Telemetry Broker ID 인증서 바꾸기

목차

소개

이 문서에서는 CTB(Cisco Telemetry Broker) 관리자 노드에서 서버 ID 인증서를 교체하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco Telemetry Broker 어플라이언스 관리
- x509 인증서

사용되는 구성 요소

이 문서에 사용된 어플라이언스는 버전 2.0.1을 실행 중입니다.

- Cisco Telemetry Broker Manager 노드
- Cisco Telemetry Broker 브로커 노드

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성

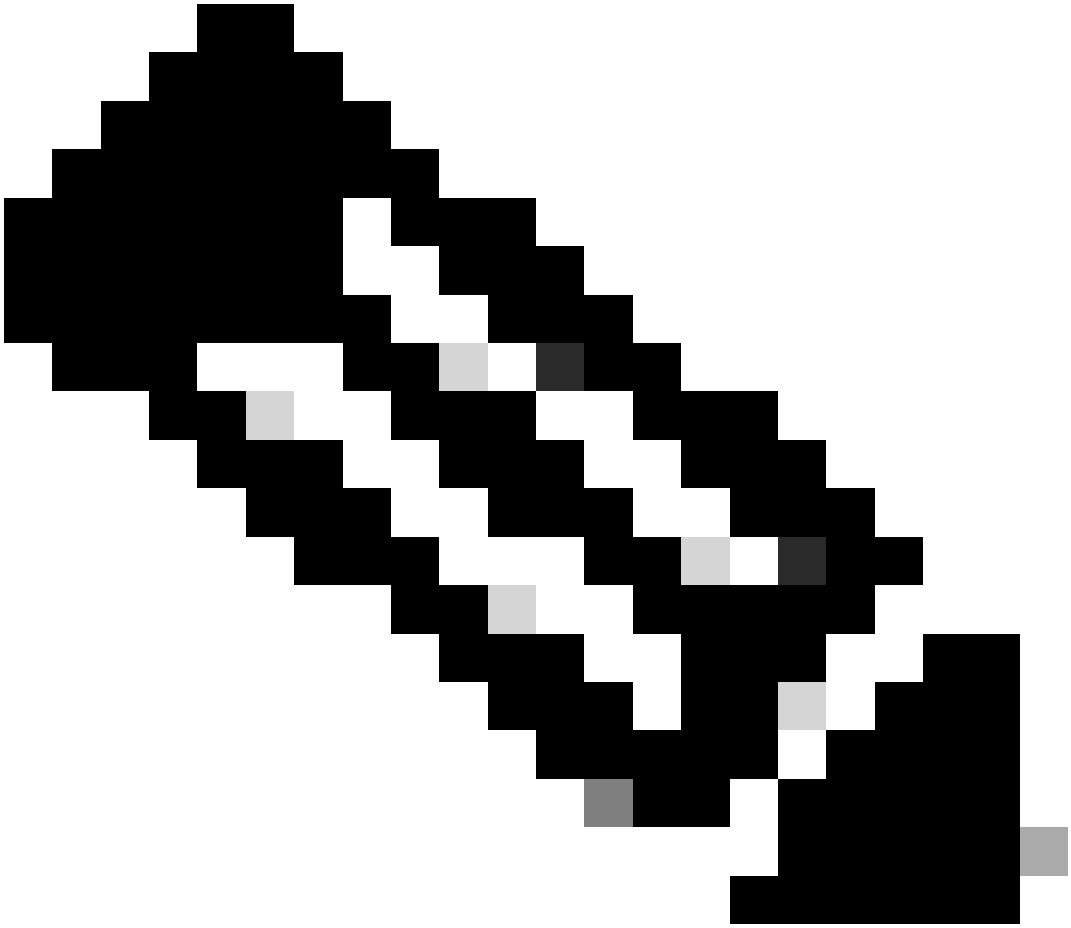
인증서 요구 사항

Cisco Telemetry Broker Manager에서 사용하는 x509 인증서는 다음 요구 사항을 충족해야 합니다.

- 인증서 및 개인 키는 일치하는 쌍이어야 합니다.
- 인증서 및 개인 키는 PEM으로 인코딩되어야 합니다.
- 개인 키는 암호로 보호되지 않아야 합니다.

인증서와 개인 키가 일치하는 쌍인지 확인합니다.

CTB Manager CLI(Command Line Interface)에 관리자 사용자로 로그인합니다.



참고: 이 섹션에서 언급한 파일이 시스템에 아직 없을 수 있습니다.

이 sudo openssl req -in server.csr -pubkey -noout -outform pem | sha256sum 명령은 Certificate Signing Request 파일에서 공개 키의 SHA-256 체크섬을 출력합니다.

이 sudo openssl pkey -in server_key.pem -pubout -outform pem | sha256sum명령은 개인 키 파일에서 공개 키의 SHA-256 체크섬을 출력합니다.

이 sudo openssl x509 -in server_cert.pem -pubkey -noout -outform pem | sha256sum명령은 발급된 인증서 파일에서 공개 키의 SHA-256 체크섬을 출력합니다.

인증서 및 개인 키 출력이 일치해야 합니다. CSR (Certificate Signing Request) 가 사용 되지 않은 경우 server_cert.pem 파일은 존재하지 않습니다.

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

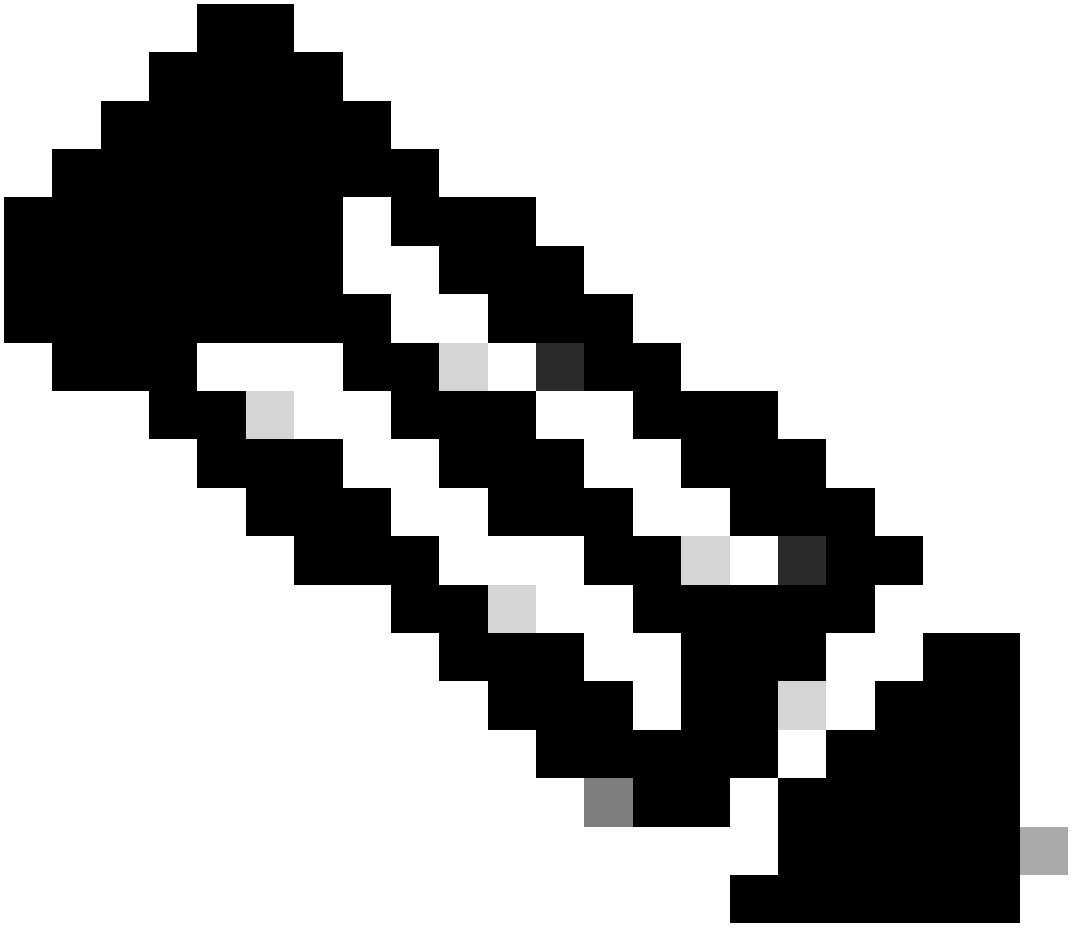
개인 키가 암호로 보호되어 있지 않은지 확인

CTB Manager에 admin 사용자로 로그인합니다. 명령을 ssh-keygen -yf server_key.pem 실행합니다.

개인 키에 암호가 필요하지 않은 경우 암호가 요청되지 않습니다.

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

인증서 및 개인 키가 PEM으로 인코딩되었는지 확인합니다.



참고: 이러한 검증은 인증서를 설치하기 전에 수행할 수 있습니다.

CTB Manager에 admin 사용자로 로그인합니다.

명령을 사용하여 server_cert.pem 파일 내용을 sudo cat server_cert.pem 봅니다. 명령을 인증서 파일 이름으로 조정합니다.

파일의 첫 줄과 마지막 줄은 각각 -----**BEGIN CERTIFICATE**----- 및-----END CERTIFICATE----- 이어야 합니다.

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

명령을 사용하여 server_key.pem 파일을 sudo cat server_key.pem 봅니다. 명령을 개인 키 파일 이름으로 조정합니다.

파일의 첫 줄과 마지막 줄은 각각 -----**BEGIN PRIVATE KEY**----- 및-----END PRIVATE KEY----- 이어야 합니다.

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

자체 서명 인증서

자체 서명 인증서 생성

- SSH(Secure Shell)를 통해 CTB Manager에 로그인합니다. 설치 중에 구성된 사용자는 대개 "admin" 사용자입니다.

- 명령을 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} 실행합니다.

  - 2048, rsa:{key_len}4096, 8192와 같이 선택한 개인 키 길이로 변경

    - CTB 관리자 {ctb_manager_ip}노드의 IP로 를 변경합니다

```
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:~$
```

- server_cert.pem 파일을 cat server_cert.pem 명령으로 보고 내용을 버퍼에 복사하여 원하는 텍스트 편집기로 로컬 워크스테이션에 붙여넣을 수 있습니다. 파일을 저장하십시오. 디렉토리에서 이러한 파일을 SCP할 수도 /home/admin 있습니다.

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

- server_key.pem 파일을 sudo cat server_key.pem 명령으로 보고 내용을 버퍼에 복사하여 로컬 워크스테이션에 선택한 텍스트 편집기로 붙여 넣을 수 있습니다. 파일을 저장하십시오. 디렉터리에서 이 파일을 SCP할 수도 /home/admin 있습니다.

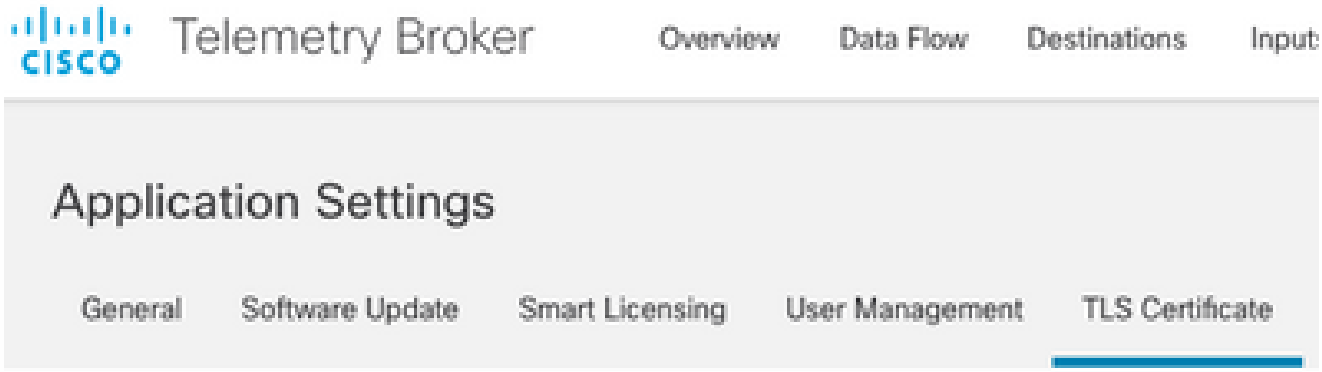
```
admin@ctb-manager:~$ sudo cat server_key.pem
-----BEGIN PRIVATE KEY-----
{removed_for_brevity}
-----END PRIVATE KEY-----
admin@ctb-manager:~$
```

자체 서명 인증서 업로드

1. CTB Manager 웹 UI로 이동하여 관리자 사용자로 로그인하고 기어 아이콘을 클릭하여 "Settings"에 액세스합니다.

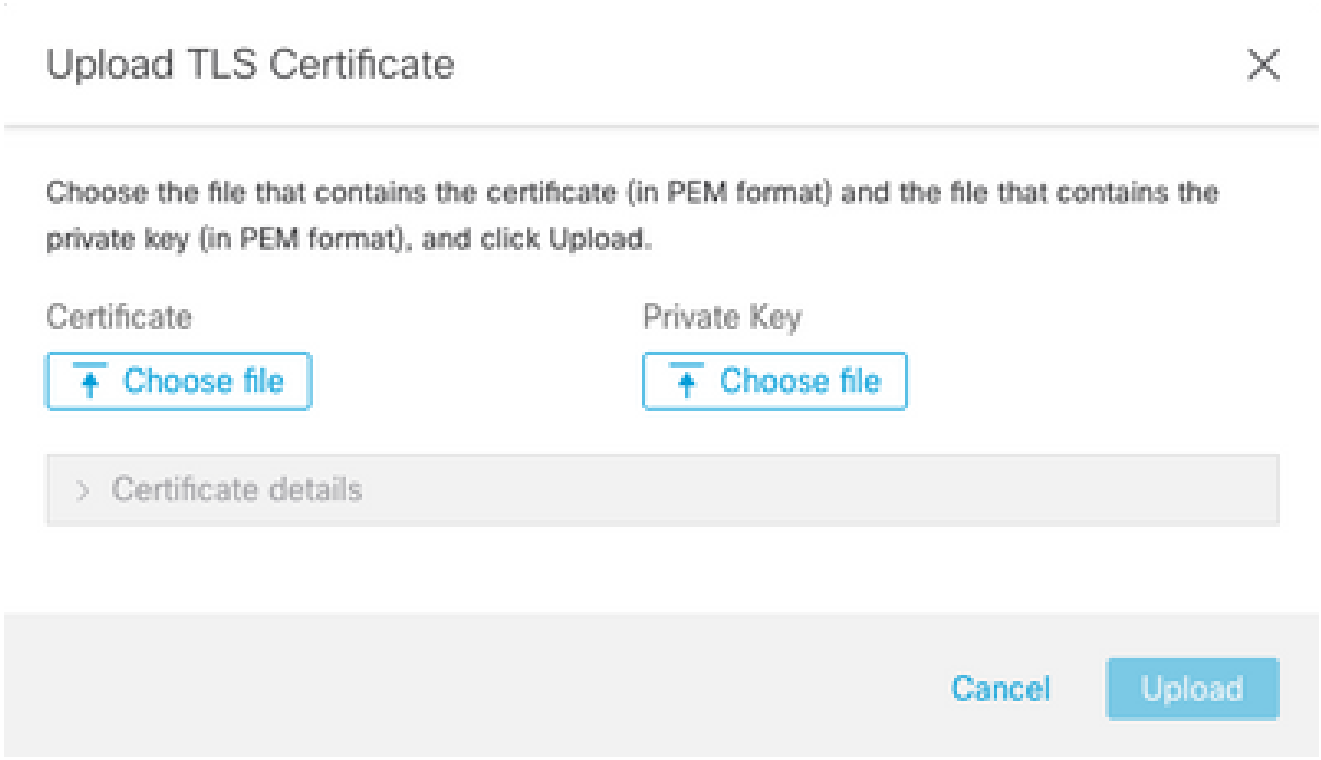
CTB 설정 아이콘

- "TLS Certificate(TLS 인증서)" 탭으로 이동합니다.

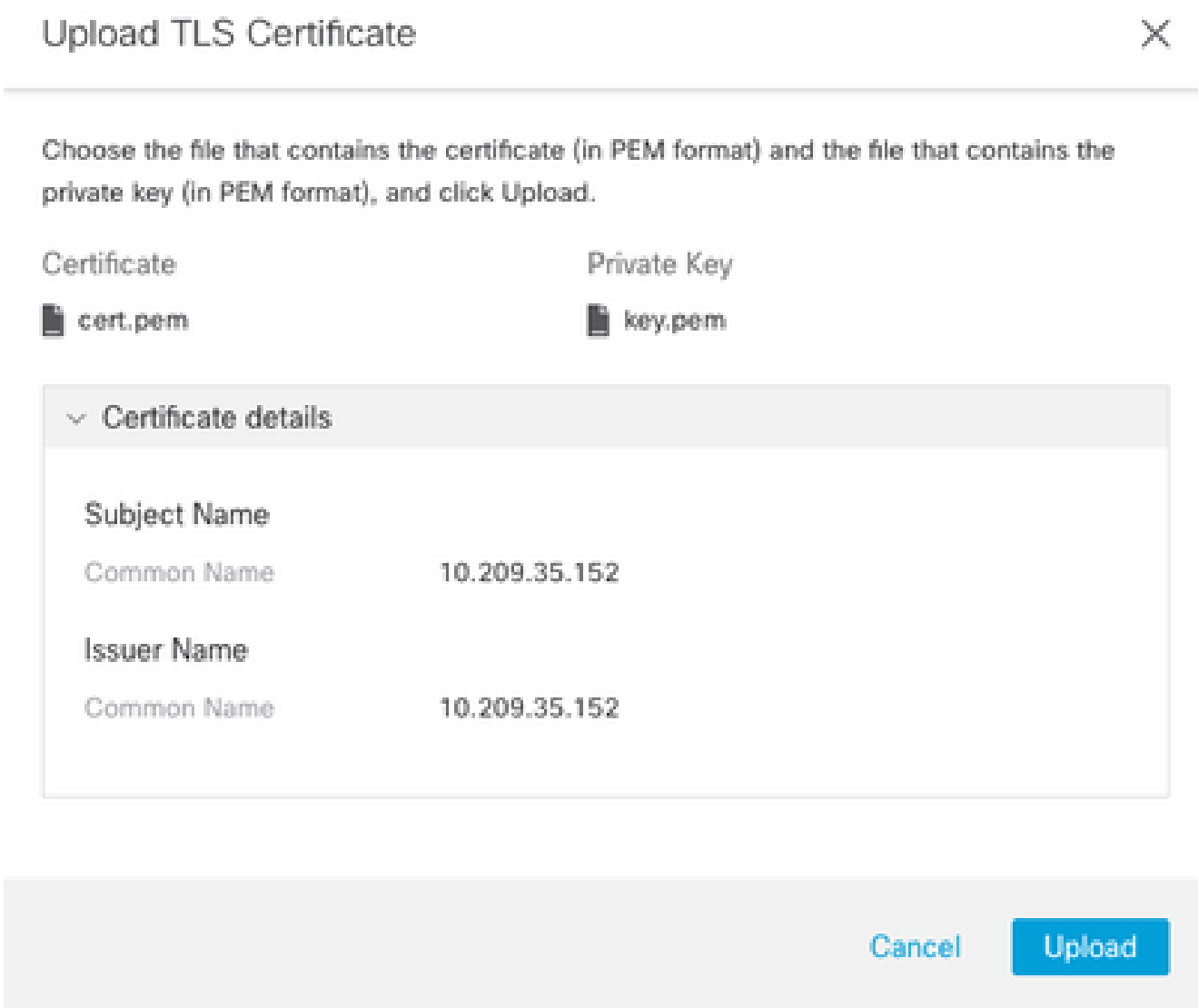


CTB 인증서 탭

- Upload TLS Certificate "Upload TLS Certificate(TLS 인증서 업로드)" 대화 상자에서 인증서 server_cert.pem 및 개인 키에 server_key.pem 대한 및 를 각각 선택한 다음 선택합니다. 파일이 선택되면 업로드를 선택합니다.



- 파일이 선택되면 확인 프로세스에서 인증서와 키 조합을 확인하고 발급자와 주체의 일반 이름을 표시합니다(그림 참조).



CTB 인증서 업로드

- "Upload(업로드)" 버튼을 선택하여 새 인증서를 업로드합니다. 웹 UI가 몇 분 후에 자동으로 다시 시작되고 다시 시작된 후 디바이스에 다시 로그인됩니다.

- CTB Manager Node 웹 콘솔에 로그인하고 로 이동하여 새 만료일과 같은 인증서 세부사항Settings > TLS Certificate 을 보거나 브라우저를 사용하여 인증서 세부사항을 보고 일련 번호와 같은 자세한 정보를 봅니다.

Broker 노드 업데이트

CTB 관리자 노드에 새 ID 인증서가 있으면 각 CTB 브로커 노드를 수동으로 업데이트해야 합니다.

1. ssh를 통해 각 broker 노드에 로그인하고 명령을 sudo ctb-manage 실행합니다

```
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:
```

- 메시지가 표시되면 옵션c을 선택합니다.

```
== 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
```

- 서명된 인증서의 값과 일치하는 경우 인증서 세부 정보를 확인하고 인증서를 수락하도록 선택합니다. 서비스 **y** 가 자동으로 시작되고 서비스가 시작되면 프롬프트가 반환됩니다. 서비스 시작은 완료하는 데 약 15분이 걸릴 수 있습니다.

```
== 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
```

CA(Certificate Authority) 발급 인증서

인증 기관에서 발급할 CSR(Certificate Signing Request) 생성

- SSH(Secure Shell)를 통해 CTB Manager에 로그인합니다. 설치 중에 구성된 사용자는 대개 "admin" 사용자입니다.

- 명령을 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 실행합니다. 원하는 경우 마지막 두 행의 'extra' 특성을 비워 둘 수 있습니다.

  - CTB Manager 노드의 DNS 이름{ctb_manager_dns_name} 으로 를 변경합니다

    - CTB 관리자 {ctb_manager_ip}노드의 IP로 를 변경합니다

    - 2048, {key_len} 4096, 8192와 같이 선택한 개인 키 길이로 를 변경합니다.

```
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 및 키 파일을 로컬 머신에 SCP하고 CSR을 CA에 제공합니다. CA가 PEM 형식으로 CSR을 발급하는 것은 이 문서의 범위를 벗어납니다.

체인으로 인증서 만들기

CA는 PEM 형식으로 서버 ID 인증서를 발급합니다. 모든 체인 인증서 및 CTB 관리자 노드의 서버 ID 인증서가 포함된 체인 파일을 만들어야 합니다.

텍스트 편집기에서는 이전 단계에서 서명된 인증서를 결합하고, 신뢰할 수 있는 CA를 포함하여 체인의 모든 인증서를 표시된 순서대로 PEM 형식의 단일 파일에 추가하여 파일을 생성합니다.

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

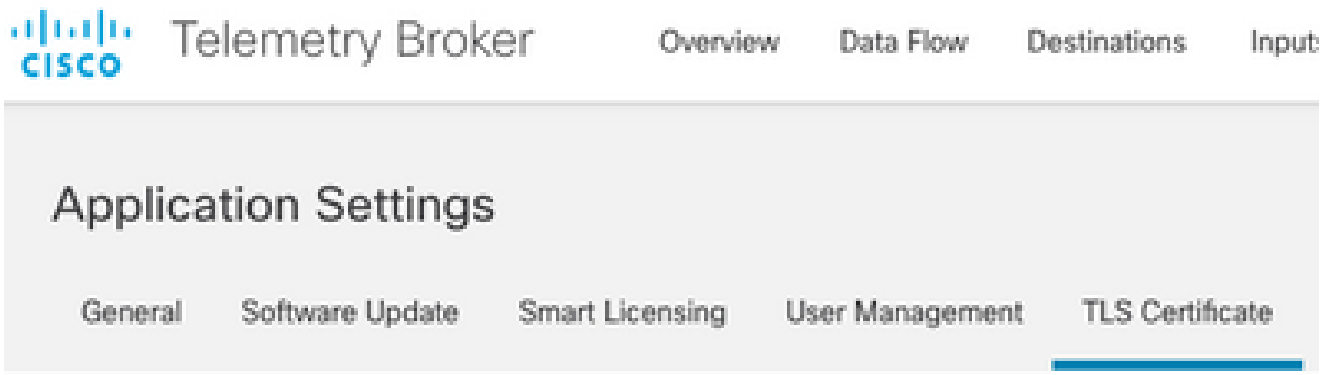
체인 파일이 있는 이 새 인증서 파일에 선행 또는 후행 공백, 빈 줄이 없고 위에 표시된 순서대로 있어야 합니다.

인증 기관 발급 인증서 업로드

1. CTB Manager 웹 UI로 이동하여 관리자로 로그인하고 기어 아이콘을 클릭하여 "Settings"에 액세스합니다.

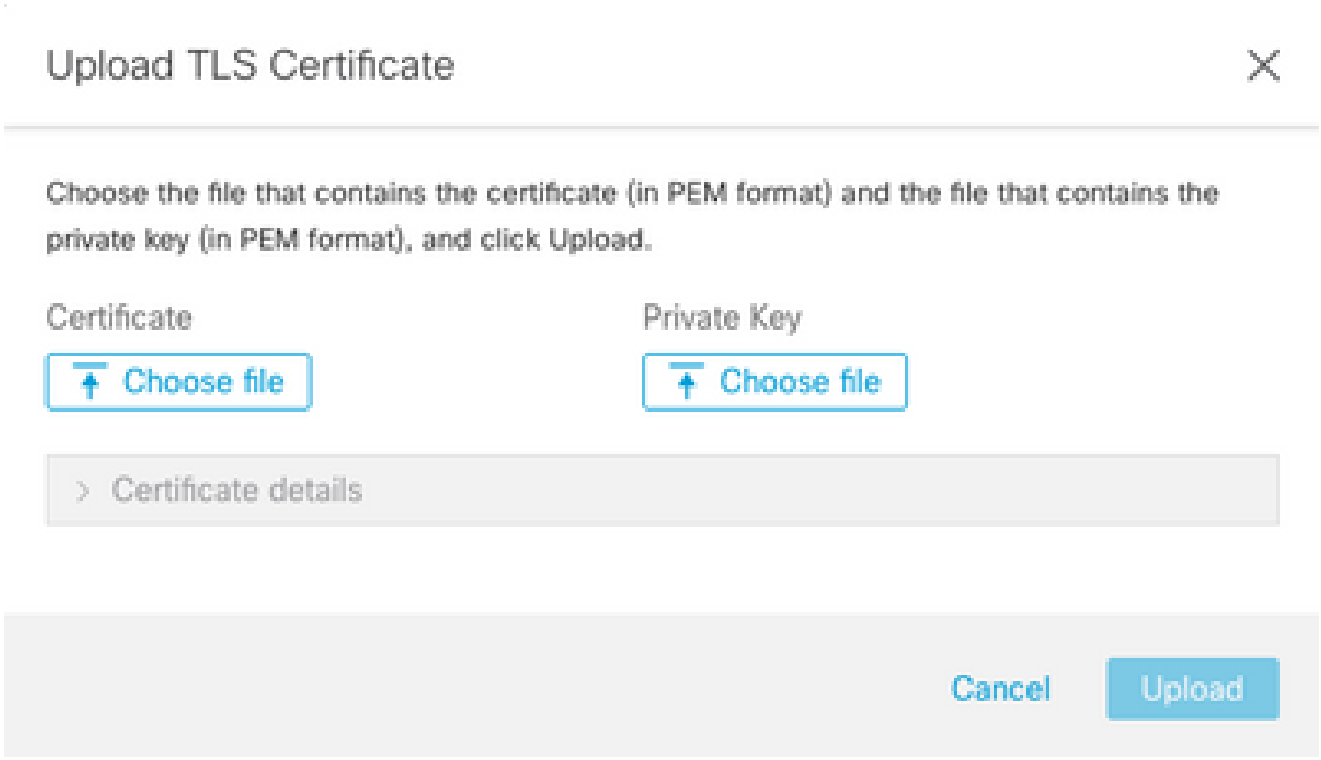
CTB 설정 아이콘

- "TLS Certificate(TLS 인증서)" 탭으로 이동합니다.

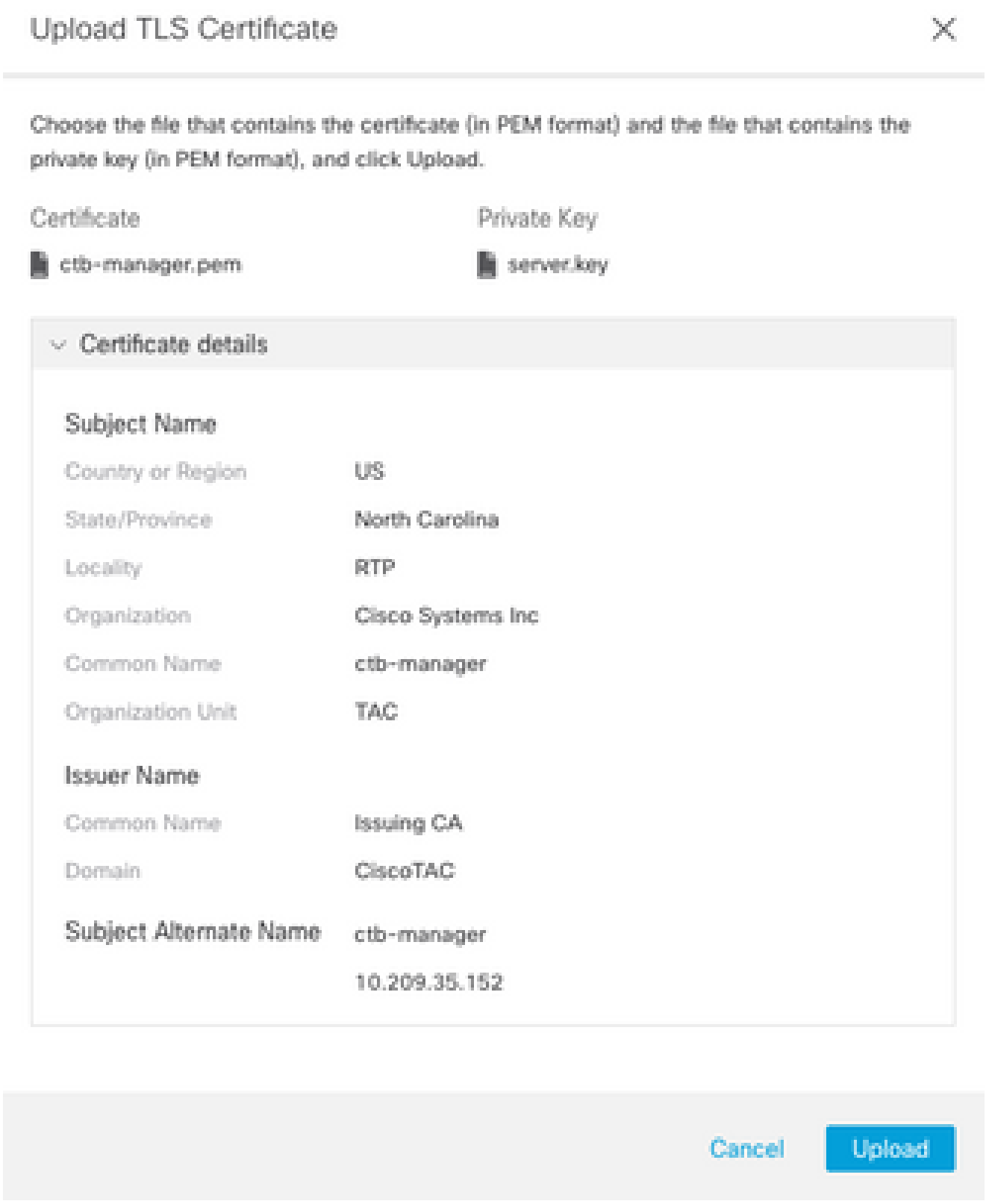


CTB 인증서 탭

- "Upload TLS Certificate TLS 인증서 업로드" 대화 상자에서 마지막 섹션에서 생성된 체인 파일이 있는 인증서와 인증서 및 개인 키에 server_key.pem 대해 생성된 CTB 관리자를 각각 선택한 다음 파일이 선택되면 업로드를 선택합니다.



- 파일이 선택되면, 검증 프로세스가 인증서 및 키 조합을 확인하고 아래와 같이 발급자 및 주체의 일반 이름을 표시합니다
.



CTB CA 발급 인증서 검증

- "Upload(업로드)" 버튼을 선택하여 새 인증서를 업로드합니다. 웹 UI가 약 60초 후에 자체적으로 다시 시작되며, 다시 시작된 후 웹 UI에 로그인합니다.

- CTB Manager Node 웹 콘솔에 로그인하고 로 이동하여 새 만료일과 같은 인증서 세부사항Settings > TLS Certificate 을 보

거나 브라우저를 사용하여 인증서 세부사항을 보고 일련 번호와 같은 자세한 정보를 봅니다.

Broker 노드 업데이트

CTB 관리자 노드에 새 ID 인증서가 있으면 각 CTB 브로커 노드를 수동으로 업데이트해야 합니다.

1. ssh를 통해 각 broker 노드에 로그인하고 명령을 sudo ctb-manage 실행합니다

```
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:
```

- 메시지가 표시되면 옵션c을 선택합니다.

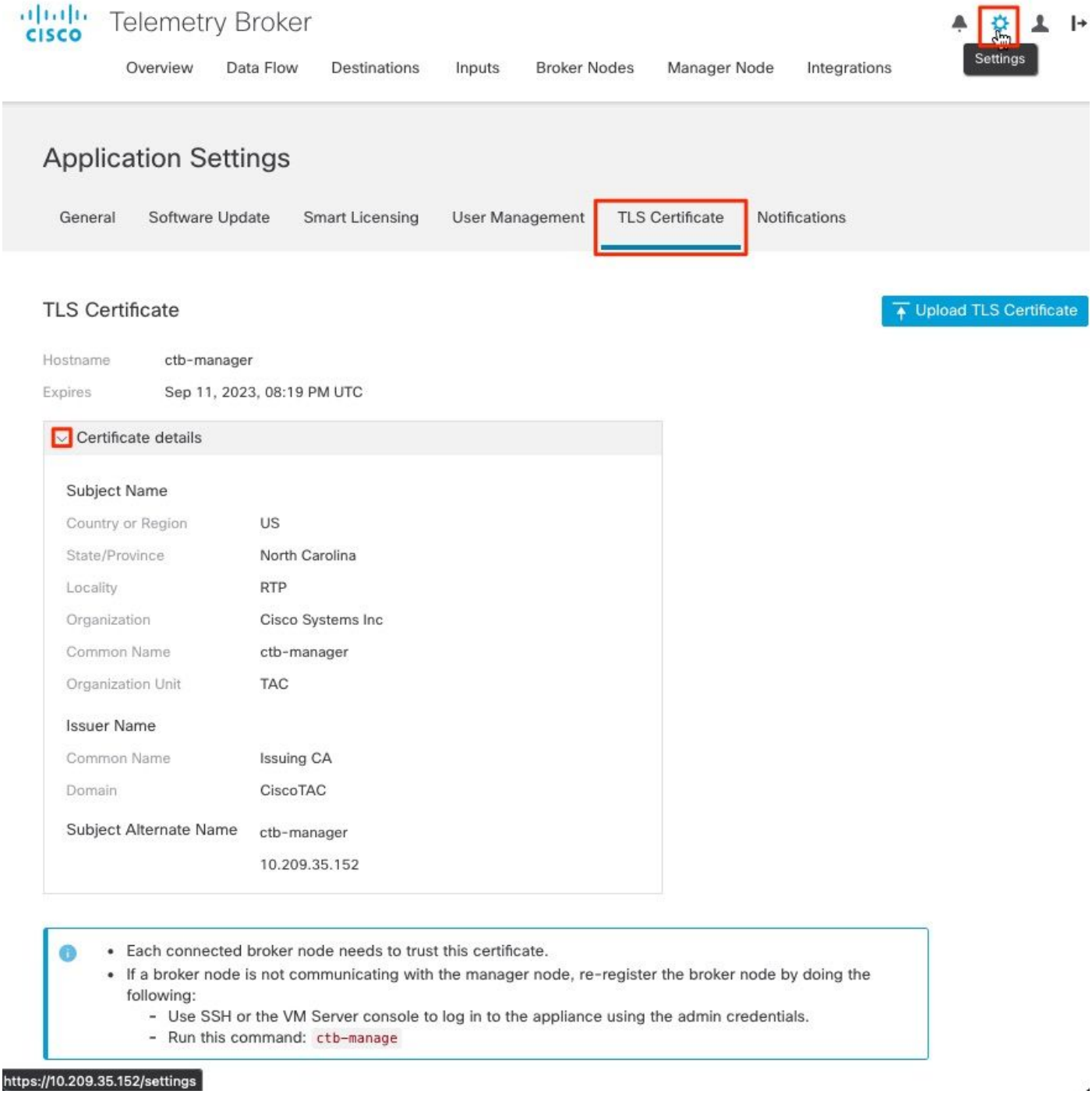
```
== Management Configuration

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
```

- 인증서 세부사항이 서명된 인증서의 값과 일치하는지 확인하고 인증서를 승인하도록 선택합니다y. 서비스가 자동으로 시작되고 서비스가 시작되면 프롬프트가 반환됩니다. 서비스 시작은 완료하는 데 약 15분이 걸릴 수 있습니다.

```
== 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
```

다음을 확인합니다.

CTB Manager Node 웹 콘솔에 로그인하고 로 이동하여 새 만료일과 같은 인증서 세부사항Settings > TLS Certificate 을 보거나 브라우저를 사용하여 인증서 세부사항을 보고 일련 번호와 같은 자세한 정보를 봅니다.



CTB 인증서 세부사항

CTB Manager 노드 웹 UI에서 CTB Broker 노드에 경보가 표시되지 않는지 확인합니다.

문제 해결

인증서가 불완전할 경우 체인 인증서가 없으면 CTB Broker 노드 노드가 관리자 노드와 통신할 수 없으며 Broker 노드 목록의 Status 열에 "Not Seen Since"가 표시됩니다.
Broker 노드는 이 상태에서 계속해서 트래픽을 복제하고 배포합니다.

CTB 관리자 노드 CLI에 로그인하고 명령을 실행하여 sudo grep -ic begin /var/lib/titan/titanium_frontend/ssl/cert.pem cert.pem 파일에 있는 인증서 수를 확인합니다.

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

반환된 출력 값은 체인에 있는 CA 디바이스 수와 CTB Manager를 합한 값과 같아야 합니다.

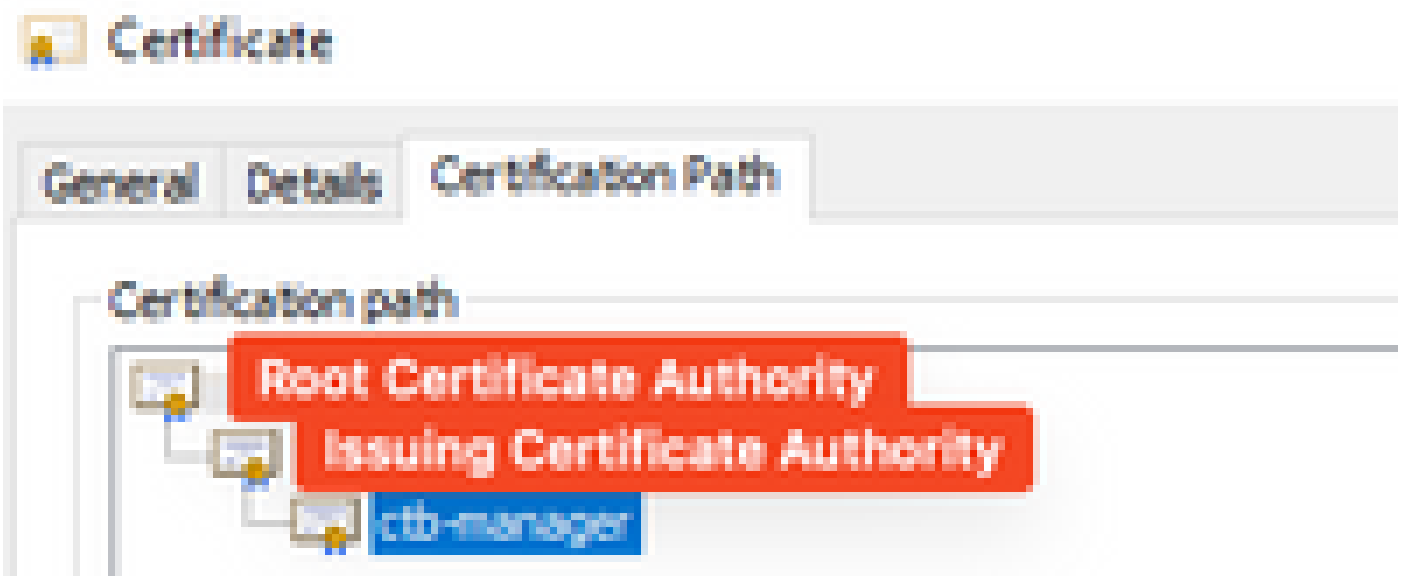
자체 서명 인증서를 사용하는 경우 1의 출력이 예상됩니다.

PKI 인프라가 발급 CA이기도 한 단일 루트 CA로 구성된 경우 2의 출력이 예상됩니다.

PKI 인프라가 루트 CA와 발급 CA로 구성된 경우 3의 출력이 예상됩니다.

PKI 인프라가 루트 CA, 하위 CA 및 발급 CA로 구성된 경우 4의 출력이 예상됩니다.

다음과 같은 다른 애플리케이션에서 인증서를 볼 때 표시되는 PKI와 출력을 Microsoft Windows Crypto Shell Extensions비교합니다.



PKI 인프라

이 그림에서 PKI 인프라는 루트 CA와 발급 CA를 포함합니다.

이 시나리오에서 명령의 출력 값은 3이 됩니다.

출력이 기대에 미치지 못할 경우 Create **a Certificate with Chain(**체인으로 인증서 **생성) 섹션**의 단계를 검토하여 인증서가 누락되었는지 확인합니다.

인증서를 볼 때 Microsoft Windows Crypto Shell Extensions 로컬 시스템에 인증서를 확인할 수 있는 충분한 정보가 없으면 일부 인증서가 제공되지 않을 수 있습니다.

CLI에서 sudo ctb-mayday 명령을 실행하여 TAC에서 검토할 수 있는 5일 번들을 생성합니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.