识别活动目录LDAP验证对象配置的对象属性

目录

简介

本文描述如何识别激活目录(AD) LDAP对象属性配置在的验证对象外部验证的。

识别LDAP对象属性

在配置在一个FireSIGHT管理中心的一个验证对象之前外部验证的，识别用户和安全组AD LDAP属性是必要为了外部验证能工作按照计划。要执行如此，我们能使用Microsoft提供了GUI基于LDAP客户端、Ldp.exe，或者所有第三方LDAP浏览器。在此条款，我们将使用ldp.exeto连接，绑定，并且浏览AD服务器并且识别属性。

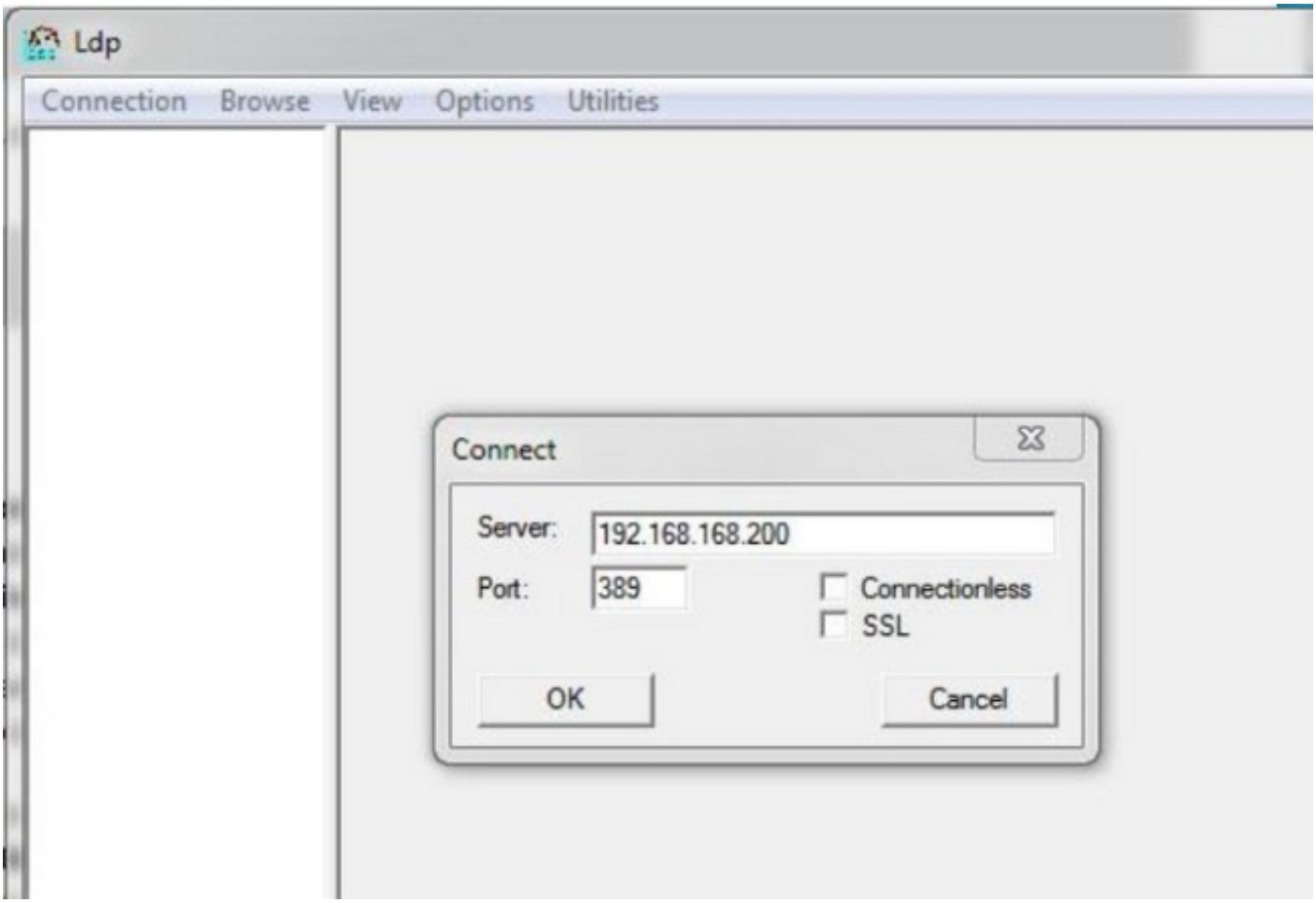
步骤 1：启动`ldp.exe`。去Startmenu并且点击运行**。键入**ldp.exeandOK按钮。

> **注意**：默认情况下在Windows服务器上2008年， `ldp.exe`安装。对于远程连接的Windows服务器2003年或从Windows客户端计算机，请下载Microsoft站点的support.cabor `support.msi`。解压缩.msi fileand运行ldp.exe的.cab fileor安装。

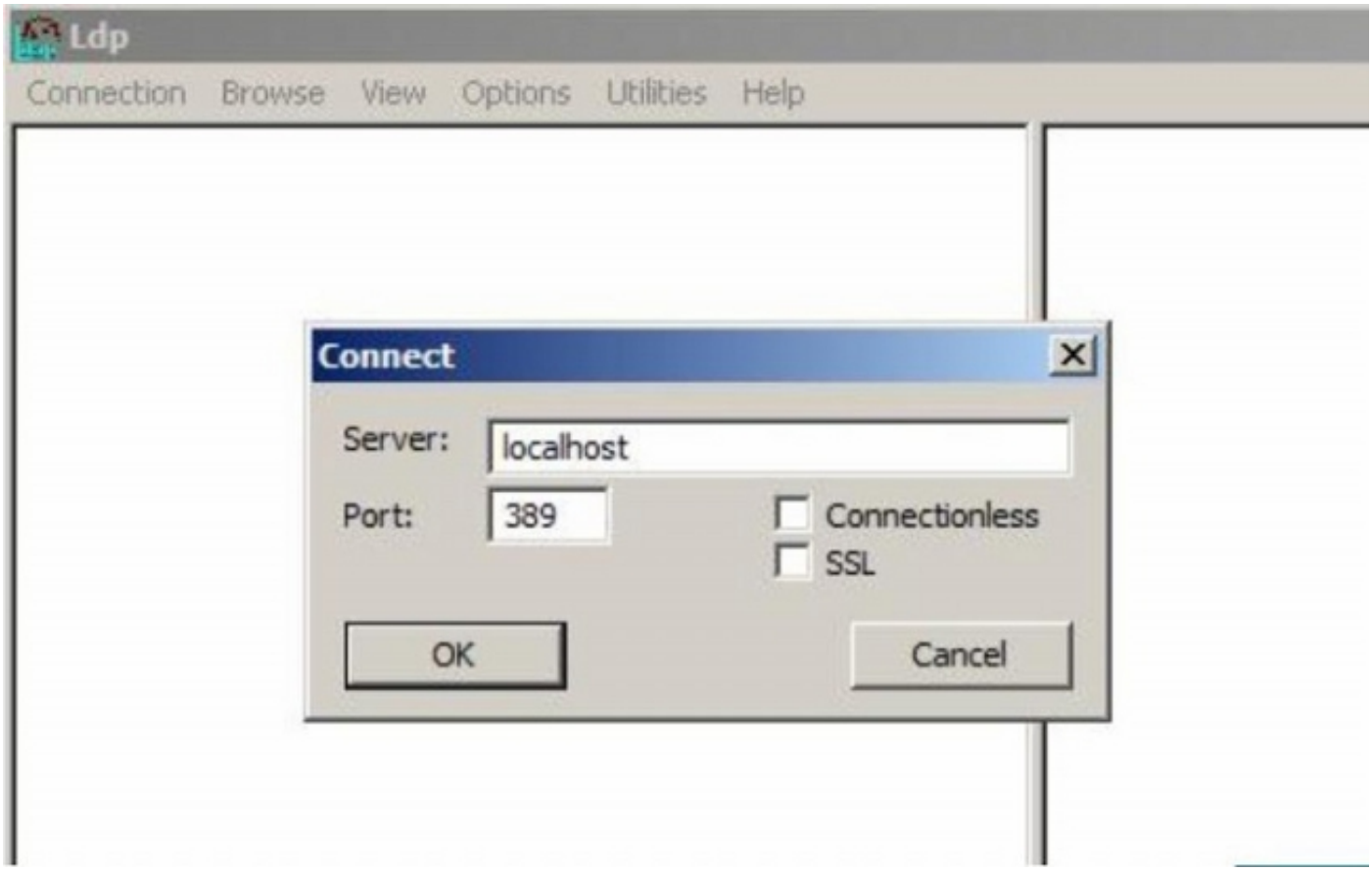
步骤 2：对服务器的连接。选择**连接**并且点击**连接**。

- 要连接到AD域控制器(DC)从本地计算机，请输入AD服务器的主机名或IP地址。
- 要连接到AD DC本地，请进入`localhost`作为**服务器**。

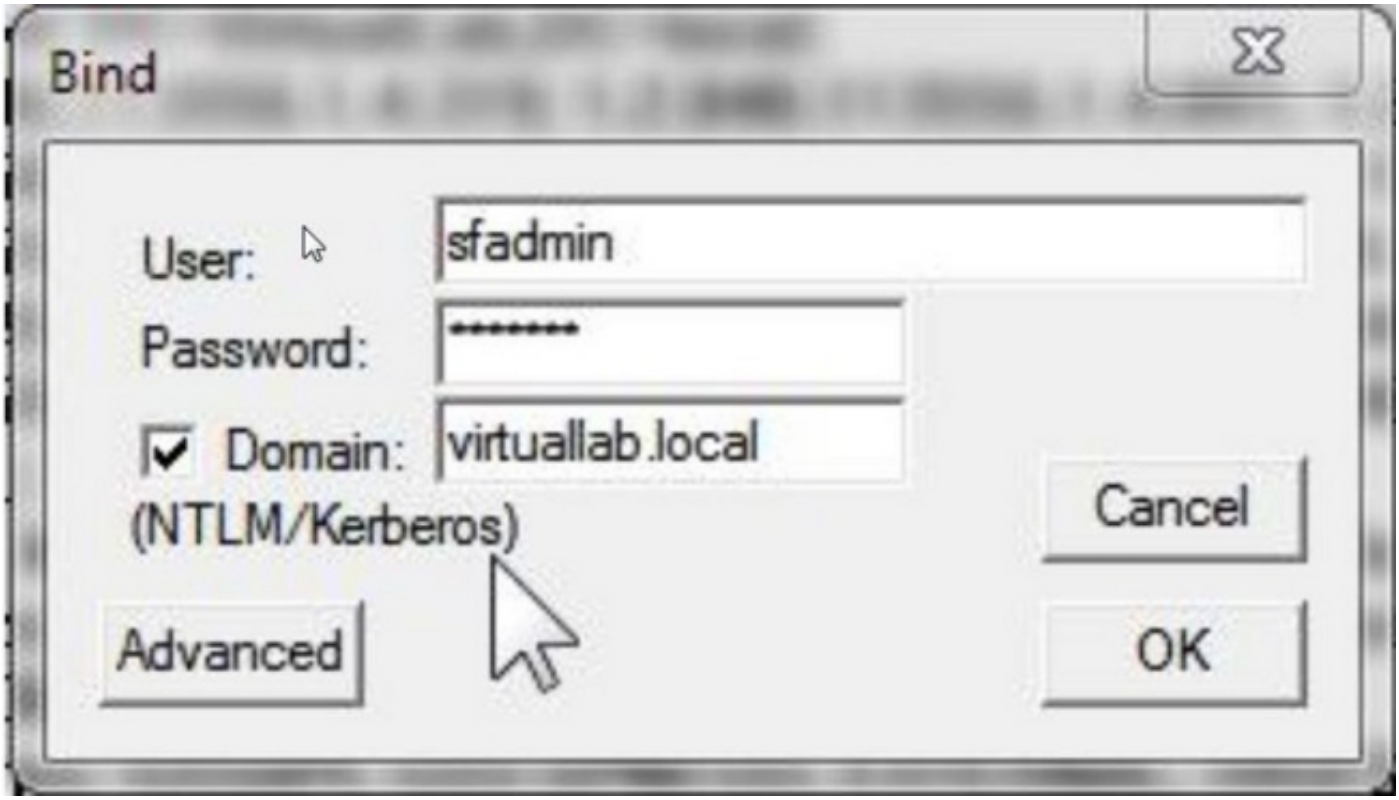
以下屏幕画面表示从Windows主机的远程连接：



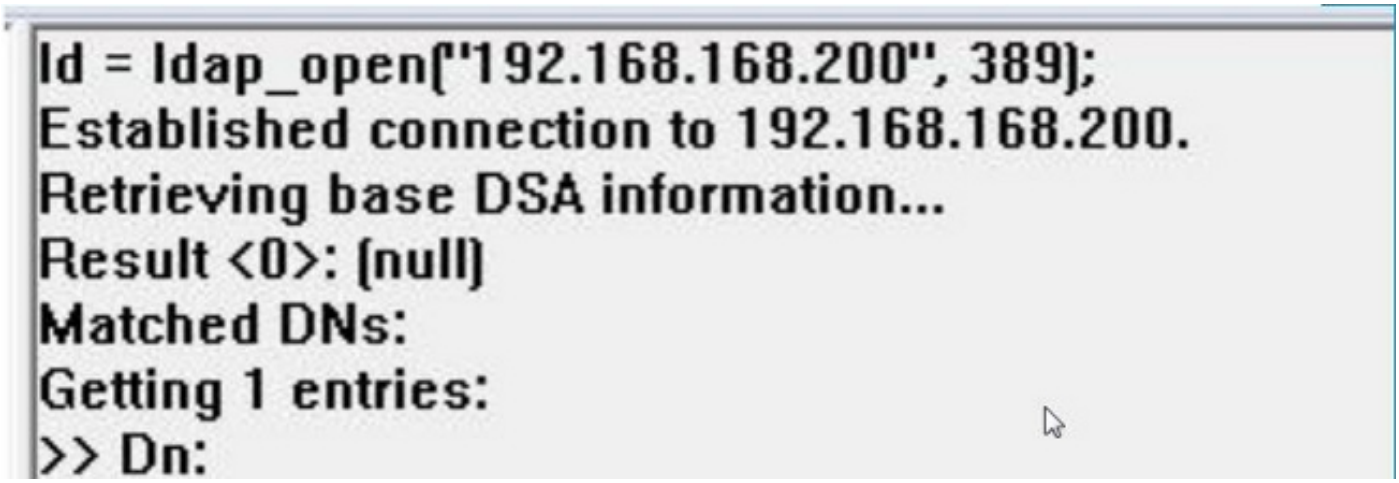
以下屏幕画面表示在AD DC:的本地连接



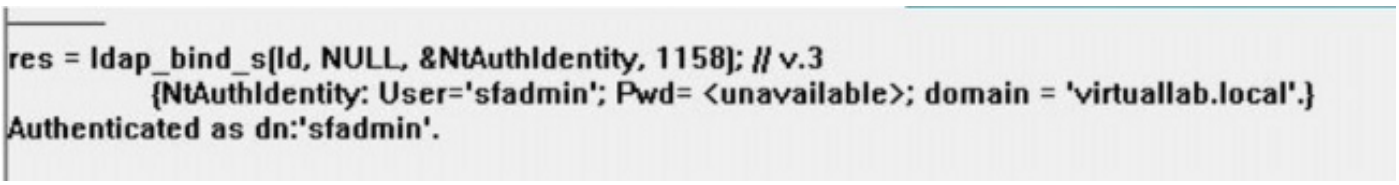
步骤3.对AD DC的捆绑。去**连接>捆绑**。输入**用户**、**密码**和**域**。单击 **Ok**。



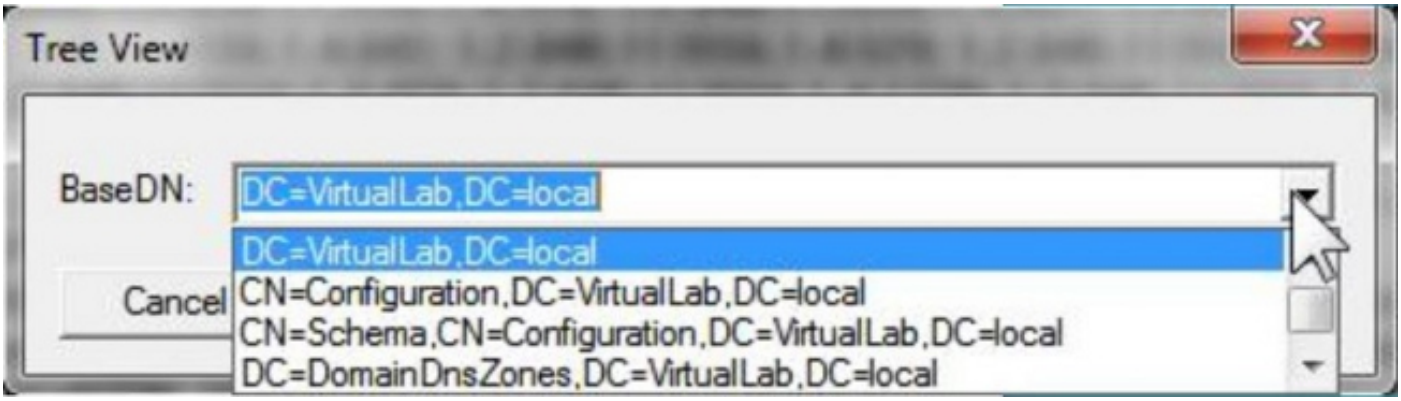
当连接尝试是成功的，您将看到一输出类似如下：



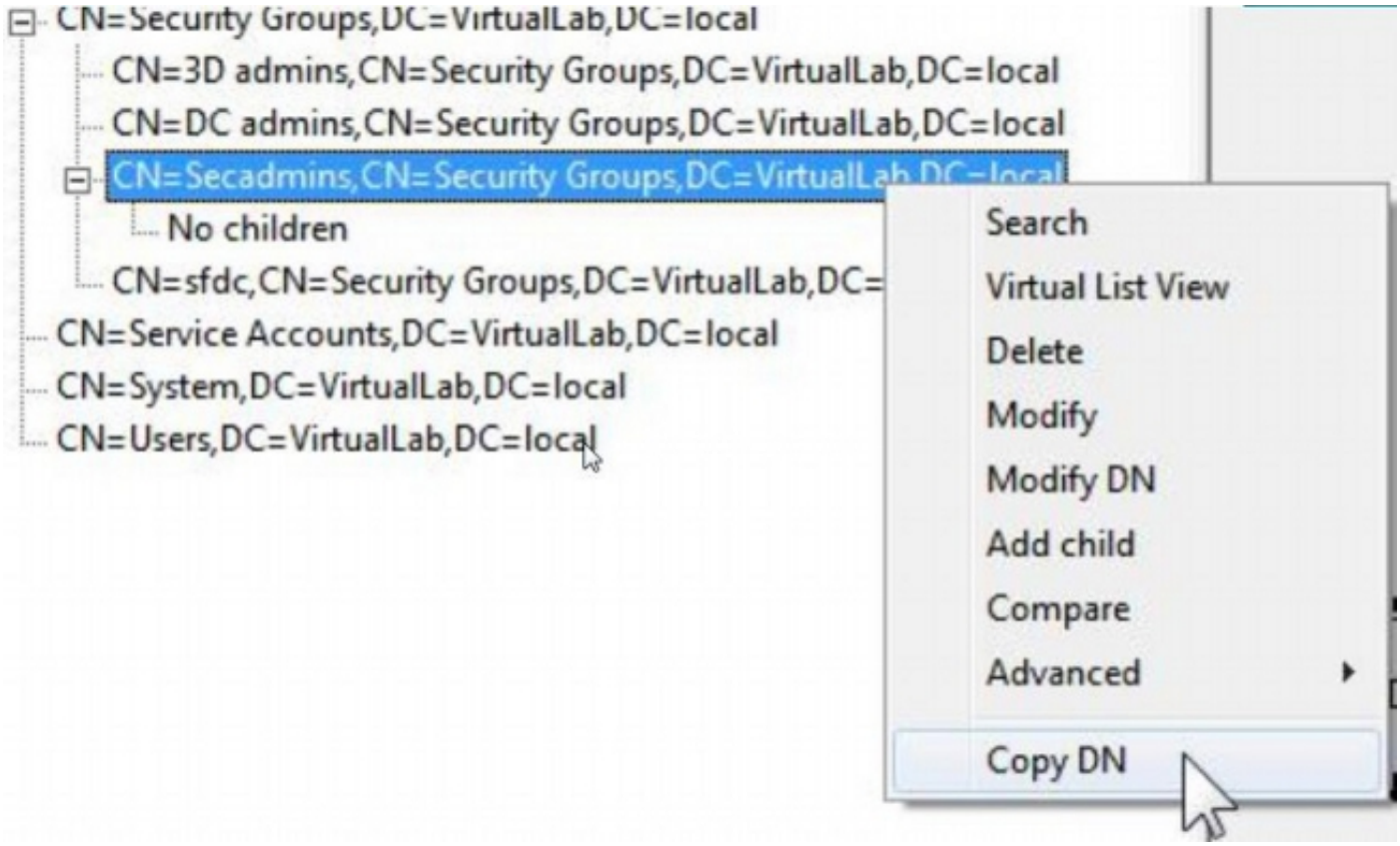
并且，在`ldp.exe`左窗格的输出将显示成功的捆绑对AD DC。



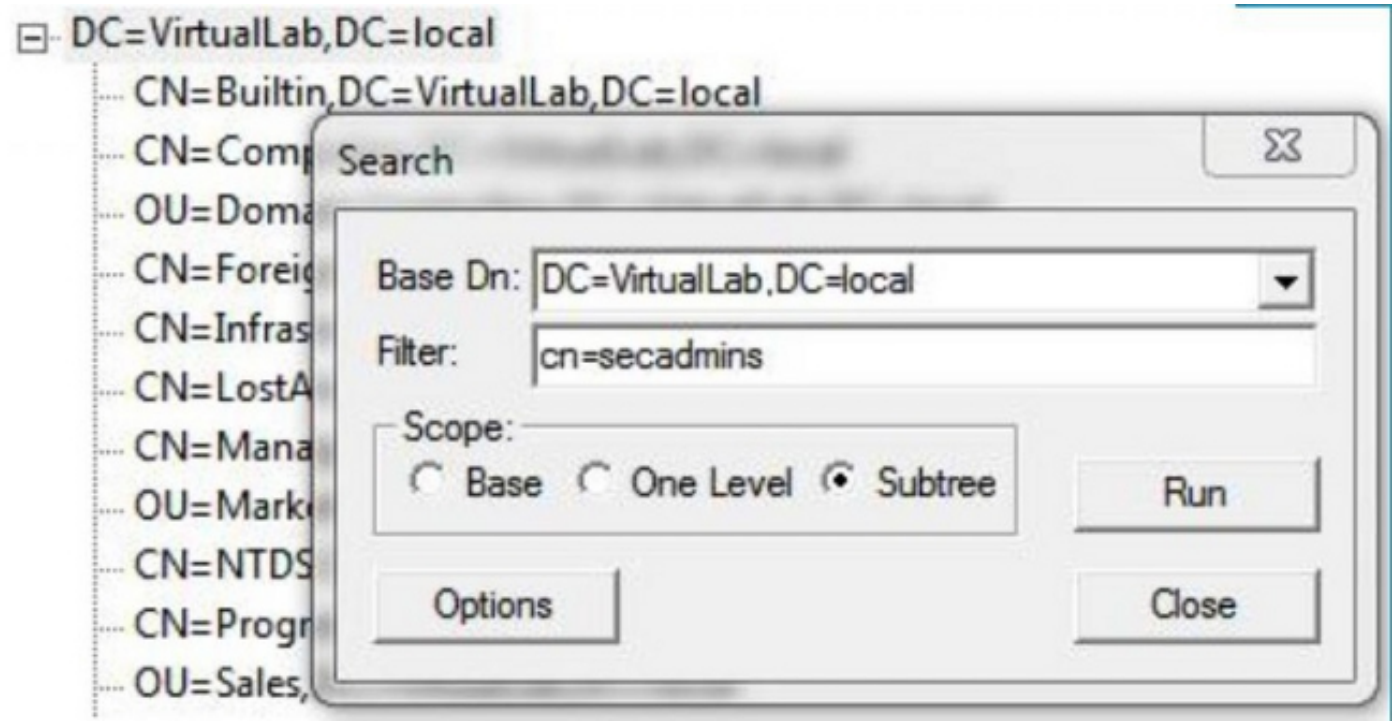
步骤 4：浏览目录树。点击**视图>树**，选择从下拉列表的域**BaseDN**，并且点击OK键。此基础DN是在验证对象使用的DN。



步骤 5：在`ldp.exe`左窗格在展开容器下来对级别分支对象和导航的AD对象的对AD安全组用户是成员。一旦寻找组，请用鼠标右键单击在组然后选择CopyDN。



如果不是肯定的在哪组织单位(OU)组查找，请用鼠标右键单击在基础DN或域并且选择**搜索**。当提示，请进入**cn=<group *name*>**作为过滤器和**子树**作为**范围**。一旦取得结果，您能然后复制组的DN属性。执行一通配符搜索例如**cn=*admin***也是可能的。




```
***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;
```

在验证对象的基本过滤器应该是作为如下：

- 组：

  基本过滤器：`(memberOf=<Security_group_DN>)`

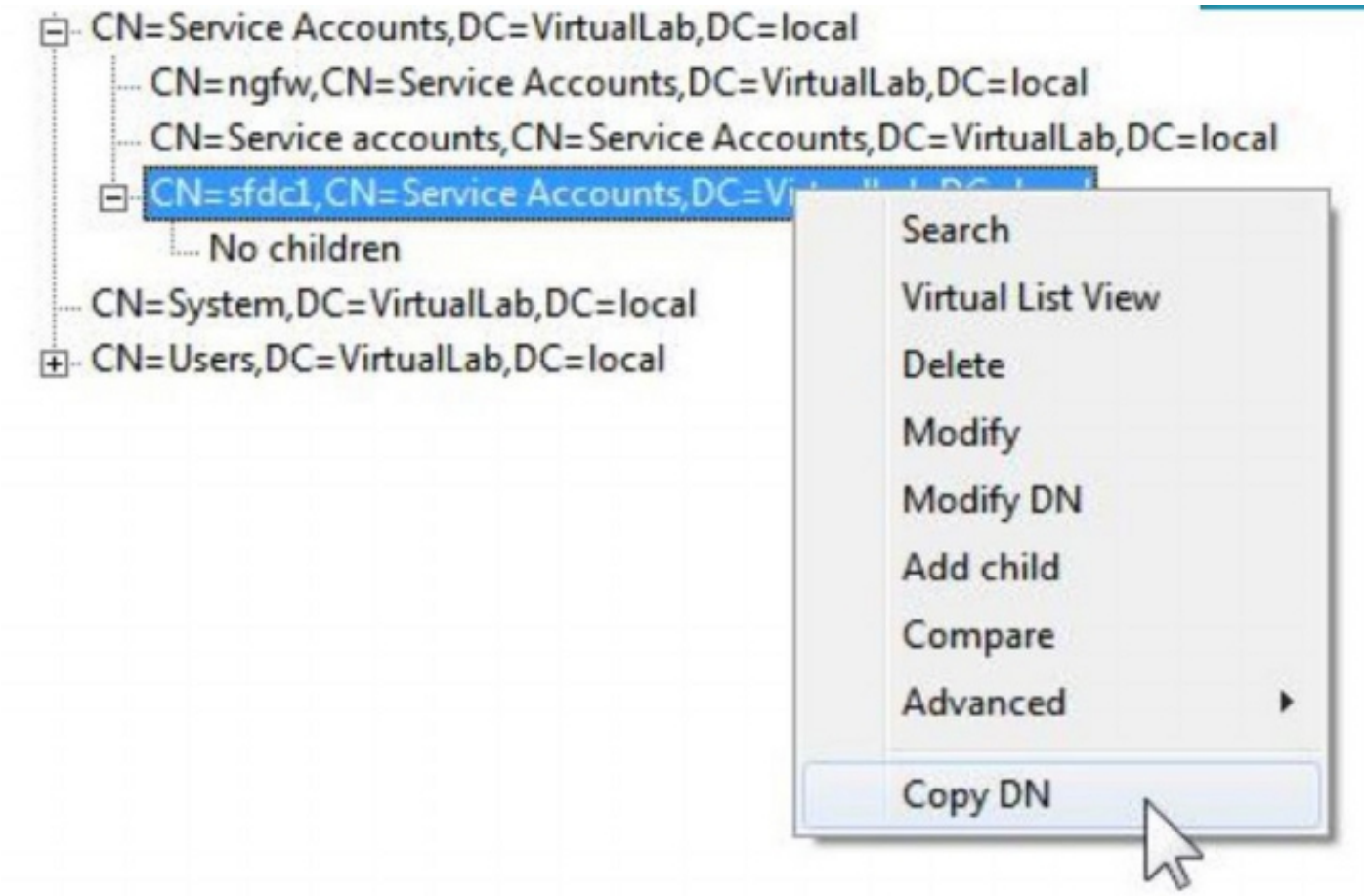
- 多个组：

  基本过滤器

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

在以下示例中，请注意有`memberOf`属性匹配基本过滤器的AD用户。编号之前的`memberOf`属性指示组数量用户是成员。用户只是一个安全组的成员， `secadmins`。

步骤 6：导航对您希望使用作为模拟帐户在验证对象的用户帐户，并且用鼠标右键单击在用户帐户**复制DN**。



请使用此DN**用户名**在验证对象。例如，

用户名：`CN=sfdc1,CN=Service DC=VirtualLab DC=local`

类似分组搜索，搜索有CN的一个用户或特定属性例如`name=sfdc1`也是可能的。