確定LDAPS的正確證書

目錄

簡介

本文檔介紹如何確定安全輕量型目錄訪問協定(LDAP)的正確證書。

必要條件

需求

本文件沒有特定需求。

採用元件

本文件所述內容不限於特定軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

背景資訊

安全LDAP要求統一計算系統(UCS)域安裝正確的證書或證書鏈作為受信任點。

如果設定的證書（或鏈）不正確，或者不存在該證書，則身份驗證失敗。

以確定證書是否出現問題。

如果您的Secure LDAP存在問題，請使用LDAP調試檢查證書是否正確。

```
[username]
[password]
connect nxos      *(make sure we are on the primary)
debug ldap all
term mon
```
然後，開啟第二個會話並嘗試使用您的安全LDAP憑據登入。

啟用調試的會話記錄嘗試的登入。在日誌記錄會話上運行**undebug**命令以停止進一步的輸出。

```
undebug all
```
要確定證書是否有潛在問題，請檢視這些行的調試輸出。

```
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
```
如果TLS失敗，則安全連線無法建立，身份驗證失敗。

決定您應使用的憑證/鏈結。

確定建立安全連線失敗後，確定正確的證書是什麼。

使用ethanlyzer捕獲通訊，然後從檔案中提取證書（或鏈）。

在調試會話中運行命令：

```
ethanalyzer local interface mgmt capture-filter "host <address of controller/load balancer>"
limit-captured-frames 100 write volatile:ldap.pcap
```
接下來，嘗試使用您的憑據再次通過登入。

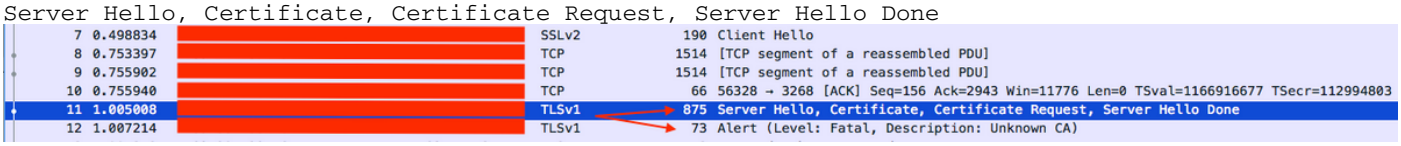
在調試會話中不再看到任何新輸出後，停止捕獲。使用(**ctrl + c**)。

使用以下命令從交換矩陣互聯(FI)傳輸資料包捕獲：

```
copy volatile:ldap.pcap tftp:
```
收到ldap.pcap檔案後，在Wireshark中開啟該檔案，然後查詢開始初始化TLS連線的包。

您可以在封包的**資訊**一節中看到類似訊息，如下圖所示：

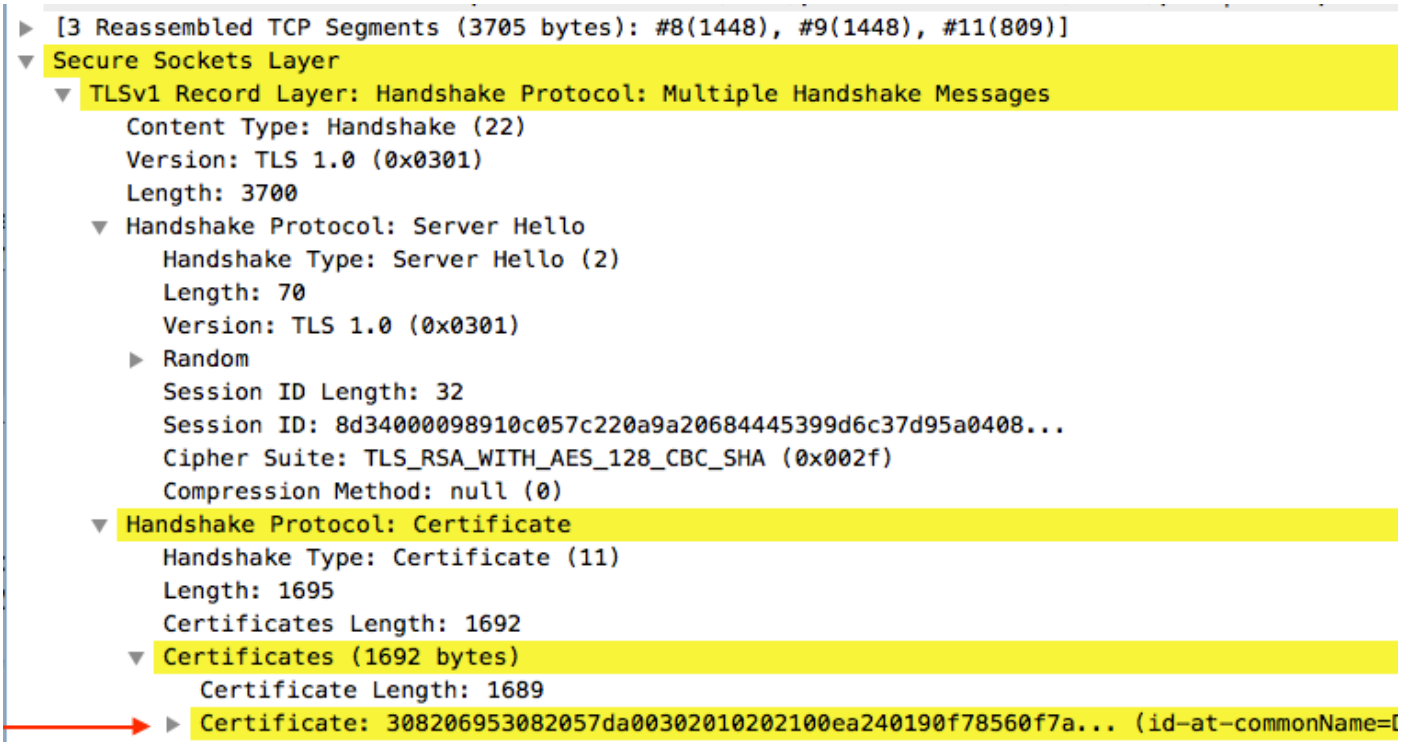
```
Server Hello, Certificate, Certificate Request, Server Hello Done
```



選擇此資料包並展開它：

```
Secure Sockets Layer
-->TLSv? Record Layer: Handshake Protocol: Multiple Handshake Messages
---->Handshake Protocol: Certificate
```

```
------>Certificates (xxxx bytes)
```



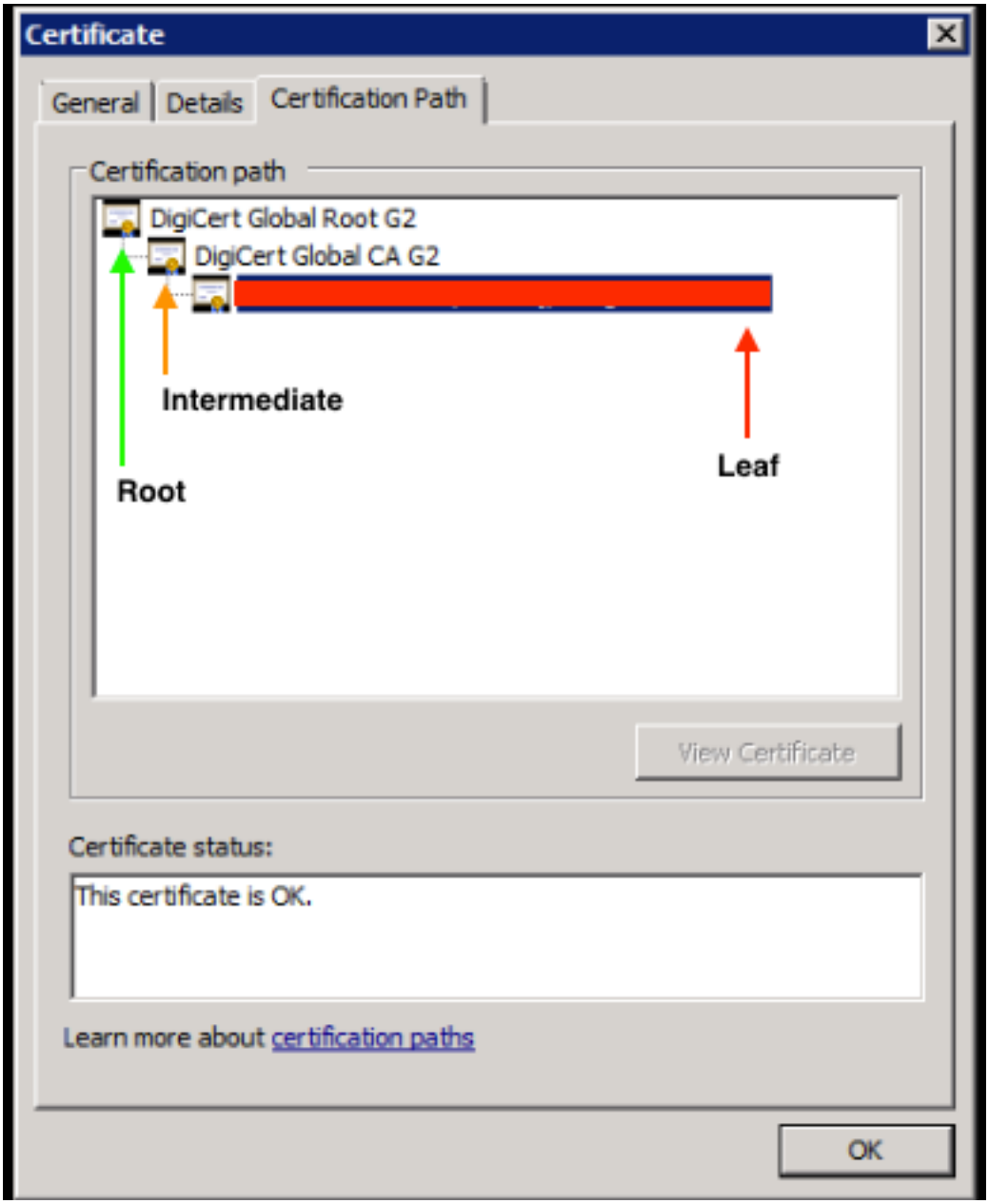
選擇標題為**Certificate**的行。

按一下右鍵此行，然後選擇**Export Packet Bytes**，然後將檔案另存為**.der**檔案。

在Windows中開啟證書，然後導航到**證書路徑**頁籤。

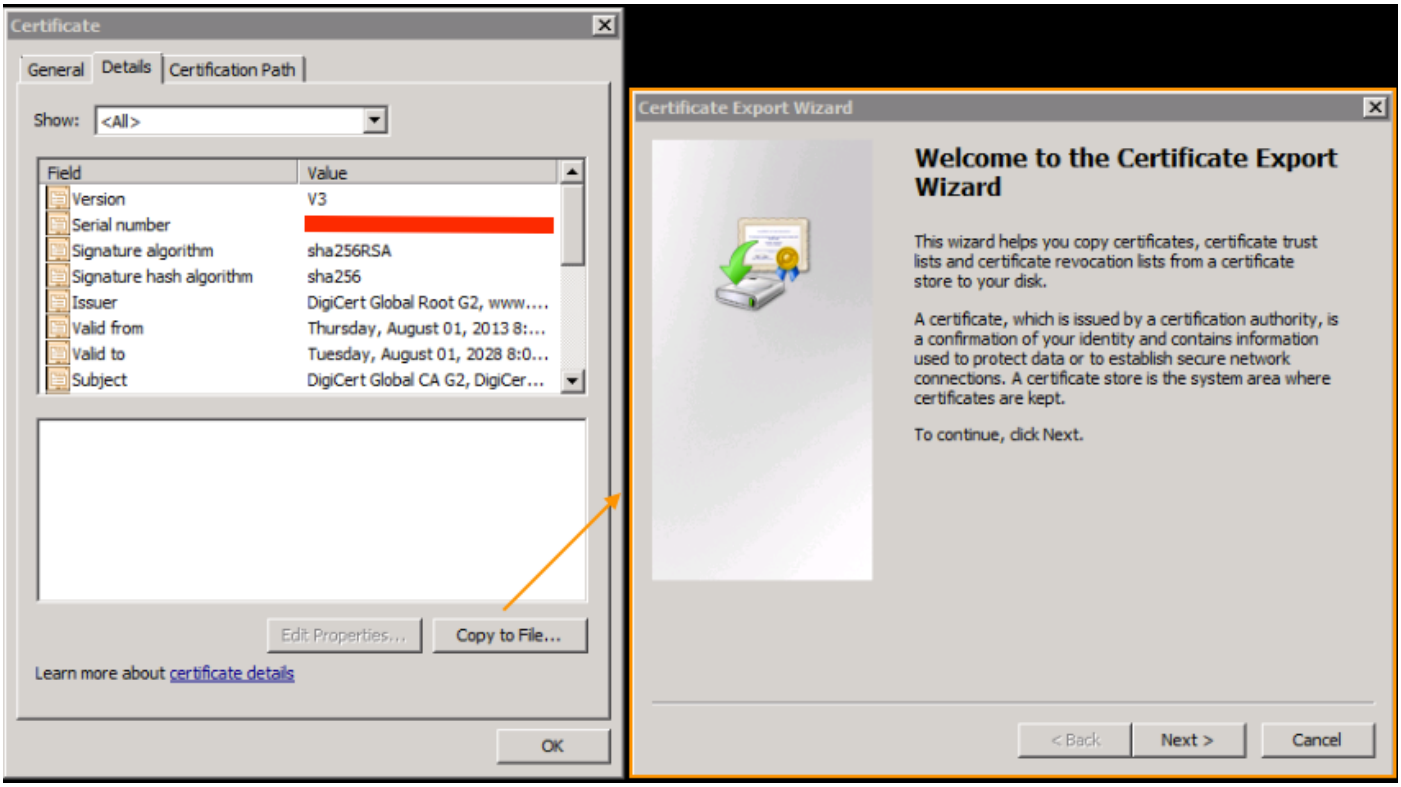
這向您顯示了從**根證書**到**枝葉（終端主機）的完整路徑。** 對列出的所有節點（枝葉除外）執行以下操作。

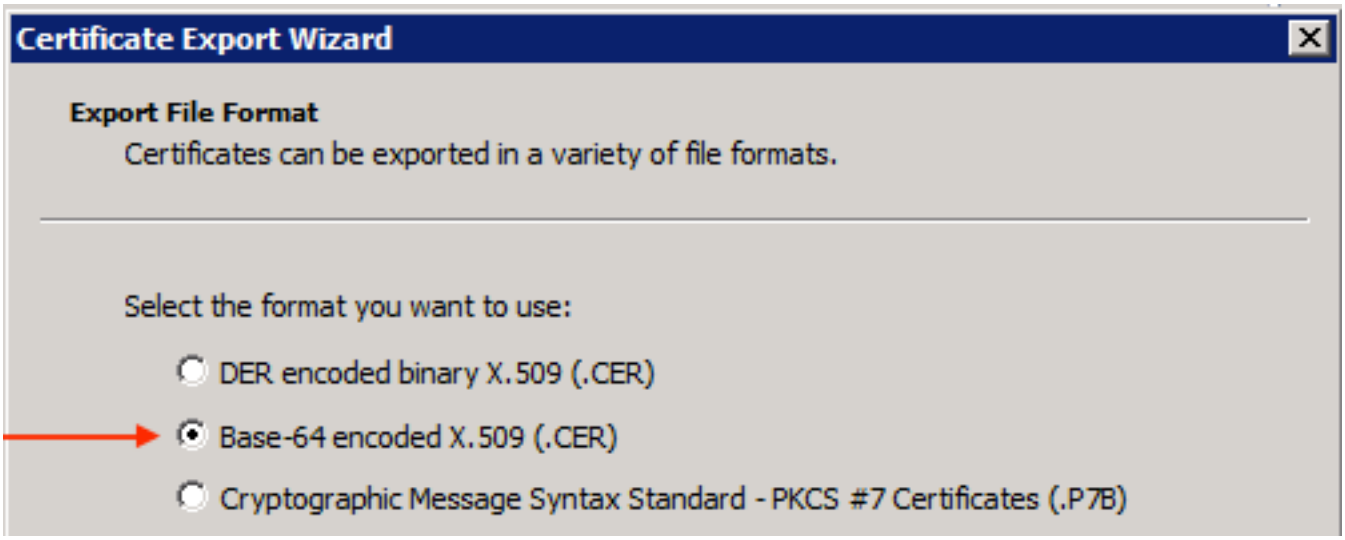
```
Select the node
-->Select 'View Certificate'
---->Select the 'Details' tab
```



選擇Copy to File選項並按照Certificate Export Wizard操作（確保使用Base-64編碼格式）。

這會為清單中的每個節點生成一個.cer檔案，當您完成它們時。





在記事本、記事本、Superlime++等中開啟這些檔案以檢視雜湊證書。

若要生成該鏈（如果有），請開啟一個新文檔，然後貼上到最後一個節點的雜湊證書中。

沿清單向上貼上每個雜湊證書，以**根CA**結尾。

將**根CA**（如果沒有鏈）或生成的整個鏈貼上到受信任點。