Dicas e truques de automação de LAN para o Digital Network Architecture (DNA) Center

Contents

Introduction

Este documento fornece uma visão geral da Automação de Rede Local (LAN) para ajudá-lo a diagnosticar problemas quando a Automação de LAN não funciona como esperado no Centro de Arquitetura de Rede Digital (DNA).

Contribuído por Alexandro Carrasquedo, engenheiro do TAC da Cisco.

Glossário

Agente Plug and Play (PnP):Novo dispositivo que você acabou de ligar sem configuração e sem certificados que serão automaticamente configurados pelo DNA Center.

Dispositivo semente: dispositivo que o DNA Center já provisionou e que atua como o servidor DHCP (Dynamic Host Configuration Protocol).

Prerequisites

Requisitos

A Cisco recomenda que você tenha um conhecimento geral da LAN Automation e da Solução Plug and Play. oferece uma visão geral da LAN Automation embora seja baseada no DNA Center 1.0, o mesmo conceito se aplica ao DNA Center 1.1 e superior.

Informações de Apoio

A automação de LAN é uma solução de implantação quase totalmente automatizada que permite configurar e provisionar seus dispositivos de rede com o uso do ISIS como o protocolo de roteamento básico.

Antes de Começar

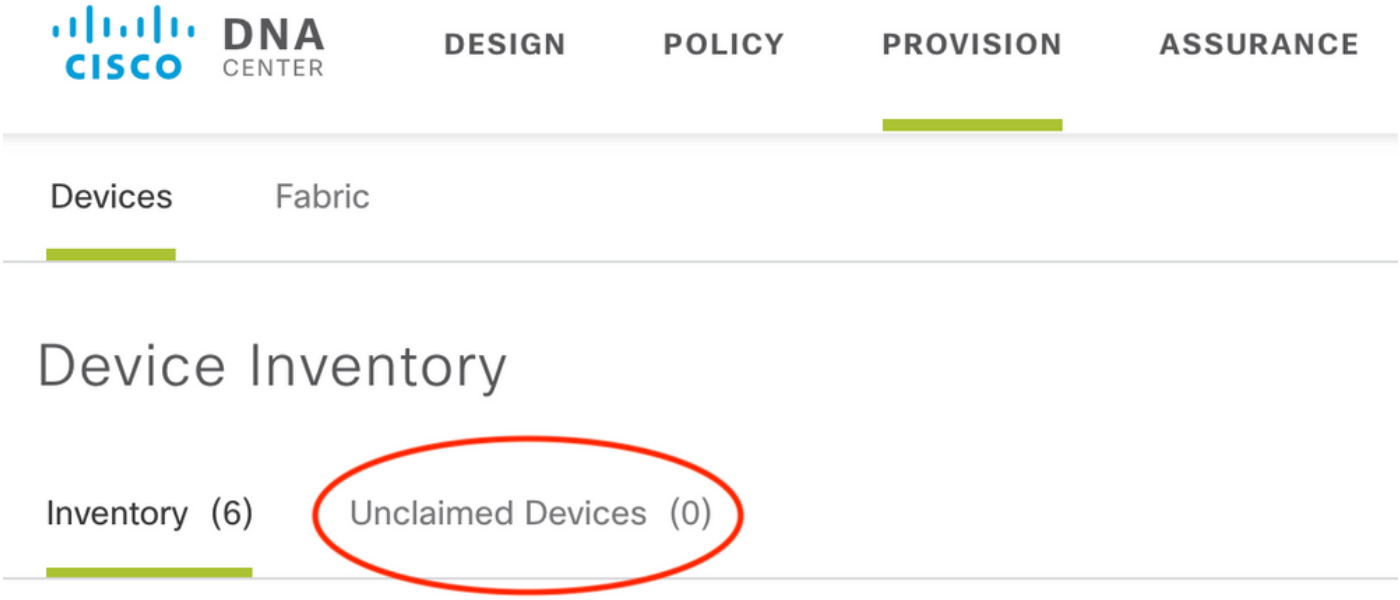
Antes de executar a automação de LAN, verifique se o seu agente PnP não tem nenhum certificado carregado na NVRAM.

```
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
```

Certifique-se de que não haja nenhum dispositivo não solicitado na página Provisioning > Devices > Device Inventory:



Por causa do CSCvh68847 , algumas pilhas podem não sair do estado não reivindicado e você pode receber uma mensagem de erro ERROR_STACK_UNSUPPORTED. Essa mensagem acontece quando a automação da LAN tenta reivindicar o provisionamento do dispositivo como se fosse um único switch. No entanto, como o dispositivo é uma pilha de switches Catalyst 9300, a automação de LAN não pode reivindicar o dispositivo e o dispositivo aparece como não reivindicado. Da mesma forma, o PnP não reivindica o dispositivo porque ele é uma pilha, portanto, o dispositivo não é provisionado.

Quais são as etapas pelas quais a automação da LAN passa enquanto ela é executada?

O DNA Center provisiona o dispositivo de seed com a configuração DHCP. O escopo dos endereços IP que o dispositivo de seed obtém é um segmento do pool inicial que você definiu quando reservou o pool de endereços IP para o seu site. Observe que esse pool deve ser pelo menos /25.

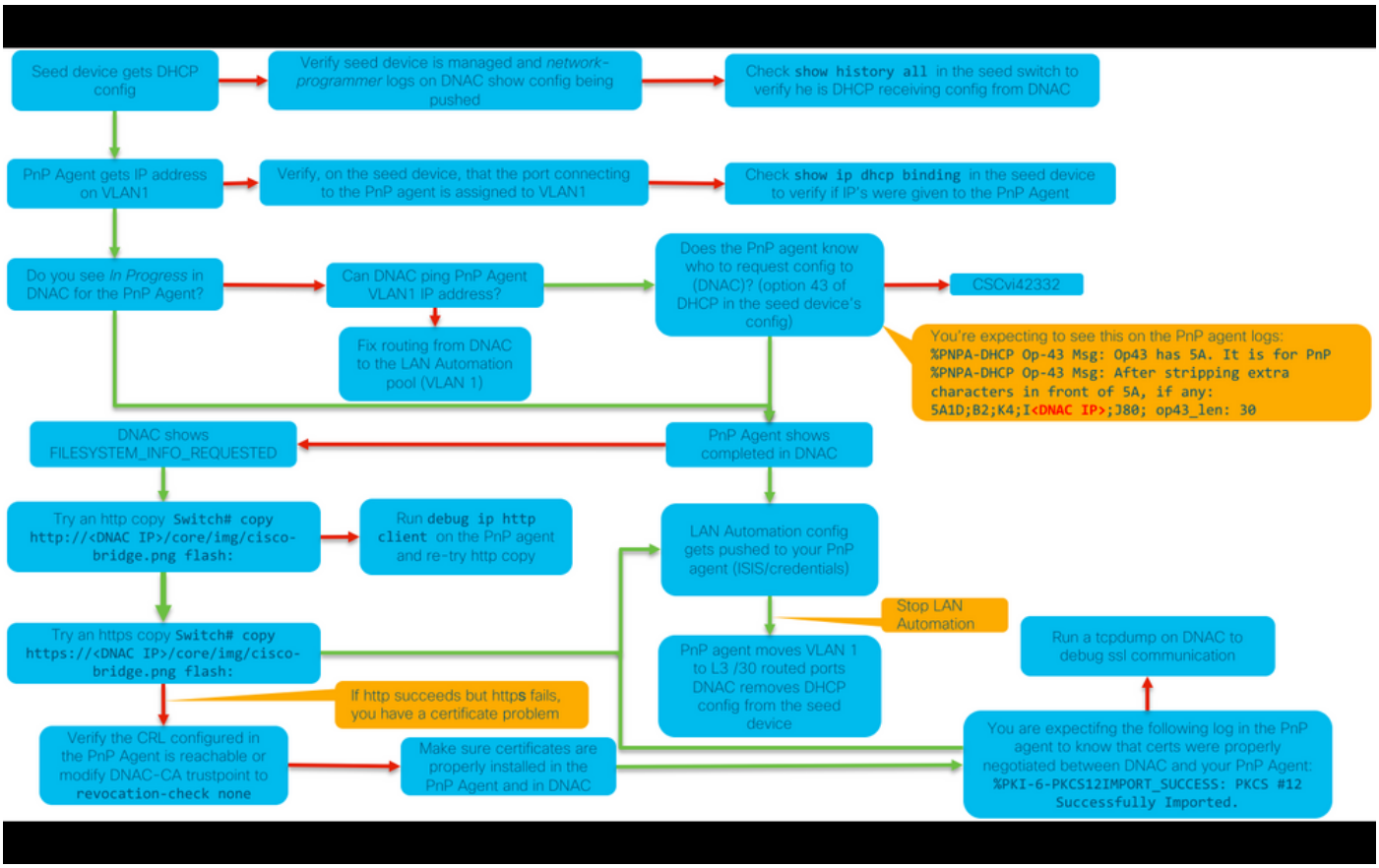
> **Note**: Esse pool é dividido em 3 segmentos:
> 1. Os endereços IP que são enviados para a VLAN 1 em seus agentes PnP.
> 2. Os endereços IP que são enviados para Loopbac0 em seus agentes PnP.
> 3. Os endereços IP /30 que são enviados aos agentes PnP no link que se conecta ao seu dispositivo de seed ou a outros dispositivos de estrutura.

Para que o DNA Center provisione seus agentes PnP, a configuração DHCP que o dispositivo de seed recebe deve ter a opção 43 definida com o endereço IP da placa de interface de rede (NIC) do DNA Center para empresa ou o endereço IP virtual (VIP), se você tiver um cluster de n nós.

Quando os agentes PnP inicializam, eles não têm configuração. Portanto, todas as portas fazem parte da VLAN 1. Consequentemente, os dispositivos enviam mensagens de descoberta de DHCP ao dispositivo de seed. O dispositivo de seed responde com uma oferta de endereços IP dentro do pool de automação de LAN.

Agora que você entende a sequência inicial da automação de LAN, é possível solucionar problemas do processo se ele não estiver funcionando conforme esperado.

Diagrama de solução de problemas



Logs relevantes da automação de LAN do DNA Center 1.1

- network-orquestration-service
- pnp-service

Logs relevantes da automação de LAN do DNA Center 1.2

Na versão 1.2, não há mais um pnp-service, portanto, você precisa procurar os seguintes serviços ao solucionar problemas de automação de LAN:

- orquestração de rede
- projeto de rede
- conexão-manager-service
- serviço de integração *(este é o antigo equivalente de serviço pnp de 1.1)*

Registros relevantes do DNA Center 1.x Public Key Infrastructure (PKI)

- apic-em-pki-broker-service
- apic-em-jchefe-ejbca

Como executar o tcpdump mostrado no fluxograma?

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

*Para parar isso, use CTRL+C

Isso armazena o arquivo pnp_capture.pcap em /data/tmp/. Você precisa copiar o arquivo do DNA Center usando o comando secure copy (SCP) ou ler o arquivo do DNA Center usando o seguinte 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
```

Qual é o arquivo bridge.png que você está tentando copiar?

Éum arquivo de imagem de 191 bytes localizado no DNA Center que você deseja copiar usando HTTP (sem usar certificados) ou HTTPS (usando certificados) para testar a comunicação entre o DNA Center e seu PnP Agent.

Exemplos de capturas quando a comunicação SSL (Secure Sockets Layer) não está funcionando conforme o esperado (arquivos .pcap completos anexados a este artigo)

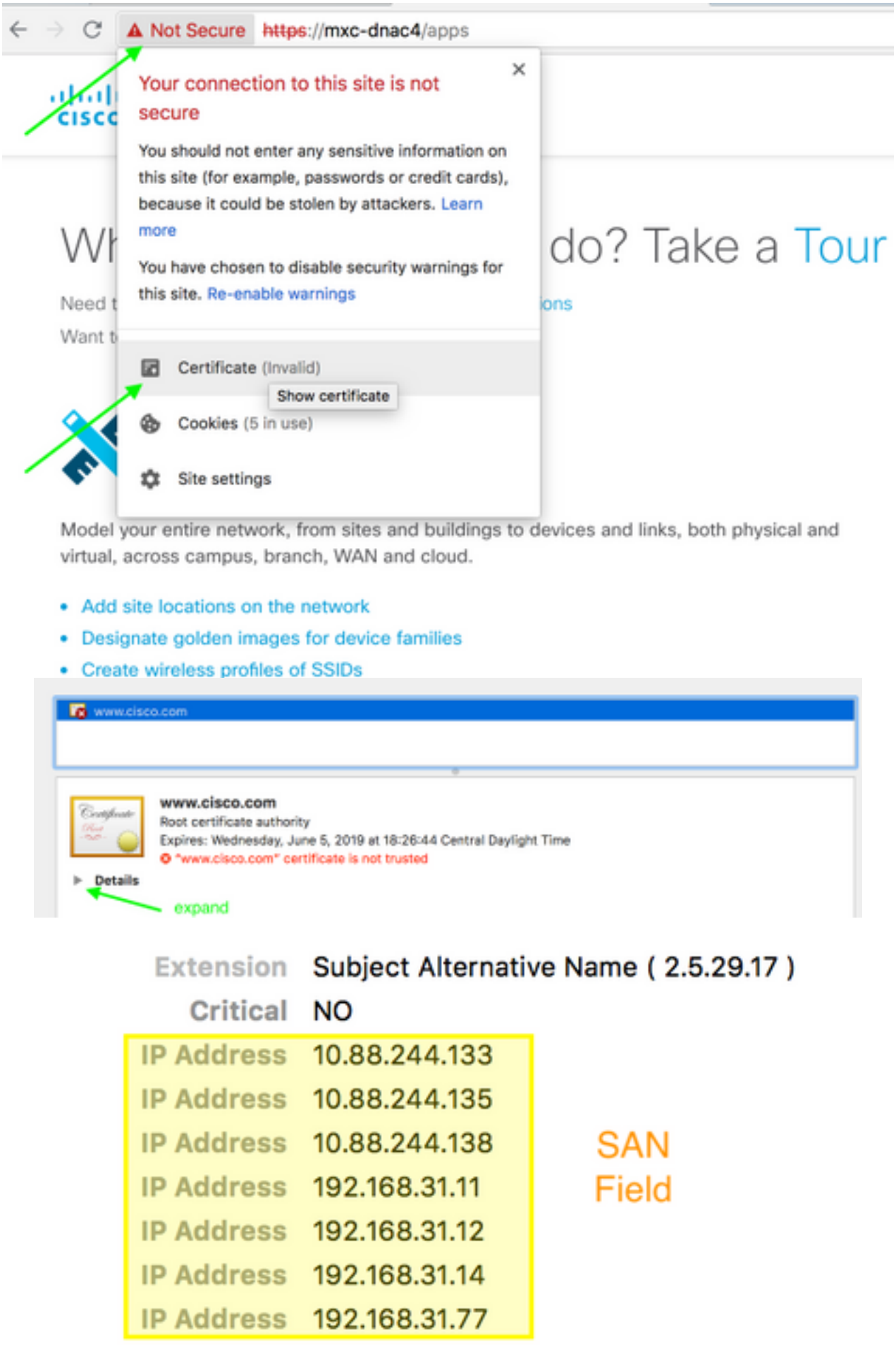
Certificado inválido

Possível causa:

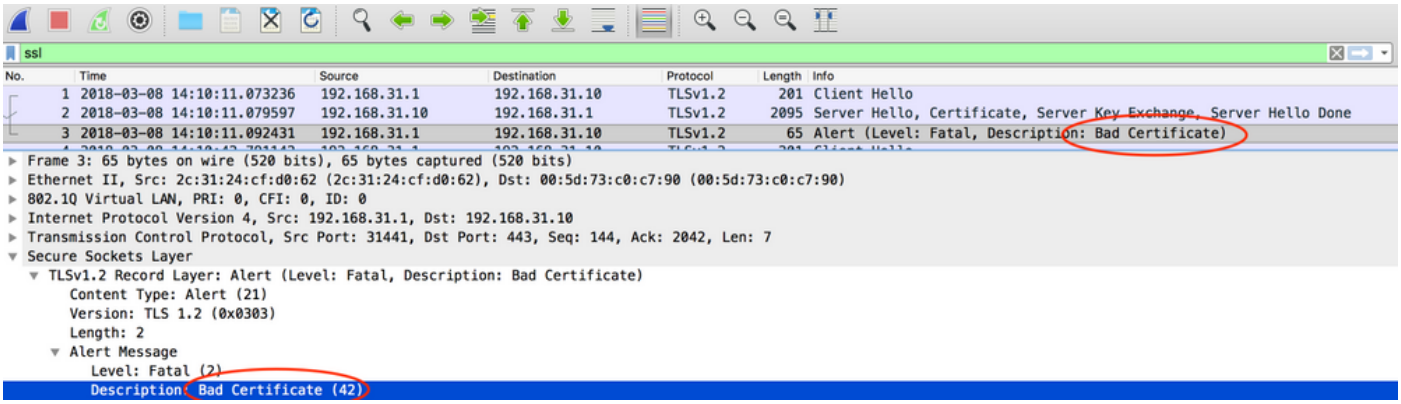
- O certificado do DNA Center não tem o endereço IP correto no campo Nome alternativo do assunto (SAN).

Para verificar os campos de SAN no certificado, você pode fazer o seguinte:

Verificar o certificado usando um navegador



Captura de amostra



Resolução.

Se você tiver uma CA de terceiros (autoridade de certificação), certifique-se de que ela forneça um certificado com os endereços IP do DNA Center e o VIP nele. Se você não tiver uma CA de terceiros, o DNA Center pode gerar um certificado para você. Entre em contato com o Cisco TAC para orientá-lo nesse processo.

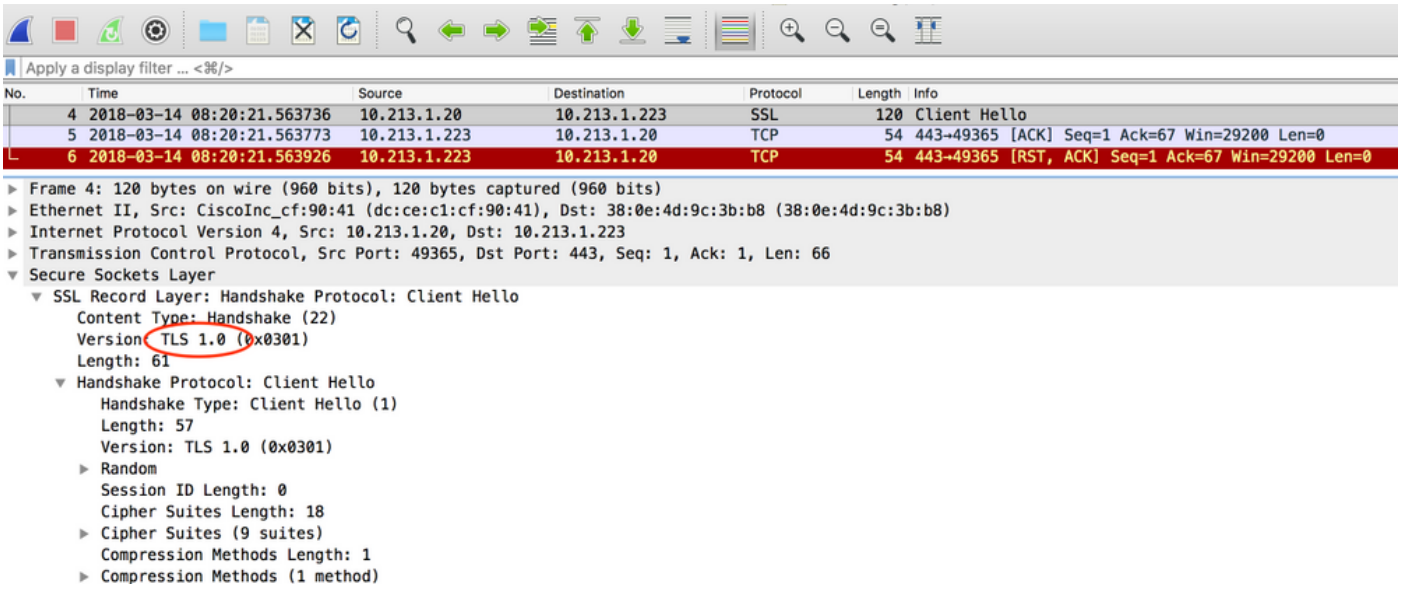
O DNA Center redefine a conexão

Possível causa:

Por padrão, o DNA Center suporta apenas TLS v1.2.

Para contornar isso, habilite o DNA Center a usar TLS v1 após este guia

Captura de amostra



Comandos de depuração úteis no PnP Agent para problemas relacionados ao certificado

- 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

A resposta está faltando na chave de sessão autenticada estabelecida anteriormente

Teoricamente, você não deve ter dispositivos não reivindicados na página Provisioning > Devices > Device Inventory, mas houve problemas em que, após excluir os dispositivos não reivindicados desta página, os dispositivos ainda estavam sendo exibidos em https://<DNA Center ip>/mypnp. Se você encontrar esse cenário e vir um log semelhante ao seguinte nos registros PnP ou uma indicação do mesmo na GUI, verifique se o dispositivo não aparece como não reivindicado no 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
```

Conseguir automação e empilhamento de LANs

- No DNA Center 1.2, a pilha precisa ser um anel completo (um cabo de pilha para uma pilha de 2 membros pode não funcionar).
- O dispositivo de pilha precisa ser reivindicado imediatamente pela automação da LAN, aproximadamente menos de 10 minutos.
- Depois de conectado ao DNA Center, ele aparece como Não reivindicado no PnP. O PnP usa a janela de tempo de 10 minutos para a determinação da pilha e, uma vez expirado, permanecerá na seção não reivindicada da automação da LAN.

Se você tiver os registros RCA ou PnP, poderá procurar mensagens de dispositivo não reivindicadas:

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

Se não houver mensagens, as notificações de dispositivos não reivindicados não estarão chegando ao DNA Center e o PnP não poderá reivindicar.

Como fazer a automação de LAN em uma pilha

1. Desligue os uplinks no(s) dispositivo(s) de semente.
2. Inicie a automação da LAN no DNA Center.
3. Exclua a configuração de inicialização da pilha. **# write erase**
4. Remova todos os certificados da NVRAM. **# excluir nvram:*.cer**
5. Remova o arquivo vlan.dat. **# delete flash:vlan.dat**
6. No switch primário, exclua os certificados no switch de standby. **# delete stby-nvram:*.cer**

a. Desconecte os cabos da pilha.

b. Efetue login no console de cada switch membro.

c. Exclua os certificados. **# excluir nvram:*.cer**

d. Exclua o banco de dados flas vlan. **# delete flash:vlan.dat**

e. Reconecte os cabos da pilha.

7. Reinicialização.

8. Aguarde o switch se registrar como pilha, ative todos os membros e tente iniciar o diálogo de configuração 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. Ative os uplinks para o(s) dispositivo(s) de semente. **# no shutdown**

Formato do arquivo do mapa do nome do host que posso importar para minha tarefa de LAN Automation?

O DNA Center espera um arquivo CSV com o nome do host e o número de série (nome do host, número de série) conforme mostrado no exemplo a seguir:

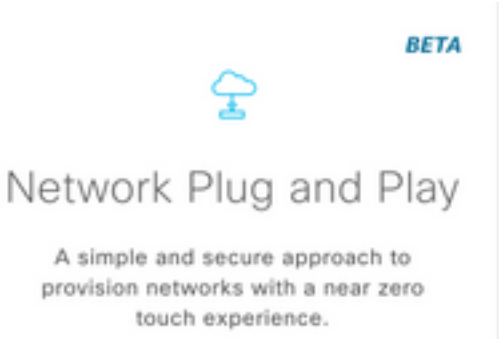
A	B
Edge1	FCW2048Cxxx
Edge2	FCW2131Lxxx, FCW2131Gxxx, FCW2131Gxxx, FCW2131Gxxx
Edge3	FOC2052Xxxx, FCW2052Cxxx, FCW2052Fxxx
Edge4	FXS2131Qxxx

Para a automação da LAN da pilha, o arquivo CSV permite inserir um nome de host e vários números de série por linha. Os números de série precisam ser separados por vírgulas. Consulte o arquivo CSV anexado para referência.

Onde /mypnp foi no 1.2?

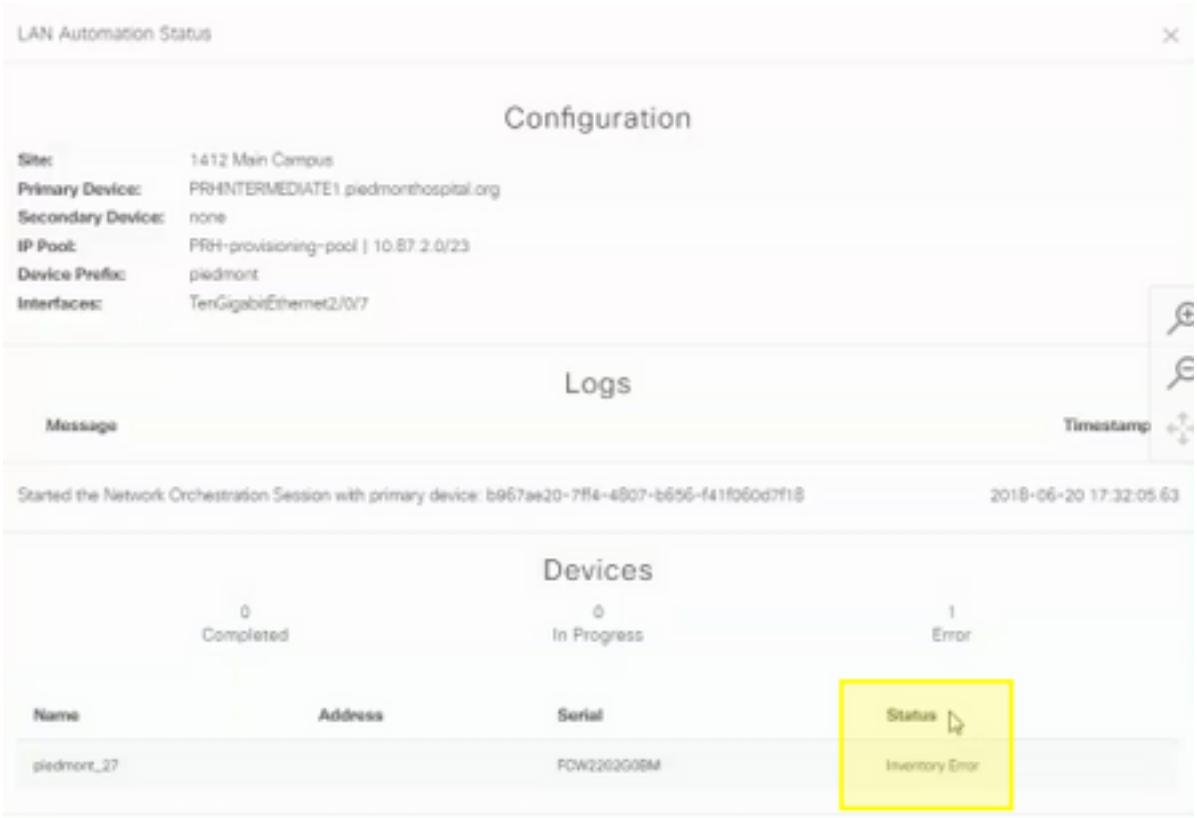
Acesse PnP de uma das seguintes maneiras:

- No navegador da Web, digite https://<DNA Center IP>/networkpnp
- Na página inicial do DNA Center, selecione a seguinte ferramenta Network Plug and Play:



Ou acesse https://<DNA Center IP>/networkpnp

Erro de inventário



O erro de inventário significa que o dispositivo, depois de ser reivindicado pela automação de LAN e receber sua configuração falhou, deve ser adicionado ao inventário. Esse erro geralmente ocorre devido a problemas de configuração, roteamento ou credenciais CLI.

Para verificar se você está tentando ativar o dispositivo correto por meio da LAN Automation, acesse remotamente o endereço IP da interface de loopback 0 no dispositivo usando o protocolo de conexão preferencial (SSH ou Telnet).

A conectividade existe, mas os certificados PKI não são enviados com êxito aos Agentes PnP

Há momentos em que os dispositivos no meio podem ligar o bit *Não Fragmentar*(DF) dos pacotes entre o DNAC e os Agentes PnP. Isso pode fazer com que os pacotes maiores que 1500 bytes, geralmente os pacotes que contêm o certificado, sejam descartados e, portanto, a automação da LAN pode não ser concluída. Alguns dos registros comuns vistos nos registros *de integração* do

DNA Center são:

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

A ação sugerida neste caso é garantir que o caminho entre o DNA Center e os PnP Agents permita que frames grandes passem usando o **sistema** de comando **mtu 9100**.

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