Périphériques de périphérie WAN NFVIS intégrés

Table des matières

Introduction

Ce document décrit le processus d'intégration de systèmes compatibles NFVIS dans un environnement Catalyst™ SD-WAN pour la gestion et l'exploitation.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco SDWAN
- VIS-NFV
- Plug-and-Play (PNP)

Il est présumé que :

- Les contrôleurs SD-WAN (vManage, vBond et vSmart) sont déjà déployés avec des certificats valides.
- Cisco WAN Edge (NFVIS dans ce cas) est accessible à l'orchestrateur vBond et à d'autres

contrôleurs SD-WAN qui sont accessibles via des adresses IP publiques sur le(s) transport(s) WAN
- La version NFVIS doit être conforme au Guide de compatibilité des composants de contrôle.

Composants utilisés

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Matériel

- C8300-UCPE-1N20 (mais peut être appliqué à toute plate-forme compatible NFVIS)

le logiciel Cisco IOS

- vManage 20.14.1
- vSmart et vBond 20.14.1
- NFVIS 4.14.1

Workflow PnP

La fiabilité des périphériques de périphérie WAN est assurée à l'aide des certificats de chaîne racine préchargés en fabrication, chargés manuellement, distribués automatiquement par vManage ou installés lors du processus de provisionnement du déploiement automatisé PnP ou ZTP.

La solution SD-WAN utilise un modèle de liste d'autorisation, ce qui signifie que les périphériques de périphérie WAN qui sont autorisés à rejoindre le réseau de superposition SDWAN doivent être connus au préalable par tous les contrôleurs SD-WAN. Pour ce faire, ajoutez les périphériques de périphérie WAN dans le portail de connexion Plug-and-Play (PnP) à l'adresse https://software.cisco.com/software/pnp/devices

Cette procédure exige toujours que le périphérique soit identifié, approuvé et autorisé dans le même réseau de superposition. L'authentification mutuelle doit avoir lieu sur tous les composants SD-WAN avant d'établir des connexions de contrôle sécurisées entre les composants SD-WAN dans le même réseau de superposition. L'identité du périphérique WAN Edge est identifiée de manière unique par l'ID du châssis et le numéro de série du certificat. Selon le routeur de périphérie WAN, les certificats sont fournis de différentes manières :

- vEdge basé sur le matériel : Le certificat est stocké dans la puce TPM (Tamper Proof Module) intégrée installée lors de la fabrication.
- Cisco IOS®-XE SD-WAN matériel : Le certificat est stocké dans la puce SUDI embarquée installée lors de la fabrication.
- Plate-forme virtuelle ou périphériques Cisco IOS-XE SD-WAN : aucun certificat racine (tel que la plate-forme ASR1002-X) n'est préinstallé sur le périphérique. Pour ces périphériques,

un mot de passe à usage unique (OTP) est fourni par vManage pour authentifier le périphérique avec les contrôleurs SD-WAN.

Un serveur DHCP doit être disponible pour effectuer la mise en service automatique (ZTP). Dans le cas contraire, une adresse IP peut être attribuée manuellement pour poursuivre les étapes restantes du processus Plug-and-Play (PnP).

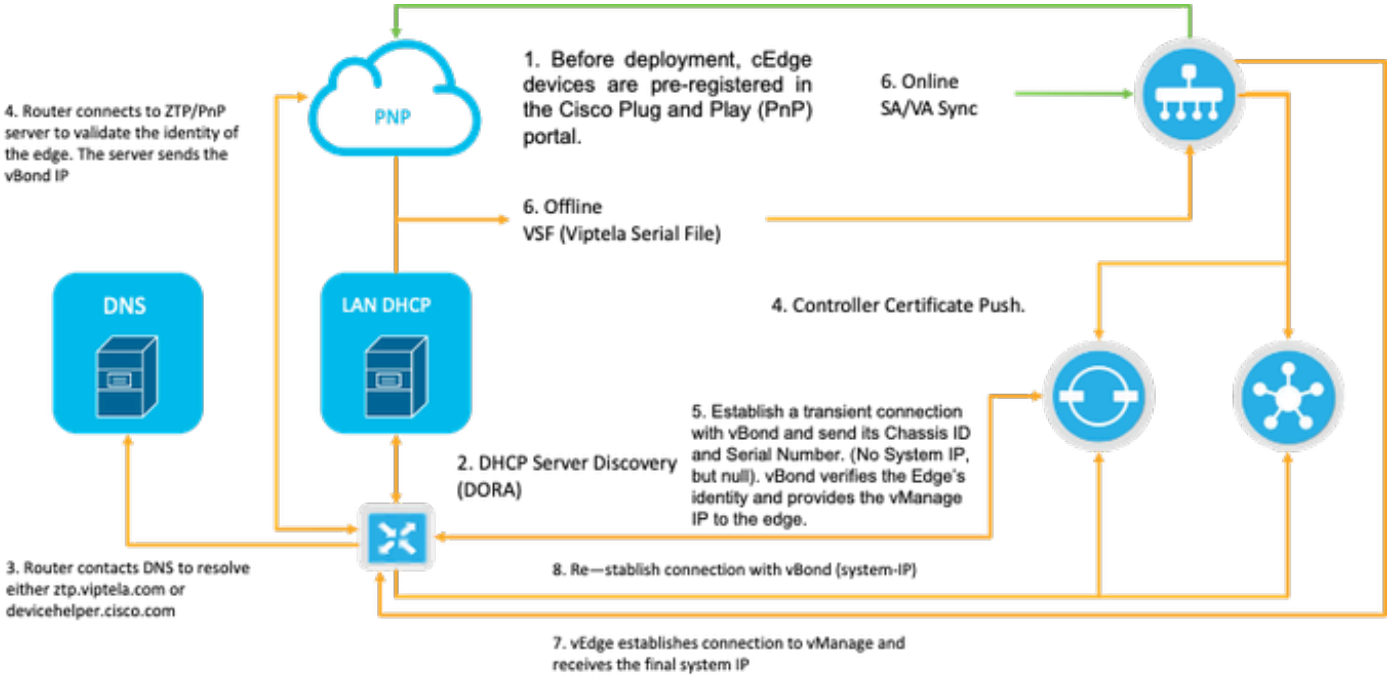


Fig. 1. Diagramme de workflow de confiance des périphériques Plug and Play et WAN Edge.

Intégration sécurisée de l'appareil compatible NFVIS

Récupérer le numéro de série et le certificat

La puce matérielle SUDI (Secure Unique Device Identifier) du matériel compatible NFVIS est utilisée pour garantir que seuls les périphériques autorisés peuvent établir un tunnel TLS ou DTLS sécurisé vers l'orchestrateur SD-WAN Manager. Recueillez le numéro de série correspondant à l'aide de la commande support show chassis executive level :

```
C8300-UCPE-NFVIS# support show chassis
Product Name              : C8300-UCPE-1N20
Chassis Serial Num        : XXXXXXXXX
Certificate Serial Num    : XXXXXXXXXXXXXXXXX
```

Ajout du périphérique au portail Plug and Play

Accédez à https://software.cisco.com/software/pnp/devices et sélectionnez le compte Smart et le compte virtuel appropriés pour votre environnement d'utilisateur ou de laboratoire. (si plusieurs

comptes Smart portent le même nom, vous pouvez les distinguer de l'identificateur de domaine).

Si vous ou votre utilisateur ne savez pas avec quel compte Smart (SA) / compte virtuel (VA) travailler, vous pouvez toujours rechercher et numéro de série existant/intégré dans le lien texte « Recherche de périphérique » pour voir à quel SA/VA il appartient.

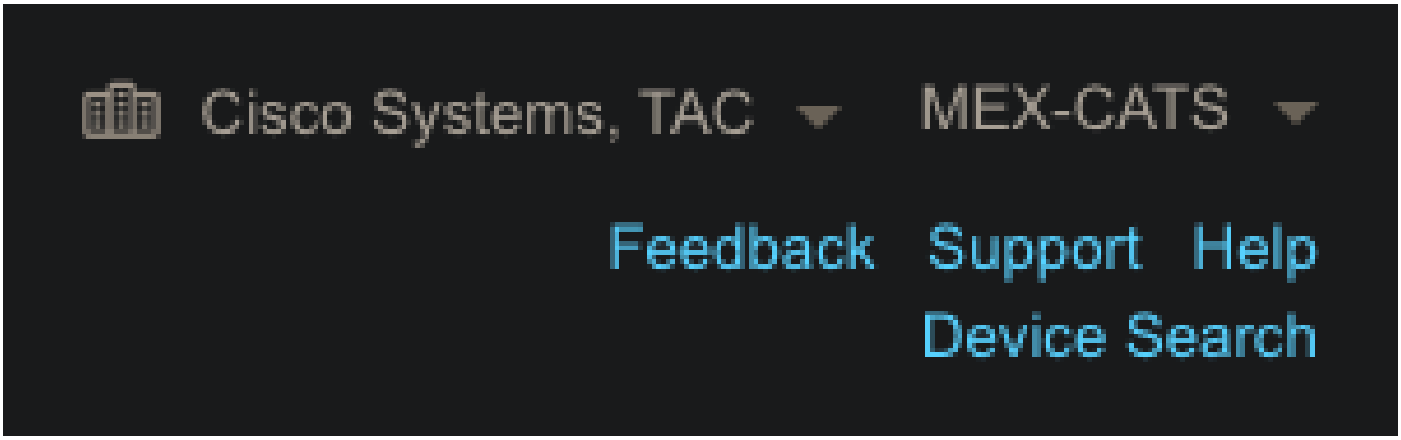


Fig. 2. Bouton Sélection SA/VA et Recherche de périphériques.

Une fois la SA/VA sélectionnée, cliquez sur « Ajouter des périphériques... » :

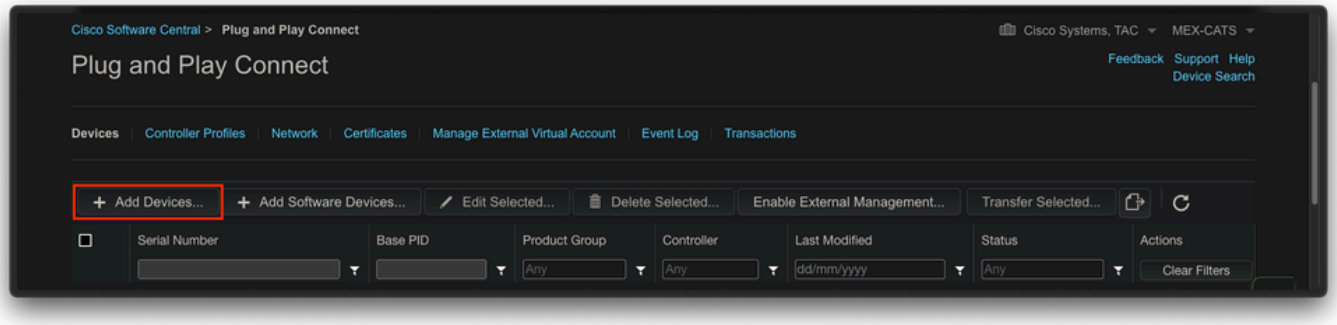


Fig. 3. « Ajouter des périphériques... » Bouton sur lequel cliquer pour enregistrer le périphérique physique.

Pour ce cas particulier, à bord d'un seul périphérique, une saisie manuelle suffit :

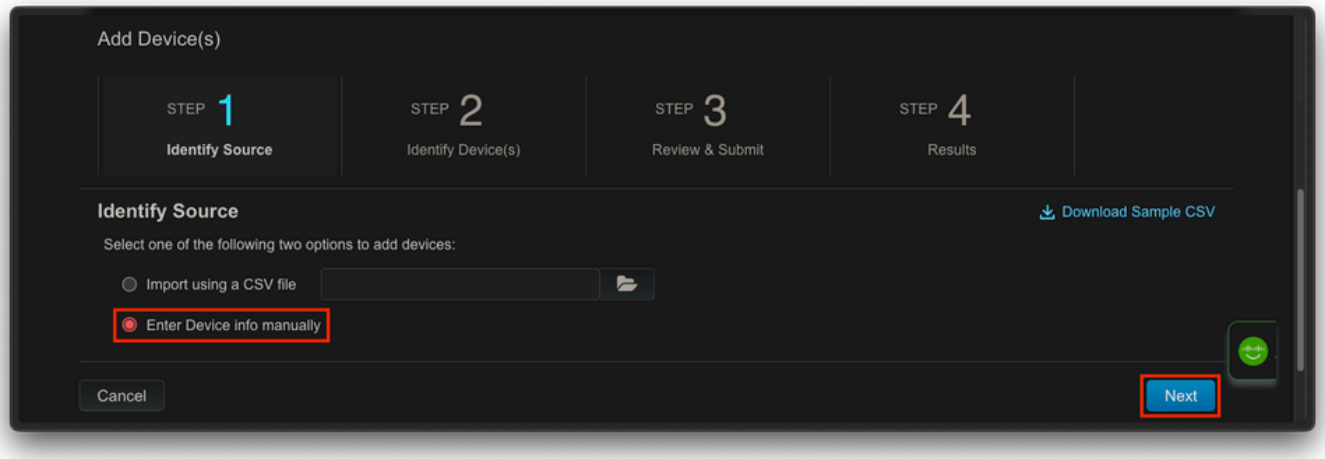


Fig. 4. Alternative "Add Devices..." pour la saisie d'informations sur les périphériques, manuelle (individuelle) ou CSV (multiple).

Pour l'étape 2, cliquez sur le bouton « + Identifier le périphérique... ». Un mode Formulaire apparaît. Complétez les détails avec les informations affichées sur le résultat de la commande support show chassis de NFVIS et sélectionnez le profil de contrôleur vBond correspondant.

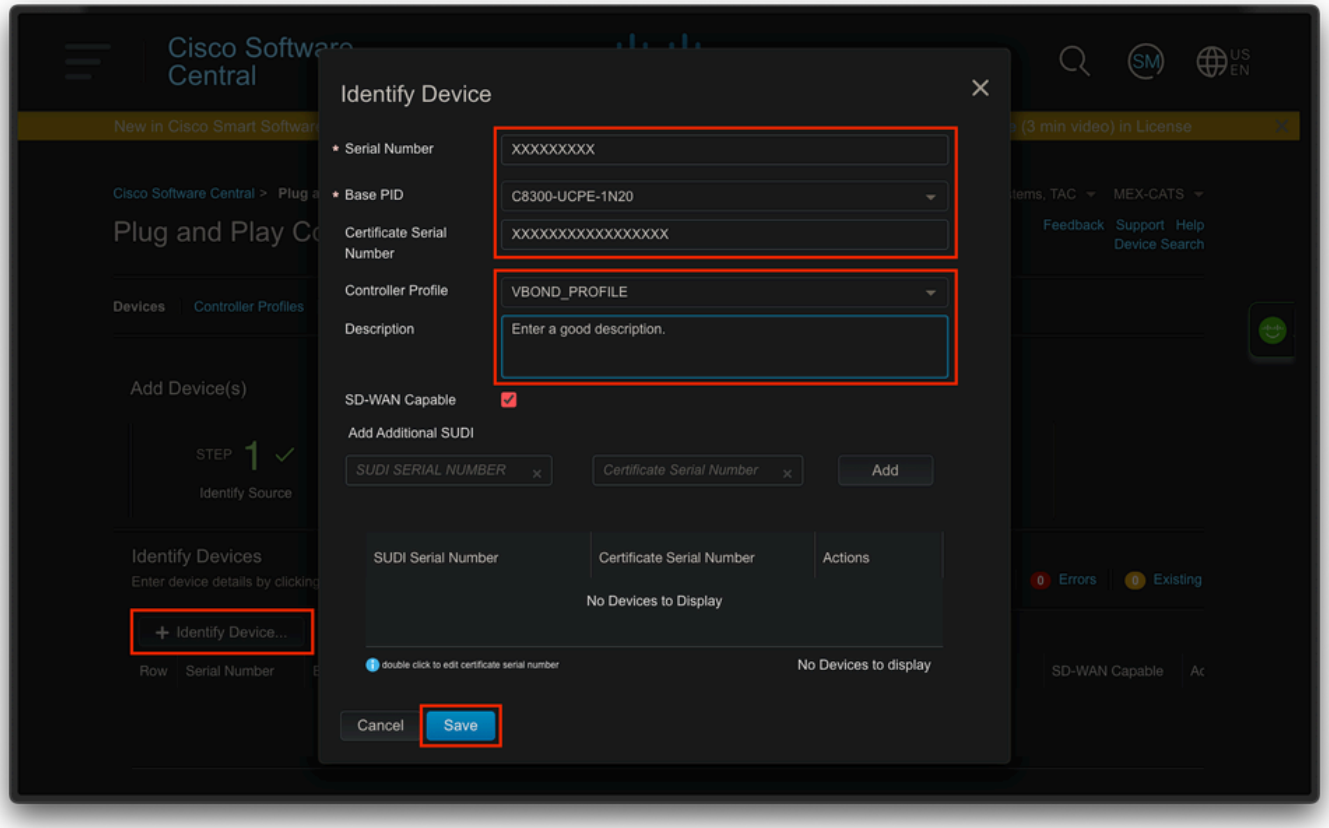


Fig. 5. Formulaire d'identification du dispositif.

Une fois qu'il est enregistré, cliquez sur Next pour l'étape 3 et enfin sur Submit pour l'étape 4.

PnP dans NFVIS

Pour plus d'informations sur les divers paramètres de configuration pour PnP dans NFVIS, couvrant à la fois les modes automatique et statique, veuillez vous référer à la ressource : [Commandes PnP NFVIS.]

Il est à noter que PnP est activé par défaut sur toutes les versions NFVIS.

vManage Synchronization avec PnP

Mode en ligne

Si vManage peut accéder à Internet et au portail Plug and Play, vous devez être en mesure d'effectuer une synchronisation SA/VA. Pour cela, accédez à Configuration > Devices, et cliquez

sur un bouton de texte qui indique Sync Smart Account. Les informations d'identification utilisées pour la connexion à Cisco Software Central sont requises. Assurez-vous d'envoyer le certificat à tous les contrôleurs.

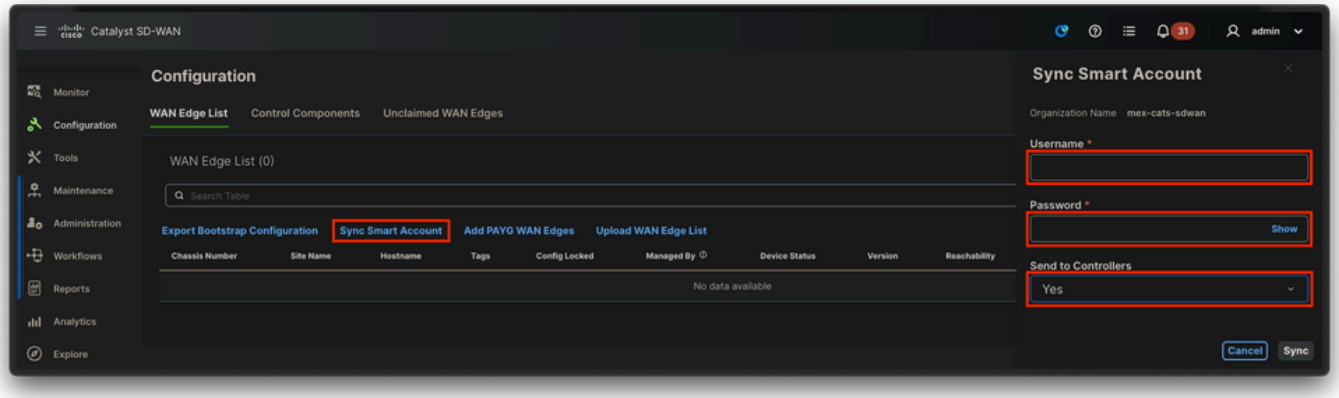


Figure 6. Mise à jour du routeur de périphérie WAN via la synchronisation SA/VA

Mode hors connexion

Si vManage se trouve dans un environnement de travaux pratiques ou n'a pas d'accès à Internet, vous pouvez télécharger manuellement un fichier d'approvisionnement à partir du Plug and Play qui doit contenir le numéro de série ajouté à la liste des périphériques. Ce fichier est de type .viptela (Viptela Serial File), qui peut être obtenu à partir de l'onglet «Profils de contrôleur» :

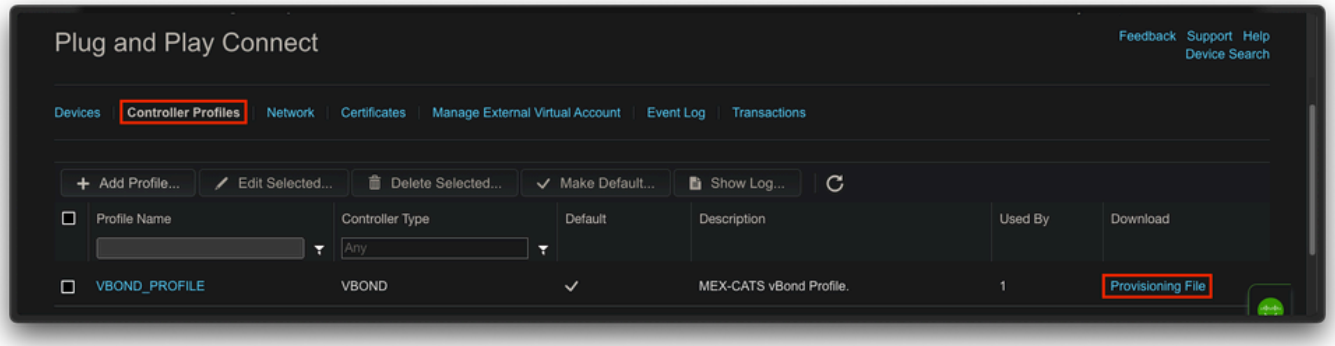


Fig. 7. Téléchargement du fichier d’approvisionnement pour la mise à jour de la liste CEdge WAN.

Pour le téléchargement manuel du fichier d'approvisionnement, accédez à Configuration > Devices, et cliquez sur un bouton de texte qui indique Upload WAN Edge List. Une barre latérale apparaît où vous pouvez faire glisser et déposer le fichier respectif (si le bouton Upload ne surligne pas après que ces actions ont été faites, cliquez sur Choisir un fichier et recherchez le fichier manuellement dans la fenêtre d'exploration de fichier pop-up). Assurez-vous d'envoyer le certificat à tous les contrôleurs.

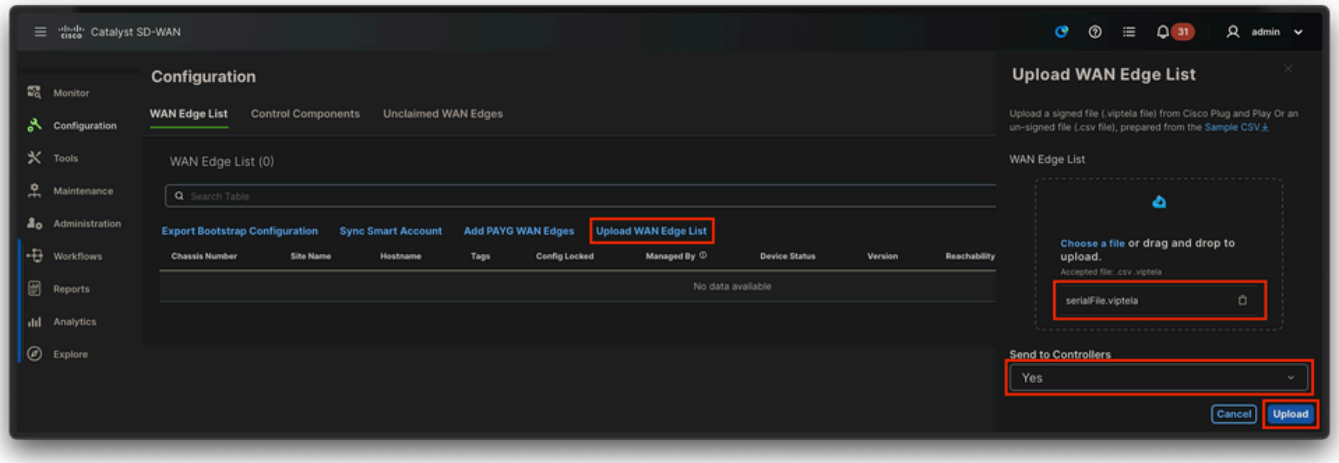


Figure 8. Mise à jour de la liste WAN à l'aide du fichier d'approvisionnement (VSF, Viptela Serial File) téléchargé depuis le portail PnP.

Une fois la méthode Online (En ligne) ou Offline (Hors ligne) terminée, vous devez pouvoir voir une entrée de périphérique dans le tableau WAN Edge List (Liste des périphériques WAN) qui correspond au numéro de série du périphérique enregistré dans PnP :

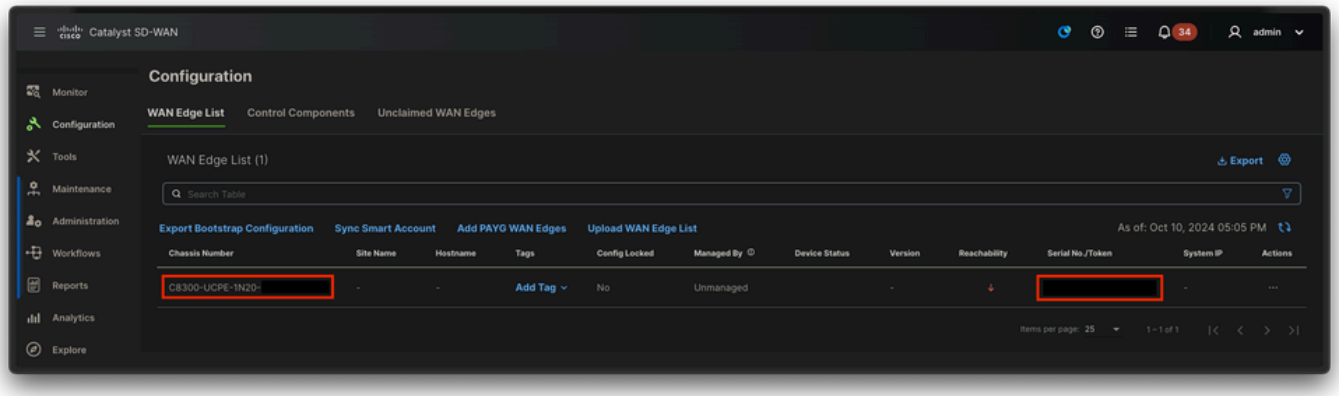
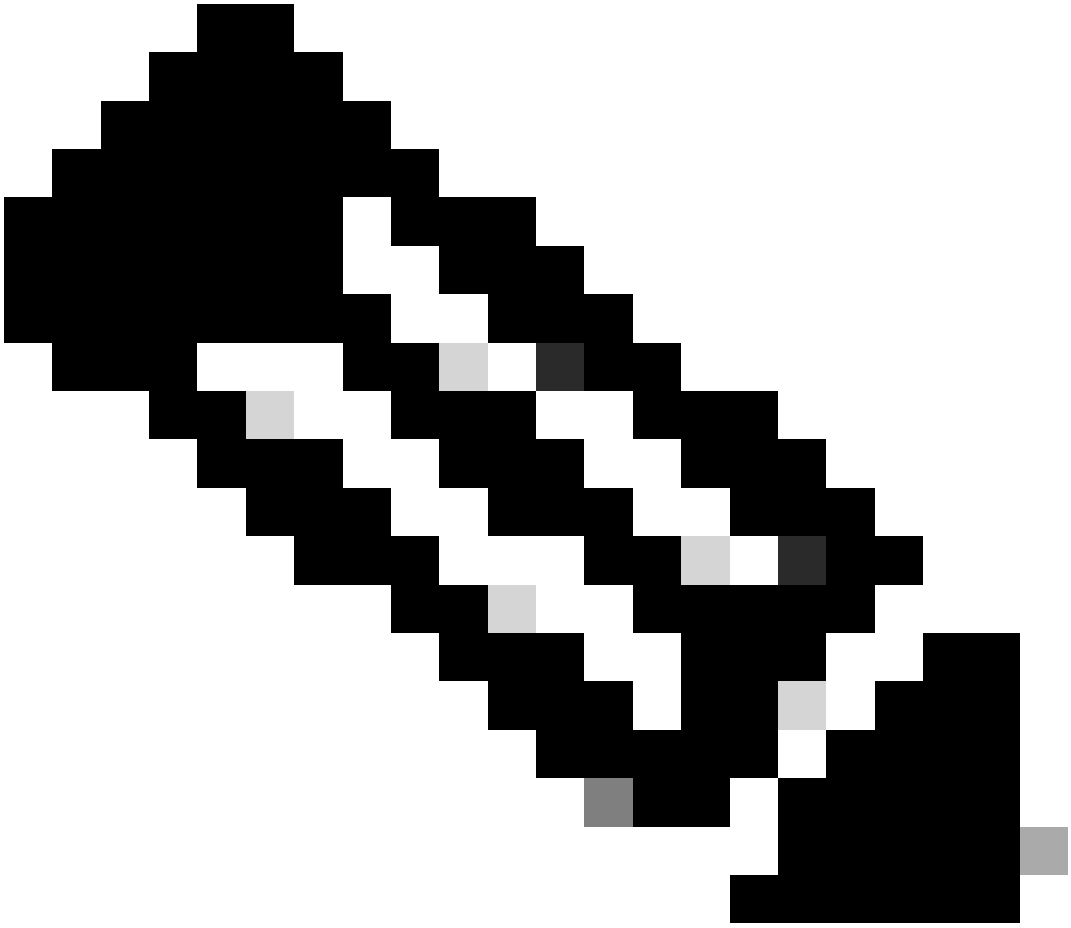


Figure 9. Périphérique 8300 dans la liste des périphériques.

Connexions d'intégration et de contrôle automatiques NFVIS

Si NFVIS peut résoudre devicehelper.cisco.com (atteindre PnP via Internet), l'intégration est automatiquement effectuée. Un système NFVIS intégré présente automatiquement une configuration viptela-system:system et vpn 0 qui contient des informations de contrôleur de base.

Depuis la version 4.9.1 de Cisco NFVIS, l'établissement d'une connexion de contrôle au plan de gestion via le port de gestion est pris en charge. Le port de gestion doit être accessible avec SD-WAN Manager pour que la connexion au plan de contrôle soit établie.



Remarque : Chaque commande contenant le mot clé "system" doit être écrite comme system:system. Si la touche de tabulation est utilisée pour compléter, elle s'adapte automatiquement à cette nouvelle norme.

```
C8300-UCPE-NFVIS# show running-config viptela-system:system
viptela-system:system
 admin-tech-on-failure
 no vrrp-advt-with-phymac
 sp-organization-name "Cisco Systems"
 organization-name "Cisco Systems"
 vbond



        port 12346
 logging
  disk
   enable
  !
 !
```

```
 ntp
  parent
   no enable
   stratum 5
  exit
 !
!
```

VPN 0 est le VPN de transport prédéfini de la solution SD-WAN. Il ne peut pas être supprimé ni modifié. L'objectif de ce VPN est d'imposer une séparation entre les réseaux de transport WAN (sous-jacents) et les services réseau (superposés) :

```
C8300-UCPE-NFVIS# show running-config vpn 0
vpn 0
 interface wan-br
  no shutdown
  tunnel-interface
   color gold
   allow-service all
   no allow-service bgp
   allow-service dhcp
   allow-service dns
   allow-service icmp
   no allow-service sshd
   no allow-service netconf
   no allow-service ntp
   no allow-service ospf
   no allow-service stun
   allow-service https
   encapsulation ipsec
  !
 !
!
```

Les connexions de contrôle sont des sessions DTLS établies entre différents noeuds (contrôleurs et routeurs de périphérie) de la structure SD-WAN. NFVIS n'étant pas une plate-forme de routage responsable des décisions de routage, il ne forme pas de connexions de contrôle avec les vSmarts. Dès la livraison, vous pouvez observer un état de « défi » pour vManage :

```
C8300-UCPE-NFVIS# show control connection
                                                                                    PEER
PEER    PEER PEER            SITE       DOMAIN PEER                                 PRIV  PEER
TYPE    PROT SYSTEM IP       ID         ID     PRIVATE IP                           PORT  PUBLIC IP
-------------------------------------------------------------------------------------------------
vbond   dtls 0.0.0.0         0          0      10.88.247.79                         12346 10.88.247.
vmanage dtls 10.10.10.10     100        0      10.88.247.71                         12946 10.88.247.
```

Cela indique généralement qu'il n'y a pas d'ip système, et/ou que le nom de l'organisation est mal configuré ou n'est pas configuré du tout. Le portail Plug and Play et vBond doivent établir le nom de l'organisation et une fois que la connexion de contrôle avec vManage a été établie. Sinon, poussez ces informations dans un NFV Config-Group (Supported from 20.14.1) avec les system-ip et site-id respectifs dans le modèle, ou configurez-le statiquement dans la sous-configuration viptela-system:system :

```
C8300-UCPE-NFVIS#(config)# viptela-system:system
C8300-UCPE-NFVIS#(config-viptela-system:system)# system-ip


C8300-UCPE-NFVIS#(config-viptela-system:system)# site-id


C8300-UCPE-NFVIS#(config-viptela-system:system)# organization-name


C8300-UCPE-NFVIS#(config-viptela-system:system)# commit
Commit complete.
```

Ces éléments sont disponibles dans vManage :

- Nom de l'entreprise : Administration > Paramètres > Système > Nom de l'organisation
- IP et port du validateur : Administration > Paramètres > Système > Validateur

Une fois que la configuration restante est entrée dans la sous-configuration viptela-system:system, vous avez besoin de connexions de contrôle actives/établies.

```
C8300-UCPE-NFVIS# show control connections
                                                                                    PEER
PEER    PEER PEER            SITE       DOMAIN PEER                                 PRIV  PEER
TYPE    PROT SYSTEM IP       ID         ID     PRIVATE IP                           PORT  PUBLIC IP
-------------------------------------------------------------------------------------------------
vbond   dtls 0.0.0.0         0          0      10.88.247.79                         12346 10.88.247.
vmanage dtls 10.10.10.10     100        0      10.88.247.71                         12946 10.88.247.
```

Désadministration de NFVIS

Si vous souhaitez revenir à l'état « Non géré » de NFVIS, vous devez effectuer les actions suivantes :

1. Supprimez l'entrée de périphérique du portail Plug-and-Play :

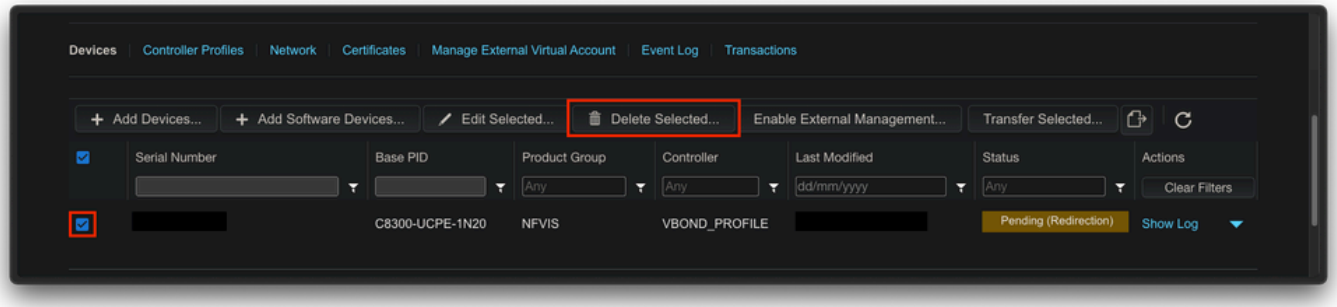


Figure 10. Retrait du périphérique 8300 du portail PnP.

2. NFVIS réinitialisé en usine.

```
C8300-UCPE-NFVIS# factory-default-reset all
```

3. Étapes facultatives : Supprimez le périphérique de la liste vManage Edge :

3.1 Invalidation du certificat de périphérique

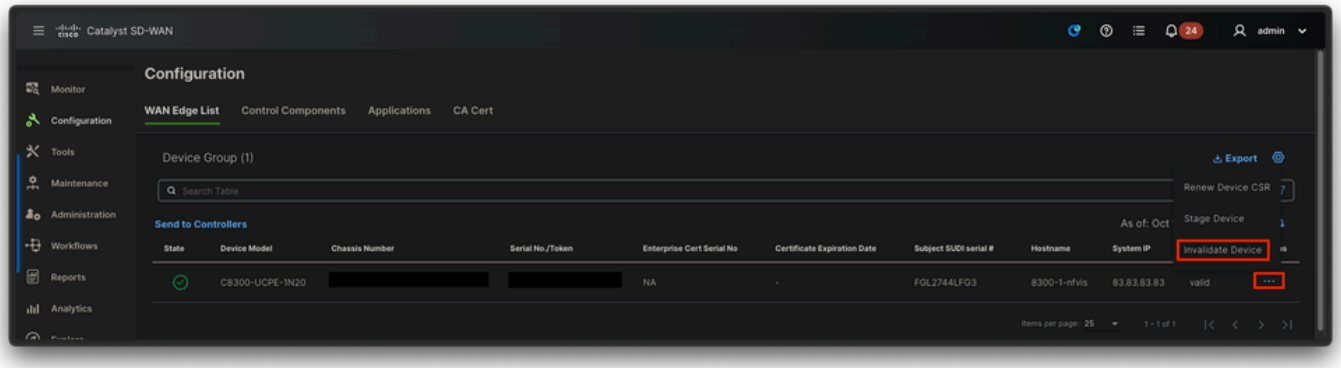


Fig. 11. Invalidation du certificat 8300.

3.2 Supprimez le périphérique de la liste WAN Edge.

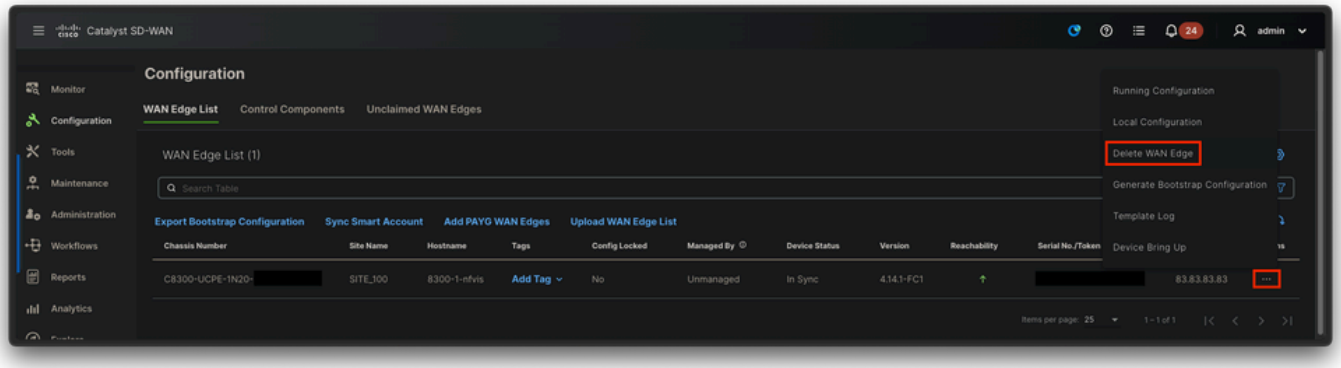


Fig. 12. Suppression du 8300 de la liste WAN Edge.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.