Creazione di certificati autofirmati con più URL

Sommario

Introduzione

Questo documento descrive come creare un certificato autofirmato che può essere utilizzato da CloudCenter con più URL.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Certificati
- Linux

Componenti usati

Le informazioni di questo documento si basano su CentOS7.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Problema

I certificati forniti con CloudCenter o che possono essere creati con la configurazione guidata di Cisco Call Manager (CCM) non dispongono di una SAN (Subject Alternative Name) che alcuni browser, ad esempio Google Chrome, considerano un errore e avvisa l'utente. È possibile ignorare questa impostazione, ma senza SAN un certificato può essere valido solo da un URL specifico.

Ad esempio, se si dispone di un certificato valido per l'indirizzo IP 10.11.12.13 e il nome DNS (Domain Name System) www.opencart.com, si riceverà un messaggio di errore di certificato in quanto l'URL non corrisponde a quello del certificato (ciò è valido anche se www.opencart.com è elencato nel file hosts come l'URL appartenente a 10.11.12.13). Questa situazione può verificarsi

se i subtenant di CloudCenter utilizzano l'SSO (Single Sign On), in quanto ogni server SSO ha il proprio URL.

Soluzione

Il modo più semplice per risolvere il problema è creare un nuovo certificato autofirmato con una SAN che elenchi qualsiasi URL che indirizza allo stesso indirizzo IP. La guida rappresenta un tentativo di applicare le procedure ottimali a questo processo.

Passaggio 1. Passare alla **directory principale** e creare una nuova cartella in cui memorizzare i certificati:

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

Passaggio 2. Accedere alla nuova cartella e creare sottocartelle per organizzare i certificati, le chiavi private e i registri.

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

Passaggio 3. Copiare il contenuto di **CAopenssl.conf in /root/ca/openssl.cnf**

> **Nota:** Questo file contiene le opzioni di configurazione per un'Autorità di certificazione (CA) e le opzioni predefinite che potrebbero essere appropriate per CloudCenter.

Passaggio 4. Generare una chiave privata e un certificato per la 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
```

Passaggio 5. L'autorità di certificazione (CA) è il modo più efficace per verificare la validità di un certificato. Questo certificato non deve essere mai utilizzato da utenti non autorizzati e non deve mai essere esposto a Internet. A causa di questa restrizione, è necessario creare una CA intermedia che firmi il certificato finale, creando un'interruzione in cui se il certificato dell'autorità intermedia viene compromesso può essere revocato e ne può essere emesso uno nuovo.

Passaggio 6. Creare una nuova sottodirectory per la CA intermedia.

```
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
```

Passaggio 7. Copiare il contenuto di **Intermediateopenssl.conf** in **/root/ca/intermediate/openssl.cnf** .

> **Nota:** Questo file contiene opzioni di configurazione quasi identiche per la CA, diverse da alcune piccole modifiche per renderla specifica per un intermedio.

Passaggio 8. Generare la chiave intermedia e il certificato.

```
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
```

Passaggio 9. Firmare il certificato intermedio con il certificato CA per creare una catena di attendibilità utilizzata dal browser per verificare l'autenticità di un certificato.

```
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
```

Passaggio 10. Creare una catena di CA, poiché non si desidera che la CA sia in Internet, è possibile creare una catena di CA che i browser utilizzano per verificare l'autenticità fino alla 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
```

Passaggio 11. Creare una nuova chiave e un nuovo certificato per 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
```

Passaggio 12. Il comando contiene tutti i campi obbligatori e deve essere modificato manualmente.

- **/C=US** si riferisce al paese (limite di 2 caratteri)
- **/ST=NC** fa riferimento allo stato e può includere spazi
- **/O=Cisco** si riferisce all'organizzazione
- **/CN=ccm.com** fa riferimento al nome comune, che dovrebbe essere l'URL principale utilizzato per accedere al CCM.
- **SAN\nsubjectAltName=** sono i nomi alternativi, il nome comune deve essere incluso in questo elenco e non vi sono limiti al numero di SAN disponibili.

Passaggio 13. Firmare il certificato finale utilizzando il certificato 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
```

Passaggio 14. Verificare che il certificato sia stato firmato correttamente.

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

Passaggio 15. Può restituire un OK o un Fail.

Passaggio 16. Copiare il nuovo certificato, la relativa chiave e il concatenamento CA nella cartella **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
```

Passaggio 17. Concedere la proprietà dell'utente client e impostare correttamente le autorizzazioni.

```
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
```

Passaggio 18. Eseguire il backup del file **server.xml** prima di apportare modifiche.

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

Passaggio 19. Modificare **server.xml:**

1. Individuare la sezione che inizia con **<Connector port="10443" maxHttpHeaderSize="8192"**
2. Modificare **SSLCertificateFile** in modo che punti a ccm.com.crt
3. Modificare **SSLCertificateKeyFile** in modo che punti a ccm.com.key
4. Modificare **SSLCACertificateFile** in modo che punti a ca-chain.crt

Passaggio 20. Riavviare Tomcat.

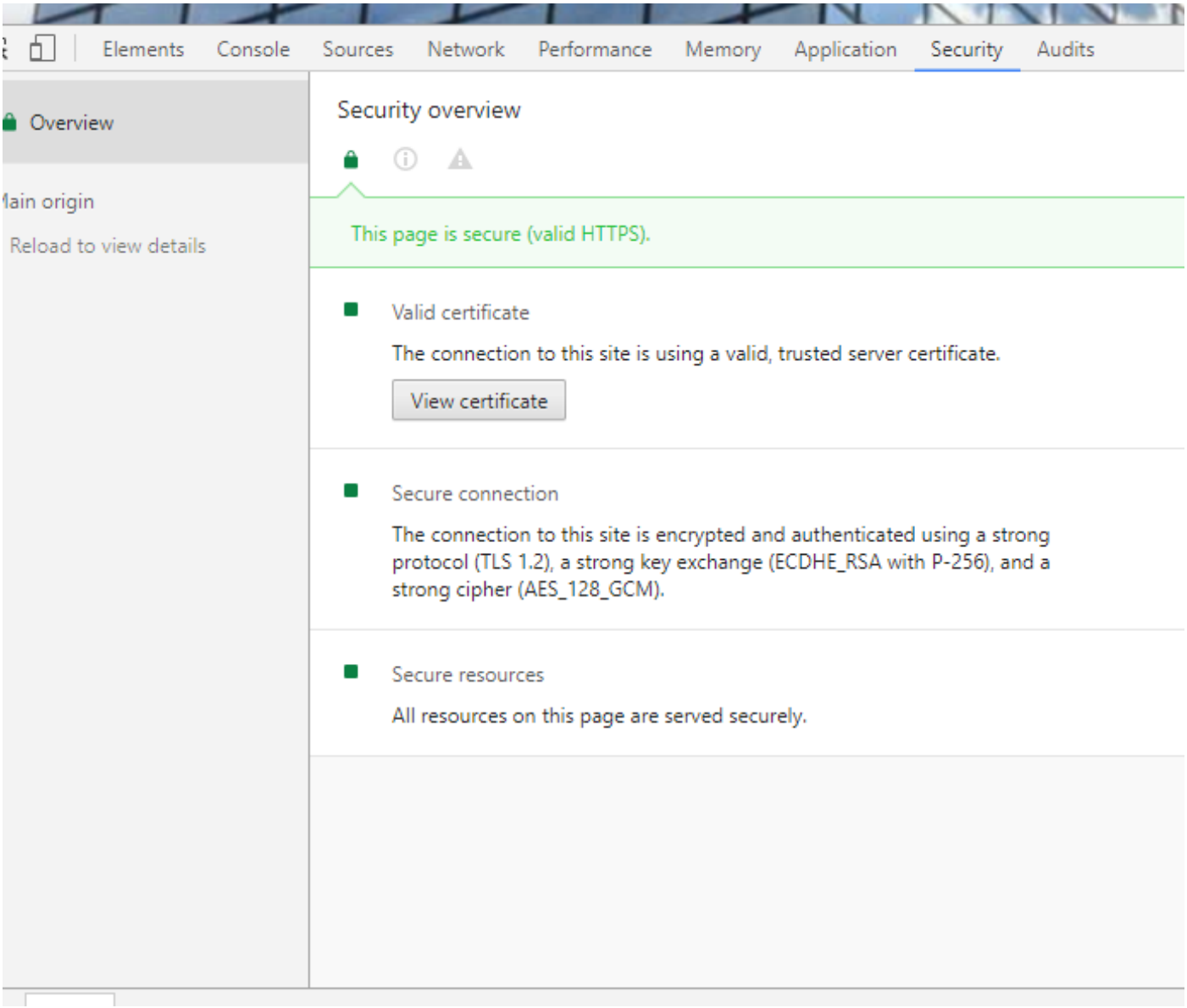
```
service tomcat stop
service tomcat start
```

Passaggio 21. La CCM utilizza ora il nuovo certificato valido per tutti i nomi DNS e gli indirizzi IP specificati nel passaggio 13.

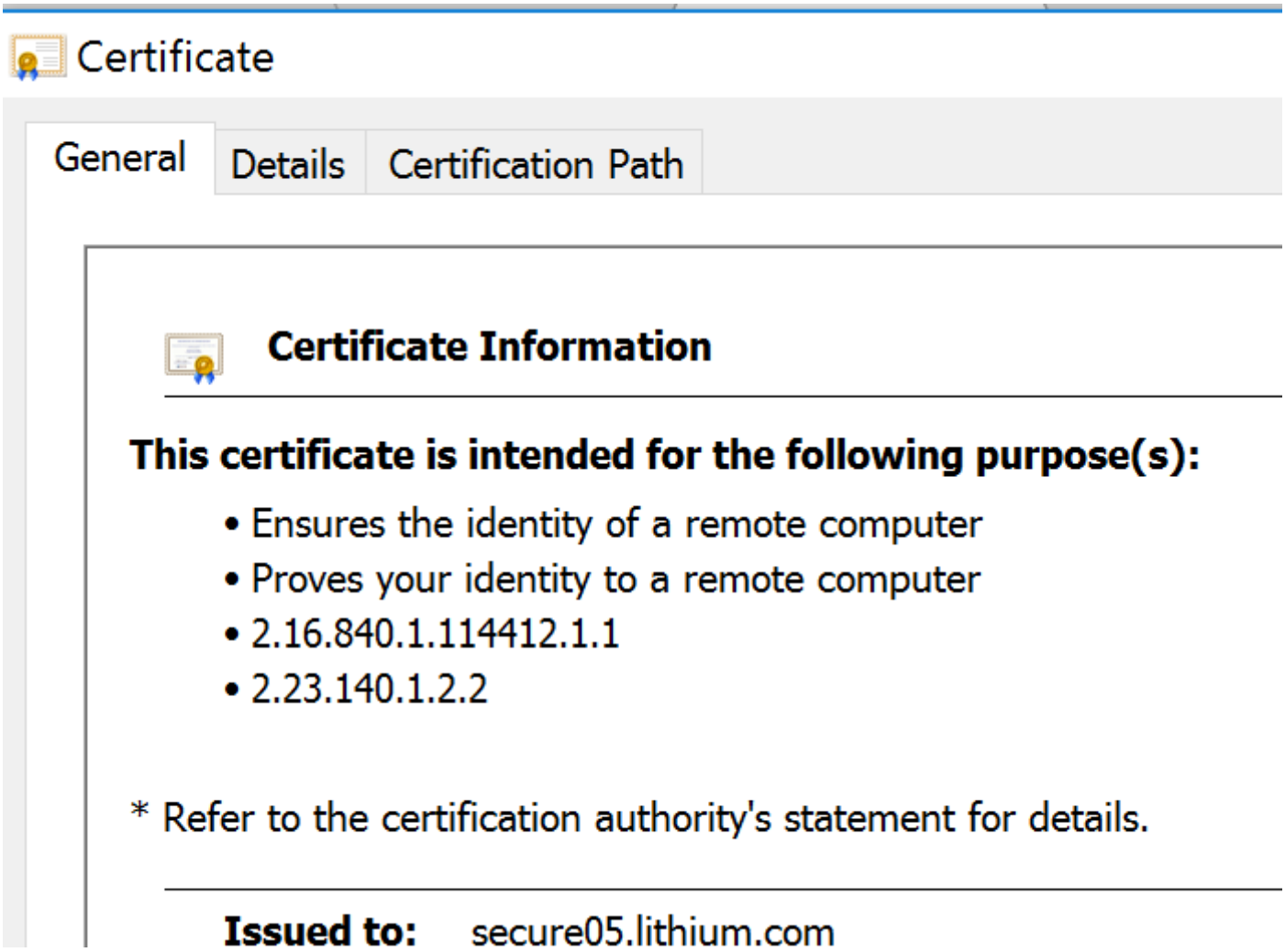
Passaggio 22. Poiché la CA è stata creata al momento della pubblicazione della Guida, i browser non la riconoscono come valida per impostazione predefinita, è necessario importare manualmente il certificato.

Passaggio 23. Passare alla **CCM** utilizzando un URL valido e premere **Ctrl+Maiusc+i** per aprire gli strumenti di sviluppo.

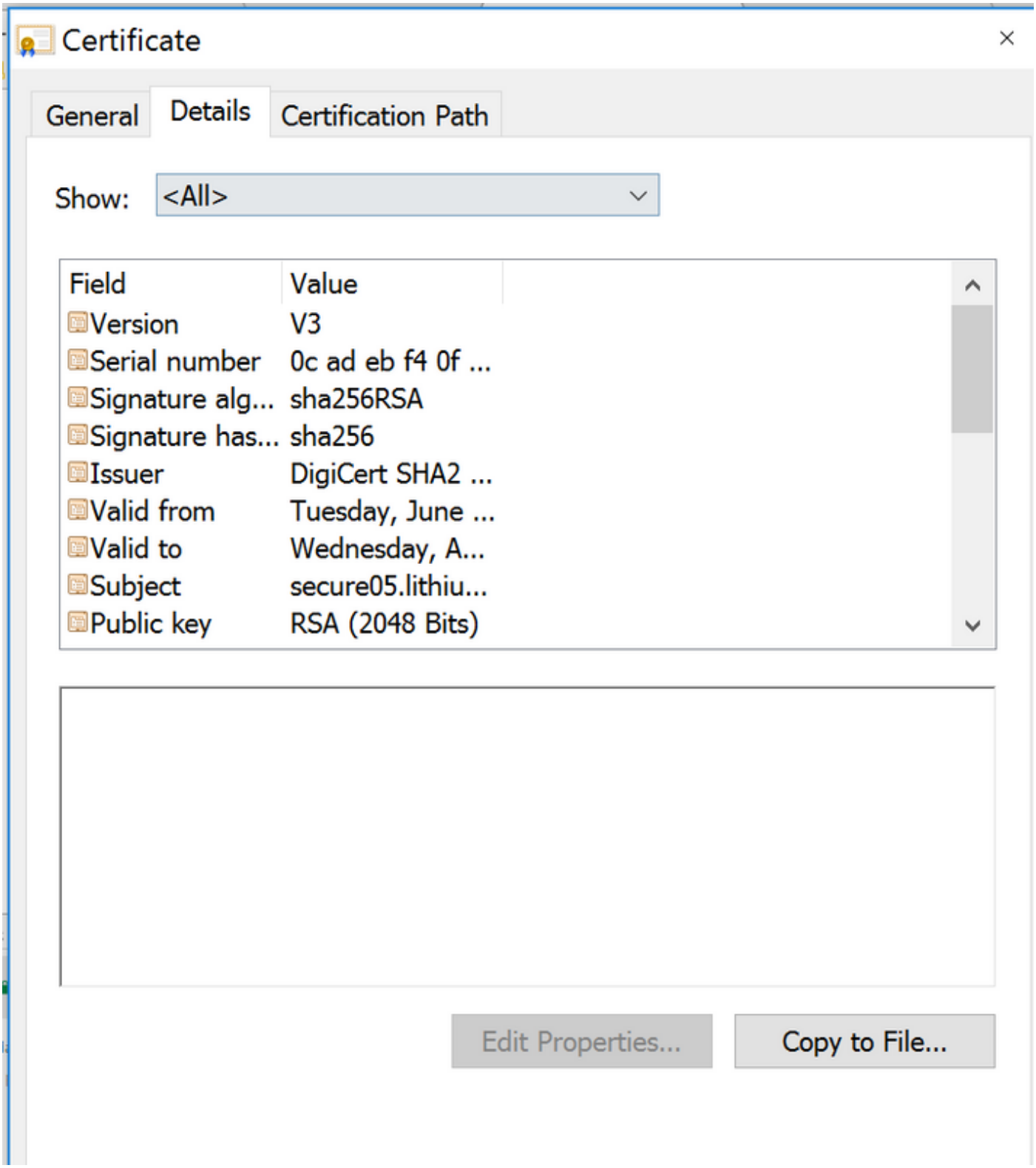
Passaggio 24. Selezionare **Visualizza certificato** come illustrato nell'immagine.



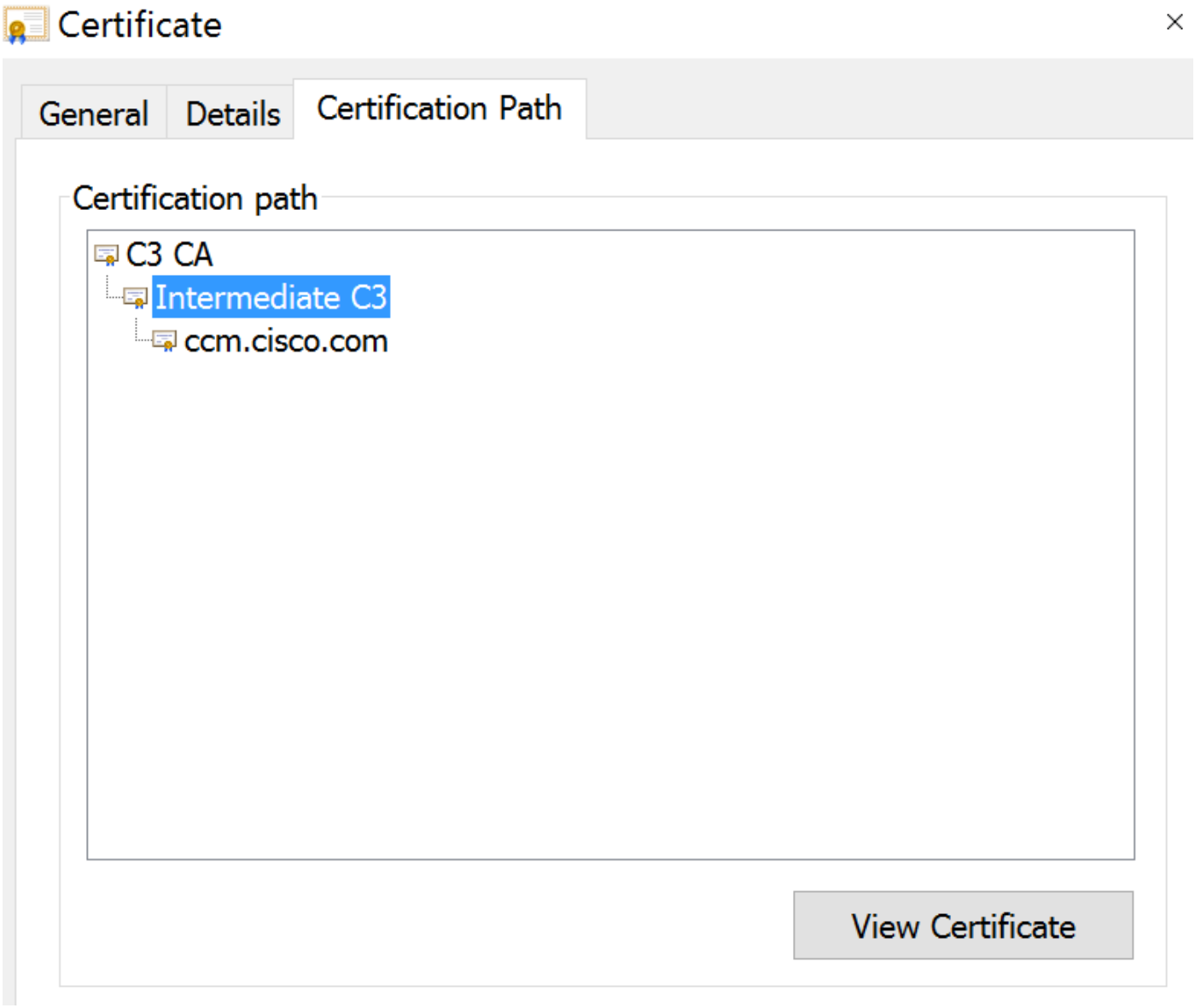
Passaggio 25. Selezionare **Dettagli** come mostrato nell'immagine.



Passaggio 26. Selezionare **Copia su file** come illustrato nell'immagine.



Passaggio 27. Se si verificano errori relativi a una CA non attendibile, passare al **Percorso certificazione** per visualizzare il certificato intermedio e il certificato radice. È possibile fare clic su di essi e visualizzare il loro certificato e anche copiarli in file come mostrato nell'immagine.



Passaggio 28. Dopo aver scaricato i certificati, seguire le istruzioni del sistema operativo o del browser per installare questi certificati come autorità attendibili e autorità intermedie.