Dispositivi onboard NFVIS WAN Edge

Sommario

Introduzione

Questo documento descrive il processo di integrazione di sistemi compatibili con NFVIS in un ambiente Catalyst™ SD-WAN per la gestione e il funzionamento.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

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

Si presume che:

- I controller SD-WAN (vManage, vBond e vSmart) sono già distribuiti con certificati validi.
- Cisco WAN Edge (NFVIS in questo caso) è raggiungibile dall'orchestrator vBond e da altri controller SD-WAN raggiungibili tramite indirizzi IP pubblici sui trasporti WAN
- La versione NFVIS deve essere conforme alla Control Components Compatibility Guide.

Componenti usati

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Hardware

- C8300-UCPE-1N20 (ma può essere applicato a qualsiasi piattaforma compatibile con NFVIS)

Software

- vManage 20.14.1
- vSmart e vBond 20.14.1
- NFVIS 4.14.1

Flusso di lavoro Plug and Play

L'attendibilità dei dispositivi perimetrali WAN viene ottenuta utilizzando i certificati della catena principale precaricati in fase di produzione, caricati manualmente, distribuiti automaticamente da vManage o installati durante il processo di provisioning dell'installazione automatizzata PnP o ZTP.

La soluzione SD-WAN utilizza un modello di elenco dei dispositivi consentiti, il che significa che i dispositivi WAN Edge a cui è consentito collegarsi alla rete di overlay SDWAN devono essere noti da tutti i controller SD-WAN in anticipo. A tale scopo, aggiungere i dispositivi edge WAN nel portale di connessione Plug-and-Play (PnP) all'indirizzo https://software.cisco.com/software/pnp/devices

Questa procedura richiede sempre che il dispositivo sia identificato, considerato attendibile e consentito nella stessa rete di sovrapposizione. L'autenticazione reciproca deve avvenire su tutti i componenti SD-WAN prima di stabilire connessioni di controllo sicure tra i componenti SD-WAN nella stessa rete di sovrapposizione. L'identità del dispositivo WAN Edge è identificata in modo univoco dall'ID dello chassis e dal numero di serie del certificato. A seconda del router WAN Edge, i certificati vengono forniti in modi diversi:

- vEdge basato su hardware: Il certificato è memorizzato nel chip TPM (Tamper Proof Module) installato durante la produzione.
- Cisco IOS®-XE SD-WAN basato su hardware: è memorizzato nel chip SUDI di bordo installato durante la fabbricazione.
- Piattaforma virtuale o dispositivi Cisco IOS-XE SD-WAN: non dispongono di certificati radice preinstallati nel dispositivo, ad esempio la piattaforma ASR1002-X. Per questi dispositivi, vManage fornisce una One-Time Password (OTP) per autenticare il dispositivo con i

controller SD-WAN.

Per eseguire Zero Touch Provisioning (ZTP), deve essere disponibile un server DHCP. In caso contrario, è possibile assegnare manualmente un indirizzo IP per continuare le fasi rimanenti del processo Plug and Play (PnP).

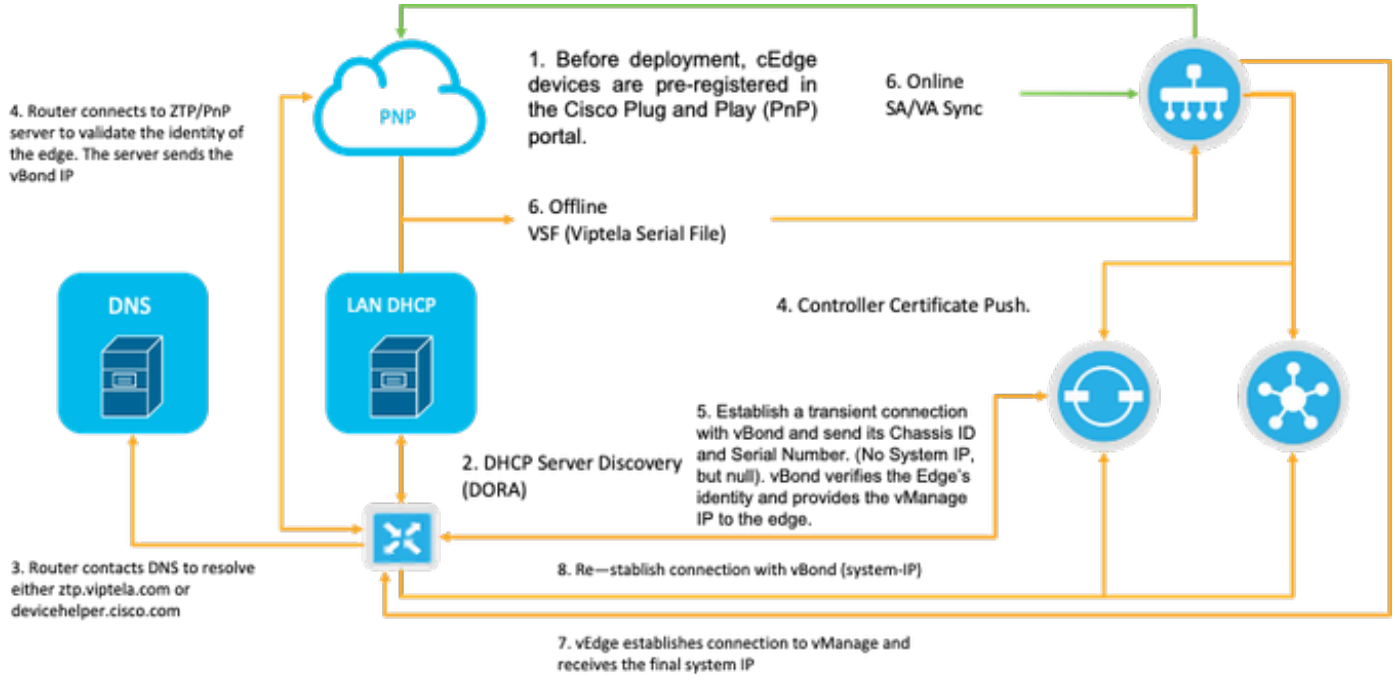


Fig. 1. Diagramma del flusso di lavoro relativo all'attendibilità dei dispositivi VPN e WAN Edge.

Caricamento sicuro del dispositivo compatibile NFVIS

Recupera numero di serie e numero di serie certificato

Il chip SUDI (Secure Unique Device Identifier) basato su hardware, proveniente da hardware compatibile con NFVIS, viene utilizzato per garantire che solo i dispositivi autorizzati possano stabilire un controllo TLS o DTLS sicuro: pianificare il tunnel verso l'orchestrator di SD-WAN Manager. Raccogliere il numero di serie corrispondente utilizzando il comando support show chassis executive level:

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

Aggiungi il dispositivo al portale Plug and Play

Passare a https://software.cisco.com/software/pnp/devices e selezionare lo Smart Account e l'account virtuale corretti per l'utente o l'ambiente lab. (se il nome di più Smart Account coincide, è

possibile distinguerli dall'identificatore di dominio).

Se l'utente non sa con quale account Smart Account (SA)/account virtuale (VA) lavorare, è sempre possibile cercare e inserire il numero di serie esistente/caricato nel collegamento di testo "Ricerca dispositivo" per verificare a quale SA/VA appartiene.

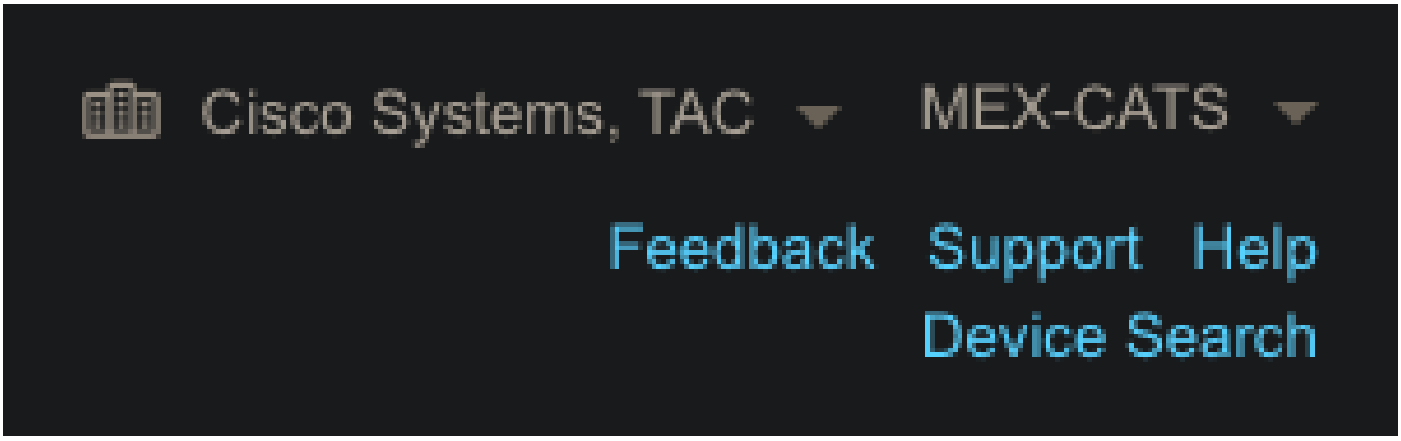


Fig. 2. Pulsante Selezione SA/VA e Ricerca periferica.

Dopo aver selezionato l'SA/VA corretto, fare clic su "Add Devices...":

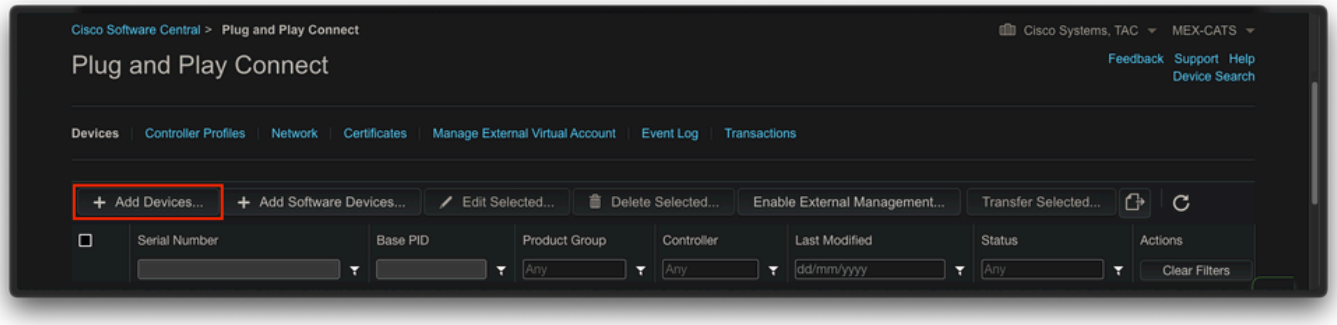


Fig. 3. "Aggiungi dispositivi..." Pulsante su cui fare clic per la registrazione del dispositivo fisico.

Per questo caso particolare, solo 1 dispositivo a bordo, quindi è sufficiente un inserimento manuale:

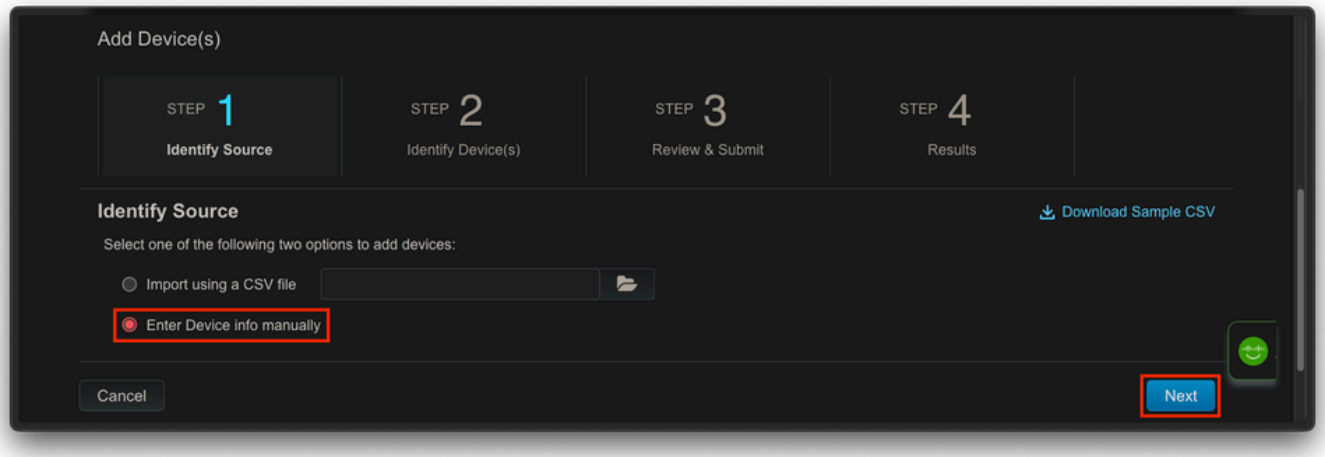


Fig. 4. Alternativa "Add Devices..." (Aggiungi dispositivi...) per l'immissione di informazioni sui dispositivi, manuale (individuale) o CSV (multipla).

Per il punto 2, fare clic sul pulsante "+ Identify Device...". Viene visualizzato un modulo modale. Completare i dettagli con le informazioni mostrate sul supporto show chassis output di NFVIS e selezionare il profilo controller vBond corrispondente.

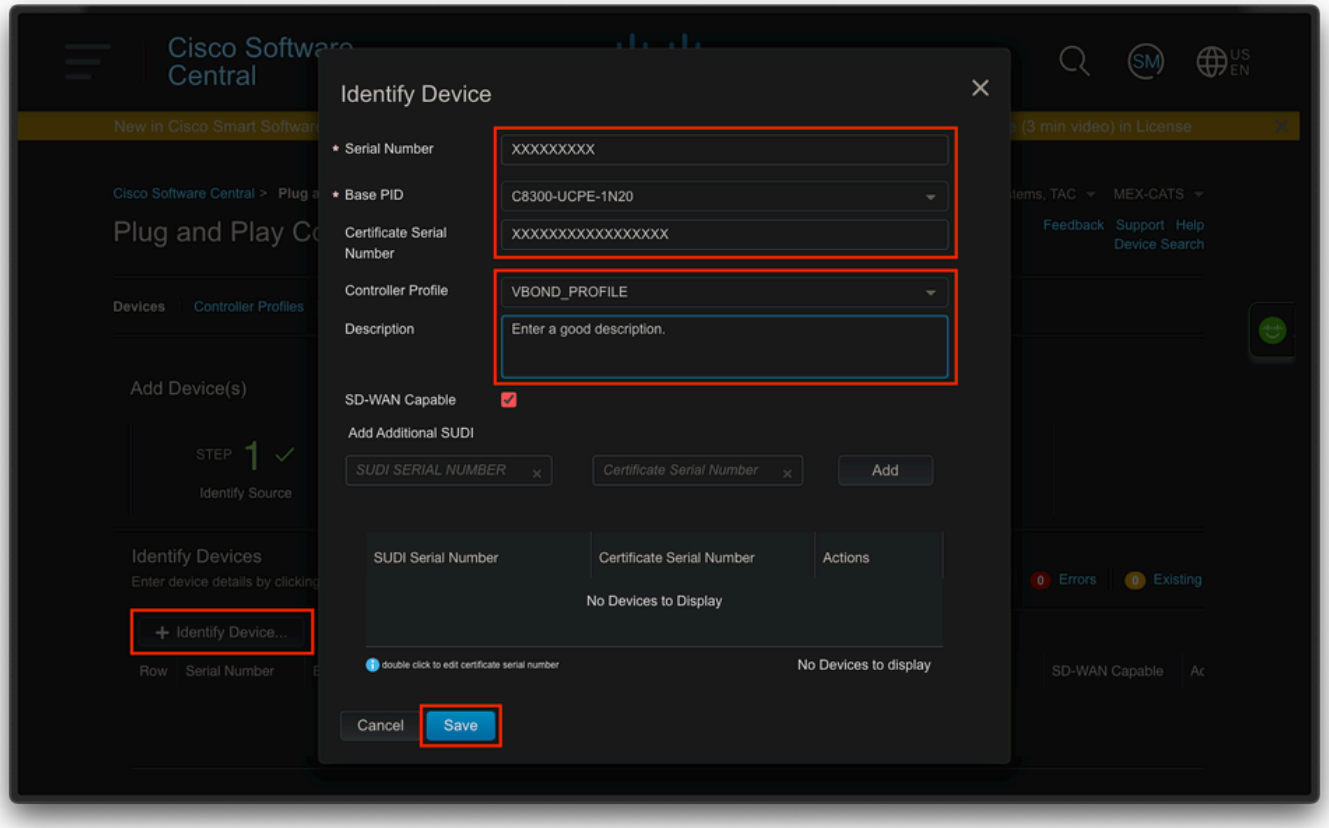


Fig. 5. Modulo di identificazione del dispositivo.

Una volta salvato, fare clic su Next (Avanti) per il passo 3 e infine su Submit per il passo 4.

PnP In NFVIS

Per ulteriori informazioni sulle diverse impostazioni di configurazione per PnP all'interno di NFVIS, relative sia alla modalità automatica che statica, fare riferimento alla risorsa Comandi PnP NFVIS.

Si noti che PnP è abilitato per impostazione predefinita su tutte le versioni NFVIS.

vManage - sincronizzazione con PnP

Modalità online

Se vManage è in grado di raggiungere Internet e il portale PnP, è sufficiente eseguire una sincronizzazione SA/VA. A tale scopo, selezionare Configuration > Devices, quindi fare clic su un pulsante di testo che indica Sync Smart Account. Sono necessarie le credenziali utilizzate per

accedere a Cisco Software Central. Assicurarsi di inviare il push del certificato a tutti i controller.

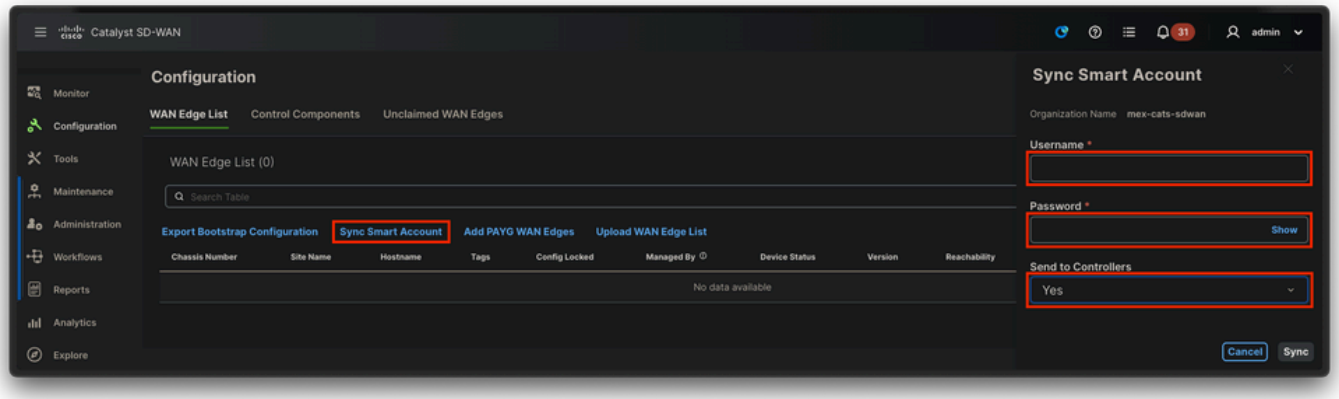


Fig. 6. Aggiornamento del WAN Edge Router tramite sincronizzazione SA/VA.

Modalità offline

Se vManage si trova in un ambiente lab o non dispone di accesso a Internet, è possibile caricare manualmente un file di provisioning da PnP che deve contenere il numero di serie aggiunto all'elenco dei dispositivi. Questo file è di tipo .viptela (Viptela Serial File), disponibile nella scheda "Profili controller":

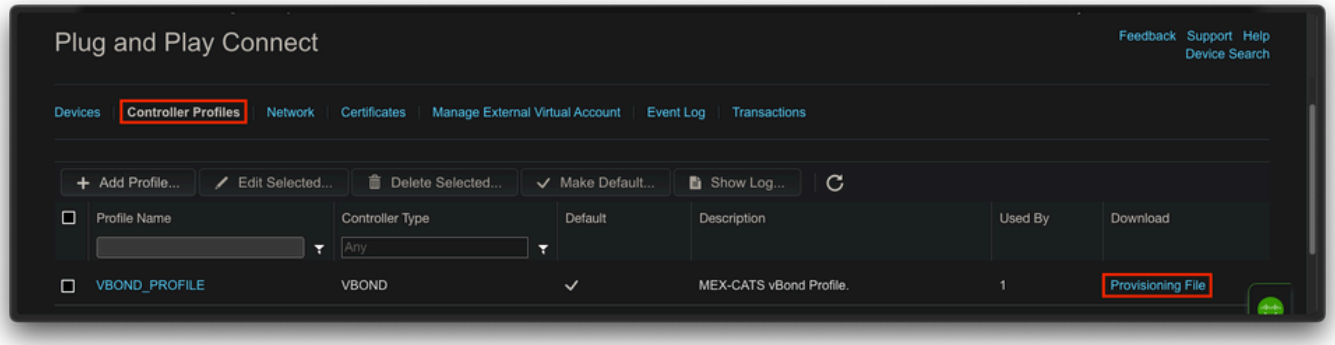


Fig. 7. Download dei file di provisioning per l'aggiornamento dell'elenco WAN CEdge.

Per il caricamento manuale del file di provisioning, selezionare Configuration > Devices, quindi fare clic su un pulsante di testo che indica Upload WAN Edge List. Viene visualizzata una barra laterale in cui è possibile trascinare il file corrispondente. Se il pulsante Upload non viene evidenziato dopo aver eseguito queste operazioni, fare clic su Choose a file and search for the file manual all'interno della finestra pop-up file explorer. Assicurarsi di inviare il push del certificato a tutti i controller.

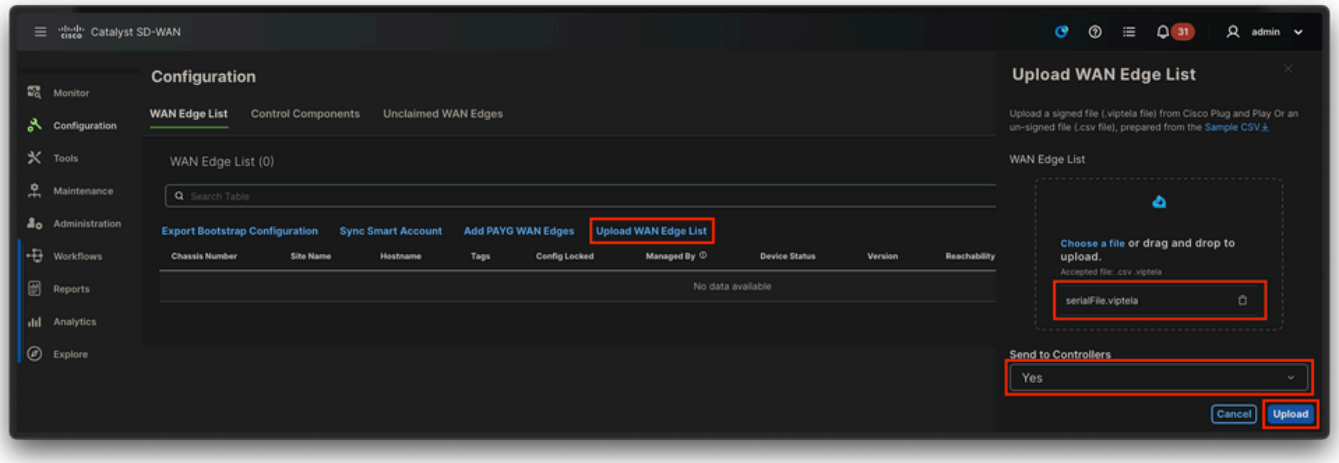


Fig. 8. Aggiornamento dell'elenco WAN utilizzando il file di provisioning (VSF, Viptela Serial File) scaricato dal portale PnP.

Dopo aver completato il metodo Online o Offline, è necessario essere in grado di visualizzare una voce di dispositivo nella tabella Elenco bordi WAN corrispondente al numero di serie del dispositivo registrato in PnP:

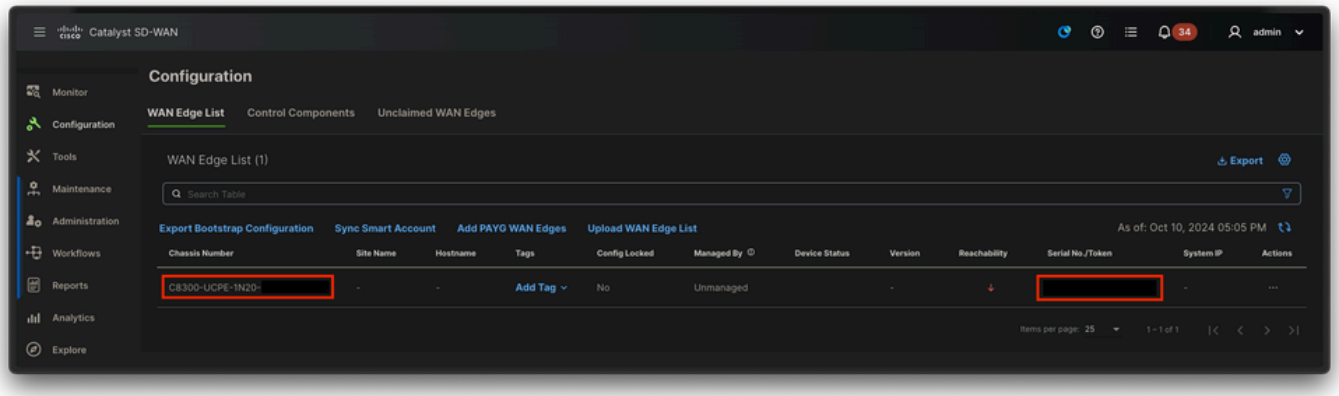
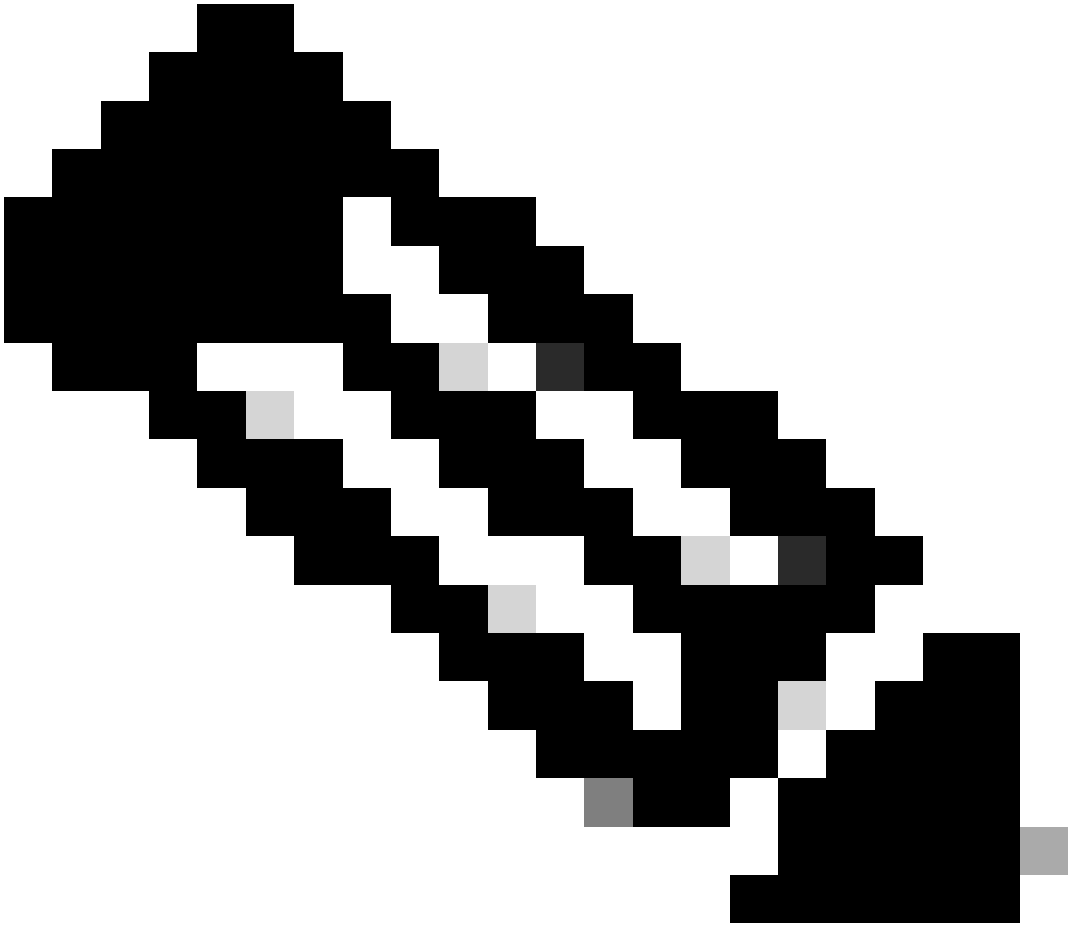


Fig. 9. Dispositivo 8300 all'interno dell'elenco dei bordi.

Connessioni di caricamento e controllo automatici NFVIS

Se NFVIS è in grado di risolvere devicehelper.cisco.com (raggiungere PnP tramite Internet), l'onboarding viene eseguito automaticamente. Un sistema NFVIS integrato presenta automaticamente una configurazione vptela-system:system e vpn 0 contenente le informazioni di base sul controller.

A partire dalla versione 4.9.1 di Cisco NFVIS, è supportata la creazione di una connessione di controllo al piano di gestione tramite la porta di gestione. La porta di gestione deve essere raggiungibile con SD-WAN Manager per una connessione riuscita al control plane.



Nota: Ogni comando contenente la parola chiave "system" deve essere scritto come system:system. Se viene utilizzato il tasto TAB per il completamento, si adatta automaticamente a questo nuovo standard.

```
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 è la VPN di trasporto predefinita della soluzione SD-WAN. Non può essere eliminato né modificato. Lo scopo di questa VPN è quello di imporre una separazione tra le reti di trasporto WAN (l'underlay) e i servizi di rete (l'overlay):

```
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
  !
 !
!
```

Le connessioni di controllo sono sessioni DTLS stabilite tra nodi diversi (controller e router perimetrali) della struttura SD-WAN. Poiché NFVIS non è una piattaforma di routing responsabile delle decisioni di instradamento, non crea connessioni di controllo con vSmarts. È possibile osservare lo stato di "verifica" per vManage:

```
C8300-UCPE-NFVIS# show control connection
                                                                                    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                        12346 10.88.247.
vmanage dtls 10.10.10.10     100        0      10.88.247.71                        12946 10.88.247.
```

Ciò indica in genere che non esiste alcun ip di sistema e/o che il nome dell'organizzazione è errato o non è configurato affatto. Il portale PnP e vBond devono stabilire il nome dell'organizzazione e una volta stabilita la connessione di controllo con vManage. In caso contrario, inserire le informazioni in un NFV Config-Group (supportato a partire dalla versione 20.14.1) con l'ip del sistema e l'id del sito rispettivi nel modello o configurarlo staticamente nella sottoconfigurazione vlan-system: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.
```

Questi elementi sono disponibili in vManage:

- Nome organizzazione: Amministrazione > Impostazioni > Sistema > Nome organizzazione
- Validator IP and Port: Amministrazione > Impostazioni > Sistema > Convalida

Dopo aver immesso la configurazione rimanente nella sottoconfigurazione vlan-system:system, sono necessarie connessioni di controllo attive/stabilite.

```
C8300-UCPE-NFVIS# show control connections
                                                                                    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                        12346 10.88.247.
vmanage dtls 10.10.10.10     100        0      10.88.247.71                        12946 10.88.247.
```

Non gestione NFVIS

Se si desidera ripristinare lo stato "Non gestito" di NFVIS, è necessario eseguire le azioni

seguenti:

1. Rimuovere la voce relativa al dispositivo dal portale PnP:

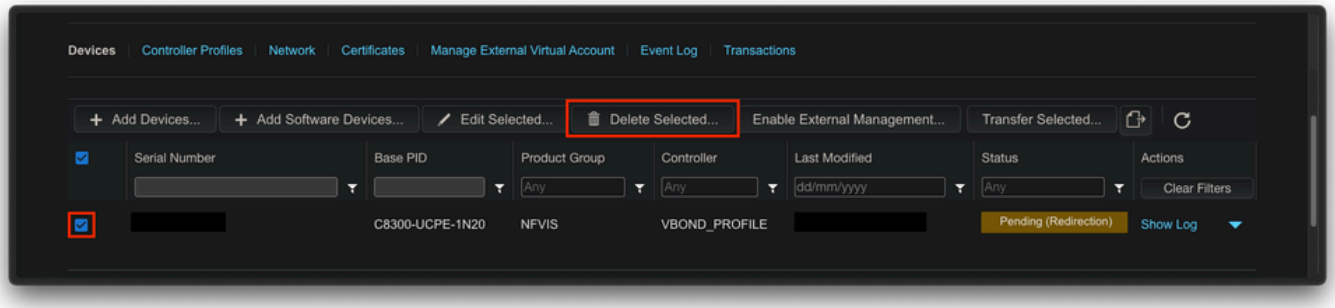


Fig. 10. 8300 rimozione di dispositivi dal portale PnP.

2. NFVIS ripristinato in fabbrica.

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

3. Fasi facoltative: Rimuovere il dispositivo dall'elenco vManage Edge:

3.1 Invalidare il certificato del dispositivo.

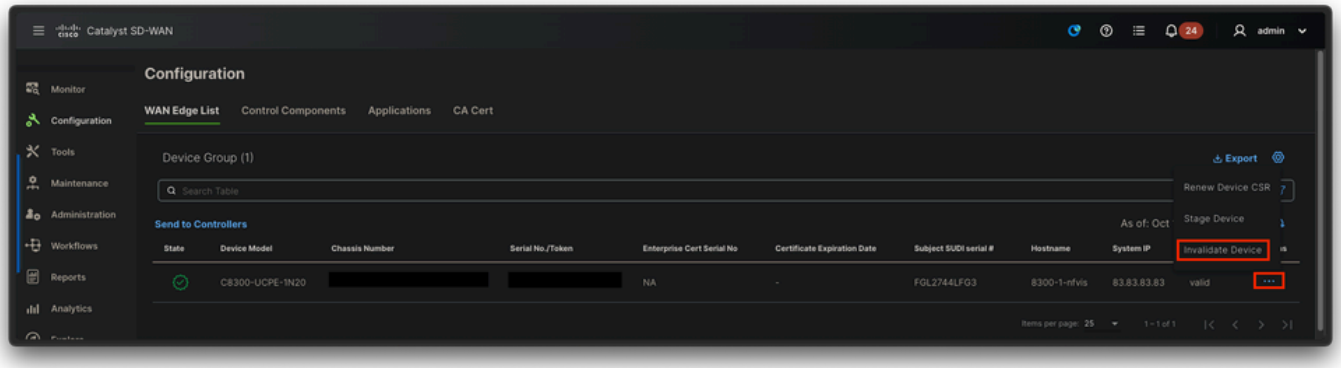


Fig. 11. Invalidazione del certificato 8300.

3.2 Eliminare il dispositivo dall'elenco dei bordi WAN.

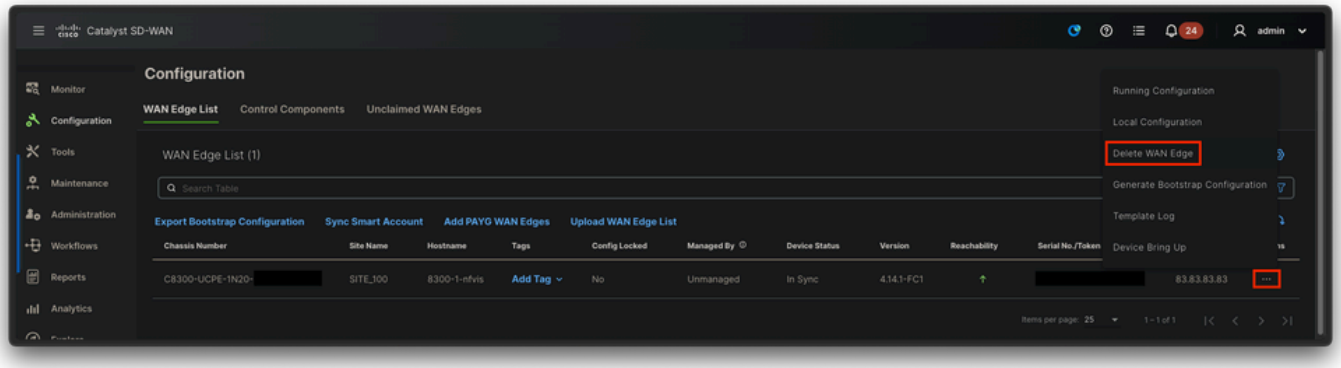


Fig. 12. 8300 rimozione dall'elenco dei bordi della WAN.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).