인증 객체 구성을 위한 Active Directory LDAP 객체 속성 식별

목차

소개

이 문서에서는에서 외부 인증을 위해 인증 객체를 구성하기 위해 AD(Active Directory) LDAP 객체 속성을 식별하는 방법에 대해 설명합니다.

LDAP 객체 속성 식별

외부 인증을 위해 FireSIGHT Management Center에서 인증 객체를 구성하기 전에 외부 인증이 의도한 대로 작동하려면 사용자 및 보안 그룹의 AD LDAP 특성을 식별해야 합니다. 이를 위해 Microsoft에서 제공하는 GUI 기반 LDAP 클라이언트, Ldp.exe 또는 타사 LDAP 브라우저를 사용할 수 있습니다. 이 문서에서는 ldp.exe를 사용하여 AD 서버를 로컬로 또는 원격으로 연결, 바인딩 및 탐색하고 특성을 식별합니다.

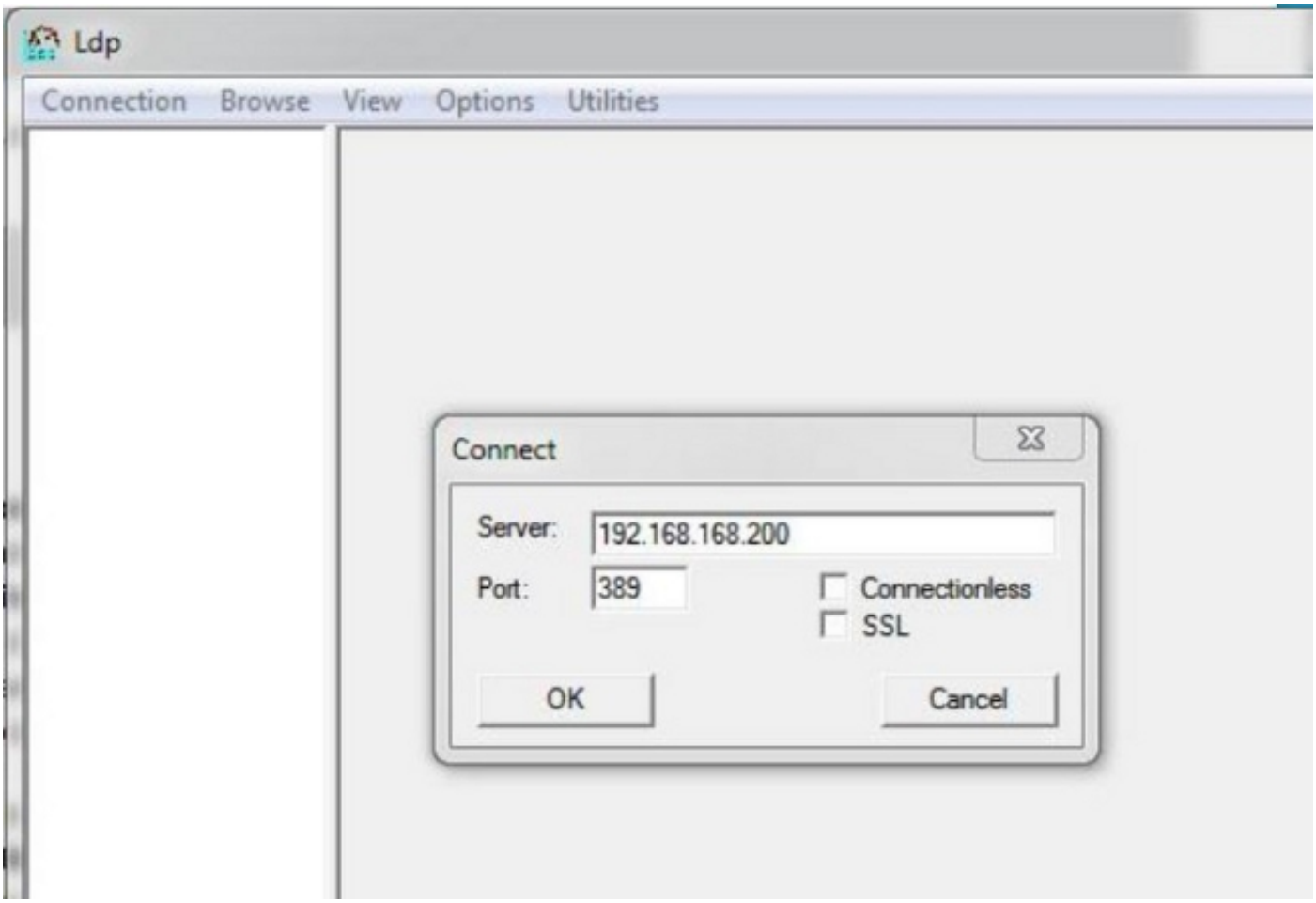
1단계: ldp.exe 응용 프로그램을 시작합니다. **시작** 메뉴로 **이동하여** 실행을 **클릭합니다**. ldp**.exe**를 입력하고 **OK**(**확인**) 버튼을 누릅니다.

> **참고:** Windows Server 2008에서는 ldp.exe가 기본적으로 설치됩니다. Windows Server 2003의 경우 또는 Windows 클라이언트 컴퓨터에서 원격 연결하려는 경우 Microsoft 사이트에서 support.cab 또는 support.msi 파일을 다운로드하십시오. .cab 파일의 압축을 풀거나 .msi 파일을 설치하고 ldp.exe를 실행합니다.

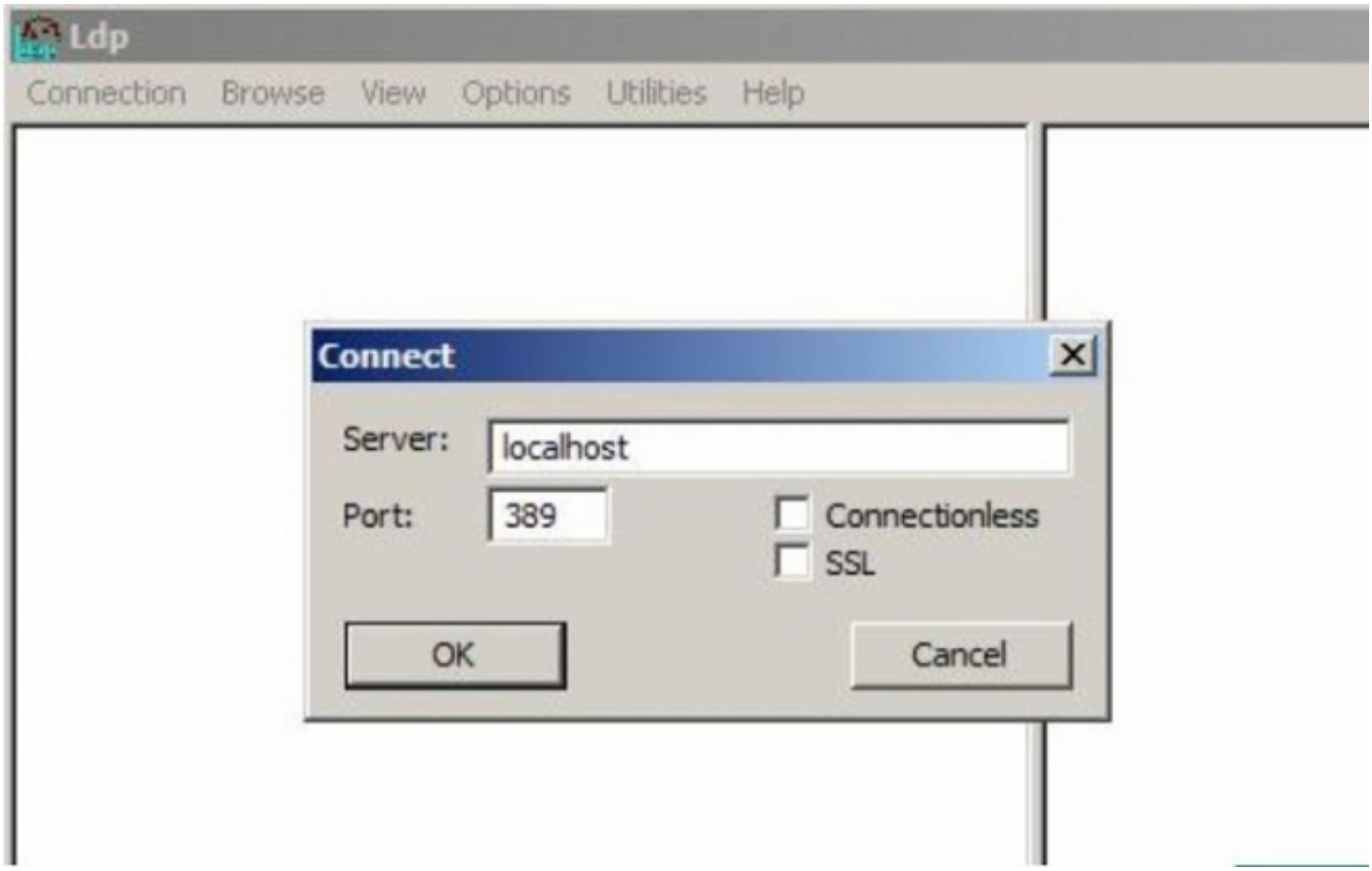
2단계: 서버에 연결합니다. 연결**을** 선택하고 연결을 **클릭합니다**.

- 로컬 컴퓨터에서 AD DC(Domain Controller)에 연결하려면 AD 서버의 호스트 이름 또는 IP 주소를 입력합니다.
- AD DC에 로컬로 연결하려면 localhost를 Server로 **입력합니다**.

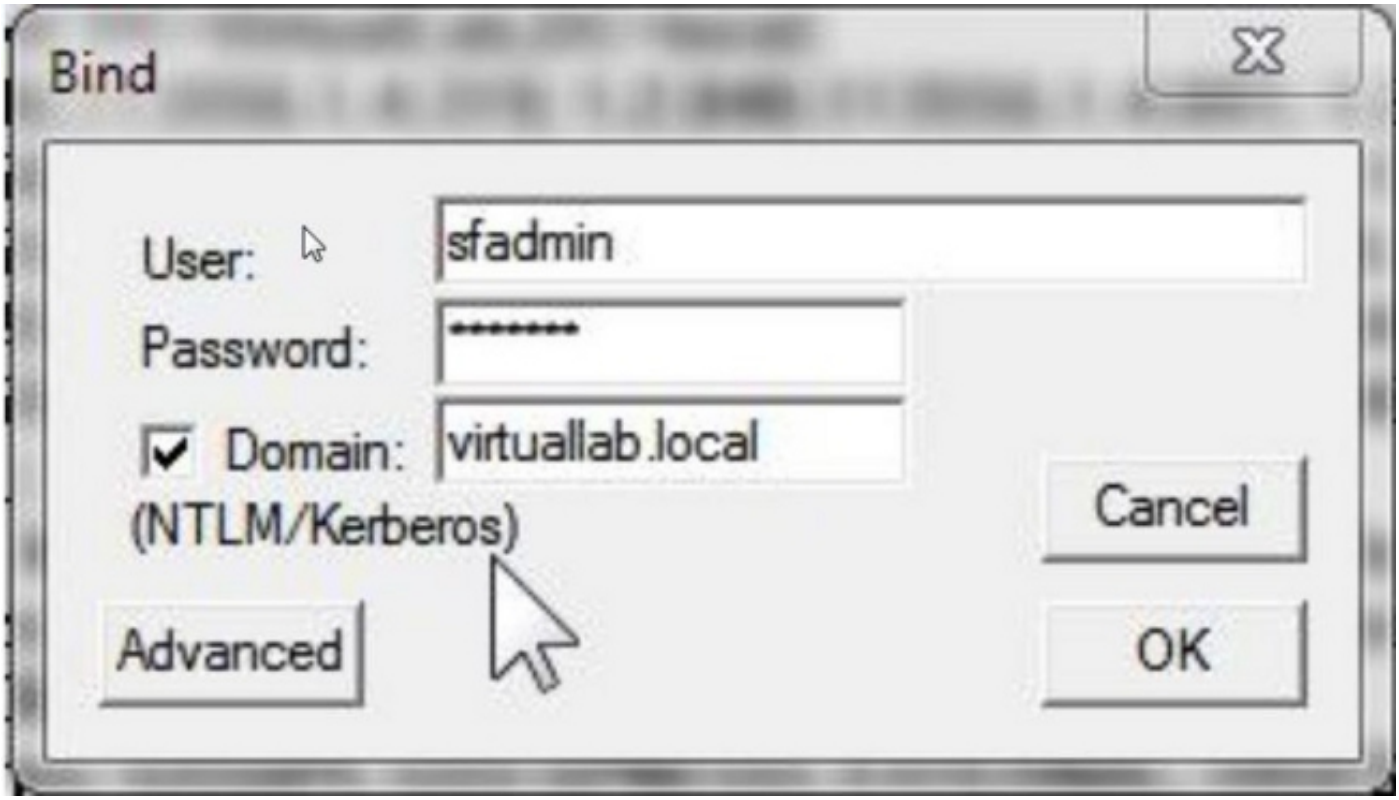
다음 스크린샷은 Windows 호스트로부터의 원격 연결을 보여줍니다.



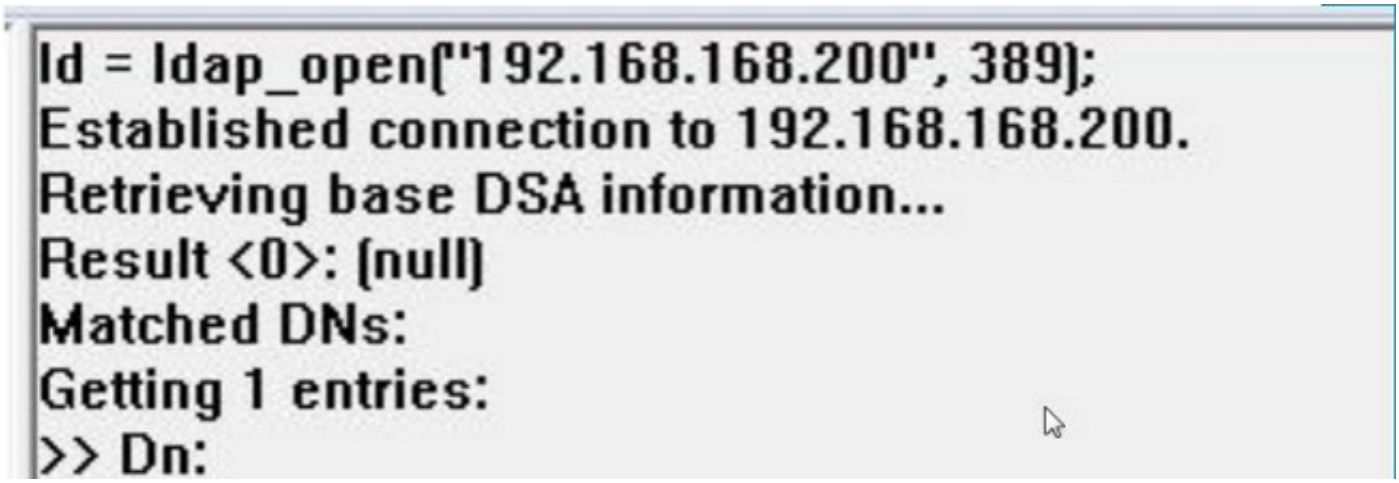
다음 스크린샷은 AD DC의 로컬 연결을 보여줍니다.



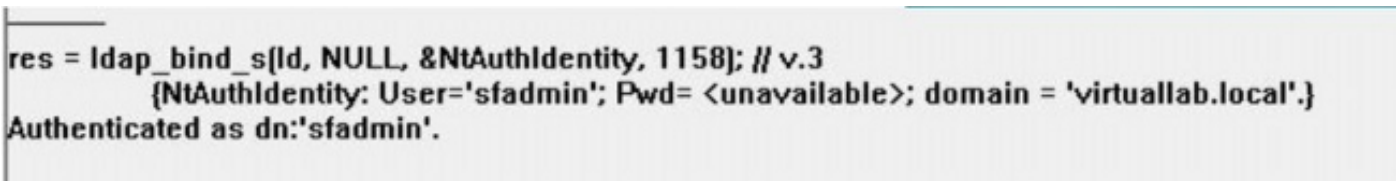
3단계. AD DC에 바인딩합니다. Connection(연결) **> Bind(바인딩)로 이동합니다**. **User**, **Password** 및 Domain을 **입력합니다. OK(확인)**를 클릭합니다.



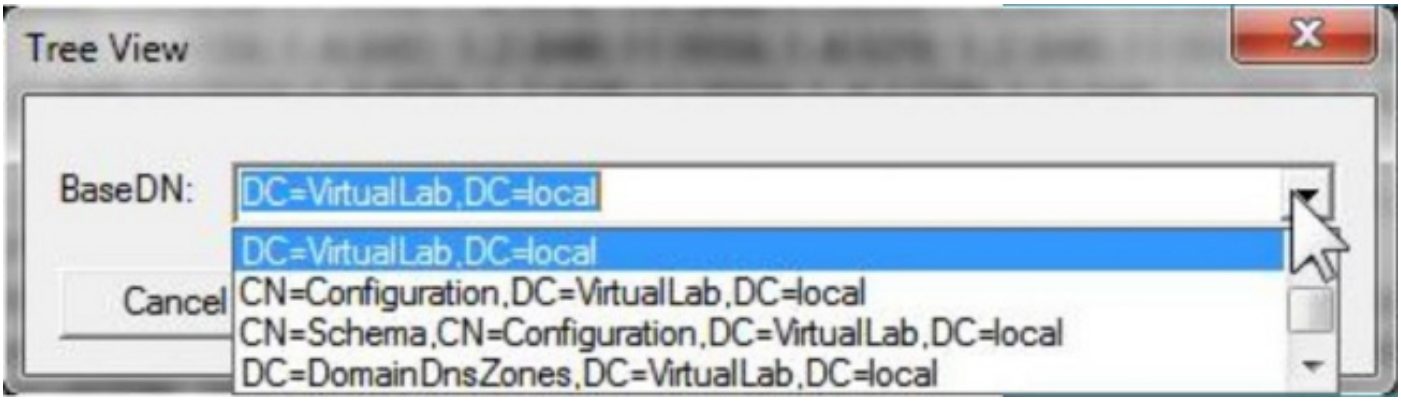
연결 시도가 성공하면 다음과 같은 출력이 표시됩니다.



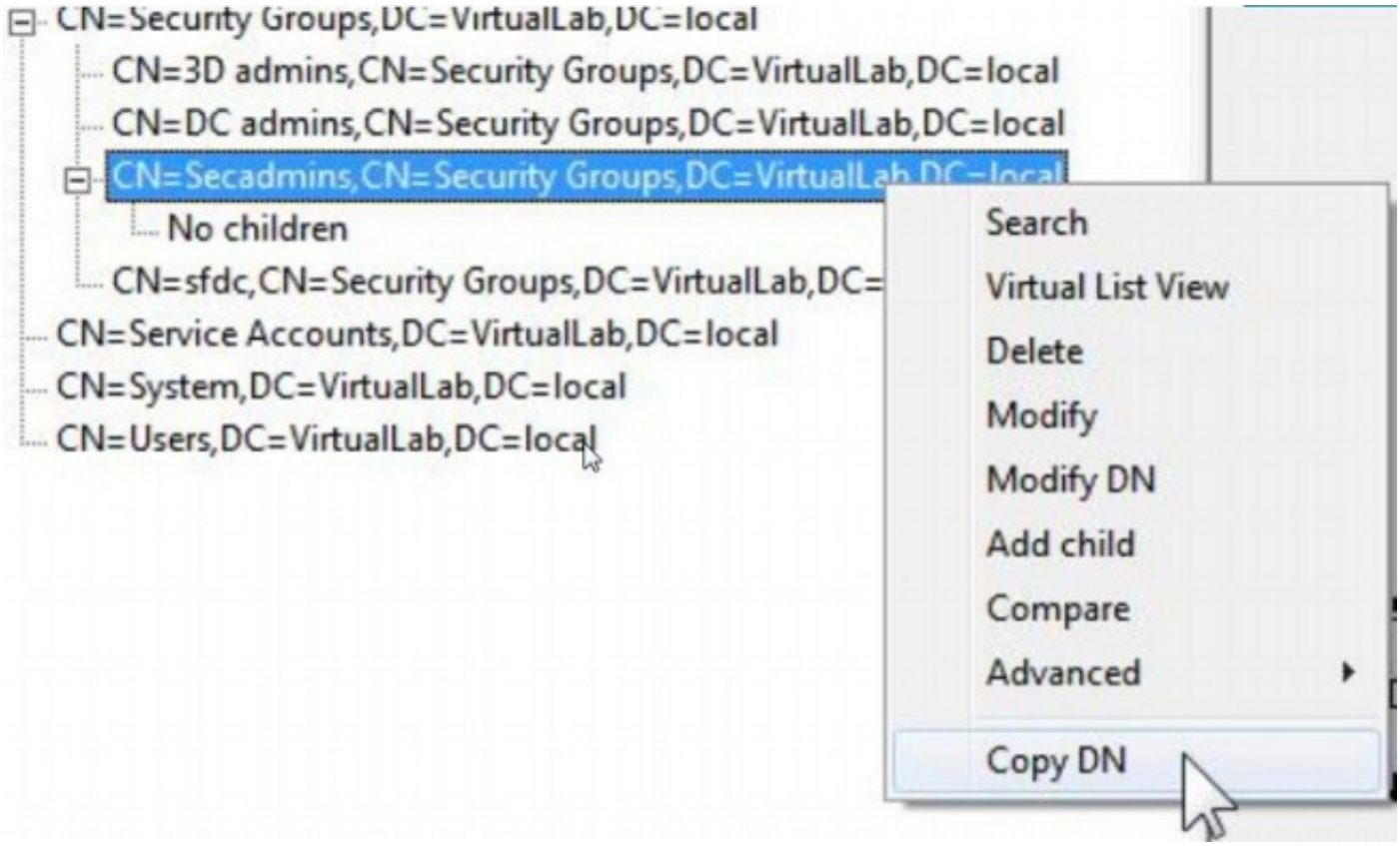
또한 ldp.exe의 왼쪽 창에 있는 출력에서는 AD DC에 성공적으로 바인딩되었음을 보여 줍니다.



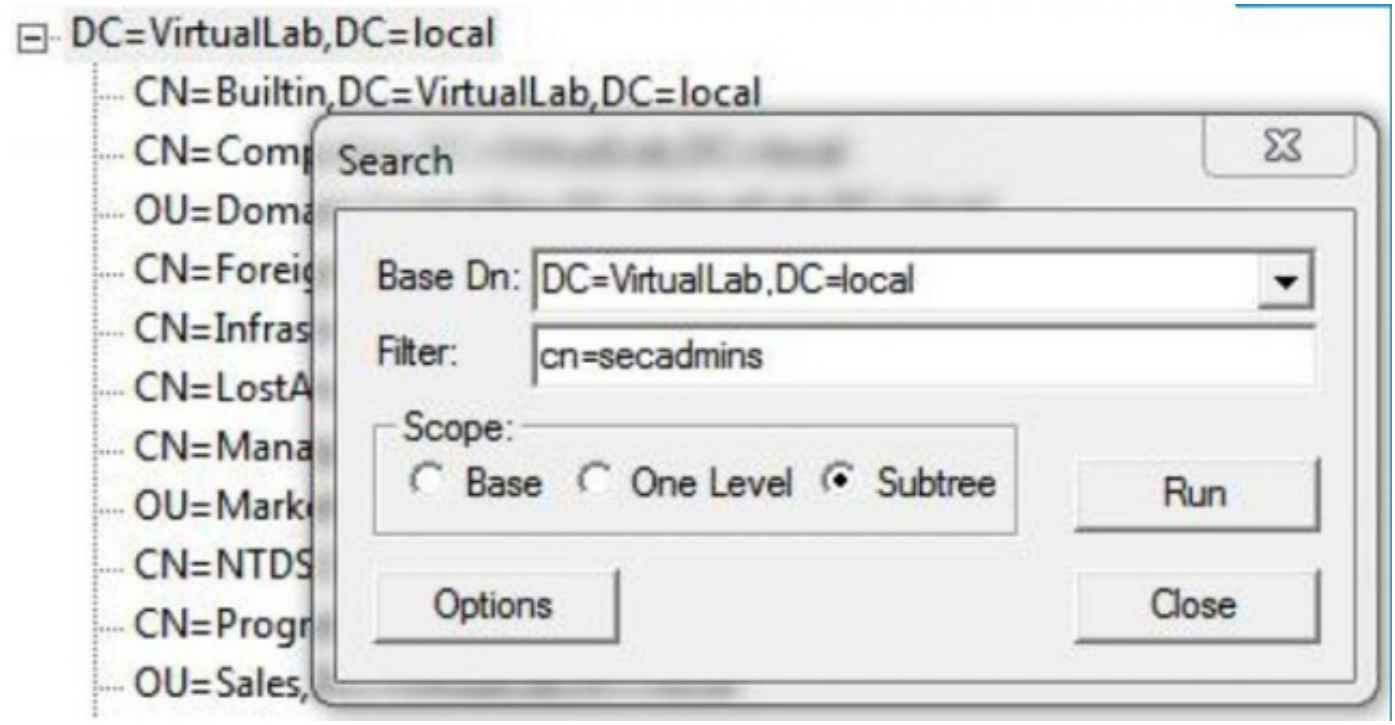
4단계: 디렉토리 트리를 찾습니다. View(**보기**) > **Tree(트리**)를 클릭하고 드롭다운 목록에서 도메인 **BaseDN**을 선택한 다음 **OK(확인**)를 클릭합니다. 이 기본 DN은 인증 객체에서 사용되는 DN입니다.



5단계: ldp.exe의 왼쪽 창에서 AD 개체를 두 번 클릭하여 컨테이너를 리프 개체 수준까지 확장하고 사용자가 속한 AD 보안 그룹으로 이동합니다. 그룹을 찾은 다음 마우스 오른쪽 버튼으로 그룹을 클릭하고 **Copy DN(DN 복사)**을 선택합니다.



그룹이 있는 OU(Organizational Unit)를 잘 모를 경우 Base DN 또는 Domain(도메인)을 마우스 오른쪽 버튼으로 클릭하고 **Search(검색)**를 선택합니다. 프롬프트가 표시되면 ***cn=<group name>을 필터*** 로 입력하고 Subtree를 **범위**로 **입력합니다**. 결과를 얻은 후 그룹의 DN 특성을 복사할 수 있습니다. **cn=*admin***과 같은 와일드카드 검색을 수행할 수도 있습니다.




```
***Searching...
ldap_search_s(ld, "DC=VirtualLab,DC=local", 2, "cn=secadmins", attrList, 0, &msg)
Result <0>: (null)
Matched DNs:
Getting 1 entries:
>> Dn: CN=Secadmins,CN=Security Groups,DC=VirtualLab,DC=local
        2> objectClass: top; group;
        1> cn: Secadmins;
        1> distinguishedName: CN=Secadmins,CN=Security Groups,DC=VirtualLab,DC=local;
        1> name: Secadmins;
        1> canonicalName: VirtualLab.local/Security Groups/Secadmins;
```

인증 객체의 기본 필터는 다음과 같아야 합니다.

- 단일 그룹:

  기본 필터: (memberOf=<Security_group_DN>)

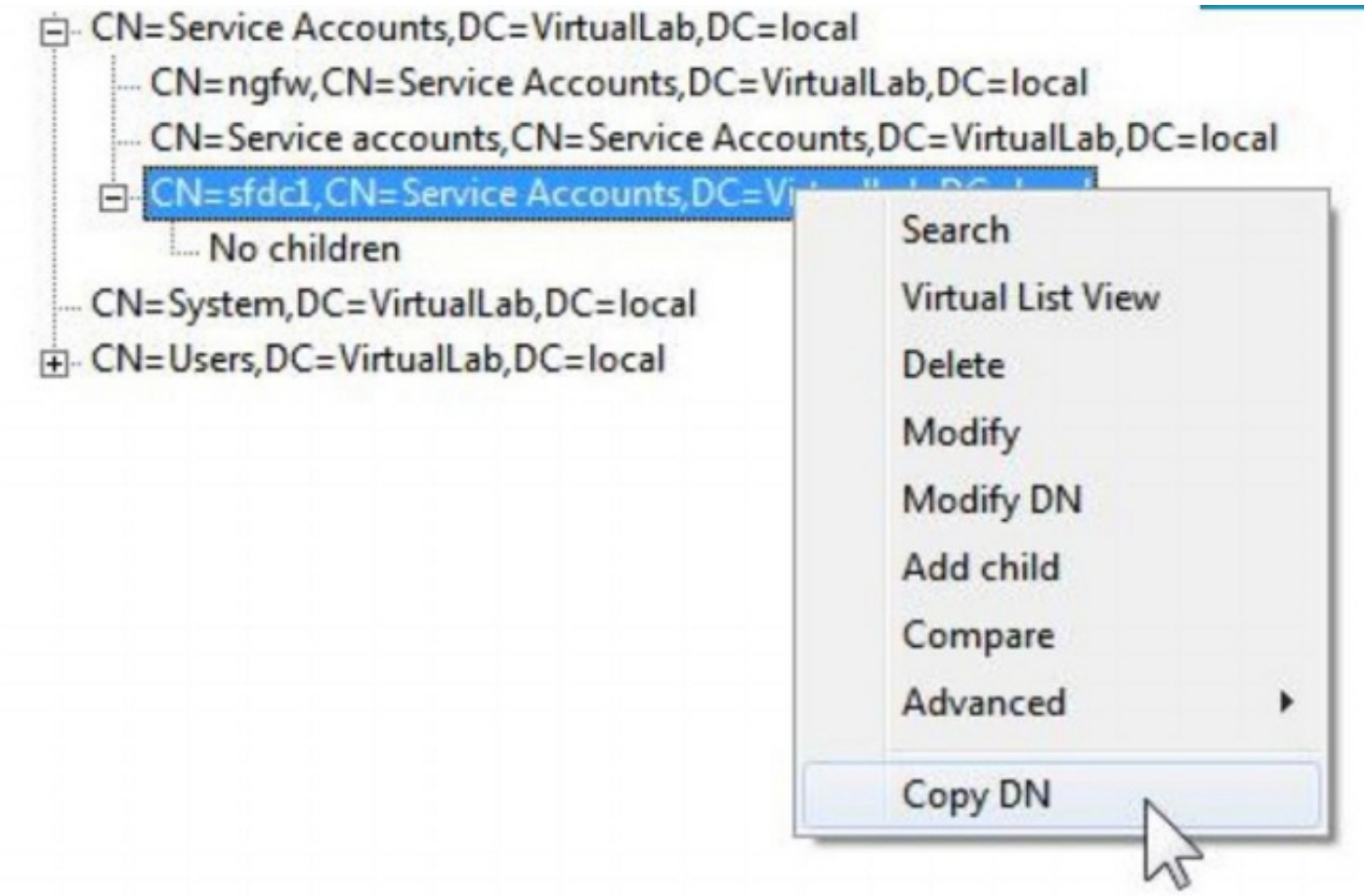
- 여러 그룹:

  기본 필터:
  (|(memberOf=<group1_DN>)(memberOf=<group2_DN>)(memberOf=<groupN_DN))

다음 예에서는 AD 사용자에게 기본 필터와 일치하는 memberOf 특성이 있습니다. memberOf 특성 앞의 숫자는 사용자가 구성원으로 속한 그룹의 수를 나타냅니다. 사용자가 보안 그룹 secadmins의 구성원만 있습니다.

```
1> memberOf: CN=Secadmins,CN=Security Groups,DC=VirtualLab,DC=local;
```

6단계: Authentication Object(인증 개체)에서 가장 계정으로 사용할 사용자 계정으로 이동하고 마우스 오른쪽 버튼으로 Copy DN(**DN 복사**)할 사용자 계정을 클릭합니다.



인증 개체의 **사용자 이름**에 이 DN을 사용합니다. 예를 들면 다음과 같습니다.

사용자 이름: CN=sfdc1,CN=서비스 계정,DC=VirtualLab,DC=로컬

그룹 검색과 마찬가지로 CN 또는 name=sfdc1과 같은 특정 속성을 가진 사용자를 검색할 수도 있습니다.