板載NFVIS WAN邊緣裝置

目錄

簡介

本文檔介紹將支援NFVIS的系統註冊到Catalyst™ SD-WAN環境以進行管理和操作的過程。

必要條件

需求

思科建議您瞭解以下主題：

- Cisco SDWAN
- NFVIS
- 即插即用(PNP)

推定：

- SD-WAN控制器（vManage、vBond和vSmart）已部署為有效的證書。
- Cisco WAN Edge（此案例中為NFVIS）可訪問vBond orchestrator和其他SD-WAN控制器，這些控制器可通過廣域網傳輸中的公共IP地址訪問
- NFVIS版本必須符合《控制組件相容性指南》。

採用元件

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

硬體

- C8300-UCPE-1N20(但可應用於任何具有NFVIS功能的平台)

軟體

- vManage 20.14.1
- vSmart和vBond 20.14.1
- NFVIS 4.14.1

PnP工作流

WAN邊緣裝置的信任通過根鏈證書來完成，根鏈證書是在製造過程中預載入的、手動載入的、由vManage自動分發的，或者是在PnP或ZTP自動部署調配過程中安裝的。

SD-WAN解決方案使用允許清單模式，這意味著允許加入SDWAN重疊網路的WAN邊緣裝置需要事先由所有SD-WAN控制器知道。這是通過在即插即用連線門戶(PnP)的 https://software.cisco.com/software/pnp/devices中新增WAN邊緣裝置來實現的

此過程始終要求在同一重疊網路中標識、信任和允許列出裝置。在相同重疊網路中的SD-WAN元件之間建立安全控制連線之前，需要在所有SD-WAN元件之間執行相互身份驗證。WAN邊緣裝置的身份由機箱ID和證書序列號唯一標識。根據WAN邊緣路由器，證書提供方式不同：

- 基於硬體的vEdge:證書儲存在製造期間安裝的板載防篡改模組(TPM)晶片中。
- 基於硬件的Cisco IOS®-XE SD-WAN:證書儲存在製造期間安裝的板載SUDI晶片中。
- Cisco IOS-XE SD-WAN裝置的虛擬平台：裝置上未預安裝根證書（如ASR1002-X平台）。對於這些裝置，vManage提供一次性密碼(OTP)以使用SD-WAN控制器驗證裝置。

要執行零接觸調配(ZTP)，必須有DHCP伺服器。如果沒有，可以手動分配IP地址以繼續執行即插即用(PnP)過程的其餘步驟。

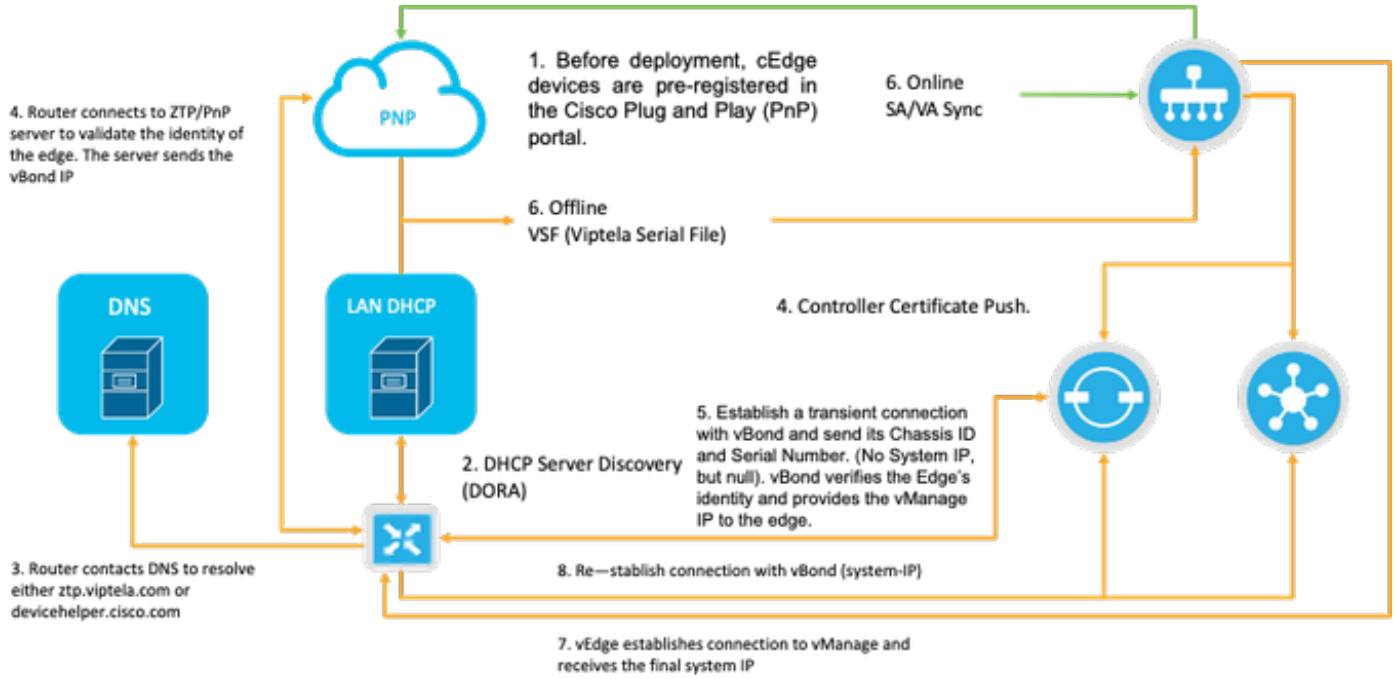


圖1. PnP和WAN Edge裝置信任工作流程圖。

支援NFVIS的裝置安全自註冊

檢索SN和證書序列號

基於硬體的SUDI（安全唯一裝置識別符號）晶片來自支援NFVIS的硬體，用於確保只有授權裝置才能建立安全的TLS或DTLS控制 — 通向SD-WAN Manager協調器的平面隧道。使用support show chassis executive level命令收集相應的序列號：

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

將裝置新增到PnP門戶

導航到https://software.cisco.com/software/pnp/devices，並為您的使用者或實驗室環境選擇正確的智慧帳戶和虛擬帳戶。（如果多個智慧帳戶的名稱一致，則您可以將其與域識別符號區分開來）。

如果您或您的使用者不知道使用哪個智慧帳戶(SA)/虛擬帳戶(VA)，您始終可以在「裝置搜尋」文本連結中搜尋現有/已登入的序列號以檢視它屬於哪個SA/VA。

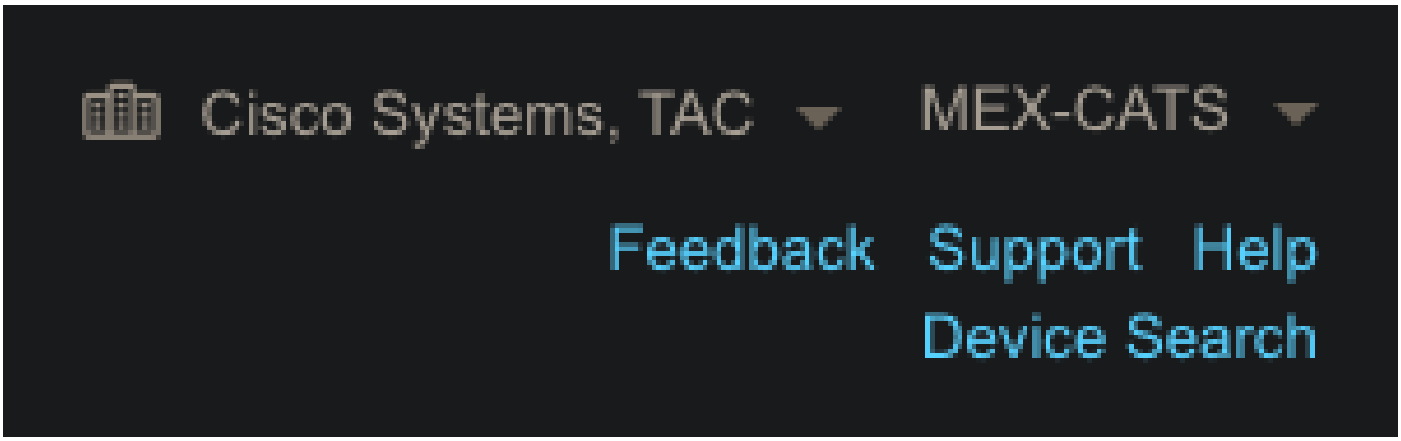


圖2. SA/VA選擇和裝置搜尋按鈕。

選擇正確的SA/VA後，按一下「Add Devices...」：

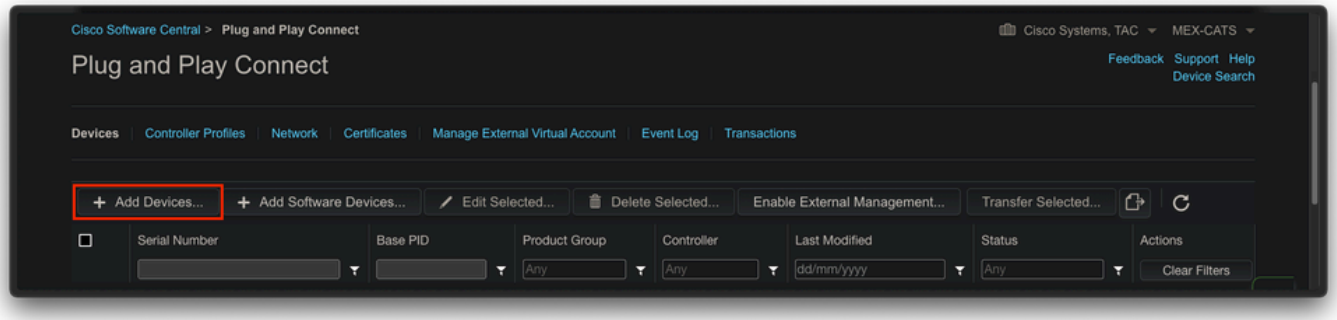


圖3. 「新增裝置.....」 按一下此按鈕進行物理裝置註冊。

對於此特定情況，僅板載1台裝置，因此手動輸入就足夠了：

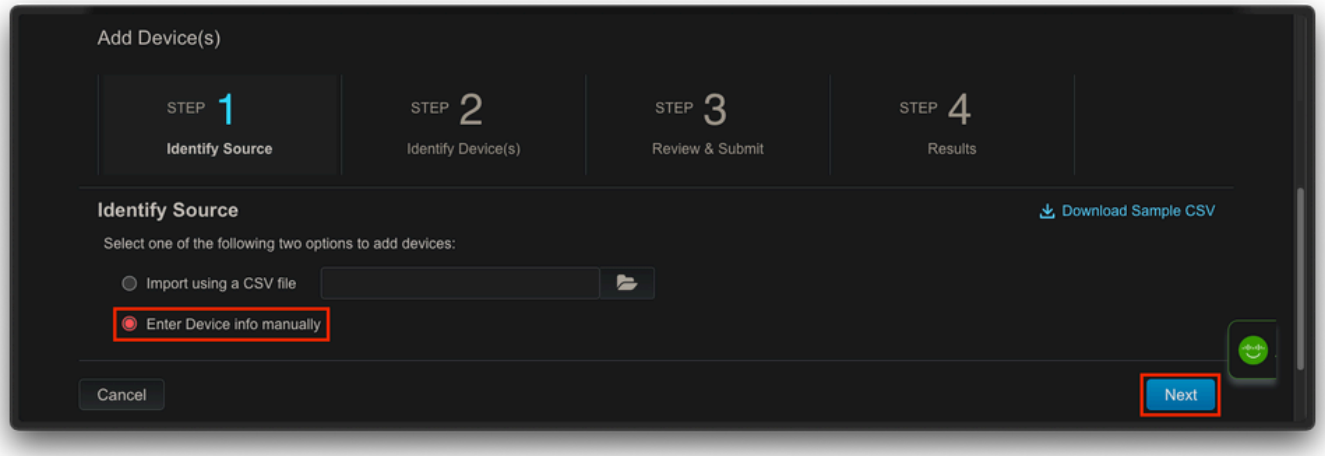


圖4.裝置資訊輸入、手動（單獨）或CSV（多重）的「新增裝置.....」替代方法。

對於步驟2，點選「+識別裝置.....」按鈕。將出現「表單」模式。使用NFVIS的support show chassis輸出中顯示的資訊填寫詳細資訊，並選擇相應的vBond控制器配置檔案。

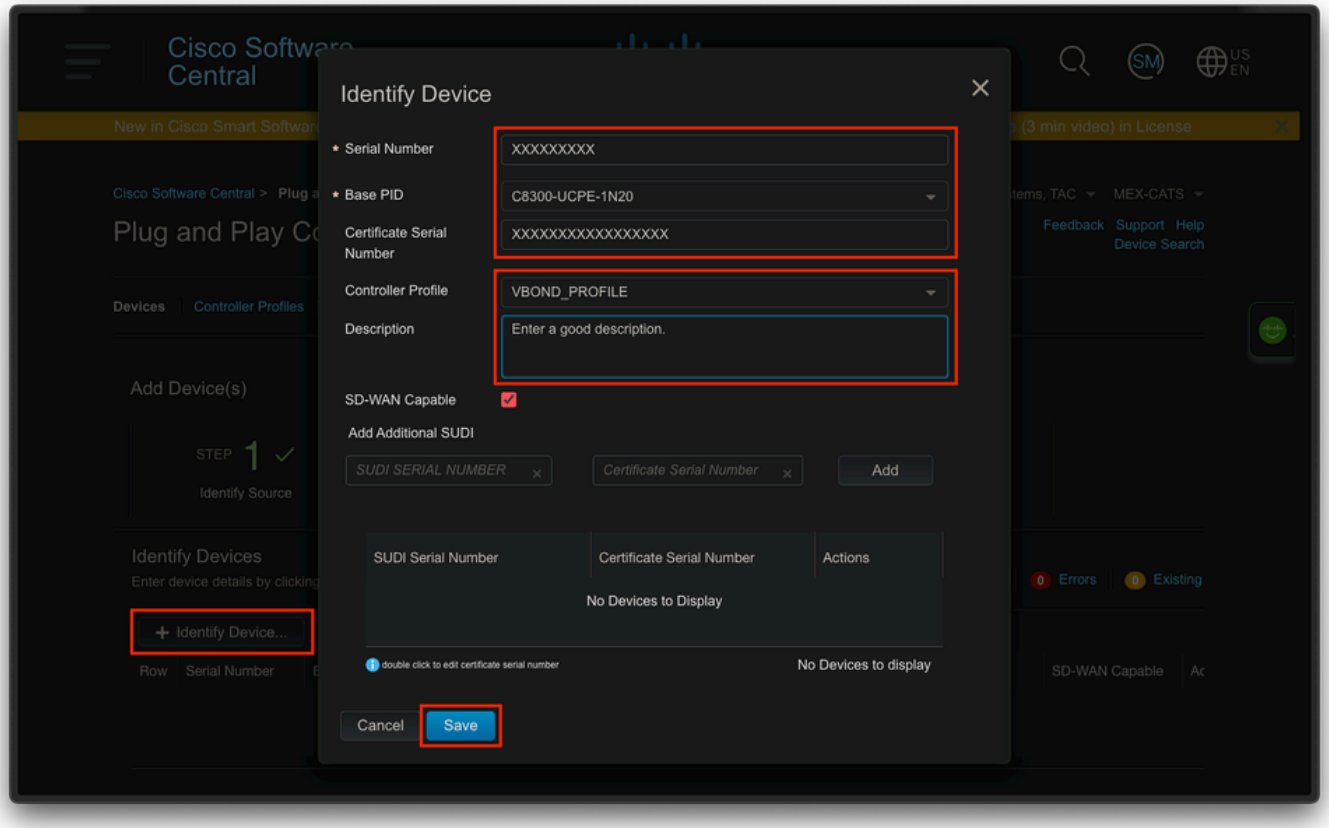


圖5.裝置標識表。

儲存後，按一下Next（下一步）執行步驟3，最後按一下Submit（提交）執行步驟4。

NFVIS中的PnP

有關NFVIS內PnP的不同配置設定（包括自動模式和靜態模式）的詳細資訊，請參閱資源：[NFVIS PnP命令。]

應注意，所有NFVIS版本上預設都啟用PnP。

vManage與PnP的同步

線上模式

如果vManage可以訪問Internet和PnP門戶，您必須能夠僅執行SA/VA同步。為此，請導航到Configuration > Devices，然後按一下指示Sync Smart Account的文本按鈕。需要用於登入思科軟體中心的憑證。請確保將證書推送傳送到所有控制器。

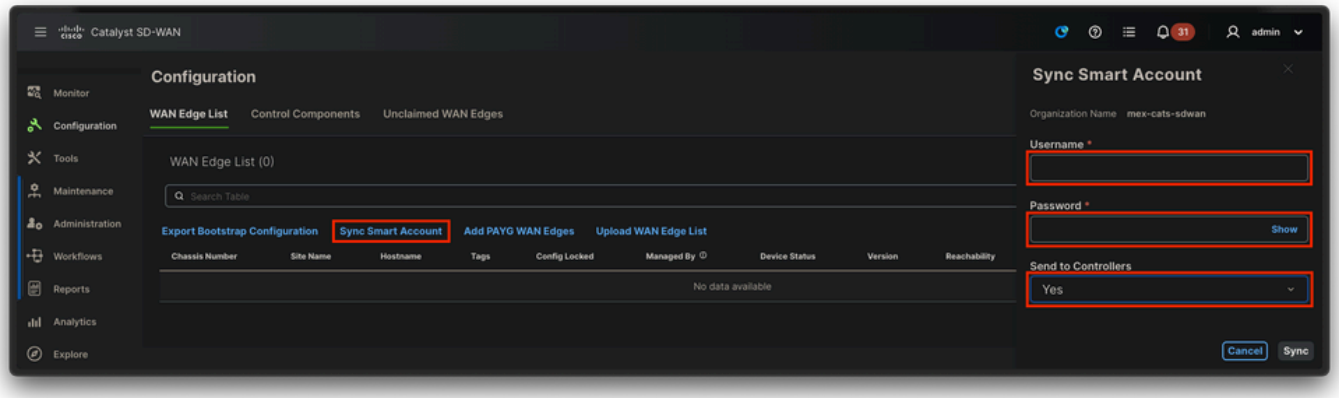


圖6.通過SA/VA同步進行的WAN邊緣路由器更新。

離線模式

如果vManage在實驗室環境中或者無法訪問Internet，則可以從PnP手動上傳必須包含已新增到裝置清單的SN的調配檔案。此檔案的型別為.viptela(Viptela Serial File)，可從「Controller Profiles」索引標籤取得：

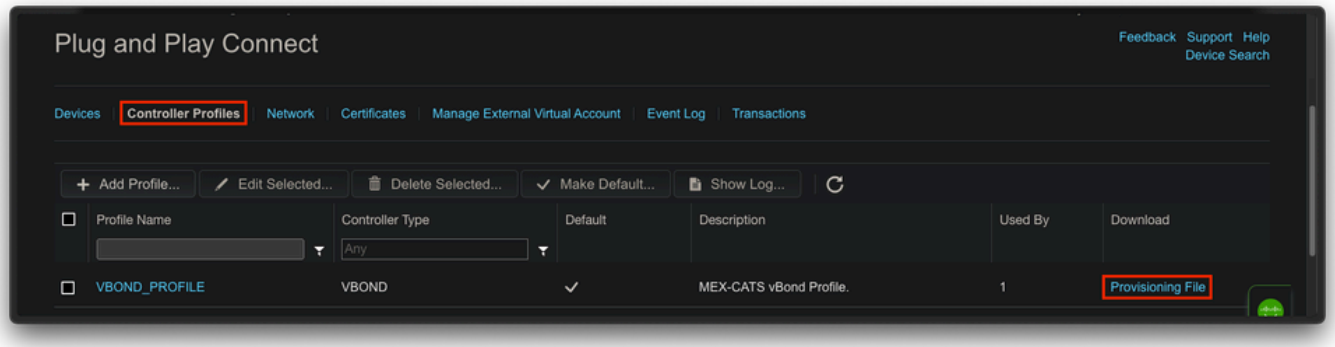


圖7.為CEdge WAN清單更新調配檔案下載。

要手動上傳調配檔案，請導航到Configuration > Devices，然後點選指示Upload WAN Edge List的文本按鈕。系統將顯示一個側欄，您可以在其中拖放各個檔案(如果在執行這些操作後沒有選中Upload 按鈕，則按一下Choose a file，然後在彈出檔案資源管理器視窗中手動搜尋檔案)。 請確保將證書推送傳送到所有控制器。

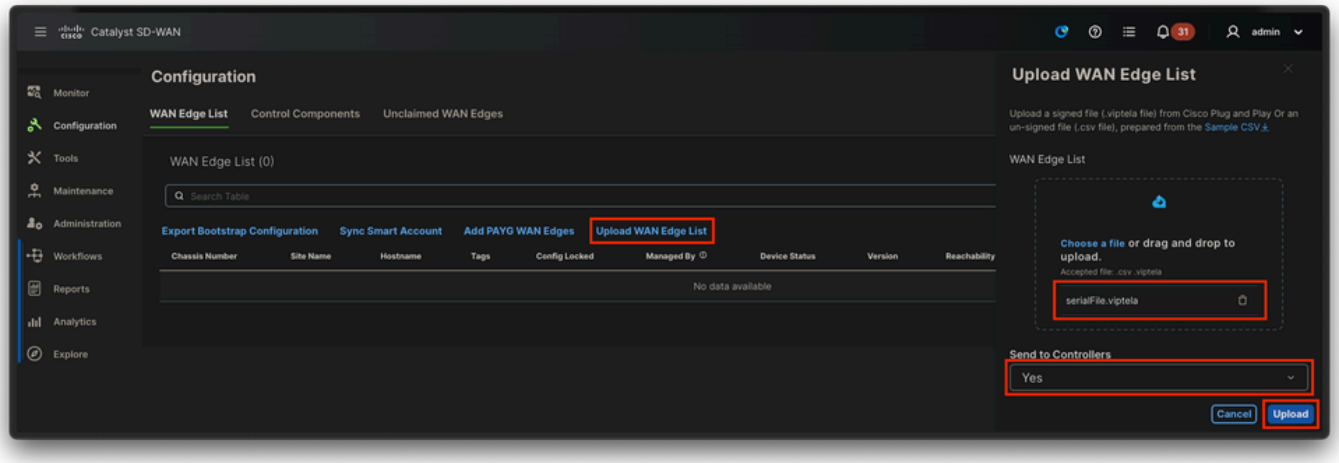


圖8.使用從PnP門戶下載的調配檔案（VSF、Viptela串列檔案）更新WAN清單。

完成Online或Offline方法後，您必須能夠在WAN邊緣清單表中看到與PnP中註冊的裝置的SN對應的裝置條目：

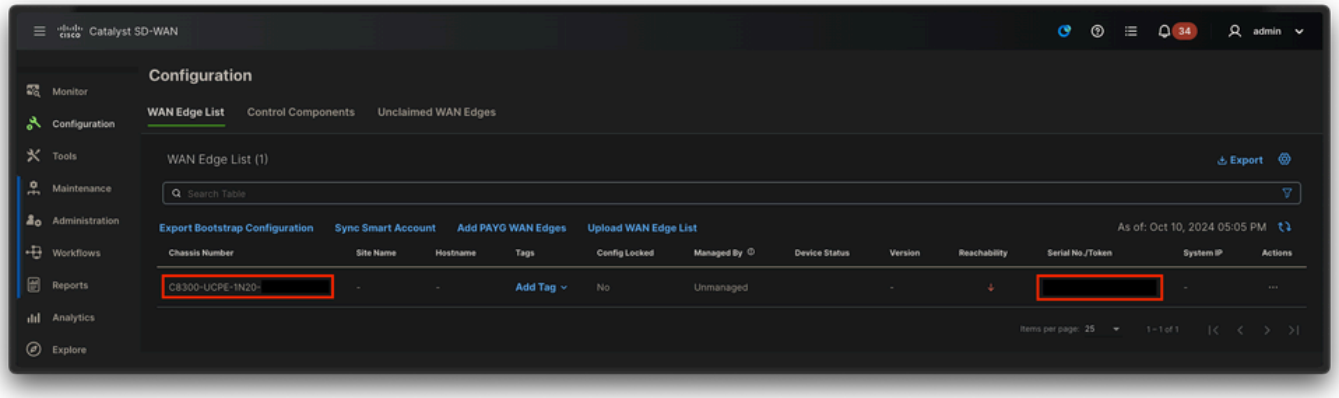
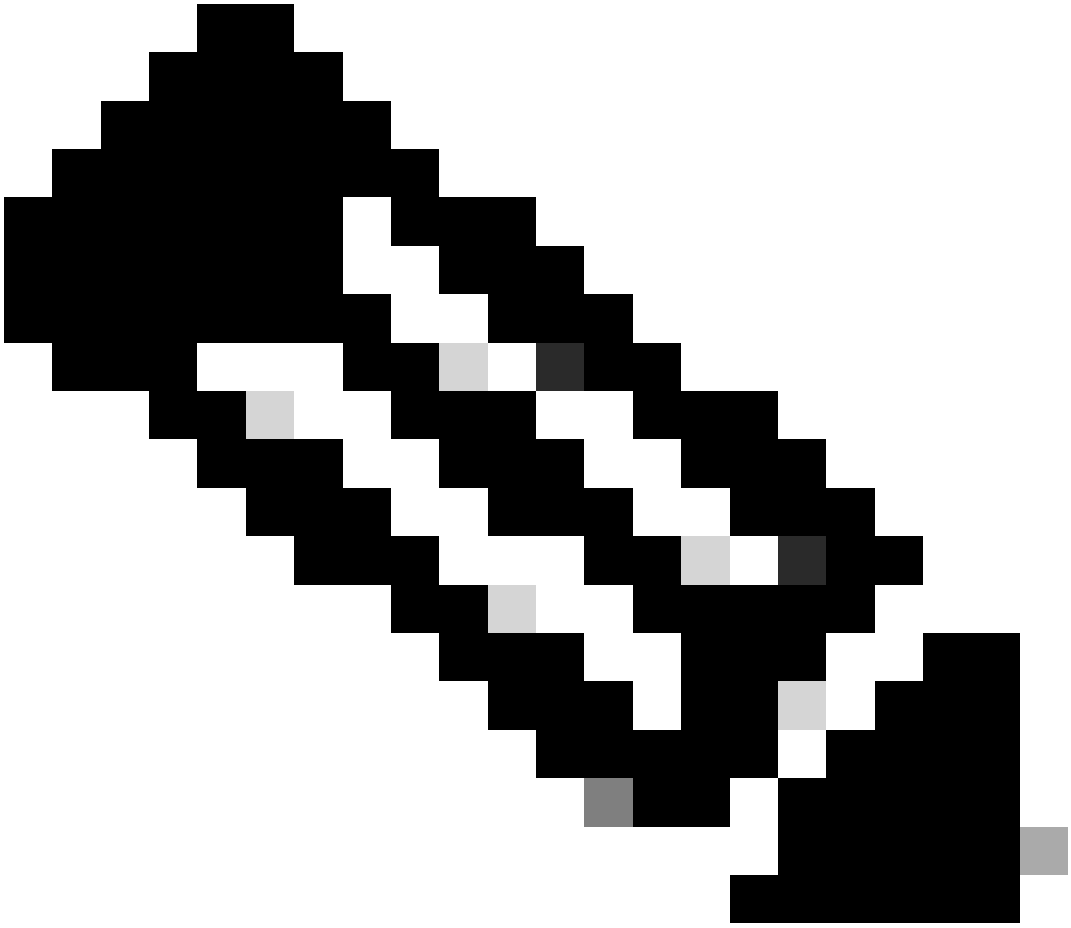


圖9.邊緣清單中的裝置8300。

NFVIS自動載入和控制連線

如果NFVIS能夠解析devicehelper.cisco.com（通過Internet訪問PnP），則會自動執行入網。已入網的NFVIS系統會自動顯示包含基本控制器資訊的viptela-system:system和vpn 0配置。

從Cisco NFVIS版本4.9.1開始，支援通過管理埠建立到管理平面的控制連線。需要使用SD-WAN管理器訪問管理埠，才能成功連線到控制平面。



附註：每個包含"system"關鍵字的命令都需要寫為system:system。如果tab鍵用於完成，它將自動適應此新標準。

```
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是SD-WAN解決方案的預定義傳輸VPN。不能刪除或修改。此VPN的目的是在WAN傳輸網路（底層）和網路服務（重疊）之間實施隔離：

```
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
  !
 !
!
```

控制連線是在SD-WAN交換矩陣的不同節點（控制器和邊緣路由器）之間建立的DTLS會話。由於NFVIS不是負責路由決策的路由平台，因此它不會與vSmarts形成控制連線。開箱即用，您可以觀察vManage的「challenge」狀態：

```
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.
```

這通常表示沒有system-ip、和/或organization-name配置錯誤或根本未配置。PnP門戶和vBond必須建立組織名稱，並且與vManage建立控制連線後。否則，請使用模板中各自的system-ip和site-id在NFV Config-Group（從20.14.1開始支援）中推送此資訊，或在viptela-system:system子配置中靜態配置此信息：

```
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.
```

可在vManage中找到以下專案：

- 組織名稱：管理>設定>系統>組織名稱
- 驗證器IP和埠：管理>設定>系統>驗證器

在viptela-system:system子配置中輸入其餘配置後，您需要活動/已建立的控制連線。

```
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.
```

取消管理NFVIS

如果您想將NFVIS恢復到「非託管」狀態，您需要執行以下操作：

1. 從PnP門戶刪除裝置條目：

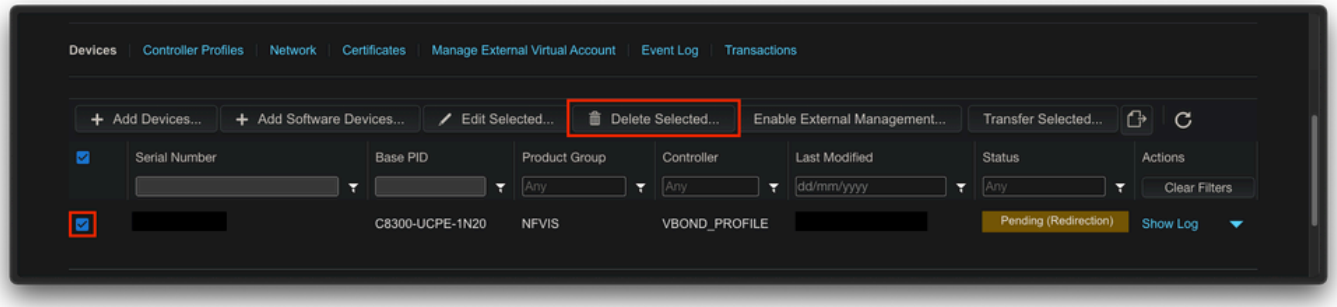


圖10.從PnP入口移除裝置。

2.出廠重置NFVIS。

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

3.可選步驟：從vManage Edge清單中刪除裝置：

3.1使裝置證書無效。

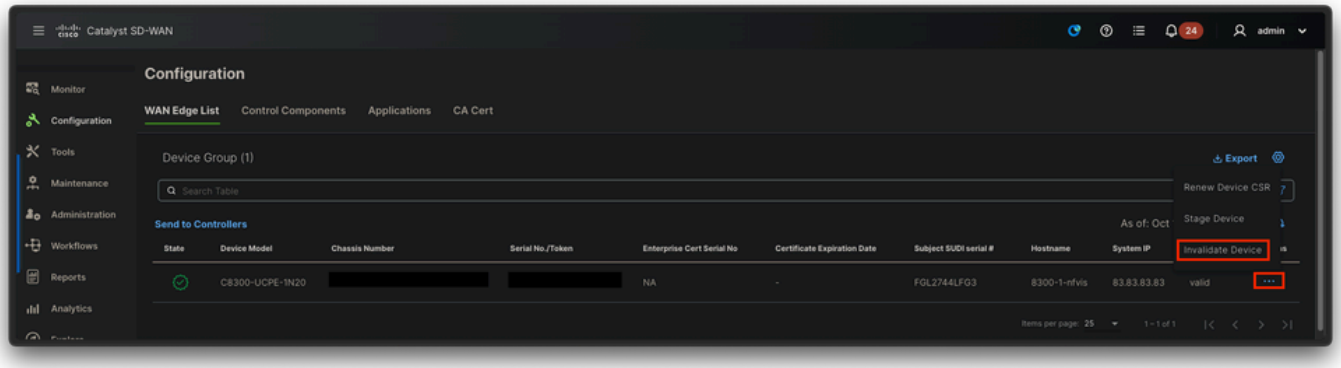


圖11. 8300證書失效。

3.2從WAN Edge清單中刪除裝置。

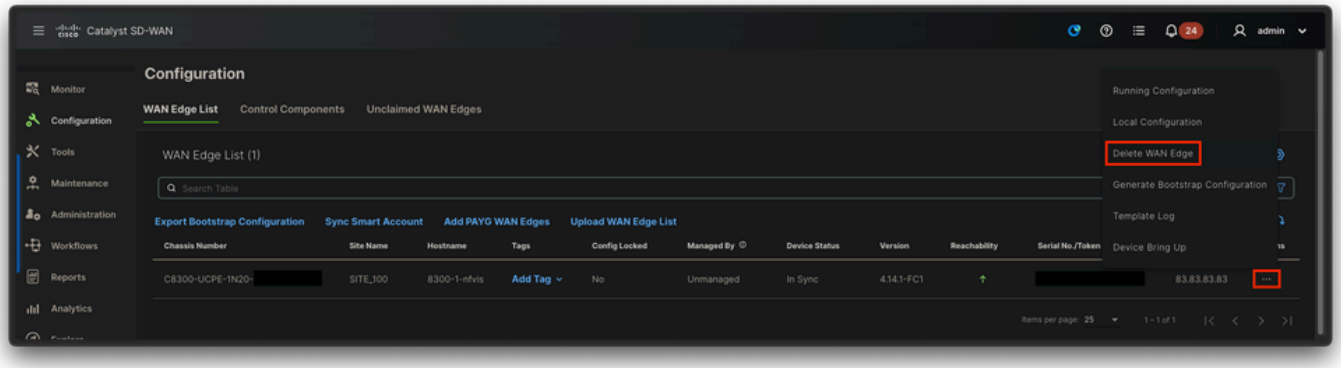


圖12.從WAN Edge清單中刪除的8300。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。