Criação dos certificados auto-assinados com URL múltiplas

Índice

[Introdução](#)
[Pré-requisitos](#)
[Requisitos](#)
[Componentes Utilizados](#)
[Problema](#)
[Solução](#)

Introdução

Este documento descreve como criar um certificado auto-assinado que possa ser usado por CloudCenter com URL múltiplas.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Certificados
- Linux

Componentes Utilizados

A informação neste documento é baseada em CentOS7.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Problema

Os Certificados que vêm padrão com CloudCenter, ou que podem ser criados com o uso do wizard de configuração do Cisco Call Manager (CCM), não têm um nome alternativo sujeito (SAN) que determinados navegadores, tais como Google Chrome, tratem como um erro e advirtam o. Isto pode ser cancelado, mas sem SAN, um certificado pode somente ser válido de uma URL específica.

Por exemplo, se você tem um certificado que seja válido para o endereço IP de Um ou Mais Servidores Cisco ICM NT de 10.11.12.13, se você tem um nome do Domain Name System (DNS)

de www.opencart.com, você receba um erro do certificado porque essa URL não é o que o certificado é para (este é verdadeiro mesmo se www.opencart.com é alistado em seus anfitriões arquiva como esse que pertence a 10.11.12.13). Isto pode colher acima se os sublocatários de CloudCenter estão no uso do único sinal sobre (SSO), porque cada server SSO tem sua própria URL.

Solução

A maneira a mais fácil de fixar esta edição é criar um certificado auto-assinado novo que tenha o SAN que alista toda a URL que o dirigir ao mesmo endereço IP de Um ou Mais Servidores Cisco ICM NT. O guia é uma tentativa de aplicar melhores prática a este processo.

Etapa 1. Navegue ao **diretório raiz** e faça um dobrador novo para abrigar os Certificados:

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

Etapa 2. Navegue no dobrador novo e faça subpastas para organizar os Certificados, as chaves privadas, e os logs.

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

Etapa 3. Copie os índices de **CAopenssl.conf a /root/ca/openssl.cnf**

> Nota: Este arquivo contém as opções de configuração para um Certificate Authority (CA) e as opções padrão que possam ser apropriados para CloudCenter.

Etapa 4. Gerencia uma chave privada e um certificado para 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
```

Etapa 5. Seu CA é a maneira final de verificar que todo o certificado é válido, este certificado deve nunca ser alcançado por indivíduos desautorizados e deve nunca ser exposto ao Internet. Devido a esta limitação, você tem que criar CA intermediário que assina o certificado da extremidade, isto cria uma ruptura onde se o certificado intermediário da autoridade lhe é comprometido possa ser revogado e um novo emitido.

Etapa 6. Faça um sub-diretório novo para CA intermediário.

```
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
```

Etapa 7. Copie os índices de **Intermediateopenssl.conf a** /root/ca/intermediate/openssl.cnf**.**

Nota: Este arquivo contém quase opções de configuração idêntica para CA a não ser algumas emendas pequenas para fazê-lo específico a um intermediário.

Etapa 8. Gerencia a chave e o certificado intermediários.

```
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
```

Etapa 9. Assine o certificado intermediário com o certificado de CA, isto constrói uma corrente da confiança que o navegador se use para verificar a autenticidade de um certificado.

```
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
```

Etapa 10. Crie uma corrente de CA, desde que você não quer CA no Internet, você pode fazer uma corrente de CA que os navegadores se usem para verificar a autenticidade toda a maneira até CA.

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

Etapa 11. Crie uma chave e um certificado novos para o 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
```

Etapa 12. Isto tem todos os campos requerido no comando e tem que ser editado manualmente.

- **/C =US** refere o país (2 carbonizam o limite)
- **/ST =NC** refere o estado e pôde incluir espaços
- **o =Cisco de /O** refere a organização
- **/CN =ccm.com refere o** Common Name, isto deve ser a URL principal usada para alcançar o CCM.
- **O SAN \ nsubjectAltName=** são os nomes alternativos, o Common Name deve estar nesta lista e não há nenhum limite ao quanto você do SAN tem.

Etapa 13. Assine o certificado final com o uso do certificado intermediário.

```
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
```

Etapa 14. Verifique que o certificado esteve assinado corretamente.

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

Etapa 15. Pode retornar uma APROVAÇÃO ou uma falha.

Etapa 16. Copie o certificado novo, é chave, e a CA-corrente ao dobrador de **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
```

Etapa 17. Permissões da posse e do grupo do cliqruser de Grant corretamente.

```
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
```

Etapa 18. Backup o **arquivo server.xml** antes que você fizer todas as mudanças.

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

Etapa 19. Edite **server.xml:**

1. Encontre a seção que começa com **<Connector port="10443" maxHttpHeaderSize="8192"**
2. Mude **SSLCertificateFile** para apontar a ccm.com.crt
3. Mude **SSLCertificateKeyFile** para apontar a ccm.com.key
4. Mude **SSLCACertificateFile** para apontar a ca-chain.crt

Etapa 20. Reinício Tomcat.

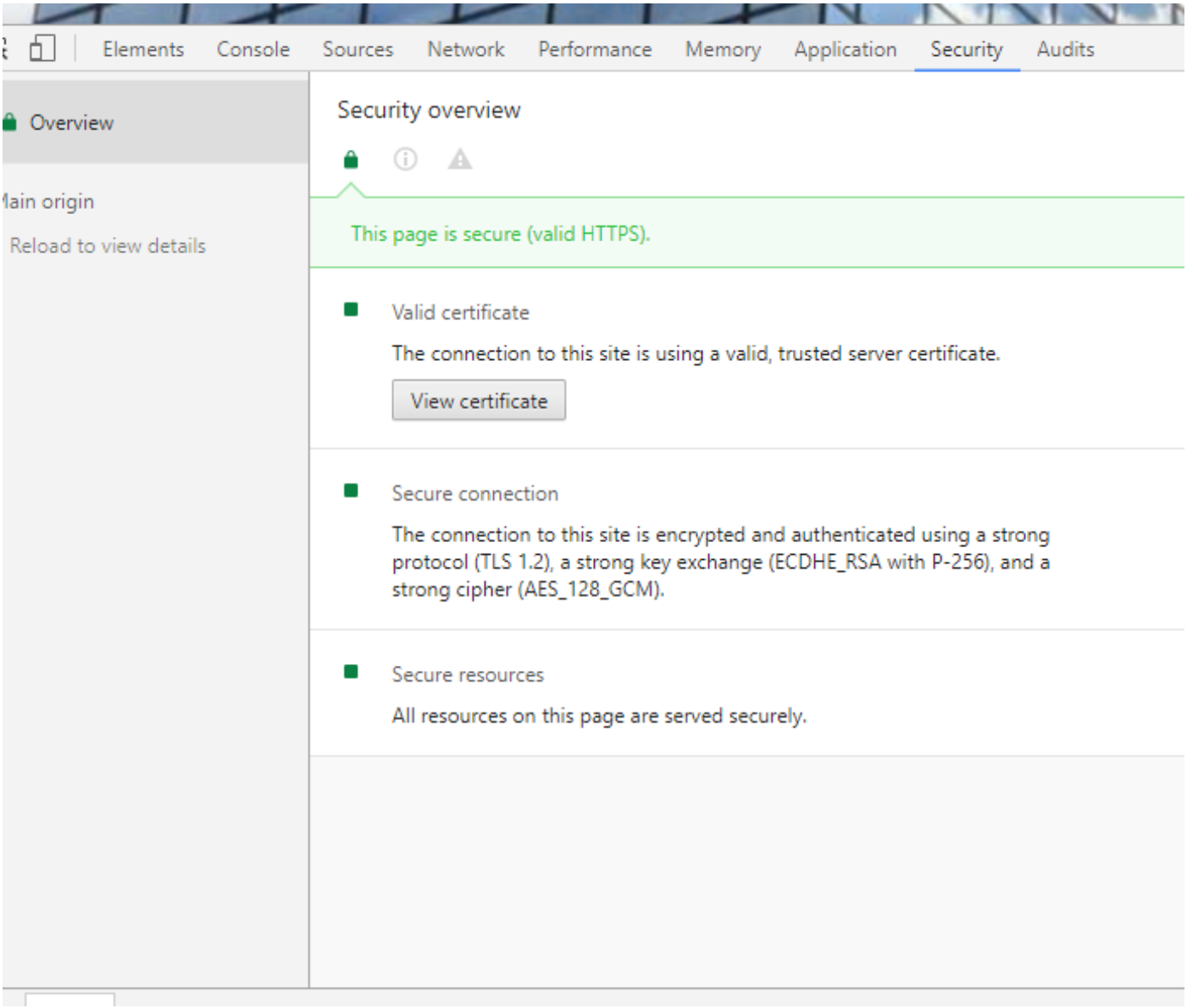
```
service tomcat stop
service tomcat start
```

Etapa 21. O CCM usa agora o certificado novo que é válido para todos os nomes de DNS e endereços IP de Um ou Mais Servidores Cisco ICM NT especificados em etapa 13.

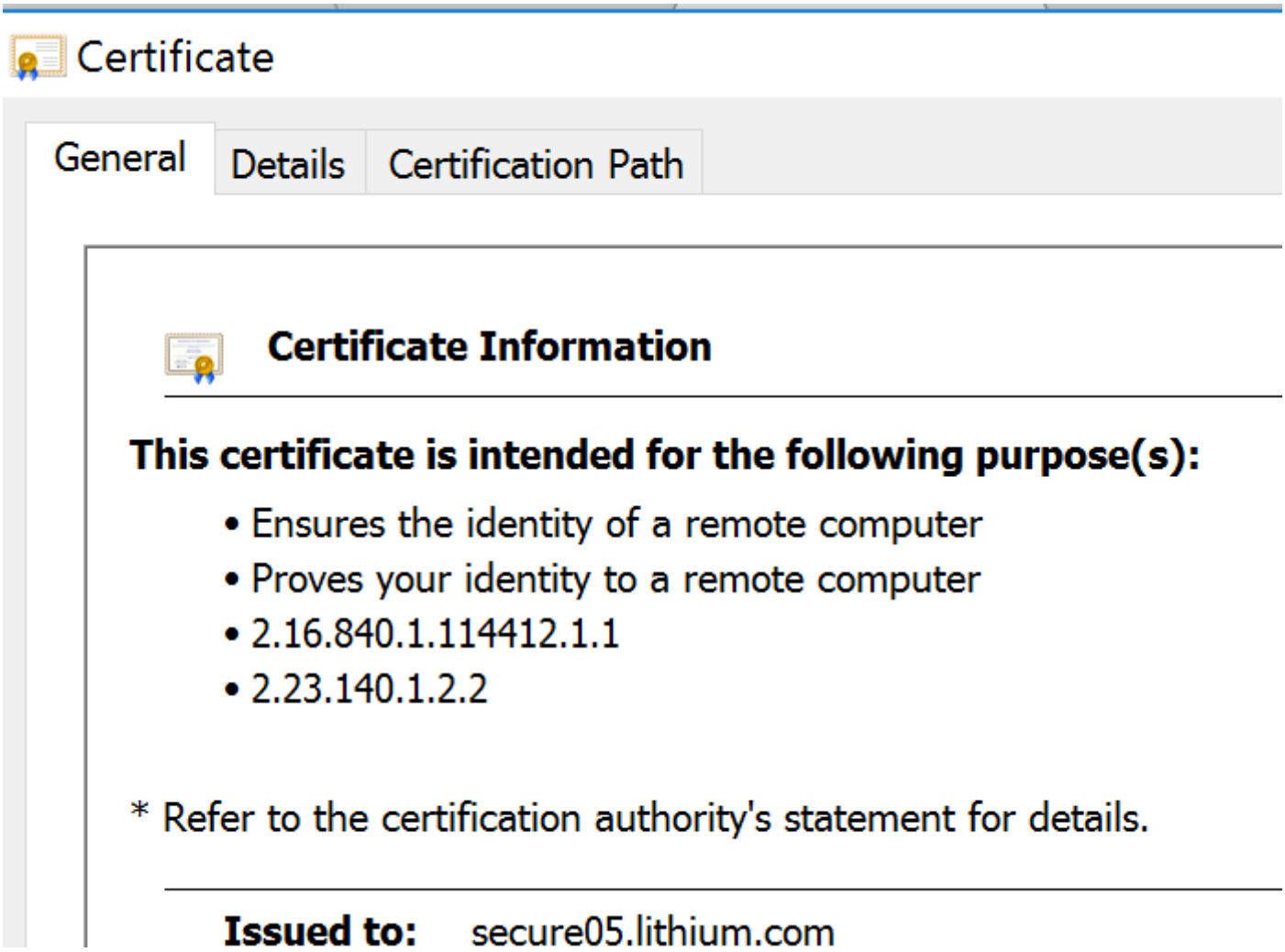
Etapa 22. Porque CA foi criado na altura do guia, seus navegadores não o reconhecerão como válido à revelia, você tem que manualmente importar o certificado.

Etapa 23. Navegue ao **CCM** com o uso de toda a URL válida e pressione **Ctrl+Shift+i**, isto abre as ferramentas do colaborador.

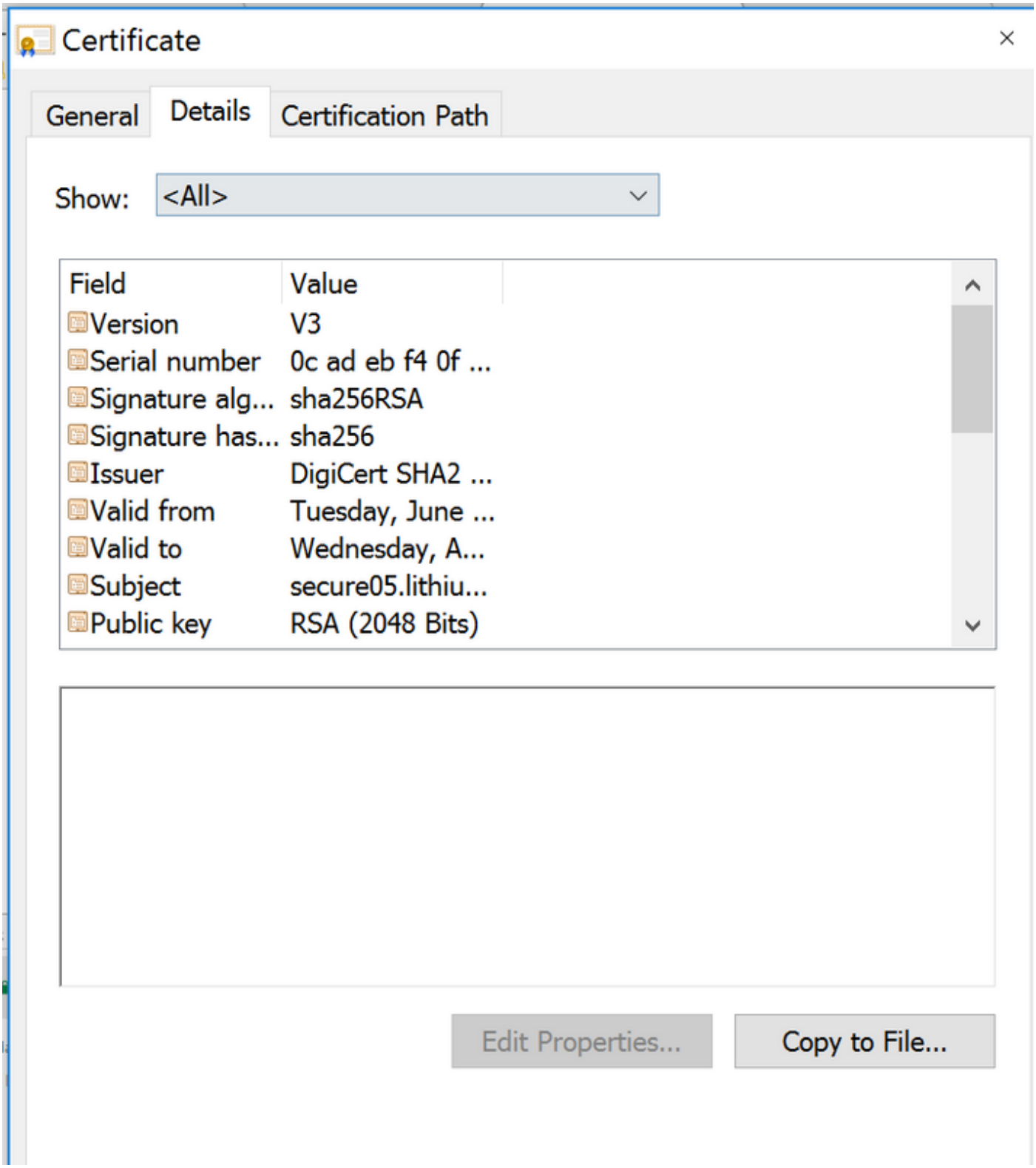
Etapa 24. Selecione o **certificado da vista** segundo as indicações da imagem.



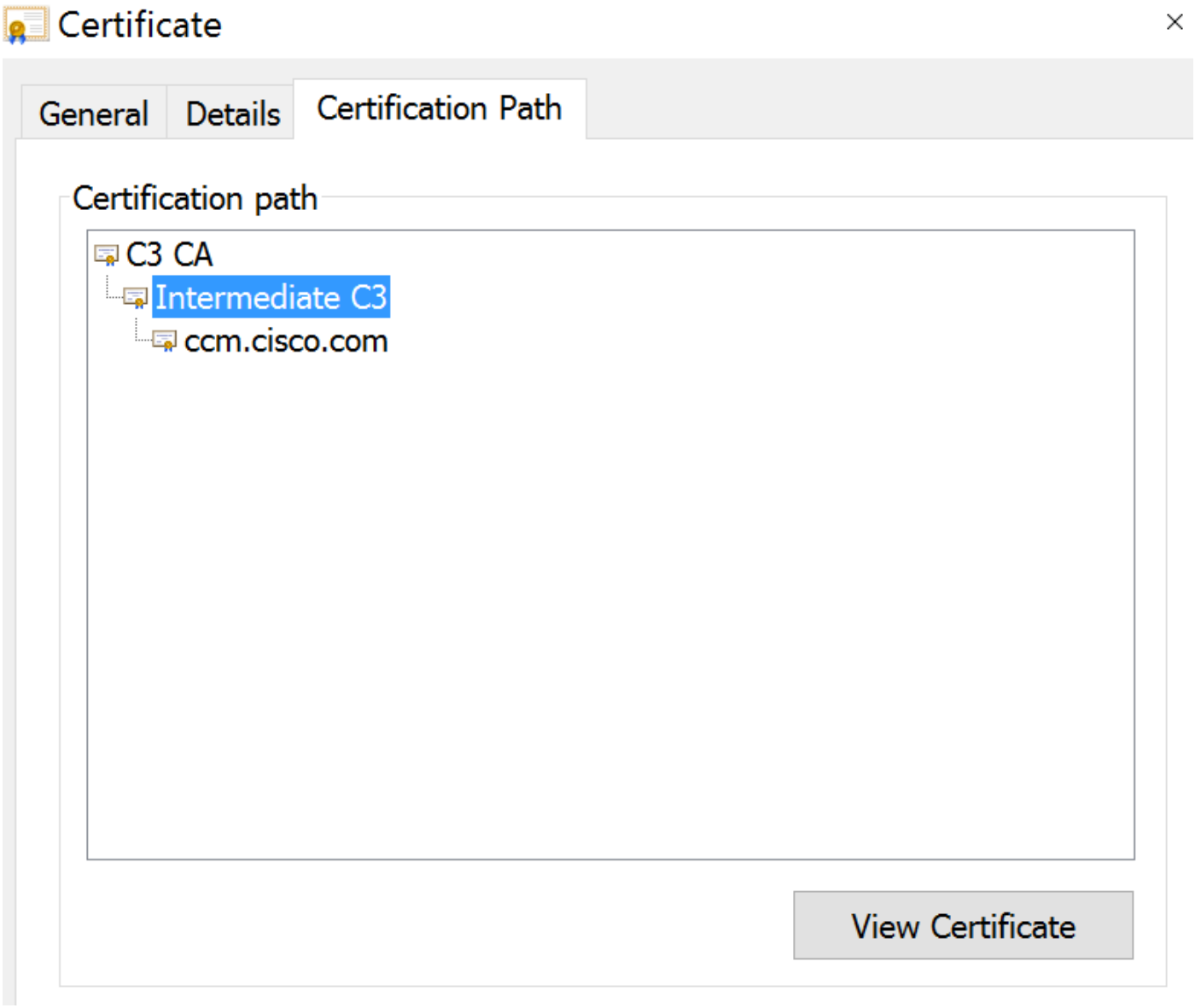
Etapa 25. Selecione **detalhes** segundo as indicações da imagem.



Etapa 26. Selecione a **cópia para arquivar** segundo as indicações da imagem.



Etapa 27. Se você obtém erros sobre CA não confiável, a seguir navegue ao **caminho de certificação** para ver o intermediário e o certificado de raiz. Você pode clicá-los sobre e ver seu certificado e igualmente copiar aqueles aos arquivos segundo as indicações da imagem.



Etapa 28. Uma vez que você tem os Certificados transferidos, siga suas instruções do sistema operacional (OS) ou do navegador para instalar estes Certificados como a autoridade confiada e autoridades intermediárias.