

Determinación del Certificado Correcto para LDAPS

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Para determinar si puede haber un problema con los certificados.](#)

[Para determinar qué certificado/cadena debe utilizar.](#)

Introducción

Este documento describe cómo determinar los certificados correctos para el protocolo ligero de acceso a directorios (LDAP) seguro.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

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.

Antecedentes

LDAP seguro requiere que el dominio Unified Computing System (UCS) tenga instalado el certificado o la cadena de certificados correctos como punto de confianza.

Si se configura un certificado (o cadena) incorrecto o si no existe ninguno, la autenticación falla.

Para determinar si puede haber un problema con los certificados.

Si tiene problemas con LDAP seguro, utilice la depuración LDAP para verificar si los certificados son correctos.

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

A continuación, abra una segunda sesión e intente iniciar sesión con sus credenciales LDAP seguras.

La sesión con depuración habilitada registra el inicio de sesión intentado. En la sesión de registro, ejecute el comando **undebug** para detener más resultados.

```
undebug all
```

Para determinar si hay un problema potencial con el certificado, observe el resultado de depuración para estas líneas.

```
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
```

Si se produjo un error en TLS, no se pudo establecer una conexión segura y la autenticación falla.

Para determinar qué certificado/cadena debe utilizar.

Una vez que haya determinado que no se pudo establecer la conexión segura, determine cuáles deben ser los certificados correctos.

Utilice etanalyzer para capturar la comunicación y, a continuación, extraer el certificado (o cadena) del archivo.

En la sesión de depuración, ejecute el comando:

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

A continuación, intente iniciar otra sesión con sus credenciales.

Cuando ya no vea ningún resultado nuevo en la sesión de depuración, termine la captura. Utilizar **(Ctrl + c)**.

Transferir la captura de paquetes desde Fabric Interconnect (FI) con este comando:

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

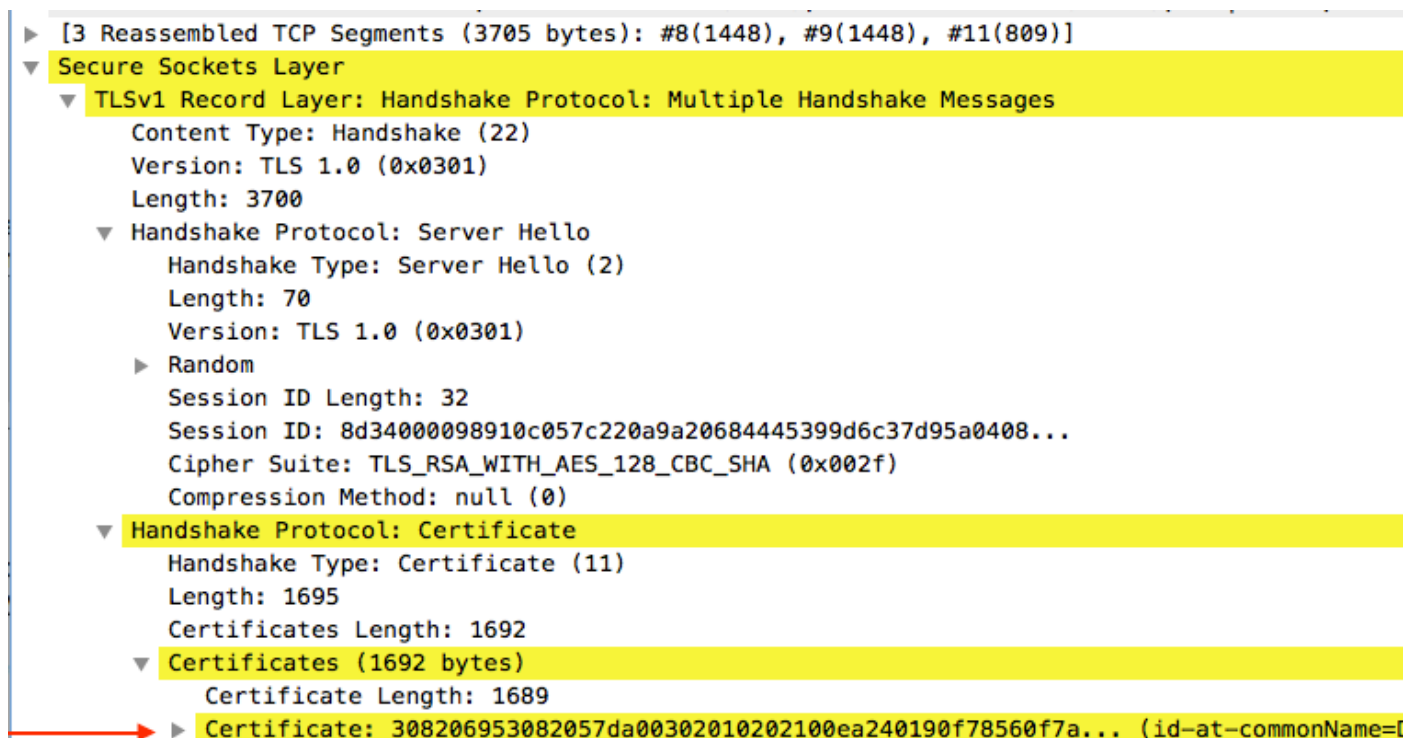
Una vez que tenga el archivo ldap.pcap, abra el archivo en Wireshark y busque un paquete que comience a inicializar la conexión TLS.

Puede ver un mensaje similar en la sección **Información** del paquete, como se muestra en la imagen:

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)

Seleccione este paquete y expúlselo:

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



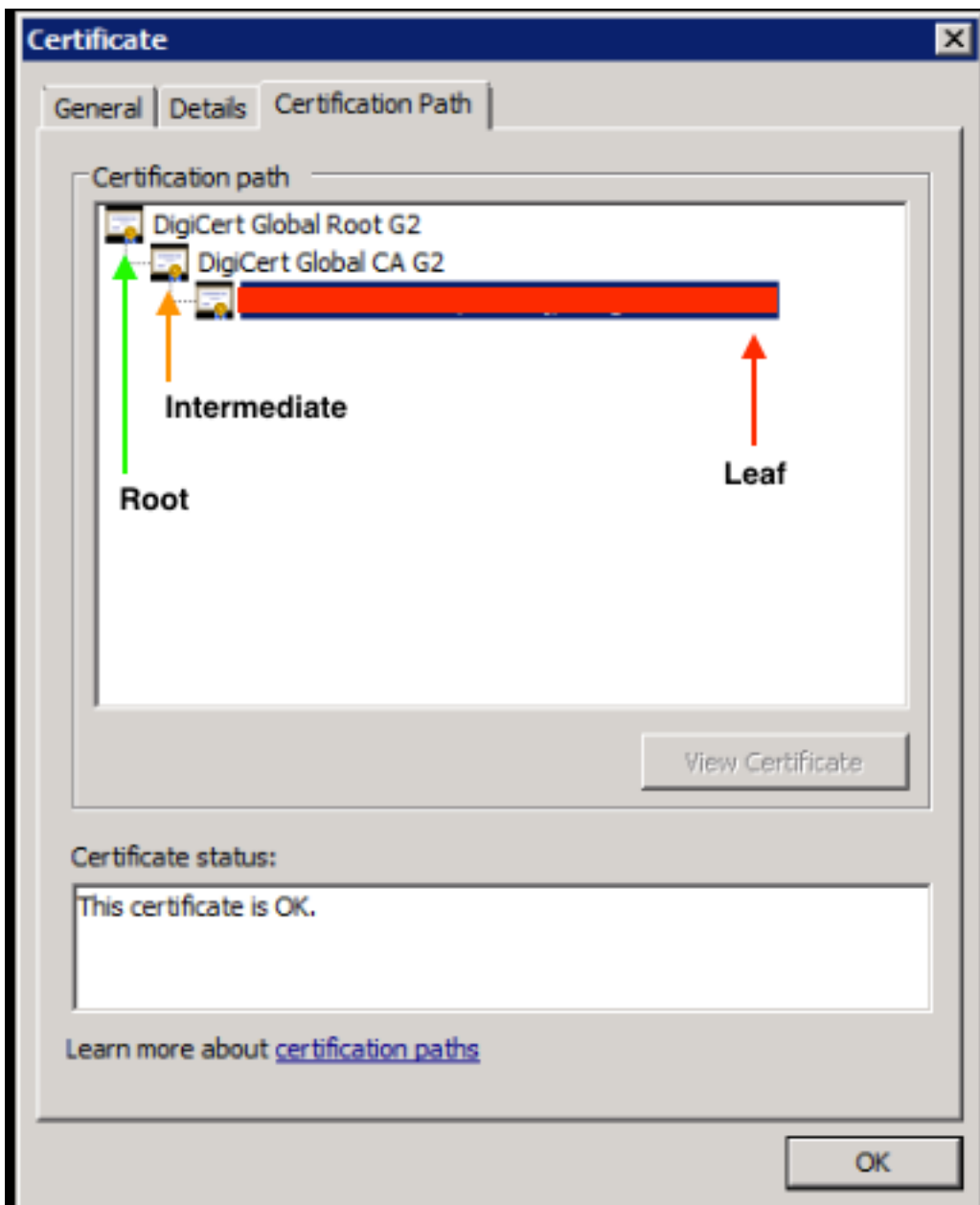
Seleccione la línea titulada **Certificate**.

Haga clic con el botón derecho del ratón en esta línea y seleccione **Exportar bytes de paquete** y guarde el archivo como un archivo **.der**.

Abra el certificado en Windows y navegue hasta la ficha **Ruta de certificado**.

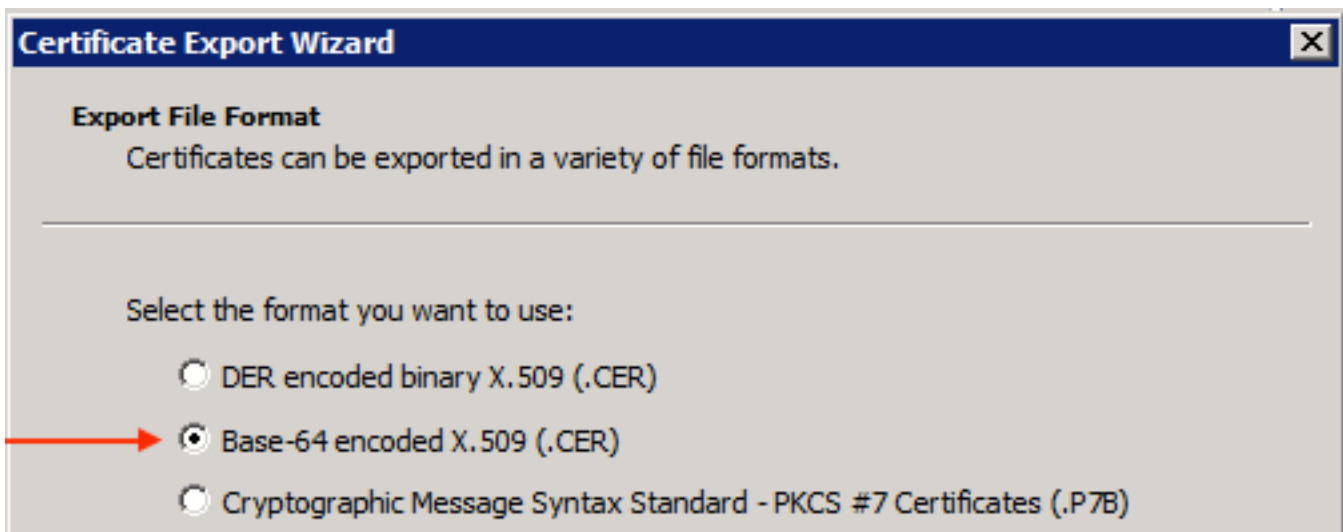
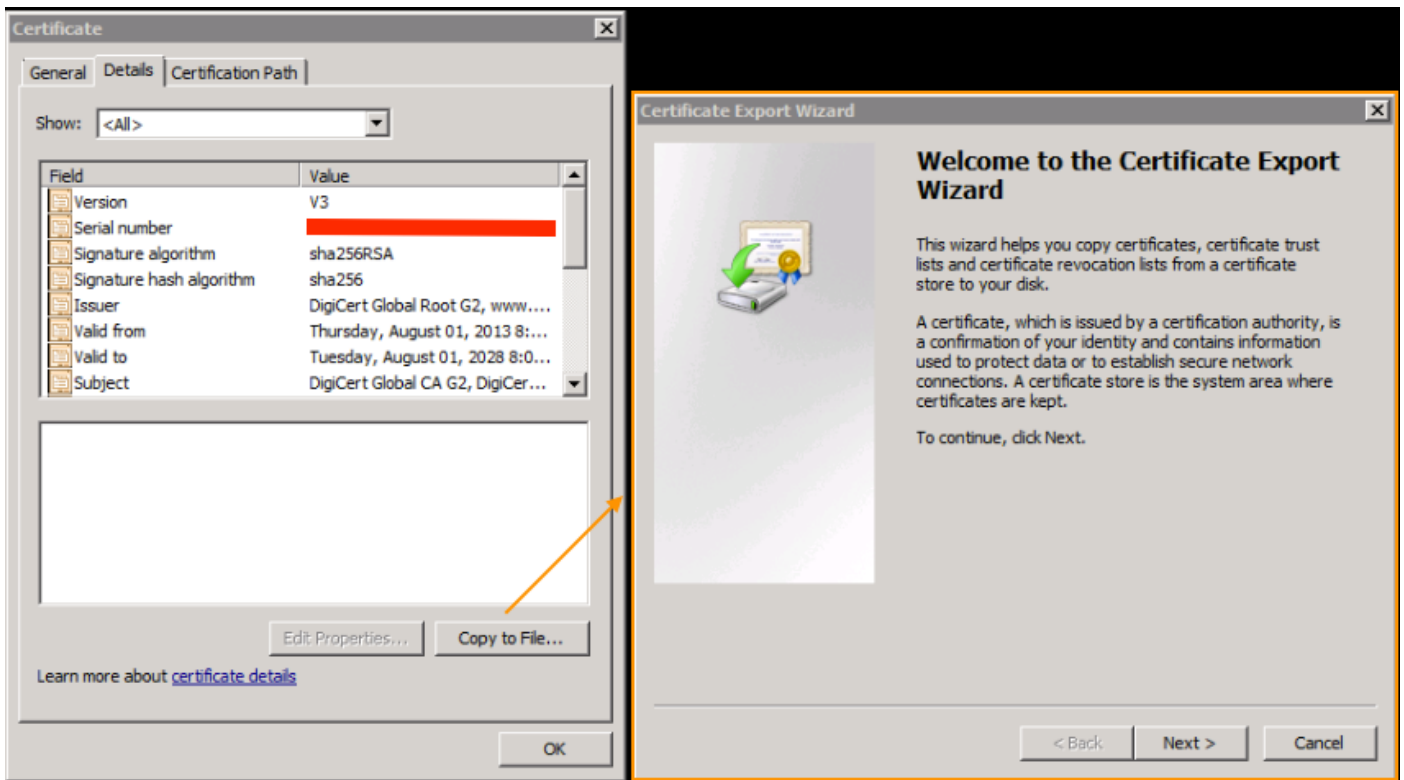
Esto le muestra la ruta completa desde el certificado **raíz** a la **hoja** (host final). Haga lo siguiente para todos los nodos enumerados excepto para la **hoja**.

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



Seleccione la opción **Copiar en archivo** y siga el **Asistente para exportación de certificados** (asegúrese de utilizar el formato codificado Base-64).

Esto genera un archivo **.cer** para cada uno de los nodos de la lista a medida que los completa.



Abra estos archivos en el Bloc de notas, Notepad++, Sublime, etc. para ver el certificado hash.

Para generar la cadena (si hay una), abra un nuevo documento y pegue en el certificado hash del último nodo.

Desplácese hacia arriba en la lista pegando cada certificado hash, terminando con la **CA raíz**.

Pegue la **CA raíz** (si no hay cadena) o toda la cadena que ha generado en el punto de confianza.