Identify Active Directory LDAP Object Attributes for Authentication Object Configuration

Document ID: 118721

Contributed by Nazmul Rajib and Binyam Demissie, Cisco TAC Engineers.
Dec 19, 2014

Contents

Introduction

This document describes how to identify Active Directory (AD) LDAP Object attributes to configure Authentication Object on the for external authentication.

Identify LDAP Object Attributes

Prior to configuring an Authentication Object on a FireSIGHT Management Center for external authentication, identifying the AD LDAP attributes of Users and Security Groups would be necessary for the external authentication to work as intended. To do so, we can use Microsoft provided GUI based LDAP client, Ldp.exe, or any third−party LDAP browser. In this article, we will use ldp.exe to locally or remotely connect, bind, and browse the AD server and identify the attributes.

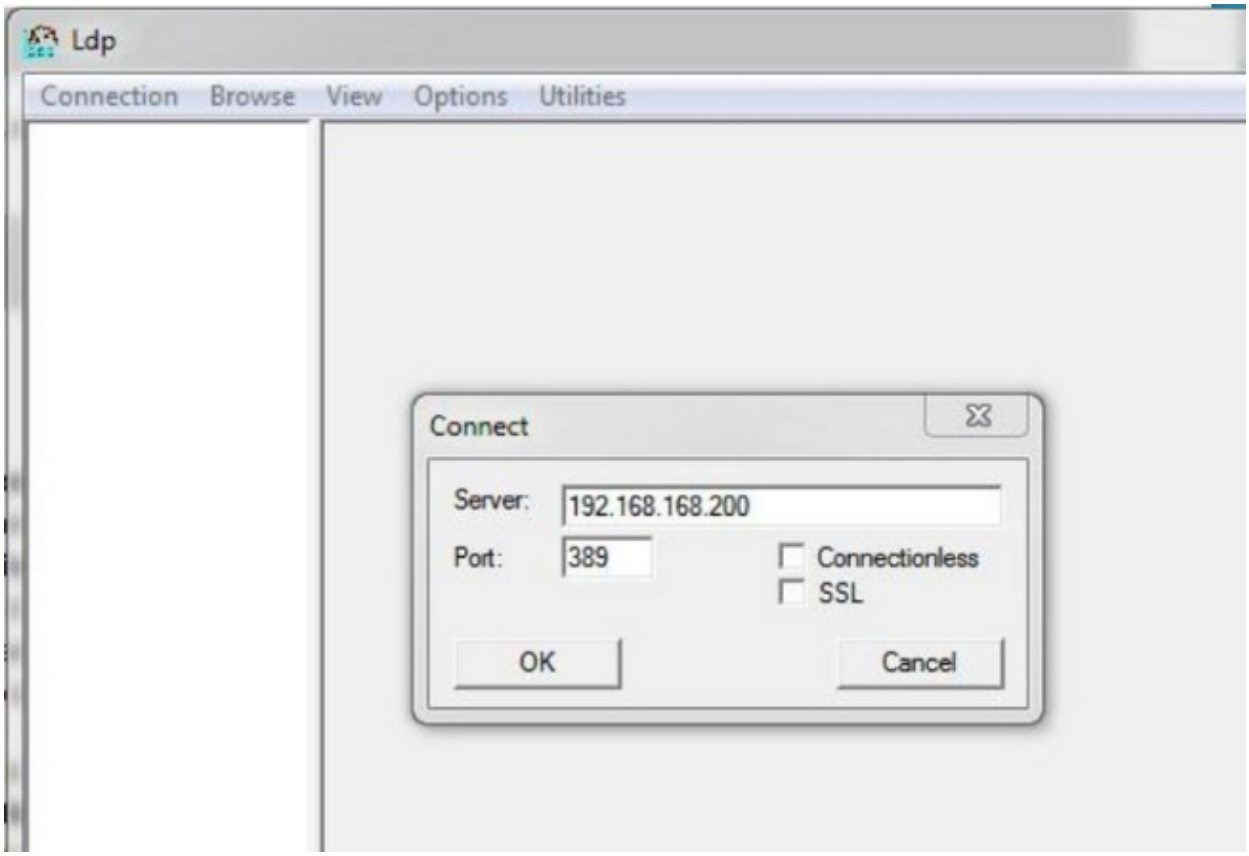
Step 1: Start ldp.exe application. Go to the ***Start*** menu and click ***Run***. Type ***ldp.exe*** and hit the ***OK*** button.

Note: On Windows Server 2008, ldp.exe is installed by default. For Windows Server 2003 or for remote connection from Windows client computer, please download the support.cab or support.msi file from the Microsoft site. Extract the .cab file or install the .msi file and run ldp.exe.

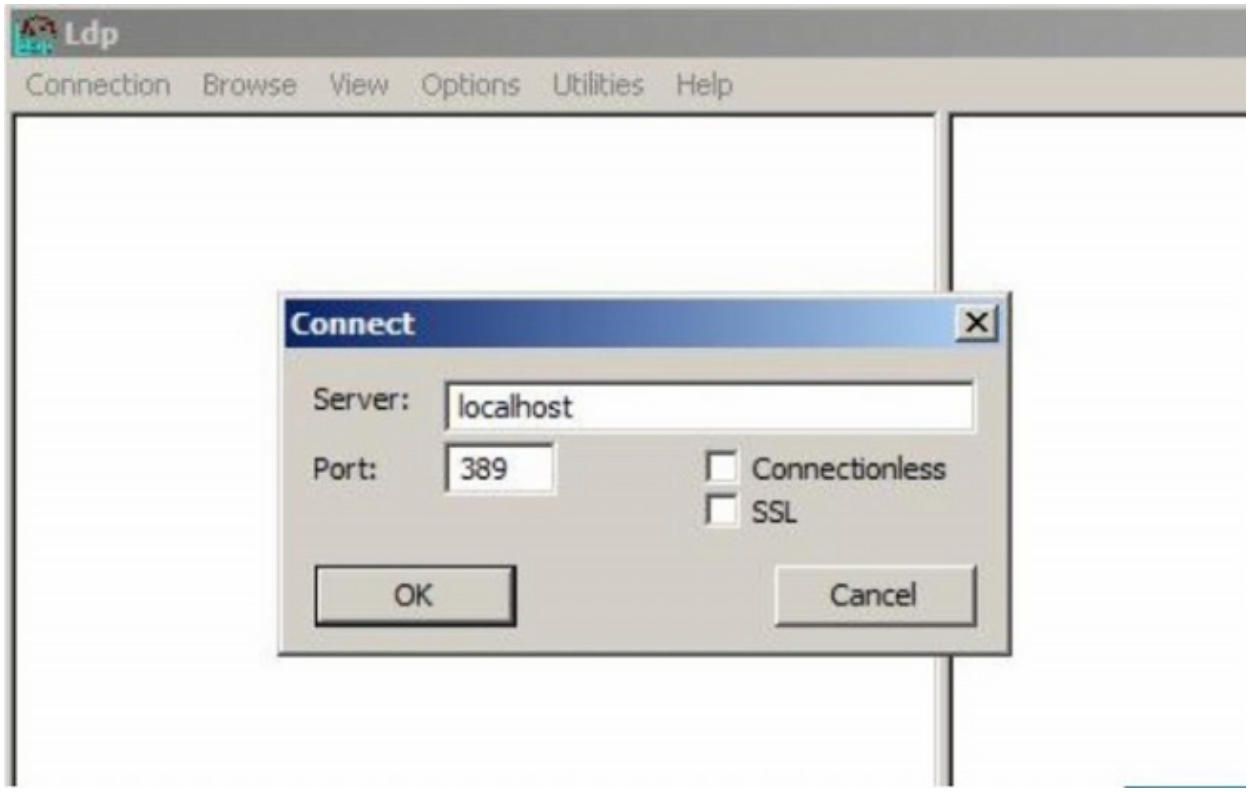
Step 2: Connect to the server. Select ***Connection*** and click ***Connect***.

- To connect to an AD Domain Controller (DC) from a local computer, enter the hostname or IP address of the AD server.
- To connect to an AD DC locally, enter localhost as ***Server***.

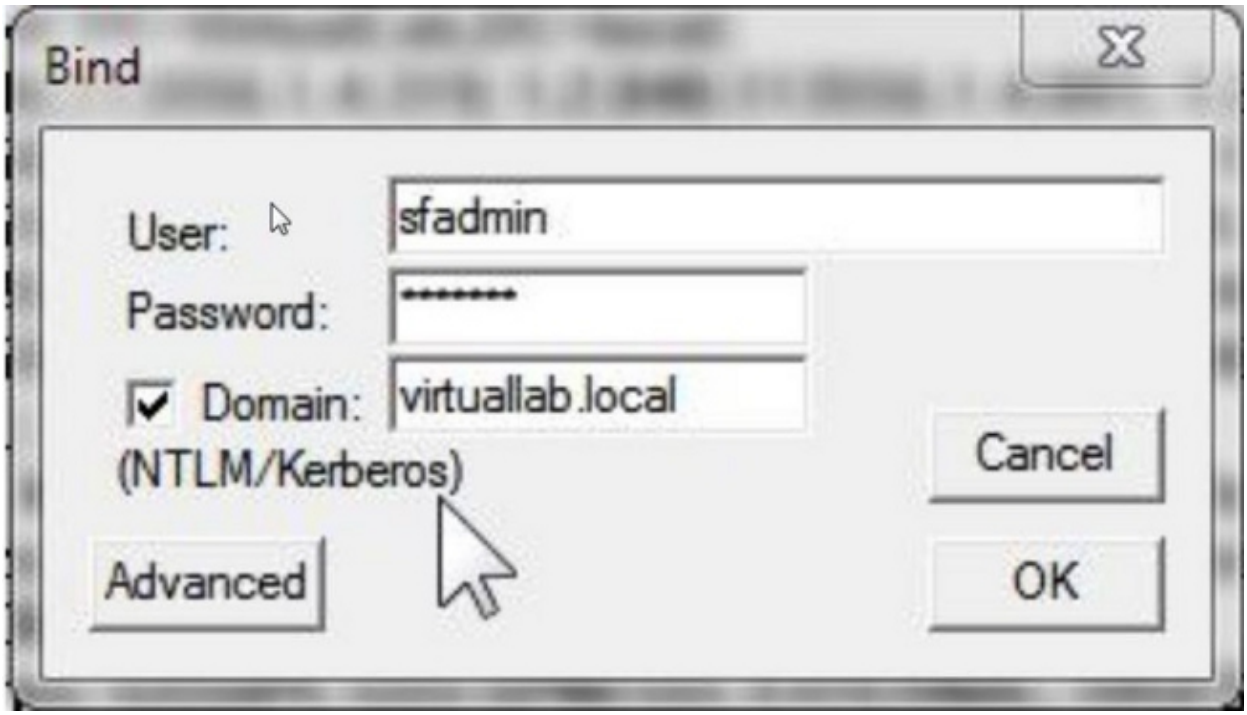
The following screenshot shows remote connection from a Windows host:



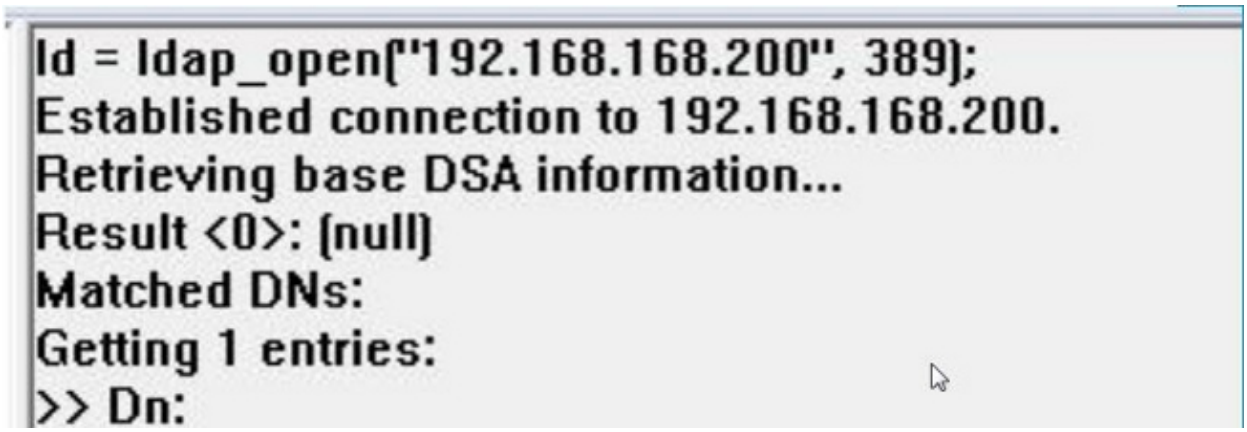
The following screenshot shows local connection on an AD DC:



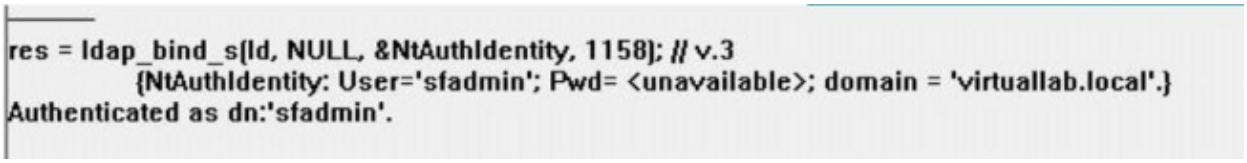
Step 3. Bind to the AD DC. Go to ***Connection*** > ***Bind***. Enter the ***User***, ***Password***, and ***Domain.*** Click ***OK***.



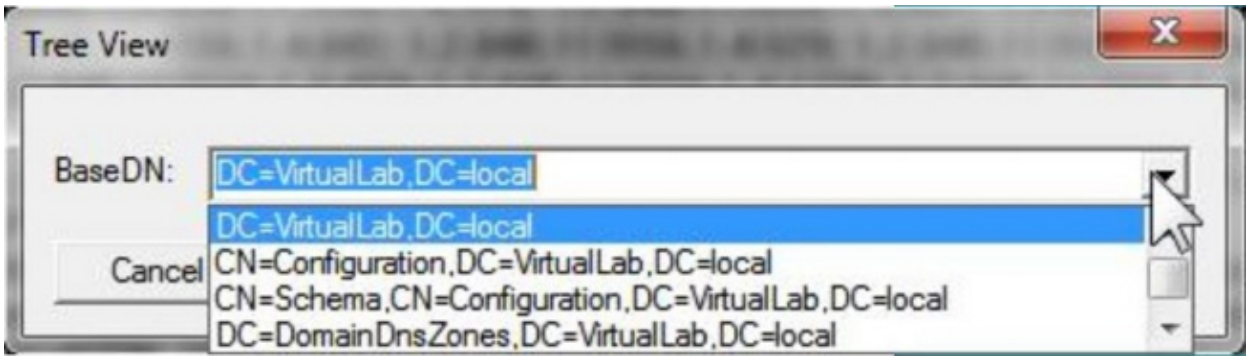
When a connection attempt is succesful, you will see an output like below:



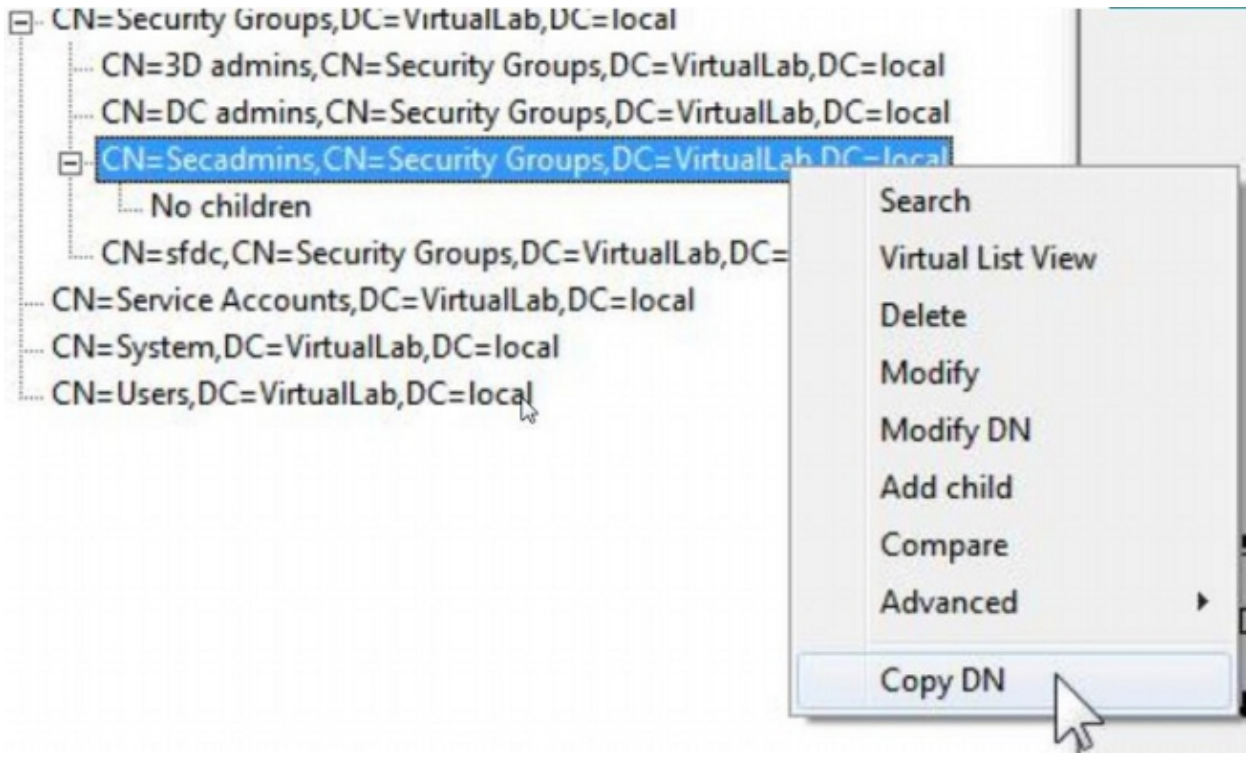
Also, the output on the left pane of ldp.exe will show successful bind to the AD DC**.**



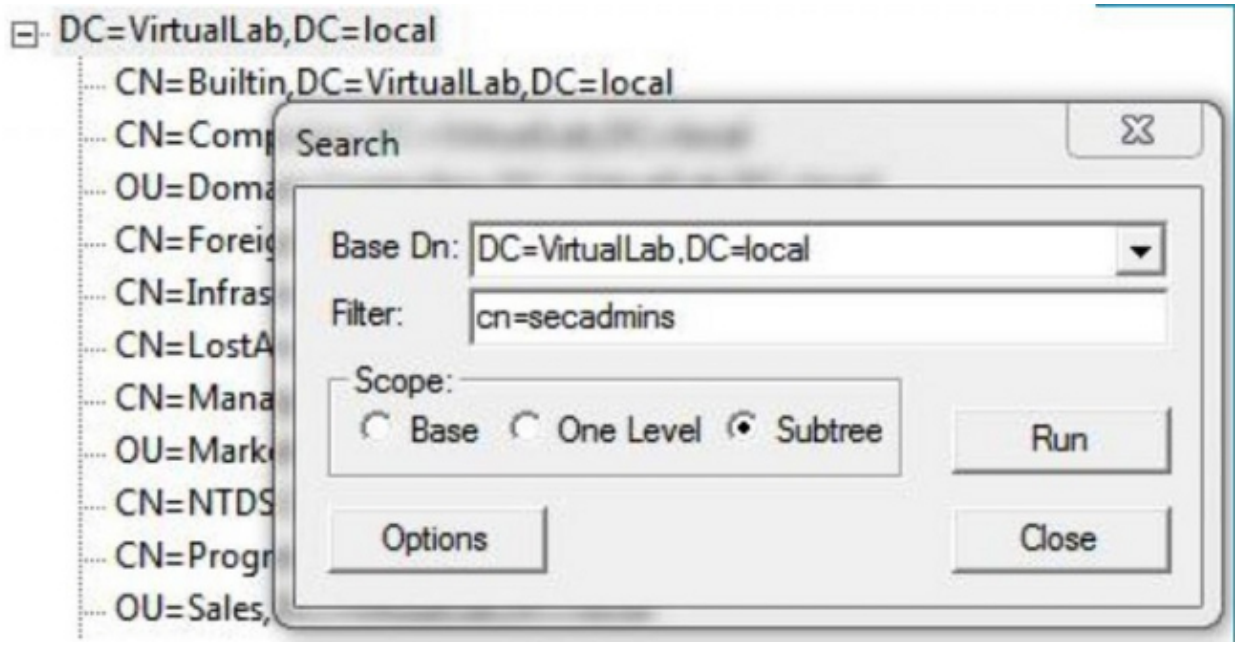
Step 4: Browse the Directory Tree. Click ***View*** **>** ***Tree*** , select the domain ***BaseDN*** from dropdown list, and click ***OK***. This Base DN is the DN that is used on the Authentication Object.



Step 5: On the left pane of ldp.exe, double click on the AD objects to expand the containers down to the level of leaf objects and navigate to the AD Security Group the users are member of. Once you find the group, right click on the group and then select ***Copy DN***.



If you are not sure in which Organizational Unit (OU) the group is located, right click on the Base DN or Domain and select ***Search***. When prompted, enter ***cn=<group name>*** as filter and ***Subtree*** as ***scope***. Once you get the result, you can then copy the DN attribute of the group. It is also possible to perform a wildcard search such as ***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;
```

The Base Filter in the Authentication Object should be as below:

- Single group:

  Base Filter: (memberOf=<Security_group_DN>)

- Multiple groups:

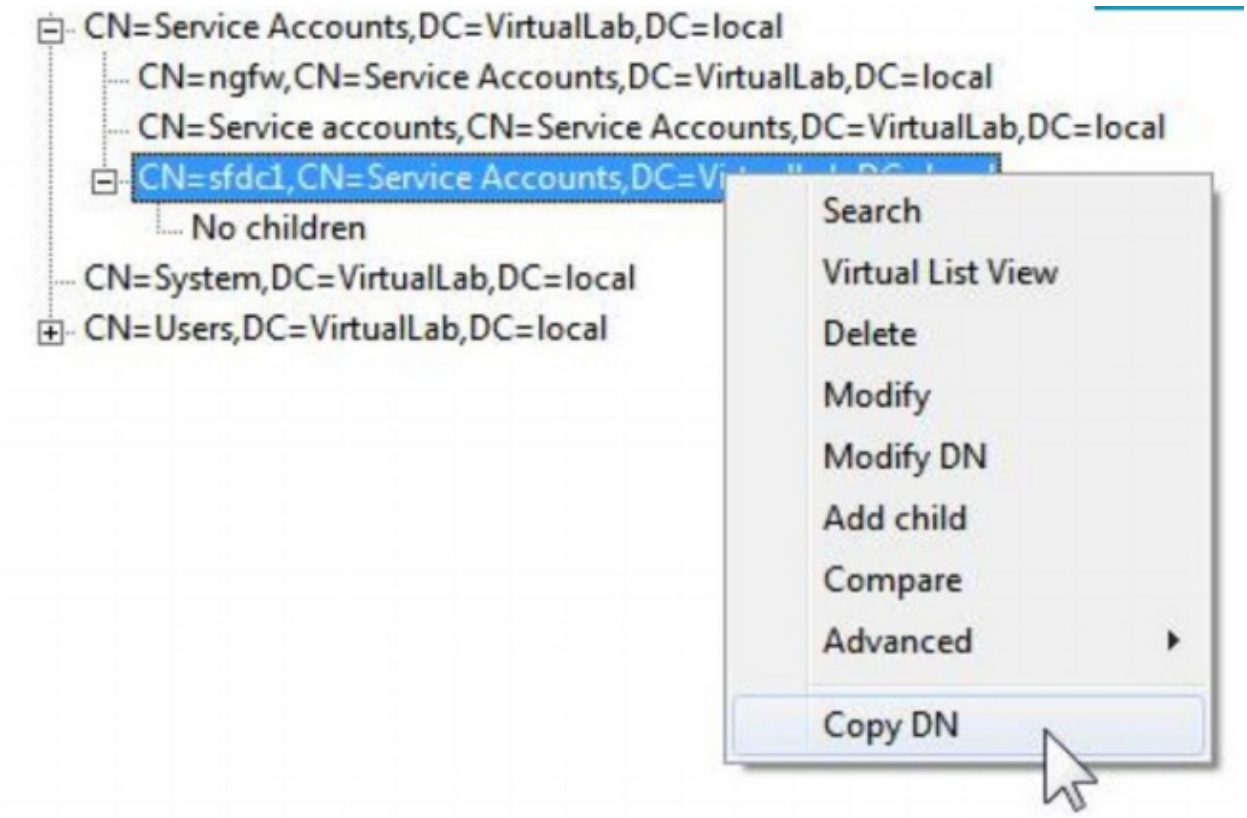
  Base Filter: (|(memberOf=<group1_DN>)(memberOf=<group2_DN>)(memberOf=<groupN_DN))

In the following example, note that AD users have memberOf attribute matching the Base Filter. The number preceding memberOf attribute indicate the number of groups the user is a member of. The user is a member of only one security group, secadmins.

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

Step 6: Navigate to the user accounts you would like to use as impersonation account in the Authentication

Object, and right click on the user account to ***Copy DN***.



Use this DN for ***User Name*** in the Authentication Object. For example,

User Name: CN=sfdc1,CN=Service Accounts,DC=VirtualLab,DC=local

Similar to group search, it is also possible to search a user with CN or specific attribute such as name=sfdc1.

Updated: Dec 19, 2014 Document ID: 118721
