使用Ldp.exe验证基于SSL/TLS的LDAP(LDAPS)和CA证书

目录

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。

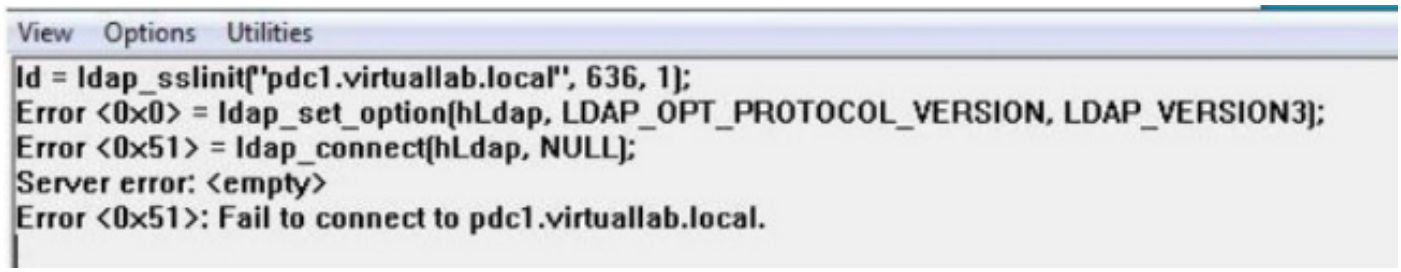
在不是域成员的本地Windows计算机上执行此测试，因为如果根或企业CA加入域，它将信任它。如果本地计算机不再位于域中，则在执行此测试之前，应从本地计算机**受信任的根证书颁发机构**存储中删除根证书或企业CA证书。

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**ldp.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**。

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。

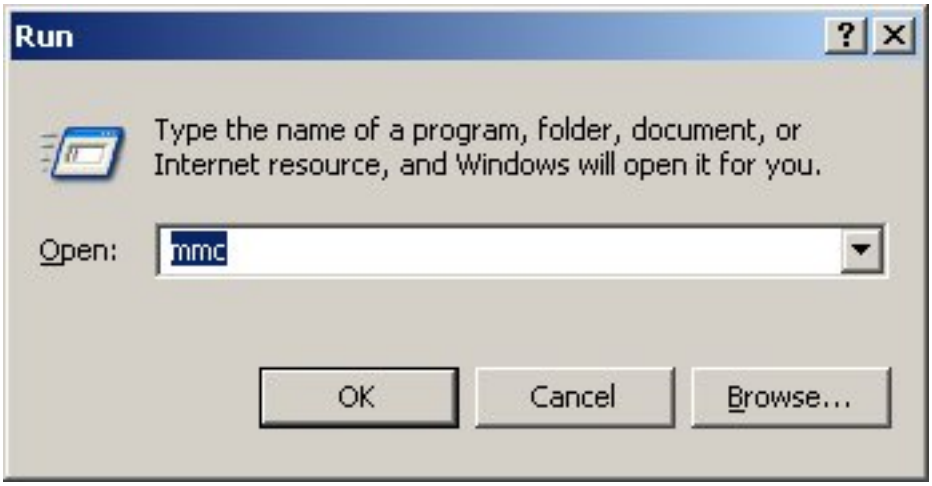


步骤 4：按以下条件过滤本地Windows计算机上的事件消息可提供特定结果：

- 事件源= Schannel
- 事件ID = 36882

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。

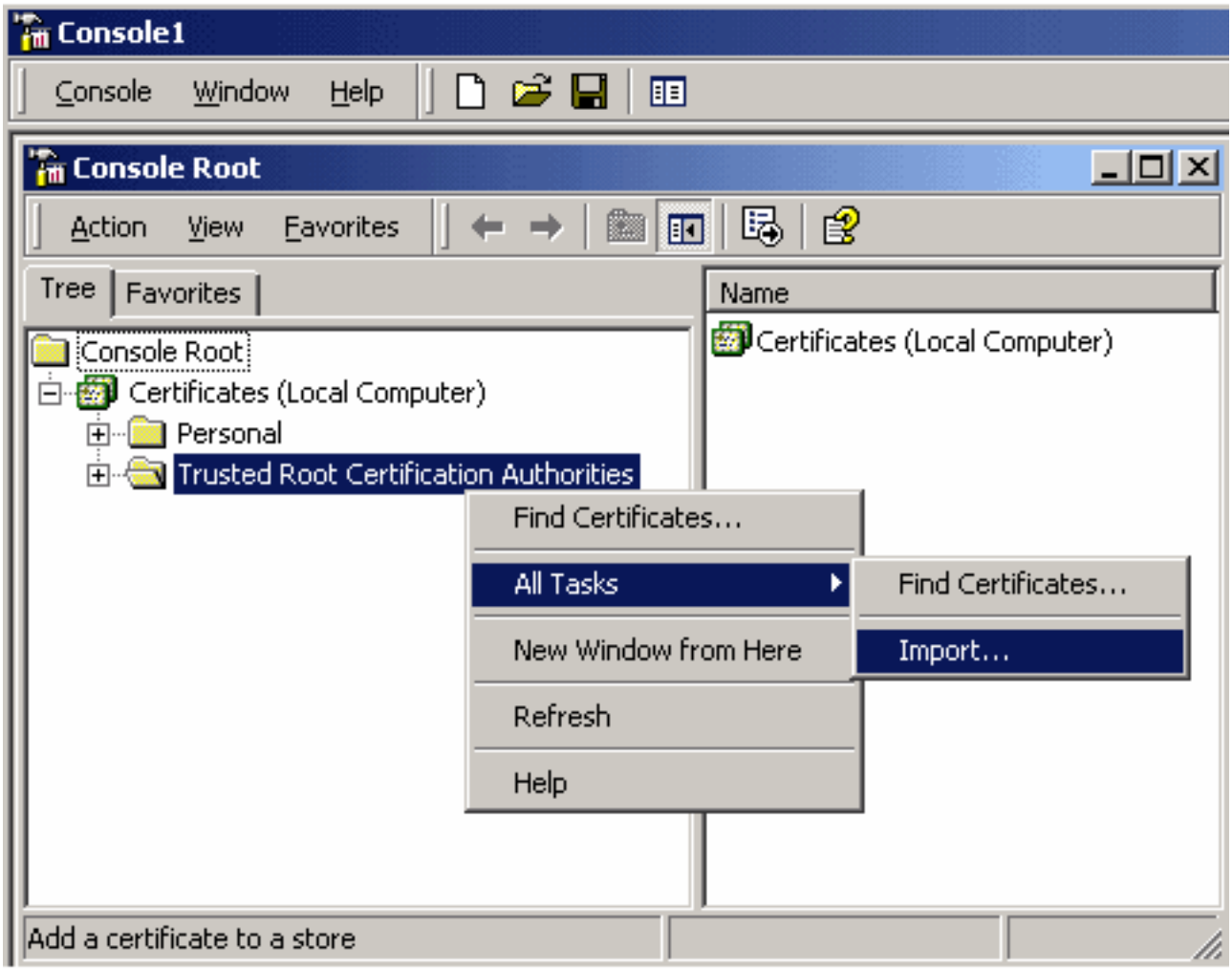


二、添加本地计算机证书管理单元。导航至**File**（文件）菜单上的以下选项：

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。

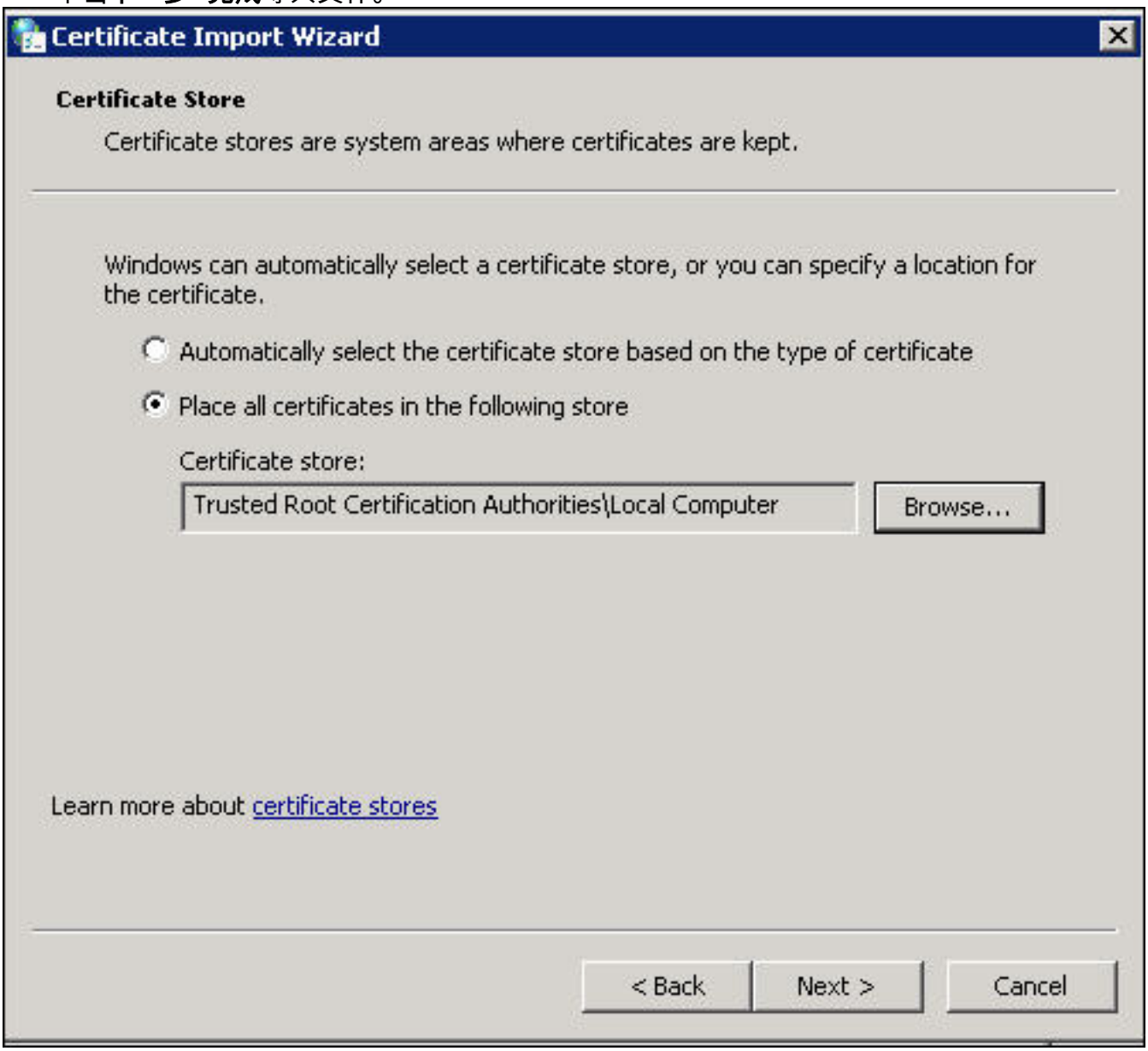
三。导入CA证书。

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



- 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。

- 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。



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：

```
ld = ldap_sslinit("pdc1.virtuallab.local", 636, 1);
Error <0x0> = ldap_set_option(hLdap, LDAP_OPT_PROTOCOL_VERSION, LDAP_VERSION3);
Error <0x0> = ldap_connect(hLdap, NULL);
Error <0x0> = ldap_get_option(hLdap,LDAP_OPT_SSL,(void*)&lv);
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

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