Richtiges Zertifikat für LDAPS ermitteln

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie die richtigen Zertifikate für sicheres Lightweight Directory Access Protocol (LDAP) ermitteln.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Hintergrundinformationen

Für sichere LDAP ist es erforderlich, dass die Unified Computing System (UCS)-Domäne als Trusted Point die richtigen Zertifikate oder Zertifikatsketten installiert hat.

Wenn ein falsches Zertifikat (oder eine fehlerhafte Kette) eingerichtet wurde oder kein Zertifikat vorhanden ist, schlägt die Authentifizierung fehl.

Um festzustellen, ob ein Problem mit dem/den Zertifikat(en) vorliegt.

Wenn Sie Probleme mit Secure LDAP haben, überprüfen Sie mithilfe des LDAP-Debuggens, ob die Zertifikate korrekt sind.

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

Öffnen Sie anschließend eine zweite Sitzung, und versuchen Sie, sich mit Ihren sicheren LDAP-Anmeldeinformationen anzumelden.

Die Sitzung mit aktiviertem Debugging protokolliert die versuchte Anmeldung. Führen Sie in der Protokollierungssitzung den Befehl **undebug aus**, um die weitere Ausgabe zu stoppen.

```
undebug all
```

Um festzustellen, ob ein potenzielles Problem mit dem Zertifikat vorliegt, sehen Sie sich die Debugausgabe für diese Zeilen an.

```
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
```

Wenn TLS fehlschlug, konnte keine sichere Verbindung hergestellt werden, und die Authentifizierung schlägt fehl.

Um zu bestimmen, welches Zertifikat/welche Kette Sie verwenden sollten.

Nachdem Sie festgestellt haben, dass die sichere Verbindung nicht hergestellt werden konnte, legen Sie fest, welches Zertifikat bzw. welche Zertifikate richtig sein sollen.

Verwenden Sie Ethanlyzer, um die Kommunikation zu erfassen und dann das Zertifikat (oder die Kette) aus der Datei zu extrahieren.

Führen Sie in der Debugsitzung den folgenden Befehl aus:

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

Versuchen Sie anschließend, sich mit Ihren Anmeldeinformationen erneut über anzumelden.

Wenn Sie keine neue Ausgabe mehr in der Debugsitzung sehen, beenden Sie die Erfassung. Verwenden (**Strg + c**).

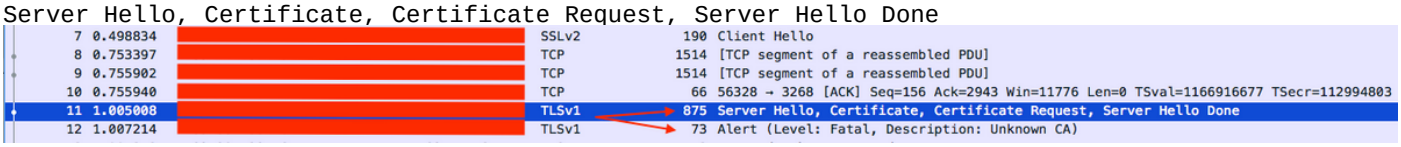
Übertragen Sie die Paketerfassung vom Fabric Interconnect (FI) mit dem folgenden Befehl:

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

Wenn Sie die Datei ldap.pcap haben, öffnen Sie die Datei in Wireshark, und suchen Sie nach einem Paket, das die TLS-Verbindung initialisiert.

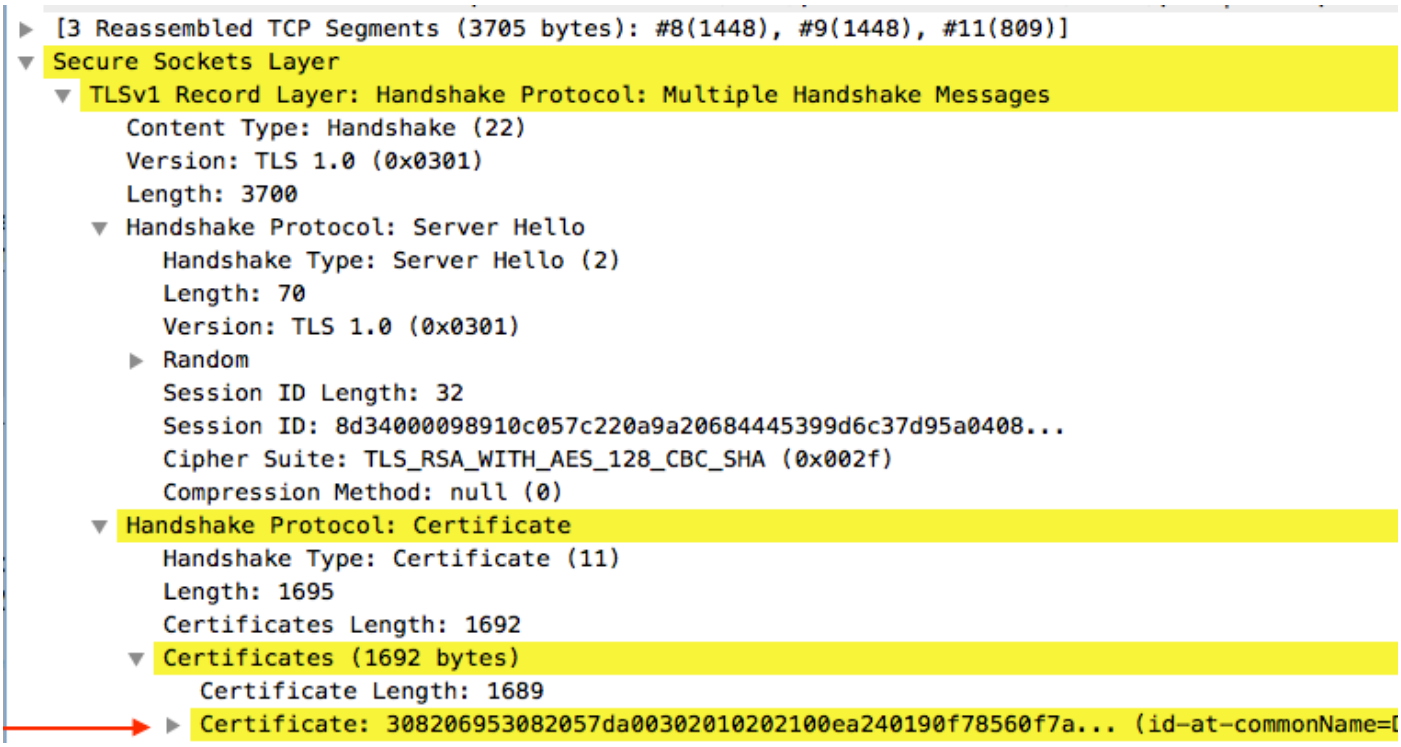
Sie sehen eine ähnliche Meldung im Abschnitt **Info** für das Paket, wie im Bild gezeigt:

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



Wählen Sie dieses Paket aus, und erweitern Sie es:

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



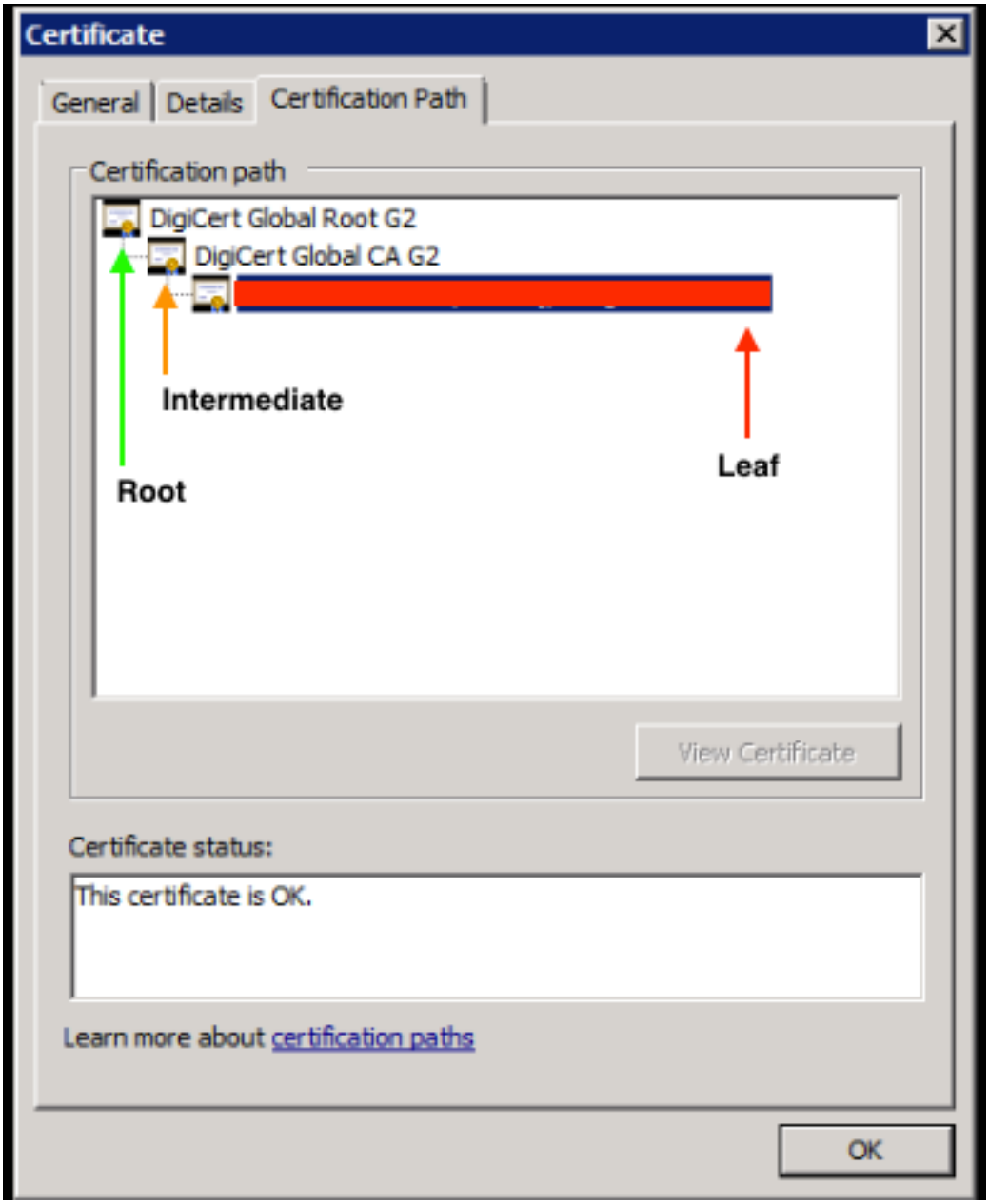
Wählen Sie die Zeile **Zertifikat aus**.

Klicken Sie mit der rechten Maustaste auf diese Zeile, wählen Sie **Packet Bytes exportieren aus**, und speichern Sie die Datei als **.der-**Datei.

Öffnen Sie das Zertifikat in Windows, und navigieren Sie zur Registerkarte **Zertifikatspfad**.

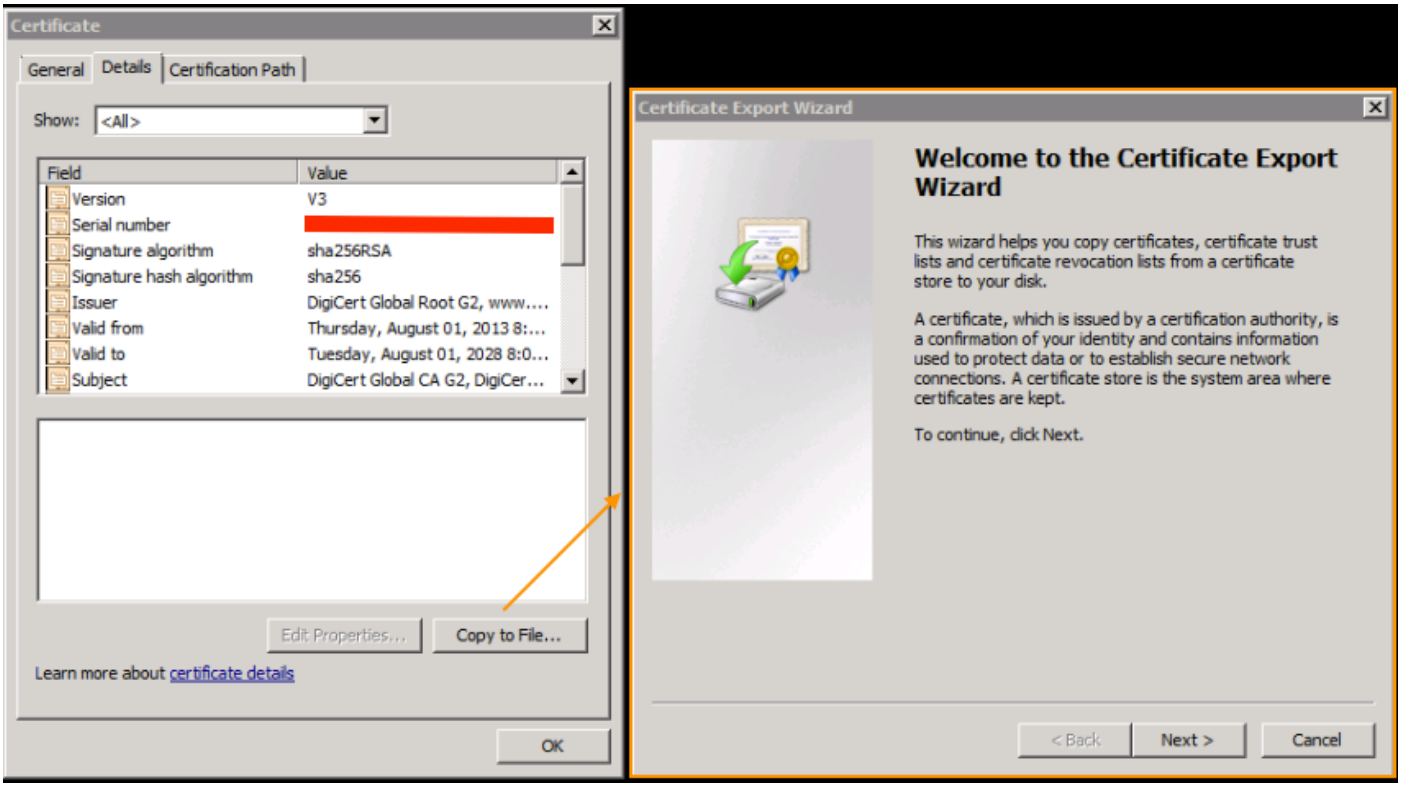
Hier wird der vollständige Pfad vom **Root-**Zertifikat zum **Leaf** (End-Host) angezeigt. Führen Sie die folgenden Schritte für alle aufgeführten Knoten aus, mit Ausnahme des **Leaf**.

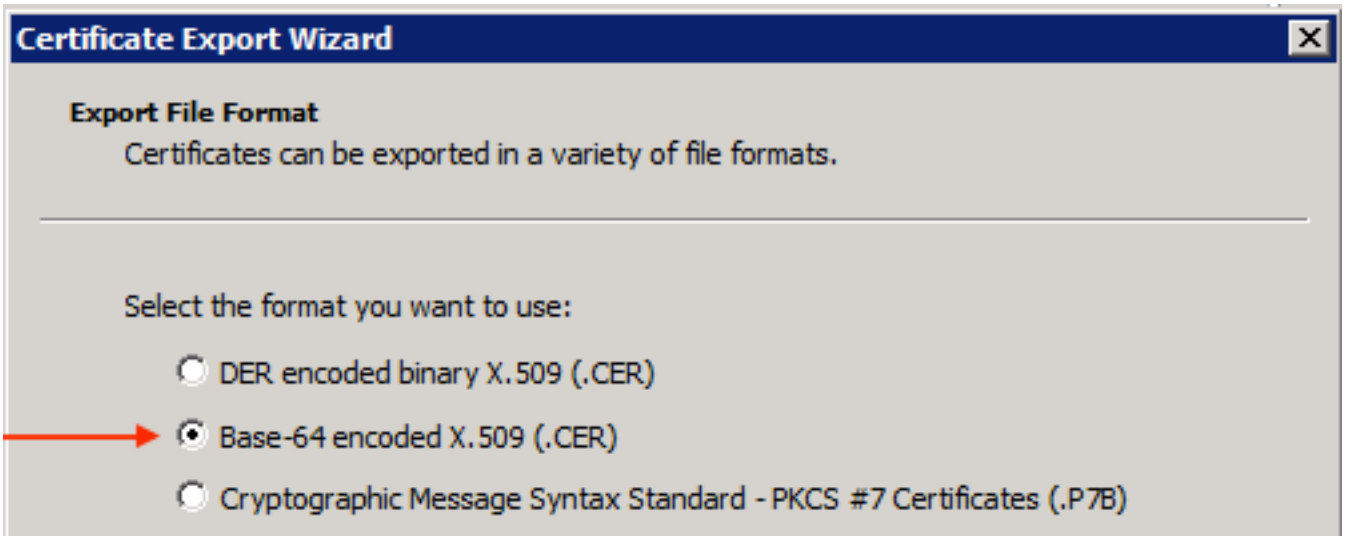
```
Select the node
-->Select 'View Certificate'
---->Select the 'Details' tab
```



Wählen Sie die Option **In Datei kopieren** aus, und befolgen Sie den **Assistenten für den Zertifikatsexport** (stellen Sie sicher, dass das Base-64-codierte Format verwendet wird).

Dadurch wird eine **.cer**-Datei für jeden Knoten in der Liste generiert, wenn Sie diese abschließen.





Öffnen Sie diese Dateien in Notepad, Editor++, Sublime usw., um das gehashte Zertifikat anzuzeigen.

Um die Kette zu generieren (falls vorhanden), öffnen Sie ein neues Dokument, und fügen Sie es in das gehashte Zertifikat des letzten Knotens ein.

Bearbeiten Sie die Liste, indem Sie die einzelnen gehashten Zertifikate einfügen und mit der **Root CA** enden.

Fügen Sie entweder die **Stammzertifizierungsstelle** (wenn keine Kette vorhanden ist) oder die gesamte Kette ein, die Sie in den Trusted Point generiert haben.