Identificar Atributos de Objeto LDAP do Ative Diretory para Configuração de Objeto de Autenticação

Contents

Introduction Identificar atributos de objeto LDAP

Introduction

Este documento descreve como identificar atributos de Objeto LDAP do Ative Diretory (AD) para configurar o Objeto de Autenticação no para autenticação externa.

Identificar atributos de objeto LDAP

Antes de configurar um Objeto de autenticação em um FireSIGHT Management Center para autenticação externa, a identificação dos atributos AD LDAP de Usuários e Grupos de segurança seria necessária para que a autenticação externa funcionasse como pretendido. Para fazer isso, podemos usar o cliente LDAP baseado em GUI da Microsoft, Ldp.exe, ou qualquer navegador LDAP de terceiros. Neste artigo, usaremos o Idp.exe para conectar, vincular e navegar no servidor do AD local ou remotamente, e identificar os atributos.

Passo 1: Inicie o aplicativo Idp.exe. Vá para o menu Iniciar e clique em Executar. Digite Idp.exe e pressione o botão OK.

Note: No Windows Server 2008, o ldp.exe é instalado por padrão. Para o Windows Server 2003 ou para conexão remota a partir do computador cliente Windows, baixe o arquivo support.cab ou support.msi do site da Microsoft. Extraia o arquivo .cab ou instale o arquivo .msi e execute ldp.exe.

Passo 2: Conecte-se ao servidor. Selecione Connection e clique em Connect.

- Para se conectar a um DC (Controlador de Domínio) do AD a partir de um computador local, insira o nome de host ou o endereço IP do servidor do AD.
- Para se conectar a um AD DC localmente, digite localhost como Servidor.

A captura de tela a seguir mostra a conexão remota de um host Windows:

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

A captura de tela a seguir mostra uma conexão local em um AD DC:

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

Etapa 3. Vincular ao AD DC. Vá para Connection > Bind. Insira User, Password e Domain. Click OK.

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

Quando uma tentativa de conexão for bem-sucedida, você verá uma saída como a seguinte:



Além disso, a saída no painel esquerdo de ldp.exe mostrará a associação bem-sucedida ao AD DC.

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

Passo 4: Procure a Árvore de Diretórios. Clique em View > Tree , selecione o domínio BaseDN na lista suspensa e clique em OK. Esse DN base é o DN usado no Objeto de autenticação.

Tree View	In CARDING STREET, STREET, STREET, STREET, STREET, ST. STREET, ST.	X
BaseDN:	DC=VirtualLab,DC=local	7
	DC=VirtualLab,DC=local	Th.
Cance	CN=Configuration,DC=VirtualLab,DC=local CN=Schema,CN=Configuration,DC=VirtualLab,DC=local DC=DomainDnsZones,DC=VirtualLab,DC=local	-

Passo 5: No painel esquerdo de ldp.exe, clique duas vezes nos objetos do AD para expandir os contêineres até o nível de objetos folha e navegue até o Grupo de Segurança do AD do qual os usuários são membros. Quando encontrar o grupo, clique com o botão direito do mouse no grupo e selecione **Copy DN**.



Se não tiver certeza de qual Unidade Organizacional (OU) o grupo está localizado, clique com o botão direito do mouse no DN base ou Domínio e selecione **Pesquisar**. Quando solicitado, insira **cn=***qroup name>* como filtro e *Subtree como* scope. Depois de obter o resultado, você pode copiar o atributo DN do grupo. Também é possível executar uma pesquisa por curinga, como **cn=*admin***.

- DC=VirtualLab,DC=local

	and the second sec	50
CN=Com	Search	25
OU=Doma		
CN=Foreig	Base Dn: DC=VirtualLab,DC=local	-
CN=Infras	Filter: Ion-secondmine	
CN=LostA	riter. Icri-secontinis	
CN=Mana	Scope:	
OU=Marke	C Base C One Level (Subtree	Run
CN=NTDS		-
CN=Progr	Options	Close
-OU=Sales		

**Searching
dap_search_s(Id, "DC=VirtualLab,DC=local", 2, "cn=secadmins", attrList, 0, &msg)
Result <0>: (null)
Aatched DNs:
Setting 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;

O filtro base no objeto de autenticação deve ser o seguinte:

• Grupo único:

Filtro base: (memberOf=<Security_group_DN>)

• Vários grupos:

Filtro base:

(|(memberOf=<grupo1_DN>)(memberOf=<grupo2_DN>)(memberOf=<grupoN_DN))

No exemplo a seguir, observe que os usuários do AD têm o atributo memberOf correspondente ao Filtro Base. O número que precede o atributo memberOf indica o número de grupos dos quais o usuário é membro. O usuário é membro de apenas um grupo de segurança, secadmins.

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

Passo 6: Navegue até as contas de usuário que deseja usar como conta de representação no Objeto de autenticação e clique com o botão direito do mouse na conta de usuário para **Copiar DN**.

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 +
	Advanced
	Copy DN

Use este DN para Nome de usuário no Objeto de autenticação. Por exemplo,

User Name: CN=sfdc1,CN=Contas de serviço,DC=VirtualLab,DC=local

Semelhante à pesquisa de grupo, também é possível pesquisar um usuário com CN ou atributo específico, como name=sfdc1.