

# Sichere Bereitstellung von Netzwerkgeräten

## Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[SSL-Zertifikat auf DNAC generieren und installieren](#)

[Vorgehensweise](#)

[DHCP-Serverkonfiguration](#)

[Zugehörige Informationen](#)

## Einleitung

In diesem Dokument wird der schrittweise Ansatz beschrieben, mit dem ein Cisco Gerät das Netzwerk über die DNS-Suche sicher integrieren kann.

## Voraussetzungen

### Anforderungen

- Grundkenntnisse der Verwaltung des Cisco DNA Center (DNAC)
- Grundkenntnisse der SSL-Zertifikate

### Verwendete Komponenten

Dieses Dokument basiert auf Cisco DNA Center (DNAC) Version 2.1.x.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

## Hintergrundinformationen

Die DNS-Suche ist eine empfohlene Methode zur Einbindung, wenn sich das Netzwerkgerät und der Cisco DNA Center (DNAC)-Controller an entfernten Standorten befinden und Sie ein Netzwerkgerät über das öffentliche Internet bereitstellen möchten.

Es gibt verschiedene Möglichkeiten, ein Netzwerkgerät mit Cisco Plug & Play Day0 zu integrieren.

- Herstellerspezifische DHCP-Optionen
- DNS-Suche

- Cisco Cloud-Umleitung

Um eine sichere Kommunikation über das öffentliche Internet zu haben, müssen Sie ein sicheres Zertifikat auf DNAC installieren. Befolgen Sie dieses Dokument, um einen DHCP-Server, einen DNS-Server einzurichten, ein SSL-Zertifikat zu generieren und zu installieren. Wenn Sie bereits über das Zertifikat + Schlüssel und müssen nur auf DNAC installieren, dann folgen Sie dem Dokument aus Schritt 11. In diesem Dokument:

- Das Gerät der Kategorie 9K ist der PNP-Agent.
- pnpserver.cisco.com ist der FQDN-Name des DNAC-Controllers.
- Der Cisco Switch wird als DNS-Server und DHCP-Server konfiguriert.

## SSL-Zertifikat auf DNAC generieren und installieren

Standardmäßig enthält DNAC ein vorinstalliertes selbstsigniertes Zertifikat, das für die Integration von Netzwerkgeräten in einem privaten Netzwerk geeignet ist. Cisco empfiehlt jedoch, ein gültiges X.509-Zertifikat von Ihrer internen Zertifizierungsstelle zu importieren, um eine sichere Kommunikation mit dem integrierten Netzwerkgerät von einem entfernten Standort über das öffentliche Internet zu gewährleisten.

Hier ist ein Beispiel zum Herunterladen und Installieren des Open SSL-Zertifikats, das von Cisco auf DNAC ausgestellt wurde.

Um das Zertifikat herunterzuladen, müssen Sie zunächst eine CSR erstellen.

## Vorgehensweise

Schritt 1: Verwenden Sie einen SSH-Client, um sich beim Cisco DNA Center-Cluster anzumelden und einen temporären Ordner unter `/home/maglev` zu erstellen. Geben Sie beispielsweise den Befehl `mkdir tls-cert;cd tls-cert` ein, während Sie sich im Home-Verzeichnis befinden.

Schritt 2: Bevor Sie fortfahren, stellen Sie sicher, dass der Cisco DNA Center-Hostname (FQDN) zum Zeitpunkt der Konfiguration des Cisco DNA Centers mit dem Befehl `maglev cluster network display` festgelegt wird:

Input :

```
$maglev cluster network display
```

Output :

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

**Hinweis:** Sie benötigen Root-Berechtigungen, um diesen Befehl auszuführen.

Wenn das Ausgabefeld `cluster_hostname` leer ist oder nicht Ihren Vorstellungen entspricht, können Sie den Cisco DNA Center-Hostnamen (FQDN) mit dem `maglev cluster config-update`-Befehl hinzufügen oder ändern:

Input :

```
$maglev-config update
```

Output :

```
Maglev Config Wizard GUI
```

**Hinweis:** Sie benötigen Root-Berechtigungen, um diesen Befehl auszuführen.

Klicken Sie auf **Weiter**, bis der Schritt MAGLEV CLUSTER DETAILS mit der Eingabeaufforderung Cluster hostname angezeigt wird. Stellen Sie den Hostnamen auf den gewünschten Cisco DNA Center FQDN ein. Klicken Sie auf **Weiter**, und fahren Sie fort, bis Cisco DNA Center mit dem neuen FQDN rekonfiguriert ist.

Schritt 3: Verwenden Sie einen Texteditor Ihrer Wahl, erstellen Sie eine Datei mit dem Namen **openssl.cnf** und laden Sie sie in das Verzeichnis hoch, das Sie im vorherigen Schritt erstellt haben. Verwenden Sie dieses Beispiel als Leitfaden, passen Sie es jedoch an Ihre Bereitstellung an.

- Passen Sie default\_bits und default\_md an, wenn das Administrator-Team der Zertifizierungsstelle stattdessen 2048/sha256 benötigt.
- Geben Sie Werte für jedes Feld in den Abschnitten req\_Distinguished\_name und alt\_names an. Die einzige Ausnahme ist das Feld "OU" (Organisationseinheit), das optional ist. Lassen Sie das OU-Feld aus, wenn das Administratorteam der Zertifizierungsstelle es nicht benötigt.
- Das E-Mail-Adressfeld ist optional. Lassen Sie es weg, wenn Ihr Zertifizierungsstellen-Admin-Team es nicht benötigt.
- alt\_names-Abschnitt: Die Konfigurationsanforderungen für Zertifikate variieren je nach Cisco DNA Center-Version.

Die vollständige Unterstützung von FQDNs im Cisco DNA Center-Zertifikat ist ab Cisco DNA Center 2.1.1 verfügbar. Für ältere Cisco DNA Center-Versionen als 2.1.1 benötigen Sie ein Zertifikat mit den im Feld "Subject Alternative Name (SAN)" (Alternativer Antragstellername) definierten IP-Adressen. Die alt\_names-Abschnittskonfigurationen für Cisco DNA Center Version 2.1.1 und höher und Cisco DNA Center Version vor 2.1.1 sind wie folgt:

Cisco DNA Center Version 2.1.1 und höher:

1. Achten Sie genau auf den alt\_names-Abschnitt, der alle DNS-Namen (einschließlich Cisco DNA Center FQDN) enthalten muss, die für den Zugriff auf Cisco DNA Center verwendet werden, entweder über einen Webbrowser oder durch einen automatisierten Prozess wie PnP oder Cisco ISE. Der erste DNS-Eintrag im alt\_names-Abschnitt muss Cisco DNA Center FQDN (DNS.1 = FQDN-of-Cisco-DNA-Center) enthalten. Sie können anstelle von Cisco DNA Center FQDN keinen Platzhalter-DNS-Eintrag hinzufügen, aber Sie können einen Platzhalter in nachfolgenden DNS-Einträgen im Abschnitt alt-names (für PnP- und andere DNS-Einträge) verwenden. Zum Beispiel ist \*.example.com ein gültiger Eintrag.

Wichtig: Wenn Sie dasselbe Zertifikat für die Disaster Recovery verwenden, sind Platzhalter nicht zulässig, während Sie im Abschnitt alt\_names einen DNS-Eintrag für einen Disaster Recovery-Systemstandort hinzufügen. Es wird jedoch empfohlen, für eine Disaster Recovery-Konfiguration ein separates Zertifikat zu verwenden. Weitere Informationen finden Sie im Abschnitt "Hinzufügen eines Disaster Recovery-Zertifikats" im [Cisco DNA Center Administrator Guide](#).

2. Der Abschnitt alt\_names muss FQDN-of-Cisco-DNA-Center als DNS-Eintrag enthalten und mit

dem Cisco DNA Center-Hostnamen (FQDN) übereinstimmen, der zum Zeitpunkt der Cisco DNA Center-Konfiguration über den Konfigurationsassistenten (im Eingabefeld "Cluster-Hostname") festgelegt wurde. Cisco DNA Center unterstützt derzeit nur einen Hostnamen (FQDN) für alle Schnittstellen. Wenn Sie sowohl den Management- als auch den Enterprise-Port auf Cisco DNA Center für Geräte verwenden, die mit Cisco DNA Center in Ihrem Netzwerk verbunden sind, müssen Sie die GeoDNS-Richtlinie so konfigurieren, dass sie zur Management-IP/virtuellen IP und zur Unternehmens-IP/virtuellen IP für den Cisco DNA Center-Hostnamen (FQDN) aufgelöst wird, der auf dem Netzwerk basiert, von dem die DNS-Abfrage empfangen wird. Sie müssen keine GeoDNS-Richtlinie einrichten, wenn Sie in Ihrem Netzwerk nur den Enterprise-Port des Cisco DNA Center für Geräte verwenden, die mit dem Cisco DNA Center verbunden sind.

**Hinweis:** Wenn Sie die Notfallwiederherstellung für Cisco DNA Center aktiviert haben, müssen Sie die GeoDNS-Richtlinie so konfigurieren, dass die virtuelle IP des Notfallwiederherstellungsmanagements und die virtuelle IP des Notfallwiederherstellungsunternehmens für den Cisco DNA Center-Hostnamen (FQDN) aufgelöst werden, basierend auf dem Netzwerk, von dem die DNS-Abfrage empfangen wird.

### 3. Cisco DNA Center-Versionen vor 2.1.1:

Beachten Sie den Abschnitt `alt_names`, der alle IP-Adressen und DNS-Namen enthalten muss, die für den Zugriff auf Cisco DNA Center verwendet werden, entweder über einen Webbrowser oder durch einen automatisierten Prozess wie PnP oder Cisco ISE. (In diesem Beispiel wird von einem Cluster aus Cisco DNA Center mit drei Knoten ausgegangen. Wenn Sie über ein eigenständiges Gerät verfügen, verwenden Sie SANs nur für diesen Knoten und das VIP. Wenn Sie das Gerät zu einem späteren Zeitpunkt zu einem Cluster zusammenfassen, müssen Sie das Zertifikat neu erstellen und die IP-Adressen der neuen Cluster-Mitglieder einfügen.)

Wenn keine Cloud-Schnittstelle konfiguriert ist, lassen Sie die Cloud-Port-Felder aus.

- In der Erweiterung `extendedKeyUsage` sind die Attribute `serverAuth` und `clientAuth` obligatorisch. Wenn Sie eines der Attribute auslassen, lehnt Cisco DNA Center das SSL-Zertifikat ab.
- Wenn Sie ein selbstsigniertes Zertifikat importieren (nicht empfohlen), muss es die Erweiterung "CA:TRUE" der X.509 Basic Constraints enthalten.

Beispiel `openssl.cnf` (Gilt für Cisco DNA Center Version 2.1.1 und höher):

```
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

```

**Hinweis:** Wenn Sie die Cluster-IP-Adressen nicht in die Datei **openssl.cnf** einfügen, können Sie die Aktivierung des Software-Images nicht planen. Um dieses Problem zu beheben, fügen Sie die Cluster-IP-Adressen als SANs zum Zertifikat hinzu.

Verwenden Sie einen Texteditor Ihrer Wahl, erstellen Sie eine Datei mit dem Namen **openssl.cnf**

und laden Sie sie in das Verzeichnis hoch, das Sie im vorherigen Schritt erstellt haben. Verwenden Sie dieses Beispiel als Leitfaden, passen Sie es jedoch an Ihre Bereitstellung an.

- Passen Sie `default_bits` und `default_md` an, wenn das Administrator-Team der Zertifizierungsstelle stattdessen 2048/sha256 benötigt.
- Geben Sie Werte für jedes Feld in den Abschnitten `req_Distinguished_name` und `alt_names` an. Die einzige Ausnahme ist das Feld "OU" (Organisationseinheit), das optional ist. Lassen Sie das OU-Feld aus, wenn das Administratorteam der Zertifizierungsstelle es nicht benötigt.
- Das E-Mail-Adressenfeld ist optional. Lassen Sie es weg, wenn das Administratorteam der Zertifizierungsstelle es nicht benötigt.
- `alt_names`-Abschnitt: Die Konfigurationsanforderungen für Zertifikate variieren je nach Cisco DNA Center-Version.
- Die FQDNs-Unterstützung ist ab Cisco DNA Center 2.1.1 verfügbar. Für ältere Cisco DNA Center-Versionen als 2.1.1 benötigen Sie ein Zertifikat mit IP-Adressen im Subject Alternative Name (SAN). Die `alt_names`-Abschnittskonfigurationen für Cisco DNA Center Version 2.1.1 und höher und Cisco DNA Center Version vor 2.1.1 sind wie folgt:
- Cisco DNA Center Version 2.1.1 und höher: Beachten Sie den Abschnitt `alt_names`, der alle DNS-Namen (einschließlich des Cisco DNA Center FQDN) enthalten muss, die für den Zugriff auf Cisco DNA Center verwendet werden. Dies kann entweder über einen Webbrowser oder durch einen automatisierten Prozess wie PnP oder Cisco ISE erfolgen. Der erste DNS-Eintrag im `alt_names`-Abschnitt muss den FQDN von Cisco DNA Center enthalten (DNS.1 = FQDN-of-Cisco-DNA-Center). Sie können anstelle von FQDN von Cisco DNA Center keinen DNS-Eintrag mit Platzhalter hinzufügen. Sie können jedoch einen Platzhalter in nachfolgenden DNS-Einträgen im Bereich "alt-names" (für PnP- und andere DNS-Einträge) verwenden. Beispielsweise ist `*.example.com` ein gültiger Eintrag.

Wichtig: Wenn Sie dasselbe Zertifikat für die Disaster Recovery verwenden, sind Platzhalter nicht zulässig, während Sie im Abschnitt `alt_names` einen DNS-Eintrag für einen Disaster Recovery-Systemstandort hinzufügen. Es wird jedoch empfohlen, für eine Disaster Recovery-Konfiguration ein separates Zertifikat zu verwenden. Weitere Informationen finden Sie im Abschnitt "Hinzufügen eines Disaster Recovery-Zertifikats" im [Cisco DNA Center Administrator Guide](#).

- Der Abschnitt `alt_names` muss FQDN-of-Cisco-DNA-Center als DNS-Eintrag enthalten und mit dem Cisco DNA Center-Hostnamen (FQDN) übereinstimmen, der zum Zeitpunkt der Cisco DNA Center-Konfiguration über den Konfigurationsassistenten (im Eingabefeld "Cluster-Hostname") festgelegt wurde.

Cisco DNA Center unterstützt derzeit nur einen Hostnamen (FQDN) für alle Schnittstellen. Sie müssen die GeoDNS-Richtlinie so konfigurieren, dass sie zur Verwaltungs-IP/virtuellen IP und Unternehmens-IP/virtuellen IP für den Cisco DNA Center-Hostnamen (FQDN) aufgelöst wird, der auf dem Netzwerk basiert, von dem die DNS-Abfrage empfangen wird.

**Hinweis:** Wenn Sie die Notfallwiederherstellung für Cisco DNA Center aktiviert haben, müssen Sie die GeoDNS-Richtlinie so konfigurieren, dass die virtuelle IP des Notfallwiederherstellungsmanagements und die virtuelle IP des Notfallwiederherstellungsunternehmens für den Cisco DNA Center-Hostnamen (FQDN) aufgelöst werden, basierend auf dem Netzwerk, von dem die DNS-Abfrage empfangen wird.

- Cisco DNA Center-Versionen vor 2.1.1:

Beachten Sie den Abschnitt `alt_names`, der alle IP-Adressen und DNS-Namen enthalten muss, die

für den Zugriff auf Cisco DNA Center verwendet werden, entweder über einen Webbrowser oder durch einen automatisierten Prozess wie PnP oder Cisco ISE. (In diesem Beispiel wird von einem Cluster aus Cisco DNA Center mit drei Knoten ausgegangen. Wenn Sie über ein eigenständiges Gerät verfügen, verwenden Sie SANs nur für diesen Knoten und das VIP. Wenn Sie das Gerät zu einem späteren Zeitpunkt zu einem Cluster zusammenfassen, müssen Sie das Zertifikat neu erstellen und die IP-Adressen der neuen Cluster-Mitglieder einfügen.)

- Wenn keine Cloud-Schnittstelle konfiguriert ist, lassen Sie die Cloud-Port-Felder aus.
  - In der Erweiterung `extendedKeyUsage` sind die Attribute `serverAuth` und `clientAuth` obligatorisch. Wenn Sie eines der Attribute auslassen, lehnt Cisco DNA Center das SSL-Zertifikat ab.
  - Wenn Sie ein selbstsigniertes Zertifikat importieren (nicht empfohlen), muss es die Erweiterung "CA:TRUE" der X.509 Basic Constraints enthalten.

### Beispiel `openssl.cnf` (Zutreffend für Cisco DNA Center Versionen 2.1.1 und höher)

```
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
```

### Beispiel `openssl.cnf` (Anwendbar für Cisco DNA Center-Versionen vor 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
```

**Hinweis:** Wenn Sie die Cluster-IP-Adressen nicht in die Datei `openssl.cnf` einfügen, können Sie die Aktivierung des Software-Images nicht planen. Um dieses Problem zu beheben, fügen Sie die Cluster-IP-Adressen als SANs zum Zertifikat hinzu.

In diesem Fall ist die nächste Ausgabe die Konfiguration meiner `openssl.cnf`

```
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
```

Schritt 4: Geben Sie diesen Befehl ein, um einen privaten Schlüssel zu erstellen. Passen Sie die Schlüssellänge auf 2048 an, falls dies vom Administrator-Team Ihrer Zertifizierungsstelle erforderlich ist. **openssl genrsa -out csr.key 4096**

Schritt 5: Nachdem die Felder in die Datei **openssl.cnf** gefüllt wurden, verwenden Sie den privaten Schlüssel, den Sie im vorherigen Schritt erstellt haben, um die Zertifikatsignierungsanforderung zu generieren.

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

Schritt 6: Überprüfen Sie den Inhalt der Zertifikatsignierungsanforderung, und stellen Sie sicher, dass die DNS-Namen (und IP-Adressen für die Cisco DNA Center-Version vor 2.1.1) im Feld "Subject Alternative Name" (Alternativer Antragstellername) korrekt eingetragen sind.

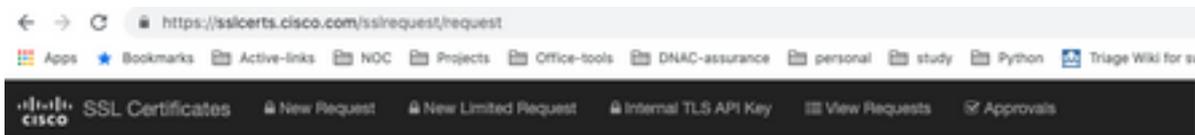
```
openssl req -text -noout -verify -in DNAC.csr
```

Schritt 7. Kopieren Sie die Signaturzertifikatanforderung, und fügen Sie sie in eine Zertifizierungsstelle (z. B. Cisco Open SSL) ein.

Klicken Sie auf den Link, um das Zertifikat herunterzuladen. [Cisco SSL-Zertifikate](#)

Klicken Sie auf "Zertifikat anfordern", um das permanente Zertifikat herunterzuladen.

Oder klicken Sie auf "Request Limited Test Certificate" für einen begrenzten Zweck.



Der Benutzer erhält eine E-Mail mit den Zertifikatinformationen. Klicken Sie mit der rechten Maustaste, und laden Sie alle drei PEM-Dateien auf Ihren Laptop herunter. In diesem Fall habe ich 3 separate Dateien erhalten, also überspringen Sie Schritt 8 und fahren Sie mit Schritt 9 fort.

Schritt 8: Wenn der Zertifikatsaussteller die vollständige Kette des Zertifikats (Server und CA) in p7b bereitstellt:

Laden Sie das Paket p7b im DER-Format herunter, und speichern Sie es unter **dnac-chain.p7b**.

Kopieren Sie das dnac-chain.p7b-Zertifikat über SSH in den Cisco DNA Center-Cluster.

Geben Sie folgenden Befehl ein:

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

Schritt 9. Wenn der Zertifikatsaussteller das Zertifikat und die CA-Kette des Ausstellers in losen Dateien bereitstellt:

Laden Sie die PEM-Dateien (base64) herunter oder verwenden Sie openssl, um DER in PEM zu konvertieren.

Verbinden Sie das Zertifikat und seine Ausstellerzertifizierungsstelle, beginnen Sie mit dem Zertifikat, gefolgt von der untergeordneten Zertifizierungsstelle, bis hin zur Stammzertifizierungsstelle, und geben Sie sie in die Datei dnac-chain.pem aus.

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

Schritt 10. Kopieren Sie die Datei dnac-chain.pem von Ihrem Laptop nach Cisco DNA Center in das oben erstellte tls-cert dir.

Schritt 11. Klicken Sie in der GUI von Cisco DNA Center auf das Menüsymbol (☰), und wählen Sie System > Settings > Certificates (System > Einstellungen > Zertifikate) aus.

Schritt 12: Klicken Sie auf Zertifikat ersetzen.

Schritt 13: Klicken Sie im Feld Zertifikat auf das Optionsfeld PEM, und führen Sie die nächsten Aufgaben aus.

- Importieren Sie für das Zertifikatfeld die Datei **dnac-chain.pem**, ziehen Sie diese Datei einfach in das Feld Drag n' Drop a File Here.
- Importieren Sie für das Feld Privater Schlüssel den privaten Schlüssel (csr.key), und ziehen Sie diese Datei einfach in das Feld Drag n' Drop a File Here.
- Wählen Sie in der Dropdown-Liste "Verschlüsselt" die Option Nein für den privaten Schlüssel aus.

Certificate

Type

PEM

PKCS

dnac-chain.pem

Private Key

csr.key

Encrypted

NO

Schritt 14: Klicken Sie auf Hochladen/Aktivieren. Melden Sie sich ab, und melden Sie sich bei DNAC erneut an.

## DHCP-Serverkonfiguration

Konfigurieren Sie einen DHCP-Server-Pool, um dem DUT die IP-Adresse zuzuweisen. Auch DHCP-Server konfigurieren

um den Domännennamen und die IP-Adresse des DNS-Servers zu senden.

```
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
```

Konfiguration des DNS-Servers. Konfigurieren Sie einen DNS-Server in Ihrem Netzwerk, um den FQDN-Namen des DNAC aufzulösen.

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

Schritt 1: Das neue Gerät, das integriert werden soll, ist verkabelt und eingeschaltet. Da die Startkonfiguration im NVRAM leer ist, wird der PnP-Agent ausgelöst und sendet "Cisco PnP" in der DHCP-Option 60 in der DHCP DISCOVER-Nachricht.

Schritt 2: Der DHCP-Server ist nicht für die Erkennung von "Cisco PnP" in Option 60 konfiguriert. Option 60 wird ignoriert. Der DHCP-Server weist eine IP-Adresse zu und sendet ein DHCP-Angebot zusammen mit dem konfigurierten Domännennamen und der IP-Adresse des DNS-Servers.

Schritt 3: Der PnP-Agent liest den Domännennamen und formuliert den vollqualifizierten PnP-Serverhostnamen und hängt den Domännennamen an die Zeichenfolge "pnpserver" an. Wenn der Domänenname "example.com" lautet, lautet der vollqualifizierte Hostname des PnP-Servers "pnpserver.example.com". Der PnP-Agent löst "pnpserver.example.com" für seine IP-Adresse mit dem DNS-Server auf, der in den DHCP-Optionen empfangen wurde.

Beispiel, wenn der pnp-Agent für das Onboarding ausgelöst wird:

Einschalten eines neuen Switches oder "write erase" (Schreiblöschung), gefolgt von einem Neuladen bei Bereitstellung eines braunen Felds

Überprüfen Sie den nächsten Workflow auf der Switch-Konsole.

```
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!

## Zugehörige Informationen

- [PnP-Servererkennung](#)
- [Cisco DNA Center Security Best Practices Guide](#)
- [Technischer Support und Dokumentation für Cisco Systeme](#)

## Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.