安全网络设备调配

目录

简介

本文档介绍思科设备通过DNS查找安全加入网络的分步方法。

先决条件

要求

- Cisco DNA Center(DNAC)管理基础知识
- SSL证书的基本知识

使用的组件

本文档基于Cisco DNA Center(DNAC)版本2.1.x。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

当网络设备和思科DNA中心(DNAC)控制器位于远程站点，并且您希望通过公共互联网调配网络设备时，推荐使用DNS查找进行登录。

可以使用思科即插即用第0天功能加入网络设备，方法多种多样。

- DHCP供应商特定选项
- DNS查找
- 思科云重定向

为了通过公共互联网进行安全通信，您需要在DNAC上安装安全证书。按照本文档设置DHCP服务器、DNS服务器，生成并安装SSL证书。如果您已经拥有证书+密钥，并且只需将其安装在DNAC上，则按照步骤11中的文档进行操作。在本文档中：

- Cat9K设备是PNP代理。
- pnpserver.cisco.com是DNAC控制器的FQDN名称。
- Cisco交换机配置为DNS服务器和DHCP服务器。

在DNAC上生成和安装SSL证书

默认情况下，DNAC附带预安装的自签名证书，可用于在专用网络中载入网络设备。但是，思科建议您从内部CA导入有效的X.509证书，以便通过公共互联网从远程位置安全地与板载网络设备通信。

以下是下载和安装思科在DNAC上颁发的Open SSL证书的示例。

要下载证书，您必须首先创建CSR。

步骤

步骤1:使用SSH客户端登录到Cisco DNA Center集群，并在**/home/maglev**下创建临时文件夹，例如，在主目录中输入**mkdir tls-cert;cd tls-cert**命令。

第二步：在继续操作之前，请确保在Cisco DNA Center配置时使用**maglev cluster network display**命令设置Cisco DNA Center主机名(FQDN):

```
Input:

$maglev cluster network display

Output:

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

注：您需要具有root权限才能运行此命令。

如果输出字段cluster_hostname为空或不是您想要的，请使用maglev cluster config-update命令添加或更改Cisco DNA Center主机名(FQDN):

```
Input:

$maglev-config update

Output:

Maglev Config Wizard GUI
```

注：您需要具有root权限才能运行此命令。

单击**Next**，直到看到标题为MAGLEV CLUSTER DETAILS的步骤，该步骤包含输入提示符Cluster hostname。将主机名设置为所需的Cisco DNA Center FQDN。单击**Next**并继续，直到使用新的FQDN重新配置Cisco DNA Center。

第三步：使用您选择的文本编辑器，创建一个名为**openssl.cnf**的文件，然后将其上传到您在上一步中创建的目录。请将此示例用作指南，但请对其进行调整以适应您的部署。

- 如果您的证书颁发机构管理团队需要2048/sha256，请调整default_bits和default_md。
- 指定req_distinguished_name和alt_names部分中每个字段的值。唯一的例外是OU字段，该字段是可选的。如果您的证书颁发机构管理团队不需要此字段，请省略OU字段。
- 电子邮件地址字段是可选的；如果您的证书颁发机构管理员团队不需要该字段，请省略该字段。
- alt_names部分：证书配置要求因Cisco DNA Center版本而异。

从Cisco DNA Center 2.1.1开始，Cisco DNA Center证书中提供FQDN的完全支持。对于早于2.1.1的Cisco DNA Center版本，您需要具有在Subject Alternative Name(SAN)字段中定义的IP地址的证书。Cisco DNA Center 2.1.1版及更高版本以及2.1.1版之前的Cisco DNA Center版本的alt_names部分配置如下：

Cisco DNA Center版本2.1.1及更高版本：

1.密切注意alt_names部分，该部分必须包含用于通过Web浏览器或自动进程（例如PnP或Cisco ISE）访问Cisco DNA Center的所有DNS名称（包括Cisco DNA Center FQDN）。alt_names部分中的第一个DNS条目必须包含Cisco DNA Center FQDN(DNS.1 = FQDN-of-Cisco-DNA-Center)。您无法添加通配符DNS条目来代替Cisco DNA Center FQDN，但您可以在后续DNS条目的alt-names部分使用通配符（对于PnP和其他DNS条目）。例如，*.example.com是有效条目。

重要信息：如果您将同一证书用于灾难恢复设置，则在alt_names部分中为灾难恢复系统站点添加DNS条目时，不允许使用通配符。但是，我们建议您使用单独的证书进行灾难恢复设置。有关详细信息，请参阅Cisco DNA Center管理员指南中的“添加灾难恢复证书”部分。

2. alt_names部分必须包含FQDN-of-Cisco-DNA-Center作为DNS条目，并且必须通过配置向导（在输入字段“Cluster hostname”中）在Cisco DNA Center配置时设置的Cisco DNA Center主机名(FQDN)。Cisco DNA Center当前仅支持所有接口的一个主机名(FQDN)。如果将Cisco DNA Center上的管理和企业端口用于连接到网络中思科DNA中心的设备，则必须配置GeoDNS策略，以便根据接收DNS查询的网络解析为思科DNA中心主机名(FQDN)的管理IP/虚拟IP和企业IP/虚拟IP。如果仅使用Cisco DNA Center上的企业端口连接到您网络中的思科DNA Center，则不需要设置GeoDNS策略。

> **注意**：如果已为Cisco DNA Center启用了灾难恢复，则必须配置GeoDNS策略，以便根据接收DNS查询的网络为Cisco DNA Center主机名(FQDN)解析灾难恢复管理虚拟IP和灾难恢复企业虚拟IP。

3.早于2.1.1的Cisco DNA Center版本：

请密切注意alt_names部分，其中必须包含用于访问Cisco DNA Center的所有IP地址和DNS名称（通过Web浏览器或自动进程，例如PnP或Cisco ISE）。(此示例假设三节点Cisco DNA Center集群。如果您有独立设备，请仅为该节点和VIP使用SAN。如果稍后对设备进行集群，则需要重新创建证书以包含新集群成员的IP地址。)

如果未配置云接口，请忽略云端口字段。

- 在extendedKeyUsage扩展中，属性serverAuth和clientAuth是必需的。如果忽略任一属性，Cisco DNA Center将拒绝SSL证书。
- 如果导入自签名证书（不推荐），该证书必须包含X.509 Basic Constraints "CA:TRUE"扩展。

openssl.cnf示例（适用于Cisco DNA Center 2.1.1版及更高版本）：

```
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
```

> **注意**：如果在**openssl.cnf文件中不包括集群IP地址**，则无法计划软件映像激活。要解决此问题，请将集群IP地址作为SAN添加到证书中。

使用您选择的文本编辑器，创建一个名为**openssl.cnf**的文件，然后将其上传到您在上一步中创建的目录。请将此示例用作指南，但请对其进行调整以适应您的部署。

- 如果您的证书颁发机构管理团队需要2048/sha256，请调整default_bits和default_md。
- 指定req_distinguished_name和alt_names部分中每个字段的值。唯一的例外是OU字段，该字段是可选的。如果您的证书颁发机构管理团队不需要此字段，请省略OU字段。
- emailAddress字段是可选的；如果您的证书颁发机构管理员团队不需要该字段，请忽略该字段。
- alt_names部分：证书配置要求因Cisco DNA Center版本而异。
- 从Cisco DNA Center 2.1.1开始，FQDN支持可用。对于早于2.1.1的Cisco DNA Center版本，您需要使用主题备用名称(SAN)中包含IP地址的证书。Cisco DNA Center 2.1.1版及更高版本以及2.1.1版之前的Cisco DNA Center版本的alt_names部分配置如下：
- Cisco DNA Center版本2.1.1及更高版本：密切注意alt_names部分，该部分必须包含用于通过Web浏览器或自动进程（例如PnP或Cisco ISE）访问Cisco DNA Center的所有DNS名称（包括Cisco DNA Center FQDN）。alt_names部分中的第一个DNS条目必须包含Cisco DNA Center的FQDN(DNS.1 = FQDN-of-Cisco-DNA-Center)。您不能添加通配符DNS条目代替Cisco DNA Center的FQDN。但是，您可以在alt-names部分的后续DNS条目中使用通配符（对于PnP和其他DNS条目）。例如，*.example.com是有效条目。

重要信息：如果您将同一证书用于灾难恢复设置，则在alt_names部分中为灾难恢复系统站点添加DNS条目时，不允许使用通配符。但是，我们建议您使用单独的证书进行灾难恢复设置。有关详细信息，请参阅Cisco DNA Center管理员指南中的“添加灾难恢复证书”部分。

- alt_names部分必须包含FQDN-of-Cisco-DNA-Center作为DNS条目，并且必须匹配通过配置向导（输入字段“Cluster hostname”）在Cisco DNA Center配置时设置的Cisco DNA Center主机名(FQDN)。

Cisco DNA Center当前仅支持所有接口的一个主机名(FQDN)。您必须配置GeoDNS策略以根据接收DNS查询的网络解析为Cisco DNA Center主机名(FQDN)的管理IP/虚拟IP和企业IP/虚拟IP。

> **注意**：如果已为Cisco DNA Center启用了灾难恢复，则必须配置GeoDNS策略，以便根据接收DNS查询的网络为Cisco DNA Center主机名(FQDN)解析灾难恢复管理虚拟IP和灾难恢复企业虚拟IP。

- 早于2.1.1的Cisco DNA Center版本：

请密切注意alt_names部分，其中必须包含用于访问Cisco DNA Center的所有IP地址和DNS名称

（通过Web浏览器或自动进程，例如PnP或Cisco ISE）。(此示例假设三节点Cisco DNA Center集群。如果您有独立设备，请仅为该节点和VIP使用SAN。如果稍后对设备进行集群，则需要重新创建证书以包含新集群成员的IP地址。)

- 如果未配置云接口，请忽略云端口字段。
  - 在extendedKeyUsage扩展中，属性serverAuth和clientAuth是必需的。如果忽略任一属性，Cisco DNA Center将拒绝SSL证书。
  - 如果导入自签名证书（不推荐），该证书必须包含X.509 Basic Constraints "CA:TRUE"扩展。

示例openssl.cnf(适用于Cisco DNA Center 2.1.1版及更高版本)

```
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示例(适用于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
```

> **注意**：如果在**openssl.cnf文件中不包括集群IP地址**，则无法计划软件映像激活。要解决此问题，请将集群IP地址作为SAN添加到证书中。

在本例中，下一个输出是**openssl.conf**的配置

```
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
```

第四步：输入此命令以创建私钥。如果您的证书颁发机构管理团队需要，将密钥长度调整为2048。

openssl genrsa -out csr.key 4096

第五步：在**openssl.cnf**文件中填充这些字段后，使用您在上一步中创建的私钥生成证书签名请求。

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

第六步：验证证书签名请求内容，并确保在Subject Alternative Name字段中正确填充DNS名称（以及Cisco DNA Center 2.1.1之前版本的IP地址）。

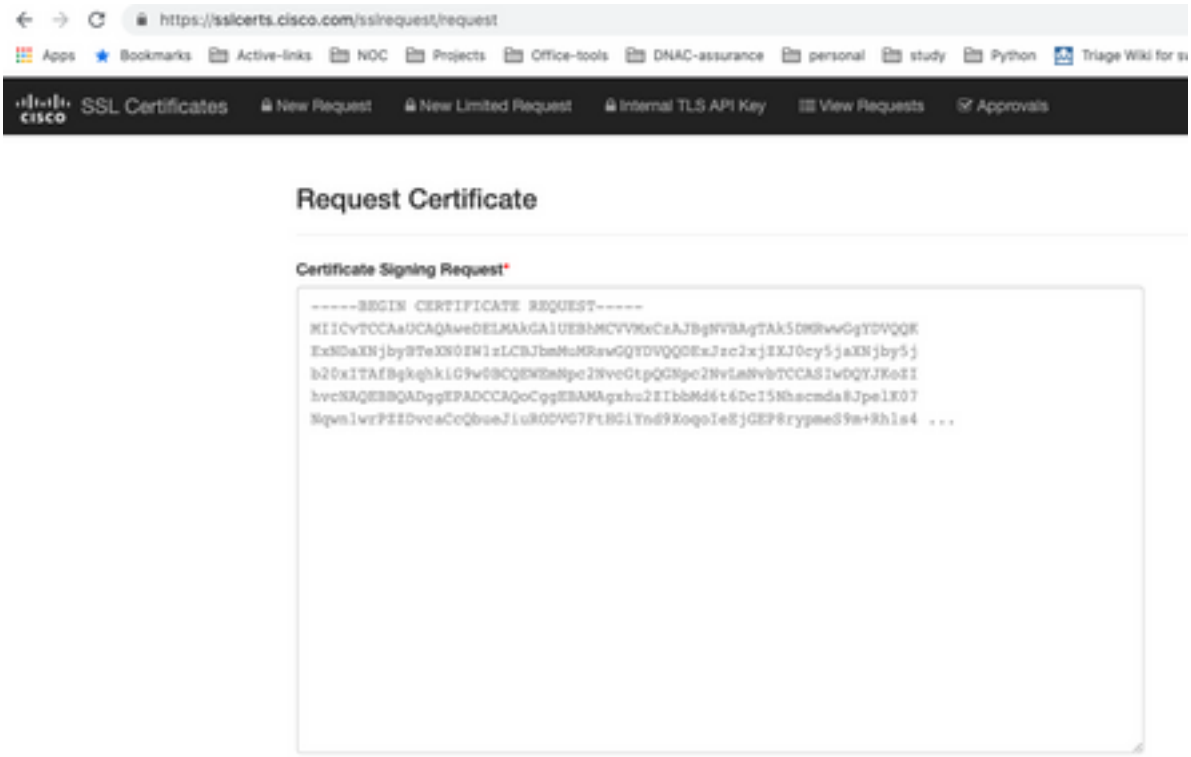
```
openssl req -text -noout -verify -in DNAC.csr
```

步骤 7.复制证书签名请求并将其粘贴到CA（例如Cisco Open SSL）。

请转至链接以下载证书。[Cisco SSL证书]

点击“Request Certificate”下载永久证书。

或者点击“Request Limited Test certificate”（请求受限测试证书）以限制用途。



用户收到包含证书信息的电子邮件。右键单击并在笔记本电脑上下载所有三个PEM文件。在本例中，我收到了3个单独的文件，因此请跳过步骤8并继续步骤9。

步骤 8 如果证书颁发者在p7b中提供证书完整链（服务器和CA）：

下载DER格式的p7b捆绑包，并另存为**dnac-chain.p7b**。

通过SSH将dnac-chain.p7b证书复制到Cisco DNA Center集群。

输入此命令：

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

步骤 9如果证书颁发者以松散文件形式提供证书及其颁发者CA链：

下载PEM(base64)文件或使用openssl将DER转换为PEM。

连接证书及其颁发者CA，以证书开头，后跟从属CA，一直到根CA，然后将其输出到dnac-chain.pem文件。

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

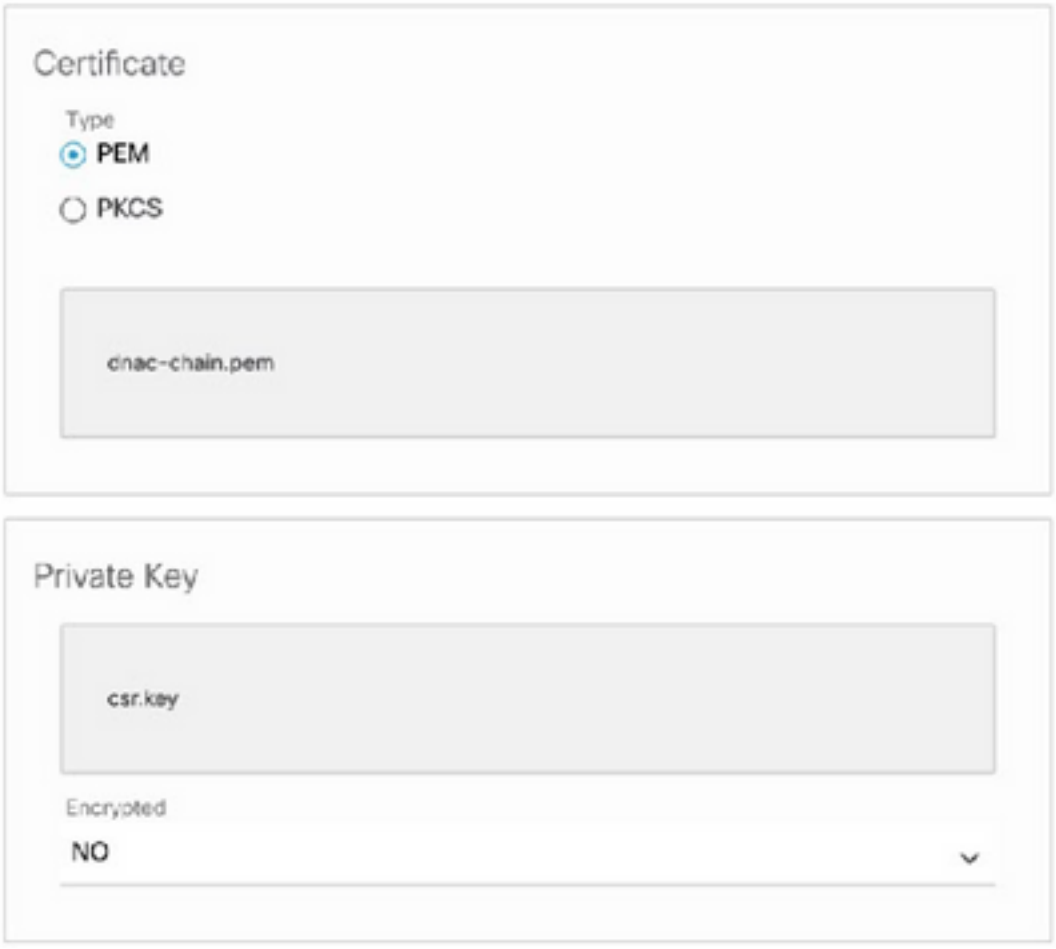
步骤 10将笔记本电脑中的文件dnac-chain.pem复制到上面创建的tls-cert dir中的Cisco DNA Center。

步骤 11在Cisco DNA Center GUI中，点击菜单图标()，然后选择系统(System)>设置(Settings)>证书(Certificates)。

步骤 12点击Replace Certificate。

步骤 13在Certificate字段中，点击PEM单选按钮并执行后续任务。

- 对于Certificate字段，请导入**dnac-chain.pem**文件，然后将此文件拖放到Drag n' Drop a File Here字段中。
- 对于Private Key字段，导入私钥(csr.key)，只需将此文件拖放到Drag n' Drop a File Here字段中。
- 从私钥的Encrypted下拉列表中选择否。



步骤 14点击Upload/Activate。注销并重新登录DNAC。

DHCP 服务器配置

配置DHCP服务器池以将IP地址分配给DUT。还配置DHCP服务器

发送域名和DNS服务器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服务器配置。配置网络中的DNS服务器以解析DNAC的FQDN名称。

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

步骤1:要安装的新设备已连接并通电。由于NVRAM中的启动配置为空，因此会触发PnP代理，并在DHCP DISCOVER消息的DHCP选项60中发送“Cisco PnP”。

第二步：DHCP服务器未配置为识别选项60中的“Cisco PnP”，而是忽略选项60。DHCP服务器分配IP地址并发送DHCP提供以及配置的域名和DNS服务器IP地址。

第三步：PnP代理读取域名并形成完全限定PnP服务器主机名，并将域名附加到字符串“pnpserver”。如果域名是“example.com”，则PnP服务器的完全限定主机名为“pnpserver.example.com”。PnP代理使用在DHCP选项中收到的DNS服务器为其IP地址解析“pnpserver.example.com”。

为自注册触发pnp代理的示例：

打开新交换机电源或“写擦除”，然后重新加载，以备棕色现场部署

验证交换机控制台上的下一个工作流程。

```
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!
```

相关信息

- PnP服务器发现
- 思科DNA中心安全最佳实践指南

- 技术支持和文档 - Cisco Systems

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。