Ldp.exe를 사용하여 LDAP over SSL/TLS(LDAPS) 및 CA 인증서 확인

목차

소개

FireSIGHT Management Center for Active Directory LDAP Over SSL/TLS(LDAPS)에서 인증 객체를 생성할 때 CA 인증서 및 SSL/TLS 연결을 테스트하고 인증 객체가 테스트에 실패하는지 확인해야 할 수도 있습니다. 이 문서에서는 Microsoft Ldp.exe를 사용하여 테스트를 실행하는 방법에 대해 설명합니다.

확인 방법

시작하기 전에

로컬 관리 권한이 있는 사용자 계정으로 Microsoft Windows 로컬 컴퓨터에 로그인하여 이 문서에 대한 단계를 수행합니다.

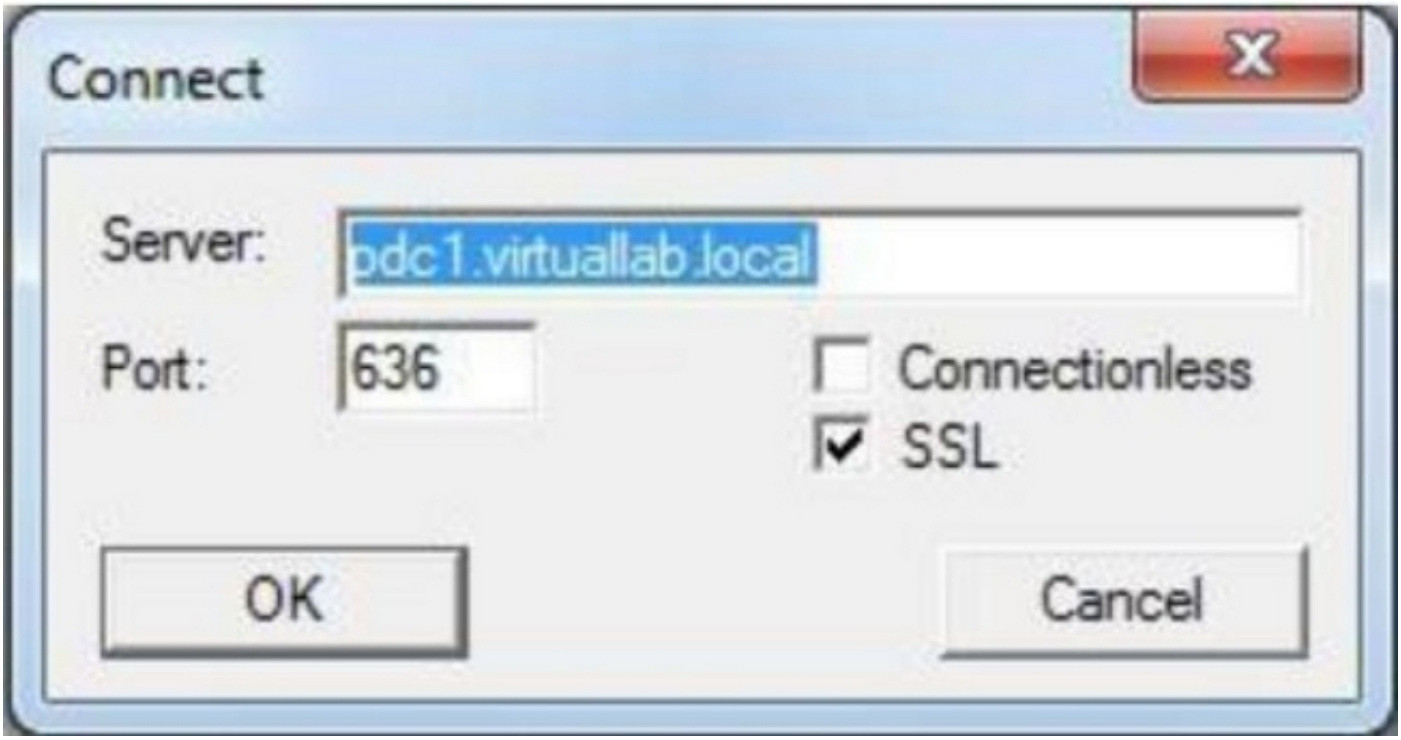
> **참고:** 현재 시스템에 ldp.exe를 사용할 수 없는 경우 먼저 **Windows 지원** 도구를 다운로드해야 **합니다**. Microsoft 웹 사이트에서 사용할 수 있습니다. **Windows 지원** 도구를 다운로드하고 설치한 **후** 다음 단계를 수행하십시오.

도메인에 가입된 경우 루트 또는 엔터프라이즈 CA를 신뢰하므로 도메인의 구성원이 아닌 로컬 Windows 컴퓨터에서 이 테스트를 수행합니다. 로컬 컴퓨터가 더 이상 도메인에 없는 경우 이 테스트를 수행하기 전에 로컬 컴퓨터의 **신뢰할 수** 있는 루트 인증 기관 저장소에서 루트 또는 엔터프라이즈 CA 인증서를 제거해야 합니다.

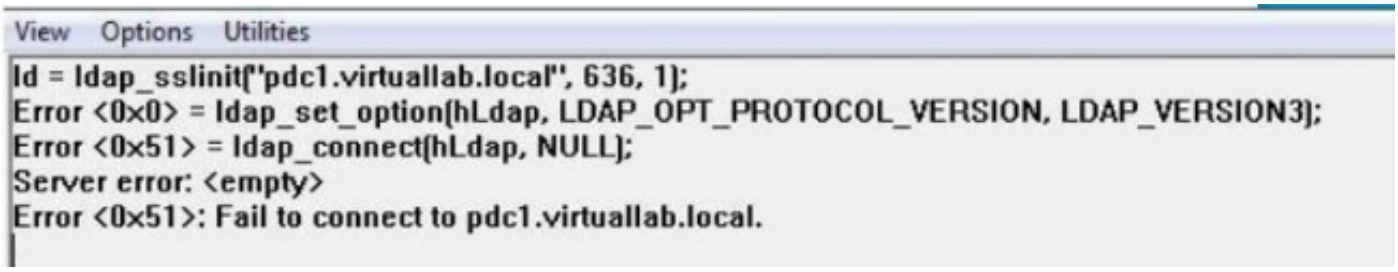
확인 단계

1단계: ldp.exe 응용 프로그램 시작 **시작** 메뉴로 **이동하여** 실행을 **클릭합니다**. ldp.**exe**를 입력하고 **OK**(**확인**) 버튼을 누릅니다.

2단계: 도메인 컨트롤러 FQDN을 사용하여 도메인 컨트롤러에 연결합니다. 연결하려면 Connection(연결) **> Connect(연결)**로 이동하여 도메인 컨트롤러 FQDN을 입력합니다. 그런 다음 **SSL을** 선택하고, 아래와 같이 포트 **636**을 지정하고, **OK**를 클릭합니다.



3단계: 로컬 컴퓨터에서 루트 또는 엔터프라이즈 CA를 신뢰할 수 없는 경우 결과는 다음과 같습니다. 오류 메시지는 원격 서버에서 받은 인증서가 신뢰할 수 없는 인증 기관에서 발급되었음을 나타냅니다.

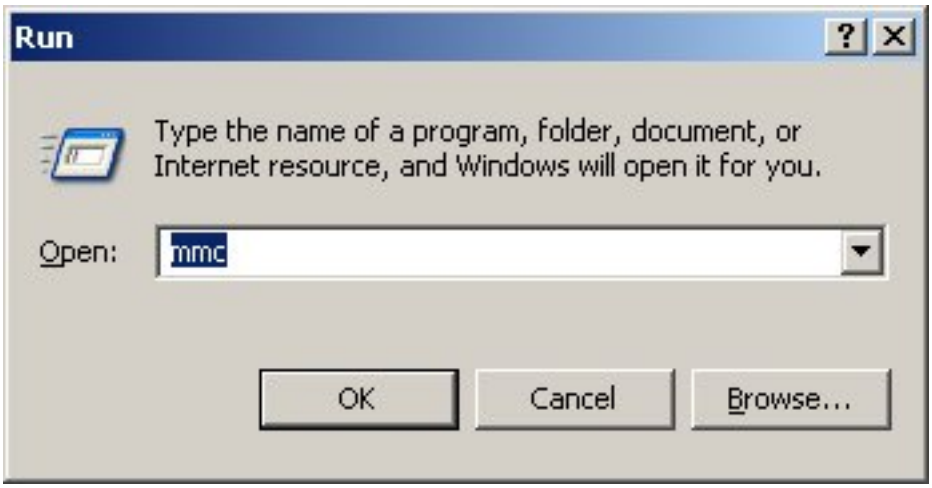


4단계: 로컬 Windows 컴퓨터에서 다음 조건으로 이벤트 메시지를 필터링하면 특정 결과가 나타납니다.

- 이벤트 소스 = Schannel
- 이벤트 ID = 36882

5단계: 로컬 Windows 컴퓨터 인증서 저장소로 CA 인증서를 가져옵니다.

i. MMC(Microsoft Management Console)를 실행합니다. **시작** 메뉴로 **이동하여** 실행을 **클릭합니다**. mmc**를** 입력하고 **OK** 버튼을 누릅니다.

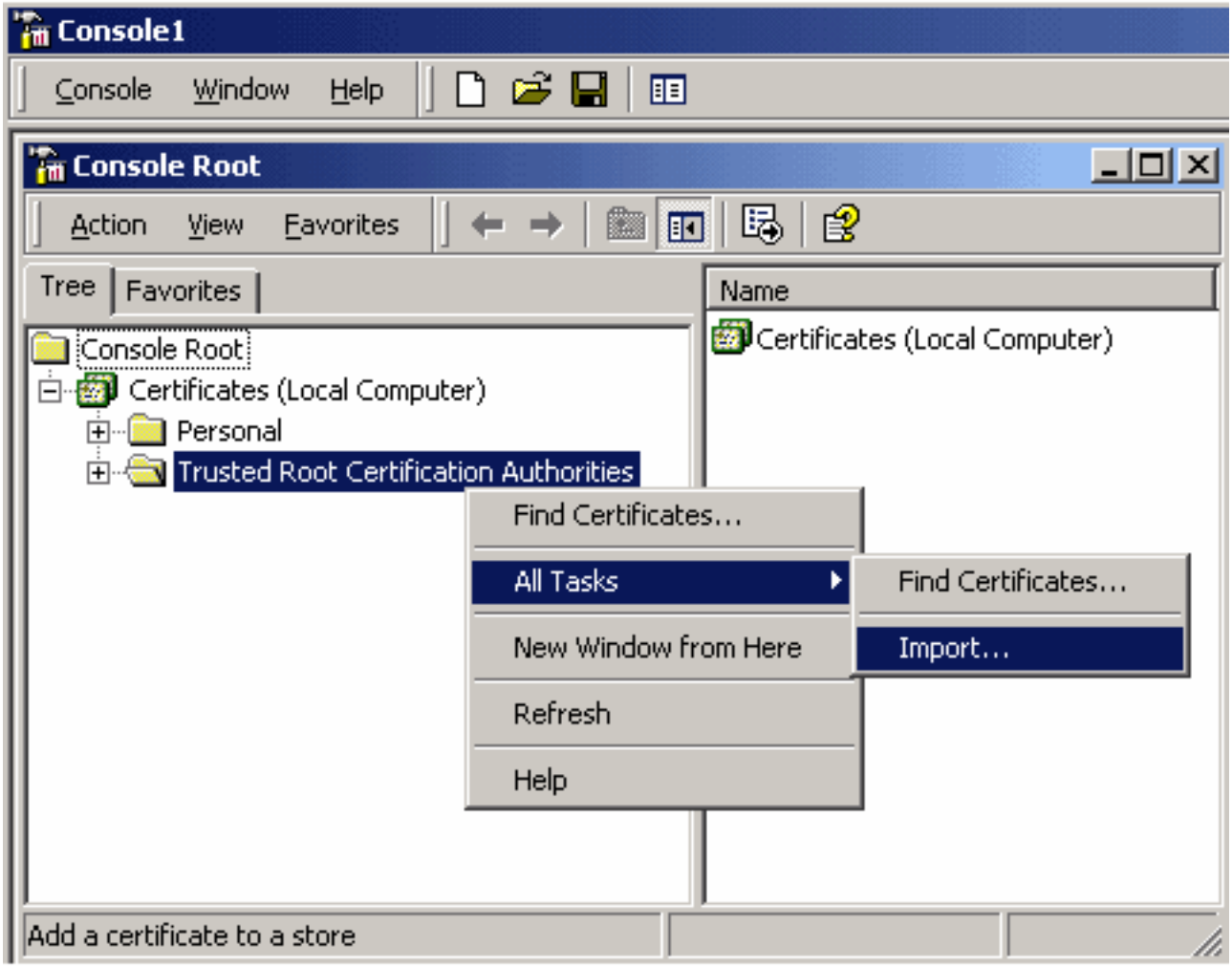


그래 로컬 컴퓨터 인증서 스냅인을 추가합니다. **파일** 메뉴에서 다음 옵션으로 이동합니다.

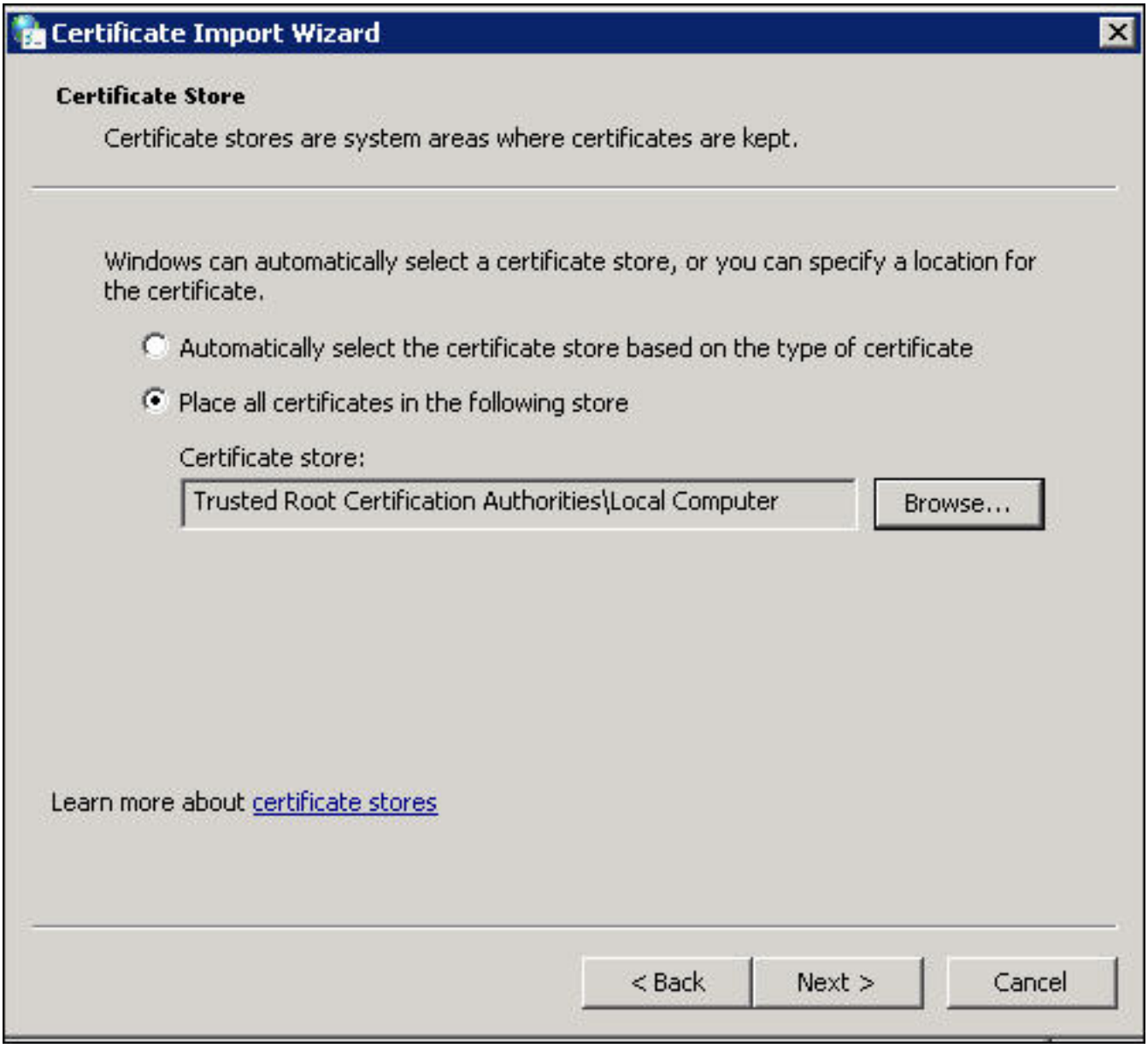
Add/Remote Snap-in(추가/원격 스냅인) > Certificates(인증서) > Add(추가) > Choose "Computer Account(컴퓨터 계정)" > Local Computer(로컬 컴퓨터)를 선택합니다. (이 콘솔이 실행 중인 컴퓨터) > 마침 > 확인.

iii. CA 인증서를 가져옵니다.

Console Root(콘솔 루트) > Certificates (Local Computer)(인증서(로컬 컴퓨터)) **>Trusted Root Certification Authorities(신뢰할 수 있는 루트 인증 기관) > Certificates(인증서)** > Right Click(오른쪽 클릭) > **All Tasks(모든 작업)** >Import(가져오기)를 **클릭합니다.**



- Next(**다음**)를 클릭하고 Base64 Encoded X.509 Certificate (*.cer, *.crt) CA 인증서 파일을 찾습니다. 그런 다음 파일을 선택합니다.
- Open(**열기**) > **Next(다음)**를 클릭하고 **Place all certificates in the following store(다음 저장소에 모든 인증서 배치)를** 선택합니다. **신뢰할 수 있는 루트 인증 기관**.
- 파일을 **가져오려면 Next(다음) > Finish(마침)**를 클릭합니다.



iv. CA가 다른 신뢰할 수 있는 루트 CA와 함께 나열되는지 확인합니다.

6단계: 1단계와 2단계를 따라 SSL을 통해 AD LDAP 서버에 연결합니다. CA 인증서가 올바르면 ldp.exe의 오른쪽 창에 있는 처음 10개 줄은 아래와 같아야 합니다.

```
ld = ldap_sslinit("pdc1.virtuallab.local", 636, 1);
Error <0x0> = ldap_set_option(hLdap, LDAP_OPT_PROTOCOL_VERSION, LDAP_VERSION3);
Error <0x0> = ldap_connect(hLdap, NULL);
Error <0x0> = ldap_get_option(hLdap,LDAP_OPT_SSL,(void*)&lv);
Host supports SSL, SSL cipher strength = 128 bits
Established connection to pdc1.virtuallab.local.
Retrieving base DSA information...
Result <0>: (null)
Matched DNs:
Getting 1 entries:
>> Dn:
```

테스트 결과

인증서 및 LDAP 연결이 이 테스트를 통과할 경우 SSL/TLS를 통해 LDAP에 대한 인증 객체를 성공

적으로 구성할 수 있습니다. 그러나 LDAP 서버 컨피그레이션 또는 인증서 문제로 인해 테스트가 실패할 경우 FireSIGHT Management Center에서 인증 객체를 구성하기 전에 AD 서버에서 문제를 해결하거나 올바른 CA 인증서를 다운로드하십시오.

관련 문서

- 인증 객체 구성을 위한 Active Directory LDAP 객체 속성 식별
- FireSIGHT 시스템의 LDAP 인증 객체 컨피그레이션