板载NFVIS广域网边缘设备

目录

简介

先决条件

- 要求
- 使用的组件

Hardware

软件

PnP工作流

支持NFVIS的设备的安全登录

- 检索SN和证书序列号
- 将设备添加到PnP门户

NFVIS中的PnP

vManage与PnP同步

- 在线模式
- 离线模式

NFVIS自动注册和控制连接

取消管理NFVIS

简介

本文档介绍将支持NFVIS的系统注册到Catalyst™ SD-WAN环境以进行管理和操作的过程。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科SDWAN
- NFVIS
- 即插即用(PNP)

假定：

- SD-WAN控制器（vManage、vBond和vSmart）已部署了有效证书。
- 思科广域网边缘（本例中为NFVIS）可访问vBond协调器和其他SD-WAN控制器，这些控制器可通过广域网传输中的公共IP地址访问
- NFVIS版本必须符合《控制组件兼容性指南》。

使用的组件

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

Hardware

- C8300-UCPE-1N20(但可以应用于任何支持NFVIS的平台)

软件

- vManage 20.14.1
- vSmart和vBond 20.14.1
- NFVIS 4.14.1

PnP工作流

广域网边缘设备的信任通过根链证书完成，根链证书在制造过程中预加载、手动加载、由vManage自动分配，或在PnP或ZTP自动部署调配过程中安装。

SD-WAN解决方案使用允许列表模型，这意味着允许加入SDWAN重叠网络的广域网边缘设备需要事先由所有SD-WAN控制器知道。这可以通过在即插即用连接门户(PnP)中添加WAN Edge设备来完成，网址为https://software.cisco.com/software/pnp/devices

此过程始终要求在同一重叠网络中识别、信任和允许列出设备。在相同重叠网络中的SD-WAN组件之间建立安全控制连接之前，需要跨所有SD-WAN组件进行相互身份验证。广域网边缘设备的身份由机箱ID和证书序列号唯一标识。根据WAN Edge路由器，提供证书的方式不同：

- 基于硬件的vEdge:证书存储在制造期间安装的板载防篡改模块(TPM)芯片中。
- 基于硬件的Cisco IOS®-XE SD-WAN:证书存储在制造期间安装的板载SUDI芯片中。
- 虚拟平台或Cisco IOS-XE SD-WAN设备：请勿在设备上预安装根证书（例如ASR1002-X平台）。对于这些设备，vManage提供一次性密码(OTP)以使用SD-WAN控制器验证设备。

要执行零接触调配(ZTP)，必须有DHCP服务器。如果没有，可以手动分配IP地址以继续执行即插即用(PnP)过程的其余步骤。

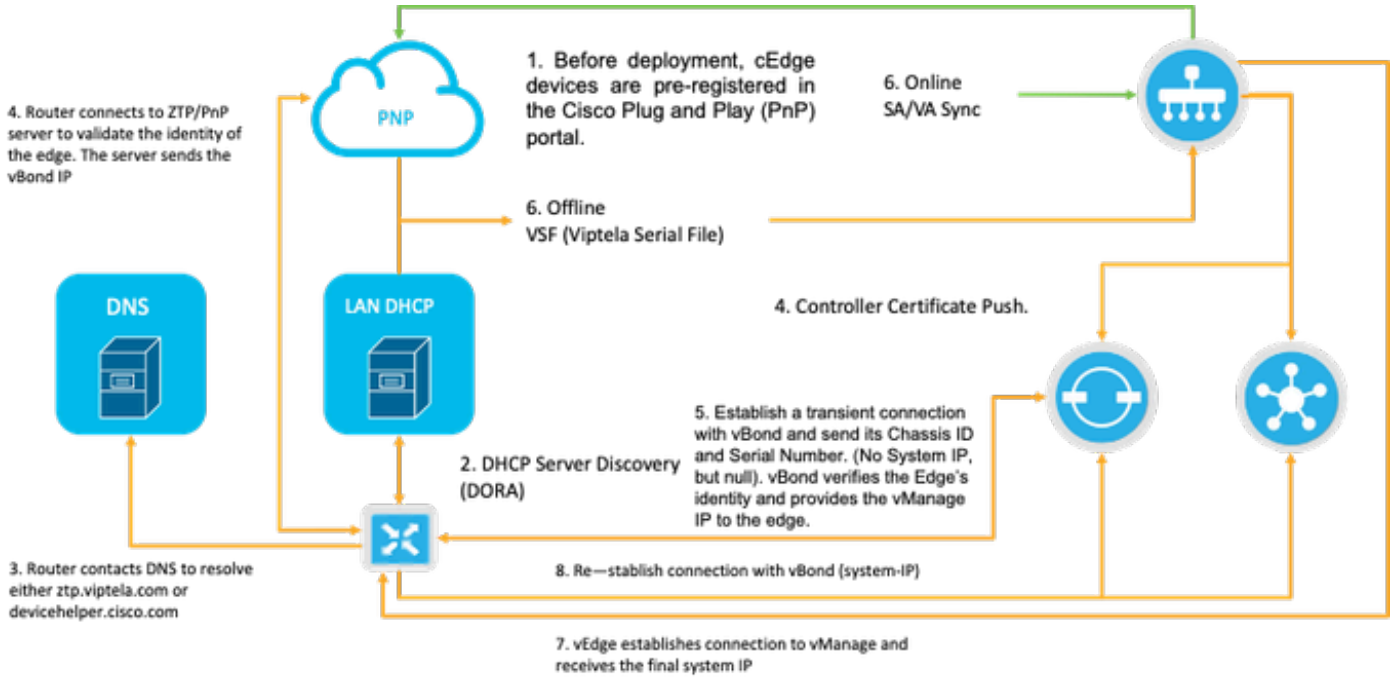


图1. PnP和广域网边缘设备信任工作流程图。

支持NFVIS的设备的安全登录

检索SN和证书序列号

基于硬件的SUDI（安全唯一设备标识符）芯片来自支持NFVIS的硬件，用于确保只有授权设备才能建立安全的TLS或DTLS控制 — 通向SD-WAN Manager协调器的平面隧道。使用support show chassis executive level命令收集相应的序列号：

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

将设备添加到PnP门户

导航到https://software.cisco.com/software/pnp/devices，并为您的用户或实验室环境选择正确的智能帐户和虚拟帐户。（如果多个智能帐户的名称一致，则可以使用域标识符来区分它们）。

如果您或您的用户不知道使用哪个智能帐户(SA)/虚拟帐户(VA)，您可以始终在“Device Search”文本链接中搜索和现有/已注册序列号以查看它属于哪个SA/VA。

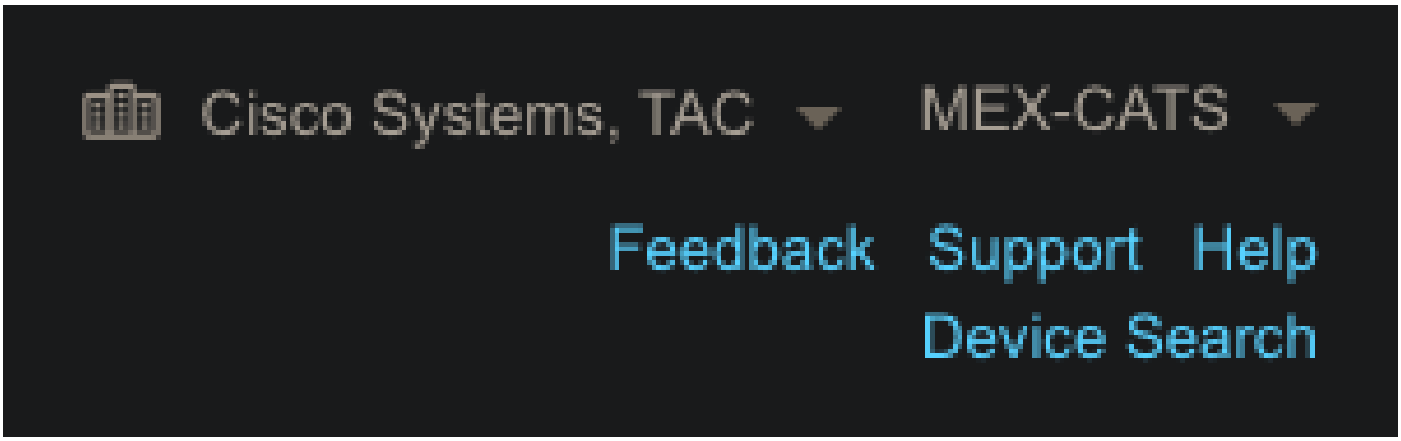


图2. SA/VA选择和设备搜索按钮。

选择正确的SA/VA后，点击“Add Devices...”:

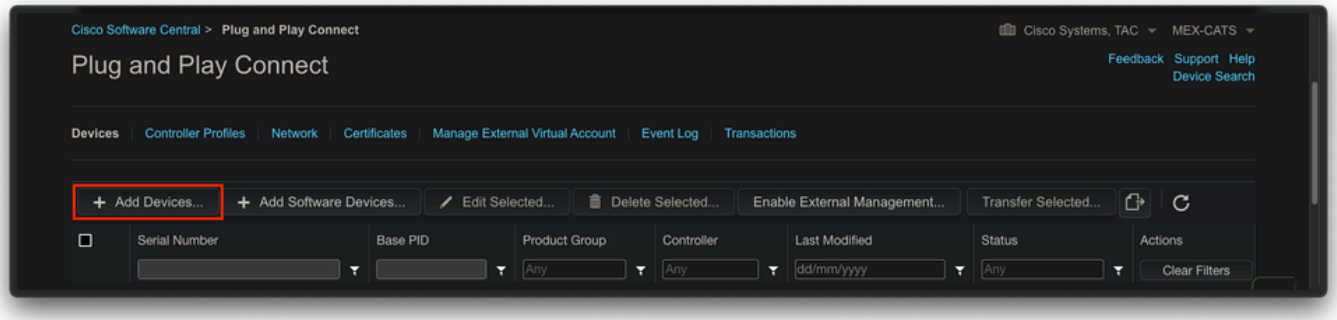


图3. “添加设备……” 单击按钮进行物理设备注册。

对于此特定情况，仅板载1台设备，因此手动输入就足够了：

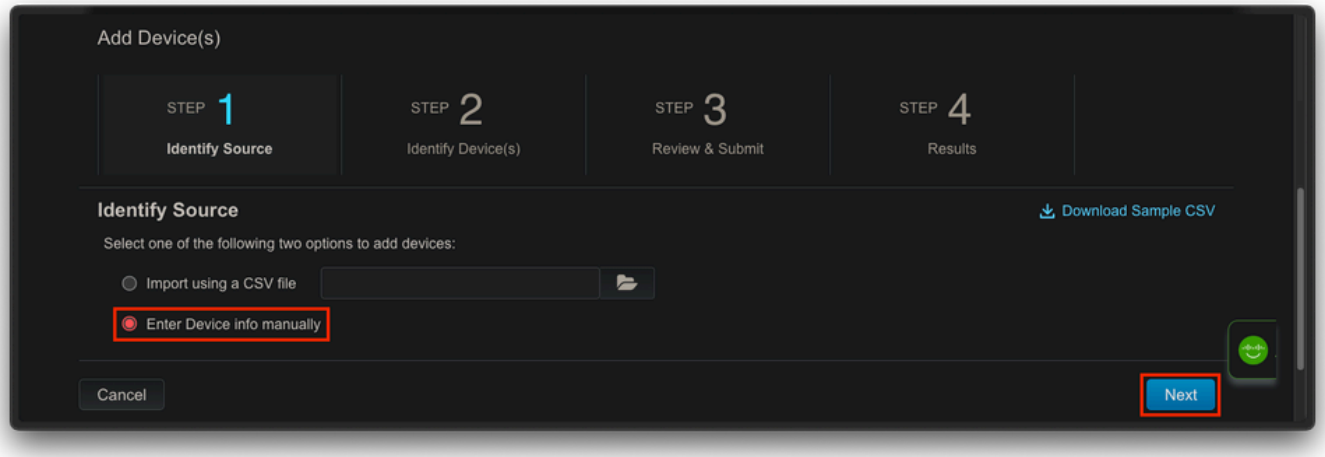


图4. “添加设备……”用于设备信息输入，手动（单独）或CSV（多重）。

对于第2步，点击“+ Identify Device..”按钮。此时将出现“表单”模式。使用NFVIS的support show chassis输出中所显示的信息填写详细信息，并选择相应的vBond控制器配置文件。

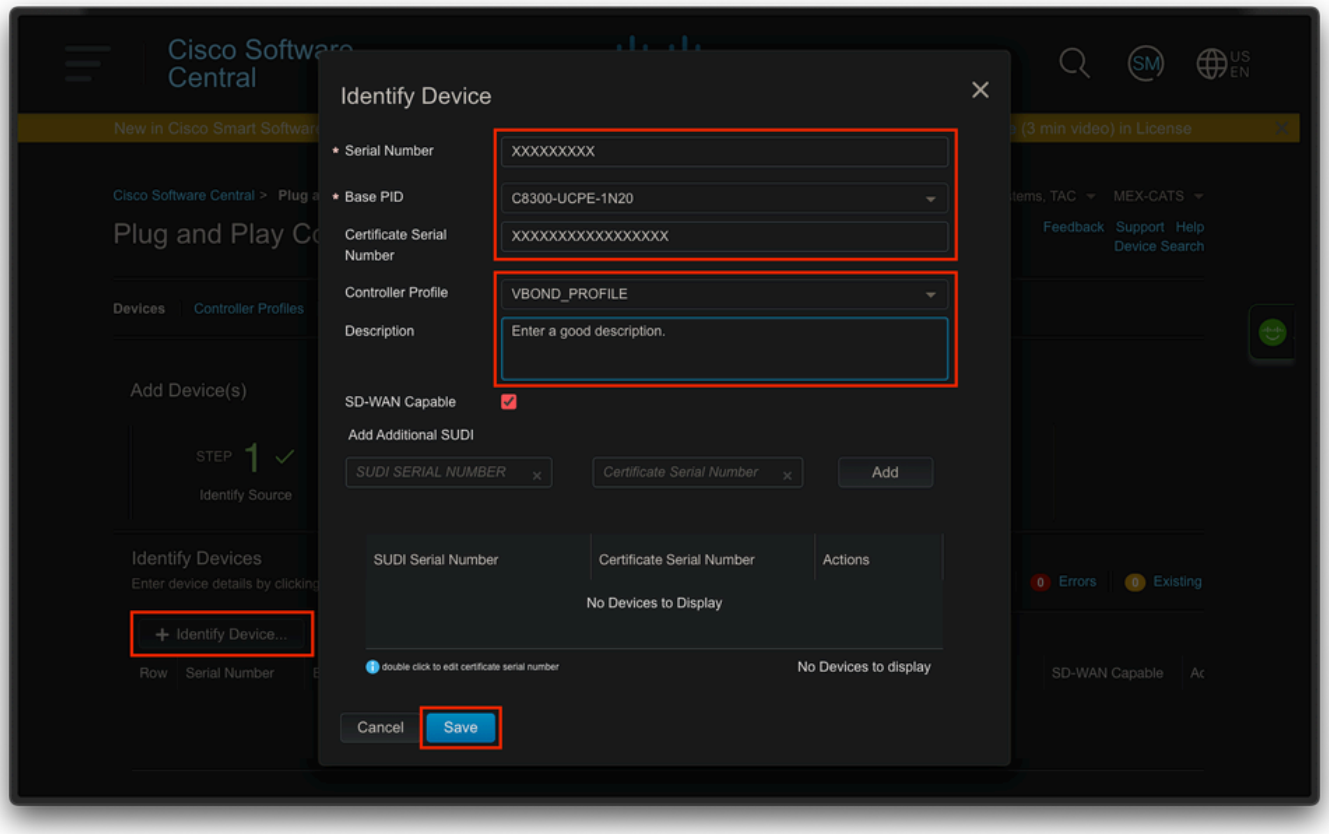


图5.设备标识表。

保存后，单击Next执行步骤3，最后单击Submit执行步骤4。

NFVIS中的PnP

有关NFVIS中PnP的各种配置设置（包括自动和静态模式）的详细信息，请参阅资源：[NFVIS PnP命令。]

请注意，所有NFVIS版本上默认启用PnP。

vManage与PnP同步

在线模式

如果vManage可以访问Internet和PnP门户，您必须能够仅执行SA/VA同步。为此，请导航到Configuration > Devices，然后点击指示Sync Smart Account的文本按钮。需要用于登录思科软件中心的凭证。确保将证书推送发送到所有控制器。

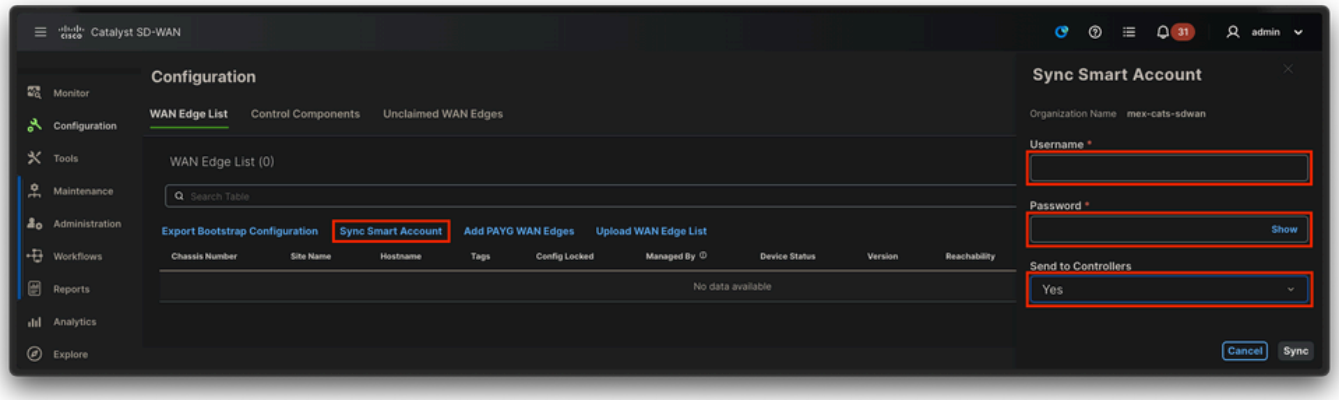


图6.通过SA/VA同步更新WAN边缘路由器。

离线模式

如果vManage在实验室环境中或者无法访问Internet，则可以从PnP手动上传必须包含已添加到设备列表的SN的调配文件。此文件的类型为.viptela(Viptela Serial File)，可通过“Controller Profiles”选项卡获取该文件：

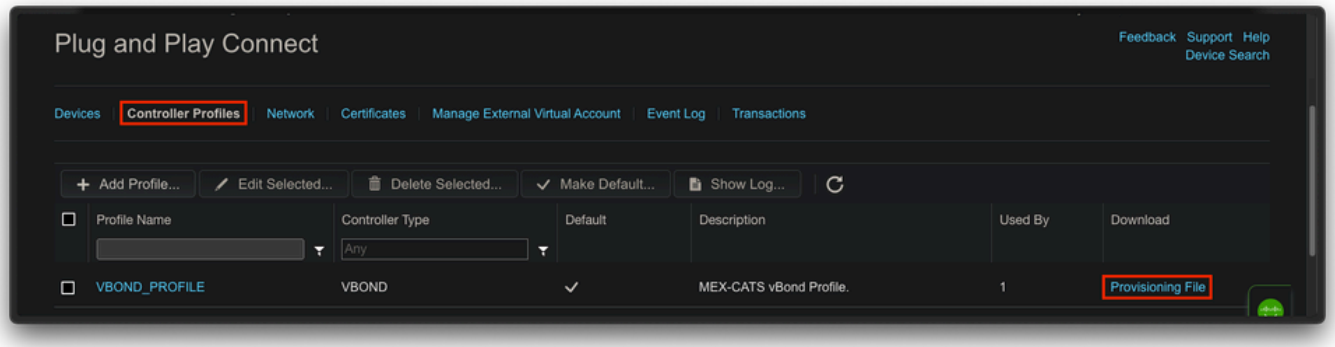


图7. CEdge WAN列表更新的调配文件下载。

要手动上传调配文件，请导航到Configuration > Devices，然后点击指示Upload WAN Edge List的文本按钮。系统将显示一个侧栏，您可以在其中拖放各个文件(如果在执行这些操作后没有选中Upload按钮，请点击Choose a file，然后在弹出文件资源管理器窗口中手动搜索文件)。 确保将证书推送发送到所有控制器。

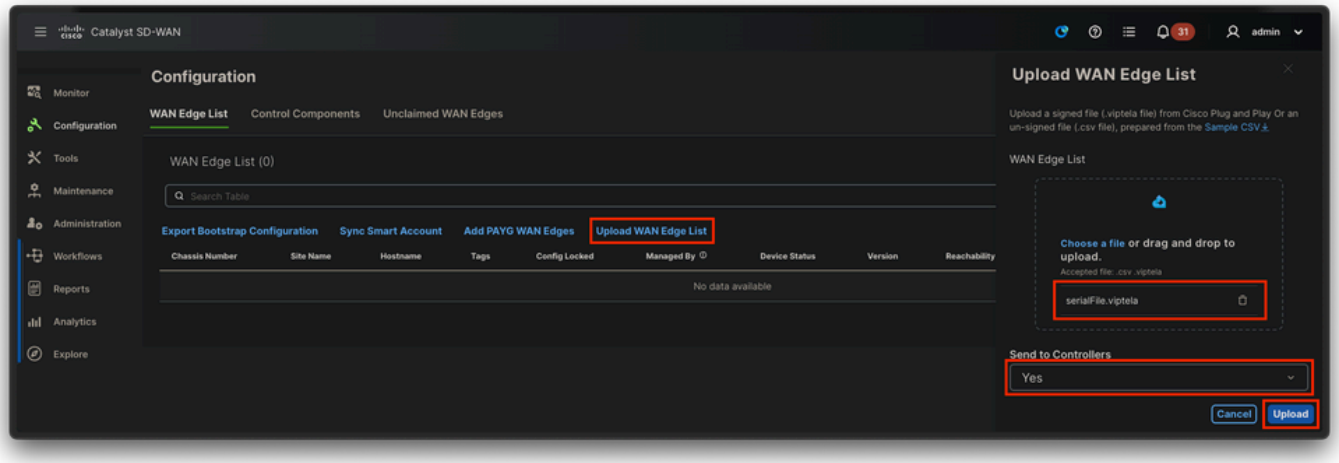


图8.使用从PnP门户下载的调配文件（VSF、Viptela串行文件）进行WAN列表更新。

完成在线或离线方法后，您必须能够在WAN边缘列表表中看到与在PnP中注册的设备的SN对应的设备条目：

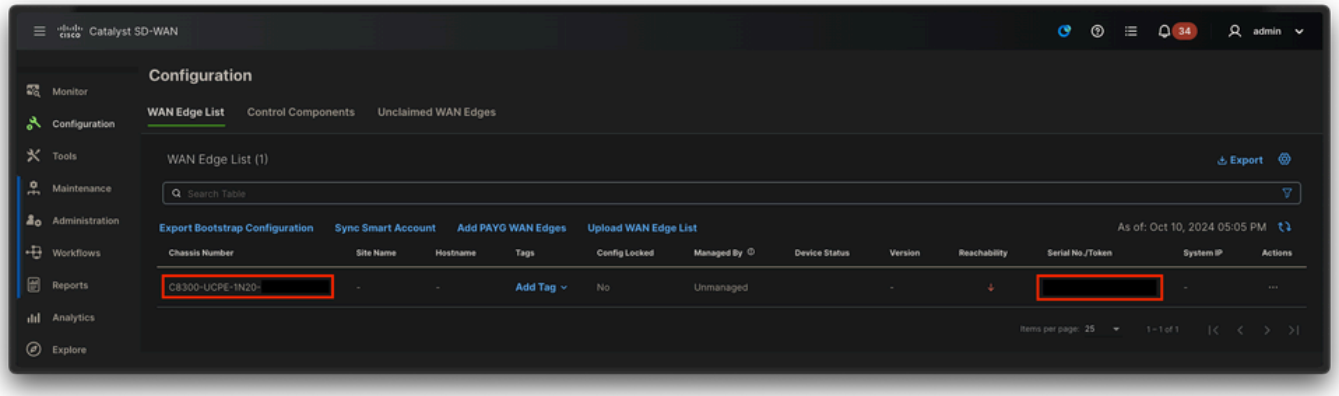
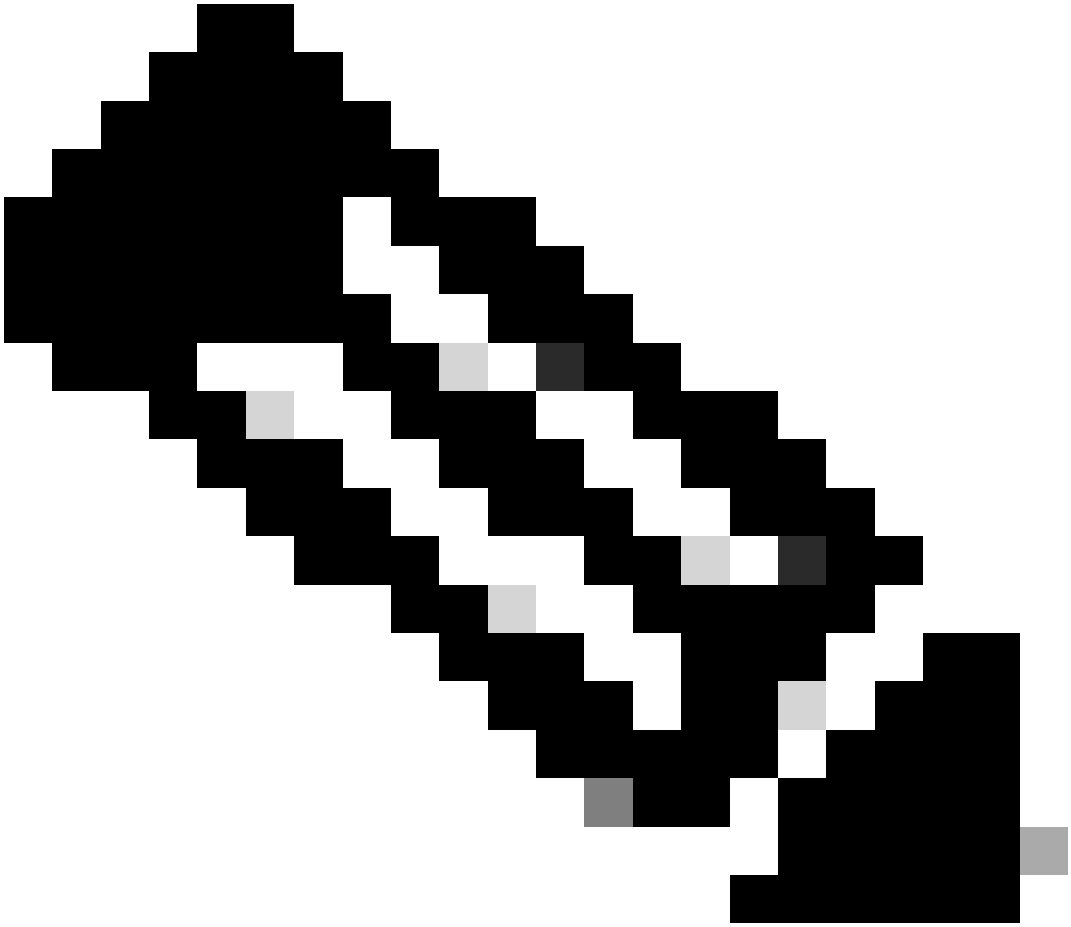


图9.边缘列表中的设备8300。

NFVIS自动注册和控制连接

如果NFVIS能够解析devicehelper.cisco.com（通过Internet访问PnP），则会自动执行自注册。入网NFVIS系统会自动显示viptela-system:system和vpn 0配置，其中包含基本控制器信息。

从Cisco NFVIS版本4.9.1开始，支持通过管理端口建立到管理平面的控制连接。需要使用SD-WAN Manager可以访问管理端口，才能成功连接到控制平面。



注意：每个包含“system”关键字的命令都需要写为system:system。如果tab键用于完成，它将自动适应此新标准。

```
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解决方案的预定义传输VPN。不能删除或修改。此VPN的目的是在WAN传输网络（底层）和网络服务（重叠）之间实施分离：

```
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
  !
 !
!
```

控制连接是在SD-WAN交换矩阵的不同节点（控制器和边缘路由器）之间建立的DTLS会话。由于NFVIS不是负责路由决策的路由平台，因此它不会与vSmarts形成控制连接。开箱即用，您可以观察vManage的“challenge”状态：

```
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.
```

这通常表示没有system-ip和/或organization-name配置错误或根本未配置。PnP门户和vBond必须建立组织名称，并且与vManage建立控制连接后。否则，请使用模板中各自的system-ip和site-id在NFV Config-Group（从20.14.1开始支持）中推送此信息，或在viptela-system:system子配置中静态

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中找到以下项目：

- 单位名称:管理>设置>系统>组织名称
- 验证器IP和端口：Administration > Settings > System > Validator

在viptela-system:system子配置中输入剩余配置后，您需要主动/已建立的控制连接。

```
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

如果要将NFVIS恢复到“非托管”状态，您需要执行以下操作：

1. 从PnP门户删除设备条目：

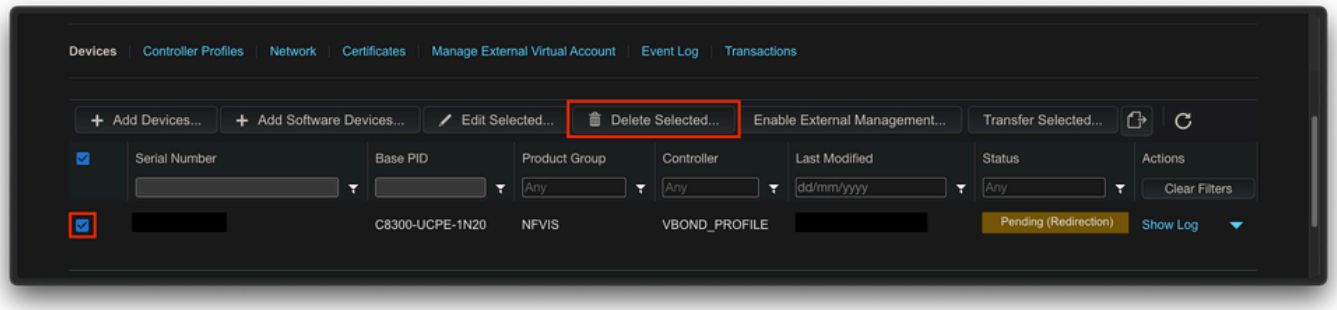


图10.从PnP门户删除设备8300。

2.出厂重置NFVIS。

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

3.可选步骤：从vManage Edge列表中删除设备：

3.1使设备证书无效。

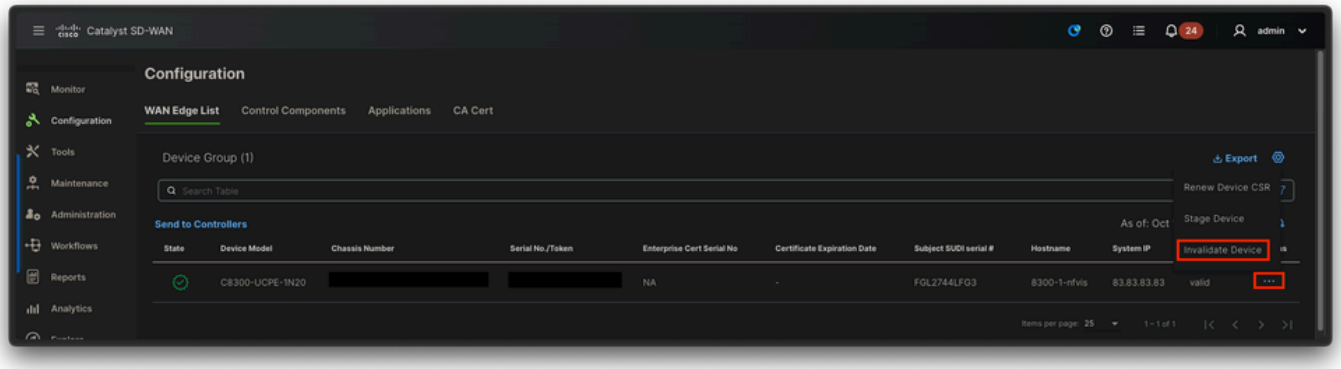


图11. 8300证书失效。

3.2从WAN Edge列表中删除设备。

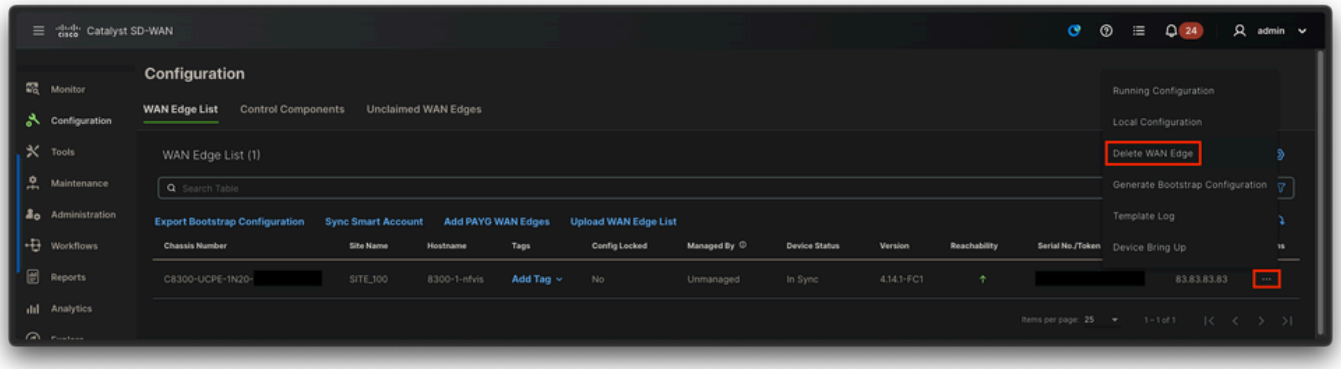


图12.从WAN Edge列表中删除的8300。

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。