Настройка доменной авторизации в РВ 8.0 через Keycloak

Окружение

- **Версия РЕД ВИРТ:** 8.0

Подготовительные работы

Вход в Портал Keycloak с начальной страницы установки

Главное окно Keycloak

Настройка подключения к каталогу LDAP/AD

Подготовительные работы

- Должна быть завершена установка РЕД ВИРТ 8.0 в соответствии с документацией.
- Необходимо ознакомиться с разделом **7.6 Управление пользователями и группами в Keycloak** документа Руководство администратора «РЕД ВИРТ 8.0» на официальной странице Ред Софт: https://redvirt.red-soft.ru/product/docs/.

Вход в Портал Keycloak с начальной страницы установки

Для входа в Портал Keycloak с начальной страницы установки нажмите на **Портал Keycloak**:

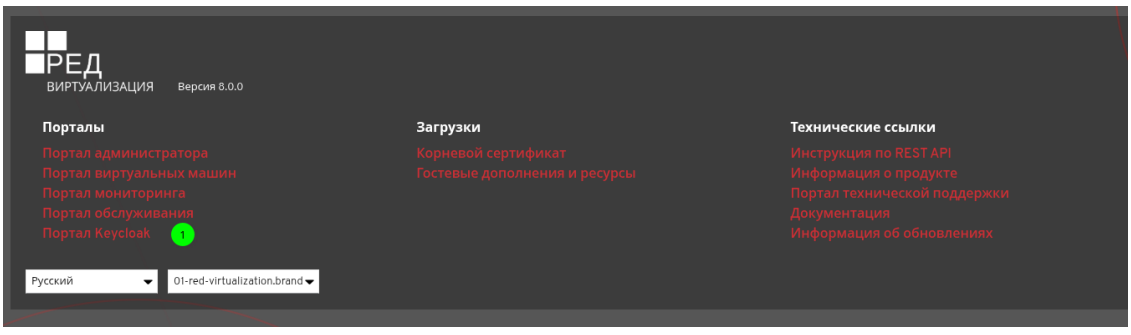


Рисунок 1 – Начальная страница. Ссылка на портал Keycloak

Для входа используются заданные при установке учетные данные в виде:

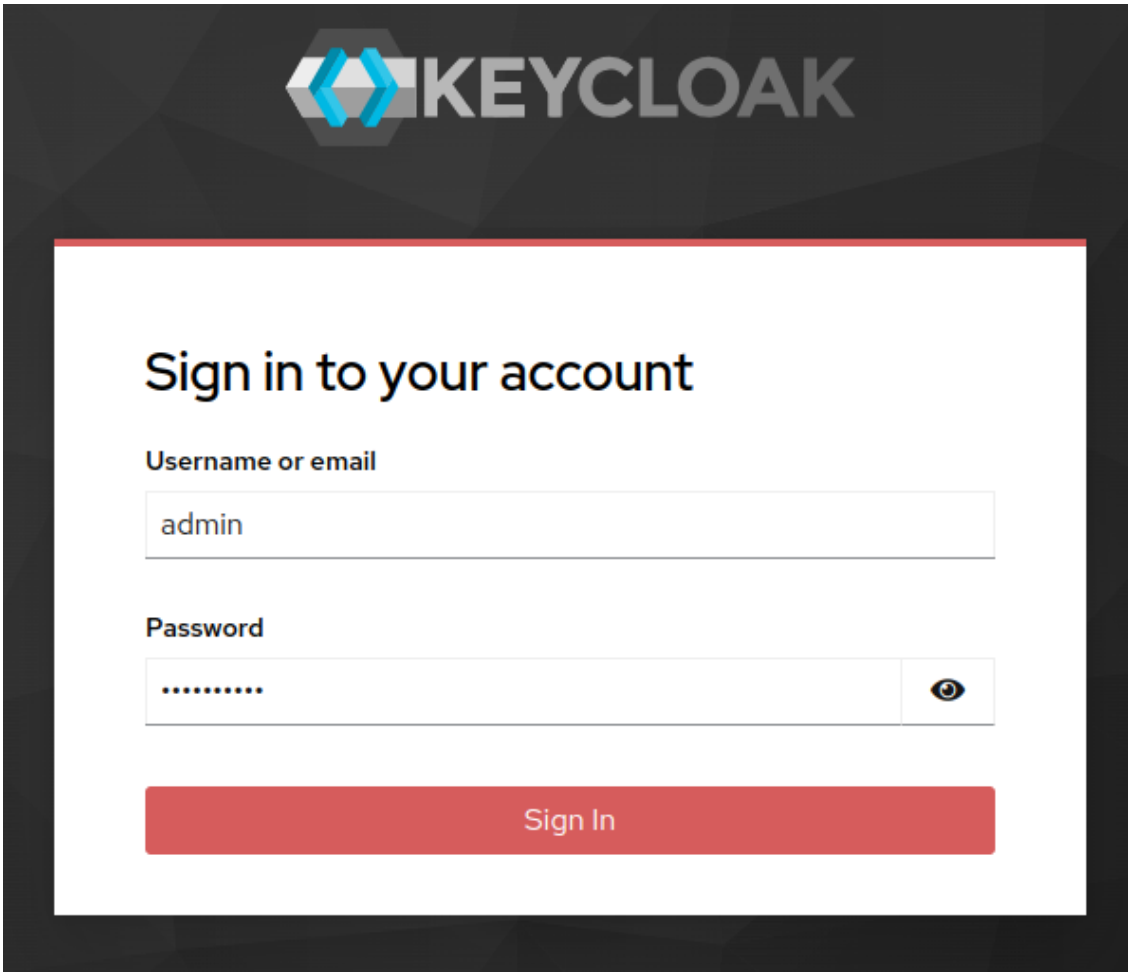


Рисунок 2 – Пример ввода учетных данных

Главное окно Keycloak

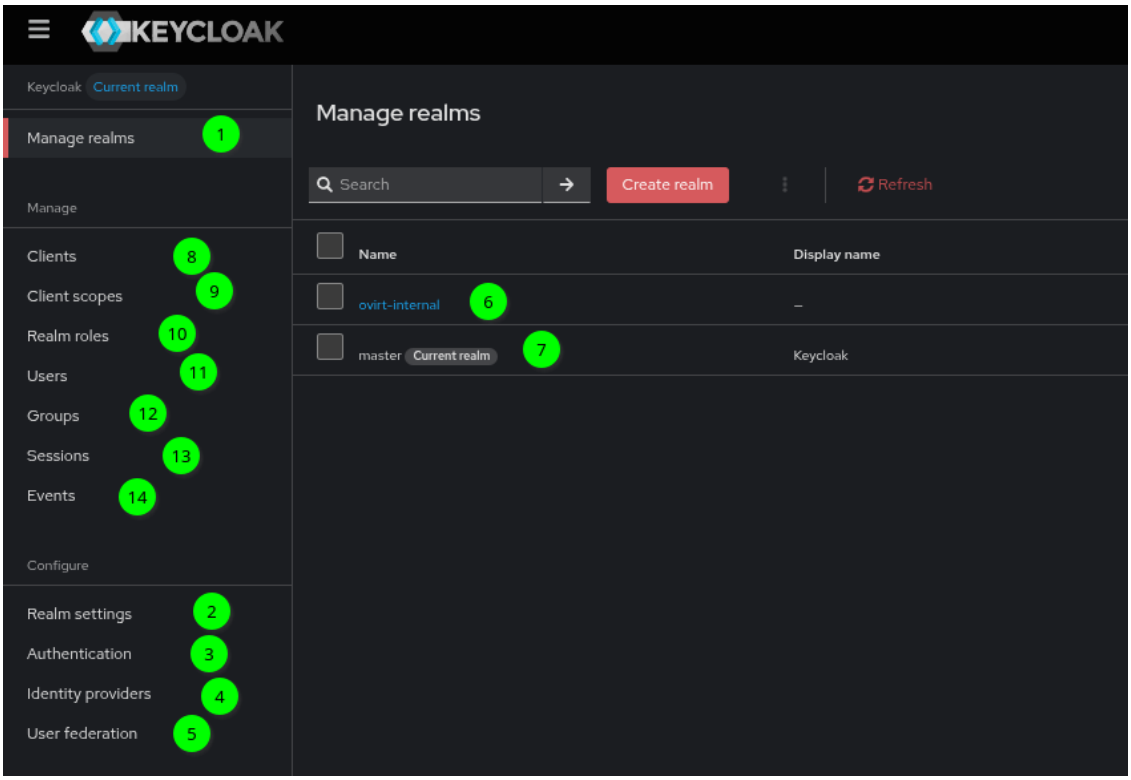


Рисунок 3 – Главное окно Keycloak. Выбран раздел **Manage realms/Управление realm**

Описание сущностей

1. **Manage realms/Управление realm** - раздел переключения между Realms (областями управления аутентификацией). Каждая область содержит свой список пользователей и способов аутентификации для приложений добавленных в эту область. В данном разделе выбирается область управления аутентификацией, с которой будет выполняться работа в других разделах. По умолчанию всего два realm:
    - ovirt-internal. Область аутентификации РЕД ВИРТ. Основной realm для настроек пользователей, ролей и групп для РЕД ВИРТ.
    - master. Область аутентификации системы Keycloak. Для настроек пользователей самой Keycloak.

    Для перехода необходимо нажать на нужный realm.

2. Пункт меню **Realm settings/Настройки realm**

    Настройки realm — это настройки, которые управляют параметрами пользователей, приложений, ролей и групп в текущем realm, такие как: внешний вид, локализация, политика аутентификации пользователей, параметры сессий.

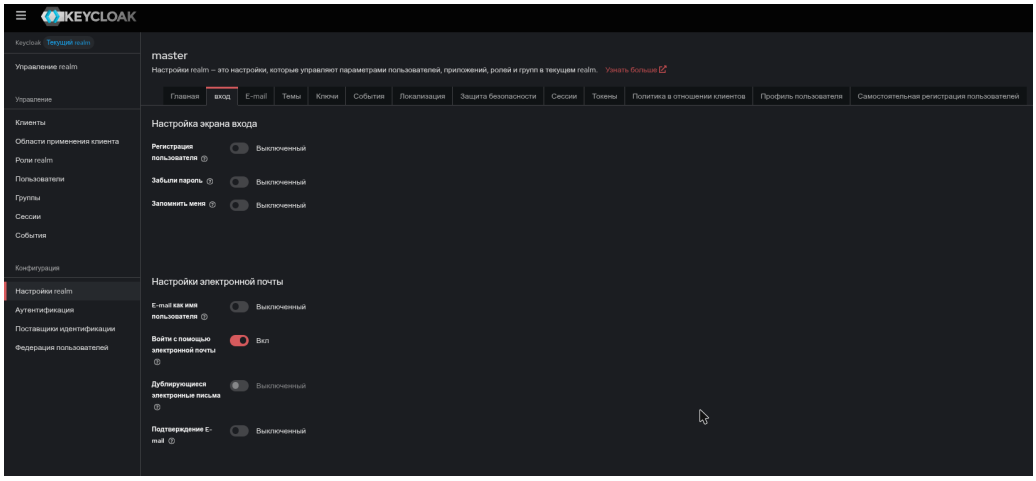


Рисунок 4 – Настройки realm

По теме данного документа настройки пункта не требуется.

3. Пункт меню **Authentication**.

   Аутентификация — это область, где вы можете настраивать и управлять сценариями аутентификации.

   По теме данного документа настройки пункта не требуется.

4. Пункт меню **Identity providers**.

   Поставщики идентификационных данных — это социальные сети или брокеры идентификации, которые позволяют пользователям проходить аутентификацию в Keycloak.

   По теме данного документа настройки пункта не требуется.

5. Пункт меню **User federation**.

   Федерация пользователей обеспечивает доступ к внешним базам данных и каталогам, таким как LDAP и Active Directory. Основной пункт для настроек по теме данного документа.

Настройка подключения к каталогу LDAP/AD

Для подключения пользователей каталога LDAP/AD необходимо выполнить следующие действия:

1. Выберите в разделе **Управление Realms** (рисунок 3) текущий realm - **ovirt-internal**.

2. Выберите в меню **Add new provider** пункт **LDAP**.

   В некоторых конфигурациях может быть выбран пункт Kerberos, но в данном документе рассматривается способ подключения через LDAP.

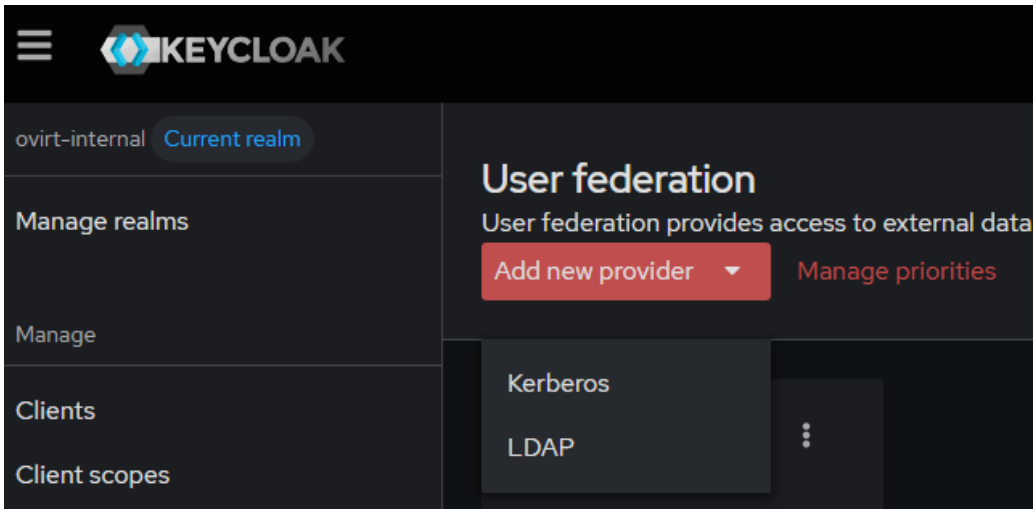


Рисунок 5 – Выбор провайдера каталога пользователей

3. Заполните поля в соответствии с настройками вашего каталога. Для примера показаны настройки типового подключения:

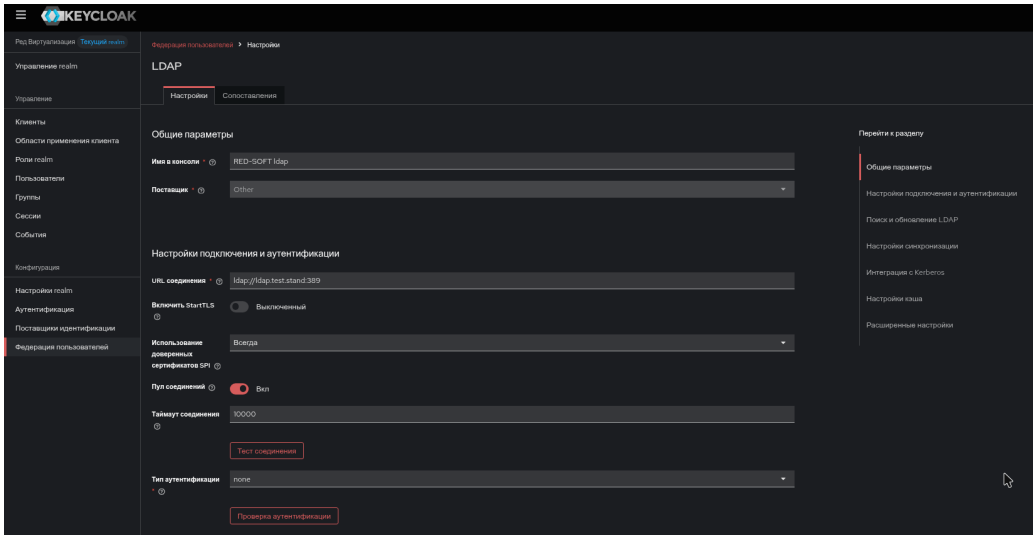


Рисунок 6 – Заполнение формы настроек подключения. Часть 1

После заполнения основных настроек проверьте подключение и аутентификацию по соответствующим кнопкам: **Тест соединения** и **Тест аутентификации**. Ответ должен быть положительным:



Рисунок 7 – Тест соединения - успешный



Рисунок 8 – Тест аутентификации - успешный

Если тесты прошли успешно - продолжайте настройку. В противном случае – необходимо проверить настройки как на стороне LDAP-сервиса, так и в данной форме подключения.

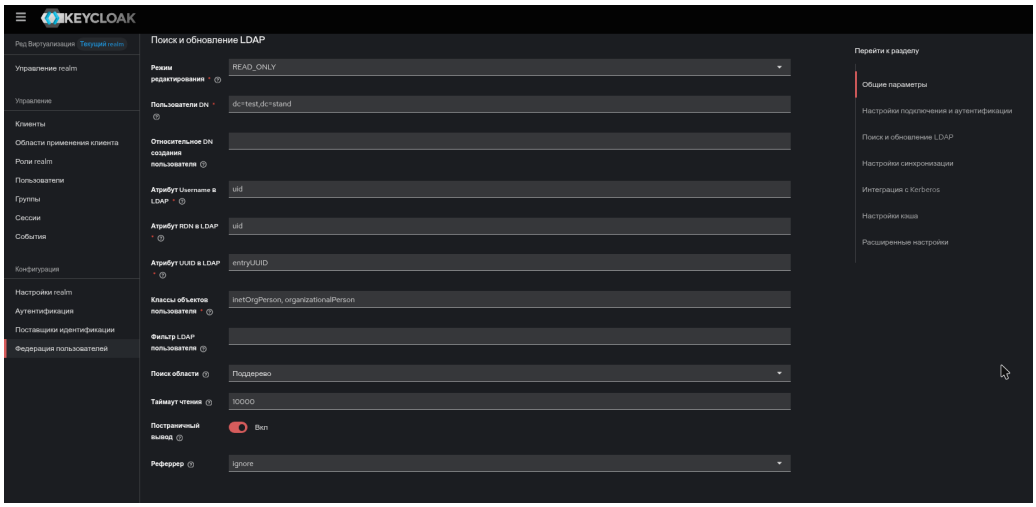


Рисунок 9 – Заполнение формы настроек подключения. Часть 2

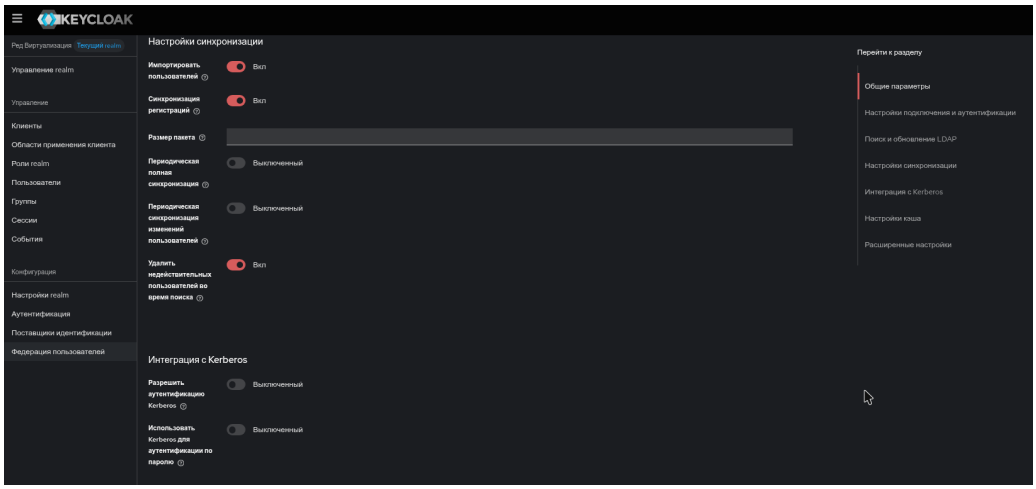


Рисунок 10 – Заполнение формы настроек подключения. Часть 3

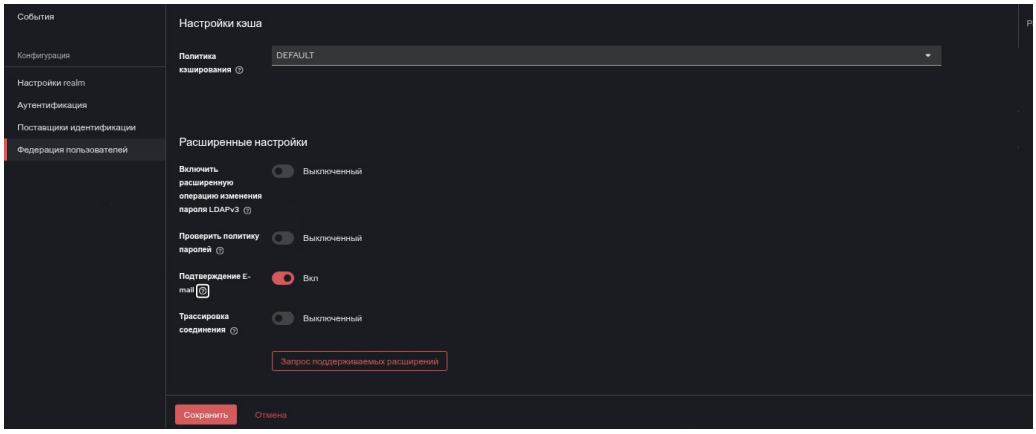


Рисунок 11 – Заполнение формы настроек подключения. Часть 4

Сохраните настройки подключения, нажав кнопку **Сохранить**.

4. Настройка прав пользователей.

Перейдите в раздел **Пользователи** для поиска пользователей и определения ролей.

После подключения внешнего каталога, локальные пользователи пропадут из списка, но будут продолжать работать и доступны при поиске.

ВАЖНО!

Сразу после подключения внешнего каталога, все пользователи получают по умолчанию роль **default-roles-ovirt-internal** и группу **ovirt-user**, что соответствует полному доступу на **Портал администратора РЕД ВИРТ**.

Чтобы найти и изменить права пользователей каталога:

- Введите первые буквы пользователя в поле поиска и нажмите клавишу **ENTER**. Будет отображен список пользователей соответствующий строке поиска (рисунок 12).
- Нажмите на имя пользователя. Откроется форма параметров пользователя.
- Перейдите на вкладку Сопоставление ролей. Убедитесь в наличии роли **default-roles-ovirt-internal** (рисунок 13). В будущем, список ролей может быть изменен.
- Перейдите на вкладку Группы. Убедитесь в наличии группы **ovirt-user** (рисунок 14). Для получения максимальных прав можете добавить группу **ovirt-administrator** (на текущий момент группа не используется). В будущем, список групп может быть изменен.

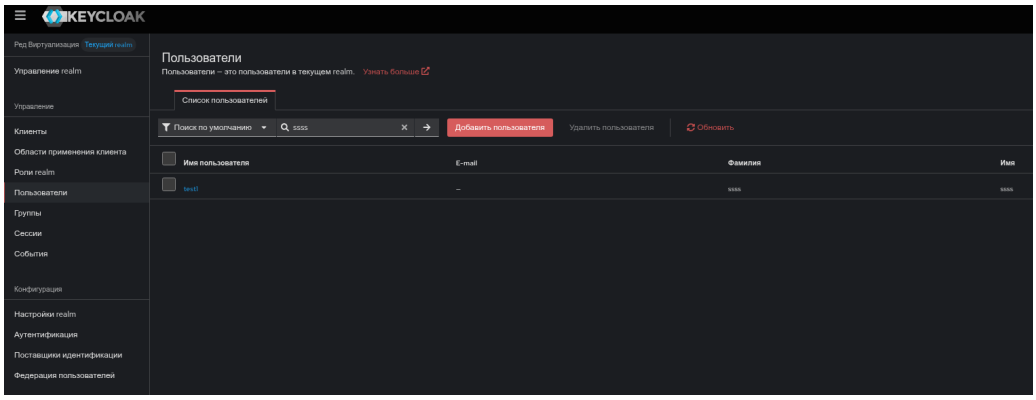


Рисунок 12 – Поиск пользователей

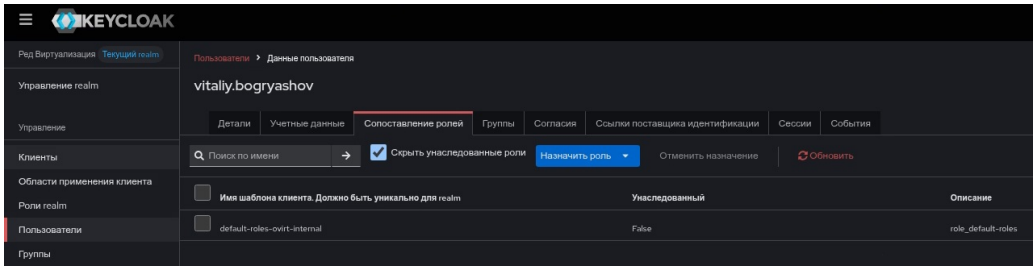


Рисунок 13 – Сопоставление ролей пользователя

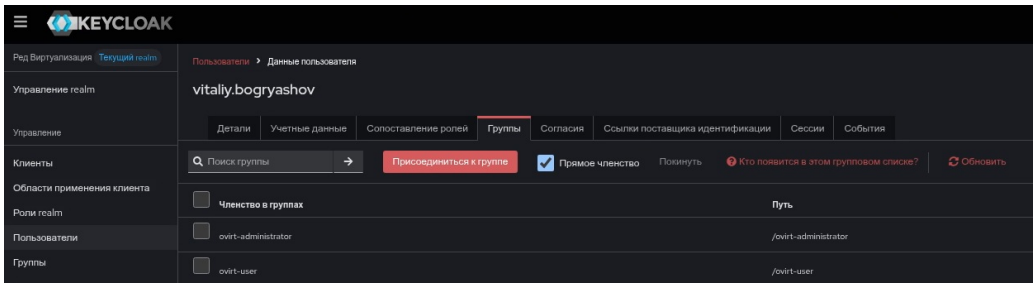


Рисунок 14 – Список групп пользователя

После подключения в Keycloak внешнего каталога **LDAP** для реалма **ovirt-internal** можно входить на портал администрирования РЕД ВИРТ под любым пользователем, входящим в группу **ovirt-user**. После первого входа автоматически добавится текущий пользователь в список пользователей портала администрирования РЕД ВИРТ (рисунок 15).

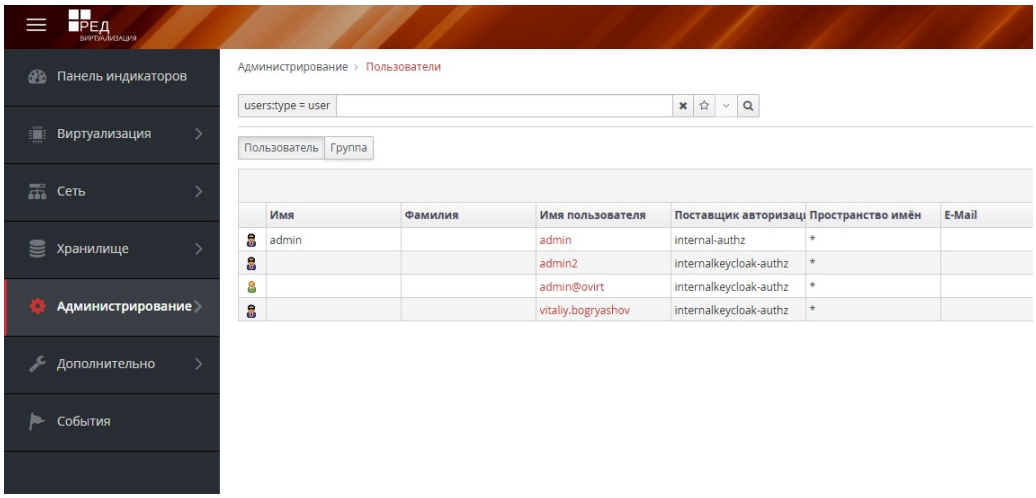


Рисунок 15 – Портал администрирования РЕД ВИРТ. Список пользователей

При необходимости, можно изменить необходимые права на вкладке **Разрешения** выбранного пользователя (рисунок 16). В дальнейшем, все изменения прав пользователей осуществляются стандартными действиями в соответствии с основным документом **Руководство администратора «РЕД ВИРТ 8.0»** доступным на официальном сайте Ред Софт.

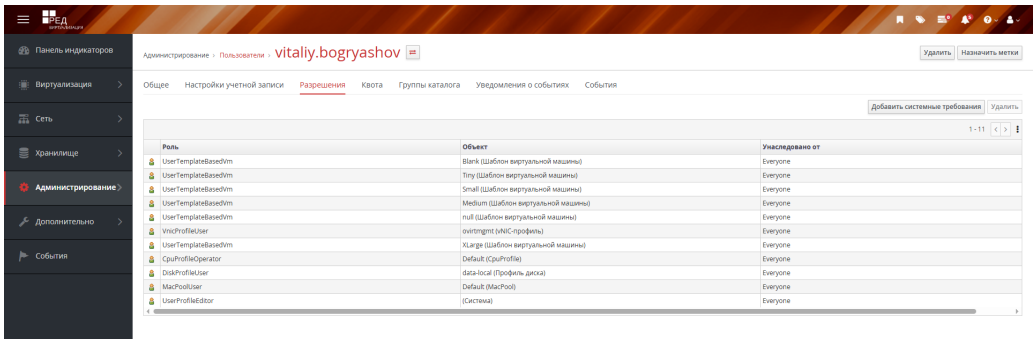


Рисунок 16 – Портал администрирования РЕД ВИРТ. Список ролей

Источник: https://redvirt.red-soft.ru/base/poleznye-stati/red-virt-8-0/nastroyka-domennoy-avtorizatsii-v-rv-8-0-cherez-keycloak/