Проверьте LDAP по SSL/TLS (LDAP) и Сертификат CA Использование Ldp.exe

Содержание

Введение

При создании Опознавательного Объекта на Центре управления FireSIGHT для LDAP Active Directory По SSL/TLS (LDAP) может иногда быть необходимо протестировать свидетельство CA и соединение SSL/TLS, и проверить не, не проходит ли Опознавательный Объект тест. Этот документ объясняет, как выполнить тестовое использование Microsoft Ldp.exe.

Как проверить

Перед началом работы

Вход в систему к локальному компьютеру Microsoft Windows с учетной записью пользователя, которая имеет локальную Администраторскую привилегию для выполнения шагов в этот документ.

> **Примечание:** Если вы в настоящее время не имеете `ldp.exe в наличии` в своей системе, необходимо сначала загрузить **Windows Support Tools**. Это доступно на Веб-узле Microsoft. Как только вы загружаете и устанавливаете **Windows Support Tools**, придерживаетесь ниже шагов.

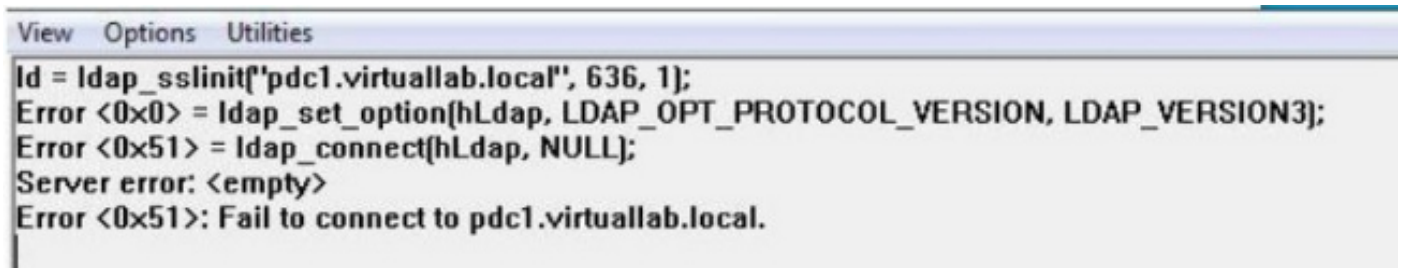
Выполните этот тест на компьютере локальных окон, который не был участником домена, поскольку он доверял бы Root или Предприятию CA, если бы он присоединился к домену. Если локальный компьютер больше не находится в домене, сертификат CA Root или Предприятия должен быть удален из хранилища **Доверенных корневых центров сертификации** локального компьютера прежде, чем выполнить этот тест.

Этапы проверки

Шаг 1: Запустите `ldp.exe` приложение. Перейдите **к Меню Пуск** и нажмите **Run**. Введите **`ldp.exe`** и поразите **кнопку OK**.

Шаг 2: Соединитесь с Контроллером домена с помощью контроллера домена FQDN. Для соединения перейдите **к Соединению> Подключение** и введите Контроллер домена FQDN. Затем выберите **SSL**, задайте **`порт 636`** как показано ниже и нажмите **OK**.

Шаг 3: Если Root или Предприятию CA не доверяют на локальном компьютере, взгляды результата как ниже. Сообщение об ошибках указывает, что сертификат, полученный от удаленного сервера, был выполнен недоверяемым центром сертификации.

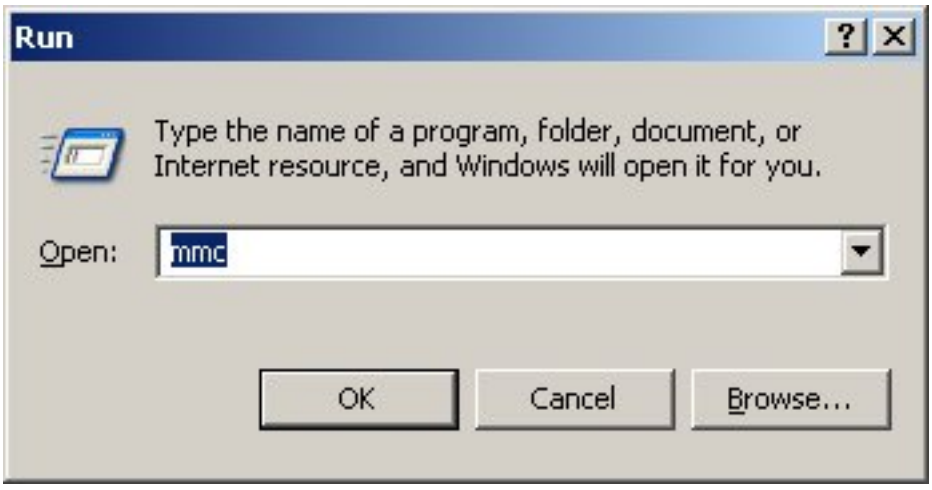


Шаг 4. : Фильтрация сообщения о событии на компьютере локальных окон со следующими критериями предоставляет определенный результат:

- Источник события = `Schannel`
- Идентификатор события = `36882`

Шаг 5. : Импортируйте Сертификат CA к компьютерному хранилищу сертификата локальных окон.

i. Выполните Консоль управления Microsoft (MMC). Перейдите **к Меню Пуск** и нажмите **Run**. Введите **mmc** и поразите **кнопку OK**.

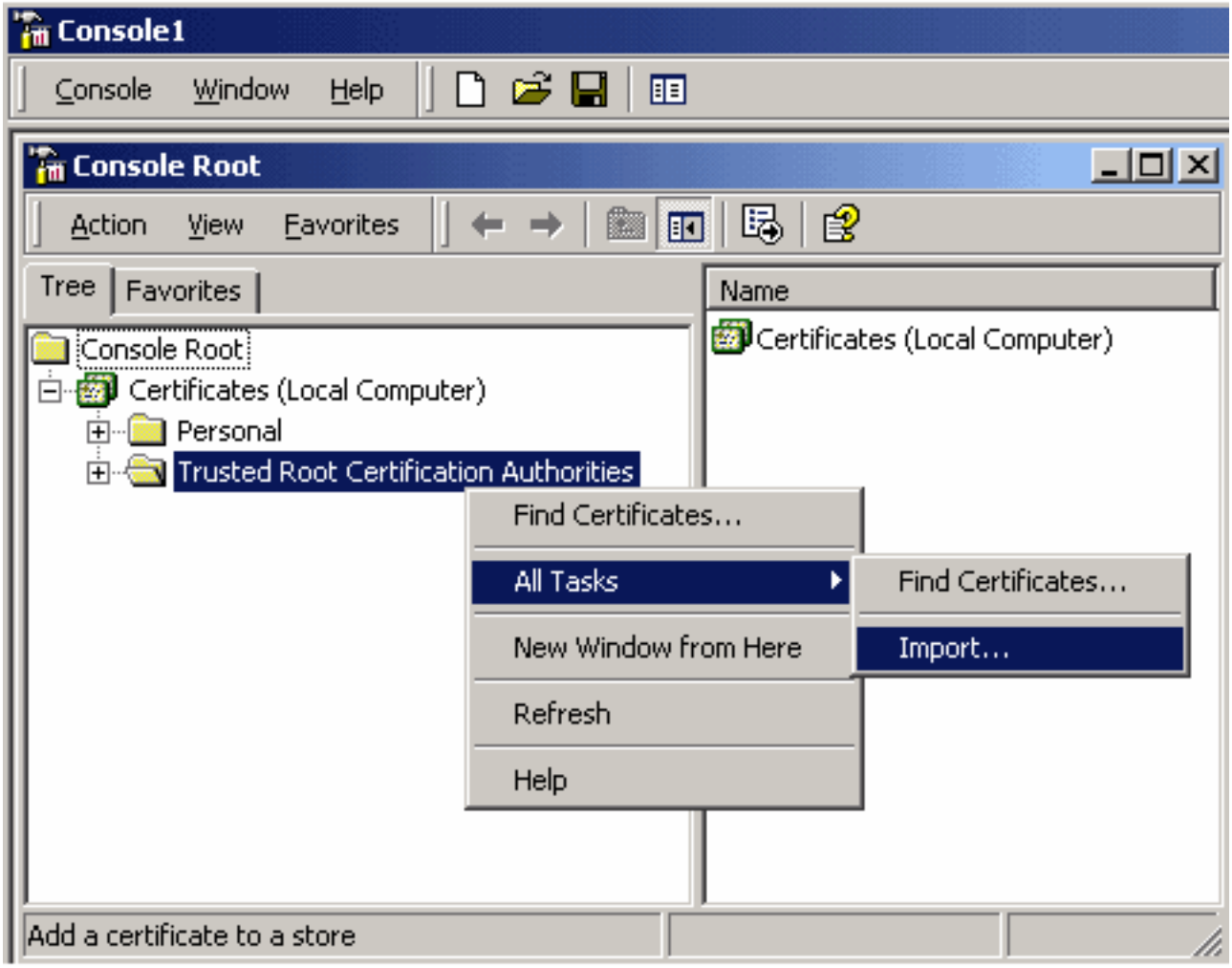


ii. Добавьте моментальный снимок сертификата локального компьютера - в. Перейдите к следующим опциям на **Меню Файл**:

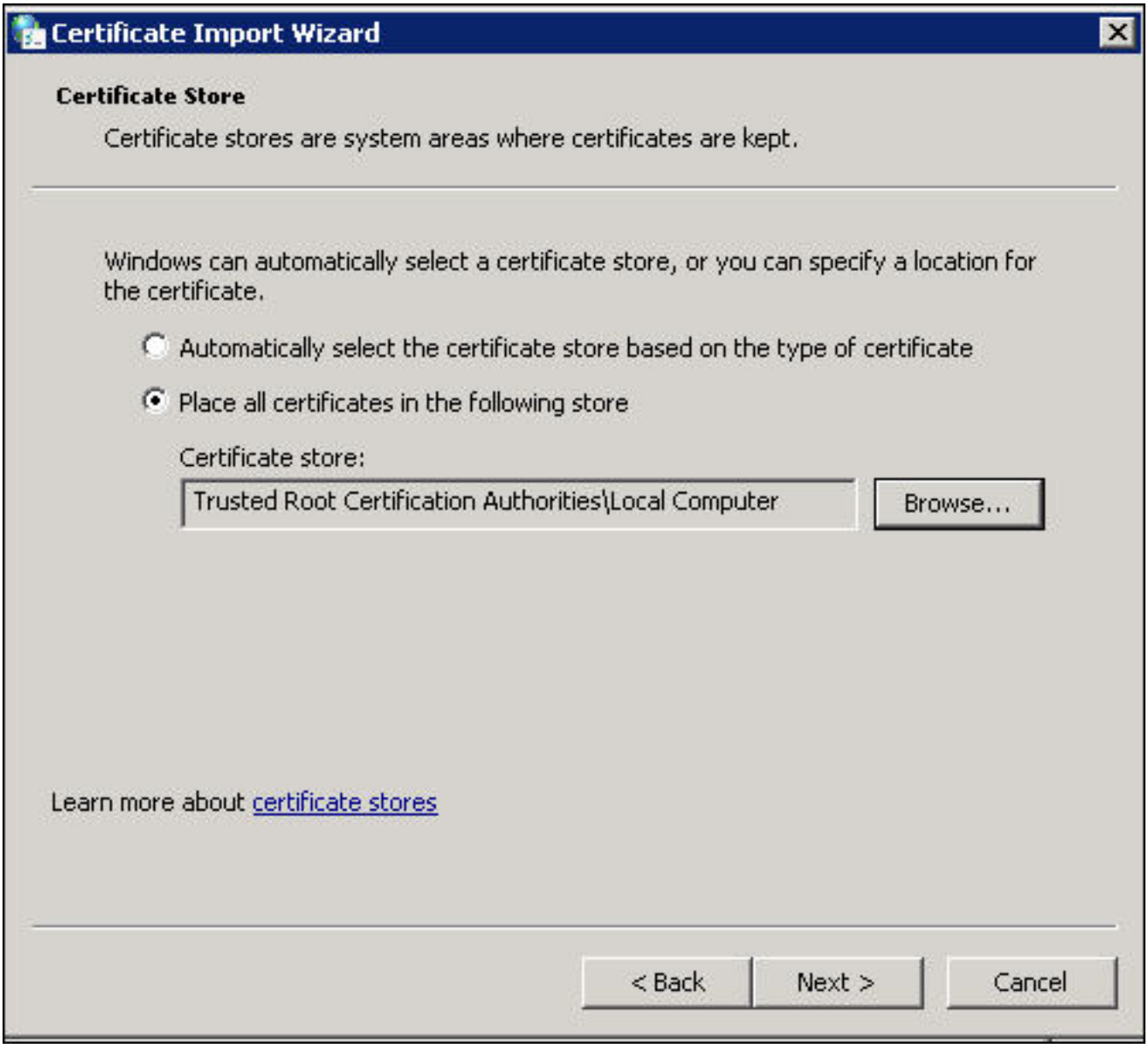
Добавьте/Удалены Моментальный снимок - в>, Сертификаты> Добавляют>, Выбирают "Computer Account"> Local Computer: (компьютер эта консоль работает),> Конец> OK.

iii. Импортируйте сертификат CA.

Корневые (сертификат) консоли> Сертификаты (Локальный компьютер)**> Доверенные корневые центры сертификации> Сертификаты>** Щелчок правой кнопкой**> Все Задачи> Импорт**.



- Нажмите **Next** и Browse to Base64 Encoded X.509 Certificate (`*.cer`, `*.crt`) файл сертификата CA. Затем выберите файл.
- Нажмите **Open> Next** и выберите **Place все сертификаты в следующем хранилище: Доверенные корневые центры сертификации**.
- Нажмите **Next> Finish** для импорта файла.



iv. Подтвердите, что CA перечислен с другим Trusted Root CAs.

Шаг 6: Придерживайтесь Шага 1 и 2 для соединения с AD Сервером LDAP по SSL. Если сертификат CA корректен, первые 10 линий на правой панели `ldp.exe` должны быть как указано ниже:

```
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:
```

Результат тестирования

Если сертификат и Соединение LDAP проходят этот тест, можно успешно настроить Опознавательный Объект для LDAP по SSL/TLS. Однако, если тестовый сбой из-за конфигурации Сервера LDAP или проблемы сертификата, решите вопрос о AD сервере или загрузите корректный сертификат ЦС перед настройкой Опознавательного Объекта на Центре управления FireSIGHT.

Дополнительная документация

- Определите атрибуты объектов LDAP Active Directory для опознавательной конфигурации объекта
- Конфигурация объекта проверки подлинности LDAP в системе FireSIGHT