Substituir Certificado de Identidade do Agente de Telemetria

Contents

Introdução

Este documento descreve como substituir o certificado de identidade do servidor no nó do gerenciador do Cisco Telemetry Broker (CTB).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Administração do dispositivo Cisco Telemetry Broker
- Certificados X509

Componentes Utilizados

Os equipamentos usados para este documento estão executando a versão 2.0.1

- Nó do gerenciador do Cisco Telemetry Broker
- Nó do agente de telemetria da Cisco

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configurar

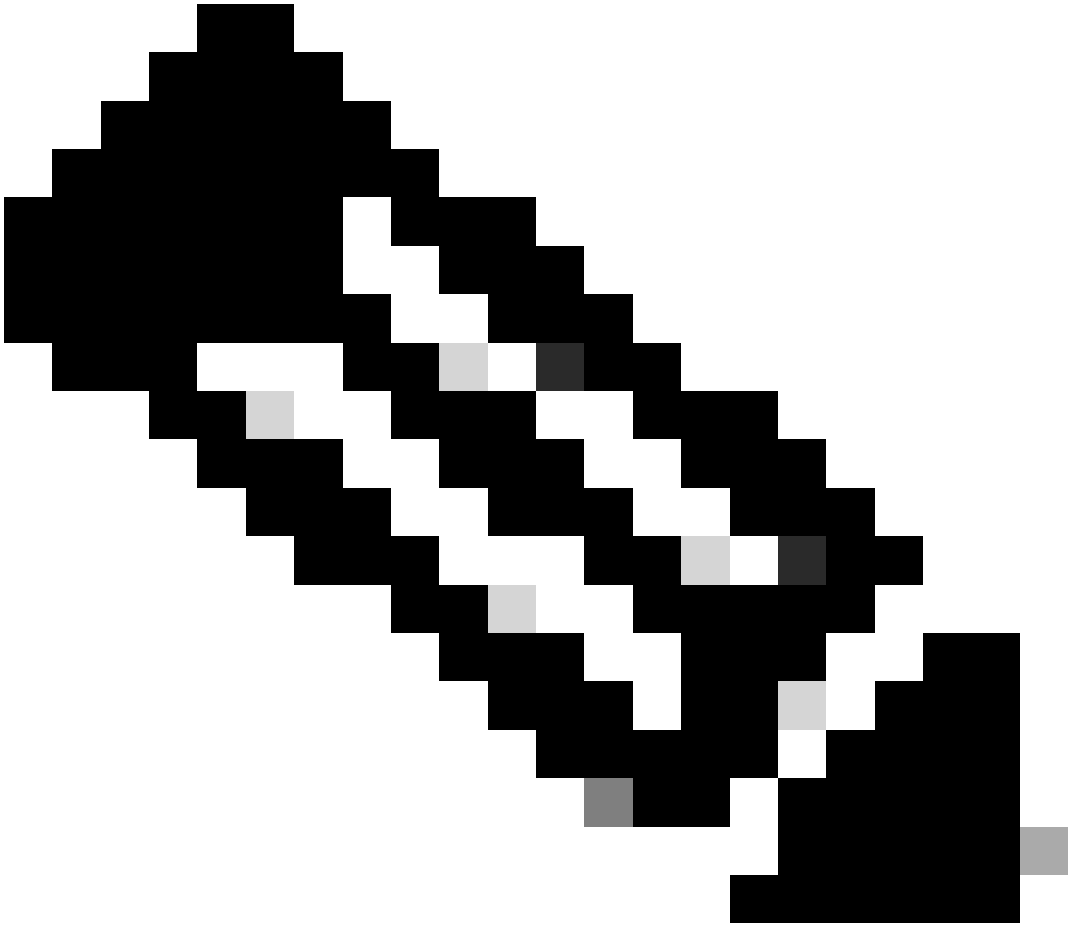
Requisitos do certificado

O certificado x509 usado pelo Cisco Telemetry Broker Manager deve atender aos seguintes requisitos:

- O Certificado e a Chave Privada devem ser um par correspondente
- O certificado e a chave privada devem ser codificados por PEM
- A chave privada não deve ser protegida por senha

Confirmar se o certificado e a chave privada correspondem ao par

Faça login na interface de linha de comando (CLI) do Gerenciador CTB como o usuário administrador.



Observação: é possível que os arquivos mencionados nesta seção ainda não existam no sistema.

O sudo openssl req -in server.csr -pubkey -noout -outform pem | sha256sum comando gera a soma de verificação SHA-256 da chave pública do arquivo de Solicitação de Assinatura de Certificado.

O sudo openssl pkey -in server_key.pem -pubout -outform pem | sha256sumcomando gera a soma de verificação SHA-256 da chave pública do arquivo de chave privada.

O sudo openssl x509 -in server_cert.pem -pubkey -noout -outform pem | sha256sumcomando gera a soma de verificação SHA-256 da chave pública do arquivo de certificado emitido.

A saída do certificado e da chave privada deve coincidir. Se uma solicitação de assinatura de certificado não foi usada, o arquivo server_cert.pem não existe.

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

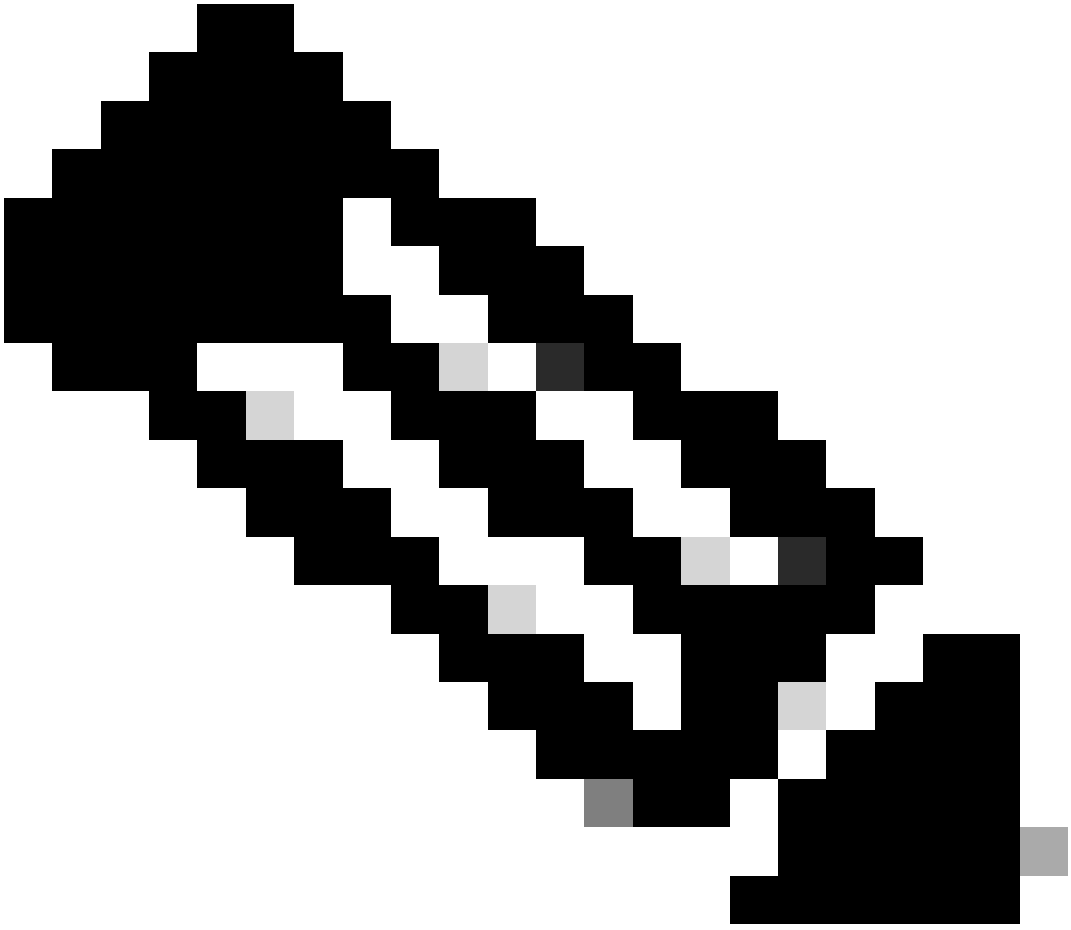
Confirmar se a chave privada não está protegida por senha

Faça login no CTB Manager como o usuário administrador. Execute o ssh-keygen -yf server_key.pem comando.

Uma senha não será solicitada se a chave privada não exigir uma.

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

Confirmar se o certificado e a chave privada estão codificados com PEM



Observação: essas validações podem ser executadas antes da instalação dos certificados.

Faça login no CTB Manager como o usuário administrador.

Exiba o conteúdo do arquivo server_cert.pem com o sudo cat server_cert.pem comando. Ajuste o comando para o nome do arquivo do certificado.

A primeira e a última linhas do arquivo devem ser **-----BEGIN CERTIFICATE-----** e -----END CERTIFICATE-----, respectivamente.

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

Exiba o arquivo server_key.pem com o comandosudo cat server_key.pem. Ajuste o comando para o nome do arquivo de chaves particulares.

A primeira e a última linhas do arquivo devem ser **-----BEGIN PRIVATE KEY-----** e -----END PRIVATE KEY-----, respectivamente.

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

Certificado autoassinado

Gerar certificado autoassinado

- Faça login no Gerenciador CTB através de um SSH (Secure Shell) como o usuário configurado durante a instalação, que geralmente é o usuário "admin".

- Emita o 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.

  - Altere o rsa:{key_len} com um comprimento de chave privada de sua escolha, como 2048, 4096 ou 8192

    - Altere o {ctb_manager_ip}com o IP do CTB Manager Node

```
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:~$
```

- Visualize o arquivo server_cert.pem com o comandocat server_cert.pem e copie o conteúdo para o buffer para que ele possa ser colado na estação de trabalho local em um editor de texto de sua escolha. Salve o arquivo. Você também pode SCP esses arquivos fora do /home/admin diretório.

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

- Visualize o arquivo server_key.pem com o comandosudo cat server_key.pem e copie o conteúdo para o buffer para que ele possa ser colado na estação de trabalho local em um editor de texto de sua escolha. Salve o arquivo. Você também pode SCP esse arquivo fora do /home/admin diretório.

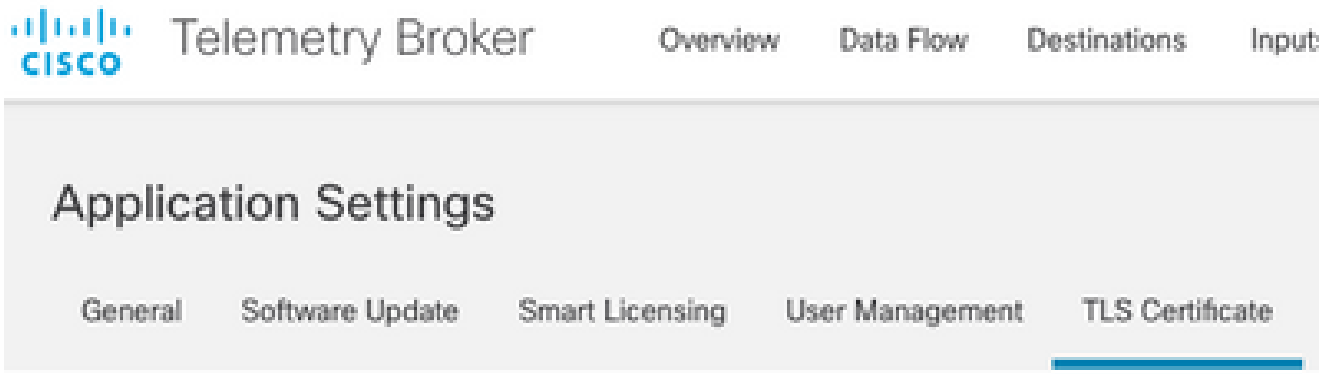
```
admin@ctb-manager:~$ sudo cat server_key.pem
-----BEGIN PRIVATE KEY-----
{removed_for_brevity}
-----END PRIVATE KEY-----
admin@ctb-manager:~$
```

Carregar certificado autoassinado

1. Navegue até a interface do usuário da Web do CTB Manager e faça login como o usuário administrador e clique no ícone da engrenagem para acessar "Settings".

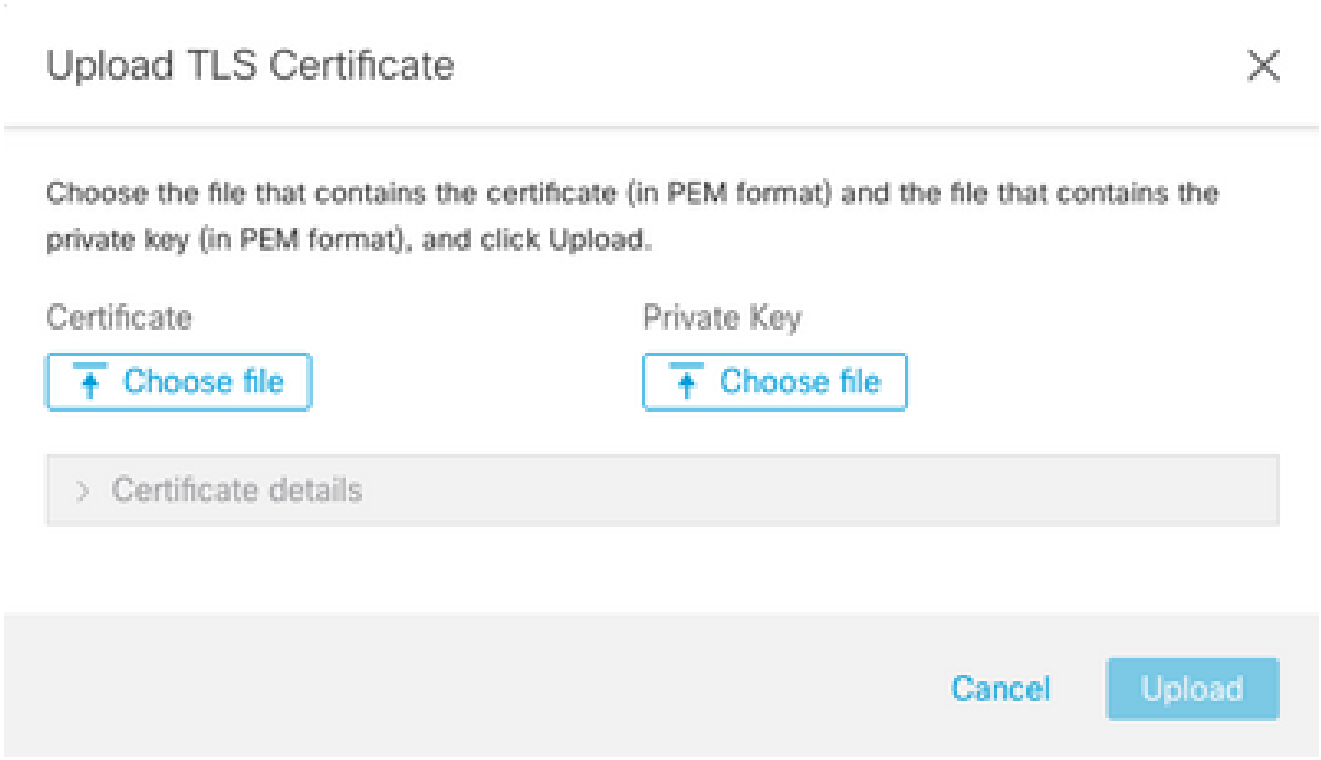
Ícone de configuração CTB

- Navegue até a guia "Certificado TLS".

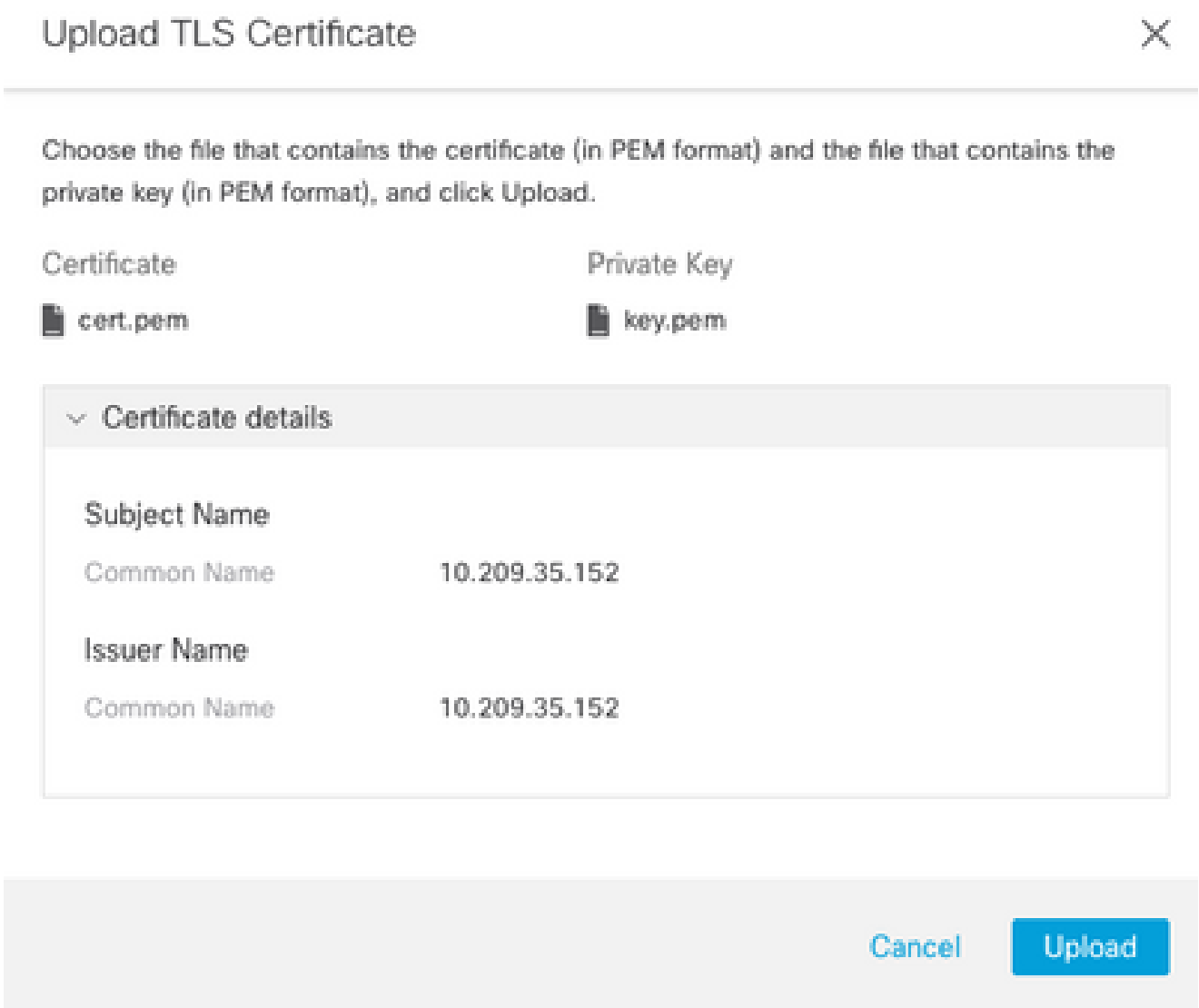


Guia Certificados CTB

- Selecione Upload TLS Certificate e, em seguida, selecione server_cert.pem e server_key.pem para o certificado e a chave privada, respectivamente, na caixa de diálogo "Carregar certificado TLS". Depois que os arquivos forem selecionados, selecione Carregar.



• Depois que os arquivos são selecionados, um processo de verificação confirma a combinação de certificado e chave e exibe o nome comum do Emissor e do Assunto como mostrado.



Carregamento de Cert CTB

- Selecione o botão "Upload" para carregar o novo certificado. A interface do usuário da Web reinicia sozinha em alguns momentos e, depois de reiniciar, faz logon no dispositivo novamente.

- Faça login no Console Web do Nó do Gerenciador CTB e navegue até Settings > TLS Certificate para ver detalhes do certificado, como uma nova data de expiração, ou exiba os detalhes do certificado usando o navegador para exibir informações mais detalhadas, como números de série.

Atualizar Nós de Agente

Quando o CTB Manager Node tiver um novo certificado de identidade, cada CTB Broker Node deve ser atualizado manualmente.

1. Efetue login em cada nó do broker via ssh e execute o 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:
```

- Selecione a opção cquando solicitado.

```
== 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
```

- Verifique os detalhes do certificado se eles correspondem aos valores do certificado assinado e selecione **y** para aceitar o certificado. Os serviços são iniciados automaticamente e, uma vez que o serviço é iniciado, o prompt é retornado. O início do serviço pode levar até cerca de 15 minutos para ser concluído.

```
== 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
```

Certificados Emitidos pela Autoridade de Certificação (CA)

Gerar CSR (Certificate Signing Request, Solicitação de assinatura de certificado) para emissão por uma autoridade de certificação

- Faça login no Gerenciador CTB através de um SSH (Secure Shell) como o usuário configurado durante a instalação, que geralmente é o usuário "admin".

- Emita o comandoopenssl 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 . Os atributos 'extras' nas duas últimas linhas podem ser deixados em branco, se desejado.

  - Altere o {ctb_manager_dns_name} com o nome DNS do nó do gerenciador CTB

    - Altere o {ctb_manager_ip}com o IP do CTB Manager Node

    - Altere o {key_len} com um comprimento de chave privada de sua escolha, como 2048, 4096 ou 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 []:
```

- SCP o CSR e os arquivos de chave para uma máquina local e forneça o CSR à CA. A emissão do CSR pela CA em formato PEM está fora do escopo deste documento.

Criar um Certificado com Cadeia

A CA emite o certificado de identidade do servidor no formato PEM. Deve ser criado um arquivo de cadeia que inclua todos os certificados de cadeia e o certificado de identidade do servidor para o Nó de gerenciador do CTB.

Em um editor de texto, crie um arquivo combinando o certificado que foi assinado na etapa anterior e anexando todos os certificados da cadeia, incluindo a CA confiável, em um único arquivo no formato PEM na ordem mostrada.

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

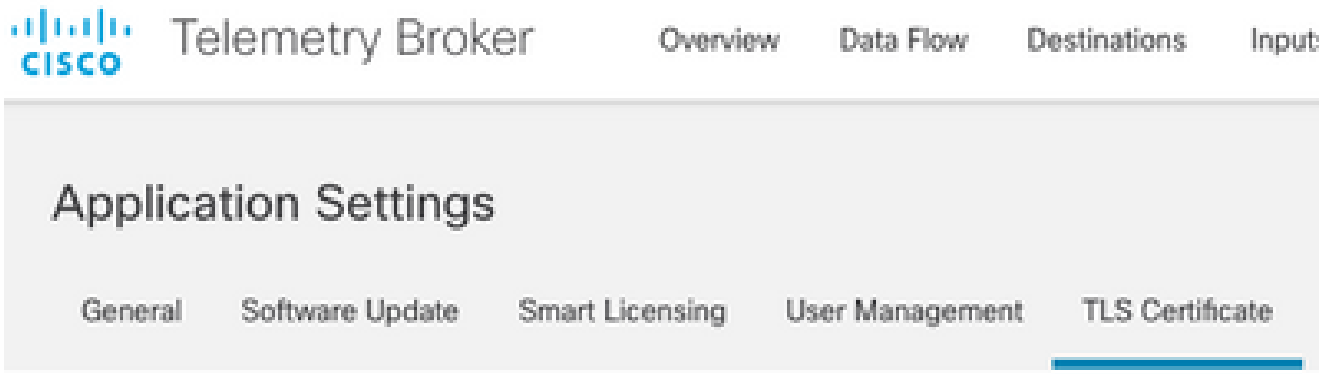
Certifique-se de que este novo arquivo de certificado com arquivo de cadeia não tenha espaços à esquerda ou à direita, linhas em branco e esteja na ordem mostrada acima.

Carregar certificado emitido pela autoridade de certificação

1. Navegue para a interface do usuário da Web do CTB Manager e faça login como admin e clique no ícone da engrenagem para acessar "Settings".

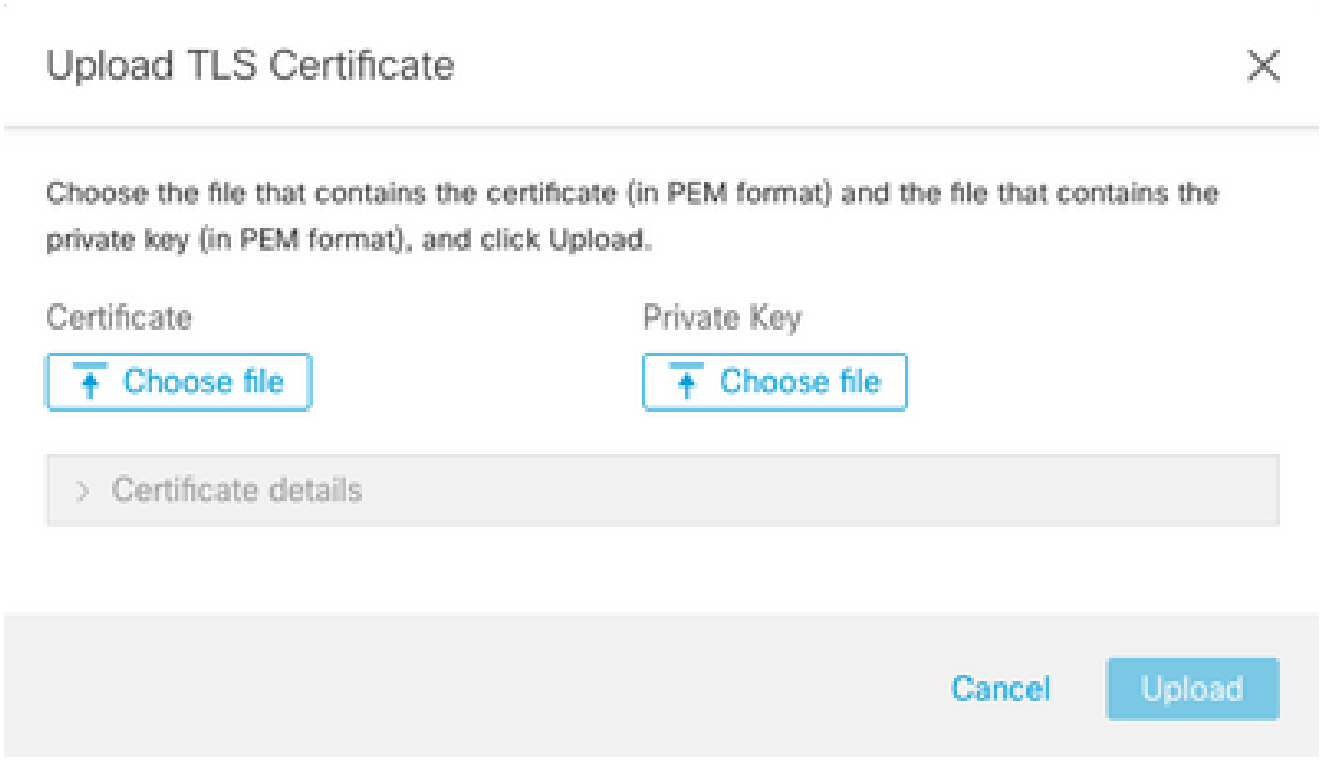
Ícone de configuração CTB

- Navegue até a guia "Certificado TLS".

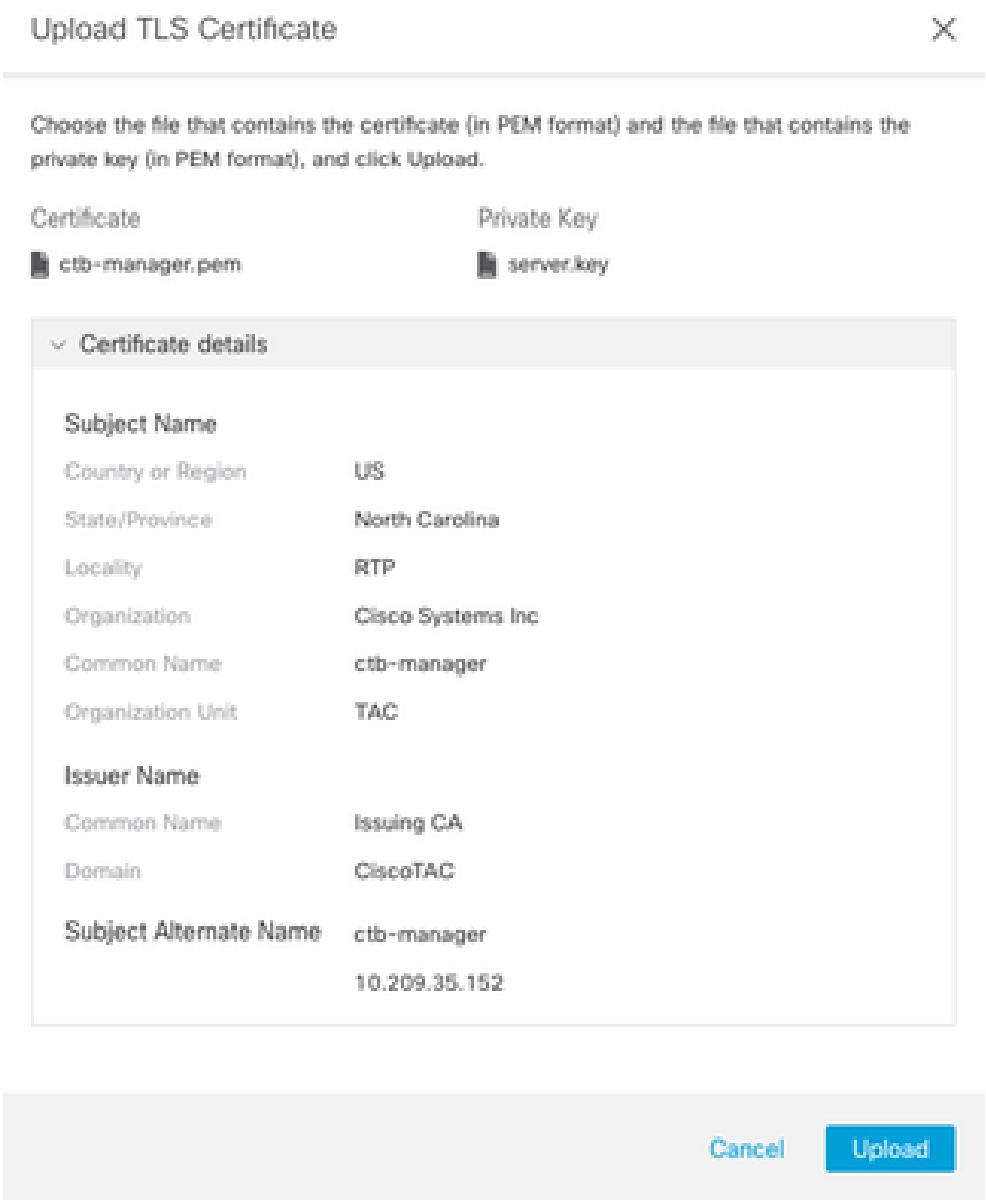


Guia Certificados CTB

- Selecione Upload TLS Certificate e, em seguida, selecione o certificado com o arquivo de cadeia criado na última seção e o Gerenciador CTB gerado server_key.pem para o certificado e a chave privada, respectivamente, na caixa de diálogo "Carregar certificado TLS". Depois que os arquivos forem selecionados, selecione Carregar.



• Depois que os arquivos são selecionados, um processo de verificação confirma a combinação de certificado e chave e exibe o nome comum do Emissor e do Assunto como mostrado abaixo.



Validação de Certificado Emitido de CA do CTB

- Selecione o botão "Upload" para carregar o novo certificado. A IU da Web é reiniciada sozinha em cerca de 60 segundos, faça login na IU da Web após a reinicialização.

- Faça login no Console Web do Nó do Gerenciador CTB e navegue até Settings > TLS Certificate para ver detalhes do certificado,

como uma nova data de expiração, ou exiba os detalhes do certificado usando o navegador para exibir informações mais detalhadas, como números de série.

Atualizar Nós de Agente

Quando o CTB Manager Node tiver um novo certificado de identidade, cada CTB Broker Node deve ser atualizado manualmente.

1. Efetue login em cada nó do broker via ssh e execute o 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:
```

- Selecione a opção cquando solicitado.

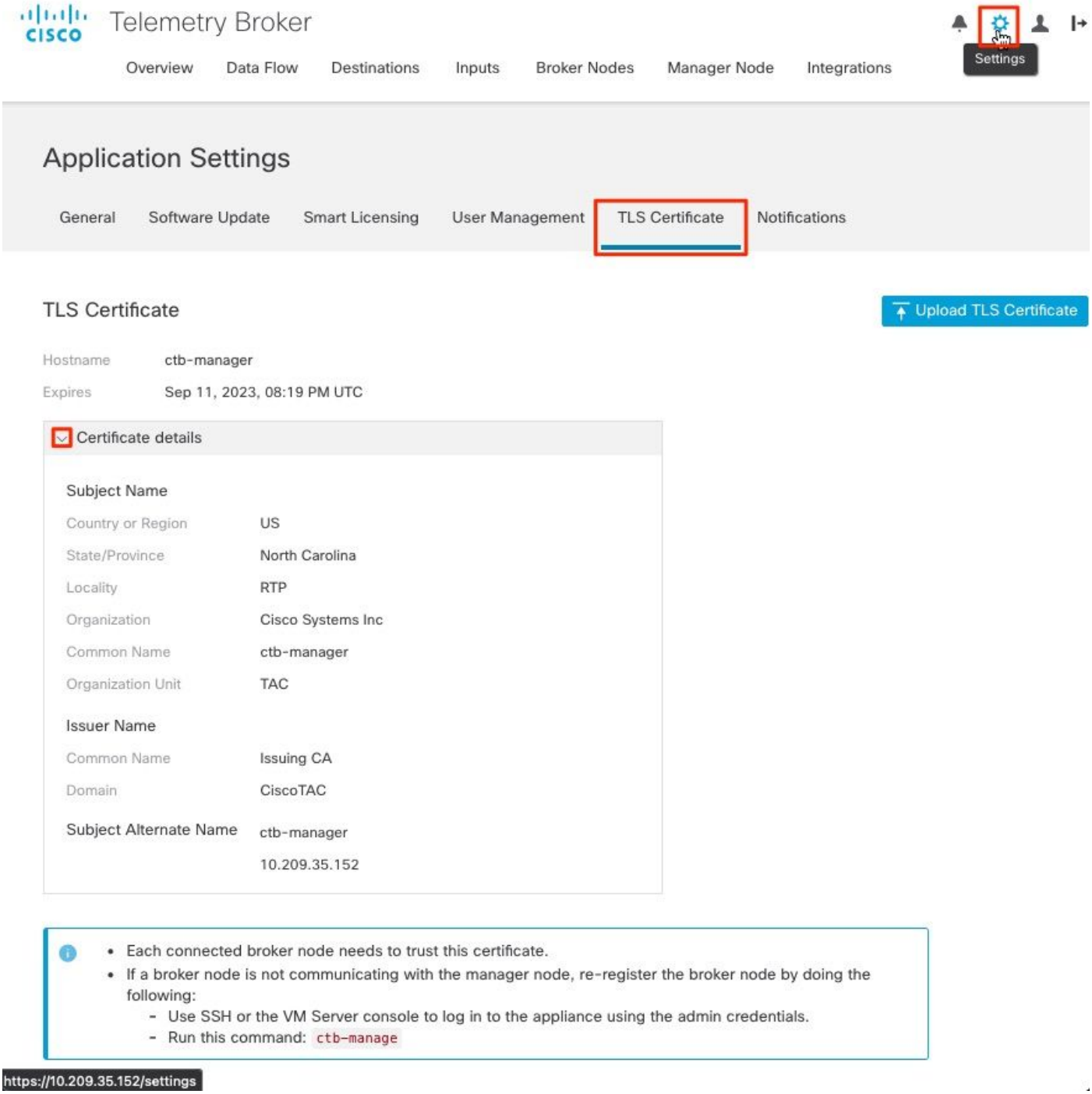
```
== Management Configuration

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
```

- Verifique os detalhes do certificado se eles correspondem aos valores do certificado assinado e selecione y para aceitar o certificado. Os serviços são iniciados automaticamente e, quando o serviço é iniciado, o prompt é retornado. O início do serviço pode levar até cerca de 15 minutos para ser concluído.

```
== 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
```

Verificar

Faça login no Console Web do Nó do Gerenciador CTB e navegue até Settings > TLS Certificate para ver detalhes do certificado, como uma nova data de expiração, ou exiba os detalhes do certificado usando o navegador para exibir informações mais detalhadas, como números de série.



Detalhes do certificado CTB

Verifique se o CTB Broker Node não mostra nenhum alarme na interface do usuário da Web do CTB Manager Node.

Troubleshooting

Se o certificado estiver incompleto, por exemplo, sem os certificados de cadeia, o Nó do agente CTB não consegue comunicar-se com o Nó do gerente e apresenta "Não visto desde" na coluna Status na lista de Nós do agente.
O nó do agente continuará a replicar e distribuir o tráfego nesse estado.

Faça login na CLI do Nó do Gerenciador CTB e emita o sudo grep -ic begin /var/lib/titan/titanium_frontend/ssl/cert.pem comando para ver quantos certificados estão no arquivo cert.pem.

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

O valor de saída retornado precisa ser igual ao número de dispositivos CA na cadeia mais o Gerenciador CTB.

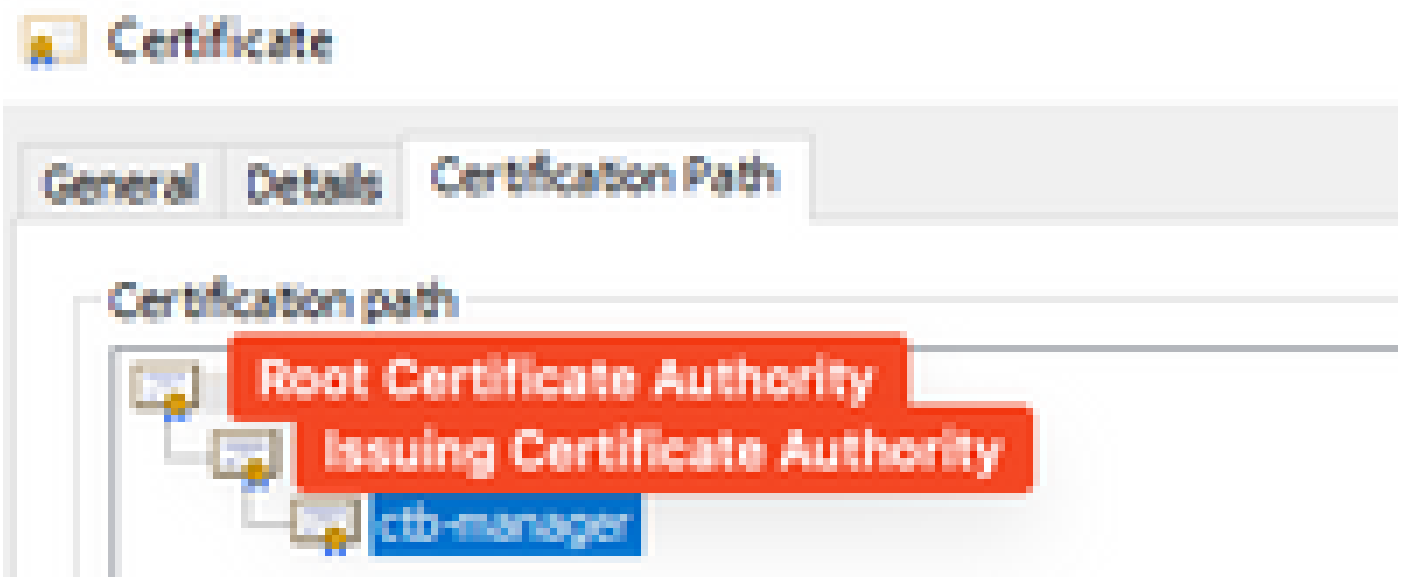
A saída de 1 é esperada se estiver usando um certificado autoassinado.

A saída de 2 é esperada se a infraestrutura PKI consiste em uma única CA raiz que também é a CA emissora.

A saída de 3 é esperada se a infraestrutura PKI consiste em uma CA raiz e na CA emissora.

A saída de 4 é esperada se a infraestrutura PKI consiste em uma CA raiz, uma CA subordinada e a CA emissora.

Compare a saída com a PKI listada ao visualizar o certificado em outro aplicativo, como Microsoft Windows Crypto Shell Extensions.



Infraestrutura PKI

Nesta imagem, a infraestrutura PKI inclui uma CA raiz e a CA emissora.

Espera-se que o valor de saída do comando seja 3 nesse cenário.

Se a saída não atender às expectativas, revise as etapas na seção **Criar um Certificado com Cadeia** para determinar se um certificado foi perdido.

Ao exibir um certificado no, Microsoft Windows Crypto Shell Extensions é possível que nem todos os certificados sejam apresentados se o computador local não tiver informações suficientes para verificar o certificado.

Emita o sudo ctb-mayday comando da CLI para gerar um pacote de maio para o TAC revisar.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.