Миграция с AAA JDBC на Keycloak

Аннотация

В этом документе описаны операции, необходимые для переключения с провайдера AAA JDBC на Keycloak.

Инструкции, описанные ниже актуальны только для zVirt 4.2 и выше.

1. Общие сведения

Если при развертывании Менеджера управления было указано использование AAA JDBC в качестве провайдера аутентификации, то для миграции на Keycloak потребуются следующие действия:

1. Активация Keycloak.
2. Ручной перенос существующих в AAA JDBC пользователей в базу Keycloak.

На текущий момент не существует никаких методов автоматизации миграции с AAA JDBC на Keycloak.

2. Активация Keycloak

Перед выполнением процедуры активации убедитесь, что системное имя Менеджера управления (хоста с Менеджером управления в режимах Standalone и Standalone All-in-One) задано в нижнем регистре. Для этого можно использовать команду `hostname`.

Если имя задано в верхнем регистре, перед выполнением активации воспользуйтесь инструкцией для смены регистра системного имени.

Описанные ниже операции выполняются на Менеджере управления под учетной записью root.

Порядок действий:

1. Создайте полную резервную копию компонентов Менеджера управления в соответствии с инструкцией и сохраните её на удаленном хранилище.
2. Запустите процесс реконфигурации Менеджера управления с активацией Keycloak:

```
engine-setup --otopi-environment="OVESETUP_CONFIG/keycloakEnable=bool:True"
```

3. В процессе ответьте на ряд вопросов:
   - Согласитесь с настройкой firewalld:

     ```
     Do you want Setup to configure the firewall? (Yes, No) [Yes]:
     ```

   - Укажите способ размещения базы данных keycloak:

     ```
     Where is the Keycloak database located? (Local, Remote) [Local]:
     ```

   - В случае локального размещения новой базы Keycloak, согласитесь с автоматической настройкой:

     ```
     Would you like Setup to automatically configure postgresql and create
     Keycloak database, or prefer to perform
              that manually? (Automatic, Manual) [Automatic]:
     ```

   - Откажитесь от создания резервной копии БД (она была сделана вручную на первом шаге):

     ```
     Would you like to backup the existing database before upgrading it?
     (Yes, No) [Yes]:No
     ```

   - Подтвердите отказ от создания резервной копии БД:

     ```
     Are you sure you do not want to backup the DWH database?(Yes, No)
     [No]:Yes
     ```

   - Откажитесь от процедуры full vacuum для БД DWH:

     ```
     Perform full vacuum on the oVirt engine history
     database ovirt_engine_history@localhost?
     This operation may take a while depending on this setup health and the
     configuration of the db vacuum process.
     See https://www.postgresql.org/docs/16/sql-vacuum.html
     (Yes, No) [No]:
     ```

   - Откажитесь от процедуры full vacuum для БД engine:

     ```
     Perform full vacuum on the engine database engine@localhost?
     This operation may take a while depending on this setup health and the
     configuration of the db vacuum process.
     See https://www.postgresql.org/docs/16/sql-vacuum.html
     (Yes, No) [No]:
     ```

- Создайте пароль для администратора (пользователь **admin@zvirt**):

```
Keycloak [admin] password:
Please confirm password:
```

- Подтвердите остановку сервиса ovirt-engine:

```
During execution engine service will be stopped (OK, Cancel) [OK]:
```

- Проверьте сводные данные и запустите реконфигурацию:

```
Please confirm installation settings (OK, Cancel) [OK]:
```

1. При успешном завершении операции вы получите следующее сообщение:

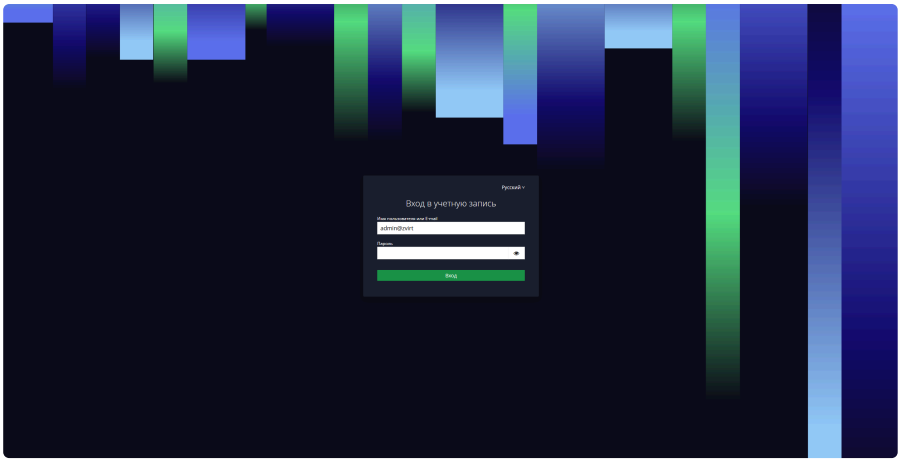
```
          --== END OF SUMMARY ==--

[ INFO  ] Restarting httpd
[ INFO  ] Starting keycloak service
[ INFO  ] Keycloak admin password will be used as ovirt admin password.
[ INFO  ] Start with setting up Keycloak for zVirt Engine
[ INFO  ] Done with setting up Keycloak for zVirt Engine
[ INFO  ] Stage: Clean up
          Log file is located at /var/log/ovirt-engine/setup/ovirt-
engine-setup-20240611154634-3fx0no.log
[ INFO  ] Generating answer file '/var/lib/ovirt-
engine/setup/answers/20240611160300-setup.conf'
[ INFO  ] Stage: Pre-termination
[ INFO  ] Stage: Termination
[ INFO  ] Execution of setup completed successfully
```

2. Перезапустите сервис zvirt-engine-backend:

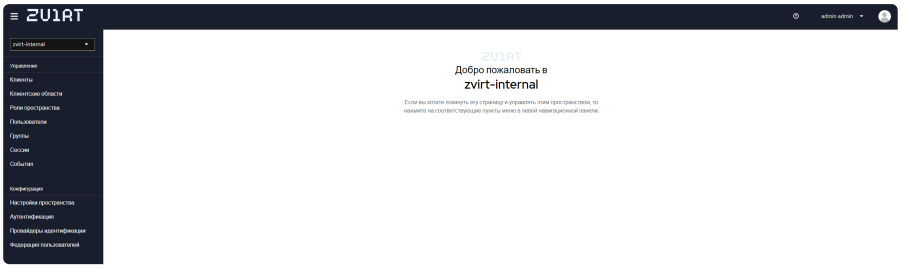
```
systemctl restart zvirt-engine-backend
```

BASH

1. Для проверки перейдите на веб-портал и аутентифицируйтесь на портале администрирования с пользователем **admin@zvirt**:



2. Также перейдите на портал Keycloak по адресу **https://<ENGINE-FQDN>/ovirt-engine-auth/admin/zvirt-internal/console** и аутентифицируйтесь под пользователем **admin@zvirt** с паролем, заданным в процессе реконфигурации.



3. Перенос пользователей

На текущий момент не существует никаких методов автоматизации миграции пользователей и групп с AAA JDBC на Keycloak. Поэтому данная операция выполняется вручную.

Для переноса пользователей необходимо выполнить следующие действия:

1. На портале keycloak в области **zvirt-internal** создать необходимых пользователей и установить для них пароли. Подробнее см. в разделе Создание пользователей руководстве по управлению.
2. На портале администрирования zVirt:
   a. Удалить старых пользователей и группы. Подробнее см. в разделе Удаление пользователей руководства администратора.

   Не удаляйте пользователей **admin@zvirt** и **SYSTEM**.

   b. Добавить нужных пользователей и группы из Keycloak. Подробнее см. в разделе Добавление пользователей в zVirt руководства по управлению.

c. Назначить новым пользователям и группам необходимые роли. Подробнее см. в разделе Назначение роли администратора или пользователя ресурсу руководства администратора.

Переключение конфигурации Менеджера управления с Keycloak на AAA JDBC

При необходимости можно отключить интеграцию с Keycloak и переключить конфигурацию Менеджера управления на использование AAA JDBC.

1. Процедура переключения с Keycloak на AAA JDBC

После переключения на AAA JDBC все пользователи, созданные ранее в Keycloak, станут недоступны.

Для доступа в портал администрирования необходимо использовать пользователя *admin*.

Порядок действий:

1. Выполните полное резервное копирование конфигурации Менеджера управления в соответствии с инструкцией.
2. Активируйте режим глобального обслуживания.
3. Подключитесь по SSH к Менеджеру управления и авторизуйтесь под пользователем *root*.
4. Любым удобным способом загрузите в домашний каталог пользователя *root* архив с необходимыми скриптами.
5. Распакуйте архив:

```bash
tar -xzvf kc-aaajdbc-tools.tar.gz
```

6. Откройте для редактирования файл **./kc2aaajdbc.sh** и укажите FQDN Менеджера управление в переменной `FQDN`:

```
#!/bin/bash
#FQDN=example.engine.local
FQDN=en.vlab.local ①
if [ -z $FQDN ]; then
    echo "Отредактируйте скрипт - укажите FQDN энджина"
    exit 1
fi

...
```

① Указать FQDN Менеджера управления

7. Сохраните и запустите скрипт:

```
./kc2aaajdbc.sh
```
BASH

8. После окончания выполнения скрипта, перейдите на веб-портал Менеджера и проверьте возможность входа на портал администрирования.
9. Деактивируйте режим глобального обслуживания.

2. Откат конфигурации на Keycloak

После отката конфигурации на Keycloak все пользователи, созданные ранее в Keycloak, будут восстановлены.

Для доступа в портал администрирования необходимо использовать пользователя *admin@zvirt*.

В случае если процедура переключения с Keycloak на AAA JDBC привела к ошибкам, можно откатить выполненные скриптом изменения. Для этого:

1. Активируйте режим глобального обслуживания.
2. Подключитесь по SSH к Менеджеру управления и авторизуйтесь под пользователем *root*.
3. Запустите скрипт:

```
./back2kc.sh
```
BASH

4. После окончания выполнения скрипта, перейдите на веб-портал Менеджера и проверьте возможность входа на портал администрирования.
5. Деактивируйте режим глобального обслуживания.

Ошибка в работе Keycloak после обновления

1. Окружение

zVirt 4.2.

2. Проблема

После обновления до 4.2, запуска Keycloak и применения пакета безопасности:

- Портал администратора/пользователя не работают.
- Возвращается код 500 от ovirt-auth.
- При попытке войти в Keycloak отображается загрузка UI, но загрузка не происходит
- В консоли разработки код HTTP 204.
- Через curl получить токен получается

3. Решение

Необходимо проверить FQDN Менеджера управления (хоста с Менеджером управления в режимах Standalone и Standalone All-in-One). Имя должно быть задано в нижнем регистре.

Если имя задано в верхнем регистре, необходимо выполнить следующее:

1. Перевести fqdn в нижний регистр:
   - В файлах конфигурации в каталоге **/etc/ovirt-engine/engine.conf.d/**
   - В системном имени с помощью `hostnamectl set-hostname <fqdn>`.
2. Исправить имя на нижний регистр в сертификатах в поле **CN**.
3. Исправить имя на нижний регистр в конфигурации Apache в файле **/etc/httpd/conf.d/internalsso-openidc.conf** в полях:
   - **OIDCProviderMetadataURL**
   - **OIDCRedirectURI**
   - **OIDCDefaultURL**
4. Перезапустить сервисы

```
systemctl restart ovirt-engine
systemctl restart httpd
systemctl restart ovirt-engine-keycloak
```

5. Перевести все упоминания FQDN в нижний регистр в настройках клиента в Keycloak. Для этого:
   a. Авторизуйтесь на портале Keycloak пользователем admin@zvirt.
   b. Перейдите в раздел **Clients** и нажмите на **zvirt-engine-internal**
   c. На вкладке **Settings** в группе настроек **Access Settings** исправьте все FQDN, заданные в верхнем регистре.
   d. Нажмите **[Save]**.

Настройка федерации пользователей с Active Directory через LDAPs

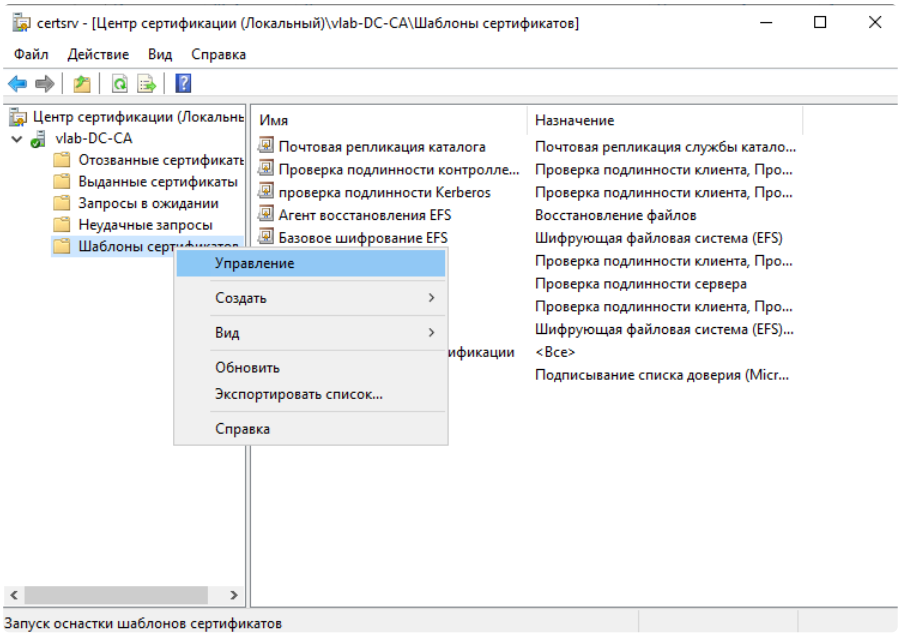
По-умолчанию в Active Directory трафик по протоколу LDAP между контроллерами домена и клиентами не шифруется. Это ограничивает некоторые возможности Keycloak zVirt. Так, например, операция смены пароля должна обязательно осуществляться через безопасный канал. Это означает, что, например, используя инструменты Keycloak, изменить пароль пользователя в домене не удастся.

Защитить данные, передаваемые по протоколу LDAP между Keycloak и контроллером домена можно с помощью SSL версии протокола LDAP - LDAPS, который работает по порту 636. Для этого на контроллере домена необходимо установить специальный SSL сертификат. Сертификат может быть сторонним, самоподписанным или выданным корпоративным центром сертификации.

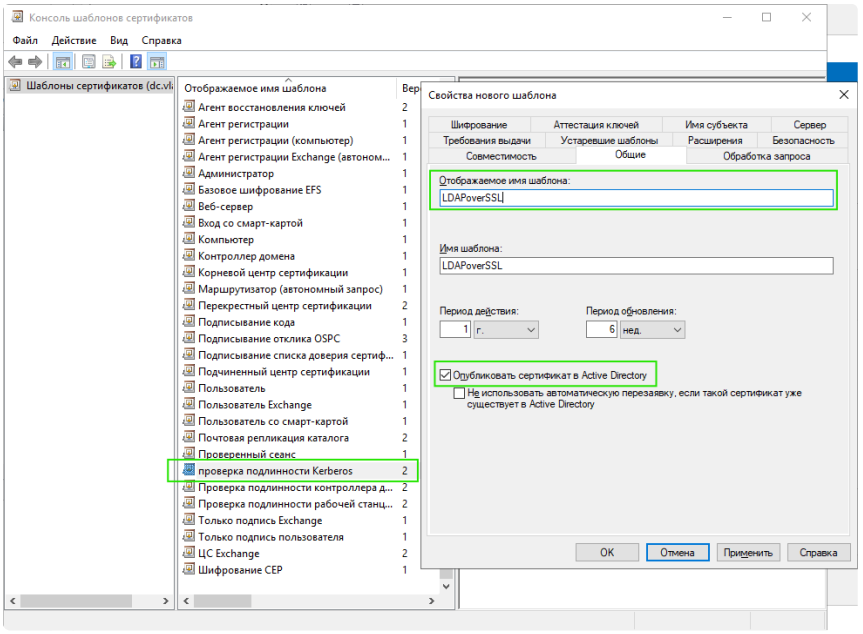
Ниже приведен пример настройки подключения LDAPs с использованием сертификата, выданного корпоративным центром сертификации, развернутым на Windows Server 2019.

Порядок действий:

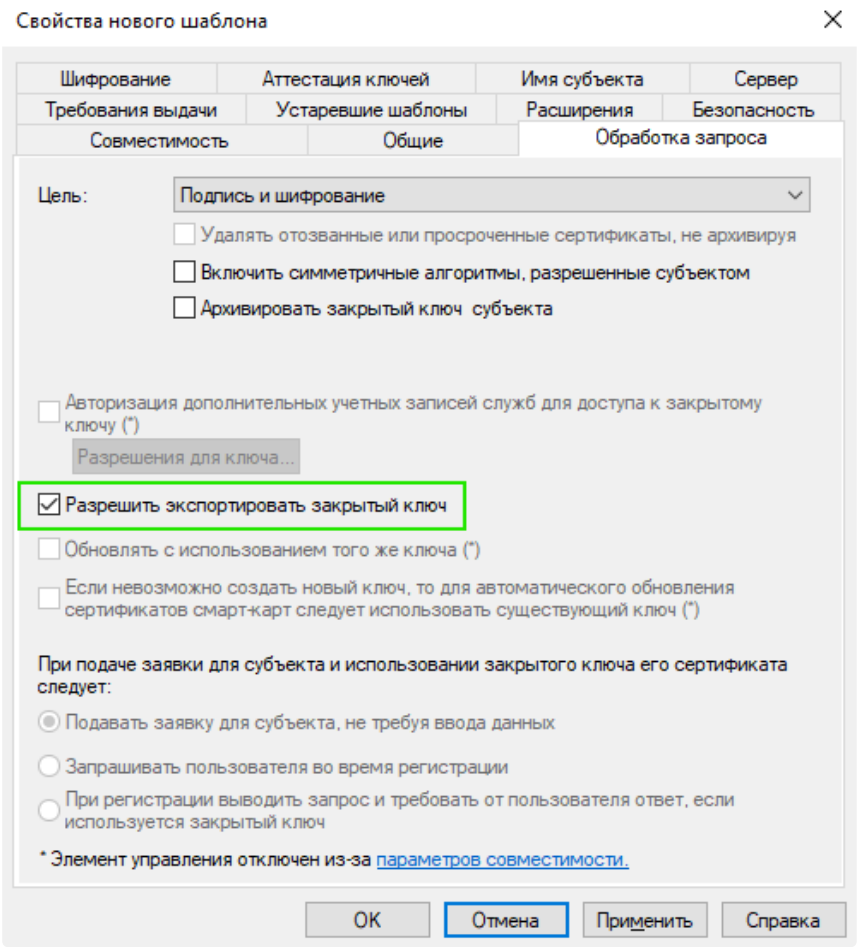
1. В **центре сертификации** откройте оснастку управления центром сертификации (**Средства > Центр сертификации**).
2. Перейдите в управление шаблонами сертификатов.



3. Скопируйте шаблон "Проверка подлинности Kerberos" и в окне свойств нового шаблона:
    - На вкладке **Общее** задайте для него имя и активируйте опцию **Опубликовать сертификат в Active Directory**.



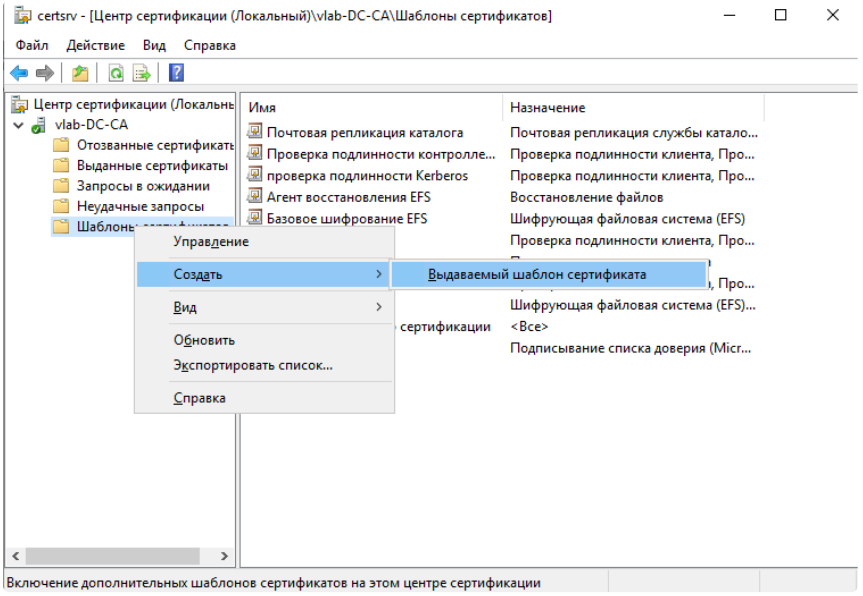
- На вкладке **Обработка запроса** активируйте опцию **Разрешить экспортировать закрытый ключ**.



- Нажмите **[OK]**.

4. Опубликуйте новый тип сертификата:

   a. В контекстном меню **Шаблонов сертификатов** выберите **Создать > Выдаваемый шаблон сертификата**.

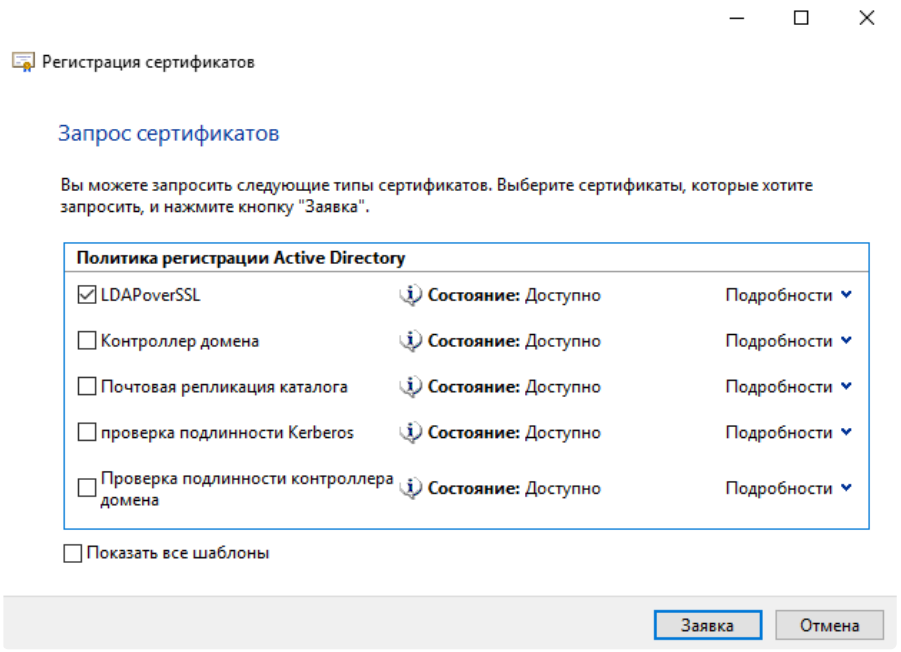


b. В окне включения шаблонов выберите созданную ранее копию и нажмите **[OK]**.

5. Экспортируйте корневой сертификат удостоверяющего центра, например через cmd:

```shell
certutil –ca.cert ca_root.cer
```

6. Скопируйте экспортированный сертификат на контроллер домена и на Менеджер управления (например в каталог **/root**).
7. На **контроллере домена, для которого планируется задействовать LDAPS**, откройте оснастку управления сертификатами.
8. В хранилище **Личное** запросите новый сертификат через контекстное меню: **Все задачи > Запросить новый сертификат**.
9. В окне регистрации сертификатов на этапе **Запрос сертификатов** выберите опубликованный ранее шаблон и нажмите **[Заявка]**, а затем **[Готово]**.



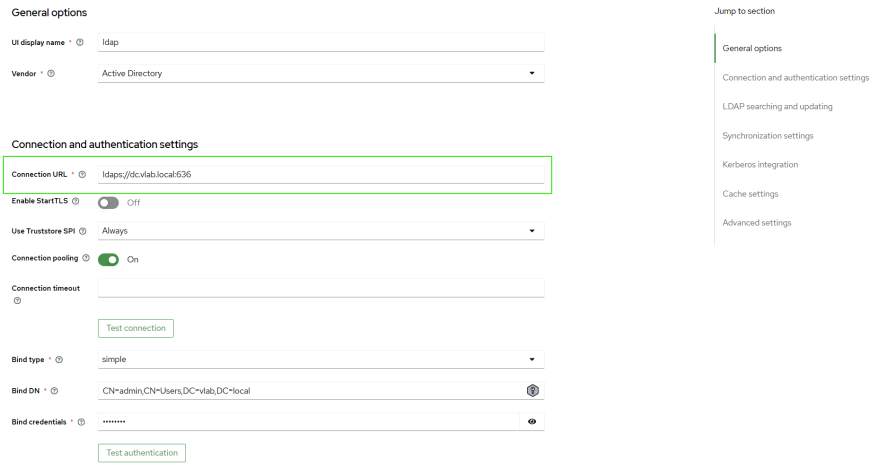
10. Добавьте экспортированный ранее корневой сертификат в доверенные корневые центры сертификации, например через оснастку управления сертификатами:
    a. В cmd или powershell выполните команду `mmc`.
    b. Нажмите `Ctrl`+`M`.
    c. Выберите сертификаты > Учетной записи компьютера.
    d. В хранилище **Доверенные корневые центры сертификации** через контекстное меню выберите **Все задачи > Импорт**.
    e. Выберите файл корневого сертификата и импортируйте его.
11. Перезапустите **Доменные службы Active Directory**.
12. Подключитесь по SSH к Менеджеру управления.
13. Добавьте корневой сертификат в доверенные:

```bash
mv /root/ca_root.cer /etc/pki/ca-trust/source/anchors
update-ca-trust enable
update-ca-trust extract
```

14. Перезапустите сервис Keycloak:

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

15. Перейдите на портал Keycloak и настройте федерацию пользователей в соответствии с инструкцией. При настройке в поле **Connection URL** укажите схему **ldaps**, FQDN контроллера домена и порт **636**.



После сохранения конфигурации на странице **Users** убедитесь, что пользователи синхронизировались.

Если для подключения по ldaps был отредактирован существующий провайдер, синхронизируйте пользователей вручную:

1. На портале Keycloak перейдите в **User Federation**.

2. Нажмите на имя настроенного провайдера.

3. В меню **Action** выберите **Sync all users**.

Руководство по управлению Keycloak

Аннотация

Это руководство содержит описание различных операций с ключевыми для zVirt сущностями Keycloak. Эти сущности включают:

- Пользователей
- Группы пользователей
- Методы аутентификации

Все операции, описанные в этом руководстве, выполняются на портале Keycloak, если явно не указано иное.

По умолчанию при установке zVirt создается два пользователя с административными правами:

- **admin** - суперпользователь, имеющий административные права на управление всем сервером аутентификации. Эта учетная запись может быть полезна, например, в случае, если по каким-то причинам был заблокирован пользователь **admin@zvirt**.

  Чтобы аутентифицироваться под этим пользователем в Keycloak необходимо перейти по адресу **https://<ENGINE-FQDN>/ovirt-engine-auth/** и нажать **Administration Console**.

- **admin@zvirt** - пользователь, имеющий административные права только в области **zvirt-internal**. Данный пользователь имеет достаточные разрешения для выполнения описанных в этом руководстве операций. Рекомендуем использовать именно эту учетную запись.

  Чтобы аутентифицироваться под этим пользователем в Keycloak:

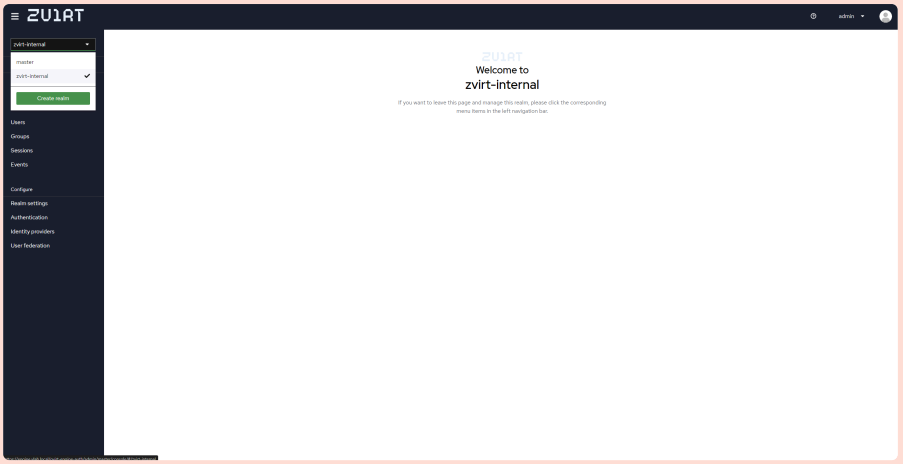
  1. Перейдите на страницу приветствия zVirt по адресу **https://<ENGINE-FQDN>/ovirt-engine/**.
  2. Нажмите на ссылку **Портал Keycloak**.

Оба пользователя по умолчанию имеют одинаковый пароль, указанный при развертывании Менеджера управления.

Пароли пользователей **admin** и **admin@zvirt** не связаны между собой. Т.е. при изменении пароля одного пользователя, пароль второго не изменяется.

Обратите внимание, что все операции, описанные в этом руководстве, zVirt должны выполняться в области **zvirt-internal**, если не указано иное.

Для переключения на эту область выберите её в выпадающем меню:



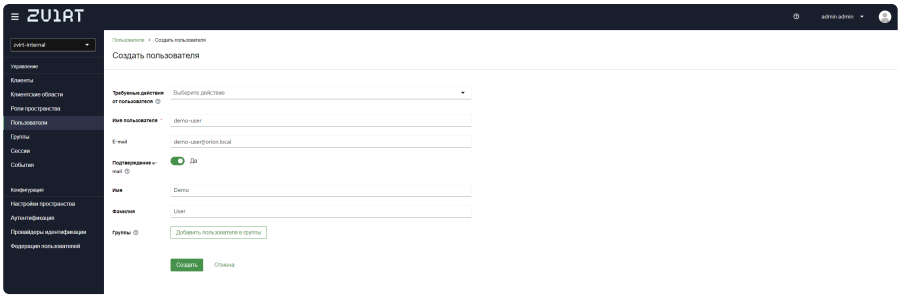
1. Управление пользователями

1.1. Создание пользователей

Убедитесь, что добавление пользователя выполняется в области **zvirt-internal**.

Для добавления пользователя выполните следующие действия:

1. В боковой панели выберите раздел **Users**.
2. Нажмите **[Add user]**.
3. В оснастке добавления пользователя задайте необходимые параметры:
    - (Опционально) **Required user actions** — необходимые действия пользователя при входе в систему. Подробнее о требуемых действиях см. в разделе Определение действий, необходимых при входе в систему.
    - (Обязательно) **Username** — имя пользователя, используемое для аутентификации.
    - (Опционально) **Email** — адрес электронной почты пользователя.
    - (Опционально) **Email verified** — при включении опции **Email verified** пользователю на указанный e-mail придет письмо с инструкцией по активации аккаунта.
    - (Опционально) **First name** — имя пользователя.
    - (Опционально) **Last name** — фамилия пользователя.
    - (Опционально) **Groups** — при нажатии на **[Join Groups]** позволяет добавить пользователя в группы.

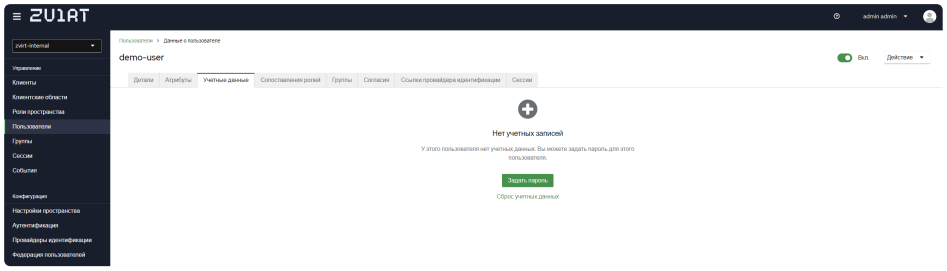


4. Нажмите **[Create]**.

После создания пользователя необходимо определить его учетные данные.

1.2. Определение учетных данных пользователя

Управление учетными данными пользователя осуществляется на вкладке **Credentials** в подробном представлении.



При наличии нескольких учетных данных, можно изменить их приоритет, перетаскивая строки. Самая верхняя учетная запись имеет наивысший приоритет.

Каждая запись учетных данных имеет следующие атрибуты:

- **Type** - указывает на тип учетных данных, например, **password** или **OTP**.
- **User label** - назначаемая метка для распознавания учетной записи при представлении ее в качестве опции выбора во время входа в систему. Для описания учетной записи можно задать любое значение.
- **Created at** - дата и время создания записи учетных данных.
- **Data** - неконфиденциальная техническая информация об учетной записи. По умолчанию она скрыта. Для отображения данных для учетной записи можно нажать кнопку **[Показать данные]** (**[Show data]**).
- **Actions** - включает операции сброса пароля и удаления учетных данных.

1.2.1. Установка пароля пользователя

Если у пользователя нет пароля или он был удален, его можно установить следующими способами:

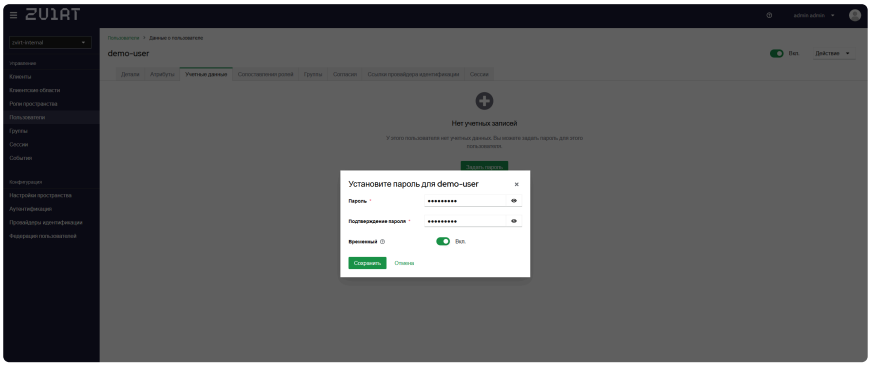
- Администратор может использовать кнопку **[Set password]** на вкладке **Credentials** для установки постоянного или временного пароля.

- Администратор может отправить запрос на email пользователя со ссылкой на страницу установки пароля.

> Этот способ возможно использовать только после настройки SMTP на вкладке **Email** в разделе **Realm Settings**.

Установка пароля администратором

1. В боковой панели выберите раздел **Users**.
2. Нажмите на имя пользователя для перехода в подробное представление.
3. Перейдите на вкладку **Credentials**.
4. Нажмите **[Set password]**.
5. В открывшейся оснастке:
    a. Введите пароль в поля **Password** и **Password confirmation**.
    b. Переключателем **Temporary** укажите будет ли пароль временным. Если эта опция активна, пользователь должен изменить пароль при первом входе в систему.
6. Нажмите **[Save]**.
7. Подтвердите операцию, нажав **[Save password]**.



После выполнения данной операции пользователь сможет войти в систему с заданным паролем.

Отправка запроса на email пользователя для установки пароля

1. В боковой панели выберите раздел **Users**.
2. Нажмите на имя пользователя для перехода в подробное представление.
3. Перейдите на вкладку **Credentials**.
4. Нажмите **[Credential Reset]**.
5. В открывшейся оснастке:
    a. В поле **resetAction** выберите **Update password**.
    b. В поле **Expires In** введите срок действия ссылки на сброс пароля, которая будет включена в письмо, отправленное пользователю.

6. Нажмите **[Send Email]**.

После выполнения данной операции, пользователь получит письмо со ссылкой на страницу установки нового пароля.

1.2.2. Сброс пароля пользователя

Пароль пользователя может быть изменён следующими способами:

- Администратор может сбросить пароль пользователя и самостоятельно установить новый пароль.
- Администратор может установить для пользователя требование обновить пароль при следующем входе в систему.
- Администратор может послать запрос на email пользователя со ссылкой для обновления пароля.

> Этот способ возможно использовать только после настройки SMTP на вкладке **Email** в разделе **Realm Settings**.

Сброс пароля

1. В боковой панели выберите раздел **Users**.
2. Нажмите на имя пользователя для перехода в подробное представление.
3. Перейдите на вкладку **Credentials**.
4. В строке нужных учетных данных **[Reset password]**.
5. В открывшейся оснастке:
    a. Введите пароль в поля **Password** и **New password confirmation**.
    b. Переключателем **Temporary** укажите будет ли пароль временным. Если эта опция активна, пользователь должен изменить пароль при первом входе в систему.
6. Нажмите **[Save]**.
7. Подтвердите операцию, нажав **[Reset password]**.

После выполнения этой операции, пользователь должен будет аутентифицироваться с новым паролем.

Установка требования на обновление пароля

1. В боковой панели выберите раздел **Users**.
2. Нажмите на имя пользователя для перехода в подробное представление.
3. На вкладке **Details** в выпадающем меню **Required user actions** выберите **Update password**.

4. Нажмите **[Save]**.

Поле выполнения данной операции, пользователь должен будет аутентифицироваться со старым паролем, после чего он будет перенаправлен на страницу обновления пароля.

Отправка запроса на email пользователя для обновления пароля

1. В боковой панели выберите раздел **Users**.
2. Нажмите на имя пользователя для перехода в подробное представление.
3. Перейдите на вкладку **Credentials**.
4. Нажмите **[Credential Reset]**.
5. В открывшейся оснастке:
    a. В поле **resetAction** выберите **Update password**.
    b. В поле **Expires In** введите срок действия ссылки на сброс пароля, которая будет включена в письмо, отправленное пользователю.
6. Нажмите **[Send Email]**.

После выполнения данной операции, пользователь получит письмо со ссылкой на страницу обновления пароля.

Данная операция также может быть использована для запроса на первоначальную установку пароля.

1.2.3. Установка одноразового пароля (OTP)

OTP позволяет использовать для аутентификации одноразовые пароли, которые генерируются в специальном приложении - аутентификаторе.

Пользователи могут использовать следующие приложения для генерации OTP:

- Google Authenticator
- Microsoft Authenticator
- Ya.Key
- FreeOTP
- Indeed
- Multifactor

OTP используется только в комплексе со стандартным паролем. Т.е. запрос на конфигурацию OTP необходимо отправлять пользователю после того, как сконфигурирован стандартный (временный или постоянный) пароль.

Настройку OTP можно запросить следующими способами:

Установка требования на настройку OTP

1. В боковой панели выберите раздел **Users**.
2. Нажмите на имя пользователя для перехода в подробное представление.
3. На вкладке **Credentials** убедитесь, что для пользователя установлен стандартный пароль.
4. На вкладке **Details** в выпадающем меню **Required user actions** выберите **Configure OTP**.
5. Нажмите **[Save]**.

После выполнения данной операции:

- Если ранее для учетной записи не был сконфигурирован OTP - пользователь должен будет войти со стандартным паролем, после чего он будет перенаправлен на страницу с описанием настройки OTP.
- Если ранее для учетной записи был сконфигурирован OTP - пользователь должен будет войти со стандартным паролем, затем ввести одноразовый пароль из настроенного приложения-аутентификатора, после чего он будет перенаправлен на страницу с описанием настройки OTP, на которой можно настроить новый аутентификатор.

Отправка запроса на email пользователя для конфигурации OTP

1. В боковой панели выберите раздел **Users**.
2. Нажмите на имя пользователя для перехода в подробное представление.
3. На вкладке **Credentials** убедитесь, что для пользователя установлен стандартный пароль.
4. Нажмите **[Credential Reset]**.
5. В открывшейся оснастке:
    a. В поле **resetAction** выберите **Configure OTP**.
    b. В поле **Expires In** введите срок действия ссылки, которая будет включена в письмо, отправленное пользователю.
6. Нажмите **[Send Email]**.

После выполнения данной операции, пользователь получит письмо со ссылкой на страницу конфигурации OTP.

1.2.4. Настройка политик

Настройка политик для заданной области осуществляется в разделе **Authentication** на вкладке **Policies**.

Перед изменением политик, убедитесь, что текущая активная область - **zvirt-internal**.

1.2.4.1. Парольные политики

По умолчанию для области **zvirt-internal** не заданы парольные политики, поэтому допустимы пароли любой сложности.

В следующей таблице содержится описание возможных параметров политики паролей.

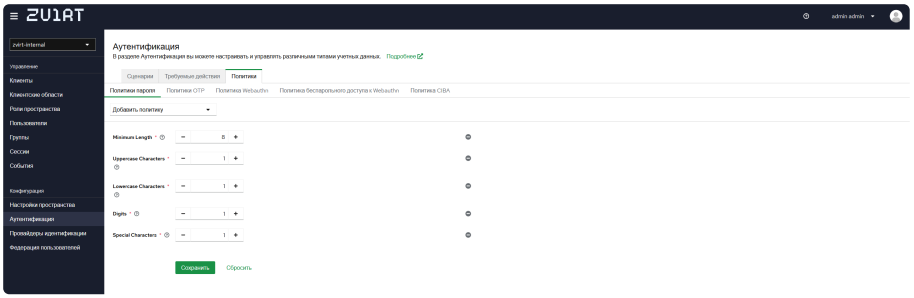
Политика	**Описание**
Expire Password	Количество дней, в течение которых действует пароль. По истечении этого срока пользователь должен сменить пароль.
Hashing Iterations	Указывает количество раз, которое Keycloak хэширует пароли перед хранением или проверкой. При указании значения **-1** будут использоваться значения по умолчанию для выбранного алгоритма хэширования: • argon2 - 5 • pbkdf2-sha512 - 210 000 • pbkdf2-sha256 - 600 000 • pbkdf2 - 1 300 000
Not Recently Used	Количество предыдущих паролей, которые не могут быть использованы пользователем.
Password Blacklist	Черный список, пароли из которого не могут быть использованы. Список представляет собой текстовый файл, путь к которому передаётся в этом поле.
Regular Expression	Пароль должен соответствовать одному или нескольким определенным шаблонам регулярных выражений Java. Синтаксис этих выражений см. в документации по регулярным выражениям Java.
Minimum Length	Ограничение минимальной длины пароля.
Not Username	Пароль не может быть таким же, как имя пользователя.
Not Email	Пароль не может совпадать с адресом электронной почты пользователя.
Special Characters	Количество специальных символов, необходимых в строке пароля.
Uppercase Characters	Количество букв верхнего регистра в строке пароля.
Lowercase Characters	Количество букв нижнего регистра в строке пароля.
Digits	Количество цифр в строке пароля.

Политика	Описание
Maximum Authentication Age	Указывает максимальный срок аутентификации пользователя в секундах, в течение которого пользователь может обновить пароль без повторной аутентификации. Значение 0 означает, что пользователь должен всегда проходить повторную аутентификацию с текущим паролем, прежде чем он сможет обновить пароль.
Hashing Algorithm	Алгоритм хэширования, применяемый к паролям перед сохранением и валидацией. Поддерживаются следующие варианты: • argon2 • pbkdf2-sha512 • pbkdf2-sha256 • pbkdf2 (устаревший)
Maximum Length	Ограничение максимальной длины пароля.

В отношении парольных политик доступны следующие операции:

Добавление политики

1. Перейдите на вкладку **Policies** в разделе **Authentication**.
2. Откройте страницу **Password policy**.
3. В выпадающем списке **Add policy** выберите нужную политику и задайте соответствующее значение.
4. При необходимости повторите операцию для добавления дополнительных политик.
5. Для сохранения нажмите **[Save]**.



Изменение политики

1. Перейдите на вкладку **Policies** в разделе **Authentication**.
2. Откройте страницу **Password policy**.
3. Измените значение нужных политик.
4. Для сохранения нажмите **[Save]**.

Удаление политики

1. Перейдите на вкладку **Policies** в разделе **Authentication**.
2. Откройте страницу **Password policy**.
3. Напротив нужной политики нажмите ⛔.
4. Для сохранения нажмите **[Save]**.

1.2.4.2. Политики OTP

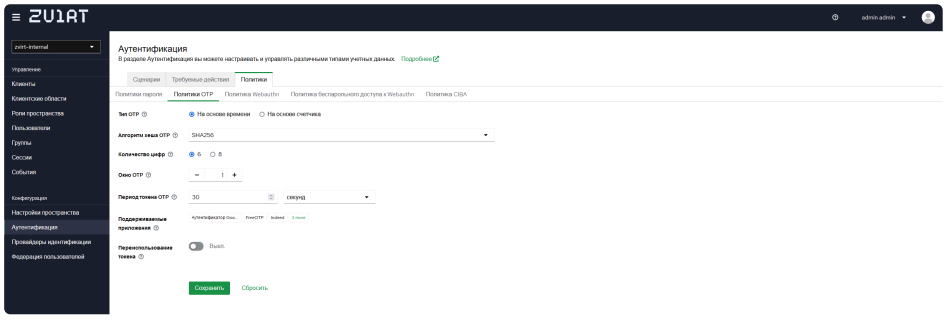
В следующей таблице содержится описание возможных параметров политики OTP и значения по умолчанию.

Политика	**Описание**	**Значение по умолчанию**
OTP type	Алгоритм генерации OTP. Поддерживаются следующие значения: • time-based - генерация на основе времени. При использовании одноразовых паролей, основанных на времени (TOTP), генератор токенов хэширует текущее время и общий секрет. Сервер проверяет OTP, сравнивая хэши за определенный промежуток времени с предоставленным значением. TOTP действительны в течение короткого промежутка времени. • counter-based - генерация на основе счетчика. При использовании одноразовых паролей на основе счетчика (HOTP) Keycloak использует не текущее время, а общий счетчик. Сервер Keycloak увеличивает счетчик при каждом успешном входе в систему OTP. Действительный OTP меняется после успешного входа.	time-based
OTP hash algorithm	Алгоритм хеширования, применяемый к OTP. Допустимы следующие значения: • SHA1 • SHA256 • SHA512	SHA1
Number of digits	Длина OTP. Короткие OTP удобны для пользователя, их легче набирать и легче запомнить. Длинные OTP более безопасны, чем короткие.	6

Политика	Описание	Значение по умолчанию
Look around window	Количество интервалов, в течение которых сервер пытается сопоставить хэш. При Эта опция полезна, если часы генератора TOTP или сервера аутентификации не синхронизированы. Значение по умолчанию (**1**) является достаточным. Например, если временной интервал для токена (OTP Token period) составляет 30 секунд, значение по умолчанию 1 означает, что он будет принимать действительные токены в 90-секундном окне (временной интервал 30 секунд + 30 секунд **до** интервала + 30 секунд **после** интервала). Каждое увеличение этого значения увеличивает допустимое окно на 60 секунд (30 секунд **до** + 30 секунд **после**).	1
OTP Token period	Интервал времени в секундах, в течение которого OTP остаётся действительным. Каждый раз, когда проходит этот интервал, генератор токенов генерирует новый TOTP.	30 секунд
Supported applications	Поддерживаемые приложения-аутентификаторы.	• FreeOTP • Google Authenticator • Indeed • Microsoft Authenticator • Multifactor • Ya.Key
Reusable token	Определяет, можно ли использовать OTP-токены повторно в процессе аутентификации или пользователю нужно ждать следующего токена.	Отключено

Для политик OTP возможно только изменение существующих значений. Для этого:

1. Перейдите на вкладку **Policies** в разделе **Authentication**.
2. Откройте страницу **OTP policy**.
3. Измените значение нужных политик.
4. Для сохранения нажмите **[Save]**.



1.3. Удаление записей учетных данных пользователя

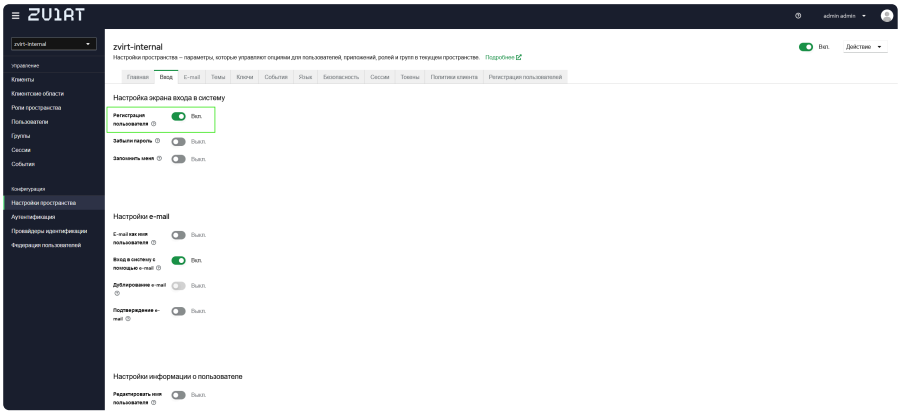
Для удаления ненужных записей учетных данных пользователя выполните следующие действия:

1. В боковой панели выберите раздел **Users**.
2. Нажмите на имя нужного пользователя для перехода в подробное представление.
3. На вкладке **Credentials** в строке учетных данных, которые требуется удалить нажмите **[Delete]** в меню ⋮.
4. Подтвердите удаление, нажав **[Delete]**.

1.4. Самостоятельная регистрация пользователей

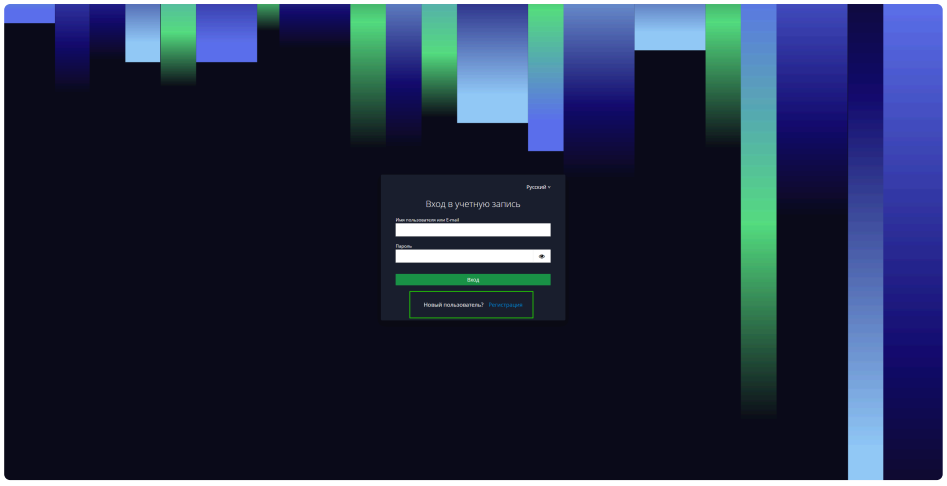
При необходимости можно активировать функцию самостоятельной регистрации пользователей. Для этого выполните следующие действия:

1. Убедитесь, что текущая активная область - **zvirt-internal**.
2. В боковой панели выберите раздел **Realm settings**.
3. На вкладке **Login** активируйте переключатель **User registration**.

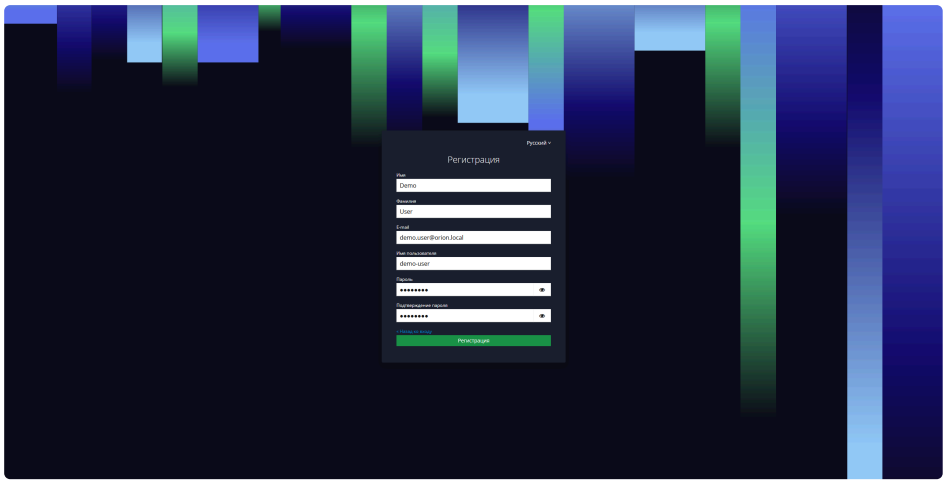


4. Изменения области будут сохранены автоматически.

После активации функции самостоятельной регистрации на страницах входа в порталы zVirt будет добавлена ссылка на страницу регистрации:



Для самостоятельной регистрации пользователю необходимо перейти по этой ссылке и ввести в соответствующую информацию в поля и нажать **[Register]**:



1.5. Определение действий, необходимых при входе в систему

Можно задать действия, которые пользователь должен выполнить при входе в систему. Эти действия требуются после того, как пользователь предоставит учетные данные. После входа в систему и выполнения указанных действий повторное их выполнение не требуется. Требуемые действия добавляются на вкладке **Details** в подробном представлении пользователя.

Некоторые необходимые действия автоматически запускаются для пользователя при входе в систему, даже если они не были явно добавлены администратором для этого пользователя. Например, действие **Update password** может быть вызвано, если политики паролей настроены таким образом, что пароль пользователя необходимо менять каждые **X** дней. Или действие **Update profile** может потребовать от пользователя обновить профиль, если некоторые атрибуты пользователя не соответствуют требованиям конфигурации профиля пользователя.

Основные действия включают:

- **Update Password** - заставляет пользователя сменить пароль при следующем входе.
- **Configure OTP** - заставляет пользователя сконфигурировать OTP при следующем входе.
- **Verify Email** - заставляет пользователя подтвердить email при следующем входе. Пользователю будет отправлено электронное письмо со ссылкой для проверки, на которую он должен перейти. После успешного завершения этого процесса пользователю будет разрешено войти в систему.

> Это действие возможно использовать только после настройки SMTP на вкладке **Email** в разделе **Realm Settings**.

- **Update Profile** - заставляет пользователя обновить информацию в профиле, такую как имя, фамилия, email и т.д.

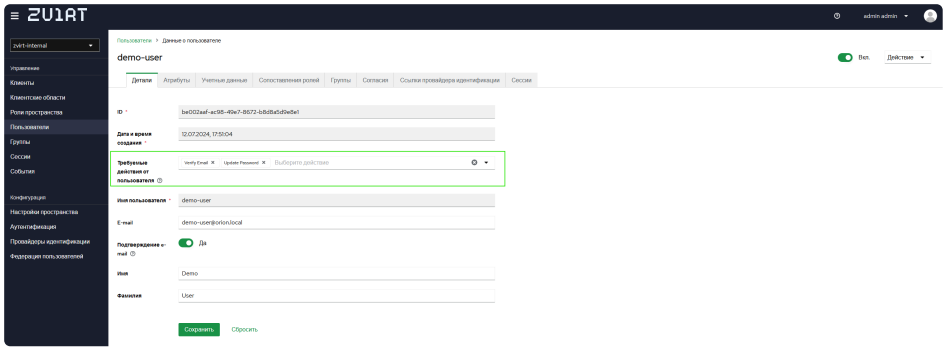
1.5.1. Установка необходимых действий для одного пользователя

Администратор может запросить выполнение необходимого действия для конкретного пользователя. Для этого:

1. В боковой панели выберите раздел **Users**.
2. Нажмите на имя пользователя для перехода в подробное представление.
3. На вкладке **Details** в выпадающем меню **Required user actions** выберите нужные действия.

> Можно выбрать несколько действий.

4. Нажмите **[Save]** для сохранения.

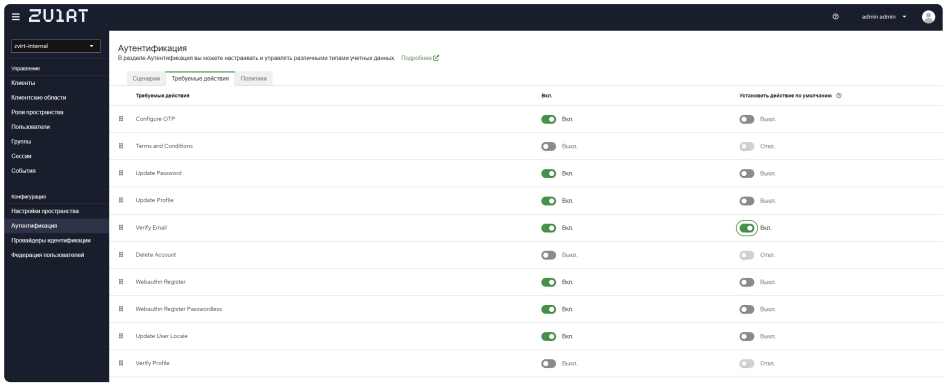


1.5.2. Установка необходимых действий для всех пользователей

Можно указать, какие действия необходимо выполнить перед первым входом в систему для всех **новых пользователей**. Эти требования применяются к пользователям, созданным с помощью кнопки **[Add user]** на странице **Users** или ссылки **Register** на странице входа в систему.

Включите необходимые действия для всех пользователей, выполнив следующие действия:

1. Убедитесь, что текущая активная область - **zvirt-internal**.
2. В боковой панели выберите раздел **Authentication** и перейдите на вкладку **Required actions**.
3. В столбце **Set as default action** активируйте переключатели напротив тех действий, которые должны требоваться от новых пользователей.
4. Изменения сохранятся автоматически.



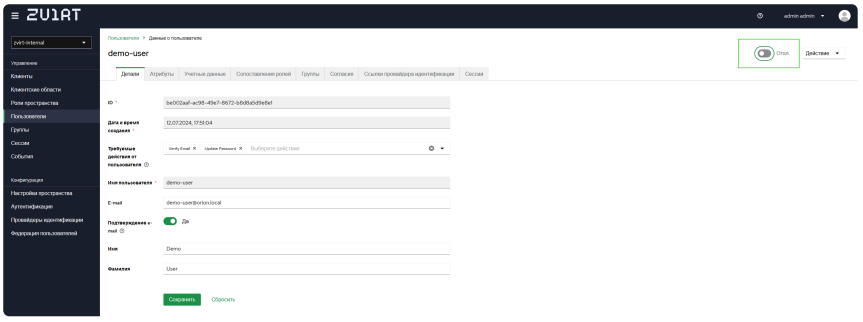
1.6. Отключение и блокировка пользователей

Выбор способа отключения пользователя зависит от желаемого результата.

Например, чтобы временно отключить пользователя, сохранив его роли в zVirt, можно установить для него статус **Disabled**. Если же учетная запись больше не требуется - целесообразно удалить её.

Если пользователю необходимо запретить вход в zVirt, можно использовать один из следующих способов:

- Отключение учетной записи:
    1. В боковой панели выберите раздел **Users**.
    2. Нажмите на имя пользователя для перехода в подробное представление.
    3. Установите переключатель статуса в состояние **Disabled**.



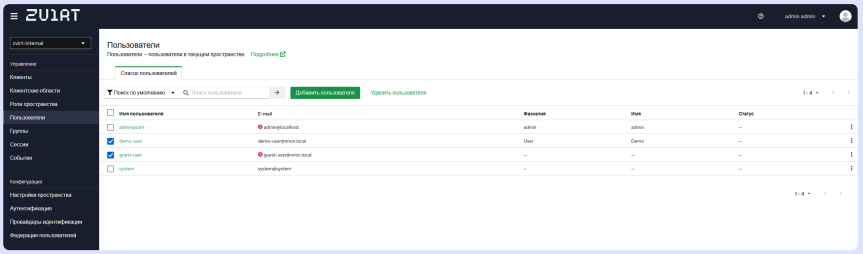
    4. Статус сохранится автоматически.
- Удаление пользователя:

Данная операция необратима.

1. В боковой панели выберите раздел **Users**.
2. В строке пользователя, которого требуется удалить нажмите **[Delete]** в меню ⋮.
3. Подтвердите удаление, нажав **[Delete]**.

Также можно удалить несколько пользователей. Для этого:

1. В списке пользователей отметьте пользователей, которых необходимо удалить.
2. Нажмите **[Delete user]** над списком.
3. Подтвердите удаление, нажав **[Delete]**.



2. Управление группами

Группы в Keycloak управляют общим набором атрибутов для каждого пользователя. Пользователи могут быть членами любого количества групп и наследовать атрибуты, назначенные каждой группе.

Группы являются иерархическими. Группа может иметь несколько подгрупп, но у группы может быть только один родитель.

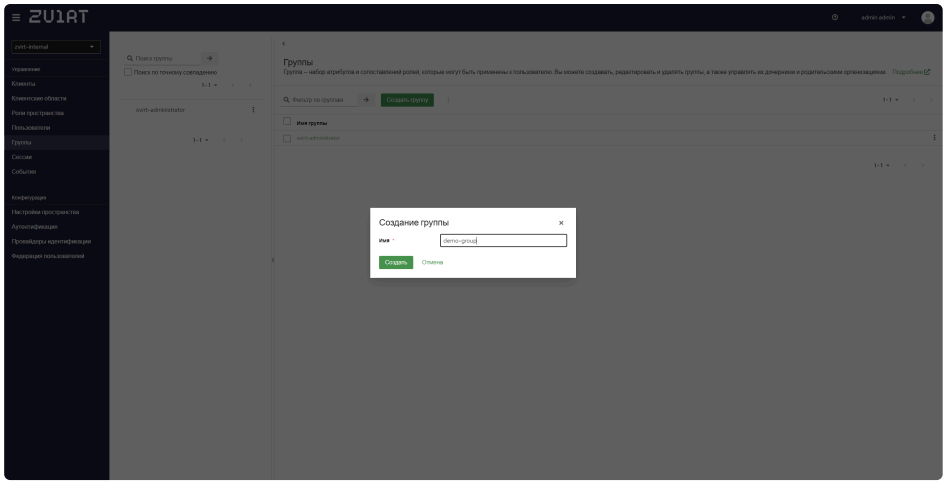
Управление группами осуществляется в разделе **Groups**.

На странице в списке отображаются только группы верхнего уровня. Для просмотра и выполнения операций с дочерними группами, выделите родительскую группу и откройте вкладку **Child groups**. В дополнительном меню (⋮) дочерних групп доступны те же операции, что и в дополнительном меню родительских.

2.1. Создание группы

Для создания новой группы выполните следующие действия:

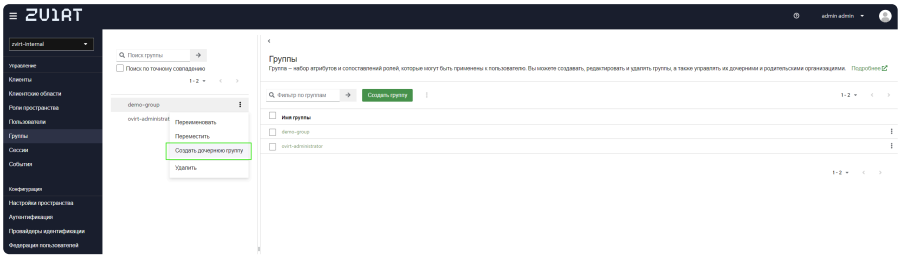
1. В боковой панели выберите раздел **Groups**.
2. Нажмите **[Create group]**.
3. Введите имя группы.
4. Нажмите **[Create]**.



2.2. Создание дочерней группы

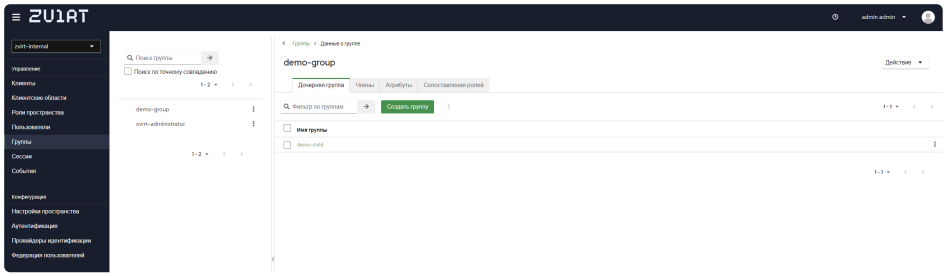
Для создания дочерней группы выполните следующие действия:

1. В боковой панели выберите раздел **Groups**.
2. В дополнительном меню (⋮) нужной группы нажмите **[Create child group]**.



3. Введите имя группы.
4. Нажмите **[Create]**.

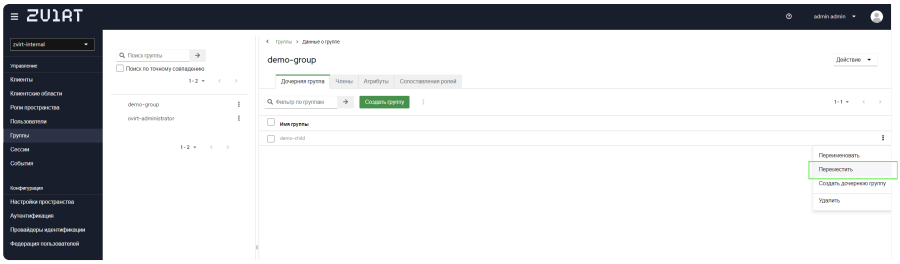
Подгруппа появится в списке дочерних групп.



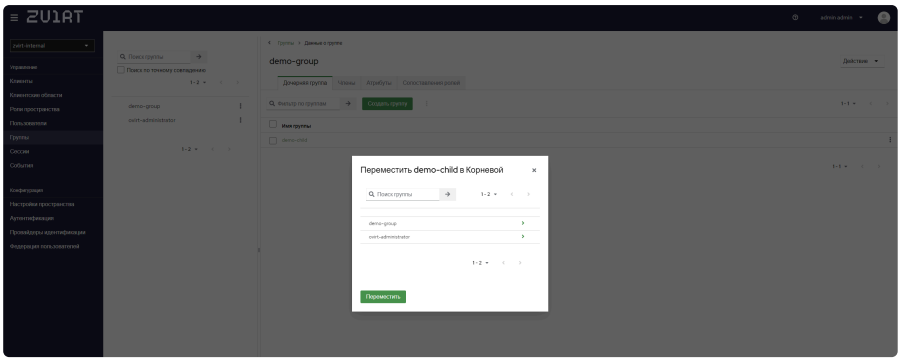
2.3. Перемещение группы

Группы можно перемещать между уровнями и другими группами. Для этого:

1. В боковой панели выберите раздел **Groups**.
2. В дополнительном меню (⋮) нужной группы нажмите **[Move To]**.



3. В появившемся окне выберите группу,в которую хотите переместить выбранную группу. Если целевая группа не выбрана - будет выполнено перемещение на верхний уровень.

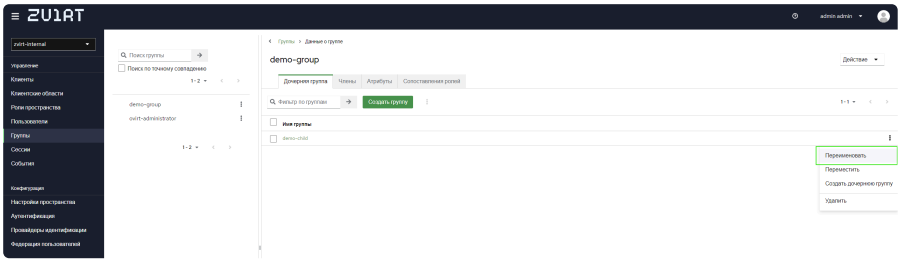


4. Для подтверждения нажмите **[Move Here]**.

2.4. Переименование группы

Для переименования группы выполните следующие действия:

1. В боковой панели выберите раздел **Groups**.
2. В дополнительном меню (⋮) нужной группы нажмите **[Rename]**.

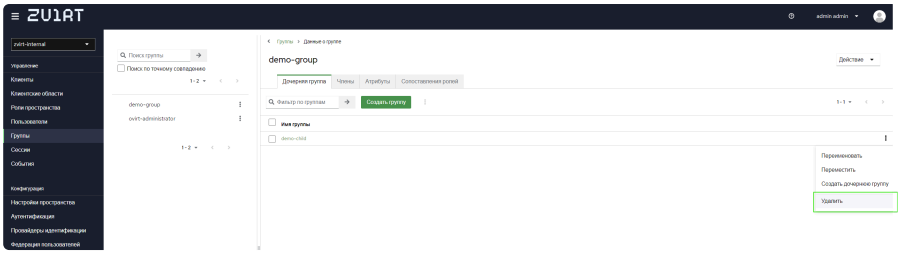


3. В появившемся окне введите новое имя.
4. Для подтверждения нажмите **[Rename]**.

2.5. Удаление группы

Для удаления группы выполните следующие действия:

1. В боковой панели выберите раздел **Groups**.
2. В дополнительном меню (⋮) нужной группы нажмите **[Delete]**.

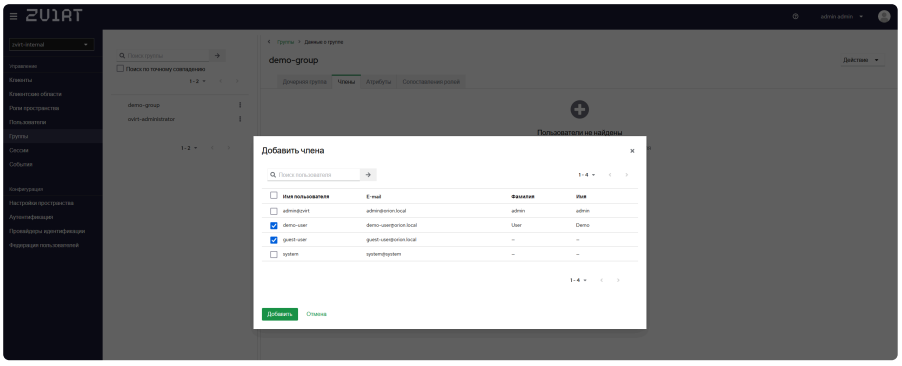


3. Для подтверждения нажмите **[Delete]**.

2.6. Добавление пользователей в группы

Для добавления пользователей в группу выполните следующие действия:

1. В боковой панели выберите раздел **Groups**.
2. Выберите нужную группу верхнего уровня:
    - Если пользователя необходимо добавить в эту группу - перейдите на вкладку **Members**.
    - Если пользователя необходимо добавить в дочернюю группу - нажмите на имя нужной дочерней группы и перейдите на вкладку **Members**.
3. Нажмите **[Add member]**.
4. В появившемся окне отметьте пользователей, которых необходимо добавить в группу.



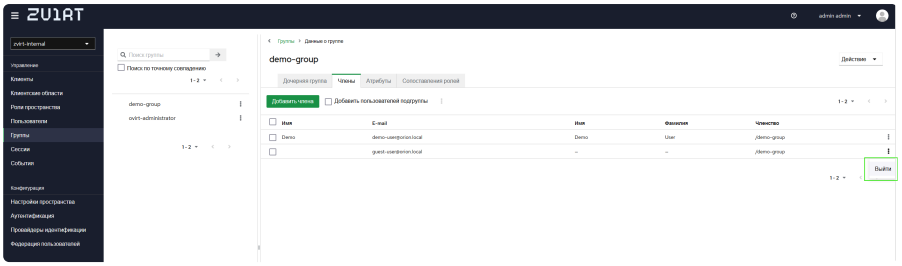
5. Нажмите **[Add]**.

2.7. Исключение пользователей из группы

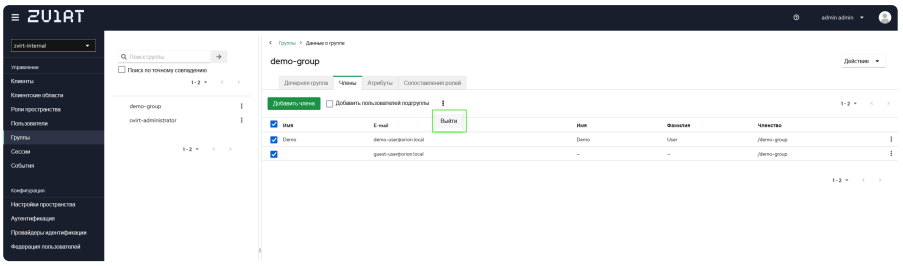
Для исключения пользователей из группы выполните следующие действия:

1. В боковой панели выберите раздел **Groups**.
2. Выберите нужную группу верхнего уровня:
    - Если пользователей необходимо исключить из этой группы - перейдите на вкладку **Members**.
    - Если пользователей необходимо исключить из дочерней группы - нажмите на имя нужной дочерней группы и перейдите на вкладку **Members**.

3. Для исключения конкретного пользователя из группы в дополнительном меню (⋮) этого пользователя нажмите **[Leave]**.



Для исключения нескольких пользователей из группы отметьте этих пользователей и в дополнительном меню (⋮) списка нажмите **[Leave]**.



3. Импорт пользователей и групп в zVirt

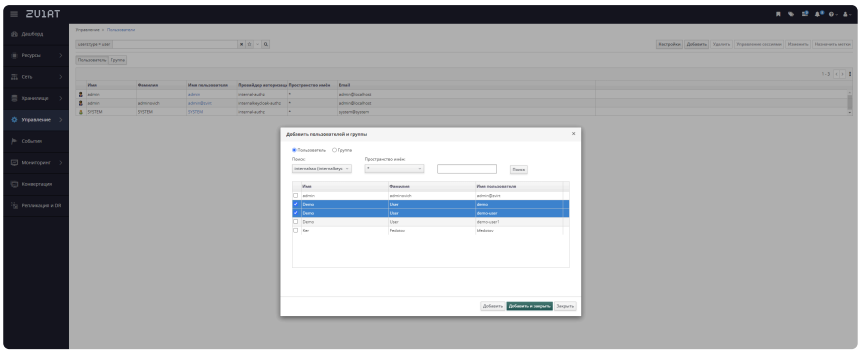
После создания пользователей и групп в Keycloak их нужно импортировать в среду zVirt и назначить им роли. Возможны два способа импорта:

- Автоимпорт. Эта функция запускается при **авторизации** пользователей на портале администрирования или пользовательском портале. При этом для успешного автоимпорта должны быть соблюдены следующие условия:
  - Пользователь должен быть добавлен в группу, которая уже импортирована в zVirt. По умолчанию, такой группой является группа **ovirt-administrator**.
  - Импортированной группе должна быть назначена какая-либо административная или пользовательская роль. Например, группе **ovirt-administrator** назначена роль **SuperUser**.
  - Пользователь должен успешно авторизоваться на портале администрирования или пользовательском портале в соответствии с ролью группы.
- Ручной импорт. Требует вмешательства администратора для импорта пользователей и групп из Keycloak в zVirt. Порядок действий для выполнения этой операции описан ниже.

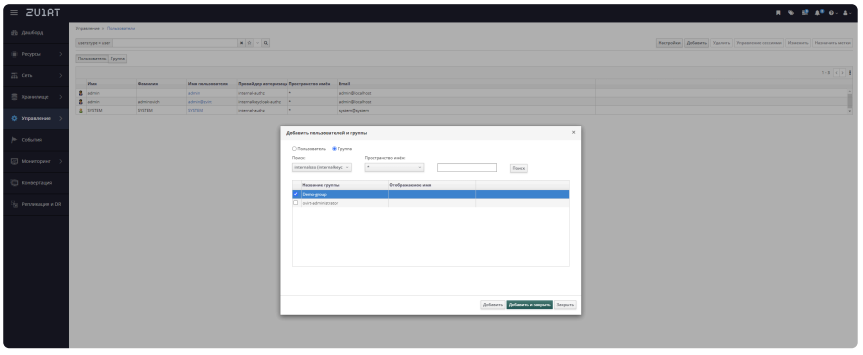
Порядок действий

1. Аутентифицируйтесь на портале администрирования zVirt с учетной записью, имеющей достаточные права для управления пользователями (по умолчанию **admin@zvirt**).
2. Перейдите в **Управление** > **Пользователи**.

3. Нажмите **[Добавить]**.
4. В открывшейся оснастке:
    - Если необходимо импортировать пользователей:
        a. Убедитесь, что активна опция **Пользователь**.
        b. Выберите поиск в **insternalsso**.
        c. Нажмите **[Поиск]**.
        d. Отметьте нужных пользователей и нажмите **[Добавить]** или **[Добавить и закрыть]**.



    - Если необходимо импортировать группы:
        a. Активируйте опцию **Группа**.
        b. Выберите поиск в **insternalsso**.
        c. Нажмите **[Поиск]**.
        d. Отметьте нужные группы и нажмите **[Добавить]** или **[Добавить и закрыть]**.



5. Назначьте импортированным пользователям/группам необходимые роли в соответствии с описанием в разделе Назначение роли администратора или пользователя ресурсу руководства администратора.

4. Подключение служб каталогов к Keycloak

4.1. Введение

Keycloak предоставляет функцию федерации внешних баз данных пользователей, чтобы упростить процесс аутентификации и авторизации для организаций, которые уже имеют собственные системы управления пользователями. Это позволяет организациям интегрировать свои существующие базы данных с Keycloak без необходимости переноса всех данных в новую систему.

Функция федерации внешних баз данных пользователей в Keycloak работает следующим образом:

1. Пользователь пытается войти в систему, используя свои учётные данные.
2. Keycloak проверяет, есть ли пользователь в его собственной базе данных. Если да, то процесс аутентификации продолжается. Если пользователя нет в базе данных Keycloak, система начинает искать совпадение во внешних базах данных, с которыми она интегрирована.
3. Когда совпадение найдено, Keycloak получает информацию о пользователе из внешней базы данных и создаёт запись в своей базе данных для этого пользователя.
4. После успешной аутентификации пользователь может получить доступ к ресурсам, которые защищены Keycloak.

Keycloak не содержит явных ограничений на количество пользователей, получаемых со служб каталогов. На текущий момент успешно протестировано подключение 1200 пользователей.

4.2. Настройка федерации с LDAP

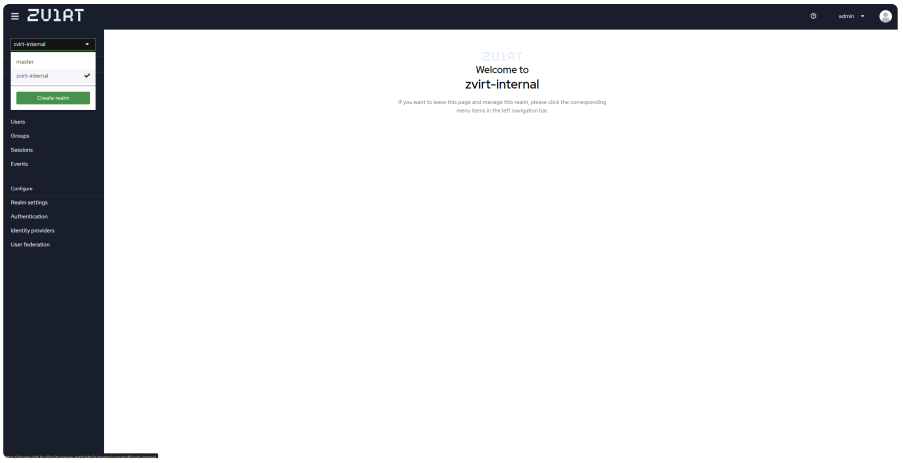
Провайдер хранилища LDAP позволяет настроить интеграцию со следующими службами каталогов:

- FreeIPA
- SambaDC
- Astra ALD Pro
- RedADM
- Active Directory

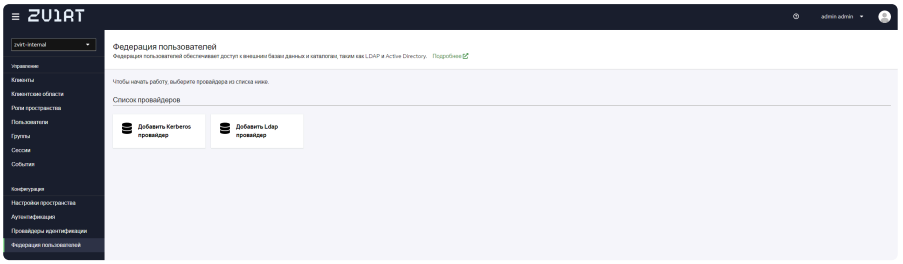
При наличии 2 и более доменов для каждого должен быть настроен отдельный провайдер LDAP.

Для добавления провайдера LDAP выполните следующие действия:

1. Аутентифицируйтесь на портале Keycloak с учетной записью, имеющей достаточные права для управления областью (по умолчанию **admin@zvirt**).
2. Убедитесь, что активирована область **zvirt-internal**:



3. Перейдите в меню **User federation**.



4. Выберите провайдера LDAP с помощью карточек или в списке **Add new provider**.

5. Введите необходимые параметры:

   В разделе General options

   - В поле **UI display name** введите отображаемое имя провайдера.
   - В выпадающем списке **Vendor** выберите подходящего провайдера LDAP:
     - Для **FreeIPA** - Red Hat Directory Server
     - Для **SambaDC** - Active Directory
     - Для **Astra ALD Pro** - Other
     - Для **RedADM** - Active Directory
     - Для **Active Directory** - Active Directory

   В разделе Connection and authentication settings

   - В поле **Connection URL** - введите адрес домена в формате `<scheme>://<ldap-address>:<port>`. Например:

     ```
     ldap://ldap.example.com:389
     ```

     или для защищенного соединения через SSL/TLS:

     ```
     ldaps://ldap.example.com:636
     ```

     В этих примерах:

- `ldap` или `ldaps` указывает на протокол подключения: **LDAP** или **LDAP over SSL/TLS** соответственно.
- `ldap.example.com` — это доменное имя или IP-адрес LDAP-сервера.
- `389` или `636` — стандартные порты для LDAP и LDAPS соединений соответственно.

- Переключатель **Enable StartTLS** позволяет включить шифрование с использованием STARTTLS для связи с LDAP.
- Значение в выпадающем списке **Use Truststore SPI** определяет, будет ли соединение LDAP использовать Service Provider Interface (SPI) для хранилища доверенных сертификатов (Truststore) во время установления защищенного соединения. Можно выбрать одно из двух значений:
  - **Always** - LDAP соединение всегда будет использовать Truststore SPI, который настроен в Keycloak, для управления доверенными сертификатами при установлении соединения.
  - **Never** - LDAP соединение никогда не будет использовать Truststore SPI, даже если он настроен в Keycloak.

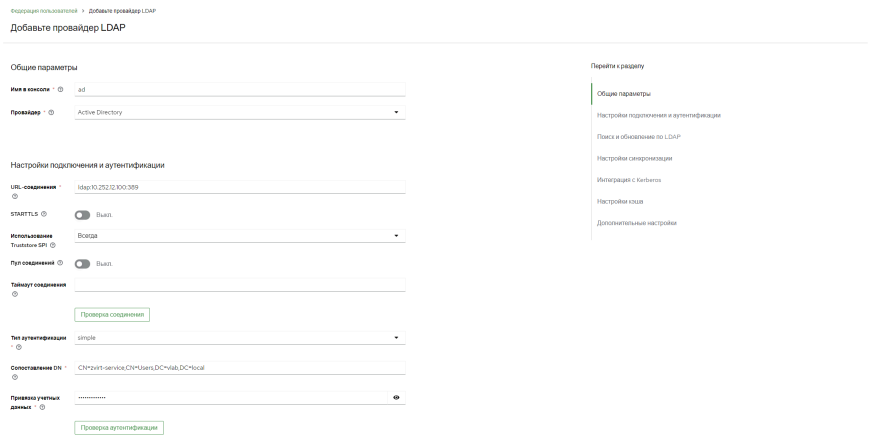
Если Truststore SPI не используется, то LDAP соединение будет опираться на стандартное хранилище доверенных сертификатов Java (cacerts) или на сертификат, указанный в системном свойстве 'javax.net.ssl.trustStore'.

- Переключатель **Connection pooling** позволяет использовать пул соединений для управления LDAP соединениями. **Пул соединений** — это кэш установленных соединений с LDAP сервером, который может быть повторно использован для последующих запросов, что уменьшает накладные расходы, связанные с открытием и закрытием соединений.
  - Если переключатель в состоянии **Включен**, Keycloak сохраняет активные соединения с LDAP сервером в пуле, чтобы они могли быть быстро и эффективно повторно использованы при выполнении LDAP запросов.
  - Если переключатель в состоянии **Отключен**, каждый LDAP запрос будет открывать новое соединение, что может быть более затратно по времени и ресурсам.
- В поле **Connection timeout** при необходимости введите таймаут соединения с LDAP в миллисекундах. Этот параметр определяет максимальное время ожидания установления соединения с LDAP сервером перед тем, как операция будет прервана с ошибкой таймаута.

  Для проверки соединения нажмите **[Test connection]**
- В поле **Bind type** выберите тип аутентификации, который будет использоваться для соединения с LDAP сервером:

- **simple** - это базовый метод аутентификации, при котором клиент передает имя пользователя (часто в форме DN, Distinguished Name) и пароль в открытом тексте (или через защищенное соединение).
- **none** - анонимная аутентификация LDAP.

- В поле **Bind DN** укажите уникальный путь к объекту в LDAP каталоге, который Keycloak будет использовать для аутентификации перед выполнением операций в LDAP.
- В поле **Bind credentials** укажите пароль, который будет использоваться при аутентификации.



Для проверки аутентификации нажмите **[Test authentication]**.

В разделе LDAP searching and updating

- В выпадающем списке **Edit mode** выберите режим взаимодействия Keycloak с сервером LDAP. Этот параметр управляет тем, разрешено ли Keycloak редактировать данные пользователей в LDAP и как это должно быть выполнено.
  - **READ_ONLY** - Keycloak не будет вносить изменения в записи LDAP. Все операции по управлению пользователями (например, изменение пароля, профиля и т. д.) должны выполняться непосредственно через LDAP. Этот режим подходит, когда Keycloak используется только для аутентификации и авторизации пользователей, а управление пользователями осуществляется вне Keycloak.
  - **WRITABLE** - Keycloak может вносить изменения в записи LDAP. Это включает в себя создание, обновление и удаление пользовательских учетных записей. Этот режим позволяет администраторам Keycloak управлять пользователями непосредственно из Keycloak, и изменения будут синхронизированы с LDAP.

    Данный режим необходим для работы двухфакторной аутентификации (с использованием OTP) при подключении к SambaDC, RedADM и MS AD.

        - **UNSYNCED** - Пользователи могут редактировать свои профили и изменять пароли через Keycloak, но изменения не будут синхронизированы с LDAP. Это может быть полезно, если изменения должны быть временными или если LDAP используется только как начальный источник учетных данных.
    - В поле **Users DN** укажите базовый DN (Distinguished Name), откуда начинается поиск пользователей в LDAP каталоге.
    - В поле **Username LDAP attribute** при необходимости измените имя атрибута LDAP, который будет сопоставляться с именем пользователя Keycloak. Для многих провайдеров LDAP-серверов это может быть **uid**. Для Active directory это может быть **sAMAccountName** или **cn**. Атрибут должен быть заполнен для всех записей пользователей LDAP, которые необходимо импортировать из LDAP в Keycloak.
    - В поле **RDN LDAP attribute** при необходимости измените имя атрибута LDAP, который будет использоваться для формирования относительного имени (Relative Distinguished Name, RDN) учетных записей пользователей. RDN является уникальной идентифицирующей частью DN (Distinguished Name) и служит для различия записей на одном и том же уровне в иерархии LDAP. Обычно для RDN используются такие атрибуты, как **uid** - идентификатор пользователя и **cn** - общее имя.
    - В поле **UUID LDAP attribute** при необходимости измените значение атрибута, который будет использоваться для уникальной идентификации каждой учетной записи пользователя. UUID означает "Universally Unique Identifier" (универсальный уникальный идентификатор). Этот атрибут содержит значение, которое должно быть уникальным для каждого пользователя во всем LDAP каталоге.

      В разных системах LDAP этот атрибут может иметь разные названия. Например, в Microsoft Active Directory часто используется атрибут **objectGUID**, а в OpenLDAP — **entryUUID**.
    - В поле **User object classes** при необходимости измените список классов объектов, которые будут использоваться для идентификации объектов пользователей в LDAP каталоге. Классы объектов в LDAP определяют набор атрибутов, которые могут быть связаны с объектом, и правила, которым эти объекты должны соответствовать. При синхронизации и поиске пользователей Keycloak будет искать объекты в LDAP, которые соответствуют всем указанным классам объектов.
    - В поле **User LDAP filter** при необходимости укажите фильтр поиска LDAP, который будет использоваться для ограничения выборки пользовательских записей при запросах к LDAP серверу. Этот фильтр используется для уточнения критериев поиска, чтобы в результаты включались только объекты, соответствующие определенным условиям.

Например, фильтр может быть настроен таким образом, чтобы включать только пользователей с определенным атрибутом или принадлежащих к определенной группе. Фильтр LDAP обычно записывается в формате, который определен стандартом LDAP (RFC 4515).

Пример фильтра, который выбирает только пользователей, у которых установлен атрибут **employeeType** равным **active**:

```
(employeeType=active)
```

Или более сложный фильтр, который выбирает пользователей, которые являются членами определенной группы и у которых есть адрес электронной почты:

```
(&(memberOf=cn=usersGroup,ou=groups,dc=example,dc=com)(mail=*))
```

- В поле **Search scope** при необходимости измените глубину поиска в дереве LDAP для поиска пользовательских записей. Этот параметр управляет тем, какие уровни в дереве LDAP будут включены в поиск, начиная с базового DN (Distinguished Name), указанного для поиска.

  Можно выбрать одно из следующих значений:

  - **One Level** - поиск ограничивается только дочерними объектами непосредственно под базовым DN. Это не включает сам базовый DN или любые объекты на более глубоких уровнях.
  - **Subtree** - поиск включает все объекты в поддереве, начиная с базового DN и распространяясь вниз по всем ветвям дерева до самого нижнего уровня.

    Выбор области поиска зависит от структуры LDAP каталога и требований к поиску пользователей. **Subtree** обычно используется, когда необходимо выполнить более широкий поиск, в то время как **One Level** может быть предпочтительнее для более ограниченного и быстрого поиска.
- В поле **Read timeout** при необходимости укажите максимальное время ожидания для операций чтения данных от сервера. Если данные не получены в течение указанного времени, операция чтения прерывается с ошибкой таймаута.
- При необходимости активируйте переключатель **Pagination**, который позволяет включить функцию разбиения результатов LDAP запроса на страницы, что позволяет обрабатывать большие объемы данных по частям. Это особенно полезно при работе с каталогами, содержащими тысячи или даже миллионы объектов, так как позволяет избежать проблем с производительностью и ограничениями памяти, которые могут возникнуть при попытке загрузить все результаты запроса одновременно.

В разделе Synchronization settings

- Переключатель **Import users** определяет, будут ли пользователи из LDAP автоматически импортированы в базу данных Keycloak во время первой аутентификации пользователя. Если этот параметр включен, то при успешной аутентификации пользователя через LDAP его учетная запись будет скопирована в локальную базу данных Keycloak.
- Переключатель **Sync Registrations** определяет, будут ли новые учетные записи пользователей, созданные в Keycloak, синхронизироваться обратно в LDAP. Это означает, что если новый пользователь регистрируется непосредственно через Keycloak, его учетная запись может быть автоматически создана в LDAP каталоге.

  Если этот параметр включен, то при регистрации нового пользователя через пользовательский интерфейс Keycloak или API, соответствующая учетная запись будет создана не только в Keycloak, но и в LDAP. Это позволяет поддерживать синхронизацию между локальными учетными записями Keycloak и учетными записями в LDAP.
- В поле **Batch size** при необходимости укажите размер пакета (количество записей), который будет обрабатываться за один раз при синхронизации данных между Keycloak и LDAP сервером. Этот параметр важен для управления производительностью и нагрузкой на систему при выполнении операций с большими объемами данных.

  Установка оптимального размера пакета помогает балансировать между скоростью синхронизации и использованием системных ресурсов. Если размер пакета слишком мал, это может привести к увеличению количества операций ввода-вывода и сетевого трафика, что замедлит процесс. Если размер пакета слишком велик, это может привести к чрезмерному потреблению памяти и других ресурсов, что также может негативно сказаться на производительности.
- С помощью переключателя **Periodic full sync** можно активировать периодическую полную синхронизацию пользовательских учетных записей между LDAP и Keycloak. При включении Keycloak будет автоматически запускать полную синхронизацию через заданные промежутки времени, чтобы убедиться, что учетные записи в Keycloak соответствуют учетным записям в LDAP.

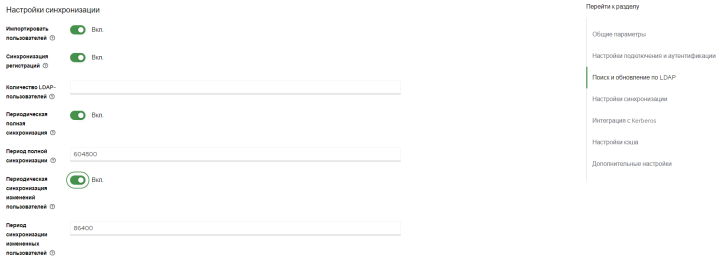
Полная синхронизация обновляет все пользовательские записи, вне зависимости от того, были ли они изменены с момента последней синхронизации. Это может быть полезно для поддержания актуальности данных в Keycloak, особенно если в LDAP происходят изменения, которые не могут быть отслежены в реальном времени.

При активации этой функции появляется поле **Full sync period**, в котором необходимо указать период синхронизации в секундах. По умолчанию указано значение **604800**, что соответствует синхронизации раз в неделю.

- С помощью переключателя **Periodic changed users sync** можно активировать периодическую синхронизацию только тех пользовательских учетных записей, которые были изменены с момента последней полной синхронизации. Этот процесс обновляет в Keycloak только измененные записи, что является более эффективным по сравнению с полной синхронизацией, так как включает в себя меньший объем данных.

  Эта функция особенно полезна для поддержания актуальности данных в средах, где профили пользователей часто обновляются, и требуется регулярно отражать эти изменения в Keycloak без необходимости полной синхронизации всех пользователей.

  При активации этой функции появляется поле **Changed users sync period**, в котором необходимо указать период синхронизации в секундах. По умолчанию указано значение **86400**, что соответствует синхронизации раз в сутки.



В разделе Kerberos integration

- С помощью переключателя **Allow Kerberos authentication** можно включить возможность аутентификации пользователей с помощью протокола Kerberos.

  Когда этот параметр активирован, Keycloak может использовать Kerberos для аутентификации пользователей, которые уже вошли в систему в домене Windows или другой среде, поддерживающей Kerberos. Это позволяет реализовать Single Sign-On (SSO), при котором пользователи не должны повторно вводить свои учетные данные при доступе к различным приложениям, интегрированным с Keycloak.

  Для работы Kerberos аутентификации необходимо настроить Keycloak для взаимодействия с Kerberos сервером (например, с Active Directory), что включает

в себя настройку соответствующих провайдеров аутентификации и сервисных учетных записей в соответствующих полях.

- С помощью переключателя **Use Kerberos for password authentication** можно активировать функцию использования протокола Kerberos для проверки паролей пользователей в процессе аутентификации. Если этот параметр включен, то при вводе пользователем своего пароля Keycloak будет использовать Kerberos для проверки этих учетных данных вместо прямого сравнения с данными, хранящимися в LDAP.

  Для корректной работы этой функции требуется, чтобы Keycloak был правильно настроен для работы с Kerberos, включая наличие соответствующих сервисных учетных записей и ключей.

В разделе Cache settings

- В выпадающем списке **Cache policy** можно выбрать политику кэширования данных пользователей, полученных из LDAP. Этот параметр управляет тем, как и когда данные пользователей, аутентифицированных через LDAP, будут сохраняться в кэше Keycloak.

  Возможные варианты политики кэширования включают:

  - **No Cache** - данные пользователей не кэшируются в Keycloak. Каждый раз при аутентификации пользователя данные будут запрашиваться непосредственно из LDAP.
  - **Default** - используется стандартная политика кэширования Keycloak, которая может включать временное сохранение данных в кэше для ускорения последующих операций аутентификации.
  - **Eviction** - данные в кэше могут быть вытеснены после определенного времени. В списке представлена двумя вариантами:
    - **Evict_daily** - ежедневное вытеснение.
    - **Evict_weekly** - еженедельное вытеснение.
  - **Max Lifespan** - данные в кэше сохраняются в течение максимально установленного времени, после чего они удаляются или обновляются.

    При выборе данного варианта необходимо указать срок хранения (в миллисекундах) в поле **Max lifespan**.

  Выбор политики кэширования зависит от требований к производительности и актуальности данных. Кэширование может существенно ускорить процесс аутентификации за счет уменьшения количества запросов к LDAP серверу, но также может потребовать дополнительных мер для обеспечения согласованности данных между кэшем и LDAP.

В разделе Advanced settings

- Переключатель **Enable the LDAPv3 password modify extended operation** позволяет включить поддержку расширенной операции изменения пароля, определенной в LDAP версии 3. Эта операция позволяет изменять пароль пользователя с помощью специального протокольного запроса, который предназначен для этой цели.

  Когда этот параметр активирован, Keycloak может использовать стандартный LDAP механизм для изменения паролей пользователей, что обеспечивает более безопасный и стандартизированный способ выполнения этой операции. Это также позволяет использовать функции, связанные с политиками паролей, такие как требования к сложности пароля и управление сроками его действия, которые могут быть настроены на LDAP сервере.

- Переключатель **Validate password policy** позволяет включить проверку паролей пользователей на соответствие установленной политике паролей при их изменении или создании новой учетной записи. Если этот параметр включен, Keycloak будет применять свои собственные правила политики паролей к паролям, которые устанавливаются или изменяются через Keycloak, даже если операция происходит в контексте LDAP.

- Переключатель **Trust Email** используется для указания, доверять ли адресам электронной почты, которые импортируются из LDAP без необходимости их дополнительной верификации. Если этот параметр включен, Keycloak будет считать, что электронные адреса, полученные из LDAP, уже проверены и могут быть использованы для различных целей без дополнительных мер подтверждения.

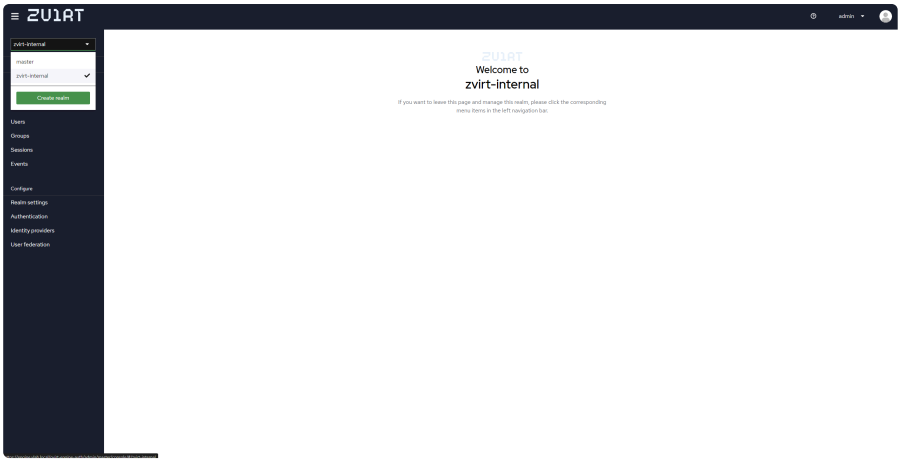
6. Нажмите **[Save]** для сохранения конфигурации.

После сохранения выполняется синхронизация, по окончании которой в разделе **Users** появятся пользователи, полученные с LDAP.

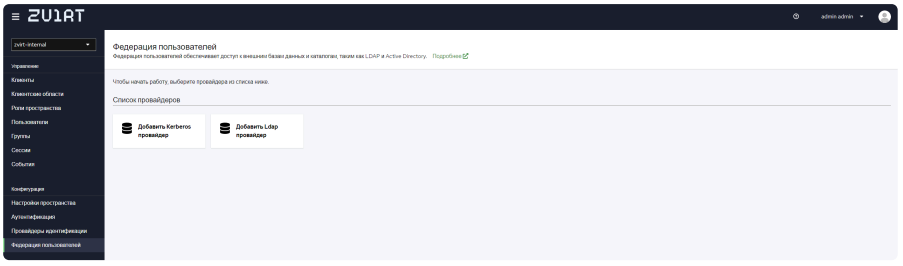
4.3. Добавление групп

После настройки провайдера LDAP синхронизируются только пользователи. Для получения групп из служб каталогов, необходимо в настройке соответствующего провайдера добавить сопоставление с группами. Для этого:

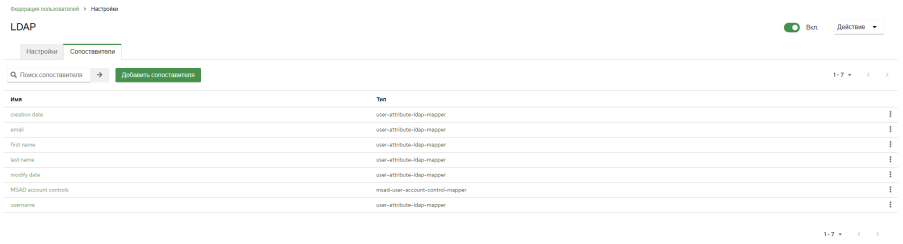
1. Аутентифицируйтесь на портале Keycloak с учетной записью, имеющей достаточные права для управления областью (по умолчанию **admin@zvirt**).
2. Убедитесь, что активирована область **zvirt-internal**:



3. Перейдите в меню **User federation**.



4. Нажмите на имя нужного провайдера и перейдите на вкладку **Mappers**.



5. Нажмите **[Add mapper]**.

6. Введите следующие данные:

   - В поле **Name** введите произвольное имя сопоставления.
   - В выпадающем списке **Mapper type** выбрать **group-ldap-mapper**.
   - В поле **LDAP Groups DN** указать Distinguished Name (DN), который определяет местоположение групп в LDAP дереве. Этот параметр используется для настройки базового пути, с которого Keycloak начнет поиск групп в LDAP каталоге.
   - В поле **Group Name LDAP Attribute** при необходимости измените атрибут в записях LDAP, который будет использоваться для обозначения имени группы. Этот атрибут используется Keycloak для идентификации и сопоставления названий групп в LDAP с группами в Keycloak.
   - В поле **Group Object Classes** при необходимости измените классы объектов, которые будут использоваться для идентификации групп в LDAP каталоге. Класс объекта в LDAP определяет набор атрибутов, которые могут быть связаны с объектом, и правила, которым этот объект должен соответствовать.

В контексте LDAP, классы объектов для групп обычно включают такие типы, как **groupOfNames**, **groupOfUniqueNames**, **posixGroup**, и другие, в зависимости от схемы LDAP и типа каталога.

- Переключатель **Preserve Group Inheritance** позволяет включить сохранение иерархии наследования групп, которая существует в LDAP при их синхронизации. Это означает, что если в LDAP группы организованы в иерархической структуре, где одни группы могут быть вложены в другие, активация этой опции позволит отразить такую же структуру внутри Keycloak.

  Если опция включена, Keycloak будет учитывать вложенность групп при синхронизации, что позволит сохранить уровни подчиненности и наследования ролей и доступов, как они были настроены в LDAP.

  > В сложных иерархических структурах активация этой опции может приводить к ошибке **unknown error**. Если при синхронизации групп возникает данная ошибка - выключите эту опцию.

- Переключатель **Ignore Missing Groups** определяет, как Keycloak будет реагировать на отсутствие групп в LDAP, которые присутствуют в Keycloak.

  Если этот параметр включен, то при синхронизации групп между LDAP и Keycloak, отсутствующие группы в LDAP будут игнорироваться, и не будет происходить удаление соответствующих групп в Keycloak.

  Это может быть полезно в ситуациях, когда некоторые группы управляются исключительно в Keycloak и не имеют или не должны иметь прямого соответствия в LDAP. Включение этого параметра позволяет избежать потери групп и связанных с ними политик доступа в Keycloak в случае их отсутствия в LDAP.

  Если параметр выключен, то при синхронизации, если в LDAP не найдена группа, которая есть в Keycloak, такая группа может быть удалена из Keycloak, чтобы состояние групп в Keycloak соответствовало состоянию групп в LDAP.

- В поле **Membership LDAP Attribute** при необходимости измените атрибут в записях LDAP, который будет использоваться для обозначения членства пользователя в группах. Этот атрибут указывает на то, какие объекты (пользователи) являются членами определенной группы в LDAP.

  Например, во многих LDAP системах для обозначения членства в группах используется атрибут **member** или **uniqueMember**.

- В выпадающем списке **Membership Attribute Type** при необходимости измените тип атрибута членства, который будет использоваться в LDAP для связывания пользователей с группами. Этот параметр указывает, каким образом членство пользователя в группе представлено в LDAP

Возможные значения для **Membership Attribute Type** включают:

- **DN** - членство пользователя в группе будет представлено в LDAP через полный DN пользователя. Это означает, что атрибут членства группы будет содержать полные DN пользователей, которые являются её членами.
- **UID** - членство пользователя в группе будет представлено через уникальный идентификатор пользователя (например, его имя пользователя). В этом случае атрибут членства группы будет содержать UID пользователей.

- В поле **Membership User LDAP Attribute** при необходимости измените атрибут учетной записи пользователя в LDAP, который будет использоваться для сопоставления с атрибутом членства группы. Этот параметр важен при настройке связи между пользователями и группами, особенно когда членство в группе определяется через атрибуты пользователей, включенные в запись группы.

  Например, если группы в LDAP содержат атрибут **member** или **memberUid**, который ссылается на уникальные идентификаторы пользователей, то **Membership User LDAP Attribute** должен соответствовать атрибуту учетной записи пользователя, который используется в этих ссылках.
- В поле **LDAP Filter** при необходимости укажите фильтр поиска LDAP, который будет использоваться для ограничения выборки записей групп при запросах к LDAP серверу.
- В выпадающем списке **Mode** при необходимости измените способ синхронизации групп между LDAP и Keycloak. Этот параметр управляет тем, как Keycloak будет обрабатывать данные о группах, хранящиеся в LDAP.

  Варианты значения параметра *Mode*включают:

  - **READ_ONLY** - в этом режиме Keycloak только читает информацию о группах из LDAP, не внося в неё изменений. Управление группами происходит исключительно на стороне LDAP.
  - **LDAP_ONLY** - Keycloak использует группы непосредственно из LDAP, и любые изменения в группах должны производиться через LDAP. В этом режиме группы не синхронизируются и не импортируются в базу данных Keycloak.
  - **IMPORT** - группы из LDAP импортируются в базу данных Keycloak, и после импорта управление группами осуществляется через Keycloak. В этом режиме изменения в группах, сделанные в Keycloak, не отражаются обратно в LDAP.
- В выпадающем списке **User Groups Retrieve Strategy** при необходимости измените стратегию, которую Keycloak будет использовать для извлечения информации о группах пользователя из LDAP. Этот параметр влияет на то, как Keycloak определяет, к каким группам принадлежит пользователь.

  Возможные значения для **User Groups Retrieve Strategy** включают:

- **LOAD_GROUPS_BY_MEMBER_ATTRIBUTE** - при использовании этой стратегии Keycloak будет искать группы, в которых пользователь указан в атрибуте членства группы (например, **member** или **memberUid**). Это требует, чтобы LDAP содержал обратные ссылки от групп к пользователям.
- **GET_GROUPS_FROM_USER_MEMBEROF_ATTRIBUTE** - эта стратегия используется, когда LDAP поддерживает атрибут **memberOf** в записях пользователя, который автоматически содержит информацию о всех группах, к которым пользователь принадлежит.
- **LOAD_GROUPS_BY_MEMBER_ATTRIBUTE_RECURSIVELY** - похожа на первую стратегию, но также поддерживает рекурсивный поиск групп. Это означает, что если группы вложены друг в друга, Keycloak будет искать не только непосредственные группы пользователя, но и все родительские группы.

- В поле **Member-Of LDAP Attribute** при необходимости измените атрибут в записях пользователя LDAP, который указывает на группы, к которым этот пользователь принадлежит. Этот атрибут используется, когда информация о членстве в группах хранится непосредственно в записи пользователя, а не в записях самих групп.

  Во многих LDAP-серверах, таких как Microsoft Active Directory, атрибут **memberOf** используется для хранения списка DN групп, к которым принадлежит пользователь.

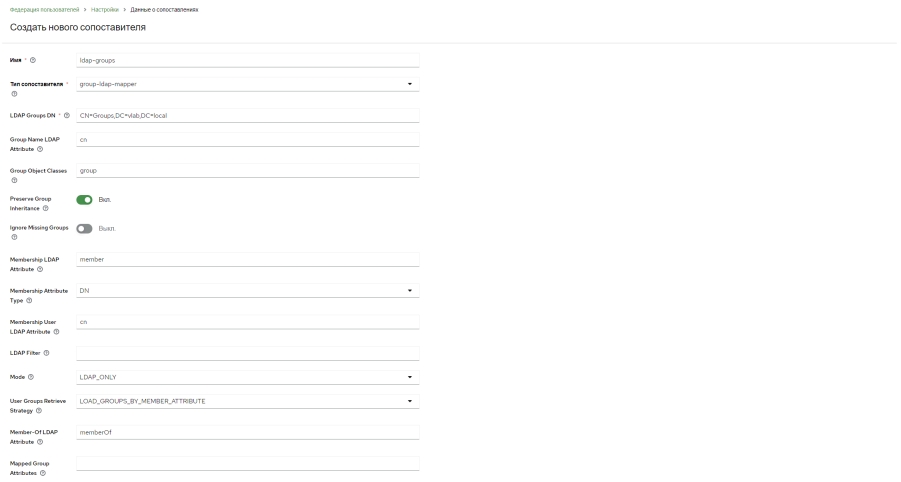
  Когда Keycloak настроен на использование атрибута **memberOf**, он может автоматически извлекать информацию о группах пользователя на основе этого атрибута, что упрощает процесс синхронизации групп и членства в них.
- В поле **Mapped Group Attributes** при необходимости укажите атрибуты группы LDAP, которые должны быть синхронизированы и отображены в атрибуты группы в Keycloak. Это позволяет выбирать, какие конкретные данные о группах из LDAP будут доступны в Keycloak и как они будут использоваться.

  Например, если в LDAP у групп есть атрибуты, такие как описание (**description**), адрес электронной почты (**mail**) или идентификатор группы (**gidNumber**), и требуется, чтобы эти данные были доступны в Keycloak, их можно указать в параметре **Mapped Group Attributes**.
- Переключатель **Drop non-existing groups during sync** определяет, будут ли удалены группы в Keycloak, которые больше не существуют в LDAP, во время процесса синхронизации. Если этот параметр включен, то во время синхронизации, если определенная группа присутствует в Keycloak, но отсутствует в LDAP, она будет удалена из Keycloak.

  Эта опция помогает поддерживать консистентность данных между Keycloak и LDAP, удаляя устаревшие или удаленные в LDAP группы из Keycloak, что предотвращает расхождение информации о группах между двумя системами.

Если параметр выключен, то даже если группы были удалены или переименованы в LDAP, они останутся в Keycloak до тех пор, пока не будут удалены вручную или через другие процессы синхронизации.

- В поле **Groups Path** при необходимости измените путь в иерархии Keycloak, куда будут помещены группы, синхронизированные из LDAP. Этот параметр позволяет задать конкретное местоположение в структуре групп Keycloak для размещения импортированных групп.



7. Нажмите **[Save]** для сохранения конфигурации.

После сохранения конфигурации, для запуска синхронизации групп выполните следующее:

1. На вкладке **Mappers** нажмите на имя созданного сопоставления.
2. В выпадающем списке **Actions** выберите **Sync LDAP groups to Keycloak**.

3. В разделе **Groups** основного меню убедитесь, что нужные группы импортировались в Keycloak.

4.4. Сопоставление атрибутов

По умолчанию при настройке федерации сопоставляются следующие атрибуты пользователей:

Имя сопоставителя	**Атрибут модели Keycloak**	**Атрибут LDAP**	**Описание**
creation date	createTimestamp	whenCreated	Дата создания пользователя
full name	fullName	cn	Полное имя пользователя, как указано в CommonName (cn)

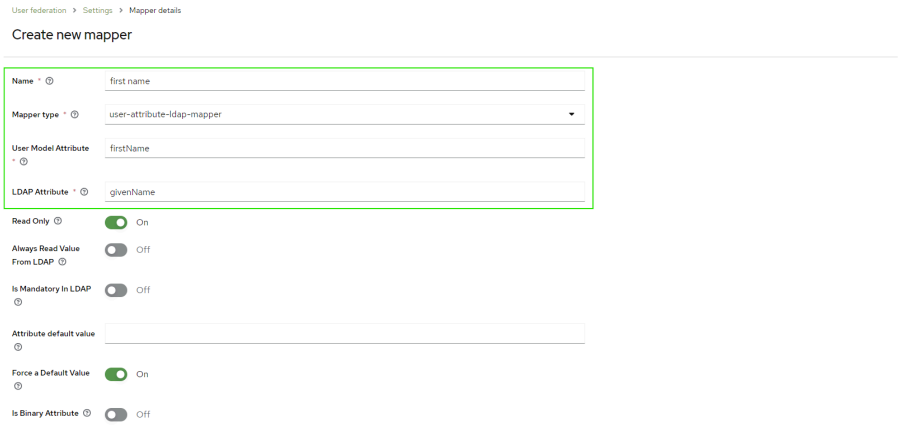
Имя сопоставителя	Атрибут модели Keycloak	Атрибут LDAP	Описание
last name	lastName	sn	Фамилия пользователя, как указано в Surname (sn)
modify date	modifyTime-stamp	whenChanged	Дата изменения пользователя
username	username	Зависит от поля **Username LDAP attribute** в настройке федерации	Имя пользователя, используемое для аутентификации

При настройке сопоставления групп, по умолчанию никакие атрибуты для групп не добавляются.

Для настройки или добавления сопоставления атрибутов пользователей выполните следующие действия:

1. Авторизуйтесь на портале Keycloak администратором области zvirt-internal.
2. Перейдите в **User federation**.
3. Нажмите на имя нужного провайдера и перейдите на вкладку **Mappers**.
4. Нажмите **[Add mapper]**.
5. В оснастке создания сопоставителя:
    a. Введите уникальное имя.
    b. В списке **Mapper type** выберите **user-attribute-ldap-mapper**.
    c. В поле **User Model Attribute** введите необходимый атрибут пользователя Keycloak.
    d. В поле **LDAP Attribute** введите сопоставляемый атрибут LDAP.
    e. При необходимости измените дополнительные параметры.
    f. Нажмите **[Save]**

Пример настройки сопоставления имени пользователя для ActiveDirectory:



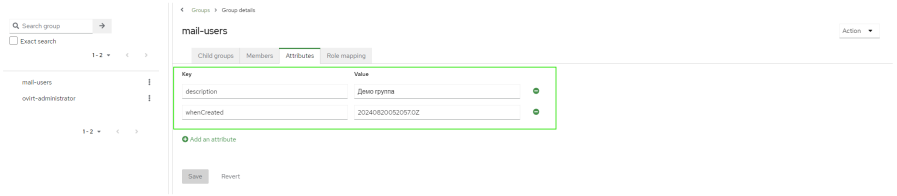
6. В меню **Action (Действия)** выберите **Синхронизировать всех пользователей (Sync all users)**.

После синхронизации указанный атрибут LDAP будет сопоставлен с указанным атрибутом пользователя Keycloak.

Для сопоставления атрибутов групп выполните следующие действия:

1. Авторизуйтесь на портале Keycloak администратором области zvirt-internal.
2. Перейдите в **User federation**.
3. Нажмите на имя нужного провайдера и перейдите на вкладку **Mappers**.
4. Нажмите на имя сопоставителя групп LDAP.
5. В поле **Mapped Group Attributes** через запятую перечислите необходимые атрибуты LDAP.

6. Нажмите **[Save]**
7. Синхронизируйте группы в меню **Action (Действия)** сопоставителя групп.
8. Проверить доступность атрибутов можно на вкладке **Attributes** выбранной группы в разделе **Groups** .



4.5. Настройка интеграции с Kerberos

Предварительные требования:

- В Keycloak корректно настроена федерация пользователей с использованием Active Directory.
- В AD созданы пользователи, для которых будет настроена аутентификация Kerberos.

Порядок действий:

1. На контроллере домена Active directory:
    a. Для нужных пользователей включите 128- и 256-битное шифрование (Свойства пользователя → Учетная запись → Параметры учетной записи).
    b. Запустите powershell от имени администратора и создайте keytab для нужных пользователей с помощью следующей команды:

```
ktpass -out keycloak.keytab -princ HTTP/$engine_fqdn@$DOMAIN_SUFFIX -
mapUser $userUPN -pass $password -ptype KRB5_NT_PRINCIPAL -crypto ALL
```
POWERSHELL

Необходимые параметры:

- **-out keycloak.keytab** - путь для сохранения сгенерированного файла;
- **-princ HTTP/$engine_fqdn@$DOMAIN_SUFFIX** - FQDN Менеджера управления ($engine_fqdn) и доменный суффикс в верхнем регистре ($DOMAIN_SUFFIX)
- **-mapUser $userUPN** - UPN пользователя, для которого генерируется keytab. Домен необходимо указать в верхнем регистре.
- **-pass $password** - пароль пользователя, для которого генерируется keytab.

Например:

```
ktpass -out ad-user1.keytab -princ HTTP/en-user1.vlab.local@VLAB.LOCAL -
mapUser ad-user1@VLAB.LOCAL -pass P@ssw0rd! -ptype KRB5_NT_PRINCIPAL -
crypto ALL
```

c. Скопируйте полученный файл keytab на Менеджер управления, например в каталог /root. Например:

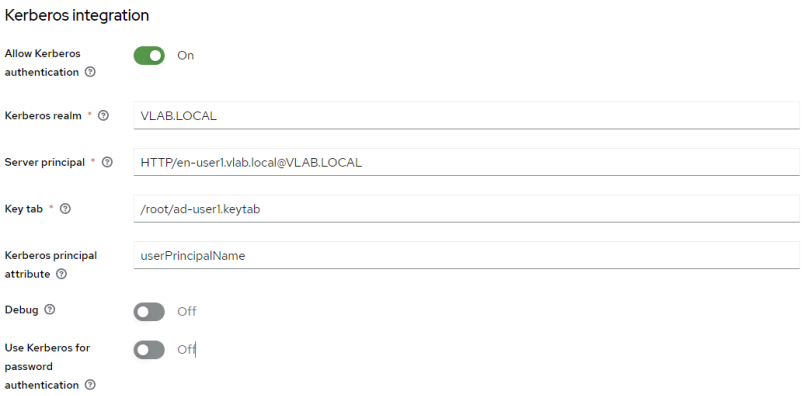
```
scp $PWD\ad-user1.keytab root@10.252.12.10:/root/
root@10.252.12.10's password:
ad-user1.keytab               100%  372    23.3KB/s   00:00
```

2. На портале Keycloak:

a. В разделе **User federation** нажмите на имя соответствующего LDAP-провайдера.

b. На вкладке **Settings** в разделе **Kerberos integration**:

- Активируйте опцию **Allow Kerberos authentication**.
- В поле **Kerberos realm** введите доменный суффикс, использованный при генерации keytab.
- В поле **Server principal** введите principal, как в опции `-princ` при генерации keytab.
- В поле **Key tab** введите абсолютный путь к файлу keytab на Менеджере управления.
- Остальные параметры можно оставить по умолчанию. Например:

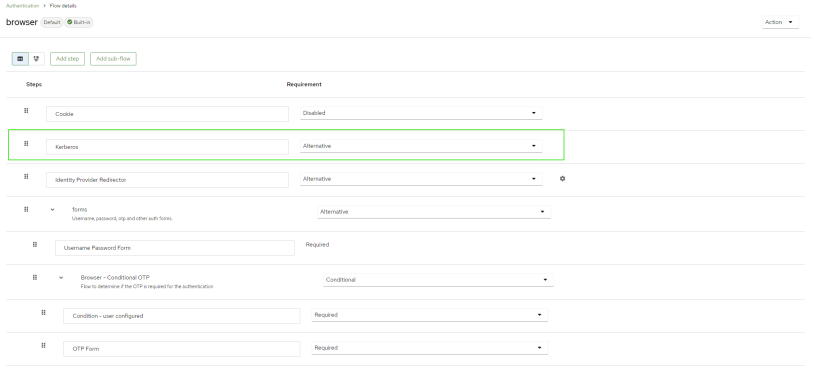


- Нажмите **[Save]**.

c. Перенастройте параметры аутентификации:

i. В разделе **Authentication** нажмите на имя потока **browser**.

ii. Для **Kerberos** выберите **Alternative**.



3. Настройте браузер для доверия соответствующему домену. Например:

- Для Edge:

a. Нажмите **[Пуск]** в windows введите `свойства браузера` и откройте окно настройки.

b. Перейдите на вкладку **Безопасность**.

c. Выделите **Местная интрасеть** и нажмите **[Сайты]**.

d. Нажмите **[Дополнительно]** и добавьте в зону используемый домен. Используйте `*` для задания шаблона. Например:

```
*.vlab.local
```

e. Сохраните настройки.

- Для Google Chrome:

a. Запустите браузер со следующими параметрами:

```
chrome.exe --auth-server-whitelist="*.<engine-domain>" --auth-negotiate-delegate-whitelist="*.<engine-domain>"
```

Например:

```
chrome.exe --auth-server-whitelist="*.vlab.local" --auth-negotiate-delegate-whitelist="*.vlab.local"
```

- Для Firefox:
  a. В адресной строке браузера введите `about:config`.
  b. Найдите настройки `network.negotiate-auth.trusted-uris` и `network.automatic-ntlm-auth.trusted-uris` и запишите в них адрес Менеджера управления.

После этого доменные пользователи, для которых будут разрешения на вход, смогут входить без пароля.

Самостоятельная смена пароля пользователем

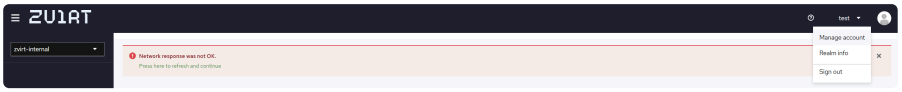
Keycloak предоставляет пользователям возможность самостоятельной смены пароля.

1. Локальные пользователи

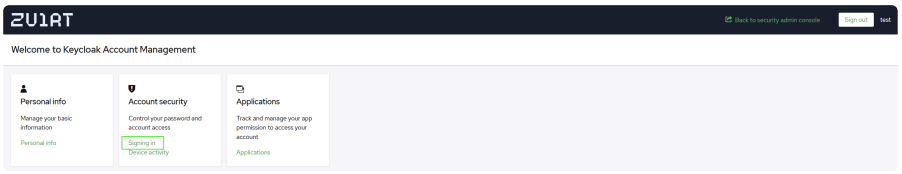
У локальных пользователей по умолчанию есть право на самостоятельный сброс пароля. Никаких дополнительных настроек со стороны администратора не требуется.

Для смены пароля выполните следующие действия:

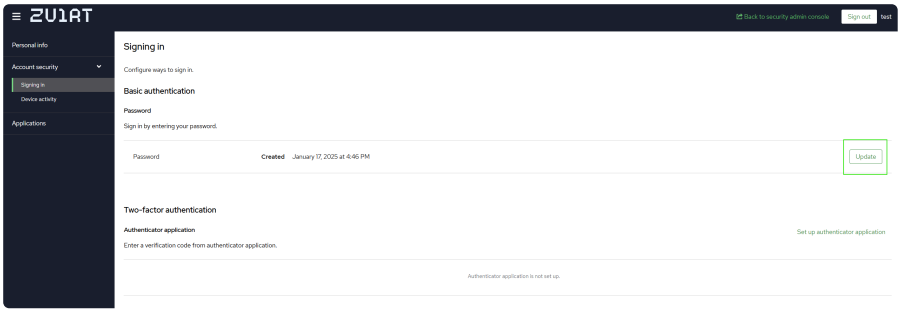
1. Аутентифицируйтесь на портале Keycloak нужным пользователем.
2. В меню учетной записи нажмите **[Manage account]**.



3. На странице управления учетной записью в разделе **Account security** нажмите **[Signing in]**.



4. В разделе **Basic authentication** в строке **Password** нажмите **[Update]**.



5. В открывшейся форме **Update password** введите введите и подтвердите новый пароль.

> Если сессия была завершена, перед обновлением потребуется ввести старый пароль.

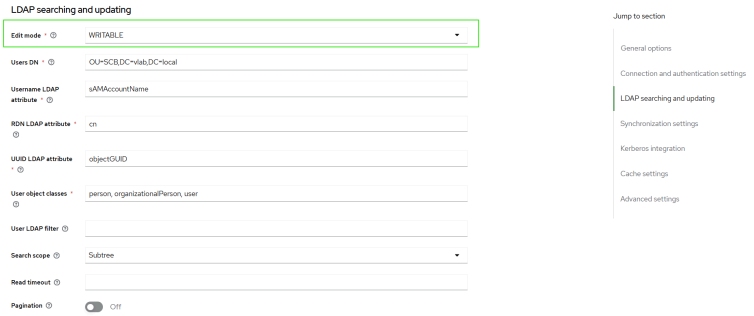
6. Нажмите **[Submit]**.

2. Пользователи Active Directory

По умолчанию, пользователи Active Directory, синхронизированные с Keycloak не имеют права на самостоятельную смену пароля.

Для предоставления этой возможности На портале Keycloak под учетной записью администратора:

1. Настройте провайдер LDAP на использование защищенного протокола LDAP (LDAPs).
2. Установите режим **Writable**.



> При подключении к LDAP в режиме **Writable** убедитесь, что при настройке провайдера указан пользователь, имеющий достаточные права для изменения параметров учетных записей (пароли, атрибуты) пользователей в LDAP.

3. Сохраните изменения.

Для самостоятельного изменения пароля пользователь может воспользоваться инструкцией выше

База знаний zVirt

- ▸ Жизненный цикл
- ▸ Релизы и обновления
- ▸ Общие инструкции
- ▸ Автоматизация
- ▸ Безопасность
- ▸ Виртуальные машины
- ▸ Виртуальные GPU
- ▸ Гипервизоры
- ▸ Keycloak
- ▸ Менеджер управления
- ▸ Мониторинг
- ▸ Пользователи и группы
- ▸ Сертификаты

▶ Сети

▶ Утилиты

▶ Хранилище

▶ SDS