# Provisionamento seguro de dispositivos de rede

## Contents



## Introduction

Este documento descreve a abordagem passo a passo para um dispositivo Cisco integrar com segurança a rede através de pesquisa de DNS.

## Prerequisites

### Requirements

- Conhecimento básico do gerenciamento do Cisco DNA Center (DNAC)
- Conhecimento básico de certificados SSL

### Componentes Utilizados

Este documento é baseado no Cisco DNA Center (DNAC) versão 2.1.x.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

## Informações de Apoio

A pesquisa de DNS é uma maneira recomendada de integrar quando o dispositivo de rede e o controlador do Cisco DNA Center (DNAC) estão em locais remotos e você deseja provisionar um dispositivo de rede pela Internet pública.

Há diferentes maneiras de integrar um dispositivo de rede com o uso do Cisco Plug & Play Day0.

- Opções específicas do fornecedor de DHCP
- pesquisa de DNS
- Redirecionamento de nuvem Cisco

Para ter uma comunicação segura pela Internet pública, você precisa instalar um certificado seguro no DNAC. Siga este documento para configurar um servidor DHCP, servidor DNS, gerar e instalar o certificado SSL. Se você já tiver o certificado + a chave e só precisar instalá-lo no DNAC, siga o documento da Etapa 11. Neste documento:

- O dispositivo Cat9K é o agente PNP.
- pnpserver.cisco.com é o nome FQDN do controlador DNAC.
- O switch Cisco está configurado como Servidor DNS e Servidor DHCP.

### Gerar e instalar certificado SSL no DNAC

Por padrão, o DNAC vem com um certificado autoassinado pré-instalado, válido para dispositivos de rede integrados em uma rede privada. No entanto, a Cisco recomenda que você importe um certificado X.509 válido de sua CA interna para comunicação segura para o dispositivo de rede integrado de um local remoto pela Internet pública.

Este é um exemplo para baixar e instalar o certificado Open SSL emitido pela Cisco no DNAC.

Para fazer o download do certificado, primeiro você precisa criar um CSR.

## Procedimento

Etapa 1. Use um cliente SSH para fazer login no cluster do Cisco DNA Center e criar uma pasta temporária em **/home/maglev**, por exemplo, insira o comando **mkdir tls-cert;cd tls-cert** no diretório inicial.

Etapa 2. Antes de prosseguir, verifique se o FQDN (nome de host do Cisco DNA Center) está definido no momento da configuração do Cisco DNA Center com o uso do comando **maglev cluster network display**:

```
Input:

$maglev cluster network display

Output:

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

> **Observação**: você precisa ter privilégios de raiz para executar este comando.

Se o campo de saída cluster_hostname estiver vazio ou não for o que você deseja, adicione ou altere o FQDN (nome de host do Cisco DNA Center) com o uso do comando maglev cluster config-update:

```
Input:

$maglev-config update

Output:
```

**Observação**: você precisa ter privilégios de raiz para executar este comando.

Clique em **Avançar** até ver a etapa intitulada DETALHES DO CLUSTER MAGLEV que contém o prompt de entrada Nome do host do cluster. Defina o nome do host para o FQDN do Cisco DNA Center desejado. Clique em **Avançar** e continue até que o Cisco DNA Center seja reconfigurado com o novo FQDN.

Etapa 3. Use um editor de texto de sua escolha, crie um arquivo chamado **openssl.cnf** e carregue-o no diretório criado na etapa anterior. Use este exemplo como guia, mas ajuste-o para se adequar à sua implantação.

- Ajuste default_bits e default_md se a equipe admin da autoridade de certificação exigir 2048/sha256.
- Especifique valores para cada campo nas seções req_distinguished_name e alt_names. A única exceção é o campo OU, que é opcional. Omita o campo OU se a equipe de administração da autoridade de certificação não exigir isso.
- O campo de endereço de e-mail é opcional; omita-o se a equipe de administração da autoridade de certificação não o exigir.
- seção alt_names: Os requisitos de configuração do certificado variam de acordo com a versão do Cisco DNA Center.

O suporte completo de FQDNs no certificado do Cisco DNA Center está disponível a partir do Cisco DNA Center 2.1.1. Para versões do Cisco DNA Center anteriores à 2.1.1, você precisa de um certificado com endereços IP definidos no campo Nome alternativo do assunto (SAN). As configurações da seção alt_names para o Cisco DNA Center versões 2.1.1 e posterior e para as versões do Cisco DNA Center anteriores à versão 2.1.1 são as seguintes:

Cisco DNA Center versões 2.1.1 e posteriores:

1. Preste muita atenção à seção alt_names, que deve conter todos os nomes DNS (que incluem o FQDN do Cisco DNA Center) usados para acessar o Cisco DNA Center, por um navegador da Web ou por um processo automatizado, como PnP ou Cisco ISE. A primeira entrada DNS na seção alt_names deve conter o FQDN do Cisco DNA Center (DNS.1 = FQDN-of-Cisco-DNA-Center). Não é possível adicionar uma entrada de DNS curinga no lugar do FQDN do Cisco DNA Center, mas você pode usar um curinga em entradas de DNS subsequentes na seção alt-names (para PnP e outras entradas de DNS). Por exemplo, *.example.com é uma entrada válida.

Importante: se você usar o mesmo certificado para a configuração da recuperação de desastres, não serão permitidos curingas enquanto você adicionar uma entrada DNS para um site do sistema de recuperação de desastres na seção alt_names. No entanto, recomendamos que você use um certificado separado para uma configuração de recuperação de desastres. Para obter mais informações, consulte a seção "Adicionar certificado de recuperação de desastres" no Guia do administrador do Cisco DNA Center.

2. A seção alt_names deve conter FQDN-of-Cisco-DNA-Center como uma entrada DNS e deve corresponder ao FQDN (nome de host do Cisco DNA Center) definido no momento da configuração do Cisco DNA Center por meio do assistente de configuração (no campo de entrada "Nome de host do cluster"). O Cisco DNA Center atualmente suporta apenas um nome de host (FQDN) para todas as interfaces. Se você usar a porta de gerenciamento e a porta corporativa no Cisco DNA Center para conexão de dispositivos ao Cisco DNA Center em sua rede, será

necessário configurar a política GeoDNS para resolver o IP/IP virtual de gerenciamento e o IP/IP virtual corporativo para o nome de host do Cisco DNA Center (FQDN) com base na rede da qual a consulta DNS é recebida. A configuração da política do GeoDNS não é necessária se você usar apenas a porta corporativa no Cisco DNA Center para conexão de dispositivos ao Cisco DNA Center em sua rede.

> **Observação**: se você habilitou a recuperação de desastres para o Cisco DNA Center, deverá configurar a política GeoDNS para resolver o IP virtual de gerenciamento de recuperação de desastres e o IP virtual corporativo de recuperação de desastres para o FQDN (nome de host do Cisco DNA Center) com base na rede da qual a consulta DNS é recebida.

3. Versões do Cisco DNA Center anteriores a 2.1.1:

Preste muita atenção à seção alt_names, que deve conter todos os endereços IP e nomes DNS usados para acessar o Cisco DNA Center, por um navegador da Web ou por um processo automatizado, como PnP ou Cisco ISE. (Este exemplo presume um cluster de três nós do Cisco DNA Center. Se você tiver um dispositivo autônomo, use SANs somente para esse nó e para o VIP. Se você agrupar o dispositivo posteriormente, precisará recriar o certificado para incluir os endereços IP dos novos membros do cluster.)

Se uma interface de nuvem não estiver configurada, omita os campos de porta de nuvem.

- Na extensão extendedKeyUsage, os atributos serverAuth e clientAuth são obrigatórios. Se você omitir qualquer atributo, o Cisco DNA Center rejeitará o certificado SSL.
- Se você importar um certificado autoassinado (não recomendado), ele deverá conter a extensão "CA:TRUE" das Restrições Básicas X.509.

Exemplo openssl.cnf (aplicável para o Cisco DNA Center versões 2.1.1 e posterior):

```
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
```

> **Observação**: se você não incluir os endereços IP do cluster no arquivo **openssl.cnf**, não poderá agendar a ativação da imagem do software. Para corrigir esse problema, adicione os endereços IP do cluster como SANs ao certificado.

Use um editor de texto de sua escolha, crie um arquivo chamado **openssl.cnf** e carregue-o no diretório criado na etapa anterior. Use este exemplo como guia, mas ajuste-o para se adequar à sua implantação.

- Ajuste default_bits e default_md se a equipe admin da autoridade de certificação exigir 2048/sha256.
- Especifique valores para cada campo nas seções req_distinguished_name e alt_names. A única exceção é o campo OU, que é opcional. Omita o campo OU se a equipe de

administração da autoridade de certificação não exigir isso.
- O campo emailAddress é opcional; omita-o se a equipe administrativa da autoridade de certificação não o exigir.
- seção alt_names: Os requisitos de configuração do certificado variam de acordo com a versão do Cisco DNA Center.
- O suporte a FQDNs está disponível a partir do Cisco DNA Center 2.1.1. Para versões do Cisco DNA Center anteriores à 2.1.1, você precisa de um certificado com endereços IP no SAN (nome alternativo do assunto). As configurações da seção alt_names para o Cisco DNA Center versões 2.1.1 e posterior e para as versões do Cisco DNA Center anteriores a 2.1.1. são as seguintes:
- Cisco DNA Center versões 2.1.1 e posteriores:Preste muita atenção à seção alt_names, que deve conter todos os nomes DNS (que incluem o FQDN do Cisco DNA Center) usados para acessar o Cisco DNA Center, por um navegador da Web ou por um processo automatizado, como PnP ou Cisco ISE.A primeira entrada DNS na seção alt_names deve conter o FQDN do Cisco DNA Center (DNS.1 = FQDN-of-Cisco-DNA-Center). Não é possível adicionar uma entrada de DNS curinga no lugar do FQDN do Cisco DNA Center. Mas você pode usar um curinga nas entradas DNS subsequentes na seção alt-names (para PnP e outras entradas DNS). Por exemplo, *.example.com é uma entrada válida.

Importante: se você usar o mesmo certificado para a configuração da recuperação de desastres, não serão permitidos curingas enquanto você adicionar uma entrada DNS para um site do sistema de recuperação de desastres na seção alt_names. No entanto, recomendamos que você use um certificado separado para uma configuração de recuperação de desastres. Para obter mais informações, consulte a seção "Adicionar certificado de recuperação de desastres" no Guia do administrador do Cisco DNA Center.

- A seção alt_names deve conter FQDN-of-Cisco-DNA-Center como uma entrada DNS e deve corresponder ao FQDN (nome de host do Cisco DNA Center) definido no momento da configuração do Cisco DNA Center por meio do assistente de configuração (no campo de entrada "Nome de host do cluster").

O Cisco DNA Center atualmente suporta apenas um nome de host (FQDN) para todas as interfaces. Você deve configurar a política GeoDNS para resolver o IP de gerenciamento/IP virtual e o IP corporativo/virtual para o FQDN (nome de host do Cisco DNA Center) com base na rede da qual a consulta DNS é recebida.

**Observação**: se você habilitou a recuperação de desastres para o Cisco DNA Center, deverá configurar a política GeoDNS para resolver o IP virtual de gerenciamento de recuperação de desastres e o IP virtual corporativo de recuperação de desastres para o FQDN (nome de host do Cisco DNA Center) com base na rede da qual a consulta DNS é recebida.

- Versões do Cisco DNA Center anteriores à 2.1.1:

Preste muita atenção à seção alt_names, que deve conter todos os endereços IP e nomes DNS usados para acessar o Cisco DNA Center, por um navegador da Web ou por um processo automatizado, como PnP ou Cisco ISE. (Este exemplo presume um cluster de três nós do Cisco DNA Center. Se você tiver um dispositivo autônomo, use SANs somente para esse nó e para o VIP. Se você agrupar o dispositivo posteriormente, precisará recriar o certificado para incluir os endereços IP dos novos membros do cluster.)

- Se uma interface de nuvem não estiver configurada, omita os campos de porta de nuvem.

- Na extensão extendedKeyUsage, os atributos serverAuth e clientAuth são obrigatórios. Se você omitir qualquer atributo, o Cisco DNA Center rejeitará o certificado SSL.
- Se você importar um certificado autoassinado (não recomendado), ele deverá conter a extensão "CA:TRUE" das Restrições Básicas X.509.

**Exemplo openssl.cnf** (Aplicável para Cisco DNA Center versões 2.1.1 e posteriores)

```
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
```

**Exemplo openssl.cnf** (aplicável para versões do Cisco DNA Center anteriores a 2.1.1)

```
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
```

> **Observação**: se você não incluir os endereços IP do cluster no arquivo **openssl.cnf**, não poderá agendar a ativação da imagem do software. Para corrigir esse problema, adicione os endereços IP do cluster como SANs ao certificado.

Nesse caso, a próxima saída é a configuração do my **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
```

Etapa 4. Digite este comando para criar uma chave privada. Ajuste o comprimento da chave para 2048, se exigido pela equipe de administração da autoridade de certificação. **openssl genrsa -out csr.key 4096**

Etapa 5. Depois que os campos forem preenchidos no arquivo **openssl.cnf**, use a chave privada que você criou na etapa anterior para gerar a solicitação de assinatura de certificado.

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

Etapa 6. Verifique o conteúdo da solicitação de assinatura de certificado e certifique-se de que os nomes DNS (e os endereços IP para o Cisco DNA Center versão anterior à 2.1.1) sejam preenchidos corretamente no campo Nome alternativo do assunto.

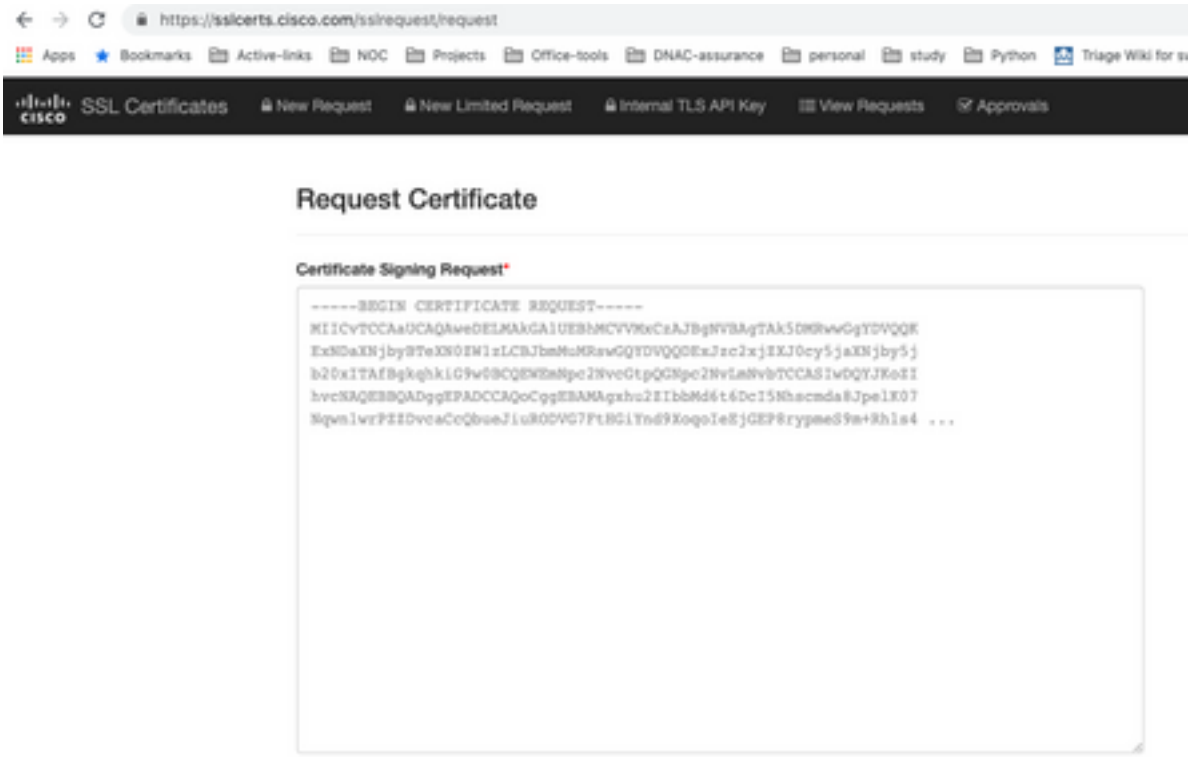
```
openssl req -text -noout -verify -in DNAC.csr
```

Passo 7. Copie a solicitação de assinatura de certificado e cole-a em uma CA (exemplo: Cisco Open SSL).

Acesse o link para baixar o certificado. Certificados SSL da Cisco

Clique em "Solicitar certificado" para fazer o download do certificado permanente.

Ou clique em "Solicitar certificado de teste limitado" para fins limitados.




O usuário recebe um email com as informações do certificado. Clique com o botão direito do mouse e faça o download de todos os três arquivos PEM em seu notebook. Nesse caso, recebi 3 arquivos separados, portanto, ignore a etapa 8 e continue na etapa 9.

Etapa 8. Se o emissor do certificado fornecer a cadeia completa do certificado (servidor e CA) na p7b:

Baixe o pacote p7b no formato DER e salve-o como **dnac-chain.p7b**.

Copie o certificado dnac-chain.p7b para o cluster do Cisco DNA Center através do SSH.

Digite este comando:

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

Etapa 9. Se o emissor do certificado fornecer o certificado e sua cadeia de CA do emissor em arquivos soltos:

Faça o download dos arquivos PEM (base64) ou use o openssl para converter DER em PEM.

Concatenar o certificado e sua CA emissora, iniciar com o certificado, seguido pela CA subordinada, até a CA raiz e enviá-lo para o arquivo dnac-chain.pem.

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

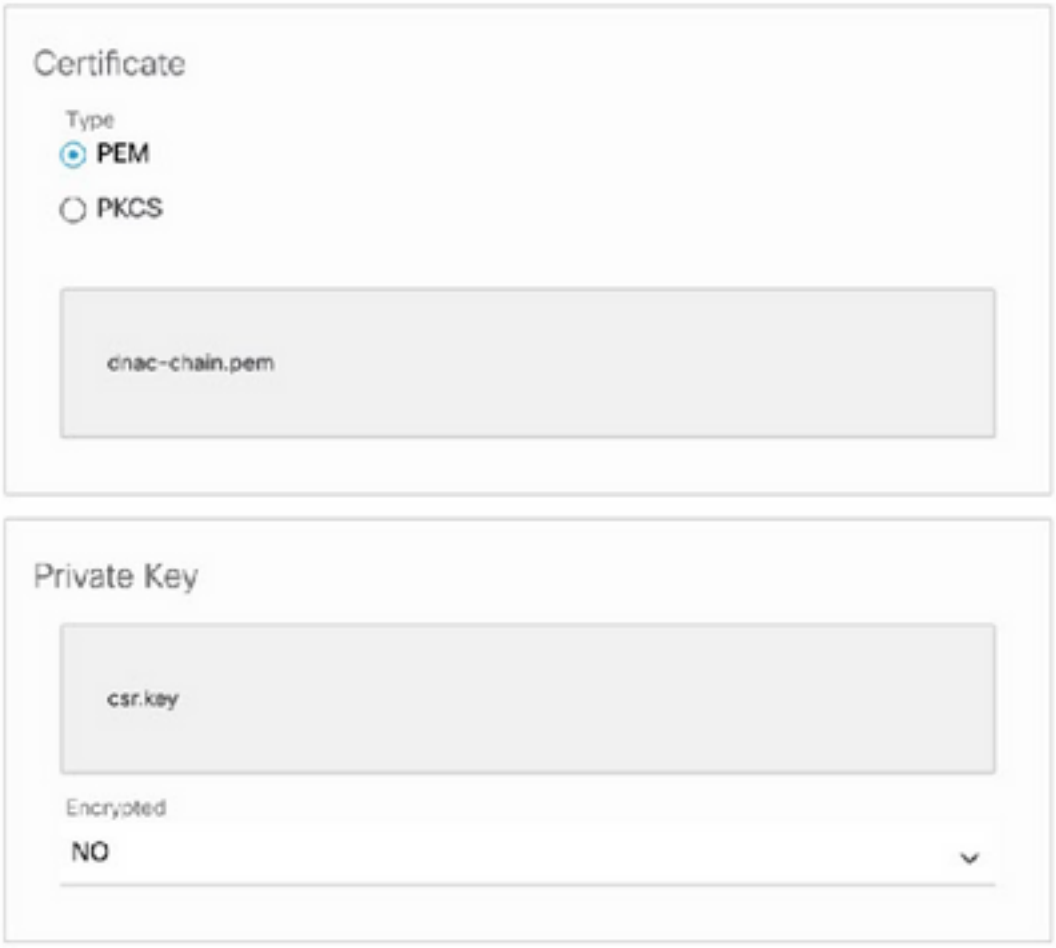
Etapa 10. Copie o arquivo dnac-chain.pem do seu laptop para o Cisco DNA Center no diretório tls-cert criado acima.

Etapa 11. Na GUI do Cisco DNA Center, clique no ícone Menu () e escolha Sistema > Configurações > Certificados.

Etapa 12. Clique em Substituir certificado.

Etapa 13. No campo Certificado, clique no botão de opção PEM e execute as próximas tarefas.

- Para o campo Certificado, importe o arquivo **dnac-chain.pem**, apenas arraste e solte esse arquivo no campo Arrastar e soltar um arquivo aqui.
- Para o campo Chave privada, importe a chave privada (csr.key), apenas arraste e solte este arquivo no campo Arrastar e Soltar um Arquivo Aqui.
- Escolha Não na lista suspensa Criptografado para a chave privada.




Etapa 14. Clique em Carregar/Ativar. Faça logoff e logon no DNAC novamente.

## Configuração do servidor DHCP

Configure um pool do Servidor DHCP para atribuir um endereço IP ao DUT. Também configura o servidor DHCP

para enviar o nome de domínio e o endereço IP do servidor DNS.

```
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
```

Configuração do servidor DNS. Configure um servidor DNS em sua rede para resolver o nome FQDN do DNAC.

```
 ip dns server
```

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

Etapa 1. O novo dispositivo a ser integrado é cabeado e ligado. Como a configuração de inicialização na NVRAM está vazia, o agente PnP é acionado e envia "Cisco PnP" na Opção de DHCP 60 na mensagem DHCP DISCOVER.

Etapa 2. O servidor DHCP não está configurado para reconhecer o "Cisco PnP" na Opção 60, ele ignora a Opção 60. O servidor DHCP atribui um endereço IP e envia a oferta DHCP junto com o nome de domínio configurado e o endereço IP do servidor DNS.

Etapa 3. O agente PnP lê o nome de domínio e formula o nome de host do servidor PnP totalmente qualificado e anexa o nome de domínio à sequência "pnpserver". Se o nome de domínio for "example.com", o nome de host totalmente qualificado do servidor PnP será "pnpserver.example.com". O agente PnP resolve "pnpserver.example.com" para seu endereço IP com o servidor DNS recebido nas opções de DHCP.

Exemplo de quando o agente pnp é acionado para integração:

Ligue um novo switch ou "write erase" seguido de recarregamento em caso de implantação em campo marrom

Verifique o próximo fluxo de trabalho no console do switch.

```
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!
```

# Informações Relacionadas

- Descoberta de servidor PnP
- Guia de práticas recomendadas de segurança do Cisco DNA Center
- **Suporte Técnico e Documentação - Cisco Systems**

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.