Verificación de LDAP sobre SSL/TLS (LDAPS) y certificado de CA mediante Ldp.exe

Contenido

Introducción

Cuando crea un objeto de autenticación en un FireSIGHT Management Center para Active Directory LDAP sobre SSL/TLS (LDAP), a veces puede ser necesario probar el certificado de CA y la conexión SSL/TLS, y verificar si el objeto de autenticación no supera la prueba. Este documento explica cómo ejecutar la prueba con Microsoft Ldp.exe.

Cómo verificar

Antes de comenzar

Inicie sesión en un equipo local de Microsoft Windows con una cuenta de usuario con privilegios administrativos locales para realizar los pasos de este documento.

> **Nota:** Si actualmente no tiene ldp.exe disponible en su sistema, primero debe descargar las **Herramientas de soporte técnico de Windows**. Esta opción está disponible en el sitio web de Microsoft. Una vez que descargue e instale las **Herramientas de soporte técnico de Windows**, siga los pasos que se indican a continuación.

Realice esta prueba en un equipo Windows local que no haya sido miembro de un dominio, ya que confiaría en la CA raíz o empresarial si se uniera a un dominio. Si un equipo local ya no está en un dominio, el certificado de CA raíz o de empresa debe quitarse del almacén de **entidades emisoras raíz de confianza del** equipo local antes de realizar esta prueba.

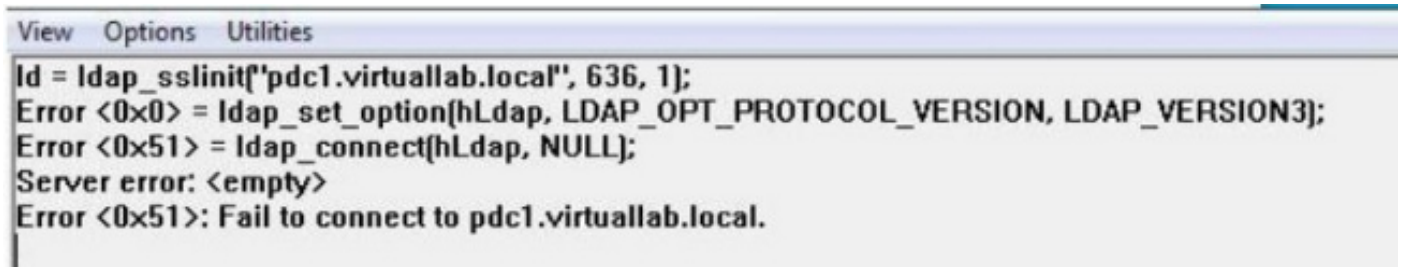
Pasos de verificación

Paso 1: Inicie la aplicación ldp.exe. Vaya al menú **Inicio** y haga clic en **Ejecutar**. Escriba **ldp.exe** y

presione el botón **OK**.

Paso 2: Conéctese al controlador de dominio mediante el FQDN del controlador de dominio. Para conectarse, vaya a **Connection > Connect** e ingrese el FQDN del controlador de dominio. A continuación, seleccione **SSL**, especifique el puerto **636** como se muestra a continuación y haga clic en **Aceptar**.

Paso 3: Si la entidad emisora de certificados raíz o empresarial no es de confianza en un equipo local, el resultado será el siguiente. El mensaje de error indica que el certificado recibido del servidor remoto fue emitido por una entidad emisora de certificados no confiable.

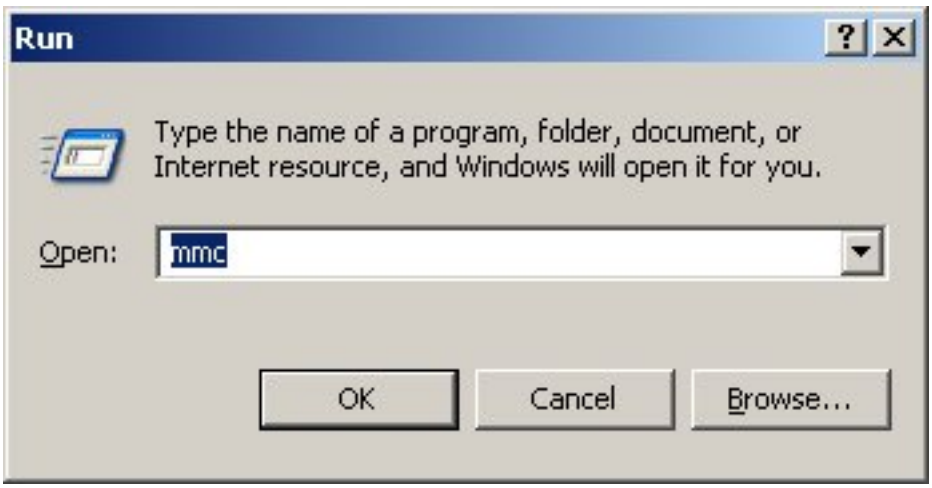


Paso 4: Filtrar los mensajes de eventos en el equipo Windows local con los siguientes criterios proporciona un resultado específico:

- Origen de evento = Schannel
- ID de evento = 36882

Paso 5: Importe el certificado de CA en el almacén de certificados del equipo Windows local.

i. Ejecute Microsoft Management Console (MMC). Vaya al menú **Inicio** y haga clic en **Ejecutar**. Escriba **mmc** y presione el botón **OK**.

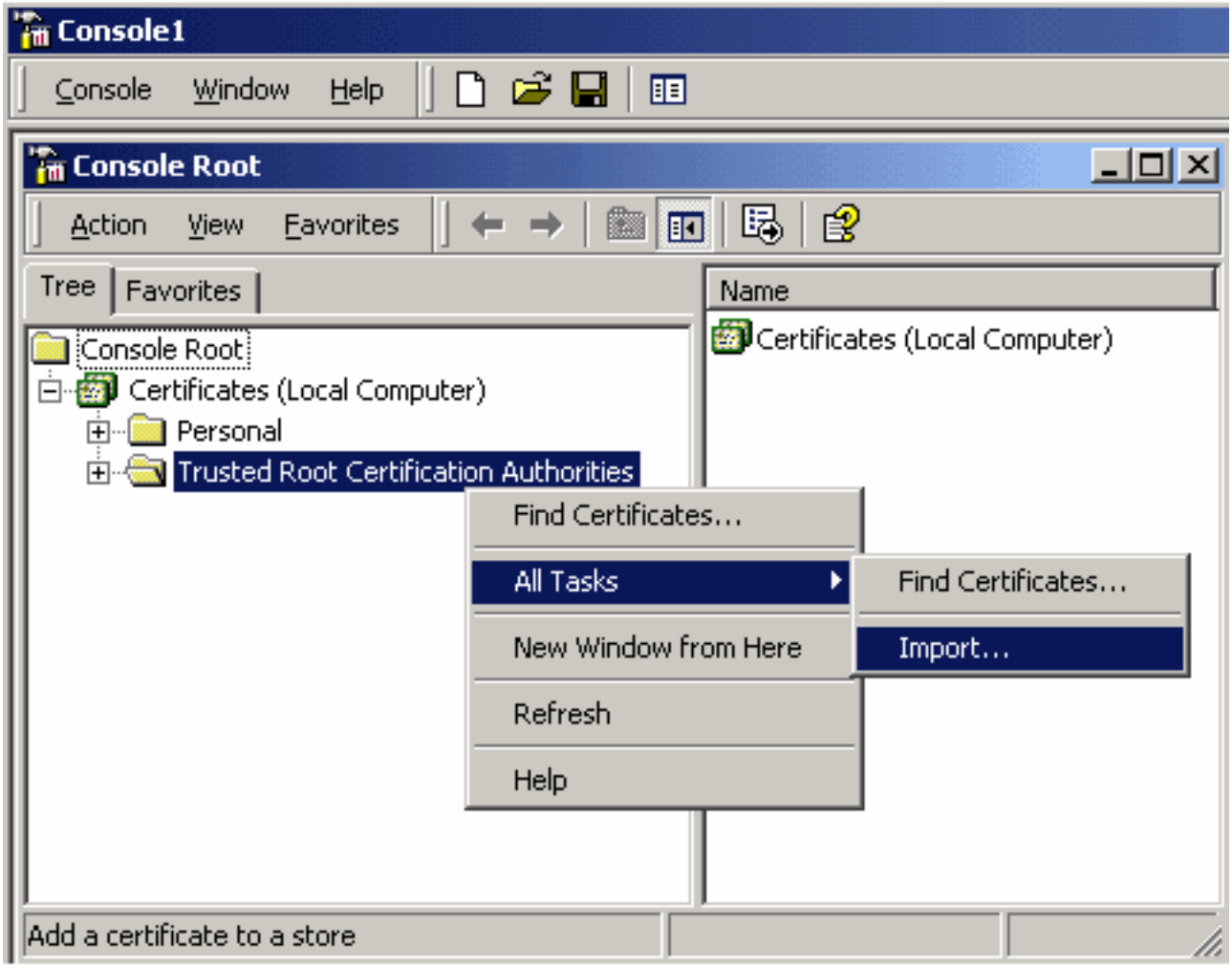


ii. Agregar complemento de certificado de equipo local. Vaya a las opciones siguientes del menú **Archivo**:

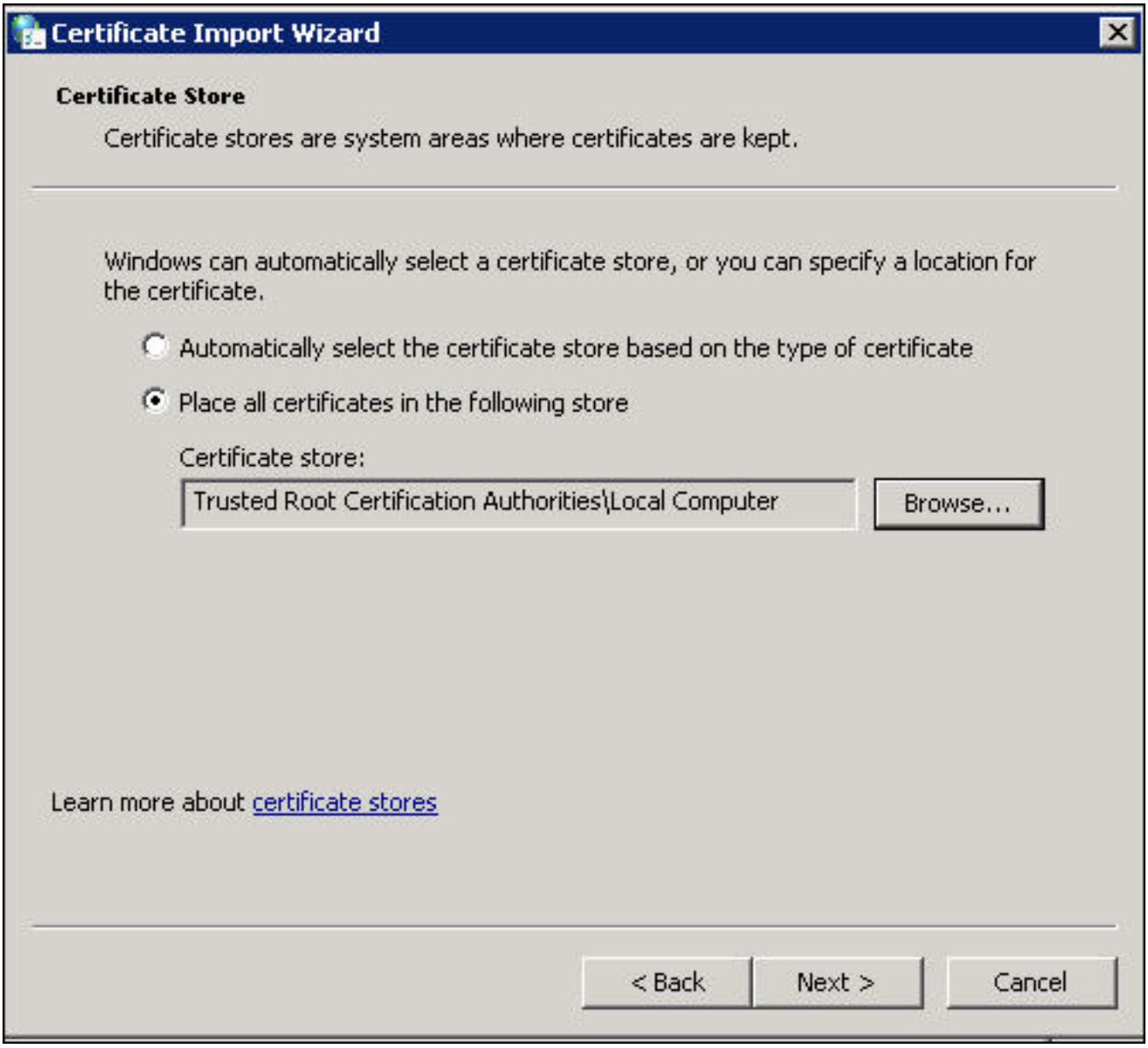
Complemento Agregar/Remoto > Certificados > Agregar > Elija "Cuenta de equipo" > Equipo local: (el ordenador en el que se está ejecutando esta consola) > Finish > OK.

iii. Importe el certificado de la CA.

Raíz de consola > Certificados (equipo local) **> Entidades emisoras de certificados raíz de confianza > Certificados >** Haga clic con el botón secundario **> Todas las tareas > Importar**.



- Haga clic en **Next** y busque el archivo de certificado de CA con codificación Base64 X.509 (*.cer, *.crt). A continuación, seleccione el archivo.
- Haga clic en **Abrir > Siguiente** y seleccione **Colocar todos los certificados en el siguiente almacén: Entidades de certificación raíz de confianza**.
- Haga clic en **Next > Finish** para importar el archivo.



iv. Confirme que la CA aparezca con otras CA raíz de confianza.

Paso 6: Siga los pasos 1 y 2 para conectarse al servidor LDAP de AD sobre SSL. Si el certificado de la CA es correcto, las primeras 10 líneas del panel derecho de ldp.exe deben ser las siguientes:

```
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:
```

Resultado de la prueba

Si un certificado y una conexión LDAP pasan esta prueba, puede configurar correctamente el objeto de autenticación para LDAP sobre SSL/TLS. Sin embargo, si la prueba falla debido a una configuración del servidor LDAP o a un problema de certificado, resuelva el problema en el servidor AD o descargue el certificado de CA correcto antes de configurar el objeto de autenticación en FireSIGHT Management Center.

Documentos Relacionados

- Identificar atributos de objeto LDAP de Active Directory para la configuración del objeto de autenticación
- Configuración del objeto de autenticación LDAP en el sistema FireSIGHT