# Verifique o LDAP sobre SSL/TLS (LDAP) e o certificado de CA usando Ldp.exe

## Índice



## Introdução

Quando você criar um objeto da autenticação em um centro de gerenciamento de FireSIGHT para o diretório ativo LDAP sobre SSL/TLS (LDAP), pode às vezes ser necessário testar o CERT de CA e a conexão SSL/TLS, e verifica se o objeto da autenticação falha o teste. Este documento explica como executar o teste usando Microsoft Ldp.exe.

## Como verificar

### Antes de Começar

Entre a um computador local de Microsoft Windows com uma conta de usuário que tenha o privilégio administrativo local executar as etapas neste documento.

> Nota: Se você não tem atualmente `ldp.exe disponível em` seu sistema, você deve primeiramente transferir as **ferramentas de** WindowsSupport**. Isto** está disponível na site do microsoft. Uma vez que você transfere e instala as **ferramentas de** WindowsSupport**, siga as** etapas abaixo.

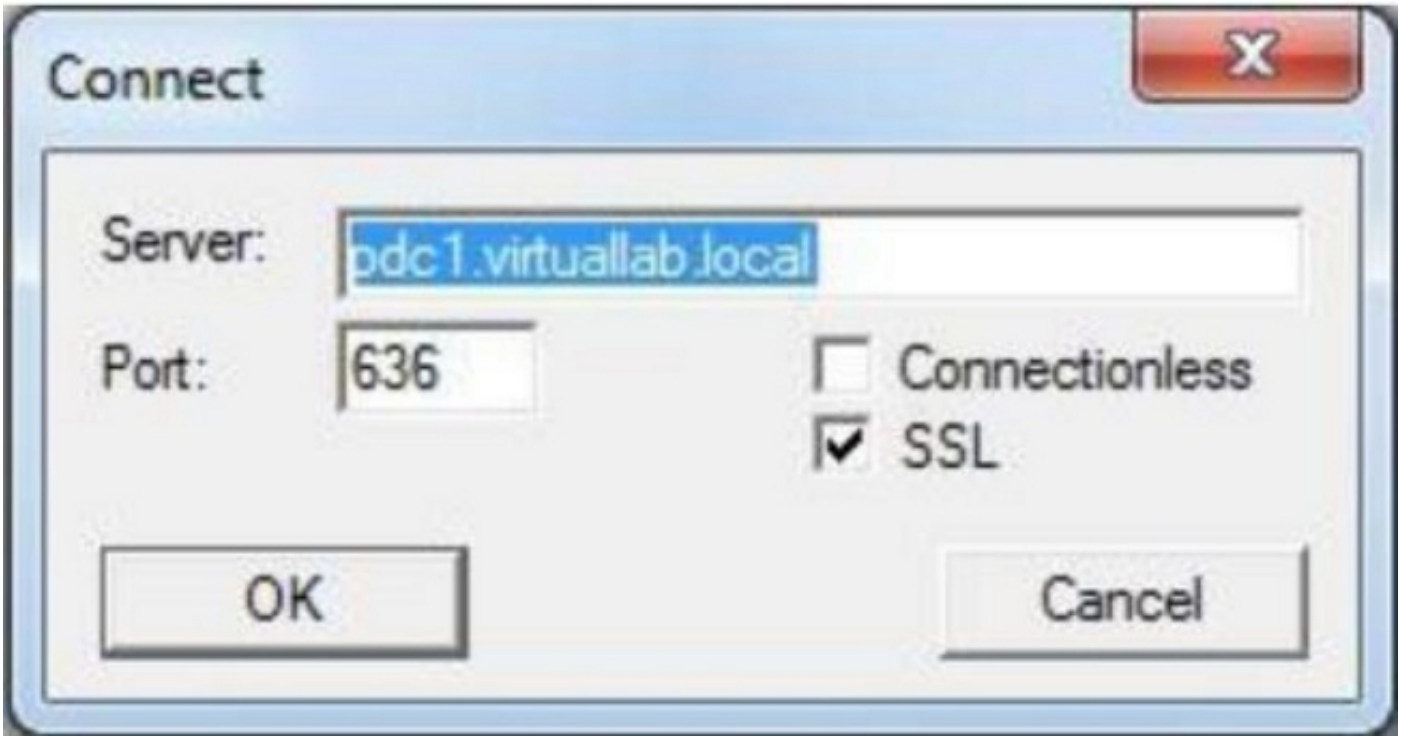
Execute este teste em um computador das janelas local que não seja um membro de um domínio, porque confiaria a raiz ou a empresa CA se se juntou a um domínio. Se um computador local está já não em um domínio, a raiz ou o certificado de CA da empresa devem ser removidos da loja das **Autoridades de certificação de raiz confiável do** computador local antes de executar este teste.

### Etapas de verificação

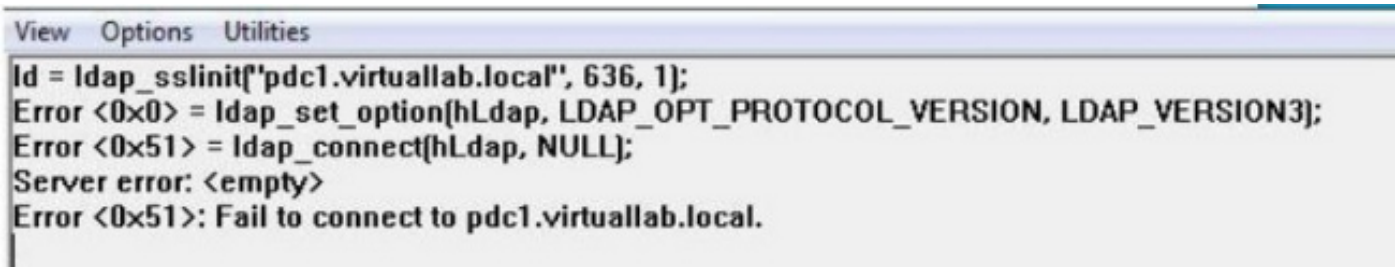
**Passo 1:** Comece o `aplicativo ldp.exe`. Vá ao Startmenu e clique a corrida**. Datilografe**

ldp.exeand **batem o** botão OK.

**Passo 2:** Conecte ao controlador de domínio usando o FQDN do controlador de domínio. A fim conectar, vá à **conexão > conectam** e incorporam o FQDN do controlador de domínio. Então selecione o **SSL**, especifique a porta **636** como mostrado abaixo e clique a **APROVAÇÃO**.




**Passo 3:** Se a raiz ou a empresa CA não são confiadas em um computador local, o resultado olha como abaixo. O Mensagem de Erro indica que o certificado recebido do servidor remoto esteve emitido por um Certificate Authority não confiável.

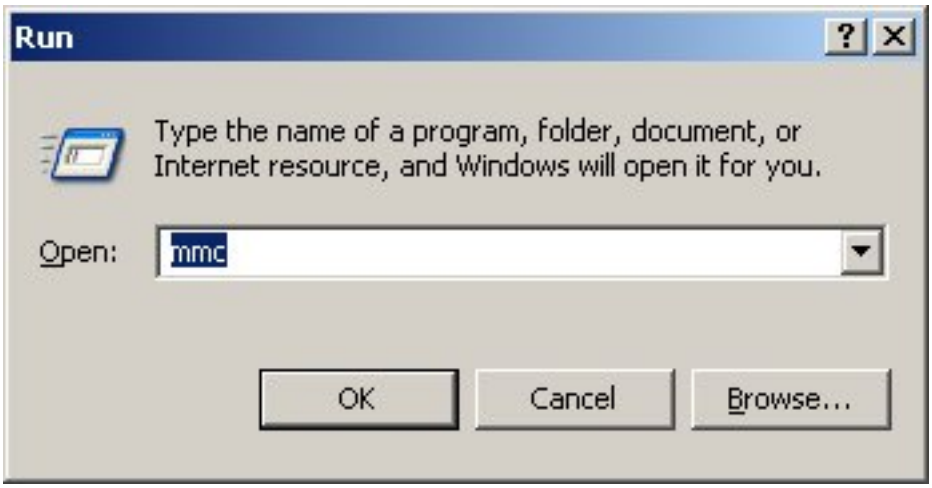



**Passo 4:** Filtrar os mensagens de evento no computador das janelas local com os seguintes critérios fornece um resultado específico:

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


**Passo 5:** Importe o certificado de CA à loja do certificado do computador das janelas local.

i. Execute o Microsoft Management Console (MMC). Vá ao **menu de início** e clique a **corrida**. Datilografe o `mmc` e bata o **botão OK**.

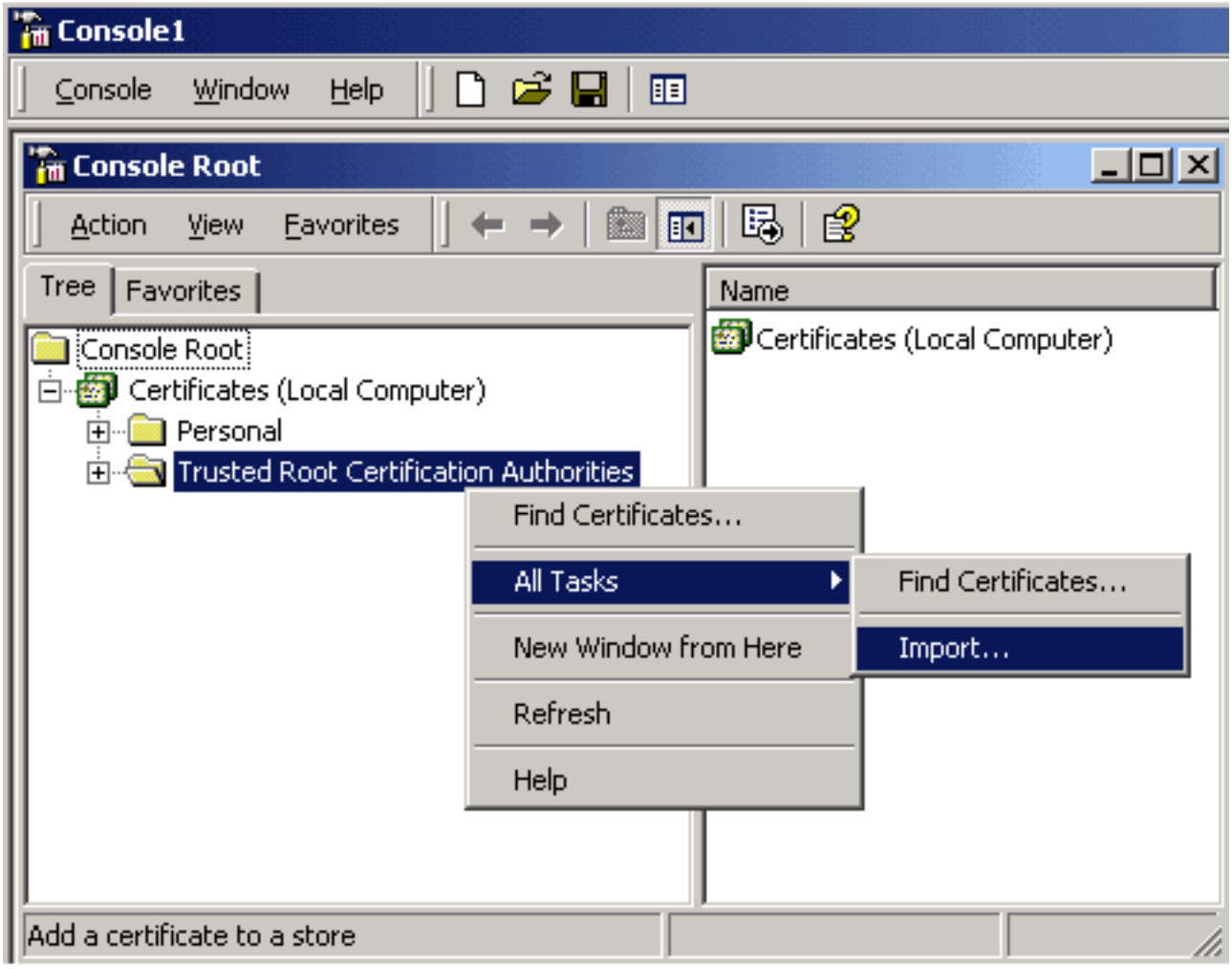



ii. Adicionar o certificado do computador local pressão-em. Navegue às seguintes opções no **menu de arquivo**:

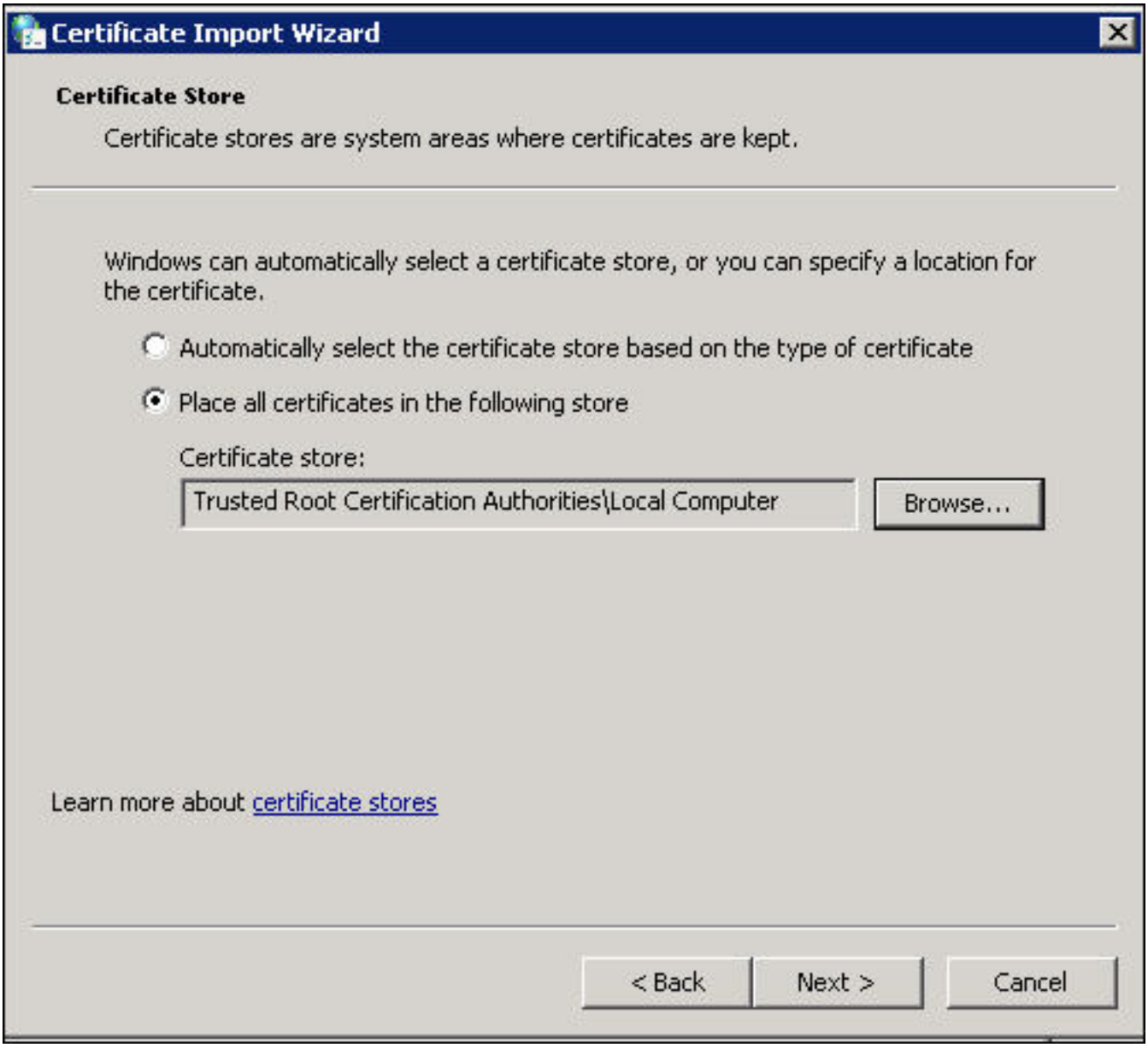
**Adicionar/telecontrole Pressão-em** > > Add dos **Certificados > escolhem do "a conta computador" > computador local: (o computador que este console está executando sobre) > revestimento > APROVADO**.

iii. Importe o certificado de CA.

**O fundamento de console > os Certificados** (computador local) > **Autoridades de certificação de raiz confiável > Certificados** > clicam com o botão direito > **todas as tarefas > importação**.




- Clique **em seguida** e consulte a Base64 codificou o arquivo de certificado de CA do certificado X.509 (`*.cer`, `*.crt`). Selecione então o arquivo.
- Clique **aberto > em seguida** e o **lugar** seleto **todos os Certificados na seguinte loja: Autoridades de certificação de raiz confiável**.
- Clique **em seguida > revestimento** para importar o arquivo.




iv. Confirme que CA está alistado com o outro root confiável CA.

**Passo 6:** Siga etapa 1 e 2 para conectar ao servidor ldap AD sobre o SSL. Se o certificado de CA está correto, as primeiras linhas 10 no painel correto de `ldp.exe devem` ser como abaixo:

```
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 teste

Se um certificado e uma conexão ldap passam este teste, você pode com sucesso configurar o

objeto da autenticação para o LDAP sobre o SSL/TLS. Contudo, se a falha do teste devido à configuração de servidor ldap ou à edição do certificado, resolve por favor a edição no server AD ou transfere o certificado de CA correto antes que você configurar o objeto da autenticação no centro de gerenciamento de FireSIGHT.

## Documentos relacionados

- Identifique atributos de objeto do diretório ativo LDAP para a configuração do objeto da autenticação
- Configuração do objeto da autenticação LDAP no sistema de FireSIGHT