Creatie van zelfgetekende certificaten met meerdere URL's

Inhoud

Inleiding

Dit document beschrijft hoe u een zelf-ondertekend certificaat kunt maken dat door CloudCenter met meerdere URL's kan worden gebruikt.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Certificaten
- Linux

Gebruikte componenten

De informatie in dit document is gebaseerd op CentOS7.

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 de potentiële impact van elke opdracht begrijpen.

Probleem

De certificaten die standaard worden geleverd met CloudCenter, of die kunnen worden gemaakt met het gebruik van de configuratiwizard Cisco Call Manager (CCM), hebben geen Onderwerp Alternative Name (SAN), die bepaalde browsers, zoals Google Chrome, als een fout beschouwen en u waarschuwt. Dit kan worden gecorrigeerd, maar zonder SAN's kan een certificaat alleen geldig zijn vanaf één specifieke URL.

Als u bijvoorbeeld een certificaat hebt dat geldig is voor het IP-adres van 10.11.12.13 en u een DNS-naam (Domain Name System) van www.opencart.com hebt, dan ontvangt u een

certificaatfout omdat die URL niet het certificaat is (dit is waar zelfs als www.opencart.com in uw hostbestand wordt genoemd en die tot 10.11.1 behoort 2.13). Dit kan oplopen als gebruikers van CloudCenter in het gebruik van Single Sign On (SSO) zijn, omdat elke SSO-server een eigen URL heeft.

Oplossing

De makkelijkste manier om deze kwestie te repareren is om een nieuw zelfgetekend certificaat te creëren dat SAN's heeft, dat elke URL die u naar hetzelfde IP-adres stuurt, lijsten. De gids is een poging om de beste praktijken op dit proces toe te passen.

Stap 1. Navigeer naar de **basismap** en maak een nieuwe map om de certificaten te huisvesten:

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

Stap 2. Navigeer in de nieuwe map en maak submappen om de certificaten, privé-toetsen en logbestanden te organiseren.

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

Stap 3. Kopieer de inhoud van **CAopenssl.conf naar /root/ca/openssl.cnf**

> Opmerking: Dit bestand bevat de configuratieopties voor een certificaatinstantie (CA) en standaardopties die geschikt zijn voor CloudCenter.

Stap 4. Generate a private key and Certificate for the 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
```

Stap 5. Uw CA is de ultieme manier om te controleren of een certificaat geldig is, dit certificaat mag nooit toegankelijk zijn voor onbevoegden en mag nooit aan internet worden blootgesteld. Als gevolg van deze beperking moet u een intermediaire CA creëren die het eindcertificaat tekent, creëert dit een breuk waar, als het certificaat van tussenliggende autoriteit in gevaar is, het kan worden ingetrokken en een nieuw afgegeven.

Stap 6. Maak een nieuwe subdirectory voor de intermediaire 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
```

Stap 7. Kopieer de inhoud van **Intermediateopenssl.conf** naar **/root/ca/intermediate/openssl.cnf**.

> Opmerking: Dit bestand bevat bijna identieke configuratieopties voor de CA, anders dan een paar kleine tweaks om het specifiek te maken voor een intermediair.

Stap 8. genereren de intermediaire sleutel en het certificaat.

```
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
```

Stap 9. Teken het intermediaire certificaat met het CA certificaat, dit bouwt een keten van vertrouwen dat browser gebruikt om de authenticiteit van een certificaat te verifiëren.

```
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
```

Stap 10. Maak een CA-keten, aangezien u de CA niet op het internet wilt, kunt u een CA-keten maken die browsers gebruiken om authenticiteit tot aan de CA te controleren.

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

Stap 1. Maak een nieuwe sleutel en een nieuw certificaat voor het 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
```

Stap 12. Dit heeft alle gewenste velden in de opdracht en moet handmatig worden bewerkt.

- **/C=VS** verwijst naar het land (2-kaartlimiet)
- **/ST=NC** verwijst naar de staat en kan ruimtes bevatten
- **/O=Cisco** verwijst naar de Organisatie
- **/CN=ccm.com** verwijst naar de Gemeenschappelijke Naam, dit moet de belangrijkste URL zijn die wordt gebruikt om toegang te krijgen tot het CCM.
- **SAN\nsubjectAltName=** zijn de alternatieve namen, de veelgebruikte naam moet in deze lijst staan en er is geen limiet aan hoeveel SAN's u heeft.

Stap 13. Teken het definitieve certificaat met behulp van het tussentijdse certificaat.

```
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
```

Stap 14. Controleer dat het certificaat correct is ondertekend.

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

Stap 15. Het kan een OK of een Fail teruggeven.

Stap 16. Kopieer het nieuwe certificaat, het is de sleutel en de CA-keten naar de map **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
```

Stap 17. Geef het eigendom van de klant en stel de rechten correct in.

```
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
```

Stap 18. Maak een back-up van het bestand **server.xml** voordat u wijzigingen aanbrengt.

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

Stap 19. **Server.xml** bewerken:

1. Pak het gedeelte vast dat begint met **<Connector poort="10443" maxHTTPHeaderSize="8192"**
2. **CSL-bestand** op ccm.com.cr wijzigen
3. Verander **SSLCcertificaatKeyFile** naar ccm.com.key
4. Verander **SSLCACcertificaatFile** naar ca-chain.crt

Stap 20. Start Tomcat opnieuw.

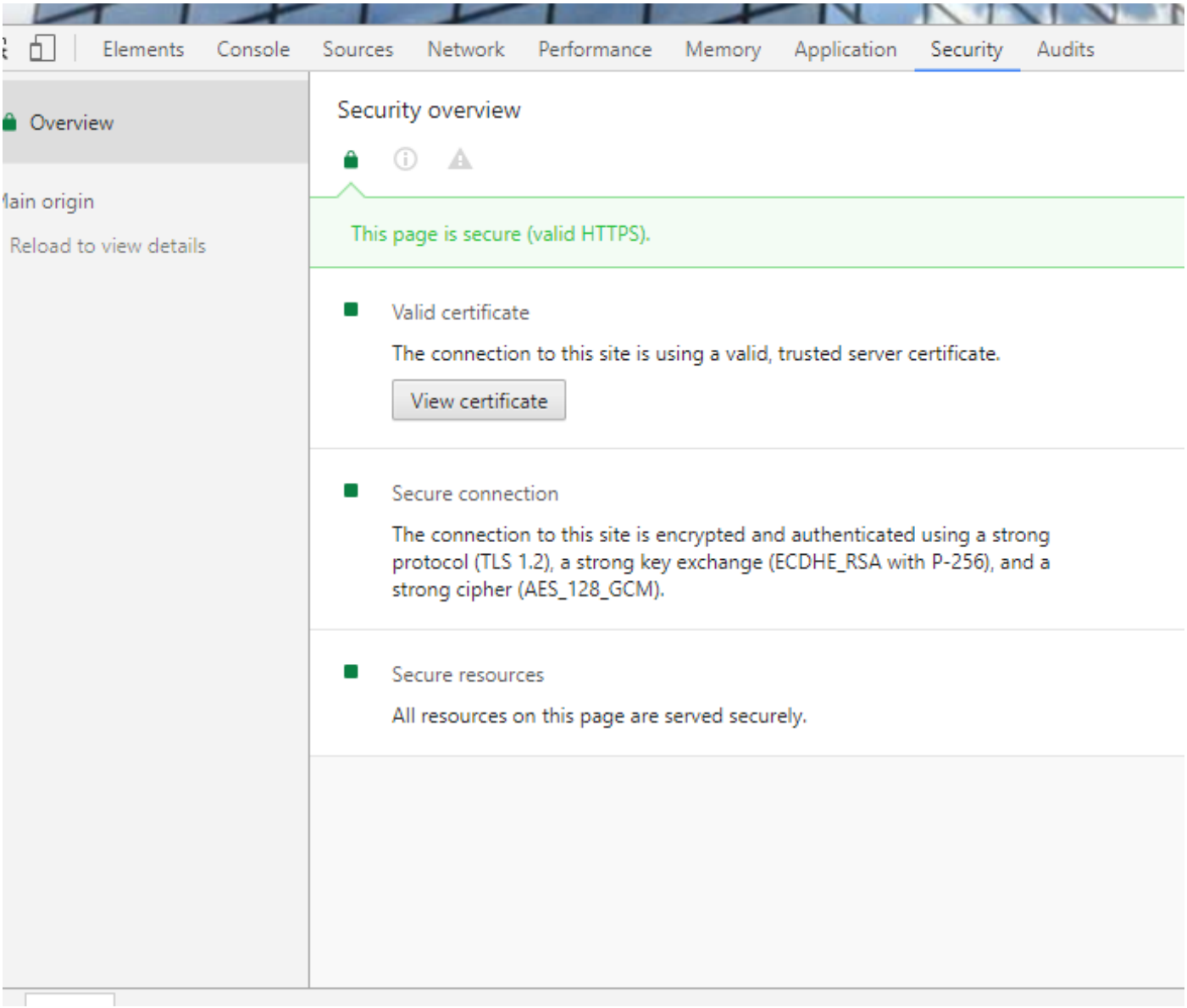
```
service tomcat stop
service tomcat start
```

Stap 21. Het CCM gebruikt nu het nieuwe certificaat dat geldig is voor alle DNS-namen en IP-adressen die in Stap 13 gespecificeerd zijn.

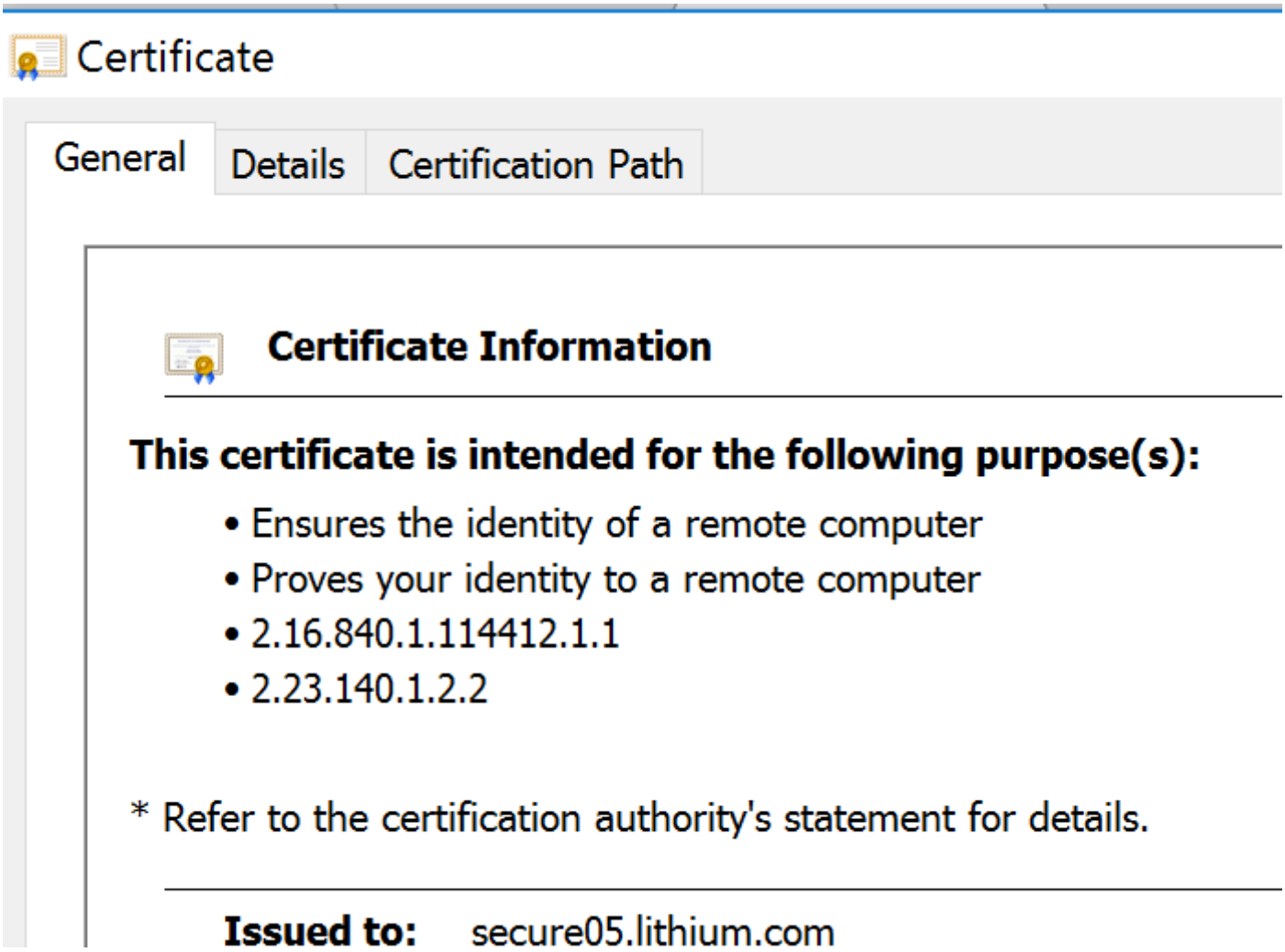
Stap 2. Aangezien de CA ten tijde van de handleiding is gemaakt, herkennen uw webbrowsers de standaard niet als geldig, moet u het certificaat handmatig importeren.

Stap 23. Navigeer naar het **CCM** met het gebruik van een geldige URL en druk op **Ctrl+Shift+i**, dit opent de ontwikkelingsgereedschappen.

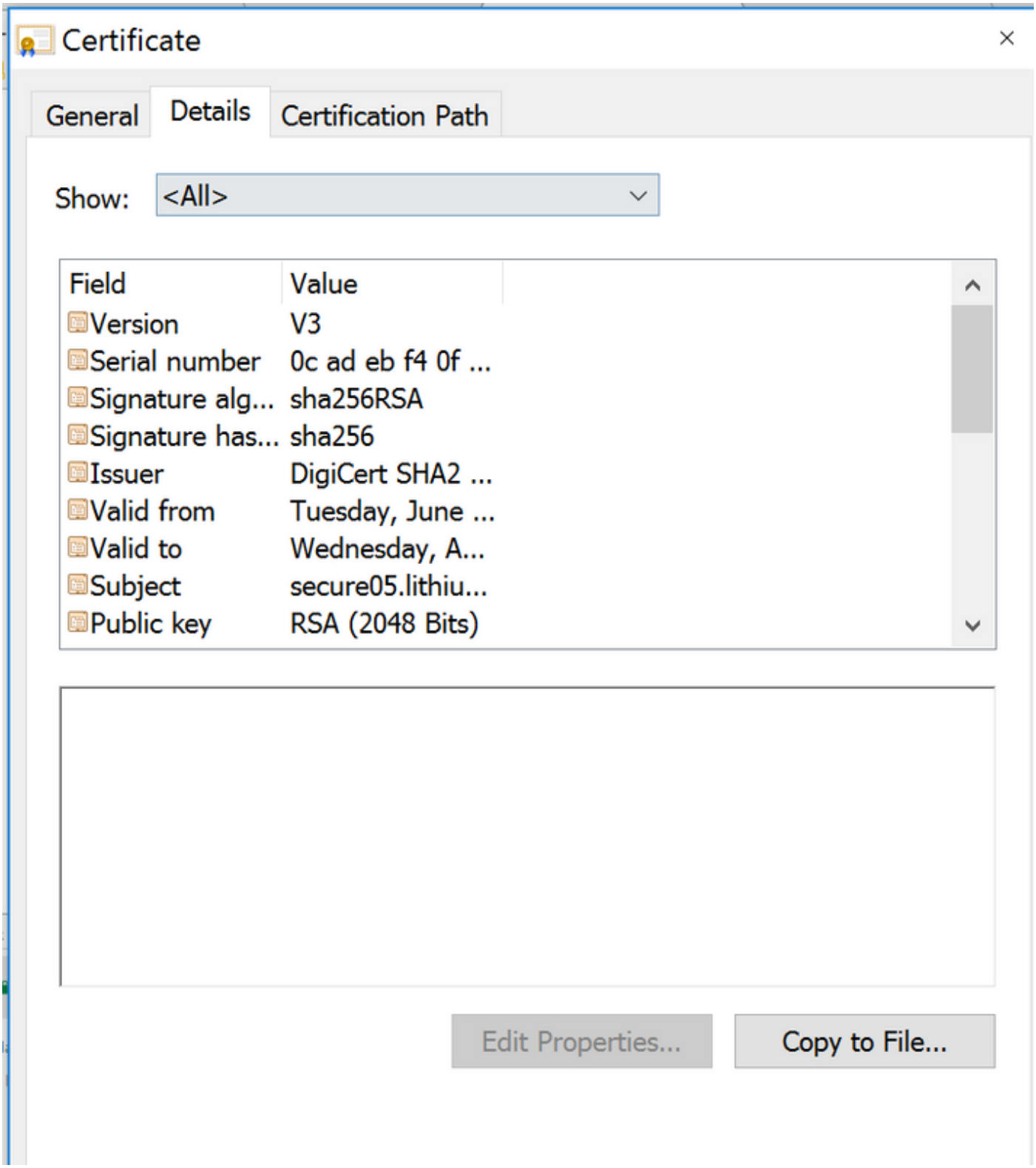
Stap 24. Selecteer **Certificaat bekijken** zoals in de afbeelding.



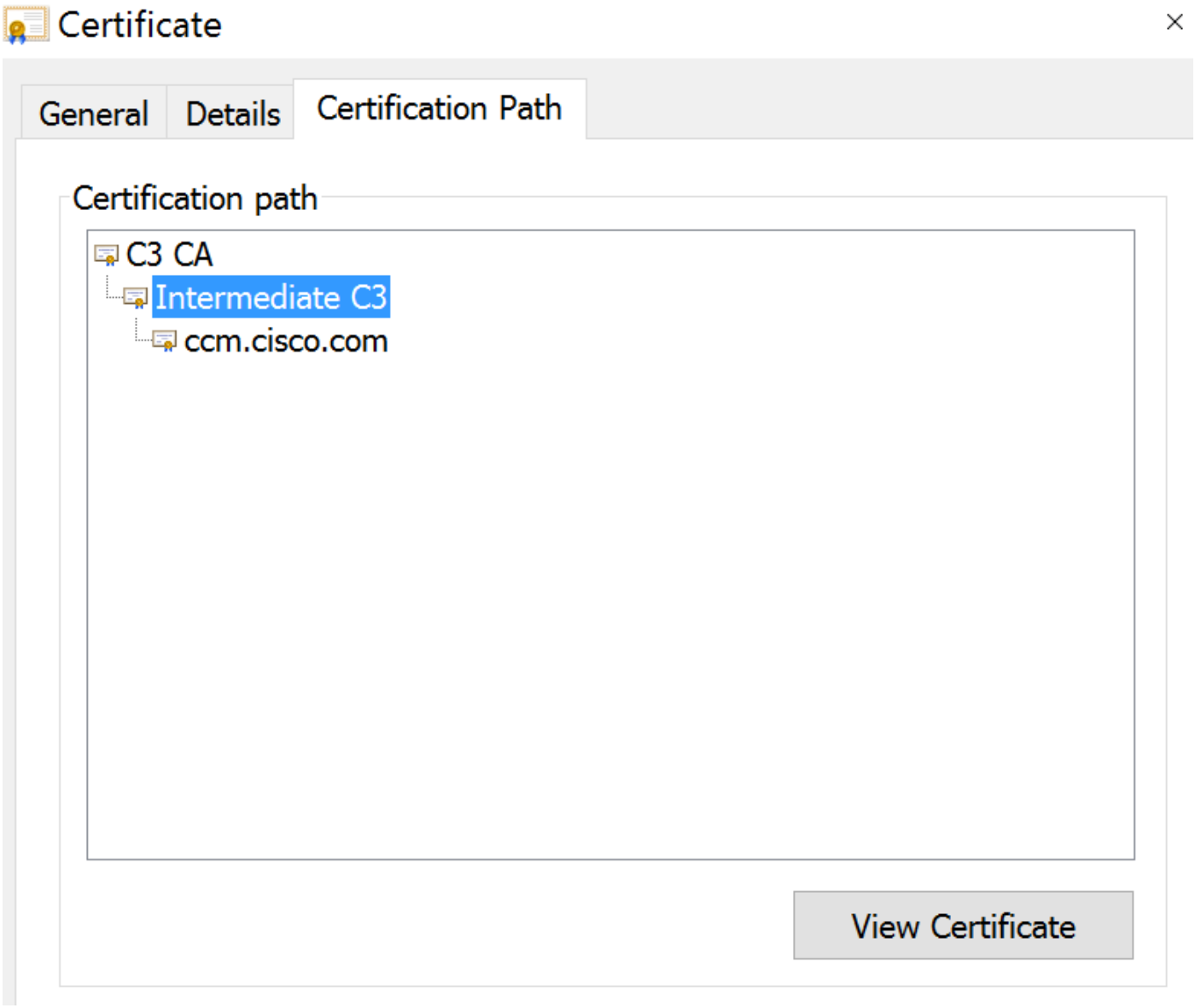
Stap 25. Selecteer **Details** zoals in de afbeelding.



Stap 26. Selecteer **Kopie naar bestand** zoals in de afbeelding.



Stap 27. Als u fouten over een onvertrouwde CA krijgt, navigeer dan naar **certificeringspad** om het certificaat Intermediate and Root te bekijken. U kunt op deze bestanden klikken en hun certificaat bekijken en deze ook naar bestanden kopiëren zoals in de afbeelding.



Stap 28. Zodra u de certificaten hebt gedownload, volgt u de instructies van uw besturingssysteem of browser om deze certificaten als vertrouwde instantie en intermediaire autoriteiten te installeren.