適用於數位網路架構(DNA)中心的LAN自動化提示和技巧

目錄

簡介

本檔案將概述區域網(LAN)自動化，以幫助您診斷LAN自動化在數位網路架構(DNA)中心中無法按預期運作的問題。

作者：Alexandro Carrasquedo，思科TAC工程師。

手套

即插即用(PnP)代理：您剛剛開啟的新裝置，沒有配置，也沒有由DNA Center自動配置的證書。

種子裝置:DNA Center已調配並用作動態主機配置協定(DHCP)伺服器的裝置。

必要條件

要求

思科強烈建議您瞭解LAN自動化和即插即用解決方案的一般知識。概述了LAN自動化（儘管它基於DNA Center 1.0），同一概念適用於DNA Center 1.1及更高版本。

背景資訊

LAN自動化是一種近零接觸部署解決方案，使您能夠使用ISIS作為底層路由協定來配置和調配網路裝置。

開始之前

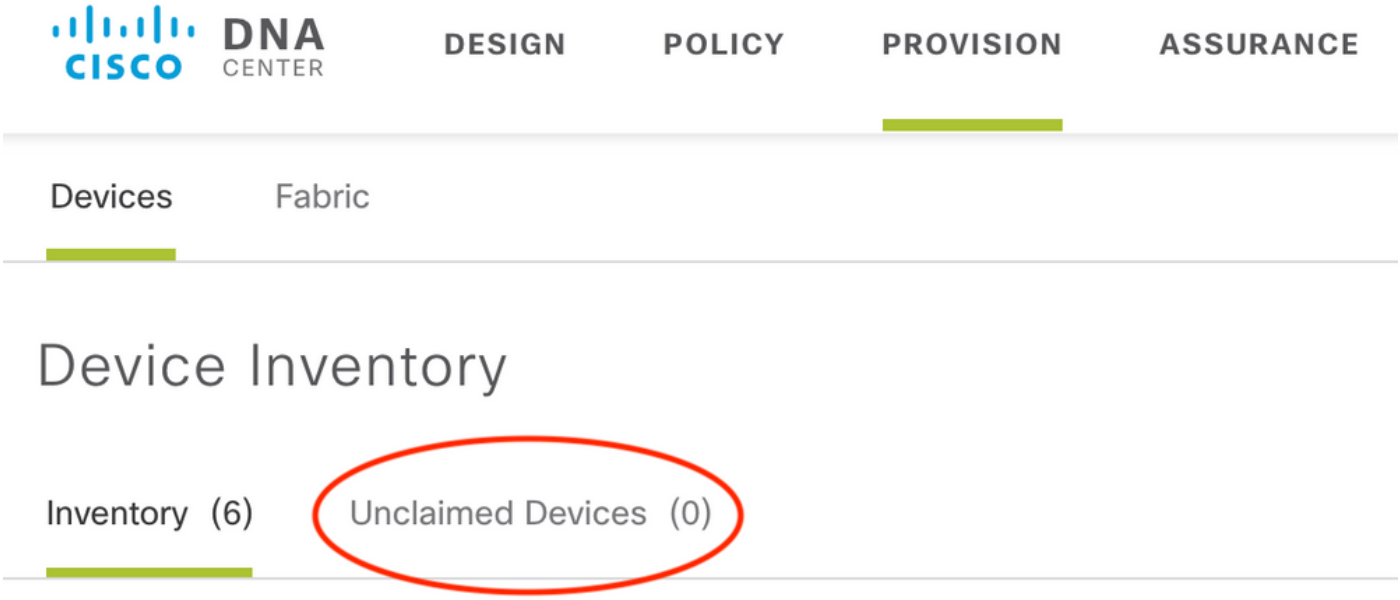
運行LAN自動化之前，請確保PnP代理沒有在NVRAM中載入任何證書。

```
Edge1#dir nvram:*.cer
Directory of nvram:/*.cer

Directory of nvram:/

    4  -rw-         820                    <no date>  IOS-Self-Sig#1.cer
    6  -rw-         763                    <no date>  kube-ca#468ACA.cer
    7  -rw-         882                    <no date>  sdn-network-#616F.cer
    8  -rw-         807                    <no date>  sdn-network-#4E13CA.cer
2097152 bytes total (2033494 bytes free)
Edge1#delete nvram:*.cer
```

在Provisioning > Devices > Device Inventory頁面中，確保沒有任何未申請的裝置：



因為CSCvh68847 中，某些堆疊可能不會保留未宣告的狀態，而且您可能會收到ERROR_STACK_UNSUPPORTED錯誤訊息。當LAN自動化嘗試將裝置宣告為如同單個交換機一樣進行調配時，會出現此消息。但是，由於裝置是Catalyst 9300交換機堆疊，LAN自動化無法宣告該裝置，裝置顯示為未宣告。同樣，PnP不會宣告該裝置，因為它是一個堆疊，因此未調配該裝置。

LAN自動化在運行時要執行哪些步驟？

DNA Center使用DHCP配置調配種子裝置。種子裝置獲取的IP地址範圍是您在為站點保留IP地址池時定義的初始池的一個段。請注意，此池必須至少為/25。

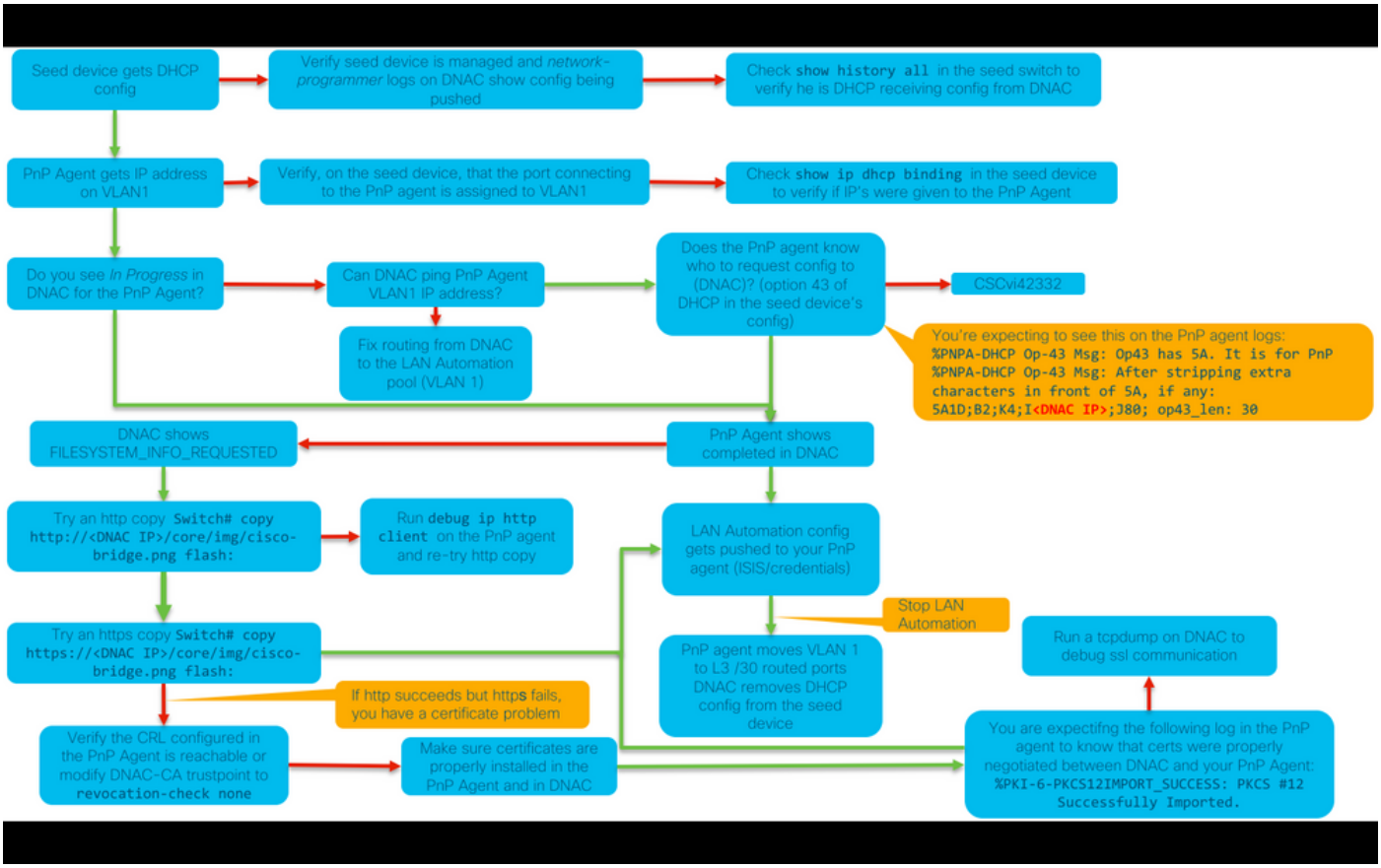
> **附註**：此池分為3個網段：
> 1.在PnP代理上推送到VLAN 1的IP地址。
> 2.推送到PnP代理上的Loopbac0的IP地址。
> 3.在連線到種子或其他交換矩陣裝置的鏈路上推送到您的PnP代理的/30 IP地址。

對於DNA Center要調配PnP代理，種子裝置收到的DHCP配置必須具有選項43，該選項定義為DNA Center面向企業的網路介面卡(NIC)的IP地址或虛擬IP(VIP)地址（如果您有n節點群集）。

PnP代理啟動時，它們沒有配置。因此，它們的所有埠都是VLAN 1的一部分。因此，裝置向種子裝置傳送DHCP發現消息。種子裝置會響應LAN自動化池中提供的IP地址。

現在您已瞭解LAN自動化的初始順序，如果過程沒有按預期運行，您可以排除故障。

疑難排解圖表



DNA Center 1.1 LAN自動化相關日誌

- network-orchestration-service
- pnp服務

DNA Center 1.2 LAN自動化相關日誌

在版本1.2中，不再提供pnp服務，因此您在排除LAN自動化故障時，需要查詢以下服務：

- 網路協調
- 網路設計
- 連線-manager-service
- 自註冊服務*（這是舊版pnp服務，相當於1.1版）*

DNA Center 1.x公開金鑰基礎架構(PKI)相關日誌

- apic-em-pki-broker-service
- apic-em-jboss-ejbca

如何運行流程圖中顯示的tcpdump?

```
sudo tcpdump -i <DNA Center fabric's interface> host <PnP Agent ip address> -w
/data/tmp/pnp_capture.pcap
```

*要停止此操作，請使用CTRL+C

這會將pnp_capture.pcap檔案儲存在/data/tmp/中。您需要使用secure copy(SCP)命令從DNA Center複製檔案，或使用以下命令從DNA Center讀取檔案：

```
$ sudo tcpdump -ttttnnr /data/tmp/pnp_capture.pcap
[sudo] password for maglev:
reading from file capture.pcap, link-type EN10MB (Ethernet)
2018-03-08 20:09:27.369544 IP 192.168.31.1 > 192.168.31.10: ICMP host 192.168.1.2 unreachable,
length 36
2018-03-08 20:09:39.369175 IP 192.168.31.1 > 192.168.31.10: ICMP host 192.168.1.2 unreachable,
length 36
2018-03-08 20:09:44.373056 ARP, Request who-has 192.168.31.1 tell 192.168.31.10, length 28
2018-03-08 20:09:44.374834 ARP, Reply 192.168.31.1 is-at 2c:31:24:cf:d0:62, length 46
2018-03-08 20:09:50.628539 IP 192.168.31.10.57234 > 192.168.31.1.22: Flags [S], seq 1113323684,
win 29200, options [mss 1460,sackOK,TS val 274921400 ecr 0,nop,wscale 7], length 0
2018-03-08 20:09:50.630523 IP 192.168.31.1.22 > 192.168.31.10.57234: Flags [S.], seq 2270495802,
ack 1113323685, win 4128, options [mss 1460], length 0
2018-03-08 20:09:50.630604 IP 192.168.31.10.57234 > 192.168.31.1.22: Flags [.], ack 1, win
29200, length 0
2018-03-08 20:09:50.631712 IP 192.168.31.10.57234 > 192.168.31.1.22: Flags [P.], seq 1:25, ack
1, win 29200, length 24
```

您要複製的bridge.png檔案是什麼？

這是一個位於DNA Center中的191位元組的影象檔案，您要使用HTTP（不使用證書）或HTTPS（使用證書）來測試DNA Center與PnP代理之間的通訊。

安全套接字層(SSL)通訊未按預期正常工作時的捕獲示例（本文附有完整的.pcap檔案）

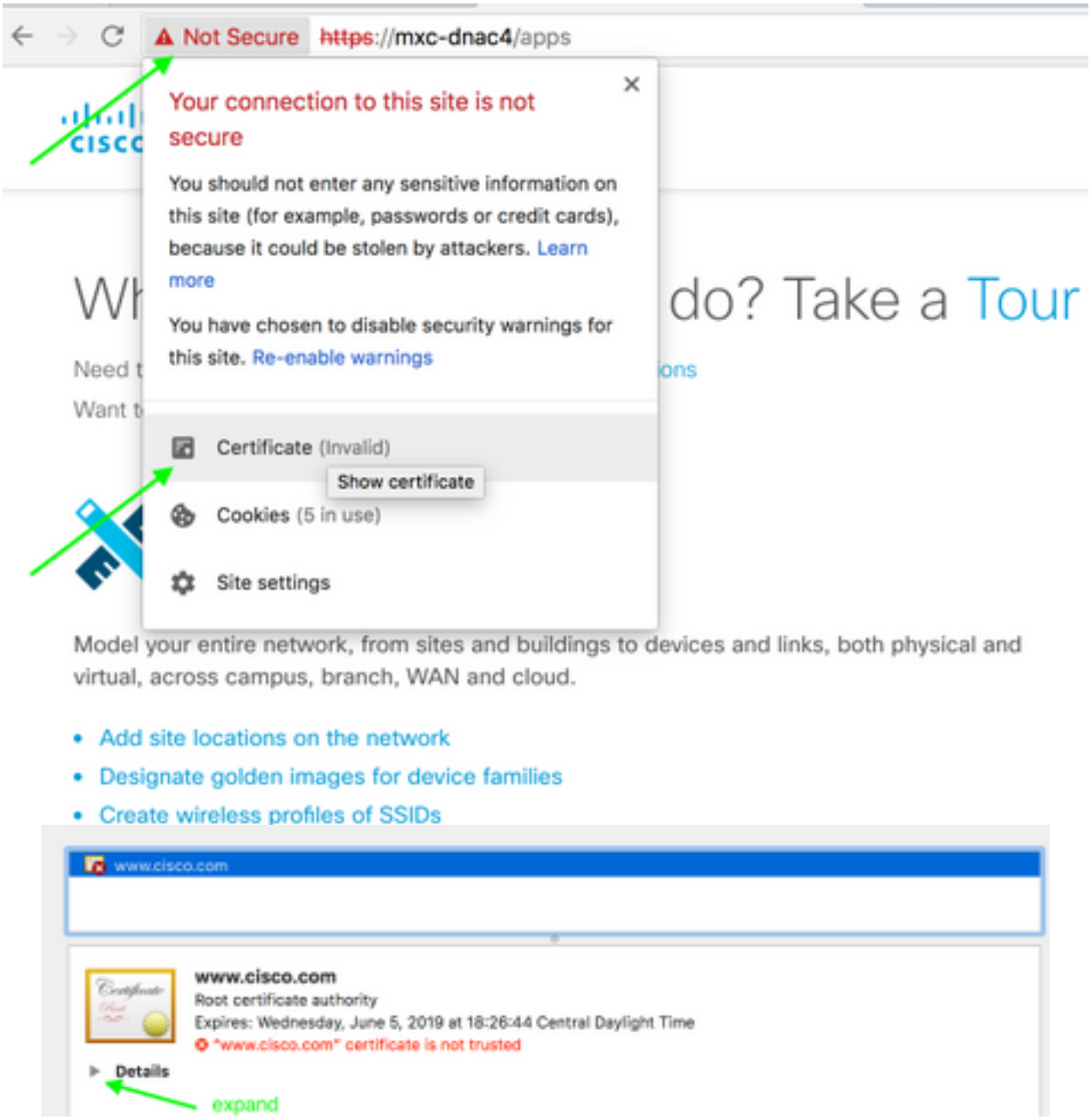
證書錯誤

可能的原因：

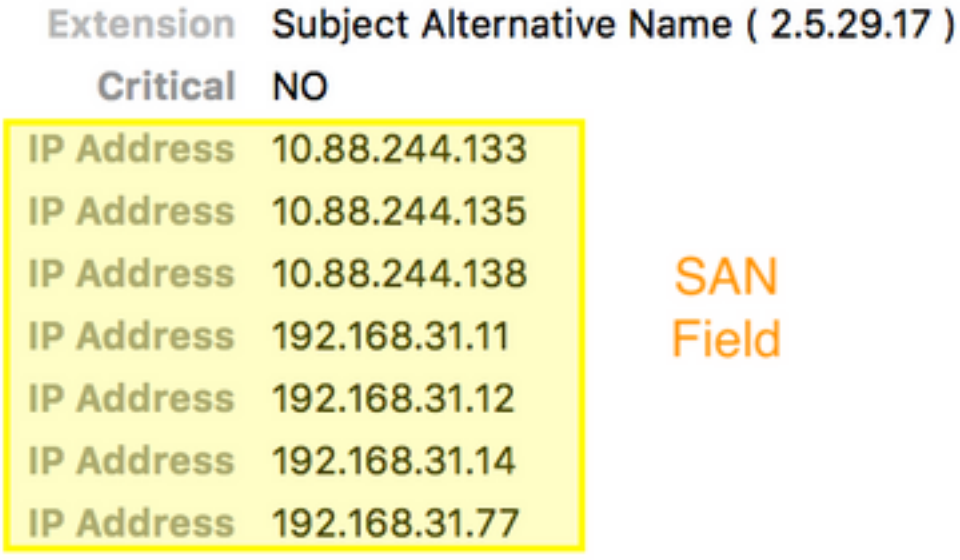
- DNA Center的證書在「Subject Alternative Name(SAN)(主題備用名稱(SAN))」欄位中沒有正確的IP地址。

要檢查證書中的SAN欄位，可以執行以下操作：

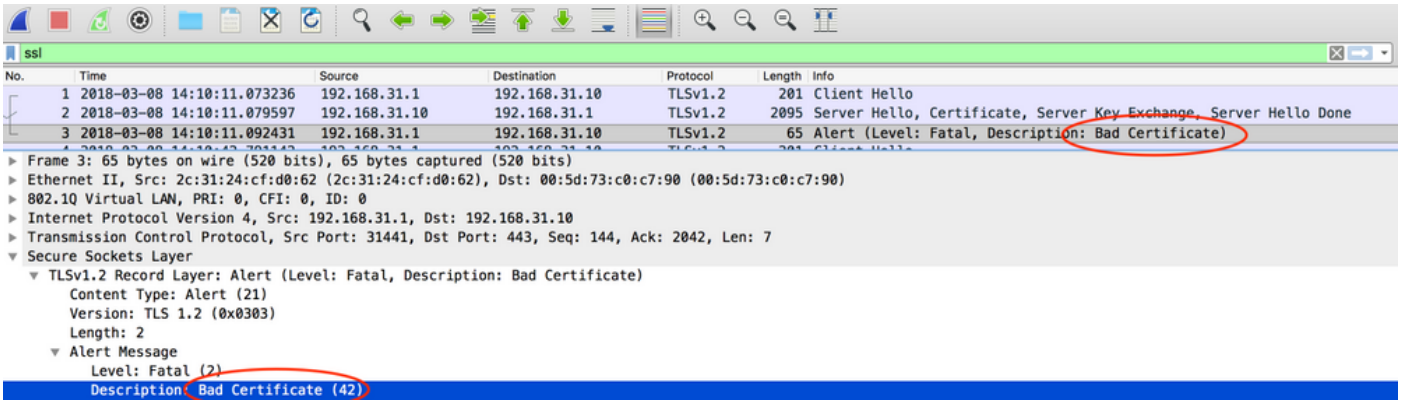
使用瀏覽器驗證憑證


Not Secure
https://mxc-dnac4/apps
Your connection to this site is not secure
You should not enter any sensitive information on this site (for example, passwords or credit cards), because it could be stolen by attackers. Learn more
You have chosen to disable security warnings for this site. Re-enable warnings
Certificate (Invalid)
Show certificate
Cookies (5 in use)
Site settings
do? Take a Tour
Model your entire network, from sites and buildings to devices and links, both physical and virtual, across campus, branch, WAN and cloud.
Add site locations on the network
Designate golden images for device families
Create wireless profiles of SSIDs

www.cisco.com
www.cisco.com
Root certificate authority
Expires: Wednesday, June 5, 2019 at 18:26:44 Central Daylight Time
"www.cisco.com" certificate is not trusted
Details
expand


Extension Subject Alternative Name (2.5.29.17)
Critical NO
IP Address 10.88.244.133
IP Address 10.88.244.135
IP Address 10.88.244.138
IP Address 192.168.31.11
IP Address 192.168.31.12
IP Address 192.168.31.14
IP Address 192.168.31.77
SAN Field

捕獲示例



解析.

如果您有第三方CA（證書頒發機構），請確保他們為您頒發的證書中包含DNA Center的IP地址及其VIP。如果您沒有第三方CA，DNA Center可以為您生成證書。請聯絡Cisco TAC以指導您完成此過程。

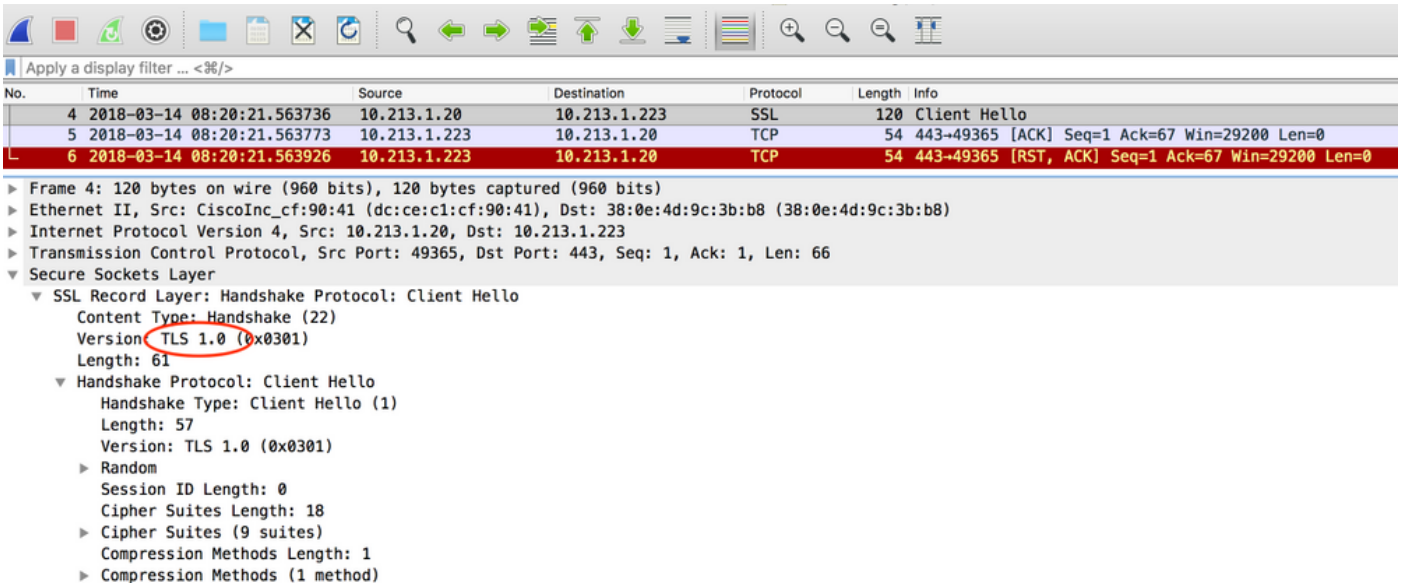
DNA Center重置連線

可能的原因：

預設情況下，DNA Center僅支援TLS v1.2。

要解決此問題，請按照本指南啟用DNA Center以使用TLS v1

捕獲示例



PnP代理上用於解決證書相關問題的有用調試命令

- debug crypto pki transactions
- debug ssl openssl
- debug ssl openssl errores
- debug ssl openssl errors

- debug crypto pki API
- debug crypto pki transactions
- debug ssl openssl msg

響應缺少以前建立的經過身份驗證的會話金鑰

理論上，您不應在Provisioning > Devices > Device Inventory頁面中有未領到的裝置，但在從該頁面刪除未領到的裝置後，仍在https://<DNA Center ip>/mypnp中顯示這些裝置時出現問題。如果您遇到這種情況，在PnP日誌中看到類似於以下內容的日誌，或在GUI中看到類似情況的指示，請確保裝置在PnP中不會顯示為未宣告的情況：

```
ERROR | qtp604107971-170 | | c.c.e.z.impl.ZtdHistoryServiceImpl | Device authentication status
has changed to Error(PNP response com.cisco.enc.pnp.messages.PnpBackoffResponse is missing
previously established authenticated session key) | address=192.168.31.10, sn=FCW212XXXXX
```

LAN自動化和堆疊的難點

- 在DNA Center 1.2中，堆疊需要是滿環（2成員堆疊使用一個堆疊電纜可能不能工作）。
- LAN自動化需要立即宣告堆疊裝置的費用，大約在10分鐘之內。
- 一旦連線到DNA Center，在PnP中將顯示為「未申請」。 PnP使用10分鐘時間視窗來確定堆疊，超過此時間視窗後，它將停留在LAN自動化中未宣告的部分中。

如果您有RCA或PnP日誌，您可以查詢未宣告的裝置消息：

```
more pnp.log | egrep "(Received unclaimed notification|ZtdDeviceUnclaimedMessage)"
```

如果沒有消息，則未宣告的裝置通知不會到達DNA Center，並且PnP無法宣告該消息。

如何在堆疊上執行LAN自動化

1. 關閉到種子裝置的上行鏈路。
2. 啟動DNA Center上的LAN自動化。
3. 從堆疊中刪除啟動組態。**#寫擦除**
4. 從NVRAM中刪除所有證書。 **# delete nvram:*.cer**
5. 移除vlan.dat檔。**# delete flash:vlan.dat**
6. 在主交換機上，刪除備用交換機上的證書。**# delete stby-nvram:*.cer**

a.拔下堆疊纜線。

b.登入到每台成員交換機的控制檯。

c.刪除證書。 **# delete nvram:*.cer**

d.刪除flas vlan資料庫。**# delete flash:vlan.dat**

e.重新連線堆疊纜線。

7.重新啟動。

8.等待交換機註冊為堆疊，調出所有成員，然後嘗試啟動初始配置對話方塊。

```
%INIT: waited 0 seconds for NVRAM to be available


         --- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]:
```

9.啟用到種子裝置的上行鏈路。**# no shutdown**

我可以匯入到我的LAN自動化任務的主機名對映檔案的格式？

DNA Center需要一個包含主機名和序列號（主機名、序列號）的CSV檔案，如以下示例所示：

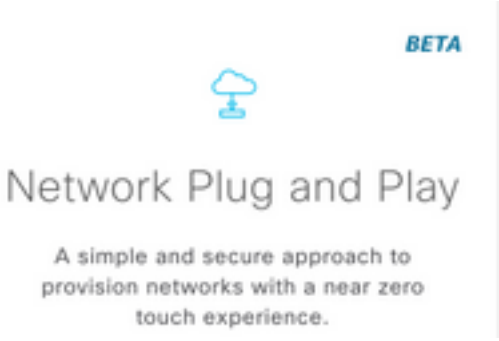
A	B
Edge1	FCW2048Cxxx
Edge2	FCW2131Lxxx, FCW2131Gxxx, FCW2131Gxxx, FCW2131Gxxx
Edge3	FOC2052Xxxx, FCW2052Cxxx, FCW2052Fxxx
Edge4	FXS2131Qxxx

對於堆疊LAN自動化，CSV檔案允許您輸入主機名和每行多個序列號。序列號需要用逗號分隔。請參閱附加的CSV檔案以供參考。

/mypnp在1.2中去哪兒了？

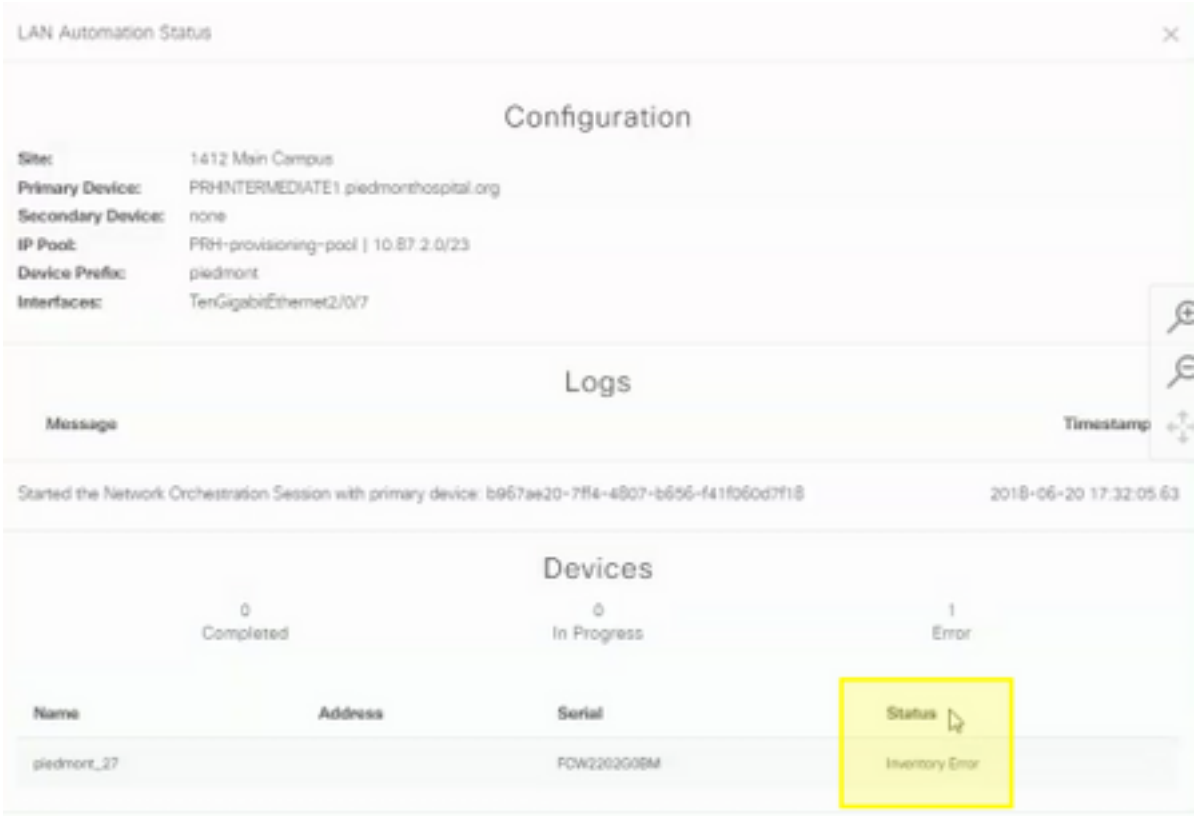
通過以下方式之一訪問PnP:

- 從您的Web瀏覽器輸入https://<DNA Center IP>/networkpnp
- 從DNA Center首頁中，選擇以下網路即插即用工具：



或者訪問https://<DNA Center IP>/networkpnp

庫存錯誤



清單錯誤表示裝置在被LAN自動化要求並收到其配置失敗後，將被新增到清單中。發生此錯誤的原因通常是配置、某些路由或CLI憑據問題。

要驗證您嘗試通過LAN自動化啟動正確的裝置，請使用首選連線協定（SSH或Telnet）遠端訪問裝置上loopback 0介面的IP地址。

存在連線，但PKI證書未成功推送到PnP代理

有時，中間的裝置可能會開啟DNAC和PnP代理之間資料包的*不分段*(DF)位。這可能會導致大於1500位元組（通常為包含憑證的資料包）的封包被捨棄，因此LAN自動化可能無法完成。在DNA Center的載入日誌中看到的一些*常見*日誌是：

```
errorMessage=Failed to format the url for trustpoint
```

在這種情況下，建議的操作是確保DNA Center和PnP Agent之間的路徑允許使用命令系統**mtu 9100通過巨型幀**。

Switch(config)# **system mtu 9100**