

确定LDAPS的正确证书

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[确定证书是否存在问题。](#)

[要确定应使用的证书/链。](#)

简介

本文档介绍如何确定安全轻量目录访问协议(LDAP)的正确证书。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始(默认)配置。如果您使用的是真实网络,请确保您已经了解所有命令的潜在影响。

背景信息

安全LDAP要求统一计算系统(UCS)域将正确的证书或证书链安装为受信任点。

如果设置了错误的证书(或链),或者如果不存在,则身份验证失败。

确定证书是否存在问题。

如果安全LDAP有问题,请使用LDAP调试检查证书是否正确。

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

接下来，打开第二个会话并尝试使用您的安全LDAP凭证登录。

启用调试的会话记录尝试的登录。在日志记录会话上，运行undebug命令以停止进一步的输出。

```
undebug all
```

要确定证书是否存在潜在问题，请查看这些行的调试输出。

```
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失败，则安全连接无法建立，身份验证失败。

要确定应使用的证书/链。

一旦您确定无法建立安全连接，请确定正确的证书。

使用ethanalyzer捕获通信，然后从文件中提取证书（或链）。

在调试会话中，运行以下命令：

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

接下来，尝试使用您的凭据通过进行其他登录。

一旦您在调试会话中不再看到任何新输出，请终止捕获。使用(ctrl + c)。

使用以下命令从交换矩阵互联(FI)传输数据包捕获：

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

获得ldap.pcap文件后，在Wireshark中打开该文件，并查找开始初始化TLS连接的数据包。

如图所示，您可以在数据包的Info部分看到类似的消息：

Server Hello, Certificate, Certificate Request, Server Hello Done			
7	0.498834	SSLv2	190 Client Hello
8	0.753397	TCP	1514 [TCP segment of a reassembled PDU]
9	0.755982	TCP	1514 [TCP segment of a reassembled PDU]
10	0.755948	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)

选择此数据包并展开：

```
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
    ▼ Handshake Protocol: Server Hello
      Handshake Type: Server Hello (2)
      Length: 70
      Version: TLS 1.0 (0x0301)
      ▶ Random
        Session ID Length: 32
        Session ID: 8d3400098910c057c220a9a20684445399d6c37d95a0408...
        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=I
```

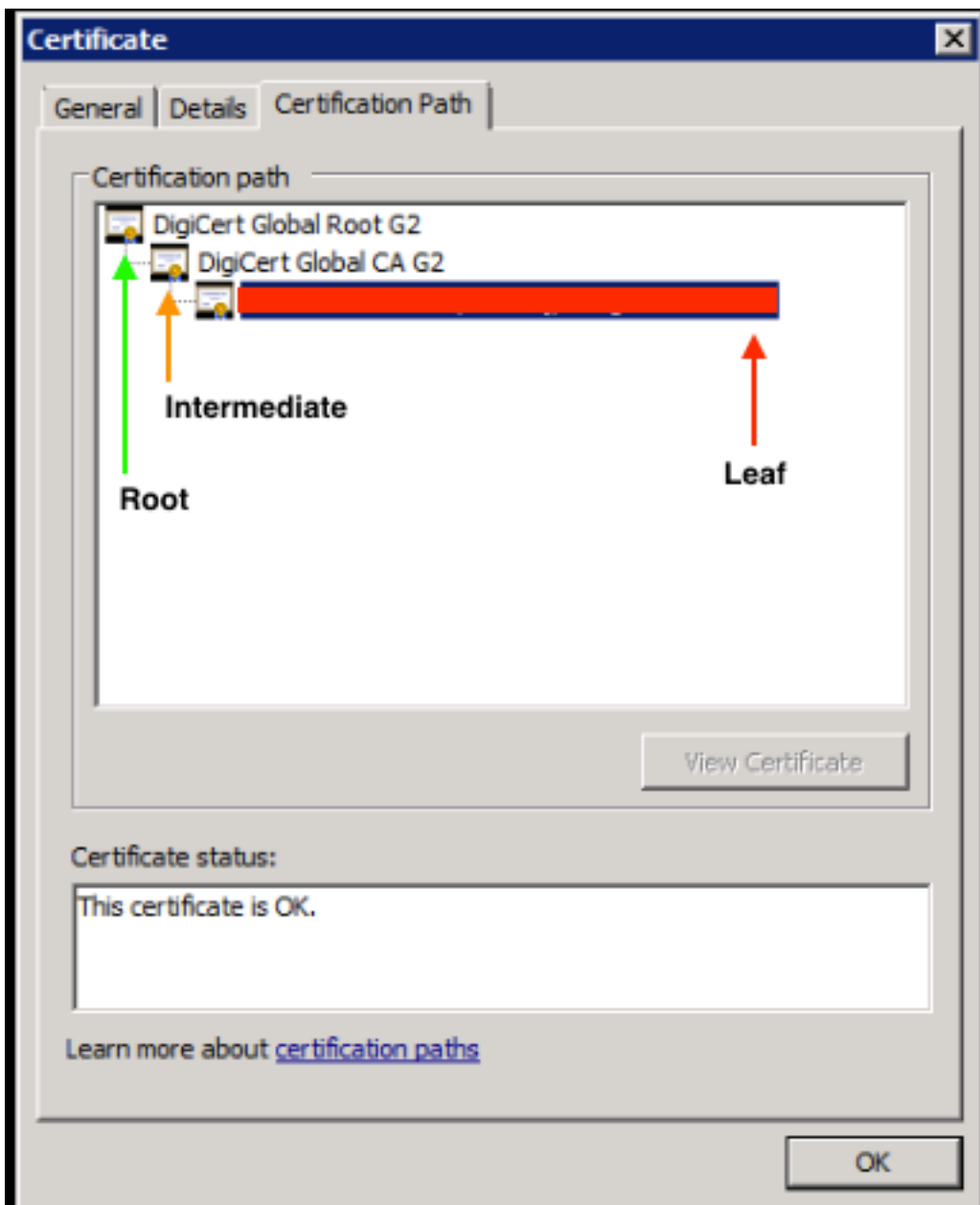
选择标题为“证书”的行。

右键单击此行，选择**导出数据包字节**(Export Packet Bytes)并将文件另存为 .der 文件。

在Windows中打开证书并导航至“**证书路径**”选项卡。

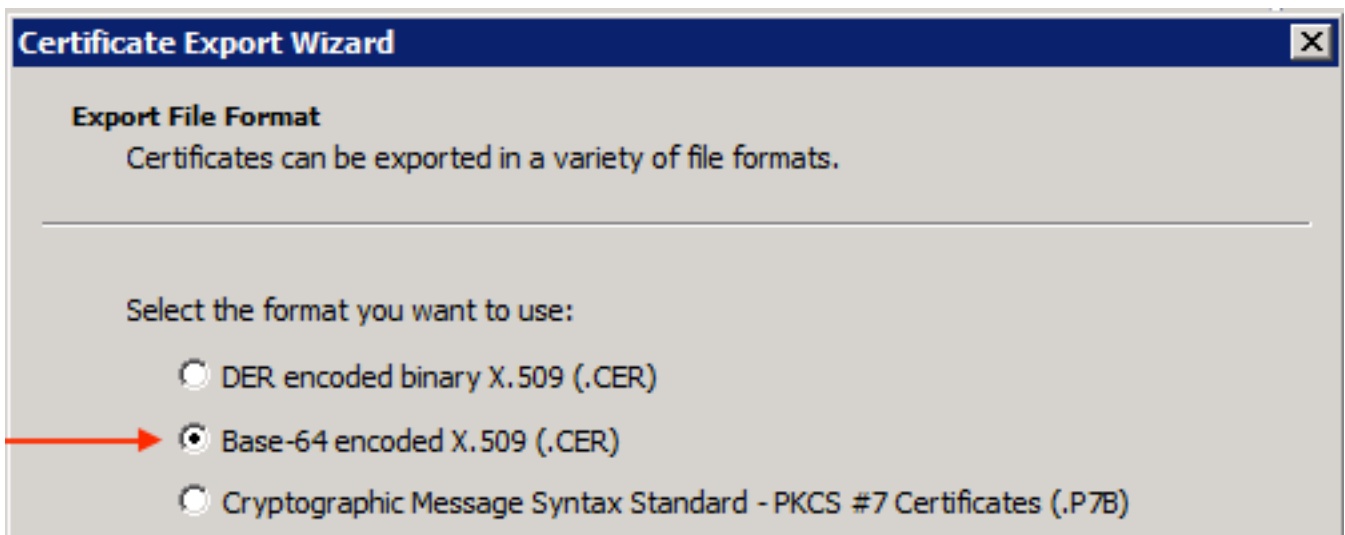
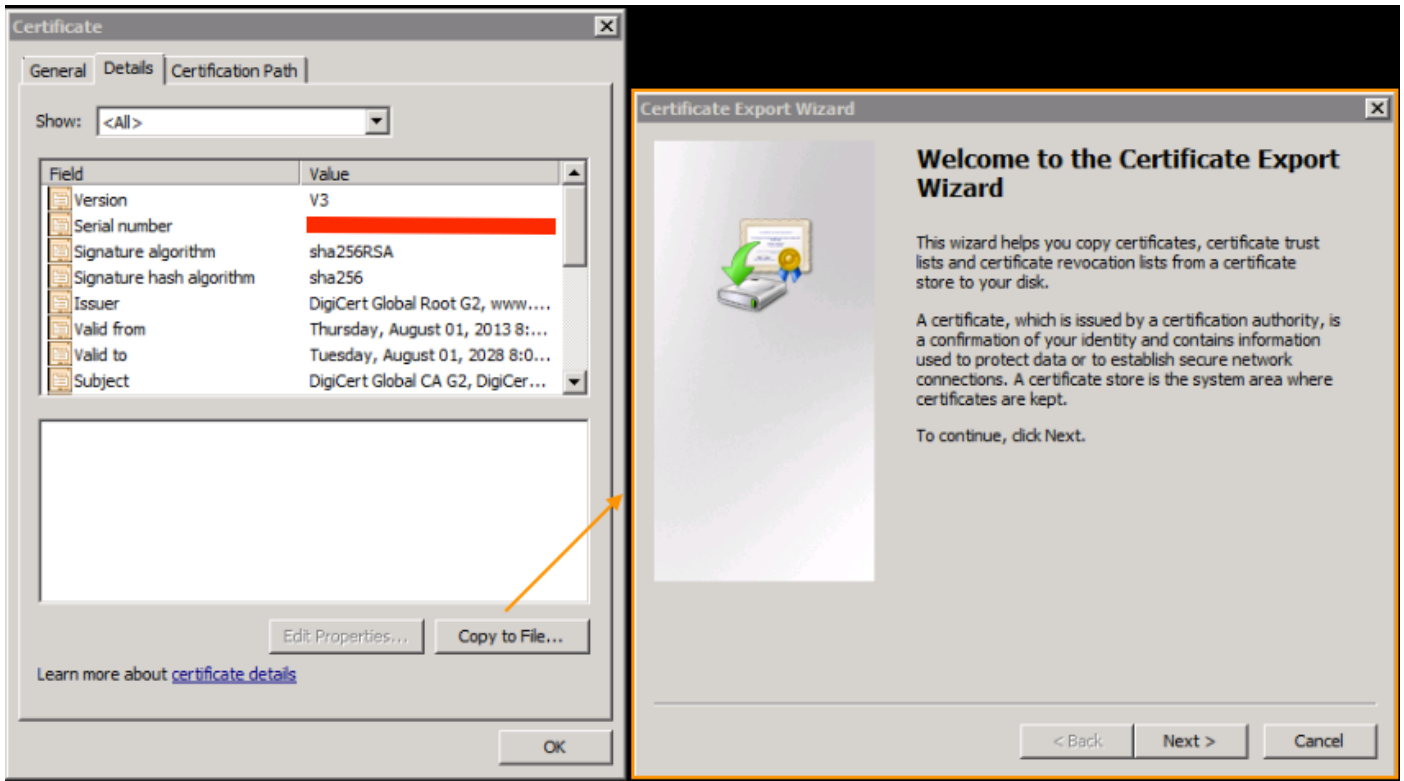
这将显示从根证书到**枝叶**(终端主机)的完整路径。对除枝叶之外列出的所有节点执行以下操作。

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



选择复制到文件选项并遵循证书导出向导（确保使用Base-64编码格式）。

这会为列表中的每个节点生成一个.cer文件，当您完成这些节点时。



在记事本、记事本++、崇高等中打开这些文件，查看经过哈希处理的证书。

要生成链（如果有），请打开新文档并粘贴最后一个节点的散列证书。

按顺序排列，粘贴每个散列证书，以根CA结束。

将根CA（如果没有链）或您生成的整个链粘贴到受信任点中。