確定身份驗證對象配置的Active Directory LDAP對象屬性

目錄

簡介

本文檔介紹如何標識Active Directory(AD)LDAP對象屬性以在上配置身份驗證對象以進行外部身份驗證。

標識LDAP對象屬性

在FireSIGHT管理中心上配置身份驗證對象以進行外部身份驗證之前，需要標識使用者和安全組的AD LDAP屬性才能使外部身份驗證按預期工作。為此，我們可以使用微軟提供的基於GUI的LDAP客戶端、Ldp.exe或任何第三方LDAP瀏覽器。在本文中，我們將使用ldp.exe本地或遠端連線、繫結和瀏覽AD伺服器並確定屬性。

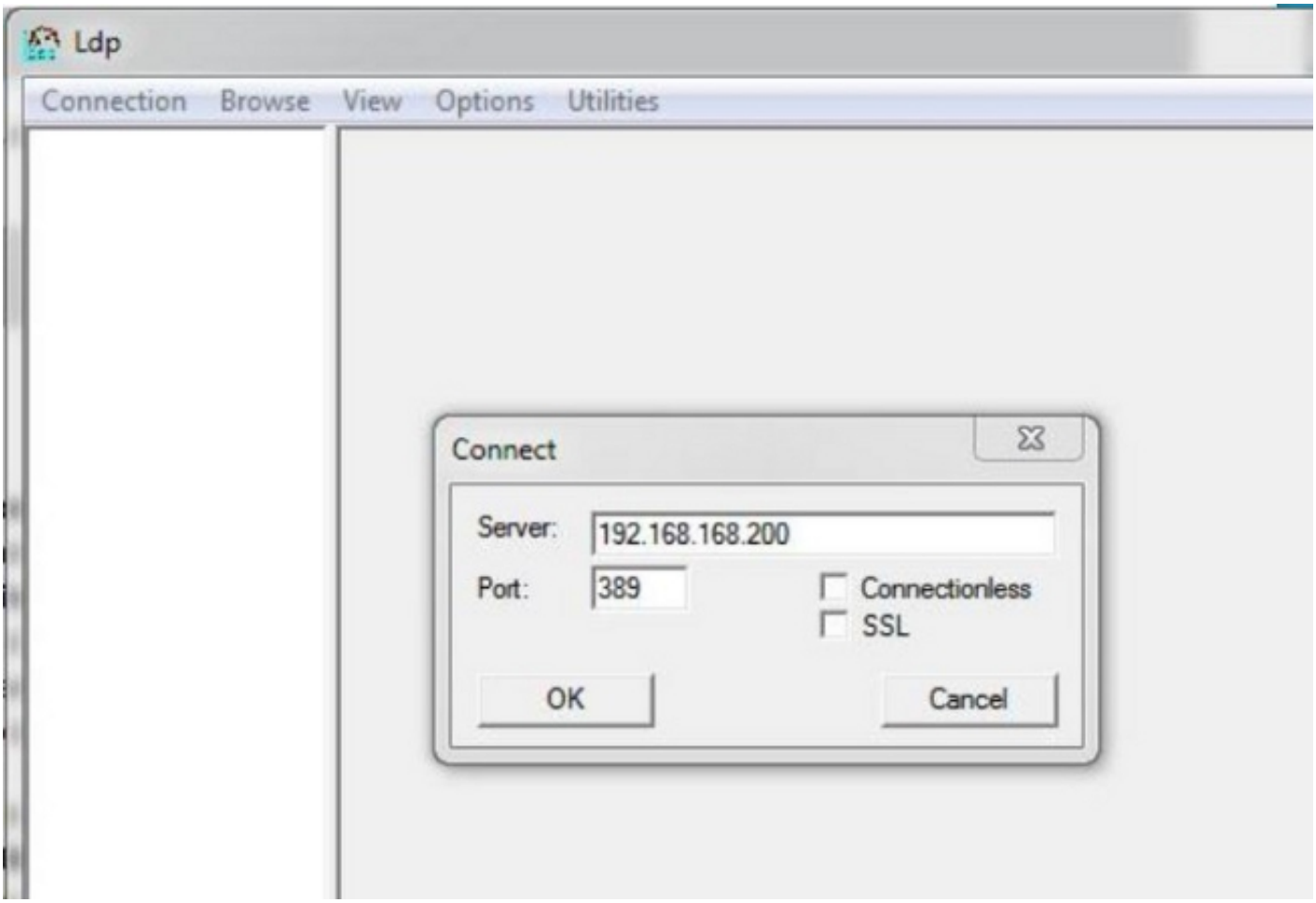
步驟1:啟動ldp.exe應用程式。轉到「**Start**」選單，然後按一下「**Run**」。鍵入**ldp.exe**並按**OK**按鈕。

> **附註**：在Windows Server 2008上，預設情況下安裝ldp.exe。對於Windows Server 2003或從Windows客戶端電腦進行遠端連線，請從Microsoft站點下載support.cab或support.msi檔案。解壓.cab檔案或安裝.msi檔案並運行ldp.exe。

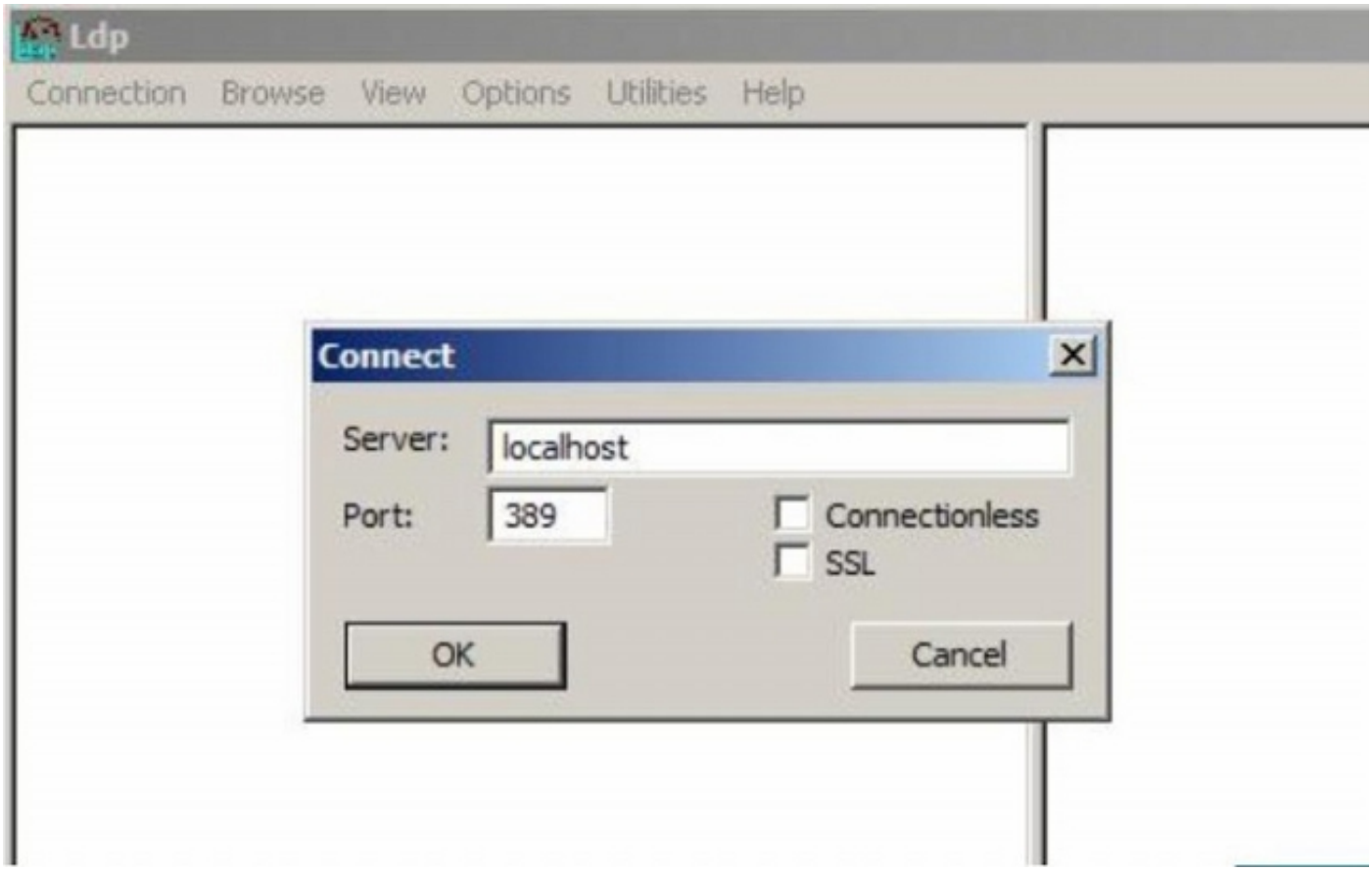
步驟2:連線到伺服器。選擇**Connection**，然後按一下**Connect**。

- 要從本地電腦連線到AD域控制器(DC)，請輸入AD伺服器的主機名或IP地址。
- 要本地連線到AD DC，請輸入localhost作為**Server**。

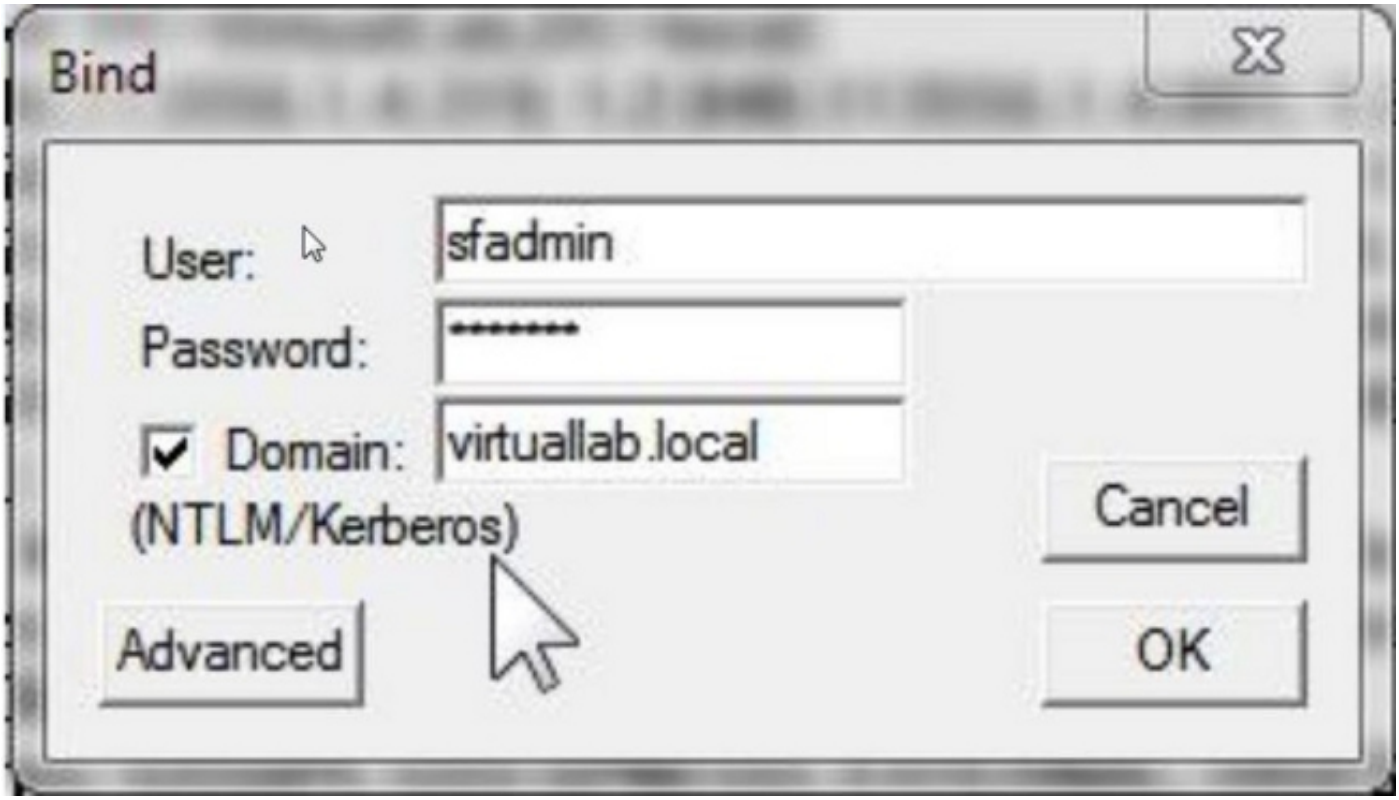
以下螢幕截圖顯示了從Windows主機進行的遠端連線：



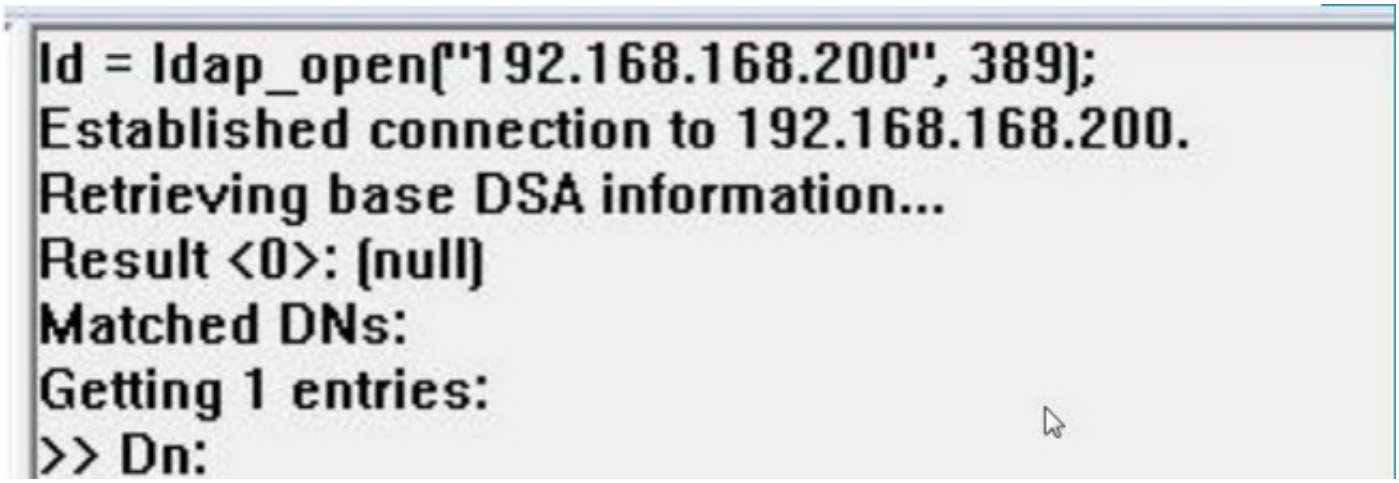
以下螢幕截圖顯示了AD DC上的本地連線：



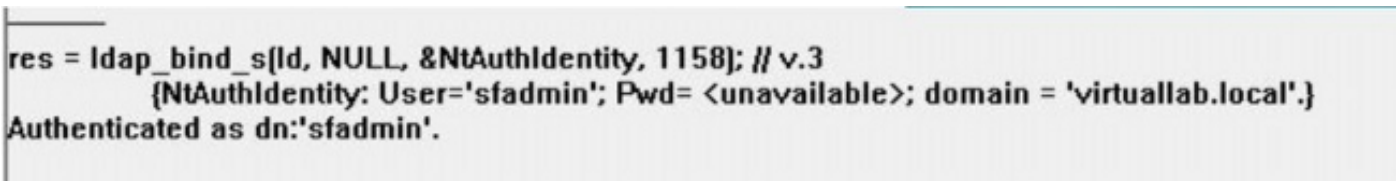
步驟3.繫結到AD DC。轉至**Connection > Bind**。輸入**User**、**Password**和**Domain**。按一下「**OK**」（確定）。



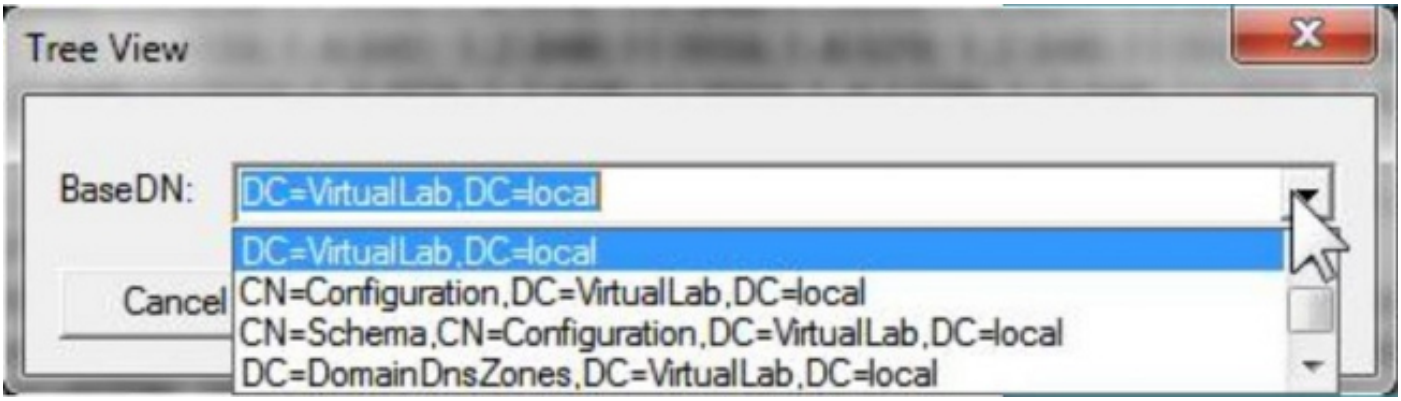
連線嘗試成功後，您會看到如下所示的輸出：



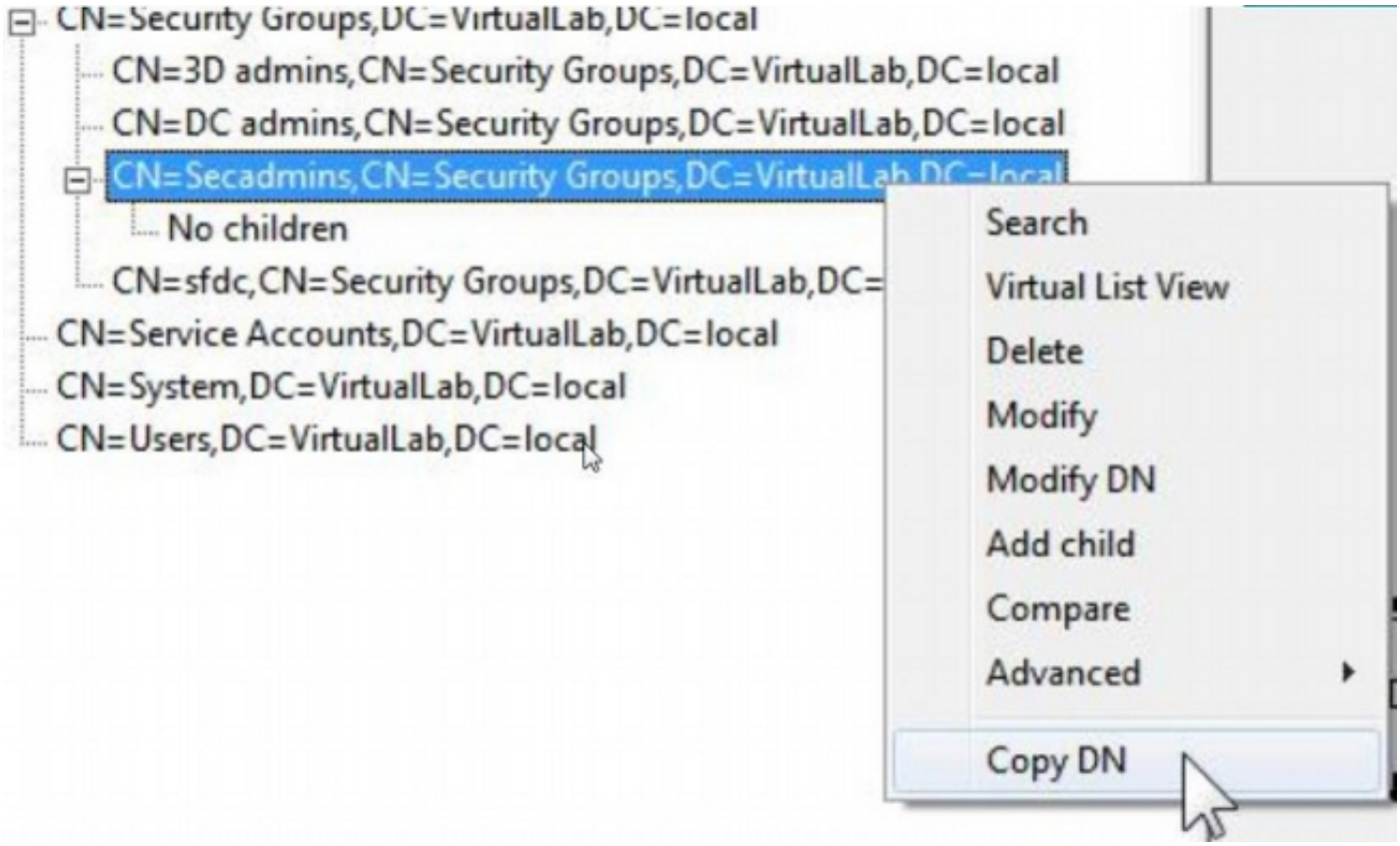
此外，ldp.exe左窗格中的輸出將顯示成功繫結到AD DC。



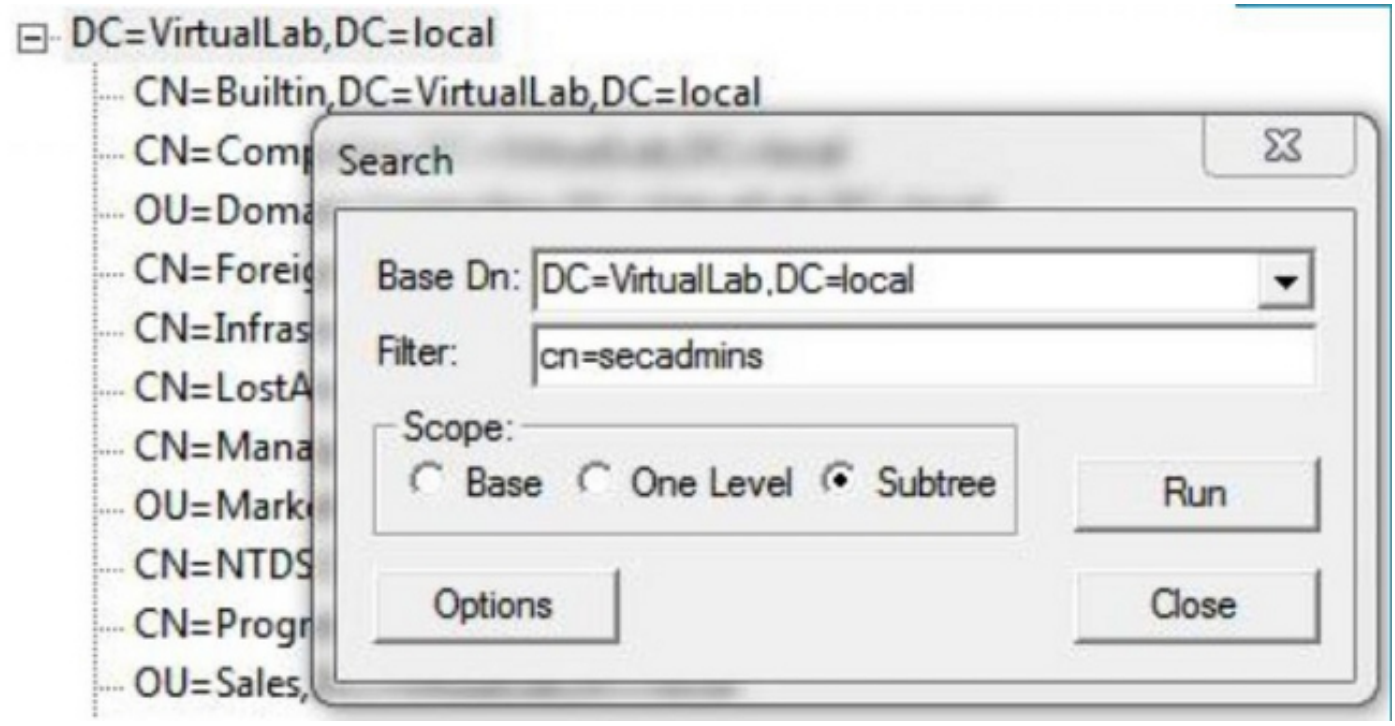
第4步：瀏覽目錄樹。按一下**View > Tree**，從下拉選單中選擇**BaseDN**域，然後按一下**OK**。此基本DN是在驗證對象上使用的DN。



第5步：在ldp.exe的左窗格中，按兩下AD對象以將容器向下展開到葉對象的級別，然後導航到使用者所屬的AD安全組。找到組後，按一下右鍵該組，然後選擇**Copy DN**。



如果您不確定該組位於哪個組織單位(OU)，請按一下右鍵基本DN或域，然後選擇**搜尋**。出現提示時，輸入**cn=<*group name*>**作為過濾器，**Subtree**作為**範圍**。獲得結果後，即可複製組的DN屬性。也可以執行萬用字元搜尋，例如**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;
```

身份驗證對象中的基本過濾器應如下所示：

- 單個組：

  基本篩選器：(memberOf=<Security_group_DN>)

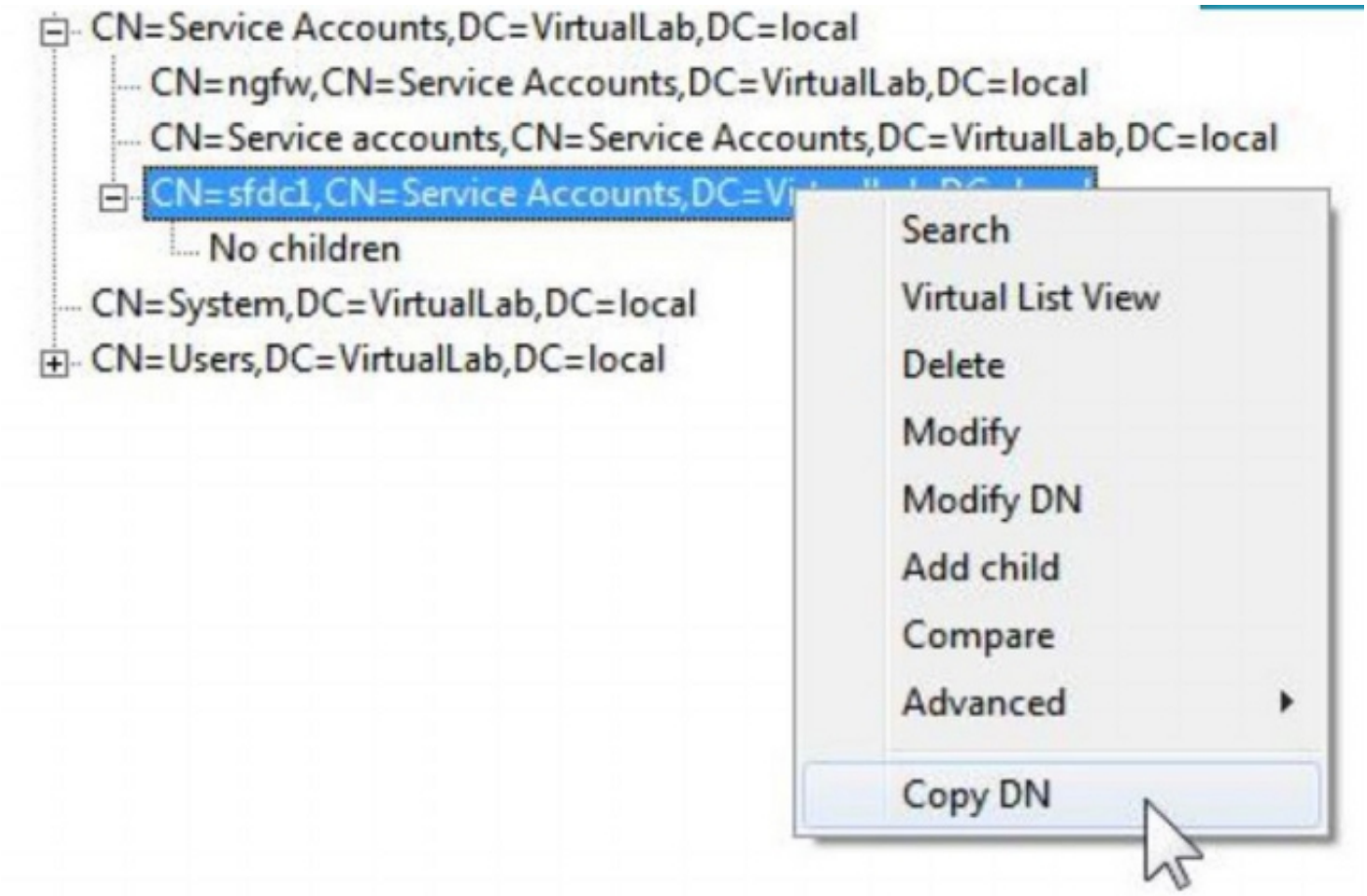
- 多個組：

  基本篩選器
  ：(|(memberOf=<group1_DN>)(memberOf=<group2_DN>)(memberOf=<groupN_DN))

在以下示例中，請注意AD使用者的memberOf屬性與基本篩選器匹配。memberOf屬性前面的數字表示使用者所屬的組數。該使用者僅是一個安全組secadmins的成員。

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

第6步：導航到要在身份驗證對象中用作模擬帳戶的使用者帳戶，然後按一下右鍵該使用者帳戶以複製DN。



在身份驗證對**象中**將此DN用作使用者名稱。例如，

使用者名稱：CN=sfdc1,CN=服務帳戶，DC=虛擬實驗室，DC=本地

與組搜尋類似，也可以搜尋具有CN或特定屬性(例如name=sfdc1)的使用者。