Identificare gli attributi dell'oggetto LDAP di Active Directory per la configurazione dell'oggetto di autenticazione

Sommario

[Introduzione](#)
[Identifica attributi oggetto LDAP](#)

Introduzione

In questo documento viene descritto come identificare gli attributi dell'oggetto LDAP di Active Directory (AD) per configurare l'oggetto di autenticazione in per l'autenticazione esterna.

Identifica attributi oggetto LDAP

Prima di configurare un oggetto di autenticazione su un centro di gestione FireSIGHT per l'autenticazione esterna, l'identificazione degli attributi LDAP di AD di utenti e gruppi di sicurezza è necessaria affinché l'autenticazione esterna funzioni come previsto. A tale scopo, è possibile utilizzare il client LDAP basato su GUI fornito da Microsoft, Ldp.exe o qualsiasi browser LDAP di terze parti. In questo articolo verrà utilizzato ldp.exe per connettersi, associare e sfogliare il server AD in locale o in remoto e identificare gli attributi.

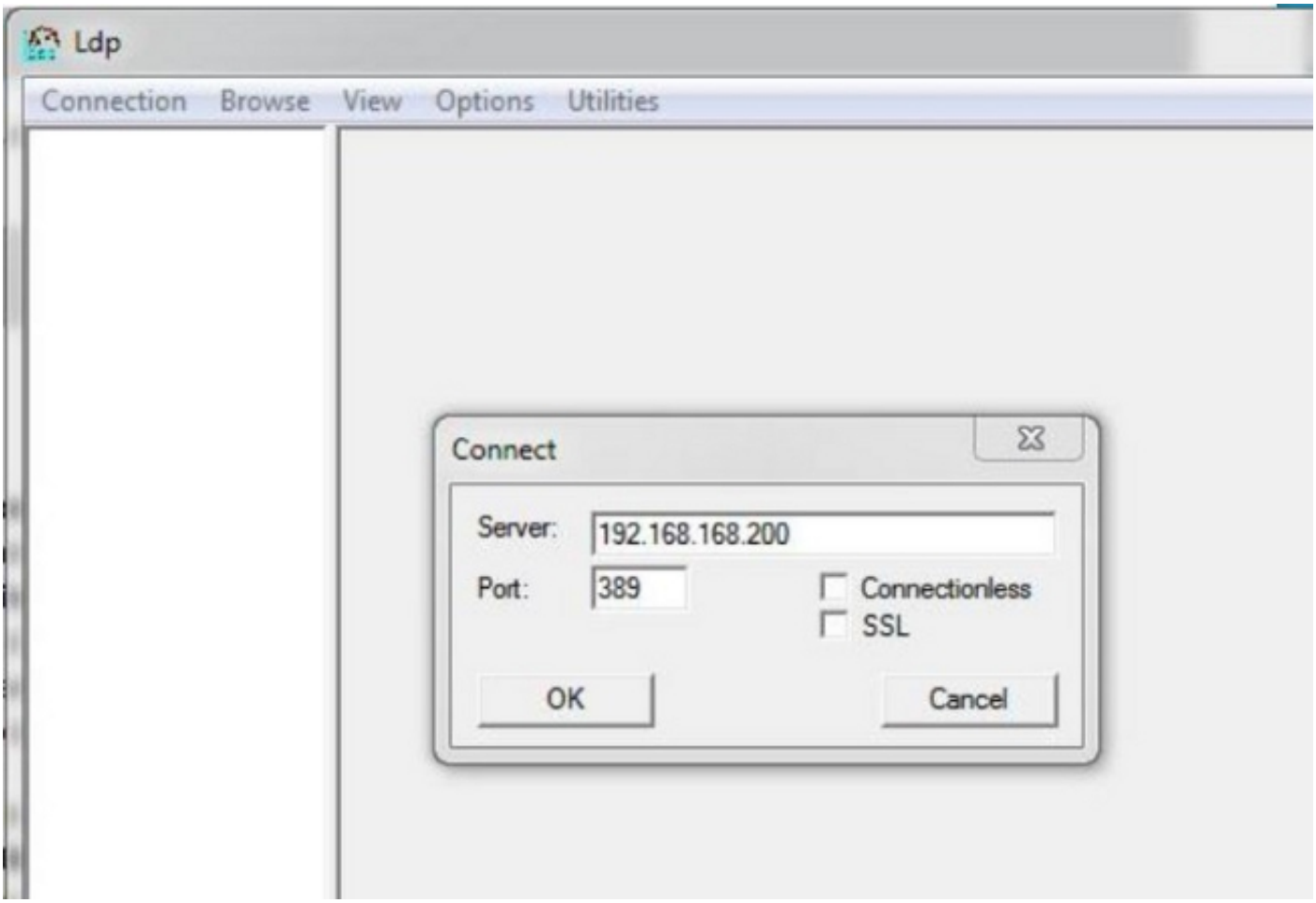
Passaggio 1: Avviare l'applicazione ldp.exe. Andare al menu **Start** e fare clic su **Esegui**. Digitare **ldp.exe** e fare clic sul pulsante **OK**.

> **Nota:** In Windows Server 2008, ldp.exe è installato per impostazione predefinita. Per Windows Server 2003 o per la connessione remota dal computer client Windows, scaricare il file support.cab o support.msi dal sito Microsoft. Estrarre il file .cab o installare il file .msi ed eseguire ldp.exe.

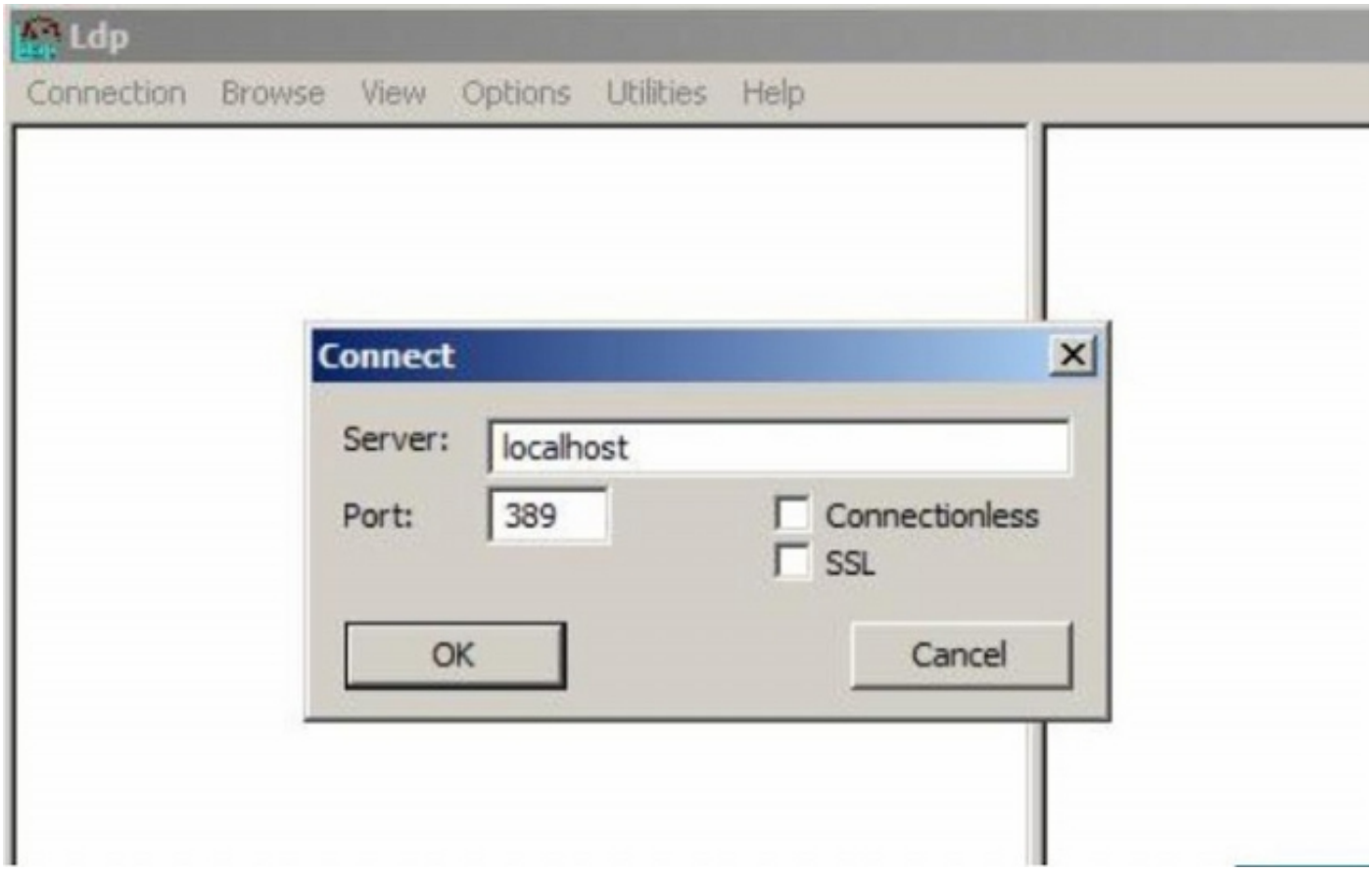
Passaggio 2: Connettersi al server. Selezionare **Connessione** e fare clic su **Connetti**.

- Per connettersi a un controller di dominio Active Directory da un computer locale, immettere il nome host o l'indirizzo IP del server Active Directory.
- Per connettersi localmente a un controller di dominio Active Directory, immettere localhost come **Server**.

Nello screenshot seguente viene illustrata la connessione remota da un host Windows:

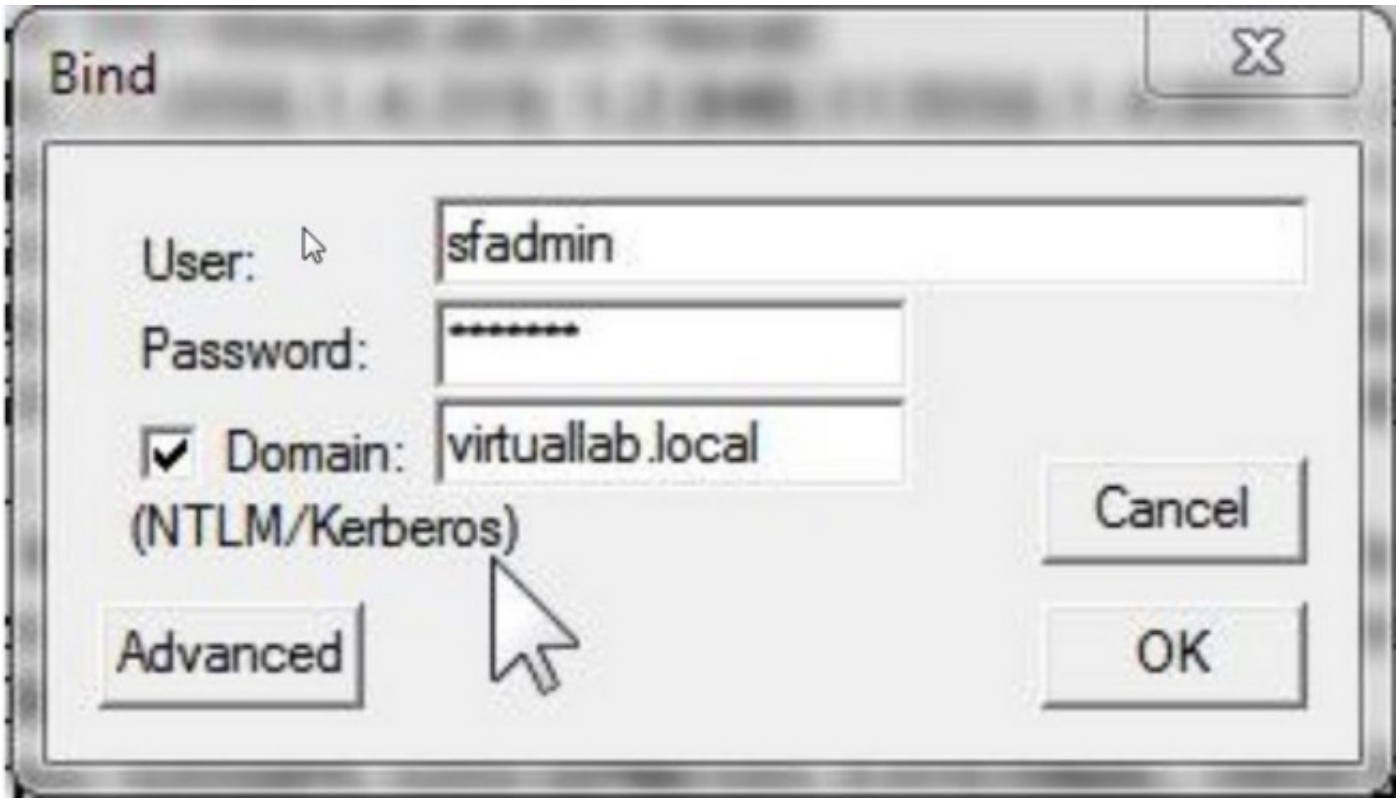


Nello screenshot seguente viene illustrata la connessione locale in un controller di dominio Active Directory:

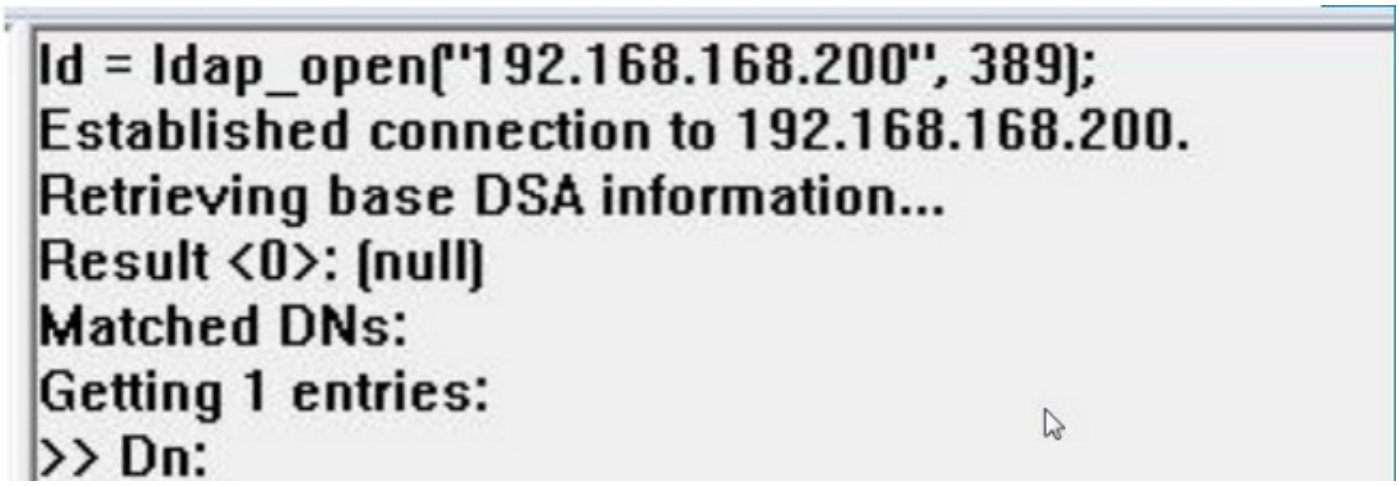


Passaggio 3. Eseguire il binding al controller di dominio Active Directory. Selezionare **Connessione >**

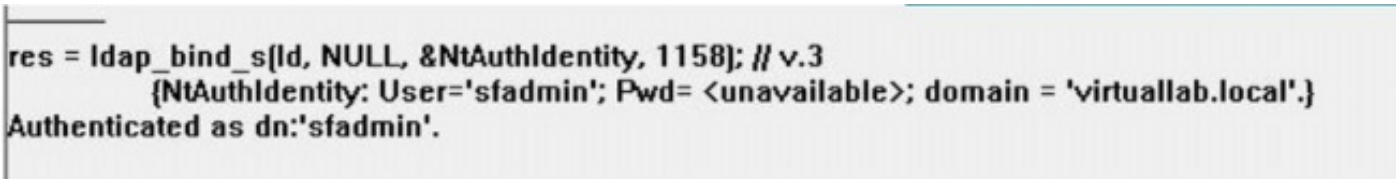
Binding. Immettere **User**, **Password** e **Domain.** Fare clic su **OK**.



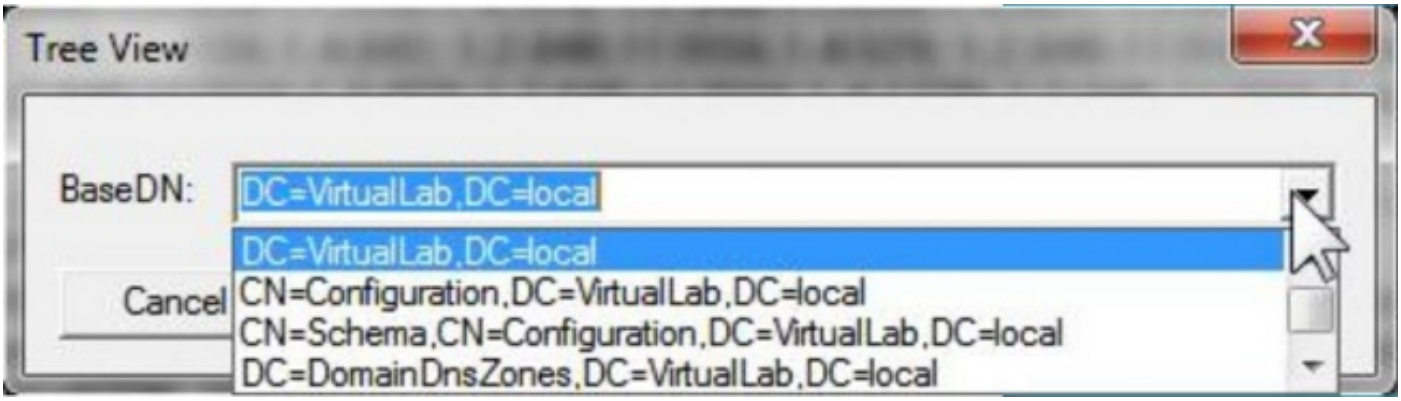
Quando un tentativo di connessione riesce, viene visualizzato un output simile al seguente:



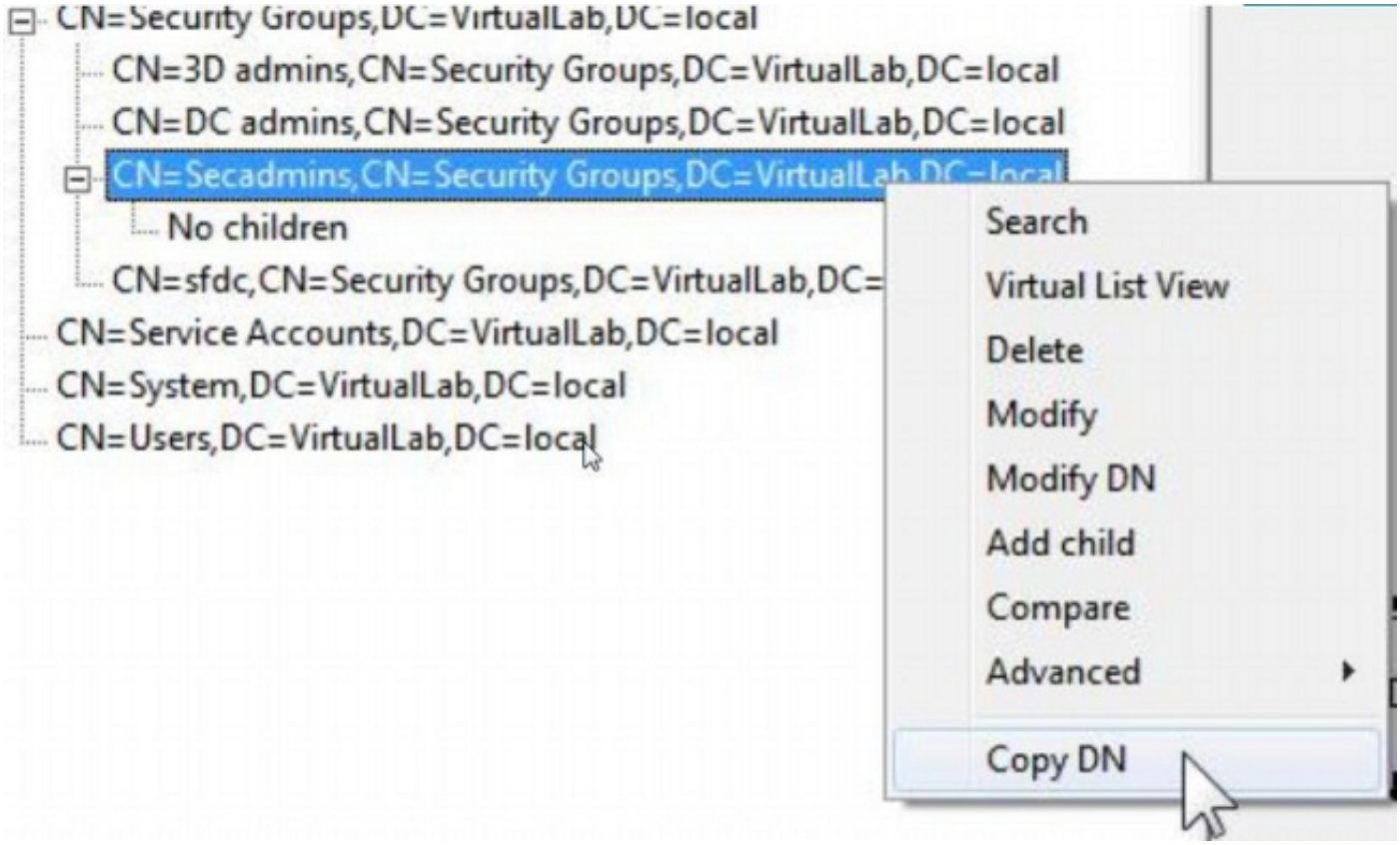
Inoltre, l'output nel riquadro sinistro di ldp.exe mostrerà il binding al controller di dominio Active Directory.



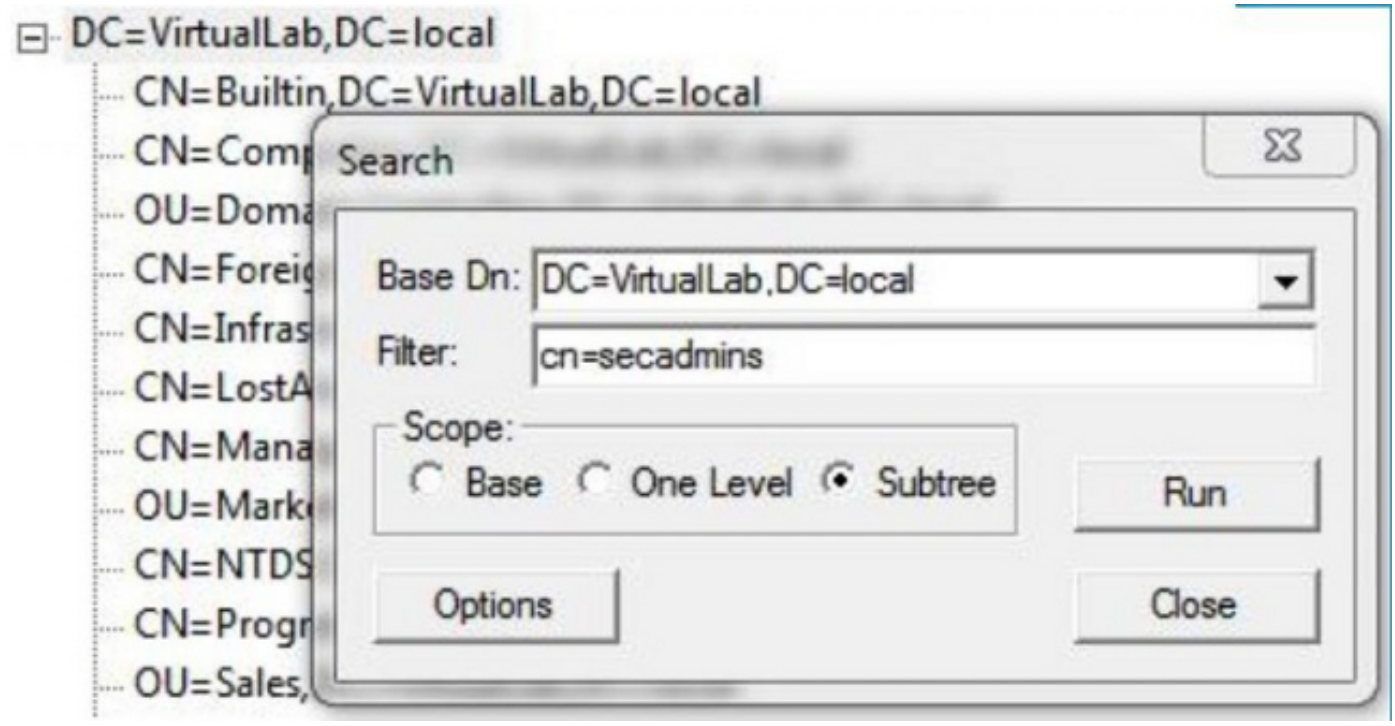
Passaggio 4: Esplorare la struttura delle directory. Fare clic su **Visualizza > Albero** , selezionare il dominio **BaseDN** dall'elenco a discesa e fare clic su **OK**. Questo DN di base è il DN utilizzato nell'oggetto di autenticazione.



Passaggio 5: Nel riquadro sinistro di ldp.exe, fare doppio clic sugli oggetti AD per espandere i contenitori fino al livello degli oggetti foglia e passare al gruppo di sicurezza AD di cui gli utenti sono membri. Una volta trovato il gruppo, fare clic con il pulsante destro del mouse sul gruppo e selezionare **Copia DN**.



Se non si è certi dell'unità organizzativa in cui si trova il gruppo, fare clic con il pulsante destro del mouse sul DN di base o sul Dominio e selezionare **Cerca**. Quando richiesto, immettere **cn=*<nome gruppo>*** come filtro e **Subtree** come **ambito**. Una volta ottenuto il risultato, è possibile copiare l'attributo DN del gruppo. È inoltre possibile eseguire una ricerca con caratteri jolly, ad esempio **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;
```

Il filtro di base nell'oggetto di autenticazione deve essere il seguente:

- Gruppo singolo:

  Filtro di base: (memberOf=<DN_gruppo_protezione>)

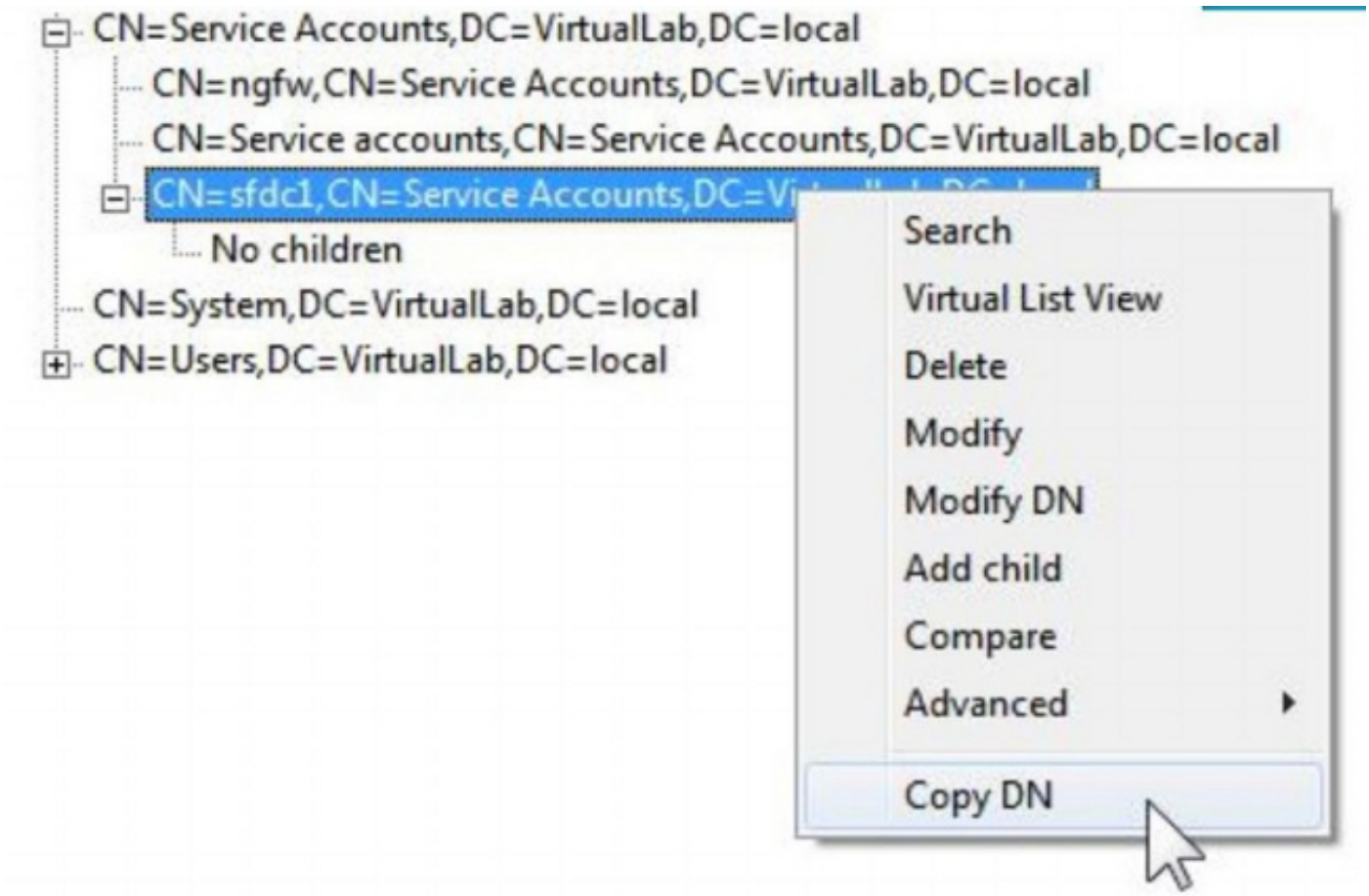
- Più gruppi:

  Filtro di base:
  (|(memberOf=<DN_gruppo1>)(memberOf=<DN_gruppo2>)(memberOf=<DN_gruppo))

Nell'esempio seguente si noti che gli utenti di Active Directory dispongono dell'attributo memberOf corrispondente al filtro di base. Il numero che precede l'attributo memberOf indica il numero di gruppi di cui l'utente è membro. L'utente è membro di un solo gruppo di sicurezza, secadmins.

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

Passaggio 6: Passare agli account utente che si desidera utilizzare come account di rappresentazione nell'oggetto di autenticazione e fare clic con il pulsante destro del mouse sull'account utente per **copiare** il **DN**.



Utilizzare questo DN per il **nome utente** nell'oggetto di autenticazione. Ad esempio,

Nome utente: CN=sfdc1,CN=Account servizio,DC=VirtualLab,DC=locale

Analogamente alla ricerca di gruppi, è anche possibile eseguire ricerche in un utente con CN o con un attributo specifico, ad esempio name=sfdc1.