替换遥测代理身份证书

目录

简介

先决条件

- 要求
- 使用的组件

配置

- 证书要求
  - 确认证书和私钥是否匹配
  - 确认私钥未受密码保护
  - 确认证书和私钥是PEM编码的
- 自签证书
  - 生成自签名证书
  - 上传自签名证书
  - 更新Broker节点
- 证书颁发机构(CA)颁发的证书
  - 生成证书签名请求(CSR)供证书颁发机构颁发
  - 使用链创建证书
  - 上传证书颁发机构颁发的证书
  - 更新Broker节点

验证

故障排除

简介

本文档介绍如何替换思科遥测代理(CTB)管理器节点上的服务器身份证书。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科遥测代理设备管理
- x509证书

使用的组件

用于本文档的设备运行版本2.0.1

- 思科遥测代理管理器节点
- 思科遥测代理节点

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

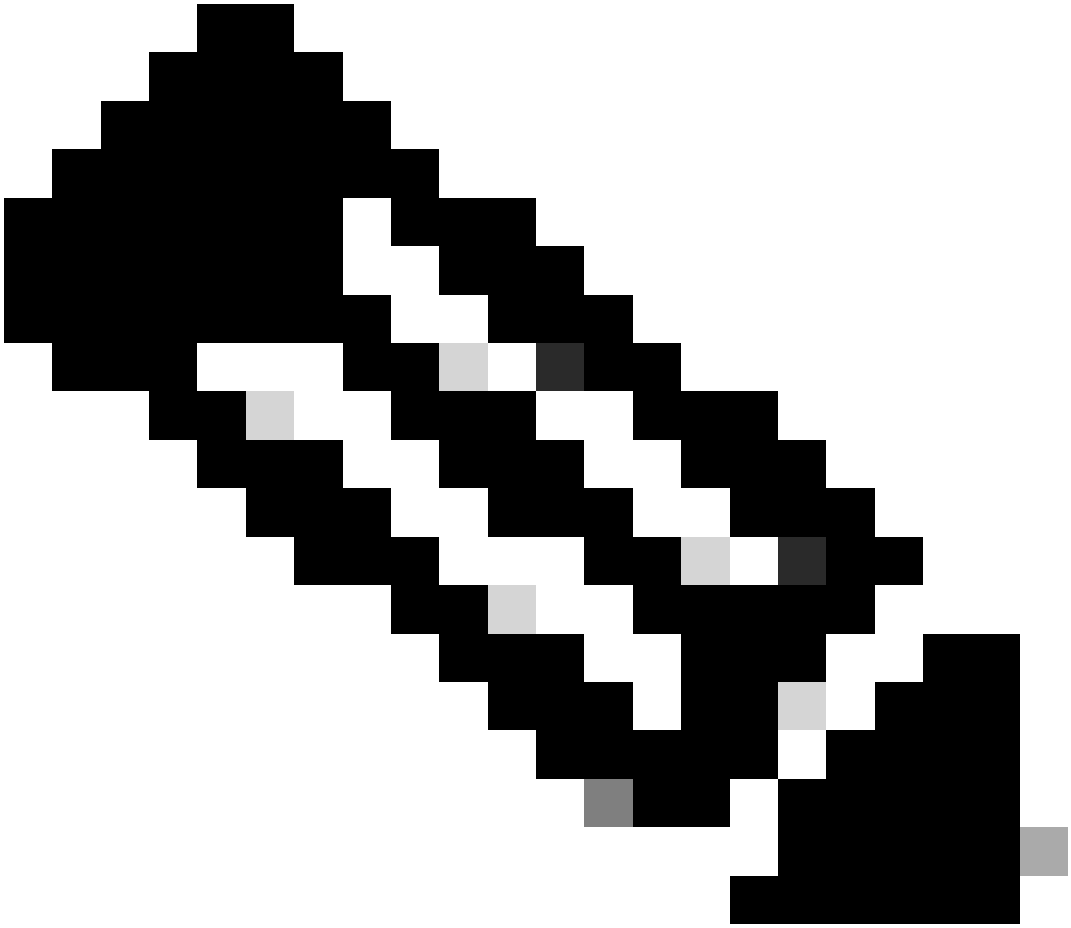
证书要求

思科遥测代理管理器使用的x509证书必须满足以下要求：

- 证书和私钥必须是匹配对
- 证书和私钥必须采用PEM编码
- 私钥不能受密码保护

确认证书和私钥是否匹配

以管理员用户身份登录到CTB管理器命令行界面(CLI)。



注意：此部分中提到的文件可能尚不存在于系统上。

命sudo openssl req -in server.csr -pubkey -noout -outform pem | sha256sum令从证书签名请求文件输出公钥的SHA-256校验和。

命sudo openssl pkey -in server_key.pem -pubout -outform pem | sha256sum令从私钥文件输出公钥的SHA-256校验和。

此命sudo openssl x509 -in server_cert.pem -pubkey -noout -outform pem | sha256sum令从颁发的证书文件中输出公钥的SHA-256校验和。

证书和私钥输出必须匹配。如果未使用证书签名请求，则server_cert.pem文件不存在。

```
admin@ctb-manager:~$ sudo openssl req -in server.csr -pubkey -noout -outform pem | sha256sum
3e8e6b0d397ada1be7e89be21eb555c9527741460074385730d524c60e3ae315  -
admin@ctb-manager:~$

admin@ctb-manager:~$ sudo openssl pkey -in server_key.pem -pubout -outform pem | sha256sum
3e8e6b0d397ada1be7e89be21eb555c9527741460074385730d524c60e3ae315  -

admin@ctb-manager:~$ sudo openssl x509 -in server_cert.pem -pubkey -noout -outform pem | sha256sum
3e8e6b0d397ada1be7e89be21eb555c9527741460074385730d524c60e3ae315  -
```

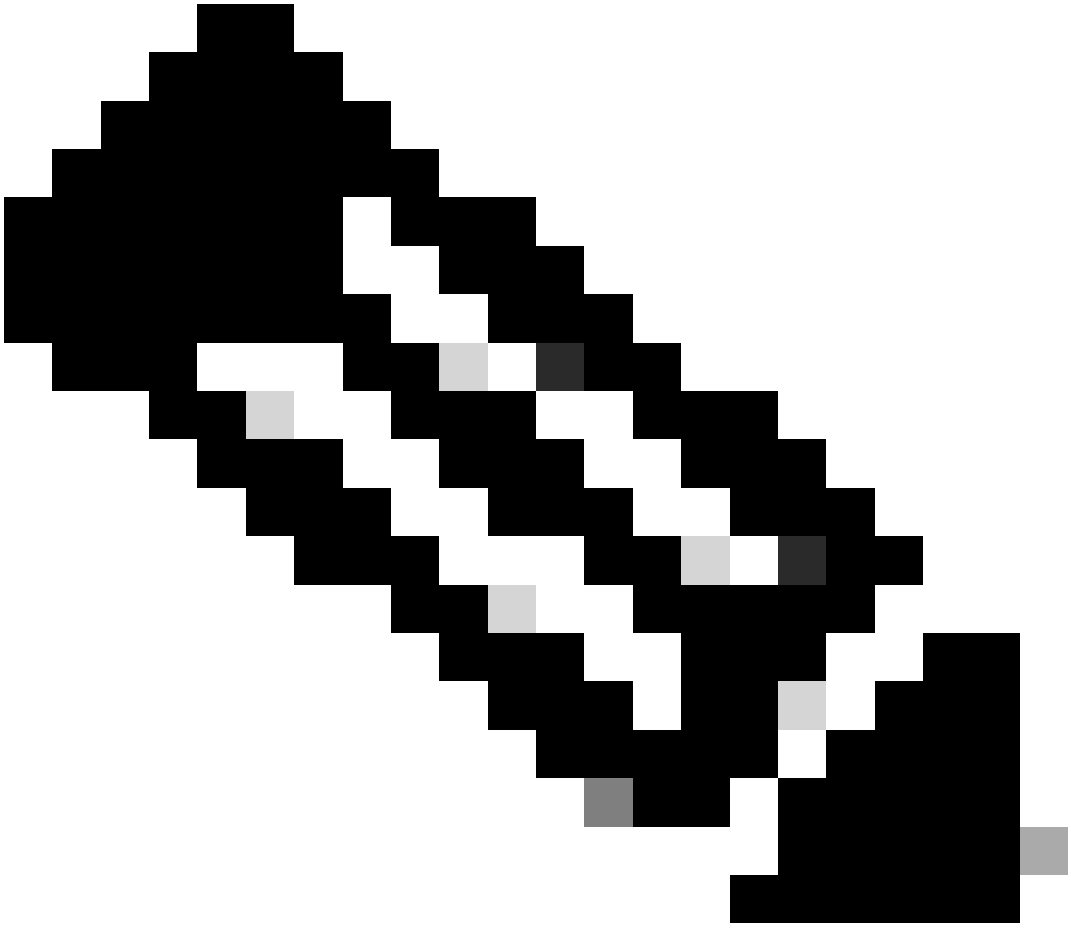
确认私钥未受密码保护

以管理员用户身份登录到CTB管理器。运行 命令。ssh-keygen -yf server_key.pem

如果私钥不需要密码，则不需要密码。

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

确认证书和私钥是PEM编码的



注意：这些验证可以在安装证书之前执行。

以管理员用户身份登录到CTB管理器。

使用命令查看server_cert.pem文件内sudo cat server_cert.pem容。将命令调整为您的证书文件名。

文件的第一行和第二行应分别-----**BEGIN CERTIFICATE**-----为-----END CERTIFICATE-----。

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

使用命令查看server_key.pem文sudo cat server_key.pem件。将命令调整为您的私钥文件名。

文件的第一行和第二行应分别-----**BEGIN PRIVATE KEY**-----为-----END PRIVATE KEY-----。

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

自签证书

生成自签名证书

1. 以安装过程中配置的用户身份通过SSH（安全外壳）登录到CTB管理器，通常是“admin”用户。
2. 发出命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}令。
   - 使用rsa:{key_len}您选择的私钥长度（例如2048、4096或8192）更改
   - 使用{ctb_manager_ip}CTB管理器节点的IP更改

   ```
   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:~$
   ```

3. 使用命令查看server_cert.pem文件cat server_cert.pem，并将内容复制到缓冲区，以便将其粘贴到本地工作站的所选文本编辑器中。保存文件。您也可以将这些文件从目录SCP出/home/admin去。

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

4. 使用命令查看server_key.pem文件sudo cat server_key.pem，并将内容复制到缓冲区，以便将其粘贴到本地工作站的所选文本编辑器中。保存文件。您也可以将此文件从目录SCP出/home/admin去。

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

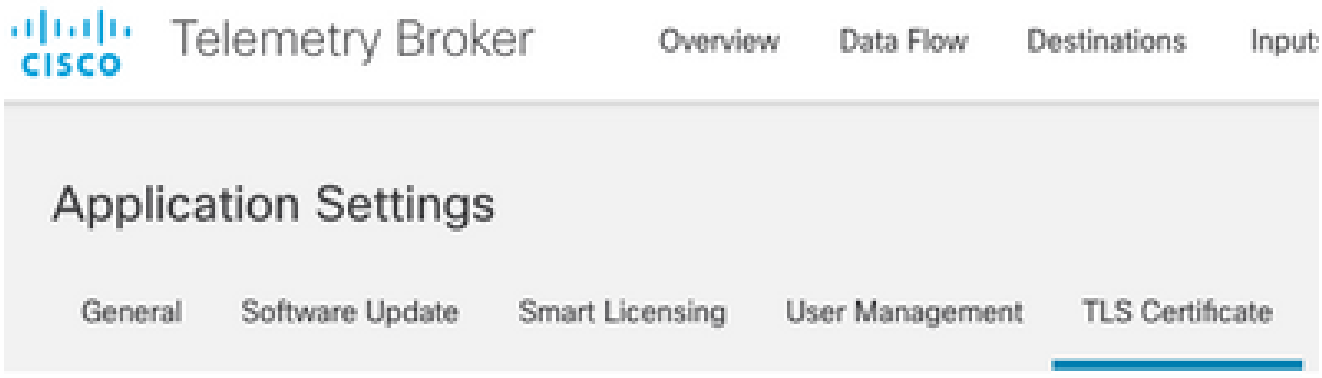
上传自签名证书

1. 导航到CTB Manager Web UI并以管理员用户身份登录，然后点击齿轮图标访问"Settings"。



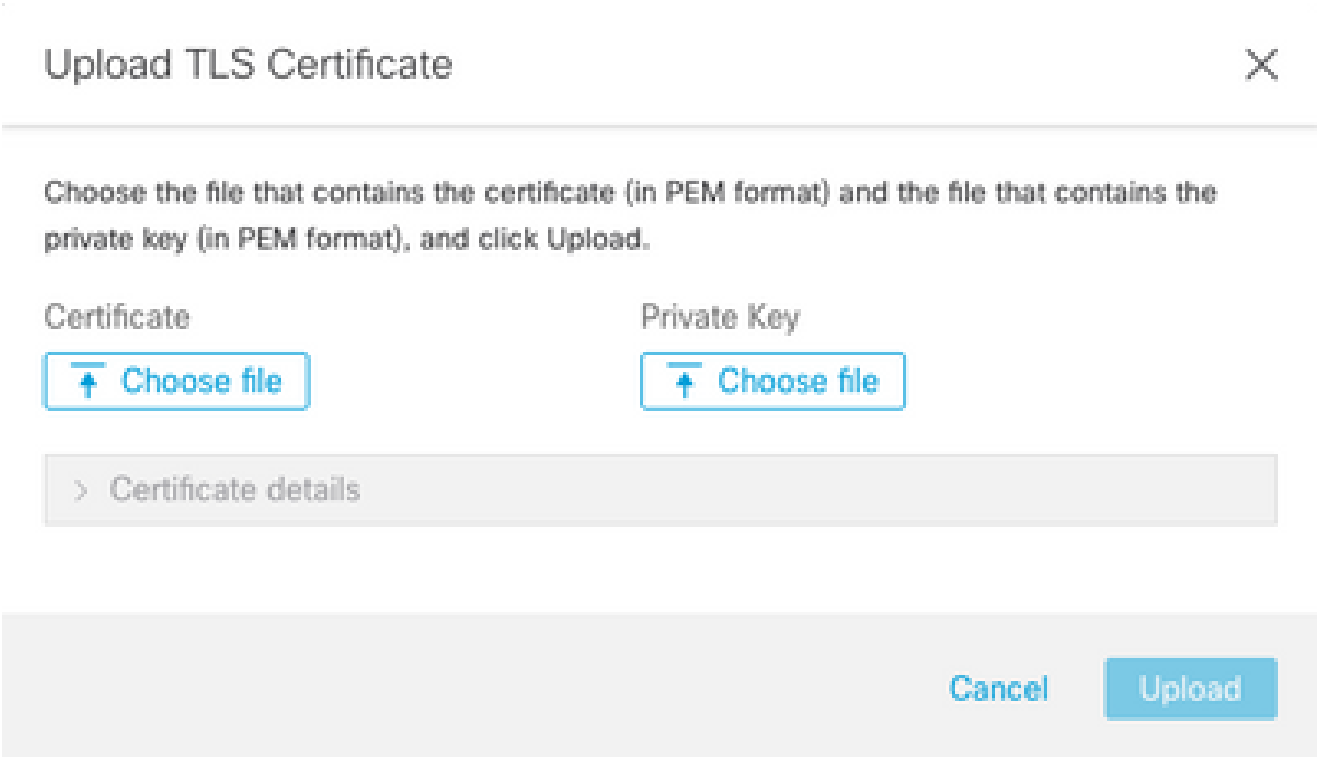
CTB设置图标

2. 导航至“TLS证书”选项卡。

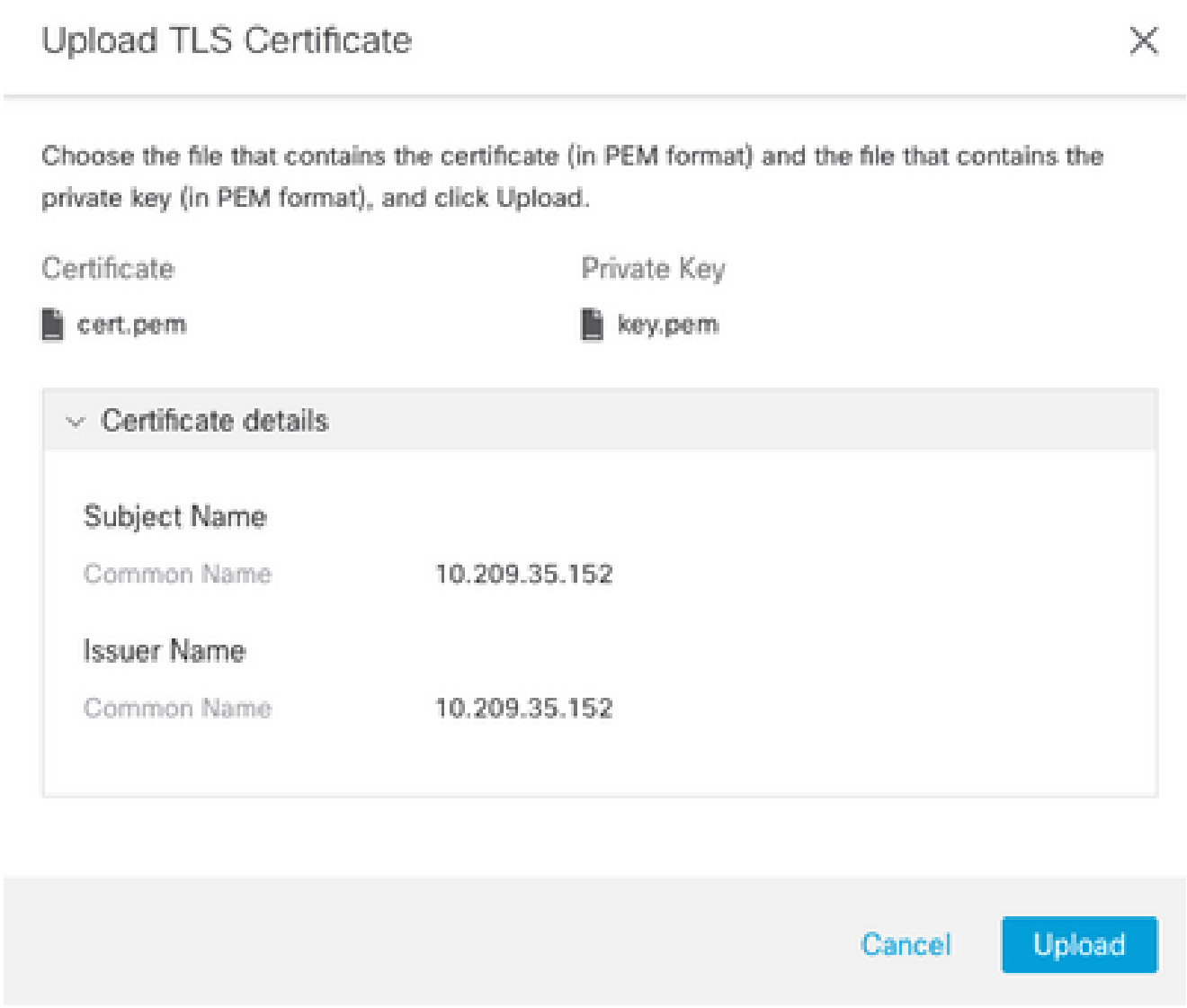


CTB证书选项卡

3. 选择Upload TLS Certificate ，然后在“上传server_cert.pemTLS证server_key.pem书”(Upload TLS Certificate)对话框中分别选择证书和私钥的。选择文件后，选择Upload。



4. 选择文件后，验证过程会确认证书和密钥的组合，并显示颁发者和主题的公用名称，如下所示。



CTB证书上传

5. 选择“上传”按钮上传新证书。Web UI会在几分钟内自行重新启动，重新启动后再次登录设备。

6. 登录到CTB管理器节点Web控制台，并导航到以查看证书详细信息（如新到期日期），或使用浏览器查看证书详细信息（如序列号）。Settings > TLS Certificate

更新Broker节点

一旦CTB管理器节点拥有新的身份证书，就必须手动更新每个CTB代理节点。

1. 通过ssh登录到每个Broker节点并运行命令。sudo ctb-manage

```
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:
```

2. 出现提示时c选择选项。

```
== 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
```

3. 验证证书详细信息（如果它们与签名证书的值匹配），y并选择接受证书。服务将自动启动，一旦服务启动，提示将返回。服务启动可能需要大约15分钟才能完成。

```
== 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
```

证书颁发机构(CA)颁发的证书

生成证书签名请求(CSR)供证书颁发机构颁发

1. 以安装过程中配置的用户身份通过SSH（安全外壳）登录到CTB管理器，通常是“admin”用户。

2. 发出命令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。如果需要，可将最后两行上的“extra”属性留空。
   - 使用{ctb_manager_dns_name}CTB管理器节点的DNS名称更改
   - 使用{ctb_manager_ip}CTB管理器节点的IP更改
   - 使用{key_len}您选择的私钥长度（例如2048、4096或8192）更改。

```
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 []:
```

3. 将CSR和密钥文件scp到本地计算机，并向CA提供CSR。CA以PEM格式发布CSR不属于本文档的范围。

使用链创建证书

CA以PEM格式颁发服务器身份证书。必须创建一个链文件，其中包含CTB管理器节点的所有链证书和服务器身份证书。

在文本编辑器中，通过合并上一步中签名的证书，并一直按显示顺序将链中的所有证书（包括受信任CA）附加到PEM格式的单个文件中来创建文件。

```
– BEGIN CERTIFICATE –
{CTB Manager Issued Certificate}
– END CERTIFICATE –
– BEGIN CERTIFICATE –
{Issuing Certificate Authority Certificate}
– END CERTIFICATE –
– BEGIN CERTIFICATE –
{Intermediate Certificate Authority Certificate}
– END CERTIFICATE –
– BEGIN CERTIFICATE –
{Root Certificate Authority Certificate}
– END CERTIFICATE –
```

确保此包含链文件的新证书文件没有前导或尾随空格、空行，并且按上面显示的顺序排列。

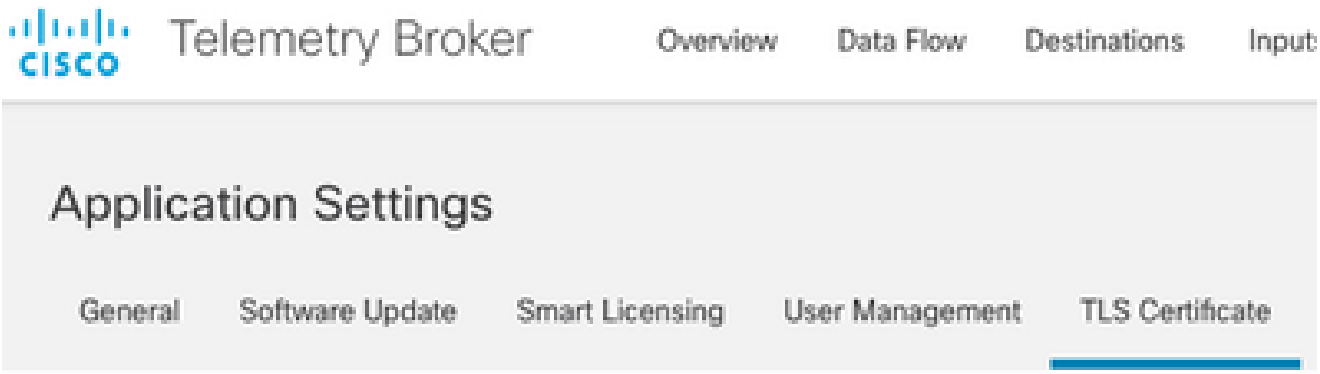
上传证书颁发机构颁发的证书

1. 导航到CTB Manager Web UI并以管理员身份登录，然后点击齿轮图标访问"Settings"。



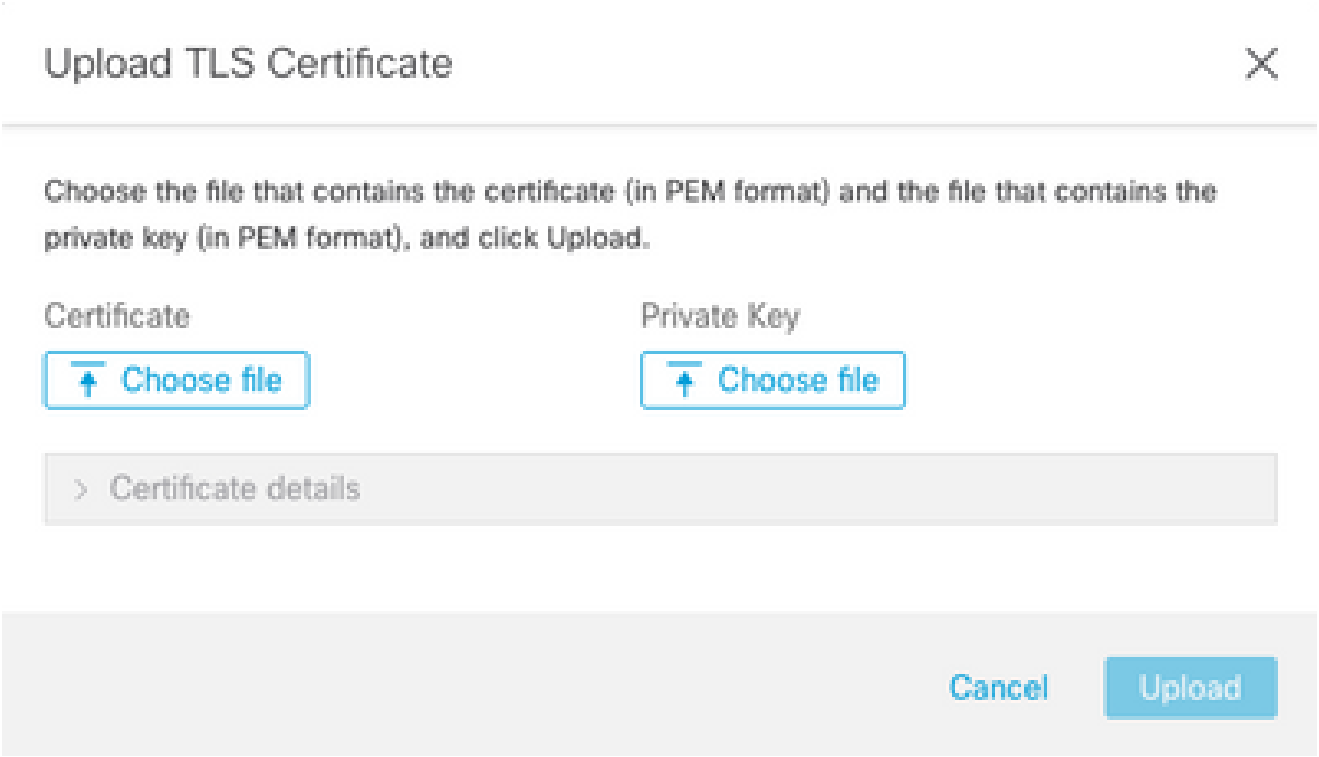
CTB设置图标

2. 导航至“TLS证书”选项卡。

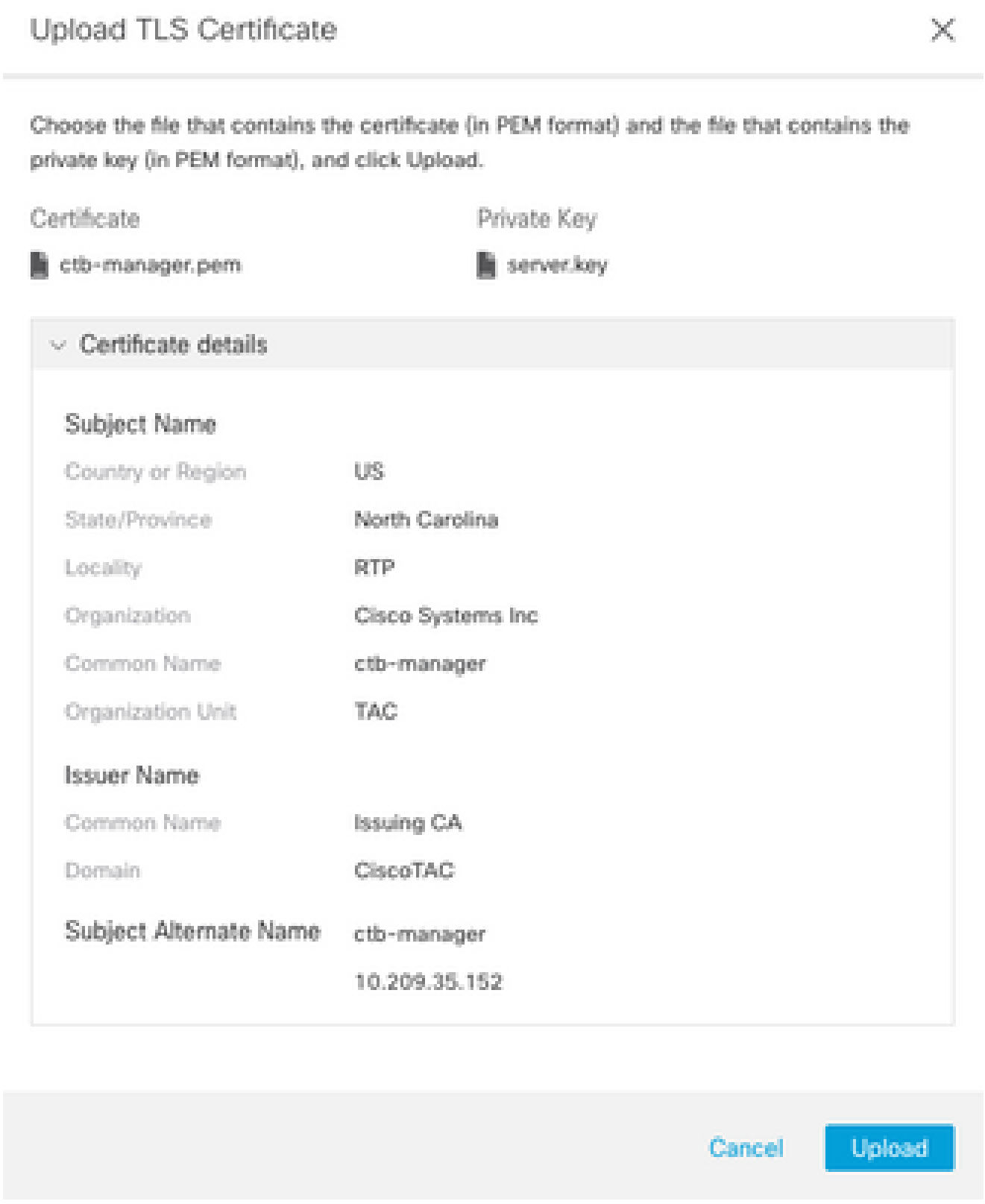


CTB证书选项卡

3. 选择Upload TLS Certificate，然后选择在最后一节创建的具有链文件的证书，并在“上传TLS证书”对话框中分别为证书和私钥生成CTB管理server_key.pem器。选择文件后，选择Upload。



4. 选择文件后，验证过程会确认证书和密钥的组合，并显示颁发者和主题的公用名称，如下所示。



CTB CA颁发的证书验证

5. 选择“上传”按钮上传新证书。Web UI将在大约60秒后自行重新启动，并在重新启动后登录到Web UI。

6. 登录到CTB管理器节点Web控制Settings > TLS Certificate台，并导航到以查看证书详细信息（如新到

期日期），或使用浏览器查看证书详细信息（如序列号）。

更新Broker节点

一旦CTB管理器节点拥有新的身份证书，就必须手动更新每个CTB代理节点。

1. 通过ssh登录到每个Broker节点并运行命sudo ctb-manage令

```
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:
```

2. 出现提示时c选择选项。

```
== 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
```

3. 验证证书详细信息（如果它们与已签名证书的值匹配），然后选择y(1)接受证书。服务将自动启动，一旦服务启动，提示将返回。服务启动可能需要大约15分钟才能完成。

```
== 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

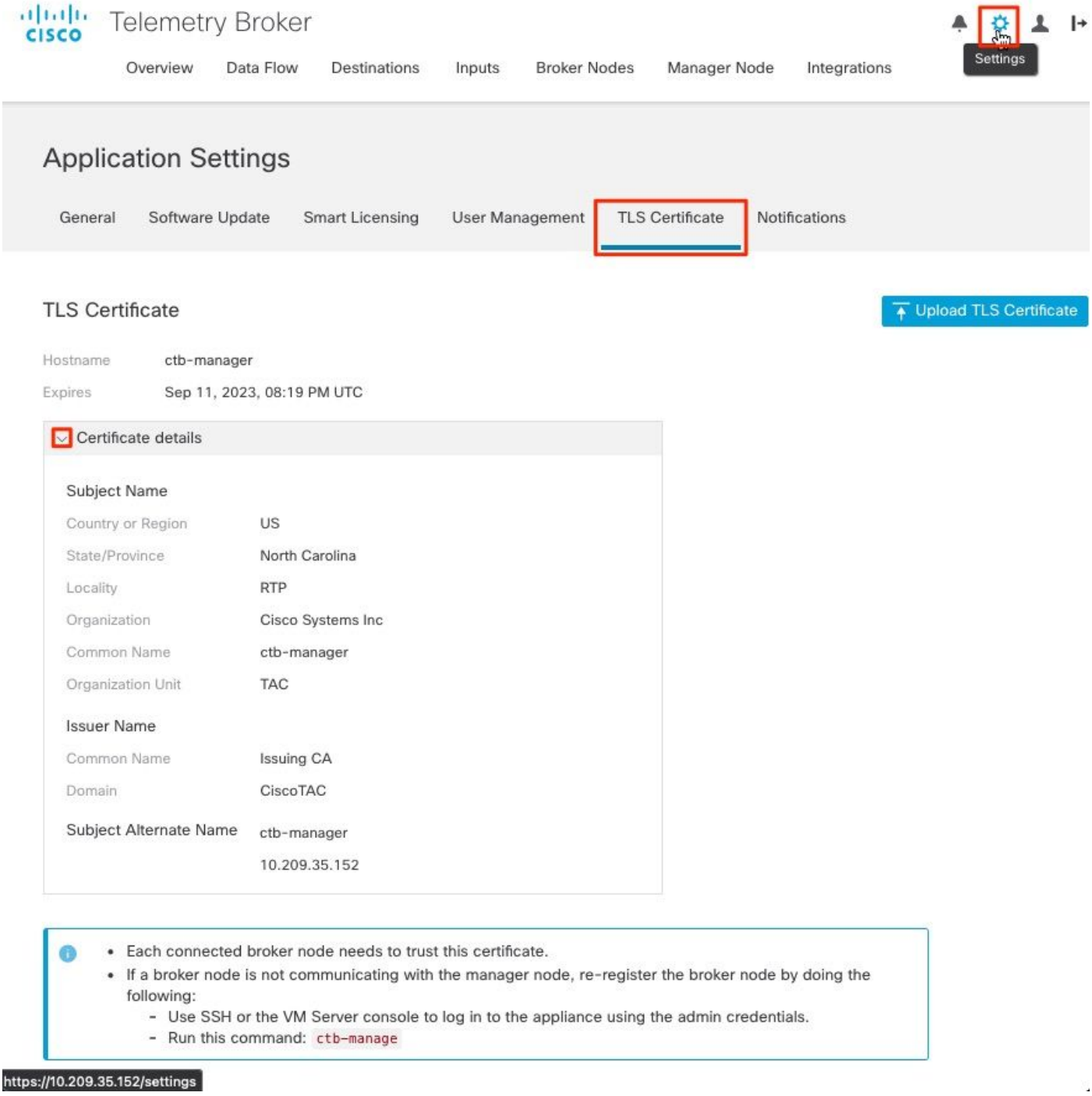
Do you accept the authenticity of the server? [y/n] y

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

== Starting service
```

验证

登录到CTB管理器节点Web控制Settings > TLS Certificate台，并导航到以查看证书详细信息（如新到期日期），或使用浏览器查看证书详细信息（如序列号）。



CTB证书详细信息

验证CTB代理节点在CTB管理器节点Web UI中是否显示警报。

故障排除

如果证书不完整（如缺少链式证书），CTB代理节点无法与管理器节点通信，并且在Broker节点列表的Status列中显示“Not Seen Since”。
Broker节点将继续复制和分发处于此状态的流量。

登录到CTB管理器节点CLI，然后发sudo grep -ic begin /var/lib/titan/titanium_frontend/ssl/cert.pem出命令以查看cert.pem文件中的证书数量。

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

返回的输出值需要等于链中的CA设备数加上CTB管理器。

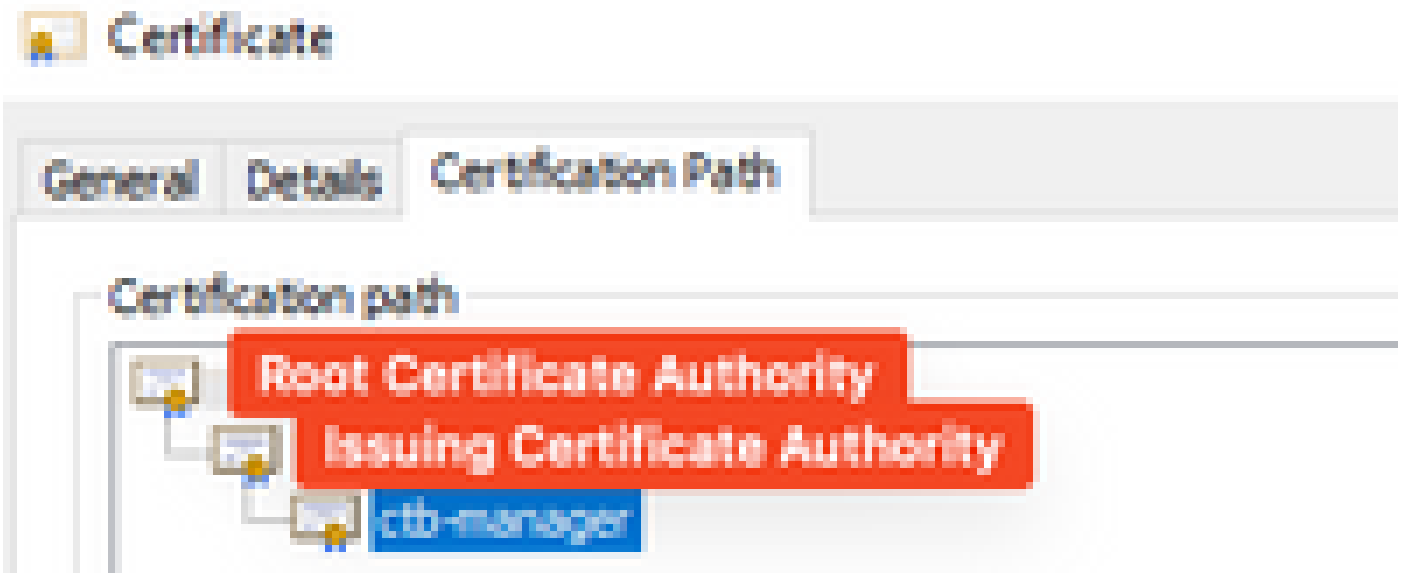
如果使用自签名证书，则预期输出1。

如果PKI基础设施包含单个根CA（也称为发布CA），则预期输出2。

如果PKI基础设施包含根CA和颁发CA，则预期输出3。

如果PKI基础设施由根CA、从属CA和颁发CA组成，则预期输出4。

将输出与查看其他应用程序（如）中的证书时列出的PKI进行比Microsoft Windows Crypto Shell Extensions较。



PKI基础设施

在此图中，PKI基础设施包括根CA和颁发CA。

在此场景中，命令的输出值预期为3。

如果输出未达到预期，请查看使用链创建证书部分中的步骤，确定是否错过了证书。

查看中的证书Microsoft Windows Crypto Shell Extensions时，如果本地计算机没有足够的信息来验证证书，则可能无法显示所有证书。

从CLIsudo ctb-mayday ，发出命令以生成一个Mayday捆绑包，供TAC审核。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。