Provisioning dei dispositivi di rete protetti

Sommario

Introduzione

Questo documento descrive l'approccio dettagliato di un dispositivo Cisco per una connessione protetta alla rete tramite ricerca DNS.

Prerequisiti

Requisiti

- Conoscenze base della gestione di Cisco DNA Center (DNAC)
- Conoscenze base dei certificati SSL

Componenti usati

Questo documento è basato sulla versione 2.1.x di Cisco DNA Center (DNAC).

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

La ricerca DNS è un metodo consigliato per la connessione quando il dispositivo di rete e il controller Cisco DNA Center (DNAC) si trovano in siti remoti e si desidera effettuare il provisioning di un dispositivo di rete tramite Internet pubblica.

Ci sono diversi modi per integrare un dispositivo di rete con l'uso di Cisco Plug & Play Day0.

- Opzioni specifiche del fornitore DHCP
- Ricerca DNS

- Cisco Cloud Redirection

Per garantire comunicazioni protette su Internet, è necessario installare un certificato protetto su DNAC. Seguire questo documento per configurare un server DHCP, un server DNS, generare e installare un certificato SSL. Se si dispone già del certificato + della chiave ed è sufficiente installarlo su DNAC, seguire il documento dal Passaggio 11. Nel presente documento:

- Il dispositivo Cat9K è l'agente PNP.
- pnpserver.cisco.com è il nome FQDN del controller DNAC.
- Lo switch Cisco è configurato come server DNS e server DHCP.

Genera e installa certificato SSL su DNAC

Per impostazione predefinita, DNAC viene fornito con un certificato autofirmato preinstallato valido per i dispositivi di rete integrati in una rete privata. Tuttavia, Cisco consiglia di importare un certificato X.509 valido dalla CA interna per garantire una comunicazione sicura con il dispositivo di rete integrato da una postazione remota tramite Internet pubblica.

Di seguito è riportato un esempio per scaricare e installare il certificato Open SSL rilasciato da Cisco su DNAC.

Per scaricare il certificato, è innanzitutto necessario creare un CSR.

Procedura

Passaggio 1. Utilizzare un client SSH per accedere al cluster Cisco DNA Center e creare una cartella temporanea in **/home/maglev**, ad esempio, immettere il comando **mkdir tls-cert;cd tls-cert** nella directory principale.

Passaggio 2. Prima di procedere, verificare che il nome host (FQDN) di Cisco DNA Center sia impostato al momento della configurazione di Cisco DNA Center con il comando **maglev cluster network display**:

```
Input:

$maglev cluster network display

Output:

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

Nota: per eseguire questo comando è necessario disporre dei privilegi root.

Se il campo di output cluster_hostname è vuoto o non è quello desiderato, aggiungere o modificare il nome host Cisco DNA Center (FQDN) con il comando maglev cluster config-update:

```
Input:

$maglev-config update
```

```
Output:

Maglev Config Wizard GUI
```

> **Nota**: per eseguire questo comando è necessario disporre dei privilegi root.

Fare clic su **Avanti** finché non viene visualizzato il passo denominato DETTAGLI CLUSTER MAGLEV contenente il prompt di input Nome host cluster. Impostare il nome host sul nome FQDN Cisco DNA Center desiderato. Fare clic su **Avanti** e continuare finché Cisco DNA Center non viene riconfigurato con il nuovo FQDN.

Passaggio 3. Utilizzare un editor di testo, creare un file denominato **openssl.cnf** e caricarlo nella directory creata nel passaggio precedente. Utilizzare questo esempio come guida, ma modificarlo per adattarlo alla distribuzione.

- Regolare default_bits e default_md se il team di amministrazione dell'autorità di certificazione richiede 2048/sha256.
- Specificare i valori per ogni campo nelle sezioni req_distinguished_name e alt_names. L'unica eccezione è rappresentata dal campo OU, che è facoltativo. Omettere il campo OU se non è richiesto dal team di amministrazione dell'Autorità di certificazione.
- Il campo dell'indirizzo di posta elettronica è facoltativo. Ometterlo se non è richiesto dal team di amministrazione dell'autorità di certificazione.
- sezione alt_names: i requisiti di configurazione dei certificati variano in base alla versione di Cisco DNA Center.

Il supporto completo degli FQDN nel certificato Cisco DNA Center è disponibile a partire da Cisco DNA Center 2.1.1. Per le versioni di Cisco DNA Center precedenti alla 2.1.1, è necessario un certificato con indirizzi IP definiti nel campo SAN (Subject Alternative Name). Di seguito sono riportate le configurazioni della sezione alt_names per Cisco DNA Center versioni 2.1.1 e successive e per Cisco DNA Center versioni precedenti alla 2.1.1:

Cisco DNA Center versione 2.1.1 e successive:

1. Prestare particolare attenzione alla sezione alt_names, che deve contenere tutti i nomi DNS (che include il nome di dominio completo (FQDN) di Cisco DNA Center, utilizzati per accedere a Cisco DNA Center, sia tramite un browser Web sia tramite un processo automatizzato, quale PnP o Cisco ISE. La prima voce DNS nella sezione alt_names deve contenere Cisco DNA Center FQDN (DNS.1 = FQDN-of-Cisco-DNA-Center). Non è possibile aggiungere una voce DNS con caratteri jolly al posto dell'FQDN di Cisco DNA Center, ma è possibile utilizzare un carattere jolly nelle voci DNS successive nella sezione alt-names (per PnP e altre voci DNS). Ad esempio, *.example.com è una voce valida.

Importante: se si utilizza lo stesso certificato per l'installazione del ripristino di emergenza, i caratteri jolly non sono consentiti quando si aggiunge una voce DNS per un sito di sistema di ripristino di emergenza nella sezione alt_names. È tuttavia consigliabile utilizzare un certificato separato per l'installazione del ripristino di emergenza. Per ulteriori informazioni, vedere la sezione "Add Disaster Recovery Certificate" nel manuale Cisco DNA Center Administrator Guide.

2. La sezione alt_names deve contenere l'FQDN di Cisco DNA-Center come voce DNS e deve corrispondere al nome host Cisco DNA Center (FQDN) impostato al momento della configurazione di Cisco DNA Center tramite la configurazione guidata (nel campo di input "Cluster hostname"). Cisco DNA Center supporta attualmente un solo nome host (FQDN) per tutte le interfacce. Se si utilizzano sia la porta di gestione che la porta enterprise su Cisco DNA Center per

la connessione dei dispositivi a Cisco DNA Center nella rete, è necessario configurare i criteri GeoDNS per risolvere i problemi relativi all'IP/IP virtuale e all'IP/IP virtuale dell'organizzazione per il nome host (FQDN) di Cisco DNA Center in base alla rete da cui viene ricevuta la query DNS. L'impostazione dei criteri GeoDNS non è richiesta se si utilizza solo la porta enterprise su Cisco DNA Center per la connessione dei dispositivi a Cisco DNA Center nella rete.

> Nota: se è stato abilitato il ripristino di emergenza per Cisco DNA Center, è necessario configurare i criteri GeoDNS per risolvere l'IP virtuale di gestione del ripristino di emergenza e l'IP virtuale aziendale di ripristino di emergenza per il nome host Cisco DNA Center (FQDN) in base alla rete da cui viene ricevuta la query DNS.

3. Cisco DNA Center versioni precedenti alla 2.1.1:

Prestare particolare attenzione alla sezione alt_names, che deve contenere tutti gli indirizzi IP e i nomi DNS utilizzati per accedere a Cisco DNA Center, sia tramite un browser Web sia tramite un processo automatizzato, quale PnP o Cisco ISE. (Nell'esempio si presuppone un cluster Cisco DNA Center a tre nodi. Se si dispone di un dispositivo autonomo, utilizzare le SAN solo per il nodo e l'indirizzo VIP. Se il dispositivo viene inserito in un cluster in un secondo momento, sarà necessario ricreare il certificato per includere gli indirizzi IP dei nuovi membri del cluster.)

Se non è configurata un'interfaccia cloud, omettere i campi della porta cloud.

- Nell'estensione extendedKeyUsage, gli attributi serverAuth e clientAuth sono obbligatori. Se si omette uno degli attributi, Cisco DNA Center rifiuta il certificato SSL.
- Se si importa un certificato autofirmato (scelta non consigliata), deve contenere l'estensione X.509 Basic Constraints "CA:TRUE".

Esempio di openssl.cnf (applicabile a Cisco DNA Center versione 2.1.1 e successive):

```
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
```

> **Nota**: se gli indirizzi IP del cluster non vengono inclusi nel file **openssl.cnf**, non è possibile pianificare l'attivazione dell'immagine software. Per risolvere il problema, aggiungere gli indirizzi IP del cluster come SAN al certificato.

Utilizzare un editor di testo, creare un file denominato **openssl.cnf** e caricarlo nella directory creata nel passaggio precedente. Utilizzare questo esempio come guida, ma modificarlo per adattarlo alla distribuzione.

- Regolare default_bits e default_md se il team di amministrazione dell'autorità di certificazione richiede 2048/sha256.
- Specificare i valori per ogni campo nelle sezioni req_distinguished_name e alt_names. L'unica eccezione è rappresentata dal campo OU, che è facoltativo. Omettere il campo OU se non è richiesto dal team di amministrazione dell'Autorità di certificazione.

- Il campo emailAddress è facoltativo. Ometterlo se non è richiesto dal team di amministrazione dell'autorità di certificazione.
- sezione alt_names: i requisiti di configurazione dei certificati variano in base alla versione di Cisco DNA Center.
- Il supporto per gli FQDN è disponibile da Cisco DNA Center versione 2.1.1 in poi. Per le versioni di Cisco DNA Center precedenti alla 2.1.1, è necessario un certificato con indirizzi IP nella rete SAN (Subject Alternative Name). Di seguito sono riportate le configurazioni della sezione alt_names per Cisco DNA Center versioni 2.1.1 e successive e per Cisco DNA Center versioni precedenti alla 2.1.1.:
- Cisco DNA Center versione 2.1.1 e successive:Prestare particolare attenzione alla sezione alt_names, che deve contenere tutti i nomi DNS (che include il nome di dominio completo (FQDN) di Cisco DNA Center, utilizzati per accedere a Cisco DNA Center, sia tramite un browser Web sia tramite un processo automatizzato, quale PnP o Cisco ISE.La prima voce DNS nella sezione alt_names deve contenere il nome FQDN di Cisco DNA Center (DNS.1 = FQDN-of-Cisco-DNA-Center). Non è possibile aggiungere una voce DNS con caratteri jolly al posto dell'FQDN di Cisco DNA Center. È tuttavia possibile utilizzare un carattere jolly nelle voci DNS successive nella sezione alt-names (per PnP e altre voci DNS). *.example.com, ad esempio, è una voce valida.

Importante: se si utilizza lo stesso certificato per l'installazione del ripristino di emergenza, i caratteri jolly non sono consentiti quando si aggiunge una voce DNS per un sito di sistema di ripristino di emergenza nella sezione alt_names. È tuttavia consigliabile utilizzare un certificato separato per l'installazione del ripristino di emergenza. Per ulteriori informazioni, vedere la sezione "Add Disaster Recovery Certificate" nel manuale Cisco DNA Center Administrator Guide.

- La sezione alt_names deve contenere l'FQDN di Cisco DNA-Center come voce DNS e deve corrispondere al nome host Cisco DNA Center (FQDN) impostato al momento della configurazione di Cisco DNA Center tramite la configurazione guidata (nel campo di input "Nome host cluster").

Cisco DNA Center supporta attualmente un solo nome host (FQDN) per tutte le interfacce. È necessario configurare il criterio GeoDNS per la risoluzione dell'IP/IP virtuale e dell'IP/IP virtuale dell'organizzazione per il nome host (FQDN) di Cisco DNA Center in base alla rete da cui viene ricevuta la query DNS.

Nota: se è stato abilitato il ripristino di emergenza per Cisco DNA Center, è necessario configurare i criteri GeoDNS per risolvere l'IP virtuale di gestione del ripristino di emergenza e l'IP virtuale aziendale di ripristino di emergenza per il nome host Cisco DNA Center (FQDN) in base alla rete da cui viene ricevuta la query DNS.

- Cisco DNA Center versioni precedenti alla 2.1.1:

Prestare particolare attenzione alla sezione alt_names, che deve contenere tutti gli indirizzi IP e i nomi DNS utilizzati per accedere a Cisco DNA Center, sia tramite un browser Web sia tramite un processo automatizzato, quale PnP o Cisco ISE. (Nell'esempio si presuppone un cluster Cisco DNA Center a tre nodi. Se si dispone di un dispositivo autonomo, utilizzare le SAN solo per il nodo e l'indirizzo VIP. Se il dispositivo viene inserito in un cluster in un secondo momento, sarà necessario ricreare il certificato per includere gli indirizzi IP dei nuovi membri del cluster.)

- Se non è configurata un'interfaccia cloud, omettere i campi della porta cloud.
  - Nell'estensione extendedKeyUsage, gli attributi serverAuth e clientAuth sono obbligatori.

Se si omette uno degli attributi, Cisco DNA Center rifiuta il certificato SSL.

- Se si importa un certificato autofirmato (scelta non consigliata), deve contenere l'estensione X.509 Basic Constraints "CA:TRUE".

Esempio di openssl.cnf (applicabile a Cisco DNA Center versioni 2.1.1 e successive)

```
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
```

Esempio di openssl.cnf (applicabile alle versioni di Cisco DNA Center precedenti alla 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
```

> **Nota**: se gli indirizzi IP del cluster non vengono inclusi nel file **openssl.cnf**, non è possibile pianificare l'attivazione dell'immagine software. Per risolvere il problema, aggiungere gli indirizzi IP del cluster come SAN al certificato.

In questo caso, l'output successivo è la configurazione di **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
```

Passaggio 4. Immettere questo comando per creare una chiave privata. Impostare la lunghezza della chiave su 2048 se richiesto dal team di amministrazione dell'autorità di certificazione.
openssl genrsa -out csr.key 4096

Passaggio 5. Dopo aver popolato i campi nel file **openssl.cnf**, utilizzare la chiave privata creata nel passaggio precedente per generare la richiesta di firma del certificato.

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

Passaggio 6. Verificare il contenuto della richiesta di firma del certificato e assicurarsi che i nomi DNS (e gli indirizzi IP per Cisco DNA Center versione precedente alla 2.1.1) siano popolati correttamente nel campo Nome alternativo soggetto.

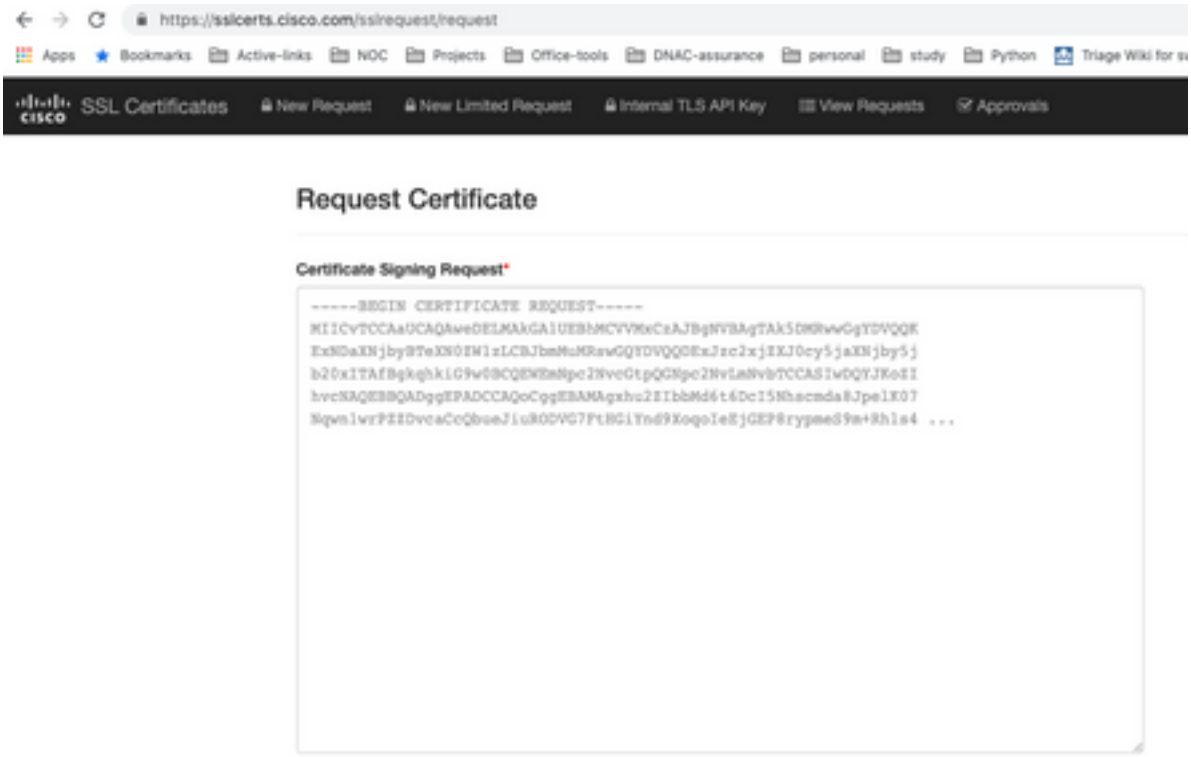
```
openssl req -text -noout -verify -in DNAC.csr
```

Passaggio 7. Copiare la richiesta di firma del certificato e incollarla in una CA (ad esempio, Cisco Open SSL).

Fare clic sul collegamento per scaricare il certificato. Certificati SSL Cisco

Fare clic su "Request Certificate" (Richiedi certificato) per scaricare il certificato permanente.

In alternativa, fare clic su "Richiedi certificato di prova limitato" per scopi limitati.



L'utente riceve un messaggio di posta elettronica con le informazioni sul certificato. Fare clic con il pulsante destro del mouse e scaricare tutti e tre i file PEM sul notebook. In questo caso, sono stati ricevuti 3 file separati, quindi saltare il passaggio 8 e passare al passaggio 9.

Passaggio 8. Se l'autorità di certificazione fornisce la catena completa del certificato (server e CA) in p7b:

Scaricate il pacchetto p7b in formato DER e salvatelo come **dnac-chain.p7b**.

Copiare il certificato dnac-chain.p7b sul cluster Cisco DNA Center tramite SSH.

Immettere questo comando:

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

Passaggio 9. Se l'autorità di certificazione fornisce il certificato e la catena di CA dell'autorità di certificazione in file liberi:

Scaricare i file PEM (base64) o utilizzare openssl per convertire DER in PEM.

Concatenare il certificato e la relativa CA emittente, iniziare con il certificato, seguito dalla CA subordinata, fino alla CA radice e inviarlo al file dnac-chain.pem.

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

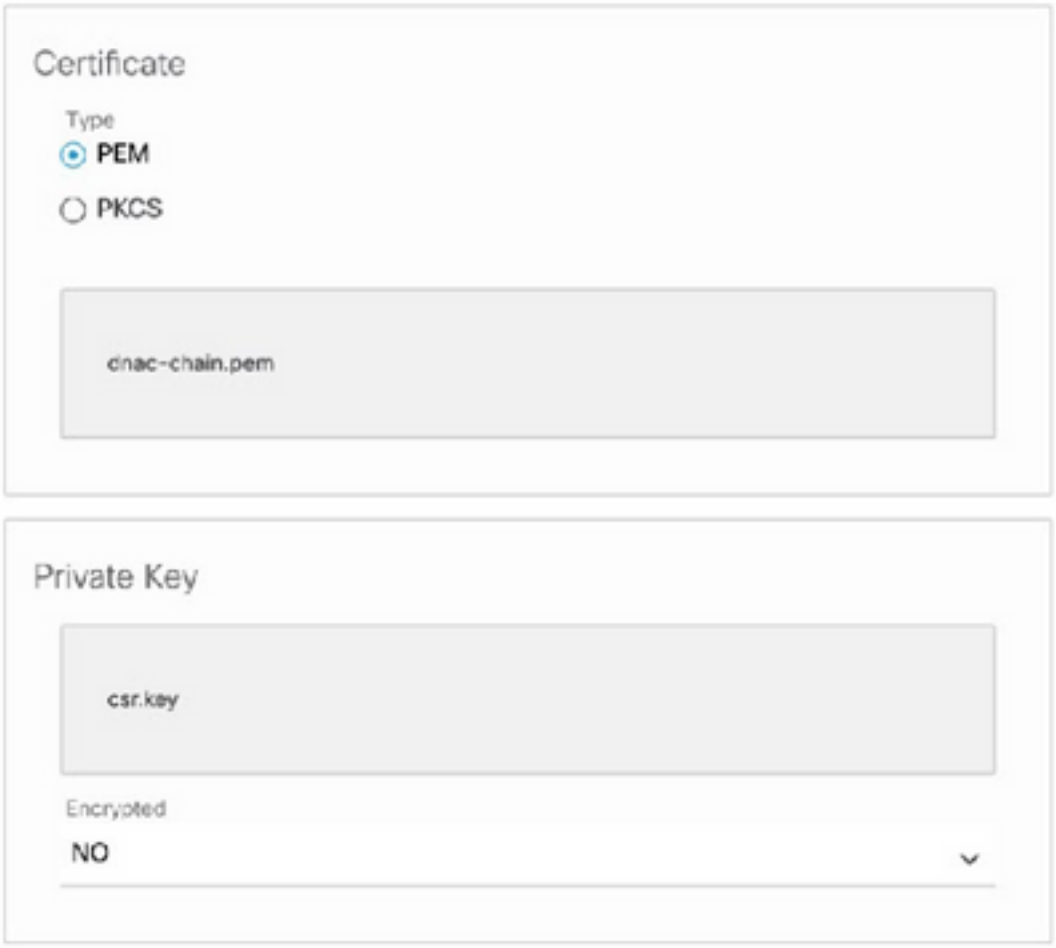
Passaggio 10. Copiare il file dnac-chain.pem dal notebook al Cisco DNA Center in tls-cert dir creato in precedenza.

Passaggio 11. Nell'interfaccia utente di Cisco DNA Center, fare clic sull'icona Menu () e scegliere Sistema > Impostazioni > Certificati.

Passaggio 12. Scegliere Sostituisci certificato.

Passaggio 13. Nel campo Certificato, fare clic sul pulsante di opzione PEM ed eseguire le operazioni successive.

- Per il campo Certificato, importare il file **dnac-chain.pem**, quindi trascinare e rilasciare il file nel campo Trascina un file qui.
- Per il campo Chiave privata, importare la chiave privata (csr.key), trascinare e rilasciare questo file nel campo Trascina un file qui.
- Scegliere No dall'elenco a discesa Crittografato per la chiave privata.



Passaggio 14. Fare clic su Carica/Attiva. Uscire e accedere nuovamente a DNAC.

Configurazione server DHCP

Configurare un pool di server DHCP per assegnare l'indirizzo IP alla rete DUT. Configura anche il server DHCP

per inviare nome di dominio e indirizzo IP del server 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
```

Configurazione del server DNS. Configurare un server DNS nella rete per risolvere il nome FQDN del DNAC.

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

Passaggio 1. La nuova periferica da caricare è collegata e accesa. Poiché la configurazione di avvio nella NVRAM è vuota, viene attivato l'agente PnP che invia "Cisco PnP" nell'opzione DHCP 60 nel messaggio DHCP DISCOVER.

Passaggio 2. Il server DHCP non è configurato per riconoscere "Cisco PnP" nell'opzione 60, quindi ignora l'opzione 60. Il server DHCP assegna un indirizzo IP e invia l'offerta DHCP insieme al nome di dominio configurato e all'indirizzo IP del server DNS.

Passaggio 3. L'agente PnP legge il nome di dominio e formula il nome host completo del server PnP e aggiunge il nome di dominio alla stringa "pnpserver". Se il nome di dominio è "example.com", il nome host completo del server PnP sarà "pnpserver.example.com". L'agente PnP risolve "pnpserver.example.com" per il proprio indirizzo IP con il server DNS ricevuto nelle opzioni DHCP.

Esempio di attivazione dell'agente pnp per la registrazione:

Accendere un nuovo switch o eseguire la "cancellazione in scrittura", quindi ricaricarlo in caso di installazione sul campo

Verificare il workflow successivo sulla console dello 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!
```

Informazioni correlate

- Individuazione server PnP
- Guida alle best practice per Cisco DNA Center Security
- **Documentazione e supporto tecnico – Cisco Systems**

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).