Identificeer actieve Directory LDAP Objectkenmerken voor verificatie Objectconfiguratie

Inhoud

Inleiding

Dit document beschrijft hoe u de eigenschappen van de Actief Map (AD) LDAP kunt identificeren om verificatie object te configureren op de manier waarop u de externe verificatie kunt controleren.

Identificeer LDAP-doelkenmerken

Alvorens een verificatieobject op een FireSIGHT Management Center voor externe authenticatie te configureren, is het nodig de AD LDAP-eigenschappen van gebruikers en beveiligingsgroepen te identificeren zodat de externe verificatie naar behoren kan functioneren. Om dit te doen, kunnen we gebruik maken van een door Microsoft opgegeven LDAP-client, Ldp.exe of een browser van een derde partij, die u aan de achterzijde van de gebruiker kunt aanbieden. In dit artikel zullen we ldp.exe gebruiken om op lokaal niveau of op afstand de AD server aan te sluiten, te binden en door te bladeren en de eigenschappen te identificeren.

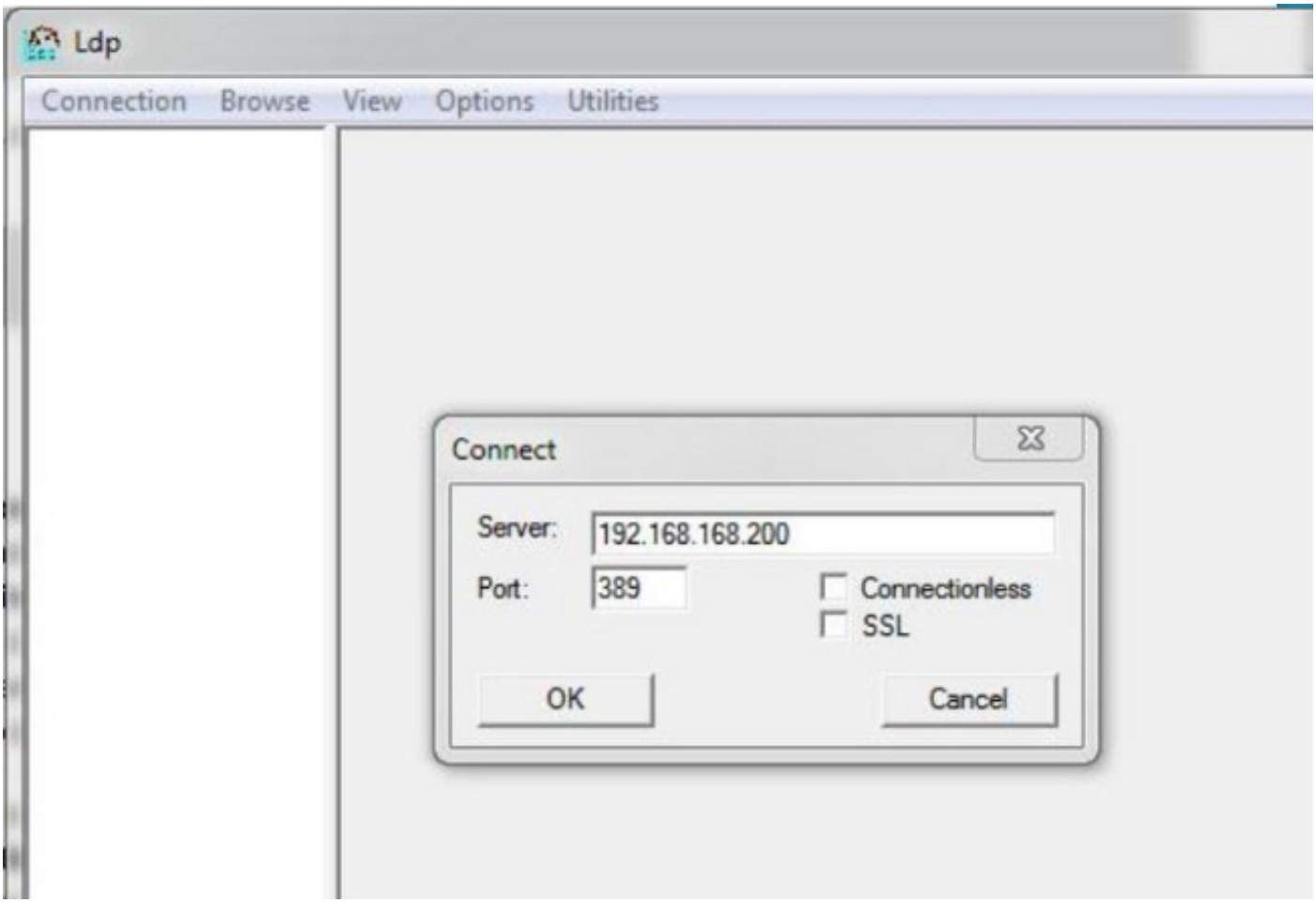
Stap 1: Start ldp.exe-toepassing. Ga naar het menu **Start** en klik op **Uitvoeren**. Type **ldp.exe** en druk op de knop **OK**.

> Opmerking: Op Windows Server 2008 wordt ldp.exe standaard geïnstalleerd. Voor Windows Server 2003 of voor een externe verbinding van Windows-clientcomputer, kunt u het bestand support.cab of support.msi downloaden van de Microsoft-site. Pak het .cab-bestand uit of installeer het .msi-bestand en voer ldp.exe uit.

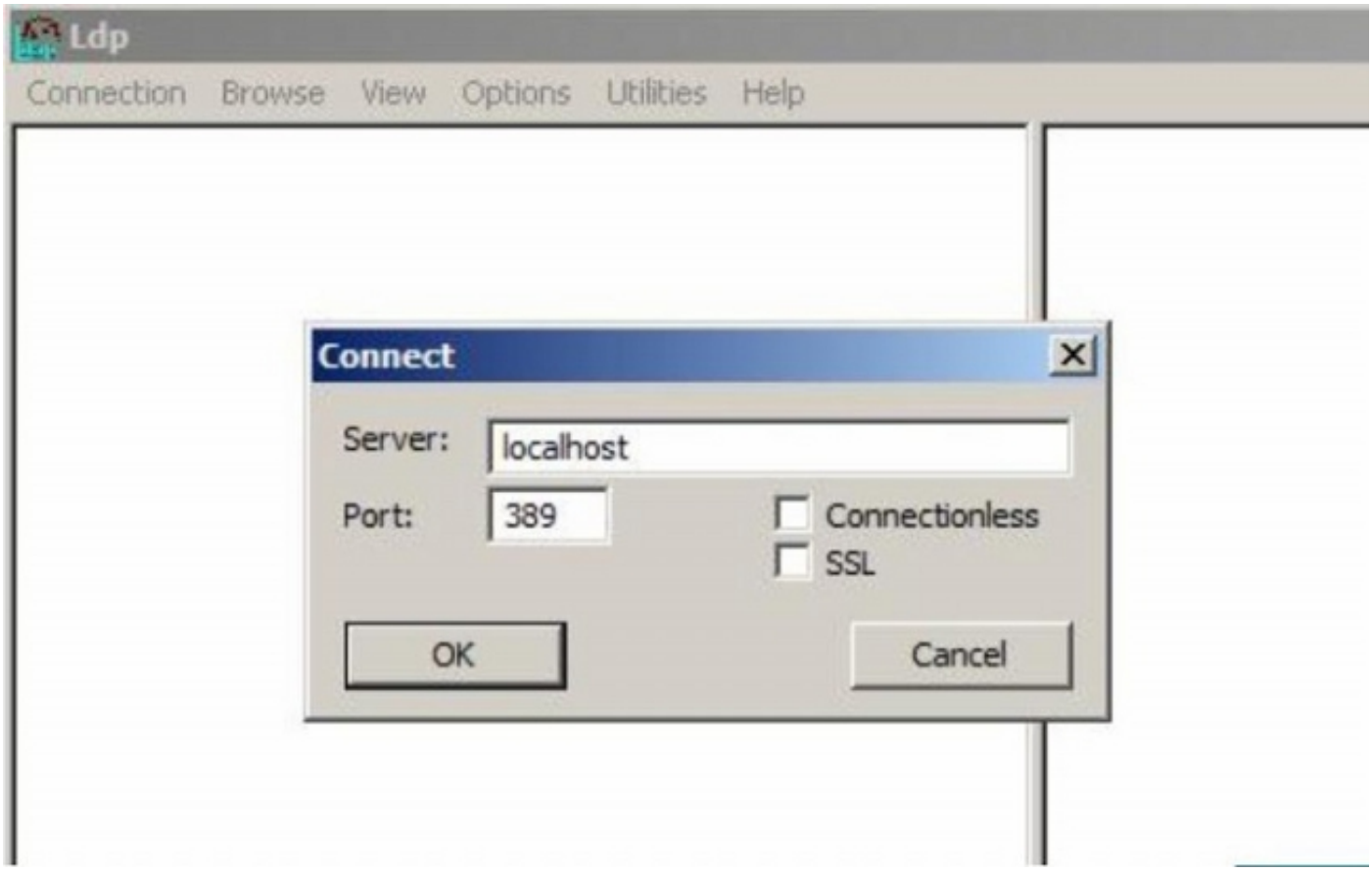
Stap 2: Connect met de server. Selecteer **Connection** en klik op **Connect**.

- Om aan te sluiten op een AD Domain Controller (DC) van een lokale computer, voer het hostname of IP adres van de AD server in.
- Om lokaal aan een AD DC te verbinden, voer localhost in als **server**.

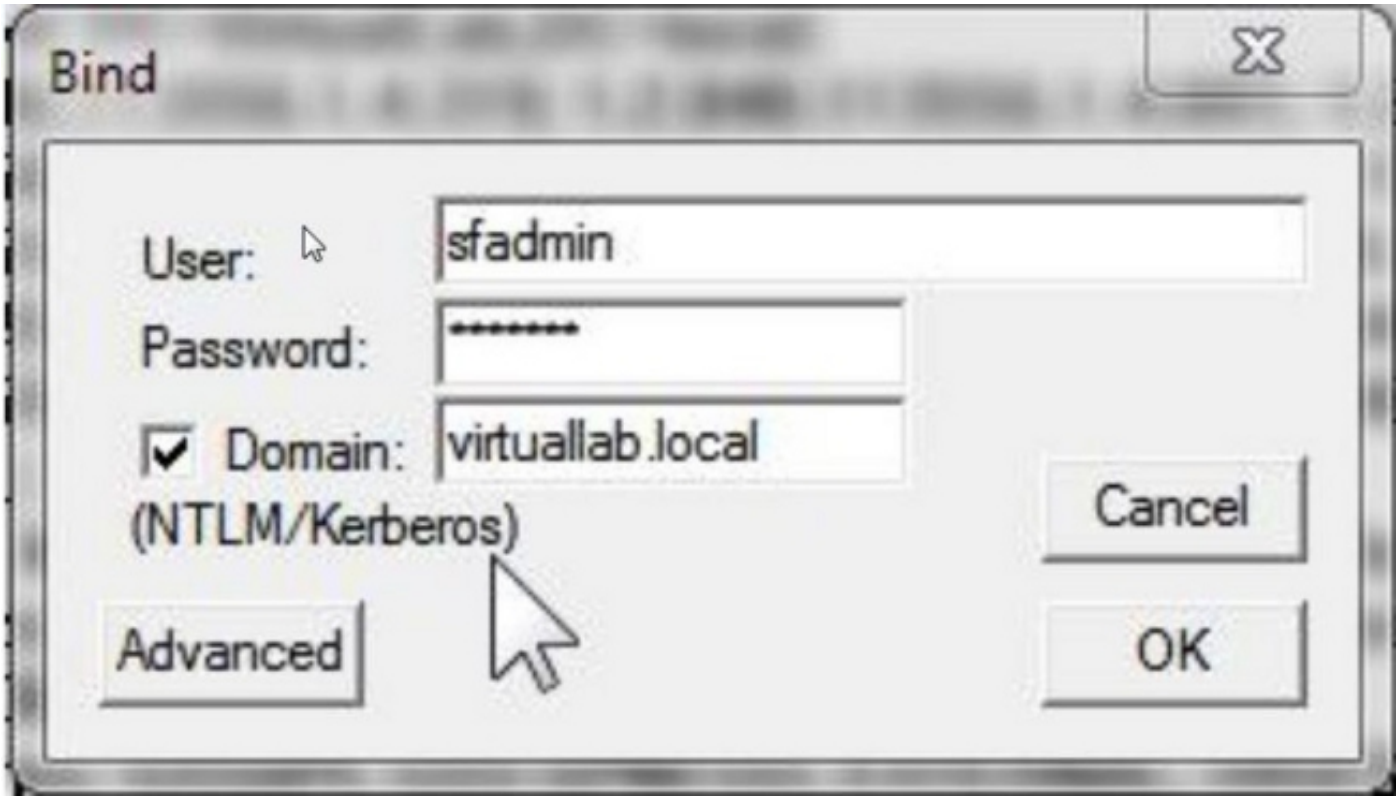
Het volgende screenshot toont een externe verbinding van een Windows-host:



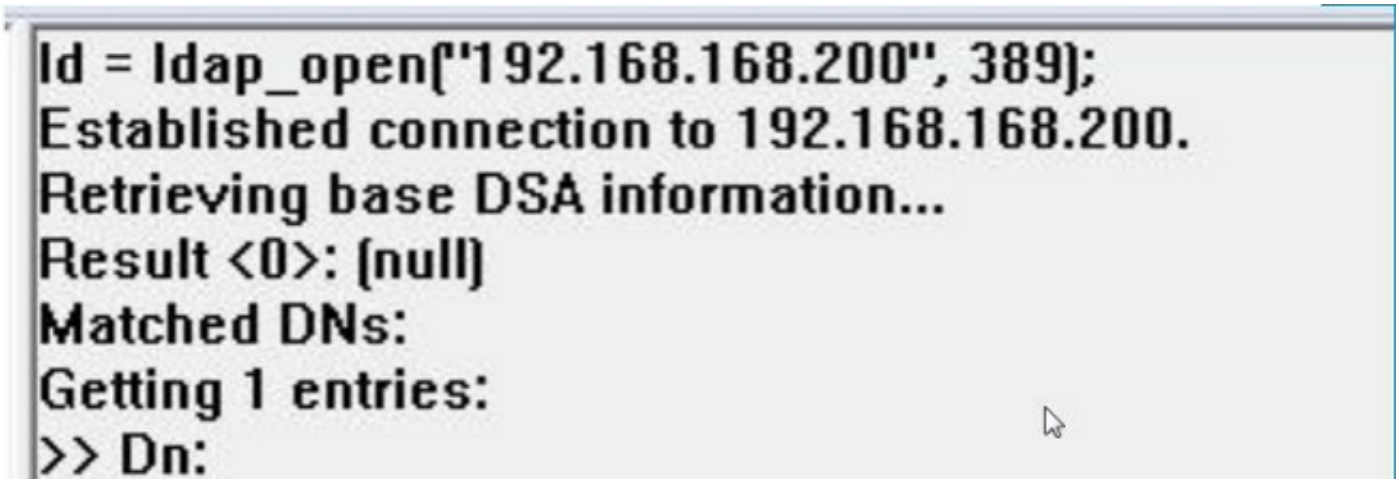
De volgende screenshot toont een lokale verbinding op een AD DC:



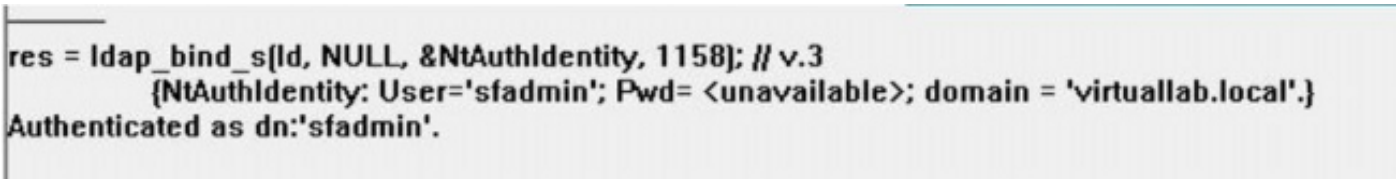
Stap 3. Bind naar de AD DC. Ga naar **verbinding > Bind**. Voer de **gebruiker**, het **wachtwoord** en het **domein in.** Klik op **OK**.



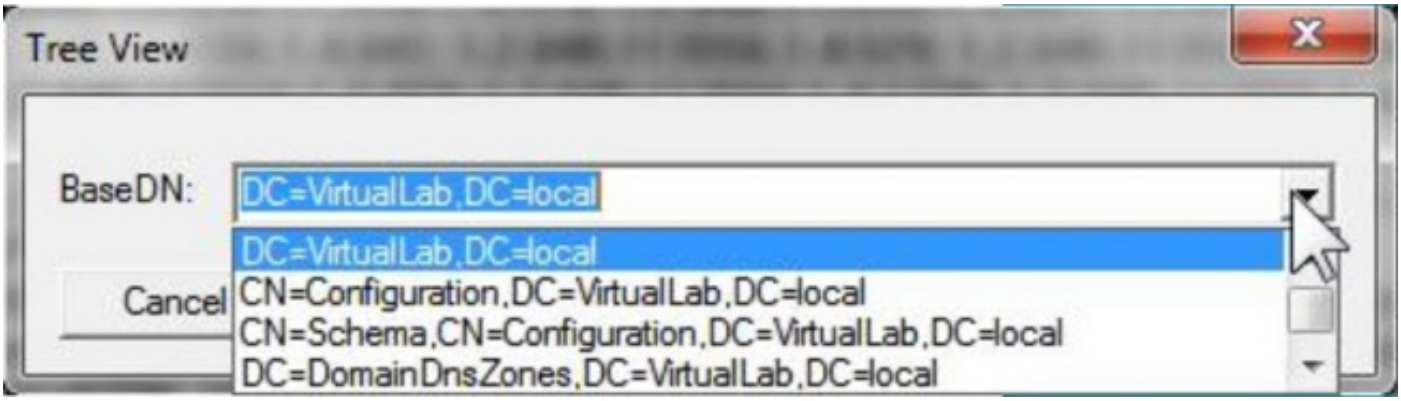
Wanneer een poging tot aansluiting succesvol is, ziet u een uitvoer zoals hieronder:



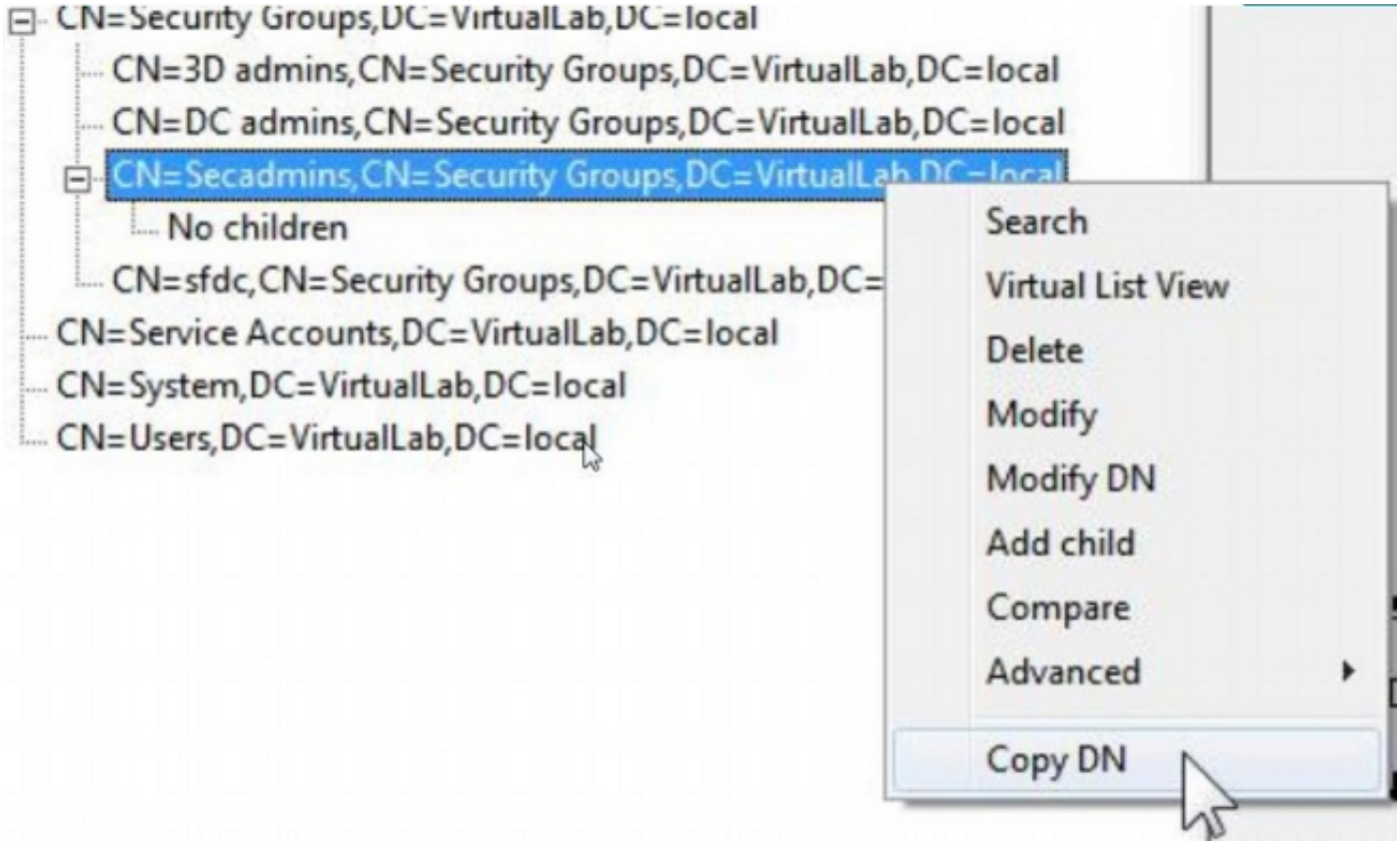
Tevens zal het resultaat in het linker deelvenster van ldp.exe succesvolle bindingen aan de AD DC laten zien.



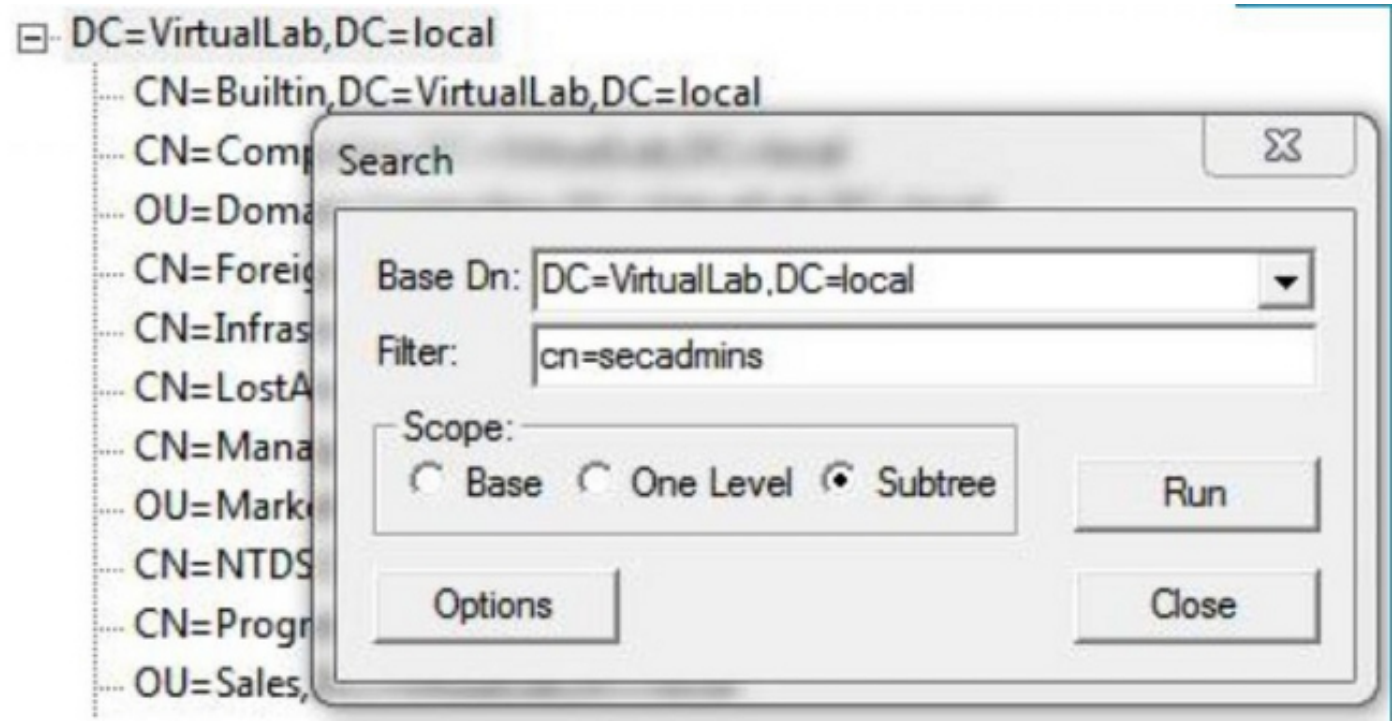
Stap 4: Bladeren in de map. Klik op **Beeld > Tree**, selecteer de domein**BaseDN** uit de vervolgkeuzelijst en klik op **OK**. Deze Base DN is de DNA die op het object van verificatie wordt gebruikt.



Stap 5: In het linker venster van ldp.exe, dubbelklik op de AD voorwerpen om de containers uit te vouwen tot het niveau van bladvoorwerpen en navigeer naar de AD Security Group waarvan de gebruikers lid zijn. Zodra u de groep vindt, klikt u met de rechtermuisknop op de groep en vervolgens selecteert u **DN kopiëren**.



Als u niet zeker weet in welke Organisatorische Eenheid (OU) de groep is gelokaliseerd, klik met de rechtermuisknop op Base DN of Domain en selecteer **Zoeken**. Voer desgevraagd **cn=*<groepsnaam>in*** als filter en **Subboom** als **bereik**. Zodra je het resultaat hebt, kun je dan de DNA-eigenschap van de groep kopiëren. Het is ook mogelijk om een wildkaartzoekactie uit te voeren zoals **cn=*admin***.




```
***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;
```

Het basisfilter in de verificatieobject moet als volgt zijn:

- Enkelvoudige groep:

  Basisfilter: (lid van=<Security_group_DN>)

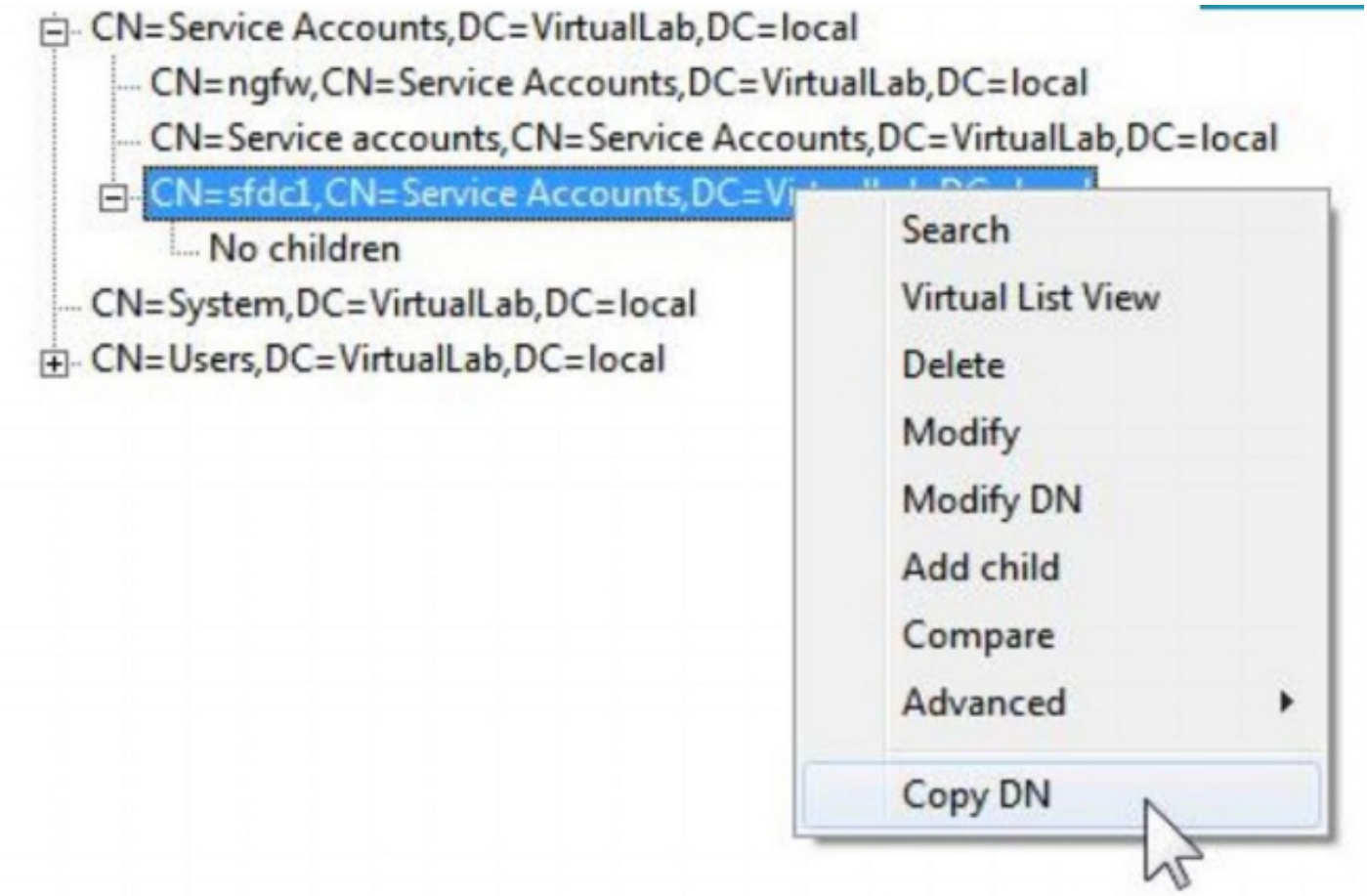
- Meervoudige groepen:

  Basisfilter: (|(lidOf=<group1_DN>)(lidOf=<group2_DN>)(lidOf=<groupN_DN))

In het volgende voorbeeld, let op dat AD gebruikers lidOf hebben dat het basisfilter aanpast. Het nummer dat aan lidOf eigenschap voorafgaat geeft het aantal groepen aan waarvan de gebruiker lid is. De gebruiker is slechts lid van één beveiligingsgroep, seconden.

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

Stap 6: Navigeer naar de gebruikersrekeningen die u als imitatie-account in het object Verificatie wilt gebruiken, en klik met de rechtermuisknop op de gebruikersaccount naar **DN-kopie**.



Gebruik deze DNA voor **gebruikersnaam** in het verificatieobject. Bijvoorbeeld:

Gebruikersnaam: CN=sfdc1,CN=Service Account,DC=VirtualLab,DC=Local

Overeenkomstig met groepszoekingen is het ook mogelijk om een gebruiker te doorzoeken met GN of een specifieke eigenschap zoals name=sfdc1.