

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。

sco Software Centr	al > Plug a	and	Play Connect						tB PnP Test Account - KB				
vices Controlle	er Profiles		Vetwork Certificate	s Manage	External Virtual	Account Event Log	Transaction			Personal S			
Id Device(s)													
STEP 1	-		STEP 2		ST	ep 3	STEP 2	4					
Identify Se	ource		Identify Dev	ice(s)	Rev	view & Submit	Res	ults					
dentify Sour	ce									🛃 Download Sar	mple CSV		
Select one of the	following tw	0 05	tions to add devices:		•								
 Import usin 	ng a CSV file	P											
Enter Device	ce info ma	1	Instructions	udiSoria	Number	controllerProfil	0	description	SLIDI Number	Cortificato SN			
		3	ENCS5406/K9	FGL202	B11JH	ENFV-SDWAN	c	Upload1	Sobrivaniber	00EA60C0			
incel		4	ENCS5406/K9	FGL204	91052	ENFV-SDWAN		Upload1		012FDBFA	Next		
	1	5	ENC\$5406/K9	FGL212	880QA	ENFV-SD Prod	s# support act Name	t show chas:	sis : ENCS5408/K9	01B2AC89			
		6	ENCS5406/K9	FGL204	411CQ	ENFV-SD\Chas	sis Serial	l Num	: FGL2116117H	011F7F0C			
		/	ENCS5408/K9	FGL211	511/H	ENFV-SDVCert:	ificate Se	erial Num	: 17C4313	01/C4313			
			É	È C	isco vľ	Manage 20	4 以降	では、]	ENCS ディ	バイス証明	月		
				書	のシ	リアル番号	けが使用	用できな	い場合、	[SUDI			
				Ν	umber	1列にデバ	イスの	シリア	ル番号をフ	- 人力する、	_		
				لح	で、	デバイスの	· シシリフ	アル番号	を使用し	てデバイ			
				ア	を認	証できます	Cis	co vMan	age スマー		Ũ		
				1-	- デ	バイスのシ	/リア/	レ番号な	使用して	デバイス			
				10			,,,	・田小乙		////			
				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。

Ξ	Cisco Software Cent	ra Download Provisioning	File		×		ର୍ 📧	₩ ^{US} EN
	Cisco's E	Controller Versions 18.3 and	newer		¥ ts chang	jed		\rightarrow
	Cisco Software Central > Plug and Play Conn Plug and Play Connect Devices Controller Profiles Network	Certificates Manage External Virtual A	ccount Event Log	Transactions	Download In PriP To	est Account - KB	✓ ENFV-SDWAN ✓ Idback Support Help	
	+ Add Profile	Delete Selected VMake	Default 🗈 Si	how Log C	13			
	Profile Name	Controller Type	Default	Description		Used By	Download	
	ENFV-SDWAN-DEMO	VEOND	• •	enfv sdwan demo		14	Provisioning File	4
		Controller profile name, Org Name, PODNIP address of vBond, Root Certificate					Showing 1 Record	52055

- 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。

=	-dische Cisco vitanage	٠		 admin 					
	© configuration jericis								
	MAN Edge Lise Controllers								
۰	E Change Mode = 1 Spland MAN Edge Like 🖸 Equant Biostomp Configuration 🔯 Spin Ernert Account			St >O					
٩	Q, Involtigates v			Total Rows:					
	State Device Model Channels Ramber Seriel No./Sitem Enterprise Cert Enter No. Enterprise Cert Enter No. Enterprise Cert Enter No. Enterprise Cert Enter No.	Dente	ie Status	Veday 2					

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	NFVIS 4.6.1	この機能を使用すると、イ
ジのアップロードのサポート	Cisco vManage リリース 20.6.1	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 バッ
		ケーンをアッフロートして、
		VNF イメーンを登録でさま オ
		90

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。

Upload VNF's P	ackage to vManage		×
		Upload Image (Total:1)	
Drag and Drop File Or	 viptela-edge-genericx86-64.qcow2 330.31 MB Description for vedge 	Ū	l
Browse	Disk Image + ROUTER + 20.6	Cisco	L
	cow2 × custom_tag ×	•	
Note : Please ensure Container image	are not deleted when Container is in use	Upload	

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。

30.31	I MB
	Description for vEdge Disk Image
	Disk Image • ROUTER • 20.6 Cisco
	SHA-256 • 9e36/2be4962daa63bce923709155f0dbefeb5d5606837dfaad2ec71a3836f5c
	qcow2 × custom_tag ×

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。

trans Name	###+1721				Ter 68 4.	Manufact citeres						
and a second												
-	(pulad)(h)		Version	1221			Type	ROVTER				-
	Day 9 Configuration	Advance Options										
been see												
mage												
Upload Image	• • •											
	Charlington	and the second sec										
	Carrystee	AND TO DE PROPERTY AND										
	Carotia	Add 12 (2) Hope, Ricgrood, R.										
	Carcular	Ark 1172 Drogs, Aligned										
Day & Cardy	Caronia	Add 1102 Dirop, Aligand X										
Day 0 Config	gration	dd 1122 Bropp, Richard X									_	
Day 0 Coefig	proton	An ISSE Strong, Kingered	_	_	_				_	_	_	
Day 0 Config	Convertion paration	Add State Drogs, Mayood, K.		_	_		-	-	-	-	-	
Day 0 Config	uration period	dd 1212 Drug, Maynell X						_		-	_	
Day D Config Day B Config Day B C	puration bunkg Filer	Mill Prop. Revel X	Persodar		KA Prime	Secondary			Attion			
Day D Config Day B Config Day B C Day B C Day B C Day B C	guration unity File	Mine Are of a col	Personality Evolution	_	RA Pilma Sandara	Secondary	Ves (ofgest	e file	Ation			
Day D Config Day B Config Da	guration autog File (Jac.dy	Manuel Joint poline could be accessed at the second	Persolar Collini Evalued		RA Prime Sandalan Sandalan	Secondary	Van Sonfgord Van Sonfgord	e The e The	Artise 2 1 2 1			
Day D Config Day B Config Da	guration and the grade dust of the dust of the	March Print Information (March 1997) Strandbard (March 1997) Strandbard (March 1997) Strandbard (March 1997)	Personality Continuel Established Established		RA Piles Sandalan Sandalan Sandalan	Secondary	Van Sonfgord Van Gonfgord Van Gonfgord	e Fla e Fla e Fla	Action C 1 C 1 C 1			-

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。

	Gu Comfiguration G, Swerth IV Under 🗰 Rystein Variable 🗰 Custon Variable	r i la companya de la
	1. (anter-fyer: https://doi.box/00/p/*	
b	s. riget-sension 1.4 6. constat-basel-baselage: Bit 9. constat-baselage: articlement; Channer-God-cod'(g* 8. bit-baselage); provide articlement; Channer-God-cod'(g*	
	Id - Anto Mar Id Galerta, Variabi Nane Proven drifte Proven drifte	
	A Contract C	
	D BALLANDA B BALLANDA B HACKTONE R RACKTONE R RACKTONE	
	2) Defection 2) Defection 2) Characteria 3) Characteria 4) Characteria 4) Characteria 5)	
	n terestowani n engologia Nationali Nationali n Montani n	
	in glavovana Zimonen 17. učevnena 28. vyskljava – Line – L	
	er vichował c prosławie v zastawa o prosława c pro	
	Mi wetskowiji di stalovaty mi kazycjowi O Bi Anady	
	Konstruction K	
	0 dOver 4	
	Coroll	
		057
	ter la contra de	52(

3. 必要に応じてイメージプロパティを選択できます。

A DETERMINED IN CONTRACTOR		
CANTENANCE SOFTWARE	for Annu heles	
Advance Onlines	NN ANNE ODDIN	
Additional Image Upload		
Add Storage		
Image Properties		
SR-X2V3Mode	Cable	
Monitored	C Dubie	
Bootup Time (Seconds)	60	
Serial Console	Cubie	
Privleget Mode	Date	
Dedicate Cores (Optimize)	Colle	
WECHLK.AM	Dude	
which must declarize	B Duda	
NOID	Code Evente	
Resource Requirements		
Day 0 Configuration Orive	Cyclone	

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。

•	Cisco vManage							۵	o 🍋 o	admin •
	Software Images Veh	ual Images								
•	O Upload Writed Image	Add Custom VNF Package								00
a.	۹.	fearsh (pri	ana w						,	stal Rows: 6
~	Software Version	Software Location	Network Function Type	Inage Type	Achilecture	Version Type Name	Ventor	Available Files	Updated On	
٠	the(2 server	vnarage	Other	VirtueMachine	x85,64	redHat.	RedHat	OTHER, redHat, thei? server, linux tar.gz	09 Apr 2020 11:27:09 AM PDT	
л.	6.5.0-115	vmanage	Frewal	VirtueMachine	x85,64	FTDv	Once	FREWAUL/FT0+c6.5-0-115_hthrcs.5-0-115_000-	14 Apr 2020 10 49:06 AM PD1	
	19.2.099	vmenage	Rocher	VirtueMachine	x\$6,64	v6rge	Cisce	ROUTER_#Enge_19.2.099_#Enge_19.2.099_#Ena	29 Mar 2020 2:33 24 PM PDT	
5	17.2.1	vmanage	Roder	VirtuaMachine	x86,64	UnifiedSilly	cisco	ROUTOR, Unifed SPIv, 17.2.1, JSRv 1721.1ar gz	03 May 2020 9:36:24 PM PDT	

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。

I