Vérifiez le LDAP au-dessus de SSL/TLS (LDAP) et le certificat de CA utilisant Ldp.exe

Contenu

Introduction

Quand vous créez un objet d'authentification à un centre de Gestion de FireSIGHT pour le LDAP de Répertoire actif au-dessus de SSL/TLS (LDAP), il peut parfois être nécessaire de tester le CERT CA et la connexion SSL/TLS, et vérifie si l'objet d'authentification échoue le test. Ce document explique comment exécuter le test utilisant Microsoft Ldp.exe.

Comment vérifier

Avant de commencer

Ouvrez une session à un ordinateur local de Microsoft Windows avec un compte utilisateur qui a le privilège d'administrateur local d'exécuter les étapes sur ce document.

> Remarque: Si vous n'avez pas actuellement `ldp.exe disponible` sur votre système, vous devez d'abord télécharger les **outils de** WindowsSupport**. C'**est disponible sur le site Web de Microsoft. Une fois que vous téléchargez et installez les **outils de** WindowsSupport**, suivez les** étapes ci-dessous.

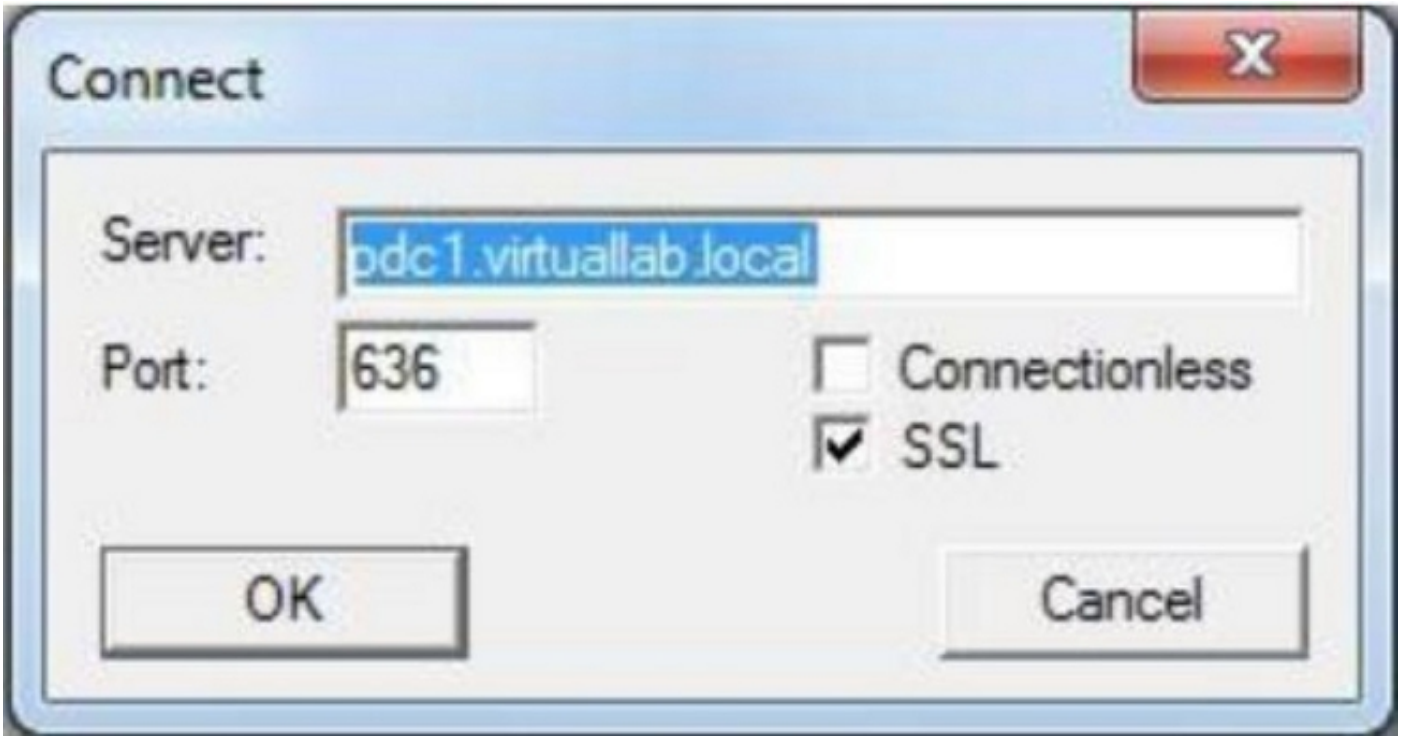
Réalisez cet essai sur un ordinateur Windows local qui n'a pas été un membre d'un domaine, car il ferait confiance à la racine ou à l'entreprise CA s'il joignait un domaine. Si un ordinateur local n'est plus dans un domaine, la racine ou le certificat de CA d'entreprise devrait être retirée de la mémoire d'**Autorités de certification racine approuvée d'**ordinateur local avant d'exécuter ce test.

Étapes de vérification

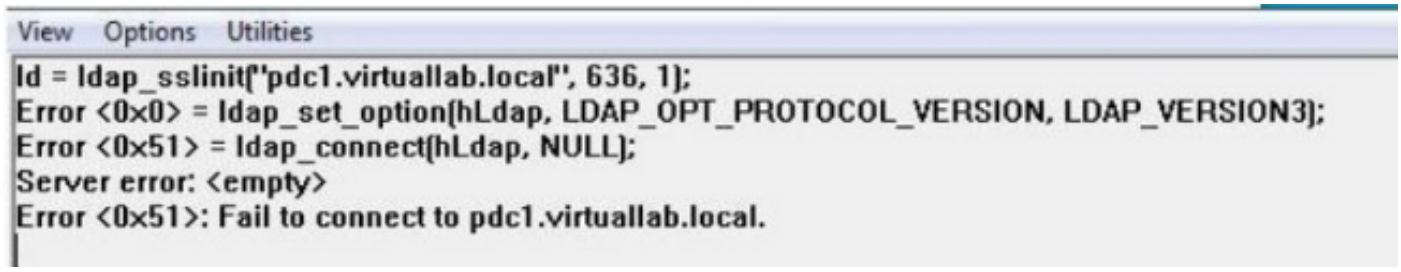
Étape 1 : `Application du` début `ldp.exe`. Allez au Startmenu et cliquez sur Run**. Le type**

ldp.exeand **`a frappé le`** bouton CORRECT.

Étape 2 : Connectez au contrôleur de domaine utilisant le FQDN de contrôleur de domaine. Afin de se connecter, allez à la **connexion > connectent** et écrivent le FQDN de contrôleur de domaine. Alors sélectionnez le **SSL**, spécifiez le port **`636`** comme affiché ci-dessous et cliquez sur OK.



Étape 3 : Si la racine ou l'entreprise CA n'est pas faite confiance sur un ordinateur local, le résultat regarde en tant que ci-dessous. Le message d'erreur indique que le certificat reçu du serveur distant a été délivré par une autorité de certification non approuvée.

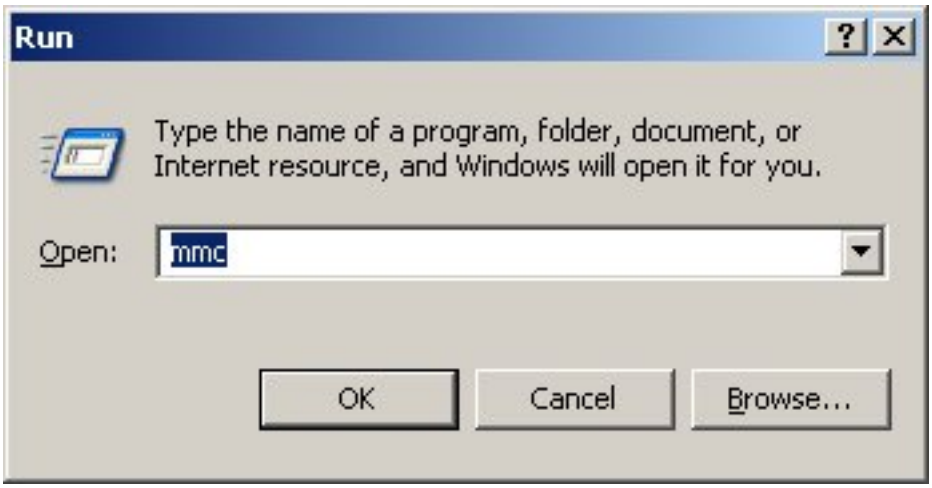


Étape 4 : Le filtrage des messages d'événement sur l'ordinateur Windows local avec les critères suivants fournit un résultat spécifique :

- Source d'événement = `Schannel`
- ID d'événement = `36882`

Étape 5 : Importez le certificat de CA à la mémoire locale de certificat d'ordinateur de fenêtres.

i. Exécutez Microsoft Management Console (MMC). Allez au **menu de démarrage** et cliquez sur Run. Type **mmc** et frappé le bouton **CORRECT**.

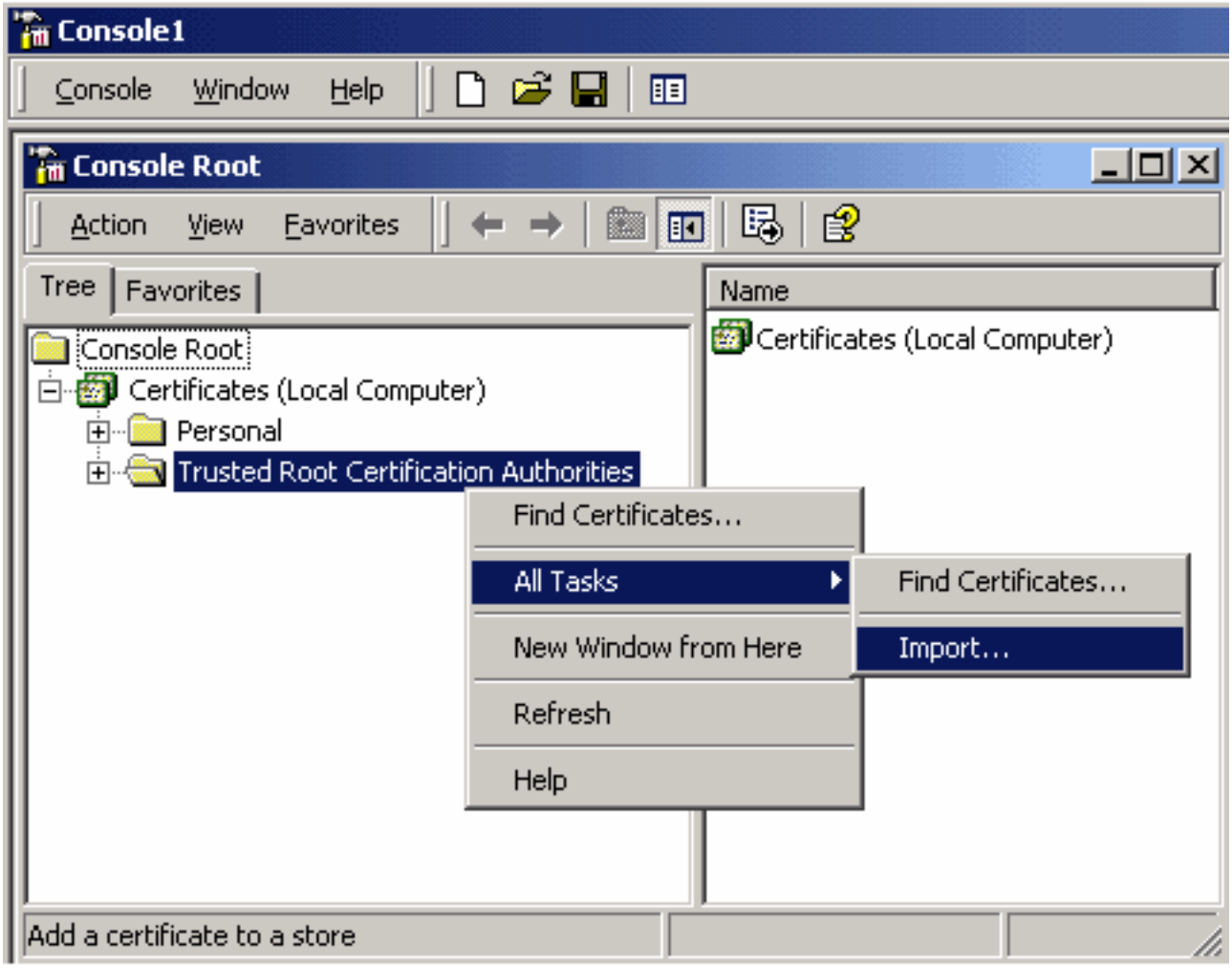


ii. Ajoutez le certificat d'ordinateur local SNAP-dans. Naviguez vers les options suivantes sur le **menu File** :

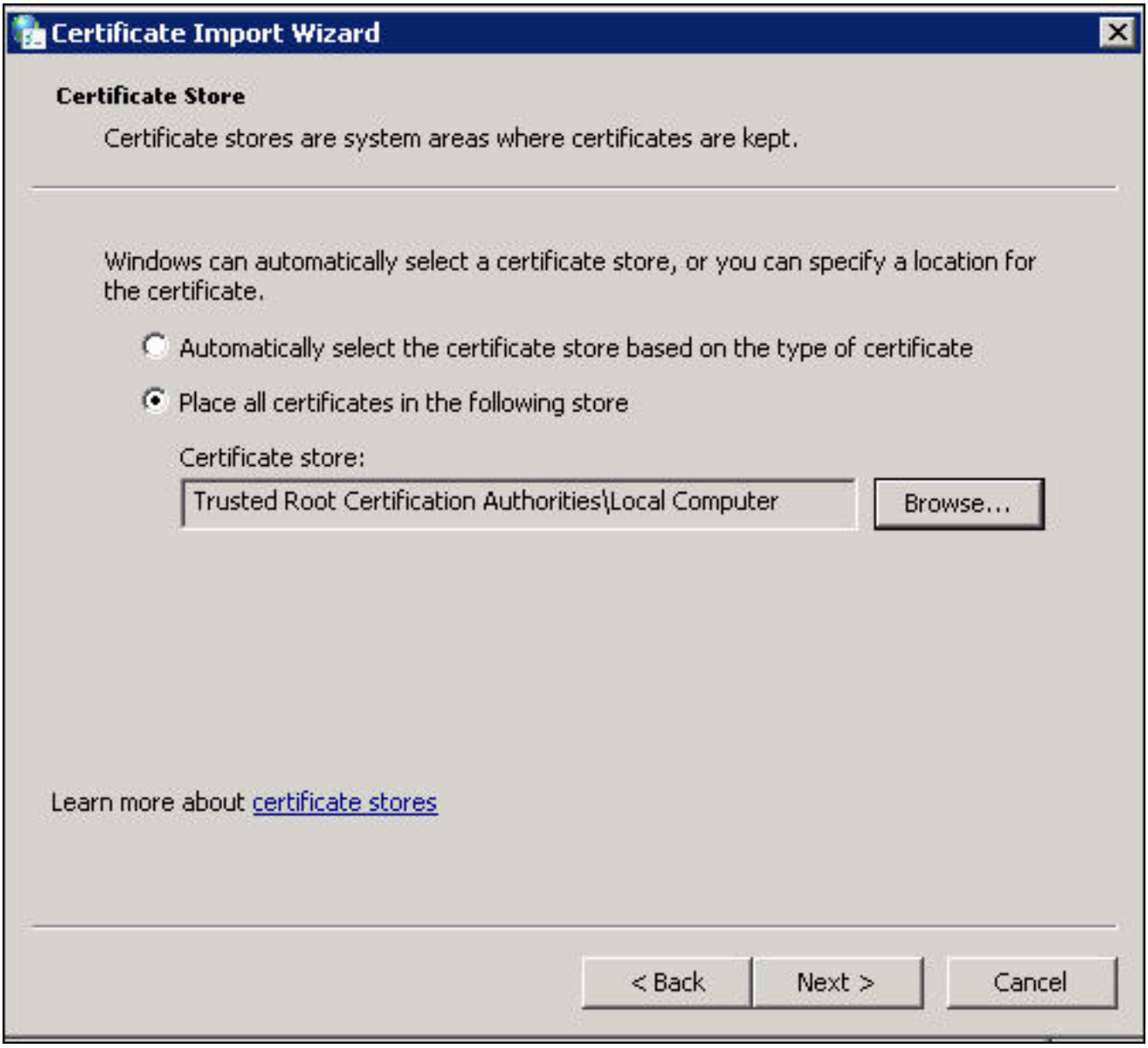
Ajoutez/distant SNAP-dans > des **Certificats > ajoutent > choisissent le « compte d'ordinateur » > ordinateur local : (l'ordinateur que cette console exécute en fonction) > finition > CORRECT**.

iii. Importez le certificat de CA.

La racine de console > délivre un certificat (ordinateur local) **>** des **Autorités de certification racine approuvée >** des **Certificats >** clic droit **> toutes les tâches > importation**.



- Cliquez sur Next et parcourez au fichier de certificat de CA du certificat X.509 encodé par Base64 (`*.cer`, `*.crt`). Sélectionnez alors le fichier.
- Le clic **ouvert > ensuite** et sélectionnent l'**endroit tous les Certificats dans la mémoire suivante : Autorités de certification racine approuvée**.
- Cliquez sur Next **> finition** pour importer le fichier.



iv. Confirmez que le CA est répertorié avec autre la racine de confiance CAs.

Étape 6 : Suivez l'étape 1 et 2 pour connecter à l'AD le serveur LDAP au-dessus du SSL. Si le certificat de CA est correct, les 10 premières lignes sur le volet de droite de `ldp.exe devraient` être en tant que ci-dessous :

```
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:
```

Résultat de test

Si un certificat et une connexion de LDAP passent ce test, vous pouvez avec succès configurer l'objet d'authentification pour le LDAP au-dessus de SSL/TLS. Cependant, si l'échouer de test dû à la configuration de serveur LDAP ou à la question de certificat, résolvent s'il vous plaît le problème sur le serveur d'AD ou téléchargent le certificat de CA correct avant que vous configuriez l'objet d'authentification au centre de Gestion de FireSIGHT.

Documents connexes

- Identifiez les attributs d'objet de LDAP de Répertoire actif pour la configuration d'objet d'authentification
- Configuration d'objet d'authentification LDAP sur le système de FireSIGHT