Citrix SD-WAN Center 11.3

Machine translated content

Disclaimer

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

Contents

Configuration système requise et installation

February 17, 2022

Avant d'installer Citrix SD-WAN Center sur une machine virtuelle, assurez-vous que vous devez comprendre la configuration matérielle et logicielle requise et que vous avez satisfait aux conditions préalables.

> **Remarque**
>
> La configuration système requise est commune à la fois pour le réseau à une seule région et pour le réseau multirégion.

Configuration matérielle requise

Citrix SD-WAN Center a la configuration matérielle requise suivante.

Processeur

- 4 Core, 3 GHz (ou équivalent) processeur ou supérieur pour un serveur gérant jusqu'à 64 sites.
- Processeur 8 Core, 3 GHz (ou équivalent) ou supérieur pour un serveur gérant jusqu'à 128 sites.
- Processeur 16 Core, 3 GHz (ou équivalent) ou supérieur pour un serveur gérant jusqu'à 256 sites.
- Processeur 32 cœurs, 3 GHz (ou équivalent) ou supérieur pour un serveur gérant jusqu'à 550 sites.

Mémoire

- Un minimum de 8 Go de RAM est fortement recommandé pour une machine virtuelle gérant jusqu'à 64 sites.
- Un minimum de 16 Go de RAM est fortement recommandé pour une machine virtuelle gérant jusqu'à 128 sites.
- Un minimum de 32 Go de RAM est fortement recommandé pour une machine virtuelle gérant jusqu'à 256 sites.
- Un minimum de 32 Go de RAM est fortement recommandé pour une machine virtuelle gérant jusqu'à 550 sites.

Besoins en espace disque

Le tableau suivant fournit quelques conseils pour déterminer l'espace disque requis pour le stockage des données Citrix SD-WAN Center. Utilisez un stockage à accès direct avec un SSD de 5 000 à 10 000

IOPS.

Estimation de l'espace disque requis

# Sites clients	Nombre moyen de liens WAN par site	Nombre moyen de services Intranet/Internet par site	Nombre moyen de chemins virtuels par site	Taille de la base de données (To) pour 1 an
32	2	2	2	1,2 T
32	4	4	4	1,8 T
32	8	8	8	5,3 T
64	2	2	2	1,5 T
64	4	4	4	2,6 T
64	8	8	8	9,6 T
96	2	2	2	1,8 T
96	4	4	4	3,3 T
96	8	8	8	14,0 T
128	2	2	2	2,0 T
128	4	4	4	4.1T
128	8	8	8	18,0 T
192	2	2	2	2,6 T
192	4	4	4	5,6 T
192	8	8	8	27,0 T
256	2	2	2	3,0 T
256	4	4	4	7,2 T
256	8	8	8	35,0 T
550	2	2	2	15,9 T
550	4	4	4	41,9 T
550	8	8	8	195,6 T

Bande passante réseau

Le tableau suivant fournit des instructions pour déterminer les besoins en bande passante réseau pour la machine virtuelle Citrix SD-WAN Center.

Estimation des besoins en bande passante réseau

# Sites clients	Nombre moyen de liens WAN	Nombre moyen de chemins virtuels par site	Données VWAN totales par sondage de 5 minutes (Mo)	Taux de bande passante à configurer par sondage de 5 minutes (Kbit/s)
32	2	2	1.2	Par défaut 1000
32	4	4	3.6	Par défaut 1000
32	8	8	20.0	Par défaut 1000
64	2	2	2.3	Par défaut 1000
64	4	4	7.2	Par défaut 1000
64	8	8	40.0	2 000
96	2	2	3.5	Par défaut 1000
96	4	4	10.8	Par défaut 1000
96	8	8	60.0	3000
128	2	2	4.6	Par défaut 1000
128	4	4	14.4	Par défaut 1000
128	8	8	80.0	4000
192	2	2	6.9	Par défaut 1000
192	4	4	21.6	2 000
192	8	8	120.0	6000
256	2	2	9.2	Par défaut 1000
256	4	4	28,8	2 000
256	8	8	160	10000
550	2	2	34,0	2 000
550	4	4	89,3	6000
550	8	8	415,7	24000

Logiciel

Citrix SD-WAN Center VPX peut être configuré sur les plates-formes suivantes :

Hyperviseur

- Serveur VMware ESXi, version 6.5.
- Citrix XenServer 6.5 ou version ultérieure.
- Microsoft Hyper-V 2012 R2 ou supérieur.

Plateforme Cloud

- Microsoft Azure
- Amazon Web Services

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

L'interface Web du centre Citrix SD-WAN est prise en charge sur les navigateurs suivants :

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

Conditions préalables

Voici les conditions préalables à l'installation et au déploiement de Citrix SD-WAN Center :

- Le MCN (Master Control Node) SD-WAN et les nœuds clients existants doivent être mis à niveau vers la dernière version du logiciel Citrix SD-WAN.
- Il est recommandé d'avoir un serveur DHCP disponible et configuré dans le réseau SD-WAN.
- Vous devez disposer des fichiers d'installation de Citrix SD-WAN Center.

> **Remarque**
>
> Vous ne pouvez pas personnaliser ou installer un logiciel tiers sur Citrix SD-WAN Center. Toutefois, vous pouvez modifier les paramètres du vCPU, de la mémoire et du stockage.

Télécharger le logiciel Citrix SD-WAN Center

Téléchargez les fichiers d'installation du logiciel Citrix SD-WAN Center Management Console, pour la version et la plate-forme requises, à partir de la page Téléchargements .

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

ctx-sdwc-version_number-platform.extension

- *version_number* est le numéro de version de Citrix SD-WAN Center.
- *est le type de plate-forme, l'hyperviseur ou le nom de plate-forme cloud.*
- *extension* est l'extension du fichier d'installation.

Plateforme	Extension de fichier
Citrix XenServer	.xva
VMware ESXi	-vmware.ova
Microsoft Hyper-V	-hyperv.vhd.zip
Microsoft Azure	-azure.vhd.zip

Recueillir les informations d'installation et de configuration du Citrix SD-WAN Center

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

Recueillir ou déterminer les informations suivantes :

- Adresse IP du serveur ESXi, XenServer, Hyper-V ou Azure qui héberge la machine virtuelle (VM) Citrix SD-WAN Center.
- Nom unique à attribuer à la machine virtuelle Citrix SD-WAN Center.
- Quantité de mémoire à allouer pour la machine virtuelle Citrix SD-WAN Center.
- Quantité de capacité de disque à allouer pour le disque virtuel pour la machine virtuelle.
- Adresse IP de la passerelle que le Centre Citrix SD-WAN utilisera pour communiquer avec les réseaux externes.
- Masque de sous-réseau pour le réseau dans lequel la machine virtuelle Citrix SD-WAN Center sera installée.

Installer et configurer Citrix SD-WAN Center sur ESXi Server

February 17, 2022

Installer le client VMware vSphere

Voici les instructions de base pour le téléchargement et l'installation du client VMware vSphere que vous allez utiliser pour créer et déployer la machine virtuelle Citrix SD-WAN Center. Pour plus d'informations, consultez la documentation VMware vSphere Client.

Pour télécharger et installer VMware vSphere Client, procédez comme suit :

1. Ouvrez un navigateur et accédez au serveur ESXi qui héberge votre instance vSphere Client et Citrix SD-WAN Center Virtual Machine (VM).

   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.

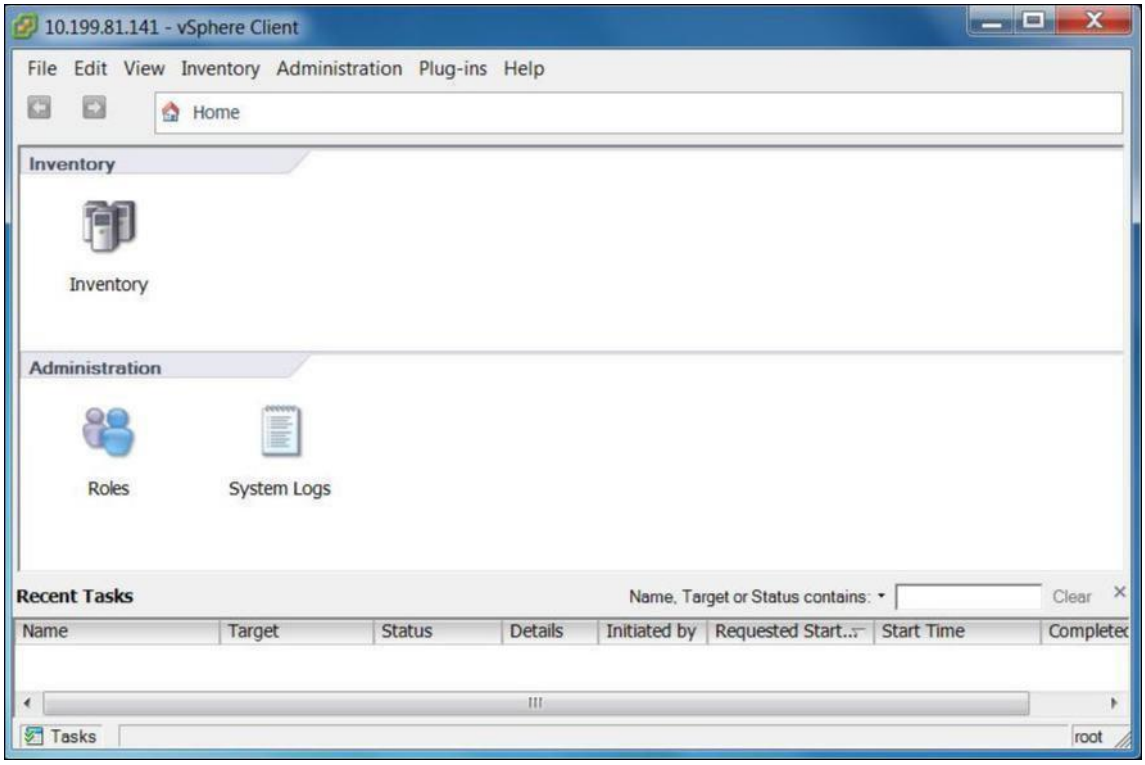
   La page de connexion VMware vSphere Client s'affiche et vous invite à entrer les informations d'identification de connexion du serveur ESXi.

5. Entrez les informations d'identification de connexion du 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 Center.
   - **Nom d'utilisateur** : entrez le nom du compte d'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 de la machine virtuelle Citrix SD-WAN Center à l'aide du modèle OVF

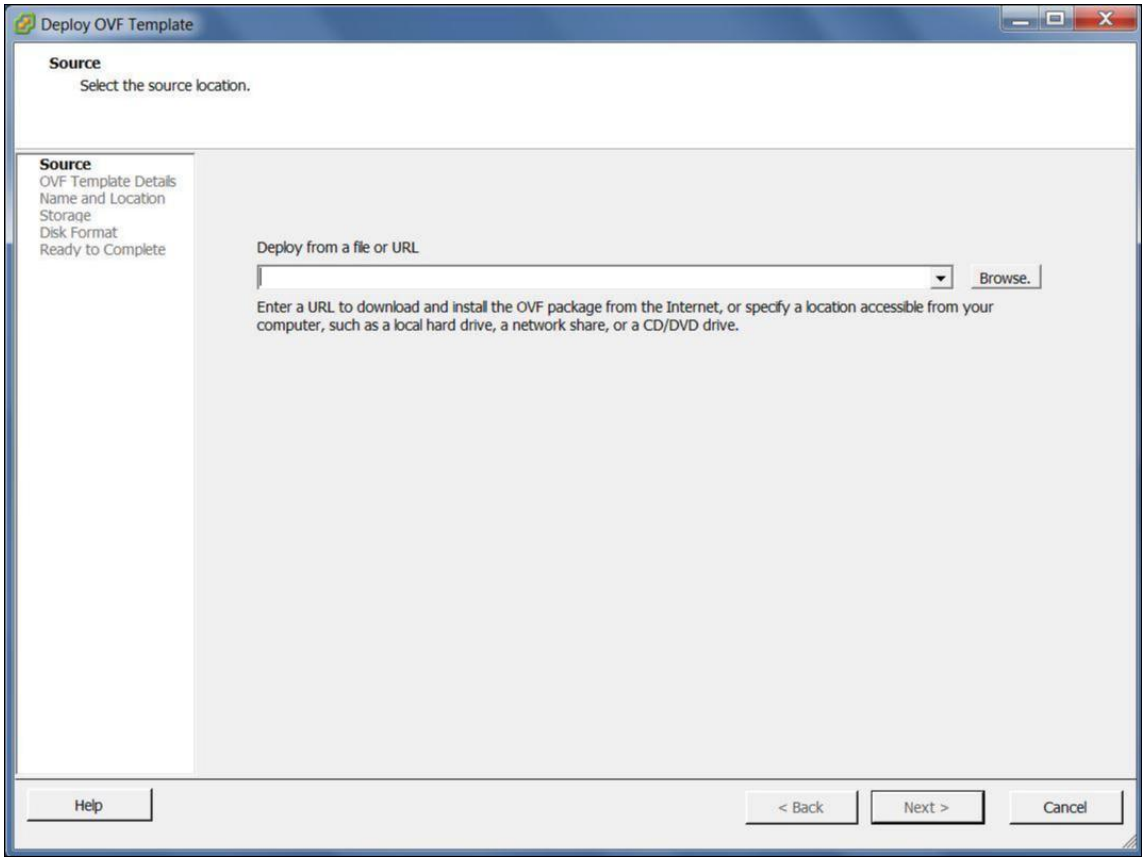
Après avoir installé le client VMware vSphere, créez la machine virtuelle Citrix SD-WAN Center.

1. Si vous ne l'avez pas encore fait, téléchargez le fichier modèle OVF Citrix SD-WAN Center (fichier. ova) sur le PC local.

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

2. Dans vSphere Client, cliquez sur **Fichier**, puis sélectionnez **Déployer le modèle OVF** dans le menu déroulant.

   L'assistant **Déployer un modèle OVF** apparaît.

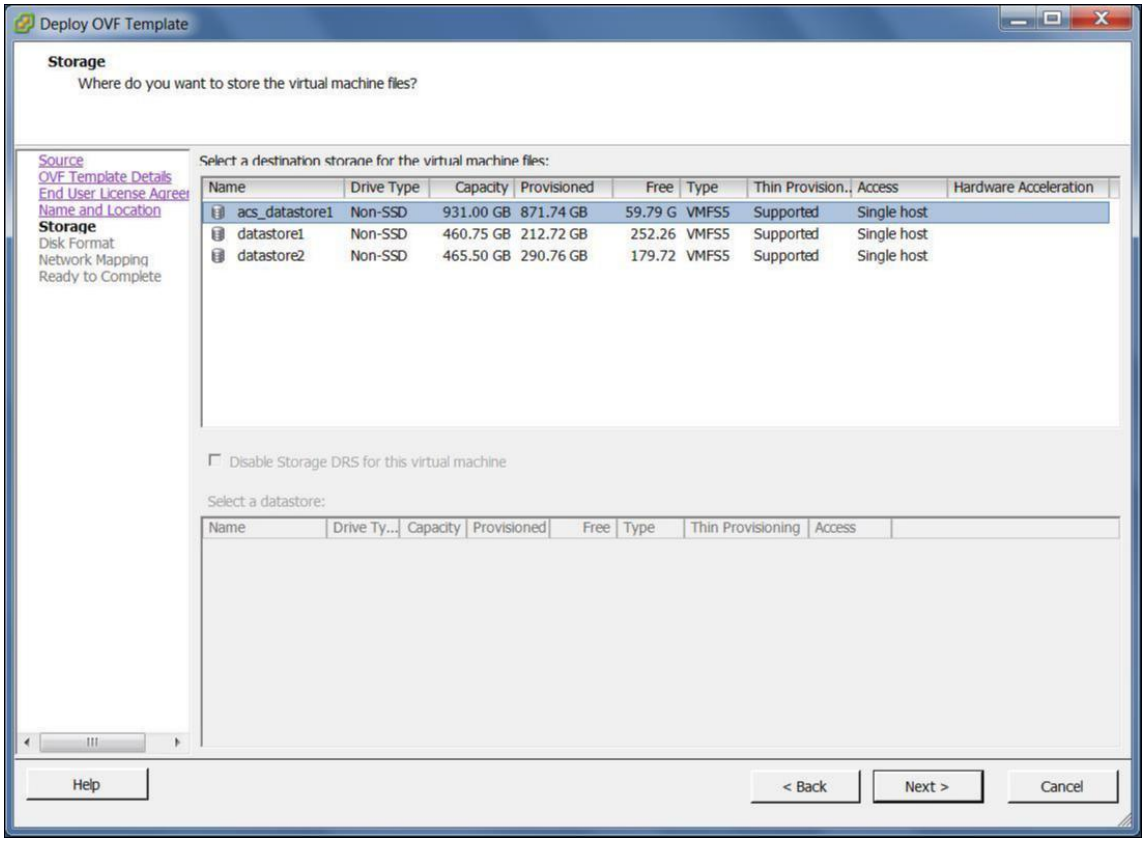


3. Cliquez sur **Parcourir** et sélectionnez le modèle OVF Citrix SD-WAN Center (fichier .ova) que vous souhaitez installer.
4. Cliquez sur **Suivant**.

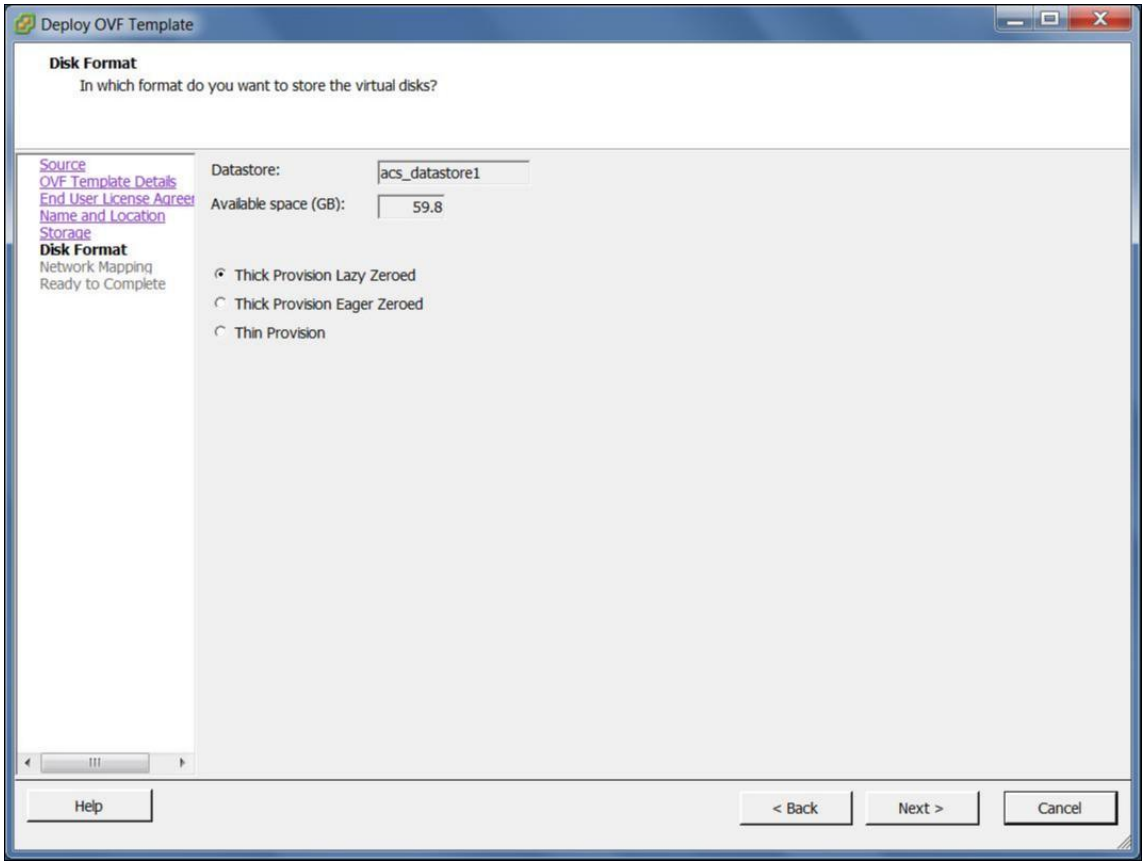
   Le fichier ova est importé et la page Détails du modèle OVF apparaît.
5. Cliquez sur **Suivant**.
6. Dans la page Contrat de licence utilisateur final, cliquez sur **Accepter**, puis cliquez sur **Suivant**.
7. Dans la page Nom et emplacement, entrez un nom unique pour la nouvelle machine virtuelle (ou acceptez la valeur par défaut).

   Le nom doit être unique dans le dossier **Stock** actuel et peut contenir jusqu'à 80 caractères.
8. Cliquez sur **Suivant**.

   La page Stockage s'affiche.



9. Pour l'instant, acceptez la ressource de stockage par défaut en cliquant sur **Suivant**. Vous pouvez également configurer la banque de données. Pour plus d'informations, consultez Ajouter et configurer la banque de données sur le serveur ESXi.



10. Sur la page Format de disque, acceptez les paramètres par défaut, puis cliquez sur **Suivant**.
11. Sur la page Mappage réseau, acceptez la valeur par défaut (VM Network) et cliquez sur **Suivant**.
12. Dans 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.

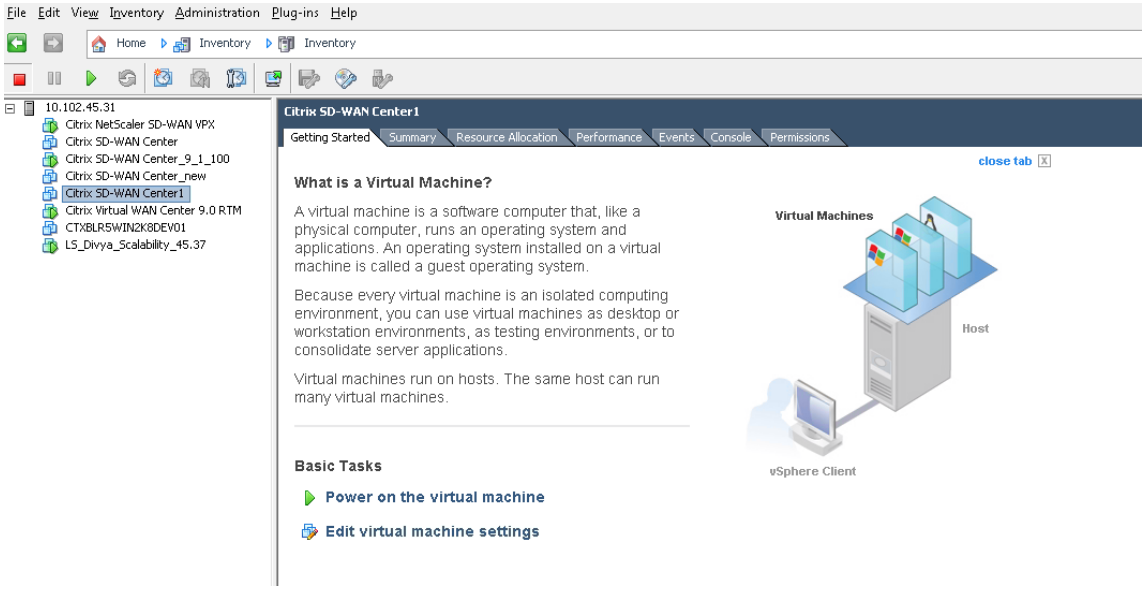
13. Cliquez sur **Fermer**.

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

L'adresse IP de gestion est l'adresse IP de la machine virtuelle SD-WAN Center, utilisez cette adresse IP pour vous connecter à l'interface utilisateur Web Citrix SD-WAN Center.

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

1. Sur la page Inventaire du client vSphere, sélectionnez la nouvelle machine virtuelle Citrix SD-WAN Center dans l'arborescence de l'**inventaire** (volet gauche).

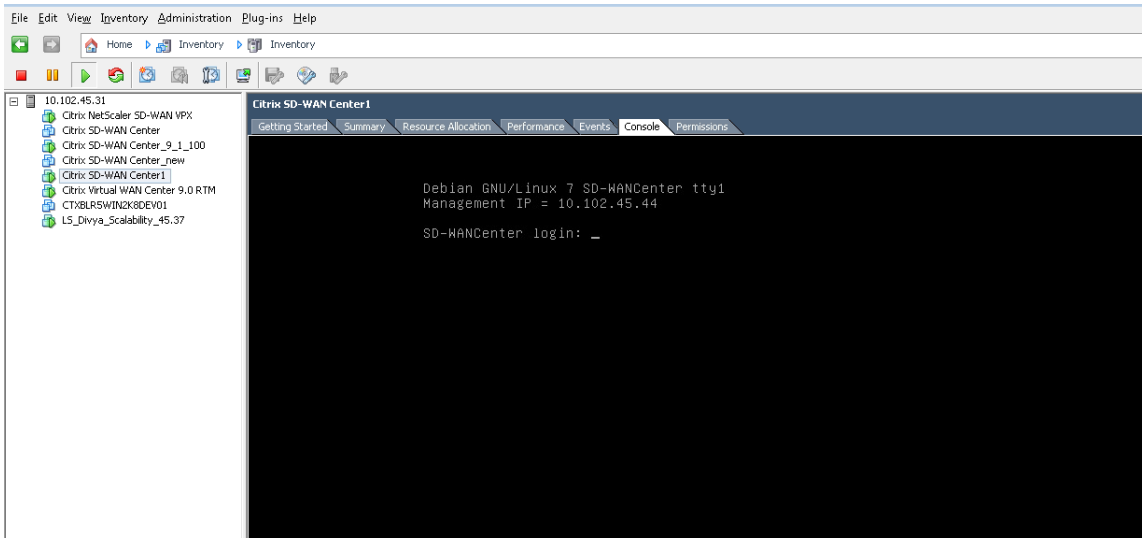


2. Sur la page Centre Citrix SD-WAN, sous Tâches de base, cliquez sur **Mise sous tension sur la machine virtuelle**.
3. Sélectionnez l'onglet **Console**, puis cliquez n'importe où dans la zone de la console pour passer en mode console.

   Cela transforme le contrôle du curseur de votre souris sur la console de la machine virtuelle.

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

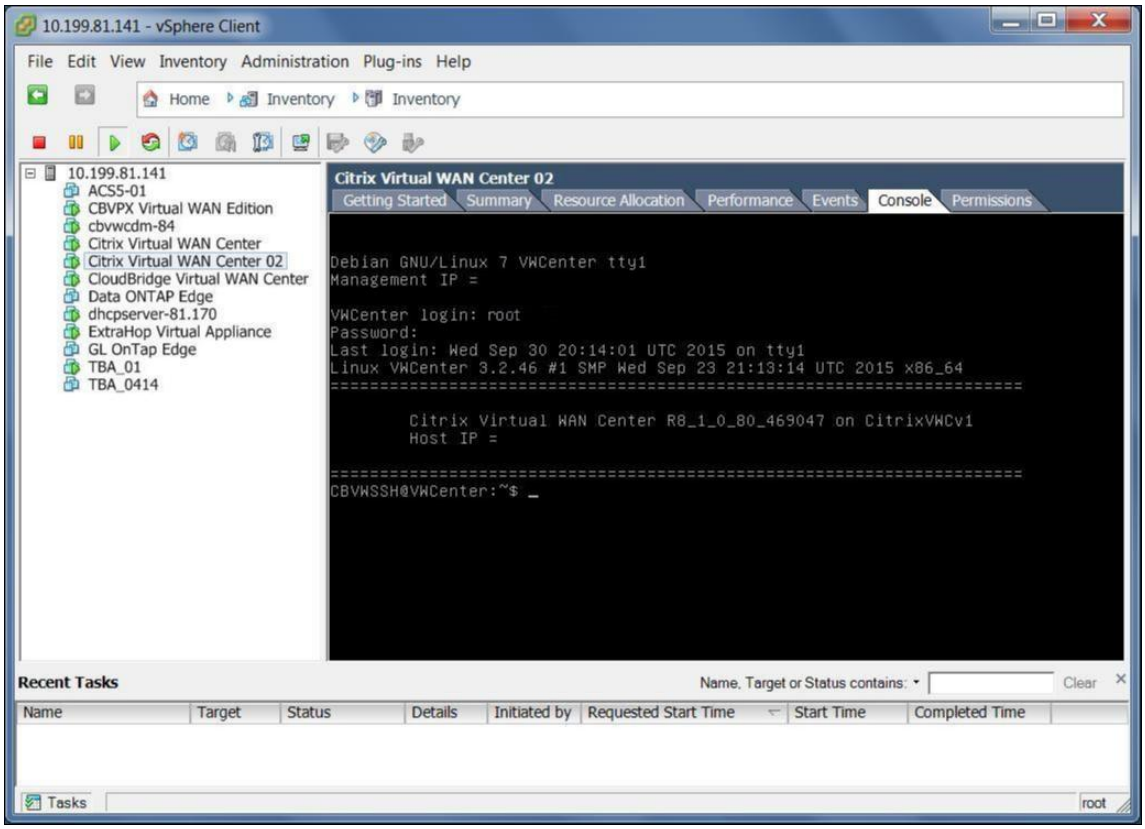
4. Appuyez sur **Entrée** pour afficher l'invite de connexion à la console.



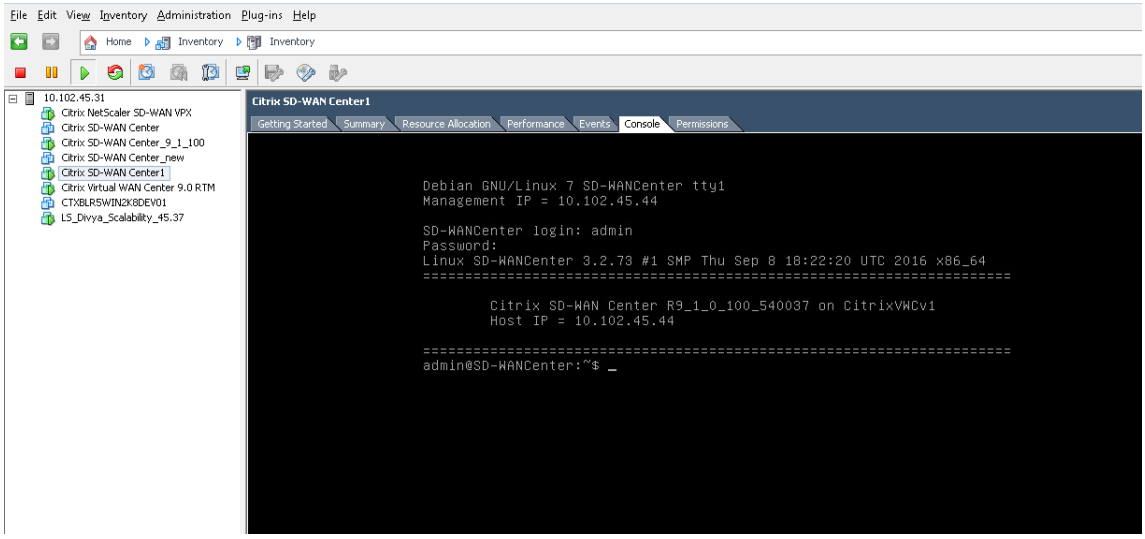
5. Connectez-vous à la console de la machine virtuelle.

Les informations d'identification de connexion par défaut pour la nouvelle machine virtuelle Citrix SD-WAN Center sont les suivantes :

- Connexion : admin
- Mot de passe : password



6. Enregistrez l'adresse IP de gestion de la machine virtuelle Citrix SD-WAN Center, qui s'affiche comme adresse IP de l'hôte dans un message de bienvenue qui apparaît lorsque vous ouvrez une session.



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

Si le serveur DHCP n'est pas configuré dans 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 d'identification de connexion par défaut pour la nouvelle machine virtuelle Citrix SD-WAN Center sont les suivantes :

   Connexion : admin

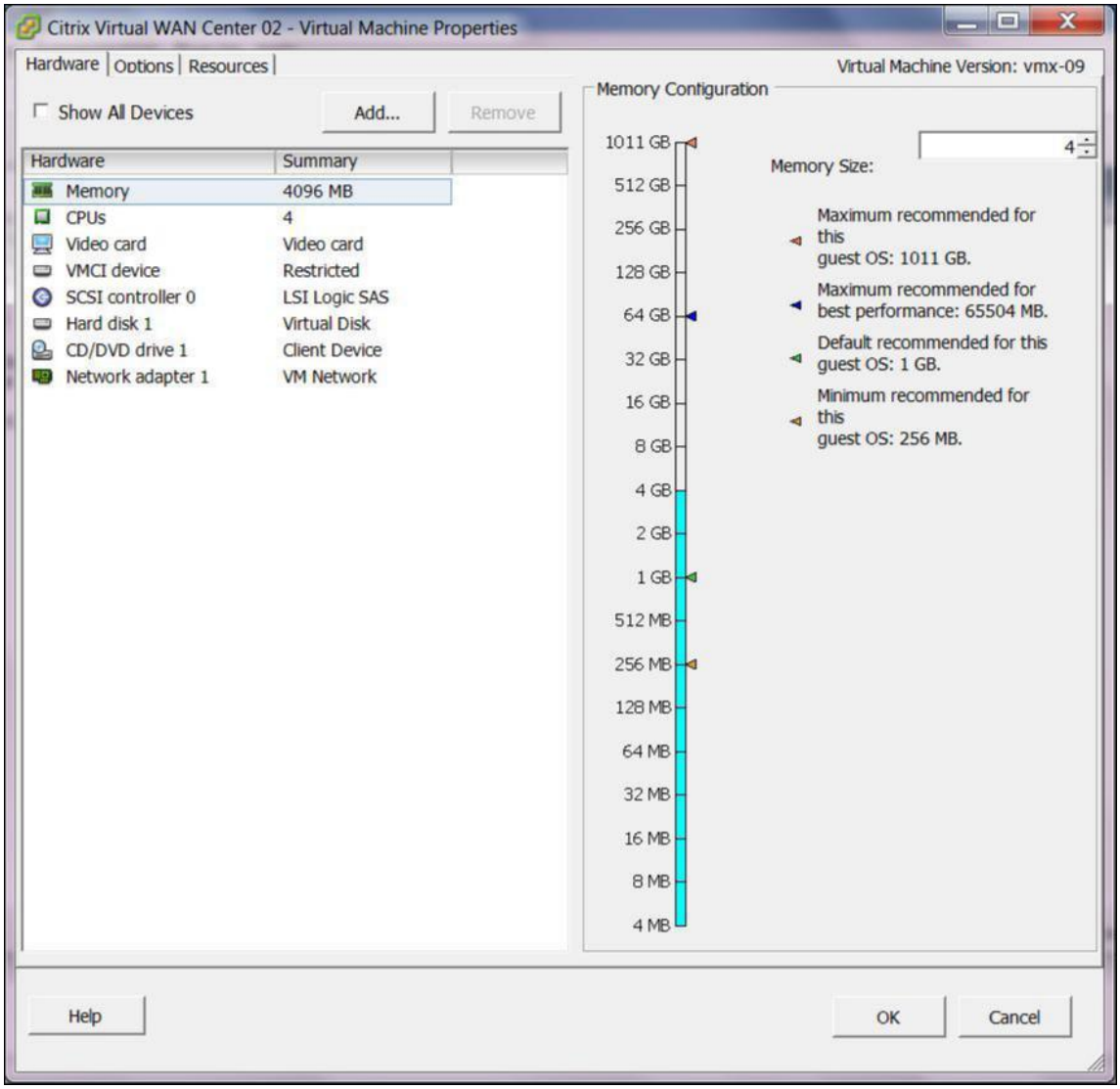
   Mot de passe : password
3. Dans la console, entrez la commande **management_ip** de l'interface de ligne de commande.
4. Entrez la commande **set interface <ipaddress> <subnetmask> <gateway>** pour configurer l'adresse IP de gestion.

Ajouter et configurer la banque de données sur un serveur ESXi

Vous pouvez ajouter et configurer une banque de données pour stocker des statistiques à partir du Centre Citrix SD-WAN.

Pour ajouter et configurer la banque de données :

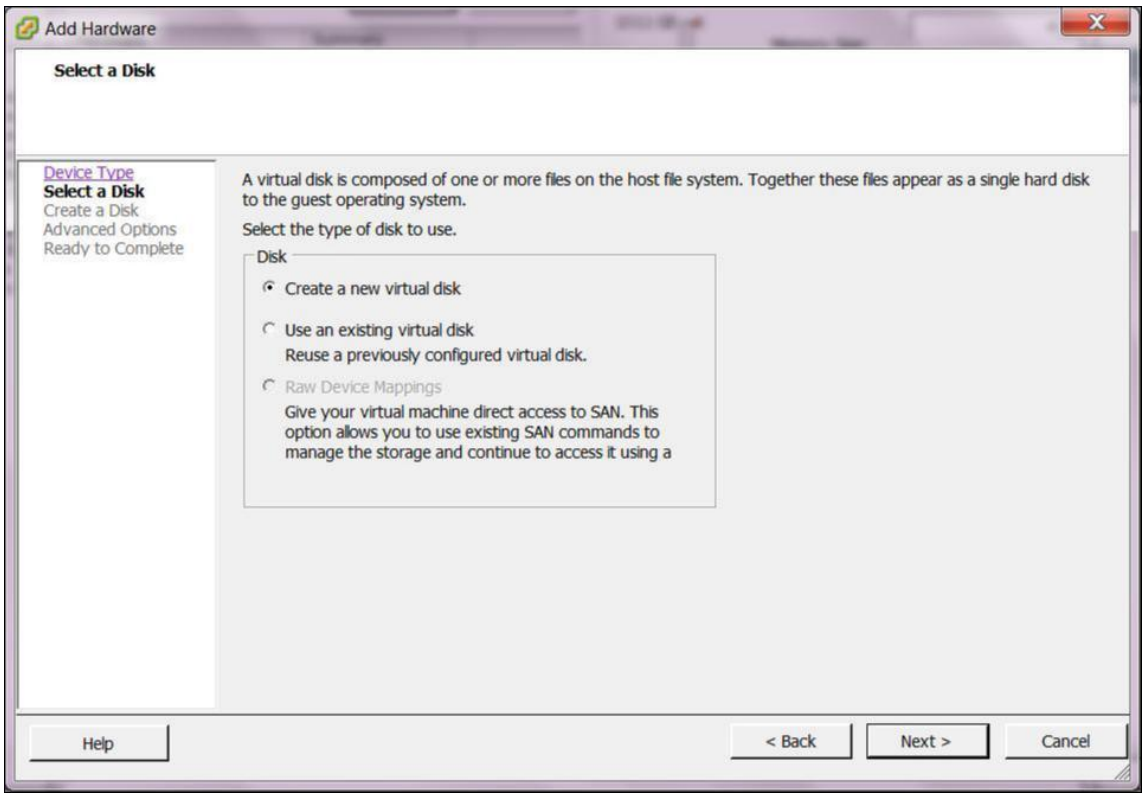
1. Dans vSphere client, cliquez sur l'icône **Inventaire** pour ouvrir la page Inventaire.
2. Développez la succursale d'arborescence d'**inventaire** pour le serveur hôte Citrix SD-WAN Center VM.
3. Dans le volet gauche, cliquez sur **+** en regard de l'adresse IP du serveur hébergeant la machine virtuelle Citrix SD-WAN Center que vous avez créée.
4. Ouvrez la nouvelle machine virtuelle Citrix SD-WAN Center pour la modification.
5. Dans l'arborescence d'**inventaire**, cliquez avec le bouton droit sur le nom de la machine virtuelle Citrix SD-WAN Center que vous avez créée et sélectionnez **Modifier le paramètre** dans le menu déroulant.



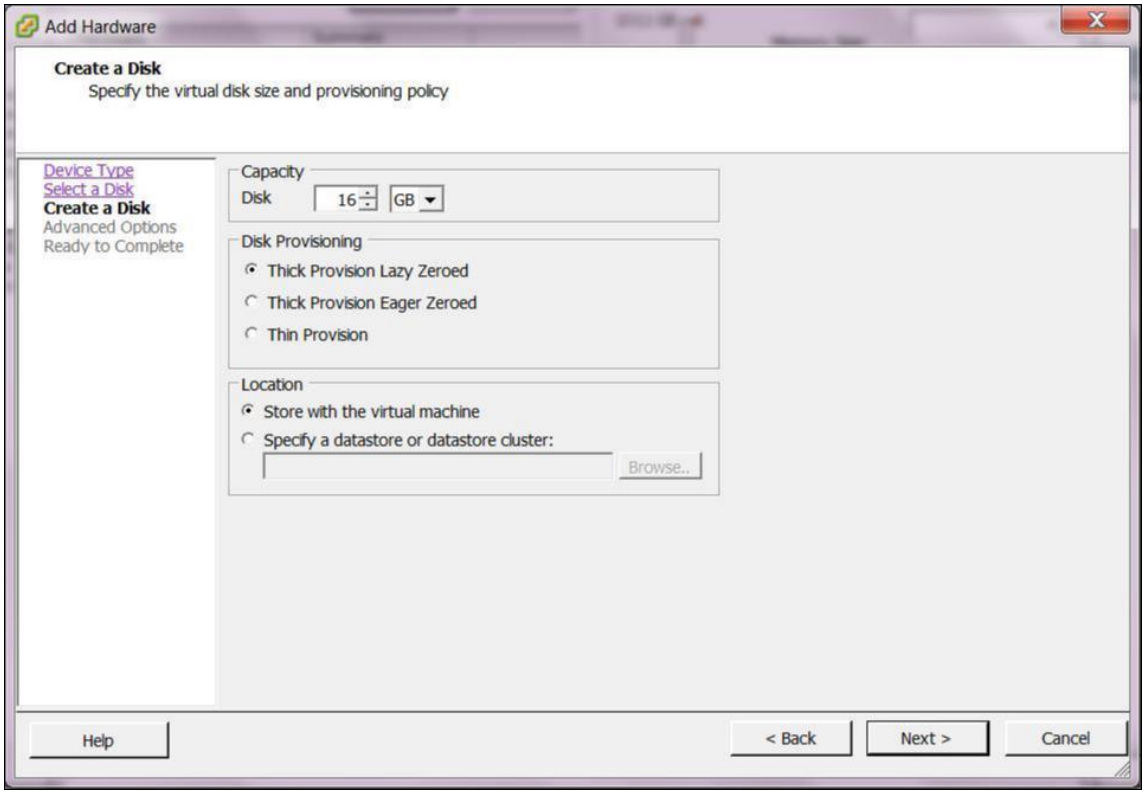
6. Dans le champ Taille de la mémoire, entrez la quantité de mémoire à allouer à cette machine virtuelle.

   Pour plus d'informations, consultez la section Mémoire requise.

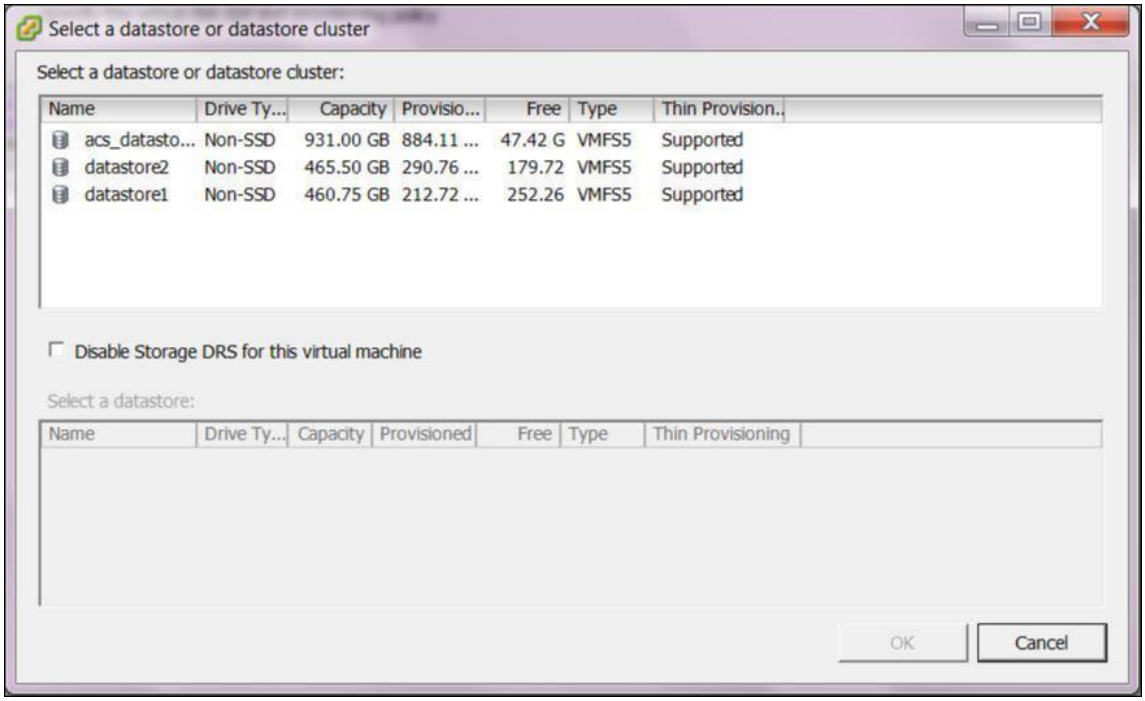
7. Cliquez sur **Ajouter**.
8. Dans la page Type de périphérique de l'Assistant Ajout de matériel, sélectionnez **Disque dur**, puis cliquez sur **Suivant** .



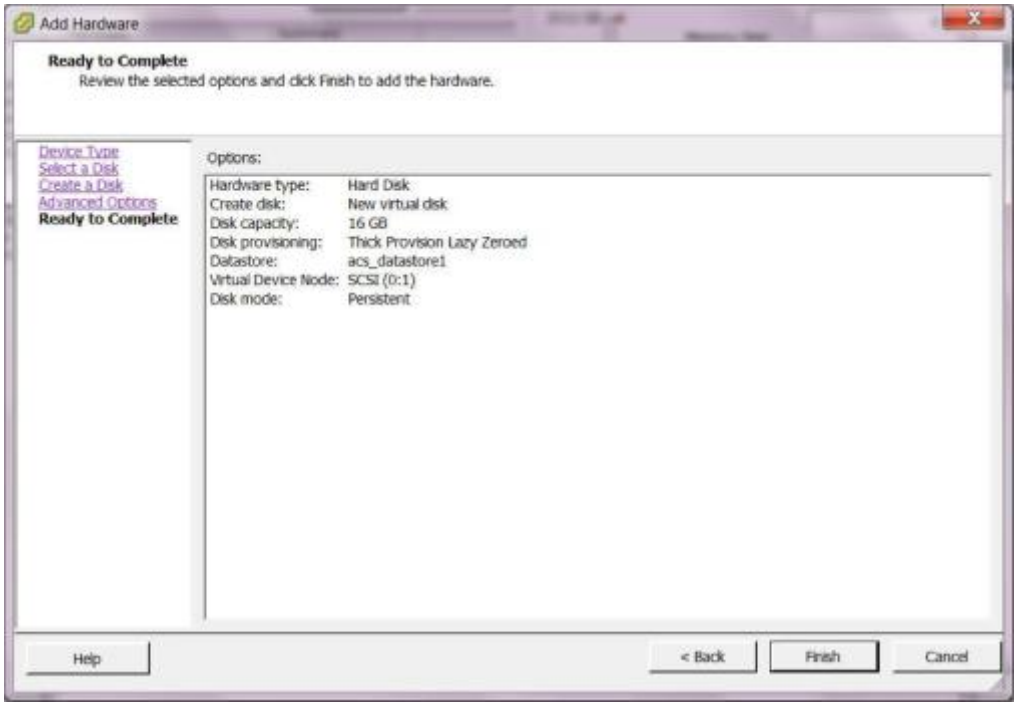
9. Dans la page Sélectionner un disque, sélectionnez **Créer un disque virtuel** et cliquez sur **Suivant**.



10. Dans la page Créer un disque, dans la section **Capacité**, sélectionnez la capacité du disque du nouveau disque virtuel.
11. Dans la section Provisioning de disque, sélectionnez **Provisionnement épais Lazy Zeroed** (valeur par défaut).
12. Dans la section Emplacement, sélectionnez **Spécifier une banque de données ou un cluster de banque de données**.
13. Cliquez sur **Parcourir**.



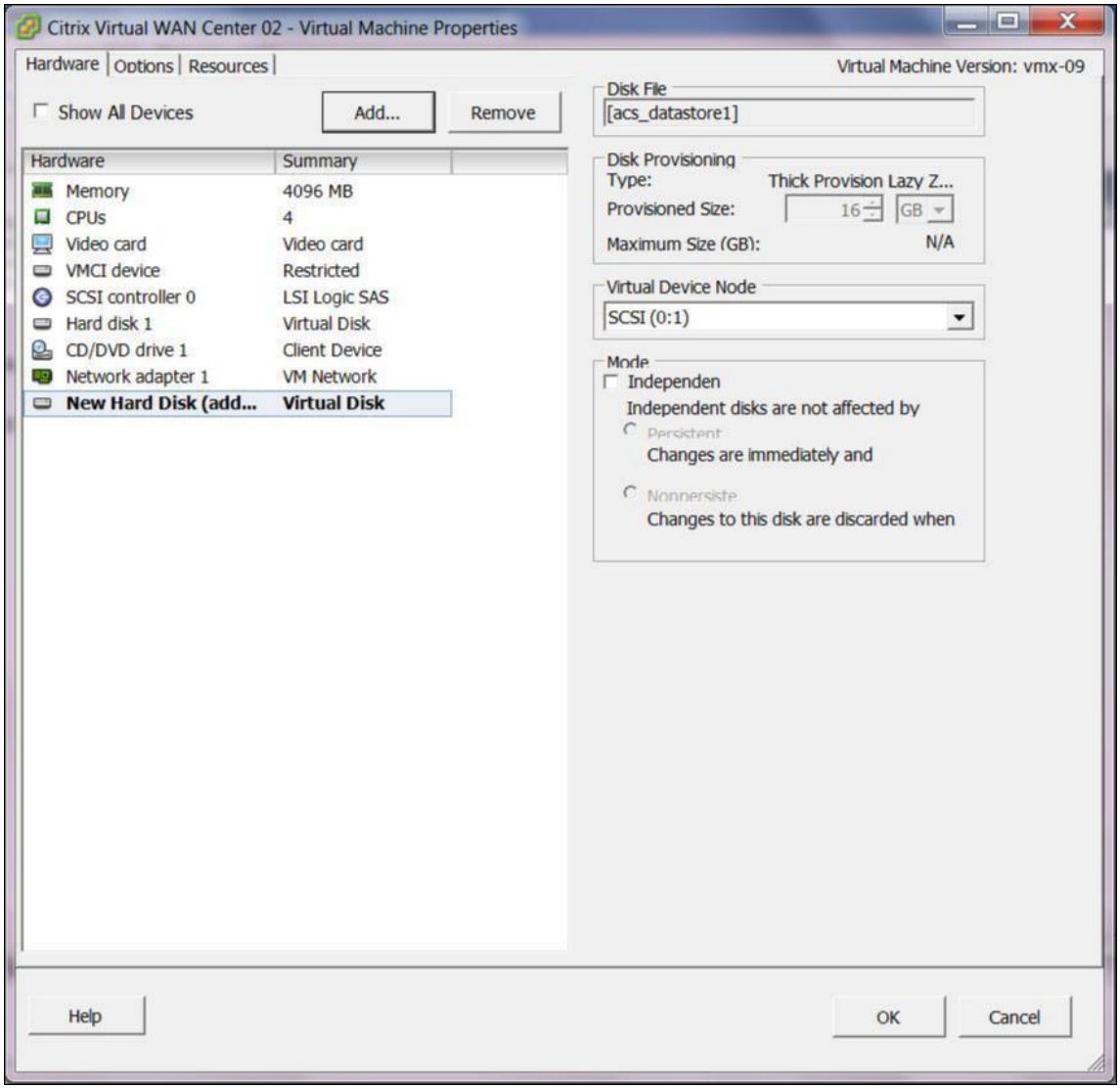
14. Sélectionnez une banque de données avec suffisamment d'espace disponible, puis cliquez sur **OK**.
15. Cliquez sur **Suivant**.
16. Dans la page Options avancées, acceptez les paramètres par défaut **Options avancées** et cliquez sur **Suivant**.



17. Cliquez sur **Terminer**.

    Cela ajoute le nouveau disque virtuel, rejette l'Assistant Ajout de matériel et vous renvoie à la page Propriétés de la machine virtuelle.

18. Cliquez sur **OK**.



Installer et configurer Citrix SD-WAN Center sur XenServer

February 17, 2022

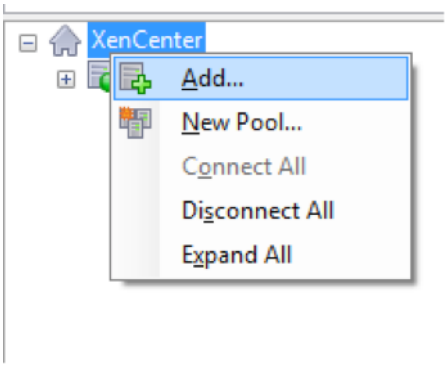
Avant d'installer la machine virtuelle Citrix SD-WAN Center sur un serveur XenServer, collectez les informations nécessaires, comme décrit dans la section Collecte des informations d'installation et de configuration de Citrix SD-WAN Center.

Installer le serveur XenServer

Pour installer le serveur Citrix XenServer sur lequel vous allez déployer la machine virtuelle Citrix SD-WAN Center, vous devez disposer de XenCenter installé sur votre ordinateur. Si vous ne l'avez pas déjà fait, téléchargez et installez XenCenter.

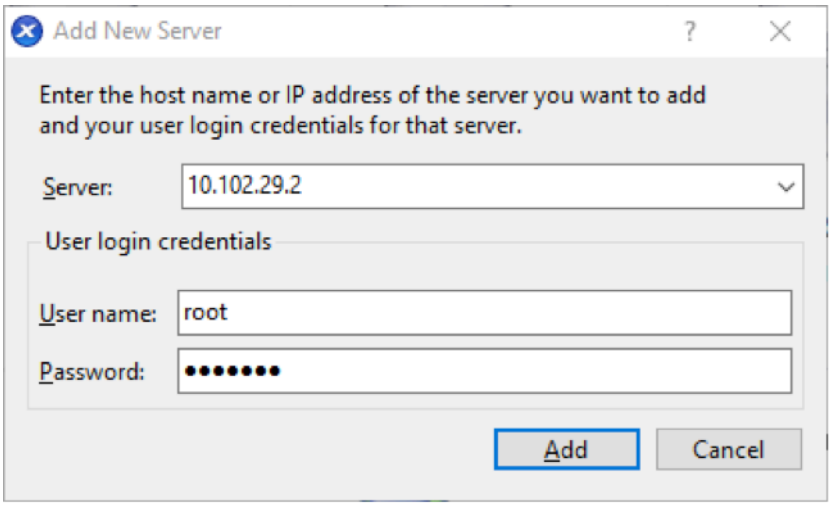
Pour installer un serveur XenServer :

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 hébergera votre instance de machine virtuelle Citrix SD-WAN Center.
   - **Nom d'utilisateur** : entrez le nom du compte d'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**.

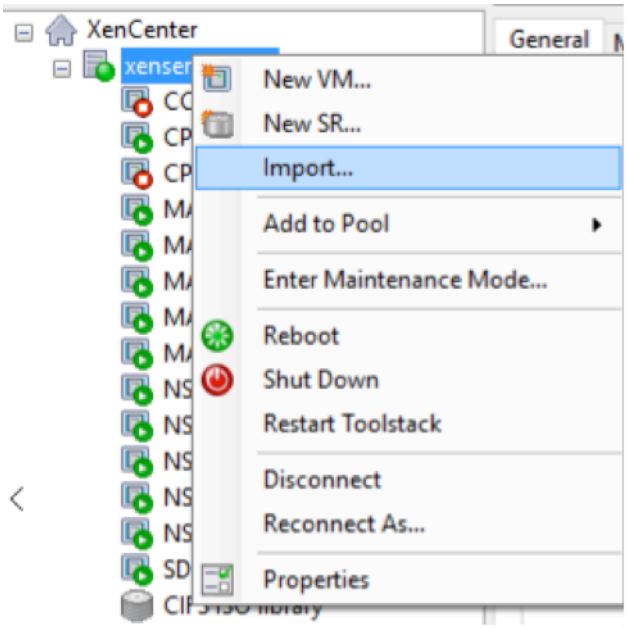
   L'adresse IP du nouveau serveur apparaît dans le volet gauche.

Créez la machine virtuelle Citrix SD-WAN Center à l'aide du fichier XVA

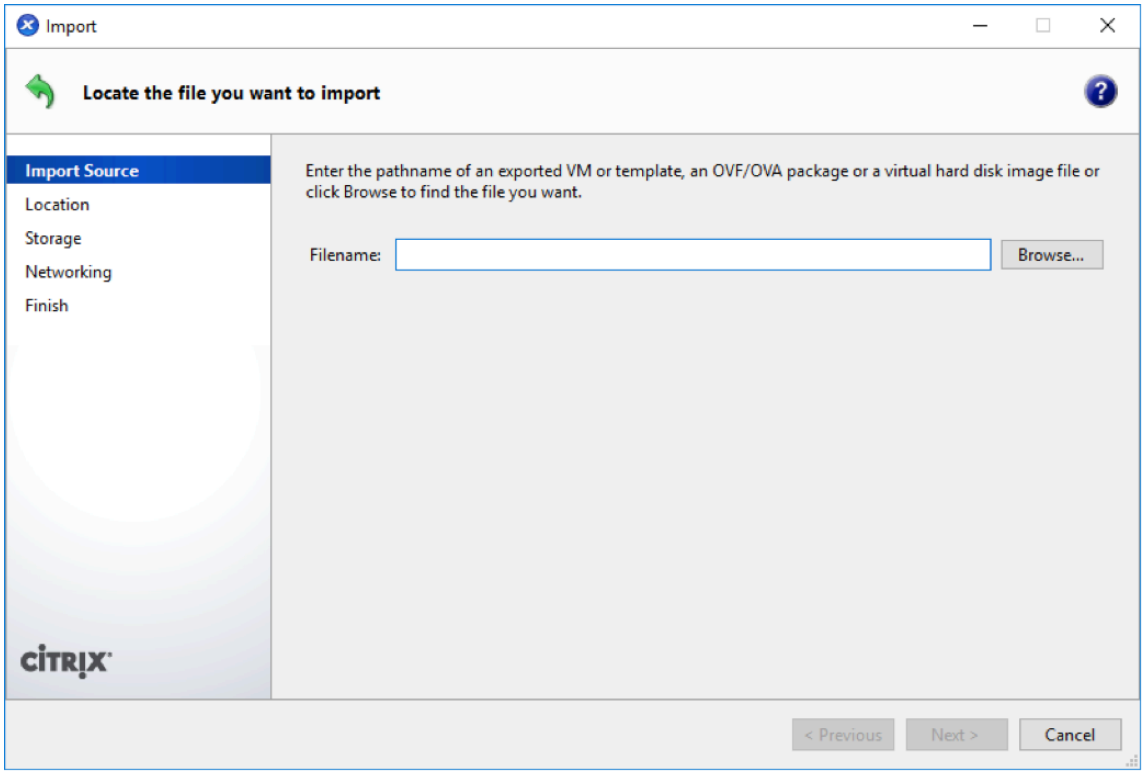
Le logiciel de machine virtuelle Citrix SD-WAN Center est distribué sous la forme d'un fichier XVA. Si vous ne l'avez pas déjà fait, téléchargez le fichier .xva. Pour plus d'informations, consultez Configuration système requise et installation.

Pour créer la machine virtuelle Citrix SD-WAN Center :

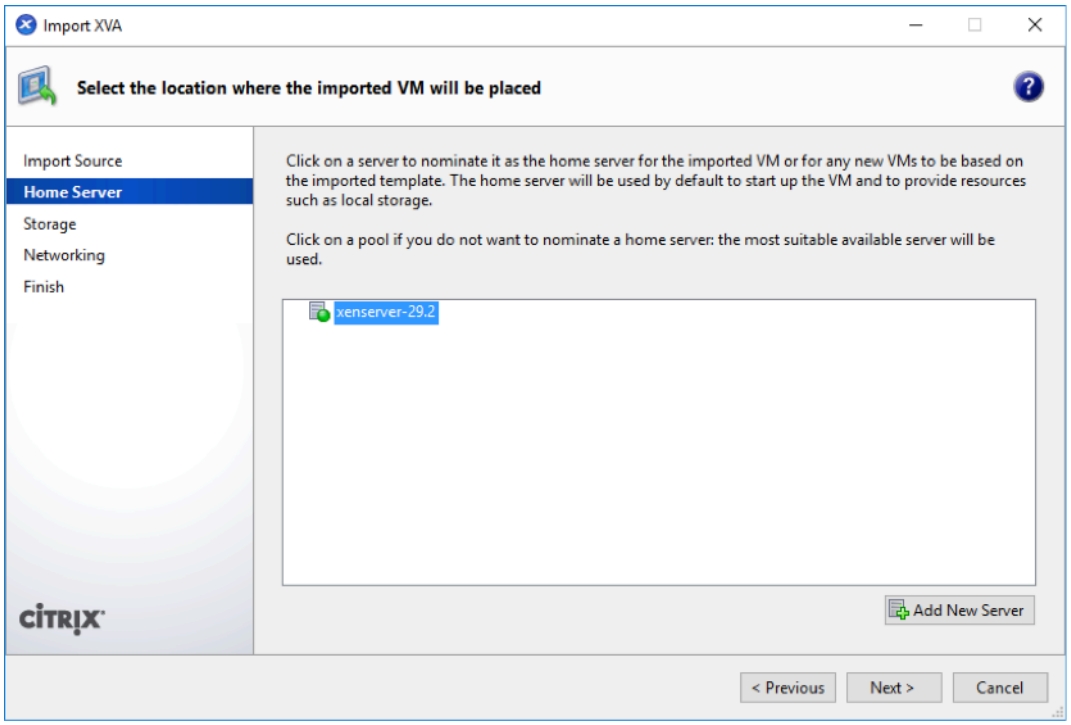
1. Dans XenCenter, cliquez avec le bouton droit sur **XenServer** et cliquez sur **Importer**



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

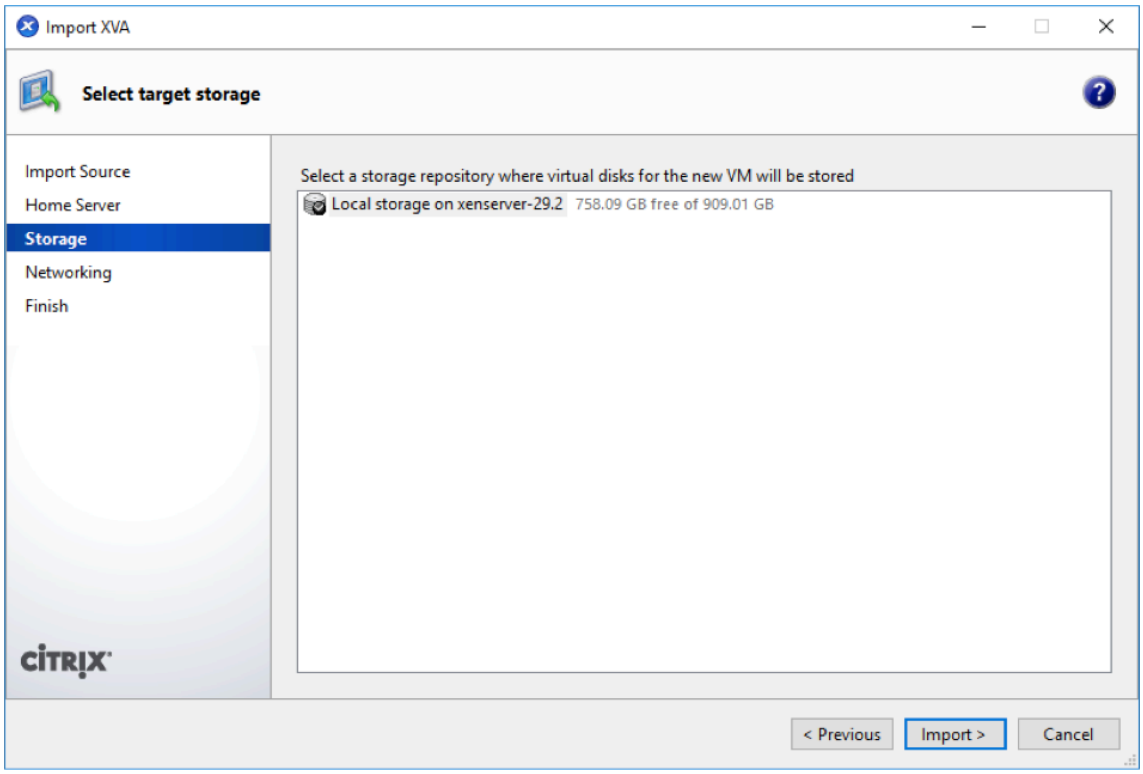


3. Sélectionnez un serveur XenServer précédemment créé comme emplacement vers lequel importer la machine virtuelle, puis cliquez sur **Suivant**.



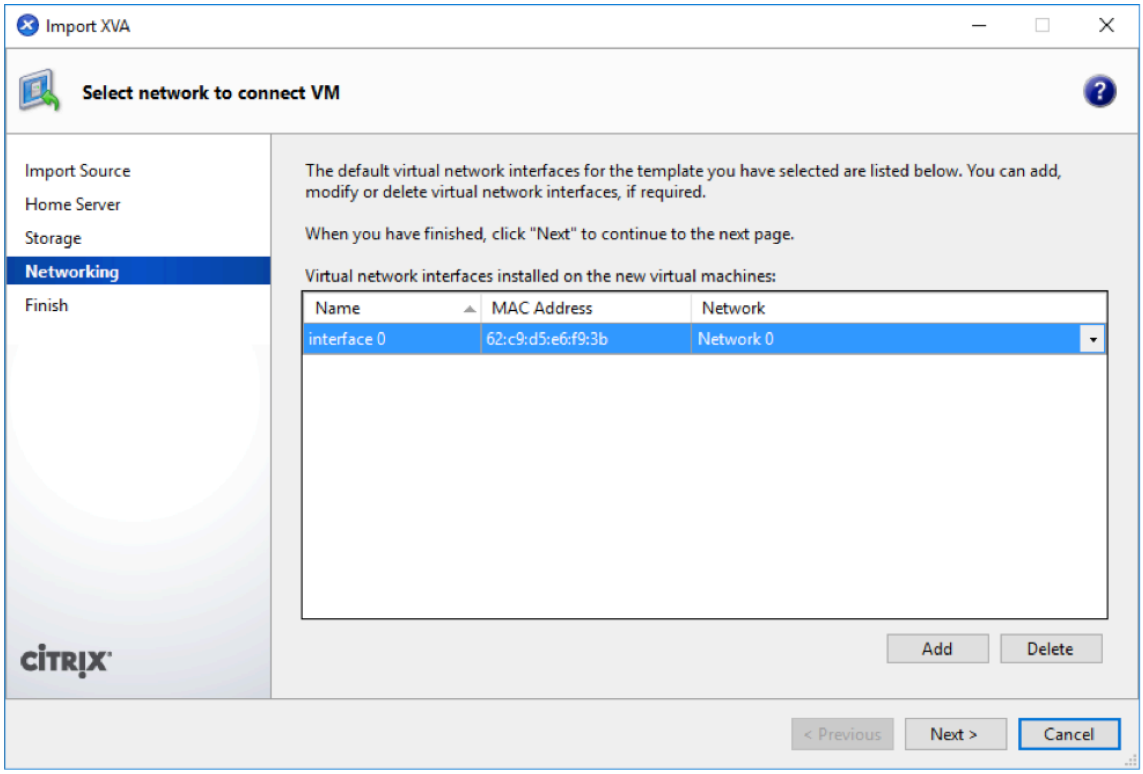
4. Sélectionnez un référentiel de stockage où le disque virtuel de la nouvelle machine virtuelle sera stocké, puis cliquez sur **Importer.**

Pour l'instant, vous pouvez accepter la ressource de stockage par défaut. Ou vous pouvez configurer la banque de données. Pour plus d'informations, consultez la section **Ajouter et configurer la banque de données sur XenServer**.



La machine virtuelle Citrix SD-WAN Center importée apparaît dans le volet gauche.

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



6. Cliquez sur **Terminer**.

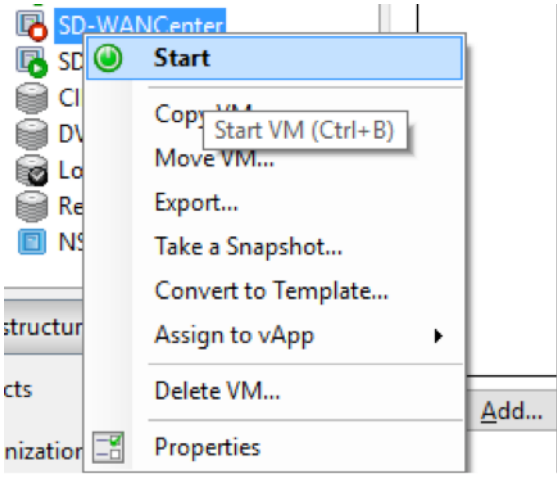
Afficher et enregistrer l'adresse IP de gestion sur XenServer

L'adresse IP de gestion est l'adresse IP de la machine virtuelle Citrix SD-WAN Center, utilisez cette adresse IP pour vous connecter à l'interface utilisateur Web Citrix SD-WAN Center.

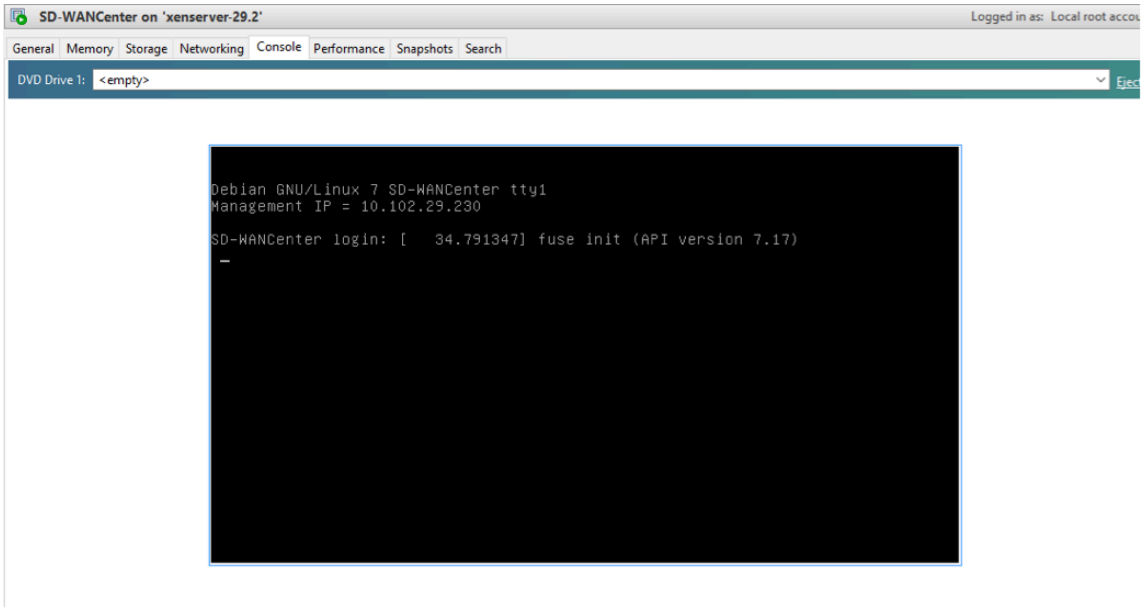
> **Remarque**
>
> Le serveur DHCP doit être présent et disponible dans le réseau SD-WAN.

Pour afficher l'adresse IP de gestion :

1. Dans l'interface XenCenter, dans le volet gauche, cliquez avec le bouton droit sur la nouvelle machine virtuelle Citrix SD-WAN Center et sélectionnez **Démarrer**.



2. Lorsque la machine virtuelle est démarrée, cliquez sur l'onglet **Console**.



3. Notez l'adresse IP de gestion.

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

4. Connectez-vous à la machine virtuelle. Les informations d'identification de connexion par défaut pour la nouvelle machine virtuelle Citrix SD-WAN Center sont les suivantes :

   Identifiant : admin

   Mot de passe : password

   Si le serveur DHCP n'est pas configuré dans le réseau Citrix SD-WAN, vous devez entrer 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 d'identification de connexion par défaut pour la nouvelle machine virtuelle Citrix SD-WAN Center sont les suivantes :

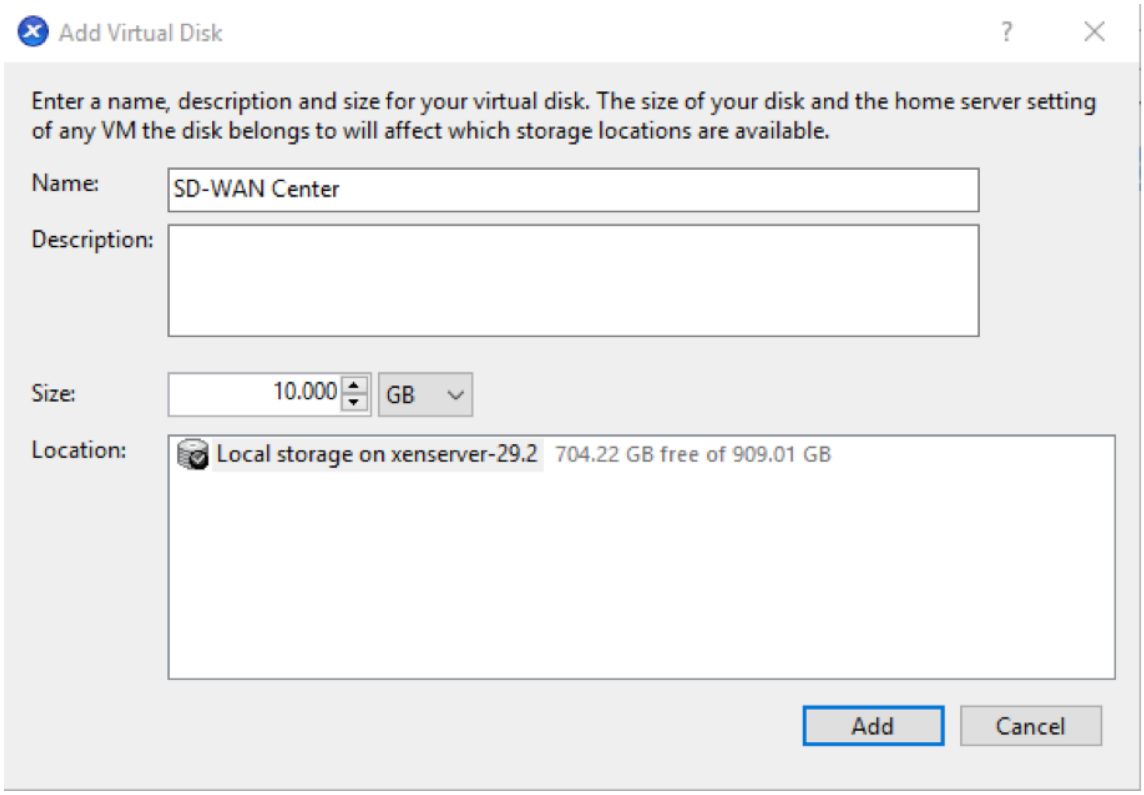
   Connexion : admin
   , **Mot de passe** : password
3. Dans la console, entrez la commande CLI **management_ip.**
4. Entrez la commande **set interface <ipaddress> <subnetmask> <gateway>** pour configurer l'adresse IP de gestion.

Ajout et configuration du stockage de données pour un serveur XenServer

Vous pouvez ajouter et configurer le stockage de données pour stocker des statistiques à partir du centre Citrix SD-WAN.

Pour ajouter et configurer le stockage des données :

1. Dans XenCenter, arrêtez la machine virtuelle Citrix SD-WAN Center.
2. Sous l'onglet **Stockage**, cliquez sur **Ajouter**.



3. Dans le champ **Nom**, entrez un nom pour le disque virtuel.
4. Dans le champ **Description**, entrez une description du disque virtuel.
5. Dans le champ **Taille**, sélectionnez la taille requise.
6. Dans le champ **Emplacement**, sélectionnez le stockage local.
7. Cliquez sur **Ajouter**.

Installer et configurer Citrix SD-WAN Center sur Microsoft Hyper-V

February 17, 2022

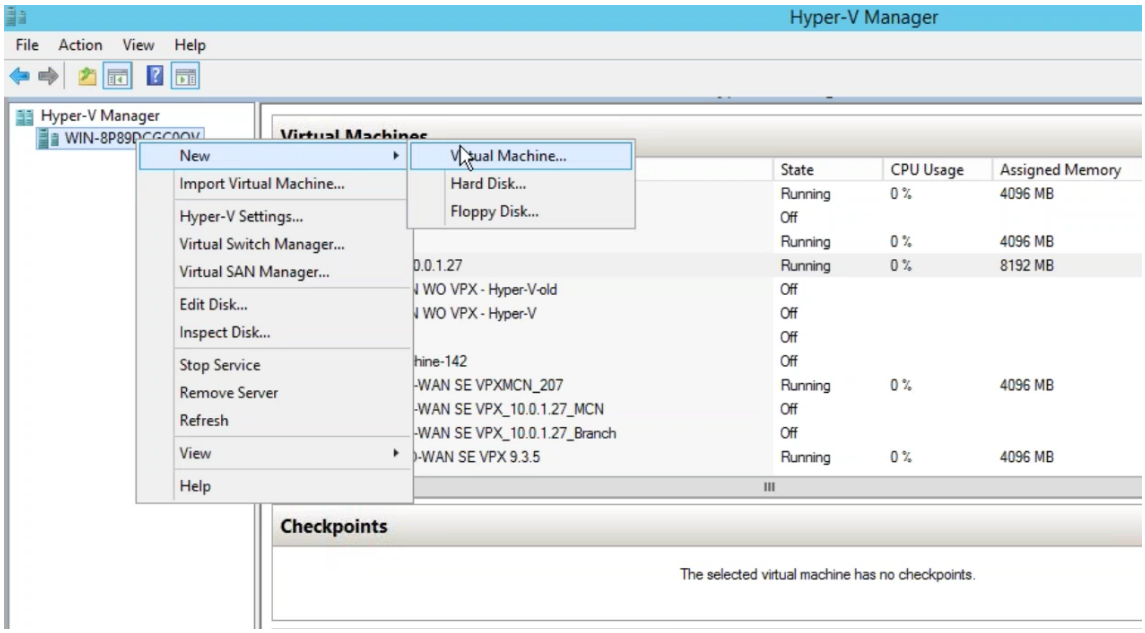
Avant d'installer la machine virtuelle (VM) Citrix SD-WAN Center sur le serveur Microsoft Hyper-V, collectez les informations nécessaires comme décrit dans Configuration système requise et installation.

Téléchargez le logiciel SD-WAN Center pour Hyper-V, comme décrit dans la section Téléchargement du logiciel Citrix SD-WAN Center de la sectionConfiguration système requise et installation.

Assurez-vous que la fonctionnalité Hyper-V et l'outil de gestion sont activés sur votre serveur Windows.

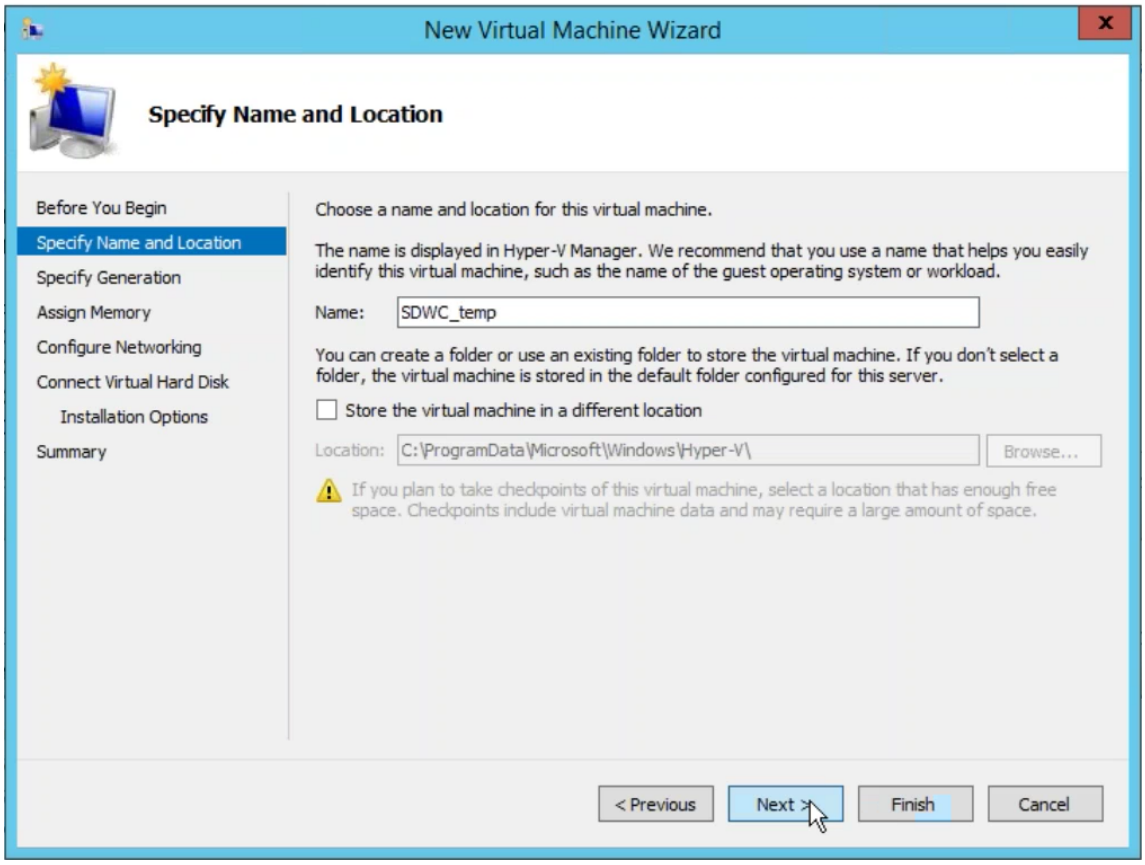
Pour créer la machine virtuelle SD-WAN Center sur le serveur Hyper-V :

1. Dans le Gestionnaire Hyper-V, cliquez avec le bouton droit sur le serveur Hyper-V et sélectionnez **Nouveau** > **Machine virtuelle**.



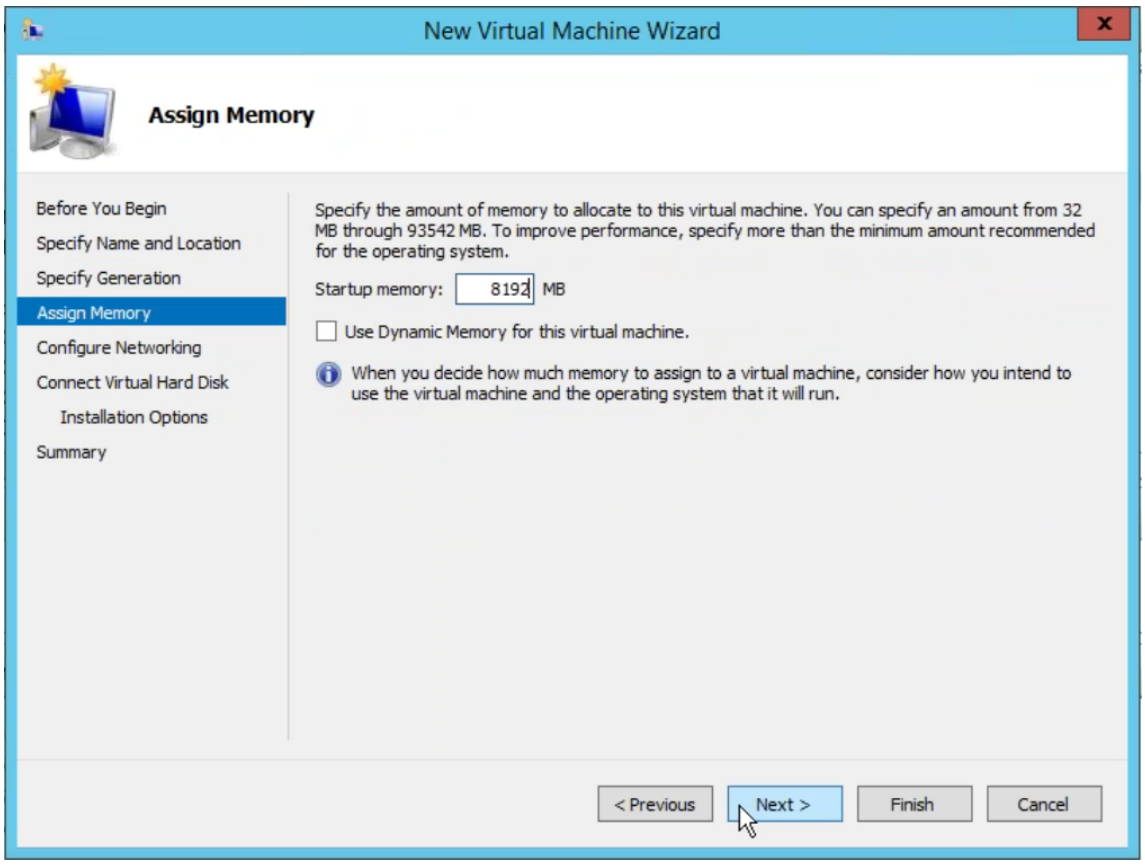
L'**Assistant Nouvelle machine virtuelle** s'affiche. Cliquez sur **Suivant**.

2. Spécifiez un nom pour votre machine virtuelle SD-WAN Center et modifiez l'emplacement de stockage de la machine virtuelle, si nécessaire.Cliquez sur **Suivant**.

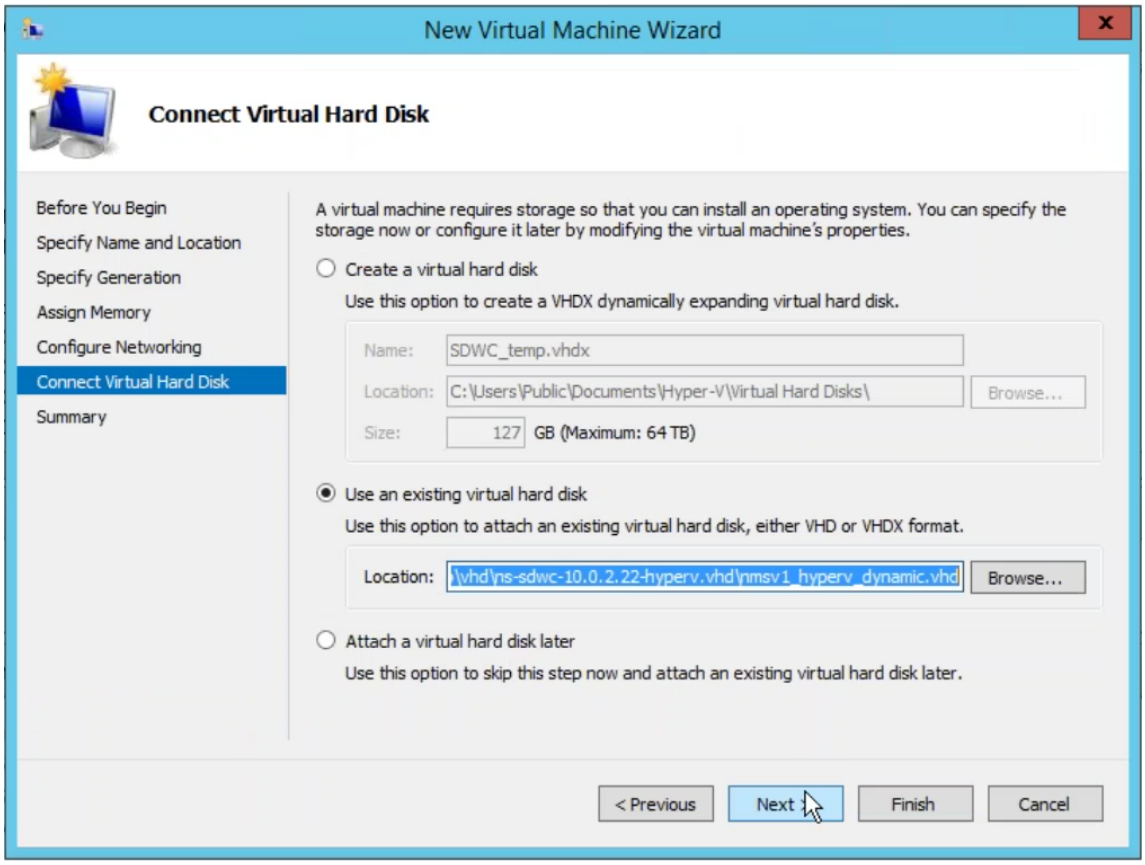


3. Choisissez la génération de machine virtuelle requise. Cliquez sur **Suivant**.
4. Attribuez une mémoire de 8 Go à la machine virtuelle. Cliquez sur **Suivant**.

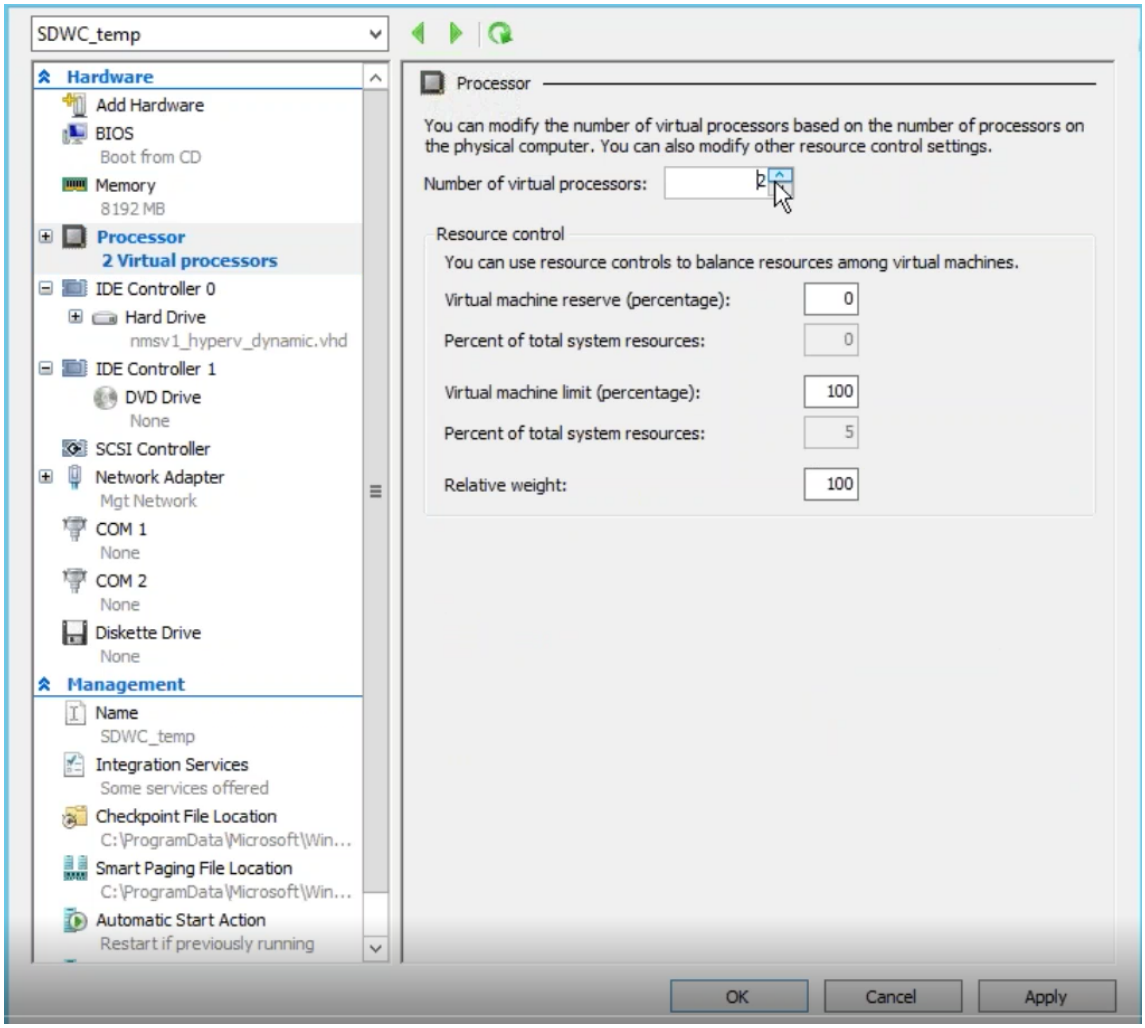
> **Remarque**
>
> La machine virtuelle Citrix SD-WAN Center nécessite un minimum de 8 Go de mémoire pour gérer jusqu'à 64 sites. Pour plus d'informations sur la correspondance entre la mémoire et le nombre de sites, consultez Configuration système requise et installation.



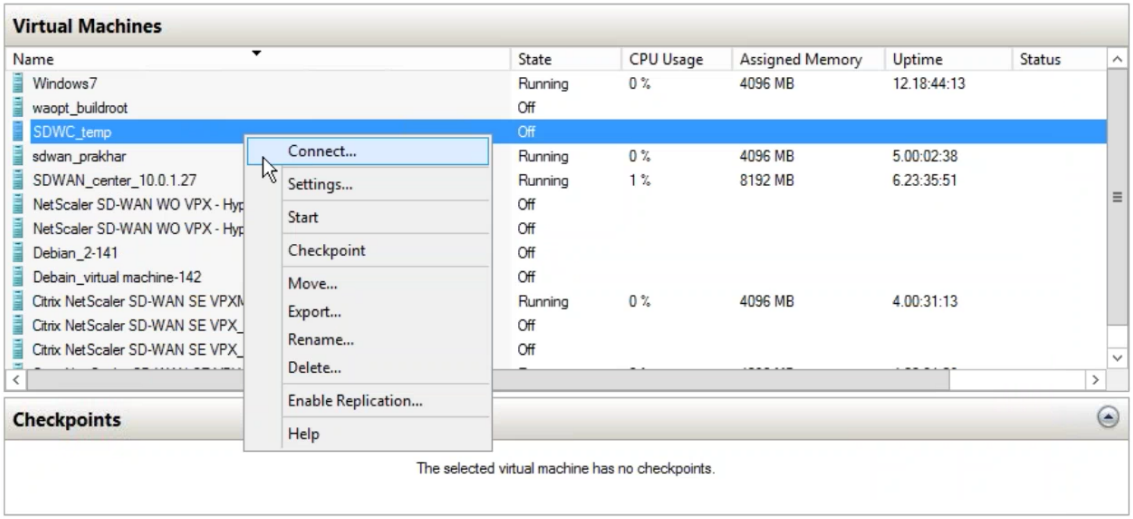
5. Choisissez le commutateur virtuel à utiliser par la carte réseau de la machine virtuelle, cliquez sur **Suivant**.
6. Sélectionnez **Utiliser un disque dur virtuel existant**, parcourez et sélectionnez le fichier VHD SD-WAN Center que vous avez téléchargé. Cliquez sur **Suivant**.



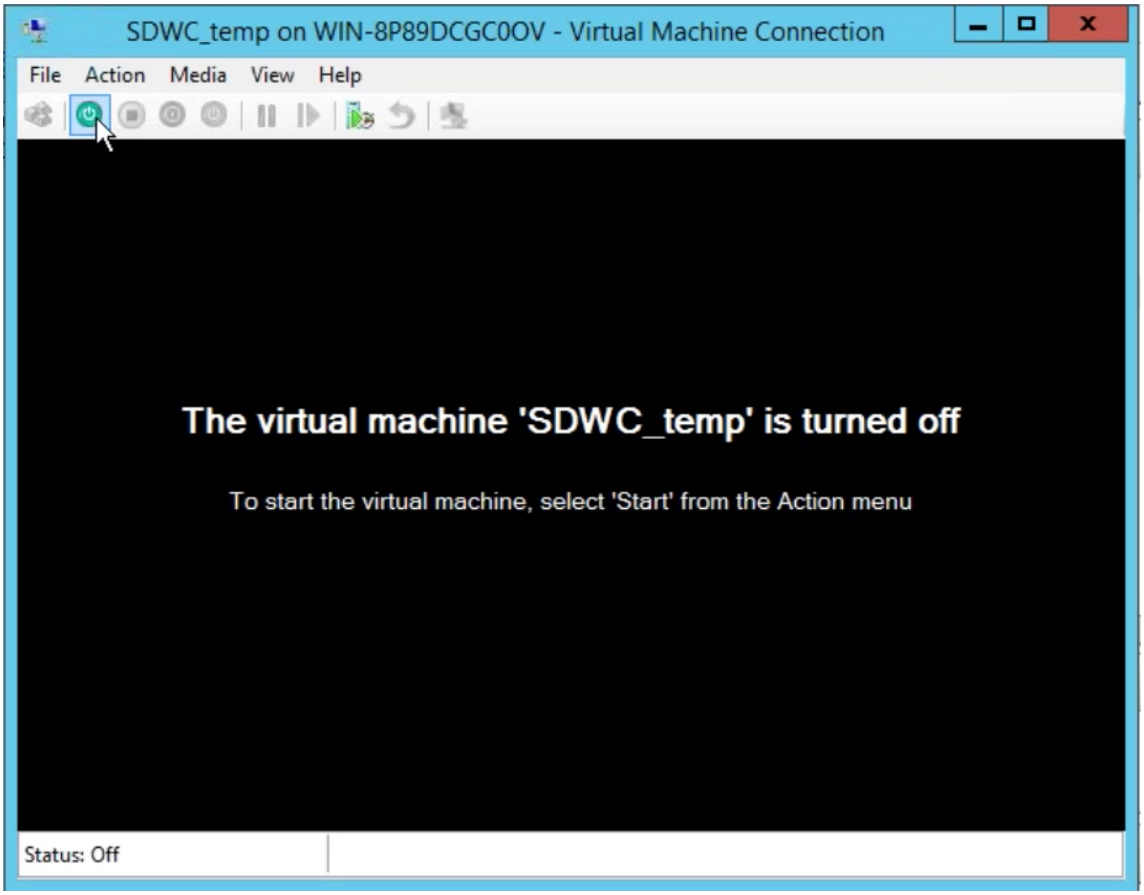
7. Consultez le récapitulatif de la machine virtuelle et modifiez les paramètres si nécessaire, sinon cliquez sur **Terminer**.La machine virtuelle SD-WAN Center est créée et est répertoriée dans la section **Machines virtuelles**.
8. Cliquez avec le bouton droit de la souris sur la machine virtuelle SD-WAN Center et sélectionnez **Paramètres**. Définissez le nombre de processeurs virtuels sur quatre et cliquez sur **Appliquer**.



9. Cliquez avec le bouton droit sur la machine virtuelle SD-WAN Center et cliquez sur **Se connecter**.

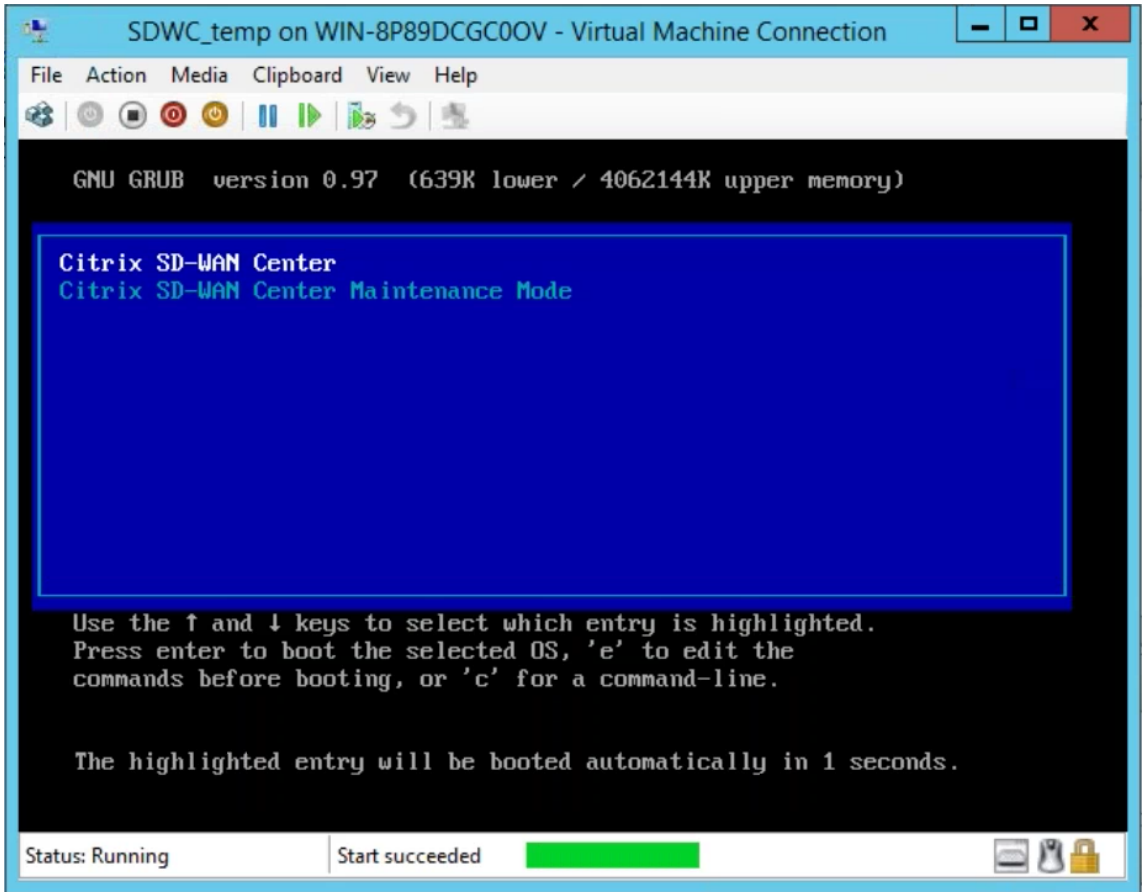


10. Cliquez sur le bouton **Démarrer**.



> **Remarque**
>
> L'installation initiale peut prendre jusqu'à 50 minutes, en fonction du nombre de CPU et de RAM que vous avez configurés.

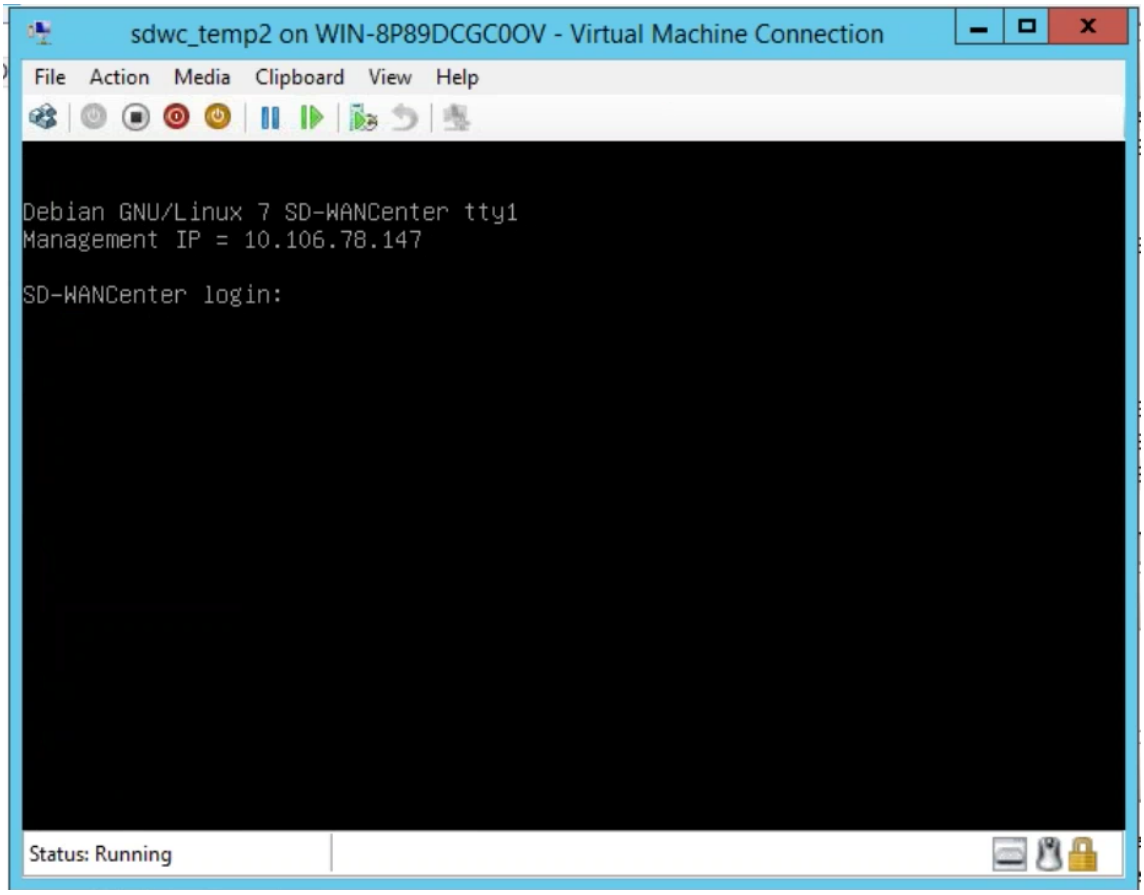
11. Une fois la machine virtuelle démarrée, sélectionnez Citrix SD-WAN Center et appuyez sur Entrée.



12. Connectez-vous à la machine virtuelle. Les informations d'identification de connexion par défaut pour la nouvelle machine virtuelle SD-WAN Center sont les suivantes :

    Identifiant : admin

    Mot de passe : password



L'adresse IP de gestion est affichée dans la console utiliser cette adresse IP pour accéder à l'interface Web de SD-WAN Center.

> **Remarque**
>
> Si DHCP n'est pas configuré dans le réseau SD-WAN, vous devez entrer une adresse IP statique manuellement.

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

1. Connectez-vous à la machine virtuelle. Les informations d'identification de connexion par défaut pour la nouvelle machine virtuelle SD-WAN Center sont les suivantes :

   Identifiant : admin

   Mot de passe : password

2. Dans la console, entrez la commande ***management_ip***de l'interface de ligne de commande.
3. Entrez la commande **set interface <ipaddress> <subnetmask> <gateway>** pour configurer l'adresse IP de gestion.

Utilisez l'adresse IP de gestion pour accéder à l'interface Web de Citrix SD-WAN Center.

Citrix SD-WAN Center sur Azure Marketplace à l'aide d'un modèle de solution

February 17, 2022

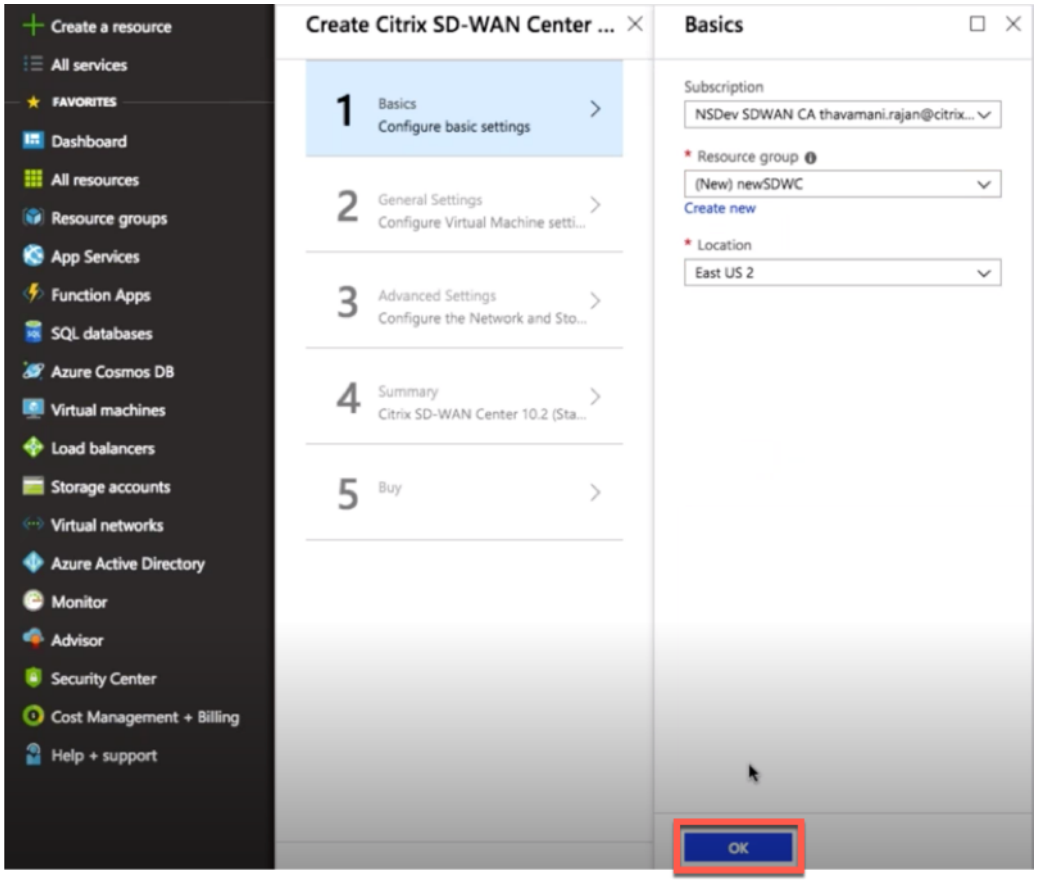
Citrix SD-WAN Center est désormais disponible sur la Place de marché Azure. Vous pouvez déployer Citrix SD-WAN Center en tant que machine virtuelle (VM) dans Azure Cloud à l'aide d'un modèle de solution.

Avant d'installer la machine virtuelle (VM) Citrix SD-WAN Center sur Microsoft Azure, collectez les informations nécessaires comme décrit dans Configuration système requise et installation.

Assurez-vous d'avoir accès à Microsoft Azure.

Pour déployer Citrix SD-WAN Center VPX sur Microsoft Azure :

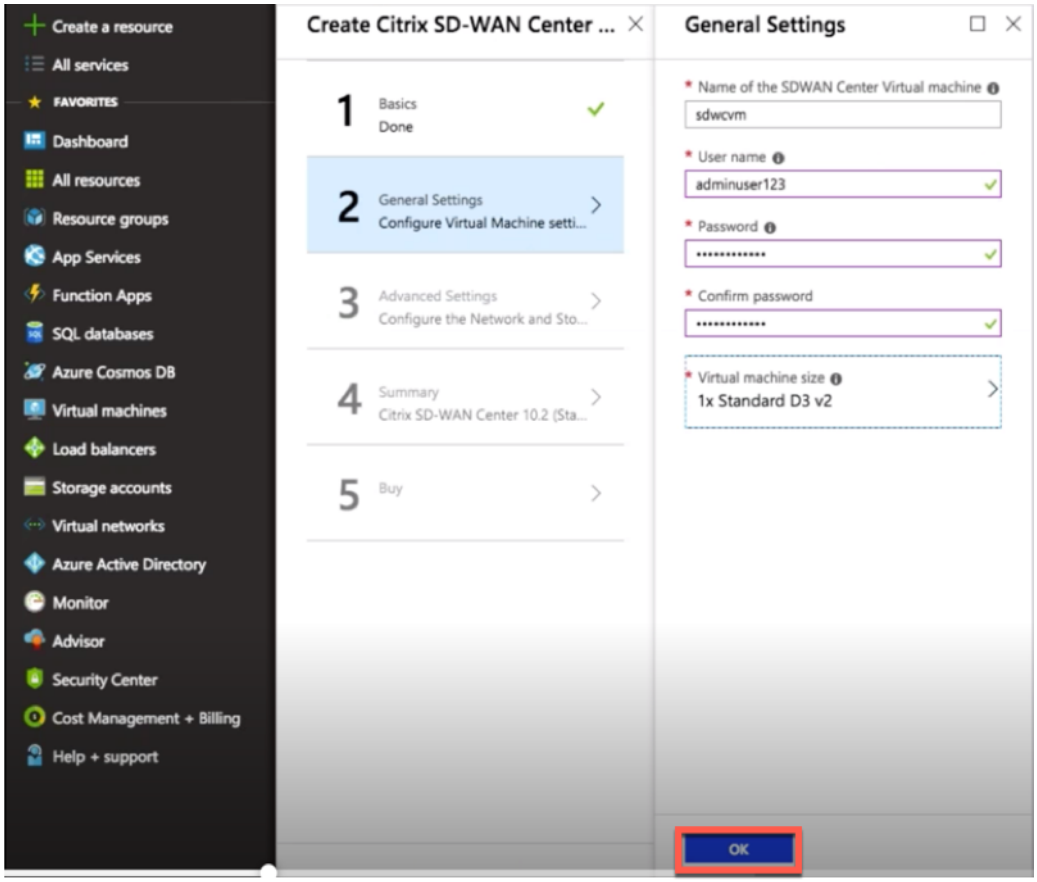
1. Dans Microsoft Azure, accédez à **Accueil > Marketplace**. Recherchez et sélectionnez **Citrix SD-WAN Center**.
2. Cliquez sur **Créer** dans la page **Centre Citrix SD-WAN**. La page **Créer un centre Citrix SD-WAN** s'affiche.
3. Dans la section **Bases**, sélectionnez le type d'abonnement, le groupe de ressources et l'emplacement. Cliquez sur **OK**.



> **REMARQUE :**
>
> Un groupe de ressources est un conteneur qui contient des ressources associées pour une solution Azure. Le groupe de ressources peut inclure toutes les ressources de la solution, ou uniquement les ressources que vous souhaitez gérer en tant que groupe. Vous pouvez décider de la façon dont vous souhaitez allouer des ressources aux groupes de ressources en fonction de votre déploiement.

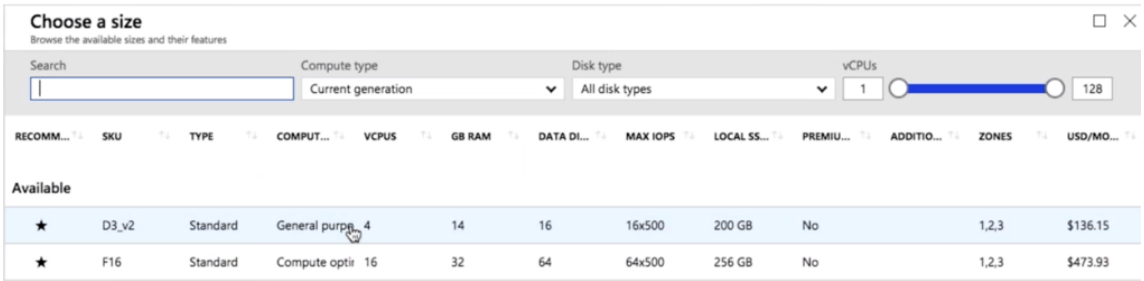
4. Dans la section **Paramètres généraux**, entrez le nom et les informations d'identification qui fournissent un accès ou des privilèges de niveau administrateur pour la machine virtuelle Citrix SD-WAN Center.

   Les informations d'identification fournies dans cette étape 4 seront également utilisées pour définir le mot de passe pour le compte de connexion utilisateur **Admin** (le mot de passe du compte administrateur par défaut peut être modifié avec ces informations d'identification de mot de passe). Cliquez sur **OK**.

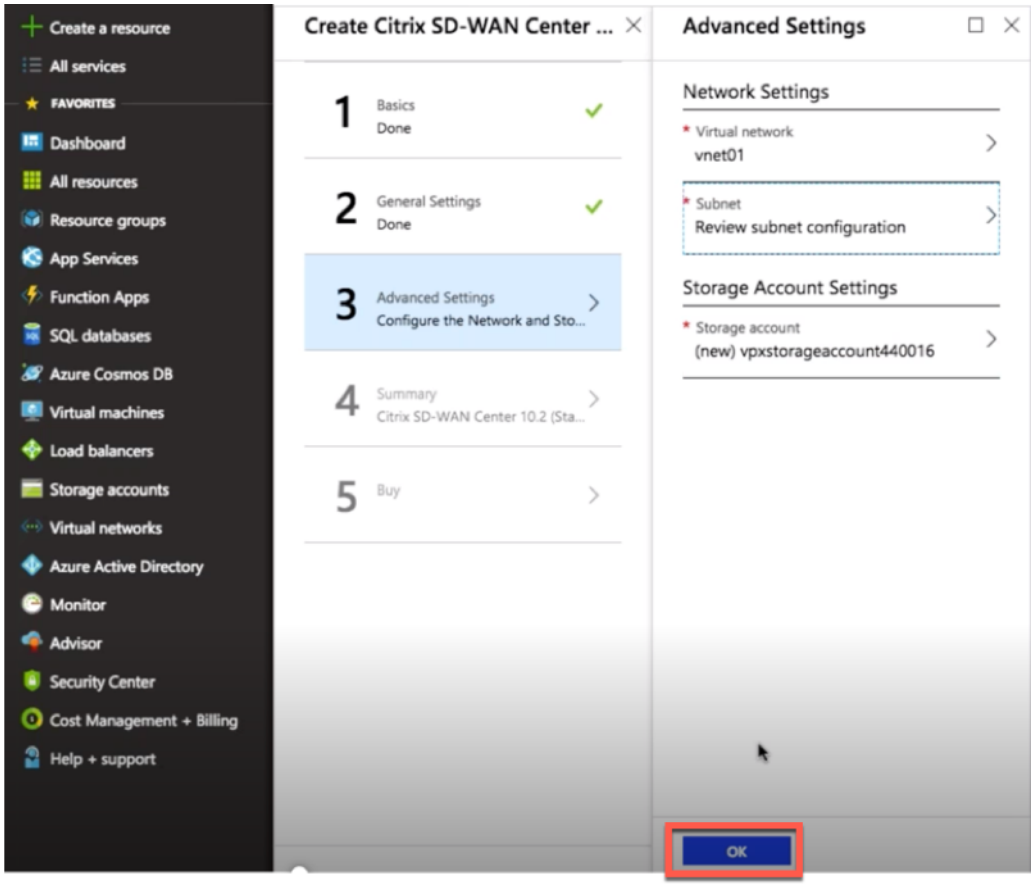


REMARQUE :

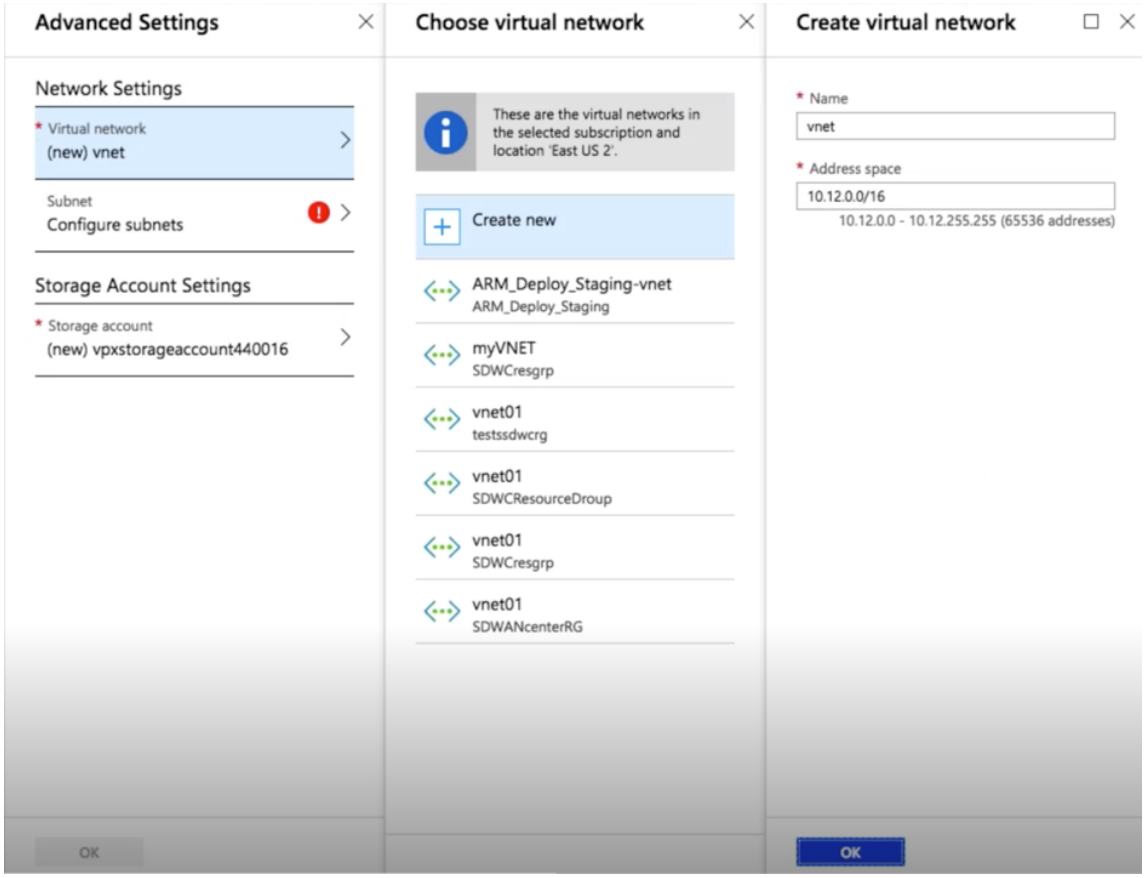
Actuellement, il existe deux tailles de types d'instance disponibles : **Standard_D3_v2** et **Standard_F16**. L'instance D3_v2 peut être utilisée pour surveiller un réseau qui a jusqu'à 64 sites. L'instance F16 est utile pour surveiller un réseau qui a jusqu'à 128 sites. Vous pouvez également rechercher et choisir une taille de machine virtuelle disponible.



5. Dans la section **Paramètres avancés**, configurez le paramètre de **compte réseau et stockage** pour **Citrix SD-WAN Center VPX** en fonction du nombre de sites à surveiller.

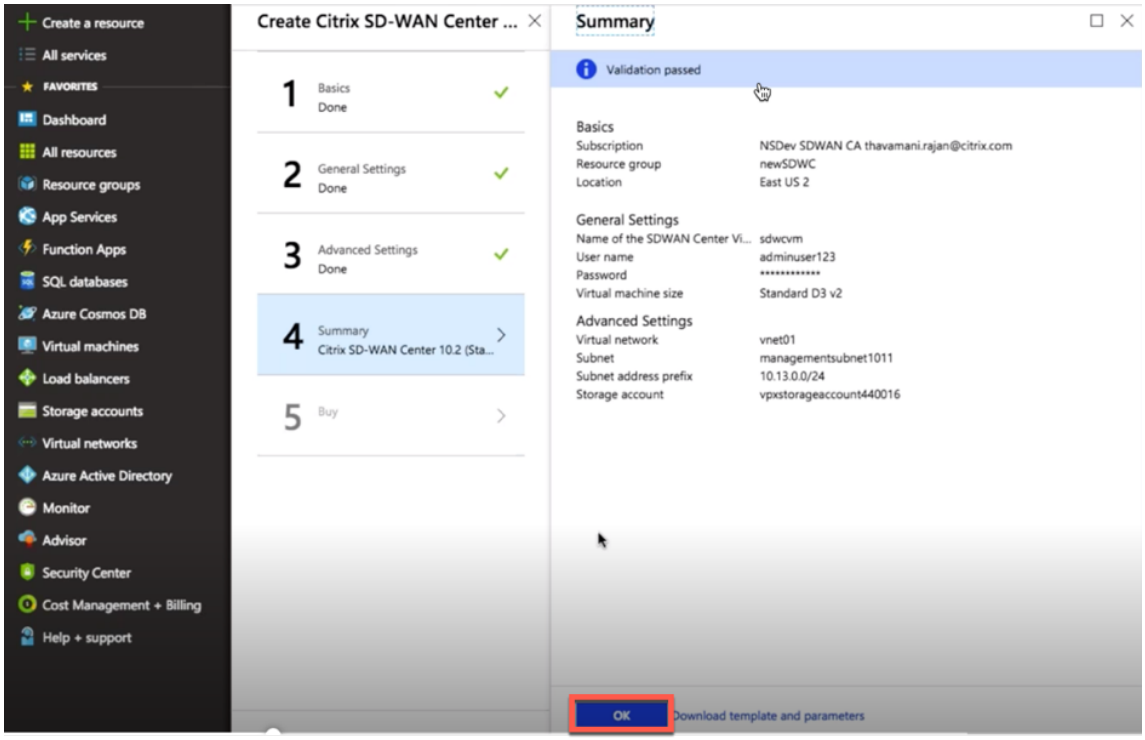


Sélectionnez réseau virtuel dans la liste disponible ou vous pouvez créer un nouveau réseau virtuel en donnant un **nom** et un **espace d'adressage**.

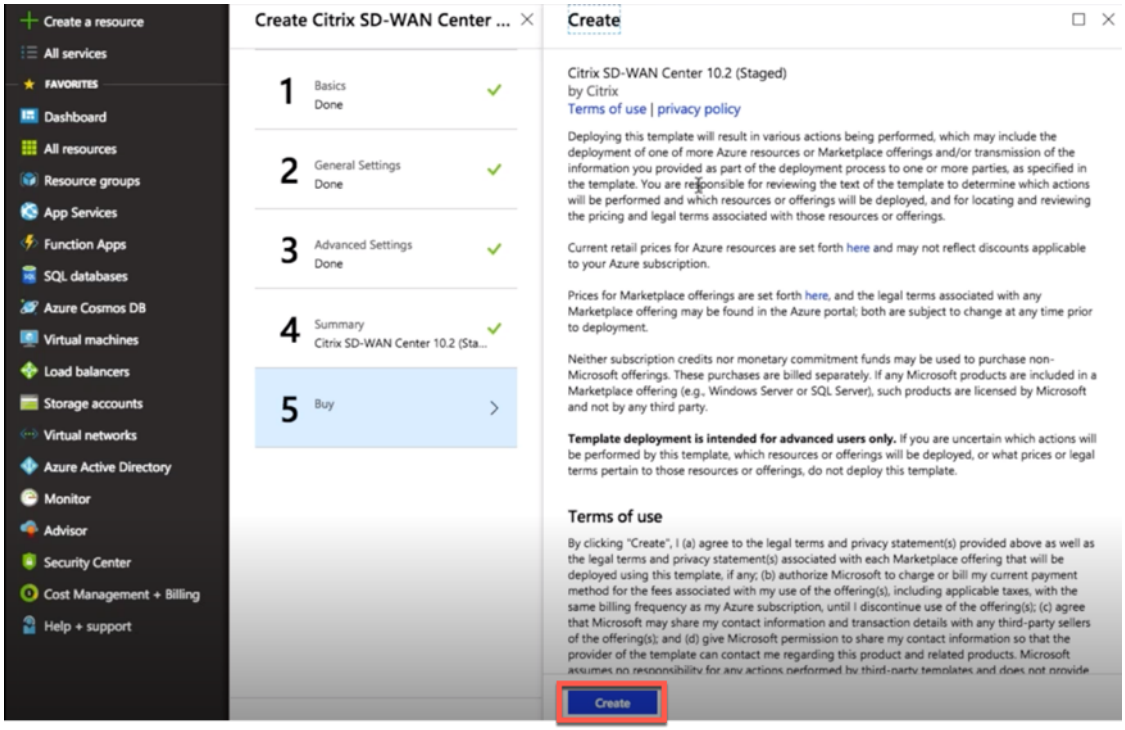


Sélectionnez **Sous-réseau** dans la liste déroulante. Créez un **compte de stockage** et cliquez sur **OK**.

6. La configuration que vous avez fournie lors des étapes précédentes est validée et appliquée. Si vous avez configuré correctement, le message de validation passé s'affiche. Cliquez sur **OK**.



7. Après le déploiement réussi, la page **Créer** s'affiche. Lisez attentivement les **conditions d'utilisation et la politique de confidentialité** et cliquez sur **Créer**.



Attendez que le Provisioning de la machine virtuelle soit terminé, puis connectez-vous avec l'adresse IP qui a été attribuée à cette machine virtuelle (en vérifiant la section mise en réseau et en utilisant

les informations d'identification d'administrateur (définies à l'étape 4) et suivez les instructions générales de déploiement du SD-WAN Center.

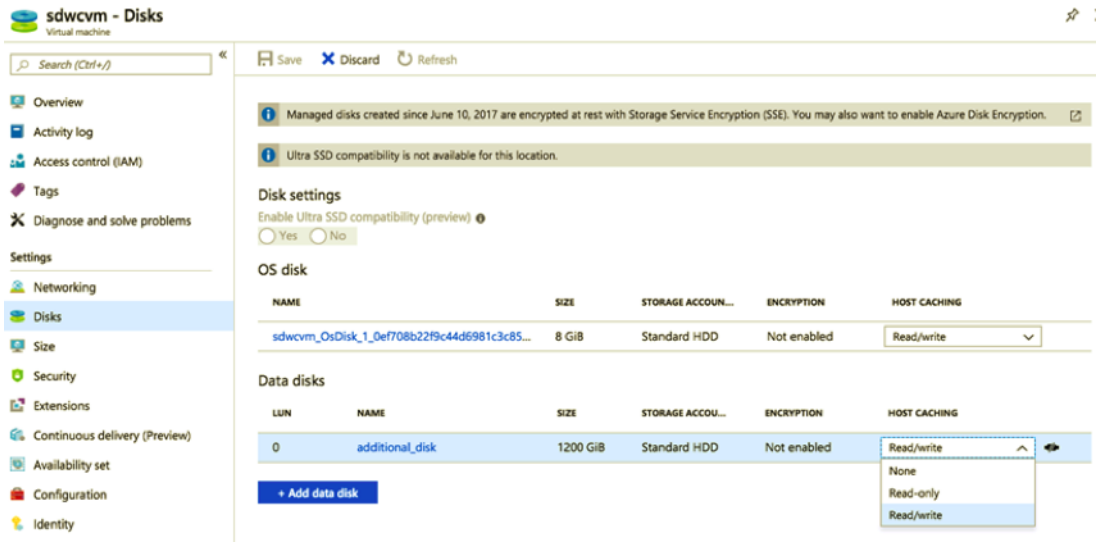
Ajouter un disque de données

Cette section explique comment attacher un nouveau disque de données géré à une machine virtuelle (VM) à l'aide du portail Azure. La taille de la machine virtuelle détermine le nombre de disques de données que vous pouvez attacher.

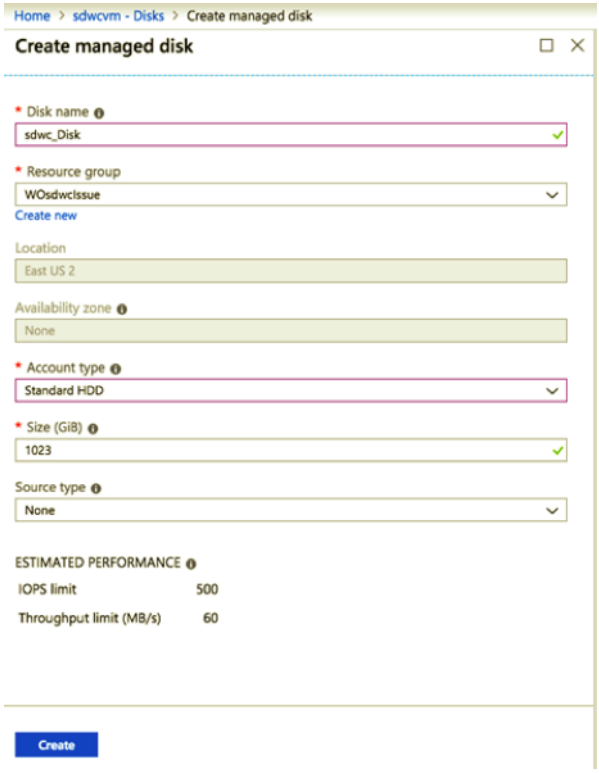
Dans le portail Azure, dans le menu de gauche, sélectionnez **Machines virtuelles** et sélectionnez une machine virtuelle dans la liste.

Effectuez les actions suivantes pour ajouter un disque de données supplémentaire dans Azure SD-WAN Center :

1. Arrêtez la machine virtuelle.
2. Dans le tableau de bord de la machine virtuelle, sélectionnez **Disques** sous la section **Paramètres**.



3. Cliquez sur **+ Ajouter un disque de données** et créez un nouveau disque de données avec l'autorisation de lecture et d'écriture.



Joignez un disque en remplissant les informations obligatoires suivantes :

- **Nom du disque** —Indiquez un nom pour le disque de données de SD-WAN Center.
- **Groupe de ressources** : sélectionnez un groupe de ressources dans la liste déroulante.
- **Type de compte** : sélectionnez un type de compte dans la liste déroulante.
- **Taille (GIB)** —Fournir une taille en gibioctet.
- **Type de stockage** : sélectionnez un type de source dans la liste déroulante.

4. Une fois que vous avez terminé, cliquez sur **OK**.

Pour activer la machine virtuelle, reportez-vous à la rubrique Basculer le stockage actif vers un nouveau stockage de données .

Citrix SD-WAN Center sur AWS au format d'image importable VM

February 17, 2022

Citrix SD-WAN Center est un système de gestion centralisé ou un seul volet de solution de gestion du verre qui permet aux entreprises de configurer, de surveiller et d'analyser toutes les appliances Citrix SD-WAN sur leur WAN.

Instanciation d'un dispositif virtuel (AMI) SD-WAN Center sur AWS

Vous avez besoin d'un compte AWS pour installer une appliance virtuelle SD-WAN Center dans un VPC AWS. Vous pouvez créer un compte AWS ici. Le SD-WAN Center est disponible en tant qu'image machine Amazon (AMI) dans AWS Marketplace.

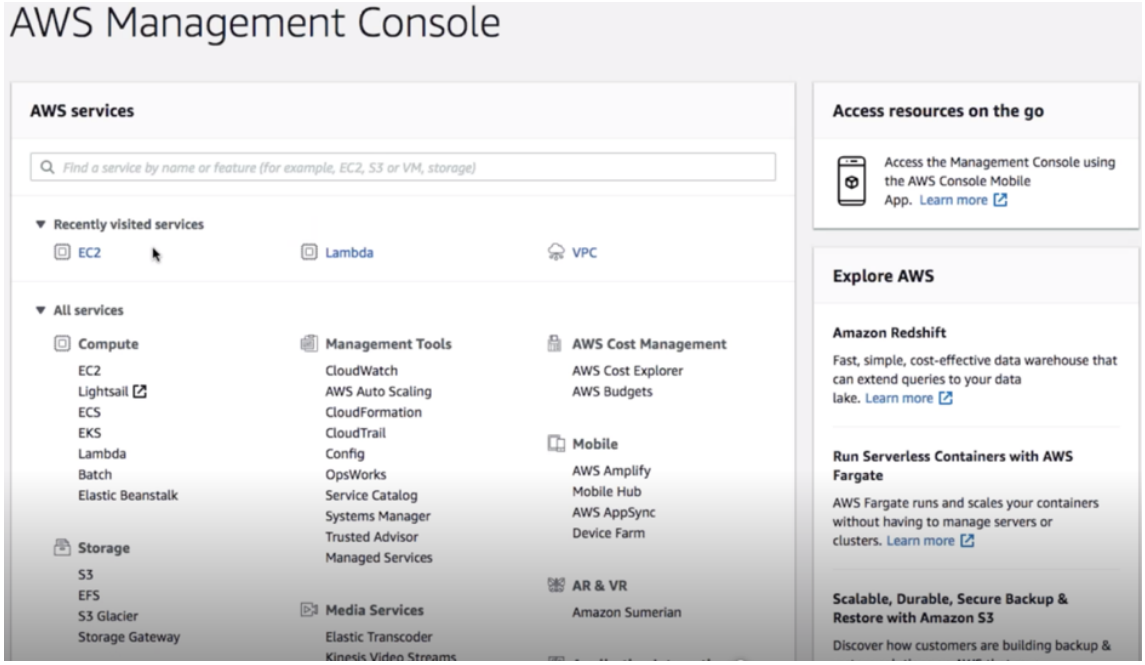
> **Remarque :**
>
> Amazon apporte des modifications fréquentes à ses pages AWS, de sorte que les instructions suivantes peuvent ne pas être mises à jour.

Il existe deux approches pour instancier une appliance virtuelle (AMI) SD-WAN Center sur AWS :

1. **Première approche :** Dans un navigateur Web, tapez http://aws.amazon.com/. Sélectionnez AWS Management Console sous My Account pour ouvrir Amazon Web Services (AWS).

   Deuxième approche :
   dans un navigateur Web, tapez http://console.aws.amazon.com pour ouvrir **Amazon Web Services**.

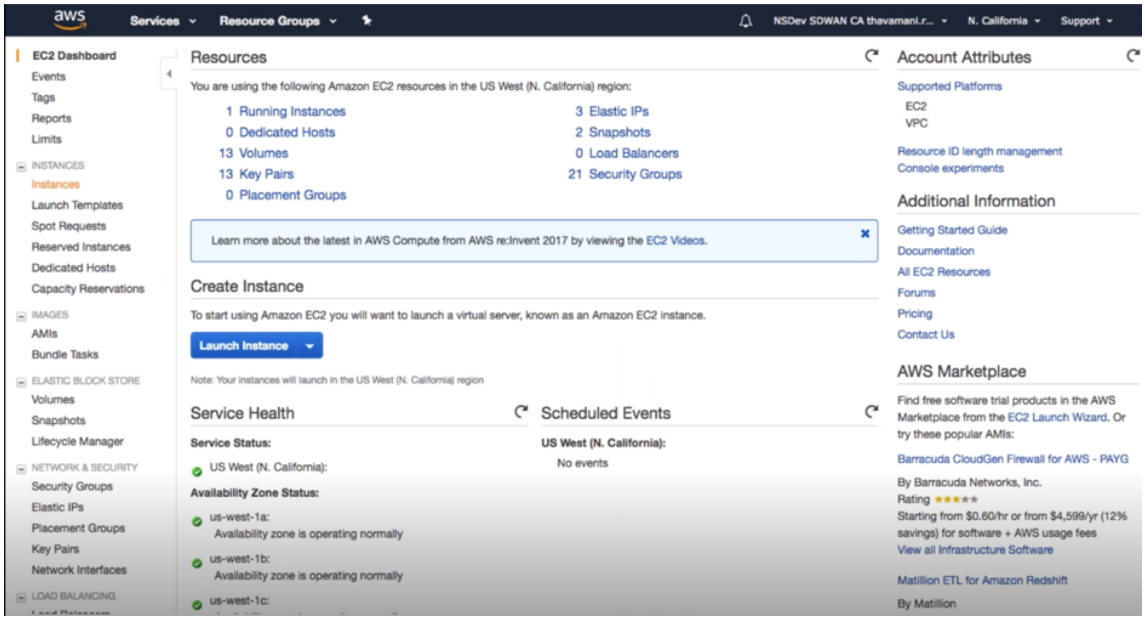
2. Utilisez les informations d'identification de votre compte AWS pour vous connecter. Cela vous amène à la page **Amazon Web Services**. Vous pouvez consulter la liste des **services récemment visités** ainsi que tous les autres services.

   Les appliances Citrix SD-WAN Center offrent l'EC2 en tant qu'instances de service AWS.

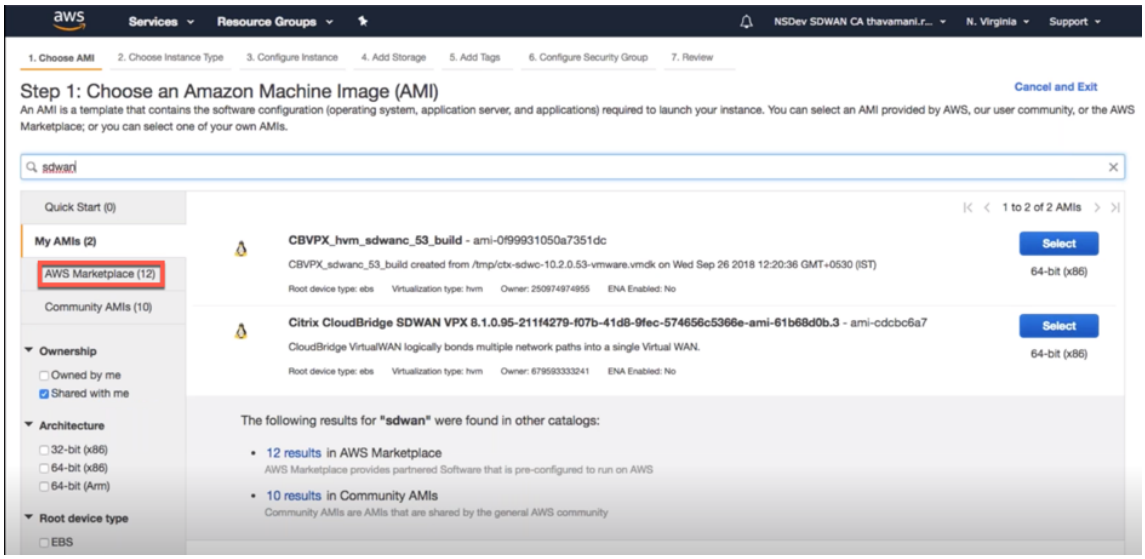
   - **EC2 Dashboard** - cloud de calcul élastique, services virtuels/instances redimensionnables

3. Cliquez sur **EC2** dans la section **Calcul**, puis sélectionnez **Launch Instance**.



Vous pouvez sélectionner l'option **Lancer l'instance** ou accéder manuellement à l'écran **Instance** en sélectionnant l'emplacement de l'option **Instances** sur le côté gauche sous **INSTANCES** (reportez-vous à la capture d'écran ci-dessus).

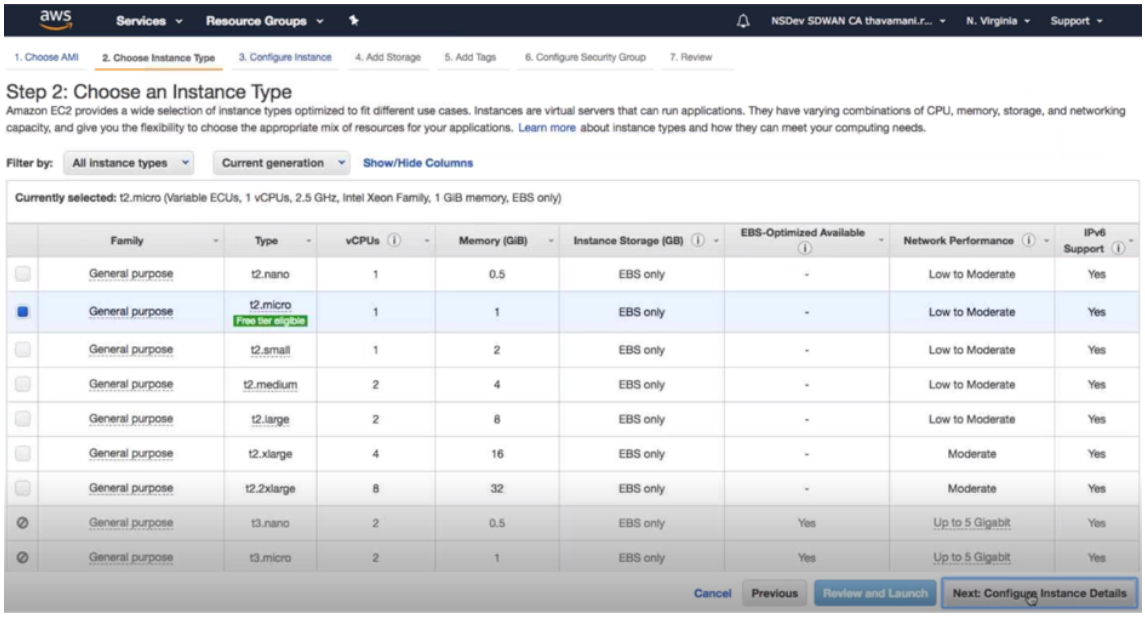
4. Dans la page **Choisir une AMI**, cliquez sur l'onglet **AWS Marketplace**.
5. Dans le champ de texte Rechercher, tapez SD-WAN pour rechercher l'AMI SD-WAN, puis cliquez sur **Rechercher**.



Sur la page des résultats de la recherche, sélectionnez l'une des AMI Citrix SD-WAN Center avec la dernière version, cliquez sur **Sélectionner**.

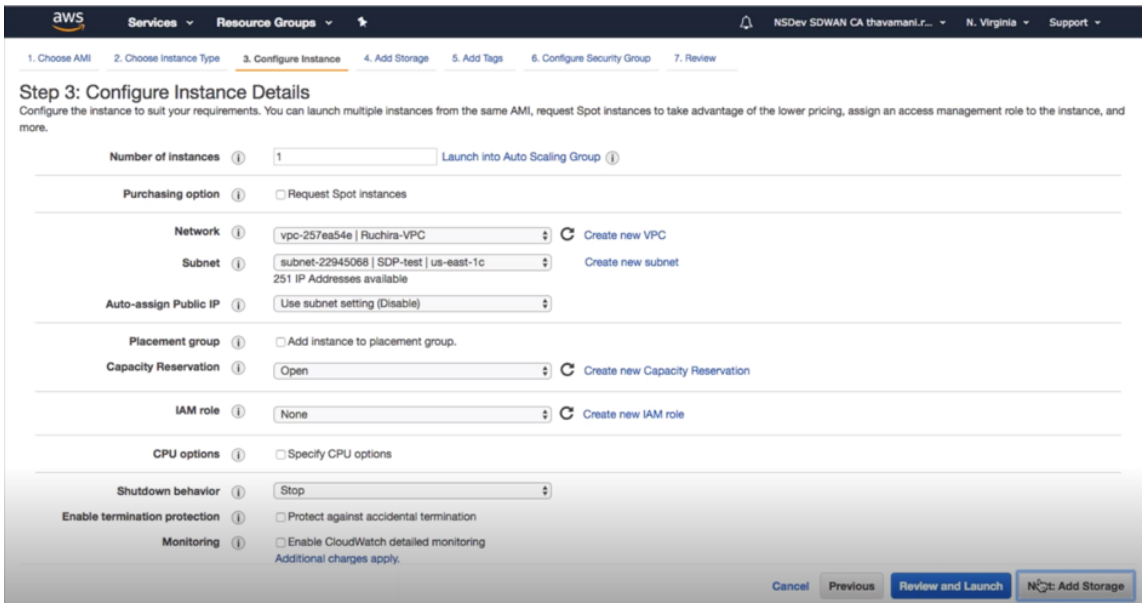
Un modèle d'**AMI** contient la configuration logicielle, y compris le système d'exploitation, le serveur d'applications et les applications. Ce modèle est requis pour lancer des instances.

6. Choisissez un type d'instance et sélectionnez **Suivant : Configurer le détail de l'instance**. Vous pouvez filtrer votre recherche en sélectionnant un type d'instance spécifique ou tout type d'instance avec la génération actuelle.

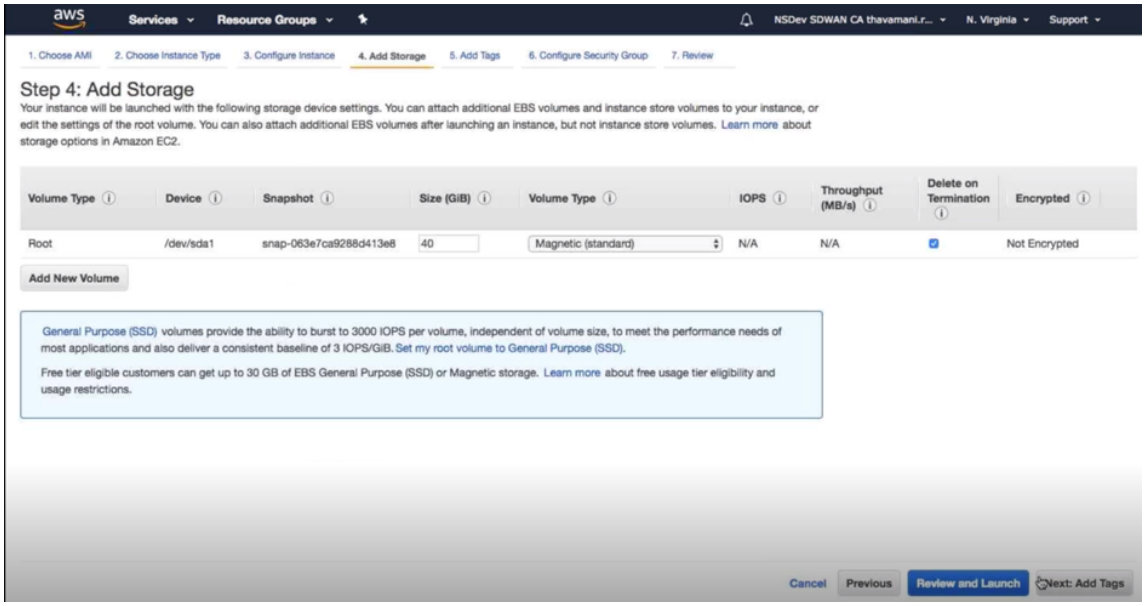


Amazon EC2 fournit un large choix de types d'instance optimisés pour s'adapter à différents cas d'utilisation. Les instances sont des serveurs virtuels capables d'exécuter des applications.

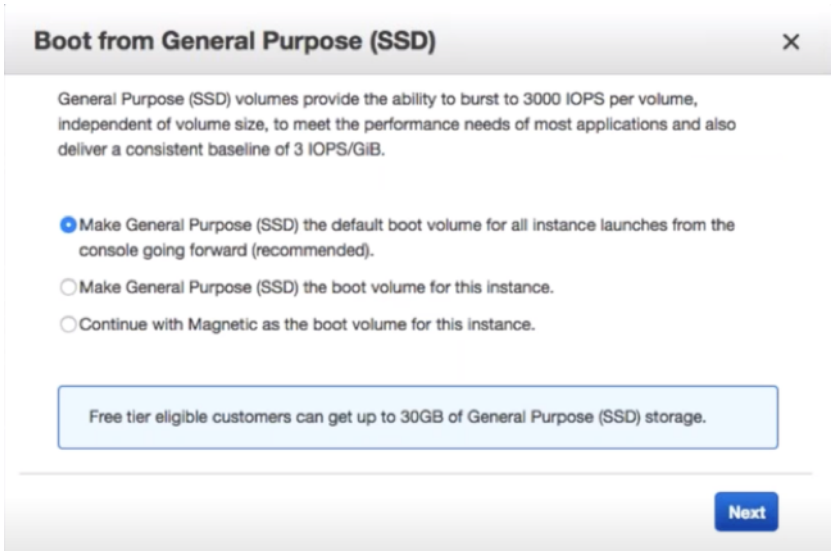
7. Dans la page **Configurer l'instance**, tapez 1 dans la zone **de texte Nombre d'instances** et remplissez les autres détails tels que Réseau, Sous-réseau, etc. pour une instance spécifique, selon les besoins. Cliquez sur **Suivant : Ajouter un stockage**.



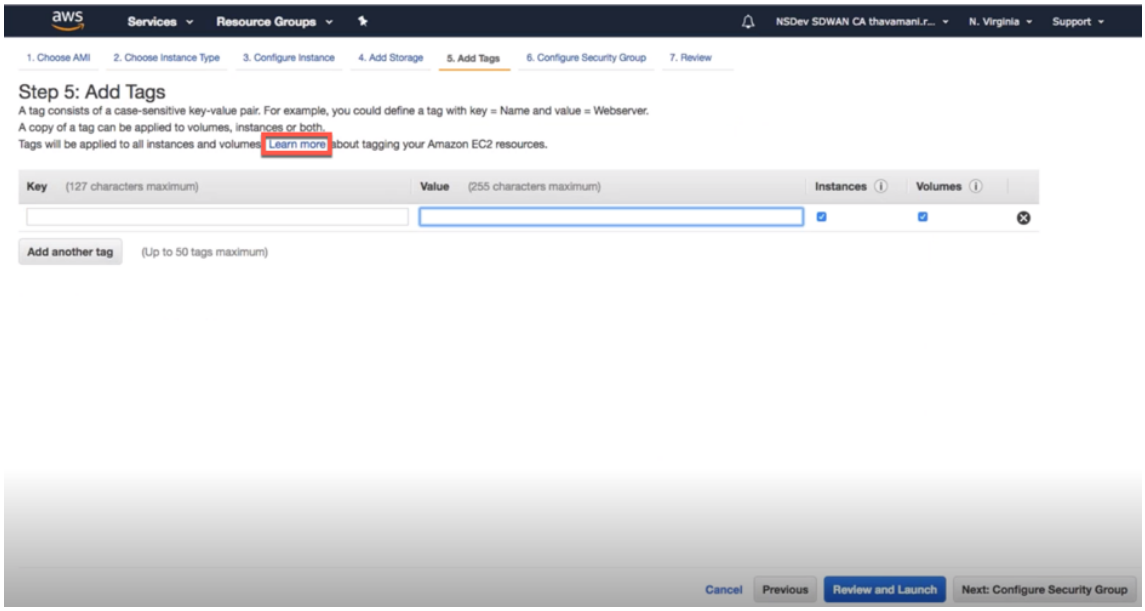
8. L'instance est lancée avec les paramètres du périphérique de stockage. Vous pouvez ajouter un nouveau volume séparément une fois l'instance provisionnée.



9. Cliquez sur **Review and Launch** pour sélectionner l'option de volume de démarrage selon vos besoins. Cliquez sur **Suivant**.



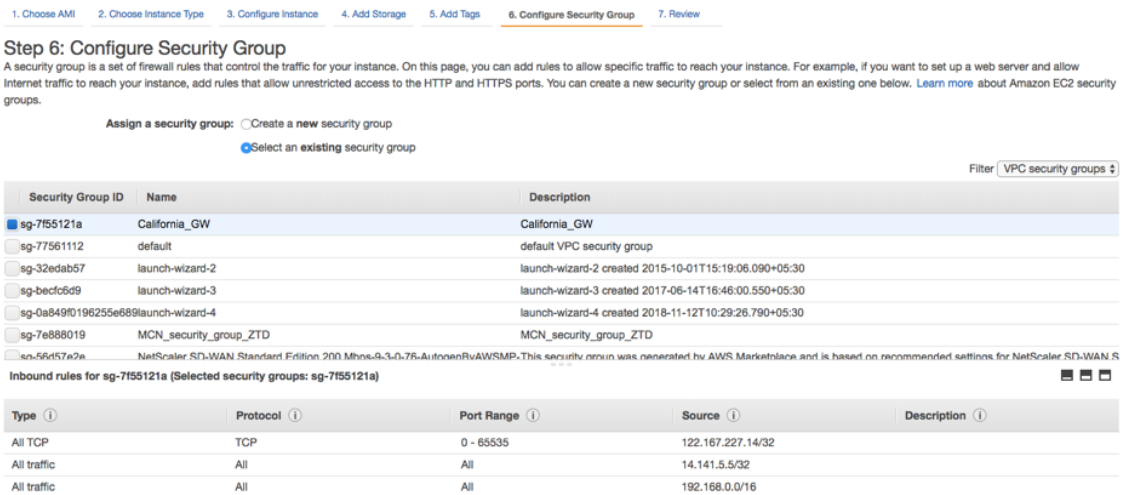
10. Ajoutez ou définissez une balise avec un **nom de clé** et une **valeur**. Cliquez sur **En savoir plus** pour en savoir plus sur le balisage. Vous pouvez ajouter jusqu'à 50 balises au maximum. Cliquez sur **Suivant : Configurer le groupe de sécurité**.



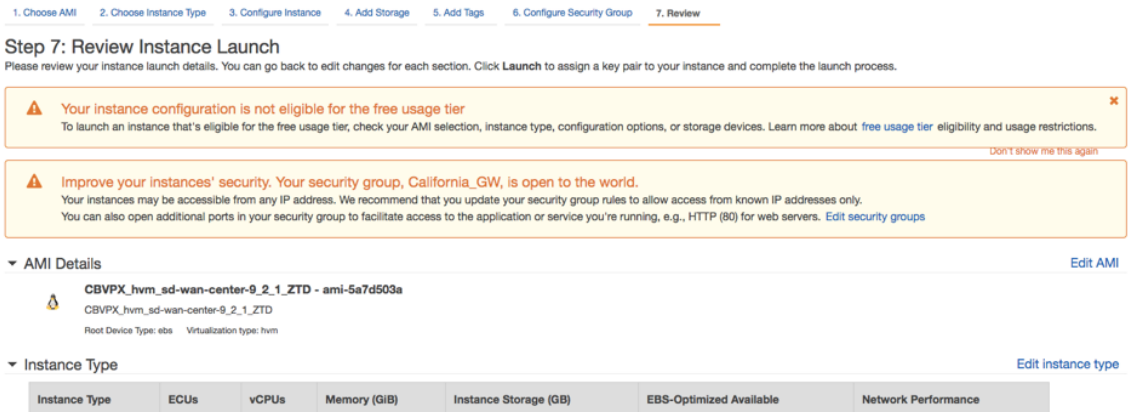
> **Remarque :**
>
> REMARQUE : La longueur d'une clé de balise doit être comprise entre 1 et 127 caractères.

11. Vous pouvez créer un groupe de sécurité général qui aide à contrôler le trafic de l'instance. Vous pouvez créer un nouveau groupe de sécurité ou sélectionner un groupe de sécurité existant dans la liste.

> **Remarque :**
>
> Assurez-vous que le groupe de sécurité permet aux connexions entrantes sur le port 2156 de collecter des données à partir des appliances Citrix SD-WAN.



12. Vérifiez les détails de lancement de l'instance, puis cliquez sur **Lancer**. Une fenêtre contextuelle apparaît pour demander la création d'une paire de clés. Il est obligatoire de créer une paire de clés pour l'instance.



Authentification à deux facteurs

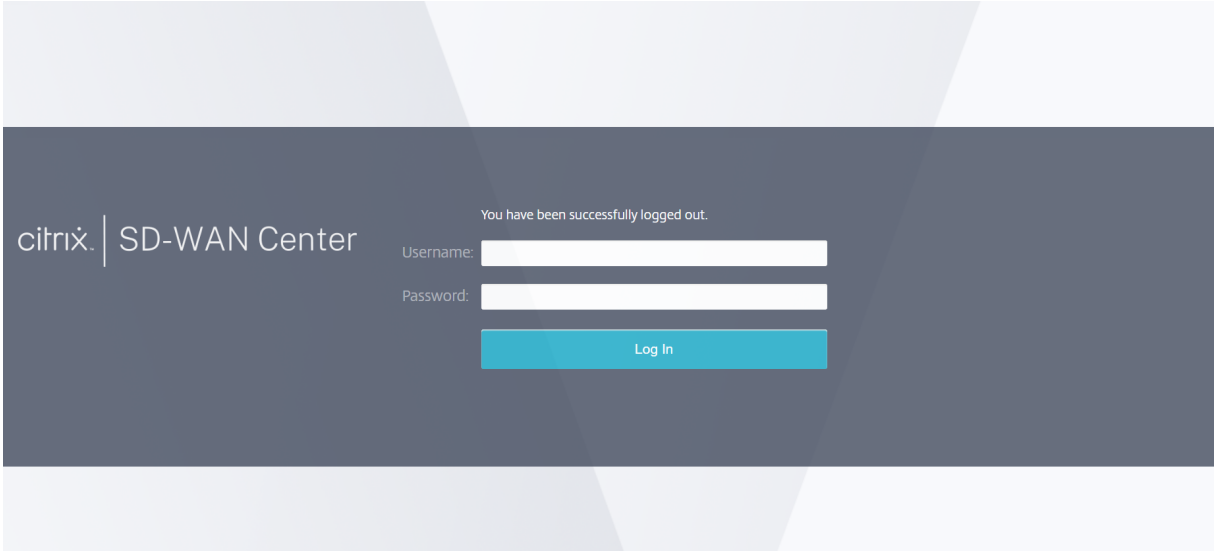
February 17, 2022

L'authentification à deux facteurs (TFA) présente deux facteurs d'authentification pour accéder au Centre Citrix SD-WAN pour les comptes d'utilisateurs locaux et distants. Il introduit une couche de sécurité supplémentaire dans la séquence de connexion Citrix SD-WAN Center.

Le premier niveau d'authentification pour un compte d'utilisateur local est atteint à l'aide du mot de passe configuré sur Citrix SD-WAN Center. Pour plus d'informations, consultez la section Comptes d'utilisateurs.

Le premier niveau d'authentification pour un compte d'utilisateur distant est atteint en utilisant le serveur d'authentification principal RADIUS ou TACACS+. Pour plus d'informations, consultez Authentification principale.

Un serveur d'authentification supplémentaire RADIUS ou TACACS+ secondaire peut être configuré pour les comptes d'utilisateurs locaux et distants afin d'activer l'authentification à deux facteurs. Pour plus d'informations, consultez Authentification secondaire.



Informations d'identification de connexion au Centre Citrix SD-WAN :

- **Nom d'utilisateur** : nom d'utilisateur configuré sur SD-WAN Center ou sur le serveur d'authentification principal.
- **Mot de passe** : mot de passe configuré sur SD-WAN Center ou sur le serveur d'authentification principal.
- **Mot de passe secondaire** : mot de passe configuré sur le serveur d'authentification secondaire.

> **Remarque**
>
> L'option **Mot de passe secondaire** apparaît uniquement lorsque le serveur d'authentification secondaire est configuré.

Authentification

February 17, 2022

Vous pouvez configurer des serveurs d'authentification tels que RADIUS ou TACACS+ pour authentifier les utilisateurs distants qui se connectent à Citrix SD-WAN Center. L'authentification principale est le premier facteur d'authentification pour les utilisateurs distants lorsque l'authentification à deux facteurs est activée. Pour plus d'informations, consultez Authentification à deux facteurs.

> **Remarque**
>
> Assurez-vous que les comptes d'utilisateur sont créés sur les serveurs d'authentification requis.

Serveur d'authentification RADIUS

Pour utiliser l'authentification RADIUS, vous devez spécifier et configurer au moins un serveur RADIUS. Vous pouvez également configurer des serveurs de sauvegarde redondants, jusqu'à trois serveurs RADIUS au maximum. Les serveurs sont vérifiés séquentiellement, en commençant par le serveur répertorié en premier dans la section **Serveurs**. Assurez-vous que les comptes d'utilisateur requis sont créés sur le serveur d'authentification RADIUS.

Pour activer et configurer l'authentification RADIUS :

1. Dans l'interface Web Citrix SD-WAN Center, accédez à **Administration** > **Paramètres d'utilisateur/d'authentification**.
2. Dans la section **Authentification principale** > **Authentification RADIUS**, **activez la case à cocher Activer l'authentification RADIUS**.

   > **Remarque**
   >
   > Si l'authentification TACACS+ est déjà activée, elle est désactivée.

3. Dans le champ **Délai d'expiration**, entrez l'intervalle de temps (en secondes) pour attendre une réponse d'authentification du serveur RADIUS.

   La valeur du délai d'attente doit être inférieure ou égale à 60 secondes.
4. Dans le champ **Clé serveur**, entrez une clé secrète à utiliser lors de la connexion aux serveurs RADIUS.
5. Dans les champs **Confirmer la clé du serveur**, entrez à nouveau la clé secrète.

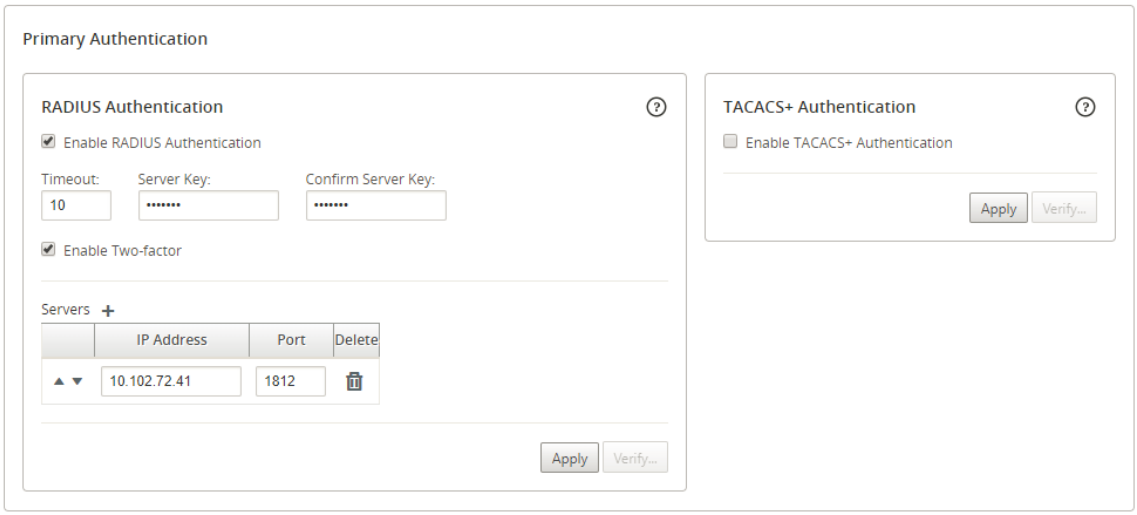
   > **Remarque**
   >
   > Les paramètres de **délai d'attente** et de **clé de serveur** sont appliqués à tous les serveurs configurés**.**

6. Sélectionnez **Activer deux facteurs** pour activer l'authentification à deux facteurs.

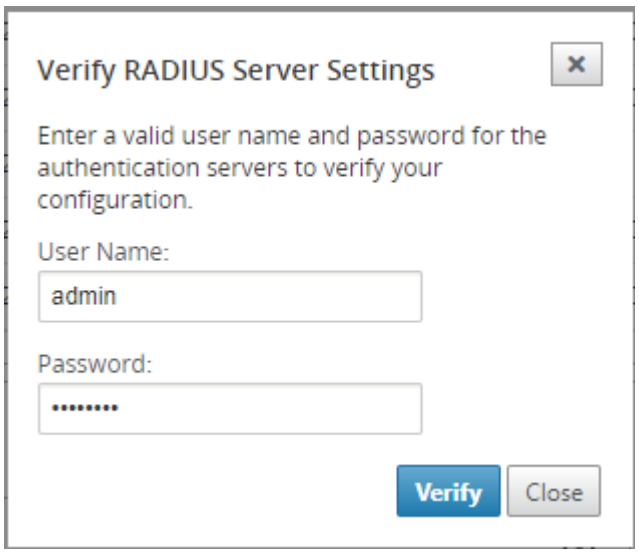
   > **Remarque**
   >
   > L'option **Activer deux facteurs** s'affiche uniquement lorsque le serveur d'authentification secondaire est configuré.
   >
   > Configurez un serveur d'authentification secondaire, RADIUS ou TACAS+. Pour plus d'informations, consultez Authentification secondaire.

7. Cliquez sur l'icône plus (+) en regard de **Serveurs** pour ajouter un serveur RADIUS.
8. Dans le champ **Adresse IP**, entrez l'adresse IP de l'hôte du serveur RADIUS.

9. Dans le champ **Port**, entrez le numéro de port du serveur RADIUS. Le numéro de port par défaut est 1812.



10. Cliquez sur **Apply**.
11. Cliquez sur **Vérifier** pour vérifier la connexion au serveur RADIUS. La boîte de dialogue **Vérifier les paramètres du serveur RADIUS** s'affiche.



12. Entrez un nom d'utilisateur et un mot de passe valides pour les serveurs d'authentification, puis cliquez sur**Vérifier**.

Pour configurer plus de serveurs, répétez les étapes 7 à 12.

Serveur d'authentification TACACS+

Pour utiliser TACACS+, vous devez spécifier et configurer au moins un serveur TACACS+. Vous pouvez également configurer des serveurs de sauvegarde redondants, jusqu'à un maximum de trois serveurs

TACACS+. Les serveurs sont vérifiés séquentiellement, en commençant par le serveur répertorié en premier dans la section **Serveurs**. Assurez-vous que les comptes utilisateur requis sont créés sur le serveur d'authentification TACACS+.

Pour activer et configurer l'authentification TACACS+:

1. Dans l'interface Web Citrix SD-WAN Center, accédez à **Administration** > **Paramètres d'utilisateur/d'authentification**.
2. Dans la section **Authentification primaire > AuthentificationTACACS+**,**activez la case à cocher Activer l'authentification TACACS+**.

   > **Remarque**
   >
   > Si l'authentification RADIUS est déjà activée, elle est désactivée.

3. Dans le champ Délai d'**expiration**, entrez l'intervalle de temps (en secondes) pour attendre une réponse d'authentification du serveur TACACS+.

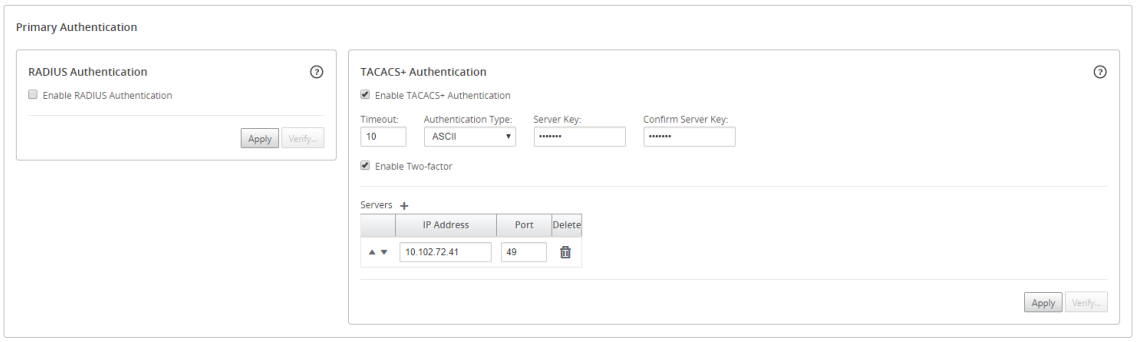
   La valeur du délai d'attente doit être inférieure ou égale à 60 secondes.
4. Dans le champ **Type d'authentification**, sélectionnez la méthode de chiffrement à utiliser pour envoyer le nom d'utilisateur et le mot de passe au serveur TACACS+.
5. Dans le champ **Clé serveur**, entrez une clé secrète à utiliser lors de la connexion aux serveurs TACACS+.
6. Dans les champs **Confirmer la clé du serveur**, entrez à nouveau la clé secrète.

   > **Remarque**
   >
   > Les paramètres de **délai d'expiration**, de **type d'authentification** et de **clé de serveur** sont appliqués à tous les serveurs configurés.

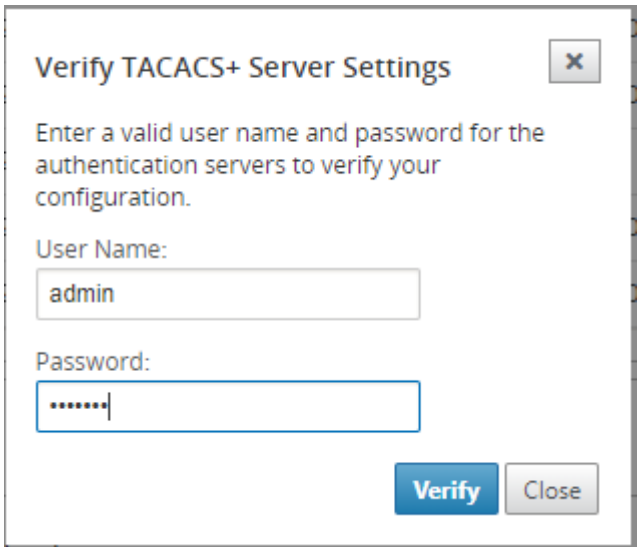
7. Sélectionnez **Activer deux facteurs** pour activer l'authentification à deux facteurs.

   > **Remarque**
   >
   > L'option **Activer deux facteurs** s'affiche uniquement lorsque le serveur d'authentification secondaire est configuré.
   >
   > Configurez un serveur d'authentification secondaire, RADIUS ou TACAS+. Pour plus d'informations, consultez Authentification secondaire.

8. Cliquez sur l'icône plus (+) en regard de **Serveurs** pour ajouter un serveur TACACS+.
9. Dans le champ **Adresse IP**, entrez l'adresse IP de l'hôte du serveur TACACS+.
10. Dans le champ **Port**, entrez le numéro de port du serveur TACACS+. Le numéro de port par défaut est 49.



11. Cliquez sur **Apply**.
12. Cliquez sur **Vérifier** pour vérifier la connexion au serveur RADIUS. La boîte de dialogue **Vérifier les paramètres du serveur TACACS+** s'affiche.



13. Entrez un nom d'utilisateur et un mot de passe valides pour les serveurs d'authentification, puis cliquez sur**Vérifier**.

    Pour configurer plus de serveurs, répétez les étapes 8 à 13.

Authentification

February 17, 2022

L'authentification secondaire est configurée pour activer l'authentification à deux facteurs pour les comptes d'utilisateurs locaux et distants. Vous pouvez configurer le serveur d'authentification RADIUS ou TACACS+ comme service d'authentification secondaire. Pour plus d'informations, consultez Authentification à deux facteurs.

> **Remarque**
>
> Assurez-vous que les comptes d'utilisateur sont créés sur les serveurs d'authentification requis. Le mot de passe du compte d'utilisateur doit être utilisé comme deuxième facteur dans la séquence de connexion Citrix SD-WAN Center.

Serveur d'authentification RADIUS secondaire

Pour utiliser l'authentification RADIUS, vous devez spécifier et configurer au moins un serveur RADIUS. Vous pouvez également configurer des serveurs de sauvegarde redondants, jusqu'à trois serveurs RADIUS au maximum. Les serveurs sont vérifiés séquentiellement, en commençant par le serveur répertorié en premier dans la section **Serveurs**. Assurez-vous que les comptes d'utilisateur requis sont créés sur le serveur d'authentification RADIUS.

Pour activer et configurer l'authentification RADIUS :

1. Dans l'interface Web Citrix SD-WAN Center, accédez à **Administration** > **Paramètres d'utilisateur/d'authentification**.
2. Dans la section **Authentification secondaire** > **Authentification RADIUS**, **activez la case à cocher Activer l'authentification RADIUS secondaire**.

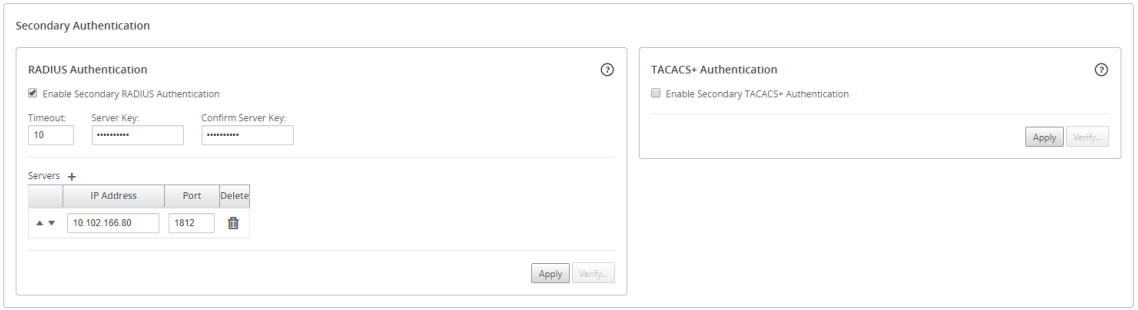
   > **Remarque**
   >
   > Si l'authentification TACACS+ est déjà activée, elle est désactivée.

3. Dans le champ **Délai d'expiration**, entrez l'intervalle de temps (en secondes) pour attendre une réponse d'authentification du serveur RADIUS.

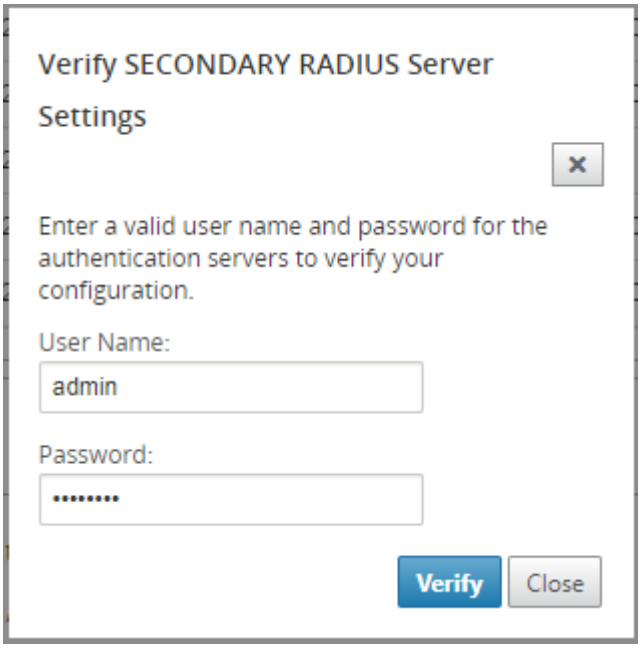
   La valeur du délai d'attente doit être inférieure ou égale à 60 secondes.
4. Dans le champ **Clé serveur**, entrez une clé secrète à utiliser lors de la connexion aux serveurs RADIUS.
5. Dans les champs **Confirmer la clé du serveur**, entrez à nouveau la clé secrète.

   > **Remarque**
   >
   > Les paramètres de **délai d'attente** et de **clé de serveur** sont appliqués à tous les serveurs configurés**.**

6. Cliquez sur l'icône plus (+) en regard de **Serveurs** pour ajouter un serveur RADIUS.
7. Dans le champ **Adresse IP**, entrez l'adresse IP de l'hôte du serveur RADIUS.
8. Dans le champ **Port**, entrez le numéro de port du serveur RADIUS. Le numéro de port par défaut est 1812.



9. Cliquez sur **Apply**.
10. Cliquez sur **Vérifier** pour vérifier la connexion au serveur RADIUS. La boîte de dialogue **Vérifier les paramètres du serveur RADIUS secondaire** s'affiche.



11. Entrez un nom d'utilisateur et un mot de passe valides pour les serveurs d'authentification, puis cliquez sur**Vérifier**.

Pour configurer plus de serveurs, répétez les étapes 6 à 11.

Serveur d'authentification TACACS+ secondaire

Pour utiliser TACACS+, vous devez spécifier et configurer au moins un serveur TACACS+. Vous pouvez également configurer des serveurs de sauvegarde redondants, jusqu'à un maximum de trois serveurs TACACS+. Les serveurs sont vérifiés séquentiellement, en commençant par le serveur répertorié en premier dans la section **Serveurs**. Assurez-vous que les comptes utilisateur requis sont créés sur le serveur d'authentification TACACS+.

Pour activer et configurer l'authentification TACACS+:

1. Dans l'interface Web de SD-WAN Center, accédez à **Administration** > **Paramètres utilisateur/authentification**.
2. Dans la section **Authentification secondaire** > **Authentification TACACS+**, activez la case à cocher **Activer l'authentification TACACS+ secondaire**.

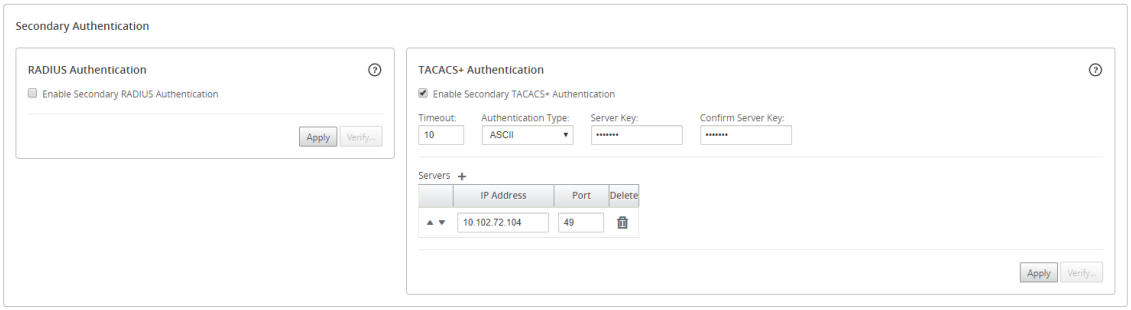
   > **Remarque**
   >
   > Si l'authentification RADIUS est déjà activée, elle est désactivée.

3. Dans le champ Délai d'**expiration**, entrez l'intervalle de temps (en secondes) pour attendre une réponse d'authentification du serveur TACACS+.

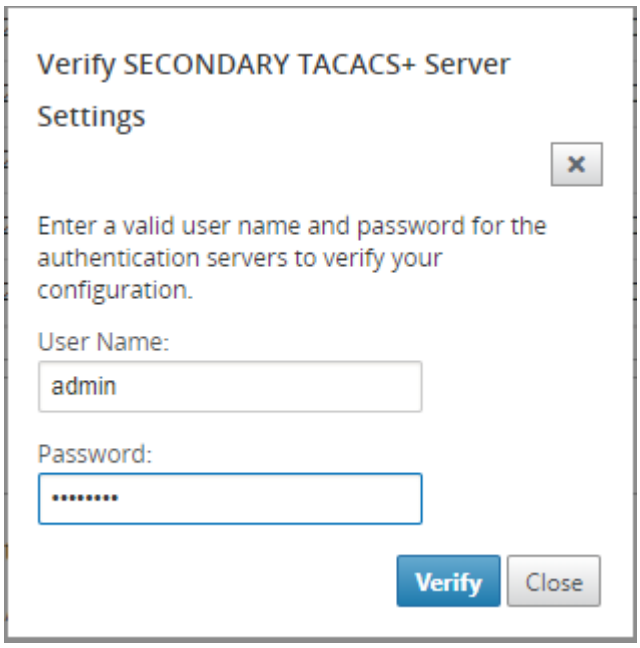
   La valeur du délai d'attente doit être inférieure ou égale à 60 secondes.
4. Dans le champ **Type d'authentification**, sélectionnez la méthode de chiffrement à utiliser pour envoyer le nom d'utilisateur et le mot de passe au serveur TACACS+.
5. Dans le champ **Clé serveur**, entrez une clé secrète à utiliser lors de la connexion aux serveurs TACACS+.
6. Dans les champs **Confirmer la clé du serveur**, entrez à nouveau la clé secrète.

   > **Remarque**
   >
   > Les paramètres de **délai d'expiration**, de **type d'authentification** et de **clé de serveur** sont appliqués à tous les serveurs configurés.

7. Cliquez sur l'icône plus (+) en regard de **Serveurs** pour ajouter un serveur TACACS+.
8. Dans le champ **Adresse IP**, entrez l'adresse IP de l'hôte du serveur TACACS+.
9. Dans le champ **Port**, entrez le numéro de port du serveur TACACS+. Le numéro de port par défaut est 49.



10. Cliquez sur **Apply**.
11. Cliquez sur **Vérifier** pour vérifier la connexion au serveur RADIUS. La boîte de dialogue **Vérifier les paramètres du serveur TACACS+** s'affiche.



12. Entrez un nom d'utilisateur et un mot de passe valides pour les serveurs d'authentification, puis cliquez sur**Vérifier**.

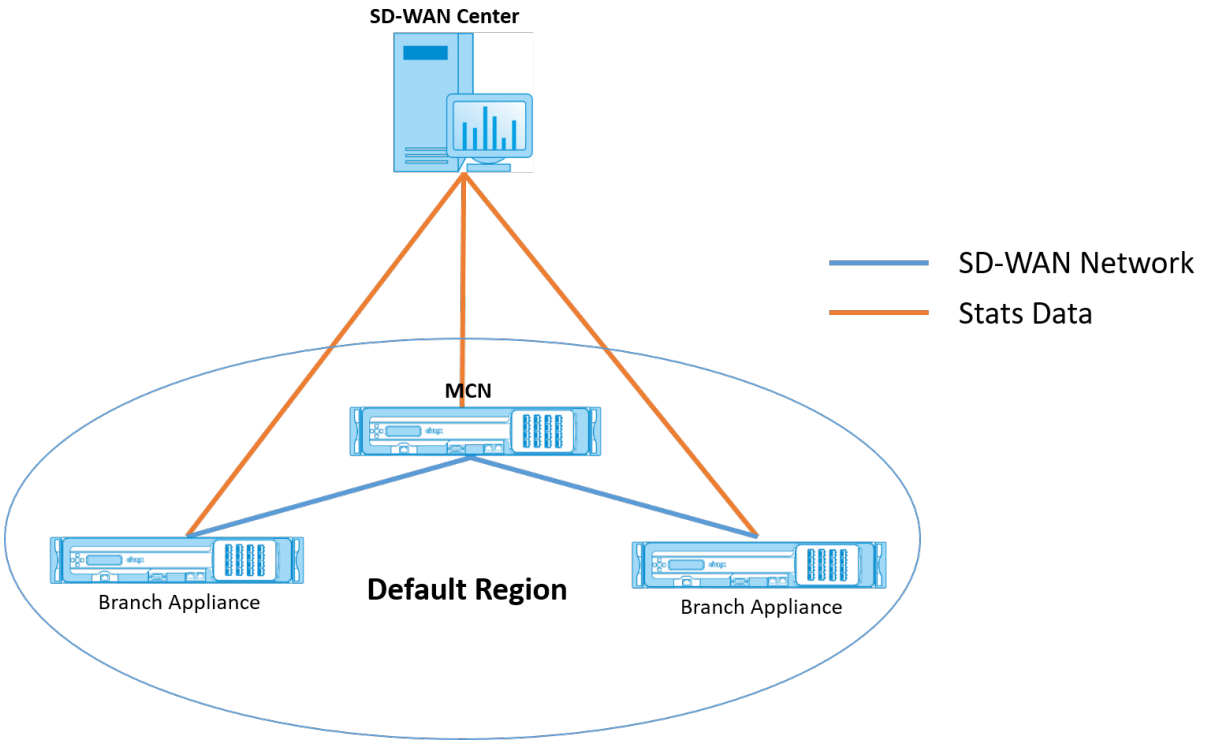
    Pour configurer plus de serveurs, répétez les étapes 7 à 12.

Déploiement d'un réseau à région unique

February 17, 2022

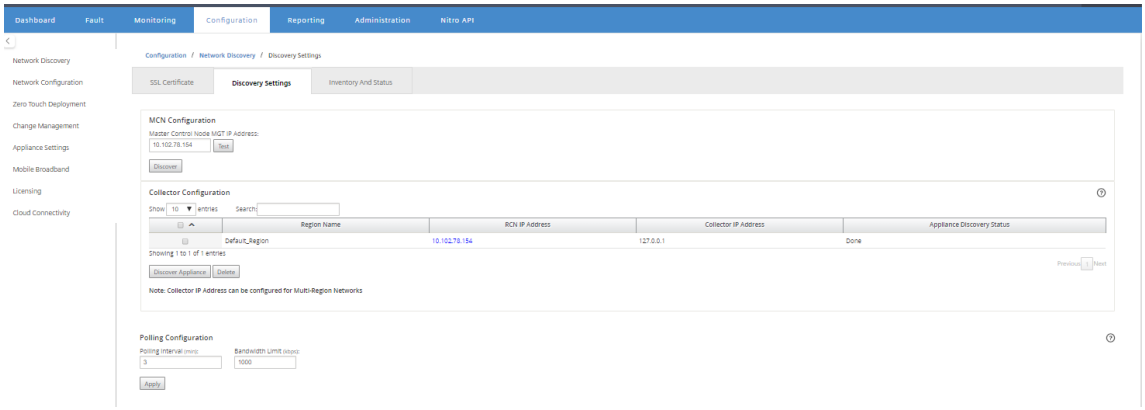
Si votre organisation dispose d'un petit réseau couvrant une limite administrative (ou géographique) unique, vous pouvez utiliser Citrix SD-WAN Center en mode par défaut (avec une seule « région par défaut »). Une région peut prendre en charge jusqu'à 550 sites.

Un réseau de région unique dispose d'un nœud de contrôle maître (MCN) pour le contrôle centralisé et d'un centre Citrix SD-WAN pour la gestion centralisée. La région associée et contrôlée par le MCN est appelée région par défaut. Le Citrix SD-WAN Center interroge le MCN et tous les matériels de succursale dans la région par défaut.



Pour déployer Citrix SD-WAN Center pour une région unique :

1. Téléchargez le logiciel Citrix SD-WAN Center. Pour plus d'informations, consultez Configuration système requise et installation.
2. Installez le Citrix SD-WAN Center sur ESXi Server, XenServer, Hyper-V ou Azure.
3. Configuration des paramètres de l'interface de gestion. Pour plus d'informations, consultezConfigurer les paramètres de l'interface de gestion.
4. Générez, téléchargez et installez le certificat SSL SD-WAN MCN sur SD-WAN Center. Pour de plus amples informations, consultez la section Installer le certificat SSL Citrix SD-WAN.
5. Générez, téléchargez et installez le certificat SSL Center SD-WAN sur l'appliance MCN. Pour plus d'informations, consultez la section Installer le certificat SSL Citrix SD-WAN Center.
6. Dans l'interface graphique de Citrix SD-WAN Center, accédez à **Configuration** > **Découverte du réseau** > **Paramètres de découverte.**
7. Dans le champ **Master Controller Node MGT IP Address**, entrez l'adresse IP MCN et cliquez sur **Tester**. Cela établit une connexion entre le MCN et Citrix SD-WAN Center.



8. Cliquez sur **Découvrir**. Si vous avez déjà découvert un MCN, cette option devient **Redécouverte**.

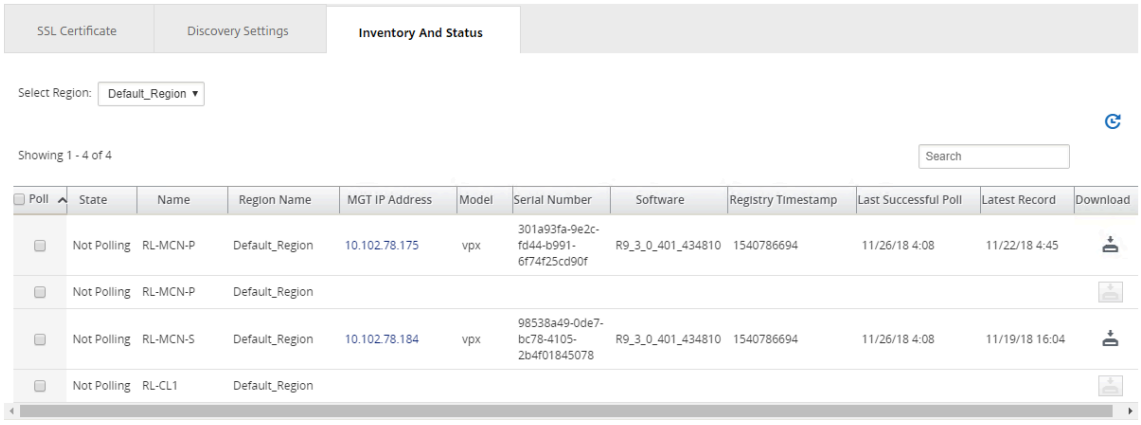
> **Remarque**
>
> Le MCN doit être actif et le service SD-WAN doit être activé. Pour plus d'informations, consultez Activation du service SD-WAN.

9. Une fois l'opération de découverte terminée, cliquez sur l'onglet **Inventaire et état**.

   Le tableau **Inventory and Status** affiche les informations d'état de toutes les appliances Citrix SD-WAN découvertes.

10. Cochez la case **Sondage** dans le coin supérieur gauche de l'en-tête du tableau.

    Cette option coche la case **Sondage** pour chaque appliance répertoriée dans le tableau. Pour exclure une appliance de la liste d'interrogation, désactivez sa case à cocher.



11. Cliquez sur **Apply**.

> **Conseil**
>
> Vous pouvez augmenter la taille de stockage du centre Citrix SD-WAN en créant un magasin de données sur votre machine virtuelle et en basculant le magasin de données. Pour plus

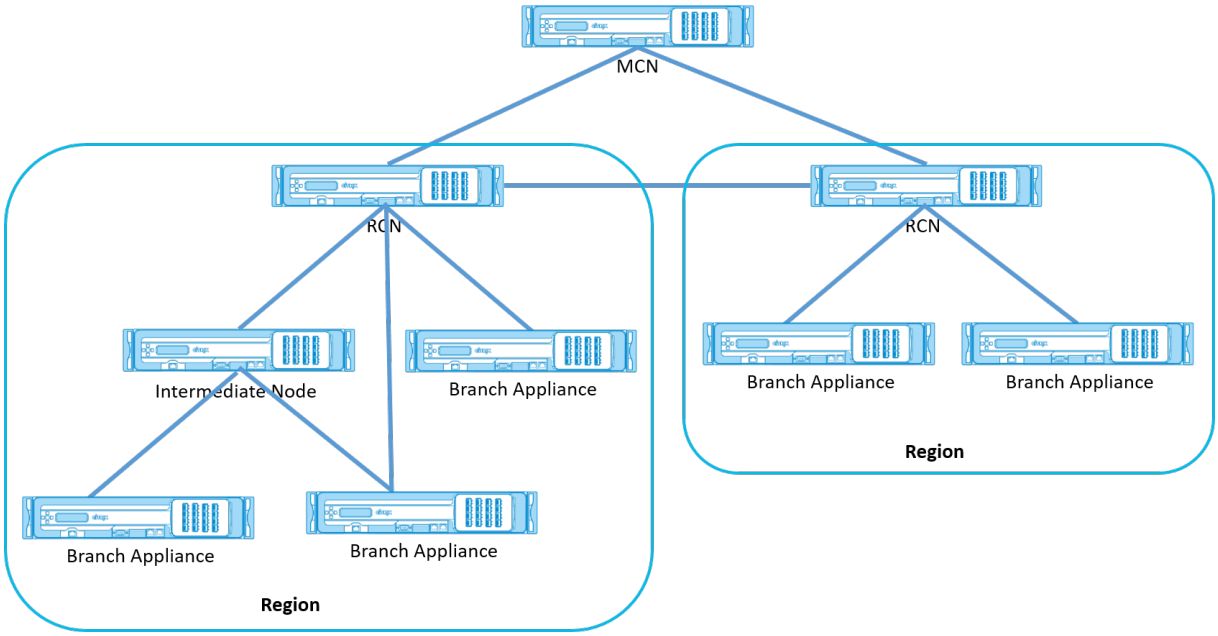
> d'informations, voir Basculer le stockage actif vers un nouveau stockage de données.

Déploiement réseau multi-région

February 17, 2022

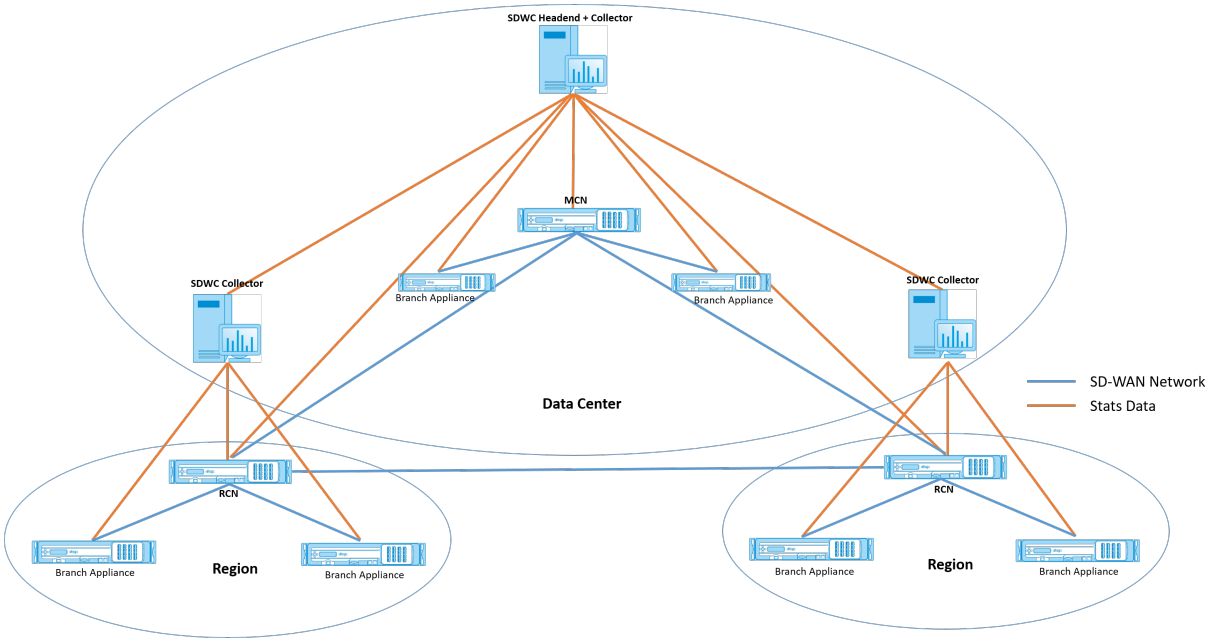
Si votre organisation dispose d'un réseau étendu couvrant plusieurs limites administratives (ou géographiques), vous pouvez utiliser Citrix SD-WAN Center en mode multi-région, chaque région prenant en charge jusqu'à 550 sites.

Le réseau multi-région prend en charge une architecture hiérarchique avec un nœud de contrôle maître (MCN) contrôlant plusieurs nœuds de contrôle régionaux (RCN). Chaque RCN, à son tour, contrôle plusieurs sites clients. Le MCN peut également être utilisé en option pour contrôler certains sites clients directement dans le cadre de la « région par défaut ». Cette architecture hiérarchique et distribuée permet une plus grande échelle et une délégation efficace de l'administration régionale.



Le Citrix SD-WAN Center interroge le MCN, les RCN et toutes les appliances de succursales associées.

L'architecture multi-région de Citrix SD-WAN Center nécessite l'ajout d'un collecteur par région, pour collecter et stocker des données et des statistiques au niveau de la région. Cette architecture distribuée permet une plus grande échelle sur plusieurs régions, tout en préservant la vue « panneau unique » pour la gestion de l'ensemble du réseau.



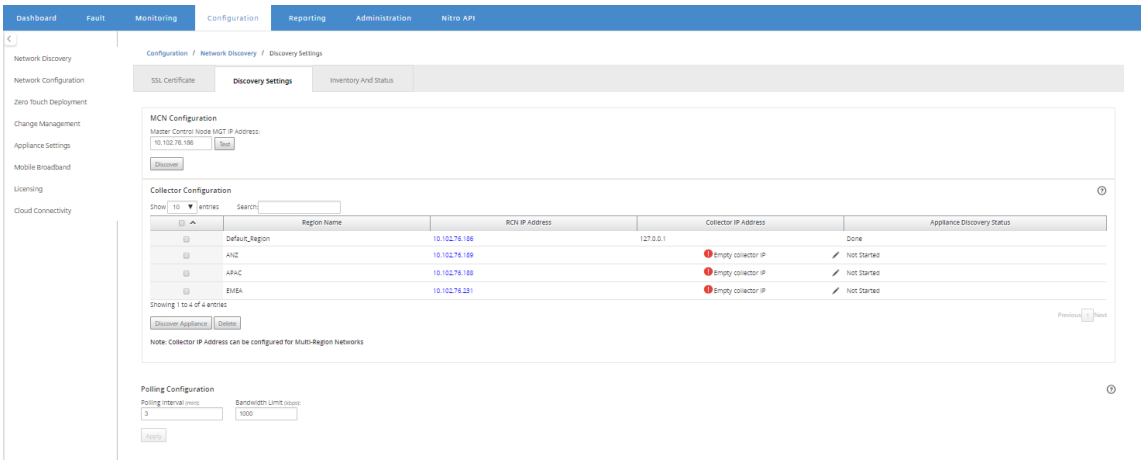
> **Remarque**
>
> Pour un déploiement multi-région, les statistiques de région par défaut incluent des statistiques de tous les sites gérés par le MCN et le RCN. Toutefois, les données RCN ne sont pas stockées sur le collecteur SD-WAN Center. Le collecteur du SD-WAN Center obtient les données du site de la MRC auprès des collecteurs régionaux respectifs.

Pour déployer Citrix SD-WAN Center pour multi-région :

1. Téléchargez le logiciel Citrix SD-WAN Center. Pour plus d'informations, consultez Configuration système requise et installation.
2. Installez le Citrix SD-WAN Center sur ESXi Server, XenServer, Hyper-V ou Azure.
3. Configuration des paramètres de l'interface de gestion. Pour plus d'informations, consultezConfigurer les paramètres de l'interface de gestion.
4. Générez, téléchargez et installez le certificat SSL SD-WAN MCN sur SD-WAN Center. Pour de plus amples informations, consultez la section Installer le certificat SSL Citrix SD-WAN.
5. Générez, téléchargez et installez le certificat SSL Center SD-WAN sur l'appliance MCN. Pour plus d'informations, consultez la section Installer le certificat SSL Citrix SD-WAN Center.
6. Dans l'interface graphique de Citrix SD-WAN Center, accédez à **Configuration** > **Découverte du réseau** > **Paramètres de découverte.**
7. Dans le champ **Master Controller Node MGT IP Address**, entrez l'adresse IP MCN et cliquez sur **Tester**. Cela établit une connexion entre le MCN et Citrix SD-WAN Center.

8. Cliquez sur **Découvrir**. Une liste de tous les RCN connectés au MCN apparaît dans la section **Configuration du collecteur**. Pour découvrir les sites de région non par défaut, vous devez disposer d'un RCN actif avec des chemins actifs vers MCN.

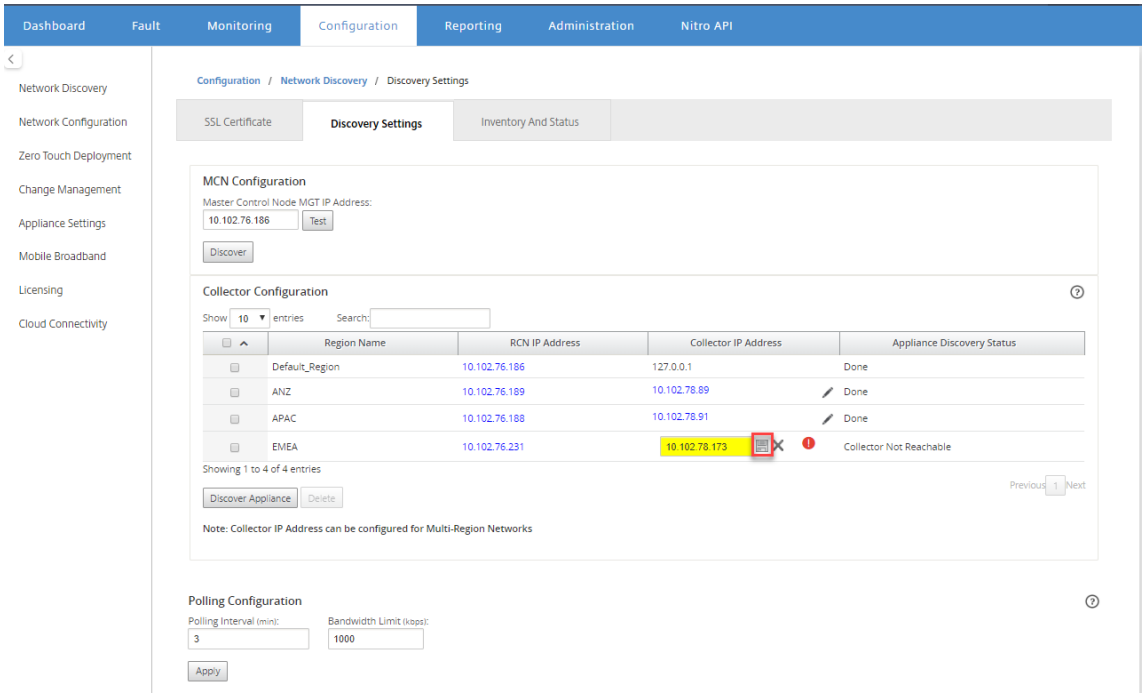
> **Remarque**
>
> Le Centre Citrix SD-WAN agit comme collecteur pour la région par défaut.



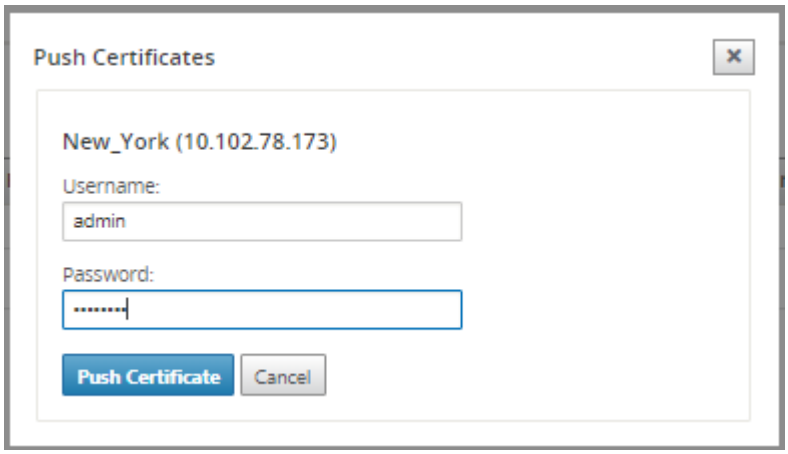
9. Cliquez sur l'icône de modification et, dans le champ **IP du collecteur**, entrez l'adresse IP du Citrix SD-WAN Center que vous souhaitez configurer en tant que collecteur pour une région.

> **Remarque**
>
> Pour configurer un collecteur, installez une machine virtuelle Citrix SD-WAN Center et configurez l'adresse IP de gestion. L'adresse IP de gestion de ce Citrix SD-WAN Center est l'adresse IP du collecteur.

10. Cliquez sur l'icône Enregistrer pour enregistrer l'adresse IP du collecteur et pousser la paire Certificat-clé vers le RCN.

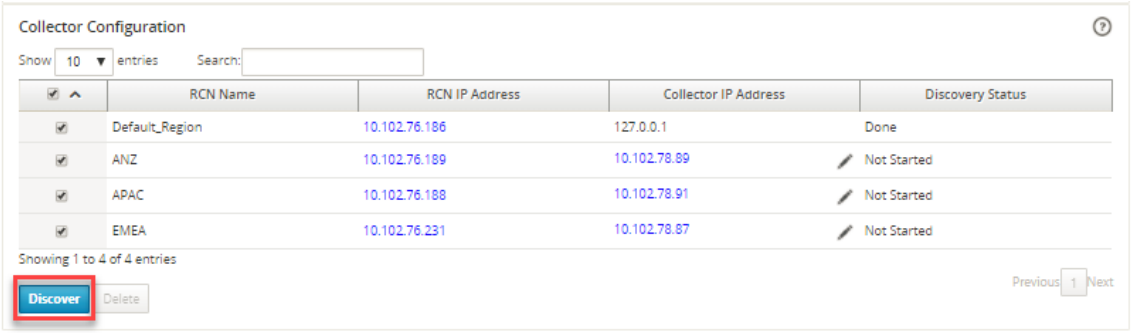


11. Entrez les informations d'identification du RCN et cliquez sur **Push Certificate**.

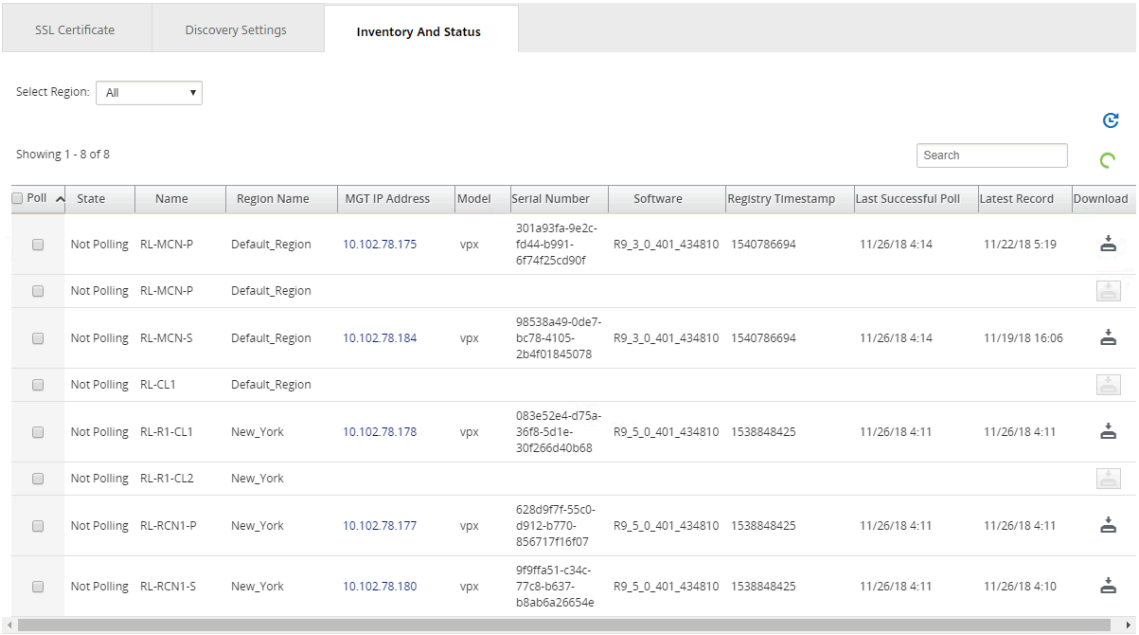


12. De même, configurez l'adresse IP du collecteur pour tous les RCN.

> **Remarque**
>
> Les appliances sont détectées automatiquement toutes les 30 minutes. Si de nouveaux RNC sont ajoutés au réseau et qu'une gestion des modifications est effectuée, vous pouvez sélectionner l'appliance et cliquer sur **Découvrir l'appliance pour découvrir** immédiatement l'appliance.



Une fois que le **Statut de découverte** est passé à **Terminé**, vous pouvez afficher les sites découverts dans la page **Stock et statut**.



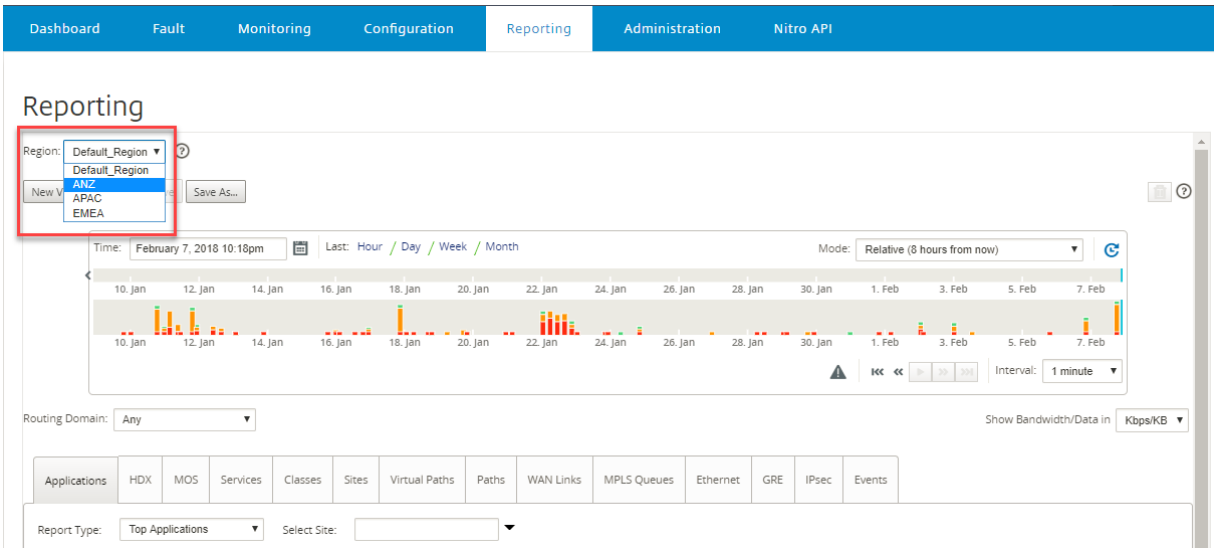
> **Conseil**
>
> Vous pouvez filtrer les sites en fonction du nom de la région. Dans le champ **Sélectionner une région**, sélectionnez la région.

13. Dans la page **Stock et état**, sélectionnez les sites que vous souhaitez lancer l'interrogation, puis cliquez sur **Appliquer** .

> **Conseil**
>
> Vous pouvez augmenter la taille de stockage du collecteur en créant un magasin de données sur votre machine virtuelle. Pour plus d'informations, reportez-vous à la section Basculement du stockage actif vers un nouveau stockage de données.

Vous pouvez sélectionner des régions spécifiques pour afficher les rapports d'événements et de statistiques.

Les données des événements et des rapports statistiques sont extraites du collecteur de la région concernée.



Configuration

February 17, 2022

Les premières étapes de configuration de Citrix SD-WAN Center sont courantes pour le réseau monorégion et le réseau multi-région. Voici une liste des procédures de configuration courantes :

- Configurer les paramètres de l'interface de gestion
- Installez les certificats Citrix SD-WAN Center.
- Basculez le stockage actif vers un nouveau stockage de données.

Configurer les paramètres de l'interface de gestion

February 17, 2022

Vous pouvez utiliser l'interface Web Citrix SD-WAN Center pour configurer les paramètres de l'interface de gestion.

Les paramètres de l'interface de gestion sont les suivants :

- Adresse IP de gestion de Citrix SD-WAN Center
- Adresse IP de la passerelle
- Masque de sous-réseau

- DNS principal
- DNS secondaire

Pour configurer les paramètres de l'interface de gestion :

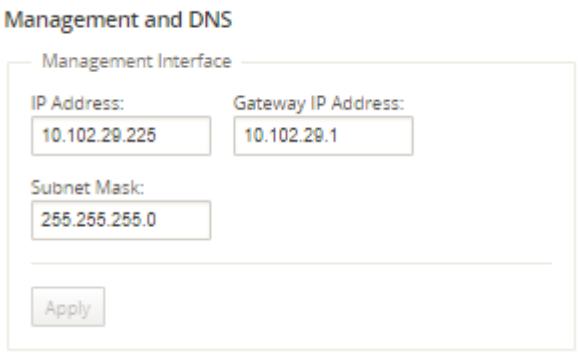
1. Dans l'interface Web Citrix SD-WAN Center, sélectionnez l'onglet **Administration**.

   Par défaut, la page **Paramètres de l'utilisateur/authentification** s'affiche.

2. Dans l'arborescence de navigation, sélectionnez **Paramètres globaux**.
3. Configurez les paramètres de gestion et DNS.

   Dans la section **Gestion et DNS**, ajoutez les informations requises aux champs suivants :

   - **Adresse IP** : Saisissez l'adresse IP de Citrix SD-WAN Center.
   - **Adresse IP de la passer**elle : entrez l'adresse IP de la passerelle que la machine virtuelle Citrix SD-WAN Center utilisera pour communiquer avec les réseaux externes.
   - **Masque de sous-réseau** : entrez le masque de sous-réseau pour définir le réseau dans lequel réside la machine virtuelle Citrix SD-WAN Center.



4. Cliquez sur**Appliquer**.

> **Remarque**
>
> La connectivité au Centre Citrix SD-WAN sera interrompue lorsque vos modifications seront appliquées.

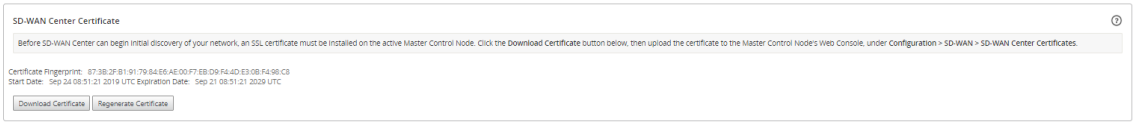
Installer le certificat SSL de SD-WAN Center

February 17, 2022

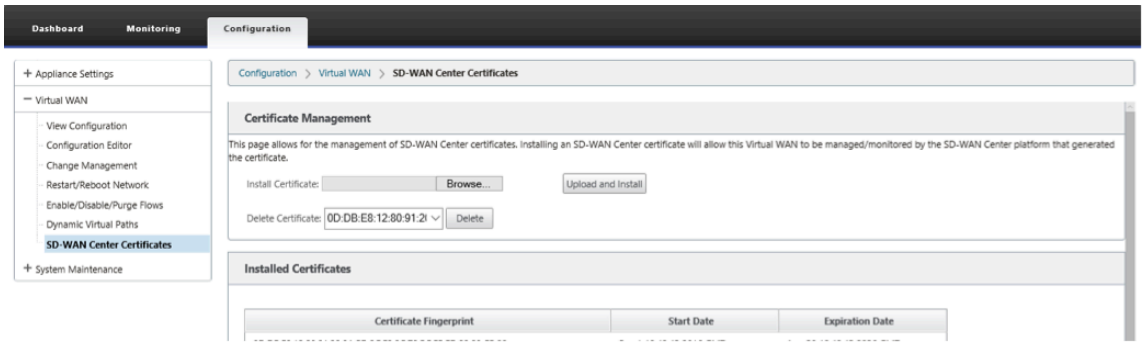
Pour établir une connexion entre Citrix SD-WAN Center et MCN (Master Control Node) Citrix SD-WAN, téléchargez le certificat SSL à partir du SD-WAN Center et installez-le sur le MCN.

Pour générer et installer le certificat Citrix SD-WAN Center :

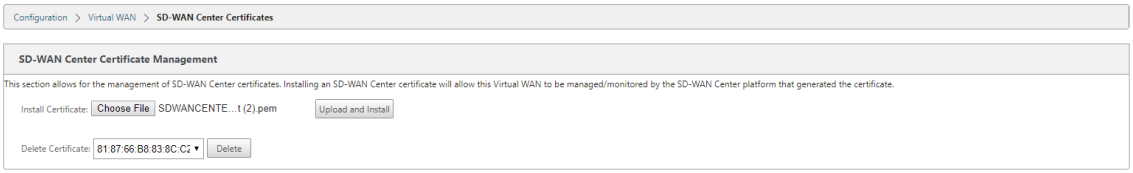
1. Dans l'interface Web Citrix SD-WAN Center, accédez à **Configuration** > **Découverte réseau** > **Certificat SSL** > **Certificat SD-WAN Center**.
2. Cliquez sur **Régénérer le certificat** pour générer un nouveau certificat SSL afin d'établir une communication avec le MCN.



3. Cliquez sur **Télécharger le certificat**. Accédez à l'emplacement souhaité et enregistrez le certificat.
4. Dans l'interface Web MCN Citrix SD-WAN, accédez à **Configuration** > **Réseau étendu virtuel** > **Certificats du SD-WAN Center** > **Gestion des certificats du SD-WAN Center**.



5. Cliquez sur **Choisir un fichier**, parcourez et sélectionnez le certificat SSL du SD-WAN Center téléchargé.



6. Cliquez sur **Télécharger et installer**, il télécharge le certificat SSL du SD-WAN Center vers le MCN et affiche un message de réussite lorsque l'installation est terminée.

Installer le certificat SSL Citrix SD-WAN

February 17, 2022

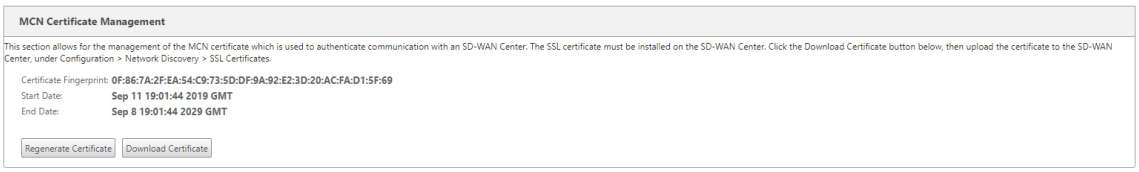
Pour établir une connexion entre Citrix SD-WAN MCN et Citrix SD-WAN Center, téléchargez le certificat SSL à partir de l'appliance MCN SD-WAN et installez-le sur SD-WAN Center.

Vous pouvez régénérer le certificat de l'appliance sur le MCN qui remplace le certificat prédéfini, puis l'installer sur le SD-WAN Center.

L'installation du certificat de l'appliance dans le SD-WAN Center est obligatoire pour les nouveaux déploiements et pour que la communication SSL fonctionne. MCN génère un certificat réseau et distribue le certificat avec une clé privée via le gestionnaire de certificats à tous les nœuds. Les certificats sont utilisés par chaque succursale pour authentifier le SD-WAN Center.

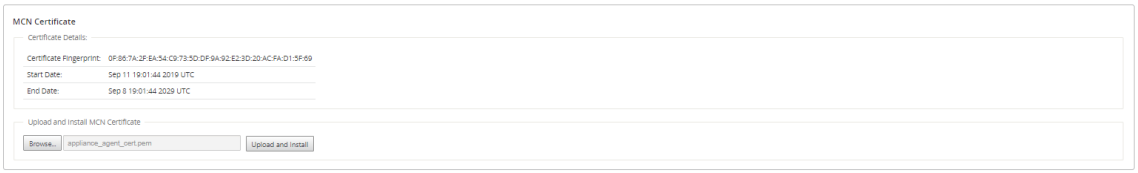
Pour générer et installer le certificat SD-WAN :

1. Dans l'appliance MCN SD-WAN, accédez à **Configuration** > **Virtual WAN** > **SD-WAN Center Certificates** > **MCN Certificate Management**.
2. Cliquez sur **Régénérer le certificat** pour générer un nouveau certificat SSL afin d'établir la communication avec le SD-WAN Center.

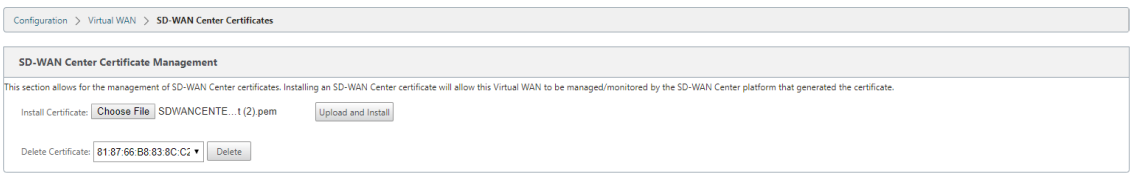


> **Remarque :**
>
> Lorsque vous régénérez le certificat SSL, l'appliance SD-WAN utilise le nouveau certificat immédiatement pour communiquer avec le SD-WAN Center découvert. Toutefois, la communication avec les appliances n'est pas établie tant que vous n'avez pas téléchargé et installé le certificat nouvellement généré sur SD-WAN Center.

3. Cliquez sur **Télécharger le certificat**. Accédez à l'emplacement souhaité et enregistrez le certificat.
4. Dans l'interface Web de Citrix SD-WAN Center, accédez à **Configuration** > **Certificat SSL** > **Certificat MCN**.



5. Cliquez sur **Parcourir** et sélectionnez le certificat SSL MCN téléchargé.



6. Cliquez sur **Télécharger et installer**, il télécharge le certificat SSL MCN vers SD-WAN Center.

Basculer le stockage actif vers un nouveau stockage de données

February 17, 2022

Dans Citrix SD-WAN Center, vous pouvez basculer le stockage actif vers le magasin de données que vous avez créé sur votre serveur virtuel. Cela vous permet de stocker plus de données statistiques obtenues en interrogeant tous les appliances Citrix SD-WAN dans le WAN. Pour plus d'informations sur la création d'une banque de données sur le serveur ESXi, reportez-vous à la section Ajout et configuration de la banque de données sur ESXi Server. Pour plus d'informations sur la création d'une banque de données sur XenServer, consultez la section Ajout et configuration du stockage de données sur XenServer

Pour spécifier le stockage actif pour la machine virtuelle Citrix SD-WAN Center :

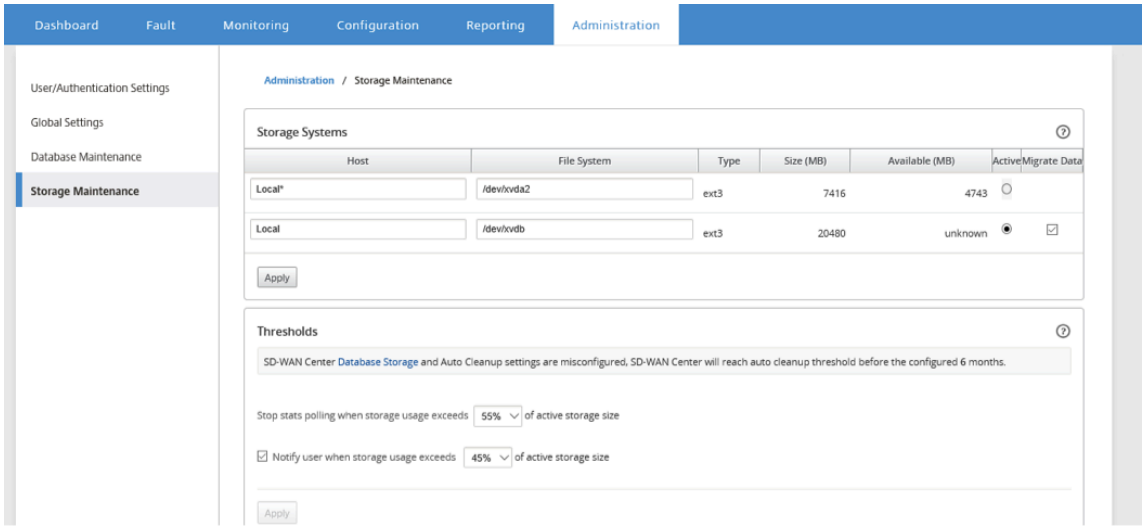
1. Connectez-vous à la VM Citrix SD-WAN Center.

   Les informations d'identification de connexion par défaut pour Citrix SD-WAN Center sont les suivantes :

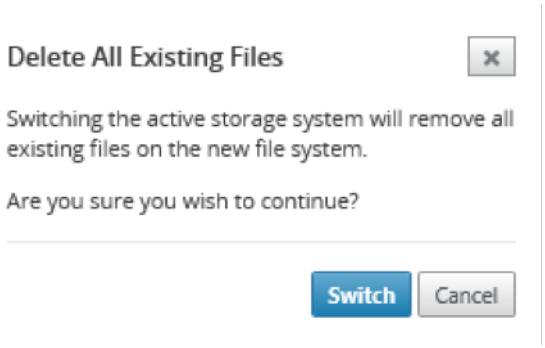
   Connexion : admin

   Mot de passe : mot

2. Cliquez sur l'onglet **Administration**, puis sur **Maintenance du stockage**.



3. Dans la colonne **Actif** du tableau Systèmes de stockage, sélectionnez le stockage que vous avez créé.
4. Sélectionnez **Migrer les données**, puis cliquez sur **Appliquer**.
5. Le message **Supprimer tous les fichiers existants** s'affiche, cliquez sur **Basculer** .



Cela place Citrix SD-WAN Center en **mode Maintenance** et affiche une barre de progression dans la zone de page principale.

6. Lorsque l'activation est terminée, cliquez sur **Continuer**.

   Cette opération rejette la barre de progression et retourne à la page principale **Maintenance du stockage**.

Déployer l'appliance Citrix SD-WAN

February 17, 2022

Vous pouvez utiliser Citrix SD-WAN Center pour créer le fichier de configuration ou de paramètres de l'appliance et utiliser l'assistant de gestion des modifications pour transmettre la configuration aux appliances sur le réseau. Pour de plus amples informations, consultez Configurer les appliances Citrix SD-WAN.

Vous pouvez configurer Citrix SD-WAN Center pour qu'il agisse en tant que serveur central de licences et fournit des services de licences à tous les nœuds du réseau. Cela élimine la nécessité d'installer des licences sur des nœuds individuels localement. Pour plus d'informations, consultez Citrix SD-WAN Center en tant que serveur de licences.

Vous pouvez utiliser Citrix SD-WAN Center pour rationaliser le processus de déploiement des appliances SD-WAN dans les succursales à l'aide de la fonctionnalité de déploiement sans intervention. Pour plus d'informations, consultez la section Déploiement Zero Touch.

Configurer les appliances Citrix SD-WAN

February 17, 2022

Utilisez l'Éditeur de configuration pour modifier les paramètres de configuration et exporter le package de configuration vers le MCN. Pour plus d'informations, reportez-vous à la section Éditeur de configuration.

Vous pouvez utiliser l'assistant de gestion des modifications de l'appliance MCN via Citrix SD-WAN Center. Pour plus d'informations, reportez-vous à la section Assistant Gestion des modifications.

Vous pouvez configurer les paramètres de l'appliance sur Citrix SD-WAN Center et l'exporter vers un ensemble d'appliances Citrix SD-WAN gérées dans votre réseau SD-WAN. Pour plus d'informations, reportez-vous à la section Paramètres du matériel.

Éditeur de configuration

February 17, 2022

L'Éditeur de configuration est disponible en tant que composant de l'interface Web Citrix SD-WAN Center et dans l'interface Web de gestion Citrix SD-WAN s'exécutant sur le nœud de contrôle maître (MCN) du réseau SD-WAN.

> **Remarque**
>
> Vous ne pouvez pas envoyer de configurations vers les appliances découvertes directement à partir de Citrix SD-WAN Center. Vous pouvez utiliser l'Éditeur de configuration pour modifier les paramètres de configuration et créer un package de configuration. Lorsque le package de configuration a été créé, vous pouvez l'exporter vers le MCN et l'installer. Les modifications sont ensuite reflétées dans le MCN.
>
> Vous devez ouvrir une session avec des droits d'administration sur l'appliance Citrix SD-WAN Center et le MCN, pour modifier les configurations sur le centre Citrix SD-WAN et pour exporter et installer les configurations sur le MCN.

Pour obtenir des instructions détaillées sur l'utilisation de l'éditeur de configuration pour configurer votre Citrix SD-WAN, consultez la documentationCitrix SD-WAN 10.1.

L'Éditeur de configuration vous permet d'effectuer les opérations suivantes :

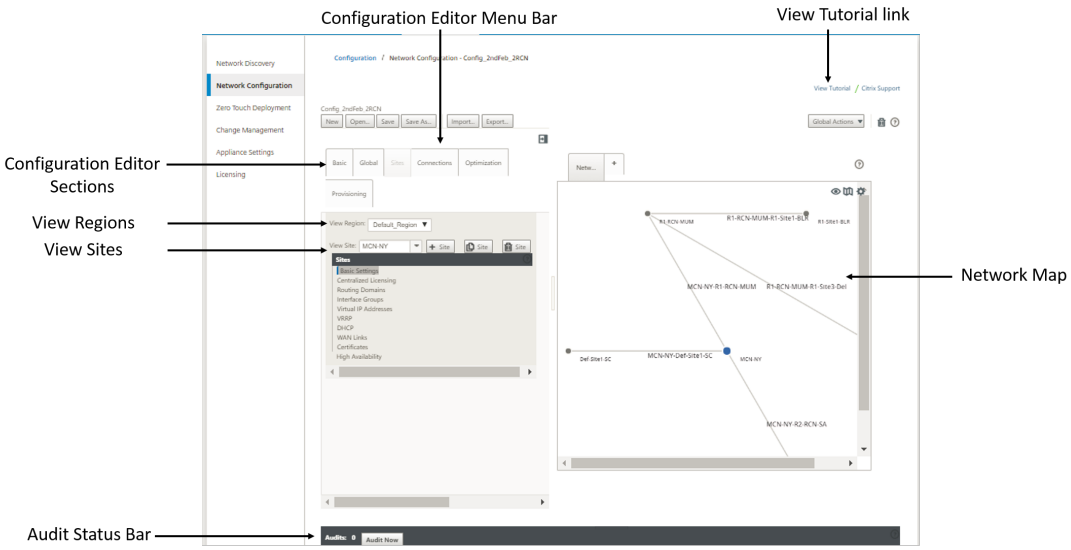
- Ajoutez et configurez des sites et des connexions Citrix SD-WAN Appliance.
- Provisionner l'appliance Citrix SD-WAN.
- Créez et définissez la configuration SD-WAN de Citrix.
- Définissez et affichez les cartes réseau de votre système SD-WAN.

Pour ouvrir l'Éditeur de configuration :

1. Dans l'interface Web Citrix SD-WAN Center, cliquez sur l'onglet **Configuration**.

2. Cliquez sur **Configuration réseau**.

   La figure ci-dessous présente les éléments de base de navigation et de page de l'**Éditeur de configuration**, ainsi que la terminologie utilisée dans ce guide pour les identifier.



   L'écran principal de l'Éditeur de configuration comporte les éléments de navigation suivants :

- **Barre de menu de l'éditeur de configuration** : contient les boutons d'activité principaux pour les opérations de l'éditeur de configuration. En outre, à l'extrémité droite de la barre de menus se trouve le bouton de lien **Afficher le didacticiel** pour lancer le didacticiel de l'éditeur de configuration. Le didacticiel vous guide à travers une série de descriptions de bulles pour chaque élément de l'éditeur de configuration.
- **Sections de l'éditeur de configuration** : chaque onglet représente une section de niveau supérieur. Il y a six sections : **Basic**,**Global**, **Sites**, **Connexions**, **Optimisation** et **Provisioning**. Cliquez sur un onglet de section pour afficher l'arborescence de configuration de cette section.
- **Voir la région** : pour le déploiement multi-région, il répertorie toutes les régions configurées. Pour le déploiement d'une seule région, la région par défaut est affichée par défaut. Pour afficher les sites d'une région, sélectionnez une région dans la liste déroulante.
- **Afficher les sites :** répertorie les nœuds de site qui ont été ajoutés à la configuration et qui sont actuellement ouverts dans l'Éditeur de configuration. Pour afficher la configuration du site, sélectionnez un site dans la liste déroulante.
- **Carte réseau :** fournit une vue schématique du réseau SD-WAN.Placez le curseur de la souris sur les sites ou le chemin d'accès pour afficher plus de détails. Cliquez sur les sites pour afficher les options de rapport.
- **Barre d'état de l'audit** : barre gris foncé située en bas de la page Éditeur de configuration et couvrant toute la largeur de la page Éditeur de configuration. La barre d'état **Audits** n'est disponible que lorsque l'**éditeur de configuration** est ouvert. Une icône d'alerte d'audit (point rouge ou delta de verge d'or) située à l'extrême gauche de la barre d'état indique une

ou plusieurs erreurs présentes dans la configuration actuellement ouverte. Cliquez sur la barre d'état pour afficher la liste complète de toutes les alertes d'audit non résolues pour cette configuration.

Assistant Gestion des modifications

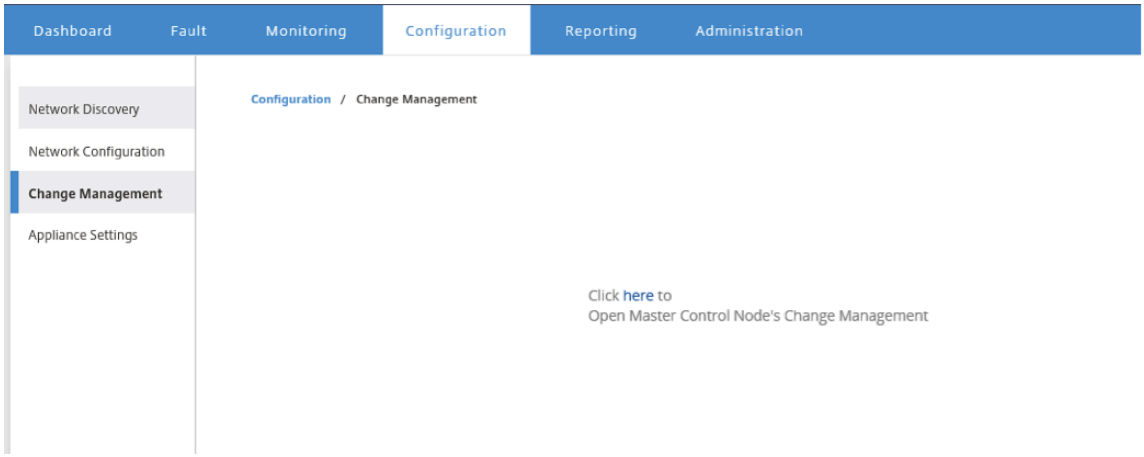
February 17, 2022

L'assistant Gestion des modifications vous guide tout au long du processus de téléchargement, de téléchargement, de transfert et d'activation du logiciel et de la configuration Citrix SD-WAN sur le dispositif MCN et les appliances clientes Master Control Node (Master Control Node).

L'Assistant Gestion des modifications est un composant de l'interface Web de gestion Citrix SD-WAN s'exécutant sur le MCN et ne fait pas partie du Citrix SD-WAN Center. Toutefois, vous pouvez utiliser Citrix SD-WAN Center pour vous connecter au MCN spécifié et accéder à l'Assistant Gestion des modifications.

Pour ouvrir l'Assistant Gestion des modifications :

1. Dans l'interface Web Citrix SD-WAN Center, cliquez sur l'onglet **Configuration**.
2. Cliquez sur **Gestion des modifications**.



3. À l'invite **de gestion des modifications du nœud de contrôle maître**, cliquez sur le lien **ici** .

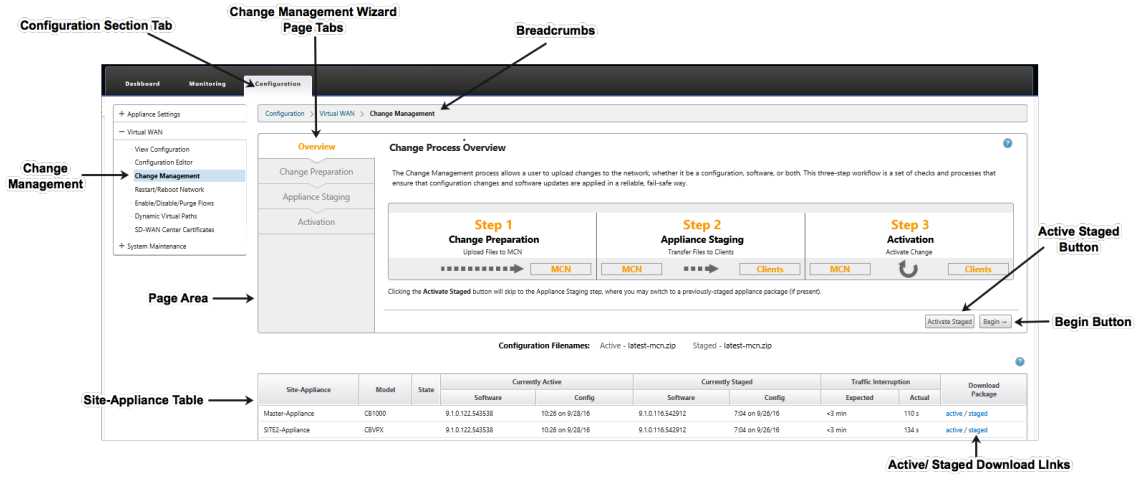
   Vous serez automatiquement connecté à l'interface graphique MCN.

   > **Remarque**
   >
   > Vous n'avez pas besoin de vous connecter à l'interface graphique MCN à l'aide des infor-

> mations d'identification MCN, la fonctionnalité de connexion automatique active la connexion unique.

4. Dans l'interface Web de gestion MCN, cliquez sur l'onglet **Configuration** .
5. Dans l'arborescence de navigation (volet gauche), cliquez sur **+** en regard de la succursale **Virtual WAN** pour développer cette succursale.
6. Cliquez sur **Gestion des modifications**.

   Ceci affiche la première page de l'Assistant **Gestion des modifications**, la page **Vue d'ensemble du processus de modification**, comme indiqué dans la figure ci-dessous.



7. Pour démarrer l'assistant, cliquez sur **Commencer**.

> **Remarque**
>
> Pour obtenir des instructions complètes sur l'utilisation de l'assistant pour télécharger, organiser et activer le logiciel SD-WAN et la configuration sur les appliances, reportez-vous au Guide de l'utilisateur SD-WAN 9.1.0.

L'Assistant **Gestion des modifications** comporte les éléments de navigation suivants :

- **Zone de page** : affiche les formulaires, les tableaux et les boutons d'activité de chaque page de l'Assistant **Gestion des modifications**.
- **Onglets de page de l'Assistant Gestion des modifications** : sur le côté gauche de la zone de page, sur chaque page de l'Assistant, les onglets sont répertoriés dans l'ordre dans lequel les étapes correspondantes se produisent dans le processus de l'Assistant. Lorsqu'un onglet est actif, vous pouvez cliquer dessus pour revenir à une page précédente de l'Assistant. Un onglet actif affiche son nom s'affiche dans une police bleue. Une police grise indique un onglet inactif. Les onglets sont inactifs jusqu'à ce que toutes les dépendances (étapes précédentes) aient été remplies sans erreur.

- **Tableau Appliance-Site** : au bas de la zone de page de l'Assistant, ce tableau contient des informations sur chaque site d'appliance configuré, ainsi que des liens permettant de télécharger les packages actifs ou mis en place pour ce modèle d'appliance et ce site. Dans ce contexte, un package est un ensemble de fichiers zip contenant le package logiciel SD-WAN approprié pour ce modèle d'appliance et le package de configuration spécifié. La section Noms des fichiers de configuration au-dessus du tableau indique le nom du package des packages actifs et préparés actuels sur l'appliance locale.
- **Liens de téléchargement actif/intermédiaire** : dans le champ **Télécharger le package**(colonne à l'extrême droite) de chaque entrée de la table **Appliance-Site**, vous pouvez cliquer sur un lien dans une entrée pour télécharger le package actif ou intermédiaire pour le site de cette appliance.
- **Bouton Commencer**: cliquez sur **Commencer** pour lancer le processus de l'Assistant **Gestion des modifications** et passez à l'onglet **Préparation des modifications**.
- **Bouton Activer le déploiement intermédiaire** : s'il ne s'agit pas d'un déploiement initial et que vous souhaitez activer la configuration en cours, vous avez la possibilité de passer directement à l'étape **Activation**. Cliquez sur **Activer la zone** de préparation pour accéder directement à la page **Activation** et lancer l'activation de la configuration en cours de préparation.

Paramètres de l'appliance

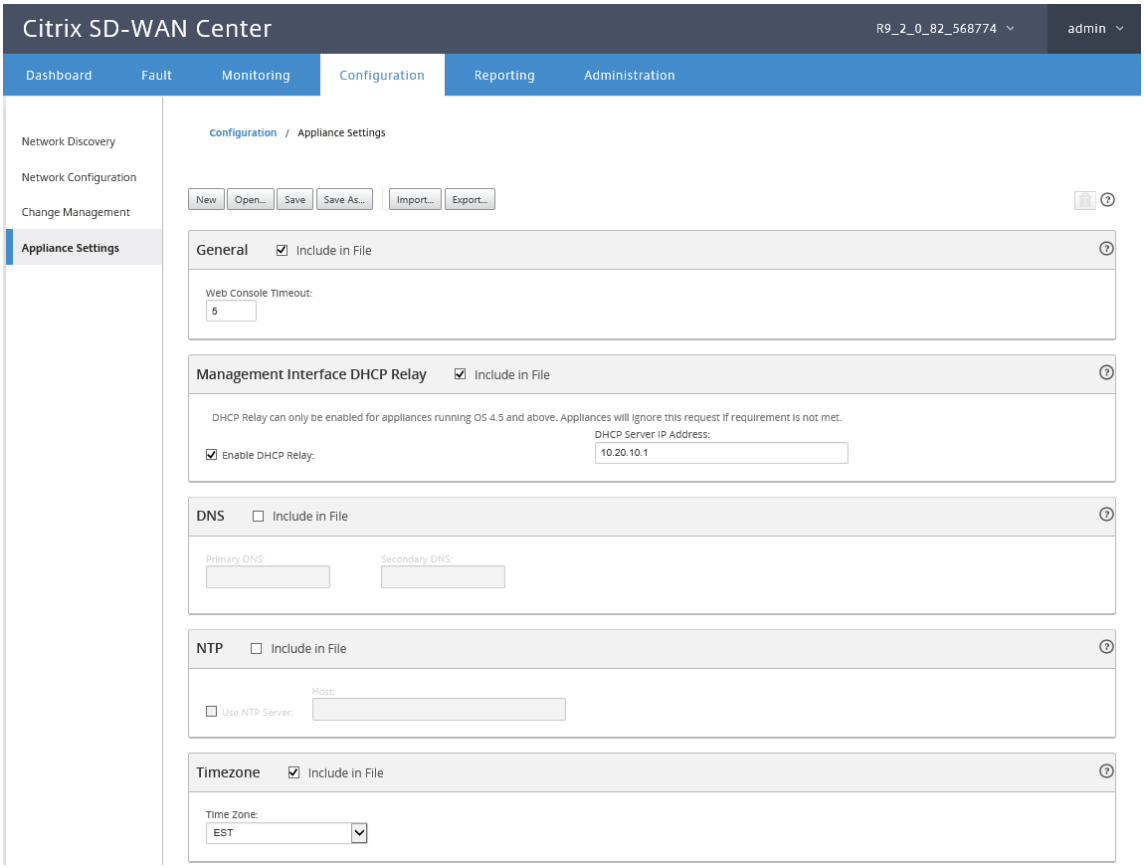
February 17, 2022

Vous pouvez configurer les paramètres de l'appliance sur Citrix SD-WAN Center et l'exporter vers un ensemble d'appliances Citrix SD-WAN gérées dans votre réseau SD-WAN.La page **Paramètres de l'appliance** vous permet d'effectuer les actions suivantes :

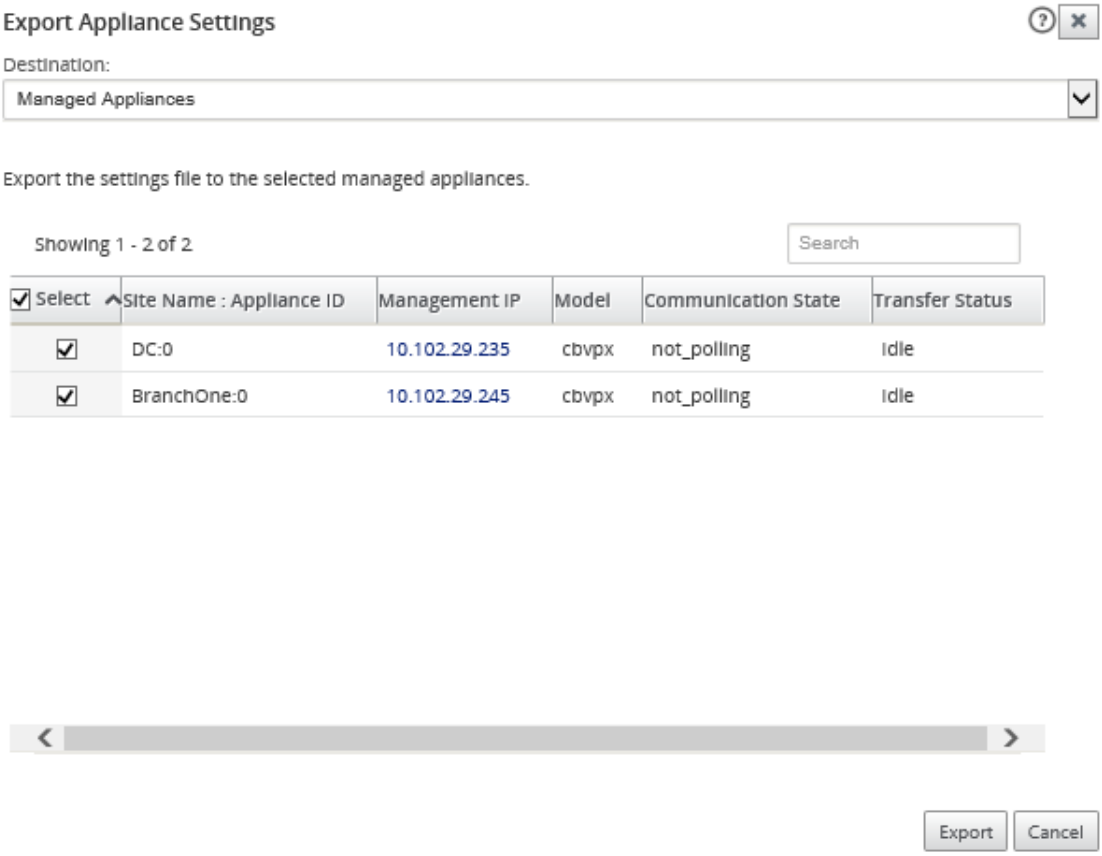
- Créez un nouveau fichier de paramètres de l'appliance.
- Ouvrez et modifiez un fichier de paramètres de l'appliance existant.
- Importez un fichier de paramètres de l'appliance à partir de votre ordinateur local.
- Téléchargez un fichier de paramètres de l'appliance sur votre ordinateur local.
- Exportez un fichier de paramètres de l'appliance vers les appliances gérées.

Pour créer un fichier de paramètres d'appliance et l'exporter vers des appliances gérées :

1. Dans l'interface Web Citrix SD-WAN Center, cliquez sur l'onglet **Configuration**.
2. Cliquez sur **Paramètres de l'appliance**, puis sur **Nouveau** .



3. Sélectionnez **Inclure dans le fichier** pour les paramètres requis et spécifiez les valeurs des paramètres. Pour plus d'informations, consultez le tableau des paramètres de l'appliance.
4. Cliquez sur **Exporter**. Dans la boîte de dialogue **Enregistrer sous**, entrez un nom pour le fichier de paramètres de l'appliance et cliquez sur **Enregistrer** . La boîte de dialogue **Exporter les paramètres de l'appliance** s'affiche.
5. Dans le champ **Destination**, sélectionnez **Appliances gérées** et sélectionnez les appliances pour lesquelles vous souhaitez exporter les paramètres de l'appliance.



> **Remarque**
>
> Pour télécharger les paramètres de l'appliance sur votre ordinateur local, dans le champ **Destination**, sélectionnez **Téléchargement de fichier** .

6. Cliquez sur **Exporter**.

Gestion de site LTE à distance

February 17, 2022

Citrix SD-WAN Center vous permet d'afficher et de gérer à distance tous les sites LTE de votre réseau. Il comprend des appareils connectés via un modem LTE interne ou un modem USB LTE externe.

Les appliances Citrix SD-WAN, telles que Citrix SD-WAN 210 SE LTE et 110 LTE Wi-Fi, disposent d'un modem LTE interne intégré. Vous pouvez également connecter un modem USB 3G/4G externe sur les appliances Citrix SD-WAN suivantes.

- Citrix SD-WAN 210 SE

- Citrix SD-WAN 210 SE LTE
- Citrix SD-WAN 110 SE
- Citrix SD-WAN 110 LTE Wi-Fi SE

CDC Ethernet, MBIM et NCM sont les trois types de modems USB externes pris en charge. Vous pouvez configurer les paramètres APN et activer/désactiver le modem via la nouvelle interface graphique Citrix SD-WAN et Citrix SD-WAN Center. Les opérations haut débit mobiles ne sont pas prises en charge sur les modems USB CDC Ethernet.

Exigences pour modem LTE externe :

- Utilisez les dongles USB LTE pris en charge. Les modèles matériels de dongle pris en charge sont Verizon USB730L et AT&T USB800.
- Assurez-vous qu'une carte SIM est insérée dans le dongle USB LTE. Les dongles CDC Ethernet LTE sont préconfigurés avec une adresse IP statique, ce qui interfère avec la configuration et provoque une défaillance de connexion ou une connexion intermittente, si la carte SIM n'est pas insérée.
- Avant d'insérer un dongle CDC Ethernet LTE dans l'appliance SD-WAN, connectez la clé USB externe à une machine Windows/Linux et assurez-vous que l'Internet fonctionne correctement avec la configuration APN et Mobile Data Roaming. Assurez-vous que le mode de connexion du dongle USB passe de la valeur par défaut Manual à Auto.

> **Remarque**
>
> - Les appliances Citrix SD-WAN prennent en charge un seul dongle USB LTE à la fois. Si plus d'un dongle USB est branché, débranchez tous les dongles et branchez un seul dongle.
> - Les appliances Citrix SD-WAN ne prennent pas en charge le nom d'utilisateur et le mot de passe pour les modems USB. Assurez-vous que la fonction de nom d'utilisateur et de mot de passe est désactivée sur le modem pendant la configuration.
> - Le débranchement ou le redémarrage d'un dongle MBIM externe a un impact sur la session de données du modem LTE interne. Il s'agit d'un comportement attendu.
> - Lorsqu'un modem LTE externe est branché, l'appliance SD-WAN prend environ 3 minutes pour le reconnaître.

Opérations prises en charge sur les modems internes et externes :

Opérations	Modem interne	Modem externe - CDC Ethernet	Modem externe - MBIM et NCM
Préférence SIM	Oui - Pour les appareils qui prennent en charge la double SIM	Non	Non

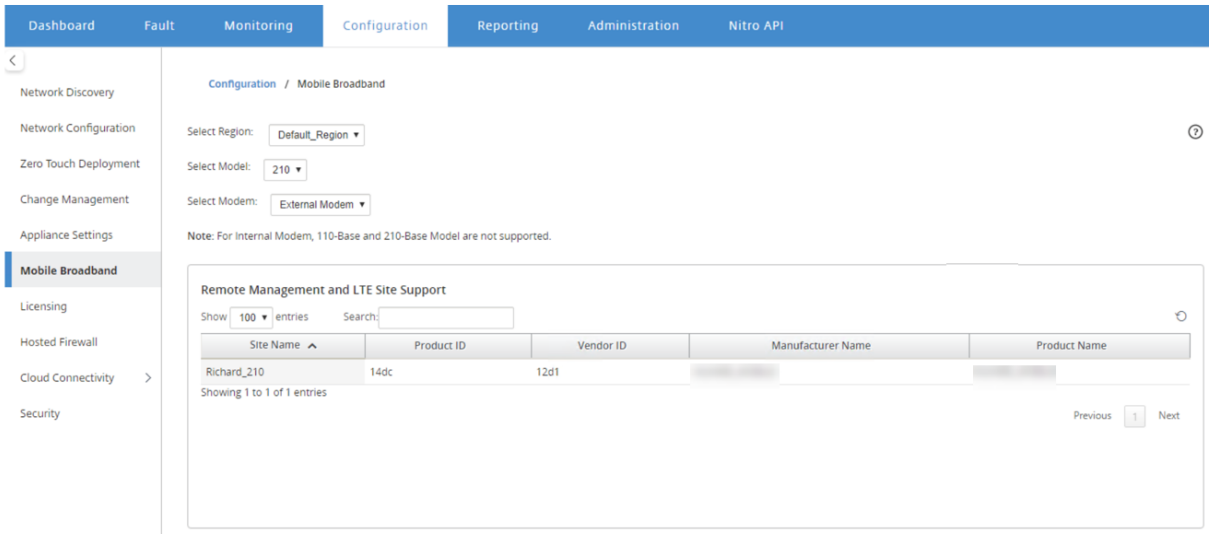
Opérations	Modem interne	Modem externe - CDC Ethernet	Modem externe - MBIM et NCM
Code PIN de la carte SIM	Oui	Non	Non
Paramètres APN	Oui	Non	Oui
Paramètres réseau	Oui	Non	Non
Itinérant	Oui	Non	Non
Gérer le firmware	Oui	Non	Non
Activer/désactiver le modem	Oui	Non	Oui
Redémarrer le modem	Oui	Non	Non
Actualiser la carte SIM	Oui	Non	Non

Pour gérer à distance les sites LTE de votre réseau, dans l'interface utilisateur de SD-WAN Center, accédez à **Configuration > Mobile Broadband**. Toutes les appliances LTE, sur tous les sites, gérées par SD-WAN Center sont répertoriées ici.

Pour un déploiement multi-région, vous pouvez sélectionner une région pour laquelle vous souhaitez gérer les sites LTE. La valeur Default_Region est sélectionnée par défaut.

Vous pouvez également sélectionner le modèle d'appliance LTE et le type de modem.

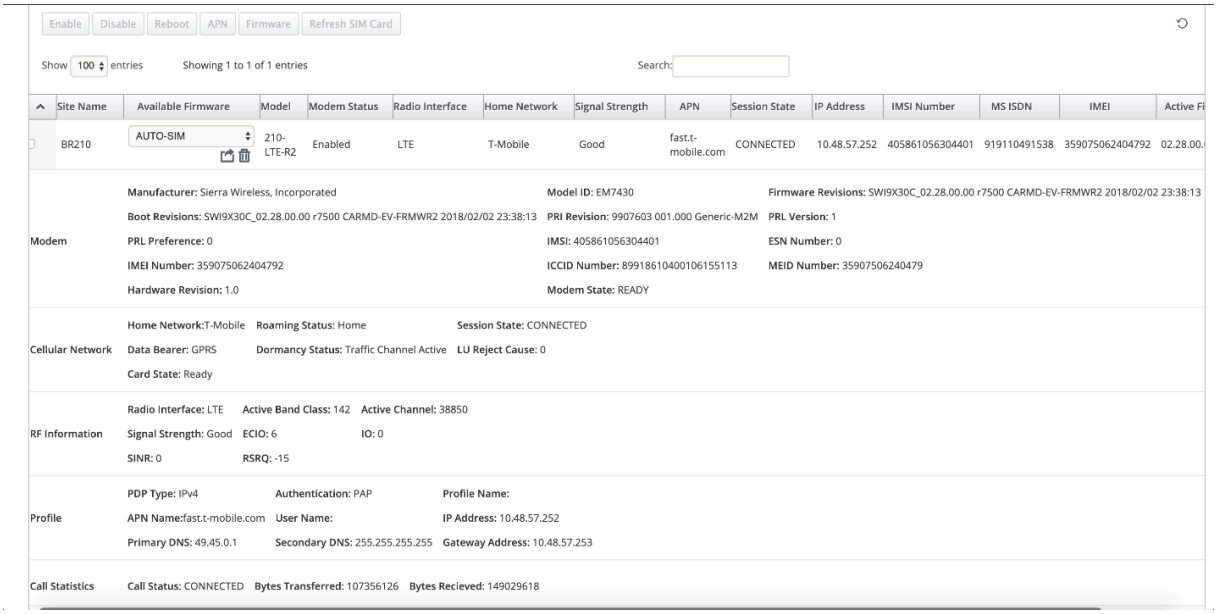
Pour répertorier les appliances à l'aide d'un modem externe, accédez à **Configuration** > **Haut débit mobile**. Sélectionnez **Modem externe** comme type de modem.



> **Remarque**
>
> Le code PIN SIM et les autres configurations de modem LTE ne sont actuellement pas pris en charge pour les modems externes.

Pour répertorier les appliances à l'aide d'un modem interne, accédez à **Configuration** > **Haut débit mobile**. Sélectionnez **Modem interne** comme type de modem.

> **Remarque**
>
> Les opérations LTE sont différentes pour différents modèles LTE.



Vous pouvez sélectionner une appliance ou plusieurs appliances pour effectuer l'opération de modem LTE suivante :

- **Activer** : activez le modem sur les sites sélectionnés.
- **Désactiver** : désactivez le modem sur les sites sélectionnés.
- **Redémarrage** : redémarrez le modem sur les sites sélectionnés.
- **APN** : configurez les paramètres APN pour les sites sélectionnés. Pour plus d'informations, consultez Configurer les paramètres APN.
- **Firmware** : Cette option s'applique uniquement à l'appliance 210 LTE. Parcourez et sélectionnez le firmware requis. Vous pouvez choisir de télécharger uniquement ou de télécharger et d'appliquer le fichier de microprogramme sur les sites sélectionnés. Dans la liste des micrologiciels disponibles, vous pouvez choisir de l'appliquer ou de le supprimer.

> **Remarque**
>
> Dans le déploiement multi-région, les opérations de microprogramme pour les sites de région autres que par défaut ne peuvent pas être effectuées à partir du Headend de SD-WAN Center. Vous pouvez effectuer des opérations de microprogramme à partir du Collector SD-WAN Center de la région spécifique.

- **Actualiser la carte SIM** : actualisez la carte SIM en la désactivant et en la réactivant sur les sites sélectionnés. Cette opération est effectuée pour détecter la nouvelle carte SIM insérée dans le modem 210 SE LTE.
- **Préférence SIM** : Cette option s'applique uniquement à l'appliance 110 LTE. L'appliance 110 LTE prend en charge la double SIM et vous pouvez définir la préférence SIM.
- **Mode réseau** : vous pouvez sélectionner le réseau mobile sur les appliances Citrix SD-WAN qui prennent en charge le modem LTE interne. Les réseaux pris en charge sont 3G, 4G ou les deux. Pour les appliances 110 LTE, sélectionnez la carte SIM sur laquelle appliquer les modifications.
- **Itinérance** : l'option d'itinérance est activée par défaut sur vos appliances LTE, vous pouvez choisir de la désactiver. Pour les appliances 110 LTE, sélectionnez la carte SIM sur laquelle appliquer les modifications.

Vous pouvez également configurer la fonctionnalité LTE sur des appliances LTE individuelles. Pour plus d'informations, consultez Configurer la fonctionnalité LTE sur 210 SE LTE.

Pour plus d'informations sur la configuration d'un appareil 110-LTE-WIFI, voir Configurer la fonctionnalité LTE sur le Wi-Fi 110 LTE.

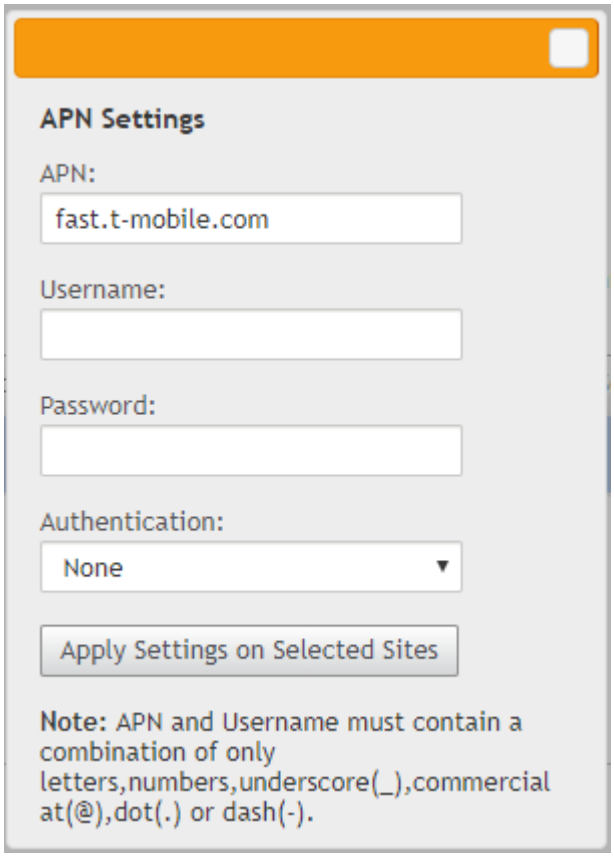
Paramètres APN

APN est le nom des paramètres que votre appliance lit pour configurer une connexion à la passerelle entre le réseau cellulaire de l'opérateur et l'Internet public. Vous pouvez obtenir les informations APN du transporteur et configurer à distance les paramètres **APN** sur un ou plusieurs appliances LTE.

> **Remarque**
>
> Les paramètres APN varient d'un transporteur à l'autre.

Pour configurer les paramètres APN :

1. Dans l'interface utilisateur du SD-WAN Center, accédez à **Configuration > Haut débit mobile**. Sélectionnez les sites LTE pour lesquels vous souhaitez configurer les paramètres APN et cliquez sur **APN**.



2. Pour une appliance LTE 110, sélectionnez la carte SIM sur laquelle les paramètres APN sont appliqués.
3. Entrez le **nom APN**, le **nom d'utilisateur**, le **mot de passe** et **l'authentification** fournis par le transporteur. Vous pouvez choisir parmi les protocoles d'authentification PAP, CHAP, PAPCHAP. Si le transporteur n'a fourni aucun type d'authentification, définissez-le sur **Aucun**.
4. Cliquez sur **Appliquer les paramètres sur les sites sélectionnés**.

Centre Citrix SD-WAN en tant que serveur de licences

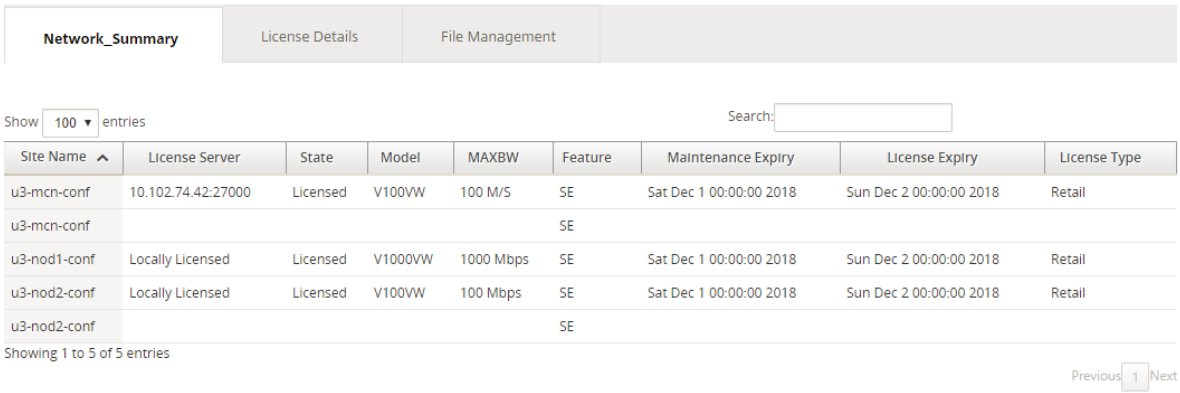
February 17, 2022

Vous pouvez acquérir les licences pour les appliances de votre réseau, les télécharger et les installer dans SD-WAN Center. Pour utiliser SD-WAN Center comme serveur de licences distant, configurez l'adresse IP du SD-WAN Center en tant que serveur distant pour la gestion centralisée des licences. Pour plus d'informations, consultez la section Gestion centralisée des licences.

Après avoir poussé la configuration réseau vers les sites via le processus de gestion des modifications, et une fois la configuration activée, les appliances de succursale obtiennent automatiquement les li-

cences du SD-WAN Center.
Pour que ces licences soient utilisées, il faut attribuer les licences à l'hôte du SD-WAN Center lui-même.

Pour afficher les détails de licence de toutes les appliances découvertes par SD-WAN Center, accédez à **Configuration** > **Licensing** > **Récapitulatif du réseau.**



Les paramètres suivants sont affichés :

- **Nom du site** : Nom du site.
- **Serveur de licences** : Adresse IP et numéro de port du serveur de licences. Si la licence a été installée localement sur l'appliance, elle s'affiche sous la forme « Licence locale ».
- **État : état**actuel de la licence de l'appliance, sous licence ou sans licence.
- **Modèle : modèle**d'appliance pris en charge par la licence.
- **MAXBW** : bande passante maximale autorisée par la licence.
- **Fonctionnalité** : l'édition Citrix SD-WAN prise en charge par la licence.
- **Expiration de maintenance** : date d'expiration de Citrix Subscription Advantage.

  > **Remarque**
  >
  > Pendant la mise à niveau du logiciel, si la date de construction du logiciel est supérieure à la date d'expiration de la maintenance, la mise à niveau du logiciel n'est pas autorisée.

- **Expiration de la licence** : date d'expiration de la licence.
- **Type de licence** : Type de licence.

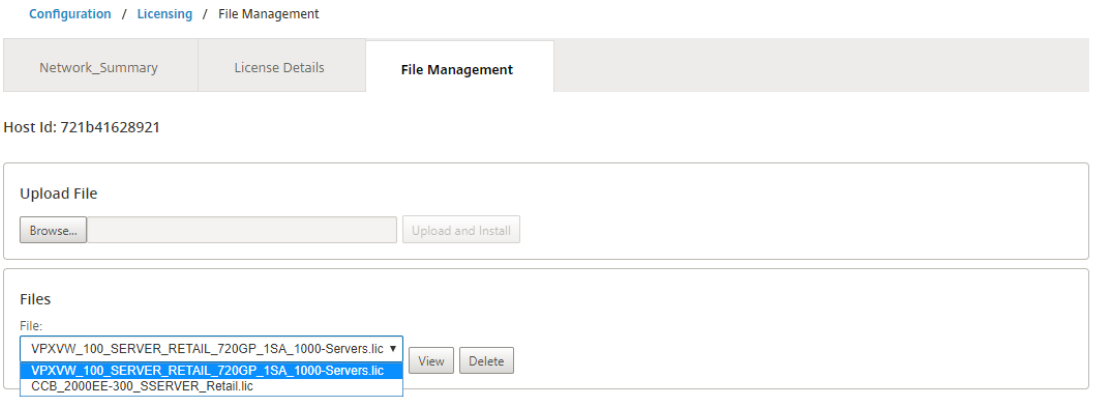
Pour télécharger et installer des fichiers de licence dans SD-WAN Center :

1. Obtenez la licence pour les appliances Citrix SD-WAN et enregistrez-la sur votre ordinateur local.

> **Remarque**
>
> Pour obtenir des instructions sur l'obtention d'une licence logicielle Citrix SD-WAN, contactez le support client Citrix SD-WAN.

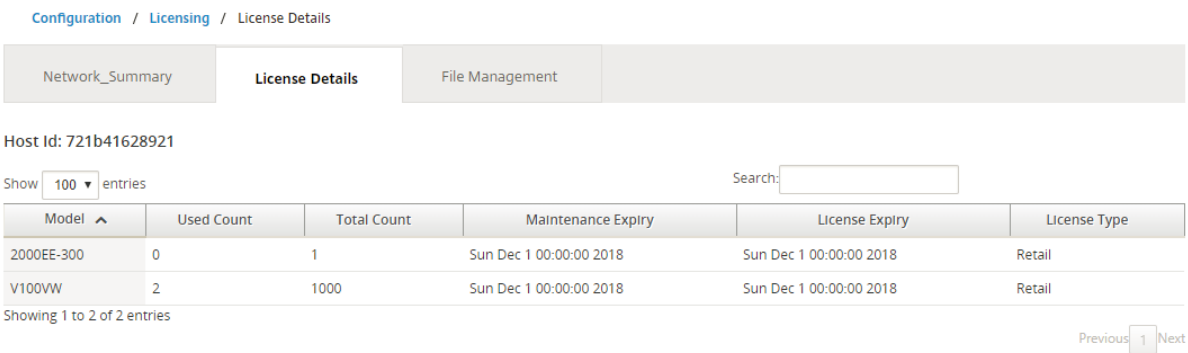
2. Dans l'interface graphique graphique du SD-WAN Center, accédez à **Licences** > **Gestion des fichiers** .
3. Dans la section **Charger un fichier**, cliquez sur **Parcourir**. Sélectionnez le fichier de licence à partir de votre ordinateur local et cliquez sur **Télécharger et installer**.

   Les fichiers de licence installés sont répertoriés dans le menu déroulant **Fichiers**, vous pouvez choisir d'afficher ou de supprimer les fichiers de licence.



> **Remarque**
>
> L'ID d'hôte est l'ID d'hôte SD-WAN Center, utilisé pour générer les fichiers de licence. Les fichiers de licence générés à l'aide d'un autre ID d'hôte ne peuvent pas être téléchargés et installés sur Citrix SD-WAN Center.

Vous pouvez afficher les détails de tous les fichiers de licences chargés et installés sur Citrix SD-WAN Center, en un coup d'œil, en accédant à **Configuration** > **Licence** > **Détails de la licence**.



Les paramètres suivants sont affichés :

- **Modèle :** modèle d'appliance pris en charge par la licence.
- **Nombre d'applications :** Nombre d'appliances sur lesquelles cette licence est installée.
- **Nombre total :** Nombre total d'appliances sur lesquelles cette licence peut être installée.
- **Expiration de maintenance** : date d'expiration de Citrix Subscription Advantage.
- **Expiration de la licence** : date d'expiration de la licence.
- **Type de licence** : Type de licence.

Déployer Citrix SD-WAN sur Azure à partir du Centre Citrix SD-WAN

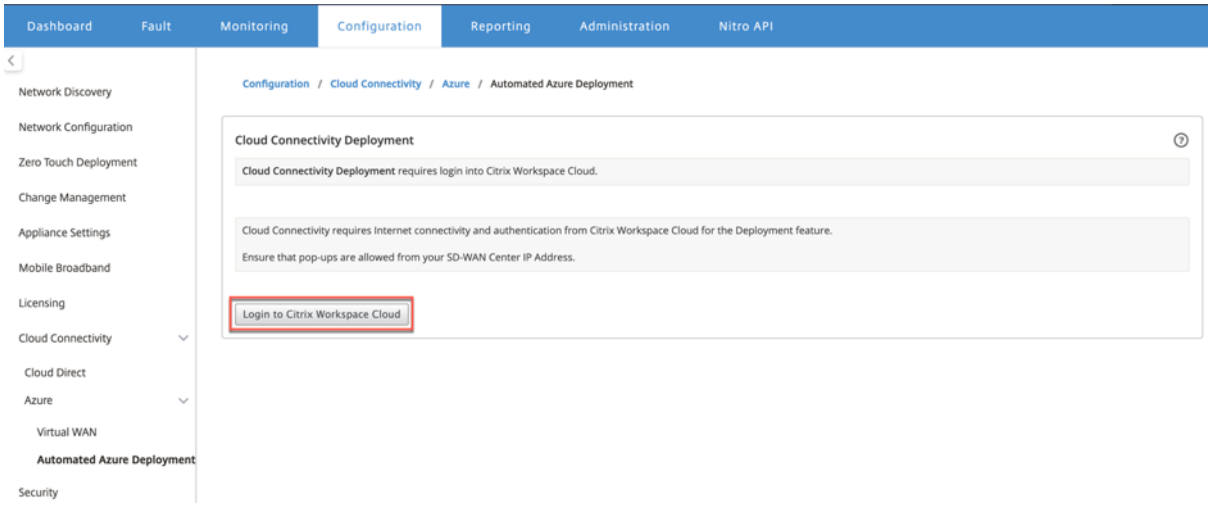
February 17, 2022

Citrix SD-WAN pour Azure permet aux entreprises d'avoir une connexion sécurisée directe de chaque succursale aux applications hébergées dans Azure, ce qui élimine la nécessité de retransmettre le trafic lié au cloud via un centre de données.

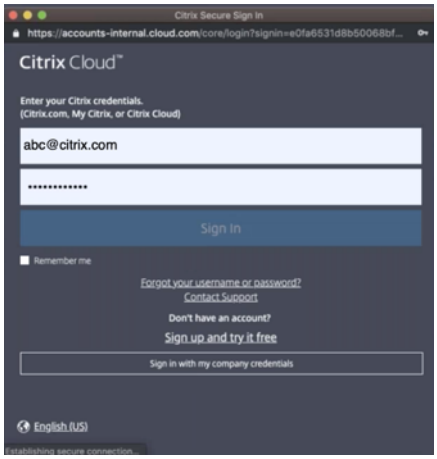
Conditions préalables

- Informations d'identification Citrix Workspace Cloud.
- Informations d'identification d'abonnement Azure
- Principal d'application et de service Azure avec le contrôle d'accès basé sur les rôles, consultez Procédure : utiliser le portail pour créer une application Azure AD et un principal de service pouvant accéder aux ressources.
- Une fois le principal de service créé, notez les détails suivants :
  - ID d'abonné Azure
  - ID de locataire
  - ID de l'application
  - Clé secrète
- Effectuez la gestion des modifications sur le MCN/SD-WAN Center à l'aide du fichier ctx-sdw-sw-xxxxxxx.zip.
- Depuis Citrix SD-WAN Center, découvrez le MCN et tirez la configuration active.

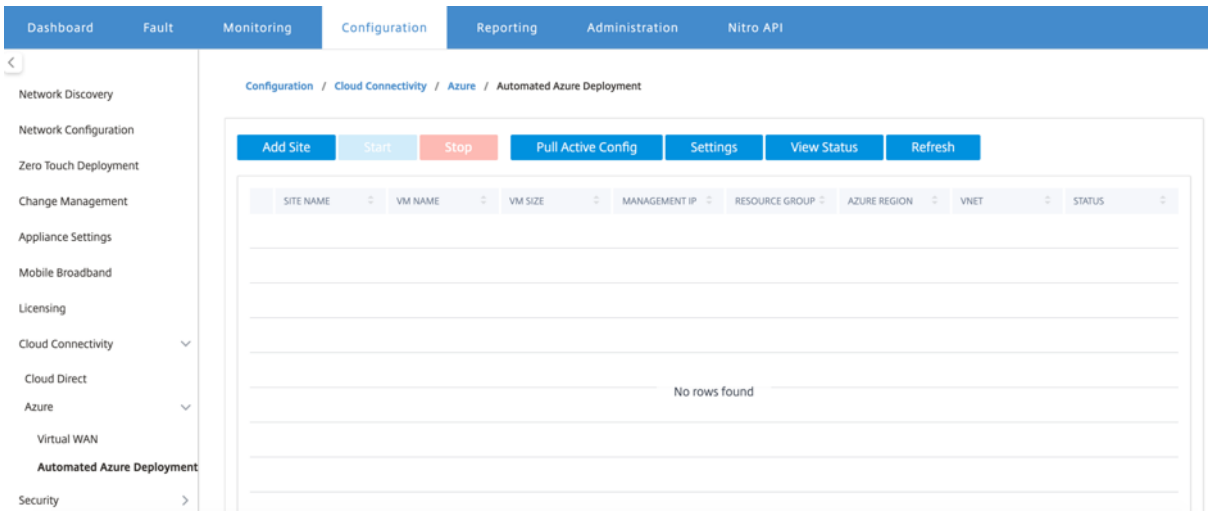
Pour déployer Citrix SD-WAN sur Azure à partir de SD-WAN Center, accédez à **Configuration > Connectivité cloud > Azure > Déploiement automatisé Azure**.



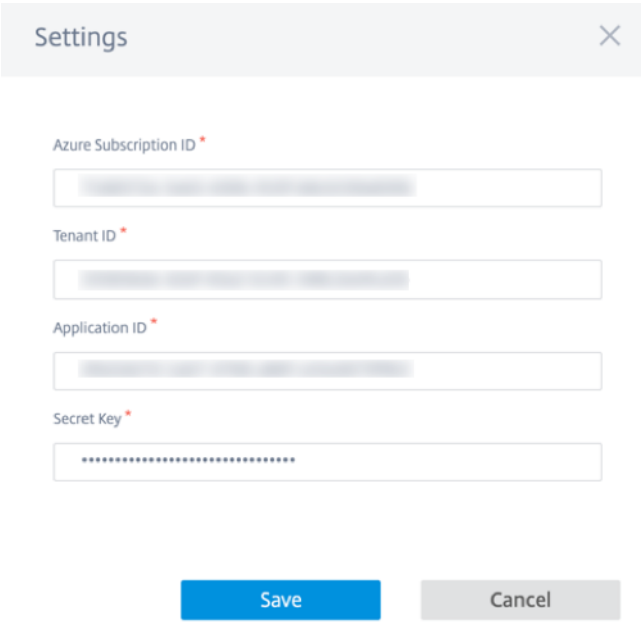
Connectez-vous avec les informations d'identification Citrix Cloud.



Déploiement automatique Azure



Cliquez sur l'option **Paramètres** et fournissez les détails de l'abonnement Azure. Cliquez sur l'option Pull Active Config pour récupérer la configuration active en cours d'exécution à partir du MCN.



Déployer Citrix SD-WAN dans Azure

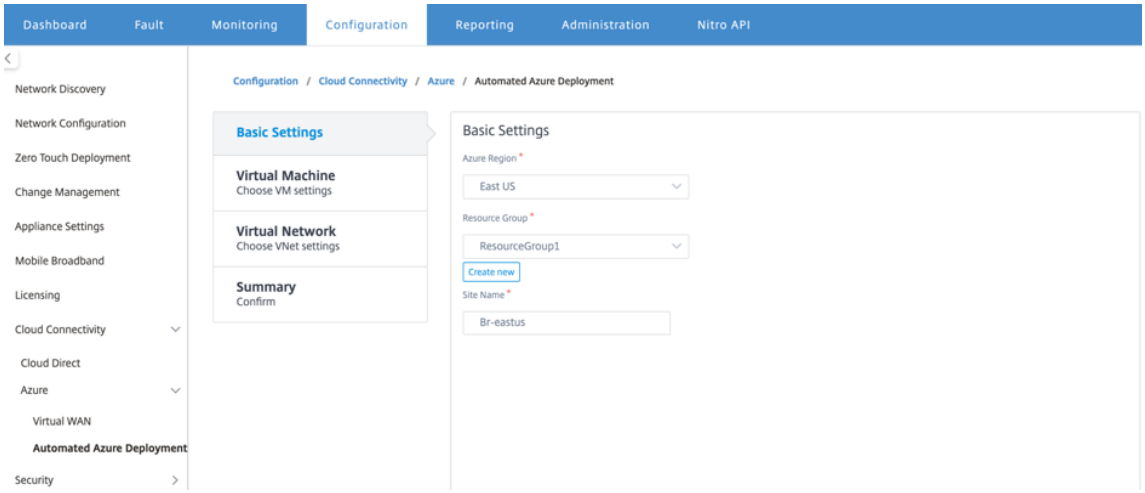
Pour déployer Citrix SD-WAN dans Microsoft Azure :

1. Cliquez sur **Ajouter un site** pour ajouter une nouvelle instance SD-WAN. Il initie la création d'une machine virtuelle SD-WAN sur Azure dans le cadre de votre abonnement actuel.

   Dans le cadre de ce déploiement, il a également :

   - Ajoute automatiquement la configuration SD-WAN pour le site nouvellement ajouté à la configuration active actuelle sur MCN.
   - Effectue la gestion des modifications.
   - Appliquez la version et la configuration du logiciel du MCN à ce nouveau site.

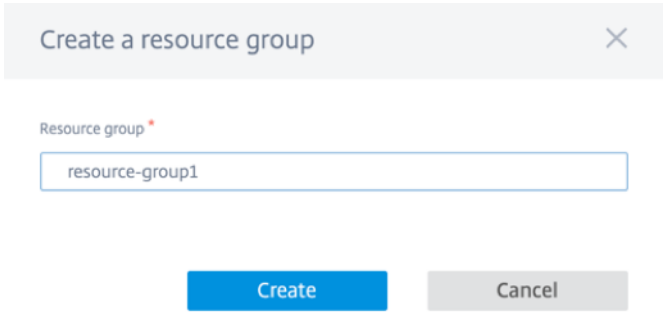
   Complétez les **paramètres de base, Machine virtuelleet Réseau virtuel**.



Sous Paramètres de base, sélectionnez la région et le groupe de ressources dans la liste déroulante. Une fois la région sélectionnée, la liste déroulante du groupe de ressources affiche tous les groupes de ressources existants dans cette région sous cet abonnement.

> **REMARQUE :**
>
> Pour ajouter un site, le groupe de ressources doit être vide.

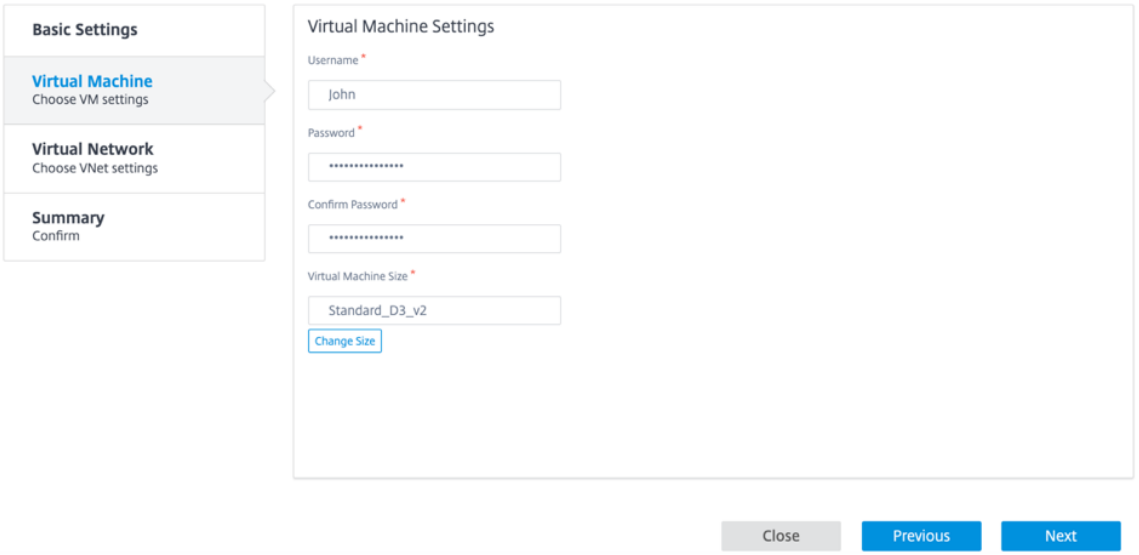
Vous pouvez choisir un groupe de ressources vide existant ou cliquer sur l'option **Créer un nouveau** pour en créer un nouveau.



2. Le nom du site est généré automatiquement avec le nom de la région. Vous pouvez toujours modifier le nom du site si nécessaire.

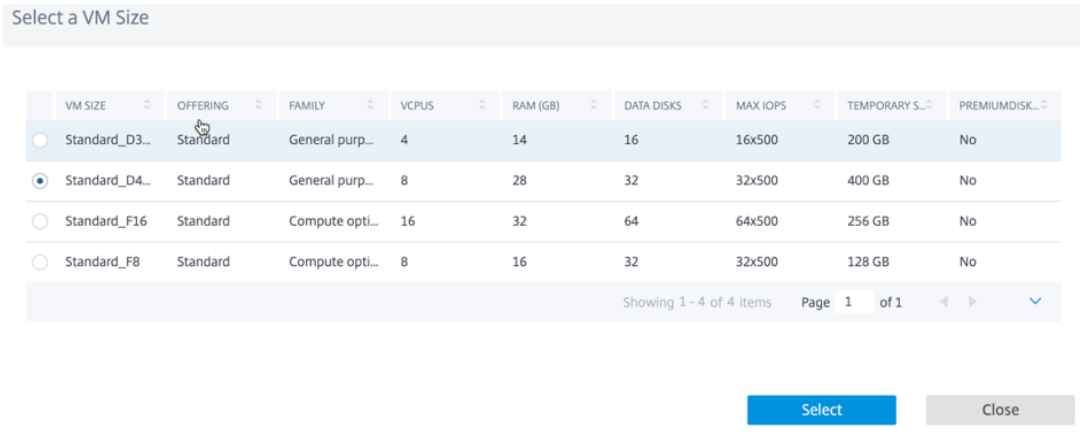
   > **REMARQUE :**
   >
   > Assurez-vous que le nom de site respecte les exigences de nom de site SD-WAN et qu'il est unique dans le réseau SD-WAN.
   >
   > Le nom de la machine virtuelle Azure est généré à partir du nom du site au format **AZ-regionname-sitename**.

3. Cliquez sur **Suivant** pour configurer la machine virtuelle.

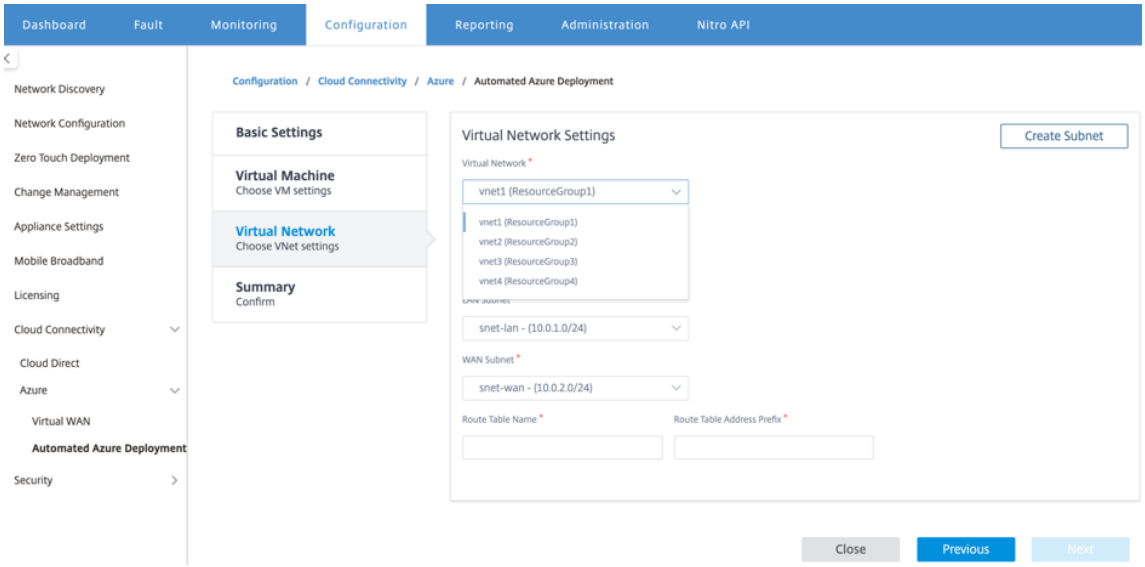


Fournissez un nom d'utilisateur, un mot de passe et un mot de passe de confirmation. Par défaut, la taille de la machine virtuelle est automatiquement remplie avec la taille standard. Cliquez sur **Modifier la taille** pour sélectionner une autre taille de machine virtuelle si nécessaire.

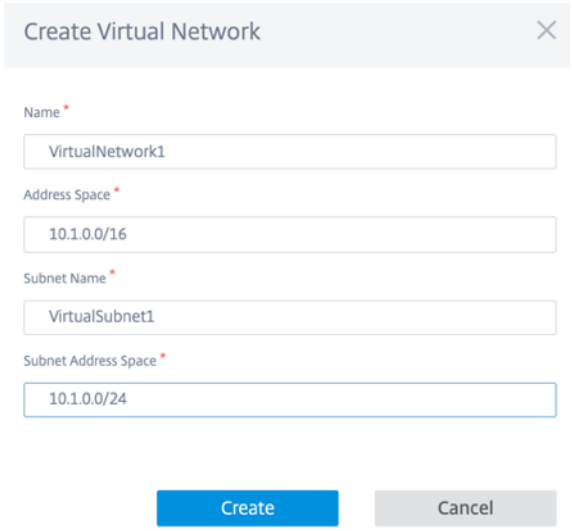
> **REMARQUE :**
>
> Ces informations d'identification utilisateur fournies pendant le déploiement disposent d'un accès en lecture seule au SD-WAN Azure. Pour les privilèges d'administration, utilisez les informations d'identification d'administrateur.



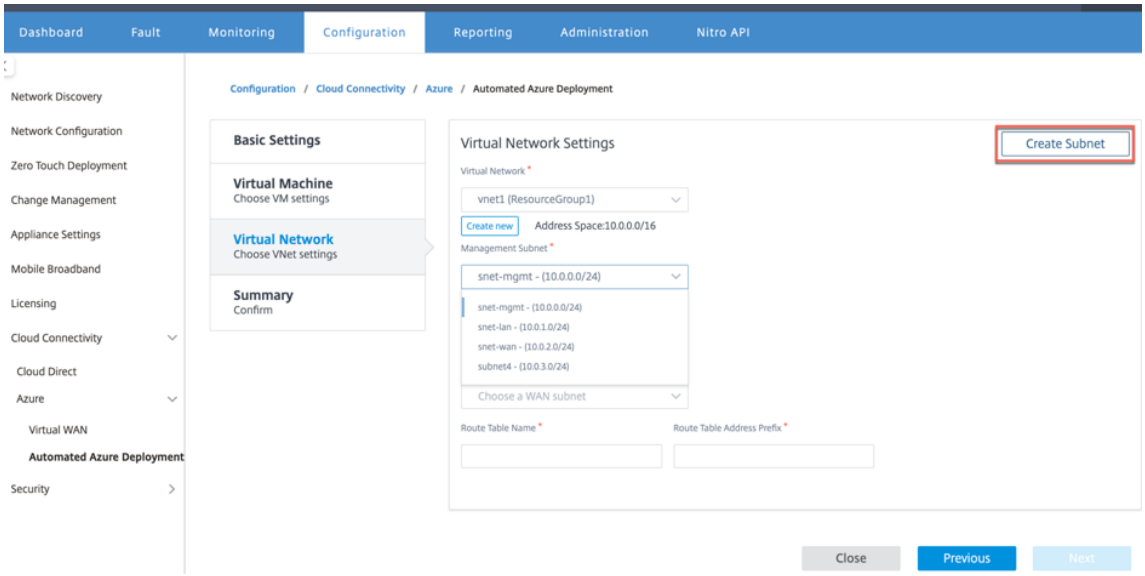
4. Cliquez sur **Suivant** pour exécuter les paramètres du réseau virtuel.
5. Sélectionnez Réseau virtuel dans la liste déroulante. La liste contient tout le réseau virtuel de la région Azure sélectionnée.



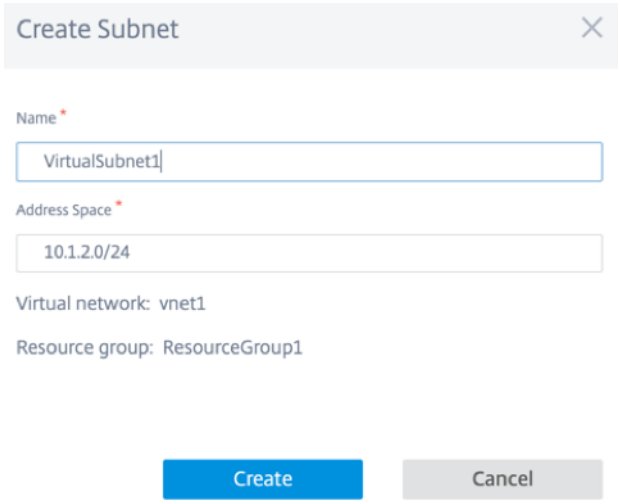
Vous pouvez déployer le site sur un réseau virtuel existant ou créer un nouveau réseau virtuel. Cliquez sur **Créer un nouveau** réseau pour créer un nouveau réseau virtuel. Indiquez le nom du réseau virtuel, l'espace d'adressage (spécifiez un espace d'adressage IP privé personnalisé), le nom du sous-réseau et l'espace d'adressage du sous-réseau.



6. Sélectionnez un sous-réseau pour la gestion.



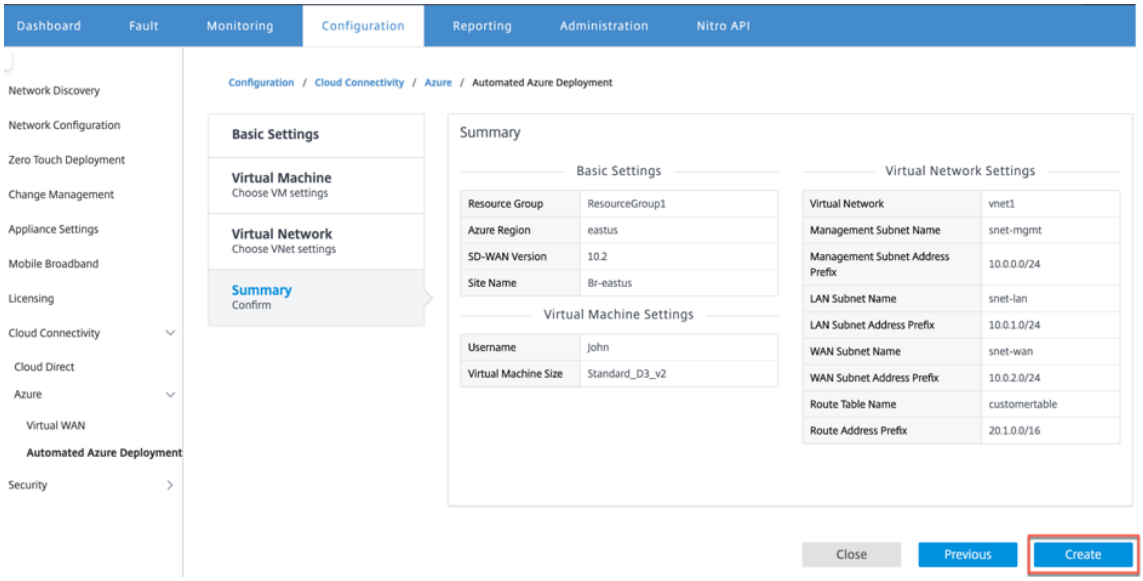
7. Vous pouvez également créer un sous-réseau à l'aide de l'option **Créer un sous-réseau** (dans le coin supérieur droit).



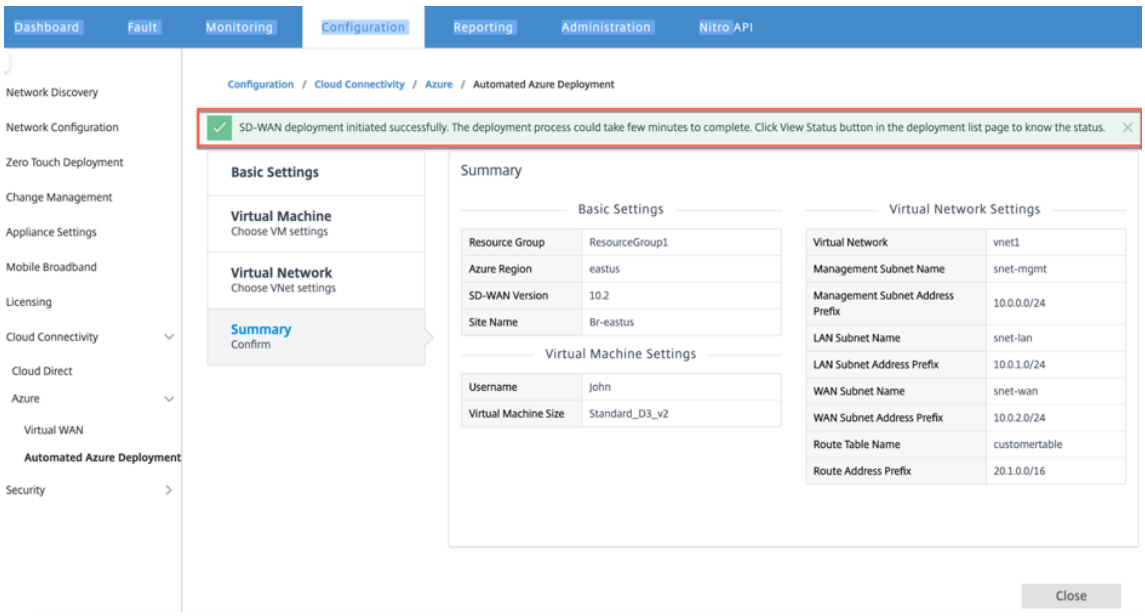
8. Dans la liste déroulante, choisissez un sous-réseau différent pour le réseau local et le réseau étendu et indiquez le **nom de la table de routage** ainsi que le **préfixe d'adresse de la table de routage**. Le **préfixe d'adresse de table de routage** est l'espace d'adressage de destination qui est redirigé vers ce dispositif SD-WAN. Les autres adresses cibles seront redirigées par le routage Azure.

> **REMARQUE :**
>
> La table de routage est associée au sous-réseau LAN. Si le sous-réseau LAN choisi possède déjà une table de routage associée, cette table de routage s'affiche et ne peut pas être modifiée. Sinon, vous pouvez spécifier le nom de la table de routage.

9. Cliquez sur **Suivant** pour vérifier et confirmer les détails du paramètre, puis cliquez sur **Créer**.



Un message d'état apparaît en haut indiquant que le déploiement a démarré correctement.



Le déploiement peut prendre du temps, il est donc recommandé de cliquer sur **Afficher l'état** pour obtenir la dernière mise à jour sur l'état du déploiement.

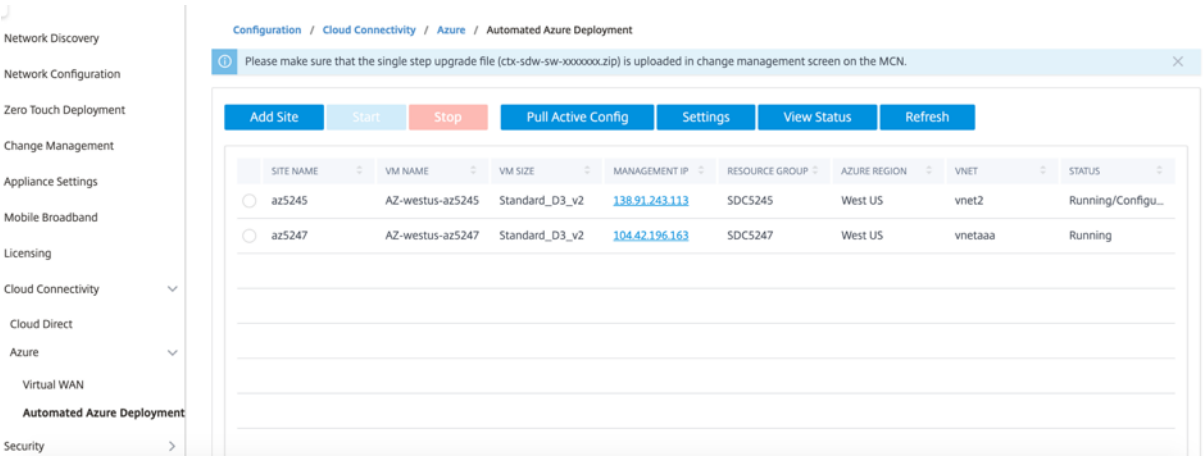
Dans le cadre du déploiement :

- La machine virtuelle est créée dans la région Azure sélectionnée.
- Un site est automatiquement ajouté à la configuration SD-WAN active dans le SD-WAN.
- La gestion des modifications est effectuée sur la machine virtuelle Azure nouvellement provisionnée.

Une fois le déploiement réussi, les chemins virtuels sont formés entre le site MCN et Azure. Si le dé-

ploiement rencontre une erreur, le processus est annulé et toutes les ressources créées automatiquement sont rétablies.

Par défaut, le site est placé dans le domaine de routage par défaut. Il appartient à la région par défaut à l'aide du groupe de chemins automatiques par défaut.



- **Nom du site** : nom du site Citrix SD-WAN. Ce nom de site est utilisé dans la configuration Citrix SD-WAN.
- **Nom de la machine virtuelle** : nom de la machine virtuelle (VM) provisionnée dans Azure.
- **Taille de la machine**virtuelle : taille de machine virtuelle sélectionnée lors de la création du site.
- **IP de gestion** : adresse IP de gestion qui a été attribuée à la machine virtuelle SD-WAN nouvellement créée.
- **Groupe de ressources** : les groupes de ressources sont des constructions logiques et l'échange de données entre les groupes de ressources est toujours possible. La machine virtuelle Azure appartient à ce groupe de ressources. Les nouvelles ressources créées lors du déploiement de Citrix SD-WAN sont regroupées sous ce groupe de ressources. En cas d'erreur lors du déploiement, les ressources créées dans ce groupe de ressources seront supprimées.
- **Région Azure** : représente l'emplacement du groupe de ressources et de ses ressources.
- **VNet** : Réseau virtuel utilisé par le site.
- **Statut** : Fournit l'état de la machine virtuelle.

Cliquez sur le bouton **Actualiser** pour obtenir le dernier état du site. Vous pouvez **démarrer** ou **arrêter** la machine virtuelle à tout moment pour le site sélectionné. Vous ne pouvez sélectionner qu'un site à la fois.

Lorsque le déploiement est terminé, connectez-vous à MCN ou à Citrix SD-WAN Center pour afficher l'état des chemins d'accès virtuels.

Déploiement sans intervention

February 17, 2022

> **Remarque**
>
> Le service de déploiement Zero Touch est pris en charge uniquement sur certains matériels Citrix SD-WAN :
>
> - SD-WAN 110 Édition Standard
> - SD-WAN 210 Édition Standard
> - SD-WAN 410 Édition Standard
> - SD-WAN 2100 Édition Standard
> - SD-WAN 1000 Standard Edition (réimageage requise)
> - SD-WAN 1000 Édition Entreprise (Édition Premium) (réimage requise)
> - SD-WAN 1100 Édition Standard
> - SD-WAN 1100 Édition Premium (Entreprise)
> - SD-WAN 2000 Standard Edition (réimage requise)
> - SD-WAN 2000 Édition Entreprise (Édition Premium (réimage requise)
> - Instance VPX AWS SD-WAN

Le service ZTD (Déploiement sans intervention) est un service cloud géré et exploité par Citrix qui permet la découverte de nouvelles appliances dans le réseau Citrix SD-WAN et automatise le processus de déploiement pour les succursales. Le service cloud ZTD est accessible depuis n'importe quel nœud du réseau via Internet et via le protocole SSL (Secure Socket Layer).

Le service cloud ZTD communique en toute sécurité avec les services réseau Citrix principal en stockant l'identification des clients ayant acheté des périphériques compatibles Zero Touch (par exemple, SD-WAN 410-SE, 2100-SE). Les services backend sont en place pour authentifier toute demande de déploiement sans intervention, validant correctement l'association entre le compte client et les numéros de série des appliances Citrix SD-WAN.

Architecture et flux de travail de haut niveau ZTD

Site DataCenter

Administrateur Citrix SD-WAN : utilisateur disposant des droits d'administration de l'environnement SD-WAN avec les responsabilités principales suivantes :

- Création de la configuration à l'aide de l'outil Citrix SD-WAN Center Network Configuration ou importation de la configuration à partir de l'appliance SD-WAN Master Control Node (MCN)

- Connexion Citrix Cloud pour lancer le service de déploiement sans intervention pour le déploiement de nouveaux nœuds de site.

> **Remarque**
>
> Si votre SD-WAN Center est connecté à Internet via un serveur proxy, vous devez configurer les paramètres du serveur proxy sur SD-WAN Center. Pour plus d'informations, consultez la sectionParamètres du serveur proxy pour le déploiement Zero Touch.

Administrateur réseau : utilisateur responsable de la gestion du réseau d'entreprise (DHCP, DNS, Internet, pare-feu, etc.)

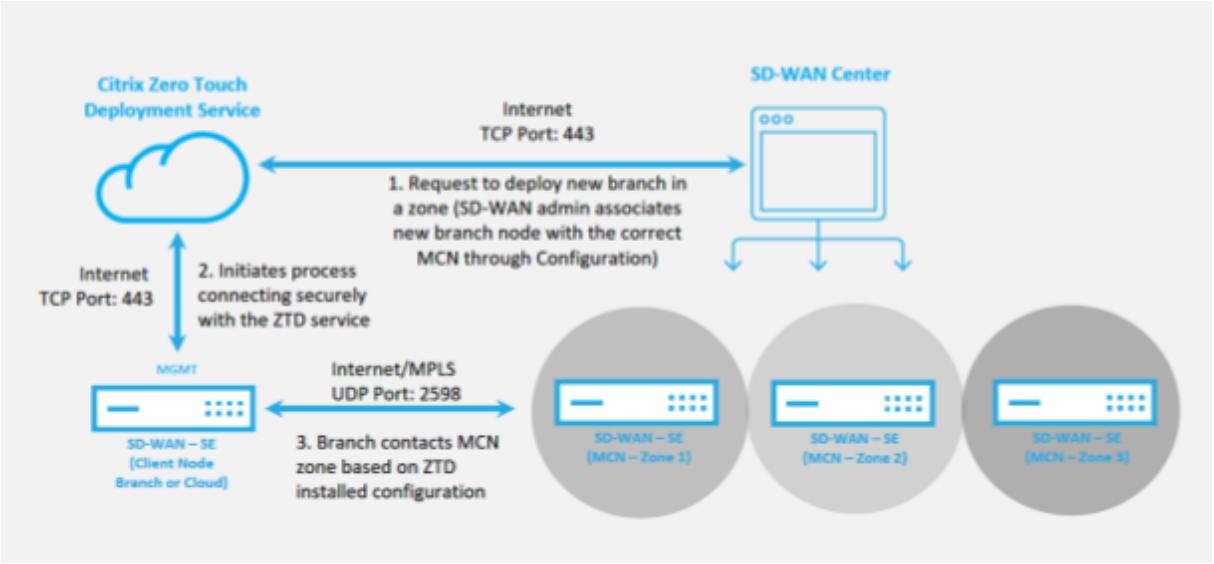
- Si nécessaire, configurez les pare-feu pour la communication sortante vers le nom de domaine complet ***sdwanzt.citrixnetworkapi.net*** à partir de SD-WAN Center.

Site distant

Installateur sur site —Un contact local ou un installateur engagé pour une activité sur site avec les principales responsabilités suivantes :

- Décompressez physiquement l'appliance Citrix SD-WAN.
- Réimagez les appliances non compatibles avec ZTD.
  - Requis pour : SD-WAN 1000-SE, 2000-SE, 1000-EE, 2000-EE
  - Non requis pour : SD-WAN 410-SE, 2100-SE
- Câble d'alimentation de l'appareil.
- Câblez-le pour la connectivité Internet sur l'interface de gestion (par exemple, MGMT ou 0/1).
- Câble l'appliance pour la connectivité WAN sur les interfaces Data (par exemple apA.WAN, apB.WAN, apC.WAN, 0/2, 0/3, 0/5, etc.).

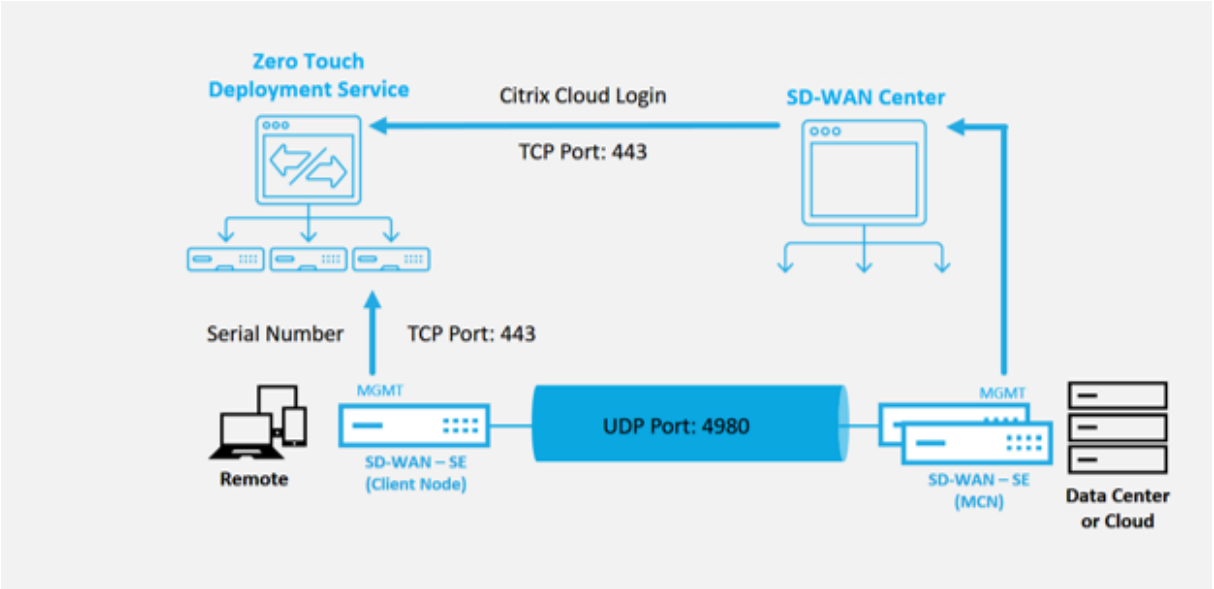
> **Remarque**
>
> La disposition de l'interface est différente pour chaque modèle, donc s'il vous plaît référencer la documentation pour l'identification des ports de données et de gestion.



Les conditions préalables suivantes sont requises avant de démarrer un service de déploiement sans intervention :

- Exécution active du SD-WAN promu au MCN (Master Control Node).
- Exécution active du SD-WAN Center avec connectivité au MCN via Virtual Path.
- Informations d'identification de connexion Citrix Cloud créées sur https://onboarding.cloud.com (reportez-vous aux instructions ci-dessous sur la création du compte).
- Connectivité réseau de gestion (SD-WAN Center et appliance SD-WAN) à Internet sur le port 443, soit directement, soit via un serveur proxy.
- Connectivité Internet sur le port 443 pour accéder au portail Web de SD-WAN Center pour la configuration initiale de ZTD.
- (Facultatif) Au moins une appliance SD-WAN en cours d'exécution active opérant dans une succursale en mode client avec une connectivité de chemin virtuel valide à MCN pour aider à valider la mise en place du chemin sur le réseau de sous-couche existant.

La dernière condition préalable n'est pas obligatoire, mais elle permet à l'administrateur SD-WAN de valider que le réseau sous-jacent autorise l'établissement de chemins virtuels lorsque le déploiement Zero Touch est terminé avec tout site nouvellement ajouté.Principalement, cela confirme que les politiques de pare-feu et d'itinéraire appropriées sont en place pour le trafic NAT en conséquence ou que la capacité du port UDP 4980 peut pénétrer avec succès le réseau pour atteindre le MCN.



Présentation du service de déploiement sans intervention

Le service de déploiement sans intervention fonctionne en tandem avec le SD-WAN Center pour faciliter le déploiement des appliances SD-WAN des succursales. SD-WAN Center est configuré et utilisé comme outil de gestion central pour les appliances SD-WAN Standard et Enterprise (Premium) Edition.Pour utiliser le service de déploiement sans intervention (ou ZTD Cloud Service), un administrateur doit commencer par déployer le premier périphérique SD-WAN dans l'environnement, puis configurer et déployer le SD-WAN Center en tant que point central de gestion.Lorsque le SD-WAN Center, version 9.1 ou ultérieure, est installé avec une connectivité à l'Internet public sur le port 443, SD-WAN Center lance automatiquement le service Cloud et installe les composants nécessaires pour déverrouiller les fonctionnalités de déploiement sans intervention et rendre l'option de déploiement sans intervention disponible dans l'interface graphique du SD-WAN Center. Le déploiement Zero Touch n'est pas disponible par défaut dans le logiciel SD-WAN Center.Ceci est conçu pour s'assurer que les composants préliminaires appropriés du réseau de sous-couche sont présents avant de permettre à un administrateur de lancer toute activité sur site impliquant le déploiement sans intervention.

Une fois qu'un environnement SD-WAN fonctionnel est en cours d'exécution, l'enregistrement dans le service de déploiement sans intervention est effectué par la création d'une connexion à un compte Citrix Cloud.Avec SD-WAN Center capable de communiquer avec le service ZTD, l'interface graphique expose les options de déploiement sans intervention sous l'onglet Configuration.La connexion au service Zero Touch authentifie l'ID client associé à l'environnement SD-WAN particulier et enregistre le SD-WAN Center en plus de déverrouiller le compte pour une authentification ultérieure des déploiements d'appliances ZTD.

À l'aide de l'outil Configuration réseau du SD-WAN Center, l'administrateur SD-WAN devra alors utiliser les modèles ou la capacité de clonage du site pour créer la configuration SD-WAN afin d'

ajouter de nouveaux sites.La nouvelle configuration est utilisée par le SD-WAN Center pour lancer le déploiement de ZTD pour les sites nouvellement ajoutés.Lorsque l'administrateur SD-WAN lance un site en vue d'un déploiement à l'aide du processus ZTD, il a la possibilité de pré-authentifier l'appliance à utiliser pour ZTD en remplissant le numéro de série et en initiant une communication par courrier électronique à l'installateur sur site pour commencer l'activité sur site.

Le programme d'installation sur site reçoit une communication électronique indiquant que le site est prêt pour le déploiement sans intervention et peut commencer la procédure d'installation de mise sous tension et de câblage de l'appliance pour l'attribution d'adresse IP DHCP et l'accès Internet sur le port MGMT.En outre, câblage dans tous les ports LAN et WAN.Tout le reste est initié par le service ZTD et la progression est surveillée par l'utilisation de l'URL d'activation. Dans le cas où le nœud distant à installer est une instance de cloud, l'ouverture de l'URL d'activation déclenche le flux de travail pour installer automatiquement l'instance dans l'environnement de cloud désigné, aucune action n'est requise par un programme d'installation local.

Le service cloud de déploiement Zero Touch automatise les actions suivantes :

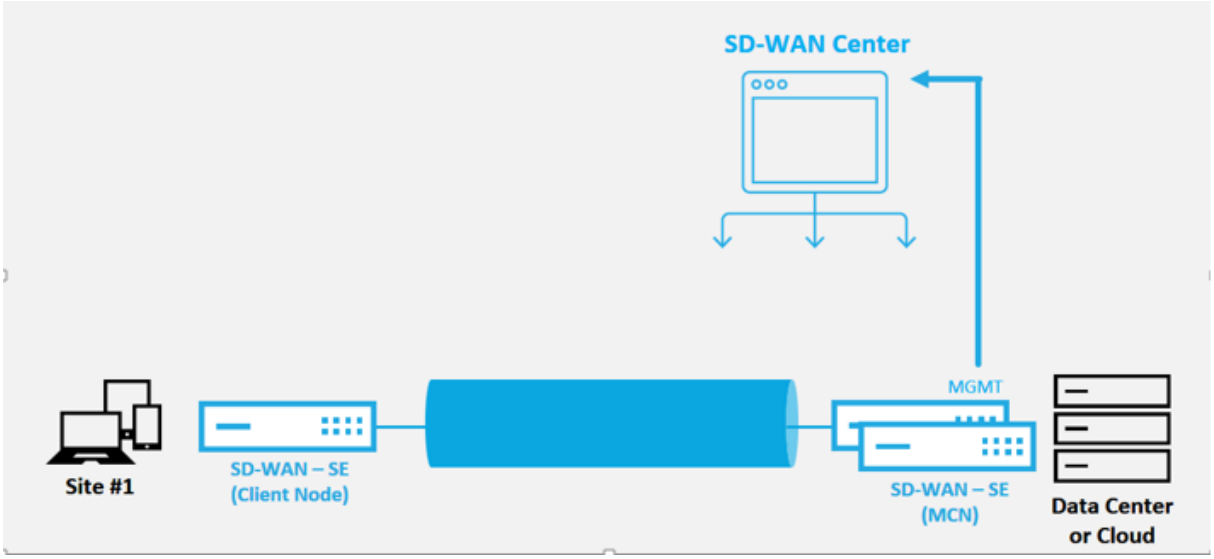
Téléchargez et mettez à jour l'agent ZTD si de nouvelles fonctionnalités sont disponibles sur l'appliance de succursale.

- Authentifiez l'appliance de succursale en validant le numéro de série.
- Authentifiez que l'administrateur SD-WAN a accepté le site pour ZTD à l'aide du SD-WAN Center.
- Extrayez le fichier de configuration spécifique à l'appliance ciblée à partir du SD-WAN Center.
- Poussez le fichier de configuration spécifique à l'appliance ciblée vers l'appliance de branche.
- Installez le fichier de configuration sur le dispositif de branche.
- Poussez tous les composants logiciels SD-WAN manquants ou les mises à jour requises vers l'appliance de succursale.
- Envoie un fichier de licence temporaire de 10 Mbps pour confirmer l'établissement du chemin virtuel vers le dispositif de succursale.
- Activez le service SD-WAN sur le dispositif de succursale.

D'autres étapes sont requises pour l'administrateur SD-WAN pour installer un fichier de licence permanent sur l'appliance.

Procédure du service de déploiement sans intervention

La procédure suivante décrit en détail les étapes requises pour déployer un nouveau site à l'aide du service de déploiement sans intervention.Avoir un MCN en cours d'exécution et un nœud client fonctionnant déjà avec une communication appropriée au SD-WAN Center, ainsi que des chemins virtuels établis confirmant la connectivité sur le réseau de sous-couche. Les étapes suivantes sont requises pour l'administrateur SD-WAN pour lancer le déploiement sans intervention :



Comment configurer le service de déploiement sans intervention

Le SD-WAN Center dispose de la fonctionnalité permettant d'accepter les demandes de connexion des appliances nouvellement connectées au réseau SD-WAN Enterprise. La demande est transmise à l'interface Web via le service de déploiement Zero Touch. Une fois l'appliance connectée au service, les packages de configuration et de mise à niveau logicielle sont téléchargés.

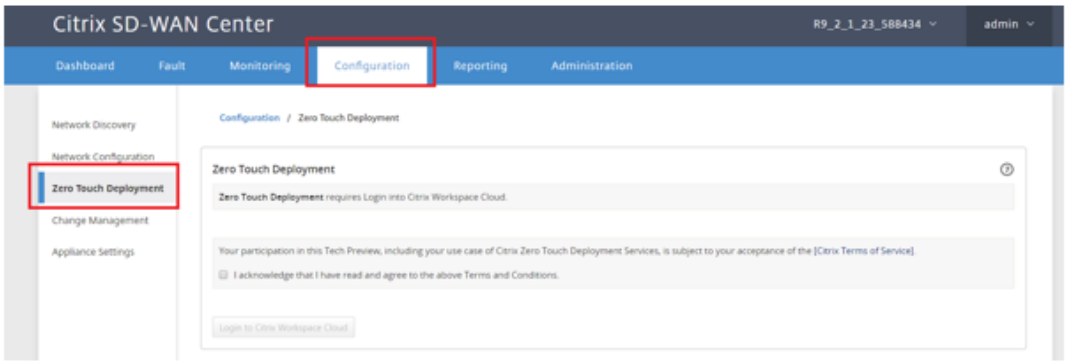
Workflow de configuration :

- Accédez à SD-WAN Center**** > ****Créer une configuration de site** ou Importer une configuration existante et enregistrez-le.
- Connectez-vous à Citrix Workspace Cloud pour activer le service ZTD. L'option de menu Déploiement sans intervention s'affiche désormais dans l'interface de gestion Web du SD-WAN Center.
- Dans SD-WAN Center, accédez à **Configuration** > **Zero Touch Deployment** > **Deploy New Site**.
- Sélectionnez une solution matérielle-logicielle, cliquez sur Activer, puis sur**Déployer**.
- Le programme d'installation reçoit un e-mail d'activation > Entrez le numéro de série > **Activer** > Appliance est déployée avec succès.

Pour configurer le service de déploiement sans intervention :

1. Installez SD-WAN Center avec les fonctionnalités de déploiement sans intervention activées.
    a) Installez SD-WAN Center avec l'adresse IP attribuée par DHCP.
    b) Vérifiez que SD-WAN Center attribue une adresse IP de gestion appropriée et une adresse DNS réseau avec une connectivité à l'Internet public sur le réseau de gestion.
    c) Mettez à niveau le SD-WAN Center vers la dernière version du logiciel SD-WAN.

d) Avec une connectivité Internet appropriée, le SD-WAN Center lance le Zero Touch Deployment (ZTD) Cloud Service et télécharge et installe automatiquement toutes les mises à jour du firmware spécifiques à ZTD. Si cette procédure d'appel échoue, l'option de déploiement sans intervention suivante ne sera pas disponible dans l'interface graphique graphique.



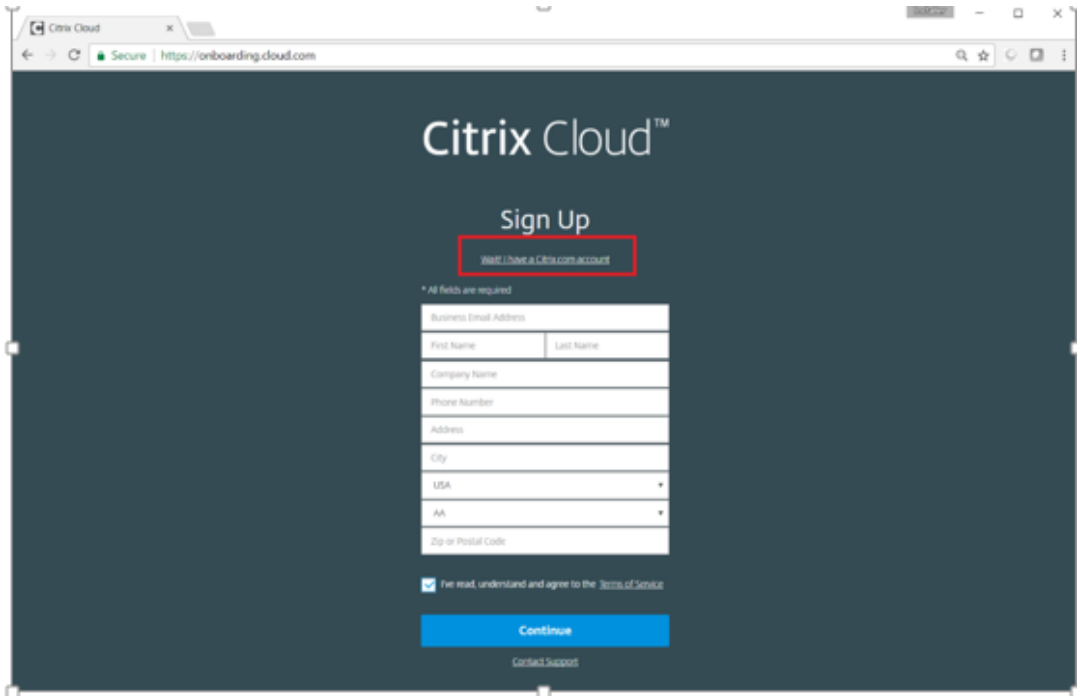
e) Lisez les Conditions générales, puis sélectionnez « **Je reconnais avoir lu et accepté les Conditions générales ci-dessus** ».

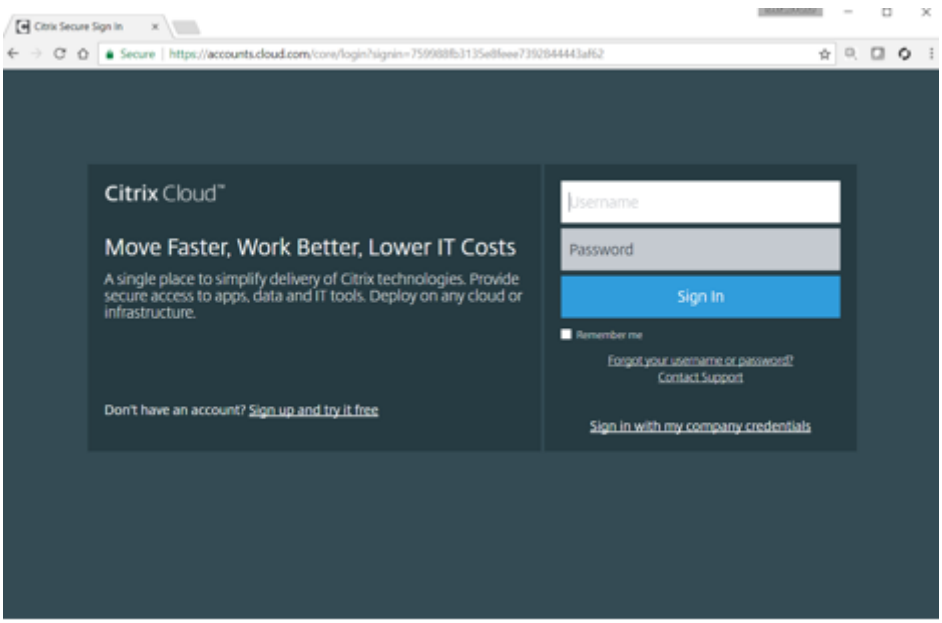
f) Cliquez sur le bouton « **Connexion à Citrix Workspace Cloud** » si un compte Citrix Cloud a déjà été créé.

g) Connectez-vous au compte Citrix Cloud et, après avoir reçu le message suivant de connexion réussie, **VEUILLEZ NE PAS FERMER CETTE FENÊTRE, LE PROCESSUS NÉCESSITE ENVIRON 20 SECONDES SUPPLÉMENTAIRES POUR QUE L'INTERFACE GRAPHIQUE DU SD-WAN CENTER SOIT ACTUALISÉE.** La fenêtre doit se fermer toute seule une fois qu'elle est terminée.**

h) Pour créer un compte Cloud Login, suivez la procédure ci-dessous :

- Ouvrez un navigateur Web à l'adresse https://onboarding.cloud.com
- Cliquez sur le lien « **Wait, I have a Citrix.com account** ».





i) Connectez-vous avec un compte Citrix existant.

j) Une fois connecté à la page SD-WAN Center Zero Touch Deployment, vous pouvez remarquer qu'aucun site n'est disponible pour le déploiement ZTD pour les raisons suivantes :

- La configuration active n'a pas été sélectionnée dans le menu déroulant Configuration
- Tous les sites de la configuration active actuelle ont déjà été déployés
- La configuration n'a pas été construite à l'aide du SD-WAN Center, mais plutôt de l'Éditeur de configuration disponible sur le MCN

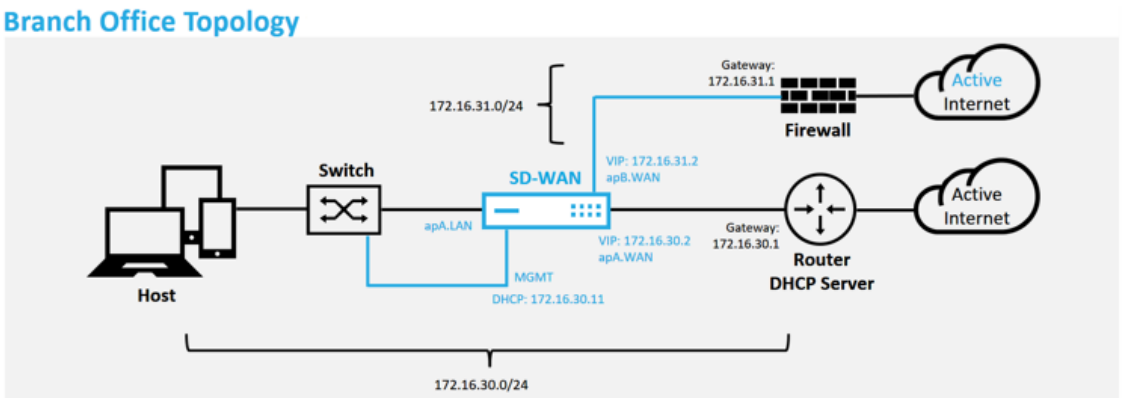
- Les sites n'ont pas été intégrés dans la configuration référençant des appliances compatibles zéro touch (p. ex. 410-SE, 2100-SE, Cloud VPX)

2. Mettez à jour la configuration pour ajouter un **nouveau site distant** avec une **appliance SD-WAN compatible ZTD** à l'aide de la configuration réseau SD-WAN Center.

   Si la configuration SD-WAN n'a pas été créée à l'aide de la configuration réseau SD-WAN Center, importez la configuration active à partir du MCN et commencez à modifier la configuration à l'aide du SD-WAN Center. Pour bénéficier de la fonctionnalité de déploiement Zero Touch, l'administrateur SD-WAN doit créer la configuration à l'aide de SD-WAN Center.La procédure suivante doit être utilisée pour ajouter un nouveau site ciblé pour le déploiement sans intervention.

   Concevez le nouveau site pour le déploiement de l'appliance SD-WAN en décrivant d'abord les détails du nouveau site (c'est-à-dire le modèle d'appliance, l'utilisation des groupes d'interface, les adresses IP virtuelles, les liens WAN avec la bande passante et leurs passerelles respectives).

   > **Important**
   >
   > Vous pouvez remarquer tout nœud de site sur lequel VPX est sélectionné car le modèle est également répertorié, mais actuellement la prise en charge de ZTD n'est disponible que pour l'instance AWS VPX.
   >
   > **Remarque**
   >
   > - Assurez-vous que vous utilisez un navigateur Web de support pour Citrix SD-WAN Center
   > - Assurez-vous que le navigateur Web ne bloque pas les fenêtres contextuelles pendant la connexion à Citrix Workspace

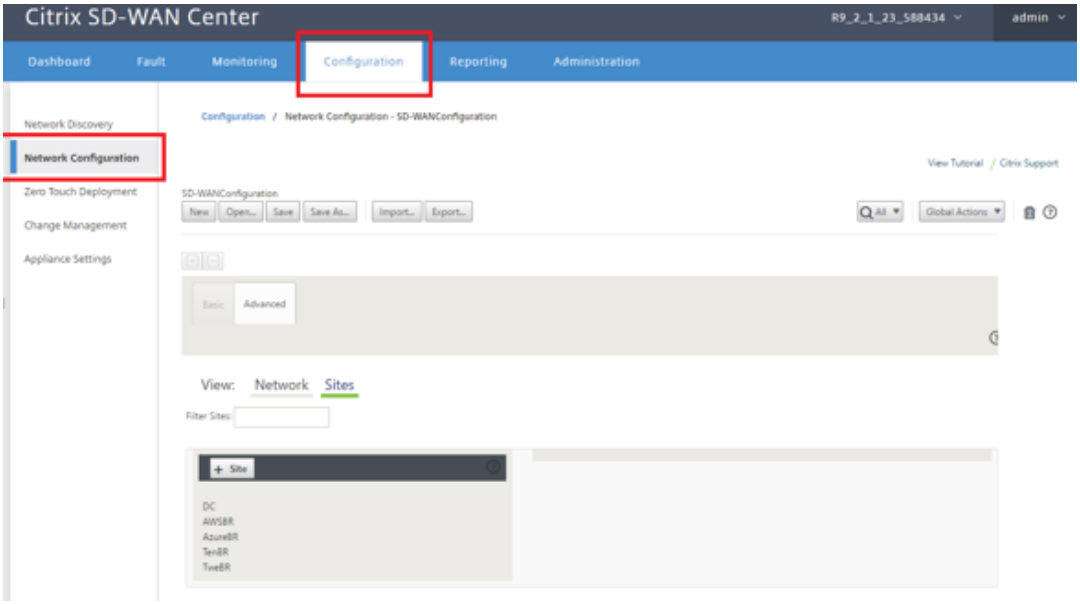
   Il s'agit d'un exemple de déploiement d'un site de succursale, l'appliance SD-WAN est déployée physiquement dans le chemin de la liaison WAN MPLS existante sur un réseau 172.16.30.0/24, et à l'aide d'une liaison de sauvegarde existante en l'activant dans un état actif et en mettant fin à cette deuxième liaison WAN directement dans l'appliance SD-WAN sur un sous-réseau différent 172.16.31.0/24.

Remarque

Les appliances SD-WAN attribuent automatiquement une adresse IP par défaut 192.168.100.1/16.Lorsque DHCP est activé par défaut, le serveur DHCP du réseau peut fournir à l'appliance une deuxième adresse IP dans un sous-réseau qui chevauche la valeur par défaut.Cela peut entraîner un problème de routage sur l'appliance où l'appliance risque de ne pas se connecter au service cloud ZTD. Configurez le serveur DHCP pour qu'il attribue des adresses IP en dehors de la plage 192.168.0.0/16.

Différents modes de déploiement sont disponibles pour le placement de produits SD-WAN dans un réseau. Dans l'exemple ci-dessus, le SD-WAN est déployé comme superposition au-dessus de l'infrastructure réseau existante.Pour les nouveaux sites, les administrateurs SD-WAN peuvent choisir de déployer le SD-WAN en mode Edge ou Passerelle, éliminant ainsi le besoin d'un routeur et d'un pare-feu périphérique WAN et consolidant les besoins réseau en matière de routage périphérique et de pare-feu sur la solution SD-WAN.

a) Ouvrez l'**interface de gestion Web SD-WAN Center** et accédez à la page **Configuration** > **Configuration réseau** .

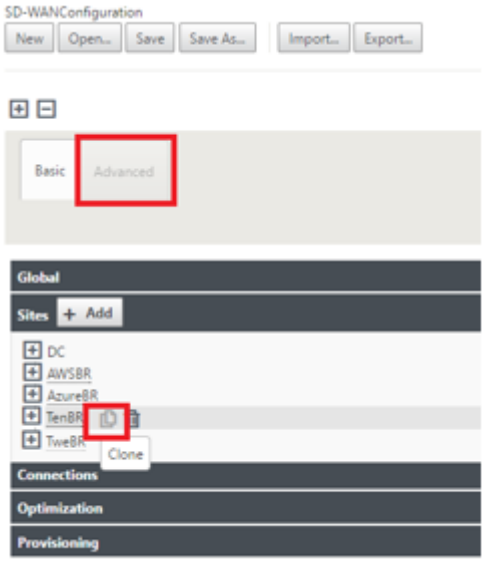


b) Assurez-vous qu'une configuration opérationnelle est déjà en place ou importez la configuration à partir du MCN.

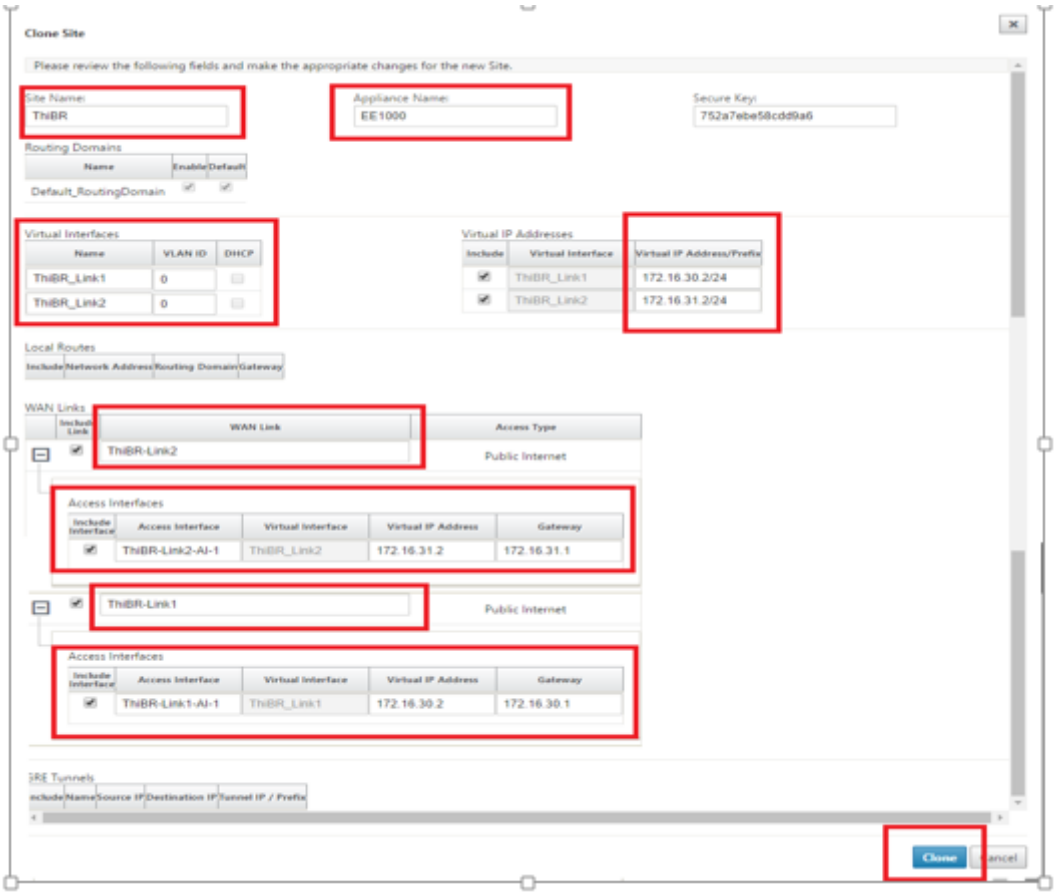
c) Accédez à l'onglet Avancé pour créer un site.

d) Ouvrez la vignette Sites pour afficher les sites actuellement configurés.

e) Construit rapidement la configuration du nouveau site en utilisant la fonctionnalité de clone de n'importe quel site existant.

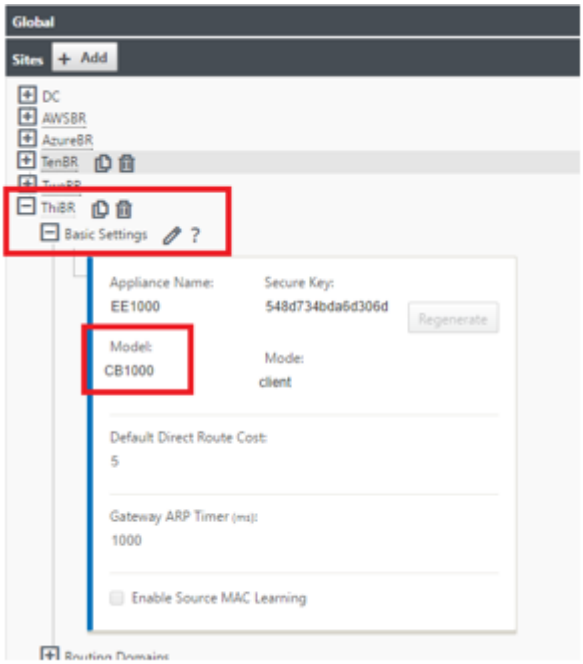


f) Remplissez tous les champs requis à partir de la topologie conçue pour ce nouveau site de succursale



g) Après le clonage d'un nouveau site, accédez aux **paramètres de base**du site et vérifiez que le modèle de SD-WAN est correctement sélectionné pour prendre en charge le service

sans intervention.



h) Le modèle SD-WAN du site peut être mis à jour, mais n'oubliez pas que les groupes d'interface peuvent devoir être redéfinis car l'appliance mise à jour peut avoir une nouvelle disposition d'interface, puis celle utilisée pour cloner.

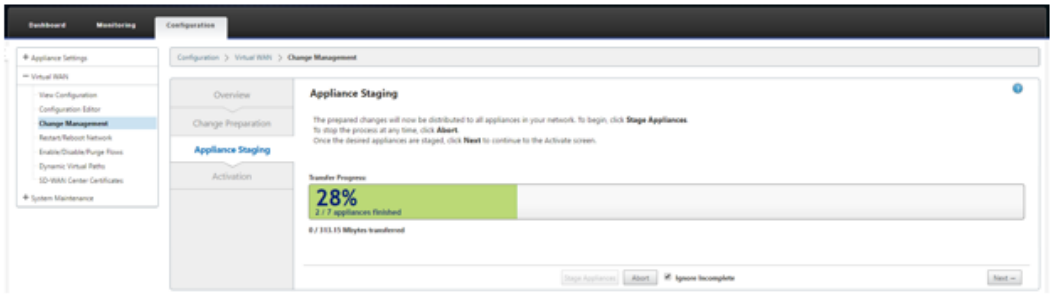
i) Enregistrez la nouvelle configuration sur SD-WAN Center et utilisez l'exportation vers l'option « **Change Management Inbox** » pour pousser la configuration à l'aide de Change Management.

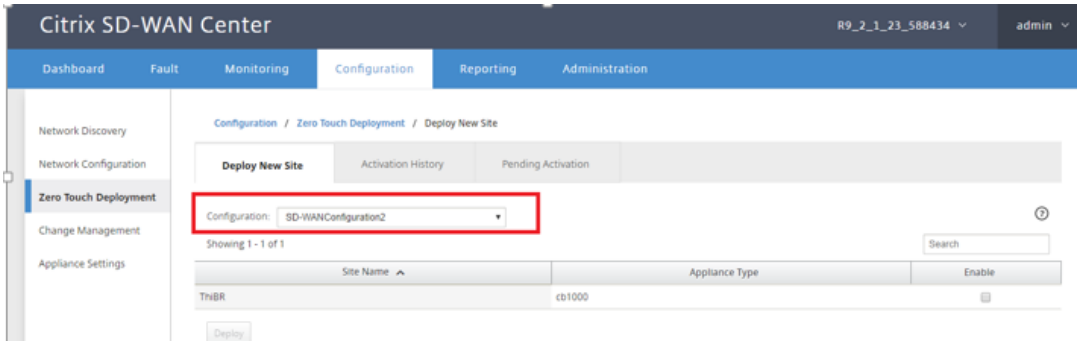
j) Suivez la procédure de gestion des modifications pour organiser correctement la nouvelle configuration, ce qui rend les périphériques SD-WAN existants conscients du nouveau site à déployer via le bouton zéro, vous devez utiliser l'option « Ignorer incomplet » pour ignorer la tentative de pousser la configuration vers le nouveau site qui doit encore aller via le flux de travail ZTD.

3. Revenez à la page SD-WAN Center Zero Touch Deployment et lorsque la nouvelle configuration active est en cours d'exécution, le nouveau site est disponible pour le déploiement.

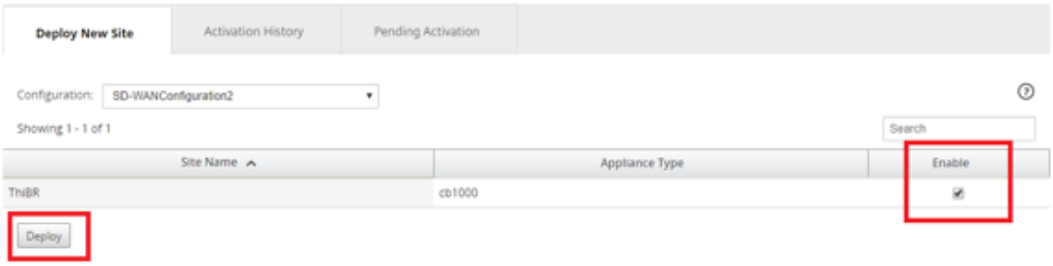
   a) Dans la page Déploiement sans intervention, sous l'onglet **Déployer un nouveau site**, sélectionnez le fichier de configuration réseau en cours d'exécution

   b) Une fois que le fichier de configuration en cours d'exécution est sélectionné, la liste de tous les sites de succursales avec des périphériques SD-WAN non déployés qui sont pris en charge pour la touche zéro s'affiche

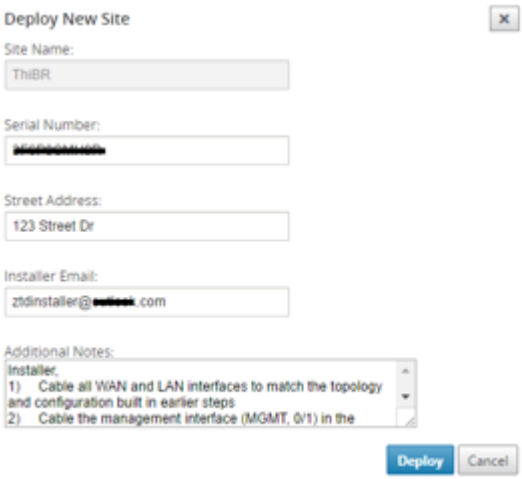




c) Sélectionnez les sites de succursale que vous souhaitez configurer pour le service Zero Touch, cliquez sur **Activer**, puis sur **Déployer**.



d) Une fenêtre contextuelle Déployer un nouveau site s'affiche, dans laquelle l'administrateur peut fournir le numéro de série, l'adresse postale du site de la succursale, l'adresse e-mail du programme d'installation et d'autres notes, si nécessaire.

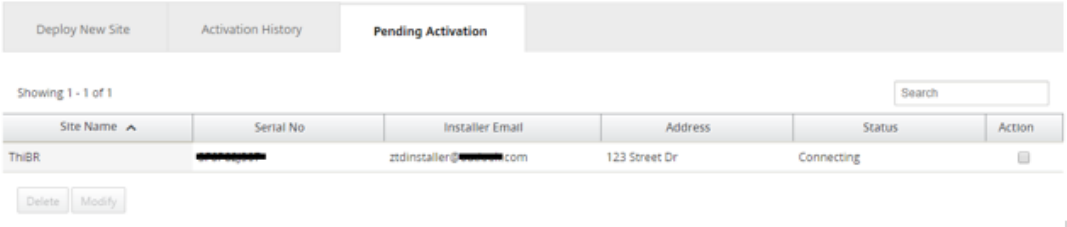


> **Remarque**
>
> Le champ de saisie du numéro de série est facultatif et, selon qu'il est renseigné ou non, entraînera une modification de l'activité sur site dont le programme d'installation est responsable.
>
> - Si le champ Numéro de série est renseigné : le programme d'installation n'est pas tenu d'entrer le numéro de série dans l'URL d'activation générée à l'aide de la commande deploy site
> - Si le champ Numéro de série est laissé noir : le programme d'installation est responsable de la saisie du numéro de série correct de l'appliance dans l'URL d'activation générée à l'aide de la commande deploy site

a) Après avoir cliqué sur le bouton **Déployer**, un message s'affiche indiquant que la configuration du site a été déployée.

b) Cette action déclenche SD-WAN Center, précédemment enregistré auprès du Service Cloud ZTD, de partager la configuration de ce site particulier pour qu'il soit temporalité stockée dans le Service Cloud ZTD.

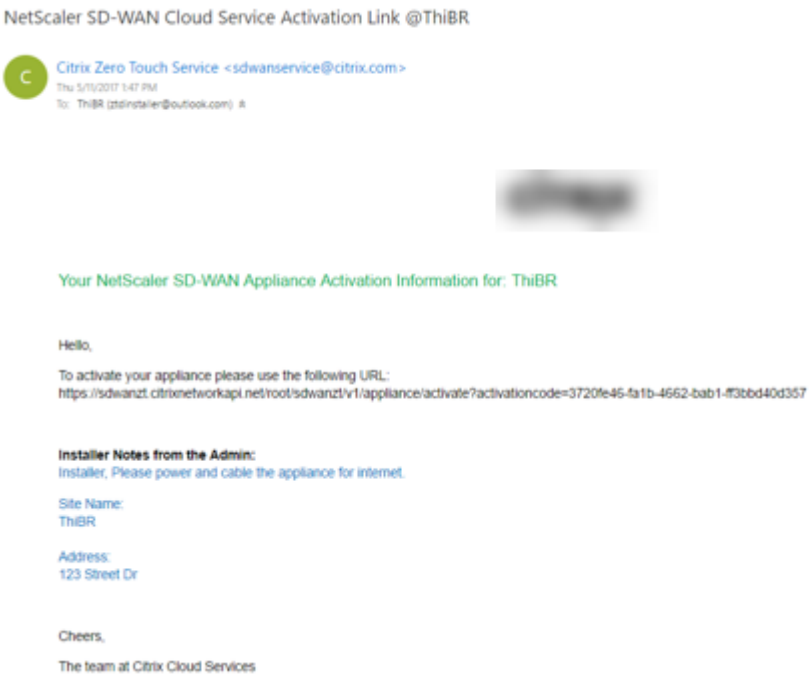
c) Accédez à l'onglet Activation en attente pour confirmer que les informations du site de succursale ont été remplies avec succès et ont été placées dans un état d'activité d'installation en attente.



> **Remarque**
>
> Un déploiement sans intervention dans l'état Activation en attente peut éventuellement être choisi pour Supprimer ou Modifier, si les informations sont incorrectes. Si un site est supprimé de la page d'activation en attente, il devient disponible pour être déployé dans la page de l'onglet Déployer un nouveau site. Une fois que vous choisissez de supprimer le site de la succursale de En attente d'activation, le lien d'activation envoyé au programme d'installation devient invalide.
>
> Si le champ Numéro de série n'a pas été renseigné par l'administrateur SD-WAN, le champ Statut indique « En attente du programme d'installation » au lieu de « Connexion ».

4. La prochaine série d'activités est effectuée par le programme d'installation sur site.

   a) Le programme d'installation vérifie dans la boîte aux lettres l'adresse e-mail utilisée par l'administrateur SD-WAN lors du déploiement du site.


NetScaler SD-WAN Cloud Service Activation Link @ThiBR

Citrix Zero Touch Service <sdwanservice@citrix.com>

Your NetScaler SD-WAN Appliance Activation Information for: ThiBR

Hello,

To activate your appliance please use the following URL:
https://sdwanzt.citrixnetworkapi.net/root/sdwanzt/v1/appliance/activate?activationcode=3720fe46-fa1b-4662-bab1-ff3bbd40d357

Installer Notes from the Admin:
Installer, Please power and cable the appliance for internet.

Site Name:
ThiBR

Address:
123 Street Dr

Cheers,

The team at Citrix Cloud Services

   b) Ouvrez l'URL d'activation du déploiement sans intervention dans une fenêtre de navigateur Internet.

   c) Si l'administrateur SD-WAN n'a pas prérenseigné le numéro de série à l'étape du site de déploiement, le programme d'installation est chargé de localiser le numéro de série sur l'appliance physique et d'entrer le numéro de série manuellement dans l'URL d'activation, puis de cliquer sur le bouton **Activer** .

d) Si l'administrateur préremplit les informations du numéro de série, l'URL d'activation aura déjà progressé à l'étape suivante.

e) Le programme d'installation doit être physiquement sur place pour effectuer les actions suivantes :

- Câblage de toutes les interfaces WAN et LAN pour qu'elles correspondent à la topologie et à la configuration construites lors des étapes précédentes.
- Câblage de l'interface de gestion (MGMT, 0/1) dans le segment du réseau qui fournit l'adresse IP DHCP et la connectivité à Internet avec la résolution DNS et FQDN vers adresse IP.
- Câble d'alimentation de l'appliance SD-WAN.
- Allumez l'interrupteur d'alimentation de l'appliance.

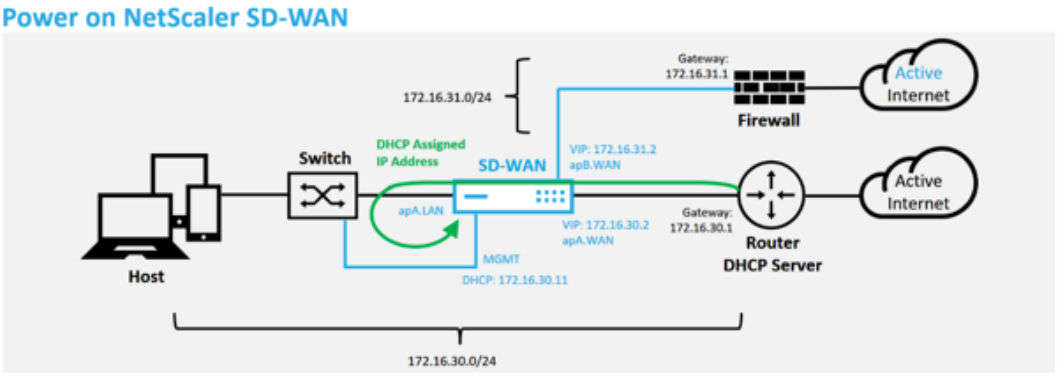
> **Remarque**
>
> La plupart des appareils s'allument automatiquement lorsque le câble d'alimentation est connecté.Certains appareils peuvent devoir être mis sous tension à l'aide du commutateur d'alimentation situé à l'avant de l'appliance, tandis que d'autres peuvent avoir l'interrupteur d'alimentation à l'arrière de l'appliance.Certains interrupteurs d'alimentation nécessitent de maintenir le bouton d'alimentation jusqu'à ce que l'appareil se mette sous tension.

5. La série d'étapes suivante est automatisée à l'aide du service déploiement sans intervention, mais nécessite que les conditions préalables suivantes soient disponibles.

- L'appliance de succursale doit être mise sous tension
- DHCP doit être disponible dans le réseau existant pour attribuer une adresse IP de gestion et DNS

- Toute adresse IP assignée DHCP nécessite une connectivité à Internet avec la possibilité de résoudre les noms de domaine complets
- L'attribution IP peut être configurée manuellement, à condition que les autres conditions préalables soient remplies

a) l'appliance obtient une adresse IP à partir du serveur DHCP des réseaux, dans cet exemple de topologie, elle est obtenue via les interfaces de données contournées d'un dispositif d'état par défaut d'usine.

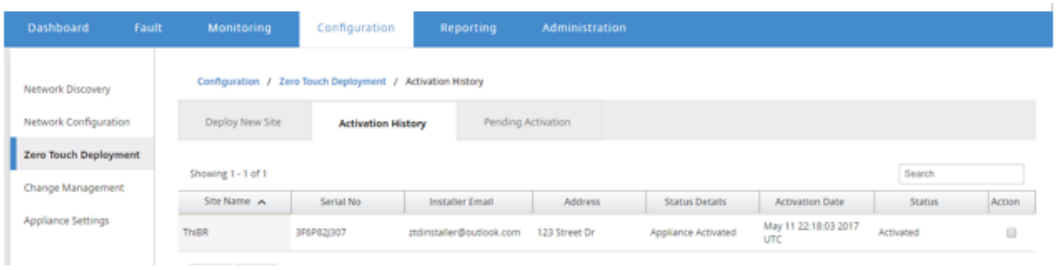


b) Lorsque l'appliance obtient la gestion Web et les adresses IP DNS du serveur DHCP du réseau de sous-couche, elle lance le service de déploiement sans intervention et télécharge toutes les mises à jour logicielles associées à ZTD.

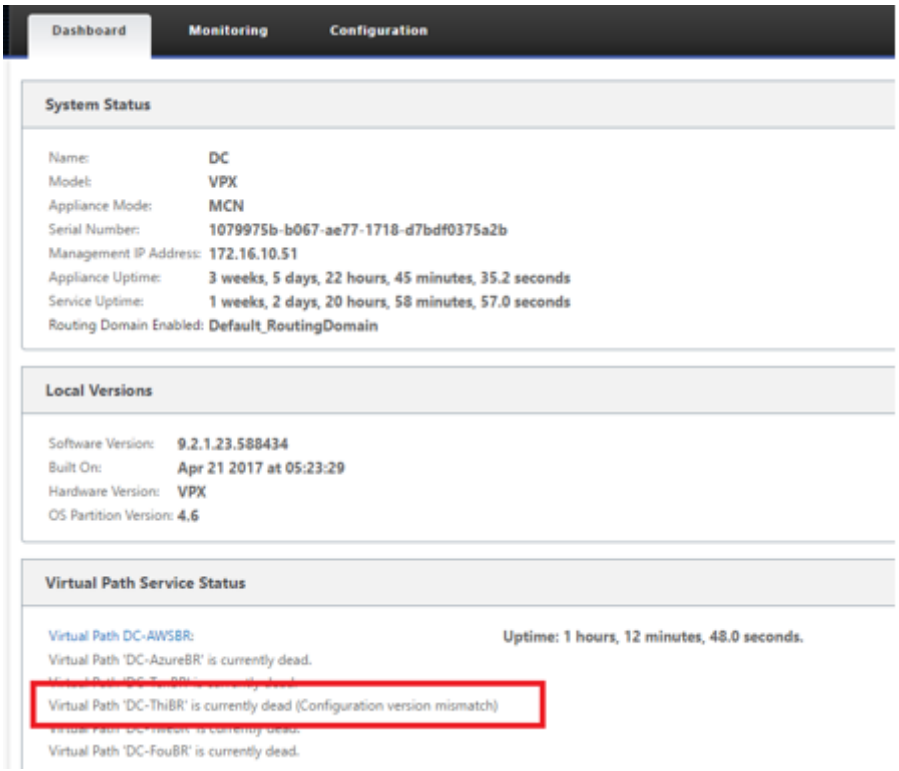
c) Avec une connectivité réussie au service cloud ZTD, le processus de déploiement effectue automatiquement les opérations suivantes :

- Télécharger le fichier de configuration stocké précédemment par le SD-WAN Center
- Application de la configuration à l'appliance locale
- Télécharger et installer un fichier de licence temporaire de 10 Mo
- Téléchargez et installez les mises à jour logicielles si nécessaire
- Activer le service SD-WAN

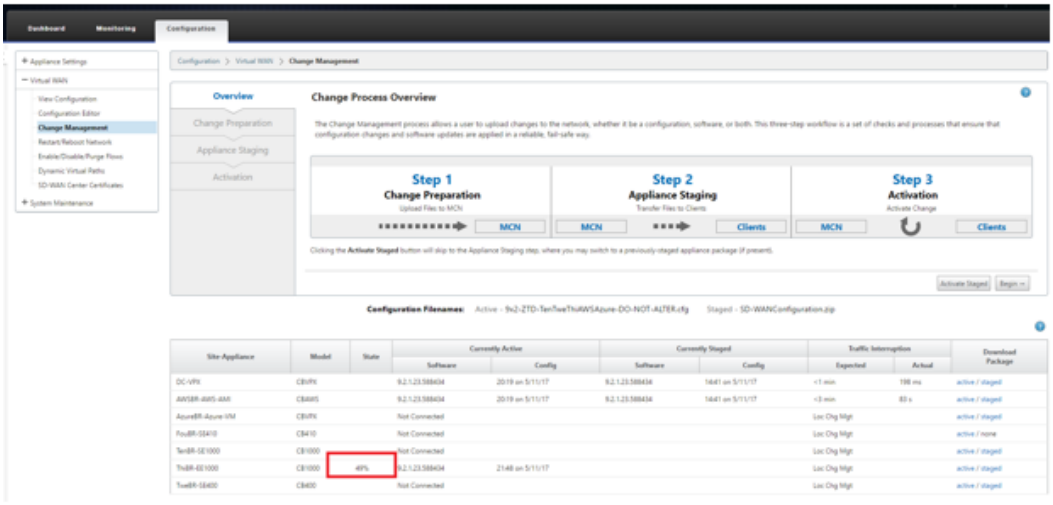
d) Une confirmation supplémentaire peut être effectuée dans l'interface de gestion Web SD-WAN Center, le menu Déploiement zéro tactile affiche les appliances activées avec succès dans l'onglet **Historique d'activation** .



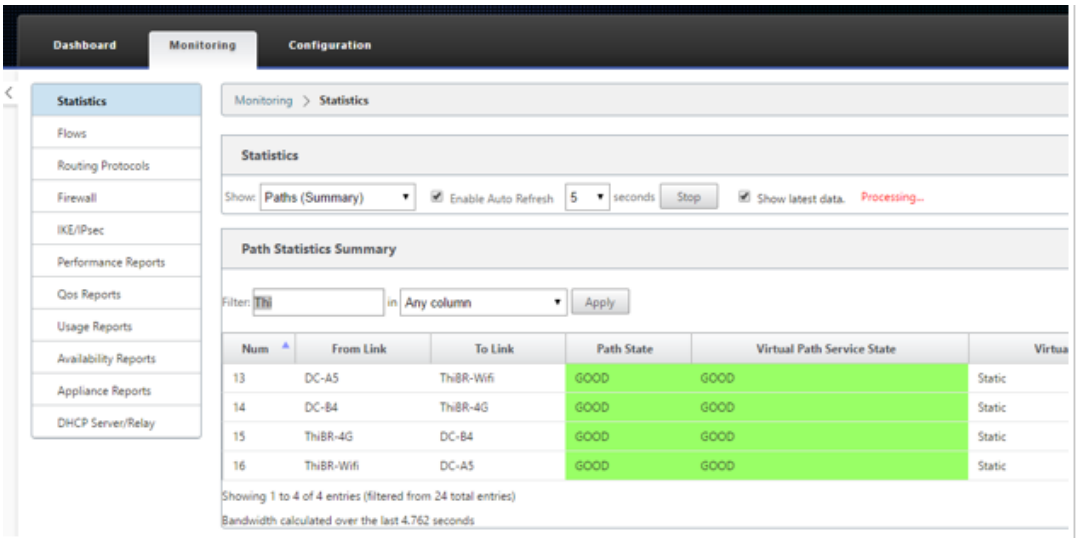
e) Les chemins virtuels peuvent ne pas s'afficher immédiatement dans un état connecté car le MCN peut ne pas approuver la configuration transmise par le service Cloud ZTD et signale une « incompatibilité de version de configuration » dans le tableau de bord MCN.



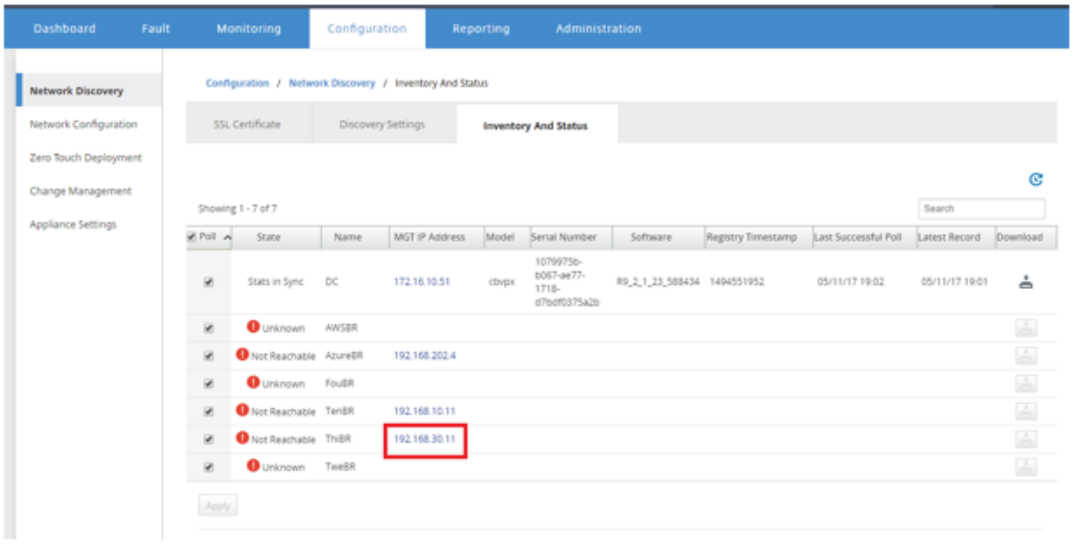
f) La configuration est redistribuée à l'appliance de filiale nouvellement installée et l'état est surveillé sur la page **MCN** > **Configuration** > **Virtual WAN** > **Change Management** (ce processus peut prendre plusieurs minutes).



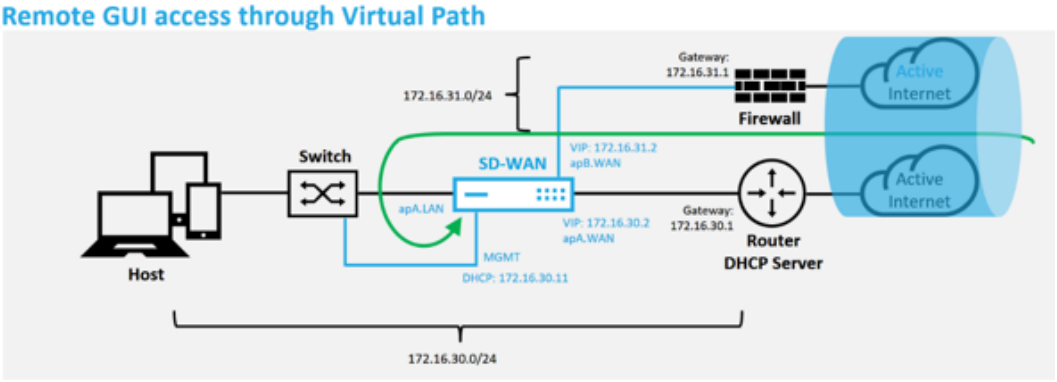
g) L'administrateur SD-WAN peut surveiller la page de gestion Web MCN tête de ligne pour les chemins virtuels établis du site distant.



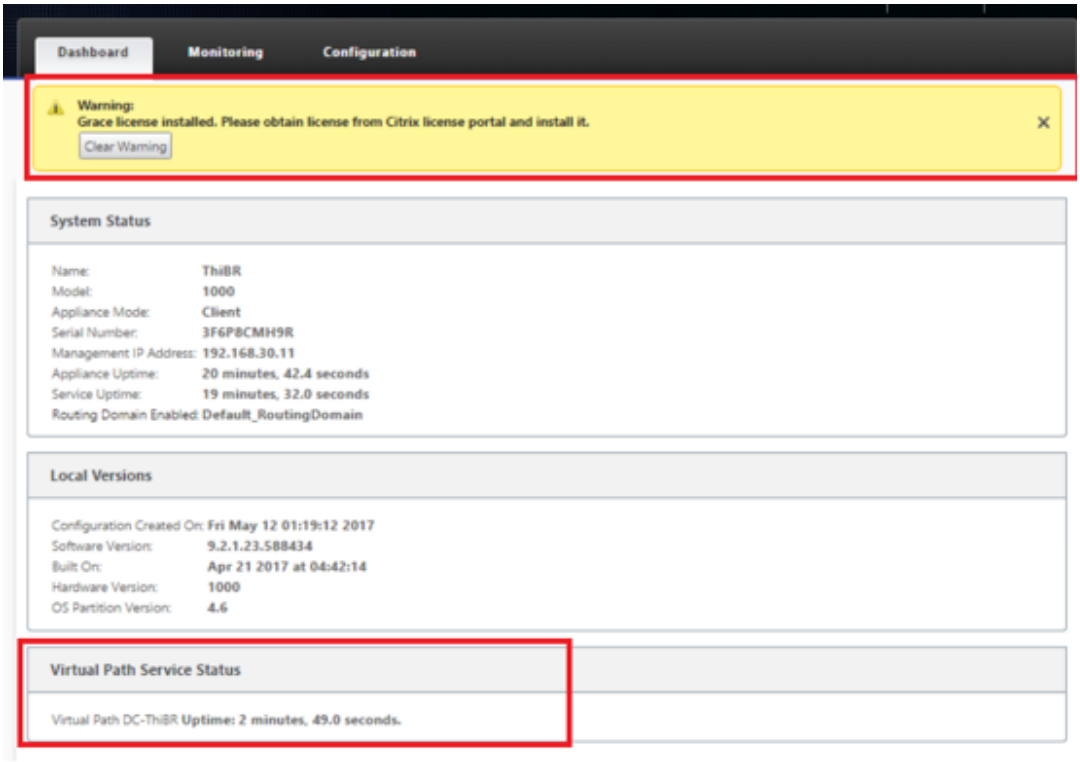
h) Le SD-WAN Center peut également être utilisé pour identifier l'adresse IP attribuée par DHCP de l'appliance sur site à partir de la page **Configuration** > **Découverte du réseau** > **Inventaire et état** .



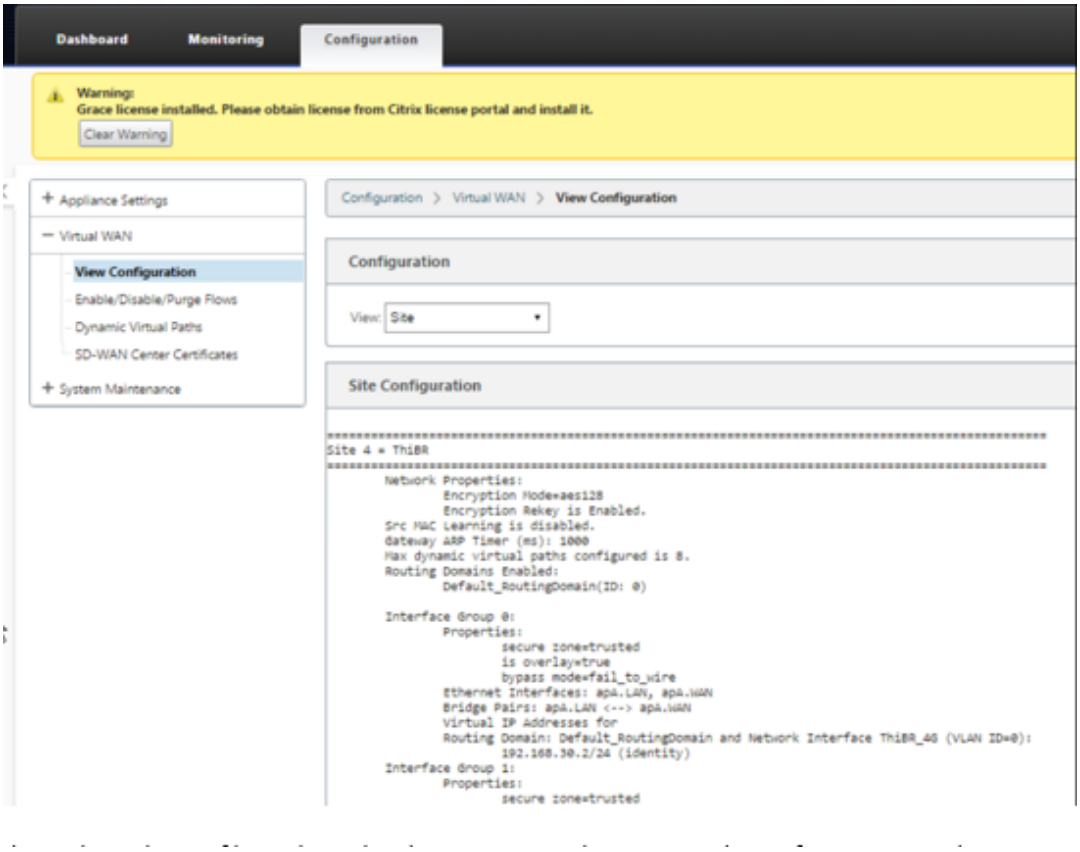
i) À ce stade, l'administrateur réseau SD-WAN peut accéder à la gestion Web à l'appliance sur site en utilisant le réseau de superposition SD-WAN.



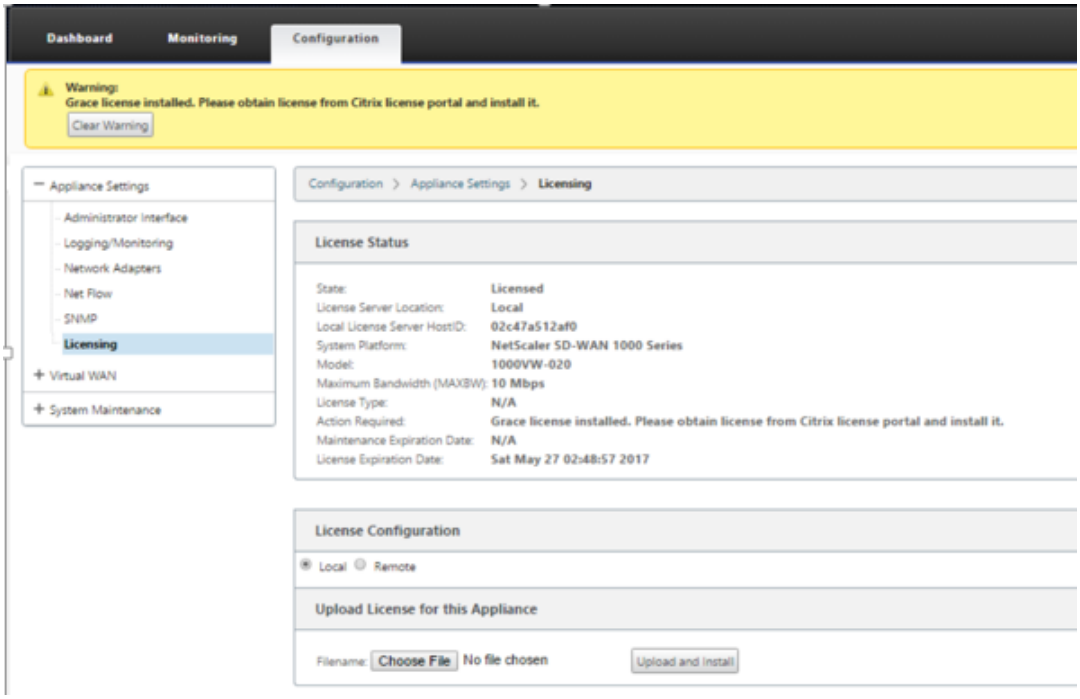
j) L'accès de gestion Web à l'appliance de site distant indique que l'appliance a été installée avec une licence Grace temporaire à 10 Mbit/s, ce qui permet à l'état du service Virtual Path de déclarer actif.



k) La configuration de l'appliance peut être validée à l'aide de la page **Configuration** > **Virtual WAN** > **Afficher la configuration** .



l) Le fichier de licence de l'appliance peut être mis à jour vers une licence permanente à l'aide de la page **Configuration** > **Paramètres de l'appliance** > **Licences** .



m) Après avoir téléchargé et installé le fichier de licence permanente, la bannière d'avertisse-

ment Grace License disparaît et pendant le processus d'installation de licence, aucune perte de connectivité au site distant ne se produira (aucun ping n'est supprimé).

Installation locale sans intervention

February 17, 2022

Pour obtenir des instructions sur le déploiement d'une appliance SD-WAN avec le service Zero Touch, consultez la rubrique Comment configurer le service de déploiement Zero Touch.

AWS

February 17, 2022

Déploiement dans AWS

Avec SD-WAN version 9.3, les capacités de déploiement sans intervention ont été étendues aux instances Cloud.La procédure de déploiement du processus de déploiement sans intervention quatre instances de cloud diffère légèrement du déploiement de l'appliance pour le service sans intervention.

1. Mettez à jour la configuration pour ajouter un nouveau site distant avec un périphérique cloud SD-WAN compatible ZTD à l'aide de la configuration réseau SD-WAN Center.

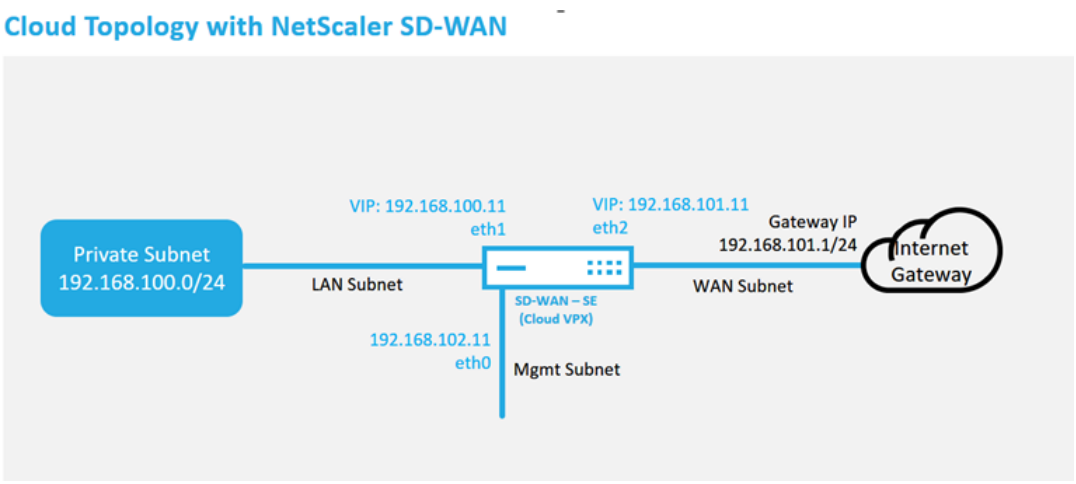
   Si la configuration SD-WAN n'a pas été créée à l'aide de la configuration réseau SD-WAN Center, importez la configuration active à partir du MCN et commencez à modifier la configuration à l'aide du SD-WAN Center.Pour la capacité de déploiement sans intervention, l'administrateur SD-WAN doit créer la configuration à l'aide du SD-WAN Center.La procédure suivante doit être utilisée pour ajouter un nouveau nœud de cloud destiné au déploiement sans intervention.

   a) Concevez le nouveau site pour le déploiement du cloud SD-WAN en décrivant d'abord les détails du nouveau site (taille VPX, utilisation des groupes d'interface, adresses IP virtuelles, lien(s) WAN avec bande passante et passerelles respectives).

   > **Remarque**
   >
   > - Les instances SD-WAN déployées dans le cloud doivent être déployées en mode Edge/Gateway.
   > - Le modèle pour l'instance de cloud est limité à trois interfaces : Gestion, LAN et

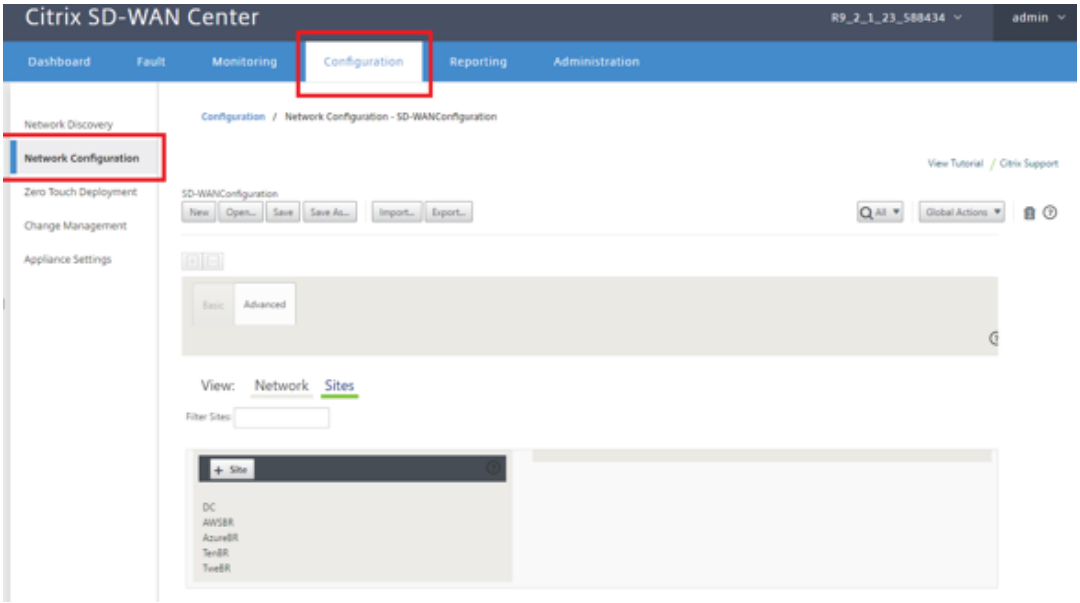
WAN (dans cet ordre).

- Les modèles de cloud disponibles pour SD-WAN VPX sont actuellement définis pour obtenir l'adresse IP #.#.#.#.11 des sous-réseaux disponibles dans le VPC.



Il s'agit d'un exemple de déploiement d'un site cloud SD-WAN déployé, le périphérique Citrix SD-WAN est déployé en tant que périphérique desservant une seule liaison WAN Internet dans ce réseau cloud.Les sites distants seront en mesure d'exploiter plusieurs liaisons WAN Internet distinctes se connectant à cette même passerelle Internet pour le cloud, offrant ainsi une résilience et une connectivité de bande passante agrégée à partir de n'importe quel site de déploiement SD-WAN vers l'infrastructure cloud.Cela fournit une connectivité rentable et hautement fiable au cloud.

b) Ouvrez l'interface de gestion Web SD-WAN Center et accédez à la page **Configuration** > **Configuration réseau**.

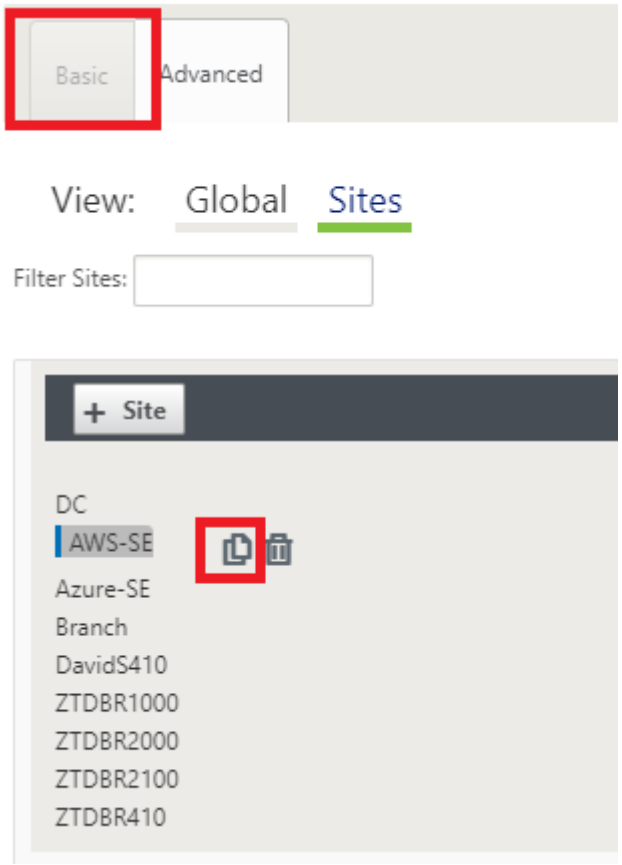


c) Assurez-vous qu'une configuration opérationnelle est déjà en place ou importez la configuration à partir du MCN.

d) Accédez à l'onglet Basic pour créer un nouveau site.

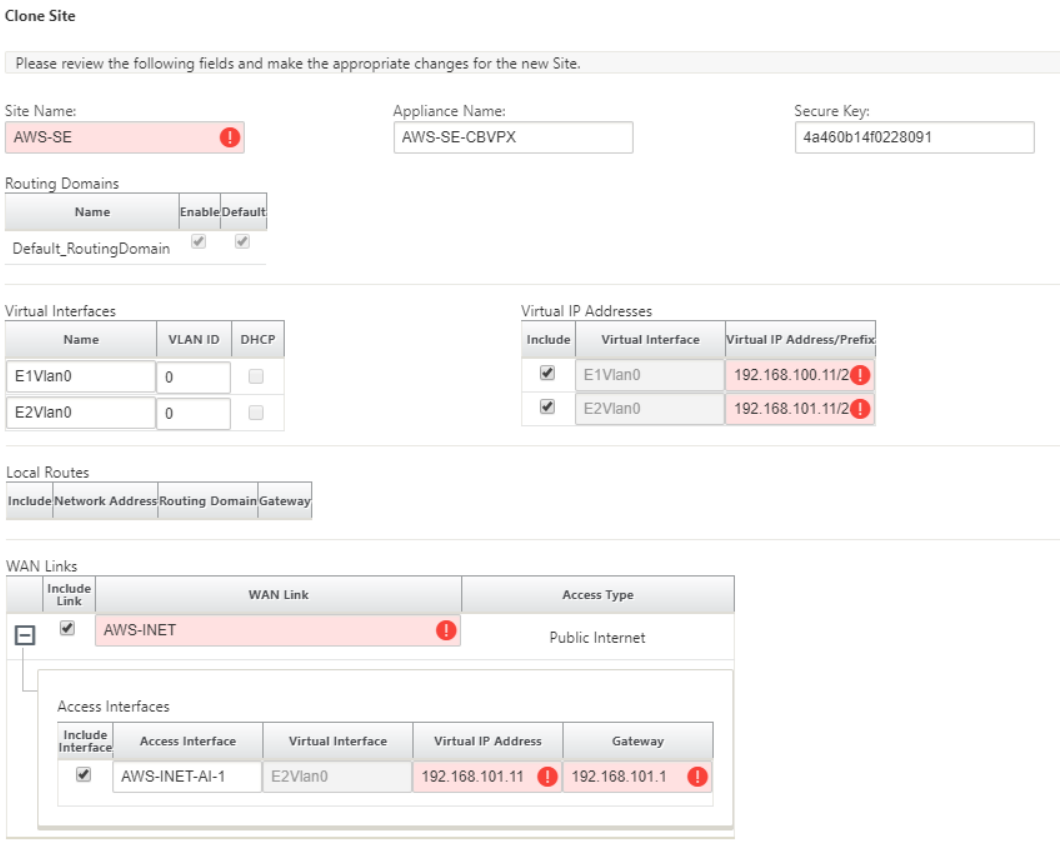
e) Ouvrez la vignette Sites pour afficher les sites actuellement configurés.

f) Créez rapidement la configuration du nouveau site cloud en utilisant la fonction de clonage de n'importe quel site existant ou créez manuellement un nouveau site.

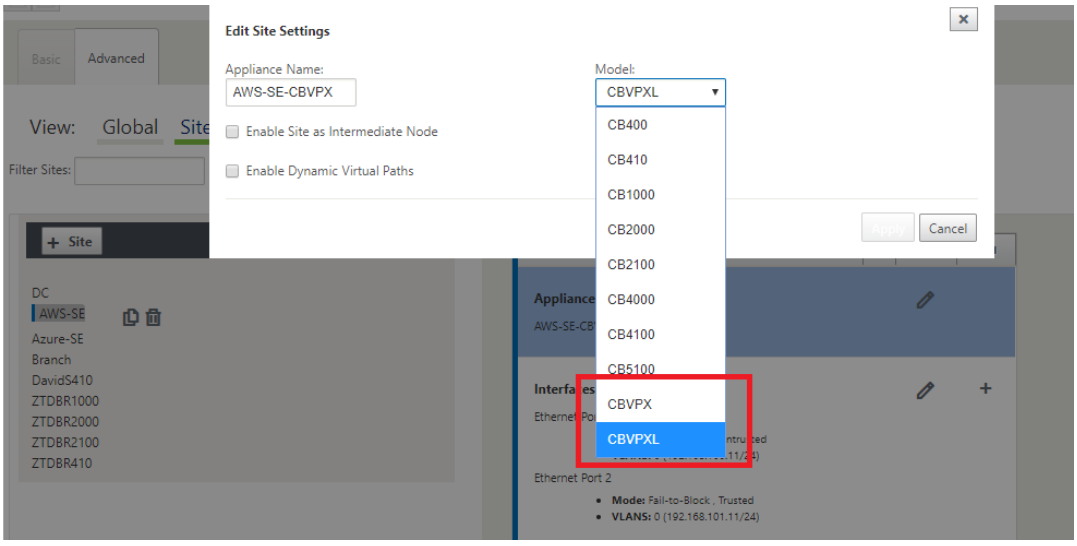


g) Remplissez tous les champs requis à partir de la topologie conçue précédemment pour ce nouveau site cloud

N'oubliez pas que le modèle disponible pour les déploiements ZTD cloud est configuré pour utiliser l'adresse IP #. #.#.11 pour les sous-réseaux Mgmt, LAN et WAN.Si la configuration n'est pas définie pour correspondre à l'adresse d'hôte IP .11 attendue pour chaque interface, le périphérique ne sera pas en mesure d'établir correctement ARP vers les passerelles d'environnement cloud et la connectivité IP au chemin virtuel du MCN.

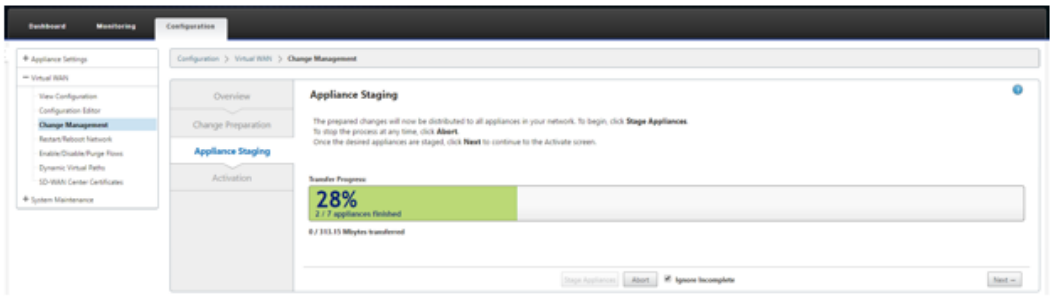


h) Après le clonage d'un nouveau site, accédez aux **paramètres de base**du site et vérifiez que le modèle de SD-WAN est correctement sélectionné pour prendre en charge le service sans intervention.



i) Enregistrez la nouvelle configuration sur SD-WAN Center et utilisez l'exportation vers l'option « **Change Management Inbox** » pour pousser la configuration à l'aide de Change Management.

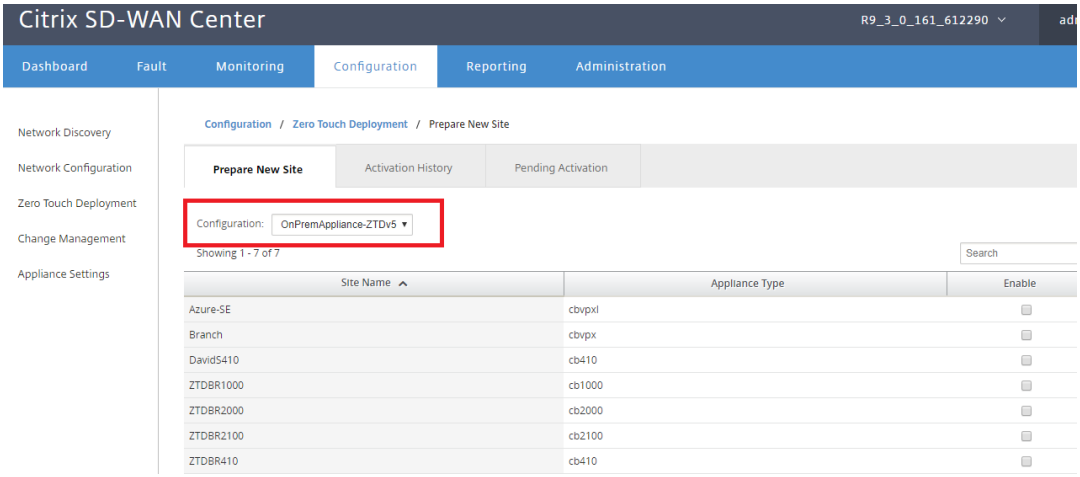
j) Suivez la procédure de gestion des modifications pour organiser correctement la nouvelle configuration, ce qui rend les périphériques SD-WAN existants conscients du nouveau site à déployer via le bouton zéro, vous devrez utiliser l'option « *Ignorer incomplet* » *pour ignorer*la tentative de pousser la configuration vers le nouveau site qui doit encore passer par le flux de travail ZTD.



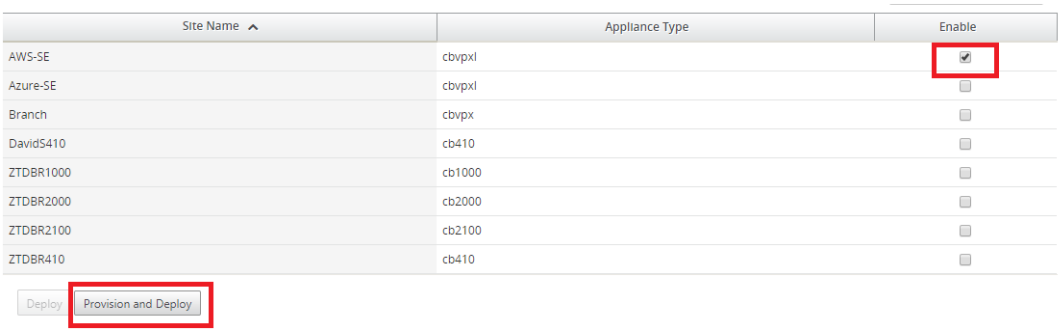
2. Revenez à la page SD-WAN Center Zero Touch Deployment et lorsque la nouvelle configuration active est en cours d'exécution, le nouveau site sera disponible pour le déploiement.

a) Dans la page Déploiement zéro tactile, sous l'onglet **Déployer un nouveau site** , sélectionnez le fichier de configuration réseau en cours d'exécution.

b) Une fois que le fichier de configuration en cours d'exécution est sélectionné, la liste de tous les sites de succursales avec des périphériques Citrix SD-WAN non déployés qui sont pris en charge pour la touche zéro s'affiche.

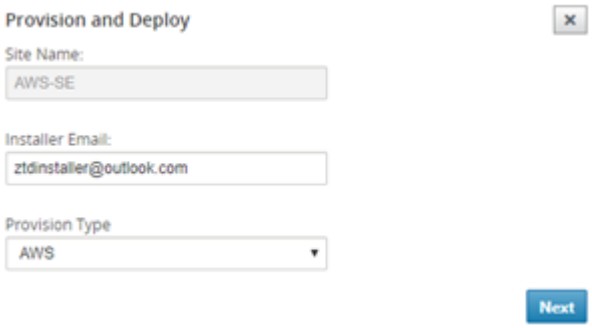


c) Sélectionnez le site cloud cible que vous souhaitez déployer à l'aide du service Zero Touch, cliquez sur**Activer**, puis **Provisionner et déployer**.

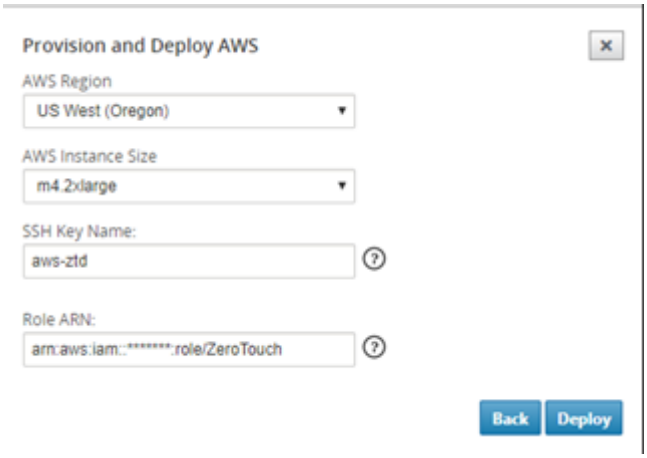


d) Une fenêtre contextuelle apparaît, dans laquelle l'administrateur Citrix SD-WAN peut lancer le déploiement pour Zero Touch.

Renseignez une adresse e-mail à laquelle l'URL d'activation peut être envoyée, puis sélectionnez le **type de provision** pour le cloud souhaité.



e) Après avoir cliqué sur **Suivant**, sélectionnez la région appropriée, la taille de l'instance, remplissez les champs Nom de clé SSH et ARN de rôle de manière appropriée.

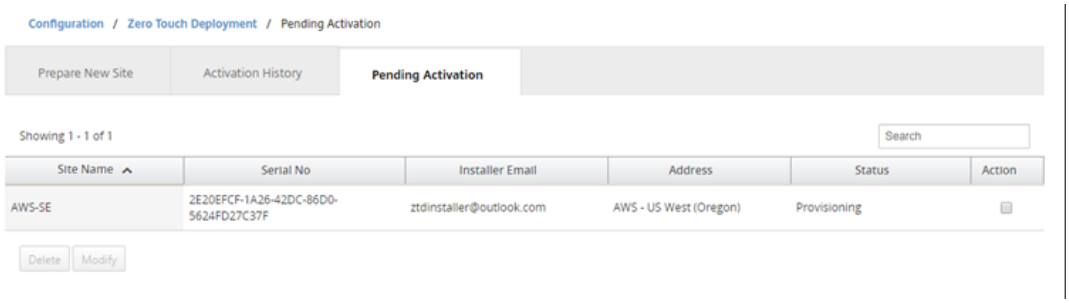


> **Remarque**
>
> Utilisez les liens d'aide pour obtenir des conseils sur la configuration de l'ARN de clé et de rôle SSH sur le compte Cloud.Assurez-vous également que la région sélectionnée correspond à ce qui est disponible sur le compte et que la taille d'instance sélec-

> tionnée correspond à VPX ou VPXL en tant que modèle sélectionné dans la configuration SD-WAN.

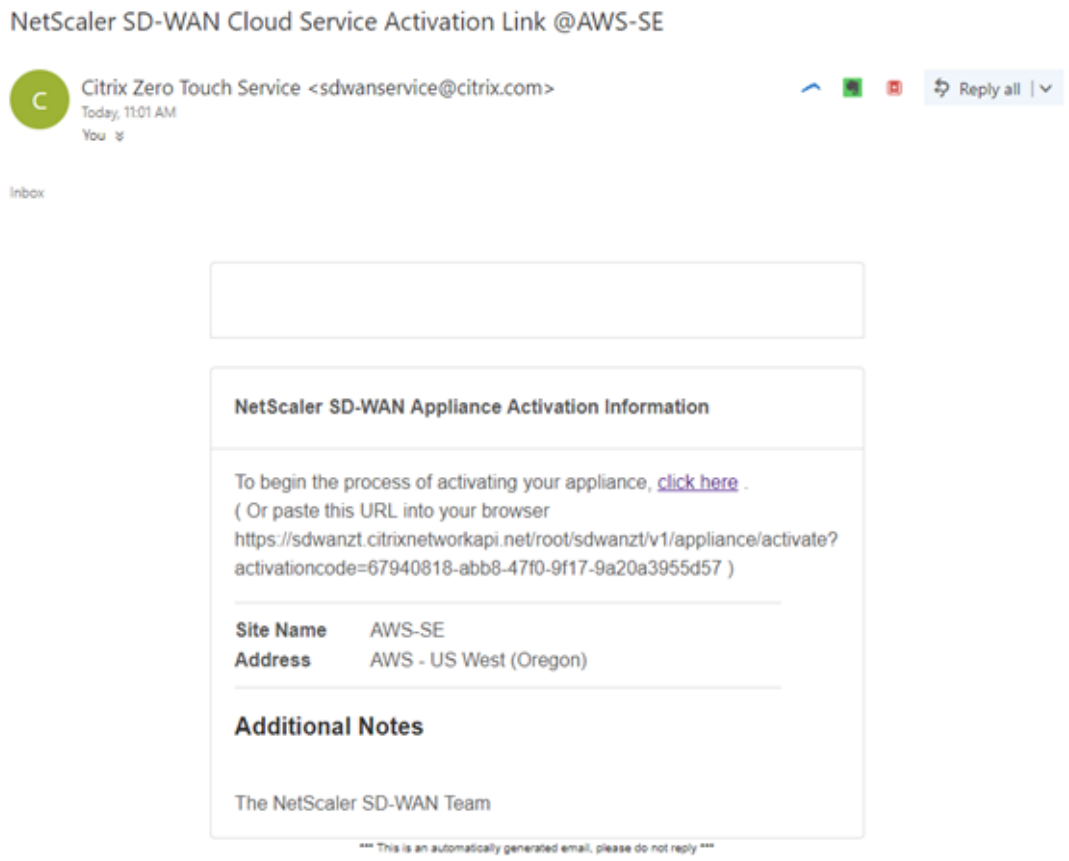
f) Cliquez sur **Déployer**, déclenchant SD-WAN Center, précédemment enregistré auprès du service cloud ZTD, pour partager la configuration de ce site afin qu'il soit stocké temporalité dans le service cloud ZTD.

g) Accédez à l'onglet **Activation en attente** pour confirmer que les informations du site ont été correctement renseignées et ont été placées dans un état de provisionnement.



3. Lancez le processus de déploiement Zero Touch en tant qu'administrateur du cloud.

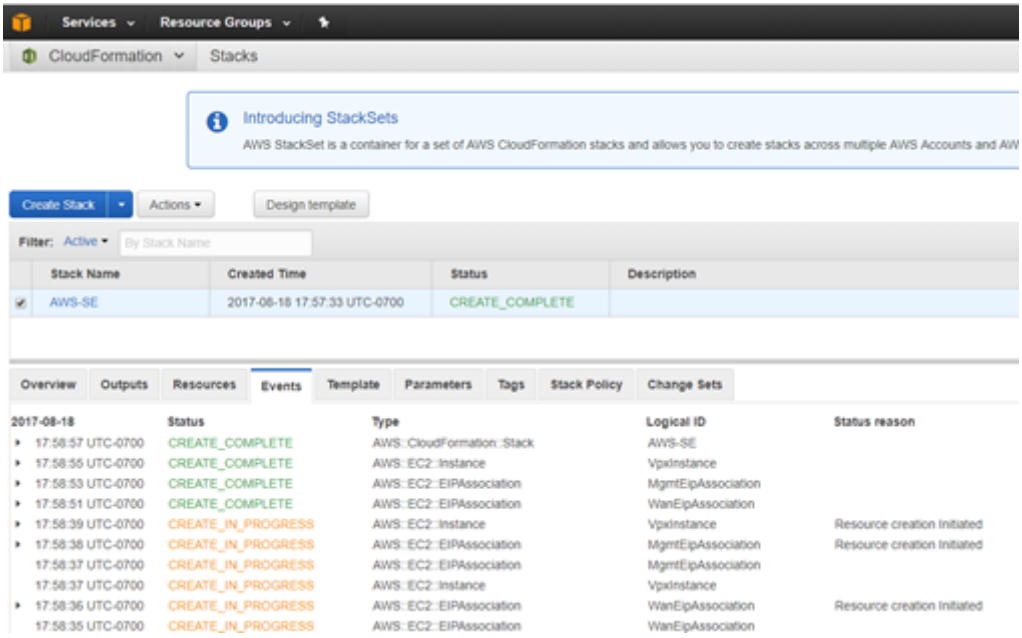
a) Le programme d'installation doit vérifier la boîte aux lettres de l'adresse e-mail utilisée par l'administrateur SD-WAN lors du déploiement du site.



b) Ouvrez l'URL d'activation trouvée dans l'e-mail dans une fenêtre de navigateur Internet.

c) Si la clé SSH et l'ARN de rôle sont correctement entrés, le service de déploiement sans intervention commencera immédiatement à provisionner l'instance SD-WAN, sinon des erreurs de connexion s'afficheront immédiatement.

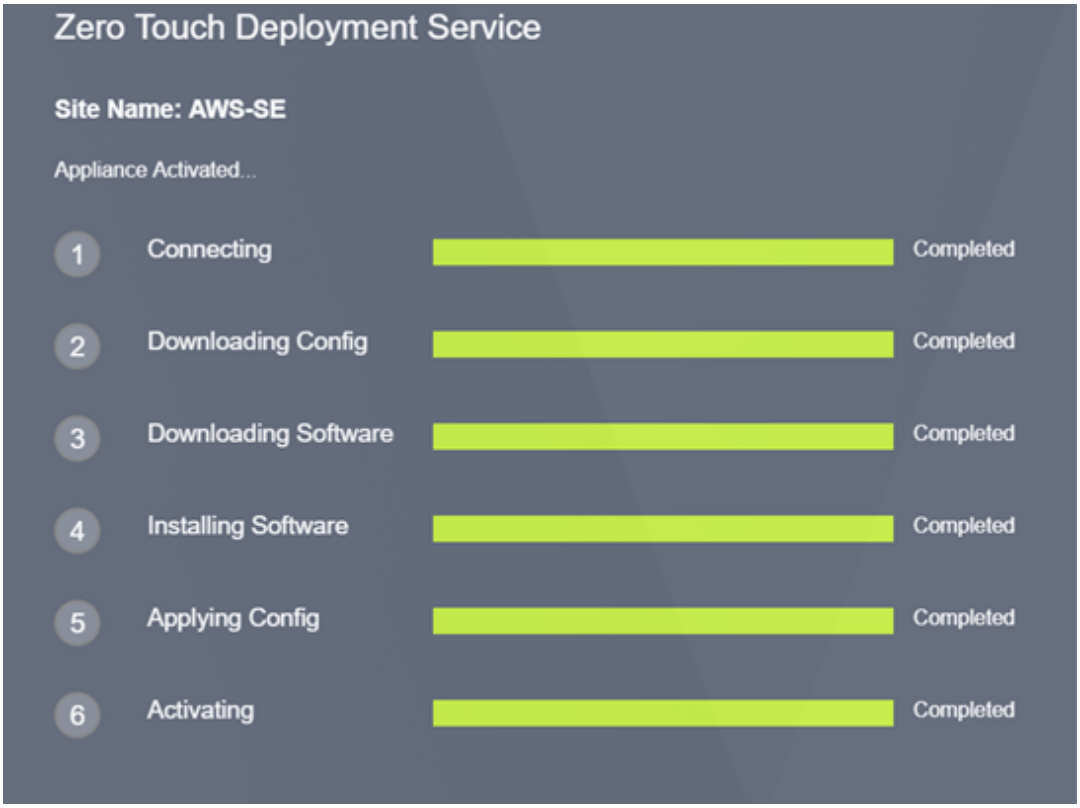
d) Pour un dépannage supplémentaire sur la console AWS, le service Cloud Formation peut être utilisé pour détecter tous les événements qui se produisent au cours du processus de Provisioning.



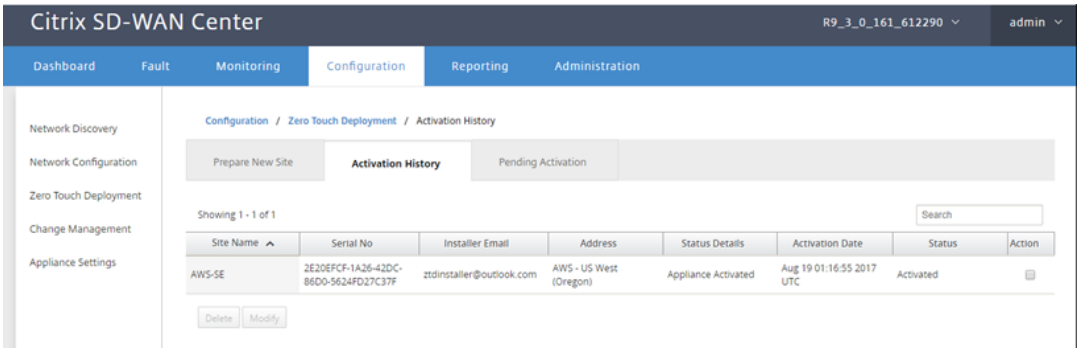
e) Laissez le processus de provisionnement environ 8 à 10 minutes et l'activation de 3 à 5 minutes supplémentaires pour se terminer complètement.

f) Une fois la connectivité réussie de l'instance cloud SD-WAN au service cloud ZTD, le service effectue automatiquement les opérations suivantes :

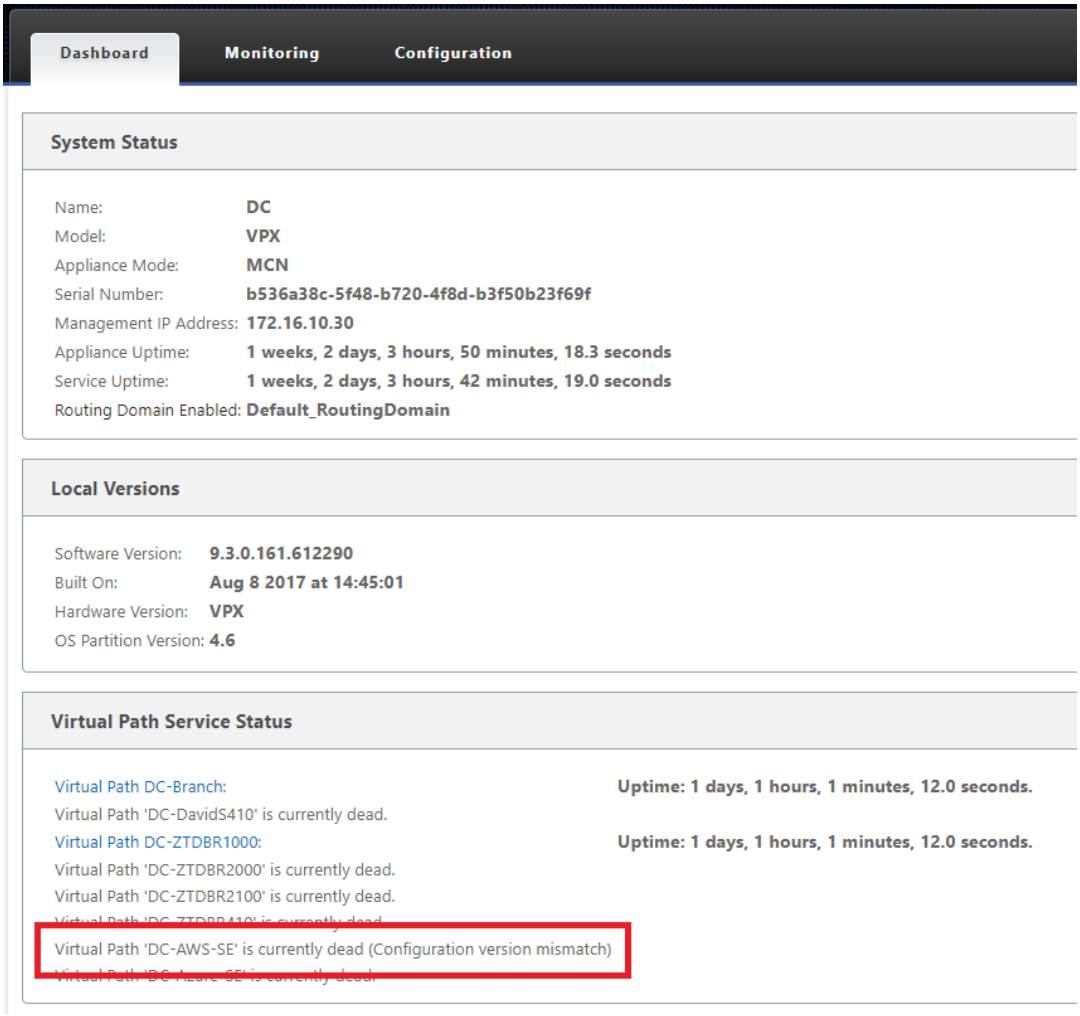
- Télécharger le fichier de configuration spécifique au site qui a été stocké précédemment par SD-WAN Center
- Application de la configuration à l'instance locale
- Télécharger et installer un fichier de licence temporaire de 10 Mo
- Téléchargez et installez les mises à jour logicielles si nécessaire
- Activer le service SD-WAN



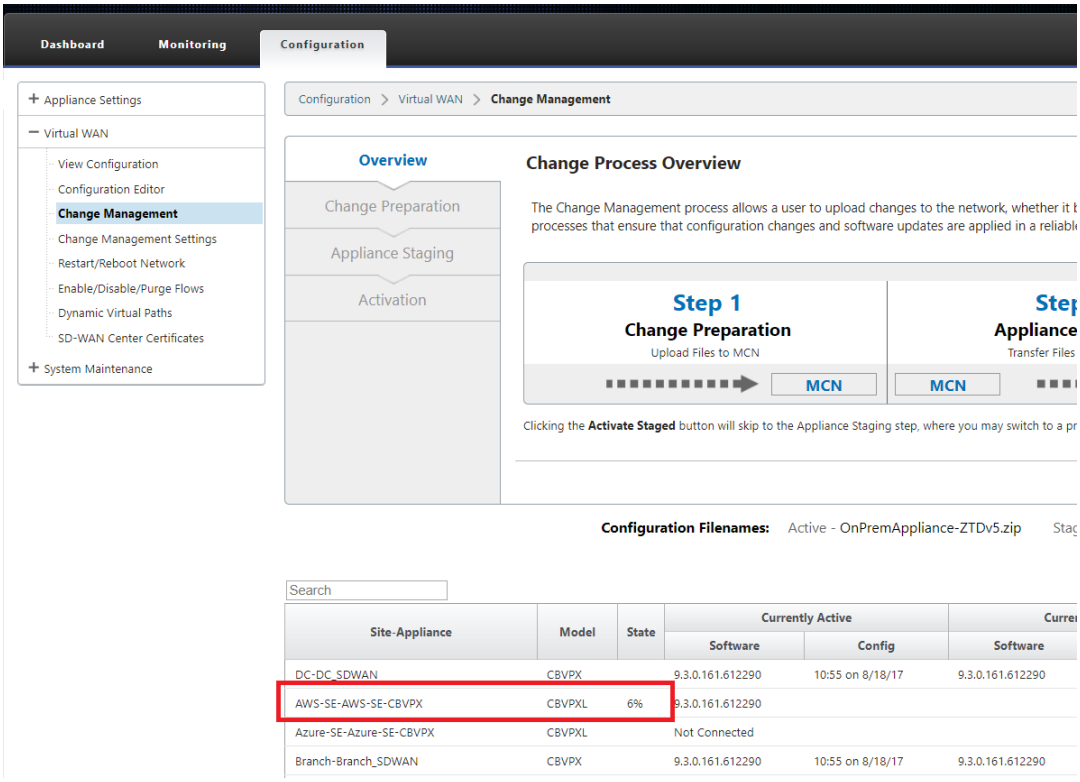
g) Une confirmation supplémentaire peut être effectuée dans l'interface de gestion Web SD-WAN Center ; le menu Déploiement zéro tactile affiche les appliances activées avec succès dans l'onglet **Historique d'activation** .



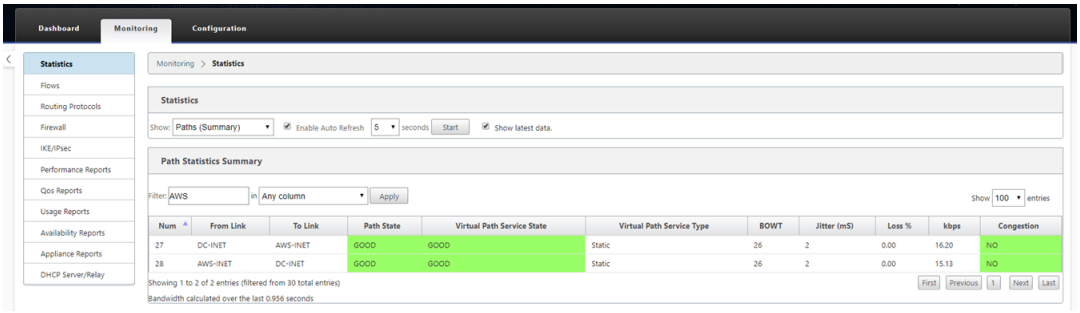
h) Les chemins virtuels peuvent ne pas apparaître immédiatement dans un état connecté, car le MCN peut ne pas faire confiance à la configuration transmise par le service de cloud ZTD et signalera « *incompatibilité de version de configuration* » dans le tableau de bord MCN.



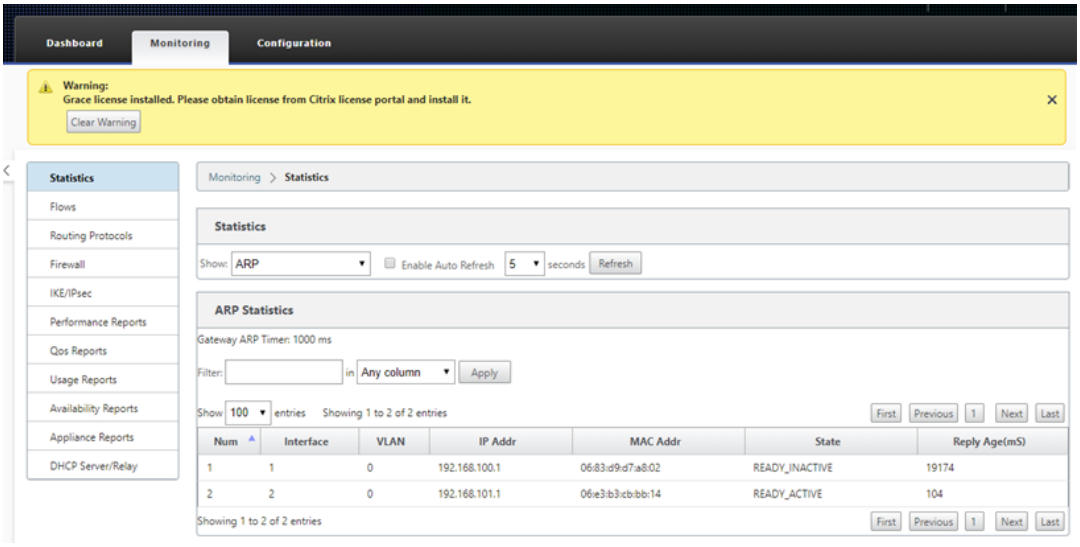
i) La configuration sera automatiquement redistribuée à l'appliance de succursale nouvellement installée, l'état de cette opération peut être suivi sur la page **MCN** > **Configuration** > **Virtual WAN** > **Gestion des modifications** (selon la connectivité, ce processus peut prendre plusieurs minutes).



j) L'administrateur SD-WAN peut surveiller la page de gestion Web MCN de tête de réseau pour les chemins virtuels établis du site cloud nouvellement ajouté.



k) Si un dépannage est nécessaire, ouvrez l'interface utilisateur des instances SD-WAN à l'aide de l'adresse IP publique attribuée par l'environnement cloud pendant le provisionnement, puis utilisez la table ARP de la page **Surveillance** > **Statistiques** pour identifier tout problème de connexion aux passerelles attendues, ou utilisez le options de suivi de route et de capture de paquets dans les diagnostics.



Azure

February 17, 2022

Avec SD-WAN version 9.3, les capacités de déploiement sans intervention ont été étendues aux instances Cloud. La procédure de déploiement du processus de déploiement sans intervention pour les instances de cloud diffère légèrement du déploiement de l'appliance pour le service sans intervention.

Mise à jour de la configuration pour ajouter un nouveau site distant avec un périphérique cloud SD-WAN compatible ZTD à l'aide de la configuration réseau SD-WAN Center

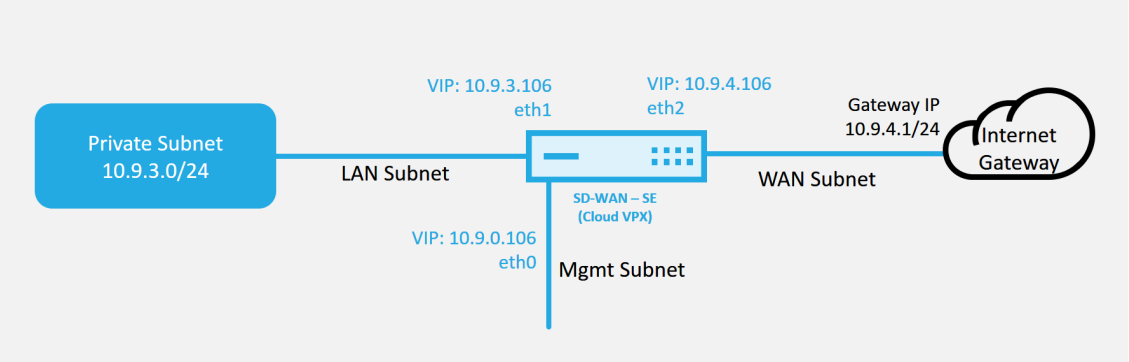
Si la configuration SD-WAN n'a pas été créée à l'aide de la configuration réseau SD-WAN Center, importez la configuration active à partir du MCN et commencez à modifier la configuration à l'aide du SD-WAN Center. Pour la capacité de déploiement sans intervention, l'administrateur SD-WAN doit créer la configuration à l'aide du SD-WAN Center. La procédure suivante doit être utilisée pour ajouter un nouveau nœud de cloud ciblé pour un déploiement sans intervention.

1. Concevez le nouveau site pour le déploiement du cloud SD-WAN en décrivant d'abord les détails du nouveau site (taille VPX, utilisation des groupes d'interface, adresses IP virtuelles, lien(s) WAN avec bande passante et passerelles respectives).

Remarque

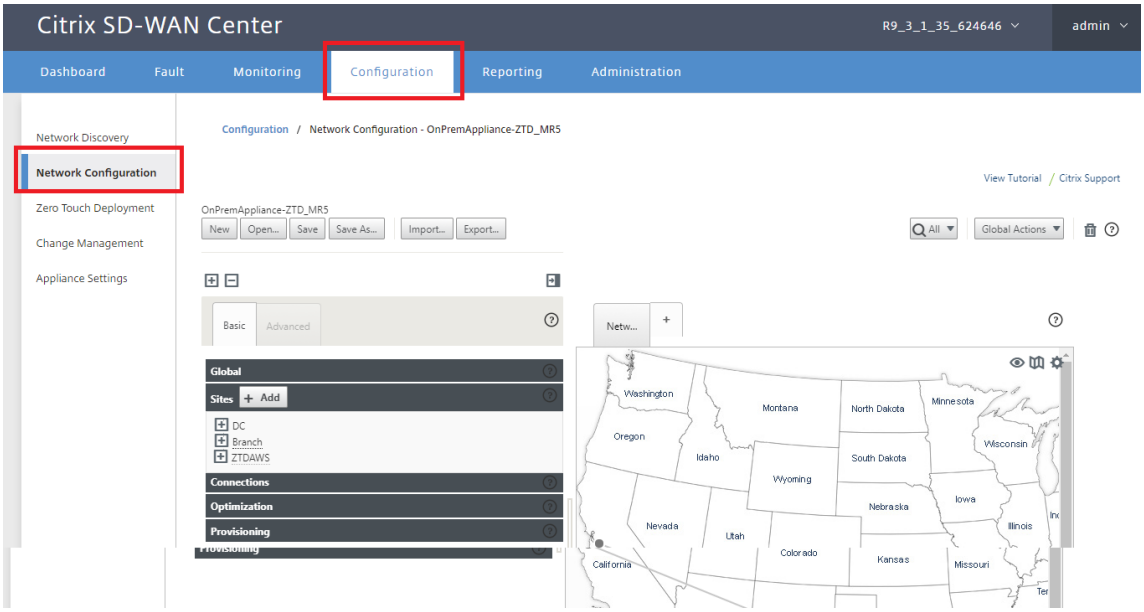
- Les instances SD-WAN déployées dans le cloud doivent être déployées en mode Edge/-Gateway.
- Le modèle pour l'instance de cloud est limité à trois interfaces : Gestion, LAN et WAN (dans cet ordre).
- Les modèles de cloud Azure disponibles pour SD-WAN VPX sont actuellement définis pour obtenir l'adresse IP 10.9.4.106 pour le réseau étendu, 10.9.3.106 IP pour le réseau local et 10.9.0.16 IP pour l'adresse de gestion.La configuration SD-WAN pour le nœud Azure ciblé pour Zero Touch doit correspondre à cette disposition.
- Le nom du site Azure dans la configuration doit être en minuscules sans caractères spéciaux (par exemple ztdazure).

Azure Cloud Topology with NetScaler SD-WAN

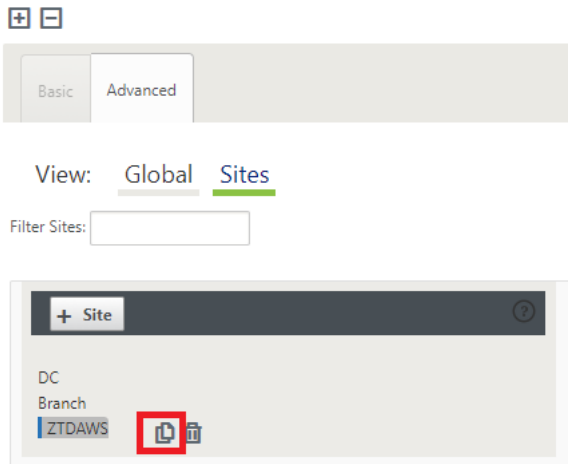


Il s'agit d'un exemple de déploiement d'un site cloud SD-WAN déployé, le périphérique Citrix SD-WAN est déployé en tant que périphérique desservant une seule liaison WAN Internet dans ce réseau cloud.Les sites distants seront en mesure d'exploiter plusieurs liaisons WAN Internet distinctes se connectant à cette même passerelle Internet pour le cloud, offrant ainsi une résilience et une connectivité de bande passante agrégée à partir de n'importe quel site de déploiement SD-WAN vers l'infrastructure cloud.Cela fournit une connectivité rentable et hautement fiable au cloud.

2. Ouvrez l'interface de gestion Web SD-WAN Center et accédez à la page **Configuration** > **Configuration réseau**.



3. Assurez-vous qu'une configuration opérationnelle est déjà en place ou importez la configuration à partir du MCN.
4. Accédez à l'onglet Basic pour créer un nouveau site.
5. Ouvrez la vignette Sites pour afficher les sites actuellement configurés.
6. Créez rapidement la configuration du nouveau site cloud en utilisant la fonction de clonage de n'importe quel site existant ou créez manuellement un nouveau site.

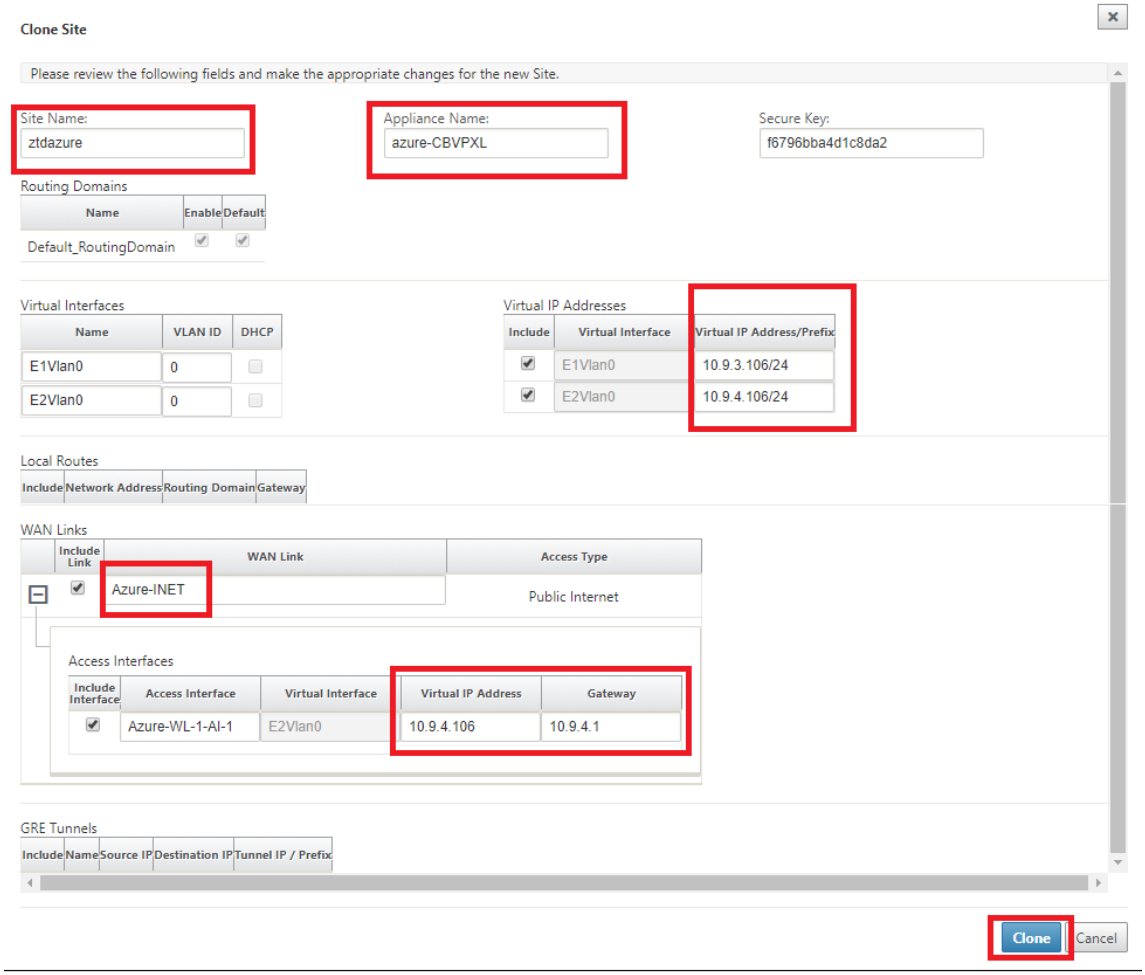


7. Remplissez tous les champs requis à partir de la topologie conçue précédemment pour ce nouveau site cloud.

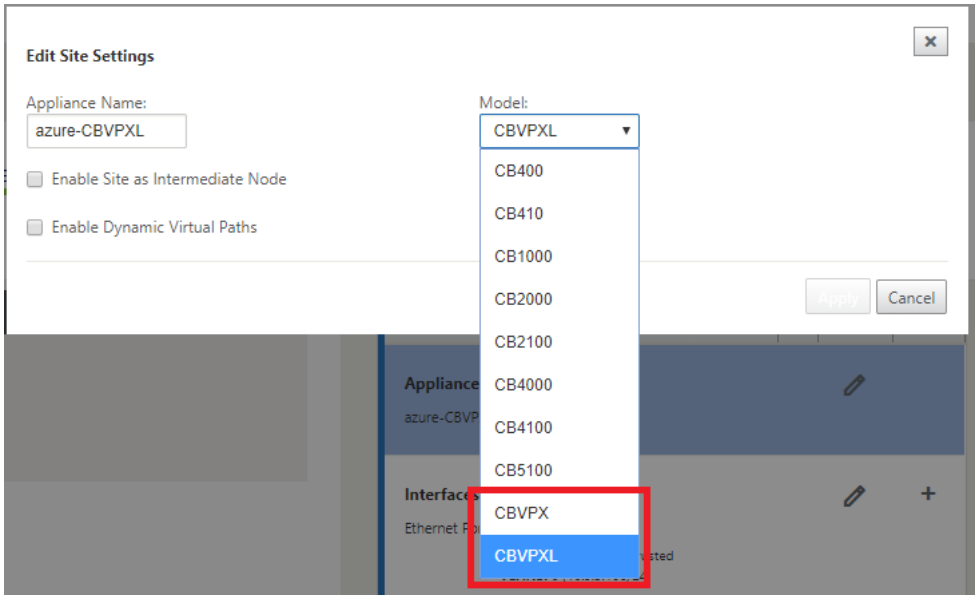
   Gardez à l'esprit que le modèle disponible pour les déploiements ZTD cloud Azure est actuellement difficile pour obtenir l'adresse IP 10.9.4.106 pour le réseau étendu, 10.9.3.106 IP pour le réseau local et 10.9.0.16 IP pour l'adresse de gestion. Si la configuration n'est pas définie pour correspondre à l'adresse VIP attendue pour chaque interface, le périphérique ne sera pas en

mesure d'établir correctement ARP aux passerelles d'environnement cloud et la connectivité IP au chemin virtuel du MCN.

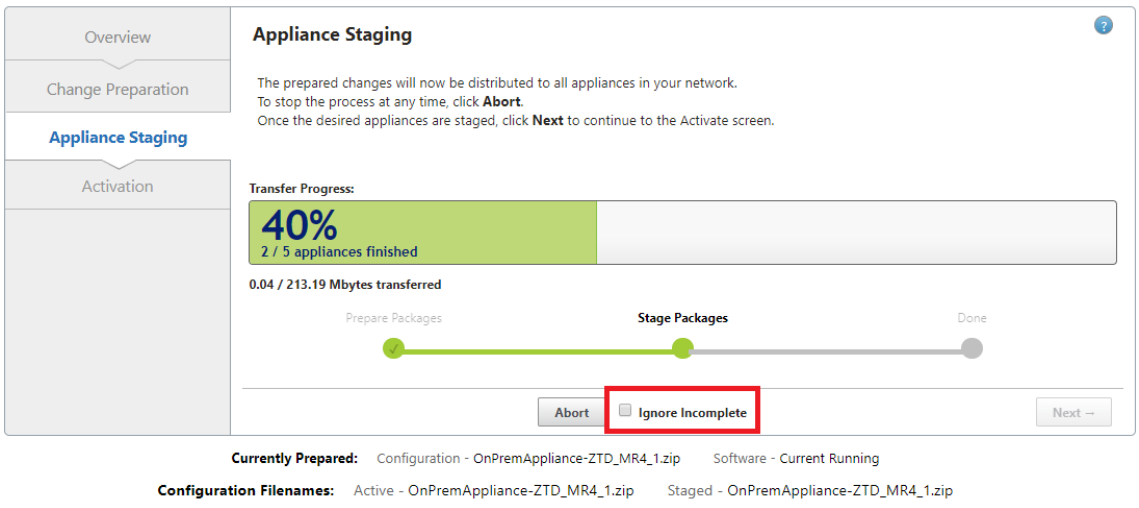
Il est d'importer que le nom du site soit conforme à ce que Azure attend.Le nom du site doit être en minuscules, au moins 6 caractères, sans caractères spéciaux, il doit confirmer l'expression régulière suivante **^[a-z][a-z0-9-]{1,61}[a-z0-9]$.**



8. Après le clonage d'un nouveau site, accédez aux **paramètres de base**du site et vérifiez que le modèle de SD-WAN est correctement sélectionné pour prendre en charge le service sans intervention.

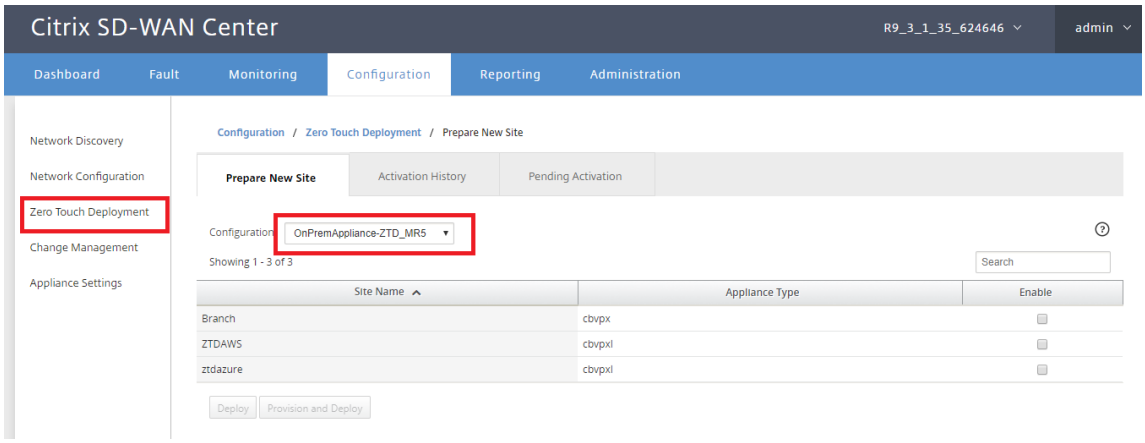


9. Enregistrez la nouvelle configuration sur SD-WAN Center et utilisez l'exportation vers l'option « **Change Management Inbox** » pour pousser la configuration à l'aide de Change Management.
10. Suivez la procédure de gestion des modifications pour organiser correctement la nouvelle configuration, ce qui rend les périphériques SD-WAN existants conscients du nouveau site à déployer via le bouton zéro, vous devrez utiliser l'option « *Ignorer incomplet* » *pour ignorer*la tentative de pousser la configuration vers le nouveau site qui doit encore passer par le flux de travail ZTD.

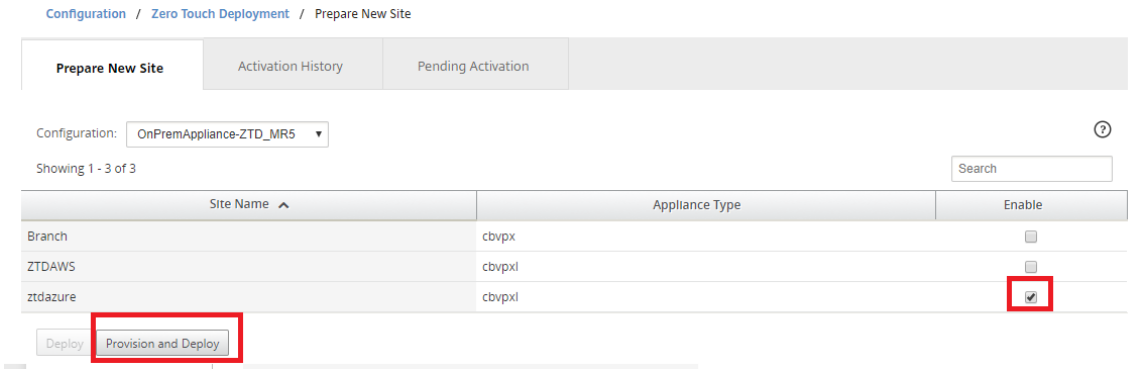


Accédez à la page Déploiement Zero Touch du SD-WAN Center, et avec la nouvelle configuration active en cours d'exécution, le nouveau site sera disponible pour SD-WAN Center Provisionnement et Déploiement d'Azure (étape 1 sur 2)

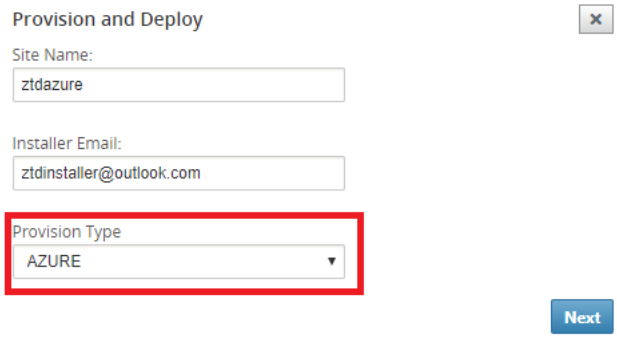
1. Dans la page déploiement sans intervention, connectez-vous avec vos informations d'identification de compte Citrix. Sous l'onglet **Déployer un nouveau site** , sélectionnez le fichier de configuration réseau en cours d'exécution.
2. Une fois le fichier de configuration en cours d'exécution sélectionné, la liste de tous les sites de succursales dotés de périphériques Citrix SD-WAN compatibles ZTD s'affiche.



3. Sélectionnez le site cloud cible que vous souhaitez déployer à l'aide du service Zero Touch, cliquez sur**Activer**, puis cliquez sur **Provisionner et déployer**.

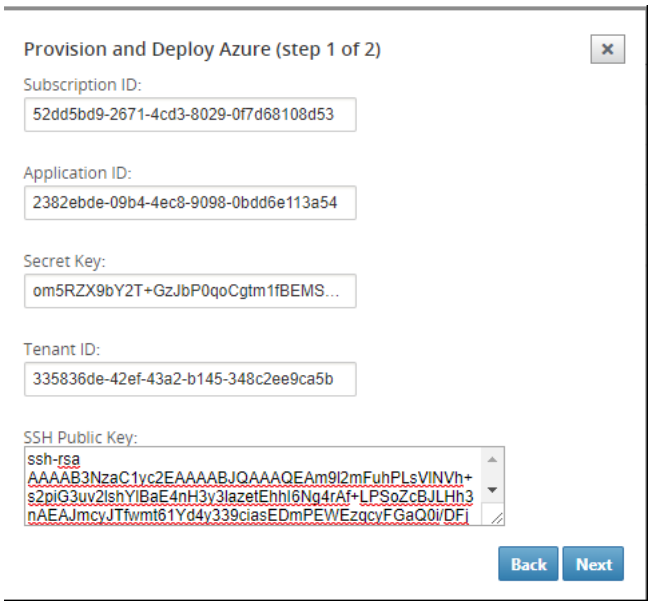


4. Une fenêtre contextuelle apparaît, dans laquelle l'administrateur Citrix SD-WAN peut lancer le déploiement pour Zero Touch. Vérifiez que le nom du site est conforme aux exigences sur Azure (minuscules sans caractères spéciaux). Renseignez une adresse e-mail où l'URL d'activation peut être fournie, puis sélectionnez Azure comme **type de fourniture** pour le cloud souhaité, avant de cliquer sur **Suivant**.

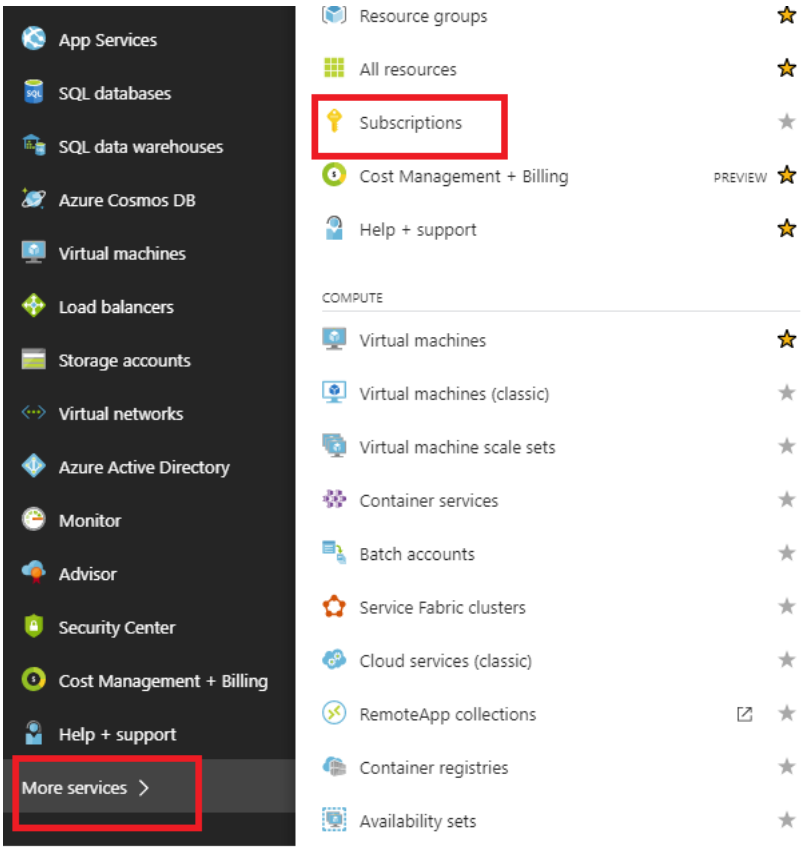


5. Après avoir cliqué sur**Suivant**, la fenêtre Provisionner et déployer Azure (étape 1sur 2) nécessitera l'entrée de obtenu à partir du compte Azure.

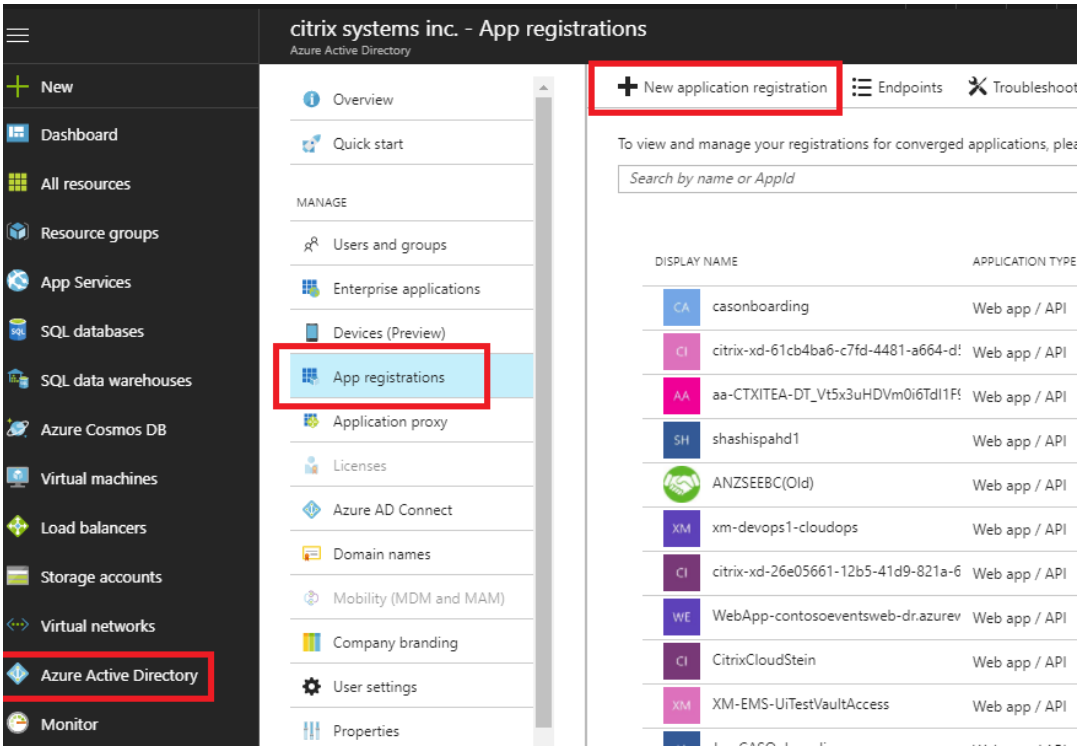
   Copiez et collez chaque champ requis après avoir obtenu les informations de votre compte Azure.Les étapes ci-dessous expliquent comment obtenir l'ID d'abonnement, l'ID d'application, la clé secrète et l'ID de locataire requis à partir de votre compte Azure, puis cliquez sur **Suivant**.



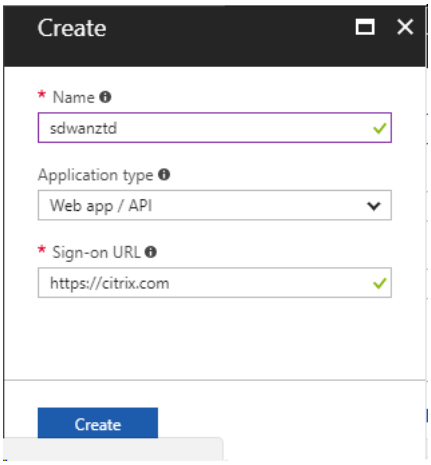
   a) Sur le compte Azure, nous pouvons identifier l'***ID d'abonnement*** requis en accédant à « Autres services » et en sélectionnant **Abonnements.**



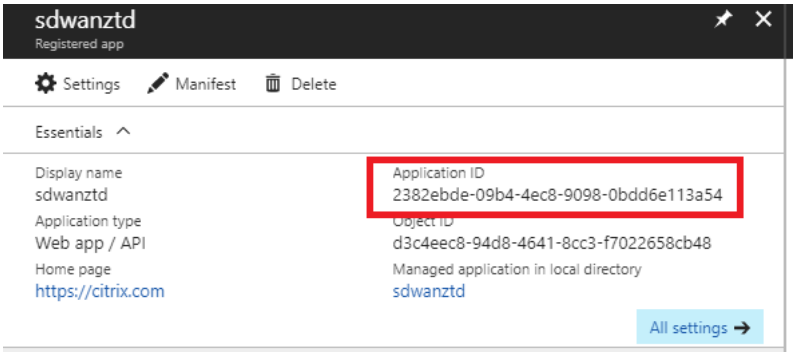
b) Pour identifier l'***ID d'application***requis, accédez à Azure Active Directory, Enregistrements d'application, puis cliquez sur **Nouvel enregistrement d'application.**



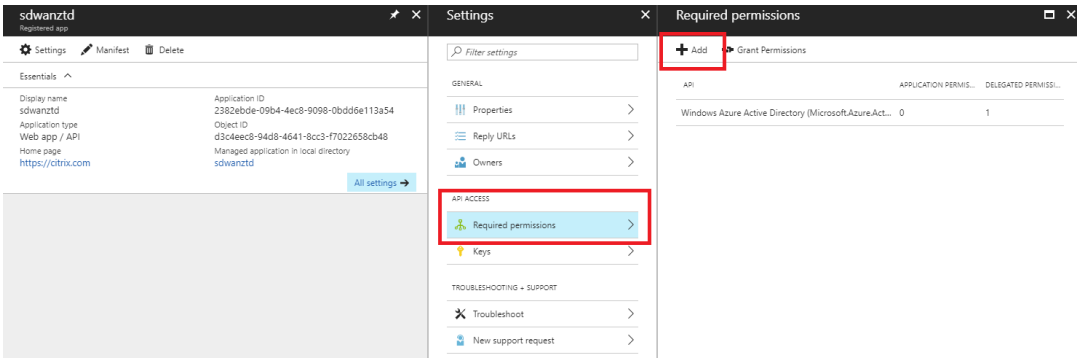
c) Dans le menu Créer l'enregistrement de l'application, entrez un nom et une URL de connexion (il peut s'agir de n'importe quelle URL, la seule condition requise est qu'elle soit valide), puis cliquez sur **Créer**.



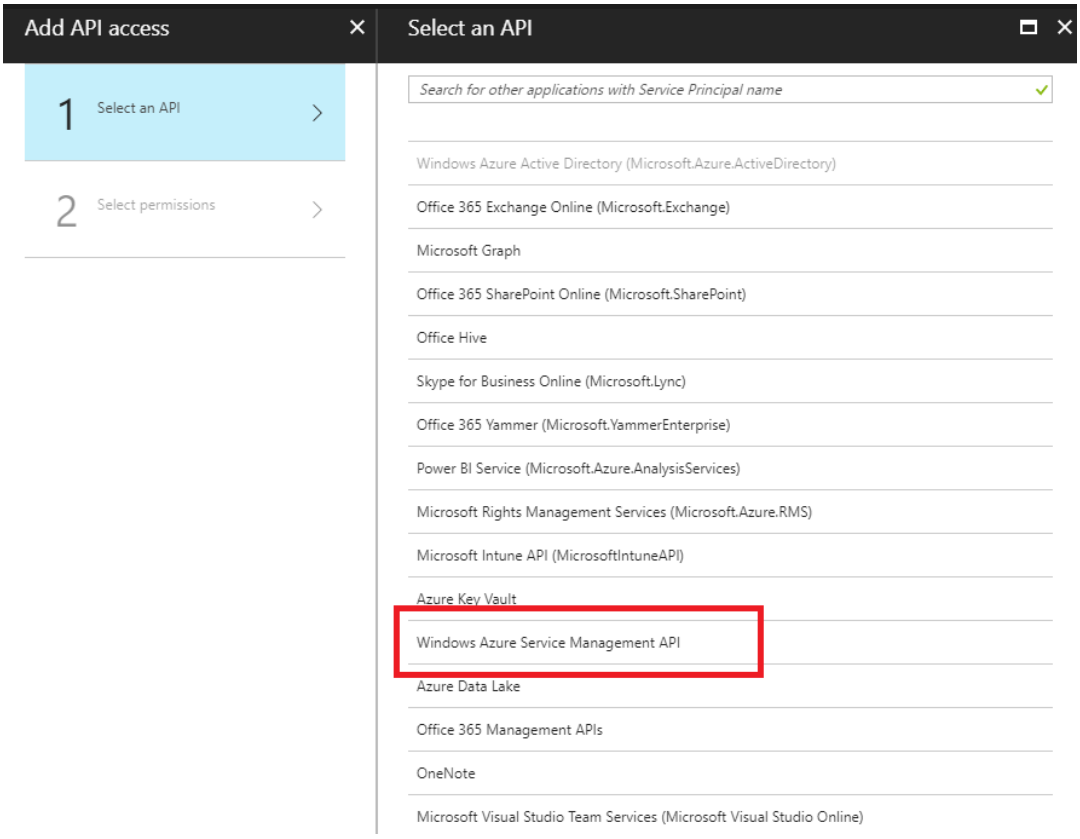
d) Recherchez et ouvrez l'application enregistrée nouvellement créée, puis notez l'ID de l'application.



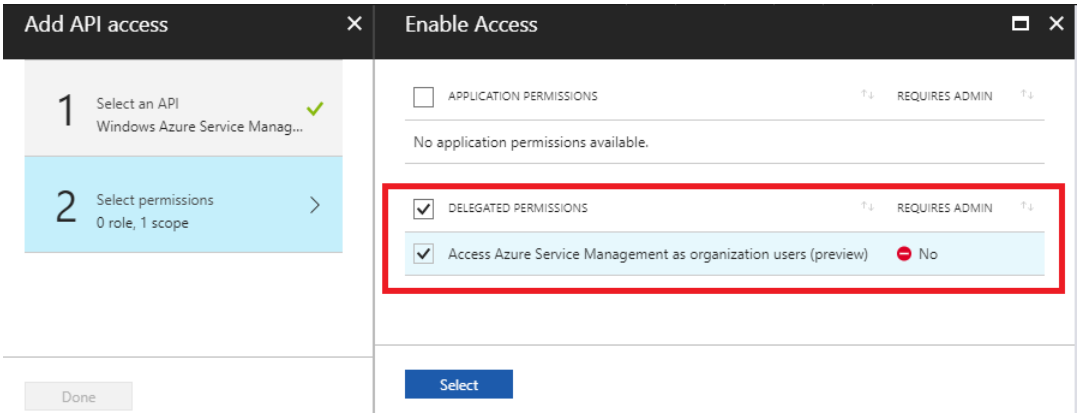
e) Ouvrez à nouveau l'application d'enregistrement nouvellement créée et, pour identifier la *clé de sécurité* requise, sous Accès API, sélectionnez **Autorisations requises** pour permettre à un tiers de provisionner et d'organiser une instance. Sélectionnez ensuite **Ajouter**.



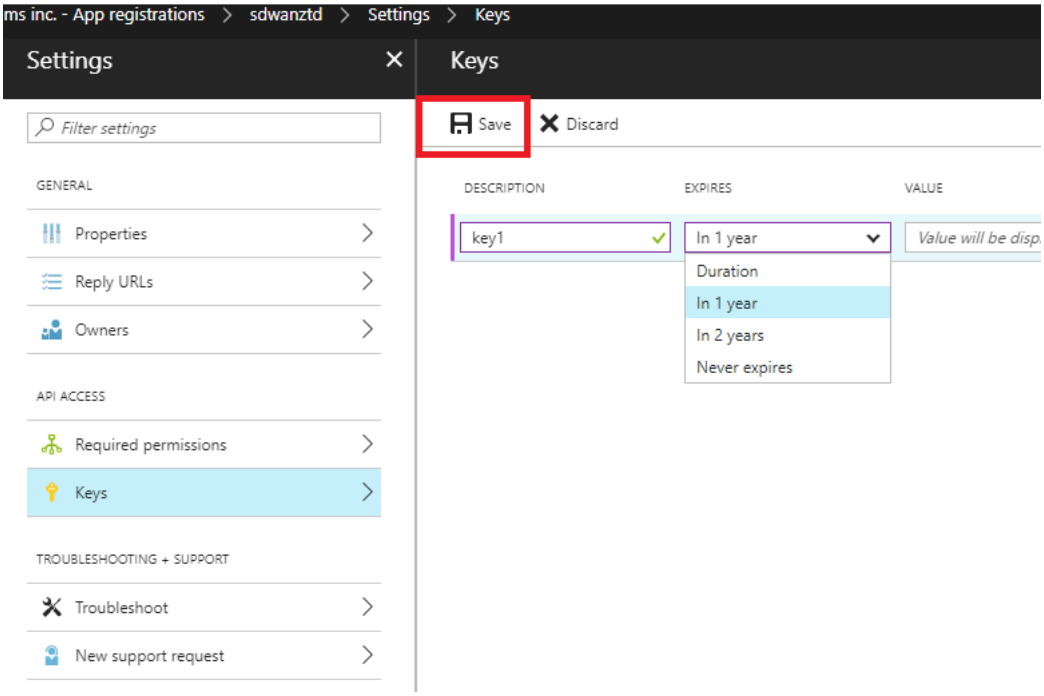
f) Lorsque vous ajoutez les autorisations requises, **sélectionnez une API,** puis mettez en surbrillance l'**API de gestion des services Windows Azure.**



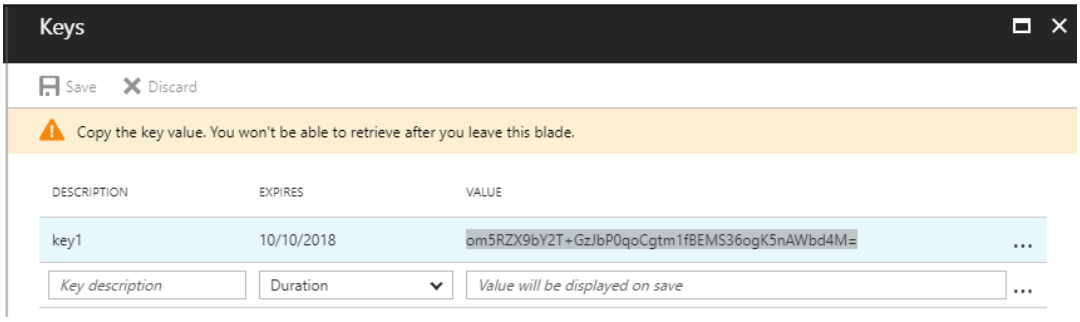
g) Activez **Delegate Permissions** pour provisionner des instances, puis cliquez sur **Sélectionner** et **Terminé**.



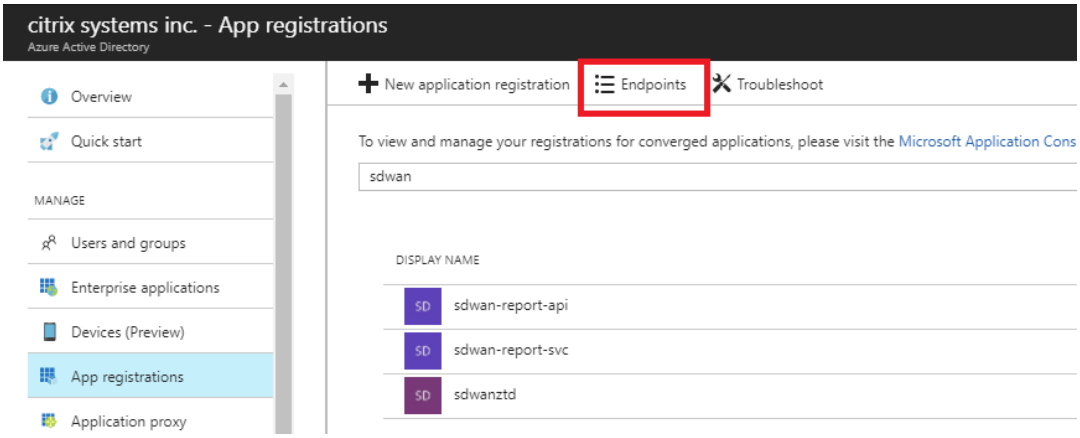
h) Pour cette application enregistrée, sous Accès API, sélectionnez **Clés,** puis créez une **description de clé** secrète et la **durée** souhaitée pour que la clé soit valide.Ensuite, cliquez sur **Enregistrer qui** produira une **clé secrète** (la clé n'est requise que pour le processus d'approvisionnement, elle peut être supprimée après la mise à disposition de l'instance).



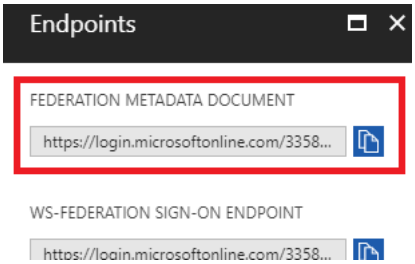
i) Copiez et enregistrez la clé secrète (notez que vous ne pourrez pas la récupérer ultérieurement).



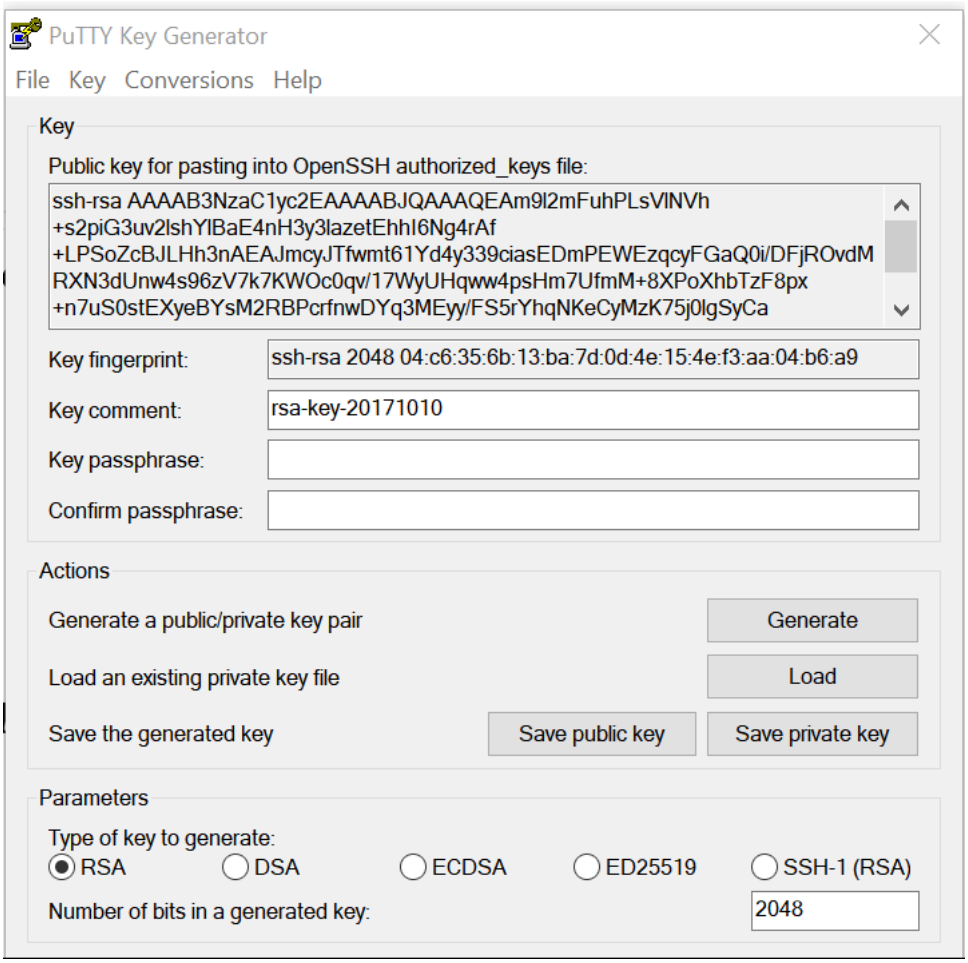
j) Pour identifier l'**ID de locataire** requis, revenez sur le volet d'enregistrement de l'application et sélectionnez **Points de terminaison**.



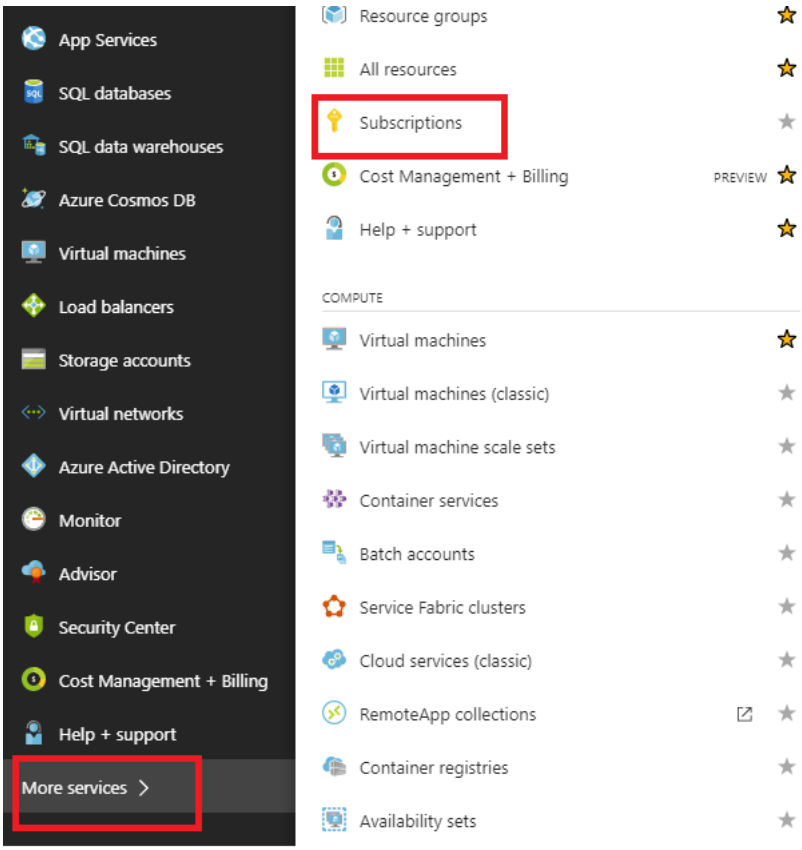
k) Copiez le **document de métadonnées de fédération**, pour identifier votre ID de locataire (notez que l'ID de locataire est une chaîne de 36 caractères située entre « online.com/ » et « /federation » dans l'URL).



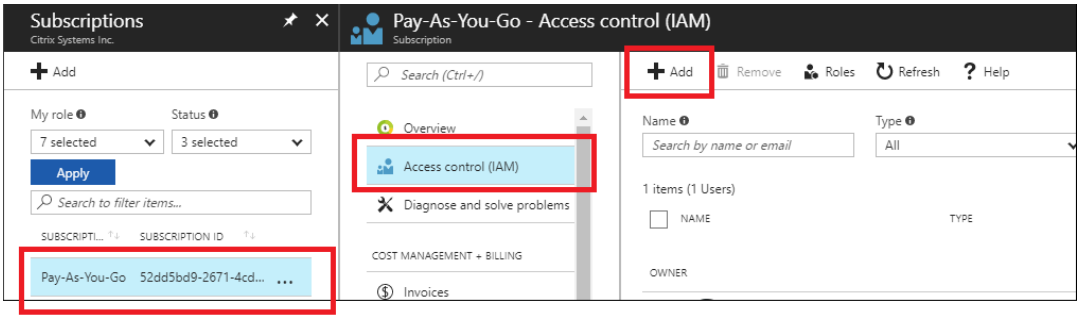
l) Le dernier élément requis est la ***clé publique SSH***.Cela peut être créé à l'aide du générateur de clés Putty ou ssh-keygen et sera utilisé pour l'authentification, éliminant ainsi le besoin de mots de passe pour se connecter.La clé publique SSH peut être copiée (y compris le titre ssh-rsa et les chaînes de clé rsa de fin).Cette clé publique sera partagée via l'entrée SD-WAN Center vers Citrix Zero Touch Deployment Service.



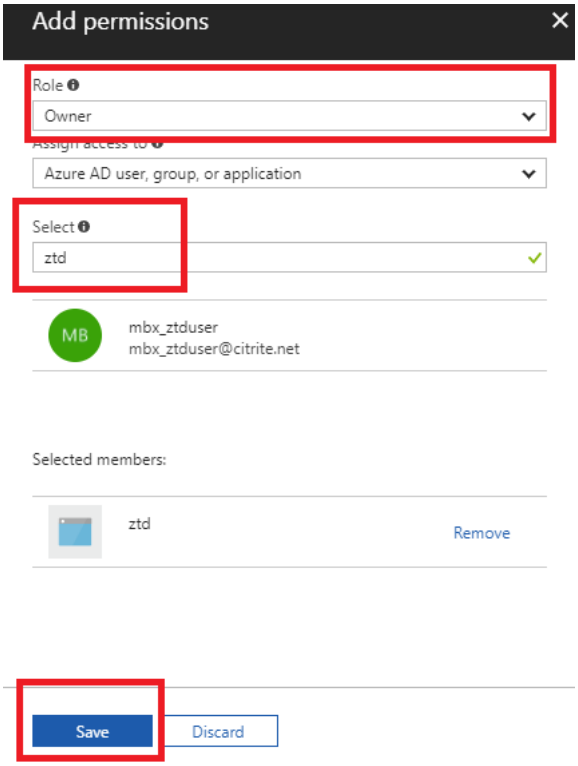
m) Des étapes supplémentaires sont nécessaires pour attribuer un rôle à l'application.Revenez à Plus de services, puis Abonnements.



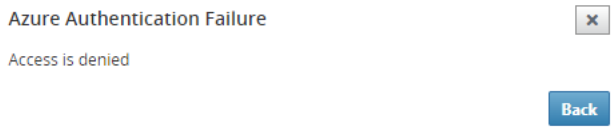
n) Sélectionnez l'abonnement actif, puis **Contrôle d'accès (AIM)**, puis cliquez sur **Ajouter.**



o) Dans le volet d'ajout d'autorisations, sélectionnez le rôle « **Propriétaire** », attribuez l'accès à **« Utilisateur, groupe ou application Azure AD »**et recherchez l'application enregistrée dans le **champ Sélectionner**pour autoriser le service Zero Touch Deployment Cloud à créer et configurer l'instance sur Azure abonnement.Une fois l'application identifiée, sélectionnez-la et assurez-vous qu'elle est remplie en tant que membre sélectionné avant de cliquer sur **Enregistrer**.

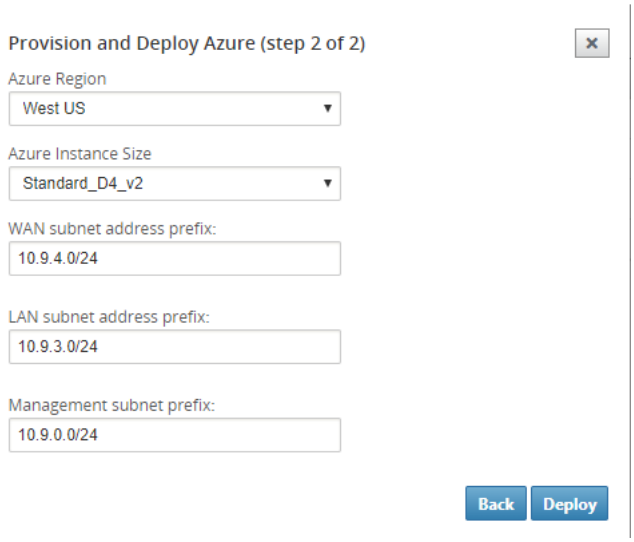


p) Après avoir collecté les entrées requises et les avoir saisies dans SD-WAN Center, cliquez sur**Suivant**.Si les entrées ne sont pas correctes, vous rencontrerez un échec d'authentification.

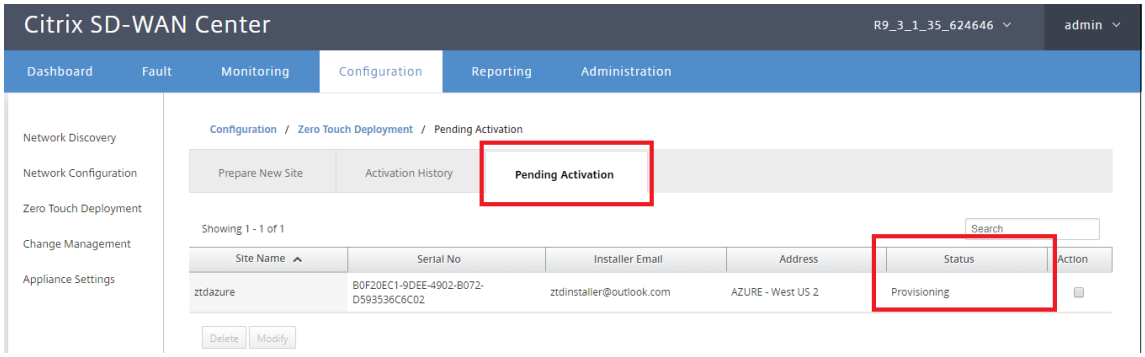


Provisioning de SD-WAN Center et déploiement d'Azure (Étape 2 sur 2)

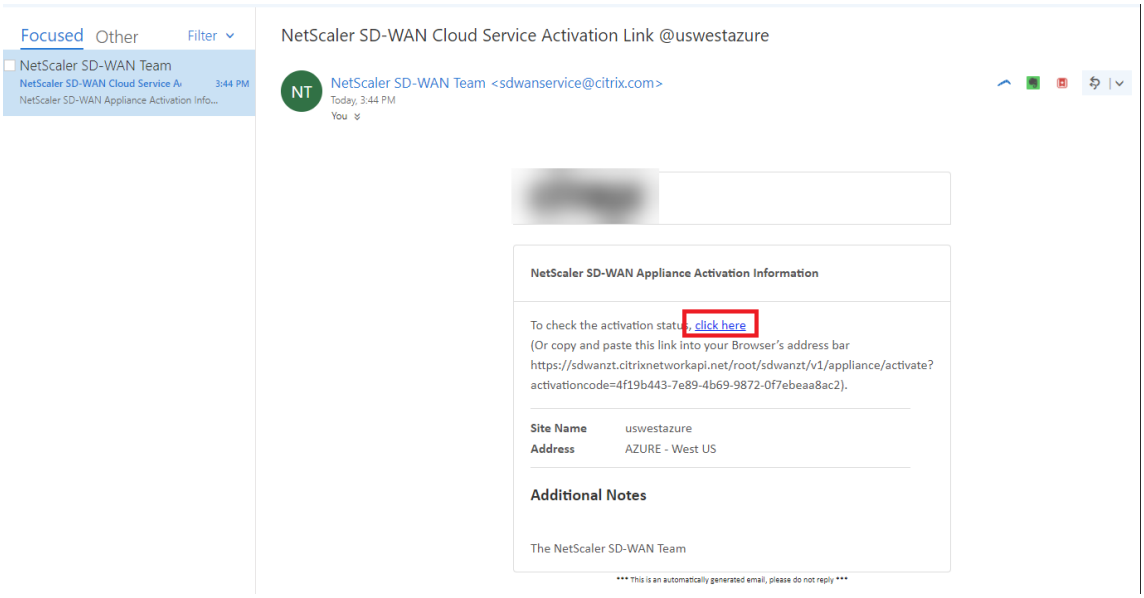
1. Une fois l'authentification Azure réussie, remplissez les champs appropriés pour sélectionner la région Azure souhaitée et la taille d'instance appropriée, puis cliquez sur **Déployer**.



2. L'utilisation de l'onglet **Activation en attente** dans SD-WAN Center permet de suivre l'état actuel du déploiement.

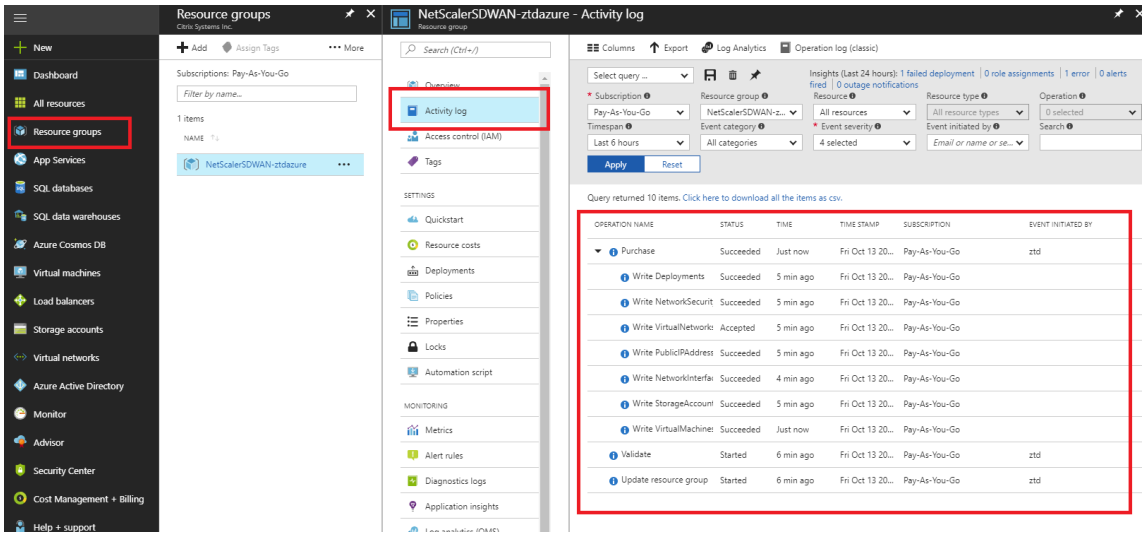


3. Un e-mail avec un code d'activation sera envoyé à l'adresse e-mail saisie à l'étape 1, obtiendra l'e-mail et ouvrira l'**URL d'activation** pour déclencher le processus et vérifier l'état de l'activation.

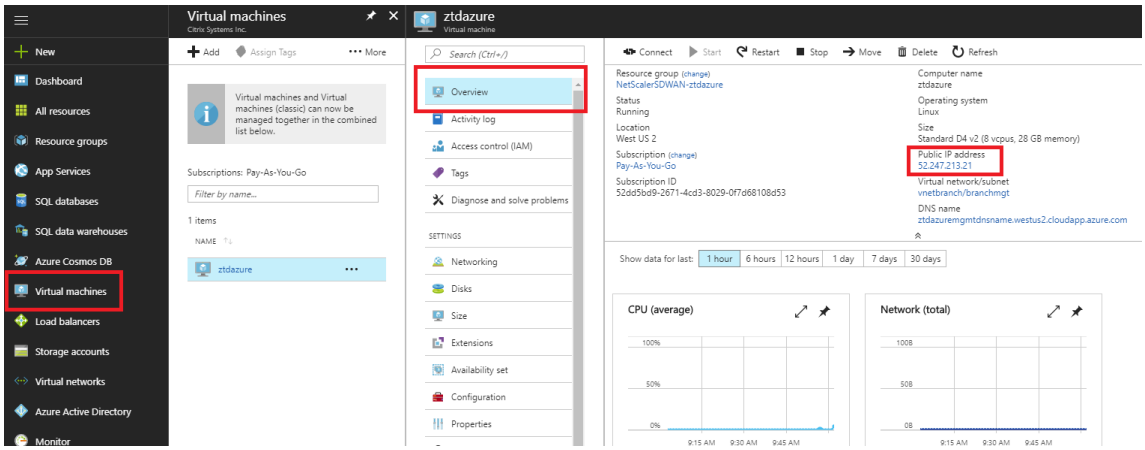


4. Un e-mail avec une URL d'activation sera remis à l'adresse e-mail saisie à l'étape 1.Obtenez l'e-mail et ouvrez l'**URL d'activation** pour déclencher le processus et vérifier l'état de l'activation.

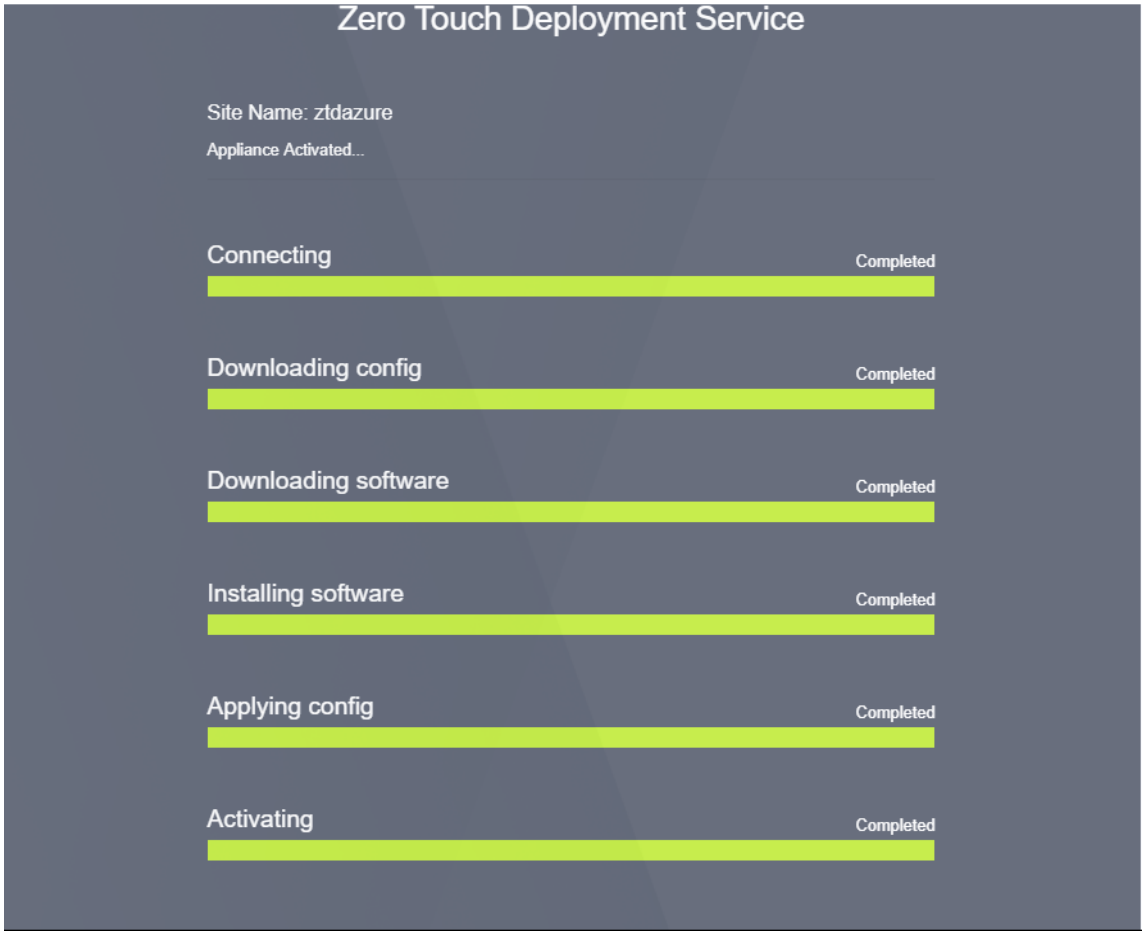
5. Il faudra quelques minutes pour que l'instance soit provisionnée par le SD-WAN Cloud Service.Vous pouvez surveiller l'activité sur le portail Azure, sous **Journal d'activité** pour le **groupe de ressources** créé automatiquement.Tous les problèmes ou erreurs liés au provisioning seront renseignés ici, ainsi que répliqués dans le SD-WAN Center dans le statut d'activation.



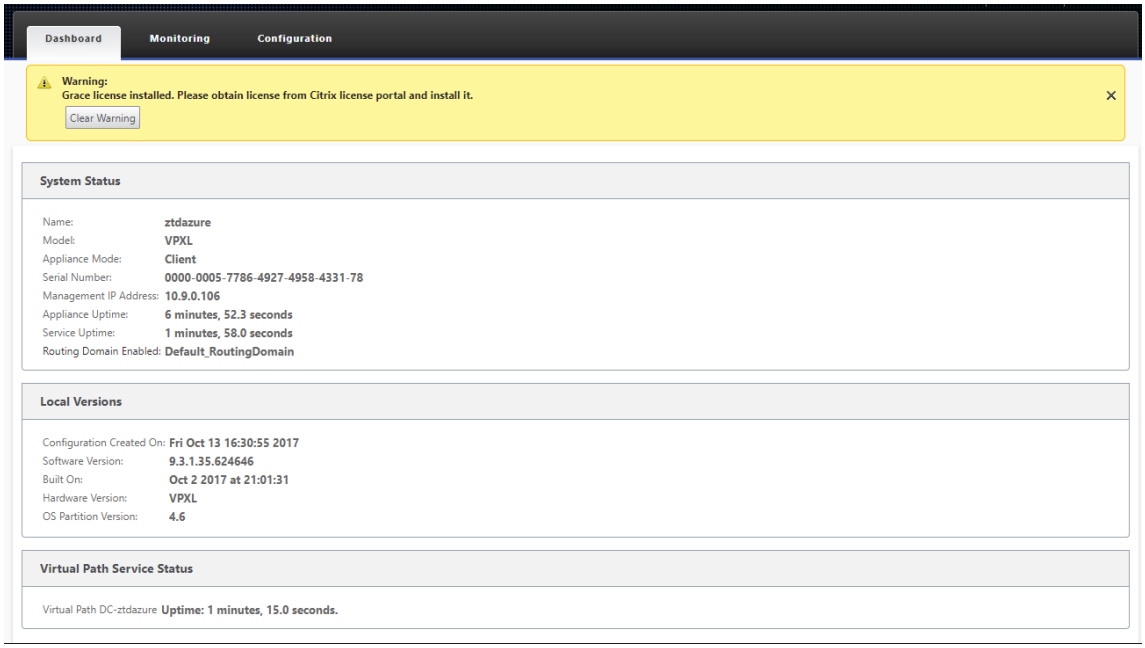
6. Dans le portail Azure, l'instance lancée avec succès sera disponible sous **Machines virtuelles.** Pour obtenir l'adresse IP publique attribuée, accédez à la vue d'ensemble de l'instance.



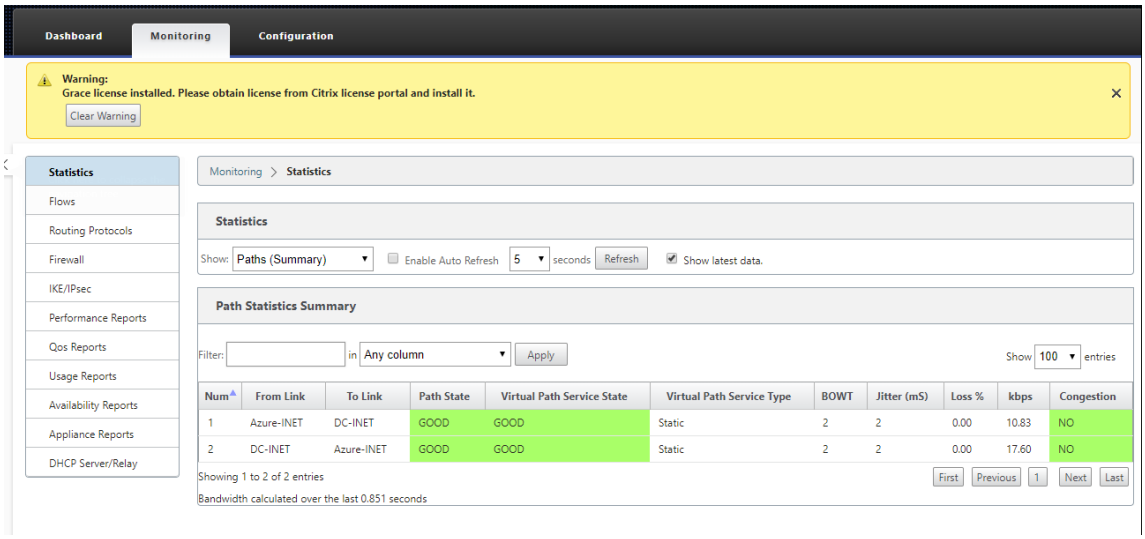
7. Une fois que la machine virtuelle est en cours d'exécution, accordez-lui une minute avant que le service ne prenne contact et démarre le processus de téléchargement de la configuration, du logiciel et de la licence.



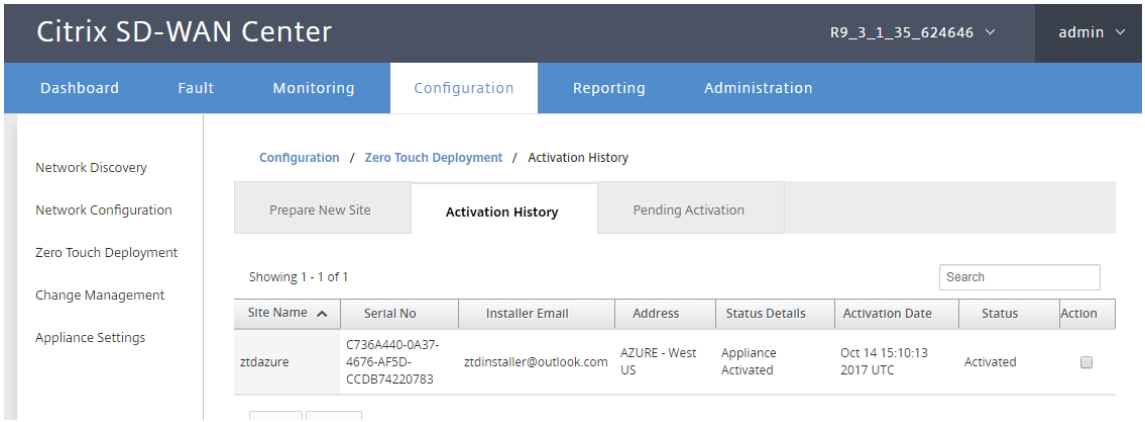
8. Une fois que chacune des étapes du service Cloud SD-WAN est automatiquement compliquée, connectez-vous à l'interface Web des instances SD-WAN à l'aide de l'adresse IP publique obtenue à partir du portail Azure.



9. La page Citrix SD-WAN Monitoring Statistics identifie la connectivité réussie du MCN à l'instance SD-WAN dans Azure.



10. En outre, la tentative de provisionnement réussie (ou infructueuse) sera consignée dans la page Historique des activations du Centre SD-WAN.



Paramètres du serveur proxy pour le déploiement sans intervention

February 17, 2022

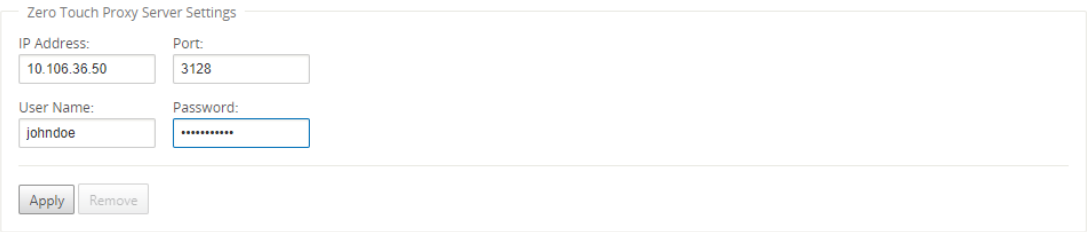
Comme condition préalable au déploiement sans intervention, le Citrix SD-WAN Center doit être connecté à Internet. Si votre centre Citrix SD-WAN est connecté à Internet via un serveur proxy, vous devez configurer les paramètres du serveur proxy sur le Centre Citrix SD-WAN.

> **Remarque**
>
> Ce paramètre de serveur proxy est utilisé uniquement pour le déploiement sans intervention.

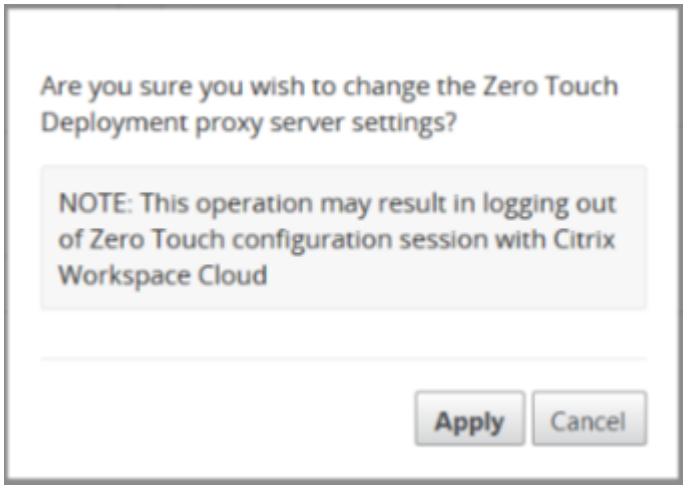
Pour configurer les paramètres du serveur proxy sans intervention :

1. Dans l'interface Web SD-WAN Center, accédez à **Administration** > **Paramètres généraux** > **Interface de gestion** .
2. Dans la section **Paramètres du serveur proxy Zero Touch**, 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 le champ **Nom d'utilisateur** et **Mot de passe** vide s'il n'y a pas d'authentification configurée sur le serveur proxy.



3. Cliquez sur **Appliquer**, une boîte de dialogue de confirmation s'affiche.

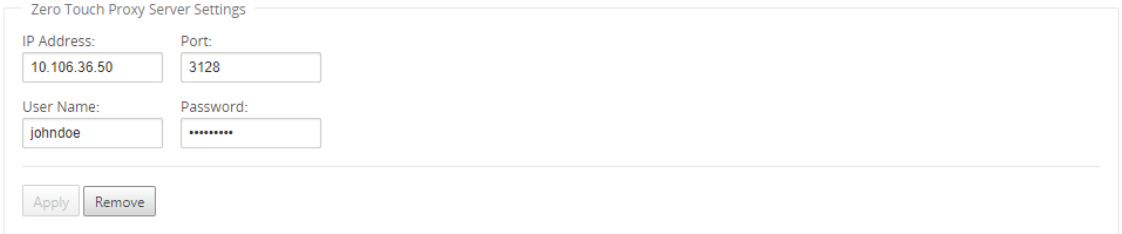


4. Cliquez sur **Apply**.

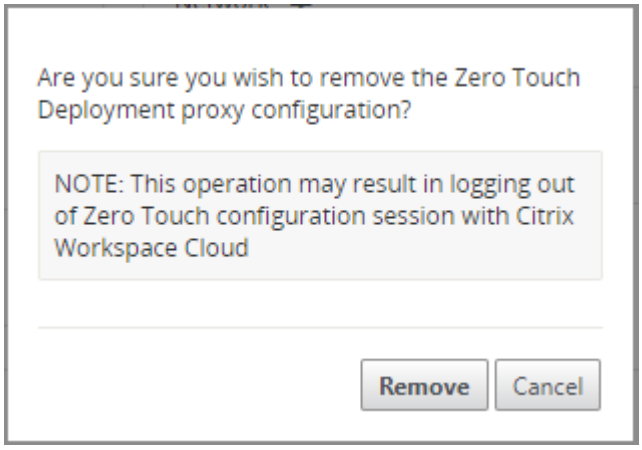
> **Remarque**
>
> Vous pouvez supprimer complètement les paramètres du serveur proxy, si Citrix SD-WAN Center est connecté directement à Internet. Vous pouvez également supprimer les paramètres du serveur proxy et configurer un autre serveur proxy, si nécessaire.

Pour supprimer les paramètres du serveur proxy :

1. Dans l'interface Web Citrix SD-WAN Center, accédez à **Administration** > **Paramètres généraux** > **Interface de gestion** .
2. Dans la section **Paramètres du serveur proxy Zero Touch**, cliquez sur **Supprimer**.



3. Cliquez sur **Supprimer**, une boîte de dialogue de confirmation s'affiche.



4. Cliquez sur **Supprimer**.

Intégration réseau Palo Alto

February 17, 2022

Les réseaux Palo Alto fournissent une infrastructure de sécurité basée sur le cloud pour la protection des réseaux distants. Il assure la sécurité en permettant aux organisations de configurer des pare-feu régionaux basés sur le cloud qui protègent la structure SD-WAN.

Le service Prisma Access pour les réseaux distants vous permet d'intégrer des emplacements réseau distants et d'assurer la sécurité des utilisateurs. Il élimine la complexité de la configuration et de la gestion des périphériques à chaque emplacement distant. Le service offre un moyen efficace d'ajouter facilement de nouveaux emplacements réseau distants et de minimiser les défis opérationnels en veillant à ce que les utilisateurs de ces sites soient toujours connectés et sécurisés. Il vous permet de gérer les stratégies de manière centralisée à partir de Panorama pour une sécurité cohérente et rationalisée pour vos emplacements réseau.

Pour connecter vos emplacements réseau distants au service Prisma Access, vous pouvez utiliser le pare-feu de nouvelle génération de Palo Alto Networks ou un périphérique tiers compatible IPSec incluant
SD-WAN, qui peut établir un tunnel IPsec vers le service.

- Planifier le service d'accès Prisma pour les réseaux distants
- Configurer le service d'accès Prisma pour les réseaux distants
- Réseaux distants intégrés avec importation de configuration

La solution Citrix SD-WAN offrait déjà la possibilité de sortir le trafic Internet de la succursale. Cela est essentiel pour offrir une expérience utilisateur plus fiable et à faible latence, tout en évitant l'in-

troduction d'une pile de sécurité coûteuse dans chaque succursale. Citrix SD-WAN et Palo Alto Networks offrent désormais aux entreprises distribuées un moyen plus fiable et plus sûr de connecter les utilisateurs des succursales aux applications dans le cloud.

Les appliances Citrix SD-WAN peuvent se connecter au réseau Palo Alto (Prisma Access Service) via des tunnels IPSec à partir d'emplacements d'appliances SD-WAN avec une configuration minimale. Vous pouvez configurer le réseau Palo Alto dans Citrix SD-WAN Center.

Avant de commencer à configurer le service d'accès Prisma pour les réseaux distants, assurez-vous que la configuration suivante est prête pour vous assurer que vous êtes en mesure d'activer le service et d'appliquer la stratégie pour les utilisateurs de vos emplacements réseau distants :

1. **Connexion de service** : si vos emplacements réseau distants nécessitent un accès à l'infrastructure de votre siège social pour authentifier les utilisateurs ou pour activer l'accès aux ressources réseau critiques, vous devez configurer Accès à votre réseau d'entreprise de sorte que le siège social et les emplacements réseau distants soient connecté.

Si l'emplacement réseau distant est autonome et n'a pas besoin d'accéder à l'infrastructure à d'autres emplacements, vous n'avez pas besoin de configurer la connexion de service (sauf si vos utilisateurs mobiles ont besoin d'un accès).

1. **Modèle** : le service Prisma Access crée automatiquement une pile de modèles (Remote_Network_Template_Stack) et un modèle de niveau supérieur (Remote_Network_Template) pour le service Prisma Access pour les réseaux distants. Pour configurer le service d'accès Prisma pour les réseaux distants, vous configurez le modèle de niveau supérieur à partir de zéro ou utilisez votre configuration existante, si vous exécutez déjà un pare-feu réseau Palo Alto sur site.

   Le modèle nécessite les paramètres pour établir la configuration du tunnel IPSec et de l'échange de clés Internet (IKE) pour la négociation de protocole entre votre emplacement réseau distant et le service Prisma Access pour les réseaux distants, les zones que vous pouvez référencer dans la stratégie de sécurité et un profil de transfert de journaux afin que vous peut transférer les journaux du service Prisma Access pour les réseaux distants vers le service de journalisation.

2. **Groupe de périphériques parent** : le service Prisma Access pour les réseaux distants nécessite que vous spécifiiez un groupe d'appareils parent qui inclut votre stratégie de sécurité, vos profils de sécurité et d'autres objets de stratégie (tels que les groupes et objets d'applications et les groupes d'adresses), ainsi qu'une stratégie d'authentification afin que le Le service Prisma Access pour réseaux distants peut appliquer de manière cohérente une stratégie pour le trafic routé via le tunnel IPsec vers le service Prisma Access pour les réseaux distants. Vous devez définir des règles et des objets de stratégie sur Panorama ou utiliser un groupe de périphériques existant pour sécuriser les utilisateurs dans l'emplacement réseau distant.

> **Remarque :**
>
> Si vous utilisez un groupe de périphériques existant qui référence des zones, assurez-vous d'ajouter le modèle correspondant qui définit les zones à Remote_Network_Template_Stack.

Cela vous permet de terminer le mappage de zone lorsque vous configurez le service d'accès Prisma pour les réseaux distants.

3. **Sous-réseaux IP** : pour que le service Prisma Access achemine le trafic vers vos réseaux distants, vous devez fournir des informations de routage pour les sous-réseaux que vous souhaitez sécuriser à l'aide du service Prisma Access. Vous pouvez définir un itinéraire statique vers chaque sous-réseau à l'emplacement réseau distant, ou configurer BGP entre vos emplacements de connexion de service et le service Prisma Access, ou utiliser une combinaison des deux méthodes.

   Si vous configurez à la fois des routes statiques et activez BGP, les routes statiques ont priorité. Bien qu'il puisse être pratique d'utiliser des routes statiques si vous n'avez que quelques sous-réseaux à vos emplacements distants, dans un déploiement volumineux avec de nombreux réseaux distants avec des sous-réseaux superposés, BGP vous permettra d'évoluer plus facilement.

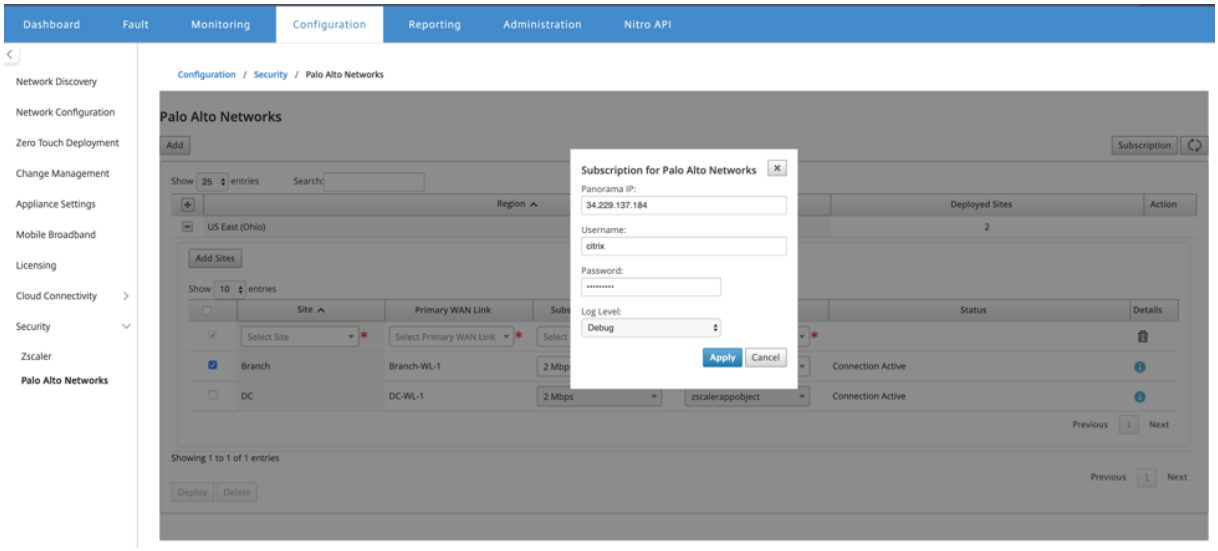
Réseau Palo Alto à SD-WAN Center

Assurez-vous que les conditions préalables suivantes sont remplies :

- Obtenir l'adresse IP panoramique du service PRISMA ACCESS.
- Obtenez le nom d'utilisateur et le mot de passe utilisateur dans le service PRISMA ACCESS.
- Configurez les tunnels IPSec dans l'interface graphique de l'appliance SD-WAN.
- Assurez-vous que le site n'est pas intégré à une région, qui a déjà un site différent configuré avec des profils ike/ipsec autres que Citrix-IKE-Crypto-Default/Citrix-IPsec-Crypto-Default/Crypto-Default.
- Assurez-vous que la configuration de Prisma Access n'est pas modifiée manuellement lorsque la configuration est mise à jour par SD-WAN Center.

Dans l'interface graphique du Centre Citrix SD-WAN, fournissez les informations d'abonnement à Palo Alto.

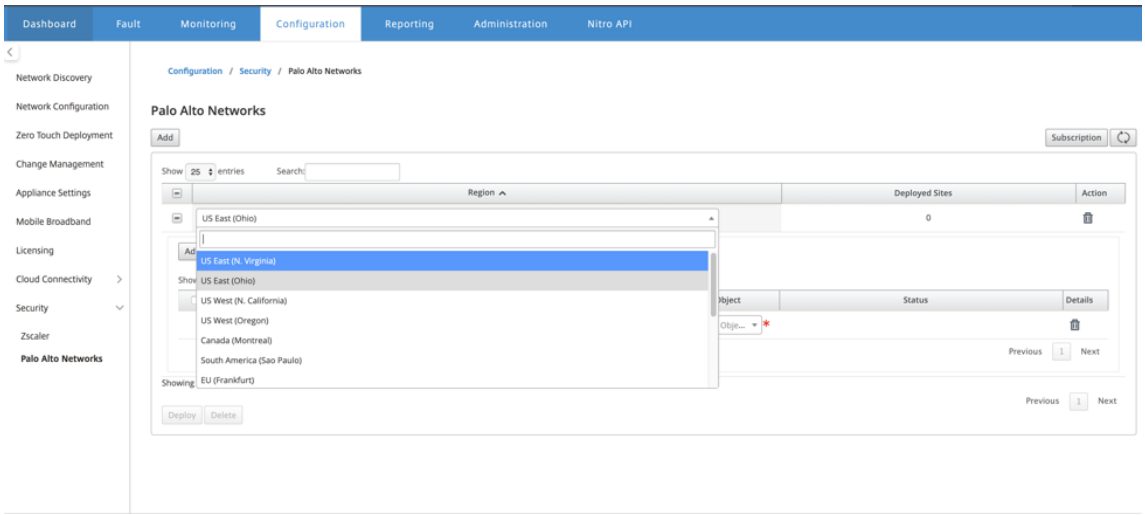
- Configurez l'adresse IP panoramique. Vous pouvez obtenir cette adresse IP auprès de Palo Alto (service PRISMA ACCESS).
- Configurez le nom d'utilisateur et le mot de passe utilisés dans le service PRISMA ACCESS.

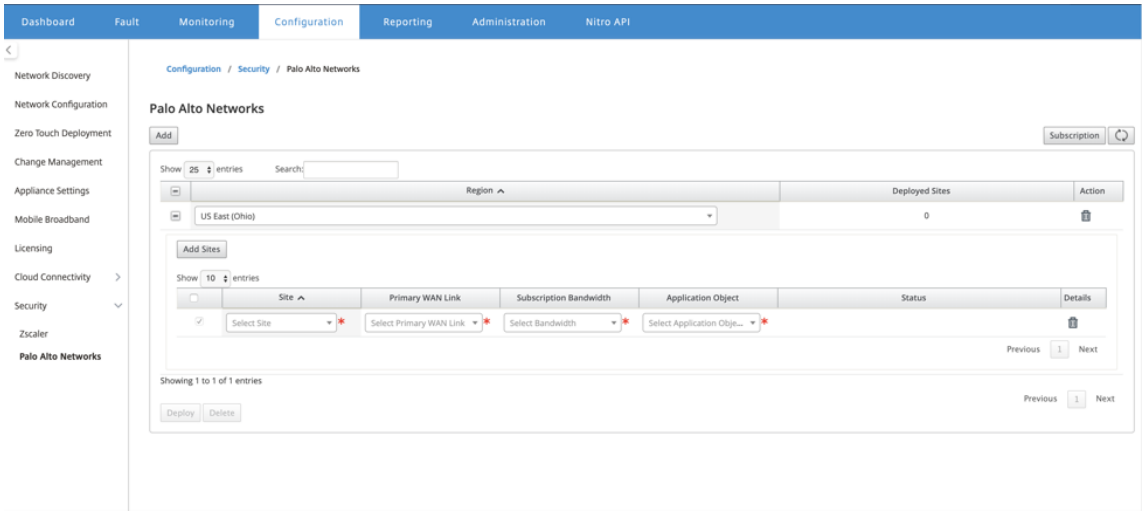


Ajouter et déployer des sites

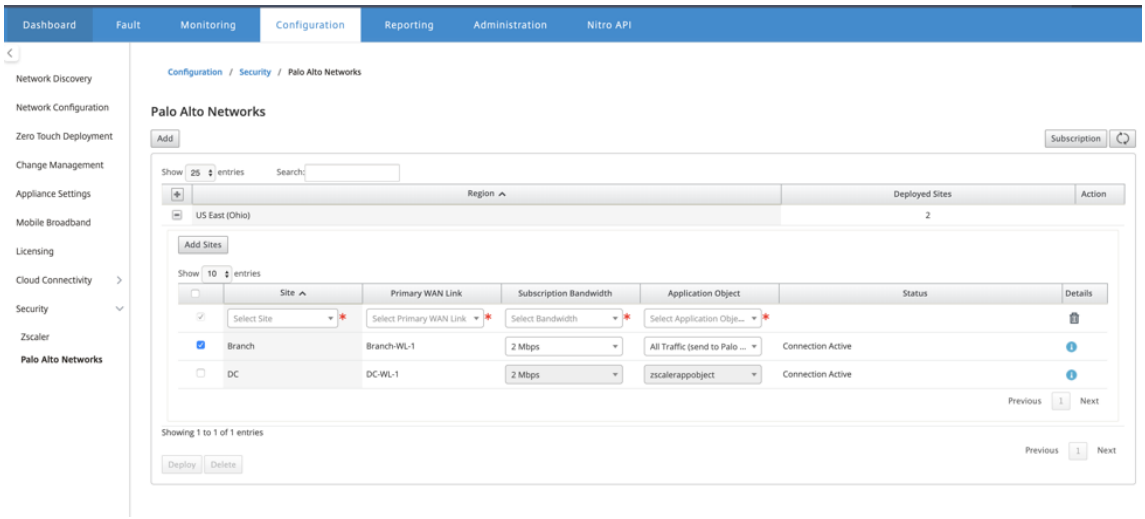
1. Pour déployer les sites, choisissez la région réseau PRISMA ACCESS et le site SD-WAN à configurer pour la région Prisma Access, puis sélectionnez la liaison WAN du site, la bande passante et l'objet d'application pour la sélection du trafic.

   > **Remarque :**
   >
   > Le flux de trafic est affecté si la bande passante sélectionnée dépasse la plage de bande passante disponible.
   >
   > Vous pouvez choisir de rediriger tout le trafic lié à Internet vers le service PRISMA ACCESS en sélectionnant l'option **Tout le trafic** sous la sélection d'objet Application.

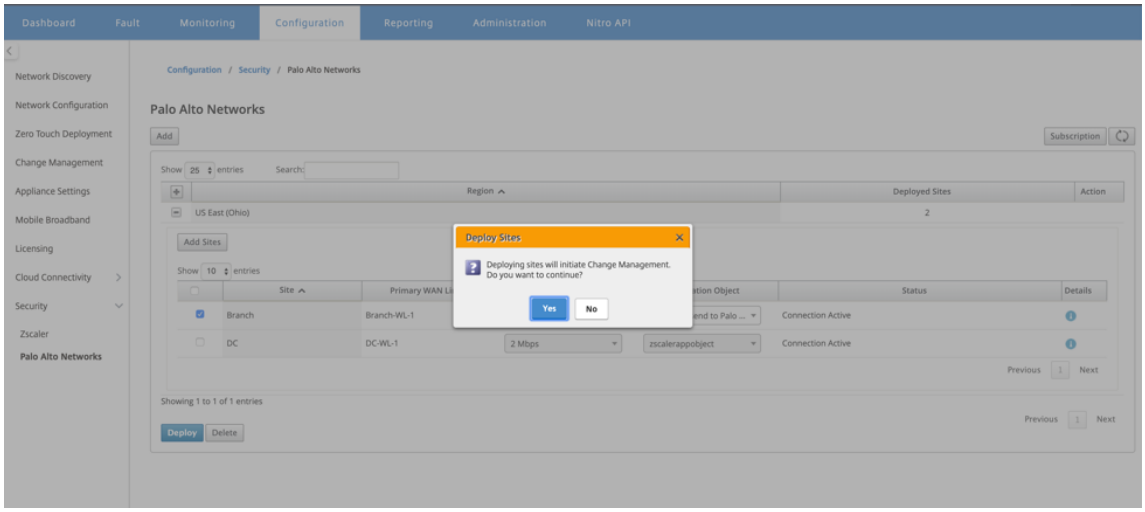




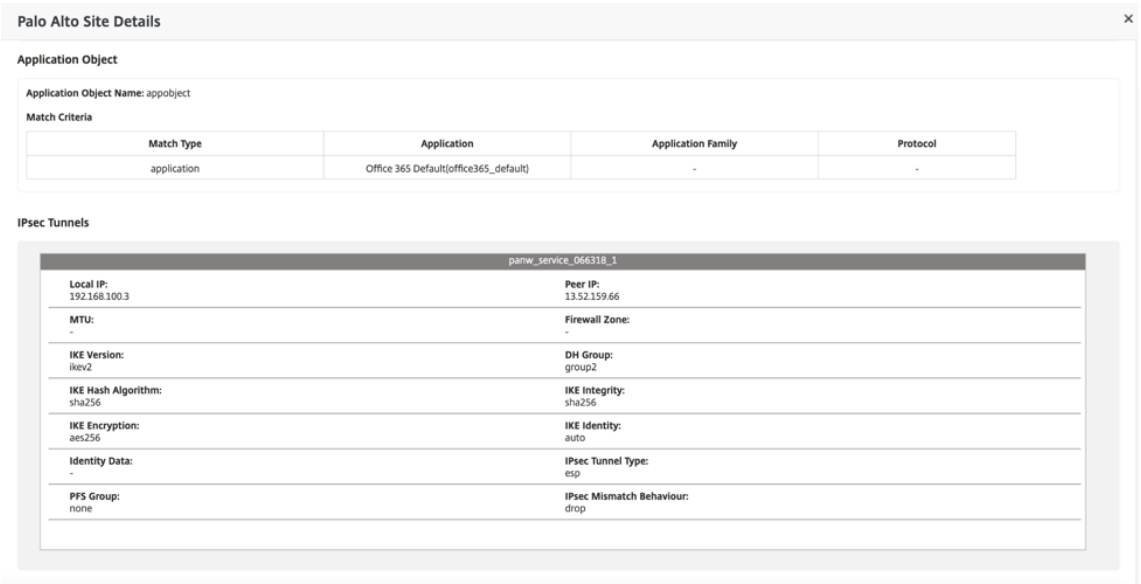
2. Vous pouvez continuer à ajouter d'autres sites de succursale SD-WAN selon vos besoins.



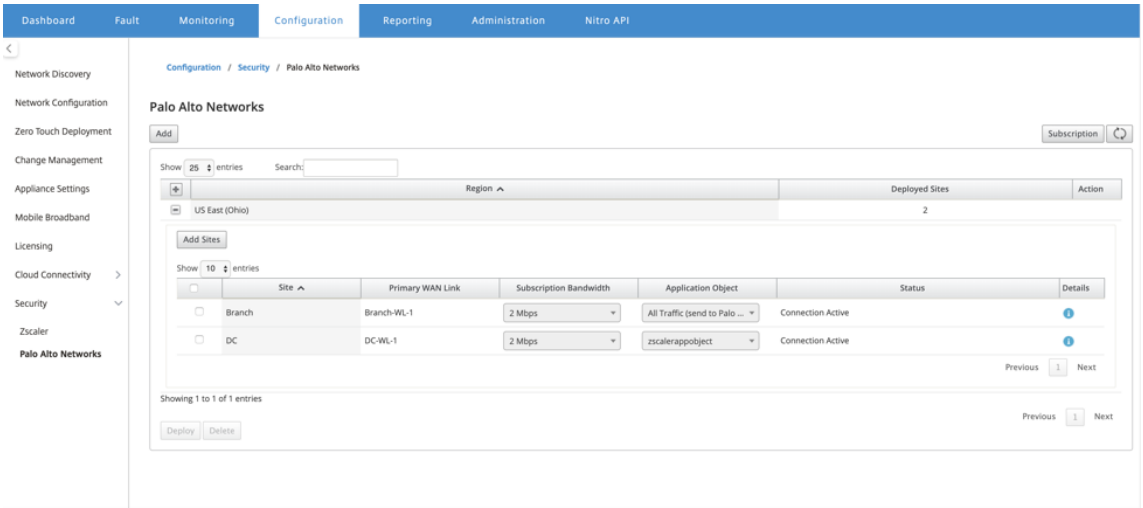
3. Cliquez sur **Déployer**. Le processus de gestion du changement est lancé. Cliquez sur **Oui** pour continuer.



Après le déploiement, la configuration du tunnel IPSec utilisée pour établir les tunnels est la suivante.



La page de destination affiche la liste de tous les sites configurés et regroupés sous différentes régions SD-WAN.



Vérifiez la connexion du trafic de bout en bout :

- À partir du sous-réseau LAN de la branche, accéder aux ressources Internet.
- Vérifiez que le trafic passe par le tunnel IPsec Citrix SD-WAN vers l'accès Palo Alto Prisma.
- Vérifiez que la stratégie de sécurité Palo Alto est appliquée sur le trafic sous l'onglet Surveillance.
- Vérifiez que la réponse d'Internet à l'hôte d'une succursale arrive.

WAN virtuel Microsoft Azure

February 17, 2022

Microsoft Azure Virtual WAN et Citrix SD-WAN fournissent une connectivité réseau simplifiée et une gestion centralisée des charges de travail du cloud hybride. Vous pouvez automatiser la configuration des appliances de succursale pour vous connecter au réseau étendu Azure et configurer les stratégies de gestion du trafic de succursale en fonction des besoins de votre entreprise. L'interface intégrée du tableau de bord fournit des informations de dépannage instantanées qui peuvent gagner du temps et fournir une visibilité pour une connectivité site à site à grande échelle.

Microsoft Azure Virtual WAN vous permet d'activer une connectivité simplifiée aux charges de travail Azure Cloud et d'acheminer le trafic sur le réseau de base Azure et au-delà. Azure fournit plus de 54 régions et plusieurs points de présence dans le monde entier. Les régions Azure servent de hubs que vous pouvez choisir de vous connecter aux succursales. Une fois les succursales connectées, utilisez le service cloud Azure via la connectivité Hub-to-Hub. Vous pouvez simplifier la connectivité en appliquant plusieurs services Azure, y compris l'appairage Hub avec les réseaux virtuels Azure. Les hubs servent de passerelles de circulation pour les succursales.

Microsoft Azure Virtual WAN offre les avantages suivants :

- Solutions de connectivité intégrées dans le hub et le rayon : automatisez la connectivité et la configuration de site à site entre le hub local et Azure à partir de diverses sources, y compris des solutions partenaires connectés.
- Configuration et configuration automatisées : connectez vos réseaux virtuels au Hub Azure en toute transparence.
- Dépannage intuitif : vous pouvez voir le flux de bout en bout dans Azure et utiliser ces informations pour effectuer les actions requises.

Communication Hub-to-Hub

À partir de la version 11.1.0, Azure Virtual WAN est pris en charge la communication Hub-to-Hub en utilisant la méthode de type **Standard**.

Les clients Azure Virtual WAN peuvent désormais tirer parti du réseau central mondial de Microsoft pour la communication entre les régions Hub-to-Hub (architecture de réseau de transit mondial). Cela permet la communication de succursale vers Azure, de succursale à succursale sur l'épine dorsale Azure et de communication de succursale à hub (dans toutes les régions Azure).

Vous ne pouvez tirer parti de l'épine dorsale d'Azure pour la communication interrégionale que lorsque vous achetez le SKU standard pour le WAN virtuel Azure. Pour plus de détails sur la tarification, consultez la section Tarification Vir Avec le SKU de base, vous ne pouvez pas utiliser l'épine

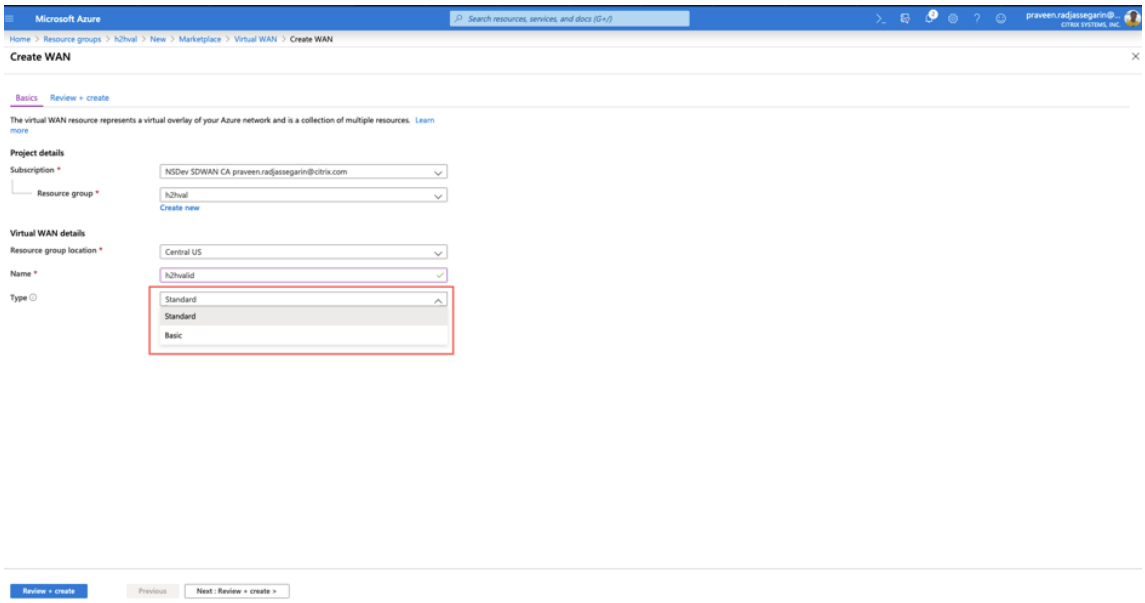
dorsale d'Azure pour la communication entre les régions Hub-to-Hub. Pour plus de détails, consultez Architecture du réseau de transit mondial et Virtual WAN.

Les concentrateurs sont tous connectés les uns aux autres dans un WAN virtuel. Cela implique qu'une succursale, un utilisateur ou un réseau virtuel connecté à un concentrateur local peut communiquer avec une autre succursale ou un réseau virtuel en utilisant l'architecture maillée complète des concentrateurs connectés.

Vous pouvez également connecter des réseaux virtuels au sein d'un concentrateur passant par le hub virtuel, et des réseaux virtuels à travers le hub, à l'aide de la structure connectée hub-to-hub.

Il existe deux types de WAN virtuel :

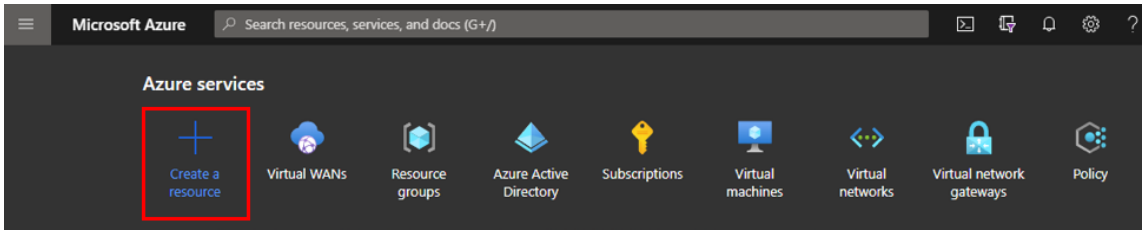
- **De base** : à l'aide de la méthode **Basic**, les communications Hub-to-Hub se produisent dans une région. Le type WAN **de base** permet de créer un concentrateur de base (SKU = Basic). Les concentrateurs de base sont limités à la fonctionnalité VPN de site à site.
- **Standard** : à l'aide de la méthode **standard**, les communications entre hub-to-hub se produisent entre différentes régions. Un WAN **standard** permet de créer un concentrateur standard (SKU = Standard). Les concentrateurs**standard** contiennent ExpressRoute, User VPN (P2S), hub maillé complet et VNET-to-VNET transit via les concentrateurs.



Créer un service WAN virtuel Azure dans Microsoft Azure

Pour créer la ressource WAN virtuel Azure, effectuez les opérations suivantes :

1. Connectez-vous au portail Azure et cliquez sur **Créer une ressource**.

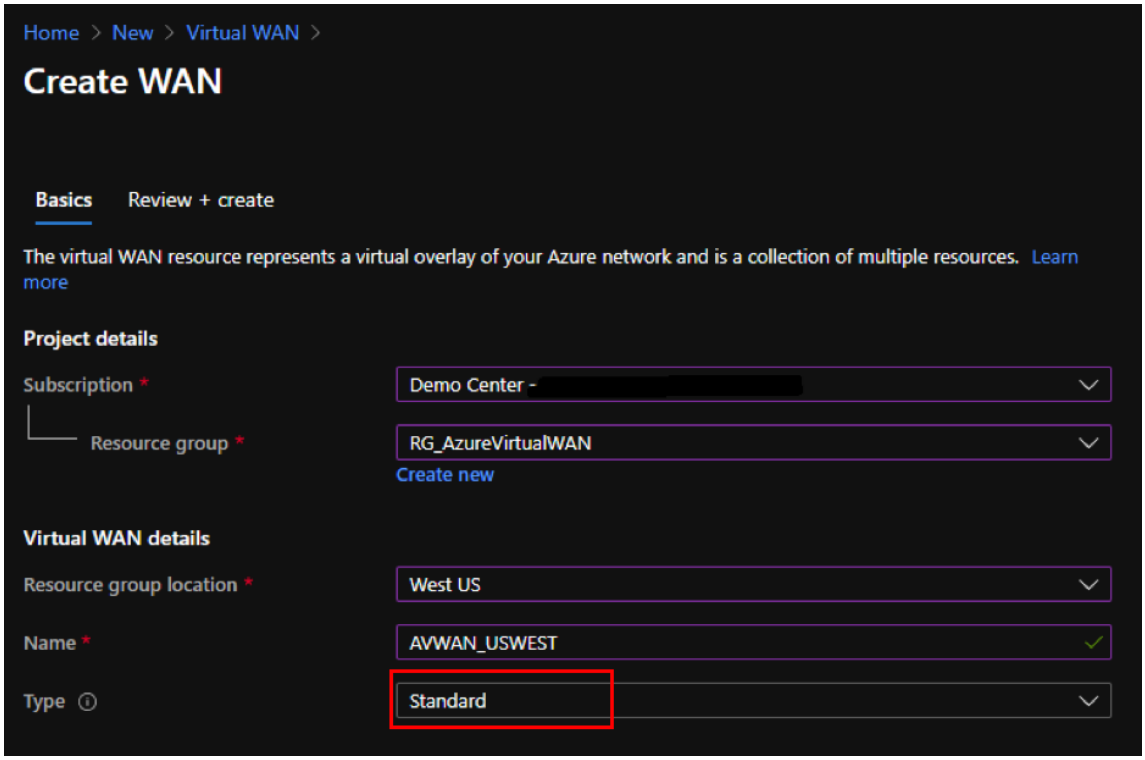


2. Recherchez **Virtual WAN** et cliquez sur **Créer**.
3. Sous **Base**, indiquez les valeurs pour les champs suivants :

   - **Abonnement** : sélectionnez et fournissez les détails de l'abonnement dans la liste déroulante.
   - **Groupe de ressources** : sélectionnez un groupe de ressources existant ou créez-en un nouveau.

     > **Remarque**
     >
     > Lors de la création du principal de service pour autoriser la communication API Azure, assurez-vous d'utiliser le même groupe de ressources qui contient le WAN virtuel. Sinon, SD-WAN Orchestrator ne dispose pas des autorisations suffisantes pour s'authentifier auprès des API Azure Virtual WAN qui activent la connectivité automatisée.

   - **Emplacement du groupe de ressources** : sélectionnez la région Azure dans la liste déroulante.
   - **Nom** : Indiquez le nom du nouveau réseau étendu virtuel.
   - **Type** : sélectionnez Type **standard** si vous souhaitez utiliser la communication Hub-to-Hub entre différentes régions, sinon sélectionnez **Basic**.



4. Cliquez sur **Réviser + Créer**.
5. Vérifiez les détails que vous avez saisis pour créer le WAN virtuel et cliquez sur **Créer** pour terminer la création du réseau étendu virtuel.

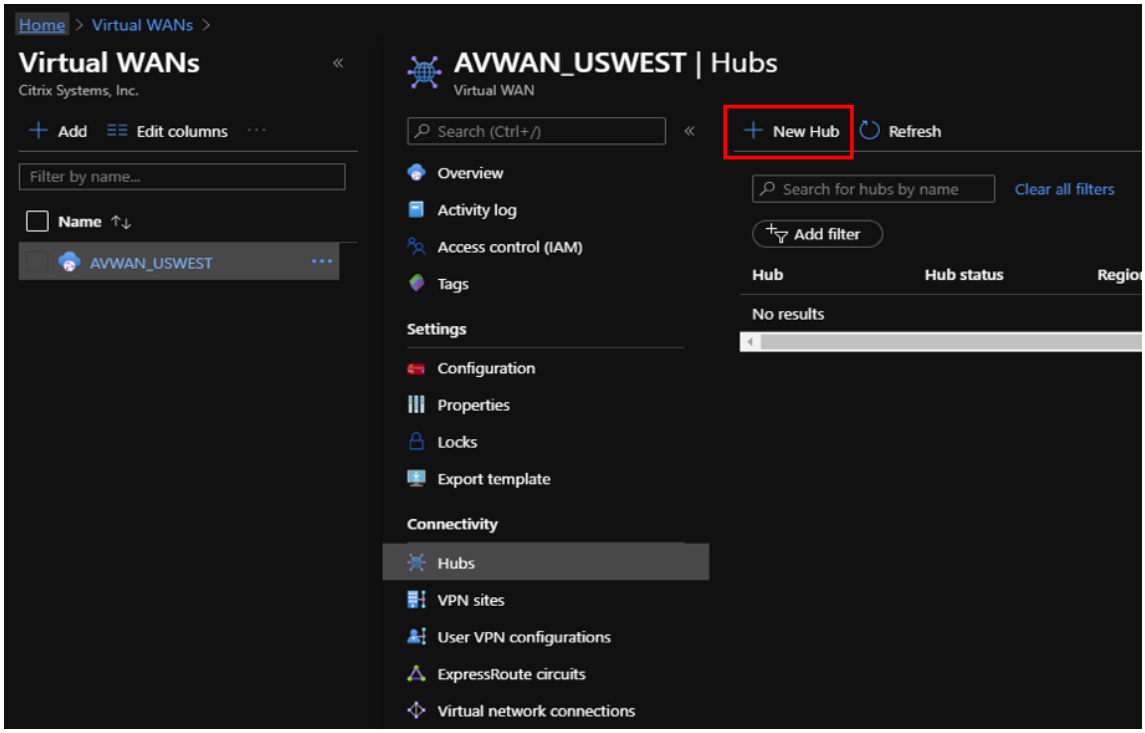
Le déploiement de la ressource prend moins d'une minute.

> **Remarque**
>
> Vous pouvez effectuer une mise à niveau de base vers Standard, mais vous ne pouvez pas revenir de Standard à Basic. Pour connaître les étapes à suivre pour mettre à niveau un réseau étendu virtuel, reportez-vous à la section Mettre à niveau un réseau étendu virtuel de base

Créer un concentrateur dans le WAN virtuel Azure

Procédez comme suit pour créer un concentrateur afin d'activer la connectivité à partir de différents points de terminaison (par exemple, des périphériques VPN locaux ou des périphériques SD-WAN) :

1. Sélectionnez le WAN virtuel Azure créé précédemment.
2. Sélectionnez **Hubs** sous la section **Connectivité**, puis cliquez sur **+ Nouveau Hub**.

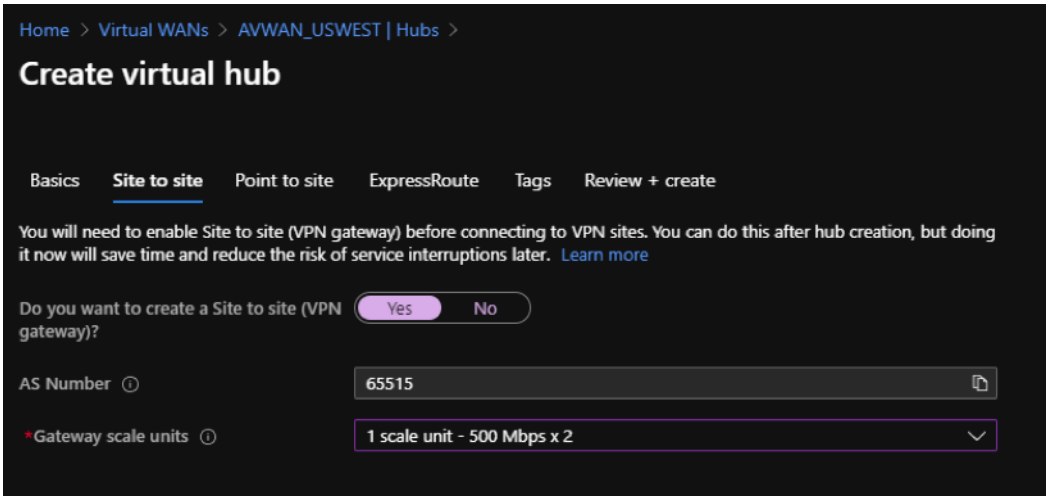


3. Sous **Base**, indiquez les valeurs pour les champs suivants :

   - **Région** : sélectionnez la région Azure dans la liste déroulante.
   - **Nom** —Entrez le nom du nouveau Hub.
   - **Espace d'adressage privé Hub** —Entrez la plage d'adresses dans CIDR. Sélectionnez un réseau unique dédié au concentrateur uniquement.

4. Cliquez sur **Suivant : Site à Site >** et indiquez les valeurs pour les champs suivants :

   - **Voulez-vous créer un site à site (passerelle VPN) ?** —Sélectionnez **Oui**.
   - **Unités d'échelle de passerelle** : sélectionnez les unités d'échelle dans la liste déroulante selon les besoins.



5. Cliquez sur **Réviser + Créer**.
6. Vérifiez les paramètres et cliquez sur **Créer** pour démarrer la création du hub virtuel.

Le déploiement de la ressource peut prendre jusqu'à 30 minutes.

Créer un principal de service pour Azure Virtual WAN et identifier les ID

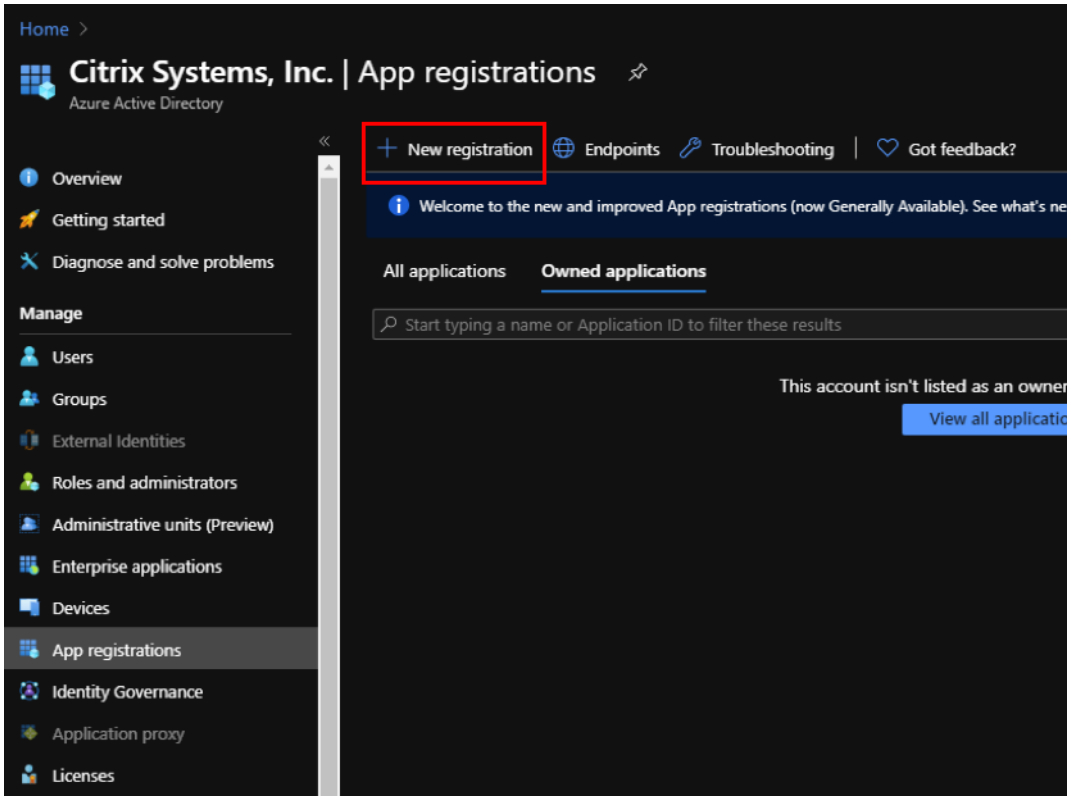
Pour que SD-WAN Orchestrator puisse s'authentifier via des API WAN virtuelles Azure et activer la connectivité automatisée, une application enregistrée doit être créée et identifiée avec les informations d'identification suivantes :

- ID d'abonnement
- ID client
- Clé secrète client
- ID de locataire

> **Remarque**
>
> Lors de la création du principal de service pour autoriser la communication API Azure, assurez-vous d'utiliser le même groupe de ressources qui contient le WAN virtuel. Sinon, SD-WAN Orchestrator ne dispose pas des autorisations suffisantes pour s'authentifier auprès des API Azure Virtual WAN qui activent la connectivité automatisée.

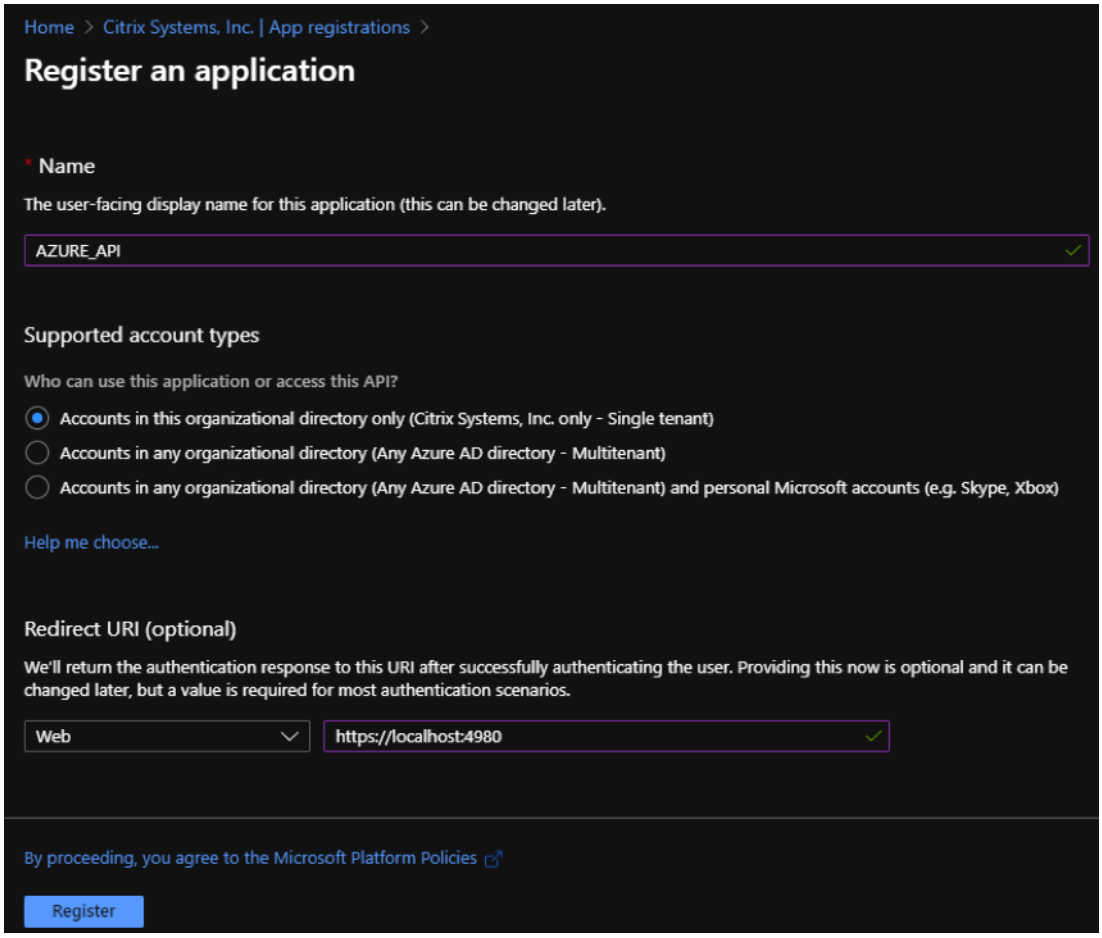
Procédez comme suit pour créer une nouvelle inscription d'application :

1. Dans le portail Azure, accédez à **Azure Active Directory**.
2. Sous Gérer, sélectionnez **Enregistrement de l'application**.
3. Cliquez sur **+ Nouvelle inscription**.

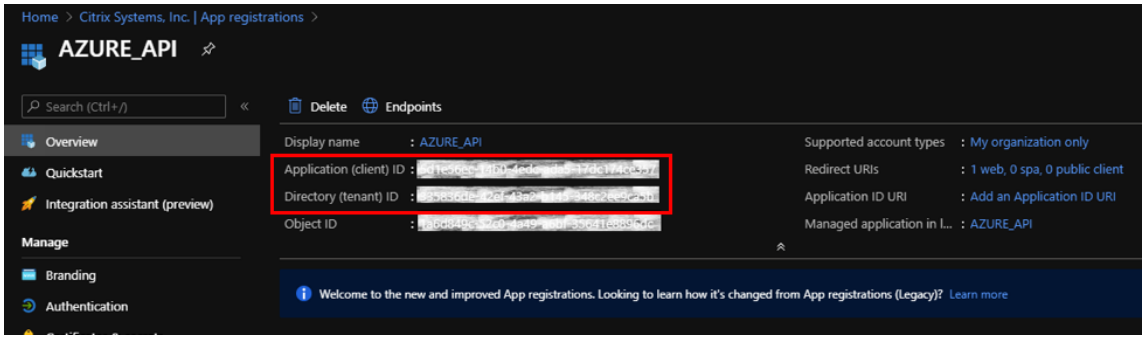


4. Fournissez des valeurs pour les champs suivants pour enregistrer une application :

   - **Nom** —Indiquez le nom de l'enregistrement de la demande.
   - **Types de compte pris en charge** : sélectionnez Comptes dans ce répertoire organisationnel uniquement (* - locataire unique) option.
   - **URI de redirection (facultatif)** : sélectionnez Web dans la liste déroulante et entrez une URL unique et aléatoire (par exemple, https:// localhost:4980)
   - Cliquez sur **Enregistrer**.



Vous pouvez copier et stocker l'ID **d'application (client) et l'ID** d'**annuaire (locataire)** qui peuvent être utilisés dans SD-WAN Orchestrator pour l'authentification à l'abonnement Azure pour l'utilisation de l'API.



L'étape suivante pour l'enregistrement de l'application, créez une clé principale de service à des fins d'authentification.

Pour créer la clé principale de service, effectuez les opérations suivantes :

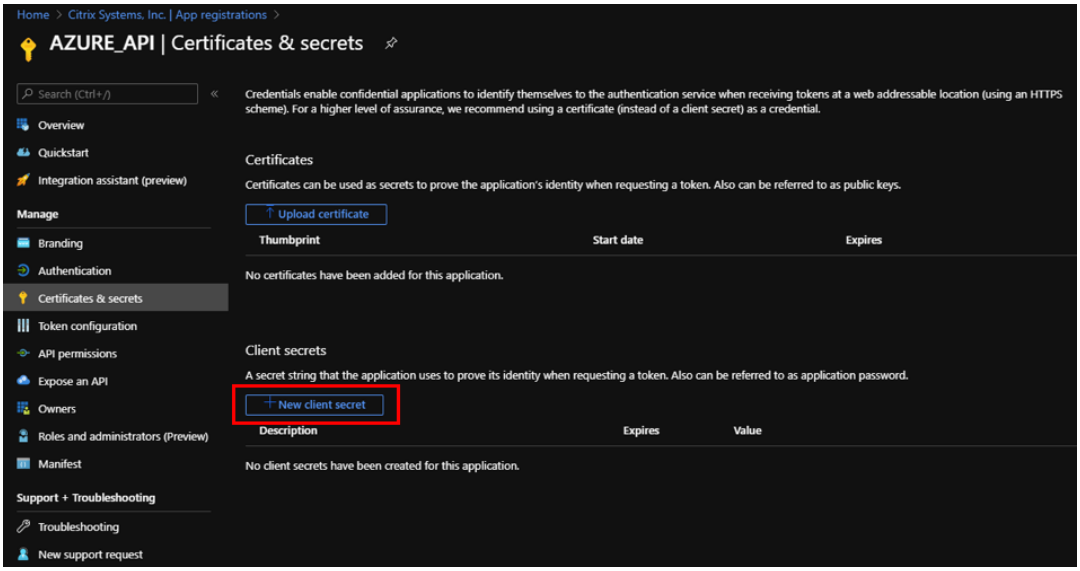
a) Dans le portail Azure, accédez à **Azure Active Directory**.

b) Sous **Gérer**, accédez à **Enregistrement des applications**.

c) Sélectionnez l'application enregistrée (créée précédemment).

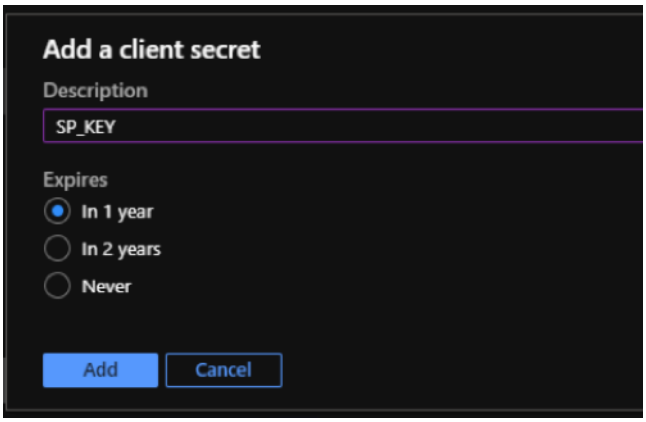
d) Sous **Gérer**, sélectionnez **Certificats et secrets**.

e) Sous **Secrets client**, cliquez sur **+ Nouveau secret client**.



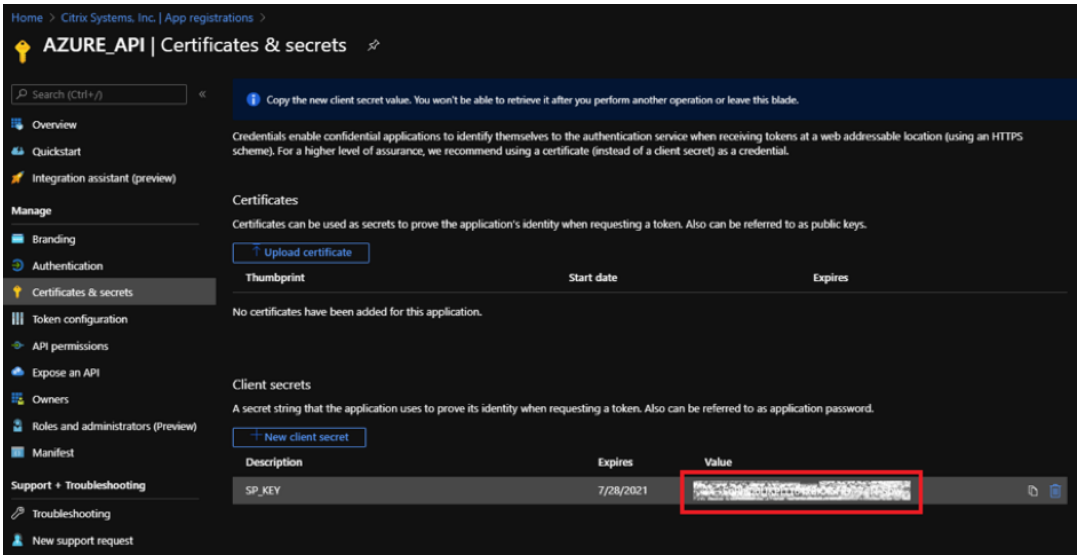
f) Pour ajouter un secret client, fournissez des valeurs pour les champs suivants :

- **Description** : Indiquez un nom pour la clé principale de service.
- **Expiration** : sélectionnez la durée d'expiration selon les besoins.



g) Cliquez sur **Ajouter**.

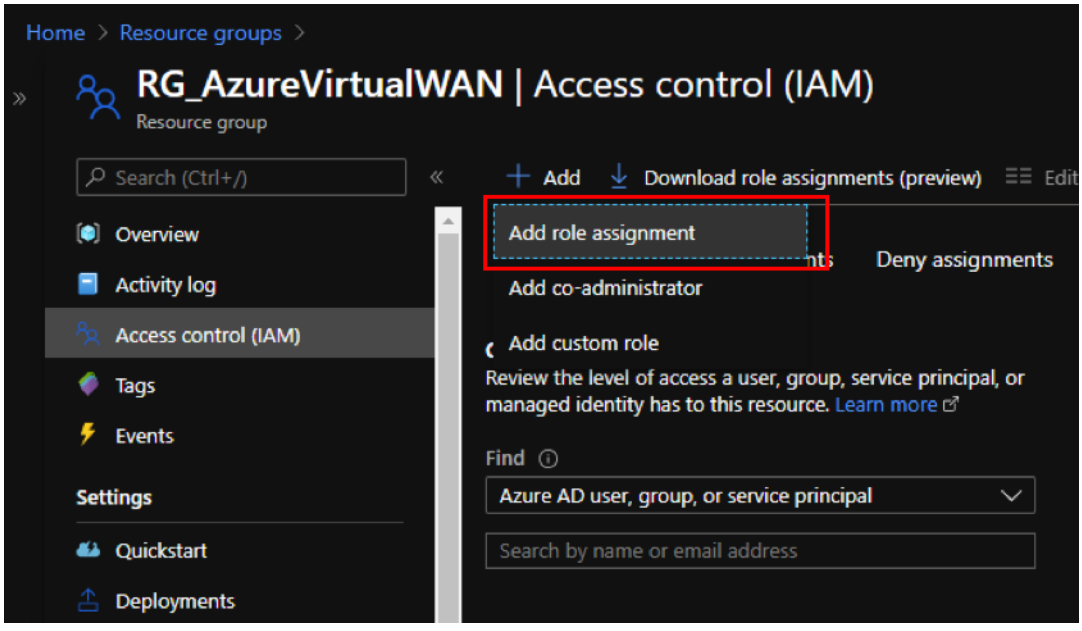
h) Le secret client est désactivé dans la colonne **Valeur**. Copiez la clé dans votre presse-papiers. Il s'agit du secret client que vous devez entrer dans SD-WAN Orchestrator.



> **Remarque**
>
> Vous devez copier et stocker la valeur de clé secrète avant de recharger la page car elle ne sera plus affichée par la suite.

Procédez comme suit pour attribuer les rôles appropriés à des fins d'authentification :

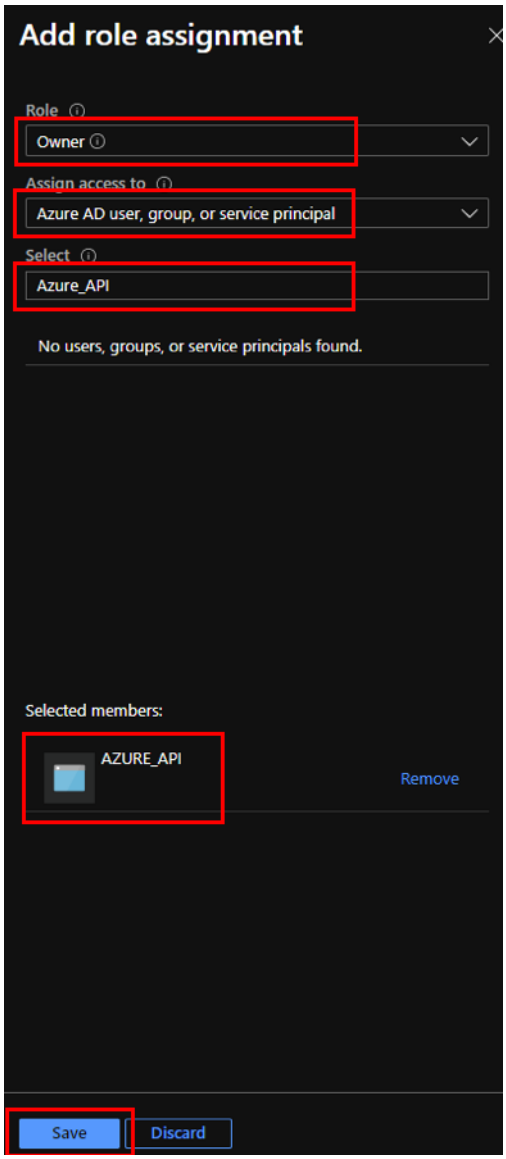
1. Dans le portail Azure, accédez au **groupe de ressources** où le WAN virtuel a été créé.
2. Accédez à **Contrôle d'accès (IAM)**.
3. Cliquez sur **+ Ajouter** et sélectionnez **Ajouter une affectation de rôle**.



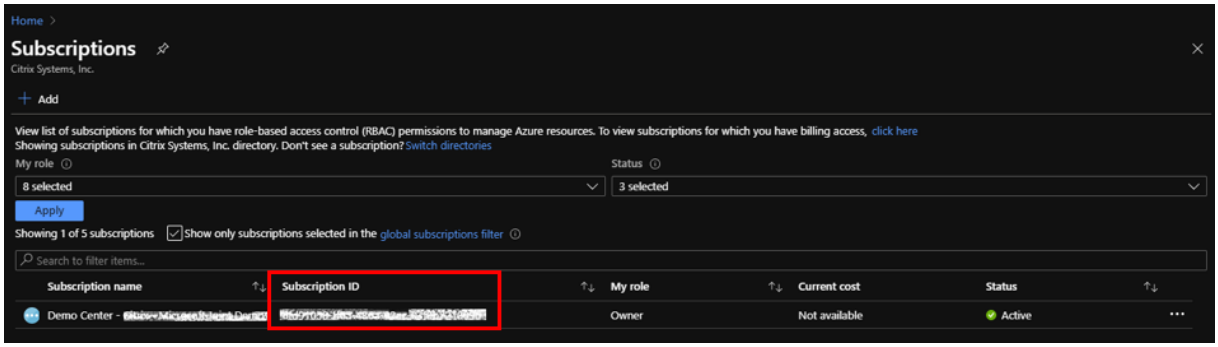
4. Pour ajouter une attribution de rôle, fournissez des valeurs pour les champs suivants :

- **Rôle** —Sélectionnez Propriétaire dans la liste déroulante. Ce rôle permet de gérer tout, y compris l'accès aux ressources.
- **Attribuer l'accès à** : sélectionnez **l'utilisateur, le groupe ou le**principal de service**Azure AD**.
- **Sélectionner** —Indiquez le nom de l'application enregistrée créée précédemment et sélectionnez l'entrée correspondante lorsqu'elle apparaît.

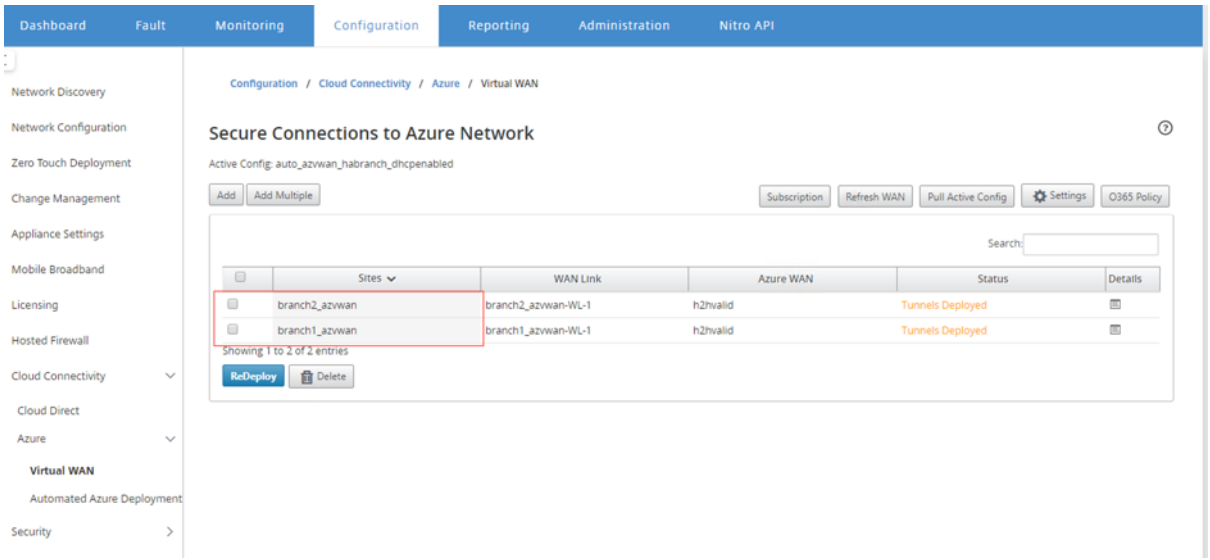
5. Cliquez sur **Save**.



Enfin, vous devez obtenir l'ID d'abonnement pour le compte Azure. Vous pouvez identifier votre **ID d'abonnement** en recherchant des abonnements dans le portail Azure.



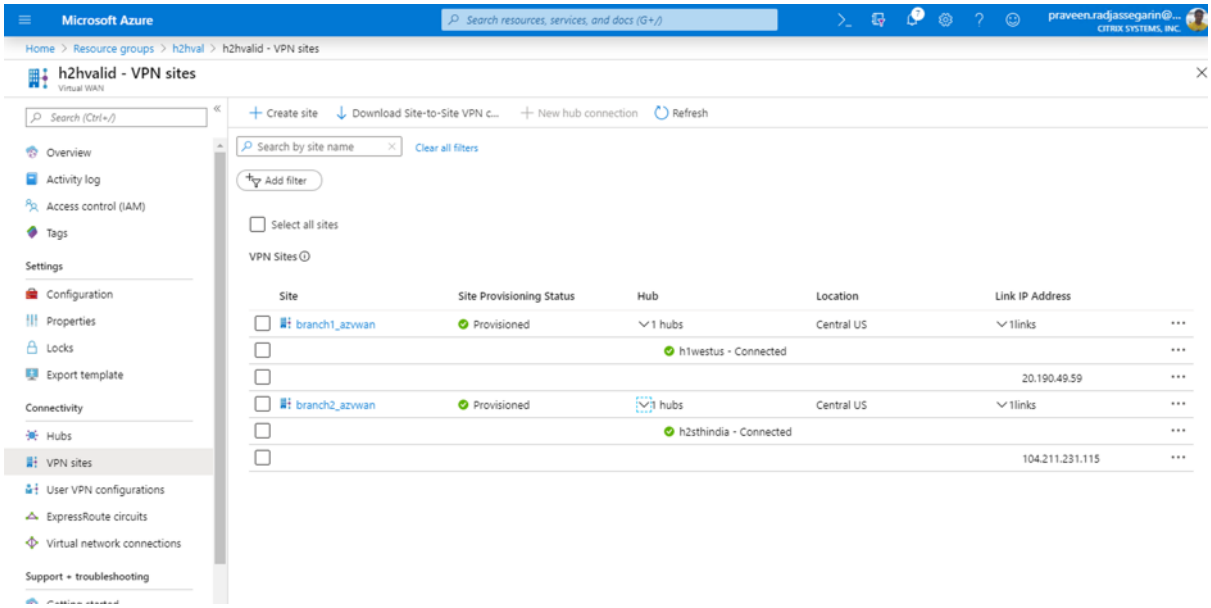
Une fois que vous avez créé le WAN virtuel, connectez-vous à l'**interface utilisateur du SD-WAN Center > Configuration > Azure > WAN virtuel**.



Sélectionnez deux sites différents et démarrez le déploiement. Une fois les sites déployés, vous pouvez associer les deux sites à deux concentrateurs différents.

> **REMARQUE**
>
> Par défaut branche à branche et BGP est désactivé. Vous pouvez créer un itinéraire statique ou activer la connectivité BGP (sous Paramètres) et branche à branche.

Activez la case à cocher BGP et branche à branche et déployez les tunnels. Une fois les tunnels déployés avec succès, vous pouvez vérifier l'état dans **Microsoft Azure > Groupes de ressources** sélectionnez le **groupe de ressources** que vous avez créé et cliquez sur **Sites VPN**.



Utilisation de Citrix SD-WAN pour se connecter à Microsoft Azure Virtual WAN

February 17, 2022

Pour que les périphériques locaux se connectent à Azure, un contrôleur est requis. Un contrôleur ingère des API Azure pour établir une connectivité de site à site avec le WAN Azure et un Hub.

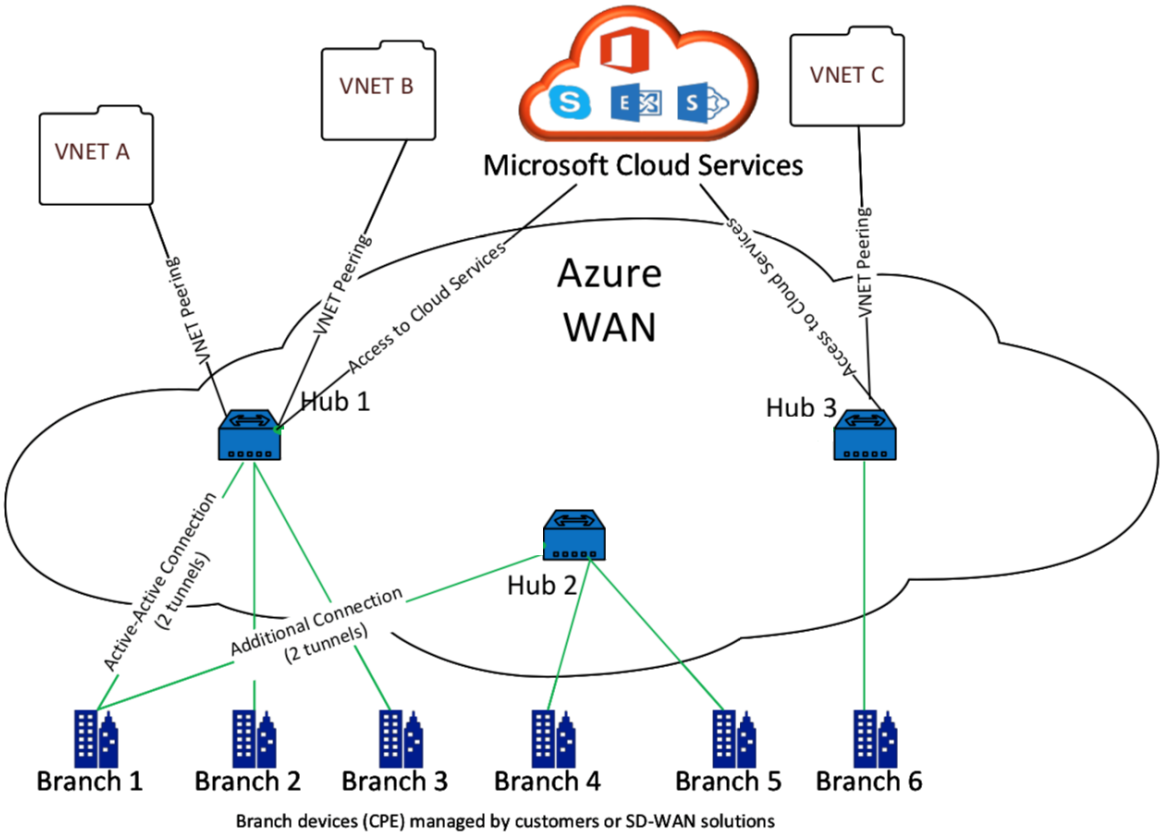
Microsoft Azure Virtual WAN inclut les composants et ressources suivants :

- WAN : représente l'ensemble du réseau dans Microsoft Azure. Il contient des liens vers tous les Hubs que vous souhaitez avoir dans ce WAN. Les réseaux locaux sont isolés les uns des autres et ne peuvent pas contenir de hub commun, ni de connexions entre deux concentrateurs dans des réseaux locaux différents.
- Site : Représente votre périphérique VPN local et ses paramètres. Un site peut se connecter à plusieurs hubs. À l'aide de Citrix SD-WAN, vous pouvez disposer d'une solution intégrée pour exporter automatiquement ces informations vers Azure.
- Hub : représente le noyau de votre réseau dans une région spécifique. Le Hub contient différents points de terminaison de service pour activer la connectivité et d'autres solutions à votre réseau local. Les connexions de site à site sont établies entre les Sites à un point de terminaison VPN Hubs.
- Connexion réseau virtuel Hub : le réseau Hub connecte le Hub virtuel WAN Hub Azure de manière transparente à votre réseau virtuel. Actuellement, la connectivité aux réseaux virtuels

qui se trouvent dans la même région Virtual Hub est disponible.

- Succursale : Les succursales sont les appliances Citrix SD-WAN locales, qui existent dans les bureaux clients. Un contrôleur SD-WAN gère les branches de manière centralisée. La connexion provient de derrière ces succursales et se termine dans Azure. Le contrôleur SD-WAN est responsable de l'application de la configuration requise à ces succursales et à Azure Hubs.

L'illustration suivante décrit les composants Virtual WAN :



Comment fonctionne Microsoft Azure Virtual WAN

1. Le SD-WAN Center est authentifié à l'aide de la fonctionnalité d'accès principal de service, principal ou rôle, qui est activée dans l'interface graphique Azure.
2. Le SD-WAN Center obtient la configuration de connectivité Azure et met à jour le périphérique local. Cela automatise le téléchargement, la modification et la mise à jour de la configuration du périphérique sur site.
3. Une fois que le périphérique a la configuration Azure correcte, une connexion site à site (deux tunnels IPSec actifs) est établie au WAN Azure. Azure nécessite le connecteur de périphérique de succursale pour prendre en charge les paramètres IKEv2. La configuration BGP est facultative.

Remarque : Les paramètres IPsec pour l'établissement de tunnels IPsec sont normalisés.

IPSec, propriété	Paramètre
Algorithme de chiffrement Ike	AES 256
Algorithme d'intégrité Ike	SHA 256
Groupe Dh	DH2
Algorithme de chiffrement IPsec	GCM AES 256
Algorithme d'intégrité IPsec	GCM AES 256
Groupe PFS	Aucune

Azure Virtual WAN automatise la connectivité entre le réseau virtuel de charge de travail et le concentrateur. Lorsque vous créez une connexion réseau virtuel Hub, elle définit la configuration appropriée entre le concentrateur provisionné et le réseau virtuel des charges de travail (VNET).

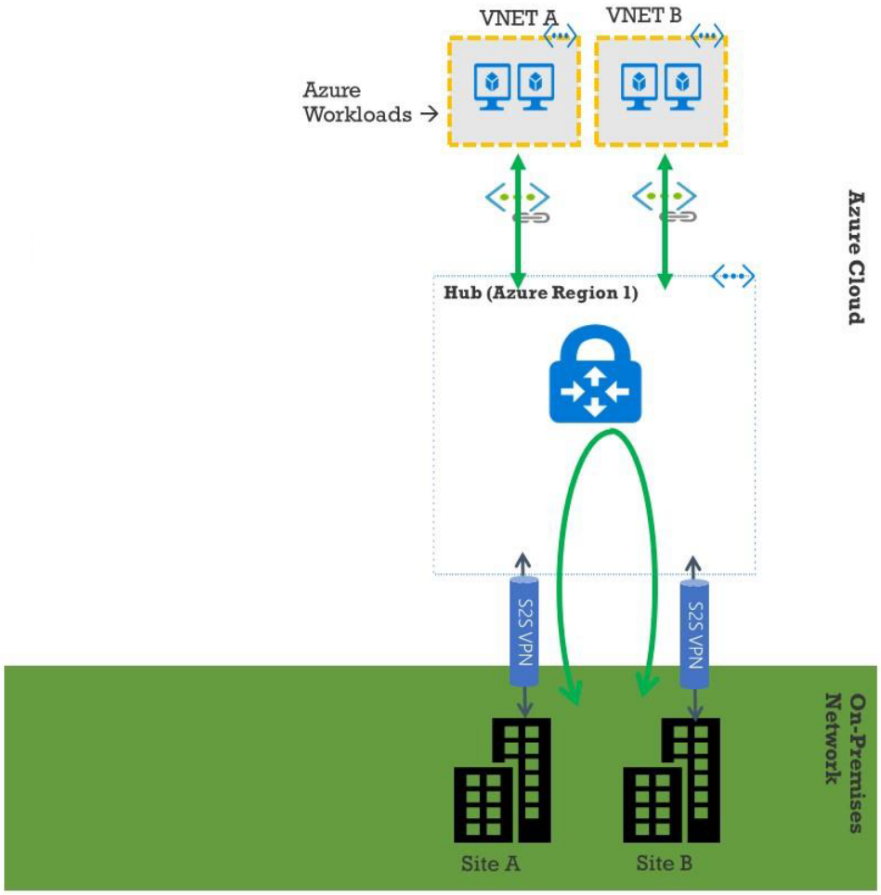
Prérequis et exigences

Lisez les exigences suivantes avant de procéder à la configuration d'Azure et SD-WAN pour gérer les sites de succursales se connectant aux hubs Azure.

1. Avoir un abonnement Azure sur liste blanche pour Virtual WAN.
2. Disposez d'une appliance sur site telle qu'une appliance SD-WAN pour établir IPsec dans les ressources Azure.
3. Avoir des liens Internet avec des adresses IP publiques. Bien qu'une seule liaison Internet soit suffisante pour établir une connectivité dans Azure, vous avez besoin de deux tunnels IPSec pour utiliser la même liaison WAN.
4. Contrôleur SD-WAN : un contrôleur est l'interface responsable de la configuration des appliances SD-WAN pour la connexion à Azure.
5. VNET dans Azure qui a au moins une charge de travail. Par exemple, une machine virtuelle, qui héberge un service. Considérez les points suivants :

    a) Le réseau virtuel ne doit pas posséder de passerelle VPN Azure ou Express Route, ni d' appliance virtuelle réseau.
    b) Le réseau virtuel ne doit pas disposer d'un itinéraire défini par l'utilisateur, qui achemine le trafic vers un réseau virtuel non virtuel WAN pour la charge de travail accessible à partir de la branche locale.
    c) Les autorisations appropriées pour accéder à la charge globale doivent être configurées. Par exemple, l'accès SSH au port 22 pour une machine virtuelle ubuntu.

Le diagramme suivant illustre un réseau avec deux sites et deux réseaux virtuels dans Microsoft Azure.



Configurer Microsoft Azure Virtual WAN

Pour que les branches SD-WAN sur site puissent se connecter à Azure et accéder aux ressources via des tunnels IPsec, les étapes suivantes doivent être effectuées.

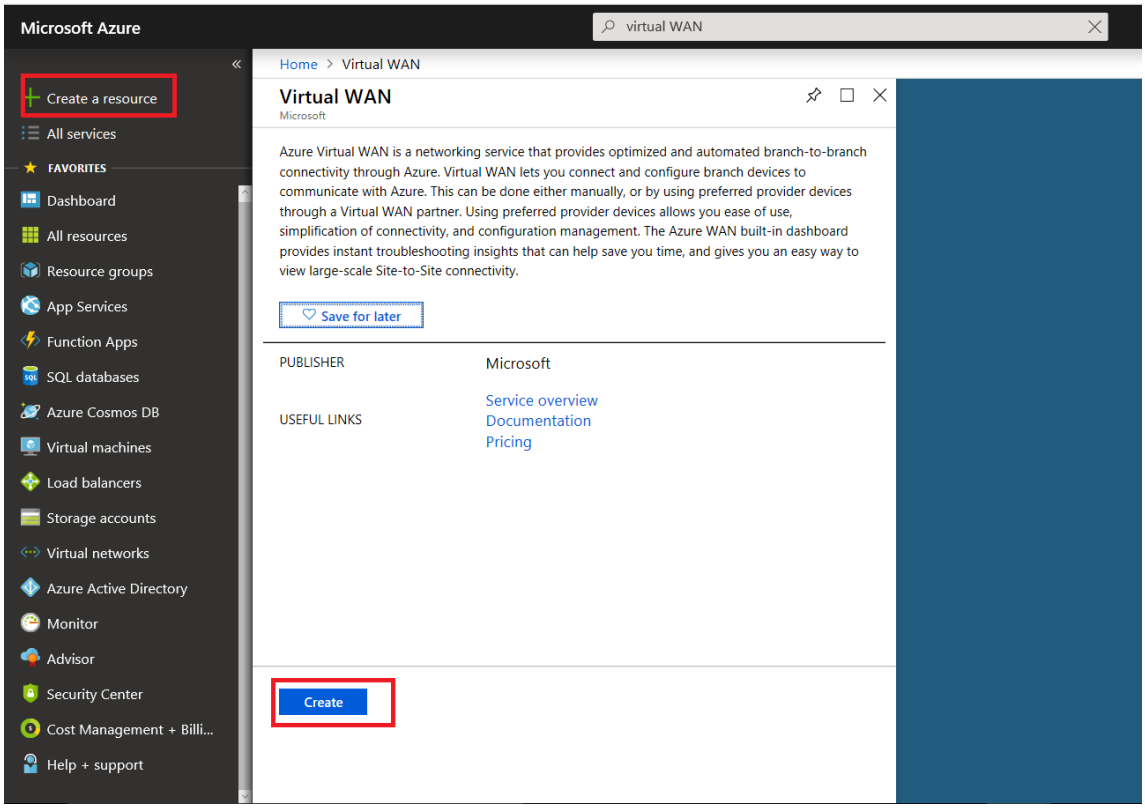
1. Configuration des ressources WAN.
2. Activation des succursales SD-WAN pour se connecter à Azure à l'aide de tunnels IPSec.

Configurez le réseau Azure avant de configurer le réseau SD-WAN, car les ressources Azure requises pour se connecter aux appliances SD-WAN doivent être disponibles au préalable. Toutefois, vous pouvez configurer la configuration SD-WAN avant de configurer les ressources Azure, si vous préférez. Cette rubrique traite de la configuration du réseau Azure Virtual WAN avant de configurer les appliances SD-WAN. https://microsoft.com Réseau étendu virtuel Azure.

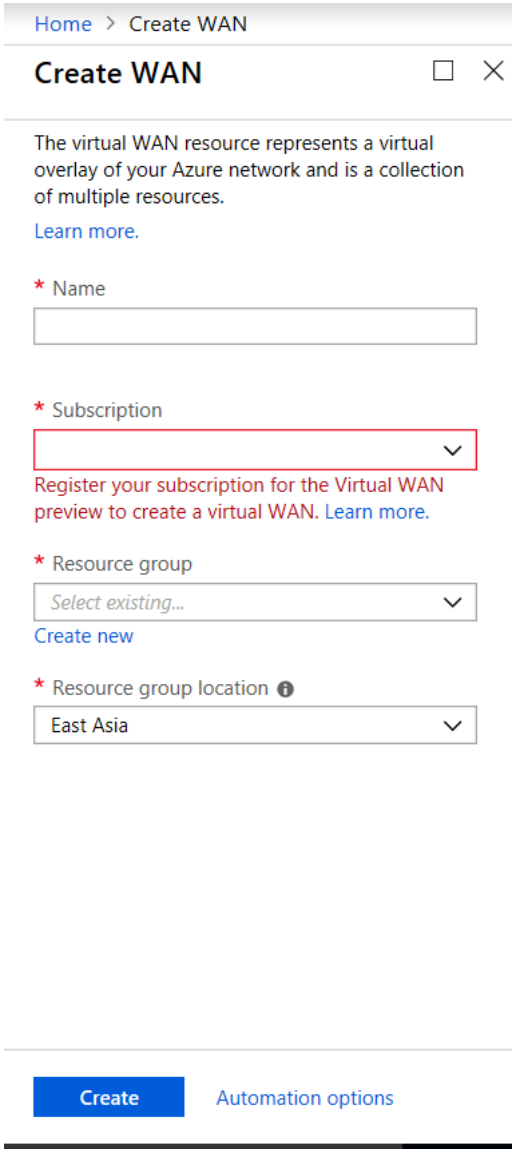
Créer une ressource WAN

Pour utiliser les fonctionnalités Virtual WAN et connecter l'appliance de succursale sur site à Azure :

1. Connectez-vous à Azure Marketplace, accédez à l'application Virtual WAN et sélectionnez **Create WAN**.



2. Entrez un nom pour le WAN et sélectionnez l'abonnement que vous souhaitez utiliser pour le WAN.



3. Sélectionnez un groupe de ressources existant ou créez un nouveau groupe de ressources. Les groupes de ressources sont des constructions logiques et l'échange de données entre les groupes de ressources est toujours possible.
4. Sélectionnez l'emplacement où vous souhaitez que votre groupe de ressources réside. WAN est une ressource globale qui n'a pas d'emplacement. Toutefois, vous devez entrer un emplacement pour le groupe de ressources contenant des métadonnées pour la ressource WAN.
5. Cliquez sur **Créer**. Cela démarre le processus de validation et de déploiement de vos paramètres.

Créer un site

Vous pouvez créer un site à l'aide d'un fournisseur préféré. Le fournisseur préféré envoie les informations sur votre appareil et votre site à Azure ou vous pouvez décider de gérer vous-même l'appareil. Si vous souhaitez gérer l'appareil, vous devez créer le site dans Azure Portal.

Réseau SD-WAN et flux de travail Microsoft Azure Virtual WAN

Configurer l'appliance SD-WAN :

1. Provisionner une appliance Citrix SD-WAN
    - Connectez l'appliance de succursale SD-WAN à l'appliance MCN.
2. Configurer l'appliance SD-WAN
    - Configurez les services Intranet pour la connexion Active-Active.

Configurer SD-WAN Center :

- Configurez SD-WAN Center pour vous connecter à Microsoft Azure.

Configurer les paramètres Azure :

- Fournissez l'ID du locataire, l'ID du client, la clé sécurisée, l'ID de l'abonné et le groupe de ressources.

Configurer l'association du site de succursale vers le réseau étendu :

1. Associer une ressource WAN à une succursale. Le même site ne peut pas être connecté à plusieurs réseaux locaux.
2. Cliquez sur **Nouveau** pour configurer l'association Site-WAN.
3. Sélectionnez **Azure Wan-Resources**.
4. Sélectionnez **Services** (Intranet) pour le site. Sélectionnez deux services pour la prise en charge Active-Veille.
5. Sélectionnez **Noms de site** à associer aux ressources Wan.
6. Cliquez sur **Déployer** pour confirmer l'association.
7. Attendez que l'état passe à **Tunnels déployés** pour afficher les paramètres du **tunnel IPsec**.
8. Utilisez la vue SD-WAN Center Reporting pour vérifier l'état des tunnels IPSec respectifs.

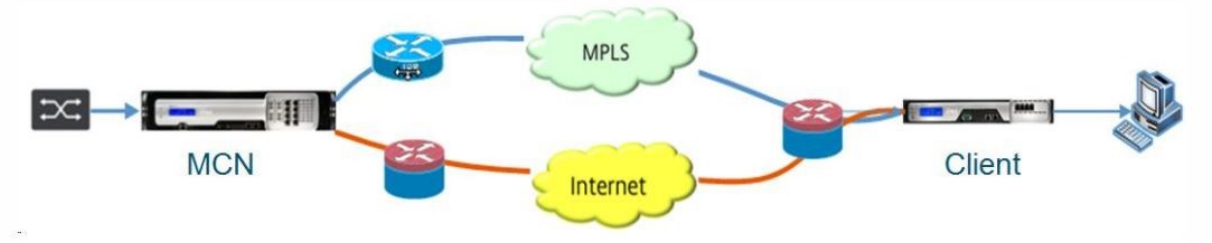
Configurer le réseau Citrix SD-WAN

MCN :

Le MCN sert de point de distribution pour la configuration initiale du système et les modifications ultérieures de configuration. Il ne peut y avoir qu'un seul MCN actif dans un WAN virtuel.
Par défaut, les solutions matérielles-logicielles ont le rôle de client pré-attribué. Pour établir une appliance en tant que MCN, vous devez d'abord ajouter et configurer le site en tant que MCN. L'interface graphique de configuration réseau devient disponible après la configuration d'un site en tant que MCN. Les mises à niveau et les modifications de configuration doivent être effectuées à partir du centre MCN ou SD-WAN uniquement.

Rôle du MCN :

Le MCN est le nœud central qui agit en tant que contrôleur d'un réseau SD-WAN et point d'administration central pour les nœuds clients. Toutes les activités de configuration, en plus de la préparation des packages de micrologiciels et de leur distribution aux clients, sont configurées sur le MCN. De plus, l'information de surveillance n'est disponible que sur le MCN. Le MCN peut surveiller l'ensemble du réseau SD-WAN, tandis que les nœuds clients ne peuvent surveiller que les Intranets locaux et certaines informations pour les clients auxquels ils sont connectés. L'objectif principal du MCN est d'établir des connexions de superposition (chemins virtuels) avec un ou plusieurs nœuds client situés sur le réseau SD-WAN pour la communication de site à site d'entreprise. Un MCN peut administrer et avoir des chemins virtuels vers plusieurs nœuds clients. Il peut y avoir plus d'un MCN, mais un seul peut être actif à un moment donné. La figure ci-dessous illustre le diagramme de base des appliances MCN et client (nœud de succursale) pour un petit réseau à deux sites.



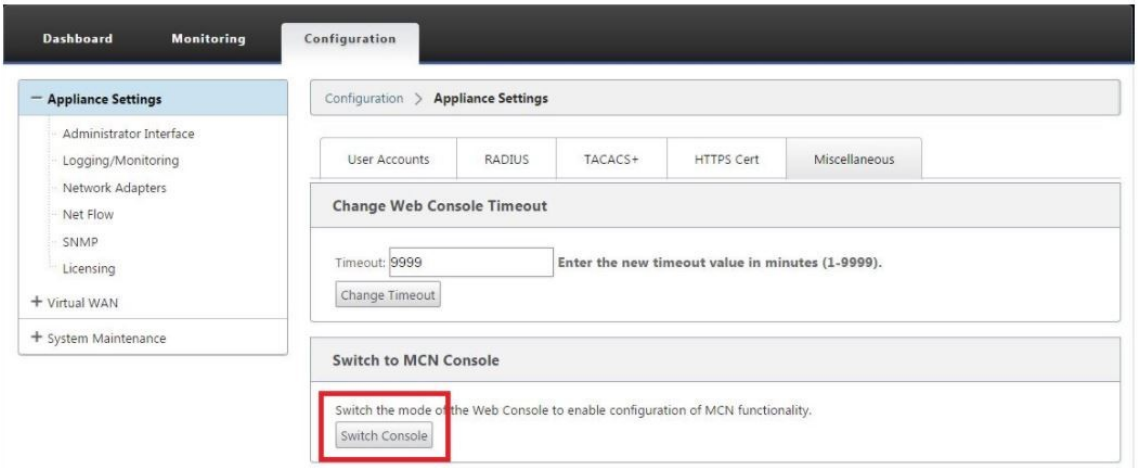
Configurer l'appliance SD-WAN en tant que MCN

Pour ajouter et configurer le MCN, vous devez d'abord vous connecter à l'interface Web de gestion de l'appliance que vous désignez en tant que MCN et passer l'interface Web de gestion en mode Console MCN. Le mode Console MCN permet d'accéder à l'éditeur de configuration dans l'interface Web de gestion à laquelle vous êtes actuellement connecté. Vous pouvez ensuite utiliser l'éditeur de configuration pour ajouter et configurer le site MCN.

Pour passer l'interface Web de gestion en mode console MCN, procédez comme suit :

1. Connectez-vous à l'interface Web de gestion SD-WAN de l'appliance que vous souhaitez configurer en tant que MCN.

2. Cliquez sur **Configuration** dans la barre de menu principale de l'écran principal de l'interface Web de gestion (barre bleue en haut de la page).
3. Dans l'arborescence de navigation (volet gauche), ouvrez la **branche Paramètres du matériel** et cliquez sur **Interface administrateur**.
4. Sélectionnez l'onglet **Divers** . La page Divers paramètres administratifs s'ouvre.



Au bas de l'onglet **Divers** se trouve la section **Basculer vers le [client, console MCN]**. Cette section contient le bouton **Switch Console** permettant de basculer entre les modes de console de l'appliance.

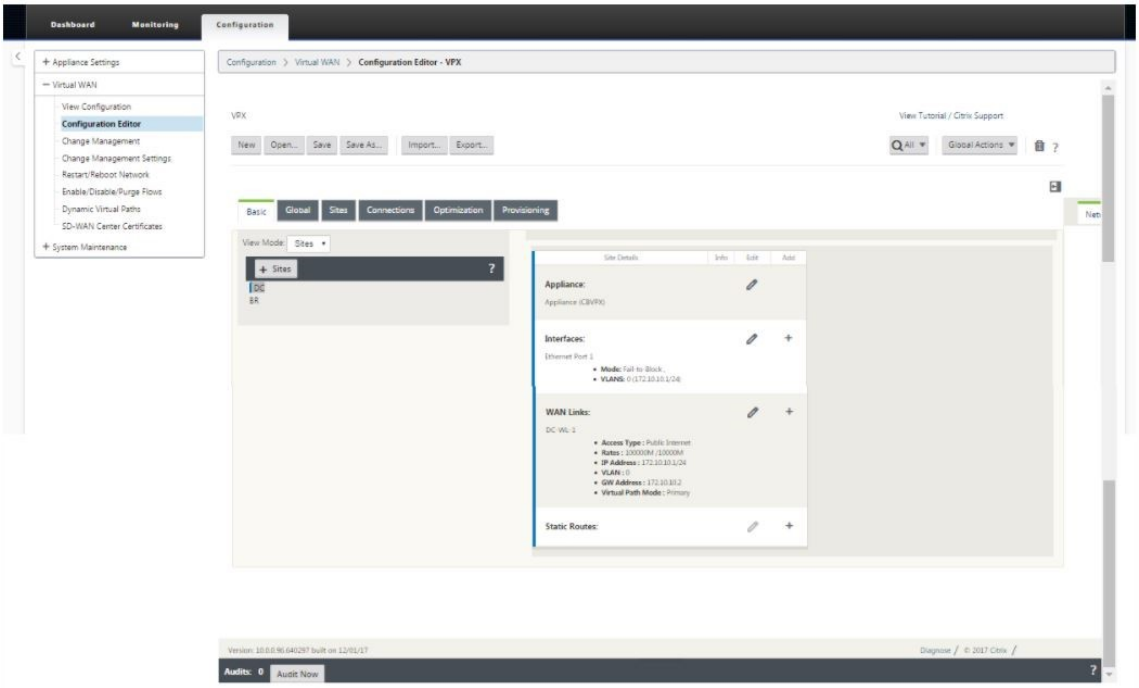
L'en-tête de la section indique le mode de console actuel, comme suit :

- En mode Console client (par défaut), l'en-tête de la section est Basculer vers la console MCN.
- En mode Console MCN, l'en-tête de la section est Basculer vers la console client.

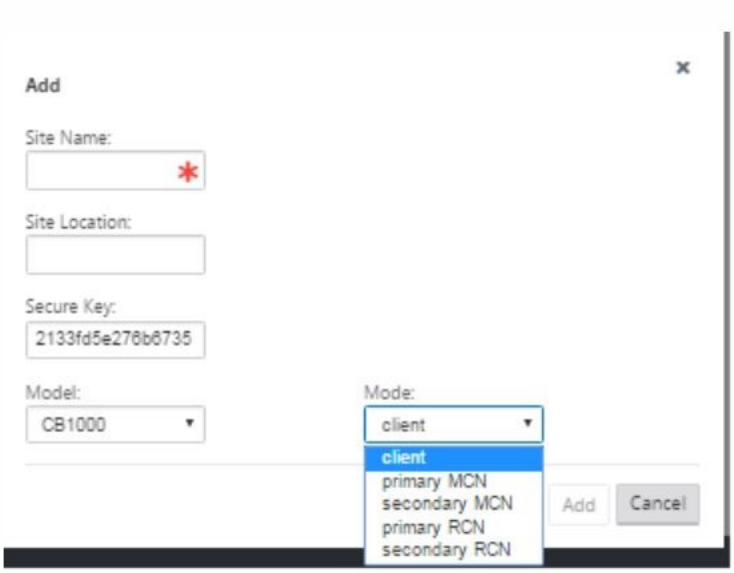
Par défaut, une nouvelle appliance est en mode Console client. Le mode Console MCN active l'affichage Éditeur de configuration dans l'arborescence de navigation. L'éditeur de configuration est disponible uniquement sur l'appliance MCN.

Configurer MCN Pour ajouter et commencer à configurer le site de l'appliance MCN, procédez comme suit :

1. Dans l'interface graphique de l'appliance SD-WAN, accédez à **Virtual WAN** > **Éditeur de configuration**.

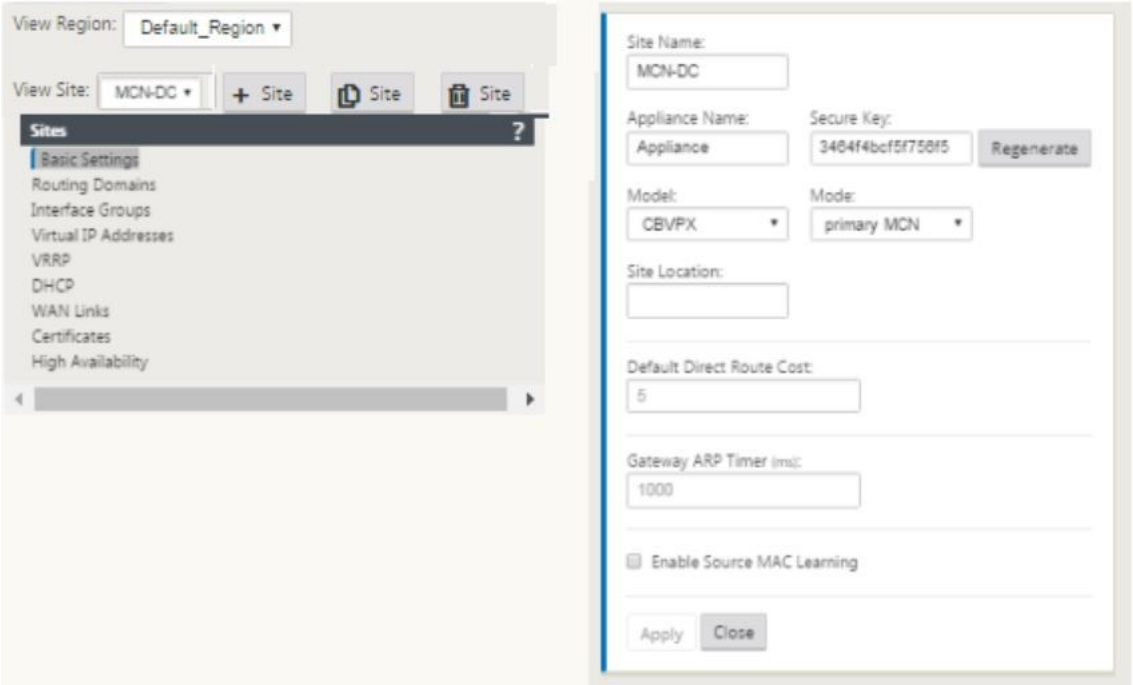


2. Cliquez sur **+ Sites** dans la barre des sites pour commencer à ajouter et à configurer le site MCN. La boîte de dialogue **Ajouter un site** s'affiche.

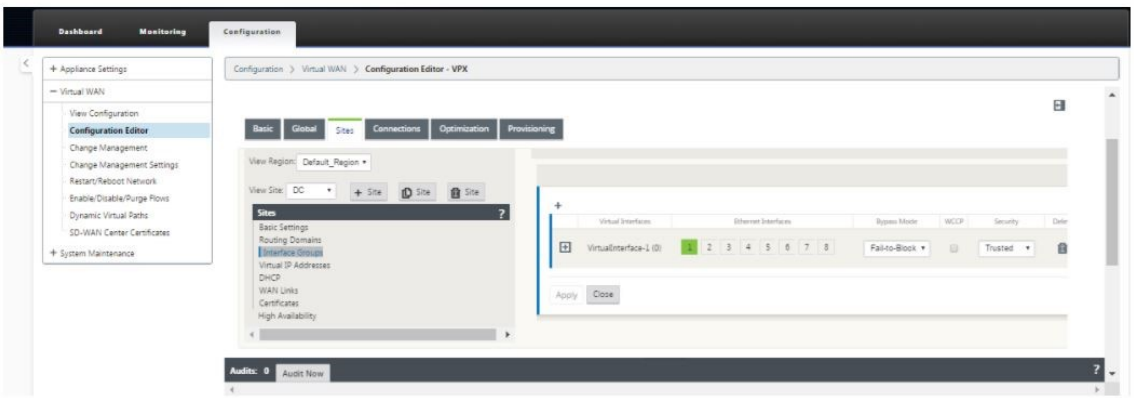


3. Entrez un nom de site qui vous permet de déterminer l'emplacement géographique et le rôle de l'appliance (CC/DC secondaire). Sélectionnez le modèle d'appliance approprié. La sélection de l'appliance appropriée est cruciale car les plates-formes matérielles diffèrent les unes des autres en termes de puissance de traitement et de licence. Étant donné que nous configurons cette solution matérielle-logicielle en tant que principal chef de gamme, choisissez le mode en tant que MCN principal et cliquez sur **Ajouter**.
4. Cela ajoute le nouveau site à l'arborescence des sites et la vue par défaut affiche la page de

configuration des paramètres de base comme indiqué ci-dessous :

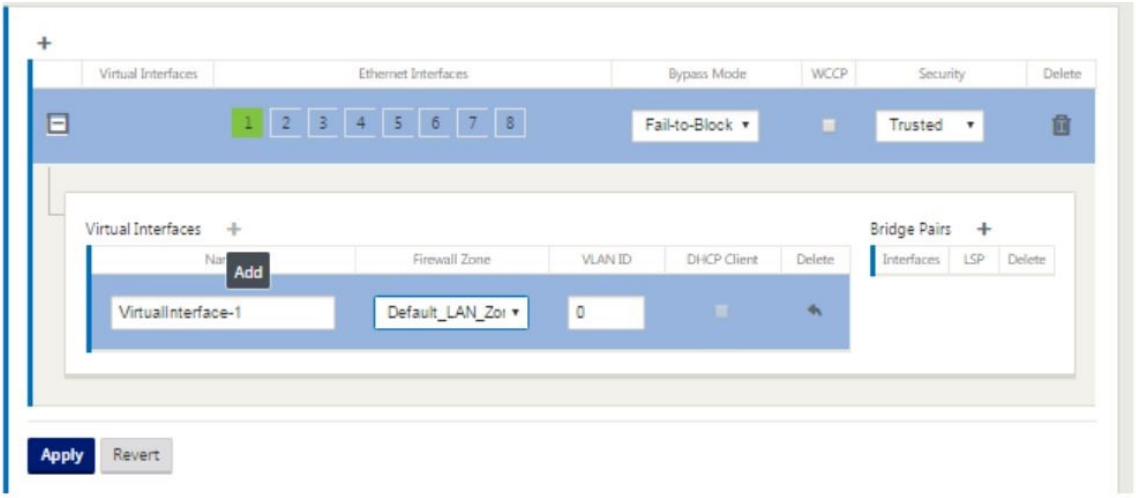


5. Entrez les paramètres de base tels que l'emplacement, le nom du site.
6. Configurez l'appliance afin qu'elle accepte le trafic depuis Internet/MPLS/large bande. Définissez les interfaces où les liens sont terminés. Cela dépend du fait que l'appliance est en mode superposition ou sous-couche.
7. Cliquez sur **Groupes d'interface** pour commencer à définir les interfaces.

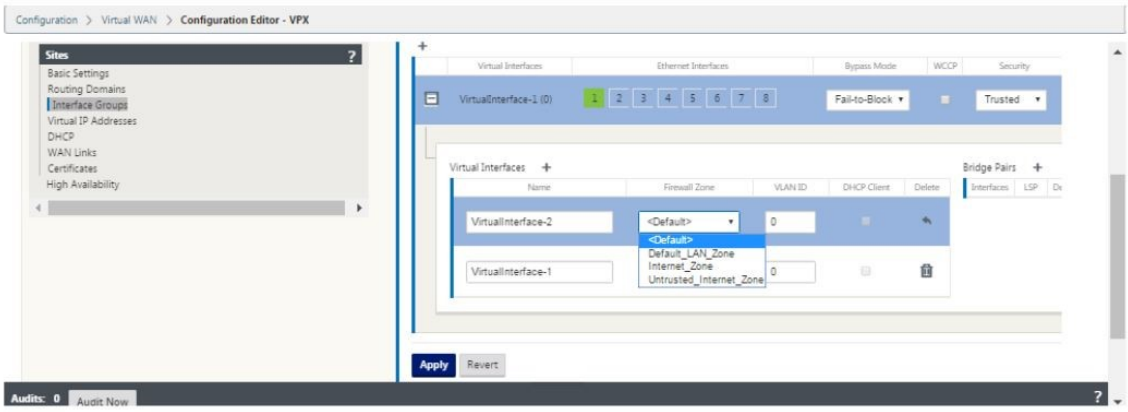


8. Cliquez sur + pour ajouter des groupes d'interface virtuelle. Cela ajoute un nouveau groupe d'interface virtuelle. Le nombre d'interfaces virtuelles dépend des liens que vous souhaitez que l'appliance gère. Le nombre de liens qu'une appliance peut gérer varie d'un modèle à l'autre et le nombre maximal de liens peut être jusqu'à huit.

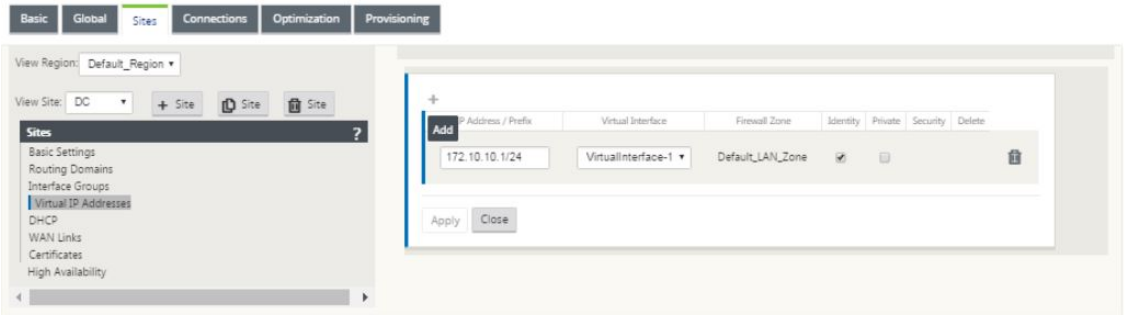
9. Cliquez sur + à droite des interfaces virtuelles pour afficher l'écran comme indiqué ci-dessous.

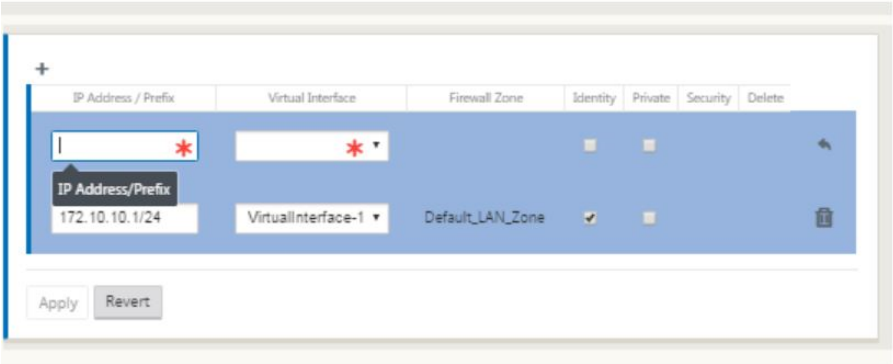


10. Sélectionnez les **interfaces Ethernet**qui font partie de cette interface virtuelle. Selon le modèle de plate-forme, les appliances disposent d'une paire d'interfaces fail-to-wire préconfigurées. Si vous souhaitez activer le basculement sur le câblage sur les appliances, assurez-vous de choisir la bonne paire d'interfaces et assurez-vous que vous choisissez le basculement du câblage dans la colonne **Mode de contournement**.
11. Sélectionnez le niveau de sécurité dans la liste déroulante. Le mode approuvé est choisi, si l'interface sert des liens MPLS et Non approuvé est choisi lorsque des liens Internet sont utilisés sur les interfaces respectives.
12. Cliquez sur + à droite de l'étiquette nommée interfaces virtuelles. Ceci affiche le nom, la zone de pare-feu et les ID de VLAN. Entrez le **nom et l'ID de VLAN** pour ce groupe d'interfaces virtuelles. L'ID de VLAN est utilisé pour identifier et marquer le trafic vers et depuis l'interface virtuelle, utilisez 0 (zéro) pour le trafic natif/non marqué.

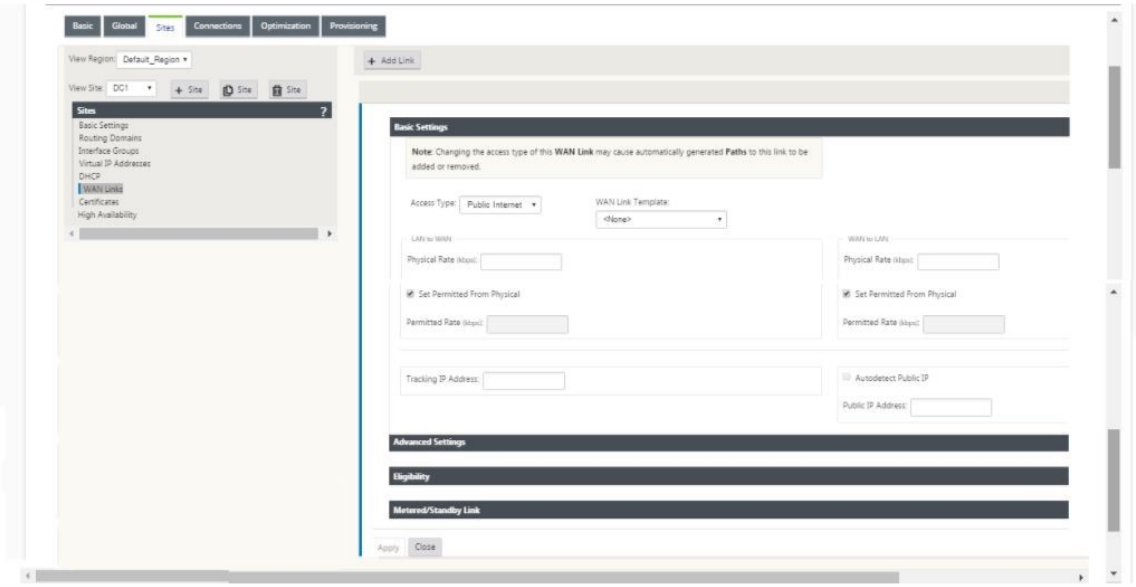


13. Pour configurer les interfaces en échec du câblage, cliquez sur Paires de pont. Cela ajoute une nouvelle paire de ponts et permet l'édition. Cliquez sur **Appliquer** pour confirmer ces paramètres.
14. Pour ajouter d'autres groupes d'interface virtuelle, cliquez sur + à droite de la succursale des groupes d'interface et procédez comme ci-dessus.
15. Une fois les interfaces choisies, l'étape suivante consiste à configurer les adresses IP sur ces interfaces. Dans la terminologie Citrix SD-WAN, c'est connu sous le nom de VIP (Virtual IP).
16. Continuez dans la vue Sites et cliquez sur l'adresse IP virtuelle pour afficher les interfaces de configuration VIP.

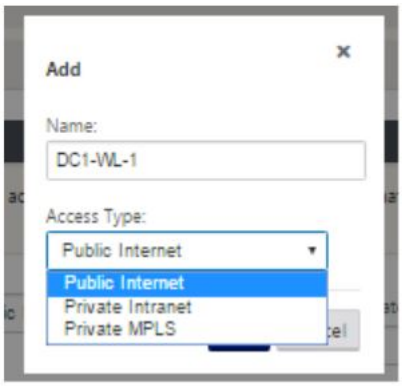




17. Entrez les informations d'adresse IP/préfixe, puis sélectionnez l'**interface virtuelle** à laquelle l'adresse est associée. L'adresse IP virtuelle doit inclure l'adresse hôte complète et le masque réseau. Sélectionnez les paramètres souhaités pour l'adresse IP virtuelle, tels que Zone de pare-feu, Identité, Privé et Sécurité. Cliquez sur **Apply**. Cette opération ajoute les informations d'adresse au site et les inclut dans la table Adresses IP virtuelles du site. Pour ajouter d'autres adresses IP virtuelles, cliquez sur + à droite des adresses IP virtuelles, puis procédez comme ci-dessus.
18. Continuez dans la section Sites pour configurer les liens WAN pour le site.



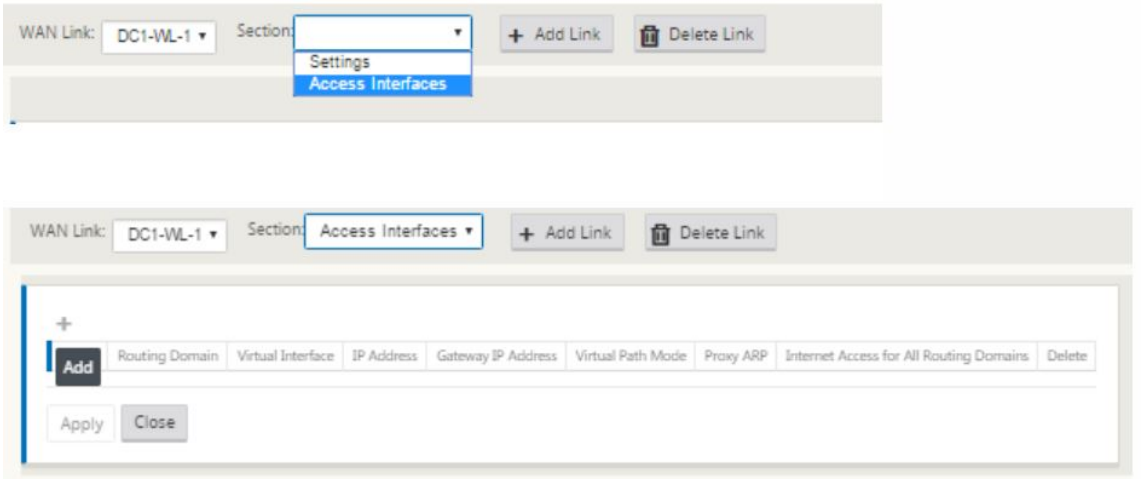
19. Cliquez sur **Ajouter un lien**, en haut du panneau sur le côté droit. Cela ouvre une boîte de dialogue qui vous permet de choisir le type de lien à configurer.



20. L'Internet public est pour les liaisons Internet/BroadBand/DSL/ADSL, tandis que les liaisons MPLS privées sont pour les liaisons MPLS. L'intranet privé est également destiné aux liaisons MPLS. La différence entre MPLS privé et les liens Intranet privés est que le MPLS privé permet de préserver les stratégies QoS des liens MPLS.
21. Si vous choisissez Internet public et que les adresses IP sont affectées via DHCP, choisissez l'

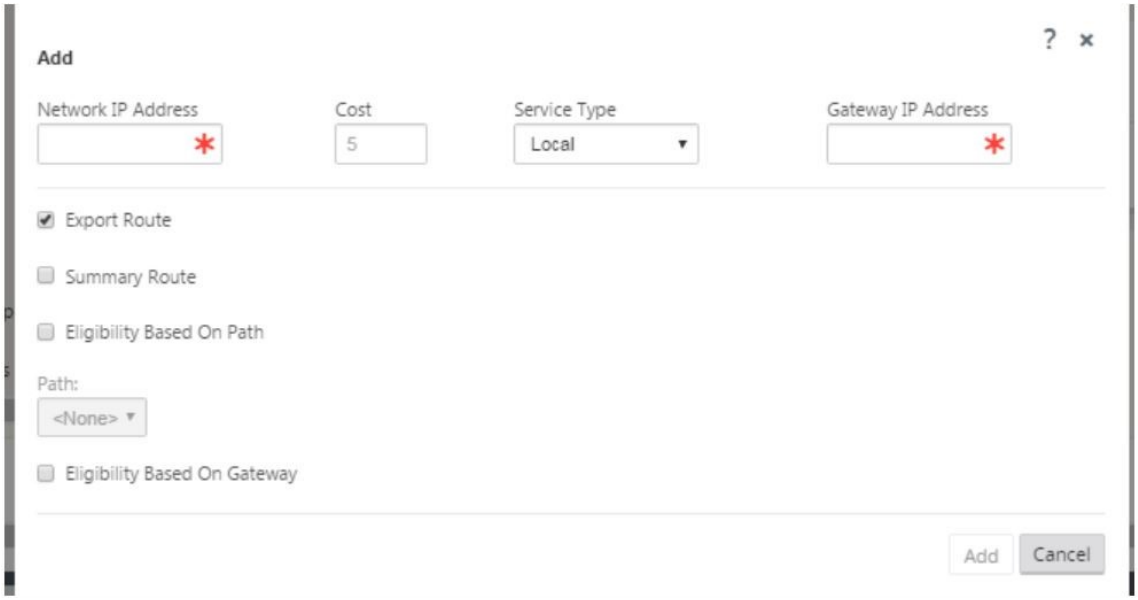
option de détection automatique de l'IP.

22. Sélectionnez **Interfaces d'accès** dans la page de configuration du lien WAN. La vue Interfaces d'accès s'ouvre pour le site. Ajoutez et configurez l'IP VIP et la passerelle pour chacun des liens comme indiqué ci-dessous.



23. Cliquez sur **+** pour ajouter une interface. Cela ajoute une entrée vide à la table et l'ouvre pour modification.
24. Entrez le nom que vous souhaitez attribuer à cette interface. Vous pouvez choisir de le nommer en fonction du type et de l'emplacement du lien. Conservez le domaine de routage par défaut si vous ne souhaitez pas séparer les réseaux et attribuer une adresse IP à l'interface.
25. Assurez-vous de fournir une adresse IP de passerelle accessible publiquement si le lien est une liaison Internet ou une adresse IP privée s'il s'agit d'une liaison MPLS. Conservez le mode chemin virtuel comme principal puisque vous avez besoin de ce lien pour former un chemin virtuel.

    Remarque : Activez l'ARP proxy lorsque l'appliance répond aux demandes ARP pour l'adresse IP de la passerelle lorsque la passerelle est inaccessible.
26. Cliquez sur **Appliquer** pour terminer la configuration du lien WAN. Si vous souhaitez configurer plus de liens WAN, répétez les étapes pour une autre liaison.
27. Configurez les itinéraires pour le site. Cliquez sur Affichage Connexions et sélectionnez des itinéraires.
28. Cliquez sur + pour ajouter des itinéraires, cela ouvre une boîte de dialogue comme illustré ci-dessous.



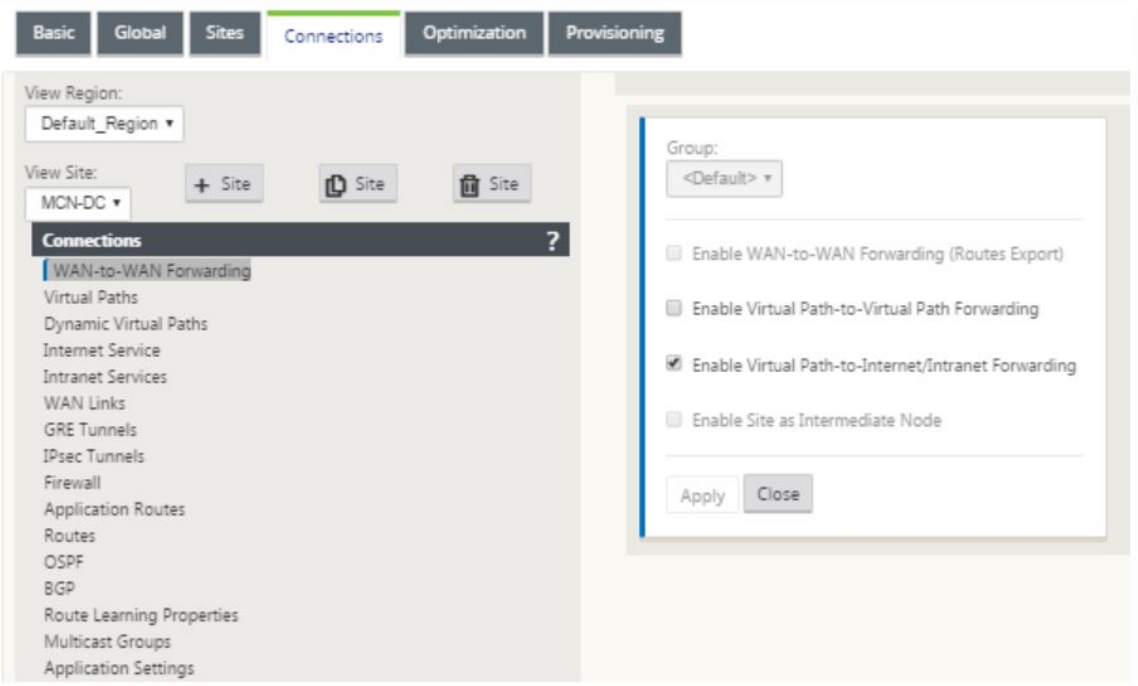
29. Entrez les informations suivantes sont disponibles pour le nouvel itinéraire :
    - Adresse IP réseau
    - Coût : le coût détermine l'itinéraire qui a priorité sur l'autre. Les chemins dont les coûts sont moins élevés ont priorité sur les itinéraires plus coûteux. La valeur par défaut est cinq.
    - Type de service : sélectionnez le service, un service peut être l'un des éléments suivants :
        - Chemin virtuel
        - Intranet
        - Internet
        - Passthrough
        - Stockage local
        - Tunnel GRE
        - Tunnel LAN IPsec
30. Cliquez sur **Apply**.

Pour ajouter d'autres itinéraires pour le site, cliquez sur + à droite de la succursale itinéraires et procédez comme ci-dessus. Pour plus d'informations, reportez-vous à la section Configurer un MCN.

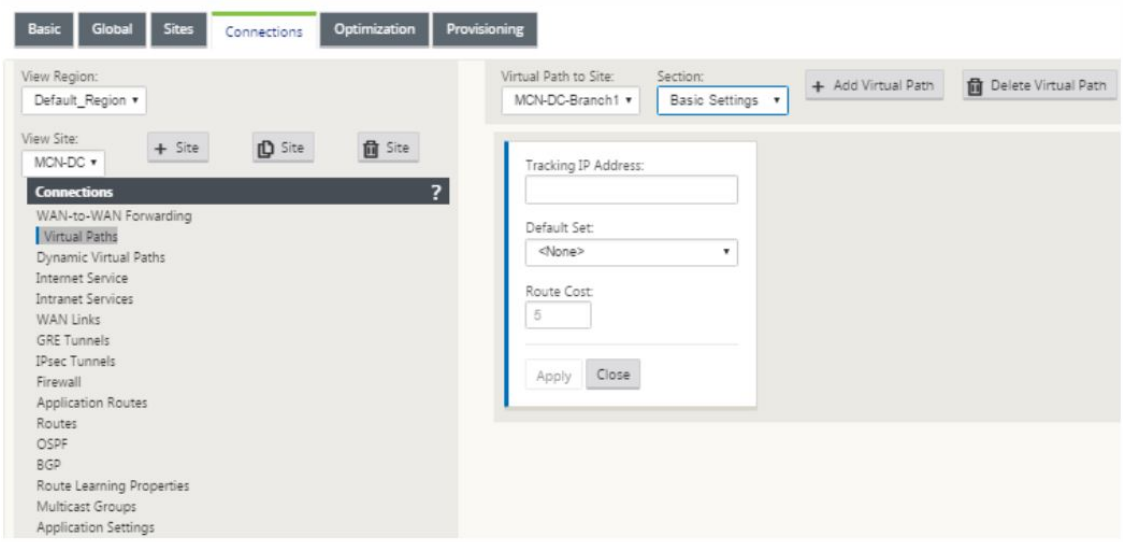
Configurer le chemin virtuel entre les sites MCN et les succursales Établir la connectivité entre le MCN et le nœud de succursale. Vous pouvez le faire en configurant un chemin virtuel entre ces deux sites. Accédez à l'onglet **Connexions** dans l'arborescence de configuration de l'éditeur de configuration.

1. Cliquez sur l'onglet **Connexions** dans la section Configuration. Cela affiche la section connexions de l'arborescence de configuration.

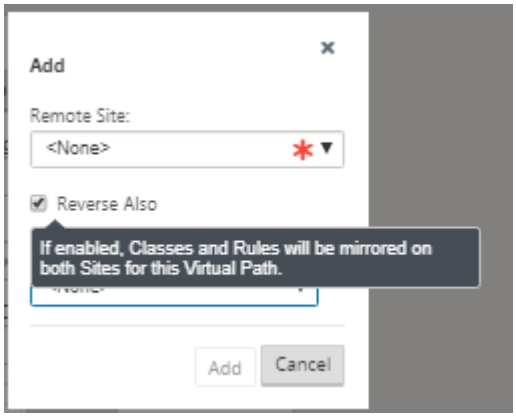
2. Sélectionnez le menu déroulant **MCN** à partir de l'affichage du site dans la page de section **Connexions**.



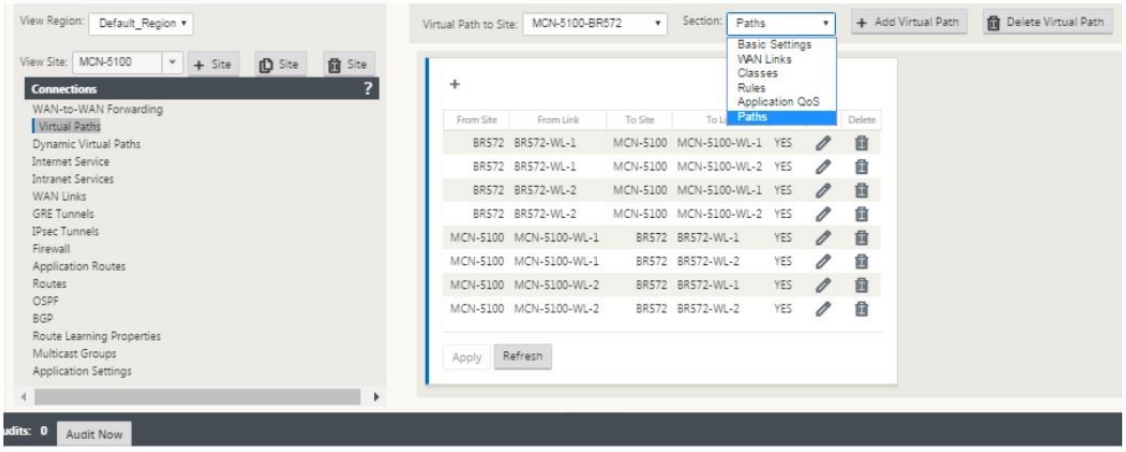
3. Sélectionnez le chemin virtuel sous l'onglet Connexions pour créer un chemin virtuel entre le MCN et les sites de succursale.



4. Cliquez sur **Ajouter un chemin virtuel** en regard du nom du chemin virtuel statique dans la section Chemins virtuels. Cela ouvre une boîte de dialogue comme illustré ci-dessous. Choisissez la succursale pour laquelle vous souhaitez configurer le chemin d'accès virtuel. Vous devez configurer cela sous l'étiquette site distant. Sélectionnez le nœud de branche dans cette liste déroulante, puis activez la case à cocher **Inverser aussi**.



La classification du trafic et la direction sont reflétés sur les deux sites du chemin virtuel. Une fois cette opération terminée, sélectionnez les chemins dans le menu déroulant sous l'étiquette section nommée comme indiqué ci-dessous.



5. Cliquez sur **+ Ajouter** au-dessus de la table des chemins, qui affiche la boîte de dialogue Ajouter un chemin. Spécifiez les points de terminaison dans lesquels le chemin virtuel doit être configuré. Maintenant, cliquez sur **Ajouter** pour créer le chemin et cliquez sur la case à **cocher Inverser aussi**.

   Remarque : Citrix SD-WAN mesure la qualité des liaisons dans les deux directions. Cela signifie que le point A au point B est un chemin et le point B au point A est un autre chemin. Grâce à la mesure unidirectionnelle des conditions de liaison, le SD-WAN est en mesure de choisir la meilleure route pour envoyer du trafic. Ceci diffère des mesures telles que la RTT, qui est une mesure bidirectionnelle pour mesurer la latence. Par exemple, une connexion entre le point A et le point B est affichée sous la forme de deux chemins et pour chacun d'eux, les mesures de performance de liaison sont calculées indépendamment.

Ce paramètre est suffisant pour amener les chemins virtuels entre le MCN et la succursale, d'autres options de configuration sont également disponibles. Pour plus d'informations, reportez-vous à la section

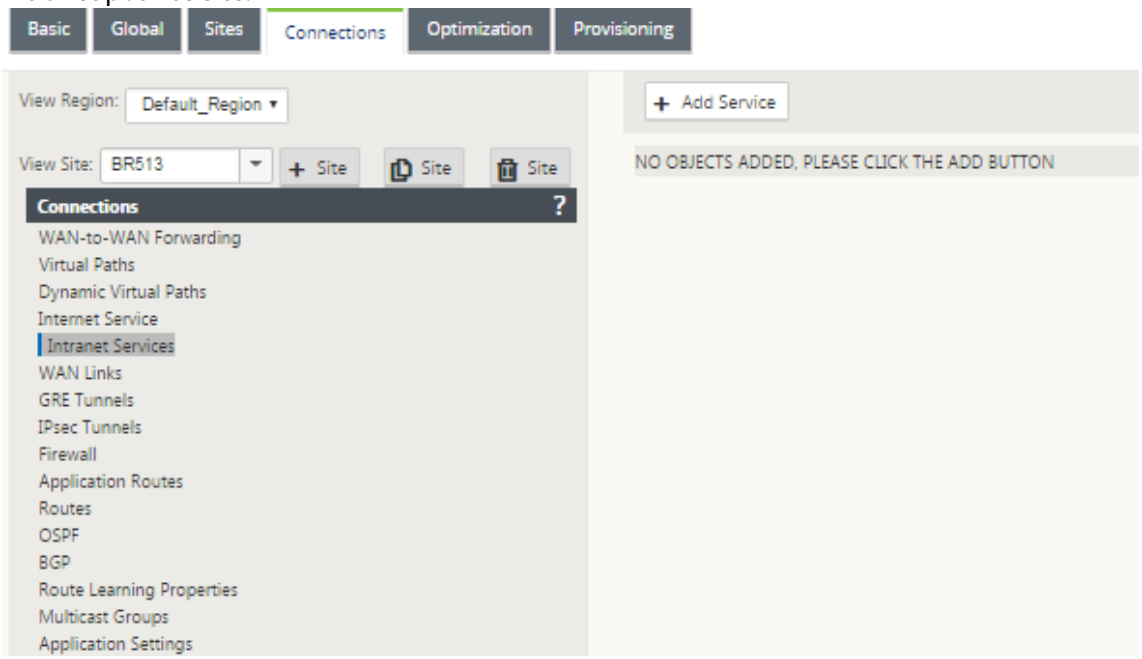
Configurer le service de chemin d'accès virtuel entre les sites MCN et clients.

Déploiement de la configuration MCN L'étape suivante consiste à déployer la configuration. Cela implique les deux étapes suivantes :

1. Exportez le package de configuration SD-WAN vers la gestion des modifications.
    - Avant de pouvoir générer les packages d'appliance, vous devez d'abord exporter le package de configuration terminé depuis l'**éditeur** de configuration vers la boîte de réception globale de la zone de réception de la zone de transit **Change Management** sur le MCN. Reportez-vous aux étapes fournies dans la section Effectuer la gestion des modifications.
2. Génération et mise en scène des paquetages de l'appliance.
    - Après avoir ajouté le nouveau package de configuration à la boîte de réception Gestion des modifications, vous pouvez générer et organiser les packages d'appliance sur les sites de succursale. Pour ce faire, vous utilisez l'Assistant Gestion des modifications dans l'interface Web de gestion sur le MCN. Reportez-vous aux étapes fournies dans la section Packages de matériel Stage.

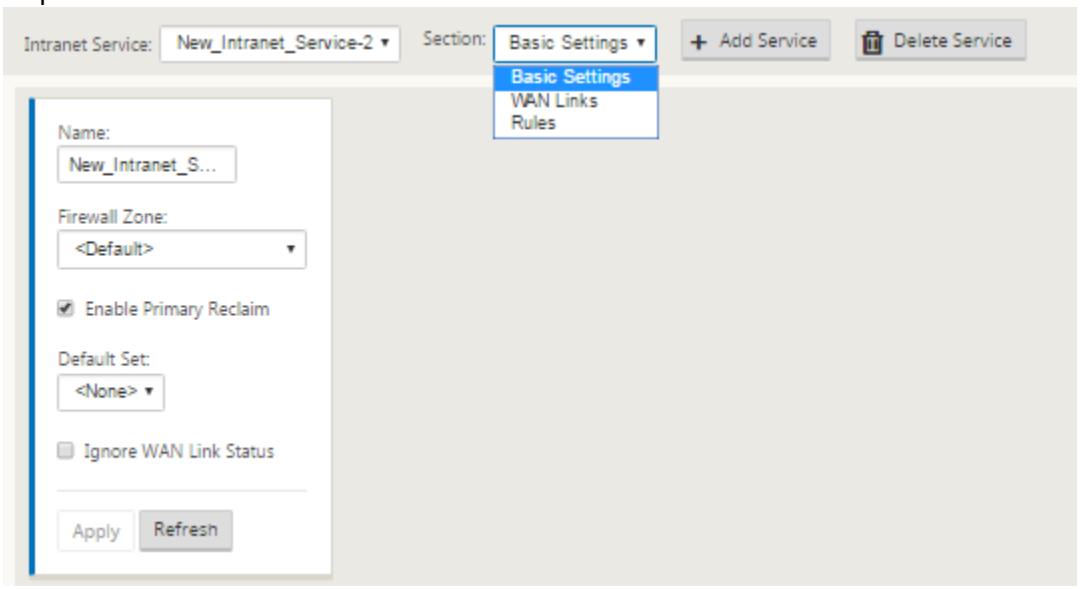
Configurer les services intranet pour se connecter aux ressources WAN Azure

1. Dans l'interface graphique de l'appliance SD-WAN, accédez à l'**éditeur de configuration**. Accédez à la vignette **Connexions** . Cliquez sur **+ Ajouter un service** pour ajouter un service Intranet pour ce site.



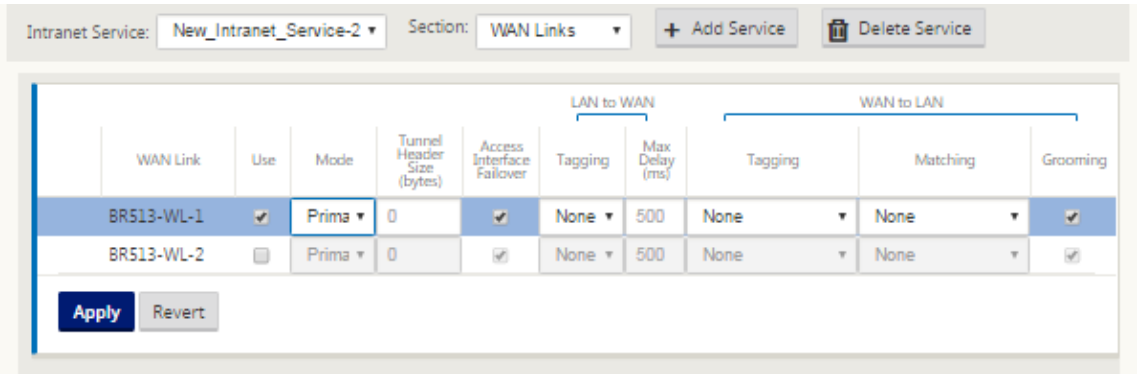
2. Dans les **Paramètres de base** du service Intranet, il existe plusieurs options sur la façon dont vous souhaitez que le service Intranet se comporte en cas d'indisponibilité des liens WAN.

   - **Activer la reprise primaire** : cochez cette case si vous souhaitez que le lien principal choisi prenne le relais lorsqu'il apparaît après un basculement. Toutefois, si vous choisissez de ne pas cocher cette option, le lien secondaire continuera à envoyer du trafic.
   - **Ignorer l'état du lien WAN** : si cette option est activée, les paquets destinés à ce service intranet continueraient à utiliser ce service même si les liens WAN constitutifs ne sont pas disponibles.



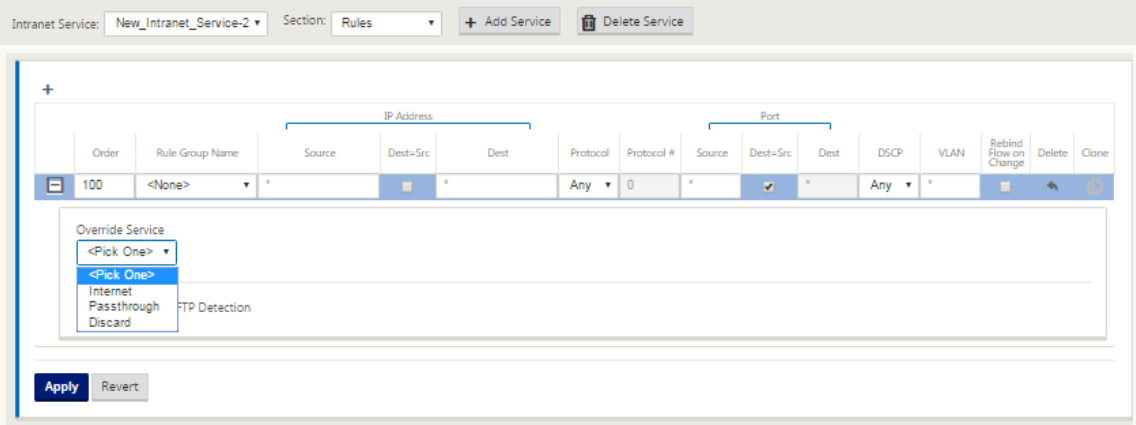
3. Après avoir configuré les paramètres de base, l'étape suivante consiste à choisir les liens WAN constitutifs pour ce service. Au maximum, deux liaisons sont choisies pour un service Intranet. Pour choisir les liens WAN, sélectionnez l'option Liens WAN dans la liste déroulante intitulée Section. Les liaisons WAN fonctionnent en mode primaire et secondaire et une seule liaison est choisie comme liaison WAN principale.

   Remarque : Lorsqu'un deuxième service intranet est créé, il doit avoir le mappage principal et secondaire de lien wan-link.

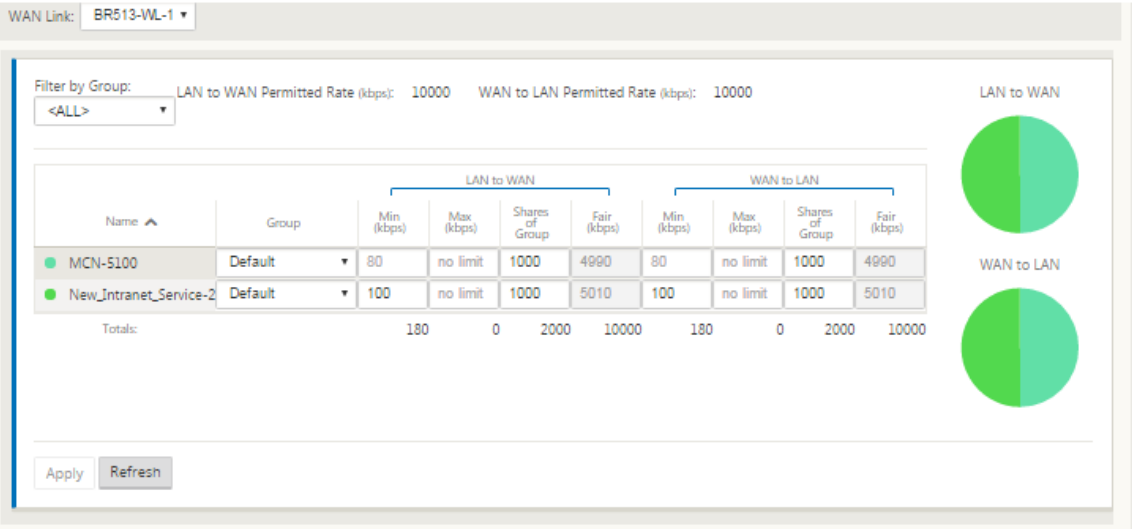


4. Des règles spécifiques au site de succursale sont disponibles, ce qui permet de personnaliser

chaque site de succursale en remplaçant de manière unique tous les paramètres généraux configurés dans le jeu global par défaut. Les modes incluent la livraison souhaitée via une liaison WAN spécifique ou en tant que service de remplacement permettant de passer ou de rejeter le trafic filtré. Par exemple, s'il y a du trafic, que vous ne voulez pas passer par le service intranet, vous pouvez écrire une règle pour ignorer ce trafic ou l'envoyer via un service différent (Internet ou passer par).

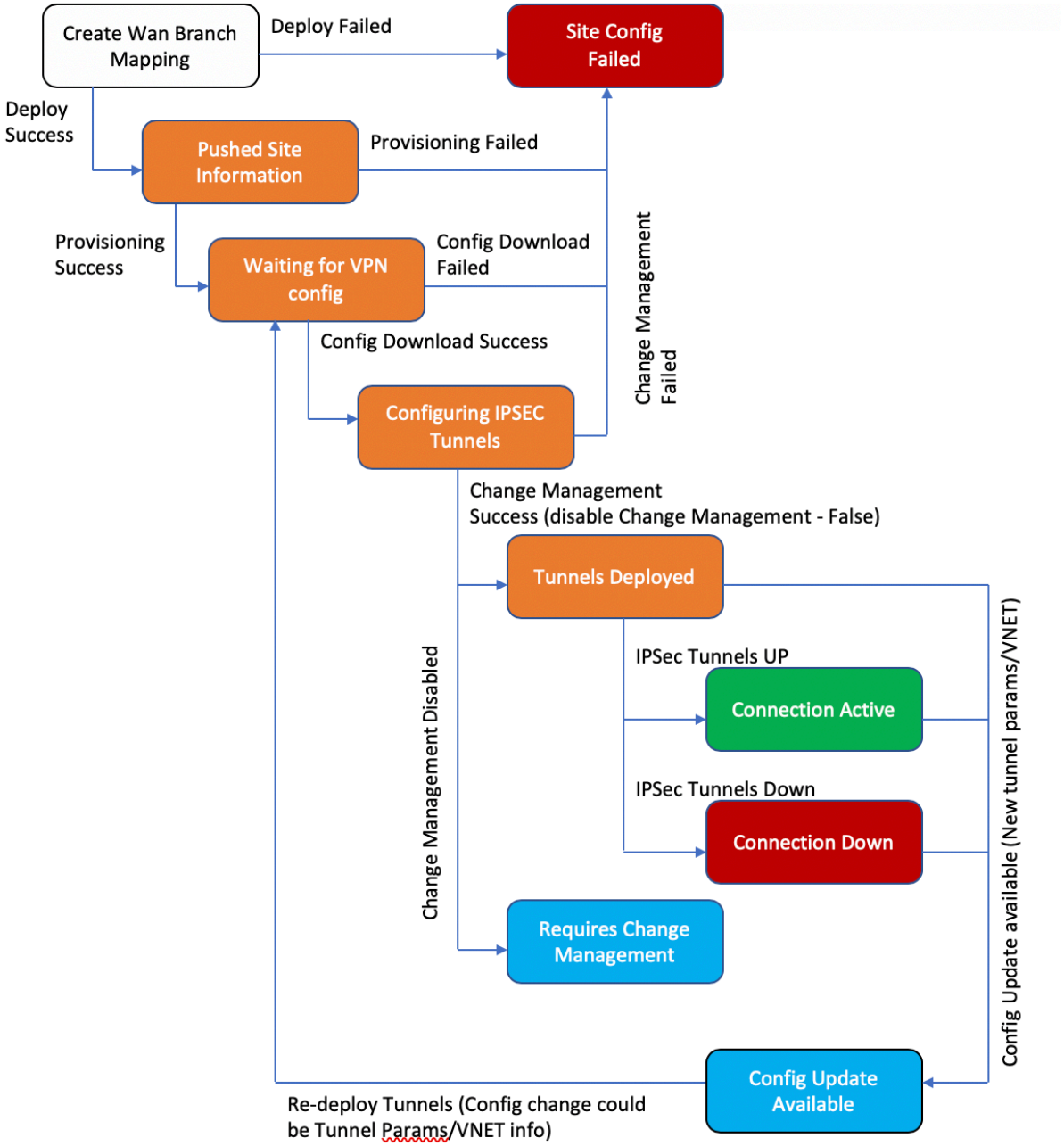


5. Lorsque le service Intranet est activé pour un site, la vignette **Provisioning** est mise à disposition pour permettre la distribution bidirectionnelle (LAN vers WAN /WAN vers LAN) de la bande passante pour une liaison WAN entre les différents services utilisant la liaison WAN. La section **Services** vous permet d'affiner davantage l'allocation de bande passante. En outre, une répartition équitable peut être activée, ce qui permet aux services de recevoir leur bande passante minimale réservée avant la mise en place d'une distribution équitable.



Configurer SD-WAN Center

Le diagramme suivant décrit le flux de travail de haut niveau de la connexion SD-WAN Center et Azure Virtual WAN et les transitions d'état correspondantes du déploiement.



Configurer les paramètres Azure :

- Fournissez l'ID client Azure, l'ID d'application, la clé secrète et l'ID d'abonnement (également

appelé principal de service).

Configurer l'association du site de succursale vers le réseau étendu :

- Associer un site de succursale à une ressource WAN. Le même site ne peut pas être connecté à plusieurs réseaux locaux.
- Cliquez sur **Nouveau** pour configurer l'association Site-WAN.
- Sélectionnez **Azure Wan-Resources**.
- Sélectionnez **Noms de site** à associer aux ressources WAN.
- Cliquez sur **Déployer** pour confirmer l'association. Les liaisons WAN à utiliser pour le déploiement de tunnels sont automatiquement remplies avec celle avec la meilleure capacité de liaison.
- Attendez que l'état passe à « Tunnels déployés » pour afficher les paramètres du **tunnel IPsec** .
- Utilisez la vue SD-WAN Center Reporting pour vérifier l'état des tunnels IPSec respectifs. L'état du tunnel IPSec doit être VERT pour que le trafic de données circule, ce qui indique que la connexion est active.

Provisionner le SD-WAN Center :

SD-WAN center est l'outil de gestion et de reporting pour Citrix SD-WAN. La configuration requise pour Virtual WAN est effectuée dans SD-WAN Center. SD-WAN Center n'est disponible qu'en tant que facteur de forme virtuel (VPX) et doit être installé sur un hyperviseur VMware ESXi ou XenServer. Les ressources minimales nécessaires pour configurer un SD-WAN Center sont 8 Go de RAM et 4 cœurs CPU. Voici les étapes à suivre pour installer et configurer une machine virtuelle de centre SD-WAN.

Configurer SD-WAN Center pour la connectivité Azure

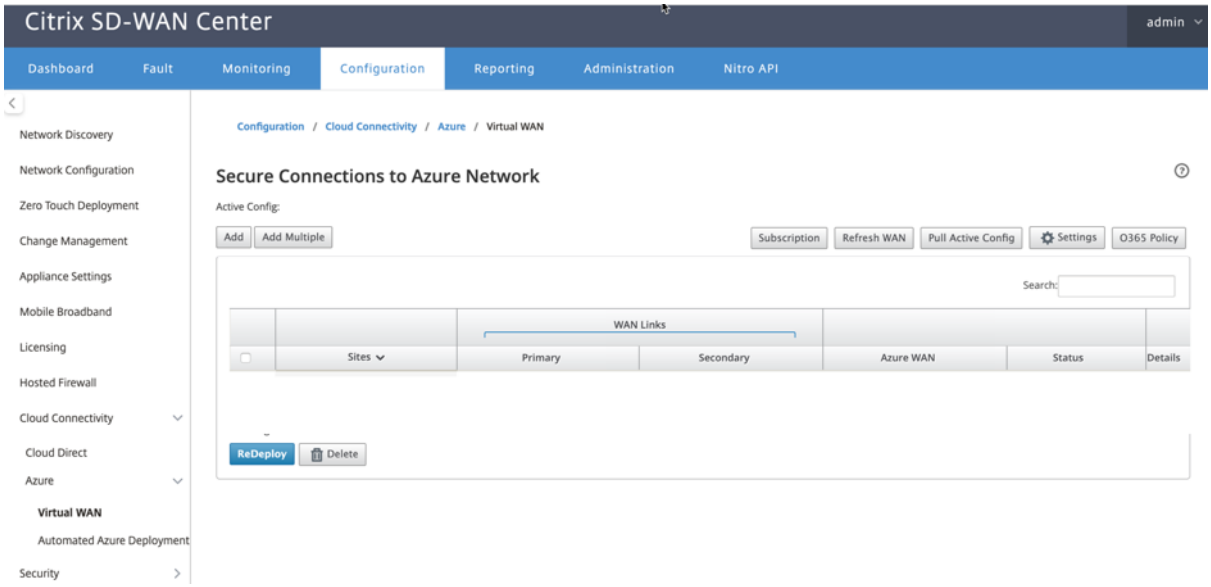
Pour plus d'informations, consultez l'article Créer un principal de service .

Pour authentifier correctement SD-WAN Center avec Azure, les paramètres suivants doivent être disponibles :

- Répertoire (ID de locataire)
- Application (ID client)
- Clé sécurisée (secret client)
- ID d'abonné

Authentifier le SD-WAN Center :

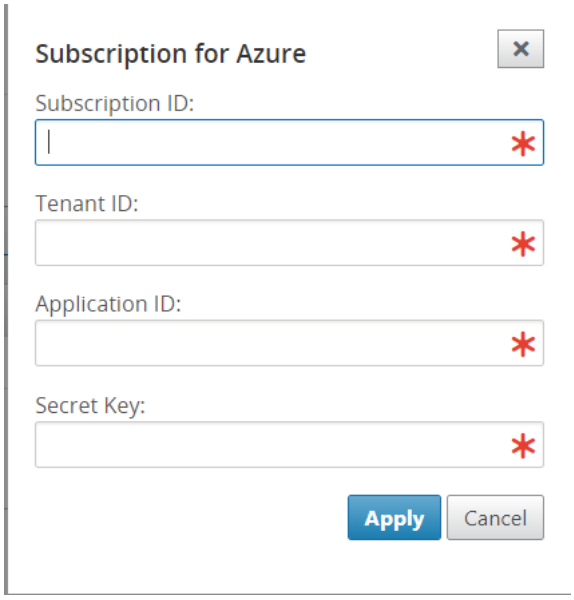
Dans l'interface utilisateur SD-WAN Center, accédez à **Configuration** > **Connectivité Cloud** > **Azure** > **Réseau étendu virtuel**. Configurer les paramètres de connexion Azure. Reportez-vous au lien suivant pour plus d'informations sur la configuration de la connexion VPN Azure,
Azure Resource Manager.



Avec la version 11.1.0 et les versions ultérieures, la configuration de liaison WAN principale et secondaire pour l'intégration Azure Virtual WAN est prise en charge. La principale raison de l'ajout d'une liaison WAN secondaire est d'avoir une redondance à partir du site Citrix SD-WAN.

Avec l'implémentation précédente, l'échec de la liaison WAN pourrait entraîner une interruption du trafic et une perte de connectivité vers Azure Virtual WAN. Avec l'implémentation actuelle, la connectivité Site vers Azure Virtual WAN est maintenue vivante même si la liaison WAN principale est en panne.

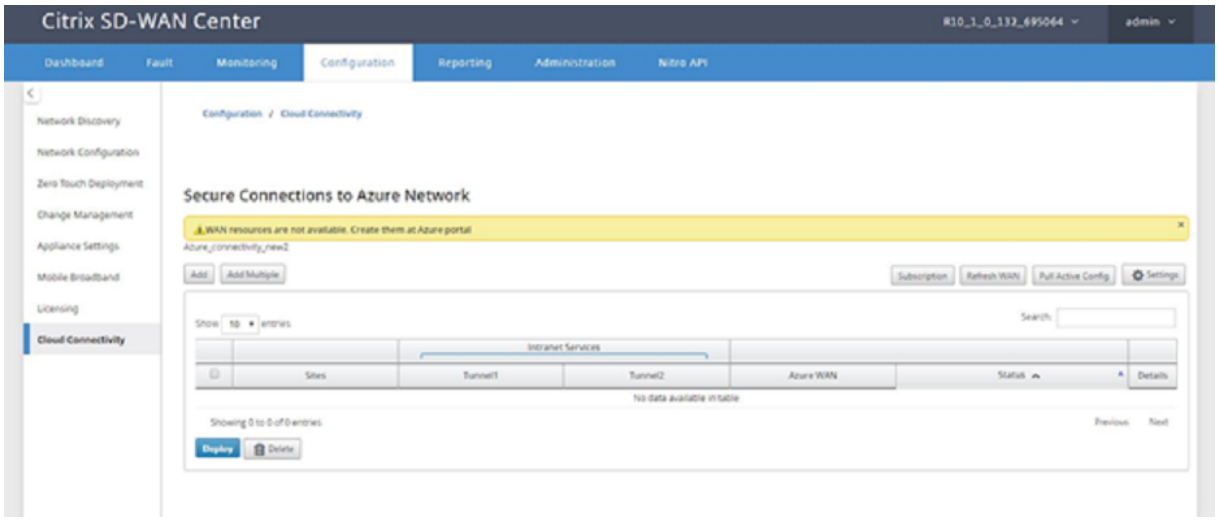
Entrez l'**ID d'abonnement**, **l'ID de locataire**, **l'ID d'application** et la **clé sécurisée**. Cette étape est requise pour authentifier SD-WAN Center avec Azure. Si les informations d'identification entrées ci-dessus ne sont pas correctes, l'authentification échoue et aucune action supplémentaire n'est autorisée. Cliquez sur **Apply**.



Le champ **Compte de stockage** fait référence au compte de stockage que vous avez créé dans Azure. Si vous n'avez pas créé de compte de stockage, un nouveau compte de stockage est automatiquement créé dans votre abonnement lorsque vous cliquez sur **Appliquer**.

Obtenir des ressources Azure Virtual WAN :

Une fois l'authentification réussie, Citrix SD-WAN interroge Azure pour obtenir une liste de ressources WAN virtuelles Azure, que vous avez créées dans la première étape après la connexion au portail Azure. Les ressources WAN représentent l'ensemble de votre réseau dans Azure. Il contient des liens vers tous les Hubs que vous souhaitez avoir dans ce WAN. Les réseaux WAN sont isolés les uns des autres et ne peuvent pas contenir de hub commun ou de connexions entre deux concentrateurs différents dans des ressources WAN différentes.



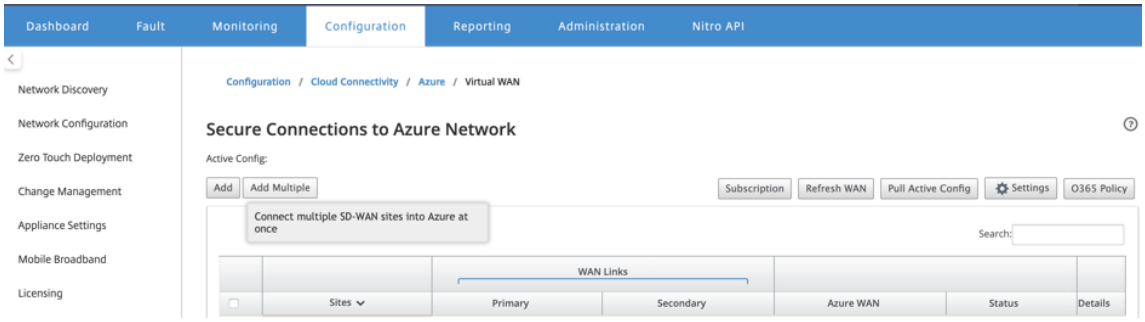
Pour associer des sites de succursales et des ressources WAN Azure :

Un site de succursale doit être associé aux ressources WAN Azure pour établir des tunnels IPSec. Une succursale peut être connectée à plusieurs hubs au sein d'une ressource WAN virtuelle Azure et une ressource WAN virtuelle Azure peut être connectée à plusieurs sites de succursale sur site. Créez des lignes uniques pour chaque déploiement de ressources Branch to Azure Virtual WAN.

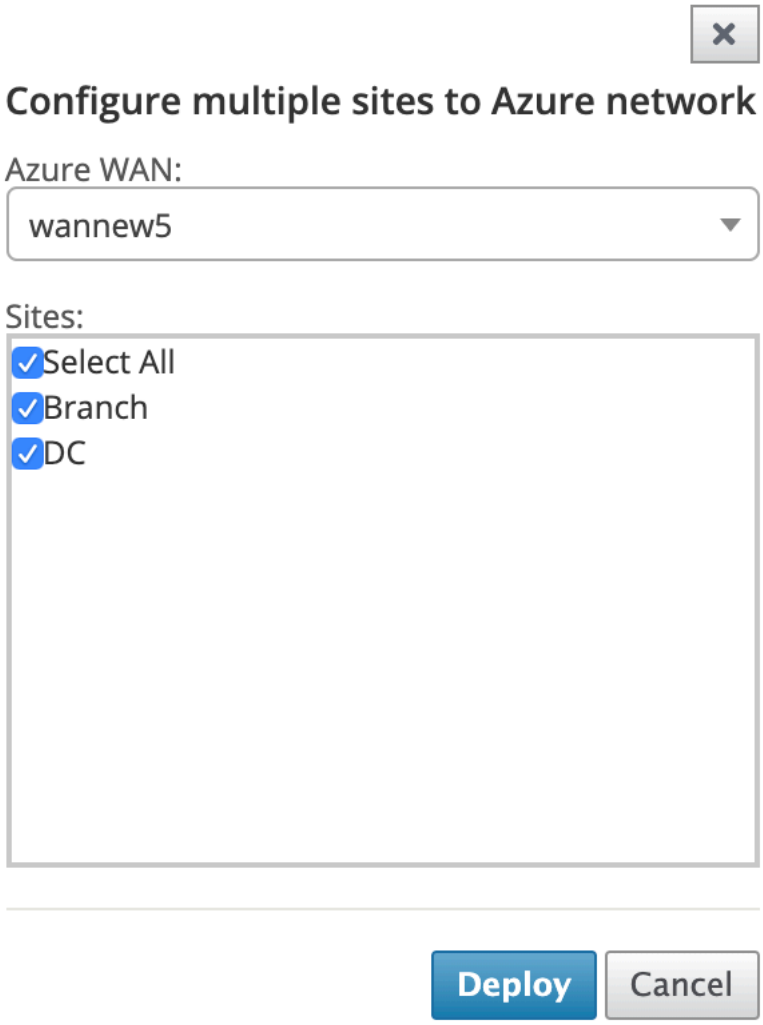
Pour ajouter plusieurs sites :

Vous pouvez choisir d'ajouter tous les sites respectifs et de les associer aux ressources WAN uniques choisies.

1. Cliquez sur **Ajouter plusieurs** pour ajouter tous les sites qui doivent être associés aux ressources WAN sélectionnées.



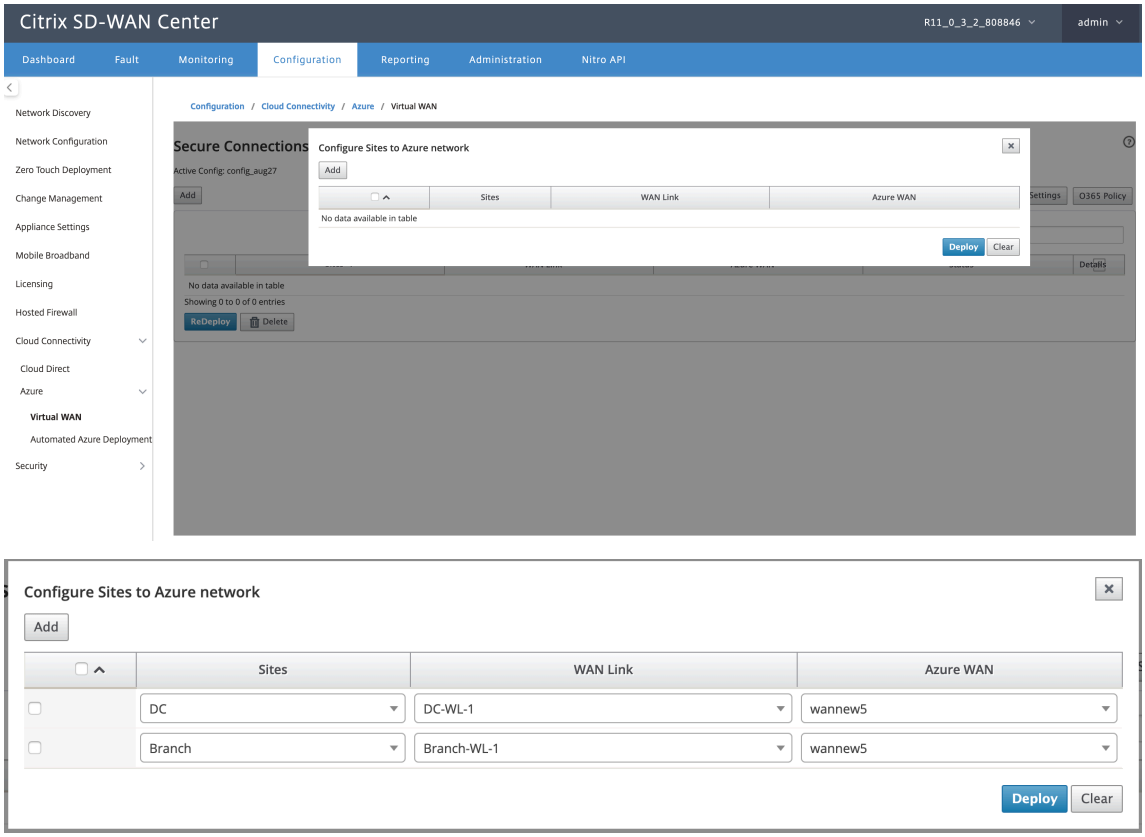
2. La liste déroulante des ressources WAN Azure (illustrée ci-dessous) est préremplie avec les ressources appartenant à votre compte Azure. Si aucune ressource WAN n'a été créée, cette liste est vide et vous devez accéder au portail Azure pour créer les ressources. Si la liste est remplie avec des ressources WAN, choisissez la **ressource WAN Azure** à laquelle vous devez connecter les sites de succursale.
3. Choisissez l'un ou l'ensemble des sites de succursales pour lancer le processus d'établissement du tunnel IPSec. Les liens WAN Internet public de capacité de meilleure capacité sont choisis automatiquement pour établir les tunnels IPSec vers les passerelles VPN Azure.



Pour ajouter un site unique :

Vous pouvez également choisir d'ajouter des sites un par un (unique) et à mesure que votre réseau se développe, ou si vous effectuez un déploiement site par site, vous pouvez choisir d'ajouter plusieurs sites comme décrit ci-dessus.

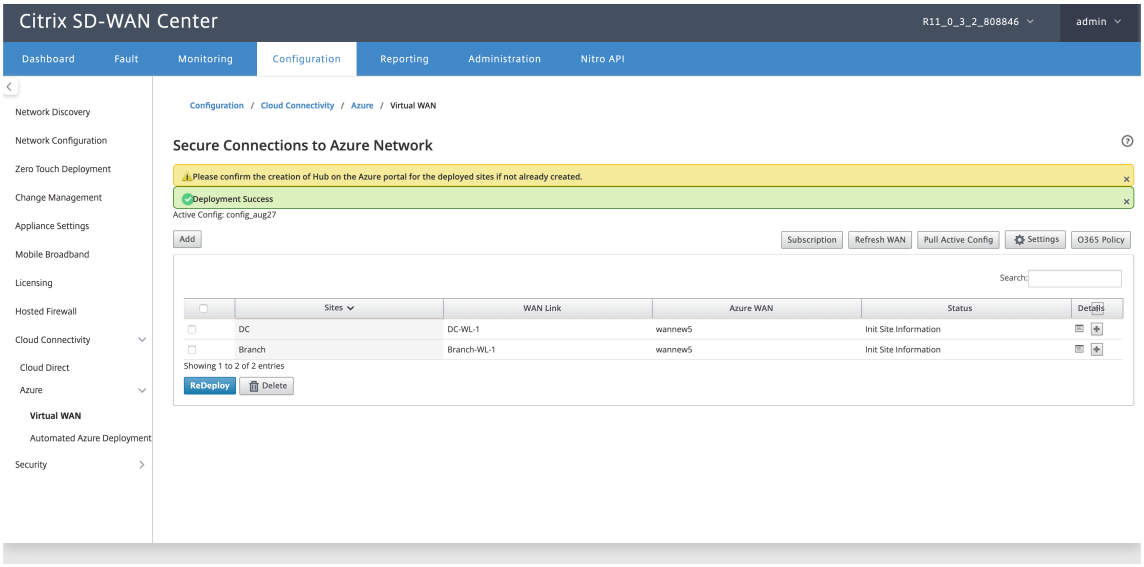
1. Cliquez sur **Ajouter une nouvelle entrée** pour sélectionner un nom de site pour l'association Site-Wan. Ajoutez des sites dans la boîte de dialogue Configurer des sites sur le **réseau Azure**.



2. Sélectionnez le site Branche à configurer sur le réseau WAN virtuel Azure.
3. Sélectionnez le lien WAN associé au site (les liens de type Internet public sont répertoriés dans l'ordre de meilleure capacité de liaison physique)
4. Sélectionnez la ressource WAN à laquelle le site doit être associé dans le menu déroulant **WANS virtuels Azure**.
5. Cliquez sur **Déployer** pour confirmer l'association. L'état (Informations sur le site d'initialisation « Informations sur le site poussé » et « En attente de la configuration VPN ») est mis à jour pour vous informer du processus.

Le processus de déploiement inclut l'état suivant :

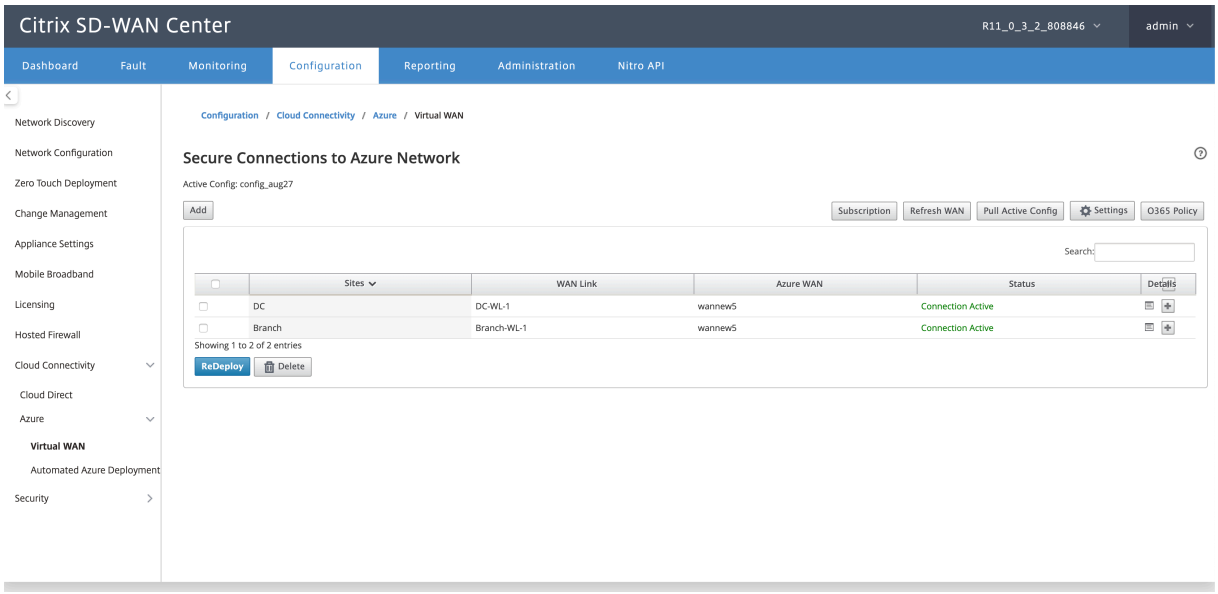
- Informations sur le site Push
- En attente de configuration VPN
- Tunnels déployés
- Connexion active (le tunnel IPsec est activé) ou Connexion en panne (le tunnel IPSec est en panne)

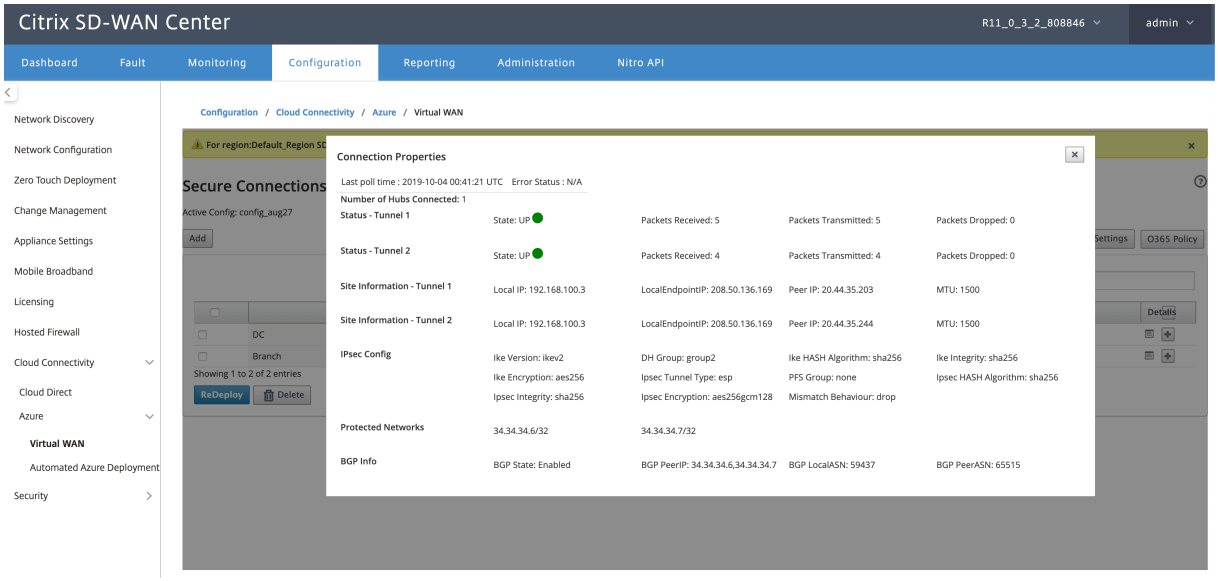


Associer des mappages de ressources WAN de site (portail Azure) :

Associez les sites déployés sur le portail Azure aux Hubs virtuels créés sous la ressource Azure Virtual WAN. Un ou plusieurs Hubs virtuels peuvent être associés au site de la succursale. Chaque Hub virtuel est créé dans une région spécifique et des charges de travail spécifiques peuvent être associées aux Hubs virtuels en créant des Connexions réseau virtuelles. Ce n'est qu'après la réussite de l'association Site de succursale à Virtual Hub que les configurations VPN sont téléchargées et les tunnels IPSec respectifs sont établis du site aux passerelles VPN.

Attendez que le statut passe à Tunnels déployés ou Connexion active pour afficher les paramètres du **tunnel IPSec**. Afficher les paramètres IPsec associés aux services sélectionnés.

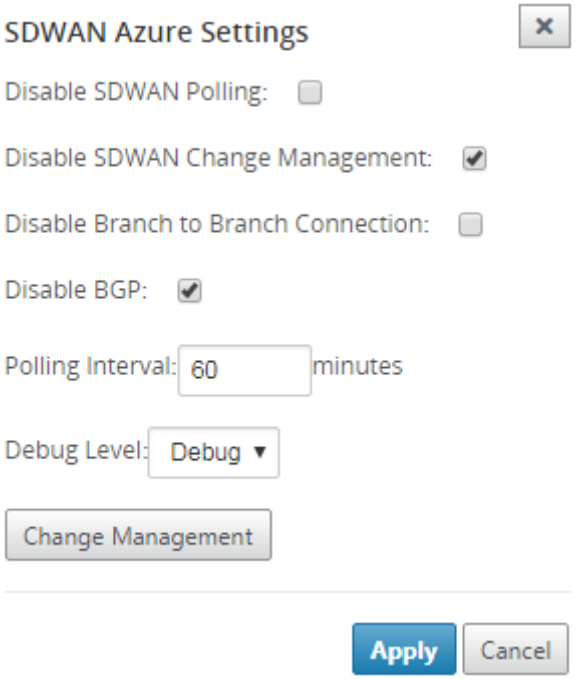




Paramètres Azure SD-WAN :

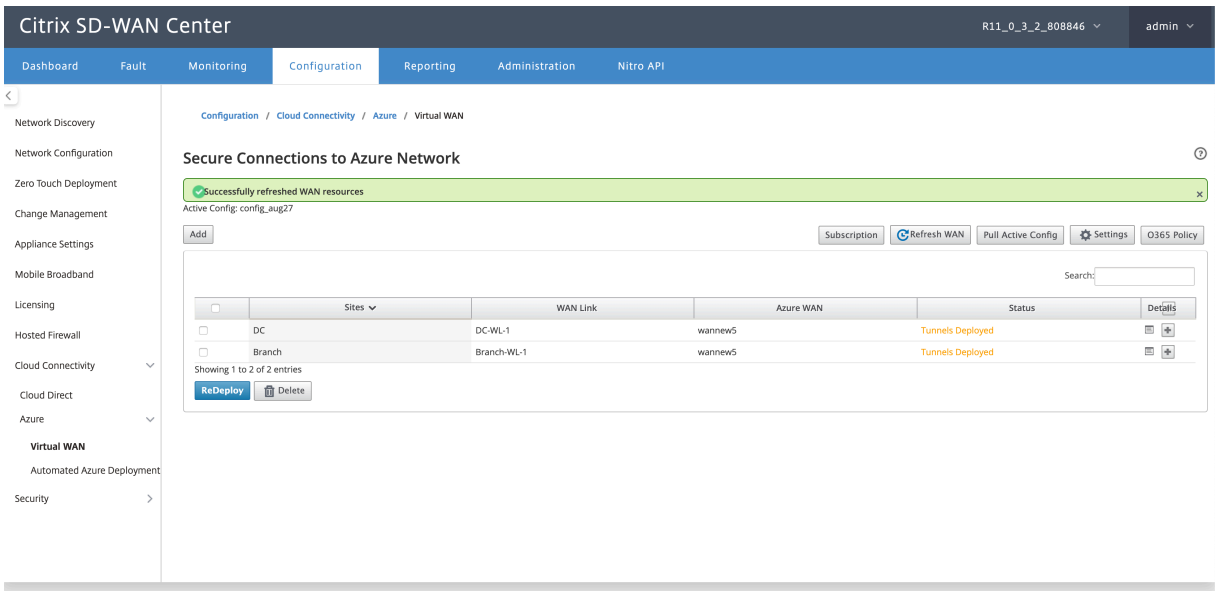
- **Désactiver la gestion des modifications SD-WAN** —Par défaut, le processus de gestion des modifications est automatisé. Cela signifie que chaque fois qu'une nouvelle configuration est disponible dans l'infrastructure réseau étendu virtuel Azure, SD-WAN Center l'obtient et commence à l'appliquer automatiquement aux succursales. Toutefois, ce comportement est contrôlé, si vous voulez contrôler quand une configuration doit être appliquée aux branches. L'un des avantages de la désactivation de la gestion automatique des modifications est que la configuration de cette fonctionnalité et d'autres fonctionnalités SD-WAN est gérée indépendamment.
- **Désactiver l'interrogation SDWAN** : désactive tous les nouveaux déploiements et l'interrogation SD-WAN Azure sur les déploiements existants.
- **Intervalle d'interrogation** - L'option Intervalle d'interrogation contrôle l'intervalle de recherche des mises à jour de configuration dans l'infrastructure Azure Virtual WAN, le temps recommandé pour l'intervalle d'interrogation est de 1 heure.
- **Désactiver la connexion succursale à succursale** : désactive la communication succursale à succursale via l'infrastructure réseau étendu virtuel Azure. Par défaut, cette option est désactivée. Une fois que vous l'avez activé, cela signifie que les succursales sur site sont en mesure de communiquer entre elles et avec les ressources derrière les branches via IPsec via l'infrastructure Virtual WAN d'Azure. Cela n'a aucun effet sur la communication de succursale à succursale via le chemin virtuel SD-WAN, les succursales sont capables de communiquer entre elles et leurs ressources/points de terminaison respectifs sur un chemin virtuel, même si cette option est désactivée.
- **Désactiver BGP** —Cela désactive BGP sur IP, par défaut, il est désactivé. Une fois activé, les itinéraires du site sont annoncés sur BGP.

- **Niveau de débogage** : permet de capturer les journaux à déboguer en cas de problème de connectivité.

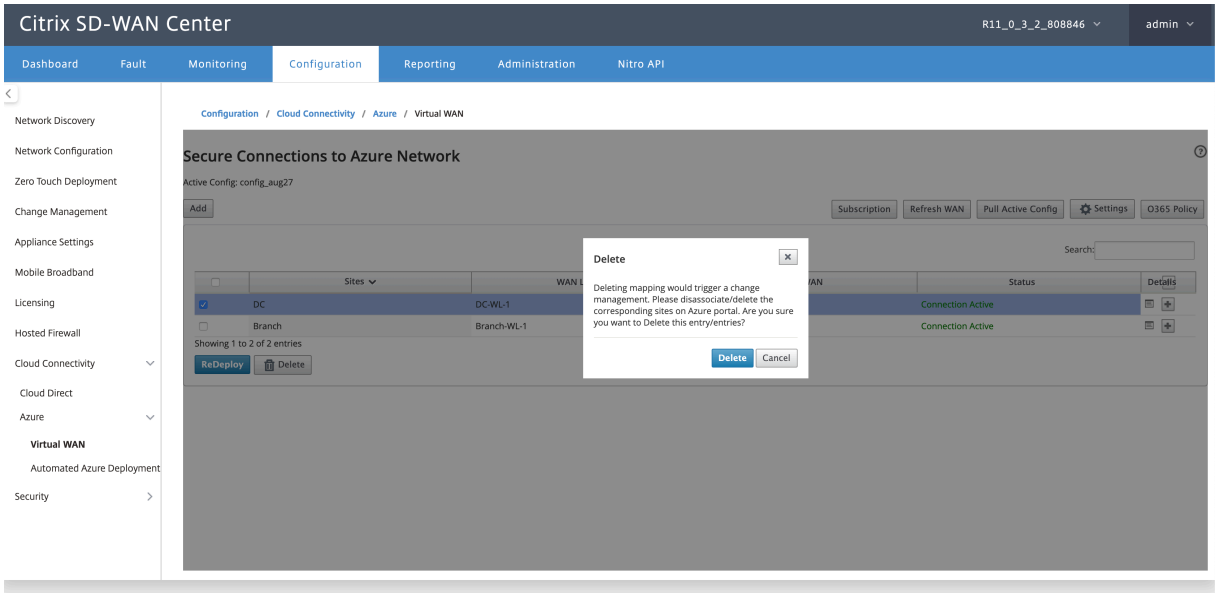


Actualiser les ressources WAN :

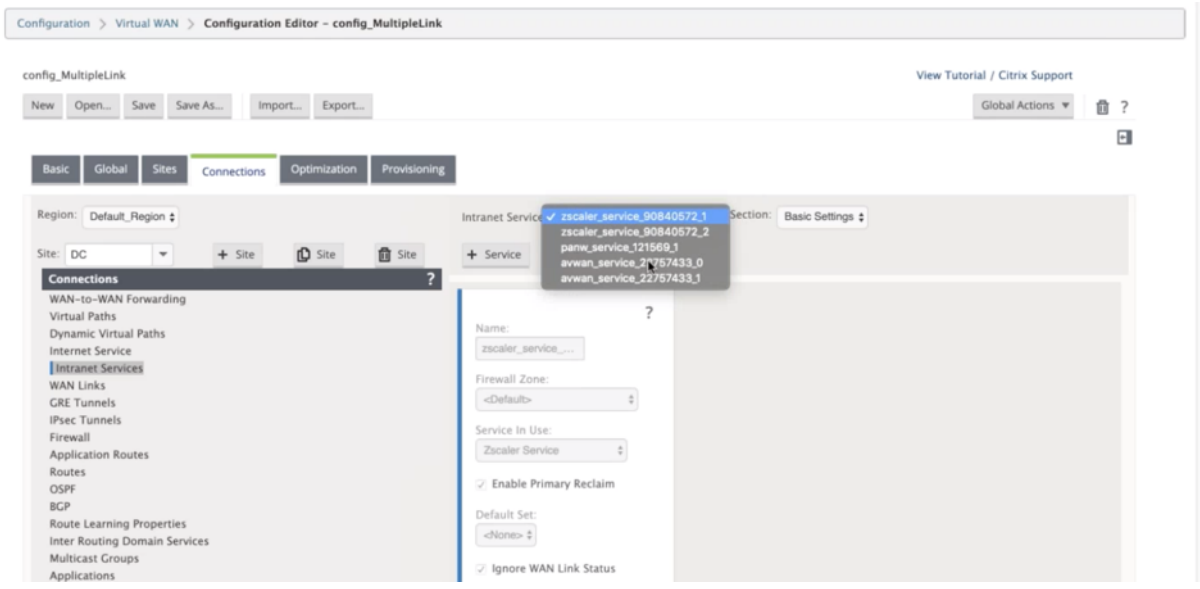
Cliquez sur l'icône **Actualiser** pour récupérer le dernier ensemble de ressources WAN que vous avez mis à jour sur le portail Azure. Un message indiquant « ressources WAN actualisées avec succès » s'affiche une fois le processus d'actualisation terminé.



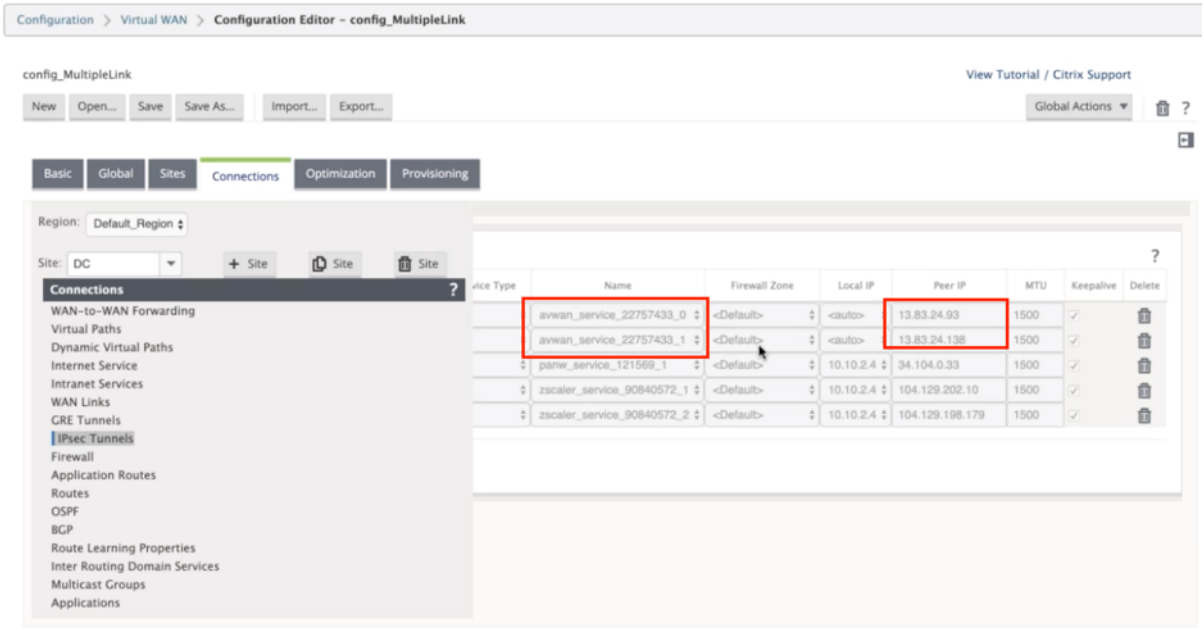
Supprimer l'association de ressources WAN du site Sélectionnez un ou plusieurs mappages pour effectuer la suppression. En interne, le processus de gestion des modifications de l'appliance SD-WAN est déclenché et jusqu'à ce qu'il réussisse, l'option Supprimer est désactivée pour empêcher d'effectuer d'autres suppressions. Pour supprimer le mappage, vous devez dissocier ou supprimer les sites correspondants dans le portail Azure. L'utilisateur doit effectuer cette opération manuellement.



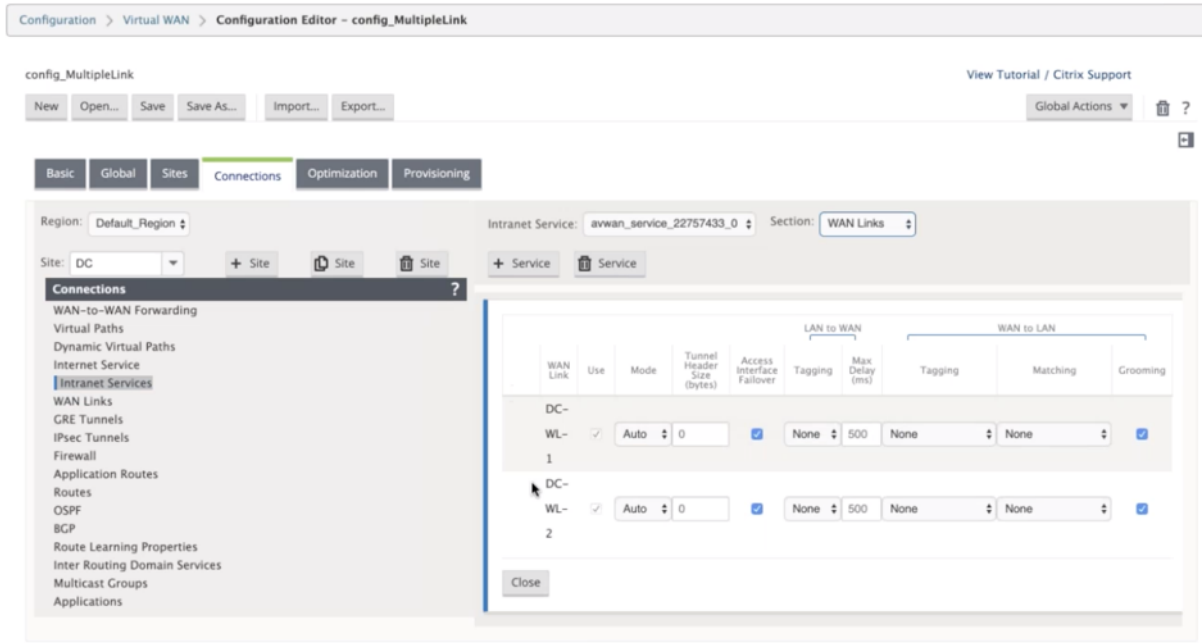
Une fois les tunnels créés, vous pouvez voir deux services intranet créés dans votre MCN.



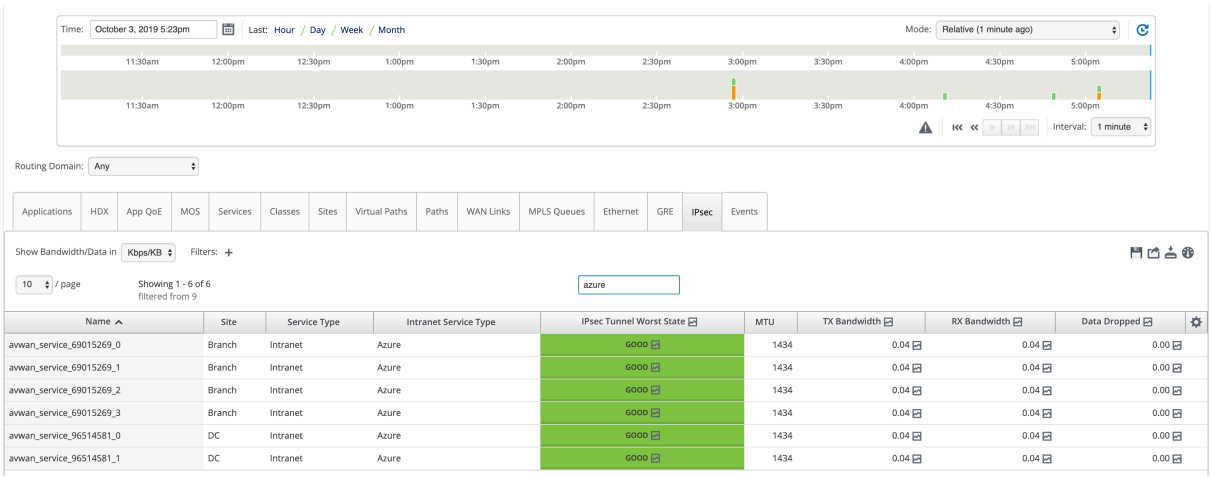
Chaque service Intranet correspond à des tunnels IPSec créés avec des IP homologues (IP de point de terminaison WAN virtuel Azure).



Dans les **Services Intranet**, si vous sélectionnez **Liens WAN** dans la liste déroulante **Section**, vous pouvez voir les liens WAN principal et secondaire que vous avez spécifiés. Par défaut, le mode est défini sur **Auto**.



Surveiller les tunnels IPSec Dans l'interface utilisateur du SD-WAN Center, accédez à **Reporting** > **IPsec** pour vérifier l'état des tunnels IPSec. L'état du tunnel doit être VERT pour que le trafic de données puisse circuler.



Service Cloud Direct

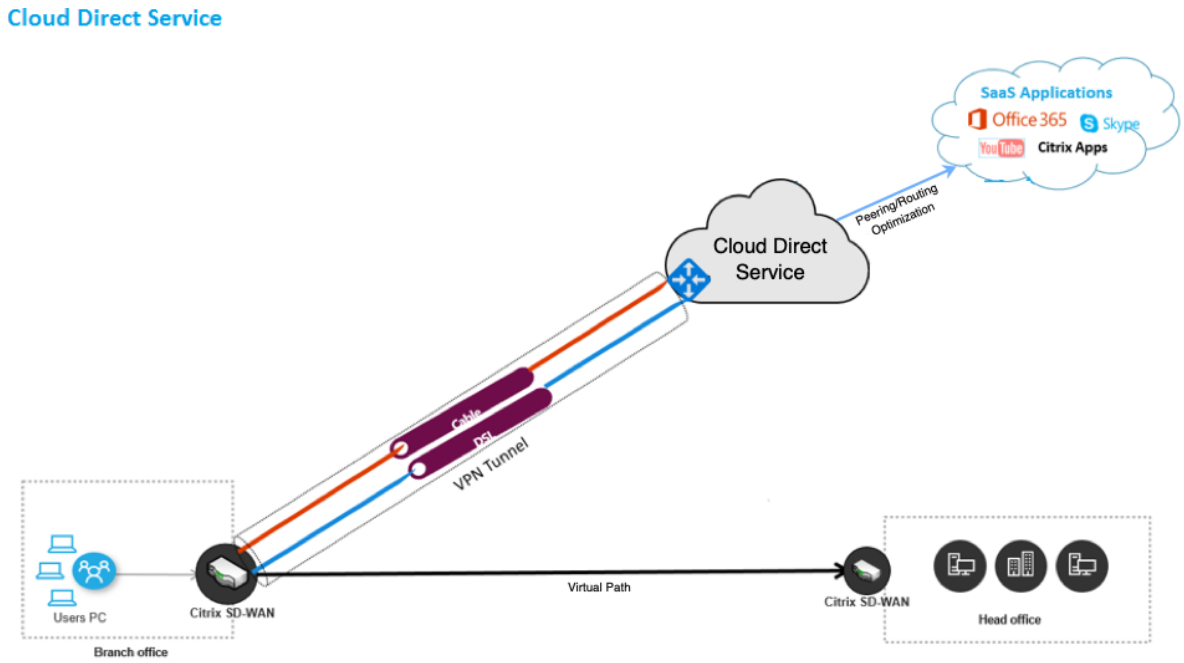
February 17, 2022

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

Le service Cloud direct offre les avantages suivants :

- **Redondance** - Utilise plusieurs liens WAN Internet et fournit un basculement fluide.
- **Agrégation de liens** - Utilise toutes les liaisons WAN Internet en même temps.
- Équilibrage intelligent de la charge entre les connexions WAN de différents fournisseurs :
  - Mesure de la perte de paquets, de la gigue et du débit.
  - Identification de l'application personnalisée.
  - Exigences des applications et correspondance des performances des circuits (s'adapter aux conditions du réseau en temps réel).
- Qualité de service dynamique de qualité de service de niveau SLA Capacité au circuit Internet :
  - S'adapte dynamiquement à un débit de circuit variable.
  - Adaptation à travers le tunnel aux extrémités d'entrée et de sortie.
- Réacheminement des appels VOIP entre les circuits sans laisser tomber l'appel.
- Surveillance et visibilité de bout en bout.

Flux de travail de service direct cloud



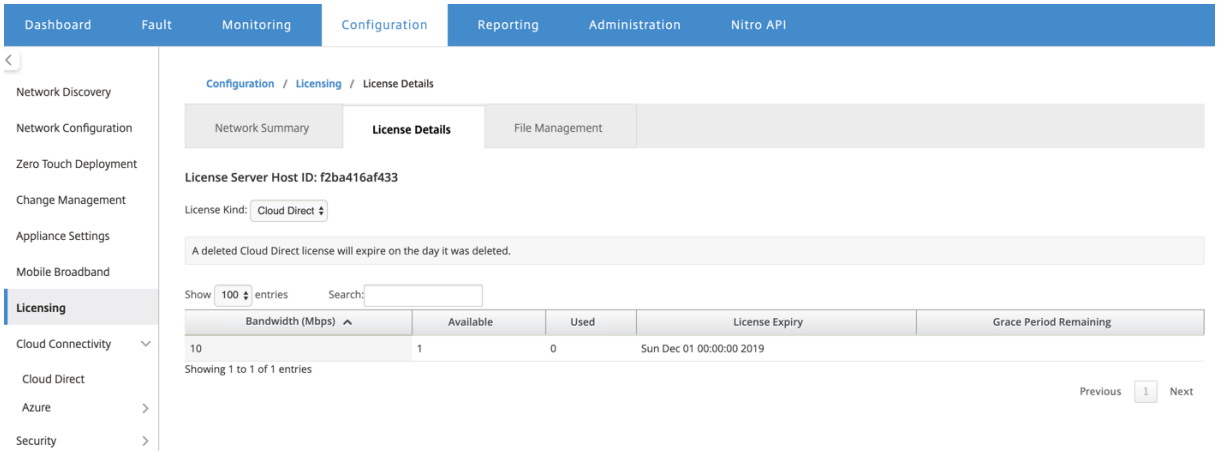
Avant de commencer le déploiement du service Cloud Direct, assurez-vous que les étapes suivantes sont terminées :

1. Disposez d'une appliance 410-SE, 210-SE ou 1100-SE/PE. Si la version SD-WAN expédiée en usine de l'appliance est antérieure à la version 9.3.5, vous devez suivre la procédure de réinitialisation USB pour mettre à niveau l'appliance vers la dernière image de base d'expédition.
2. Effectuez la procédure de mise à niveau en une étape pour installer la version du logiciel qui prend en charge Cloud Direct Service.
3. Configurez l'appliance MCN et établissez les chemins virtuels avec ses branches :
    - Configurer le site de succursale. Voir Configurer la branche pour plus d'informations.
    - Créez des objets d'application pour des itinéraires basés sur des applications.
        - Si vous avez l'intention de diriger de manière sélective les applications via le service direct Cloud, créez les objets d'application en incluant les applications correspondantes, consultez comment créer des objets d'application, qui sont routés via le service direct Cloud. Pour gérer le trafic lié à Internet, le service Internet doit être créé à partir de l'éditeur de configuration de l'appliance. Pour plus d'informations, consultez la section Service Internet.
        - Si vous avez l'intention de diriger tout le trafic lié à Internet via le service direct Citrix Cloud, vous pouvez ignorer la création des objets d'application spécifiques.

Gestion des licences

La fonctionnalité de service Cloud Direct est sous licence indépendamment des licences de base du SD-WAN. Assurez-vous d'avoir installé les licences requises pour le service Cloud Direct sur SD-WAN Center. Pour plus d'informations, consultez Citrix SD-WAN Center en tant que serveur de licences.sd-wan-center-as-license-server.

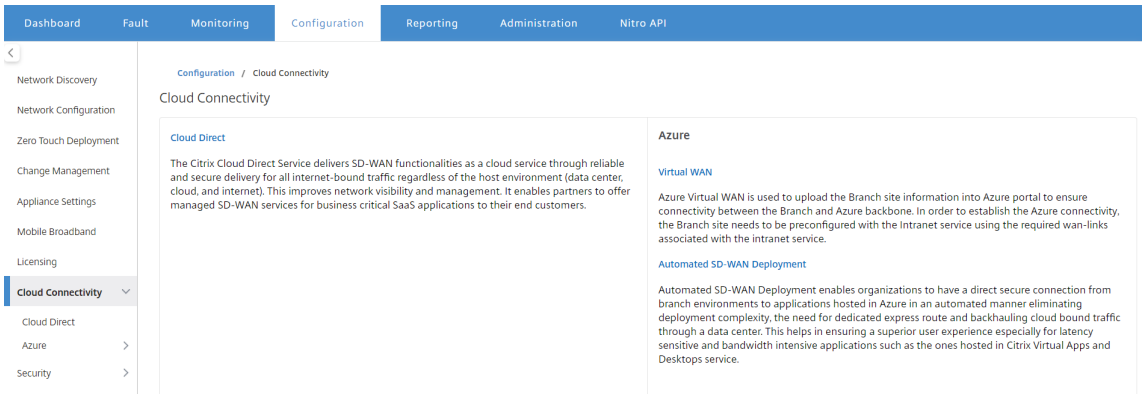
La page Licences fournit des détails sur les informations de licence du service Cloud Direct installées.



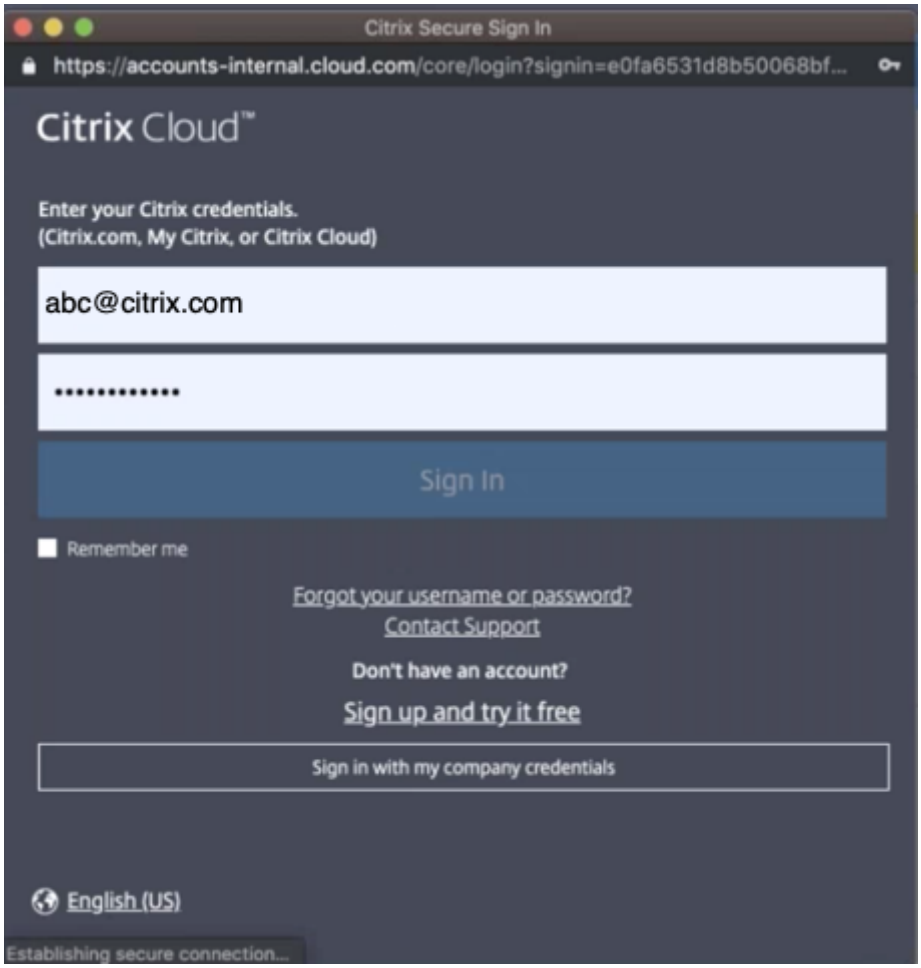
> **Remarque**
>
> Il existe un délai de grâce de 30 jours pour les licences Cloud Direct expirées ou supprimées, avant laquelle vous devez installer les licences valides pour que les sites Cloud Direct déployés soient fonctionnels. Si aucune licence valide n'est installée avant l'expiration du délai de grâce, SD-WAN Center désactive le service Cloud Direct sur site à l'aide de la licence expirée.

Configurer le service direct cloud dans SD-WAN Center

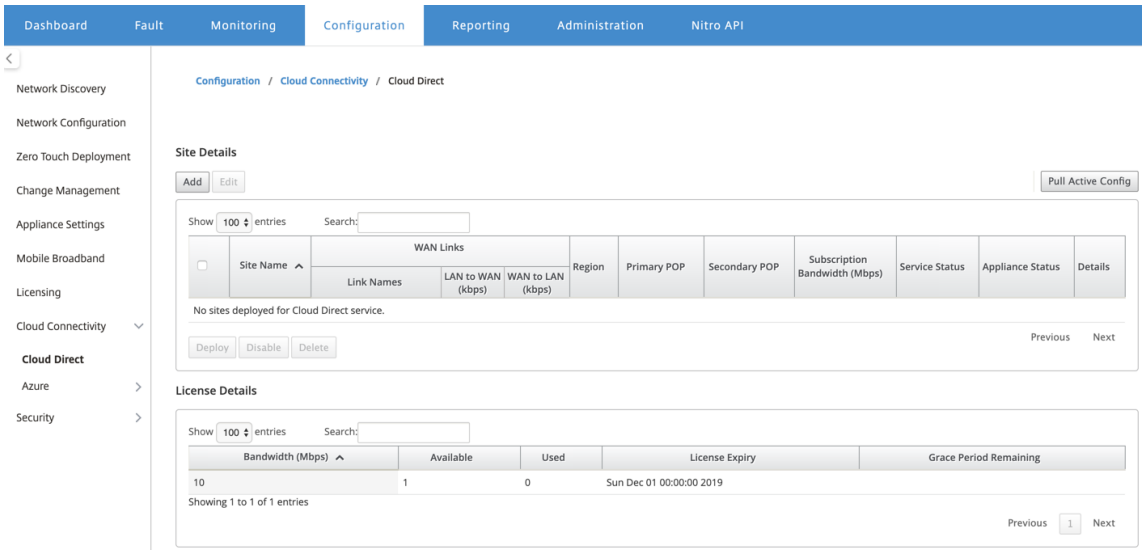
1. Dans l'interface graphique de SD-WAN Center, accédez à **Configuration** > **Cloud Connectivity** > **Cloud Direct**.



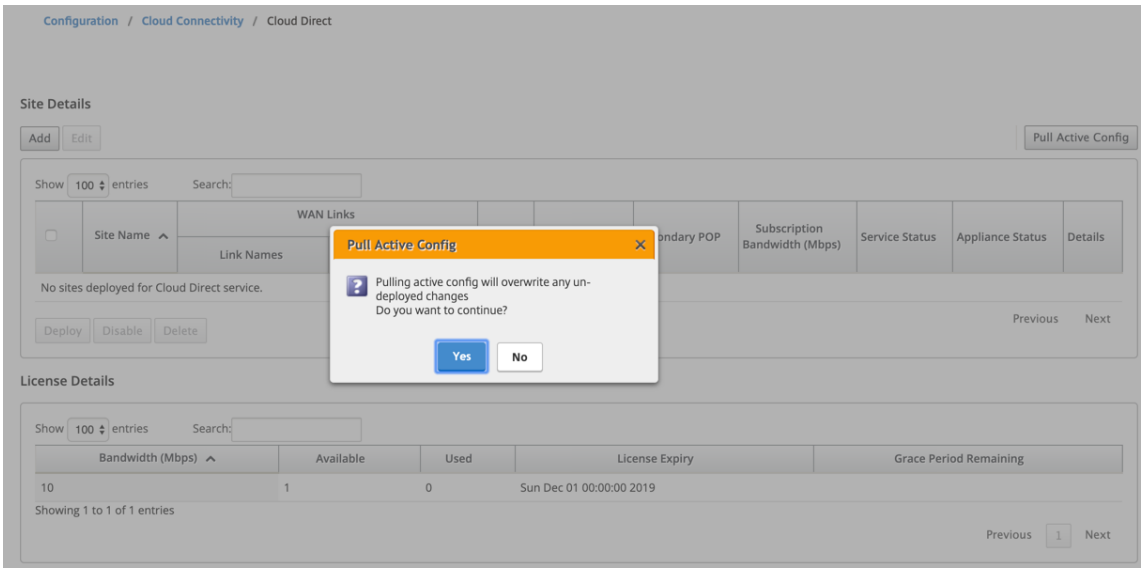
2. Connectez-vous avec les informations d'identification Citrix Cloud.



La page d'accueil Cloud Direct s'affiche une fois que vous vous êtes connecté au service Citrix Cloud.

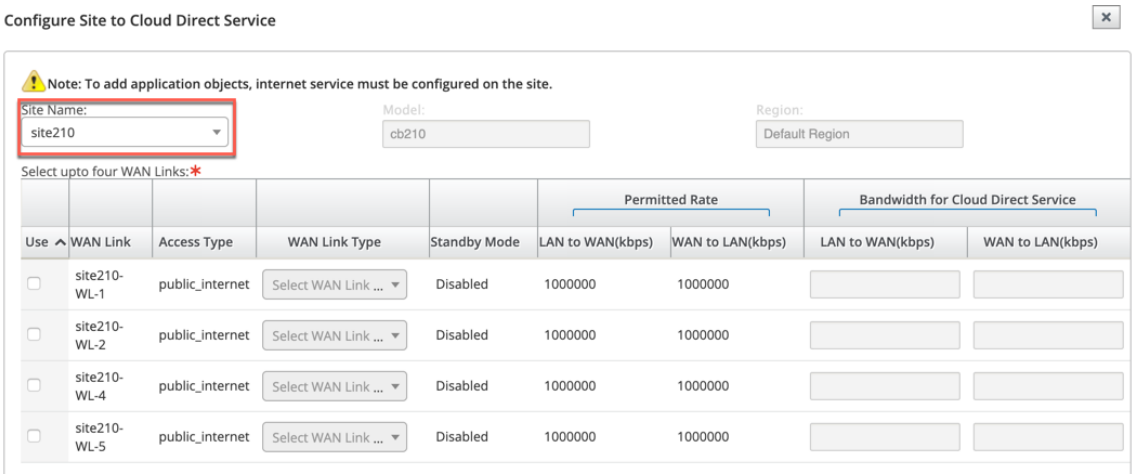


3. Cliquez sur **Pull Active Config** pour récupérer la dernière configuration MCN active.



4. Cliquez sur **Ajouter un nouveau site**. Les sites éligibles au déploiement du service Cloud Direct sont affichés dans le menu.

> **Remarque**
>
> - La fonctionnalité de service Cloud Direct est prise en charge sur les appliances matérielles 210, 410 et 1100.
> - À partir de la version 11.2, le service Cloud Direct est pris en charge sur les appliances SD-WAN 2100, 4100 et 6100. SD-WAN Center et Orchestrator permettent le déploiement de la fonctionnalité de service Cloud Direct sur les appliances SD-WAN 2100, 4100 et 6100. SD-WAN Center prend en charge jusqu'à 250 Mbit/s des licences d'abonnement pour Cloud Direct.

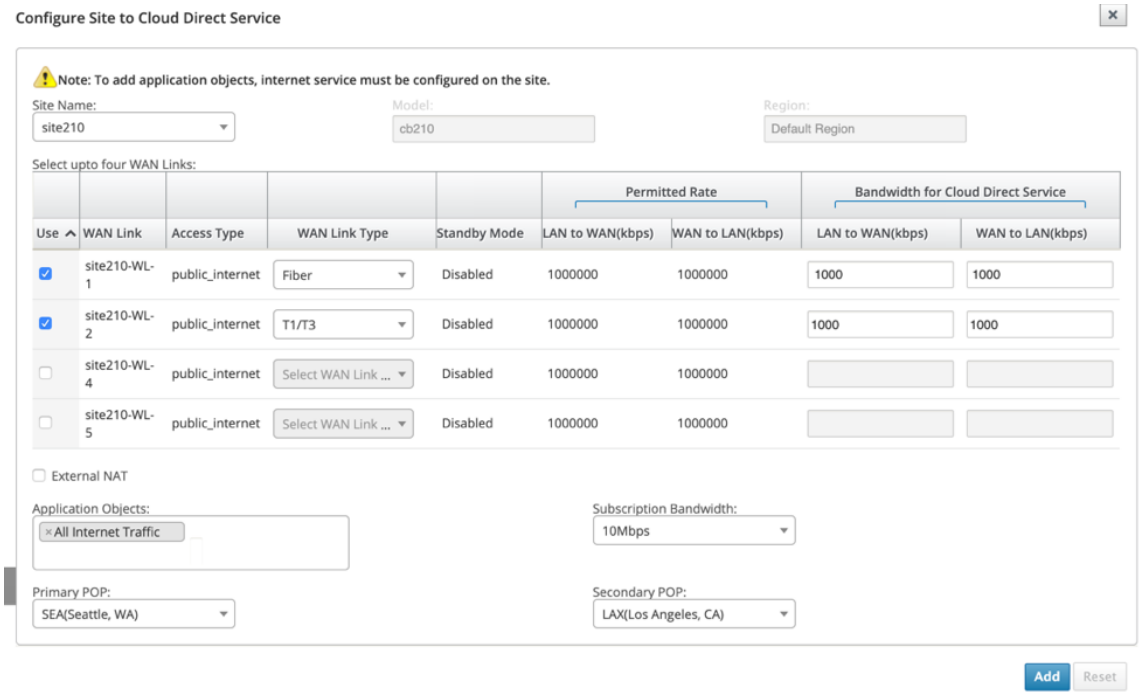


5. Lorsqu'un site est sélectionné, les liens WAN Internet publics qui sont associés au site sélec-

tionné sont affichés, ainsi que les informations sur le modèle de l'appliance et la région dans laquelle l'appliance est déployée.

6. Sélectionnez les liens WAN que vous souhaitez utiliser pour le trafic du service Cloud Direct, ainsi que les options **Type de liaison WAN**, **Objets d'application**, **Bande passante d'abonnement**, **POP principal**et **POP secondaire**.

> **Remarque**
>
> - Jusqu'à quatre liaisons WAN sont prises en charge pour le service Cloud Direct.
> - Une bande passante de liaison WAN n'est plus nécessaire pour être réservée exclusivement au service Cloud Direct. Si le service Cloud Direct n'est pas actif, les autres services tels que le chemin virtuel, les services Internet ou intranet configurés sur cette liaison WAN peuvent utiliser la bande passante selon les partages configurés.



- **Nom du site** : affiche les sites éligibles au déploiement de la fonctionnalité Cloud Direct.
- **Modèle** : pour le site sélectionné, le nom du modèle d'appliance correspondant est renseigné automatiquement.
- **Région** : pour le site sélectionné, les détails de la région déployée spécifique à l'appliance sont renseignés automatiquement.
- **Lien WAN** : pour le site sélectionné, les liens WAN Internet publics associés sont affichés.
- **Type de lien WAN** : sélectionnez le type de liaison WAN dans le menu.
- **Mode veille** : Le mode veille est récupéré à partir de la configuration de la liaison WAN.

- **Bande passante pour le service Cloud Direct** : entrez la bande passante que le service Cloud Direct peut utiliser exclusivement. La bande passante sélectionnée doit être inférieure à la bande passante autorisée configurée et ne peut pas être utilisée par les services Virtual Path, Internet et Intranet.
- **NAT externe** : Il est nécessaire que le trafic Internet public provenant du réseau local de la branche soit NAT source à partir d'une adresse IP spécifique. Par défaut, cette opération est effectuée automatiquement et prise en charge dans le cadre de la configuration du réseau SD-WAN. Si vous souhaitez configurer l'IP NAT (réseau LAN) en dehors du périphérique SD-WAN (par exemple, dans un pare-feu externe), vous pouvez choisir l'option NAT externe lors du déploiement de sites. L'adresse IP sur laquelle le trafic LAN doit être le NAT source est disponible dans la page **Détails** du site Cloud Direct déployé.
- **Objets d'application** : vous pouvez choisir des objets d'application spécifiques ou sélectionner « Tout le trafic Internet » à rediriger via le service Cloud Direct. Dans le cas où les objets d'application spécifiques sont sélectionnés, le trafic de ces applications est envoyé via le service Cloud Direct et le reste du trafic est dirigé à l'aide du service Internet configuré sur la solution matérielle-logicielle.
- **Bande passante**d'abonnement : La bande passante d'abonnement est associée à la licence pour le service cloud direct.
- **Mode de facturation** : lorsqu'un client envisage de déployer un site Cloud Direct dans le cadre de la validation de validation de principe (POC), le champ **Mode de facturation** doit être défini comme **Démo**. Dans tous les autres cas, définissez le mode de facturation sur **Production**.

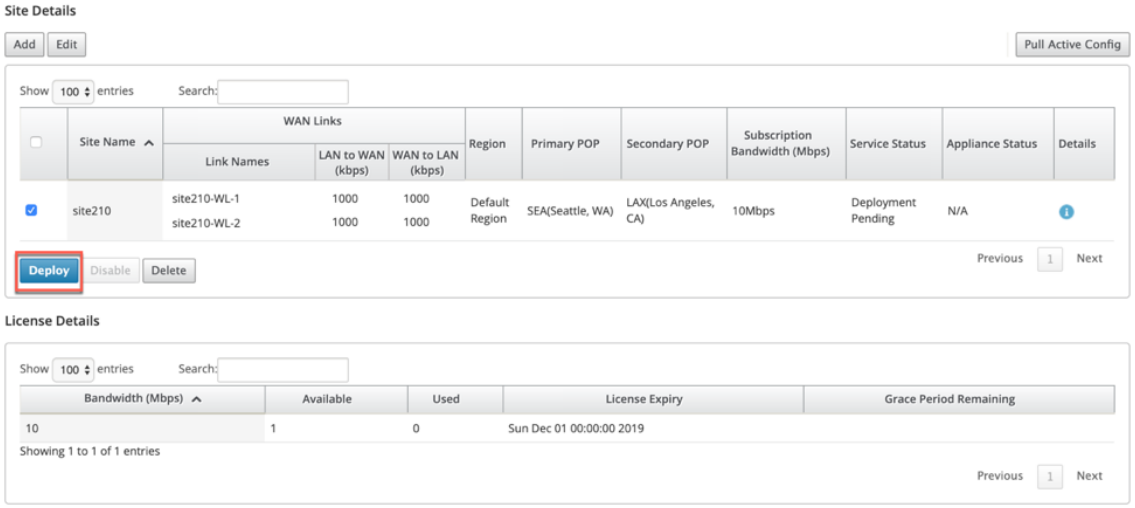
> **REMARQUE :** La situation suivante se produit, si le **mode de facturation** est sélectionné comme **Démo** ou **Production** :
>
> - Si un site Cloud Direct est créé avec le **mode de facturation en** tant que **démo**, les paramètres peuvent être modifiés dans Production.
> - Si un site Cloud Direct est créé avec le **mode de facturation en** tant que **production**, le paramètre ne peut pas être modifié sur **Démo**.

L'option **Mode de facturation** permet l'utilisation des licences d'essai et d'évaluation Cloud Direct, qui peuvent être fournies par les partenaires commerciaux Citrix ou autorisés. Les sites fonctionnant avec des licences d'évaluation Cloud Direct doivent être configurés sur l'option **Mode de facturation de démonstration**. Les sites qui sont mis à niveau vers des licences d'abonnement Cloud Direct complètes doivent être configurés sur l'option **Mode de facturation de production**.

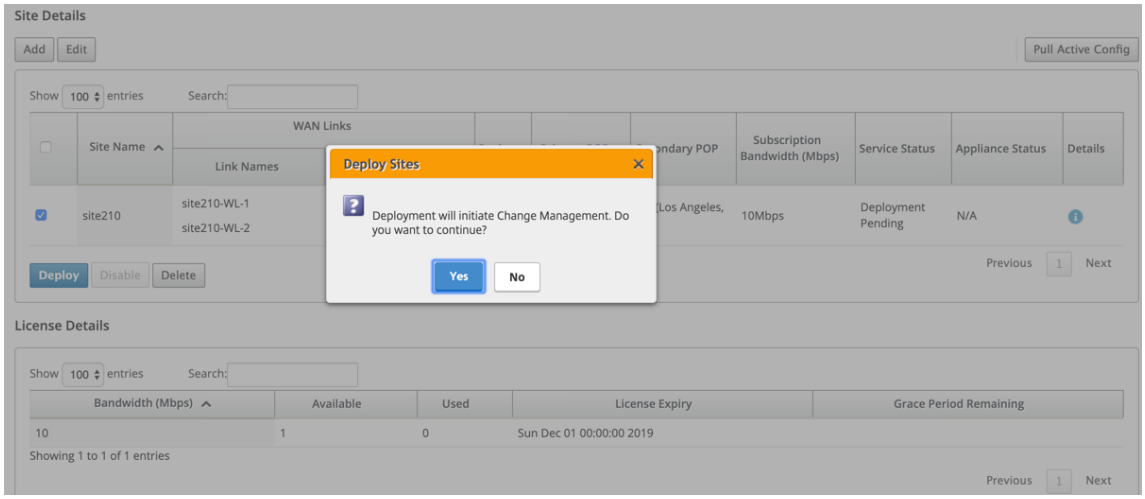
- **POP primaire/secondaire** : Assurez-vous que le POP primaire et secondaire n'est pas le même. Sélectionnez les POP en fonction de la proximité de l'emplacement. Cliquez sur

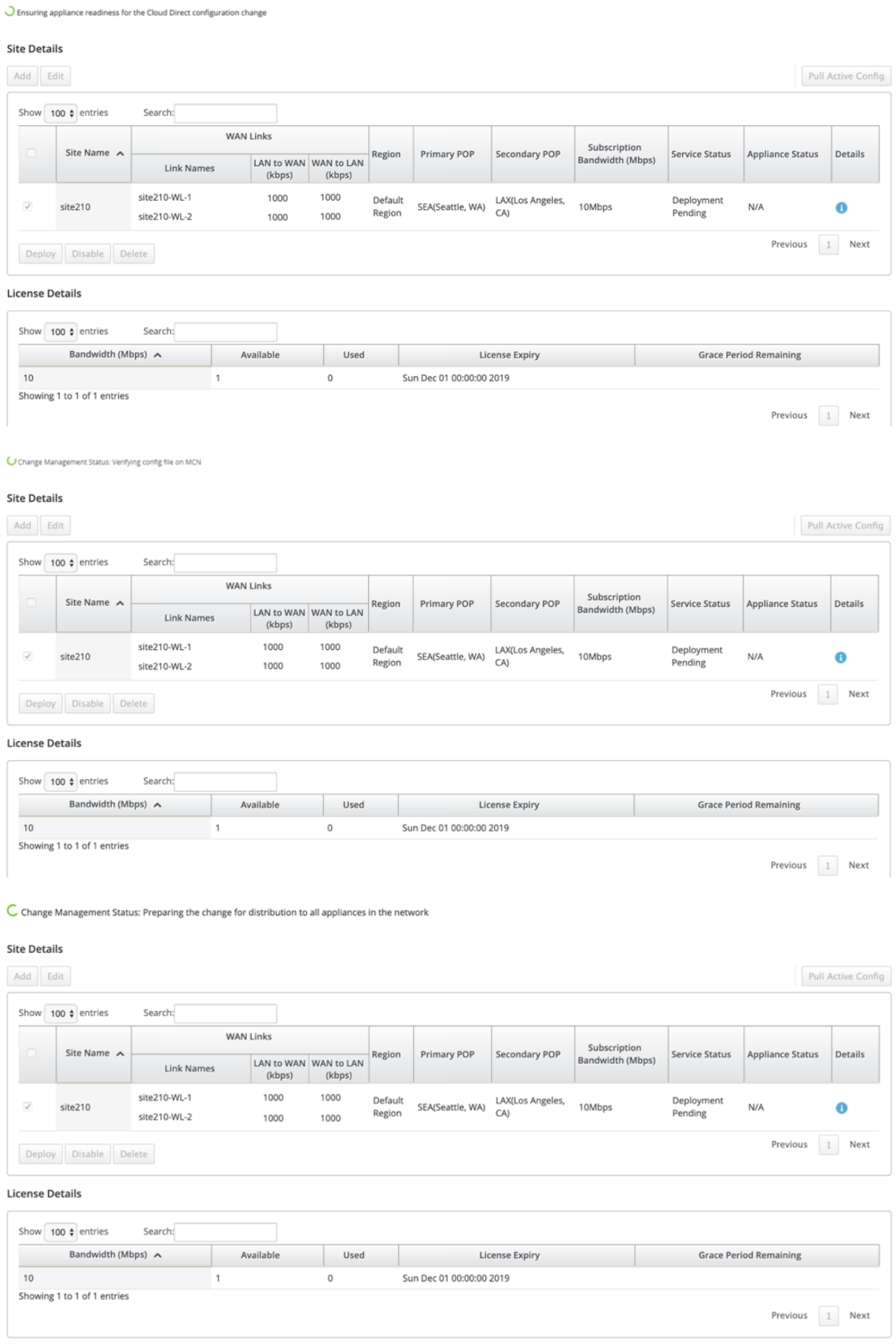
Ajouter.

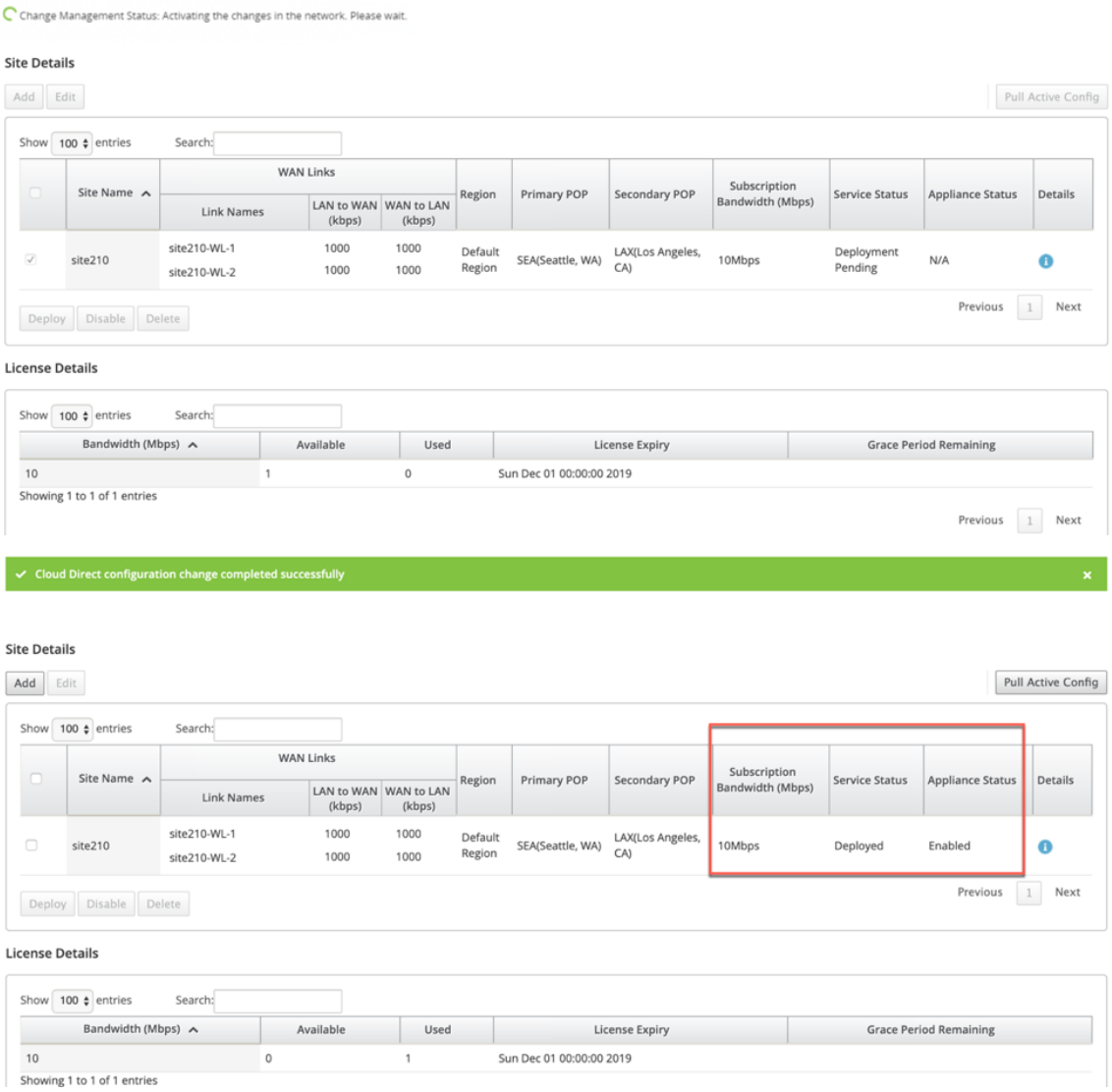
7. Une fois les sites ajoutés, l'état du service apparaît comme **Déploiement est en attente**. Sélectionnez le site pour lequel vous souhaitez déployer le service Cloud Direct, puis cliquez sur **Déployer**.



Une notification indiquant que l'opération de déploiement initie une gestion des modifications sur l'appliance MCN s'affiche. Vous pouvez cliquer sur **Oui** ou **Non**.





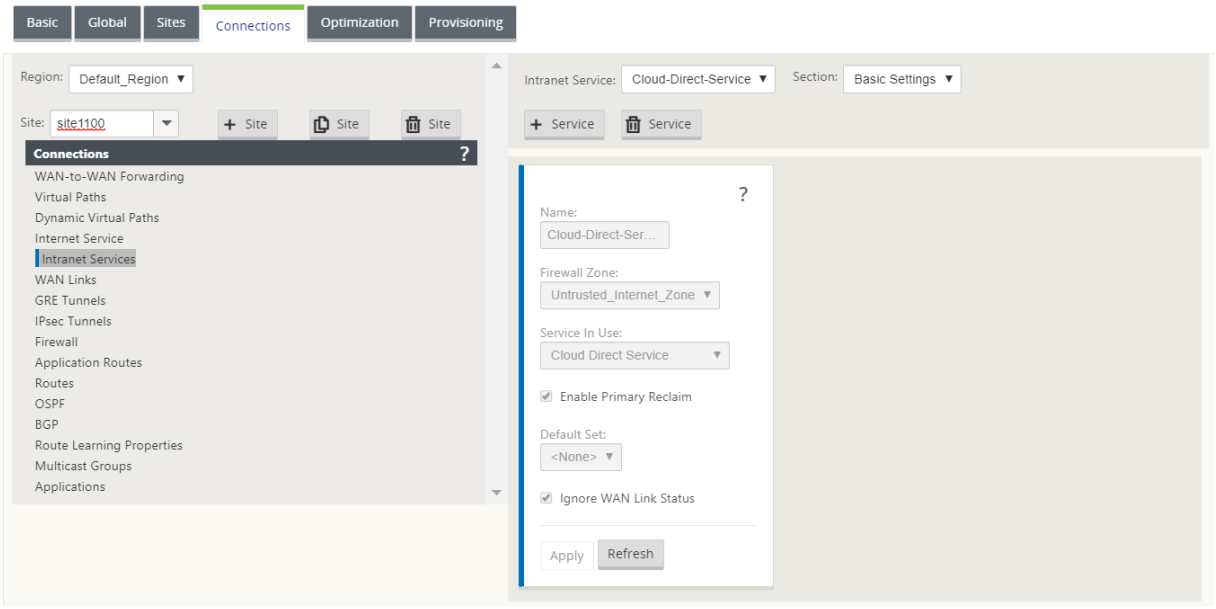


Après le déploiement réussi des sites, la page Cloud Direct Service affiche les éléments suivants :

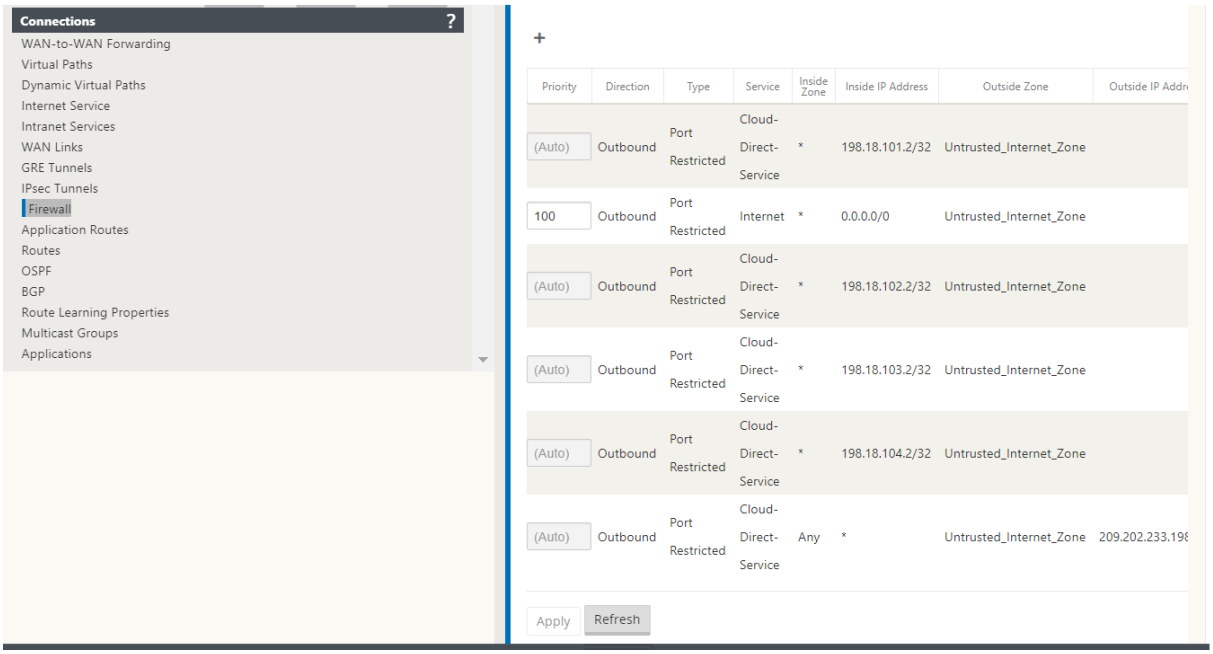
- **État du service** : déployé
- **État de l'appliance** : Activé
- **Bande passante d'abonnement (Mbps)** : 10 Mbps
- **Consommation de la licence installée**

L'étape de gestion des modifications ci-dessus génère automatiquement et ajoute les configurations de service Cloud Direct nécessaires à la configuration en cours d'exécution.

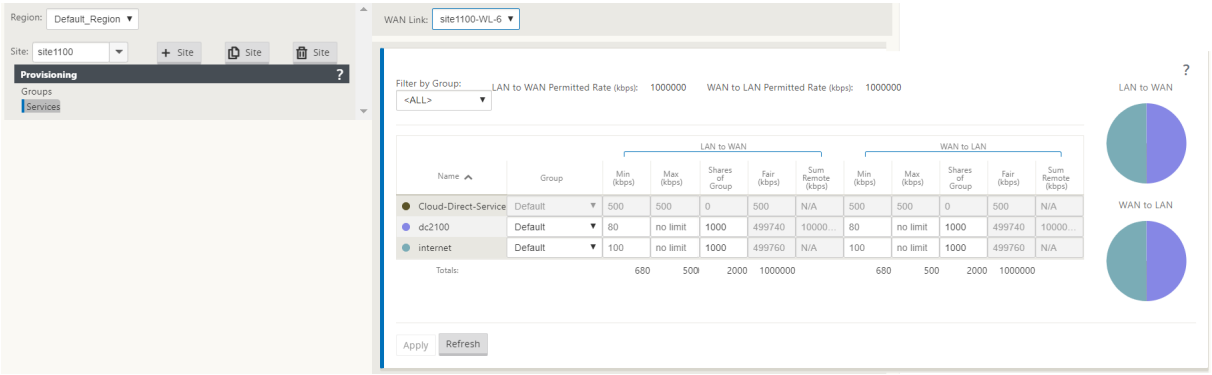
> **Remarque**
>
> Le service **Cloud Direct Service (service** intranet) créé automatiquement est associé à Default_RoutingDomain.



Paramètres pare-feu.

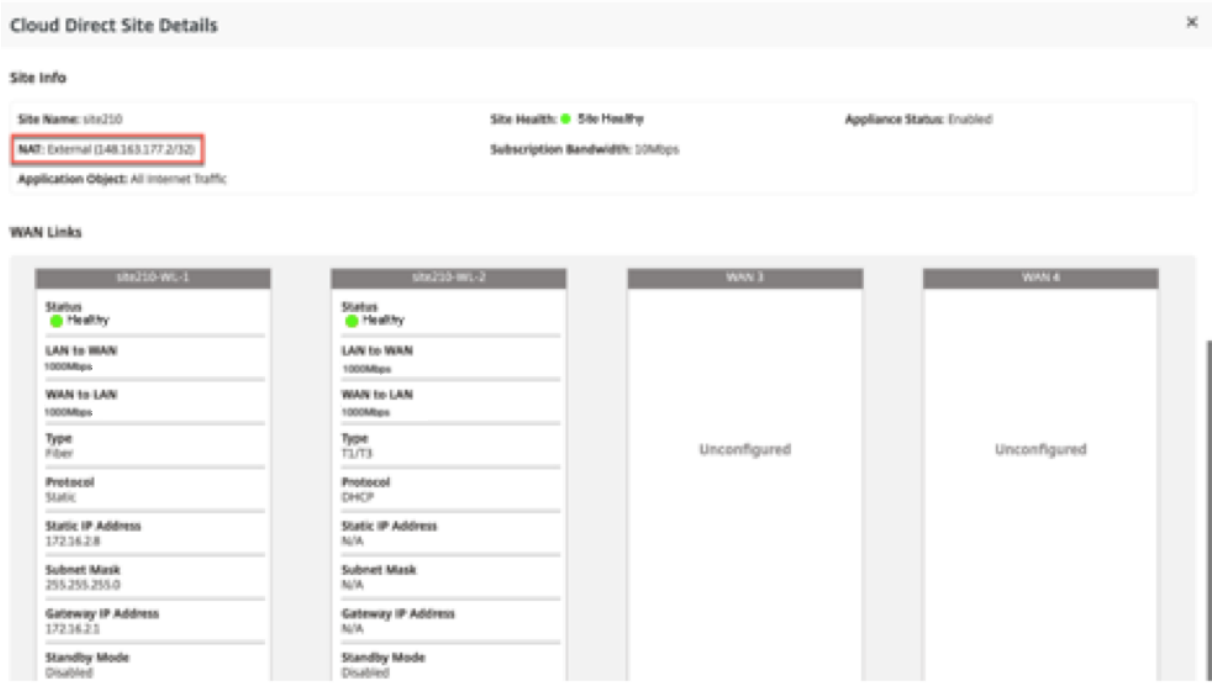


Provisioning de sites dans l'interface graphique de l'application SD-WAN

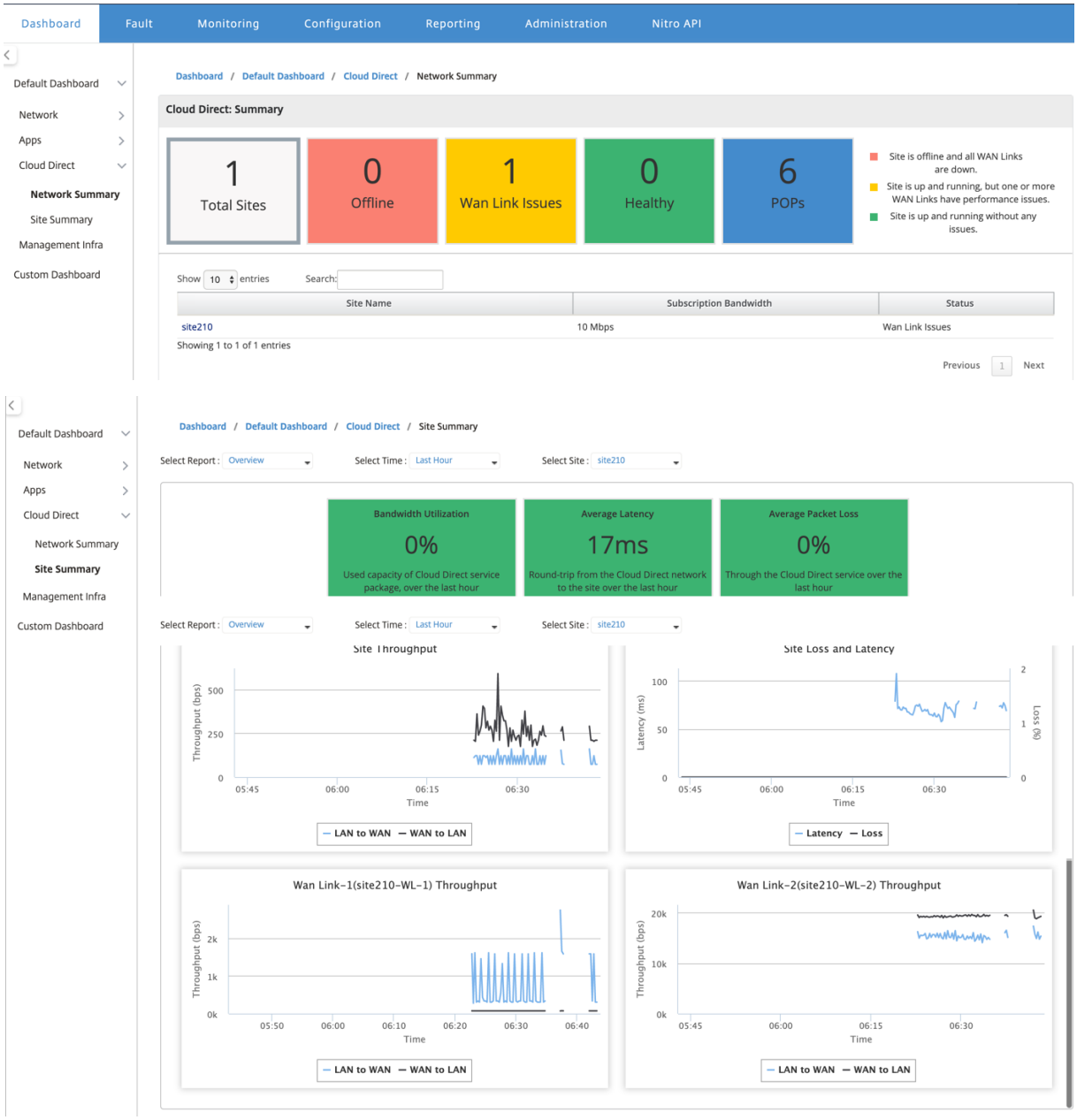


Surveillance du service Cloud Direct

Vous pouvez afficher le service Cloud Direct configuré une fois les sites déployés et activés. Cliquez sur l'icône d'exclamation dans la colonne **Détails** pour afficher les détails du site.



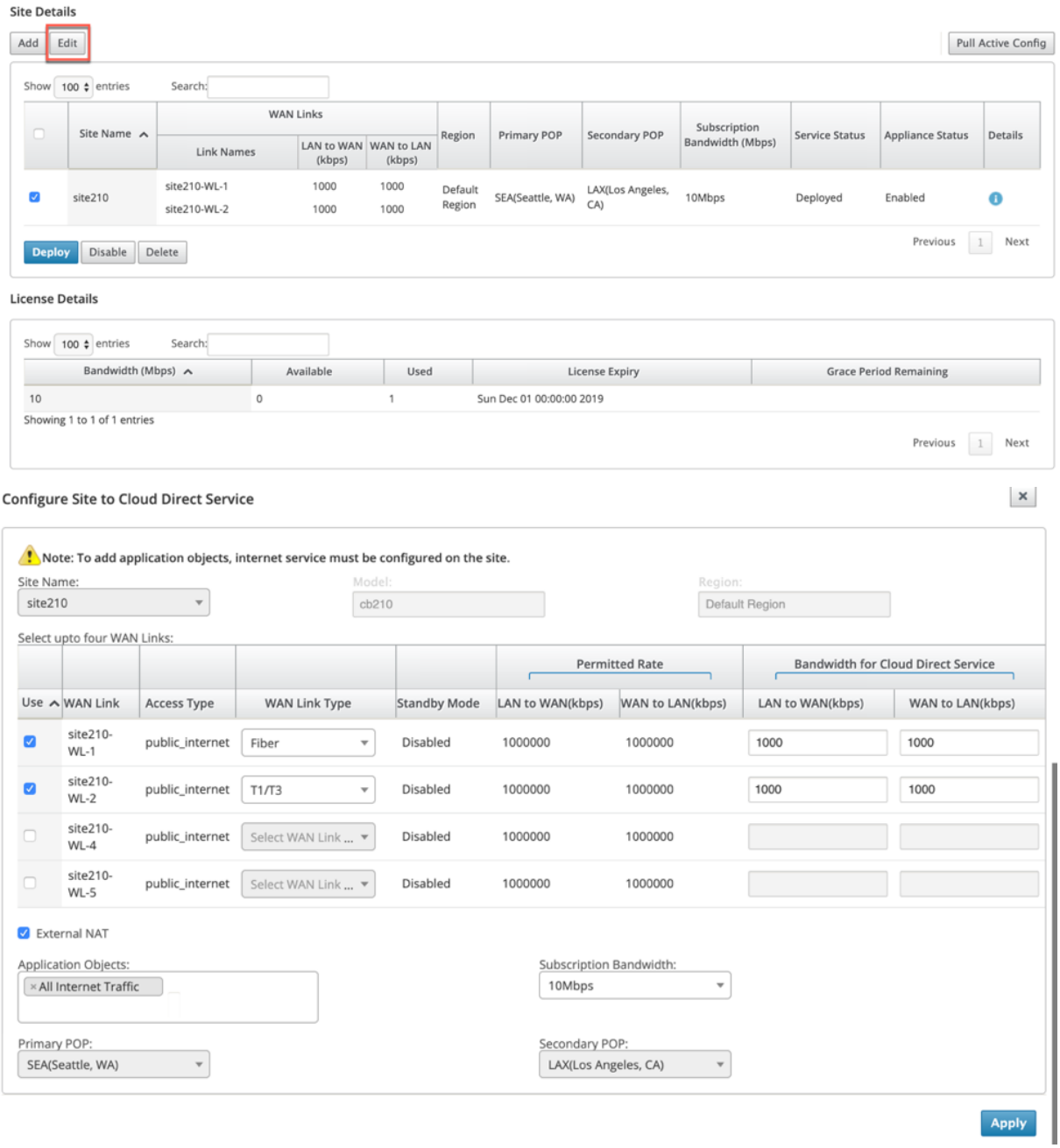
Vous pouvez afficher les graphiques récapitulatifs du site en accédant à **Tableau de bord** > **Cloud Direct** > **Récapitulatif du réseau** et **Résumé du site**.

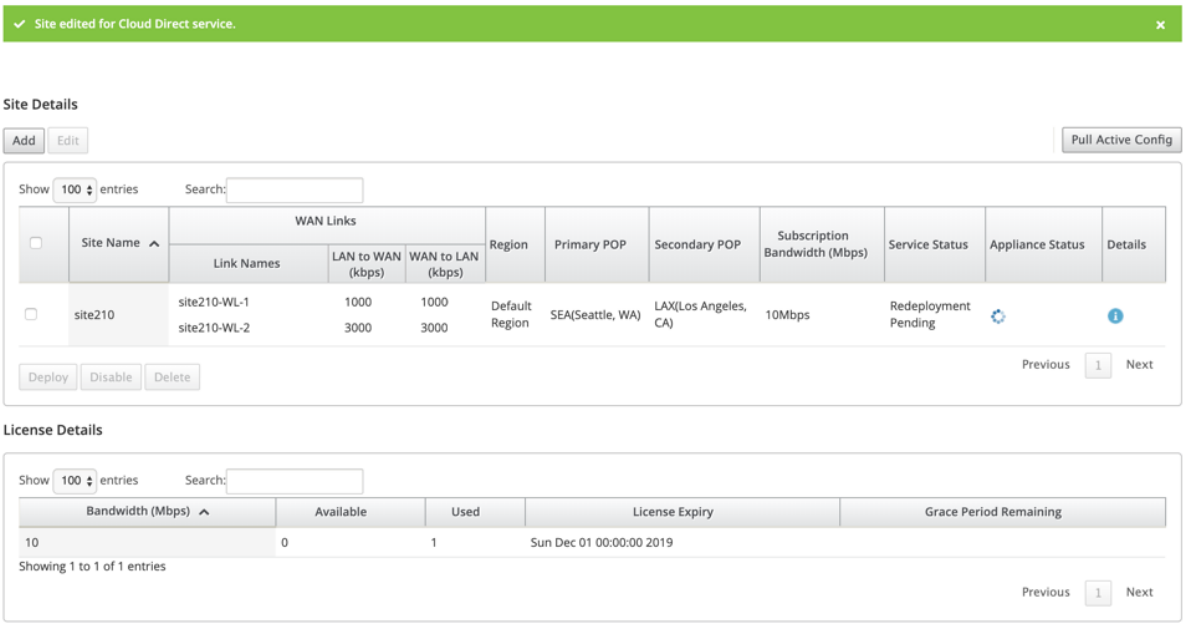


Modification du site dans SD-WAN Center

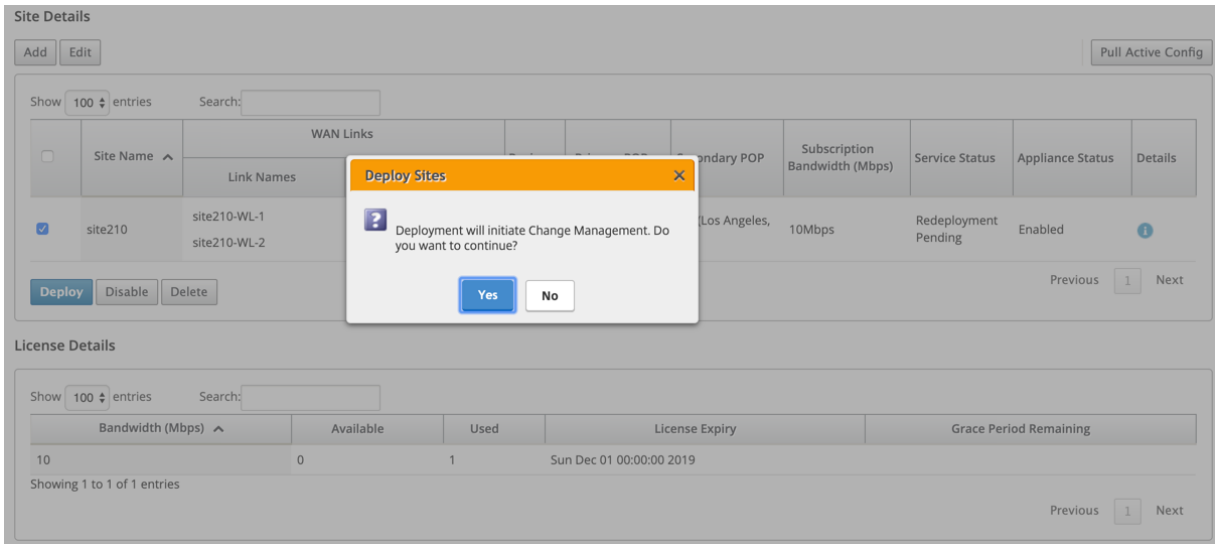
Vous pouvez choisir de modifier les sites pour modifier la bande passante et le type de lien WAN.

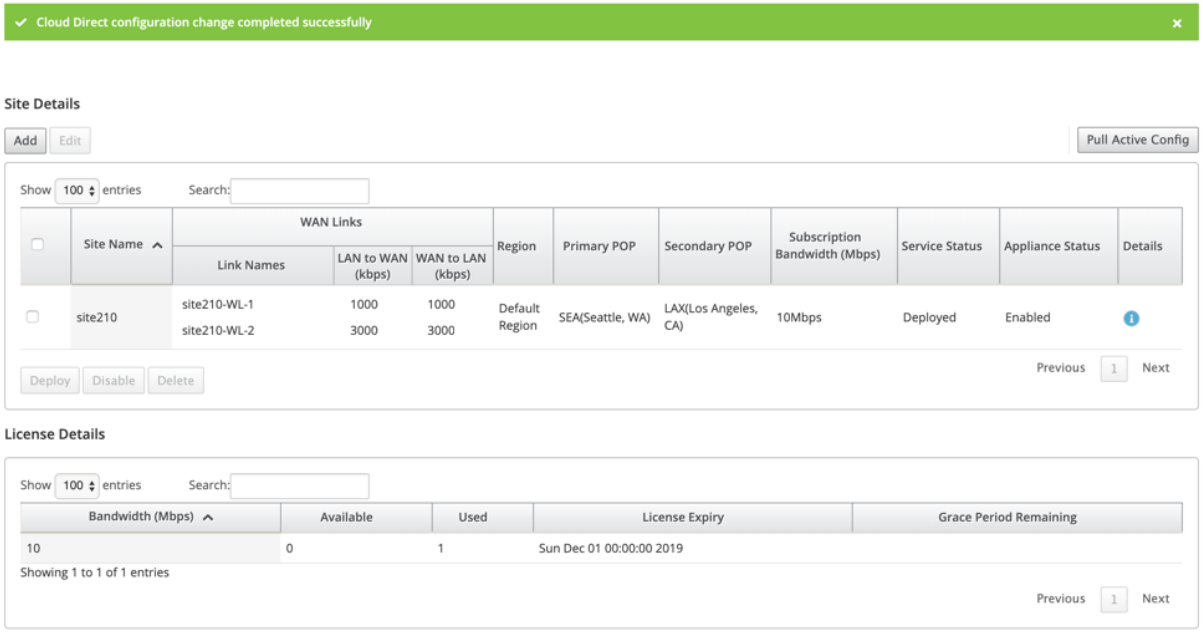
> **Remarque**
>
> Les sélections POP ne peuvent pas être modifiées.





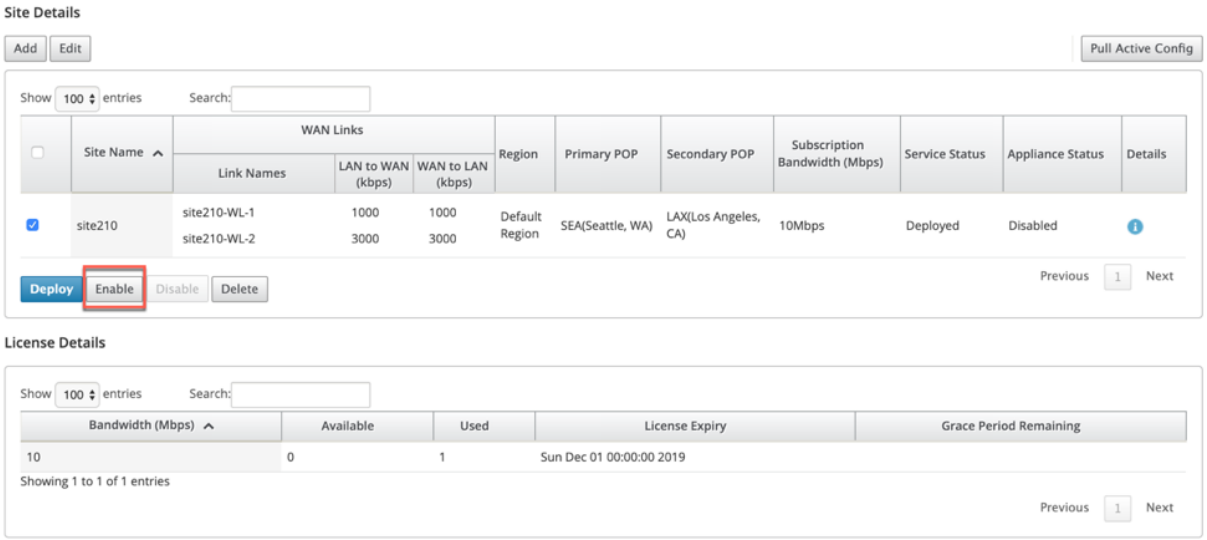
L'état du service s'affiche sous forme de redéploiement en attente. Déployez le site. Le processus de déploiement est terminé pour le site modifié.

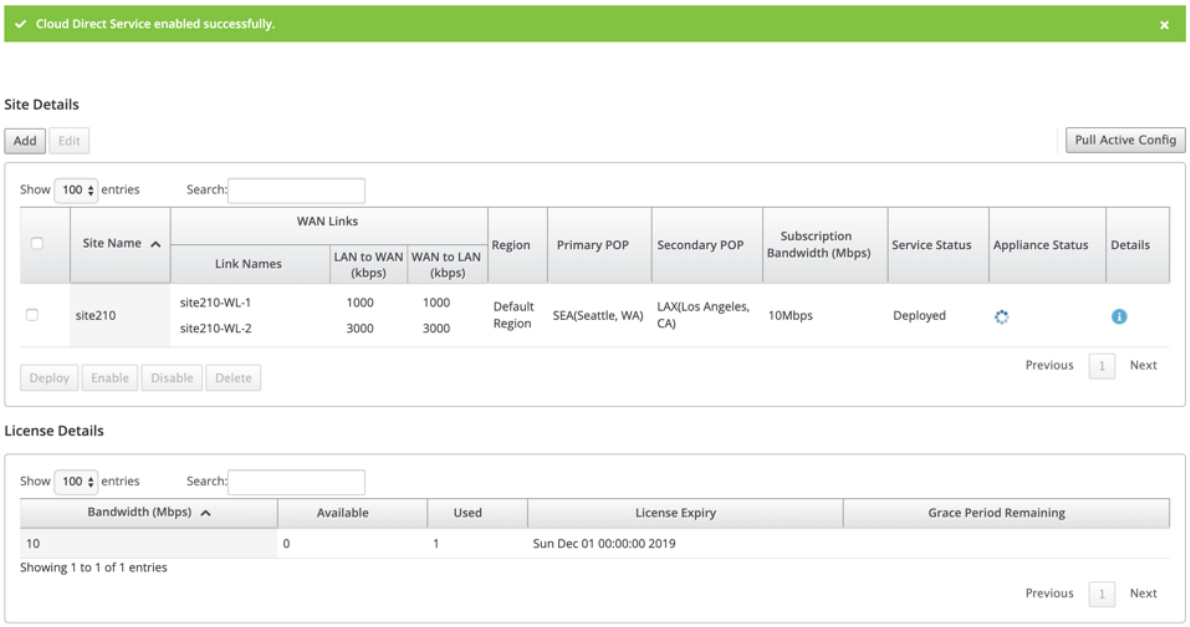




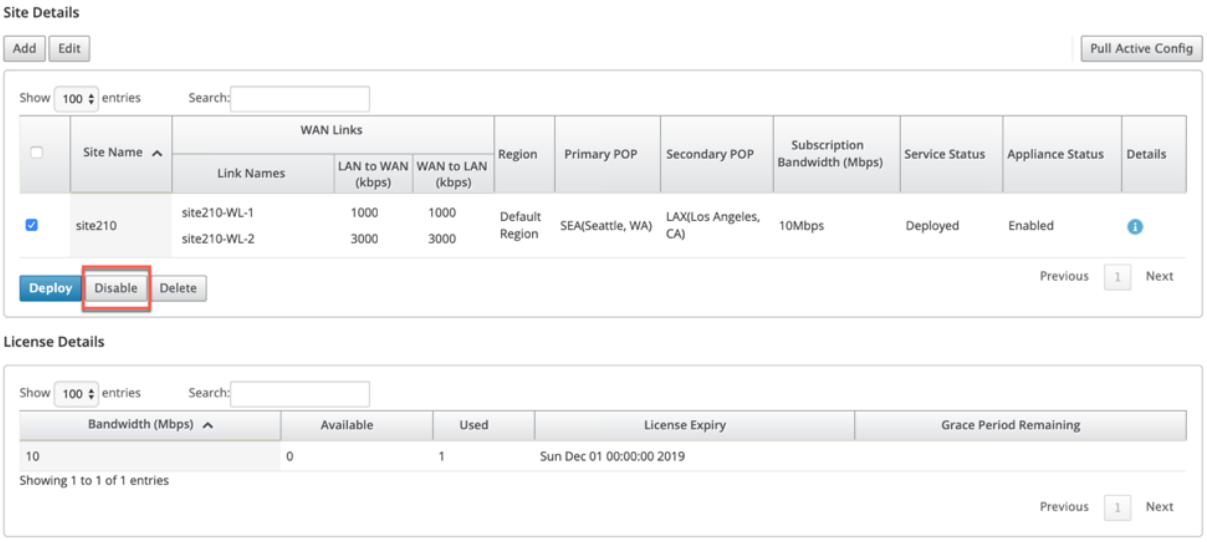
Activer et désactiver le site

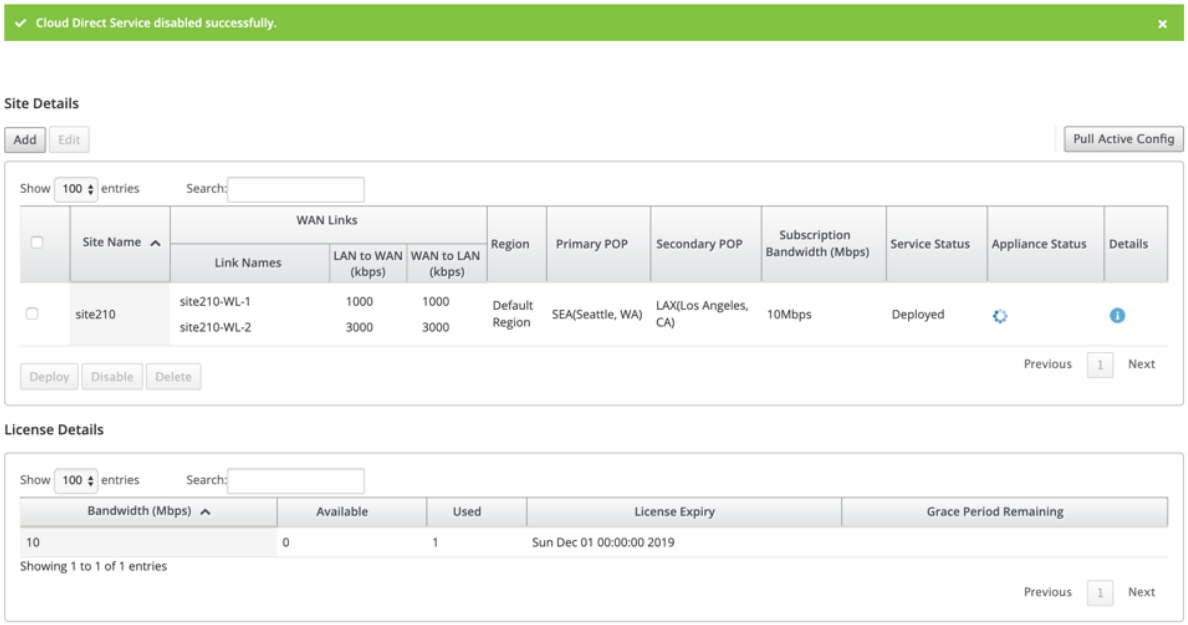
Vous pouvez activer un site déployé dont l'état de l'appliance est désactivé. Pour activer un site, cliquez sur **Activer**.





Cliquez sur **Désactiver** pour désactiver un site déployé. La désactivation du site n'utiliserait plus le service direct cloud pour diriger le trafic Internet. Tout le trafic est redirigé via le service Internet, s'il est configuré sur l'appliance.

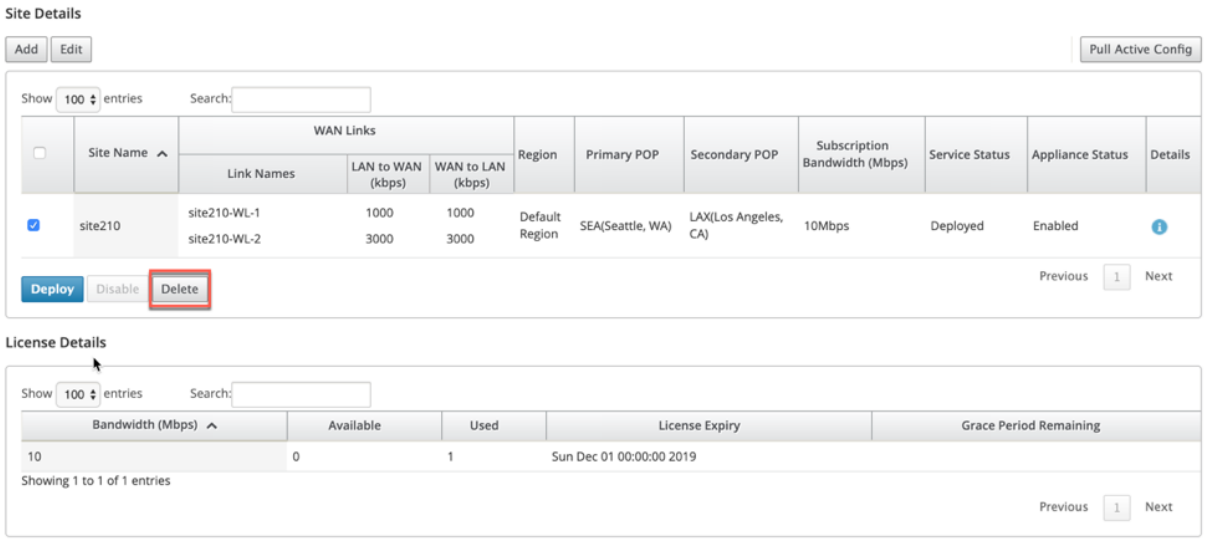


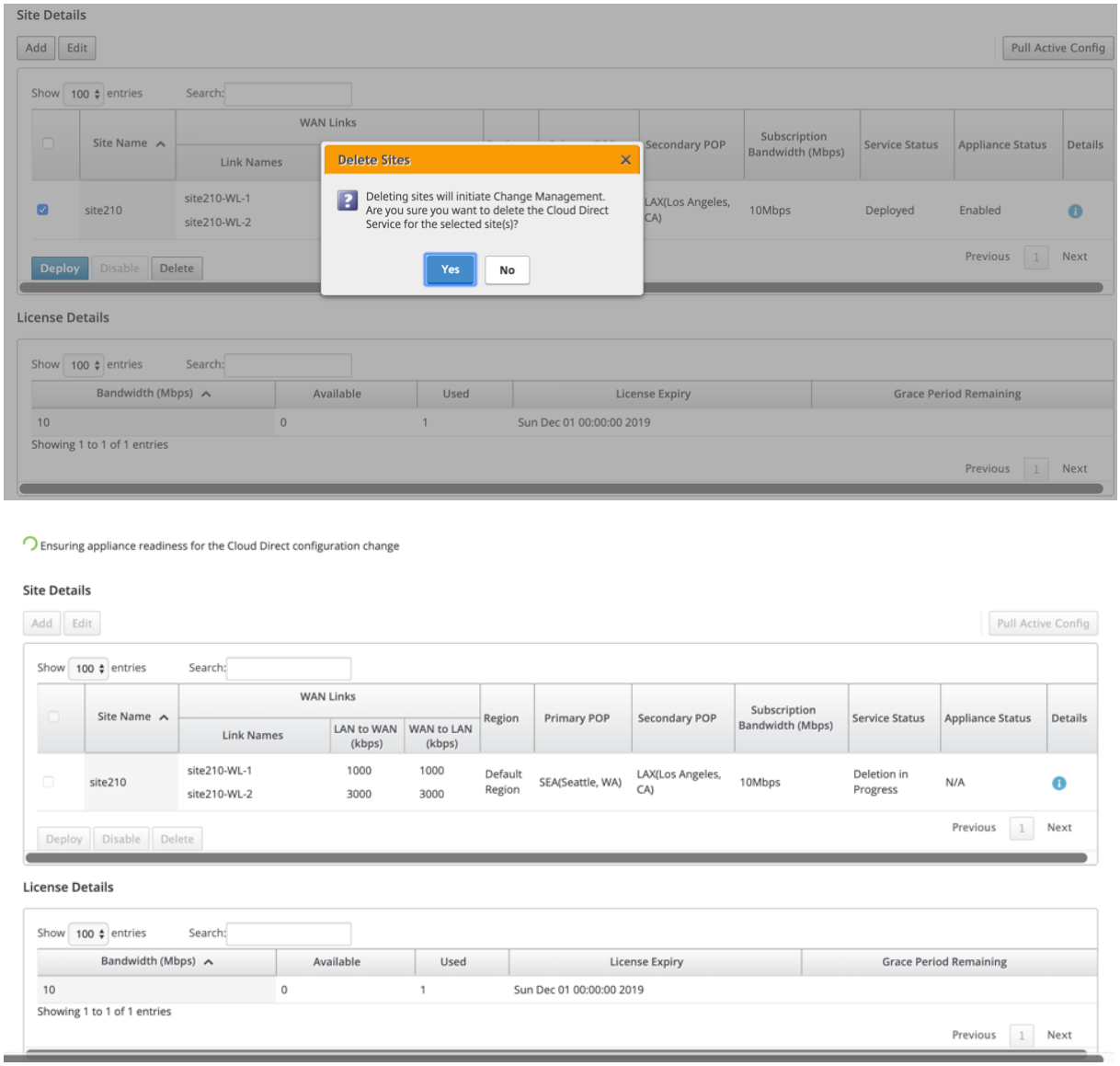


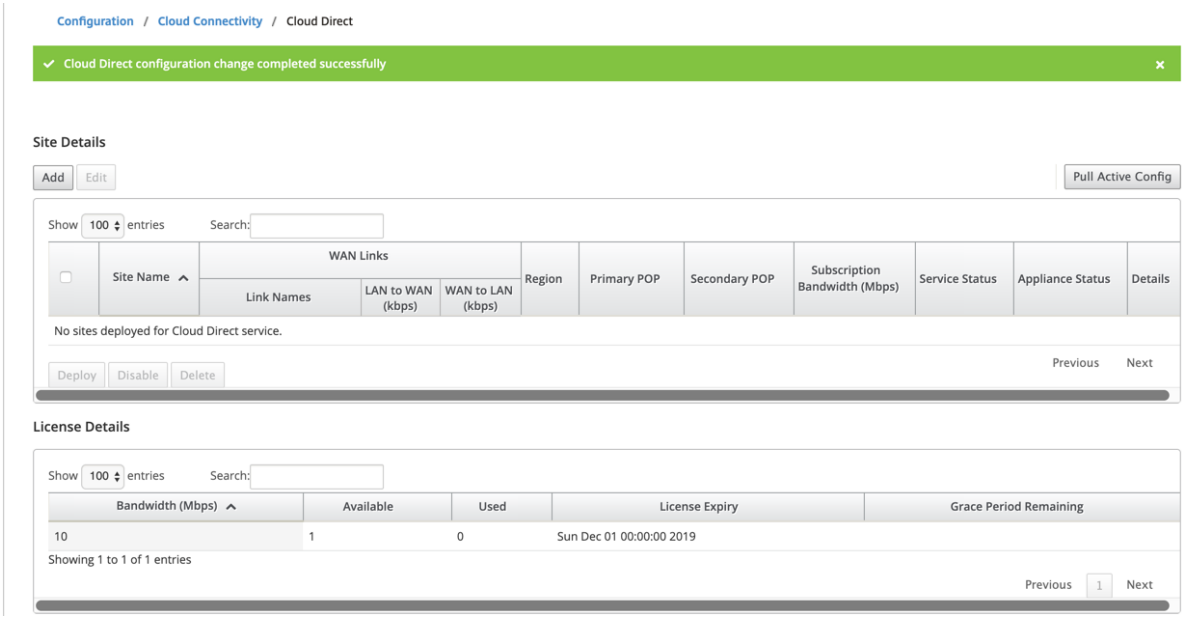
Suppression du site

Vous pouvez choisir de supprimer les sites qui ne nécessitent plus de connectivité Cloud Direct. Pour supprimer des sites, sélectionnez le site et cliquez sur **Supprimer**. Un message de confirmation pour supprimer des sites s'affiche.

Toute configuration de service direct cloud est supprimée par le processus de gestion des modifications.



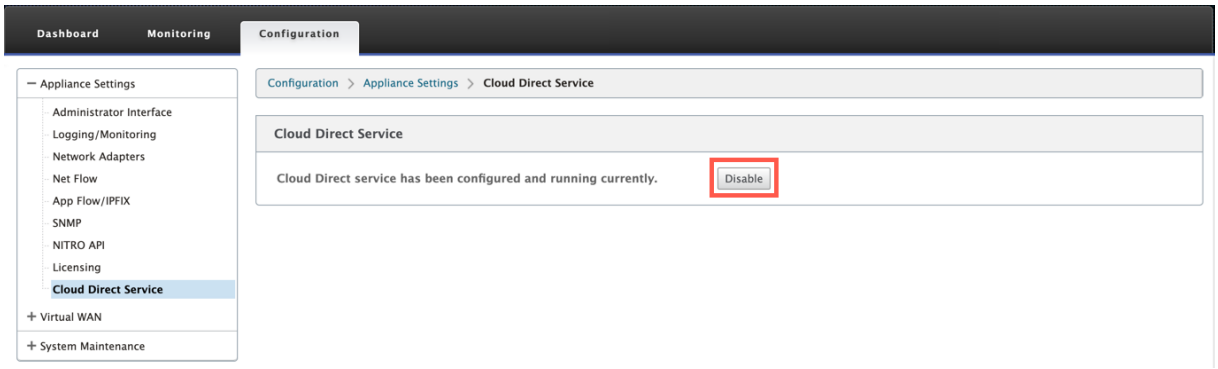




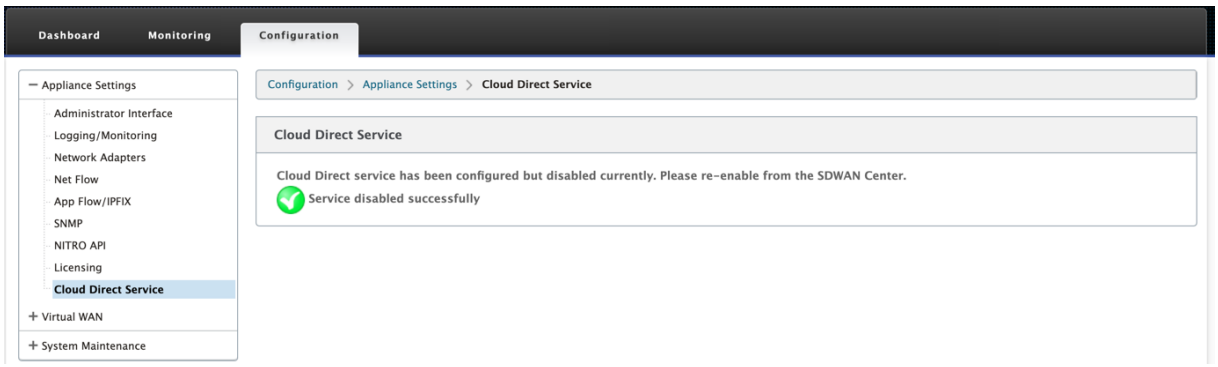
Statut du service Cloud Direct sur Citrix SD-WAN

Vous pouvez vérifier l'état du service Cloud Direct sur une appliance SD-WAN locale.

Accédez à l'interface graphique Citrix SD-WAN, accédez à **Configuration** > Développez **Paramètres de l'appliance** > sélectionnez **Cloud Direct Service**.



Cliquez sur l'option **Désactiver** pour désactiver le service Cloud Direct.



Résolution des problèmes

Les messages d'erreur les plus courants qui peuvent se produire sur SD-WAN Center lors du déploiement du service Cloud Direct sont les suivants.

Les messages d'erreur/d'état sont affichés sur SD-WAN Center sous **Configuration** > **Connectivité Cloud** > **Cloud Direct**.

'Cloud Direct License error! Veuillez télécharger une licence supplémentaire pour {bande passante} Mbps

- Téléchargez une licence Cloud Direct valide sur SD-WAN Center en accédant à **Configuration** > **Licences** > **Gestion des fichiers**, puis procédez au déploiement de cette fonctionnalité

'HA de configuration Cloud Direct en raison d'un problème de connexion Citrix Cloud Workspace

- Entrez de nouveau les informations d'identification pour la connexion Citrix Cloud Workspace sur SD-WAN Center en accédant à **Configuration** > **Cloud Connectivity** option.

'Cloud Direct configuration processing error! Le site : {site_name} (IP : {mgmt_ip}) n'est pas accessible ou il manque le support Cloud Direct'

- Vérifiez si l'appliance ou les appliances SD-WAN (en cas de déploiement HA) sont accessibles sur le port de gestion.

'Erreur de vérification de la configuration HA de configuration Cloud Direct pour le site : {site_name} '

- Vérifiez la connectivité des deux appliances dans la paire HA correspondant au site en cours de déploiement.

'Les deux appliances Paire HA doivent être joignables pour effectuer la configuration Cloud Direct'

- Lors du déploiement du service Cloud Direct sur des appliances SD-WAN en paire HA, les appliances secondaires et principales doivent être accessibles sur le port de gestion.

‘Cloud Direct configuration processing error! Site: {site_name}(IP: {mgmt_ip}) has SSO Login Issue’

- Vérifiez si l’appliance SD-WAN est en marche et accessible sur le port de gestion. Cette erreur s’affiche lorsque SD-WAN Center n’est pas en mesure d’effectuer l’authentification unique à l’appliance SD-WAN.

‘Erreur interne rencontrée lors du traitement de la configuration Cloud Direct’

- Cela peut se produire en raison de multiples conditions d’erreur lors de la vérification de la configuration ou du reste du traitement. Un utilisateur peut avoir besoin d’examiner les journaux et d’effectuer à nouveau l’opération.

‘Le traitement de la configuration Cloud Direct est annulé ! MCN n’est pas prêt pour la gestion du changer’

- Vérifiez si MCN est accessible et opérationnel et que son état de gestion des modifications est « network_staging ».

‘Cloud Direct configuration processing error! Le site : {site_name} (IP : {mgmt_ip}) ne prend pas en charge Cloud Direct. Veuillez effectuer une mise à niveau en une seule étape pour bénéficier d’un support Cloud Direct’

- Effectuez une mise à niveau logicielle en une seule étape sur l’appliance SD-WAN via **MCN** > **Gestion des modifications**. Après cette procédure, essayez à nouveau de déployer le service Cloud Direct pour ce site.

‘Cloud Direct configuration processing error! Échec de l’opération de gestion des changements SD WAN »

- L’opération de gestion du changement n’a pas réussi. Consultez les journaux de SD-WAN Center pour plus de détails.

‘Cloud Direct configuration processing error! Activation du service sur le site : {site_name} a échoué »

- Impossible d’activer le service Cloud Direct sur l’appliance SD-WAN. Vérifiez la connectivité d’une appliance spécifique ou celles en paire HA ou tout problème lors de l’authentification unique. Consultez les journaux de SD-WAN Center et de l’appliance pour plus de détails.

‘Cloud Direct configuration processing error! La désactivation du service sur le site : {site_name} a échoué’

- Impossible de désactiver le service Cloud Direct sur l’appliance SD-WAN. Vérifiez la connectivité d’une appliance spécifique ou de ceux en paire HA ou tout problème lors de l’authentification unique. Consultez les journaux de SD-WAN Center et de l’appliance pour plus de détails.

‘Cloud Direct configuration processing error! Config image push vers le site : {site_name} a échoué’

- Impossible de télécharger l’image spécifique au service sur l’appliance via l’API REST ou ne peut pas accéder aux deux appliances en paire HA.

‘Cloud Direct Service a rencontré une erreur lors du traitement de la configuration. Erreurs d’ audit trouvées dans la configuration SD WAN ! ‘

- Erreurs d’audit détectées lors de la tentative de compilation de la configuration SD-WAN. Consultez les journaux de SD-WAN Center pour plus de détails.

‘Cloud Direct configuration processing error! Échec de la création du site pour le site : {site_name} ‘

- Erreur côté service lors de la tentative de création d’un site pour l’appliance SD-WAN correspondante. Consultez les journaux de SD-WAN Center pour plus de détails.

‘Cloud Direct configuration processing error! Échec de la mise à jour du site pour le site : {site_name} ‘

- Erreur côté service lors de la tentative de modification des paramètres liés au site pour l’appliance SD-WAN correspondante. Consultez les journaux de SD-WAN Center pour plus de détails.

Messages d’erreur affichés dans les journaux (SDWAN_common.log)

Voici quelques scénarios où le service Cloud Direct est déployé sur une appliance SD-WAN, mais peut ne pas fonctionner comme prévu. Vous pouvez télécharger et consulter les journaux sur l’appliance SD-WAN locale à l’aide du fichier SDWAN_common.log pour plus de détails.

Scénario 1

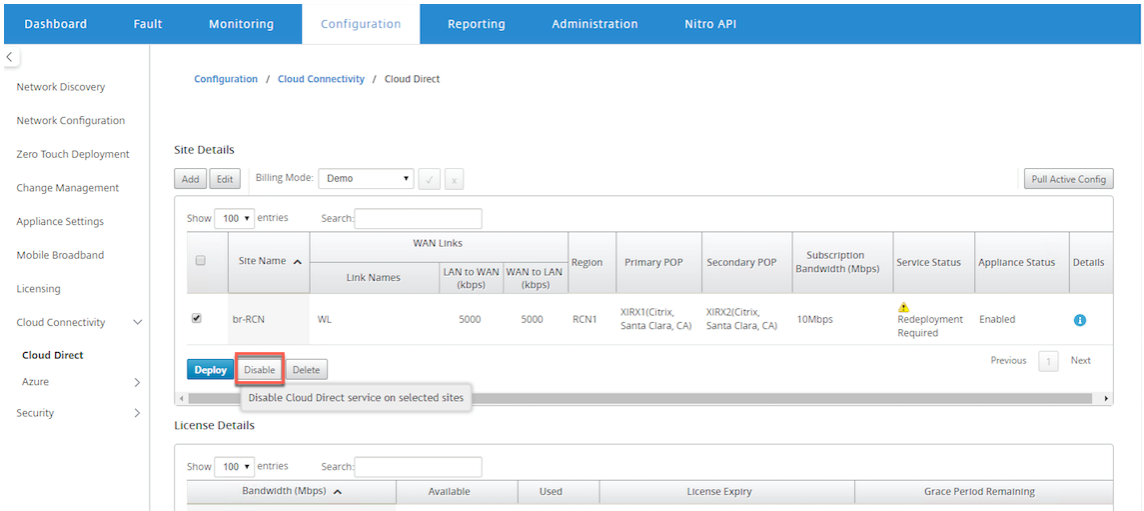
« La machine virtuelle Cloud Direct détectée ne répond pas…Désactivation du service Cloud Direct dès maintenant ! » « Le service Cloud Direct a été désactivé. » Le KVM sous-jacent s'exécutant sur une appliance SD-WAN locale ne fonctionne pas de la manière attendue. Dans ce cas, la fonctionnalité du service Cloud Direct est désactivée sur l'appliance.

Scénario 2

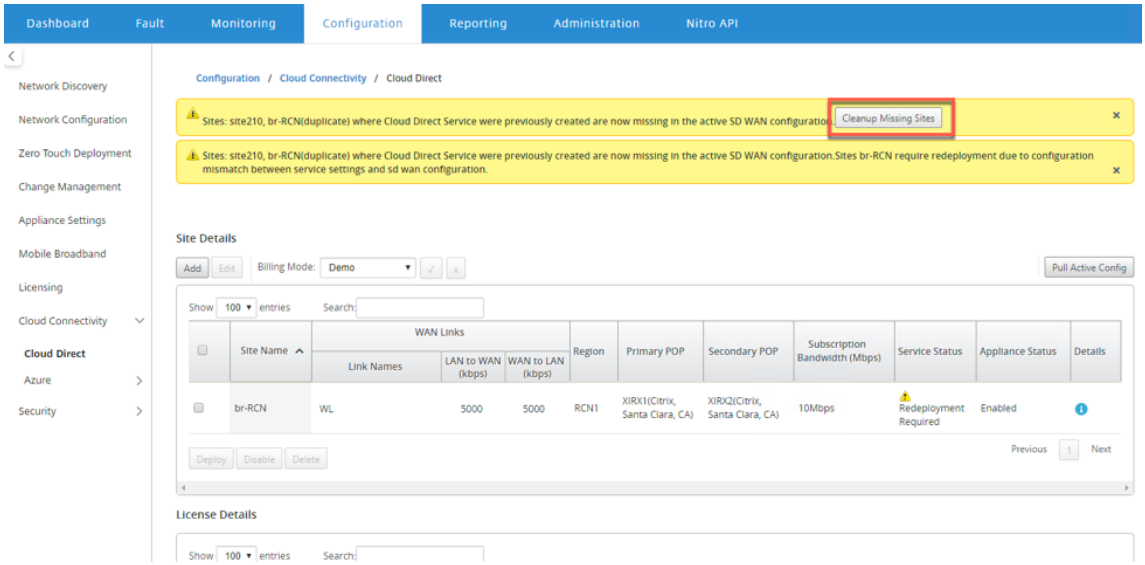
« Pas de paquets tunnels vus depuis 5 minutes…Désactivation du service Cloud Direct maintenant ! » « Le service Cloud Direct a été désactivé. » Aucun tunnel n'est établi entre l'appliance SD-WAN et le point de terminaison de tunnel utilisé pour le service Cloud Direct. Cela peut être dû à une mauvaise configuration de la liaison wan-link, à un manque de connectivité Internet sur la liaison wan-link configurée, à une image de données/config incompatibles ou invalides poussée à l'appliance ou à toute règle de pare-feu qui pourrait laisser tomber des paquets de tunnel UDP lorsqu'ils sont reçus via wan-link. Dans ce cas, la fonctionnalité du service Cloud Direct est désactivée sur l'appliance.

Lorsque vous activez une configuration sur MCN avec une configuration Cloud Direct différente (par exemple, la configuration NAT est modifiée pour Cloud Direct) et cela peut entraîner une interruption permanente du trafic. Pour surmonter ce blocage, vous pouvez suivre l'une des étapes suivantes pour sélectionner les différentes routes présentes sur l'appliance :

1. Dans l'interface graphique de SD-WAN Center, accédez à **Configuration** > **Cloud Connectivity** > **Cloud Direct**. Sélectionnez l'appliance cloud direct et cliquez sur l'option **Désactiver** pour désactiver le service direct cloud.



2. Accédez à **Configuration** > **Cloud Connectivity** > **Cloud Direct** et extrayez la configuration active pour obtenir la notification de nettoyage. Vous pouvez cliquer sur le bouton de notification **Nettoyage des sites manquants** qui s'affiche pour l'appliance Cloud Direct affectée. Cette opération désactive le service Cloud Direct en cours d'exécution sur l'appliance.



3. Redéployez le service Cloud Direct sur SD-WAN Center pour utiliser le service Cloud Direct pour les appliances affectées.

Intégrez Citrix SD-WAN et Zscaler à l'aide de Citrix SD-WAN Center

February 17, 2022

Citrix SD-WAN et Zscaler aident les entreprises à transformer leur WAN pour la migration vers le cloud en fournissant des solutions locales sécurisées aux applications et aux ressources hébergées sur Internet. Les nouvelles technologies d'infrastructure WAN telles que le SD-WAN augmentent l'agilité et l'évolutivité du réseau tout en réduisant les coûts et la complexité pour améliorer l'expérience utilisateur dans les organisations distribuées.

Les solutions SD-WAN simplifient le routage en permettant au trafic destiné au cloud de se rendre sur Internet localement. Le SD-WAN offre une flexibilité pour le routage du trafic vers Internet (suppression de l'environnement DC central) en utilisant les fonctions de pilotage des applications. Cependant, l'exposition du réseau à Internet pose des risques importants pour la sécurité. Une approche centralisée pour sécuriser le déploiement local via un service cloud élimine les frais de maintenance de l'infrastructure de sécurité dans les succursales. Tout le trafic est acheminé de manière fiable et sécurisée vers Zscaler (plate-forme de sécurité basée sur le cloud) avec Citrix SD-WAN dans le réseau de succursales. Vous pouvez éliminer l'infrastructure coûteuse et protéger votre réseau contre les menaces et les vulnérabilités.

Citrix SD-WAN

Citrix SD-WAN aide les entreprises à migrer vers le cloud en activant en toute sécurité le routage de l'Internet des succursales locales avec un pare-feu avec état intégré pour créer des stratégies qui peuvent autoriser ou refuser l'accès à Internet directement à partir de la succursale. Citrix SD-WAN identifie les applications grâce à une combinaison d'une base de données intégrée de plus de 4 000 applications, y compris des applications SaaS individuelles, et utilise une technologie d'inspection approfondie des paquets pour la découverte et la classification en temps réel des applications. Il utilise cette connaissance de l'application pour diriger le trafic de la succursale vers Internet, cloud ou SaaS.

Zscaler

Zscaler est la principale plate-forme de sécurité basée sur le cloud, qui offre une sécurité supérieure sans avoir besoin de matériel, d'appliances ou de logiciels sur site. Zscaler met un périmètre autour d'Internet, de sorte que les entreprises n'ont pas besoin de mettre un périmètre de sécurité autour de chaque bureau. Zscaler Cloud Security Platform agit comme une série de postes de contrôle de sécurité dans plus de 100 centres de données à travers le monde. En redirigeant le trafic Internet vers Zscaler, les entreprises peuvent sécuriser instantanément les magasins, les succursales et les emplacements distants. Zscaler connecte les utilisateurs et Internet, en inspectant chaque octet de trafic, même s'il est chiffré ou compressé, afin que les utilisateurs soient sécurisés et que toutes les menaces cachées soient identifiées avant de pouvoir s'infiltrer dans le réseau d'entreprise.

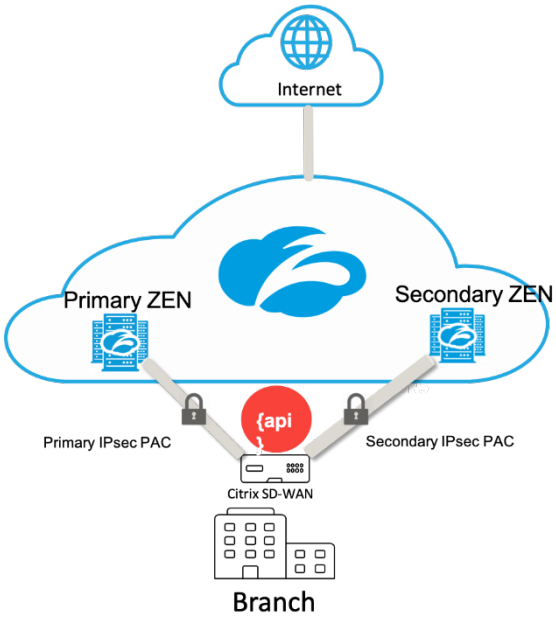
Citrix SD-WAN permet de créer des stratégies qui permettent une sortie directe d'Internet à partir de la succursale et la plateforme de sécurité cloud de Zscaler assure la sécurité de l'informatique en inspectant tout le trafic relié à Internet dans un service cloud proche de l'endroit où les utilisateurs se connectent.

Nœuds d'application Zscaler (ZEN)

Citrix SD-WAN prend en charge les API Zscaler pour automatiser la création de tunnels IPSec entre Citrix SD-WAN et Zscaler Enforcement Nodes (ZENs) dans le réseau cloud de Zscaler. Les ZEN sont des passerelles de sécurité Internet intégrées complètes qui inspectent tout le trafic Internet bidirectionnellement pour détecter les logiciels malveillants et appliquent des stratégies de sécurité et de conformité.

L'API Zscaler fournit les deux emplacements de centre de données les plus proches de chaque succursale, ce qui permet au SD-WAN de diriger efficacement le trafic. Les organisations peuvent autoriser Zscaler à choisir automatiquement le ZEN le plus proche de la branche en demandant à ZEN d'examiner les adresses IP des liens WAN configurés sur Citrix SD-WAN ou de sélectionner manuellement **les ZEN**.

> **REMARQUE**
>
> Les deux routes sont toujours en mode actif si le tunnel est UP. Si un tunnel descend l'itinéraire correspondant devient inaccessible et l'autre itinéraire reste en hausse dans ce cas.



Avantages

Les avantages de l'intégration de Citrix SD-WAN et Zscaler incluent :

- Adoption plus rapide du SaaS et du cloud dans une entreprise distribuée.
  - La centralisation de la sécurité en tant que service cloud élimine le besoin de l'avoir dans chaque succursale.
  - Élimination de la nécessité de réacheminer le trafic destiné à Internet, ce qui permet une sortie Internet locale à la succursale.
- Gestion informatique simplifiée grâce à une connectivité automatisée à Secure Web Gateway.
  - La prise en charge de l'API automatise la configuration des tunnels sécurisés vers Zscaler
- Amélioration de l'expérience utilisateur grâce à la réduction de la latence du trafic SaaS.
  - Élimine la dépendance du modèle hub-and-spoke à des fins de sécurité
- Élimination des piles de sécurité coûteuses dans les succursales
  - Réduisez les frais supplémentaires liés au déploiement et à la gestion des pare-feu dans les succursales.

- Assurance que le trafic relié à Internet est toujours sécurisé.
  - Les stratégies de sécurité ne lient pas les utilisateurs à un emplacement physique.
  - Fournit un sandboxing, une inspection de tous les ports et protocoles, y compris SSL, filtrage d'URL, protection avancée contre les menaces et bien plus encore pour protéger contre les attaques « jour zéro ».

Fonction prise en charge

Un déploiement Zscaler utilisant des appliances SD-WAN prend en charge les fonctionnalités suivantes :

- Transférer le trafic Internet défini par l'utilisateur vers Zscaler, ce qui permet l'évasion directe sur Internet.
- Accès direct à Internet (DIA) utilisant Zscaler sur une base par site client.
  - Sur certains sites, vous pouvez fournir à DIA un équipement de sécurité local et ne pas utiliser Zscaler.
  - Sur certains sites, vous pouvez choisir de rediriger le trafic vers un autre site client pour accéder à Internet.
- Déploiements de routage et de transfert virtuels.
- Une liaison WAN dans le cadre des services Internet.

Zscaler est un service cloud. Vous devez le configurer en tant que service et définir les liens WAN sous-jacents :

- Configurez un lien WAN Internet public approuvé au niveau du centre de données et des sites de succursales.
- Configurer automatiquement les tunnels IPSec pour les services intranet.

Déploiement de Zscaler dans le flux de travail Citrix SD-WAN Center

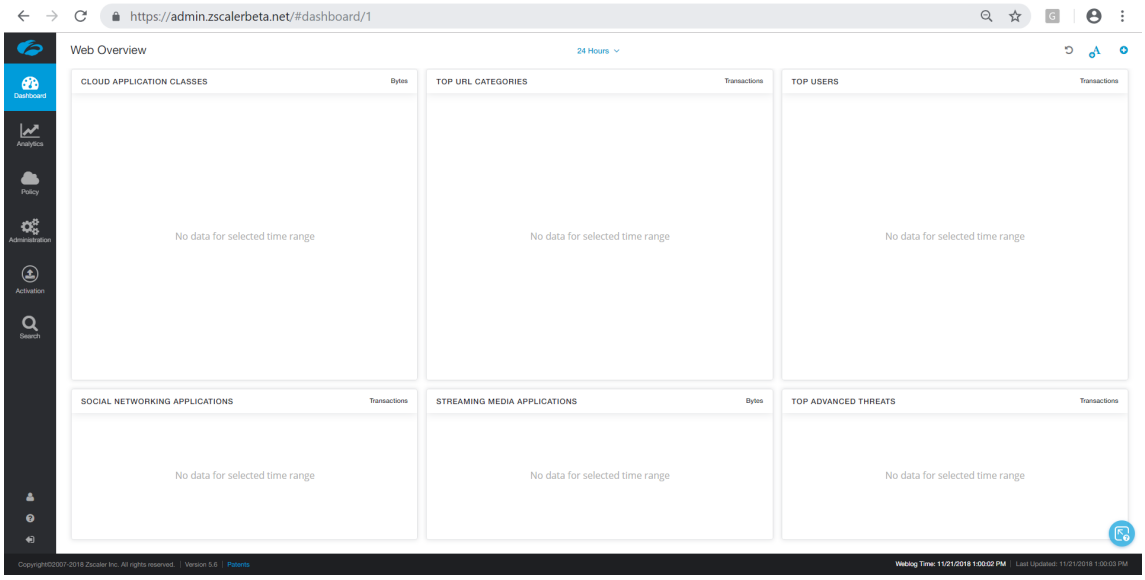
Voici les étapes de haut niveau qui définissent le flux de travail pour déployer Zscaler dans SD-WAN Center.

1. Configurez l'abonnement Zscaler au SD-WAN Center (une seule fois). Connectez-vous au site Zscaler pour obtenir des informations d'abonnement.
2. Sélectionnez **Déployer** dans l'interface graphique du centre Citrix SD-WAN.
   - Déployer la configuration du site à l'aide d'Internet wan-link et d'un objet d'application préconfiguré.
   - Établir la connectivité
   - Obtenir ou mettre à jour l'état IPSec.

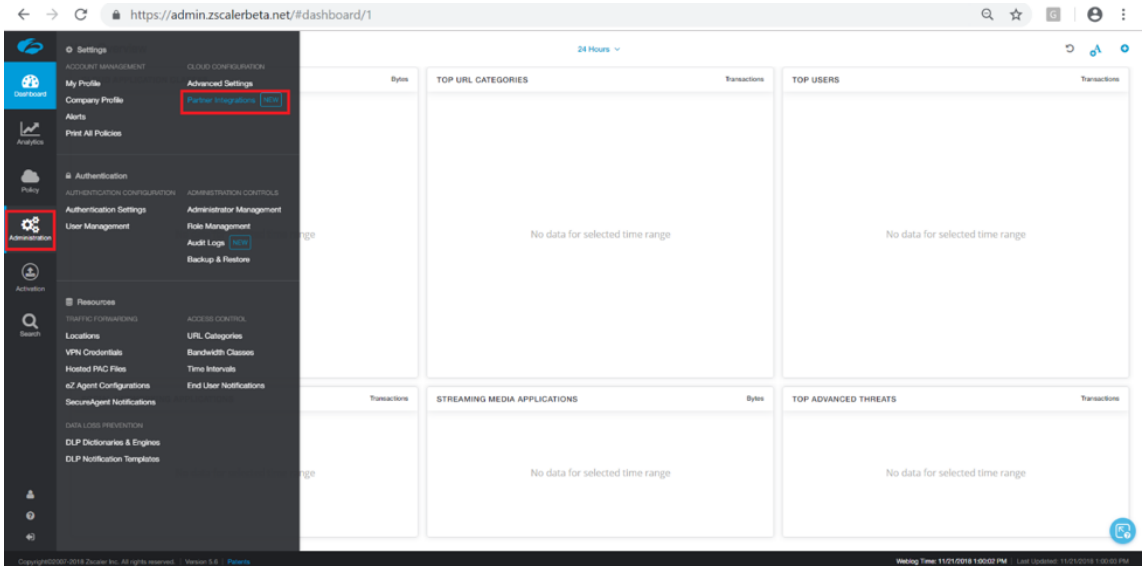
Abonnement Zscaler

Avant de procéder à la configuration de Zscaler dans SD-WAN Center, vous devez vous connecter au portail Zscaler.

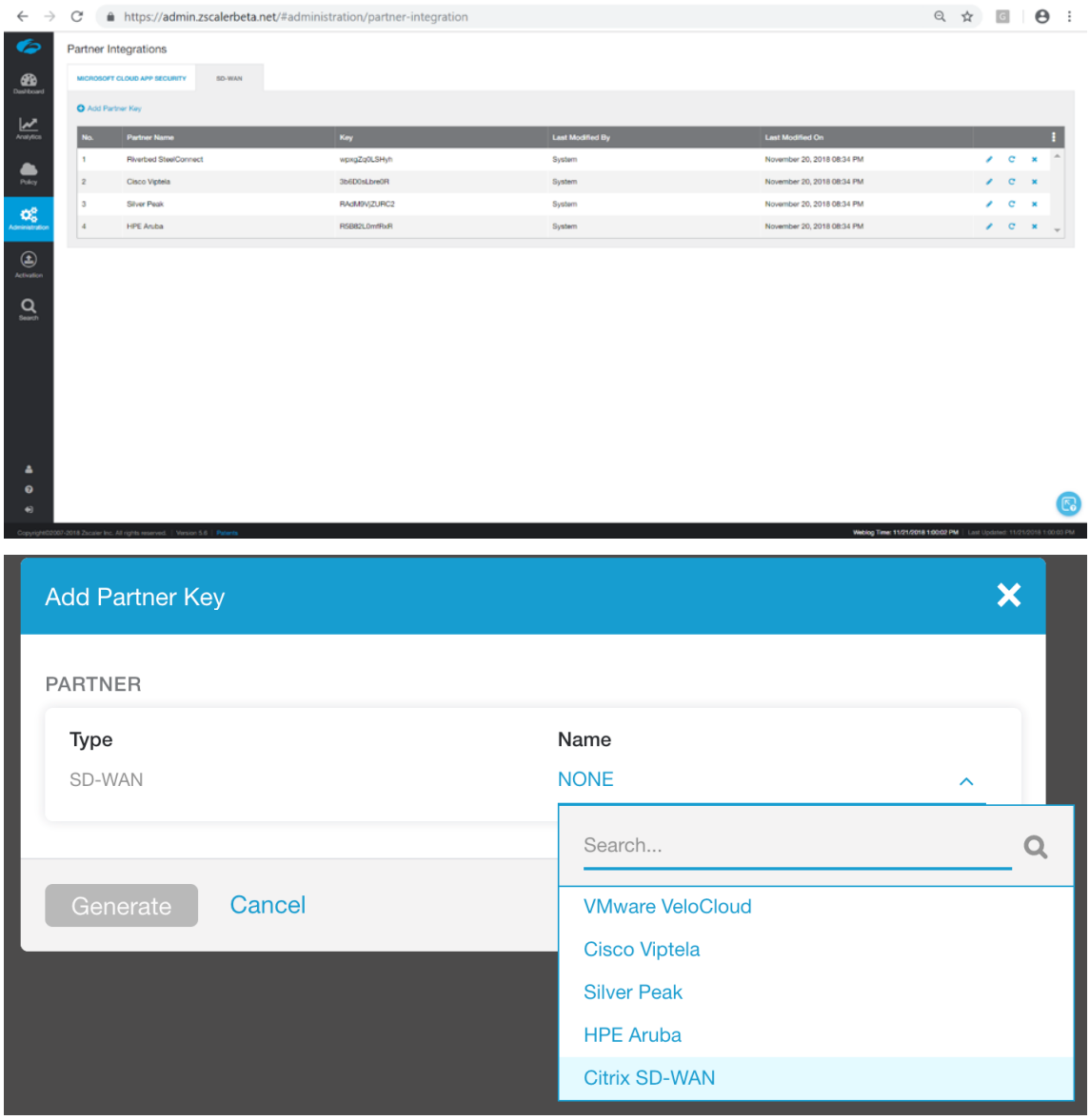
1. Connectez-vous au site Zscaler pour obtenir des informations d'abonnement. La page Tableau de bord s'ouvre.



2. Cliquez sur **Administration > Intégrations partenaires**.



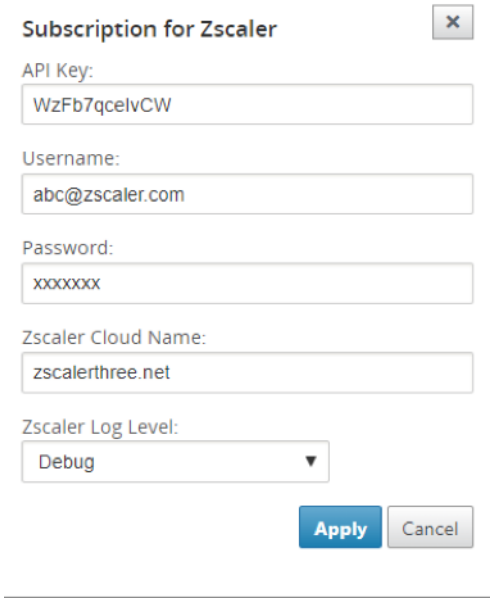
3. Sélectionnez **SD-WAN** sur la page **Intégrations de partenaires**. Cliquez sur **Ajouter une clé de partenaire**.



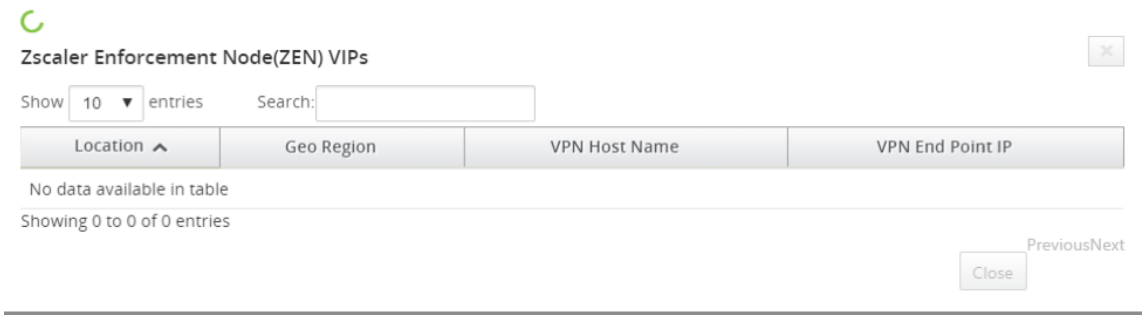
4. Choisissez **Citrix SDWAN** pour la clé de partenaire, puis cliquez sur **Générer**. Stockez la clé.

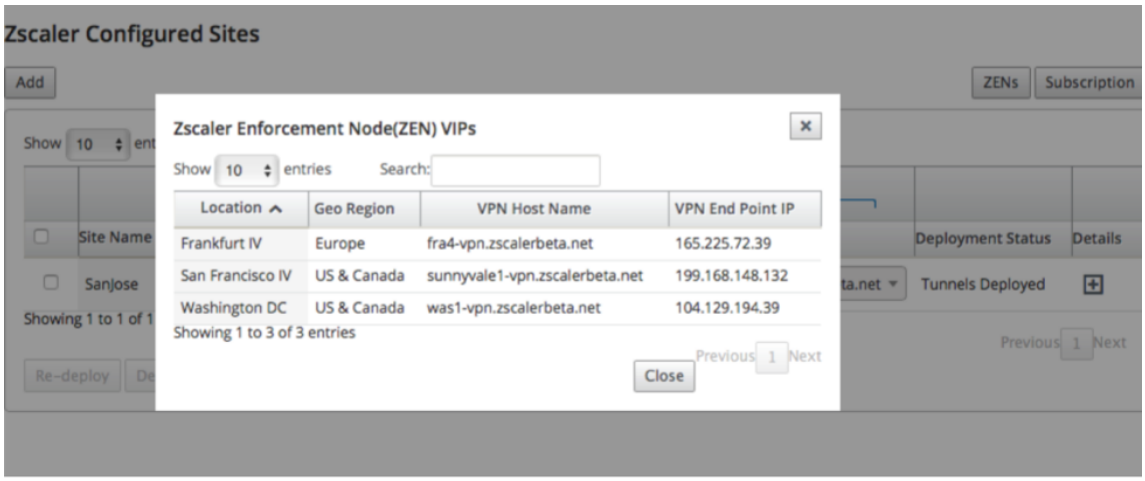
Configurer Zscaler dans le Centre Citrix SD-WAN

1. Dans l'interface graphique de Citrix SD-WAN Center, accédez à la page **Configuration > Sécurité**. La page **Sites configurés Zscaler** s'ouvre.
2. Cliquez sur **Abonnement**. Entrez l'API Zscaler (clé de partenaire) créée dans les étapes précédentes. Fournissez votre nom d'**utilisateur** et votre mot de **passe**Zscaler. Sélectionnez **Zscaler Cloud Name**, **Zscaler Log Level**, puis cliquez sur **Appliquer**.

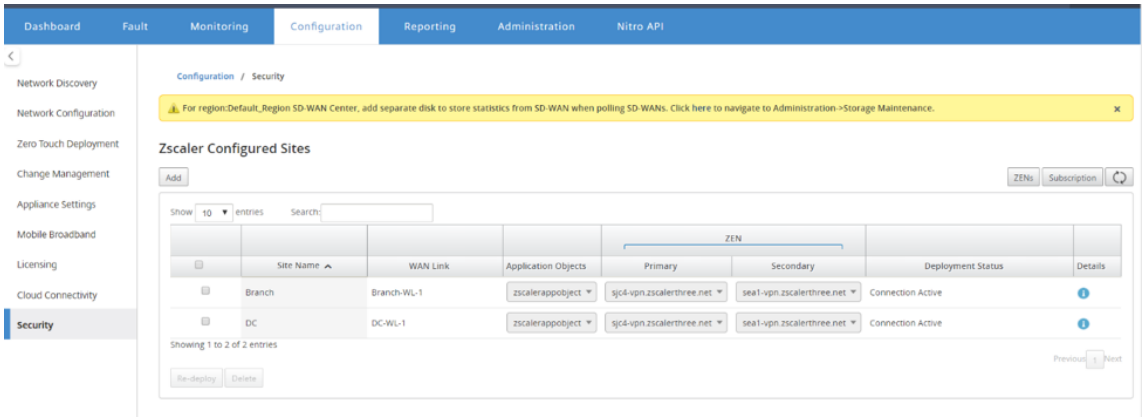


3. Zens fournit la liste des terminaux VPN disponibles pour cet abonnement au cloud Zscaler.

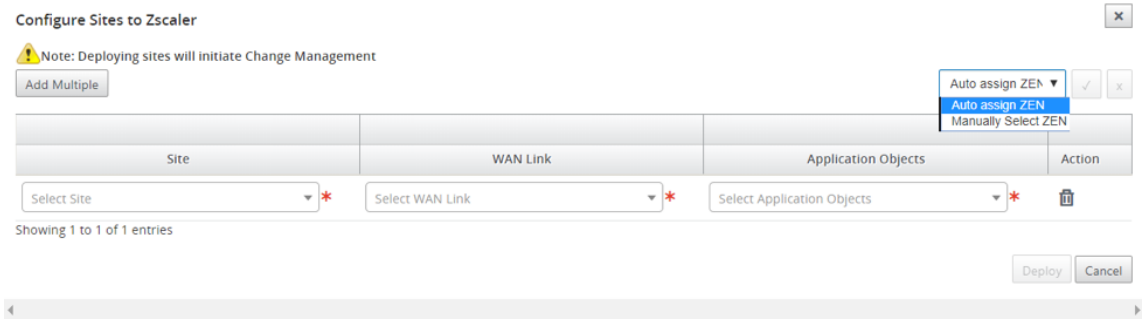




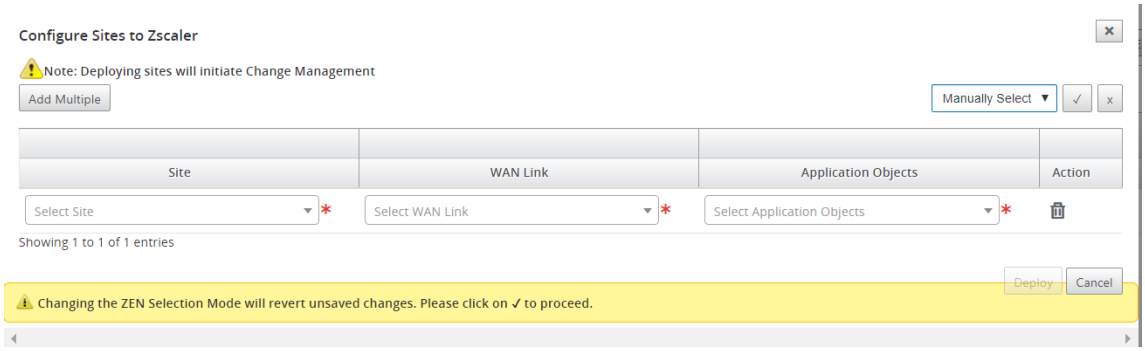
4. Après avoir entré l'abonnement Zscaler et les détails ZEN, vous pouvez commencer à ajouter des sites à Zscaler. Cliquez sur **Ajouter**.



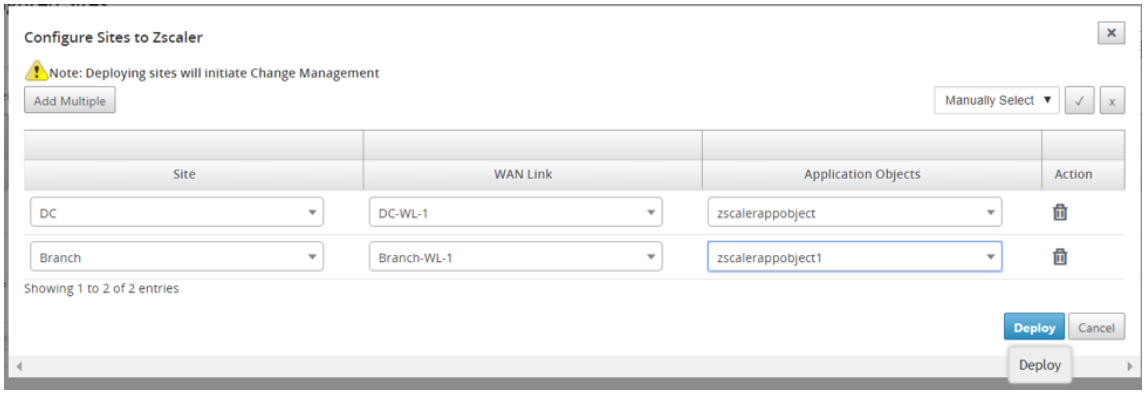
5. Dans la boîte de dialogue **Configurer les sites sur Zscaler**, ajoutez des objets **Site, WAN Link** et **Application** . Par défaut, l'option **Attribuer automatiquement ZEN** est sélectionnée.

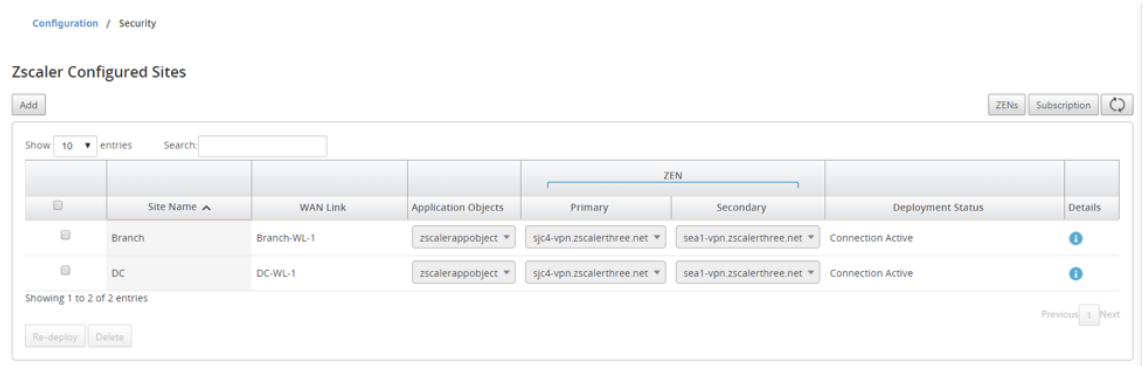


Vous pouvez **sélectionner manuellement ZEN**. Toutefois, le message suivant s'affiche pour avertir que les modifications non enregistrées sont perdues.



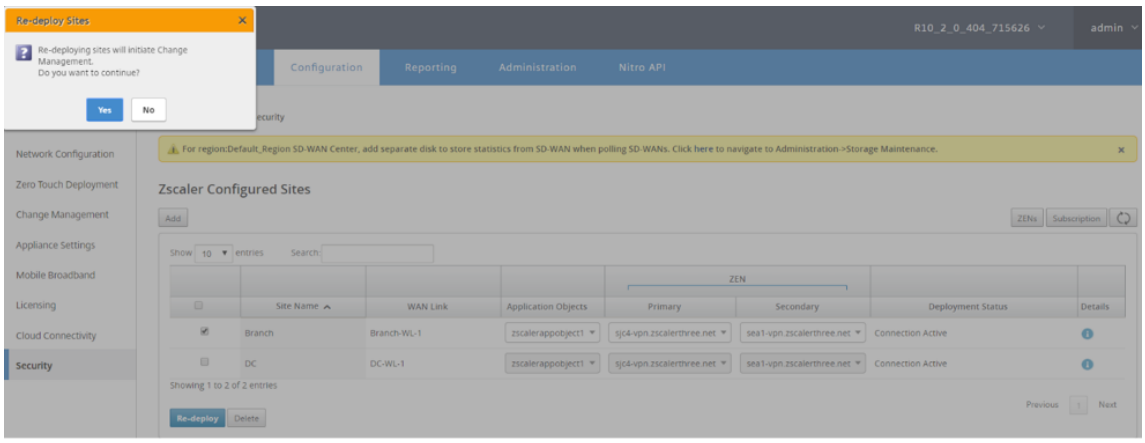
6. Sélectionnez les sites requis et cliquez sur **Déployer**. Vous pouvez choisir d'ajouter plusieurs sites en sélectionnant **Ajouter plusieurs**. Les sites sélectionnés sont déployés et la page de configuration s'affiche.



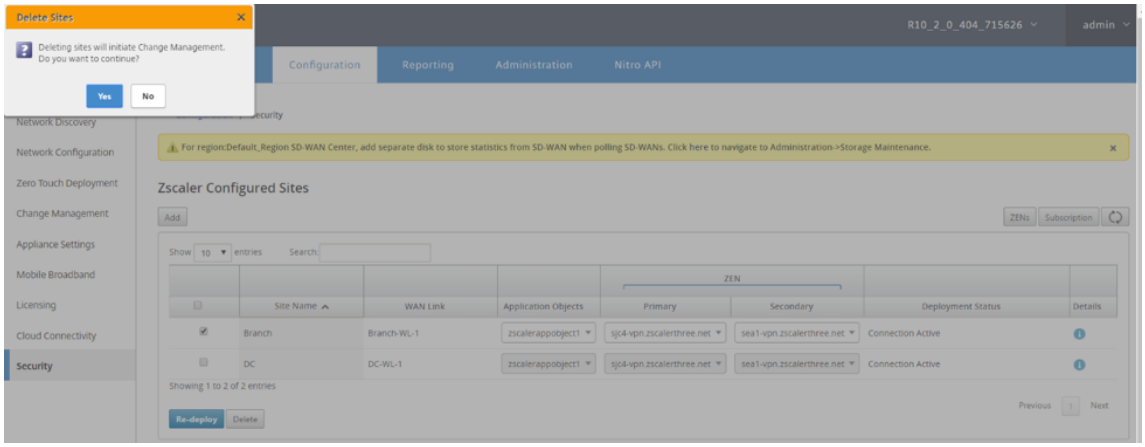


Notez que les adresses IP ZEN principales et secondaires sont renseignées et que l'état du déploiement est **Connection Active**.

7. Cliquez sur **Re-déployer**si vous apportez des modifications aux points de terminaison VPN ou aux objets d'application du site configuré. Toute modification apportée aux sites configurés dans le SD-WAN Center déclenche un processus de **gestion des modifications** sur les appliances configurées sur les sites de succursales et les sites DC.

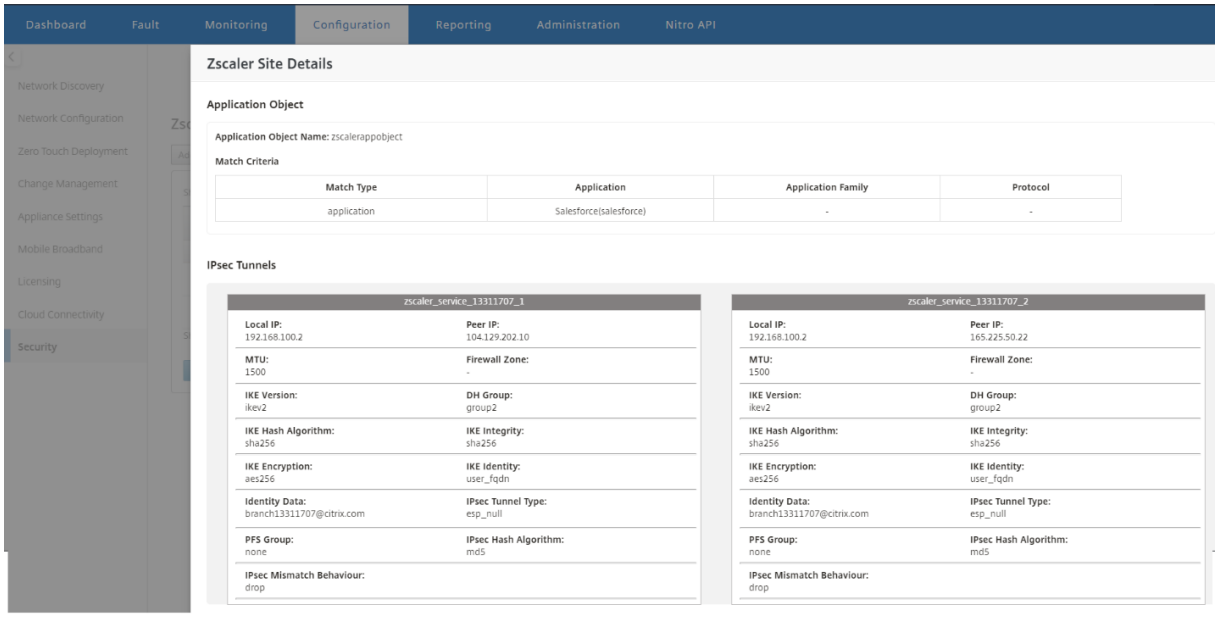


La suppression de sites déclenche également le processus de gestion des modifications.



Surveillance et dépannage

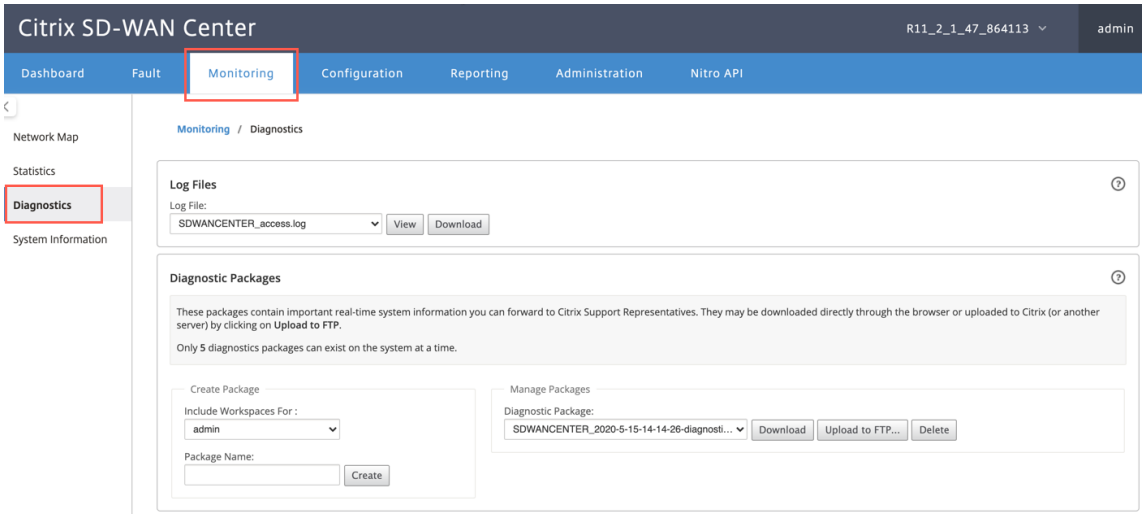
Sélectionnez les sites configurés pour afficher plus d'informations sur les objets d'application et les adresses IP principales/secondaires. Vous pouvez cliquer sur l'icône **Détails** pour afficher des informations complètes sur les sites configurés.



Vous pouvez afficher et télécharger les journaux Zscaler qui peuvent être utilisés pour résoudre les problèmes dans le Centre Citrix SD-WAN.

Pour afficher les fichiers journaux Zscaler :

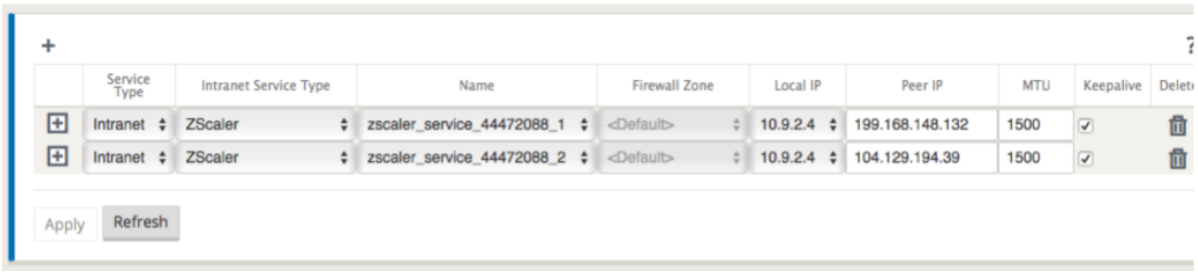
1. Dans l'interface Web Citrix SD-WAN Center, cliquez sur l'onglet **Surveillance** > **Diagnostics**.



2. Dans la liste déroulante **Fichier journal**, sélectionnez le fichier journal Zscaler que vous souhaitez afficher. Cliquez sur **Afficher**.
3. Si vous souhaitez télécharger les fichiers journaux sur votre ordinateur, cliquez sur **Télécharger**.

Configuration du tunnel IPSec

La page Détails de l'interface graphique du SD-WAN Center fournit des informations sur la configuration du tunnel IPSec vers les points de terminaison principaux et secondaires. L'IP homologue est obtenue à partir de Zscaler. Vérifiez la configuration du tunnel IPSec dans l'éditeur de configuration de l'interface graphique de l'appliance SD-WAN.

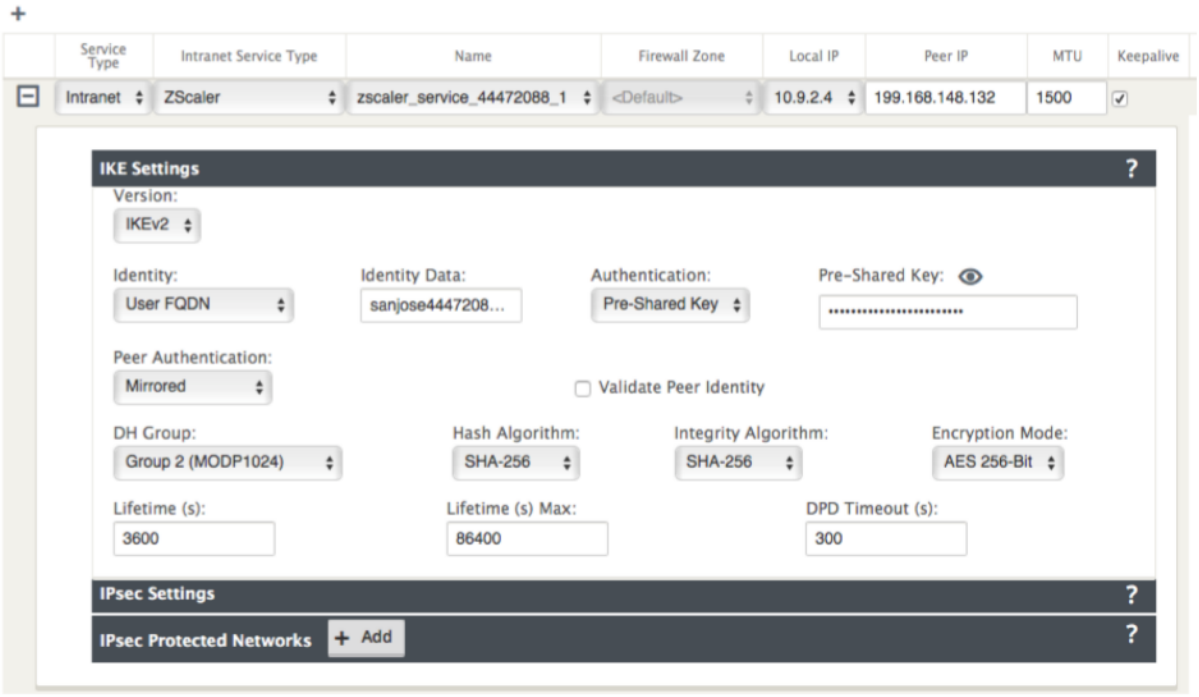


Paramètres IKE

Les paramètres IKE/IPSec suivants sont choisis pour la configuration du tunnel IPSec dans l'appliance SD-WAN. Pour plus d'informations sur la configuration du tunnel IPsec —paramètres IKE, reportez-vous à la rubrique Comment configurer un tunnel IPsec entre le SD-WAN et des périphériques tiers .

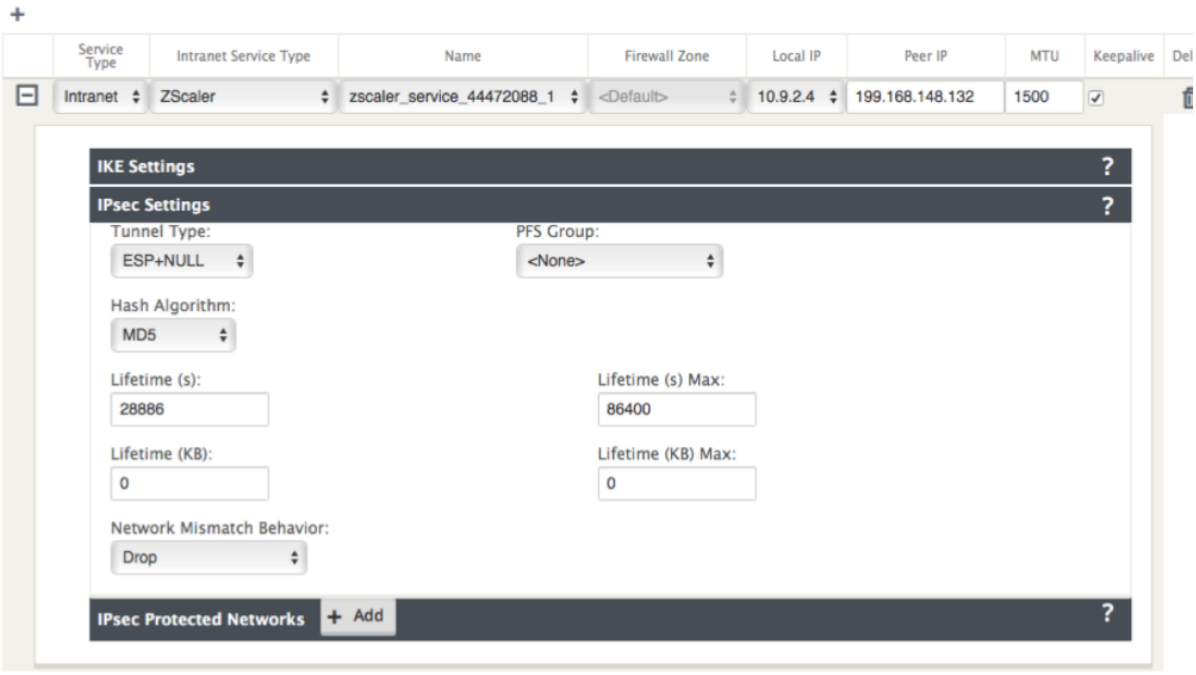
- Version IKE - IKEv2
- Identité IKE —Nom de domaine complet de l'utilisateur

- Algorithme de hachage - SHA-256
- Algorithme d'intégrité —SHA-256
- Mode de chiffrement —AES 256 bits
- IPSec —Mode tunnel
- Cryptage IPsec —Null



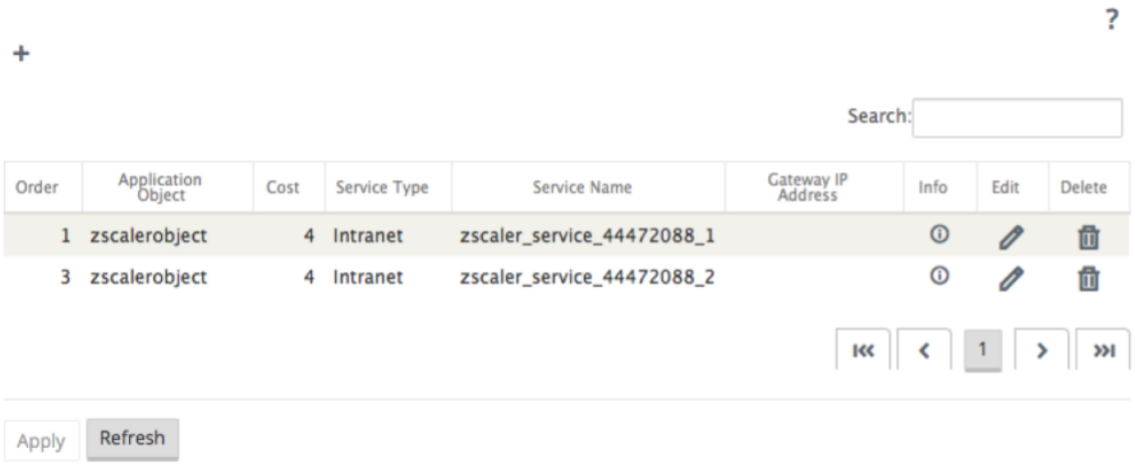
Paramètres IPsec

Pour plus d'informations sur la configuration des paramètres du tunnel IPsec, consultez la rubrique Comment configurer un tunnel IPsec entre le SD-WAN et des périphériques tiers .



Objets d'application

Assurez-vous que les objets d'application sont configurés. Pour plus d'informations sur la configuration des itinéraires d'application, consultez la rubrique Classification des applications .



> **Remarque**
>
> La configuration du tunnel GRE n'est pas prise en charge dans le cadre du workflow automatisé. Cependant, la configuration manuelle est toujours autorisée. Pour plus d'informations, consultez Intégration de Zscaler à l'aide de tunnels GRE et de tunnels IPsec.

Surveillance

February 17, 2022

Le tableau de bord de Citrix SD-WAN Center vous permet d'afficher les statistiques et les graphiques du réseau SD-WAN sur un seul volet. Pour plus d'informations, consultez Tableau de bord.

Vous pouvez également afficher les événements et les rapports du réseau SD-WAN dans Citrix SD-WAN Center.

Suivi des articles connexes :

Forfaits de diagnostic

Notifications d'événements

Fichiers journaux

vidages de mémoire

Intervalle d'interrogation

Statistiques

Informations système

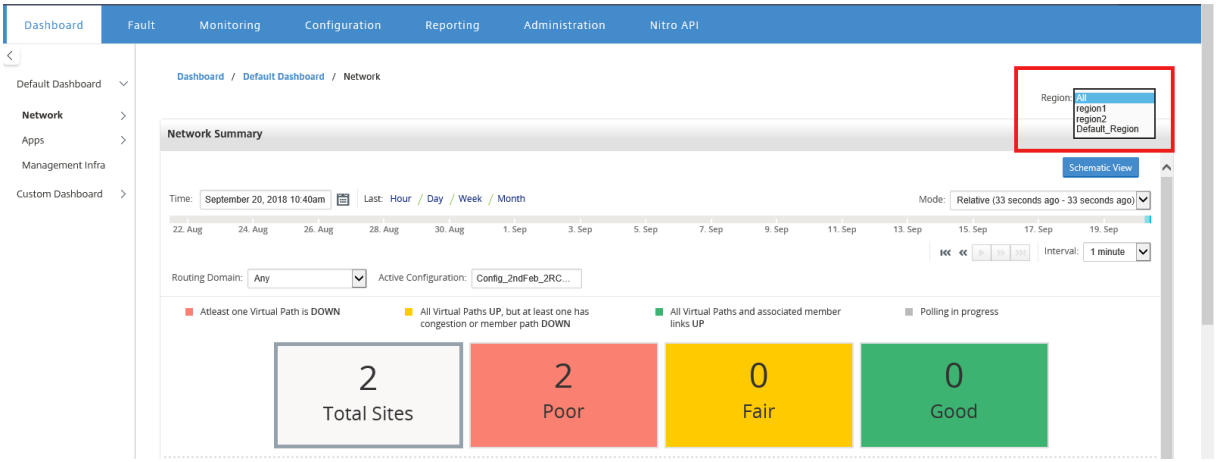
Tableau de bord

February 17, 2022

Le tableau de bord du Citrix SD-WAN Center affiche un sous-ensemble des statistiques communes en un coup d'œil. Pour un déploiement à une seule région, les statistiques sont obtenues à partir du MCN détecté dans Citrix SD-WAN Center. Pour un déploiement multi-régions, les statistiques sont obtenues à partir de tous les collecteurs régionaux Citrix SD-WAN Center pour l'intervalle de temps sélectionné. Vous pouvez afficher les statistiques suivantes :

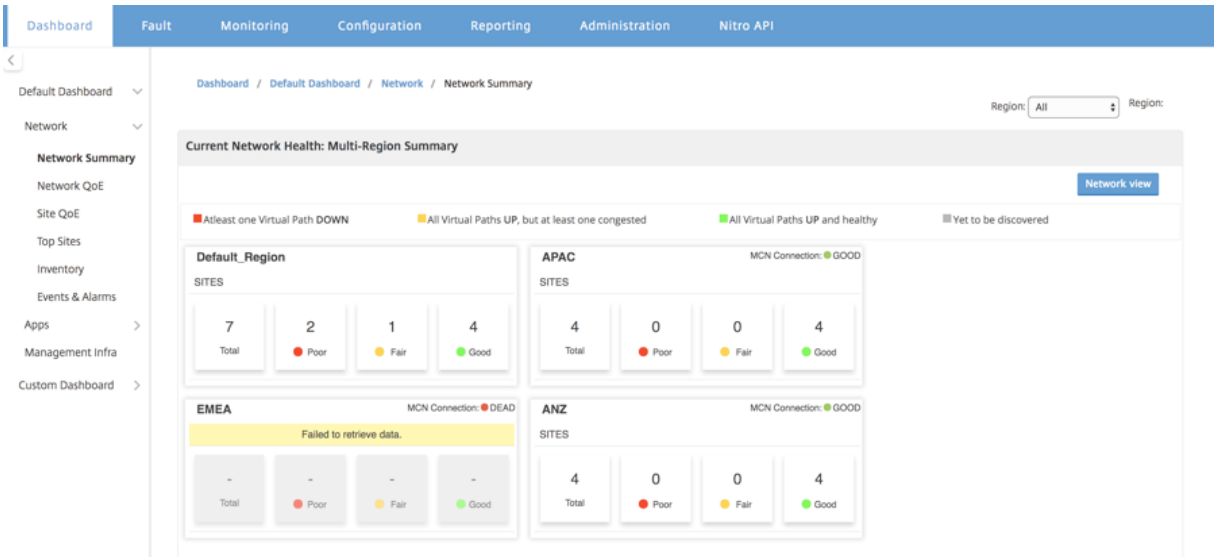
- Résumé du réseau
- QoE réseau
- Meilleurs sites
- Inventory
- Événements et alarmes
- Top Apps
- QoE HDX
- Gestion Infra

Pour un déploiement à une seule région, les statistiques de région par défaut sont affichées dans le tableau de bord. Pour un déploiement multi-régions, vous pouvez choisir d'afficher le tableau de bord multi-régions ou le tableau de bord régional. Pour afficher le tableau de bord multi-régions, sélectionnez **Tout** dans le menu **Région**.



Vous pouvez afficher l'état de la connexion MCN sur chaque vignette de région. L'état de connexion MCN est l'état d'intégrité du chemin virtuel entre un RCN et le MCN.

> **Remarque**
>
> Pour un déploiement multi-région, les statistiques de région par défaut incluent des statistiques de tous les sites gérés par le MCN. Il peut également inclure des statistiques de la MCN puisque les MRC ont des chemins virtuels vers le MCN.
>
> Le menu déroulant **Région** n'est pas disponible dans Citrix SD-WAN Center Collectors.



Le tableau de bord du Citrix SD-WAN Center est actualisé en fonction de l'intervalle d'interrogation

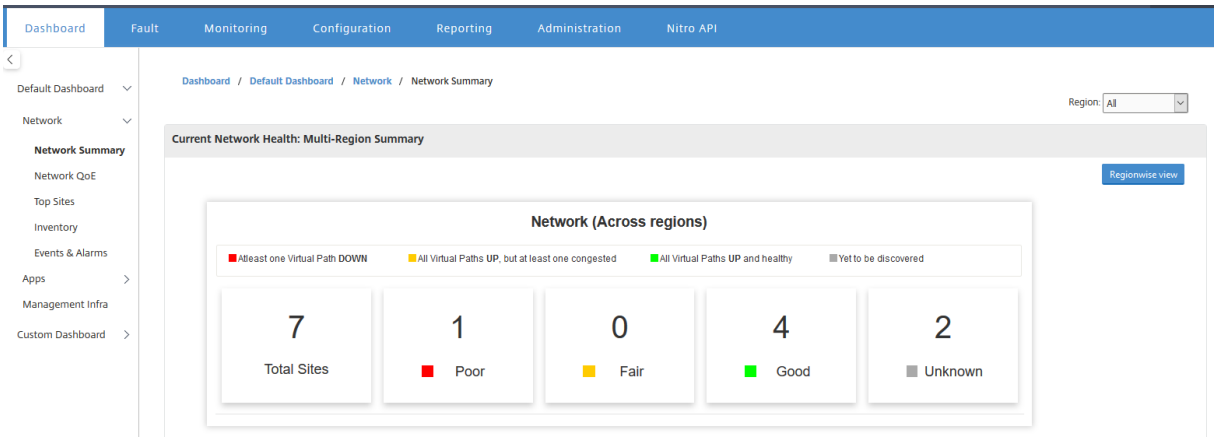
configuré. L'intervalle d'interrogation par défaut est de cinq minutes. Pour plus d'informations, consultez Intervalle d'interrogation.

Résumé du réseau

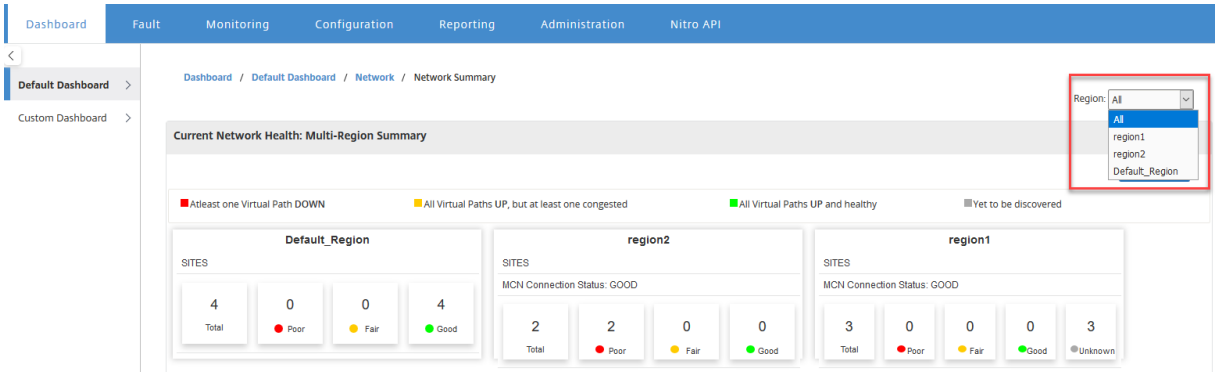
Pour un déploiement multi-régions, le widget **Récapitulatif du réseau** fournit une vue d'ensemble de l'intégrité du réseau dans toutes les régions. Une carte de région pour chaque région du réseau s'affiche avec les informations suivantes :

- Nombre total de sites dans la région.
- Le nombre de sites dans l'état pauvre. Un site est à l'état médiocre lorsqu'au moins un chemin virtuel est DOWN.
- Le nombre de sites dans l'état Acceptable. Un site est à l'état Acceptable lorsque tous les chemins virtuels du site sont actifs, mais au moins un chemin présente un problème de congestion ou un chemin membre est arrêté.
- Nombre de sites en bon état. Un site présente un bon état lorsque tous les chemins virtuels et les chemins membres associés sont actifs.
- Nombre de sites dans l'État inconnu. Un site est dans l'état Inconnu lorsque l'interrogation est en cours.

Pour afficher le résumé du réseau multirégion, accédez à **Tableau de bord** > **Tableau de bord par défaut** > **Réseau**> **Récapitulatif** du réseau et, dans le menu déroulant **Région**, sélectionnez **Tout**.



Par défaut, l'écran apparaît en **mode Réseau**. Vous pouvez voir l'intégrité réseau actuelle du récapitulatif du réseau multi-régions en cliquant sur **Region wise view**. Vous pouvez également voir l'état de la connexion MCN sur chaque vignette de région.



Cliquez sur une fiche région pour accéder au tableau de bord régional.

Pour une région donnée, le widget **Récapitulatif du réseau** fournit une vue d'ensemble de l'intégrité du réseau de la région sélectionnée.

Pour afficher le résumé du réseau régional, accédez à **Tableau de bord** > **Tableau de bord par défaut** > **Réseau** > **Récapitulatif du réseau** et, dans le menu déroulant **Région**, sélectionnez **une région**.

Vous pouvez afficher le récapitulatif du réseau régional dans la vue tuile ou la vue schématique.

Vous pouvez utiliser le contrôle chronologique pour afficher le récapitulatif de l'état du réseau pour une période sélectionnée. Vous pouvez également lire ou interrompre l'état du réseau sur une plage de temps.

Mode aide à voir le temps comme un concept relatif ou absolu.

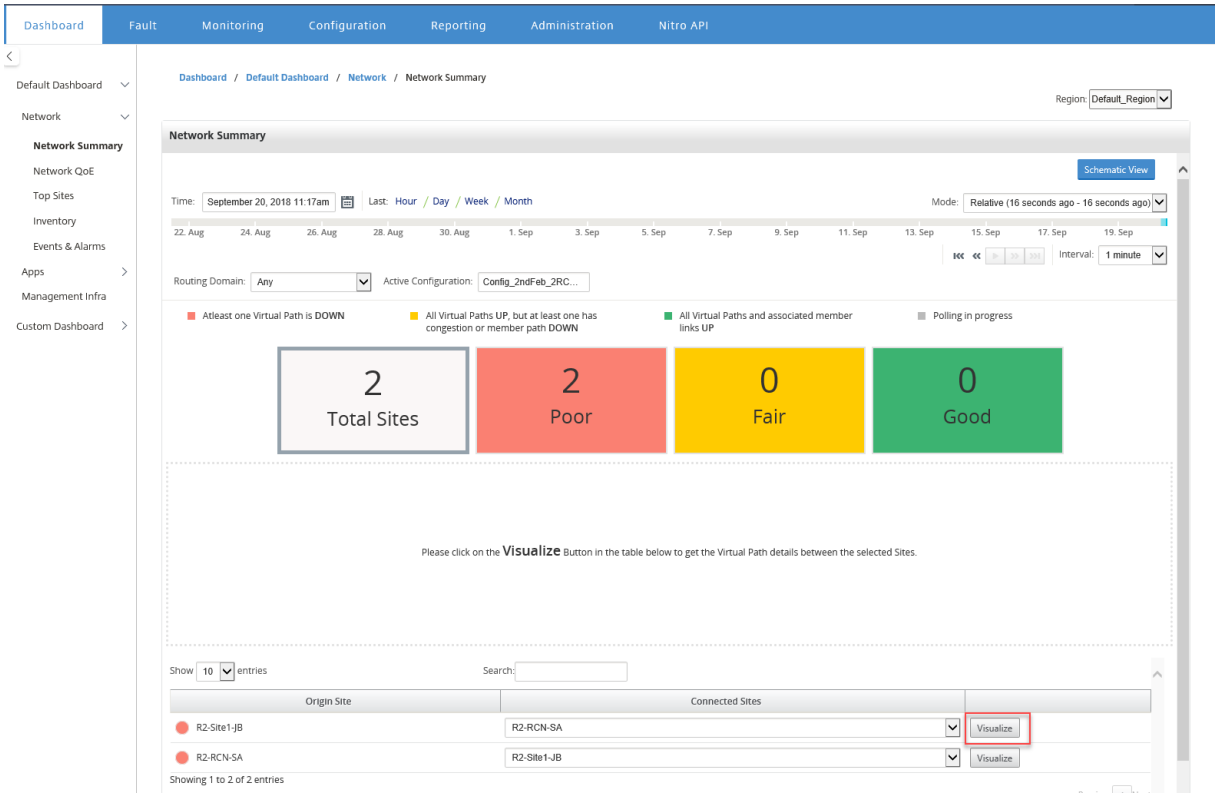
Pour plus d'informations sur la chronologie et le mode, reportez-vous à la section Commandes

Vue des tuiles

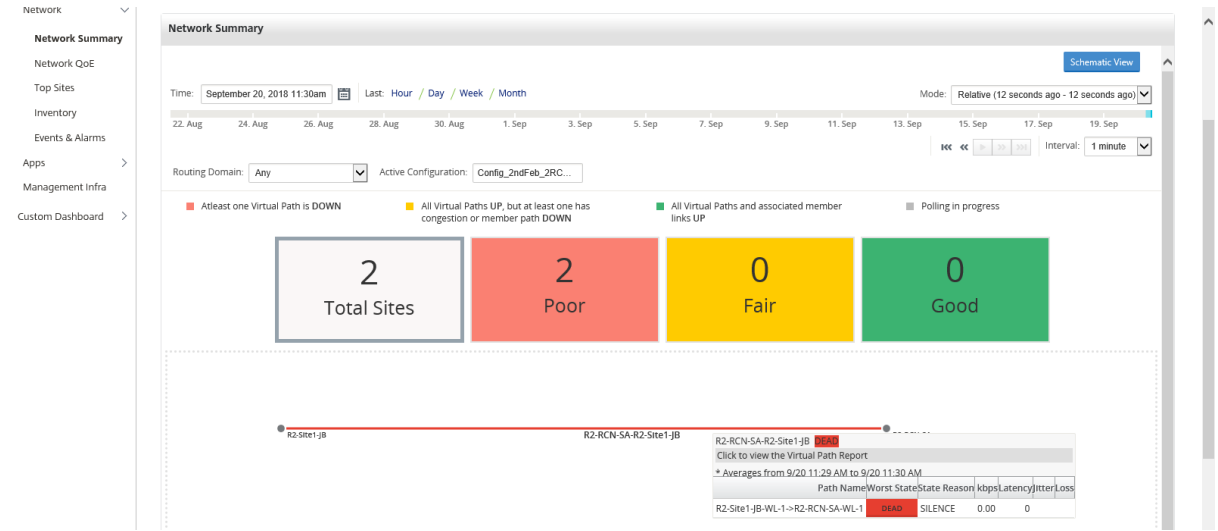
La vue de vignette fournit les informations suivantes :

- Nombre total de sites dans la région.
- Le nombre de sites dans l'état pauvre. Un site est à l'état médiocre lorsqu'au moins un chemin virtuel est DOWN.
- Le nombre de sites dans l'état Acceptable. Un site est à l'état Acceptable lorsque tous les chemins virtuels du site sont actifs, mais au moins un chemin présente un problème de congestion ou un chemin membre est arrêté.
- Nombre de sites en bon état. Un site présente un bon état lorsque tous les chemins virtuels et les chemins membres associés sont actifs.
- Nombre de sites dans l'État inconnu. Un site est dans l'état Inconnu lorsque l'interrogation est en cours.

Pour afficher une représentation graphique d'un chemin entre deux sites, sélectionnez-le et cliquez sur **Visualiser**.



Placez le curseur de la souris sur les sites ou le chemin d'accès pour afficher plus de détails. Cliquez sur les sites pour afficher et sélectionner les options de rapport.

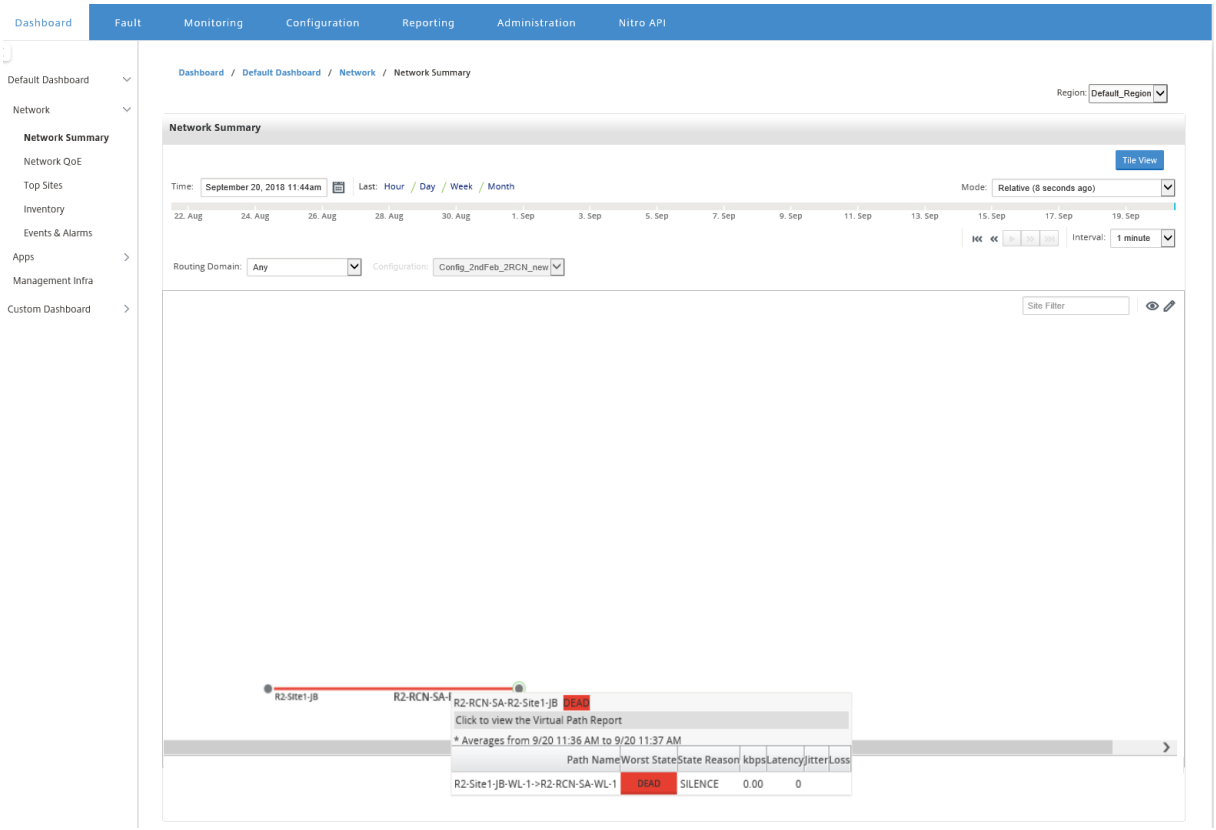


Vue schématique

La vue schématique fournit une vue graphique du réseau SD-WAN. Les informations affichées dans cette section sont mises à jour en fonction de la configuration et du domaine de routage sélectionnés. Pour afficher une carte réseau ici, vous devez importer la configuration réseau et les cartes réseau à

partir du nœud MCN (Master Controller Node). Pour plus d'informations, consultez la section Importer la configuration MCN.

Placez le curseur de la souris sur les sites ou le chemin d'accès pour afficher plus de détails. Cliquez sur les sites pour afficher les options de rapport.

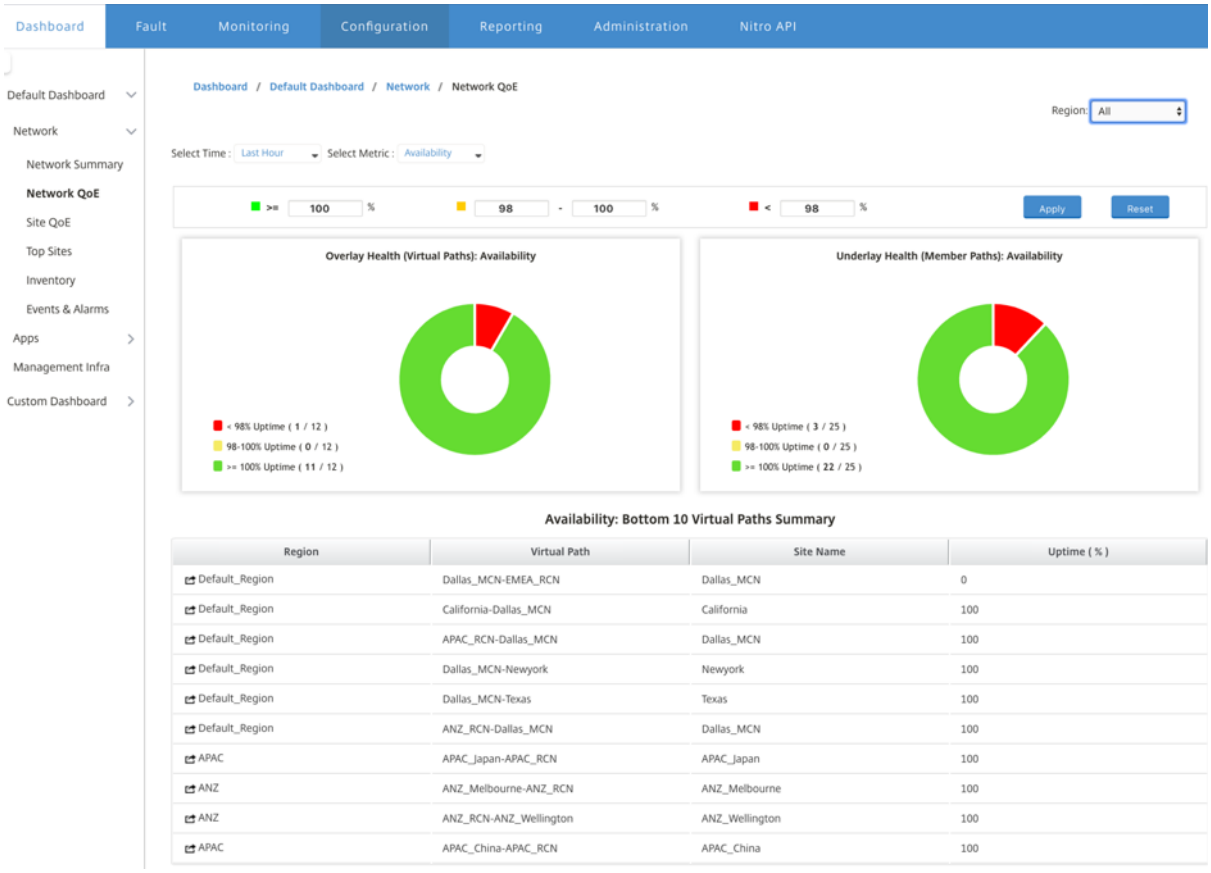


QoE réseau

Le widget **QoE réseau** fournit une représentation graphique des paramètres de disponibilité, de perte, de latence et de gigue d'un chemin virtuel. Il fournit les statistiques pour le chemin virtuel de super-position et les chemins de membre de sous-couche.

Pour un déploiement multi-région, vous pouvez afficher la liste des 10 chemins virtuels les plus bas en fonction de la mesure sélectionnée. Les données de chemin virtuel sont collectées à partir de tous les collecteurs régionaux pour l'intervalle de temps sélectionné. Vous pouvez afficher les détails de bande passante, de gigue, de perte et de congestion des chemins virtuels qui nécessitent le plus votre attention.

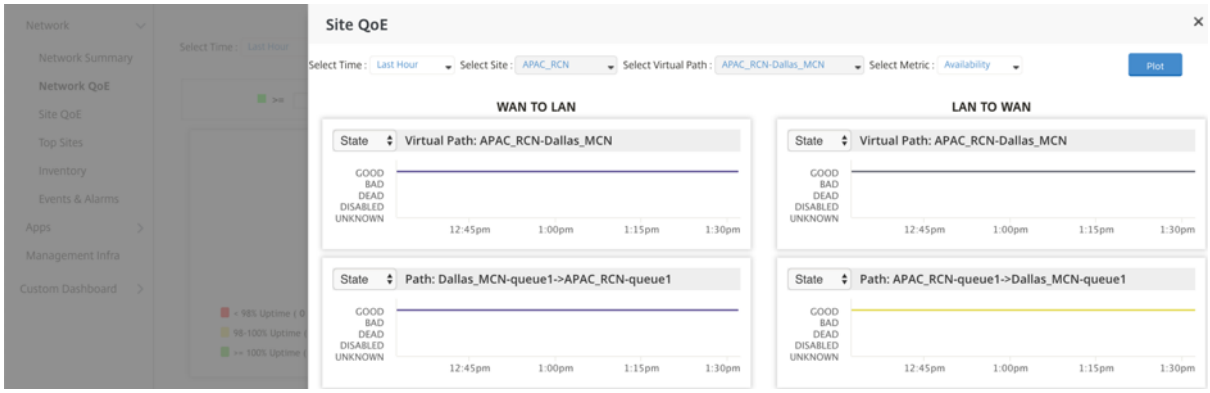
Pour afficher l'intégrité des chemins virtuels multi-régions, accédez à **Tableau de bord** > **Tableau de bord par défaut** > **Réseau**> **QoE réseau** et, dans le menu déroulant **Région**, sélectionnez **Tout.**



Pour une région donnée, vous pouvez afficher la liste des 10 chemins virtuels les plus bas en fonction de la mesure sélectionnée. Les statistiques sont collectées pour l'intervalle de temps sélectionné. Vous pouvez afficher les détails de bande passante, de gigue, de perte et de congestion des chemins virtuels qui nécessitent le plus votre attention.

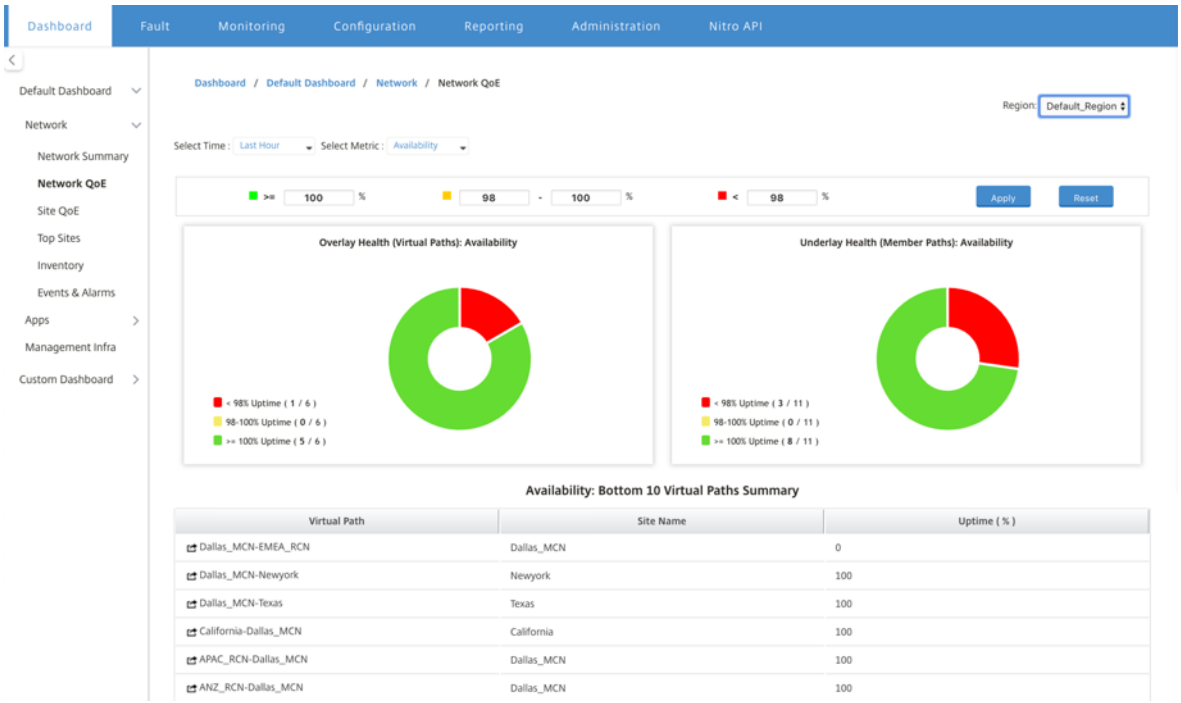
Vous pouvez comparer les chemins de superposition et de sous-couche pour la mesure sélectionnée (disponibilité, perte, gigue, latence) sur l'intervalle de temps sélectionné. Vous pouvez également définir des seuils personnalisés pour les mesures et les enregistrer en cliquant sur **Appliquer**. Cliquez sur **Réinitialiser** pour stocker les seuils par défaut.

L'utilisateur peut également effectuer une exploration vers le bas jusqu'à n'importe quel chemin virtuel dans la table en utilisant le bouton d'**exploration vers le bas** situé à gauche de chaque ligne. Un **site QoE** apparaît avec la comparaison détaillée entre le conduit et ses chemins de membre sous-jacents.



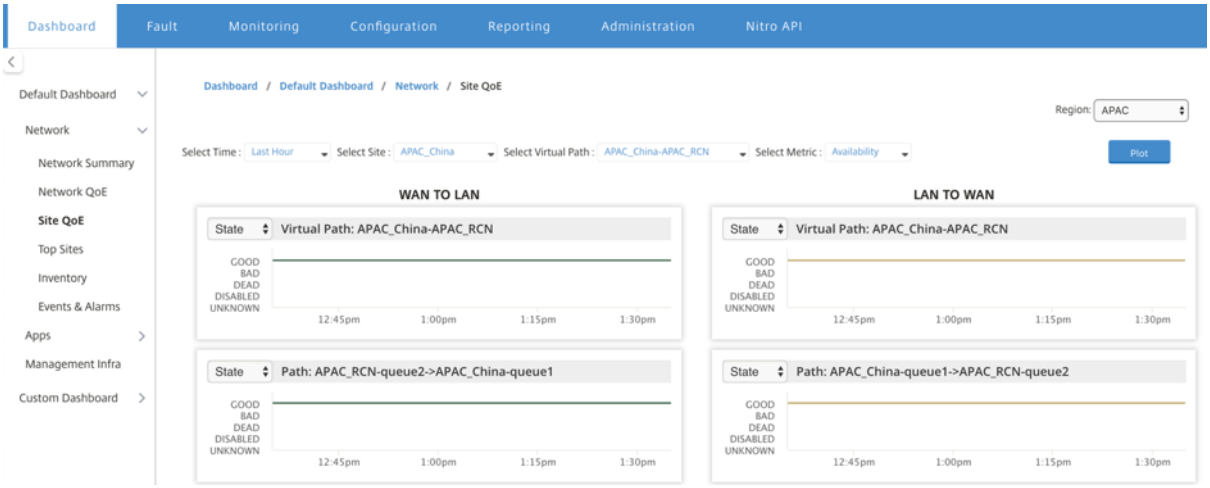
Dans le curseur, le nom du site et le chemin virtuel sont sélectionnés par défaut en fonction de la ligne sur laquelle vous avez cliqué et ils seront désactivés. Toutefois, l'utilisateur peut sélectionner une plage temporelle et une mesure différentes, puis cliquer sur l'option **Tracer** pour tracer les nouveaux graphiques.

Pour afficher les statistiques d'intégrité des chemins virtuels régionaux, accédez à **Tableau de bord**> **Tableau de bord par défaut** > **Réseau**> **QoE** réseau et, dans le menu déroulant **Région**, sélectionnez une région.



Site QoE

Vous pouvez utiliser Site QoE comme outil pour comparer le chemin virtuel et ses chemins de membre sous-jacents. Vous devez sélectionner un site et un chemin virtuel à partir de ce site et de cette mesure. Cliquez sur **Tracer**.

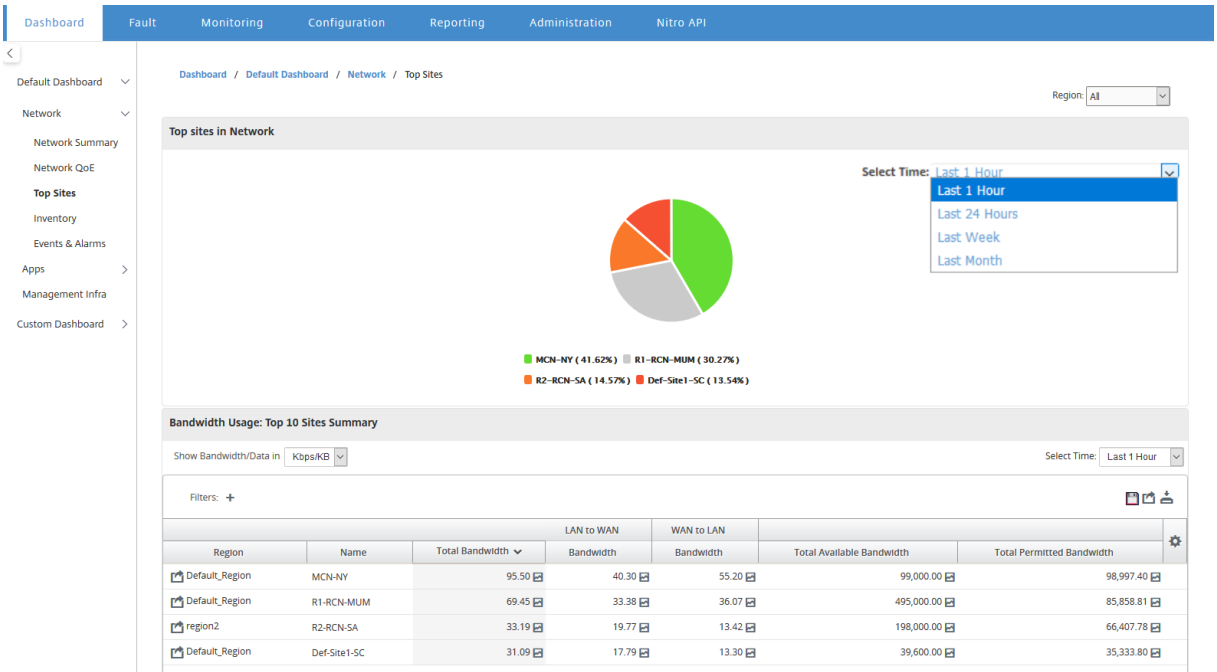


Dans la première section, il trace les statistiques des chemins virtuels dans le sens **WAN vers LAN** et **LAN vers WAN** . Ci-dessous tracent tous les graphiques des chemins de membres sous-jacents. Ces deux éléments sont présents à la fois au niveau de la région et du réseau.

Meilleurs sites

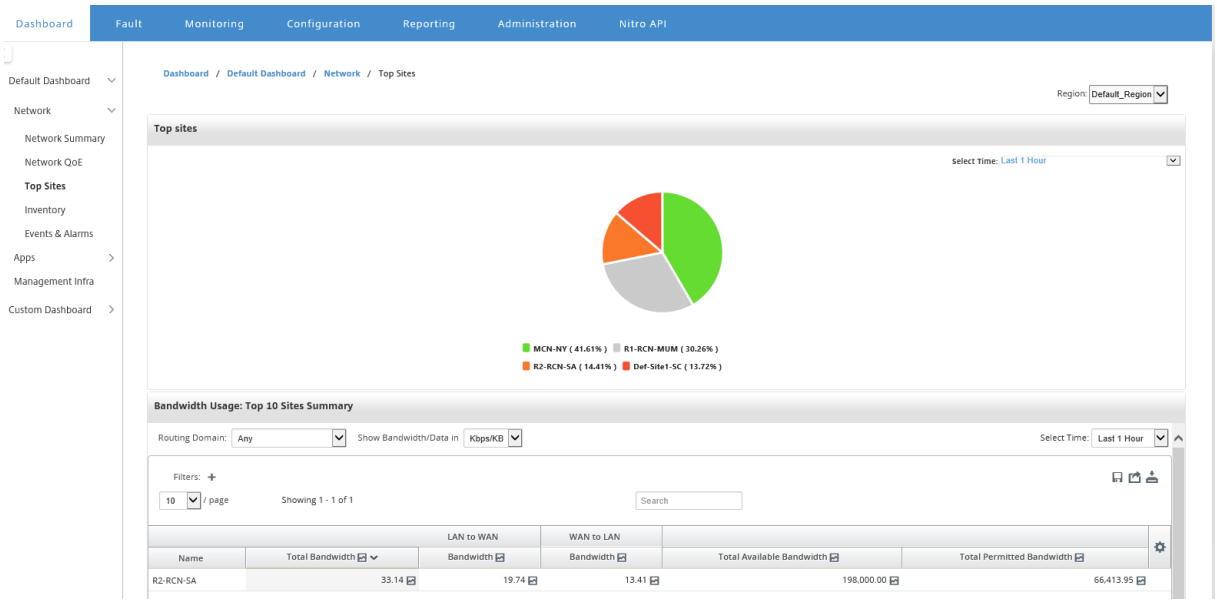
Pour un déploiement multi-régions, le widget **Sites principaux** répertorie les 10 principaux sites de toutes les régions, qui ont l'utilisation la plus élevée de la bande passante, dans l'intervalle de temps sélectionné.

Pour afficher les principaux sites dans toutes les régions, accédez à **Tableau de bord** > **Tableau de bord par défaut** > **Réseau** > **Sites principaux** et sélectionnez **Tout** dans le menu déroulant **Région**.



Cliquez sur un site ou une mesure pour afficher des rapports détaillés et des statistiques.

Pour une région donnée, le widget Sites principaux affiche les statistiques d'utilisation de la bande passante pour tous les sites de la région. Les statistiques sont collectées pour l'intervalle de temps sélectionné. Vous pouvez filtrer les sites en fonction du domaine de routage.



Inventory

Toutes les 30 minutes, le gestionnaire d'inventaire recueille les informations matérielles de toutes les appliances Citrix SD-WAN découvertes sur Citrix SD-WAN Center.

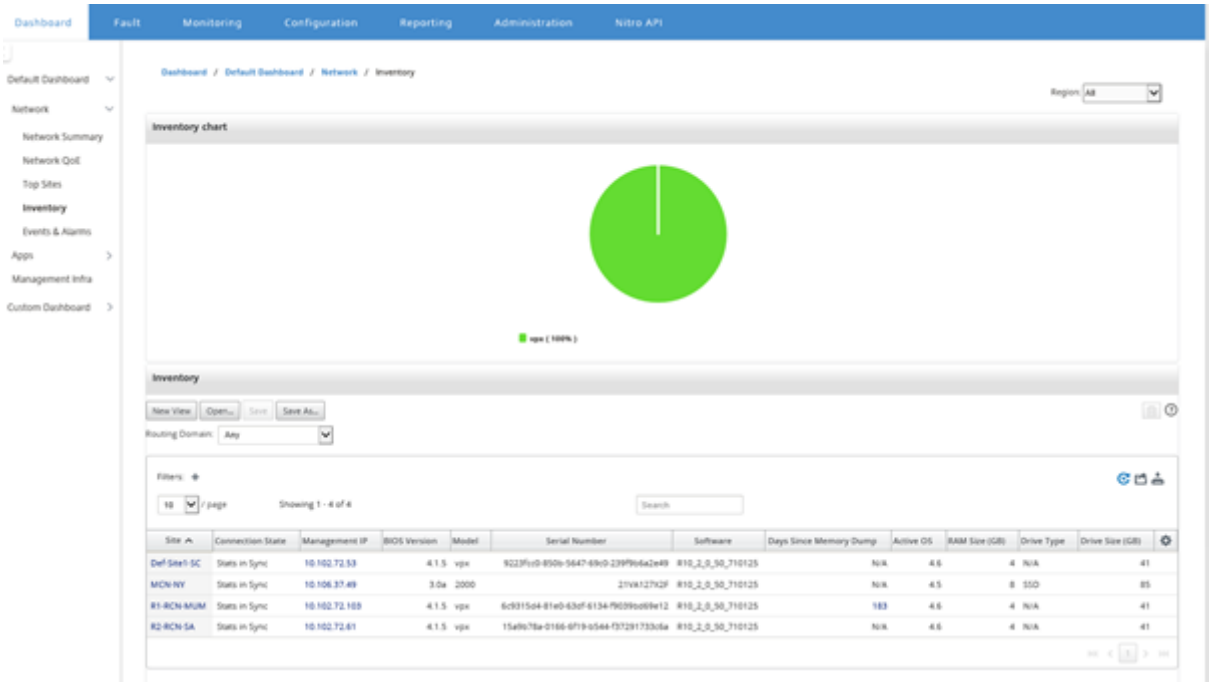
Pour afficher les statistiques d'inventaire multi-régions, accédez à **Tableau de bord** > **Tableau de bord par défaut** > **Réseau** > **Inventaire** et sélectionnez dans le menu déroulant **Région** .

Pour afficher les statistiques d'inventaire d'une région spécifique, sélectionnez la **région** dans le menu déroulant Région.

Vous pouvez consulter les statistiques de stock suivantes :

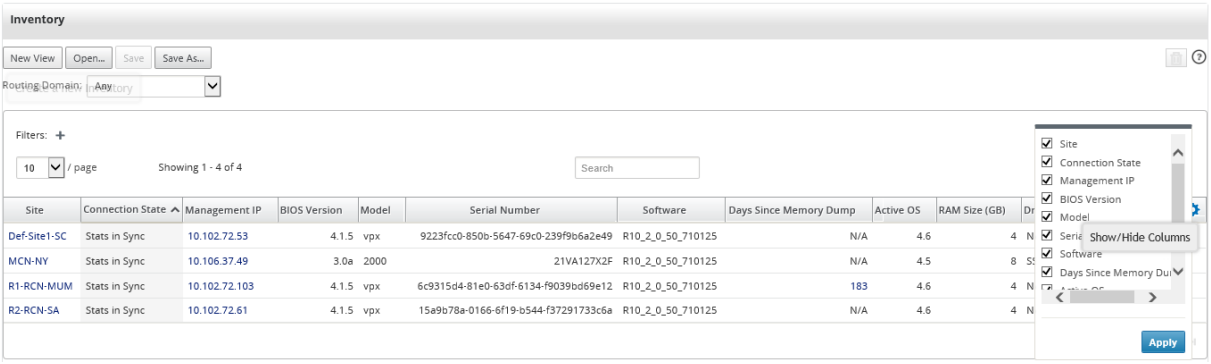
- **Site** : nom du site trouvé dans la configuration en cours d'exécution dans le MCN. Si l'appliance est un MCN secondaire, « (secondaire) » apparaît en regard du nom. Vous pouvez cliquer sur le nom pour accéder à la console Web de l'appliance.
- **Étatde la connexion** : état de la connectivité à l'appliance. Une icône rouge apparaît lorsque la connexion n'est pas accessible ou n'est pas authentifiée.
- **IP de gestion** : adresse IP de gestion de l'appliance. Vous pouvez cliquer sur l'adresse IP pour accéder à la console Web de l'appliance.
- **Version du BIOS** : version du BIOS de l'appliance.
- **Modèle** : Modèle matériel de l'appliance.

- **Numéro de série** : numéro de série de l'appliance.
- **Logiciel** ; numéro de version du logiciel SD-WAN.
- **Jours depuis le vidage de la mémoire** : Temps écoulé depuis le dernier vidage de mémoire d'erreur système. Si l'appliance a vidé sa mémoire au cours des quatre derniers jours, une icône d'erreur apparaît en regard de l'heure. Si le vidage de mémoire s'est produit il y a 5 à 10 jours, une icône d'avertissement s'affiche. N/A apparaît si aucun vidage n'est disponible. Cliquez sur l'heure pour ouvrir la page de journal du SD-WAN.
- **Système d'exploitation actif** : système d'exploitation en cours d'exécution sur l'appliance.
- **Taille de la RAM (Go)** : quantité de RAM actuellement installée sur l'appliance en Go.
- **Type de lecteur** : Type de lecteur de stockage de données installé sur l'appliance. La valeur peut être SSD (Solid State Drive) ou HDD (Dur Disk Drive).
- **Taille du disque (Go)** : taille du lecteur de stockage de données actuellement installé sur l'appliance en Go.



Remarque

Vous pouvez organiser les colonnes de la table des statistiques d'inventaire à l'aide de l'option **Afficher/Masquer les colonnes** .



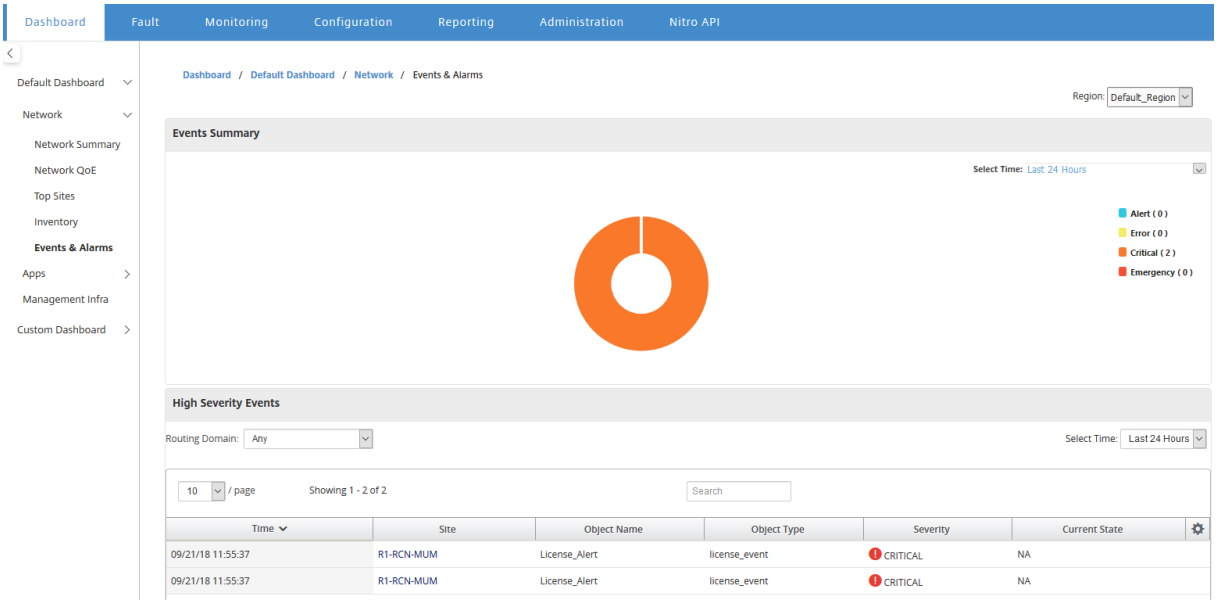
Événements et alarmes

Pour un déploiement multi-région, vous pouvez afficher les événements et les alarmes de toutes les régions du réseau. Ces informations sont collectées pour l'intervalle de temps sélectionné. Pour afficher les événements et les statistiques de plusieurs régions, accédez à **Tableau de bord** > **Tableau de bord par défaut** > **Réseau**> **Événements et alarmes**, puis sélectionnez **Tout** dans le menu déroulant **Région** .

Vous pouvez également afficher tous les événements et alarmes d'une région donnée. Ces informations sont collectées pour l'intervalle de temps sélectionné. Pour afficher les statistiques sur les événements et les alarmes, accédez à **Tableau de bord** > **Tableau de bord par défaut** > **Réseau**> **Événements et alarmes**, puis sélectionnez une région dans le menu déroulant **Région**.

La section **Récapitulatif des événements** donne un aperçu graphique du type d'événement et de la quantité d'événements. Vous pouvez cliquer sur le graphique pour afficher les événements sur la page **Fault**. L'affichage indique également le nombre d'événements dans chaque catégorie. Les déclencheurs d'alarme peuvent être configurés sur les appliances SD-WAN individuelles. Pour plus d'informations, voir Notifications d'événements.

La section **Evénements de gravité élevée** affiche la liste des événements graves. Vous pouvez filtrer les événements en fonction du domaine de routage. Les informations affichées dans cette section sont collectées à partir de l'onglet **Défaut** . Pour plus d'informations, consultez la section Événements.

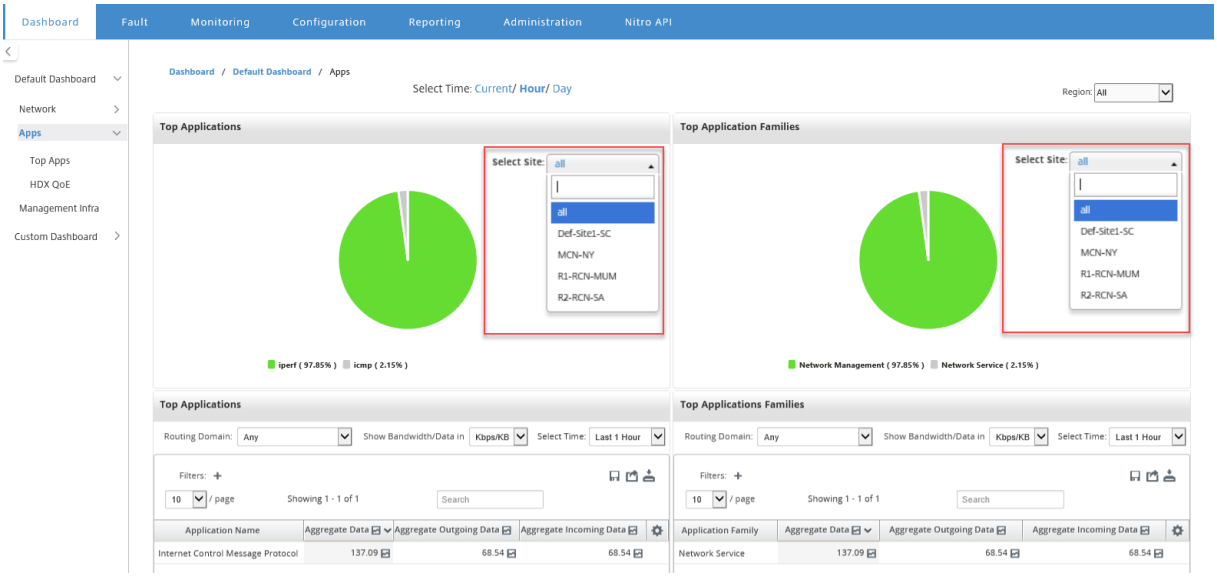


Applications

Top apps

L'inspection approfondie des paquets (DPI) permet à l'appliance SD-WAN d'analyser le trafic qui le traverse et d'identifier les types d'applications et de famille d'applications. Pour un déploiement multi-régions, vous pouvez afficher les meilleures applications et familles d'applications dans toutes les régions du réseau. Ces informations sont collectées pour l'intervalle de temps sélectionné.

Pour afficher les statistiques d'application les plus importantes dans toutes les régions du réseau, accédez à **Tableau de bord** > **Tableau de bord par défaut** > **Applications > Top Apps**, puis sélectionnez **Tout** dans le menu déroulant **Région**.

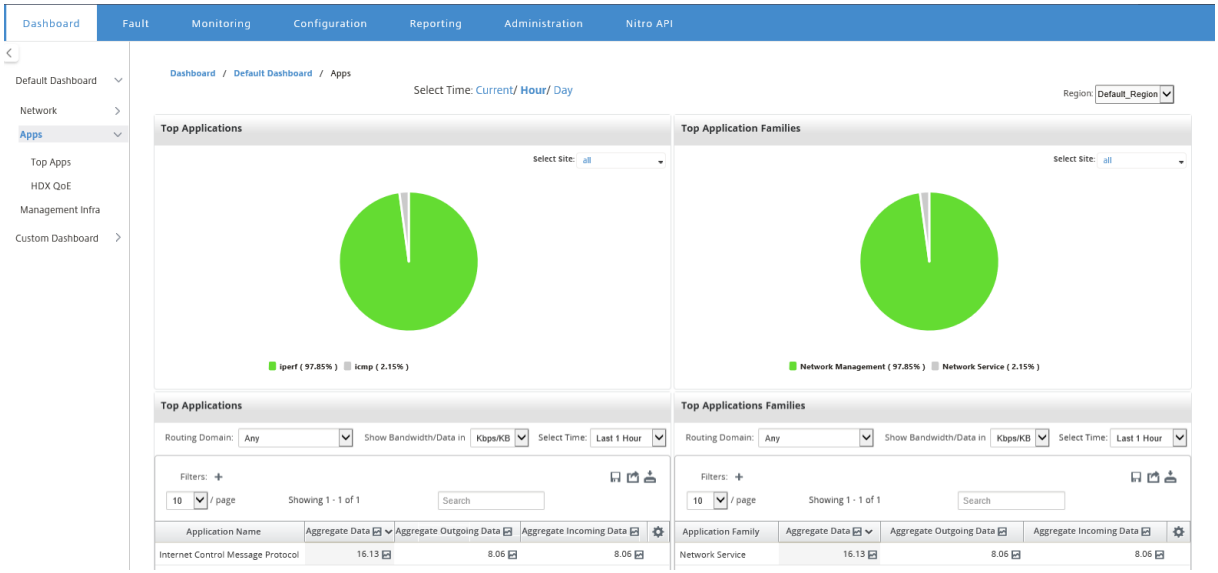


Vous pouvez afficher la liste déroulante consultable pour la sélection de sites pour les familles d'**applications les plus populaires** et les **familles d'applications les plus populaires**.

Vous pouvez également afficher les applications les plus importantes et les familles d'applications les plus importantes d'une région particulière.

Pour afficher les statistiques d'application d'une région, accédez à **Tableau de bord** > **Tableau de bord par défaut**> **Applications > Top Apps** et sélectionnez une région dans le menu déroulant **Région**.**

Vous pouvez sélectionner le site et l'intervalle de temps comme dernières 24 heures, dernière heure ou actuelle.

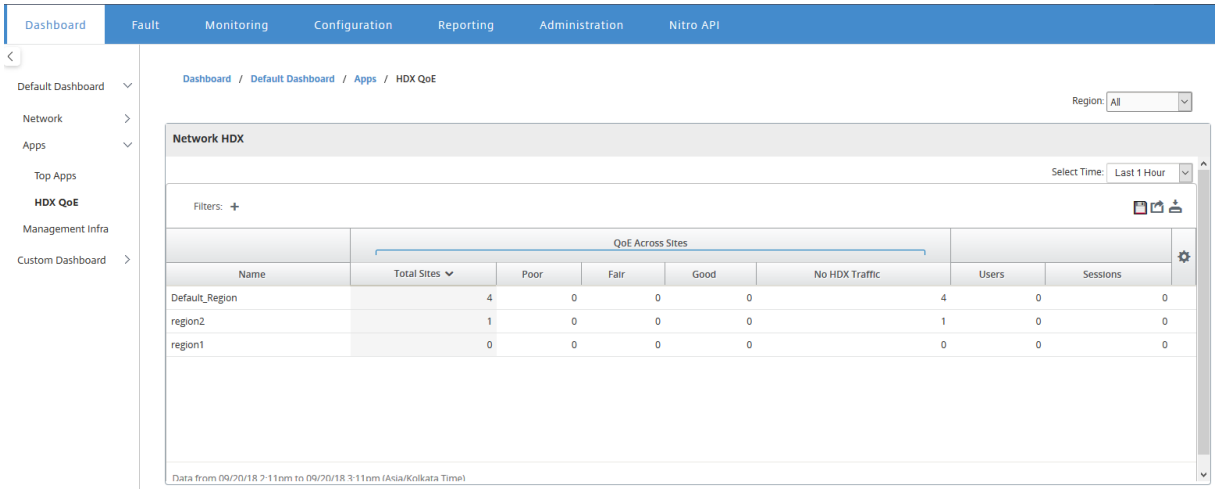


QoE HDX

La qualité de l'expérience (QoE) est un indice calculé qui vous aide à comprendre la qualité de votre expérience ICA. Cet index est calculé pour tout le trafic d'application ICA traversé du WAN vers le site. Les statistiques de chute de paquets, de gigue et de latence sont utilisées dans le calcul QoE. La QoE est un entier compris entre [0, 100], plus le nombre est élevé, meilleure est l'expérience utilisateur.Les statistiques de gigue, de latence et de dépôt de paquets sont suivies sur les chemins de données pendant le traitement des paquets.

Les sites de l'ensemble du réseau sont classés comme trafic HDX bon, passable, mauvais ou aucun trafic HDX en fonction de la QoE du trafic HDX. Pour plus d'informations, consultez QoE HDX.

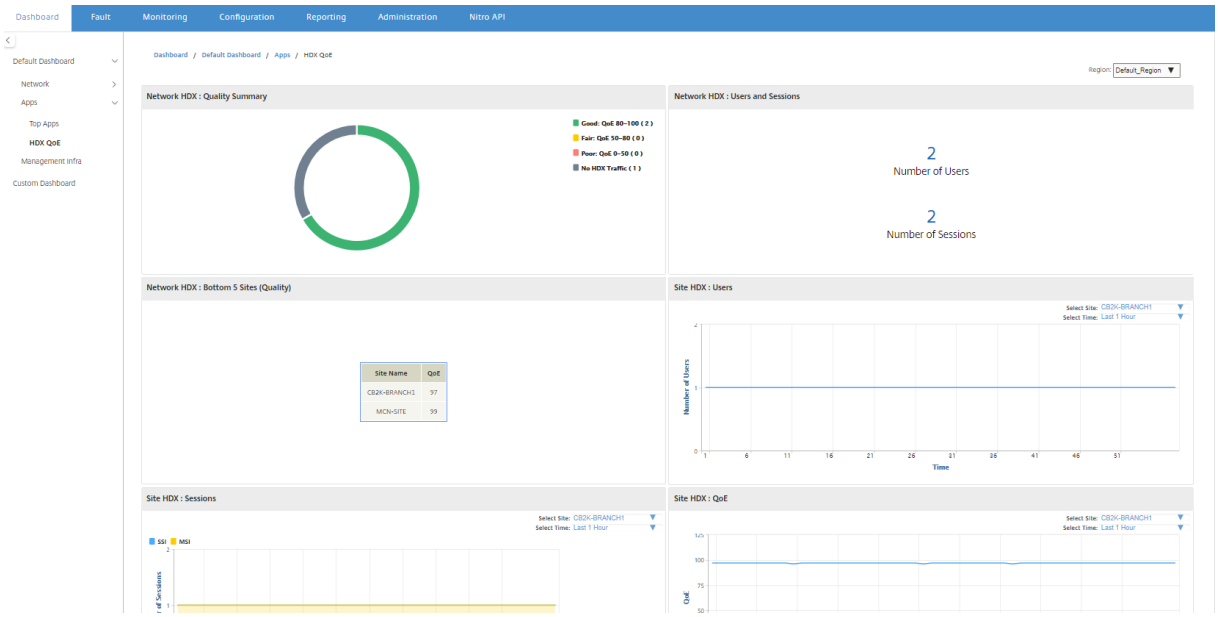
Pour afficher la QoE HDX, des sites, dans toutes les régions du réseau, accédez à **Tableau de bord** > **Tableau de bord par défaut** > **Applications > QoE HDX**, puis sélectionnez **Tout** dans le menu déroulant **Région**.



Vous pouvez afficher les mesures HDX QoE suivantes pour chaque région.

- Réseau HDX : Récapitulatif de la qualité
- Réseau HDX : Utilisateurs et sessions
- Réseau HDX : cinq sites les plus bas (qualité)
- Site HDX : Utilisateurs
- Site HDX : Sessions
- Site HDX : Qualité d'expérience

Pour afficher les statistiques HDX QoE, accédez à **Tableau de bord** > **Tableau de bord par défaut**> **Applications > HDX QoE** et dans le menu déroulant **Région**, sélectionnez une région.



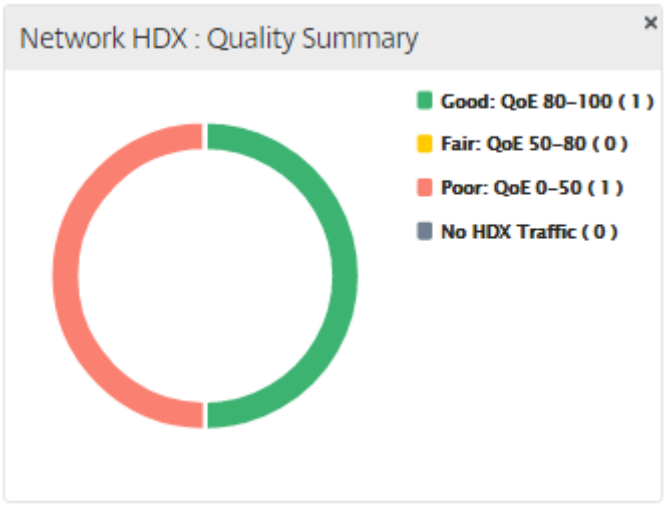
> **Remarque**
>
> Parfois, les données du tableau de bord HDX et les rapports HDX provenant de différents sites

> peuvent ne pas sembler synchronisés car chaque statistique de site est interrogé indépendamment.
>
> Sur les widgets de tableau de bord HDX, vous pouvez voir un site sans trafic HDX, mais il peut y avoir un nombre non nul de sessions HDX et d'utilisateurs. Cela se produit lorsque les sessions HDX restent inactives pendant cette période d'interrogation et restent toujours en état ouvert.

Réseau HDX : résumé de la qualité

Le trafic HDX est classé dans les catégories de qualité suivantes :

Qualité	Gamme QoE
Bon	80–100
Acceptable	50–80
Médiocre	0–50
Pas de trafic HDX	S.O.

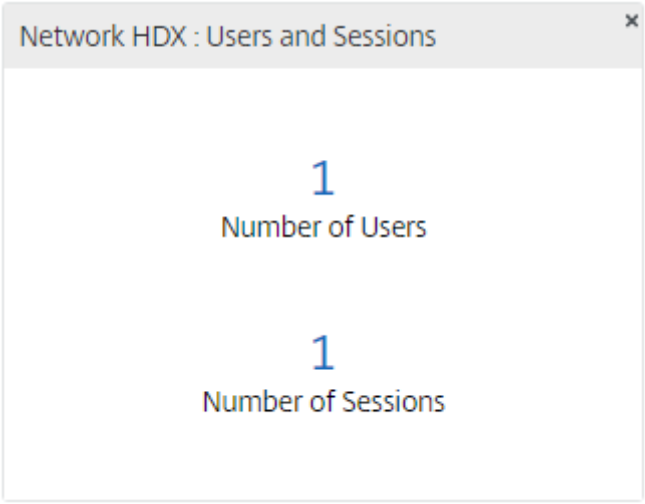


Vous pouvez cliquer sur le graphique pour afficher les rapports HDX par site. Pour plus d'informations, consultez Procédure d'affichage des rapports HDX.

Réseau HDX : Utilisateurs et sessions

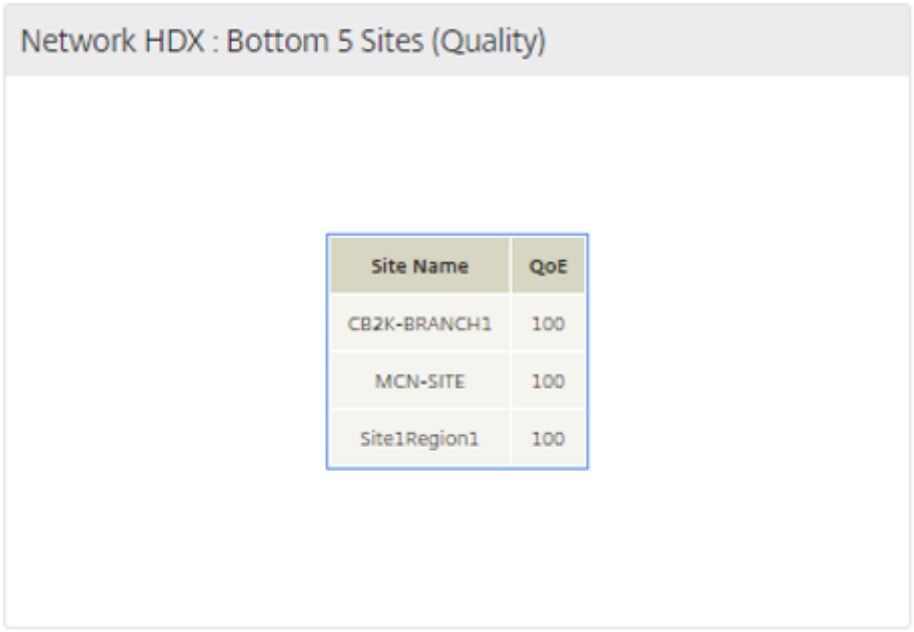
Ce widget fournit des informations sur le nombre d'utilisateurs HDX actifs et de sessions. Le nombre de sessions est le nombre total de sessions ICA de session unique (SSI) et de sessions ICA multisession (MSI) actives.

> **Remarque**
>
> Dans la version actuelle, le nombre d'utilisateurs n'est pas basé sur des noms d'utilisateur distincts. C'est-à-dire que deux sessions démarrées par un seul utilisateur sur deux machines différentes sont comptées comme deux utilisateurs.



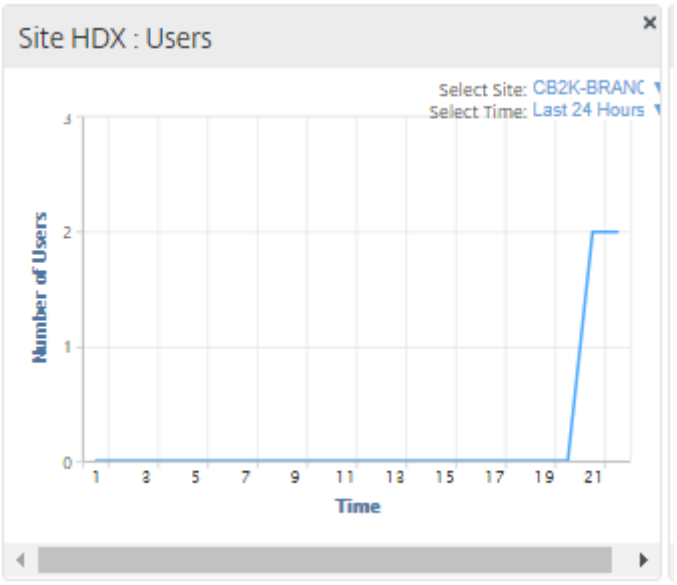
Réseau HDX : 5 sites inférieurs (qualité)

Ce widget fournit une liste des 5 sites les plus bas qui ont le moins de score QoE. Il aide à stimuler de meilleures initiatives en matière d'expérience utilisateur final.



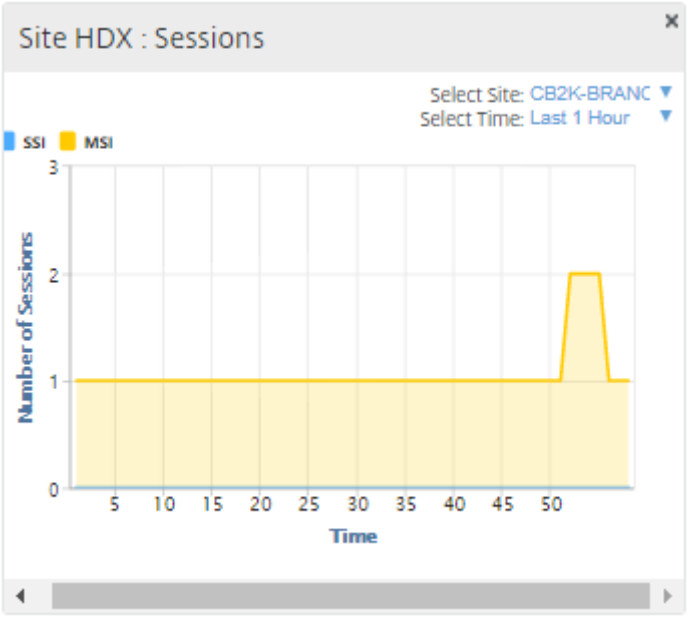
Site HDX : Utilisateurs

Ce widget fournit une représentation graphique du nombre d'utilisateurs qui étaient actifs sur un site particulier pour l'intervalle de temps sélectionné. Vous pouvez sélectionner le site et l'intervalle de temps comme les dernières 24 heures, la dernière heure ou les 5 dernières minutes.



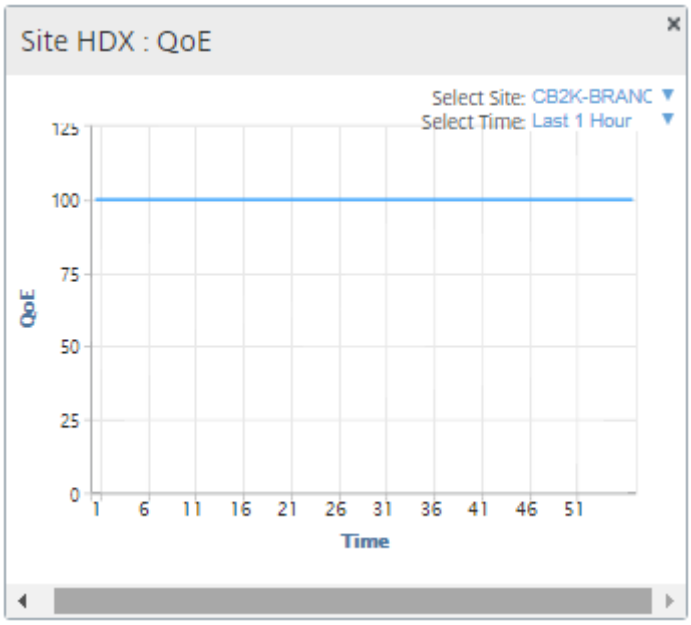
Site HDX : Sessions

Ce widget fournit une représentation graphique du nombre de sessions MSI et SSI actives sur un site particulier pour l'intervalle de temps sélectionné. Vous pouvez sélectionner le site et l'intervalle de temps comme les dernières 24 heures, la dernière heure ou les 5 dernières minutes.



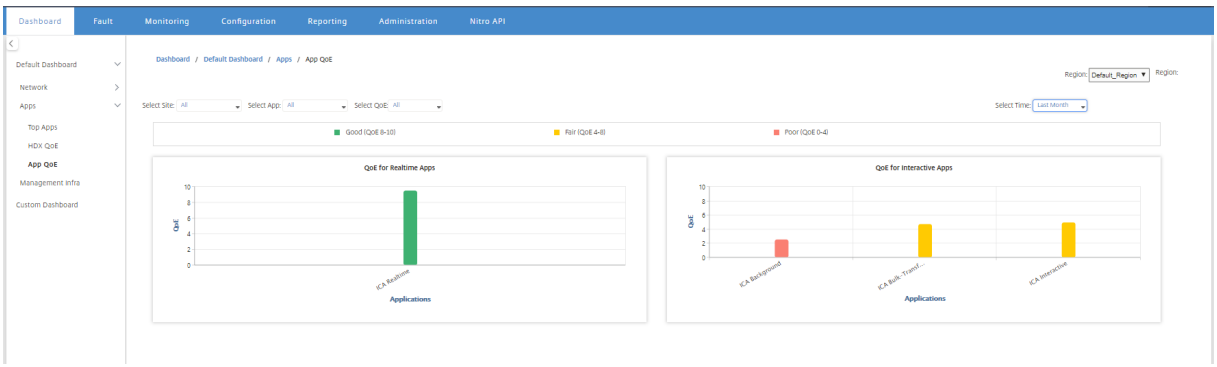
Site HDX : Qualité de l'expérience

Ce widget fournit une représentation graphique de la QoE globale sur un site particulier pour l'intervalle de temps sélectionné. Vous pouvez sélectionner le site et l'intervalle de temps comme les dernières 24 heures, la dernière heure ou les 5 dernières minutes.



QoE des applications

Application QoE est une mesure de la qualité de l'expérience pour une application. La plage de pointage QoE de l'application est de 0 à 10, où 10 représente une excellente qualité et 0 représente une mauvaise qualité. Pour plus d'informations, consultez la section QoE des applications. Vous pouvez afficher le score QoE de l'application pour le trafic en temps réel et interactif.

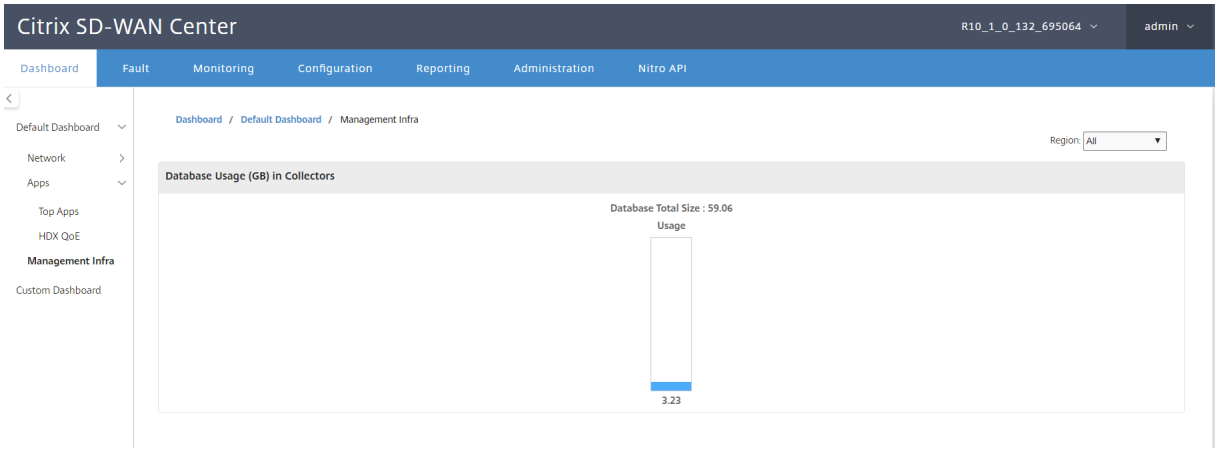


Vous pouvez filtrer les statistiques QoE de l'application par site, application ou type QoE.

Gestion infra

La page Gestion Infra vous permet d'afficher les statistiques d'utilisation de la base de données Citrix SD-WAN Center et de stockage.

Pour un déploiement multi-région, vous pouvez afficher l'utilisation de la base de données de tous les collecteurs du réseau. Pour afficher les statistiques de base de données multi-régions, accédez à **Tableau de bord**> **Tableau de bord par défaut** > **Gestion infra**, puis sélectionnez **Tout** dans le menu déroulant **Région** .



Pour afficher les statistiques de base de données Citrix SD-WAN Center pour une région particulière, accédez à **Tableau de bord** > **Tableau de bord par défaut** > **Gestion Infra,** puis sélectionnez une région dans le menu déroulant **Région**.

La section **Utilisation de la base** de données affiche une vue d'ensemble graphique de l'utilisation des ressources de base de données et des seuils d'envoi de notifications ou d'arrêt de la collecte des données. Vous pouvez cliquer sur le graphique pour afficher les détails sur la page Maintenance de la base de données.

- **Utilisation** : Capacité de base de données actuellement utilisée, en Go.
- **Notification** : Seuil de génération d'une notification d'utilisation de base de données. Le seuil est un pourcentage de la taille maximale de la base de données. Si une alerte par e-mail est configurée, une notification par e-mail est envoyée lorsque la taille de la base de données dépasse ce seuil. Pour plus d'informations, consultez Notifications d'événements.
- **Arrêter l'interrogation** : Seuil d'arrêt de l'interrogation des statistiques. Le seuil est un pourcentage de la taille maximale de la base de données. L'interrogation s'arrête lorsque la taille de la base de données dépasse ce seuil. Pour plus d'informations, consultez Gérer la base de données

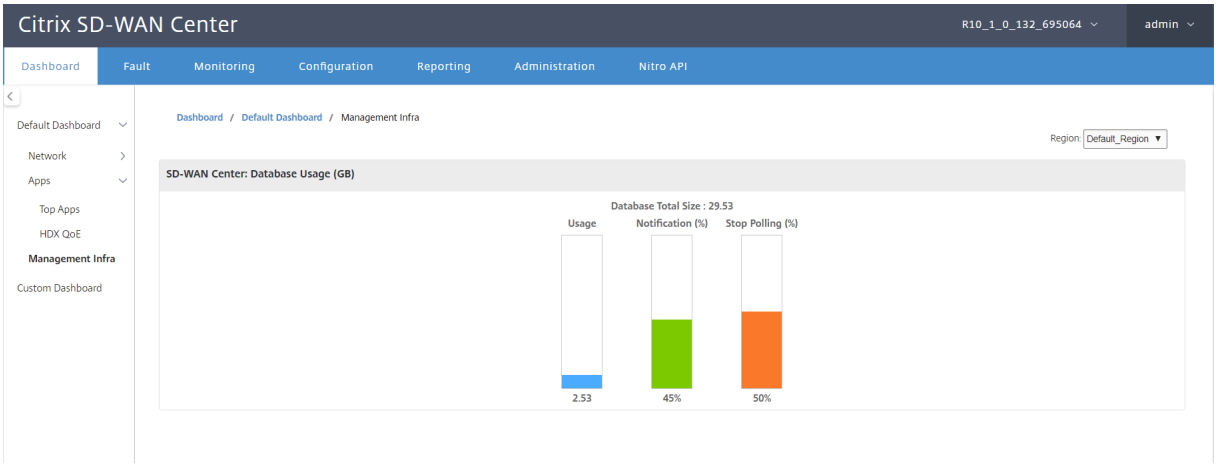
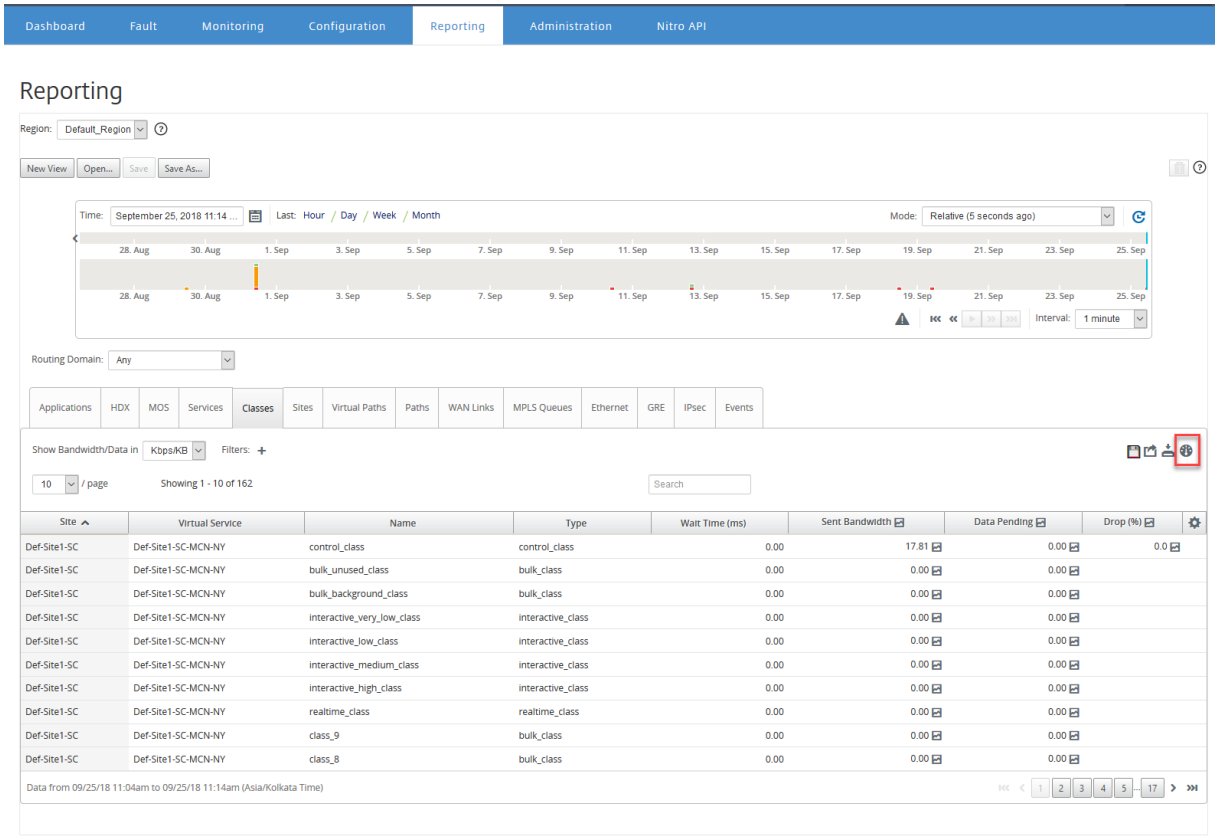


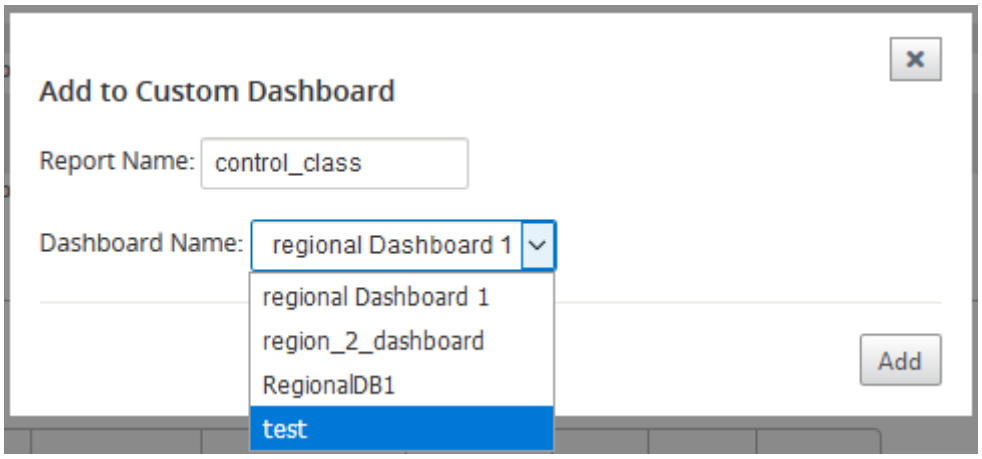
Tableau de bord personnalisé

Vous pouvez personnaliser le tableau de bord Citrix SD-WAN Center et choisir les statistiques que vous souhaitez afficher sur le tableau de bord en fonction de vos besoins analytiques. Créez un tableau de bord personnalisé de détails régionaux ou un résumé global. Vous pouvez également personnaliser un rapport existant.

> **Remarque**
>
> Vous pouvez désormais épingler un rapport en tant que widget à votre tableau de bord personnalisé, en utilisant l'option **Ajouter au tableau de bord** de la page Rapports.



Entrez le nom du rapport et sélectionnez le tableau de bord personnalisé.



Pour le tableau de bord personnalisé Détails régionaux, vous pouvez choisir parmi les widgets de niveau région suivants :

- Résumé du site
- Chemin virtuel
- Événements régionaux
- Résumé des alarmes de région
- Gestionnaire d'inventaire (par région)

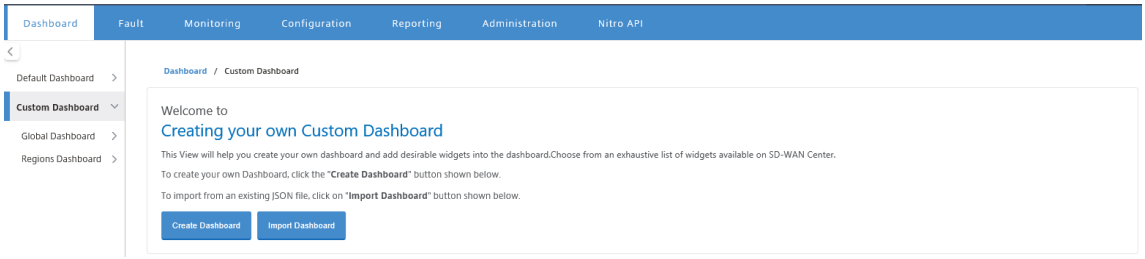
- Meilleurs sites par région
- Chemins
- Files d'attente MPLS
- Ethernet
- Tunnels LAN GRE
- Tunnels IPSec
- Résumé du service
- Classes
- Événements Site
- Applications les plus populaires par région
- Famille d'applications par région
- Site HDX : Utilisateurs
- Site HDX : Sessions
- Site HDX : QoE
- Applications MOS
- Utilisation de la base

Pour un tableau de bord personnalisé Récapitulatif global, vous pouvez choisir parmi les widgets de niveau réseau suivants :

- Résumé multi-région
- Santé du chemin virtuel dans le réseau
- Événements
- Résumé de l'alarme
- Gestionnaire d'inventaire
- Meilleurs sites dans Réseau
- Réseau HDX
- Utilisation de base de données dans les collecteurs
- Principales applications
- Meilleures familles d'applications

Pour créer un tableau de bord personnalisé :

1. Accédez à **Tableau de bord** > **Tableau de bord personnalisé**, puis cliquez sur **Créer un tableau de bord** .

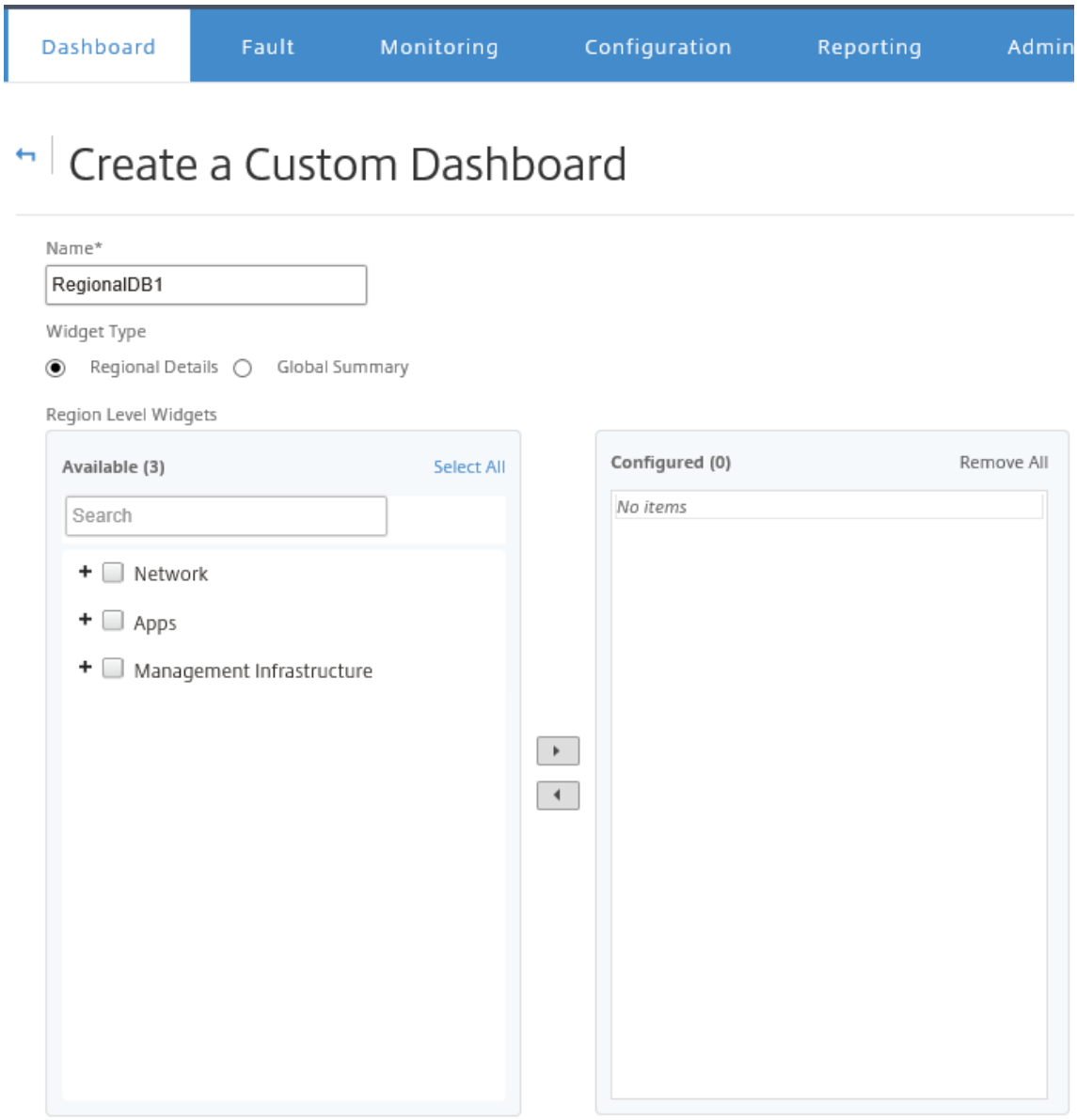


> **Remarque**
>
> Vous pouvez également importer un tableau de bord existant au format JSON en cliquant sur **Importer le tableau de bord**.

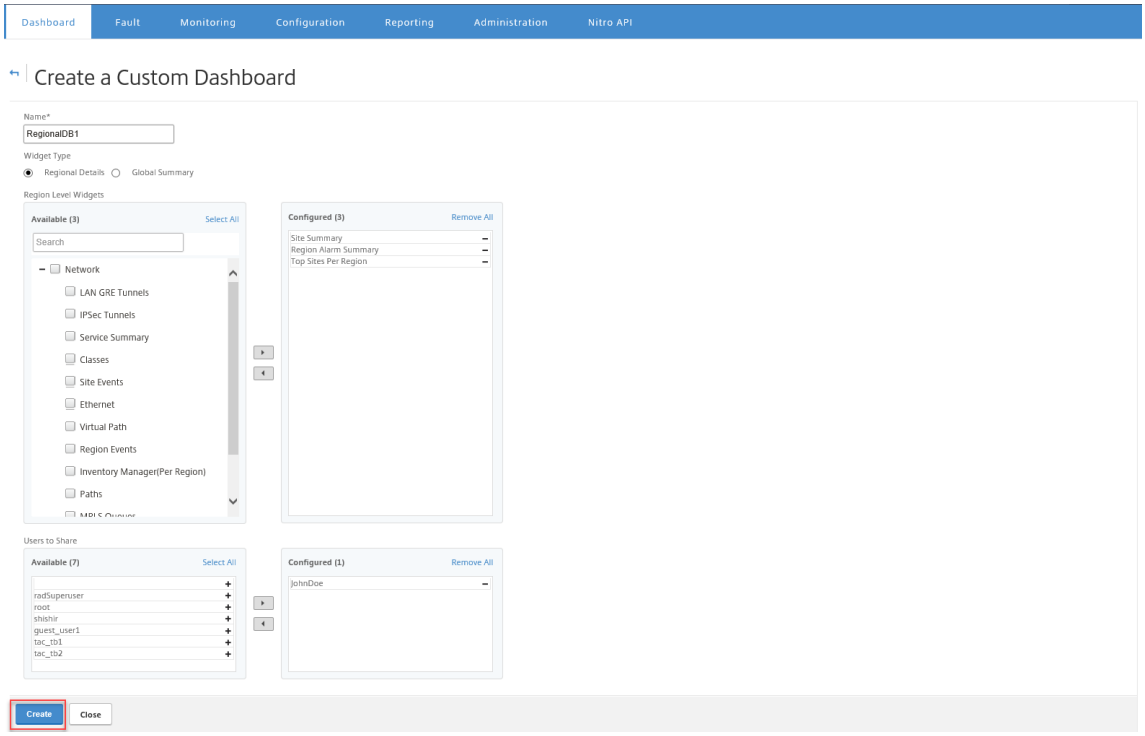
2. Dans le champ **Nom**, entrez un nom pour le tableau de bord personnalisé.
3. Sélectionnez le type de widget. Sélectionnez **Synthèse globale** pour afficher les widgets au niveau réseau, sélectionnez **Détails régionaux** pour afficher les widgets de niveau régional.

4. Cliquez sur **Ajouter** et sélectionnez les widgets requis.

   Les widgets sont classés en trois niveaux : Réseau, Applications et Infrastructure de gestion.



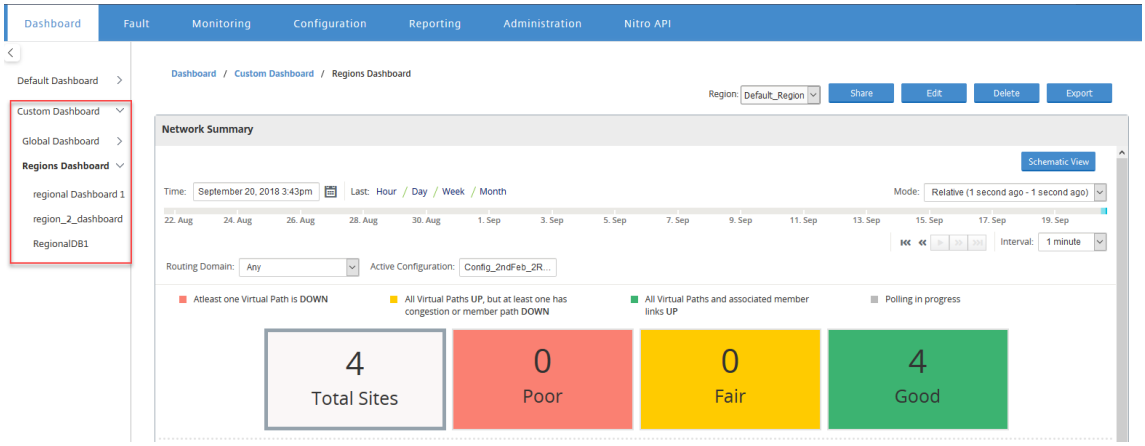
> Remarque
>
> Dans le déploiement d'une seule région, seuls les **widgets de niveau région** sont disponibles.



Vous pouvez également partager le tableau de bord personnalisé avec plusieurs utilisateurs. Pour plus d'informations sur les utilisateurs, consultez la section Comptes d'utilisateurs.

5. Cliquez sur **Créer**. Le tableau de bord personnalisé nouvellement créé est répertorié sous **Tableau de bord personnalisé**.

> **Conseil**
>
> Vous pouvez modifier ou supprimer le tableau de bord personnalisé.



Forfaits de diagnostic

February 17, 2022

Un package de diagnostic comprend tous les fichiers journaux système, les informations système et d'autres détails nécessaires qui aideront l'équipe de support Citrix SD-WAN à diagnostiquer et résoudre les problèmes liés à votre système.

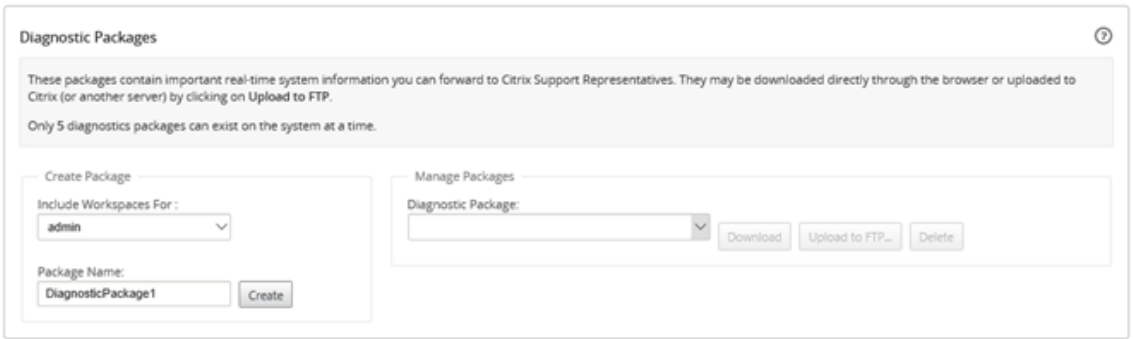
Après avoir créé le package, vous pouvez le télécharger sur votre ordinateur, puis envoyer le package de diagnostic au support client Citrix ou vous pouvez le télécharger directement sur le serveur de support client Citrix (ou un autre serveur).

> **Remarque**
>
> Citrix SD-WAN Center peut stocker au maximum cinq packages de diagnostic à la fois.

Pour créer un package de diagnostic :

1. Dans l'interface Web Citrix SD-WAN Center, cliquez sur l'onglet **Surveillance**, puis cliquez sur **Diagnostics**.
2. Dans la section **Packages de diagnostic**, sous **Créer un package**, dans la liste déroulante **Inclure des espaces de travail pour**, sélectionnez un utilisateur dont les espaces de travail seront copiés dans les diagnostics.

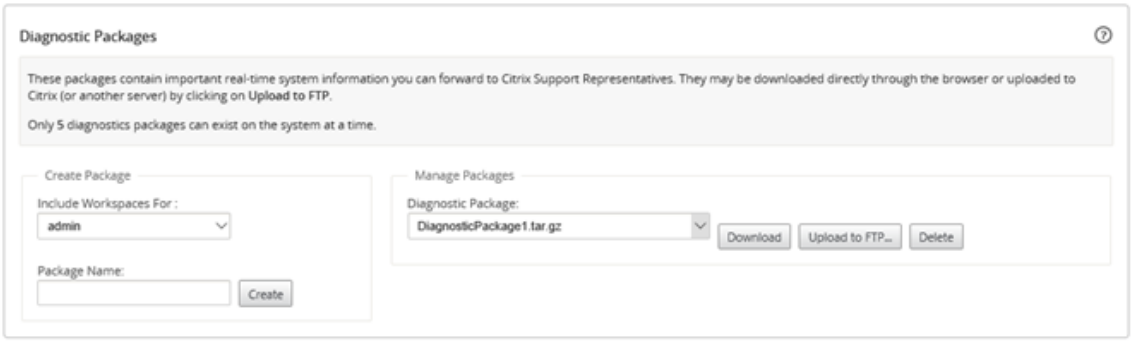
   > **Remarque**
   >
   > Le package de diagnostics inclura les cinq configurations les plus récentes modifiées par l'utilisateur sélectionné.



3. Dans le champ **Nom du package**, entrez un nom pour le package de diagnostic.
4. Cliquez sur **Créer**. Cela exécute un diagnostic système et génère un package de diagnostic.

Pour télécharger un package de diagnostic :

1. Dans la section **Packages de diagnostic**, sous **Gérer le package**, dans la liste déroulante **Packages de diagnostic**, sélectionnez le package à télécharger.



2. Cliquez sur **Download (Télécharger)**. Le package de diagnostic est téléchargé sur votre ordinateur local.

Pour télécharger un package de diagnostic sur un serveur FTP :

1. Dans la section **Packages de diagnostic**, sous **Gérer le package**, dans la liste déroulante **Packages de diagnostic**, sélectionnez un package à télécharger.
2. Cliquez sur **Télécharger vers FTP**. Cela ouvre la boîte de dialogue **Charger vers le serveur FTP** qui vous permet de spécifier vos informations d'authentification FTP et de charger le package sur le serveur FTP du support client Citrix ou sur un autre hôte FTP.

3. Dans le champ **Nom du client**, entrez un nom pour aider Citrix SD-WAN Support à identifier les packages de diagnostic.
   Un répertoire portant ce nom sera créé sur le serveur FTP Citrix et vos fichiers seront téléchargés à cet emplacement.

4. Dans le champ **Hôte FTP**, entrez l'adresse IP ou le nom d'hôte (si DNS est configuré) du serveur FTP.
5. Dans le champ **Nom d'utilisateur**, entrez un nom d'utilisateur à utiliser pour se connecter au serveur FTP.
6. Dans le champ **Mot de passe**, entrez le mot de passe associé au nom d'utilisateur.
7. Cliquez sur **Charger**.

> **Remarque**
>
> Il est recommandé de supprimer périodiquement les anciens paquets de diagnostic, afin d'éviter de dépasser la limite pour les paquets maximaux autorisés. Pour supprimer un package de diagnostic existant, sélectionnez un package de diagnostic dans la liste déroulante **Package de diagnostic**, puis cliquez sur **Supprimer** .

Événements

February 17, 2022

Citrix SD-WAN Center collecte des informations sur les événements à partir de toutes les appliances détectées dans le réseau. Ces informations d'événement peuvent être filtrées et affichées dans la page **Observateur d'événements**.

Les détails de l'événement comprennent les informations suivantes.

- **Heure :** heure à laquelle l'événement a été généré.
- **Site :** Nom du site d'origine de l'événement.
- **ID de l'appliance :** indique si l'appliance d'origine de l'événement est une solution matérielle-logicielle principale (**0**) ou secondaire (**1**).

  > **Remarque**
  >
  > La colonne ID de l'appliance est masquée par défaut. Pour afficher la colonne, cliquez sur **Afficher/Masquer** (icône d'engrenage) et cochez la case **ID du matériel** dans le menu déroulant

- **Nom de l'objet :** nom de l'objet générant l'événement.
- **Type d'objet :** type d'objet générant l'événement.
- **Gravité :** Niveau de gravité de l'événement.

- **État précédent :** état de l'objet avant l'événement. L'état sera répertorié comme **inconnu** s'il n'est pas applicable.
- **État actuel :** état de l'objet au moment de l'événement.
- **Description : description** textuelle de l'événement.

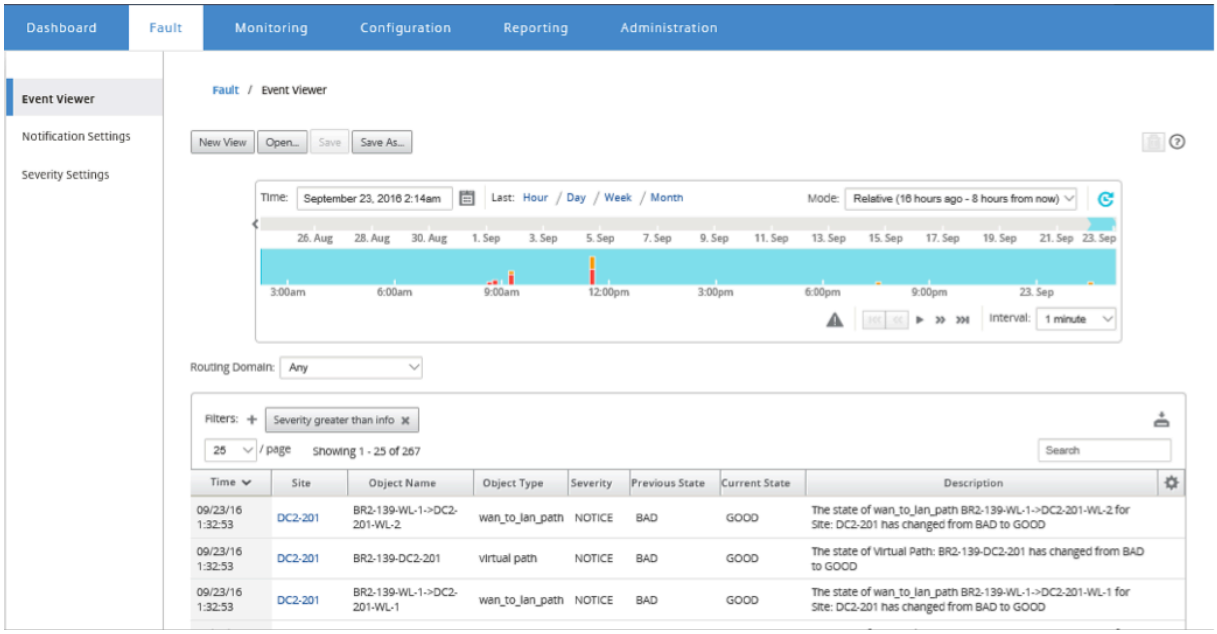
Affichage des événements

Vous pouvez afficher les événements, les filtrer et les télécharger à partir de la page Observateur d'événements.

Pour accéder à la page de l'Observateur d'événements.

Dans l'interface Web Citrix SD-WAN Center, cliquez sur l'onglet **Fault**.

La page Observateur d'événements s'affiche par défaut.



Vous pouvez sélectionner et afficher des rapports d'une période donnée à l'aide des contrôles de chronologie. Pour plus d'informations, reportez-vous à la section Contrôles du scénario.

> **Remarque**
>
> Vous pouvez afficher les données des événements des 30 derniers jours. Toutes les données au-delà de cette période sont automatiquement supprimées du collecteur de SD-WAN Center et des collecteurs régionaux respectifs.

Vous pouvez également créer, enregistrer et ouvrir des vues de rapport. Pour plus d'informations, reportez-vous à la section Gérer les vues.

Utilisation des filtres

Vous pouvez créer des filtres personnalisés pour réduire les résultats de la table Événements.

Pour créer et appliquer un filtre :

1. Cliquez sur l'icône **+** à droite de l'étiquette de la section **Filtres**.
2. Sélectionnez une catégorie dans le menu déroulant.

   Les options disponibles sont les suivantes :

   - Taille
   - Nom d'objet
   - Type d'objet
   - Gravité
   - État précédent
   - État actuel

3. Sélectionnez un opérateur dans le menu déroulant du milieu.

   Les options sont les suivantes :

   - is
   - n'est pas
   - est l'un des
   - contient
   - ne contient pas
   - inférieur à
   - inférieur ou égal à
   - supérieur à
   - supérieure ou égale à

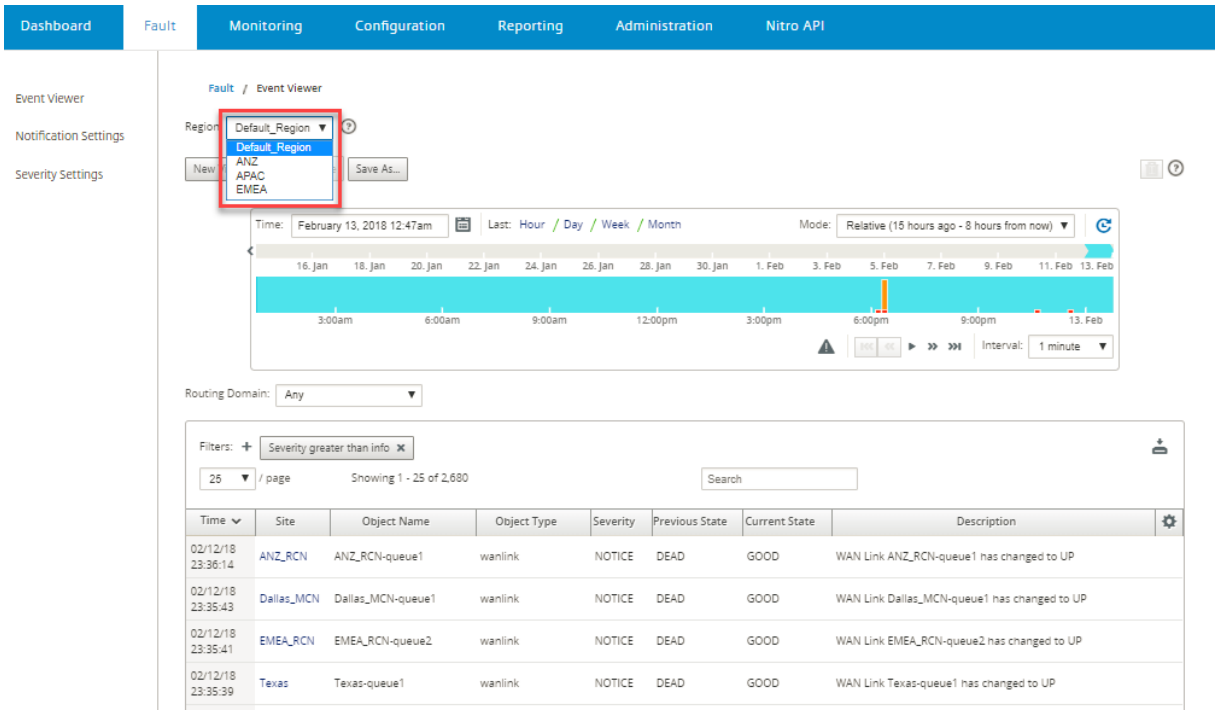
4. Entrez la chaîne ou la valeur par laquelle délimiter le filtre.

> **Remarque**
>
> Ce champ est sensible à la casse.

> **Remarque**
>
> Vous pouvez créer et appliquer plusieurs filtres.
> Pour le réseau multi-région, vous pouvez sélectionner des régions spécifiques pour afficher l'

> événement.

Les données d'événements sont récupérées à partir du collecteur de la région respective.



> **Remarque**
>
> Dans le déploiement réseau d'une seule **région, la liste déroulante Région** n'est pas disponible.

Pour télécharger la table des événements en tant que fichier CSV :

Cliquez sur l'icône Télécharger dans le coin supérieur droit de la table des événements.

Pour plus d'informations sur les statistiques des événements, voir Rapport d'événements.

Vous pouvez configurer Citrix SD-WAN Center pour envoyer des notifications d'événements externes pour différents types d'événements sous forme de courrier électronique, d'interruptions SNMP ou de messages syslog. Pour plus d'informations, consultez Notifications d'événements.

Notifications d'événements

February 17, 2022

Vous pouvez configurer Citrix SD-WAN Center pour envoyer des notifications d'événements pour différents types d'événements sous forme de courrier électronique, d'interruptions SNMP ou de messages syslog. Une fois que vous avez configuré les paramètres de notification e-mail, SNMP et syslog,

vous pouvez sélectionner la gravité des différents types d'événements et sélectionner le mode (e-mail, SNMP, syslog) pour envoyer des notifications d'événement. Les notifications sont générées pour les événements égaux ou supérieurs au niveau de gravité spécifié pour le type d'événement.

Les niveaux de gravité disponibles sont les suivants, par ordre décroissant de gravité :

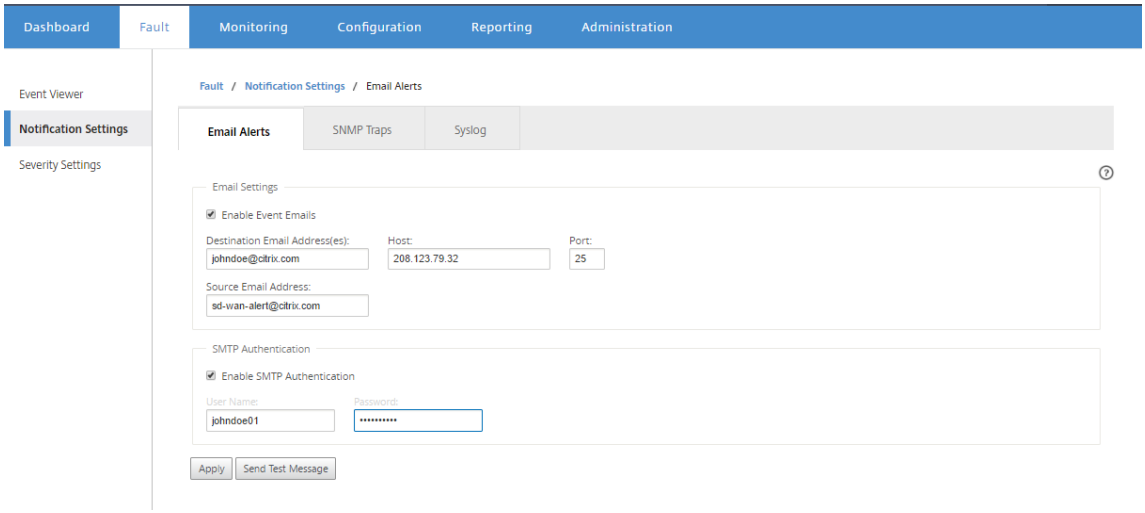
- URGENCE
- ALERTE
- CRITIQUE
- ERROR
- AVERTISSEMENT
- REMARQUE
- INFORMATIONNEL
- DEBUG

> **Conseil**
>
> Vous pouvez configurer les paramètres de notification pour recevoir des alertes d'événements par e-mail, des interruptions SNMP ou des messages Syslog sur Citrix SD-WAN Center et sur les appliances Citrix SD-WAN individuelles de votre réseau.
>
> Toutefois, l'activation des notifications sur Citrix SD-WAN Center vous permet de recevoir des notifications d'événements pour l'ensemble du réseau Citrix SD-WAN (c'est-à-dire MCN et tous les sites). Alors que l'activation des notifications sur les appliances Citrix SD-WAN vous permet de recevoir des notifications de la part des appliances individuelles uniquement.
>
> Il est conseillé d'activer les notifications sur le Centre Citrix SD-WAN uniquement, afin d'éviter les notifications redondantes des autres appliances Citrix SD-WAN de votre réseau.

Configuration des paramètres de notification par e-mail

Pour configurer les paramètres de notification par e-mail :

1. Dans l'interface de gestion Web Citrix SD-WAN Center, accédez à **Défaillance** > **Paramètres de notification** > **Alertes par e-mail.**



2. Sélectionnez **Activer les e-mails d'événements**.
3. Dans le champ **Adresse e-mail de destination**, entrez l'adresse e-mail à laquelle les notifications d'alerte doivent être envoyées.

   > **Remarque**
   >
   > Vous pouvez saisir plusieurs adresses e-mail séparées par des points-virgules.

4. Dans le champ **Hôte**, entrez l'adresse IP ou le nom d'hôte d'un serveur SMTP externe pour relayer les messages électroniques vers Internet.
5. Dans le champ **Port**, entrez le numéro de port à utiliser pour la connexion SMTP. Le port par défaut est 25.
6. Dans le champ **Adresse e-mail source**, entrez l'adresse e-mail à partir de laquelle les alertes sont envoyées.
7. Sélectionnez **Activer** l'**authentification SMTP**.
8. Dans le champ **Nom d'utilisateur**, entrez un nom d'utilisateur pour le serveur SMTP utilisé pour l'authentification.
9. Dans le champ **Mot** de passe, entrez le mot de passe associé au nom d'utilisateur du serveur SMTP utilisé pour l'authentification.

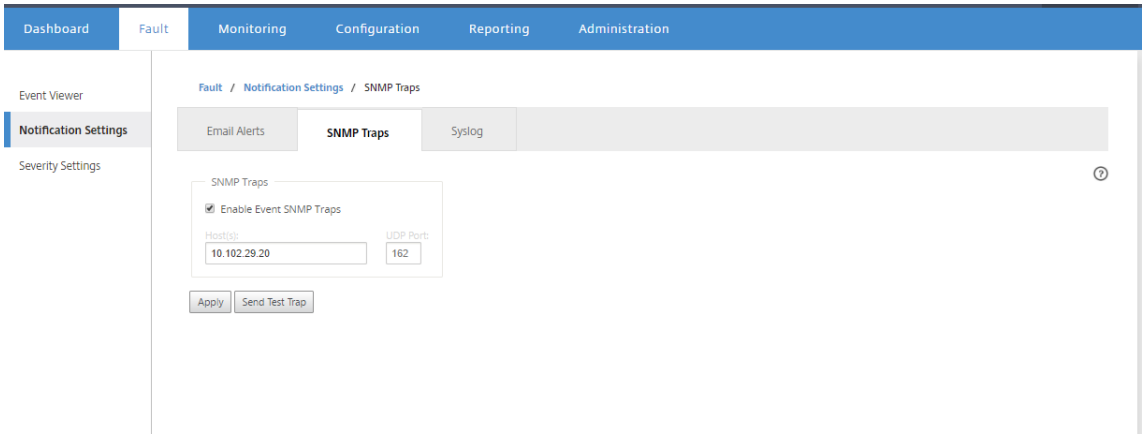
   > **Remarque**
   >
   > Cliquez sur **Envoyer un message de test** pour envoyer un exemple d'alerte par e-mail aux destinataires configurés.

10. Cliquez sur **Apply**.

Configuration des paramètres de notification d'interruption SNMP

Pour configurer les paramètres de notification d'interruption SNMP :

1. Dans l'interface de gestion Web Citrix SD-WAN Center, accédez à **Défaillance** > **Paramètres de notification** > **Interruptions SNMP**.
2. Sélectionnez **Activer les interruptions SNMP d'événement.**



3. Dans le champ **Hôte (s)**, entrez l'adresse IP ou le nom d'hôte d'un système SNMP externe. Cet hôte recevra les événements sous forme d'interruptions SNMP.

> **Remarque**
>
> Vous pouvez saisir plusieurs adresses IP ou noms d'hôte séparés par des points-virgules.

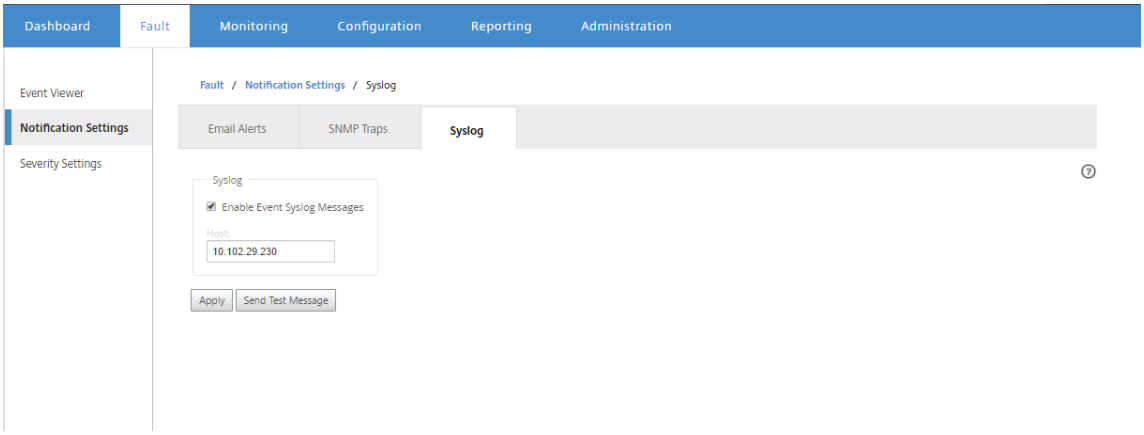
4. Dans le champ **Port UDP**, entrez le port UDP à utiliser pour envoyer les interruptions SNMP. Par défaut, le port UDP est défini sur 162.
5. Cliquez sur **Appliquer** pour appliquer les paramètres de notification des interruptions SNMP.

> **Remarque**
>
> Vous pouvez également cliquer sur **Envoyer une interruption de test** pour vérifier si le système est en mesure d'envoyer une interruption SNMP à la destination configurée.

Configuration des paramètres de notification syslog

Pour configurer les paramètres de notification Syslog :

1. Dans l'interface de gestion Web Citrix SD-WAN Center, accédez à **Fault** > **Paramètres de notification** > **Syslog**.
2. Sélectionnez **Activer les messages Syslog d'événement.**



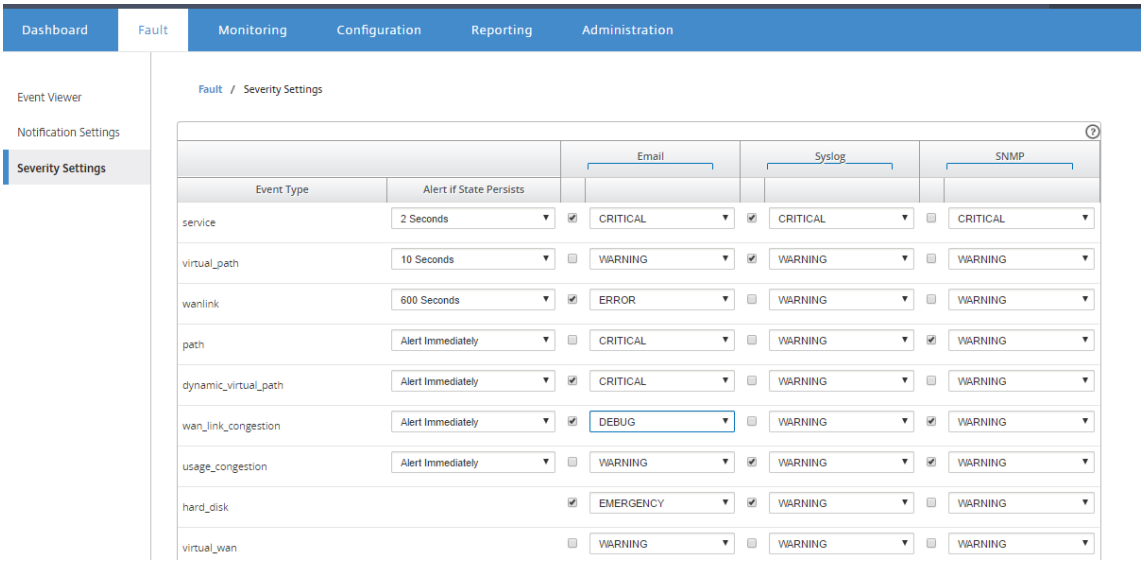
3. Dans le champ **Hôte**, entrez l'adresse IP ou le nom d'hôte d'un serveur syslog externe, qui sera utilisé pour recevoir des événements sous forme de messages syslog.
4. Cliquez sur **Appliquer** pour appliquer les paramètres de notification syslog.

> **Remarque**
>
> Vous pouvez également cliquer sur **Envoyer un message de test** pour vérifier si le système peut envoyer un message syslog à l'hôte configuré.

Configuration des notifications d'événement

Pour configurer les notifications d'événement :

1. Dans l'interface de gestion Web Citrix SD-WAN Center, accédez à **Fault** > **Paramètres de gravité**.
2. Dans le champ **Alerte si Sate persists**, sélectionnez la durée après laquelle, si l'événement persiste encore, une notification sera envoyée.



3. Pour chaque type d'événement, sélectionnez l'option de notification et sélectionnez la gravité.

> **Remarque**
>
> Les options de notification par e-mail, Syslog et SNMP ne seront activées qu'après avoir configuré les paramètres de notification respectifs.

4. Cliquez sur **Apply**.

Configuration des alarmes

Vous pouvez également configurer des alarmes dans Citrix SD-WAN Center et les transmettre à des appliances individuelles.

Pour configurer l'alarme dans Citrix SD-WAN Center, accédez à **Configuration** > Paramètres de l'**appliance > Paramètres** de **notification** > **Configuration d'alarme**, puis cliquez sur **+**.

Sélectionnez ou entrez des valeurs pour les champs suivants :

- **Type d'événement** : L'appliance Citrix SD-WAN peut déclencher des alarmes pour des sous-systèmes ou des objets particuliers du réseau, appelés types d'événements. Les types d'événements disponibles sont SERVICE, VIRTUAL_PATH, WANLINK, PATH, DYNAMIC_VIRTUAL_PATH, WAN_LINK_CONGESTION, USAGE_CONGESTION, FAN, POWER_SUPPLY, PROXY_ARP, ETHERNET, DISCOVERED_MTU, GRE_TUNNEL et IPSEC_TUNNEL.
- **État du déclencheur :** état de l'événement qui déclenche une alarme pour un type d'événement. Les options d'état de déclenchement disponibles dépendent du type d'événement choisi.
- **Durée du déclenchement** : Durée en secondes, qui détermine la rapidité avec laquelle l'appliance déclenche une alarme. Entrez « 0 » pour recevoir des alertes immédiates ou entrez une valeur comprise entre 15 et 7200 secondes.Les alarmes ne sont pas déclenchées si des événements supplémentaires se produisent sur le même objet pendant la période de durée du déclenchement. Les alarmes supplémentaires ne sont déclenchées que si un événement persiste plus longtemps que la durée du déclenchement.
- **État d'effacer** : état d'événement qui efface une alarme pour un type d'événement après le déclenchement de l'alarme. Les options d'effacement disponibles dépendent de l'état de déclenchement choisi.

- **Effacer la durée :** la durée en secondes, ce qui détermine la durée d'attente avant d'effacer une alarme.Entrez « 0 » pour effacer immédiatement l'alarme ou entrer une valeur comprise entre 15 et 7200 secondes. L'alarme n'est pas effacée si un autre événement d'état clair se produit sur le même objet dans le délai spécifié.
- **Gravité** : champ défini par l'utilisateur qui détermine l'urgence d'une alarme. La gravité est affichée dans les alertes envoyées lorsque l'alarme est déclenchée ou effacée et dans le récapitulatif de l'alarme déclenchée.
- **E-mail** : Les alertes de déclenchement d'alarme et d'effacer les alertes pour le type d'événement sont envoyées par e-mail.
- **Syslog** : les alertes de déclenchement d'alarme et d'effacer le type d'événement sont envoyées via Syslog.
- **SNMP** : le déclencheur d'alarme et les alertes effacées pour le type d'événement sont envoyées via l'interception SNMP.

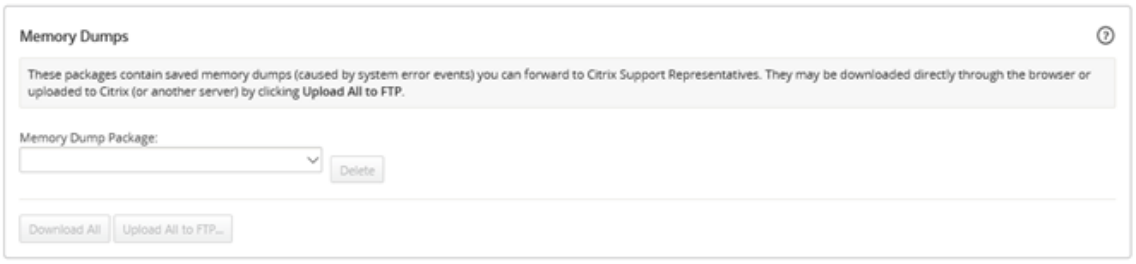
Images mémoire

February 17, 2022

Un vidage de mémoire est généré lorsqu'un processus se bloque. Tous les vidages de mémoire actuellement sur le système peuvent être téléchargés dans un package combiné et téléchargés sur un serveur FTP pour examen par l'équipe de support Citrix. Toutefois, vous pouvez supprimer des vidages de mémoire individuels.

Pour télécharger des vidages de mémoire :

1. Dans l'interface Web Citrix SD-WAN Center, cliquez sur l'onglet **Surveillance**, puis cliquez sur **Diagnostics** .
2. Dans la section **vidages de mémoire**, dans la liste déroulante **Package de vidage** de mémoire, sélectionnez un package de vidage mémoire.



3. Cliquez sur **Télécharger tout**. Enregistrez le package de vidage mémoire sur votre ordinateur local.

Pour télécharger un package de vidage mémoire sur un serveur FTP :

1. Dans la section **vidages de mémoire**, dans la liste déroulante **Package de vidage** de mémoire, sélectionnez un package de vidage mémoire.
2. Cliquez sur **Télécharger sur le serveur FTP**. Cela ouvre la boîte de dialogue **Tout télécharger vers FTP** pour spécifier vos informations d'authentification FTP et charger le package sur le serveur FTP du support client Citrix ou sur un autre hôte FTP.

3. Dans le champ **Nom du client**, entrez un nom pour aider Citrix SD-WAN Support à identifier les packages de diagnostic.

   Un répertoire portant ce nom sera créé sur le serveur FTP Citrix et vos fichiers seront téléchargés à cet emplacement.
4. Dans le champ **Hôte FTP**, entrez l'adresse IP ou le nom d'hôte (si DNS est configuré) du serveur FTP.
5. Dans le champ **Nom d'** utilisateur, entrez un nom d'utilisateur à utiliser pour se connecter au serveur FTP.
6. Dans le champ **Mot de passe**, entrez le mot de passe associé au nom d'utilisateur.
7. Cliquez sur **Charger**.

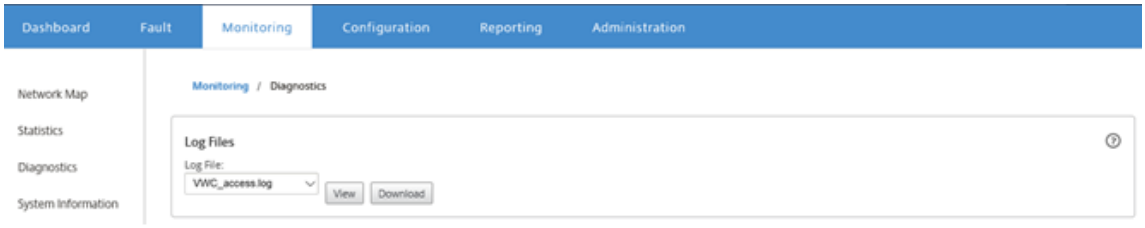
Fichiers journaux

February 17, 2022

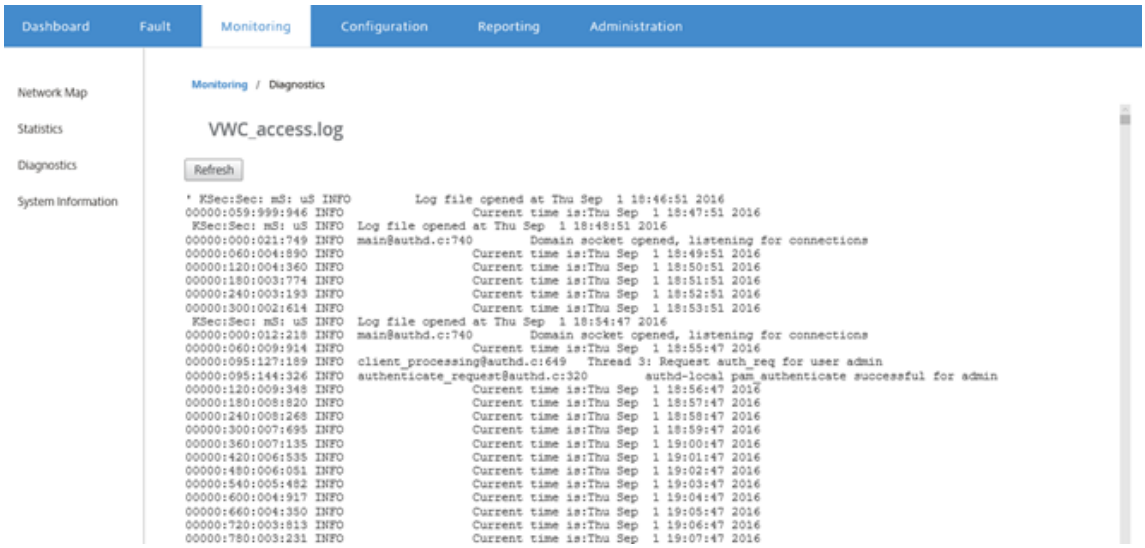
Les fichiers journaux collectent des informations relatives à la console Web, aux exceptions de l'interface utilisateur, aux plantages internes, etc. Ces journaux peuvent être utilisés pour résoudre les problèmes dans le Centre Citrix SD-WAN.

Pour afficher les fichiers journaux :

1. Dans l'interface Web Citrix SD-WAN Center, cliquez sur l'onglet **Surveillance**.
2. Cliquez sur **Diagnostics**.
3. Dans la liste déroulante **Fichier journal**, sélectionnez le fichier journal à afficher.



4. Cliquez sur **Afficher**. Le contenu du fichier journal s'affiche.



5. Si vous souhaitez télécharger les fichiers journaux sur votre ordinateur, cliquez sur **Télécharger**.

Intervalle d'interrogation

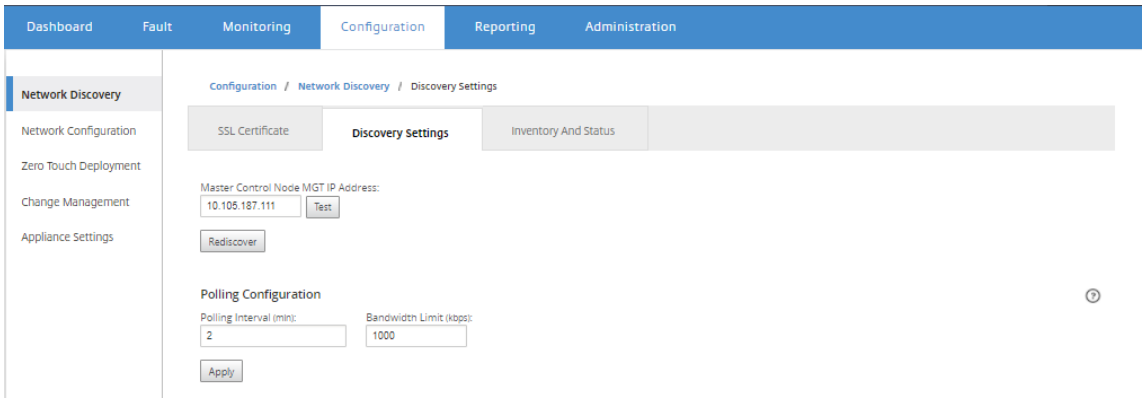
February 17, 2022

L'interrogation fait référence au processus de collecte de statistiques à partir de l'appliance découverte. Vous pouvez configurer l'intervalle et la limite de bande passante pour les opérations d'interrogation après avoir découvert les appliances. Pour plus d'informations sur la découverte de l'

appliance, reportez-vous à la section Déploiement réseau à région unique ou Déploiement réseau multirégional.

Pour effectuer la configuration d'interrogation :

1. Dans l'interface Web Citrix SD-WAN Center, accédez à **Configuration** > **Découverte du réseau** > **Paramètres de découverte** .



2. Dans le champ **Intervalle d'interrogation**, entrez la fréquence d'interrogation en minutes. La portée est de 2 à 60 minutes. La valeur par défaut est de 5 minutes.
3. Dans le champ **Limite de bande passante**, entrez la limite de bande passante d'interrogation en kbps. Le MCN limite la bande passante à la valeur spécifiée lors du transfert des statistiques d'interrogation de l'appliance vers Citrix SD-WAN Center. La gamme est de 100 Kbp —1 Gbps. La valeur par défaut est 1 Mbps.
4. Cliquez sur **Apply**.

Statistiques

February 17, 2022

Vous pouvez afficher les statistiques collectées par Citrix SD-WAN Center 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. Pour chaque site du réseau SD-WAN, vous pouvez afficher des graphiques pour les paramètres réseau suivants :

- Bande passante
- QoS
- Chemin virtuel
- Services Internet

- Services Intranet
- Services de pass-through
- Liens WAN
- Interfaces Ethernet
- Tunnels GRE
- Tunnels IPSec
- Applications
- Familles d'applications

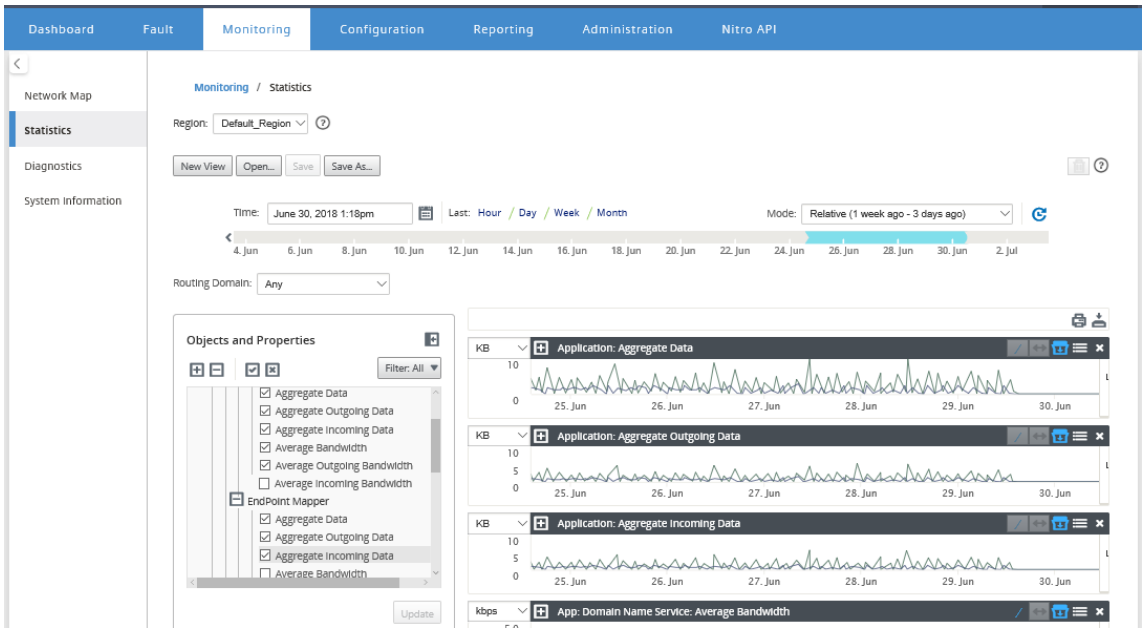
> **Conseil**
>
> Vous pouvez créer des vues selon vos besoins, les enregistrer et ouvrir des vues existantes.

Pour afficher les graphiques statistiques :

1. Dans l'interface utilisateur Web Citrix SD-WAN Center, accédez à **Surveillance** > **Statistiques**.
2. Sélectionnez une région et un domaine de routage.
3. Dans l'arborescence hiérarchique **Objets et propriétés**, recherchez et sélectionnez les propriétés qui vous intéressent.

   > **Conseil**
   >
   > Vous pouvez également utiliser le menu déroulant **Filtre** et le Menu **Préréglages** pour simplifier le processus de recherche et de sélection des propriétés.

4. Cliquez sur **Mettre à jour** pour afficher les graphiques des propriétés sélectionnées.

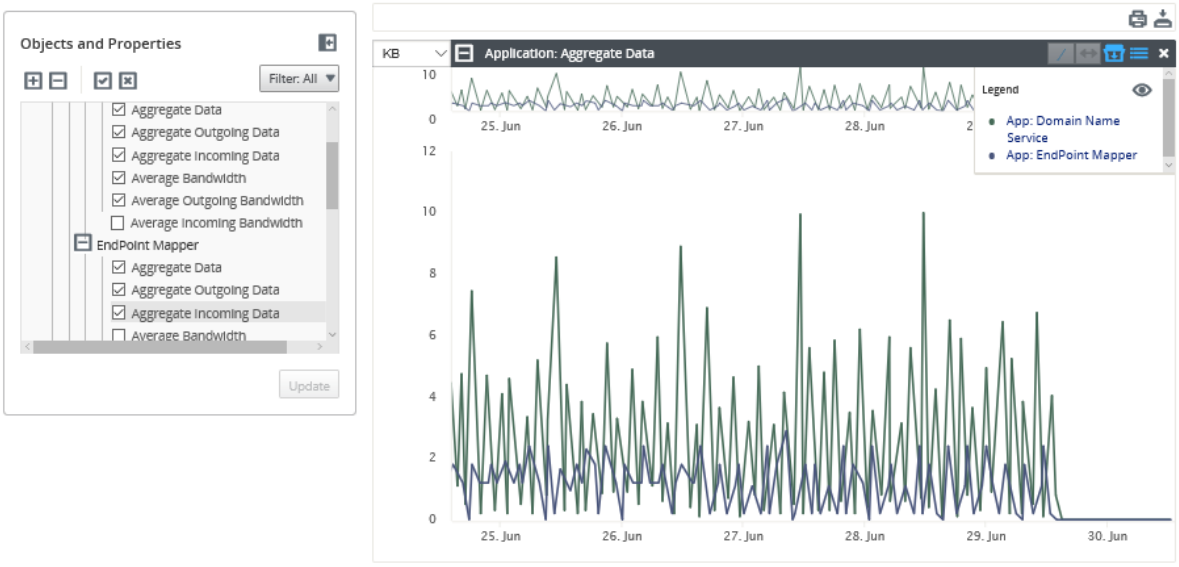


> **Conseil**
>
> Désélectionnez une propriété et cliquez sur **Mettre à jour** pour supprimer le graphique de cette propriété de la zone d'affichage des graphiques.

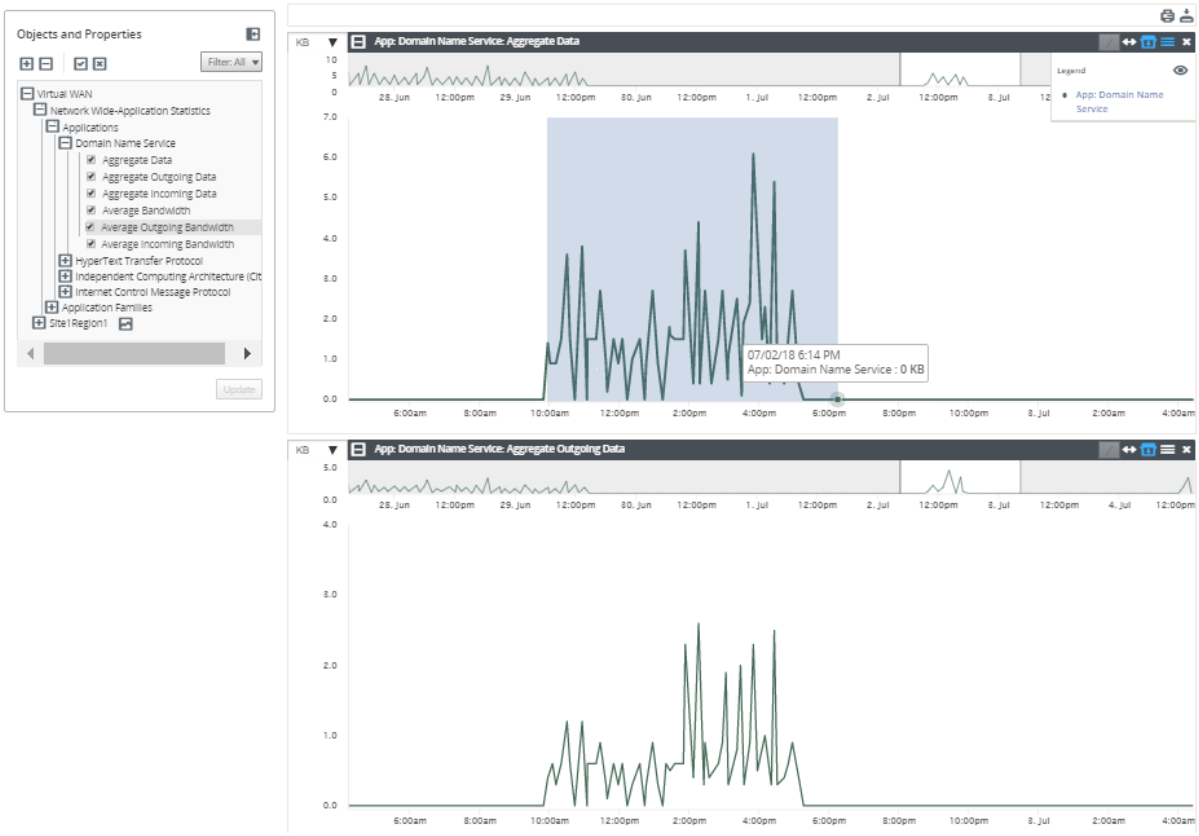
5. Sélectionnez une période pour la vue actuelle. Pour plus d'informations, voir Commandes de la chronologie

   Les graphiques sont affichés en fonction des propriétés sélectionnées.

> **Conseil**
>
> Si vous sélectionnez plusieurs propriétés, les graphiques s'affichent en mode **Tendance View** pour économiser de l'espace vertical. Cliquez sur un en-tête du graphique pour afficher et masquer le graphique complètement développé. Vous pouvez également afficher et masquer la vue de tendance et les légendes sur les graphiques.

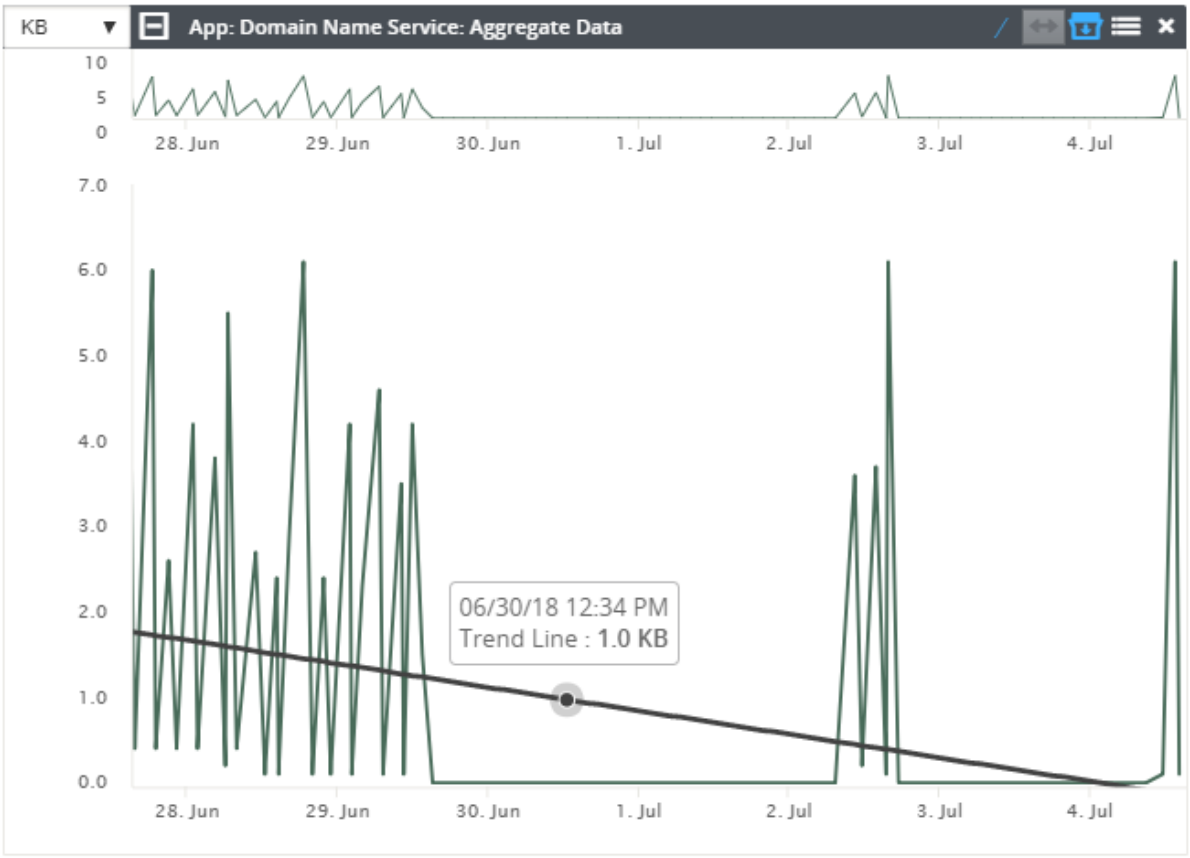


> **Conseil**
>
> Pour zoomer un graphique, cliquez et faites-le glisser sur la zone de tracé du graphique. Le zoom sur un graphique permet d'effectuer un zoom sur tous les graphiques, jusqu'à l'heure sélectionnée, afin de conserver une vue cohérente. Cliquez sur l'icône de réinitialisation (↔) pour réinitialiser le zoom.



Conseil

Vous pouvez afficher et masquer la ligne de tendance en cliquant sur l'icône (/).



> **Remarque**
>
> Vous pouvez imprimer les graphiques ou télécharger le jeu de graphiques en tant que fichier CSV.

Informations système

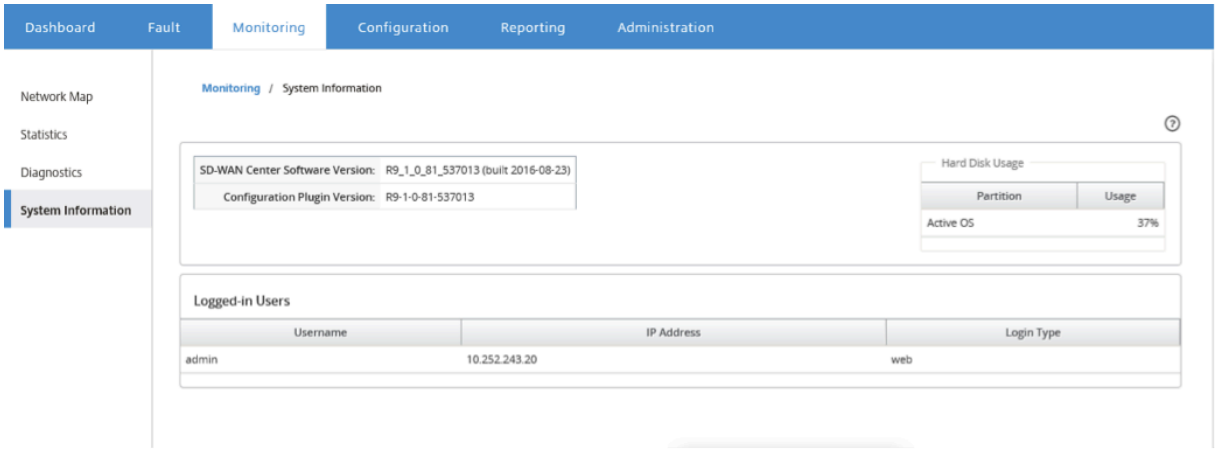
February 17, 2022

Les informations suivantes sont affichées sur la page d'informations système :

- Version**du logiciel Citrix SD-WAN Center : La version**du logiciel Citrix SD-WAN Center actuellement installée et exécutée sur cette machine virtuelle.
- **Version du plugin de configuration** : Version du plugin de l'éditeur de configuration actuellement installé et en cours d'exécution dans cette machine virtuelle Citrix SD-WAN Center.
- **Utilisation du disque dur** : quantité d'espace disque utilisée par le système d'exploitation et les partitions de données.
- **Utilisateurs connectés** : nom d'utilisateur, adresse IP et type d'ouverture de session pour chaque utilisateur actuellement connecté à cette machine virtuelle Citrix SD-WAN Center.

Pour afficher les informations système :

Dans l'interface Web Citrix SD-WAN Center, cliquez sur l'onglet **Surveillance**, puis cliquez sur **Informations système** .



Rapports

February 17, 2022

Citrix SD-WAN Center fournit les rapports suivants :

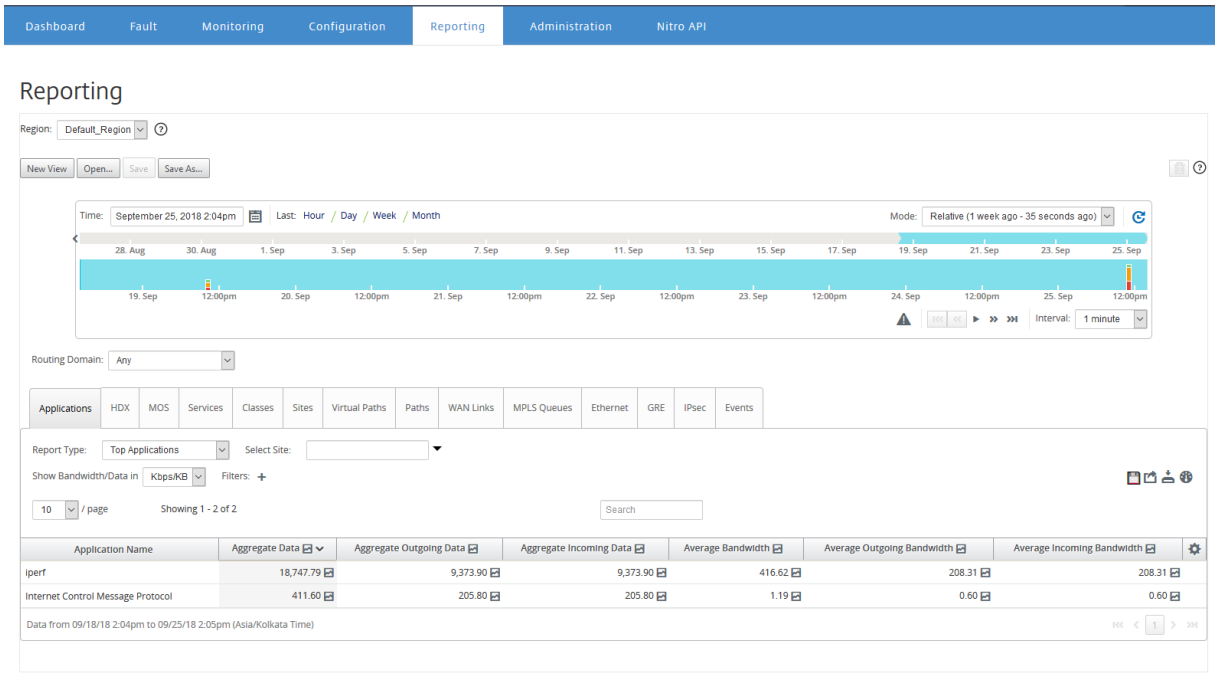
- **Applications :** affiche des détails sur le trafic entrant, le trafic sortant et le trafic total des applications, des sites et des familles d'applications les plus populaires.
- **HDX** : Affiche les données HDX détaillées pour chaque site.
- **Sites :** affiche les statistiques au niveau du site pour chaque site du réseau étendu virtuel. Les lignes Sites se développent pour afficher la table **Services** filtrée pour le site.
- **Service :** affiche des statistiques récapitulatives par type de service (chemin virtuel, Internet, Intranet et Pass-through) pour chaque site du réseau étendu virtuel. Les lignes Services se développent pour afficher les services individuels pour le type de service.
- **Chemins virtuels :** affiche les statistiques de niveau Chemin virtuel pour chaque chemin virtuel dans le SD-WAN. Les lignes Chemins virtuels se développent pour afficher les chemins contenus dans le chemin virtuel.

> **Remarque**
>
> Les données de chemin virtuel sont enregistrées du point de vue des deux points de terminaison, en tant que tels, chaque chemin virtuel peut avoir deux lignes identifiées par le site qui a enregistré les statistiques.

- **Chemins :** affiche les statistiques de niveau de chemin pour chaque chemin d'accès dans le WAN virtuel.

- **Liens WAN :** affiche les statistiques de niveau de liaison WAN pour chaque lien WAN sur chaque site du réseau étendu virtuel. Les lignes de liens WAN se développent pour afficher un récapitulatif d'utilisation pour chaque type de service pour cette liaison WAN. Chaque ligne de type de service sera ensuite développée pour afficher les utilisations de chaque service de ce type. Si la liaison WAN est une liaison MPLS privée, un deuxième tableau affiche les files d'attente MPLS pour la liaison WAN.
- **Files d'attente MPLS :** les lignes Files d'attente MPLS se développent pour afficher un récapitulatif de l'utilisation de chaque type de service pour cette file d'attente. Chaque ligne de type de service sera ensuite développée pour afficher les utilisations de chaque service de ce type.
- **Classes :** affiche les statistiques de niveau de classe pour chaque classe pour chaque chemin virtuel dans le WAN virtuel.
- **Score MOS** : Le score d'opinion moyen (MOS) fournit une mesure numérique de la qualité de l'expérience qu'une application fournit aux utilisateurs finaux.
- **Interfaces Ethernet :** affiche les statistiques de niveau d'interface Ethernet pour chaque interface de chaque site dans le WAN virtuel.
- **Tunnels GRE :** affiche les statistiques de chaque tunnel LAN GRE sur chaque site du WAN.
- **Tunnels IPSec :** affiche les statistiques de chaque tunnel de sécurité IP sur chaque site du WAN.
- **Événements :** affiche les comptes récapitulatifs des événements se produisant sur chaque site dans le réseau étendu virtuel. **Les lignes Événements** se développent pour afficher les comptes récapitulatifs par type d'objet pour ce site. Chaque Type d'objet se développera ensuite pour afficher les comptes récapitulatifs pour chaque objet de ce type.

Sous l'onglet **Rapports** de l'interface Web Citrix SD-WAN Center, vous pouvez afficher tous les rapports ou les rapports sélectionnés. Vous pouvez également télécharger des rapports.

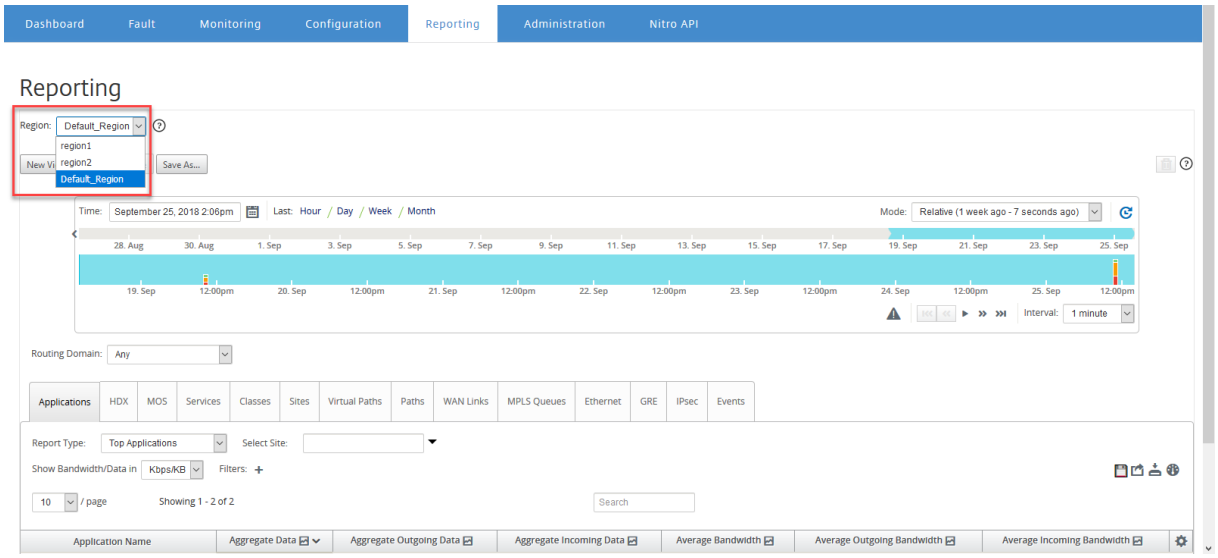


Vous pouvez sélectionner et afficher les rapports d'une période donnée à l'aide des contrôles de chronologie. Pour plus d'informations, reportez-vous à la section Contrôles du scénario.

Vous pouvez également créer, enregistrer et ouvrir des vues de rapport. Pour plus d'informations, reportez-vous à la section Gérer les vues.

Pour le réseau multirégion, vous pouvez sélectionner des régions spécifiques pour afficher les rapports statistiques.

Les données des rapports sont récupérées à partir du collecteur de la région concernée.



> **Remarque**
>
> Dans le déploiement réseau d'une seule **région, la liste déroulante Région** n'est pas disponible.

Pour plus d'informations sur l'affichage des différents rapports, consultez les rubriques suivantes :

Rapport d'application

Rapport sur la bande passante

Rapport de classe

Rapport sur l'interface Ethernet

Rapport d'événement

Rapport sur les tunnels GRE

Rapport HDX

Rapport de tunnel IPSec

Rapport sur les performances des liens

MOS pour applications

Rapport sur les files d'attente MPLS

Rapport d'application

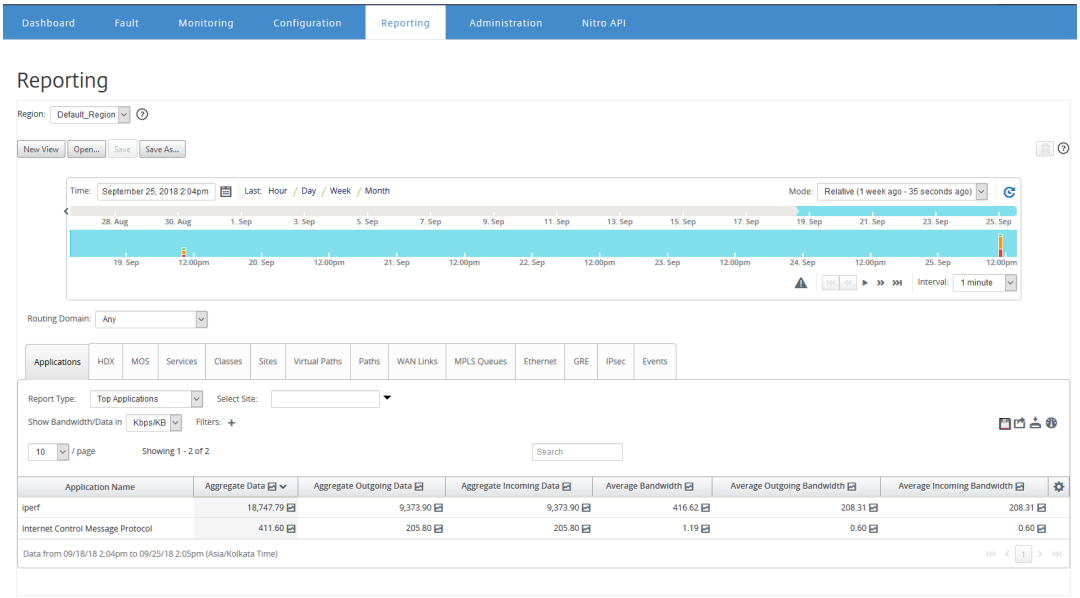
February 17, 2022

L'inspection approfondie des paquets (DPI) permet à l'appliance SD-WAN d'analyser le trafic qui le traverse et d'identifier les types d'application et de famille d'applications. L'appliance Citrix SD-WAN enregistre le nombre d'octets et la bande passante du trafic entrant et sortant de chaque application. Le SD-WAN Center interroge l'appliance SD-WAN à l'intervalle d'interrogation défini, obtient ces données et les affiche sur le tableau de bord et sous forme de rapports.

Vous pouvez afficher les principales applications, les sites les plus importants et les rapports sur les familles d'applications les plus populaires. Ces rapports fournissent des détails sur les données totales, entrantes et sortantes et la bande passante.

Pour afficher les rapports d'application dans Citrix SD-WAN Center :

1. Dans l'interface utilisateur Web Citrix SD-WAN Center, accédez à **Reporting** > **Applications**.
2. Dans le champ Ligne de temps, sélectionnez l'intervalle de temps. Pour plus d'informations, reportez-vous à la section Contrôles du scénario
3. Sélectionnez l'unité pour afficher les données. Vous pouvez choisir d'afficher les données de rapport en unités de Kbits/s, Mbps ou Gbit/s.
4. Dans la liste déroulante **Type de rapport**, sélectionnez l'un des types de rapports suivants :
    - **Applications les**plus populaires : Applications les plus utilisées dans le réseau pour l'intervalle de temps sélectionné. Vous pouvez filtrer l'application supérieure par nom de site. Par défaut, les applications les plus hautes pour tous les sites sont affichées.
    - **Familles d'applications les**plus populaires : les meilleures familles d'applications utilisées dans le réseau. Vous pouvez filtrer les familles d'applications les plus populaires par nom de site. Par défaut, les familles d'applications les plus populaires pour tous les sites sont affichées.
    - **Sites les plus populaires** : Trafic sur les principaux sites pour l'intervalle de temps sélectionné. Vous pouvez filtrer les principaux sites par nom d'application ou de famille d'application.



Pour chaque type de rapport, vous pouvez afficher les données suivantes :

- **Données entrantes agrégées** : Données d'application entrant sur le site depuis le WAN.
- **Données sortantes agrégées** : Données d'application envoyées du site au WAN.
- **Données agrégées** : Somme du trafic entrant et sortant.
- **Bande passante entrante moyenne** : Bande passante du trafic d'application entrant.
- **Bande passante sortante moyenne** : Bande passante du trafic d'application sortant.
- **Bande passante moyenne** : Bande passante totale consommée par le trafic d'applications entrant et sortant.

> **Conseil**
>
> Pour chaque valeur, vous pouvez placer le curseur de la souris sur l'icône du graphique pour afficher un mini-graphe, ou cliquer pour ouvrir la vue graphique dans une autre fenêtre. Pour plus d'informations, consultez la section Statistiques.

Rapport QoE d'application

February 17, 2022

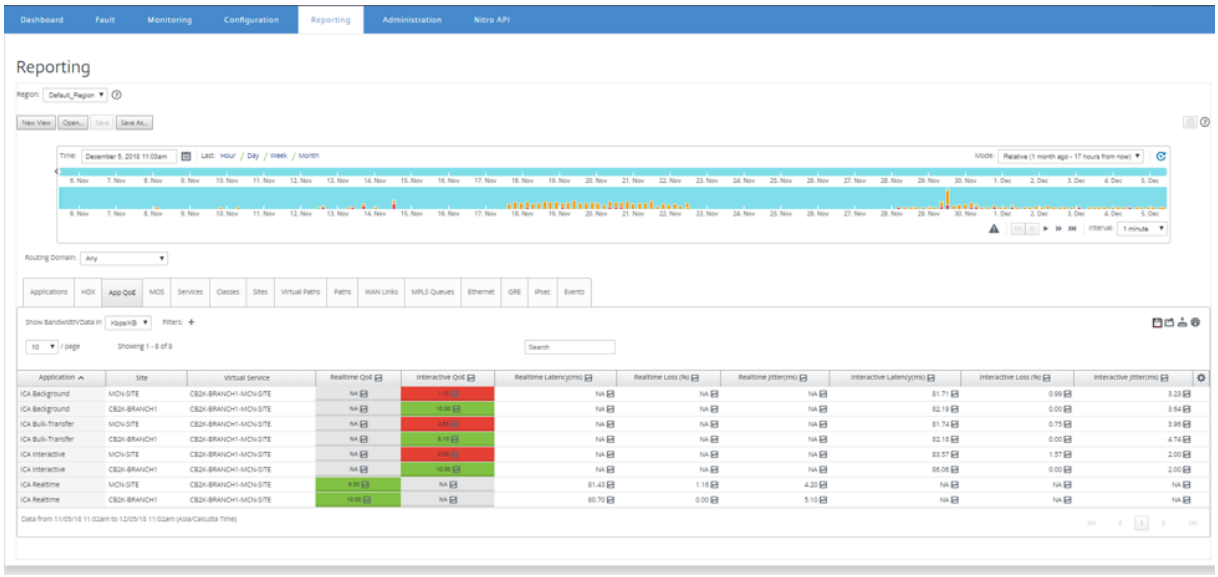
Application QoE est une mesure de la qualité de l'expérience pour une application. La plage de pointage QoE de l'application est de 0 à 10, où 10 représente une excellente qualité et 0 représente une mauvaise qualité. Pour plus d'informations, consultez la section **QoE de l'application**.

Pour afficher le rapport QoE d'application :

Dans Citrix SD-WAN Center, accédez à **Reporting > App QoE**, puis sélectionnez une période dans le contrôle de la chronologie.

Vous pouvez sélectionner et afficher des rapports d'une période donnée à l'aide des contrôles de chronologie. Pour plus d'informations, reportez-vous à la section Contrôles du scénario.

Vous pouvez également créer, enregistrer et ouvrir des vues de rapport. Pour plus d'informations, reportez-vous à la section Gérer les vues.



Vous pouvez afficher les mesures suivantes :

- **Application** : nom de l'objet de l'application ou de l'application.
- **Site** : nom du site.
- **Service virtuel : service**de chemin virtuel utilisé.
- **QoE en temps réel** : le score QoE pour le trafic en temps réel.
- **QoE interactif** : le score QoE pour le trafic interactif.
- **Latence en temps réel** : latence en millisecondes pour le trafic en temps réel.
- **Perte en temps réel** : pourcentage de perte pour le trafic en temps réel.
- **Gigue en temps réel** : La gigue observée en millisecondes pour le trafic en temps réel.
- **Latence interactive** : latence en millisecondes pour le trafic interactif.
- **Perte interactive** : pourcentage de perte pour le trafic interactif.
- **Jitter interactif** : La gigue observée en millisecondes pour le trafic interactif.

> **Conseil**
>
> Pour chaque valeur, vous pouvez placer le curseur de la souris sur l'icône du graphique pour afficher un mini-graphe, ou cliquer pour ouvrir la vue graphique dans une autre fenêtre.

Pour plus d'informations, consultez la section Statistiques.

Rapport sur la bande passante

February 17, 2022

Citrix SD-WAN Center fournit une vue centrale des données statistiques de bande passante interrogées à partir de différents sites de votre réseau SD-WAN.

Dans la configuration Citrix SD-WAN, le trafic circulant à travers les chemins virtuels est classé comme appartenant à des types de classe en temps réel, interactifs ou en vrac. Les classes sont prédéfinies, mais vous pouvez personnaliser ces classes et leur appliquer des règles. Pour plus d'informations, consultez Personnalisation des classes et des règles par adresse IP et numéro de port.

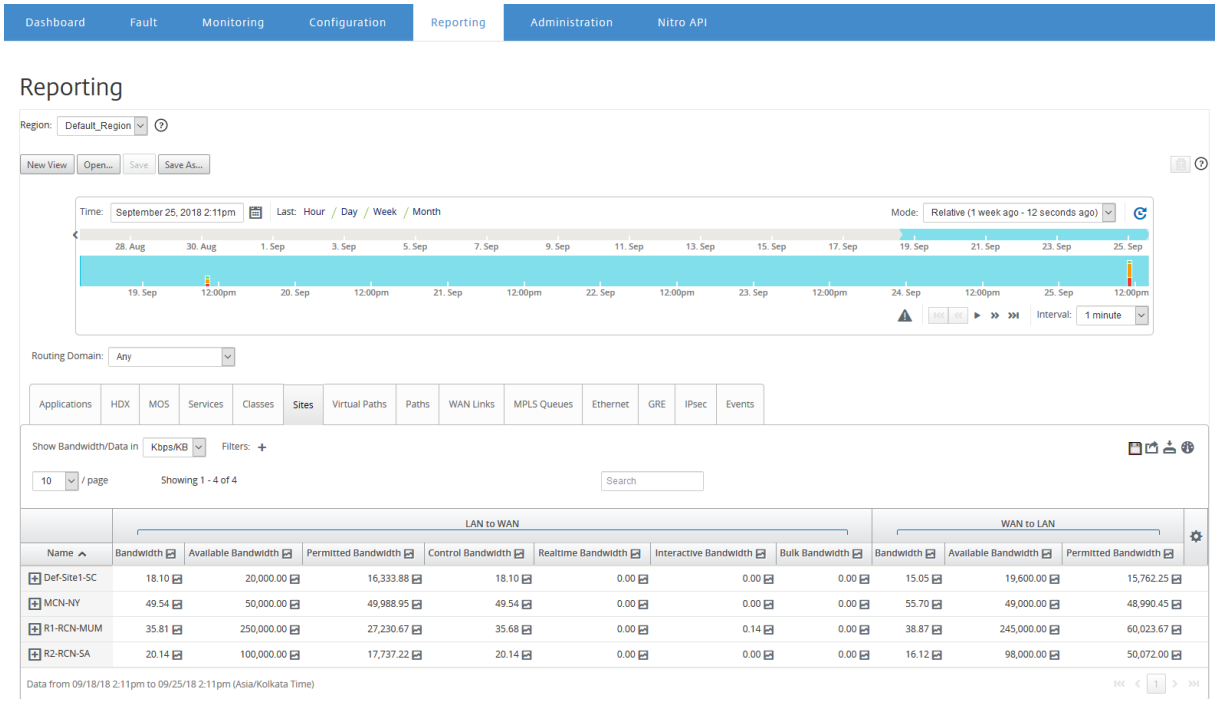
À l'aide de Citrix SD-WAN Center, vous pouvez afficher, avec les statistiques de base de bande passante, la bande passante consommée par les applications appartenant à ces types de classe à chaque niveau de site, chemin d'accès ou de liaison WAN.

Pour afficher les statistiques de bande passante :

Dans Citrix SD-WAN Center, accédez à **Reporting** > **Sites**, puis sélectionnez une période dans le contrôle de la chronologie.

Vous pouvez sélectionner et afficher les rapports d'une période donnée à l'aide des contrôles de chronologie. Pour plus d'informations, reportez-vous à la section Contrôles du scénario.

Vous pouvez également créer, enregistrer et ouvrir des vues de rapport. Pour plus d'informations, reportez-vous à la section Gérer les vues.



Vous pouvez afficher les mesures suivantes :

- **Bande passante** : bande passante totale consommée par tous les types de paquets. Bande passante = Bande passante contrôle + Bande passante en temps réel + Bande passante interactive + Bande passante en vrac. Par exemple, dans la capture d'écran ci-dessus, au SITE2, Bande passante = 1120.99+166.61+117,21+810.78+26.40
- **Bande passante disponible** : Bande passante totale allouée à tous les liens WAN d'un site.
- **Bande passante de contrôle** : bande passante utilisée pour transférer des paquets de contrôle contenant des informations de routage, de planification et de liaison.
- **Bande passante autorisée** : Bande passante disponible pour la transmission d'informations.
- **Bande passante en temps réel** : Bande passante consommée par les applications appartenant au type de classe en temps réel dans la configuration Citrix SD-WAN. Les performances de ces applications dépendent dans une large mesure 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 interactif dans la configuration Citrix SD-WAN. Les performances de ces applications dépendent dans une large mesure de la latence du réseau et de la perte de paquets (par exemple, XenDesktop, XenApp).
- **Bande passante en bloc** : Bande passante consommée par les applications appartenant au type de classe en bloc dans la configuration Citrix SD-WAN. Ces applications impliquent très peu d'intervention humaine et sont principalement gérées par les systèmes eux-mêmes (par exemple, FTP, opérations de sauvegarde).

Rapport de classe

February 17, 2022

Les services virtuels peuvent être affectés à des classes QoS particulières, et différentes restrictions de bande passante peuvent être appliquées à différentes classes. Une classe peut être l'un des trois types de base suivants :

- **Classes en temps réel** : servez les flux de trafic qui nécessitent un service rapide jusqu'à une certaine limite de bande passante. Une faible latence est préférable au débit agrégé.
- **Classes interactives** : Serve les flux de trafic sensibles à la perte et à la latence. Les classes interactives ont une priorité inférieure à celle du temps réel, mais ont une priorité absolue sur le trafic en masse.
- **Classes de masse** : Serve des flux de trafic nécessitant une bande passante élevée et sensibles aux pertes. Les classes en vrac ont la priorité la plus faible.

La spécification de différentes exigences de bande passante pour différentes classes permet au planificateur de chemins virtuels d'arbitrer les demandes de bande passante concurrentes provenant de plusieurs classes du même type. Le planificateur utilise l'algorithme Hierarchical Fair Service Curve (HFSC) pour atteindre l'équité entre les classes.

Pour plus d'informations sur la personnalisation des classes, consultez Personnalisation des classes.

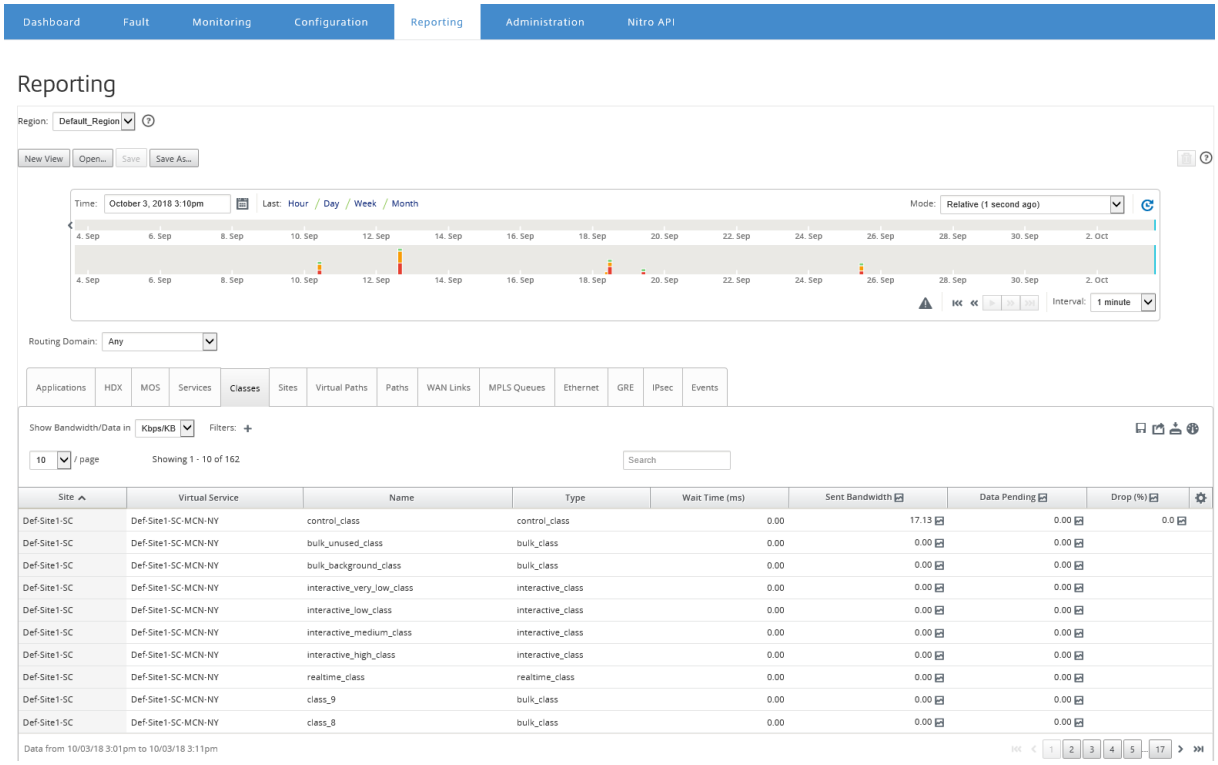
Pour afficher les statistiques de classe :

Dans Citrix SD-WAN Center, accédez à **Rapports** > **Classes**, puis sélectionnez une période dans le contrôle de montage.

Vous pouvez sélectionner et afficher des rapports d'une période donnée à l'aide des contrôles de chronologie. Pour plus d'informations, reportez-vous à la section Contrôles du scénario.

> **Remarque**
>
> Vous pouvez afficher les données de classe des 30 derniers jours. Toutes les données au-delà de cette période sont automatiquement supprimées du collecteur de SD-WAN Center et des collecteurs régionaux respectifs.

Vous pouvez également créer, enregistrer et ouvrir des vues de rapport. Pour plus d'informations, reportez-vous à la section Gérer les vues.



Vous pouvez afficher les mesures suivantes :

- **Nom** : Nom de la classe
- **Type** : Type de classe. Temps réel, interactif ou en masse.
- **Temps d'attente** : Intervalle de temps entre la transmission des paquets en millisecondes.
- **Bande passante envoyée** : bande passante transmise
- **Données envoyées** : Données envoyées, en Kbps.
- **Paquets envoyés** : Nombre de paquets envoyés.
- **Données en attente** : Données à envoyer, en Kbit/s.
- **Paquets en attente** : nombre de paquets à envoyer.
- **Drop** : Pourcentage de données supprimées.
- **Données supprimées** : données supprimées, en Kbps.
- **Paquets abandonnés** : nombre de paquets abandonnés en raison de la congestion du réseau.
- **Couverture des données** : Pourcentage de la période sélectionnée pour laquelle des données sont disponibles.

> **Remarque**
>
> Cliquez sur l'icône Paramètres pour sélectionner les mesures que vous souhaitez afficher.

Rapport sur l'interface Ethernet

February 17, 2022

Citrix SD-WAN Center fournit une vue centrale de toutes les interfaces Ethernet sur les différentes appliances Citrix SD-WAN sur votre réseau SD-WAN. Cela 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.

Les interfaces Ethernet sont configurées sur chaque appliance Citrix SD-WAN lors de la configuration du réseau SD-WAN.

Pour plus d'informations sur la configuration des groupes d'interface pour les sites MCN, consultezConfigurer un MCN.

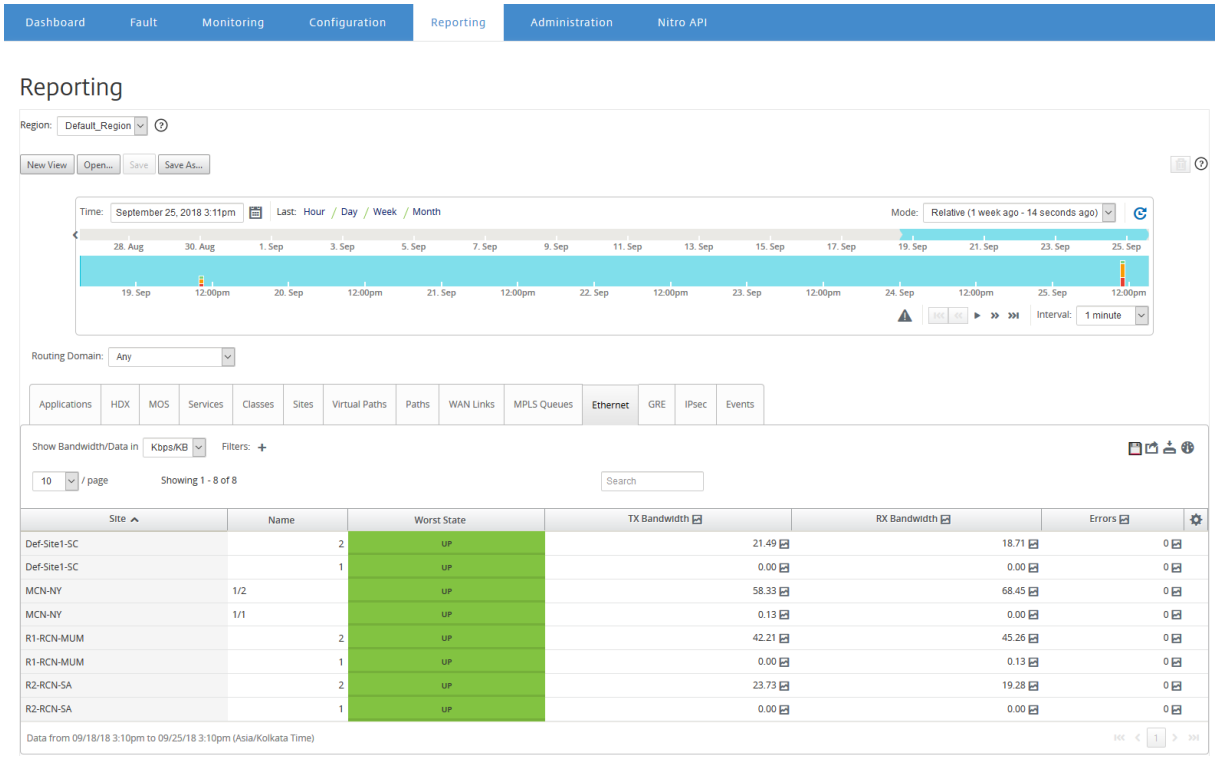
Pour plus d'informations sur la configuration des groupes d'interface pour les sites de succursale, voir Configurer un nœud de branche

Pour afficher les statistiques de l'interface Ethernet :

Dans Citrix SD-WAN Center, accédez à **Rapports** > **Ethernet**, puis sélectionnez une période dans le contrôle de la chronologie.

Vous pouvez sélectionner et afficher les rapports d'une période donnée à l'aide des contrôles de chronologie. Pour plus d'informations, reportez-vous à la section Contrôles du scénario.

Vous pouvez également créer, enregistrer et ouvrir des vues de rapport. Pour plus d'informations, reportez-vous à la section Gérer les vues.



Vous pouvez afficher les mesures suivantes :

- **Nom** : Nom de l'interface Ethernet.
- **État le plus mauvais** : pire état observé au cours de la période sélectionnée.
- **Bande passante TX** : bande passante transmise.
- **Bande passante RX** : bande passante reçue.
- **Paquets TX** : Nombre de paquets transmis.
- **Paquets RX** : Nombre de paquets reçus.
- **Erreurs** : Nombre d'erreurs observées pendant la période sélectionnée.
- **Couverture des données** : Pourcentage de la période sélectionnée pour laquelle les données sont disponibles.

> **Remarque**
>
> Cliquez sur l'icône Paramètres pour sélectionner les mesures que vous souhaitez afficher.

Rapport d'événement

February 17, 2022

Vous pouvez afficher le nombre d'événements différents qui se produisent sur chaque site du réseau SD-WAN.

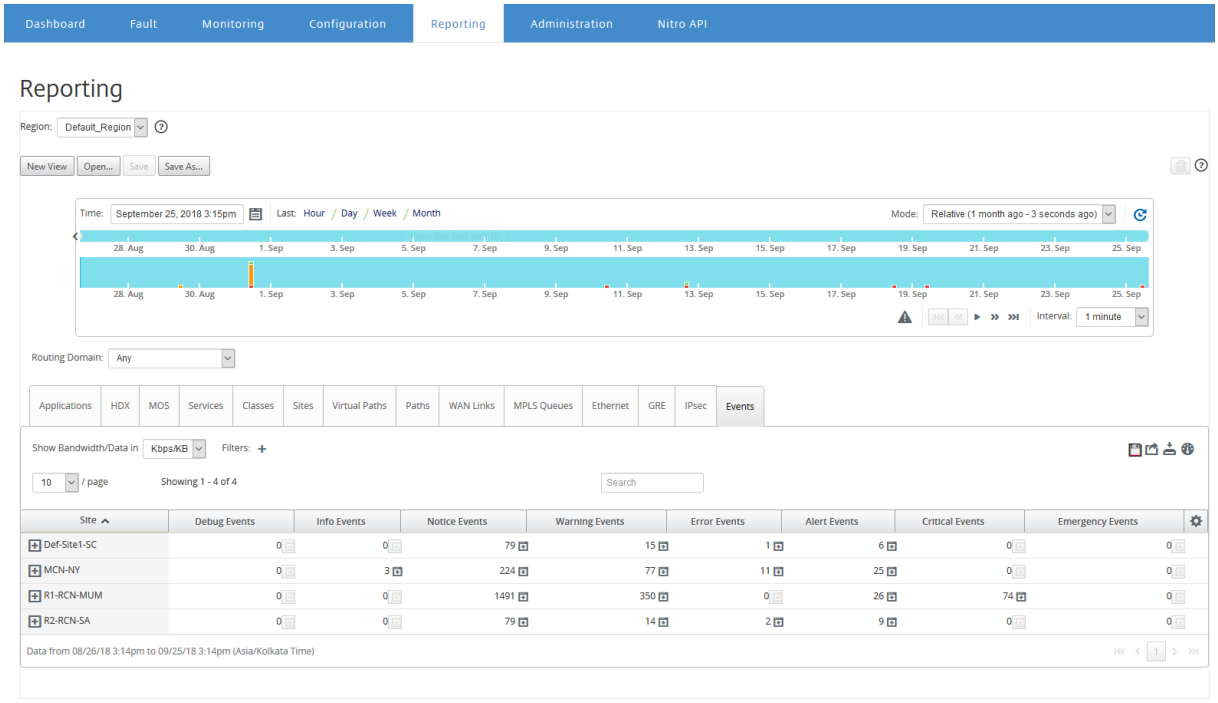
Pour plus d'informations sur les événements, reportez-vous à la section Événements.

Pour afficher les statistiques d'événements :

Dans Citrix SD-WAN Center, accédez à **Rapports** > **Événements**, puis sélectionnez une période dans le contrôle de la chronologie.

Vous pouvez sélectionner et afficher les rapports d'une période donnée à l'aide des contrôles de chronologie. Pour plus d'informations, reportez-vous à la section Contrôles du scénario.

Vous pouvez également créer, enregistrer et ouvrir des vues de rapport. Pour plus d'informations, reportez-vous à la section Gérer les vues.



Vous pouvez afficher les mesures suivantes :

- **Événements Info** : nombre d'événements d'information qui se sont produits au cours de la période sélectionnée. Ce sont des événements de bas niveau.
- **Événements**de notification : nombre d'événements de notification qui se sont produits pendant la période sélectionnée. Ce sont des événements que l'administrateur devrait connaître.
- **Événements d'**avertissement : nombre d'événements d'avertissement survenus au cours de la période sélectionnée. Ce sont des événements qui nécessitent une action dans un proche avenir.
- **Événements d'**erreur : nombre d'événements d'erreur survenus au cours de la période sélectionnée. Ce sont des événements qui indiquent un type d'erreur.
- **Événements**d'alerte : nombre d'événements d'alerte survenus au cours de la période sélectionnée. Ce sont des événements qui peuvent nécessiter une action.

- **Événements critiques** : nombre d'événements critiques survenus au cours de la période sélectionnée. Ce sont des événements qui indiquent une crise imminente.
- **Événements d'**urgence : Nombre d'événements d'urgence survenus au cours de la période sélectionnée. Ce sont des événements qui indiquent une crise immédiate (par exemple, panne d'alimentation, panne du ventilateur, seuil de disque dur dépassé, service désactivé).
- **Événements de débogage** : nombre d'événements de débogage qui se sont produits au cours de la période sélectionnée. Les événements de débogage sont générés lorsque les options Test Email ou Test Syslog sont utilisées sur les appliances Citrix SD-WAN.

> **Remarque**
>
> Cliquez sur l'icône Paramètres pour sélectionner les mesures que vous souhaitez afficher.

Le tableau suivant répertorie quelques exemples de changements d'état des objets pour lesquels des événements sont signalés.

Event	Object Type	Previous State	Current State
NOTICE	LAN to WAN path	BAD	GOOD
		GOOD	BAD
	WAN to LAN path	BAD	GOOD
		GOOD	BAD
	Dynamic virtual path	BAD	GOOD
		GOOD	BAD
WARNING	Virtual path	GOOD	BAD
	WAN link congestion	UNCONGESTED	CONGESTED
		CONGESTED	UNCONGESTED
	Usage congestion	UNCONGESTED	CONGESTED
		CONGESTED	UNCONGESTED
	LAN to WAN path	GOOD	DEAD
		BAD	DEAD
	WAN to LAN path	GOOD	DEAD
		BAD	DEAD
ALERT	Virtual path	BAD	DEAD
		DEAD	BAD
ERROR	WAN-link	GOOD	DEAD
	Ethernet	GOOD	UNDEFINED
		UNDEFINED	DEAD
INFO	Proxy-arp	UNDEFINED	ACTIVE
		UNDEFINED	STANDBY

Vous pouvez configurer Citrix SD-WAN Center pour envoyer des notifications d'événements externes

pour différents types d'événements sous forme de courrier électronique, d'interruptions SNMP ou de messages syslog. Pour plus d'informations, consultez Notifications d'événements.

Rapport sur les tunnels GRE

February 17, 2022

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 protocole de transport, et le protocole transporté s'appelle le protocole passagers. L'encapsulation de routage générique (GRE) est un mécanisme de tunneling 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.

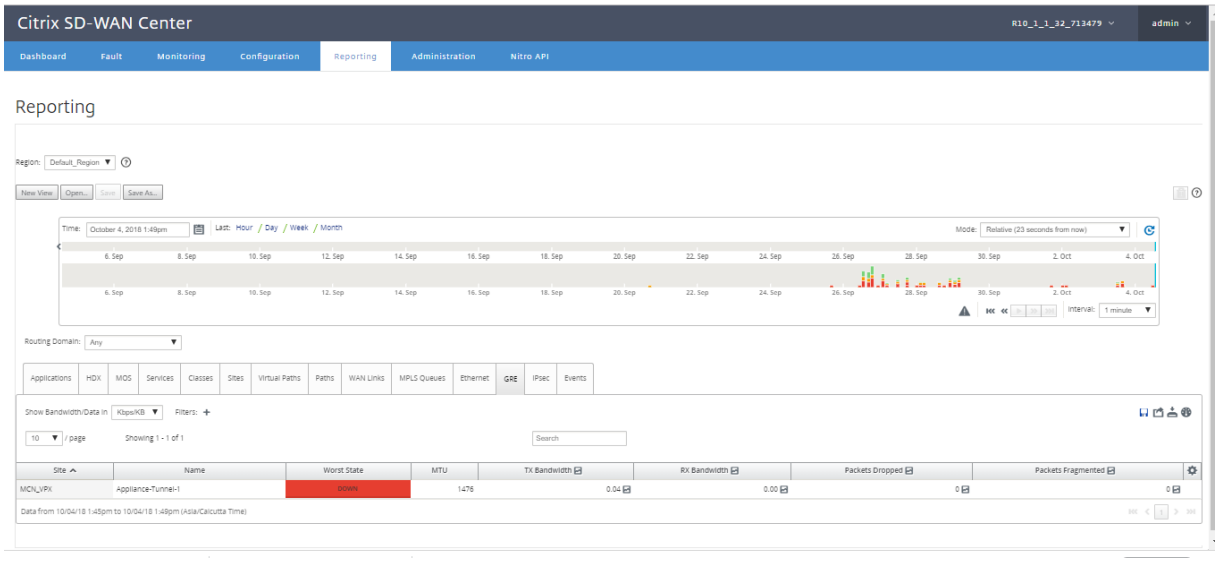
Citrix SD-WAN Center peut vous montrer l'état de tous les tunnels GRE configurés dans votre réseau Citrix SD-WAN.

Pour afficher les statistiques du tunnel GRE :

Dans Citrix SD-WAN Center, accédez à **Reporting** > **GRE**, et dans le contrôle de la chronologie, sélectionnez une période.

Vous pouvez sélectionner et afficher les rapports d'une période donnée à l'aide des contrôles de chronologie. Pour plus d'informations, reportez-vous à la section Contrôles du scénario.

Vous pouvez également créer, enregistrer et ouvrir des vues de rapport. Pour plus d'informations, reportez-vous à la section Gérer les vues.



Vous pouvez afficher les mesures suivantes :

- **État le plus mauvais** : pire état observé au cours de la période sélectionnée.
- **MTU** : Unité de transmission maximale —taille du plus grand datagramme IP pouvant être transféré via un lien spécifique.
- **Bande passante TX** : bande passante transmise.
- **Bande passante RX** : bande passante reçue.
- **Paquets TX** : Nombre de paquets transmis.
- **Paquets RX** : Nombre de paquets reçus.
- **Paquets abandonnés** : 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.
- **Couverture des données** : Pourcentage de la période sélectionnée pour laquelle les données sont disponibles.

> **Remarque**
>
> Cliquez sur l'icône Paramètres pour sélectionner les mesures que vous souhaitez afficher.

Rapport HDX

February 17, 2022

Sélectionnez l'un des types de rapports suivants dans la liste déroulante :

- Statistiques du site HDX

- Résumé HDX (applicable pour les sessions d'information HDX disponibles et non disponibles)
- Sessions utilisateur HDX (applicable uniquement pour les sessions disponibles sur les canaux d'information HDX uniquement)
- Applications HDX (applicables uniquement pour les sessions de canaux d'information HDX disponibles uniquement)

Statistiques du site HDX

Le rapport HDX fournit des données HDX détaillées par site.Les données de chaque site sont affichées en deux vues.

Vue récapitulative

La vue Récapitulative affiche les données suivantes pour un site :

- **Indice QoE** - La qualité de l'expérience (QoE) est une valeur numérique comprise entre 0 et 100. Plus la valeur est élevée, meilleure est l'expérience utilisateur.
- **Utilisateurs** : nombre d'utilisateurs actifs sur le site.
- **Flux TCP** : nombre de sessions HDX actives sur le site qui utilisent le protocole TCP.
- **Flux UDP** : nombre de sessions HDX actives sur le site qui utilisent des protocoles UDP.
- **Sessions** : nombre total de sessions HDX actives sur le site qui incluent à la fois des sessions d'intégration à petite échelle (SSI) et d'intégration à moyenne échelle (MSI).

Vue détaillée

Vous pouvez cliquer sur un site individuel pour afficher des détails sur toutes les variables affectant QoE.Chaque paire de lignes affiche les facteurs QoE pour les données calculées sur les côtés local et distant pour un chemin virtuel donné.

Les variables de latence, de gigue et de dépôt de paquets affectant QoE sont les nombres effectifs mesurés par l'appliance Citrix SD-WAN. Par exemple, il peut y avoir un pourcentage plus élevé de baisse de paquets dans le réseau, puisque Citrix SD-WAN corrige les chutes de paquets via son propre protocole, la perte effective de paquets constatée par l'application serait beaucoup plus faible, améliorant ainsi la QoE pour les applications HDX.

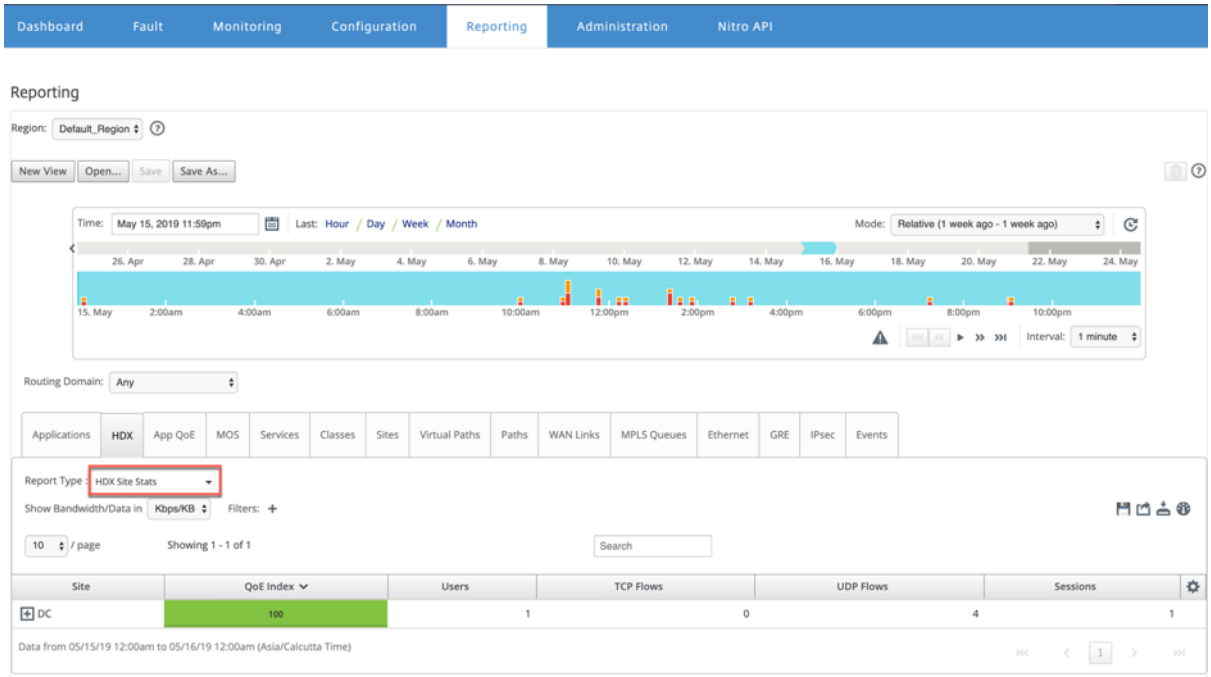
De même, l'amélioration de la latence grâce à la duplication de paquets améliore également la QoE pour les applications HDX. En d'autres termes, Citrix SD-WAN améliore le trafic QoE pour HDX en améliorant les facteurs affectant la QoE. Pour plus d'informations, reportez-vous à la section QoE HDX.

Pour afficher les rapports HDX :

Dans Citrix SD-WAN Center, accédez à **Reporting** > **HDX**, puis sélectionnez une période dans le contrôle de la chronologie.

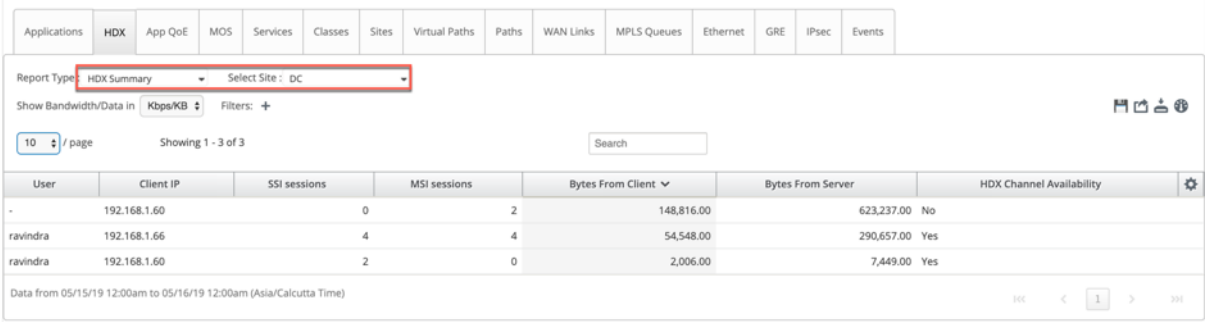
Vous pouvez sélectionner et afficher les rapports d'une période donnée à l'aide des contrôles de chronologie. Pour plus d'informations, reportez-vous à la section Contrôles du scénario.

Vous pouvez également créer, enregistrer et ouvrir des vues de rapport. Pour plus d'informations, reportez-vous à la section Gérer les vues.



Résumé HDX

Sélectionnez le rapport **HDX Summary** et le site dans la liste déroulante. Le rapport récapitulatif HDX affiche le rapport de chaque utilisateur connecté au cours de la période sélectionnée.



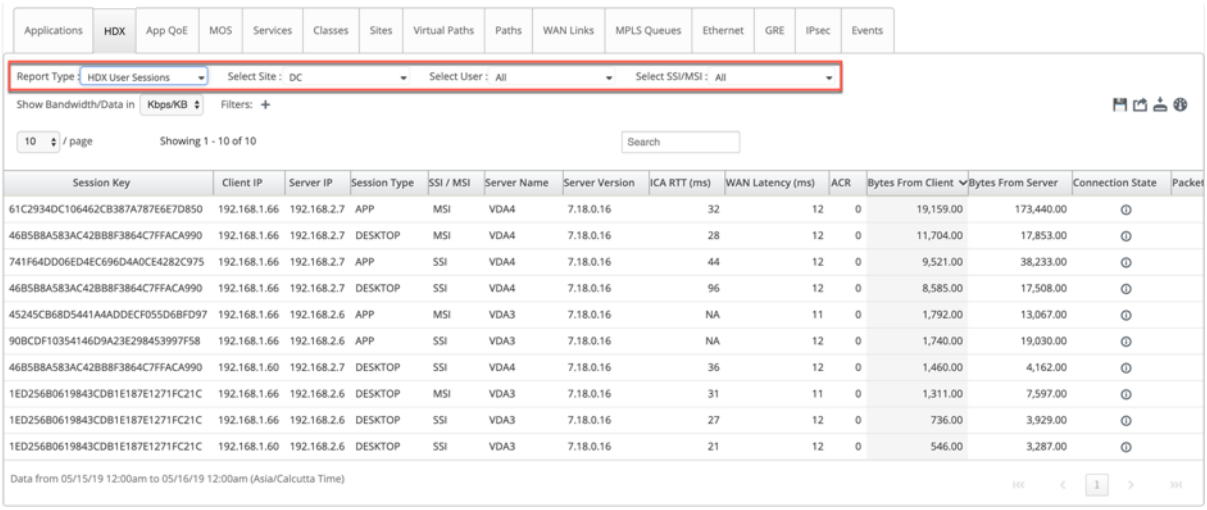
Dans le rapport de synthèse HDX, vous pouvez afficher les paramètres suivants :

- **Utilisateur** : Nom de l'utilisateur.
- **IP du client** : Adresse IP du client.

- **Sessions SSI : nombre de sessions**ICA (Single Stream ICA) actives.
- **Sessions MSI** : Nombre de sessions ICA (MSI) actives.
- **Octets du client** : Taille en octets du client.
- **Octets à partir du serveur** : Taille en octets à partir du serveur.
- **Disponibilité des canaux HDX** : fournit l'état de disponibilité du canal d'information HDX comme **Oui/Non**. Si le canal n'est pas disponible, le nom d'utilisateur s'affiche sous la forme d'un trait d'union (-).

Sessions utilisateur HDX

Dans le rapport sur les sessions utilisateur HDX, vous pouvez voir tous les détails des sessions utilisées par chaque utilisateur. Sélectionnez le site, l'utilisateur et SSI ou MSI dans la liste déroulante. Par défaut, les champs **Sélectionner un utilisateur** et **Sélectionner SSI/MSI** affichent **TOUS**.



Vous pouvez utiliser les options **Rechercher** ou **Filtrer : +** pour connaître les informations de session requises selon vos besoins.

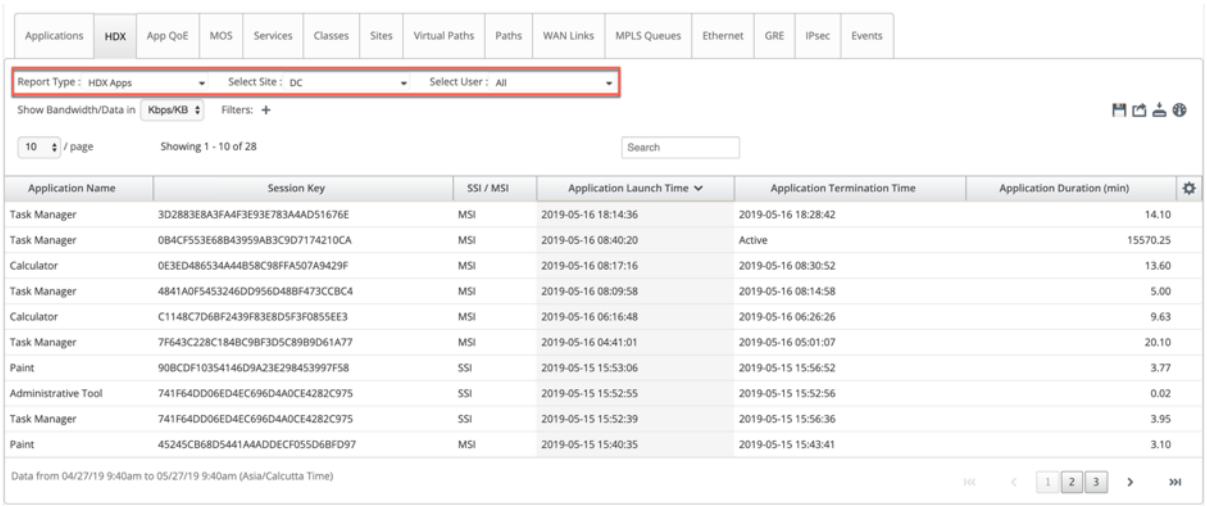
- **Clé**de session : la clé de session représente l'identité unique d'une session ICA.
- **IP du client** : adresse IP du client pour chaque session.
- **IP du serveur** : adresse IP du serveur pour chaque session.
- **Type de session** : Type des sessions (Bureau, Application).
- **SSI/MSI** : indique s'il s'agit d'une session SSI ou MSI.
- **Nom du serveur** : affiche le nom du serveur.
- **Version du serveur** : Affiche la version du serveur.
- **ICA RTT (ms)** : Affiche le temps du trajet aller-retour (RTT) de l'ICA en millisecondes. Il s'agit d'un temps aller-retour de bout en bout entre le client et le serveur.
- **Latence WAN** : latence sur le WAN, c'est-à-dire entre les deux SD-Wans sur le chemin virtuel. Cette latence n'inclut pas la latence réseau côté client ou côté serveur.

- **ACR** : affiche le nombre de reconnexion automatique du client.
- **Octets du client** : Taille en octets du client.
- **Octets à partir du serveur** : Taille en octets à partir du serveur.
- **État de connexion** : placez le curseur de la souris pour voir l'état de connexion.
  - Pour MSI, il y a quatre connexions. Ces connexions sont de niveau L4 (état TCP/UDP).
  - Pour SSI, il n'y a qu'une seule connexion.

- **Paquet à partir du client** : nombre de paquets provenant du client.
- **Paquet à partir du serveur** : nombre de paquets du serveur.

Applications HDX

Vous pouvez voir toutes les applications utilisées par un utilisateur spécifique ou par tous les utilisateurs. Sélectionnez le **site** et l'**utilisateur** pour afficher les détails des applications.



- **Nom de l'application** : fournit le nom de l'application HDX.
- **Clé de session** : fournit la clé de session unique utilisée pour cette application particulière.
- **SSI/MSI** : indique s'il s'agit d'une session SSI ou MSI.
- **Heure de lancement de l'application** : indique l'heure de lancement de l'application avec la date.

- **Heure de résiliation**de l'application : indique l'heure de fin de l'application avec la date. Si une application est active, elle s'affiche active au lieu de l'heure de résiliation.
- **Durée de l'application (min)** : fournit la durée de l'application en minutes.

> **Remarque**
>
> - S'il y a une erreur involontaire telle que, si les informations de session HDX ne sont pas disponibles sur l'appliance, les rapports HDX basés sur l'utilisateur ne s'affichent pas même si le **rapport utilisateur HDX** est activé. Certains des champs tels que le nom d'utilisateur, le nom du serveur, la version du serveur, la RTT ICA dans les rapports peuvent être affichés sous forme de **NA**.
> - L'heure de fin d'application dans le rapport **HDX Apps** est affichée uniquement si le SD-WAN reçoit **l'heure de fin d'application** de Xen Application/Xen Desktop Server. Sinon, certaines applications sont déclarées actives même si elles sont fermées.

Rapport de tunnel IPSec

February 17, 2022

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 des tunnels IPsec sur les appliances Citrix SD-WAN, consultez la section Arrêt du tunnel IPsec.

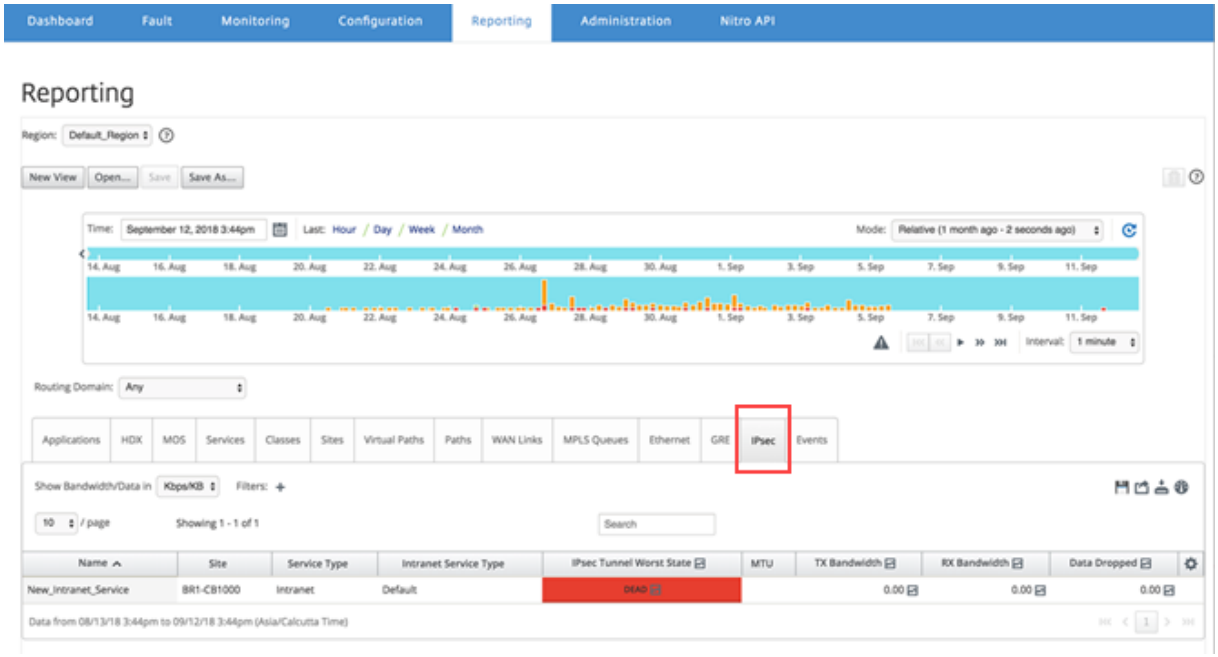
Citrix SD-WAN Center peut vous montrer l'état de tous les tunnels IPSec configurés dans votre réseau Citrix SD-WAN.

Pour afficher les statistiques du tunnel IPSec :

Dans Citrix SD-WAN Center, accédez à **Reporting** > **Tunnels IPSec**, puis sélectionnez une période dans le contrôle de la chronologie.

Vous pouvez sélectionner et afficher les rapports d'une période donnée à l'aide des contrôles de chronologie. Pour plus d'informations, reportez-vous à la section Contrôles du scénario.

Vous pouvez également créer, enregistrer et ouvrir des vues de rapport. Pour plus d'informations, reportez-vous à la section Gérer les vues.



Vous pouvez afficher les mesures suivantes :

- **Nom : Nom**de l'application.
- **Site** : Nom du site.
- **Type de service** : Type du service.
- **Type de service Intranet** : Type de service intranet associé au tunnel IPSec. Voici le type de services intranet :
  - Défaut
  - WAN virtuel Microsoft Azure
  - Zscaler
  - Passerelle SaaS Citrix
- **IPSec pire état** : pire état observé au cours de la période sélectionnée.
- **MTU** : unité de transmission maximale : taille du plus grand datagramme IP pouvant être transféré via un lien spécifique.
- **Bande passante TX** : bande passante transmise.
- **Bande passante RX** : bande passante reçue.
- **Paquets TX** : Nombre de paquets transmis.
- **Paquets RX** : Nombre de paquets reçus.
- **Données supprimées** : données supprimées, en Kbps.
- **Paquets supprimés** : Nombre de paquets déposés.

> **Remarque**
>
> Cliquez sur l'icône Paramètres pour sélectionner les mesures que vous souhaitez afficher.

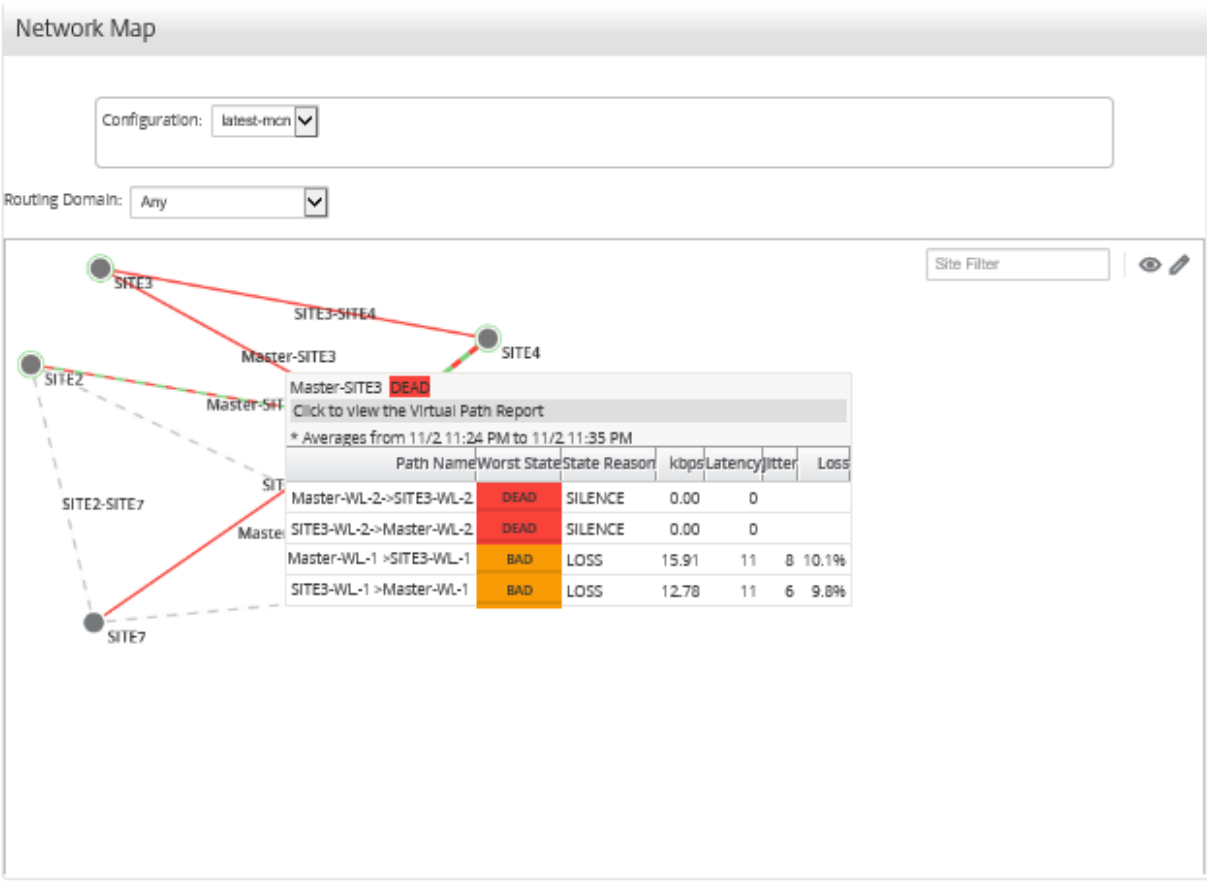
Rapport sur les performances des liens

February 17, 2022

Citrix SD-WAN Center peut afficher des statistiques de performances au niveau du site, du service, du chemin virtuel ou de la liaison Wan-Link.

Envisagez un réseau dans lequel l'organisation ABC a quatre succursales. Des coupures de courant ont été signalées sur le SITE3. C'est-à-dire que les employés sont parfois incapables de consulter les pages intranet. Vous soupçonnez que c'est à cause des performances des liens sous-jacents.

Vous pouvez obtenir une vue de haut niveau des statistiques de liaison en plaçant le curseur de votre souris sur le chemin entre un site et le centre de données sur la carte réseau du tableau de bord.



La capture d'écran ci-dessus montre qu'il existe deux liaisons WAN (WL-1 et WL-2) entre SITE 3 et MCN (Master Controller Node), et affiche des statistiques pour les 10 minutes les plus récentes.

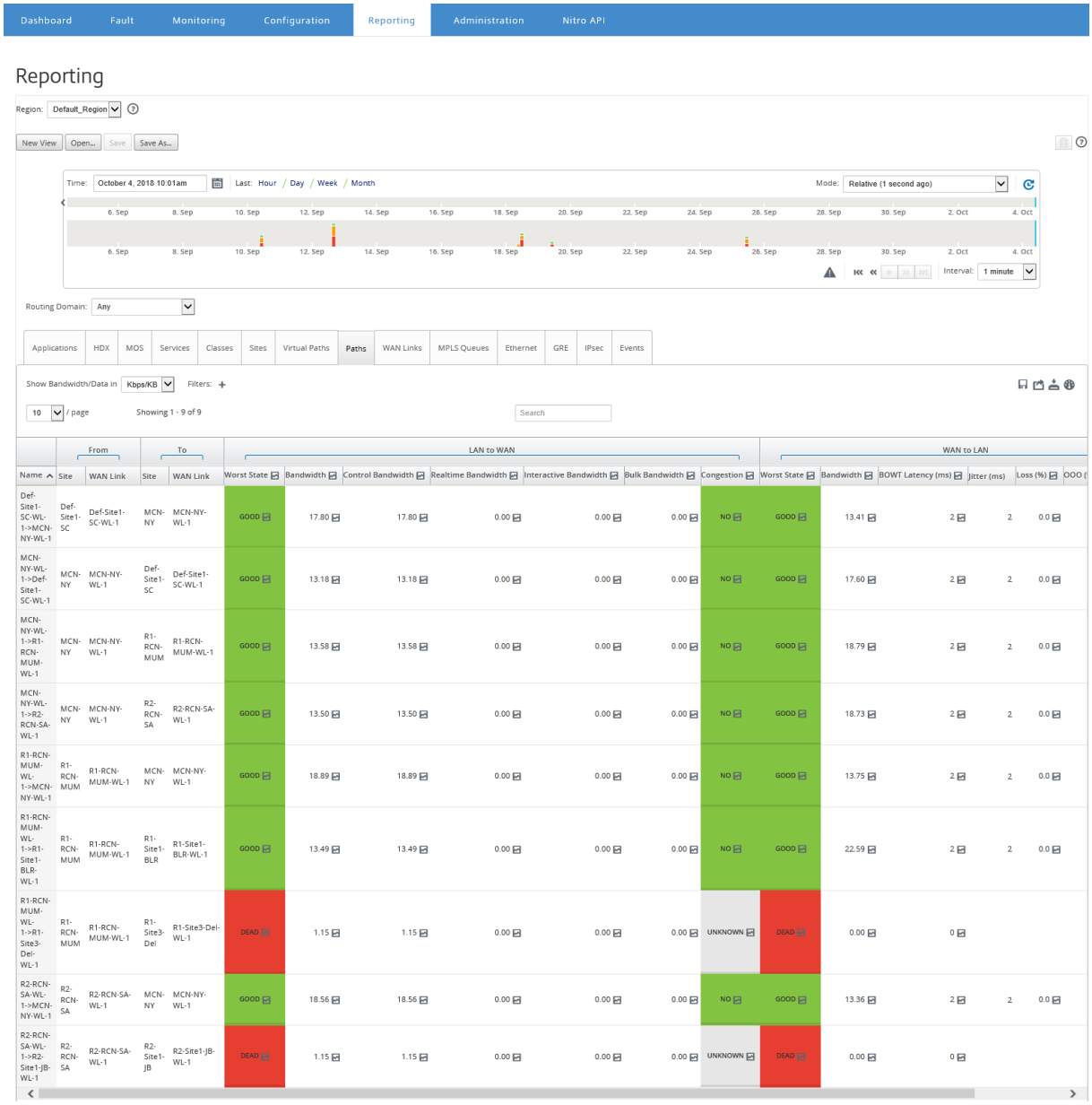
Les chemins virtuels Master-WL2->Site3-WL2 et SITE3-WL2 ->Master-WL2 ne fonctionnent pas, et les chemins alternatifs Master-WL1->Site3-WL1 et SITE3-WL1 ->Master-WL1 sont en mauvais état, perdant un pourcentage significatif des données transmises. C'est la cause probable du problème de l'épuisement au SITE3.

Vous pouvez également afficher les statistiques des liens en accédant à **ReportingChemins**.

Dans le contrôle chronologie, sélectionnez une période.

Vous pouvez sélectionner et afficher les rapports d'une période donnée à l'aide des contrôles de chronologie. Pour plus d'informations, reportez-vous à la section Contrôles du scénario.

Vous pouvez également créer, enregistrer et ouvrir des vues de rapport. Pour plus d'informations, reportez-vous à la section Gérer les vues.



Vous pouvez afficher les mesures suivantes :

- **Nom : nom**du chemin d'accès.
- **De (Site et lien WAN)** : le site source et le lien WAN.

- **À (Site et lien WAN)** : le site de destination et le lien WAN.
- **LAN vers WAN**
  - **État de travail** :
  - **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 liaison.
  - **Bande passante en temps réel** : Bande passante consommée par les applications appartenant au type de classe 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 bloc** : Bande passante consommée par les applications appartenant au type de classe en bloc dans la configuration SD-WAN. Ces applications impliquent très peu d'intervention humaine et sont principalement gérées par les systèmes eux-mêmes (par exemple, FTP, opérations de sauvegarde).
  - **Encombrement** : congestion due à une augmentation du trafic ou à un retard inattendu du flux de paquets dans le WAN.
- **WAN au réseau local** :
  - **Pire état** : Le pire état WAN vers LAN observé pendant la période.
  - **Bande passante** :
  - **Latence BOWT (ms)** : Meilleur temps unidirectionnel (BOWT) pris pour qu'un paquet se déplace d'un point à un autre, en millisecondes.
  - **Jitter (ms)** : Variation du délai des paquets reçus, en millisecondes.
  - **Perte (%)** : Pourcentage de paquets perdus.
  - **OOO (%)** : Pourcentage de paquets qui ne sont pas dans le bon ordre ou en panne (OOO).
  - **Encombrement** : congestion due à une augmentation du trafic ou à un retard inattendu du flux de paquets dans le WAN.

Cliquez sur l'icône **Paramètres** et sélectionnez les paramètres que vous souhaitez afficher sur les rapports.

MOS pour applications

February 17, 2022

Le score d'opinion moyen (MOS) fournit une mesure numérique de la qualité de l'expérience qu'une application fournit aux utilisateurs finaux. Il est principalement utilisé pour les applications VoIP. Dans Citrix SD-WAN, MOS est également utilisé pour évaluer la qualité des applications non-VoIP en jugeant le trafic comme s'il s'agissait d'un appel VoIP.

Citrix SD-WAN Center calcule et affiche MOS pour le trafic qui traverse le chemin virtuel. **Activez l'option Estimer MOS** pour chaque application sur chaque appliance Citrix SD-WAN pour afficher les scores MOS de ces applications dans Citrix SD-WAN Center.

Pour plus d'informations sur l'activation de MOS pour les applications dans Citrix SD-WAN, consultez Ajouter des groupes de règles et Activer MOS.

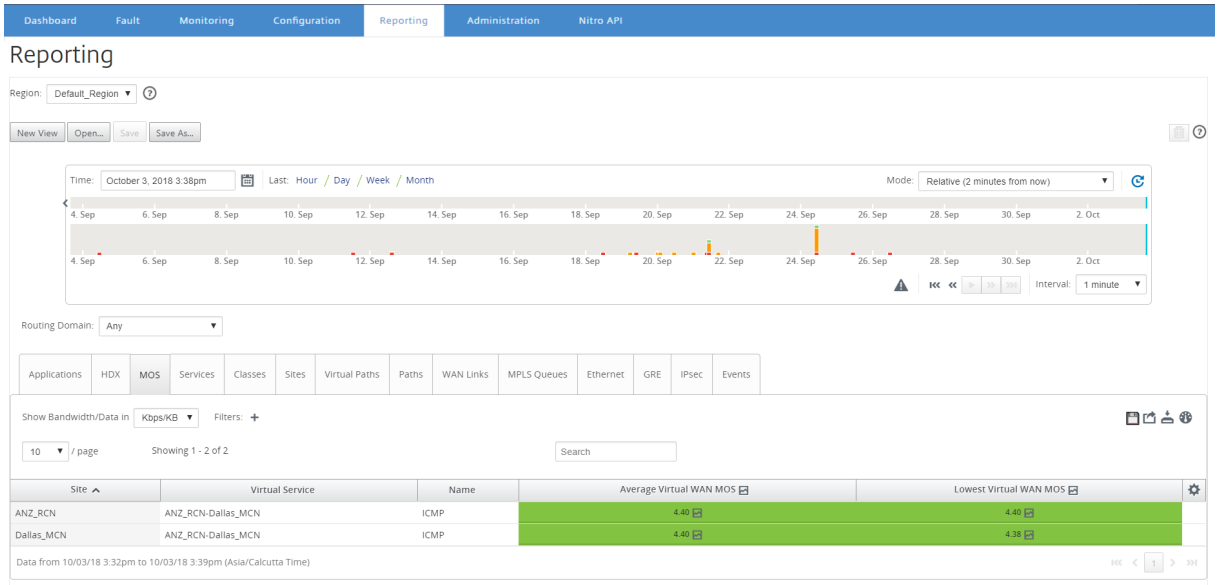
> **Remarque**
>
> Activez l'option Suivi des performances, sous Règles pour estimer les MOS pour les applications et l'afficher dans Citrix SD-WAN Center. Pour plus d'informations sur les règles, consultez Règles par adresse IP et numéro de port.

Pour afficher les MOS pour les applications :

Dans Citrix SD-WAN Center, accédez à **Reporting** > **Applications**et dans le contrôle chronologique sélectionnez une période.

Vous pouvez sélectionner et afficher les rapports d'une période donnée à l'aide des contrôles de chronologie. Pour plus d'informations, reportez-vous à la section Contrôles du scénario.

Vous pouvez également créer, enregistrer et ouvrir des vues de rapport. Pour plus d'informations, reportez-vous à la section Gérer les vues.



Vous pouvez afficher les mesures suivantes :

- **Nom** : Nom de l'application.
- **MOS WAN virtuel moyen** : score de qualité moyen calculé sur la période sélectionnée.
- **MOS WAN virtuel le**plus bas : score de qualité le plus bas calculé au cours de la période sélectionnée.

Les notes sont classées comme suit :

- 5 —Les utilisateurs sont très satisfaits.
- 4 —Les utilisateurs sont satisfaits.
- 3 —Les utilisateurs sont insatisfaits.
- 2 —Les utilisateurs sont très insatisfaits.
- 1 —Non recommandé.

Rapport des files d'attente MPLS

February 17, 2022

Les files d'attente MPLS fournissent des files d'attente de service contrôlées par des balises DSCP (Differentiated Services Code Point) standard. Les balises contrôlent la qualité du service entre deux sites sur le WAN virtuel.

Les files d'attente MPLS permettent aux fournisseurs MPLS d'identifier le trafic sur la base des marquages DSCP, de sorte que la classe de service puisse être appliquée par le fournisseur.

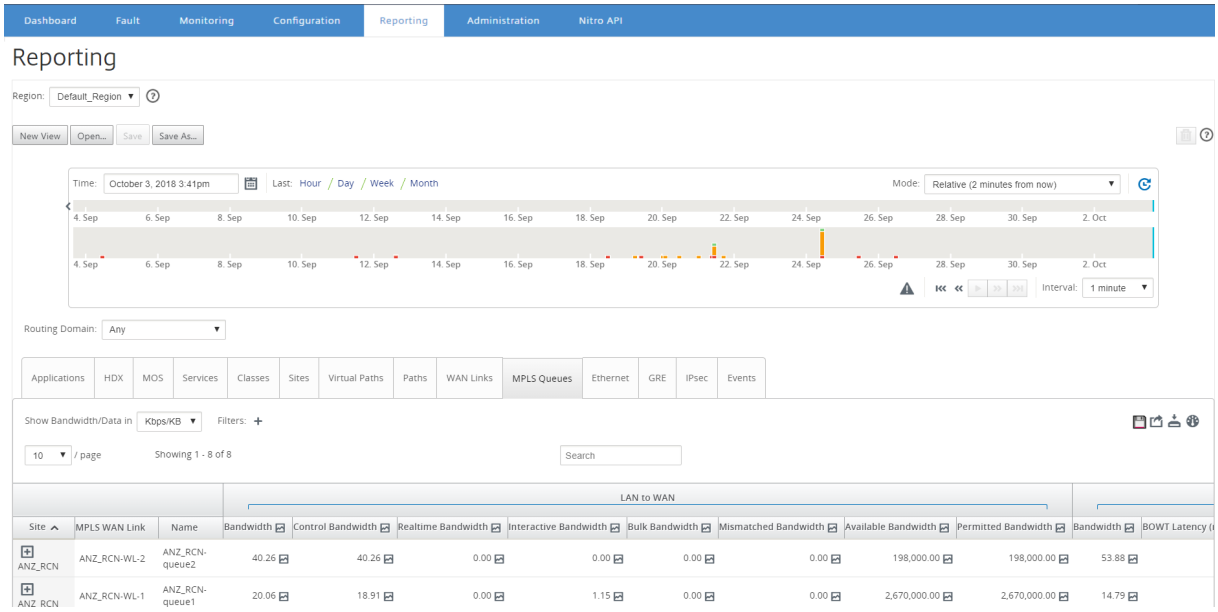
Pour plus d'informations sur la configuration de liens WAN MPLS privés sur les appliances Citrix SD-WAN, consultez Files d'attente MPLS.

Pour afficher les statistiques de file d'attente MPLS :

Dans Citrix SD-WAN Center, accédez à **Rapports** > Files d'**attente MPLS**, puis sélectionnez une période dans le contrôle de la chronologie.

Vous pouvez sélectionner et afficher les rapports d'une période donnée à l'aide des contrôles de chronologie. Pour plus d'informations, reportez-vous à la section Contrôles du scénario.

Vous pouvez également créer, enregistrer et ouvrir des vues de rapport. Pour plus d'informations, reportez-vous à la section Gérer les vues.



Vous pouvez afficher les mesures suivantes :

- **MPLS WAN Link** : nom de la liaison WAN MPLS dont la file d'attente MPLS est membre.
- **Nom : Nom**de la balise DSCP.
- **Bande passante** : bande passante totale consommée par tous les types de paquets. Bande passante = Bande passante contrôle + Bande passante en temps réel + Bande passante interactive + Bande passante en vrac.
- **Bande passante de contrôle** : bande passante utilisée pour transférer des paquets de contrôle contenant des informations de routage, de planification et de liaison.
- **Bande passante en temps réel** : Bande passante consommée par les applications appartenant au type de classe en temps réel dans la configuration Citrix SD-WAN. Les performances de ces applications dépendent dans une large mesure 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 interactif dans la configuration Citrix SD-WAN. Les performances de ces appli-

cations dépendent dans une large mesure de la latence du réseau et de la perte de paquets (par exemple, XenDesktop, XenApp).

- **Bande passante en bloc** : Bande passante consommée par les applications appartenant au type de classe en bloc dans la configuration Citrix SD-WAN. Ces applications impliquent très peu d'intervention humaine et sont principalement gérées par les systèmes eux-mêmes (par exemple, FTP, opérations de sauvegarde).
- **Bande passante incorrecte** : les trames qui ne correspondent pas aux balises DSCP définies sont mappées à une file d'attente par défaut désignée pour une bande passante inadaptée.
- **Bande passante disponible** : somme de la bande passante allouée à tous les liens WAN d'un site.
- **Bande passante autorisée** : Bande passante disponible pour la transmission d'informations.
- **Latence BOWT** : Meilleur temps à sens unique pour qu'un paquet se déplace d'un point à un autre, en millisecondes.
- **Gigue** : Variation du délai des paquets reçus, en millisecondes.
- **Paquets perdus** : Nombre de paquets perdus.
- **Perte** : Pourcentage de paquets perdus.
- **OOO** : Pourcentage de paquets qui ne sont pas dans le bon ordre.
- **Encombrement** : congestion due à une augmentation du trafic ou à un retard inattendu du flux de paquets dans le WAN.

> **Remarque**
>
> Cliquez sur l'icône Paramètres pour sélectionner les mesures que vous souhaitez afficher.

Administration

February 17, 2022

Vous pouvez gérer et gérer votre Citrix SD-WAN Center VPX à l'aide des options d'administration suivantes.

Configurer la date et l'heure

Certificats HTTPS

Importer la configuration MCN

Gérer la base

Gérer les vues

Mise à niveau logicielle

Contrôles de chronologie

Comptes utilisateur

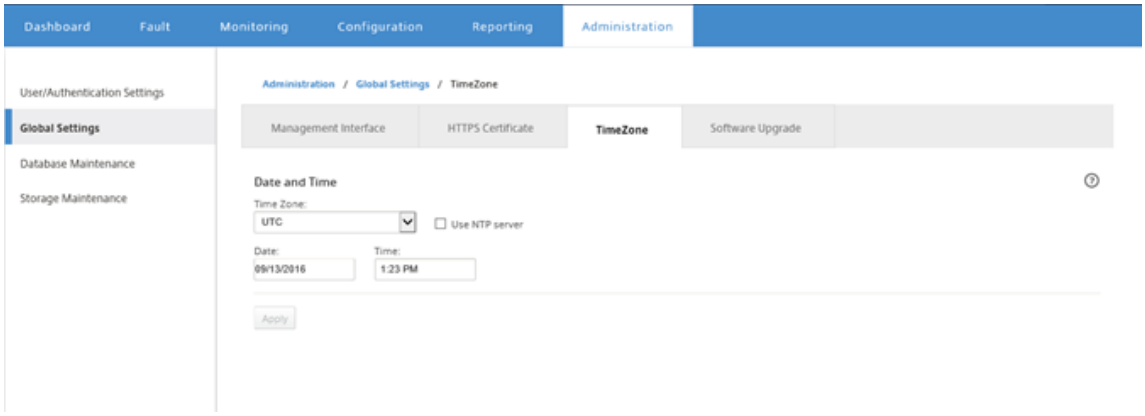
Configurer la date et l'heure

February 17, 2022

Vous pouvez modifier la date et l'heure du système de gestion Citrix SD-WAN Center manuellement ou à l'aide d'un serveur NTP. Si vous sélectionnez l'option **Utiliser le serveur NTP**, vous ne pouvez pas entrer manuellement une date et une heure actuelles.

Pour définir manuellement la date et l'heure :

1. Dans l'interface Web Citrix SD-WAN Center, cliquez sur l'onglet **Administration**.
2. Cliquez sur **Paramètres globaux**, puis cliquez sur **Fuseau horaire**.



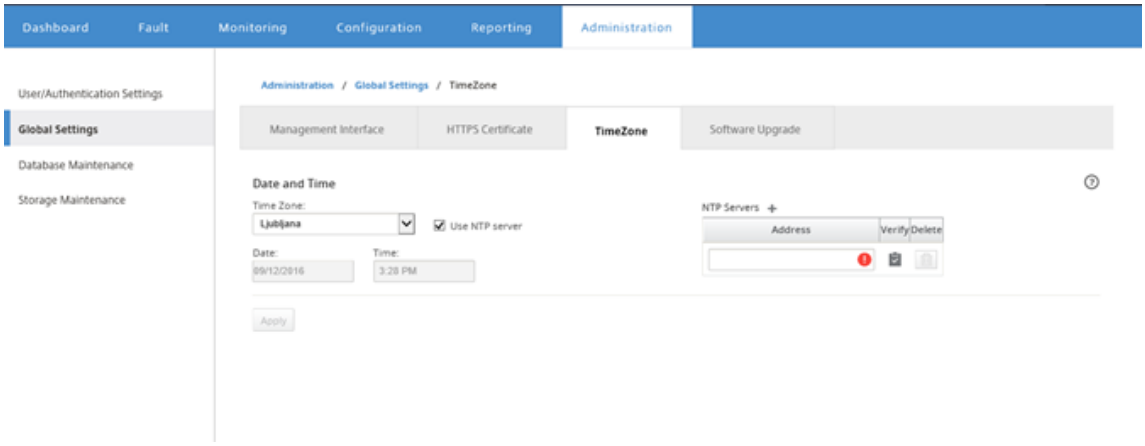
3. Dans le champ **Fuseau horaire**, sélectionnez une **ville** dans votre fuseau horaire actuel. Vous pouvez également saisir la date et l'heure actuelles de votre fuseau horaire.
4. Cliquez sur **Apply**.

Vous pouvez synchroniser l'horloge Citrix SD-WAN Center avec un serveur NTP externe.

Pour définir la date et l'heure à l'aide d'un serveur NTP :

1. Dans l'interface Web Citrix SD-WAN Center, cliquez sur l'onglet **Administration**.
2. Cliquez sur **Paramètres globaux**, puis sur **Fuseau horaire**.
3. Sélectionnez **Utiliser le serveur NTP**.

   Cette option désactive les champs Date et Heure et affiche la table Serveurs NTP.



4. Pour ajouter un nouveau serveur NTP, cliquez sur l'icône **+** en regard du serveur NTP.
5. Dans le champ **Adresse**, entrez l'**adresse IP** du serveur NTP.

   Vous pouvez spécifier jusqu'à trois serveurs NTP, mais vous devez en spécifier au moins un. Ces serveurs agissent comme des serveurs NTP de sauvegarde, si un serveur est en panne, le Citrix SD-WAN Center 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.Pour supprimer une entrée de serveur de la table, cliquez sur l'icône **Supprimer** dans la colonne Supprimer de l'entrée.
6. Cliquez sur **Vérifier** pour vérifier que le serveur est accessible, avant d'appliquer vos paramètres.
7. Cliquez sur **Apply**.

Certificats HTTPS

February 17, 2022

Un certificat HTTPS est requis pour établir une connexion HTTPS de gestion sécurisée à Citrix SD-WAN Center.

Afficher les détails du certificat HTTPS installé

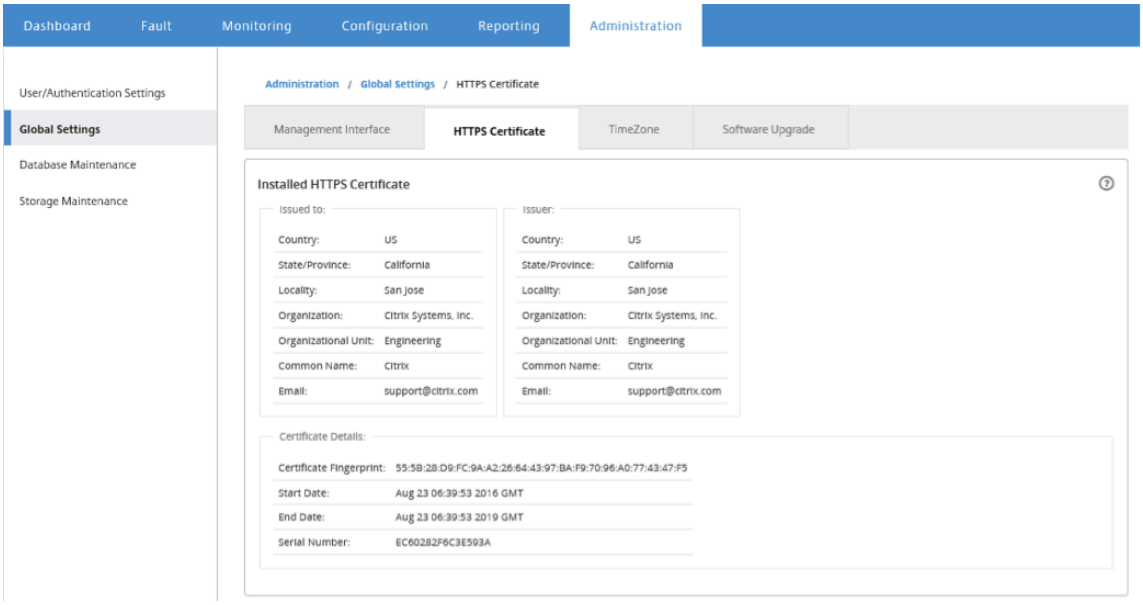
Pour évaluer le certificat actuel, vous pouvez afficher les détails du certificat.

Pour afficher les détails du certificat HTTPS déjà installé sur Citrix SD-WAN Center :

1. Dans l'interface Web Citrix SD-WAN Center, cliquez sur l'onglet **Administration**.

2. Cliquez sur **Paramètres globaux**, puis sur **Certificat HTTPS**.

   Les détails du certificat HTTPS apparaissent dans la section **Certificat HTTPS installé**.

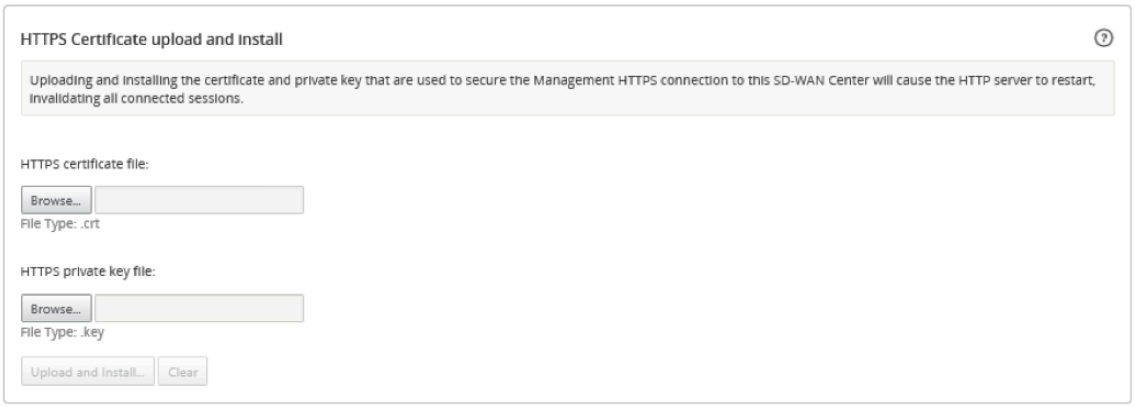


Télécharger et installer un certificat HTTPS

L'installation d'un certificat HTTPS place Citrix SD-WAN Center en mode Maintenance jusqu'à ce que l'opération soit terminée. Lorsque l'opération est terminée, le serveur Web est redémarré, invalidant toutes les sessions connectées. Si la connexion au serveur est perdue lors du redémarrage du serveur Web, l'écran du mode de maintenance recharge automatiquement la page précédente et affiche un avis de sécurité du navigateur. Si l'écran ne se recharge pas, cliquez sur **Continuer** pour recharger la page précédente.

Pour télécharger et installer le certificat HTTPS :

1. Dans l'interface Web Citrix SD-WAN Center, cliquez sur l'onglet **Administration**.
2. Cliquez sur **Paramètres globaux**, puis sur **Certificats HTTPS**.
3. Dans la section **Téléchargement et installation du certificat HTTPS**, dans le champ **Fichier de certificat HTTPS**, cliquez sur **Parcourir** et sélectionnez un certificat HTTPS.
4. Pour le champ **Fichier de clé privée HTTPS**, cliquez sur **Parcourir** et sélectionnez un fichier de clé privée HTTPS.
5. Cliquez sur **Upload and Install**.



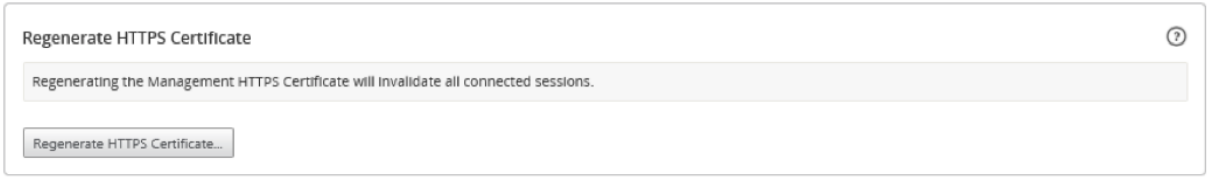
Régénérer le certificat HTTPS

Vous pouvez régénérer un certificat auto-signé qui sécurise la connexion HTTPS de gestion à Citrix SD-WAN Center. La régénération du certificat HTTPS place Citrix SD-WAN Center en mode Maintenance jusqu'à ce que l'opération soit terminée. Lorsque l'opération est terminée, le serveur Web est redémarré, invalidant toutes les sessions connectées.

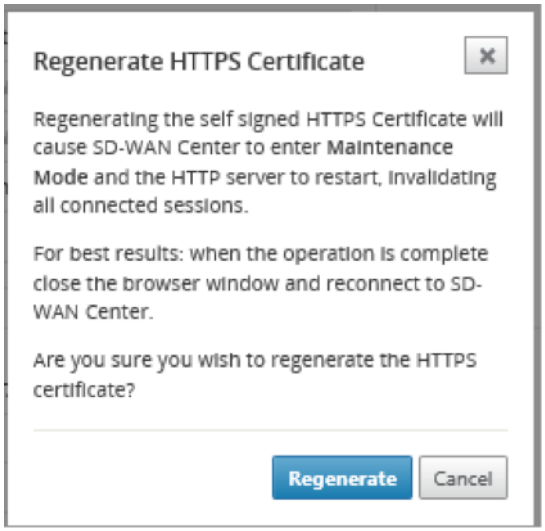
Si la connexion au serveur est perdue lors du redémarrage du serveur Web, l'écran du mode de maintenance recharge automatiquement la page précédente et affiche un avis de sécurité du navigateur. Si l'écran n'apparaît pas, cliquez sur **Continuer** pour recharger la page précédente.

Pour régénérer le certificat HTTPS :

1. Dans l'interface Web Citrix SD-WAN Center, cliquez sur l'onglet **Administration**.
2. Cliquez sur **Paramètres globaux**, puis sur **Certificats HTTPS**.
3. Dans la section **Régénérer le certificat HTTPS**, cliquez sur **Régénérer le certificat HTTPS**.



Le message Régénérer le certificat HTTPS s'affiche. Cliquez sur **Régénérer**.



Importer la configuration MCN

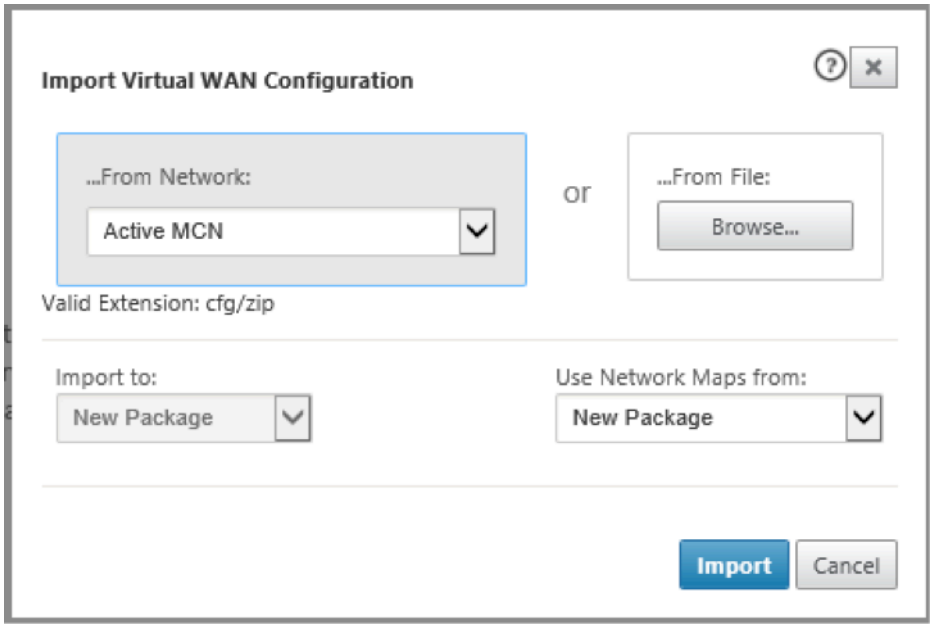
February 17, 2022

Lorsque Citrix SD-WAN Center est configuré et qu'une connexion est établie entre le nœud de contrôle maître (MCN) et Citrix SD-WAN Center, vous pouvez importer la configuration MCN dans Citrix SD-WAN Center et afficher les cartes réseau.

La fonction Importer importe une configuration dans une configuration principale Citrix SD-WAN ouverte ou nouvelle. Si une configuration principale Citrix SD-WAN est ouverte lorsque vous utilisez la fonction d'importation, elle et ses cartes sont remplacées par la nouvelle configuration principale Citrix SD-WAN. Si aucune configuration principale Citrix SD-WAN n'est ouverte, un package sans titre est créé.

Pour importer la configuration MCN dans Citrix SD-WAN Center :

1. Dans l'interface Web Citrix SD-WAN Center, cliquez sur l'onglet **Configuration**.
2. Cliquez sur **Configuration réseau**, puis sur **Importer**.



3. Dans le champ **De réseau**, sélectionnez l'une des options suivantes :

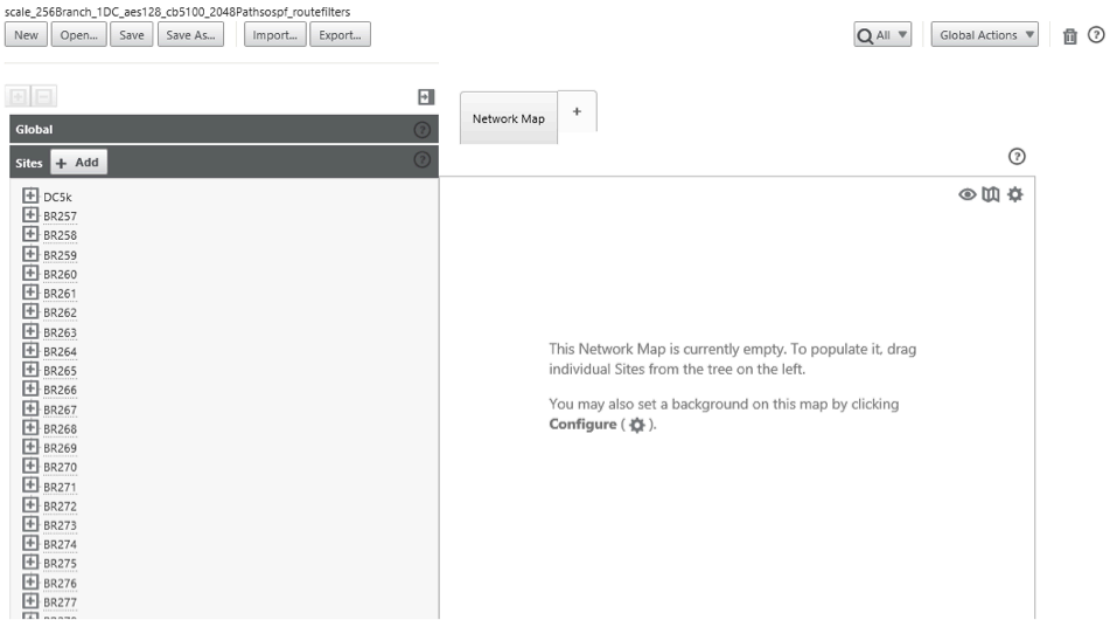
   - **MCN actif** : Connectez-vous au MCN actif et téléchargez la configuration actuelle.
   - **Autre** : Connectez-vous à une adresse IP d'un MCN différent et téléchargez la configuration actuelle. Vous devrez peut-être installer le certificat de sécurité à partir de ce Citrix SD-WAN Center dans le MCN avant de pouvoir importer la configuration.

   Pour plus d'informations, consultez la section Installer le certificat Citrix SD-WAN Center.

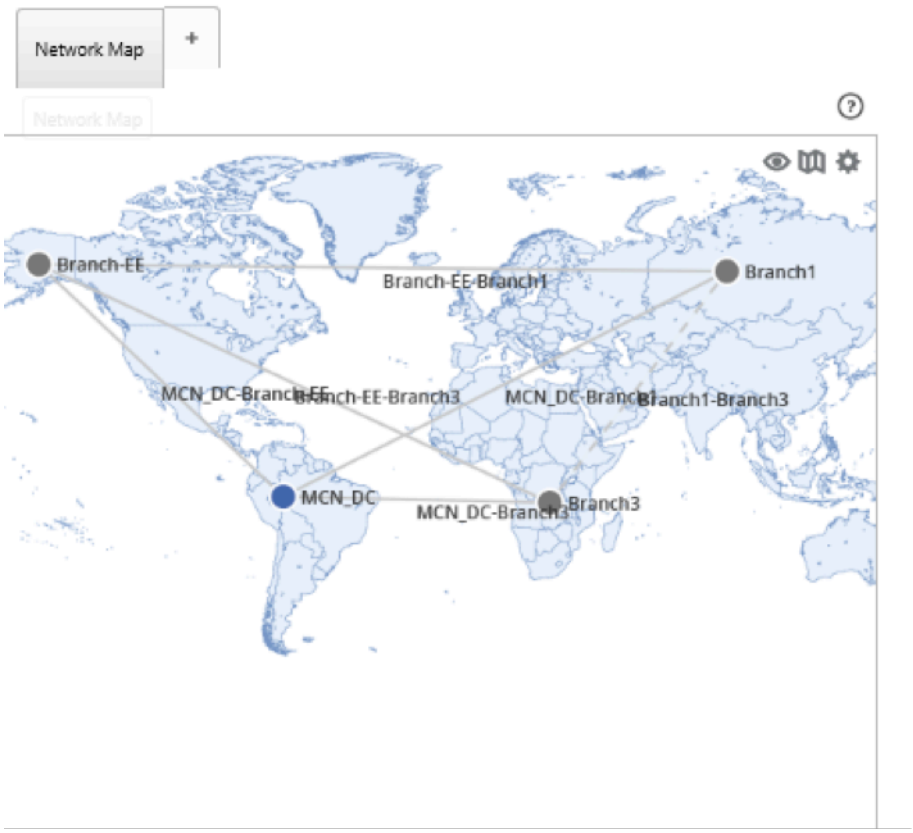
4. Sinon, dans la section **À partir du fichier**, cliquez sur **Parcourir** et sélectionnez une configuration à télécharger à partir de votre ordinateur.
5. Dans le champ **Importer** dans, sélectionnez **Package actuel** pour importer le contenu du fichier sélectionné dans le package ouvert en cours.
6. Dans le champ **Utiliser les cartes réseau à partir de**, sélectionnez l'une des options suivantes.

   - **Package actuel** : Conservez l'ensemble de cartes réseau actuellement enregistré après l'importation.
   - **Nouveau package** : utilisez les cartes réseau du package importé et ignorez l'ensemble actuel de cartes.
   - **Les deux packages** : utilisez les cartes importées en plus des cartes actuellement enregistrées.

7. Cliquez sur **Importer**. La configuration est importée.



8. Dans la section **Carte réseau**. Cliquez sur l'icône Paramètres et sélectionnez **Remplissage automatique** pour ajouter et organiser automatiquement chaque site de la configuration sur la carte.



Gérer la base

February 17, 2022

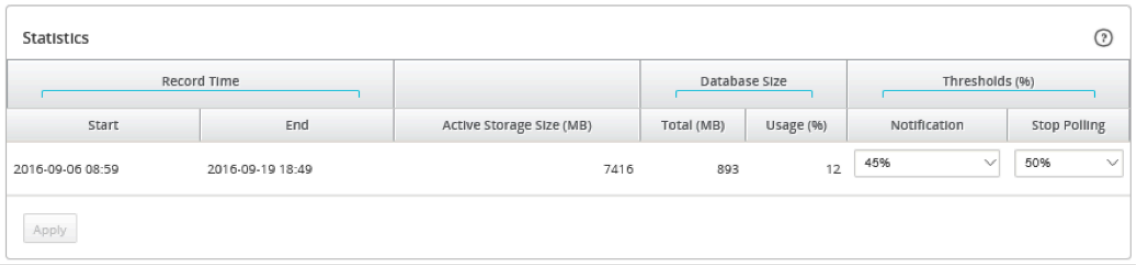
Vous pouvez surveiller et gérer la base de données pour vous assurer qu'il y a suffisamment d'espace disque disponible pour stocker les données d'interrogation de toutes les appliances découvertes sur le réseau.

Affichage des statistiques de la base

La table **Statistiques** affiche les statistiques de base de données disponibles et inclut des champs d'entrée permettant de spécifier les seuils d'utilisation du disque de base de données pour les notifications et l'interrogation.

Pour afficher les statistiques de base de données :

1. Dans l'interface utilisateur Web du Citrix SD-WAN Center, cliquez sur l'onglet **Administration**.
2. Cliquez sur **Gestion de base de données**. Sous la section **Statistiques**, les informations suivantes s'affichent.
    - **Heure de l'enregistrement :** affiche la date et l'horodatage des enregistrements les plus anciens et les plus récents de la base de données. Cette colonne contient les informations suivantes :
        - **Début :** affiche la date et l'horodatage de l'enregistrement le plus ancien de la base de données.
        - **Fin** : affiche la date et l'horodatage de l'enregistrement le plus récent de la base de données.
    - **Taille du stockage actif (Mo)** : affiche l'espace disque actuel du stockage actif.
    - **Taille de la base de données (Mo)** : affiche la taille actuelle de la base de données et les informations d'utilisation. Cette colonne contient les informations suivantes :
        - **Total (Mo)** : affiche la taille totale en Mo de la base de données.
        - **Utilisation (%)** : affiche le pourcentage d'utilisation du disque de base de données dans l'espace disque actuel du stockage actif.



Pour définir le seuil de notification et d'interrogation :

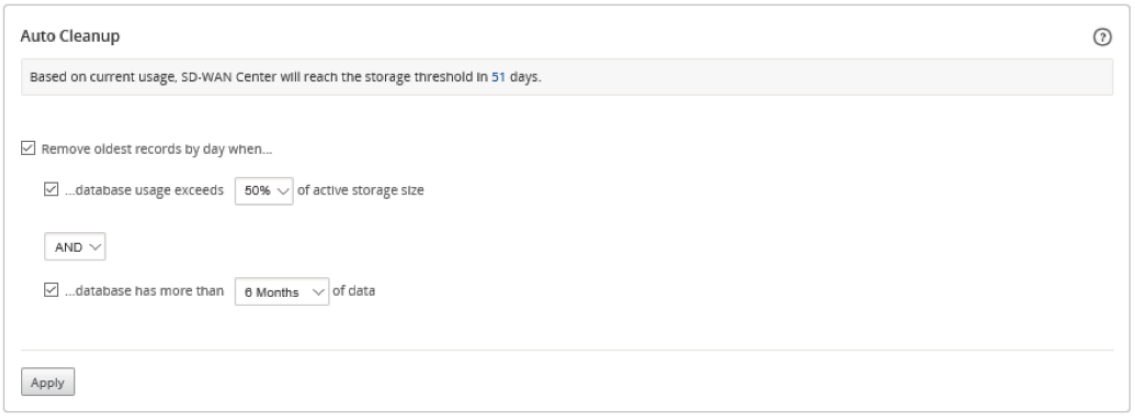
1. Dans le champ **Notification**, entrez le pourcentage de la taille de la base de données ou de la taille de stockage active à utiliser comme seuil pour générer une notification d'utilisation de la base de données. Une notification par e-mail sera envoyée lorsque l'utilisation de la base de données dépasse ce seuil.
2. Dans le champ **Arrêter l'interrogation**, entrez le seuil d'utilisation du disque de base de données (pourcentage) auquel arrêter l'interrogation des statistiques. Sélectionnez une valeur comprise entre **10 %** et **50 %** dans le menu déroulant. La valeur par défaut est **50 %**.
3. Cliquez sur **Apply**.

Configuration du nettoyage automatique

Pour contrôler l'utilisation du disque de base de données, vous pouvez spécifier des seuils qui, lorsqu'ils sont dépassés, déclenchent la suppression d'enregistrements plus anciens de la base de données.

Pour activer le nettoyage de base de données et configurer les seuils :

1. Dans l'interface utilisateur Web du Citrix SD-WAN Center, cliquez sur l'onglet **Administration**.
2. Cliquez sur **Gestion de base de données**.
3. Sous **Nettoyage automatique**, sélectionnez l'option **Supprimer les enregistrements les plus anciens par jour quand…** pour activer le nettoyage de la base de données.



Lorsque cette option est activée, la base de données est automatiquement vérifiée à 2 h 00 tous les jours. La vérification initie un nettoyage de base de données si les seuils spécifiés sont atteints ou dépassés. Par défaut, cette option n'est pas activée.

Auparavant, le paramètre par défaut pour le nettoyage automatique de la base de données SD-WAN Center était le suivant :

- Supprimez les enregistrements les plus anciens par jour lorsque :
  - …l'utilisation de la base de données dépasse 50% de la taille de stockage active
  - L'opérateur doit être sélectionné en tant que AND
  - …la base de données a plus de 6 mois de données

Avec la version 11.1.1 et les versions ultérieures, le paramètre par défaut pour le nettoyage automatique de la base de données SD-WAN Center est maintenant remplacé par le suivant :

- Supprimez les enregistrements les plus anciens par jour lorsque :
  - …l'utilisation de la base de données dépasse 50% de la taille de stockage active
  - L'opérateur doit être sélectionné en tant que OR
  - …la base de données a plus d'un mois de données

> **Remarque**
>
> La modification des paramètres n'aura aucun impact sur les systèmes SD-WAN Center déjà provisionnés qui sont mis à niveau vers la version 11.1.1. Il s'applique uniquement aux systèmes SD-WAN Center version 11.1.1 fraîchement provisionnés ou supérieurs.

4. Sélectionnez **…l'utilisation de la base de données dépasse (%) la taille de stockage active**, puis sélectionnez un pourcentage dans le menu déroulant pour spécifier le seuil d'un nettoyage de base de données. Les options sont de **10%** à **50%** par incréments de **5%**.
5. Sélectionnez **AND**ou **OR**, un opérateur dans le menu déroulant entre les seuils « …base de données dépasse… » et « …base de données a plus de… » pour spécifier à un opérateur comment appliquer cette règle. La valeur par défaut est **OR** depuis la version 11.1.1.
6. Sélectionnez **…la base de données contient plus** de [nombre de mois] **mois de données**, puis sélectionnez le nombre de mois dans le menu déroulant pour spécifier le seuil d'intervalle de temps pour un nettoyage de base de données pour lequel les données doivent être conservées dans la base de données. Les options sont de **1 mois** à **12 mois** par incréments d'un mois.
7. Cliquez sur **Apply**.

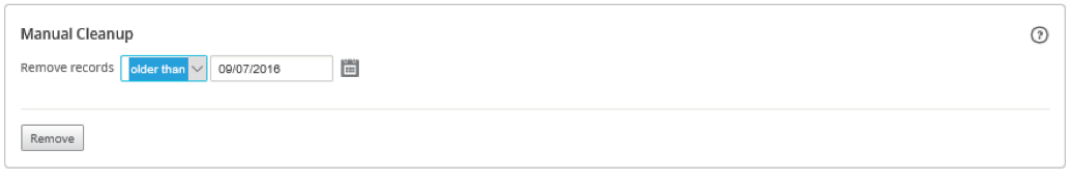
Configuration du nettoyage manuel

Vous pouvez supprimer manuellement des enregistrements de statistiques et d'événements de la base de données, en fonction de critères spécifiés.

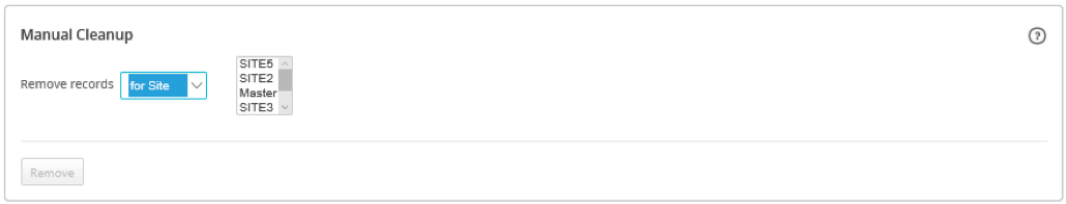
Pour effectuer un nettoyage manuel de base de données :

1. Dans l'interface Web Citrix SD-WAN Center, cliquez sur l'onglet **Administration**.
2. Cliquez sur **Gestion de base de données**.
3. Sous la **section Nettoyage manuel**, sélectionnez un filtre dans le menu déroulant **Supprimer les enregistrements**. Les options de filtre sont les suivantes :

    - **plus anciens que :** supprimez les enregistrements collectés avant une date spécifiée. Lorsque vous sélectionnez ce filtre, un champ de date et un bouton de sélection de calendrier s'affichent. Cliquez sur le bouton Calendrier pour sélectionner une date. Tous les enregistrements antérieurs à la date spécifiée seront supprimés.

    - **pour Site :** supprimez les enregistrements collectés avant une date spécifiée. Lorsque vous sélectionnez ce filtre, un champ de date et un bouton de sélection de calendrier s'affichent. Cliquez sur le bouton Calendrier pour sélectionner une date. Tous les enregistrements antérieurs à la date spécifiée seront supprimés.

4. Cliquez sur **Supprimer**.

Gérer les vues

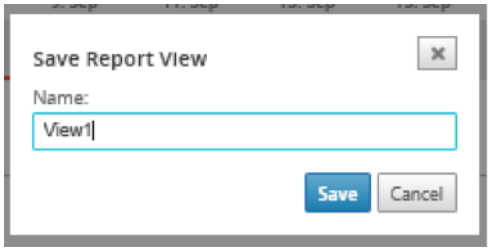
February 17, 2022

La page Fault, Reporting, Carte réseau et Statistiques vous permet de créer, afficher, modifier et supprimer les vues respectives.

> **Remarque**
>
> Les captures d'écran utilisées dans la procédure peuvent varier de l'interface utilisateur réelle en fonction du type de vue.

Pour créer une vue :

1. Cliquez sur **Nouvelle vue**, ce qui crée une nouvelle vue sans nom et réinitialise la spécification de temps à l'heure actuelle.
2. Créez et appliquez des filtres ou apportez les modifications nécessaires.
3. Cliquez sur **Enregistrer sous**.
4. Dans la boîte de dialogue **Enregistrer l'affichage**, entrez un nom pour votre affichage.
5. Cliquez sur **Save**.



Pour ouvrir et modifier une vue existante :

1. Cliquez sur **Ouvrir**.
2. Dans la boîte de dialogue **Ouvrir l'affichage**, sélectionnez une vue de rapport dans la liste déroulante.
3. Cliquez sur **Ouvrir**. La vue des événements s'ouvre.
4. Effectuez les modifications nécessaires au besoin.
5. Cliquez sur **Save**.

Pour supprimer une vue, ouvrez la vue et cliquez sur l'icône Supprimer.

Mise à niveau logicielle

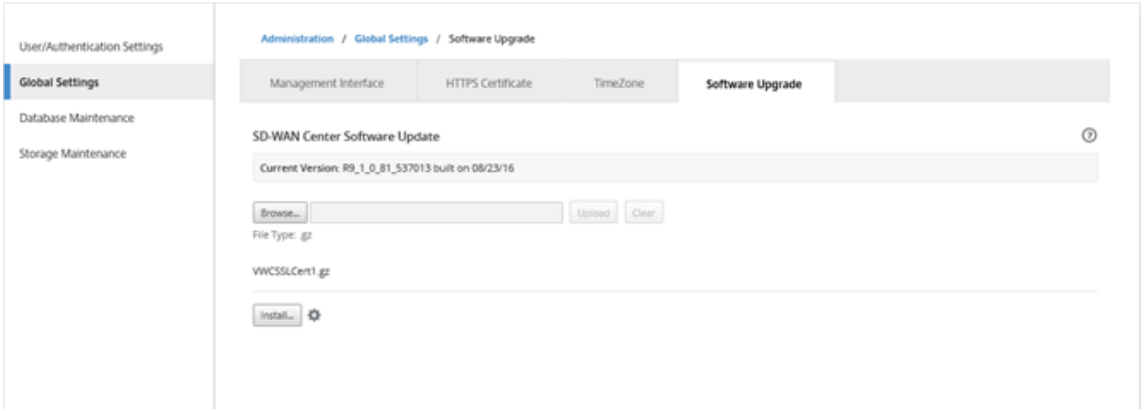
February 17, 2022

Vous pouvez utiliser l'option de mise à niveau logicielle pour effectuer la mise à niveau de votre logiciel Citrix SD-WAN Center vers la dernière version. Le processus de mise à niveau logicielle place Citrix SD-WAN Center en mode maintenance. Si une migration de base de données est requise, ce processus peut prendre plusieurs heures. Pendant ce temps, aucune donnée statistique ne sera collectée à partir du réseau étendu virtuel, et toutes les fonctionnalités du Centre Citrix SD-WAN ne seront pas disponibles.

> **Important**
>
> Il est recommandé d'exécuter la mise à niveau pendant les heures de maintenance.
>
> **Remarque**
>
> Téléchargez le progiciel Citrix SD-WAN Center approprié sur votre ordinateur local. Vous pouvez télécharger ce package à partir de la page Téléchargements .

Pour télécharger et installer une nouvelle version du logiciel Citrix SD-WAN Center

1. Dans l'interface Web Citrix SD-WAN Center, cliquez sur l'onglet **Administration**.
2. Cliquez sur **Paramètres globaux**, puis sur **Mise à niveau logicielle**.



3. Cliquez sur **Parcourir** pour ouvrir un navigateur de fichiers et sélectionnez le progiciel que vous souhaitez télécharger.
4. Cliquez sur **Télécharger** pour charger le package logiciel sélectionné sur la machine virtuelle Citrix SD-WAN Center actuelle.
5. Une fois le téléchargement terminé, cliquez sur **Installer**.
6. Lorsque vous êtes invité à confirmer, cliquez sur **Installer**.
7. Dans la boîte de dialogue qui s'affiche, activez la case à cocher **J'accepte le Contrat de licence utilisateur final**, puis cliquez sur **Installer**.

Contrôles de chronologie

February 17, 2022

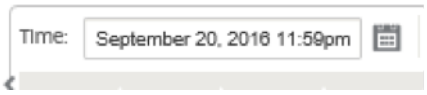
La ligne Montage située en haut de la page Défaillance, Rapport, Carte réseau et Statistiques fournit des contrôles permettant de limiter la période de la vue actuelle. Vous pouvez afficher une période allant jusqu'à 30 jours de données à partir de la base de données actuelle.

> **Remarque**
>
> En fonction de la période sélectionnée, vous pouvez afficher les données historiques indépendamment de la configuration réseau Citrix SD-WAN en cours.

Time

Vous pouvez utiliser les éléments suivants pour spécifier une période pour la vue actuelle :

- **Heure** - Saisissez une date et une heure dans le champ **Heure** pour limiter les résultats du graphique à une date et une heure spécifiques. Le format peut être l'un des formats suivants :
  - ***Jour du mois, Année Heure : Minutes*** [**am** / **pm**] Par exemple : 7 septembre 2015 14h00.
  - ***MM/JJ/AAAA HH:MM*** [**am** / **pm**] Par exemple : 09/07/2015 8:36am.
  - ***M/J/AA H:MM*** [**am** / **pm**] Par exemple : 9/7/15 22h14
- **Calendrier** - (icône Calendrier) Cliquez sur l'icône du calendrier située à droite du champ Heure et sélectionnez une date pour limiter les résultats de l'affichage à cette date.



- **Ligne de temps** - Cliquez et faites glisser vers un autre point d'une chronologie pour sélectionner une période d'au moins 30 minutes.

- **Dernier : Heure / Jour / Semaine / Mois** - Cliquez sur une option (**Heure**, **Jour**, **Semaine** ou **Mois**) pour restreindre les résultats de l'affichage à cette période.

Mode

Le mode Montage détermine la manière dont la chronologie interprète les sélections de période et comment les mises à jour automatiques sont reflétées dans l'affichage actif et dans le tableau de

bord. Il existe deux options de mode, **Relatif** (*période sélectionnée*) et **Absolue** (*période sélectionnée*), où la période sélectionnée est la période spécifiée dans le champ **Temps**.

Pour modifier le mode Montage, sélectionnez **Relatif** ou **Absolu** dans le menu déroulant **Mode** situé dans le coin supérieur droit de la ligne Montage.

Mode relatif

Si vous sélectionnez Mode **Relatif**, la chronologie traite la période spécifiée pour **Temps** comme une heure relative à maintenant. Si vous enregistrez la vue et l'ouvrez ultérieurement, les informations représentées dans la vue seront relatives à l'heure d'ouverture de la vue. Si vous avez activé les mises à jour automatiques et qu'une mise à jour des statistiques est détectée, la vue est mise à jour par rapport à la dernière heure enregistrée dans la base de données.

La période actuellement spécifiée est indiquée entre parenthèses dans le cadre de l'option de menu **Relatif**. Par exemple, si vous avez sélectionné **Dernière : Jour** comme période, l'option **Relative s' affiche comme Relatif** (il y a 1 jour - 1 minute à partir de maintenant).

Mode absolu

Si vous sélectionnez Mode **Absolu**, le scénario traite la période spécifiée pour **Time** : comme des points absolus (statiques) dans le temps. La vue représente toujours l'heure sélectionnée, même si vous l'enregistrez et l'ouvrez ultérieurement, ou si vous activez les mises à jour automatiques. La période actuellement spécifiée est indiquée entre parenthèses dans le cadre de l'option de menu **Absolue**, au format suivant :

Absolute (*start_date start_time-end_date end_time*)

Par exemple, si vous avez sélectionné **Dernière : Jour** comme période et que la date et l'heure actuelles sont 9/7 4:43 PM, l'option **Absolue** s'affiche comme **Absolue (9/6 4:43 PM - 9/7 4:43 PM)**.

Comptes utilisateur

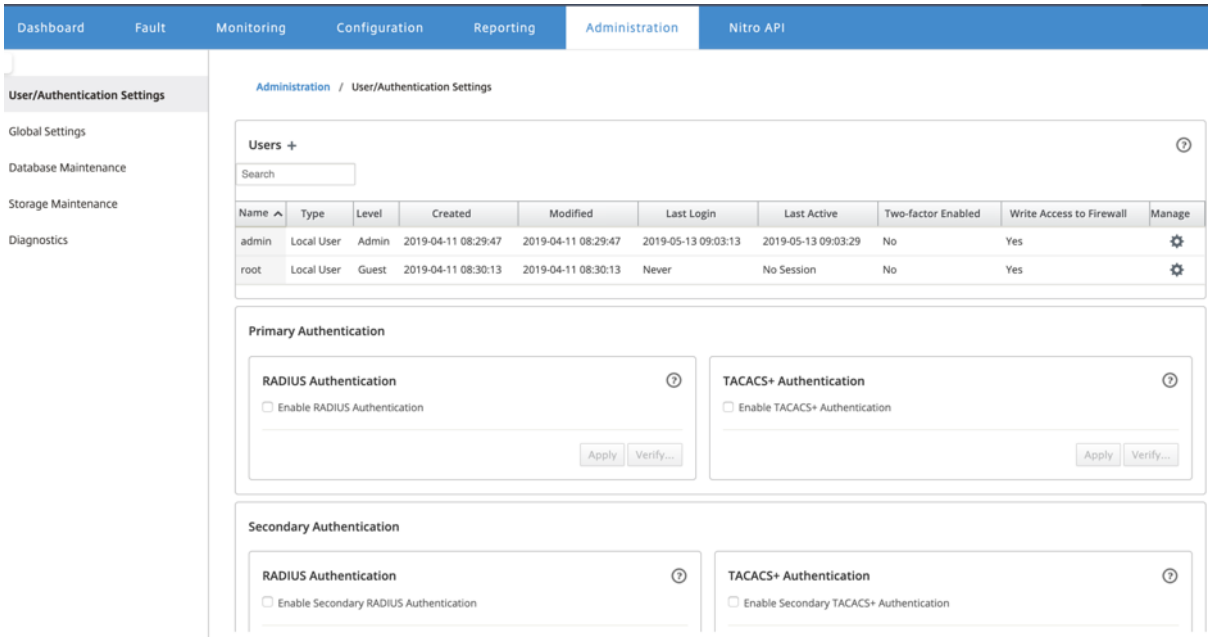
February 17, 2022

Vous pouvez afficher une liste de tous les comptes d'utilisateurs locaux et distants qui se sont connectés à la machine virtuelle Citrix SD-WAN Center au moins une fois. Les comptes d'utilisateurs distants sont authentifiés via les serveurs d'authentification RADIUS ou TACACS +. Vous pouvez également ajouter un nouveau compte d'utilisateur local à Citrix SD-WAN Center.

> **Remarque**
>
> Si un compte utilisateur est disponible sur un serveur d'authentification distant mais n'est jamais utilisé pour ouvrir une session sur Citrix SD-WAN Center, il n'est pas affiché dans la liste **Utilisateurs**.

Pour afficher les comptes d'utilisateurs dans l'interface Web du SD-WAN Center, accédez à **Administration > Paramètres d'utilisateur/d'authentification**.

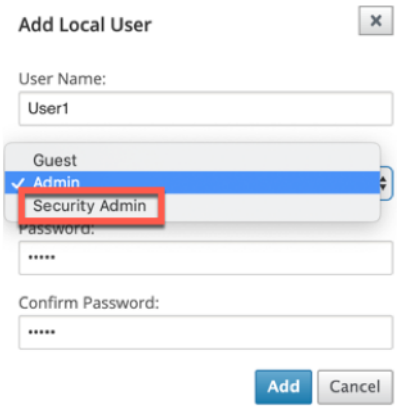
Une liste de comptes d'utilisateurs apparaît dans la section **Utilisateurs**.



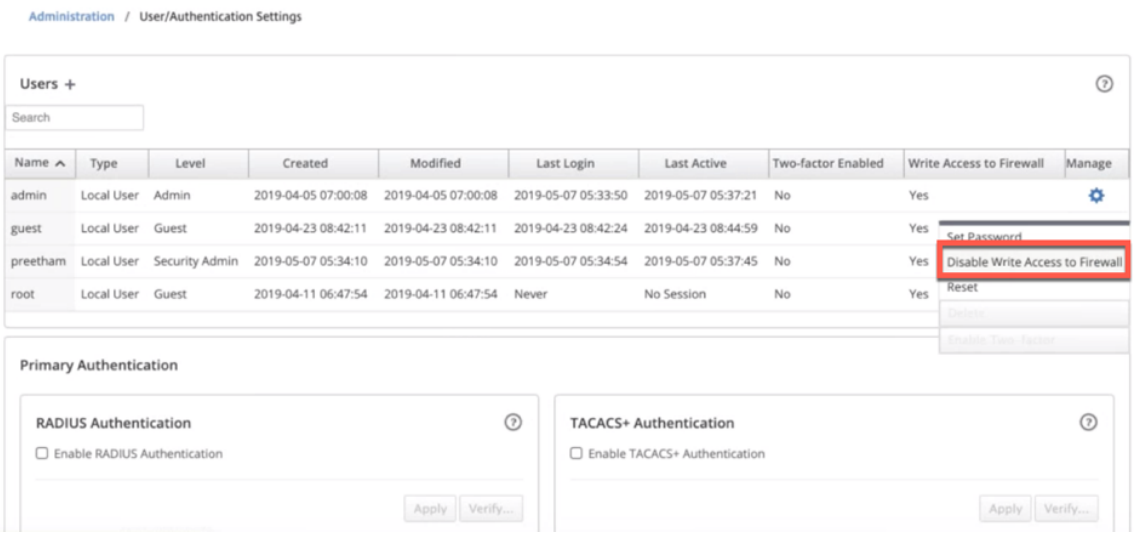
Les informations suivantes s'affichent :

- **Nom : Nom** d'utilisateur.
- **Type** : Type de compte d'utilisateur, il peut s'agir de l'un des éléments suivants :
  - **Local : les comptes** d'utilisateurs créés et gérés localement à l'aide de l'interface SD-WAN Center.
  - **RADIUS** : comptes d'utilisateurs distants authentifiés par le serveur RADIUS.
  - **TACACS +** : Comptes d'utilisateurs distants authentifiés par le serveur TACACS +.
- **Niveau :** Les trois niveaux de privilège du compte sont les suivants :
  - **Admin** : Le compte administrateur dispose de privilèges d'administration. Il dispose d'un accès en lecture-écriture à toutes les sections.
  - **Invité** : Compte invité est un compte en lecture seule avec accès à la page **Tableau de bord**, **Rapports**et **Monitoring** .

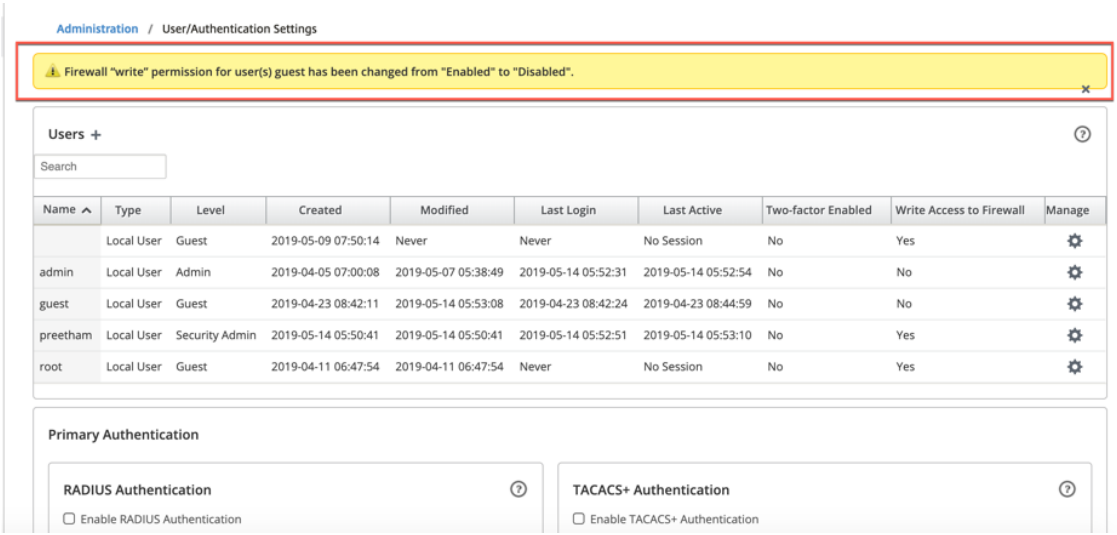
- Administrateur**de sécurité** : un **administrateur de sécurité**dispose d'un accès en lecture-écriture uniquement pour le pare-feu et les paramètres liés à la sécurité dans l'**Éditeur de configuration**, tout en disposant d'un accès en lecture seule aux sections restantes.



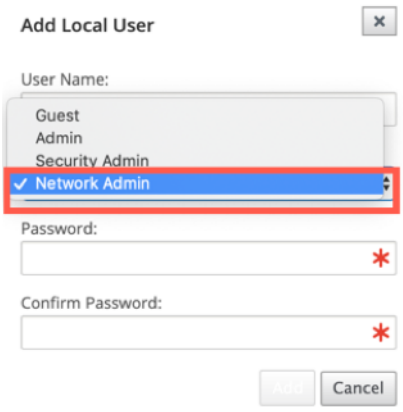
> **REMARQUE**
>
> * Seuls l'administrateur et l'administrateur de sécurité peuvent modifier ou modifier la configuration de la fonctionnalité de sécurité.
> * L'administrateur de sécurité peut activer ou désactiver l'accès en écriture au pare-feu pour tous les comptes d'utilisateurs à l'exception du super administrateur.



Une barre de notification apparaît pour tous les utilisateurs une fois que l'administrateur de sécurité a modifié l'autorisation d'écriture du pare-feu pour un utilisateur spécifique. Cette notification est affichée par utilisateur et chaque utilisateur connecté doit par conséquent accusé réception de l'avertissement pour qu'il soit supprimé.



- **Administrateur réseau** : un **administrateur réseau** dispose d'autorisations en lecture-écriture sur toutes les sections et peut fournir une branche entièrement à l'exception du pare-feu et des paramètres liés à la sécurité dans l'Éditeur de configuration.



  Le nœud de pare-feu hébergé n'est pas disponible pour l'administrateur réseau. Dans ce cas, l'administrateur réseau doit importer une nouvelle configuration. Les paramètres liés au réseau et à la sécurité sont gérés par le super administrateur (Admin).

L'administrateur réseau et l'administrateur de sécurité peuvent apporter des modifications à la configuration et la déployer sur le réseau.

> **REMARQUE**
>
> L'administrateur réseau et l'administrateur de la sécurité ne peuvent pas ajouter ou supprimer des comptes utilisateur. Ils ne peuvent modifier que leurs propres mots de passe de compte.

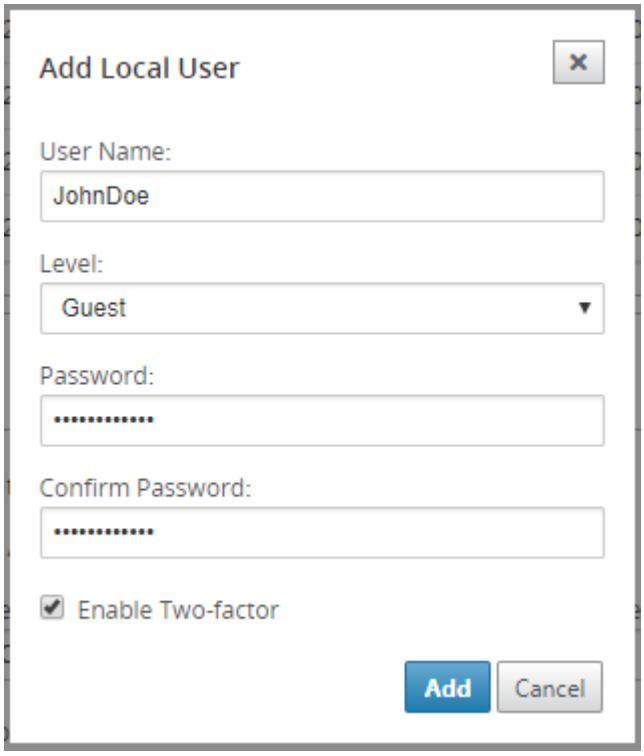
- **Créé** : pour les comptes d'utilisateurs locaux, date à laquelle le compte d'utilisateur a été créé. Pour un compte d'utilisateur distant, date de la première session de connexion.
- **Modifié** : pour les comptes d'utilisateurs locaux, date à laquelle le mot de passe a été modifié pour la dernière fois. Pour les utilisateurs distants, date de la première session de connexion.

- **Dernière connexion** : date à laquelle l'utilisateur s'est connecté pour la dernière fois. Une info-bulle affiche l'adresse IP du périphérique utilisé pour se connecter.
- **Dernière activité** : date à laquelle la dernière demande a été faite au serveur. Une info-bulle affiche l'adresse IP du périphérique utilisé pour se connecter.
- **Gérer :** cliquez sur l'icône d'engrenage pour afficher un menu contenant les options suivantes :
  - **Définir le mot de passe** : Changer le mot de passe pour le compte d'utilisateur local. Le mot de passe racine actuel est requis pour modifier le mot de passe root. Vous ne pouvez pas modifier les mots de passe des comptes d'utilisateurs distants.
  - **Réinitialiser** : supprimez les espaces de travail et les préférences de ce compte d'utilisateur.
  - **Supprimer** : supprimez le compte d'utilisateur local, les espaces de travail et les préférences du SD-WAN Center. Vous ne pouvez pas supprimer les comptes distants et administrateurs.
  - **Deux facteurs activés :** activez l'authentification à deux facteurs pour le compte d'utilisateur local et distant. Pour plus d'informations, consultez Authentification à deux facteurs.
- **Accès en écriture au pare-feu** : indique que l'accès en écriture au pare-feu est activé ou désactivé.

Pour ajouter un nouveau compte d'utilisateur local au Citrix SD-WAN Center :

> **Remarque**
>
> Les comptes d'utilisateurs créés localement sur Citrix SD-WAN Center n'ont pas le privilège de modifier et d'exporter le package de configuration réseau vers le MCN.

1. Cliquez sur l'icône Ajouter + en regard de **Utilisateurs**. **La boîte de dialogue Ajouter un utilisateur local** s'affiche.



2. Entrez des valeurs pour les paramètres suivants :

   - **Nom d'utilisateur** : nom d'utilisateur du compte d'utilisateur local.
   - **Niveau** : le privilège du compte. Un compte d'utilisateur invité est un compte en lecture seule limité à l'affichage du tableau de bord, des rapports et des statistiques. Le compte d'utilisateur invité n'a pas le privilège de modifier et d'exporter le package de configuration réseau vers le MCN.
   - **Mot de passe** : mot de passe du compte utilisateur.
   - **Confirmer le mot de passe** : Entrez à nouveau le mot de passe pour confirmation.

3. Sélectionnez **Activer deux facteurs** pour activer l'authentification à deux facteurs pour le compte d'utilisateur local.

   > **Remarque**
   >
   > L'option **Activer deux facteurs** s'affiche uniquement lorsque le serveur d'authentification secondaire est configuré.
   >
   > Configurez un serveur d'authentification secondaire, soit l'authentification RADIUS, soit l'authentification TACAS +. Assurez-vous que le compte d'utilisateur est configuré sur le serveur d'authentification secondaire. Pour plus d'informations, consultez Authentification secondaire.

4. Cliquez sur **Ajouter**.Le nouveau compte d'utilisateur est créé et les informations de compte sont ajoutées à la table **Utilisateurs**.

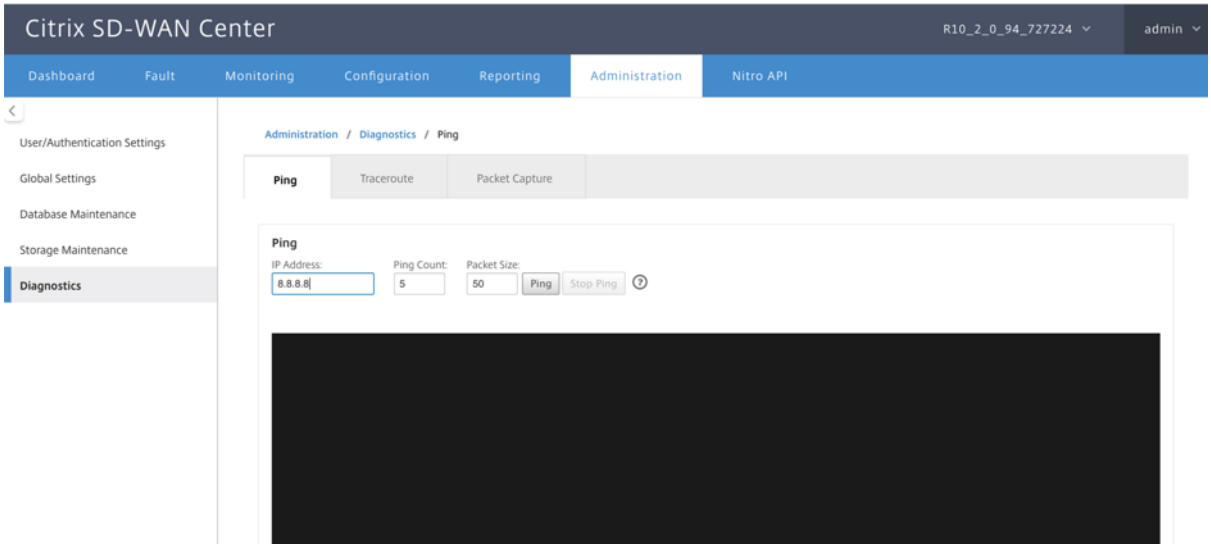
> **Remarque**
>
> Citrix SD-WAN Center peut avoir jusqu'à 600 utilisateurs locaux.

Diagnostics

February 17, 2022

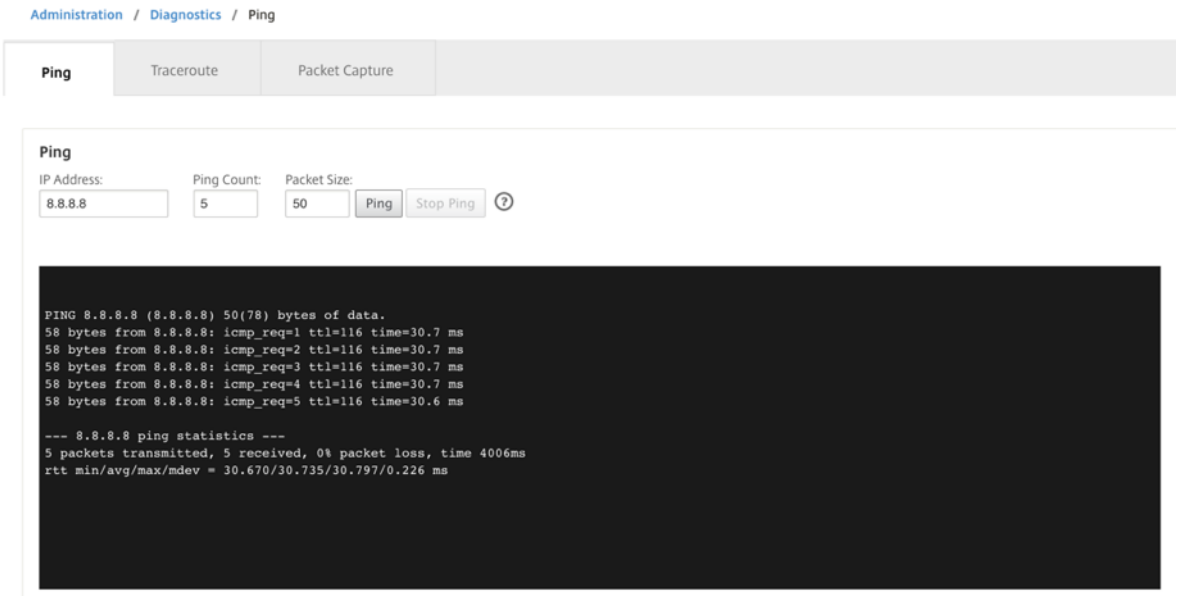
Les utilitaires**Citrix SD-WAN Center Diagnostics** fournissent les fonctionnalités Ping, Traceroute et Capture de paquets pour tester et étudier les problèmes de connectivité sur l'appliance Citrix SD-WAN Center. Les options de diagnostic du tableau de **bord Citrix SD-WAN Center contrôlent la collecte des données**.

Pour utiliser l'outil Diagnostics, accédez à **Administration > Diagnostics**.



Ping

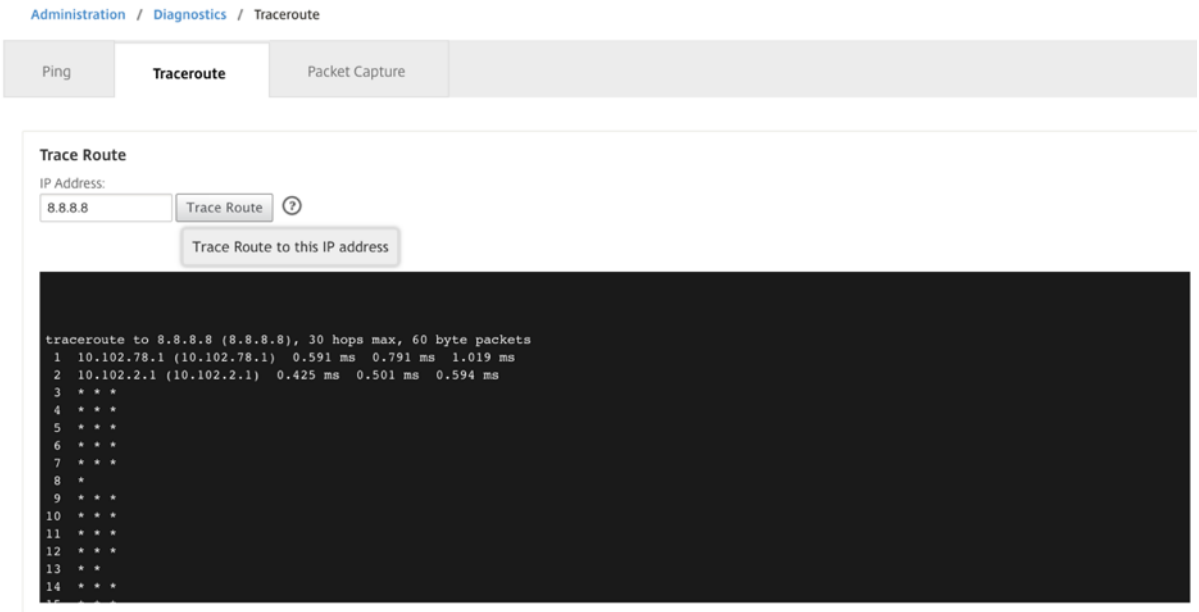
Vous pouvez effectuer un ping sur n'importe quelle adresse IP de gestion dans le réseau SD-WAN Center à l'aide de l'option **Ping**.



Indiquez une adresse IP valide ainsi que le nombre de nombres ping (nombre de fois pour envoyer la demande ping) et la taille des paquets (nombre d'octets de données). Cliquez sur **Arrêter le ping** pour arrêter une recherche ping en cours.

Traceroute

Utilisez l'option **Traceroute** pour vous assurer que les adresses IP sont accessibles. Vous pouvez appliquer traceroute n'importe à quelle adresse IP de gestion dans le réseau en affichant l'itinéraire et en mesurant les délais de transit des paquets.

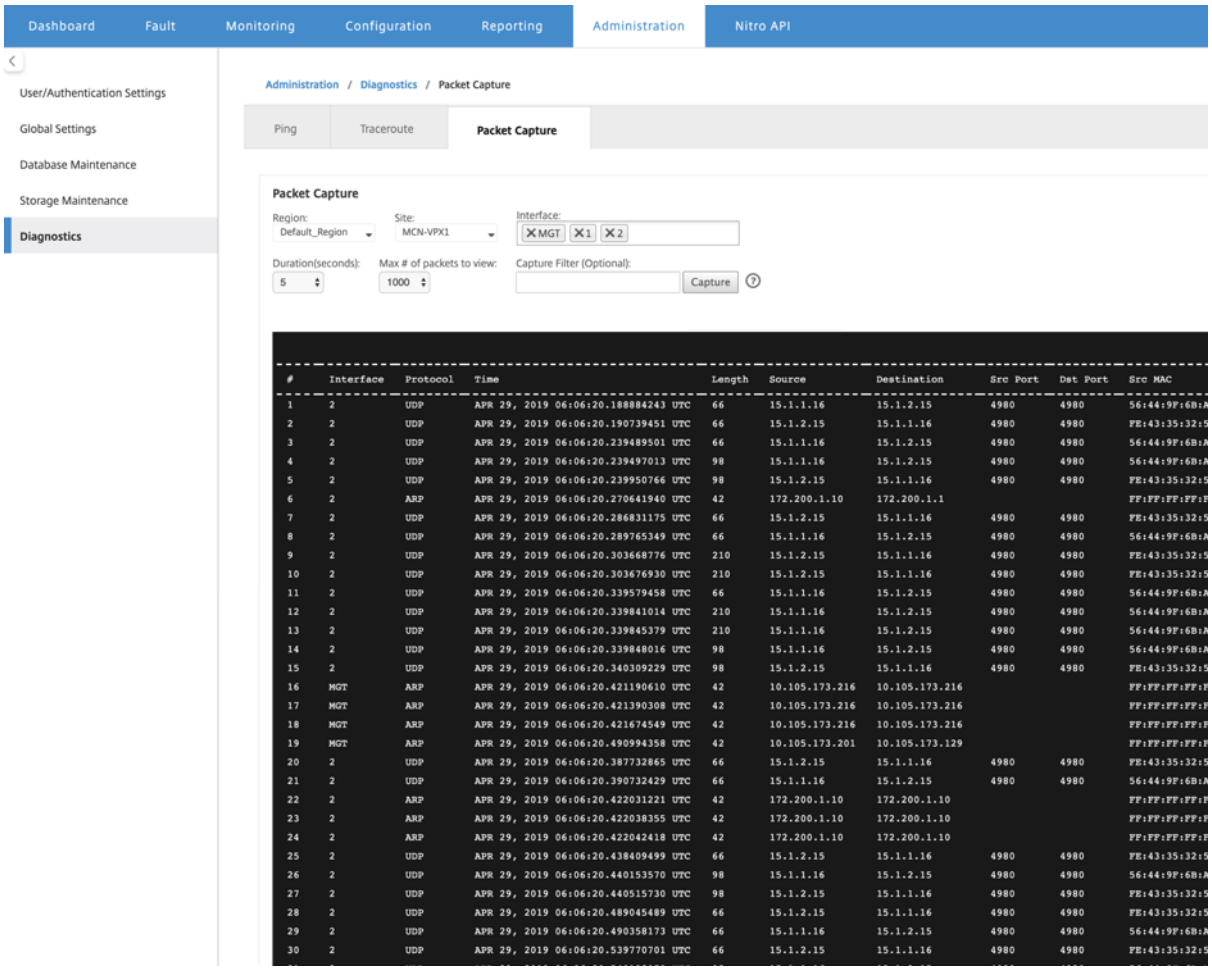


Entrez une adresse IP de gestion valide pour suivre l'itinéraire. Cliquez sur **Tracer l'itinéraire**.

> **REMARQUE :**
>
> Le résultat traceroute affiche un maximum de 30 sauts.

Capture de paquets

Utilisez l'option **Capture de paquets** pour intercepter le paquet de données qui traverse l'interface active sélectionnée présente dans le site sélectionné.



Fournissez les entrées suivantes pour l'opération de capture de paquets :

- **Région** : sélectionnez une région gérée par le SD-WAN Center dans la liste déroulante.
- **Site** - Sites disponibles dans la région sélectionnée. Sélectionnez un site dans la liste déroulante.
- **Interface** - Des interfaces actives sont disponibles pour la capture de paquets dans le site sélectionné. Sélectionnez une interface ou ajoutez des interfaces dans la liste déroulante. Sélectionnez au moins une interface pour déclencher une capture de paquets.

> **REMARQUE :**
>
> La possibilité d'exécuter la capture de paquets sur toutes les interfaces simultanément permet d'accélérer la tâche de dépannage.

- **Durée (secondes)** : durée (en secondes) pendant laquelle les données doivent être capturées.
- **Nombre maximal de paquets à afficher :** limite maximale de paquets à afficher dans le résultat de la capture de paquets.
- **Filtre de capture (facultatif)** - Le champ **Filtre de capture** facultatif accepte une chaîne de filtre utilisée pour déterminer quels paquets sont capturés. Les paquets sont comparés à la chaîne de filtre et si le résultat de la comparaison est vrai, alors le paquet est capturé. Si le filtre est vide, tous les paquets sont capturés. Pour plus d'informations, consultez la section Filtres de capture.

  Voici quelques exemples de ce filtre de capture :

  - **Ether proto \ ARP** - Capture uniquement les paquets ARP
  - **Ether proto \ IP** - Capture uniquement les paquets IPv4
  - **VLAN 100** - Capture uniquement les paquets avec un VLAN de 100\
  - **Host 10.40.10.20** - Capture uniquement les paquets IPv4 vers ou depuis l'hôte avec l'adresse 10.40.10.20
  - **Net 10.40.10.0 Mask 255.255.255.0** - Capture uniquement les paquets IPv4 dans le sous-réseau 10.40.10.0/24
  - **IP proto \ TCP** - Capture uniquement les paquets IPv4/TCP
  - **Port 80** : capture uniquement les paquets IP vers ou depuis le port 80
  - **Plage de ports 20—30** - Capture uniquement les paquets IP vers ou depuis les ports 20 à 30
  - **Hôte 10.40.10.20 et Port 80 et TCP** - Capture uniquement les paquets IP vers ou depuis le port TCP 80 sur l'hôte 10.40.10.20

> **Remarque :**
>
> La taille maximale du fichier de capture est de 575 Mo. Une fois que le fichier de capture de paquets atteint cette taille, la capture de paquets est arrêtée.

Cliquez sur **Capture** pour afficher le résultat de la capture de paquets.