Dispositivos periféricos WAN NFVIS incluidos

Contenido

Introducción
Prerequisites
Requirements
Componentes Utilizados
Hardware
Software
<u>Flujo de trabajo PnP</u>
Incorporación segura del dispositivo compatible con NFVIS
Recuperar SN y número de serie del certificado
Agregar el dispositivo al portal PnP
PnP en NFVIS
vManage Synchronization with PnP
Modo en línea
Modo sin conexión
Conexiones de control e incorporación automáticas de NFVIS
Desadministración de NFVIS

Introducción

Este documento describe el proceso de incorporación de sistemas compatibles con NFVIS en un entorno Catalyst™ SD-WAN para la gestión y el funcionamiento.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

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

Se presume que:

- Los controladores SD-WAN (vManage, vBond y vSmart) ya están implementados con certificados válidos.
- Cisco WAN Edge (NFVIS en este caso) tiene disponibilidad para el orquestador vBond y otros controladores SD-WAN que son accesibles a través de direcciones IP públicas a través de los transportes WAN

• La versión de NFVIS debe ser compatible con la <u>Guía de compatibilidad de componentes de</u> <u>control.</u>

Componentes Utilizados

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Hardware

• C8300-UCPE-1N20 (pero se puede aplicar a cualquier plataforma compatible con NFVIS)

Software

- vManage 20.14.1
- vSmart y vBond 20.14.1
- VIS 4.14.1

Flujo de trabajo PnP

La confianza de los dispositivos periféricos WAN se realiza mediante los certificados de cadena raíz que se cargan previamente en la fabricación, se cargan manualmente, se distribuyen automáticamente mediante vManage o se instalan durante el proceso de aprovisionamiento de implementación automátizada PnP o ZTP.

La solución SD-WAN utiliza un modelo de lista de permitidos, lo que significa que todos los controladores SD-WAN deben conocer de antemano los dispositivos periféricos WAN que pueden unirse a la red superpuesta SDWAN. Para ello, agregue los dispositivos periféricos WAN al portal de conexión Plug-and-Play (PnP) en <u>https://software.cisco.com/software/pnp/devices</u>

Este procedimiento siempre requiere que el dispositivo se identifique, se confíe y se le permita aparecer en la misma red superpuesta. La autenticación mutua debe producirse en todos los componentes de la SD-WAN antes de establecer conexiones de control seguras entre los componentes de la SD-WAN en la misma red superpuesta. La identidad del dispositivo de extremo de la WAN se identifica de forma exclusiva mediante el ID de chasis y el número de serie del certificado. En función del router de extremo de la WAN, los certificados se proporcionan de diferentes formas:

- vEdge basado en hardware: El certificado se almacena en el chip del módulo a prueba de manipulaciones (TPM) instalado durante la fabricación.
- Cisco IOS®-XE SD-WAN basado en hardware: El certificado se almacena en el chip SUDI instalado durante la fabricación.
- Plataforma virtual para dispositivos Cisco IOS-XE SD-WAN: no tienen certificados raíz (como la plataforma ASR1002-X) preinstalados en el dispositivo. Para estos dispositivos,

vManage proporciona una contraseña de un solo uso (OTP) para autenticar el dispositivo con los controladores SD-WAN.

Para llevar a cabo el aprovisionamiento sin intervención del usuario (ZTP), debe haber disponible un servidor DHCP. Si no es así, se puede asignar manualmente una dirección IP para continuar con los pasos restantes del proceso Plug and Play (PnP).



Fig. 1. Diagrama de flujo de trabajo de confianza de dispositivos PnP y WAN.

Incorporación segura del dispositivo compatible con NFVIS

Recuperar SN y número de serie del certificado

El chip SUDI (identificador de dispositivo único seguro) basado en hardware del hardware compatible con NFVIS se utiliza para garantizar que solo los dispositivos autorizados puedan establecer un túnel de plano de control TLS o DTLS seguro al orquestador de SD-WAN Manager. Recopile el número de serie correspondiente mediante el comando support show chassis executive level:

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

Agregar el dispositivo al portal PnP

Navegue hasta https://software.cisco.com/software/pnp/devices y seleccione la cuenta inteligente

y la cuenta virtual correctas para su usuario o entorno de laboratorio. (si varias cuentas inteligentes coinciden en el nombre, puede distinguirlas con el identificador de dominio).

Si usted o su usuario no sabe con qué cuenta inteligente (SA)/cuenta virtual (VA) trabajar, siempre puede buscar un número de serie existente/incorporado en el enlace de texto "Búsqueda de dispositivos" para ver a qué SA/VA pertenece.



Fig. 2. Selección SA/VA y botón Device Search.

Una vez seleccionada la SA/VA correcta, haga clic en "Add Devices...":

Plug a	and Play	Connect									Feedba	ck Support Help Device Search
		on Notwork Cr	ertificates	Manage External Vi	rtual Account	Event Log Tr	ransactions					
Devices	Controller Proti	es Network Ce										
Devices	Devices	+ Add Software D	Devices	 Edit Selected 	📋 Del	lete Selected	Enable Ex	ternal Managem	ent	Transfer Selected	1 (}	С

Figura 3. "Agregar dispositivos..." Haga clic en este botón para registrar el dispositivo físico.

Para este caso en particular, a bordo solo 1 dispositivo, por lo que una entrada manual es suficiente:

STEP 1	STEP 2	STEP 3	STEP 4	
Identify Source	Identify Device(s)	Review & Submit	Results	
Identify Source				L Download Sample CSV
Select one of the following two options	s to add devices:			
Import using a CSV file		*		
Enter Device info manually				

Fig. 4. Alternativa "Add Devices..." para la entrada de información del dispositivo, manual (individual) o CSV (múltiple).

Para el paso 2, haga clic en el botón "+ Identificar dispositivo...". Aparecerá un formulario modal. Rellene los detalles con la información que se muestra en la salida support show chassis de NFVIS y seleccione el perfil de controlador de vBond correspondiente.

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

Fig. 5. Formulario de identificación del dispositivo.

Una vez guardado, haga clic en Next para el paso 3 y, por último, en Submit para el paso 4.

PnP en NFVIS

Para obtener más información sobre los diversos ajustes de configuración para PnP dentro de NFVIS, que cubren los modos automático y estático, consulte el recurso: <u>Comandos PnP de NFVIS.</u>

Cabe señalar que PnP está habilitado de forma predeterminada en todas las versiones de NFVIS.

vManage Synchronization with PnP

Modo en línea

Si vManage puede acceder a Internet y al portal PnP, debe poder realizar una sincronización SA/VA. Para esto, navegue hasta Configuration > Devices, y haga clic en un botón de texto que indique Sync Smart Account. Se necesitan las credenciales que se utilizan para iniciar sesión en Cisco Software Central. Asegúrese de enviar el envío forzado del certificado a todos los controladores.

≡ disdr Catalyst	SD-WAN	ී 🗇 🏾 🖓 მdmin ✔
St Monitor	Configuration	Sync Smart Account $ imes$
A Configuration	WAN Edge List Control Components Unclaimed WAN Edges	Organization Name mex-cats-sdwan
* Tools	WAN Edge List (0)	Username *
A Maintenance		- Decement *
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 🛈 Device Status Version Reachability	Send to Controllers
Reports		Yes ~
dil Analytics		
		Cancel Syr

Fig. 6. Actualización del router de extremo WAN mediante sincronización SA/VA.

Modo sin conexión

Si vManage está en un entorno de laboratorio o no tiene acceso a Internet, puede cargar manualmente un archivo de aprovisionamiento desde PnP que debe contener el SN que se agregó a la lista de dispositivos. Este archivo es del tipo .viptela (Viptela Serial File), que se puede obtener en la pestaña "Perfiles de controlador":

Plu	ig and Play Connect					Feedback Support Help Device Search				
Device	Devices Controller Profiles Network Certificates Manage External Virtual Account Event Log Transactions									
+	Add Profile / Edit Selected	. 📋 Delete Selected 🗸	Make Default	Show Log						
	Profile Name	Controller Type	Default	Description	Used By	Download				
	VBOND_PROFILE	VBOND	~	MEX-CATS vBond Profile.		Provisioning File				

Fig. 7. Descarga del archivo de aprovisionamiento para la actualización de la lista WAN de CEdge.

Para la carga manual del archivo de aprovisionamiento, navegue hasta Configuration > Devices y haga clic en un botón de texto que indique Upload WAN Edge List. Aparece una barra lateral donde puede arrastrar y soltar el archivo correspondiente (si el botón Cargar no se resalta después de realizar estas acciones, haga clic en Elegir un archivo y busque el archivo manualmente dentro de la ventana emergente del explorador de archivos). Asegúrese de enviar el envío forzado del certificado a todos los controladores.

≡ tister Catalyst S	SD-WAN	🕐 ⑨ 🌐 Q 📵 Զ admin ✔
🕰 Monitor	Configuration	Upload WAN Edge List $ imes$
A Configuration	WAN Edge List Control Components Unclaimed WAN Edges	Upload a signed file (.viptela file) from Cisco Plug and Play Or an 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	Choose a file or drag and drop to
+ Workflows	Chassis Number Site Name Hostname Tags Config Locked Managed By ⁽¹⁾ Device Status Version Reachability	upload. Accepted file: .csv .vjptela
Reports		serialFile.viptela
dial Analytics		()
Explore		Send to Controllers
		Cancel Upload

Fig. 8. Actualización de la lista WAN mediante el archivo de aprovisionamiento (VSF, Viptela Serial File) descargado desde el portal PnP.

Después de completar el método Online (En línea) o Offline (En línea), debe poder ver una entrada de dispositivo en la tabla WAN Edge List (Lista de WAN periférica) que corresponda con el SN del dispositivo registrado en PnP:

= cisco Catalyst	SD-WAN								ଓ ଡ	≡ Q 34	A admi
d Monitor	Configuration										
Configuration	WAN Edge List Control Con	nponents Unclain	ed WAN Edges								
🕻 Tools											🕁 Export
Maintenance											
 Administration 	Export Bootstrap Configuration	n Sync Smart Acci	unt Add PAYG WAN	Edges Upload WAN	Edge List						
Administration Workflows	Export Bootstrap Configuration	n Sync Smart Acco Site Name	Hostname Tags	Edges Upload WAN Centig Locks	Edge List d Managed By [©]	Device Status	Version	Reachability	Serial No./Toker	As of: Oct 10, 2	024 05:05 PM Mem IP Act
Administration Workflows Reports	Export Bootstrap Configuration Chassis Number C8300-UCPE-1N20-	n Sync Smart Acco Site Name	Hostname Tags	Edges Upload WAN CenfigLock Tag ~ No	Edge List d Managed By © Unmanaged	Device Status	Version	Reachability	Serial No./Toke	As of: Oct 10, 2 n Syn	024 05:05 PM Mem IP Act
Administration Workflows Reports Analytics	Export Bootstrap Configuration Chassis Number C8300-UCPE-1N20-	n Sync Smart Acco Site Name -	Hostname Tags	Edges Upload WAN Config Locks Tag ~ No	Edge List d Managed By Φ Unmanaged	Device Status	Version	Reachability	Serial No./Toker	As of: Oct 10, 2 n Syn -	024 05:05 PM

Fig. 9. Dispositivo 8300 dentro de la lista de bordes.

Conexiones de control e incorporación automáticas de NFVIS

Si NFVIS puede resolver devicehelper.cisco.com (ponerse en contacto con PnP a través de

Internet), la incorporación se realiza automáticamente. Un sistema NFVIS incorporado presenta automáticamente una configuración viptela-system:system y vpn 0 que contiene información básica del controlador.

A partir de Cisco NFVIS versión 4.9.1, se admite el establecimiento de una conexión de control con el plano de administración a través del puerto de administración. El puerto de administración debe ser accesible con el Administrador de SD-WAN para una conexión exitosa al plano de control.



Nota: Cada comando que contiene la palabra clave "system" debe escribirse como system:system. Si se utiliza la tecla de tabulación para la finalización, se adapta automáticamente a este nuevo estándar.

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 es la VPN de transporte predefinida de la solución SD-WAN. No se puede eliminar ni modificar. El propósito de esta VPN es hacer cumplir una separación entre las redes de transporte WAN (la capa subyacente) y los servicios de red (la capa superpuesta):

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 ļ 1 ï

Las conexiones de control son sesiones DTLS establecidas entre diferentes nodos (controladores y routers de borde) del fabric SD-WAN. Dado que NFVIS no es una plataforma de routing encargada de las decisiones de routing, no forma conexiones de control con vsmarts. De forma inmediata, puede observar un estado de "desafío" para vManage:

C8300-UCPE-NFVIS# show control connection

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.

Esto indica comúnmente que no hay system-ip, y/o organization-name está mal o no está configurado en absoluto. El portal PnP y vBond deben establecer el nombre de la organización y una vez que se ha establecido la conexión de control con vManage. De lo contrario, inserte esta información dentro de un grupo de configuración de NFV (admitido a partir de 20.14.1) con la ip del sistema y el id del sitio respectivos en la plantilla, o configúrelo estáticamente dentro de la subconfiguración 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.
```

Estos elementos se pueden encontrar en vManage:

- Nombre de la organización: Administration > Settings > System > Organization Name
- IP y puerto del validador: Administration > Settings > System > Validator

Después de ingresar la configuración restante dentro de la subconfiguración viptelasystem:system, necesita conexiones de control activas/establecidas.

C8300-U	CPE-NF	-VIS# show contro	ol connectio	ons			
						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
vmanage	dtls	10.10.10.10	100	0	10.88.247.71

Desadministración de NFVIS

En caso de que desee devolver NFVIS a su estado "No gestionado", debe realizar estas acciones:

1. Elimine la entrada del dispositivo del portal PnP:

+ A	dd Devices	+ Add Software D	evices	/ Edit Sele	ected	📋 Del	lete	Selected	Enab	le External Management.		Transfer Selected	C)	C	
Serial Number			Base PID		D Product		ct Group Controller			Last Modified		Status		Actions	
		· ·	r 📃	τ	Any		Ŧ	Any	. T	dd/mm/yyyy	T	Any	r (Clear Filters	
			C9200 11	DE 11/20	NEV/IS							Pending (Redirection)		howloa	

Fig. 10. 8300 eliminación de dispositivos del portal PnP.

2. Reinicio de fábrica de NFVIS.

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

- 3. Pasos opcionales: Quite el dispositivo de la lista de vManage Edge:
- 3.1 Invalidar el certificado del dispositivo.

≡ diada Catalyst	SD-WAN						C	⊚ ≔ ¢	24 A admin				
Monitor	Configuration												
Configuration	WAN Edge List Control Con	ponents Applications											
🗙 Tools									🕁 Export 🔘				
Maintenance	Q Search Table												
o Administration	Send to Controllers												
Workflows	State Device Model	Chassis Number	Serial No./Token	Enterprise Cert Serial No	Certificate Expiration Date	Subject SUDI serial #	Hostname	System IP	Invalidate Device				
									valid				
II Analytics													

Fig. 11. 8300 invalidación del certificado.

3.2 Elimine el dispositivo de la lista WAN Edge (Extremo de la WAN).

	-diado Catalyst S	D-WAN									o (⊛ ≔ Q24	Q admin 🗸		
5 B	Monitor Configuration	Configuration WAN Edge List Control Components Unclaimed WAN Edges													
*													Delete WAN Edge		
	Maintenance Administration	Q Search Table		Generate Bootstrap Configuration											
۰Ð		Chassis Number	Site Name	Hostname	Tags	Config Locked	Managed By O	Device Status	Version	Reachability	Serial No./Token				
					Add Tag 🗸										
(2)	Postana		_	_		_	_	_			_	_	_		

Fig. 12. Eliminación de 8300 de la lista de WAN Edge.

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).