# Richtiges Zertifikat für LDAPS ermitteln

# Inhalt

Einleitung Voraussetzungen Anforderungen Verwendete Komponenten Hintergrundinformationen Um festzustellen, ob ein Problem mit dem/den Zertifikat(en) vorliegt. Um zu bestimmen, welches Zertifikat/welche Kette Sie verwenden sollten.

## 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.

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 Idap.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
	7	0.498834	SSLv2 190 Client Hello
L	8	0.753397	TCP 1514 [TCP segment of a reassembled PDU]
ł	9	0.755902	TCP 1514 [TCP segment of a reassembled PDU]
L	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
Γ	12	1.007214	TLSv1 73 Alert (Level: Fatal, Description: Unknown CA)

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)						
[3 Reassembled TCP Segments (3705 bytes): #8(1448), #9(1448), #11(809)]						
Secure Sockets Layer						
TLSv1 Record Layer: Handshake Protocol: Multiple Handshake Messages						
Content Type: Handshake (22)						
Version: TLS 1.0 (0x0301)						
Length: 3700						
W Handshake Protocol: Server Hello						
Handshake Type: Server Hello (2)						
Length: 70						
Version: TLS 1.0 (0x0301)						
▶ Random						
Session ID Length: 32						
Session ID: 8d34000098910c057c220a9a20684445399d6c37d95a0408						
Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)						
Compression Method: null (0)						
Handshake Protocol: Certificate						
Handshake Type: Certificate (11)						
Length: 1695						
Certificates Length: 1692						
▼ Certificates (1692 bytes)						
Certificate Length: 1689						
Certificate: 308206953082057da00302010202100ea240190f78560f7a (id-at-commonName=D						

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

Certificate	<]
General Details Certification Path	
View Certificate	
Certificate status:	
Learn more about <u>certification paths</u>	
ОК	j

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.

Certificate	×		
General Details Certification Path			
Show: <all></all>	-	Certificate Export Wizard	×
Field       Value         Version       V3         Serial number       Signature algorithm         Signature hash algorithm       sha256         Signature hash algorithm       sha256         Issuer       DigiCer         Valid from       Thursd         Valid to       Tuesda         Subject       DigiCer         Learn more about certificate details	RSA t Global Root G2, www ay, August 01, 2013 8: ty, August 01, 2028 8:0 t Global CA G2, DigiCer		Welcome to the Certificate Export Wizard
	ОК		< Back Next > Cancel

#### **Certificate Export Wizard**

#### Export File Format

Certificates can be exported in a variety of file formats.

Select the format you want to use:

O DER encoded binary X.509 (.CER)

Base-64 encoded X.509 (.CER)

Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)

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.