セキュアネットワークデバイスのプロビジョニング

内容

概要

このドキュメントでは、DNSルックアップを使用してネットワークを安全にオンボーディングするためのシスコデバイスの段階的なアプローチについて説明します。

前提条件

要件

- Cisco DNA Center(DNAC)管理の基礎知識
- SSL証明書の基礎知識

使用するコンポーネント

このドキュメントは、Cisco DNA Center(DNAC)バージョン2.1.xに基づいています。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

DNSルックアップは、ネットワークデバイスとCisco DNA Center(DNAC)コントローラがリモートサイトにあり、パブリックインターネット経由でネットワークデバイスをプロビジョニングする場合に推奨されるオンボーディング方法です。

Cisco Plug & Play Day0を使用してネットワークデバイスをオンボーディングするには、さまざまな方法があります。

- DHCPベンダー固有のオプション
- DNSルックアップ
- Cisco Cloud Redirection

パブリックインターネット上でセキュアな通信を行うには、DNACにセキュア証明書をインストールする必要があります。このドキュメントに従って、DHCPサーバ、DNSサーバを設定し、SSL証明書を生成してインストールします。すでに証明書+キーがあり、それをDNACにインストールする必要がある場合は、ステップ11のドキュメントに従ってください。このドキュメントでは、次のことを行います。

- Cat9KデバイスはPNPエージェントです。
- pnpserver.cisco.comはDNACコントローラのFQDN名です。
- CiscoスイッチがDNSサーバおよびDHCPサーバとして設定されている。

DNACでのSSL証明書の生成とインストール

デフォルトでは、DNACには、プライベートネットワーク内のネットワークデバイスのオンボーディングに適した自己署名証明書がプリインストールされています。ただし、公衆インターネットを介してリモートの場所からオンボードネットワークデバイスへの安全な通信のために、内部CAから有効なX.509証明書をインポートすることを推奨します。

DNACでシスコが発行したオープンSSL証明書をダウンロードしてインストールする例を次に示します。

証明書をダウンロードするには、まずCSRを作成する必要があります。

手順

ステップ 1：SSHクライアントを使用してCisco DNA Centerクラスタにログインし、**/home/maglev**の下に一時フォルダを作成します。たとえば、ホームディレクトリでコマンド**mkdir tls-cert;cd tls-cert**を入力します。

ステップ 2：先に進む前に、**maglev cluster network display**コマンドを使用して、Cisco DNA Centerの設定時にCisco DNA Centerのホスト名(FQDN)が設定されていることを確認します。

```
Input:

$maglev cluster network display

Output:

cluster_network:
 cluster_dns: 169.254.20.10
  cluster_hostname: fqdn.cisco.com
```

注：このコマンドを実行するには、root権限が必要です。

出力フィールドcluster_hostnameが空であるか、または必要でない場合は、maglev cluster config-updateコマンドを使用してCisco DNA Centerのホスト名(FQDN)を追加または変更します。

```
Input:
```

```
$maglev-config update

Output:

Maglev Config Wizard GUI
```

注：このコマンドを実行するには、root権限が必要です。

入力プロンプトCluster hostnameを含むMAGLEV CLUSTER DETAILSというステップが表示されるまで、**Next**をクリックします。ホスト名を目的のCisco DNA Center FQDNに設定します。**Next**をクリックし、Cisco DNA Centerが新しいFQDNで再設定されるまで続行します。

ステップ 3：任意のテキストエディタを使用して**openssl.cnf**という名前のファイルを作成し、前の手順で作成したディレクトリにアップロードします。この例をガイドとして使用しますが、配置に合わせて調整してください。

- 認証局の管理チームが代わりに2048/sha256を必要とする場合は、default_bitsとdefault_mdを調整します。
- req_distinguished_nameおよびalt_namesセクションの各フィールドに値を指定します。唯一の例外はOUフィールドで、これはオプションです。認証局管理チームで必要とされていない場合は、OUフィールドを省略します。
- 電子メールアドレスのフィールドはオプションです。認証局管理チームが必要としていない場合は省略してください。
- alt_namesセクション：証明書の設定要件は、Cisco DNA Centerのバージョンによって異なります。

Cisco DNA Center証明書でのFQDNの完全なサポートは、Cisco DNA Center 2.1.1以降で利用できます。2.1.1よりも前のバージョンのCisco DNA Centerでは、サブジェクト代替名(SAN)フィールドで定義されたIPアドレスを持つ証明書が必要です。Cisco DNA Centerバージョン2.1.1以降および2.1.1より前のCisco DNA Centerバージョンのalt_namesセクションの設定は、次のとおりです。

Cisco DNA Centerバージョン2.1.1以降：

1. alt_namesセクションには、Webブラウザ、またはPnPやCisco ISEなどの自動化されたプロセスによってCisco DNA Centerにアクセスするために使用されるすべてのDNS名（Cisco DNA CenterのFQDNを含む）が含まれている必要があることに注意してください。alt_namesセクションの最初のDNSエントリには、Cisco DNA CenterのFQDNが含まれている必要があります(DNS.1 = FQDN-of-Cisco-DNA-Center)。Cisco DNA Center FQDNの代わりにワイルドカードDNSエントリを追加することはできませんが、alt-namesセクション（PnPおよびその他のDNSエントリ）の後続のDNSエントリではワイルドカードを使用できます。たとえば、*.example.comは有効なエントリです。

重要：障害復旧のセットアップに同じ証明書を使用する場合は、alt_namesセクションで障害復旧システムサイトのDNSエントリを追加するときにワイルドカードを使用できません。ただし、ディザスタリカバリのセットアップには、別の証明書を使用することをお勧めします。詳細については、『Cisco DNA Center管理者ガイド』の「障害回復証明書の追加」セクションを参照してください。

2. alt_namesセクションには、DNSエントリとしてFQDN-of-Cisco-DNA-Centerが含まれている必要があり、設定ウィザード（入力フィールド「Cluster hostname」内）によるCisco DNA Centerの設定時に設定されたCisco DNA Centerホスト名(FQDN)と一致している必要があります。Cisco DNA Centerは現在、すべてのインターフェイスで1つのホスト名(FQDN)のみをサポート

しています。ネットワーク内のCisco DNA Centerへのデバイス接続にCisco DNA Centerの管理ポートとエンタープライズポートの両方を使用する場合は、DNSクエリーの受信元のネットワークに基づいて、Cisco DNA Centerホスト名(FQDN)の管理IP/仮想IPとエンタープライズIP/仮想IPに解決するようにGeoDNSポリシーを設定する必要があります。ネットワーク内のCisco DNA Centerへのデバイス接続にCisco DNA Centerのエンタープライズポートのみを使用する場合、GeoDNSポリシーの設定は必要ありません。

> **注**:Cisco DNA Centerのディザスタリカバリを有効にしている場合は、DNSクエリの受信元のネットワークに基づいて、Cisco DNA Centerホスト名(FQDN)に対するディザスタリカバリ管理仮想IPとディザスタリカバリのエンタープライズ仮想IPを解決するように、GeoDNSポリシーを設定する必要があります。

3. Cisco DNA Centerバージョン2.1.1より前：

alt_namesセクションには、Webブラウザ、またはPnPやCisco ISEなどの自動化プロセスによってCisco DNA Centerにアクセスするために使用されるすべてのIPアドレスとDNS名が含まれている必要があります（この例では、3ノードのCisco DNA Centerクラスタを想定しています）。スタンドアロンデバイスを使用している場合は、そのノードとVIPに対してのみSANを使用します。後でデバイスをクラスタ化する場合は、新しいクラスタメンバーのIPアドレスを含めるために証明書を再作成する必要があります)。

クラウドインターフェイスが設定されていない場合は、クラウドポートフィールドを省略します。

- extendedKeyUsage拡張では、属性serverAuthとclientAuthは必須です。いずれかの属性を省略すると、Cisco DNA CenterはSSL証明書を拒否します。
- 自己署名証明書をインポートする場合は（推奨されません）、X.509 Basic Constraintsの「CA:TRUE」拡張子を含める必要があります。

openssl.cnfの例（Cisco DNA Centerバージョン2.1.1以降に適用）：

```
req_extensions = v3_req
distinguished_name = req_distinguished_name
default_bits = 4096
default_md = sha512
prompt = no

[req_distinguished_name]

C = <two-letter-country-code>
ST = <state-or-province>
L = <city>
O = <company-name>
OU = MyDivision
CN = FQDN-of-Cisco-DNA-Center
emailAddress = responsible-user@mycompany.tld

[ v3_req ]

basicConstraints = CA:FALSE
keyUsage = digitalSignature, keyEncipherment
extendedKeyUsage=serverAuth,clientAuth
subjectAltName = @alt_names

[alt_names]
```

```
DNS.1 = FQDN-of-Cisco-DNA-Center
DNS.2 = pnpserver.DomainAssignedByDHCPDuringPnP.tld
DNS.3 = *.example.com

!--- Example openssl.cnf (Applicable for Cisco DNA Center versions earlier than 2.1.1)

req_extensions = v3_req
distinguished_name = req_distinguished_name
default_bits = 4096
default_md = sha512
prompt = no

[req_distinguished_name]

C = <two-letter-country-code>
ST = <state-or-province>
L = <city> O = <company-name>
OU = MyDivision
CN = FQDN-of-Cisco-DNA-Center
emailAddress = responsible-user@mycompany.tld

[ v3_req ]

basicConstraints = CA:FALSE
keyUsage = nonRepudiation, digitalSignature, keyEncipherment
extendedKeyUsage=serverAuth,clientAuth
subjectAltName = @alt_names

[alt_names]

DNS.1 = FQDN-of-Cisco-DNA-Center
DNS.2 = pnpserver.DomainAssignedByDHCPDuringPnP.tld
IP.1 = Enterprise port IP node #1
IP.2 = Enterprise port IP node #2
IP.3 = Enterprise port IP node #3
IP.4 = Enterprise port VIP
IP.5 = Cluster port IP node #1
IP.6 = Cluster port IP node #2
IP.7 = Cluster port IP node #3
IP.8 = Cluster port VIP
IP.9 = GUI port IP node #1
IP.10 = GUI port IP node #2
IP.11 = GUI port IP node #3
IP.12 = GUI port VIP
IP.13 = Cloud port IP node #1
IP.14 = Cloud port IP node #2
IP.15 = Cloud port IP node #3
IP.16 = Cloud port VIP
```

> **注**:**openssl.cnf**ファイルにクラスタIPアドレスを含めない場合は、ソフトウェアイメージのアクティベーションをスケジュールできません。この問題を解決するには、クラスタIPアドレスをSANとして証明書に追加します。

任意のテキスト工ディタを使用して**openssl.cnf**という名前のファイルを作成し、前の手順で作成したディレクトリにアップロードします。この例をガイドとして使用しますが、配置に合わせて調整してください。

- 認証局の管理チームが代わりに2048/sha256を必要とする場合は、default_bitsとdefault_mdを調整します。
- req_distinguished_nameおよびalt_namesセクションの各フィールドに値を指定します。唯一

の例外はOUフィールドで、これはオプションです。認証局管理チームで必要とされていない場合は、OUフィールドを省略します。
- emailAddressフィールドはオプションです。認証局の管理チームが必要としていない場合は省略してください。
- alt_namesセクション：証明書の設定要件は、Cisco DNA Centerのバージョンによって異なります。
- FQDNのサポートは、Cisco DNA Center 2.1.1以降で利用できます。2.1.1よりも前のバージョンのCisco DNA Centerでは、サブジェクト代替名(SAN)にIPアドレスを含む証明書が必要です。Cisco DNA Centerバージョン2.1.1以降および2.1.1より前のCisco DNA Centerバージョンのalt_namesセクションの設定は、次のとおりです。
- Cisco DNA Centerバージョン2.1.1以降：alt_namesセクションには、Webブラウザ、またはPnPやCisco ISEなどの自動化されたプロセスによってCisco DNA Centerにアクセスするために使用されるすべてのDNS名（Cisco DNA CenterのFQDNを含む）が含まれている必要があります。このセクションには、注意が必要です。alt_namesセクションの最初のDNSエントリには、Cisco DNA CenterのFQDNが含まれている必要があります(DNS.1 = FQDN-of-Cisco-DNA-Center)。Cisco DNA CenterのFQDNの代わりにワイルドカードDNSエントリを追加することはできません。ただし、alt-namesセクションの後続のDNSエントリ（PnPおよびその他のDNSエントリ）では、ワイルドカードを使用できます。たとえば、*.example.comは有効なエントリです。

重要：障害復旧のセットアップに同じ証明書を使用する場合は、alt_namesセクションで障害復旧システムサイトのDNSエントリを追加するときにワイルドカードを使用できません。ただし、ディザスタリカバリのセットアップには、別の証明書を使用することをお勧めします。詳細については、『Cisco DNA Center管理者ガイド』の「障害回復証明書の追加」セクションを参照してください。

- alt_namesセクションには、DNSエントリとしてFQDN-of-Cisco-DNA-Centerが含まれている必要があります。また、設定ウィザード（入力フィールド「Cluster hostname」）を使用してCisco DNA Centerを設定するときに設定されたCisco DNA Centerホスト名(FQDN)と一致している必要があります。

Cisco DNA Centerは現在、すべてのインターフェイスで1つのホスト名(FQDN)のみをサポートしています。GeoDNSポリシーを設定して、DNSクエリを受信するネットワークに基づいて、Cisco DNA Centerホスト名(FQDN)の管理IP/仮想IPおよびエンタープライズIP/仮想IPに解決する必要があります。

注:Cisco DNA Centerのディザスタリカバリを有効にしている場合は、DNSクエリの受信元のネットワークに基づいて、Cisco DNA Centerホスト名(FQDN)に対するディザスタリカバリ管理仮想IPとディザスタリカバリのエンタープライズ仮想IPを解決するように、GeoDNSポリシーを設定する必要があります。

- 2.1.1より前のバージョンのCisco DNA Center:

alt_namesセクションには、Webブラウザ、またはPnPやCisco ISEなどの自動化プロセスによってCisco DNA Centerにアクセスするために使用されるすべてのIPアドレスとDNS名が含まれている必要があります（この例では、3ノードのCisco DNA Centerクラスタを想定しています）。スタンドアロンデバイスを使用している場合は、そのノードとVIPに対してのみSANを使用します。後でデバイスをクラスタ化する場合は、新しいクラスタメンバーのIPアドレスを含めるために証明書を再作成する必要があります)。

- クラウドインターフェイスが設定されていない場合は、クラウドポートフィールドを省略し

ます。

- extendedKeyUsage拡張では、属性serverAuthとclientAuthは必須です。いずれかの属性を省略すると、Cisco DNA CenterはSSL証明書を拒否します。
- 自己署名証明書をインポートする場合は（推奨されません）、X.509 Basic Constraintsの「CA:TRUE」拡張子を含める必要があります。

openssl.cnfの例(Cisco DNA Centerバージョン2.1.1以降に適用)

```
req_extensions = v3_reqdistinguished_name = req_distinguished_namedefault_bits = 4096default_md
= sha512prompt = no[req_distinguished_name]C = <two-letter-country-code>ST = <state-or-
province>L
= <city>O = <company-name>OU = MyDivisionCN = FQDN-of-Cisco-DNA-CenteremailAddress =
responsible-user@mycompany.tld [ v3_req ]basicConstraints = CA:FALSEkeyUsage = digitalSignature,
keyEnciphermentextendedKeyUsage=serverAuth,clientAuthsubjectAltName = @alt_names[alt_names]DNS.1
=
FQDN-of-Cisco-DNA-CenterDNS.2 = pnpserver.DomainAssignedByDHCPDuringPnP.tldDNS.3 = *.example.com
```

openssl.cnfの例(2.1.1より前のバージョンのCisco DNA Centerに適用)

```
req_extensions = v3_reqdistinguished_name = req_distinguished_namedefault_bits = 4096default_md
= sha512prompt = no[req_distinguished_name]C = <two-letter-country-code>ST = <state-or-
province>L
= <city> O = <company-name>OU = MyDivisionCN = FQDN-of-Cisco-DNA-Centeron-GUI-portemailAddress =
responsible-user@mycompany.tld[ v3_req ]basicConstraints = CA:FALSEkeyUsage = nonRepudiation,
digitalSignature, keyEnciphermentextendedKeyUsage=serverAuth,clientAuthsubjectAltName =
@alt_names[alt_names]DNS.1 = FQDN-of-Cisco-DNA-Center-on-GUI-portDNS.2 =
FQDN-of-Cisco-DNA-Center-on-enterprise-portDNS.3 =
pnpserver.DomainAssignedByDHCPDuringPnP.tldIP.1 =
Enterprise port IP node #1IP.2 = Enterprise port IP node #2IP.3 = Enterprise port IP node #3IP.4
=
Enterprise port VIPIP.5 = Cluster port IP node #1IP.6 = Cluster port IP node #2IP.7 =
Cluster port IP node #3IP.8 = Cluster port VIPIP.9 = GUI port IP node #1IP.10 = GUI port IP node
#2IP.11
= GUI port IP node #3IP.12 = GUI port VIPIP.13 = Cloud port IP node #1IP.14 = Cloud port IP node
#2IP.15
= Cloud port IP node #3IP.16 = Cloud port VIP
```

注:**openssl.cnf**ファイルにクラスタIPアドレスを含めない場合は、ソフトウェアイメージのアクティベーションをスケジュールできません。この問題を解決するには、クラスタIPアドレスをSANとして証明書に追加します。

この場合、次の出力は**openssl.conf**

```
req_extensions = v3_req
distinguished_name = req_distinguished_name
default_bits = 4096
default_md = sha512
prompt = no

[req_distinguished_name]

C = US
ST = California
L = Milpitas
O = Cisco Systems Inc.
OU = MyDivision
CN = noc-dnac.cisco.com
emailAddress = sit-noc-team@cisco.com
```

```
[ v3_req ]

basicConstraints = CA:FALSE
keyUsage = digitalSignature, keyEncipherment
extendedKeyUsage=serverAuth,clientAuth
subjectAltName = @alt_names

[alt_names]

DNS.1 = noc-dnac.cisco.com
DNS.2 = pnpserver.cisco.com
IP.1 = 10.10.0.160
IP.2 = 10.29.51.160
```

ステップ 4：秘密キーを作成するには、次のコマンドを入力します。認証局の管理チームから要求があれば、キーの長さを2048に調整します。**openssl genrsa -out csr.key 4096**

ステップ 5：フィールドが**openssl.cnf**ファイルに入力されたら、前の手順で作成した秘密キーを使用して証明書署名要求(CSR)を生成します。

```
openssl req -config openssl.cnf -new -key csr.key -out DNAC.csr
```

手順 6：証明書署名要求(CSR)の内容を確認し、[サブジェクト代替名(Subject Alternative Name)]フィールドにDNS名（およびバージョン2.1.1より前のCisco DNA CenterのIPアドレス）が正しく入力されていることを確認します。

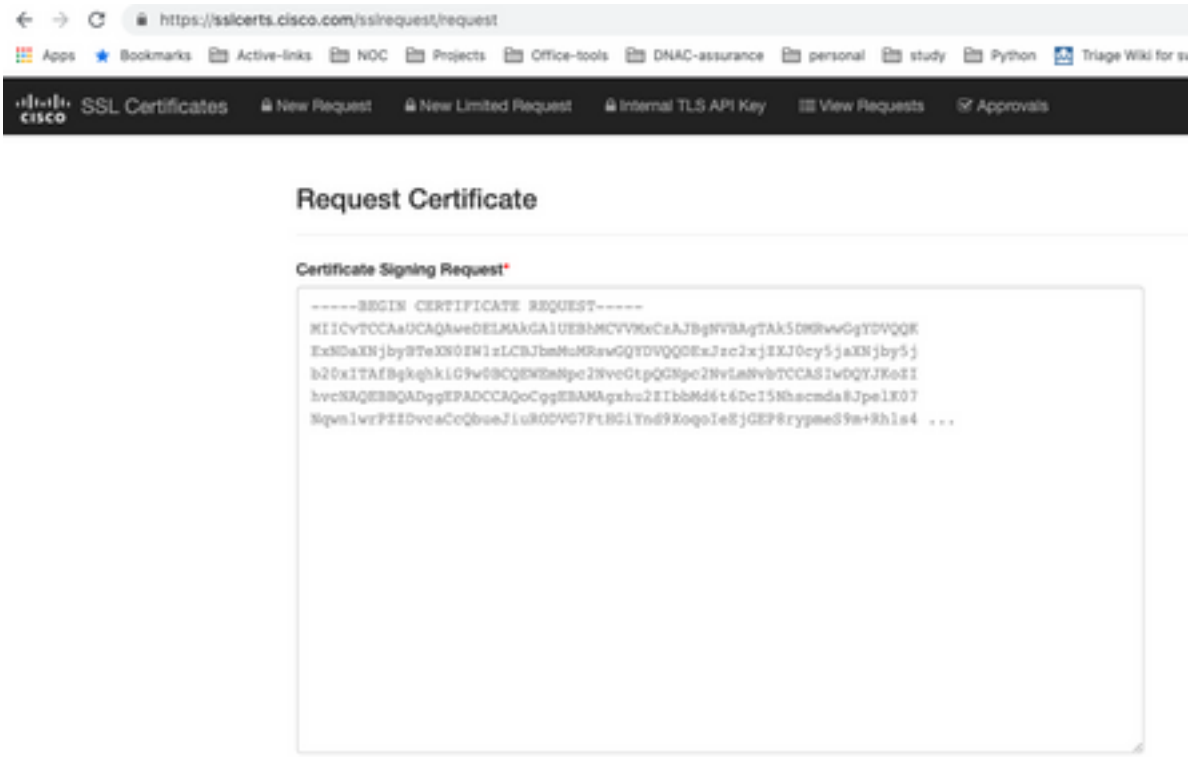
```
openssl req -text -noout -verify -in DNAC.csr
```

手順 7：証明書署名要求(CSR)をコピーしてCAに貼り付けます（Cisco Open SSLなど）。

証明書をダウンロードするリンクに移動します。Cisco SSL証明書

[Request Certificate]をクリックして、永続的な証明書をダウンロードします。

または、[Request Limited Test certificate]をクリックして目的を限定します。



ユーザは証明書情報を含む電子メールを受信します。右クリックして、ラップトップ上の3つのPEMファイルをすべてダウンロードします。この例では、3つの個別のファイルを受け取ったので、ステップ8をスキップしてステップ9に進みます。

ステップ 8： 証明書発行者が証明書のフルチェーン（サーバとCA）をp7bで提供する場合：

p7bバンドルをDER形式でダウンロードし、**dnac-chain.p7b**という名前で保存します。

SSHを介してdnac-chain.p7b証明書をCisco DNA Centerクラスタにコピーします。

次のコマンドを入力します。

```
openssl pkcs7 -in dnac-chain.p7b -inform DER -out dnac-chain.pem -print_certs
```

ステップ 9：証明書発行者がlooseファイルで証明書とその発行者CAチェーンを提供する場合：

PEM(base64)ファイルをダウンロードするか、opensslを使用してDERをPEMに変換します。

証明書と発行者CAを連結し、証明書から開始し、下位CAをルートCAまで続けて、それをdnac-chain.pemファイルに出力します。

```
cat certificate.cer subCA.cer rootCA.cer > dnac-chain.pem
```

ステップ 10：ラップトップから、上で作成したtls-cert dirにあるCisco DNA Centerにファイルdnac-chain.pemをコピーします。

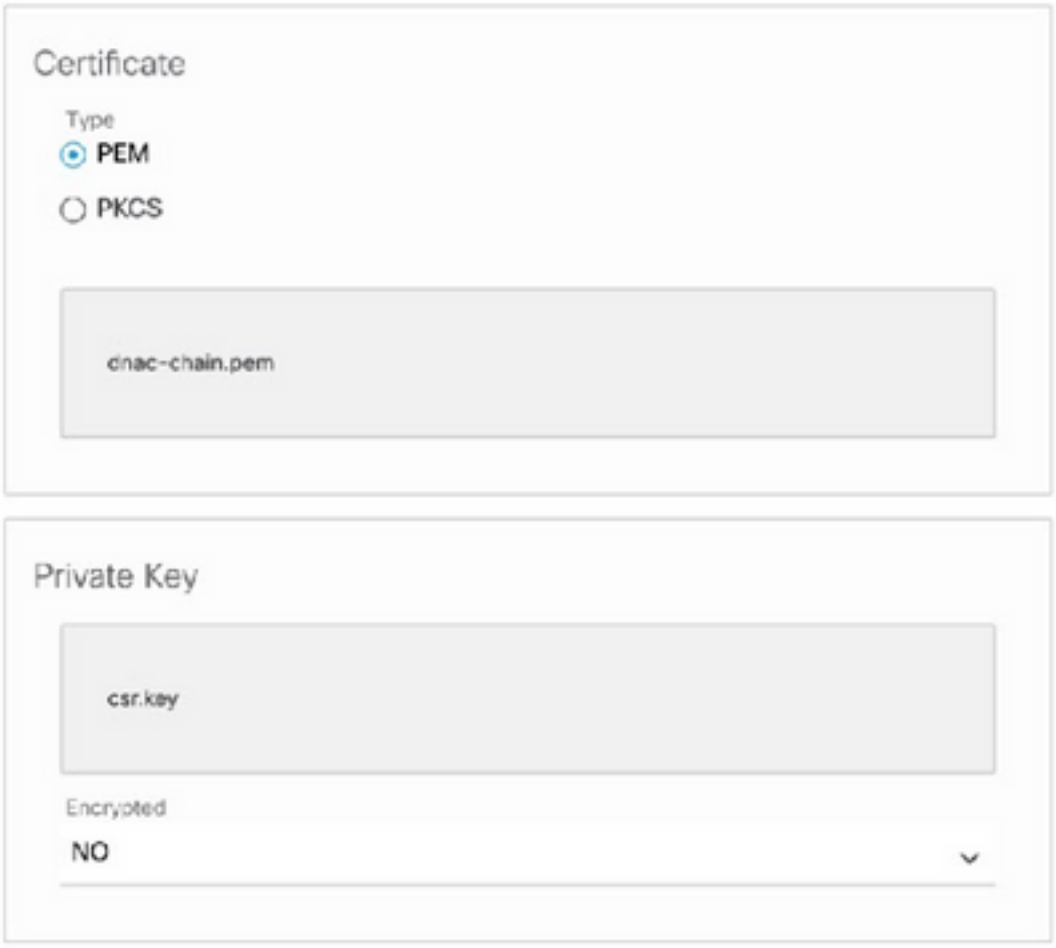
ステップ 11Cisco DNA CenterのGUIで、メニューアイコン()をクリックし、[System] > [Settings] > [Certificates]を選択します。

ステップ 12[Replace Certificate]をクリックします。

ステップ 13[Certificate]フィールドで[PEM]オプションボタンをクリックし、次のタスクを実行し

ます。

- [Certificate]フィールドで、**dnac-chain.pem**ファイルをインポートします。このファイルを[Drag n' Drop a File Here]フィールドにドラッグアンドドロップするだけです。
- [Private Key]フィールドで、秘密キー(csr.key)をインポートします。このファイルを[Drag n' Drop a File Here]フィールドにドラッグアンドドロップします。
- 秘密キーの[Encrypted]ドロップダウンリストから[No]を選択します。



ステップ 14：[Upload/Activate]をクリックします。DNACからログアウトし、再度ログインします。

DHCP サーバの設定

DHCPサーバプールを設定して、DUTにIPアドレスを割り当てます。DHCPサーバも設定します。

ドメイン名とDNSサーバのIPアドレスを送信します。

```
ip dhcp pool PNP-A4
 network 192.0.2.0 255.255.255.252
 default-router 192.0.2.2
 domain-name cisco.com
 dns-server 203.0.113.23
```

DNSサーバの設定ネットワーク内のDNSサーバを設定して、DNACのFQDN名を解決します。

```
 ip dns server
```

```
 ip host pnpserver.cisco.com <dnac-controller-ip>
```

ステップ 1：オンボーディングされる新しいデバイスがケーブル接続され、電源がオンになります。NVRAMのスタートアップコンフィギュレーションが空であるため、PnPエージェントがトリガーされ、DHCP DISCOVERメッセージでDHCPオプション60の「Cisco PnP」が送信されます。

ステップ 2：DHCPサーバは、オプション60の「Cisco PnP」を認識するように設定されていないため、オプション60を無視します。DHCPサーバはIPアドレスを割り当て、設定されたドメイン名とDNSサーバのIPアドレスとともにDHCPオファーを送信します。

ステップ 3：PnPエージェントはドメイン名を読み取り、完全修飾PnPサーバのホスト名を作成し、そのドメイン名を文字列「pnpserver」に追加します。ドメイン名が「example.com」の場合、PnPサーバの完全修飾ホスト名は「pnpserver.example.com」になります。PnPエージェントは、DHCPオプションで受信したDNSサーバを使用して、IPアドレスの「pnpserver.example.com」を解決します。

オンボーディングのためにPNPエージェントがトリガーされた場合の例：

新しいスイッチの電源を入れるか、または「write erase」を実行し、その後、ブラウンのフィールド展開の場合はリロードします。

スイッチコンソールで次のワークフローを確認します。

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

*Jan 19 22:23:21.981: %IOSXE-0-PLATFORM: R0/0: udev: disk0: has been inserted

Autoinstall trying DHCPv6 on Vlan1

Autoinstall trying DHCPv4 on Vlan1

Autoinstall trying DHCPv6 on Vlan1

Redundant RPs -

Autoinstall trying DHCPv6 on Vlan119

Autoinstall trying DHCPv6 on Vlan119

Acquired IPv4 address 192.0.2.3 on Interface Vlan119

Received following DHCPv4 options:

       domain-name     : cisco.com
       dns-server-ip   : 203.0.113.23
       si-addr         : 203.0.113.21

stop Autoip process

OK to enter CLI now...

pnp-discovery can be monitored without entering enable mode

Entering enable mode will stop pnp-discovery

Autoinstall trying DHCPv6 on Vlan119

Guestshell destroyed successfully
```

```
Autoinstall trying DHCPv6 on Vlan119

Press RETURN to get started!
```

関連情報

- PnPサーバの検出
- Cisco DNA Centerセキュリティベストプラクティスガイド
- **テクニカル サポートとドキュメント – Cisco Systems**

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。