Erstellen selbstsignierter Zertifikate mit mehreren URLs

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Sie ein selbstsigniertes Zertifikat erstellen, das von CloudCenter mit mehreren URLs verwendet werden kann.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Zertifikate
- Linux

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf CentOS7.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Problem

Die Zertifikate, die standardmäßig mit CloudCenter geliefert werden oder die mithilfe des Cisco Call Manager (CCM)-Konfigurationsassistenten erstellt werden können, verfügen nicht über einen Subject Alternative Name (SAN), den bestimmte Browser wie Google Chrome als Fehler behandeln und Sie warnen. Dies kann überschrieben werden, aber ohne SANs kann ein Zertifikat nur über eine bestimmte URL gültig sein.

Wenn Sie z. B. ein Zertifikat besitzen, das für die IP-Adresse 10.11.12.13 gültig ist, wenn Sie einen DNS-Namen (Domain Name System) von www.opencart.com haben, erhalten Sie einen

Zertifikatfehler, da dieser URL nicht dem Zertifikat entspricht (dies gilt auch dann, wenn www.opencart.com in Ihrer Hostdatei als das Zertifikat aufgeführt ist, das zu 10.11.1 gehört1 gehört. 2,13). Dies kann auftauchen, wenn Subtenants von CloudCenter Single Sign On (SSO) verwenden, da jeder SSO-Server über eine eigene URL verfügt.

Lösung

Am einfachsten lässt sich dieses Problem beheben, indem Sie ein neues selbstsigniertes Zertifikat mit SANs erstellen, das alle URLs auflistet, die Sie an dieselbe IP-Adresse weiterleiten. Der Leitfaden ist ein Versuch, Best Practices auf diesen Prozess anzuwenden.

Schritt 1: Navigieren Sie zum **Stammverzeichnis**, und erstellen Sie einen neuen Ordner, in dem die Zertifikate untergebracht sind:

```
sudo -s
cd /root
mkdir ca
```

Schritt 2: Navigieren Sie in den neuen Ordner, und erstellen Sie Unterordner, um die Zertifikate, privaten Schlüssel und Protokolle zu organisieren.

```
cd ca
mkdir certs crl newcerts private
chmod 700 private
touch index.txt
echo 1000 > serial
```

Schritt 3: Kopieren Sie den Inhalt von **CAopenssl.conf auf /root/ca/openssl.cnf**

> **Hinweis**: Diese Datei enthält die Konfigurationsoptionen für eine Zertifizierungsstelle (Certificate Authority, CA) und die Standardoptionen, die für CloudCenter geeignet sein können.

Schritt 4: Erstellen Sie einen privaten Schlüssel und ein Zertifikat für die CA.

```
openssl genrsa -aes256 -out private/ca.key.pem 4096
chmod 400 private/ca.key.pem
openssl req -config openssl.cnf -key private/ca.key.pem -new -x509 -days 7300 -sha256 -
extensions v3_ca -out certs/ca.cert.pem
chmod 444 certs/ca.cert.pem
```

Schritt 5: Ihre Zertifizierungsstelle ist der ultimative Weg, um zu überprüfen, ob ein Zertifikat gültig ist. Dieses Zertifikat darf nie von unbefugten Personen genutzt werden und darf niemals mit dem Internet verbunden sein. Aufgrund dieser Einschränkung müssen Sie eine Zwischen-Zertifizierungsstelle erstellen, die das Endzertifikat signiert, wodurch eine Unterbrechung entsteht, bei der das Zwischenzertifikat widerrufen und eine neue ausgestellt werden kann, wenn es kompromittiert wird.

Schritt 6: Erstellen Sie ein neues Unterverzeichnis für die mittlere CA.

```
mkdir /root/ca/intermediate
cd /root/ca/intermediate/
```

```
mkdir certs crl csr newcerts private
chmod 700 private
touch index.txt
echo 1000 > serial
echo 1000 > /root/ca/intermediate/crlnumber
```

Schritt 7: Kopieren Sie den Inhalt von **Intermediateopenssl.conf** auf **/root/ca/intermediate/openssl.cnf** .

> **Hinweis**: Diese Datei enthält fast identische Konfigurationsoptionen für die CA, mit Ausnahme einiger kleiner Änderungen, die sie auf ein Zwischenstufen spezifizieren.

Schritt 8: Generieren Sie den Zwischenschlüssel und das Zertifikat.

```
cd /root/ca
openssl genrsa -aes256 -out intermediate/private/intermediate.key.pem 4096
chmod 400 intermediate/private/intermediate.key.pem
openssl req -config intermediate/openssl.cnf -new -sha256 -key
intermediate/private/intermediate.key.pem -out intermediate/csr/intermediate.csr.pem
```

Schritt 9: Signieren Sie das Zwischenzertifikat mit dem Zertifizierungsstellenzertifikat. Dadurch wird eine Vertrauenskette erstellt, die der Browser zum Überprüfen der Authentizität eines Zertifikats verwendet.

```
openssl ca -config openssl.cnf -extensions v3_intermediate_ca -days 3650 -notext -md sha256 -in
intermediate/csr/intermediate.csr.pem -out intermediate/certs/intermediate.cert.pem
chmod 444 intermediate/certs/intermediate.cert.pem
```

Schritt 10: Erstellen Sie eine CA-Kette, da Sie die CA nicht im Internet haben möchten, können Sie eine CA-Kette erstellen, die Browser verwenden, um die Authentizität bis hin zur CA zu überprüfen.

```
cat intermediate/certs/intermediate.cert.pem certs/ca.cert.pem > intermediate/certs/ca-
chain.cert.pem
chmod 444 intermediate/certs/ca-chain.cert.pem
```

Schritt 11: Erstellen Sie einen neuen Schlüssel und ein neues Zertifikat für den CCM.

```
openssl genrsa -out intermediate/private/ccm.com.key.pem 2048
openssl req -new -sha256 -key intermediate/private/ccm.com.key.pem -subj
"/C=US/ST=NC/O=Cisco/CN=ccm.com" -reqexts SAN -config <(cat intermediate/openssl.cnf <(printf
"[SAN]\nsubjectAltName=DNS:ccm.com,DNS:www.ccm.com,IP:10.11.12.13")) -out
intermediate/csr/ccm.com.csr
```

Schritt 12: Dieser verfügt über alle erforderlichen Felder im Befehl und muss manuell bearbeitet werden.

- **/C=USA** bezieht sich auf das Land (Grenzwert von 2 Zeichen).
- **/ST=NC** bezieht sich auf den Status und kann Leerzeichen enthalten.
- **/O=Cisco** bezieht sich auf die Organisation
- **/CN=ccm.com** bezieht sich auf den allgemeinen Namen. Dies sollte der wichtigste URL für den Zugriff auf den CCM sein.
- **SAN\nsubjectAltName=** sind die alternativen Namen. Der allgemeine Name sollte in dieser Liste enthalten sein, und es gibt keine Beschränkung für die Anzahl der SANs, die Sie haben.

Schritt 13: Signieren Sie das endgültige Zertifikat mithilfe des Zwischenzertifikats.

```
openssl ca -config intermediate/openssl.cnf -extensions server_cert -days 375 -notext -md sha256
-in intermediate/csr/ccm.com.csr -out intermediate/certs/ccm.com.cert.pem
```

Schritt 14: Überprüfen Sie, ob das Zertifikat korrekt signiert wurde.

```
openssl verify -CAfile intermediate/certs/ca-chain.cert.pem intermediate/certs/ccm.com.cert.pem
```

Schritt 15: Es kann entweder einen OK oder einen Fehler zurückgeben.

Schritt 16: Kopieren Sie das neue Zertifikat, den Schlüssel, und die CA-Kette in den Ordner **Catalina**.

```
cd /root/ca/intermediate/certs
cp ccm.com.cert.pem /usr/local/tomcat/conf/ssl/ccm.com.crt
cp ca-chain.cert.pem /usr/local/tomcat/conf/ssl/ca-chain.crt
cd ../private
cp ccm.com.key.pem /usr/local/tomcat/conf/ssl/ccm.com.key
```

Schritt 17: Weisen Sie dem Benutzer den Besitz des Benutzers zu, und legen Sie die Berechtigungen korrekt fest.

```
chown cliqruser:cliqruser ccm.com.crt
chown cliqruser:cliqruser ccm.com.key
chown cliqruser:cliqruser ca-chain.crt
chmod 644 ccm.com.crt
chmod 644 ccm.com.key
chmod 644 ca-chain.crt
```

Schritt 18: Sichern Sie die Datei **server.xml,** bevor Sie Änderungen vornehmen.

```
cd ..
cp server.xml server.xml.bak
```

Schritt 19: **Server.xml** bearbeiten**:**

1. Suchen Sie nach dem Abschnitt, der mit **<Connector port="10443" maxHttpHeaderSize="8192" beginnt.**
2. Ändern Sie die **SSLC-Zertifikatsdatei** so, dass sie auf ccm.com.crt zeigt.
3. Ändern Sie **SSLCertificateKeyFile**, um auf ccm.com.key zu zeigen.
4. Ändern Sie **SSLCACertificateFile**, um auf ca-chain.crt zu zeigen.

Schritt 20: Starten Sie Tomcat neu.

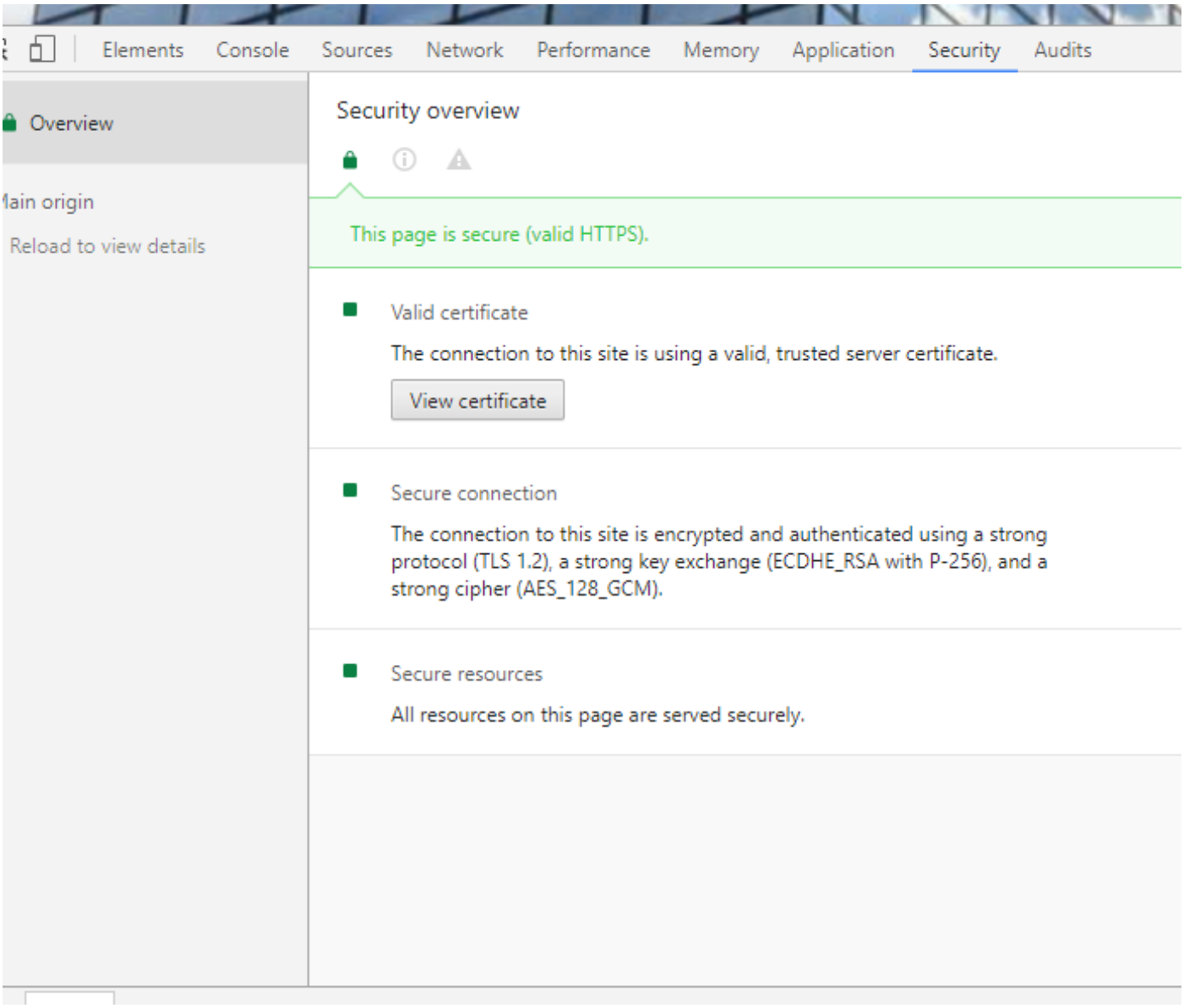
```
service tomcat stop
service tomcat start
```

Schritt 21: Der CCM verwendet jetzt das neue Zertifikat, das für alle DNS-Namen und IP-Adressen gültig ist, die in Schritt 13 angegeben sind.

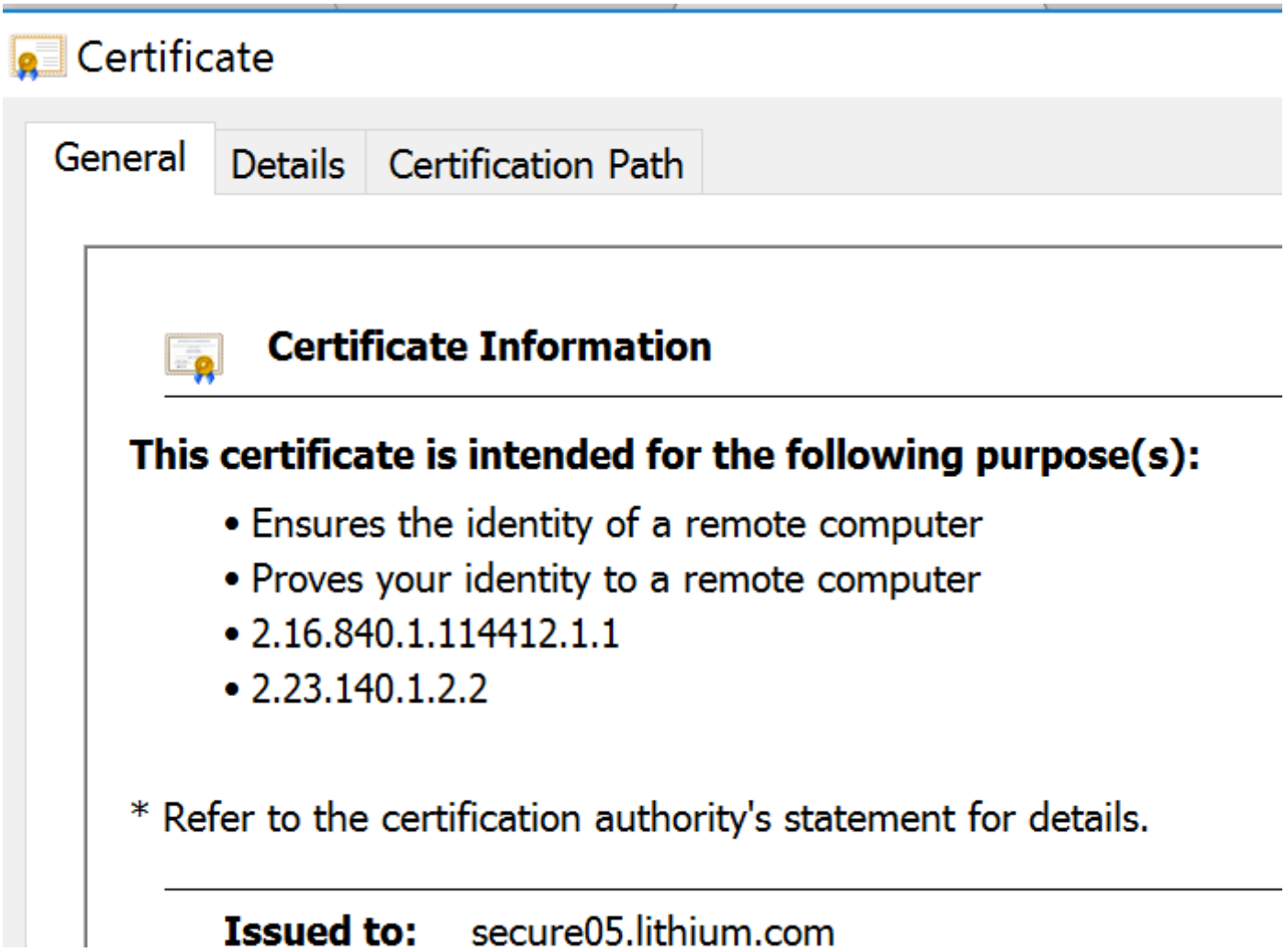
Schritt 22: Da die Zertifizierungsstelle zum Zeitpunkt des Leitfadens erstellt wurde, wird sie von Ihren Browsern standardmäßig nicht als gültig erkannt. Sie müssen das Zertifikat manuell importieren.

Schritt 23: Navigieren Sie zum **CCM** mit einer gültigen URL, und drücken Sie **Strg+Umschalt+i**, um die Entwicklungstools zu öffnen.

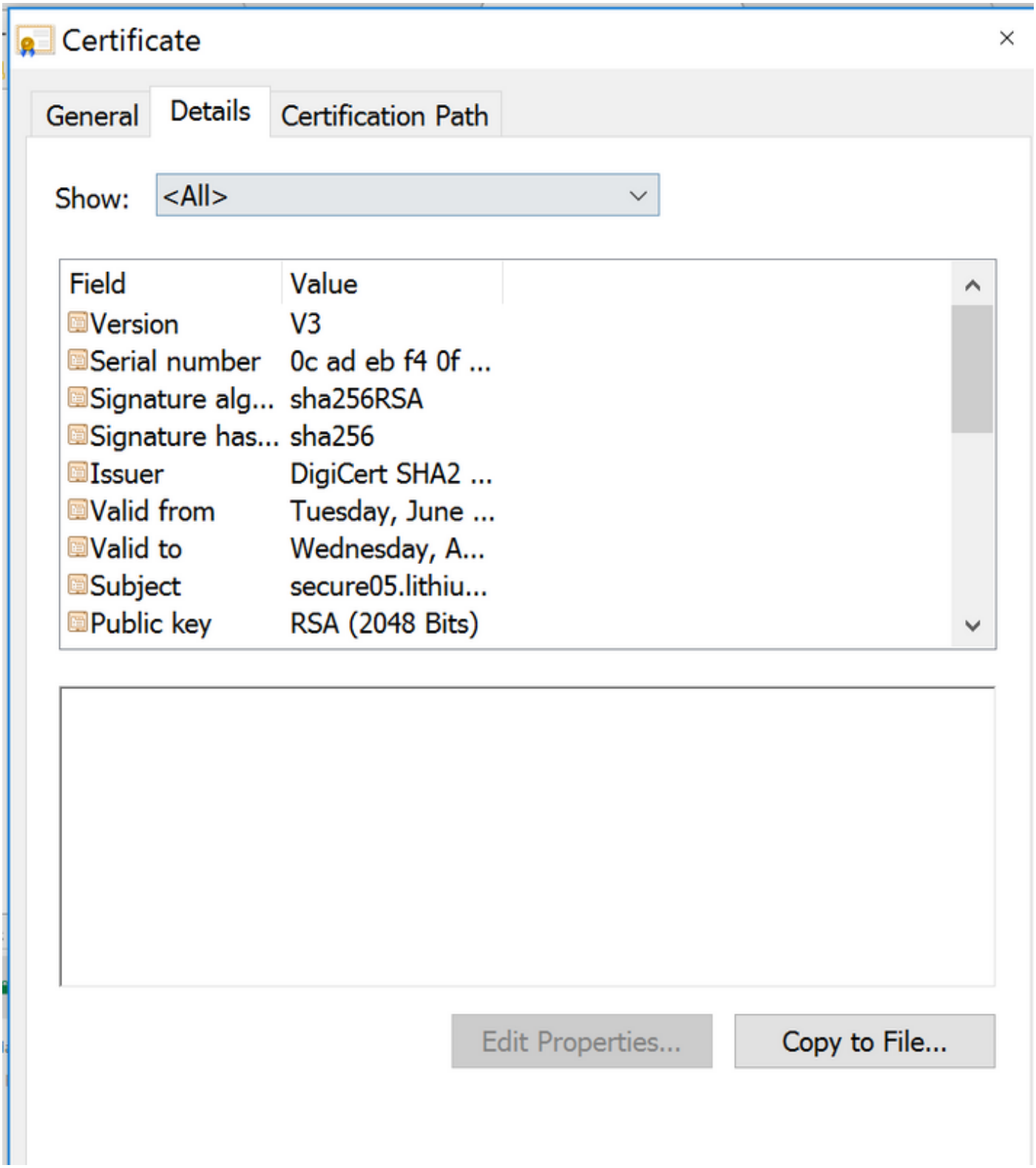
Schritt 24: Wählen Sie **Zertifikat anzeigen**, wie im Bild gezeigt.



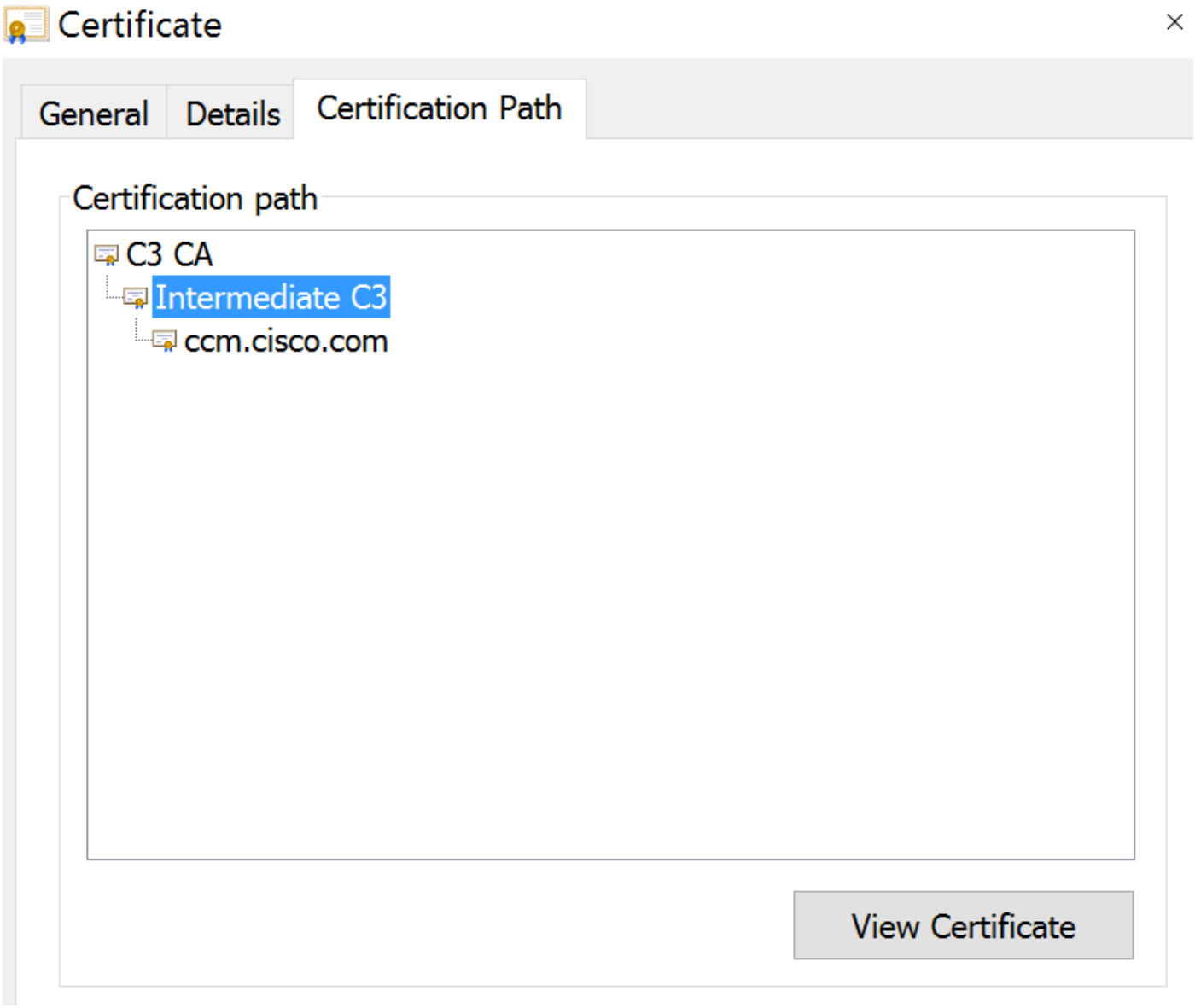
Schritt 25: Wählen Sie **Details** wie im Bild gezeigt aus.



Schritt 26: Wählen Sie **In Datei kopieren** aus, wie im Bild gezeigt.



Schritt 27: Wenn Fehler bei einer nicht vertrauenswürdigen CA auftreten, navigieren Sie zum **Zertifizierungspfad**, um das Zwischen- und Stammzertifikat anzuzeigen. Sie können auf sie klicken, ihr Zertifikat anzeigen und diese in Dateien kopieren, wie im Bild gezeigt.



Schritt 28: Wenn Sie die Zertifikate heruntergeladen haben, befolgen Sie die Anweisungen des Betriebssystems oder Browsers, um diese Zertifikate als vertrauenswürdige Behörde und zwischengeschaltete Behörden zu installieren.