Determine o certificado correto para LDAPS

Contents

Introduction

Este documento descreve como determinar os certificados corretos para o protocolo LDAP (Lightweight Diretory 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 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
```

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:

```
ethanalyzer 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**).

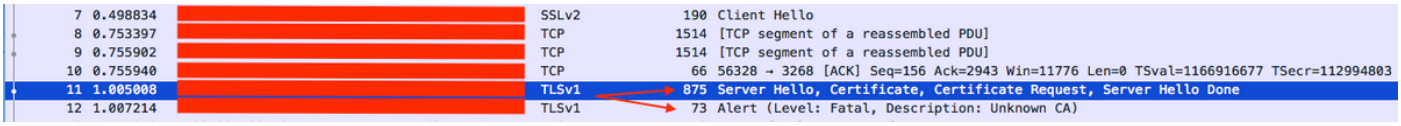
Transfira a captura de pacotes do Interconector de estrutura (FI) com este comando:

```
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.

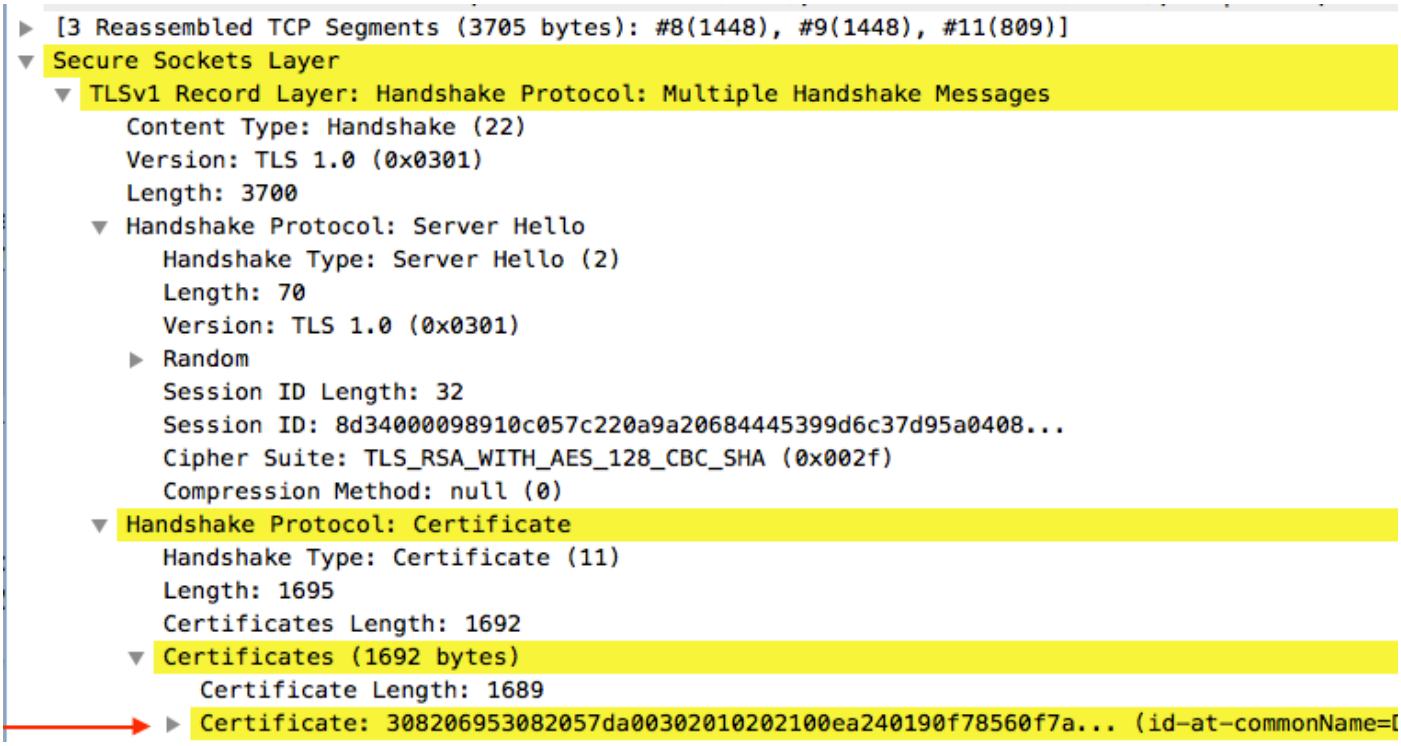
Você pode ver uma mensagem semelhante na seção **Info** do pacote, como mostrado na imagem:

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



Selecione este pacote e expanda-o:

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



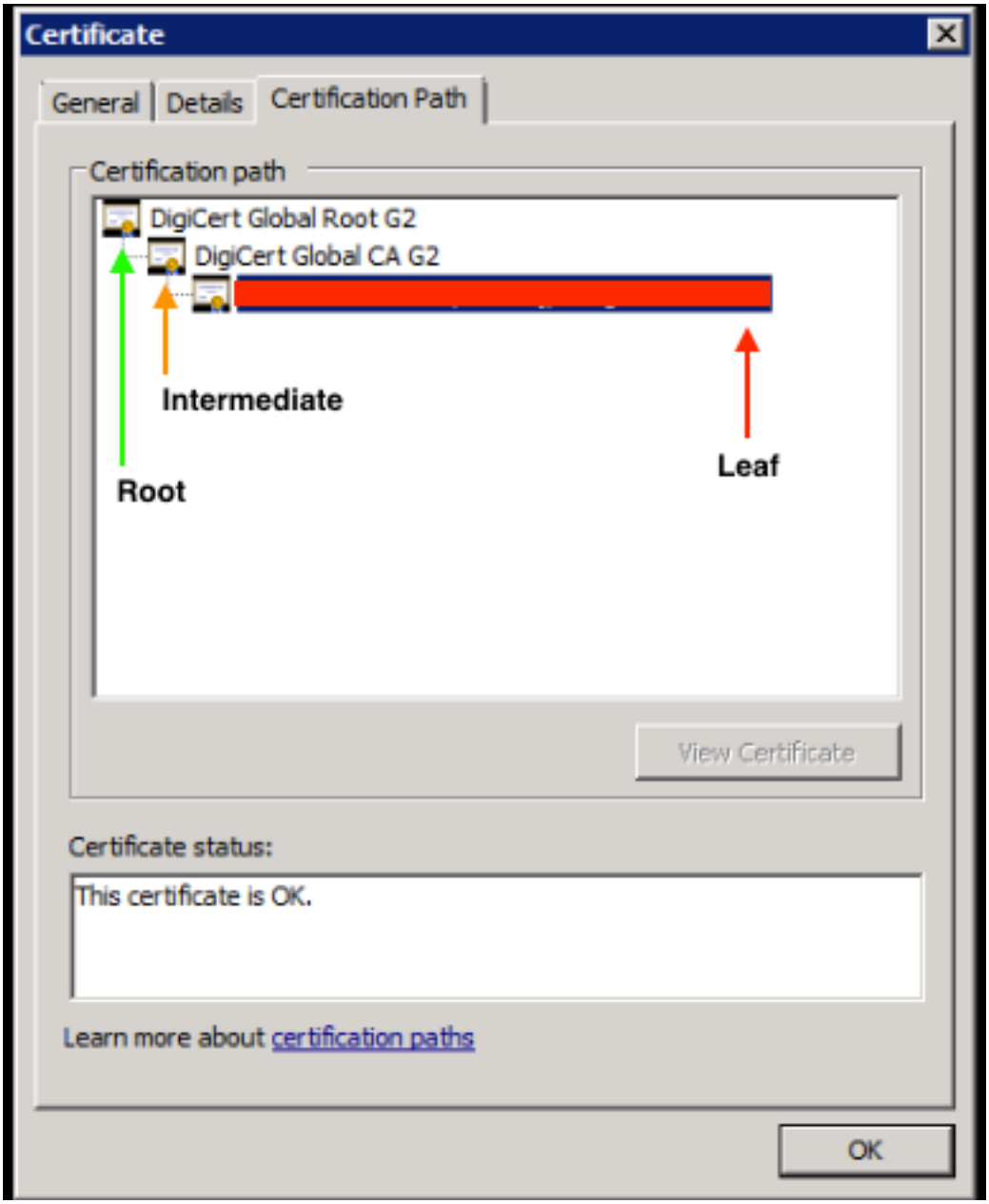
Selecione a linha intitulada **Certificado**.

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**.

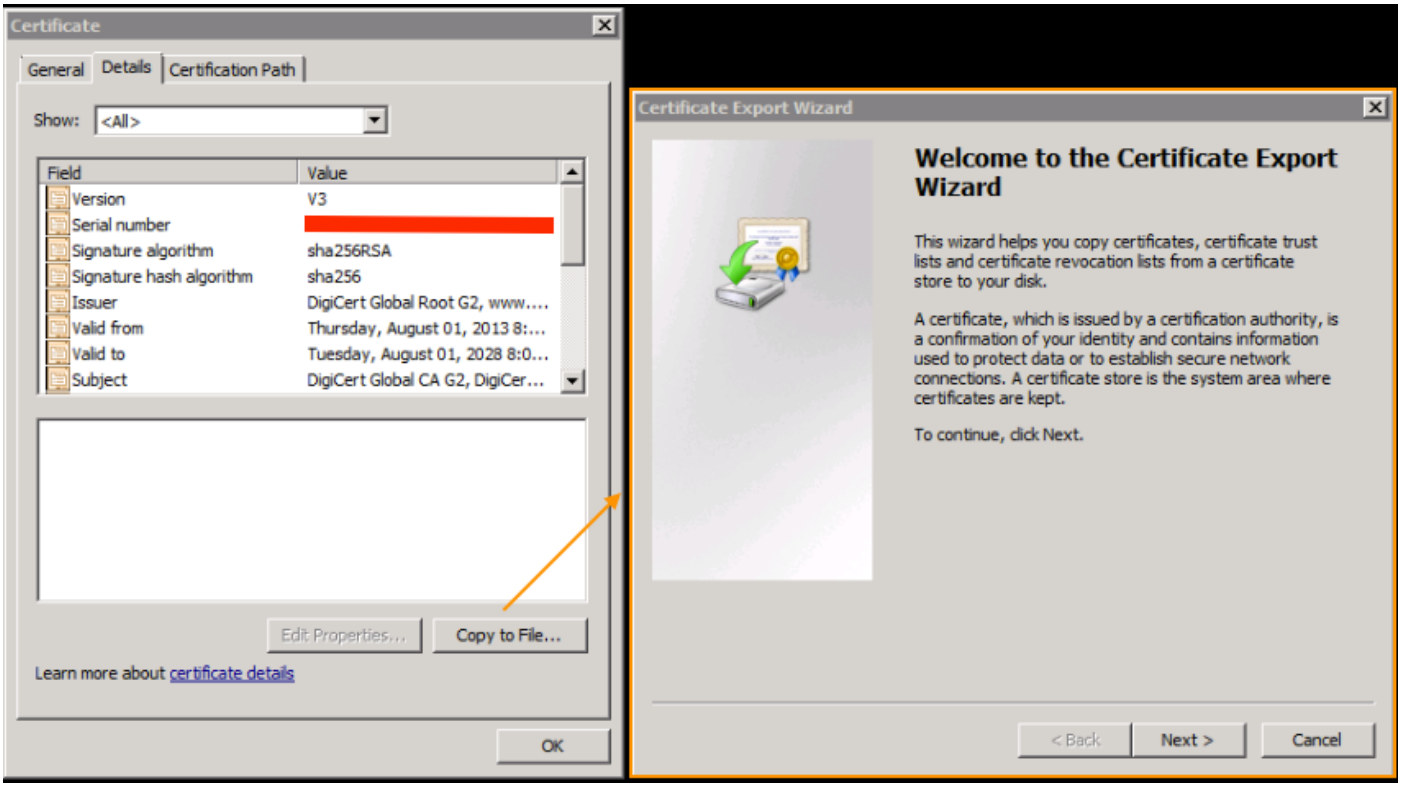
Mostra o caminho completo do certificado **raiz** para a **folha** (host final). Faça o seguinte para todos os nós listados, exceto para a **folha**.

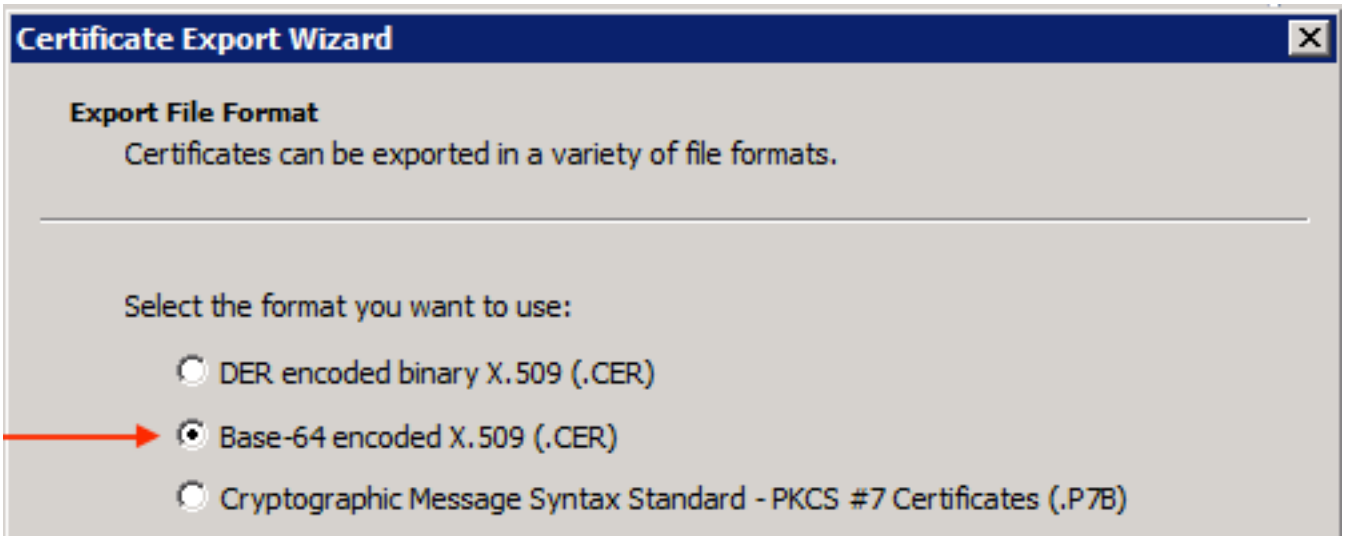
```
Select the node
-->Select 'View Certificate'
---->Select the 'Details' tab
```



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.