Remplacer le certificat d'identité du courtier de télémétrie

Table des matières

Introduction

Ce document décrit comment remplacer le certificat d'identité de serveur sur le noeud de gestionnaire du courtier de télémétrie Cisco (CTB).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Administration de l'appliance Cisco Telemetry Broker
- Certificats X509

Composants utilisés

Les appliances utilisées pour ce document exécutent la version 2.0.1

- Noeud Cisco Telemetry Broker Manager
- Noeud Broker de télémétrie Cisco

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Configurer

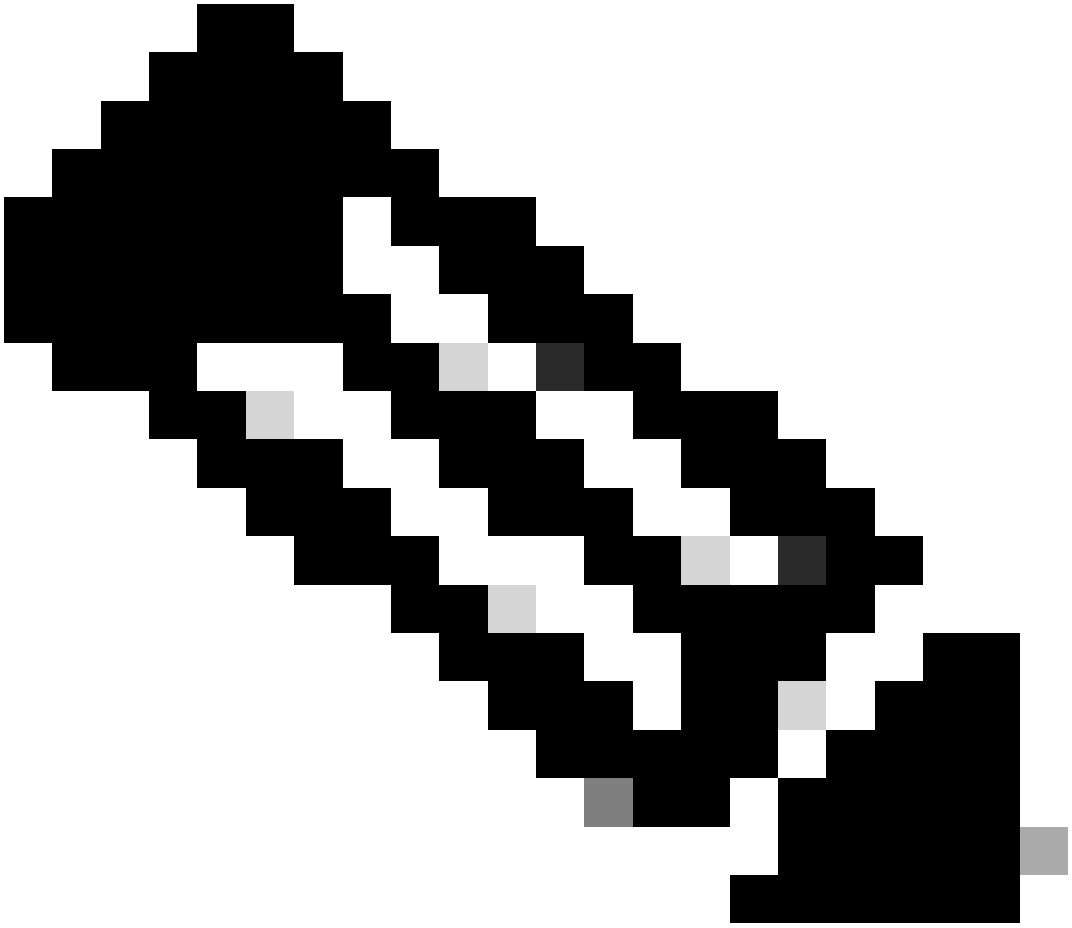
Exigences du certificat

Le certificat x509 utilisé par Cisco Telemetry Broker Manager doit répondre aux exigences suivantes :

- Les clés privée et de certification doivent correspondre
- Le certificat et la clé privée doivent être codés en PEM
- La clé privée ne doit pas être protégée par une phrase de passe

Confirmer que le certificat et la clé privée correspondent

Connectez-vous à l'interface de ligne de commande (CLI) de CTB Manager en tant qu'utilisateur admin.



Remarque : il est possible que les fichiers mentionnés dans cette section n'existent pas encore sur le système.

La sudo openssl req -in server.csr -pubkey -noout -outform pem | sha256sum commande génère la somme de contrôle SHA-256 de la clé publique à partir du fichier de demande de signature de certificat.

La sudo openssl pkey -in server_key.pem -pubout -outform pem | sha256sumcommande génère la somme de contrôle SHA-256 de la clé publique à partir du fichier de clé privée.

La sudo openssl x509 -in server_cert.pem -pubkey -noout -outform pem | sha256sumcommande génère la somme de contrôle SHA-256 de la clé publique à partir du fichier de certificat émis.

Le résultat du certificat et de la clé privée doit correspondre. Si aucune demande de signature de certificat n'a été utilisée, le fichier server_cert.pem n'existe pas.

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

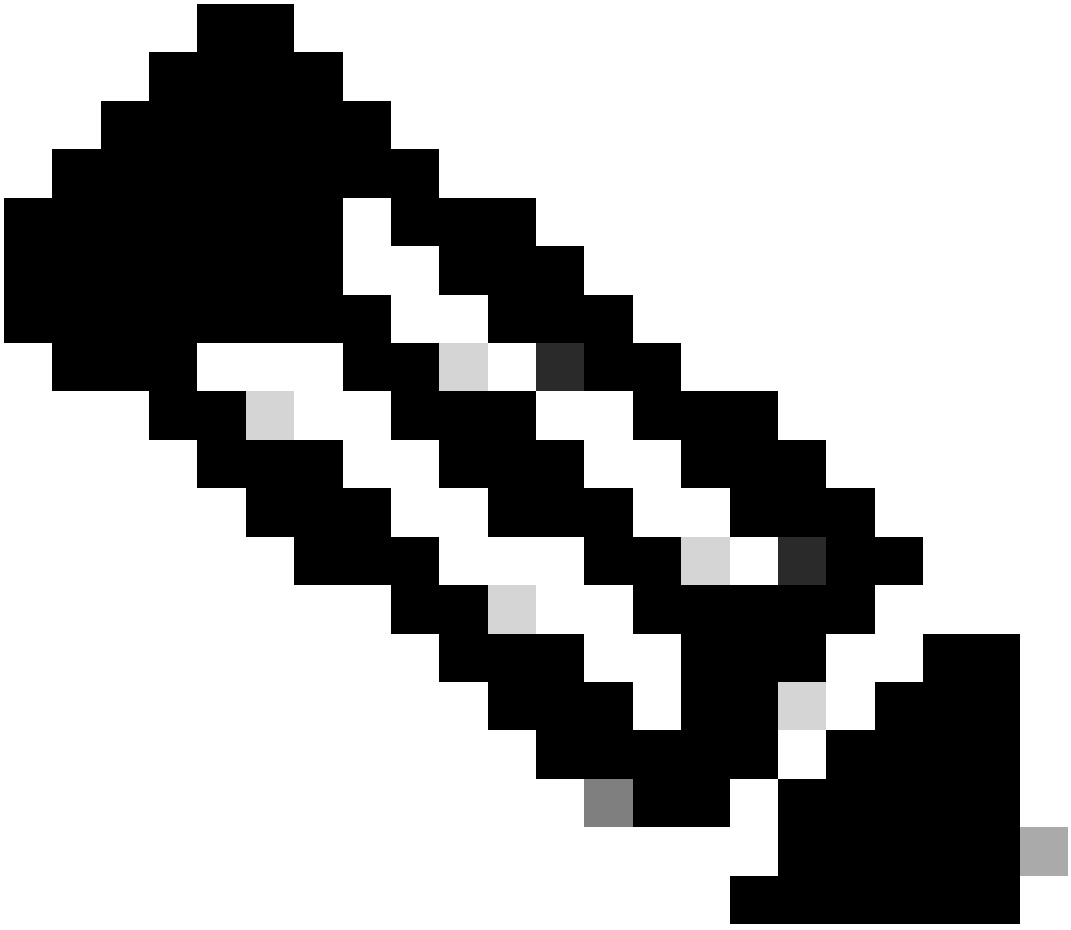
Confirmer que la clé privée n'est pas protégée par une phrase de passe

Connectez-vous au gestionnaire CTB en tant qu'utilisateur admin. Exécutez la commandessh-keygen -yf server_key.pem.

Une phrase de passe n'est pas requise si la clé privée n'en requiert pas.

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

Confirmer que le certificat et la clé privée sont codés en PEM



Remarque : ces validations peuvent être effectuées avant l'installation des certificats.

Connectez-vous au gestionnaire CTB en tant qu'utilisateur admin.

Affichez le contenu du fichier server_cert.pem à l'aide de la sudo cat server_cert.pem commande. Ajustez la commande au nom de fichier de votre certificat.

Les première et dernière lignes du fichier doivent être -----**BEGIN CERTIFICATE**----- et -----END CERTIFICATE----- respectivement.

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

Affichez le fichier server_key.pem à l'aide de la commandesudo cat server_key.pem. Réglez la commande sur le nom de fichier de vos clés privées.

Les première et dernière lignes du fichier doivent être -----**BEGIN PRIVATE KEY**----- et -----END PRIVATE KEY----- respectivement.

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

Certificat auto-signé

Générer un certificat auto-signé

- Connectez-vous au gestionnaire CTB sur SSH (Secure Shell) en tant qu'utilisateur configuré lors de l'installation. Il s'agit généralement de l'utilisateur « admin ».

- Entrez la commande suivante .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}

  - Modifiez la rsa:{key_len} avec une longueur de clé privée de votre choix, par exemple 2048, 4096 ou 8192

    - Modifier le {ctb_manager_ip}avec l'IP du noeud Gestionnaire 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:~$
```

- Affichez le fichier server_cert.pem à l'aide de la cat server_cert.pem commande et copiez le contenu dans votre mémoire tampon afin de pouvoir le coller sur la station de travail locale dans un éditeur de texte de votre choix. Enregistrez le fichier. Vous pouvez également SCP ces fichiers hors du /home/admin répertoire.

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

- Affichez le fichier server_key.pem à l'aide de la sudo cat server_key.pem commande et copiez le contenu dans votre mémoire tampon afin de pouvoir le coller sur la station de travail locale dans un éditeur de texte de votre choix. Enregistrez le fichier. Vous pouvez également SCP ce fichier hors du /home/admin répertoire.

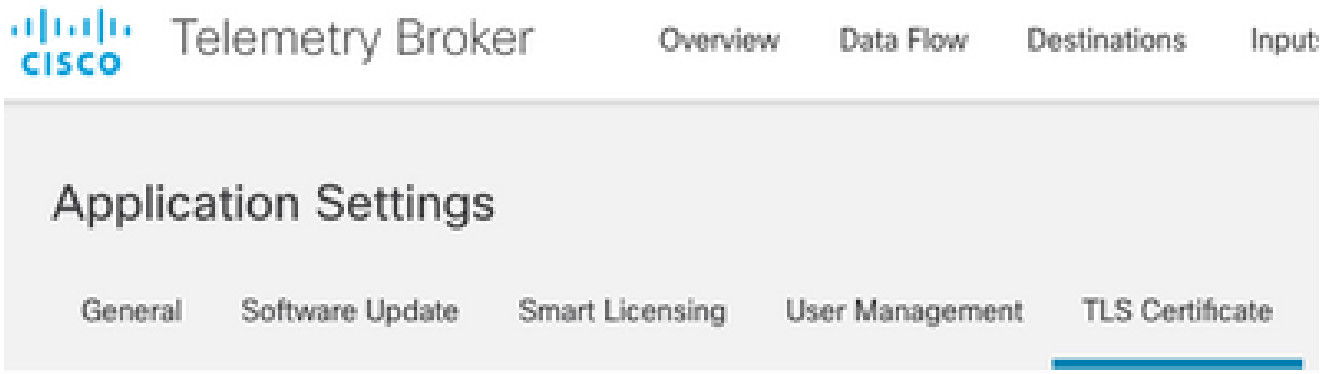
```
admin@ctb-manager:~$ sudo cat server_key.pem
-----BEGIN PRIVATE KEY-----
{removed_for_brevity}
-----END PRIVATE KEY-----
admin@ctb-manager:~$
```

Télécharger le certificat auto-signé

1. Accédez à l'interface utilisateur Web de CTB Manager et connectez-vous en tant qu'utilisateur admin, puis cliquez sur l'icône d'engrenage pour accéder à "Settings".

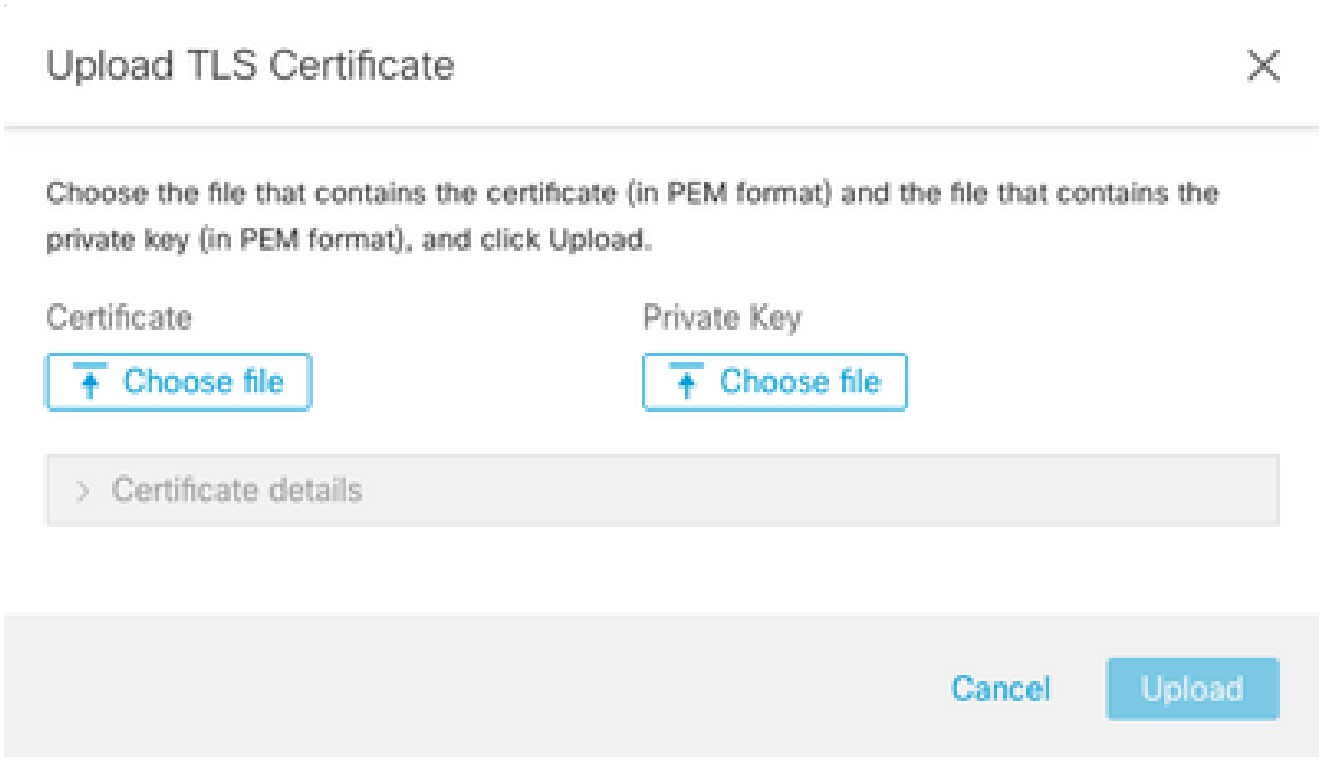
Icône de paramètre CTB

- Accédez à l'onglet « Certificat TLS ».

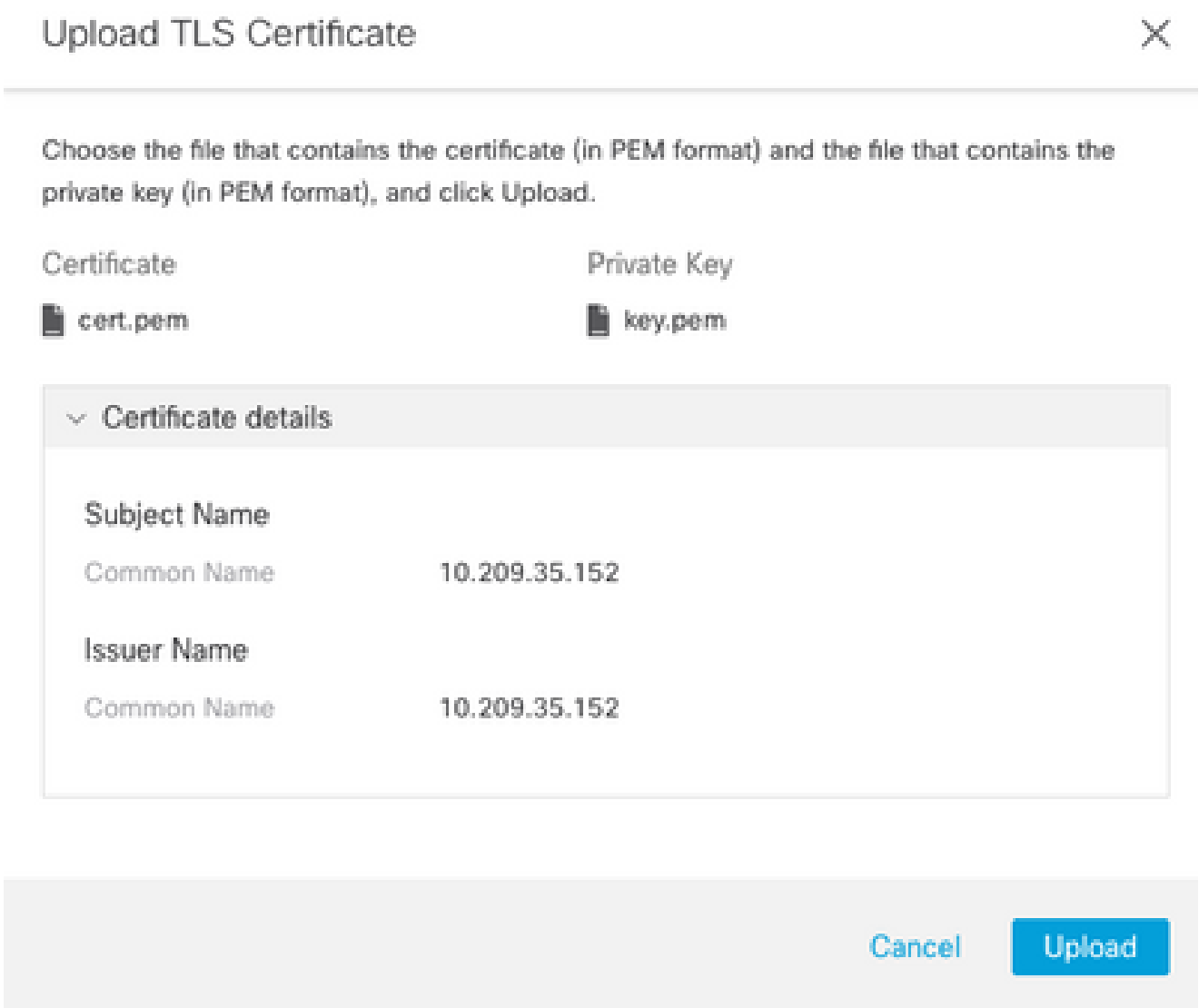


Onglet Certificats CTB

- Sélectionnez Upload TLS Certificate et sélectionnez le server_cert.pem et le server_key.pem pour le certificat et la clé privée respectivement dans la boîte de dialogue "Télécharger le certificat TLS". Une fois les fichiers sélectionnés, sélectionnez Télécharger.



• Une fois les fichiers sélectionnés, un processus de vérification confirme le certificat et la combinaison de clés et affiche le nom commun de l'émetteur et du sujet comme indiqué.



Téléchargement de certificat CTB

- Cliquez sur le bouton Télécharger pour télécharger le nouveau certificat. L'interface utilisateur Web redémarre seule dans quelques instants et, après le redémarrage, se reconnecte au périphérique.

- Connectez-vous à la console Web du noeud Gestionnaire CTB et accédez à Settings > TLS Certificate pour afficher les détails du certificat, par exemple une nouvelle date d'expiration, ou consultez les détails du certificat à l'aide du navigateur pour afficher des informations plus détaillées, telles que les numéros de série.

Mettre à jour les noeuds Broker

Une fois que le noeud Gestionnaire CTB a un nouveau certificat d'identité, chaque noeud Courtier CTB doit être mis à jour manuellement.

1. Connectez-vous à chaque noeud de courtier via ssh et exécutez la sudo ctb-manage commande

```
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:
```

- Sélectionnez une option clorsque vous y êtes invité.

```
== 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
```

- Vérifiez les détails du certificat s'ils correspondent aux valeurs du certificat signé et sélectionnez **y** pour accepter le certificat. Les services démarrent automatiquement et une fois le service démarré, l'invite est renvoyée. Le démarrage du service peut prendre jusqu'à environ 15 minutes.

```
== 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
```

Certificats émis par l'autorité de certification

Générer une demande de signature de certificat (CSR) pour émission par une autorité de certification

- Connectez-vous au gestionnaire CTB sur SSH (Secure Shell) en tant qu'utilisateur configuré lors de l'installation. Il s'agit généralement de l'utilisateur « admin ».

- Entrez la commande suivante .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 Les attributs « supplémentaires » des deux dernières lignes peuvent être laissés vides si vous le souhaitez.

  - Modifiez le {ctb_manager_dns_name} avec le nom DNS du noeud Gestionnaire CTB

    - Modifier le {ctb_manager_ip}avec l'IP du noeud Gestionnaire CTB

    - Modifiez la {key_len} avec une longueur de clé privée de votre choix, par exemple 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 []:
```

- Transmettez les fichiers CSR et Key à une machine locale et fournissez le CSR à l'autorité de certification. L'émission du REA par l'AC en format PEM n'est pas visée par le présent document.

Créer un certificat avec une chaîne

L'autorité de certification émet le certificat d'identité du serveur au format PEM. Un fichier de chaîne doit être créé qui inclut tous les certificats de chaîne et le certificat d'identité du serveur pour le noeud Gestionnaire CTB.

Dans un éditeur de texte, créez un fichier en combinant le certificat signé à l'étape précédente et en ajoutant tous les certificats de la chaîne, y compris l'autorité de certification approuvée, dans un seul fichier au format PEM, dans l'ordre indiqué.

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

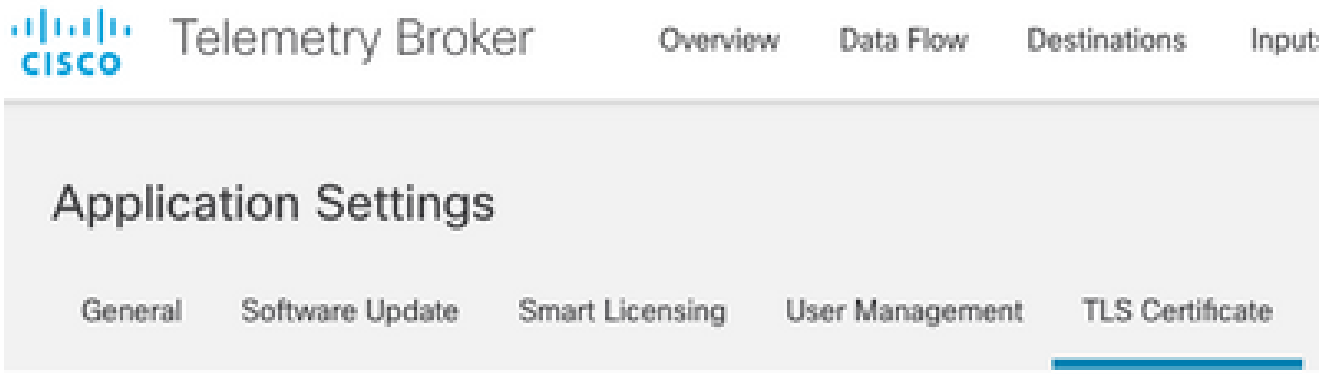
Assurez-vous que ce nouveau fichier de certificat avec fichier de chaîne ne comporte pas d'espaces de début ou de fin, de lignes vides et qu'il est dans l'ordre indiqué ci-dessus.

Télécharger le certificat émis par l'autorité de certification

1. Accédez à l'interface utilisateur Web du gestionnaire CTB, connectez-vous en tant qu'administrateur et cliquez sur l'icône d'engrenage pour accéder à "Settings".

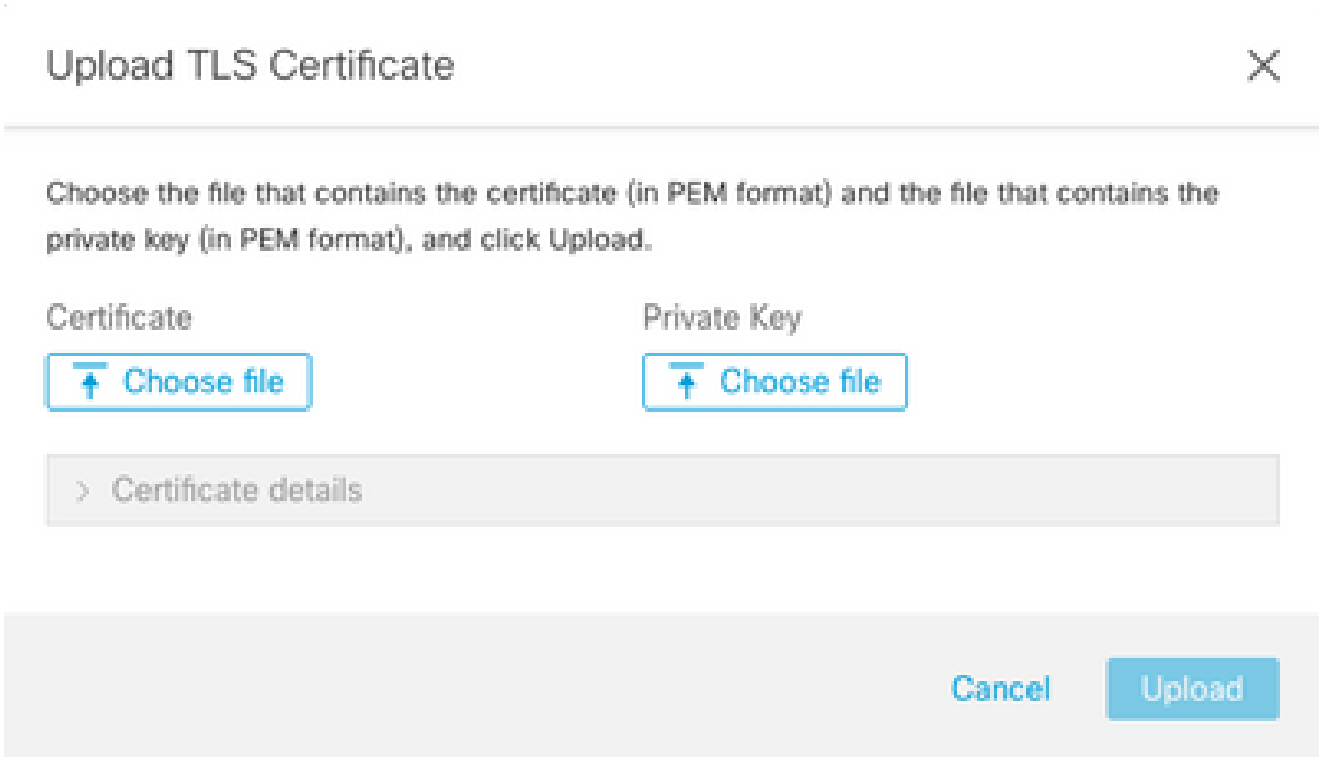
Icône de paramètre CTB

- Accédez à l'onglet « Certificat TLS ».

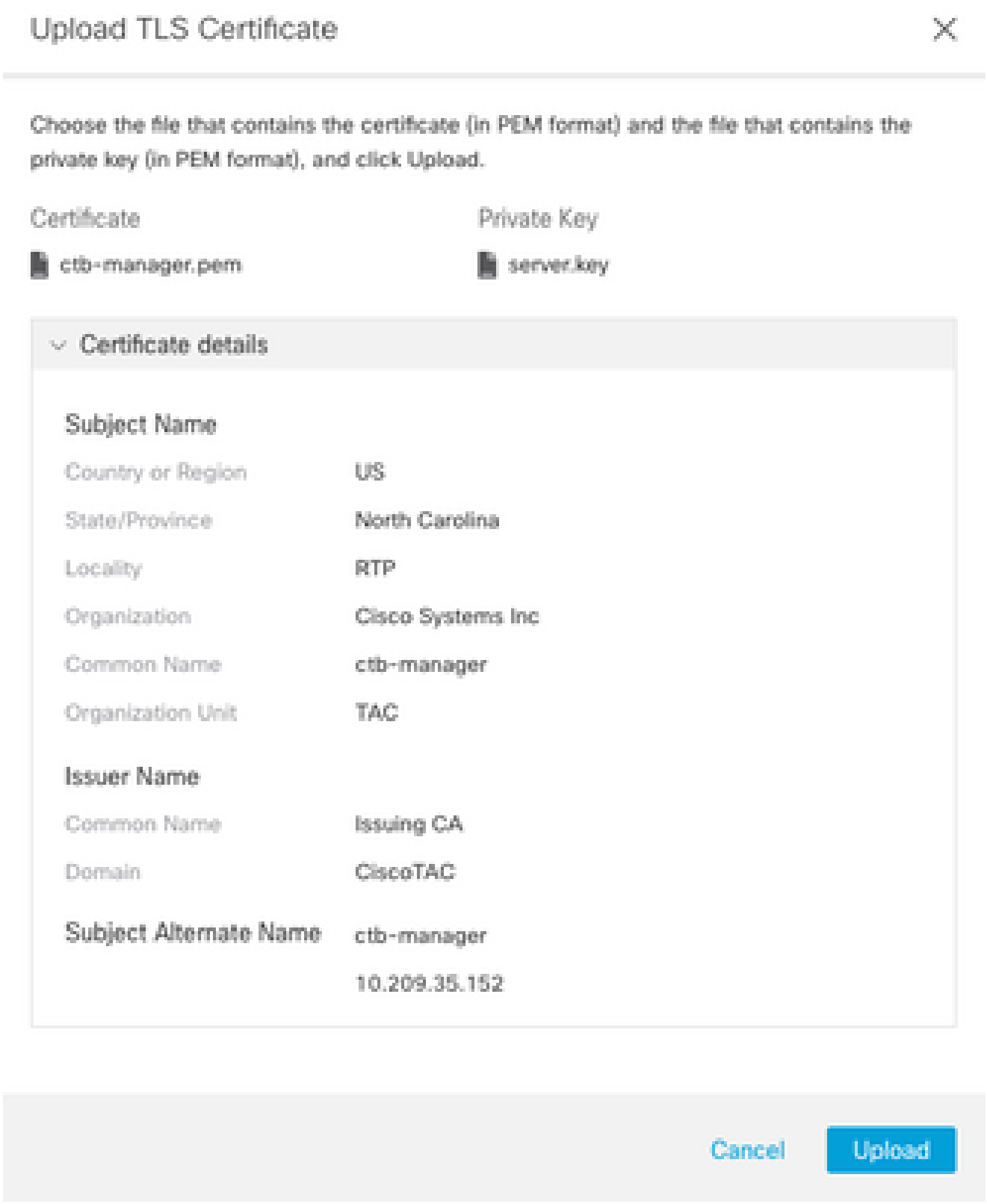


Onglet Certificats CTB

- Sélectionnez Upload TLS Certificate et sélectionnez le certificat avec le fichier de chaîne créé dans la dernière section, et le gestionnaire CTB généré server_key.pem pour le certificat et la clé privée respectivement dans la boîte de dialogue "Télécharger le certificat TLS". Une fois les fichiers sélectionnés, sélectionnez Télécharger.



• Une fois les fichiers sélectionnés, un processus de vérification confirme le certificat et la combinaison de clés et affiche le nom commun de l'émetteur et du sujet, comme indiqué ci-dessous.



Validation du certificat délivré par l'autorité de certification CTB

- Cliquez sur le bouton Télécharger pour télécharger le nouveau certificat. L'interface utilisateur Web redémarre automatiquement en 60 secondes environ, puis se connecte à l'interface utilisateur Web après le redémarrage.

- Connectez-vous à la console Web du noeud Gestionnaire CTB et accédez à Settings > TLS Certificate pour afficher les détails du

certificat, par exemple une nouvelle date d'expiration, ou consultez les détails du certificat à l'aide du navigateur pour afficher des informations plus détaillées, telles que les numéros de série.

Mettre à jour les noeuds Broker

Une fois que le noeud Gestionnaire CTB a un nouveau certificat d'identité, chaque noeud Courtier CTB doit être mis à jour manuellement.

1. Connectez-vous à chaque noeud de courtier via ssh et exécutez la sudo ctb-manage commande

```
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:
```

- Sélectionnez une option clorsque vous y êtes invité.

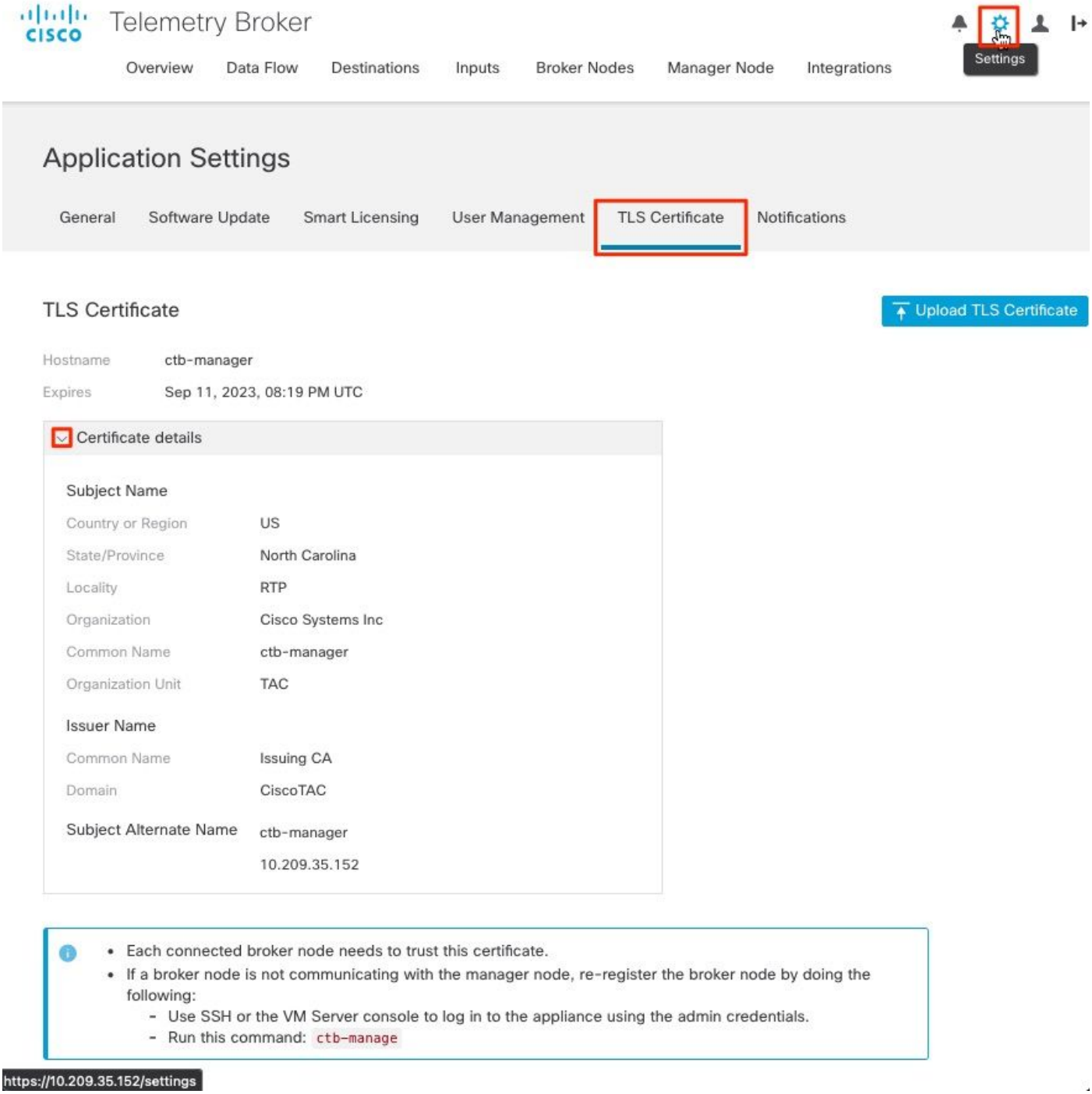
```
== Management Configuration

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
```

- Vérifiez les détails du certificat s'ils correspondent aux valeurs du certificat signé et sélectionnez y pour accepter le certificat. Les services démarrent automatiquement et une fois le service démarré, l'invite est renvoyée. Le démarrage du service peut prendre jusqu'à environ 15 minutes.

```
== 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
```

Vérifier

Connectez-vous à la console Web du noeud Gestionnaire CTB et accédez à Settings > TLS Certificate pour afficher les détails du certificat, par exemple une nouvelle date d'expiration, ou consultez les détails du certificat à l'aide du navigateur pour afficher des informations plus détaillées, telles que les numéros de série.



Détails du certificat CTB

Vérifiez que le noeud CTB Broker ne présente aucune alarme dans l'interface utilisateur Web du noeud CTB Manager.

Dépannage

Si le certificat est incomplet, par exemple en l'absence de certificats de chaîne, le noeud de noeud du courtier CTB ne peut pas communiquer avec le noeud du gestionnaire et affiche « Non vu depuis » dans la colonne État de la liste des noeuds du courtier.
Le noeud Broker continuera à répliquer et à distribuer le trafic dans cet état.

Connectez-vous à l'interface de ligne de commande du noeud du gestionnaire CTB et exécutez la sudo grep -ic begin /var/lib/titan/titanium_frontend/ssl/cert.pem commande pour connaître le nombre de certificats contenus dans le fichier cert.pem.

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

La valeur de sortie renvoyée doit correspondre au nombre de périphériques CA dans la chaîne plus le gestionnaire CTB.

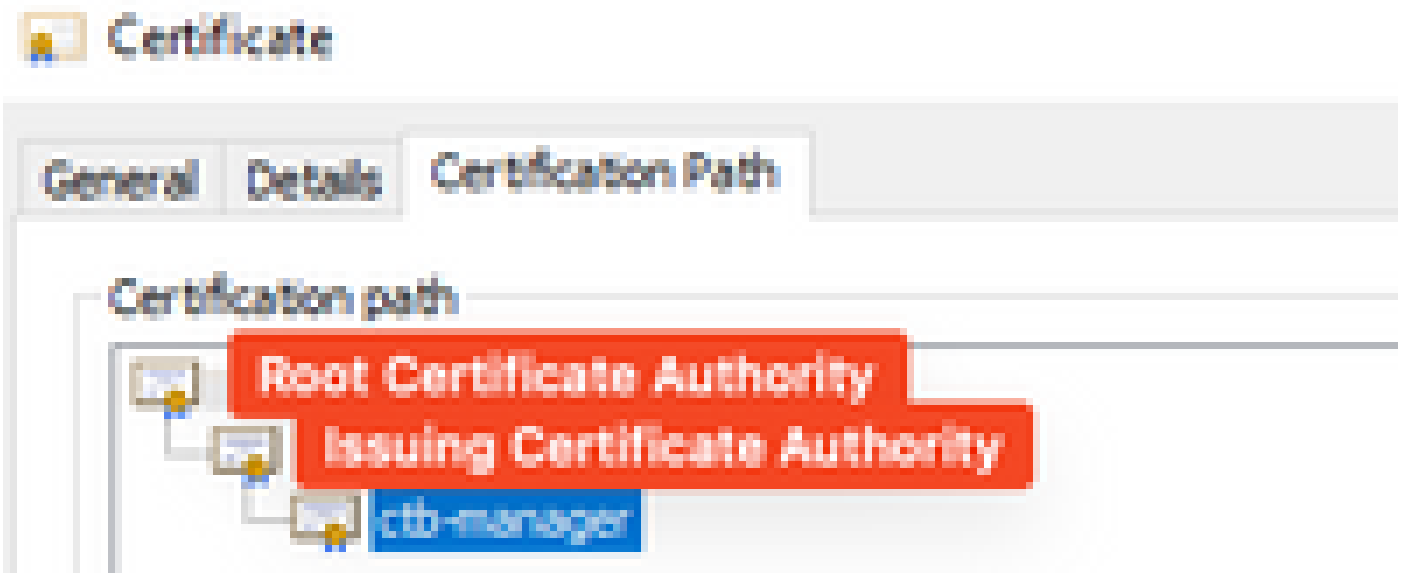
La sortie de 1 est attendue si vous utilisez un certificat auto-signé.

Le résultat de 2 est attendu si l'infrastructure PKI se compose d'une seule autorité de certification racine qui est également l'autorité de certification émettrice.

Le résultat de 3 est attendu si l'infrastructure PKI est constituée d'une autorité de certification racine et de l'autorité de certification émettrice.

Le résultat de 4 est attendu si l'infrastructure PKI est composée d'une autorité de certification racine, d'une autorité de certification subordonnée et de l'autorité de certification émettrice.

Comparez le résultat à l'ICP indiquée lors de l'affichage du certificat dans une autre application telle que Microsoft Windows Crypto Shell Extensions.



Infrastructure PKI

Dans cette image, l'infrastructure PKI inclut une autorité de certification racine et l'autorité de certification émettrice.

La valeur de sortie de la commande devrait être 3 dans ce scénario.

Si le résultat ne répond pas aux attentes, passez en revue les étapes de la section **Créer un certificat avec une chaîne** pour déterminer si un certificat a été manqué.

Lors de l'affichage d'un certificat dans, Microsoft Windows Crypto Shell Extensions il est possible que tous les certificats ne soient pas présentés si l'ordinateur local ne dispose pas d'informations suffisantes pour vérifier le certificat.

Exécutez la sudo ctb-mayday commande à partir de l'interface de ligne de commande pour générer un bundle mayday que le TAC doit examiner.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.