Überprüfen Sie LDAP über SSL/TLS (LDAPS) und das CA-Zertifikat mit Ldp.exe

Inhalt

Einleitung

Wenn Sie ein Authentifizierungsobjekt in einem FireSIGHT Management Center für Active Directory LDAP über SSL/TLS (LDAPS) erstellen, müssen Sie manchmal das Zertifizierungsstellenzertifikat und die SSL/TLS-Verbindung testen und überprüfen, ob das Authentifizierungsobjekt den Test nicht besteht. In diesem Dokument wird erläutert, wie der Test mit Microsoft Ldp.exe ausgeführt wird.

Überprüfung

Vorbereitungen

Melden Sie sich bei einem lokalen Microsoft Windows-Computer mit einem Benutzerkonto mit lokaler Administratorberechtigung an, um die Schritte in diesem Dokument auszuführen.

> **Anmerkung:** Wenn ldp.exe derzeit nicht auf Ihrem System verfügbar ist, müssen Sie zunächst die **Windows-Supporttools** herunterladen. Diese finden Sie auf der Microsoft-Website. Führen Sie nach dem Herunterladen und Installieren der **Windows-Supporttools** die folgenden Schritte aus.

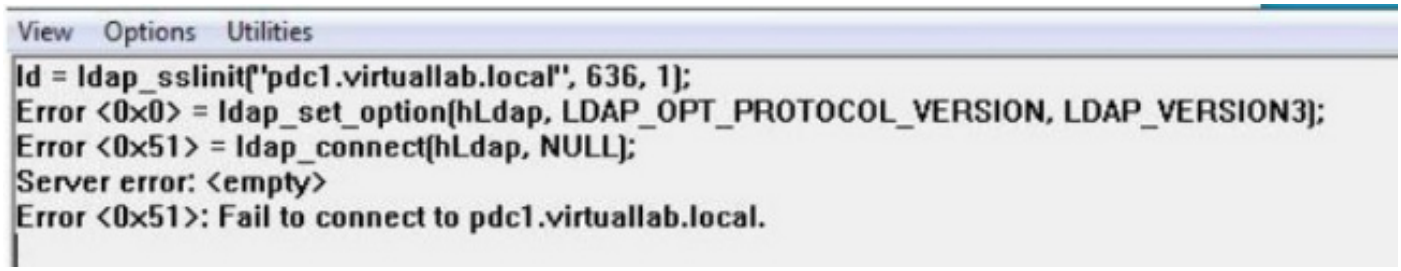
Führen Sie diesen Test auf einem lokalen Windows-Computer aus, der nicht Mitglied einer Domäne war, da er der Stamm- oder Enterprise-CA vertrauen würde, wenn sie einer Domäne beitreten würde. Wenn sich ein lokaler Computer nicht mehr in einer Domäne befindet, sollte das Zertifikat der Stammzertifizierungsstelle oder der Unternehmenszertifizierungsstelle vor dem Durchführen dieses Tests aus dem Speicher der **vertrauenswürdigen Stammzertifizierungsstellen des** lokalen Computers entfernt werden.

Verifizierungsschritte

Schritt 1: Starten Sie ldp.exe. Wechseln Sie zum Menü **Start**, und klicken Sie auf **Ausführen**. Geben Sie **ldp.exe ein**, und drücken Sie die Schaltfläche **OK**.

Phase 2: Stellen Sie über den FQDN des Domänencontrollers eine Verbindung zum Domänencontroller her. Um eine Verbindung herzustellen, gehen Sie zu **Verbindung > Verbinden,** und geben Sie den Domänen-Controller-FQDN ein. Wählen Sie anschließend **SSL aus**, geben Sie den Port **636** wie unten dargestellt an, und klicken Sie auf **OK**.

Schritt 3: Wenn die Stamm- oder Enterprise-CA auf einem lokalen Computer nicht vertrauenswürdig ist, sieht das Ergebnis wie folgt aus. Die Fehlermeldung zeigt an, dass das vom Remoteserver empfangene Zertifikat von einer nicht vertrauenswürdigen Zertifizierungsstelle ausgestellt wurde.

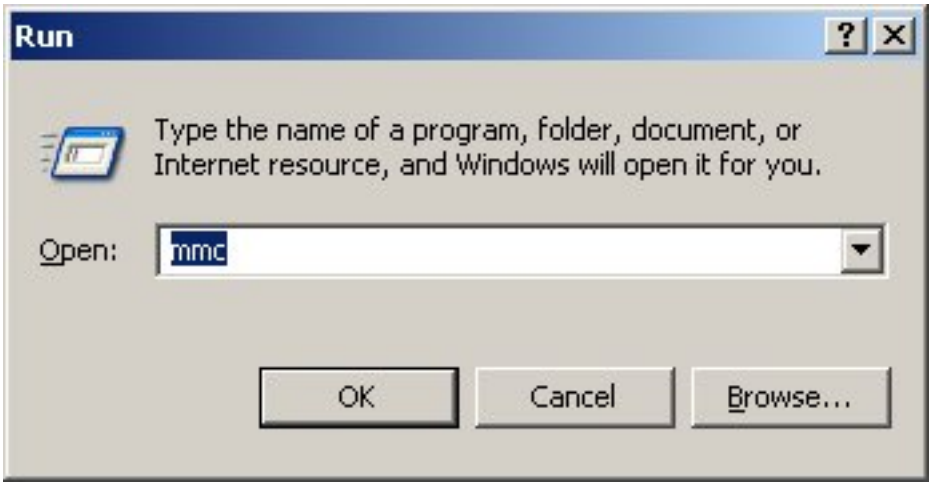


Schritt 4: Das Filtern der Ereignismeldungen auf einem lokalen Windows-Computer mit den folgenden Kriterien liefert ein bestimmtes Ergebnis:

- Ereignisquelle = Kanal
- Ereignis-ID = 36882

Schritt 5: Importieren Sie das Zertifizierungsstellenzertifikat in den Zertifikatsspeicher des lokalen Windows-Computers.

i. Führen Sie Microsoft Management Console (MMC) aus. Wechseln Sie zum Menü **Start**, und klicken Sie auf **Ausführen**. Geben Sie **mmc ein**, und drücken Sie die Taste **OK**.

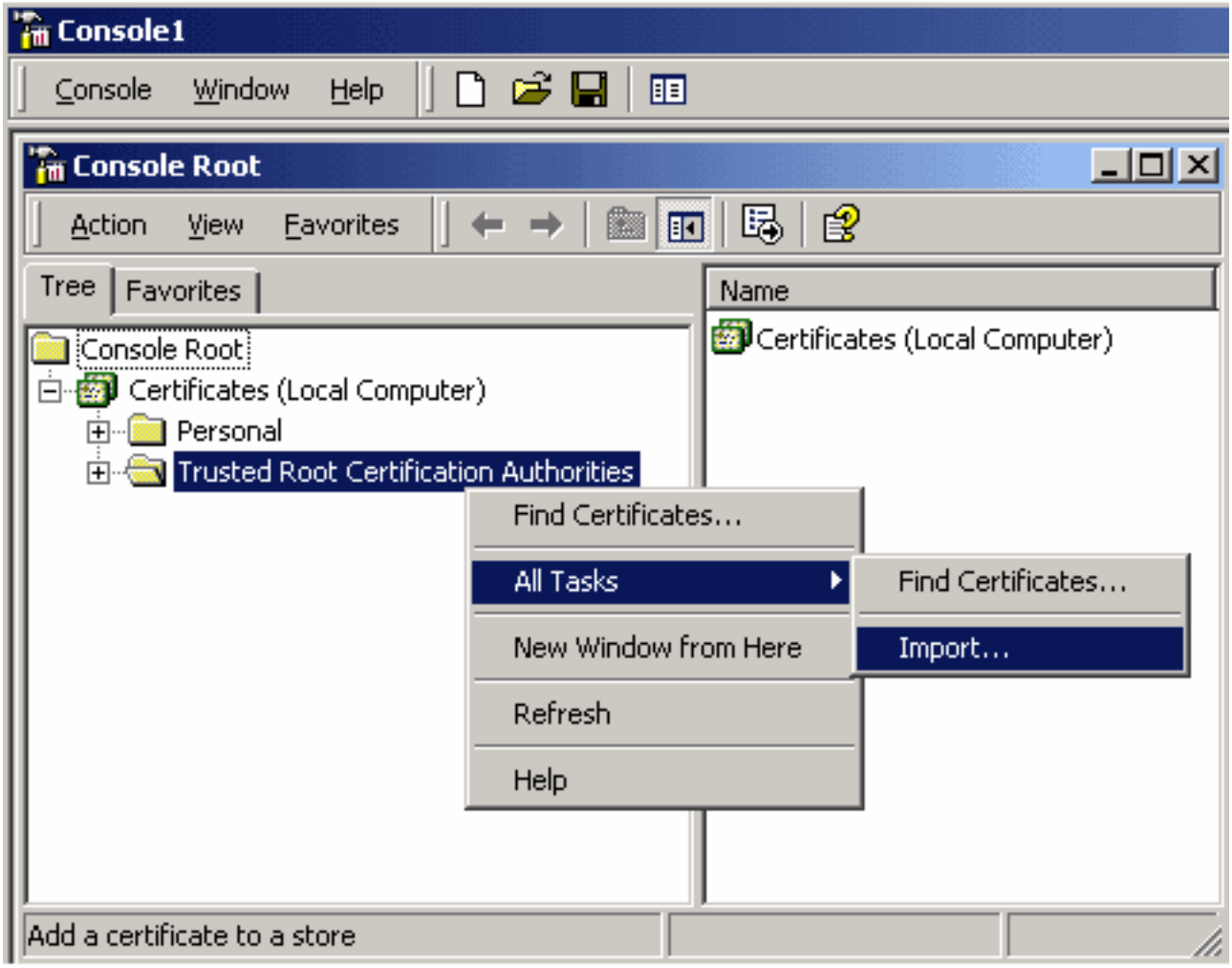


ii) Snap-In für das Zertifikat des lokalen Computers hinzufügen. Navigieren Sie im Menü **Datei** zu den folgenden Optionen:

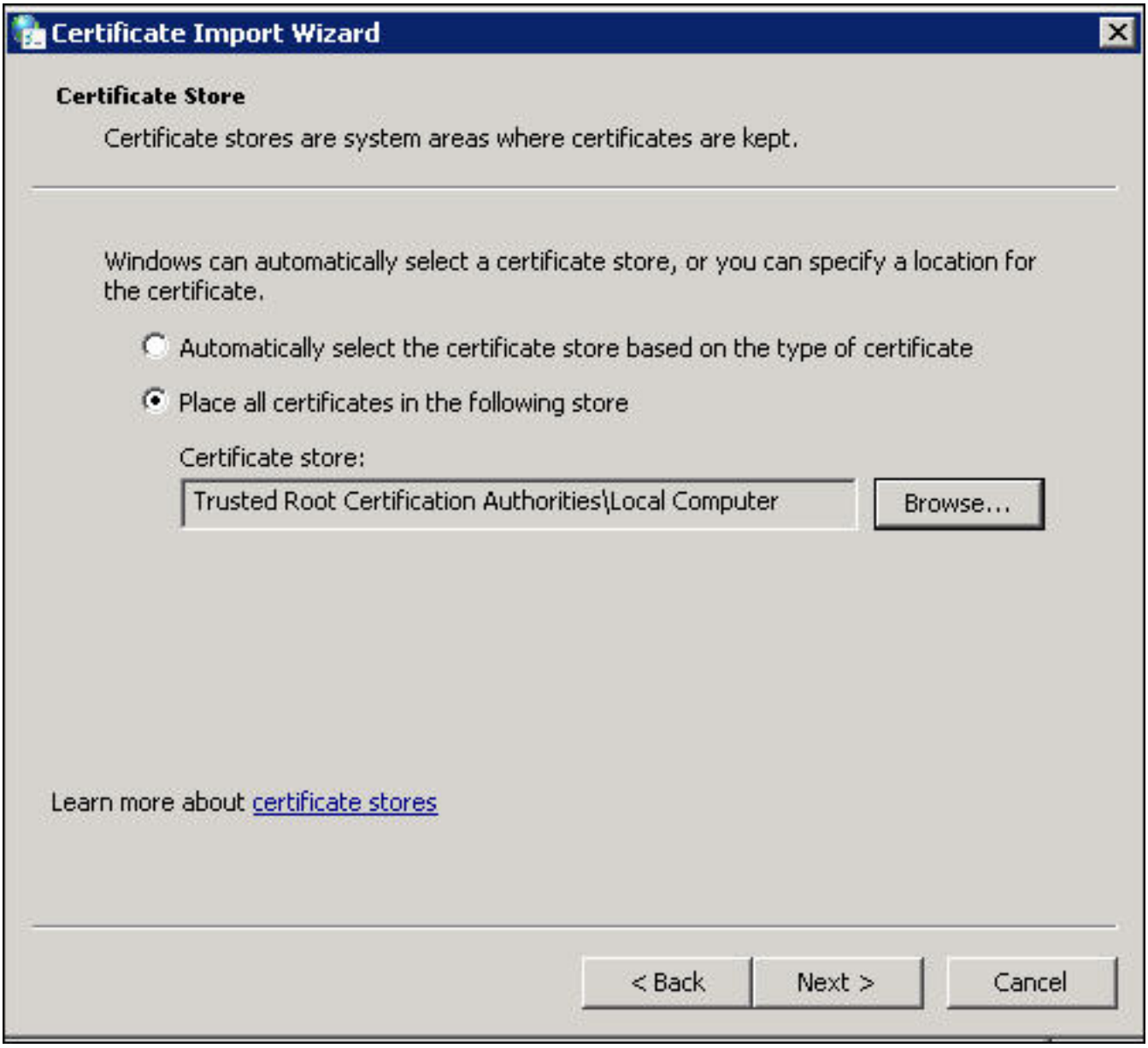
Add/Remote Snap-In > Zertifikate > Hinzufügen > Wählen Sie "Computerkonto" > Lokaler Computer: (auf dem Computer, auf dem diese Konsole ausgeführt wird) > Beenden > OK.

iii. Importieren Sie das Zertifizierungsstellenzertifikat.

Konsolenstamm > Zertifikate (Lokaler Computer) **> Vertrauenswürdige Stammzertifizierungsstellen > Zertifikate** > Rechtsklick **> Alle Aufgaben > Importieren.**



- Klicken Sie auf **Weiter**, und navigieren Sie zu Base64 Encoded X.509 Certificate (*.cer, *.crt) CA certificate file. Wählen Sie dann die Datei aus.
- Klicken Sie auf **Öffnen > Weiter**, und wählen Sie **Alle Zertifikate im folgenden Speicher platzieren: Vertrauenswürdige Stammzertifizierungsstellen**.
- Klicken Sie auf **Weiter > Fertig stellen**, um die Datei zu importieren.



iv. Bestätigen Sie, dass die Zertifizierungsstelle zusammen mit anderen vertrauenswürdigen Stammzertifizierungsstellen aufgeführt ist.

Schritt 6: Führen Sie die Schritte 1 und 2 aus, um eine Verbindung zum AD LDAP-Server über SSL herzustellen. Wenn das CA-Zertifikat korrekt ist, sollten die ersten 10 Zeilen im rechten Bereich von ldp.exe wie folgt aussehen:

```
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:
```

Testergebnis

Wenn ein Zertifikat und eine LDAP-Verbindung diesen Test bestehen, können Sie das Authentifizierungsobjekt für LDAP über SSL/TLS erfolgreich konfigurieren. Wenn der Test jedoch aufgrund einer LDAP-Serverkonfiguration oder eines Zertifikatproblems fehlschlägt, beheben Sie das Problem auf dem AD-Server, oder laden Sie das richtige CA-Zertifikat herunter, bevor Sie das Authentifizierungsobjekt im FireSIGHT Management Center konfigurieren.

Verwandte Dokumente

- Identifizieren von Active Directory-LDAP-Objektattributen für die Authentifizierungsobjektkonfiguration
- Konfiguration des LDAP-Authentifizierungsobjekts auf dem FireSIGHT-System