# Suggerimenti e suggerimenti per l'automazione LAN per il centro DNA (Digital Network Architecture)

## Sommario



## Introduzione

Questo documento offre una panoramica dell'automazione LAN (Local Area Network) per aiutare

l'utente a diagnosticare i problemi quando l'automazione LAN non funziona come previsto in Digital Network Architecture (DNA) Center.

Contributo di Alexandro Carrasquedo, Cisco TAC Engineer.

# Glossario

Agente Plug and Play (PnP): nuovo dispositivo appena acceso, senza configurazione e senza certificati che verranno automaticamente configurati da DNA Center.

Dispositivo di inizializzazione: dispositivo di cui DNA Center ha già eseguito il provisioning e che funge da server DHCP (Dynamic Host Configuration Protocol).

# Prerequisiti

## Requisiti

Cisco raccomanda una conoscenza generale dell'automazione LAN e della soluzione Plug and Play. fornisce una panoramica dell'automazione LAN, sebbene sia basata su DNA Center 1.0, lo stesso concetto si applica a DNA Center 1.1 e versioni successive.

# Premesse

L'automazione LAN è una soluzione di implementazione quasi zero-touch che consente di configurare i dispositivi di rete e di effettuarne il provisioning utilizzando ISIS come protocollo di routing sottostante.

# Operazioni preliminari

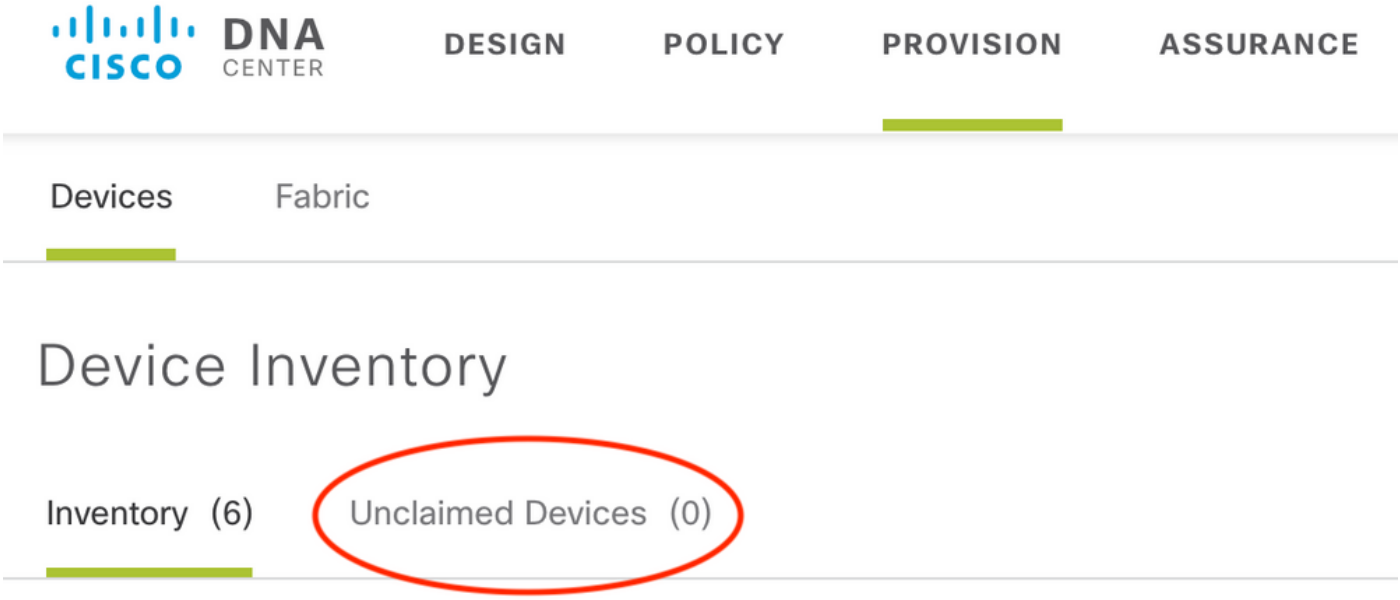
Prima di eseguire l'automazione LAN, verificare che l'agente PnP non abbia certificati caricati nella NVRAM.

```
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
```

Verificare che non vi siano dispositivi non richiesti nella pagina Provisioning > Dispositivi > Inventario dispositivi:




A causa di CSCvh68847 , alcuni stack potrebbero non lasciare lo stato non richiesto e potrebbe essere visualizzato un messaggio di errore ERROR_STACK_UNSUPPORTED. Questo messaggio viene visualizzato quando l'automazione LAN tenta di richiedere al dispositivo di eseguire il provisioning come se si trattasse di un singolo switch. Tuttavia, poiché il dispositivo è uno stack di switch Catalyst 9300, l'automazione LAN non può richiedere il dispositivo e il dispositivo viene visualizzato come non richiesto. Analogamente, il protocollo PnP non rivendica il dispositivo perché è uno stack, quindi il dispositivo non è sottoposto a provisioning.

## Quali sono i passaggi dell'automazione LAN durante l'esecuzione?

DNA Center fornisce al dispositivo di origine la configurazione DHCP. L'ambito degli indirizzi IP ottenuti dal dispositivo di inizializzazione è un segmento del pool iniziale definito al momento della prenotazione del pool di indirizzi IP per il sito. Il pool deve essere almeno /25.

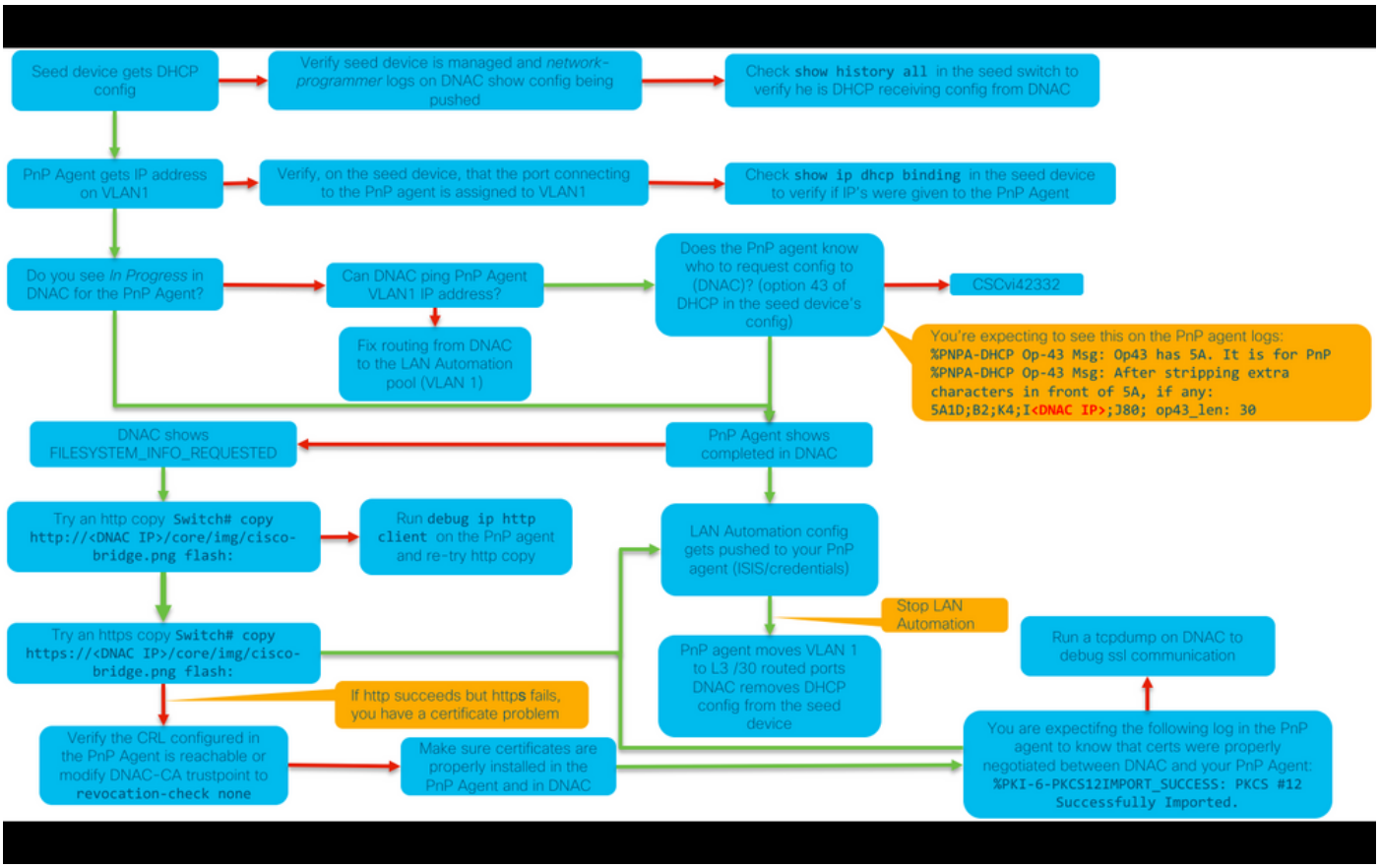
> **Nota:** Questo pool è diviso in 3 segmenti:
> 1. Gli indirizzi IP trasferiti sulla VLAN 1 sugli agenti PnP.
> 2. Gli indirizzi IP inseriti in Loopbac0 sugli agenti PnP.
> 3. Gli indirizzi IP /30 che vengono inviati agli agenti PnP sul collegamento che si connette al seed o ad altri dispositivi fabric.

Affinché DNA Center esegua il provisioning degli agenti PnP, la configurazione DHCP ricevuta dal dispositivo di inizializzazione deve avere l'opzione 43 definita con l'indirizzo IP della scheda di interfaccia di rete (NIC) aziendale di DNA Center o l'indirizzo IP virtuale (VIP), se si dispone di un cluster a n nodi.

All'avvio, gli agenti PnP non dispongono di alcuna configurazione. Pertanto, tutte le loro porte fanno parte della VLAN 1. Di conseguenza, i dispositivi inviano messaggi di individuazione DHCP al dispositivo di inizializzazione. Il dispositivo di inizializzazione risponde con un'offerta di indirizzi IP all'interno del pool di automazione LAN.

Dopo aver compreso la sequenza iniziale di automazione LAN, è possibile risolvere il problema se il processo non funziona come previsto.

# Diagramma per la risoluzione dei problemi




## Log rilevanti per l'automazione LAN di DNA Center 1.1

- network-orchestration-service
- servizio pnp

## Log rilevanti per l'automazione LAN di DNA Center 1.2

Nella release 1.2 non esiste più un servizio pnp, quindi è necessario cercare i seguenti servizi quando si stanno risolvendo i problemi di LAN Automation:

- orchestrazione rete
- progettazione della rete
- connessione-manager-service
- onboarding-service *(questo è il vecchio pnp-service equivalente da 1.1)*

## Registri rilevanti per DNA Center 1.x Public Key Infrastructure (PKI)

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

### Come eseguire tcpdump visualizzato nel diagramma di flusso?

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

*Per arrestare questa operazione utilizzare CTRL+C

Il file pnp_capture.pcap viene memorizzato in /data/tmp/. È necessario copiare il file da DNA Center utilizzando il comando secure copy (SCP) oppure leggere il file da DNA Center utilizzando il comando seguente:

```
$ 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
```

### Che cos'è il file bridge.png che si sta tentando di copiare?

Si tratta di un file immagine di 191 byte che si trova in DNA Center e che si desidera copiare utilizzando il protocollo HTTP (senza utilizzare i certificati) o HTTPS (con i certificati) per verificare la comunicazione tra DNA Center e l'agente PnP.

## Esempi di acquisizioni quando la comunicazione SSL (Secure Sockets Layer) non funziona come previsto (file .pcap completi allegati a questo articolo)

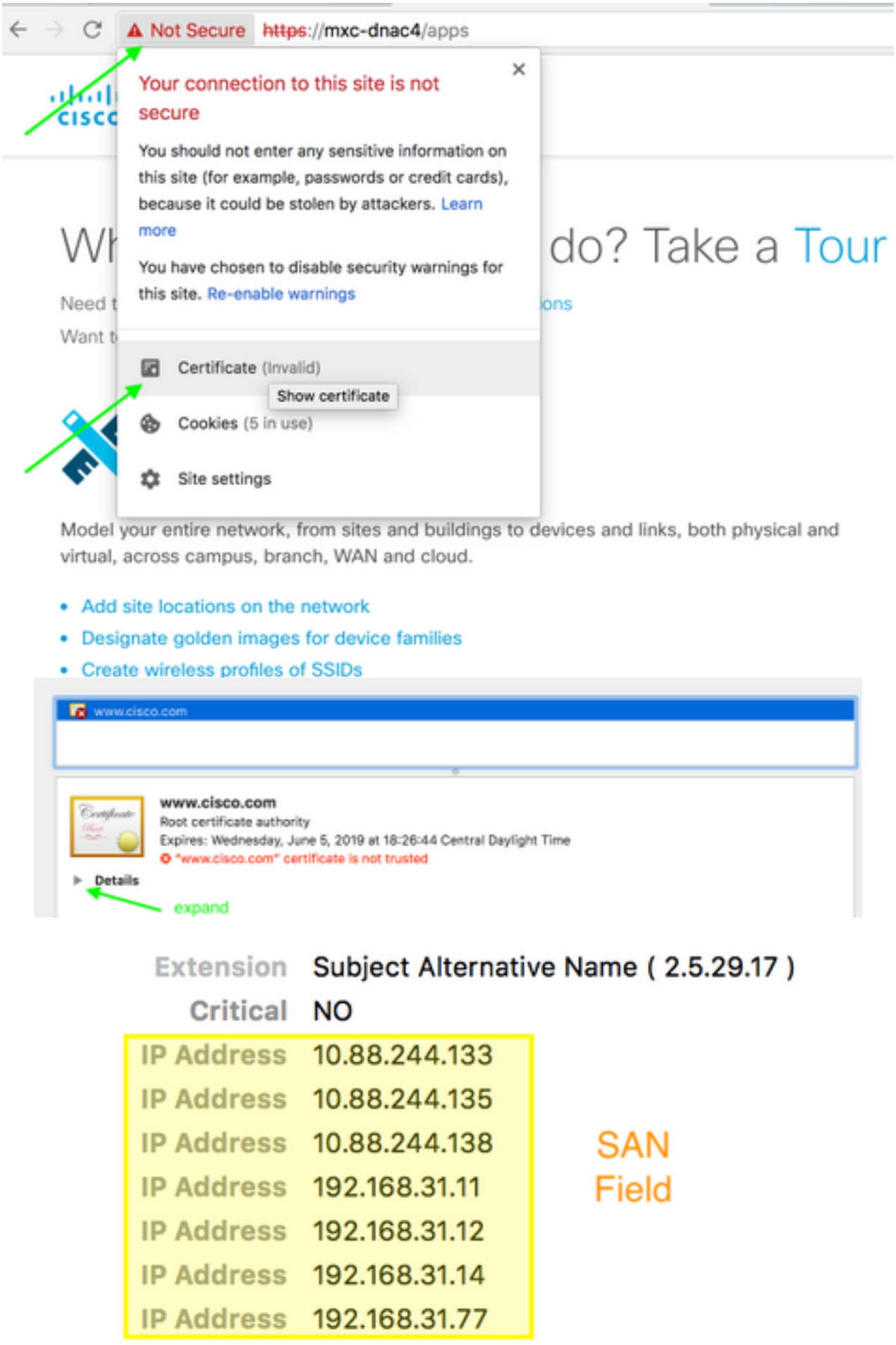
### Certificato non valido

#### Possibile causa:

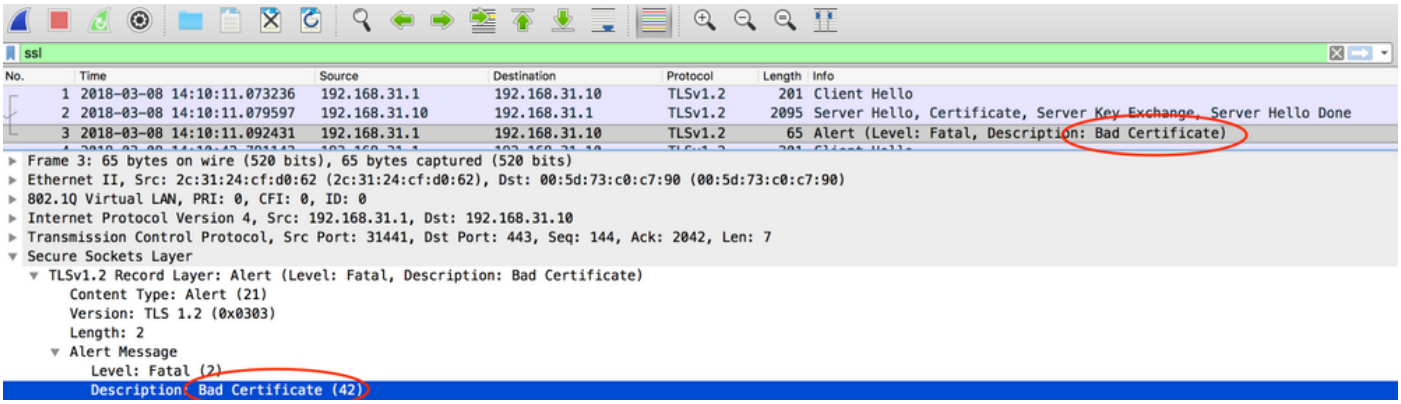
- Il certificato di DNA Center non dispone dell'indirizzo IP corretto nel campo Nome alternativo soggetto (SAN).

Per controllare i campi SAN nel certificato, è possibile eseguire le operazioni seguenti:

#### Verificare il certificato utilizzando un browser




Esempio di acquisizione




### Risoluzione.

Se si dispone di un'Autorità di certificazione (Certificate Authority) di terze parti, assicurarsi che venga fornito un certificato con gli indirizzi IP di DNA Center e l'indirizzo VIP al suo interno. Se non si dispone di un'autorità di certificazione di terze parti, DNA Center può generare automaticamente un certificato. Contatta Cisco TAC per illustrarti il processo.

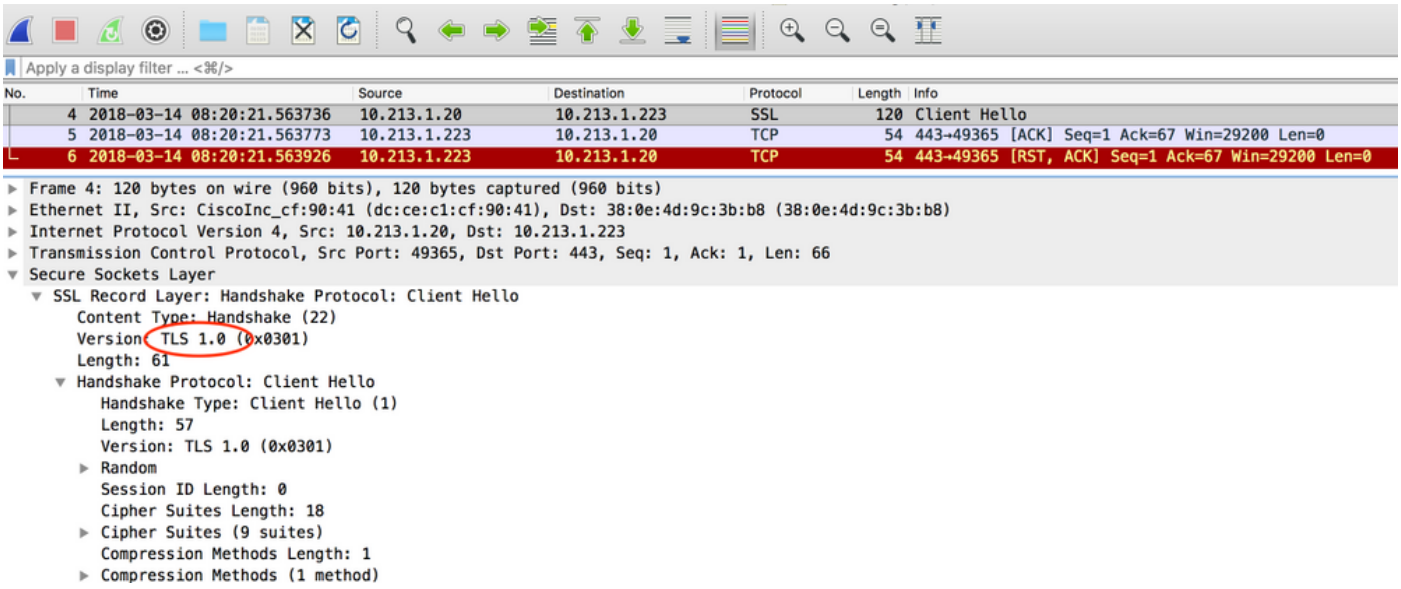
## DNA Center reimposta la connessione

### Possibile causa:

Per impostazione predefinita, DNA Center supporta solo TLS v1.2.

Per risolvere questo problema, abilitare DNA Center per l'utilizzo di TLS v1 seguendo questa guida

### Acquisizione di esempio




# Comandi di debug utili sull'agente PnP per problemi relativi ai certificati

- debug transazioni crypto pki

- debug ssl openssl
- errori debug ssl openssl
- debug errori ssl openssl
- debug crypto pki API
- debug transazioni crypto pki
- debug ssl openssl msg

# Nella risposta manca la chiave di sessione autenticata stabilita in precedenza

In teoria, nella pagina Provisioning > Dispositivi > Inventario dispositivi non si dovrebbe avere dispositivi non richiesti, ma ci sono stati problemi in cui, dopo aver eliminato i dispositivi non richiesti da questa pagina, i dispositivi erano ancora visualizzati in https://<DNA Center ip>/mypnp. Se in questo scenario viene visualizzato un registro simile a quello riportato di seguito nei registri PnP o un'indicazione analoga nella GUI, verificare che il dispositivo non venga visualizzato come non richiesto 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
```

# Vantaggi dell'automazione e dello stack LAN

- In DNA Center 1.2, lo stack deve essere un anello completo (un cavo per stack di due dispositivi potrebbe non funzionare).
- Il dispositivo stack deve essere richiesto immediatamente dall'automazione LAN, in meno di 10 minuti circa.
- Una volta collegato al DNA Center, appare come Non reclamato in PnP.  PnP utilizza l'intervallo di tempo di 10 minuti per determinare lo stack e, una volta scaduto, rimane nella sezione non richiesta dell'automazione LAN.

Se si dispone dei registri RCA o PnP, è possibile cercare messaggi di dispositivo non richiesti:

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

Se non ci sono messaggi, le notifiche dei dispositivi non reclamati non raggiungono DNA Center e PnP non può reclamarlo.

## Come eseguire l'automazione LAN su uno stack

1. Spegnere gli uplink sui dispositivi di inizializzazione.
2. Avviare LAN Automation su DNA Center.
3. Eliminare la configurazione di avvio dallo stack. **# cancellazione scrittura**
4. Rimuovere tutti i certificati dalla NVRAM. **# delete nvram:*.cer**
5. Rimuovere il file vlan.dat. **# delete flash:vlan.dat**
6. Dallo switch primario, eliminare i certificati sullo switch in standby. **# delete stby-nvram:*.cer**

r. Scollegare i cavi dello stack.

b. Accedere alla console di ciascuno switch membro.

c. Eliminare i certificati. **# eliminare nvram:*.cer**

d. Eliminare il database VLAN flash. **# delete flash:vlan.dat**

e. Ricollegare i cavi dello stack.

7. Riavviare.

8. Attendere che lo switch venga registrato come stack, visualizzare tutti i membri e provare ad avviare la finestra di dialogo di configurazione iniziale.

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


         --- System Configuration Dialog ---

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

9. Abilitare gli uplink ai dispositivi di inizializzazione. **# no shutdown**

## Formato del file di mapping dei nomi host che è possibile importare nell'attività di automazione LAN:

DNA Center prevede un file CSV con il nome host e il numero di serie (nome host, numero di serie), come mostrato nell'esempio seguente:

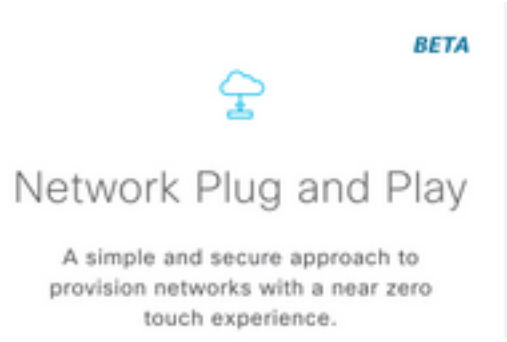
| A | B |
|---|---|
| Edge1 | FCW2048Cxxx |
| Edge2 | FCW2131Lxxx, FCW2131Gxxx, FCW2131Gxxx, FCW2131Gxxx |
| Edge3 | FOC2052Xxxx, FCW2052Cxxx, FCW2052Fxxx |
| Edge4 | FXS2131Qxxx |

Per l'automazione LAN dello stack, il file CSV consente di immettere un nome host e più numeri di serie per riga. I numeri di serie devono essere separati da virgole. Vedere il file CSV allegato per riferimento.

## Dove è andato /mypnp nella versione 1.2?

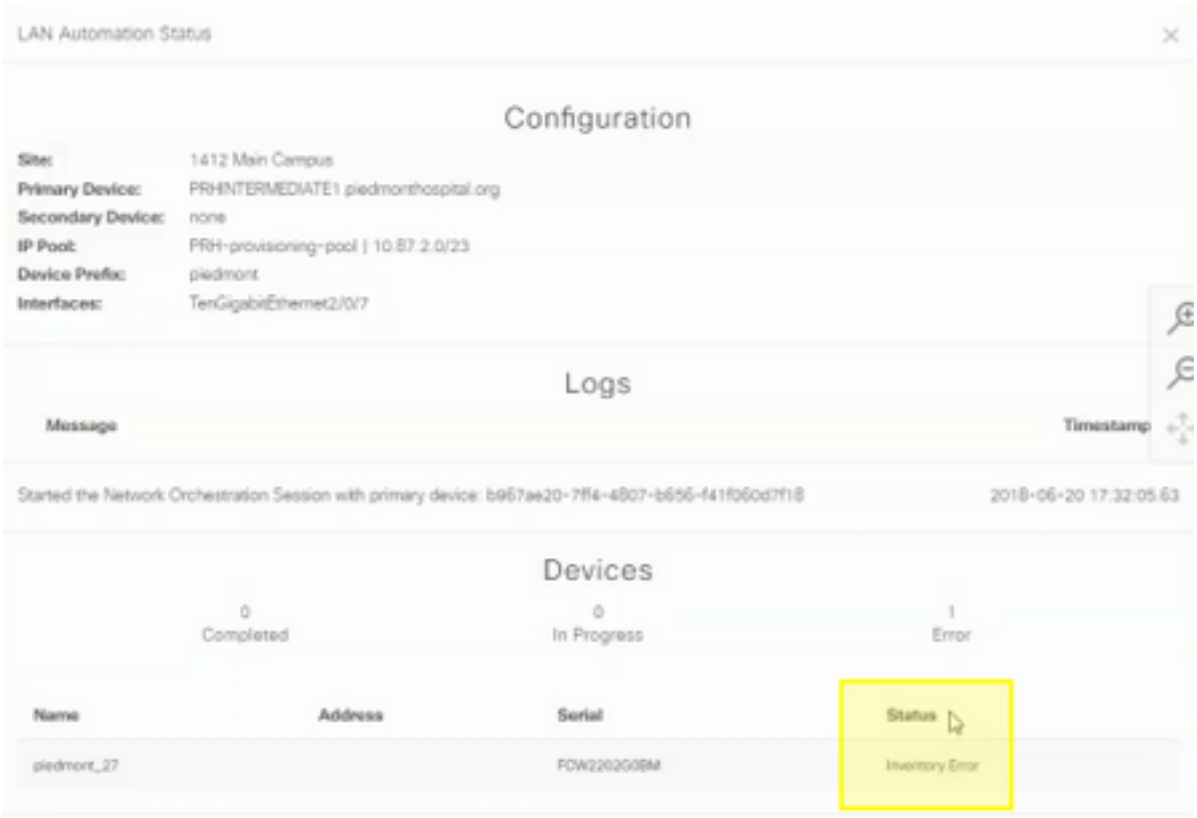
Accedere a Plug and Play in uno dei modi seguenti:

- Dal browser Web, immettere https://<DNA Center IP>/networkpnp
- Dalla home page di DNA Center, selezionare il seguente strumento Plug and Play di rete:




Oppure visitando il sito https://<DNA Center IP>/networkpnp

## Errore di inventario




L'errore di inventario indica che il dispositivo, dopo essere stato richiesto dall'automazione LAN e aver ricevuto la relativa configurazione, non è stato aggiunto all'inventario. Questo errore si verifica in genere a causa di problemi di configurazione, di routing o di credenziali CLI.

Per verificare che si stia tentando di individuare il dispositivo corretto tramite l'automazione LAN, accedere in remoto all'indirizzo IP dell'interfaccia loopback 0 sul dispositivo utilizzando il protocollo di connessione preferito (SSH o Telnet).

## La connettività esiste ma non è stato eseguito il push dei certificati PKI negli agenti PnP

In alcuni casi, i dispositivi al centro possono attivare il bit *Do not Fragment* (DF) dei pacchetti tra gli agenti DNAC e PnP. Ciò potrebbe causare l'eliminazione di pacchetti più grandi di 1500 byte, generalmente pacchetti contenenti il certificato, e quindi l'automazione LAN potrebbe non essere completata. Alcuni dei log più comuni che si trovano nei log *di caricamento di* DNA Center sono:

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

In questo caso, si consiglia di verificare che il percorso tra DNA Center e gli agenti PnP consenta il passaggio dei frame jumbo usando il **sistema di** comando **mtu 9100**.

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