Approvisionnement sécurisé des périphériques réseau

Table des matières

Introduction

Ce document décrit l'approche pas à pas pour qu'un périphérique Cisco intègre le réseau de manière sécurisée via la recherche DNS.

Conditions préalables

Exigences

- Connaissances de base de la gestion du centre Cisco DNA Center (DNAC)
- Connaissances de base des certificats SSL

Composants utilisés

Ce document est basé sur Cisco DNA Center (DNAC) version 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. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

La recherche DNS est un moyen recommandé d'intégrer un périphérique réseau et un contrôleur Cisco DNA Center (DNAC) sur des sites distants et de mettre en service un périphérique réseau sur Internet public.

Il existe différentes manières d'intégrer un périphérique réseau à l'aide de Cisco Plug & Play Day0.

- Options spécifiques au constructeur DHCP
- Recherche DNS
- Redirection du cloud Cisco

Afin d'avoir une communication sécurisée sur l'Internet public, vous devez installer un certificat sécurisé sur DNAC. Suivez ce document pour configurer un serveur DHCP, un serveur DNS, générer et installer un certificat SSL. Si vous disposez déjà du certificat + clé et que vous devez simplement l'installer sur DNAC, suivez le document de l'étape 11. Dans ce document :

- Le périphérique Cat9K est l'agent PNP.
- pnpserver.cisco.com est le nom de domaine complet (FQDN) du contrôleur DNAC.
- Le commutateur Cisco est configuré comme serveur DNS et serveur DHCP.

Générer et installer un certificat SSL sur DNAC

Par défaut, DNAC est fourni avec un certificat auto-signé préinstallé valide pour les périphériques réseau intégrés dans un réseau privé. Cependant, Cisco recommande d'importer un certificat X.509 valide de votre autorité de certification interne pour une communication sécurisée vers le périphérique réseau embarqué à partir d'un emplacement distant sur l'Internet public.

Voici un exemple pour télécharger et installer le certificat Open SSL émis par Cisco sur DNAC.

Pour télécharger le certificat, vous devez d'abord créer un CSR.

Procédure

Étape 1. Utilisez un client SSH pour vous connecter au cluster Cisco DNA Center et créer un dossier temporaire sous **/home/maglev**, par exemple, entrez la commande **mkdir tls-cert;cd tls-cert** dans le répertoire home.

Étape 2. Avant de continuer, assurez-vous que le nom d'hôte Cisco DNA Center (FQDN) est défini au moment de la configuration de Cisco DNA Center avec l'utilisation de la commande **maglev cluster network display** :

```
Input:

$maglev cluster network display

Output:

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

Remarque : vous devez disposer des privilèges racine pour exécuter cette commande.

Si le champ de sortie cluster_hostname est vide ou n'est pas celui que vous souhaitez, ajoutez ou modifiez le nom d'hôte Cisco DNA Center (FQDN) à l'aide de la commande maglev cluster config-update :

```
Input:
```

```
$maglev-config update

Output:

Maglev Config Wizard GUI
```

Remarque : vous devez disposer des privilèges racine pour exécuter cette commande.

Cliquez sur **Next** jusqu'à ce que vous voyiez l'étape intitulée MAGLEV CLUSTER DETAILS qui contient l'invite d'entrée Cluster hostname. Définissez le nom d'hôte sur le nom de domaine complet Cisco DNA Center souhaité. Cliquez sur **Next** et continuez jusqu'à ce que Cisco DNA Center soit reconfiguré avec le nouveau FQDN.

Étape 3. Utilisez un éditeur de texte de votre choix, créez un fichier nommé **openssl.cnf** et téléchargez-le dans le répertoire que vous avez créé à l'étape précédente. Utilisez cet exemple comme guide, mais adaptez-le à votre déploiement.

- Ajustez default_bits et default_md si l'équipe d'administration de votre autorité de certification requiert 2048/sha256 à la place.
- Spécifiez des valeurs pour chaque champ dans les sections req_nom_unique et alt_noms. La seule exception est le champ OU, qui est facultatif. Omettez le champ OU si l'équipe d'administration de votre autorité de certification ne l'exige pas.
- Le champ de l'adresse e-mail est facultatif ; ne l'indiquez pas si l'équipe d'administration de votre autorité de certification ne l'exige pas.
- alt_names : la configuration requise pour le certificat varie en fonction de la version de Cisco DNA Center.

La prise en charge complète des FQDN dans le certificat Cisco DNA Center est disponible à partir de Cisco DNA Center 2.1.1. Pour les versions de Cisco DNA Center antérieures à la version 2.1.1, vous devez disposer d'un certificat avec des adresses IP définies dans le champ Subject Alternative Name (SAN). Les configurations de la section alt_names pour Cisco DNA Center versions 2.1.1 et ultérieures et Cisco DNA Center versions antérieures à 2.1.1 sont les suivantes :

Cisco DNA Center versions 2.1.1 et ultérieures :

1. Soyez particulièrement attentif à la section alt_names, qui doit contenir tous les noms DNS (y compris le nom de domaine complet Cisco DNA Center) utilisés pour accéder à Cisco DNA Center, soit par un navigateur Web, soit par un processus automatisé tel que PnP ou Cisco ISE. La première entrée DNS de la section alt_names doit contenir le nom de domaine complet Cisco DNA Center (DNS.1 = FQDN-of-Cisco-DNA-Center). Vous ne pouvez pas ajouter d'entrée DNS générique à la place du nom de domaine complet Cisco DNA Center, mais vous pouvez utiliser un caractère générique dans les entrées DNS suivantes de la section alt-names (pour PnP et d'autres entrées DNS). Par exemple, *.example.com est une entrée valide.

Important : si vous utilisez le même certificat pour la configuration de la reprise après sinistre, les caractères génériques ne sont pas autorisés lorsque vous ajoutez une entrée DNS pour un site de système de reprise après sinistre dans la section alt_names. Cependant, nous vous recommandons d'utiliser un certificat distinct pour une configuration de reprise après sinistre. Pour plus d'informations, reportez-vous à la section « Add Disaster Recovery Certificate » du Guide de l'administrateur de Cisco DNA Center.

2. La section alt_names doit contenir FQDN-of-Cisco-DNA-Center en tant qu'entrée DNS et doit correspondre au nom d'hôte Cisco DNA Center (FQDN) défini lors de la configuration de Cisco

DNA Center via l'assistant de configuration (dans le champ d'entrée « Nom d'hôte du cluster »). Cisco DNA Center ne prend actuellement en charge qu'un seul nom d'hôte (FQDN) pour toutes les interfaces. Si vous utilisez à la fois le port de gestion et le port d'entreprise sur Cisco DNA Center pour les périphériques connectés à Cisco DNA Center sur votre réseau, vous devez configurer la stratégie GeoDNS pour résoudre les adresses IP/virtuelle de gestion et IP/virtuelle d'entreprise pour le nom d'hôte Cisco DNA Center (FQDN) en fonction du réseau à partir duquel la requête DNS est reçue. La configuration de la stratégie GeoDNS n'est pas nécessaire si vous utilisez uniquement le port d'entreprise sur Cisco DNA Center pour les périphériques connectés à Cisco DNA Center sur votre réseau.

> **Remarque** : si vous avez activé la reprise après sinistre pour Cisco DNA Center, vous devez configurer la stratégie GeoDNS pour résoudre l'adresse IP virtuelle de gestion de la reprise après sinistre et l'adresse IP virtuelle d'entreprise de reprise après sinistre pour le nom d'hôte Cisco DNA Center (FQDN) en fonction du réseau à partir duquel la requête DNS est reçue.

3. Versions de Cisco DNA Center antérieures à 2.1.1 :

Soyez particulièrement attentif à la section alt_names, qui doit contenir toutes les adresses IP et tous les noms DNS utilisés pour accéder à Cisco DNA Center, soit par un navigateur Web, soit par un processus automatisé tel que PnP ou Cisco ISE. (Dans cet exemple, nous supposons un cluster Cisco DNA Center à trois noeuds. Si vous disposez d'un périphérique autonome, utilisez des SAN uniquement pour ce noeud et le VIP. Si vous mettez le périphérique en grappe ultérieurement, vous devez recréer le certificat pour inclure les adresses IP des nouveaux membres de la grappe.)

Si une interface cloud n'est pas configurée, omettez les champs de port cloud.

- Dans l'extension extendedKeyUsage, les attributs serverAuth et clientAuth sont obligatoires. Si vous omettez l'un ou l'autre attribut, Cisco DNA Center rejette le certificat SSL.
- Si vous importez un certificat auto-signé (non recommandé), il doit contenir l'extension "CA : TRUE" des contraintes de base X.509.

Exemple de fichier openssl.cnf (applicable aux versions 2.1.1 et ultérieures de Cisco DNA Center) :

```
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
```

> **Remarque** : si vous n'incluez pas les adresses IP du cluster dans le fichier **openssl.cnf**, vous ne pouvez pas planifier l'activation de l'image logicielle. Pour résoudre ce problème, ajoutez les adresses IP de cluster en tant que SAN au certificat.

Utilisez un éditeur de texte de votre choix, créez un fichier nommé **openssl.cnf** et téléchargez-le dans le répertoire que vous avez créé à l'étape précédente. Utilisez cet exemple comme guide,

mais adaptez-le à votre déploiement.

- Ajustez default_bits et default_md si l'équipe d'administration de votre autorité de certification requiert 2048/sha256 à la place.
- Spécifiez des valeurs pour chaque champ dans les sections req_nom_unique et alt_noms. La seule exception est le champ OU, qui est facultatif. Omettez le champ OU si l'équipe d'administration de votre autorité de certification ne l'exige pas.
- Le champ emailAddress est facultatif ; omettez-le si l'équipe d'administration de votre autorité de certification ne l'exige pas.
- alt_names : la configuration requise pour le certificat varie en fonction de la version de Cisco DNA Center.
- La prise en charge des FQDN est disponible à partir de Cisco DNA Center 2.1.1. Pour les versions de Cisco DNA Center antérieures à la version 2.1.1, vous devez disposer d'un certificat avec des adresses IP dans le champ Subject Alternative Name (SAN). Les configurations de la section alt_names pour les versions 2.1.1 et ultérieures de Cisco DNA Center et les versions antérieures à 2.1.1 de Cisco DNA Center sont les suivantes :
- Cisco DNA Center versions 2.1.1 et ultérieures :Soyez particulièrement attentif à la section alt_names, qui doit contenir tous les noms DNS (y compris le nom de domaine complet Cisco DNA Center) utilisés pour accéder à Cisco DNA Center, soit par un navigateur Web, soit par un processus automatisé tel que PnP ou Cisco ISE.La première entrée DNS de la section alt_names doit contenir le nom de domaine complet de Cisco DNA Center (DNS.1 = FQDN-of-Cisco-DNA-Center). Vous ne pouvez pas ajouter une entrée DNS générique à la place du nom de domaine complet de Cisco DNA Center. Mais vous pouvez utiliser un caractère générique dans les entrées DNS suivantes dans la section alt-names (pour PnP et d'autres entrées DNS). Par exemple, *.exemple.com est une entrée valide.

Important : si vous utilisez le même certificat pour la configuration de la reprise après sinistre, les caractères génériques ne sont pas autorisés lorsque vous ajoutez une entrée DNS pour un site de système de reprise après sinistre dans la section alt_names. Cependant, nous vous recommandons d'utiliser un certificat distinct pour une configuration de reprise après sinistre. Pour plus d'informations, reportez-vous à la section « Add Disaster Recovery Certificate » du Guide de l'administrateur de Cisco DNA Center.

- La section alt_names doit contenir FQDN-of-Cisco-DNA-Center en tant qu'entrée DNS et doit correspondre au nom d'hôte Cisco DNA Center (FQDN) défini lors de la configuration de Cisco DNA Center via l'assistant de configuration (dans le champ d'entrée « Nom d'hôte du cluster »).

Cisco DNA Center ne prend actuellement en charge qu'un seul nom d'hôte (FQDN) pour toutes les interfaces. Vous devez configurer la stratégie GeoDNS pour résoudre les adresses IP/virtuelles de gestion et IP/virtuelles d'entreprise pour le nom d'hôte Cisco DNA Center (FQDN) en fonction du réseau à partir duquel la requête DNS est reçue.

Remarque : si vous avez activé la reprise après sinistre pour Cisco DNA Center, vous devez configurer la stratégie GeoDNS pour résoudre l'adresse IP virtuelle de gestion de la reprise après sinistre et l'adresse IP virtuelle d'entreprise de reprise après sinistre pour le nom d'hôte Cisco DNA Center (FQDN) en fonction du réseau à partir duquel la requête DNS est reçue.

- Versions de Cisco DNA Center antérieures à 2.1.1 :

Soyez particulièrement attentif à la section alt_names, qui doit contenir toutes les adresses IP et tous les noms DNS utilisés pour accéder à Cisco DNA Center, soit par un navigateur Web, soit par un processus automatisé tel que PnP ou Cisco ISE. (Dans cet exemple, nous supposons un cluster Cisco DNA Center à trois noeuds. Si vous disposez d'un périphérique autonome, utilisez des SAN uniquement pour ce noeud et le VIP. Si vous mettez le périphérique en grappe ultérieurement, vous devez recréer le certificat pour inclure les adresses IP des nouveaux membres de la grappe.)

- Si une interface cloud n'est pas configurée, omettez les champs de port cloud.
  - Dans l'extension extendedKeyUsage, les attributs serverAuth et clientAuth sont obligatoires. Si vous omettez l'un ou l'autre attribut, Cisco DNA Center rejette le certificat SSL.
  - Si vous importez un certificat auto-signé (non recommandé), il doit contenir l'extension "CA : TRUE" des contraintes de base X.509.

Exemple de fichier openssl.cnf (applicable à Cisco DNA Center versions 2.1.1 et ultérieures)

```
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
```

Exemple openssl.cnf (applicable aux versions de Cisco DNA Center antérieures à 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
```

> **Remarque** : si vous n'incluez pas les adresses IP du cluster dans le fichier **openssl.cnf**, vous ne pouvez pas planifier l'activation de l'image logicielle. Pour résoudre ce problème, ajoutez les adresses IP de cluster en tant que SAN au certificat.

Dans ce cas, le résultat suivant est la configuration de 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
```

Étape 4. Entrez cette commande pour créer une clé privée. Réglez la longueur de clé sur 2048 si l'équipe d'administration de votre autorité de certification l'exige. **openssl genrsa -out csr.key 4096**

Étape 5. Une fois les champs remplis dans le fichier **openssl.cnf**, utilisez la clé privée que vous avez créée à l'étape précédente pour générer la demande de signature de certificat.

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

Étape 6. Vérifiez le contenu de la demande de signature de certificat et assurez-vous que les noms DNS (et les adresses IP pour la version de Cisco DNA Center antérieure à 2.1.1) sont correctement renseignés dans le champ Subject Alternative Name (Autre nom de l'objet).

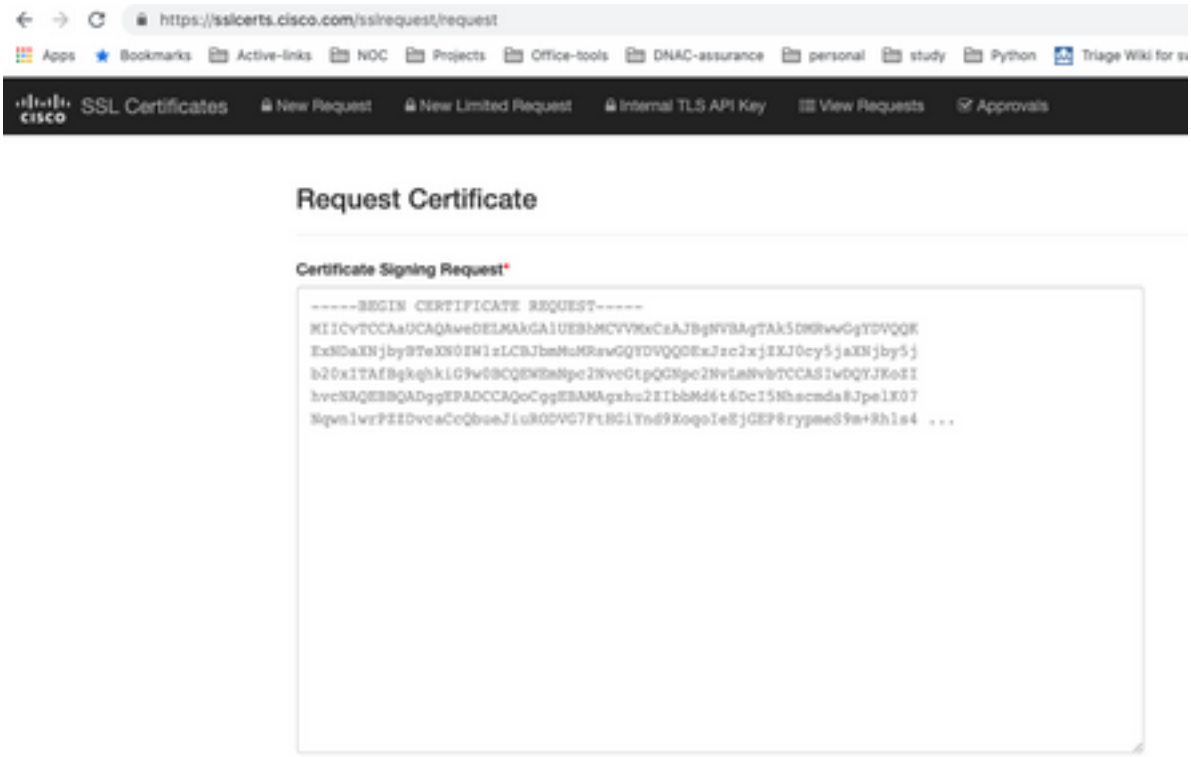
```
openssl req -text -noout -verify -in DNAC.csr
```

Étape 7. Copiez la demande de signature de certificat et collez-la dans une autorité de certification (exemple : Cisco Open SSL).

Cliquez sur le lien pour télécharger le certificat. Certificats Cisco SSL

Cliquez sur « Demander un certificat » pour télécharger un certificat permanent.

Ou cliquez sur « Demander un certificat de test limité » à des fins limitées.



L'utilisateur reçoit un e-mail contenant les informations de certificat. Cliquez avec le bouton droit et téléchargez les trois fichiers PEM sur votre ordinateur portable. Dans ce cas, j'ai reçu 3 fichiers distincts. Ignorez donc l'étape 8 et passez à l'étape 9.

Étape 8. Si l'émetteur du certificat fournit la chaîne complète du certificat (serveur et CA) dans p7b :

Téléchargez le bundle p7b au format DER et enregistrez-le sous le nom **dnac-chain.p7b**.

Copiez le certificat dnac-chain.p7b vers le cluster Cisco DNA Center via SSH.

Entrez cette commande :

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

Étape 9. Si l'émetteur du certificat fournit le certificat et sa chaîne CA d'émetteur dans des fichiers en vrac :

Téléchargez les fichiers PEM (base64) ou utilisez openssl pour convertir DER en PEM.

Concaténez le certificat et son autorité de certification émettrice, commencez par le certificat, suivi par l'autorité de certification subordonnée, jusqu'à l'autorité de certification racine, et sortez-le dans le fichier dnac-chain.pem.

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

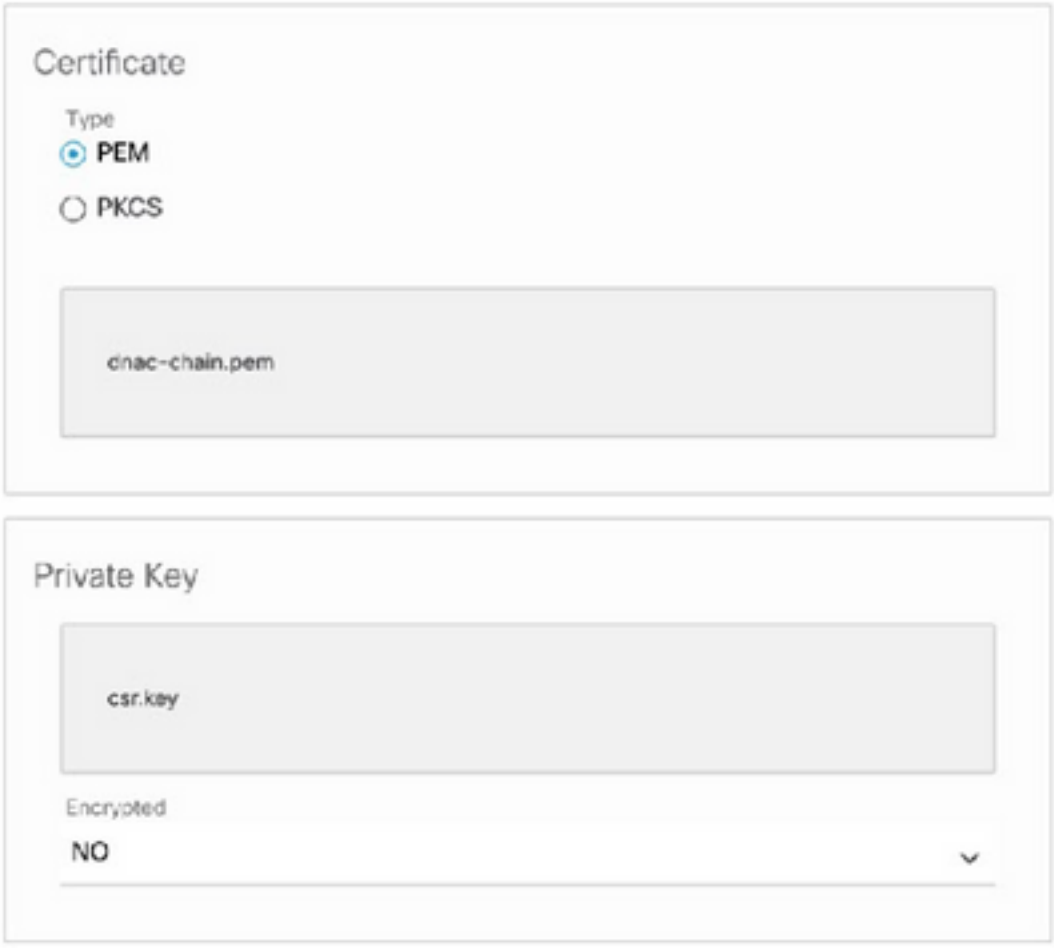
Étape 10. Copiez le fichier dnac-chain.pem de votre ordinateur portable vers Cisco DNA Center dans le répertoire tls-cert créé ci-dessus.

Étape 11. Dans l'interface utilisateur graphique de Cisco DNA Center, cliquez sur l'icône Menu () et choisissez Système > Paramètres > Certificats.

Étape 12. Cliquez sur Remplacer le certificat.

Étape 13. Dans le champ Certificate (Certificat), cliquez sur la case d'option PEM et effectuez les tâches suivantes.

- Pour le champ Certificate, importez le fichier **dnac-chain.pem**, faites simplement glisser et déposez ce fichier dans le champ Drag n'Drop a File Here.
- Pour le champ Private Key (Clé privée), importez la clé privée (csr.key), faites simplement glisser et déposez ce fichier dans le champ Drag n'Drop a File Here (Faites glisser et déposez un fichier ici).
- Sélectionnez Non dans la liste déroulante Chiffré pour la clé privée.



Étape 14. Cliquez sur Upload/Activate. Déconnectez-vous et reconnectez-vous à DNAC.

Configuration du serveur DHCP

Configurez un pool de serveurs DHCP pour attribuer une adresse IP au DUT. Configure également le serveur DHCP

pour envoyer le nom de domaine et l'adresse IP du serveur 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
```

Configuration du serveur DNS. Configurez un serveur DNS sur votre réseau pour résoudre le nom

de domaine complet du DNAC.

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

Étape 1. Le nouveau périphérique à intégrer est câblé et sous tension. Comme la configuration initiale de la mémoire NVRAM est vide, l'agent PnP est déclenché et envoie le message « Cisco PnP » dans DHCP Option 60 dans DHCP DISCOVER.

Étape 2. Le serveur DHCP n'est pas configuré pour reconnaître « Cisco PnP » dans l'option 60, il ignore l'option 60. Le serveur DHCP attribue une adresse IP et envoie une offre DHCP avec le nom de domaine configuré et l'adresse IP du serveur DNS.

Étape 3. L'agent Plug and Play lit le nom de domaine et formule le nom d'hôte complet du serveur Plug and Play et ajoute le nom de domaine à la chaîne « pnpserver ». Si le nom de domaine est « example.com », le nom d'hôte complet du serveur Plug and Play sera « pnpserver.example.com ». L'agent Plug and Play résout « pnpserver.example.com » pour son adresse IP avec le serveur DNS reçu dans les options DHCP.

Exemple lorsque l'agent pnp est déclenché pour l'intégration :

Mettez sous tension un nouveau commutateur ou « effacez l'écriture », puis rechargez-le en cas de déploiement sur un champ marron

Vérifiez le workflow suivant sur la console du commutateur.

```
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!
```

Informations connexes

- Détection de serveur PnP
- Guide des meilleures pratiques de sécurité Cisco DNA Center
- **Technical Support & Documentation - Cisco Systems**

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.