Общество с ограниченной ответственностью «СКАЛА-Р»

(ООО «СКАЛА-Р»)

Машина хранения данных

СКАЛА-Р МХД.О

(РМБГ.466535.002-565)

Руководство администратора

Приложение 3. Инструструкция по настройке KeyCloak

РМБГ.466535.002-565РА

Страниц 17

Москва 2026 г.

Содержание

Термины и определения

Термин, сокращение	Определение
Amazon S3	(англ. Amazon Simple Storage Service) Облачная система хранения в составе Amazon Web Services, организованная по объектному принципу
Authentication / Аутентификация	Идентификация и проверка пользователя
Authorization/ Авторизация	Предоставление доступа пользователю
Clients	Клиенты (приложения), которые могут обращаться к Keycloak для аутентификации пользователя. Чаще всего клиентами являются приложения и службы, которые используют Keycloak для обеспечения единого входа в систему
Client ID	Уникальный анонимный идентификатор, который система аналитики присваивает каждому клиенту сервиса
FQDN	Группа полных доменных имен
http	(англ. HyperText Transfer Protocol) Протокол, который используется для передачи данных в интернете
https	(англ. Hyper Text Transfer Protocol Secure) Расширение протокола HTTP для поддержки шифрования в целях повышения безопасности
IP-адрес	Уникальный адрес, который присваивается устройствам при подключении к интернету или локальной сети
Keycloak	Программный продукт с открытым исходным кодом для управления идентификацией и доступом
Realm	Пространство для управления пользователями, приложениями, ролями и группами Пользователь принадлежит к конкретному realm. Realm'ы изолированы друг от друга
Roles	Роли определяют тип/категорию пользователя. Читатель, писатель — типичные роли. Обычно, приложения назначают доступ и разрешения конкретным ролям, а не отдельным пользователям
S3	(англ. Simple Storage Service) Сервис хранения цифровых данных большого объема. Работает по одноименному протоколу S3 и основан на API, разработанном в Amazon Web Services (AWS)

Термин, сокращение	Определение
URL	(англ. Uniform Resource Locator) Единообразный указатель местонахождения ресурса — адрес ресурса в сети Интернет
Users	Пользователи, которые могут войти в вашу систему. Им можно назначить членство в группе и/или определенные роли
МХД.О	Машина хранения данных
ОС	Операционная система
ПО	Программное обеспечение

1 Первоначальная настройка Keycloak

Для первоначальной настройки Keycloak необходимо:

а) открыть браузер и перейти страницу http://<IP-адрес сервера keycloak>:<port>;

б) выбрать раздел Administration Console;

в) после выбора раздела будет совершен переход на страницу авторизации (рисунок 1);

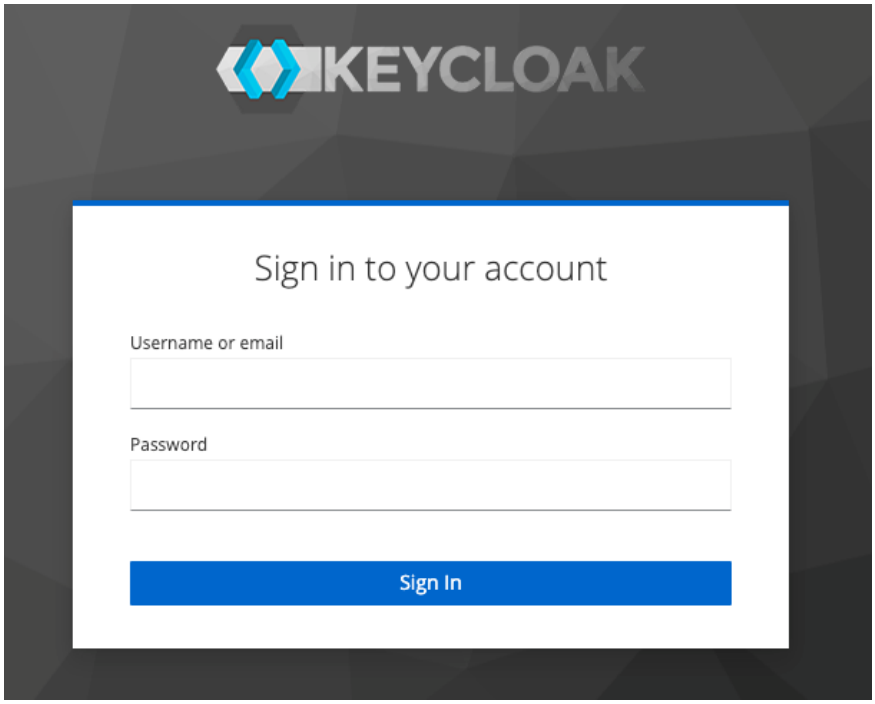

Рисунок 1 - Страница авторизации Keycloak

г) ввести в ссответствующие строки логин и пароль;

Примечание – По умолчанию логин – admin, пароль – admin

д) после ввода логина и пароля откроется административная консоль (рисунок 2);

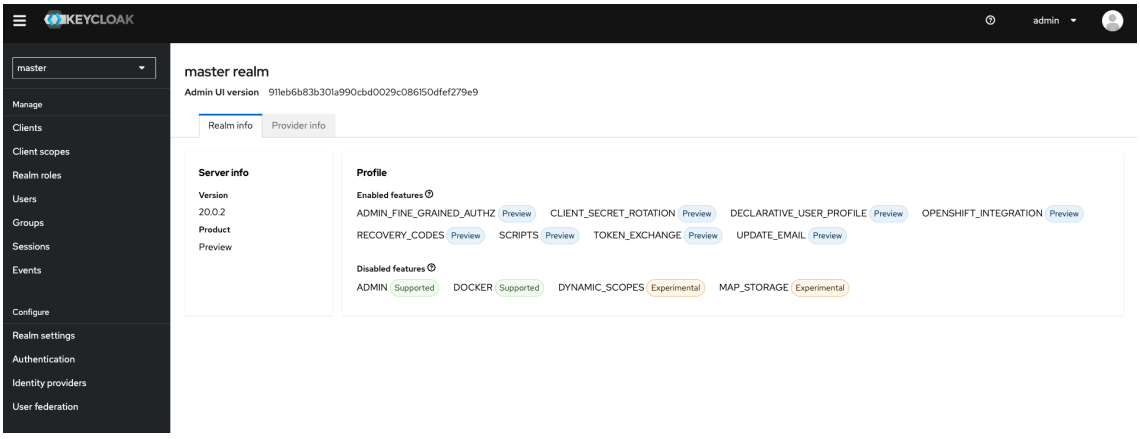

Рисунок 2 - Административная консоль

2 Создание проекта (realm)

2.1 Общие положения

Realm - область управления, которая содержит совокупность всех данных: пользователей, учетные данные, роли и группы; необходимых для аутентификации и авторизации пользователей данного realm. Каждый realm изолирован от других realm.

Для одного комплекса МХД.О достаточно одного realm.

Realm «master» можно использовать только для создания других realms.

ВНИМАНИЕ! Не редактируйте и не пытайтесь удалить данный realm.

2.2 Процедура создания проекта

Для создания нового realm необходимо:

а) нажать на список с выбором текущего realm (сразу после старта сервиса будет выбран единственный realm «master»);

б) в открывшемся меню нажать кнопку «Create Realm» (рисунок 3);

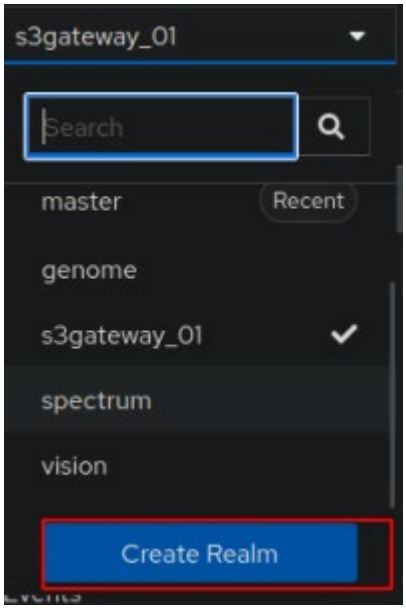

Рисунок 3 - Создание нового realm

в) в параметрах при создании нового realm достаточно указать только его имя. Имя может быть произвольным, здесь и в дальнейшем будет использовано имя realm «`s3gateway`» ();

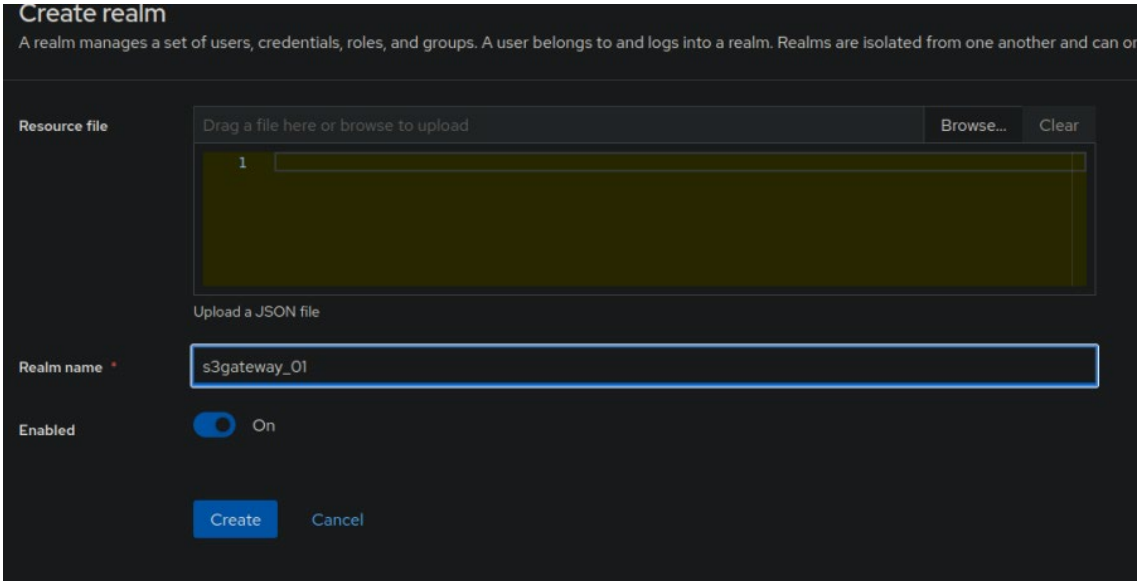

Рисунок 4 - Параметры создаваемого realm

г) нажать кнопку «**Create**». После создания, переход в новый realm выполниться автоматически, дальнейшие настройки выполняются в нем.

3 Создание клиента

3.1 Общие положения

Client - объект, который содержит совокупность параметров, необходимых для связи с определенным приложением.

3.2 Процедура создания клиента

Для настройки взаимодействия сервиса Скала^р S3 Шлюза с Keycloak необходимо:

а) создать одного клиента:

– Client type: `openid-connect;`

– Client ID: `<ИМЯ КЛИЕНТА>;`

– S3 шлюз: s3gtw-user;

б) после ввода параметров нажать `Next`;

в) в поле «Client authentication» установить ползунок в соответствии с рисунком ниже (рисунок 5);

г) в поле «Authorization» установить ползунок в соответствии с рисунком ниже (рисунок 5);

д) установить Чекбокс в поле «Standard Flow»;

е) установить Чекбокс в поле «Direct Access Grants»;

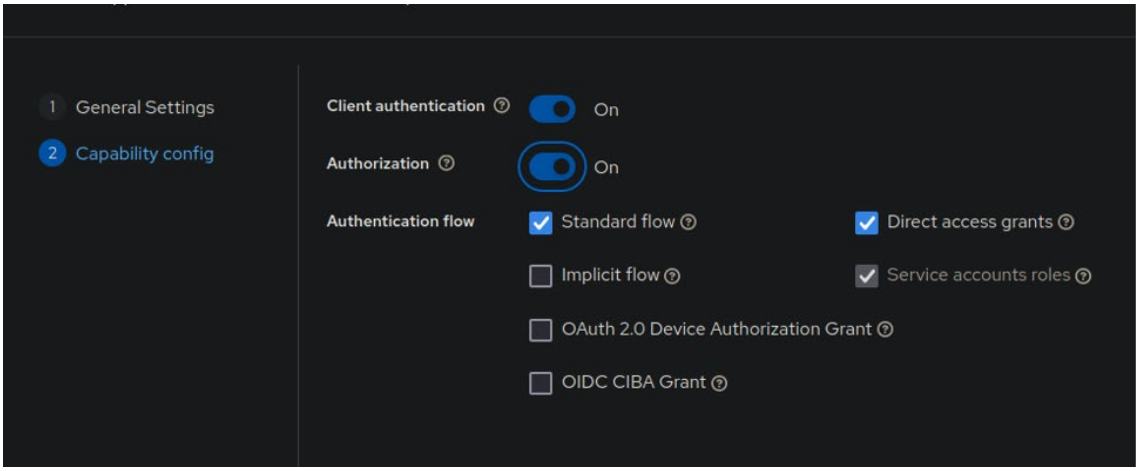

Рисунок 5 - Создание клиента

ж) после ввода параметров нажать `Save.`

4 Параметры клиента

После создания клиента откроется страница дополнительных настроек, приведенная на рисунке ниже (рисунок 6).

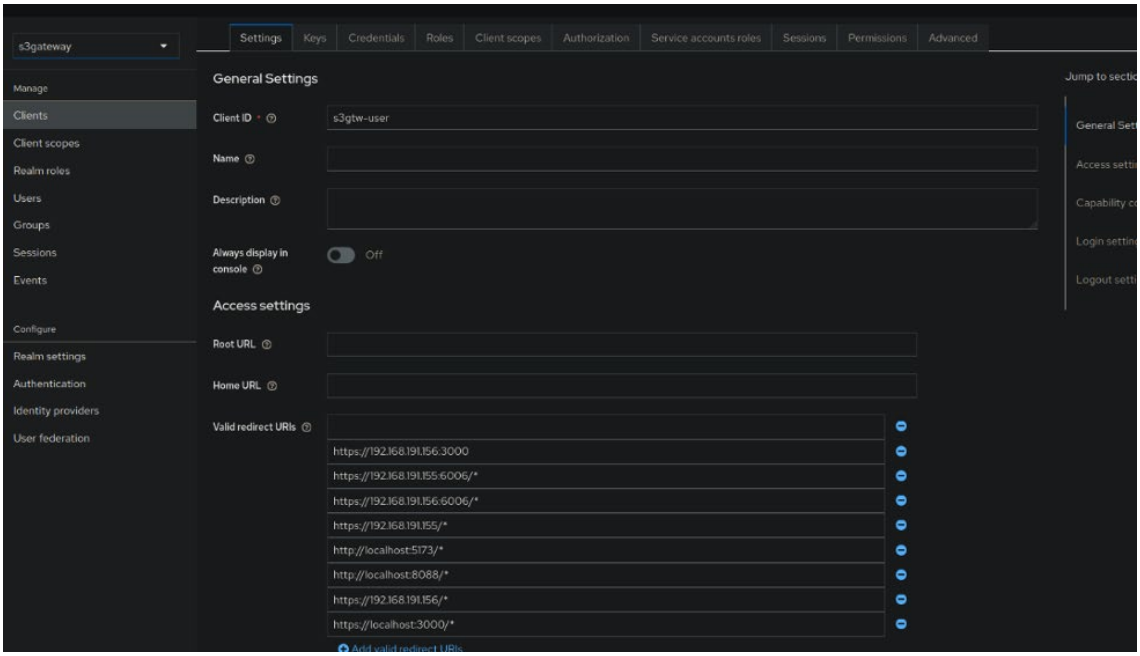

Рисунок 6 - Страница дополнительных настроек

Во вкладке «Settings» нужно задать параметр «Valid redirect URIs», где необходимо перечислить все URL, где установлено ПО Скала^р Спектр.S3 с Keycloak.

а) Root URL: <app_url> (может быть пустым);

б) Home URL (Base URL в ранних версиях): <app_url>(может быть пустым);

в) Valid Redirect URIs: список разрешенных URL шлюза включая информацию о портах;

– S3 шлюз: (пример,https://192.168.191.156:3000)

г) Web Origins: <app_url>(может быть пустым);

д) Admin URL: <app_url>(может быть пустым), где <app_url>, это основной URL приложения.

При доступности приложений с нескольких `<app_url>` (по IP, по домену) необходимо указать все допустимые варианты для `Valid redirect URIs` и `Web Origins`.

Прочие параметры конфигурации можно оставить со значениями по умолчанию.

После ввода параметров нажать `Save`.

5 Добавление пользователя

Для добавления пользователя необходимо:

а) перейти в меню Users;

б) нажать на кнопку Add user и заполнить Username (рисунок 7);

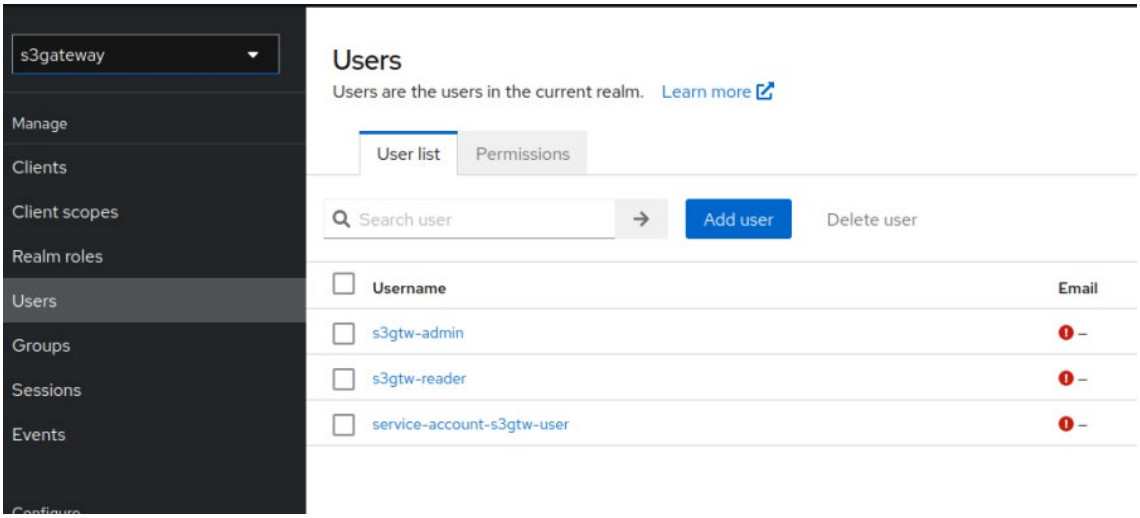

Рисунок 7 - Добавление пользователя

в) в поле «Email verified» установить ползунок в соответствии с рисунком ниже (рисунок 8);

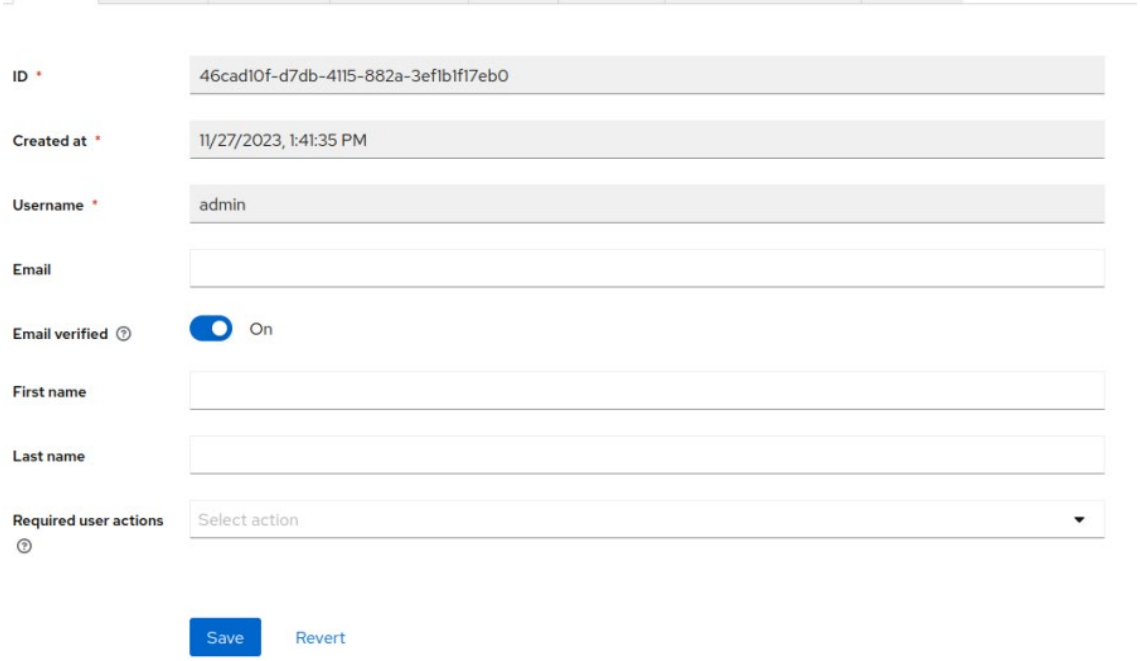

Рисунок 8 - Дополнительные настройки

г) перезайти на страницу пользователя и убираем Required user actions (рисунок 9);

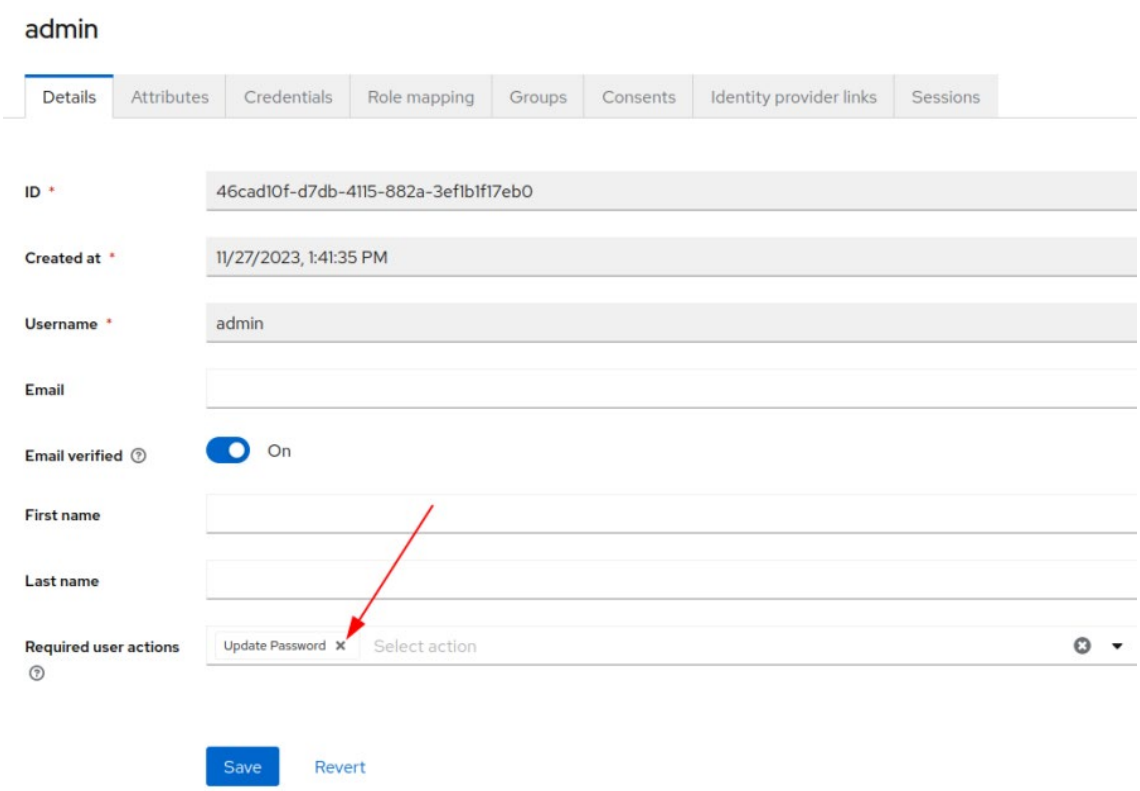

Рисунок 9 - Исключение Required user actions

д) нажать кнопку «Save».

6 Добавление ролей

Для создания роли, необходимо:

а) во вкладке «Clients» «выбрать s3gtw-user» (рисунок 10);

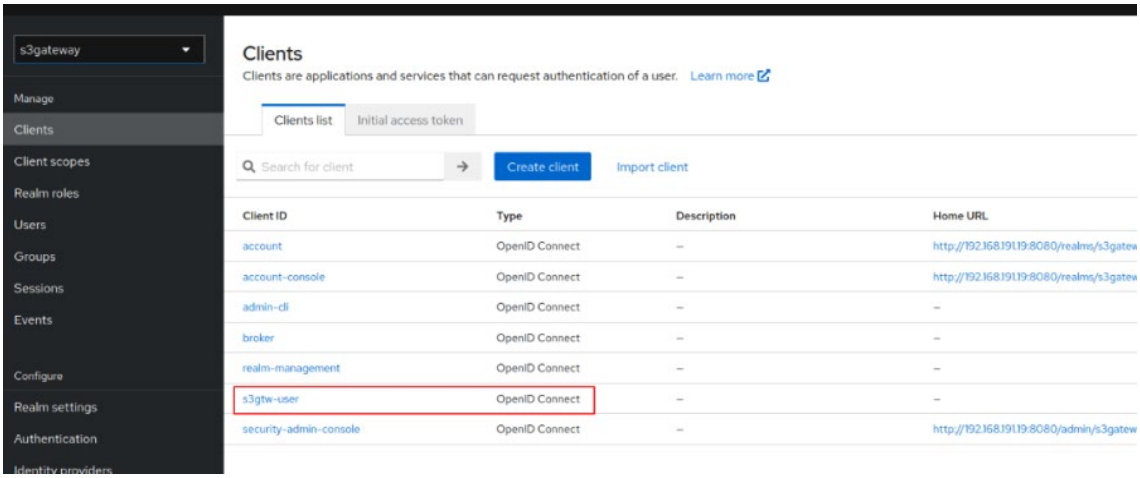

Рисунок 10 - Выбор клиента

б) перейти во вкладку «Roles» и нажать на кнопку «Create role» (рисунок 11);

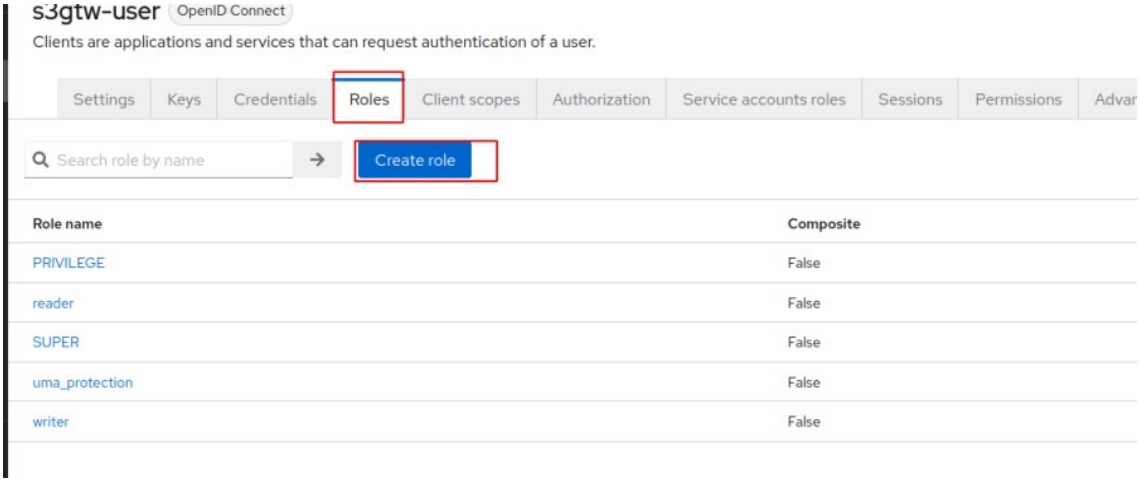

Рисунок 11 - Создание новой роли

Примечание - Названия ролей описаны в разделе 12.14 Руководства Администратора.

в) выбрать название роли и нажать «Save» (рисунок 12);

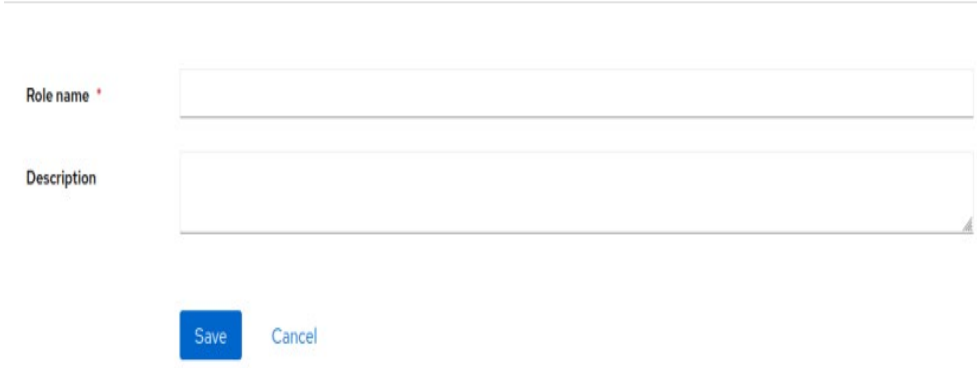

Рисунок 12 - Выбор названия роли

г) для того, чтобы привязать роль к юзеру, необходимо перейти в «Users» и выбрать нужного пользователя (рисунок 13);

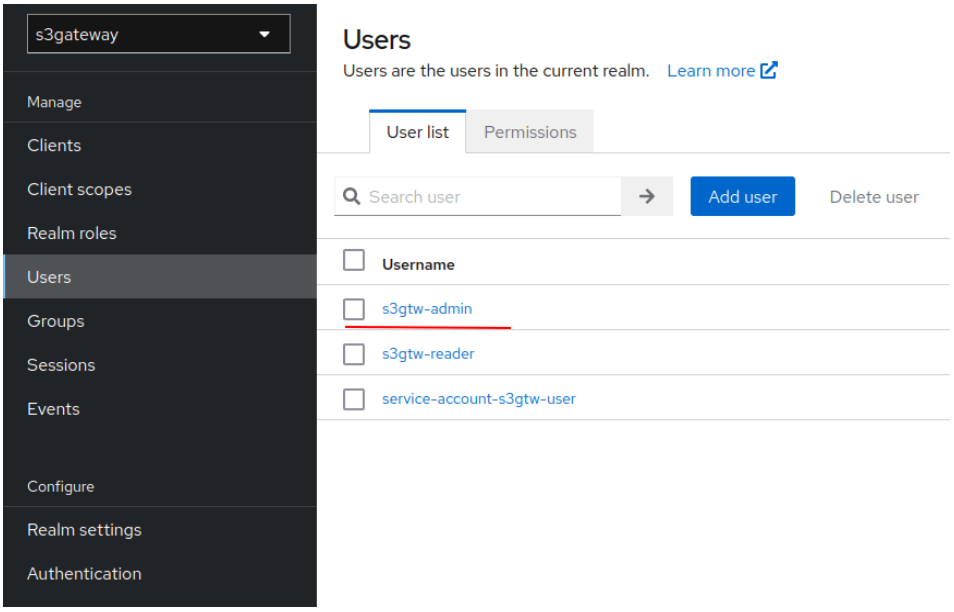

Рисунок 13 - Выбор нужного пользователя

д) переити во вкладку «Role mapping» и нажать «Assign Role» (рисунок 14);

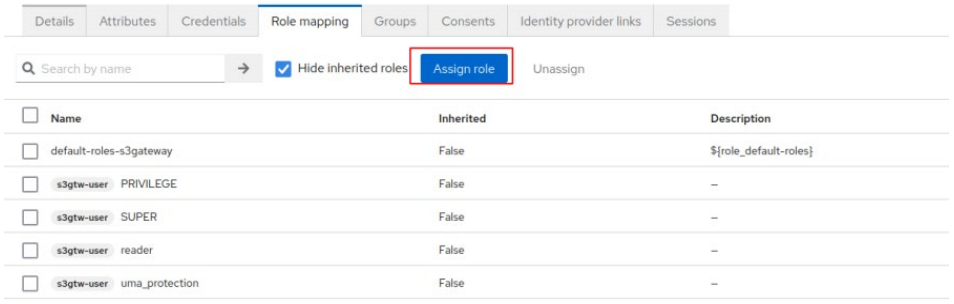

Рисунок 14 - Назначение роли

е) установить фильтрацию по клиентам, найти в поиске необходимую роль и выбрать ее (рисунок 15);

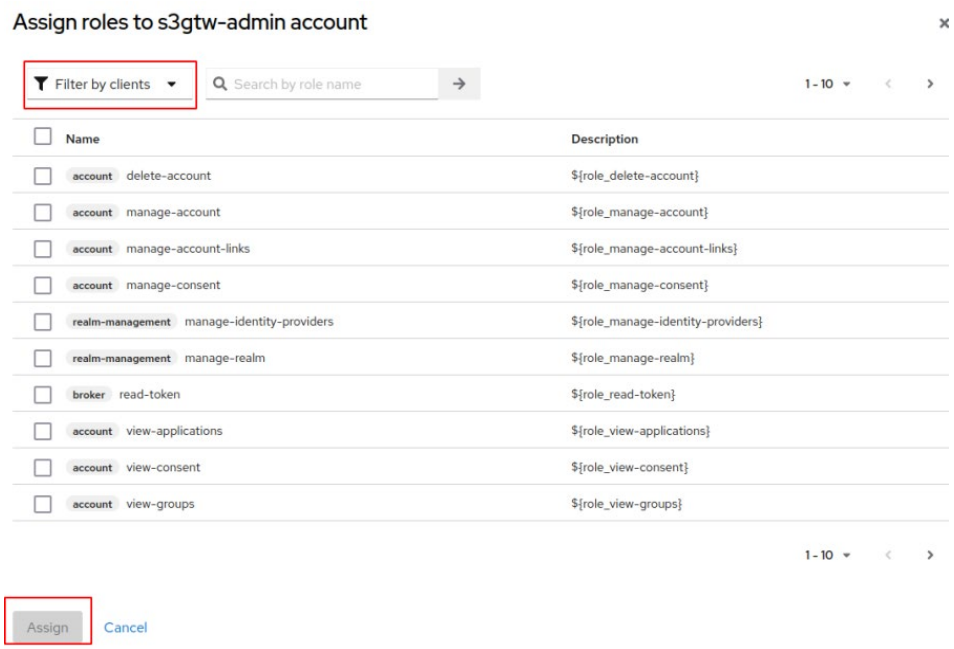

Рисунок 15 - Выбор необходимой роли

7 Смена пароля

Для смены пароля необходимо:

а) перейти на страницу юзера, во вкладке Credentials (рисунок 16).

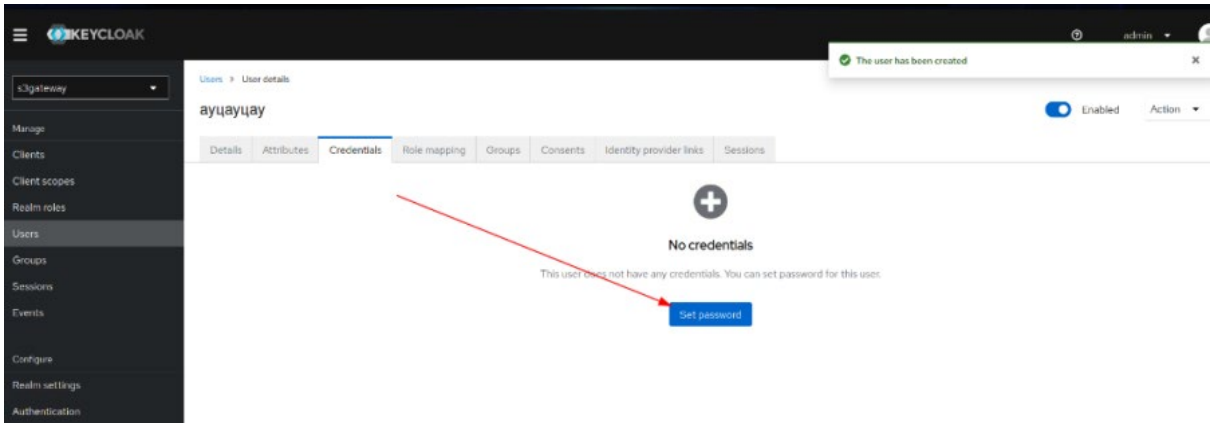

Рисунок 16 - Смена пароля

б) перейти во вкладку «Details» и убрать «Required user actions:».

8 Интеграция ПО Спектр.S3 с KeyCloak

Интеграция настраивается через конфигурационный файл:

/opt/skala-r/s3gateway/s3gateway.config.json

Используется ключ:

```
"iam_settings": {
"client_id": "",
"client_secret": "",
"realm": "",
"url": "",
"use_resource_role_mappings": true,
"skip_verify_ssl": true
},
```

где,

а) ключ "client_id" – ID приложения, зарегистрированного в проекте;

б) ключ "client_secret" – Пароль передаваемый администратором KeyCloak;

в) ключ "realm" – имя проекта в KeyCloak;

г) ключ "url" – url ссылка на KeyCloak;

д) ключ "use_resource_role_mappings": true – служебное, изменению не подлежит;

е) ключ "skip_verify_ssl" – определяет проверку сертификата сервера, если этот ключ установить в true, то при подключении к keycloak через https не будет проверяться сертификат сервера. Актуально для подключения к серверу keycloak по https с самоподписным сертификатом. При подключении к keycloak по http эта настройка не играет роли. Использование IP или FQDN от этой настройки не зависит.

Лист регистрации изменений

Изм.	Номера листов (страниц)				Всего листов (страниц) в док.	№ разреш. документа	Подпись	Дата	Примечание
	Измененных	Замененных	Новых	Аннулированных					