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

内容

[概要](#)
[の検証方法](#)
[はじめに](#)
[確認手順](#)
[テスト結果](#)
[関連資料](#)

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。

の検証方法

はじめに

このドキュメントの手順を実行するには、ローカルの管理権限を持つユーザアカウントを使用して Microsoft Windows ローカルコンピュータにログインします。

> **注**：現在システムでldp.exeを使用できない場合は、まず**Windowsサポートツール**をダウンロードする必要があります。このツールは、Microsoft 社の Web サイトで入手できます。**Windowsサポートツール**をダウンロードしてインストールしたら、次の手順に従います。

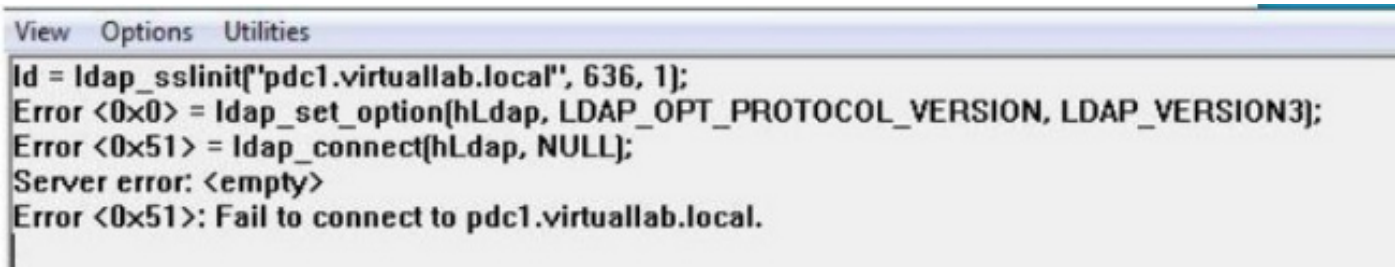
ローカル Windows コンピュータは、ドメインに参加すると、ルート CA またはエンタープライズ CA を信頼します。そのため、このテストは、ドメインのメンバーではないローカル Windows コンピュータで実行します。ローカルコンピュータがドメインに参加していない場合、このテストを実行する前に、コンピュータの [信頼されたルート証明機関（Trusted Root Certification Authorities）] ストアからルート証明書またはエンタープライズ CA 証明書を削除する必要があります。

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（Start）] メニューから [実行（Run）] を選択します。**ldp.exe**と入力し、**OK**ボタンを押します。

ステップ 2：ドメインコントローラの FQDN を使用して、ドメインコントローラに接続します。接続するには、[接続（Connection）] > [接続（Connect）] の順に移動して、ドメインコントローラの FQDN を入力します。次に、[SSL] を選択し、次に示すようにポート 636 を指定して、[OK] をクリックします。

ステップ 3：ルート CA またはエンタープライズ CA が、ローカルコンピュータで信頼されていない場合、次のような結果が表示されます。このエラーメッセージは、リモートサーバから受信し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ています。

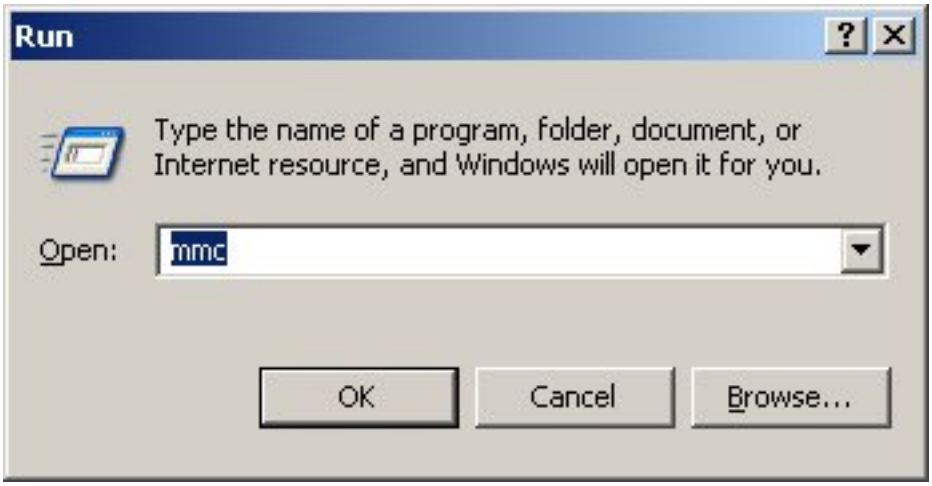


ステップ 4：ローカル Windows コンピュータのイベントメッセージを次の条件でフィルタリングすると、結果を具体的に確認できます。

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

ステップ 5：CA 証明書を、ローカル Windows コンピュータの証明書ストアにインポートします。

i.Microsoft Management Console（MMC）を起動します。 [スタートメニュー（Start）] メニューから [実行（Run）] を選択します。**mmc と入力して、[OK] ボタンをクリックします。**

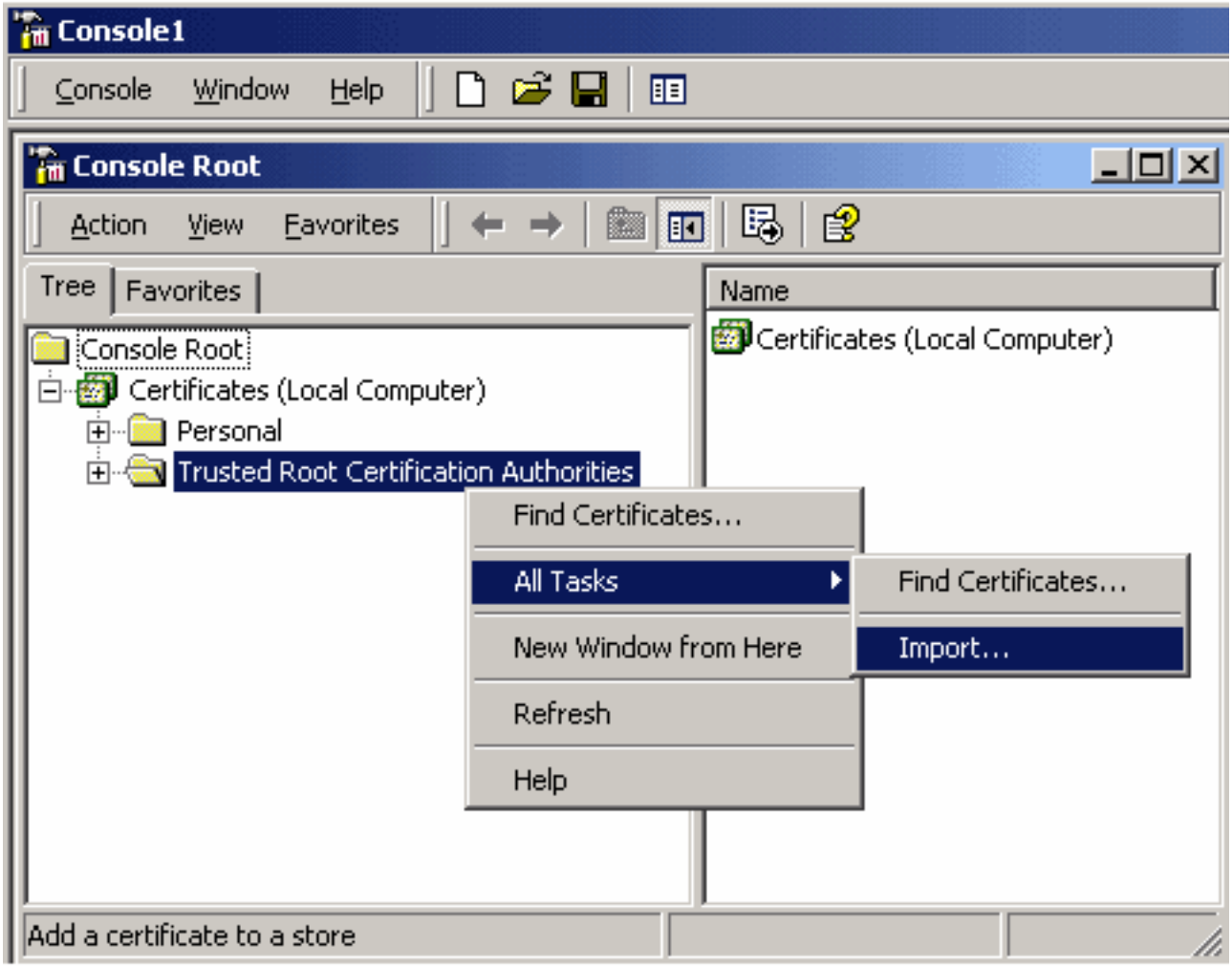


ii.ローカルコンピューター証明書スナップインを追加します。[ファイル（File）] メニューで、次のオプションに移動します。

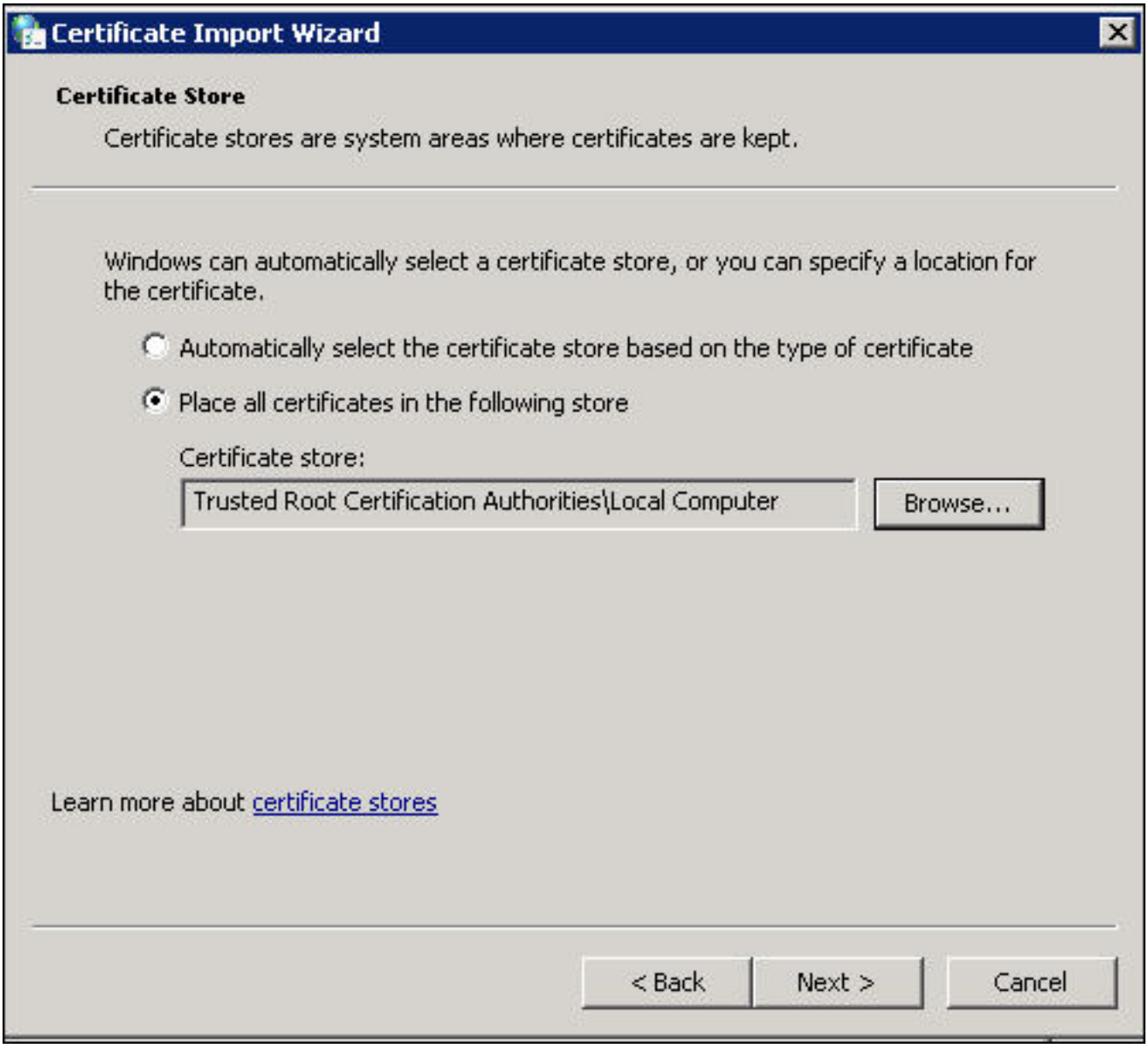
[スナップインの追加と削除（Add/Remove Snap-in）] > [証明書（Certificates）] > [追加（Add）] > [コンピューターアカウント（Computer Account）] を選択 > [ローカルコンピューター：（このコンソールを実行しているコンピューター）（Local Computer (the computer this console is running on)）] > [完了（Finish）] > [OK]

iii.CA証明書をインポートします。

[コンソールルート（Console Root）] > [証明書（ローカルコンピューター）（Certificates (Local Computer)）] > [信頼されたルート証明機関（Trusted Root Certification Authorities）] > [証明書（Certificates）] > 右クリックする > [すべてのタスク（All Tasks）] > [インポート（Import）]



- [次へ（Next）] をクリックして、Base64 でエンコードされた X.509 証明書（*.cer、*.crt）の CA 証明書ファイルを参照し、 ファイルを選択します。
- [開く（Open）] > [次へ（Next）] の順にクリックして、[証明書をすべて次のストアに配置する（Place all certificates in the following store）] : **[信頼されたルート証明機関（Trusted Root Certification Authorities）] を選択します。**
- [次へ（Next）] > [完了（Finish）] の順にクリックして、ファイルをインポートします。



iv.CAが他の信頼されたルートCAと共にリストされていることを確認します。

ステップ 6：ステップ 1 と 2 を実行し、SSL を介して AD LDAP サーバに接続します。CA 証明書が正しい場合、ldp.exe の右側のペインに表示される最初の 10 行は、次のようになります。

```
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

このテストで、証明書と LDAP 接続に問題がないことを確認できれば、SSL/TLS を介した LDAP

の認証オブジェクトを正常に設定できます。ただし、LDAP サーバの設定、または証明書の問題が原因でテストに失敗した場合は、FireSIGHT Management Center で認証オブジェクトを設定する前に、AD サーバの問題を解決するか、正しい CA 証明書をダウンロードしてください。

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