Интеграция Directum RX со службой каталога ALD Pro

06/04/2025

Содержание

1 Рекомендации по настройке 3
2 Настройка сквозной аутентификации Directum RX на Astra Linux на контроллере домена ALD Pro по протоколу Kerberos 4
2.1 Ввод Astra Linux в домен ALD PRO 4
2.2 Настройка Kerberos 4
2.2.1 Создание служебного пользователя 4
2.2.2 Настройки на контроллере домена 4
2.2.3 Синхронизация времени 5
2.2.4 Настройка сервера Directum RX 5
2.2.5 Настройка браузеров 6
2.2.5.1 Настройка web-браузера Mozilla Firefox 6
2.2.5.2 Настройка прочих браузеров 6

Directum RX является расширяемой системой электронного документооборота, которая является очень гибкой и позволяет реализовать любую логику бизнес-процессов.

Интеграция позволяет выполнять аутентификацию в сервисе Directum RX от имени доменного пользователя. Для настройки аутентификации необходимо создать пользователя в Directum RX и связать его с доменным (информация о котором будет получена из TGS-билета Kerberos). Таким образом, сейчас возможно настроить работу в Directum RX для доменных пользователей с использованием доменной SSO Kerberos без необходимости ввода пароля, но настраивать каждого пользователя придется вручную.

Инструкция по интеграции разработана компанией Directum. Вендор также оказывает поддержку по проведению пилотного тестирования и внедрению своего программного продукта.

1 Рекомендации по настройке

2 Настройка сквозной аутентификации Directum RX на Astra Linux на контроллере домена ALD Pro по протоколу Kerberos

2.1 Ввод Astra Linux в домен ALD PRO

Для ввода сервера в домен требуется установить пакеты, необходимые для работы в качестве клиента домена ALD Pro:

```
sudo DEBIAN_FRONTEND=noninteractive apt-get install -q -y aldpro-client
```

Ввод в домен производится следующей командой:

```
sudo /opt/rbta/aldpro/client/bin/aldpro-client-installer -c example.com -u admin -p
password -d hostname -i -f
```

, где:

- **example.com** - имя домена,
- **hostname –** имя сервера Directum RX,
- **admin –** логин учётной записи администратора домена,
- **password** – пароль учётной записи администратора домена.

Далее выполните перезагрузку сервера:

```
sudo reboot
```

2.2 Настройка Kerberos

2.2.1 Создание служебного пользователя

На сервере с ALD Pro создайте служебного пользователя, от имени которого будет работать система:

1. На контроллере домена откройте страницу управления «ALD Pro – пользователи и компьютеры».
2. Создайте нового пользователя. В качестве примера используется admin.

2.2.2 Настройки на контроллере домена

1. Создайте новую веб-службу следующей командой:

```
sudo ipa service-add HTTP/<доменное имя по которому доступен DirectumRX>
```

2. Далее сгенерируйте keytab-файл:

```
ipa-getkeytab -p HTTP/<доменное имя по которому доступен Directum RX>@<EXAMPLE.COM>
-k /home/admin/krb5.keytab -e aes256-cts-hmac-sha1-96,aes128-cts-hmac-sha1-96,des3-
cbc-sha1,arcfour-hmac-md5,des-cbc-crc,des-cbc-md5
```

Примечание

Также службу можно создать через панель управления ALD Pro на контроллере домена, в таком случае keytab-файл сгенерируется автоматически.

2.2.3 Синхронизация времени

Протокол Kerberos требует соответствия показания часов всех клиентов и серверов, и при рассинхронизации времени на серверах аутентификация становится невозможной. Простой и стандартный путь обеспечения синхронизации - использование сервиса Network Time Protocol(NTP).

2.2.4 Настройка сервера Directum RX

1. Подключитесь под доменным пользователем admin:

```
kinit admin
```

2. На клиентской машине нужно получить сгенерированный вами keytab-файл:

```
ipa-getkeytab -p HTTP/<доменное имя по которому доступен Directum RX>@<EXAMPLE.COM>
-k /etc/krb5.keytab
```

3. Проверьте содержимое keytab-файла следующей командой:

```
klist -k /etc/krb5.keytab
```

Внесите изменения в конфигурационный файл config.yml.

1. В секции
common_config добавьте параметр **EXTERNAL_AUTHENTICATION_TYPE** со значением '**Kerberos**':

```
common_config:
.....
      EXTERNAL_AUTHENTICATION_TYPE: 'Kerberos'
```

2. В раздел **extra_hosts** укажите FQDN и IP-адрес контроллера домена и текущего сервера:

```
extra_hosts:
       '{{ host_fqdn }}': '192.168.xxx.yyy'
       directum.example.com: '192.168.0.1'
```

3. Добавьте в секцию **variables** параметр **volume_dir** с значениями путей **'/etc/krb5.conf.d/:/etc/krb5.conf.d/'** и **'/var/lib/sss/pubconf/krb5.include.d/:/var/lib/sss/pubconf/krb5.include.d/'**:

```
   volume_dir:
    -  '/etc/krb5.conf.d/:/etc/krb5.conf.d/'
    -  '/var/lib/sss/pubconf/krb5.include.d/:/var/lib/sss/pubconf/krb5.include.d/'
```

4. Пересоберите контейнеры:

```
./do.sh all up
```

5. Добавьте доменных пользователей в систему Directum RX в формате **username@example.com**.

2.2.5 Настройка браузеров

> **Примечание**
>
> Для работы с web-сервером, настроенным в соответствии с настоящей инструкцией, web-браузер пользователя должен поддерживать аутентификацию negotiate.
>
> Если клиентская машина введена в домен ALD Pro, браузер Firefox будет настроен автоматически, настройка из пункта 1 не требуется.

2.2.5.1 *Настройка web-браузера Mozilla Firefox*

1. В веб-браузере Firefox открыть настройки конфигурации по адресу **about:config**.
2. Установитьпараметрыnetwork.negotiate-auth.delegation-uris и network.negotiate-auth.trusted-uris в значение «.<example.com>».

2.2.5.2 *Настройка прочих браузеров*

Для настройки других веб-браузеров можно воспользоваться данной ссылкой:

Настройка браузеров для использования Kerberos-аутентификации.