LDAPS에 대한 올바른 인증서 확인

목차

소개

이 문서에서는 LDAP(Secure Lightweight Directory Access Protocol)에 대한 올바른 인증서를 확인하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

보안 LDAP를 사용하려면 UCS(Unified Computing System) 도메인에 신뢰할 수 있는 지점으로 올바른 인증서 또는 인증서 체인이 설치되어 있어야 합니다.

잘못된 인증서(또는 체인)가 설정되어 있거나 없는 경우 인증이 실패합니다.

인증서에 문제가 있는지 확인하려면

보안 LDAP에 문제가 있는 경우 LDAP 디버깅을 사용하여 인증서가 올바른지 확인합니다.

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

그런 다음 두 번째 세션을 열고 보안 LDAP 자격 증명을 사용하여 로그인을 시도합니다.

디버깅이 활성화된 세션은 시도한 로그인을 로깅합니다. 로깅 세션에서 undebug 명령을 실행하여 **추가** 출력을 중지합니다.

```
undebug all
```

인증서에 잠재적인 문제가 있는지 확인하려면 이러한 행에 대한 디버깅 출력을 확인하십시오.

```
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
```

TLS가 실패하면 보안 연결을 설정할 수 없으며 인증에 실패합니다.

사용할 인증서/체인을 결정합니다.

보안 연결을 설정하는 데 실패했음을 확인한 후 올바른 인증서를 결정합니다.

에탄라이저를 사용하여 통신을 캡처하고 파일에서 인증서(또는 체인)를 추출합니다.

디버깅 세션에서 다음 명령을 실행합니다.

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

그런 다음 자격 증명을 통해 다른 로그인을 시도합니다.

디버깅 세션에서 새 출력이 표시되지 않으면 캡처를 종료합니다. (**ctrl + c**)를 사용합니다.

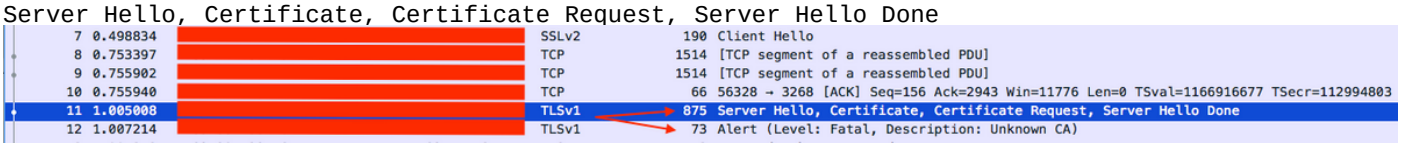
다음 명령을 사용하여 FI(Fabric Interconnect)에서 패킷 캡처를 전송합니다.

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

ldap.pcap 파일이 있는 경우 Wireshark에서 파일을 열고 TLS 연결 초기화를 시작하는 패킷을 찾습니다.

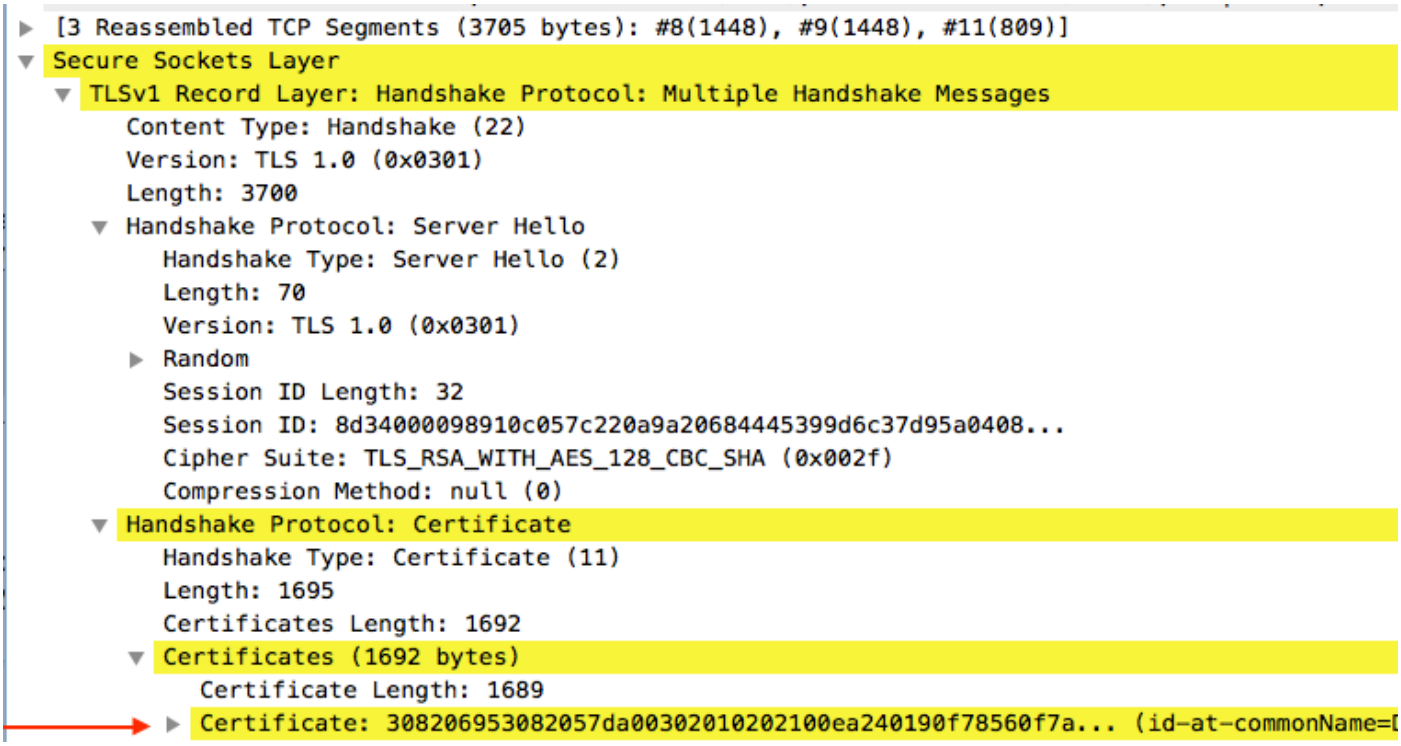
이미지에 표시된 것처럼 패킷에 대한 **Info** 섹션에서 유사한 메시지를 볼 수 있습니다.

Server Hello, Certificate, Certificate Request, Server Hello Done



이 패킷을 선택하고 확장합니다.

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



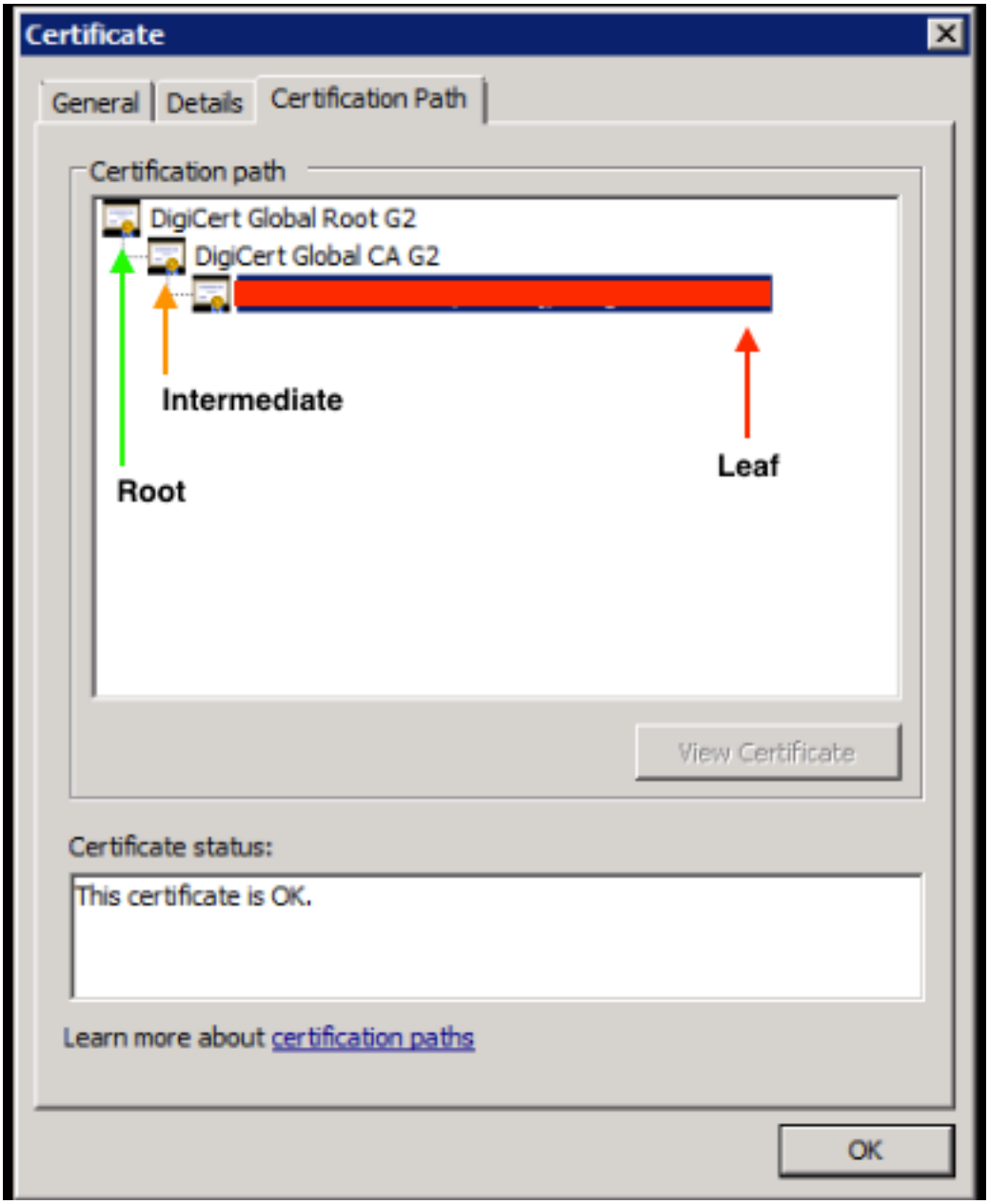
Certificate(인증서)라는 행을 **선택합니다**.

이 줄을 마우스 오른쪽 단추로 클릭하고 **Export Packet Bytes(패킷 바이트 내보내기)**를 선택하고 파일을 **.der** 파일로 저장합니다.

Windows에서 인증서를 열고 **Certificate Path** 탭으로 이동합니다.

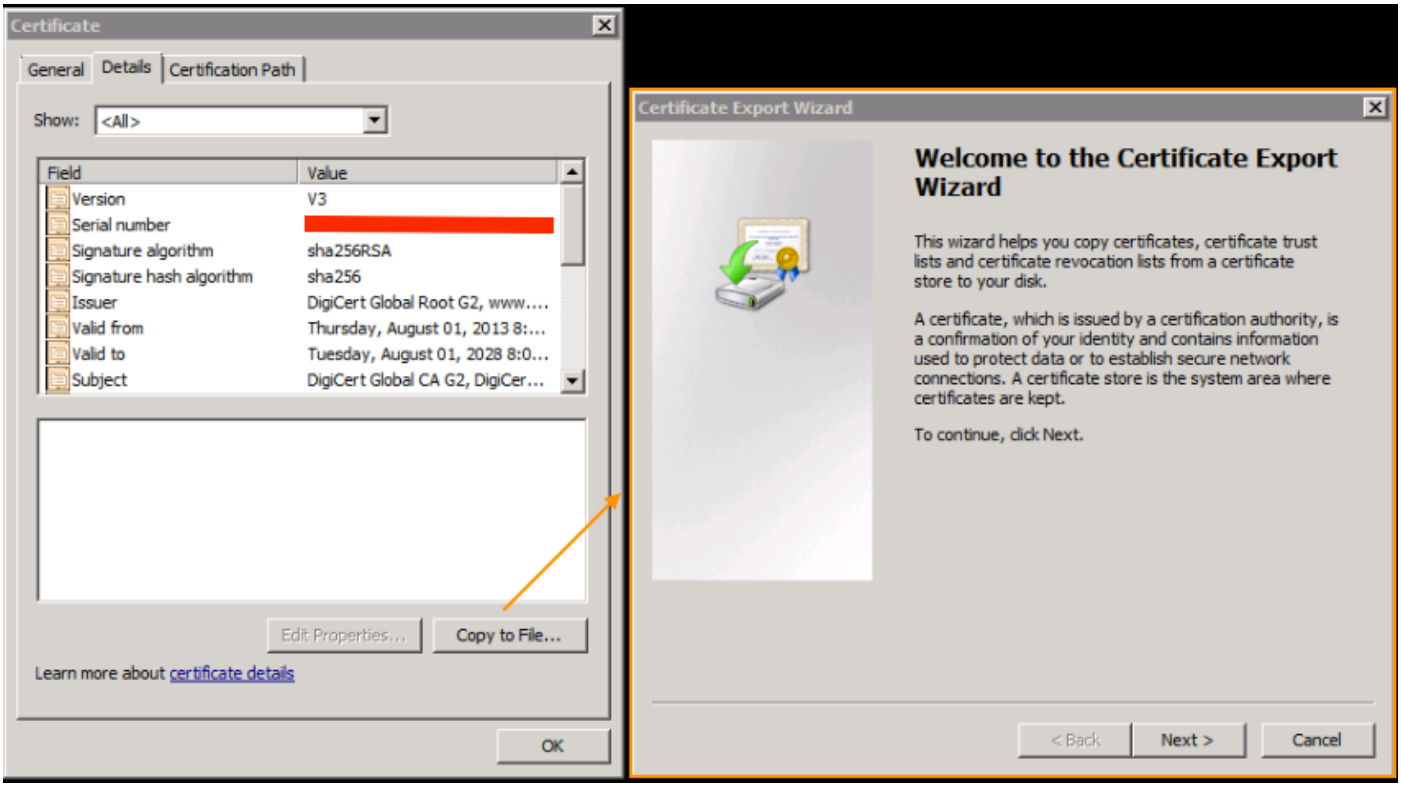
루트 인증서에서 **리프**(엔드 호스트)로의 전체 경로를 표시합니다. leaf를 제외하고 나열된 모든 노드에 대해 다음을 **수행합니다**.

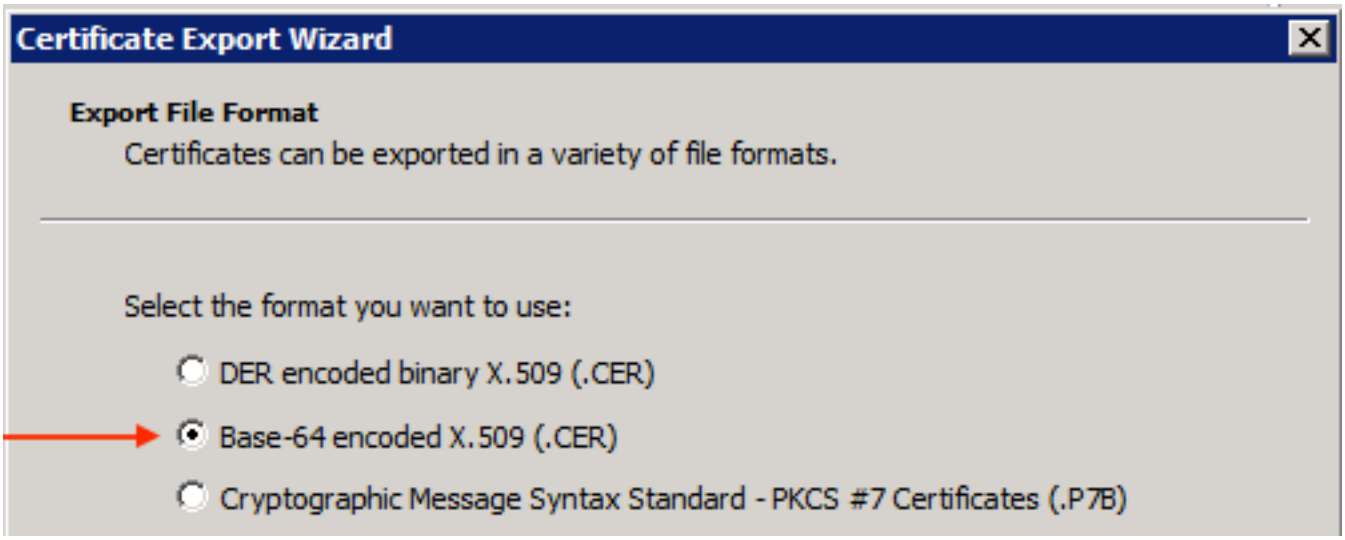
```
Select the node
-->Select 'View Certificate'
---->Select the 'Details' tab
```



Copy to **File(파일로 복사)** 옵션을 선택하고 **Certificate Export Wizard(인증서 내보내기 마법사)**를 따릅니다(Base-64 인코딩 형식을 사용해야 함).

이렇게 하면 목록의 각 노드에 대해 **.cer** 파일이 생성됩니다.





Notepad, Notepad+, Sorabe 등에서 이 파일을 열어 해시된 인증서를 봅니다.

체인을 생성하려면(있는 경우) 새 문서를 열고 마지막 노드의 해시된 인증서에 붙여넣습니다.

루트 CA로 끝나는 해시된 각 인증서를 붙여 넣는 목록을 위로 **이동합니다**.

루트 CA(체인이 없는 경우) 또는 생성한 전체 체인을 신뢰 지점에 붙여넣습니다.