

验证在SSL/TLS (LDAP)的LDAP使用Ldp.exe , 和CA证书

目录

[简介](#)

[如何验证](#)

[开始使用前](#)

[验证步骤](#)

[测试结果](#)

[相关文档](#)

简介

当您创建在一个FireSIGHT管理中心的一个验证对象在SSL/TLS (LDAP)的活动目录的LDAP , 测试CA cert和SSL/TLS连接 , 并且验证可能有时是必要的 , 如果验证对象失败测验。使用Microsoft Ldp.exe , 本文解释如何运行测验。

如何验证

开始使用前

登陆到有本地管理权限执行在本文的步骤的用户帐户的一台Microsoft Windows本地计算机。

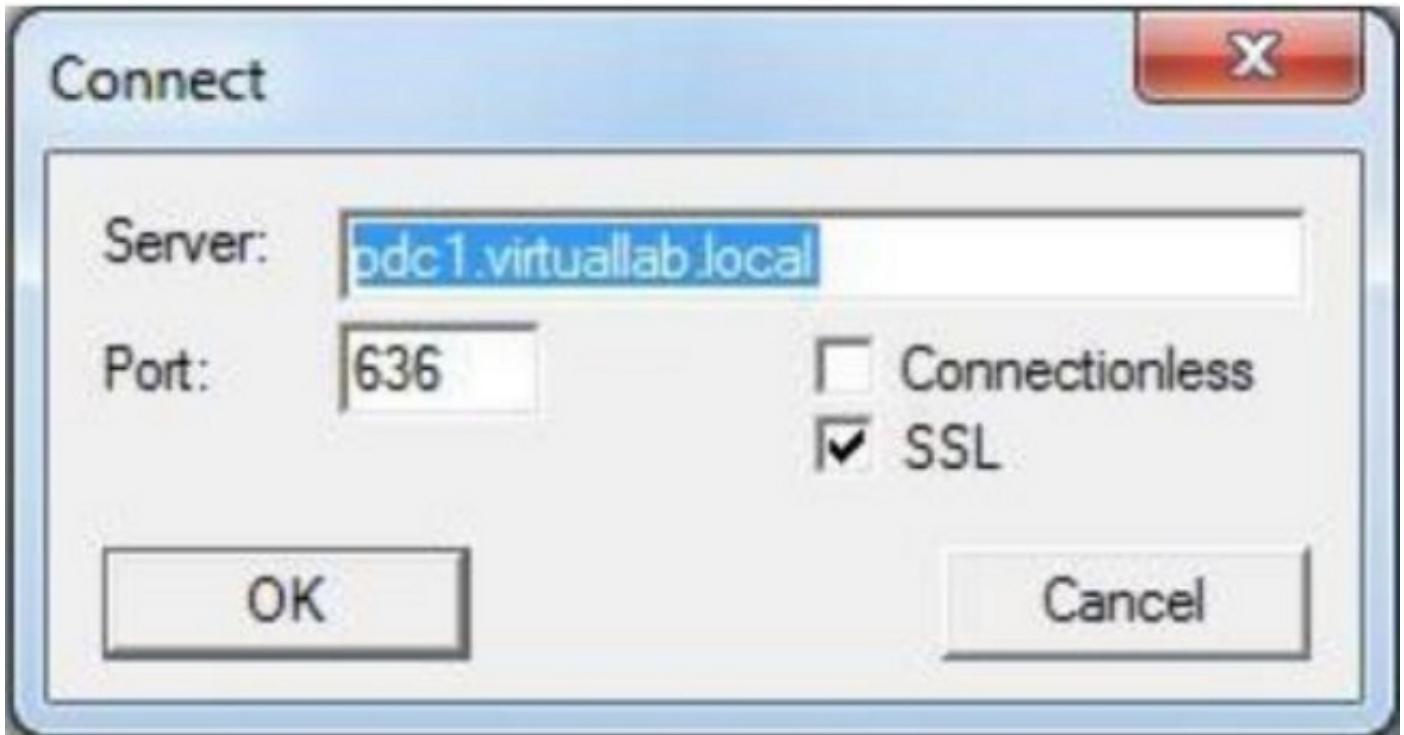
注意：如果当前没有在您的系统的ldp.exe , 您必须首先下载WindowsSupport工具。这在Microsoft网站可以找到。一旦下载并且安装WindowsSupport工具 , 请遵从下面的步骤。

执行在不是域的成员的一台本地Windows计算机的此测验 , 因为将委托根或企业CA , 如果加入域。如果本地计算机不再在域 , 应该从存储前面执行此测验的本地计算机可靠的根证书颁发机构删除根或企业CA证书。

验证步骤

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

步骤 2：连接到使用域控制器FQDN的域控制器。为了连接 , 请去连接>连接并且输入域控制器FQDN。然后请选择SSL , 指定端口636如下所示并且点击OK键。

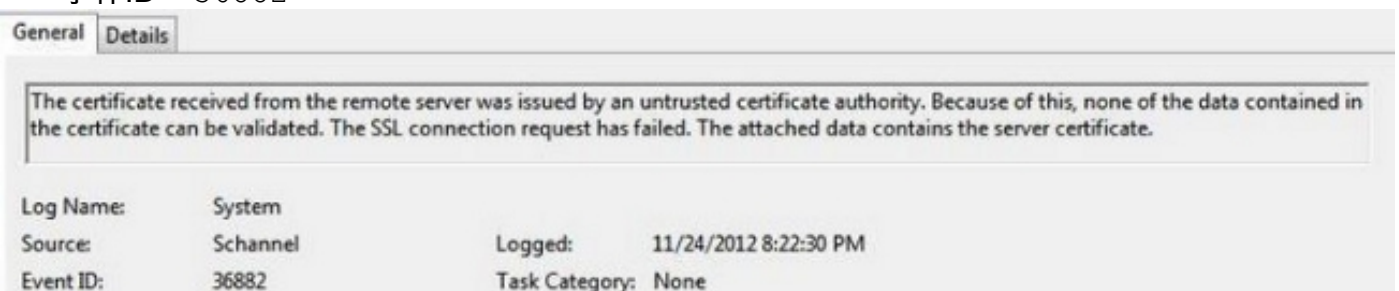


步骤 3 : 如果根或企业CA在本地计算机没有委托，结果查找作为下面。错误消息表明从远程服务器接收的证书由不信任发出认证机关。

```
View Options Utilities
ld = ldap_sslinit('pdc1.virtuallab.local', 636, 1);
Error <0x0> = ldap_set_option(hLdap, LDAP_OPT_PROTOCOL_VERSION, LDAP_VERSION3);
Error <0x51> = ldap_connect(hLdap, NULL);
Server error: <empty>
Error <0x51>: Fail to connect to pdc1.virtuallab.local.
```

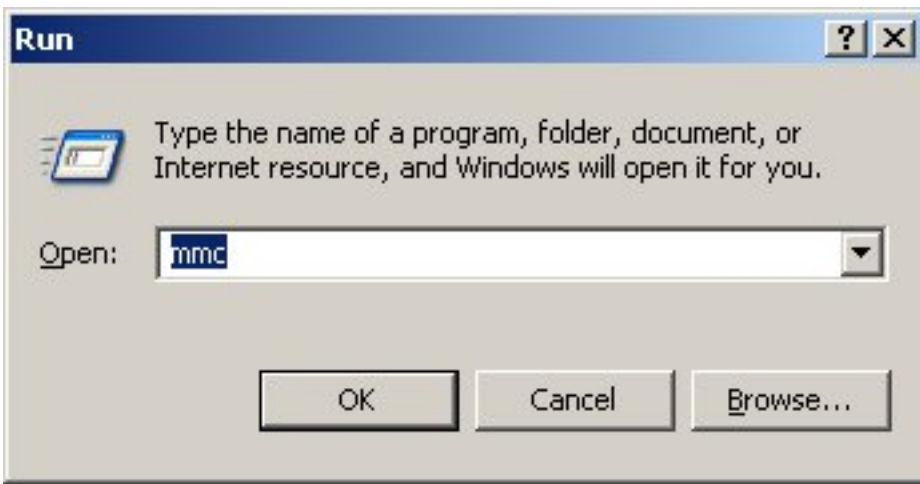
步骤 4 : 过滤在本地Windows计算机的事件消息有以下标准的提供一种特定结果：

- 事件来源= Schannel
- 事件ID = 36882



步骤 5 : 导入CA证书对本地windows计算机证书存储。

i. 运行微软管理控制台(MMC)。去**开始菜单**并且点击**运行**。键入mmc并且按下了**OK按钮**。

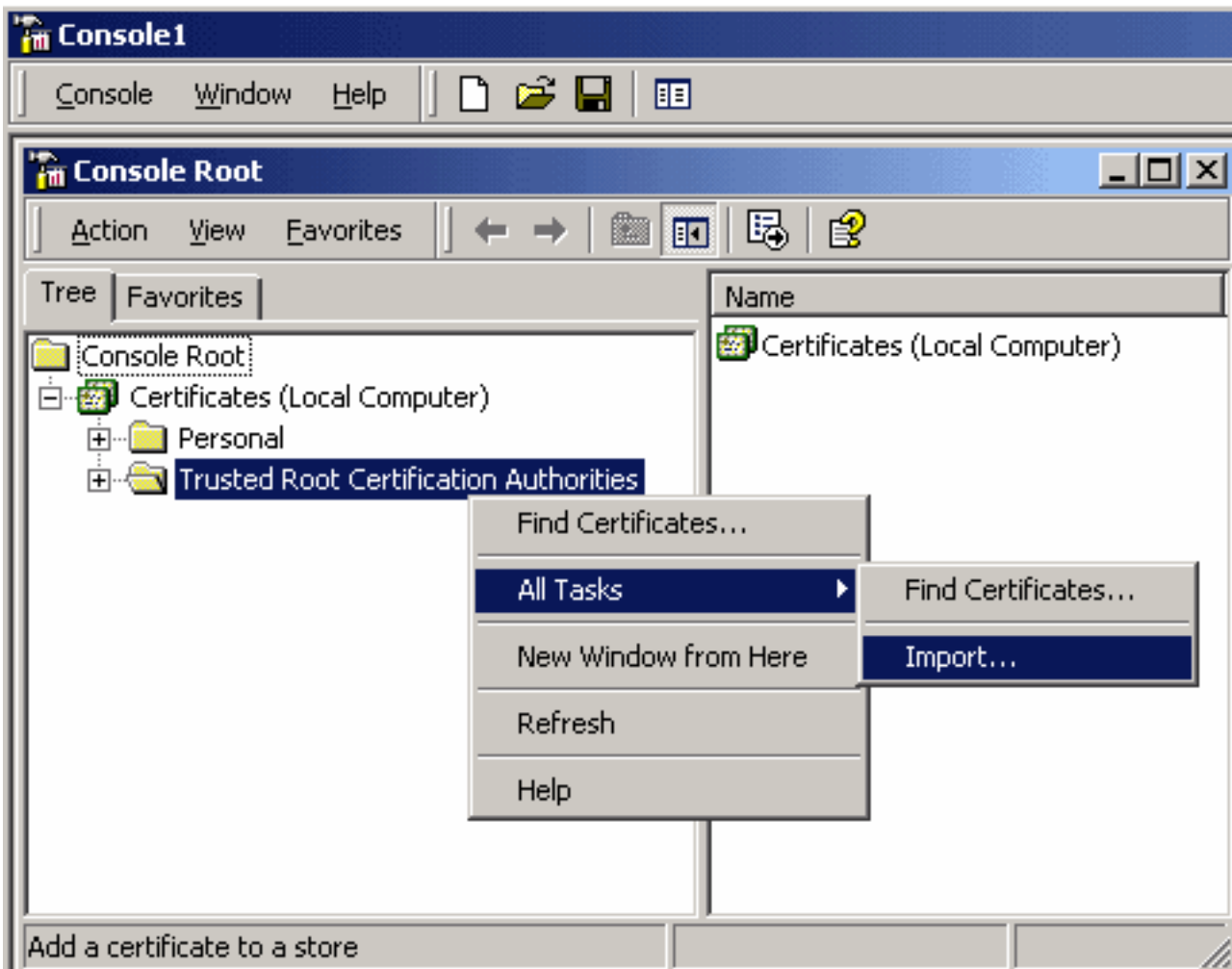


ii. 添加本地计算机证书管理单元。导航对在**文件菜单**的以下选项：

添加/Remote管理单元>证书>Add >选择"Computer Account" >本地计算机：(此控制台运行)的计算机>芬通社>好。

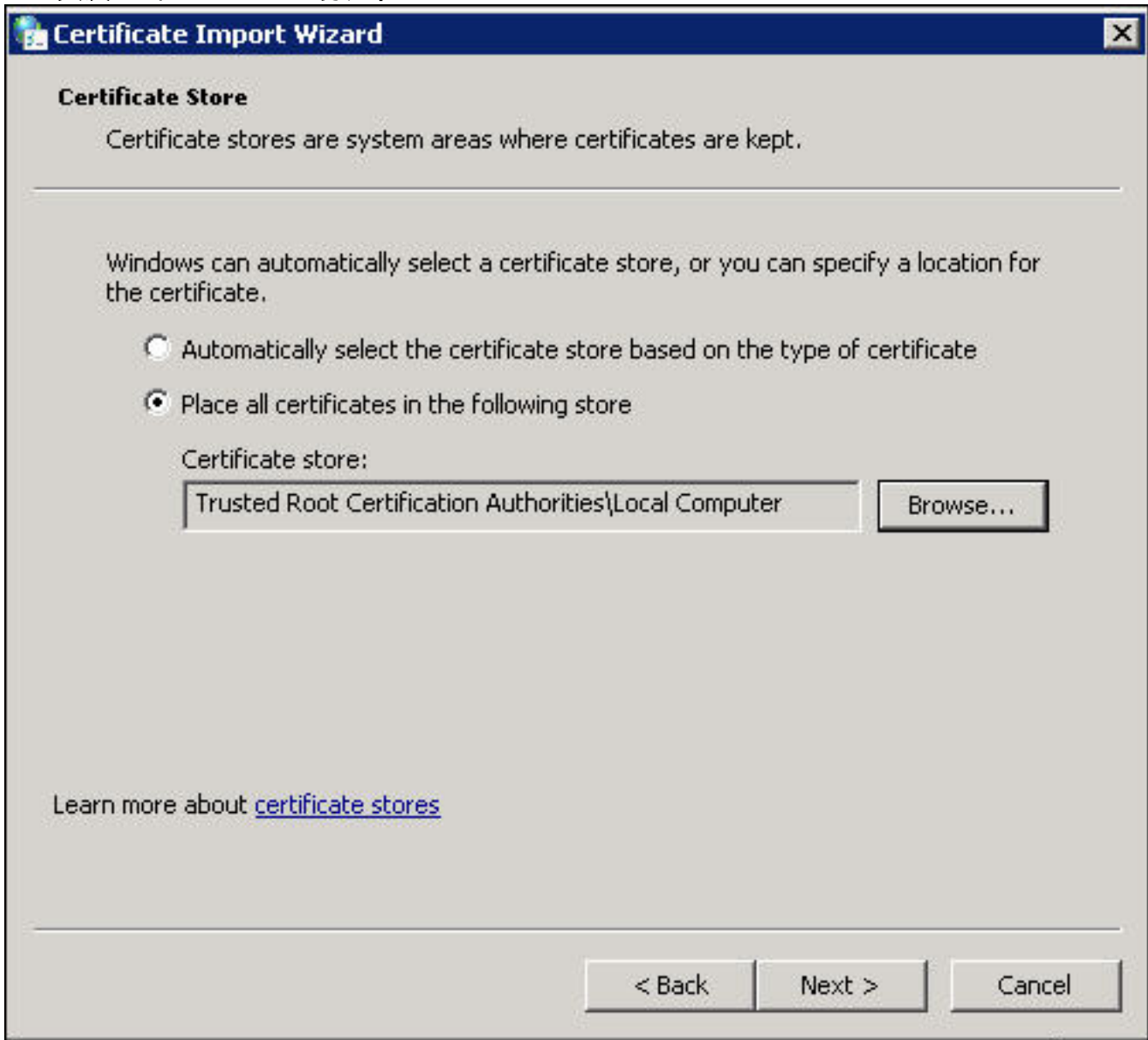
罗马数字3导入CA证书。

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



- 其次单击并且浏览到Base64编码的X.509证书(*.cer , *.crt) CA证书文件。然后请选择文件。

- 在以下存储点击开放>其次并且选择地方所有证书：可靠的根证书颁发机构。
- 其次单击>导入文件的芬通社。



罗马数字4确认CA用其他可信的根CA列出。

步骤 6：跟随Step1和2连接到AD在SSL的LDAP服务器。如果CA证书正确，在ldp.exe右窗格的前10条线路是作为如下：

```
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连接通过此测验，您能成功配置LDAP的验证对象在SSL/TLS。然而，如果测验失败由于LDAP服务器配置或证书问题，请解决在AD服务器的问题或下载正确CA证书，在您配置在FireSIGHT管理中心前的验证对象。

相关文档

- [识别活动目录LDAP验证对象配置的对象属性](#)
- [LDAP认证对象的配置在FireSIGHT系统的](#)