Création des Certificats Auto-signés avec des URL de multiple

Contenu

Introduction

Ce document décrit comment créer un certificat auto-signé qui peut être utilisé par CloudCenter avec des URL de multiple.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Certificats
- Linux

Composants utilisés

Les informations dans ce document sont basées sur CentOS7.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Problème

Les Certificats qui sont livré la norme avec CloudCenter, ou qui peuvent être créés avec l'utilisation de l'assistant de configuration de Cisco Call manager (CCM), n'ont pas un nom alternatif soumis (SAN) que certains navigateurs, tels que Google Chrome, traite comme erreur et avertit vous. Ceci peut être ignoré, mais sans SAN, un certificat peut seulement être valide d'un URL spécifique.

Par exemple, si vous avez un certificat qui est valide pour l'adresse IP de 10.11.12.13, si vous avez un nom de Système de noms de domaine (DNS) de www.opencart.com, vous reçoivent une

erreur de certificat parce que n'est pas cet URL pour ce que le certificat est (c'est vrai même si www.opencart.com est répertorié dans des vos hôtes classent en tant que celui qui appartiennent à 10.11.12.13). Ceci peut survenir si les sous locataire de CloudCenter sont dans l'utilisation de simple se connectent (SSO), car chaque serveur SSO a son propre URL.

Solution

Le moyen le plus simple de réparer cette question est de créer un nouveau certificat auto-signé qui a le SAN qui répertorie n'importe quel URL qui vous dirige vers la même adresse IP. Le guide est une tentative de s'appliquer des pratiques recommandées à ce processus.

Étape 1. Naviguez vers le **répertoire racine** et faites un nouveau répertoire pour loger les Certificats :

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

Étape 2. Naviguez dans le nouveau répertoire et faites les sous-dossiers pour organiser les Certificats, les clés privées, et les logs.

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

Étape 3. Copiez le contenu de **CAopenssl.conf sur /root/ca/openssl.cnf**

> Remarque: Ce fichier contient les options de configuration pour un Autorité de certification (CA) et les options par défaut qui pourraient être appropriés pour CloudCenter.

Étape 4. Générez une clé privée et la délivrez un certificat pour le 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
```

Étape 5. Votre CA est la manière finale de vérifier que n'importe quel certificat est valide, ce certificat doit ne jamais être accédé à par les personnes non autorisées et doit ne jamais être exposé à l'Internet. En raison de cette restriction, vous devez créer un intermédiaire CA qui signe le certificat d'extrémité, ceci crée une rupture où si le certificat intermédiaire d'autorité lui est compromis peut être retiré et un neuf émis.

Étape 6. Faites un nouveau sous-répertoire pour l'intermédiaire 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
```

Étape 7. Copiez le contenu d'**Intermediateopenssl.conf sur** /root/ca/intermediate/openssl.cnf**.**

Remarque: Ce fichier contient presque des options de configuration identique pour le CA autre que quelques petits coups secs de le rendre spécifique à une intermédiaire.

Étape 8. Éditez **/root/ca/intermediate/openssl.cnf** pour inclure le SAN qui est exigé.

Remarque: La toute dernière section est [des alternate_names], change ceci pour avoir les adresses IP et les noms DNS qui met en référence votre CCM. Vous pouvez avoir autant d'adresses IP ou noms DNS comme vous voudrez.

Étape 9. Générez la clé intermédiaire et la délivrez un certificat.

```
cd /root/ca
openssl genrsa -aes 256 -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
```

Étape 10. Signez le certificat intermédiaire avec le certificat de CA, ceci construit une chaîne de confiance que le navigateur l'utilise pour vérifier l'authenticité d'un certificat.

```
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
```

Étape 11. Créez une chaîne CA, puisque vous ne voulez pas le CA sur l'Internet, vous peut faire une chaîne CA que les navigateurs les utilisent pour vérifier l'authenticité complètement jusqu'au 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
```

Étape 12. Créez une nouvelle clé et la délivrez un certificat pour le CCM.

```
openssl genrsa -out intermediate/private/ccm.key.pem 2048
openssl req -new -sha256 -key intermediate/private/ccm.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.csr
```

Étape 13. Ceci a tous les champs requis dans la commande et doit être édité manuellement.

- **/C =US** se rapporte au pays (la limite de 2 cars)
- **/ST =NC** se rapporte à l'état et pourrait inclure les espaces
- **le =Cisco de /O** se rapporte à l'organisation
- **/CN =ccm.com se rapporte au** nom commun, ceci devrait être l'URL principal utilisé pour accéder au CCM.
- **Le SAN \ nsubjectAltName=** sont les noms alternatifs, le nom commun devrait être sur cette liste et il n'y a aucune limite combien vous du SAN avez.

Étape 14. Signez le certificat final avec l'utilisation du certificat intermédiaire.

```
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
```

Étape 15. Vérifiez que le certificat a été signé correctement.

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

Étape 16. Il peut renvoyer un OK ou un échouer.

Étape 17. Copiez le nouveau certificat, c'est principal, et la Ca-chaîne au répertoire 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
```

Étape 18. Autorisations de propriété et de positionnement de cliqruser de Grant correctement.

```
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
```

Étape 19. Sauvegarde le **fichier server.xml** avant que vous apportiez toutes les modifications.

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

Étape 20. Éditez **server.xml :**

1. Localisez la section qui commence par le **<Connector port="10443" maxHttpHeaderSize="8192"**
2. Modification **SSLCertificateFile** à indiquer ccm.com.crt
3. Modification **SSLCertificateKeyFile** à indiquer ccm.com.key
4. Modification **SSLCACertificateFile** à indiquer ca-chain.crt

Étape 21. Reprise Tomcat.

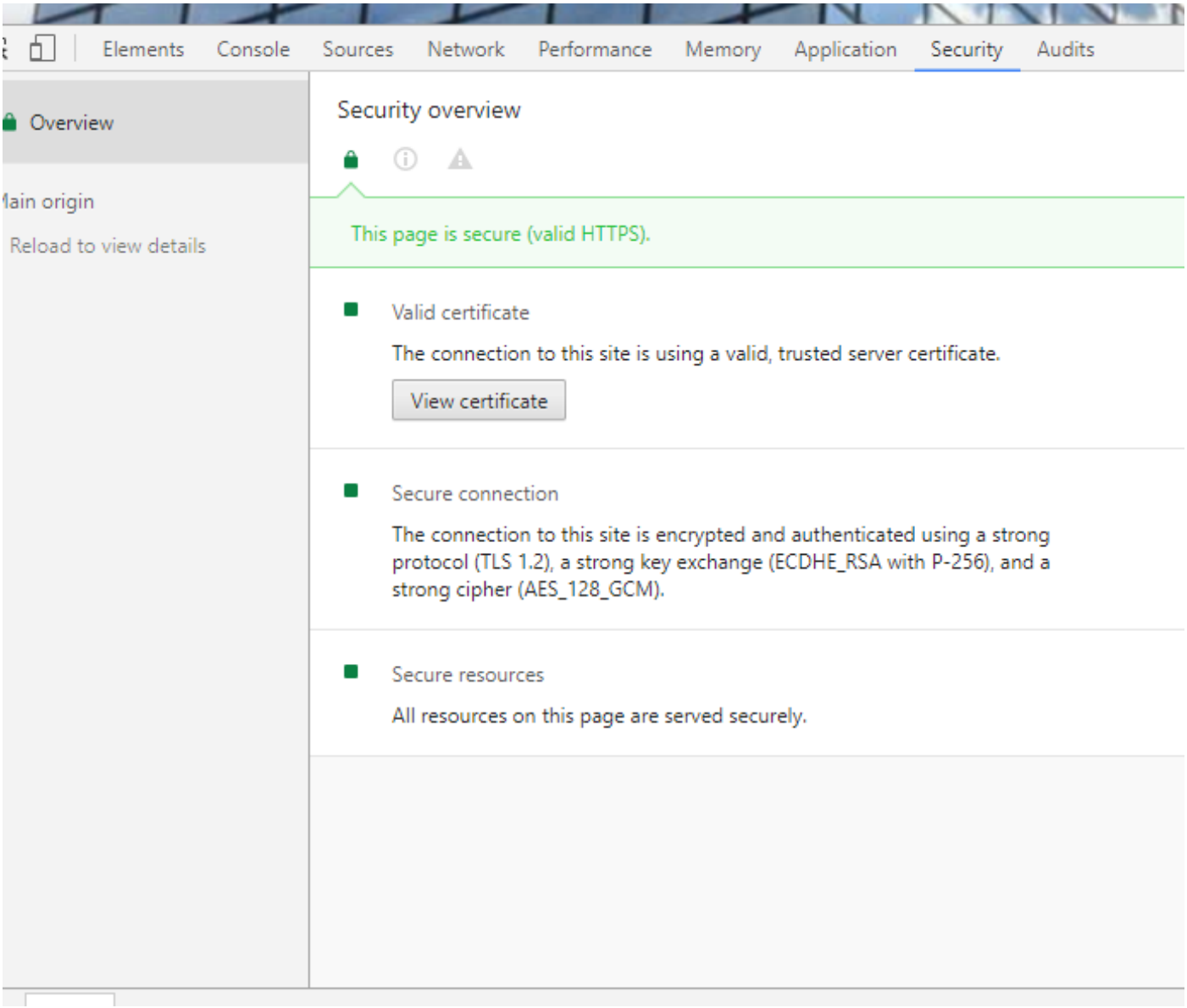
```
service tomcat stop
service tomcat start
```

Étape 22. Le CCM utilise maintenant le nouveau certificat qui est valide pour tous les noms DNS et adresses IP spécifiés dans l'étape 13.

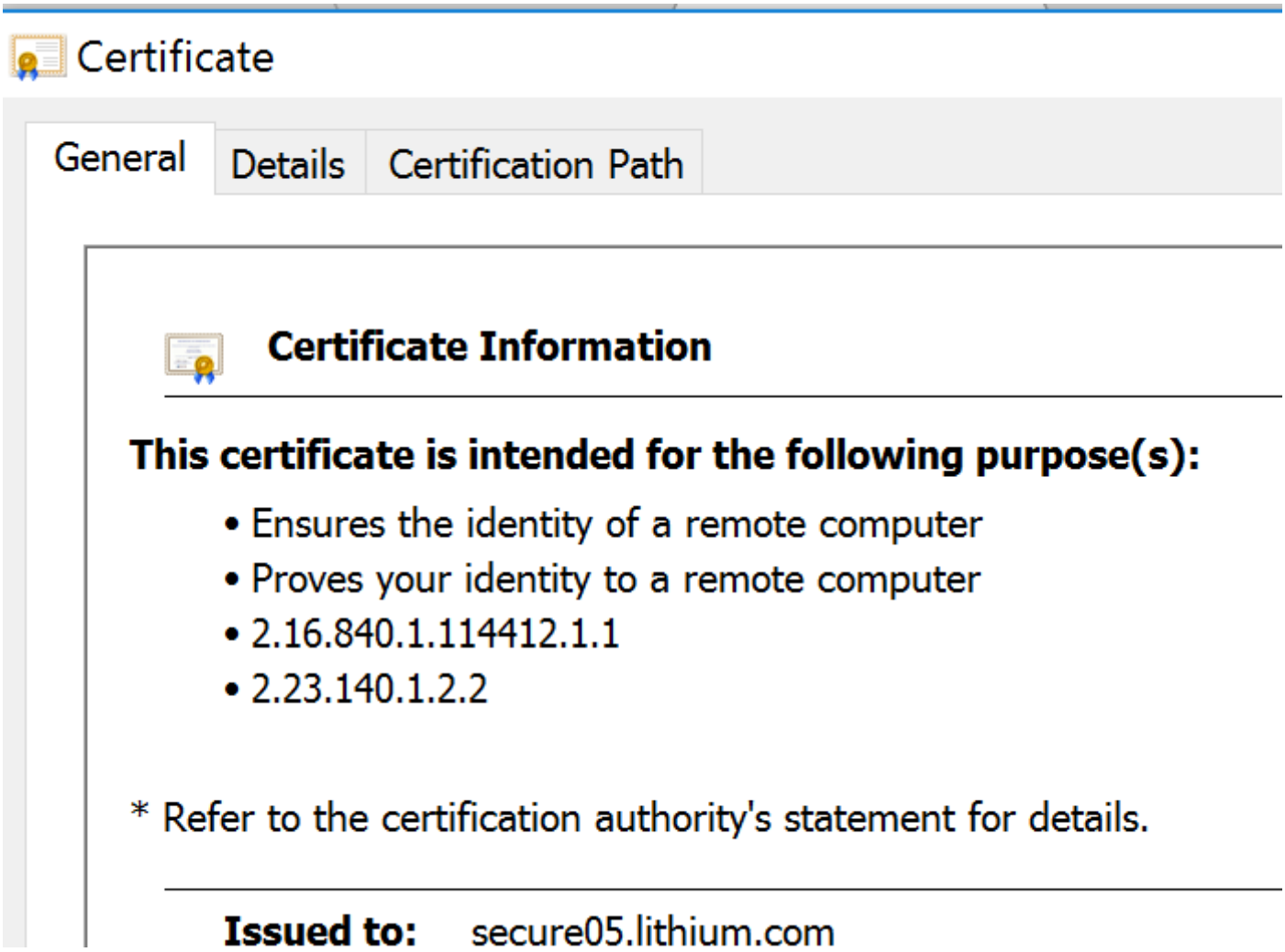
Étape 23. Car le CA a été créé au moment du guide, vos navigateurs ne l'identifieront pas en tant que valide par défaut, vous doivent manuellement importer le certificat.

Étape 24. Naviguez vers le **CCM** avec l'utilisation de n'importe quel URL valide et appuyez sur **Ctrl+Shift+i**, ceci ouvre les outils pour développeurs.

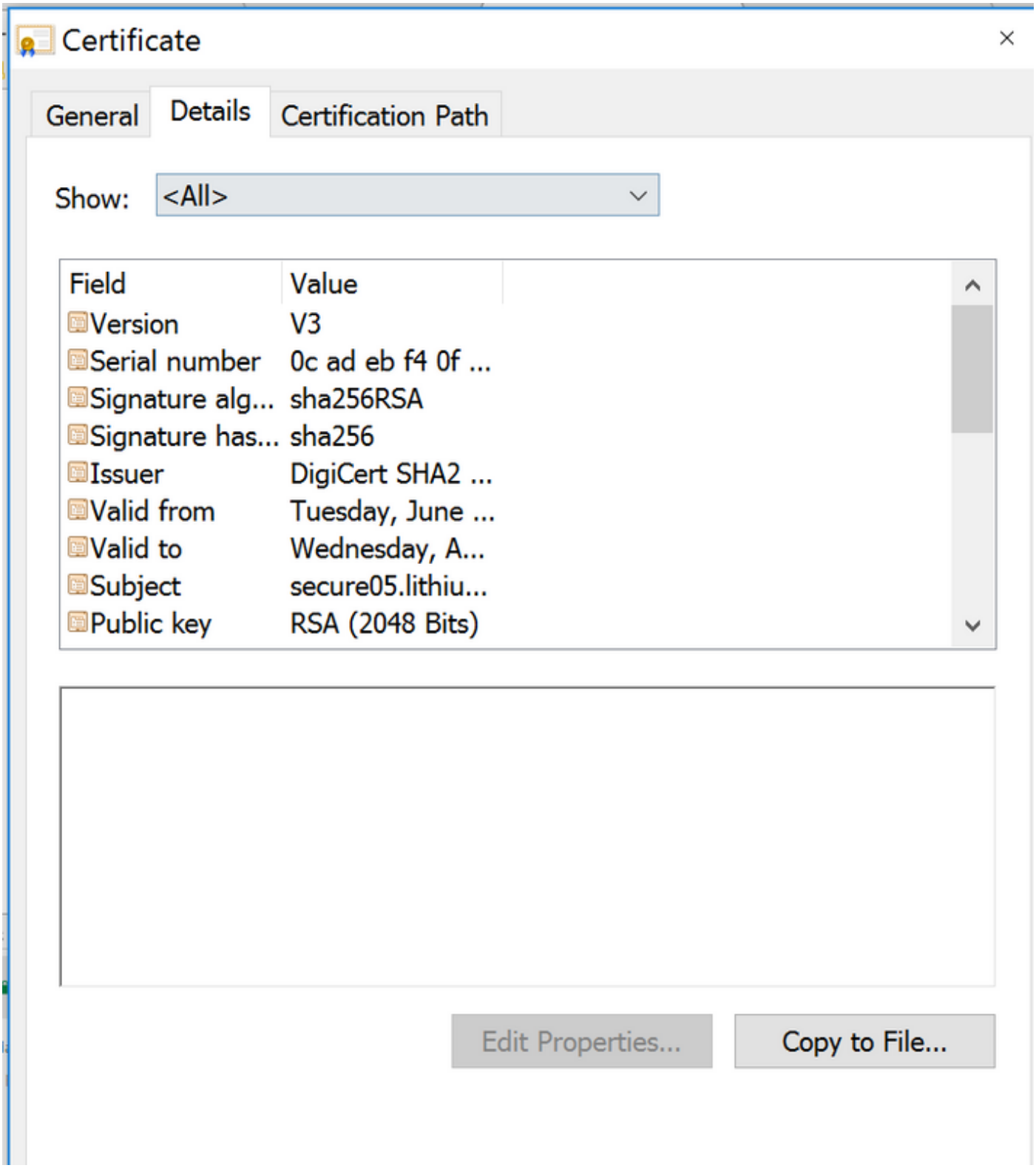
Étape 25. **Certificat** choisi de **vue** suivant les indications de l'image.



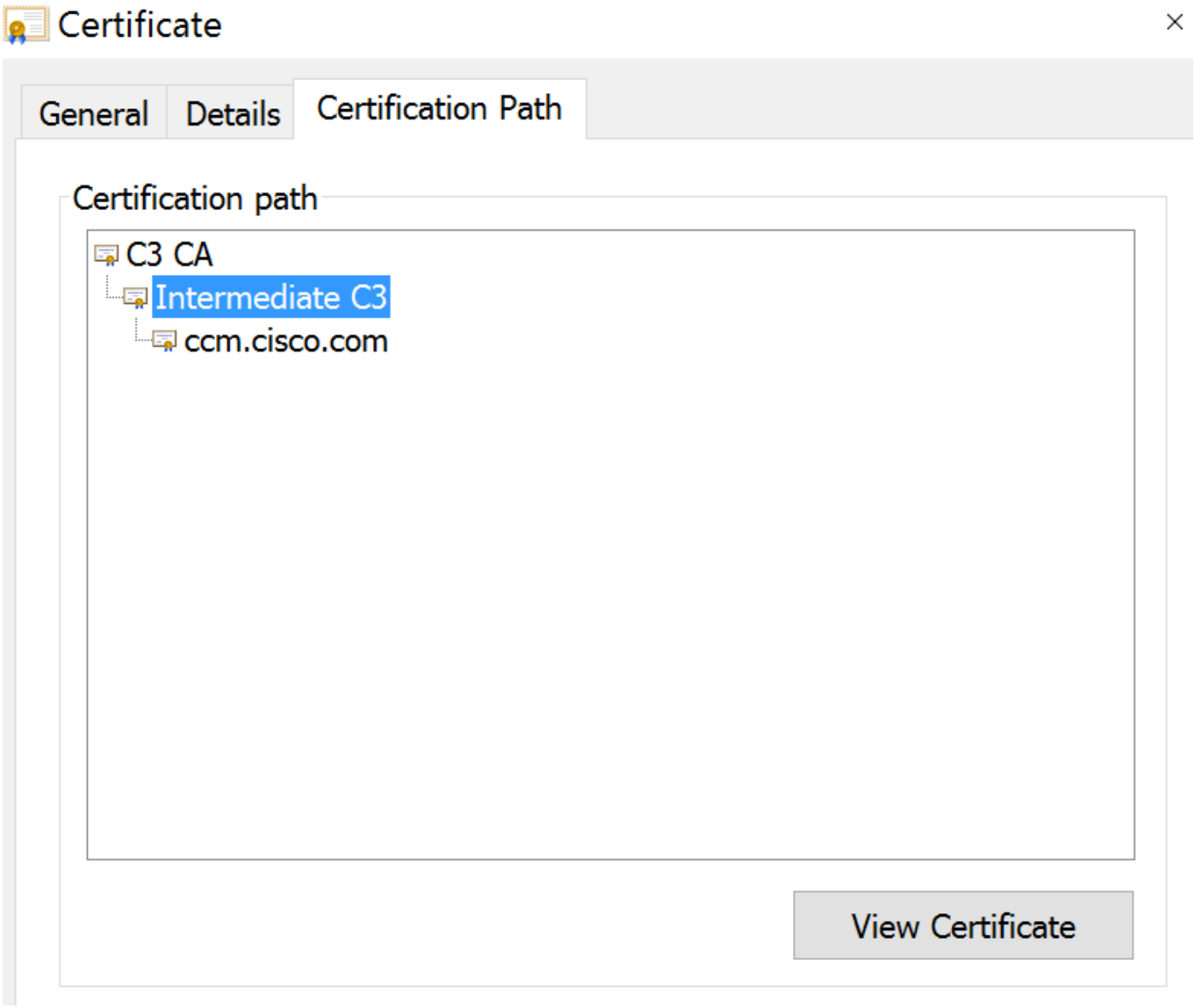
Étape 26. **Détails** choisis suivant les indications de l'image.



Étape 27. Sélectionnez la **copie pour classer** suivant les indications de l'image.



Étape 28. Si vous obtenez des erreurs au sujet d'un CA non approuvé, alors naviguez vers le **chemin de certification** pour visualiser l'intermédiaire et le certificat racine. Vous pouvez les cliquer sur en fonction et visualiser leur certificat et également copier ceux sur des fichiers suivant les indications de l'image.



Étape 29. Une fois que vous faites télécharger les Certificats, suivez vos instructions du système d'exploitation (SYSTÈME D'EXPLOITATION) ou du navigateur d'installer ces Certificats en tant qu'autorités de confiance d'autorité et d'intermédiaire.