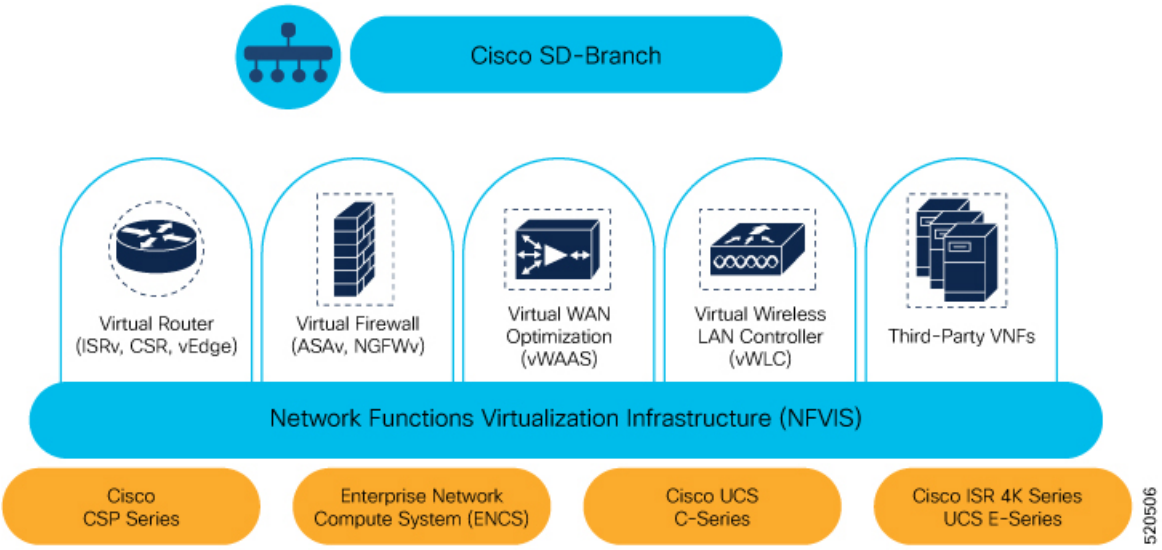
Cisco NFVIS SD-Branch ソリューションの定義

Cisco SD-Branch ソリューションは、エンタープライズグレードのネットワークおよびアプリケーションサービスを提供するフルスタックソリューションです。設計要件に合わせて、さまざまなコンピューティングプラットフォームから選択できます。サポートされているすべてのプラットフォームには、SD-Branch デバイスのライフサイクル管理用のホスト OS として NFVIS があります。このアーキテクチャでは、Cisco vManage を使用してブランチ ネットワーク コンピューティング デバイスのサービスをゼロタッチでプロビジョニングできます。



（注） NFVIS SD-Branch ソリューションは現在、ENCS 5400 デバイスのみをサポートしています。

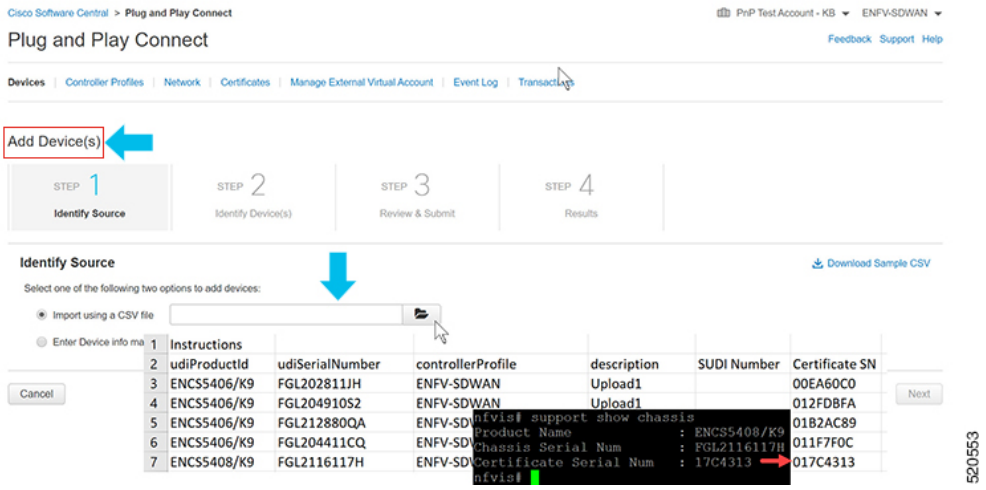
- 承認済みデバイスリストの作成 （2 ページ）
- VNF イメージパッケージの作成 （4 ページ）
- デバイスの検出と展開 （8 ページ）

承認済みデバイスリストの作成

ENCS デバイスのシリアル番号は、お客様固有の Cisco スマートアカウントとバーチャルアカウントにアップロードされます。これは自動化されたプロセスですが、場合によっては、バーチャルアカウントを手動で作成し、ENCS デバイスのシリアル番号をアップロードする必要があります。次の手順は、顧客ロケーションのデバイスを顧客固有のコントローラにリダイレクトする方法を示しています。

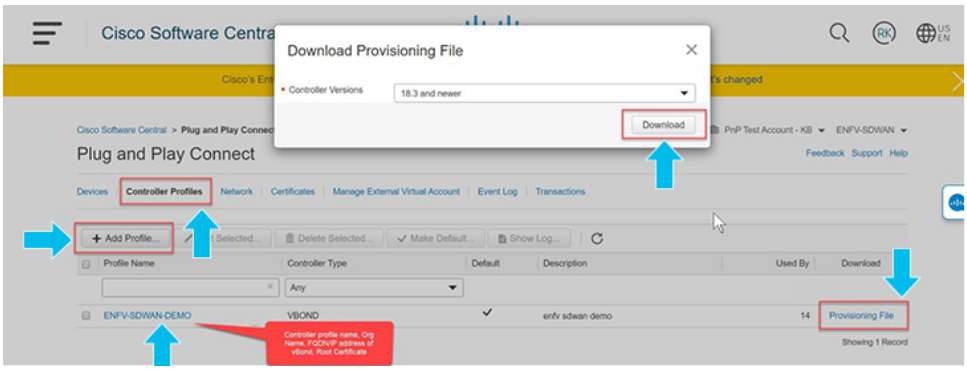
1. バーチャルアカウントにコントローラ情報を追加します。

   - PnP Connect サーバーで [Devices] を選択し、[+ Add Devices] をクリックして、PID、シリアル番号、およびコントローラに関する情報を含むCSV ファイルをアップロードします。Symantec によって発行された証明書をアップロードするか、エンタープライズのルート証明書をアップロードできます。



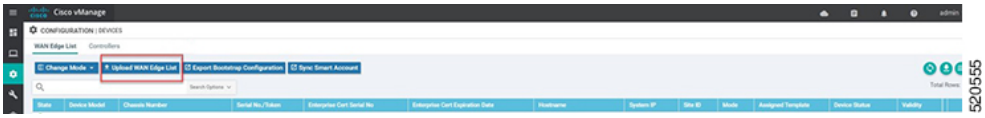
> **注** Cisco vManage 20.4 以降では、ENCS デバイス証明書のシリアル番号が使用できない場合、[SUDI Number] 列にデバイスのシリアル番号を入力することで、デバイスのシリアル番号を使用してデバイスを認証できます。Cisco vManage スマート同期では、デバイスのシリアル番号を使用してデバイスを認証します。

   - [Controller Profiles] を選択し、[+Add Profiles] をクリックします。コントローラに関連する詳細を入力して、プロファイルを作成します。[Provisioning File] を選択してダウンロードします。



2. デバイスリストを Cisco vManage に追加します。

   • 承認済みデバイスリストをバーチャルアカウントから Cisco vManage にアップロードします。



アイデンティティ、トラスト、およびホワイトリスト

NFVIS 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 エッジデバイスに応じて、次の証明書が提供されます。

- ENCS ハードウェアデバイス証明書は、製造時に取り付けられたオンボード SUDI チップに保存されます。ENCS ハードウェアは Cisco NFVIS ソフトウェアに付属しています。
- Cisco SD-WAN 仮想デバイスには、デバイスにルート証明書が事前にインストールされていません。これらのデバイスでは、ワンタイムパスワード（OTP）が Cisco vManage によって提供され、SD-WAN コントローラでデバイスを認証します。

WAN エッジデバイスの信頼性は、製造時にプリロードされたルートチェーン証明書、手動でロードされたルートチェーン証明書、Cisco vManage によって自動的に配布されたルートチェーン証明書、自動展開プロビジョニングプロセスであるプラグアンドプレイ（PnP）またはゼロタッチプロビジョニング（ZTP）でインストールされたルートチェーン証明書を使用して実現されます。

Cisco SD-Branch ソリューションはホワイトリストモデルを使用します。つまり、SD-Branch オーバーレイネットワークに参加できる NFVIS WAN Edge デバイスは、すべての SD-Branch コントローラで事前に認識されている必要があります。これを行うには、PnP 接続ポータルに WAN エッジデバイスを追加します。追加された WAN エッジデバイスは、PnP ポータル（SD-Branch オーバーレイの組織名に関連付けられている）に含まれる Cisco vBond コントローラプロファイルに接続され、プロビジョニングファイルが作成されます。このファイルは SD-Banch vManage コントローラにインポートされ、デバイスのホワイトリストが残りの SD-Branch コントローラ（vBond）と自動的に共有されます。デバイスのホワイトリストを含

むプロビジョニングファイルは、PnP 接続ポータルから Cisco vManage に REST API を使用してセキュアな SSL 接続を介して直接同期することもできます。

（注） Cisco SD-WAN コンポーネント（Cisco vManage、Cisco vBond、Cisco vSmart コントローラ、WAN エッジデバイスなど）はすべて、同じ SD-Branch オーバーレイネットワークに参加するために同じ組織名で設定する必要があります。

VNF イメージパッケージの作成

表 *1:* 機能の履歴（表）

機能名	リリース情報	説明
異なる VNF イメージパッケージのアップロードのサポート	NFVIS 4.6.1 Cisco vManage リリース 20.6.1	この機能を使用すると、イメージパッケージ、スキャフォールド、およびディスクイメージ用の個別の VNF パッケージをアップロードして、VNF イメージを登録できます。

事前にパッケージ化された Cisco VM イメージ tar.gz のアップロードは、Cisco vManage でサポートされています。また、サポートされている形式（qcow2）でルートディスクイメージを提供することで、VM イメージをパッケージ化することもできます。Linux のコマンドライン NFVIS VM パッケージツール nfvpt.py を使用して qcow2 をパッケージ化するか、Cisco vManage からカスタマイズされた VM イメージを作成します。

（注） 事前にパッケージ化された Cisco VM イメージを [ISRv Software Download] ページからダウンロードし、[Scaffold Files for Third Party VMs Software Download] ページからダウンロードします。https://software.cisco.com/download/home/286308649/type/286327969/release/17.03.01https://software.cisco.com/download/home/286308649/type/286327978/release/4.4.1

ファイアウォールなどの各 VM タイプには、カタログに追加される同じまたは異なるベンダーから Cisco vManage にアップロードされる複数の VM イメージを含めることができます。また、同じ VM のリリースに基づく異なるバージョンをカタログに追加できます。ただし、VM 名が一意であることを確認してください。

Cisco VM イメージ形式は *.tar.gz としてバンドルでき、次のものを含めることができます。

- VM を起動するルートディスクイメージ。
- パッケージ内のファイルリストのチェックサム検証用のパッケージマニフェスト。

- VM メタデータをリストする XML 形式のイメージプロパティファイル。
- （任意）0 日目設定、VM のブートストラップに必要なその他のファイル。
- VM システムプロパティをリストする XML 形式のシステム生成プロパティファイル

VM イメージは、vManage がホストする HTTP サーバーローカルリポジトリまたはリモートサーバーの両方でホストできます。

VM が tar.gz などの NFVIS でサポートされる VM パッケージ形式である場合、Cisco vManage はすべての処理を実行し、VNF プロビジョニング中に変数キーと値を指定できます。

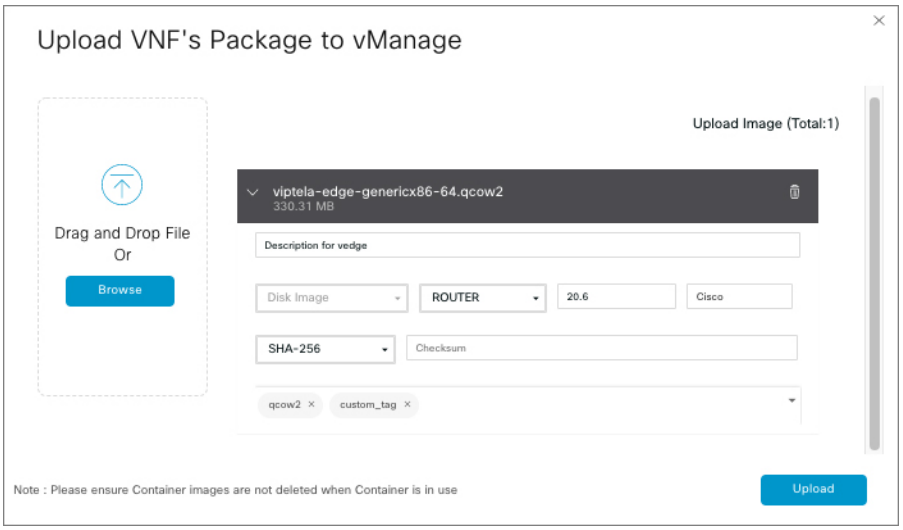
異なるイメージタイプのアップロード

NFVIS リリース 4.6.1 以降、イメージの登録プロセスはイメージプロパティのアップロードプロセスから分離されています。VNF イメージは、サポートされている任意のイメージ形式でアップロードすることで登録できます。サポートされるイメージ形式は次のとおりです。

- イメージパッケージ：完全なイメージパッケージの .tar.gz ファイル。
- Scaffold：.tar.gz ファイル（メタデータのみで構成）（イメージプロパティおよび第 0 日のコンフィギュレーション ファイル）。
- ディスクイメージ：.qcow2 ディスクイメージ。

イメージタイプをアップロードするには、次の手順を実行します。

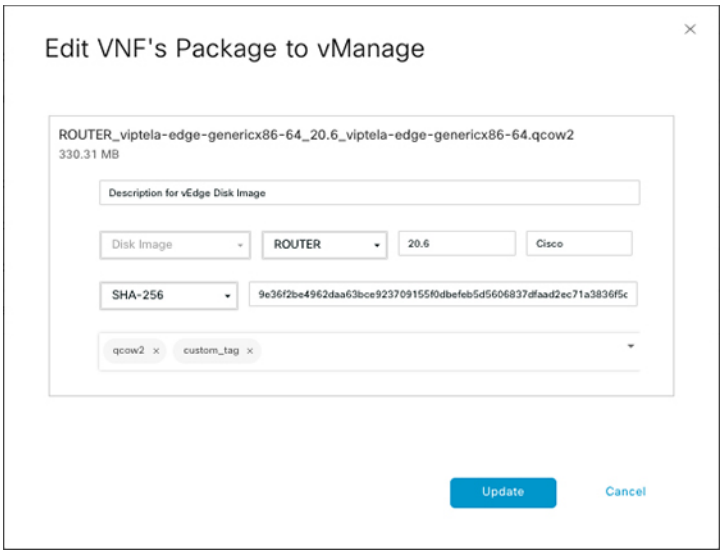
1. [Cisco vManage] メニューから、**[Maintenance]** > **[Software Repository]**を選択します。
2. [Virtual Images] をクリックします。
3. [Upload Virtual Image] ドロップダウンリストから、[vManage] を選択します。
4. [Upload VNF's Package to vManage] ウィンドウで、tar.gz または qcow2 ファイルをアップロードします。
5. [File Type] ドロップダウンリストから、イメージタイプ（[Image Package]、[Scaffold]、または [Disk Image]）を選択します。
6. （任意）説明とタグを追加して、イメージを識別しやすくします。使用可能なデフォルトタグを使用するか、独自のカスタムタグを作成できます。
7. ディスクイメージをアップロードする場合は、[VNF Type]、[VNF Type]、および [Vendor] の値を選択します。



8. [Upload] をクリックします。

VNF パッケージを編集するには、次の手順を実行します。

1. [Cisco vManage] メニューから、**[Maintenance]** > **[Software Repository]**を選択します。
2. [Virtual Images] をクリックします。
3. 目的のイメージの [...] をクリックし、[Edit] を選択します。



4. 必要な変更を行った後、[Update] をクリックします。

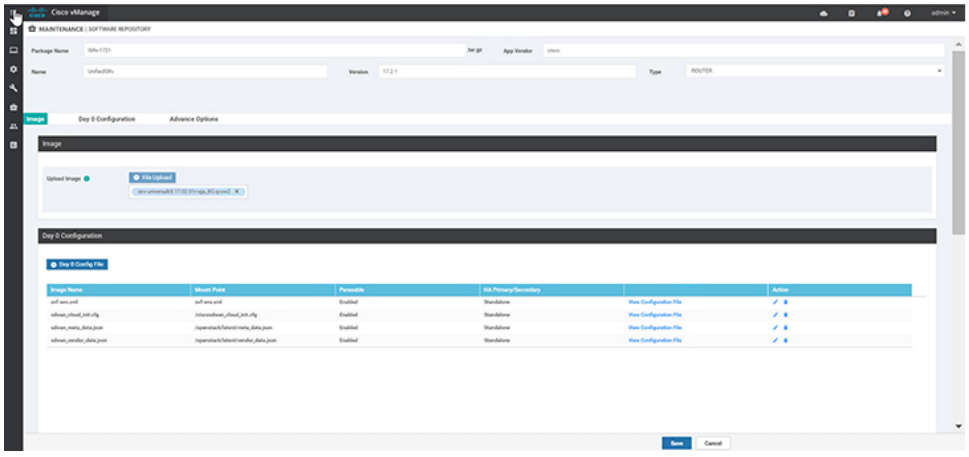
（注） Cisco vManage は Cisco VNF のみを管理しますが、VNF 内の 1 日目 および N 日目の設定は他の VNF ではサポートされません。VM パッケージの形式と内容、および image_properties.xml とマニフェスト（package.mf）のサンプルの詳細については、『NFVIS Configuration Guide』の「VM Image Packaging」[英語] を参照してください。

同じ VM、同じバージョン、Communication Manager（CM）タイプの複数のパッケージをアップロードするには、3 つの値（名前、バージョン、VNF タイプ）のいずれかが異なることを確認します。その後、アップロードする VM *.tar.gz を再パッケージ化できます。

次に、ISRv パッケージの作成方法の例を示します。

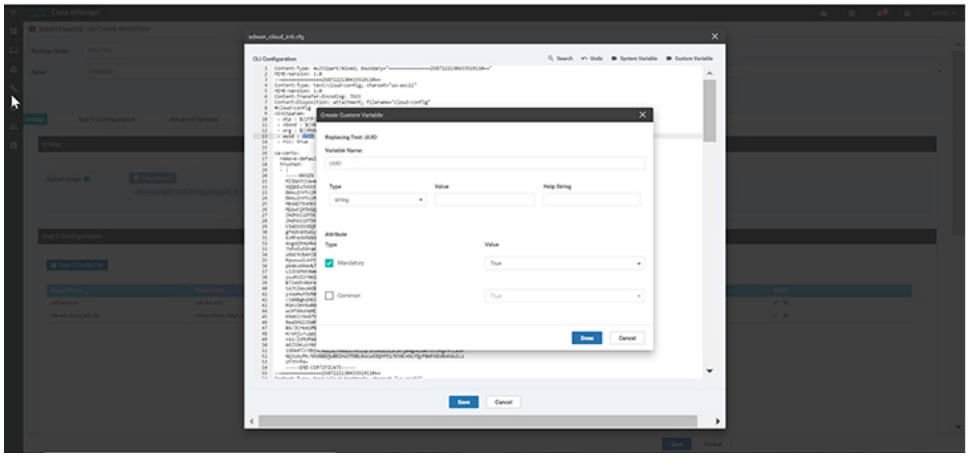
1. ブートストラップ設定のルートディスクイメージをアップロードします。

   イメージの横にある [View Configuration File] をクリックします。



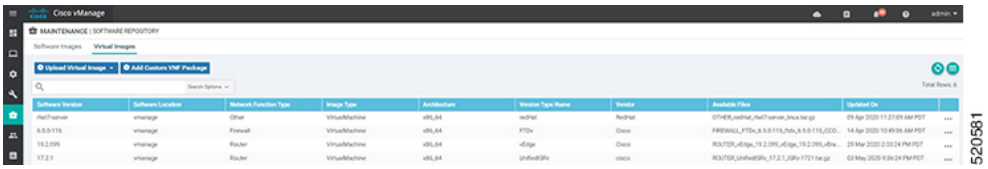
2. 変数を選択し、[Custom Variable] をクリックします。ポップアップウィンドウで、ドロップダウンメニューから変数タイプを選択します。

   [Done] をクリックしてから、 [Save] をクリックします。



3. 必要に応じてイメージプロパティを選択できます。

4. イメージパッケージが作成され、仮想イメージのリストに追加されたことを確認できます。



デバイスの検出と展開

WAN エッジデバイスは、ブートアップ時に Cisco vBond オーケストレータに接続し、セキュアな一時的な DTLS 制御接続を確立します。Cisco vBond 情報は、IP アドレスまたは解決可能なドメイン名 FQDN を使用し、WAN エッジデバイスの CLI を通じて手動で設定できます。または、PnP または ZTP プロセスによって自動的に取得することもできます。

SD-Branch コントローラ（Cisco vBond、Cisco vManage、および Cisco vSmart）と WAN Edge デバイスは、セキュアな制御接続を確立する前に、相互に認証して信頼する必要があります。SD-Branch コントローラが相互に認証し、WAN エッジデバイスが認証されると、次のようになります。

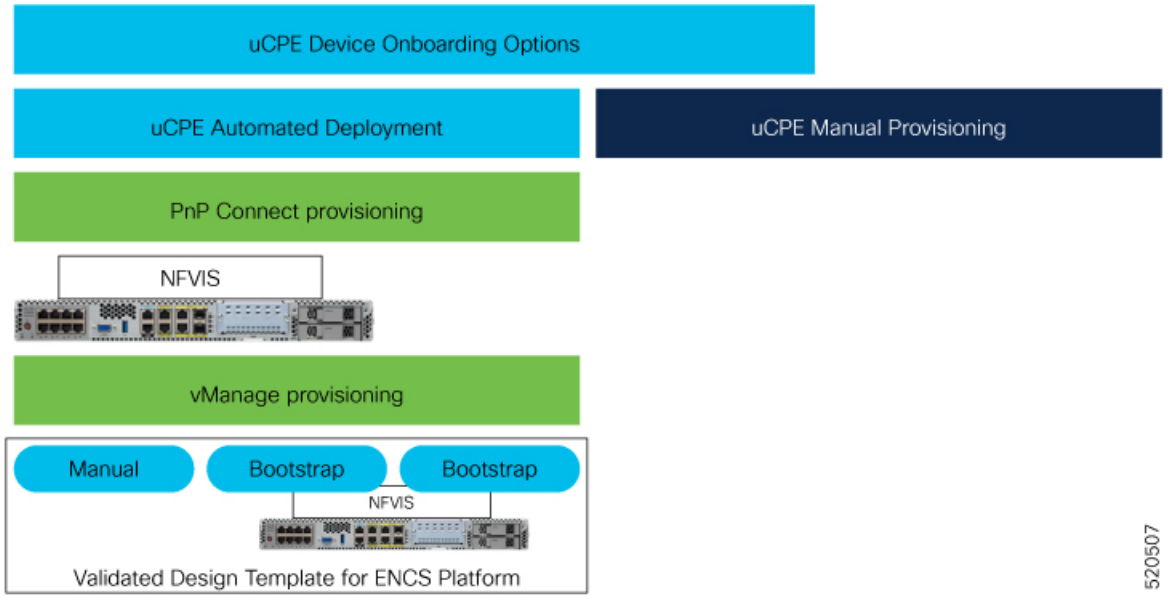
- 証明書ルート CA の信頼ルートの検証
- 受信した証明書の組織単位（OU）の組織名をローカルに設定された OU と比較します。
- 証明書のシリアル番号を承認済みのホワイトリストと比較します。

WAN エッジデバイスがコントローラを認証すると、次のようになります。

- 証明書ルート CA の信頼ルートの検証
- 受信した証明書 OU の組織名をローカルに設定された OU と比較します。

認証に成功すると、vBond オーケストレータはセキュアな一時的な DTLS 制御接続を確立し、Cisco vManage IP アドレスを共有します。この時点で、Cisco vBond オーケストレータは、他の SD ブランチコントローラ（Cisco vManage および Cisco vSmart）に、WAN エッジデバイスからの制御接続要求を予期するよう通知します。ENCS デバイスは、Cisco SD-WAN デバイスとは異なり、vSmart との制御接続を維持しません。

NFVIS WAN エッジデバイスは、Cisco vManage 情報を学習すると、Cisco vManage サーバーへの制御接続を開始します。認証に成功すると、別のセキュアで永続的な DTLS/TLS 接続が確立されます。Cisco vManage は、WAN エッジデバイスに接続されたデバイステンプレートに基づいて、NETCONF プロトコルを使用して設定をプロビジョニングします。



NFVIS WAN エッジデバイスのデフォルトの動作は、次のとおりです。

- オンボーディングプロセス中のみ、1 つの WAN トランスポートを介した Cisco vBond への一時的な DTLS 制御接続を保護します。
- 単一の WAN トランスポートを介した Cisco vManage への永続的な DTLS/TLS 制御接続を保護します。