# 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

<u>概要</u> LDAP オブジェクト属性の識別

#### 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。

Carl Part Part Part Part Part Part Part Part			
Connection Browse View Options Utilities			
	Connect 83		
	Server: 192.168.168.200		
	Port: 389 Connectionless		
	□ SSL		
	OK Cancel		

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。

Connect			×	
Server:	localhost			
Port:	389	Conn SSL	ectionless	
0	<		Cancel	

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。

User: 🗟	sfadmin	3
Password:		
Domain:	virtuallab.local	
(NTLM/Kerberos)		Cancel

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。

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

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。

Tree View	THE R. P. LEWIS CO., LANSING MICH. & MICH. & LANSING MICH. 11	X
BaseDN:	DC=VirtualLab,DC=local	7
	DC=VirtualLab,DC=local	T
Cance	CN=Configuration,DC=VirtualLab,DC=local CN=Schema,CN=Configuration,DC=VirtualLab,DC=local DC=DomainDnsZones,DC=VirtualLab,DC=local	-

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。 - DC=VirtualLab,DC=local

CNL Came		52
CN=Com	Search	
OU=Doma		
CN=Foreig	Base Dn: DC=VirtualLab,DC=local	*
CN=Infras	Filter:	
- CN=LostA	ritter. Juri-secontinits	
	Scope:	
OU=Marke	C Base C One Level ( Subtree	Run
CN=NTDS		-
- CN=Progr	Options	Close
OU=Sales		

\*\*\*Searching... Idap\_search\_s(Id, "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。

CN=sfdc1,CN=Service Accounts,DC=Vi	
No children	Search
CN=System,DC=VirtualLab,DC=local	Virtual List View
CN=Users, DC=VirtualLab, DC=local	Delete
	Modify
	Modify DN
	Add child
	Compare
	Advanced

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。