# Dispositivos de borda de WAN NFVIS onboard

## Contents

Introdução
Pré-requisitos
Requisitos
Componentes Utilizados
Hardware
Software
Fluxo de Trabalho PnP
Integração segura do dispositivo compatível com NFVIS
Recuperar Número de Série do Certificado e SN
Adicionar o dispositivo ao portal PnP
PnP em NFVIS
Sincronização do vManage com PnP
Modo on-line
Modo Offline
Conexões NFVIS Automáticas de Onboarding e Controle
<u>Não gerenciando NFVIS</u>

### Introdução

Este documento descreve o processo de integração de sistemas com capacidade NFVIS em um ambiente Catalyst™ SD-WAN para gerenciamento e operação.

### Pré-requisitos

#### Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco SDWAN
- NFVIS
- Plug and Play (PNP)

Presume-se que:

- Os controladores SD-WAN (vManage, vBond e vSmart) já estão implantados com certificados válidos.
- O Cisco WAN Edge (NFVIS, neste caso) tem acessibilidade para o orquestrador vBond e outros controladores SD-WAN que podem ser acessados por meio de endereços IP públicos nos transportes da WAN

• A versão do NFVIS deve ser compatível com o <u>Guia de compatibilidade de componentes de</u> <u>controle.</u>

#### **Componentes Utilizados**

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

#### Hardware

• C8300-UCPE-1N20 (mas pode ser aplicado a qualquer plataforma compatível com NFVIS)

#### Software

- vManage 20.14.1
- vSmart e vBond 20.14.1
- NFVIS 4.14.1

# Fluxo de Trabalho PnP

A confiança nos dispositivos de borda da WAN é feita usando os certificados da cadeia raiz que são pré-carregados na fabricação, carregados manualmente, distribuídos automaticamente pelo vManage ou instalados durante o processo de provisionamento de implantação automatizada PnP ou ZTP.

A solução de SD-WAN usa um modelo de lista de permissões, o que significa que os dispositivos de borda da WAN que têm permissão para se unir à rede de sobreposição de SDWAN precisam ser conhecidos por todos os controladores de SD-WAN com antecedência. Isso é feito adicionando-se os dispositivos de borda da WAN no portal de conexão Plug-and-Play (PnP) em <u>https://software.cisco.com/software/pnp/devices</u>

Este procedimento sempre requer que o dispositivo seja identificado, confiável e com permissão listado na mesma rede de sobreposição. A autenticação mútua precisa ocorrer em todos os componentes da SD-WAN antes de estabelecer conexões de controle seguras entre os componentes da SD-WAN na mesma rede de sobreposição. A identidade do dispositivo de borda da WAN é identificada exclusivamente pela ID do chassi e pelo número de série do certificado. Dependendo do roteador de borda da WAN, os certificados são fornecidos de diferentes maneiras:

- vEdge baseado em hardware: O certificado é armazenado no chip TPM (Módulo à prova de adulteração) instalado durante a fabricação.
- Cisco IOS®-XE SD-WAN baseado em hardware: certificado é armazenado no chip SUDI instalado durante a fabricação.
- · Plataforma virtual ou dispositivos Cisco IOS-XE SD-WAN: não têm certificados raiz (como a

plataforma ASR1002-X) pré-instalados no dispositivo. Para esses dispositivos, uma OTP (One-Time Password, senha única) é fornecida pelo vManage para autenticar o dispositivo com os controladores SD-WAN.

Para executar o ZTP (Zero Touch Provisioning), um servidor DHCP deve estar disponível. Caso contrário, um endereço IP pode ser atribuído manualmente para prosseguir com as etapas restantes do processo Plug and Play (PnP).



Fig. 1. Diagrama do fluxo de trabalho de confiança do dispositivo de Borda PnP e WAN.

### Integração segura do dispositivo compatível com NFVIS

Recuperar Número de Série do Certificado e SN

O chip SUDI (Secure Unique Device Identifier) baseado em hardware do hardware compatível com NFVIS é usado para garantir que apenas dispositivos autorizados possam estabelecer um controle TLS ou DTLS seguro — túnel plano para o orquestrador do SD-WAN Manager. Colete o número de série correspondente usando o comando de nível executivo support show chassis:

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

Adicionar o dispositivo ao portal PnP

Navegue até https://software.cisco.com/software/pnp/devices e selecione a Smart Account e a

Virtual Account corretas para seu ambiente de usuário ou laboratório. (se várias Smart Accounts coincidirem no nome, você poderá distingui-las com o identificador de domínio).

Se você ou seu usuário não souber com qual Smart Account (SA)/Virtual Account (VA) trabalhar, você sempre poderá pesquisar um número de série existente/integrado no link de texto "Pesquisa de dispositivo" para ver a qual SA/VA ele pertence.



Fig. 2. Seleção de SA/VA e botão Pesquisa de dispositivo.

Quando o SA/VA correto for selecionado, clique em "Adicionar dispositivos...":

Plug an	d Play C	Connect								Feedbad	ck Support Help Device Search
			Contification	Manage External \	/irtual Account	Event Log T	ransactions				
Devices C	ontroller Profiles	Network C	seruncates	manage External s							
Devices C	ontroller Profiles	Network C	serunicates	munugo externar y							
Devices C	ontroller Profiles evices	Add Software E	Devices	Edit Selecte	d 📋 De	lete Selected	Enable Extern	al Management.	ansfer Selected	i 🗗	С

Figura 3. "Adicionar dispositivos..." Botão para clicar para registrar o dispositivo físico.

Para esse caso específico, basta colocar um dispositivo na placa, de modo que uma entrada manual é suficiente:

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

Fig. 4. "Adicionar dispositivos..." alternativa para entrada de informações do dispositivo, manual (individual) ou CSV (múltiplo).

Para a etapa 2, clique no botão "+ Identificar dispositivo...". Um modo Formulário é exibido. Preencha os detalhes com as informações mostradas na saída do suporte show chassis do NFVIS e selecione o perfil do controlador vBond correspondente.

	Identify Device		×	
	* Serial Number	XXXXXXXXXX		
	* Base PID	C8300-UCPE-1N20		
Plug and Play Co	Certificate Serial Number	XXXXXXXXXXXXXXXXX		
	Controller Profile	VBOND_PROFILE	-	
	Description	Enter a good description.		
Add Device(s)	SD-WAN Capable	<u></u>		
	Add Additional SUDI			
		K X Certificate Senai Number X	Add	
	SUDI Serial Number	Certificate Serial Number Actions		
Enter device details by clicking		No Devices to Display		0 Errors 0 Existing
+ Identify Device				
	double click to edit certificate	serial number No Devices t	o display	
	Cancel Save			

Figura 5. Formulário de identificação do dispositivo.

Depois de salvá-lo, clique em Next para a Etapa 3 e, finalmente, em Submit para a Etapa 4.

# PnP em NFVIS

Para obter mais informações sobre as diversas definições de configuração para PnP no NFVIS, abrangendo os modos automático e estático, consulte o recurso: <u>Comandos NFVIS PnP.</u>

Observe que o PnP é habilitado por padrão em todas as versões do NFVIS.

### Sincronização do vManage com PnP

#### Modo on-line

Se o vManage puder acessar a Internet e o portal PnP, você deverá ser capaz de apenas executar uma sincronização SA/VA. Para isso, navegue até Configuration > Devices e clique em um botão de texto que indique Sync Smart Account. As credenciais usadas para fazer login na Cisco Software Central são necessárias. Certifique-se de enviar o push de certificado para todos os controladores.

≡ diada Catalyst S	D-WAN	♥ ③ ☱ 우(31) 오 admin ✔
ଙ୍କୁ Monitor	Configuration	Sync Smart Account $ imes$
🕺 Configuration	WAN Edge List Control Components Unclaimed WAN Edges	Organization Name mex-cats-sdwan
* Tools	WAN Edge List (0)	Username *
A Maintenance		Password *
20 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 <sup>©</sup> Device Status Version Reachability	Send to Controllers
Reports		Yes ~
dil Analytics		
Explore		Cancel Syr

Figura 6. Atualização do Roteador de Borda WAN via sincronização SA/VA.

#### Modo Offline

Se o vManage estiver em um ambiente de laboratório ou não tiver acesso à Internet, você poderá carregar manualmente um arquivo de provisionamento do PnP que deve conter o SN adicionado à lista de dispositivos. Este arquivo é do tipo .viptela (Viptela Serial File), que pode ser obtido na guia "Controller Profiles":

					Device dealer
Devices Controller Profiles N	etwork Certificates Manage E	xternal Virtual Account	Event Log Transactions		
+ Add Profile / Edit S	elected 📋 Delete Selected.	🗸 Make Defaul	t 🗈 Show Log 🛛 🕻		
Profile Name	Controller Type	Default	Description	Used By	Download
VBOND_PROFILE	VBOND	~	MEX-CATS vBond Profile.		Provisioning File

Figura 7. Download do arquivo de provisionamento para atualização da lista de WAN do CEdge.

Para carregar manualmente o arquivo de provisionamento, navegue para Configuration > Devices e clique em um botão de texto que indique Upload WAN Edge List. Uma barra lateral aparece onde você pode arrastar e soltar o respectivo arquivo (se o botão Upload não realçar depois que essas ações foram feitas, clique em Escolha um arquivo e procure o arquivo manualmente dentro da janela pop-up explorador de arquivos). Certifique-se de enviar o push de certificado para todos os controladores.

	Configuration	Upload WAN Edge List $ imes$
හිත් Monitor 💦 Configuration	WAN Edge List Control Components Unclaimed WAN Edges	Upload a signed file (.viptela file) from Cisco Plug and Play Or ar un-signed file (.csv file), prepared from the Sample CSV.
🗙 Tools	WAN Edge List (0)	WAN Edge List
A Maintenance		4
Administration	Export Bootstrap Configuration Sync Smart Account Add PAYG WAN Edges Upload WAN Edge List Chassis Number Site Name Hostname Tags Config Locked Managed By © Device Status Version Reachability	Choose a file or drag and drop to upload.
Reports	No data available	serialFilo.viptela
<ul> <li>Explore</li> </ul>		Send to Controllers Yes

Figura 8. Atualização da lista de WAN usando o arquivo de provisionamento (VSF, Viptela Serial File) baixado do portal PnP.

Após concluir o método Online ou Offline, você deverá ser capaz de ver uma entrada de dispositivo na tabela Lista de Borda da WAN que corresponde ao SN do dispositivo registrado no PnP:

≡ dudu Catalys	t SD-WAN									<b>ଓ</b> ⊚ ≡	Q 34	Q admin ❤
Monitor	Configuration											
Configuration	WAN Edge List Control Co	mponents Unclai	med WAN Edges									
🗙 Tools												Export 🛞
A Maintenance	Q Search Table											
Administration	Export Bootstrap Configurati	on Sync Smart Ac	ount Add PAY	'G WAN Edges	Upload WAN Edg	e List						
+ Workflows	Chassis Number	Site Name	Hostname	Tags	Config Locked	Managed By O	Device Status	Version	Reachability	Serial No./Token	System IP	Actions
Reports	C8300-UCPE-1N20-	- · ·		Add Tag ~								
dil Analytics												
Explore												

Figura 9. Dispositivo 8300 na lista de borda.

### Conexões NFVIS Automáticas de Onboarding e Controle

Se o NFVIS puder resolver devicehelper.cisco.com (acessar o PnP pela Internet), a integração será executada automaticamente. Um sistema NFVIS integrado apresenta automaticamente uma configuração de viptela-system:system e vpn 0 que contém informações básicas do controlador.

A partir do Cisco NFVIS versão 4.9.1, é possível estabelecer uma conexão de controle com o plano de gerenciamento através da porta de gerenciamento. A porta de gerenciamento precisa estar acessível com o SD-WAN Manager para uma conexão bem-sucedida com o plano de controle.



Note: Cada comando que contém a palavra-chave "system" precisa ser escrito como system:system. Se a tecla Tab for usada para completar, ela se adapta automaticamente a este novo padrão.

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 VPN 0 é a VPN de transporte predefinida da solução SD-WAN. Ele não pode ser excluído nem modificado. A finalidade dessa VPN é aplicar uma separação entre as redes de transporte da WAN (a camada subjacente) e os serviços de rede (a camada):

```
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
 !
!
```

As conexões de controle são sessões DTLS estabelecidas entre diferentes nós (controladores e roteadores de borda) da malha SD-WAN. Como o NFVIS não é uma plataforma de roteamento responsável pelas decisões de roteamento, ele não forma conexões de controle com o vSmarts. Você pode observar um estado de "desafio" para o vManage:

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	dt]s	10.10.10.10	100	0	10.88.247.71	12946	10.88.247

Isso geralmente indica que não há system-ip, e/ou organization-name está incorretamente ou não

está configurado. O portal PnP e o vBond devem estabelecer o nome da organização e uma vez que a conexão de controle com o vManage tenha sido estabelecida. Caso contrário, empurre essas informações em um <u>NFV Config-Group</u> (suportado a partir de 20.14.1) com o respectivo system-ip e site-id no modelo, ou configure-o estaticamente na subconfiguração viptela-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.

Esses itens podem ser encontrados no vManage:

- Nome da organização: Administração > Configurações > Sistema > Nome da Organização
- IP e porta do validador: Administração > Configurações > Sistema > Validador

Depois que a configuração restante for inserida na subconfiguração viptela-system:system, você precisará de conexões de controle ativas/estabelecidas.

C8300-UCPE-NFVIS#	show	control	connections
-------------------	------	---------	-------------

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.

### Não gerenciando NFVIS

Caso deseje retornar o NFVIS ao seu estado "Não gerenciado", você precisará executar estas ações:

1. Remova a entrada do dispositivo do portal PnP:

			F Luit Out	ectea	Delete	Selected	Enab	le External Management	Transfer Selected	C)	$\mathbf{C}$
lumber		Base Pl	iD T	Product Any	Group	Controller Any	<b>. .</b>	Last Modified	Status Any	Ac	ctions Clear Filters
lı	ımber	Imber	mber Base P	mber Base PID	mber Base PID Product	mber Base PID Product Group	imber Base PID Product Group Controller T Any T Any	mber Base PID Product Group Controller T Any T Any T Any T	imber Base PID Product Group Controller Last Modified	imber Base PID Product Group Controller Last Modified Status           T         Any         T<	imber Base PID Product Group Controller Last Modified Status Ar

Figura 10. Remoção do dispositivo 8300 do portal PnP.

2. NFVIS de redefinição de fábrica.

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

- 3. Etapas opcionais: Remova o dispositivo da lista vManage Edge:
- 3.1 Invalide o certificado do dispositivo.

	dials: Catalyst S	D-WAN							C	⊛ ≔ Ç	24 & adi		
578	Monitor	Configur	ation										
×	Configuration	WAN Edge Li	ist Control Compor	nents Applications									
*													
2													
<b>1</b> 0		Send to Co	ntrollers										
Ð		State	Device Model	Chassis Number	Serial No./Token	Enterprise Cert Serial No	Certificate Expiration Date	Subject SUDI serial #	Hostname	System IP	Invalidate Device		
											valid		
dil									items per page: 25				

Fig. 11. 8300 invalidação do certificado.

3.2 Exclua o dispositivo da lista de Borda da WAN.

	-ilidi: Catalyst Si	D-WAN									<b>o</b> (	⊛ ≔ Q24	Q admin 🗸		
50 50 50	Monitor	Configuration WAN Edge List Control Components Unclaimed WAN Edges											Running Configuration		
*	Tools											Delete WAN Edge			
#0 		C Search Table Export Bootstrap Configuration Sync Smart Account Add PAYG WAN Edges Upload WAN Edge List													
	Workflows Reports	Chassis Number C8300-UCPE-1N20-	Site Name	8300-1-nfvis	Add Tag ~	No No	Unmanaged By U	In Sync	4.14.1-FC1	Reachability	Serial No./Token	Device Bring Up 83.83.83.8	3		
1															

Figura 12. Remoção do 8300 da lista de Borda da WAN.

#### Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.