DNA(Digital Network Architecture) 센터를 위한 LAN 자동화 팁 및 요령

목차

소개

이 문서에서는 LAN 자동화가 DNA(Digital Network Architecture) Center에서 예상한 대로 작동하지 않을 경우 문제를 진단하는 데 도움이 되는 LAN 자동화에 대한 개요를 제공합니다.

기고자: Alexandro Carrasquedo, Cisco TAC 엔지니어

글로리

PnP(Plug and Play) Agent: 컨피그레이션 없이 전원을 켜고 DNA Center에서 자동으로 구성할 인증서가 없는 새 디바이스입니다.

시드 디바이스: DNA Center가 이미 프로비저닝되었고 DHCP(Dynamic Host Configuration Protocol) 서버 역할을 하는 디바이스.

사전 요구 사항

요구 사항

Cisco는 LAN 자동화 및 플러그 앤 플레이 솔루션에 대한 일반적인 지식을 보유하고 있는 것이 좋습니다.은(는) DNA Center 1.0을 기반으로 하지만 LAN 자동화에 대한 개요를 제공합니다. DNA Center 1.1 이상에도 동일한 개념이 적용됩니다.

배경 정보

LAN 자동화는 ISIS를 언더레이 라우팅 프로토콜로 사용하여 네트워크 디바이스를 구성하고 프로비저닝할 수 있는 제로 터치 구축 솔루션입니다.

시작하기 전에

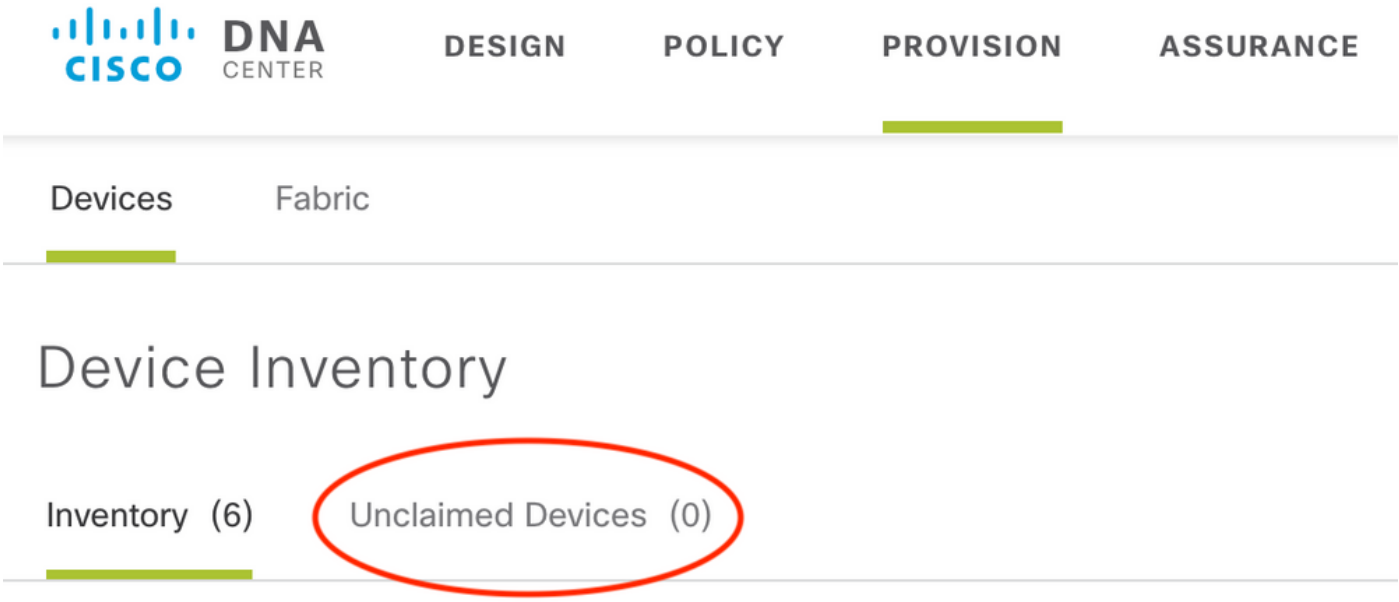
LAN 자동화를 실행하기 전에 PnP 에이전트에 NVRAM에 로드된 인증서가 없는지 확인하십시오.

```
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
```

Provisioning(프로비저닝) > Devices(디바이스) > Device Inventory(디바이스 인벤토리) 페이지에 클레임되지 않은 디바이스가 없는지 확인합니다.



CSCvh68847 때문 일부 스택은 클레임되지 않은 상태를 벗어나지 못할 수 있으며 ERROR_STACK_UNSUPPORTED 오류 메시지가 표시될 수 있습니다.이 메시지는 LAN 자동화가 디바이스를 마치 단일 스위치인 것처럼 프로비저닝하도록 요청할 때 발생합니다.그러나 디바이스는 Catalyst 9300 스위치 스택이므로 LAN 자동화는 디바이스를 클레임할 수 없으며 디바이스는 클레임되지 않은 상태로 표시됩니다.마찬가지로, PnP는 스택이므로 디바이스를 클레임하지 않으므로 디바이스가 프로비저닝되지 않습니다.

LAN 자동화가 실행되는 동안 수행되는 단계는 무엇입니까?

DNA Center는 시드 디바이스를 DHCP 구성으로 프로비저닝합니다.시드 디바이스가 가져오는 IP 주소의 범위는 사이트에 대한 IP 주소 풀을 예약할 때 정의한 초기 풀의 세그먼트입니다.이 풀은 적어도 /25여야 합니다.

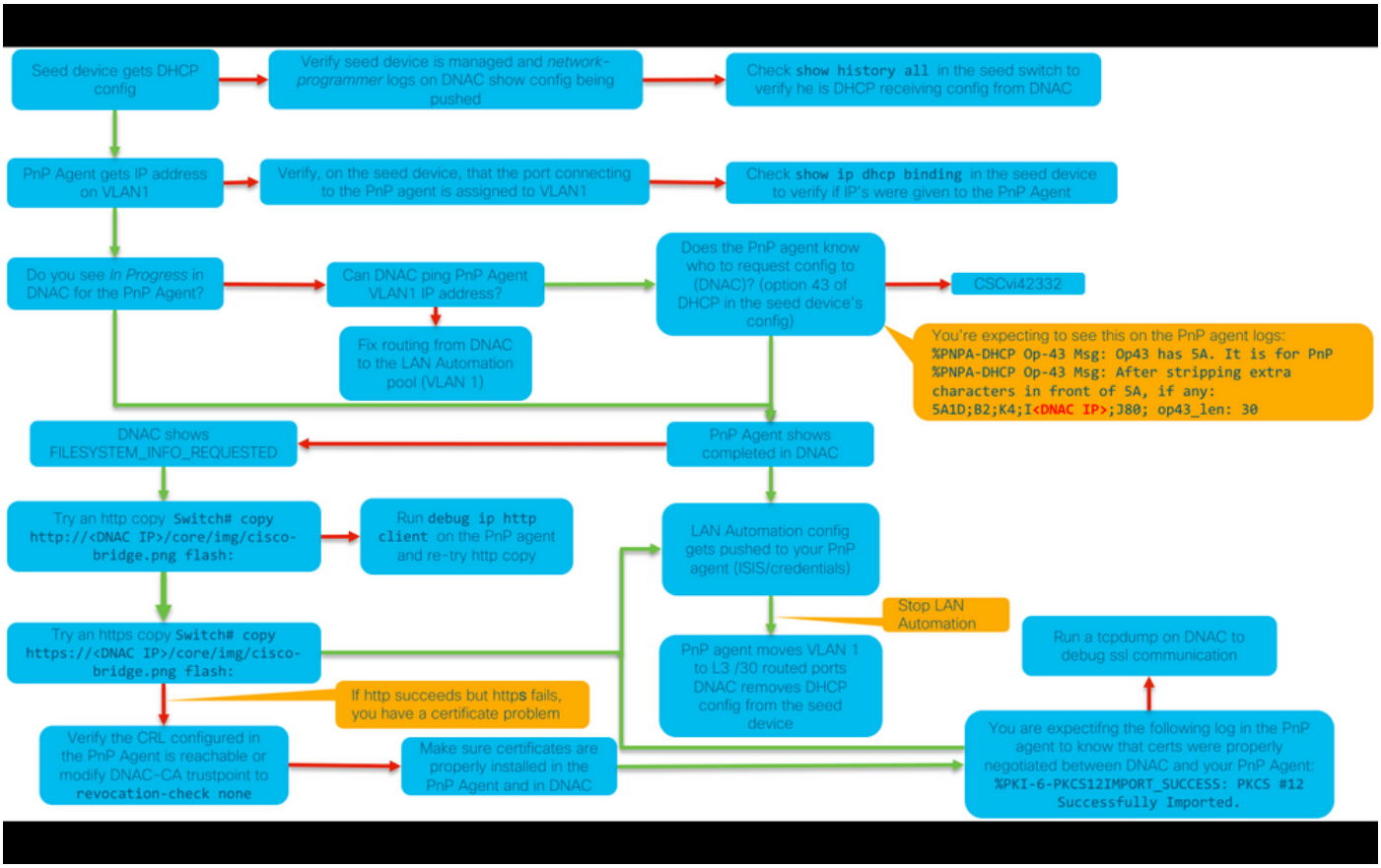
참고:이 풀은 3개의 세그먼트로 구분됩니다.
1. PnP 에이전트의 VLAN 1에 푸시되는 IP 주소.
2. PnP 에이전트의 Loopbac0으로 푸시되는 IP 주소.
3. 시드 또는 다른 패브릭 장치에 연결되는 링크에서 PnP 에이전트로 푸시되는 /30 IP 주소

DNA Center에서 PnP 에이전트를 프로비저닝하려면 시드 디바이스에서 수신하는 DHCP 컨피그레이션에 n 노드 클러스터가 있는 경우 DNA 센터 NIC(Enterprise-Facing Network Interface Card) 또는 VIP(Virtual IP) 주소의 IP 주소로 옵션 43이 정의되어 있어야 합니다.

PnP 에이전트가 부팅되면 컨피그레이션이 없습니다.따라서 모든 포트가 VLAN 1의 일부입니다. 따라서 디바이스는 DHCP 검색 메시지를 시드 디바이스로 전송합니다.시드 디바이스는 LAN 자동화 풀 내의 IP 주소를 제공하여 응답합니다.

이제 LAN 자동화의 초기 시퀀스를 이해했으므로 프로세스가 예상대로 작동하지 않으면 문제를 해결할 수 있습니다.

문제 해결 다이어그램



DNA Center 1.1 LAN Automation 관련 로그

- 네트워크 오케스트레이션 서비스
- pnp 서비스

DNA Center 1.2 LAN Automation 관련 로그

릴리스 1.2에는 더 이상 pnp 서비스가 없으므로 LAN 자동화를 트러블슈팅할 때 다음 서비스를 찾아야 합니다.

- 네트워크 오케스트레이션
- 네트워크 설계
- 연결-관리자 서비스
- onboarding-service*(1.1과 동일한 이전 pnp-service)*

DNA Center 1.x PKI(Public Key Infrastructure) 관련 로그

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

순서도에 표시된 tcpdump를 실행하는 방법

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

*이 작업을 중지하려면 Ctrl+C를 사용하십시오.

이렇게 하면 pnp_capture.pcap 파일이 /data/tmp/에 저장됩니다.SCP(secure copy) 명령을 사용하여 DNA 센터에서 파일을 복사하거나 다음 명령을 사용하여 DNA 센터에서 파일을 읽어야 합니다.

```
$ 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
```

복사하려는 bridge.png 파일

DNA Center에 있는 191바이트 이미지 파일로서 인증서를 사용하지 않고 HTTP(인증서 사용) 또는 HTTPS(인증서 사용)를 사용하여 DNA Center와 PnP 에이전트 간의 통신을 테스트하려는 경우

SSL(Secure Sockets Layer) 통신이 예상대로 작동하지 않을 경우 샘플 캡처(이 문서에 첨부된 전체 .pcap 파일)

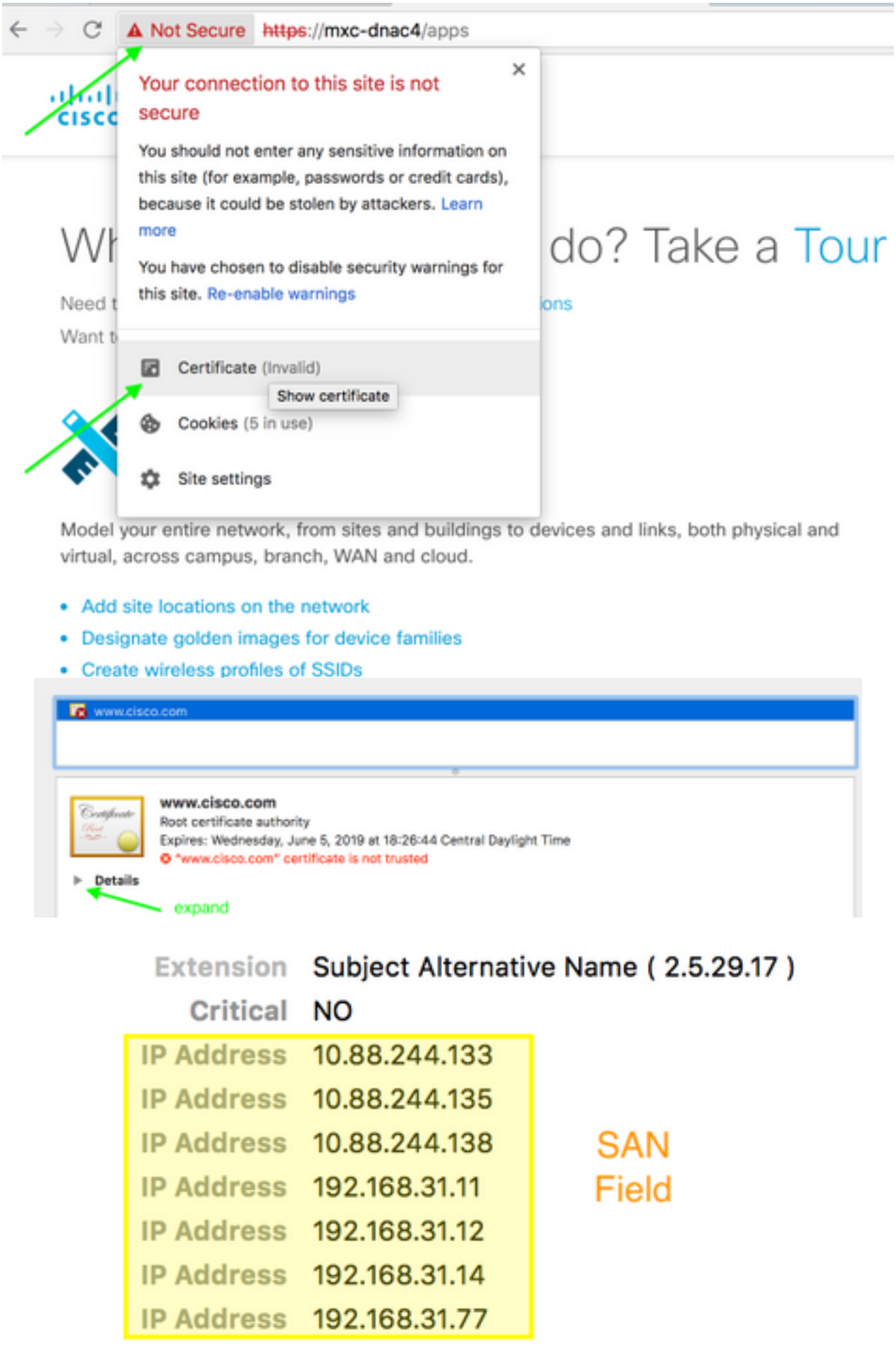
잘못된 인증서

가능한 원인:

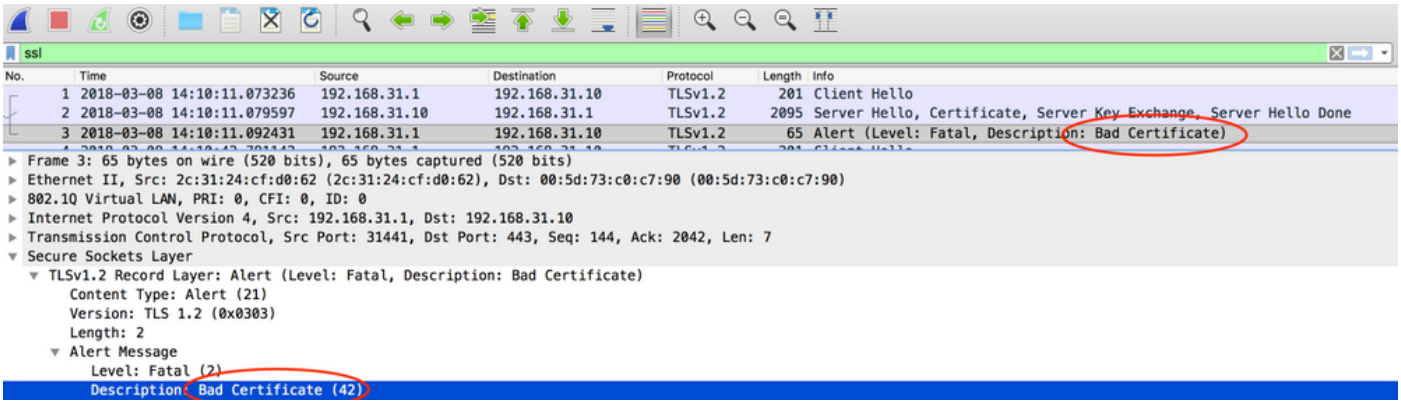
- DNA Center의 인증서에 SAN(Subject Alternative Name) 필드에 올바른 IP 주소가 없습니다.

인증서의 SAN 필드를 확인하려면 다음을 수행할 수 있습니다.

브라우저를 사용하여 인증서 확인


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

샘플 캡처



해결.

서드파티 CA(Certificate Authority)가 있는 경우 DNA Center의 IP 주소와 VIP가 포함된 인증서를 제공해야 합니다.서드파티 CA가 없는 경우 DNA Center에서 인증서를 생성할 수 있습니다.이 프로세스를 안내하려면 Cisco TAC에 문의하십시오.

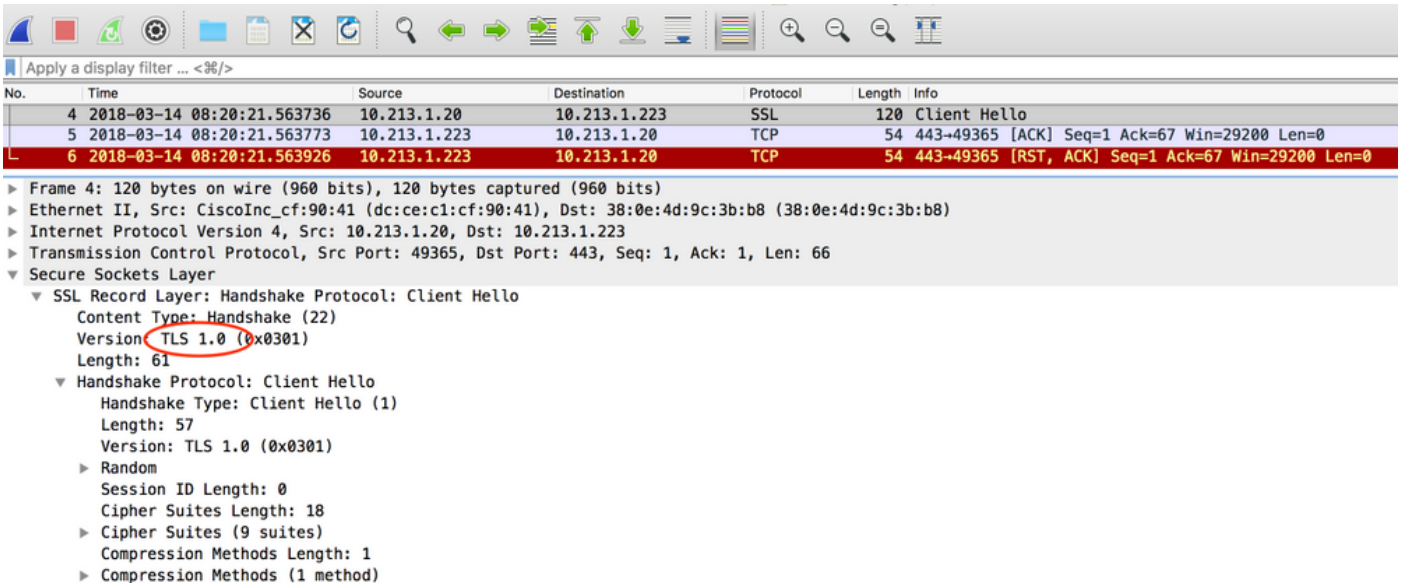
DNA Center로 연결 재설정

가능한 원인:

DNA Center는 기본적으로 TLS v1.2만 지원합니다.

이를 해결하려면 이 가이드에 따라 DNA Center에서 TLS v1을 사용하도록 설정하십시오.

샘플 캡처



인증서 관련 문제에 대한 PnP 에이전트의 유용한 디버그 명령

- 디버그 암호화 pki 트랜잭션
- 디버그 ssl openssl
- 디버그 ssl openssl error
- ssl openssl 오류 디버그

- debug crypto pki API
- 디버그 암호화 pki 트랜잭션
- ssl openssl 메시지 디버그

이전에 설정된 인증된 세션 키가 응답이 없습니다.

이론적으로, Provisioning(프로비저닝) > Devices(디바이스) > Device Inventory(디바이스 인벤토리) 페이지에 클레임되지 않은 디바이스가 없어야 하지만, 이 페이지에서 클레임되지 않은 디바이스를 삭제한 후에도 디바이스가 여전히 https://<DNA Center ip>/mypnp에 표시되는 문제가 있었습니다 .이 시나리오가 발생하여 PnP 로그에서 다음과 유사한 로그 또는 GUI에서 동일하다는 표시가 나타나면 디바이스가 PnP에서 클레임되지 않은 것으로 표시되지 않는지 확인합니다.

```
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 자동화 및 스태킹의 중요

- DNA Center 1.2에서는 스택이 풀 링이어야 합니다(2멤버 스택의 스택 케이블 하나가 작동하지 않을 수 있음).
- LAN 자동화를 통해 신속하게 스택 디바이스를 요청해야 하며, 이는 약 10분 미만입니다.
- DNA Center에 연결되면 PnP에서 Unclaimed로 표시됩니다. PnP는 스택 확인을 위해 10분 시간 창을 사용하며, 만료되면 LAN 자동화의 클레임되지 않은 섹션에 유지됩니다.

RCA 또는 PnP 로그가 있는 경우 클레임되지 않은 디바이스 메시지를 찾을 수 있습니다.

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

메시지가 없는 경우 클레임되지 않은 디바이스 알림이 DNA 센터에 도달하지 않으며 PnP는 이를 청구할 수 없습니다.

스택에서 LAN 자동화를 수행하는 방법

1. 시드 디바이스에 대한 업링크를 종료합니다.
2. DNA 센터에서 LAN 자동화를 시작합니다.
3. 스택에서 시작 컨피그레이션을 삭제합니다.**# 쓰기 지우기**
4. NVRAM에서 모든 인증서를 제거합니다. **# nvram 삭제:*.cer**
5. vlan.dat 파일을 제거합니다.**플래시:vlan.dat 삭제**
6. Primary 스위치에서 스탠바이 스위치의 인증서를 삭제합니다.**# stby nvram 삭제:*.cer**

a.스택 케이블을 분리합니다.

b.각 멤버 스위치의 콘솔에 로그인합니다.

c. 인증서를 삭제합니다. **# nvram 삭제:*.cer**

d.flas vlan 데이터베이스를 삭제합니다.**플래시:vlan.dat 삭제**

e.스택 케이블을 다시 연결합니다.

7. 재부팅

8. 스위치가 스택으로 등록될 때까지 기다린 후 모든 구성원을 불러온 다음 초기 구성 대화 상자를 시작하십시오.

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


         --- System Configuration Dialog ---

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

9. 시드 디바이스에 대한 업링크를 활성화합니다. **# 종료 안 함**

LAN Automation 작업으로 가져올 수 있는 호스트 이름 맵 파일의 형식

DNA Center에서는 다음 예와 같이 호스트 이름 및 일련 번호(호스트 이름, 일련 번호)가 있는 CSV 파일이 필요합니다.

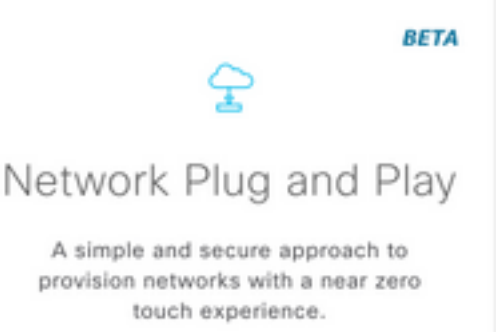
A	B
Edge1	FCW2048Cxxx
Edge2	FCW2131Lxxx, FCW2131Gxxx, FCW2131Gxxx, FCW2131Gxxx
Edge3	FOC2052Xxxx, FCW2052Cxxx, FCW2052Fxxx
Edge4	FXS2131Qxxx

스택 LAN 자동화의 경우 CSV 파일을 사용하여 한 행에 하나의 호스트 이름과 여러 개의 일련 번호를 입력할 수 있습니다.일련 번호는 쉼표로 구분해야 합니다.자세한 내용은 첨부된 CSV 파일을 참조하십시오.

/mypnp는 1.2에서 어디로 갔습니까?

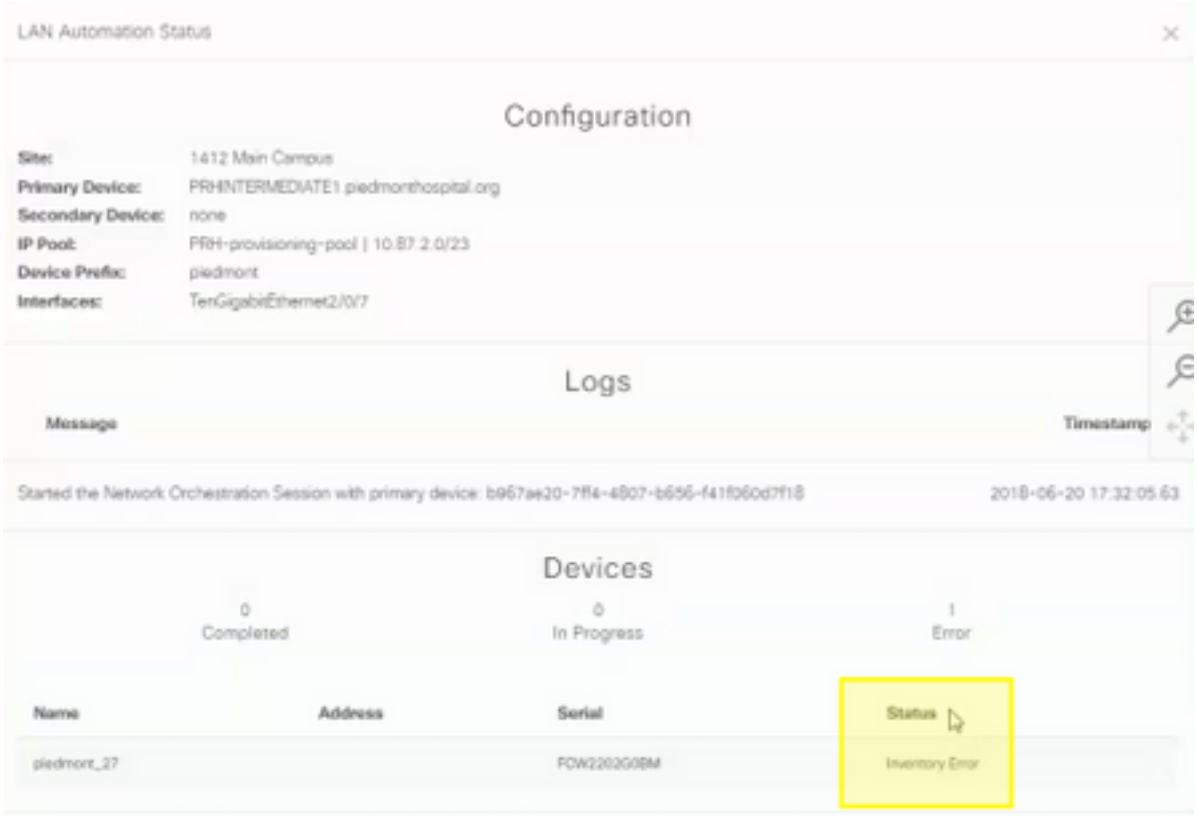
다음 방법 중 하나로 PnP에 액세스합니다.

- 웹 브라우저에서 https://<DNA Center IP>/networkpnp를 입력합니다.
- DNA Center 홈 페이지에서 다음 Network Plug and Play 툴을 선택합니다.



또는 https://<DNA Center IP>/networkpnp로 이동하여

인벤토리 오류



인벤토리 오류는 LAN 자동화에 의해 요청되고 컨피그레이션을 수신한 후 디바이스가 인벤토리에 추가되었음을 의미합니다.이 오류는 일반적으로 컨피그레이션, 일부 라우팅 또는 CLI 자격 증명 문제로 인해 발생합니다.

LAN Automation을 통해 올바른 디바이스를 설정하려는 경우 기본 연결 프로토콜(SSH 또는 텔넷)을 사용하여 디바이스에서 루프백 0 인터페이스의 IP 주소에 원격으로 액세스합니다.

연결이 있지만 PKI 인증서가 PnP 에이전트에 성공적으로 푸시되지 않았습니다.

중간에 있는 디바이스가 DNAC와 PnP 에이전트 간 패킷의 *Do Not Fragment*(DF) 비트를 켜는 경우도 있습니다.이로 인해 1500바이트보다 큰 패킷(일반적으로 인증서를 포함하는 패킷)이 삭제되므로 LAN 자동화가 완료되지 않을 수 있습니다.DNA Center의 *온보딩* 로그에 표시되는 일반적인 로그 중 일부는 다음과 같습니다.

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

이 경우 DNA Center와 PnP 에이전트 간의 경로가 명령 **시스템 mtu 9100**을 사용하여 점보 프레임을 통과하도록 허용하는지 확인하는 것이 좋습니다.

Switch(config)# **시스템 mtu 9100**