

Determine o certificado correto para LDAPS

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Para determinar se pode haver um problema com o\(s\) certificado\(s\).](#)

[Para determinar qual certificado/cadeia você deve usar.](#)

Introduction

Este documento descreve como determinar os certificados corretos para o protocolo LDAP (Lightweight Directory Access Protocol) seguro.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Informações de Apoio

O LDAP seguro exige que o domínio do Unified Computing System (UCS) tenha o certificado ou a cadeia de certificados corretos instalados como um ponto confiável.

Se um certificado (ou cadeia) incorreto estiver configurado ou se não existir nenhum, a autenticação falhará.

[Para determinar se pode haver um problema com o\(s\) certificado\(s\).](#)

Se você tiver problemas com o LDAP seguro, use a depuração LDAP para verificar se os certificados estão corretos.

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

Em seguida, abra uma segunda sessão e tente fazer login com suas credenciais LDAP seguras.

A sessão com debugging enabled registra a tentativa de login. Na sessão de registro, execute o comando **undebug** para interromper a saída.

```
undebug all
```

Para determinar se há um problema potencial com o certificado, examine a saída de depuração dessas linhas.

```
2018 Sep 25 10:10:29.144549 ldap: ldap_do_process_tls_resp: (user f-ucsapac-01) - ldap start TLS
sent successfully;          Calling ldap_install_tls
2018 Sep 25 10:10:29.666311 ldap: ldap_do_process_tls_resp: (user f-ucsapac-01) - TLS START
failed
```

Se o TLS falhou, uma conexão segura não pôde ser estabelecida e a autenticação falhou.

Para determinar qual certificado/cadeia você deve usar.

Depois de determinar que houve uma falha ao estabelecer a conexão segura, determine quais devem ser os certificados corretos.

Use o analisador de erros para capturar a comunicação e depois extrair o certificado (ou cadeia) do arquivo.

Em sua sessão de depuração, execute o comando:

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

Em seguida, tente fazer outro login via com suas credenciais.

Quando você não vir mais nenhuma saída nova na sessão de depuração, mate a captura. Usar (**ctrl + c**).

Transfira a captura de pacotes do Interconector de estrutura (FI) com este comando:

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

Depois de ter o arquivo ldap.pcap, abra o arquivo no Wireshark e procure um pacote que inicialize a conexão TLS.

Você pode ver uma mensagem semelhante na seção **Info** do pacote, como mostrado na imagem:

```
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	0.755902		TCP	1514	[TCP segment of a reassembled PDU]
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
12	1.007214		TLSv1	73	Alert (Level: Fatal, Description: Unknown CA)

Selecione este pacote e expanda-o:

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: 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=

```

Selecione a linha intitulada **Certificado**.

Clique com o botão direito do mouse nesta linha e selecione **Exportar bytes de pacote** e salve o arquivo como um arquivo **.der**.

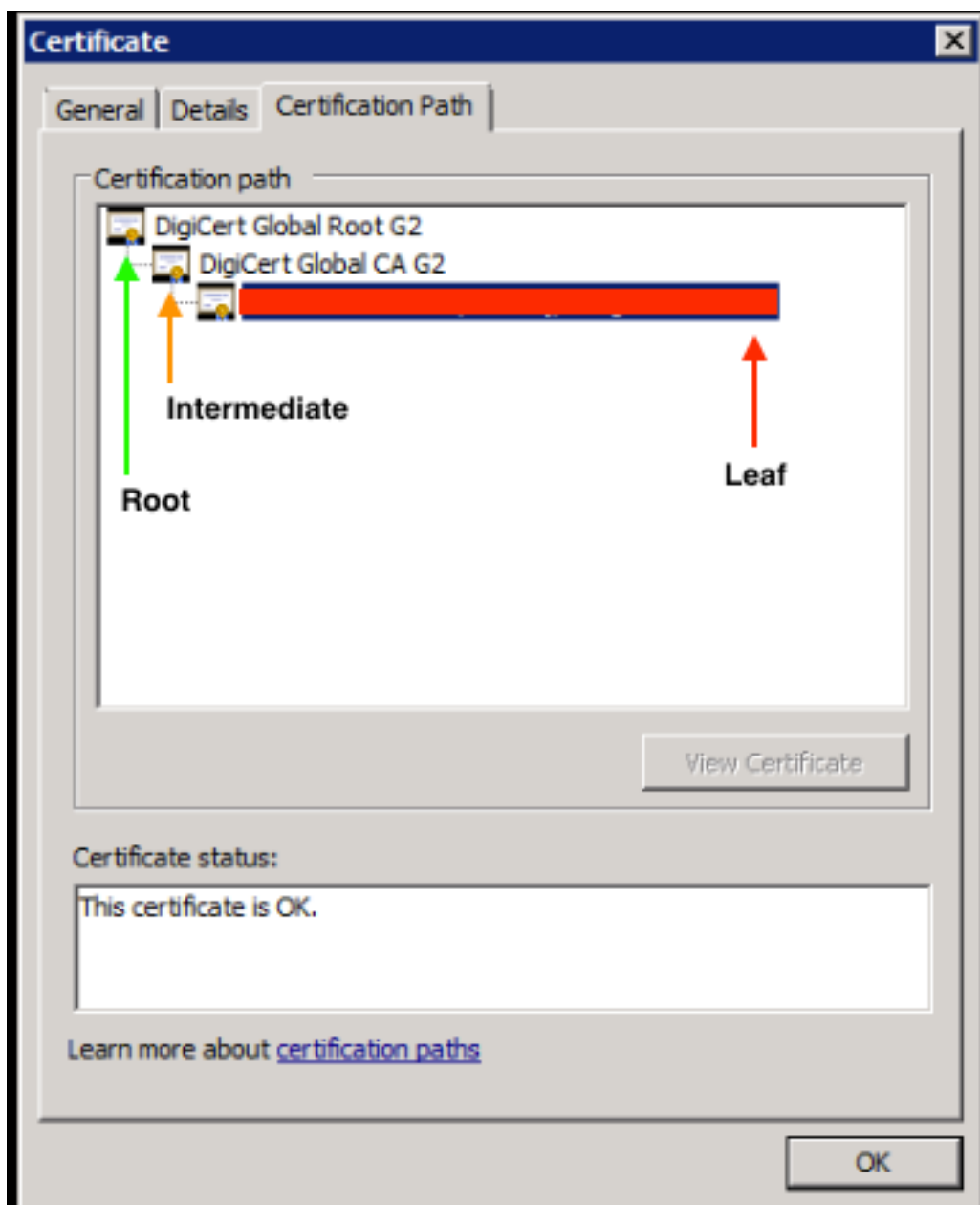
Abra o certificado no Windows e navegue até a guia **Caminho do certificado**.

Mostra o caminho completo do certificado **raiz** para a **folha** (host final). Faça o seguinte para todos os nós listados, exceto para a **folha**.

Select the node

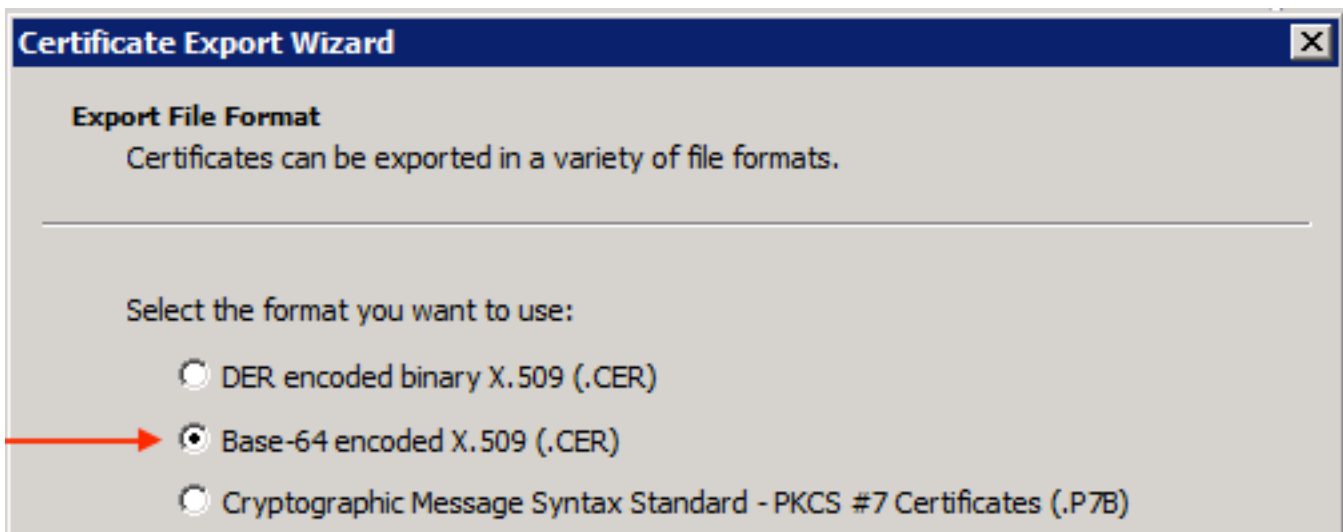
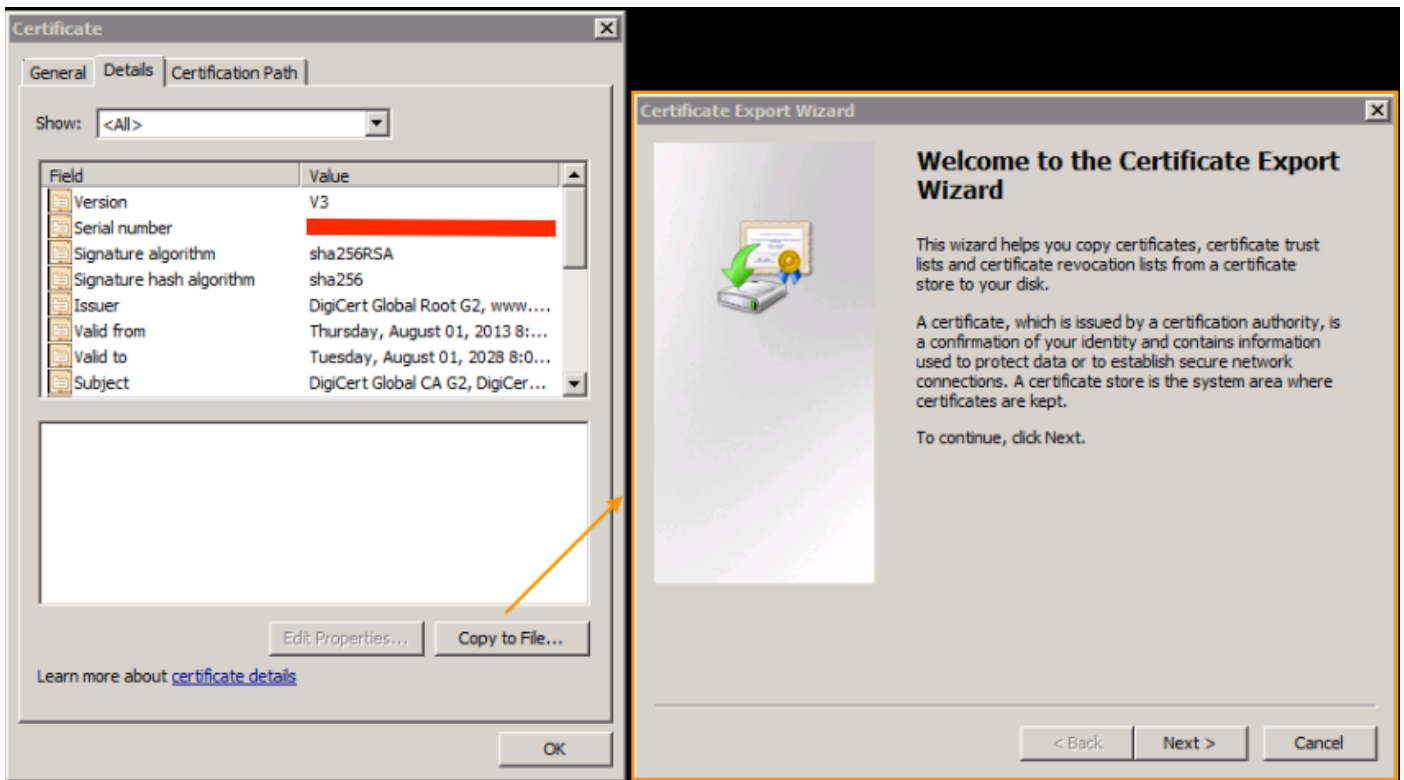
-->Select 'View Certificate'

---->Select the 'Details' tab



Selecione a opção **Copiar para arquivo** e siga o **Assistente para exportação de certificado** (certifique-se de usar o formato codificado de Base 64).

Isso gera um arquivo **.cer** para cada um dos nós da lista quando você os conclui.



Abra esses arquivos no Bloco de notas, Bloco de notas++, Sublime etc. para exibir o certificado hash.

Para gerar a cadeia (se houver um), abra um novo documento e cole no certificado hash do último nó.

Vá até a lista colando cada certificado hash, terminando com a **CA raiz**.

Cole a **CA raiz** (se não houver cadeia) ou toda a cadeia gerada no ponto confiável.