Verificar LDAP sobre SSL/TLS (LDAPS) e Certificado CA Usando Ldp.exe

Contents

Introduction

Quando você cria um Objeto de autenticação em um FireSIGHT Management Center para LDAP do Ative Diretory sobre SSL/TLS (LDAPS), às vezes pode ser necessário testar o certificado CA e a conexão SSL/TLS e verificar se o Objeto de autenticação falha no teste. Este documento explica como executar o teste usando o Microsoft Ldp.exe.

Como verificar

Antes de Começar

Faça login em um computador local Microsoft Windows com uma conta de usuário que tenha privilégio administrativo local para executar as etapas neste documento.

> **Note**: Se você não tiver o ldp.exe disponível no momento em seu sistema, será necessário primeiro baixar as **Ferramentas de Suporte do Windows**. Disponível no site da Microsoft. Após baixar e instalar as **Ferramentas de Suporte do Windows**, siga as etapas abaixo.

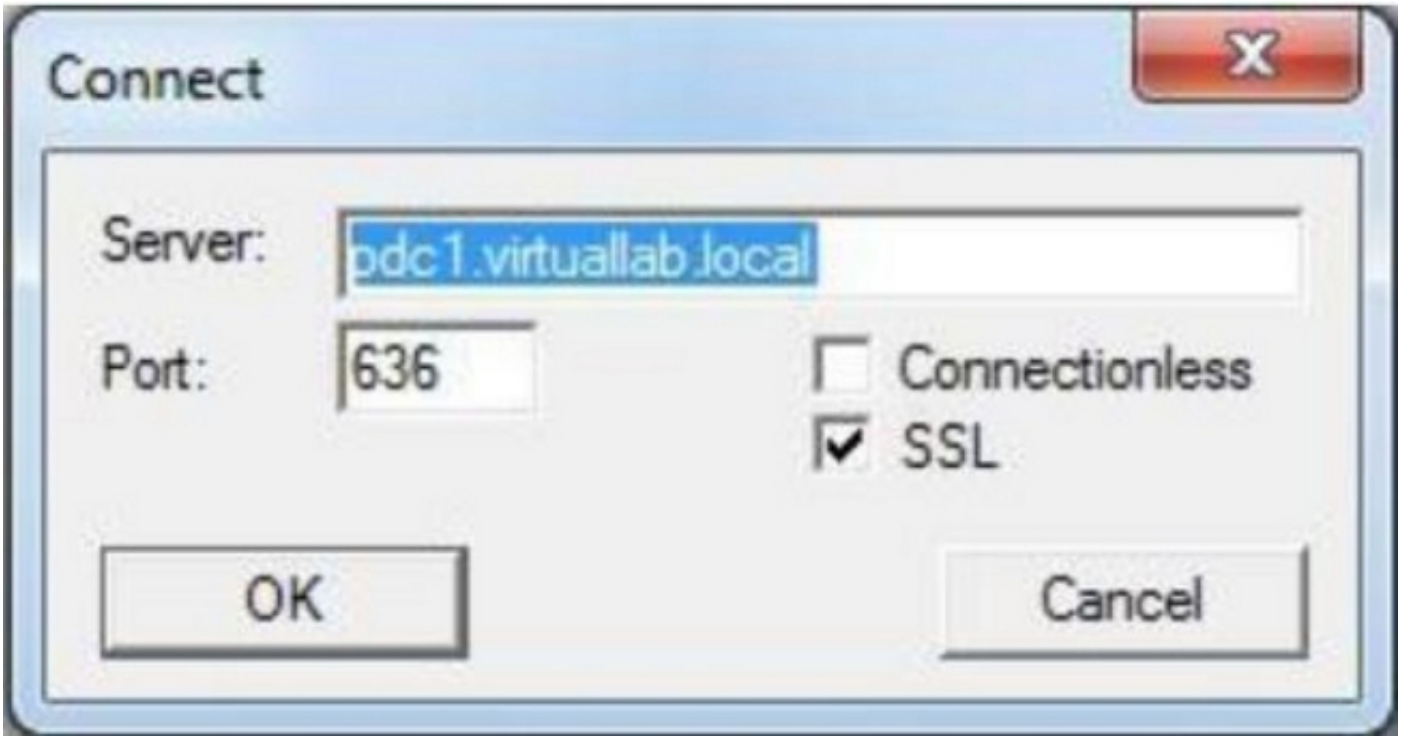
Execute este teste em um computador local Windows que não tenha sido membro de um domínio, pois ele confiaria na raiz ou na autoridade de certificação empresarial se ingressasse em um domínio. Se um computador local não estiver mais em um domínio, o certificado de CA Corporativa ou Raiz deverá ser removido do **armazenamento de Autoridades de Certificação Raiz Confiáveis** do computador local antes da execução deste teste.

Etapas de verificação

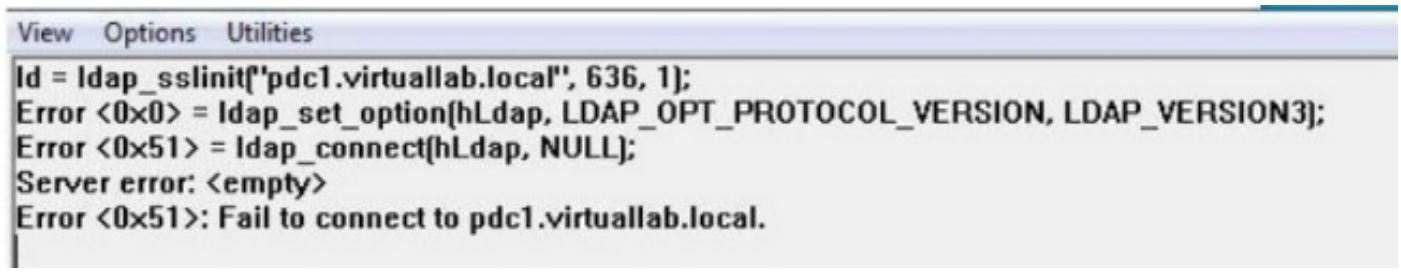
Etapa 1: Inicie o aplicativo ldp.exe. Vá para o menu **Iniciar** e clique em **Executar**. Digite **ldp.exe** e

pressione o botão **OK**.

Passo 2: Conecte-se ao Controlador de Domínio usando o FQDN do controlador de domínio. Para se conectar, vá para **Connection > Connect** e insira o FQDN do controlador de domínio. Em seguida, selecione **SSL**, especifique a porta **636** conforme mostrado abaixo e clique em **OK**.



Passo 3: Se a raiz ou a autoridade de certificação empresarial não for confiável em um computador local, o resultado será semelhante ao mostrado abaixo. A mensagem de erro indica que o certificado recebido do servidor remoto foi emitido por uma autoridade de certificação não confiável.

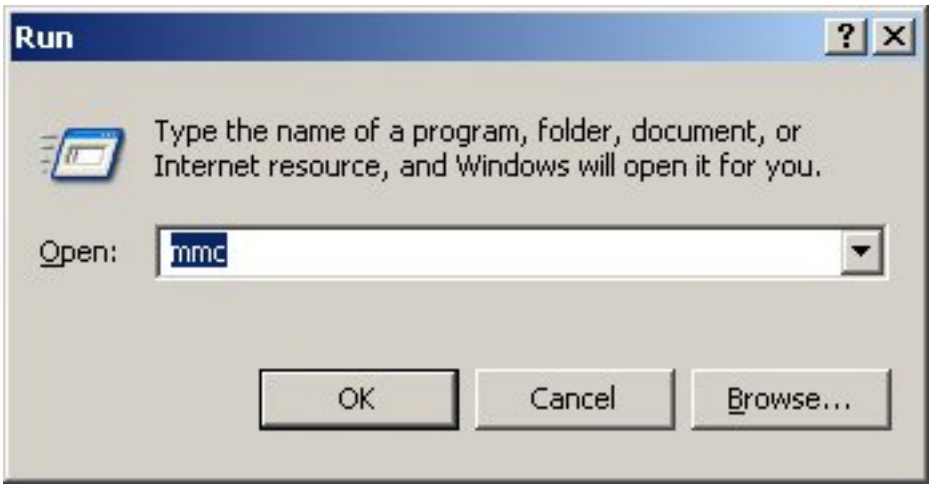


Passo 4: A filtragem das mensagens de evento no computador local do Windows com os critérios a seguir fornece um resultado específico:

- Origem do evento = Schannel
- ID do evento = 36882

Passo 5: Importe o Certificado de Autoridade de Certificação para o repositório local de certificados de computadores do Windows.

i. Execute o Console de Gerenciamento Microsoft (MMC). Vá para o menu **Iniciar** e clique em **Executar**. Digite **mmc** e pressione o botão **OK**.

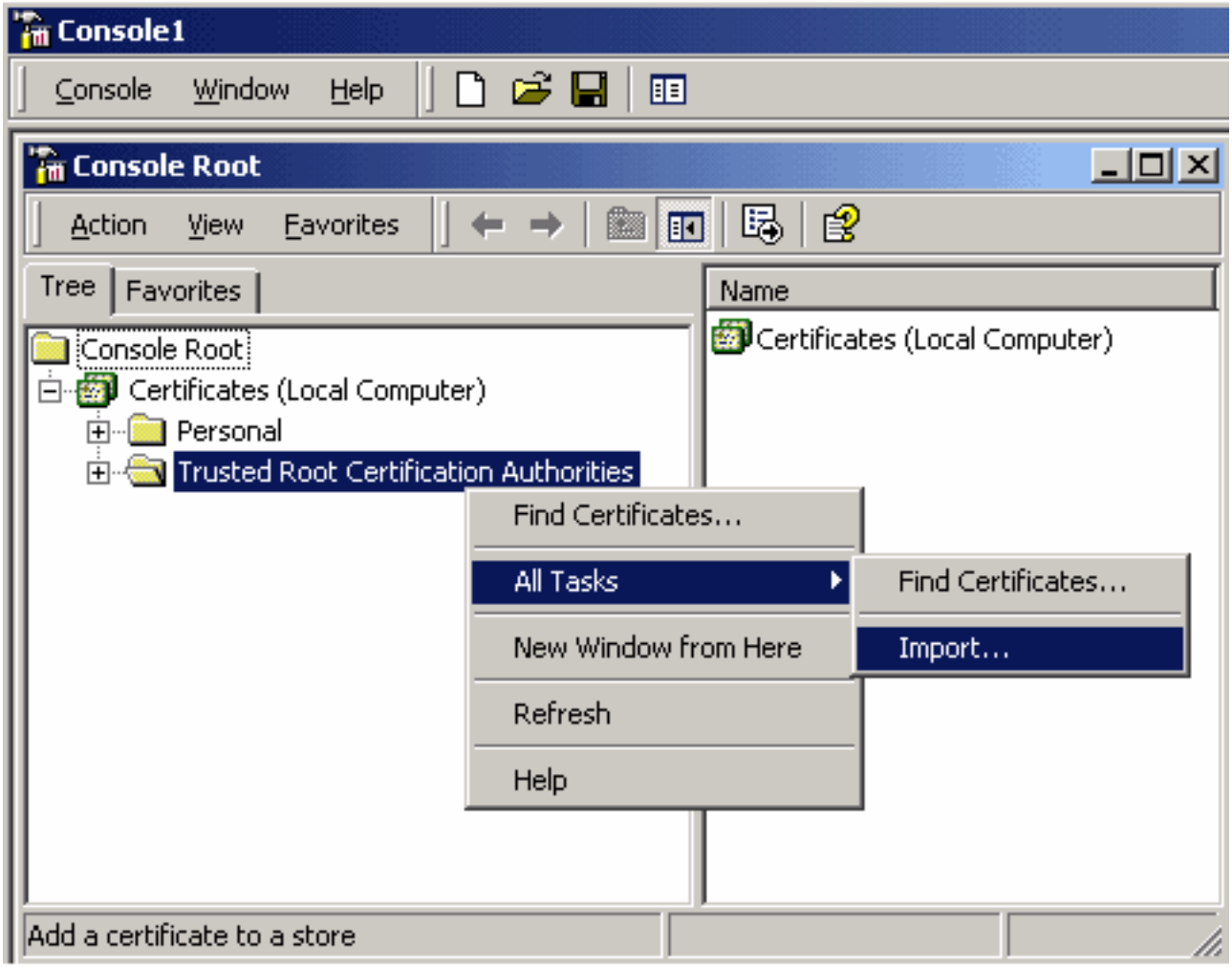


ii) Adicionar snap-in de certificado de computador local. Navegue até as seguintes opções no menu **Arquivo**:

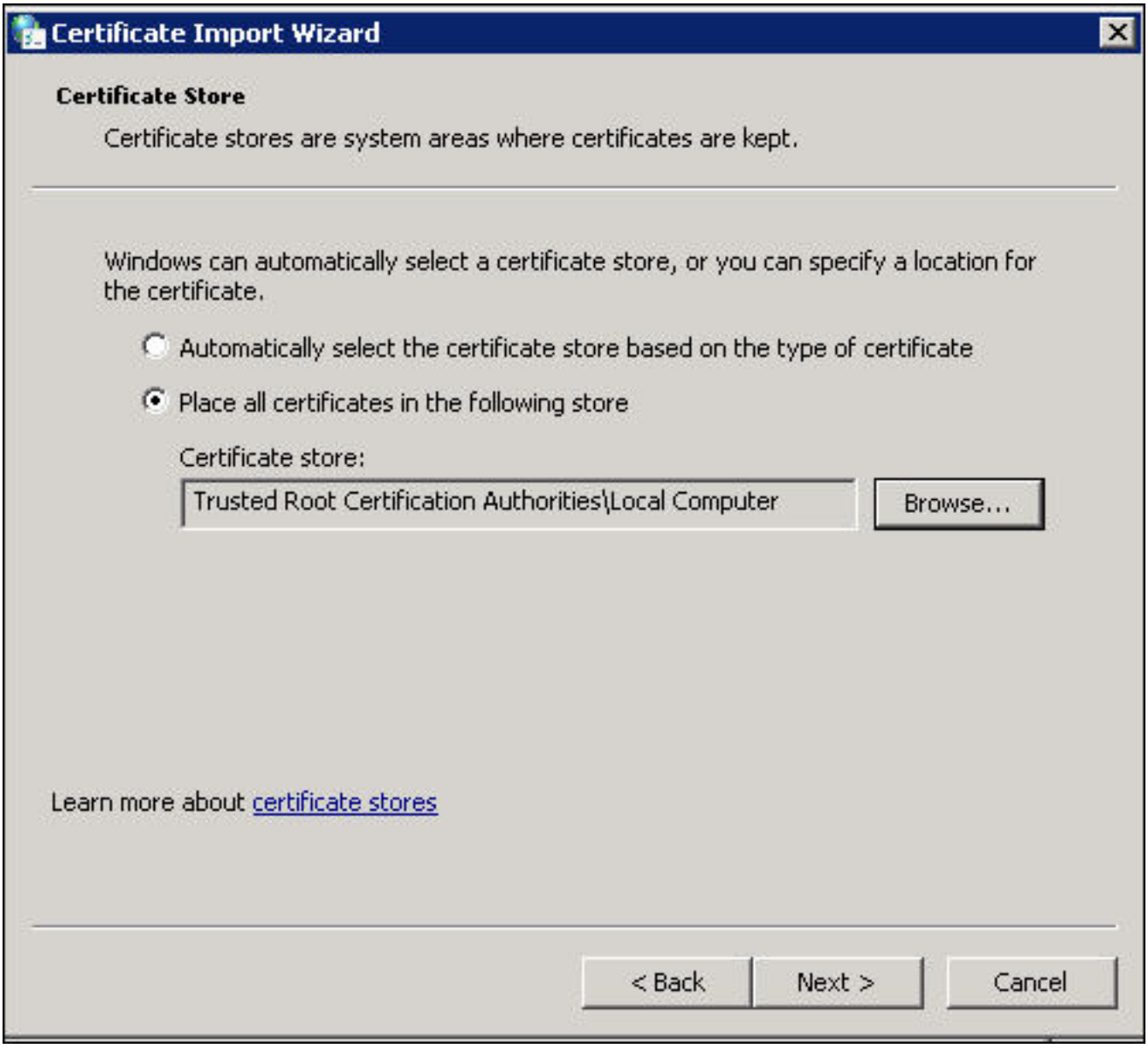
Add/Remote Snap-in > Certificates > Add > Selecione "Computer Account" > Computador local: (o computador no qual este console está sendo executado) > Concluir > OK.

iii) Importe o certificado CA.

Raiz do Console > Certificados (Computador Local) **> Autoridades de Certificação Raiz Confiáveis > Certificados** > Clique com o botão direito do mouse **> Todas as Tarefas > Importar**.



- Clique em **Avançar** e navegue até o arquivo de certificado CA Base64 codificado X.509 (*.cer, *.crt). Em seguida, selecione o arquivo.
- Clique em **Abrir > Próximo** e selecione **Colocar todos os certificados no seguinte armazenamento: Autoridades de Certificação Raiz Confiáveis**.
- Clique em **Avançar > Concluir** para importar o arquivo.



iv) Confirme se a CA está listada com outras CAs raiz confiáveis.

Passo 6: Siga as etapas 1 e 2 para se conectar ao servidor AD LDAP por SSL. Se o certificado CA estiver correto, as 10 primeiras linhas no painel direito de ldp.exe devem ser as seguintes:

```
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 do teste

Se um certificado e uma conexão LDAP forem aprovados nesse teste, você poderá configurar

com êxito o Objeto de autenticação para LDAP sobre SSL/TLS. No entanto, se o teste falhar devido à configuração do servidor LDAP ou a um problema de certificado, resolva o problema no servidor AD ou baixe o certificado CA correto antes de configurar o Objeto de autenticação no FireSIGHT Management Center.

Documentos relacionados

- Identificar Atributos de Objeto LDAP do Ative Diretory para Configuração de Objeto de Autenticação
- Configuração do objeto de autenticação LDAP no sistema FireSIGHT