

# Secure Network Device Provision

## Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[SSL-certificaat op DNAC genereren en installeren](#)

[Procedure](#)

[DHCP-serverconfiguratie](#)

[Gerelateerde informatie](#)

## Inleiding

Dit document beschrijft de stap-voor-stap benadering voor een Cisco-apparaat om veilig aan boord van het netwerk te zijn via DNS-lookup.

## Voorwaarden

### Vereisten

- Basiskennis van Cisco DNA Center (DNAC)-beheer
- Basiskennis van SSL-certificaten

### Gebruikte componenten

Dit document is gebaseerd op versie 2.1.x van Cisco DNA Center (DNAC).

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

## Achtergrondinformatie

DNS-raadpleging is een aanbevolen manier om aan boord te zijn wanneer netwerkapparaten en Cisco DNA Center (DNAC)-controller zich op externe locaties bevinden en u een netwerkapparaat via het openbare internet wilt provisioneren.

Er zijn verschillende manieren om aan boord van een netwerkapparaat te gaan met het gebruik van Cisco Plug & Play Day0.

- DHCP-leverancierspecifieke opties

- DNS-raadpleging
- Cisco Cloud-omleiding

Om een veilige communicatie via het openbare internet te hebben, moet u een beveiligd certificaat installeren op DNAC. Volg dit document om een DHCP-server, DNS-server in te stellen, SSL-certificaat te genereren en te installeren. Als u reeds de certificaat + sleutel hebt en het op DNAC moet installeren, dan volg het document van Stap 11. In dit document:

- Cat9K-apparaat is de PNP-agent.
- pnpserver.cisco.com is de FQDN-naam van de DNAC-controller.
- Cisco switch is ingesteld als DNS-server en DHCP-server.

## SSL-certificaat op DNAC genereren en installeren

Standaard wordt DNAC geleverd met een vooraf geïnstalleerd zelfondertekend certificaat dat geschikt is voor netwerkapparaten in een privénetwerk. Cisco raadt u echter aan een geldig X.509-certificaat van uw interne CA te importeren voor beveiligde communicatie naar het onboard netwerkapparaat vanaf een externe locatie via het openbare internet.

Hier is een voorbeeld om het Open SSL-certificaat te downloaden en te installeren dat door Cisco op DNAC is verstrekt.

Om het certificaat te downloaden, moet je eerst een MVO creëren.

## Procedure

Stap 1. Gebruik een SSH-client om in te loggen op het Cisco DNA Center-cluster en maak een tijdelijke map onder `/home/maglev`, bijvoorbeeld, voer de opdracht `mkdir tls-cert;cd tls-cert` in terwijl u in de hoofdmap zit.

Stap 2. Zorg er voordat u verder gaat voor dat de hostnaam van Cisco DNA Center (FQDN) is ingesteld op het moment van de configuratie van Cisco DNA Center met behulp van de opdracht voor de weergave van het **maglev-cluster**netwerk:

Input :

```
$maglev cluster network display
```

Output :

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

**Opmerking:** u moet hoofdrechten hebben om deze opdracht te kunnen uitvoeren.

Als het uitvoerveld `cluster_hostname` leeg is of niet is wat u wilt, voegt u de Cisco DNA Center hostname (FQDN) toe of wijzigt u met behulp van de `maglev cluster config-update` opdracht:

Input :

```
$maglev-config update
```

Output:

Maglev Config Wizard GUI

**Opmerking:** u moet hoofdrechten hebben om deze opdracht te kunnen uitvoeren.

Klik op **Volgende** totdat u de stap genaamd MAGLEV CLUSTER DETAILS ziet die de invoerprompt Cluster hostname bevat. Stel de hostnaam in op het gewenste Cisco DNA Center FQDN. Klik op **Volgende** en ga verder totdat Cisco DNA Center opnieuw is geconfigureerd met de nieuwe FQDN.

Stap 3. Gebruik een teksteditor naar keuze, maak een bestand met de naam **openssl.cnf** en upload het naar de map die u in de vorige stap hebt gemaakt. Gebruik dit voorbeeld als uw gids, maar pas het aan om uw plaatsing te passen.

- Pas default\_bits en default\_md aan als uw certificaat autoriteit admin team 2048/sha256 vereist.
- Specificeer waarden voor elk veld in de secties req\_distished\_name en alt\_names. De enige uitzondering is het OU veld, dat optioneel is. Laat het OU-veld weg als uw certificaatautoriteit-team het niet nodig heeft.
- Het e-mailadresveld is optioneel. Laat het veld weg als het team van uw certificaatinstantie het niet nodig heeft.
- alt\_names: De vereisten voor de certificaatconfiguratie variëren op basis van de versie van Cisco DNA Center.

Volledige ondersteuning van FQDN's in het Cisco DNA Center-certificaat is vanaf Cisco DNA Center 2.1.1 beschikbaar. Voor versies van Cisco DNA Center eerder dan 2.1.1 hebt u een certificaat met IP-adressen nodig dat is gedefinieerd in het veld Alternatieve naam (SAN). De configuraties van de alt\_names sectie voor Cisco DNA Center versies 2.1.1 en hoger en Cisco DNA Center-versies eerder dan 2.1.1 zijn als volgt:

Cisco DNA Center versies 2.1.1 en hoger:

1. Let goed op de sectie alt\_names, die alle DNS-namen moet bevatten (waaronder het Cisco DNA Center FQDN) die worden gebruikt voor toegang tot Cisco DNA Center, ofwel door een webbrowser of door een geautomatiseerd proces zoals PnP of Cisco ISE. De eerste DNS-ingang in de sectie alt\_names moet Cisco DNA Center FQDN bevatten (DNS.1 = FQDN-of-Cisco-DNA-Center). U kunt geen wildcard-DNS-vermeldingen toevoegen in plaats van Cisco DNA Center FQDN, maar u kunt een jokerteken gebruiken in latere DNS-vermeldingen in de sectie met alt-namen (voor PnP- en andere DNS-vermeldingen). Bijvoorbeeld, \*.example.com is een geldige ingang.

Belangrijk: Als u hetzelfde certificaat gebruikt voor de installatie van de Disaster Recovery-instellingen, zijn wildcards niet toegestaan terwijl u een DNS-vermelding toevoegt voor een site van het Disaster Recovery-systeem in de sectie alt\_names. Het wordt echter aanbevolen om een apart certificaat te gebruiken voor de installatie voor noodherstel. Raadpleeg de sectie "Add Disaster Recovery Certificate" in de [Cisco DNA Center Administrator Guide voor](#) meer informatie.

2. De sectie alt\_names moet FQDN-of-Cisco-DNA-Center als DNS-ingang bevatten, en moet overeenkomen met de hostnaam van Cisco DNA Center (FQDN) die is ingesteld ten tijde van de configuratie van Cisco DNA Center via de configuratiewizard (in het invoerveld "Cluster hostname"). Cisco DNA Center ondersteunt momenteel slechts één hostnaam (FQDN) voor alle

interfaces. Als u zowel beheer- als ondernemingspoort op Cisco DNA Center gebruikt voor de verbinding van apparaten met Cisco DNA Center in uw netwerk, moet u het GeoDNS-beleid configureren om het beheer van IP/virtuele IP en IP/virtuele IP voor de onderneming voor Cisco DNA Center hostname (FQDN) op te lossen, op basis van het netwerk waarvan de DNS-query is ontvangen. Het instellen van het GeoDNS-beleid is niet vereist als u alleen de Enterprise Port op Cisco DNA Center gebruikt voor de verbinding van apparaten met Cisco DNA Center in uw netwerk.

**Opmerking:** als u Disaster Recovery voor Cisco DNA Center hebt ingeschakeld, moet u het GeoDNS-beleid configureren om de virtuele IP voor Disaster Recovery Management en de virtuele IP voor de Disaster Recovery-onderneming voor de hostnaam Cisco DNA Center (FQDN) op te lossen op basis van het netwerk waaruit de DNS-query is ontvangen.

### 3. Versies van Cisco DNA Center eerder dan 2.1.1:

Let goed op de sectie `alt_names`, die alle IP-adressen en DNS-namen moet bevatten die worden gebruikt voor toegang tot Cisco DNA Center, ofwel door een webbrowser, ofwel door een geautomatiseerd proces zoals PnP of Cisco ISE. (Dit voorbeeld gaat uit van een Cisco DNA Center-cluster met drie knooppunten. Als u een standalone apparaat hebt, gebruik SAN's voor alleen die knooppunt en de VIP. Als u het apparaat later clusterd, moet u het certificaat opnieuw maken om de IP-adressen van de nieuwe clusterleden op te nemen.)

Als een cloud-interface niet is geconfigureerd, moet u de cloud-poortvelden weglaten.

- In de extensie `extendedKeyUsage` zijn de attributen `serverAuth` en `clientAuth` verplicht. Als u een van beide attributen weglaat, wijst Cisco DNA Center het SSL-certificaat af.
- Als u een zelf-ondertekend certificaat importeert (niet aanbevolen), moet dit de extensie `X.509 Basic Constraints "CA:TRUE"` bevatten.

Voorbeeld `openssl.cnf` (van toepassing voor Cisco DNA Center versies 2.1.1 en hoger):

```
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

```

**Opmerking:** als u de IP-adressen van het cluster niet opneemt in het bestand **openssl.cnf**, kunt u de activering van het softwareimage niet plannen. Om dit probleem te verhelpen, voegt u de IP-adressen van het cluster als SAN's toe aan het certificaat.

Gebruik een teksteditor naar keuze, maak een bestand met de naam **openssl.cnf** en upload het naar de map die u in de vorige stap hebt gemaakt. Gebruik dit voorbeeld als uw gids, maar pas het aan om uw plaatsing te passen.

- Pas **default\_bits** en **default\_md** aan als uw certificaat autoriteit admin team 2048/sha256 vereist.
- Specificeer waarden voor elk veld in de secties **req\_distished\_name** en **alt\_names**. De enige

uitzondering is het OU veld, dat optioneel is. Laat het OU-veld weg als uw certificaatautoriteitsteam het niet nodig heeft.

- Het e-mailadres veld is optioneel; laat het weg als uw certificaat autoriteit admin team het niet nodig.
- alt\_names: De vereisten voor de certificaatconfiguratie variëren op basis van de versie van Cisco DNA Center.
- De ondersteuning van FQDN's is vanaf Cisco DNA Center 2.1.1 beschikbaar. Voor versies van Cisco DNA Center eerder dan 2.1.1 hebt u een certificaat met IP-adressen in de alternatieve onderwerpnaam (SAN) nodig. De configuraties van de alt\_names sectie voor Cisco DNA Center versies 2.1.1 en hoger, en Cisco DNA Center-versies eerder dan 2.1.1 zijn als volgt:
- Cisco DNA Center versies 2.1.1 en hoger: Let goed op de sectie alt\_names, die alle DNS-namen moet bevatten (waaronder het Cisco DNA Center FQDN) die worden gebruikt voor toegang tot Cisco DNA Center, ofwel door een webbrowser of door een geautomatiseerd proces zoals PnP of Cisco ISE. De eerste DNS-ingang in de sectie alt\_names moet de FQDN van Cisco DNA Center bevatten (DNS.1 = FQDN-of-Cisco-DNA-Center). U kunt geen DNS-vermeldingen met jokertekens toevoegen in plaats van FQDN van Cisco DNA Center. Maar u kunt een wildcard gebruiken in latere DNS-vermeldingen in de sectie Alt-namen (voor PnP en andere DNS-vermeldingen). Bijvoorbeeld, \*.example.com is een geldige ingang.

Belangrijk: Als u hetzelfde certificaat gebruikt voor de installatie van de Disaster Recovery-instellingen, zijn wildcards niet toegestaan terwijl u een DNS-vermelding toevoegt voor een site van het Disaster Recovery-systeem in de sectie alt\_names. Het wordt echter aanbevolen om een apart certificaat te gebruiken voor de installatie voor noodherstel. Raadpleeg de sectie "Add Disaster Recovery Certificate" in de [Cisco DNA Center Administrator Guide voor](#) meer informatie.

- De sectie alt\_names moet FQDN-of-Cisco-DNA-Center als DNS-ingang bevatten, en moet overeenkomen met de hostnaam van Cisco DNA Center (FQDN) die is ingesteld ten tijde van de configuratie van Cisco DNA Center via de configuratiewizard (in het invoerveld "Cluster hostnaam").

Cisco DNA Center ondersteunt momenteel slechts één hostnaam (FQDN) voor alle interfaces. U moet het GeoDNS-beleid configureren om IP/virtuele IP en IP/virtuele IP voor het beheer van het Cisco DNA Center hostname (FQDN) te kunnen oplossen op basis van het netwerk waarmee de DNS-query is ontvangen.

**Opmerking:** als u Disaster Recovery voor Cisco DNA Center hebt ingeschakeld, moet u het GeoDNS-beleid configureren om de virtuele IP voor Disaster Recovery Management en de virtuele IP voor de Disaster Recovery-onderneming voor de hostnaam Cisco DNA Center (FQDN) op te lossen op basis van het netwerk waaruit de DNS-query is ontvangen.

- Versies van Cisco DNA Center eerder dan 2.1.1:

Let goed op de sectie alt\_names, die alle IP-adressen en DNS-namen moet bevatten die worden gebruikt voor toegang tot Cisco DNA Center, ofwel door een webbrowser, ofwel door een geautomatiseerd proces zoals PnP of Cisco ISE. (Dit voorbeeld gaat uit van een Cisco DNA Center-cluster met drie knooppunten. Als u een standalone apparaat hebt, gebruik SAN's voor alleen die knooppunt en de VIP. Als u het apparaat later clusterd, moet u het certificaat opnieuw maken om de IP-adressen van de nieuwe clusterleden op te nemen.)

- Als een cloud-interface niet is geconfigureerd, moet u de cloud-poortvelden weglaten.

- In de extensie `extendedKeyUsage` zijn de attributen `serverAuth` en `clientAuth` verplicht. Als u een van beide attributen weglaat, wijst Cisco DNA Center het SSL-certificaat af.
- Als u een zelf-ondertekend certificaat importeert (niet aanbevolen), moet dit de extensie `X.509 Basic Constraints "CA:TRUE"` bevatten.

### Voorbeeld `openssl.cnf` (van toepassing voor Cisco DNA Center versies 2.1.1 en hoger)

```
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
```

### Voorbeeld `openssl.cnf` (van toepassing voor eerdere Cisco DNA Center-versies dan 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
```

**Opmerking:** als u de IP-adressen van het cluster niet opneemt in het bestand `openssl.cnf`, kunt u de activering van het softwareimage niet plannen. Om dit probleem te verhelpen, voegt u de IP-adressen van het cluster als SAN's toe aan het certificaat.

In dit geval is de volgende uitvoer de configuratie van mijn `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
```

Stap 4. Voer deze opdracht in om een persoonlijke sleutel te maken. Pas de sleutellengte aan 2048 indien nodig door uw certificaat autoriteit admin team. **openssl genrsa -out csr.key 4096**

Stap 5. Nadat de velden zijn ingevuld in het bestand **openssl.cnf** gebruikt u de privé-sleutel die u in de vorige stap hebt gemaakt om het verzoek voor certificaatondertekening te genereren.

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

Stap 6. Controleer de inhoud van de aanvraag voor certificaatondertekening en zorg ervoor dat de DNS-namen (en IP-adressen voor de versie van Cisco DNA Center eerder dan 2.1.1) correct worden ingevuld in het veld Alternatieve naam onderwerp.

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

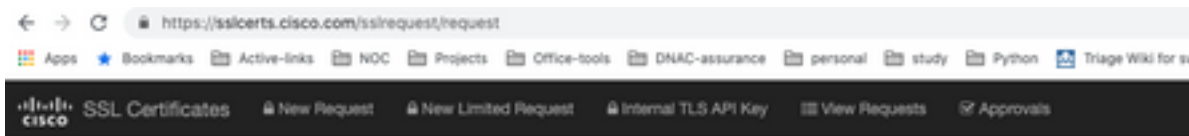
Stap 7. Kopieer de aanvraag voor het ondertekenen van het certificaat en plak deze op een CA (bijvoorbeeld Cisco Open SSL).

Ga naar de link om certificaat te downloaden. [Cisco SSL-certificaten](#)

Klik op "Certificaat aanvragen" om permanent certificaat te downloaden.

Of klik op "Vraag een beperkt testcertificaat aan" voor een beperkt doel.





De gebruiker ontvangt een e-mail met de certificaatinformatie. Klik met de rechtermuisknop en download alle drie PEM-bestanden op uw laptop. In dit geval heb ik 3 afzonderlijke bestanden ontvangen, dus sla stap 8 over en ga verder met stap 9.

Stap 8. Indien de certificaatverlener de volledige keten van het certificaat (server en CA) in p7b verstrekt:

Download de p7b bundel in DER formaat en bewaar het als **dnac-chain.p7b**.

Kopieer het certificaat dnac-chain.p7b naar het Cisco DNA Center-cluster via SSH.

Voer deze opdracht in:

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

Stap 9. Indien de certificaatuitgever het certificaat en de CA-keten van de uitgever in losse bestanden verstrekt:

Download de PEM (base64) bestanden of gebruik openssl om DER naar PEM te converteren.

Verbind het certificaat en zijn uitgever CA, begin met het certificaat, gevolgd door ondergeschikte CA, al manier aan de wortel CA, en output het aan dnac-chain.pem- dossier.

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

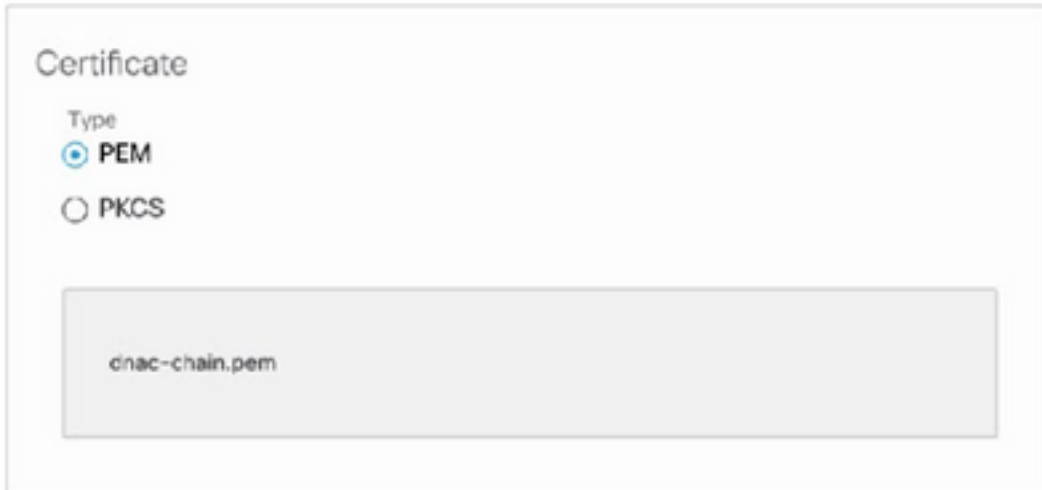
Stap 10. Kopieer het bestand dnac-chain.pem van uw laptop naar Cisco DNA Center in de tabel-cert dir die hierboven is gemaakt.

Stap 11. Klik in de Cisco DNA Center GUI op het pictogram Menu () en kies Systeem > Instellingen > Certificaten.

Stap 12. Klik op Certificaat vervangen.

Stap 13. Klik in het veld Certificaat op de radioknop PEM en voer de volgende taken uit.

- Voor het veld Certificaat importeert u het bestand **dnac-chain.pem**, sleept u dit bestand naar het veld Sleep n' Drop a File Here.
- Voor het veld Private Key importeert u de private sleutel (csr.key), sleept u dit bestand en zet u het in het veld Sleep n' Drop a File Here.
- Kies Nee in de vervolgkeuzelijst Versleuteld voor de persoonlijke sleutel.



Certificate

Type

PEM

PKCS

dnac-chain.pem



Private Key

csr.key

Encrypted

NO

Stap 14. Klik op Upload/Activate. Log uit en log opnieuw in bij DNAC.

## DHCP-serverconfiguratie

Configureer een DHCP-servergroep om IP-adres aan de DUT toe te wijzen. Configureert DHCP-server

om domeinnaam en DNS server IP adres te verzenden.

```
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-serverconfiguratie. Configureer een DNS-server in uw netwerk om de FQDN-naam van de DNAC op te lossen.

```
ip dns server
```

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

Stap 1. Het nieuwe apparaat dat wordt meegeleverd, wordt bekabeld en ingeschakeld. Aangezien de opstartconfiguratie in NVRAM leeg is, wordt PnP-agent geactiveerd en wordt "Cisco PnP" in DHCP-optie 60 in DHCP ONTDEK-bericht verzonden.

Stap 2. De DHCP-server is niet geconfigureerd om "Cisco PnP" in optie 60 te herkennen. Optie 60 wordt genegeerd. DHCP-server kent een IP-adres toe en verstuurt DHCP-aanbod samen met de geconfigureerde domeinnaam en DNS-server IP-adres.

Stap 3. PnP agent leest domeinnaam en formuleert volledig gekwalificeerde PnP server hostname en voegt de domeinnaam toe aan de string "pnpserver". Als de domeinnaam "example.com" is, dan zou de volledig gekwalificeerde hostnaam van PnP server "pnpserver.example.com" zijn. PnP-agent lost "pnpserver.example.com" op voor het IP-adres met de DNS-server die is ontvangen in de DHCP-opties.

Voorbeeld wanneer pnp-agent wordt geactiveerd voor onboarding:

Schakel een nieuwe switch in of "schrijf wissen", gevolgd door opnieuw laden in het geval van een bruine veldinzet

Controleer de volgende workflow op de 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!

## Gerelateerde informatie

- [Detectie van PnP-servers](#)
- [Handleiding voor beste praktijken voor Cisco DNA Center Security](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)

## Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.