Настройка подключения к LDAP Active Directory

Расширение ovirt-engine-extension-aaa-ldap поддерживает множество различных типов серверов LDAP и позволяет пользователям легко определять настройки внешнего каталога.

Подготовка к установке:

- необходимо знать доменное имя сервера DNS или LDAP;
- для безопасного соединения между сервером LDAP и менеджером управления РЕД ВИРТ необходимо убедиться, что подготовлен сертификат ЦС с PEMкодировкой;
- необходимо иметь хотя бы один набор имени учетной записи и пароля, готовых для выполнения запросов поиска и входа на сервер LDAP.

Процедура установки производится в терминале менеджера управления – ВМ **HostedEngine**:

1. Выполните установку LDAP:

   ```
   dnf install ovirt-engine-extension-aaa-ldap-setup
   ```

2. Пропишите IP-адрес домена в /etc/resolv.conf.
3. Запустите ovirt-engine-extension-aaa-ldap-setup, чтобы начать интерактивную настройку:

   ```
   ovirt-engine-extension-aaa-ldap-setup
   ```

4. Выберите тип LDAP – Active Directory, введя соответствующий номер:

   ```
   Please select: 3
   ```

5. Введите имя Active Directory Forest:

   ```
   Please enter Active Directory Forest name: redvirt.redos
   ```

6. Выберите метод безопасного подключения, который поддерживает ваш сервер LDAP:

   ```
   Please select protocol to use (startTLS,ldaps,plain) [startTLS]:
   startTLS
   ```

7. Укажите метод получения сертификата CA в кодировке PEM:
   - File – позволяет указать полный путь к сертификату.
   - URL – позволяет указать URL-адрес сертификата.
   - Inline – позволяет вставить содержимое сертификата в терминал.
   - System – позволяет указать расположение по умолчанию для всех файлов

CA.

- Insecure – пропускает проверку сертификата, но соединение по-прежнему шифруется с помощью TLS.

```
Please select method to obtain PEM encoded CA certificate (File,
URL, Inline, System, Insecure): Insecure
```

8. Введите путь LDAP до пользователя AD:

```
Enter search user DN (for example uid=username, dc=example,
dc=com or leave empty for anonymous): cn=Administrator, cn=Users,
dc=redvirt, dc=redos
```

9. Введите пароль пользователя:

```
Enter search user password:*********
```

10. Выберите **Yes**, если хотите настроить единый вход для виртуальных машин. Однако следует обратить внимание, что данную функцию нельзя использовать для единого входа на портал администратора.

```
Are you going to use Single Sign-On for Virtual Machines (Yes,No)
[Yes]: Yes
```

11. Укажите имя профиля, которое будет видно пользователям на странице авторизации (в примере указано redvirt.redos):

```
Please specify profile name that will be visible to users
[redvirt.redos]: redvirt.redos
```

> **Примечание.**
>
> Пользователи должны выбрать профиль из раскрывающегося списка при первом входе в систему. Информация хранится в файлах cookie браузера и предварительно выбирается при следующем входе пользователя в систему.

12. Выполните тестовый вход в систему, чтобы убедиться, что ваш LDAP-сервер правильно подключен к вашей среде РЕД ВИРТ. Для запроса входа введите имя учетной записи и пароль:

```
Enter user name: ivan
Enter user password:
[ INFO ] Executing login sequence...
```

```
...
[ INFO ] Login sequence executed successfully
```

13. В случае успешного входа **Login sequence executed successfully** введите **Готово**, чтобы завершить настройку:

```
Select test sequence to execute (Done,Abort,Login,Search) [Done]:
Done
```

14. Выполните перезапуск службы управления РЕД ВИРТ:

```
systemctl restart ovirt-engine.service
```

Созданный профиль будет доступен на портале администрирования и на странице авторизации в портале виртуальных машин.

Источник: https://redvirt.red-soft.ru/base/red-virtualizatsiya-8-0/upravlenie-polzovatelyami-8/nastroyka-podklyucheniya-k-ldap-active-directory/