识别激活目录LDAP认证对象配置的对象属性

Contents

<u>Introduction</u> <u>识别LDAP对象属性</u>

Introduction

本文描述如何识别激活目录(AD) LDAP对象属性配置在的认证对象外部认证的。

识别LDAP对象属性

在配置在一个FireSIGHT管理中心的一个认证对象之前外部认证,识别用户和安全组AD LDAP属性 是必要为了外部认证能工作按照计划。要执行如此,我们能使用Microsoft提供了GUI基于LDAP客户 端、Ldp.exe,或者所有第三方LDAP浏览器。在此条款上,我们将使用ldp.exeto连接,捆绑,并且 访问AD服务器并且识别属性。

步骤1:运行ldp.exe。去Startmenu并且点击运行。键入ldp.exeandOK按钮。

Note:默认情况下在Windows服务器上2008年,安装ldp.exe。对于远程连接的Windows服务器2003年或从Windows客户端计算机,Microsoft站点请下载support.cabor support.msi。 提取.msi fileand运行ldp.exe的.cab fileor安装。

步骤 2: 连接到服务器。选择连接并且点击连接。

•要连接到一个AD域控制器(DC)从一台本地计算机,请输入AD服务器的主机名-或IP地址。

•要连接到AD DC本地,请进入localhost作为服务器。

以下屏幕画面表示从Windows主机的远程连接:

Cdp	
Connection Browse View	Options Utilities
	53
	Connect
	Server: 192,168,168,200
	Port 389 Connectionless
	□ SSL
	OK Cancel

以下屏幕画面表示在AD DC的本地连接:

Connect			×
Server:	localhost	_	
Port:	389	Connecti	onless
	_	-	
			ncei

步骤3.对AD DC的捆绑。去**连接>捆绑**。输入用户、密码和域。单击 Ok。

User: 🗟	sfadmin	
Password:		
Domain:	virtuallab.local	1
(NTLM/Kerberos)		Cancel

当连接尝试是成功的,您将看到一个输出类似如下:

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:

并且,在ldp.exe左窗格的输出将显示成功的捆绑AD DC。

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

步骤 4 : 访问目录树。点击**视图>树**,选择域**BaseDN**从下拉列表,并且点击OK键。此基础DN是在认 证对象使用的DN。

Tree View	IN CARDING STREET, STREET, STREET, STREET, STREET, ST.	×
BaseDN:	DC=VirtualLab,DC=local	R
-	DC=VirtualLab,DC=local	A.
Cance	- CN=Schema,CN=Configuration,DC=VirtualLab,DC=local DC=DomainDnsZones,DC=VirtualLab,DC=local	-

步骤 5:在ldp.exe左窗格在扩展容器下来对分支对象的级别和连接的AD对象的对AD安全组用户是成员。一旦寻找组,请用鼠标右键单击在组然后选择CopyDN。



如果不是肯定的在哪组织单位(OU)找出组,请用鼠标右键单击在基础DN或域并且选择**搜索**。当提示,请进入cn=<group *name>*作为过滤器和**子树**作为**范围**。一旦取得结果,您能然后复制组的 DN属性。执行通配符搜索例如cn=*admin*也是可能的。 DC=VirtualLab,DC=local

CNI Camel		52
CN=Com	Search	_ 63
OU=Doma		
CN=Foreig	Base Dn: DC=VirtualLab,DC=local	-
CN=Infras	Ether:	
CN=LostA	riller. cn=secadmins	
CN=Mana	Scope:	
OU=Marke	C Base C One Level Subtree	Run
CN=NTDS		
	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;

在认证对象的基本过滤器应该是作为如下:

•组:

基本过滤器: (memberOf=<Security_group_DN>)

多个组:

基本过滤器

: (| (memberOf=<group1_DN>) (memberOf=<group2_DN>) (memberOf=<groupN_DN)
)

在以下示例中,请注意AD用户有匹配基本过滤器的memberOf属性。编号之前的memberOf属性指示组的数量用户是成员。用户只是一个安全组的成员, secadmins。

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

步骤 6 : 连接对您希望使用作为模拟帐户在认证对象的在**复制DN的**用户帐户的用户帐户和用鼠标右键 单击。

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

请使用此DN**用户名**在认证对象。例如,

用户名:CN=sfdc1,CN=Service DC=VirtualLab DC=local

类似组队搜索,搜索有CN的一个用户或特定属性例如name=sfdc1也是可能的。