安全網路裝置調配

目錄

簡介

本文檔介紹思科裝置通過DNS查詢安全加入網路的逐步方法。

必要條件

需求

- Cisco DNA Center(DNAC)管理基礎知識
- SSL憑證的基本知識

採用元件

本檔案是根據Cisco DNA Center(DNAC)版本2.1.x。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

當網路裝置和思科DNA中心(DNAC)控制器位於遠端站點，並且您想要通過公共網際網路調配網路裝置時，推薦使用DNS查詢。

使用思科即插即用第0天時，可以使用不同的方法來加入網路裝置。

- DHCP廠商專屬選項
- DNS查詢
- 思科雲端重新導向

為了通過公共Internet進行安全通訊，您需要在DNAC上安裝安全證書。按照本文檔設定DHCP伺服器、DNS伺服器、生成並安裝SSL證書。如果您已經有憑證+金鑰，且只需將其安裝在DNAC上，則請依照步驟11中的檔案操作。在本檔案中：

- Cat9K裝置是PNP代理。
- pnpserver.cisco.com是DNAC控制器的FQDN名稱。
- Cisco交換機配置為DNS伺服器和DHCP伺服器。

在DNAC上生成和安裝SSL證書

預設情況下，DNAC隨附預安裝的自簽名證書，該證書可用於在專用網路中載入網路裝置。但是，思科建議您從您的內部CA匯入有效的X.509證書，以便通過公共Internet從遠端位置安全地與板載網路裝置通訊。

以下範例顯示在DNAC上下載和安裝思科發出的Open SSL憑證。

若要下載憑證，您必須首先建立CSR。

程式

步驟1.使用SSH客戶端登入到Cisco DNA Center群集並在**/home/maglev**下建立一個臨時資料夾，例如，在home目錄中輸入**mkdir tls-cert;cd tls-cert**命令。

步驟2.在繼續操作之前，請確保使用**maglev cluster network display**命令在Cisco DNA Center配置時設定Cisco DNA Center主機名(FQDN):

```
Input:

$maglev cluster network display

Output:

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

註：您需要具有root許可權才能運行此命令。

如果輸出欄位cluster_hostname為空或不是您想要的，請使用maglev cluster config-update命令新增或更改Cisco DNA Center主機名(FQDN):

```
Input:

$maglev-config update

Output:

Maglev Config Wizard GUI
```

註：您需要具有root許可權才能運行此命令。

按一下**下一步**，直到看到標題為MAGLEV CLUSTER DETAILS的步驟，該步驟包含輸入提示符Cluster hostname。將主機名設定為所需的Cisco DNA Center FQDN。按一下**Next**並繼續，直到用新的FQDN重新配置Cisco DNA Center。

步驟3.使用您選擇的文本編輯器，建立一個名為**openssl.cnf**的檔案，並將其上傳到您在上一步中建立的目錄中。請將此示例用作指南，但請對其進行調整以適應您的部署。

- 如果您的憑證授權管理團隊需要2048/sha256，請調整default_bits和default_md。
- 在req_distinguished_name和alt_names節中為每個欄位指定值。唯一的例外是OU欄位，它是可選的。如果您的證書頒發機構管理團隊不需要，請忽略OU欄位。
- 電子郵件地址欄位是可選的；如果您的證書頒發機構管理團隊不需要，請忽略該欄位。
- alt_names部分：證書配置要求因Cisco DNA Center版本而異。

從Cisco DNA Center 2.1.1開始，可以獲得Cisco DNA Center證書中對FQDN的完全支援。對於低於2.1.1的Cisco DNA Center版本，您需要具有在Subject Alternative Name(SAN)欄位中定義的IP地址的證書。Cisco DNA Center 2.1.1及更高版本以及2.1.1之前的Cisco DNA Center版本的alt_names部分配置如下：

Cisco DNA Center 2.1.1及更高版本：

1.密切注意alt_names部分，該部分必須包含用於通過Web瀏覽器或通過自動進程（如PnP或Cisco ISE）訪問Cisco DNA Center的所有DNS名稱（包括Cisco DNA Center FQDN）。alt_names部分中的第一個DNS條目必須包含Cisco DNA Center FQDN(DNS.1 = FQDN-of-Cisco-DNA-Center)。您無法新增萬用字元DNS條目來代替Cisco DNA Center FQDN，但可以在alt-names部分中的後續DNS條目中使用萬用字元（對於PnP和其他DNS條目）。例如，*.example.com是有效條目。

重要資訊：如果您將同一證書用於災難恢復設定，則在alt_names部分為災難恢復系統站點新增DNS條目時，不允許使用萬用字元。但是，我們建議您將單獨的證書用於災難恢復設定。有關詳細資訊，請參閱Cisco DNA Center管理員指南中的「新增災難恢復證書」部分。

2. alt_names部分必須包含作為DNS條目的Cisco-DNA-Center的FQDN，並且必須匹配通過配置嚮導（在輸入欄位「Cluster hostname」中）在Cisco DNA Center配置時設定的Cisco DNA Center主機名(FQDN)。Cisco DNA Center當前僅支援所有介面的一個主機名(FQDN)。如果將Cisco DNA Center上的管理和企業埠用於連線到網路中思科DNA中心的裝置，則必須配置GeoDNS策略，以便根據接收DNS查詢的網路解析為思科DNA中心主機名(FQDN)的管理IP/虛擬IP和企業IP/虛擬IP。如果僅使用Cisco DNA Center上的企業埠來連線網路中與Cisco DNA Center連線的裝置，則無需設定GeoDNS策略。

> **註**：如果您已為Cisco DNA Center啟用災難恢復，則必須配置GeoDNS策略，以便根據接收DNS查詢的網路為Cisco DNA Center主機名(FQDN)解析災難恢復管理虛擬IP和災難恢復企業虛擬IP。

3.低於2.1.1的Cisco DNA Center版本：

密切注意alt_names部分，該部分必須包含用於訪問Cisco DNA Center的所有IP地址和DNS名稱(通過Web瀏覽器或通過自動進程（如PnP或Cisco ISE）。(此示例假設三節點Cisco DNA Center集群。如果您有獨立裝置，請僅為該節點和VIP使用SAN。如果以後對裝置進行集群，則需要重新建立證書以包含新集群成員的IP地址。)

如果未配置雲介面，則忽略雲埠欄位。

- 在extendedKeyUsage擴展中，屬性serverAuth和clientAuth是必需的。如果忽略其中任一屬性，Cisco DNA Center將拒絕SSL證書。
- 如果匯入自簽名證書（不推薦），則必須包含X.509基本約束「CA:TRUE」副檔名。

openssl.cnf範例（適用於Cisco DNA Center 2.1.1版及更新版本）：

```
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
```

註：如果在**openssl.cnf**檔案中不包括集群IP地址，則無法計畫軟體映像啟用。要解決此問題，請將集群IP地址作為SAN新增到證書中。

使用您選擇的文本編輯器，建立一個名為**openssl.cnf**的檔案，並將其上傳到您在上一步中建立的目錄中。請將此示例用作指南，但請對其進行調整以適應您的部署。

- 如果您的憑證授權管理團隊需要2048/sha256，請調整default_bits和default_md。
- 在req_distinguished_name和alt_names節中為每個欄位指定值。唯一的例外是OU欄位，它是可選的。如果您的證書頒發機構管理團隊不需要，請忽略OU欄位。
- emailAddress欄位是可選的；如果您的證書頒發機構管理團隊不需要，請忽略該欄位。
- alt_names部分：證書配置要求因Cisco DNA Center版本而異。
- 從Cisco DNA Center 2.1.1開始，FQDN支援可用。對於低於2.1.1的Cisco DNA Center版本，您需要一個證書，其IP地址應包含在主體備用名稱(SAN)中。Cisco DNA Center 2.1.1及更高版本以及2.1.1之前的Cisco DNA Center版本的alt_names部分配置如下：
- Cisco DNA Center 2.1.1及更高版本：密切注意alt_names部分，該部分必須包含用於通過Web瀏覽器或自動進程（如PnP或Cisco ISE）訪問Cisco DNA Center的所有DNS名稱（包括Cisco DNA Center FQDN）。alt_names部分中的第一個DNS條目必須包含Cisco DNA Center的FQDN(DNS.1 = FQDN-of-Cisco-DNA-Center)。您無法新增萬用字元DNS條目代替Cisco DNA Center的FQDN。但是您可以在alt-names部分的後續DNS條目中使用萬用字元（對於PnP和其他DNS條目）。例如，*.example.com是有效的條目。

重要資訊：如果您將同一證書用於災難恢復設定，則在alt_names部分為災難恢復系統站點新增DNS條目時，不允許使用萬用字元。但是，我們建議您將單獨的證書用於災難恢復設定。有關詳細資訊，請參閱Cisco DNA Center管理員指南中的「新增災難恢復證書」部分。

- alt_names部分必須包含FQDN-of-Cisco-DNA-Center作為DNS條目，並且必須匹配通過配置嚮導（在輸入欄位「Cluster hostname」中）在Cisco DNA Center配置時設定的Cisco DNA Center主機名(FQDN)。

Cisco DNA Center當前僅支援所有介面的一個主機名(FQDN)。您必須配置GeoDNS策略，以根據接收DNS查詢的網路解析為Cisco DNA Center主機名(FQDN)的管理IP/虛擬IP和企業IP/虛擬IP。

註：如果您已為Cisco DNA Center啟用災難恢復，則必須配置GeoDNS策略，以便根據接收DNS查詢的網路為Cisco DNA Center主機名(FQDN)解析災難恢復管理虛擬IP和災難恢復企業虛擬IP。

- 低於2.1.1的Cisco DNA Center版本：

密切注意alt_names部分，該部分必須包含用於訪問Cisco DNA Center的所有IP地址和DNS名稱(通過Web瀏覽器或通過自動進程（如PnP或Cisco ISE）。(此示例假設三節點Cisco DNA Center集群。如果您有獨立裝置，請僅為該節點和VIP使用SAN。如果以後對裝置進行集群，則需要重新建立證書以包含新集群成員的IP地址。)

- 如果未配置雲介面，則忽略雲埠欄位。
  - 在extendedKeyUsage擴展中，屬性serverAuth和clientAuth是必需的。如果忽略其中任一屬性，Cisco DNA Center將拒絕SSL證書。
  - 如果匯入自簽名證書（不推薦），則必須包含X.509基本約束「CA:TRUE」副檔名。

openssl.cnf範例(適用於Cisco DNA Center 2.1.1版及更新版本)

```
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範例(適用於2.1.1之前的Cisco DNA Center版本)

```
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
```

註：如果在**openssl.cnf**檔案中不包括集群IP地址，則無法計畫軟體映像啟用。要解決此問題，請將集群IP地址作為SAN新增到證書中。

在這種情況下，下一個輸出是**openssl.conf的設定**

```
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
```

步驟4.輸入以下命令以建立私鑰。如果您的憑證授權管理團隊需要，將金鑰長度調整為2048。

openssl genrsa -out csr.key 4096

步驟5.在**openssl.cnf**檔案中填充欄位後，使用您在上一步中建立的私密金鑰產生憑證簽署請求。

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

步驟6.驗證證書簽名請求內容，並確保在Subject Alternative Name欄位中正確填寫DNS名稱（以及低於2.1.1的Cisco DNA Center版本的IP地址）。

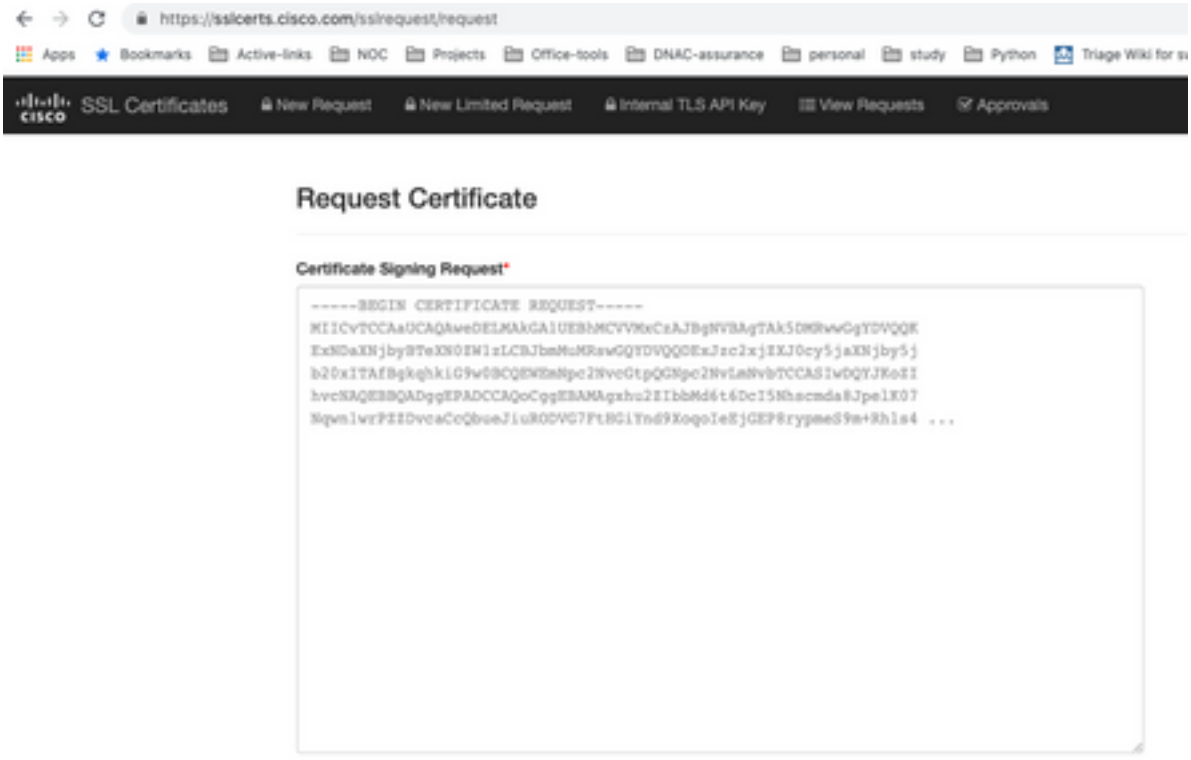
```
openssl req -text -noout -verify -in DNAC.csr
```

步驟7.複製憑證簽署請求，並將其貼上到CA（例如Cisco Open SSL）。

前往連結下載憑證。[Cisco SSL憑證]

按一下「Request Certificate」下載永久證書。

或者，點選「Request Limited Test certificate」（請求受限測試證書）以限制用途。



使用者會收到含有憑證資訊的電子郵件。按一下右鍵並下載筆記型電腦上的所有三個PEM檔案。在本例中，我收到了3個單獨的檔案，因此請跳過步驟8並繼續步驟9。

步驟8. 如果證書頒發者在p7b中提供證書完整鏈（伺服器和CA）：

下載DER格式的p7b捆綁包，並將其儲存為**dnac-chain.p7b**。

通過SSH將dnac-chain.p7b證書複製到Cisco DNA Center集群。

輸入以下命令：

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

步驟9.如果證書頒發者以鬆散檔案形式提供證書及其頒發者CA鏈：

下載PEM(base64)檔案或使用openssl將DER轉換為PEM。

將證書及其頒發者CA串聯，從證書開始，接著從屬CA一直連線到根CA，然後將其輸出到dnac-chain.pem檔案。

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

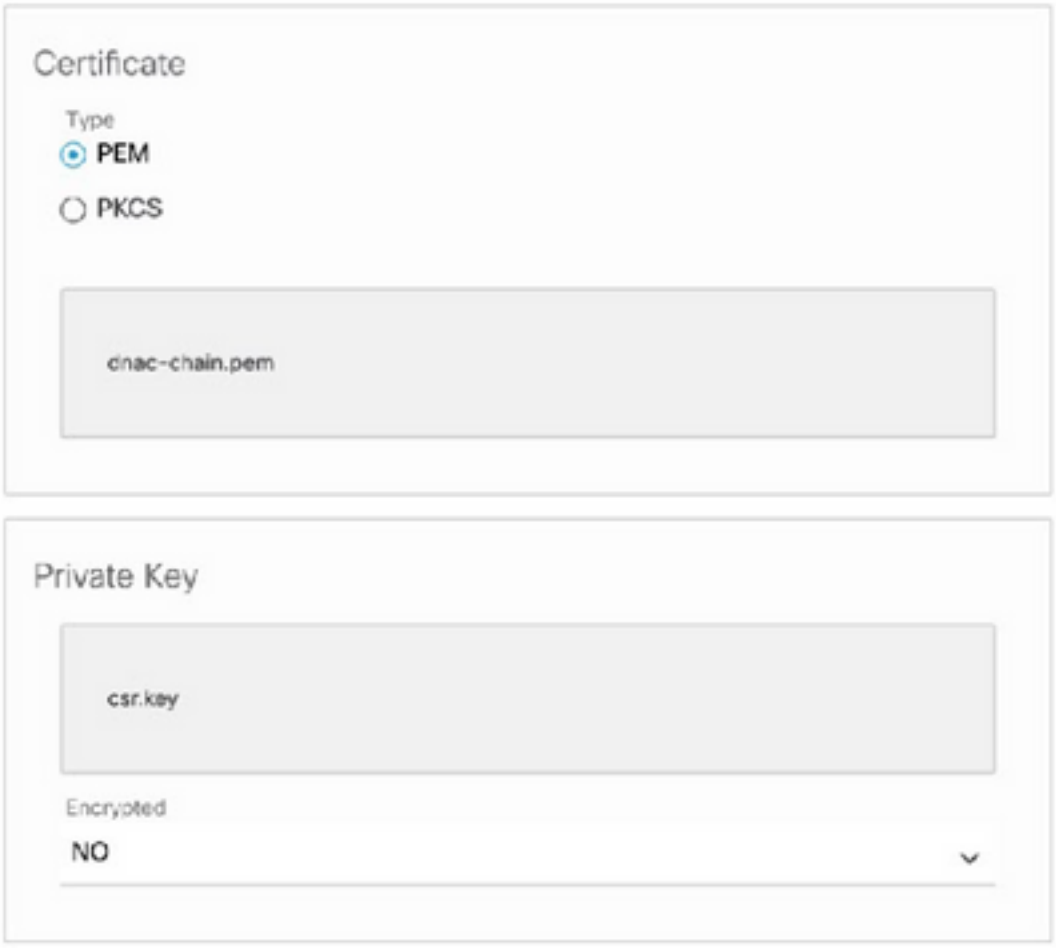
步驟10.在上方建立的tls-cert dir中，將檔案dnac-chain.pem從筆記型電腦複製到Cisco DNA Center。

步驟11.在Cisco DNA Center GUI中，點選選單圖示()，然後選擇System > Settings > Certificates。

步驟12.按一下替換證書。

步驟13.在Certificate欄位中，點選PEM單選按鈕並執行後續任務。

- 對於Certificate欄位，請匯入**dnac-chain.pem**檔案，然後將此檔案拖放到Drag n' Drop a File Here欄位中。
- 對於Private Key欄位，匯入私鑰(csr.key)，只需將此檔案拖放到Drag n' Drop a File Here欄位。
- 從私鑰的Encrypted下拉選單中選擇No。



步驟14.按一下「Upload/Activate」。註銷並重新登入DNAC。

DHCP伺服器配置

配置DHCP伺服器池以將IP地址分配給DUT。另外配置DHCP伺服器

傳送域名和DNS伺服器IP地址。

```
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伺服器配置。在網路中配置DNS伺服器以解析DNAC的FQDN名稱。

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

步驟1.要安裝的新裝置通過電纜連線並通電。由於NVRAM中的啟動配置為空，因此會觸發PnP代理，並在DHCP發現消息的DHCP選項60中傳送「Cisco PnP」。

步驟2.DHCP伺服器未配置為識別選項60中的「Cisco PnP」，而是忽略選項60。DHCP伺服器分配IP地址並傳送DHCP提供以及配置的域名和DNS伺服器IP地址。

步驟3.PnP代理讀取域名並形成完全限定的PnP伺服器主機名，並將域名附加到字串「pnpserver」。如果域名是「example.com」，則PnP伺服器的完全限定主機名將是「pnpserver.example.com」。PnP代理使用在DHCP選項中接收的DNS伺服器為其IP地址解析「pnpserver.example.com」。

例如，為自註冊觸發pnp代理：

在新交換機上通電或「寫擦除」，然後重新載入，以防棕色現場部署

驗證交換機控制檯上的下一工作流程。

```
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!
```

相關資訊

- PnP伺服器發現
- 思科DNA中心安全最佳實踐指南
- 技術支援與文件 - Cisco Systems

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。