# Identifier les attributs d'objet LDAP Active Directory pour la configuration des objets d'authentification

#### Contenu

Introduction Identifier les attributs d'objet LDAP

## Introduction

Ce document décrit comment identifier les attributs d'objet LDAP Active Directory (AD) pour configurer l'objet d'authentification sur le pour l'authentification externe.

### Identifier les attributs d'objet LDAP

Avant de configurer un objet d'authentification sur FireSIGHT Management Center pour l'authentification externe, il est nécessaire d'identifier les attributs AD LDAP des utilisateurs et des groupes de sécurité pour que l'authentification externe fonctionne comme prévu. Pour ce faire, nous pouvons utiliser le client LDAP basé sur une interface graphique utilisateur fournie par Microsoft, Ldp.exe, ou tout navigateur LDAP tiers. Dans cet article, nous allons utiliser ldp.exe pour nous connecter localement ou à distance, nous lier et parcourir le serveur AD et identifier les attributs.

Étape 1 : Démarrez l'application ldp.exe. Accédez au menu **Démarrer** et cliquez sur **Exécuter**. Tapez **Idp.exe** et appuyez sur le bouton **OK**.

**Note**: Sur Windows Server 2008, ldp.exe est installé par défaut. Pour Windows Server 2003 ou pour une connexion à distance à partir d'un ordinateur client Windows, téléchargez le fichier support.cab ou support.msi à partir du site Microsoft. Extrayez le fichier .cab ou installez le fichier .msi et exécutez ldp.exe.

Étape 2 : Connectez-vous au serveur. Sélectionnez Connection et cliquez sur Connect.

- Pour vous connecter à un contrôleur de domaine Active Directory à partir d'un ordinateur local, entrez le nom d'hôte ou l'adresse IP du serveur Active Directory.
- Pour vous connecter localement à un contrôleur de domaine Active Directory, entrez localhost en tant que **Server**.

La capture d'écran suivante illustre une connexion à distance à partir d'un hôte Windows :

Connection Browse View Options Utilities	
Connect           Server:         192.168.168.200           Port:         389           OK         Connect	23 ctionless Cancel

La capture d'écran suivante illustre une connexion locale sur un contrôleur de domaine Active Directory :

Connect			×
Server:	localhost		_
Port:	389		ss
		) SSL Cancel	1
	<u>`</u>		

Étape 3. Liaison au contrôleur de domaine Active Directory Accédez à **Connection > Bind**.

Saisissez l'utilisateur, le mot de passe et le domaine. Click OK.

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

Lorsqu'une tentative de connexion réussit, le résultat suivant s'affiche :



En outre, le résultat affiché dans le volet gauche de ldp.exe indique une liaison réussie au contrôleur de domaine Active Directory.

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

Étape 4 : Parcourez l'arborescence du répertoire. Cliquez sur View > Tree , sélectionnez le domaine BaseDN dans la liste déroulante, puis cliquez sur OK. Ce DN de base est le DN utilisé sur l'objet d'authentification.

Tree View	the Constant Number of Street, Street, Street, Street, Street, St.	×
BaseDN:	DC=VirtualLab,DC=local	R
	DC=VirtualLab,DC=local	The second
Cancel	CN=Configuration,DC=VirtualLab,DC=local CN=Schema,CN=Configuration,DC=VirtualLab,DC=local DC=DomainDnsZones,DC=VirtualLab,DC=local	-

Étape 5 : Dans le volet gauche de ldp.exe, double-cliquez sur les objets AD pour développer les conteneurs jusqu'au niveau des objets leaf et naviguer jusqu'au groupe de sécurité AD dont les utilisateurs sont membres. Une fois que vous avez trouvé le groupe, cliquez avec le bouton droit sur le groupe, puis sélectionnez **Copier DN**.



Si vous n'êtes pas sûr de l'unité d'organisation dans laquelle se trouve le groupe, cliquez avec le bouton droit sur le DN de base ou le domaine et sélectionnez **Rechercher**. Lorsque vous y êtes invité, entrez **cn=***<group name>* comme filtre et **Subtree** comme **étendue**. Une fois le résultat obtenu, vous pouvez copier l'attribut DN du groupe. Il est également possible d'effectuer une recherche générique telle que **cn=\*admin**\*.

DC=VirtualLab, DC=local

	and the second second lines and the	82
CN=Com	Search	25
-OU=Doma		
CN=Foreig	Base Dn: DC=VirtualLab,DC=local	-
CN=Infras	Filter: Ion-secondmine	
CN=LostA	inter. Jui-secadmins	
CN=Mana	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;

Le filtre de base de l'objet d'authentification doit être le suivant :

• Groupe unique :

Filtre de base : (memberOf=<DN\_groupe\_sécurité>)

• Plusieurs groupes :

#### Filtre de base :

(|(memberOf=<group1\_DN>)(memberOf=<group2\_DN>)(memberOf=<groupN\_DN)) Dans l'exemple suivant, notez que les utilisateurs AD ont l'attribut memberOf correspondant au filtre de base. L'attribut memberOf qui précède le nombre indique le nombre de groupes dont l'utilisateur est membre. L'utilisateur est membre d'un seul groupe de sécurité, secadmins.

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

Étape 6 : Accédez aux comptes d'utilisateurs que vous souhaitez utiliser comme compte d'emprunt d'identité dans l'objet Authentication, et cliquez avec le bouton droit sur le compte d'utilisateur pour copier DN.

CN=stdc1,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 >

Utilisez ce DN comme nom d'utilisateur dans l'objet d'authentification. Exemple :

nom de l'utilisateur: CN=sfdc1,CN=Comptes de service,DC=VirtualLab,DC=local

Comme pour la recherche de groupe, il est également possible de rechercher un utilisateur avec CN ou un attribut spécifique tel que name=sfdc1.