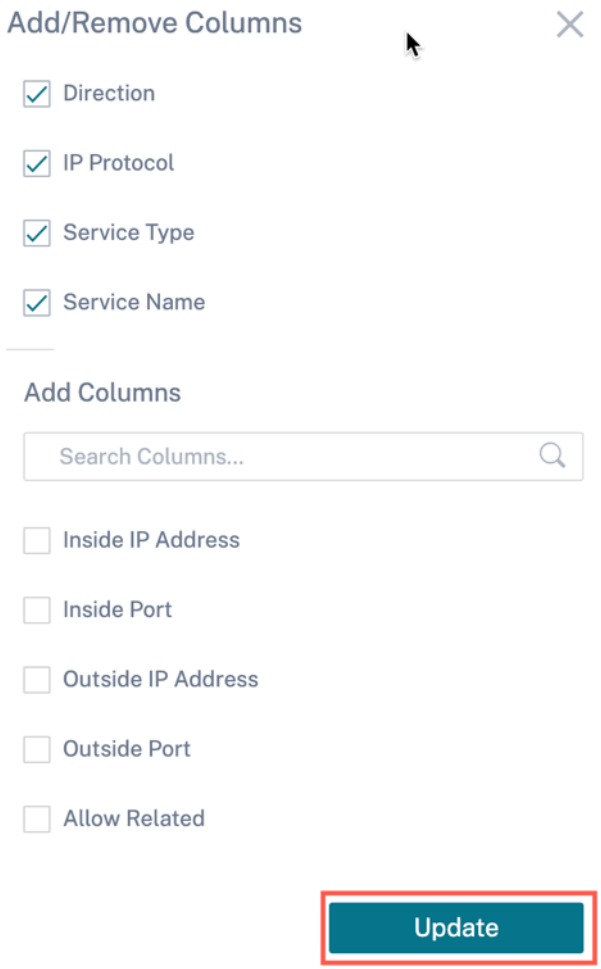
Statistiques de pare-feu

La page des **statistiques du pare-feu** fournit l'état de la connexion, les politiques du protocole d'adresse réseau (NAT) et les politiques de filtrage liées à une session particulière en fonction de l'action de pare-feu configurée. Les connexions pare-feu fournissent également des détails complets sur la source et la destination de la connexion.

Vous pouvez obtenir les informations statistiques du pare-feu en temps réel sous **Rapports > Temps réel > Statistiques du pare-feu**. Sélectionnez le type de statistiques dans la liste déroulante (connexion, politiques NAT, politiques de filtrage). Sélectionnez le nombre maximum d'entrées à afficher, puis cliquez sur **Récupérer les dernières données**.

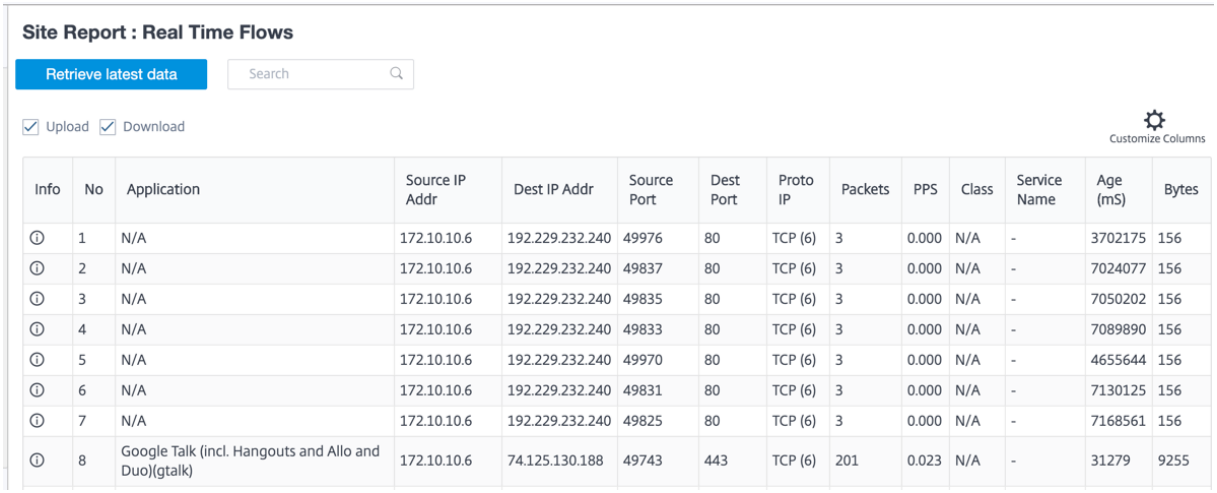


Cliquez sur le symbole plus (+) si vous souhaitez ajouter ou supprimer une colonne du tableau des statistiques, puis cliquez sur **Mettre à jour**.



Flux

La fonction **Flows** fournit des informations de flux unidirectionnelles relatives à une session particulière passant par l'appliance. Ceci fournit des informations sur le type de service de destination dans lequel se trouve le flux, ainsi que les informations relatives à la règle et au type de classe ainsi que sur le mode de transmission.



Info	No	Application	Source IP Addr	Dest IP Addr	Source Port	Dest Port	Proto IP	Packets	PPS	Class	Service Name	Age (mS)	Bytes
ⓘ	1	N/A	172.10.10.6	192.229.232.240	49976	80	TCP (6)	3	0.000	N/A	-	3702175	156
ⓘ	2	N/A	172.10.10.6	192.229.232.240	49837	80	TCP (6)	3	0.000	N/A	-	7024077	156
ⓘ	3	N/A	172.10.10.6	192.229.232.240	49835	80	TCP (6)	3	0.000	N/A	-	7050202	156
ⓘ	4	N/A	172.10.10.6	192.229.232.240	49833	80	TCP (6)	3	0.000	N/A	-	7089890	156
ⓘ	5	N/A	172.10.10.6	192.229.232.240	49970	80	TCP (6)	3	0.000	N/A	-	4655644	156
ⓘ	6	N/A	172.10.10.6	192.229.232.240	49831	80	TCP (6)	3	0.000	N/A	-	7130125	156
ⓘ	7	N/A	172.10.10.6	192.229.232.240	49825	80	TCP (6)	3	0.000	N/A	-	7168561	156
ⓘ	8	Google Talk (incl. Hangouts and Allo and Duo)(gtalk)	172.10.10.6	74.125.130.188	49743	443	TCP (6)	201	0.023	N/A	-	31279	9255

Protocoles de routage

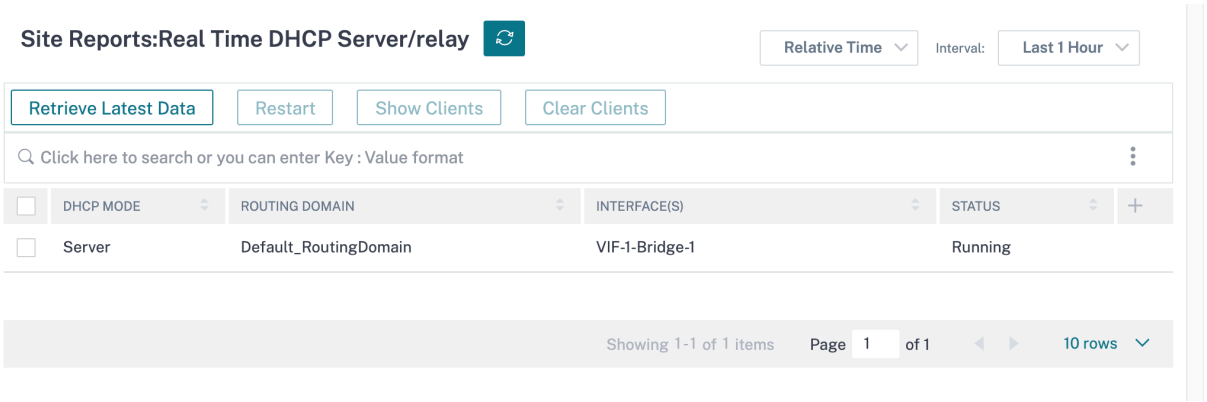
Le rapport sur les protocoles de routage fournit les détails des paramètres associés aux protocoles de routage. Choisissez un protocole dans la liste déroulante **Afficher** et un domaine de routage dans la liste déroulante **Domaine de routage** . Cliquez sur **Récupérer les dernières données** pour afficher les données actuelles.

Vous pouvez consulter les détails des paramètres associés aux éléments suivants :

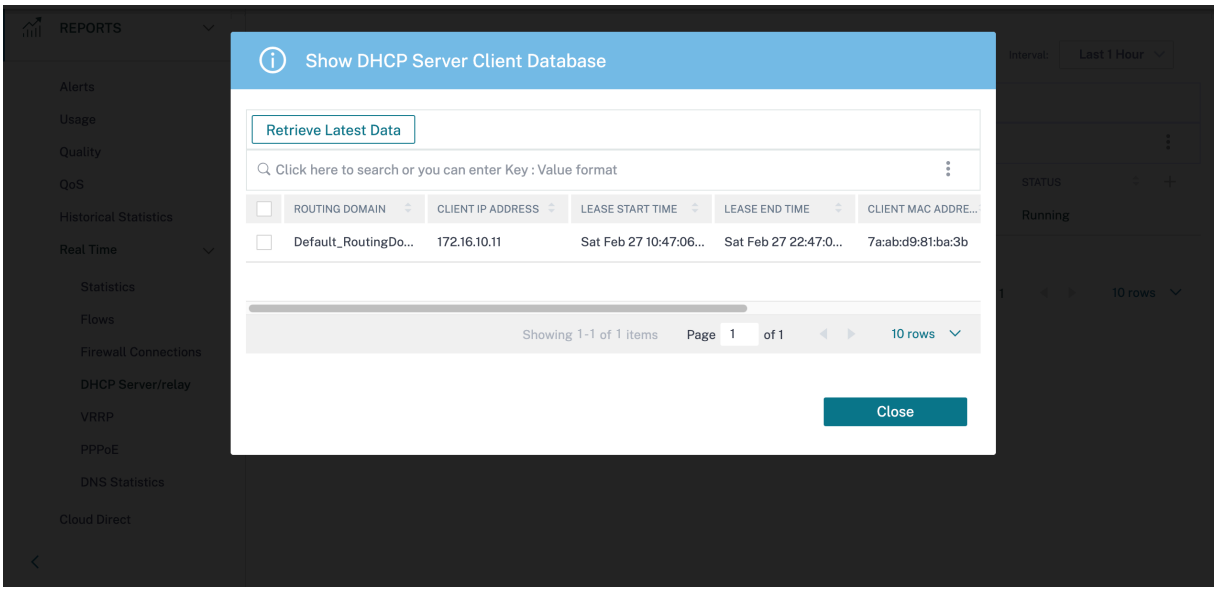
- État du BGP
- État OSPF
- Topologie OSPF
- Interface OSPF
- OSPF LSADB
- voisins OSPF
- Tableau des itinéraires

Serveur et relais DHCP

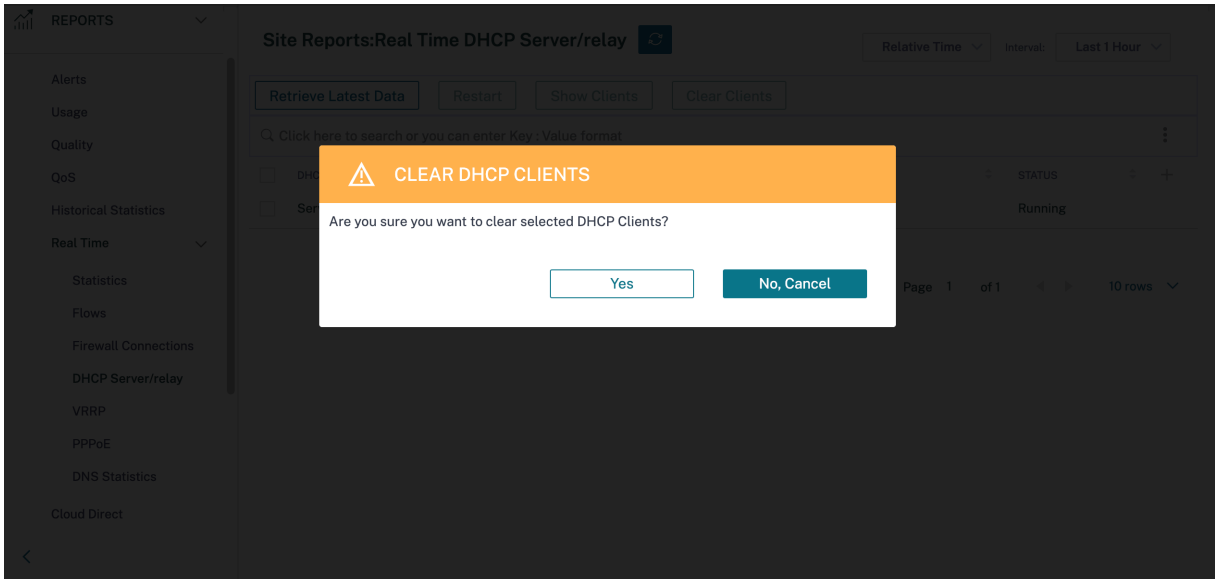
Le rapport **Serveur/Relais DHCP** fournit des informations sur les interfaces configurées en tant que serveur ou relais DHCP, ainsi que sur le domaine et l'état de routage associés. Vous pouvez rechercher les informations de serveur ou de relais DHCP requises à l'aide du format **Key : Value** .



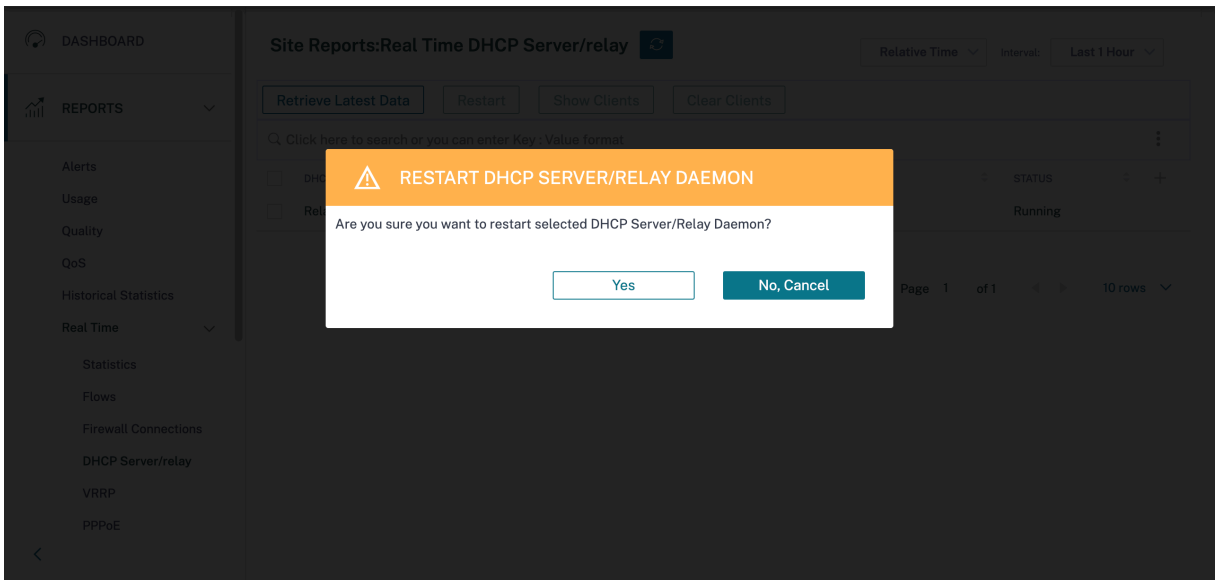
Si le mode est **Serveur**, vous pouvez cliquer sur **Afficher les clients** et afficher la liste des clients DHCP associés au serveur DHCP.



Cliquez sur **Effacer les clients** pour supprimer les clients DHCP actuellement associés au serveur DHCP.



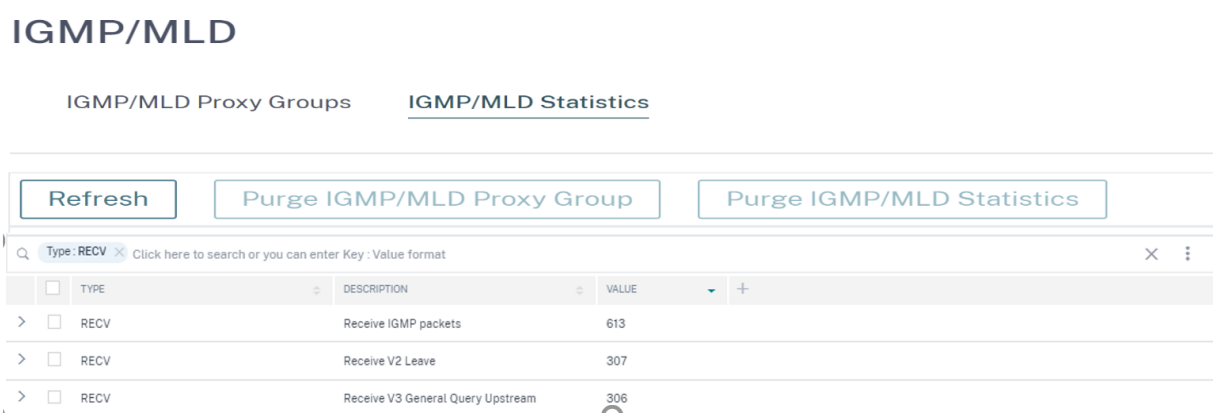
Cliquez sur **Redémarrer** pour redémarrer le serveur ou le relais DHCP.



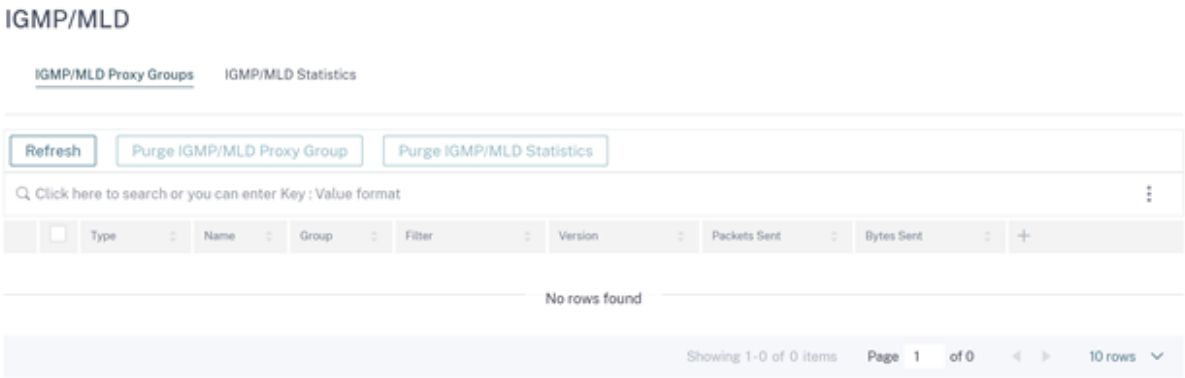
IGMP/MLD

Lorsque les récepteurs de multidiffusion lancent une demande de jointure de groupe, vous pouvez consulter les détails du récepteur sous **Rapports** > **Temps réel** > **IGMP/MLD** > **Statistiques IGMP/MLD**. Vous pouvez consulter ces informations à la fois à la source et à la destination. Cliquez sur **Actualiser** pour obtenir les données actuelles.

L'image suivante montre que les paquets IGMP reçus et le type de filtre RECV sont utilisés pour inclure les paquets de réception IGMP.



Pour afficher les détails des groupes proxy IGMP, accédez à **Rapports** > **Temps réel** > **IGMP/MLD** > **Groupes proxy IGMP/MLD**. Cliquez sur **Actualiser** pour obtenir les données actuelles.

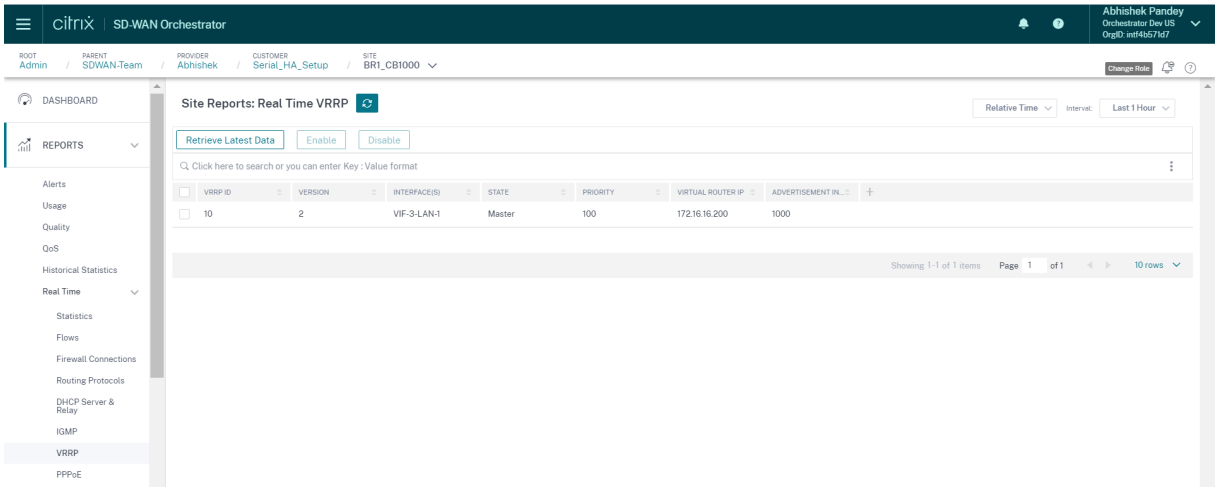


Sélectionnez **Purger les statistiques IGMP/MLD** pour supprimer les données statistiques IGMP du tableau des statistiques IGMP.

Sélectionnez **Purger les groupes IGMP/MLD** pour supprimer les données des groupes IGMP du tableau des groupes IGMP.

VRRP

Le rapport VRRP en temps réel fournit des détails sur les groupes VRRP configurés.
Pour consulter le rapport Virtual Router Redundancy Protocol (VRRP), accédez à **Rapports** > **Temps réel** > **VRRP**. Cliquez sur **Récupérer les dernières données** pour obtenir les données actuelles.



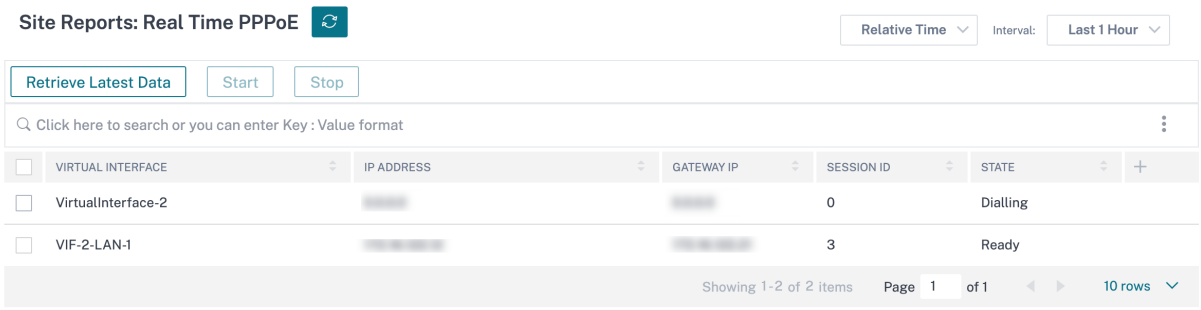
PPPoE

Le rapport PPPoE fournit des informations sur l'état de l'interface virtuelle configurée avec le mode client statique ou dynamique PPPoE. Il vous permet de démarrer ou d'arrêter manuellement les sessions à des fins de dépannage.

- **Interface virtuelle** : interface virtuelle associée au PPPoE.
- **Adresse IP** : adresse IP associée à l'interface virtuelle. Si l'interface virtuelle est prête, affiche les valeurs récemment reçues. Si l'interface virtuelle est arrêtée ou en panne, affiche les dernières valeurs reçues.
- **IP de la passerelle** : adresse IP associée à la passerelle. Si l'interface virtuelle est prête, affiche les valeurs récemment reçues. Si l'interface virtuelle est arrêtée ou en panne, affiche les dernières valeurs reçues.
- **ID de session** : identifiant unique associé à la session PPPoE.
- **État** : La colonne **État** affiche l'état de la session PPPoE. Le tableau suivant décrit les états et les descriptions.

Type de session PPPoE	Description
Configuré	Un VNI est configuré avec PPPoE. C'est un état initial.
Numérotation	Une fois qu'un VNI est configuré, l'état de la session PPPoE passe à l'état de numérotation en démarrant la découverte PPPoE. Les informations sur les paquets sont capturées.

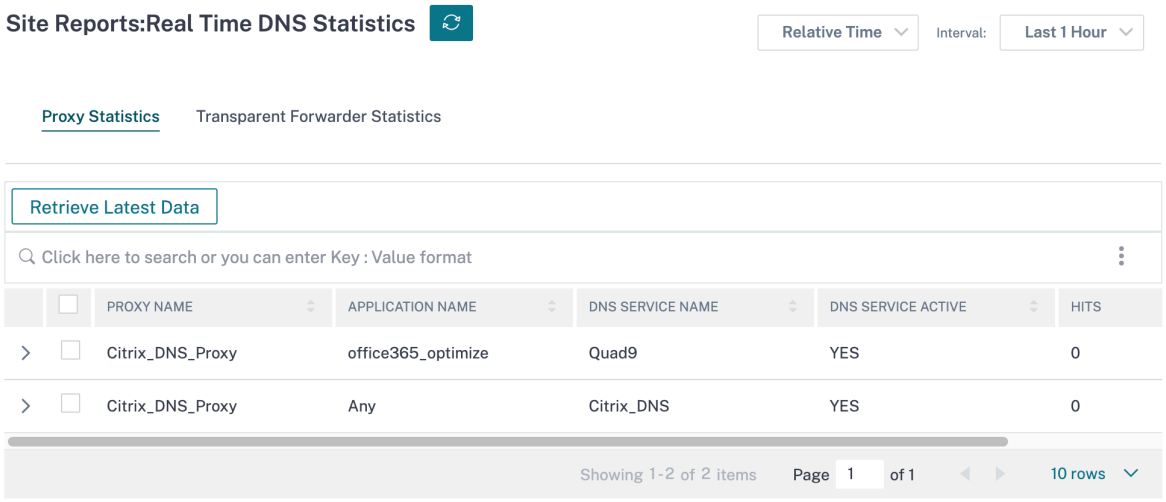
Type de session PPPoE	Description
La	Le VNI passe de l'état de découverte à l'état de session, en attendant de recevoir une adresse IP, s'il est dynamique, ou en attente d'un accusé de réception du serveur pour l'adresse IP annoncée, si elle est statique.
Prêt	Les paquets IP sont reçus et VNI et le lien WAN associé sont prêts à l'emploi.
Échec	La session PPP/PPPoE est terminée. La raison de l'échec peut être due à une configuration non valide ou à une erreur fatale. La session tente de se reconnecter après 30 secondes.
Arrêté	La session PPP/PPPoE est arrêtée manuellement.
Terminer	Un état intermédiaire se terminant pour une raison. Cet état démarre automatiquement après une certaine durée (5 secondes pour une erreur normale ou 30 secondes pour une erreur fatale).
Désactivé	Le service SD-WAN est désactivé.



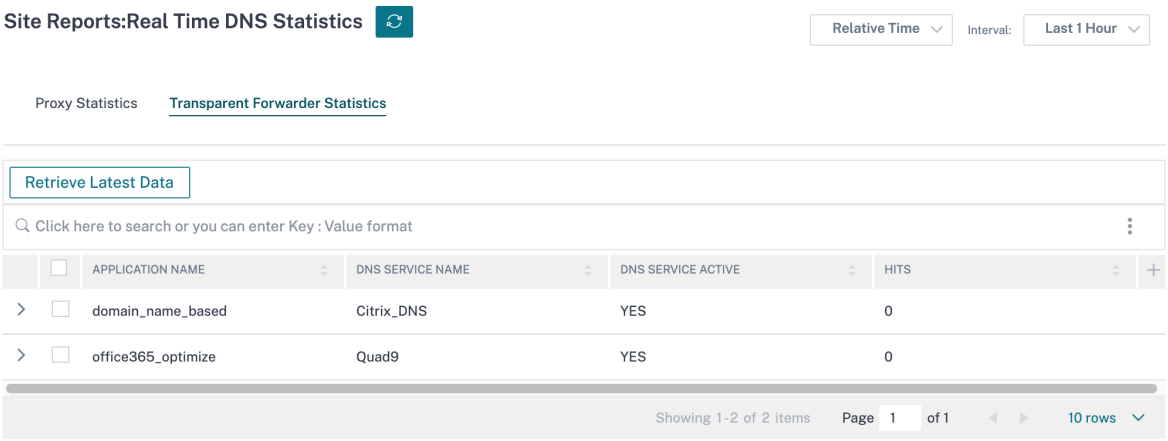
Statistiques DNS

Les **statistiques DNS** fournissent des informations sur le nom de l'application, le nom du service DNS, l'état du service DNS et le montant du `hits` service DNS. Les informations relatives au proxy DNS et au redirecteur transparent DNS sont affichées sur deux onglets différents.

Statistiques de proxy



Statistiques transparentes du transitaire



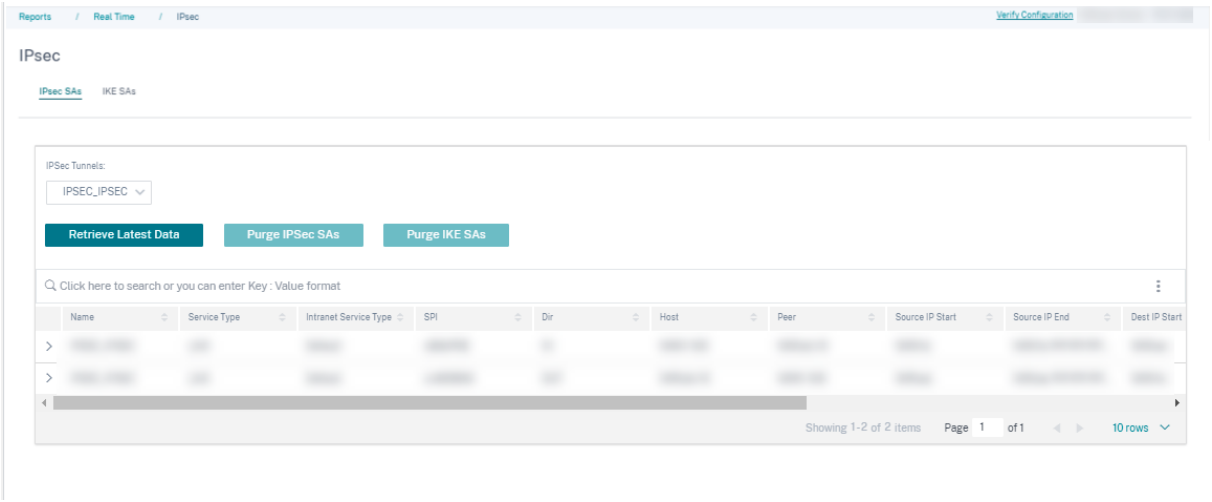
IPSec

Le rapport IPsec en temps réel fournit des détails sur les paramètres du tunnel IPsec sur votre réseau.

Pour afficher des informations détaillées sur les associations de sécurité IPsec (IPsec SA), accédez à **Rapports** > **Temps réel** > **IPsec** > **IPsec SA**. Cliquez sur **Récupérer les dernières données** pour obtenir les données actuelles.

Pour afficher les détails des associations de sécurité d'échange de clés Internet (IKE SA), accédez à **Rapports** > **Temps réel** > **IPsec** > **IKE SA**. Cliquez sur **Récupérer les dernières données** pour obtenir les données actuelles.

Vous pouvez également purger les données du groupe IPsec et les données statistiques en sélectionnant respectivement **Purger le groupe IPsec** et **Purger les statistiques IKE** .

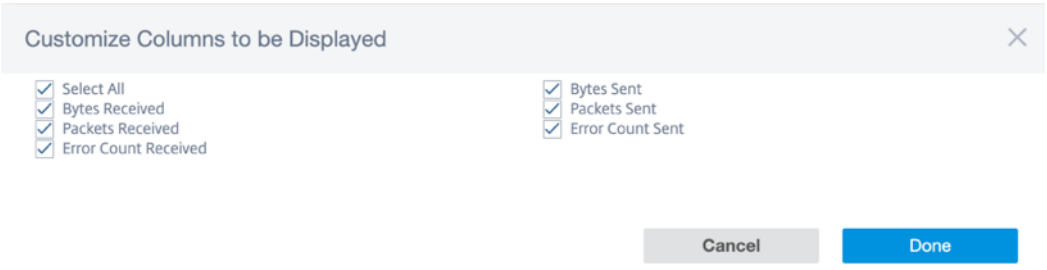


Rapports sur l'appliance (Aperçu)

Les rapports sur l'appliance fournissent le trafic réseau et les rapports d'utilisation du système. À l'aide de ces données, vous pouvez résoudre les problèmes réseau ou analyser le comportement de vos périphériques Citrix SD-WAN. Vous pouvez voir les onglets suivants sous la page Rapports sur le matériel :

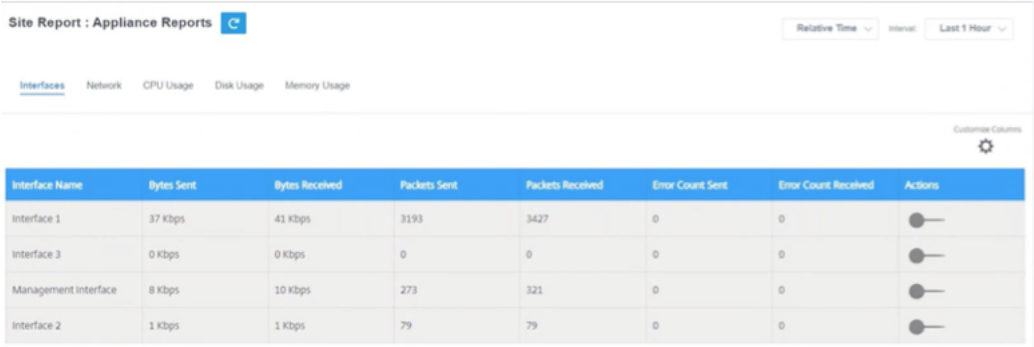
- Interface
- Réseau
- Utilisation du processeur
- Utilisation du disque
- Utilisation de mémoire

Cliquez sur chaque onglet pour afficher ou surveiller le graphique de l'appliance par heure, jour, hebdomadaire et mensuel. Vous pouvez basculer entre le temps absolu et le temps relatif selon vos besoins. Les colonnes du tableau sont personnalisables. Cliquez sur **Personnaliser** la colonne dans le coin supérieur droit du tableau et sélectionnez/désélectionnez les options que vous souhaitez afficher ou masquer dans le tableau.



Interface

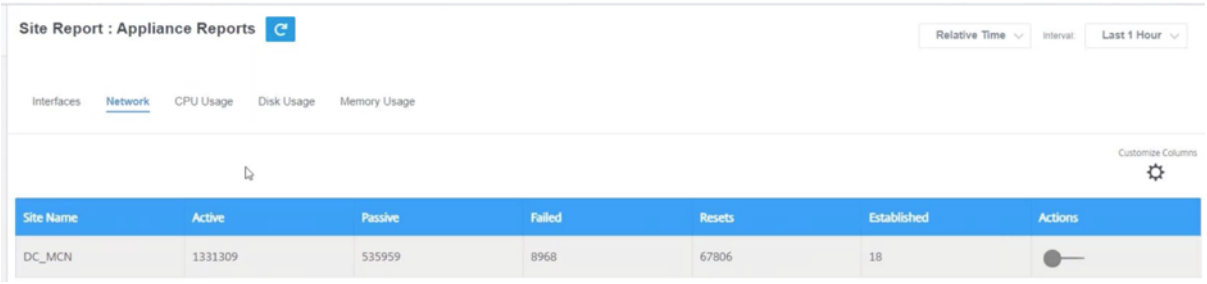
La page **Interface** affiche les erreurs/le trafic de l'interface de gestion. Tout le réseau est divisé en interface différente, telle que l'interface de gestion, l'interface 1/2/3.



- **Nom de l'interface** —Affiche le nom de l'interface.
- **Octets envoyés** : nombre moyen d'octets envoyés pendant la durée sélectionnée, en Kbits/s.
- **Octets reçus** : nombre moyen d'octets reçus pendant la durée sélectionnée, en Kbits/s.
- **Paquets envoyés** —Nombre moyen de paquets envoyés pendant la durée sélectionnée.
- **Paquets reçus** —Nombre moyen de paquets reçus pendant la durée sélectionnée.
- **Nombre d'erreurs envoyées** : nombre d'erreurs envoyées pendant la durée sélectionnée.
- **Nombre d'erreurs reçues** : nombre d'erreurs reçues pendant la durée sélectionnée.
- **Actions** —Vous pouvez activer le bouton d'action pour afficher le graphe du réseau.

Réseau

La page **Réseau** indique le nombre de connexions TCP pour chaque site configuré.



- **Nom du site** —Affiche le nom du site.
- **Actif** : nombre moyen de connexions TCP actives pendant la durée sélectionnée.
- **Passif** —Nombre moyen de connexions TCP passives pour la durée sélectionnée.
- **Échec** : nombre moyen de connexions TCP ayant échoué pendant la durée sélectionnée.
- **Réinitialisations** : nombre moyen de connexions TCP réinitialisées pour la durée sélectionnée.
- **Établi** : nombre moyen de connexions TCP établies pour la durée sélectionnée.
- **Actions** —Vous pouvez activer le bouton d'action pour afficher le graphe du réseau.

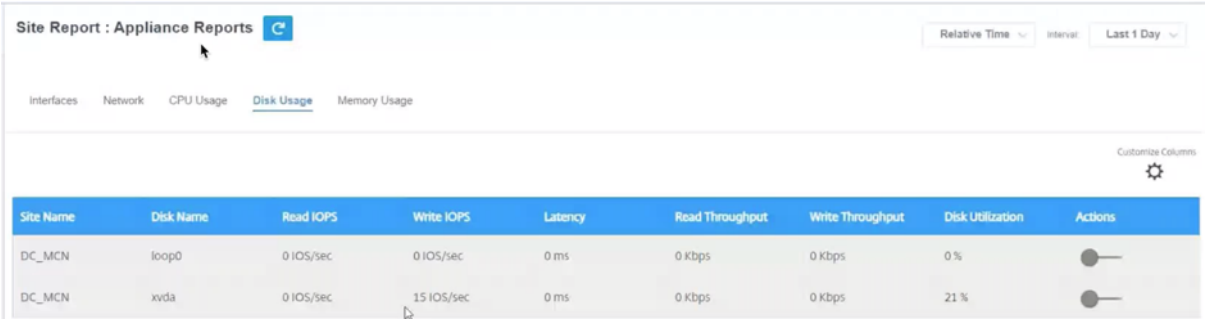
Utilisation UC

La page **Utilisation du processeur** affiche l'utilisation du processeur du périphérique SD-WAN sous forme de pourcentage. Le graphique CPU montre la consommation moyenne de CPU pour les intervalles réguliers sur le temps sélectionné.

- **Nom du site** —Affiche le nom du site.
- **Système** : pourcentage du temps total passé par le processeur à traiter les programmes de l'espace système.
- **Utilisateurs** : pourcentage du temps total passé par le processeur à traiter les programmes de l'espace utilisateur.
- **Nice** —C'est bien lorsque le processeur exécute une tâche utilisateur dont la priorité est inférieure à la normale.
- **Inactif** : pourcentage du temps total pendant lequel le processeur est resté en mode inactif.
- **Io Wait** : pourcentage du temps total passé par le processeur à attendre les opérations d'E/S.
- **Irq** —La valeur des demandes d'interruption (IRQ) que le noyau sert.
- **Vol** : lorsqu'il fonctionne dans un environnement virtualisé, l'hyperviseur peut voler les cycles destinés à vos processeurs et les transmettre à un autre, pour diverses raisons. Ce processus est connu comme voler.
- **Actions** —Vous pouvez activer le bouton d'action pour afficher le graphe du réseau.

Utilisation du disque

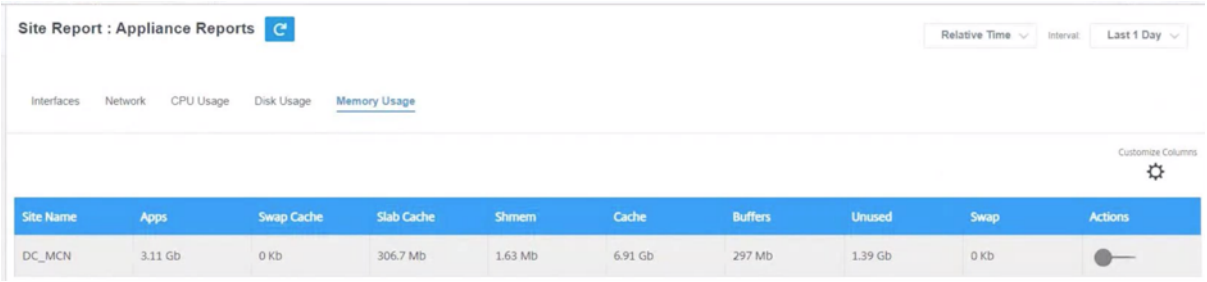
La page **Utilisation du disque** indique la quantité d'espace disque utilisée par le système d'exploitation et la partition de données sous la forme d'une valeur d'E/S par seconde (IOPS).



- **Nom du site** —Affiche le nom du site.
- **Nom du disque** —Affiche le nom du disque dur.
- **IOPS en lecture** —Affiche le nombre moyen d'IOPS de lecture par seconde sur la période sélectionnée.
- **IOPS d'écriture** —Affiche le nombre moyen d'IOPS d'écriture par seconde sur la période sélectionnée.
- **Latence** —Affiche la valeur de latence des demandes de lecture et d'écriture réussies provenant de la charge de travail du volume sélectionné sur la période sélectionnée. Il est recommandé que la valeur de latence inférieure à 10 ms soit la meilleure pour les performances d'E/S.
- **Débit de lecture** —Affiche la valeur moyenne du débit disque de l'opération de lecture du disque sur la durée sélectionnée, en Kbits/s.
- **Débit d'écriture** —Affiche la valeur moyenne du débit disque de l'opération d'écriture sur disque pendant la durée sélectionnée en Kbits/s.
- **Utilisation du disque** —Affiche la valeur moyenne d'utilisation du disque en pourcentage sur la période sélectionnée.
- **Actions** —Vous pouvez activer le bouton d'action pour afficher le graphe du réseau.

Utilisation de mémoire

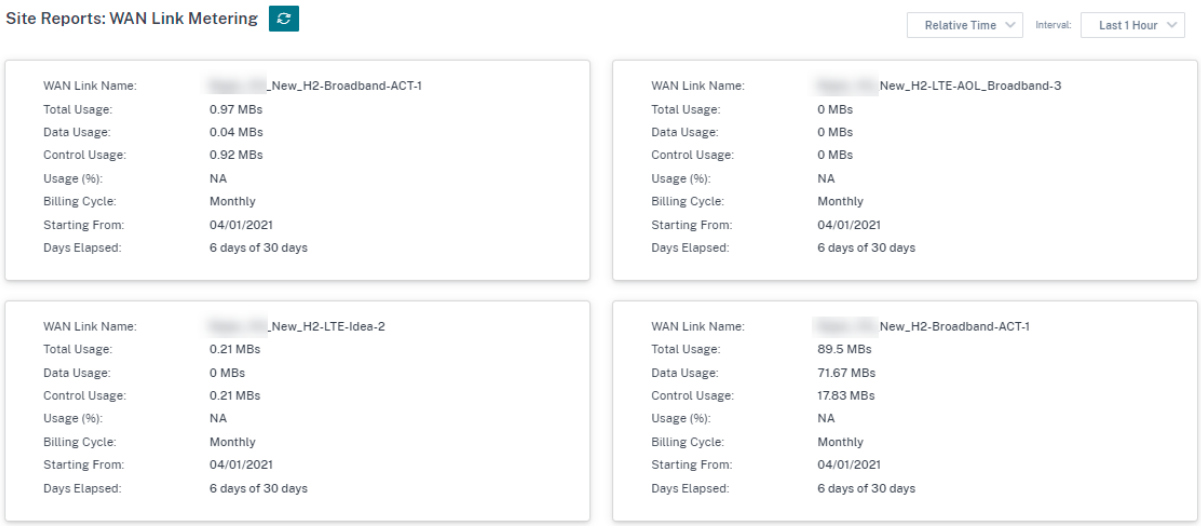
La page **Utilisation de la mémoire** affiche le rapport sur la quantité de mémoire utilisée.



- **Nom du site** —Affiche le nom du site.
- **Applications** : affiche la valeur de l'application utilisée en Go.
- **Cache d'échange** —Affiche le numéro du cache d'échange en Mo. Le cache d'échange est une liste d'entrées de table de pages avec une entrée par page physique.
- **Cache de dalles** —Affiche le nombre de tranches de mémoire pré-allouées. En Mo
- **Shmem** —Affiche la valeur totale de la mémoire partagée utilisée en Mo.
- **Cache** —Affiche le nombre de mémoires cache utilisées en Go.
- **Buffers** : affiche le numéro de la mémoire physique utilisée par le cache de la mémoire tampon.
- **Non utilisé** —Affiche le nombre de mémoires non utilisées pour le cache.
- **Swap** —Affiche le nombre d'espaces de permutation. L'espace d'échange est utilisé si vous avez besoin d'une extension d'espace pour votre mémoire physique.
- **Actions** —Vous pouvez activer le bouton d'action pour afficher le graphe du réseau.

Comptage des liaisons WAN

Les rapports de mesure des liaisons WAN fournissent des détails sur l'utilisation des liaisons WAN mesurées. Vous pouvez consulter les rapports pour obtenir des informations sur la consommation de données des liaisons WAN mesurées. Pour consulter les rapports de mesure des liaisons WAN, accédez à **Rapports > Comptage des liaisons WAN**.

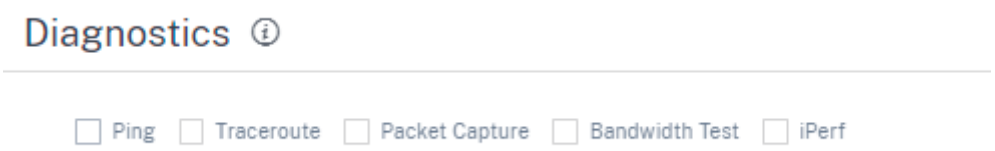


Diagnostics

October 21, 2022

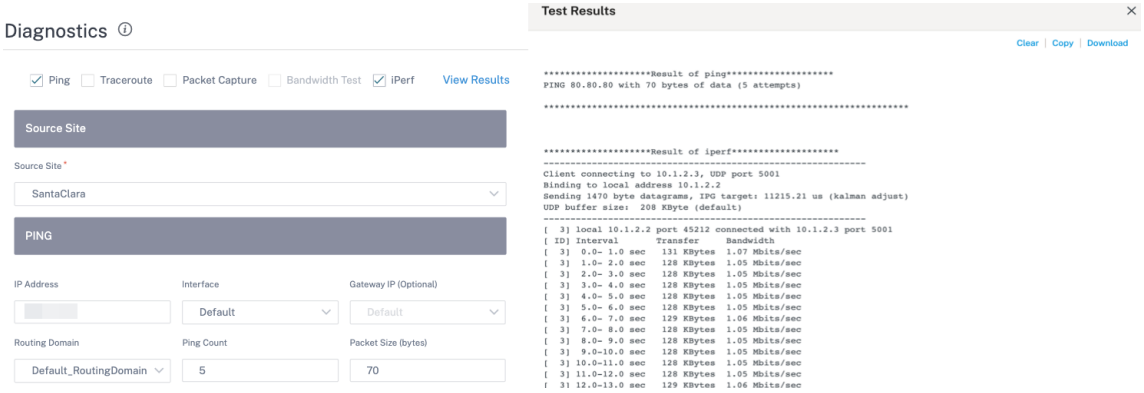
Vous pouvez utiliser les utilitaires de diagnostic Ping, Traceroute, Packet Capture, Bandwidth Test et iPerf pour tester et étudier les problèmes de connectivité réseau sur votre réseau SD-WAN. Pour afficher la page Diagnostics, accédez à **Résolution des problèmes** > **Diagnostics**.

Pour afficher les résultats des diagnostics, cliquez sur **Afficher les résultats** dans le coin supérieur droit de la page Diagnostics. Vous pouvez **télécharger**, **copier**et **effacer** les résultats du rapport selon vos besoins.

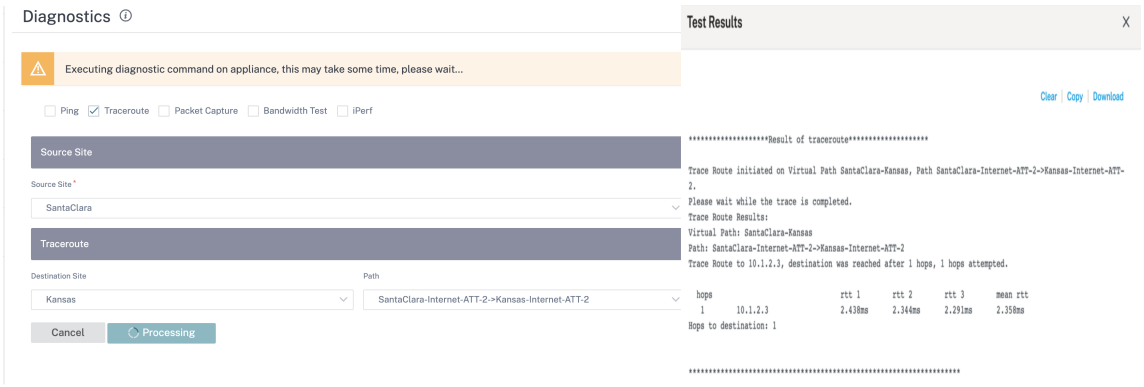


- **Ping** : vous pouvez vérifier la connectivité réseau en envoyant un ping à un hôte distant ou à un site. Entrez les détails de destination, spécifiez le nombre de fois où la demande ping doit être

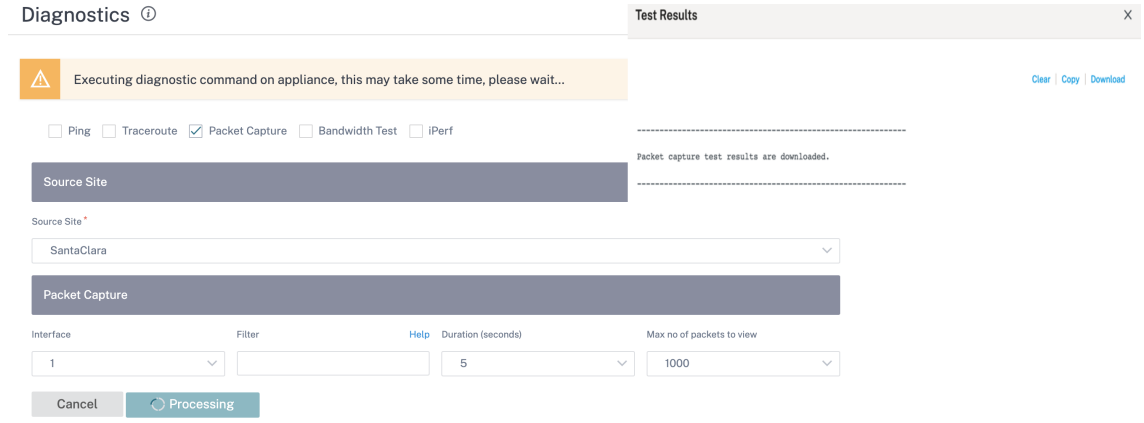
envoyée et le nombre d'octets de données. Fournissez l'**adresse IP** de destination et cliquez sur **Exécuter**.



- **Traceroute** - Vous pouvez suivre l'itinéraire et le nombre de sauts entre les sites. Sélectionnez le site source et de destination ainsi que le chemin à tracer, puis cliquez sur **Exécuter**.



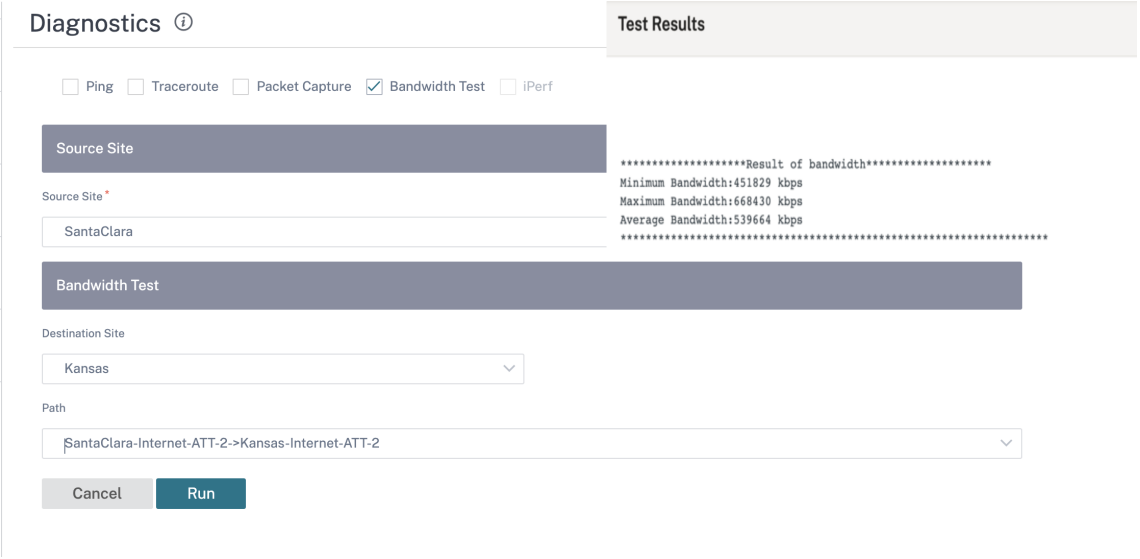
- **Capture de paquets** —Vous pouvez intercepter le paquet de données qui traverse l'interface active sélectionnée présente sur le site sélectionné. Vous pouvez afficher les détails de la source et de la destination.



L'option **Aide** fournit plus de détails sur les **options de filtre**.

- **Test de bande passante** : vous pouvez exécuter un test de bande passante sur un chemin

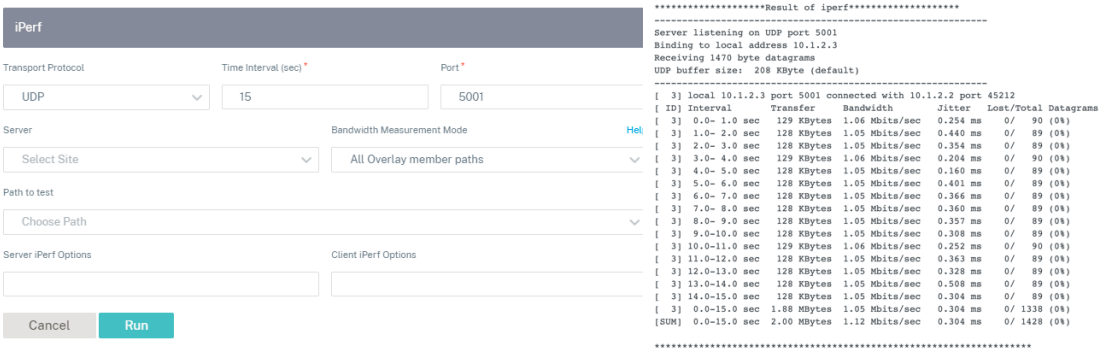
spécifique d'un site afin de visualiser l'utilisation maximale, minimale et moyenne de la bande passante. Entrez le site source, le site de destination et sélectionnez le chemin d'accès. Cliquez sur **Exécuter**.



- **iPerf** —Vous pouvez exécuter un test iPerf sur un chemin spécifique d'un site. L'outil de diagnostic iPerf est utilisé pour générer du trafic de test qui vous permet de résoudre les problèmes réseau susceptibles d'entraîner :

  - Changement fréquent de l'état de la trajectoire, passant de bon à mauvais
  - Faibles performances des applications
  - Perte de paquets plus élevée

  Pour exécuter un test de diagnostic iPerf, au niveau du client, accédez à **Résolution des problèmes** > **Diagnostics** et cochez la case **iPerf** . Entrez le protocole de transport, l'intervalle de temps, le numéro de port, le serveur, le mode de mesure de la bande passante, le chemin à tester, les options iPerf du serveur, puis cliquez sur **Exécuter**.

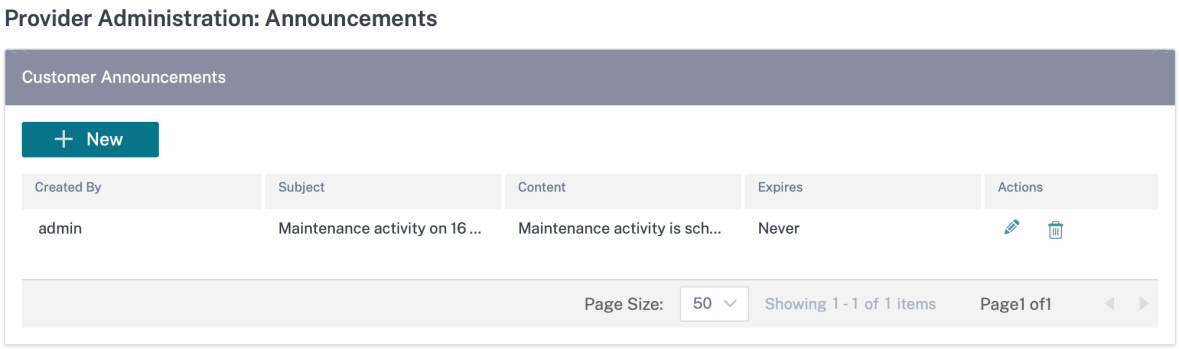


Annonces

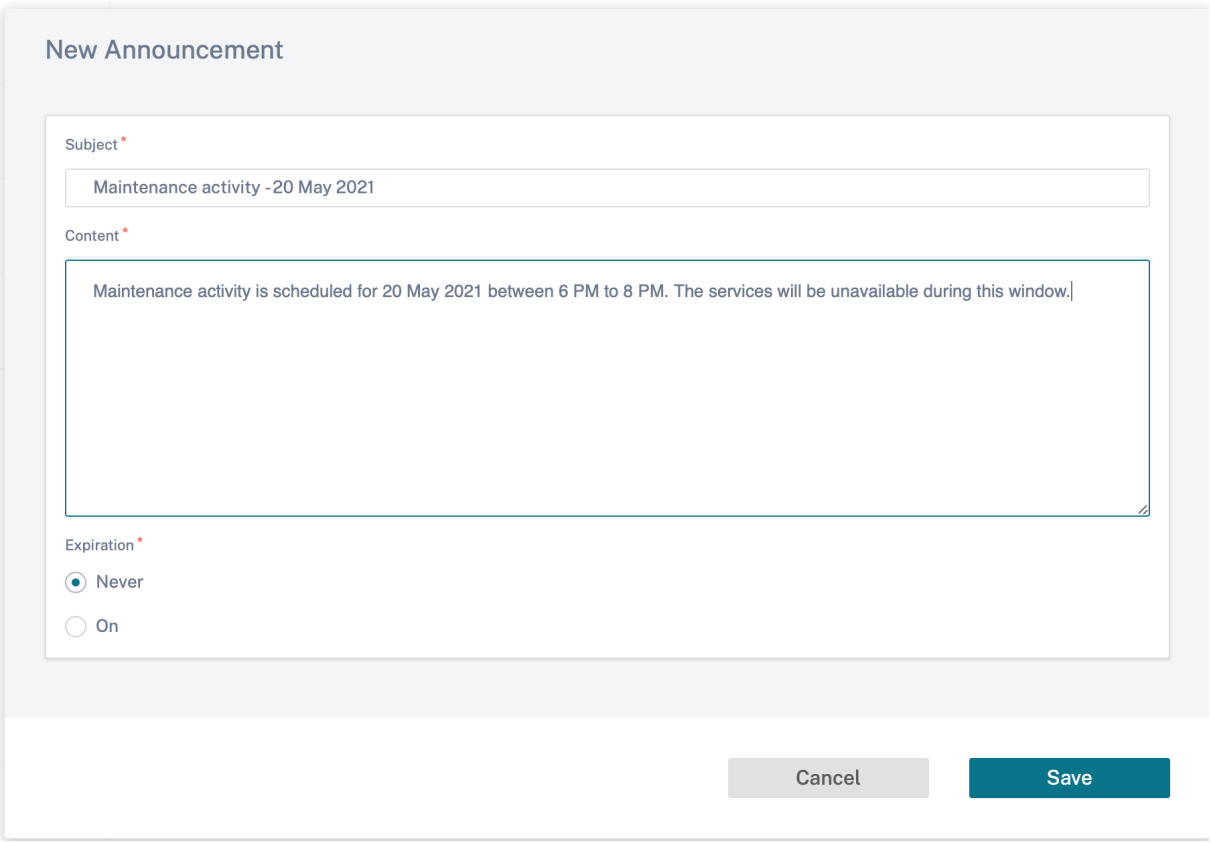
October 21, 2022

Les fournisseurs peuvent utiliser l'option **Annonces** pour envoyer des annonces ou des notifications à leurs clients.

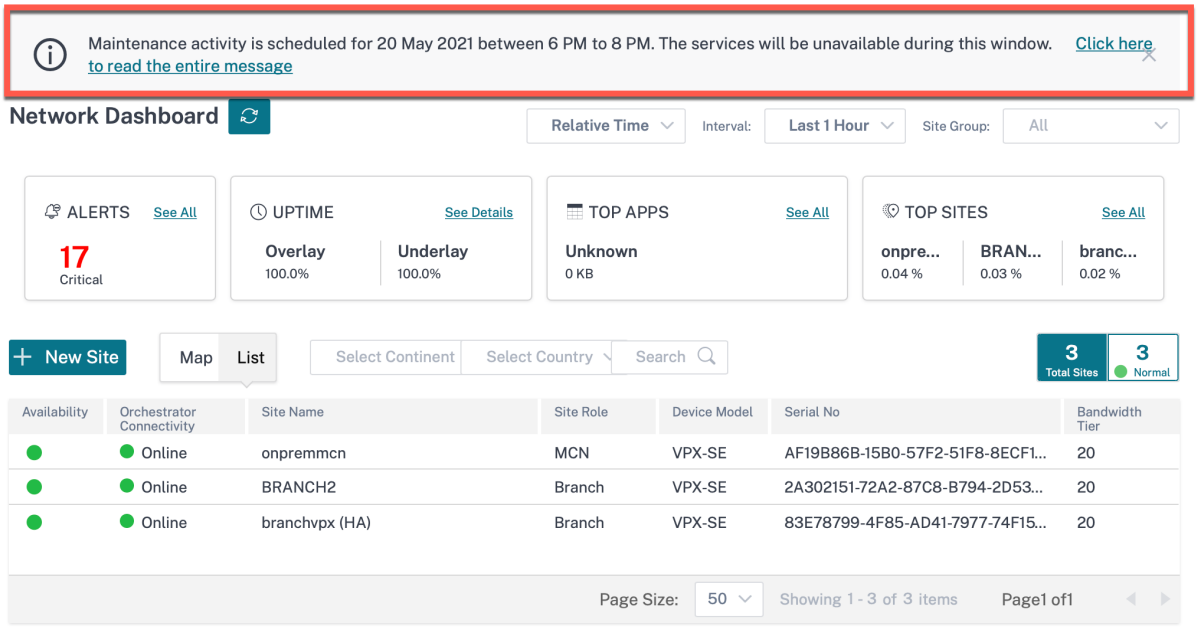
Vous pouvez créer une annonce de fournisseur en accédant à **Administration > Annonces** et en cliquant sur l'option **+ Nouveau** .



Fournissez une ligne d'objet et entrez le contenu au format HTML ou texte brut. Vous pouvez également définir l'expiration de l'annonce.



Les annonces enregistrées sont affichées à tous les clients.



Administration des utilisateurs

October 2, 2024

Citrix SD-WAN Orchestrator pour locaux prend en charge le contrôle d'accès basé sur les rôles (RBAC). Le RBAC régule l'accès aux ressources du SD-WAN Orchestrator en fonction des rôles assignés aux utilisateurs individuels. RBAC permet aux utilisateurs d'accéder uniquement aux données exigées par leur rôle et restreint toute autre donnée.

Un rôle définit les autorisations permettant d'afficher et d'effectuer diverses activités sur Citrix SD-WAN Orchestrator pour locaux. Vous pouvez attribuer un rôle à un utilisateur dans la liste des rôles prédéfinis.

Par défaut, un compte utilisateur est créé sur Citrix SD-WAN Orchestrator for On-premises avec le nom d'utilisateur **admin** et le mot de passe définis comme **mot de passe**. L'utilisateur est invité à modifier le mot de passe par défaut lors de la connexion initiale.

Vous pouvez ajouter des utilisateurs qui peuvent être authentifiés localement et à distance. Les utilisateurs authentifiés à distance sont authentifiés via des serveurs d'authentification RADIUS ou TACACS+.

Rôles fournisseur

Le tableau suivant répertorie les rôles de fournisseur prédéfinis.

Rôle du fournisseur	Description
Provider-Master-Admin-All	Un administrateur capable de gérer le fournisseur et toutes ses informations clients
Provider-Master-Admin-Tenant	Un administrateur capable de gérer le fournisseur et un sous-ensemble de ses informations clients
Provider-Master-ReadOnly-All	Un administrateur qui ne peut consulter que les informations sur les fournisseurs et les clients
Provider-Network-Admin (version préliminaire)	Un administrateur qui peut uniquement consulter et modifier les informations relatives au réseau
Provider-Security-Admin (version préliminaire)	Un administrateur qui peut uniquement consulter et modifier les informations relatives à la sécurité

Le rôle **Provider-Master-Admin-All** peut effectuer les opérations suivantes :

- Attribuer des rôles aux utilisateurs dans le réseau Fournisseur et Client
- Gérer l'accès aux clients pour tous les autres rôles d'administrateur
- Modifier ou supprimer des rôles attribués

Rôles des clients

Le tableau suivant répertorie les rôles clients prédéfinis :

Rôle	Description
Customer-Master-Admin	Un administrateur client qui peut consulter et modifier les informations des clients
Customer-Master-readonly-Admin	Un administrateur client qui ne peut consulter que les informations des clients
Clients-Network-Admin (version préliminaire)	Un administrateur client qui peut uniquement consulter et modifier les informations relatives au réseau
Customer-Security-Admin (version préliminaire)	Un administrateur client qui peut uniquement consulter et modifier les informations relatives à la sécurité

Un utilisateur doté du rôle **Customer-Master-Admin** peut effectuer les opérations suivantes :

- Ajouter des utilisateurs et attribuer des rôles aux clients
- Modifier ou supprimer des rôles attribués

> **Remarque :**
>
> Il est important d'attribuer les rôles critiques (administrateur principal, administrateur de sécurité et administrateur réseau) exclusivement aux utilisateurs de confiance.

Rôles d'assistance

À des fins de résolution des problèmes, les clients peuvent attribuer des rôles d'assistance et permettre aux membres de l'équipe d'assistance de consulter et de modifier leurs informations. Les rôles de support ont une période de validité définie lors de l'attribution du rôle. Une fois la période de validité expirée, l'utilisateur du support perd l'accès aux informations du client. Toutefois, les détails de l'utilisateur du support continuent d'apparaître sous **Administration > Administration des utilisateurs**. En fonction des besoins, l'administrateur du client peut supprimer ou prolonger la validité du rôle de support.

Rôle	Description
Customer-Support-ReadWrite	Un membre de l'équipe d'assistance qui peut consulter et modifier les informations du client
Customer-Support-ReadOnly	Un membre de l'équipe d'assistance qui ne peut consulter que les informations du client

Types d'authentification

Citrix SD-WAN Orchestrator pour locaux prend en charge les types d'authentification suivants :

- **Authentification**à facteur unique : L'authentification à facteur unique présente une méthode d'authentification pour accéder à Citrix SD-WAN Orchestrator pour les utilisateurs sur site.
- **Authentification à deux facteurs (TFA)** : L'authentification à deux facteurs présente deux méthodes d'authentification pour accéder à Citrix SD-WAN Orchestrator pour les utilisateurs sur site. Il introduit un niveau de sécurité supplémentaire dans la séquence de connexion.

Les méthodes d'authentification suivantes sont prises en charge pour l'authentification à un facteur et à deux facteurs :

- **Local** : lorsque cette option est sélectionnée, l'utilisateur doit utiliser le mot de passe configuré sur Citrix SD-WAN Orchestrator pour les applications locales pour y accéder.
- **RADIUS** : lorsque cette option est sélectionnée, l'utilisateur doit utiliser le mot de passe du serveur RADIUS pour y accéder.
- **TACACS+** : Lorsque cette option est sélectionnée, les utilisateurs doivent utiliser le mot de passe du serveur TACACS+ pour y accéder.

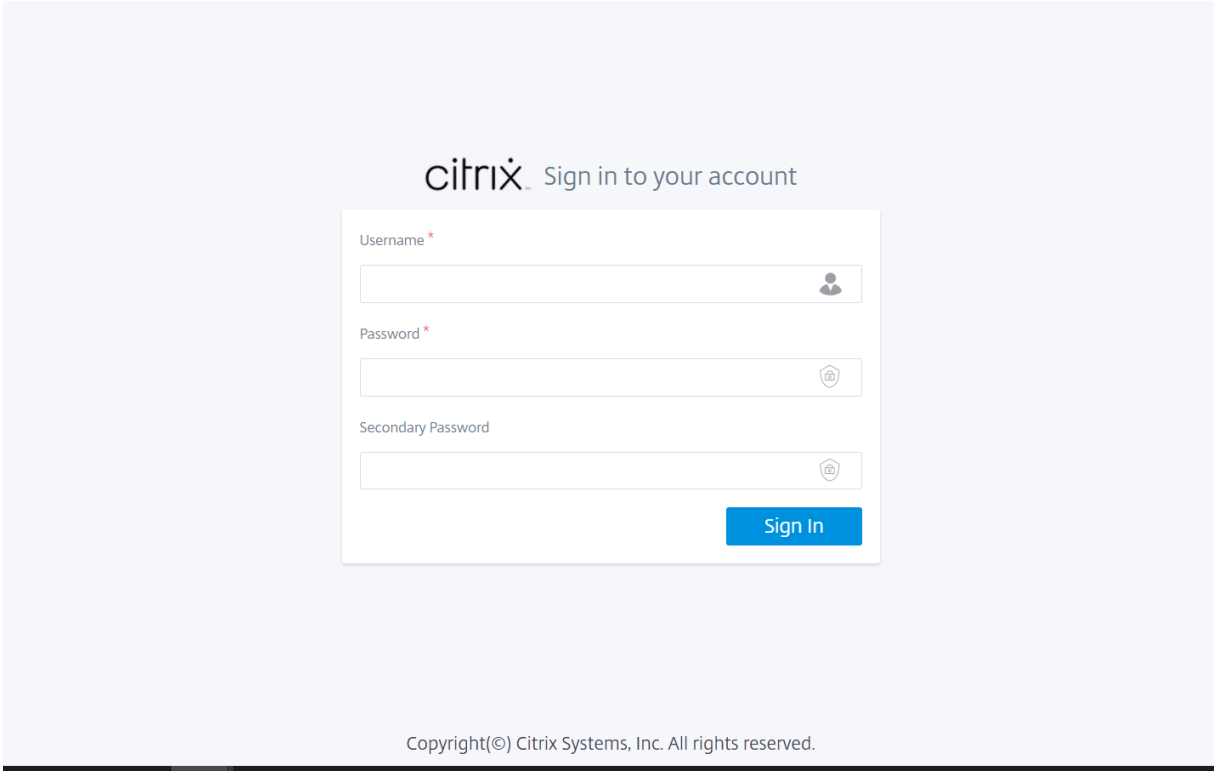
Le tableau suivant répertorie les méthodes d'authentification principales et secondaires prises en charge pour les utilisateurs authentifiés localement :

	Type d'authentification principal	Type d'authentification secondaire
authentification à facteur unique	Stockage local	-
Authentification à deux facteurs	Stockage local	RADIUS ou TACACS+

Le tableau suivant répertorie les méthodes d'authentification principales et secondaires prises en charge pour les utilisateurs authentifiés à distance :

	Type d'authentification principal	Type d'authentification secondaire
authentification à facteur unique	Local, RADIUS ou TACACS+	-
Authentification à deux facteurs	Local, RADIUS ou TACACS+	RADIUS ou TACACS+

Si **l'authentification à deux facteurs** est activée et que les serveurs RADIUS/TACACS+ sont configurés comme type d'authentification secondaire, le champ **Mot de passe secondaire** est visible sur la page de connexion.



Ajouter un utilisateur

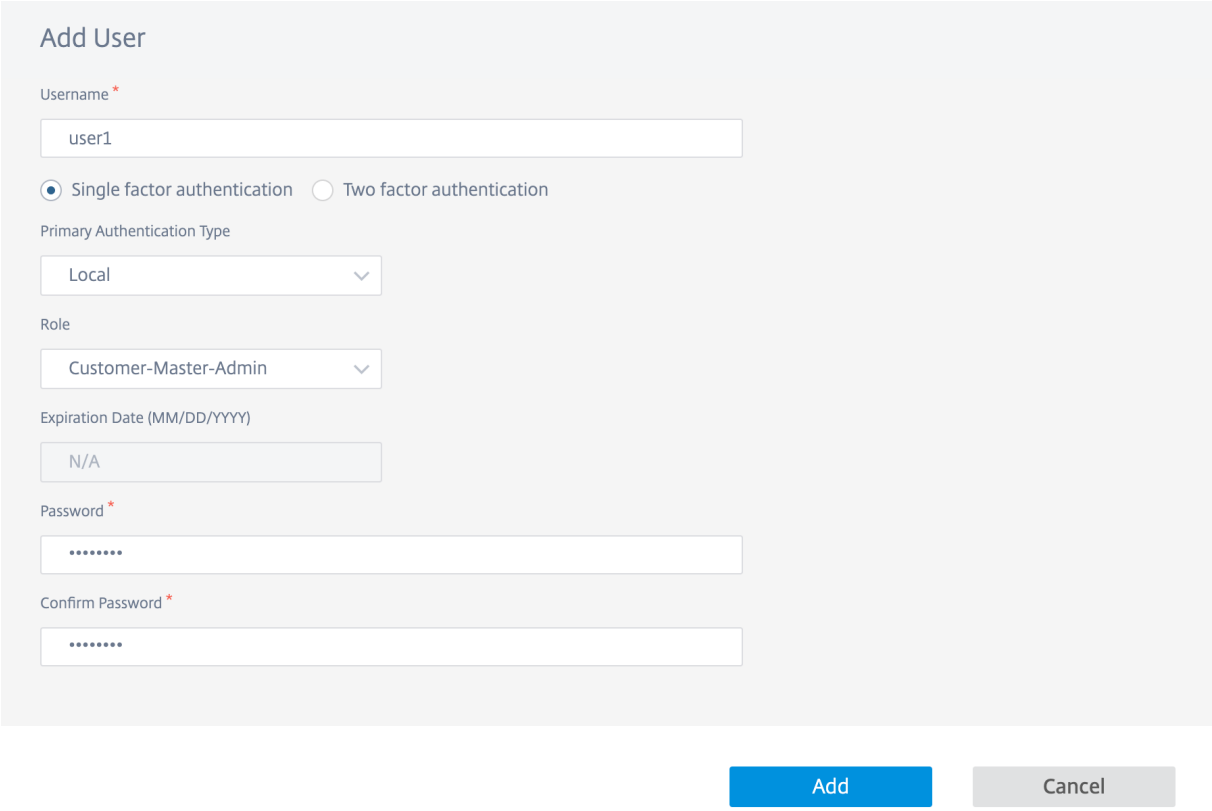
Accédez à **Administration > Administration** des **utilisateurs**, cliquez sur **+ Nouveau** > Entrez les informations suivantes, puis cliquez sur **Ajouter**.

- Entrez le nom d'utilisateur.
- **Authentification à facteur unique** : active uniquement l'authentification principale pour la connexion des utilisateurs.

- **Authentification à deux facteurs** : active l'authentification principale et secondaire pour la connexion des utilisateurs. Pour plus d'informations, voir Serveurs d'authentification à distance.
- **Type d'authentification principal** : sélectionnez Local ou l'adresse IP du serveur d'authentification distant.
- **Type d'authentification secondaire** : sélectionnez l'adresse IP du serveur d'authentification à distance.

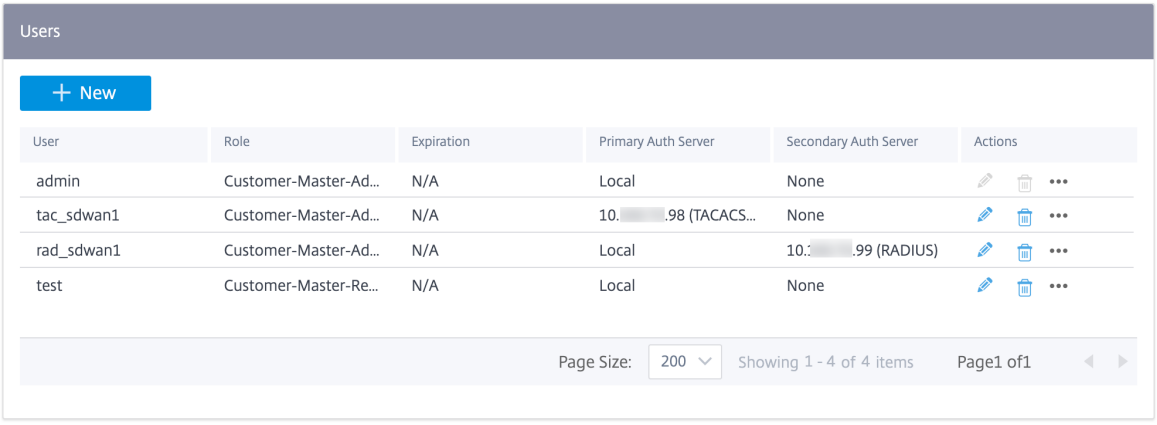
  > **NOTE**
  >
  > Le champ **Type d'authentification secondaire** est grisé si l'authentification à facteur unique est sélectionnée.

- **Rôle** : Sélectionnez un rôle dans la liste des rôles disponibles.
- **Refuser l'accès aux clients** : (Disponible uniquement au niveau du fournisseur). Lors de l'ajout d'utilisateurs, les fournisseurs peuvent refuser l'accès à des clients spécifiques.
- **Date d'expiration (MM/DD/YYYY)** : date jusqu'à laquelle l'utilisateur du support a accès aux informations du client. La période de validité par défaut est de deux semaines à compter de la date à laquelle le rôle est attribué.
- Entrez votre mot de passe. La longueur du mot de passe doit être comprise entre 8 et 128 caractères.



À l'aide de la colonne **Actions**, vous pouvez modifier le rôle de l'utilisateur, mettre à jour le mot de passe et modifier le type d'authentification. Vous pouvez également supprimer l'utilisateur si nécessaire.

Network Administration: User Administration



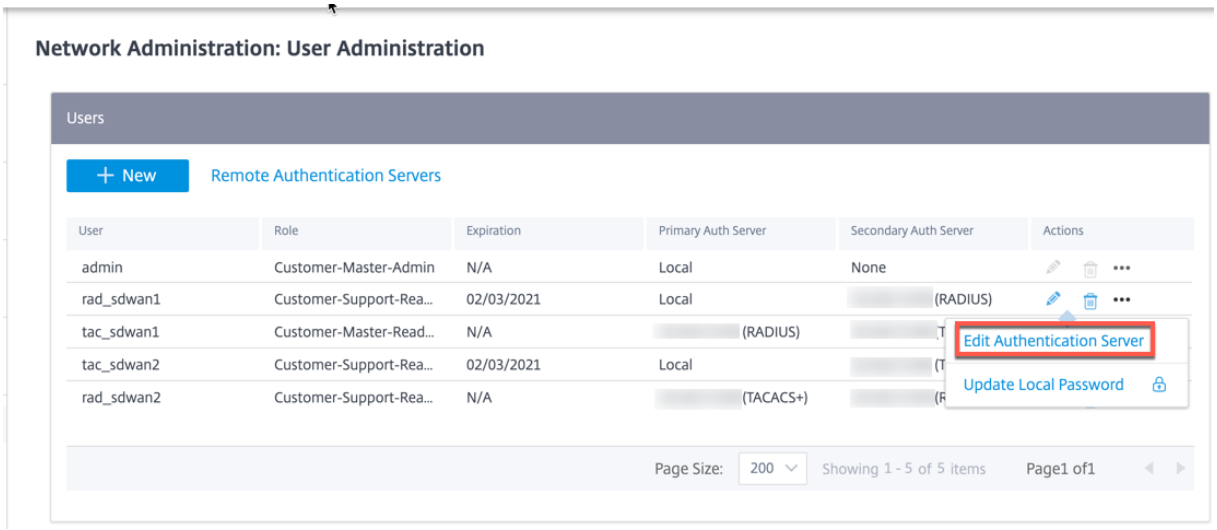
Limitation

Citrix SD-WAN Orchestrator pour locaux ne prend pas en charge la duplication des noms d'utilisateur d'un autre client auprès du même fournisseur. Lorsque cette action est effectuée, le message d'erreur Erreur lors de la **création du compte s'**affiche.

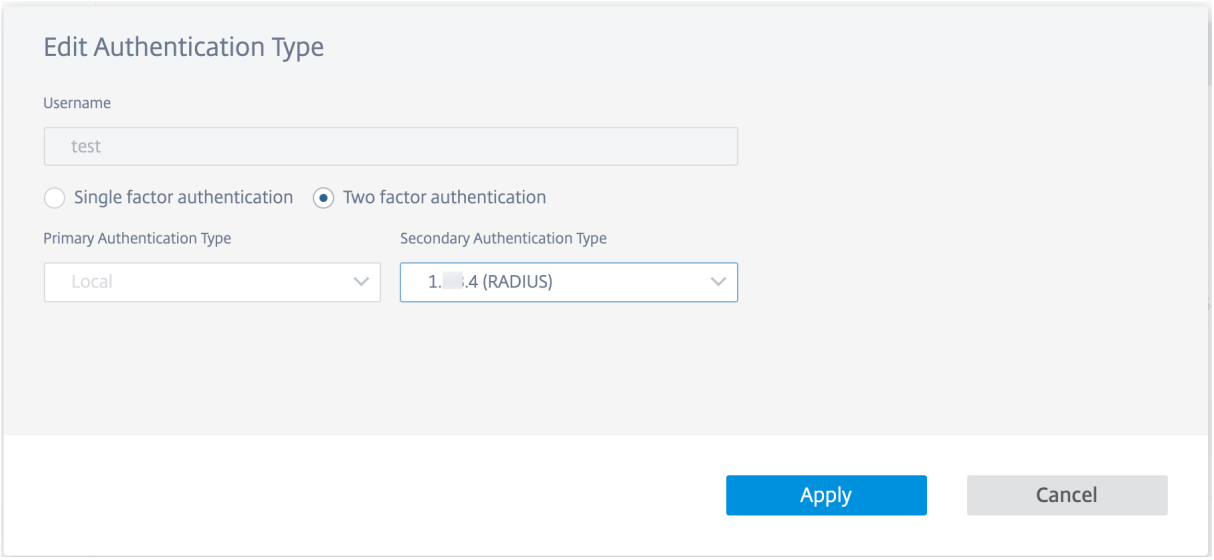
Modifier le type d'authentification

Vous pouvez modifier le type d'authentification d'un utilisateur de l'authentification à un facteur à l'authentification à deux facteurs et inversement.

Pour modifier le type d'authentification d'un utilisateur, dans la colonne **Actions**, cliquez sur **...** puis sur **Modifier le serveur d'authentification**.



Si vous avez actuellement sélectionné l'**authentification à un seul facteur**, vous pouvez passer à l'authentification à deux facteurs. Cliquez sur **Authentification à deux facteurs** et sélectionnez le serveur distant dans la liste déroulante **Type d'authentification secondaire** . Cliquez sur **Appliquer**.



Si vous avez actuellement sélectionné l'authentification à deux facteurs, vous pouvez choisir de modifier uniquement le type d'authentification secondaire ou de passer à l'authentification à facteur unique.

Pour passer à l'authentification à facteur unique, cliquez sur **Authentification à facteur unique**. La liste déroulante **Type d'authentification secondaire** est désactivée et seule la liste déroulante **Type d'authentification principal** est activée.

Le**type d'authentification principal** ne peut être défini qu'au moment de la création de l'utilisateur et ne peut pas être modifié ultérieurement.

Modifier le mot de passe

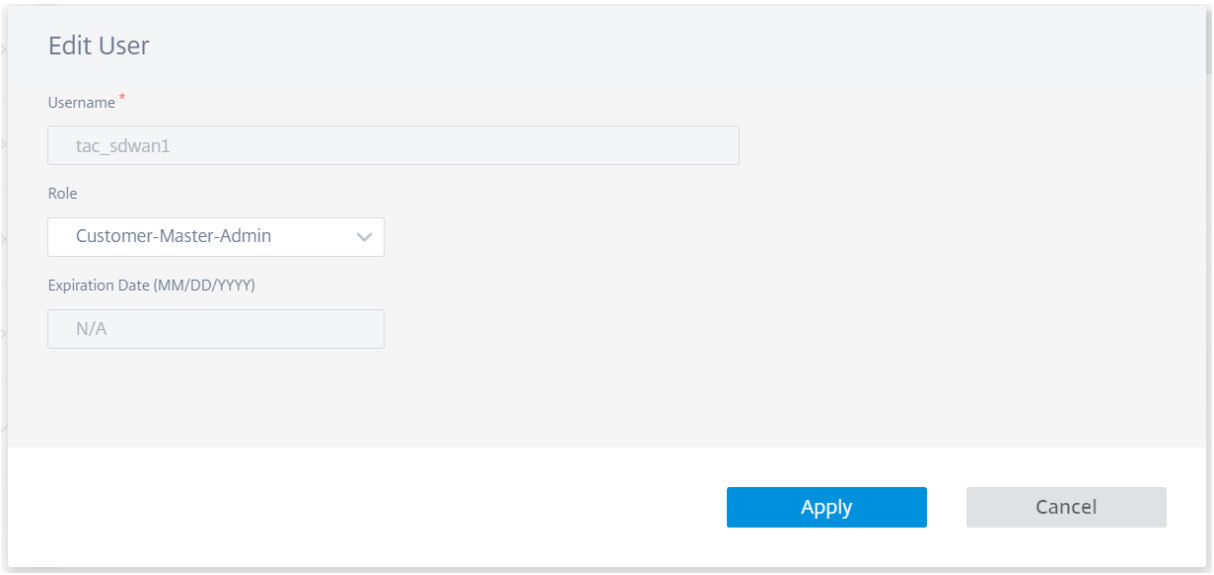
Vous pouvez modifier le mot de passe des utilisateurs locaux. Pour modifier le mot de passe d'un utilisateur, dans la colonne **Actions**, cliquez sur **...** et sur **Mettre à jour le mot de passe local**.

> **NOTE**
>
> Vous ne pouvez modifier le mot de passe que pour les utilisateurs locaux. Pour les utilisateurs authentifiés à distance, vous devez mettre à jour le mot de passe sur le serveur externe.

Modifier le rôle d'utilisateur

Pour modifier le rôle de l'utilisateur, cliquez sur l'icône **Modifier** dans la colonne **Actions** . Sélectionnez un **rôle** et cliquez sur **Appliquer**.

> **NOTE**
>
> Vous ne pouvez pas modifier le rôle de l'utilisateur administrateur par défaut.



Nom de domaine

October 21, 2022

Le nom de domaine est une URL personnalisée utilisée dans la barre d'adresse pour accéder à Citrix SD-WAN Orchestrator pour les applications locales. L'utilisation d'un nom de domaine facilite sa mémorisation et vous permet également d'utiliser le nom de marque de votre entreprise.

Pour utiliser un nom de domaine, assurez-vous qu'un serveur DNS local est configuré avec un enregistrement DNS liant le nom de domaine à l'adresse IP Citrix SD-WAN Orchestrator pour la gestion sur site. Assurez-vous que le nom de domaine est configuré lors de la configuration initiale. Lors de la configuration d'un nom de domaine, Citrix SD-WAN Orchestrator pour les redémarrages locaux et les certificats sont régénérés automatiquement. Le même nom de domaine doit être configuré sur les différentes appliances. Pour plus de détails, voir Configuration de l'SD-WAN Orchestrator sur site sur une appliance SD-WAN.

Il n'est pas obligatoire de configurer un nom de domaine. Si vous n'avez pas de nom de domaine et que vous souhaitez tout de même utiliser le serveur DNS pour la résolution des adresses IP, configurez les enregistrements DNS qui pointent vers Citrix SD-WAN Orchestrator pour IP sur site pour les trois noms de domaine complets suivants :

- sdwanzt.citrixnetworkapi.net

- download.citrixnetworkapi.net
- sdwan-home.citrixnetworkapi.net

Par exemple, si un Citrix SD-WAN Orchestrator pour domaine local est configuré en tant que **citrix.com**, vous devez créer l'enregistrement DNS sur le serveur DNS pour le nom de domaine complet ci-dessous et l'adresse IP Citrix SD-WAN Orchestrator pour site local :

- download.citrix.com
- sdwanzt.citrix.com
- sdwan-home.citrix.com

En configuration avancée :

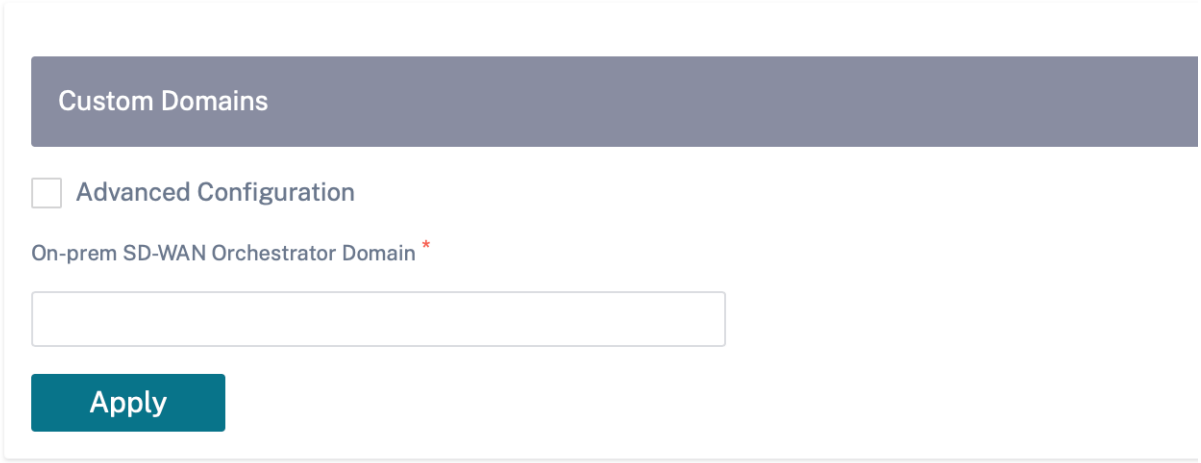
Par exemple : si un domaine Citrix SD-WAN Orchestrator pour site local est configuré en tant que **citrix.com**, le **domaine du service de gestion des téléchargements** est configuré en tant que **download.citrix.com**et le **domaine du service de gestion des statistiques** est configuré en tant que **statistiques. citrix.com**, vous devez ensuite créer l'enregistrement DNS dans le serveur DNS pour le nom de domaine complet ci-dessous et l'adresse IP correspondante :

- download.citrix.com
- sdwanzt.citrix.com
- statistics.citrix.com

La configuration ou la modification d'un nom de domaine pour une configuration existante affecte Citrix SD-WAN Orchestrator pour la connectivité sur site et des appliances. Vous devez effectuer manuellement le processus d'authentification par certificat ou utiliser l'option Paramètres de déploiement Zero Touch du site .

> **Remarque**
>
> Dans une configuration gérée par un fournisseur, seuls les administrateurs du fournisseur ont accès à la modification des informations relatives aux noms de domaine.

Pour configurer un nom de domaine, au niveau du réseau, accédez à **Administration > Nom de domaine** et fournissez un Citrix SD-WAN Orchestrator pour le nom de domaine sur site.



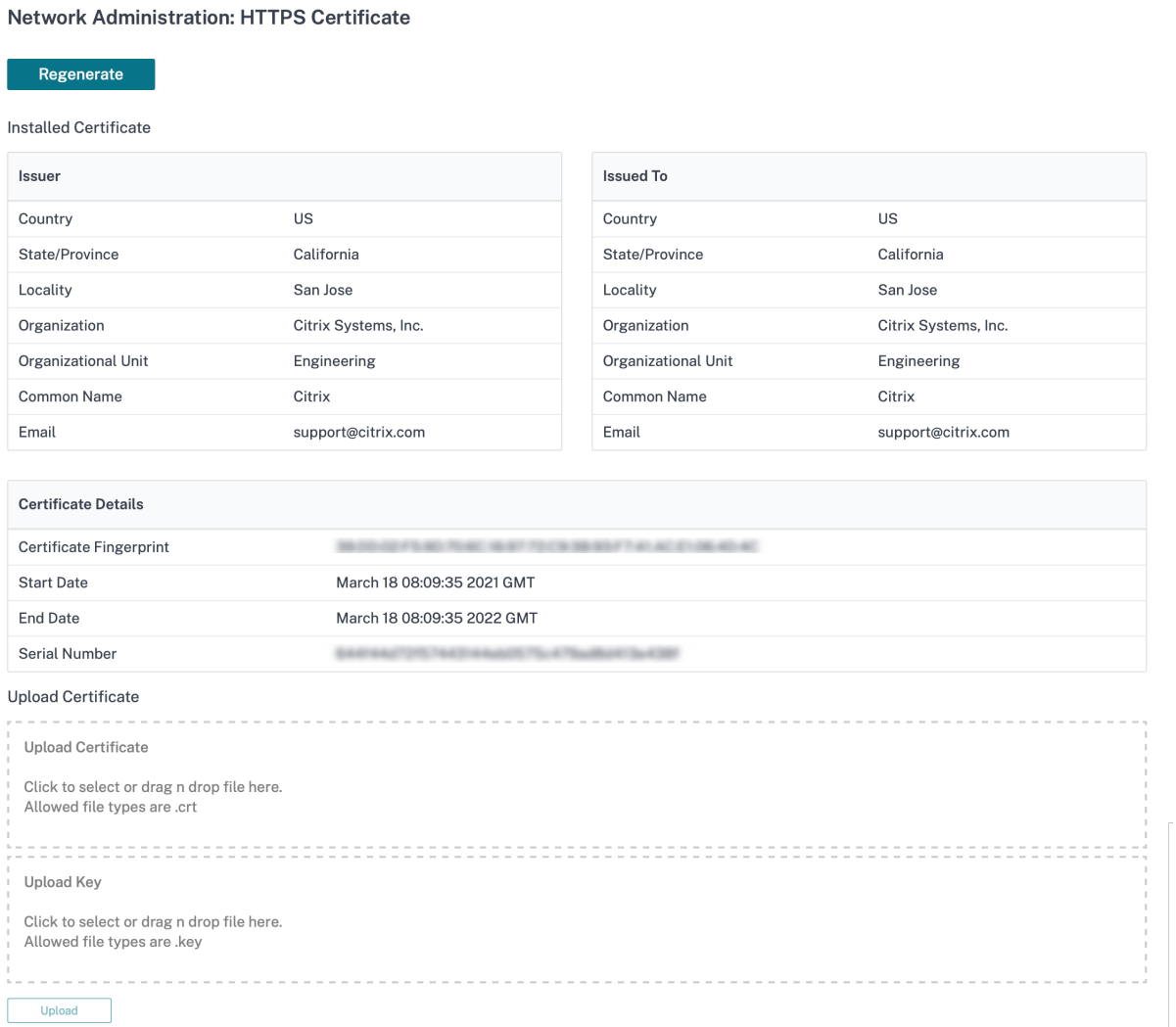
Certificat HTTPS

October 21, 2022

Un certificat HTTPS est requis pour établir une connexion HTTPS de gestion sécurisée à Citrix SD-WAN Orchestrator for On-premises. Vous pouvez utiliser le certificat HTTPS par défaut disponible sur l'interface utilisateur graphique Citrix SD-WAN Orchestrator for On-premises ou télécharger un certificat HTTPS personnalisé généré à partir de tout autre framework tel qu'OpenSSL ou d'une autorité de confiance. Le certificat HTTPS personnalisé vous permet de contrôler la sécurité et les autres paramètres du sujet liés au certificat.

Pour afficher le certificat par défaut, accédez à **Administration > Certificat HTTPS**.

> **Remarque**
>
> Dans une configuration gérée par un fournisseur, seuls les administrateurs du fournisseur ont accès à la régénération et au téléchargement du certificat HTTPS.



La section **Certificat installé** fournit un résumé du certificat installé sur l'appliance. L'appliance utilise ce certificat pour s'identifier au sein du réseau.

La section **Délivré à** fournit des détails sur la personne à qui le certificat a été émis. Le **nom commun** du certificat correspond au nom de l'appliance, car le certificat est lié au nom de l'appliance. La section **Émetteur** fournit les détails de l'autorité de signature du certificat, qui a signé le certificat. Les détails du certificat comprennent l'empreinte digitale du certificat, le numéro de série et la période de validité du certificat.

Pour régénérer le certificat, accédez à **Administration > Certificat HTTPS** et cliquez sur **Régénérer**.

> **Remarque**
>
> La régénération du certificat déconnecte toutes les sessions HTTPS connectées existantes et redémarre le serveur HTTPS. Une fois le certificat régénéré avec succès, l'interface graphique est actualisée automatiquement.

Vous pouvez générer des certificats HTTPS à partir de n'importe quel autre framework tel qu'OpenSSL ou d'une autorité de confiance et les télécharger sur Citrix SD-WAN Orchestrator for On-premises. Le format de certificat pris en charge est .crt et le format de clé pris en charge est .key.

Pour télécharger un certificat HTTPS personnalisé, cliquez sur **Charger** ou faites glisser le certificat et les fichiers clés dans les zones **Télécharger le certificat** et **Télécharger la clé** respectivement. Une fois le téléchargement réussi, l'interface graphique est actualisée automatiquement.

Gestion de l'espace disque

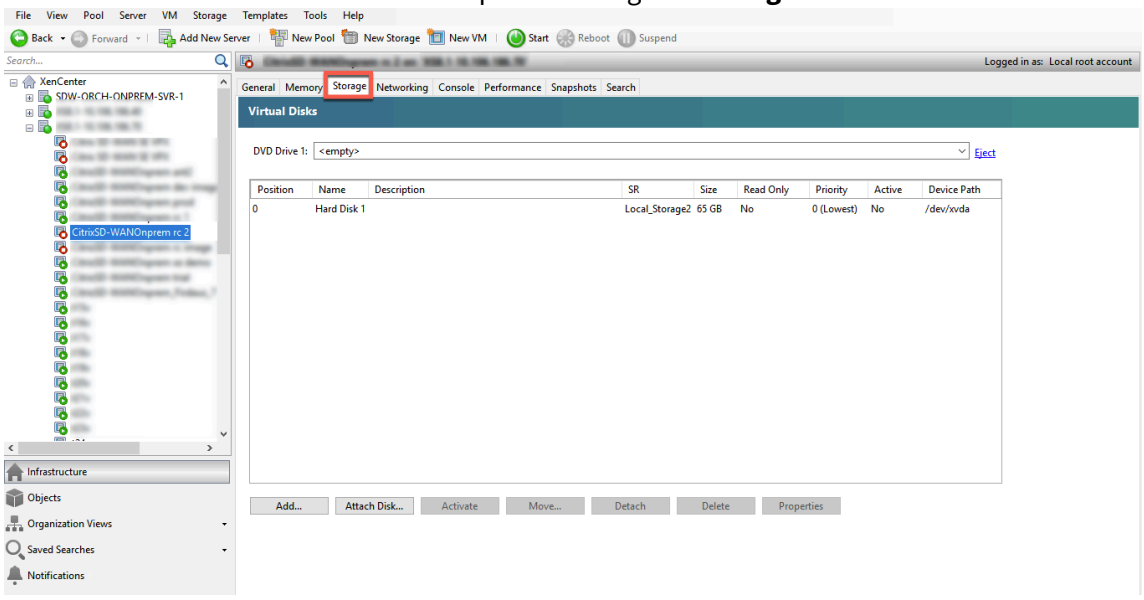
October 21, 2022

Vous pouvez augmenter l'espace disque alloué à Citrix SD-WAN Orchestrator pour les applications locales.

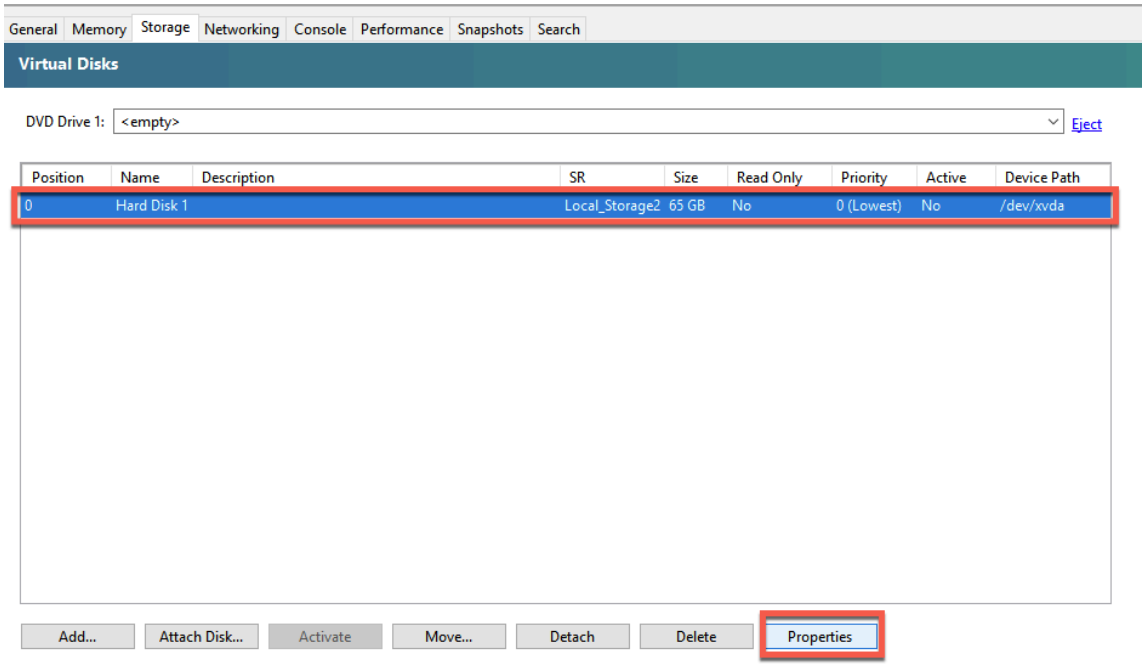
Augmentez l'espace disque sur Citrix Hypervisor

Pour augmenter l'espace disque sur Citrix Hypervisor.

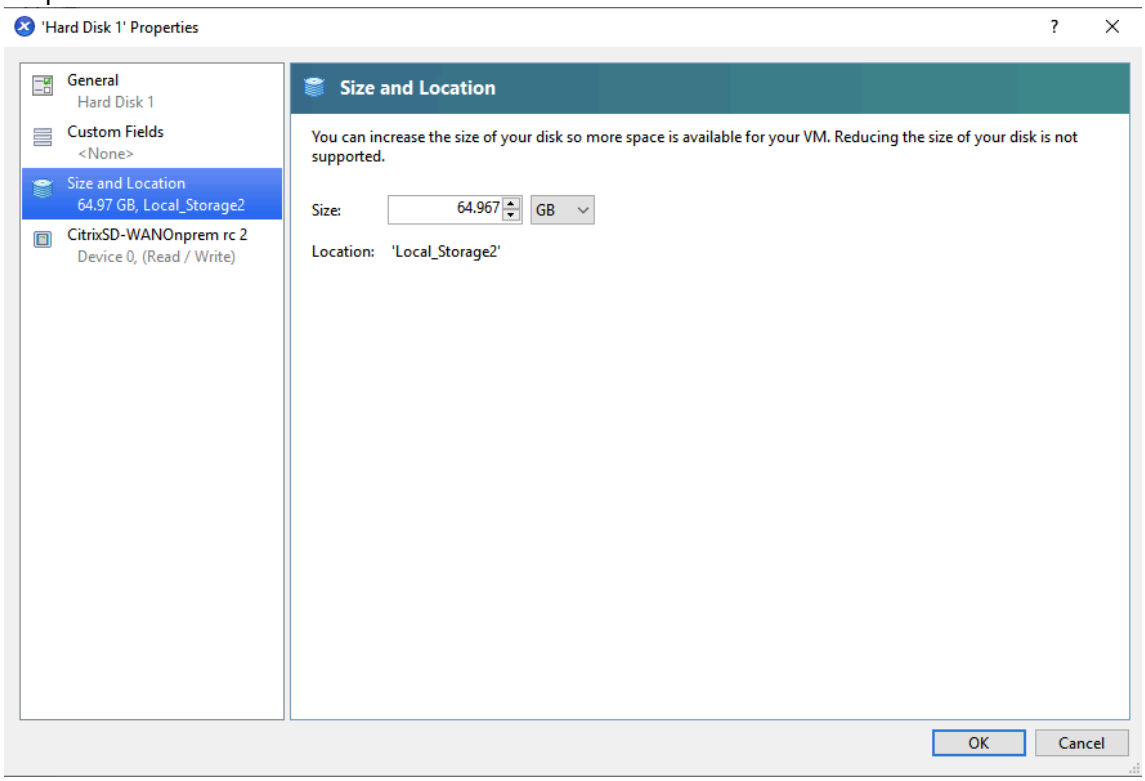
1. Arrêtez la machine virtuelle (VM) depuis l'hyperviseur.
2. Sélectionnez la machine virtuelle et cliquez sur l'onglet **Stockage** .



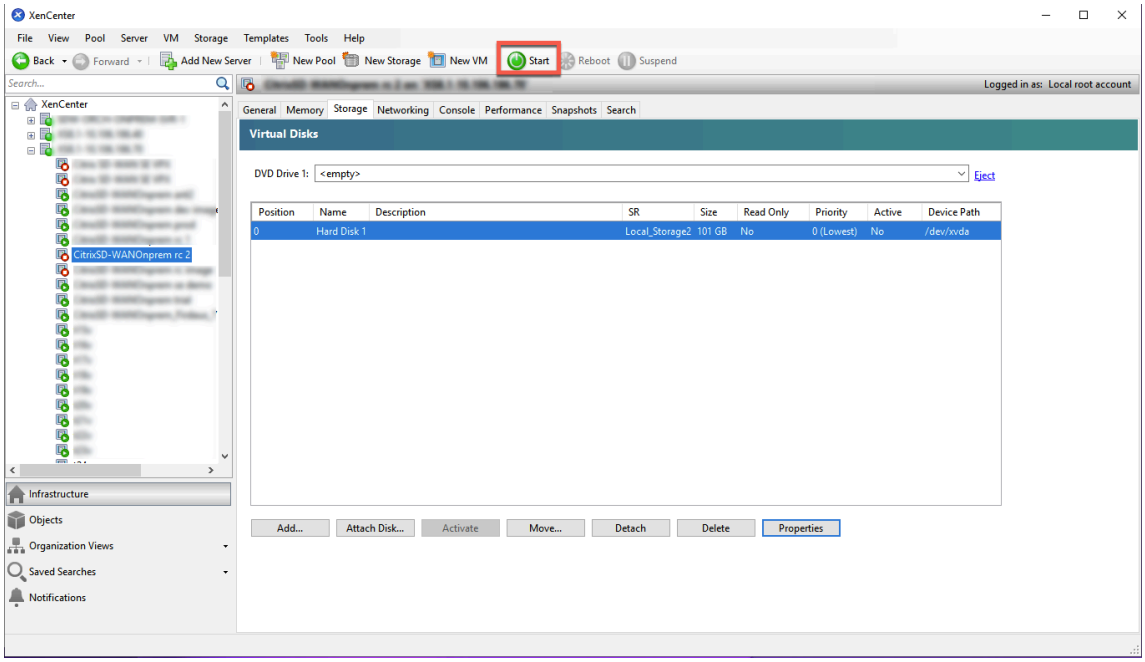
3. Sélectionnez le disque dur et cliquez sur **Propriétés**.



4. Cliquez sur l'option **Taille et emplacement** et mettez à jour la **taille** de votre espace disque. Cliquez sur **OK**.



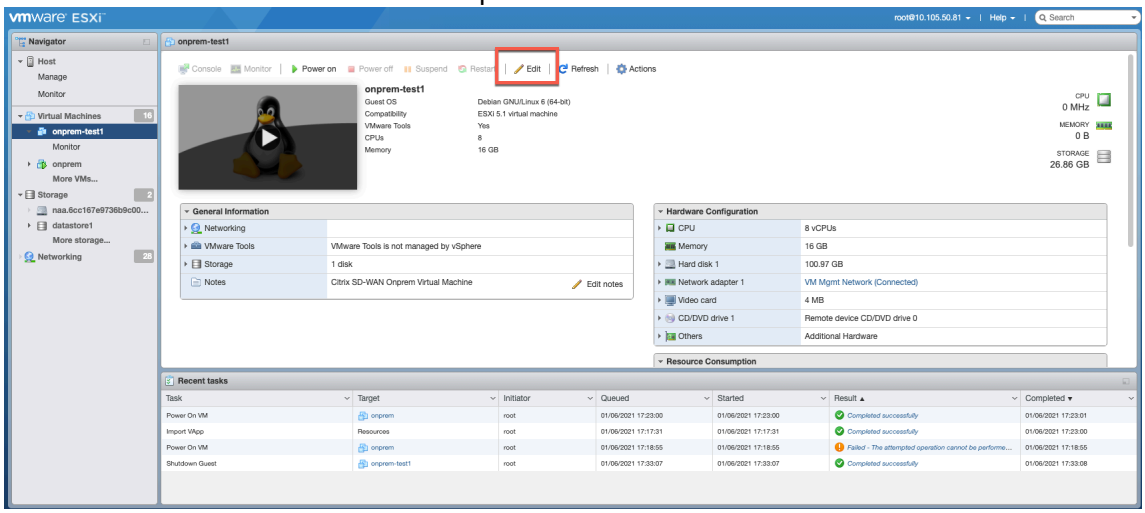
5. Cliquez sur **Démarrer**.



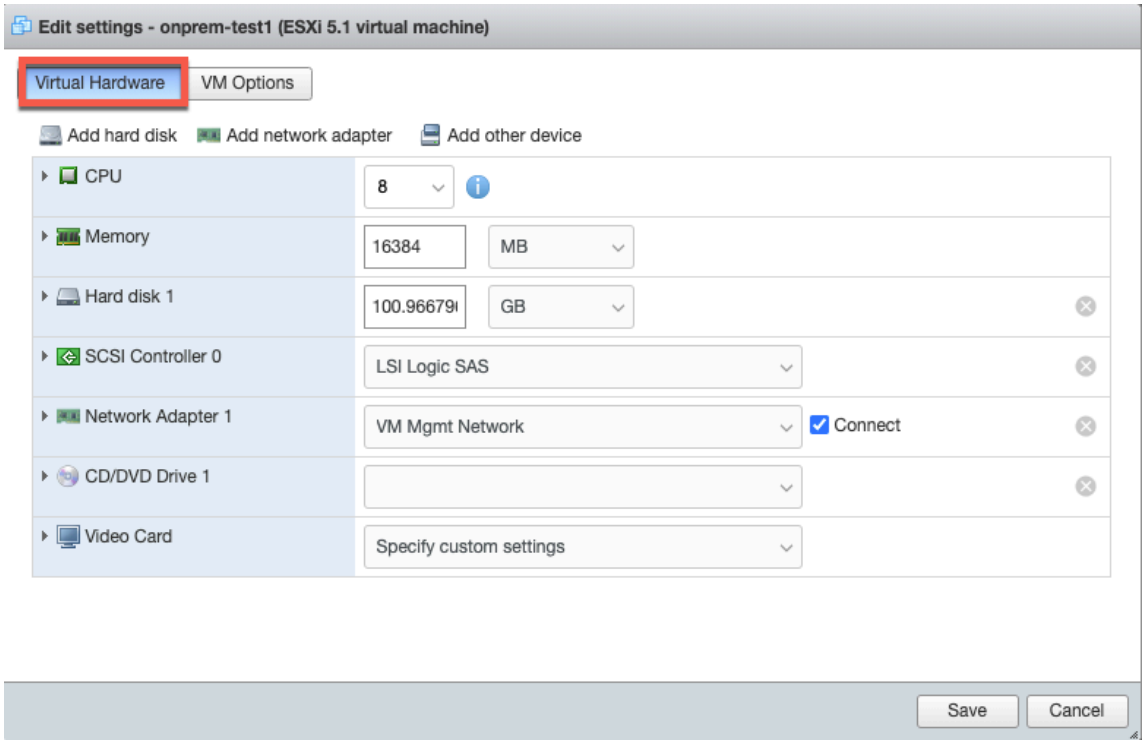
Augmentez l'espace disque sur le serveur ESXi

Pour augmenter l'espace disque sur le serveur ESXi.

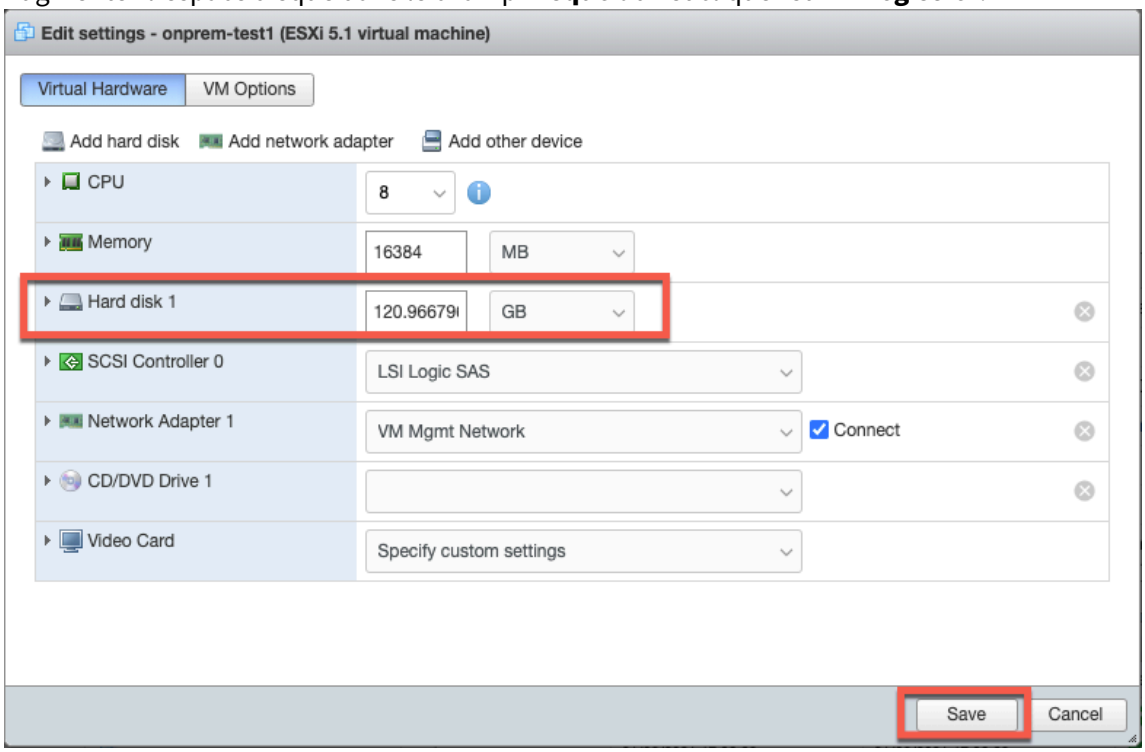
1. Arrêtez la machine virtuelle (VM) depuis l'hyperviseur.
2. Sélectionnez la machine virtuelle et cliquez sur **Modifier**.



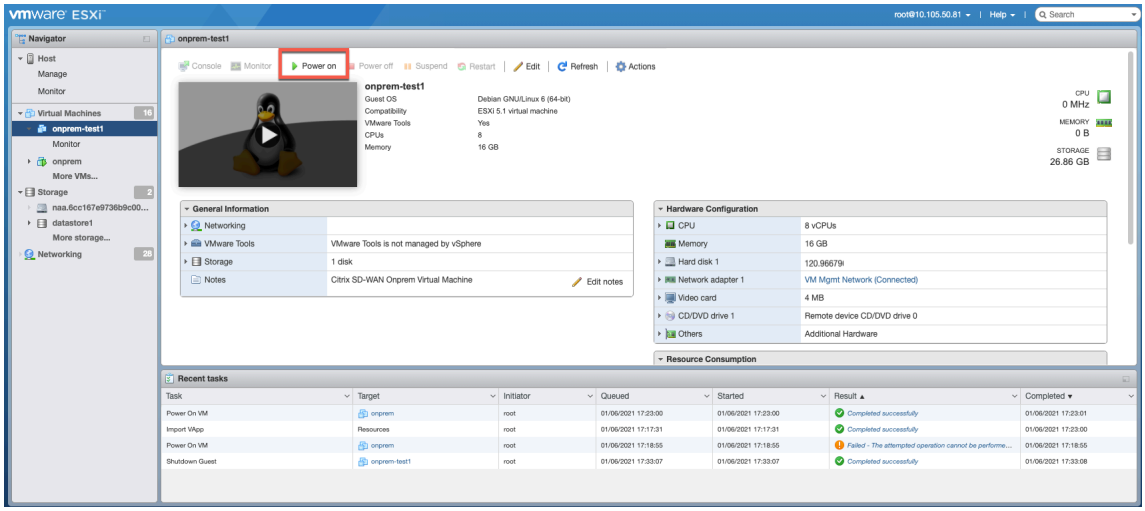
3. Sélectionnez l'onglet **Matériel virtuel** .



4. Augmentez l'espace disque dans le champ **Disque dur** et cliquez sur **Enregistrer**.



5. Cliquez sur **Allumer**.



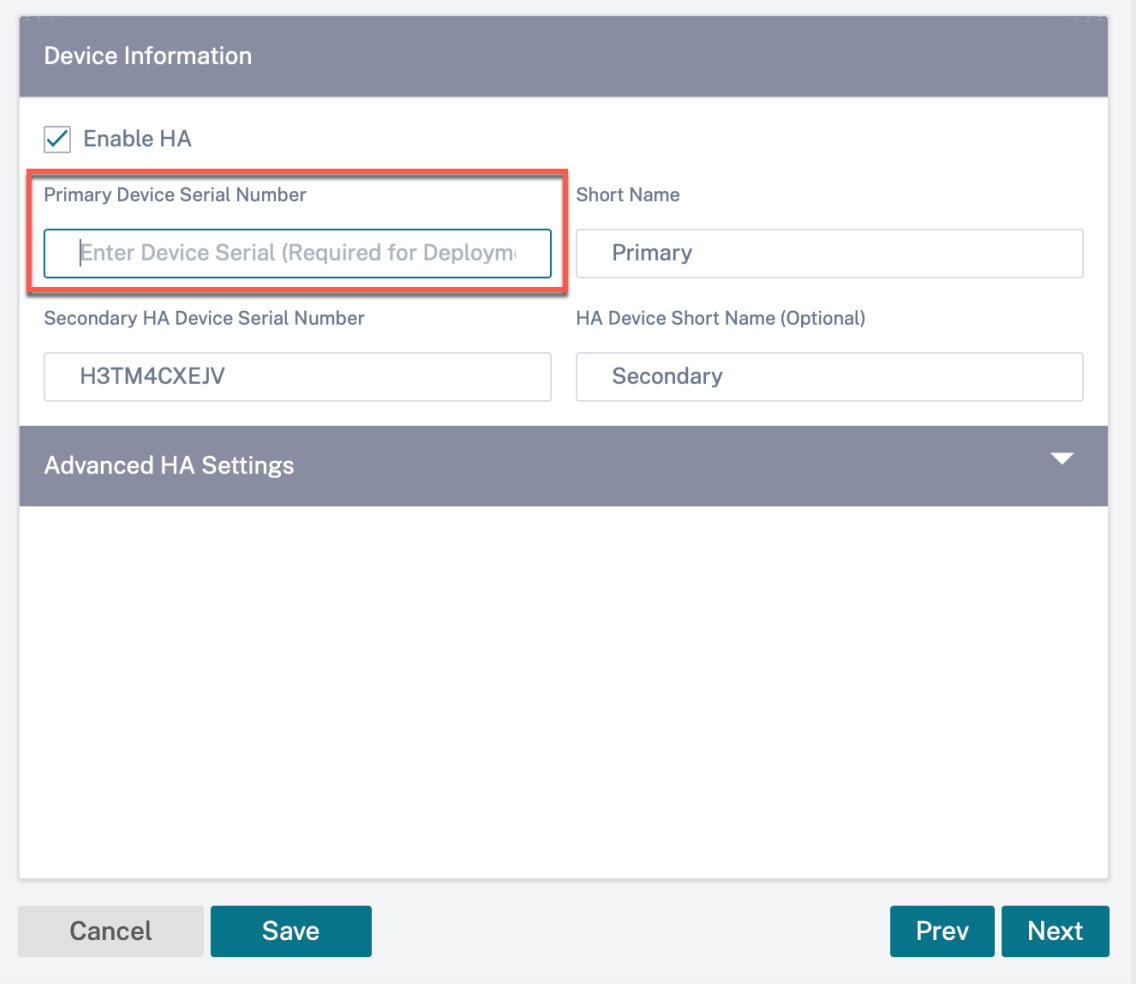
Remplacer une appliance Citrix SD-WAN affectée

October 21, 2022

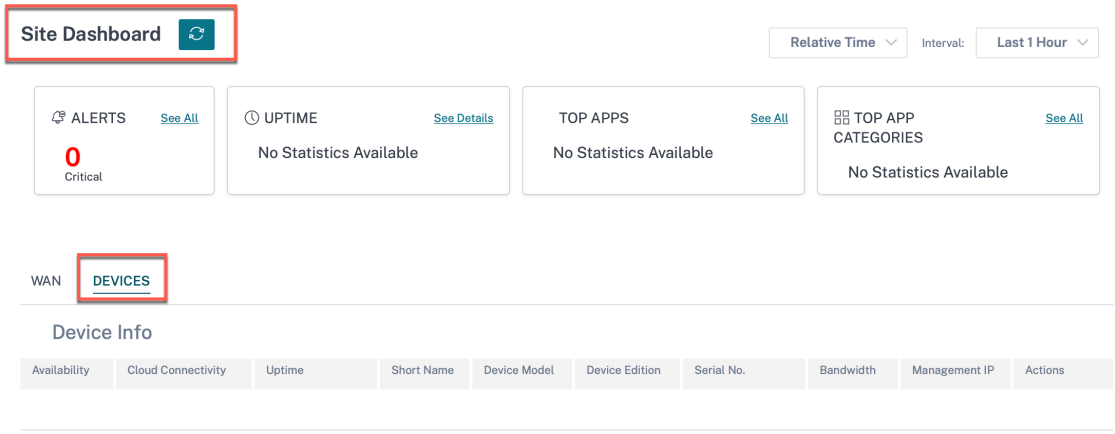
Pour remplacer un dispositif concerné dans Citrix SD-WAN Orchestrator pour locaux :

1. Connectez-vous à Citrix SD-WAN Orchestrator for On-premises et sélectionnez le site concerné. Au niveau du site, accédez à **Configuration > Configuration du site > Informations sur le périphérique** et supprimez le numéro de série du champ **Numéro de série du périphérique principal** . Cliquez sur **Enregistrer**.

   > **Remarque**
   >
   > Si l'appliance est toujours accessible via Citrix SD-WAN Orchestrator for On-premises, l' appliance est dans l'état « Factory Reset ».

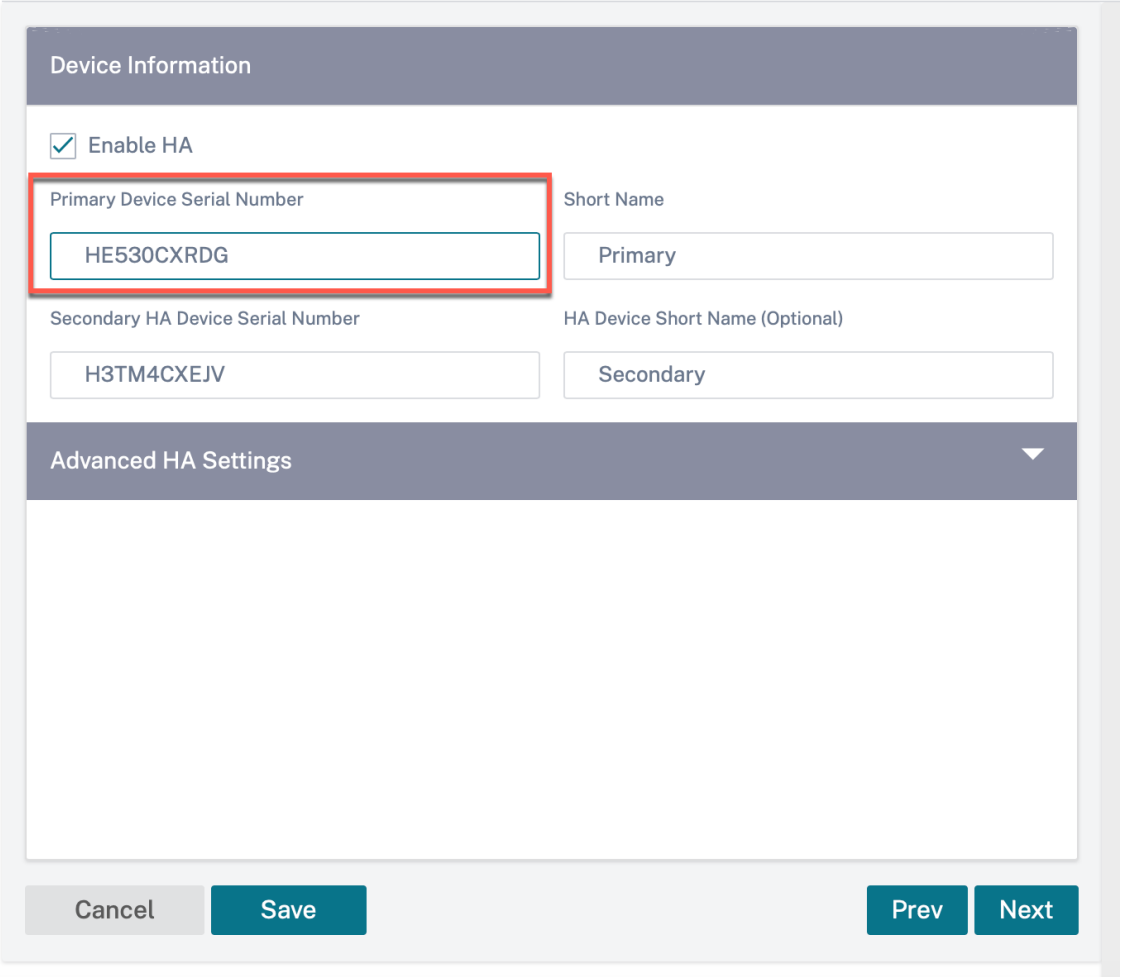


2. Accédez à **Tableau de bord > Appareils** et assurez-vous que l'appliance concernée est supprimée de la liste.

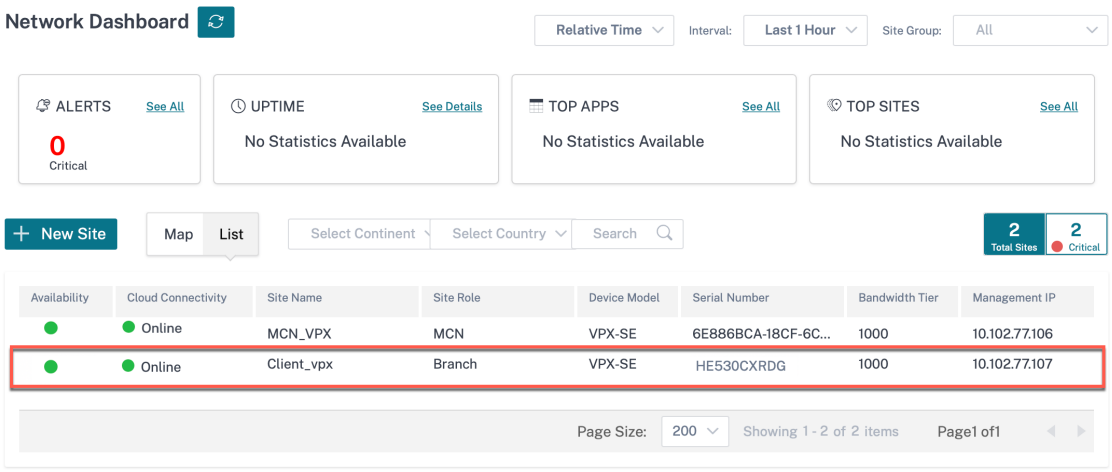


3. Prenez note de la configuration de l'alimentation et du câblage de l'appliance concernée, puis retirez l'appliance du rack.

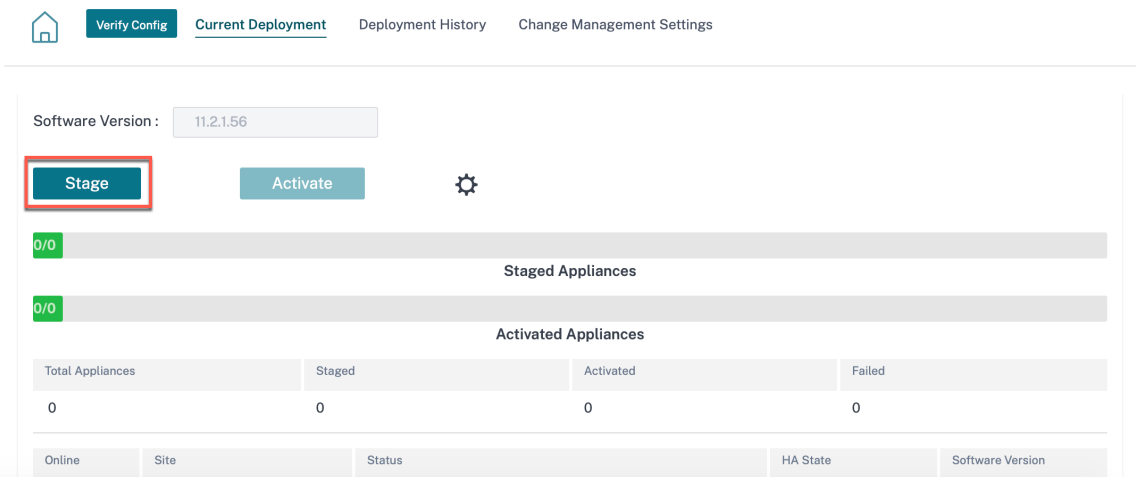
4. Montez la nouvelle appliance sur le rack et refaites l'alimentation et le câblage comme pour l'appliance concernée.
5. Dans l'interface utilisateur de Citrix SD-WAN Orchestrator for On-premises, au niveau du site, accédez à **Configuration > Configuration du site > Détails de l'appareil**. Ajoutez le numéro de série du nouvel appareil dans le champ **Numéro de série de l'appareil principal** . Cliquez sur **Enregistrer**.



6. Configurez le déploiement Zero-touch. Pour plus d'informations, voir Déploiement sans contact.
7. Patientez quelques minutes pour que l'appliance mette à jour la connectivité cloud sur le tableau de bord du site.



8. Au niveau du réseau, accédez à **Configuration > Page d'accueil de la configuration réseau** et cliquez sur **Déployer la configuration/le logiciel**.
9. Cliquez sur **Stage**.



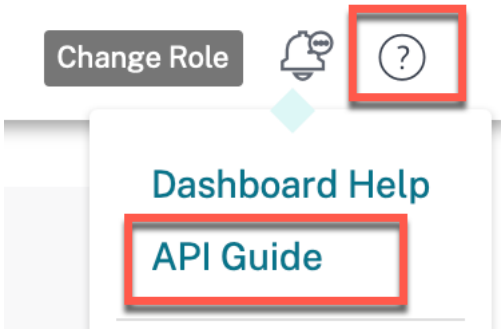
10. Cliquez sur **Activer** une fois la phase intermédiaire terminée.
11. Accédez au tableau de bord du site et vérifiez que l'appliance a bien été activée.

Guide d'API pour Citrix SD-WAN Orchestrator pour locaux

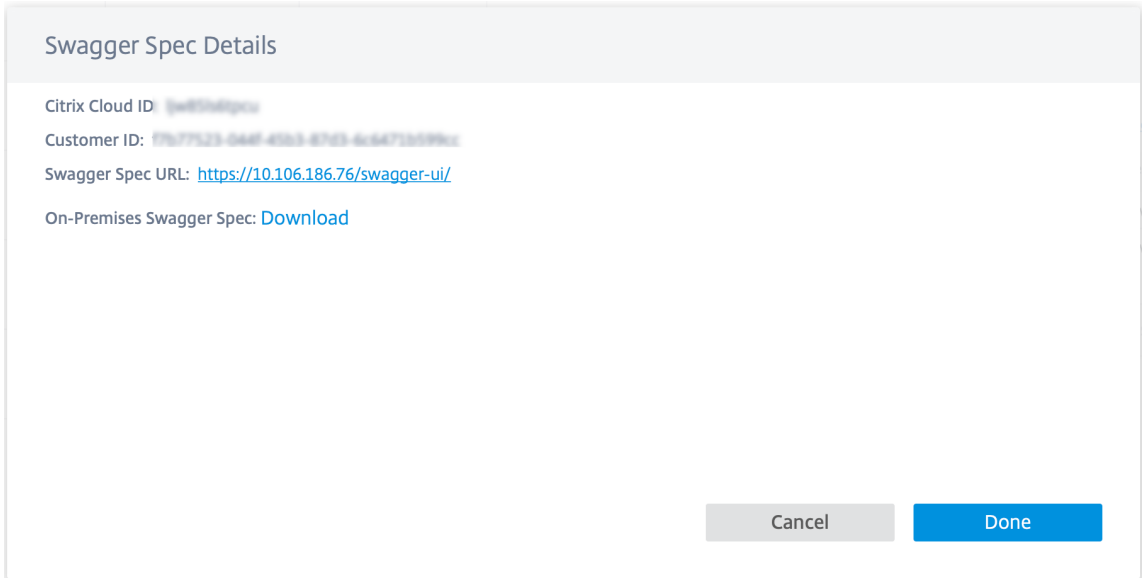
October 21, 2022

Pour accéder au guide de l'API Citrix SD-WAN Orchestrator pour locaux sur l'interface utilisateur Swagger, procédez comme suit :

1. Connectez-vous au Citrix SD-WAN Orchestrator for On-premises et cliquez sur **?** dans le coin supérieur droit de l'interface utilisateur, puis cliquez sur **Guide des API**.



Les détails de la spécification Swagger sont affichés.



2. Cliquez sur l'URL de la spécification Swagger pour accéder au guide de l'API.

Citrix SD-WAN Orchestrator pour les API locales via curl

Conditions préalables

- Connexion au cloud
- Connexion locale

Effectuez les étapes suivantes pour utiliser les API d'orchestrateur sur site Citrix via curl :

1. **Connexion au cloud** : dans le cas d'un nouveau XVA, vous devez d'abord vous connecter au cloud.


```
curl -k -X POST -H "Content-Type: application/json "https://<
    onprem-orchestrator-ip>/policy/v1/onprem/cloudLogon  – data '{
 "clientId":"<clientId>","clientSecret":"<clientSecret> ","ccId":"
    <ccid>", "pop": "<popName>" }
 '
```

Les `clientIdclientSecret`, et `ccId` peuvent être obtenus sur la page IAM.

> **Remarque**
>
> Assurez-vous que le compte client est déjà créé dans le cloud avant de tenter de vous connecter au cloud.

2. **Connexion locale** : effectuez ensuite une connexion locale pour obtenir le jeton d'authentification.

```
curl -k -X POST -H "Content-Type: application/json" https://<
    onprem-orchestrator-ip>/onpm/v1/logon --data '{
 "username":"admin","password":"<passwordField>" }
 '
```

Cela renvoie le **token** et le **CustomerID** en réponse. Le CustomerID reste fixe et il est nécessaire dans les autres appels d'API. Enregistrez le **CustomerID** pour une utilisation ultérieure. Le jeton reste valide pendant une heure. Plus tard, vous devrez effectuer une nouvelle connexion.

Exemple : utilisez le jeton d'**authentification** et l'**ID client** pour déclencher d'autres API Citrix locales.

```
curl -k -X GET -H "authorization:CWSAuth bearer= <token> " -H "
    Content-Type: application/json"https://<onprem-orchestrator-ip
    >/onpm/v1/scope/<customerId>/globalSettings/ntpSettings
```

Administration de l'orchestrateur

October 21, 2022

Cette section vous fournit des informations sur les activités administratives qui peuvent être effectuées sur la plate-forme Citrix SD-WAN Orchestrator for On-premises.

Logiciel

Vous pouvez télécharger la version du logiciel de l'appliance Citrix SD-WAN requise pour toutes les appliances de votre réseau et stockée dans Citrix SD-WAN Orchestrator pour les applications locales. Utilisez le logiciel stocké pour mettre à niveau votre logiciel Citrix SD-WAN Orchestrator for On-premises vers la dernière version.

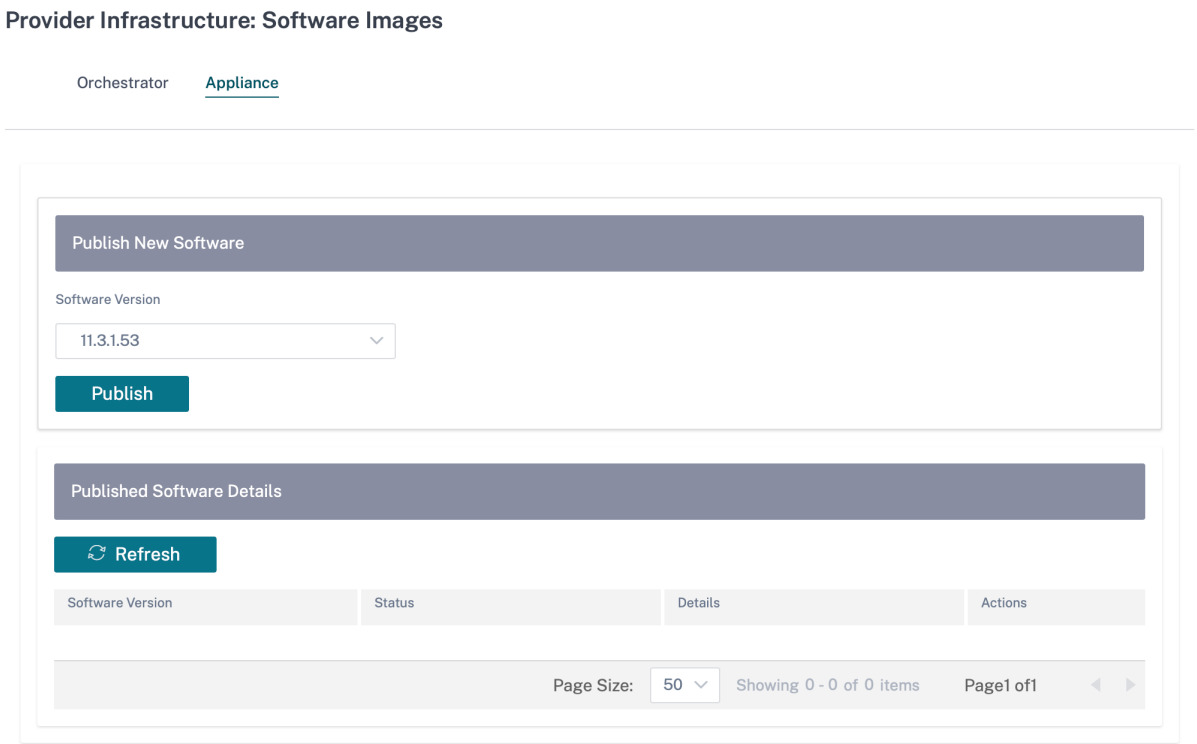
> **Remarque**
>
> La configuration gérée par le fournisseur est introduite à partir de Citrix SD-WAN Orchestrator pour la version 10.3 sur site. La rétrogradation vers des versions logicielles inférieures à la version 10.3 de Citrix SD-WAN Orchestrator for On-premises n'est pas prise en charge.

Publier des logiciels

Dans une configuration gérée par un fournisseur, Citrix SD-WAN Orchestrator pour locaux permet aux administrateurs du fournisseur de télécharger la version du logiciel de l'appliance Citrix SD-WAN requise pour toutes les appliances de votre réseau. Les administrateurs du fournisseur peuvent publier la version logicielle téléchargée. Le logiciel publié est téléchargé et stocké dans Citrix SD-WAN Orchestrator for On-premises. Les administrateurs clients peuvent déployer le logiciel publié sur toutes les appliances gérées par Citrix SD-WAN Orchestrator pour les applications sur site.

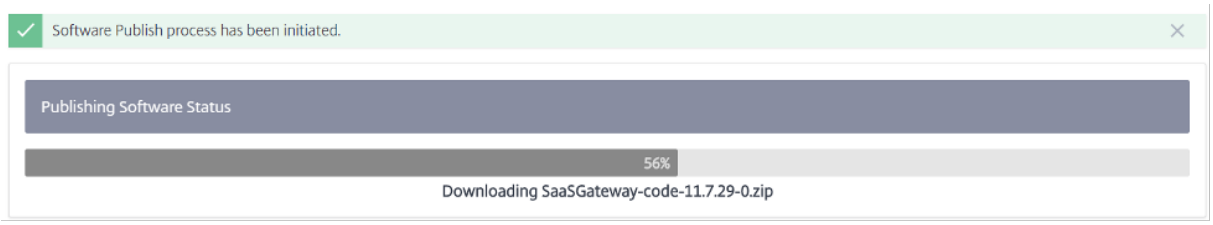
Dans une configuration gérée par le client, les administrateurs clients peuvent télécharger la version du logiciel de l'appliance Citrix SD-WAN requise pour toutes les appliances du réseau. Ils peuvent publier le logiciel dans Citrix SD-WAN Orchestrator for On-premises et déployer le logiciel sur toutes les appliances.

Pour publier un logiciel, accédez à **Infrastructure > Administration de l'orchestrateur > Images logicielles > Appliance**.

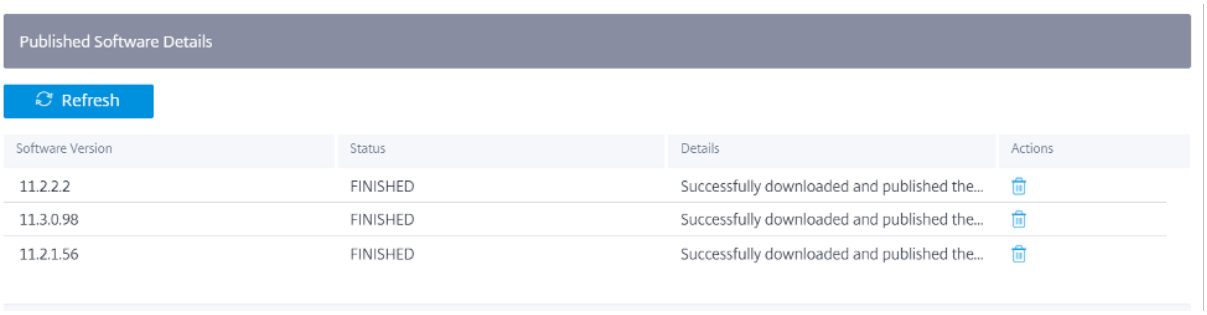


Vous pouvez choisir une version logicielle à publier à partir d'une liste prédéfinie de versions logicielles prises en charge par l'actuel Citrix SD-WAN Orchestrator for On-premises. Pour les nouvelles versions du logiciel qui ne sont pas disponibles dans la liste, effectuez une mise à niveau vers la dernière version de Citrix SD-WAN Orchestrator pour site qui prend en charge la nouvelle version logicielle. Pour plus d'informations sur la mise à niveau de Citrix SD-WAN Orchestrator pour locaux, consultez la section Mise à niveau logicielle.

Citrix SD-WAN Orchestrator pour locaux télécharge le logiciel Citrix SD-WAN de la version sélectionnée pour toutes les plateformes. Une barre de progression indique la progression du processus de publication.



Les versions logicielles publiées sont affichées sous **Détails du logiciel publié**. À tout moment, Citrix SD-WAN Orchestrator pour locaux peut stocker jusqu'à trois versions logicielles publiées. Si vous avez l'intention de publier une autre version du logiciel, supprimez l'une des trois versions disponibles avant de commencer le processus de publication.



Une fois la publication réussie, vous pouvez déployer, transférer et activer le logiciel sur toutes les appliances du réseau à partir de la page de **configuration du réseau** . Pour plus d'informations, voir Configuration réseau. Pour un déploiement réussi, assurez-vous que toutes les appliances sont connectées à Citrix SD-WAN Orchestrator for On-premises. Pour plus de détails, consultez la section Con-

nectivité avec les appliances Citrix SD-WAN.

Mise à niveau logicielle

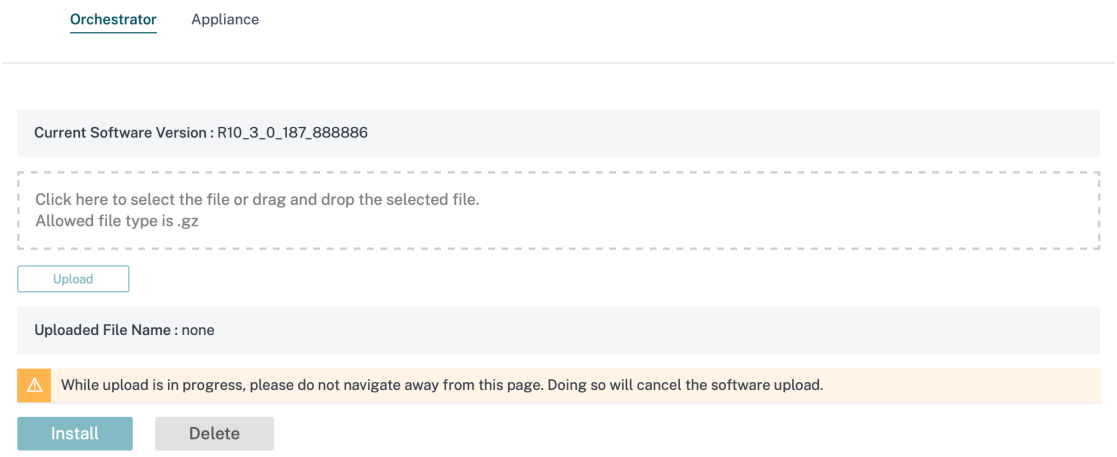
Dans une configuration gérée par un fournisseur, seuls les administrateurs du fournisseur peuvent mettre à niveau le logiciel Citrix SD-WAN Orchestrator for On-premises vers la dernière version.

Dans une configuration gérée par le client, les administrateurs clients peuvent mettre à niveau le logiciel Citrix SD-WAN Orchestrator for On-premises vers la dernière version.

> **REMARQUE**
>
> - Téléchargez le package logiciel Citrix SD-WAN Orchestrator for On-premises approprié sur votre ordinateur local. Vous pouvez télécharger ce package à partir de la page Téléchargements .
> - Citrix recommande de prendre des instantanés de la machine virtuelle dans l'hyperviseur. De plus, la configuration SD-WAN est téléchargée avant la mise à niveau.
> - Citrix recommande également de prendre régulièrement des instantanés des configurations des machines virtuelles et du SD-WAN.

Effectuez les étapes suivantes pour télécharger et installer une nouvelle version du logiciel Citrix SD-WAN Orchestrator for On-premises :

1. Dans l'interface utilisateur de Citrix SD-WAN Orchestrator pour site, accédez à **Infrastructure > Administration de l'orchestrateur > Images logicielles > Orchestrator**.
2. Cliquez à l'intérieur de la boîte et sélectionnez le fichier binaire ctx-onprem-1 (date la plus récente) .tar.gz que vous avez téléchargé et enregistré sur votre système local.



3. Cliquez sur **Télécharger** pour télécharger le package logiciel sélectionné vers la machine virtuelle Citrix SD-WAN Orchestrator pour machine virtuelle sur site actuelle.

4. Une fois le téléchargement terminé, cliquez sur **Installer**.
5. Lorsque vous êtes invité à confirmer, cliquez sur **Installer**.

Paramètres de gestion

> **Remarque**
>
> Dans une configuration gérée par un fournisseur, seuls les administrateurs du fournisseur peuvent modifier la configuration sous **Infrastructure > Administration de l'orchestrateur > Paramètres de gestion**.

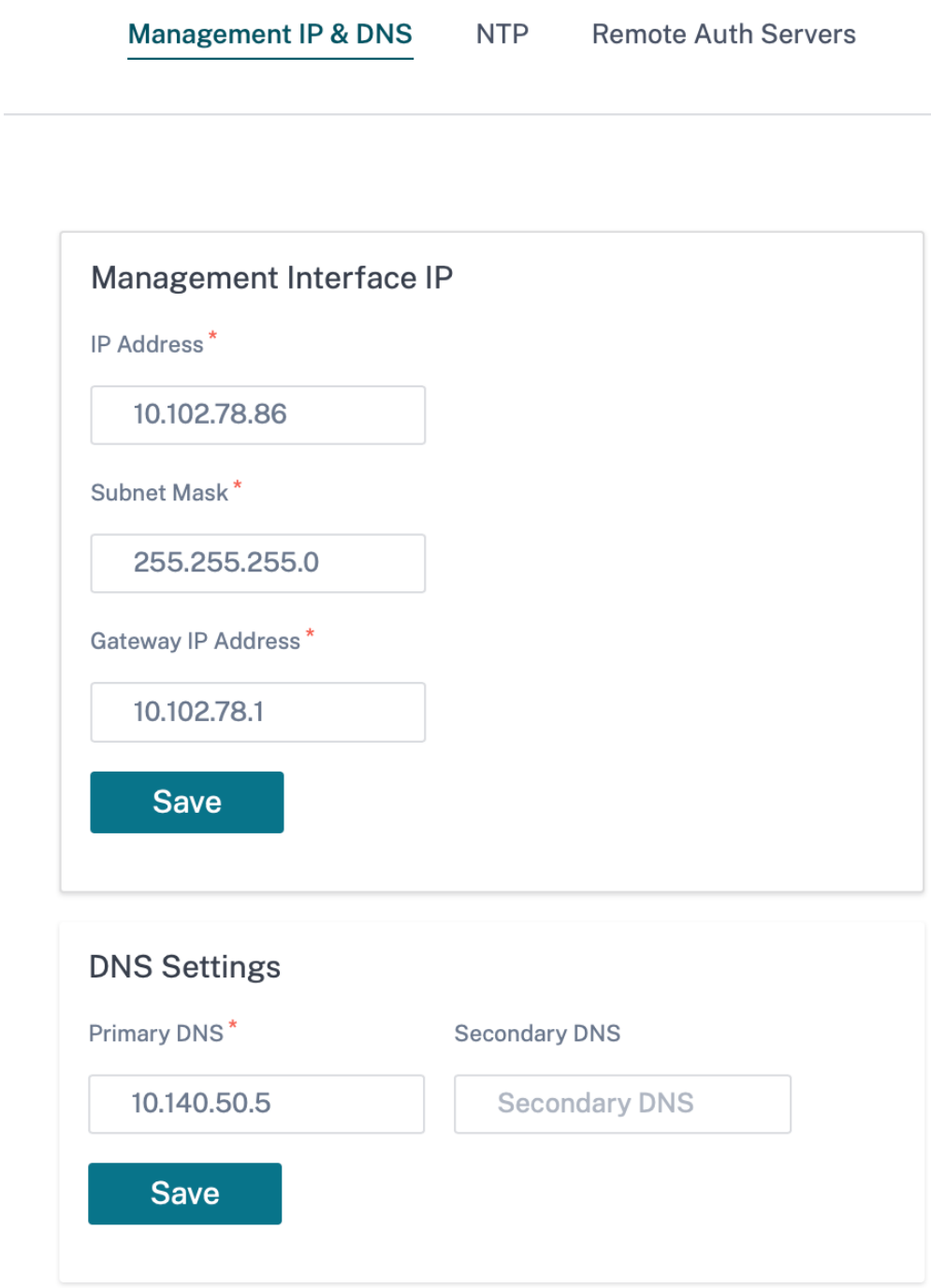
IP de gestion et DNS

Une fois que Citrix SD-WAN Orchestrator pour machine virtuelle (VM) sur site est déployé et qu'une adresse IP de gestion est configurée manuellement ou via DHCP, vous pouvez modifier les paramètres de l'**adresse IP de gestion et du DNS** via Citrix SD-WAN Orchestrator pour l'interface utilisateur graphique locale. Le redémarrage de Citrix SD-WAN Orchestrator pour stack sur site prend environ 3 minutes. Une fois l'adresse IP de gestion modifiée, les connexions SSH sont rétablies.

Pour configurer/modifier les paramètres de gestion IP et DNS, au niveau du réseau, accédez à **Infrastructure > Administration de l'orchestrateur > Paramètres de gestion > IP de gestion et DNS**.

Fournissez les détails suivants :

- **Adresse IP : adresse**IP de Citrix SD-WAN Orchestrator pour machine virtuelle sur site.
- **Adresse IP de passerelle : adresse**IP de passerelle que Citrix SD-WAN Orchestrator pour les applications locales utilise pour communiquer avec des réseaux externes.
- **Masque de sous-réseau** : masque de sous-réseau permettant de définir le réseau dans lequel Citrix SD-WAN Orchestrator pour locaux est disponible.
- **DNS principal** : adresse IP du serveur DNS principal vers lequel toutes les requêtes DNS provenant de Citrix SD-WAN Orchestrator pour locaux sont transférées.
- **DNS secondaire** : adresse IP du serveur DNS secondaire pour résoudre les requêtes DNS si le serveur DNS principal n'est pas disponible.

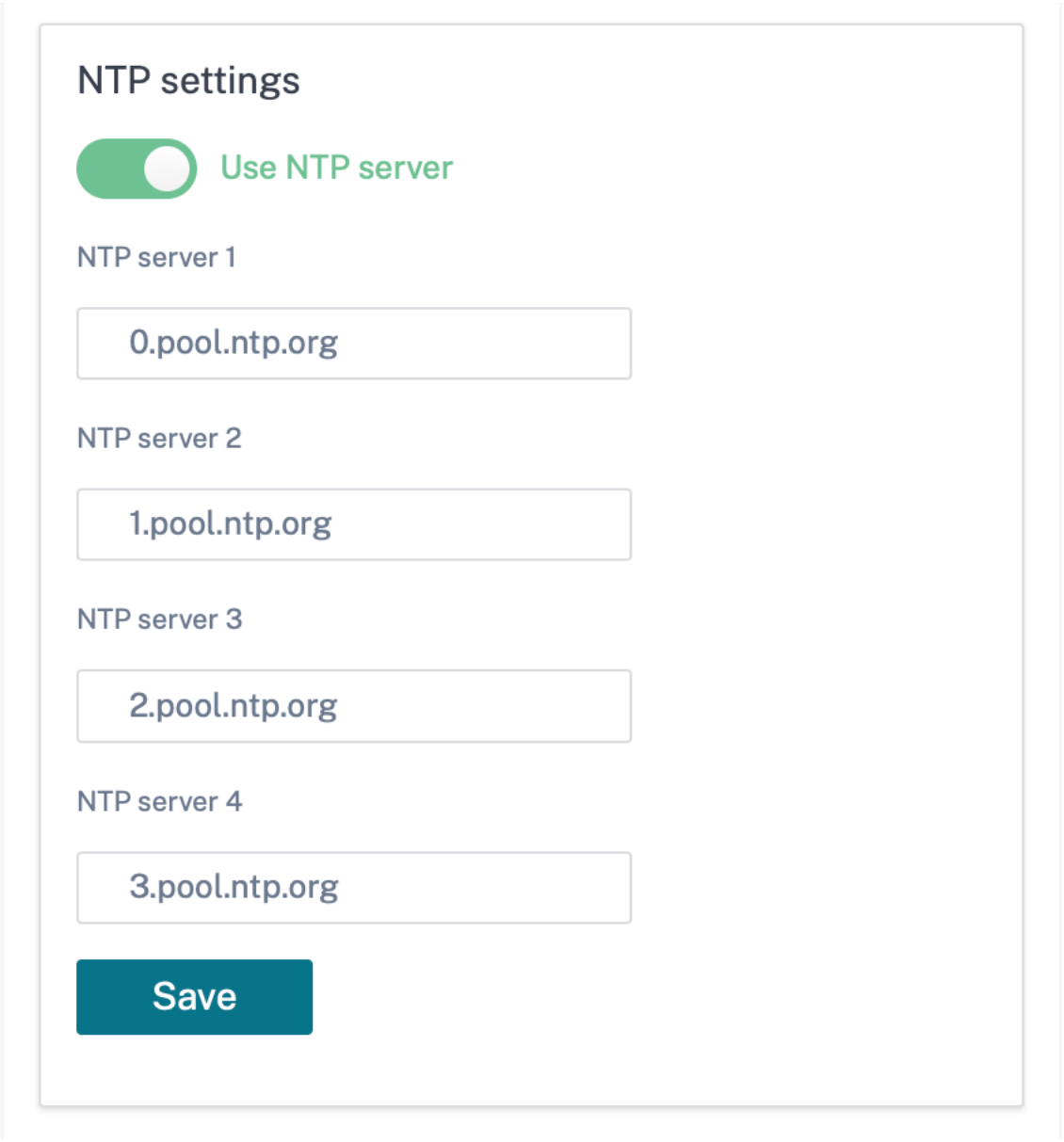


Paramètres NTP

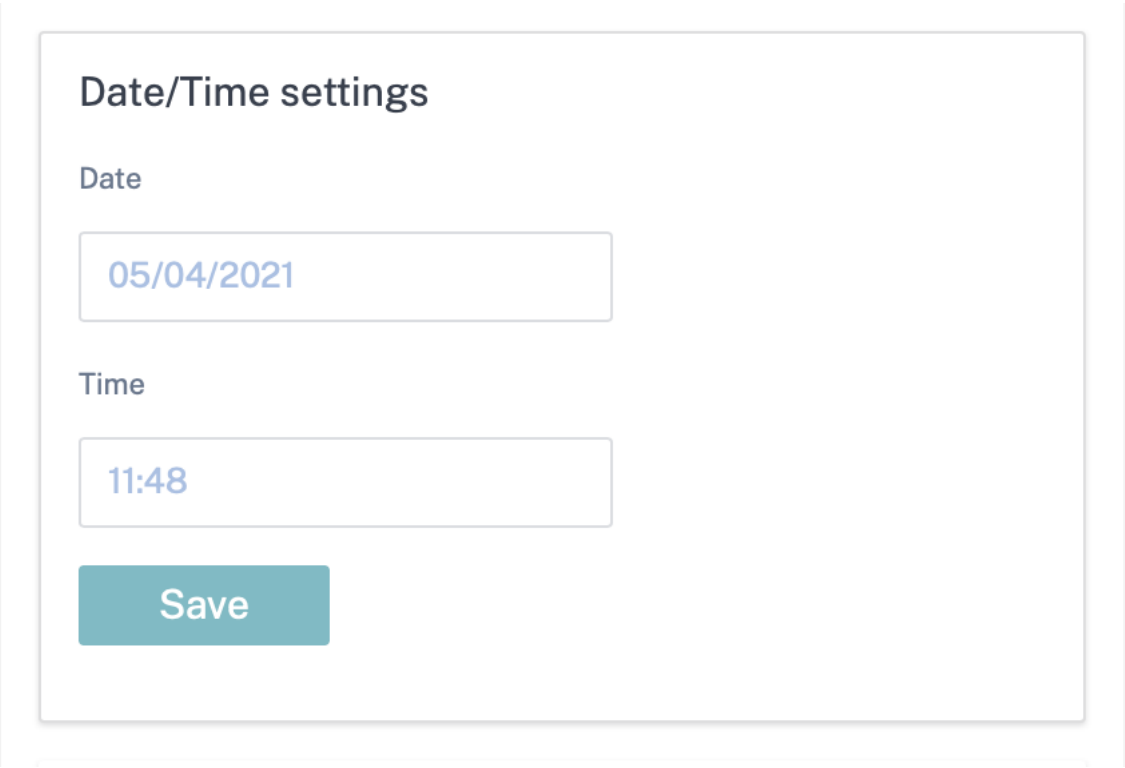
Vous pouvez soit définir la date et l'heure manuellement, soit utiliser un serveur NTP (Network Time Protocol) pour synchroniser l'heure de Citrix SD-WAN Orchestrator pour locaux avec le temps universel coordonné (UTC).

Pour configurer le serveur NTP, au niveau du réseau, accédez à **Infrastructure > Administration de l'orchestrateur > Paramètres de gestion > NTP** et activez **Utiliser un serveur NTP**.

Fournissez l'adresse IP ou le nom de domaine du serveur NTP. Vous pouvez fournir jusqu'à quatre serveurs NTP, mais assurez-vous qu'au moins un est configuré. Si un serveur NTP est en panne, Citrix SD-WAN Orchestrator for On-premises se synchronise automatiquement avec l'autre serveur NTP. Si vous spécifiez un nom de domaine pour un serveur NTP, assurez-vous que le serveur DNS externe est configuré pour pointer le nom de domaine vers l'adresse IP.

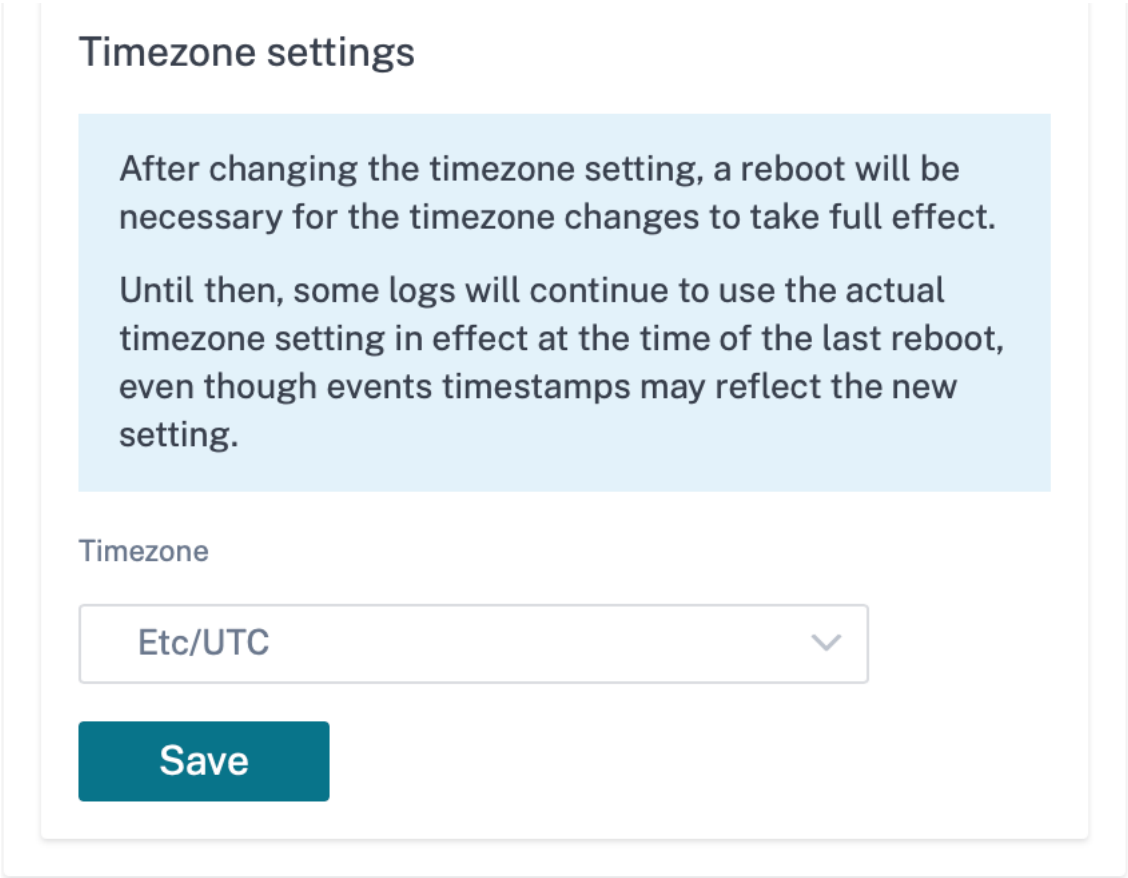


Pour configurer la date et l'heure manuellement, désactivez l'option **Utiliser le serveur NTP** et sélectionnez manuellement la date et l'heure.



Sélectionnez le fuseau horaire en fonction de votre pays/ville.

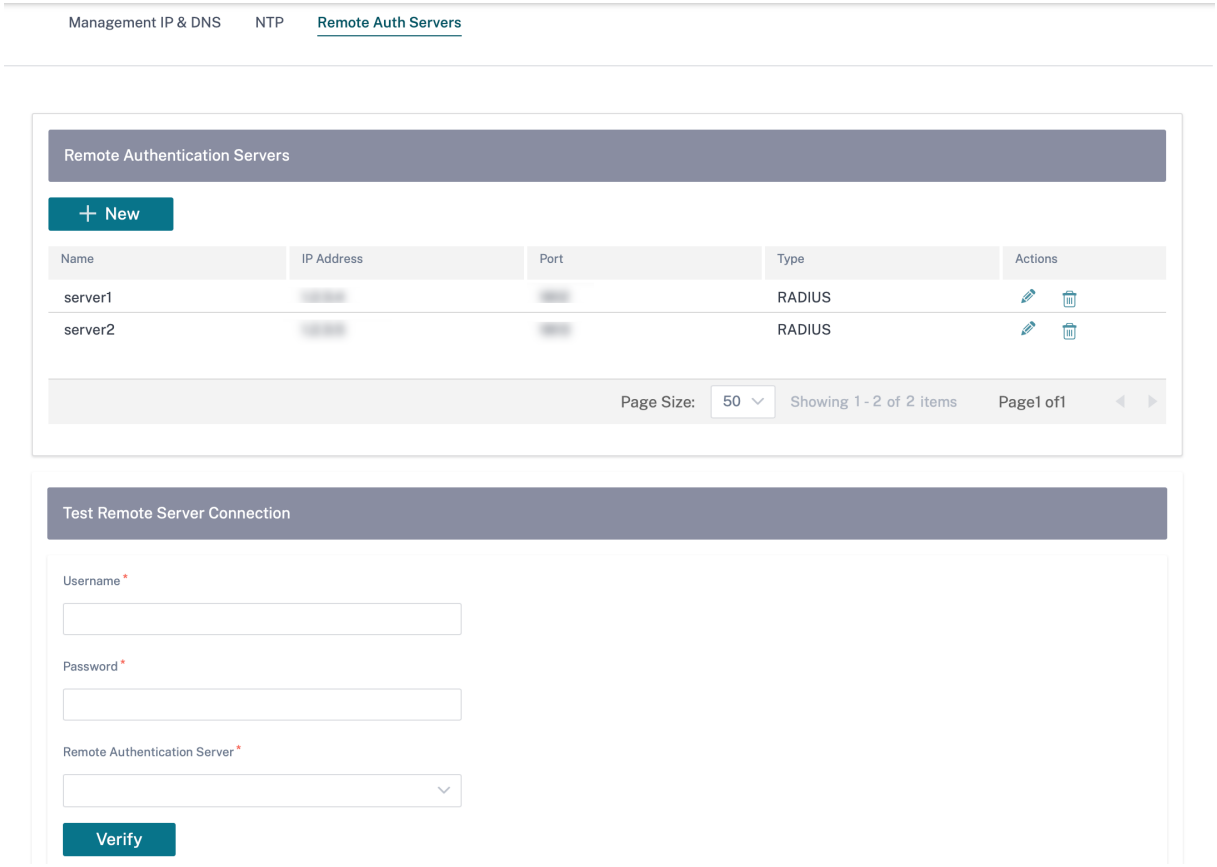
> **REMARQUE**
>
> Redémarrez la machine virtuelle Orchestrator après avoir modifié le fuseau horaire. Certains journaux continuent à utiliser le fuseau horaire précédent, jusqu'à ce que le redémarrage soit terminé. Pour obtenir des instructions, voir Redémarrer la machine virtuelle Orchestrator



serveurs d'authentification à distance

Dans une configuration gérée par un fournisseur, seuls les administrateurs du fournisseur peuvent configurer des serveurs RADIUS ou TACACS+ pour les utilisateurs authentifiés à distance. Les administrateurs clients peuvent utiliser les serveurs d'authentification à distance configurés par les administrateurs du fournisseur. Dans une configuration gérée par le client, les administrateurs clients peuvent configurer des serveurs RADIUS ou TACACS+.

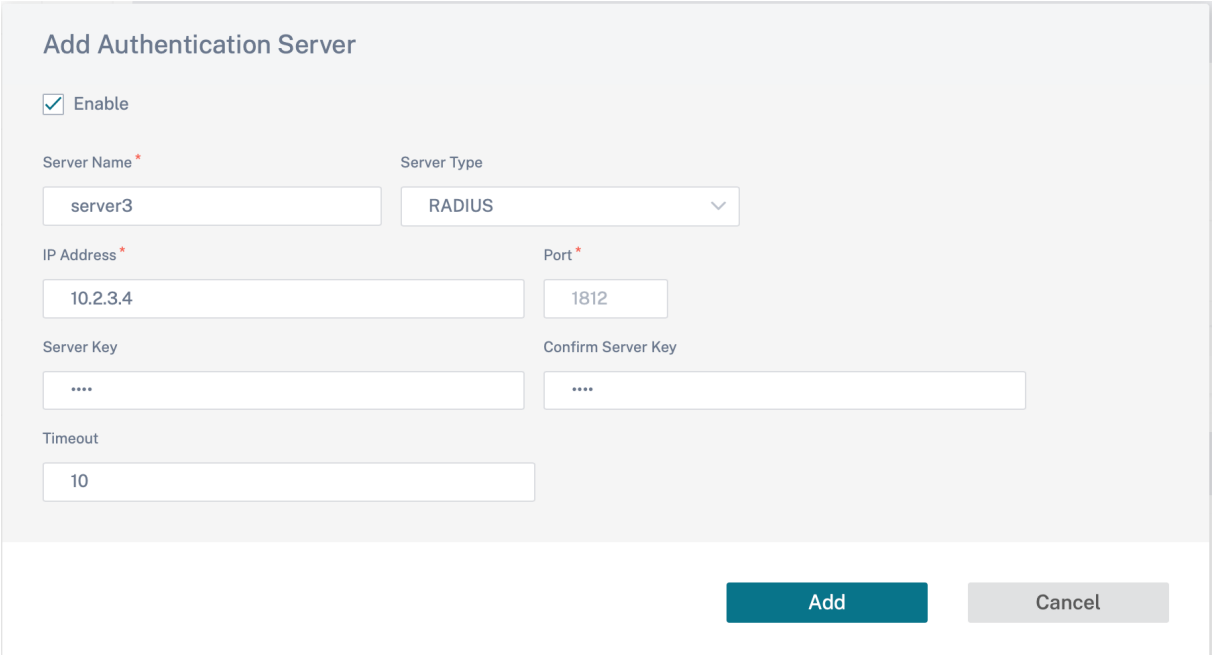
> **REMARQUE**
>
> Assurez-vous que les comptes utilisateur requis sont créés sur le serveur d'authentification RADIUS ou TACACS+.



Pour configurer l'authentification à distance, accédez à **Infrastructure > Administration de l'orchestrateur > Paramètres de gestion > Serveurs d'authentification à distance**. Cliquez sur **+ Nouveau**. Entrez les informations suivantes :

- **Activer** : active la configuration du serveur d'authentification à distance.
- **Nom du serveur** : nom du serveur d'authentification à distance.
- **Type de serveur** : type de serveur d'authentification à distance : RADIUS ou TACACS+.
- **Adresse IP : adresse**IP de l'hôte pour le serveur d'authentification à distance.
- **Port** : numéro de port du serveur d'authentification à distance. Le port par défaut pour le serveur RADIUS est 1812 et le port 49 pour le serveur TACACS+.
- Clé de **serveur et**clé**de confirmation du serveur** : clé secrète à utiliser lors de la connexion au serveur d'authentification distant.
- **Type d'authentification** : (disponible uniquement pour le serveur TACACS+) Sélectionnez la méthode de cryptage à utiliser pour envoyer le nom d'utilisateur et le mot de passe au serveur TACACS+.
  - **PAP** : utilise le protocole d'authentification par mot de passe (PAP) pour renforcer l'authentification des utilisateurs en attribuant un secret partagé fort au serveur TACACS+.
  - **ASCII** : utilise le jeu de caractères ASCII pour renforcer l'authentification des utilisateurs en attribuant un secret partagé fort au serveur TACACS+.

- **Délai**d'attente : intervalle de temps (en secondes) pendant lequel vous devez attendre une réponse d'authentification de la part du serveur d'authentification distant.



Vous pouvez également tester la connexion au serveur distant. Sous **Tester la connexion au serveur distant**, saisissez votre **nom d'utilisateur** et votre **mot de passe** Sélectionnez le serveur d'authentification à distance et cliquez sur **Vérifier**.

Gestion de la base

Vous pouvez créer une sauvegarde de la base de données actuelle exécutée sur Citrix SD-WAN Orchestrator for On-premises et utiliser ultérieurement le fichier sauvegardé pour restaurer le même état de base de données.

> **Remarque**
>
> - Dans une configuration gérée par un fournisseur, seuls les administrateurs du fournisseur peuvent créer une sauvegarde de base de données et la restaurer.
> - Vous ne pouvez pas restaurer la sauvegarde de base de données effectuée dans une configuration gérée par le fournisseur sur une configuration gérée par le client. De même, vous ne pouvez pas restaurer la sauvegarde de base de données effectuée dans une configuration gérée par le client sur une configuration gérée par le fournisseur.

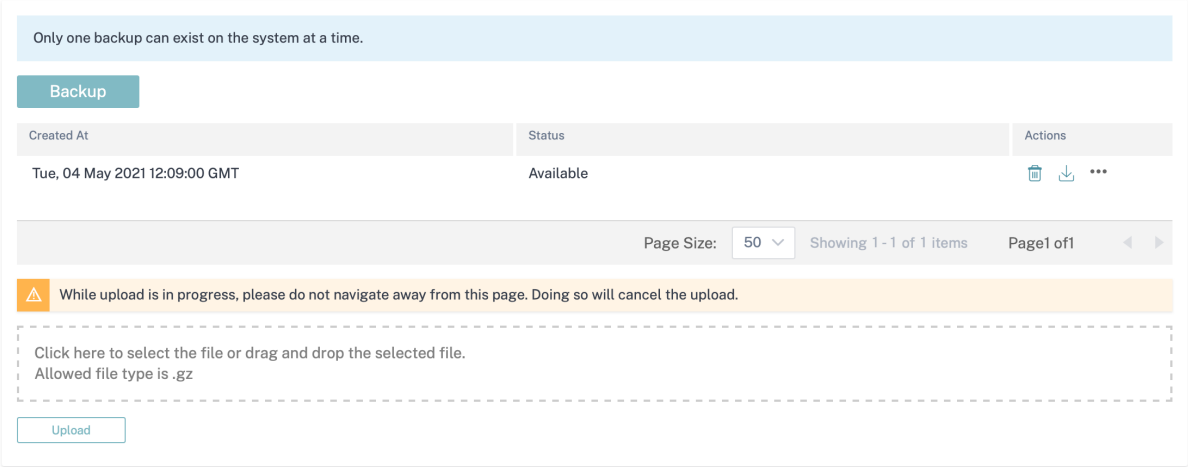
Pour créer une sauvegarde de base de données, accédez à **Infrastructure** > **Administration de l'orchestrateur** > **Gestion des bases de données**. Cliquez sur **Sauvegarde**.

Cliquez sur Télécharger dans la colonne **Actions** pour télécharger la base de données sauvegardée.

Cliquez sur **Télécharger** pour parcourir et télécharger le fichier téléchargé. Vous pouvez également faire glisser le fichier téléchargé et le déposer sur l'écran.

Pour restaurer, cliquez sur **Restaurer** dans la colonne **Actions** .

> **REMARQUE**
>
> - Vous ne pouvez enregistrer qu'une seule sauvegarde de base de données à la fois. Pour remplacer une sauvegarde existante par la plus récente, supprimez la sauvegarde existante et cliquez sur **Sauvegarder**.
> - La restauration de la base de données doit être effectuée vers la même version de Citrix SD-WAN Orchestrator for On-premises à partir de laquelle la sauvegarde des données a été effectuée.
> - La sauvegarde de la base de données se limite à la sauvegarde de la configuration et des statistiques. Il ne sauvegarde pas les données relatives à la plateforme.



Gestion du stockage

Citrix SD-WAN Orchestrator pour locaux prend en charge la migration des configurations client, des statistiques, de la base de données locale et de la version publiée de Citrix SD-WAN d'un disque existant vers un nouveau disque.

Dans une configuration gérée par un fournisseur, seuls les administrateurs du fournisseur peuvent effectuer la migration du disque. Les administrateurs clients de la configuration gérée par le fournisseur ne disposent pas des privilèges nécessaires pour effectuer la migration de disques. Dans une configuration gérée par le client, les administrateurs clients peuvent effectuer une migration de disque.

Vous pouvez effectuer une migration de disque pour augmenter l'espace disque ou pour une reprise après sinistre.

- **Ajouter un nouveau disque** : vous pouvez ajouter un nouveau disque dont la taille de stockage est au moins deux fois supérieure à celle des données actuelles consommées par Citrix SD-WAN Orchestrator for On-premises. Grâce à Citrix SD-WAN Orchestrator pour l'interface utilisateur locale, vous pouvez activer le nouveau disque et migrer les configurations client existantes, les statistiques, la base de données locale et la version publiée de Citrix SD-WAN. Une fois que le disque nouvellement ajouté est activé, Citrix SD-WAN Orchestrator for On-premises est redémarré.
- **Reprise après sinistre** : en cas de sinistre, vous pouvez associer le disque contenant les données à une nouvelle instance de Citrix SD-WAN Orchestrator pour machine virtuelle sur site qui se trouve sur la même version de Citrix SD-WAN Orchestrator pour locaux. Activez le disque sans choisir l'option **Migrer les données** dans l'interface utilisateur Citrix SD-WAN Orchestrator for On-premises. Une fois le disque activé, Citrix SD-WAN Orchestrator for On-premises est redémarré.

> **REMARQUE**
>
> - Lorsque la migration de disque est en cours, n'éteignez pas et ne redémarrez pas manuellement Citrix SD-WAN Orchestrator pour locaux. La mise hors tension ou le redémarrage manuel peuvent entraîner une perte de données.
> - Lorsqu'un disque est migré d'une partition de disque ajoutée précédemment vers une partition de disque nouvellement créée, les données de l'ancien disque ne sont pas supprimées après la migration. Pour supprimer les données de l'ancien disque, connectez-le à un autre système d'exploitation et supprimez les données de manière sécurisée.

Limitations

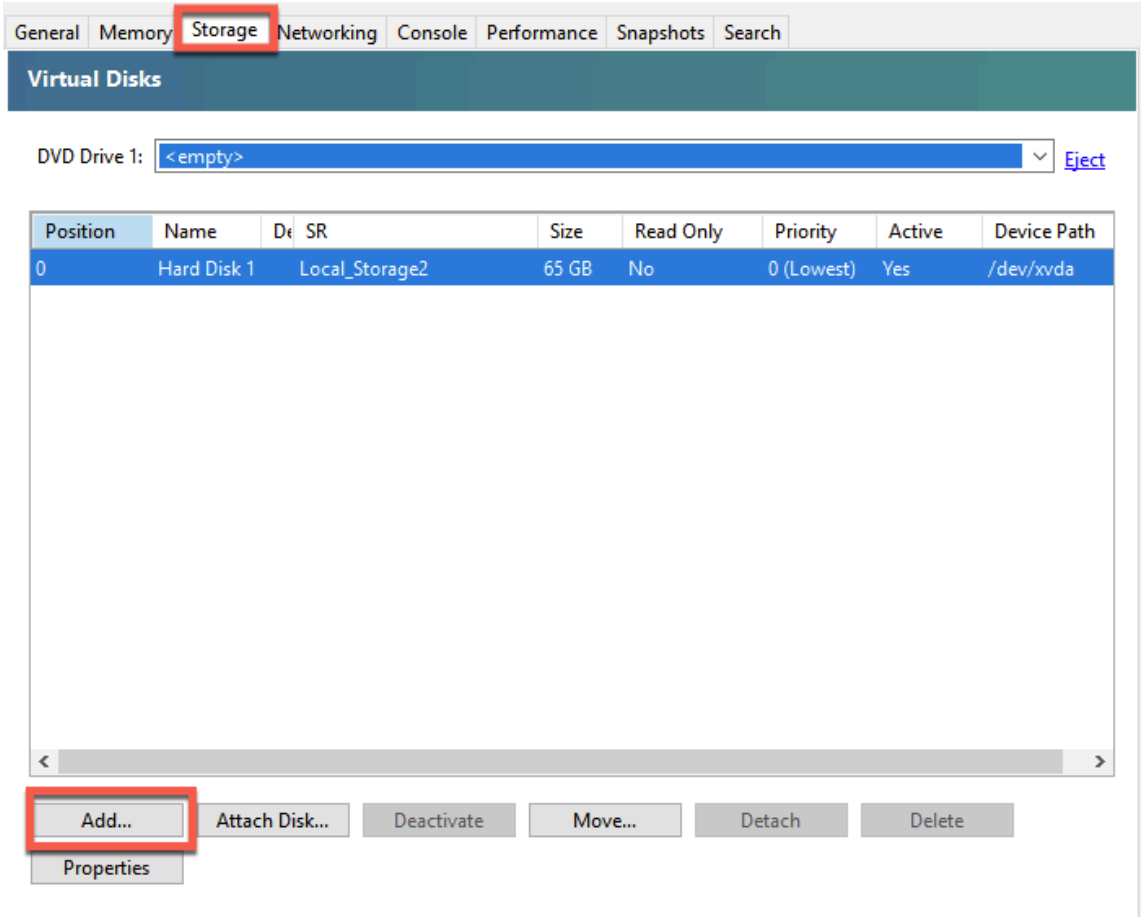
Les limites du processus de migration de disque sont les suivantes :

- Les utilisateurs de l'ancienne version ne sont pas migrés vers la nouvelle version. Après la migration, supprimez les utilisateurs et créez-les à nouveau.
- Le STS créé sur l'ancien Citrix SD-WAN Orchestrator pour machine virtuelle locale n'est pas migré. Toutefois, après la migration, l'interface utilisateur répertorie les STS générés sur l'ancien Citrix SD-WAN Orchestrator pour machine virtuelle sur site. Supprimez le STS manuellement.
- La sauvegarde de base de données créée dans l'ancien Citrix SD-WAN Orchestrator pour locaux n'est pas migrée. Après la migration, s'il est répertorié, supprimez-le manuellement.
- Par défaut, il est supposé que le nouveau Citrix SD-WAN Orchestrator pour site local vers lequel le disque est migré est connecté aux serveurs d'authentification à deux facteurs. Si le compte administrateur utilise des serveurs d'authentification à deux facteurs et si les connexions aux serveurs d'authentification à deux facteurs ne sont pas disponibles, même l'administrateur ne peut pas se connecter. Dans de tels scénarios, contactez le support Citrix.

- Après avoir migré vers le nouveau disque, vous ne pouvez pas augmenter l'espace disque alloué à Citrix SD-WAN Orchestrator for On-premises.
- Dans le scénario de reprise après sinistre, vous devez reconfigurer le domaine personnalisé après avoir activé le disque.
- Dans le scénario de reprise après sinistre, après avoir activé le disque, vous devez soit effectuer un déploiement Zero Touch hors cloud, soit un déploiement Zero Touch négocié dans le cloud pour établir la connectivité entre les appliances Citrix SD-WAN sur les sites avec Citrix SD-WAN Orchestrator for On-premises.

Ajouter un nouveau disque sur Citrix Hypervisor

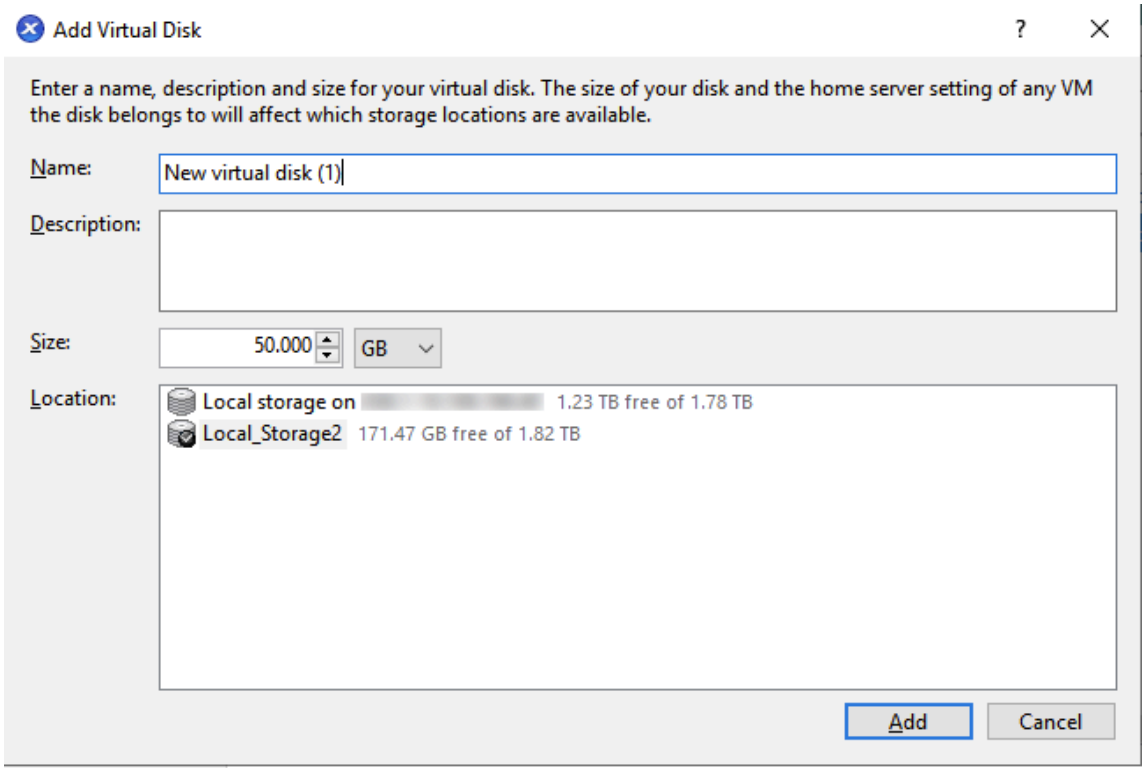
1. Sélectionnez la machine virtuelle (VM) dans l'hyperviseur. Sélectionnez l'onglet **Stockage** et cliquez sur **Ajouter**.

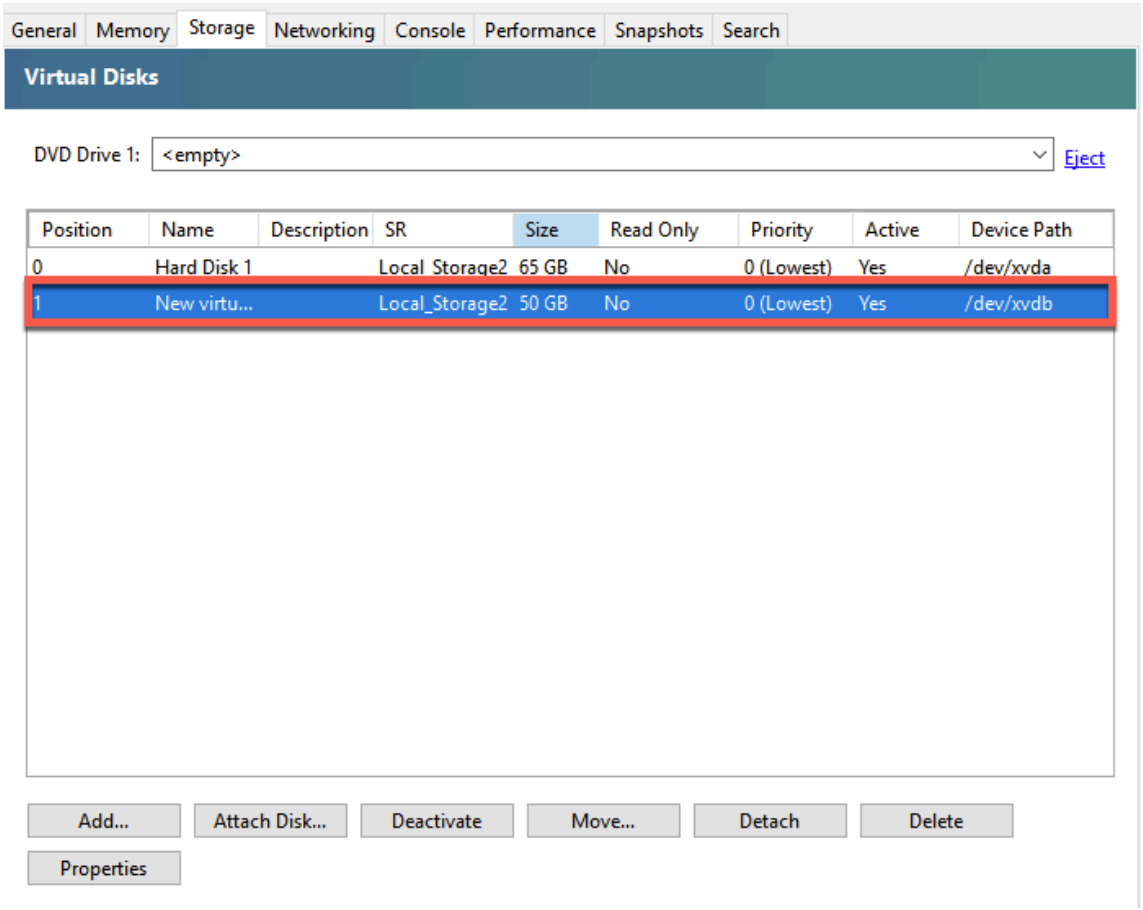


2. Fournissez des informations telles que le nom, la description, la taille et l'emplacement du nouveau disque. Cliquez sur **Ajouter**. Le disque que vous venez d'ajouter est répertorié sous l'onglet **Stockage** .

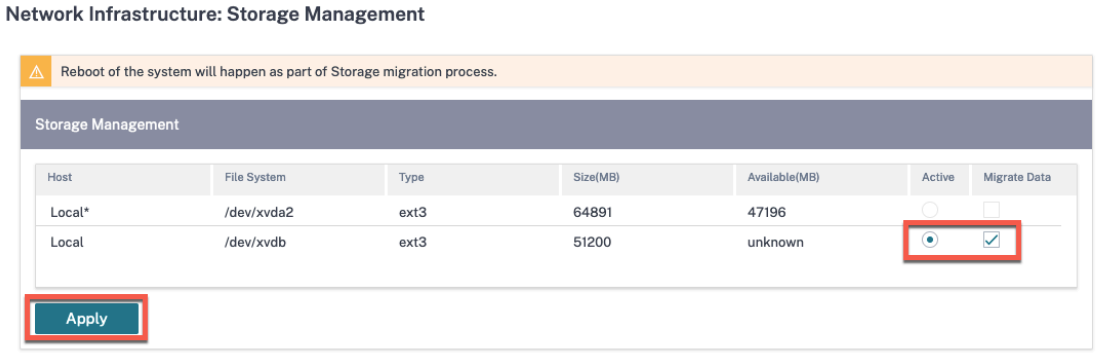
REMARQUE

La taille du disque doit être au moins deux fois supérieure à celle des données actuelles consommées par Citrix SD-WAN Orchestrator for On-premises.

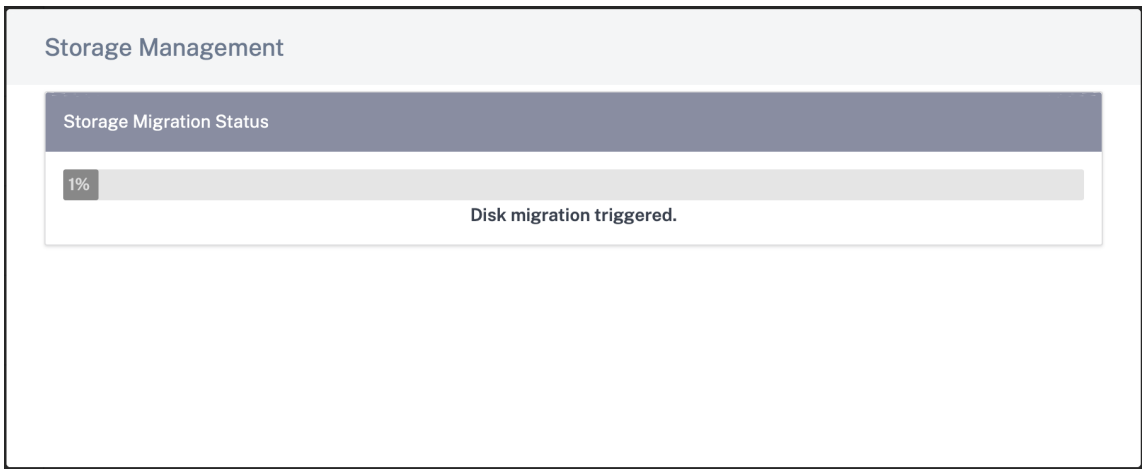


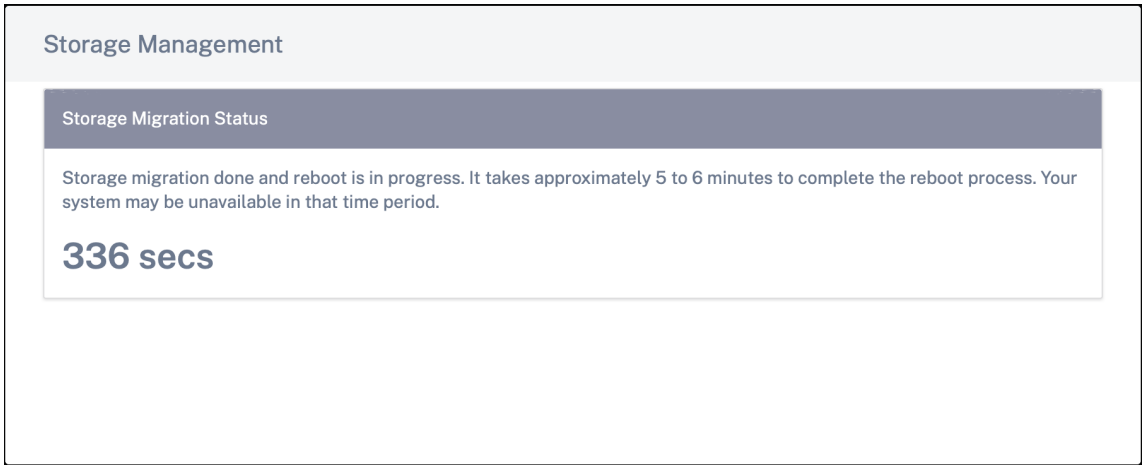


3. Connectez-vous à l'interface utilisateur Citrix SD-WAN Orchestrator pour site et accédez à **INFRASTRUCTURE > Administration d'Orchestrator > Gestion du stockage**. Le disque nouvellement connecté est automatiquement répertorié sous **Gestion du stockage**.
4. Cliquez sur le bouton radio **Active** et cochez la case **Migrer les données** . Cliquez sur **Appliquer**.



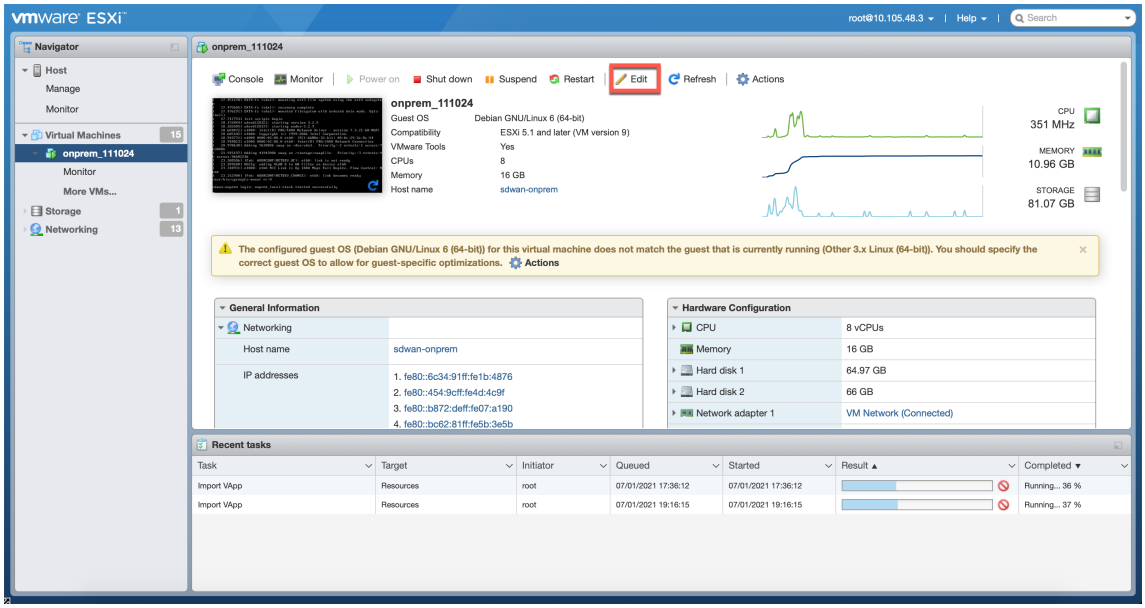
5. Le processus de migration du disque est déclenché. Les configurations client, les statistiques, la base de données locale et la version de version de Citrix SD-WAN sur le disque existant sont migrées vers le nouveau disque. Une fois la migration terminée, Citrix SD-WAN Orchestrator pour locaux est redémarré.



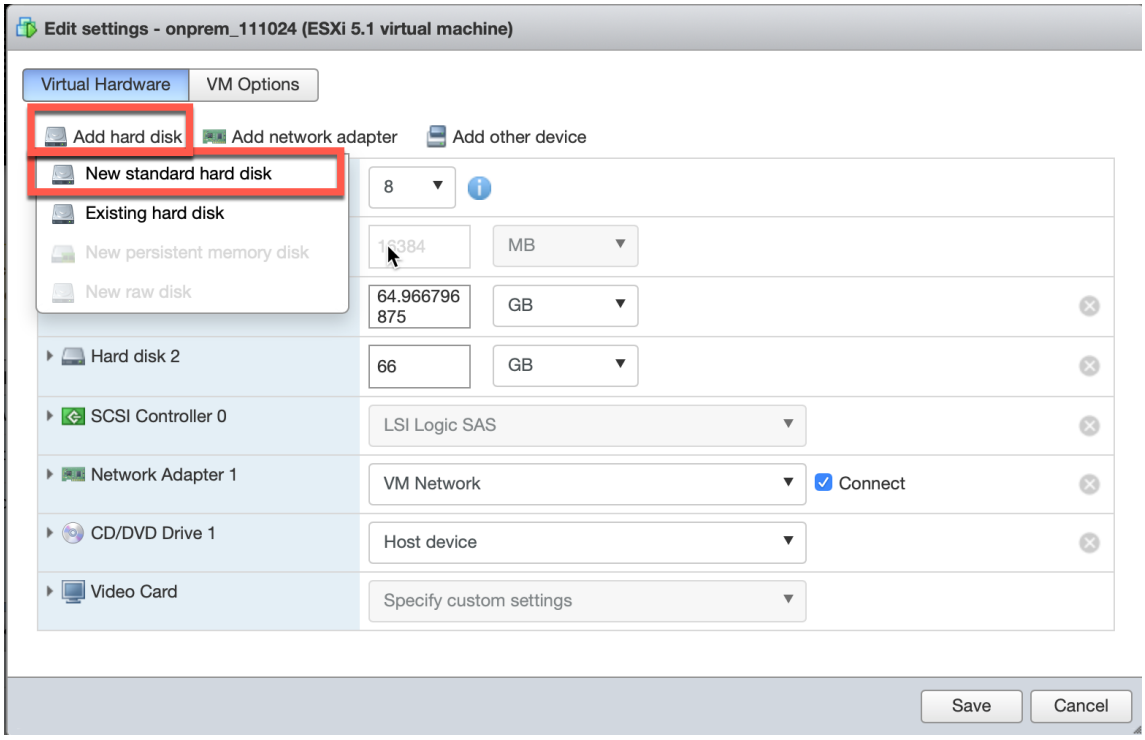


Ajouter un nouveau disque sur le serveur ESXi

1. Connectez-vous à votre serveur ESXi et sélectionnez la machine virtuelle. Cliquez sur **Modifier**.

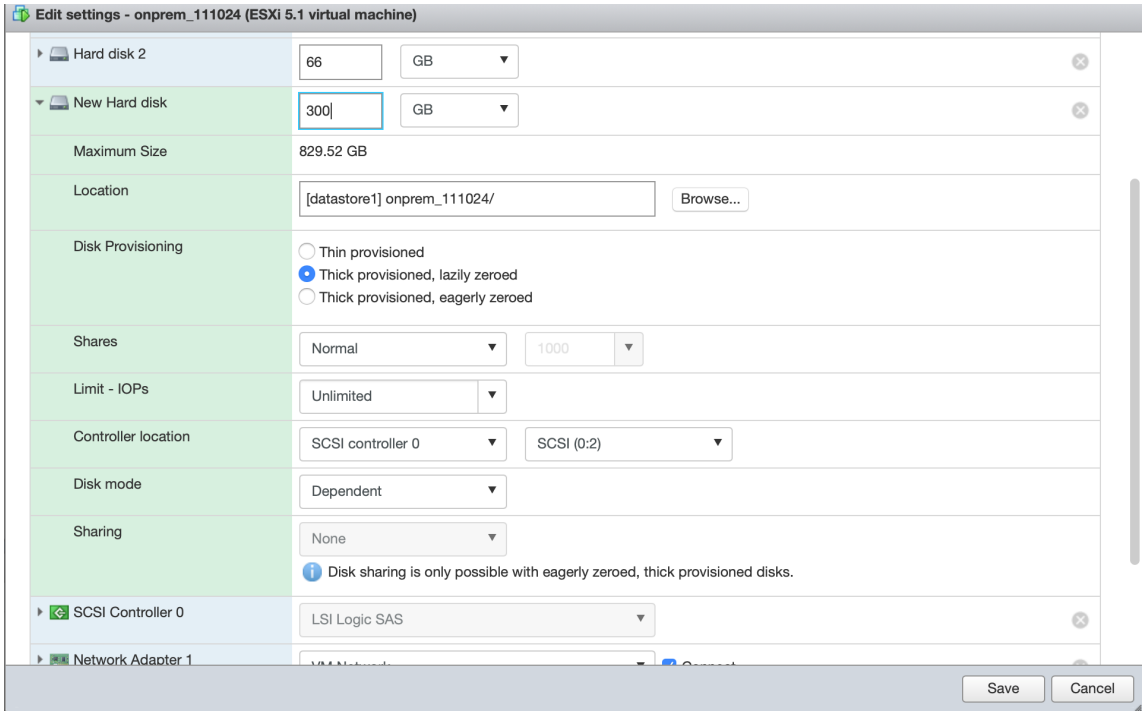


2. Cliquez sur **Ajouter un disque dur > Nouveau disque dur standard**.

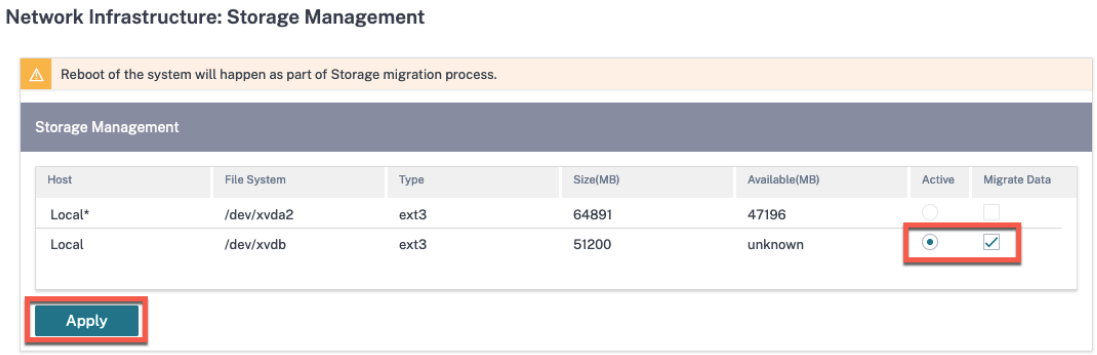


3. Entrez l'espace de stockage sur disque et les autres paramètres en fonction de vos préférences. Cliquez sur **Enregistrer**.

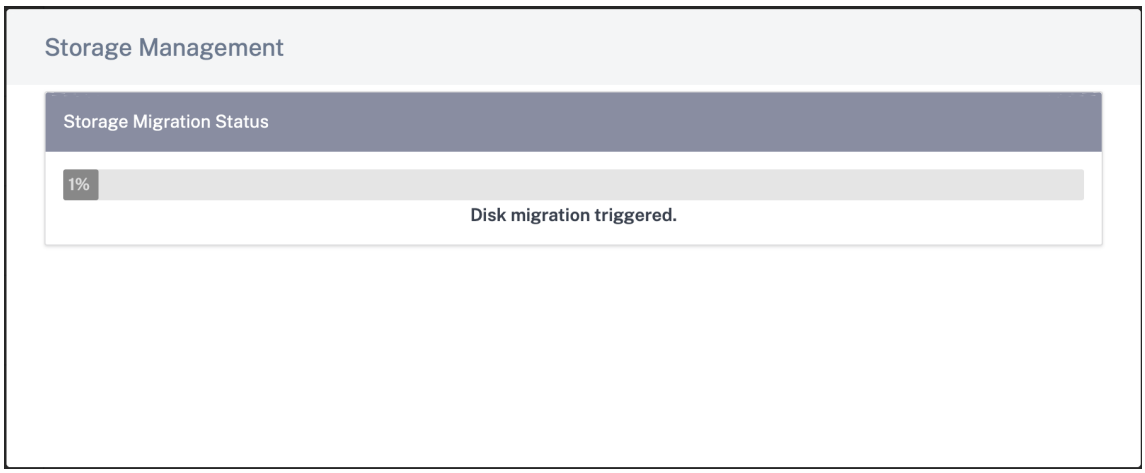
> **REMARQUE**
>
> La taille du disque doit être au moins deux fois supérieure à celle des données actuelles consommées par Citrix SD-WAN Orchestrator for On-premises.

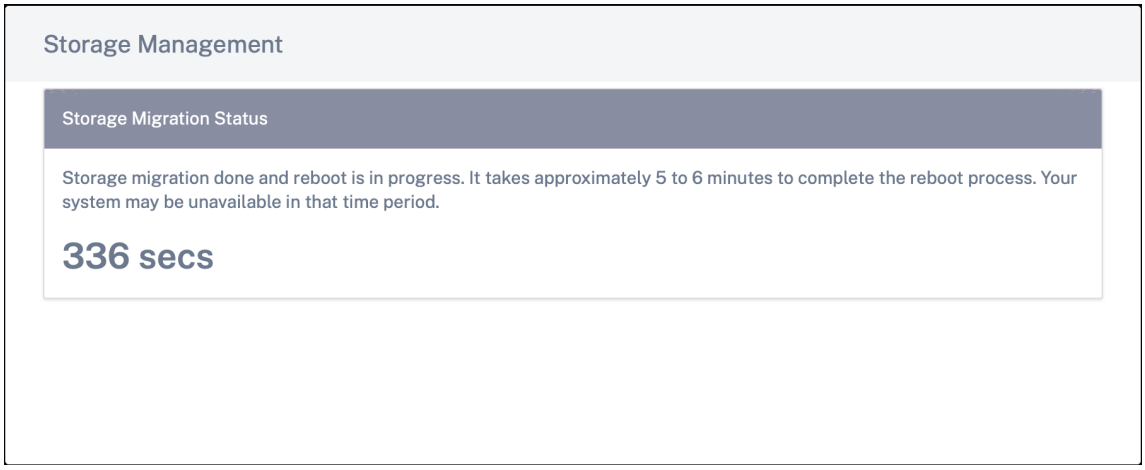


4. Connectez-vous à Citrix SD-WAN Orchestrator pour les applications locales et accédez à **INFRASTRUCTURE > Administration de l'orchestrateur > Gestion du stockage**. Le disque nouvellement connecté est répertorié ici.
5. Cliquez sur le bouton radio **Active** et cochez la case **Migrer les données** . Cliquez sur **Appliquer**.



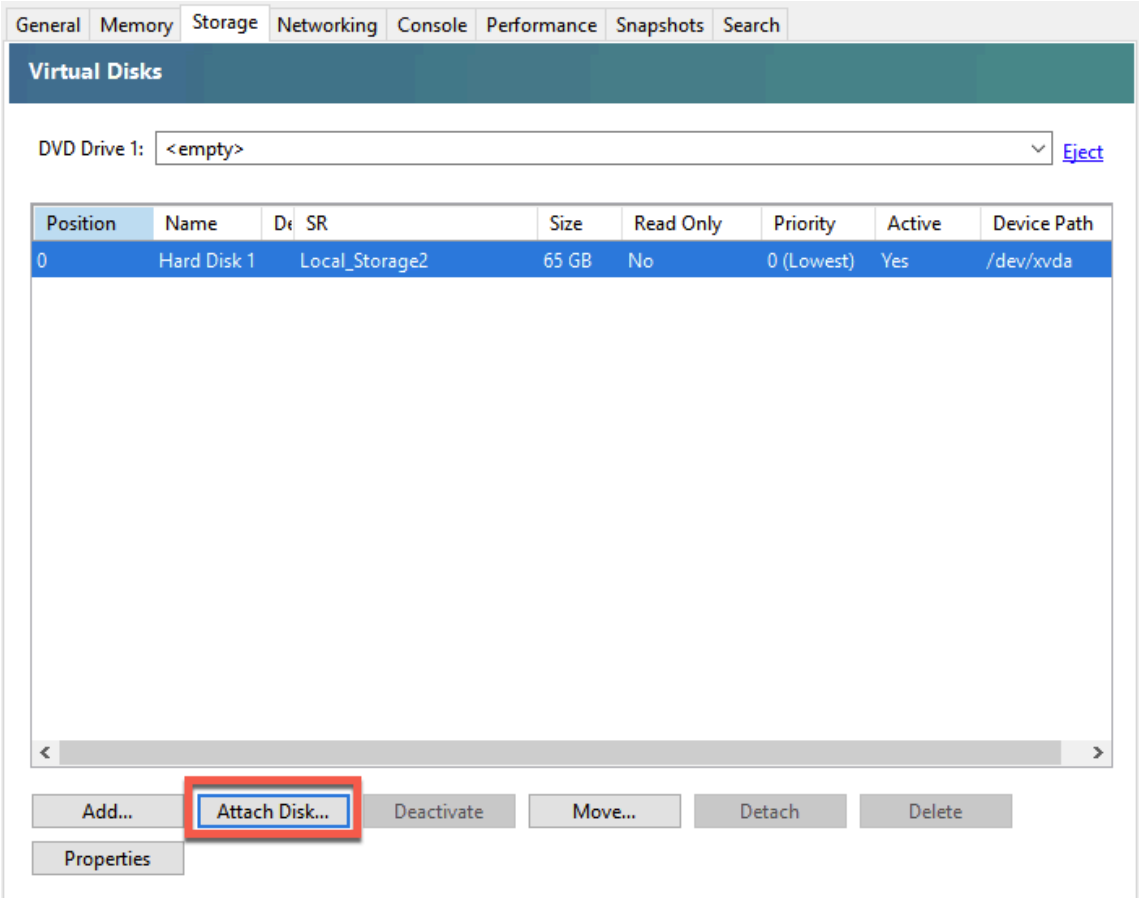
6. Le processus de migration du disque est déclenché. Les configurations client, la base de données locale, la version de Citrix SD-WAN et les statistiques de base de données sur le disque existant sont migrées vers le nouveau disque. Une fois la migration terminée, Citrix SD-WAN Orchestrator pour locaux est redémarré.





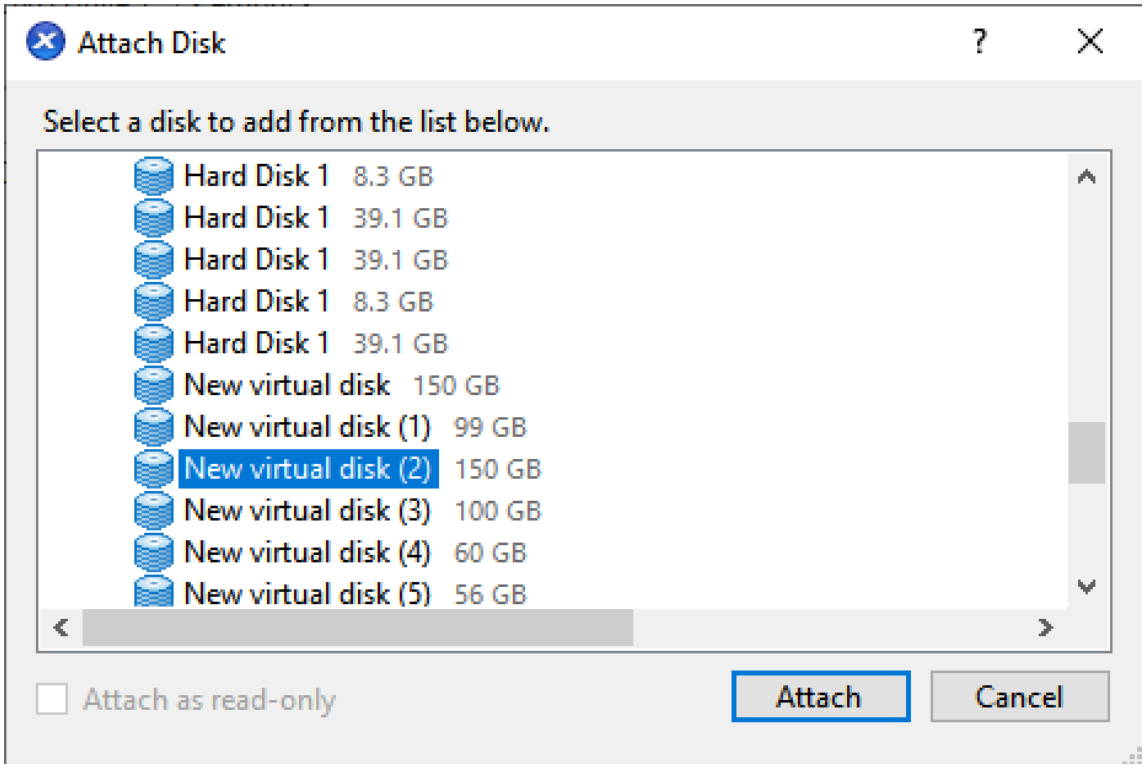
Reprise après sinistre sur Citrix Hypervisor

1. Sélectionnez la machine virtuelle (VM) dans l'hyperviseur. Sélectionnez l'onglet **Stockage** et cliquez sur **Joindre un disque**.



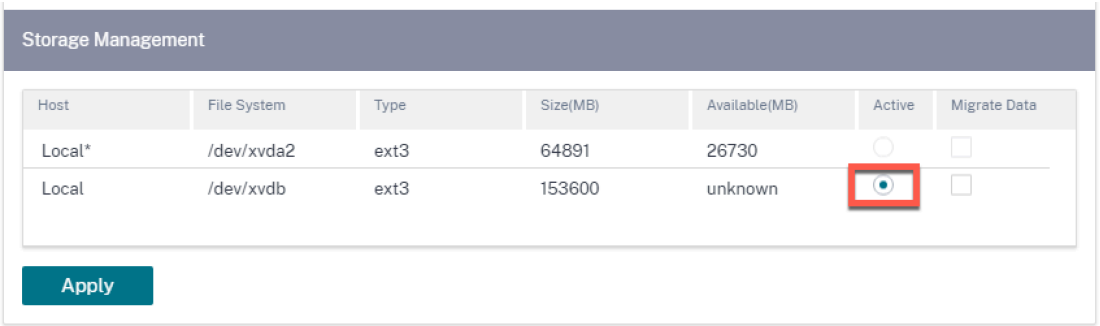
2. Sélectionnez le disque connecté au Citrix SD-WAN Orchestrator for On-premises qui survient en cas de sinistre et cliquez sur **Joindre**.

   Si le disque n'est pas répertorié, assurez-vous que le disque connecté à Citrix SD-WAN Orchestrator pour locaux qui a provoqué un sinistre est détaché et que Citrix SD-WAN Orchestrator pour locaux est en état d'arrêt.

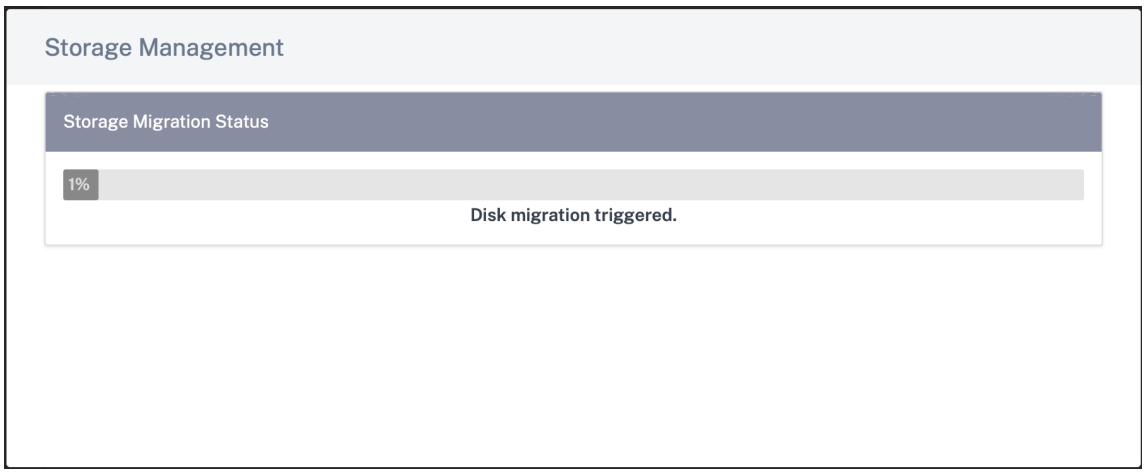


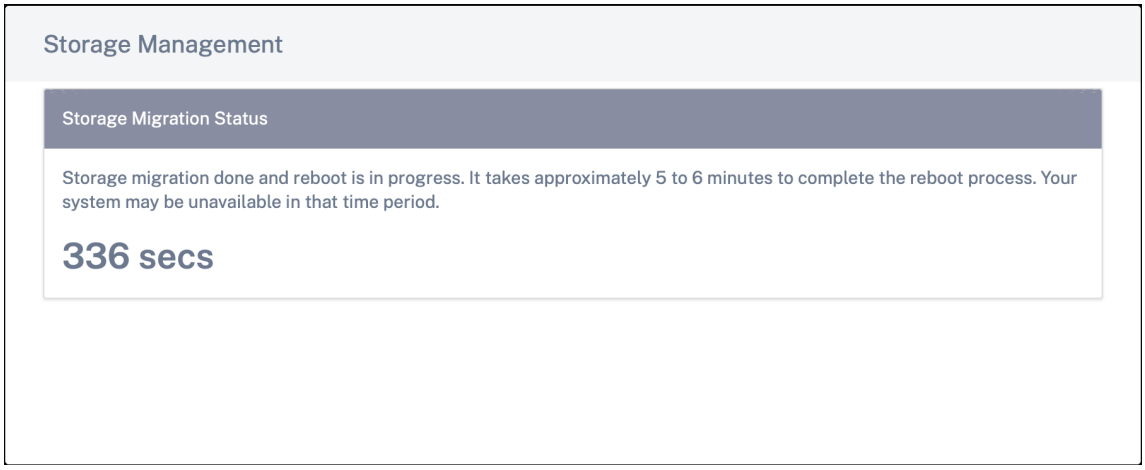
3. Connectez-vous à l'interface utilisateur Citrix SD-WAN Orchestrator pour site et accédez à **INFRASTRUCTURE > Administration d'Orchestrator > Gestion du stockage**. Le disque nouvellement connecté est répertorié ici.
4. Choisissez uniquement le bouton radio **Actif** (désactivez la case à cocher **Migrer les données** si cette case est sélectionnée) et cliquez sur **Appliquer**.

> **Remarque**
>
> Ne cochez pas la case **Migrer les données** . Citrix SD-WAN Orchestrator pour locaux déclenche la migration au niveau du back-end et redémarre automatiquement une fois la migration terminée.



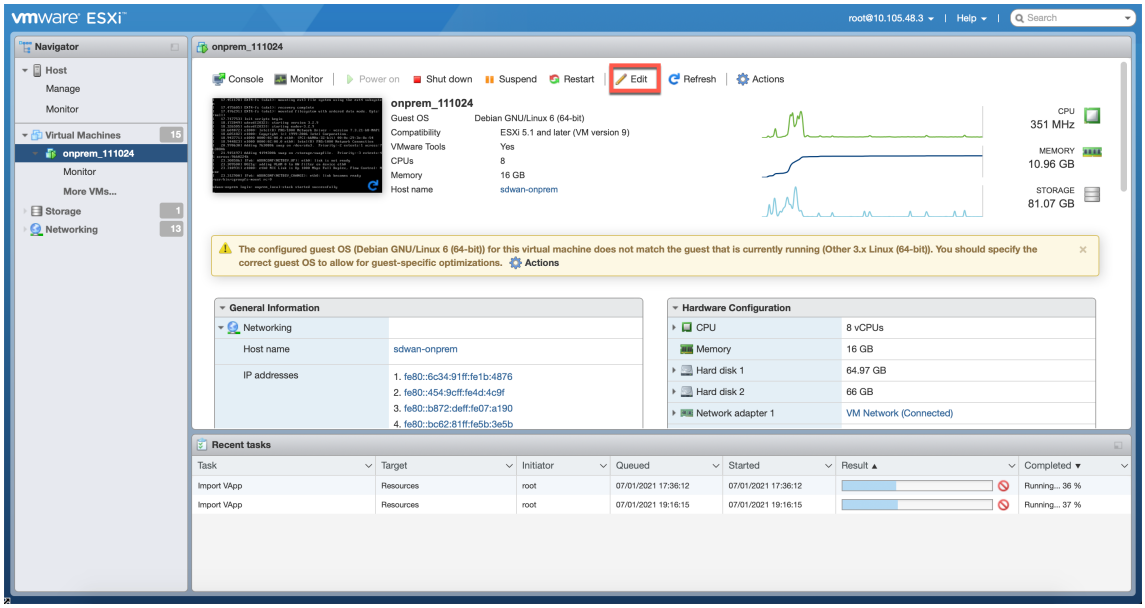
5. Une fois la migration terminée, Citrix SD-WAN Orchestrator pour locaux est redémarré.



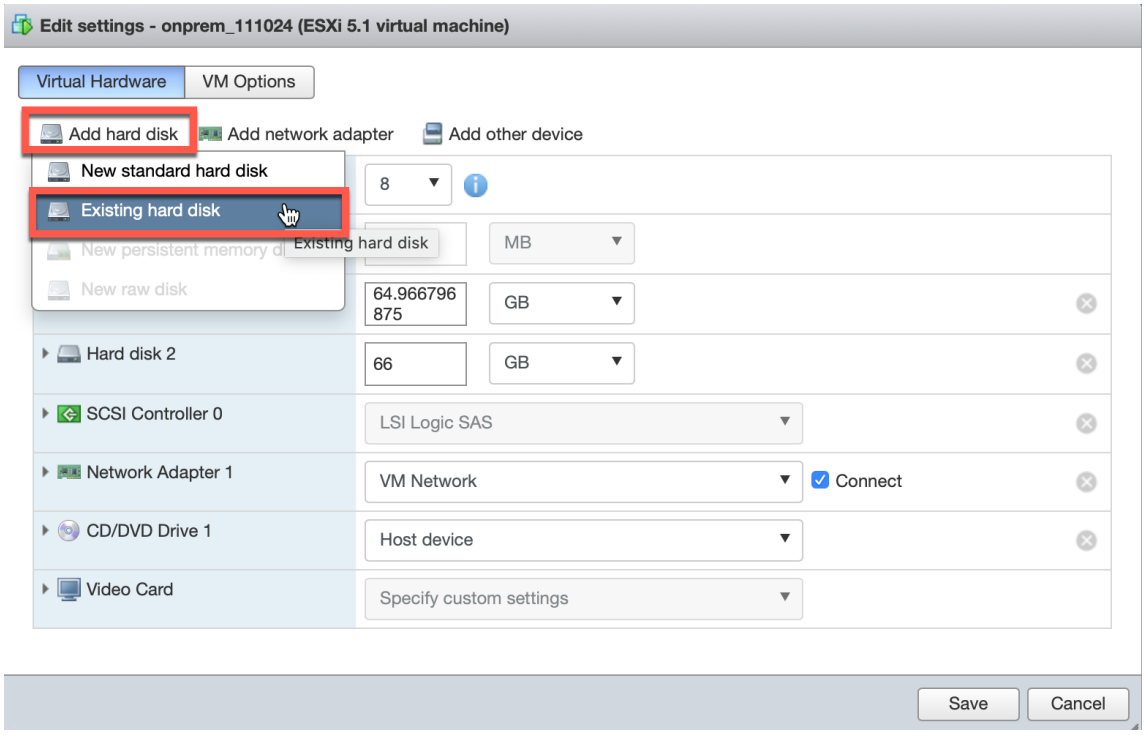


Reprise après sinistre sur le serveur ESXi

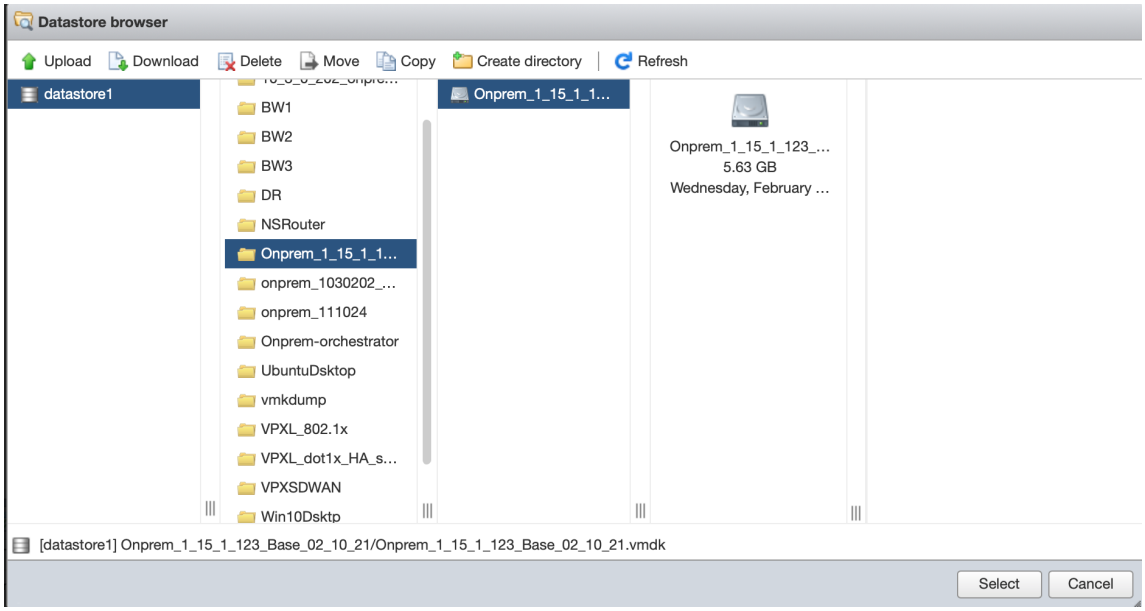
1. Connectez-vous au serveur ESXi et sélectionnez la machine virtuelle. Cliquez sur **Modifier**.



2. Cliquez sur **Ajouter un disque dur > Disque dur existant**.

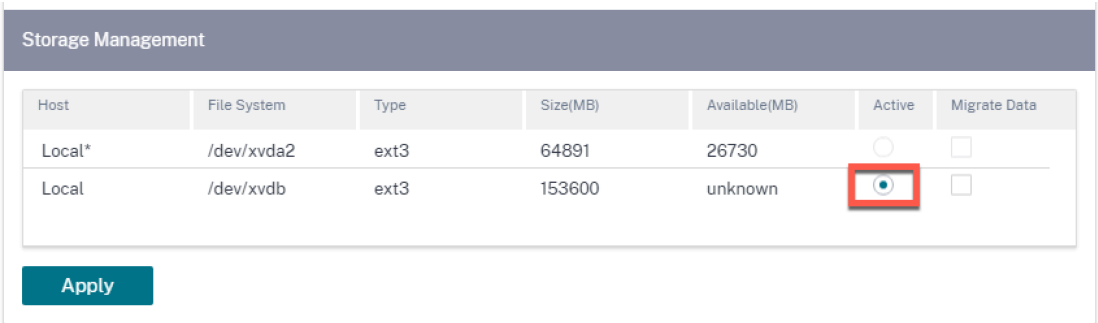


3. Recherchez le disque connecté au Citrix SD-WAN Orchestrator for On-premises qui a connu un sinistre et cliquez sur **Sélectionner**.

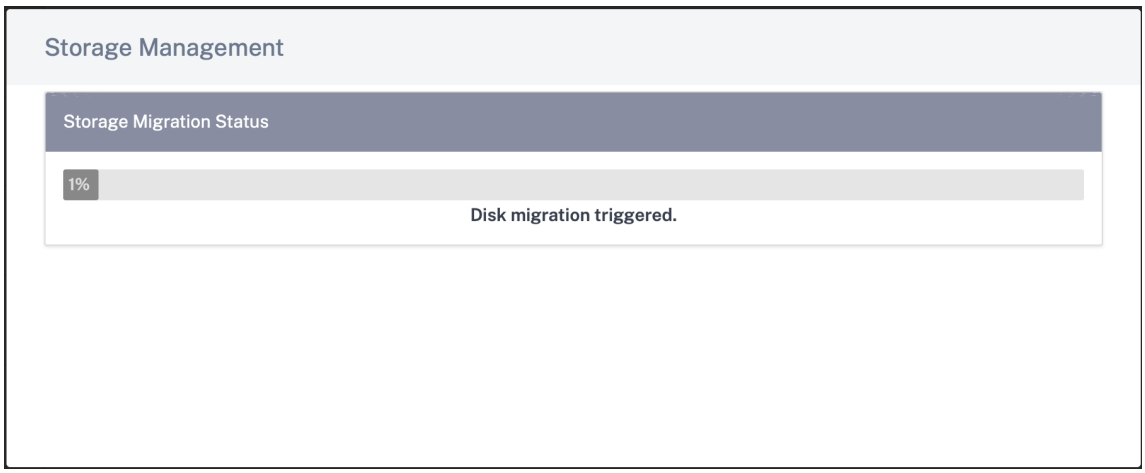


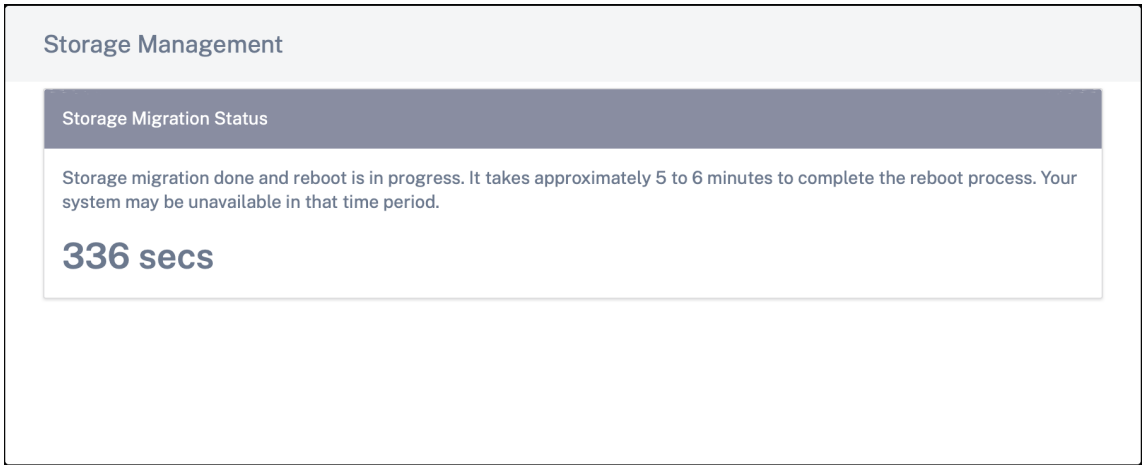
4. Connectez-vous à l'interface utilisateur Citrix SD-WAN Orchestrator pour site et accédez à **INFRASTRUCTURE > Administration d'Orchestrator > Gestion du stockage**. Le disque nouvellement connecté est répertorié ici.
5. Choisissez uniquement le bouton radio **Actif** (désactivez la case à cocher **Migrer les données** si cette case est sélectionnée) et cliquez sur **Appliquer**.

> **Remarque**
>
> Ne cochez pas la case **Migrer les données** . Citrix SD-WAN Orchestrator pour locaux déclenche la migration au niveau du back-end et redémarre automatiquement une fois la migration terminée.



6. Une fois la migration terminée, Citrix SD-WAN Orchestrator pour locaux est redémarré.





Proxy HTTP

Citrix SD-WAN Orchestrator pour locaux nécessite une connexion Internet pour les licences, la connexion au cloud, le ZTD négocié dans le cloud, Cloud direct et les logiciels de publication. Si Citrix SD-WAN Orchestrator pour locaux est connecté à Internet via un serveur proxy HTTP, vous pouvez configurer les paramètres du serveur proxy HTTP sur votre machine virtuelle Citrix SD-WAN Orchestrator pour machine virtuelle locale.

Le paramètre de proxy HTTP centralise la gestion de toutes les demandes sortantes adressées à Citrix Cloud. Les administrateurs peuvent acheminer les demandes sortantes depuis Citrix SD-WAN Orchestrator pour site local vers Citrix Cloud via un serveur proxy HTTP.

Avant de commencer

Pour utiliser le proxy HTTP pour la première connexion au cloud, vous devez configurer les paramètres du proxy HTTP via la console CLI de Citrix SD-WAN Orchestrator for On-premises.

Sur la page de connexion au cloud d'un nouveau Citrix SD-WAN Orchestrator pour machine virtuelle locale, si vous souhaitez que le proxy HTTP soit utilisé pour toutes les connexions sortantes entre Citrix SD-WAN Orchestrator pour site et le service Citrix SD-WAN Orchestrator, vous devez configurer les détails du proxy HTTP à l'aide de l'interface de ligne de commande. Une fois que la connexion au Cloud est terminée et que vous accédez à la page de configuration, vous pouvez configurer les détails du serveur proxy HTTP sur l'interface utilisateur.

Configuration des paramètres du proxy HTTP sur la CLI

Configurez les paramètres du proxy HTTP en exécutant la `set_http_proxy` commande. Vous pouvez configurer le proxy HTTP à l'aide de l'une des options ci-dessous :

- Lorsque l'authentification est activée sur le serveur proxy :

  ```
  set <ip address> <port> <user name> <password>
  ```

- Lorsque l'authentification n'est pas activée sur le serveur proxy :

  ```
  set <ip address> <port>
  ```

Afficher les paramètres du proxy HTTP

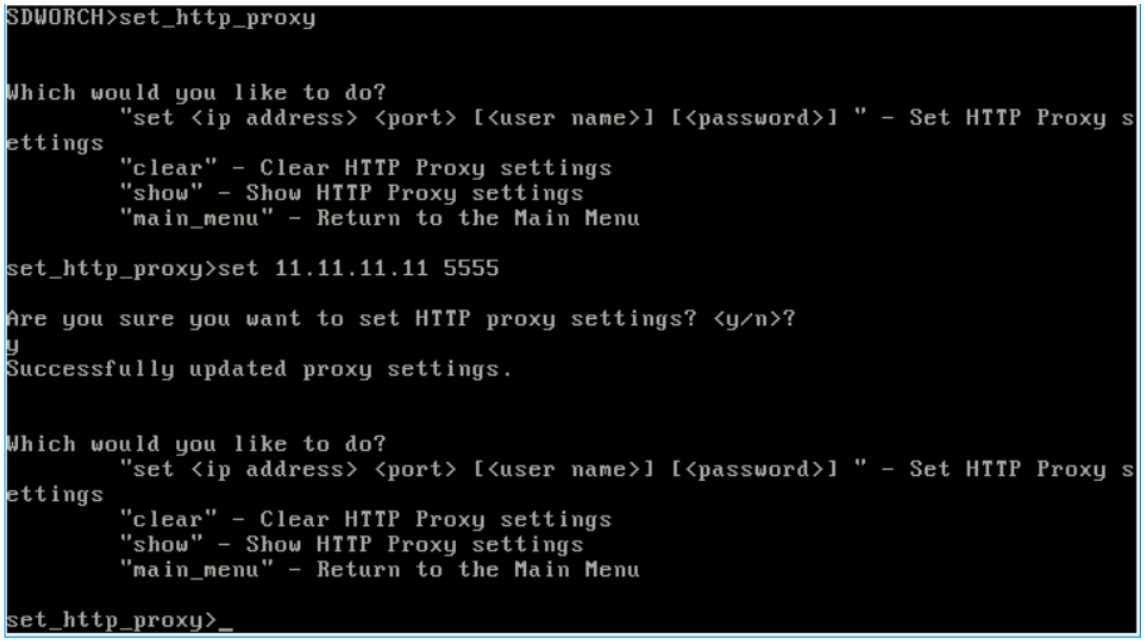
- `show`: Cette commande affiche les paramètres du proxy sur l'interface de ligne de commande. La sortie n'affiche pas le mot de passe.

Effacer les paramètres du proxy HTTP

- `clear`: Cette commande supprime les paramètres du proxy HTTP.

Retourner au menu principal

- `main_menu`: Cette commande vous redirige vers la console CLI de Citrix SD-WAN Orchestrator for On-premises.



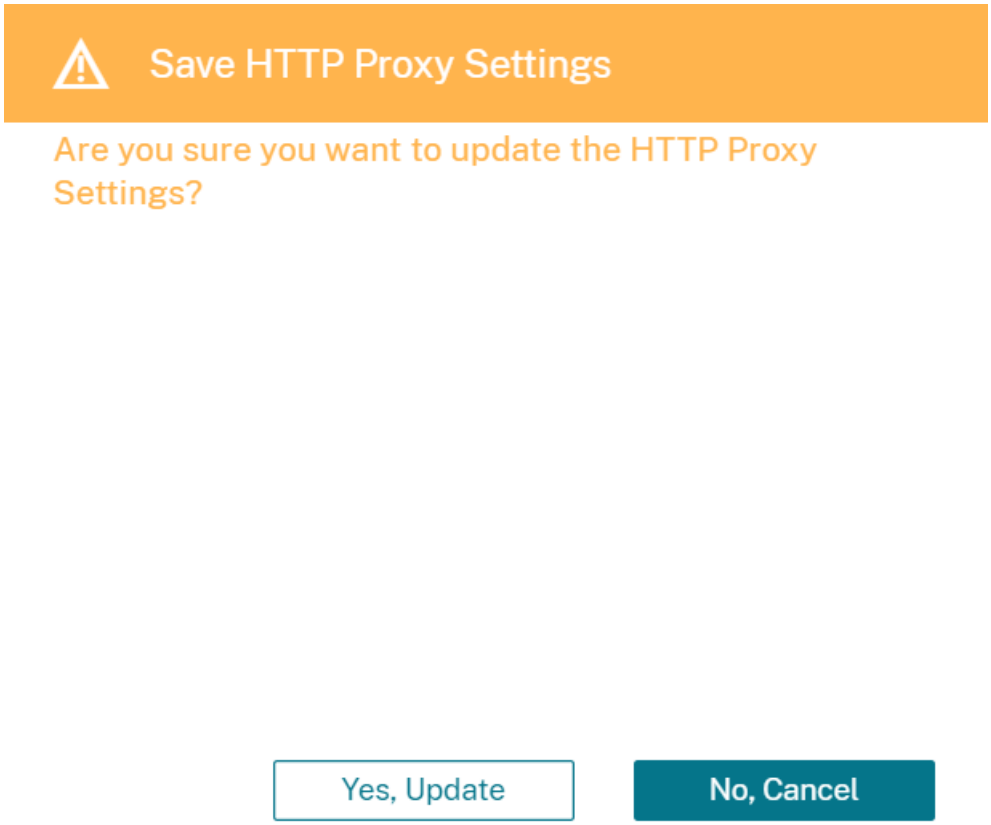
Configuration des paramètres du serveur proxy HTTP sur l'interface utilisateur

1. Connectez-vous à l'interface utilisateur Citrix SD-WAN Orchestrator pour site et accédez à **Infrastructure** > **Administration de l'orchestrateur** > **Proxy HTTP**.
2. Dans la section **Infrastructure réseau : proxy HTTP**, entrez des valeurs pour les champs suivants :

   - **Adresse IP** : adresse IP du serveur proxy.
   - **Port** : numéro de port réseau sur lequel le serveur proxy accepte les connexions.
   - **Nom d'**utilisateur : nom d'utilisateur du serveur proxy.
   - **Mot de passe** : mot de passe du serveur proxy.

   > **Remarque**
   >
   > Vous pouvez laisser les champs Nom d'utilisateur et Mot de passe vides si aucune authentification n'est configurée sur le serveur proxy.

3. Cliquez sur Appliquer. Une boîte de dialogue de confirmation s'affiche.
4. Cliquez sur Oui, mettre à jour.



Remarques

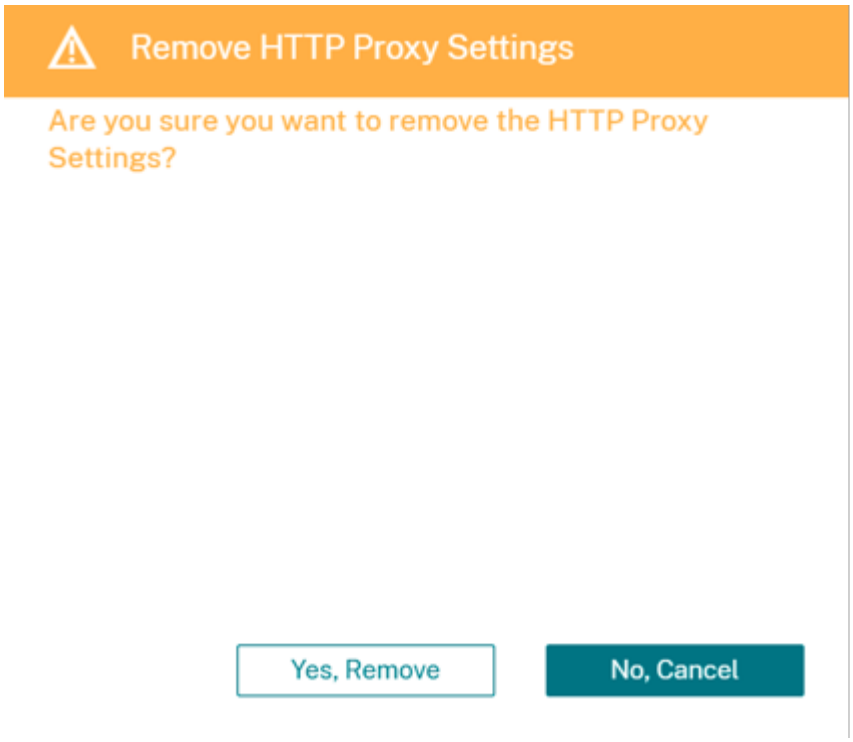
- Pour utiliser le serveur proxy HTTP pour le trafic sortant de Citrix SD-WAN Orchestrator pour site vers Citrix Cloud, le serveur proxy doit être configuré comme un proxy HTTP

SSL transparent ou un serveur proxy HTTP de contournement SSL. Le serveur ne doit pas usurper le certificat SSL du service Citrix SD-WAN Orchestrator.

- Vous pouvez supprimer complètement les paramètres du serveur proxy si Citrix SD-WAN Orchestrator for On-premises est connecté directement à Internet. Vous pouvez également supprimer les paramètres du serveur proxy et configurer un autre serveur proxy, si nécessaire.

Supprimer les paramètres du serveur proxy sur l'interface utilisateur

1. Dans l'interface utilisateur de Citrix SD-WAN Orchestrator pour site, accédez à **Infrastructure** > **Administration de l'orchestrateur** > **Proxy HTTP**.
2. Dans la section **Infrastructure réseau : proxy HTTP**, cliquez sur **Supprimer**. Une boîte de dialogue de confirmation s'affiche.
3. Cliquez sur **Oui, Supprimer**.



Paramètres de purge

Vous pouvez effacer les statistiques/données historiques pour un intervalle de temps sélectionné. Les statistiques/données plus anciennes que les jours définis sont effacées. Une fois les données effacées, elles ne sont plus disponibles. Par défaut, Citrix SD-WAN Orchestrator pour locaux efface les statistiques et les données historiques datant de plus de 30 jours.

Au niveau du réseau, accédez à **Infrastructure** > **Administration de l'orchestrateur** > **Paramètres de purge**, sélectionnez l'intervalle de temps et cliquez sur **Appliquer**. Par exemple, si vous souhaitez purger les statistiques/données historiques datant de plus de 180 jours, sélectionnez 180 dans la liste déroulante **Intervalle des statistiques de purge (jours)** et cliquez sur **Appliquer**. Le processus de purge a lieu vers 0h48 tous les jours, dans le fuseau horaire défini sur votre appliance SD-WAN.

Diagnostics d'orchestrateur

October 21, 2022

Cette section fournit des informations sur les activités de diagnostic qui peuvent être effectuées sur Citrix SD-WAN Orchestrator pour l'infrastructure sur site.

> **Remarque :**
>
> Dans une configuration gérée par un fournisseur, les administrateurs du fournisseur ont accès à toutes les pages de l'interface graphique **Infrastructure > Orchestrator Diagnostics**. Les administrateurs clients peuvent uniquement consulter les **événements et les journaux de la plate-forme, ainsi** que les pages de l'interface utilisateur graphique de **santé**

Événements et journaux de la plateforme

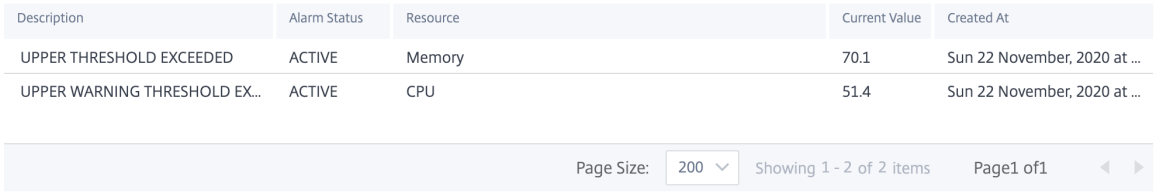
Toute modification des attributs au niveau de la plate-forme, tels que le processeur, la mémoire ou le stockage dans le système, est enregistrée en tant qu'événement et affichée sur Citrix SD-WAN Orchestrator for On-premises.

Par exemple, si l'utilisation du processeur dépasse la limite définie, un événement de plate-forme est enregistré et une alarme est déclenchée. L'alarme s'affiche dans la barre de notifications. La notification est effacée si l'utilisation du processeur diminue. La page **Événements et journaux de la plate-forme** conserve l'historique de toutes les alarmes liées à la plate-forme qui ont été déclenchées. Si l'utilisation du processeur diminue, l'état de l'alarme devient INACTIF. S'il est toujours au-dessus des limites, l'état de l'alarme reste ACTIF.

Pour afficher les événements de la plate-forme, accédez à **Infrastructure** > **Diagnostics de l'orchestrateur** > **Événements et journaux de la plate-forme**.

Les informations suivantes s'affichent pour les événements de plateforme enregistrés :

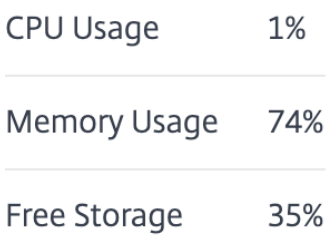
- **Description** : Description de l'événement de plateforme.
- **État de l'alarme** : état de l'alarme. Si l'attribut de plate-forme dépasse la limite définie, le statut est ACTIF. Si l'attribut au niveau de la plate-forme passe à une valeur comprise dans la limite définie, l'état de l'alarme est INACTIF.
- **Ressource** : attribut au niveau de la plate-forme : processeur, mémoire ou stockage.
- **Valeur actuelle** : dernière valeur de l'attribut de plate-forme enregistré.
- **Date de création : heure à**laquelle l'événement de plateforme s'est produit.



État de la plateforme

Vous pouvez consulter l'état de santé de Citrix SD-WAN Orchestrator pour la plate-forme sur site. Les informations de santé incluent des valeurs en temps réel (en pourcentage) pour l'utilisation du processeur, l'utilisation de la mémoire et le stockage gratuit disponible.

Pour consulter l'état de la plate-forme, accédez à **Infrastructure > Diagnostics de l'orchestrateur > État de la plate-forme**.

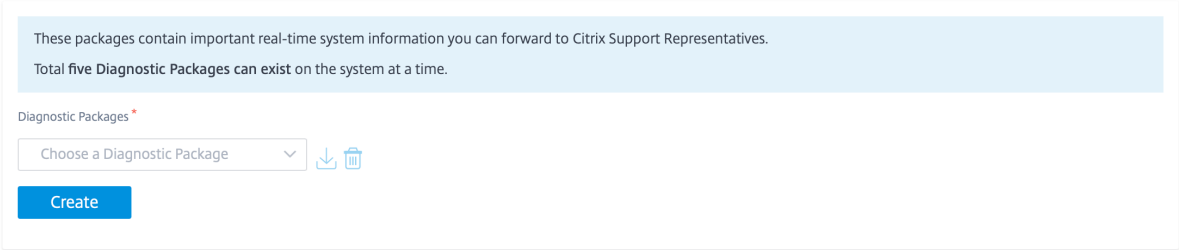


Informations diagnostiques

Un package de diagnostic comprend des fichiers journaux système, des informations système et d'autres informations nécessaires qui aident l'équipe d'assistance à diagnostiquer et à résoudre les problèmes liés à votre système.

Pour créer un package de diagnostic, accédez à **Infrastructure** > **Diagnostics d'Orchestrator** > **Informations de diagnostic**. Cliquez sur **Créer**. Une fois le package créé, vous pouvez le télécharger sur votre ordinateur, puis le partager avec l'équipe d'assistance.

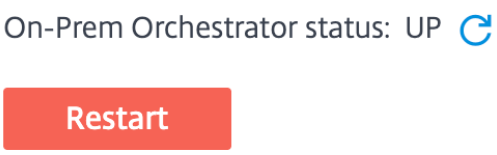
> **REMARQUE**
>
> Citrix SD-WAN Orchestrator pour locaux peut stocker jusqu'à cinq packages de diagnostic à la fois.



Redémarrez Citrix SD-WAN Orchestrator pour l'application locale

Vous pouvez uniquement redémarrer l'application Citrix SD-WAN Orchestrator for On-premises sans redémarrer le système d'exploitation (OS). Lors du redémarrage, l'application Citrix SD-WAN Orchestrator for On-premises se déconnecte et tous les services deviennent indisponibles. Le redémarrage prend environ 6 minutes. Après le redémarrage, la page de connexion de Citrix SD-WAN Orchestrator for On-premises s'affiche.

Pour redémarrer l'application Citrix SD-WAN Orchestrator pour site, accédez à **Infrastructure > Orchestrator Diagnostics > Restart Orchestrator App**. Cliquez sur **Redémarrer**, puis sur **Oui, redémarrer** pour confirmer.

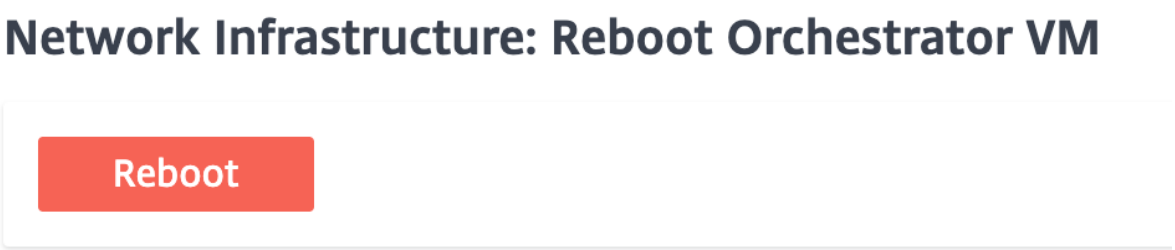


Redémarrez Citrix SD-WAN Orchestrator pour les machines virtuelles locales

Le processus de redémarrage redémarre le système d'exploitation (OS) de Citrix SD-WAN Orchestrator pour locaux. Lors du redémarrage, Citrix SD-WAN Orchestrator pour locaux se déconnecte et tous les services deviennent indisponibles. Le redémarrage prend environ 6 à 8 minutes. Après le redémarrage, la page de connexion de Citrix SD-WAN Orchestrator for On-premises s'affiche.

Vous pouvez redémarrer Citrix SD-WAN Orchestrator pour locaux dans le cadre d'une activité de dépannage ou d'une activité de maintenance.

Pour redémarrer, accédez à **Infrastructure > Diagnostics d'Orchestrator > Redémarrer la machine virtuelle Orchestrator**. Cliquez sur **Redémarrer**, puis sur **Oui, redémarrer** pour confirmer.



Alarmes

October 21, 2022

Vous pouvez consulter les alarmes spécifiques à la plate-forme et au service associées à Citrix SD-WAN Orchestrator pour les environnements locaux. Les alarmes spécifiques à la plate-forme affichent les alertes liées à la plate-forme, telles que les problèmes de stockage, de RAM, Les alarmes de service indiquent l'état des microservices exécutés dans Citrix SD-WAN Orchestrator pour locaux.

Pour afficher les alarmes, cliquez sur l'icône en forme de cloche dans le coin supérieur droit de l'interface utilisateur Citrix SD-WAN Orchestrator for On-premises et sélectionnez Alarmes de **plate-forme ou Alarmesde service** selon vos besoins.