Identifizieren von Active Directory-LDAP-Objektattributen für die Konfiguration von Authentifizierungsobjekten

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Sie Active Directory (AD)-LDAP-Objektattribute identifizieren, um das Authentifizierungsobjekt auf dem für die externe Authentifizierung zu konfigurieren.

Identifizieren von LDAP-Objektattributen

Bevor ein Authentifizierungsobjekt in einem FireSIGHT Management Center für die externe Authentifizierung konfiguriert wird, muss die AD-LDAP-Attribute von Benutzern und Sicherheitsgruppen identifiziert werden, damit die externe Authentifizierung wie vorgesehen funktioniert. Dazu können wir den von Microsoft bereitgestellten GUI-basierten LDAP-Client, Ldp.exe oder einen beliebigen LDAP-Browser eines Drittanbieters verwenden. In diesem Artikel verwenden wir ldp.exe, um lokal oder remote eine Verbindung herzustellen, eine Bindung herzustellen und den AD-Server zu durchsuchen und die Attribute zu identifizieren.

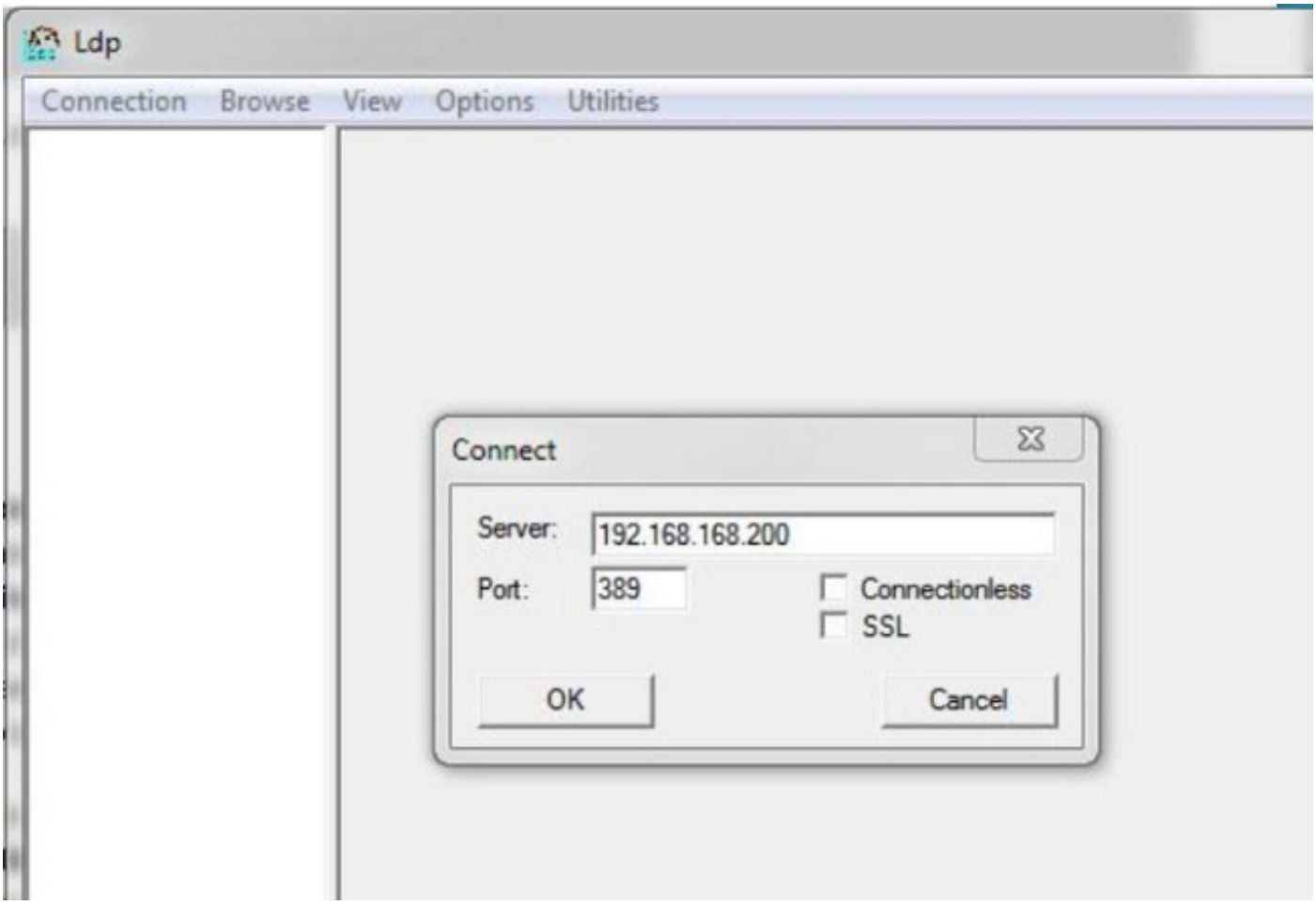
Schritt 1: Starten Sie die Anwendung ldp.exe. Öffnen Sie das **Startmenü**, und klicken Sie auf **Ausführen**. Geben Sie **ldp.exe ein**, und drücken Sie die Schaltfläche **OK**.

> **Hinweis**: Auf Windows Server 2008 ist ldp.exe standardmäßig installiert. Laden Sie für Windows Server 2003 oder für Remote-Verbindungen vom Windows-Clientcomputer die Datei support.cab oder support.msi von der Microsoft-Website herunter. Extrahieren Sie die Datei .cab, oder installieren Sie die Datei .msi, und führen Sie ldp.exe aus.

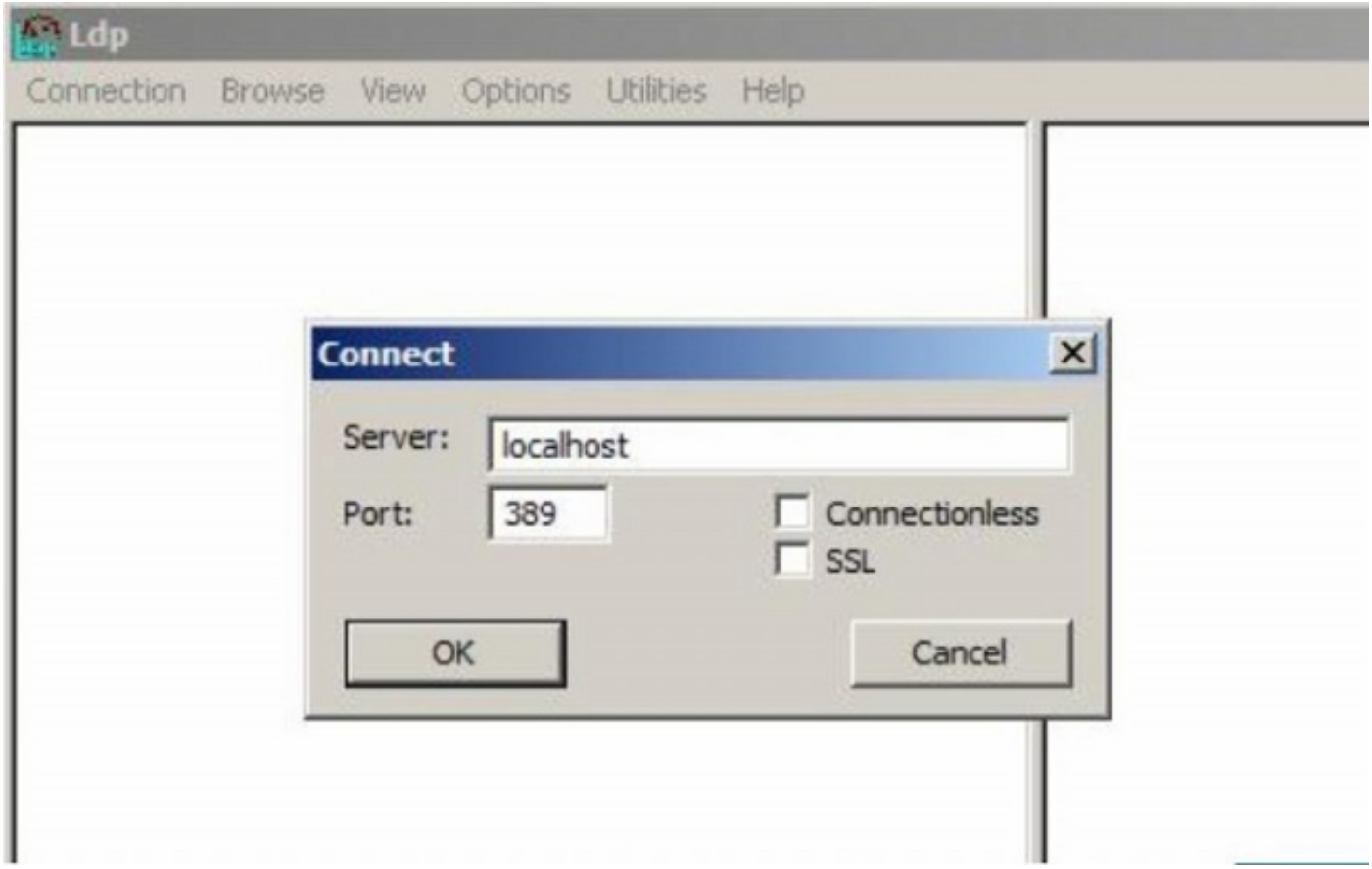
Schritt 2: Stellen Sie eine Verbindung zum Server her. Wählen Sie **Verbindung** aus, und klicken Sie auf **Verbinden**.

- Um über einen lokalen Computer eine Verbindung zu einem AD Domain Controller (DC) herzustellen, geben Sie den Hostnamen oder die IP-Adresse des AD-Servers ein.
- Um eine lokale Verbindung zu einem AD-Rechenzentrum herzustellen, geben Sie localhost als **Server ein**.

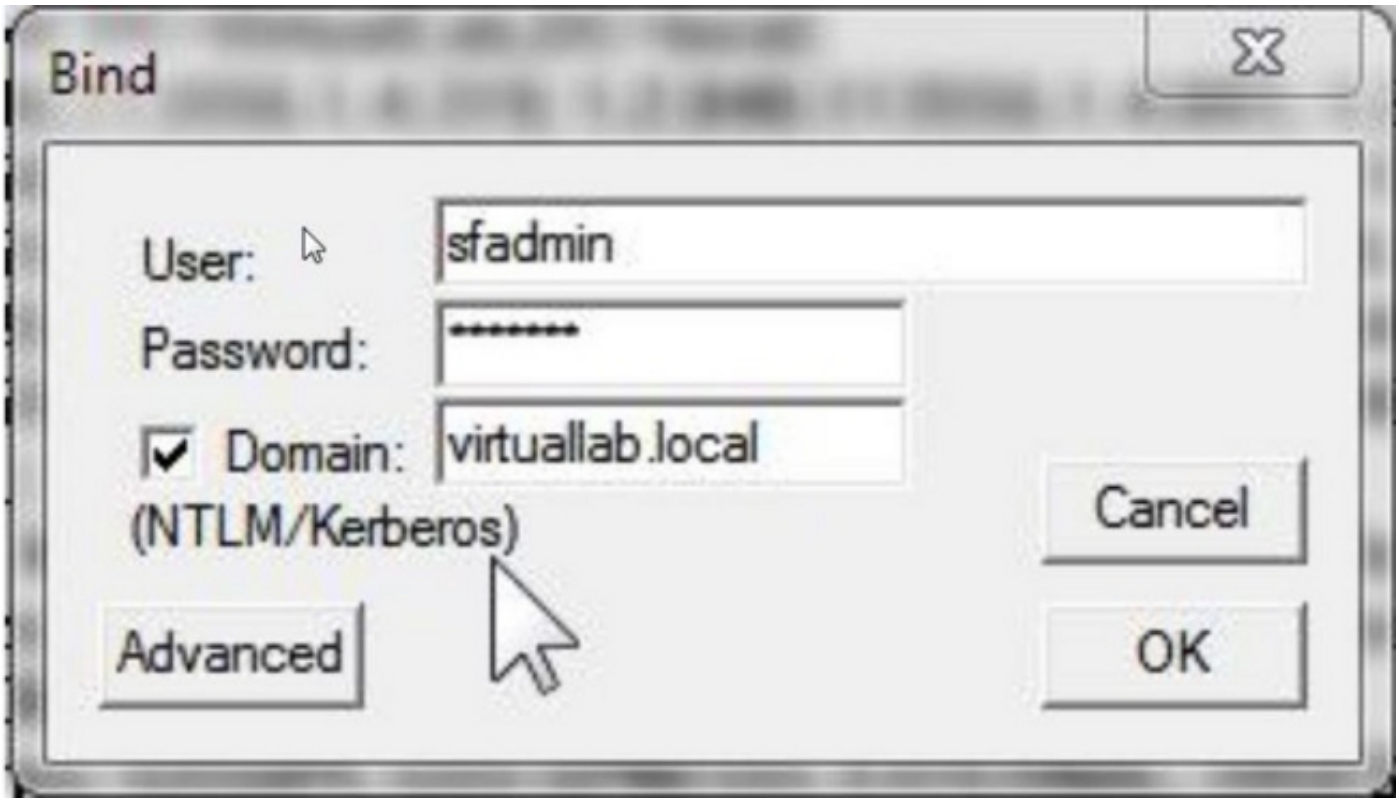
Der folgende Screenshot zeigt die Remoteverbindung von einem Windows-Host aus:



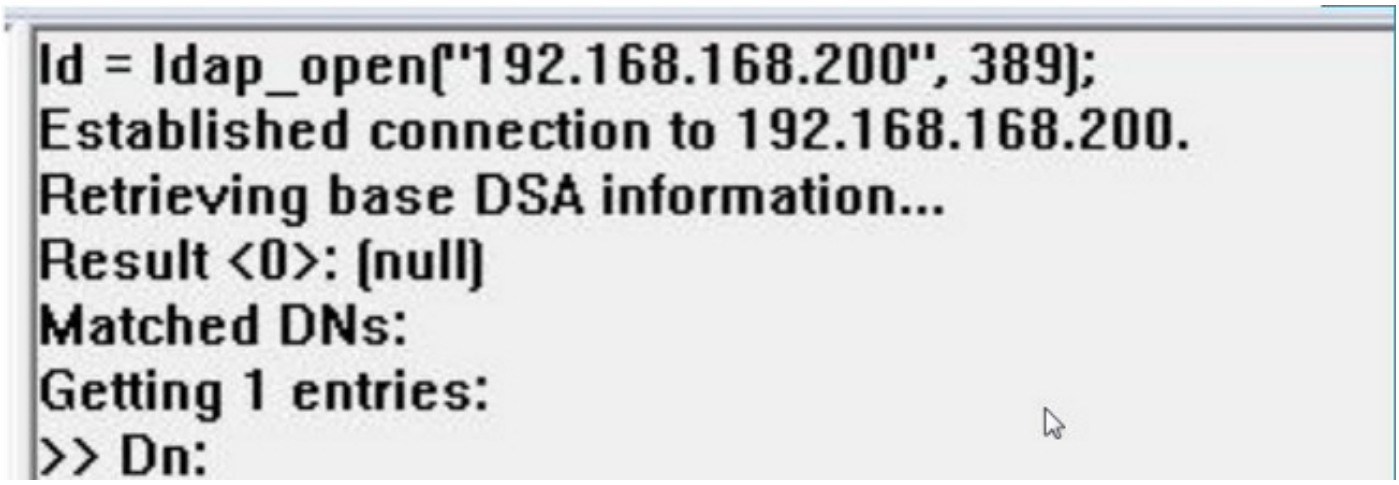
Der folgende Screenshot zeigt die lokale Verbindung in einem AD-Rechenzentrum:



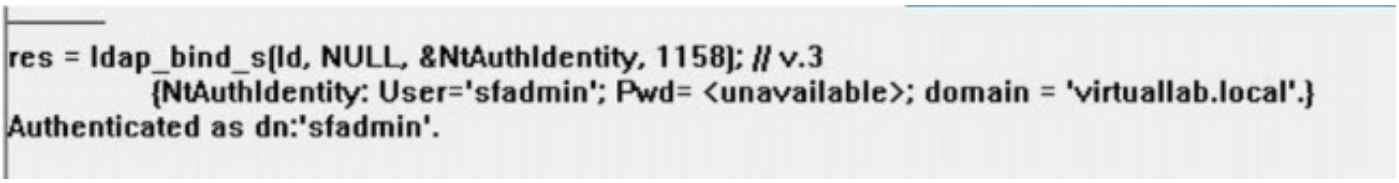
Schritt 3: An AD DC binden. Gehen Sie zu **Verbindung > Bind**. Geben Sie **Benutzer**, **Kennwort** und **Domäne ein.** Klicken Sie auf **OK**.



Wenn ein Verbindungsversuch erfolgreich ist, wird eine Ausgabe wie folgt angezeigt:

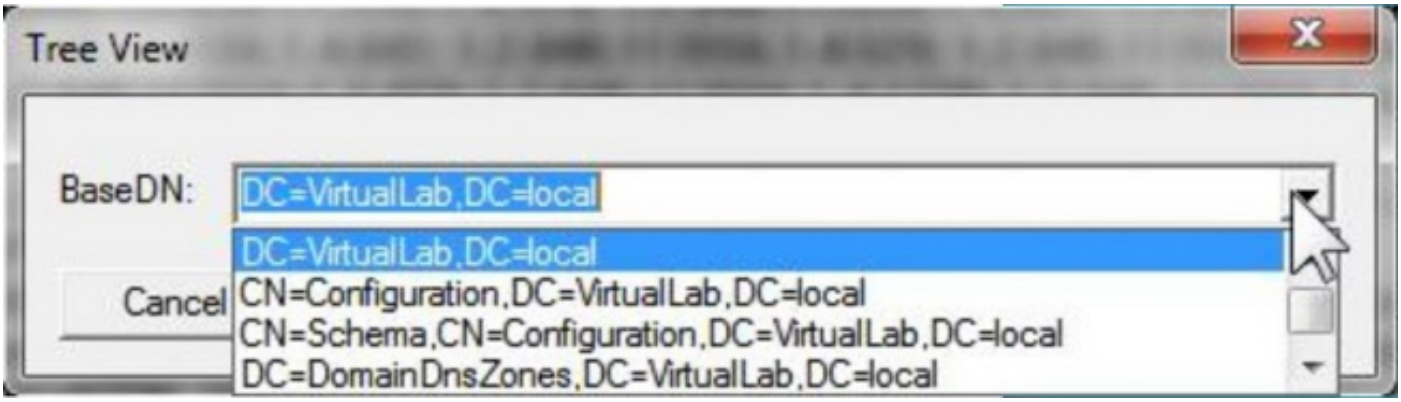


Außerdem zeigt die Ausgabe im linken Bereich von ldp.exe eine erfolgreiche Bindung an das AD-DC.

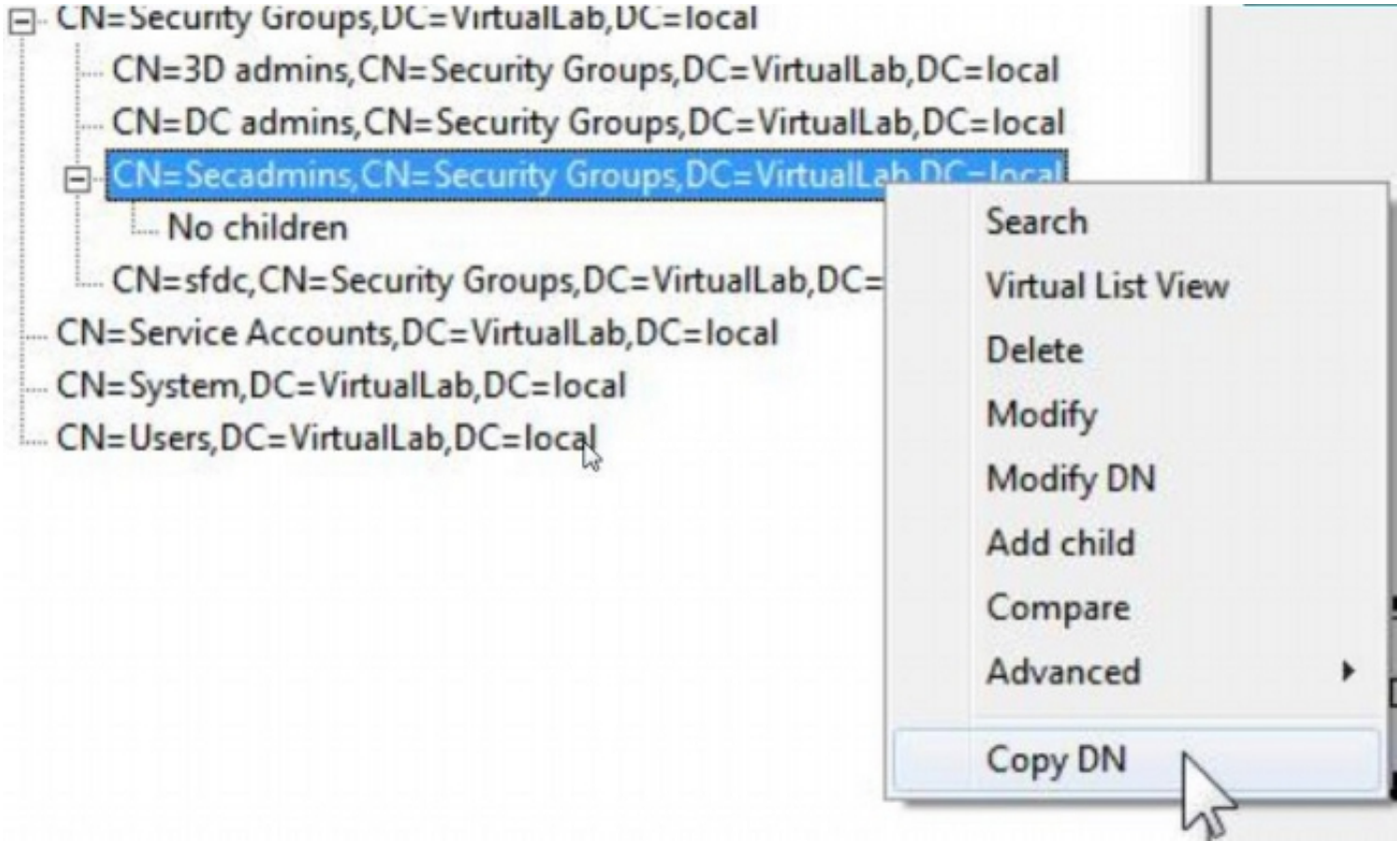


Schritt 4: Durchsuchen Sie die Verzeichnisstruktur. Klicken Sie auf **Ansicht > Struktur**, wählen Sie die Domäne **BaseDN** aus der Dropdown-Liste aus, und klicken Sie auf **OK**. Diese Basis-DN ist die

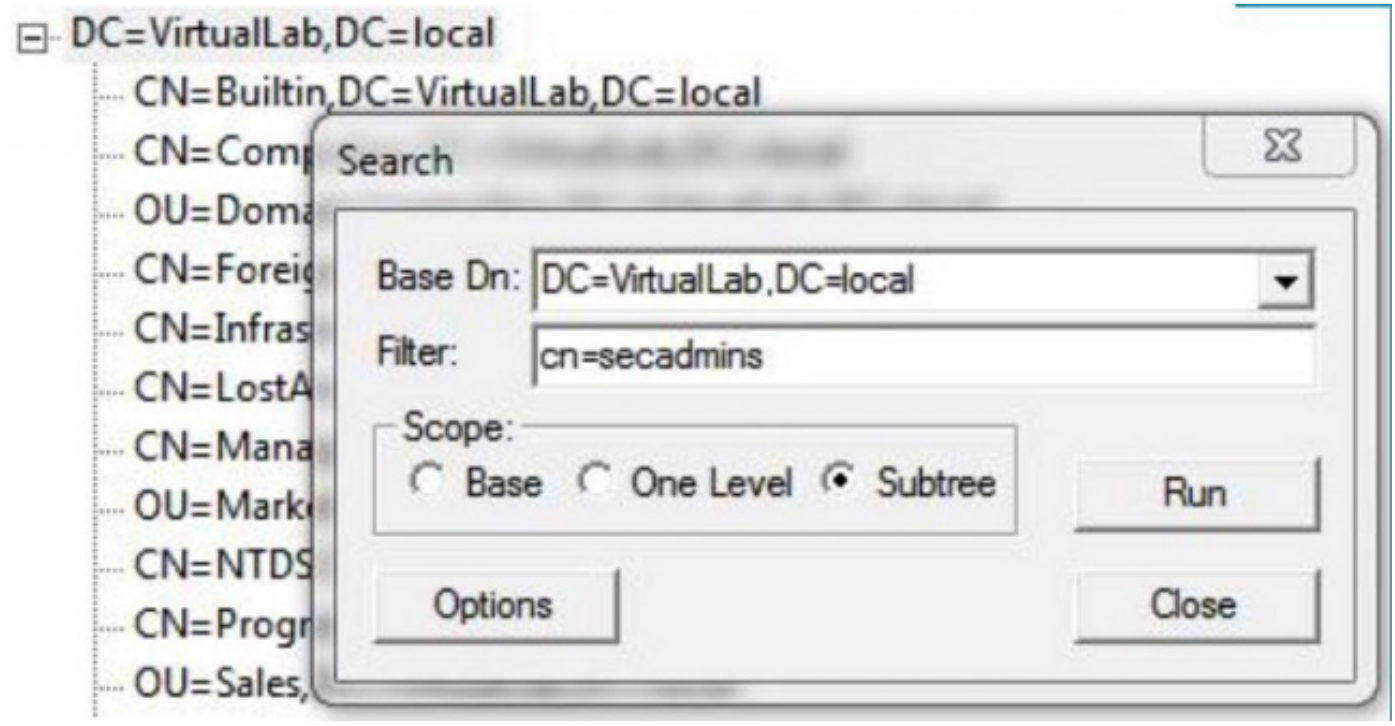
DN, die für das Authentifizierungsobjekt verwendet wird.



Schritt 5: Doppelklicken Sie im linken Bereich von ldp.exe auf die AD-Objekte, um die Container bis auf die Ebene der Leaf-Objekte zu erweitern, und navigieren Sie zur AD-Sicherheitsgruppe, der die Benutzer angehören. Sobald Sie die Gruppe gefunden haben, klicken Sie mit der rechten Maustaste auf die Gruppe, und wählen Sie **DN kopieren aus**.



Wenn Sie nicht sicher sind, in welcher Organisationseinheit (OU) sich die Gruppe befindet, klicken Sie mit der rechten Maustaste auf die Basis-DN oder -Domäne, und wählen Sie **Suchen aus**. Geben Sie bei Aufforderung **cn=*<Gruppenname>*** als Filter und **Subtree** als **Bereich ein**. Nachdem Sie das Ergebnis erhalten haben, können Sie das DN-Attribut der Gruppe kopieren. Es ist auch möglich, eine Platzhaltersuche wie **cn=*admin*** durchzuführen.




```
***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;
```

Der Basisfilter im Authentifizierungsobjekt sollte wie folgt lauten:

- Eine Gruppe:

  Basisfilter: (memberOf=<Security_group_DN>)

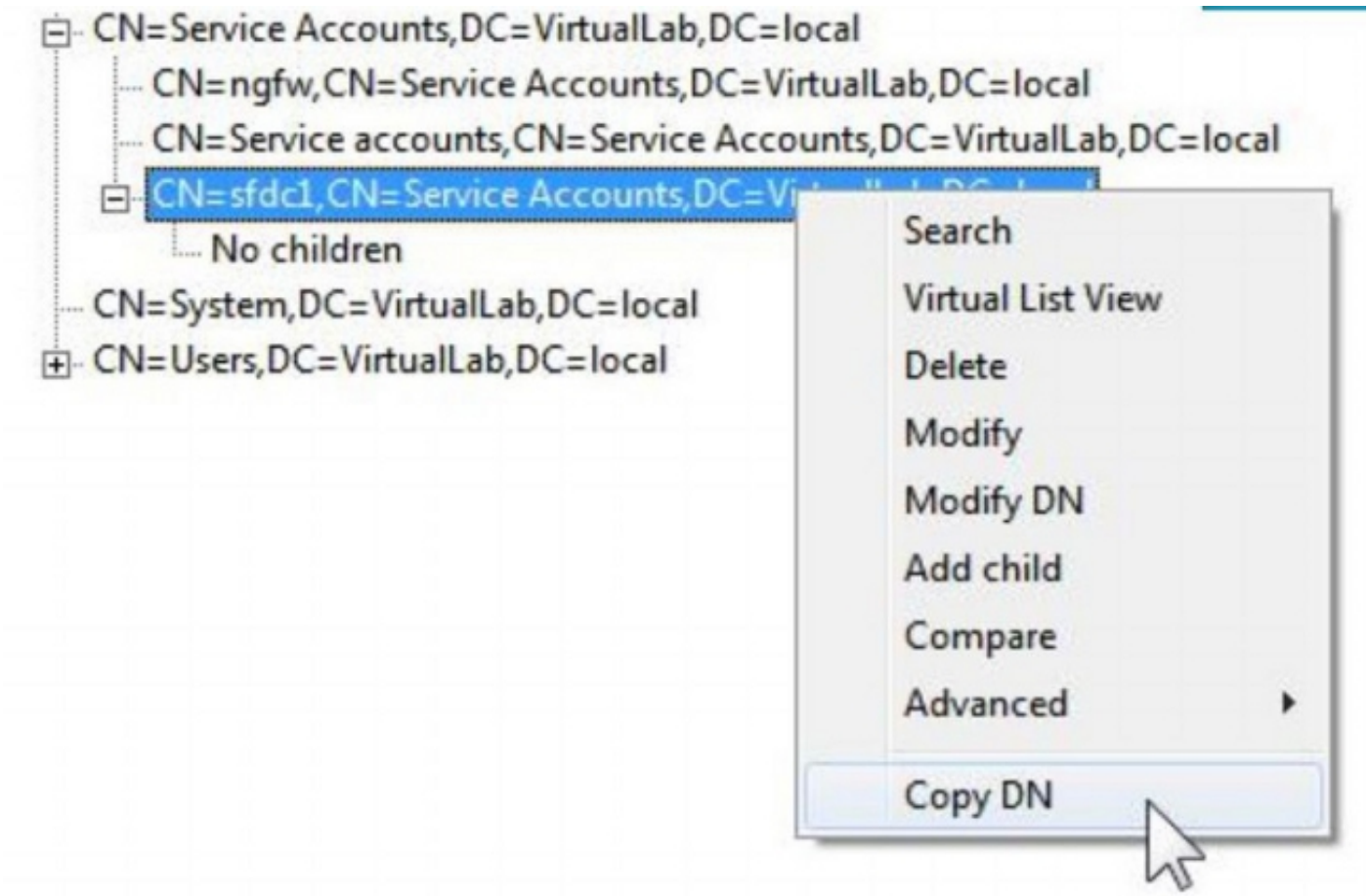
- Mehrere Gruppen:

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

Beachten Sie im folgenden Beispiel, dass AD-Benutzer das memberOf-Attribut haben, das dem Base Filter entspricht. Die Nummer vor dem memberOf-Attribut gibt die Anzahl der Gruppen an, der der Benutzer angehört. Der Benutzer ist Mitglied einer einzigen Sicherheitsgruppe, Secadmins.

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

Schritt 6: Navigieren Sie zu den Benutzerkonten, die Sie im Authentication Object (Authentifizierungsobjekt) als Identitätskonto verwenden möchten, und klicken Sie mit der rechten Maustaste auf das Benutzerkonto, um **DN** zu **kopieren**.



Verwenden Sie diesen DN für den **Benutzernamen** im Authentifizierungsobjekt. Beispiel:

Benutzername: CN=sfdc1,CN=Service Accounts,DC=VirtualLab,DC=local

Ähnlich wie bei der Gruppensuche können Sie auch einen Benutzer mit einem CN oder einem bestimmten Attribut wie name=sfdc1 durchsuchen.