Verify LDAP over SSL/TLS (LDAPS) and CA Certificate Using Ldp.exe

TAC **Document ID: 118761**

Contributed by Nazmul Rajib and Binyam Demissie, Cisco TAC Engineers.
Jan 14, 2015

Contents

Introduction

When you create an Authentication Object on a FireSIGHT Management Center for Active Directory LDAP Over SSL/TLS (LDAPS), it may sometimes be necessary to test the CA cert and SSL/TLS connection, and verify if the Authentication Object fails the test. This document explains how to run the test using Microsoft Ldp.exe.

How to Verify

Before You Begin

Login to a Microsoft Windows local computer with a user account that has local Administrative privilege to perform the steps on this document.

Note: If you do not currently have `ldp.exe` available on your system, you must first download the ***Windows Support Tools***. This is available on the Microsoft website. Once you download and install the ***Windows Support Tools***, follow the below steps.

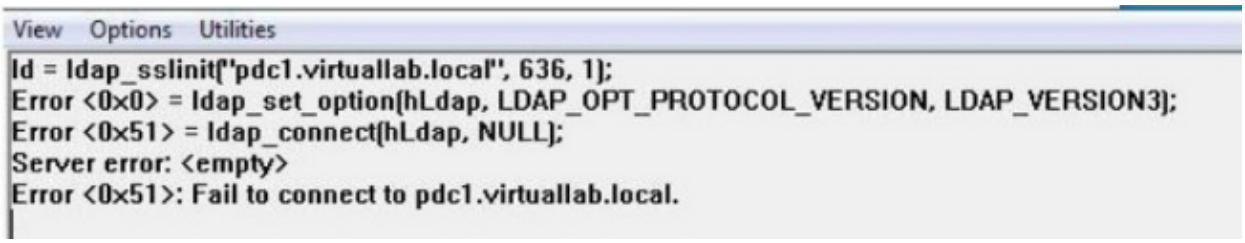
Perform this test on a local Windows computer that has not been a member of a domain, as it would trust the Root or Enterprise CA if it joined a domain. If a local computer is no longer in a domain, the Root or Enterprise CA certificate should be removed from the local computer ***Trusted Root Certification Authorities*** store before performing this test.

Verification Steps

Step 1: Start ldp.exe application. Go to the ***Start*** menu and click ***Run***. Type ***ldp.exe*** and hit the ***OK*** button.

Step 2: Connect to the Domain Controller using the domain controller FQDN. In order to connect, go to ***Connection*** > ***Connect*** and enter the Domain Controller FQDN. Then select ***SSL***, specify port ***636*** as shown below and click ***OK***.

Step 3: If the Root or Enterprise CA is not trusted on a local computer, the result looks as below. The error message indicates that the certificate received from the remote server was issued by an untrusted certificate authority.

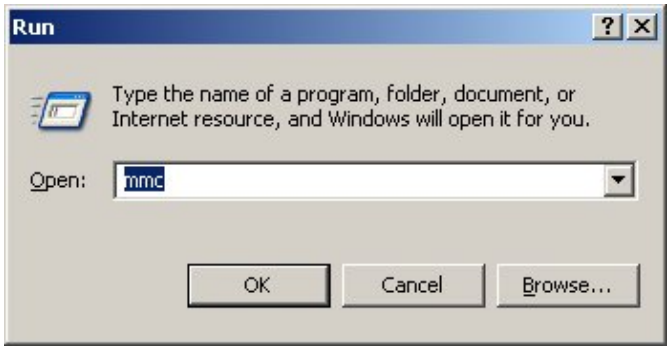


Step 4: Filtering the event messages on local Windows computer with the following criteria provides a specific result:

- Event Source = `Schannel`
- Event ID = `36882`

Step 5: Import the CA Certificate to the local windows computer certificate store.

i. Run Microsoft Management Console (MMC). Go to the ***Start*** menu and click ***Run***. Type ***mmc*** and hit the ***OK*** button.

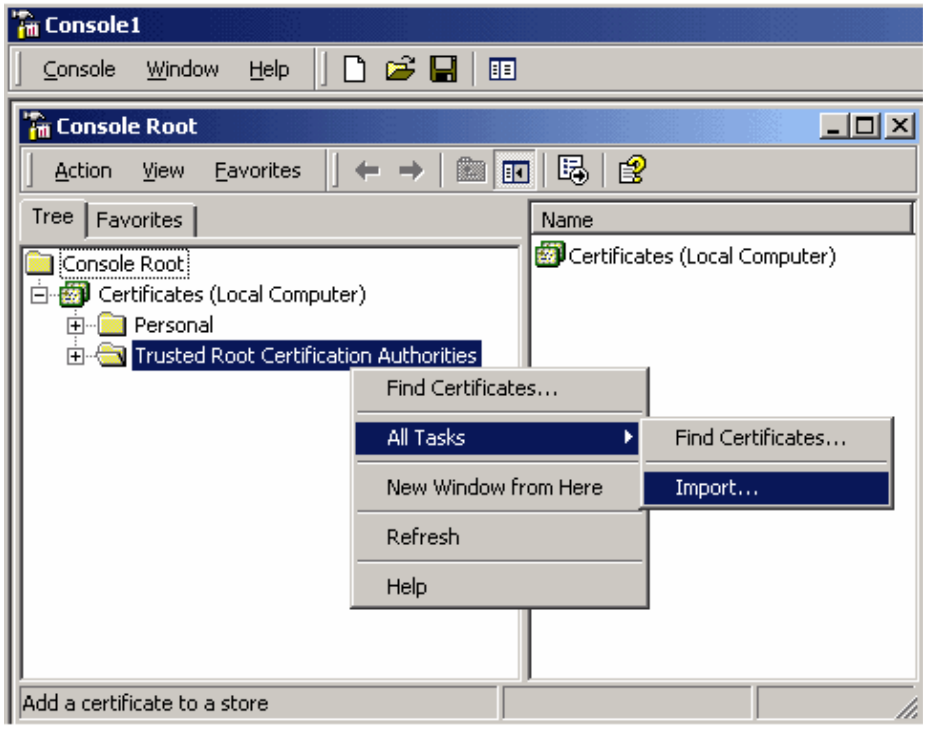


ii. Add local computer certificate snap−in. Navigate to the following options on the ***File*** menu:

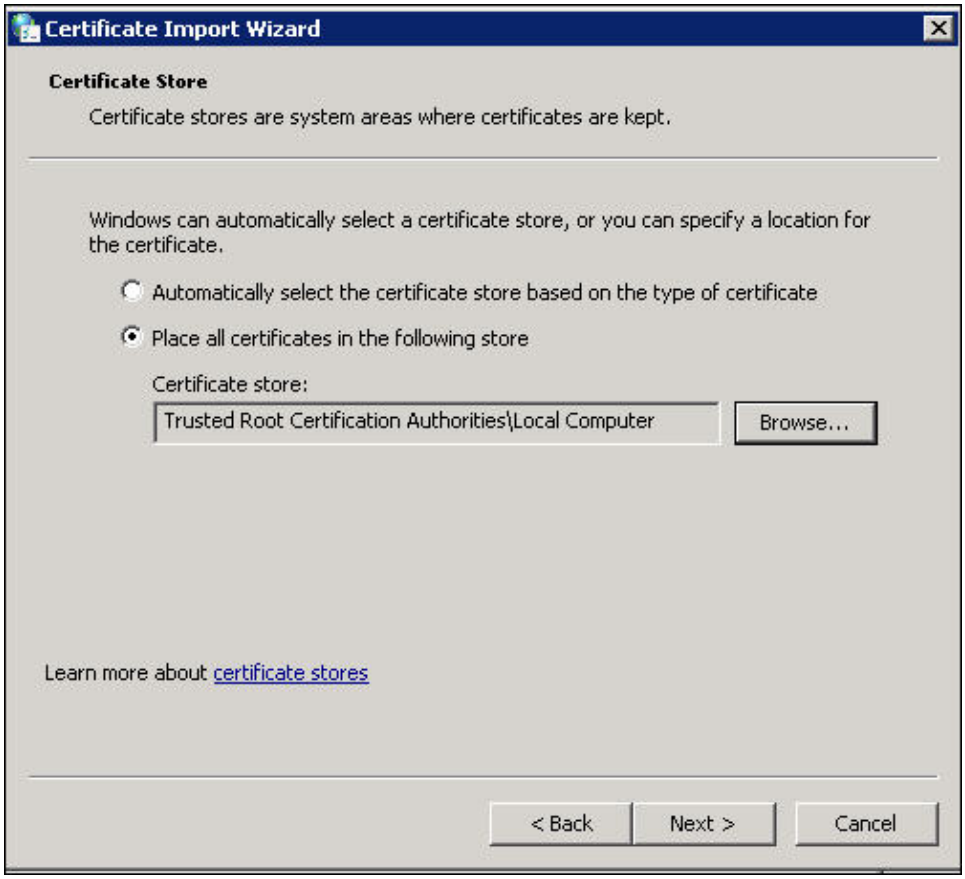
Add/Remote Snap−in > ***Certificates*** > ***Add*** > ***Choose "Computer Account"*** > ***Local Computer: (the computer this console is running on)*** > ***Finish*** > ***OK***.

iii. Import the CA certificate.

Console Root > Certificates (Local Computer) > ***Trusted Root Certification Authorities*** > ***Certificates*** > Right click > ***All Tasks*** > ***Import***.



- Click ***Next*** and Browse to Base64 Encoded X.509 Certificate (`*.cer`, `*.`crt) CA certificate file. Then select the file.
- Click ***Open > Next*** and select ***Place all certificates in the following store: Trusted Root Certification Authorities***.
- Click ***Next > Finish*** to import the file.



iv. Confirm that the CA is listed with other trusted root CAs.

Step 6: Follow the Step 1 and 2 to connect to the AD LDAP server over SSL. If the CA certificate is correct, the first 10 lines on the right pane of `ldp.exe` should be as below:

```
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:
```

Test Result

If a certificate and LDAP connection pass this test, you can successfully configure the Authentication Object for LDAP over SSL/TLS. However, if the test fail due to LDAP server configuration or certificate issue, please resolve the issue on the AD server or download the correct CA certificate before you configure the Authentication Object on the FireSIGHT Management Center.

Related Documents

- Identify Active Directory LDAP Object Attributes for Authentication Object Configuration
- Configuration of LDAP Authentication Object on FireSIGHT System