Vérification du certificat LDAP sur SSL/TLS (LDAPS) et CA à l'aide de Ldp.exe

Contenu

Introduction

Lorsque vous créez un objet d'authentification sur FireSIGHT Management Center pour Active Directory LDAP sur SSL/TLS (LDAPS), il peut parfois être nécessaire de tester le certificat CA et la connexion SSL/TLS, et de vérifier si l'objet d'authentification échoue au test. Ce document explique comment exécuter le test à l'aide de Microsoft Ldp.exe.

Procédure de vérification

Avant de commencer

Connectez-vous à un ordinateur local Microsoft Windows avec un compte d'utilisateur disposant du privilège d'administration local pour effectuer les étapes de ce document.

> **Note**: Si ldp.exe n'est pas actuellement disponible sur votre système, vous devez d'abord télécharger les **outils de support Windows**. Ce document est disponible sur le site Web de Microsoft. Une fois que vous avez téléchargé et installé les **outils de support Windows**, suivez les étapes ci-dessous.

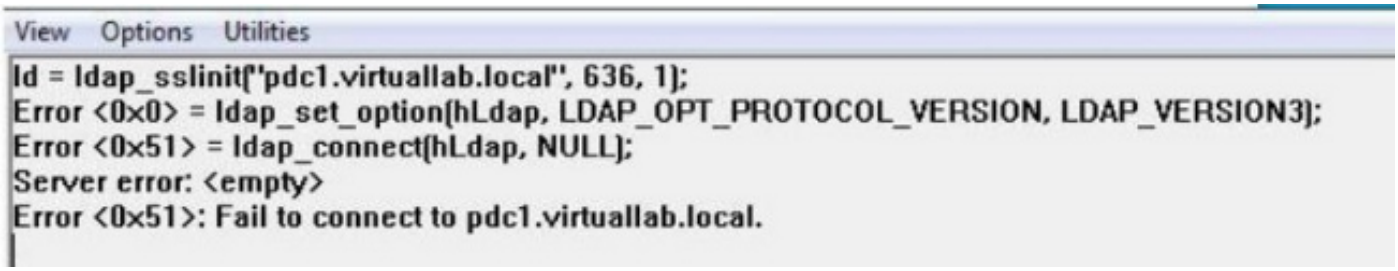
Effectuez ce test sur un ordinateur Windows local qui n'a pas été membre d'un domaine, car il ferait confiance à l'autorité de certification racine ou d'entreprise si elle rejoignait un domaine. Si un ordinateur local ne se trouve plus dans un domaine, le certificat d'autorité de certification racine ou d'entreprise doit être supprimé du magasin d'**autorités de certification racine de confiance de l'**ordinateur local avant d'effectuer ce test.

Étapes de vérification

Étape 1 : Démarrez l'application ldp.exe. Accédez au menu **Démarrer** et cliquez sur **Exécuter**. Tapez **ldp.exe** et appuyez sur le bouton **OK**.

Étape 2 : Connectez-vous au contrôleur de domaine en utilisant le nom de domaine complet du contrôleur de domaine. Pour vous connecter, allez à **Connection > Connect** et entrez le nom de domaine complet du contrôleur de domaine. Sélectionnez ensuite **SSL**, spécifiez le port **636** comme indiqué ci-dessous et cliquez sur **OK**.

Étape 3 : Si l'autorité de certification racine ou d'entreprise n'est pas approuvée sur un ordinateur local, le résultat est le suivant. Le message d'erreur indique que le certificat reçu du serveur distant a été émis par une autorité de certification non approuvée.

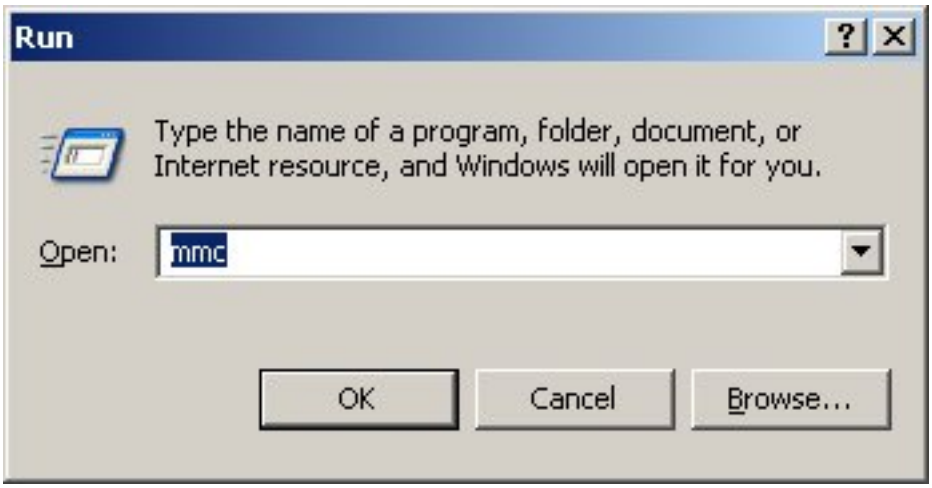


Étape 4 : Le filtrage des messages d'événement sur l'ordinateur Windows local selon les critères suivants fournit un résultat spécifique :

- Source d'événement = Canal
- ID d'événement = 36882

Étape 5 : Importez le certificat CA dans le magasin de certificats local de l'ordinateur Windows.

i. Exécutez la console MMC (Microsoft Management Console). Accédez au menu **Démarrer** et cliquez sur **Exécuter**. Tapez **mmc** et appuyez sur le bouton **OK**.

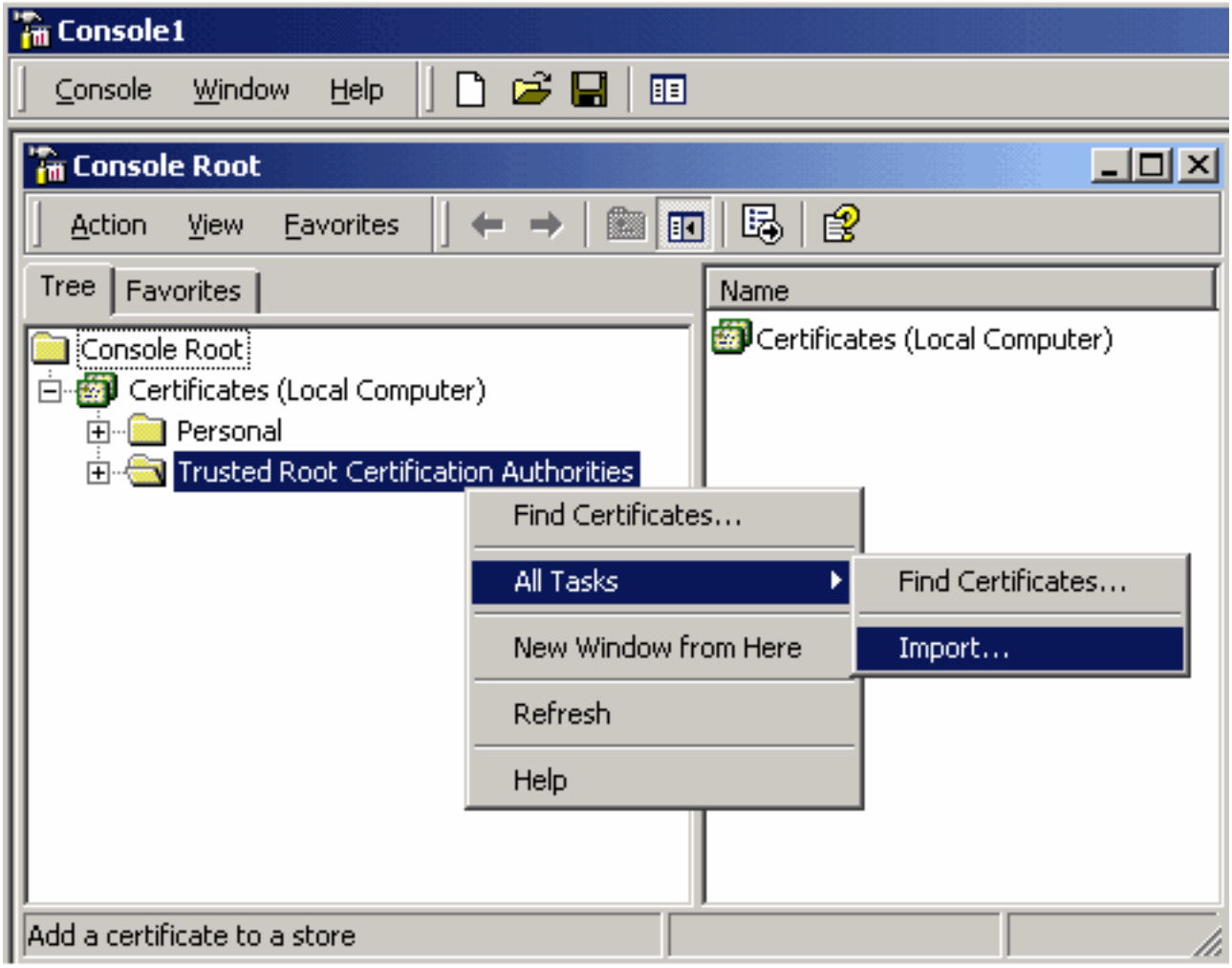


ii. Ajouter un composant logiciel enfichable Certificat d'ordinateur local. Accédez aux options suivantes du menu **Fichier** :

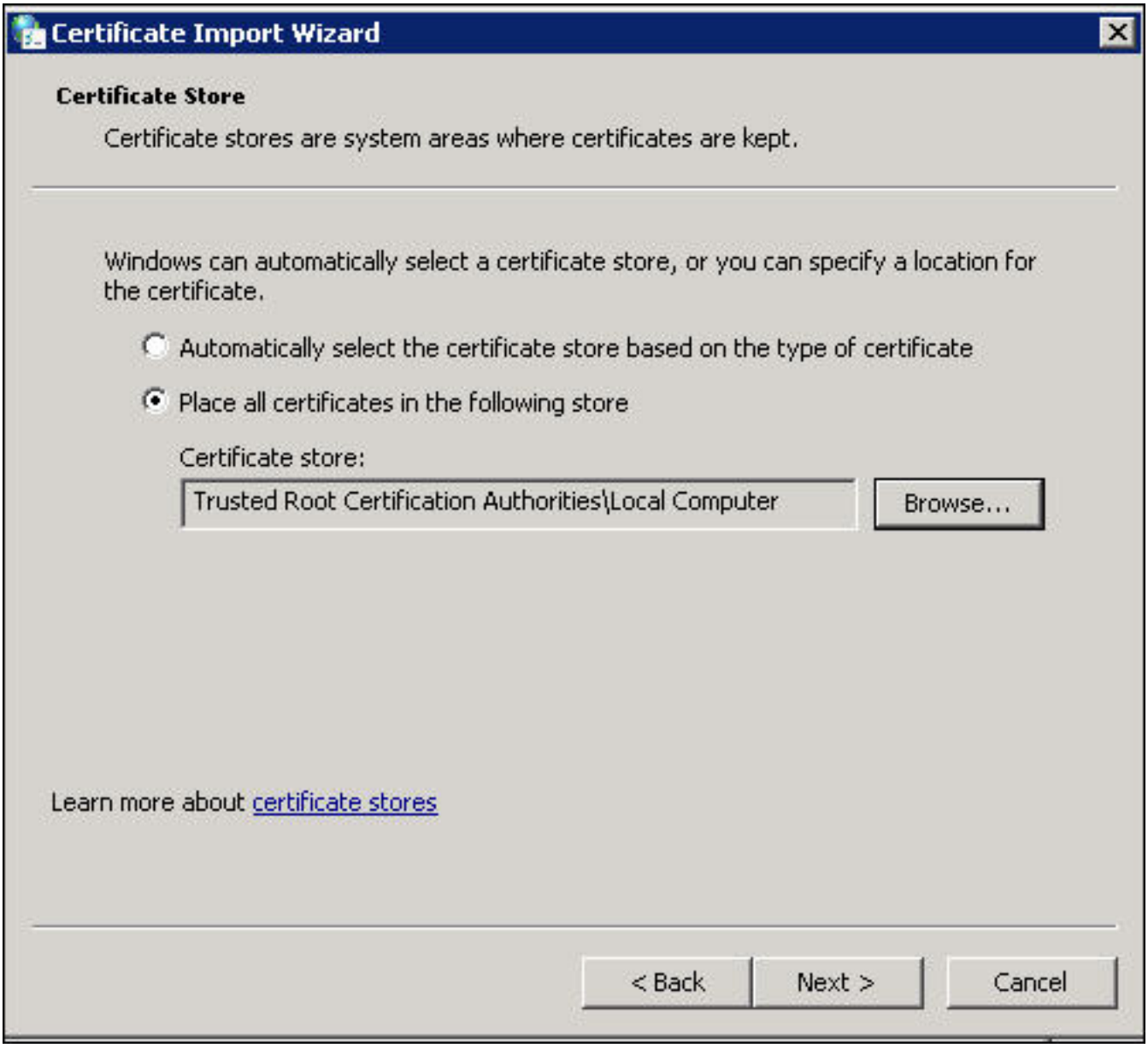
Add/Remote Snap-in > Certificates > Add > Choisissez "Computer Account" > Local Computer : (l'ordinateur sur lequel cette console est exécutée) > Terminer > OK.

iii. Importez le certificat CA.

Racine de la console > Certificats (Ordinateur local) **> Autorités de certification racines de confiance > Certificats** > Clic droit **> Toutes les tâches > Importer**.



- Cliquez sur **Next** et accédez au fichier de certificat X.509 codé en base64 (*.cer, *.crt) CA. Sélectionnez ensuite le fichier.
- Cliquez sur **Ouvrir > Suivant** et sélectionnez **Placer tous les certificats dans le magasin suivant : Autorités de certification racine de confiance**.
- Cliquez sur **Next > Finish** pour importer le fichier.



iv. Vérifiez que l'autorité de certification est répertoriée avec d'autres autorités de certification racine approuvées.

Étape 6 : Suivez les étapes 1 et 2 pour vous connecter au serveur AD LDAP via SSL. Si le certificat de l'autorité de certification est correct, les 10 premières lignes du volet droit de ldp.exe doivent être comme suit :

```
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 du test

Si un certificat et une connexion LDAP réussissent ce test, vous pouvez configurer correctement l'objet d'authentification pour LDAP sur SSL/TLS. Toutefois, si le test échoue en raison d'un problème de configuration du serveur LDAP ou de certificat, résolvez le problème sur le serveur AD ou téléchargez le certificat CA correct avant de configurer l'objet Authentication sur FireSIGHT Management Center.

Documents associés

- Identifier les attributs d'objet LDAP Active Directory pour la configuration des objets d'authentification
- Configuration de l'objet d'authentification LDAP sur le système FireSIGHT