Содержание

Введение

Можно настроить Центр управления FireSIGHT, чтобы позволить внешним пользователям LDAP Active Directory аутентифицировать доступ к интерфейсу веба - пользователя и CLI. Эта статья обсуждает, как настроить, протестировать, устраните неполадки Опознавательного Объекта для Microsoft AD Authentication Over SSL/TLS.

Предпосылка

Cisco рекомендует ознакомиться на управлении пользователями и системе внешней проверки подлинности на Центре управления FireSIGHT.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Процедура

Шаг 1. Настройте Опознавательный Объект без шифрования SSL/TLS.

1. Настройте Опознавательный Объект, как вы обычно были бы. Базовые шаги конфигурации для зашифрованного и незашифрованной проверки подлинности являются тем же.
2. Подтвердите, что Опознавательный Объект работает, и AD пользователи LDAP могут аутентифицироваться дешифрованный.

Шаг 2. Протестируйте опознавательный объект по SSL и TLS без сертификата CA.

Протестируйте опознавательный объект по SSL и TLS без свидетельства CA. При обнаружении с проблемой консультируйтесь с System Admin для решения этого вопроса о AD Сервере LDS. Если сертификат был ранее загружен к опознавательному объекту, выберите **"Certificate has been loaded (Select to clear loaded certificate)"** для очистки свидетельства и тестового AO снова.

Если Опознавательный Объект отказывает, консультируйтесь со своим System Admin для проверки AD конфигурации SSL/TLS LDS, прежде чем вы перейдете к следующему шагу. Однако не стесняйтесь продолжать к следующим шагам тестировать Опознавательный

Объект далее с Сертификатом CA.

Шаг 3. **Base64** загрузки CA свидетельство.

1. Вход в систему к AD LDS.
2. Откройте Web-браузер и соединитесь с `http://localhost/certsrv`
3. Щелкните **по "Download a CA certificate, certificate chain, or CRL"**
4. Выберите свидетельство CA из списка **"Сертификата CA"** и **"Base64"** от **"Способа кодирования"**
5. Щелкните по ссылке **"Download CA certificate"** для загрузки `certnew.cer` файла.

Шаг 4. Проверьте **Подчиненное** значение в свидетельстве.

1. Щелкните правой кнопкой по `certnew.cer` и выберите **открытый**.
2. Щелкните по вкладке **Details** и выберите **<All>** от **Показа** выпадающие опции
3. Проверьте значение для каждого поля. В частности проверьте, что **Подчиненное** значение совпадает **с Именем хоста Основного сервера** Опознавательного Объекта.

Шаг 5. Протестируйте Свидетельство на машине Microsoft Windows. Можно выполнить этот тест на Рабочей группе, или Домен присоединился к машине Windows.

> **Совет:** Этот шаг может использоваться для тестирования Сертификата CA на Системе Windows прежде, чем создать Опознавательный Объект на Центре управления FireSIGHT.

1. Скопируйте свидетельство CA к `C:\Certficate` или любой предпочтительный каталог.
2. Выполните командную строку Windows, `cmd.exe.` как администратор
3. Протестируйте сертификат CA с командой Certutil

```
cd c:\Certificate

certutil -v -urlfetch -verify certnew.cer >cacert.test.txt
```

Если к машине Windows уже присоединяются домен, сертификат CA должен быть в хранилище сертификата и в `cacert.test.txt` не должно быть никакой ошибки. Однако, если машина Windows находится на рабочей группе, можно видеть одно из двух сообщений в зависимости от существования свидетельства CA в доверяемом списке CA.

o. CA доверяют, но никакой CRL не найден для CA:

```
ERROR: Verifying leaf certificate revocation status returned The revocation function
was unable to check revocation because the revocation server was offline. 0x80092013
(-2146885613)

CertUtil: The revocation function was unable to check revocation because the
revocation server was offline.
```

b. CA не доверяют:

```
Verifies against UNTRUSTED root
Cert is a CA certificate
Cannot check leaf certificate revocation status
CertUtil: -verify command completed successfully.
```

Если вы получаете какие-либо другие Сообщения об ошибках как ниже, консультируйтесь со своим System Admin для решения вопроса о AD LDS и Промежуточном CA., Эти

сообщения об ошибках являются показательным из неправильного Свидетельства, предмета в свидетельстве CA, недостающей цепочке сертификатов, и т.д.

```
Verifies against UNTRUSTED root
Cert is a CA certificate
Cannot check leaf certificate revocation status
CertUtil: -verify command completed successfully.
```

Шаг 6. Как только вы подтверждаете, что свидетельство CA допустимо и прошло тест в Шаге 5, загружает свидетельство к Опознавательному Объекту и запускает тест.

Шаг 7. Сохраните Опознавательный Объект и повторно примените системную политику.