認証オブジェクトに関する Active Directory LDAP オブジェクト属性の識別の設定

内容

概要

このドキュメントでは、外部認証用に認証オブジェクトを設定するための Active Directory (AD) LDAP オブジェクト属性を特定する方法について説明します。

LDAP オブジェクト属性の識別

外部認証用に FireSIGHT Management Center で Authentication Object を設定する前に、外部認証が意図したとおりに動作するためにユーザおよびセキュリティ グループの AD LDAP 属性を識別する必要があります。この目的で、Microsoft が提供する GUI ベースの LDAP クライアントである Ldp.exe、またはサードパティの LDAP ブラウザを使用することができます。この記事では、ldp.exeを使用してローカルまたはリモートでADサーバに接続、バインド、および参照し、属性を特定します。

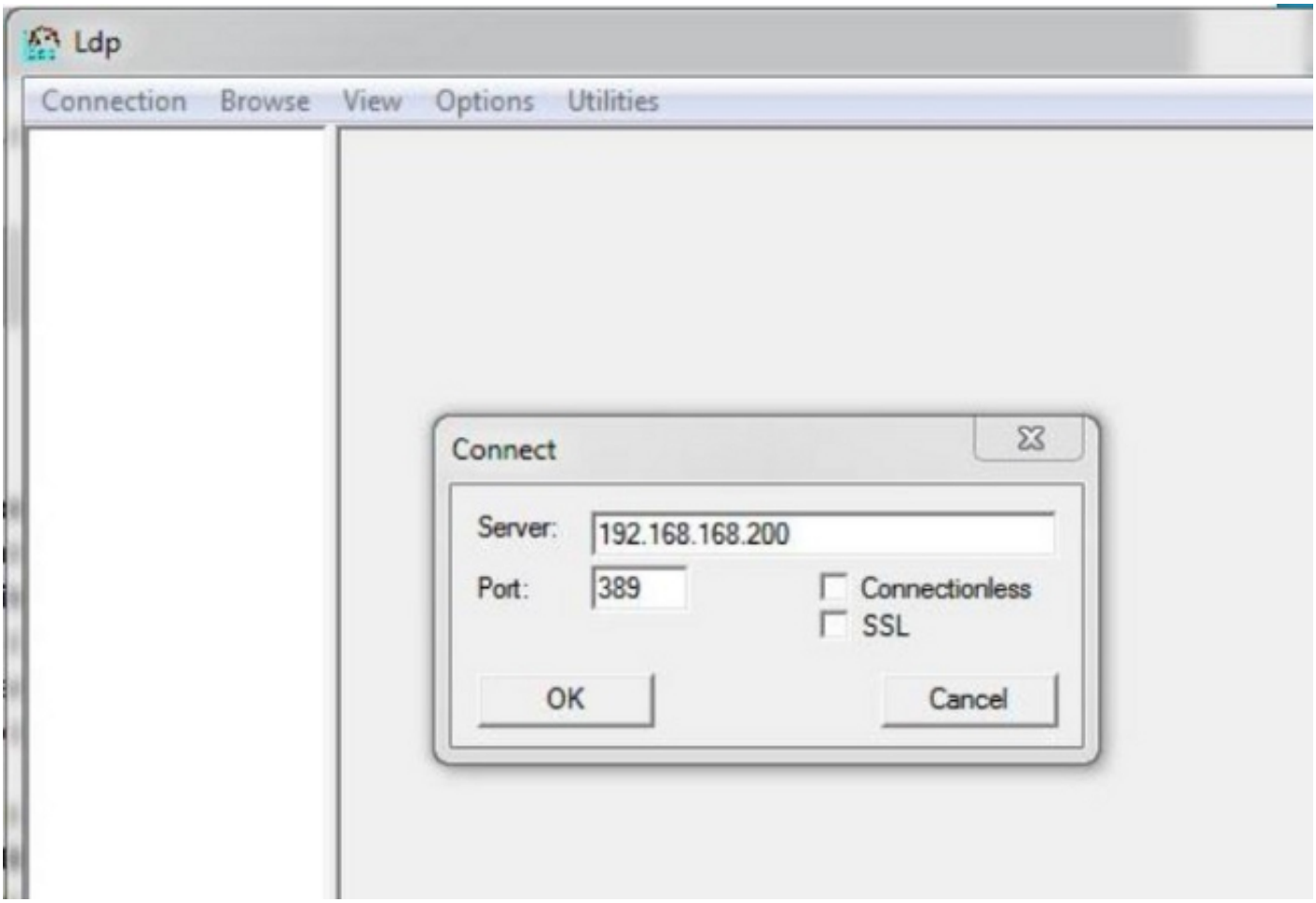
ステップ 1 : ldp.exe アプリケーションを起動します。[スタートメニュー (Start)] メニューから [実行 (Run)] を選択します。**ldp.exe**と入力し、**OK**ボタンを押します。

> **注：**Windows Server 2008 では、ldp.exe はデフォルトでインストールされています。Windows Server 2003の場合、またはWindowsクライアントコンピュータからのリモート接続の場合は、Microsoftサイトからsupport.cabまたはsupport.msiファイルをダウンロードしてください。.cabファイルを展開するか、.msiファイルをインストールしてldp.exeを実行します。

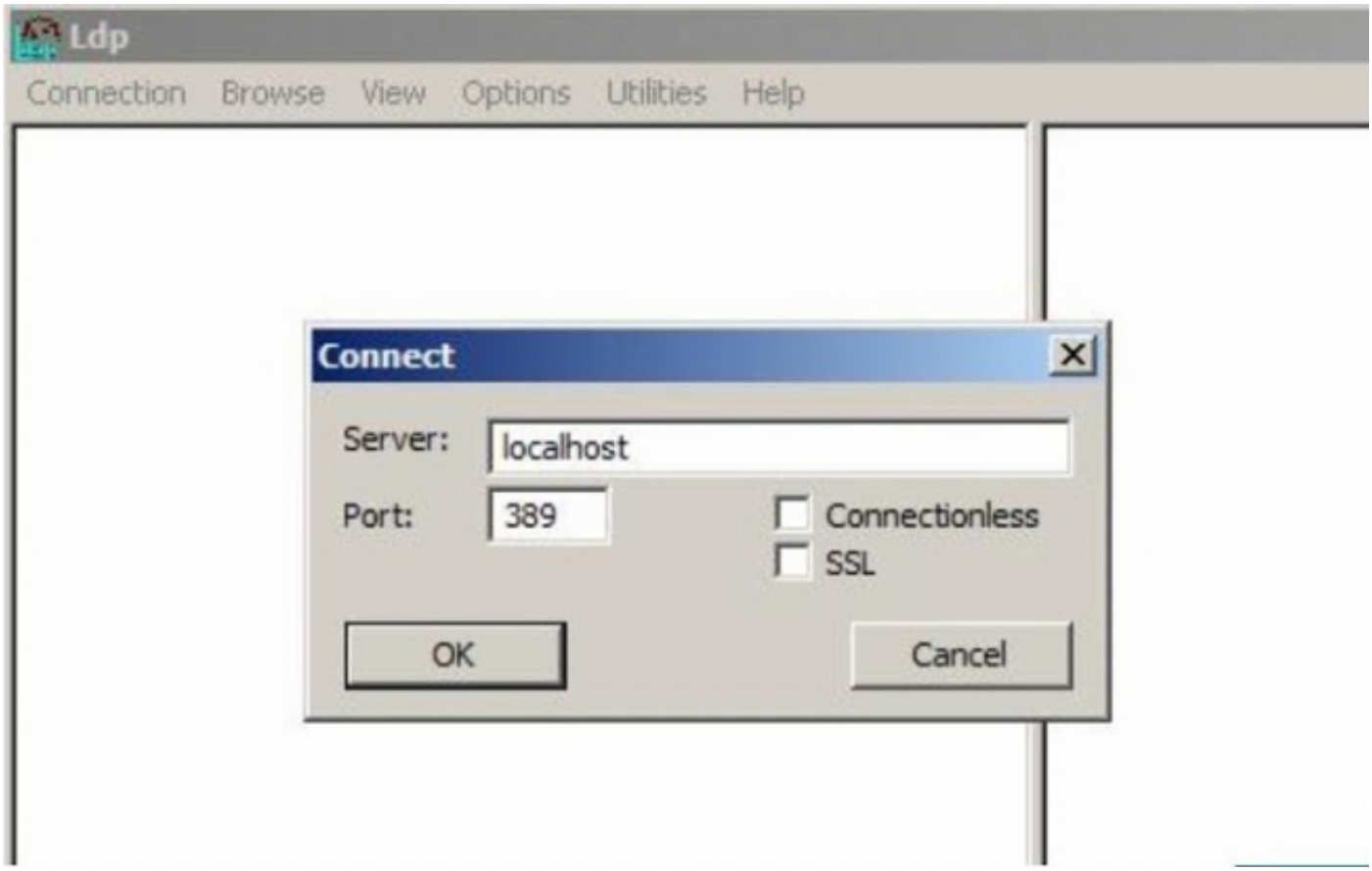
ステップ 2 : サーバに接続します。[Connection] を選択して [Connect] をクリックします。

- ローカル コンピュータから AD のドメイン コントローラ (DC) に接続するには、AD サーバのホスト名または IP アドレスを入力します。
- AD DC にローカルに接続するには、[Server] **に** localhost を入力します。

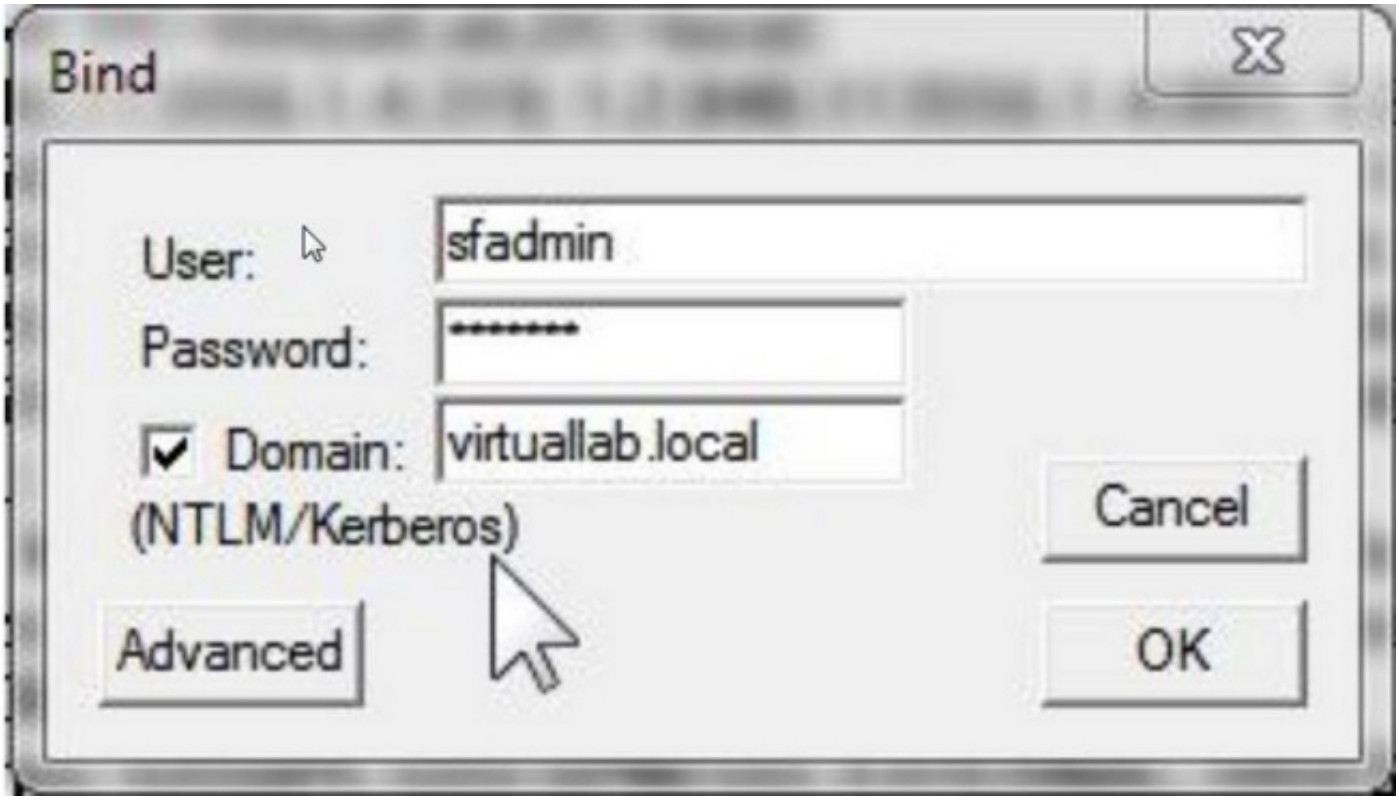
次のスクリーンショットは、Windows ホストからのリモート接続を示しています。



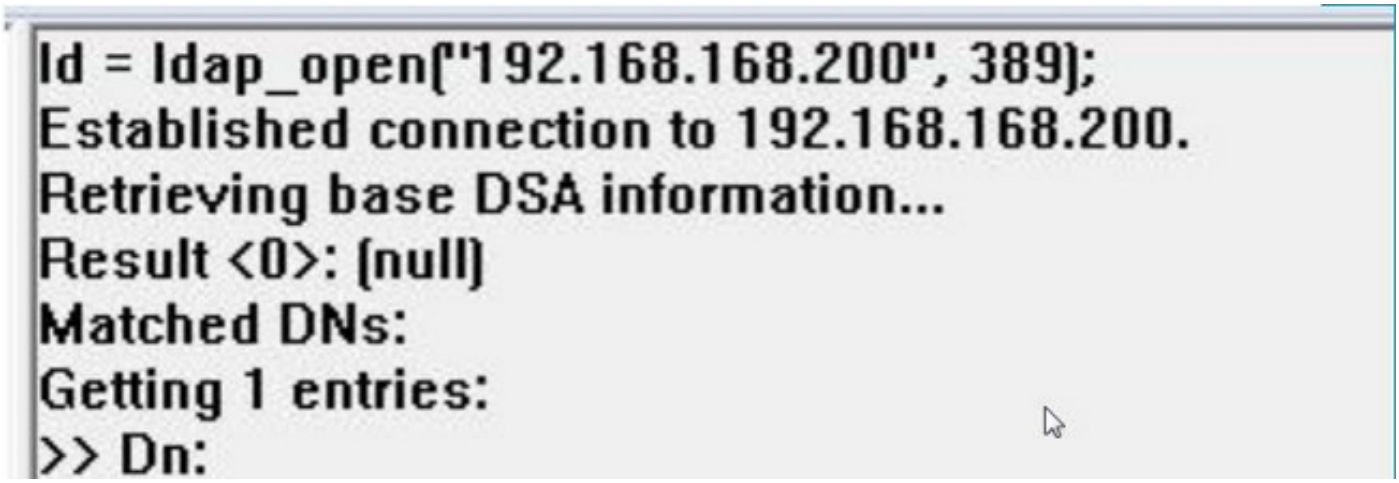
次のスクリーンショットは、AD DC のローカル接続を示しています。



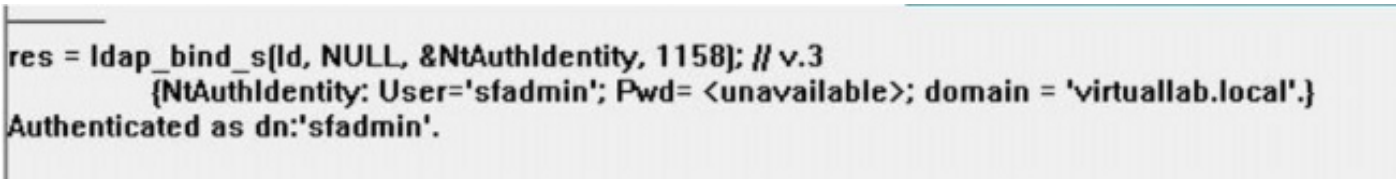
ステップ 3 : AD DC へバインドします。[Connection] > [Bind] を選択します。[User]、[Password]、および [Domain] **に入力します。**[OK] をクリックします。



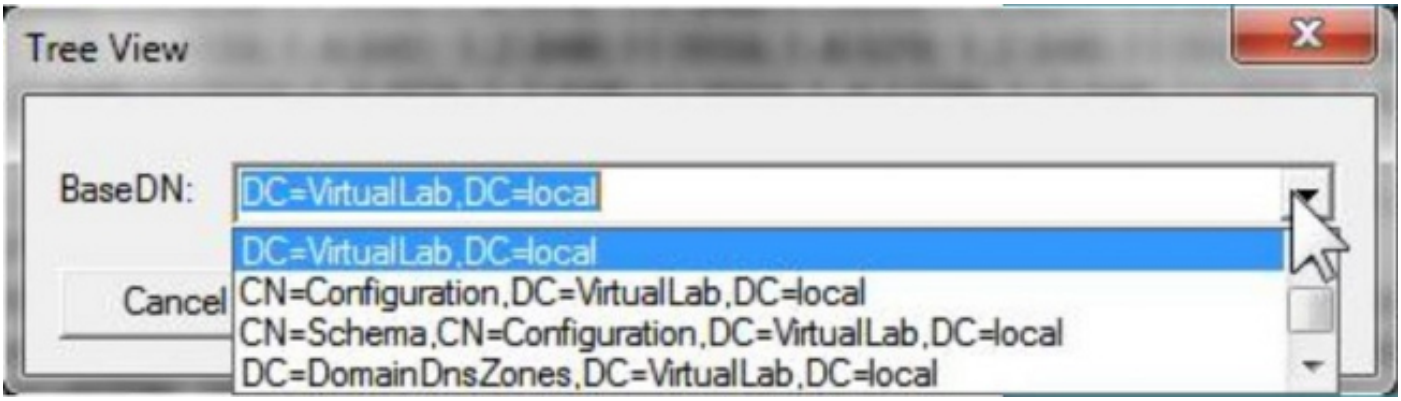
接続の試行が成功すると、次のような出力が表示されます。



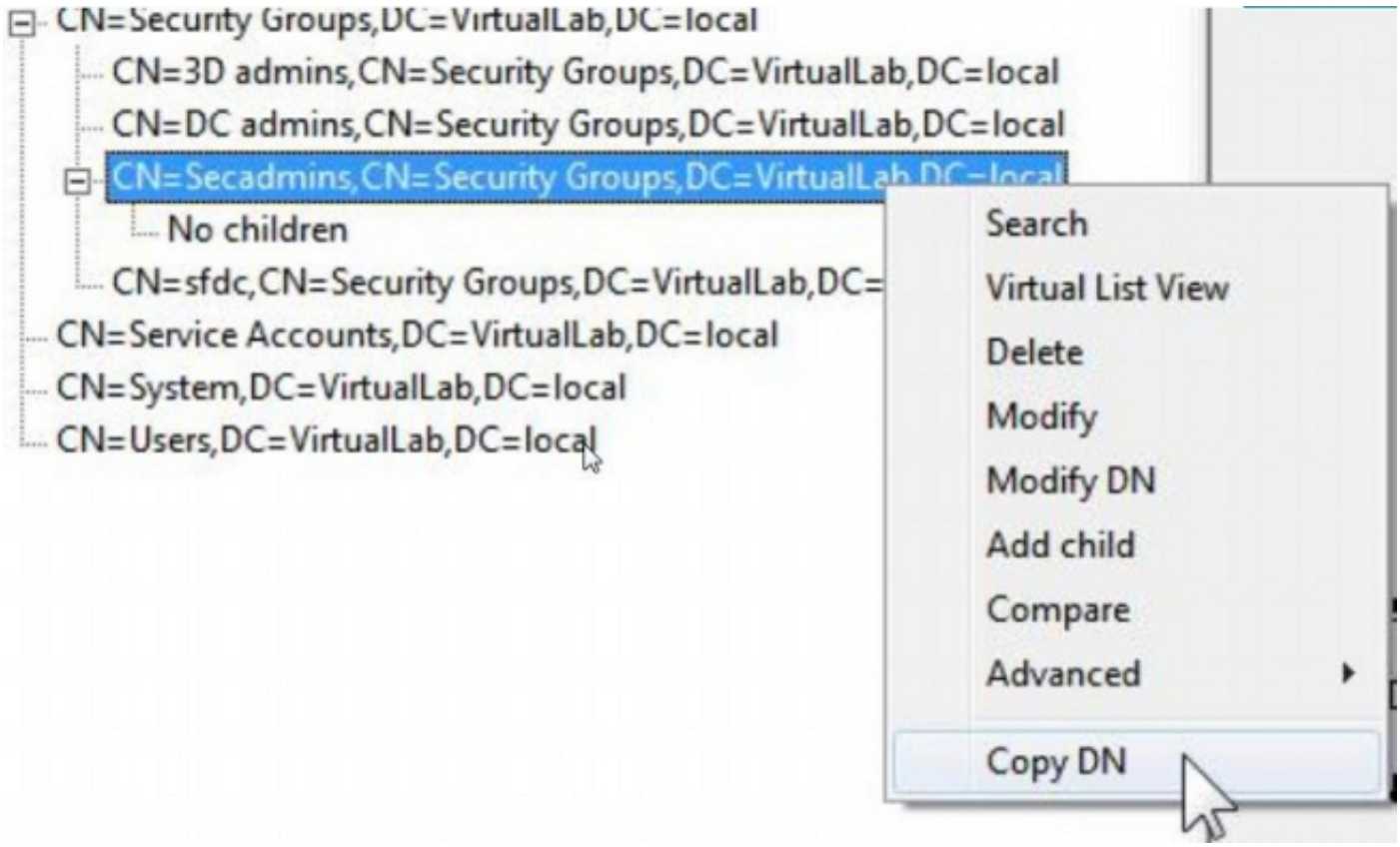
また、ldp.exe の左側のペインの出力には、AD DC へのバインドが成功したことが表示されます。



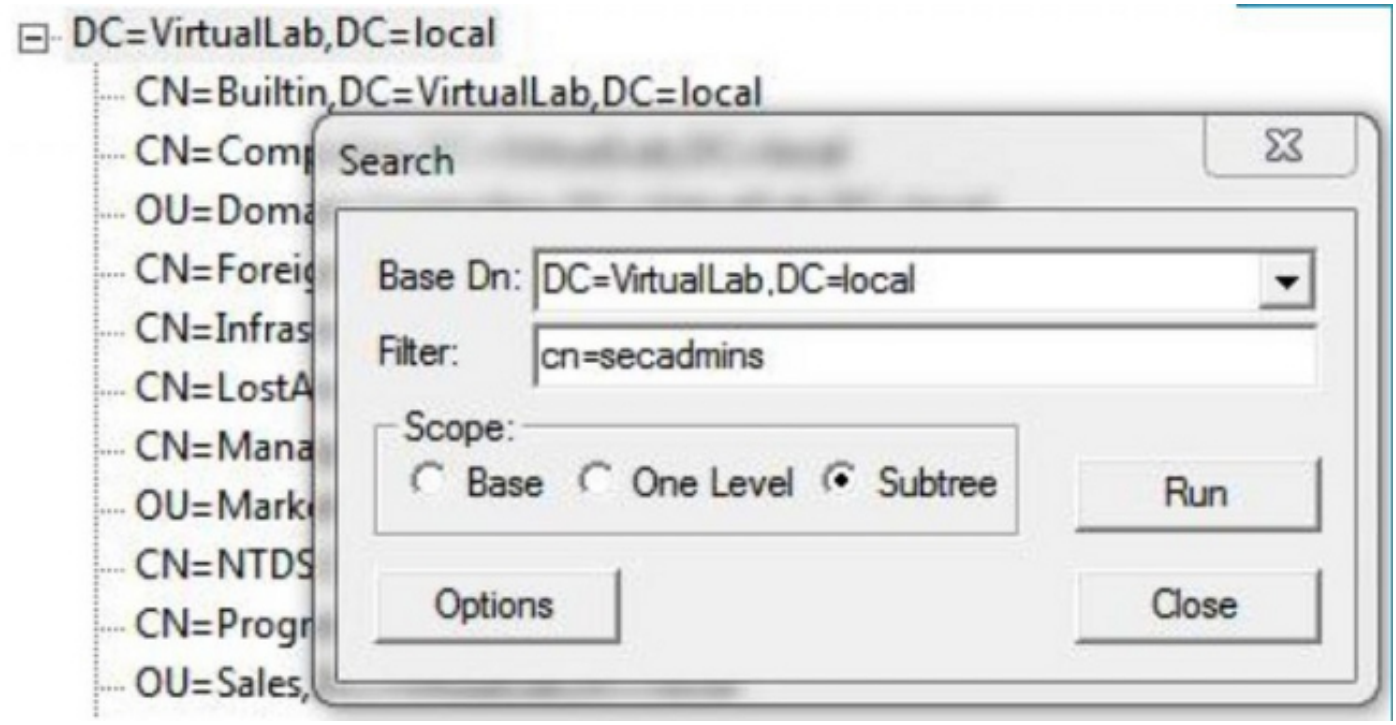
ステップ 4 : ディレクトリ ツリーを参照します。[View] > [Tree] をクリックしてドロップダウン リストから BaseDN **ドメインを選択し、[OK] をクリックします。**この Base DN は、Authentication Object で使用される DN です。



ステップ 5 : ldp.exe の左側のペインで AD オブジェクトをダブルクリックし、リーフ オブジェクトのレベルまでコンテナを展開して、対象ユーザが属している AD セキュリティ グループにナビゲートします。グループが見つかったら、そのグループを右クリックして、**Copy DN**を選択します。



グループがどの組織ユニット（OU）に属しているかわからない場合は、[Base DN] または [Domain] を右クリックして [Search] を選択します。プロンプトが表示されたら、[Filter] に **cn=<group name> と入力し、[Scope] で** [Subtree] を選択します。結果が表示されたら、グループの DN 属性をコピーすることができます。**cn=*admin* のようにワイルドカード検索を実行することもできます。**




```
***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;
```

Authentication Object の基本フィルタは、次のようになっています。

- 1 つのグループ：

  基本フィルタ：(memberOf=<Security_group_DN>)

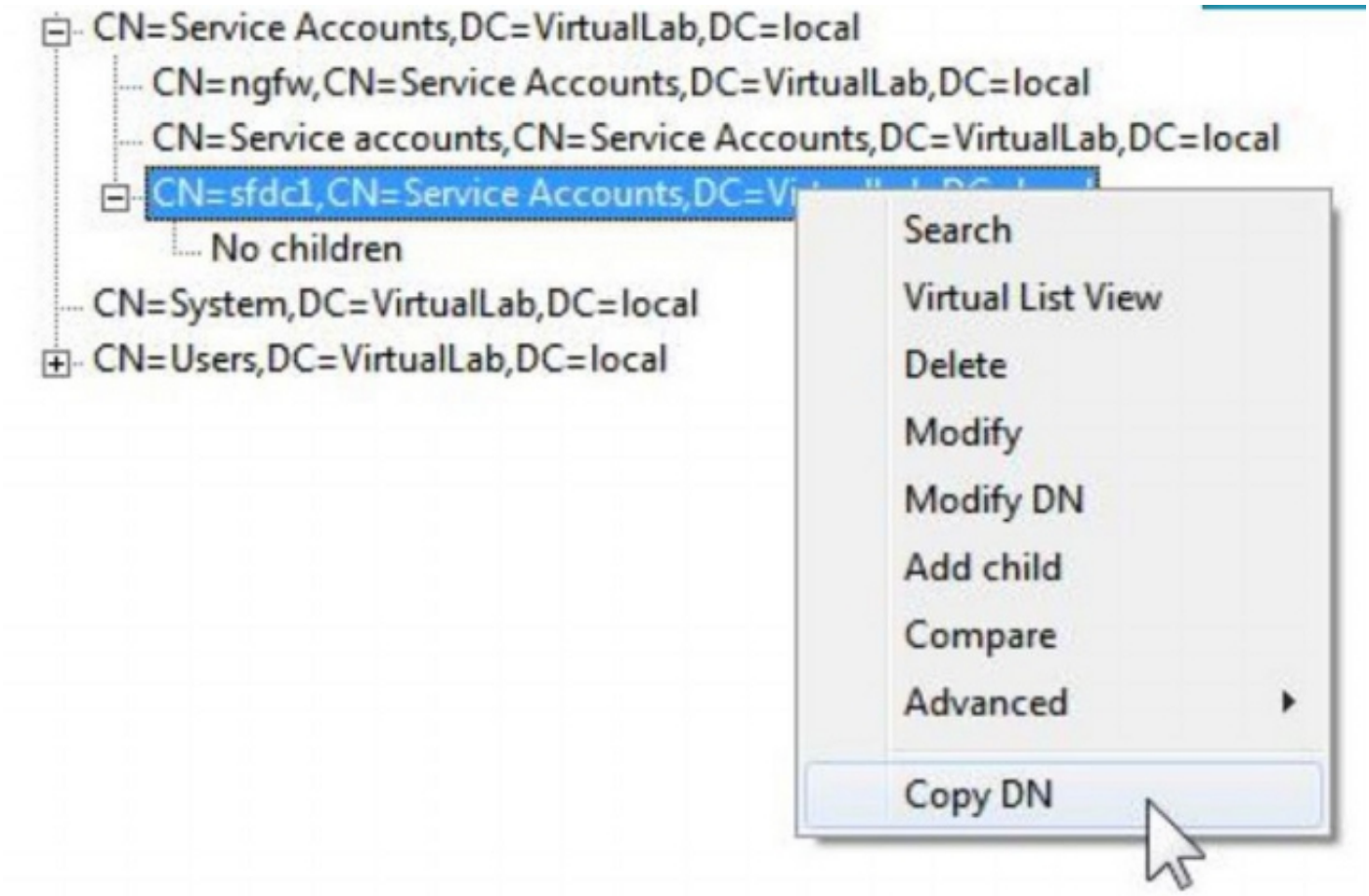
- 複数のグループ：

  基本フィルタ
  ：(|(memberOf=<group1_DN>)(memberOf=<group2_DN>)(memberOf=<groupN_DN))

次の例では、AD ユーザが、基本フィルタと一致する memberOf 属性を持っていることに注意してください。memberOf 属性の前にある数字は、ユーザが属しているグループの番号を示しています。ユーザは、1 つのセキュリティ グループ secadmins だけのメンバーです。

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

ステップ 6 : Authentication Object で偽装アカウントとして使用するユーザ アカウントにナビゲートし、そのユーザ アカウントを右クリックして [Copy DN] を選択します。



Authentication Object で、[User Name] **としてこの DN を使用します。**たとえば、

ユーザ名：CN=sfdc1,CN=Service Accounts,DC=VirtualLab,DC=local

グループ検索と同様に、CN のユーザを検索することも、name=sfdc1 などの特別な属性のユーザを検索することもできます。