Sostituisci certificato di identità di Gestore telemetria

Sommario

Introduzione

In questo documento viene descritto come sostituire il certificato di identità del server nel nodo di gestione CTB (Cisco Telemetry Broker).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Amministrazione appliance Cisco Telemetry Broker
- Certificati X509

Componenti usati

Gli accessori utilizzati per questo documento eseguono la versione 2.0.1

- Nodo gestione broker di telemetria Cisco
- Nodo broker di telemetria Cisco

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.

Configurazione

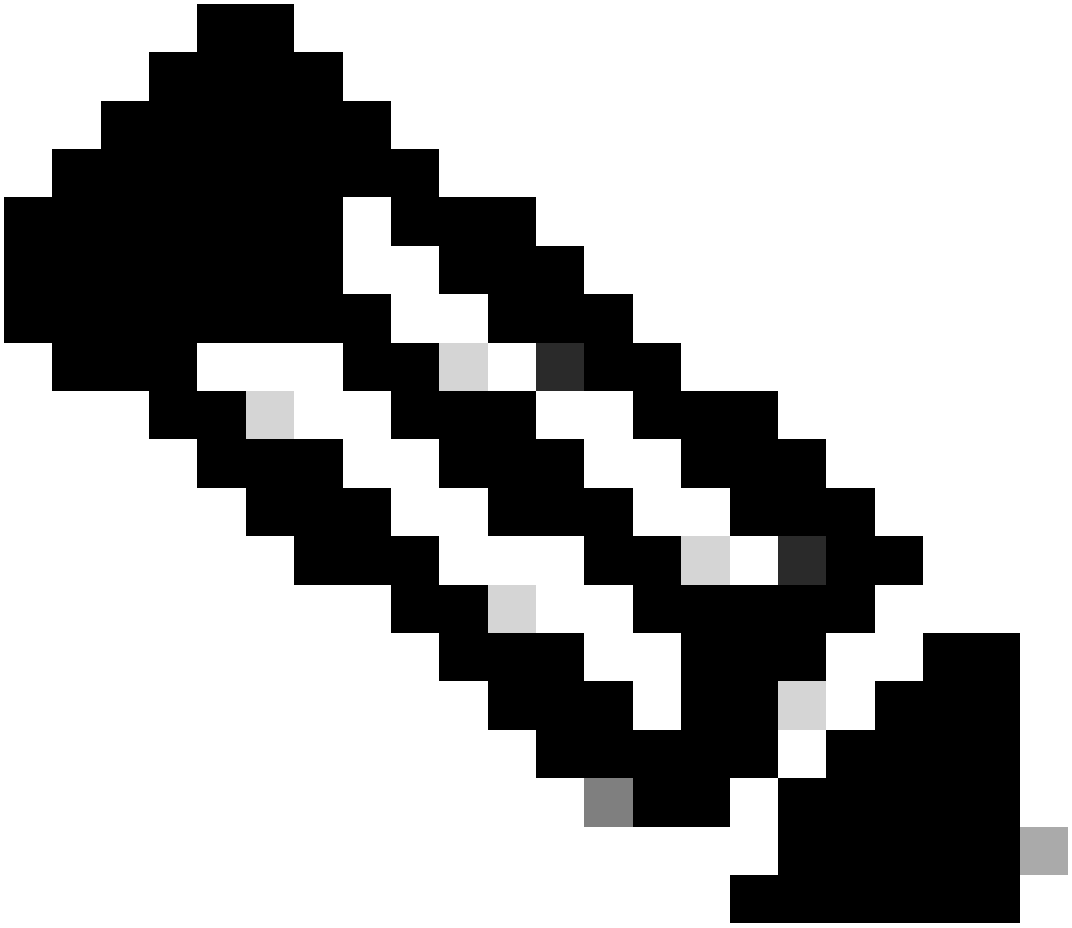
Requisiti dei certificati

Il certificato x509 utilizzato da Cisco Telemetry Broker Manager deve soddisfare i seguenti requisiti:

- Il certificato e la chiave privata devono essere una coppia corrispondente
- Il certificato e la chiave privata devono essere codificati PEM
- La chiave privata non deve essere protetta da passphrase

Conferma coppia certificato e chiave privata

Accedere all'interfaccia della riga di comando di CTB Manager (CLI) come utente amministratore.



Nota: è possibile che i file menzionati in questa sezione non esistano ancora nel sistema.

Il sudo openssl req -in server.csr -pubkey -noout -outform pem | sha256sum comando restituisce il checksum SHA-256 della chiave pubblica dal file di richiesta di firma del certificato.

Il sudo openssl pkey -in server_key.pem -pubout -outform pem | sha256sumcomando restituisce il checksum SHA-256 della chiave pubblica dal file della chiave privata.

Il sudo openssl x509 -in server_cert.pem -pubkey -noout -outform pem | sha256sumcomando restituisce il checksum SHA-256 della chiave pubblica dal file del certificato rilasciato.

L'output del certificato e della chiave privata deve corrispondere. Se non è stata utilizzata una richiesta di firma del certificato, il file server_cert.pem non esiste.

```
admin@ctb-manager:~$ sudo openssl req -in server.csr -pubkey -noout -outform pem | sha256sum 3e8e6b0d39
```

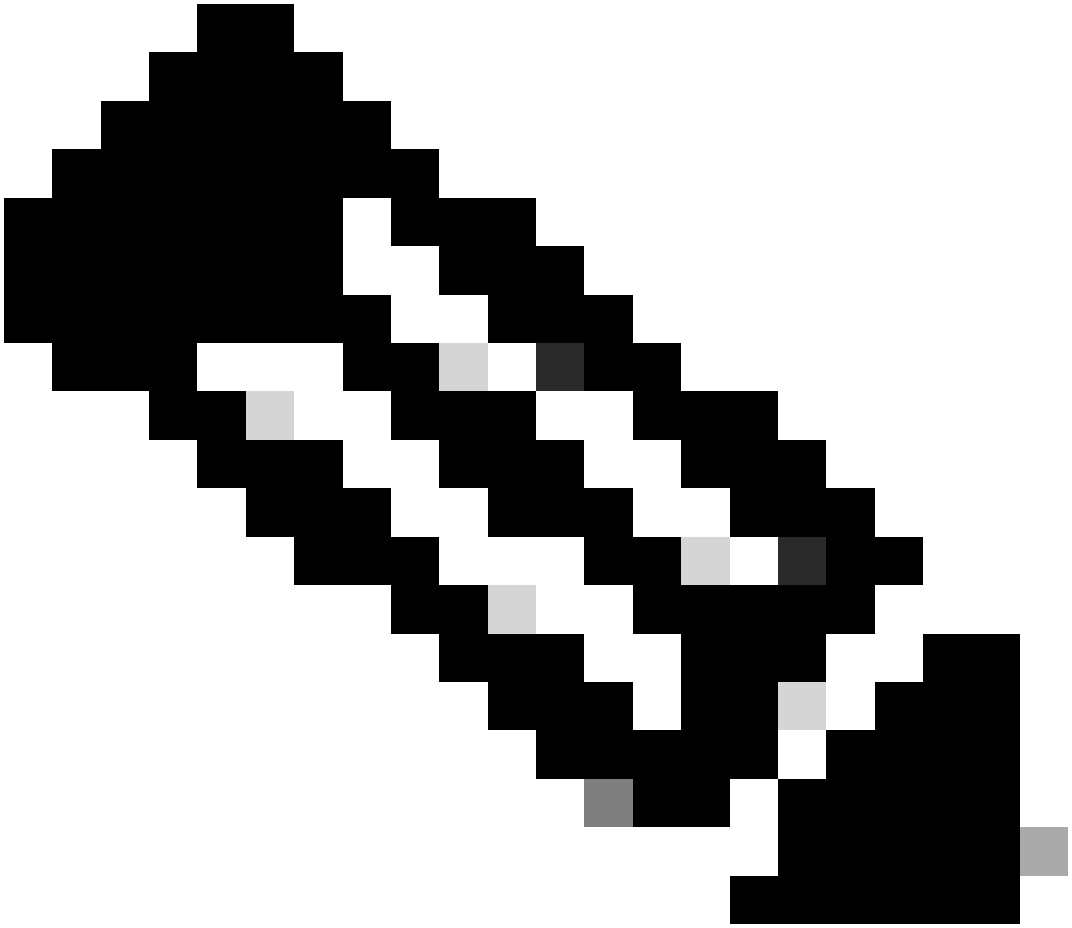
Conferma che la chiave privata non è protetta da passphrase

Accedere a Gestione CTB come utente amministratore. Eseguire il ssh-keygen -yf server_key.pem comando.

Se la chiave privata non ne richiede una, non è necessaria una passphrase.

```
admin@ctb-manager:~$ ssh-keygen -yf server_key.pem ssh-rsa {removed for brevity} admin@ctb-manager:~$
```

Confermare che il certificato e la chiave privata siano codificati PEM



Nota: queste convalide possono essere eseguite prima dell'installazione dei certificati.

Accedere a Gestione CTB come utente amministratore.

Visualizzare il contenuto del file server_cert.pem con il sudo cat server_cert.pem comando. Impostare il comando sul nome del file del certificato.

La prima e l'ultima riga del file devono essere rispettivamente **-----BEGIN CERTIFICATE-----** e-----END CERTIFICATE-----.

```
admin@ctb-manager:~$ sudo cat server_cert.pem -----BEGIN CERTIFICATE----- {removed_for_brevity} -----EN
```

Visualizzare il file server_key.pem con il sudo cat server_key.pem comando. Impostare il comando sul nome del file delle chiavi private.

La prima e l'ultima riga del file devono essere rispettivamente **-----BEGIN PRIVATE KEY-----** e-----END PRIVATE KEY-----.

```
admin@ctb-manager:~$ sudo cat server_key.pem -----BEGIN PRIVATE KEY----- {removed_for_brevity} -----END
```

Certificato autofirmato

Genera certificato autofirmato

- Accedere a CTB Manager tramite SSH (Secure Shell) come utente configurato durante l'installazione. In genere si tratta dell'utente "admin".
- Eseguire il sudo openssl req -x509 -newkey rsa:{key_len} -nodes -keyout server_key.pem -out server_cert.pem -sha256 -days 3650 -subj /CN={ctb_manager_ip} comando.
  - Modificare la lunghezza dellarsa:{key_len} chiave privata desiderata, ad esempio 2048, 4096 o 8192
    - Modificare l'indirizzo {ctb_manager_ip}con l'indirizzo IP del nodo di gestione CTB

```
admin@ctb-manager:~$ sudo openssl req -x509 -newkey rsa:4096 -nodes -keyout server_key.pem -
[sudo] password for admin:
Generating a RSA private key
.....................................................................................++++
.....................................................................++++
writing new private key to 'server_key.pem'
-----
admin@ctb-manager:~$
```

- Visualizzare il file server_cert.pem con il comandocat server_cert.pem e copiare il contenuto nel buffer in modo che possa essere incollato sulla workstation locale in un editor di testo a scelta. Salvare il file. È inoltre possibile eseguire il SCP di questi file all'esterno della /home/admin directory.

```
admin@ctb-manager:~$ cat server_cert.pem
-----BEGIN CERTIFICATE-----
{removed_for_brevity}
-----END CERTIFICATE-----
admin@ctb-manager:~$
```

- Visualizzare il file server_key.pem con il comandosudo cat server_key.pem e copiare il contenuto nel buffer in modo che possa essere incollato sulla workstation locale in un editor di testo a scelta. Salvare il file. È inoltre possibile estrarre il file dalla /home/admin directory.

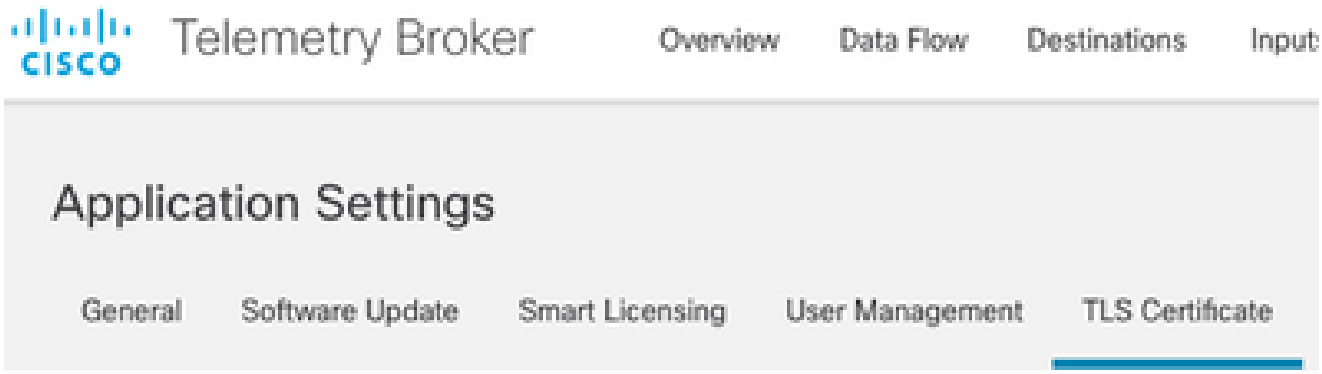
```
admin@ctb-manager:~$ sudo cat server_key.pem
-----BEGIN PRIVATE KEY-----
{removed_for_brevity}
-----END PRIVATE KEY-----
admin@ctb-manager:~$
```

Carica certificato autofirmato

1. Accedere all'interfaccia utente Web di CTB Manager come utente amministratore e fare clic sull'icona a forma di ingranaggio per accedere a "Settings".

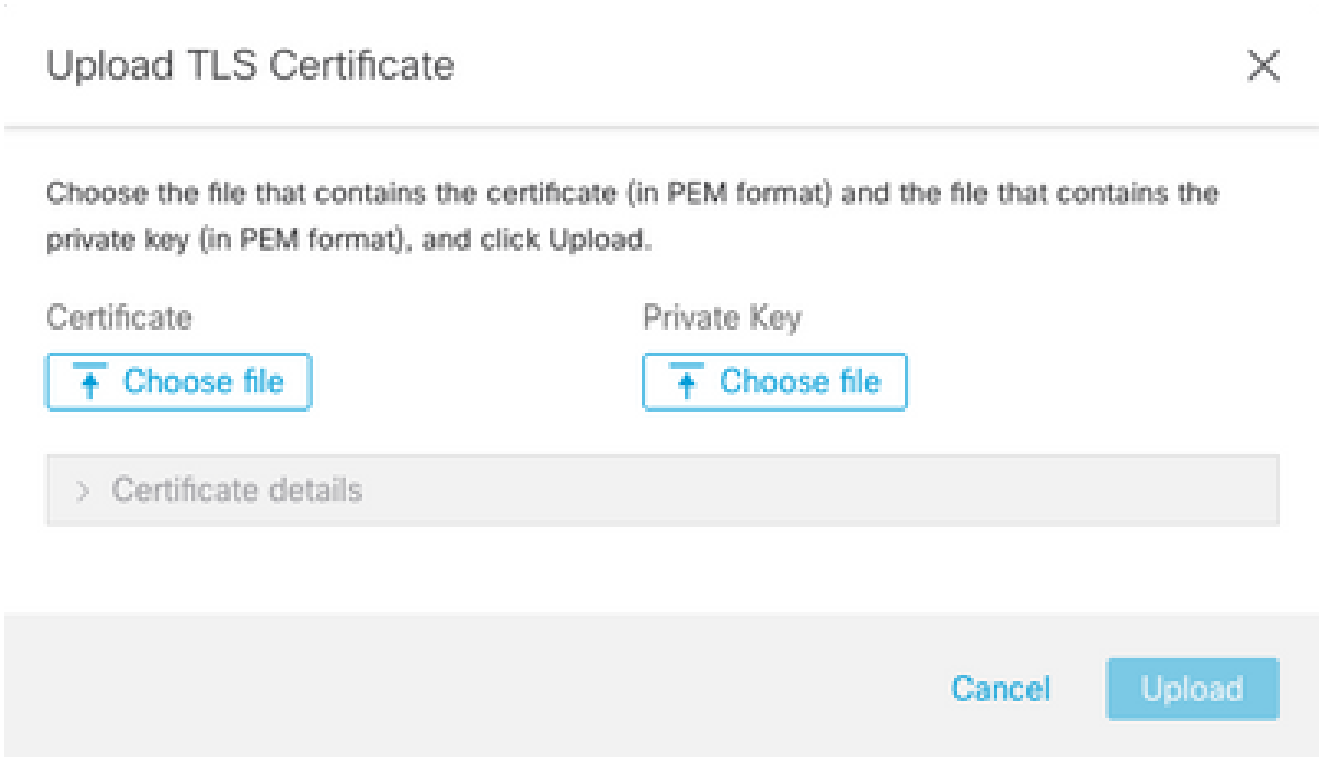
Icona impostazione CTB

- Passare alla scheda Certificato TLS.

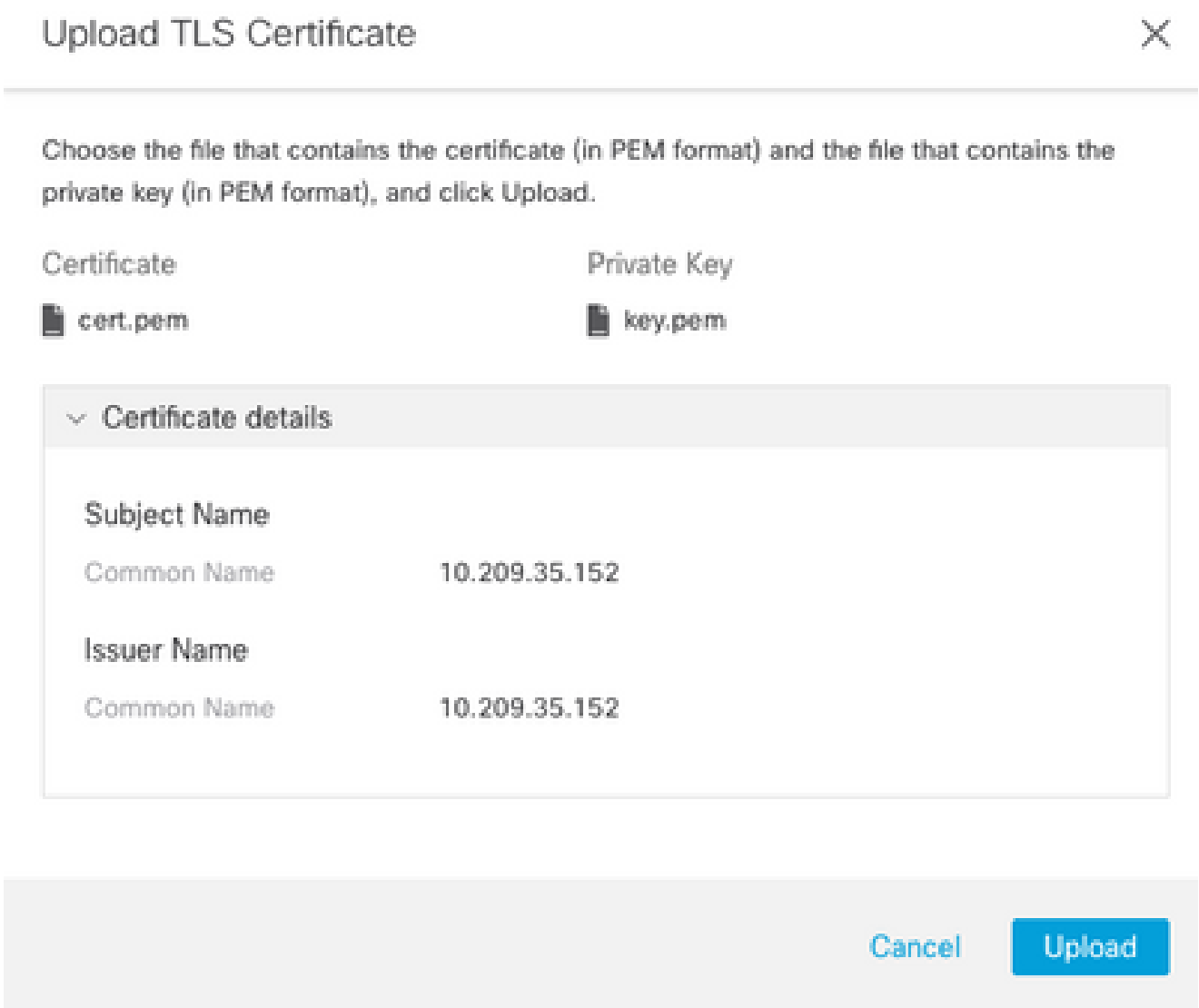


Scheda Certificati CTB

- Selezionare Upload TLS Certificate e quindi selezionare rispettivamente server_cert.pem e server_key.pem per il certificato e la chiave privata nella finestra di dialogo "Carica certificato TLS". Una volta selezionati i file, selezionare Upload.



• Una volta selezionati i file, un processo di verifica conferma la combinazione di certificato e chiave e visualizza il nome comune dell'autorità emittente e dell'oggetto come mostrato.



Caricamento certificato CTB

- Selezionare il pulsante "Upload" per caricare il nuovo certificato. L'interfaccia utente Web si riavvia da sola in pochi istanti e dopo il riavvio esegue nuovamente l'accesso al dispositivo.

- Accedere alla console Web del nodo di CTB Manager e passare Settings > TLS Certificate a per visualizzare i dettagli del certificato, ad esempio una nuova data di scadenza, oppure visualizzare i dettagli del certificato utilizzando il browser per visualizzare informazioni più dettagliate, ad esempio i numeri di serie.

Aggiorna nodi broker

Quando il nodo di gestione CTB dispone di un nuovo certificato di identità, ogni nodo di broker CTB deve essere aggiornato manualmente.

1. Accedere a ciascun nodo broker tramite ssh ed eseguire il sudo ctb-manage comando

```
admin@ctb-broker:~$ sudo ctb-manage

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for admin:
```

- Selezionare l'opzione cquando richiesto.

```
== Management Configuration

A manager configuration already exists for 10.209.35.152
Options:

(o) Associate this node with a new manager
(c) Re-fetch the manager's certificate but keep everything else
(d) Deactivate this node (should be done after removing this node on the manager UI)
(a) Abort

How would you like to proceed? [o/c/d/a] c
```

- **y** Verificare i dettagli del certificato se corrispondono ai valori per il certificato firmato e scegliere di accettare il certificato. I servizi verranno avviati automaticamente e, una volta avviato il servizio, verrà restituito il prompt. L'avvio del servizio può richiedere fino a circa 15 minuti.

```
== Testing connection to server exists

== Fetching certificate from 10.209.35.152
Subject Hash
3fcbcd3c
subject=CN = 10.209.35.152
issuer=CN = 10.209.35.152
Validity:
notBefore=Mar 28 13:12:43 2023 GMT
notAfter=Mar 27 13:12:43 2024 GMT
X509v3 Subject Alternative Name:
IP Address:10.209.35.152

Do you accept the authenticity of the server? [y/n] y

== Writing /var/lib/titan/titanium_proxy/ssl/titanium.pem
```

```
done

== Starting service
```

Certificati rilasciati da CA (Certification Authority)

Genera richiesta di firma del certificato (CSR) per il rilascio da parte di un'Autorità di certificazione

- Accedere a CTB Manager tramite SSH (Secure Shell) come utente configurato durante l'installazione. In genere si tratta dell'utente "admin".

- Eseguire il openssl req -new -newkey rsa:{key_len} -nodes -addext "subjectAltName = DNS:{ctb_manager_dns_name},IP:{ctb_manager_ip}" -keyout server_key.pem -out server.csr comando. Se lo si desidera, è possibile lasciare vuoti gli attributi "extra" delle ultime due righe.

  - Modificare il nome {ctb_manager_dns_name} con il nome DNS del nodo di gestione CTB

    - Modificare l'indirizzo {ctb_manager_ip}con l'indirizzo IP del nodo di gestione CTB

    - Modificare la chiave {key_len} con una lunghezza di chiave privata a scelta, ad esempio 2048, 4096 o 8192.

```
admin@ctb-manager:~$ openssl req -new -newkey rsa:4096 -nodes -addext "subjectAltName = DNS:
Generating a RSA private key
.....................++++
.....................................++++
writing new private key to 'server_key.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:North Carolina
Locality Name (eg, city) []:RTP
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Cisco Systems Inc
Organizational Unit Name (eg, section) []:TAC
Common Name (e.g. server FQDN or YOUR name) []:ctb-manager
Email Address []:noreply@cisco.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

- Eseguire il SCP del CSR e dei file di chiave su un computer locale e fornire il CSR alla CA. Il rilascio del CSR da parte dell'autorità di certificazione in formato PEM esula dall'ambito del presente documento.

Crea un certificato con concatenamento

La CA emette il certificato di identità del server in formato PEM. È necessario creare un file concatenato che includa tutti i certificati concatenati e il certificato di identità del server per il nodo di gestione CTB.

In un editor di testo creare un file combinando il certificato firmato nel passaggio precedente e aggiungendo tutti i certificati della catena, inclusa la CA attendibile, in un unico file in formato PEM nell'ordine indicato.

```
– BEGIN CERTIFICATE – {CTB Manager Issued Certificate} – END CERTIFICATE – – BEGIN CERTIFICATE – {Issui
```

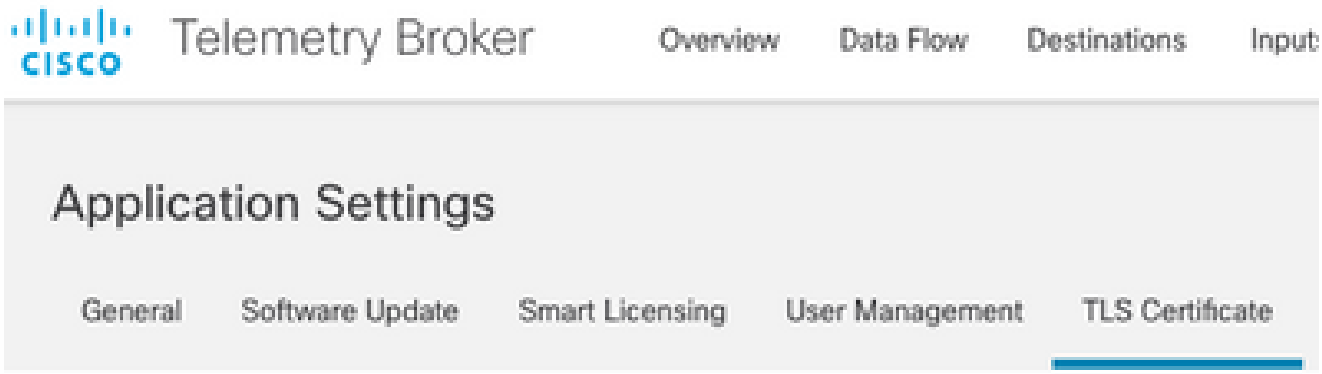
Verificare che il nuovo file di certificato con file concatenato non contenga spazi iniziali o finali, righe vuote e sia nell'ordine indicato sopra.

Carica certificato rilasciato dall'Autorità di certificazione

1. Accedere all'interfaccia utente Web di CTB Manager come admin e fare clic sull'icona a forma di ingranaggio per accedere a "Settings".

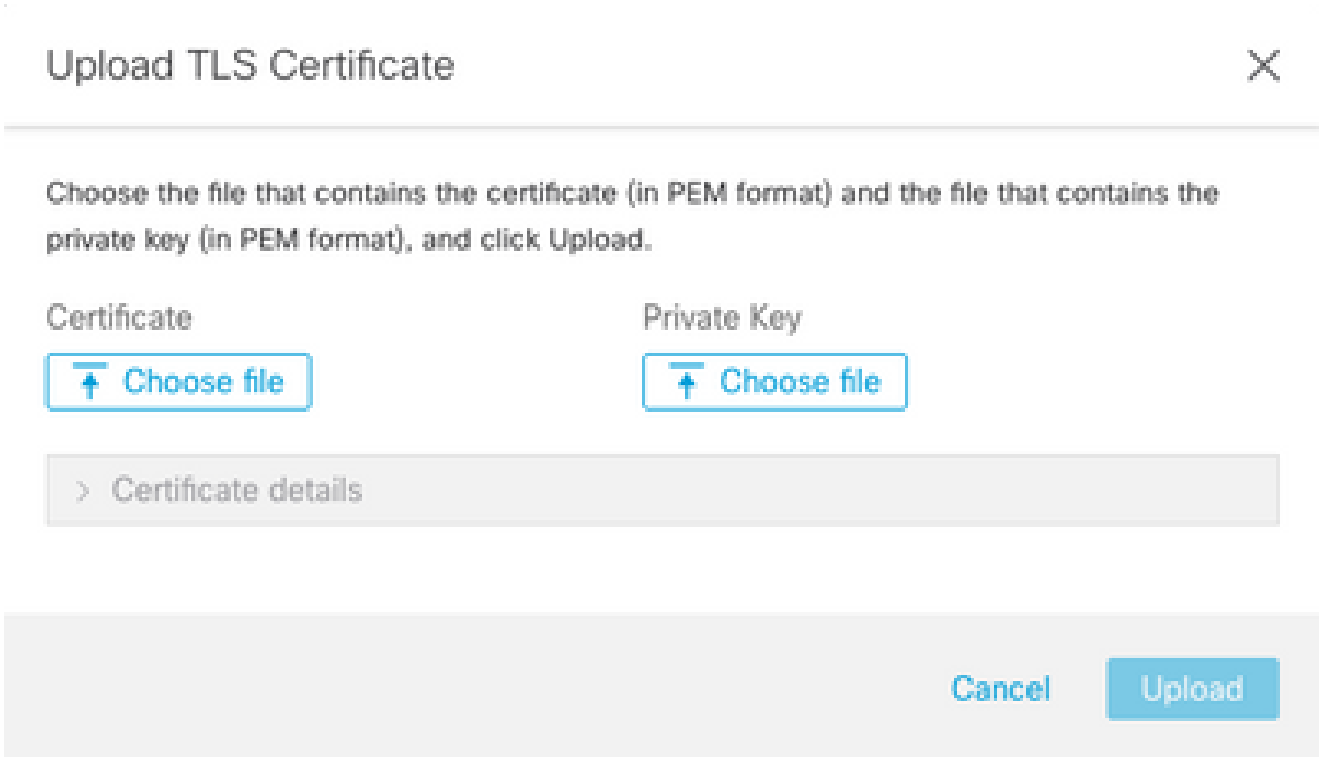
Icona impostazione CTB

- Passare alla scheda Certificato TLS.

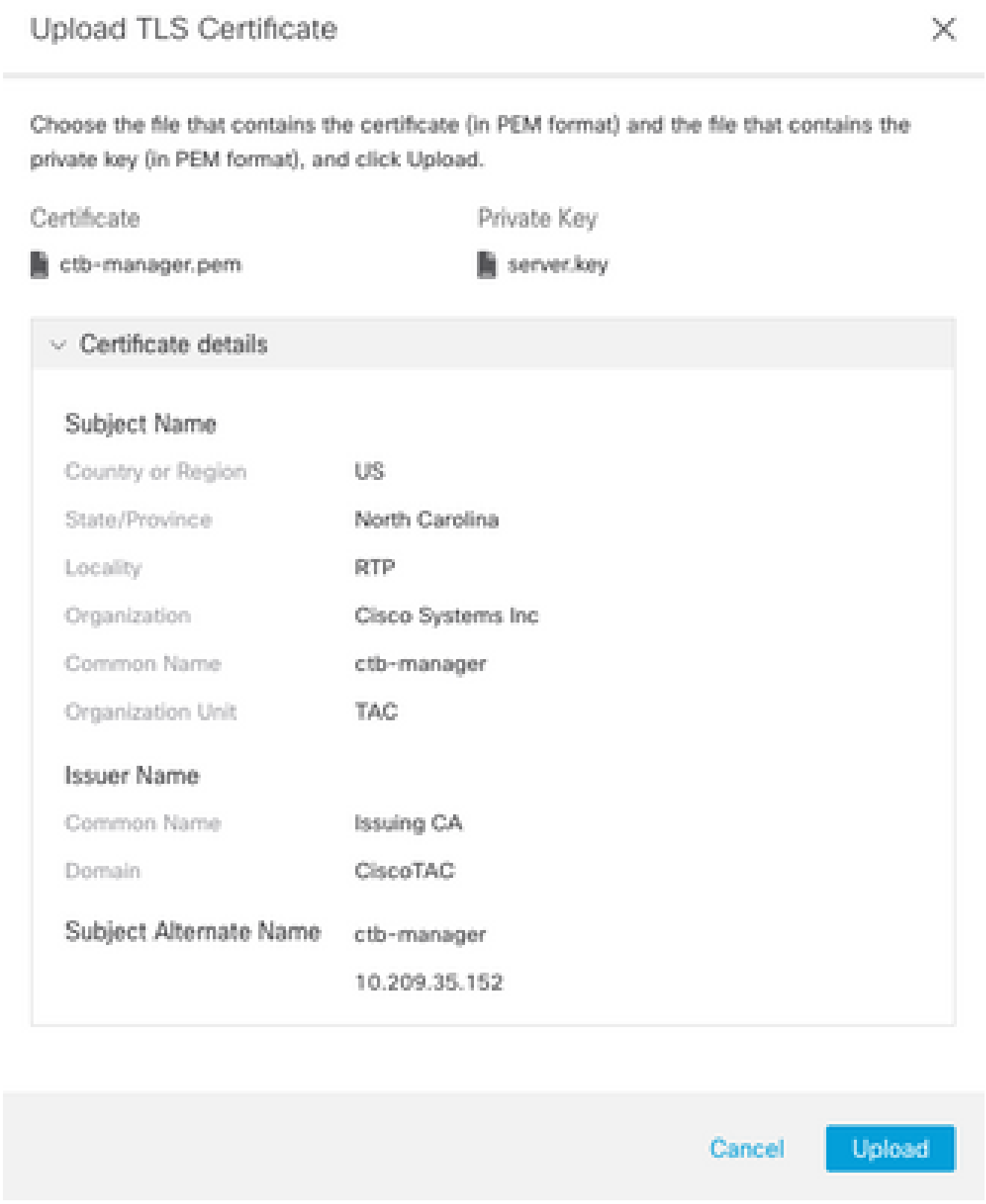


Scheda Certificati CTB

- Selezionare Upload TLS Certificate e quindi selezionare il certificato con il file della catena creato nell'ultima sezione e il gestore CTB generato rispettivamente server_key.pem per il certificato e la chiave privata nella finestra di dialogo "Carica certificato TLS". Una volta selezionati i file, selezionare Upload.



• Una volta selezionati i file, un processo di verifica conferma la combinazione di certificato e chiave e visualizza il nome comune dell'autorità emittente e dell'oggetto come mostrato di seguito.



Convalida certificato rilasciato CA CTB

- Selezionare il pulsante "Upload" per caricare il nuovo certificato. L'interfaccia utente Web viene riavviata automaticamente in circa 60 secondi. Dopo il riavvio, accedere all'interfaccia utente Web.

- Accedere alla console Web del nodo di CTB Manager e passare Settings > TLS Certificate a per visualizzare i dettagli del

certificato, ad esempio una nuova data di scadenza, oppure visualizzare i dettagli del certificato utilizzando il browser per visualizzare informazioni più dettagliate, ad esempio i numeri di serie.

Aggiorna nodi broker

Quando il nodo di gestione CTB dispone di un nuovo certificato di identità, ogni nodo di broker CTB deve essere aggiornato manualmente.

1. Accedere a ciascun nodo broker tramite ssh ed eseguire il sudo ctb-manage comando

```
admin@ctb-broker:~$ sudo ctb-manage

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for admin:
```

- Selezionare l'opzione cquando richiesto.

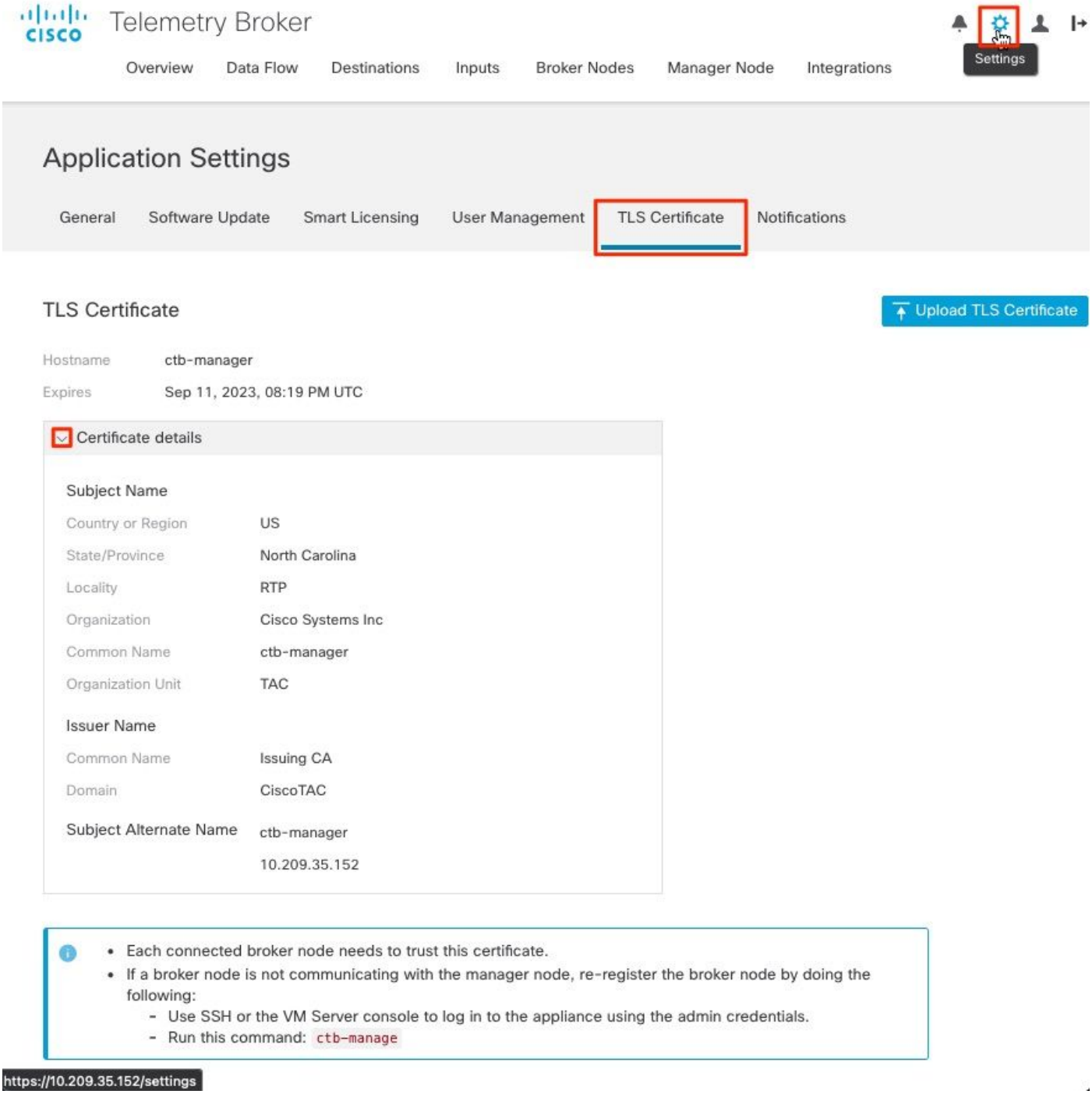
```
== Management Configuration

A manager configuration already exists for 10.209.35.152
Options:

(o) Associate this node with a new manager
(c) Re-fetch the manager's certificate but keep everything else
(d) Deactivate this node (should be done after removing this node on the manager UI)
(a) Abort

How would you like to proceed? [o/c/d/a] c
```

- Verificare i dettagli del certificato se corrispondono ai valori del certificato firmato e selezionare y per accettare il certificato. I servizi vengono avviati automaticamente e, una volta avviato il servizio, viene visualizzato il prompt. L'avvio del servizio può richiedere fino a circa 15 minuti.

```
== Testing connection to server exists

== Fetching certificate from 10.209.35.152
Subject Hash
fa7fd0fb
subject=C = US, ST = North Carolina, L = RTP, O = "Cisco Systems Inc", OU = TAC, CN = ctb-manager,
issuer=DC = CiscoTAC, CN = Issuing CA
Validity:
notBefore=Jun 13 16:09:29 2023 GMT
notAfter=Sep 11 16:19:29 2023 GMT
X509v3 Subject Alternative Name:
DNS:ctb-manager, IP Address:10.209.35.152

Do you accept the authenticity of the server? [y/n] y

== Writing /var/lib/titan/titanium_proxy/ssl/titanium.pem
done

== Starting service
```

Verifica

Accedere alla console Web del nodo di CTB Manager e passare Settings > TLS Certificate a per visualizzare i dettagli del certificato, ad esempio una nuova data di scadenza, oppure visualizzare i dettagli del certificato utilizzando il browser per visualizzare informazioni più dettagliate, ad esempio i numeri di serie.



Dettagli certificato CTB

Verificare che il nodo Broker CTB non presenti avvisi nell'interfaccia utente Web del nodo Gestore CTB.

Risoluzione dei problemi

Se il certificato è incompleto, ad esempio se mancano i certificati della catena, il nodo del nodo Broker CTB non è in grado di comunicare con il nodo Manager e presenta "Non visto da" nella colonna Stato dell'elenco dei nodi Broker.
Il nodo Broker continuerà a replicare e distribuire il traffico in questo stato.

Accedere alla CLI del nodo di gestione CTB ed eseguire il sudo grep -ic begin /var/lib/titan/titanium_frontend/ssl/cert.pem comando per verificare il numero di certificati presenti nel file cert.pem.

```
admin@ctb-manager:~$ sudo grep -ic begin /var/lib/titan/titanium_frontend/ssl/cert.pem [sudo] password
```

Il valore di output restituito deve essere uguale al numero di dispositivi CA nella catena più il gestore CTB.

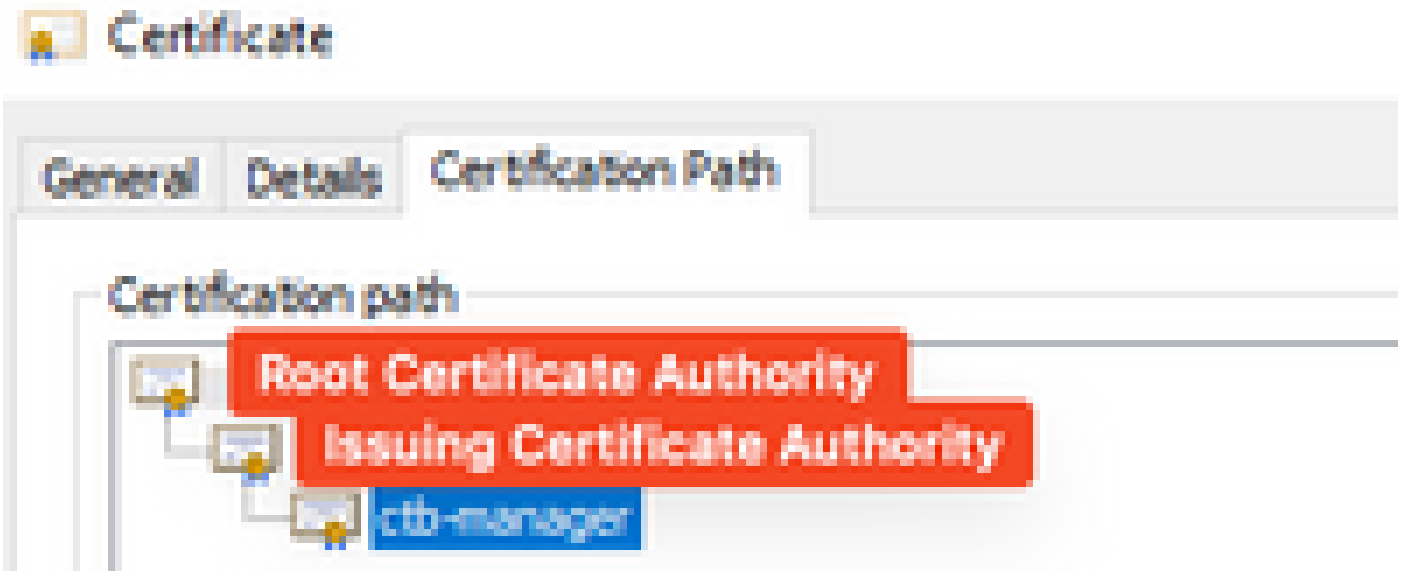
Se si utilizza un certificato autofirmato, è previsto l'output 1.

L'output di 2 è previsto se l'infrastruttura PKI è costituita da una singola CA radice che è anche la CA emittente.

L'output di 3 è previsto se l'infrastruttura PKI è costituita da una CA radice e dalla CA emittente.

L'output di 4 è previsto se l'infrastruttura PKI è costituita da una CA radice, una CA subordinata e la CA emittente.

Confrontare l'output con la PKI elencata quando si visualizza il certificato in un'altra applicazione, ad esempio Microsoft Windows Crypto Shell Extensions.



Infrastruttura PKI

In questa immagine l'infrastruttura PKI include una CA radice e la CA emittente.

In questo scenario, il valore di output del comando dovrebbe essere 3.

Se l'output non soddisfa le aspettative, esaminare i passaggi nella sezione **Creazione di un certificato con catena** per determinare se un certificato è stato omesso.

Quando si visualizza un certificato in, Microsoft Windows Crypto Shell Extensions è possibile che non tutti i certificati da presentare siano disponibili se il computer locale non dispone di informazioni sufficienti per verificare il certificato.

Eseguire il sudo ctb-mayday comando dalla CLI per generare un bundle mayday per TAC da rivedere.

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).