Identifiez les attributs d'objet de LDAP de Répertoire actif pour la configuration d'objet d'authentification

Contenu

Introduction

Ce document décrit comment identifier des attributs d'objet de LDAP de Répertoire actif (AD) pour configurer l'objet d'authentification sur pour l'authentification externe.

Identifiez les attributs d'objet de LDAP

Avant de configurer un objet d'authentification à un centre de Gestion de FireSIGHT pour l'authentification externe, identifier les attributs de LDAP d'AD des utilisateurs et des groupes de sécurité serait nécessaire pour que l'authentification externe fonctionne comme prévu. Pour faire ainsi, nous pouvons utiliser Microsoft avons fourni le client de LDAP basé par GUI, le Ldp.exe, ou n'importe quel tiers navigateur de LDAP. En cet article, nous utiliserons ldp.exeto `localement` ou à distance connecter, lier, et parcourir le serveur d'AD et identifierons les attributs.

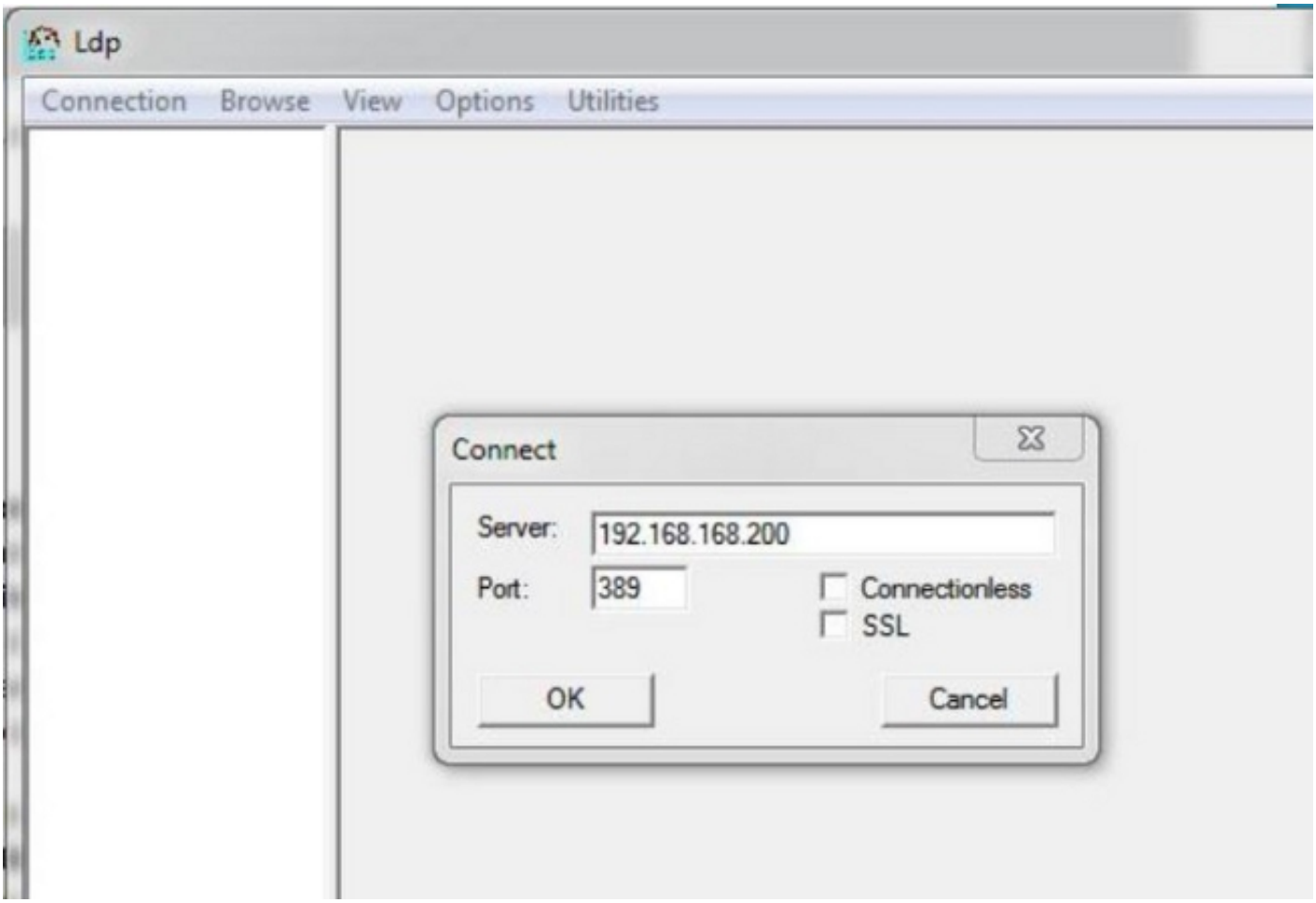
Étape 1 : `Application du` début `ldp.exe`. Allez au Startmenu et cliquez sur Run**. Le type** ldp.exeand **`a frappé le`** bouton CORRECT.

> Remarque: Sur les Windows Server 2008, `ldp.exe` est installé par défaut. Pour les Windows Server 2003 ou pour la connexion distante à partir de l'ordinateur de client Windows, téléchargez s'il vous plaît le `fichier` support.cabor `support.msi du` site de Microsoft. Extrayez le fileor .cab installent le passage ldp.exe de fileand .msi.

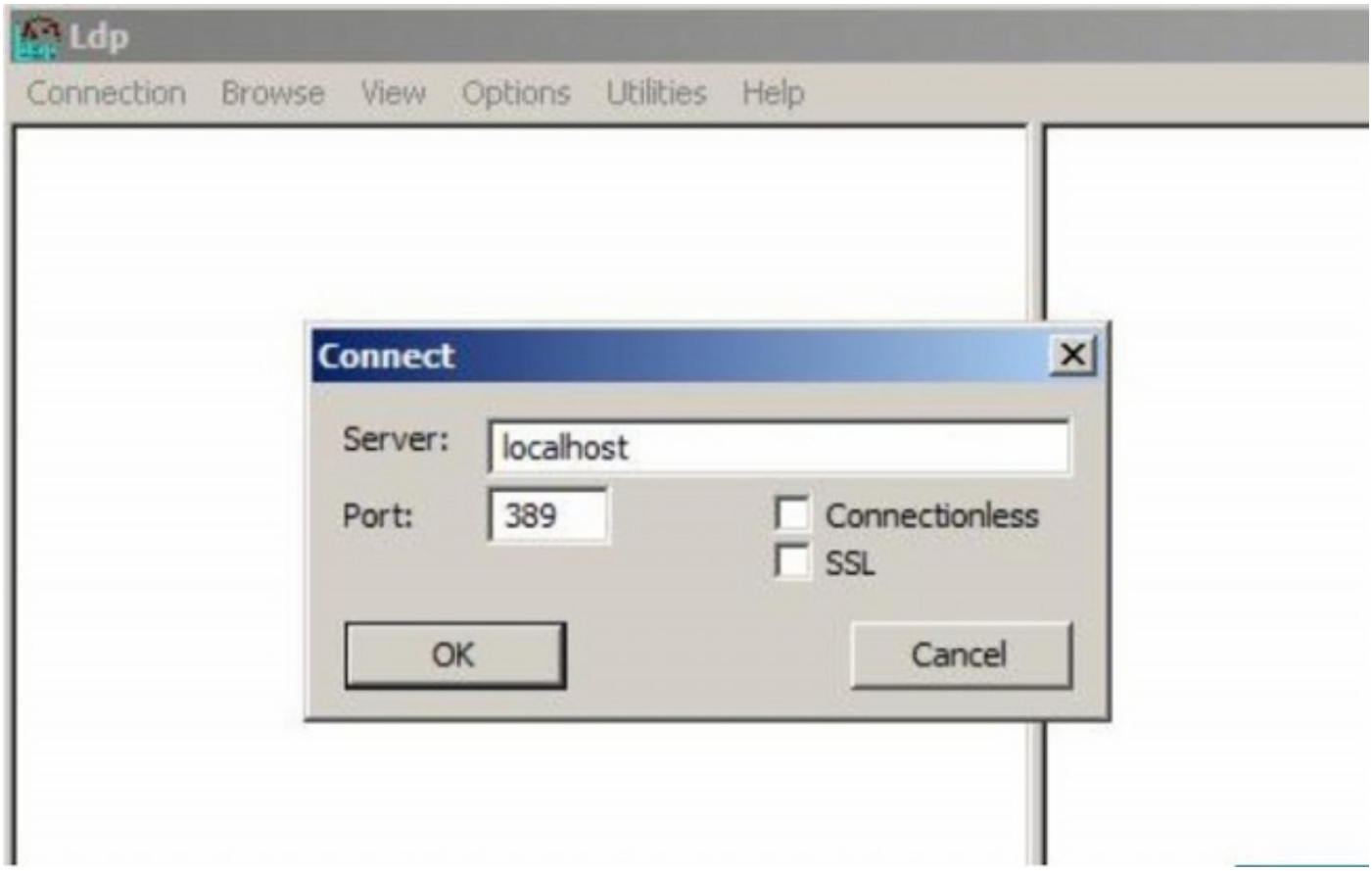
Étape 2 : Connectez au serveur. **La connexion** et le clic choisis **se connectent**.

- Pour connecter à l'AD un contrôleur de domaine (C.C) à partir d'un ordinateur local, écrivez l'adresse Internet ou l'adresse IP du serveur d'AD.
- Pour connecter à l'AD un C.C localement, écrivez le `localhost` comme **serveur**.

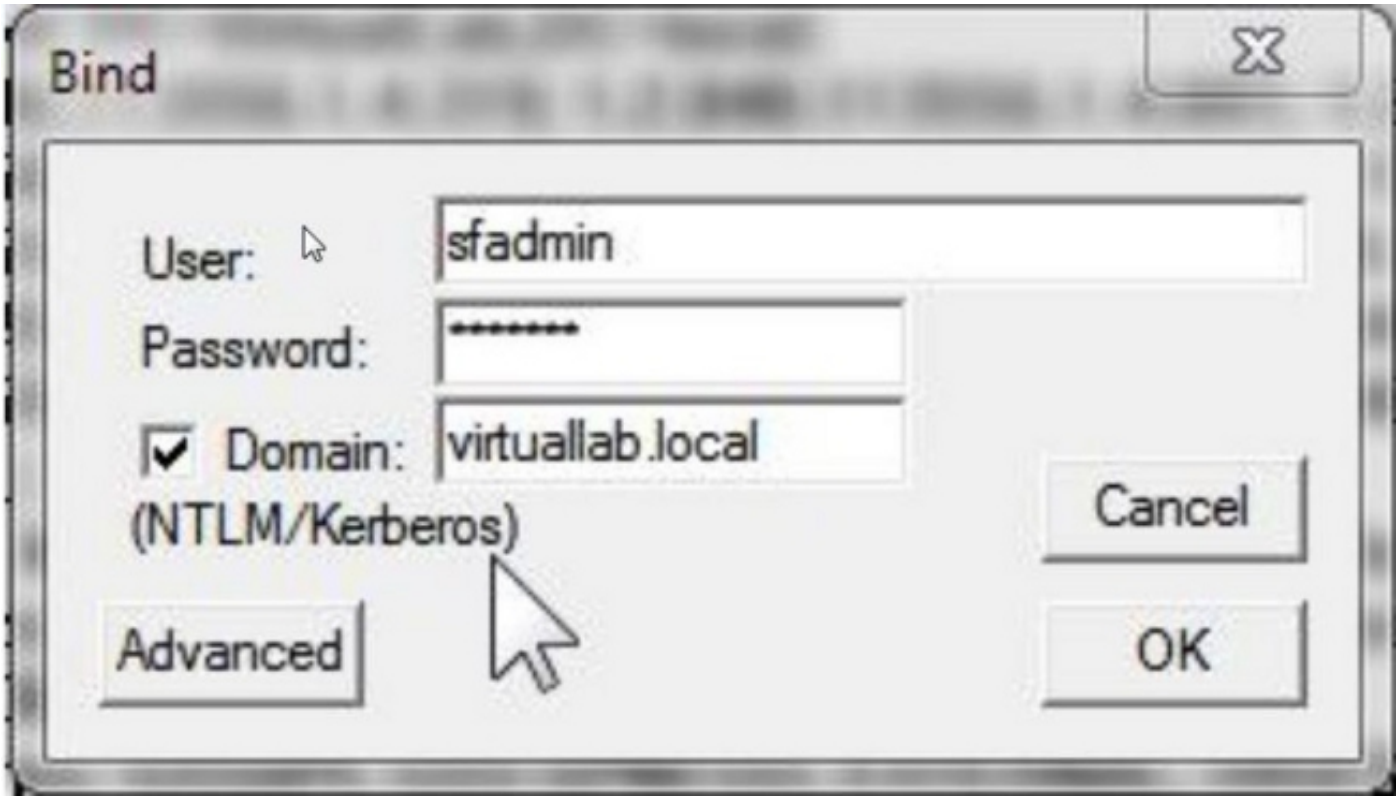
La connexion distante suivante d'expositions de tir d'écran d'un hôte de Windows :



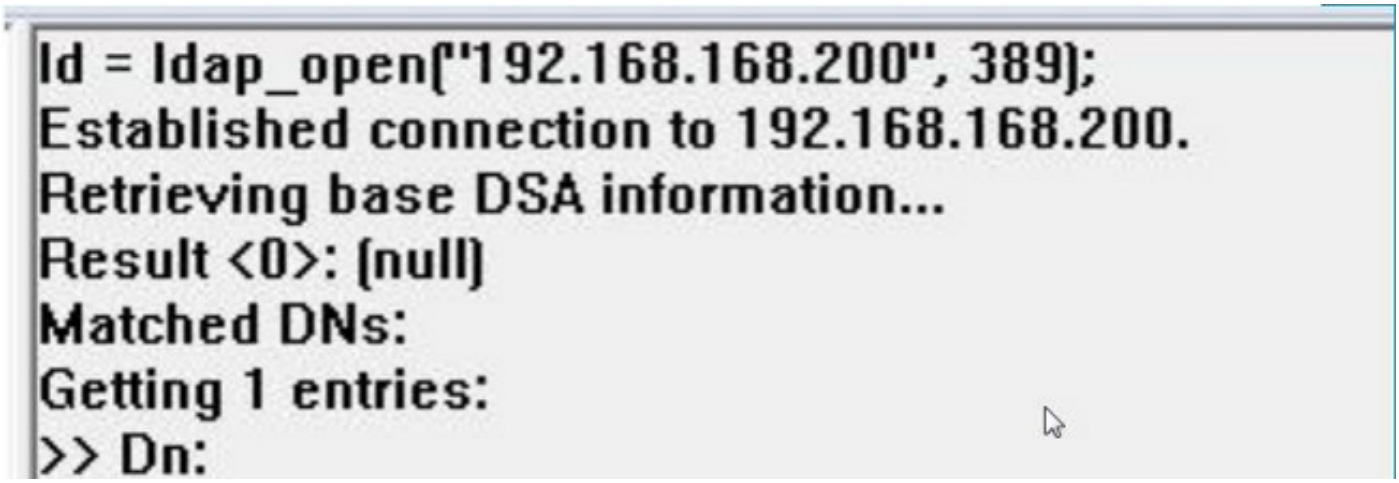
Le tir d'écran suivant affiche la connexion locale sur un C.C d'AD :



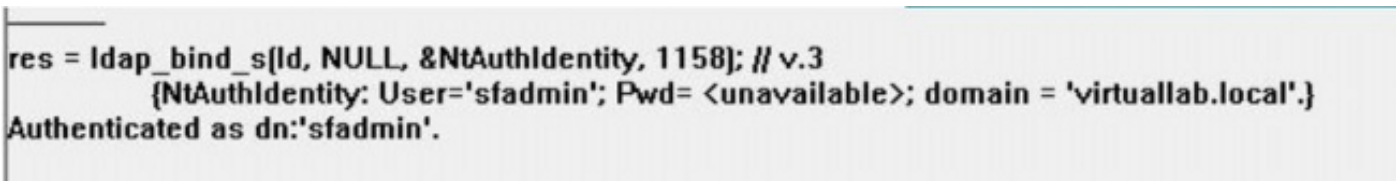
Étape 3. Grippage au C.C d'AD. Allez à la **connexion > au grippage**. Entrez dans l'**utilisateur**, le **mot de passe**, et le **domaine.** Cliquez sur **OK**.



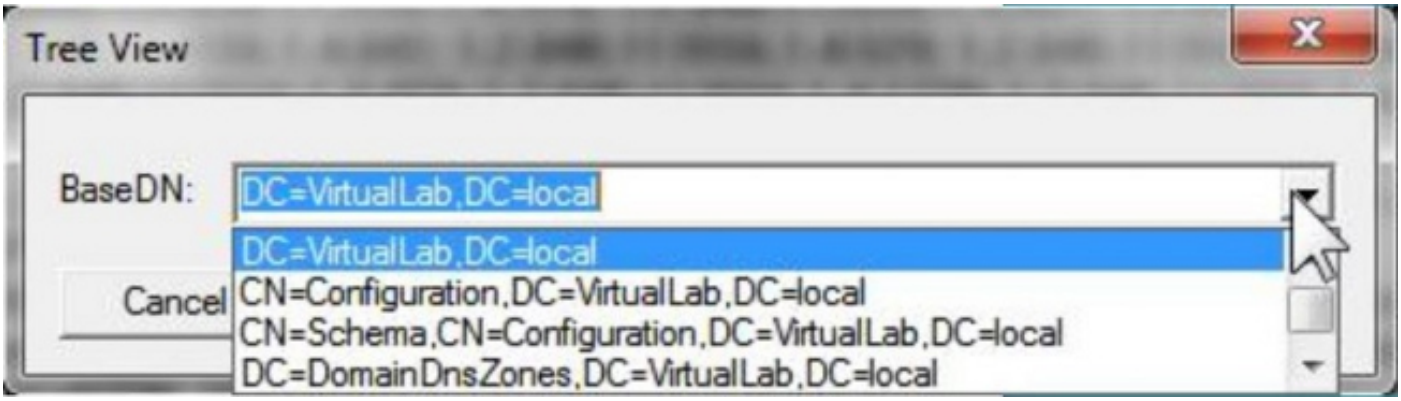
Quand une tentative de connexion est réussie, vous verrez un résultat comme ci-dessous :



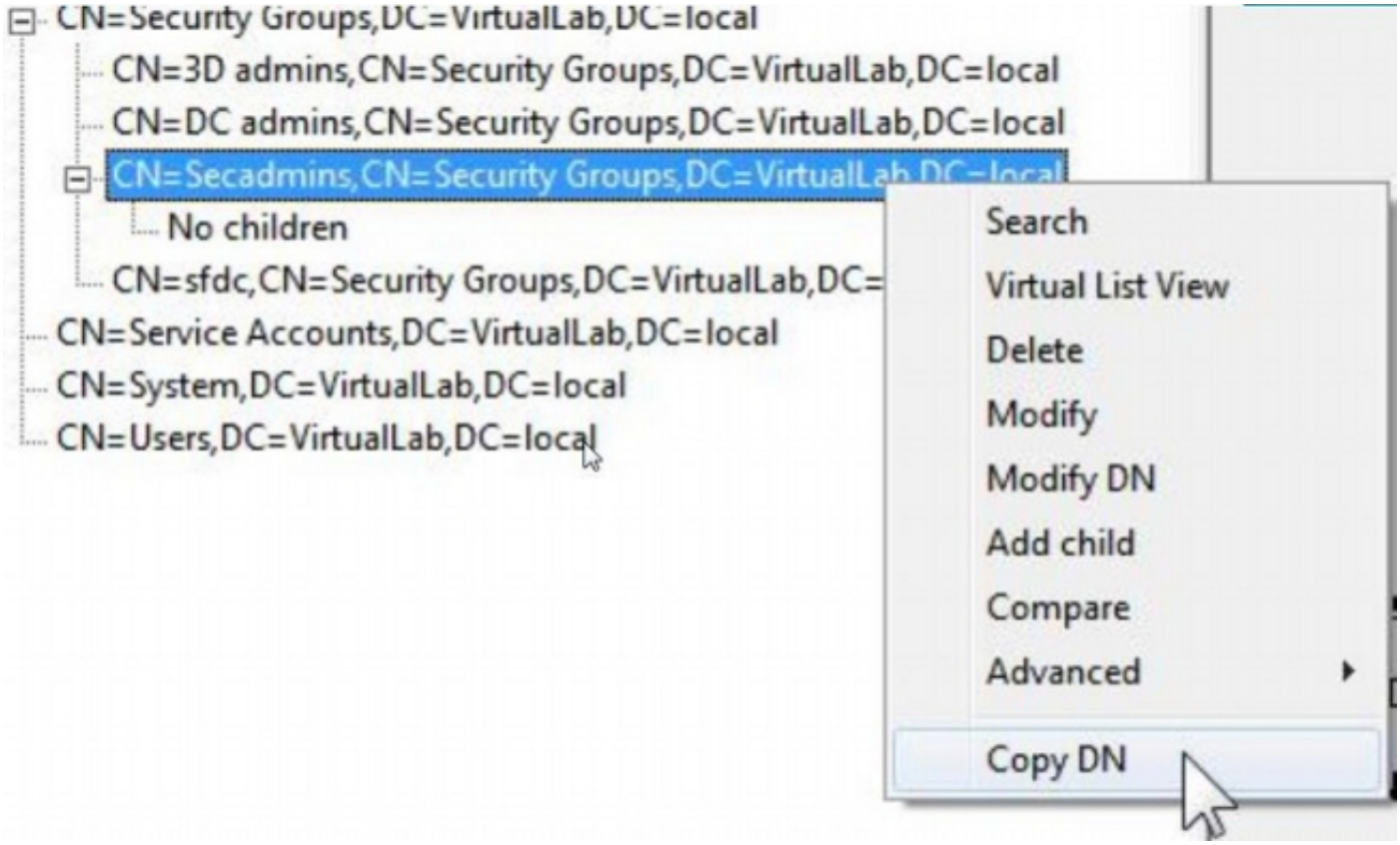
En outre, la sortie sur le volet gauche de `ldp.exe` affichera le grippage réussi au C.C d'AD.



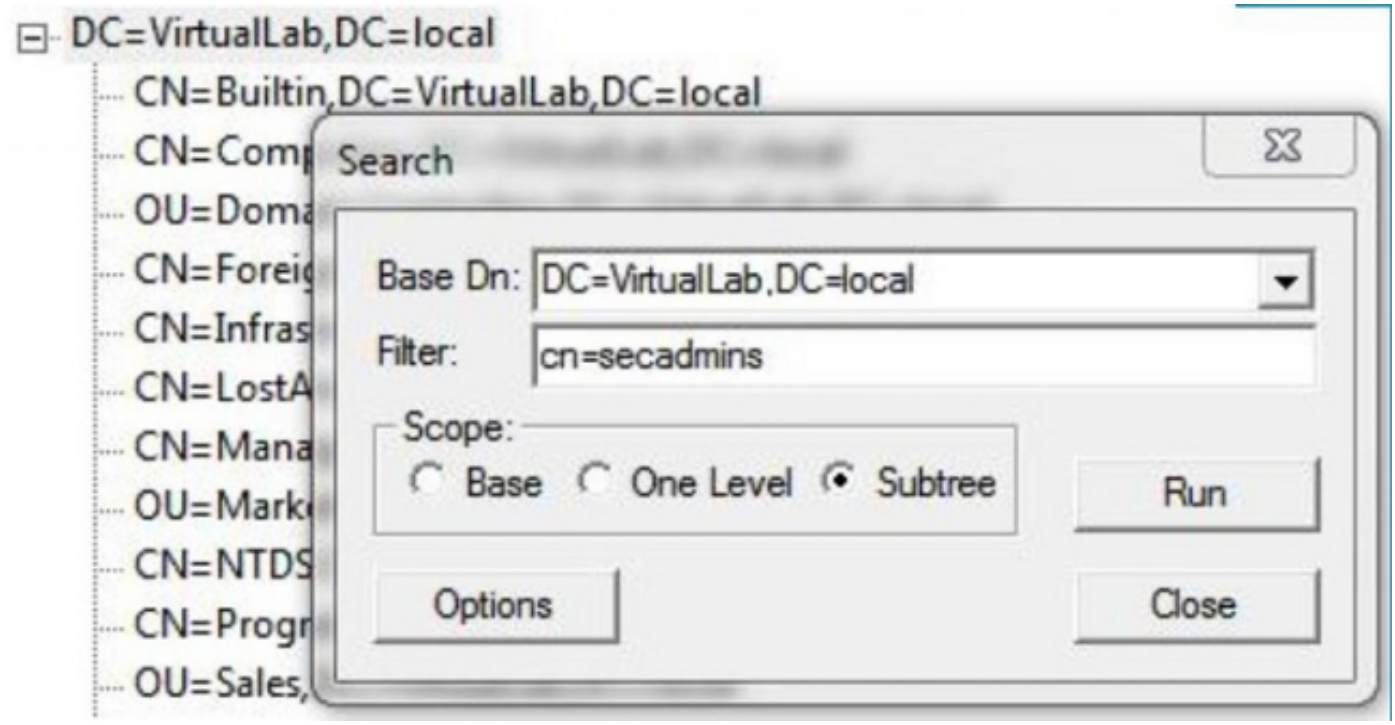
Étape 4 : Parcourez l'arborescence des répertoires. Cliquez sur la **vue > l'arborescence**, sélectionnez le **baseDN de** domaine de la liste déroulante, et cliquez sur OK. Ce DN de base est le DN qui est utilisé sur l'objet d'authentification.



Étape 5 : Sur le volet gauche de `ldp.exe, double-cliquer` sur les objets d'AD pour développer les conteneurs vers le bas au niveau des objets de feuille et naviguer vers le groupe de sécurité d'AD les utilisateurs sont membre de. Une fois que vous trouvez le groupe, cliquez avec le bouton droit sur le groupe et puis sélectionnez CopyDN.



Si vous n'êtes pas sûr dans quelle unité organisationnelle (OU) le groupe se trouve, cliquez avec le bouton droit sur le DN ou le domaine de base et sélectionnez la **recherche**. Une fois incité, entrez dans le ***name> de cn=<group*** comme filtre et le **sous-arbre** comme **portée**. Une fois que vous obtenez le résultat, vous pouvez alors copier l'attribut de DN du groupe. Il est également possible d'exécuter une recherche de masque telle que le **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;
```

Le filtre de base dans l'objet d'authentification devrait être en tant que ci-dessous :

- Seul groupe :

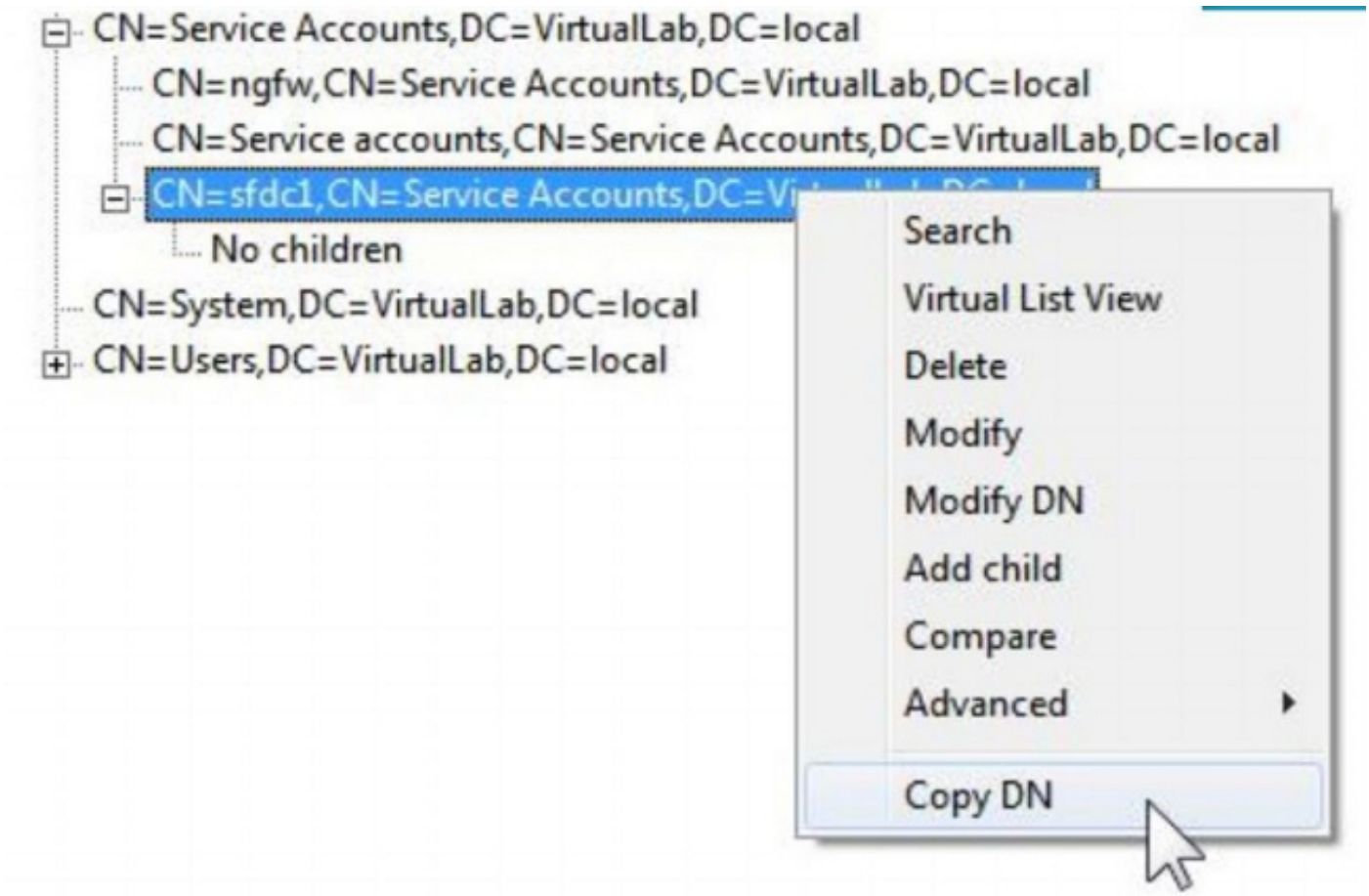
  Filtre de base : `(memberOf=<Security_group_DN>)`

- Plusieurs groupes :

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

Dans l'exemple suivant, notez que les utilisateurs d'AD ont l'attribut de `memberOf` appariant le filtre de base. L'attribut précédent de `memberOf de` nombre indiquent que le nombre de groupes l'utilisateur est un membre de. L'utilisateur est un membre de seulement un groupe de sécurité, des `secadmins`.

Étape 6 : Naviguez vers les comptes utilisateurs que vous voudriez utiliser comme compte de personnification dans l'objet d'authentification, et cliquez avec le bouton droit sur le compte utilisateur **pour copier le DN**.



Utilisez ce DN pour le **nom d'utilisateur** dans l'objet d'authentification. Exemple :

Nom d'utilisateur : `Comptes CN=sfdc1,CN=Service, DC=VirtualLab, DC=local`

Semblable pour grouper la recherche, il est également possible de rechercher un utilisateur avec la NC ou l'attribut spécifique tel que `name=sfdc1`.