Correct certificaat voor LDAPS bepalen

Inhoud

Inleiding

Dit document beschrijft hoe u het juiste certificaat of de juiste certificaten kunt bepalen voor een beveiligd lichtgewicht Directory Access Protocol (LDAP).

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Achtergrondinformatie

Secure LDAP vereist dat het Unified Computing System (UCS)-domein over de juiste certificaat- of certificeringsketen beschikt als een betrouwbaar punt.

Indien een onjuist certificaat (of keten) is ingesteld of indien er geen bestaat, mislukt de authenticatie.

Om vast te stellen of er een afgifte met het (de) certificaat(en) kan(en) zijn.

Als u problemen hebt met Secure LDAP, gebruik dan de optie voor het debuggen van LDAP om te controleren of de certificaten juist zijn.

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

Daarna opent u een tweede sessie en probeert u in te loggen met uw Secure LDAP-referenties.

De sessie met het foutoptreden liet de poging tot inloggen zien. Op de logsessie voer de **undebug** opdracht uit om verdere uitvoer te stoppen.

```
undebug all
```

Om te bepalen als er een potentieel probleem met het certificaat is, kijk naar de het zuiveren output voor deze lijnen.

```
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
```

Als TLS faalde, kon een beveiligde verbinding niet tot stand worden gebracht en is de verificatie mislukt.

Om te bepalen welk certificaat/keten u moet gebruiken.

bepalen wat het juiste certificaat of de juiste certificaten moet zijn wanneer u heeft vastgesteld dat de beveiligde verbinding niet tot stand is gebracht.

Gebruik ethanlyzer om de communicatie op te nemen en het certificaat (of de keten) uit het bestand te halen.

In uw debugsessie voert u de opdracht uit:

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

Probeer vervolgens nog een logbestand via uw geloofsbrieven in te loggen.

Zodra u geen nieuwe output meer ziet in de het debuggen sessie, vermoord u de opname. Gebruik (**ctrl + c**).

Breng de pakketvastlegging van Fabric Interconnect (FI) met deze opdracht over:

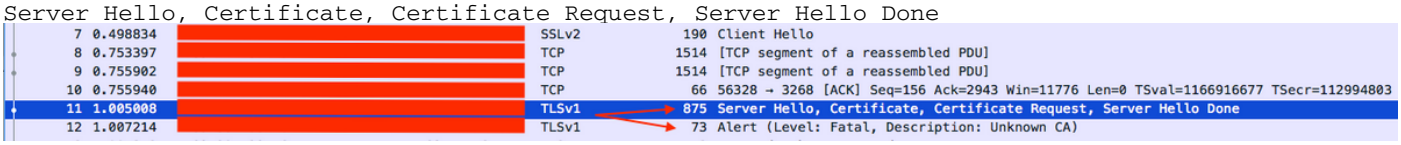
```
copy volatile:ldap.pcap tftp:
```

Zodra u het bestand ldap.pcap hebt, opent u het bestand in Wireshark en zoekt u een pakje dat de TLS-verbinding start.

U kunt een soortgelijk bericht zien in het gedeelte **Info** voor het pakket, zoals in de afbeelding

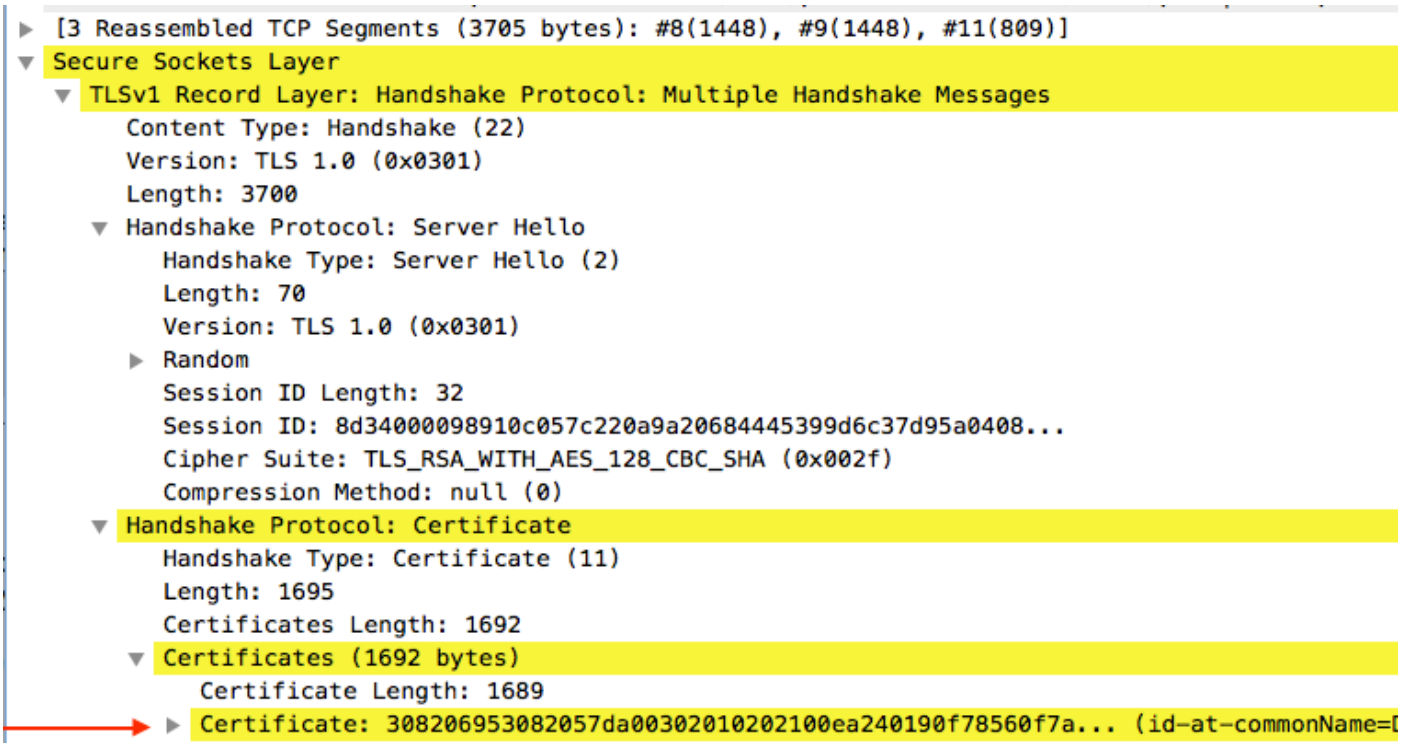
weergegeven:

```
Server Hello, Certificate, Certificate Request, Server Hello Done
```



Selecteer dit pakket en voudig het uit:

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



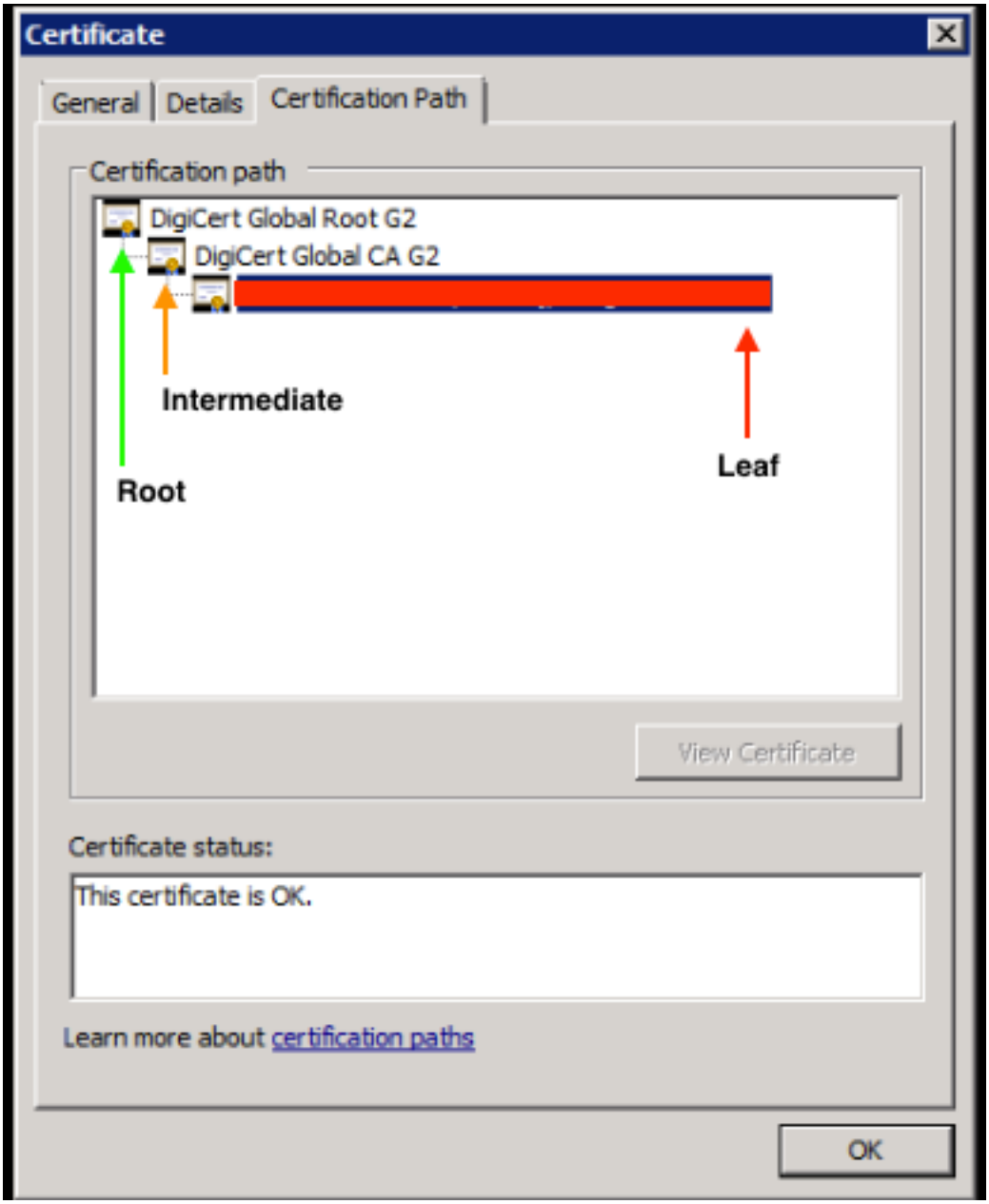
Selecteer de regel **certificaatnummer**.

Klik met de rechtermuisknop op deze regel en selecteer **Packet Bytes exporteren** en slaat het bestand op als een bestand **.der**.

Open het certificaat in Windows en navigeer naar het tabblad **certificaatpad**.

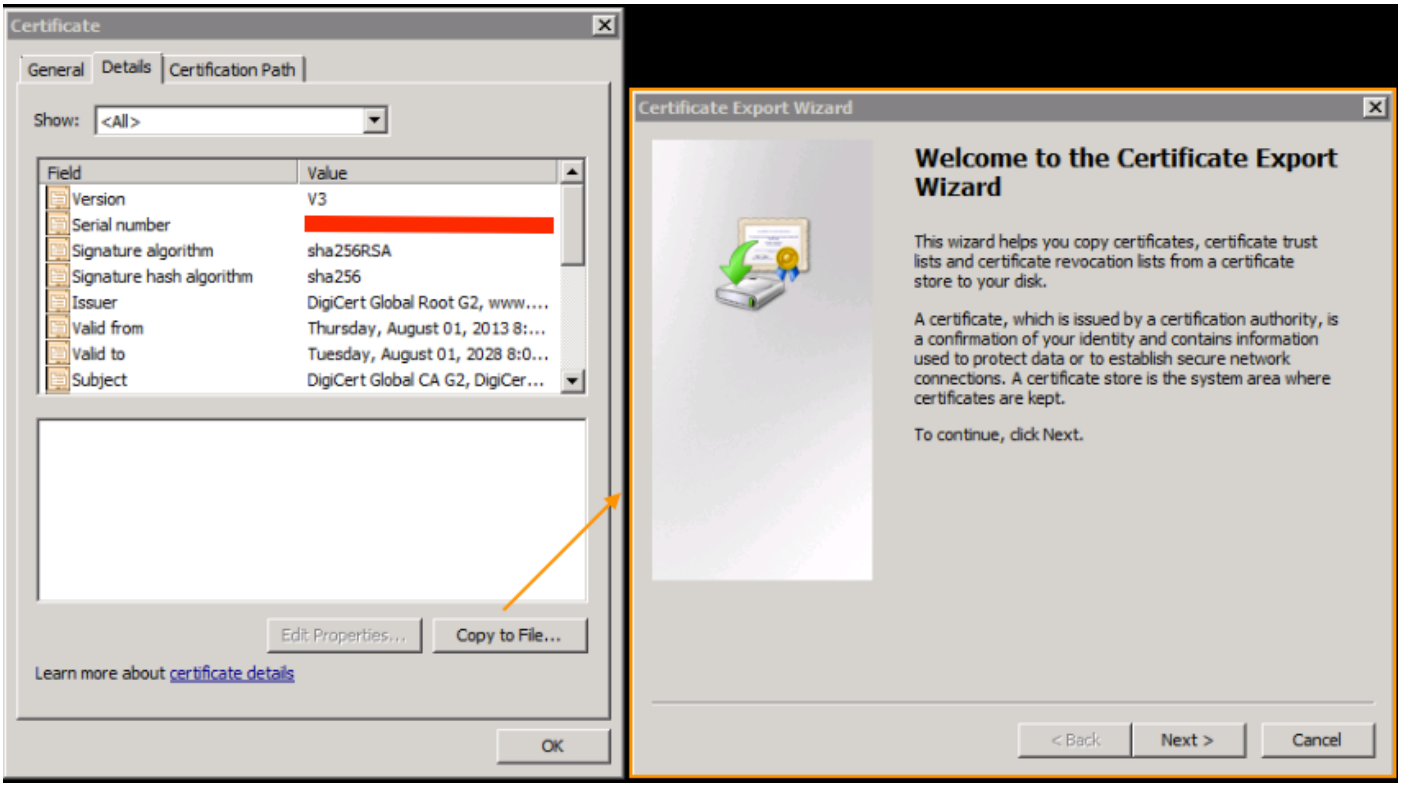
Dit toont u het volledige pad van het **Root** certificaat naar het **blad** (end host). Doe het volgende voor alle knooppunten die in de lijst staan, behalve voor het **blad**.

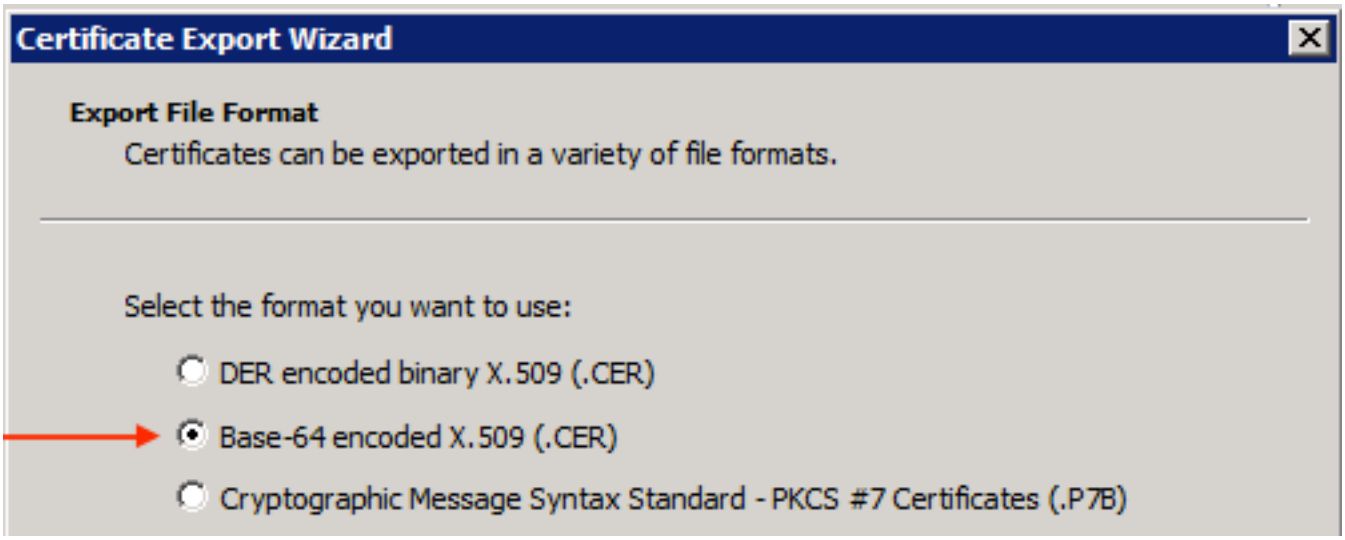
```
Select the node
-->Select 'View Certificate'
---->Select the 'Details' tab
```



Selecteer de optie **Kopie naar bestand** en volg de **wizard Certificaat exporteren** (controleer of u de gecodeerde basisindeling 64 wilt gebruiken).

Dit genereert een **.cer**-bestand voor elk van de knooppunten in de lijst naarmate u ze aanvult.





Open deze bestanden in Kladblok, Kladblok+, Sublik, enz. om het gehashed certificaat te bekijken.

Om de ketting (als er een is) te genereren, opent u een nieuw document en een nieuw pasta in het gehashed certificaat van de laatste knooppunt.

Werk omhoog de lijst door elk gehashed certificaat te plakken, eindigend met de **voet CA**.

Plakt ofwel de **Root CA** (indien er geen keten is) of de gehele keten die u gegenereerd hebt in het Trusted Point.