

Determinazione del certificato corretto per LDAPS

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Determinare se il certificato o i certificati possono essere emessi.](#)

[Per determinare quale certificato/catena utilizzare.](#)

Introduzione

In questo documento viene descritto come determinare i certificati corretti per il protocollo LDAP (Lightweight Directory Access Protocol) sicuro.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

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.

Premesse

Secure LDAP richiede che nel dominio UCS (Unified Computing System) sia installato il certificato o la catena di certificati corretta come punto attendibile.

Se è stato configurato un certificato (o una catena) errato o non ne esiste alcuno, l'autenticazione

non riesce.

Determinare se il certificato o i certificati possono essere emessi.

In caso di problemi con Secure LDAP, utilizzare il debug LDAP per verificare se i certificati sono corretti.

```
[username]
[password]
connect nxos      *(make sure we are on the primary)
debug ldap all
term mon
```

Aprire quindi una seconda sessione e tentare di accedere con le credenziali LDAP sicure.

La sessione con il debug attivato registra il tentativo di accesso. Nella sessione di registrazione eseguire il comando **undebug** per interrompere l'output.

```
undebug all
```

Per determinare se esiste un potenziale problema con il certificato, esaminare l'output di debug per queste righe.

```
2018 Sep 25 10:10:29.144549 ldap: ldap_do_process_tls_resp: (user f-ucsapac-01) - ldap start TLS
sent succesfully;          Calling ldap_install_tls
2018 Sep 25 10:10:29.666311 ldap: ldap_do_process_tls_resp: (user f-ucsapac-01) - TLS START
failed
```

Se TLS non è riuscito, non è stato possibile stabilire una connessione protetta e l'autenticazione non riesce.

Per determinare quale certificato/catena utilizzare.

Dopo aver determinato che la connessione protetta non è stata stabilita, determinare i certificati corretti.

Utilizzare l'etanalizzatore per acquisire la comunicazione e quindi estrarre il certificato (o la catena) dal file.

Nella sessione di debug eseguire il comando:

```
ethalyzer local interface mgmt capture-filter "host <address of controller/load balancer>"
limit-captured-frames 100 write volatile:ldap.pcap
```

Tentare quindi un altro accesso tramite con le credenziali.

Quando non viene più visualizzato alcun nuovo output nella sessione di debug, terminare l'acquisizione. Utilizzare (**ctrl + c**).

Trasferire l'acquisizione del pacchetto dall'interfaccia Fabric Interconnect (FI) con questo comando:

```
copy volatile:ldap.pcap tftp:
```

Una volta ottenuto il file ldap.pcap, aprirlo in Wireshark e cercare un pacchetto che inizi a inizializzare la connessione TLS.

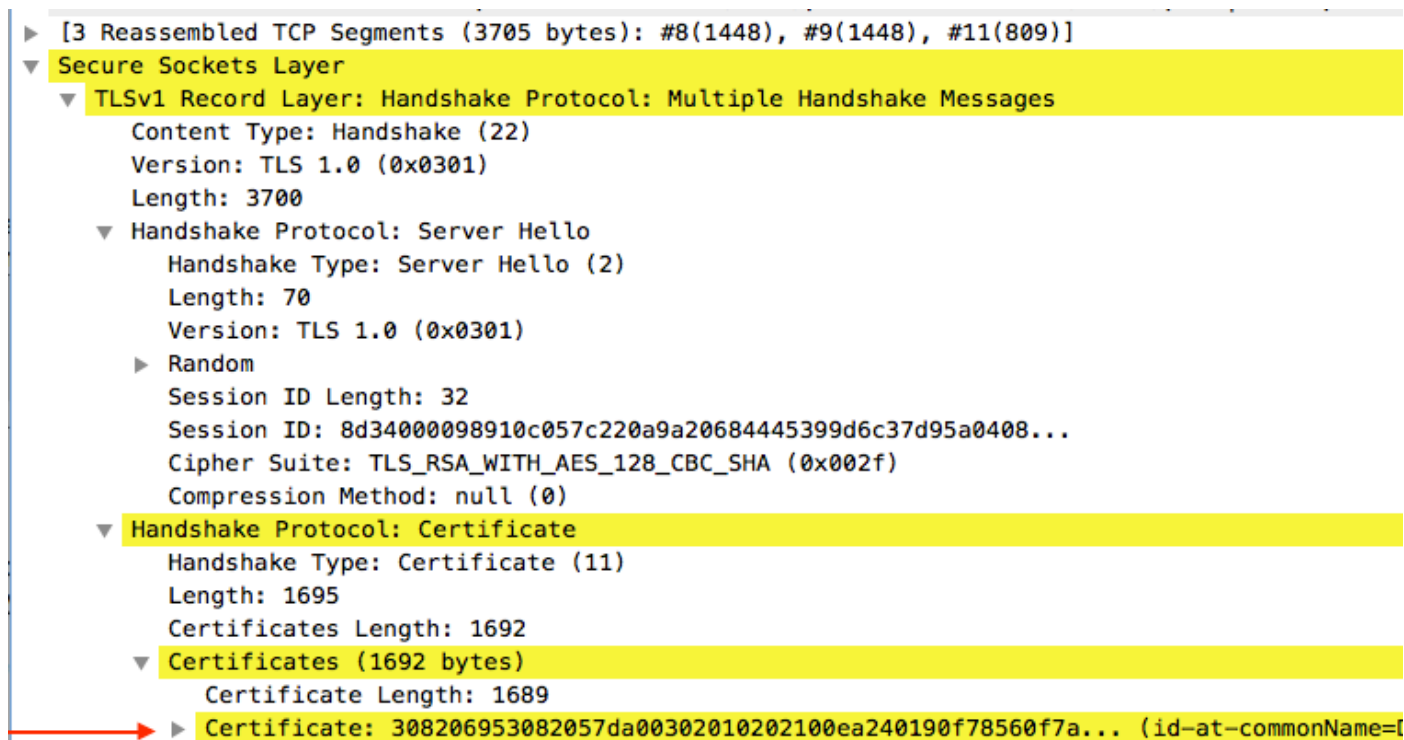
È possibile visualizzare un messaggio simile nella sezione **Info** del pacchetto, come mostrato nell'immagine:

No.	Time	Source	Destination	Protocol	Length	Info
7	0.498834			SSLv2	190	Client Hello
8	0.753397			TCP	1514	[TCP segment of a reassembled PDU]
9	0.755902			TCP	1514	[TCP segment of a reassembled PDU]
10	0.755940			TCP	66	56328 → 3268 [ACK] Seq=156 Ack=2943 Win=11776 Len=0 TSval=1166916677 TSecr=112994803
11	1.005008			TLSv1	875	Server Hello, Certificate, Certificate Request, Server Hello Done
12	1.007214			TLSv1	73	Alert (Level: Fatal, Description: Unknown CA)

Selezionare il pacchetto ed espanderlo:

Secure Sockets Layer

```
-->TLSv? Record Layer: Handshake Protocol: Multiple Handshake Messages  
---->Handshake Protocol: Certificate  
----->Certificates (xxxx bytes)
```



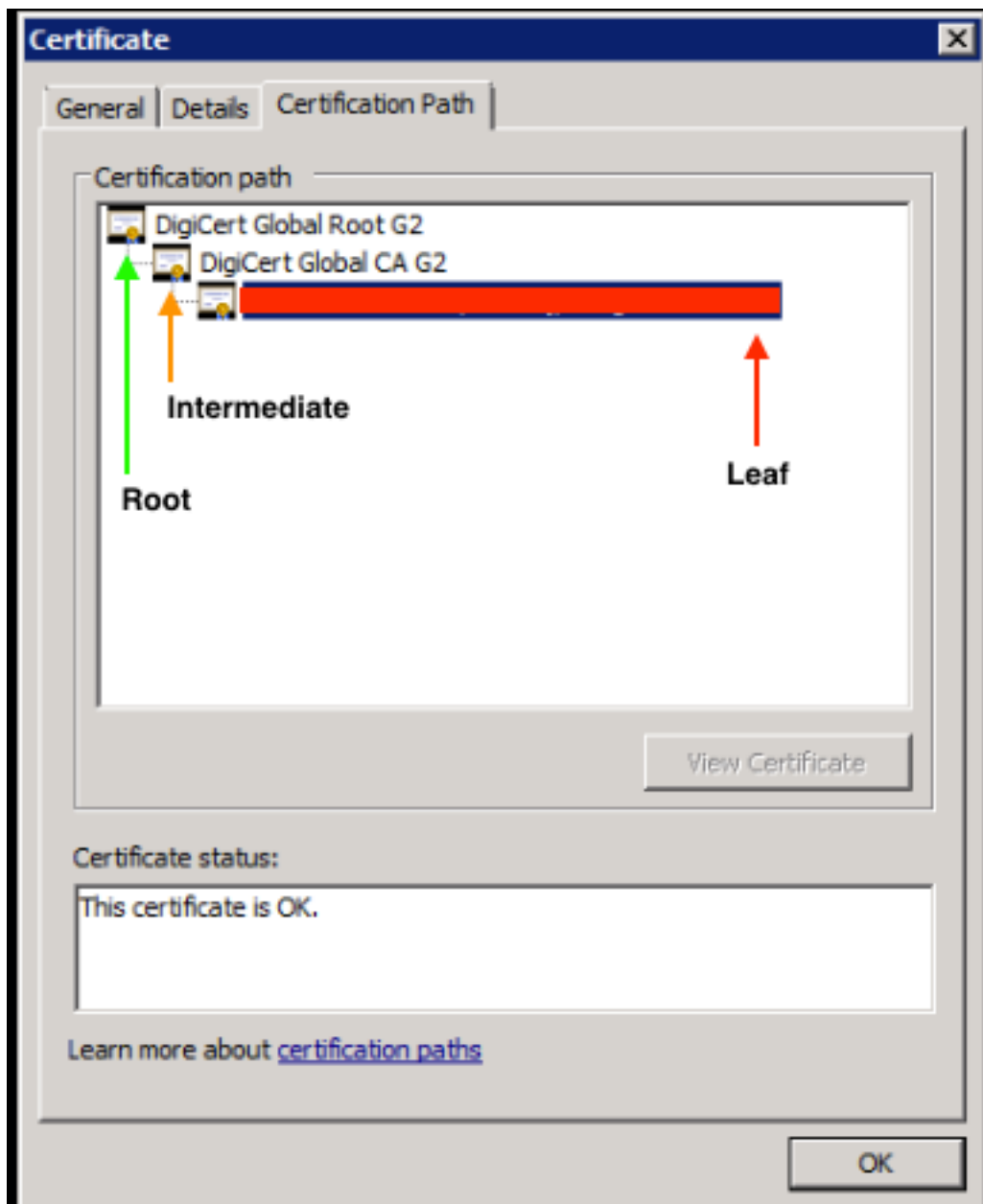
Selezionare la riga **Certificato**.

Fare clic con il pulsante destro del mouse su questa riga, selezionare **Esporta byte pacchetto** e salvare il file come file **.der**.

Aprire il certificato in Windows e passare alla scheda **Percorso certificato**.

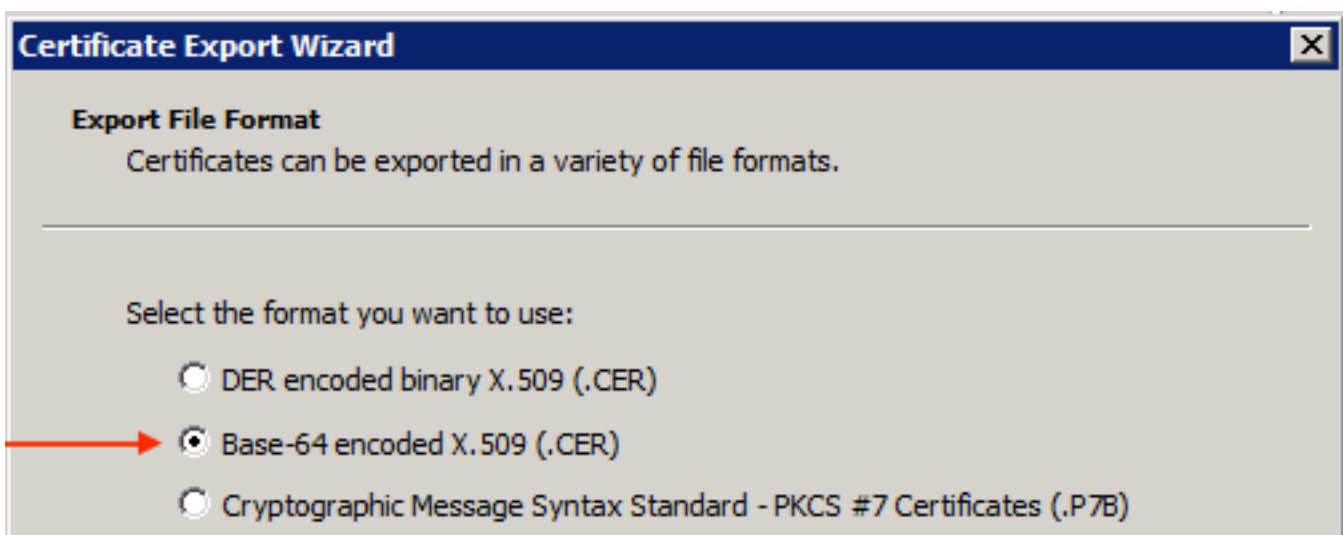
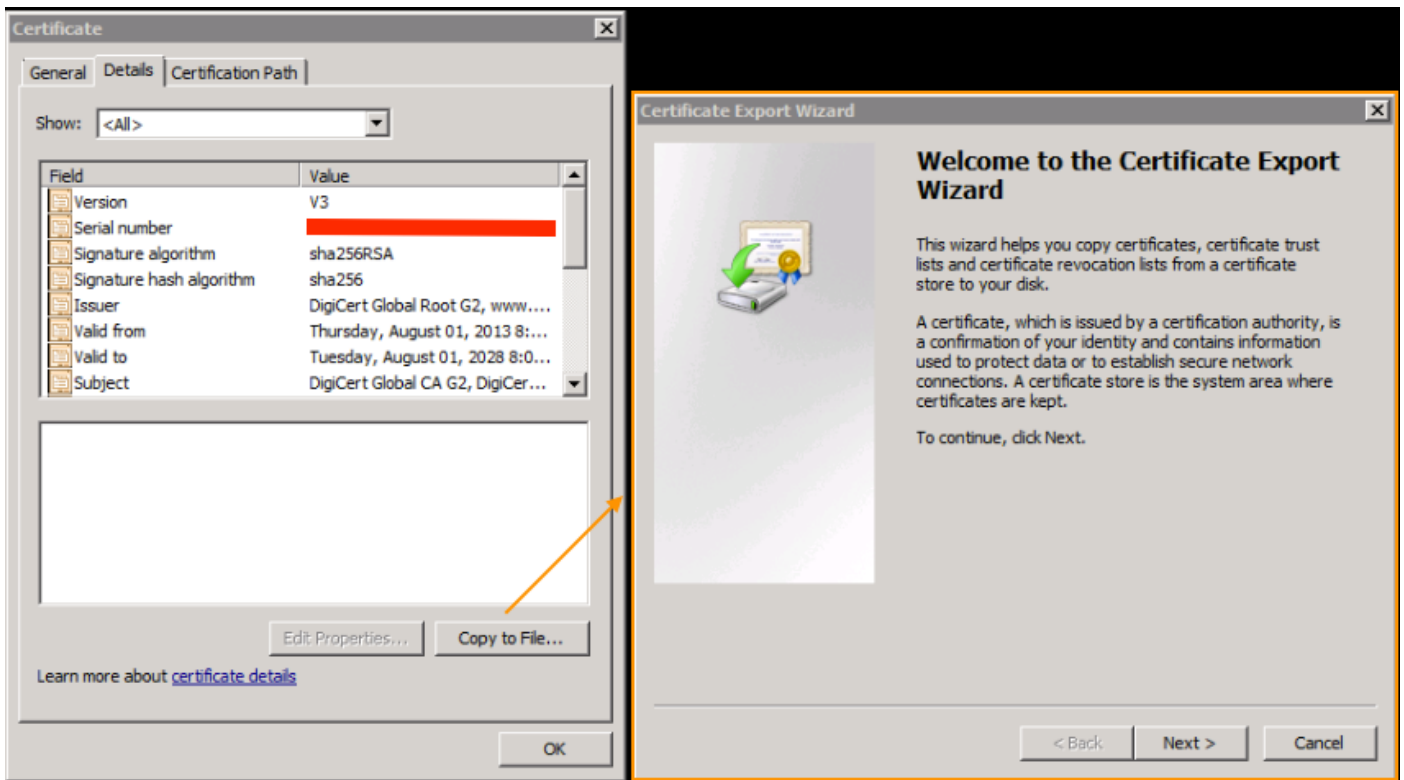
In questo modo viene mostrato il percorso completo dal certificato **radice** alla **foglia** (host finale). Eseguire le operazioni seguenti per tutti i nodi elencati ad eccezione della **foglia**.

```
Select the node  
-->Select 'View Certificate'  
---->Select the 'Details' tab
```



Selezionare l'opzione **Copia su file** e seguire l'**Esportazione guidata certificati** (assicurarsi di utilizzare il formato codificato Base 64).

In questo modo viene generato un file **.cer** per ogni nodo dell'elenco man mano che vengono completati.



Aprire questi file in Blocco note, Blocco note++, Sublime e così via per visualizzare il certificato con hash.

Per generare la catena, se presente, aprire un nuovo documento e incollarlo nel certificato con hash dell'ultimo nodo.

Andare all'inizio dell'elenco incollando ogni certificato con hash, terminando con la **CA radice**.

Incollare la **CA radice** (se non è presente una catena) o l'intera catena generata nel punto attendibile.