替换遥测代理身份证书

目录

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

本文档中使用的设备运行的是2.0.1版

- 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

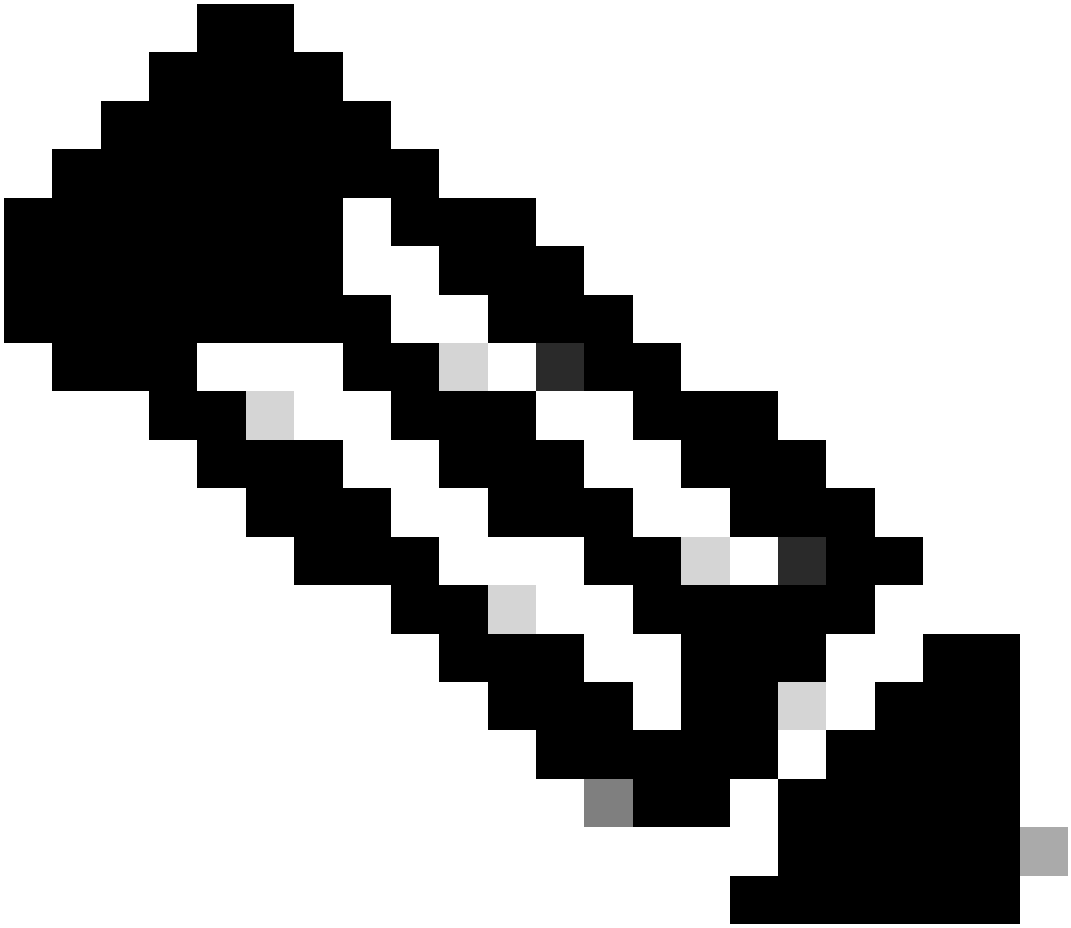
证书要求

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
- 私钥不能受密码短语保护

确认证书和私钥匹配

以管理员用户身份登录到CTB管理器命令行界面(CLI)。



注意：此部分中提及的文件可能尚未存在于系统中。

sudo openssl req -in server.csr -pubkey -noout -outform pem | sha256sum

命令从证书签名请求文件输出公钥的SHA-256校验和。

sudo openssl pkey -in server_key.pem -pubout -outform pem | sha256sum命令输出私钥文件中公钥的SHA-256校验和。

sudo openssl x509 -in server_cert.pem -pubkey -noout -outform pem | sha256sum命令从发出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 3e8e6b0d39
```

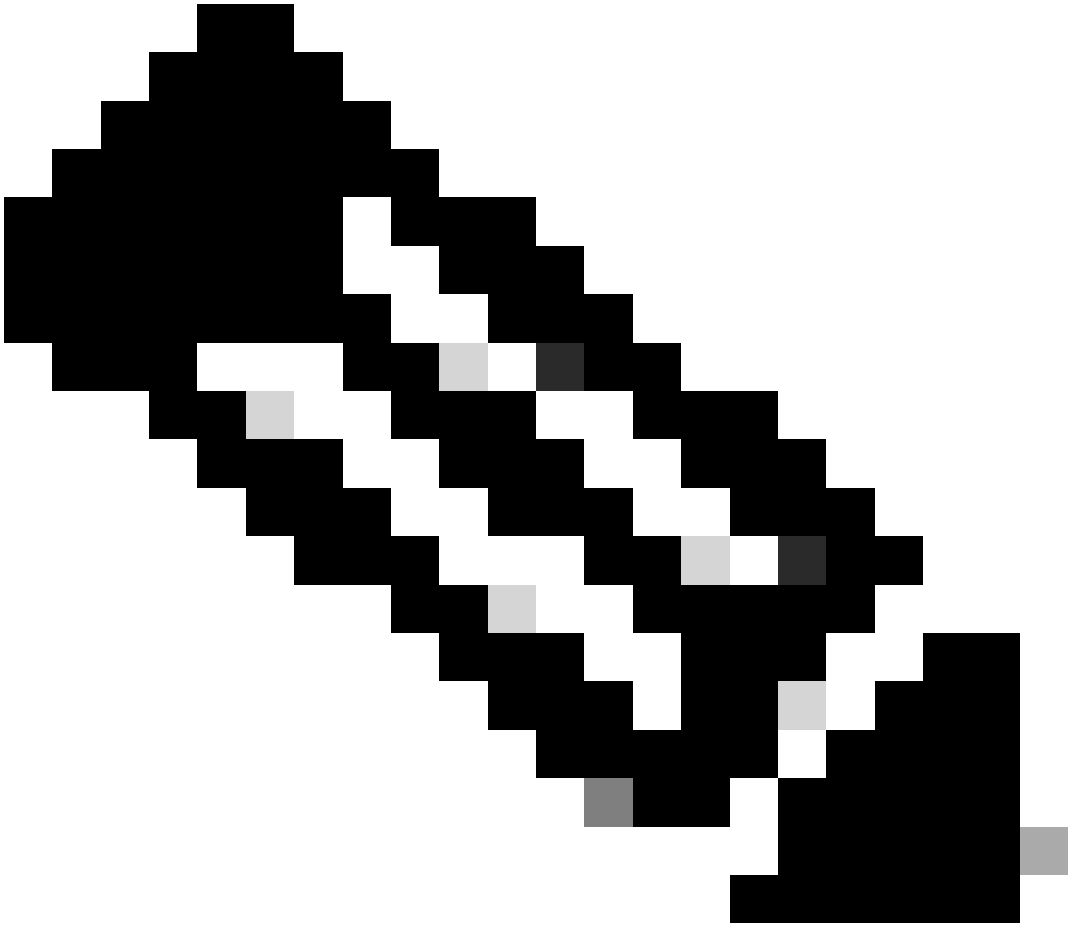
确认私钥未受密码短语保护

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

如果私钥不需要密码，则不请求密码。

```
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：可以在安装证书之前执行这些验证。

以管理员用户身份登录到CTB管理器。

使用sudo cat server_cert.pem 命令查看server_cert.pem文件内容。根据您的证书文件名调整命令。

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

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

使用sudo cat server_key.pem命令查看server_key.pem文件。根据您的私钥文件名调整命令。

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

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

自签证书

生成自签名证书

- 以安装过程中配置的用户身份通过SSH (Secure Shell)登录到CTB管理器，该用户通常为“admin”用户。

- 发出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} 命令。

  - 使用您选择的私钥长度（例如2048、4096或8192）更改rsa:{key_len}

    - 使用CTB管理器节点的IP更改{ctb_manager_ip}

```
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:~$
```

- 使用cat server_cert.pem命令查看server_cert.pem文件，然后将内容复制到您的缓冲区中，以便可以将其粘贴到本地工作站所选的文本编辑器中。保存文件。您也可以将这些文件从目 /home/admin 录中SCP出来。

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

- 使用sudo cat server_key.pem命令查看server_key.pem文件，并将内容复制到您的缓冲区中，以便可以将其粘贴到本地工作站所选的文本编辑器中。保存文件。您也可以将此文件从目 /home/admin 录中SCP出来。

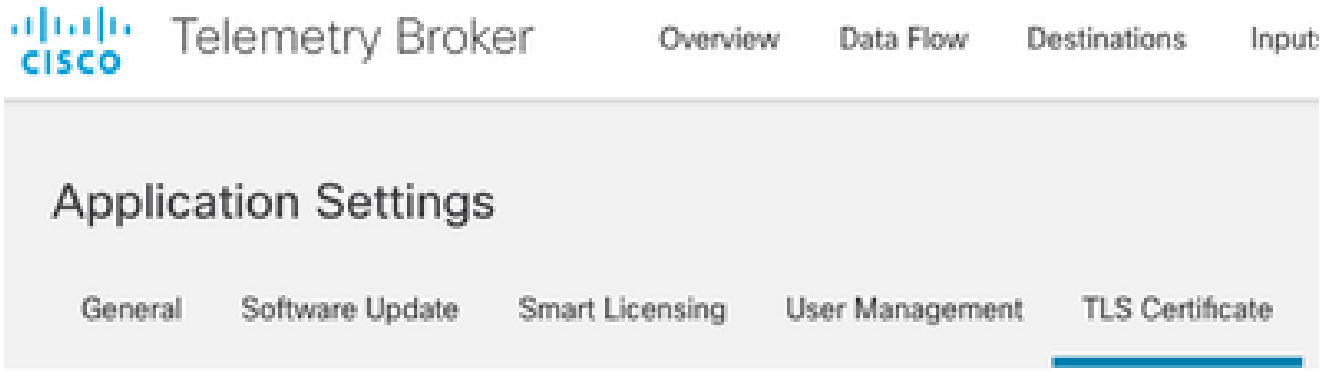
```
admin@ctb-manager:~$ sudo cat server_key.pem
-----BEGIN PRIVATE KEY-----
{removed_for_brevity}
-----END PRIVATE KEY-----
admin@ctb-manager:~$
```

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”。

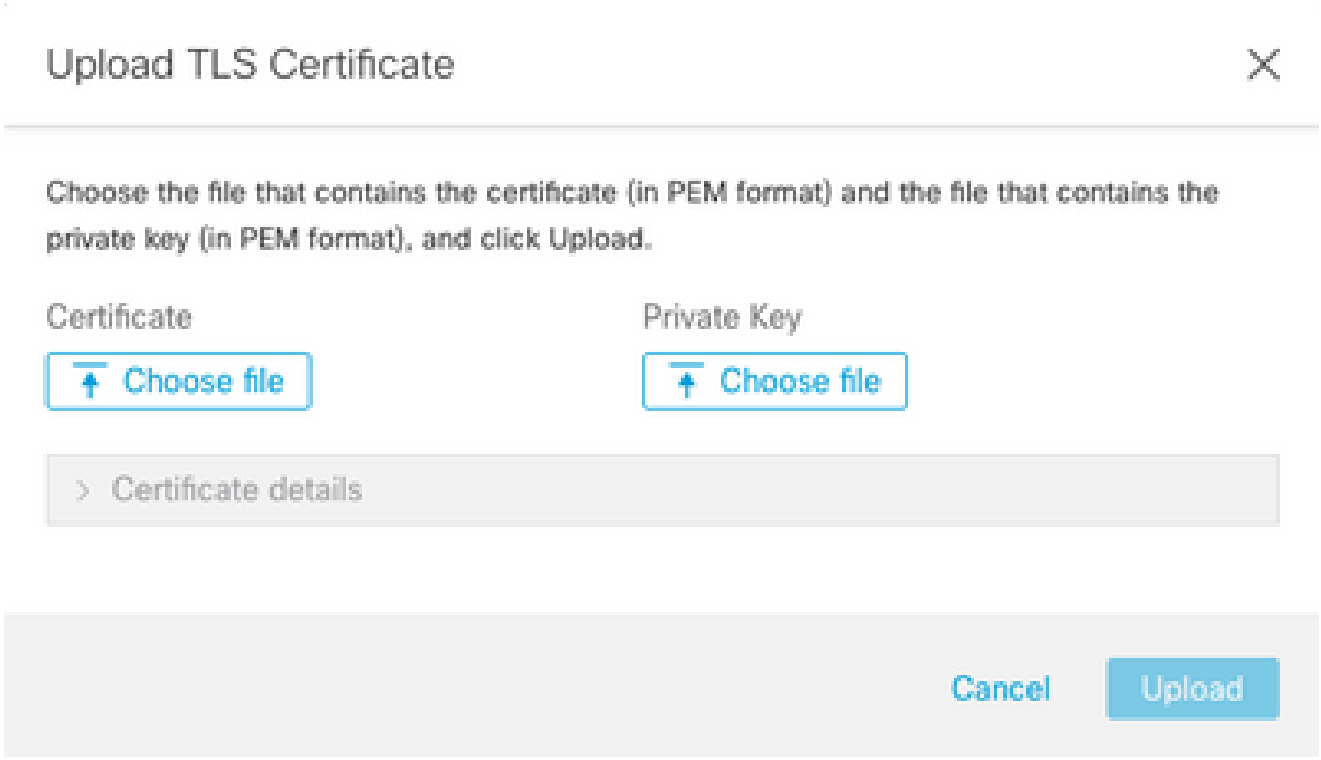
*CTB*设置图标

- 导航到“TLS证书”(TLS Certificate)选项卡。

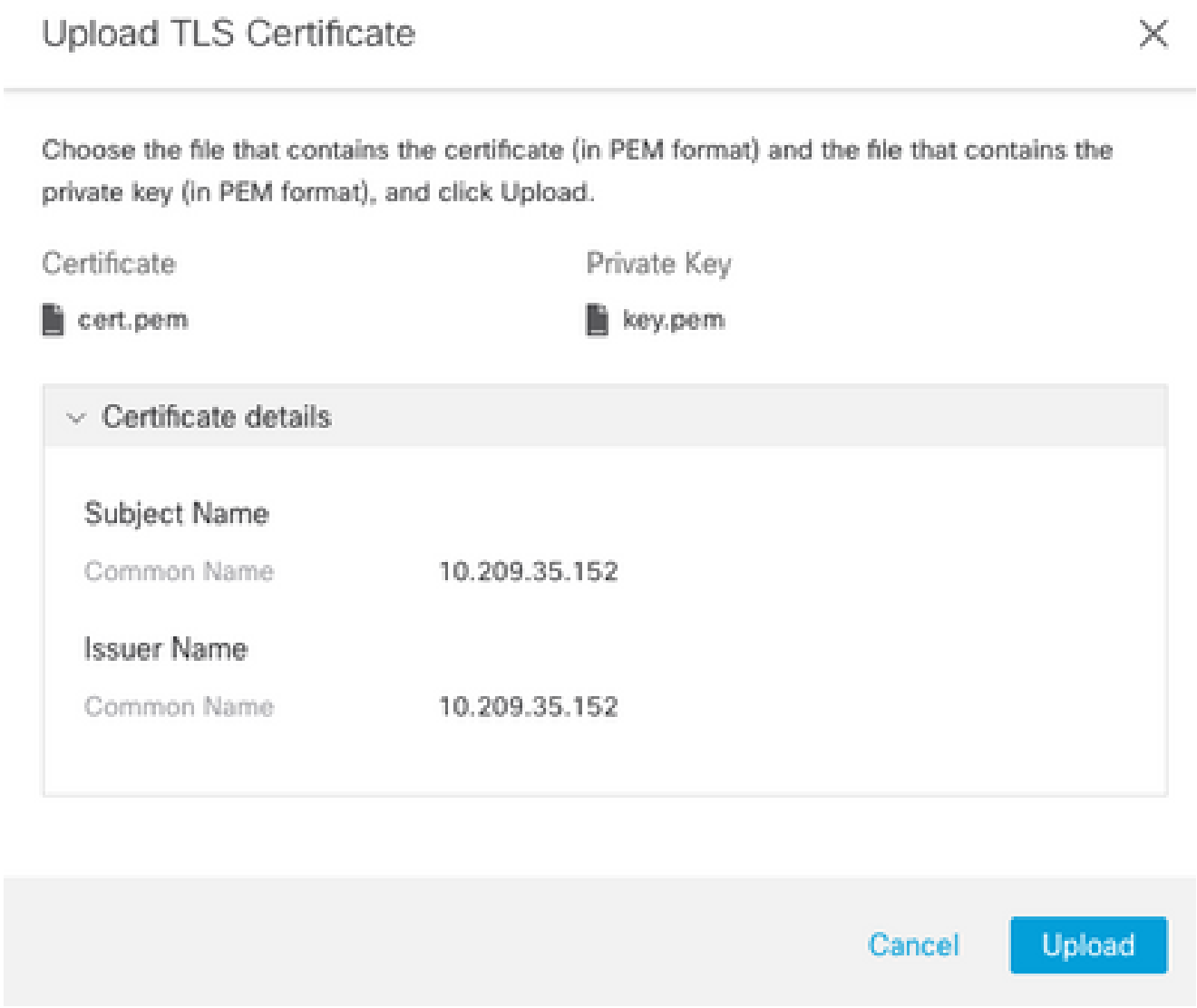


*CTB*证书选项卡

- 选择Upload TLS Certificate ，然后在“上传TLS证书”对话框中选择证书和私钥的server_cert.pem 和server_key.pem 。选择文件后，选择上传。



- 选择文件后，验证过程将确认证书和密钥组合，并显示颁发者和主题的公用名称，如下所示。



*CTB*证书上传

- 选择“上传”按钮以上传新证书。Web UI会在几分钟内自行重新启动，重新启动后会再次登录设备。

- 登录到CTB Manager节点Web控制台并导航到Settings > TLS Certificate 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管理器节点有新的身份证书，每个CTB代理节点必须手动更新。

1. 通过ssh登录每个代理节点并运行sudo ctb-manage 命令

```
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:
```

- 出现提示时c请选择选项。

```
== 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
```

- 验证证书详细信息（如果它们与签名证书的值匹配），并选择 **y** 以接受证书。服务自动启动，启动服务后返回提示。服务启动最多可能需要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

生成证书颁发机构颁发的证书签名请求(CSR)

- 以安装过程中配置的用户身份通过SSH (Secure Shell)登录到CTB管理器，该用户通常为“admin”用户。

- 发出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命令。如果需要，可将最后两行的“额外”属性留空。

  - 更改{ctb_manager_dns_name} 为CTB管理器节点的DNS名称

    - 使用CTB管理器节点的IP更改{ctb_manager_ip}

    - 使用您选择的私钥长度（例如2048、4096或8192）更改{key_len}。

```
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 []:
```

- 将CSR和密钥文件scp到本地计算机，并向CA提供CSR。CA颁发PEM格式的CSR不在本文档的讨论范围之内。

创建带链的证书

CA以PEM格式颁发服务器身份证书。必须创建包含CTB管理器节点的所有链证书和服务器身份证书的链文件。

在文本编辑器中，通过合并上一步中签名的证书并按照所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 – {Issui
```

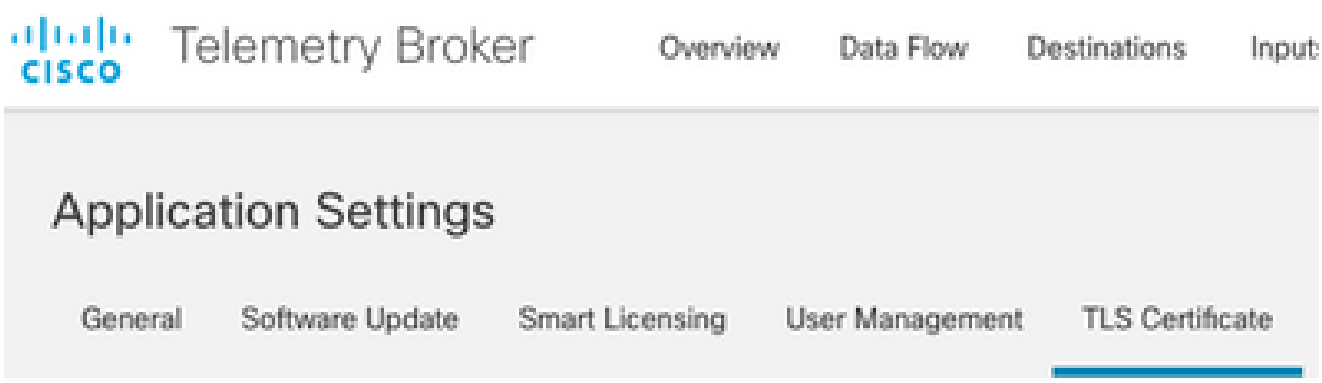
确保此包含链文件的新证书文件没有前导空格或尾随空格、空行，并且顺序如上所示。

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”。

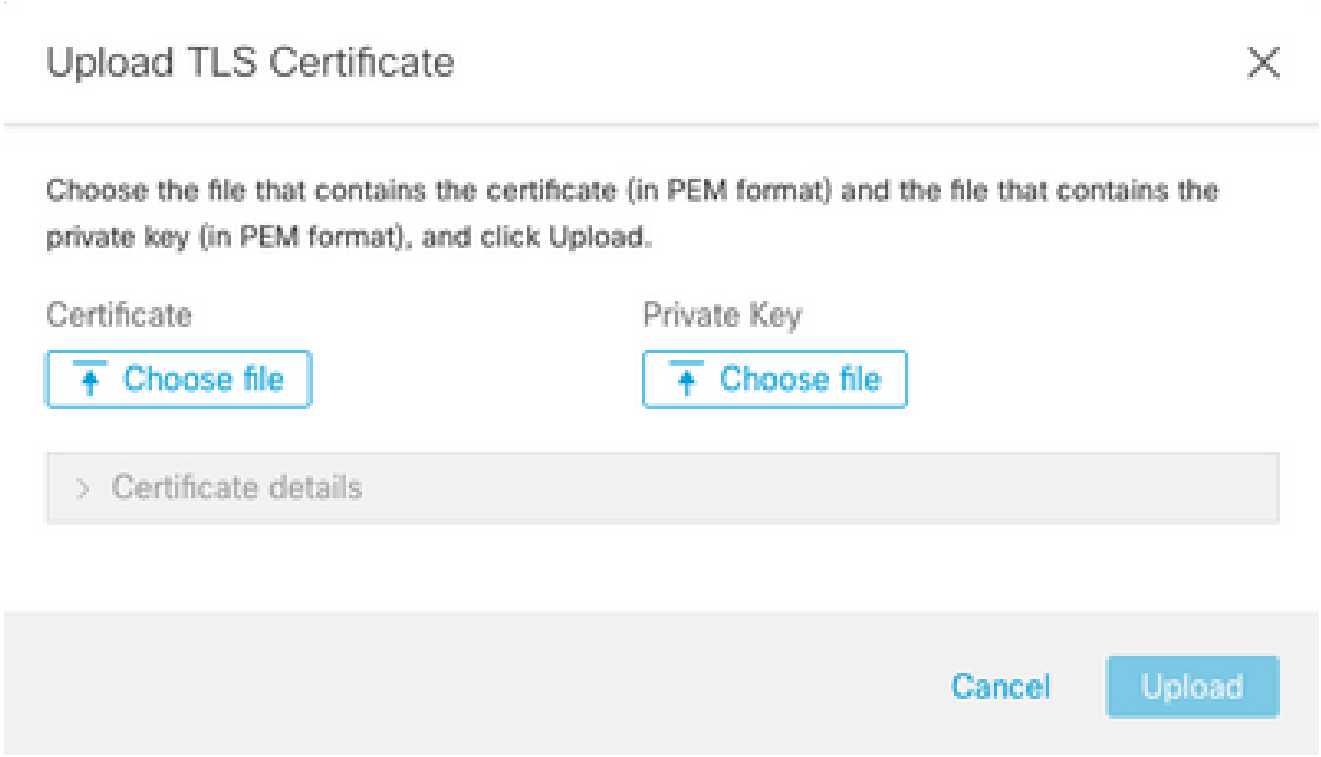
*CTB*设置图标

- 导航到“TLS证书”(TLS Certificate)选项卡。

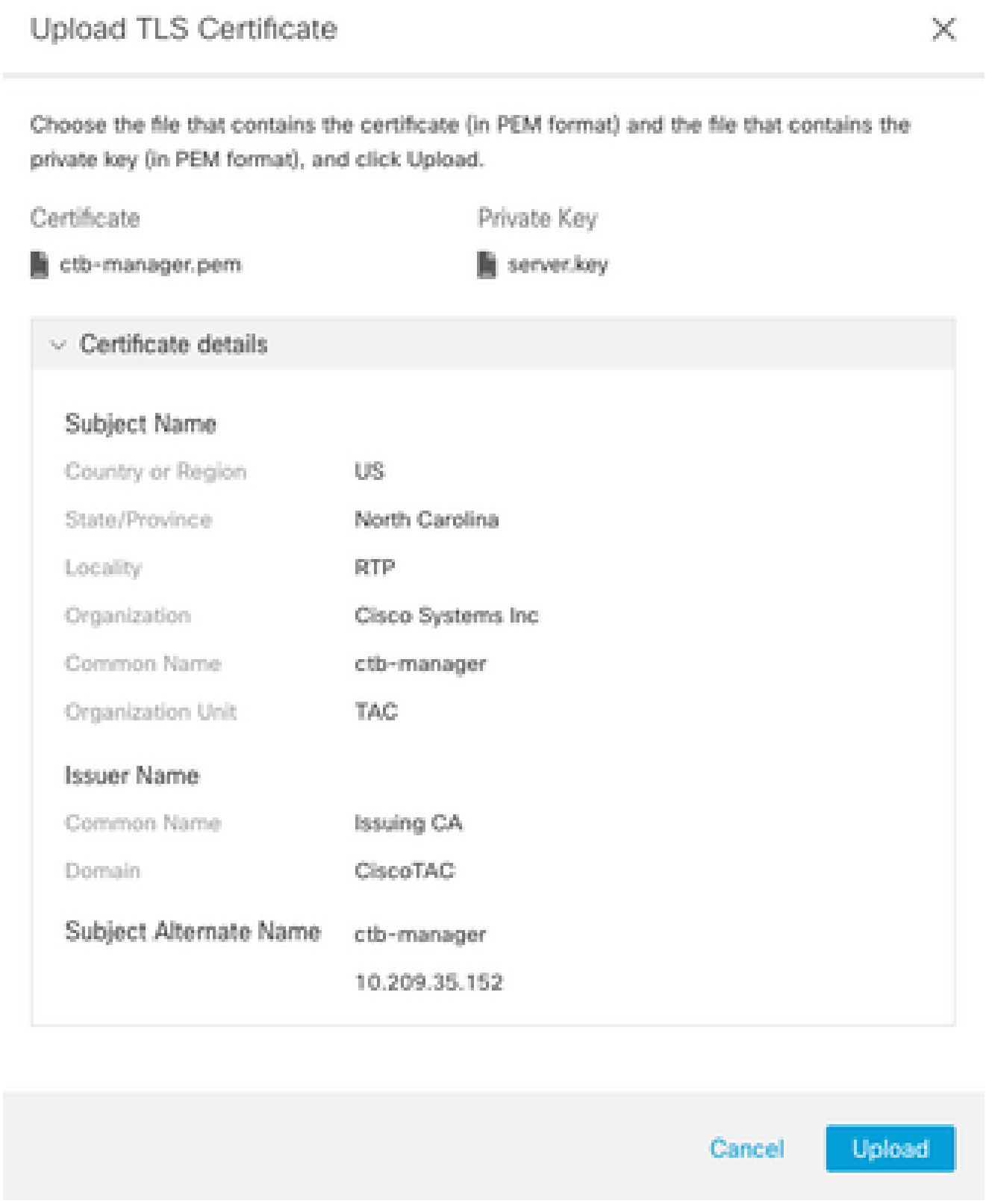


*CTB*证书选项卡

- 选择Upload TLS Certificate 然后选择在上一节中创建的具有链文件的证书，并在“上传TLS证书”对话框中 server_key.pem 分别为证书和私钥生成的CTB管理器。选择文件后，选择上传。



- 选择文件后，验证过程将确认证书和密钥组合，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

- 选择“上传”按钮以上传新证书。Web UI将在约60秒内自行重新启动，并在重新启动后登录到Web UI。

- 登录到CTB Manager节点Web控制台并导航到Settings > TLS Certificate 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管理器节点有新的身份证书，每个CTB代理节点必须手动更新。

1. 通过ssh登录每个代理节点并运行sudo ctb-manage 命令

```
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:
```

- 出现提示时c请选择选项。

```
== 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
```

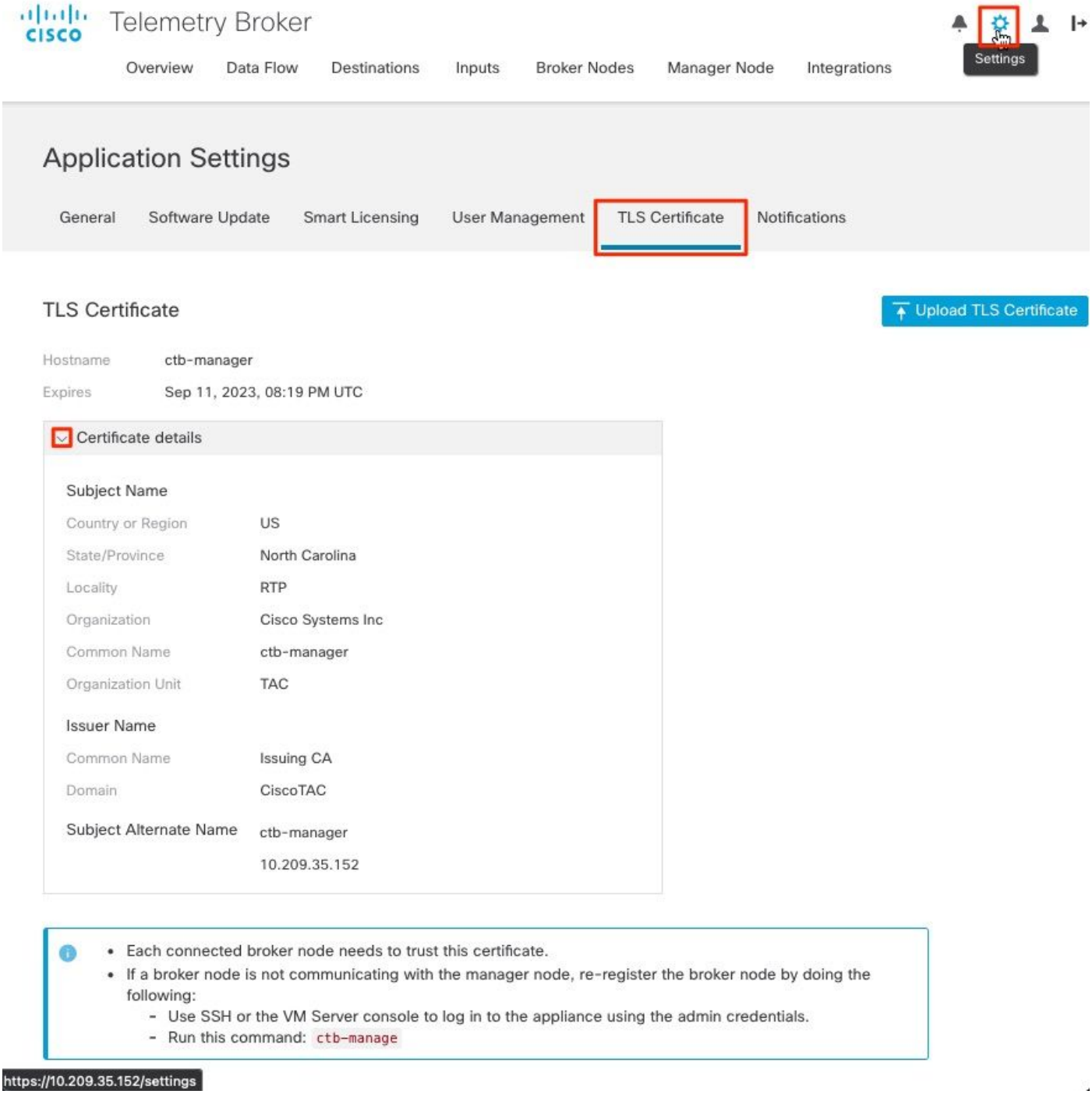
- 验证证书详细信息（如果它们与签名证书的值匹配），并选择y以接受证书。服务将自动启动，一旦启动服务，将返回提示。服务启动最多可能需要15分钟才能完成。

```
== 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 Manager节点Web控制台并导航到Settings > TLS Certificate 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（例如缺少链证书），则CTB代理节点无法与管理器节点通信，并在代理节点列表的Status列中显示“Not Seen Since”。
Broker节点将继续复制和分发此状态的流量。

登录到CTB Manager节点CLI并发出sudo grep -ic begin /var/lib/titan/titanium_frontend/ssl/cert.pem 命令，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
```

返回的输出值需要等于链中的CA设备数加上CTB管理器。

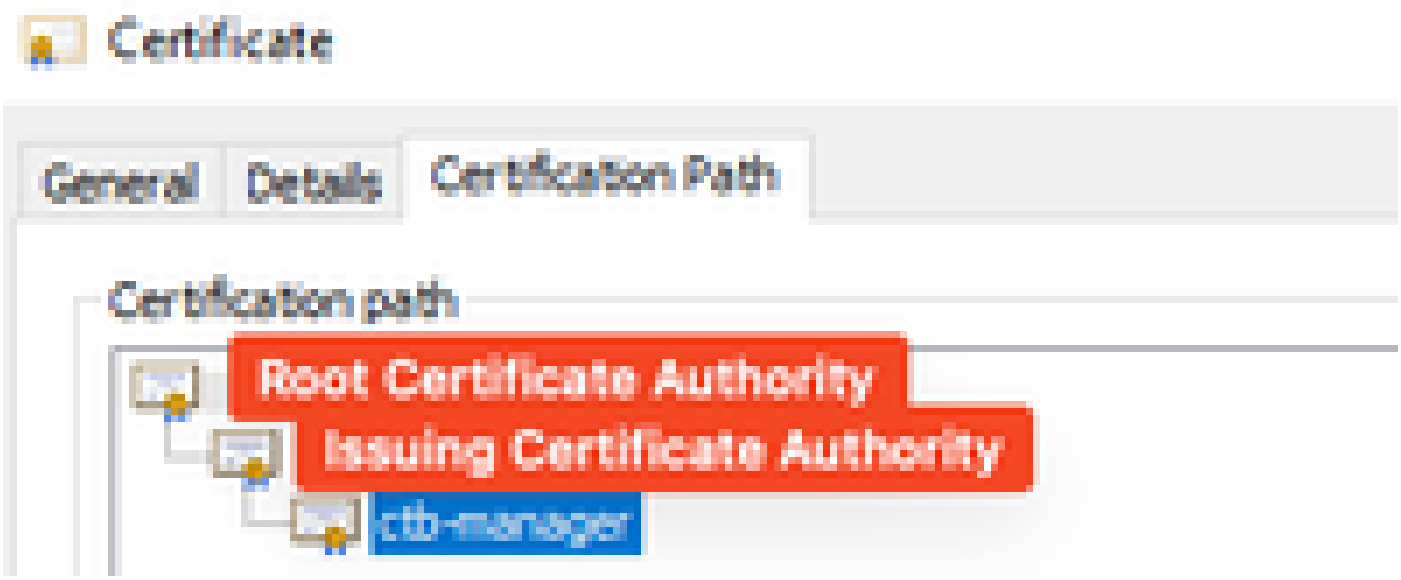
如果使用自签名证书，则应为1的输出。

如果PKI基础设施由也作为颁发CA的单个根CA组成，则预期输出2。

如果PKI基础设施包含一个根CA和一个发出CA，则预期输出3。

如果PKI基础设施包含一个根CA、一个从属CA和一个发出CA，则预期输出4。

将输出与在其他应用(如 Microsoft Windows Crypto Shell Extensions)中查看证书时列出的PKI进行比较。



*PKI*基础设施

在此图中，PKI基础设施包括一个根CA和发出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，以确定证书是否缺失。

在中查看证书时，Microsoft Windows Crypto Shell Extensions 如果本地计算机没有足够的信息来验证证书，则可能并非所有证书都会显示。

从CLI发出sudo ctb-mayday 命令，生成Mayday捆绑包，供TAC审阅。

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）。