# オンボードNFVIS WANエッジデバイス

内容 はじめに 前提条件 要件 <u>使用するコンポーネント</u> <u>ハードウェア</u> [ソフトウェア (Software)] PnPワークフロー <u>NFVIS対応デバイスのセキュアなオンボーディング</u> シリアル番号と証明書シリアル番号の取得 PnPポータルへのデバイスの追加 <u>NFVISでのPnP</u> <u>PnPを使用したvManage同期</u> <u>オンラインモード</u> オフラインモード NFVISの自動オンボーディングおよび制御接続 NFVISの管理解除

## 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、『<u>制御コンポーネント互換性ガイド</u>』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、

<u>https://software.cisco.com/software/pnp/devices</u>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。



receives the final system IP

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 : XXXXXXXX Certificate Serial Num : XXXXXXXXXXXXXXXXXX

#### PnPポータルへのデバイスの追加

<u>https://software.cisco.com/software/pnp/devices</u>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。

Plug and F	lay Con	nect						Feedback	Device Search
				al Assault 1. Even	at Loa Transpo	lions			
Devices Controll	er Profiles   Ne	etwork Certificates	Manage External Virtu	ai Account Ever	ni Log Transac				
Devices Controll	er Profiles Ne	etwork Certificates	Manage External Virtu						a
Devices Controlle	er Profiles   Ne	etwork Certificates	Edit Selected	Delete S	elected En	able External Management	Transfer S	Selected	C

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。

STEP	STEP 2	STEP 3	STEP <b>4</b>	
Identify Source	Identify Device(s)	Review & Submit	Results	
Identify Source				
Select one of the following two options	to add devices:			
Import using a CSV file		<b>&gt;</b>		
Enter Device info manually				

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。

Cisco Softwa Central	Identify Device		×	Q €M ⊕ <sup>us</sup> en
	* Serial Number	XXXXXXXXXXX		
Cisco Software Central > Plug a	* Base PID	C8300-UCPE-1N20 ~		
	Number Controller Profile	VBOND_PROFILE ~		
	Description	Enter a good description.	ĺ	
Add Device(s)	SD-WAN Capable Add Additional SUDI	2	2	
		Certificate Serial Number × Add		
	SUDI Serial Numbe	Certificate Serial Number Actions No Devices to Display		
+ Identify Device Row Serial Number B	double click to edit certificat	serial number No Devices to display		
	Cancel Save			

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「<u>NFVIS PnPコマンド</u>」を参照してください<u>。</u>

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。

≡ disco Catalyst S	HD-WAN	ී 🖗 🏛 Q 🛐 Զ admin ✔		
22 Monitor	Configuration	Sync Smart Account $ imes$		
X Configuration	WAN Edge List Control Components Unclaimed WAN Edges	Organization Name mex-cats-sdwan		
🗙 Tools	WAN Edge List (0)	Username *		
A Maintenance	Q: Search Table	Password *		
<b>å</b> o Administration	Export Bootstrap Configuration Sync Smart Account Add PAYG WAN Edges Upload WAN Edge List	Show		
+ Workflows	Chassis Number Site Name Hostname Tags Config Locked Managed By 🛈 Device Status Version Reachability	Send to Controllers		
Reports		Yes ~		
III Analytics				
Explore		Cancel Sync		

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。

Plu	ig and Play	Connect						Feedback Support Help Device Search
Device	es Controller Pro	files Network	Certificates Manage Extern	al Virt	ual Account Event	Log Transactions		
+	Add Profile	<ul> <li>Edit Selected</li> </ul>	Delete Selected	~	Make Default	🗈 Show Log		
	Profile Name	Ţ	Controller Type	<b>. .</b>	Default	Description	Used By	Download
	VBOND_PROFILE		VBOND		~	MEX-CATS vBond Profile.		Provisioning File

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。

	≔ Q 💷 🛛 🗙 admin 🗸
Configuration Upload WAN	N Edge List ×
Configuration Configuration Control Components Unclaimed WAN Edges Upload a signed file (x un-signed f	viptela file) from Cisco Plug and Play Or an ie), prepared from the Sample CSV±
★ Tools WAN Edge List (0) WAN Edge List	
Maintenance     Q Search Table	۵
Administration Export Bootstrap Configuration Sync Smart Account Add PAYG WAN Edges Upload WAN Edge List Choose a	file or drag and drop to
Chassis Number Site Name Hostname Tags Config Locked Managed By      Device Status Version Reachability upload,     Accepted fil	ie:.csv.viptela
er Reports volume available serialFile:	viptela 🗍
III Animynes	s
Yes	
	Cancel Upload

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。

≡ "lindin Catalyst	SD-WAN ( ) ( ) ( ) ( ) ( ) ( ) ( ) ( ) ( ) (
Sa Monitor	Configuration
A Configuration	WAN Edge List Control Components Unclaimed WAN Edges
🗙 Tools	WAN Edge List (1)
A Maintenance	Q. Search Table
20 Administration	Export Bootstrap Configuration Sync Smart Account Add PAYO WAN Edges Upload WAN Edge List As of: Oct 10, 2024 05:05 PM 📢
+ Workflows	Chassis Number Site Name Hostname Tags Config Locked Managed By D Device Status Version Reachability Berlal Na /Token System P Actions
Reports	C8300-UCPE-IN20 Add Tag v No Unmanaged
dd Analytics	

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 1 1

ï

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 TYPE	PEER PROT	PEER SYSTEM IP	SITE ID	DOMAIN ID	PEER PRIVATE IP	PEER PRIV PORT	PEER 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<u>NFV Config-</u> <u>Group</u>(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)# 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
ТҮРЕ	PROT	SYSTEM IP	ID	ID	PRIVATE IP	PORT	PUBLIC IP
vbond	dt]s	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。

+ /	dd Devices	+ Add Software	Devid	ces / Edit Se	lected	📋 D	elete	Selected	Enab	le External Management		Transfer Selected	Ľ*	C
Serial Number Bas		Base PID	ID Product G			Controller		Last Modified		Status		Actions		
			T	τ	An		] 🕇	Any	<b>. .</b>	dd/mm/yyyy	Ŧ	Any		Clear Filters
				00000 11005 4100								Dending (Deditection)		

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。

≡ disco Catalyst :	SD-WAN						C	⊛ ≔ ¢	) 24 오 ad	imin 🗸
କିନ୍ସ୍ Monitor	Configuration									
\Lambda Configuration	WAN Edge List Control Componen	nts Applications C	A Cert							
* Tools									🕁 Export	0
A Maintenance										7
<b>a</b> o Administration	Send to Controllers									4
+ Workflows	State Device Model	Chassis Number	Serial No./Token	Enterprise Cert Serial No	Certificate Expiration Date	Subject SUDI serial #	Hostname	System IP	Invalidate Device	2
Reports									valid 💽	-
III Analytics										э

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。

≡ diada Catalyst	SD-WAN				C	③ ≔ Q 💶 🎗 admin 🗸
罷 Monitor み Configuration	Configuration WAN Edge List Ontrol Components Unclaimed	WAN Edges				
★ Tools		Delete WAN Edge				
<b>åo</b> Administration ← → → Workflows	Export Bootstrap Configuration Sync Smart Accoun Chassis Number Site Name	t Add PAYG WAN Edges Upk Hostname Tags	oad WAN Edge List Config Locked Managed By ©	Device Status Version	Reachability Serial No./Token	
Reports		8300-1-nfvis Add Tag 🗸				83.83.83
III Analytics					Items per page: 25	T-Teft

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。