替換遙測代理身份證書

目錄

簡介

本文檔介紹如何替換Cisco Telemetry Broker (CTB)管理器節點上的伺服器身份證書。

必要條件

需求

思科建議您瞭解以下主題：

- Cisco Telemetry Broker裝置管理
- x509憑證

採用元件

本文檔中使用的裝置運行的是2.0.1版

- 思科遙測代理管理器節點
- 思科遙測代理節點

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

設定

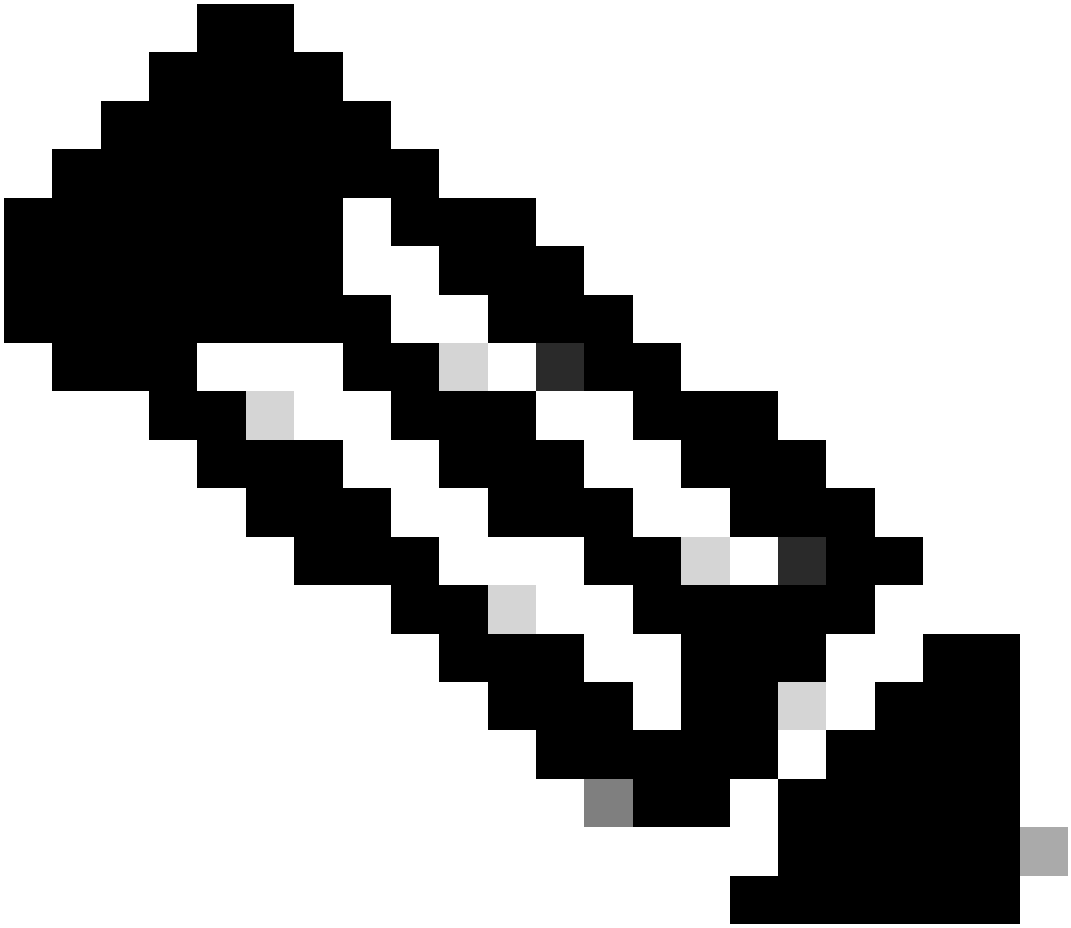
憑證需求

思科遙測代理管理器使用的x509證書必須滿足以下要求：

- 證書和私鑰必須是匹配的對
- 憑證和私密金鑰必須以PEM編碼
- 私密金鑰不得有密碼保護

確認證書和私鑰是匹配對

以admin使用者身份登入到CTB Manager命令列介面(CLI)。



注意：系統中可能還不存在本節中提到的檔案。

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

命令從證書簽名請求檔案中輸出公鑰的SHA-256校驗和。

sudo openssl pkey -in server_key.pem -pubout -outform pem | sha256sum命令從私鑰檔案中輸出公鑰的SHA-256校驗和。

sudo openssl x509 -in server_cert.pem -pubkey -noout -outform pem | sha256sum命令從發出的證書檔案中輸出公鑰的SHA-256校驗和。

憑證和私密金鑰輸出必須相符。如果未使用證書簽名請求，則server_cert.pem檔案不存在。

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

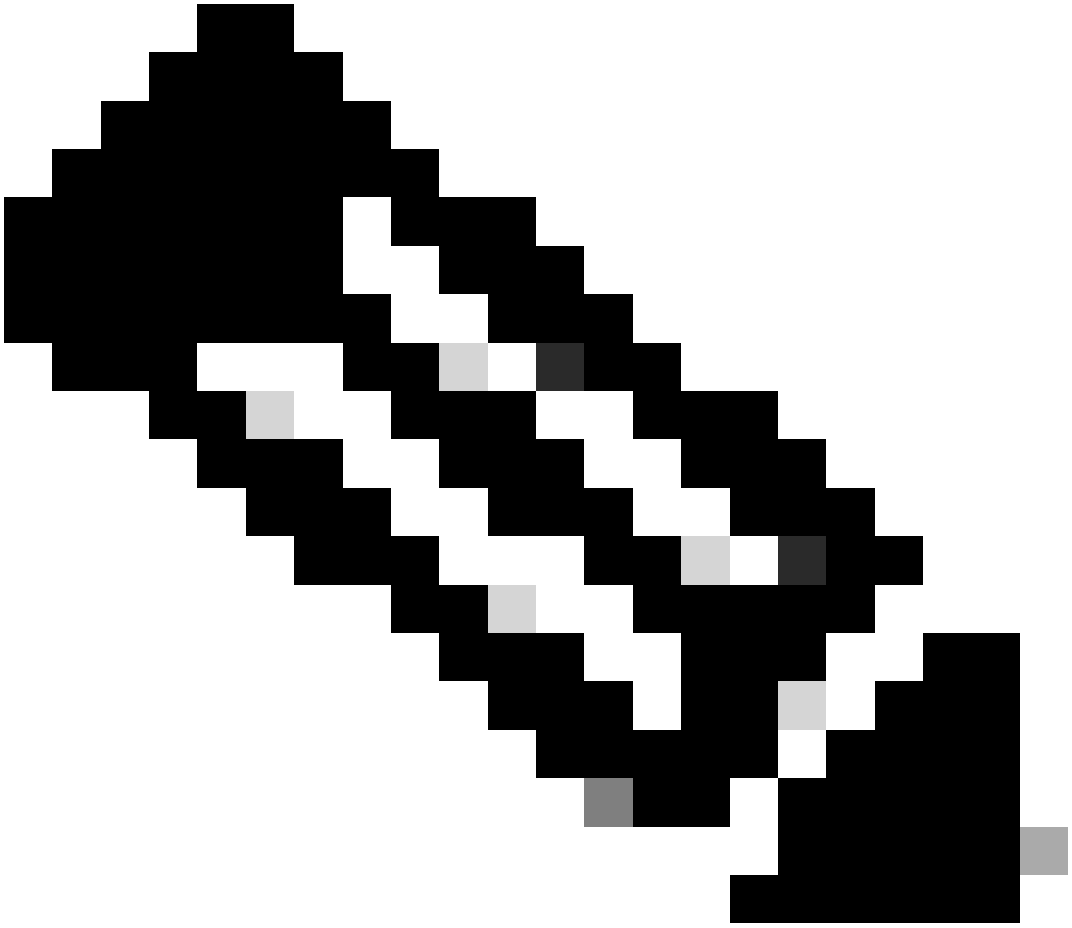
確認私密金鑰未受密碼保護

以admin使用者身份登入到CTB管理器。運行ssh-keygen -yf server_key.pem命令。

如果私密金鑰不需要密碼，則不會要求密碼。

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

確認證書和私鑰是PEM編碼的



注意：這些驗證可以在安裝證書之前執行。

以admin使用者身份登入到CTB管理器。

使用sudo cat server_cert.pem 命令檢視server_cert.pem檔案內容。將命令調整為您的證書檔名。

檔案的第一行與最後一行應分別是 -----**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命令檢視server_key.pem檔案。將命令調整為您的私鑰檔名。

檔案的第一行與最後一行應分別是 -----**BEGIN PRIVATE KEY**----- 和-----END PRIVATE KEY-----。

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

自簽名證書

生成自簽名證書

- 以安裝期間配置的使用者身份透過SSH（安全外殼）登入到CTB管理器，通常為「管理員」使用者。

- 發出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。

  - 使用您選擇的私鑰長度（例如2048、4096或8192）更改rsa:{key_len}

    - 使用CTB Manager節點的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命令檢視server_cert.pem檔案，並將內容複製到緩衝區中，以便將其貼上到本地工作站所選的文本編輯器中。儲存檔案。您也可以將這些檔案從 /home/admin 目錄中SCP出去。

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

- 使用sudo cat server_key.pem命令檢視server_key.pem檔案，並將內容複製到緩衝區中，以便將內容貼上到本地工作站所選的文本編輯器中。儲存檔案。您也可以將此檔案從目 /home/admin 錄中SCP出去。

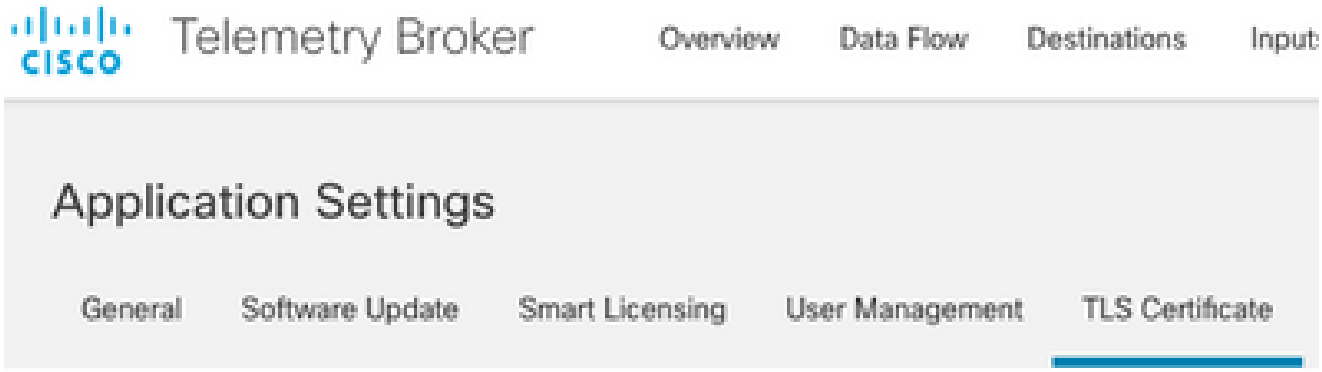
```
admin@ctb-manager:~$ sudo cat server_key.pem
-----BEGIN PRIVATE KEY-----
{removed_for_brevity}
-----END PRIVATE KEY-----
admin@ctb-manager:~$
```

上傳自簽名證書

1. 導航到CTB Manager Web UI並以管理員使用者身份登入，然後點選齒輪圖示訪問「Settings」。

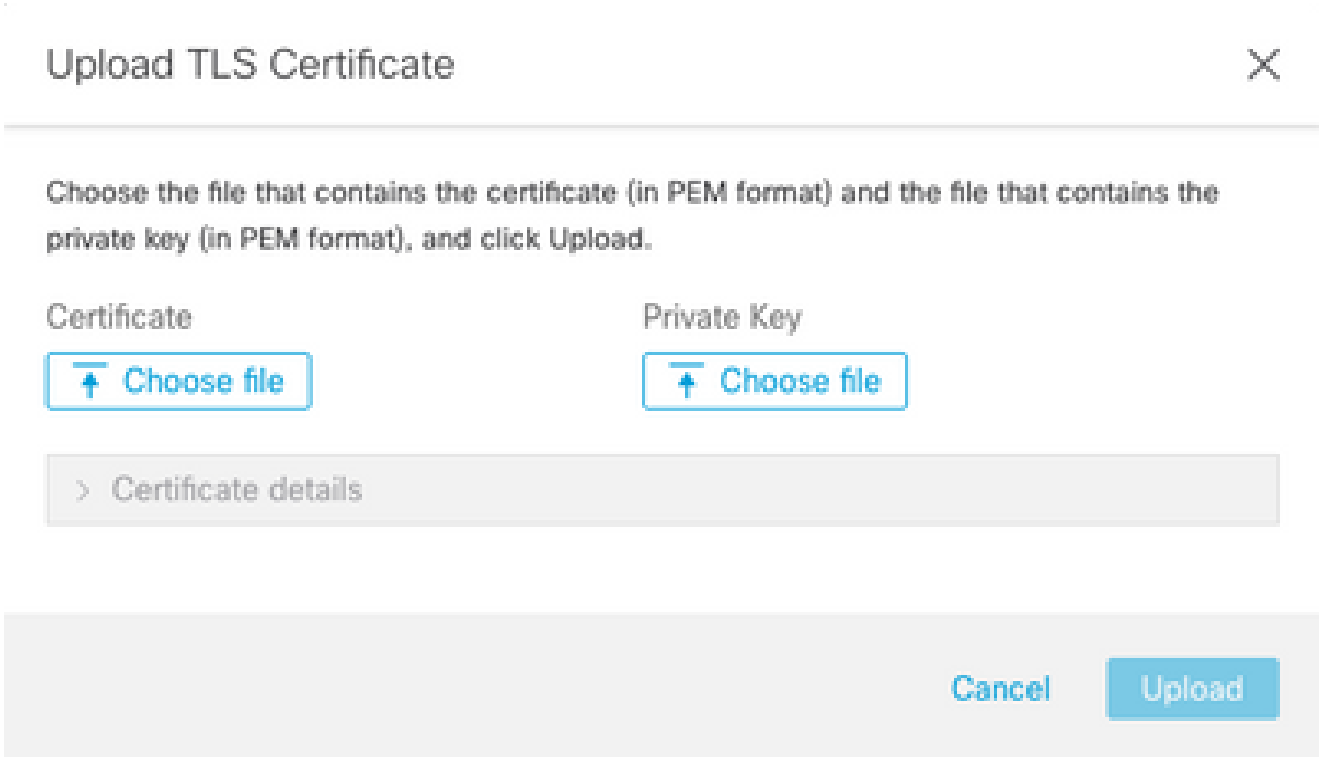
*CTB*設定圖示

- 導航到「TLS證書」頁籤。

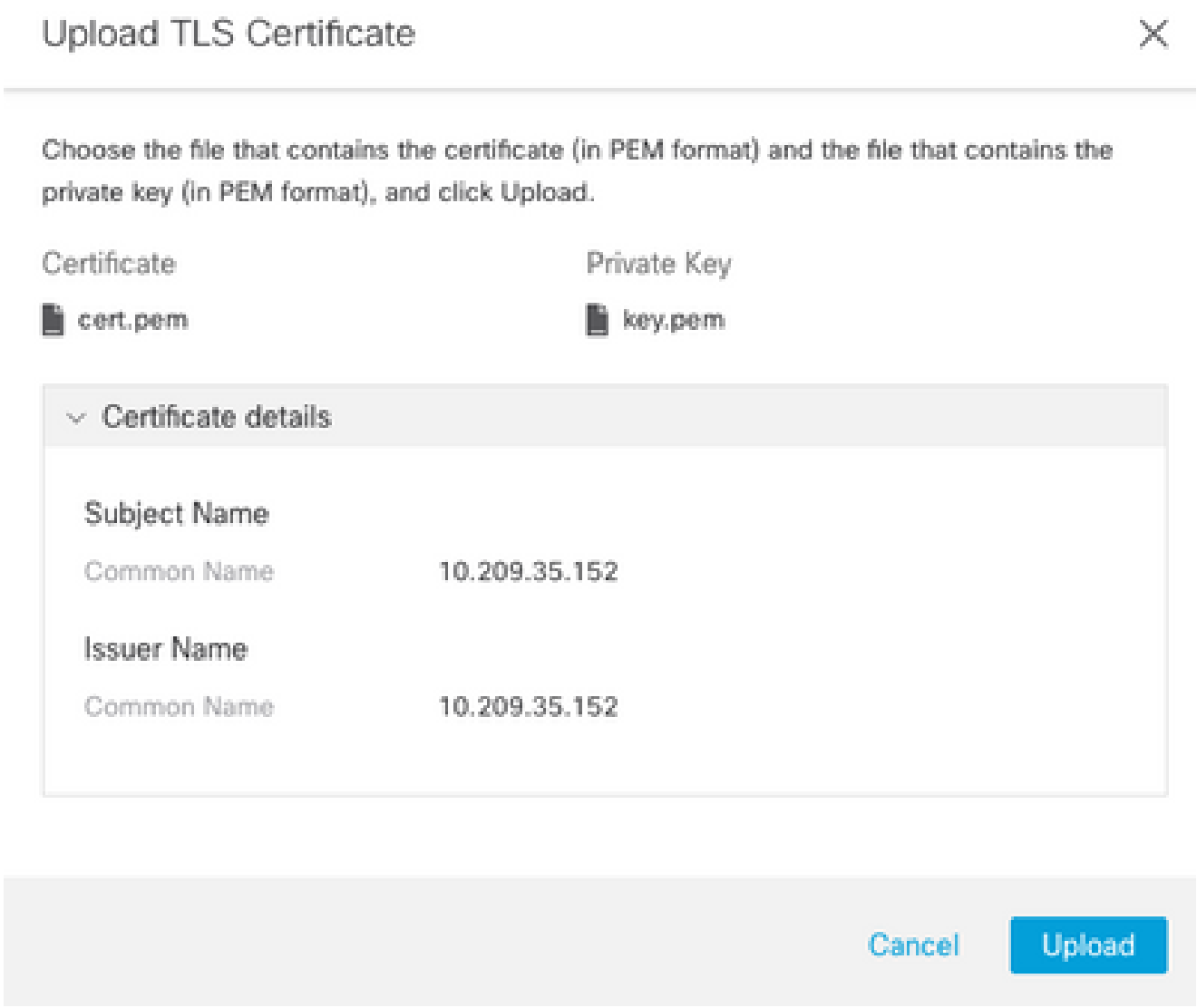


*CTB*證書頁籤

- 選擇Upload TLS Certificate ，然後在「上傳TLS證書」對話方塊中選擇server_cert.pem 和server_key.pem 分別用於證書和私鑰。選取檔案後，選取「上傳」。



- 一旦檔案被選定，驗證過程將確認證書和金鑰的組合，並顯示頒發者和主體的公用名稱，如下所示。



*CTB*證書上傳

- 選擇「上傳」按鈕以上傳新憑證。Web UI會在幾分鐘內自行重新啟動，重新啟動後再次登入裝置。

- 登入到CTB Manager節點Web控制檯並導航到Settings > TLS Certificate 以檢視證書詳細資訊（如新的到期日期），或使用瀏覽器檢視證書詳細資訊（如序列號）。

更新Broker節點

一旦CTB管理器節點擁有新的身份證書，就必須手動更新每個CTB代理節點。

1. 透過ssh登入每個broker節點並運行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:
```

- 出現提示c時選擇選項。

```
== 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
```

- 驗證證書詳細資料（如果它們與簽名證書的值匹配），並選擇 **y** 以接受證書。服務將自動啟動，啟動服務後將返回提示。服務啟動可能需要大約15分鐘才能完成。

```
== 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
```

證書頒發機構(CA)頒發的證書

生成證書頒發機構頒發的證書簽名請求(CSR)

- 以安裝期間配置的使用者身份透過SSH（安全外殼）登入到CTB管理器，通常為「管理員」使用者。

- 發出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，可以將最後兩行上的「extra」屬性留空。

  - 使用CTB管理器節點的DNS名稱更改{ctb_manager_dns_name}

    - 使用CTB Manager節點的IP更改{ctb_manager_ip}

    - 使用您選擇的私鑰長度（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 []:
```

- 將CSR和金鑰檔案scp到本地電腦，並向CA提供CSR。CA以PEM格式發出CSR不在本檔案範圍內。

建立具有鏈結的憑證

CA以PEM格式頒發伺服器身份證書。必須建立鏈結檔案，其中包含CTB Manager節點的所有鏈結憑證和伺服器辨識憑證。

在文本編輯器中，透過組合上一步中簽名的證書並按照所示順序將鏈中的所有證書（包括受信任CA）附加到PEM格式的單個檔案中來建立檔案。

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

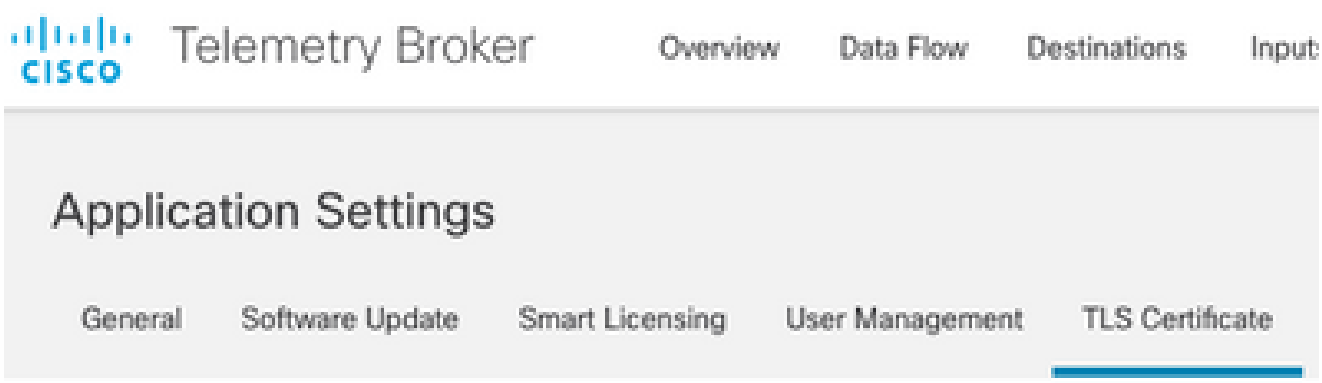
請確認這個含有鏈結檔案的新憑證檔案沒有前置或尾端空格、空白行，並且順序如上。

上載證書頒發機構頒發的證書

1. 導航到CTB Manager Web UI並以管理員身份登入，然後點選齒輪圖示以訪問「Settings」。

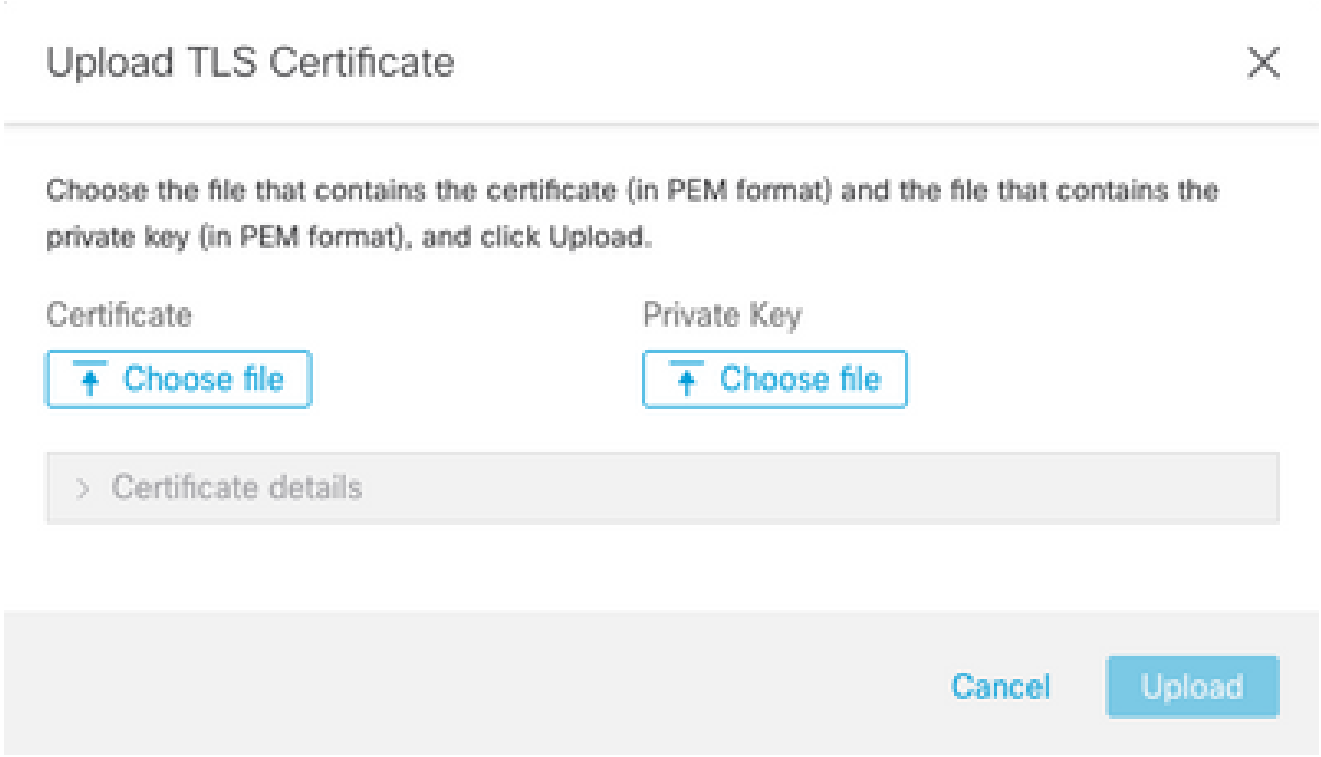
*CTB*設定圖示

- 導航到「TLS證書」頁籤。

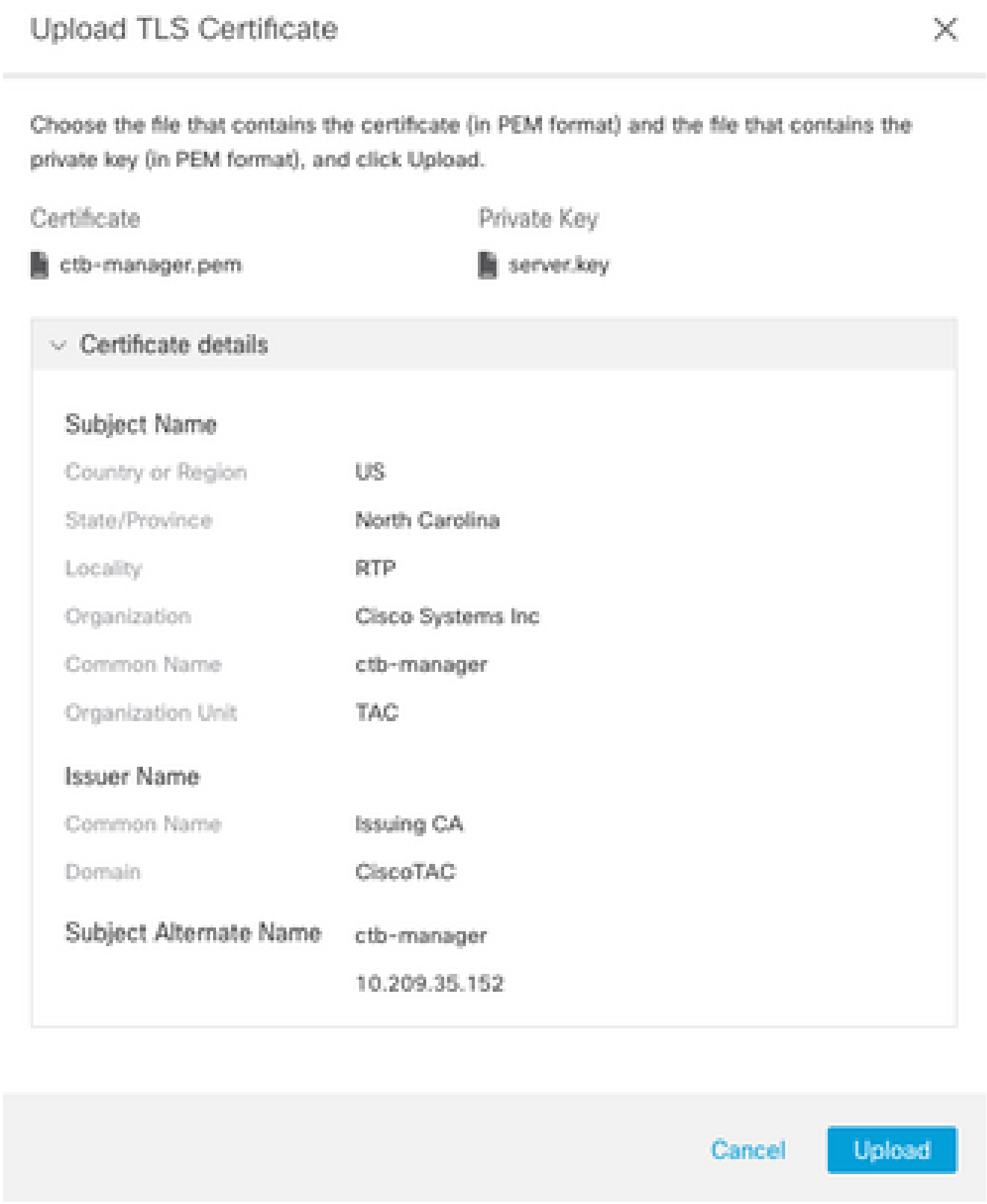


*CTB*證書頁籤

- 選擇Upload TLS Certificate ，然後選擇在最後部分建立的具有鏈結檔案的證書， server_key.pem 並在「上傳TLS證書」對話方塊中分別為證書和私鑰生成的CTB管理器。選取檔案後，選取「上傳」。



- 選擇檔案後，驗證過程將確認證書和金鑰組合，並顯示頒發者和主體的公用名稱，如下所示。



CTB CA頒發的證書驗證

- 選擇「上傳」按鈕以上傳新憑證。Web UI會在大約60秒內自行重新啟動，並在重新啟動後登入Web UI。

- 登入到CTB Manager節點Web控制檯並導航到Settings > TLS Certificate 以檢視證書詳細資訊（如新的到期日期），或使用瀏覽器檢視證書詳細資訊（如序列號）。

更新Broker節點

一旦CTB管理器節點擁有新的身份證書，就必須手動更新每個CTB代理節點。

1. 透過ssh登入每個broker節點並運行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:
```

- 出現提示c時選擇選項。

```
== 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
```

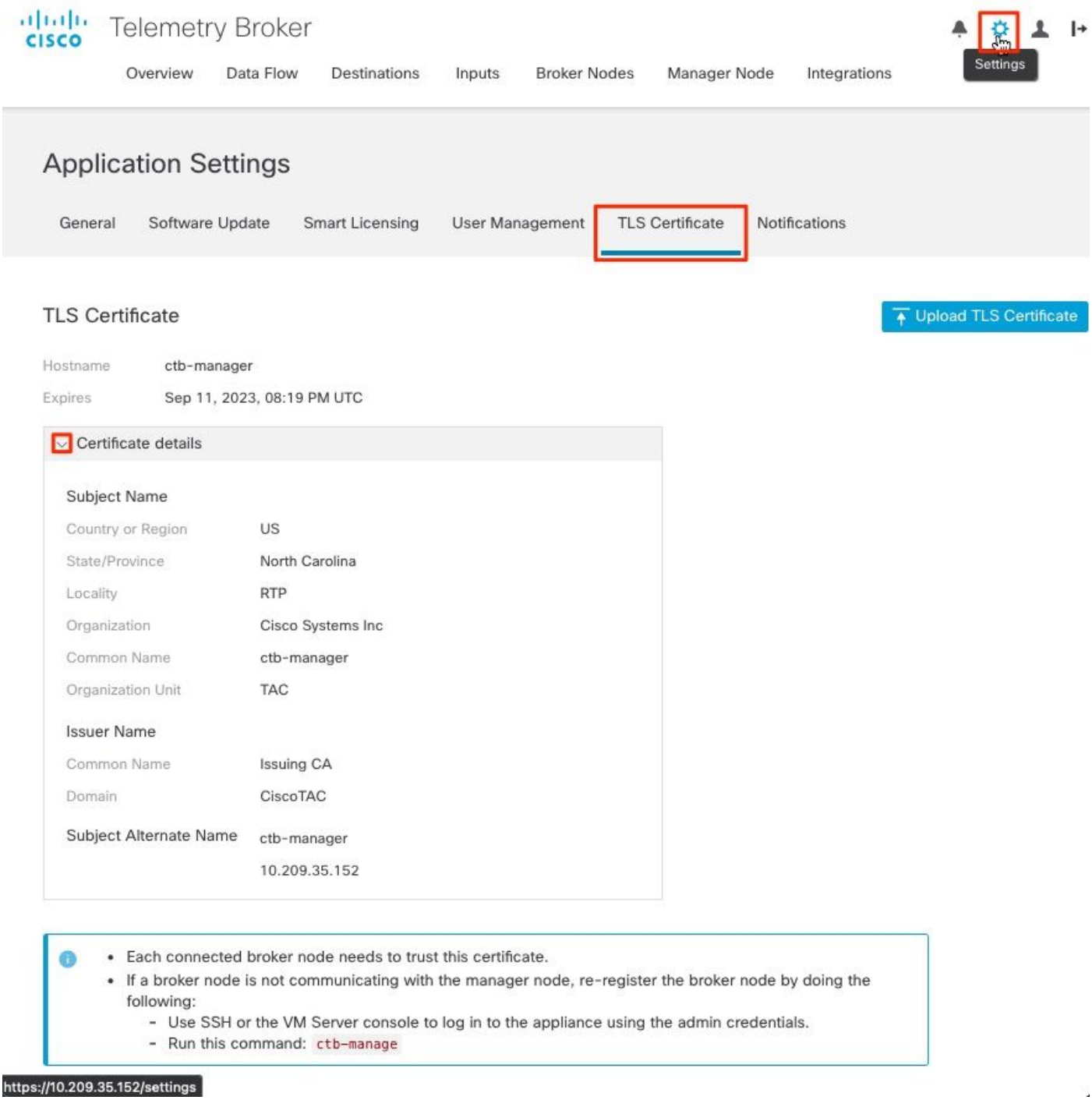
- 驗證證書詳細資料（如果它們與簽名證書的值匹配），並選擇y以接受證書。服務將自動啟動，一旦啟動服務，就會返回提示。服務啟動可能需要大約15分鐘才能完成。

```
== 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
```

驗證

登入到CTB Manager節點Web控制檯並導航到Settings > TLS Certificate 以檢視證書詳細資訊（如新的到期日期），或使用瀏覽器檢視證書詳細資訊（如序列號）。



*CTB*證書詳細資訊

驗證CTB代理節點在CTB管理器節點Web UI中未顯示警報。

疑難排解

如果憑證不完整（例如缺少鏈結憑證），CTB Broker Node節點就無法與Manager Node通訊，並在Broker Nodes清單的Status欄中顯示「Not Seen Since」。
Broker節點將繼續複製和分發處於此狀態的流量。

登入CTB Manager節點CLI並發出sudo grep -ic begin /var/lib/titan/titanium_frontend/ssl/cert.pem 命令，檢視cert.pem檔案中的證書數量。

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

返回的輸出值需要等於鏈中的CA裝置數加上CTB管理器。

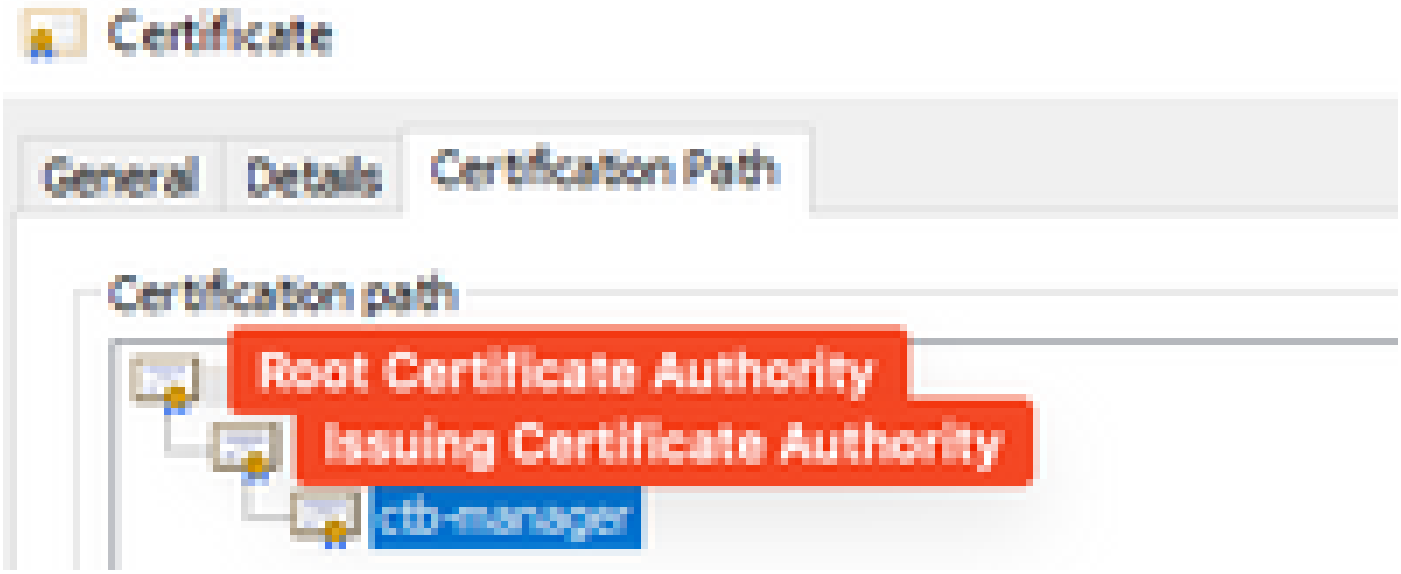
如果使用自簽名證書，則應為1的輸出。

如果PKI基礎設施包含也作為頒發CA的單個根CA，則預期輸出2。

如果PKI基礎設施包含根CA和頒發CA，則預期輸出3。

如果PKI基礎設施由根CA、從屬CA和頒發CA組成，則預期輸出4。

在其他應用程式(如 Microsoft Windows Crypto Shell Extensions)中檢視證書時，將輸出與列出的PKI進行比較。



*PKI*基礎設施

在此圖中，PKI基礎設施包括根CA和頒發CA。

在此案例中，指令的輸出值預期為3。

如果輸出未達到預期，請檢視**建立帶鏈的證書**部分中的步驟，以確定證書是否缺失。

在檢視憑證時，Microsoft Windows Crypto Shell Extensions 如果本機電腦沒有足夠資訊來驗證憑證，則可能無法顯示所有憑證。

從CLI發出sudo ctb-mayday 命令，生成用於TAC檢查的五月天捆綁包。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。