Consejos y trucos de automatización de LAN para el centro de arquitectura de red digital (DNA)

Contenido

Introducción

Este documento proporciona una descripción general de la automatización de la red de área local

(LAN) para ayudarle a diagnosticar problemas cuando la automatización de la LAN no funciona como se espera en el Centro de arquitectura de red digital (DNA).

Colaborado por Alexandro Carrasquedo, Ingeniero del TAC de Cisco.

Glosario

Agente Plug and Play (PnP): Nuevo dispositivo que acaba de encender sin configuración y sin certificados que el Centro de DNA configure automáticamente.

Dispositivo simiente: Dispositivo que el Centro DNA ya ha aprovisionado y que actúa como servidor del Protocolo de configuración dinámica de host (DHCP).

Prerequisites

Requisitos

Cisco recomienda encarecidamente que tenga un conocimiento general de la automatización de la LAN y de la solución Plug and Play. ofrece una visión general de la automatización de LAN, aunque se basa en DNA Center 1.0, el mismo concepto se aplica al DNA Center 1.1 y superiores.

Antecedentes

La automatización de LAN es una solución de implementación casi sin intervención del usuario que permite configurar y aprovisionar los dispositivos de red con el uso de ISIS como protocolo de ruteo subyacente.

Antes de comenzar

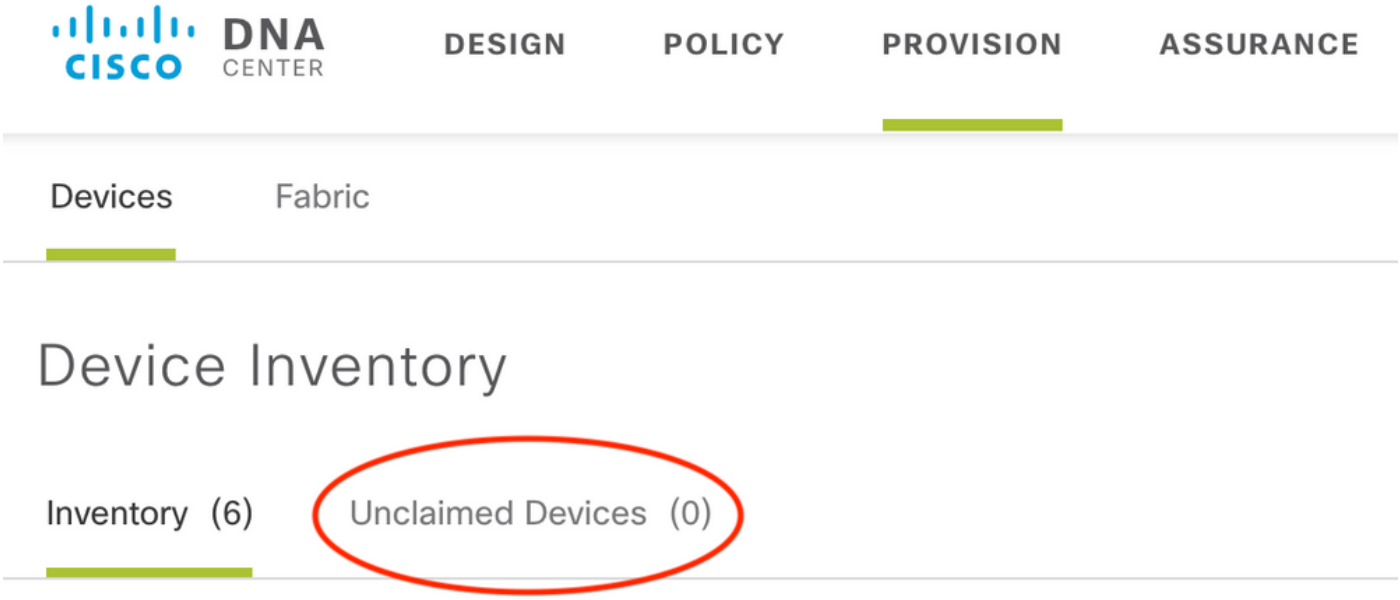
Antes de ejecutar LAN Automation, asegúrese de que el PnP Agent no tenga certificados cargados en NVRAM.

```
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
```

Asegúrese de que no tiene dispositivos no reclamados en la página Provisioning > Devices > Device Inventory:



Debido a CSCvh68847 , es posible que algunas pilas no salgan del estado no reclamado y que aparezca un mensaje de error ERROR_STACK_UNSUPPORTED. Este mensaje ocurre cuando la automatización de la LAN intenta solicitar que el dispositivo se aprovisione como si fuera un único switch. Sin embargo, debido a que el dispositivo es una pila de switches Catalyst 9300, la automatización de LAN no puede reclamar el dispositivo y el dispositivo aparece como no reclamado. De manera similar, PnP no reclama el dispositivo porque es una pila, por lo que el dispositivo no se aprovisiona.

¿Cuáles son los pasos que sigue la automatización de la LAN mientras se ejecuta?

DNA Center aprovisiona el dispositivo simiente con la configuración DHCP. El alcance de las direcciones IP que obtiene el dispositivo simiente es un segmento del conjunto inicial que definió cuando reservó el conjunto de direcciones IP para el sitio. Tenga en cuenta que este conjunto debe ser al menos /25.

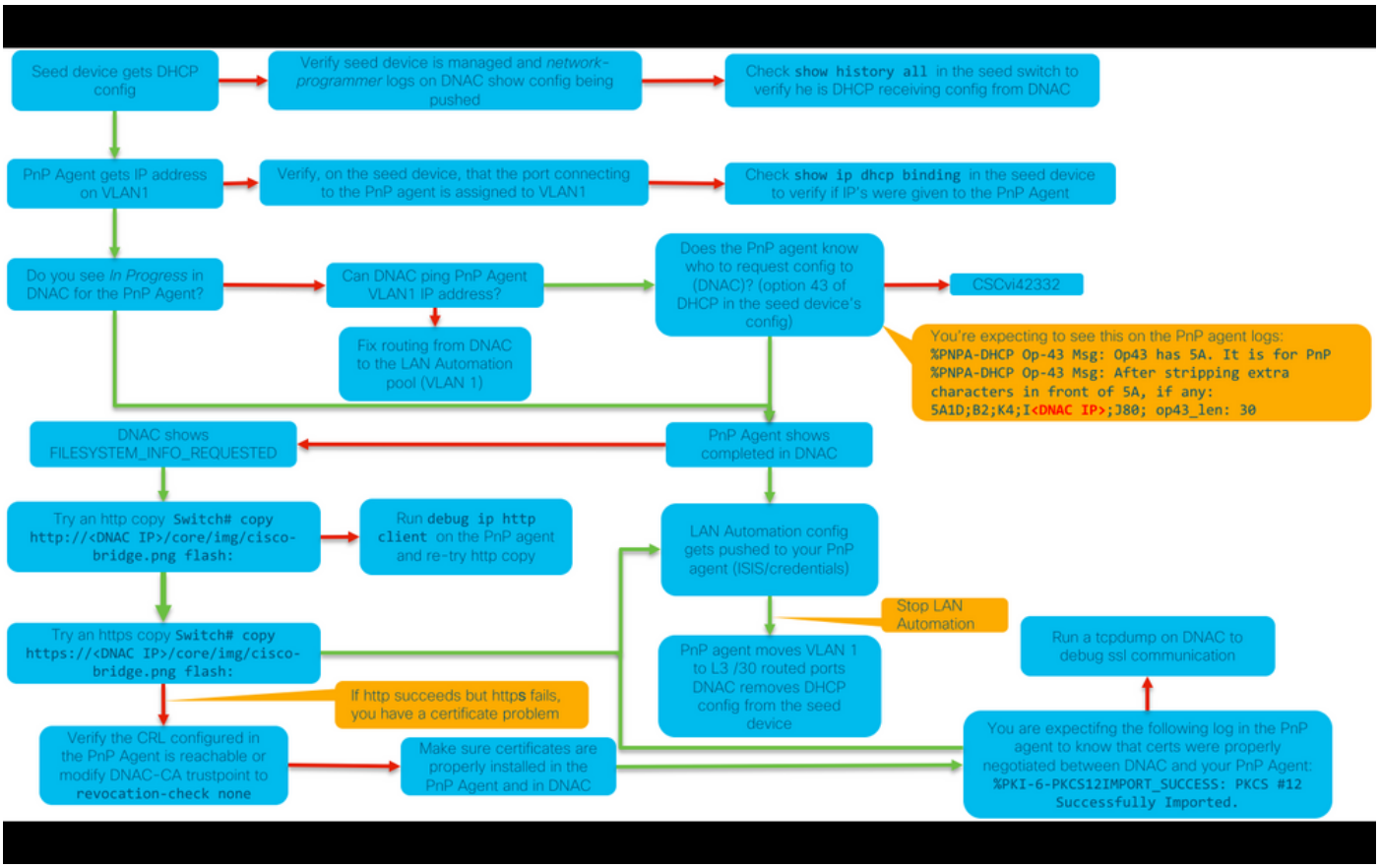
> **Nota:** Este conjunto se divide en 3 segmentos:
> 1. Las direcciones IP que se envían a VLAN 1 en sus agentes PnP.
> 2. Las direcciones IP que se envían a Loopbac0 en sus agentes PnP.
> 3. Las direcciones IP /30 que se envían a los agentes PnP en el link que se conecta a su inicialización u otros dispositivos de fabric.

Para que DNA Center aprovisione sus agentes PnP, la configuración DHCP que recibe el dispositivo simiente debe tener la opción 43 definida con la dirección IP de la tarjeta de interfaz de red (NIC) orientada a la empresa del centro DNA o la dirección IP virtual (VIP), si tiene un clúster de n nodos.

Cuando los agentes PnP se inician, no tienen ninguna configuración. Por lo tanto, todos sus puertos son parte de la VLAN 1. En consecuencia, los dispositivos envían mensajes de detección DHCP al dispositivo simiente. El dispositivo simiente responde con una oferta de las direcciones IP dentro del conjunto de automatización de LAN.

Ahora que comprende la secuencia inicial de automatización de LAN, puede resolver problemas del proceso si no funciona como se esperaba.

Diagrama de resolución de problemas



Registros relevantes de automatización de LAN de DNA Center 1.1

- network-orquestación-service
- pnp-service

Registros relevantes de automatización de LAN de DNA Center 1.2

En la versión 1.2 ya no hay un pnp-service, por lo que debe buscar los siguientes servicios cuando esté solucionando problemas de LAN Automation:

- orquestación de red
- diseño de red
- Conexión-manager-service
- onboarding-service *(este es el antiguo pnp-service equivalente de 1.1)*

Registros relevantes de la infraestructura de clave pública (PKI) de DNA Center 1.x

- apic-em-pki-broker-service
- apic-em-jpatrón-ejbca

¿Cómo se ejecuta el tcpdump que se muestra en el diagrama de flujo?

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

*Para detener esto, utilice CTRL+C

Esto almacena el archivo pnp_capture.pcap en /data/tmp/. Debe copiar el archivo desde el Centro de DNA usando el comando secure copy (SCP) o leer el archivo desde el Centro de DNA usando el siguiente comando:

```
$ 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
```

¿Qué es ese archivo bridge.png que intenta copiar?

Se trata de un archivo de imagen de 191 bytes que se encuentra en el centro de ADN y que desea copiar mediante HTTP (sin utilizar certificados) o HTTPS (mediante certificados) para probar la comunicación entre el centro de ADN y su agente de PnP.

Muestra de capturas cuando la comunicación de Secure Sockets Layer (SSL) no funciona como se esperaba (archivos .pcap completos adjuntos a este artículo)

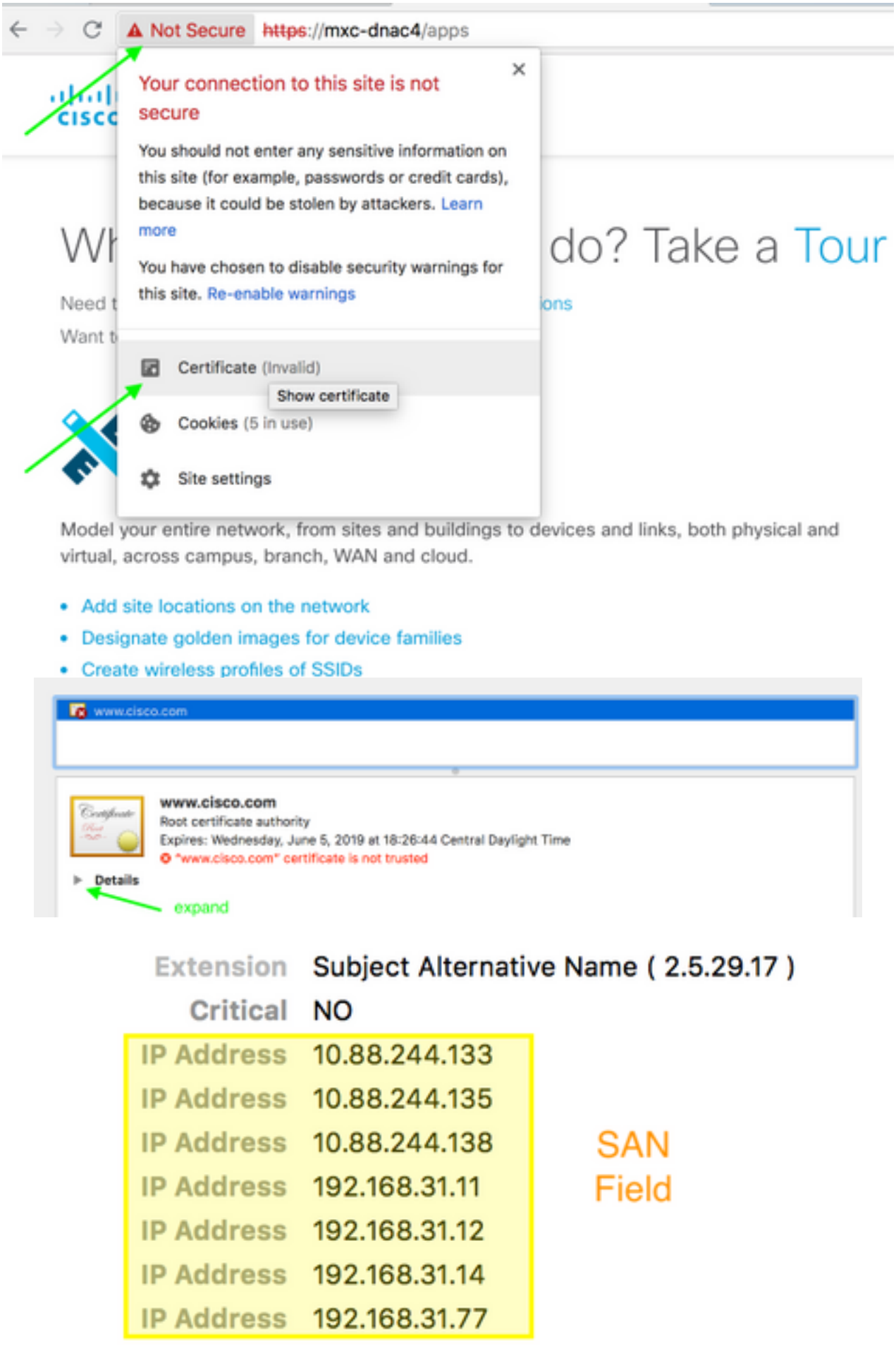
Certificado incorrecto

Posible causa:

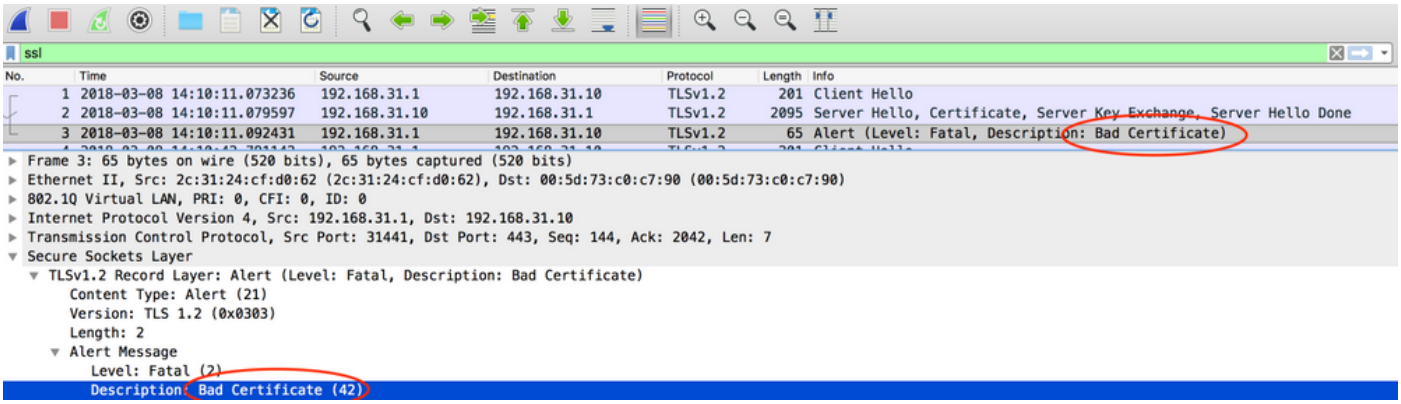
- El certificado de DNA Center no tiene la dirección IP correcta en el campo Subject Alternative Name (SAN) (Nombre alternativo del sujeto).

Para verificar los campos de SAN en su certificado, puede hacer lo siguiente:

Verificar el certificado mediante un navegador



Captura de muestra



Resolución.

Si tiene una CA de terceros (Autoridad de Certificación), asegúrese de que le proporcionen un certificado con las direcciones IP de DNA Center y el VIP en él. Si no tiene una CA de terceros, DNA Center puede generar un certificado para usted. Póngase en contacto con el TAC de Cisco para guiarle en este proceso.

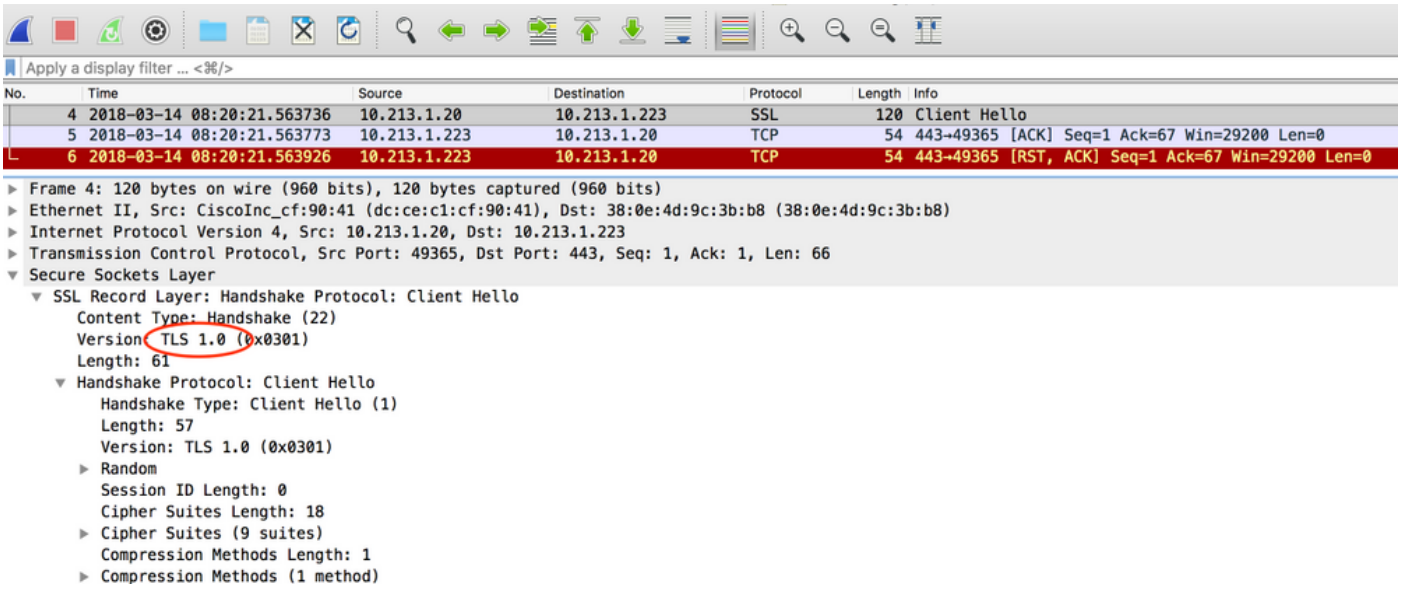
DNA Center restablece la conexión

Posible causa:

El Centro de DNA sólo admite TLS v1.2 de forma predeterminada.

Para solucionar esto, habilite DNA Center para utilizar TLS v1 después de esta guía

Captura de muestra



Comandos de depuración útiles en el agente PnP para problemas relacionados con certificados

- debug crypto pki Transactions
- debug ssl openssl

- debug ssl openssl errors
- debug ssl openssl errors
- debug crypto pki API
- debug crypto pki Transactions
- debug ssl openssl msg

Falta la respuesta de la clave de sesión autenticada previamente establecida

En teoría, no debería tener dispositivos no reclamados en la página Provisioning > Devices > Device Inventory (Aprovisionamiento > Dispositivos > Inventario de dispositivos), pero ha habido problemas en los que, después de eliminar los dispositivos no reclamados de esta página, los dispositivos todavía se mostraban en https://<DNA Center ip>/mypnp. Si encuentra este escenario y ve un registro similar al siguiente en los registros de PnP o una indicación de lo mismo en la GUI, asegúrese de que el dispositivo no aparece como no reclamado en 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
```

Gotchas de automatización y apilamiento de LAN

- En el centro de ADN 1.2, la pila debe estar llena (es posible que un cable de pila para una pila de 2 miembros no funcione).
- La automatización de la LAN debe reclamar rápidamente el dispositivo de pila, aproximadamente menos de 10 minutos.
- Una vez conectado al Centro de ADN aparece como No reclamado en PnP. PnP utiliza la ventana de tiempo de 10 minutos para determinar la pila y, una vez que caduque, permanecerá en la sección no reclamada de LAN Automation.

Si tiene los registros RCA o PnP, puede buscar mensajes de dispositivo no reclamados:

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

Si no hay mensajes, entonces las notificaciones de dispositivos no reclamados no llegan al DNA Center y PnP no puede reclamarlo.

Cómo realizar la automatización de LAN en una pila

1. Cierre los enlaces ascendentes a los dispositivos simientes.
2. Inicie la automatización de la LAN en el centro DNA.
3. Elimine la configuración de inicio de la pila. **# write erase**
4. Elimine todos los certificados de NVRAM. **# delete nvram:*.cer**
5. Quite el archivo vlan.dat. **# delete flash:vlan.dat**
6. En el switch principal, elimine los certificados en el switch en espera. **# delete stby-nvram:*.cer**

a. Desconecte los cables de la pila.

b. Inicie sesión en la consola de cada switch miembro.

c. Elimine los certificados. **# delete nvram:*.cer**

d. Elimine la base de datos de flas vlan. **# delete flash:vlan.dat**

e. Vuelva a conectar los cables de la pila.

7. Reiniciar.

8. Espere a que el switch se registre como stack, active todos los miembros e intente iniciar el diálogo de configuración inicial.

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


         --- System Configuration Dialog ---

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

9. Habilite los enlaces ascendentes a los dispositivos simientes. **# no shutdown**

¿Formato del archivo de mapa de nombres de host que puedo importar a mi tarea de automatización de LAN?

DNA Center espera un archivo CSV con el nombre de host y el número de serie (nombre de host,número de serie), como se muestra en el siguiente ejemplo:

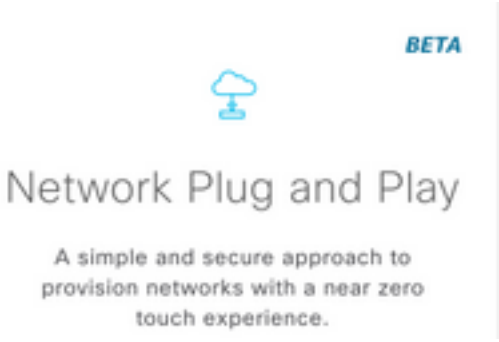
A	B
Edge1	FCW2048Cxxx
Edge2	FCW2131Lxxx, FCW2131Gxxx, FCW2131Gxxx, FCW2131Gxxx
Edge3	FOC2052Xxxx, FCW2052Cxxx, FCW2052Fxxx
Edge4	FXS2131Qxxx

Para la automatización de LAN de pila, el archivo CSV le permite introducir un nombre de host y varios números de serie por fila. Los números de serie deben estar separados por comas. Consulte el archivo CSV adjunto como referencia.

¿Adónde fue /mypnp en 1.2?

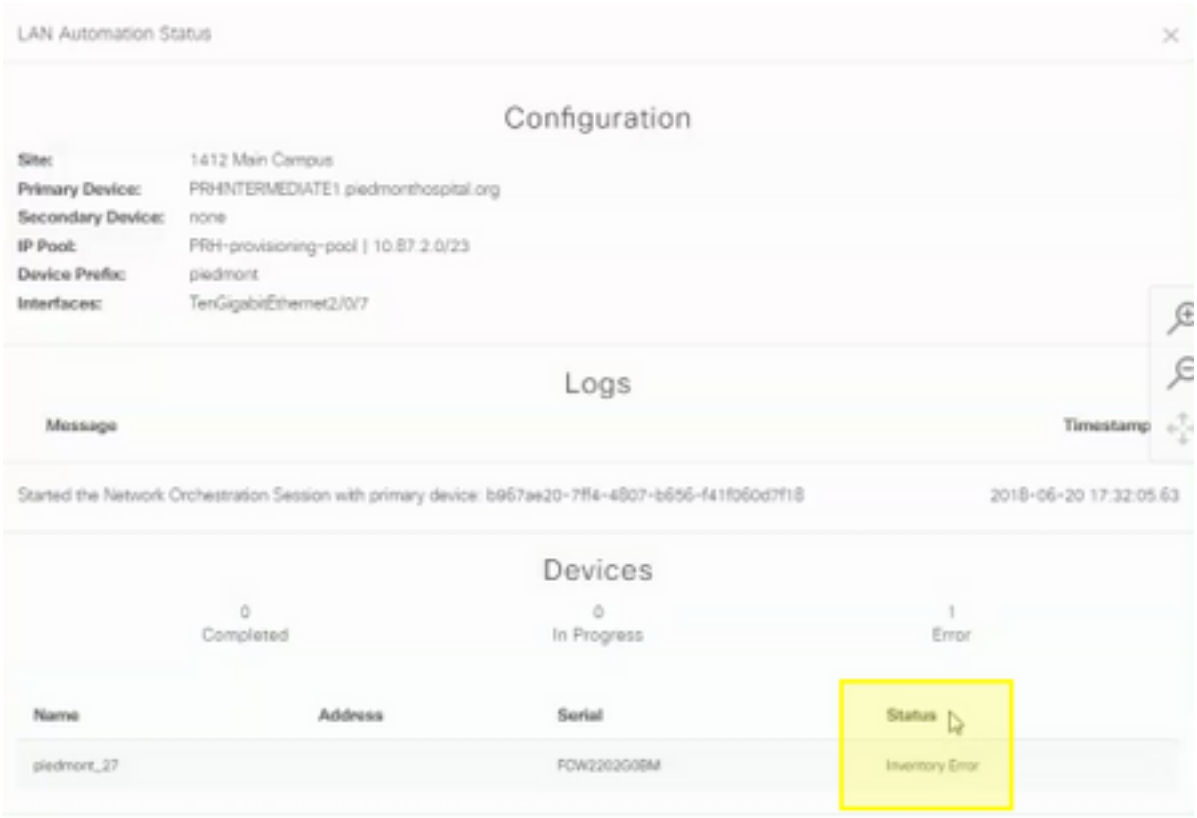
Acceda a PnP de una de las siguientes maneras:

- Desde su navegador web, introduzca https://<DNA Center IP>/networkpnp
- En la página de inicio de DNA Center, seleccione la siguiente herramienta Network Plug and Play:



O visitando https://<DNA Center IP>/networkpnp

Error de inventario



El error de inventario significa que el dispositivo, después de ser reclamado por la automatización de LAN y de recibir su configuración fallida, se debe agregar al inventario. Este error suele ocurrir debido a problemas de configuración, de enrutamiento o de credenciales de CLI.

Para verificar que está intentando activar el dispositivo correcto a través de LAN Automation, acceda de forma remota a la dirección IP de la interfaz de loopback 0 en el dispositivo mediante el protocolo de conexión preferido (SSH o Telnet).

La conectividad existe pero los certificados PKI no se envían correctamente a los agentes PnP

Hay ocasiones en las que los dispositivos en el medio pueden activar el bit *No fragmentar* (DF) de los paquetes entre DNAC y los agentes PnP. Esto puede hacer que los paquetes mayores de 1500 bytes, normalmente los paquetes que contienen el certificado, se descarten y, por lo tanto, es posible que la automatización de la LAN no se complete. Algunos de los registros comunes

que se ven en los registros de *onboarding* del DNA Center son:

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

La acción sugerida en este caso es asegurar que el trayecto entre el Centro de DNA y los Agentes PnP permita que las tramas jumbo pasen usando el comando **system mtu 9100**.

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