Reemplazar certificado de identidad de agente de telemetría

Contenido

Introducción

Este documento describe cómo reemplazar el Certificado de identidad del servidor en el nodo del administrador de Cisco Telemetry Broker (CTB).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Administración de dispositivos de Cisco Telemetry Broker
- Certificados X509

Componentes Utilizados

Los dispositivos utilizados para este documento están ejecutando la versión 2.0.1

- Nodo de Cisco Telemetry Broker Manager
- Nodo de Cisco Telemetry Broker

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

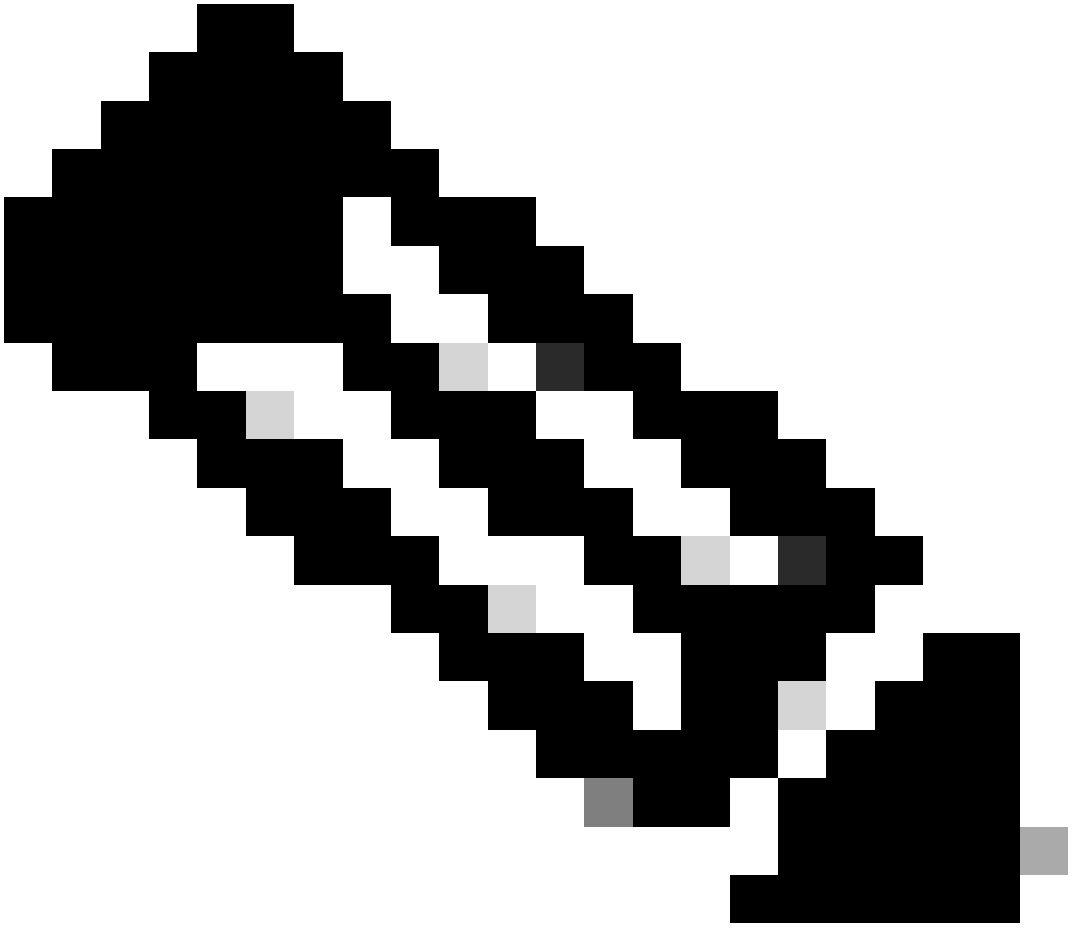
Requisitos del certificado

El certificado x509 utilizado por Cisco Telemetry Broker Manager debe cumplir estos requisitos:

- El certificado y la clave privada deben ser un par coincidente
- El certificado y la clave privada deben estar codificados con PEM
- La clave privada no debe estar protegida por una frase de paso

Confirmar que el certificado y la clave privada coinciden

Inicie sesión en la interfaz de línea de comandos (CLI) del administrador de CTB como usuario administrador.



Nota: Es posible que los archivos mencionados en esta sección aún no existan en el sistema.

El sudo openssl req -in server.csr -pubkey -noout -outform pem | sha256sum comando genera la suma de comprobación SHA-256 de la clave pública a partir del archivo de solicitud de firma de certificado.

El sudo openssl pkey -in server_key.pem -pubout -outform pem | sha256sumcomando genera la suma de comprobación SHA-256 de la clave pública a partir del archivo de clave privada.

El sudo openssl x509 -in server_cert.pem -pubkey -noout -outform pem | sha256sumcomando genera la suma de comprobación SHA-256 de la clave pública a partir del archivo de certificado emitido.

La salida del certificado y la clave privada deben coincidir. Si no se utilizó una solicitud de firma de certificado, el archivo server_cert.pem no existe.

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

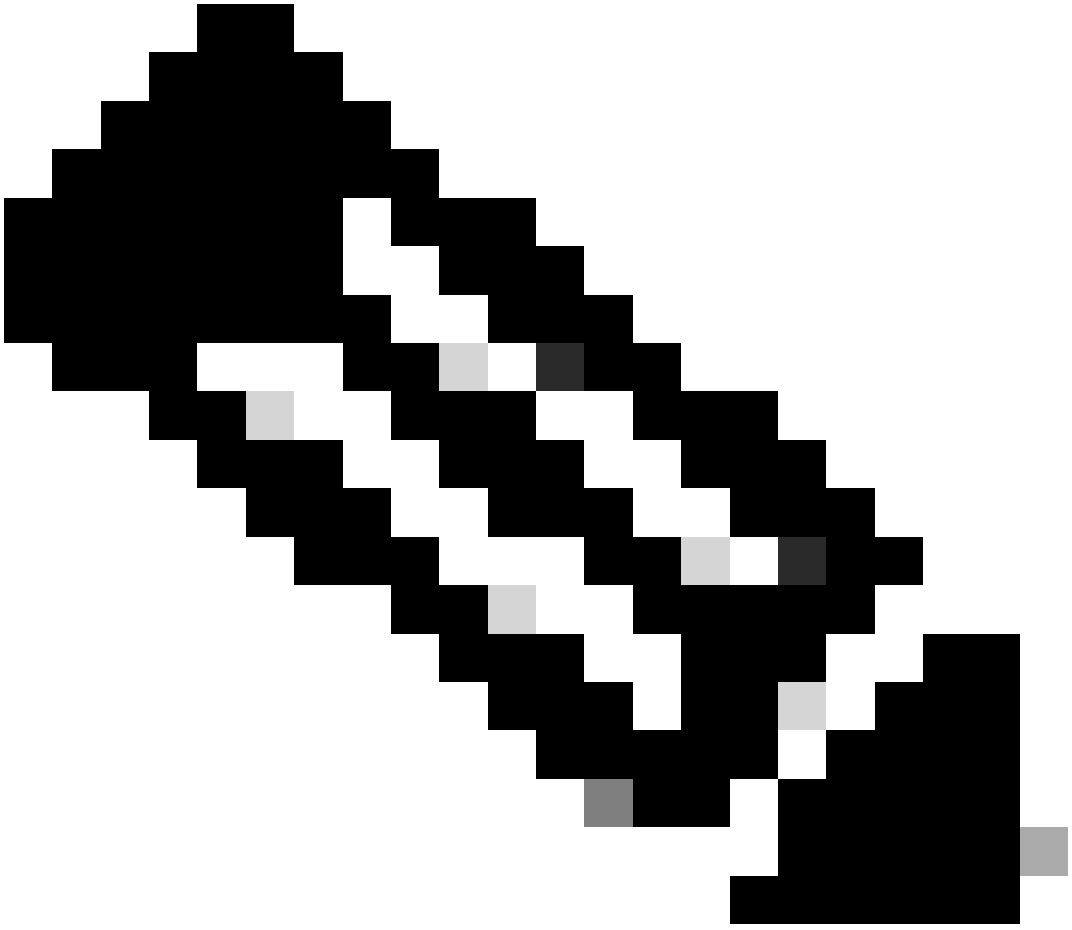
Confirmar clave privada no está protegida con frase de paso

Inicie sesión en el administrador de CTB como el usuario administrador. Ejecute el ssh-keygen -yf server_key.pem comando.

No se solicita una frase de paso si la clave privada no la requiere.

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

El certificado de confirmación y la clave privada están codificados con PEM



Nota: Estas validaciones se pueden realizar antes de instalar los certificados.

Inicie sesión en el administrador de CTB como el usuario administrador.

Vea el contenido del archivo server_cert.pem con el sudo cat server_cert.pem comando. Ajuste el comando al nombre de archivo del certificado.

La primera y la última línea del archivo deben ser **-----BEGIN CERTIFICATE-----** y -----END CERTIFICATE----- respectivamente.

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

Vea el archivo server_key.pem con el sudo cat server_key.pem comando. Ajuste el comando al nombre del archivo de claves privadas.

La primera y la última línea del archivo deben ser **-----BEGIN PRIVATE KEY-----** y -----END PRIVATE KEY----- respectivamente.

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

Certificado autofirmado

Generar certificado autofirmado

- Inicie sesión en el CTB Manager a través de un SSH (Secure Shell), ya que el usuario configurado durante la instalación suele ser el usuario "admin".

- Ejecute el 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.

  - Cambie la rsa:{key_len} clave con la longitud privada que desee, como 2048, 4096 u 8192

  - Cambie el {ctb_manager_ip}con la IP del nodo del administrador de 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:~$
```

- Vea el archivo server_cert.pem con el cat server_cert.pem comando y copie el contenido en el búfer para pegarlo en la estación de trabajo local en el editor de texto que desee. Guarde el archivo. También puede desconectar estos archivos del /home/admin directorio mediante SCP.

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

- Vea el archivo server_key.pem con el sudo cat server_key.pem comando y copie el contenido en el búfer para que pueda pegarse en la estación de trabajo local en el editor de texto que desee. Guarde el archivo. También puede enviar a SCP este archivo fuera del /home/admin directorio.

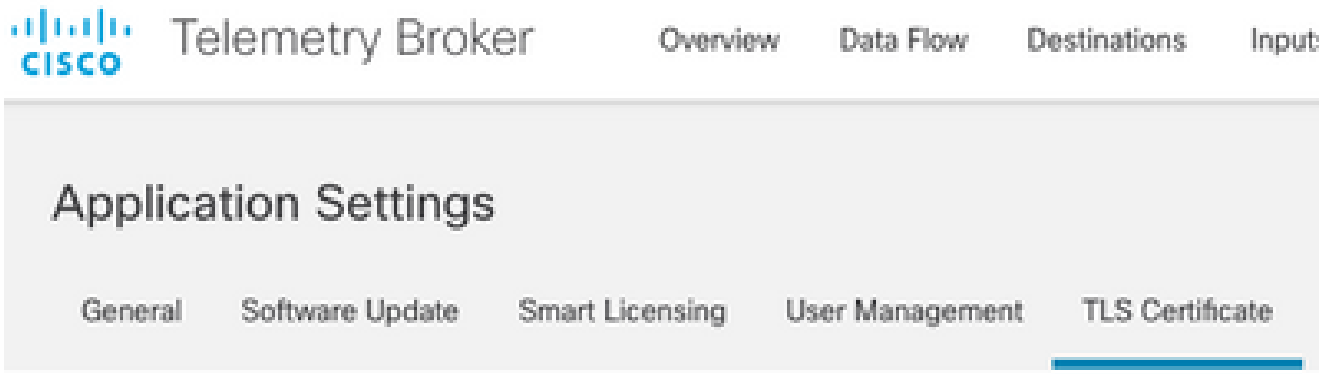
```
admin@ctb-manager:~$ sudo cat server_key.pem
-----BEGIN PRIVATE KEY-----
{removed_for_brevity}
-----END PRIVATE KEY-----
admin@ctb-manager:~$
```

Cargar certificado autofirmado

1. Navegue hasta la interfaz de usuario web del administrador de CTB, inicie sesión como el usuario administrador y haga clic en el icono del engranaje para acceder a "Settings".

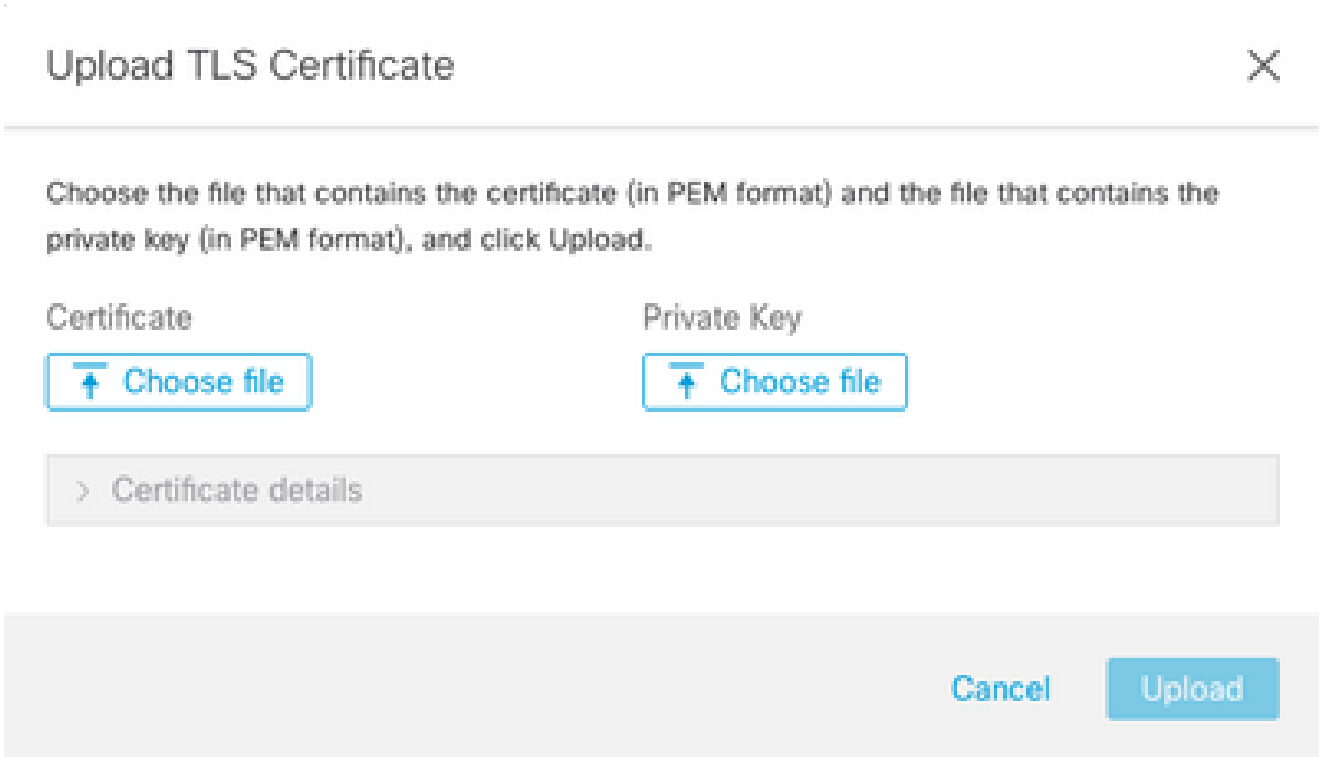
Icono de configuración de CTB

- Vaya a la ficha "Certificado TLS".

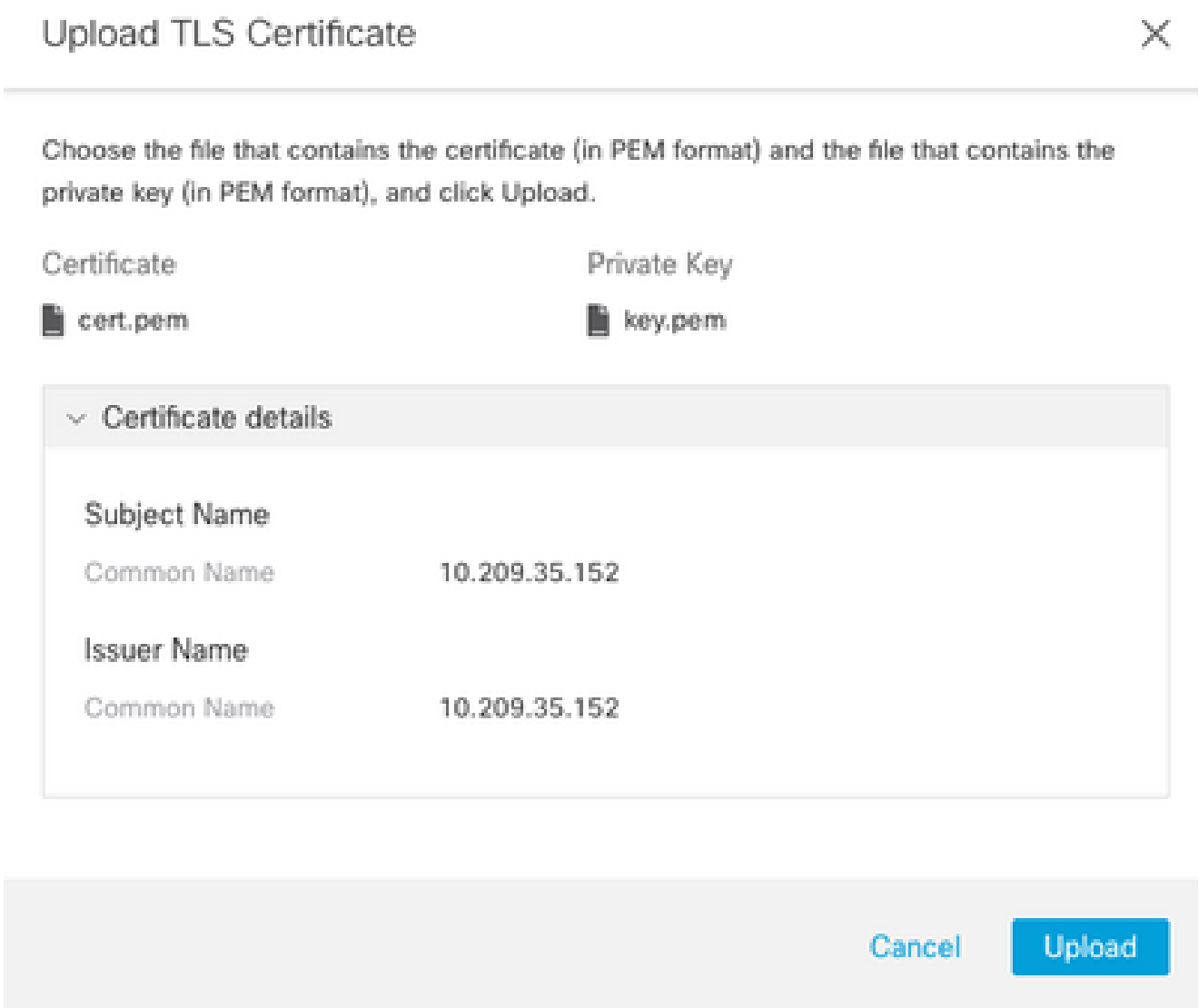


Ficha Certificados CTB

- Seleccione Upload TLS Certificate y, a continuación, seleccione el server_cert.pem y el server_key.pem para el certificado y la clave privada respectivamente en el cuadro de diálogo "Cargar certificado TLS". Una vez seleccionados los archivos, seleccione Cargar.



• Una vez que se seleccionan los archivos, un proceso de verificación confirma la combinación de certificado y clave y muestra el nombre común del emisor y el asunto como se muestra.



Carga de certificados de CTB

- Seleccione el botón "Cargar" para cargar el nuevo certificado. La interfaz de usuario web se reinicia por sí sola en unos instantes y, después de reiniciarla, vuelve a iniciar sesión en el dispositivo.

- Inicie sesión en la consola web del nodo de CTB Manager y navegue hasta Settings > TLS Certificate para ver los detalles del certificado, como una nueva fecha de vencimiento, o ver los detalles del certificado mediante el explorador para ver información más detallada, como los números de serie.

Actualizar nodos de Broker

Una vez que el nodo de CTB Manager tiene un nuevo certificado de identidad, cada nodo de CTB Broker se debe actualizar manualmente.

1. Inicie sesión en cada nodo de broker mediante ssh y ejecute el 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:
```

- Seleccione la opción ccuando se le solicite.

```
== 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** Compruebe los detalles del certificado si coinciden con los valores del certificado firmado y seleccione aceptar el certificado. Los servicios se inician automáticamente y, una vez iniciado el servicio, se devuelve el mensaje. El inicio del servicio puede tardar unos 15 minutos en completarse.

```
== 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 por la autoridad certificadora (CA)

Generar solicitud de firma de certificado (CSR) para su emisión por una autoridad de certificados

- Inicie sesión en el CTB Manager a través de un SSH (Secure Shell), ya que el usuario configurado durante la instalación suele ser el usuario "admin".

- Ejecute el 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. Los atributos 'extra' de las últimas dos líneas se pueden dejar en blanco si se desea.

  - Cambie el {ctb_manager_dns_name} con el nombre DNS del nodo del administrador de CTB

    - Cambie el {ctb_manager_ip}con la IP del nodo del administrador de CTB

    - Cambie la clave {key_len} con una longitud de clave privada como 2048, 4096 u 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 agrega los archivos CSR y Key a una máquina local y proporciona el CSR a la CA. La emisión de la CSR por la CA en formato PEM queda fuera del alcance de este documento.

Crear un certificado con cadena

La CA emite el certificado de identidad del servidor en formato PEM. Se debe crear un archivo de cadena que incluya todos los certificados de cadena y el certificado de identidad del servidor para el nodo del administrador de CTB.

En un editor de texto, cree un archivo combinando el certificado firmado en el paso anterior y anexando todos los certificados de la cadena, incluida la CA de confianza, en un solo archivo en formato PEM en el orden mostrado.

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

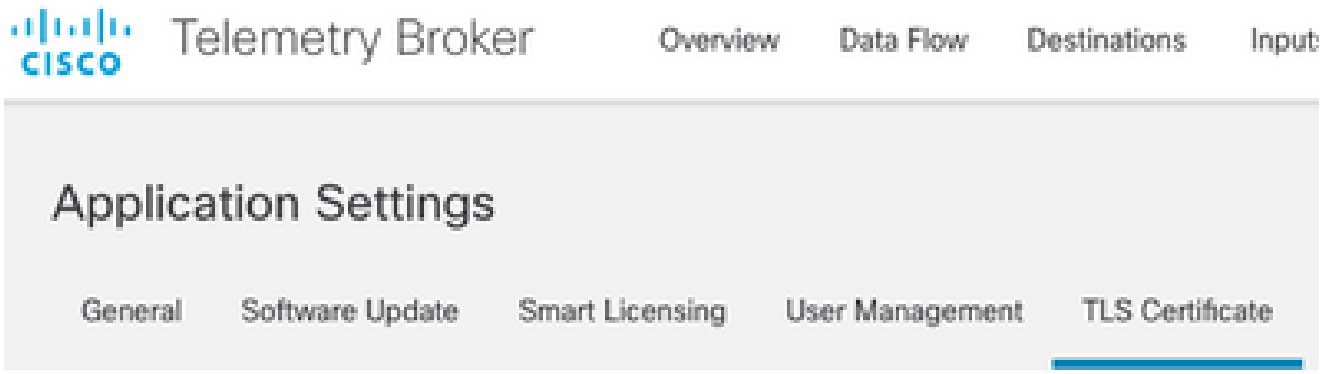
Asegúrese de que este nuevo archivo de certificado con archivo de cadena no tenga espacios iniciales ni finales, líneas en blanco y esté en el orden indicado anteriormente.

Cargar certificado emitido por autoridad certificadora

1. Navegue hasta la interfaz de usuario web del administrador de CTB, inicie sesión como administrador y haga clic en el icono del engranaje para acceder a "Settings".

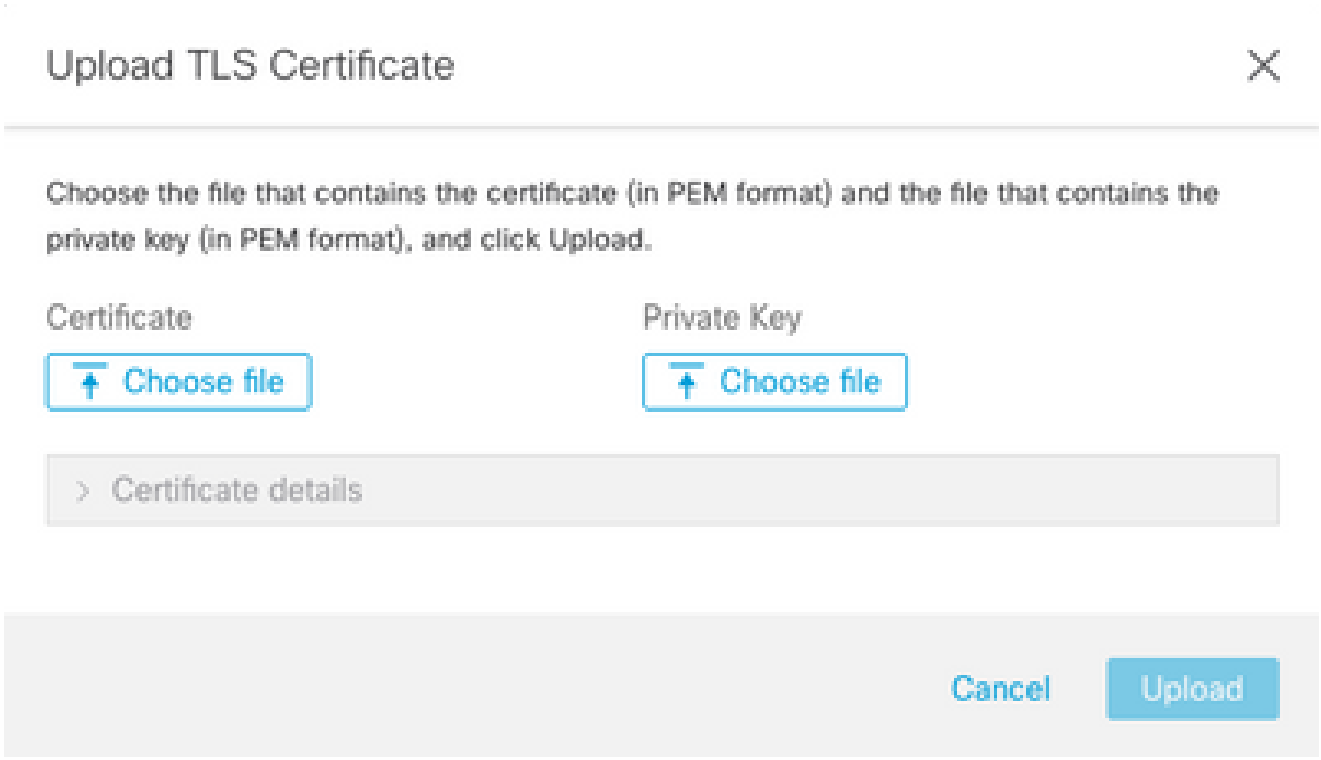
Icono de configuración de CTB

- Vaya a la ficha "Certificado TLS".

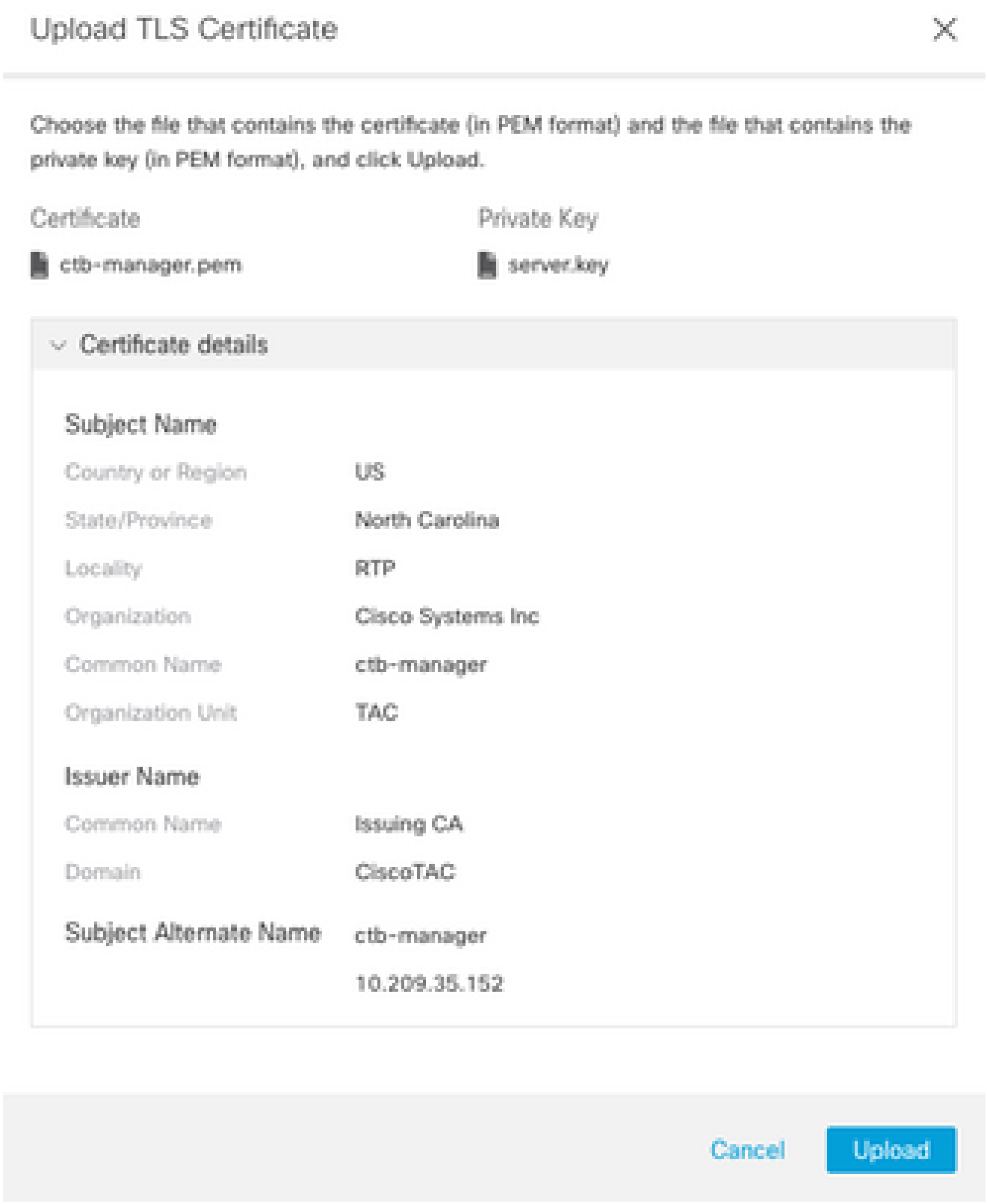


Ficha Certificados CTB

- Seleccione Upload TLS Certificate y, a continuación, seleccione el certificado con el archivo de cadena creado en la última sección y el Administrador de CTB generado server_key.pem para el certificado y la clave privada respectivamente en el cuadro de diálogo "Cargar certificado TLS". Una vez seleccionados los archivos, seleccione Cargar.



• Una vez seleccionados los archivos, un proceso de verificación confirma la combinación de certificado y clave y muestra el nombre común del emisor y el asunto, como se muestra a continuación.



Validación de certificado emitido por CA de CTB

- Seleccione el botón "Cargar" para cargar el nuevo certificado. La interfaz de usuario web se reinicia por sí sola en unos 60 segundos, inicie sesión en la interfaz de usuario web después de reiniciarse.

- Inicie sesión en la consola web del nodo de CTB Manager y navegue hasta Settings > TLS Certificate para ver los detalles del

certificado, como una nueva fecha de vencimiento, o ver los detalles del certificado mediante el explorador para ver información más detallada, como los números de serie.

Actualizar nodos de Broker

Una vez que el nodo de CTB Manager tiene un nuevo certificado de identidad, cada nodo de CTB Broker se debe actualizar manualmente.

1. Inicie sesión en cada nodo de broker mediante ssh y ejecute el 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:
```

- Seleccione la opción ccuando se le solicite.

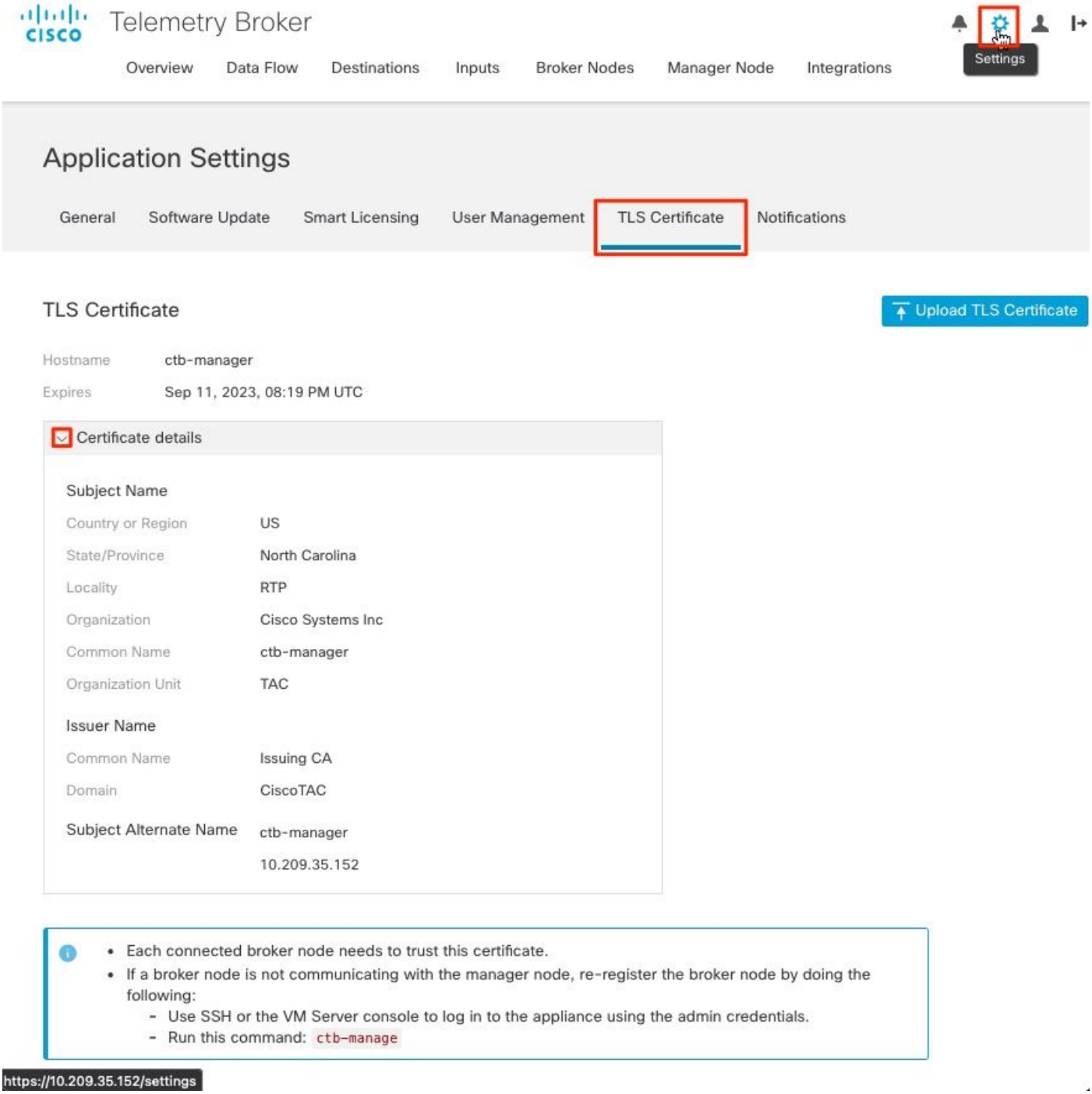
```
== Management Configuration

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 los detalles del certificado si coinciden con los valores del certificado firmado y seleccione y aceptar el certificado. Los servicios se inician automáticamente y, una vez iniciado el servicio, se devuelve el mensaje. El inicio del servicio puede tardar unos 15 minutos en completarse.

```
== 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
```

Verificación

Inicie sesión en la consola web del nodo de CTB Manager y navegue hasta Settings > TLS Certificate para ver los detalles del certificado, como una nueva fecha de vencimiento, o ver los detalles del certificado mediante el explorador para ver información más detallada, como los números de serie.



Detalles del certificado CTB

Verifique que el nodo de broker de CTB no muestre alarmas en la interfaz de usuario web del nodo de gerente de CTB.

Troubleshoot

Si el certificado está incompleto, como por ejemplo si faltan los certificados de cadena, el nodo de nodo de broker de CTB no puede comunicarse con el nodo de gerente y presenta "No visto desde" en la columna Estado de la lista de nodos de broker.
El nodo de Broker continuará replicando y distribuyendo el tráfico en este estado.

Inicie sesión en la CLI del nodo del administrador de CTB y ejecute el sudo grep -ic begin /var/lib/titan/titanium_frontend/ssl/cert.pem comando para ver cuántos certificados hay en el archivo cert.pem.

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

El valor de salida devuelto debe ser igual al número de dispositivos CA de la cadena más el Administrador de CTB.

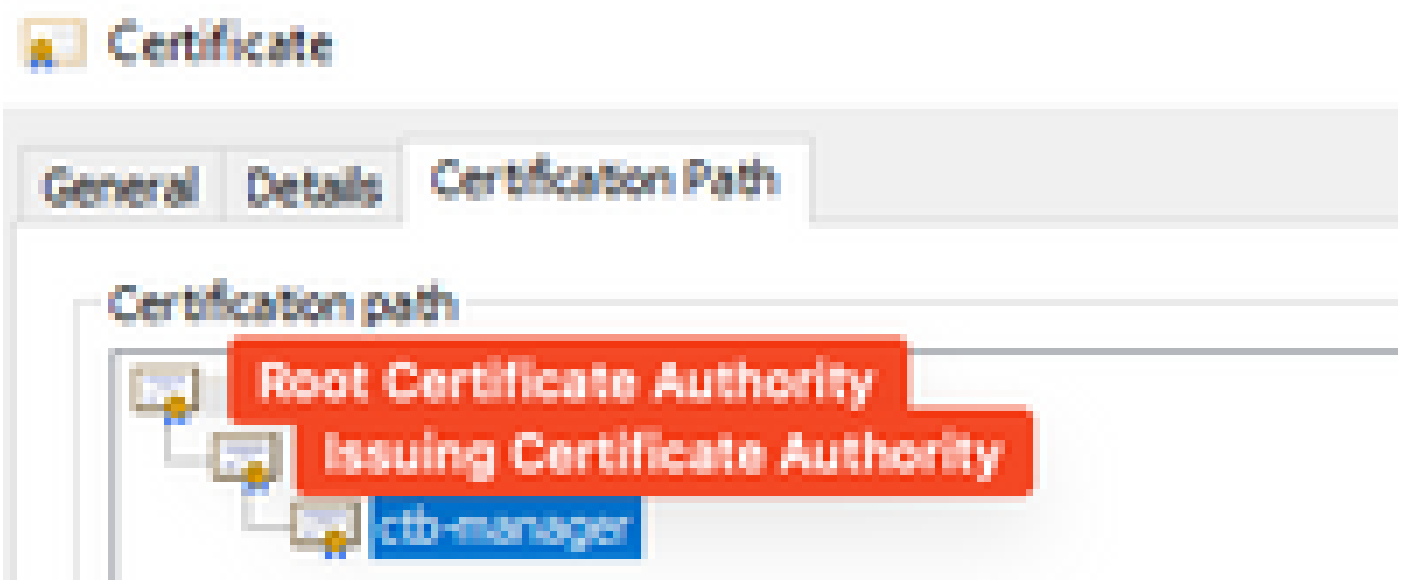
Se espera el resultado de 1 si se utiliza un certificado autofirmado.

Se espera el resultado de 2 si la infraestructura PKI consta de una única CA raíz que también es la CA emisora.

Se espera el resultado de 3 si la infraestructura PKI consta de una CA raíz y la CA emisora.

Se espera el resultado de 4 si la infraestructura PKI consta de una CA raíz, una CA subordinada y la CA emisora.

Compare la salida con la PKI enumerada al visualizar el certificado en otra aplicación como Microsoft Windows Crypto Shell Extensions.



Infraestructura PKI

En esta imagen, la infraestructura PKI incluye una CA raíz y la CA emisora.

Se espera que el valor de salida del comando sea 3 en este escenario.

Si el resultado no cumple las expectativas, revise los pasos de la sección **Creación de un Certificado con Cadena** para determinar si se ha omitido un certificado.

Al ver un certificado en Microsoft Windows Crypto Shell Extensions él es posible que no se presenten todos los certificados si el equipo local no tiene suficiente información para verificar el certificado.

Ejecute el sudo ctb-mayday comando desde la CLI para generar un paquete de mayday para que el TAC lo revise.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).