Controleer LDAP via SSL/TLS (LDAPS) en CA-certificaat met behulp van Ldp.exe

Inhoud

[Inleiding](#)
[Verifiëren](#)
[Voordat u begint](#)
[Verificatiestappen](#)
[Testresultaat](#)
[Verwante documenten](#)

Inleiding

Wanneer u een verificatieobject maakt op een FireSIGHT Management Center voor Active Directory LDAP over SSL/TLS (LDAPS), kan het soms nodig zijn om de CA cert en SSL/TLS-verbinding te testen en na te gaan of het verificatieobject de test niet heeft gedaan. Dit document legt uit hoe u de test kunt uitvoeren met Microsoft Ldp.exe.

Verifiëren

Voordat u begint

Meld u aan bij een lokale computer van Microsoft Windows met een gebruikersaccount met een lokaal beheerrecht om de stappen in dit document uit te voeren.

> **Opmerking:** Als u momenteel geen ldp.exe hebt dat op uw systeem beschikbaar is, moet u eerst de **Windows Support Tools** downloaden. Dit is beschikbaar op de Microsoft website. Nadat u de **Windows-ondersteuningstools** hebt gedownload en geïnstalleerd, volgt u de onderstaande stappen.

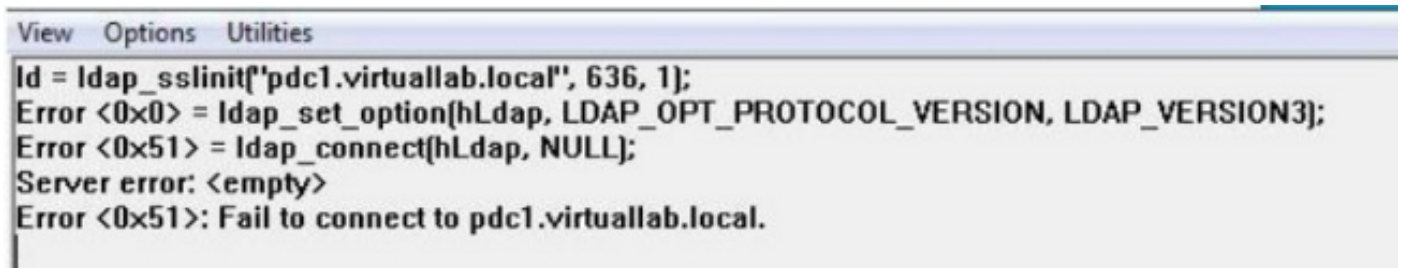
Voer deze test uit op een lokale Windows computer die geen lid van een domein is geweest, omdat het Root of Enterprise CA zou vertrouwen als het zich bij een domein aansluit. Als een lokale computer niet langer in een domein is, moet het certificaat Root of Enterprise CA voordat deze test wordt uitgevoerd, worden verwijderd uit de winkel van de lokale computer **Trusted Root-certificeringsinstanties**.

Verificatiestappen

Stap 1: Start ldp.exe-toepassing. Ga naar het menu **Start** en klik op **Uitvoeren**. Type **ldp.exe** en druk op de knop **OK**.

Stap 2: Connect met de Domain Controller met behulp van de domeincontroller FQDN. Ga om verbinding te maken naar **Connection > Connect** en voer de Domain Controller FQDN in. Selecteer vervolgens **SSL**, specificeer poort **636** zoals hieronder weergegeven en klik op **OK**.

Stap 3: Als Root of Enterprise CA niet op een lokale computer is vertrouwd, ziet het resultaat er als volgt uit. De foutmelding geeft aan dat het certificaat dat van de externe server is ontvangen, is afgegeven door een onvertrouwde certificeringsinstantie.

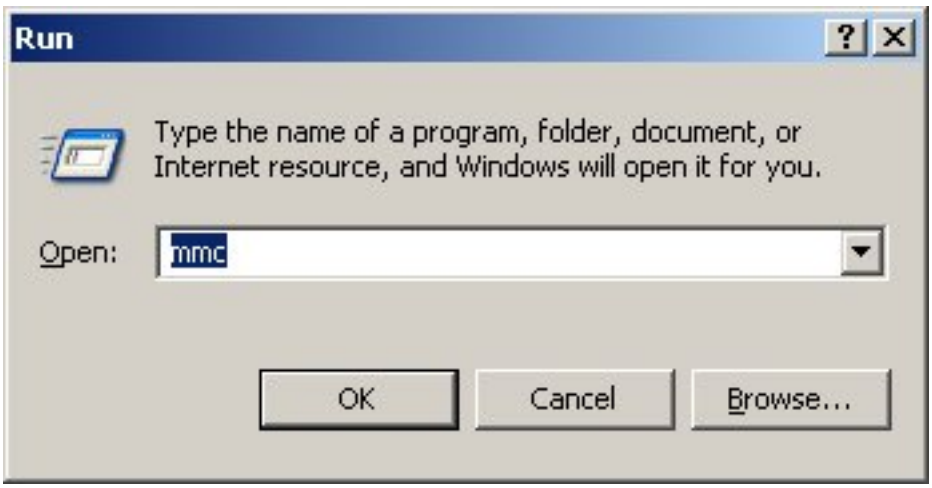


Stap 4: Het filteren van de gebeurtenis berichten op lokale Windows computer met de volgende criteria verstrekt een specifiek resultaat:

- Event Source = Schannel
- Event-ID = 36882

Stap 5: Importeer het CA-certificaat aan de lokale Windows-computercertificeringswinkel.

i. Start Microsoft Management Console (MMC). Ga naar het menu **Start** en klik op **Uitvoeren**. Typ **mmc** en druk op de knop **OK**.

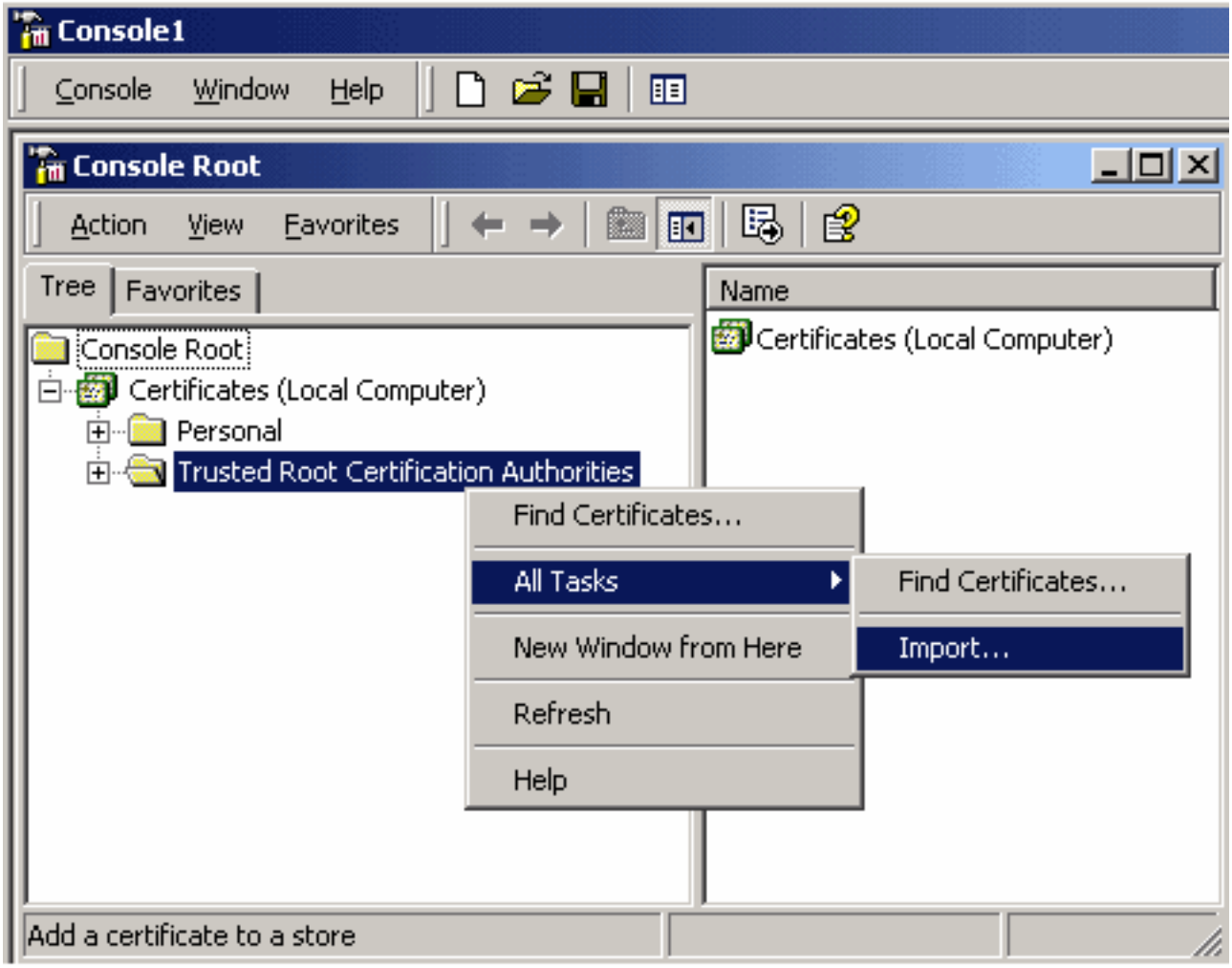


ii. Voeg lokaal computercertificaat toe. navigeren naar de volgende opties in het menu **Bestand**:

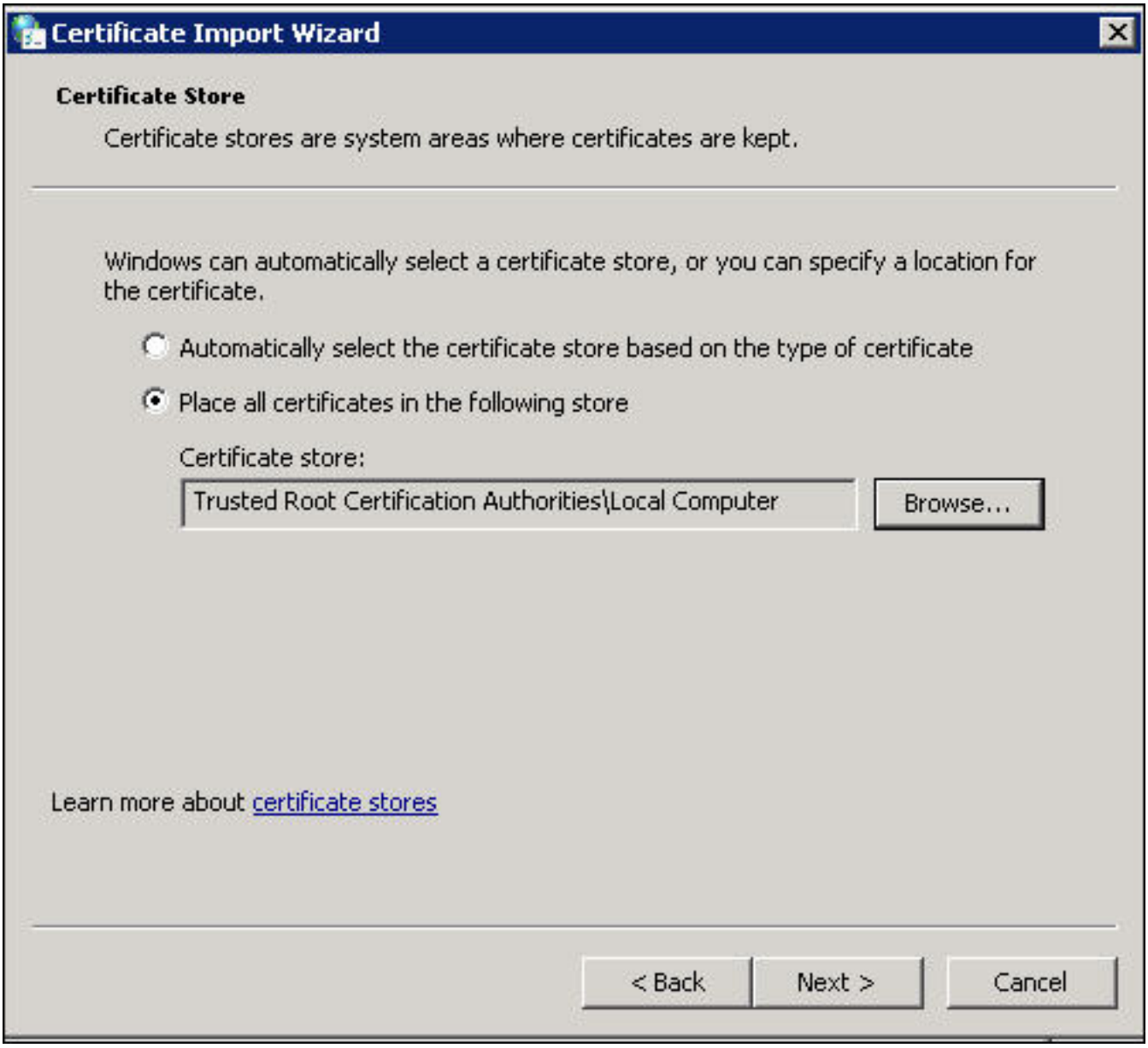
Add/Remote Magnetisch-in > Certificaten >Add >"Computer-account" >Local Computer: (de computer waarop deze console is ingeschakeld) > Voltooien > OK.

iii. Importeer het CA-certificaat.

Console Root > Certificaten (lokale computer) **> Trusted Root-certificeringsinstanties > Certificaten** > Rechtsklik **> Alle taken >Importeren**.



- Klik op **Next** en Bladeren naar Base64 Encoded X.509 certificaatbestand (*.cer, *.crt) bij CA-certificaat. Selecteer vervolgens het bestand.
- Klik op **Openen > Volgende** en selecteer **Plaats alle certificaten in de volgende winkel: Trusted Root-certificeringsinstanties**.
- Klik op **Volgende > Voltooien** om het bestand te importeren.



iv. Bevestig dat de CA in de lijst staat met andere vertrouwde bron-CA's.

Stap 6: Volg stap 1 en 2 om verbinding te maken met de AD LDAP server via SSL. Als het CA-certificaat juist is, dienen de eerste 10 lijnen in het rechter venster van ldp.exe als volgt te zijn:

```
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:
```

Testresultaat

Als een certificaat en LDAP verbinding deze test doorstaan, kunt u met succes de verificatieobject

voor LDAP via SSL/TLS configureren. Als de test echter mislukt vanwege de configuratie van de LDAP-server of de certificatenkwestie, lost u de kwestie op op de AD-server of download u het juiste CA-certificaat voordat u de verificatieobject op het FireSIGHT Management Center configureren.

Verwante documenten

- Identificeer actieve Directory LDAP Objectkenmerken voor verificatie Objectconfiguratie
- Configuratie van LDAP verificatieobject op FireSIGHT-systeem