使用Ldp.exe验证基于SSL/TLS的 LDAP(LDAPS)和CA证书

目录

<u>简介</u> <u>如何验证</u> <u>开始使用前</u> <u>验证步骤</u> <u>测试结果</u> 相关文档

简介

在FireSIGHT管理中心上为Active Directory LDAP Over SSL/TLS(LDAPS)创建身份验证对象时,有 时可能需要测试CA证书和SSL/TLS连接,并验证身份验证对象是否未通过测试。本文档说明如何使 用Microsoft Ldp.exe运行测试。

如何验证

开始使用前

使用具有本地管理权限的用户帐户登录到Microsoft Windows本地计算机,以执行本文档上的步骤。

注意:如果当前系统上没有ldp.exe,则必须先下载**Windows支持工具**。可在Microsoft网站上 找到。下载并安装**Windows支持工具**后,请执行以下步骤。

在不是域成员的本地Windows计算机上执行此测试,因为如果根或企业CA加入域,它将信任它。如 果本地计算机不再位于域中,则在执行此测试之前,应从本地计算机**受信任的根证书颁发机构**存储 中删除根证书或企业CA证书。

验证步骤

第1步:启动ldp.exe应用。转到**Start**(开始**)菜**单,然后单击**Run(运行**)。键入l**dp.exe**,然后单击 OK按钮。

步骤 2:使用域控制器FQDN连接到域控制器。要连接,请转到Connection > Connect并输入域控制器FQDN。然后选择SSL,按如下所示指定端口636,然后单击OK。

Server: pdc1.v	irtuallab local
Port: 636	Connectionless
OK	Cancel

步骤 3:如果根或企业CA在本地计算机上不受信任,结果如下所示。错误消息表明从远程服务器收 到的证书是由不受信任的证书颁发机构颁发的。

View	Options Utilities
ld = 1	up_sslinit("pdc1.virtuallab.local", 636, 1);
Error	0x0> = Idap_set_option(hLdap, LDAP_OPT_PROTOCOL_VERSION, LDAP_VERSION3
Error	0x51> = Idap_connect(hLdap, NULL);
Serv	error: <empty></empty>
Error	0x51>: Fail to connect to pdc1.virtuallab.local.

步骤4:按以下条件过滤本地Windows计算机上的事件消息可提供特定结果:

- 事件源= Schannel
- 事件ID = 36882

-			
the certificate	received from the remo can be validated. The SS	te server was issued by an L connection request has f	untrusted certificate authority. Because of this, none of the data contained in ailed. The attached data contains the server certificate.
,			
Log Name:	System		
Log Name: Source:	System Schannel	Logged:	11/24/2012 8:22:30 PM

步骤 5:将CA证书导入到本地Windows计算机证书存储区。

i.运行Microsoft管理控制台(MMC)。 转到**Start**(开始**)菜**单,然后单击**Run(运行**)。键入**mmc**,然后单 击**OK**按钮。

Run	<u>?×</u>
	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:	mmc
	OK Cancel <u>B</u> rowse

二、添加本地计算机证书管理单元。导航至File(文件)菜单上的以下选项:

Add/Remote Snap-in > Certificates > Add >选择"Computer Account">Local Computer:(运行此控制台的计算机)>完成>确定。

三。导入CA证书。

Console Root > Certificates(Local Computer)> Trusted Root Certification Authorities > Certificates > 右键单击>所有任务>导入。

🚡 Console1				
∫ <u>C</u> onsole <u>W</u> indow <u>H</u> elp ∫ [) 🖻 🖬 🗉			
🚡 Console Root				- D ×
<u>Action</u> <u>View</u> <u>F</u> avorites	← → 🛍 💽	1 🗟 😫		
Tree Favorites		Name		
Console Root		🗐 Certificat	es (Local Co	omputer)
🖻 👹 Certificates (Local Computer))			
⊕…	n Authorities			
	Find Certificate	s		
	All Tasks	•	Find Cert	ificates
	New Window fr	om Here	Import	
	Refresh			
	Help			
Add a certificate to a store				1.

• 单击Next并浏览到Base64 Encoded X.509 Certificate(*.cer, *.crt)CA证书文件。然后选择文件

o

• 单击Open > Next,然后选择Place all certificates in the following store:受信任的根证书颁发机 构。

•单击下一步>完成导入文件。

ertificat	e Import Wizard
Certificate	e Store
Certifi	icate stores are system areas where certificates are kept.
Windo the ce	ows can automatically select a certificate store, or you can specify a location for artificate.
С	Automatically select the certificate store based on the type of certificate
œ	Place all certificates in the following store
	Certificate store:
	Trusted Root Certification Authorities\Local Computer Browse
earn more	e about <u>certificate stores</u>
	< Back Nevt > Cancel
	STICLS I DEAL 2 I ACULT

四。确认CA与其他受信任的根CA一起列出。

步骤 6:按照步骤1和2通过SSL连接到AD LDAP服务器。如果CA证书正确,ldp.exe右窗格中的前 10行应如下所示:

Id = Idap_sslinit("pdc1.virtuallab.local", 636, 1); Error <0x0> = Idap_set_option(hLdap, LDAP_OPT_PROTOCOL_VERSION, LDAP_VERSION3); Error <0x0> = Idap_connect(hLdap, NULL); Error <0x0> = Idap_get_option(hLdap,LDAP_OPT_SSL,[void*]&Iv]; Host supports SSL, SSL cipher strength = 128 bits Established connection to pdc1.virtuallab.local. Retrieving base DSA information... Result <0>: [null] Matched DNs: Getting 1 entries: >> Dn:

测试结果

如果证书和LDAP连接通过此测试,您可以成功配置通过SSL/TLS的LDAP的身份验证对象。但是 ,如果测试由于LDAP服务器配置或证书问题而失败,请解决AD服务器上的问题或下载正确的CA证 书,然后才在FireSIGHT管理中心上配置身份验证对象。

相关文档

- <u>识别身份验证对象配置的Active Directory LDAP对象属性</u>
- 在FireSIGHT系统上配置LDAP身份验证对象