Creación de los certificados autofirmados con los URL múltiples

Contenido

Introducción

Este documento describe cómo crear un certificado autofirmado que se pueda utilizar por CloudCenter con los URL múltiples.

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Certificados
- Linux

Componentes Utilizados

La información en este documento se basa en CentOS7.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Problema

Los Certificados que vienen estándar con CloudCenter, o que se pueden crear con el uso del asistente de configuración del Cisco Call Manager (CCM), no tienen un nombre alternativo sujeto (SAN) que ciertos navegadores, tales como Google Chrome, traten como error y adviertan le. Esto puede ser reemplazada, pero sin los SAN, un certificado puede solamente ser válido a partir de un URL específico.

Por ejemplo, si usted tiene un certificado que sea válido para la dirección IP de 10.11.12.13, si usted tiene un nombre del Sistema de nombres de dominio (DNS) de www.opencart.com, usted

reciba un error del certificado porque ese URL no es para cuál está el certificado (éste es verdad incluso si www.opencart.com se enumera en sus host clasifía como el que pertenece a 10.11.12.13). Esto puede surgir si los subarrendatarios de CloudCenter están en el uso de la sola muestra prendido (SSO), pues cada servidor SSO tiene su propio URL.

Solución

La manera más fácil de reparar este problema es crear un nuevo certificado autofirmado que tenga SAN que enumere cualquier URL que le dirija a la misma dirección IP. La guía es una tentativa de aplicar las mejores prácticas a este proceso.

Paso 1. Navegue al **directorio raíz** y haga una nueva carpeta para contener los Certificados:

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

Paso 2. Navegue en la nueva carpeta y haga el subfolders para ordenar los Certificados, las claves privadas, y los registros.

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

Paso 3. Copie el contenido de **CAopenssl.conf a /root/ca/openssl.cnf**

> Nota: Este archivo contiene las opciones de configuración para un Certificate Authority (CA) y las opciones predeterminadas que pudieron ser apropiados para CloudCenter.

Paso 4. Genere una clave privada y un 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
```

Paso 5. Su CA es la última manera de verificar que cualquier certificado es válido, este certificado se debe nunca acceder por los individuos desautorizados y se debe nunca exponer a Internet. Debido a esta restricción, usted tiene que crear CA intermedio que firma el certificado del extremo, esto crea una rotura donde si el certificado intermedio de la autoridad se compromete le puede ser revocado y un nuevo publicado.

Paso 6. Haga un nuevo sub-directório para CA intermedio.

```
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
```

Paso 7. Copie el contenido de **Intermediateopenssl.conf a** /root/ca/intermediate/openssl.cnf**.**

Nota: Este archivo contiene casi las opciones de configuración idéntica para CA con excepción de algunos pequeños pellizcos para hacerlo específico a un intermedio.

Paso 8. Genere la clave y el certificado intermedios.

```
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
```

Paso 9. Firme el certificado intermedio con el certificado de CA, esto construye un encadenamiento de la confianza que el navegador utilice para verificar la autenticidad de un 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
```

Paso 10. Cree un encadenamiento de CA, puesto que usted no quiere CA en Internet, usted puede hacer un encadenamiento de CA que los navegadores utilicen para verificar la autenticidad hasta el final hasta 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
```

Paso 11 Cree una nuevos clave y certificado para 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
```

Paso 12. Esto tiene todos los campos obligatorios en el comando y tiene que ser editada manualmente.

- **/C =US** refiere al país (2 carbonizan el límite)
- **/ST =NC** refiere al estado y pudo incluir los espacios
- **el =Cisco de /O** refiere a la organización
- **/CN =ccm.com refiere al** Common Name, esto debe ser el URL principal usado para acceder CCM.
- **El SAN \ el nsubjectAltName=** son los nombres alternativos, el Common Name debe estar en esta lista y no hay límite a cuánto usted SAN tiene.

Paso 13. Firme el certificado final con el uso del certificado intermedio.

```
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
```

Paso 14. Verifique que el certificado fuera firmado correctamente.

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

Paso 15. Puede volver una AUTORIZACIÓN o un fall.

Paso 16. Copie el nuevo certificado, es dominante, y el CA-encadenamiento a la carpeta 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
```

Paso 17. Permisos de la propiedad y del conjunto del cliqruser de Grant correctamente.

```
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
```

Paso 18. Respaldo el **archivo server.xml** antes de que usted realice cualquier cambio.

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

Paso 19. Edite **server.xml:**

1. Localice la sección que comienza con el **<Connector el port="10443" el maxHttpHeaderSize="8192"**
2. Cambie **SSLCertificateFile** para señalar a ccm.com.crt
3. Cambie **SSLCertificateKeyFile** para señalar a ccm.com.key
4. Cambie **SSLCACertificateFile** para señalar a ca-chain.crt

Paso 20. Reinicio Tomcat.

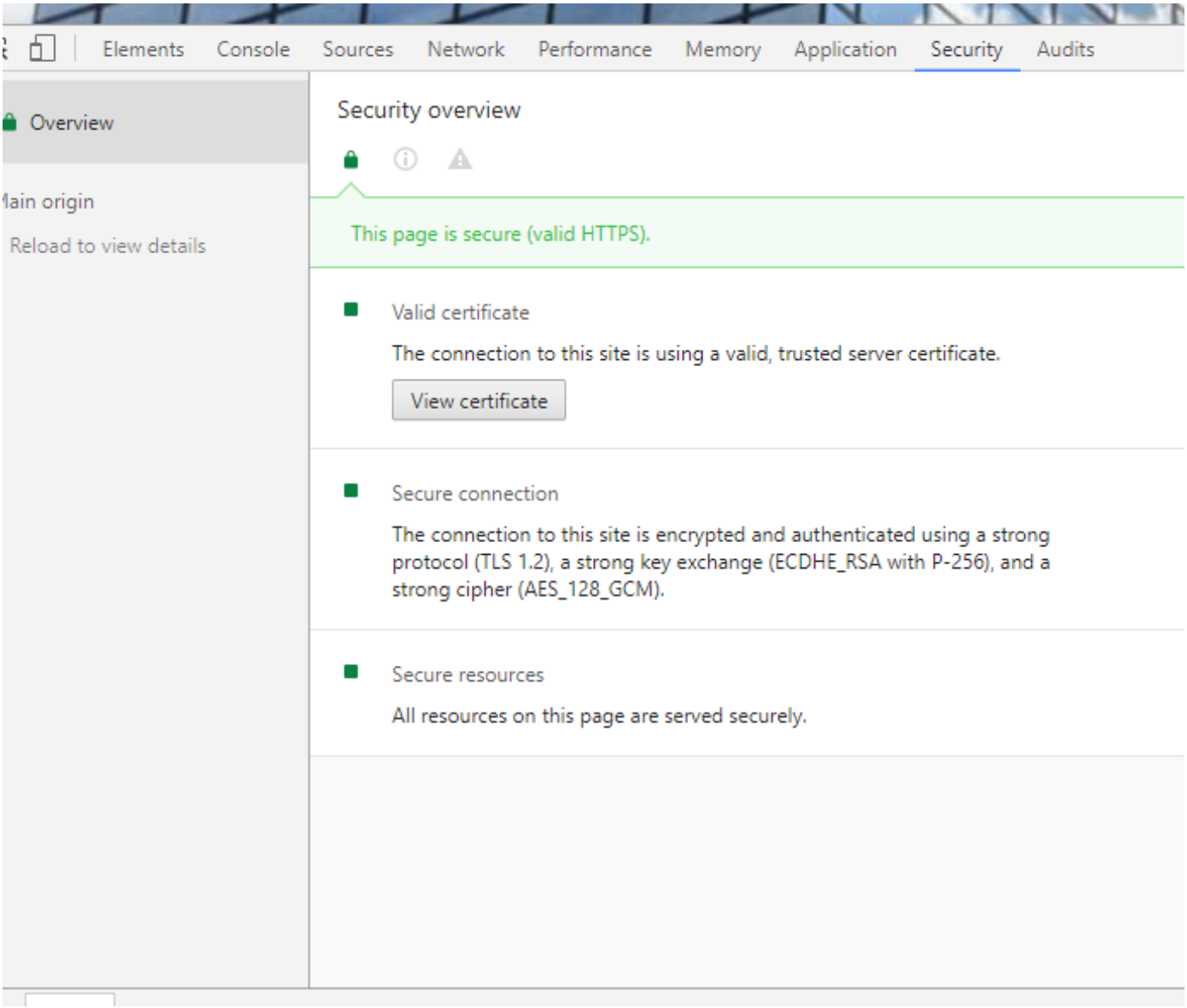
```
service tomcat stop
service tomcat start
```

Paso 21. CCM ahora utiliza el nuevo certificado que es válido para todos los nombres DNS y IP Addresses especificados en el paso 13.

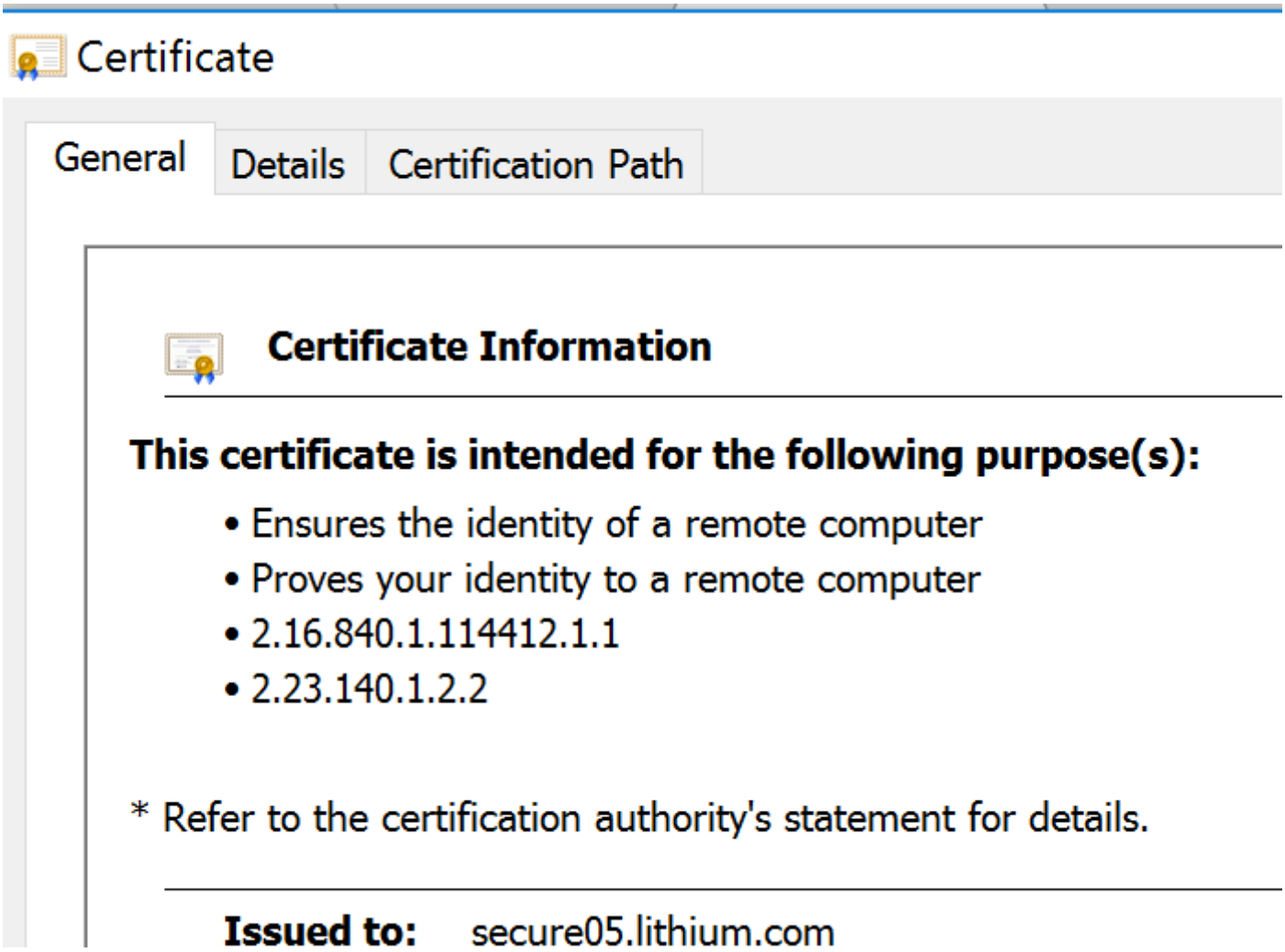
Paso 22. Pues CA fue creado a la hora de la guía, sus navegadores no la reconocerán como válido por abandono, usted tiene que importar manualmente el certificado.

Paso 23. Navegue a **CCM** con el uso de cualquier URL válido y presione **Ctrl+Shift+i**, esto abre las herramientas del desarrollador.

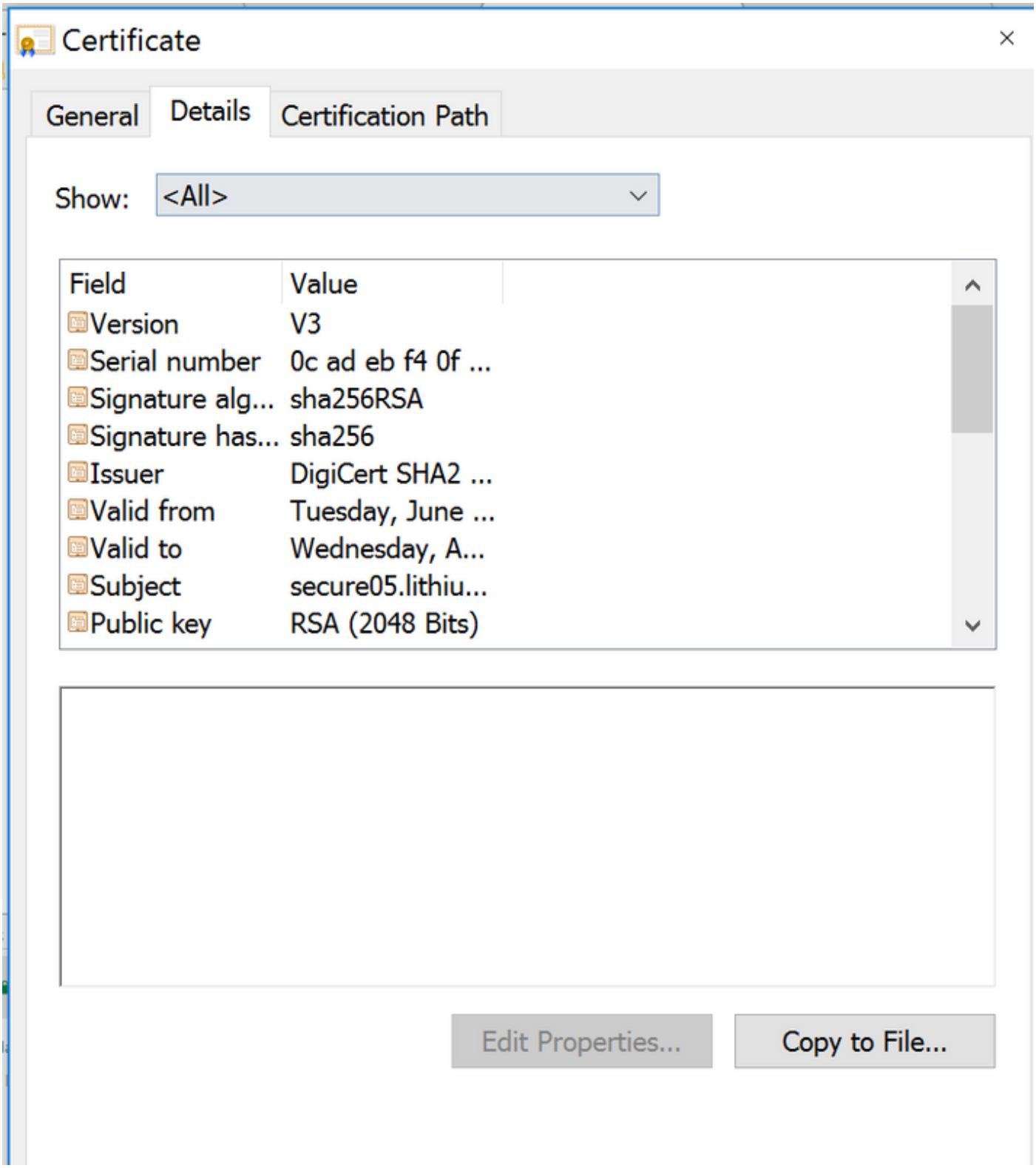
Paso 24. Seleccione el **certificado de la visión** tal y como se muestra en de la imagen.



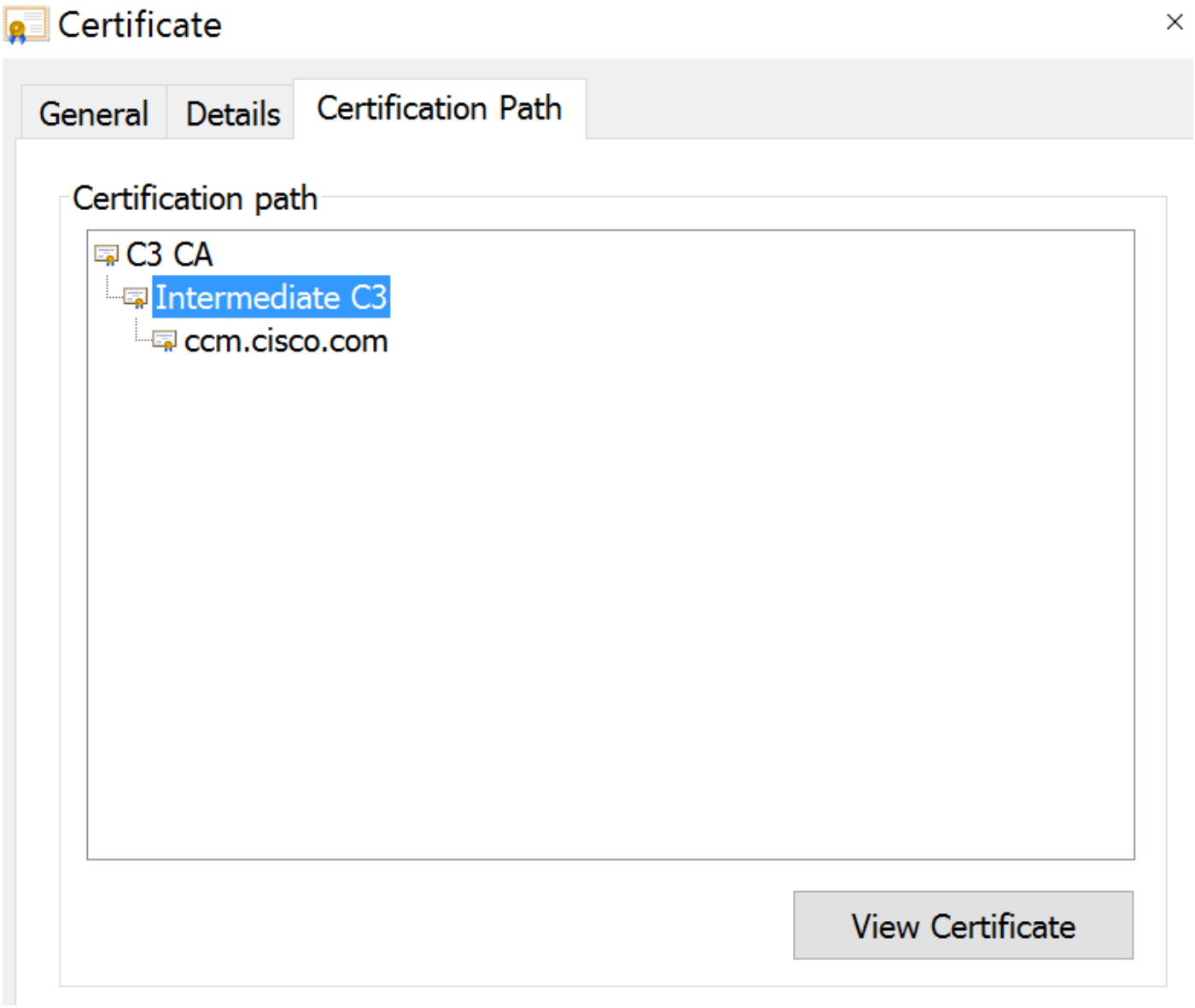
Paso 25. Seleccione los **detalles** tal y como se muestra en de la imagen.



Paso 26. Seleccione la **copia para clasifiar** tal y como se muestra en de la imagen.



Paso 27. Si usted consigue los errores sobre un CA untrusted, después navegue al **trayecto de certificación** para ver el intermedio y el certificado raíz. Usted puede hacerlos clic en y ver su certificado y también copiar ésos a los archivos tal y como se muestra en de la imagen.



Paso 28. Una vez que usted hace los Certificados descargar, siga sus instrucciones del sistema operativo (OS) o del navegador de instalar estos Certificados como la autoridad de confianza y autoridades intermedias.