Tipps und Tricks zur LAN-Automatisierung für das Digital Network Architecture (DNA) Center

Inhalt

Einführung

Dieses Dokument bietet eine Übersicht über die LAN-Automatisierung (Local Area Network), um Ihnen bei der Diagnose von Problemen zu helfen, wenn die LAN-Automatisierung nicht wie

erwartet im Digital Network Architecture (DNA) Center funktioniert.

Mitarbeiter: Alexandro Carrasquedo, Cisco TAC Engineer.

Glosse

Plug and Play (PnP) Agent:Neues Gerät, das Sie gerade ohne Konfiguration und ohne Zertifikate eingeschaltet haben, die automatisch vom DNA Center konfiguriert werden.

Seed-Gerät: Gerät, das vom DNA Center bereits bereitgestellt wurde und als DHCP-Server (Dynamic Host Configuration Protocol) fungiert.

Voraussetzungen

Anforderungen

Cisco empfiehlt dringend, allgemeine Kenntnisse über LAN-Automatisierung und die Plug-and-Play-Lösung zu erwerben. gibt einen Überblick über LAN Automation, obwohl es auf DNA Center 1.0 basiert, gilt dasselbe Konzept auch für DNA Center 1.1 und höher.

Hintergrundinformationen

Die LAN-Automatisierung ist eine Bereitstellungslösung, die nahezu ohne Benutzereingriff bereitstellt und es Ihnen ermöglicht, Netzwerkgeräte mithilfe des ISIS als untergeordnetes Routing-Protokoll zu konfigurieren und bereitzustellen.

Bevor Sie beginnen

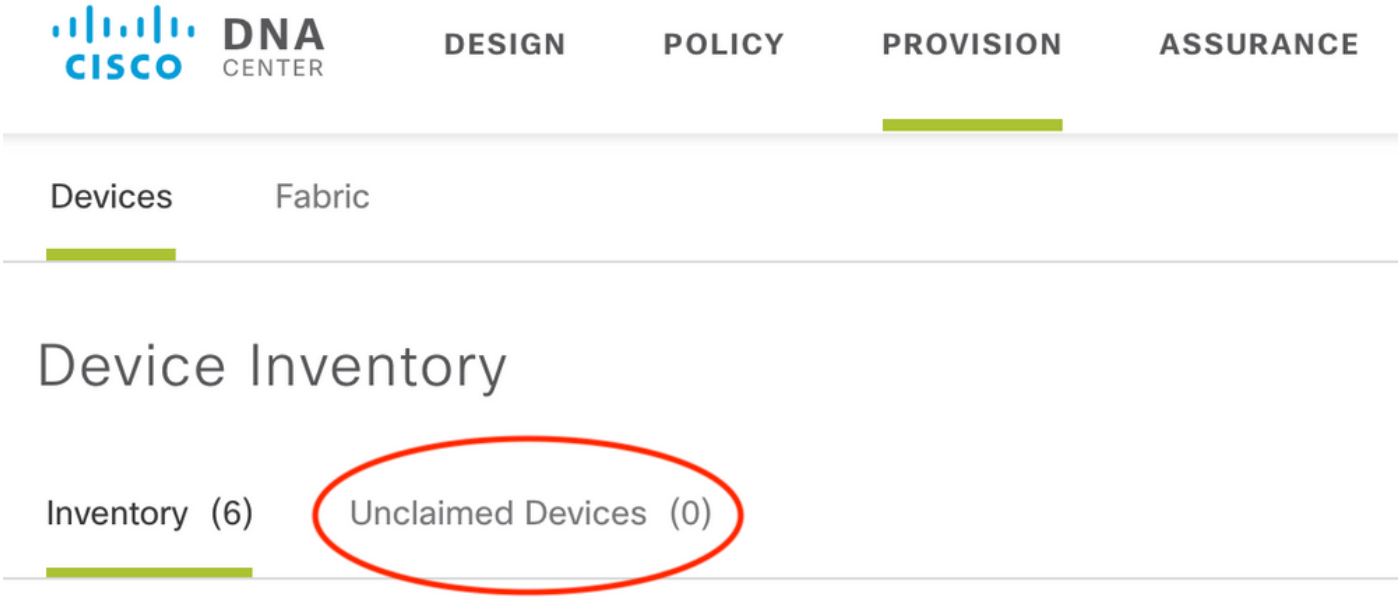
Bevor Sie LAN Automation ausführen, stellen Sie sicher, dass Ihr PnP-Agent keine Zertifikate im NVRAM geladen hat.

```
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
```

Vergewissern Sie sich, dass die Seite Provisioning > Devices > Device Inventory (Bereitstellung > Geräte > Gerätebestand) keine nicht beanspruchten Geräte enthält:



Aufgrund von CSCvh68847 , verlassen einige Stacks möglicherweise nicht den nicht beanspruchten Zustand, und es wird möglicherweise eine Fehlermeldung ausgegeben, die ERROR_STACK_UNSUPPORTED enthält. Diese Meldung tritt auf, wenn die LAN-Automatisierung versucht, das Gerät als einen einzelnen Switch bereitzustellen. Da es sich bei dem Gerät jedoch um einen Catalyst 9300-Switch-Stack handelt, kann die LAN-Automatisierung das Gerät nicht in Anspruch nehmen, und das Gerät wird als nicht beansprucht angezeigt. Ebenso fordert PnP das Gerät nicht an, da es sich um einen Stack handelt, sodass das Gerät nicht bereitgestellt wird.

Welche Schritte werden bei der LAN-Automatisierung ausgeführt?

DNA Center stellt das Seed-Gerät mit DHCP-Konfiguration bereit. Der Umfang der IP-Adressen, die Seed-Gerät erhält, ist ein Segment des ursprünglichen Pools, den Sie definiert haben, wenn Sie den IP-Adresspool für Ihren Standort reserviert haben. Beachten Sie, dass dieser Pool mindestens /25 sein muss.

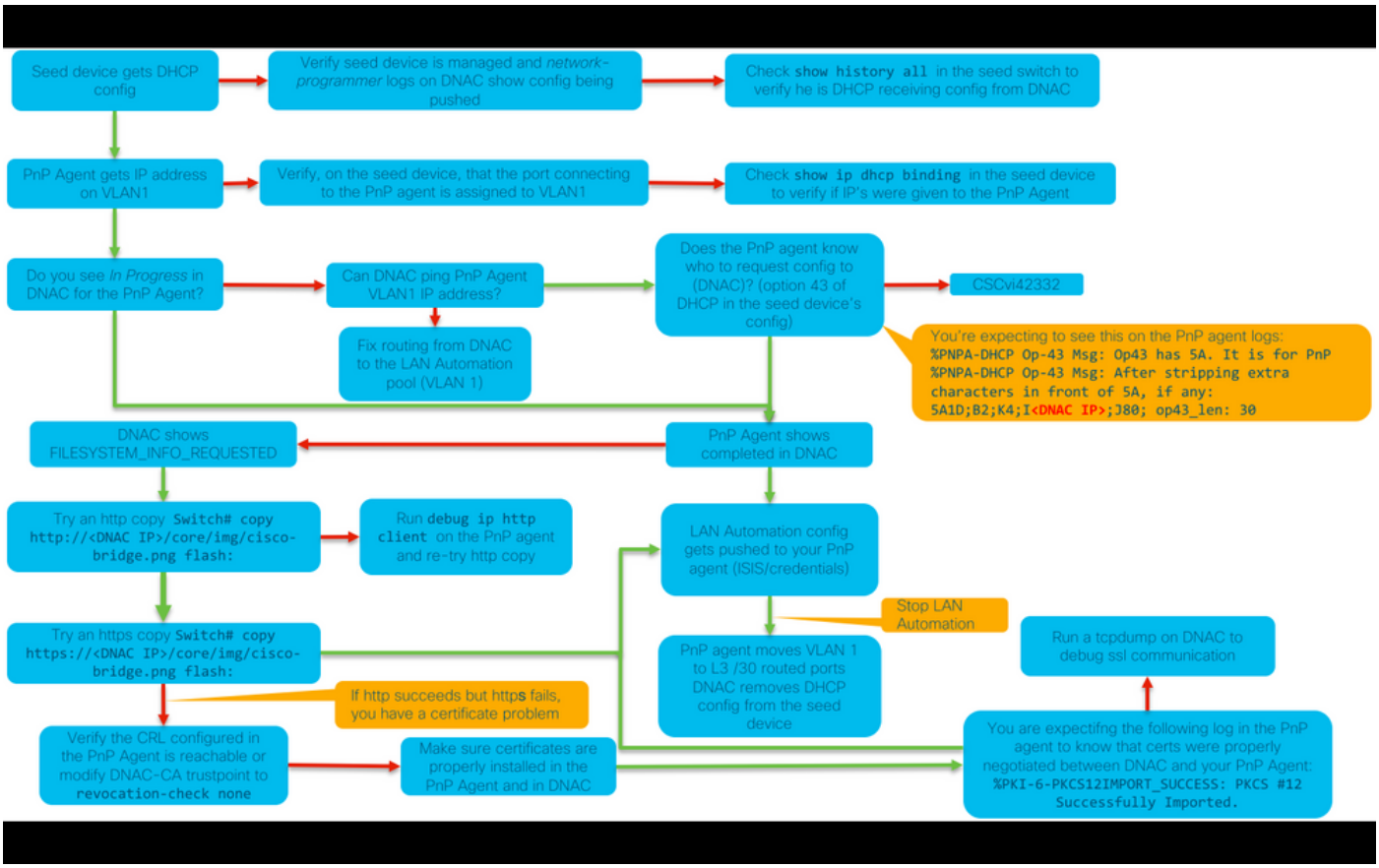
> **Hinweis**: Dieser Pool ist in drei Segmente unterteilt:
> 1. Die IP-Adressen, die in VLAN 1 Ihrer PnP-Agenten übertragen werden.
> 2. Die IP-Adressen, die auf Ihren PnP-Agenten an Loopbac0 übertragen werden.
> 3. Die /30-IP-Adressen, die an die PnP-Agenten der Verbindung weitergeleitet werden, die mit dem Seed oder anderen Fabric-Geräten verbunden ist.

Damit DNA Center Ihre PnP-Agenten bereitstellen kann, muss für die DHCP-Konfiguration, die das Seed-Gerät empfängt, die Option 43 definiert sein, die mit der IP-Adresse der geschäftsorientierten Network Interface Card (NIC) des DNA-Centers oder der Virtual IP (VIP)-Adresse definiert ist, wenn Sie über einen n-Node-Cluster verfügen.

Beim Booten von PnP-Agenten haben diese keine Konfiguration. Daher sind alle Ports Teil von VLAN 1. Folglich senden die Geräte DHCP-Erkennungsmeldungen an das Seed-Gerät. Das Seed-Gerät antwortet mit einem Angebot der IP-Adressen im LAN-Automatisierungspool.

Nachdem Sie die anfängliche Abfolge der LAN-Automatisierung verstanden haben, können Sie den Prozess beheben, wenn er nicht wie erwartet funktioniert.

Fehlerbehebungsdiagramm



DNA Center 1.1 LAN Automation relevante Protokolle

- Netzwerkorchestrierungs-Service
- Pnp-Service

DNA Center 1.2 LAN Automation relevante Protokolle

In Version 1.2 gibt es keinen PnP-Service mehr, daher müssen Sie bei der Fehlerbehebung für die LAN-Automatisierung nach den folgenden Services suchen:

- Netzwerkorchestrierung
- Netzwerkdesign
- VerbindungManager-Service
- Onboarding-Service *(dies ist das alte Pnp-Service-Äquivalent von 1.1)*

DNA Center 1.x Public Key Infrastructure (PKI) - relevante Protokolle

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

Wie wird die tcpdump ausgeführt, die im Flussdiagramm angezeigt wird?

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

* Um diese Einstellung zu beenden, drücken Sie STRG+C.

Dadurch wird die Datei pnp_capture.pcap in /data/tmp/ gespeichert. Sie müssen die Datei mithilfe des Befehls Secure Copy (SCP) vom DNA Center kopieren oder die Datei mithilfe des folgenden Befehls vom DNA Center lesen:

```
$ 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
```

Was ist die Datei bridge.png, die Sie kopieren möchten?

Es ist eine 191-Byte-Bilddatei, die sich im DNA-Center befindet und mit HTTP (ohne Zertifikate) oder HTTPS (mithilfe von Zertifikaten) kopiert werden soll, um die Kommunikation zwischen dem DNA-Center und Ihrem PnP-Agent zu testen.

Beispielerfassungen, wenn die SSL-Kommunikation (Secure Sockets Layer) nicht wie erwartet funktioniert (vollständige Pcap-Dateien, die diesem Artikel beigefügt sind)

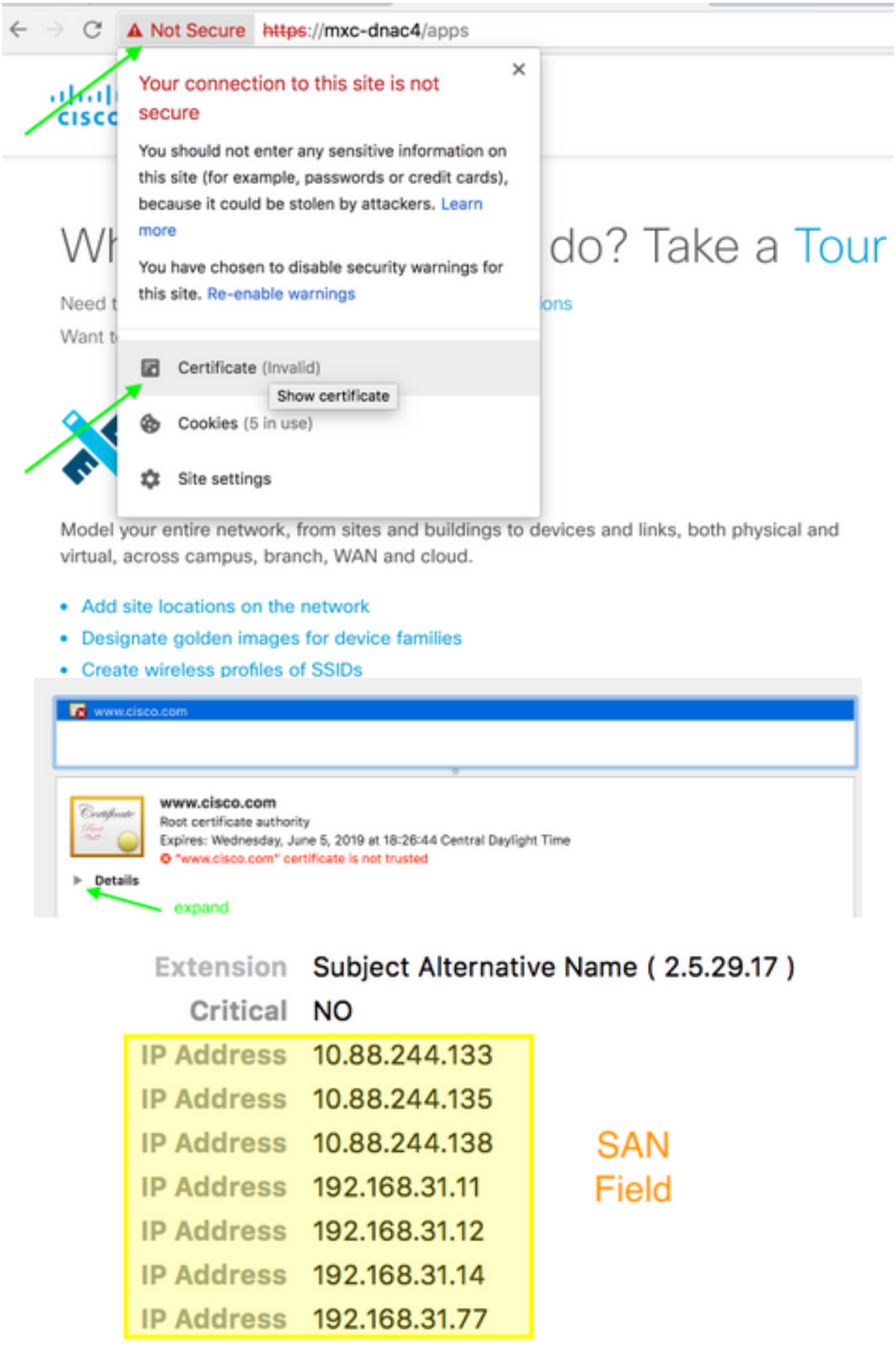
Ungültiges Zertifikat

Mögliche Ursache:

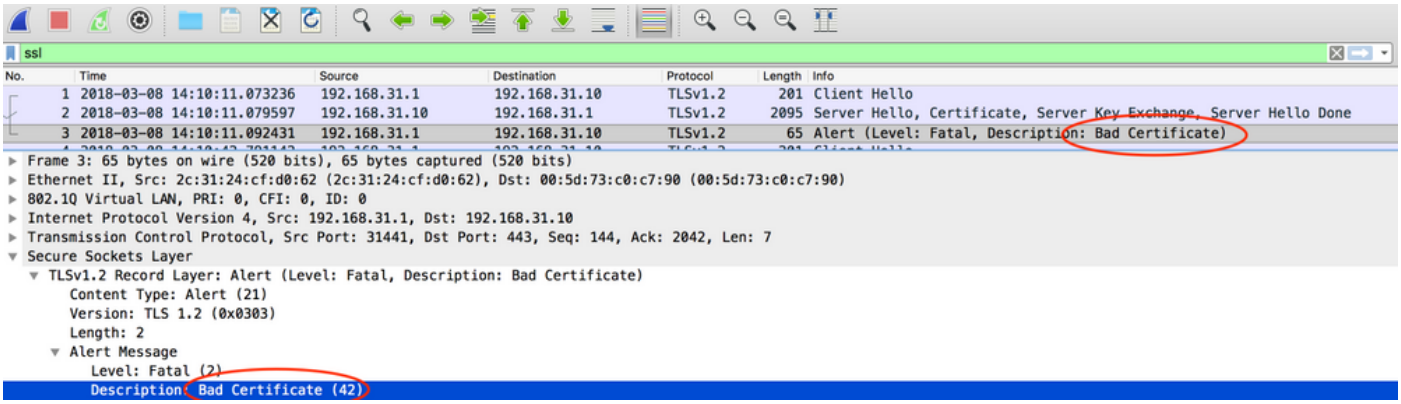
- Das Zertifikat von DNA Center hat im Feld Subject Alternative Name (SAN) nicht die richtige IP-Adresse.

So überprüfen Sie die SAN-Felder im Zertifikat:

Überprüfen Sie das Zertifikat mithilfe eines Browsers.



Beispielerfassung



Lösung.

Wenn Sie eine Zertifizierungsstelle eines Drittanbieters (Certificate Authority, Zertifizierungsstelle eines Drittanbieters) haben, stellen Sie sicher, dass Sie ein Zertifikat mit den IP-Adressen des DNA-Zentrums und des VIP erhalten. Wenn Sie keine Zertifizierungsstelle eines Drittanbieters haben, kann DNA Center ein Zertifikat für Sie generieren. Wenden Sie sich an das Cisco TAC, um diesen Prozess zu durchlaufen.

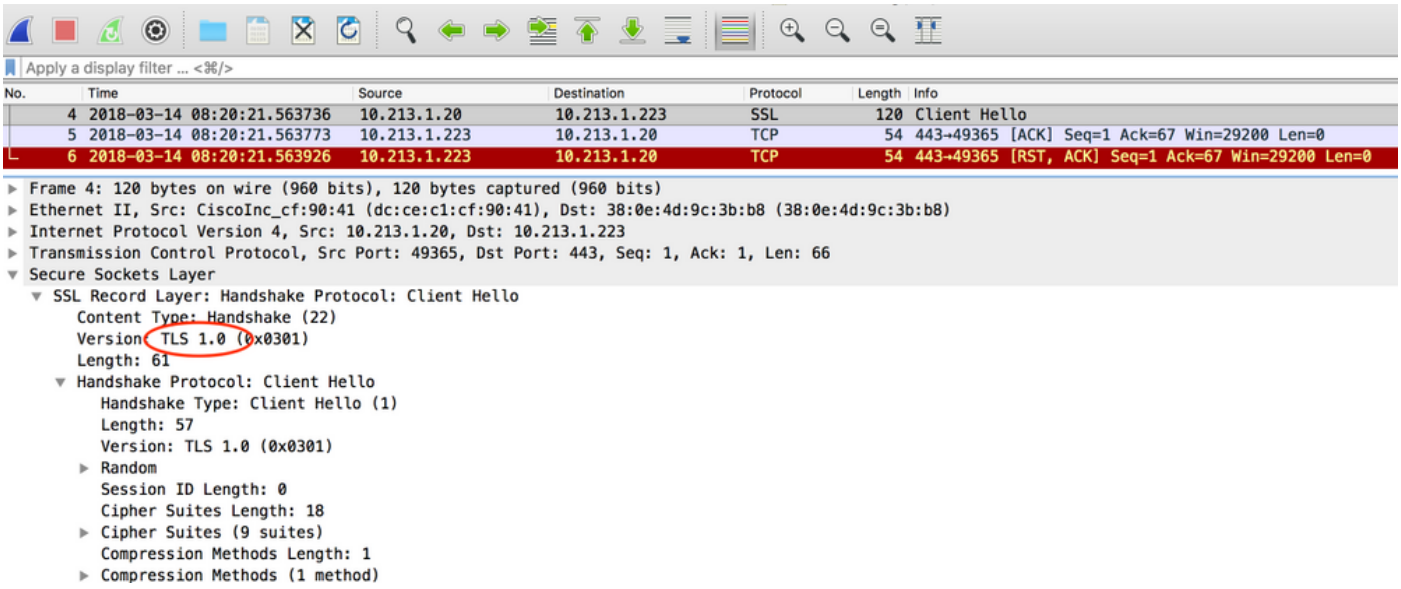
DNA Center setzt Verbindung zurück

Mögliche Ursache:

DNA Center unterstützt standardmäßig nur TLS v1.2.

Um dies zu umgehen, aktivieren Sie das DNA-Center, um TLS v1 entsprechend diesem Leitfaden zu verwenden.

Beispielerfassung



Nützliche Debug-Befehle auf dem PnP-Agent für zertifikatbezogene Probleme

- Debuggen von Krypto-Pki-Transaktionen
- debug ssl openssl
- debuggen ssl openssl-Fehler
- debuggen ssl openssl fehler
- debuggen crypto pki API
- Debuggen von Krypto-Pki-Transaktionen
- debug ssl openssl msg

Die Antwort fehlt, nachdem ein authentifizierter Sitzungsschlüssel erstellt wurde.

Theoretisch sollten Sie keine nicht beanspruchten Geräte auf der Seite Provisioning > Devices > Device Inventory (Bereitstellung > Geräte > Gerätebestand) finden. Es gab jedoch Probleme, bei denen die Geräte nach dem Löschen der nicht beanspruchten Geräte von dieser Seite noch unter https://<DNA Center ip>/mypnp angezeigt wurden. Wenn Sie auf dieses Szenario stoßen und ein Protokoll ähnlich dem folgenden in den PnP-Protokollen oder ein Hinweis darauf in der GUI sehen, stellen Sie sicher, dass das Gerät nicht als in PnP nicht als nicht beansprucht angezeigt wird:

```
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
```

Gotchas von LAN-Automatisierung und Stacking

- In DNA Center 1.2 muss der Stack einen vollständigen Ring aufweisen (ein Stack-Kabel für einen Stack mit zwei Elementen funktioniert möglicherweise nicht).
- Stack-Geräte müssen umgehend durch die LAN-Automatisierung beansprucht werden (ca. 10 Minuten).
- Sobald er mit dem DNA Center verbunden ist, wird er in PnP als "Nicht beansprucht" angezeigt. Der PnP verwendet für die Stack-Bestimmung das 10-minütige Zeitfenster, das nach Ablauf dieses Zeitfensters im nicht beanspruchten Abschnitt der LAN-Automatisierung verbleibt.

Wenn Sie die RCA- oder PnP-Protokolle haben, können Sie nach nicht beanspruchten Gerätemeldungen suchen:

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

Wenn keine Nachrichten vorliegen, erreichen die nicht beanspruchten Gerätebenachrichtigungen nicht das DNA Center, und PnP kann dies nicht behaupten.

LAN-Automatisierung in einem Stack

1. Schließen Sie die Uplinks zu den Seed-Geräten.
2. Starten Sie LAN Automation im DNA-Center.
3. Löschen Sie die Startkonfiguration aus dem Stapel. **# Schreibfreigabe**

4. Entfernen Sie alle Zertifikate aus dem NVRAM. **# Löschen nvram:*.cer**
5. Entfernen Sie die Datei "vlan.dat". **# delete flash:vlan.dat**
6. Löschen Sie die Zertifikate auf dem Standby-Switch vom primären Switch aus. **# stby-nvram löschen:*.cer**

a) Trennen Sie die Stack-Kabel.

b) Melden Sie sich bei der Konsole jedes Mitglieds-Switches an.

c) Löschen Sie die Zertifikate. **# Löschen nvram:*.cer**

d) Löschen Sie die Flas-VLAN-Datenbank. **# delete flash:vlan.dat**

e Schließen Sie die Stack-Kabel wieder an.

7. Neustart.

8. Warten Sie, bis der Switch als Stack registriert ist, alle Mitglieder aufrufen und versuchen Sie, den ersten Konfigurationsdialog zu starten.

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


         --- System Configuration Dialog ---

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

9. Aktivieren Sie die Uplinks zu den Seed-Geräten. **# Kein Herunterfahren**

Format der Hostnamenzuweisungsdatei, die ich in meine LAN-Automatisierungsaufgabe importieren kann?

DNA Center erwartet eine CSV-Datei mit dem Hostnamen und der Seriennummer (Hostname, Seriennummer), wie im folgenden Beispiel gezeigt:

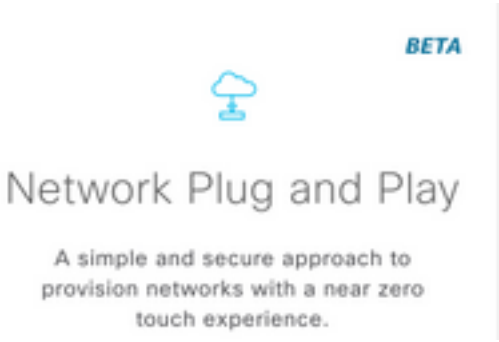
A	B
Edge1	FCW2048Cxxx
Edge2	FCW2131Lxxx, FCW2131Gxxx, FCW2131Gxxx, FCW2131Gxxx
Edge3	FOC2052Xxxx, FCW2052Cxxx, FCW2052Fxxx
Edge4	FXS2131Qxxx

Für die Stack-LAN-Automatisierung können Sie mit der CSV-Datei einen Hostnamen und mehrere Seriennummern pro Zeile eingeben. Die Seriennummern müssen durch Kommas getrennt werden. Referenz siehe angehängte CSV-Datei.

Wohin ging /mypnp in 1.2?

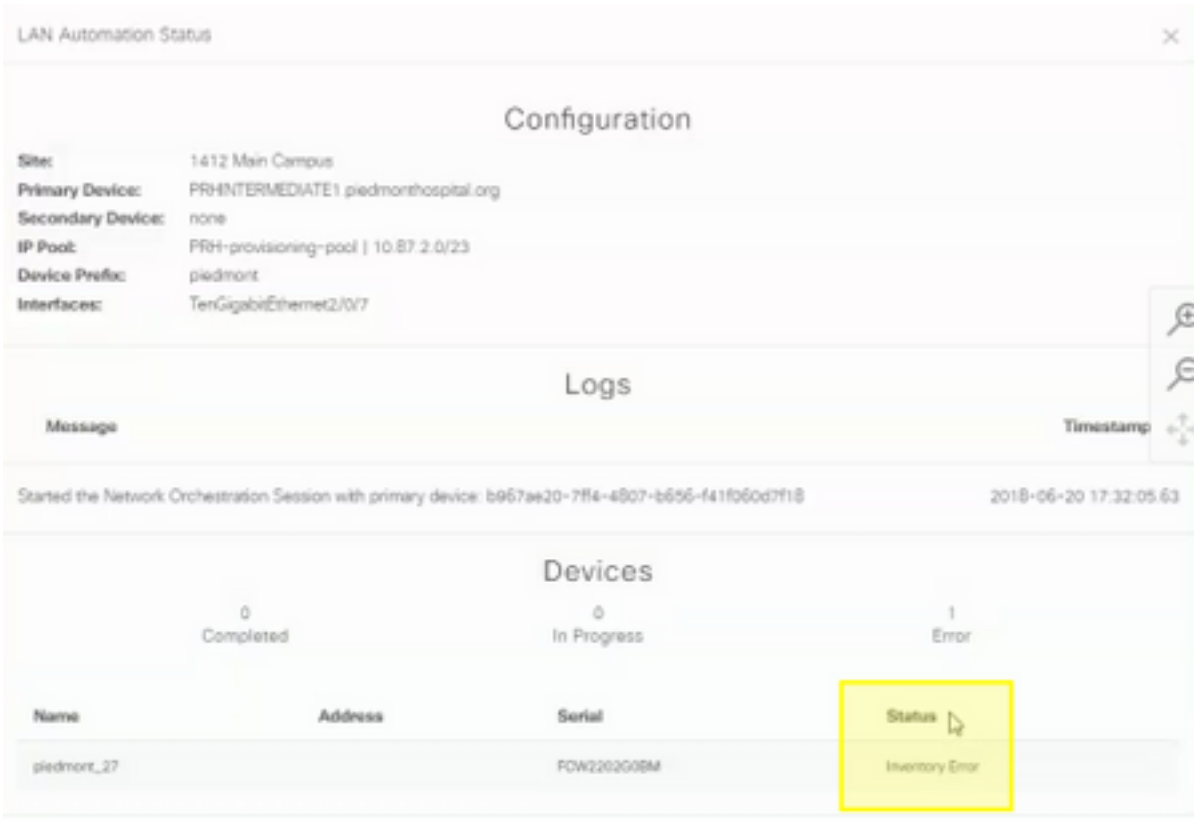
Sie haben folgende Möglichkeiten, auf PnP zuzugreifen:

- Geben Sie in Ihren Webbrowser https://<DNA Center IP>/networkpnp ein.
- Wählen Sie auf der DNS Center-Startseite das folgende Plug-and-Play-Tool für Netzwerke aus:



Oder besuchen Sie https://<DNA Center IP>/networkpnp

Inventarfehler



Der Inventarfehler bedeutet, dass das Gerät, nachdem es von der LAN-Automatisierung beansprucht und die Konfiguration empfangen wurde, nicht mehr im Bestand enthalten ist. Dieser Fehler tritt in der Regel aufgrund von Problemen mit der Konfiguration, einigen Routing- oder CLI-Anmeldeinformationen auf.

Um zu überprüfen, ob Sie versuchen, das richtige Gerät über die LAN-Automatisierung aufzurufen, greifen Sie mithilfe des bevorzugten Verbindungsprotokolls (SSH oder Telnet) remote auf die IP-Adresse der Loopback-0-Schnittstelle des Geräts zu.

Es besteht eine Verbindung, aber PKI-Zertifikate werden nicht erfolgreich an die PnP-Agenten weitergeleitet.

Manchmal schalten die Geräte in der Mitte die Paketbitrate *Do not Fragment* (DF) zwischen DNAC und den PnP-Agenten ein. Dies kann dazu führen, dass Pakete mit mehr als 1.500 Byte, in der Regel Pakete mit dem Zertifikat, verworfen werden und die LAN-Automatisierung daher möglicherweise nicht abgeschlossen wird. Einige der gängigen Protokolle, die in den *Onboarding*-Protokollen des DNA Center zu sehen sind, sind:

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

In diesem Fall wird empfohlen, sicherzustellen, dass der Pfad zwischen dem DNA Center und den PnP-Agenten Jumbo Frames mithilfe des Befehlssystems **mtu 9100** durchlaufen lässt.

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