إستبدال شهادة هوية وسيط بيانات تتبع الاستخدام

المحتويات

المقدمة

يوضح هذا المستند كيفية إستبدال شهادة هوية الخادم على عقدة إدارة وسيط بيانات تتبع إستخدام البيانات (CTB) من Cisco.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- إدارة جهاز وسيط بيانات تتبع الاستخدام من Cisco
- شهادات x509

المكونات المستخدمة

تقوم الأجهزة المستخدمة لهذا المستند بتشغيل الإصدار 2.0.1

- عقدة مدير وسيط بيانات تتبع الاستخدام من Cisco
- عقدة وسيط بيانات تتبع الاستخدام من Cisco

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

التكوين

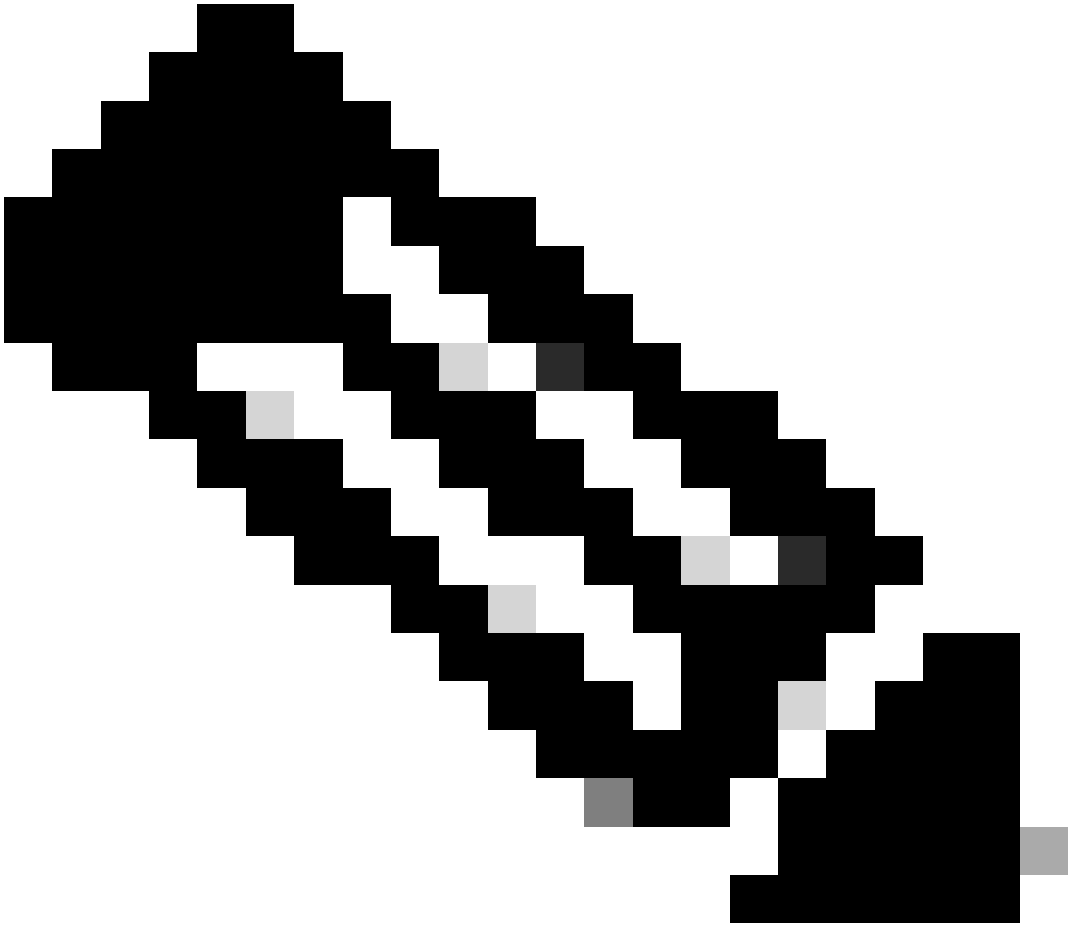
متطلبات الشهادة

يجب أن تستوفي شهادة X509 التي يستخدمها مدير وسيط بيانات تتبع إستخدام البيانات من Cisco هذه المتطلبات:

- يجب أن يكون CERT و Private Key زوج مطابق
- يجب أن تكون الشهادة والمفتاح الخاص مرمزين بتشفير PEM
- يجب عدم حماية عبارة المرور للمفتاح الخاص

تأكيد الشهادة والمفتاح الخاص هما زوجان متطابقان

سجل الدخول إلى واجهة سطر الأوامر (CLI) الخاصة ب CTB Manager كمستخدم مسؤول.



ملاحظة: من الممكن ألا تكون الملفات المذكورة في هذا القسم موجودة على النظام بعد.

ينتج sudo openssl req -in server.csr -pubkey -noout -outform pem | sha256sum الأمر المجموع الاختباري للمفتاح العام SHA-256 من ملف طلب توقيع الشهادة.

ينتج sudo openssl pkey -in server_key.pem -pubout -outform pem | sha256sum الأمر المجموع الاختباري للمفتاح العام SHA-256 من ملف المفتاح الخاص.

ينتج sudo openssl x509 -in server_cert.pem -pubkey -noout -outform pem | sha256sum الأمر المجموع الاختباري للمفتاح العام SHA-256 من ملف الشهادات الصادر.

يجب أن تتطابق إخراج الشهادة والمفتاح الخاص. إذا لم يتم استخدام "طلب توقيع الشهادة"، فإن ملف server_cert.pem غير موجود.

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

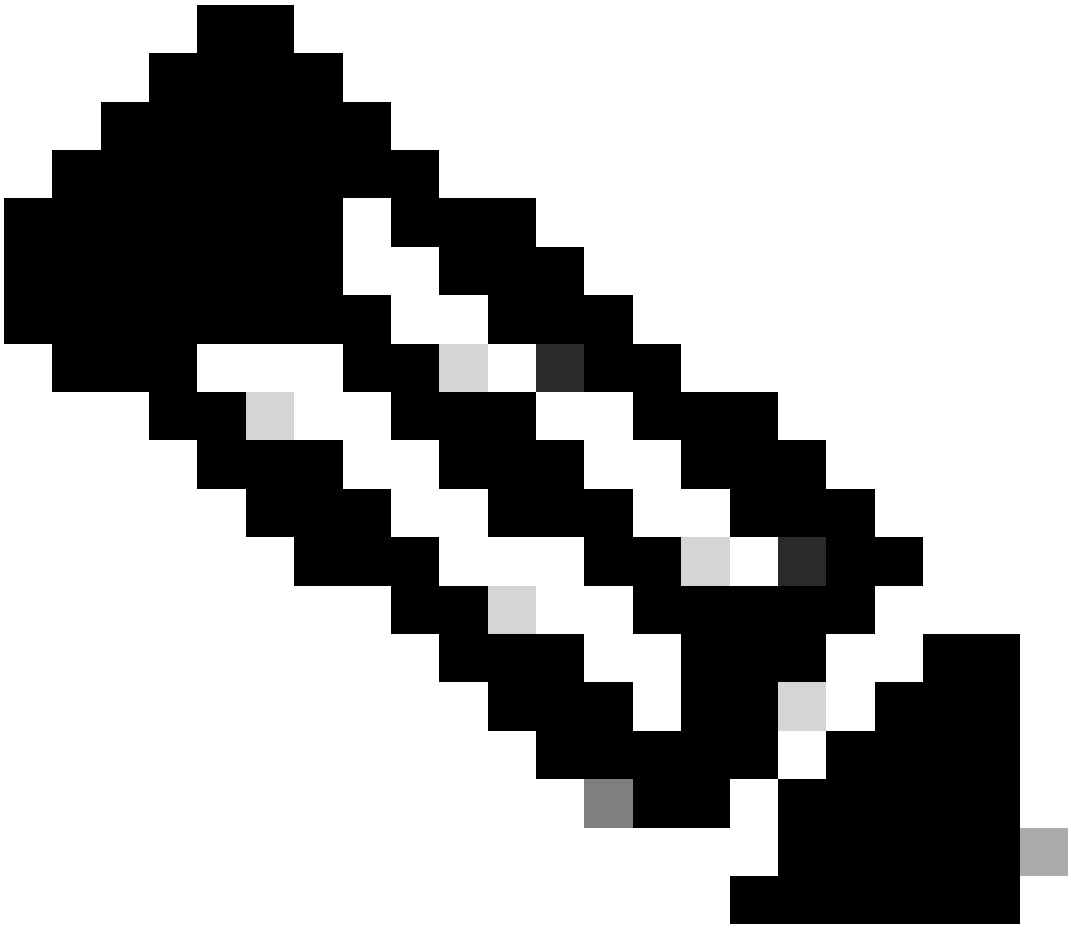
تأكيد المفتاح الخاص ليس عبارة مرور محمية

قم بتسجيل الدخول إلى "إدارة CTB" كمستخدم مسؤول. قم بتشغيل ssh-keygen -yf server_key.pem الأمر.

إذا كان المفتاح الخاص الذي تم طلب عبارة مرور لا يتطلب واحدة.

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

تأكيد الشهادة والمفتاح الخاص مرمزان بواسطة PEM



ملاحظة: يمكن إجراء عمليات التحقق هذه قبل تثبيت الشهادات.

قم بتسجيل الدخول إلى "إدارة CTB" كمستخدم مسؤول.

قم بضبط الأمر على اسم ملف ترخيصك. الأمر sudo cat server_cert.pem باستخدام server_cert.pem لعرض محتوى الملف.

يجب أن تكون الأسطر الأولى والأخيرة من الملف -----**BEGIN CERTIFICATE**----- و-----END CERTIFICATE----- على التوالي.

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

قم بضبط الأمر على اسم ملف المفاتيح الخاصة. الأمر sudo cat server_key.pem باستخدام server_key.pem لعرض الملف.

يجب أن تكون الأسطر الأولى والأخيرة من الملف -----**BEGIN PRIVATE KEY**----- و-----END PRIVATE KEY----- على التوالي.

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

شهادة موقعة ذاتيا

إنشاء شهادة موقعة ذاتيا

- قم بتسجيل الدخول إلى "إدارة CTB" عبر SSH (Secure Shell) بما أن المستخدم الذي تم تكوينه أثناء التثبيت، وهذا عادة ما يكون المستخدم "admin".
- أصدر 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} الأمر.
  - قم بتغيير rsa:{key_len} المفاتيح الخاص الذي تختاره لشم 2048 أو 4096 أو 8192
  - تغيير {ctb_manager_ip} باستخدام IP الخاص بعقدة إدارة 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:~$
```

• قم بعرض ملف server_cert.pem باستخدام cat server_cert.pem الأمر، وانسخ المحتويات إلى المخزن المؤقت لديك حتى يمكنك لصقه إلى محطة العمل المحلية في محرر نصوص من اختيارك. ثم احفظ الملف. يمكنك أيضا مسح هذه الملفات عن طريق /home/admin الدليل.

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

• يمكنك عرض ملف server_key.pem باستخدام sudo cat server_key.pem الأمر ونسخ المحتويات إلى المخزن المؤقت لديك حتى يمكنك لصقه إلى محطة العمل المحلية في محرر نصوص من اختيارك. ثم احفظ الملف. يمكنك أيضا مسح اذه الملف خارج /home/admin الدليل.

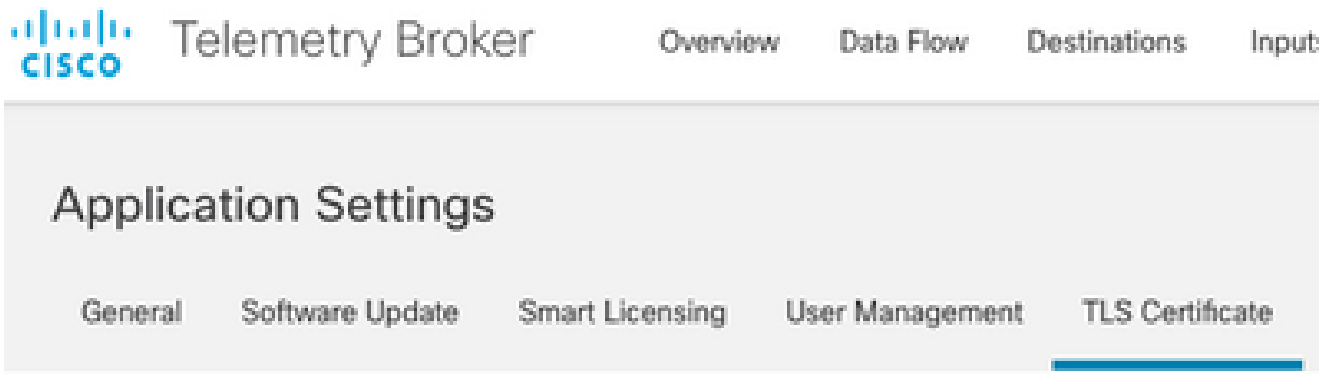
```
admin@ctb-manager:~$ sudo cat server_key.pem
-----BEGIN PRIVATE KEY-----
{removed_for_brevity}
-----END PRIVATE KEY-----
admin@ctb-manager:~$
```

تحميل الشهادة الموقعة ذاتيا

1. انتقل إلى واجهة مستخدم ويب الخاصة بإدارة CTB وسجل الدخول كمستخدم مسؤول وانقر فوق رمز التروس للوصول إلى "Settings.

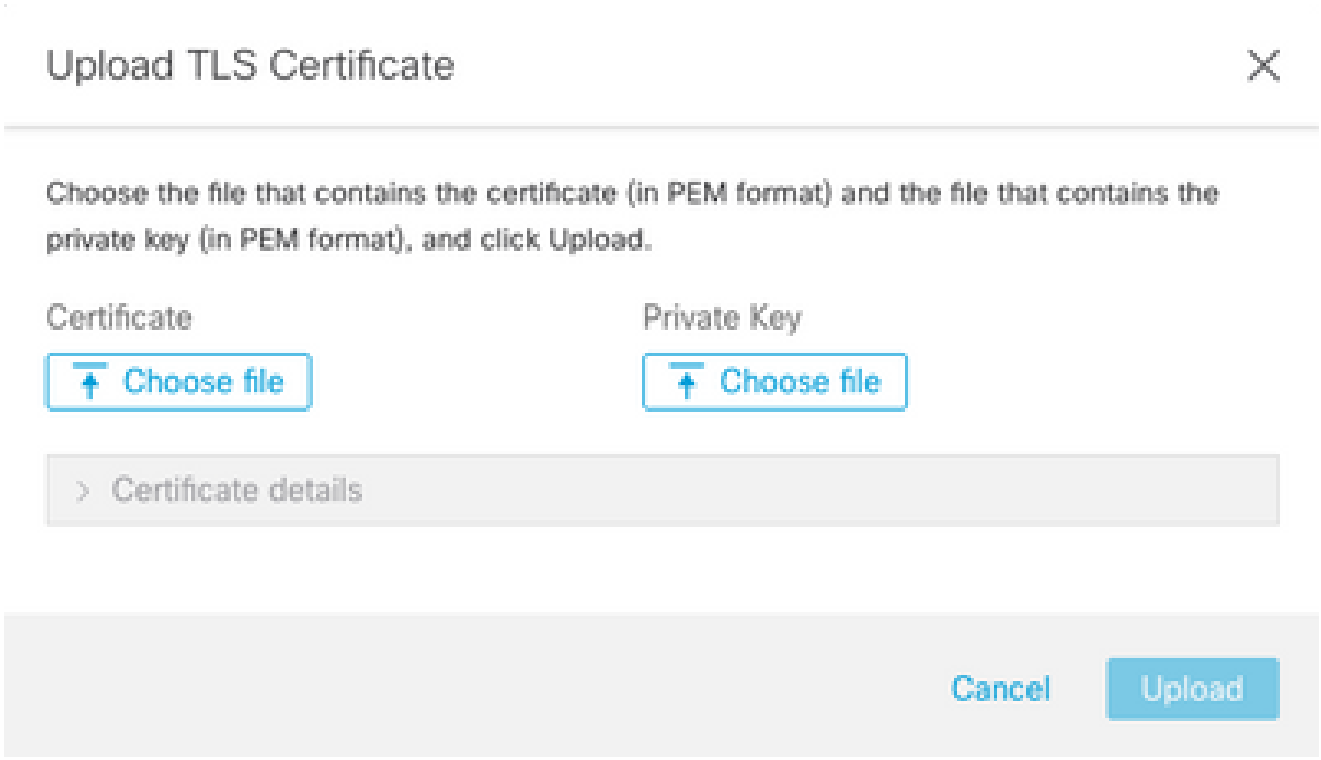
أيقونة إعداد *CTB*

- انتقل إلى علامة التبويب "شهادة TLS".

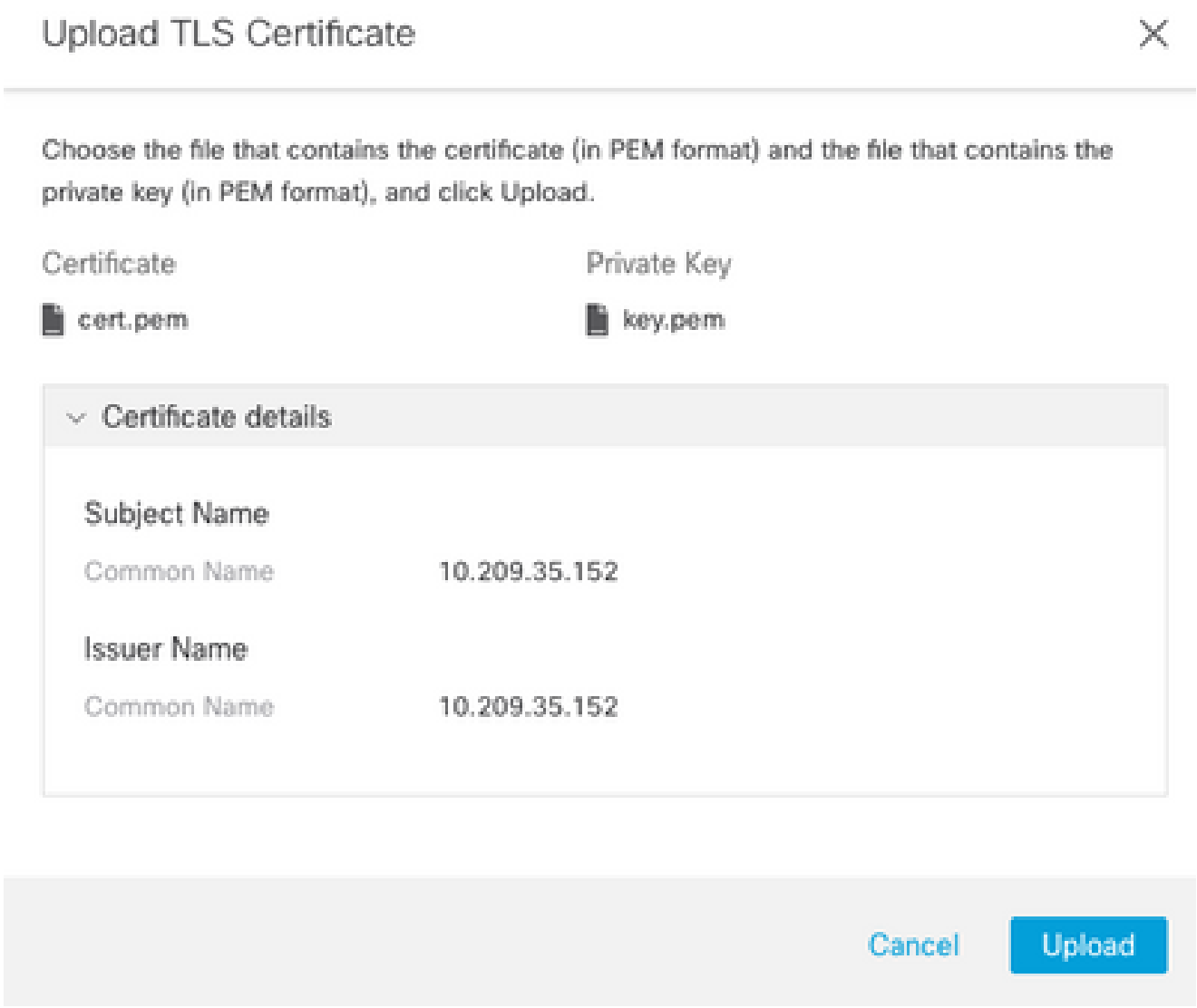


علامة التبويب شهادات *CTB*

- حدد Upload TLS Certificate ثم حدد server_cert.pem و server_key.pem للشهادة والمفتاح الخاص على التوالي في مربع الحوار "تحميل شهادة TLS". بمجرد تحديد الملفات، حدد تحميل.



• بمجرد تحديد الملفات، تؤكد عملية التحقق من الصحة تركيب الشهادة والمفتاح وتعرض الاسم الشائع للمصدر والموضوع كما هو موضح.



تحميل شهادة *CTB*

- حدد الزر "تحميل" لتحميل الشهادة الجديدة. تتم إعادة تشغيل واجهة مستخدم الويب من تلقاء نفسها في بضع دقائق، وبعد ذلك تقوم بإعادة تشغيل تسجيل الدخول إلى الجهاز مرة أخرى.

- قم بتسجيل الدخول إلى وحدة تحكم ويب عقدة إدارة CTB وانتقل Settings > TLS Certificate لمشاهدة تفاصيل الشهادة مثل تاريخ انتهاء صلاحية جديد، أو عرض تفاصيل الشهادة باستخدام المستعرض لعرض معلومات أكثر تفصيلا مثل الأرقام التسلسلية.

تحديث عقد الوسيط

بمجرد أن تحتوي عقدة إدارة CTB على شهادة هوية جديدة، يجب تحديث كل عقدة وسيط CTB يدويا.

1. سجل الدخول إلى كل عقدة وسيط عبر SSH وقم بتشغيل الأمر sudo ctb-manage

```
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:
```

- حدد الخيار c عند طلبها.

```
== 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
```

- تحقق من تفاصيل الشهادة إذا كانت مطابقة لقيم الشهادة الموقعة وحدد y قبول الشهادة. تبدأ الخدمات تلقائيا وبمجرد بدء تشغيل الخدمة يتم إرجاع المطالبة. يمكن أن تستغرق عملية بدء الخدمة ما يصل إلى 15 دقيقة لإكمالها.

```
== 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
```

الشهادات التي يصدرها المرجع المصدق (CA)

إنشاء طلب توقيع الشهادة (CSR) للإصدار من قبل مرجع مصدق

- قم بتسجيل الدخول إلى "إدارة CTB" عبر SSH (Secure Shell) بما أن المستخدم الذي تم تكوينه أثناء التثبيت، فهذا عادة ما يكون المستخدم "admin".

- أصدرت 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 الأمر. يمكنك ترك السمات 'extra' في السطرين الأخيرين فارغة إذا رغبت في ذلك.

  - تغيير {ctb_manager_dns_name} باستخدام اسم DNS لعقدة إدارة CTB

    - تغيير {ctb_manager_ip} باستخدام IP الخاص بعقدة إدارة CTB

    - قم بتغيير المفاتيح {key_len} باستخدام طول مفاتيح خاص من إختيارك مثل 2048 أو 4096 أو 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 الـ CSR والملفات الأساسية إلى جهاز محلي ووفر الـ CSR إلى الـ CA. إصدار CSR من قبل CA بتنسيق PEM خارج نطاق هذا المستند.

إنشاء شهادة باستخدام سلسلة

يصدر المرجع المصدق شهادة هوية الخادم بتنسيق PEM. يجب إنشاء ملف سلسلة يحتوي على كافة شهادات السلسلة وشهادة هوية الخادم لعقدة إدارة CTB.

في محرر نصي قم بإنشاء ملف عن طريق تجميع الترخيص الموقع في الخطوة السابقة وإقران كل الشهادات في السلسلة على كل حال متضمنا المرجع المصدق الثقة في ملف واحد بتنسيق PEM بالترتيب الموضح.

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

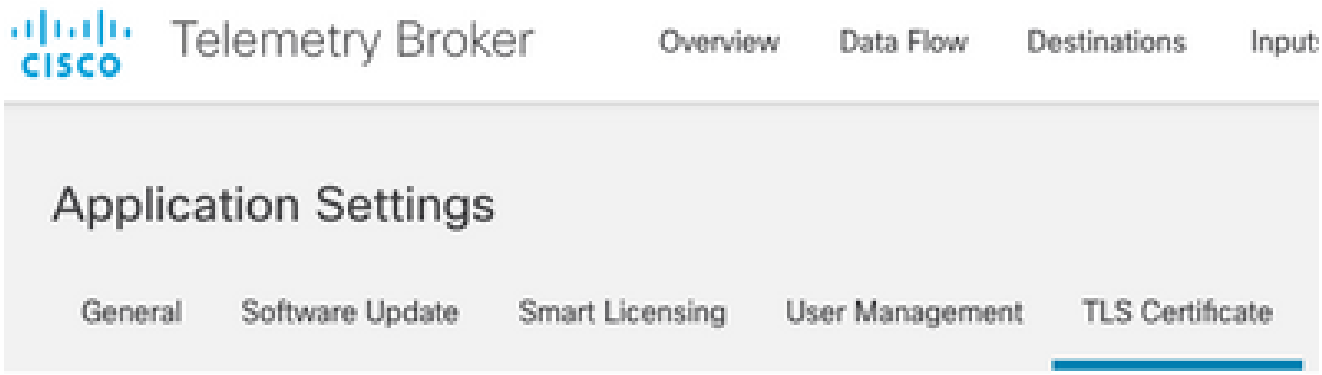
تأكد من أن ملف الشهادة الجديد مع ملف السلسلة ليس له مسافات بادئة أو تالية، وبدون فارغة، وهو بالترتيب الظاهر أعلاه.

تحميل الشهادة التي أصدرها المرجع المصدق

1. انتقل إلى واجهة مستخدم ويب الخاصة بإدارة CTB وسجل الدخول كمسؤول وانقر فوق رمز الترس للوصول إلى "Settings.

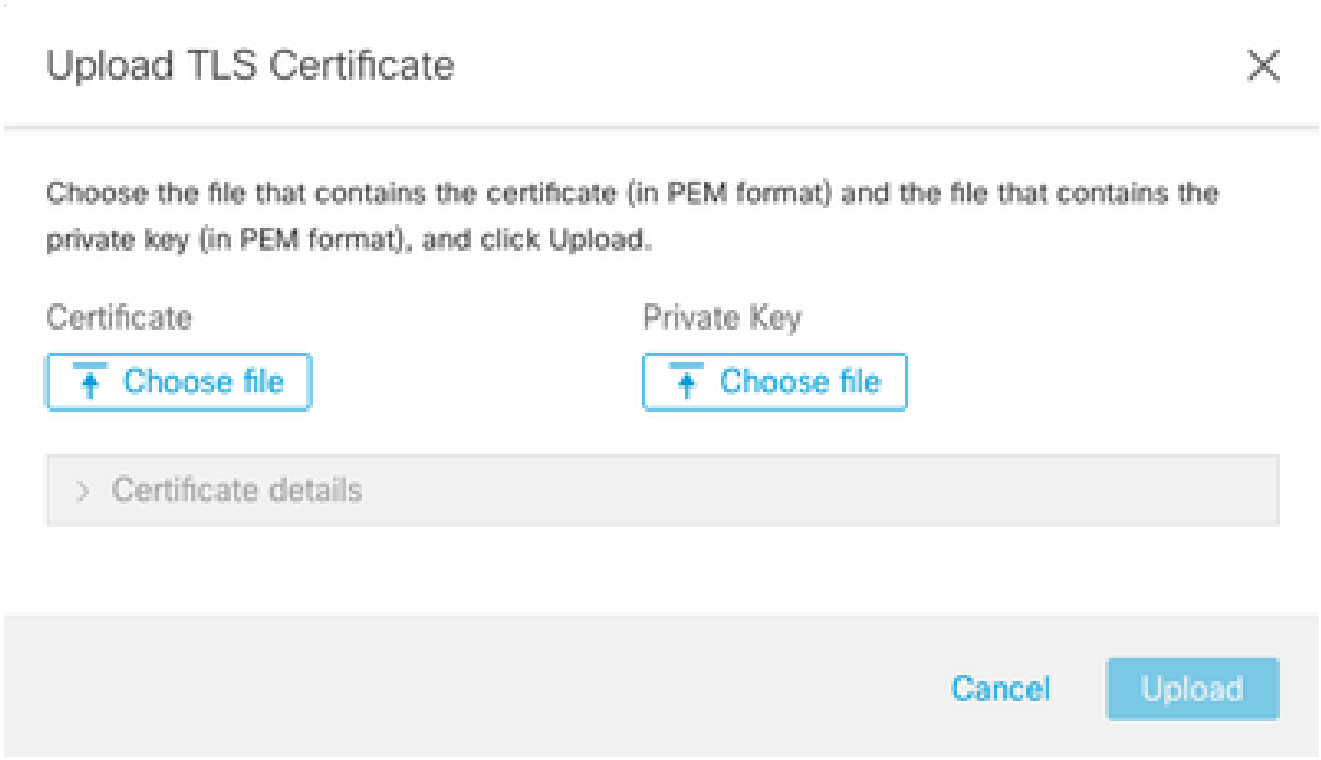
أيقونة إعداد *CTB*

- انتقل إلى علامة التبويب "شهادة TLS".

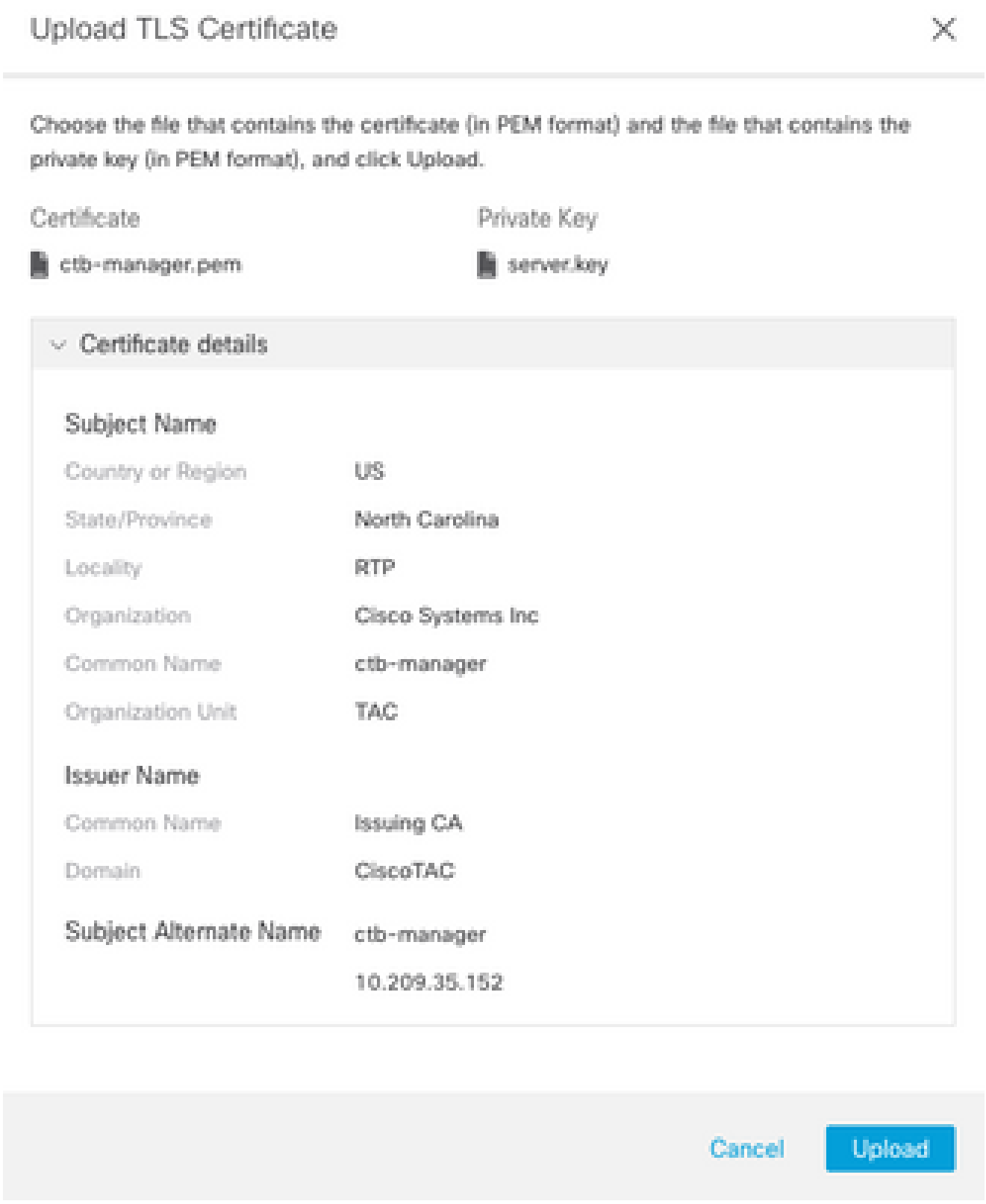


علامة التبويب شهادات *CTB*

- حدد Upload TLS Certificate ثم حدد الشهادة ذات ملف السلسلة الذي تم إنشاؤه في القسم الأخير، وأحدث مدير CTB server_key.pem للشهادة والمفتاح الخاص على التوالي في مربع الحوار "تحميل شهادة TLS". بمجرد تحديد الملفات، حدد تحميل.



• بمجرد تحديد الملفات، تؤكد عملية التحقق من الصحة مجموعة الشهادات والمفاتيح وتعرض الاسم المشترك للمصدر والموضوع كما هو موضح أدناه.



التحقق من صحة شهادة *CTB* التي تم إصدارها

- حدد الزر "تحميل" لتحميل الشهادة الجديدة. تتم إعادة تشغيل واجهة مستخدم ويب بنفسها في حوالي 60 ثانية، قم بتسجيل الدخول إلى واجهة مستخدم ويب بعد إعادة تشغيلها.

- قم بتسجيل الدخول إلى وحدة تحكم ويب عقدة إدارة CTB وانتقل Settings > TLS Certificate لمشاهدة تفاصيل

الشهادة مثل تاريخ انتهاء صالحية جديد، أو عرض تفاصيل الشهادة باستخدام المستعرض لعرض معلومات أكثر تفصيلا مثل الأرقام التسلسلية.

تحديث وسيط CTB

بمجرد أن تحتوي عقدة إدارة CTB على شهادة هوية جديدة، يجب تحديث كل عقدة وسيط CTB يدويا.

1. سجل الدخول إلى كل عقدة وسيط عبر SSH وقم بتشغيل الأمر sudo ctb-manage

```
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:
```

- حدد الخيار c عند طلبها.

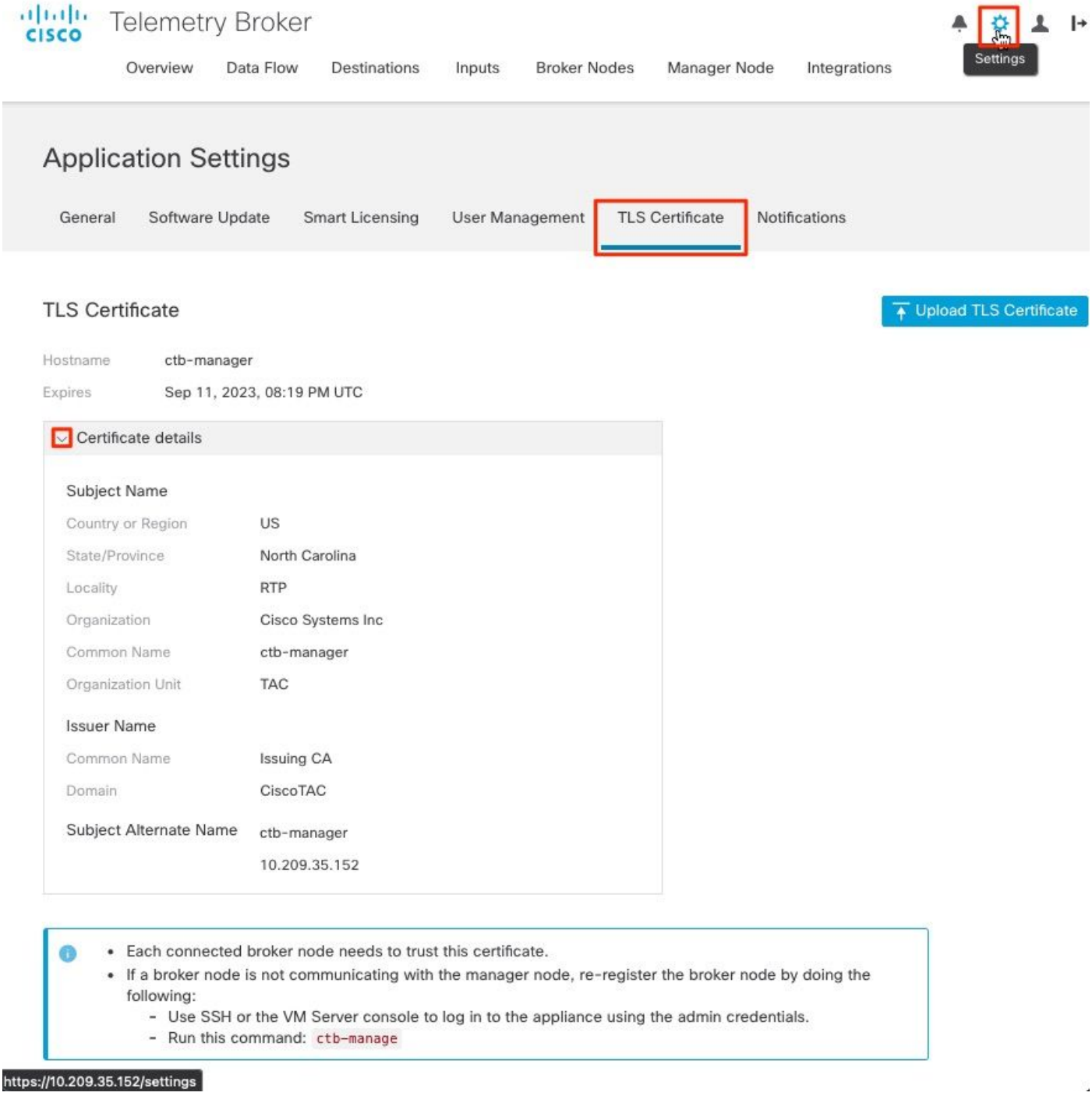
```
== Management Configuration

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
```

- تحقق من تفاصيل الشهادة إذا كانت مطابقة لقيم الشهادة الموقعة وحدد y لقبول الشهادة. تبدأ الخدمات وبمجرد بدء تشغيل الخدمة يتم إرجاع المطالبة. يمكن أن تستغرق عملية بدء الخدمة ما يصل إلى 15 دقيقة لإكمالها.

```
== 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
```

التحقق من الصحة

قم بتسجيل الدخول إلى وحدة تحكم ويب عقدة إدارة CTB وانتقل إلى Settings > TLS Certificate لمشاهدة تفاصيل الشهادة مثل تاريخ انتهاء صلاحية جديد، أو عرض تفاصيل الشهادة باستخدام المستعرض لعرض معلومات أكثر تفصيلا مثل الأرقام التسلسلية.



تفاصيل شهادة *CTB*

تحقق من عدم إظهار عقدة وسيط CTB أية تنبيهات في واجهة مستخدم ويب عقدة إدارة CTB.

استكشاف الأخطاء وإصلاحها

إذا كانت الشهادة غير مكتملة مثل عدم وجود شهادات السلسلة، فلن تتمكن عقدة وسيط CTB من الاتصال بعقدة الإدارة وتعرض "لم يتم مشاهدتها منذ ذلك الحين" في عمود الحالة في قائمة عقد الوسيط.
ستستمر عقدة الوسيط في نسخ حركة مرور البيانات وتوزيعها في هذه الحالة.

قم بتسجيل الدخول إلى واجهة سطر الأوامر (CLI) الخاصة بعقدة إدارة CTB وأصدر sudo grep -ic begin /var/lib/titan/titanium_frontend/ssl/cert.pem الأمر للاطلاع على عدد الشهادات الموجودة في ملف cert.pem.

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

تحتاج قيمة الإخراج التي تم إرجاعها إلى تساوي عدد أجهزة CA في السلسلة بالإضافة إلى "إدارة CTB".

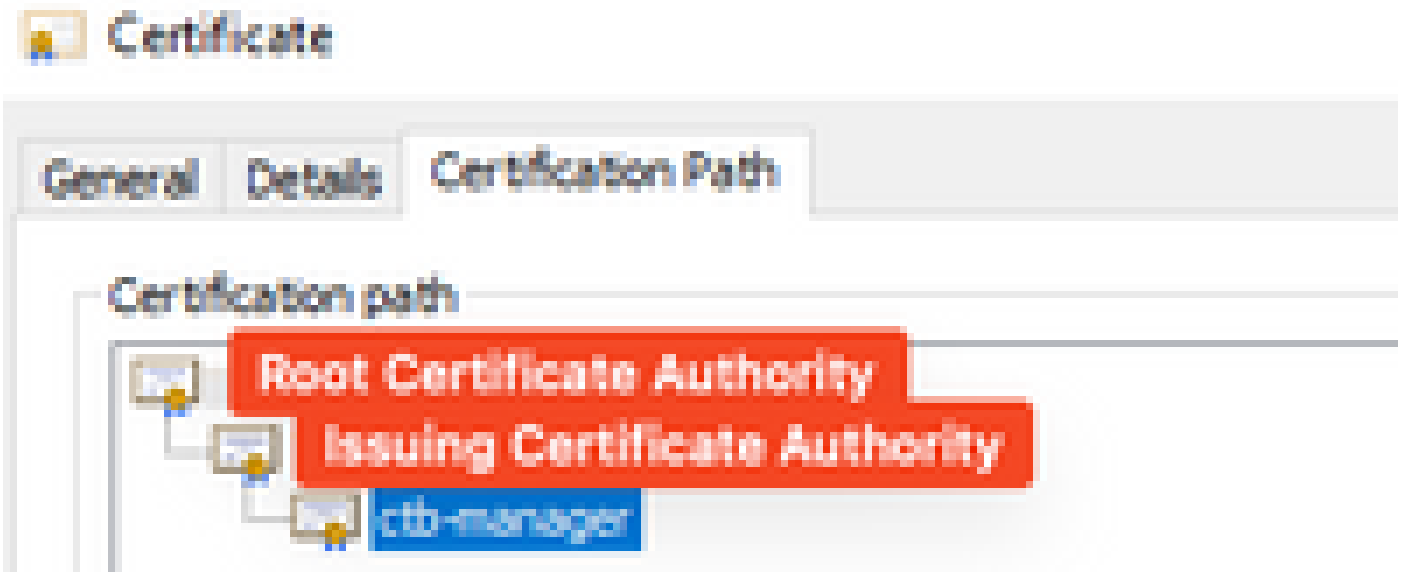
من الموقوع إخراج 1 في حالة إستخدام شهادة موقعة ذاتيا.

من الموقوع إخراج 2 إذا كانت البنية الأساسية ل PKI تتكون من مرجع مصدق جذر واحد يكون هو أيضا المرجع المصدق الذي يتم إصداره.

من الموقوع إخراج 3 إذا كانت البنية الأساسية ل PKI تتكون من مرجع مصدق رئيسي، وإصدار CA.

من الموقوع أن يكون الناتج 4 إذا كانت البنية الأساسية ل PKI تتكون من CA الجذر و CA التابع و CA الإصدار.

قارن المخرج مع PKI المسرود عند عرض التخيص في تطبيق آخر مثل Microsoft Windows Crypto Shell Extensions.



البنية الأساسية ل *PKI*

في هذه الصورة تتضمن البنية الأساسية ل PKI المرجع المصدق الجذر و المرجع المصدق الإصدار.

من الموقوع أن تكون قيمة الإخراج من الأمر 3 في هذا السيناريو.

إذا كان الإخراج ال يفي بالتوقعات، راجع الخطوات الموجودة في قسم **إنشاء شهادة باستخدام سلسلة** لتحديد ما إذا كانت الشهادة قد تم فقدها.

عند عرض شهادة فيها Microsoft Windows Crypto Shell Extensions من الممكن أال تكون كل الشهادات معروضة إذا لم يكن للجهاز المحلي معلومات كافية للتحقق من الشهادة.

أصدرت sudo ctb-mayday الأمر من ال CLI أن يدل ووم حزمة ل TAC أن يراجع.

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).