

Identifique los atributos de objeto del Active Directory LDAP para la configuración del objeto de la autenticación

Contenido

[Introducción](#)

[Identifique los atributos de objeto LDAP](#)

Introducción

Este documento describe cómo identificar los atributos de objeto del Active Directory (AD) LDAP para configurar el objeto de la autenticación en para la autenticación externa.

Identifique los atributos de objeto LDAP

Antes de configurar un objeto de la autenticación en un centro de administración de FireSIGHT para la autenticación externa, la identificación de los atributos AD LDAP de los usuarios y de los grupos de seguridad sería necesaria para que la autenticación externa trabaje según lo previsto. Para hacer así pues, podemos utilizar Microsoft proporcionamos al cliente LDAP basado GUI, a Ldp.exe, o a cualquier navegador de tercera persona LDAP. En este artículo, utilizaremos ldp.exe localmente o conectar, atar, y hojear el servidor AD e identificaremos remotamente los atributos.

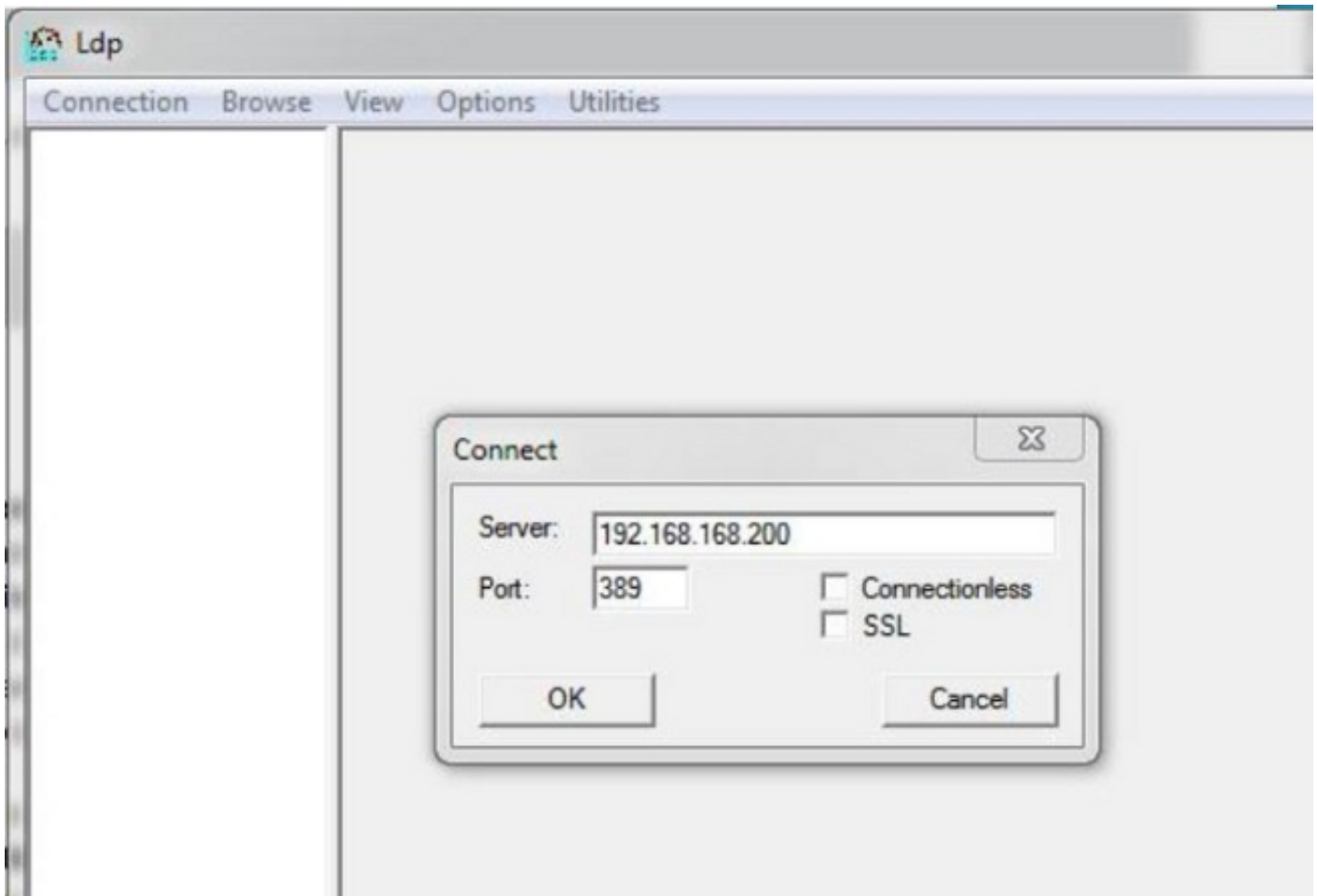
Paso 1: Comience la aplicación ldp.exe. Vaya al Startmenu y haga clic el funcionamiento. Teclee ldp.exe and golpear el botón OK.

Nota: En el Servidor Windows 2008, ldp.exe está instalado por abandono. Para el Servidor Windows 2003 o para la conexión remota del ordenador del cliente de Windows, descarga por favor el archivo support.cab or support.msi del sitio de Microsoft. Extraiga el file or .cab instalan el funcionamiento ldp.exe del file and .msi.

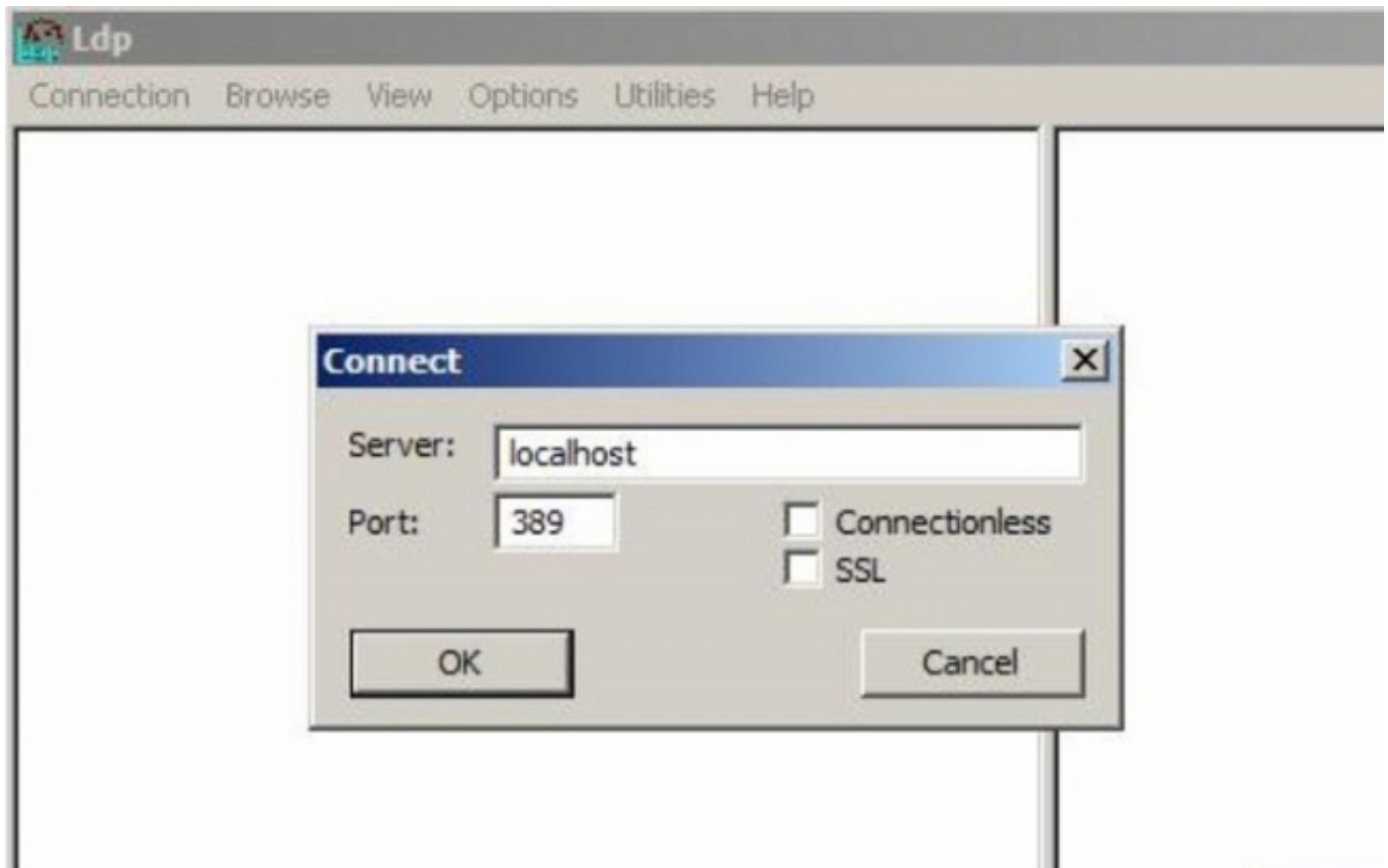
Paso 2: Conecte con el servidor. Seleccione la **conexión** y el tecleo **conecta**.

- Para conectar con un controlador de dominio AD (CC) de una computadora local, ingrese el nombre de host o el IP Address del servidor AD.
- Para conectar con un AD CC localmente, ingrese el localhost como **servidor**.

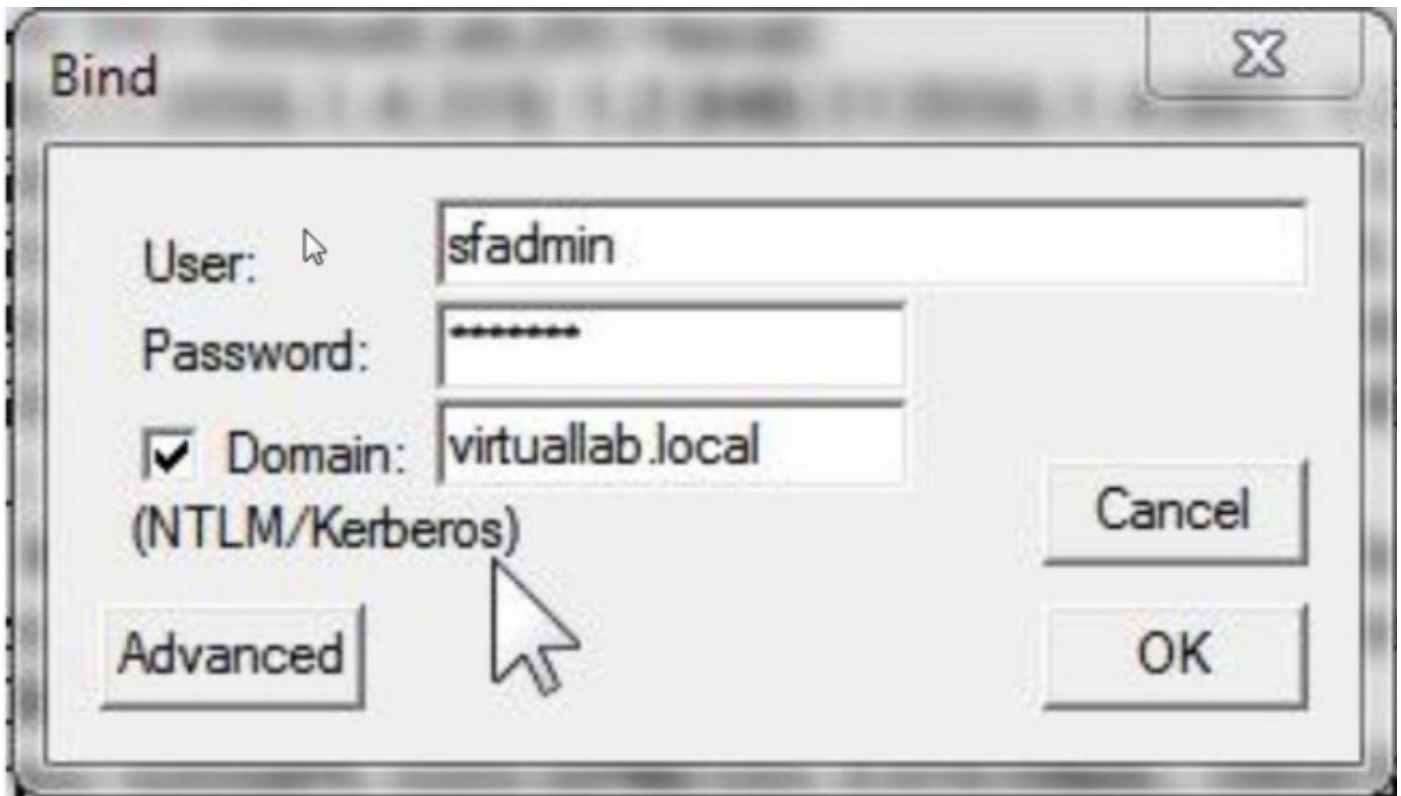
La conexión remota siguiente de las demostraciones del tiro de pantalla de un host de Windows:



El tiro de pantalla siguiente muestra la conexión local en un AD DC:



Paso 3. Lazo al AD DC. Vaya a la **conexión > al lazo**. Ingrese el **usuario**, la **contraseña**, y el **dominio**. Haga clic en **OK**.



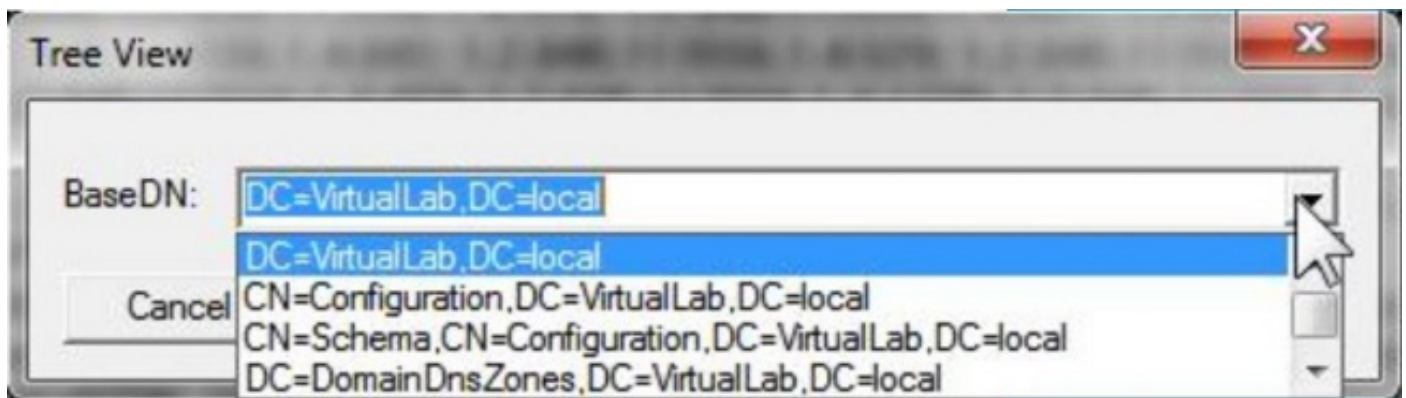
Cuando un intento de conexión es acertado, usted verá una salida como abajo:

```
Id = ldap_open('192.168.168.200', 389);
Established connection to 192.168.168.200.
Retrieving base DSA information...
Result <0>: [null]
Matched DNs:
Getting 1 entries:
>> Dn:
```

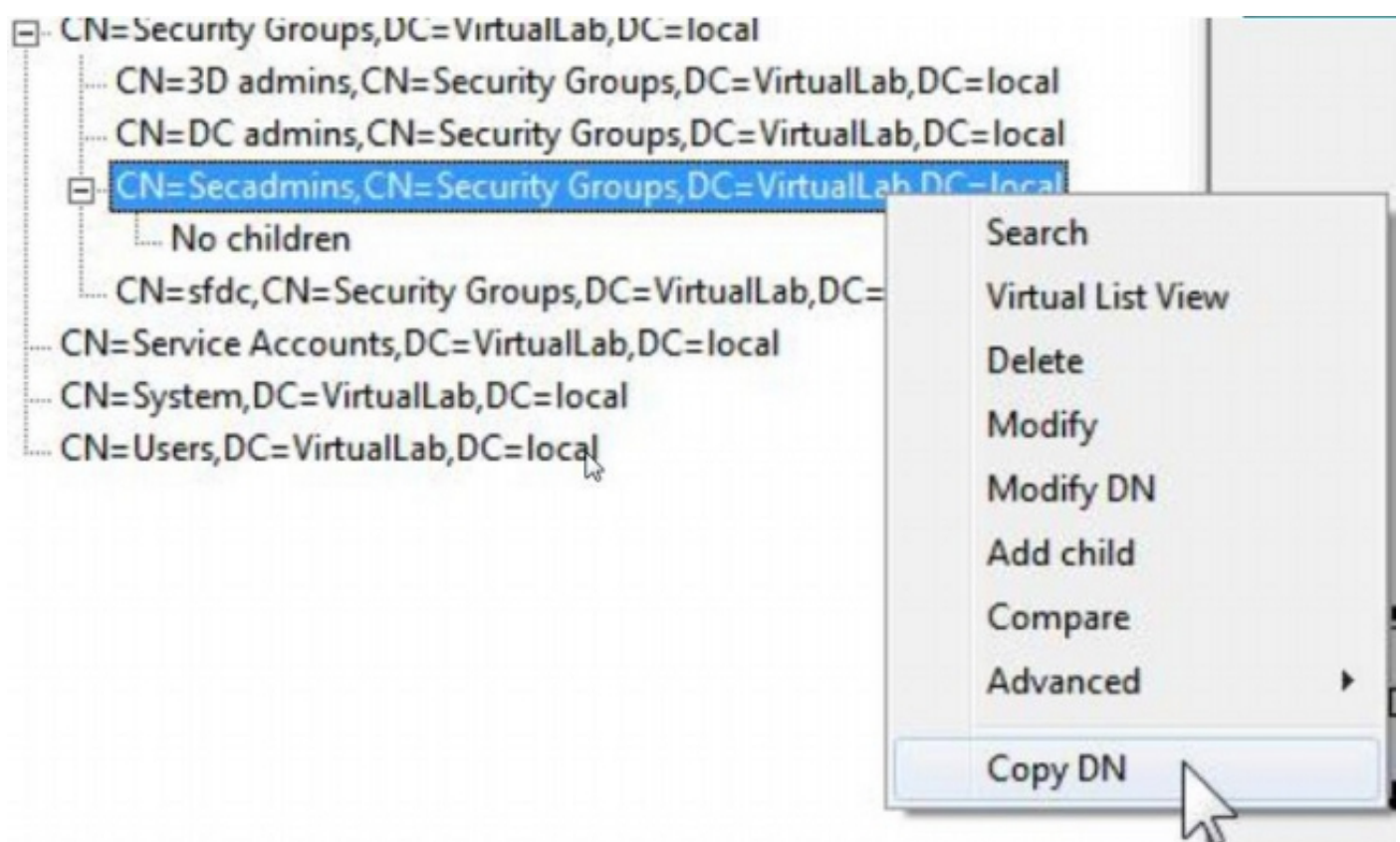
También, la salida en el panel izquierdo de `ldp.exe` mostrará el lazo acertado al AD DC.

```
res = ldap_bind_s(ld, NULL, &NtAuthIdentity, 1158); // v.3
      {NtAuthIdentity: User='sfadmin'; Pwd= <unavailable>; domain = 'virtuallab.local'.}
Authenticated as dn:'sfadmin'.
```

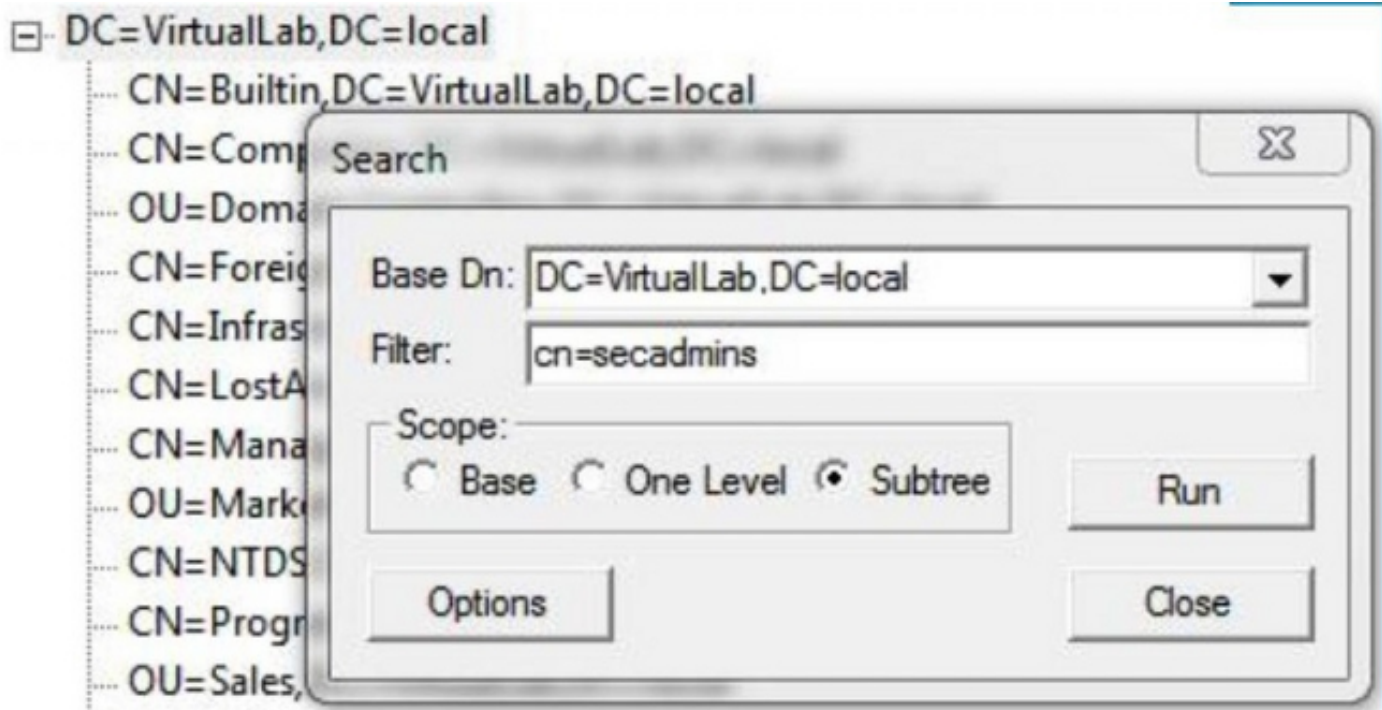
Paso 4: Hojee el árbol de directorio. Haga clic la **visión > el árbol**, seleccione el dominio **BaseDN** de la lista desplegable, y haga clic la **AUTORIZACIÓN**. Esta base DN es el DN que se utiliza en el objeto de la autenticación.



Paso 5: En el panel izquierdo de `ldp.exe`, el doble hace clic en los objetos AD para ampliar los envases abajo al nivel de objetos de la hoja y navegar al grupo de seguridad AD los usuarios son miembro de. Una vez que usted encuentra al grupo, haga clic con el botón derecho del ratón en el grupo y después seleccione CopyDN.



Si usted no está seguro en qué unidad organizativa (OU) localizan el grupo, haga clic con el botón derecho del ratón en la base DN o el dominio y seleccione la **búsqueda**. Cuando se le pregunte, ingrese el *name* > `del cn=<group` como filtro y la **sub-estructura** como **alcance**. Una vez que usted consigue el resultado, usted puede entonces copiar el atributo DN del grupo. Es también posible realizar una búsqueda del comodín tal como `cn=*admin*`.



```

***Searching...
ldap_search_s(lid, "DC=VirtualLab,DC=local", 2, "cn=secadmins", attrList, 0, &msg)
Result <0>: [null]
Matched DN's:
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;

```

El filtro bajo en el objeto de la autenticación debe estar como abajo:

- Solo grupo:

Filtro bajo: (memberOf=<Security_group_DN>)

- Múltiples grupos:

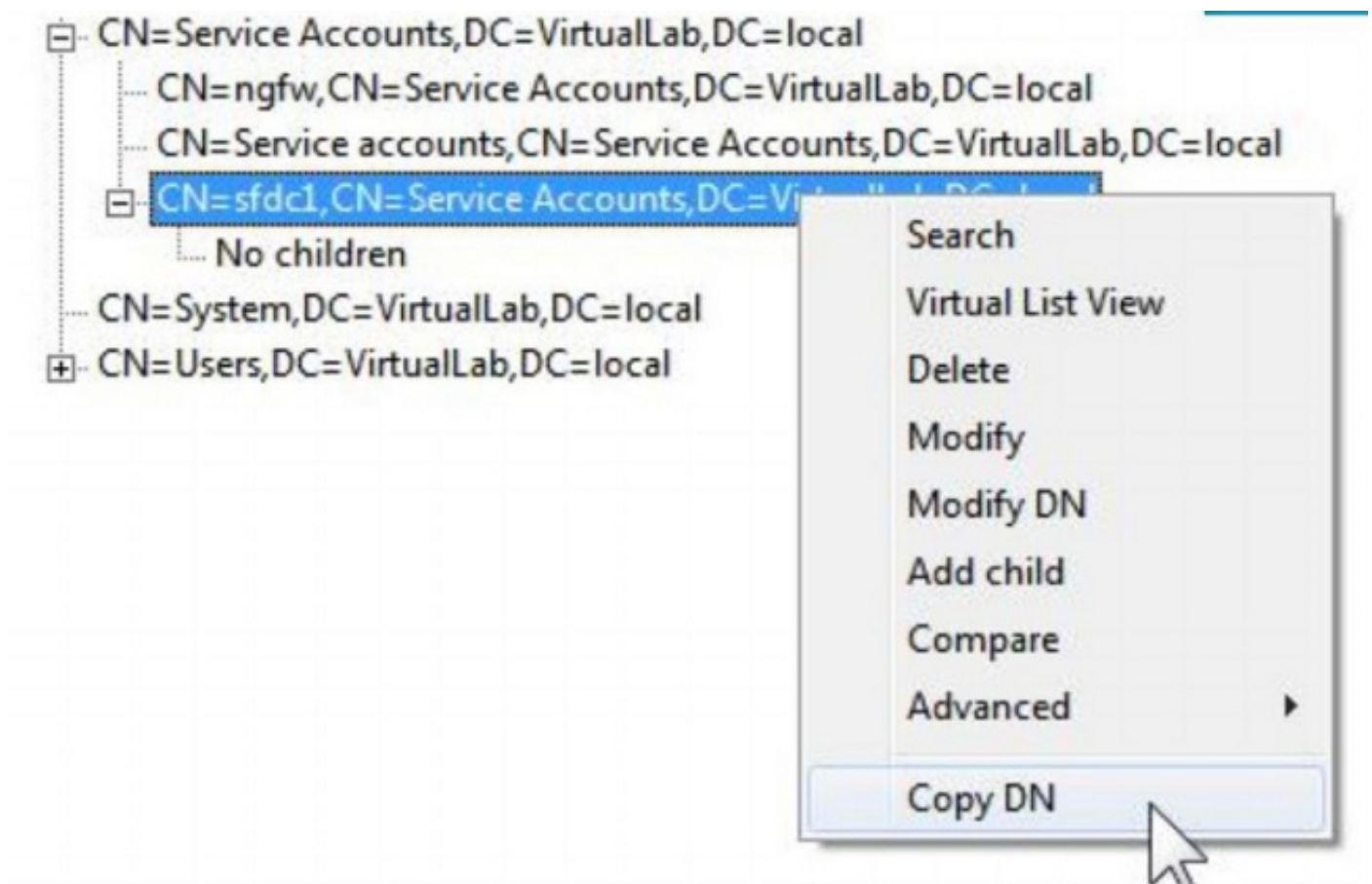
Filtro bajo:

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

En el siguiente ejemplo, observe que los usuarios AD tienen atributo del `memberOf` que corresponde con el filtro bajo. El atributo precedente del `memberOf` del número indica que el número de grupos el usuario es un miembro de. El usuario es un miembro de solamente un grupo de seguridad, los `secadmins`.

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

Paso 6: Navegue a las cuentas de usuario que usted quisiera utilizar como cuenta de la personalización en el objeto de la autenticación, y haga clic con el botón derecho del ratón en la cuenta de usuario **para copiar el DN**.



Utilice este DN para el **Nombre de usuario** en el objeto de la autenticación. Por ejemplo,

Nombre de usuario: `Cuentas CN=sfdc1,CN=Service, DC=VirtualLab, DC=local`

Similar para agrupar la búsqueda, es también posible buscar un usuario con el CN o el atributo específico tal como `name=sfdc1`.