Ldp.exe を使用して SSL/TLS（LDAPS）および CA 証明書で LDAP を検証する

目次

概要

FireSIGHT Management Center で、Active Directory LDAP Over SSL/TLS（LDAP）用の認証オブジェクトを作成する場合、CA 証明書と SSL/TLS 接続をテストし、認証オブジェクトがテストに失敗しないか確認することが必要になることがあります。 このドキュメントでは、Microsoft Ldp.exe を使用してテストを実行する方法について説明します。

確認する方法

はじめに

この資料のステップを実行するローカル管理権限があるユーザアカウントの Microsoft Windows ローカル コンピュータにログインして下さい。

> **注:** 現在 システムで `ldp.exe` ない場合最初に WindowsSupport **ツールを**ダウンロードして下さい。 **これは**マイクロソフト社Webサイトで利用可能です。 WindowsSupport **ツールを**ダウンロードし、インストールしたら、下記のステップに**従って下さい**。

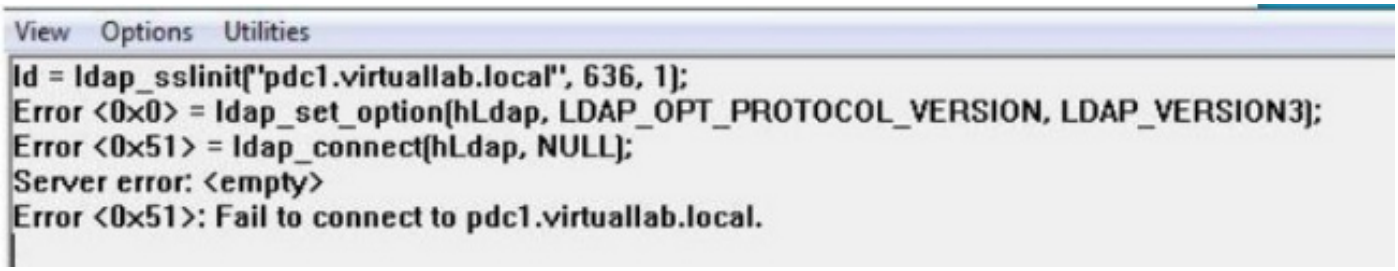
ドメインに加入した場合ルートかエンタープライズ CA を信頼するので、ずっとドメインのメンバーではないローカル Windows コンピュータのこのテストを行って下さい。 ローカル コンピュータがドメインにもはやない場合、ルートかエンタープライズ CA 認証はこのテストを行う前のローカル コンピュータ **信頼できるルート認証機関** ストアから取除く必要があります。

確認手順

ステップ 1： ldp.exe アプリケーションを起動します。 スタートメニューで [Run] をクリックします。「ldp.exeand」と入力して [OK] ボタンをクリックします。

ステップ 2： ドメインコントローラ FQDN を使用してドメインコントローラに接続して下さい。接続するために、**接続 > 接続応答**に行き、ドメインコントローラ FQDN を入力して下さい。 それから **SSL を**選択し、下記に示されているようにポート 636 規定 し、『OK』 をクリック して下さい。

ステップ 3： ルートかエンタープライズ CA がローカル コンピュータで信頼されない場合、下記にとして結果外観。 エラーメッセージはリモートサーバから届いた証明書が信頼できない認証局によって発行されたことを示します。



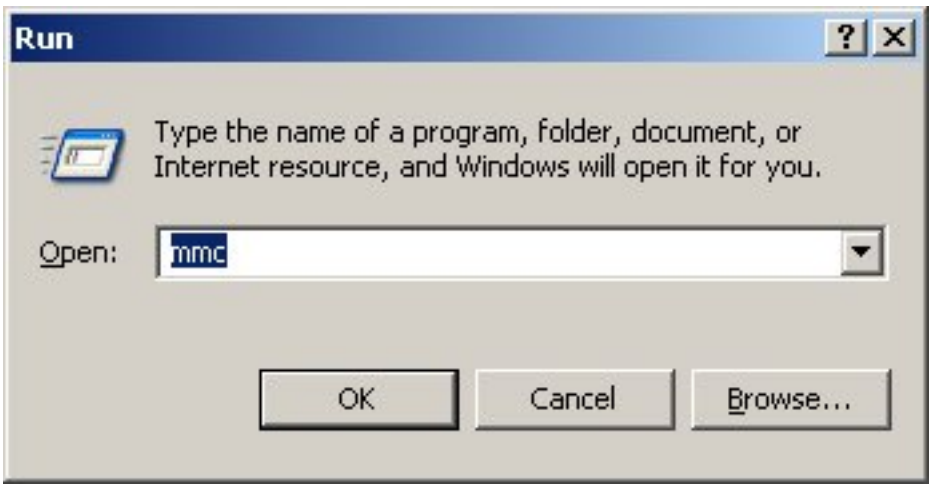
ステップ 4： 次の基準のローカル Windows コンピュータのイベントメッセージをフィルタリングすることは特定の結果を提供します:

- イベントソース = `Schannel`
- イベント ID = `36882`

ステップ 5： ローカル ウィンドウ コンピュータ 証明書 ストアに CA 認証をインポートして下さ

い。

i. Microsoft Management Console（MMC）を実行して下さい。 **Start メニュー**に行き、『Run』をクリック して下さい。 `mmc` タイプし、**OK ボタンを**押して下さい。

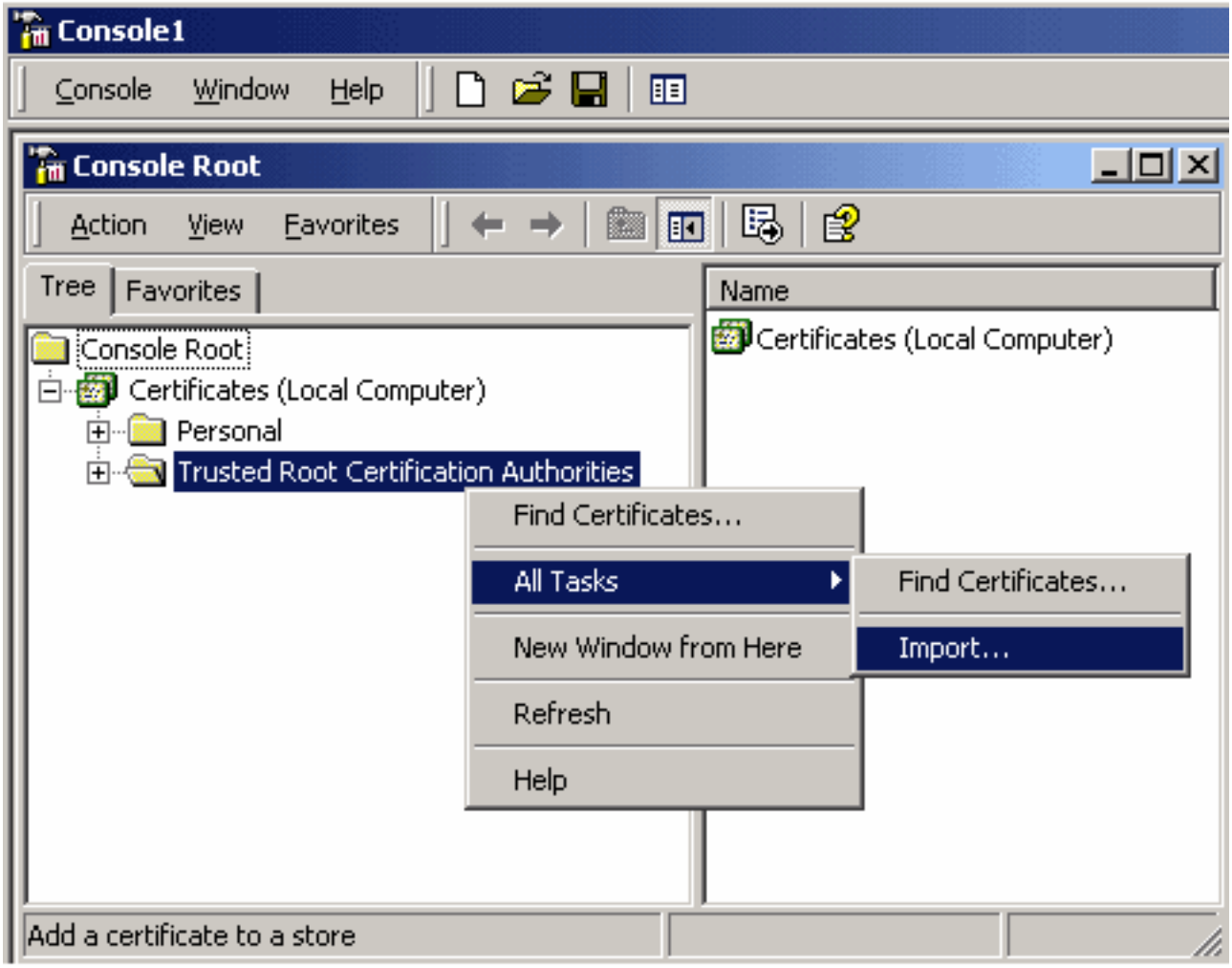


II.スナップ式ローカル コンピュータ 証明書を追加して下さい。 **File メニュー**の次のオプションにナビゲート して下さい:

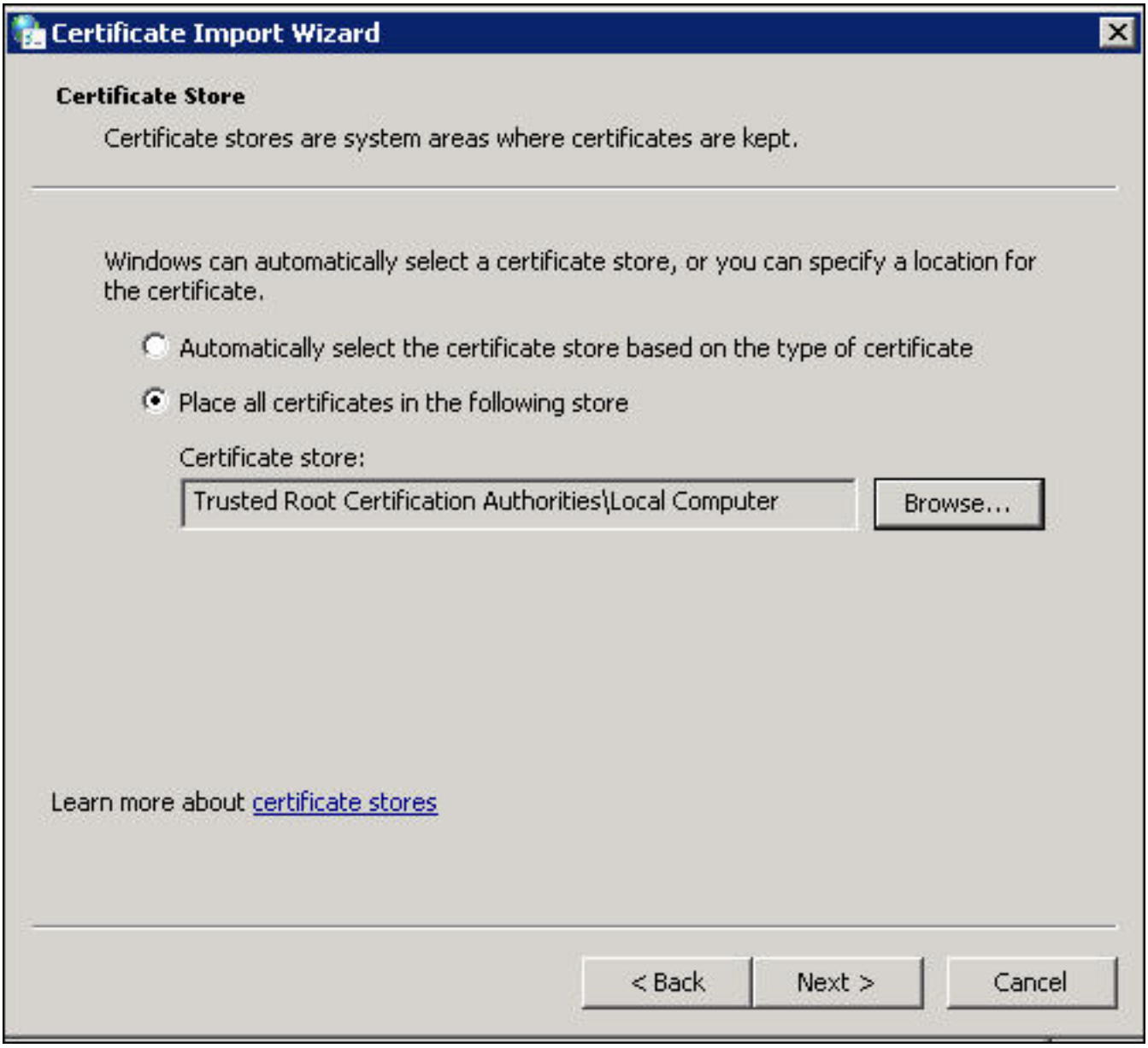
>証明書 > Add > **"Computer Account"を 選択する** > **ローカル コンピュータ追加して下さい/リモート スナップ式:（このコンソールが動かしているコンピュータ）** > **完了** > **良い。**

III. CA 認証をインポートして下さい。

Console Root > **Certificates（Local Computer）** > **Trusted Root Certification Authorities** > **Certificates** > 右クリック > **すべてのタスク** > **インポート。**



- Base64 によって符号化される X.509 証明書（`*.cer`、`*.crt`）CA 認証 ファイルに『Next』 をクリック し、参照して下さい。 それからファイルを選択して下さい。
- **> 次に**『Open』 をクリック し、『Place all certificates in the following store』 を選択 して下さい: **信頼できるルート認証機関**。
- **>** ファイルをインポートする**完了**『Next』 をクリック して下さい。



IV. CA が他の信頼されたルート CA によってリストされていることを確認して下さい。

ステップ 6： SSL 上の AD LDAPサーバに接続するためにステップ 1 および 2 に従って下さい。CA 認証が正しい場合、`ldp.exe` の右のペインの最初の 10 ラインは下記にとしてある:

```
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:
```

テスト結果

証明書および LDAP 接続がこのテストに合格する場合、うまく SSL/TLS 上の LDAP のための認

証 オブジェクトを設定できます。 ただし FireSIGHT Management Center の認証 オブジェクトを設定する前に、LDAPサーバ 設定か証明書問題によるテスト失敗が AD サーバの問題を解決するか、または正しい CA 認証をダウンロードすれば。

関連資料

- 認証オブジェクトに関する Active Directory LDAP オブジェクト属性の識別の設定
- FireSIGHT システムでの LDAP 認証オブジェクトの設定