デジタルネットワークアーキテクチャ(DNA)センターのLAN自動化のヒントとテクニック

内容

概要

このドキュメントでは、LANオートメーションがデジタルネットワークアーキテクチャ(DNA)センターで想定どおりに動作しない場合の問題の診断に役立つローカルエリアネットワーク(LAN)オートメーションの概要について説明します。

著者：Cisco TACエンジニア、Alexandro Carrasquedo

数珠

プラグアンドプレイ(PnP)エージェント：構成や証明書なしで電源を入れたばかりの新しいデバイスで、DNA Centerによって自動的に設定されます。

シードデバイス：DNA Centerが既にプロビジョニングし、Dynamic Host Configuration Protocol(DHCP)サーバーとして機能するデバイス。

前提条件

要件

LANオートメーションとプラグアンドプレイソリューションに関する一般的な知識があることが強く推奨されます。は、LANオートメーションの概要を示していますが、DNA Center 1.0をベースにしていますが、DNA Center 1.1以降にも同じ概念が適用されます。

背景説明

LAN自動化は、アンダーレイルーティングプロトコルとしてISISを使用してネットワークデバイスを設定およびプロビジョニングできる、ほぼゼロタッチ導入ソリューションです。

はじめる前に

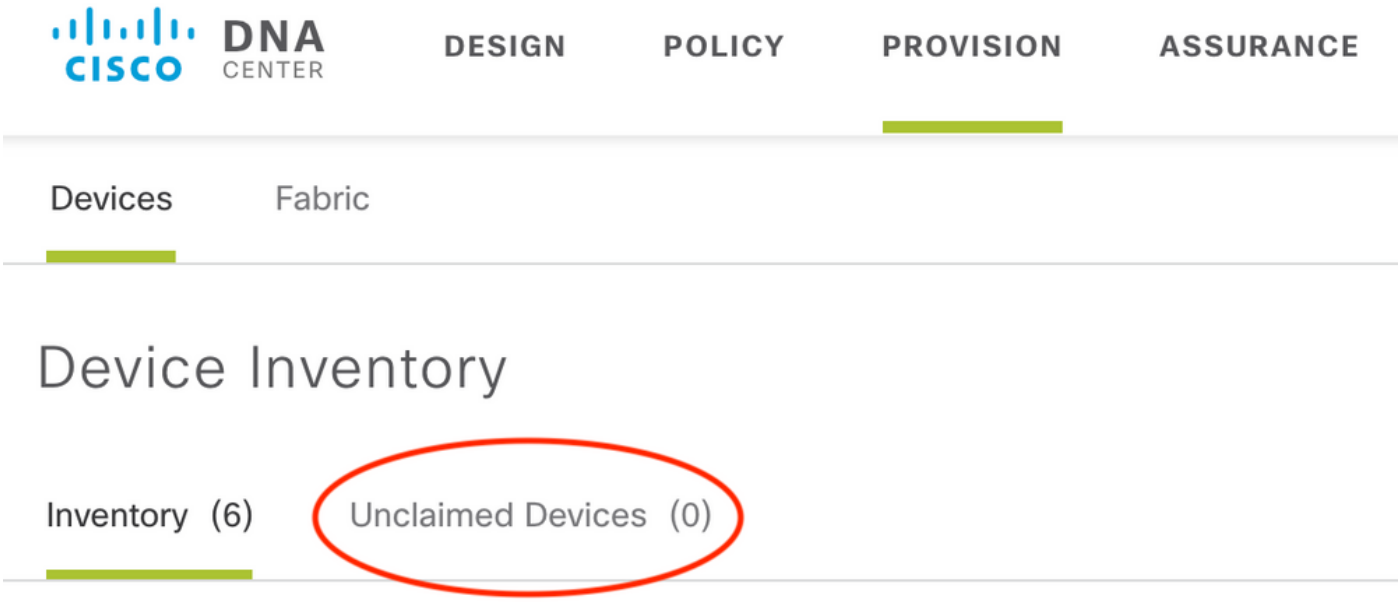
LAN Automationを実行する前に、PnPエージェントにNVRAMにロードされている証明書がないことを確認してください。

```
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
```

[プロビジョニング(Provisioning)] > [デバイス(Devices)] > [デバイスインベントリ(Device Inventory)]ページで、要求されていないデバイスがないことを確認します。



CSCvh68847が原因　一部のスタックは要求されていない状態のままになり、ERROR_STACK_UNSUPPORTEDエラーメッセージが表示されることがあります。このメッセージは、LANオートメーションがデバイスを単一のスイッチのようにプロビジョニングするように要求しようとすると発生します。ただし、デバイスはCatalyst 9300スイッチスタックであるため、LANオートメーションはデバイスを要求できず、デバイスは要求されていないものとして表示されます。同様に、PnPはスタックであるため、デバイスを要求しないため、デバイスはプロビジョニングされません。

LAN Automationの実行中に実行される手順は何ですか。

DNA Centerは、シードデバイスにDHCP設定をプロビジョニングします。シードデバイスが取得するIPアドレスの範囲は、サイトのIPアドレスプールを予約したときに定義した初期プールのセグメントです。このプールは/25以上である必要があります。

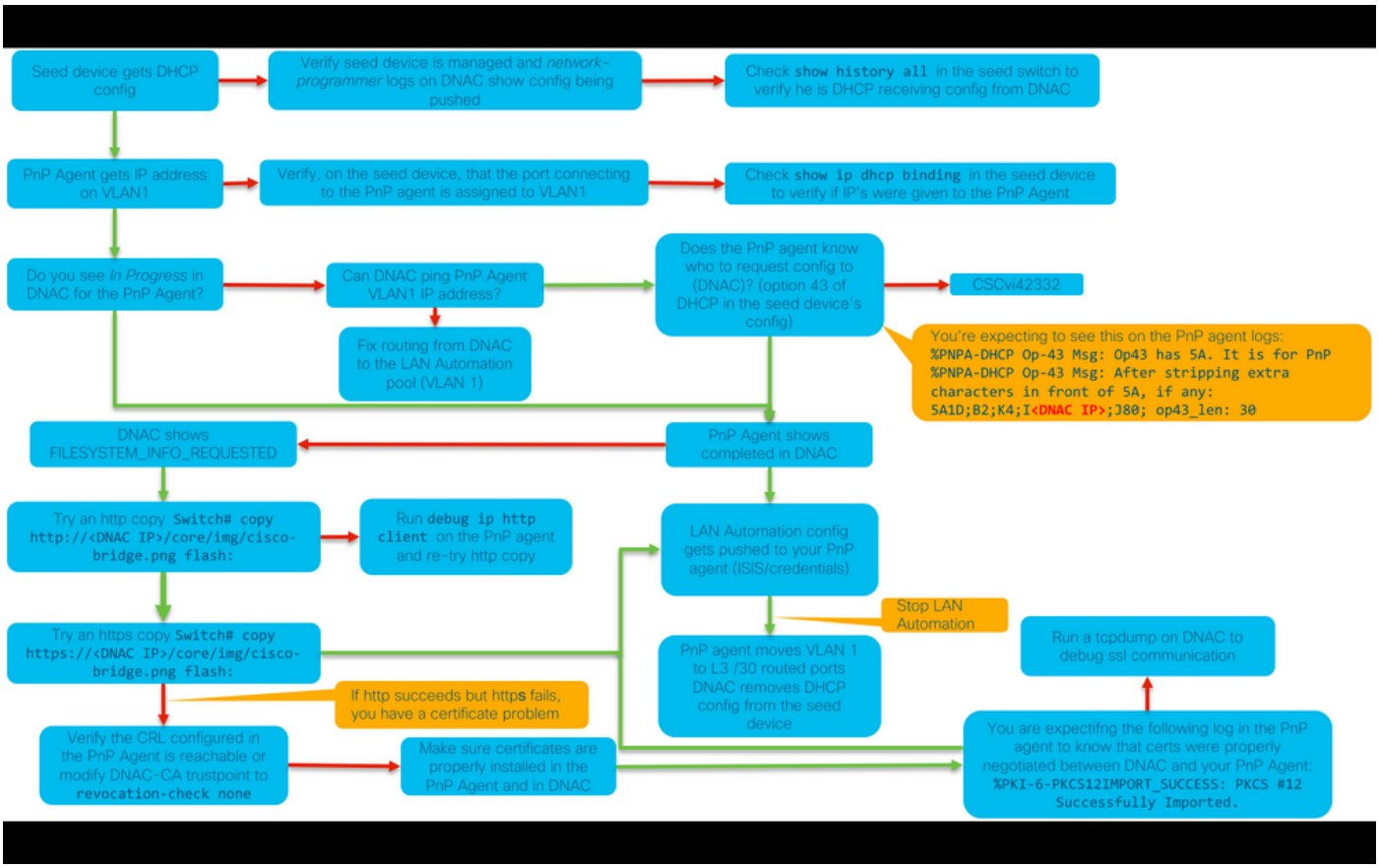
> **注**：このプールは3つのセグメントに分割されます。
> 1. PnPエージェントのVLAN 1にプッシュされるIPアドレス。
> 2. PnPエージェントのLoopbac0にプッシュされるIPアドレス。
> 3.シードまたは他のファブリックデバイスに接続するリンク上のPnPエージェントにプッシュされる/30 IPアドレス。

DNA CenterがPnPエージェントをプロビジョニングするには、シードデバイスが受信するDHCP設定で、nノードクラスタの場合は、DNA Centerエンタープライズ向けネットワークインターフェイスカード(NIC)のIPアドレスまたは仮想IP(VIP)アドレスを指定する必要があります。

PnPエージェントが起動しても、設定はありません。したがって、すべてのポートがVLAN 1の一部です。その結果、デバイスはDHCPディスカバリメッセージをシードデバイスに送信します。シードデバイスは、LAN自動化プール内のIPアドレスのオファーを使用して応答します。

LAN自動化の初期シーケンスを理解したので、プロセスが期待どおりに動作しない場合は、トラブルシューティングを行うことができます。

トラブルシューティングダイアグラム



DNA Center 1.1 LAN Automation関連ログ

- network-orchestration-service
- pnp-service

DNA Center 1.2 LAN Automation関連ログ

リリース1.2ではPNPサービスがなくなったため、LANオートメーションのトラブルシューティングを行う際には、次のサービスを探す必要があります。

- ネットワークオーケストレーション
- ネットワーク設計
- connection-manager-service
- onboarding-service *（これは1.1に相当する古いpnp-serviceです）*

DNA Center 1.x公開キーインフラストラクチャ(PKI)関連ログ

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

フローチャートに示されているtcpdumpの実行方法を教えてください。

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

*これを停止するには、Ctrl+Cを使用します

これにより、pnp_capture.pcapファイルが/data/tmp/に保存されます。セキュアコピー(SCP)コマンドを使用してDNA Centerからファイルをコピーするか、次のコマンドを使用してDNA Centerからファイルを読み取る必要があります。

```
$ 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
```

コピーしようとしているbridge.pngファイルは何ですか。

DNA Centerに含まれる191バイトのイメージファイルで、HTTP（証明書を使用しない）またはHTTPS（証明書を使用する）を使用してコピーし、DNA CenterとPnPエージェント間の通信をテストします。

セキュアソケットレイヤ(SSL)通信が期待どおりに動作しない場合のキャプチャの例（この記事に添付されている.pcapファイル全体）

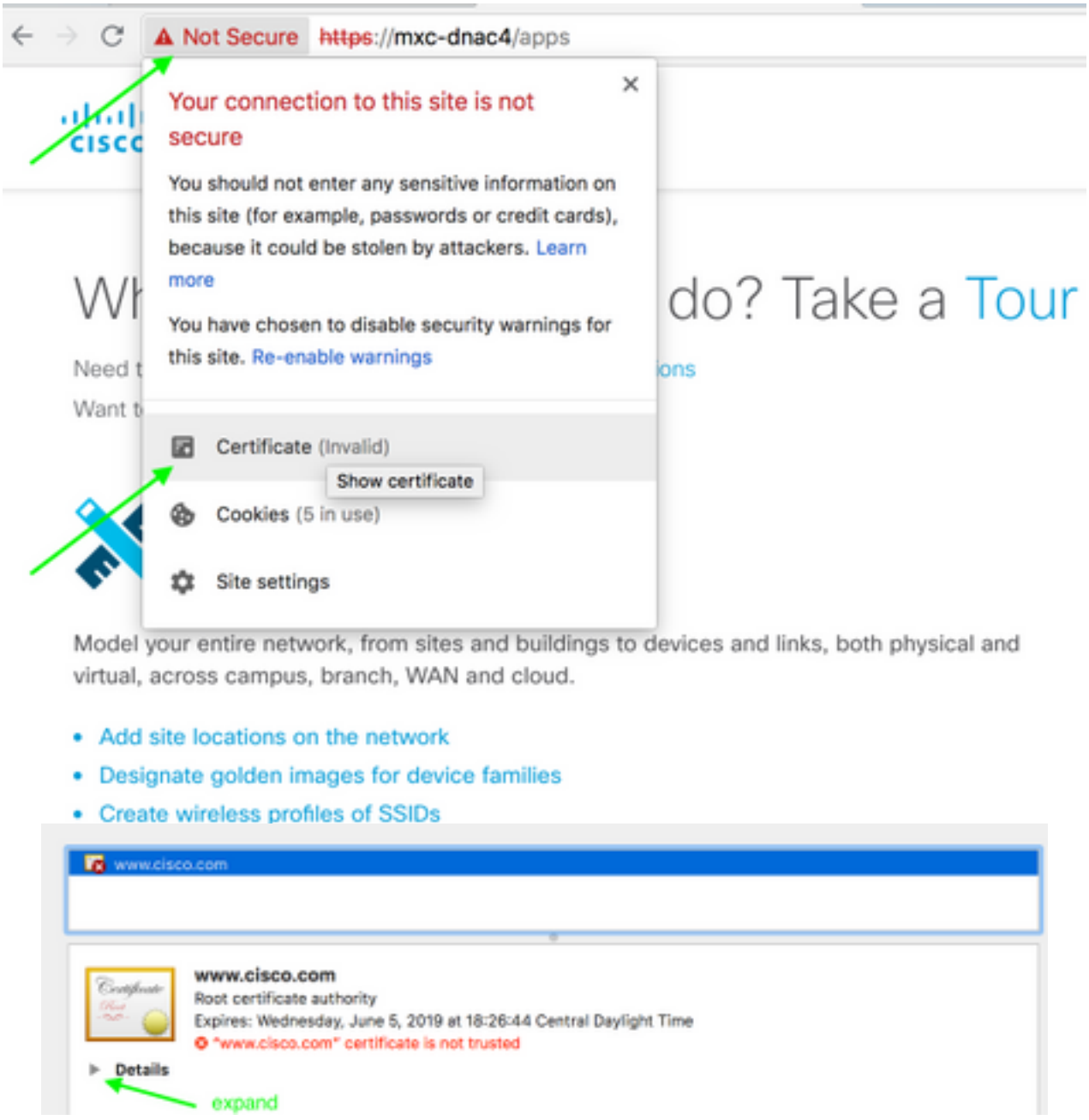
不正な証明書

考えられる原因：

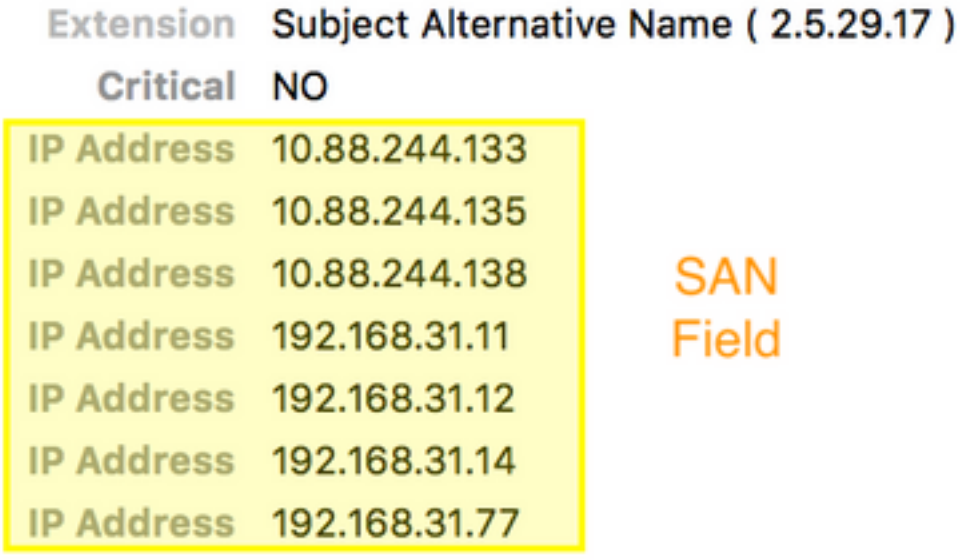
- DNA Centerの証明書の[サブジェクト代替名(SAN)]フィールドに正しいIPアドレスがありません。

証明書のSANフィールドを確認するには、次の手順を実行します。

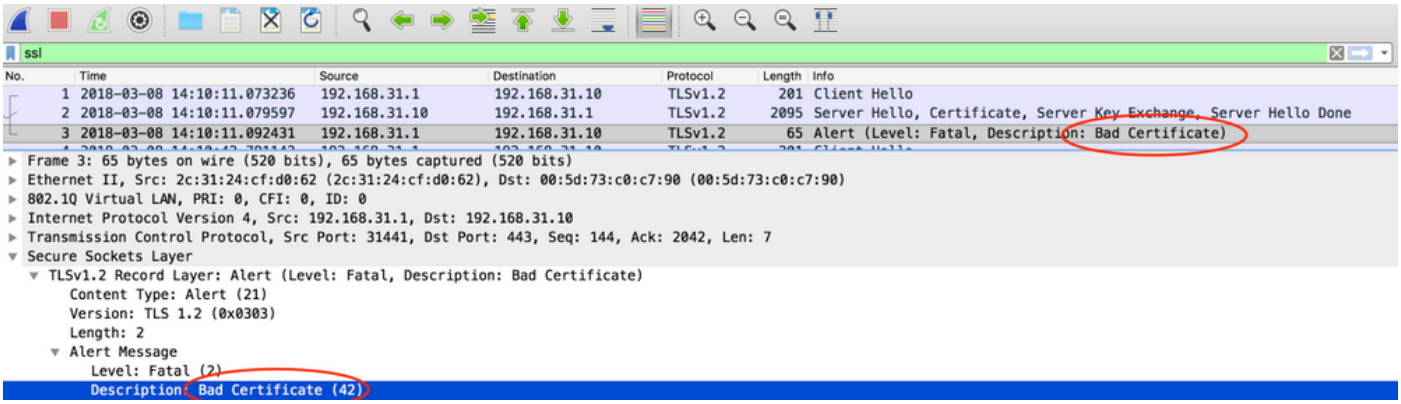
ブラウザを使用して証明書を確認します


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

キャプチャ例



解決方法.

サードパーティCA（認証局）がある場合は、DNA CenterのIPアドレスとVIPが含まれた証明書が提供されていることを確認してください。サードパーティCAがない場合、DNA Centerは証明書を生成できます。このプロセスの手順については、Cisco TACにお問い合わせください。

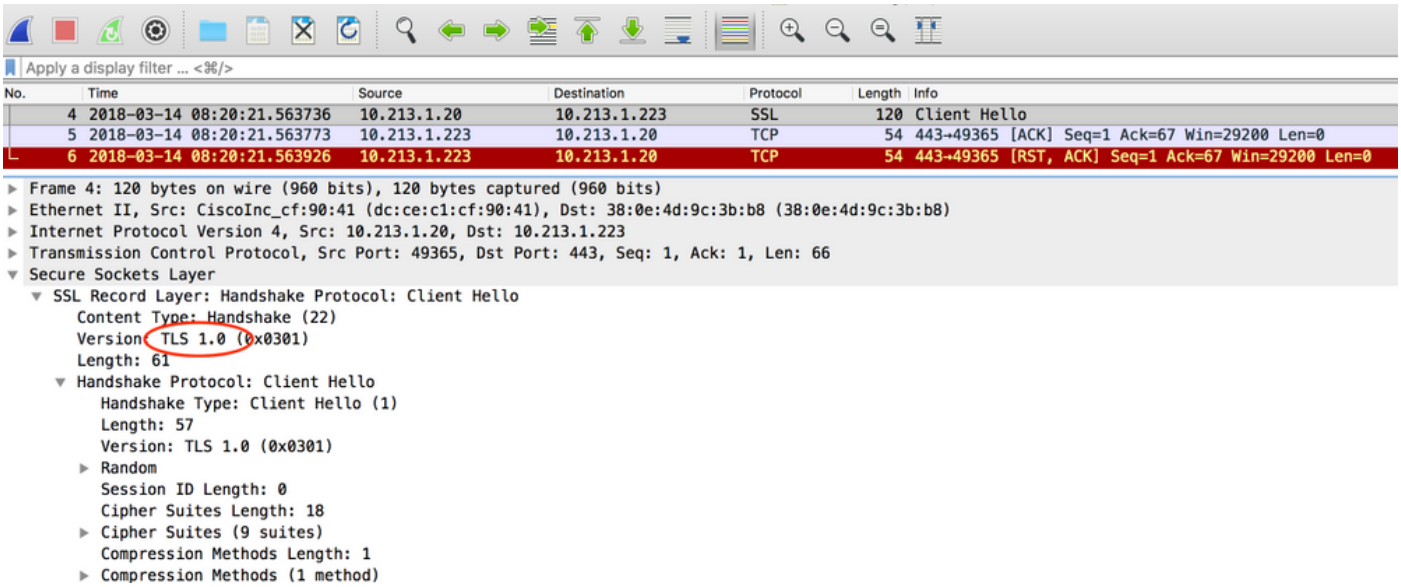
DNA Centerが接続をリセットします

考えられる原因：

DNA Centerはデフォルトで TLS v1.2のみをサポートします。

これを回避するには、このガイドに従ってDNA CenterでTLS v1を使用できるようにしてください

キャプチャ例



証明書関連の問題に関するPnPエージェントでの便利なdebugコマンド

- 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

以前に確立された認証済みセッションキーの応答がありません

理論上は、[Provisioning] > [Devices] > [Device Inventory]ページで未請求のデバイスを表示する必要はありませんが、このページから未請求のデバイスを削除した後も、デバイスがhttps://<DNA Center ip>/mynpに表示される問題があります。このシナリオが発生し、PnPログに次のようなログが表示される場合、またはGUIに次のようなログが表示される場合は、デバイスがPnPで未請求として表示されないことを確認します。

```
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の自動化とスタック構成の検討事項

- DNA Center 1.2では、スタックはフルリングである必要があります（2メンバーのスタックに1本のスタックケーブルが機能しない場合があります）。
- スタックデバイスは、LANの自動化によって迅速に要求する必要があります。これは約10分未満です。
- DNA Centerに接続されると、PnPでUnclaimedと表示されます。 PnPは、スタックの判別に10分間の時間枠を使用し、期限が切れると、LANオートメーションの未請求セクションに残ります。

RCAまたはPnPログがある場合は、未請求のデバイスメッセージを検索できます。

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

メッセージがない場合、要求されていないデバイス通知はDNA Centerに到達せず、PnPはこれを要求できません。

スタックでLANオートメーションを行う方法

1. シードデバイスへのアップリンクをシャットダウンします。
2. DNA CenterでLAN Automationを開始します。
3. スタックからスタートアップコンフィギュレーションを削除します。**# write erase**
4. NVRAMからすべての証明書を削除します。**# delete nvram:*.cer**
5. vlan.datファイルを削除します。**# delete flash:vlan.dat**
6. プライマリスイッチから、スタンバイスイッチの証明書を削除します。**# delete stby-nvram:*.cer**

a.スタックケーブルを外します。

b.各メンバスイッチのコンソールにログインします。

c.証明書を削除します。**# delete nvram:*.cer**

d.flas vlanデータベースを削除します。**# delete flash:vlan.dat**

e.スタックケーブルを再接続します。

7.リブートします。

8.スイッチがスタックとして登録されるまで待ち、すべてのメンバを起動し、初期設定ダイアログを開始します。

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


         --- System Configuration Dialog ---

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

9.シードデバイスへのアップリンクを有効にします。**# no shutdown**

LAN自動化タスクにインポートできるホスト名マップファイルの形式は？

DNA Centerでは、次の例に示すように、ホスト名とシリアル番号（ホスト名、シリアル番号）を含むCSVファイルが必要です。

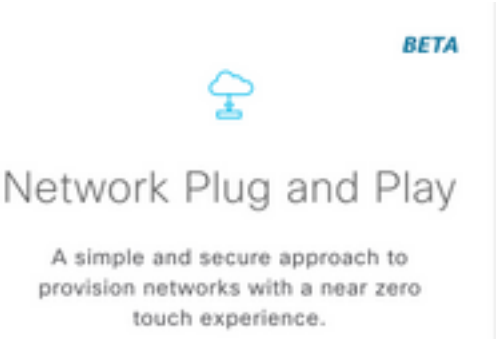
A	B
Edge1	FCW2048Cxxx
Edge2	FCW2131Lxxx, FCW2131Gxxx, FCW2131Gxxx, FCW2131Gxxx
Edge3	FOC2052Xxxx, FCW2052Cxxx, FCW2052Fxxx
Edge4	FXS2131Qxxx

スタックLANオートメーションでは、CSVファイルを使用して、1行に1つのホスト名と複数のシリアル番号を入力できます。シリアル番号はカンマで区切る必要があります。詳細については、添付のCSVファイルを参照してください。

/mypnpは1.2のどこに行きましたか。

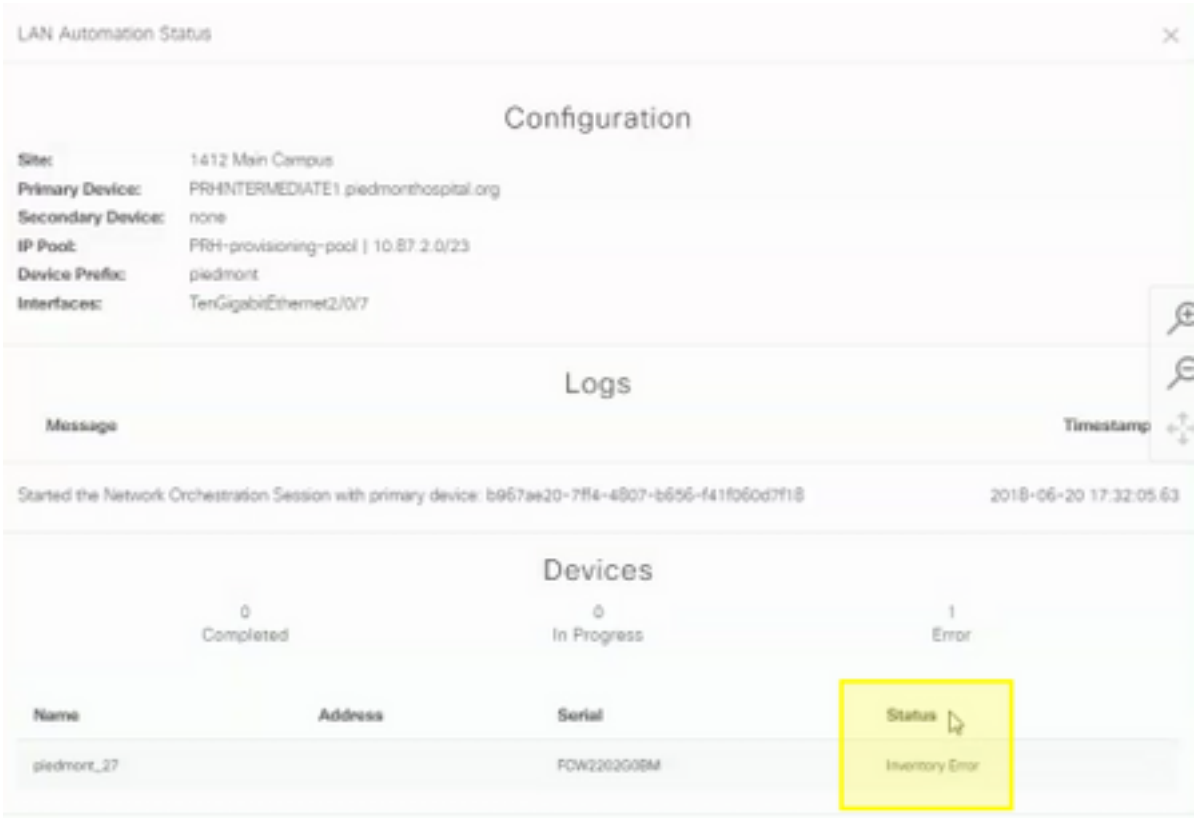
次のいずれかの方法でPnPにアクセスします。

- Webブラウザで、https://<DNA Center IP>/networkpnpと入力します
- DNA Centerホームページから、次のネットワークプラグアンドプレイツールを選択します。



または、https://<DNA Center IP>/networkpnpにアクセスします

インベントリエラー



インベントリエラーは、LANオートメーションによって要求され、設定を受信した後、デバイスがインベントリに追加されることを意味します。通常、このエラーは、設定、ルーティング、またはCLIクレデンシャルの問題が原因で発生します。

LAN Automationを使用して正しいデバイスを起動しようとしていることを確認するには、優先接続プロトコル（SSHまたはTelnet）を使用して、デバイス上のloopback 0インターフェイスのIPアドレスにリモートアクセスします。

接続は存在しますが、PKI証明書はPnPエージェントに正常にプッシュされません

途中のデバイスで、DNACとPnPエージェント間のパケットの*Don't Fragment*(DF)ビットがオンになる場合があります。これにより、1500バイトを超えるパケット（通常は証明書を含むパケット）が廃棄される可能性があるため、LAN Automationが完了しない可能性があります。DNA Centerのオンボーディングログに見られる一般的なログの*一部*を次に示します。

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

この場合の推奨処置は、DNA CenterとPnPエージェントの間のパスで、**system mtu 9100コマンドを使用してジャンボフレームが通過できるようにすることです。**

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