Conseils et astuces d'automatisation LAN pour le centre DNA (Digital Network Architecture)

Contenu

Introduction

Ce document fournit une vue d'ensemble de l'automatisation des réseaux locaux (LAN) pour vous aider à diagnostiquer les problèmes lorsque l'automatisation des réseaux locaux ne fonctionne pas comme prévu dans le centre DNA (Digital Network Architecture).

Contribué par Alexandro Carrasquedo, ingénieur TAC Cisco.

Glossaire

Agent Plug-and-Play (PnP) : nouveau périphérique que vous venez de mettre sous tension sans configuration et sans certificat qui sera automatiquement configuré par DNA Center.

Périphérique de démarrage : Périphérique que DNA Center a déjà provisionné et qui agit en tant que serveur DHCP (Dynamic Host Configuration Protocol).

Conditions préalables

Exigences

Cisco recommande vivement que vous ayez une connaissance générale de l'automatisation LAN et de la solution Plug-and-Play. donne une vue d'ensemble de LAN Automation, bien qu'il soit basé sur DNA Center 1.0, le même concept s'applique à DNA Center 1.1 et versions ultérieures.

Informations générales

L'automatisation LAN est une solution de déploiement quasi automatique qui vous permet de configurer et de provisionner vos périphériques réseau avec l'utilisation d'ISIS comme protocole de routage sous-jacent.

Avant de commencer

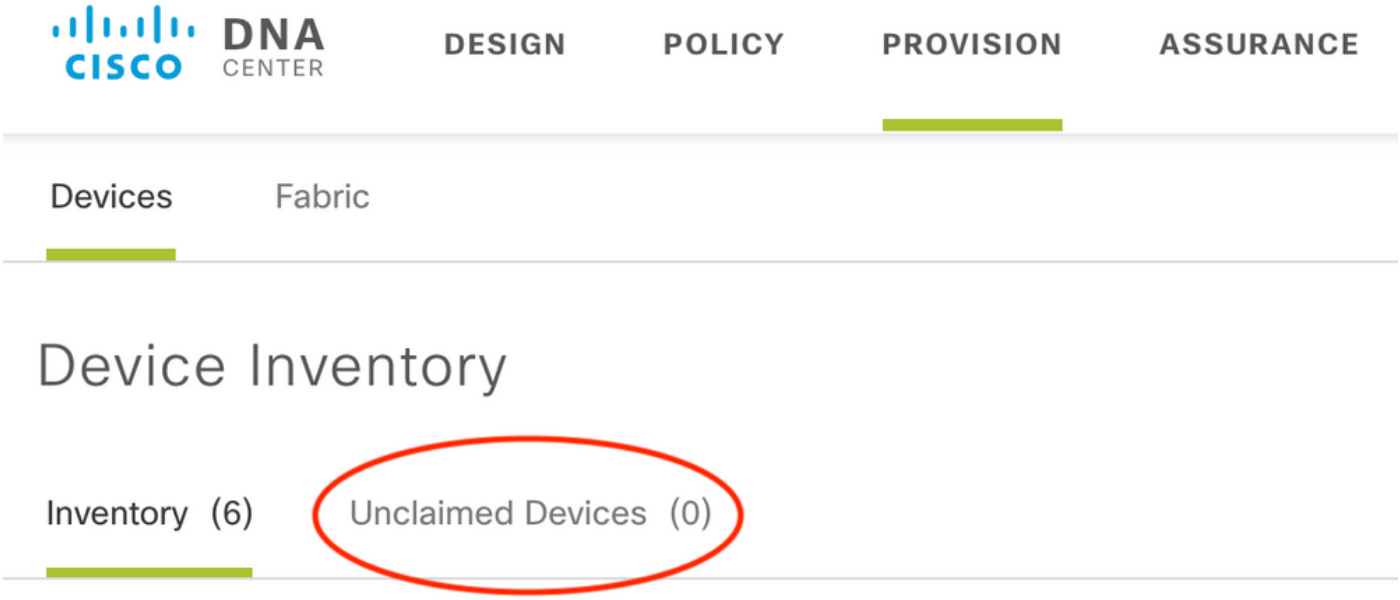
Avant d'exécuter LAN Automation, assurez-vous que votre agent PnP n'a aucun certificat chargé dans la mémoire NVRAM.

```
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
```

Assurez-vous de ne pas avoir de périphériques non réclamés dans la page Provisioning > Devices > Device Inventory :



À cause de CSCvh68847 , certaines piles risquent de ne pas quitter l'état non réclamé et vous pourriez recevoir un message d'erreur ERROR_STACK_UNSUPPORTED. Ce message se produit lorsque l'automatisation du LAN tente de demander au périphérique de provisionner comme s'il s'agissait d'un commutateur unique. Cependant, comme le périphérique est une pile de commutateurs Catalyst 9300, l'automatisation LAN ne peut pas revendiquer le périphérique et celui-ci apparaît comme non revendiqué. De même, PnP ne revendique pas le périphérique car il s'agit d'une pile, de sorte que le périphérique n'est pas provisionné.

Quelles sont les étapes de l'automatisation LAN pendant son exécution ?

DNA Center provisionne le périphérique de démarrage avec la configuration DHCP. L'étendue des adresses IP que le périphérique d'amorçage obtient est un segment du pool initial que vous avez défini lorsque vous avez réservé le pool d'adresses IP pour votre site. Notez que ce pool doit être au moins /25.

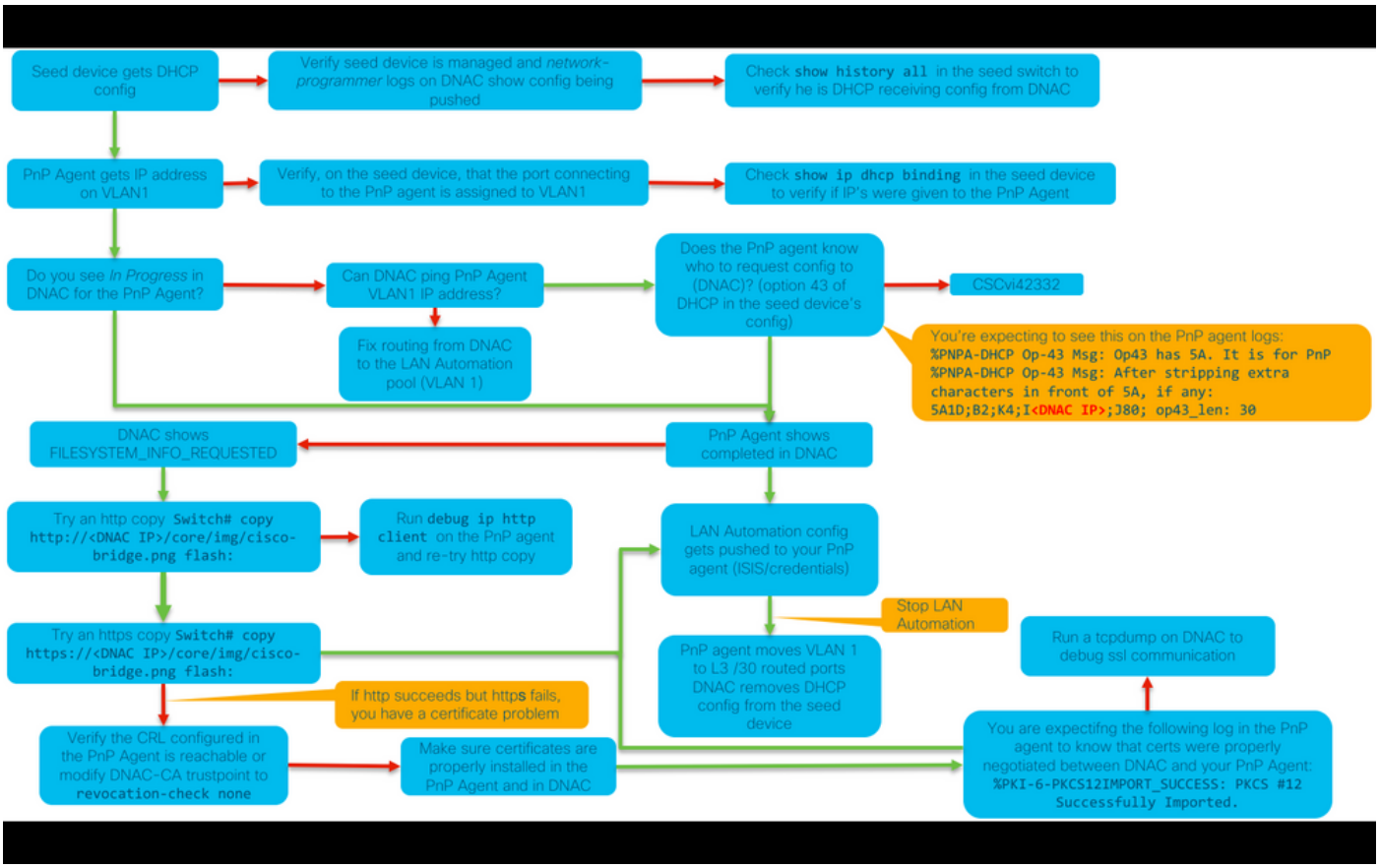
> **Note**: Ce pool est divisé en 3 segments :
> 1. Les adresses IP qui sont transmises au VLAN 1 sur vos agents PnP.
> 2. Les adresses IP envoyées à Loopbac0 sur vos agents PnP.
> 3. Les adresses IP /30 qui sont envoyées à vos agents PnP sur la liaison qui se connecte à vos équipements de base ou autres périphériques de fabric.

Pour que DNA Center puisse provisionner vos agents PnP, la configuration DHCP que le périphérique de démarrage reçoit doit avoir l'option 43 définie avec l'adresse IP de la carte réseau (NIC) d'entreprise de DNA Center ou l'adresse IP virtuelle (VIP), si vous avez un cluster n-noeud.

Lorsque les agents PnP démarrent, ils n'ont aucune configuration. Par conséquent, tous leurs ports font partie du VLAN 1. Par conséquent, les périphériques envoient des messages de détection DHCP au périphérique de démarrage. Le périphérique de démarrage répond par une offre d'adresses IP au sein du pool d'automatisation du LAN.

Maintenant que vous comprenez la séquence initiale de l'automatisation LAN, vous pouvez dépanner le processus s'il ne fonctionne pas comme prévu.

Schéma de dépannage



Journaux pertinents de DNA Center 1.1 LAN Automation

- network-orchestration-service
- pnp-service

Journaux pertinents de DNA Center 1.2 LAN Automation

Dans la version 1.2, il n'y a plus de service pnp. Vous devez donc rechercher les services suivants lors du dépannage de LAN Automation :

- orchestration du réseau
- conception de réseau
- connection-manager-service
- onboarding-service *(l'ancien équivalent pnp-service de la version 1.1)*

Journaux pertinents de l'infrastructure à clé publique (PKI) DNA Center 1.x

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

Comment exécuter le tcpdump affiché dans l'organigramme ?

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

*Pour arrêter cette utilisation, cliquez sur CTRL+C

Ceci stocke le fichier pnp_capture.pcap dans /data/tmp/. Vous devez copier le fichier à partir de DNA Center à l'aide de la commande secure copy (SCP) ou lire le fichier à partir de DNA Center à l'aide de la commande suivante :

```
$ 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
```

Quel est le fichier bridge.png que vous essayez de copier ?

Il s'agit d'un fichier image de 191 octets qui se trouve dans DNA Center que vous voulez copier en utilisant HTTP (sans utiliser de certificats) ou HTTPS (en utilisant des certificats) pour tester la communication entre DNA Center et votre agent PnP.

Exemples de captures lorsque la communication SSL (Secure Sockets Layer) ne fonctionne pas comme prévu (fichiers .pcap complets joints à cet article)

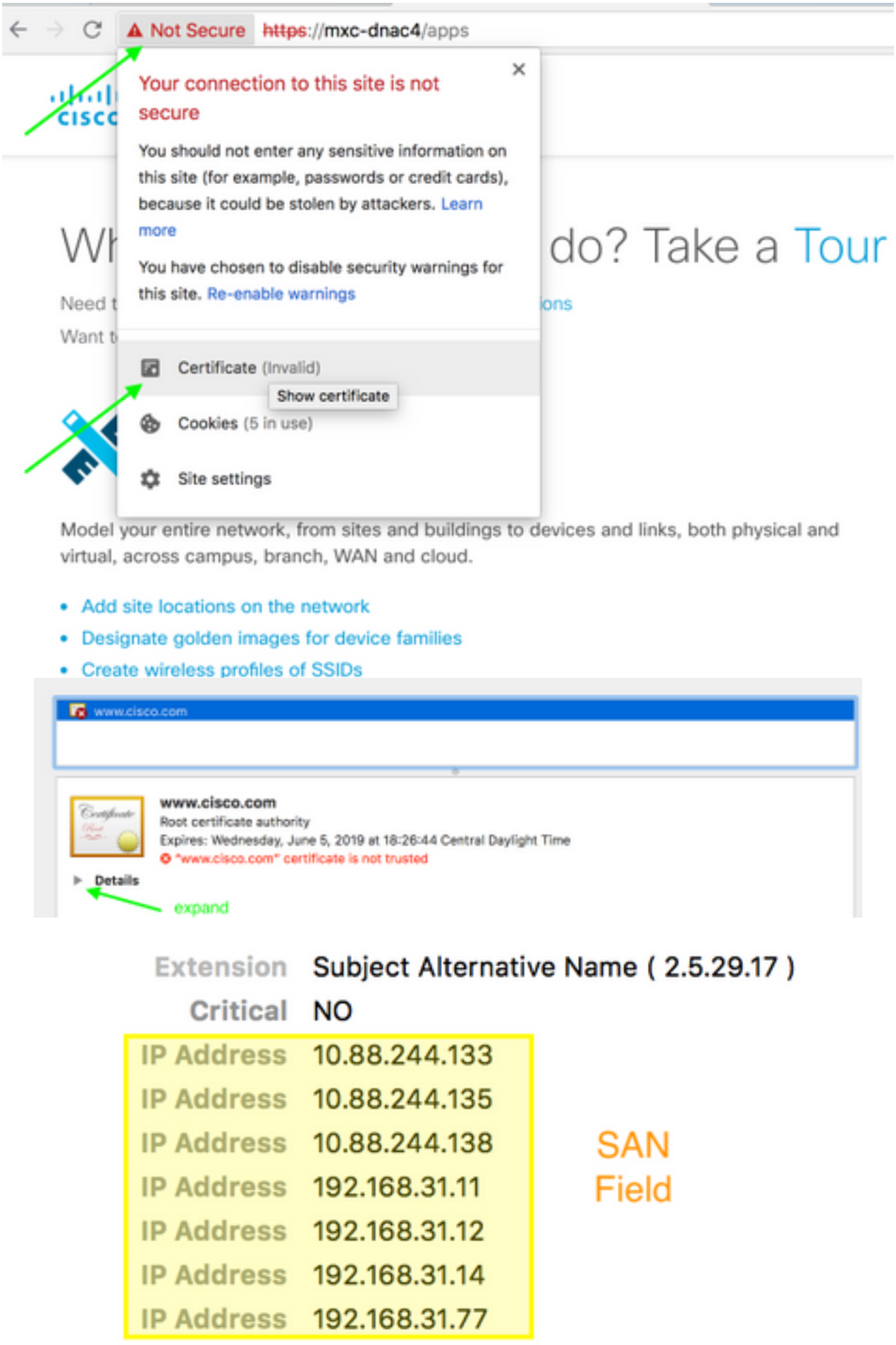
Certificat incorrect

Cause possible:

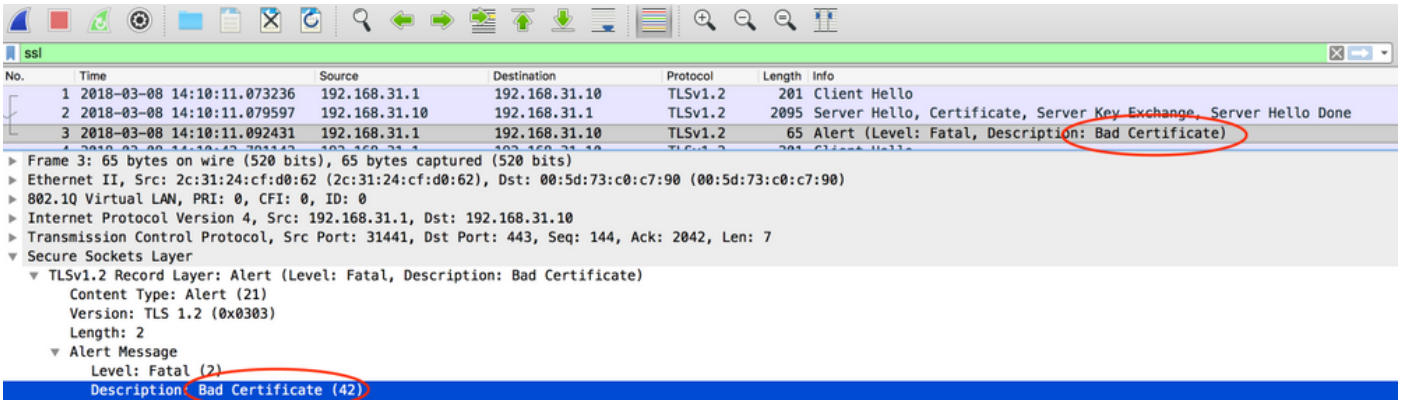
- Le certificat de DNA Center ne possède pas l'adresse IP appropriée dans le champ Subject Alternative Name (SAN).

Pour vérifier les champs SAN de votre certificat, procédez comme suit :

Vérifier le certificat à l'aide d'un navigateur



Capture d'échantillons



Résolution.

Si vous avez une autorité de certification tierce, assurez-vous qu'elle vous donne un certificat avec les adresses IP de DNA Center et le VIP dedans. Si vous n'avez pas de CA tierce, DNA Center peut générer un certificat pour vous. Contactez le TAC Cisco pour vous guider tout au long de ce processus.

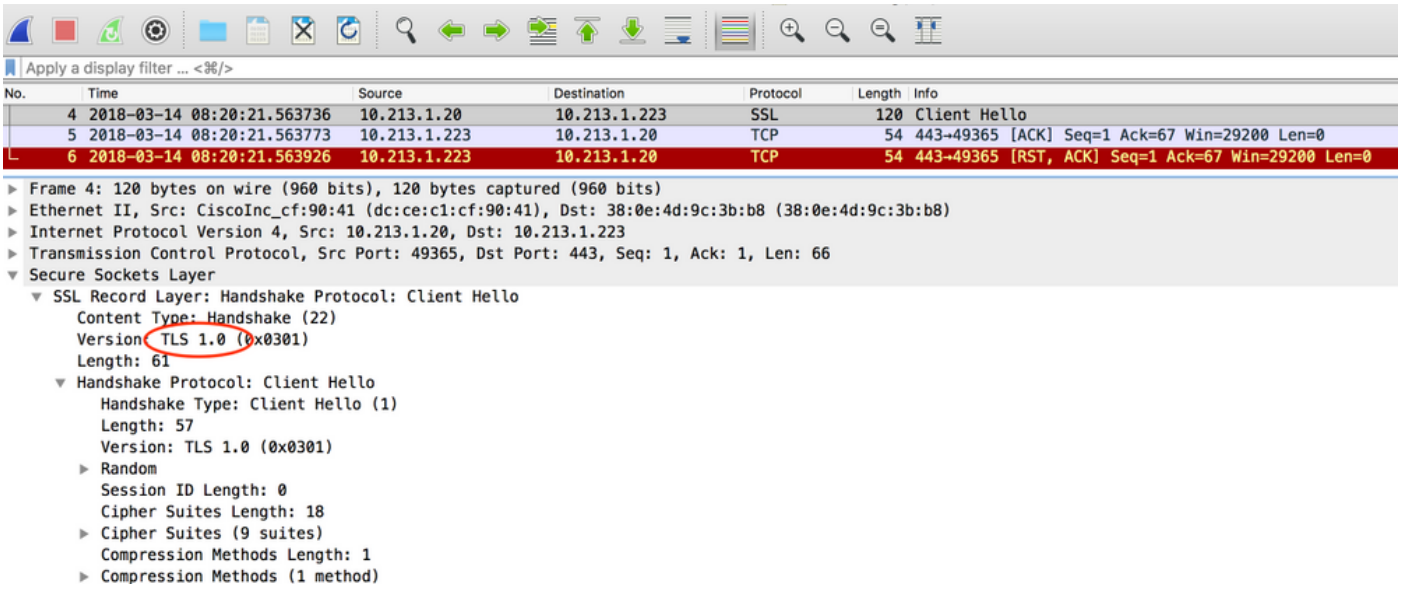
DNA Center réinitialise la connexion

Cause possible:

DNA Center prend uniquement en charge TLS v1.2 par défaut.

Pour contourner ce problème, activez DNA Center pour utiliser TLS v1 en suivant ce guide

Exemple de capture



Commandes de débogage utiles sur l'agent PnP pour les problèmes liés aux certificats

- debug crypto pki transactions
- debug ssl openssl

- debug ssl openssl errations
- debug ssl openssl errors
- debug crypto pki API
- debug crypto pki transactions
- debug ssl openssl msg

La clé de session authentifiée précédemment établie est manquante pour la réponse

En théorie, vous ne devriez pas avoir de périphériques non réclamés dans la page Provisioning > Devices > Device Inventory, mais il y a eu des problèmes où, après avoir supprimé les périphériques non réclamés de cette page, les périphériques étaient toujours affichés dans https://<DNA Center ip>/mypnp. Si vous rencontrez ce scénario et que vous voyez un journal similaire à celui qui suit dans les journaux PnP ou une indication de la même dans l'interface utilisateur graphique, assurez-vous que le périphérique n'apparaît pas comme non revendiqué dans 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
```

Intégration de l'automatisation et de l'empilage LAN

- Dans DNA Center 1.2, la pile doit être en anneau complet (un câble de pile pour une pile de 2 membres peut ne pas fonctionner).
- L'automatisation du LAN doit rapidement revendiquer le périphérique de la pile, soit environ moins de 10 minutes.
- Une fois connecté à DNA Center, il apparaît comme Non réclamé dans PnP. PnP utilise la fenêtre de 10 minutes pour déterminer la pile et une fois qu'elle expire, elle restera dans la section non réclamée de l'automatisation LAN.

Si vous avez des journaux RCA ou PnP, vous pouvez rechercher des messages de périphérique non réclamés :

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

S'il n'y a aucun message, les notifications des périphériques non réclamés n'atteignent pas DNA Center et PnP ne peut pas le réclamer.

Comment faire l'automatisation LAN sur une pile

1. Arrêtez les liaisons ascendantes vers le ou les périphériques de démarrage.
2. Démarrez LAN Automation sur DNA Center.
3. Supprimez la configuration de démarrage de la pile. **# write erase**
4. Supprimez tous les certificats de la mémoire NVRAM. **# delete nvram:*.cer**
5. Supprimez le fichier vlan.dat. **# delete flash:vlan.dat**
6. Àpartir du commutateur principal, supprimez les certificats du commutateur de secours. **#**

delete stby-nvram:*.cer

a. Déconnectez les câbles de la pile.

b. Connectez-vous à la console de chaque commutateur membre.

c. Supprimez les certificats. **# delete nvram:*.cer**

d. Supprimez la base de données flas vlan. **# delete flash:vlan.dat**

e. Reconnectez les câbles de la pile.

7. Redémarrez.

8. Attendez que le commutateur s'enregistre en tant que pile, qu'il affiche tous les membres et qu'il tente de démarrer la boîte de dialogue de configuration initiale.

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


         --- System Configuration Dialog ---

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

9. Activez les liaisons ascendantes vers le ou les périphériques d'amorçage. **# no shutdown**

Format du fichier de mappage de nom d'hôte que je peux importer dans ma tâche d'automatisation LAN ?

DNA Center attend un fichier CSV avec le nom d'hôte et le numéro de série (nom d'hôte, numéro de série), comme indiqué dans l'exemple suivant :

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

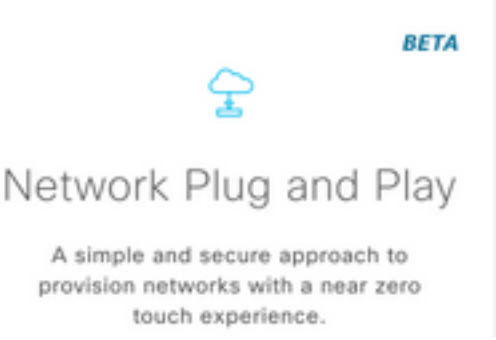
Pour l'automatisation du réseau local de la pile, le fichier CSV vous permet d'entrer un nom d'hôte et plusieurs numéros de série par ligne. Les numéros de série doivent être séparés par des virgules. Voir le fichier CSV joint pour référence.

Où est passé /mypnp dans 1.2 ?

Accédez à PnP de l'une des manières suivantes :

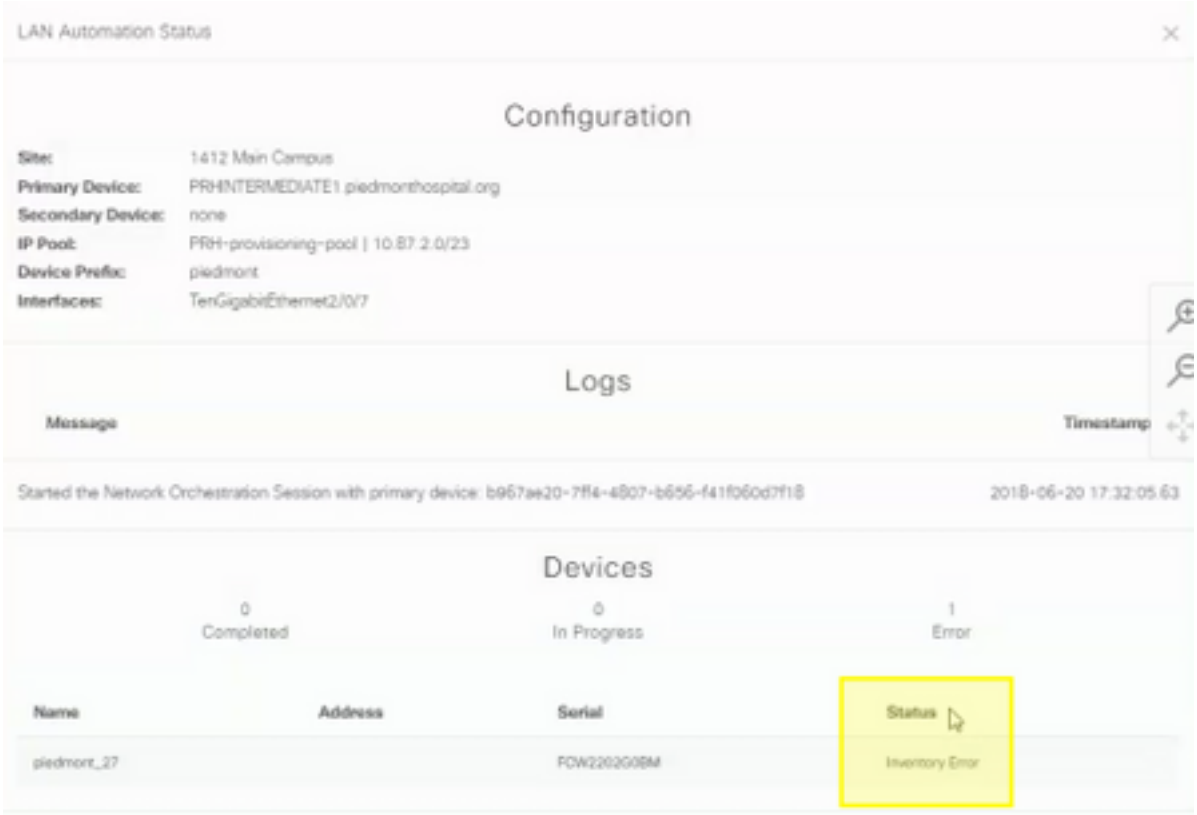
- Àpartir de votre navigateur Web, saisissez https://<DNA Center IP>/networkpnp

- Sur la page d'accueil de DNA Center, sélectionnez l'outil Network Plug and Play suivant :



Ou en accédant à https://<DNA Center IP>/networkpnp

Erreur d'inventaire



L'erreur d'inventaire signifie que le périphérique, après avoir été revendiqué par l'automatisation LAN et avoir reçu sa configuration, a échoué, à être ajouté à l'inventaire. Cette erreur se produit généralement en raison de problèmes de configuration, de routage ou d'informations d'identification CLI.

Pour vérifier que vous essayez d'activer le périphérique correct via LAN Automation, accédez à distance à l'adresse IP de l'interface de bouclage 0 sur le périphérique à l'aide du protocole de connexion préféré (SSH ou Telnet).

La connectivité existe, mais les certificats PKI ne sont pas transmis correctement aux agents PnP

Il peut arriver que les périphériques du milieu activent le bit *Ne pas fragmenter* (DF) des paquets entre DNAC et les agents PnP. Cela peut entraîner l'abandon de paquets de plus de 1 500 octets, généralement des paquets contenant le certificat, et donc l'automatisation du réseau local peut ne pas être terminée. Voici quelques-uns des journaux courants qui sont visibles dans les journaux *d'intégration* du Centre ADN :

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

L'action suggérée dans ce cas est de s'assurer que le chemin entre DNA Center et les agents PnP permet aux trames jumbo de passer à l'aide du **système de** commande **mtu 9100**.

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