LAN Automation Tips en Tricks voor Digital Network Architecture (DNA) Center

Inhoud

[Inleiding](#)
[glanzend](#)
[Voorwaarden](#)
[Voorschriften](#)
[Achtergrondinformatie](#)
[Voordat u begint](#)
[Wat zijn de stappen die LAN Automation uitvoert?](#)
[Diagram van een probleemoplossing](#)
[DNA Center 1.1 LAN-automatiseringsrelevante bestanden](#)
[DNA Center 1.2 LAN-automatiseringsrelevante bestanden](#)
[Voor DNA Center 1.x openbare sleutelinfrastructuur (PKI) relevante stammen](#)
[Hoe voert u de romp uit die in het stroomschema staat?](#)
[Wat is dat bridge.png-bestand dat je probeert te kopiëren?](#)
[Monster neemt op wanneer Secure Socket Layer (SSL) communicatie niet werkt zoals verwacht (volledige .pcap-bestanden die aan dit artikel zijn gekoppeld)](#)
[Slecht certificaat](#)
[Mogelijke oorzaak:](#)
[Controleer het certificaat met een browser](#)
[Monsteropname](#)
[Resolutie.](#)
[DNA Center stelt de verbinding opnieuw in](#)
[Mogelijke oorzaak:](#)
[Beeldopname](#)
[Handige debug-opdrachten in de VPNP-agent voor certificaatproblemen](#)
[De respons ontbreekt eerder ingestelde geauthentiseerde sessie-toets](#)
[Gezond verstand van LAN-automatisering en -stapeling](#)
[LAN Automation op een stapel doen](#)
[Format van het hostname-kaartbestand dat ik naar mijn LAN Automation-taak kan importeren?](#)
[Waar ging /mypnp in 1.2?](#)
[Fantasiefout](#)
[Connectiviteit bestaat maar PKI-certificaten worden niet met succes naar de VPN-agents geduwd](#)

Inleiding

Dit document geeft een overzicht van LAN-automatisering (Local Area Network) om u te helpen problemen diagnosticeren wanneer LAN Automation niet werkt zoals verwacht in Digital Network Architecture (DNA) Center.

Bijgedragen door Alexandro Carrasquedo, Cisco TAC Engineer.

glanzend

Plug and Play Agent (PnP): Nieuw apparaat dat u hebt ingeschakeld zonder configuratie en zonder certificaten die automatisch worden ingesteld door DNA Center.

Seed device: Apparaat dat DNA Center al voorzieningen heeft getroffen en dat fungeert als de Dynamic Host Configuration Protocol (DHCP) server.

Voorwaarden

Voorschriften

Cisco raadt sterk aan dat u een algemene kennis van LAN Automation en de Plug and Play Solutions hebt. geeft een overzicht van LAN Automation, hoewel het gebaseerd is op DNA Center 1.0, is hetzelfde concept van toepassing op DNA Center 1.1 en hoger.

Achtergrondinformatie

LAN-automatisering is een vrijwel nulpunt-implementatieoplossing waarmee u uw netwerkapparaten kunt configureren en configureren met het gebruik van ISIS als onderliggende routingprotocol.

Voordat u begint

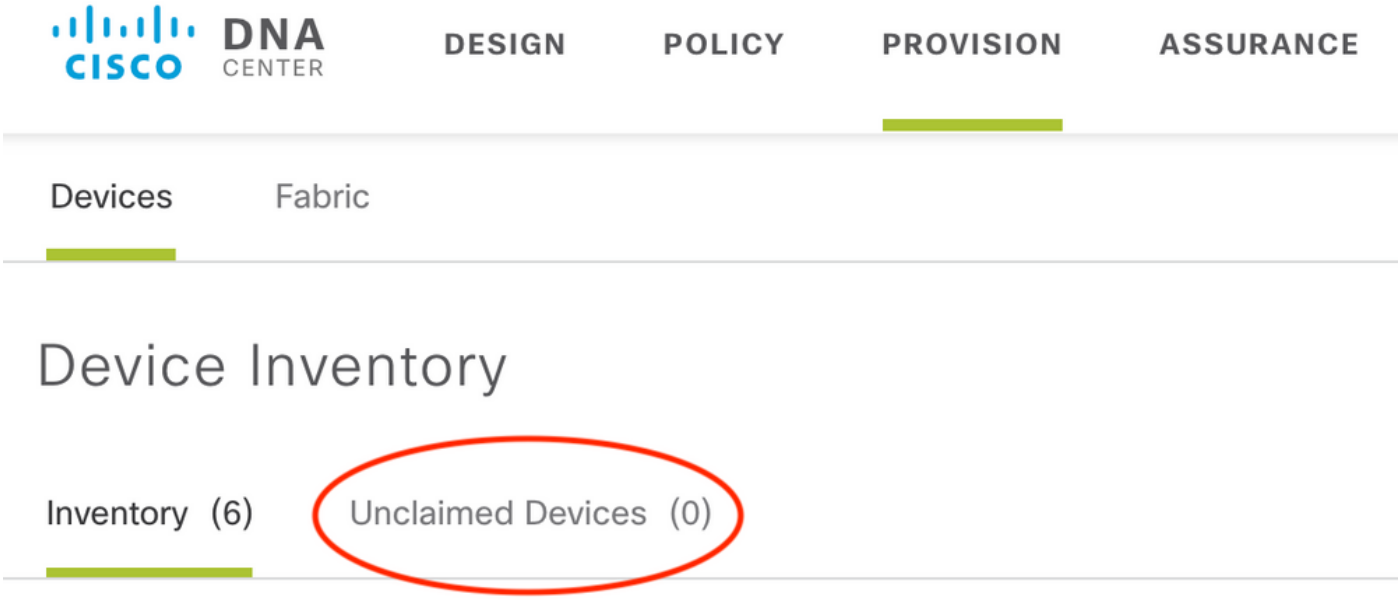
Voordat u LAN Automation start, moet u ervoor zorgen dat uw VPNP Agent geen certificaten heeft die in NVRAM zijn geladen.

```
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
```

Zorg ervoor dat u geen niet-geclaimde apparaten hebt in de pagina Provisioning > Apparaten > Apparaatinventaris:



Vanwege CSCvh68847 Het kan zijn dat sommige stapels de niet geclaimde staat niet achterlaten en dat je een error_STACK_UNSUPPORTED foutmelding krijgt. Dit bericht gebeurt wanneer de LAN-automatisering probeert de voorziening van het apparaat op te eisen alsof het om één schakelaar gaat. Omdat het apparaat echter een Catalyst 9300 switchstack is, kan LAN-automatisering het apparaat niet opeisen en verschijnt het apparaat als niet-geclaimd. Op dezelfde manier beweert PnP het apparaat niet omdat het een stapel is, dus wordt het apparaat niet voorzien.

Wat zijn de stappen die LAN Automation uitvoert?

DNA Center regelt het zaadapparaat met de DHCP-configuratie. Het bereik van IP adressen dat het zaadapparaat krijgt is een segment van de eerste pool die u definieerde wanneer u de IP adrespool voor uw site gereserveerd hebt. Deze pool moet ten minste /25 zijn.

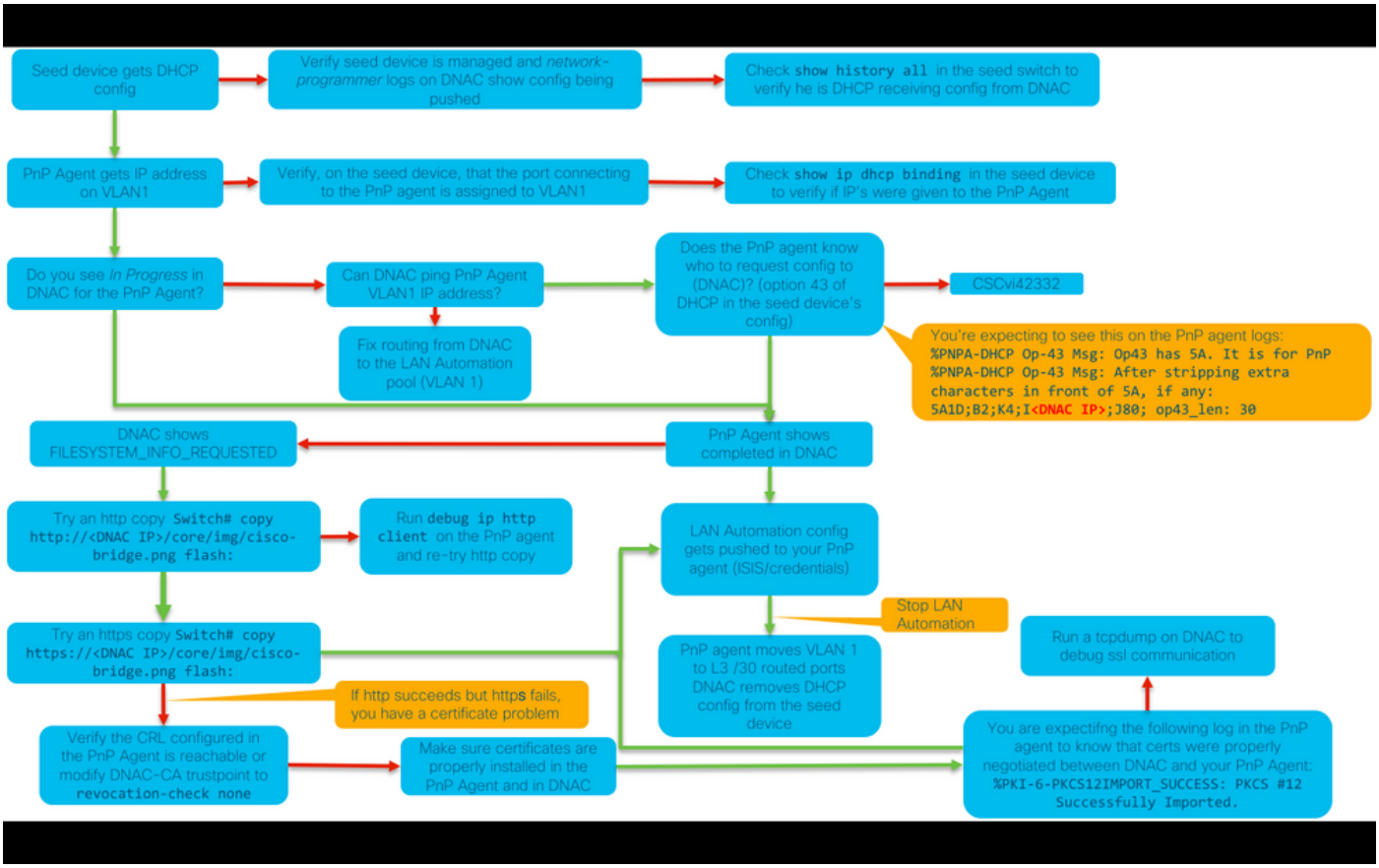
> Opmerking: Deze groep is verdeeld in drie segmenten:
> 1. De IP-adressen die op uw VPN-agents naar VLAN 1 worden geduwd.
> 2. De IP-adressen die naar Loopbac0 op uw VPN-agents worden geduwd.
> 3. De /30 IP-adressen die naar uw VPN-agents zijn geduwd op de link die op uw zaadje of andere wasapparaten is aangesloten.

Voor DNA Center om uw PPP-agents aan te bieden, moet de DHCP-configuratie die het zaadapparaat ontvangt, optie 43 hebben, gedefinieerd met het IP-adres van het DNA Center ondernemings-facing Network Interface Card (NIC) of het Virtual IP-adres (VIP), als u een n-knooppunt-cluster hebt.

Als de PnP agenten beginnen, hebben ze geen configuratie. Daarom maken al hun poorten deel uit van VLAN 1. Dientengevolge, verzenden de apparaten DHCP ontdekking berichten naar het zaadapparaat. Het zaadapparaat beantwoordt met een aanbod van de IP adressen binnen de LAN automatiseringspool.

Nu u de eerste reeks LAN-automatisering begrijpt, kunt u het proces problemen oplossen als het niet werkt zoals verwacht.

Diagram van een probleemoplossing



DNA Center 1.1 LAN-automatiseringsrelevante bestanden

- netwerkorkestratiedienst
- PPP-service

DNA Center 1.2 LAN-automatiseringsrelevante bestanden

In release 1.2 is er niet langer een PPP-service, dus u moet naar de volgende services zoeken wanneer u LAN-automatisering wilt oplossen:

- netwerkorkestratie
- netwerkontwerp
- connectiebedrijfsleidingsdienst
- instapservice *(dit is het oude PPP-servicesequivalent van 1.1)*

Voor DNA Center 1.x openbare sleutelinfrastructuur (PKI) relevante stammen

- apic-em-pki-makelaar
- apic-em-jbaas-ejbca

Hoe voert u de romp uit die in het stroomschema staat?

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

*Om dit gebruik te stoppen CTRL+C

Dit slaat het bestand pnp_catch.pcap op in /data/tmp/. U moet het bestand vanuit DNA Center kopiëren met de beveiligde kopie (SCP) opdracht of het bestand vanuit DNA-centrum lezen met de volgende opdracht:

```
$ 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
```

Wat is dat bridge.png-bestand dat je probeert te kopiëren?

Het is een 191 byte-beeldbestand dat in DNA-centrum is gelokaliseerd dat u wilt kopiëren met HTTP (zonder certificaten te gebruiken) of HTTPS (met certificaten) om communicatie tussen DNA-centrum en uw PnP-agent te testen.

Monster neemt op wanneer Secure Socket Layer (SSL) communicatie niet werkt zoals verwacht (volledige .pcap-bestanden die aan dit artikel zijn gekoppeld)

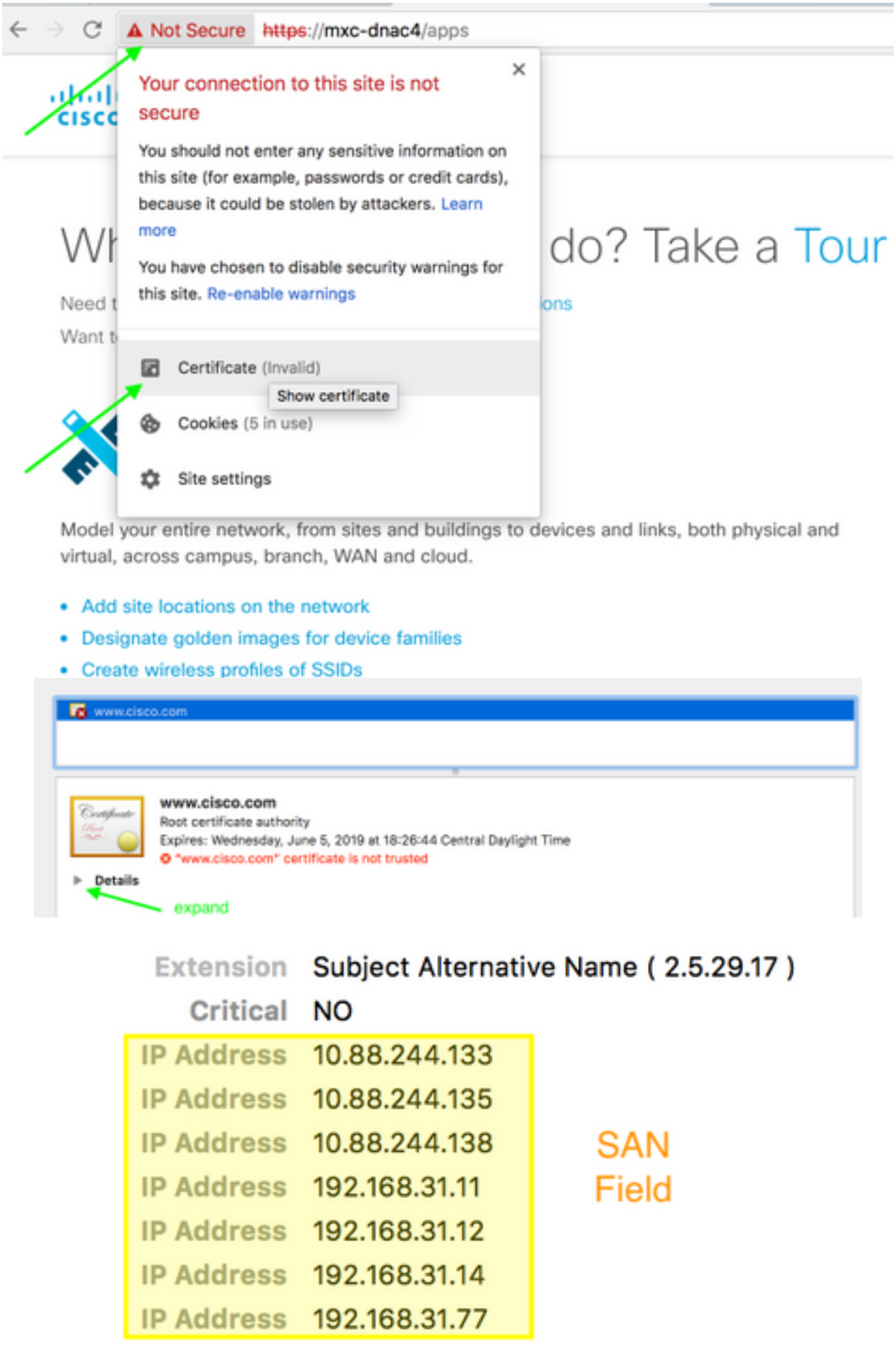
Slecht certificaat

Mogelijke oorzaak:

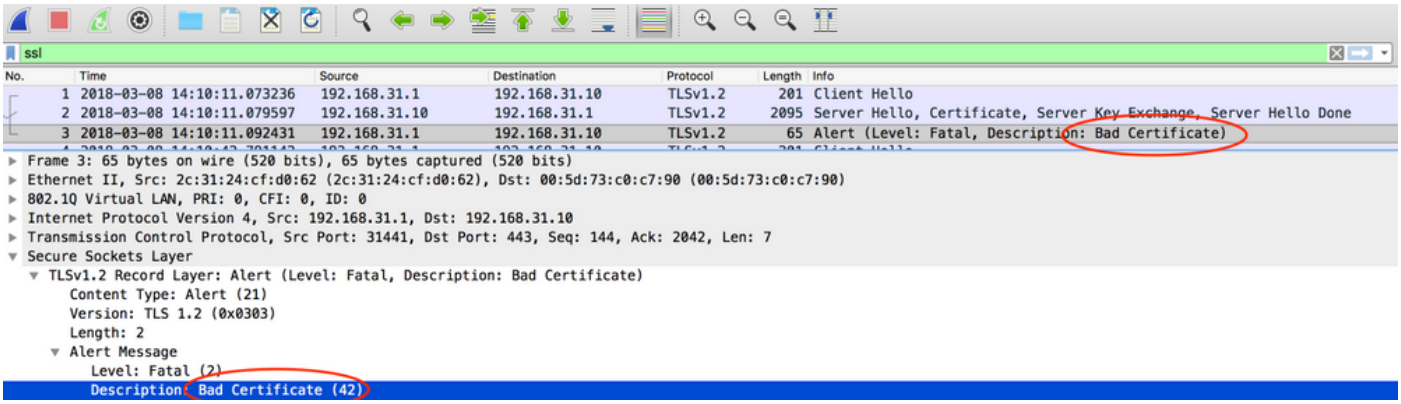
- Het certificaat van DNA Center heeft niet het juiste IP-adres in het veld Onderwerp Alternative Name (SAN).

U kunt de SAN-velden in uw certificaat als volgt controleren:

Controleer het certificaat met een browser



Monsteropname



Resolutie.

Als u een CA (certificaatinstantie) van derden hebt, zorg er dan voor dat u een certificaat met de IP-adressen van het DNA-centrum en de VIP in het certificaat krijgt. Als je geen derde partij CA hebt, kan DNA Center een certificaat voor je genereren. Neem contact op met Cisco TAC om u door dit proces te leiden.

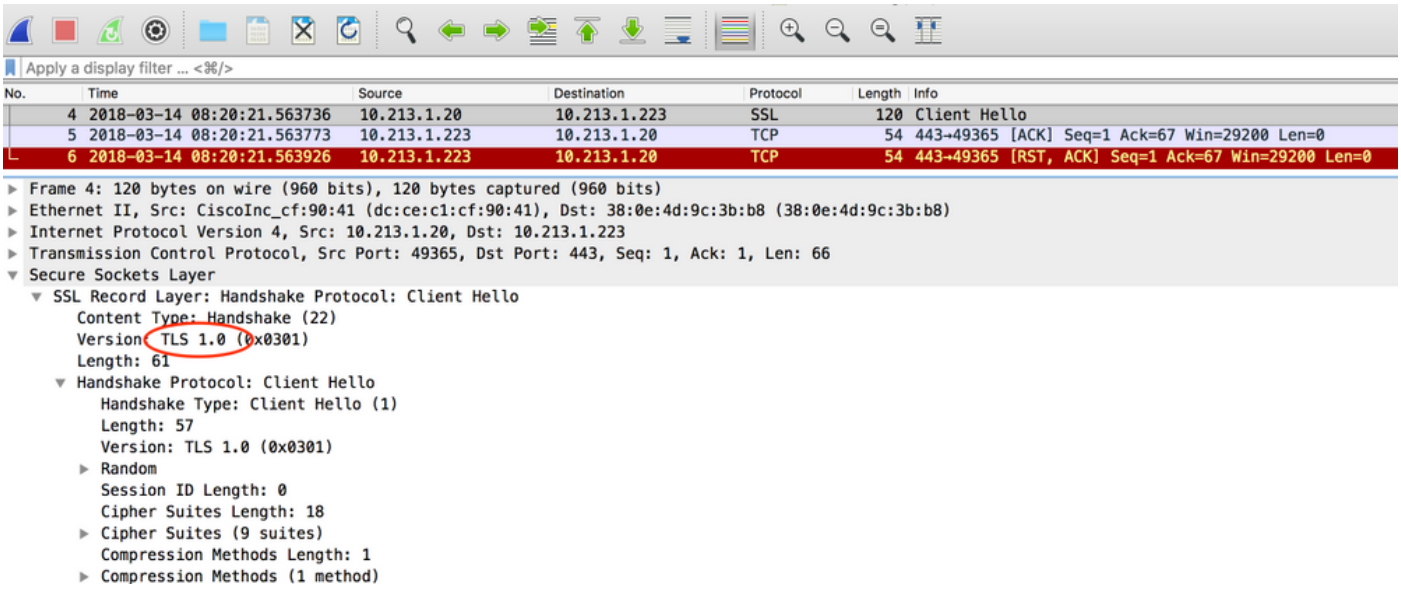
DNA Center stelt de verbinding opnieuw in

Mogelijke oorzaak:

DNA Center ondersteunt TLS v1.2 standaard alleen.

Om dit aan te passen, stelt u DNA Center in om TLS v1 te gebruiken volgens deze handleiding

Beeldopname



Handige debug-opdrachten in de VPNP-agent voor certificaatproblemen

- debug van crypto pki - transacties
- debug ssl openssl

- debug ssl openssl errores
- fouten van ssl openssl debug
- API voor boekingen met cryptoom
- debug van crypto pki - transacties
- debug van ssl openssl msg

De respons ontbreekt eerder ingestelde geauthentiseerde sessie-toets

In theorie, zou u geen ongevraagde apparaten in de pagina Provisioning > Apparaten > Apparaatinventaris moeten hebben, maar er zijn problemen geweest waar de apparaten, na het verwijderen van de niet geclaimde apparaten van deze pagina, nog steeds werden weergegeven in https://<DNA Center ip>/mypnp. Als u dit scenario tegenkomt en u een logbestand ziet dat lijkt op het volgende in de PnP-logbestanden of een indicatie van hetzelfde in de GUI, zorg er dan voor dat het apparaat niet verschijnt zoals niet wordt geclaimd in PnP:

```
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
```

Gezond verstand van LAN-automatisering en -stapeling

- In DNA Center 1.2 moet de stapel volledig zijn (één stapelkabel voor een stapel van 2 leden werkt misschien niet).
- Stapelapparaat moet door LAN-automatisering onmiddellijk worden opgeëist, ongeveer minder dan 10 minuten.
- Zodra het is verbonden met DNA Center verschijnt het in PnP als niet-geclaimd. PnP gebruikt het venster van 10 minuten voor het bepalen van de stapel en zodra het verlopen is zal het in het niet-geclaimde gedeelte van de LAN Automation blijven.

Als u de RCA of PPP logboeken hebt, kunt u naar niet-geclaimde apparaatberichten zoeken:

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

Als er geen berichten zijn, bereiken de meldingen van ongevraagde apparaten niet het DNA Center en kan PnP dat niet claimen.

LAN Automation op een stapel doen

1. Sluit de uplinks aan op de zaaddrager(s).
2. Start LAN Automation op DNA Center.
3. Verwijdert de opstartconfiguratie vanaf de stapel. **# schrijven wissen**
4. Verwijder alle certificaten van NVRAM. **# verwijderde nvram:*.cer**
5. Verwijder het bestand vlan.dat. **# verwijdert flitser:vlan.dat**
6. Verwijder de certificaten in de standby-schakelaar van de primaire schakelaar. **# verwijdert stby-nvram:*.cer**

a. Koppel de stapelkabels los.

b. Log in op de console van elke switch.

c. Verwijdert de certificaten. **# verwijderde nvram:*.cer**

d. Verwijdert de VLAN-database. **# verwijdert flitser:vlan.dat**

e. Sluit de stapelkabels weer aan.

7. Herstart.

8. Wacht tot de schakelaar om als stapel te registreren, breng alle leden op, en probeer het eerste configuratiedialoogvenster te 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. Schakel de uplinks in op het/de zaden. **# afgesloten**

Format van het hostname-kaartbestand dat ik naar mijn LAN Automation-taak kan importeren?

DNA Center verwacht een CSV-bestand met de hostnaam en het serienummer (hostname, serienummer) zoals in het volgende voorbeeld:

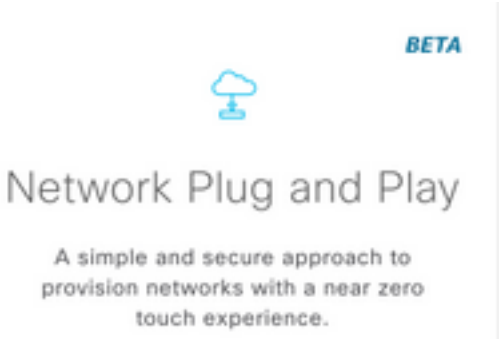
A	B
Edge1	FCW2048Cxxx
Edge2	FCW2131Lxxx, FCW2131Gxxx, FCW2131Gxxx, FCW2131Gxxx
Edge3	FOC2052Xxxx, FCW2052Cxxx, FCW2052Fxxx
Edge4	FXS2131Qxxx

Voor stapel LAN Automation kunt u met het CSV-bestand één hostnaam en meerdere serienummers per rij invoeren. De serienummers moeten van elkaar worden gescheiden door komma's. Zie Bijgevoegd CSV-bestand voor nadere informatie.

Waar ging /mypnp in 1.2?

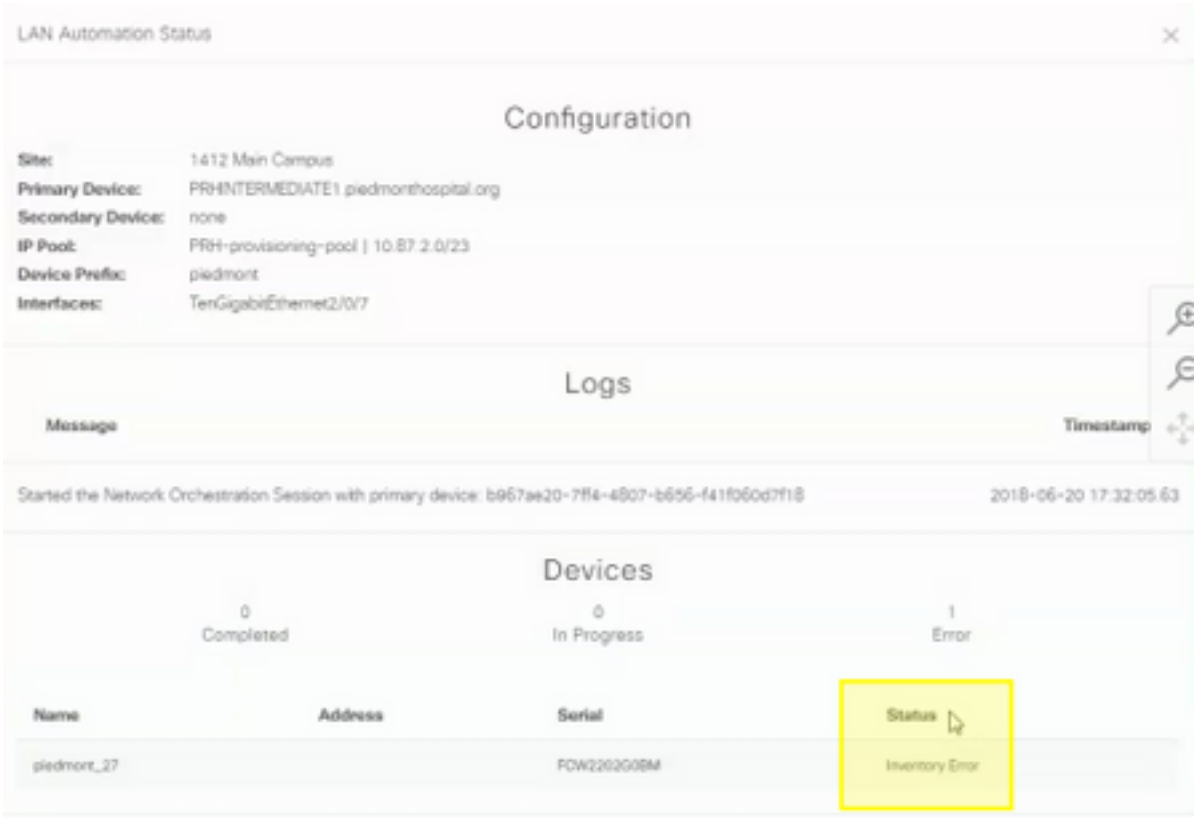
Toegang tot VPNP op een van de volgende manieren:

- Voer vanuit uw webbrowser https://<DNA Center IP>/netwerk in
- Selecteer in de startpagina van het DNA-centrum de volgende stekker en afspeelgereedschap:



Of door naar https:// te gaan.

Fantasiefout



De opslagfout betekent dat het apparaat, nadat het door LAN-automatisering is geclaimd en de configuratie is ontvangen, niet aan de inventaris wordt toegevoegd. Deze fout komt gewoonlijk voor vanwege of de configuratie, sommige routing, of CLI aanmeldingsproblemen.

Om te verifiëren dat u het juiste apparaat via LAN Automation probeert op te zetten, toegang van afstand tot het IP-adres van de loopback 0 interface op het apparaat met het favoriete verbindingsprotocol (SSH of telnet).

Connectiviteit bestaat maar PKI-certificaten worden niet met succes naar de VPN-agents geduwd

Er zijn een aantal keren dat de apparaten in het midden de pagina's tussen de DNA- en de PnP-agents kunnen *inschakelen*. Dit kan ervoor zorgen dat pakketten die groter zijn dan 1500 bytes, veel pakketten met het certificaat worden verzonden, worden verwijderd en daarom kan LAN Automation niet voltooid zijn. Een aantal gemeenschappelijke logs die te zien zijn in de

onboarding logs van DNA Center zijn:

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

De voorgestelde actie in dit geval is om ervoor te zorgen dat het pad tussen DNA Center en de PnP agents jumboframes mogelijk maakt door gebruik van het opdrachtsysteem **mtu 9100**.

Switch (configuratie)# **systeem mtu 9100**