テレメトリブローカーID証明書の置き換え

内容

はじめに

このドキュメントでは、Cisco Telemetry Broker(CTB)Managerノードでサーバ ID証明書(SID)を置き換える方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco Telemetry Brokerアプライアンス管理
- x509証明書

使用するコンポーネント

このドキュメントで使用するアプライアンスは、バージョン2.0.1を実行しています

- Cisco Telemetry Broker Managerノード
- Cisco Telemetry Brokerブローカーノード

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

設定

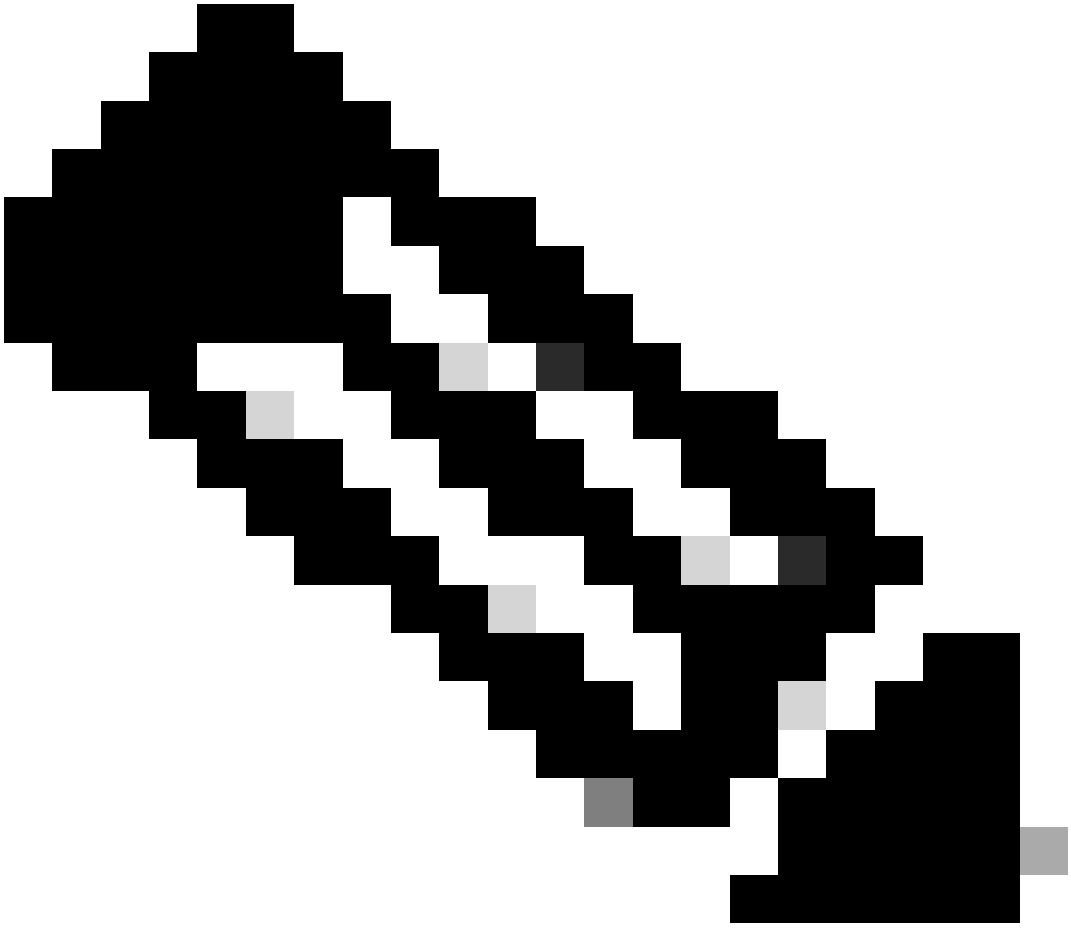
証明書の要件

Cisco Telemetry Broker Managerが使用するx509証明書は、次の要件を満たす必要があります。

- 証明書と秘密キーは一致するペアでなければなりません
- 証明書と秘密キーはPEMでエンコードする必要があります
- 秘密キーはパスフレーズで保護できません

証明書と秘密キーがペアで一致していることを確認します

CTB Managerコマンドラインインターフェイス(CLI)にadminユーザとしてログインします。



注：このセクションで説明するファイルがシステム上にまだ存在していない可能性があります。

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

---

コマンドは、証明書署名要求(CSR)ファイルの公開キーのSHA-256チェックサムを出力します。

sudo openssl pkey -in server_key.pem -pubout -outform pem | sha256sumコマンドは、秘密キーファイルから公開キーのSHA-256チェックサムを出力します。

sudo openssl x509 -in server_cert.pem -pubkey -noout -outform pem | sha256sumコマンドは、発行された証明書ファイルの公開キーのSHA-256チェックサムを出力します。

証明書と秘密キーの出力が一致している必要があります。証明書署名要求(CSR)が使用されていない場合、server_cert.pemファイルは存在しません。

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

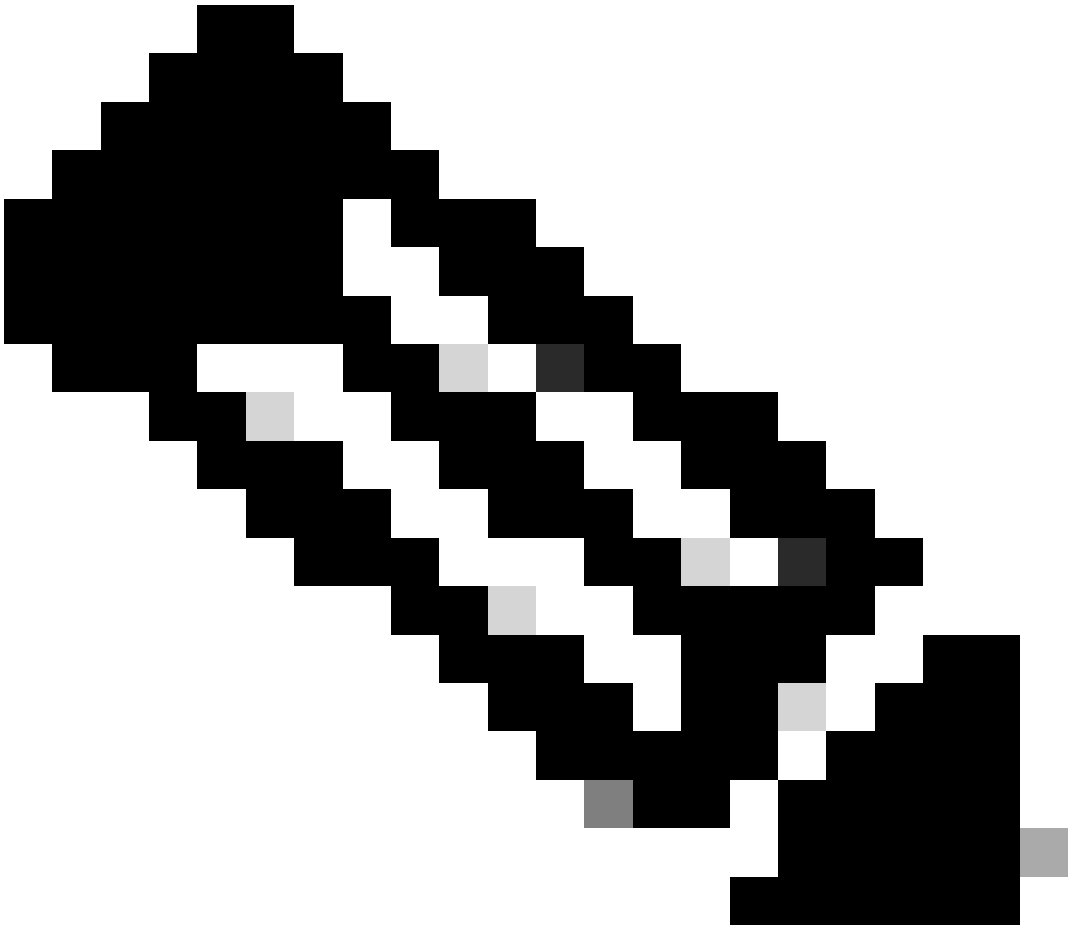
秘密キーがパスフレーズで保護されていないことを確認します

管理ユーザとしてCTB Managerにログインします。ssh-keygen -yf server_key.pemコマンドを実行します。

秘密鍵が不要な場合、パスフレーズは要求されません。

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

証明書と秘密キーがPEMでエンコードされていることの確認



注：これらの検証は、証明書をインストールする前に実行できます。

管理ユーザとしてCTB Managerにログインします。

sudo cat server_cert.pem コマンドを使用して、server_cert.pemファイルの内容を表示します。証明書ファイル名に合わせてコマンドを調整します。

ファイルの最初の行は -----**BEGIN CERTIFICATE**----- 、最後の行は-----END CERTIFICATE-----にする必要があります。

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

sudo cat server_key.pemコマンドを使用して、server_key.pemファイルを表示します。秘密キーのファイル名に合わせてコマンドを調整します。

ファイルの最初の行は -----**BEGIN PRIVATE KEY**----- 、最後の行は-----END PRIVATE KEY-----にする必要があります。

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

自己署名証明書

自己署名証明書の生成

- インストール時に設定したユーザとして、SSH（セキュアシェル）を介してCTBマネージャにログインします。通常は「admin」ユーザです。

- 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} コマンドを発行します。

  - 2048、4096、8192など、選択した秘密キーの長さでrsa:{key_len}を変更します

  - CTBマネージャノードのIPを使用した{ctb_manager_ip}の変更

```
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:~$
```

- cat server_cert.pemコマンドでserver_cert.pemファイルを表示し、内容をバッファにコピーして、ローカルワークステーションに任意のテキストエディタで貼り付けられるようにします。ファイルを保存します。これらのファイルは、デ /home/admin ィレクトリからSCPでダウンロードすることもできます。

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

- sudo cat server_key.pemコマンドでserver_key.pemファイルを表示し、内容をバッファにコピーして、選択したテキストエディタでローカルワークステーションに貼り付けられるようにします。ファイルを保存します。また、このファイルをデ /home/admin ィレクトリからSCP送信することもできます。

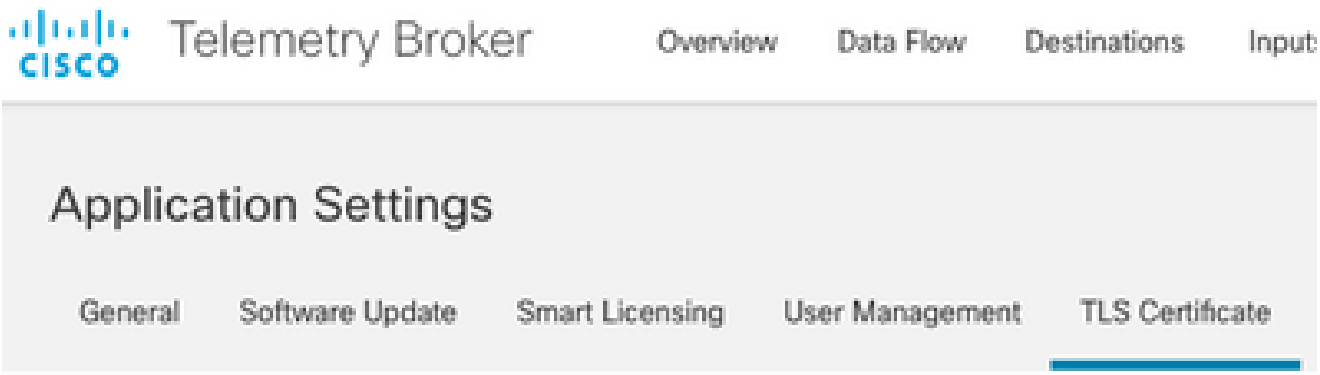
```
admin@ctb-manager:~$ sudo cat server_key.pem
-----BEGIN PRIVATE KEY-----
{removed_for_brevity}
-----END PRIVATE KEY-----
admin@ctb-manager:~$
```

自己署名証明書のアップロード

1. CTB Manager Web UIに移動し、管理者ユーザとしてログインし、歯車アイコンをクリックして「Settings」にアクセスします。

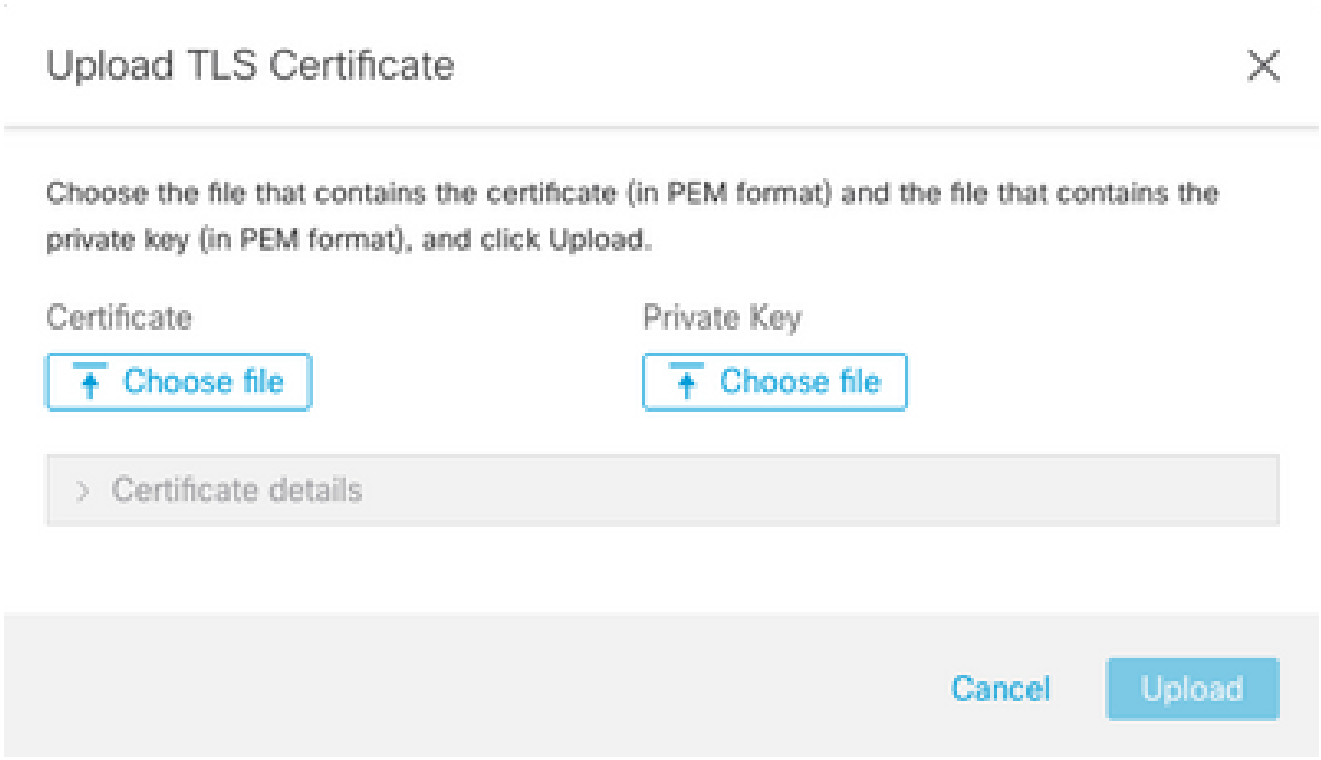
*CTB*設定アイコン

- 「TLS証明書」タブに移動します。

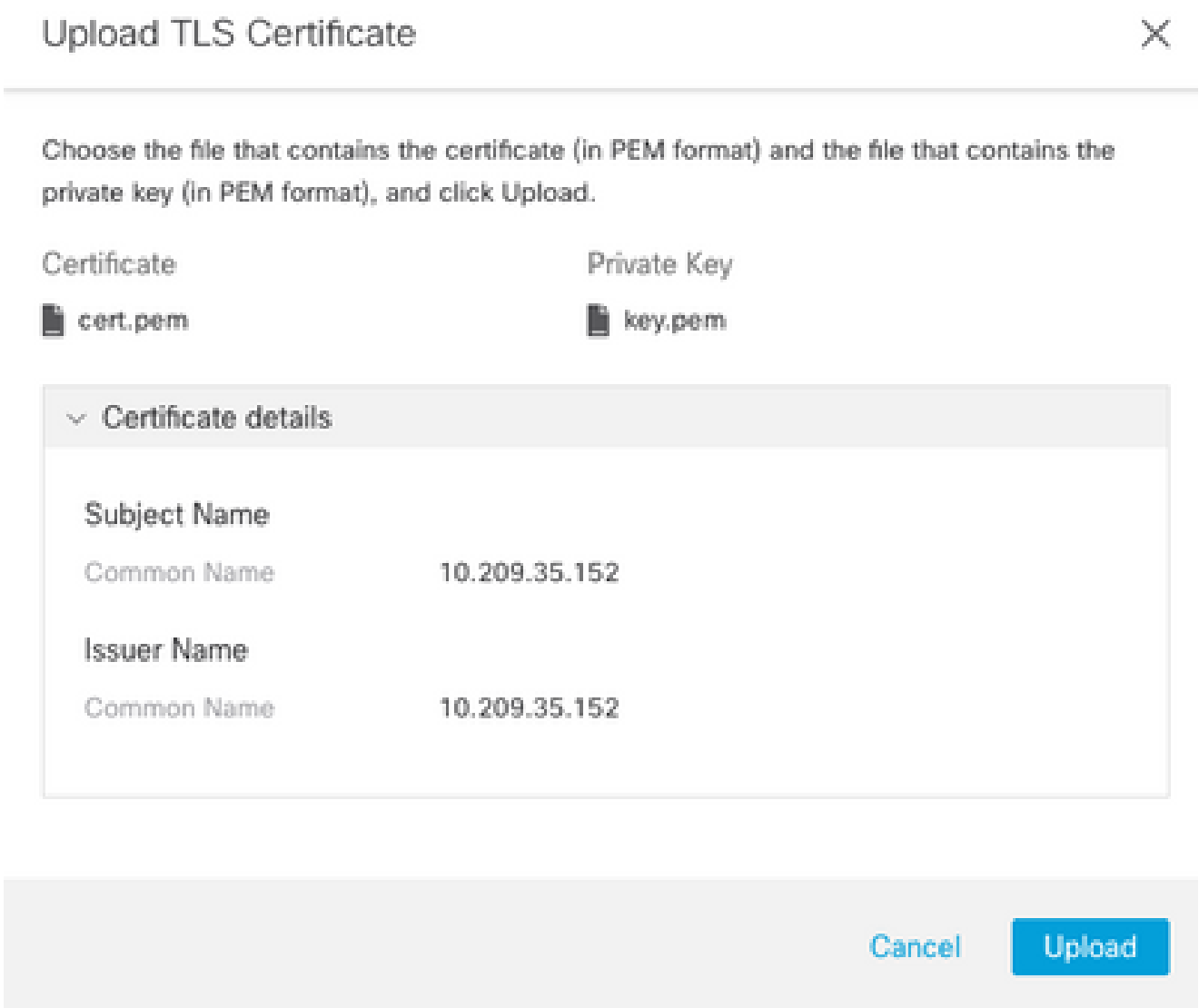


*CTB Certificates*タブ

- Upload TLS CertificateダUpload TLS Certificate イアログボックスで、CertificateとPrivate Keyにそれぞれserver_cert.pem と server_key.pem を選択します。ファイルを選択したら、Uploadを選択します。



- ファイルが選択されると、検証プロセスによって証明書とキーの組み合わせが確認され、図のように発行者とサブジェクトの共通名が表示されます。



*CTB*証明書のアップロード

- 「アップロード」ボタンを選択して、新しい証明書をアップロードします。Web UIが数分後に自動的に再起動し、再起動後にデバイスに再度ログインします。

- CTBマネージャノードのWebコンソールにログインし、Settings > TLS Certificate に移動して、新しい有効期限などの証明書の詳細を表示するか、ブラウザを使用してシリアル番号などの詳細な情報を表示します。

ブローカーノードの更新

CTB Managerノードに新しいID証明書が追加されたら、各CTB Brokerノードを手動で更新する必要があります。

1. ssh経由で各ブローカノードにログインし、sudo ctb-manage コマンドを実行します。

```
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:
```

- プロンプトが表示されcたら、オプションを選択します。

```
== 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
```

- 証明書の詳細が署名付き証明書の値と一致するかどうかを確認し、証明書の受け入れを選択し **y** ます。サービスが自動的に開始し、サービスが開始されると、プロンプトが返されます。サービスの開始が完了するまでに最大15分かかることがあります。

```
== 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
```

認証局(CA)が発行した証明書

証明機関による発行のための証明書署名要求(CSR)の生成

- インストール時に設定したユーザとして、SSH（セキュアシェル）を介してCTBマネージャにログインします。通常は「admin」ユーザです。

- 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コマンドを発行します。最後の2行の「extra」属性は、必要に応じて空白にしておくことができます。
{ctb_manager_dns_name}

  - を、CTBマネージャノードのDNS名に変更します

  - CTBマネージャノードのIPを使用した{ctb_manager_ip}の変更

    - 2048、4096、8192など、選択した秘密キーの長さで{key_len} を変更します。

```
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 []:
```

- CSRとキーファイルをローカルマシンにSCPし、CAにCSRを提供します。PEM形式でのCAによるCSRの発行は、このドキュメントの対象範囲外です。

チェーンを使用した証明書の作成

CAは、PEM形式でサーバID証明書を発行します。CTB Managerノードのすべてのチェーン証明書とサーバID証明書を含むチェーンファイルを作成する必要があります。

テキストエディタで、前の手順で署名した証明書を組み合わせ、信頼できるCAを含むチェーン内のすべての証明書を示されている順序で単一のPEM形式のファイルに追加して、ファイルを作成します。

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

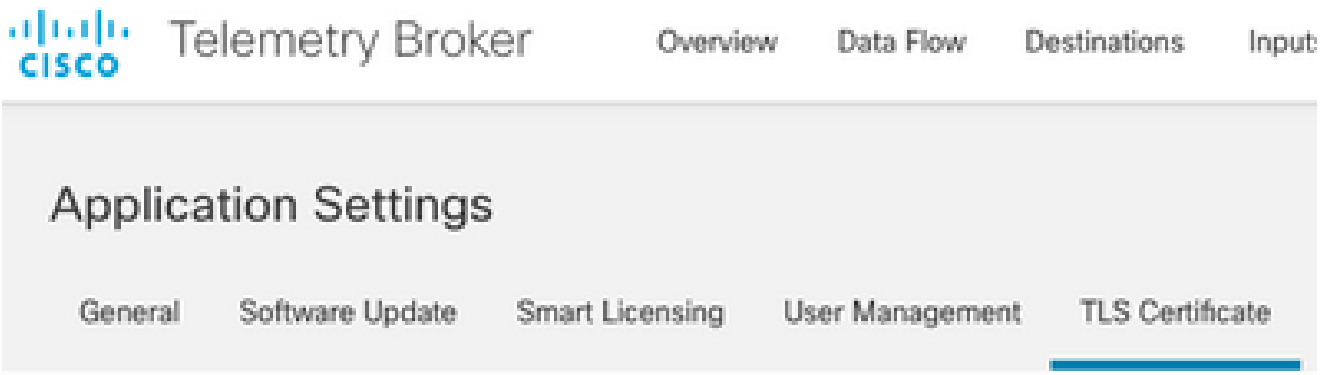
この新しい証明書ファイルとチェーンファイルの先頭または末尾にスペースと空白行が含まれていないこと、および証明書ファイルが上記の順序になっていることを確認します。

認証局が発行した証明書のアップロード

1. CTB Manager Web UIに移動し、adminとしてログインし、歯車アイコンをクリックして「Settings」にアクセスします。

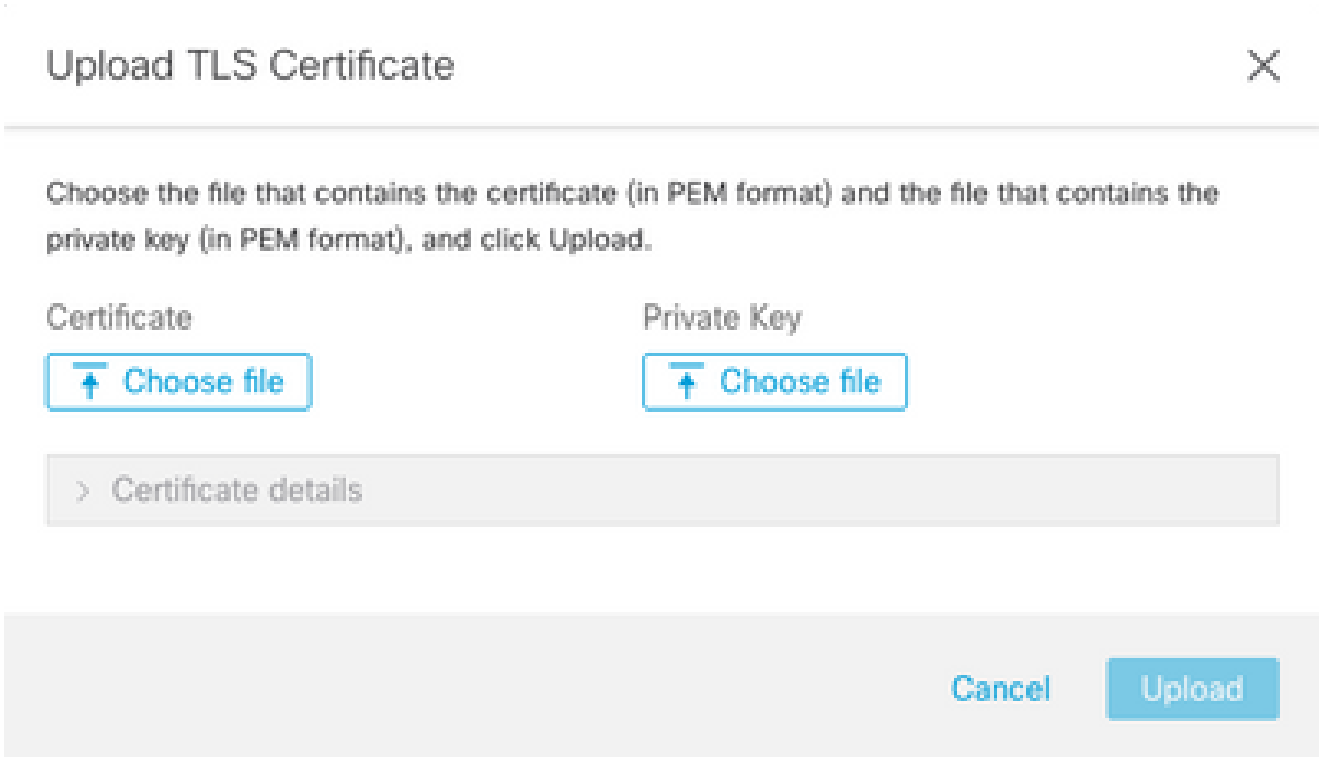
*CTB*設定アイコン

- 「TLS証明書」タブに移動します。

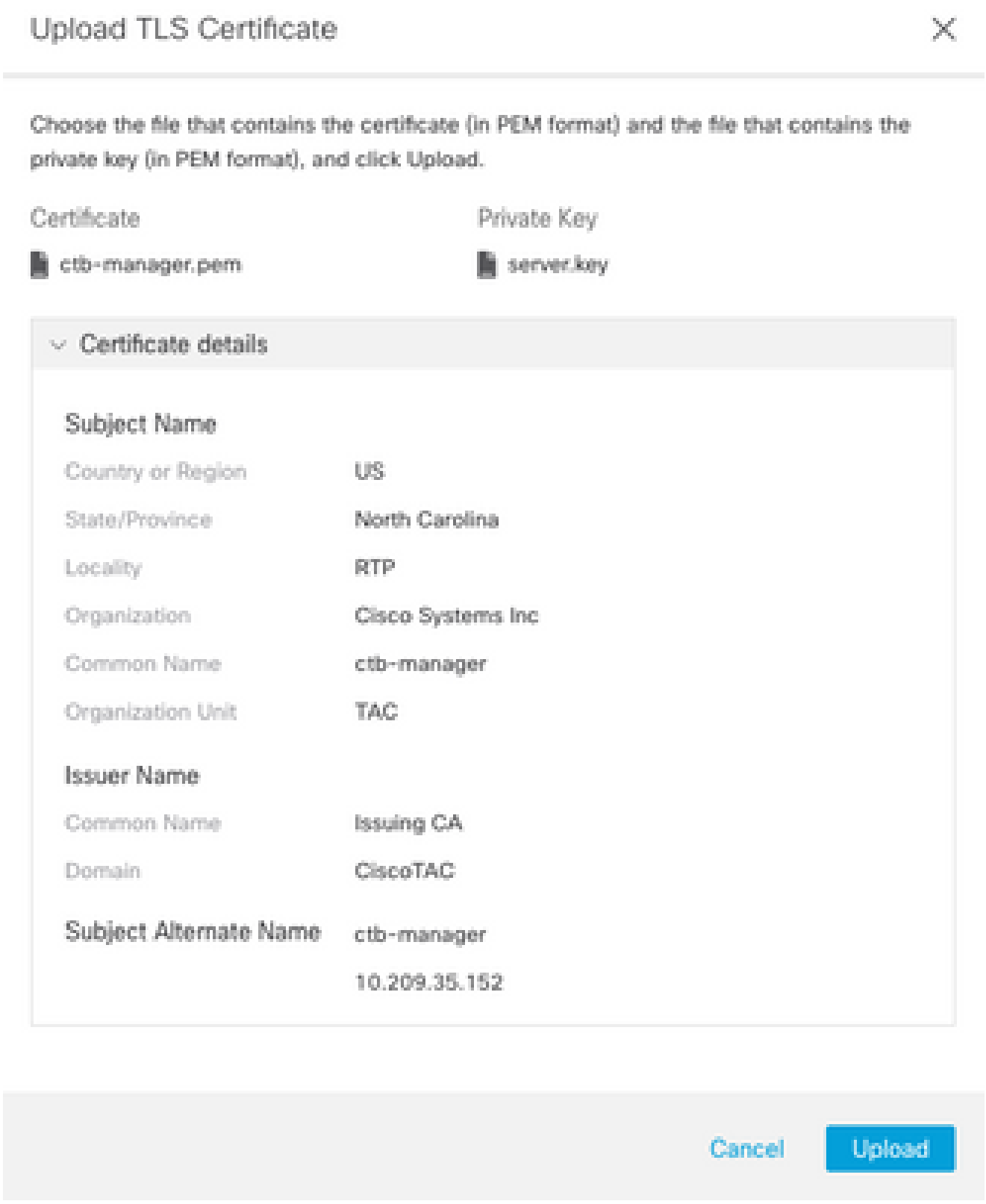


*CTB Certificates*タブ

- を選択Upload TLS Certificate し、最後のセクションで作成したチェーンファイルを使用して証明書を選択し、「TLS証明書のアップロード」ダイアログボックス server_key.pem で証明書と秘密キーに対して生成したCTBマネージャをそれぞれ選択します。ファイルを選択したら、Uploadを選択します。



- ファイルが選択されると、検証プロセスによって証明書とキーの組み合わせが確認され、次に示すように発行者とサブジェクトの共通名が表示されます。



*CTB CA*発行の証明書検証

- 「アップロード」ボタンを選択して、新しい証明書をアップロードします。Web UIは約60秒で自動的に再起動し、再起動後にWeb UIにログインします。

- CTBマネージャノードのWebコンソールにログインし、Settings > TLS Certificate に移動して、新しい有効期限などの証

明書の詳細を表示するか、ブラウザを使用してシリアル番号などの詳細な情報を表示します。

ブローカーノードの更新

CTB Managerノードに新しいID証明書が追加されたら、各CTB Brokerノードを手動で更新する必要があります。

1. ssh経由で各ブローカノードにログインし、sudo ctb-manage コマンドを実行します。

```
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:
```

- プロンプトが表示されcたら、オプションを選択します。

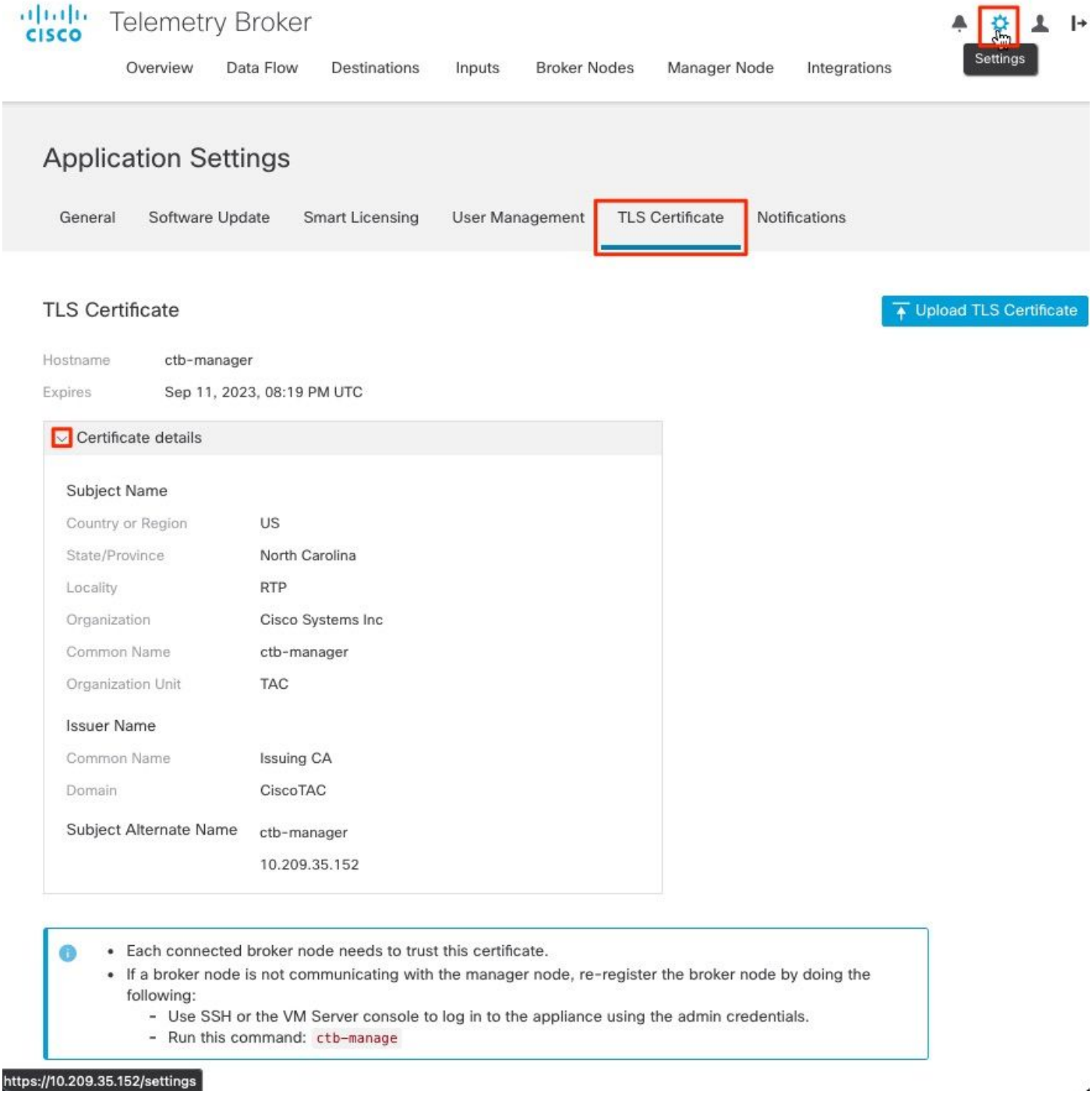
```
== Management Configuration

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
```

- 証明書の詳細が署名付き証明書の値と一致するかどうかを確認し、yを選択して証明書を受け入れます。サービスは自動的に開始し、サービスが開始されるとプロンプトが返されます。サービスの開始が完了するまでに最大15分かかることがあります。

```
== 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
```

確認

CTBマネージャノードのWebコンソールにログインし、Settings > TLS Certificate に移動して、新しい有効期限などの証明書の詳細を表示するか、ブラウザを使用してシリアル番号などの詳細な情報を表示します。



*CTB*証明書の詳細

CTBマネージャノードのWeb UIで、CTBブローカノードにアラームが表示されていないことを確認します。

トラブルシュート

チェーン証明書がないなど、証明書が不完全な場合、CTBブローカノードノードはマネージャノードと通信できず、ブローカノードリストの「Status」列に「Not Seen Since」と表示されます。
ブローカノードは、この状態のトラフィックの複製と分散を継続します。

CTBマネージャノードCLIにログインし、sudo grep -ic begin /var/lib/titan/titanium_frontend/ssl/cert.pem コマンドを発行してcert.pemファイル内の証明書の数を確認します。

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

返される出力値は、チェーン内のCAデバイスの数にCTB Managerを加えた数と同じである必要があります。

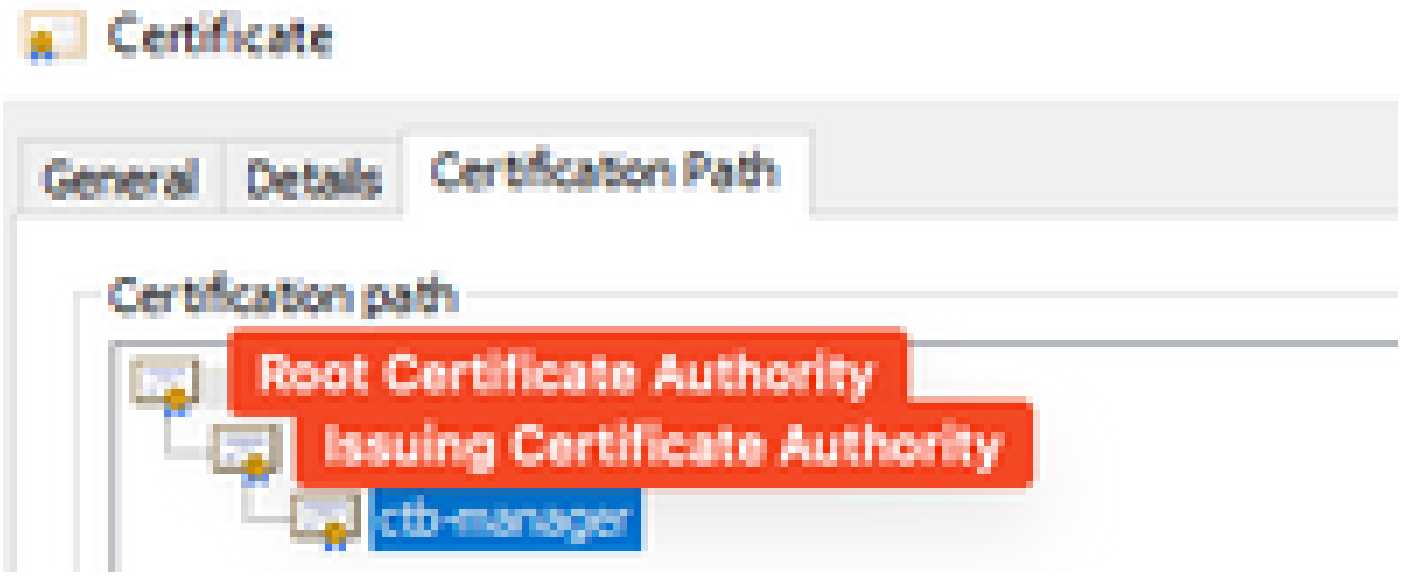
自己署名証明書を使用している場合は、1の出力が予期されます。

PKIインフラストラクチャが、発行側CAでもある単一のルートCAで構成されている場合、2の出力が予想されます。

PKIインフラストラクチャがルートCAと発行側CAで構成されている場合、3の出力が予想されます。

PKIインフラストラクチャがルートCA、下位CA、および発行側CAで構成されている場合は、4の出力が予想されます。

Microsoft Windows Crypto Shell Extensionsなどの別のアプリケーションで証明書を表示する際にリストされるPKIと出力を比較してください。



PKI インフラストラクチャ

次の図では、PKIインフラストラクチャにルートCAと発行側CAが含まれています。

このシナリオでは、コマンドの出力値は3になると想定されています。

出力が期待した結果にならない場合は、「**チェーンによる証明書の作成**」セクションの手順を確認して、証明書が失われたかどうかを確認します。

Microsoft Windows Crypto Shell Extensions の証明書を表示する際、ローカルマシンに証明書を確認するための十分な情報がないと、一部の証明書が表示されないことがあります。

CLIからsudo ctb-mayday コマンドを発行して、TACが確認できるようにメイデイバンドルを生成します。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。