# 確定身份驗證對象配置的Active Directory LDAP對象屬性

#### 目錄

<u>簡介</u> 標識LDAP對象屬性

## 簡介

本文檔介紹如何標識Active Directory(AD)LDAP對象屬性以在上配置身份驗證對象以進行外部身份 驗證。

### 標識LDAP對象屬性

在FireSIGHT管理中心上配置身份驗證對象以進行外部身份驗證之前,需要標識使用者和安全組的 AD LDAP屬性才能使外部身份驗證按預期工作。為此,我們可以使用微軟提供的基於GUI的 LDAP客戶端、Ldp.exe或任何第三方LDAP瀏覽器。在本文中,我們將使用ldp.exe本地或遠端連線 、繫結和瀏覽AD伺服器並確定屬性。

步驟1:啟動ldp.exe應用程式。轉到「Start」選單,然後按一下「Run」。鍵入ldp.exe並按OK按鈕。

**附註**:在Windows Server 2008上,預設情況下安裝ldp.exe。對於Windows Server 2003或從 Windows客戶端電腦進行遠端連線,請從Microsoft站點下載support.cab或support.msi檔案。 解壓.cab檔案或安裝.msi檔案並運行ldp.exe。

步驟2:連線到伺服器。選擇Connection,然後按一下Connect。

•要從本地電腦連線到AD域控制器(DC),請輸入AD伺服器的主機名或IP地址。

• 要本地連線到AD DC,請輸入localhost作為Server。

以下螢幕截圖顯示了從Windows主機進行的遠端連線:

Connection Browse View Options Utilities				
	Connect ∑3   Server: 192.168.168.200   Port: 389   □ Connectionless   □ SSL			
	OK Cancel			

以下螢幕截圖顯示了AD DC上的本地連線:

Connect	1
Server: localhost	
Port: 389 Connectionless	
OK Cancel	

步驟3.繫結到AD DC。轉至Connection > Bind。輸入User、Password和Domain。按一下「OK」 (確定)。

User: 🗟	sfadmin	
Password:		
Domain:	virtuallab.local	
(NTLM/Kerbe	eros)	Cancel

連線嘗試成功後,您會看到如下所示的輸出:

Id = Idap\_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: 2 >> Dn:

此外,ldp.exe左窗格中的輸出將顯示成功繫結到AD DC。

res = Idap\_bind\_s(Id, NULL, &NtAuthIdentity, 1158); // v.3 {NtAuthIdentity: User='sfadmin'; Pwd= <unavailable>; domain = 'virtuallab.local'.} Authenticated as dn:'sfadmin'.

**第4步**:瀏覽目錄樹。按一下View > Tree,從下拉選單中選擇BaseDN域,然後按一下OK。此基本 DN是在驗證對象上使用的DN。

Tree View	THE P. P. LEWIS CO., LANSING MICH. & MICH. &C. MICH. &C. MICH. &C.	×
BaseDN:	DC=VirtualLab,DC=local	R
	DC=VirtualLab,DC=local	N.
Cance	- CN=Schema,CN=Configuration,DC=VirtualLab,DC=local DC=DomainDnsZones,DC=VirtualLab,DC=local	-

**第5步**:在ldp.exe的左窗格中,按兩下AD對象以將容器向下展開到葉對象的級別,然後導航到使用者 所屬的AD安全組。找到組後,按一下右鍵該組,然後選擇**Copy DN**。



如果您不確定該組位於哪個組織單位(OU),請按一下右鍵基本DN或域,然後選擇**搜尋**。出現提示時,輸入**cn=***<group name>***作為過濾器,Subtree**作為**範圍**。獲得結果後,即可複製組的DN屬性。 也可以執行萬用字元搜尋,例如**cn=\*admin**\*。 - DC=VirtualLab,DC=local

CN-Com		52
CIV-COIN	Search	
OU=Doma		
CN=Foreig	Base Dn: DC=VirtualLab,DC=local	*
CN=Infras	Filter: Innersonadmine	
CN=LostA	chief. Juie secontins	
	Scope:	
OU=Marke	○ Base ○ One Level ○ Subtree	Run
CN=NTDS		-
CN=Progr	Options	Close
OU=Sales		

1> canonicalName: VirtualLab.local/Security Groups/Secadmins;

身份驗證對象中的基本過濾器應如下所示:

• 單個組:

基本篩選器:(memberOf=<Security\_group\_DN>)

• 多個組:

#### 基本篩選器

: (|(memberOf=<group1\_DN>)(memberOf=<group2\_DN>)(memberOf=<groupN\_DN)) 在以下示例中,請注意AD使用者的memberOf屬性與基本篩選器匹配。memberOf屬性前面的數字 表示使用者所屬的組數。該使用者僅是一個安全組secadmins的成員。

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

第6步: 導航到要在身份驗證對象中用作模擬帳戶的使用者帳戶,然後按一下右鍵該使用者帳戶以複 製DN。



在身份驗證對象中將此DN用作使用者名稱。例如,

使用者名稱:CN=sfdc1,CN=服務帳戶,DC=虛擬實驗室,DC=本地

與組搜尋類似,也可以搜尋具有CN或特定屬性(例如name=sfdc1)的使用者。