Identiteitscertificaat van telemetriemakelaar vervangen

Inhoud

Inleiding

Dit document beschrijft hoe u het Server Identity Certificate vervangt op het Cisco Telemetry Broker (CTB) Manager-knooppunt.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco TelePresence Broker-apparaatbeheer
- x509-certificaten

Gebruikte componenten

Op de apparatuur die voor dit document wordt gebruikt, wordt versie 2.0.1 uitgevoerd

- Cisco TelePresence Broker Manager-knooppunt
- Cisco TelePresence Broker Broker Node

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Configureren

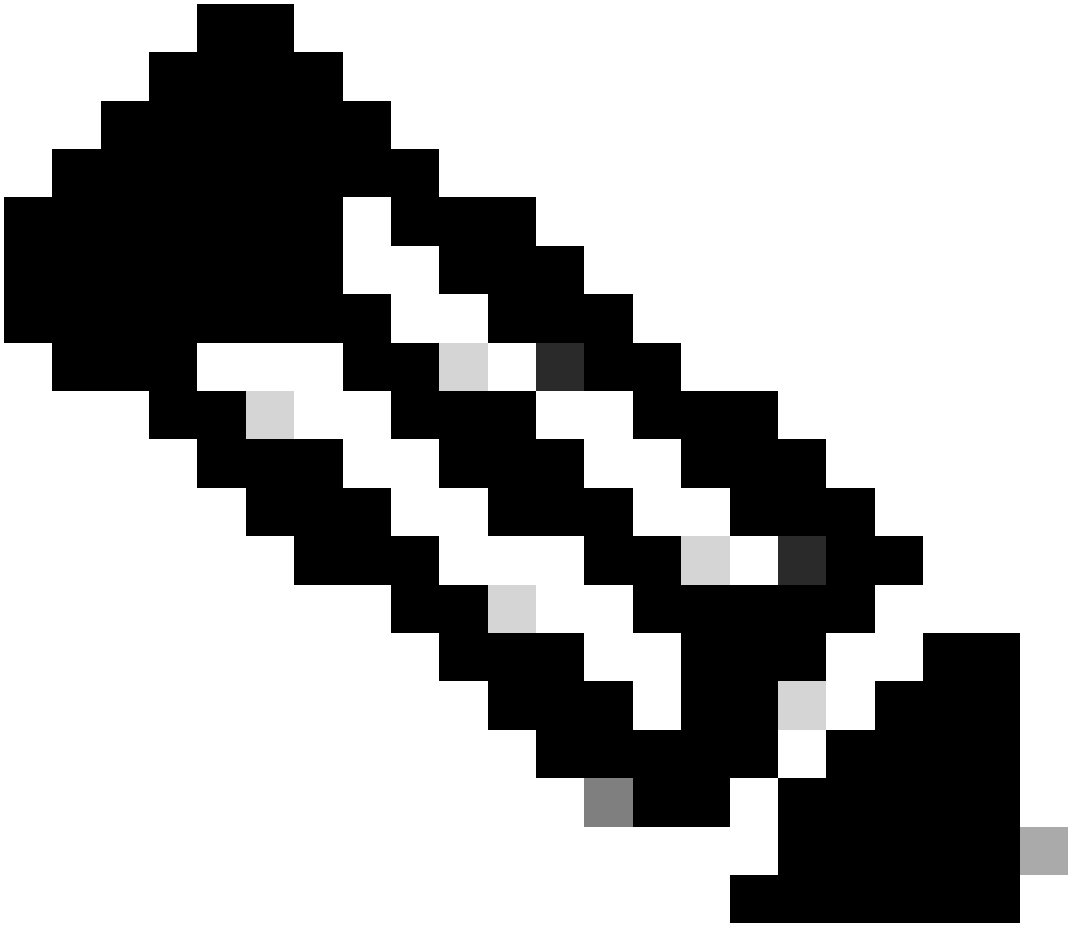
Certificaatvereisten

Het x509-certificaat dat wordt gebruikt door Cisco Telemetry Broker Manager moet aan deze vereisten voldoen:

- De Cert en Private Key moeten een overeenkomend paar zijn
- Het certificaat en de persoonlijke sleutel moeten PEM-gecodeerd zijn
- De persoonlijke sleutel mag niet worden beveiligd met een wachtwoord

Bevestig Certificaat en Privé Sleutel zijn passend paar

Log in op de CTB Manager commando line interface (CLI) als beheerder gebruiker.



Opmerking: het is mogelijk dat de bestanden die in deze sectie worden genoemd nog niet op het systeem bestaan.

De sudo openssl req -in server.csr -pubkey -noout -outform pem | sha256sum opdrachtoutput van de SHA-256-checksum van de openbare sleutel uit het aanvraagbestand voor certificaatondertekening.

De sudo openssl pkey -in server_key.pem -pubout -outform pem | sha256sumopdrachtoutput van de SHA-256-checksum van de openbare sleutel uit het privé-sleutelbestand.

De sudo openssl x509 -in server_cert.pem -pubkey -noout -outform pem | sha256sumopdrachtoutput van de SHA-256-checksum van de openbare sleutel uit het afgegeven certificaatbestand.

Het certificaat en de Private Key-uitvoer moeten overeenkomen. Als een certificaatondertekeningsaanvraag niet is gebruikt, bestaat het bestand server_cert.pem niet.

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

Bevestig dat privésleutel niet is beveiligd met een wachtwoord

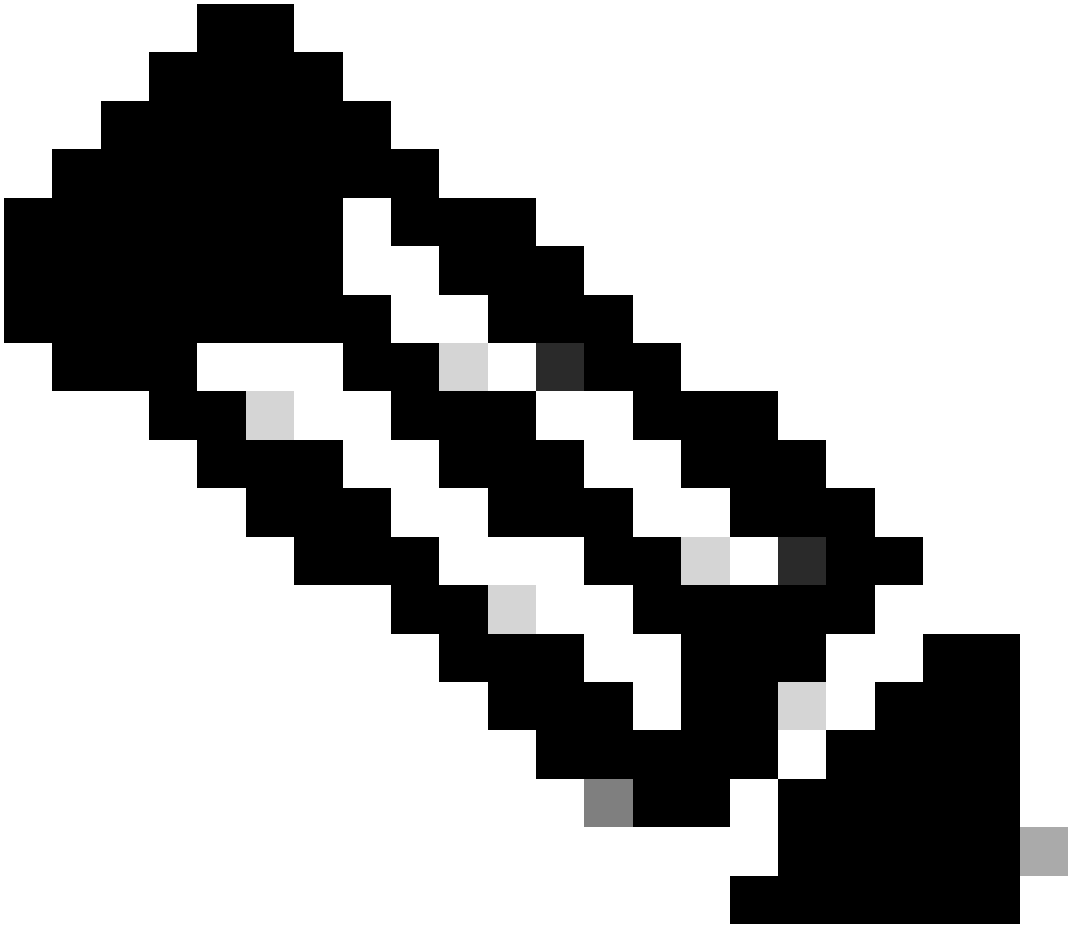
Log in op CTB Manager als beheerder. Start de ssh-keygen -yf server_key.pem opdracht.

Een wachtwoord wordt niet gevraagd als de privé sleutel niet vereist.

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

Bevestig het Certificaat en de Privé Sleutel worden PEM-gecodeerd

---



Opmerking: deze valideringen kunnen worden uitgevoerd voordat de certificaten worden geïnstalleerd.

Log in op CTB Manager als beheerder.

Bekijk de server_cert.pem bestandsinhoud met de sudo cat server_cert.pem opdracht. Pas de opdracht aan de naam van het certificaatbestand.

De eerste en de laatste regel van het bestand moeten respectievelijk **-----BEGIN CERTIFICATE-----** en -----END CERTIFICATE----- zijn.

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

Bekijk het server_key.pem bestand met de opdrachtsudo cat server_key.pem. Stel de opdracht in op de bestandsnaam van uw privésleutels.

De eerste en de laatste regel van het bestand moeten respectievelijk **-----BEGIN PRIVATE KEY-----** en -----END PRIVATE KEY----- zijn.

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

Zelfondertekend certificaat

Generate Self Signed Certificate

- Log in op de CTB Manager via een SSH (Secure Shell) als de gebruiker die tijdens de installatie is geconfigureerd, dit is meestal de "admin"-gebruiker.

- Geef de 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} opdracht uit.

  - Verander het rsa:{key_len} scherm met een persoonlijke sleutellengte naar keuze, zoals 2048, 4096 of 8192

  - Verander de IP-status {ctb_manager_ip}van het CTB Manager-knooppunt

```
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 Bekijk het server_cert.pem bestand met de opdracht en kopieer de inhoud naar uw buffer, zodat het naar het lokale werkstation kan worden geplakt in een teksteditor naar keuze. Sla het bestand op. U kunt deze bestanden ook uit de /home/admin map verwijderen.

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

- sudo cat server_key.pem Bekijk het server_key.pem bestand met de opdracht en kopieer de inhoud naar uw buffer, zodat het kan worden geplakt op het lokale werkstation in een teksteditor naar keuze. Sla het bestand op. U kunt dit bestand ook uit de /home/admin map verwijderen.

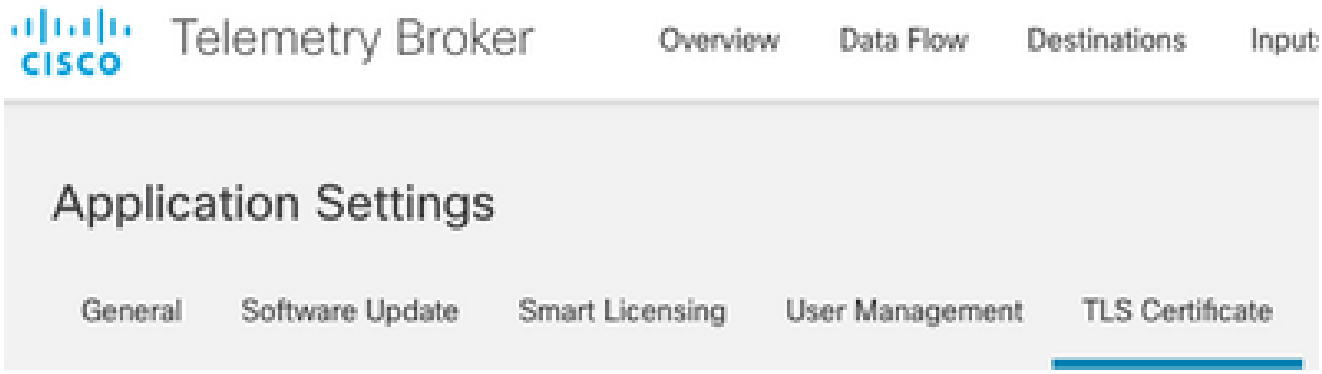
```
admin@ctb-manager:~$ sudo cat server_key.pem
-----BEGIN PRIVATE KEY-----
{removed_for_brevity}
-----END PRIVATE KEY-----
admin@ctb-manager:~$
```

Zelfondertekend certificaat uploaden

1. Navigeer naar de CTB Manager Web UI en log in als de beheerder gebruiker en klik op het tandwielpictogram om toegang te krijgen "Settings.

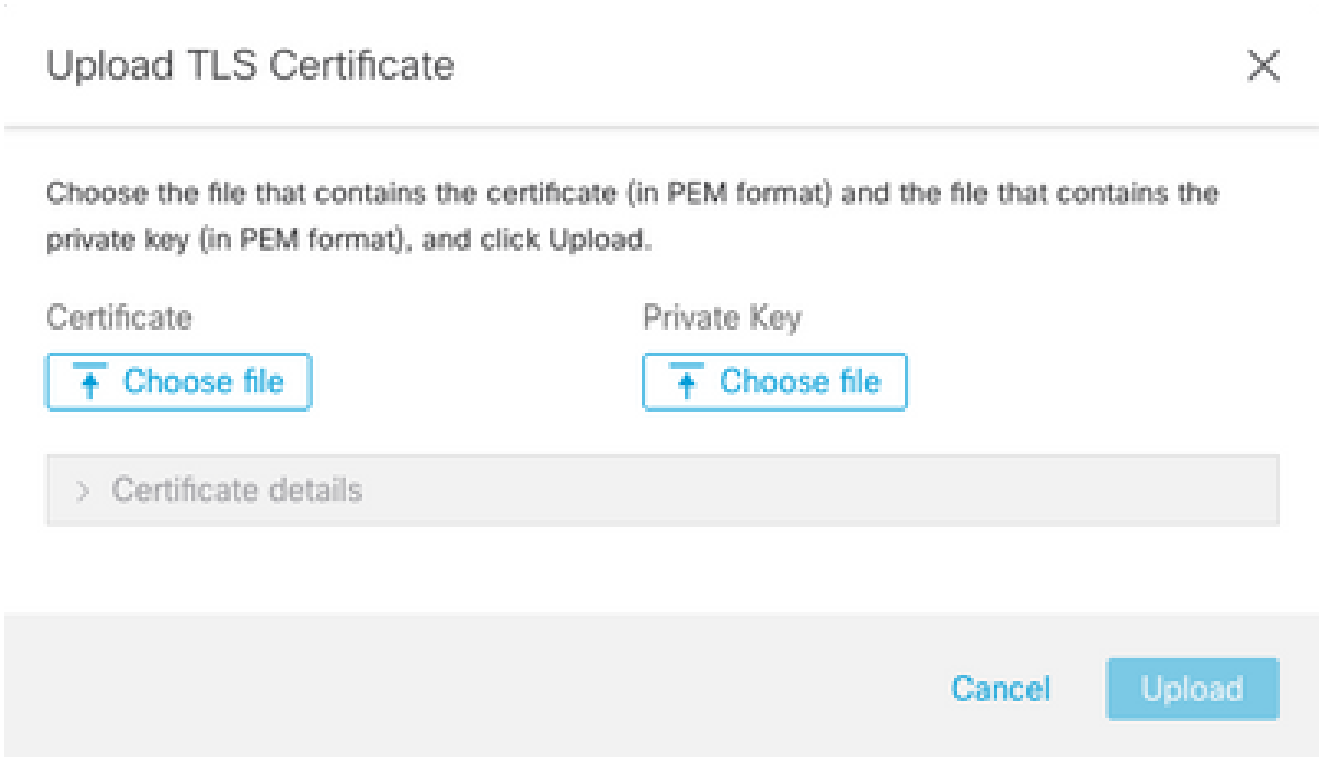
CTB-instellingspictogram

- Ga naar het tabblad "TLS-certificaat".

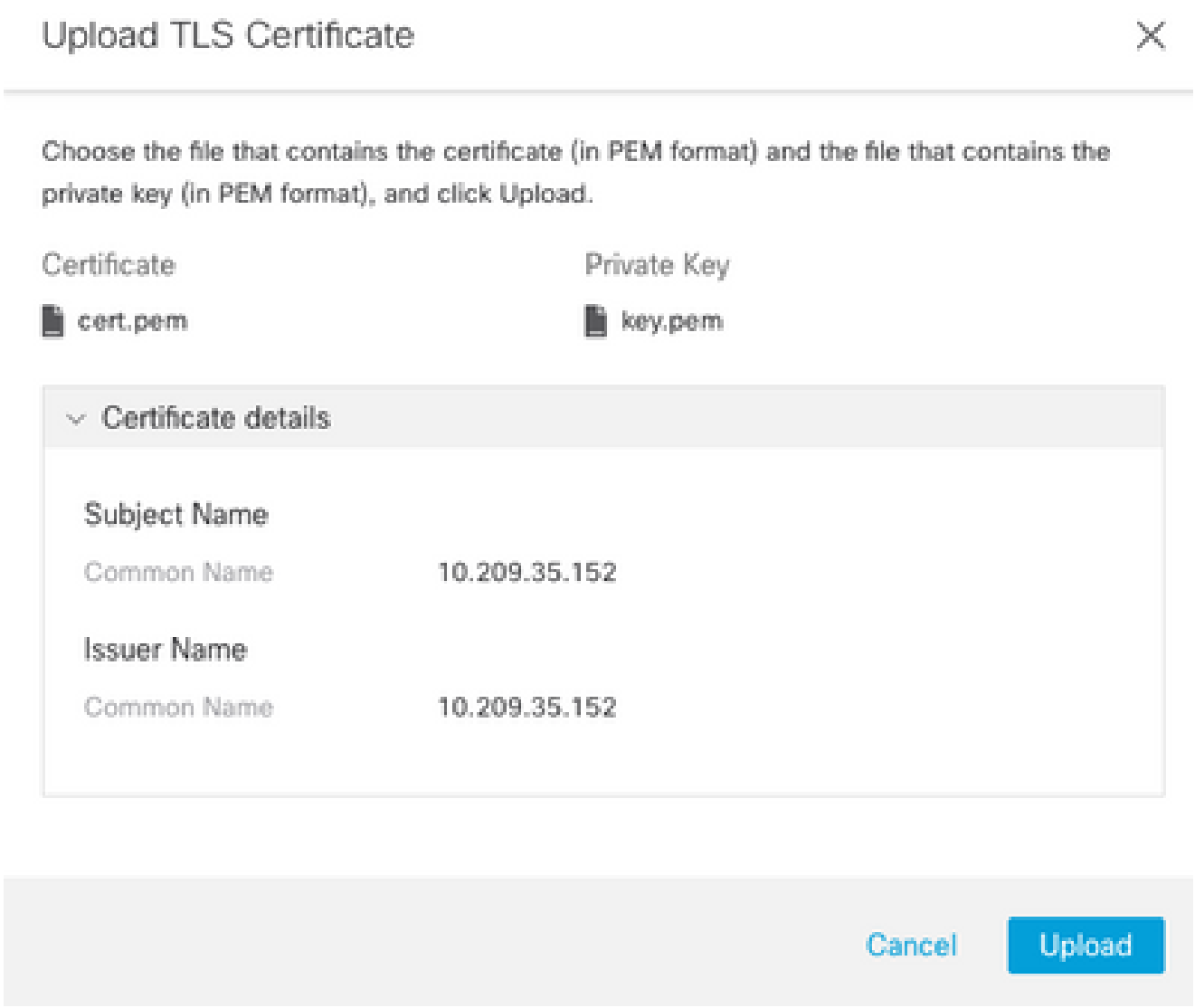


CTB-certificaten - tabblad

- Selecteer Upload TLS Certificate en selecteer vervolgens de server_cert.pem en de server_key.pem voor het certificaat en de privé-sleutel in het dialoogvenster "TLS-certificaat uploaden". Zodra de bestanden zijn geselecteerd, selecteert u Upload.



- Zodra de bestanden zijn geselecteerd, bevestigt een verificatieproces het certificaat en de toetscombinatie en geeft het de gebruikelijke naam van de uitgevende instelling en het onderwerp weer zoals aangegeven.



CTB Cert uploaden

- Selecteer de knop "Upload" om het nieuwe certificaat te uploaden. De Web UI herstart op eigen in een paar momenten, en nadat het opnieuw begint log in het apparaat opnieuw.

- Log in op de CTB Manager Node-webconsole en navigeer om Settings > TLS Certificate de certificaatgegevens te zien, zoals een nieuwe vervaldatum, of bekijk de certificaatgegevens met behulp van de browser om meer gedetailleerde informatie te bekijken, zoals serienummers.

Update Broker Knooppunten

Zodra het CTB Manager Node een nieuw identiteitscertificaat heeft, moet elk CTB Broker Node handmatig worden bijgewerkt.

1. Log in op elk broker knooppunt via ssh en voer de sudo ctb-manage opdracht uit

```
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:
```

- Selecteer optie cwanneer dit wordt gevraagd.

```
== 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
```

- Controleer de certificaatdetails als ze overeenkomen met de waarden voor het ondertekende certificaat en selecteer **y** om het certificaat te aanvaarden. De services starten automatisch en zodra de service is gestart wordt de prompt teruggestuurd. Het starten van de service kan tot ongeveer 15 minuten duren.

```
== 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
```

Certificaatautoriteit (CA) Afgegeven certificaten

Genereren van aanvraag voor certificatie-ondertekening (CSR) voor afgifte door een certificeringsinstantie

- Log in op de CTB Manager via een SSH (Secure Shell) als de gebruiker die tijdens de installatie is geconfigureerd, dit is meestal de "admin"-gebruiker.

- Geef de opdrachtopenssl 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 uit. De 'extra' attributen op de laatste twee lijnen kunnen desgewenst leeg worden gelaten.

  - Wijzig de {ctb_manager_dns_name} DNS-naam van het CTB Manager-knooppunt

    - Verander de IP-status {ctb_manager_ip}van het CTB Manager-knooppunt

    - Verander het {key_len} met een persoonlijke sleutellengte naar keuze, zoals 2048, 4096 of 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 de CSR en de Key files naar een lokale machine en de CSR leveren aan de CA. De uitgifte van het MVO door de CA in PEM-formaat valt buiten het toepassingsgebied van dit document.

Een certificaat met keten maken

CA geeft het server identiteitsbewijs in PEM-formaat uit. Er moet een kettingbestand worden gemaakt dat alle kettingcertificaten en het serveridentiteitscertificaat voor het CTB Manager Node bevat.

In een teksteditor maakt u een bestand door het certificaat dat in de vorige stap is ondertekend te combineren en alle certificaten in de keten helemaal toe te voegen, inclusief de vertrouwde CA, in één bestand in PEM-formaat in de getoonde volgorde.

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

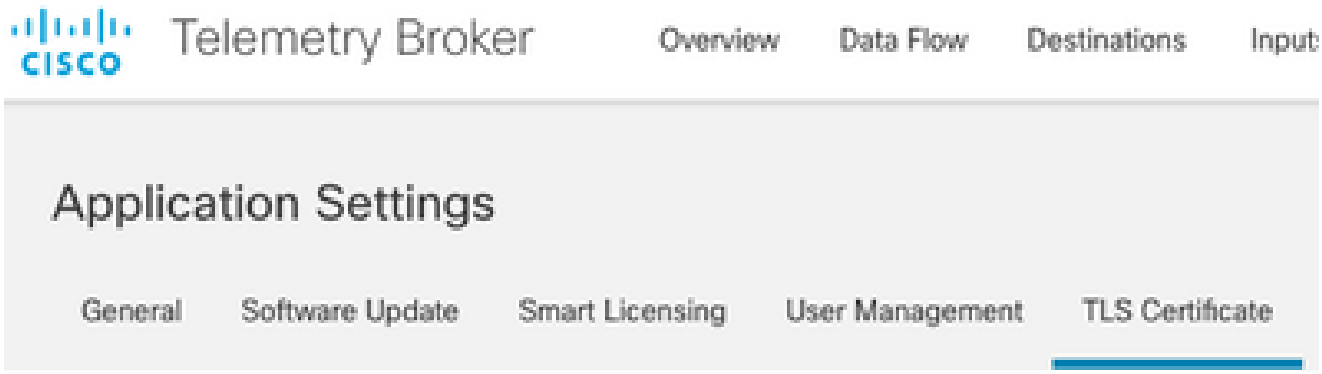
Zorg ervoor dat dit nieuwe certificaat bestand met kettingbestand geen spaties voor de kop of achterkant, lege regels heeft en in de bovenstaande volgorde staat.

Certificaatautoriteit voor uploaden van bestanden Afgegeven certificaat

1. Navigeer naar de CTB Manager Web UI en log in als beheerder en klik op het tandwielpictogram voor toegang "Settings.

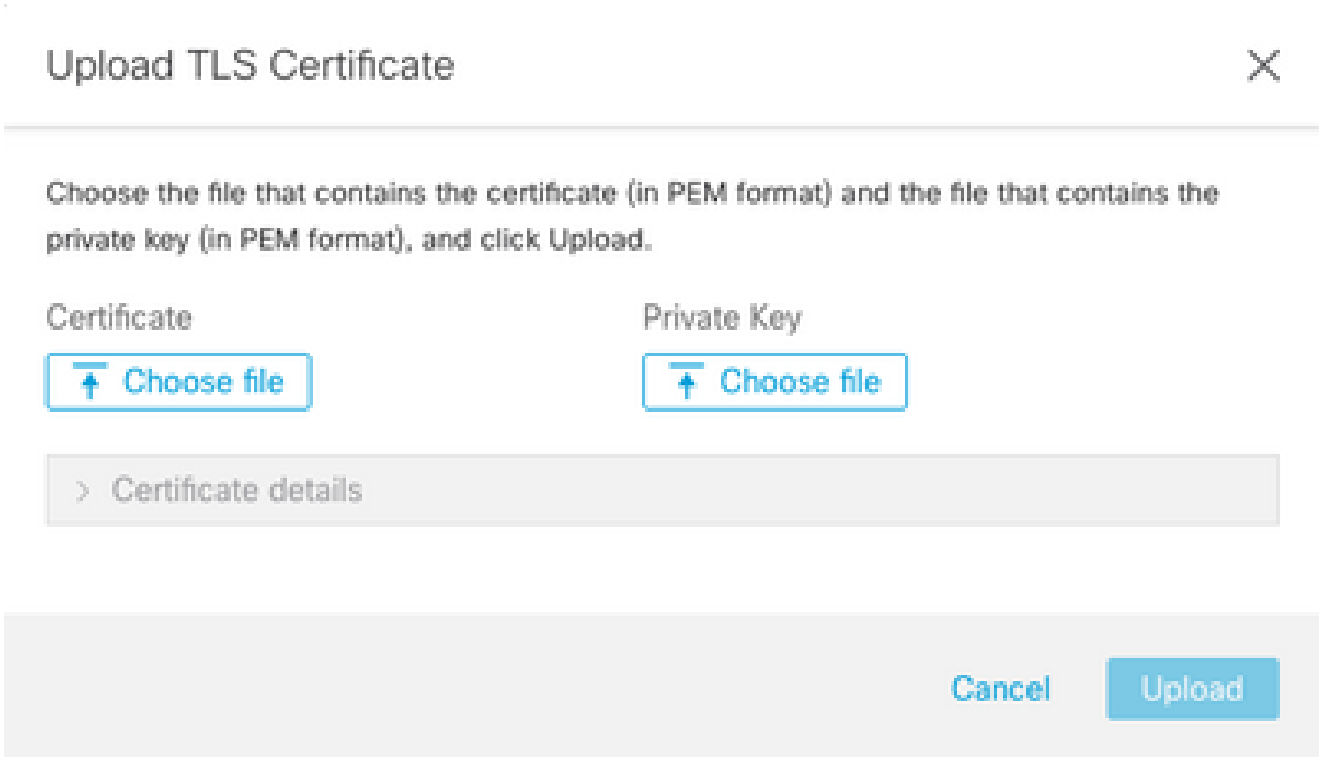
CTB-instellingspictogram

- Ga naar het tabblad "TLS-certificaat".

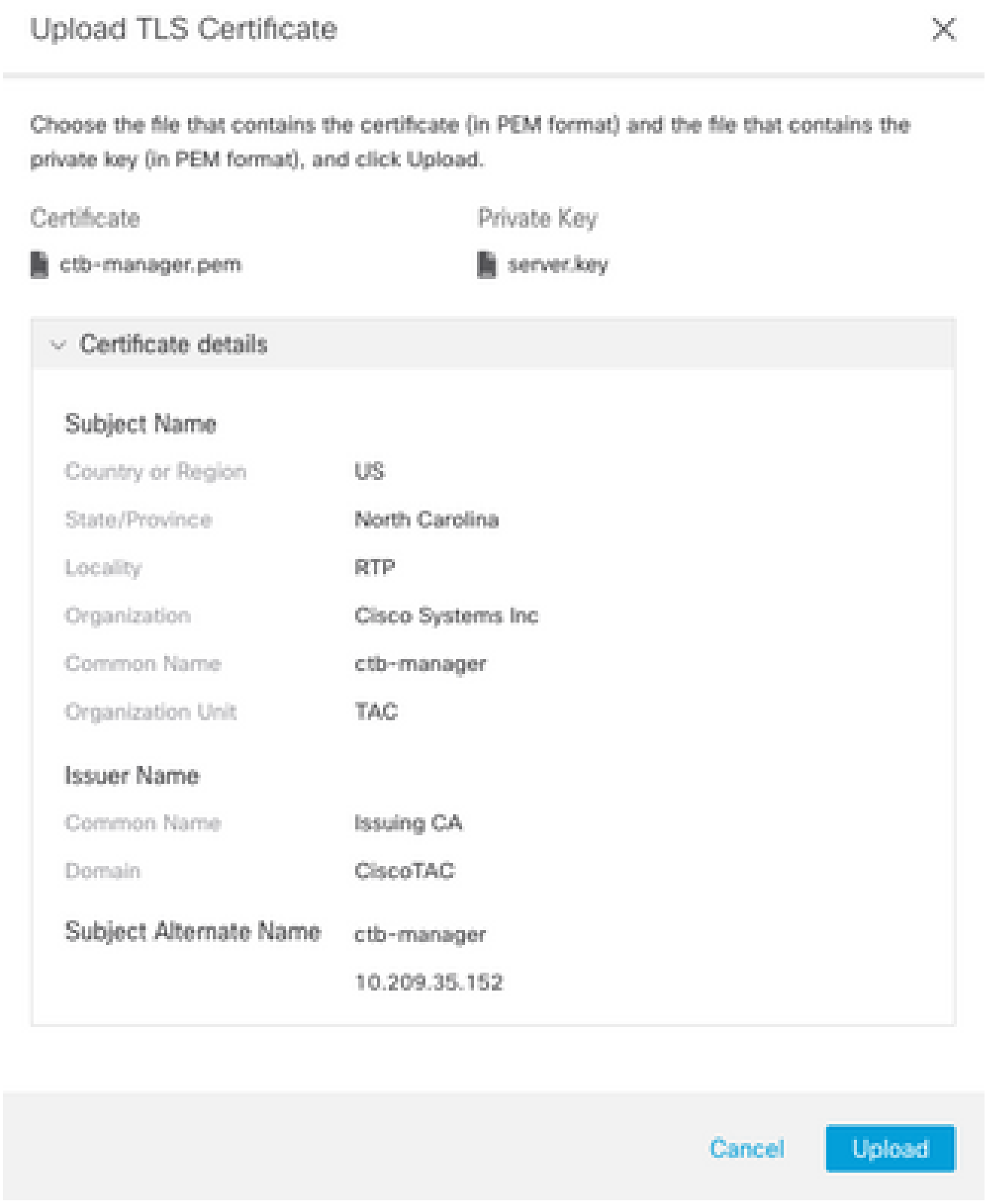


CTB-certificaten - tabblad

- Selecteer Upload TLS Certificate en selecteer vervolgens het certificaat met kettingbestand dat in de laatste sectie is gemaakt en de CTB-beheerder die is gegenereerd server_key.pem voor het certificaat en de persoonlijke sleutel in het dialoogvenster "TLS-certificaat uploaden". Zodra de bestanden zijn geselecteerd, selecteert u Upload.



• Zodra de bestanden zijn geselecteerd, bevestigt een verificatieproces het certificaat en de toetscombinatie en geeft de algemene naam van de uitgevende instelling en het onderwerp weer zoals hieronder wordt getoond.



CTB CA afgegeven validering door Cert

- Selecteer de knop "Upload" om het nieuwe certificaat te uploaden. De Web UI herstart op eigen in ongeveer 60 seconden, inloggen op de Web UI nadat het herstart.

- Log in op de CTB Manager Node-webconsole en navigeer om Settings > TLS Certificate de certificaatgegevens te zien, zoals een

nieuwe vervaldatum, of bekijk de certificaatgegevens met behulp van de browser om meer gedetailleerde informatie te bekijken, zoals serienummers.

Update Broker Knooppunten

Zodra het CTB Manager Node een nieuw identiteitscertificaat heeft, moet elk CTB Broker Node handmatig worden bijgewerkt.

1. Log in op elk broker knooppunt via ssh en voer de sudo ctb-manage opdracht uit

```
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:
```

- Selecteer optie cwanneer dit wordt gevraagd.

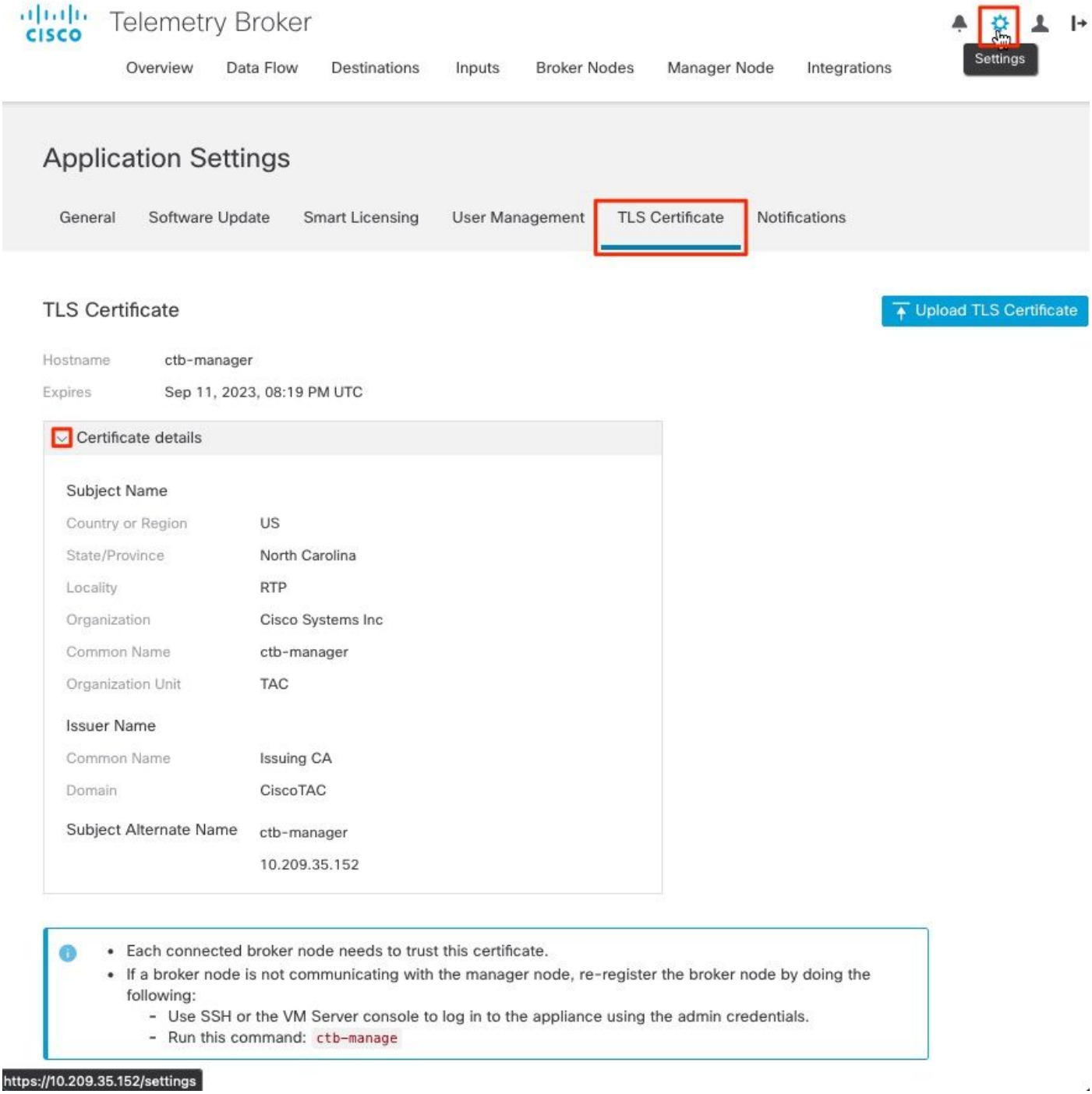
```
== Management Configuration

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
```

- Controleer de certificaatgegevens of deze overeenkomen met de waarden voor het ondertekende certificaat en selecteer y om het certificaat te aanvaarden. De services starten automatisch en zodra de service is gestart wordt de prompt teruggegeven. Het starten van de service kan tot ongeveer 15 minuten duren.

```
== 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
```

Verifiëren

Log in op de CTB Manager Node-webconsole en navigeer om Settings > TLS Certificate de certificaatgegevens te zien, zoals een nieuwe vervaldatum, of bekijk de certificaatgegevens met behulp van de browser om meer gedetailleerde informatie te bekijken, zoals serienummers.



CTB-certificaatgegevens

Controleer of het CTB Broker Node geen alarmen toont in de CTB Manager Node Web UI.

Problemen oplossen

Als het certificaat onvolledig is, zoals het ontbreken van de kettingcertificaten, kan het CTB Broker Node niet communiceren met het Manager Node en geeft "Not Seen Since" weer in de kolom Status in de lijst van Broker Nodes.
Het Broker Node zal verkeer in deze staat blijven repliceren en verdelen.

Log in op de CTB Manager Node CLI en geef de sudo grep -ic begin /var/lib/titan/titanium_frontend/ssl/cert.pem opdracht uit om te zien hoeveel certificaten er in het cert.pem-bestand staan.

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

De teruggegeven outputwaarde vergt gelijk het aantal apparaten van CA in de ketting plus de Manager van CTB.

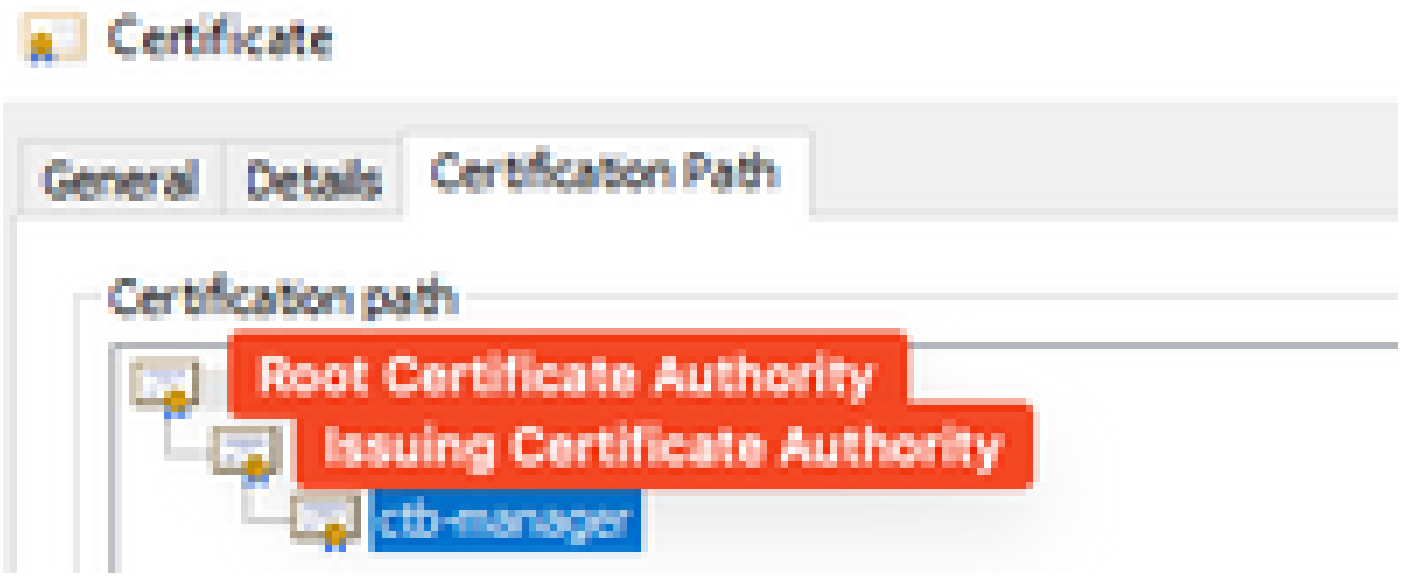
De output van 1 wordt verwacht als het gebruiken van een zelf ondertekend certificaat.

De output van 2 wordt verwacht als de PKI-infrastructuur uit één root-CA bestaat die ook de uitgevende CA is.

De output van 3 wordt verwacht als de PKI-infrastructuur uit een root-CA en de uitgevende CA bestaat.

De output van 4 wordt verwacht als de PKI-infrastructuur bestaat uit een root-CA, een ondergeschikte CA en de uitvaardigende CA.

Vergelijk de uitvoer naar de vermelde PKI bij het bekijken van het certificaat in een andere toepassing zoals Microsoft Windows Crypto Shell Extensions.



PKI-infrastructuur

In deze afbeelding omvat de PKI-infrastructuur een root-CA en de uitvaardigende CA.

De uitvoerwaarde van de opdracht wordt in dit scenario verwacht 3 te zijn.

Als de output niet aan de verwachtingen voldoet, herzie de stappen in **Create a Certificate with Chain** sectie om te bepalen of een certificaat is gemist.

Bij het bekijken van een certificaat in Microsoft Windows Crypto Shell Extensions is het mogelijk dat niet alle certificaten worden gepresenteerd als de lokale machine niet genoeg informatie heeft om het certificaat te verifiëren.

Geef het sudo ctb-mayday bevel van CLI uit om een bundel van de Mayday voor TAC te produceren om te herzien.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.