보안 네트워크 디바이스 프로비저닝

목차

[소개](#)
[사전 요구 사항](#)
[요구 사항](#)
[사용되는 구성 요소](#)
[배경 정보](#)
[DNAC에 SSL 인증서 생성 및 설치](#)
[절차](#)
[DHCP 서버 컨피그레이션](#)
[관련 정보](#)

소개

이 문서에서는 Cisco 디바이스가 DNS 조회를 통해 네트워크를 안전하게 온보딩하는 단계별 접근 방식을 설명합니다.

사전 요구 사항

요구 사항

- Cisco DNAC(DNA Center) 관리에 대한 기본 지식
- SSL 인증서에 대한 기본 지식

사용되는 구성 요소

이 문서는 Cisco DNAC(DNA Center) 버전 2.1.x를 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

DNS 조회는 네트워크 장치와 Cisco DNA Center(DNAC) 컨트롤러가 원격 사이트에 있고 공용 인터넷을 통해 네트워크 장치를 프로비저닝하려는 경우 온보딩하는 권장 방법입니다.

Cisco Plug & Play Day0를 사용하여 네트워크 디바이스를 온보딩하는 방법에는 여러 가지가 있습니다.

- DHCP 공급업체별 옵션
- DNS 조회
- Cisco 클라우드 리디렉션

공용 인터넷을 통한 보안 통신을 위해서는 DNAC에 보안 인증서를 설치해야 합니다. DHCP 서버, DNS 서버를 설정하고 SSL 인증서를 생성 및 설치하려면 이 문서를 따르십시오. 이미 인증서 + 키가 있고 DNAC에 설치해야 하는 경우 11단계의 문서를 따르십시오. 이 문서에서는

- Cat9K 디바이스는 PNP 에이전트입니다.
- pnpserver.cisco.com은 DNAC 컨트롤러의 FQDN 이름입니다.
- Cisco 스위치는 DNS 서버 및 DHCP 서버로 구성됩니다.

DNAC에 SSL 인증서 생성 및 설치

기본적으로 DNAC는 프라이빗 네트워크에서 네트워크 디바이스를 온보딩하기 위해 사전 설치된 자체 서명 인증서와 함께 제공됩니다. 그러나 공용 인터넷을 통해 원격 위치에서 온보드 네트워크 디바이스로 안전하게 통신하기 위해 내부 CA에서 유효한 X.509 인증서를 가져오는 것이 좋습니다.

다음은 DNAC에서 Cisco가 발급한 Open SSL 인증서를 다운로드하고 설치하는 예입니다.

인증서를 다운로드하려면 먼저 CSR을 생성해야 합니다.

절차

1단계. SSH 클라이언트를 사용하여 Cisco DNA Center 클러스터에 로그인하고 **/home/maglev 아래**에 임시 폴더를 생성합니다. 예를 들어, 홈 디렉토리에 있는 동안 mkdir tls**-cert;cd tls-cert 명령**을 입력합니다.

2단계. 계속 진행하기 전에 **maglev cluster network display** 명령을 사용하여 Cisco DNA Center 컨피그레이션 시 Cisco DNA Center 호스트 이름(FQDN)이 설정되었는지 확인합니다.

```
Input:

$maglev cluster network display

Output:

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

주: 이 명령을 실행하려면 루트 권한이 있어야 합니다.

출력 필드 cluster_hostname이 비어 있거나 원하는 필드가 아닌 경우 maglev cluster config-update 명령을 사용하여 Cisco DNA Center 호스트 이름(FQDN)을 추가하거나 변경합니다.

```
Input:

$maglev-config update

Output:

Maglev Config Wizard GUI
```

주: 이 명령을 실행하려면 루트 권한이 있어야 합니다.

입력 프롬프트 Cluster hostname을 포함하는 MAGLEV CLUSTER DETAILS라는 단계가 표시될 때까지 **Next**를 클릭합니다. 호스트 이름을 원하는 Cisco DNA Center FQDN으로 설정합니다. Next(**다음**)를 클릭하고 Cisco DNA Center가 새 FQDN으로 재구성될 때까지 계속 진행합니다.

3단계. 원하는 텍스트 편집기를 사용하여 openssl.**cnf**라는 파일을 생성하고 이전 단계에서 생성한 디렉토리에 업로드합니다. 이 예를 지침으로 사용하되 구축에 맞게 조정합니다.

- CA(Certificate Authority) 관리 팀에 2048/sha256이 필요한 경우 default_bits 및 default_md를 조정합니다.
- req_distinguished_name 및 alt_names 섹션의 모든 필드에 대한 값을 지정합니다. 유일한 예외는 선택 사항인 OU 필드입니다. 인증 기관 관리 팀에 OU 필드가 필요하지 않은 경우 OU 필드를 생략합니다.
- 이메일 주소 필드는 선택 사항입니다. 인증 기관 관리 팀에서 요구하지 않는 경우 생략합니다.
- alt_names 섹션: 인증서 컨피그레이션 요건은 Cisco DNA Center 버전에 따라 다릅니다.

Cisco DNA Center 인증서의 FQDN에 대한 모든 지원은 Cisco DNA Center 2.1.1 이상에서 제공됩니다. 2.1.1 이전 버전의 Cisco DNA Center의 경우 SAN(주체 대체 이름) 필드에 IP 주소가 정의된 인증서가 필요합니다. Cisco DNA Center 버전 2.1.1 이상 및 Cisco DNA Center 2.1.1 이전 버전에 대한 alt_names 섹션 컨피그레이션은 다음과 같습니다.

Cisco DNA Center 버전 2.1.1 이상:

1. alt_names 섹션에 주의하십시오. 이 섹션에는 웹 브라우저 또는 PnP 또는 Cisco ISE와 같은 자동화된 프로세스를 통해 Cisco DNA Center에 액세스하는 데 사용되는 모든 DNS 이름(Cisco DNA Center FQDN 포함)이 포함되어 있어야 합니다. alt_names 섹션의 첫 번째 DNS 항목은 Cisco DNA Center FQDN(DNS.1 = FQDN-of-Cisco-DNA-Center)을 포함해야 합니다. Cisco DNA Center FQDN 대신 와일드카드 DNS 항목을 추가할 수 없지만 대체 이름 섹션의 후속 DNS 항목에서 와일드카드를 사용할 수 있습니다(PnP 및 기타 DNS 항목의 경우). 예를 들어 *.example.com은 유효한 항목입니다.

중요: 재해 복구 설정에 동일한 인증서를 사용하는 경우 alt_names 섹션에서 재해 복구 시스템 사이트에 대한 DNS 항목을 추가하는 동안에는 와일드카드를 사용할 수 없습니다. 그러나 재해 복구 설정에는 별도의 인증서를 사용하는 것이 좋습니다. 자세한 내용은 Cisco DNA Center Administrator Guide의 "Add Disaster Recovery Certificate" 섹션을 참조하십시오.

2. alt_names 섹션은 DNS 항목으로 Cisco-DNA-Center의 FQDN을 포함해야 하며, 구성 마법사를 통해 Cisco DNA Center 구성 시 설정된 Cisco DNA Center 호스트 이름(FQDN)과 일치해야 합니다("클러스터 호스트 이름" 입력 필드). Cisco DNA Center는 현재 모든 인터페이스에 대해 하나의 호스트 이름(FQDN)만 지원합니다. 네트워크의 Cisco DNA Center에 대한 디바이스 연결을 위해 Cisco DNA Center의 관리 및 엔터프라이즈 포트를 모두 사용하는 경우, DNS 쿼리를 수신한 네트워크를 기반으로 Cisco DNA Center 호스트 이름(FQDN)에 대한 관리 IP/가상 IP 및 엔터프라이즈 IP/가상 IP로 확인하도록 GeoDNS 정책을 구성해야 합니다. 네트워크의 Cisco DNA Center에 대한 디바이스 연결을 위해 Cisco DNA Center의 엔터프라이즈 포트만 사용하는 경우 GeoDNS 정책을 설정할 필요가 없습니다.

> **참고**: Cisco DNA Center에 대해 재해 복구를 활성화한 경우, DNS 쿼리를 받은 네트워크를 기반으로 Cisco DNA Center 호스트 이름(FQDN)에 대한 재해 복구 관리 가상 IP 및 재해 복구 엔터프라이즈 가상 IP를 확인하도록 GeoDNS 정책을 구성해야 합니다.

3. 2.1.1 이전 버전의 Cisco DNA Center:

웹 브라우저 또는 PnP 또는 Cisco ISE와 같은 자동화된 프로세스를 통해 Cisco DNA Center에 액세

스하는 데 사용되는 모든 IP 주소 및 DNS 이름을 포함해야 하는 alt_names 섹션을 주의하십시오. 이 예에서는 3노드 Cisco DNA Center 클러스터를 가정합니다. 독립형 디바이스가 있는 경우 해당 노드 및 VIP에 대해서만 SAN을 사용합니다. 나중에 디바이스를 클러스터링하는 경우 새 클러스터 멤버의 IP 주소를 포함하도록 인증서를 다시 생성해야 합니다.)

클라우드 인터페이스가 구성되지 않은 경우 클라우드 포트 필드를 생략합니다.

- extendedKeyUsage 확장에서 serverAuth 및 clientAuth 특성은 필수입니다. 두 특성 중 하나를 생략하면 Cisco DNA Center에서 SSL 인증서를 거부합니다.
- 자체 서명 인증서를 가져오는 경우(권장하지 않음) X.509 Basic Constraints "CA:TRUE" 확장을 포함해야 합니다.

예 openssl.cnf(Cisco DNA Center 버전 2.1.1 이상에 적용):

```
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
```

> **참고**: openssl.cnf 파일에 클러스터 IP 주소를 포함하지 않으면 소프트웨어 이미지 활성화를 예약할 수 없습니다. 이 문제를 해결하려면 클러스터 IP 주소를 SAN으로 인증서에 추가합니다.

원하는 텍스트 편집기를 사용하여 openssl.cnf라는 파일을 생성하고 이전 단계에서 생성한 디렉토리에 업로드합니다. 이 예를 지침으로 사용하되 구축에 맞게 조정합니다.

- CA(Certificate Authority) 관리 팀에 2048/sha256이 필요한 경우 default_bits 및 default_md를 조정합니다.
- req_distinguished_name 및 alt_names 섹션의 모든 필드에 대한 값을 지정합니다. 유일한 예외는 선택 사항인 OU 필드입니다. 인증 기관 관리 팀에 OU 필드가 필요하지 않은 경우 OU 필드를 생략합니다.
- emailAddress 필드는 선택 사항입니다. 인증 기관 관리 팀에 필요하지 않은 경우 생략합니다.
- alt_names 섹션: 인증서 컨피그레이션 요건은 Cisco DNA Center 버전에 따라 다릅니다.
- FQDN은 Cisco DNA Center 2.1.1 이상에서 지원됩니다. 2.1.1 이전 버전의 Cisco DNA Center의 경우 SAN(주체 대체 이름)에 IP 주소가 있는 인증서가 필요합니다. Cisco DNA Center 버전 2.1.1 이상 및 2.1.1 이전 버전의 alt_names 섹션 구성은 다음과 같습니다.
- Cisco DNA Center 버전 2.1.1 이상:웹 브라우저 또는 PnP 또는 Cisco ISE와 같은 자동화된 프로세스에 의해 Cisco DNA Center에 액세스하는 데 사용되는 모든 DNS 이름(Cisco DNA Center FQDN 포함)을 포함해야 하는 alt_names 섹션을 주의하십시오.alt_names 섹션의 첫 번째 DNS 항목은 Cisco DNA Center의 FQDN을 포함해야 합니다(DNS.1 = FQDN-of-Cisco-DNA-Center). Cisco DNA Center의 FQDN 대신 와일드카드 DNS 항목을 추가할 수 없습니다. 그러나 alt-names 섹션의 후속 DNS 항목에서는 와일드카드를 사용할 수 있습니다(PnP 및 기타 DNS 항목의 경우). 예를 들어, *.example.com은 유효한 항목입니다.

중요: 재해 복구 설정에 동일한 인증서를 사용하는 경우 alt_names 섹션에서 재해 복구 시스템 사이트에 대한 DNS 항목을 추가하는 동안에는 와일드카드를 사용할 수 없습니다. 그러나 재해 복구 설정에는 별도의 인증서를 사용하는 것이 좋습니다. 자세한 내용은 Cisco DNA Center Administrator

Guide의 "Add Disaster Recovery Certificate" 섹션을 참조하십시오.

- alt_names 섹션은 DNS 항목으로 Cisco-DNA-Center의 FQDN을 포함해야 하며, 구성 마법사를 통해 Cisco DNA Center 컨피그레이션 시 설정된 Cisco DNA Center 호스트 이름(FQDN)과 일치해야 합니다("클러스터 호스트 이름" 입력 필드).

Cisco DNA Center는 현재 모든 인터페이스에 대해 하나의 호스트 이름(FQDN)만 지원합니다. DNS 쿼리를 받은 네트워크를 기반으로 Cisco DNA Center 호스트 이름(FQDN)에 대한 관리 IP/가상 IP 및 엔터프라이즈 IP/가상 IP로 확인하도록 GeoDNS 정책을 구성해야 합니다.

> **참고**: Cisco DNA Center에 대해 재해 복구를 활성화한 경우, DNS 쿼리를 받은 네트워크를 기반으로 Cisco DNA Center 호스트 이름(FQDN)에 대한 재해 복구 관리 가상 IP 및 재해 복구 엔터프라이즈 가상 IP를 확인하도록 GeoDNS 정책을 구성해야 합니다.

- Cisco DNA Center 2.1.1 이전 버전:

웹 브라우저 또는 PnP 또는 Cisco ISE와 같은 자동화된 프로세스를 통해 Cisco DNA Center에 액세스하는 데 사용되는 모든 IP 주소 및 DNS 이름을 포함해야 하는 alt_names 섹션을 주의하십시오. 이 예에서는 3노드 Cisco DNA Center 클러스터를 가정합니다. 독립형 디바이스가 있는 경우 해당 노드 및 VIP에 대해서만 SAN을 사용합니다. 나중에 디바이스를 클러스터링하는 경우 새 클러스터 멤버의 IP 주소를 포함하도록 인증서를 다시 생성해야 합니다.)

- 클라우드 인터페이스가 구성되지 않은 경우 클라우드 포트 필드를 생략합니다.
  - extendedKeyUsage 확장에서 serverAuth 및 clientAuth 특성은 필수입니다. 두 특성 중 하나를 생략하면 Cisco DNA Center에서 SSL 인증서를 거부합니다.
  - 자체 서명 인증서를 가져오는 경우(권장하지 않음) X.509 Basic Constraints "CA:TRUE" 확장을 포함해야 합니다.

예 openssl.cnf(Cisco DNA Center 버전 2.1.1 이상에 적용)

```
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
```

예 openssl.cnf(2.1.1 이전 Cisco DNA Center 버전에 적용)

```
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
```

> **참고**: openssl.cnf 파일에 클러스터 IP 주소를 포함하지 않으면 소프트웨어 이미지 활성화를 예약할 수 없습니다. 이 문제를 해결하려면 클러스터 IP 주소를 SAN으로 인증서에 추가합니다.

이 경우 다음 출력은 my openssl.conf의 **컨피그레이션입니다**

```
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
```

4단계. 개인 키를 만들려면 이 명령을 입력합니다. 인증 기관 관리 팀에서 필요한 경우 키 길이를 2048로 조정합니다. openssl genrsa **-out csr.key 4096**

5단계. 필드가 openssl.**cnf 파일**에 채워지면 이전 단계에서 생성한 개인 키를 사용하여 Certificate Signing Request를 생성합니다.

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

6단계. CSR(Certificate Signing Request) 내용을 확인하고 DNS 이름(및 2.1.1 이전 버전의 Cisco DNA Center IP 주소)이 Subject Alternative Name(주체 대체 이름) 필드에 올바르게 입력되었는지 확인합니다.

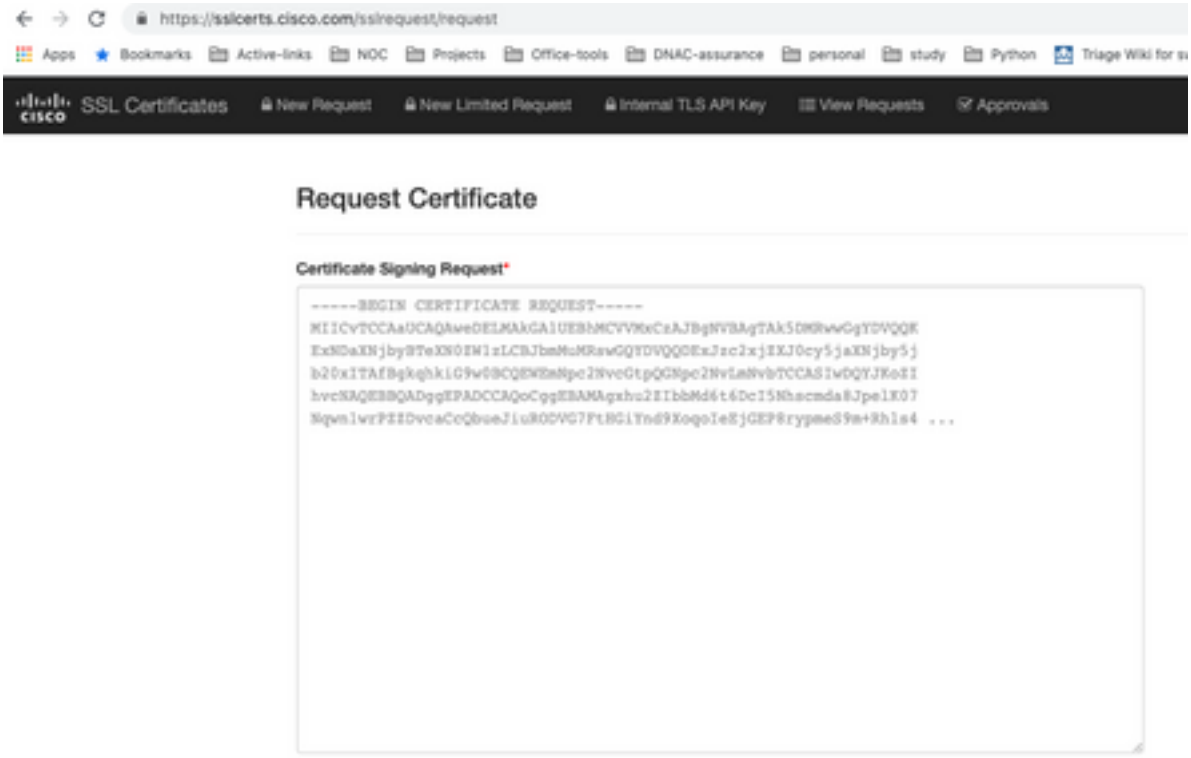
```
openssl req -text -noout -verify -in DNAC.csr
```

7단계. CSR(Certificate Signing Request)을 복사하여 CA(예: Cisco Open SSL)에 붙여넣습니다.

링크를 통해 인증서를 다운로드합니다. [Cisco SSL 인증서]

영구 인증서를 다운로드하려면 "Request Certificate(인증서 요청)"를 클릭합니다.

또는 제한된 용도로 "Request Limited Test Certificate(제한된 테스트 인증서 요청)"를 클릭합니다.



사용자는 인증서 정보가 포함된 이메일을 받습니다. 마우스 오른쪽 버튼을 클릭하고 노트북 컴퓨터의 PEM 파일 3개를 모두 다운로드합니다. 이 경우 3개의 파일을 따로 받았으므로 8단계를 건너뛰고 9단계로 진행합니다.

8단계. 인증서 발급자가 p7b에서 인증서 전체 체인(서버 및 CA)을 제공하는 경우:

DER 형식으로 p7b 번들을 다운로드하고 dnac**-chain.p7b로 저장합니다**.

SSH를 통해 dnac-chain.p7b 인증서를 Cisco DNA Center 클러스터에 복사합니다.

다음 명령을 입력합니다.

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

9단계. 인증서 발급자가 느슨한 파일에 인증서 및 발급자 CA 체인을 제공하는 경우:

PEM(base64) 파일을 다운로드하거나 openssl을 사용하여 DER를 PEM으로 변환합니다.

인증서와 발급자 CA를 연결하고, 인증서로 시작하고 그 뒤에 하위 CA를 추가하여 루트 CA까지 이동한 다음 dnac-chain.pem 파일로 출력합니다.

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

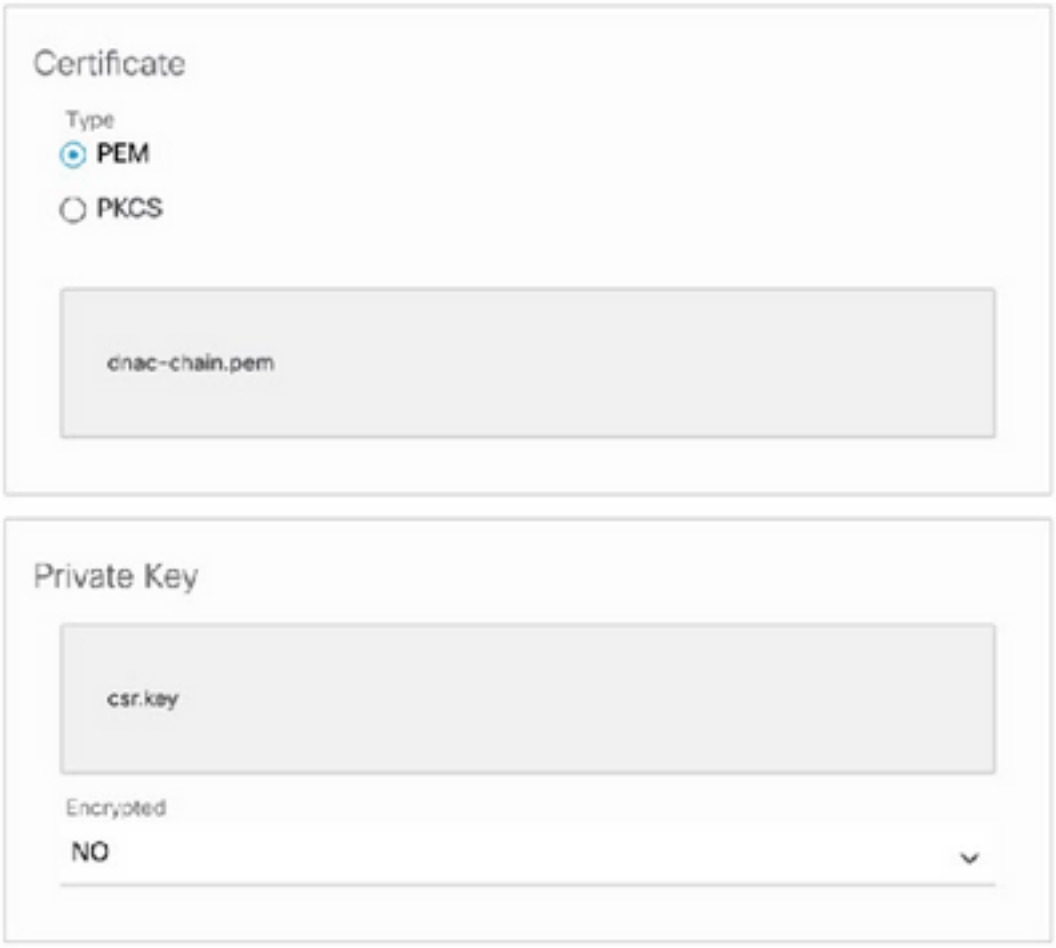
10단계. 위에서 생성한 tls-cert dir의 dnac-chain.pem 파일을 랩톱에서 Cisco DNA Center로 복사합니다.

11단계. Cisco DNA Center GUI에서 메뉴 아이콘()을 클릭하고 System(시스템) > Settings(설정) > Certificates(인증서)를 선택합니다.

12단계. Replace Certificate를 클릭합니다.

13단계. Certificate(인증서) 필드에서 PEM 라디오 버튼을 클릭하고 다음 작업을 수행합니다.

- Certificate(인증서) 필드에서 dnac-**chain.pem 파일**을 가져오려면 이 파일을 Drag n' Drop a File Here(여기에 파일 끌어놓기) 필드로 끌어서 놓습니다.
- Private Key(개인 키) 필드에서 개인 키(csr.key)를 가져오고 이 파일을 Drag n' Drop a File Here(여기에 파일 끌어오기) 필드로 끌어다 놓습니다.
- 개인 키에 대해 Encrypted(암호화됨) 드롭다운 목록에서 No(아니요)를 선택합니다.



14단계. Upload/Activate를 클릭합니다. 로그아웃했다가 DNAC에 다시 로그인합니다.

DHCP 서버 컨피그레이션

DUT에 IP 주소를 할당하도록 DHCP 서버 풀을 구성합니다. 또한 DHCP 서버를 구성합니다

도메인 이름 및 DNS 서버 IP 주소를 보냅니다.

```
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 서버 구성. 네트워크에서 DNS 서버를 구성하여 DNAC의 FQDN 이름을 확인합니다.

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

1단계. 온보딩할 새 디바이스의 케이블과 전원이 켜져 있습니다. NVRAM의 시작 컨피그레이션이

비어 있으므로 PnP 에이전트가 트리거되어 DHCP DISCOVER 메시지의 DHCP Option 60에서 "Cisco PnP"를 전송합니다.

2단계. DHCP 서버는 옵션 60에서 "Cisco PnP"를 인식하도록 구성되지 않으며 옵션 60을 무시합니다. DHCP 서버는 IP 주소를 할당하고 구성된 도메인 이름 및 DNS 서버 IP 주소와 함께 DHCP 제안을 보냅니다.

3단계. PnP 에이전트는 도메인 이름을 읽고 정규화된 PnP 서버 호스트 이름을 공식화한 다음 "pnpserver" 문자열에 도메인 이름을 추가합니다. 도메인 이름이 "example.com"인 경우 PnP 서버의 정규화된 호스트 이름은 "pnpserver.example.com"이 됩니다. PnP 에이전트는 DHCP 옵션에서 수신한 DNS 서버를 사용하여 IP 주소에 대해 "pnpserver.example.com"을 확인합니다.

온보딩을 위해 pnp 에이전트가 트리거되는 경우의 예:

브라운 필드 구축의 경우 새 스위치 또는 "write erase" 전원을 켠 다음 다시 로드

스위치 콘솔에서 다음 워크플로를 확인합니다.

```
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!
```

관련 정보

- PnP 서버 검색
- Cisco DNA Center 보안 모범 사례 가이드
- **기술 지원 및 문서 – Cisco Systems**

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.