オンボードNFVIS WANエッジデバイス

内容

はじめに

このドキュメントでは、管理と運用のためにNFVIS対応システムをCatalyst™ SD-WAN環境にオンボーディングするプロセスについて説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- シスコSDWAN
- NFVIS
- プラグアンドプレイ(PNP)

次の事項を推定する。

- SD-WANコントローラ（vManage、vBond、およびvSmart）は、有効な証明書を使用してすでに導入されています。
- Cisco WAN Edge（この場合はNFVIS）は、WANトランスポート全体のパブリックIPアドレスを介して到達可能なvBondオーケストレータおよびその他のSD-WANコントローラに到達できます

- NFVISバージョンは、『制御コンポーネント互換性ガイド』に準拠している必要があります。

使用するコンポーネント

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

ハードウェア

- C8300-UCPE-1N20(ただし、任意のNFVIS対応プラットフォームに適用可能)

[ソフトウェア（Software）]

- vManage 20.14.1
- vSmartおよびvBond 20.14.1
- NFVIS 4.14.1

PnPワークフロー

WANエッジデバイスの信頼は、ルートチェーン証明書を使用して行われます。ルートチェーン証明書は、製造時に事前にロードされているか、手動でロードされるか、vManageによって自動的に配布されるか、またはPnPやZTPの自動導入プロビジョニングプロセス中にインストールされます。

SD-WANソリューションは許可リストモデルを使用します。つまり、SDWANオーバーレイネットワークへの参加を許可されるWANエッジデバイスは、すべてのSD-WANコントローラによって事前に認識される必要があります。そのためには、https://software.cisco.com/software/pnp/devicesのプラグアンドプレイ接続ポータル(PnP)でWANエッジデバイスを追加します

この手順では、常にデバイスを特定し、信頼して、同じオーバーレイネットワーク内に許可リストを作成する必要があります。同じオーバーレイネットワーク内のSD-WANコンポーネント間でセキュアな制御接続を確立するには、事前にすべてのSD-WANコンポーネント間で相互認証を行う必要があります。WANエッジデバイスのIDは、シャーシIDと証明書のシリアル番号によって一意に識別されます。WANエッジルータに応じて、証明書はさまざまな方法で提供されます。

- ハードウェアベースのvEdge：証明書は、製造時に取り付けられたオンボードの改ざん防止モジュール(TPM)チップに格納されます。
- ハードウェアベースのCisco IOS®-XE SD-WAN：証明書は、製造時にインストールされたオンボードのSUDIチップに保存されます。
- 仮想プラットフォームまたはCisco IOS-XE SD-WANデバイス：デバイスにルート証明書（ASR1002-Xプラットフォームなど）がプリインストールされていない。これらのデバイスでは、SD-WANコントローラでデバイスを認証するために、vManageによってワンタイ

ムパスワード(OTP)が提供されます。

ゼロタッチプロビジョニング(ZTP)を実行するには、DHCPサーバが使用可能である必要があります。そうでない場合は、IPアドレスを手動で割り当てて、プラグアンドプレイ(PnP)プロセスの残りの手順に進むことができます。

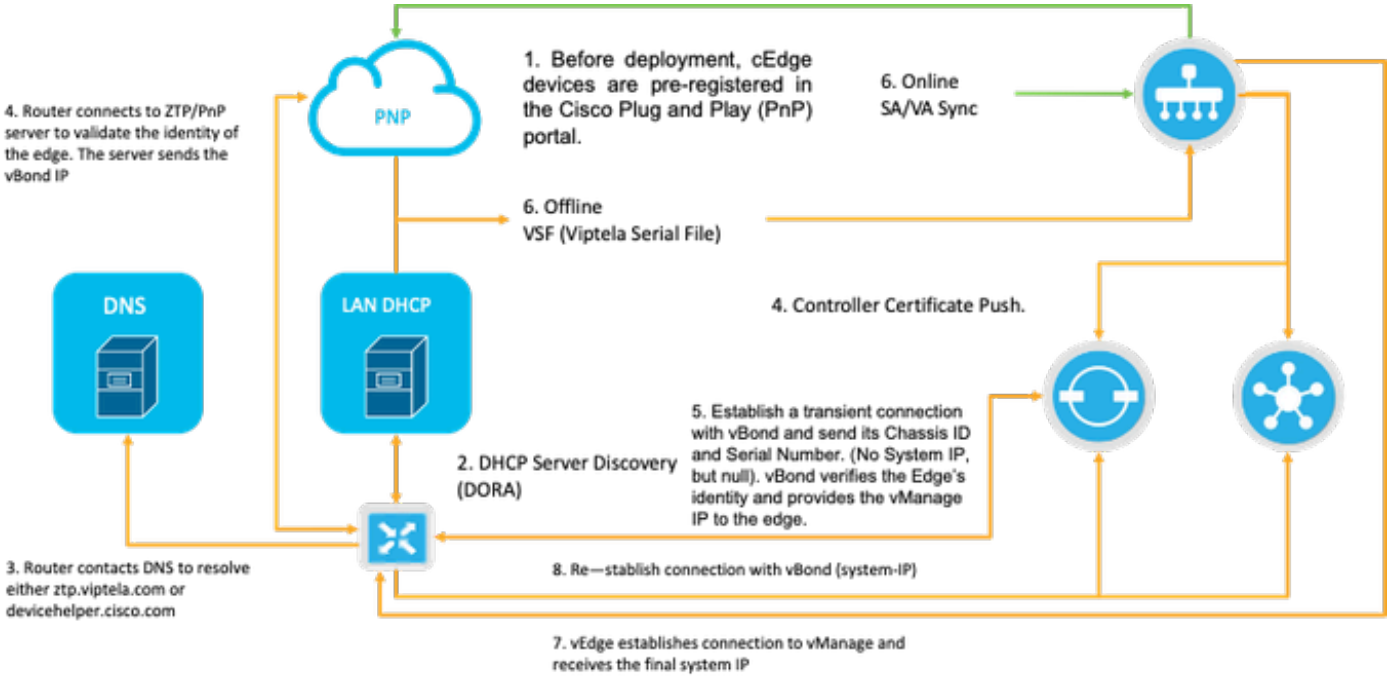


図1.PnPおよびWANエッジデバイスの信頼ワークフロー図。

NFVIS対応デバイスのセキュアなオンボーディング

シリアル番号と証明書シリアル番号の取得

NFVIS対応ハードウェアのハードウェアベースのSUDI(Secure Unique Device Identifier)チップを使用して、許可されたデバイスだけがセキュアなTLSまたはDTLS制御（SD-WAN Managerオーケストレータへのプレーントンネル）を確立できるようにします。support show chassisエグゼクティブレベルコマンドを使用して、対応するシリアル番号を収集します。

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

PnPポータルへのデバイスの追加

https://software.cisco.com/software/pnp/devicesに移動し、ユーザまたはラボ環境に適したスマートアカウントと仮想アカウントを選択します。（名前に複数のスマートアカウントが一致する場合は、ドメインIDで識別できます）。

使用するスマートアカウント(SA)/バーチャルアカウント(VA)がわからない場合は、いつでも「デバイス検索」テキストリンクで既存またはオンボードのシリアル番号を検索して、それが属するSA/VAを確認できます。

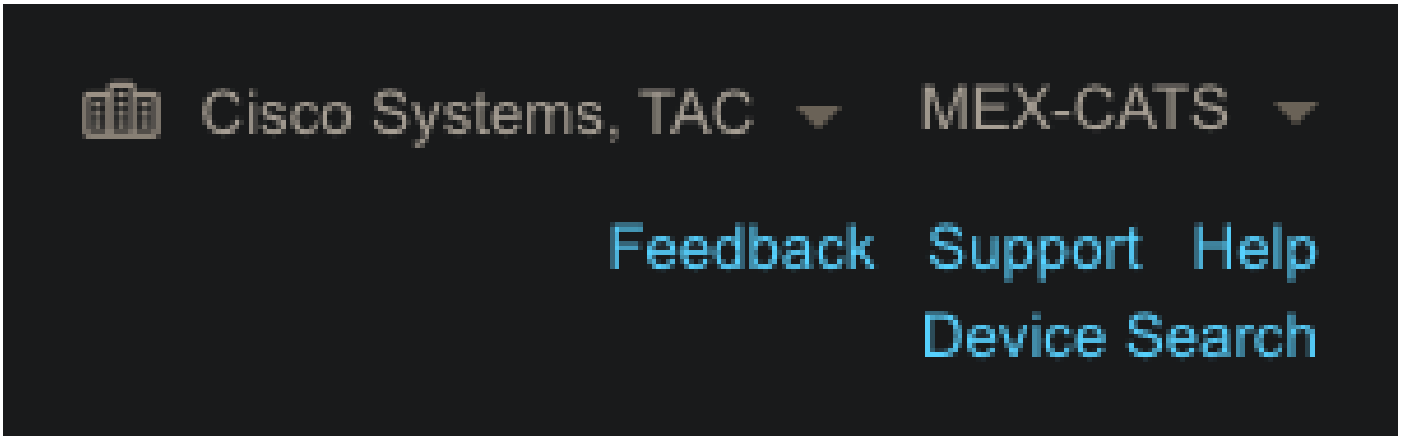


図2.SA/VAの選択とデバイス検索ボタン

正しいSA/VAを選択したら、「Add Devices...」をクリックします。

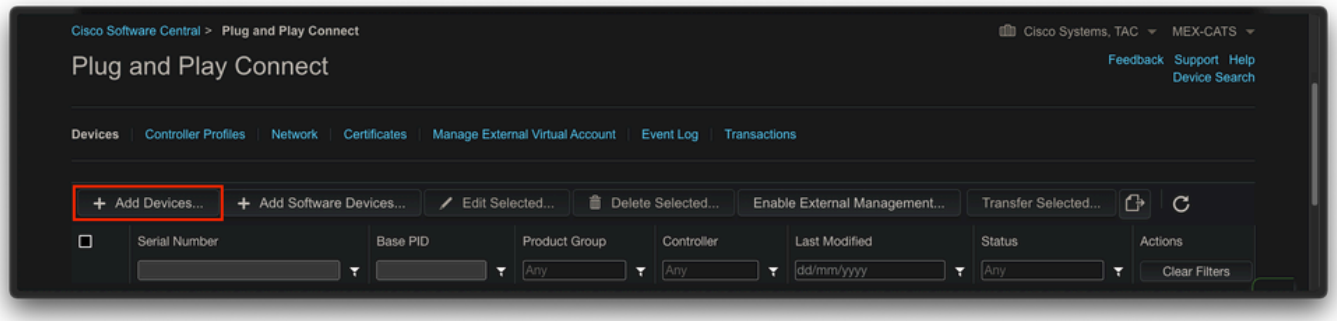


図3.「デバイスの追加...」 ボタンをクリックすると、物理デバイスが登録されます。

この特定のケースでは、オンボードのデバイスは1台だけなので、手動で入力するだけで十分です。

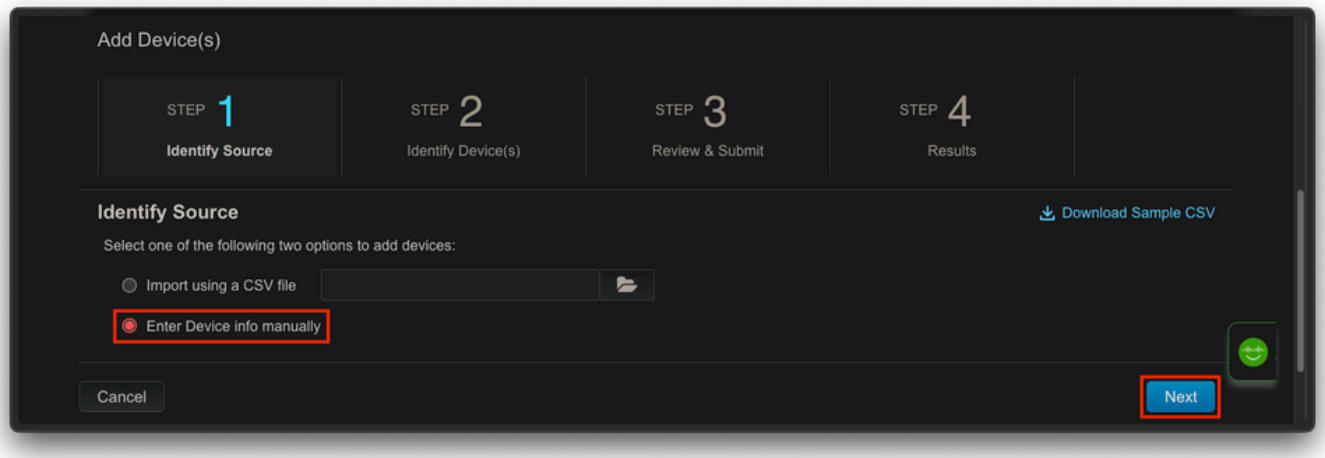


図4.機器情報入力の代替となる「機器の追加...」、マニュアル（個別）又はCSV（複数）

ステップ2では、「+デバイスの識別...」ボタンをクリックします。フォームのモーダルが表示されます。NFVISからのsupport show chassisの出力に示されている情報を詳細に入力し、対応するvBondコントローラプロファイルを選択します。

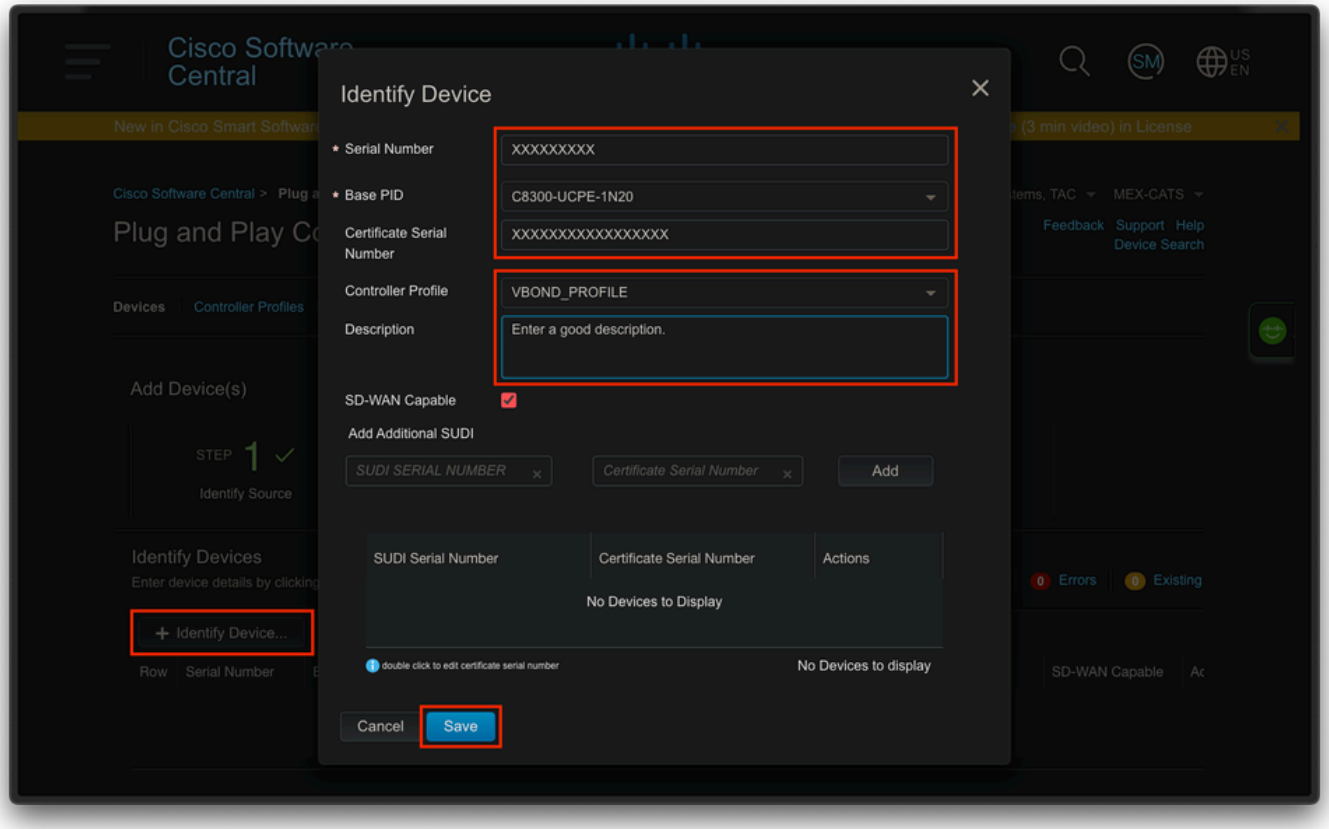


図5.Device Identificationフォーム

保存されたら、ステップ3でNextをクリックし、最後にステップ4でSubmitをクリックします。

NFVISでのPnP

自動モードと静的モードの両方を対象とする、NFVIS内のPnPのさまざまな構成設定の詳細については、リソース「NFVIS PnPコマンド」を参照してください。

すべてのNFVISバージョンで、PnPがデフォルトで有効になっていることに注意してください。

PnPを使用したvManage同期

オンラインモード

vManageがインターネットとPnPポータルに到達できる場合は、SA/VA同期を実行できるだけです。それには、Configuration > Devicesの順に移動し、Sync Smart Accountを示すテキストボタンをクリックします。Cisco Software Centralへのログインに使用するクレデンシャルが必要です。すべてのコントローラに証明書プッシュを送信します。

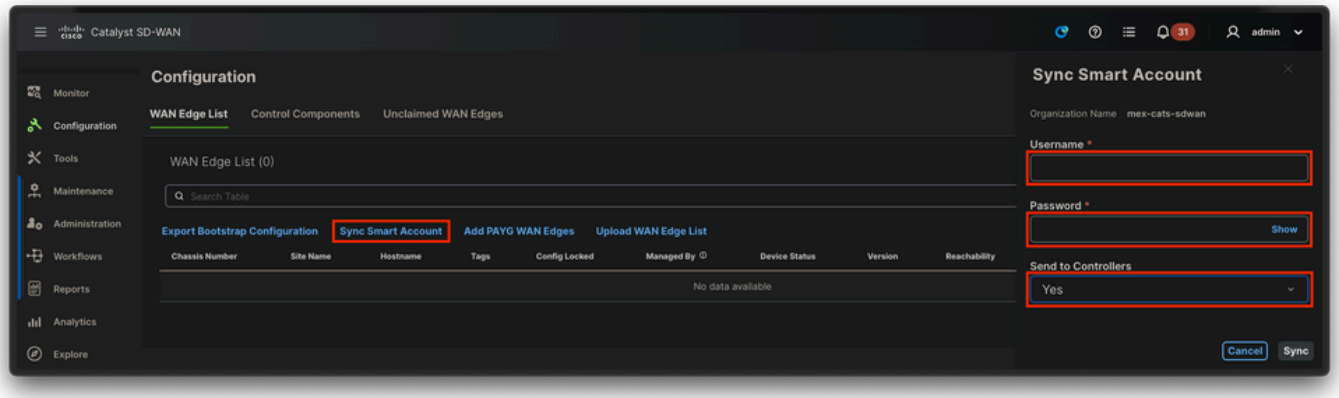


図6.SA/VA同期によるWANエッジルータのアップデート

オフラインモード

vManageがラボ環境にあるか、インターネットにアクセスできない場合は、デバイスリストに追加されたSNを含む必要があるプロビジョニングファイルをPnPから手動でアップロードできます。このファイルのタイプは.viptela(Viptela Serial File)で、「Controller Profiles」タブから取得できます。

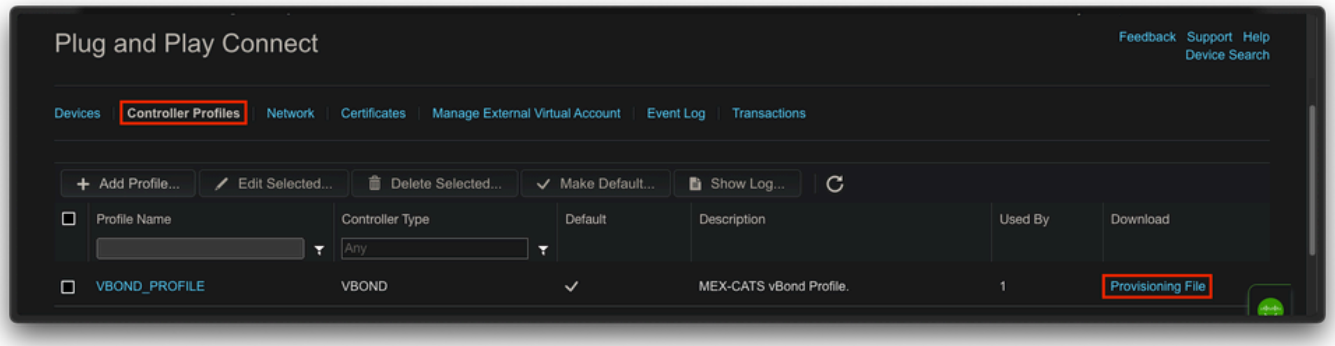


図7.CEdge WANリスト更新のためのプロビジョニングファイルのダウンロード。

プロビジョニングファイルを手動でアップロードする場合は、Configuration > Devicesの順に移動し、Upload WAN Edge Listを示すテキストボタンをクリックします。サイドバーが表示され、該当するファイルをドラッグアンドドロップできます(これらのアクションを行った後でUploadボタンが強調表示されない場合は、Choose a fileをクリックして、ポップアップエクスプローラーのウィンドウで手動でファイルを検索します)。 すべてのコントローラに証明書プッシュを送信します。

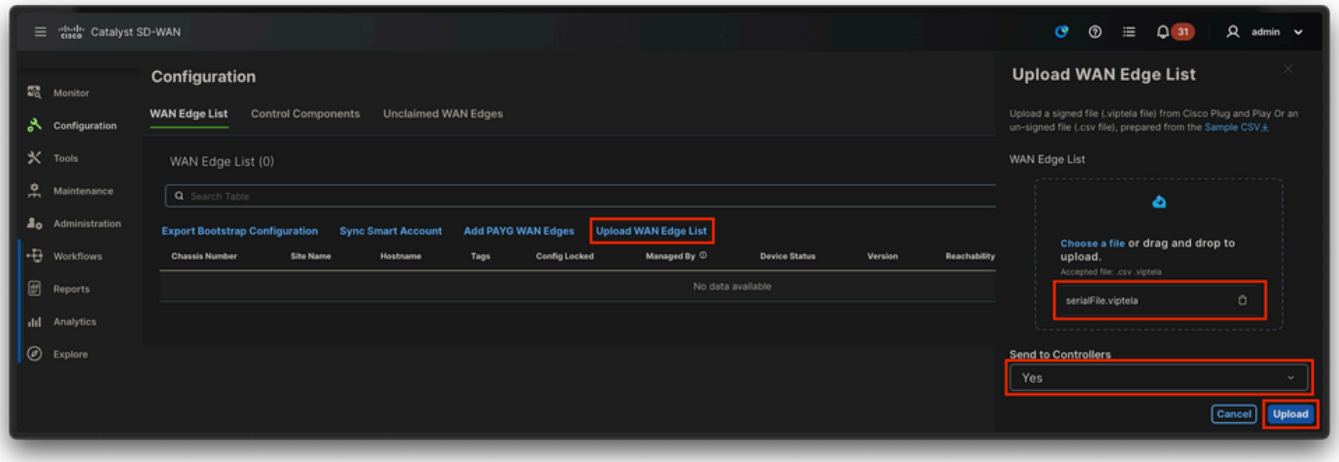


図8.PnPポータルからダウンロードしたプロビジョニングファイル（VSF、Viptelaシリアルファイル）を使用したWANリストの更新。

オンラインまたはオフラインのいずれかの方法を完了すると、WANエッジリストテーブルに、PnPに登録されているデバイスのSNに対応するデバイスエントリが表示されます。

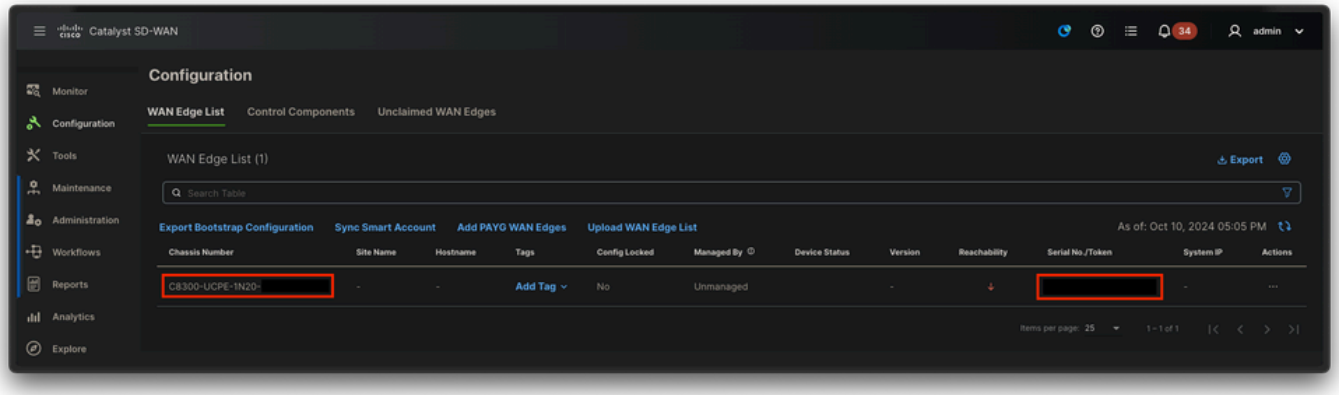
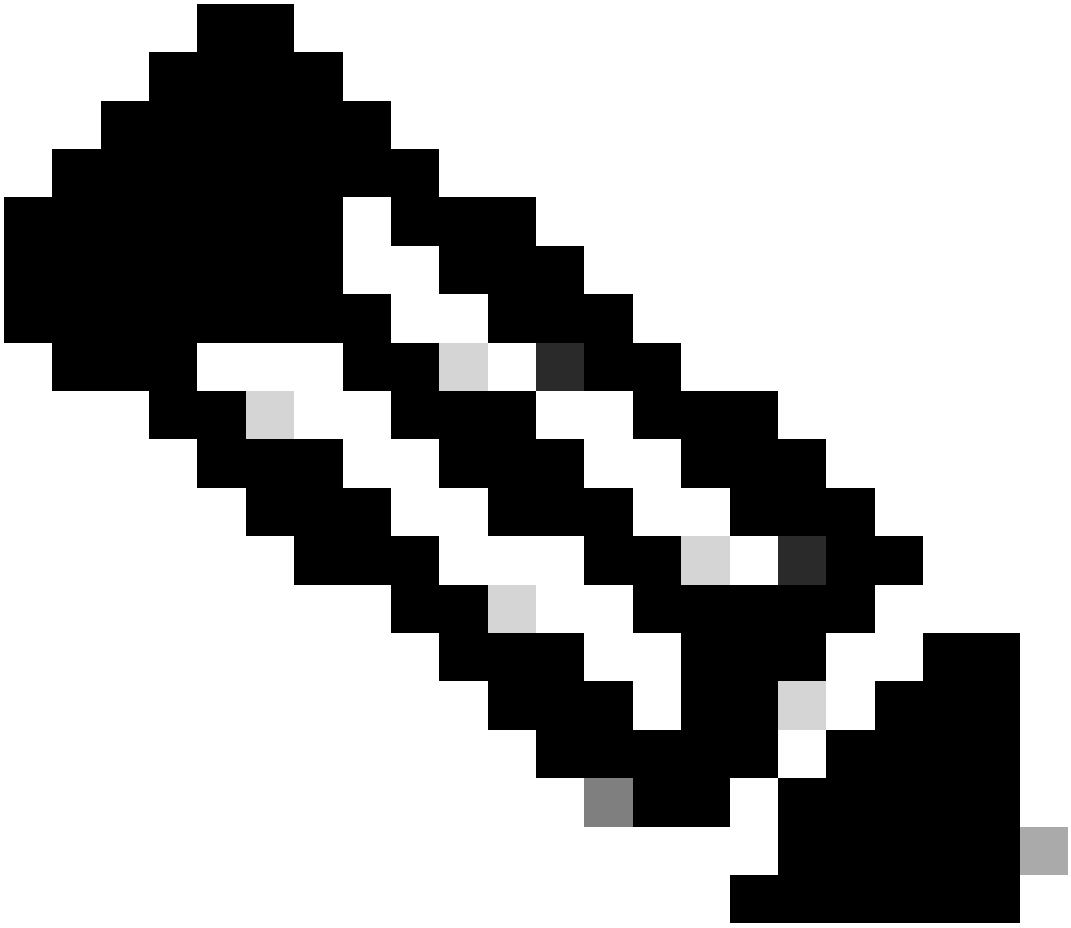


図9.エッジリスト内の8300デバイス

NFVISの自動オンボーディングおよび制御接続

NFVISがdevicehelper.cisco.comを解決できれば（インターネット経由でPnPに到達）、オンボーディングは自動的に実行されます。オンボードのNFVISシステムは、基本的なコントローラ情報を含むviptela-system:systemおよびvpn 0設定を自動的に表示します。

Cisco NFVISリリース4.9.1以降では、管理ポートを介した管理プレーンへの制御接続の確立がサポートされています。コントロールプレーンへの接続が成功するには、SD-WAN Managerを使用して管理ポートに到達できる必要があります。



注:「system」キーワードを含むすべてのコマンドは、system:systemと記述する必要があります。完了にTabキーを使用すると、この新しい標準に自動的に適応します。

```
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は、SD-WANソリューションの事前定義されたトランスポートVPNです。削除も変更もできません。このVPNの目的は、WANトランスポートネットワーク（アンダーレイ）とネットワークサービス（オーバーレイ）の分離を適用することです。

```
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
  !
 !
!
```

制御接続は、SD-WANファブリックの異なるノード（コントローラおよびエッジルータ）間で確立されるDTLSセッションです。 NFVISは、ルーティングの決定を担当するルーティングプラットフォームではないため、vSmartsとの制御接続を形成しません。 初期状態では、vManageの「challenge」状態は次のように表示されます。

```
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.
```

これは通常、system-ipがないか、organization-nameが誤っているか、まったく設定されていないことを示します。 PnPポータルとvBondは組織名を確立し、vManageとのコントロール接続が確立された後に確立する必要があります。それ以外の場合は、この情報をNFV Config-Group（20.14.1以降でサポート）内に適用し、テンプレート内のそれぞれのsystem-ipとsite-idを使用するか、viptela-system:systemサブ設定内に情報を静的に設定します。

```
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.
```

vManageには次の項目があります。

- 組織名：「管理」>「設定」>「システム」>「組織名」
- Validator IPおよびポート：Administration > Settings > System > Validator

viptela-system:systemサブ設定に残りの設定を入力した後は、アクティブ/確立された制御接続が必要です。

```
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.
```

NFVISの管理解除

NFVISを「Non-managed」状態に戻す場合は、次のアクションを実行する必要があります。

1. PnPポータルからデバイスエントリを削除します。

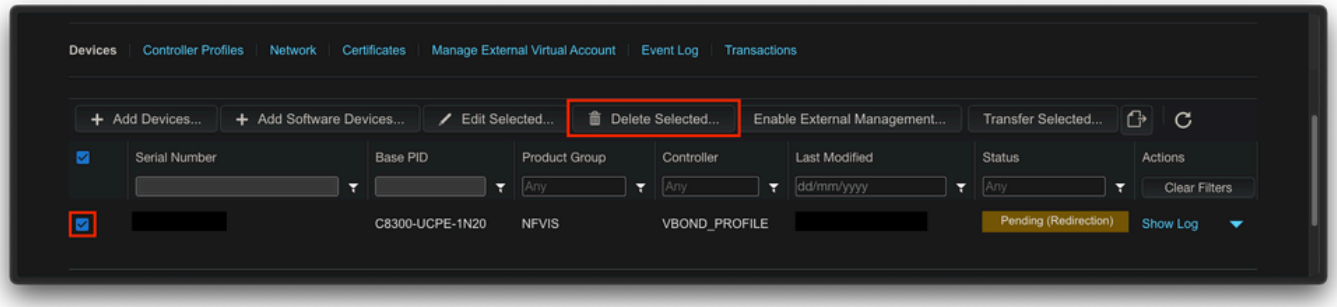


図10. PnPポータルからの8300デバイスの削除

2. NFVISを出荷時の状態にリセットします。

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

3. オプションの手順：vManageエッジリストからデバイスを削除します。

3.1デバイス証明書を無効にする。

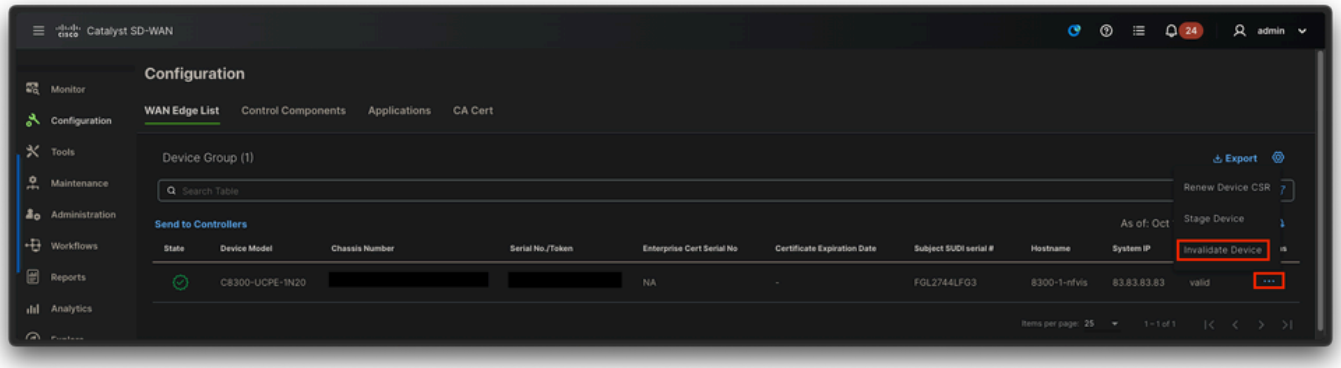


図11.8300証明書無効化

3.2 WANエッジリストからデバイスを削除する。

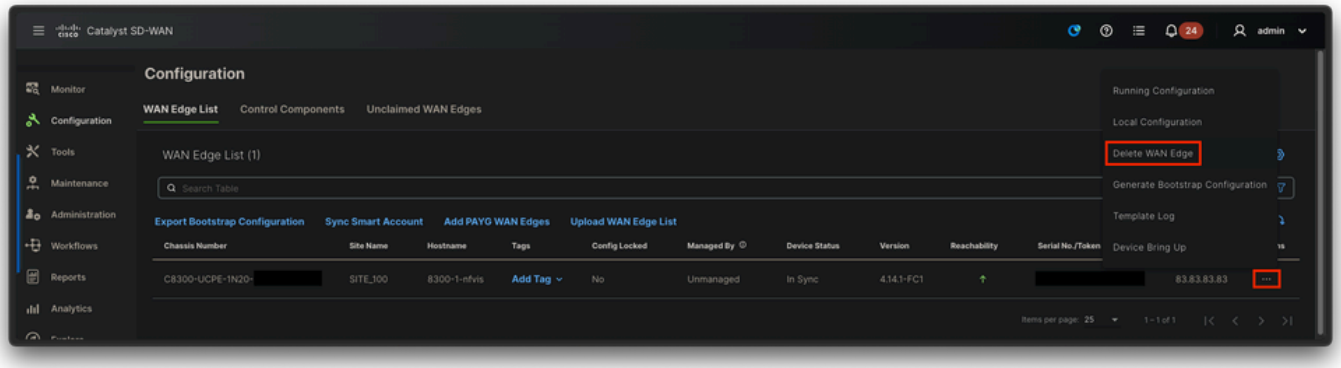


図12. WANエッジリストからの8300の削除。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。