

Инструкция к новому СУРу

Описание системы

СУР — система управления ролями доступа к объектам. Здесь настраиваются разрешения, роли и наборы значений для датасетов.

СУР представляет собой систему, реализующую функционал RLS.

RLS (Row-level security — безопасность на уровне строк) позволяет ограничить доступ к данным для пользователей в рамках одного набора данных.

СУР позволяет организовать следующие виды доступов:

1. Полный доступ.
2. Ограниченный доступ по набору значений.
3. Ограниченный доступ по ключевому слову. Для работы СУРа на вашем стенде

необходимы:

1. коннектор, работающий с СУРом
2. СУР
3. БД authority и БД configuration, соответствующие бэки.
4. Необходимо выдать роли для просмотра и редактирования таблиц в админ. панели для администратора (чтобы он настраивал доступ к наборам данных).

Что вам необходимо сделать в редакторе для использования СУРа:

1. добавить коннектор с СУРом в редактор
2. добавить внутрь коннектора с СУРом подключения, к таблицам в которых вы хотите выдавать доступы
3. создать приложение
4. добавить авторизацию и авторизоваться
5. добавить провайдеры данных:
 - a. выбрать коннектор к СУРу
 - b. выбрать подключение, где хранятся датасеты, к которым нужно

выдать датасеты.

По умолчанию, в приложении, использующее подключение через СУР, доступ к датасету запрещён. Чтобы это исправить, необходимо выдать полный или ограниченный доступ к датасету.

Полный доступ от ограниченного отличается тем, что при полном доступе пользователь видит все записи датасета, а при ограниченном — только часть.

Схему настройки доступов можно найти в соответствующем документе с план-схемой настройки СУРа.

Ограниченный доступ можно настроить двумя способами:

1. По набору значений.
2. По ключевому слову.

Термины

Набор данных— это таблица(датасет или вью), которую вы хотите разграничить.

Объект — это надстройка над набором данных, на которую могут быть наложены ограничения.

Объекты ограничения нужны за тем, чтобы поддерживать несколько способов обращения к датасету. К одному датасету можно настроить два доступа: полный и ограниченный. Для этого необходимо создать два объекта к этому датасету:

1. объект с кодом «название_датасета/all» - полный доступ
2. объект с кодом «название_датасета/название_поля» - ограниченный доступ, где название_поля — поле, по которому будет резаться датасет

Атрибут — поле, по которому будет фильтроваться датасет. Для одного объекта можно создать несколько атрибутов.

Ограничение — связка объекта и атрибута. Если для объекта существует несколько атрибутов, то их все нужно связать с их объектами.

Разрешение — полномочие, связывающее роль и объект.

Названия для ролей:

1. объект с кодом «название_датасета/all» - роль «название_датасета/all_role»
2. объект с кодом «название_датасета/название_поля» - роль «название_датасета/название_поля_role»

Примечание: если у вас есть много датасетов, к которым нужно выдавать однотипный доступ, то роль можно использовать одну и ту же, просто связывая её со всеми объектами для этих датасетов.

Набор значений — список значений, которыми будет фильтроваться датасет по определенному столбцу-атрибуту.

Набор значений можно заполнить:

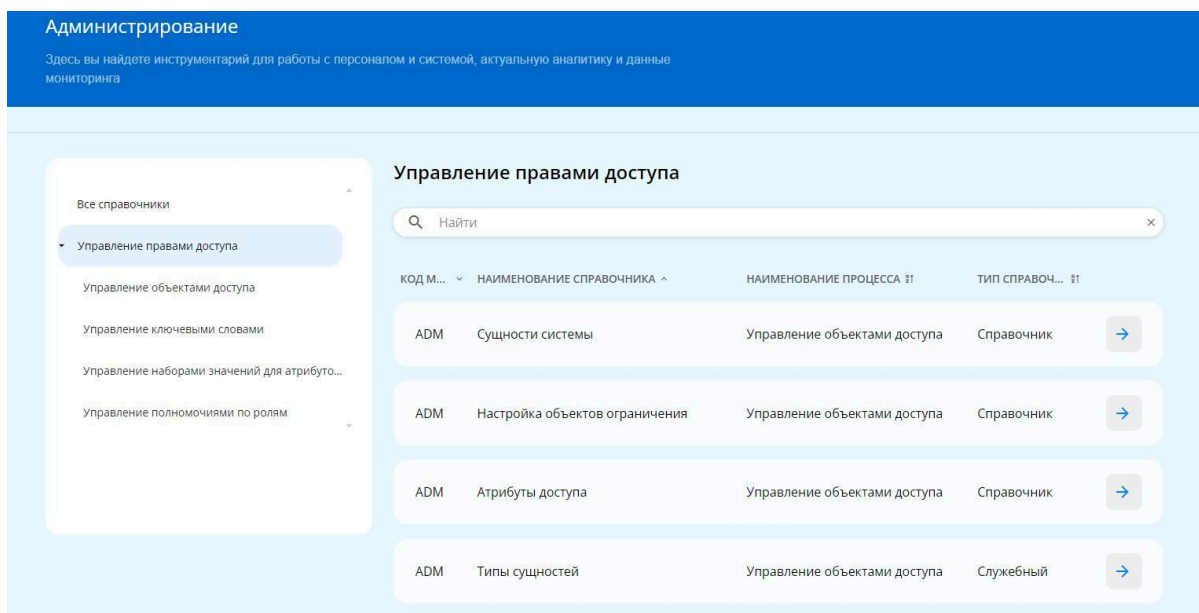
1. данными, не зависящими от пользователя — явно заданными значениями
2. данными, зависящими от пользователя — ключевыми словами

Ключевые слова — наборы ограничений, зависящие от пользователя.

В админ-панели мы будем использовать ключевые слова типа token. Это значит, что ключевое слово и его значение будет забираться из атрибутов пользователя Keycloak.

Знакомство с админ. панелью

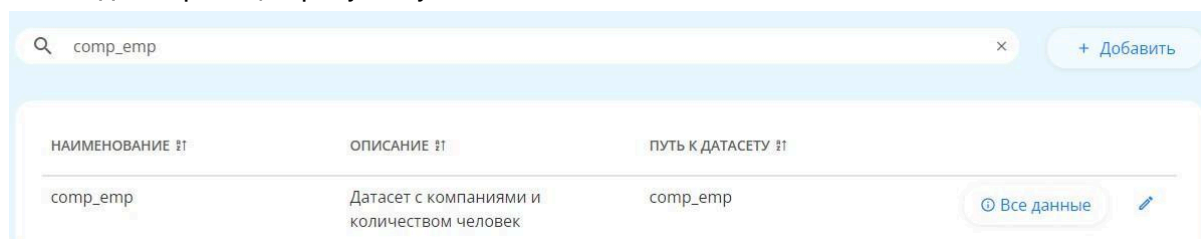
Админ. панель - приложение, позволяющее, помимо прочего, осуществлять настройки СУР.



Админ. панель - приложение, позволяющее, помимо прочего, осуществлять настройки СУР.

Для настройки СУР необходимо перейти в раздел “Администрирование” и слева в разделах выбрать “Управление правами доступа”. Справа отобразятся страницы, относящиеся к выбранному разделу. С помощью последовательного перехода по ним и осуществления действий, описанных в инструкциях, можно настроить СУР.

На каждой странице присутствует поиск.



Есть кнопка «+ Добавить запись», которая открывает окно для добавления новой записи. Есть кнопка редактирования в виде карандаша, которая позволяет редактировать записи и удалять их.

Изменение записей проводите с большим вниманием: изменять поля можно только те поля, которые не участвуют в связях с другими таблицами СУРА.

Например, изменить путь к датасету вы сможете, но изменить код объекта, если уже есть разрешение к этому объекту, не получится.

На странице так же есть кнопка «Все данные» для просмотра всех технических данных записи.

Примечание: при долгой паузе при работе с админ-панелью вы можете обнаружить, что новые записи не добавляются или данные в самой админ-панели пропали. Это может происходить из-за истекшей срока авторизации. В таком случае просто перезагрузите страницу с админ-панелью.

Полный доступ

Полный доступ обычно используется для проверки видимости сущности. Но так же этот доступ может использоваться в случае, когда у вас только один коннектор, работающий с СУРом. В таком случае данные в проекте/дашборде по умолчанию не видны. Это значит, что надо завести все датасеты в СУР.

Для настройки этого доступа необходимо:

1. Создать сущность.
2. Добавить ей объект и связать его с сущностью.
3. Создать разрешение для этого объекта.
4. Создать роль в Keycloak и добавить её нужному пользователю.

Например, нужно выдать полный доступ на датасет rev_exp с доходами и расходами:

list	type	amount
Торговая точка "Мария"	Доход	96920
Торговая точка "Люксор"	Доход	73688
Сдача помещения в аренду	Доход	22000
Сдача авто Nissan в аренду	Доход	12000
Заработная плата	Доход	56000
Аренда торговой площади в ТЦ Нива	Расход	18000
Аренда торговой площади в ТЦ Мир	Расход	13000
Связь (телефон, интернет)	Расход	1000
Платежи по кредиту	Расход	10000
Затраты на доставку товаров	Расход	2000
Оплата ЖКХ	Расход	5000
Заработная плата продавцам	Расход	45328

Сущности системы

Заполнение СУРа начинаем со страницы "Сущности системы". Нажимаем кнопку «+ Добавить запись», после чего откроется окно для ввода данных.

Добавить
✕

ПОКАЗАТЕЛЬ	ДАННЫЕ
ID	<input type="text"/>
Название *	<input type="text"/>
Тип *	- ▼
Системность *	<input type="checkbox"/> True/False
Описание *	<input type="text"/>
Название бизнес-объекта *	<input type="text"/>
Дата закрытия	<input type="text"/>
ID пользователя Keycloak, создавшего запись	<input type="text"/>

В "Названии" указываем название датасета — «insight.rev_exp», тк создаем сущность для виджетов версии 2.1.

Важно!

Если датасет будет использоваться в виджетах версии 2.1 (SDK), то в названии необходимо указать путь к датасету в виде:

- 1) Если датасет на Dremio - "БД.схема.путь до таблицы, включая папки".
- 2) Если датасет на PostgreSQL - "БД.путь до таблицы, включая папки".

Если датасет будет использоваться в виджетах с idp (или будет открываться в разделе редактора "Датасеты" или "Библиотека"), то в названии необходимо указать путь к датасету в виде "код подключения.схема.таблица".

В выпадающем списке "Тип" указываем «Объект данных БД — view или table».

«Бизнес-объект» — это дополнительный функционал на будущее, его не надо использовать.

В поле "Системность" флаг ставить не нужно, поле может быть отключено, так и должно быть.

"Описание" в этом пункте, как и в других пунктах далее, лучше заполнять подробностями, иначе будет тяжело ориентироваться.

“Название бизнес-объекта” указываем по аналогии с пунктом “Название”, **если будем просматривать сущность через IDP. Если объект данных будет просматриваться через виджеты версии 2.1**, то в “Название бизнес-объекта” следует вставить только название датасета или выю, которые заносим в систему.
Вводим все параметры и нажимаем кнопку «Сохранить».

Настройка объектов ограничения

Переходим на вкладку “Настройка объектов ограничения” и нажимаем кнопку “+ Добавить запись”.

Добавить

ПОКАЗАТЕЛЬ	ДАННЫЕ
ID	<input type="text"/>
Код *	<input type="text"/>
Название *	<input type="text"/>
Название сущности *	<div>-</div>
Системность	<input type="checkbox"/> True/False
Описание *	<div><input type="text"/></div>
Дата закрытия	<div></div>
ID пользователя Keycloak, создавшего запись	<input type="text"/>

Код — системное поле, которое поддается жёсткому неймингу. Продублируем название сущности из п. “Сущности системы” и допишем нужный постфикс.

В качестве кода объекта указываем «rev_exp/all». Приписка /all означает, что это объект полного доступа.

В “Названии” продублируем название сущности из п. “Сущности системы”.

В выпадающем списке “Название сущности” выбираем датасет, к которому создаём объект — authority.rev_exp.

В “Описании” указываем, что это объект полного доступа к датасету «authority.rev_exp».

Вводим все параметры и нажимаем кнопку «Сохранить».

Полномочия и правила доступа

Переходим на вкладку "Полномочия и правила доступа" и нажимаем кнопку "+ Добавить запись".

Добавить

ПОКАЗАТЕЛЬ

ДАННЫЕ

ID

Роль *

Код объекта *

-

Включено *

☐ True/False

Разрешение на запись *

☐ True/False

Системность *

☐ True/False

Описание

Дата закрытия

ID пользователя Keycloak,

"Роль" — роль, которую в дальнейшем нужно будет прописать в Keycloak пользователю, которому необходимо предоставить доступ к датасету.

Указываем роль "rev_exp/all_role".

В выпадающем списке "Код объекта" указываем объект, к которому создаём роль, — «rev_exp/all».

В пункте "Включено" ставим параметр True (ставим галку).

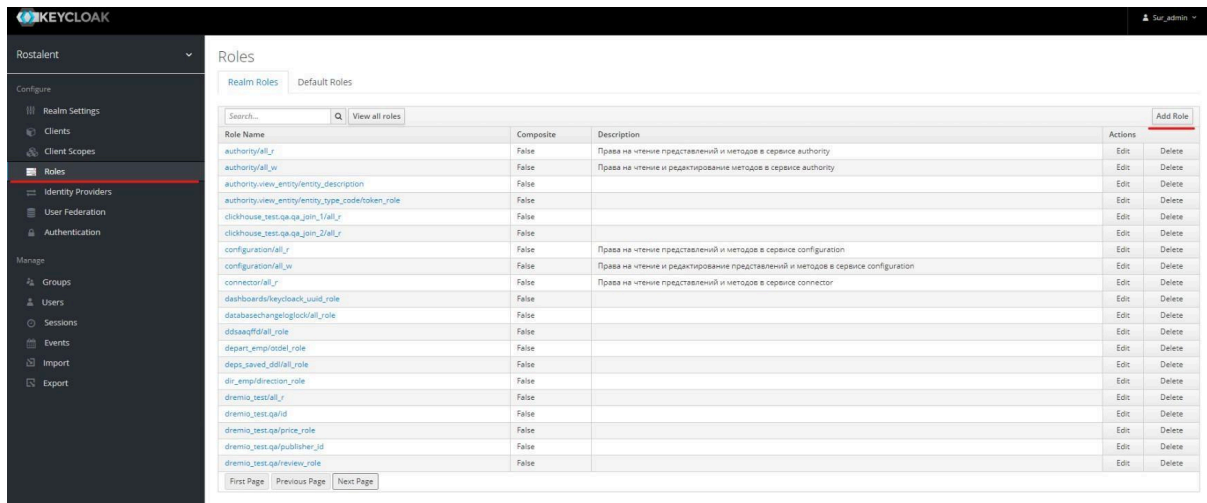
"Разрешение на запись" и "Системность" — это дополнительный функционал на будущее, их не надо использовать.

В Описании указываем, что выдаём разрешение на полный доступ к датасету «insight.rev_exp».

Вводим все параметры и нажимаем кнопку «Сохранить».

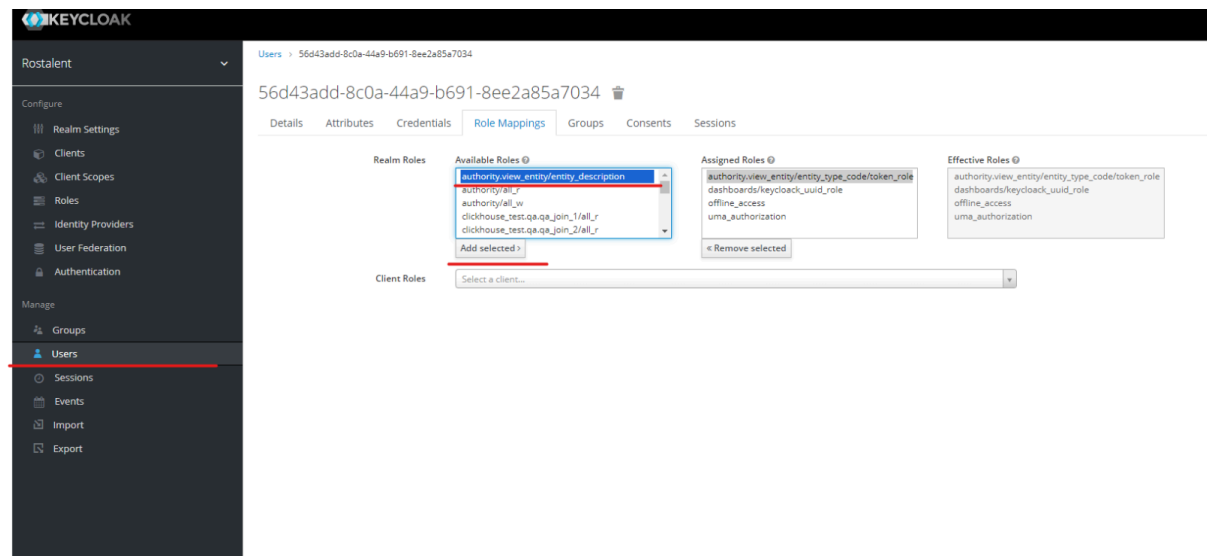
Keycloak

Пользователю необходимо перейти в Keycloak.



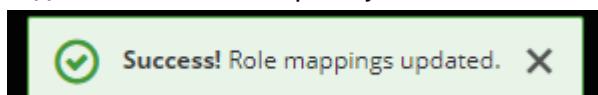
В разделе “Roles” в Keycloak, путём нажатия на «Add role», создаем роль с таким же названием, как в СУРБ в п. “Полномочия и правила доступа”. В нашем случае - “rev_exp/all_role”.

После этого кликаем на пункт «Users» и переходим к поиску нужного пользователя.



Кликаем на ID пользователя, переходим в его настройки и выбираем пункт «Role mappings».

Кликаем на роль «rev_exp/all_role», а дальше на «Add selected». После чего появится надпись «Success!» — роль успешно назначена пользователю.



Проверка полного доступа

Переходим к проверке доступа. Для этого откройте приложение, где используется этот датасет и авторизуйтесь.

В нашем примере мы сделали приложение и два провайдера данных: с СУРом и без СУРа.

Переходим в приложение и видим, что в таблицах слева и справа одни и те же строки.

Без СУРа			С СУРом		
list	type	amount	list	type	amount
Торговая точка "Мария"	Доход	96920	Торговая точка "Мария"	Доход	96920
Торговая точка "Люксор"	Доход	73688	Торговая точка "Люксор"	Доход	73688
Сдача помещения №1 в аренду	Доход	22000	Сдача помещения №1 в аренду	Доход	22000
Сдача авто Nissan в аренду	Доход	12000	Сдача авто Nissan в аренду	Доход	12000
Заработная плата	Доход	56000	Заработная плата	Доход	56000
Аренда торговой площади в ТЦ Нива	Расход	18000	Аренда торговой площади в ТЦ Нива	Расход	18000
Аренда торговой площади в ТЦ Мир	Расход	13000	Аренда торговой площади в ТЦ Мир	Расход	13000
Связь (телефон, интернет)	Расход	1000	Связь (телефон, интернет)	Расход	1000
Платежи по кредиту	Расход	10000	Платежи по кредиту	Расход	10000

Ограниченный доступ по набору значений

Такой доступ позволяет делиться с пользователем только частью данных, хранящихся в датасете. В качестве аналогии можно привести датасет, отфильтрованный по полю. Только в случае ограниченного доступа по набору значений значения фильтра указываются в админ. панели СУРа, а пользователь, для которого отфильтрованы данные, не знает о том, что он видит не весь датасет.

Для настройки этого доступа необходимо:

1. Нужно создать необходимый датасет или представление.
2. Нужно создать объект ограничения, то, как необходимо предоставлять доступ (ко всей таблице, по определенному полю).

3. Нужно создать атрибут доступа. Это поле, по которому будет разграничение. Также необходимо связать атрибут доступа и объект ограничения.
4. Необходимо создать набор значений (Наборы значений — это наборы для заполнения ими значениями). Нужно также привязать атрибут доступа к набору значений.
5. Необходимо создать конкретные значения для набора значений.
6. В этом разделе нужно создать роль, которую затем необходимо будет прописать пользователю в Keycloak. Прежде чем записать роль в Keycloak ее необходимо связать с набором значений и объектом ограничения.
7. В разделе Roles в Keycloak создаем роль с таким же названием, как в СУРе.
8. В разделе Users в Keycloak переходим к нужному пользователю, находим созданную роль и присваиваем пользователю.

Например, нужно выдать ограниченный доступ на датасет, который мы рассматривали в Полном доступе, — insight.rev_exp. Разграничивать будем по полю type со значением «Доход».

list	type	amount
Торговая точка "Мария"	Доход	96920
Торговая точка "Люксор"	Доход	73688
Сдача помещения в аренду	Доход	22000
Сдача авто Nissan в аренду	Доход	12000
Заработная плата	Доход	56000
Аренда торговой площади в ТЦ Нива	Расход	18000
Аренда торговой площади в ТЦ Мир	Расход	13000
Связь (телефон, интернет)	Расход	1000
Платежи по кредиту	Расход	10000
Затраты на доставку товаров	Расход	2000
Оплата ЖКХ	Расход	5000
Заработная плата продавцам	Расход	45328

Сущности системы

Так как мы уже создали сущность системы для датасета, создавать ее заново не нужно.

Настройка объектов ограничения

Переходим на вкладку "Настройка объектов ограничения" и нажимаем кнопку "+ Добавить запись".

ПОКАЗАТЕЛЬ	ДАННЫЕ
ID	<input type="text"/>
Код *	<input type="text"/>
Название *	<input type="text"/>
Название сущности *	<input type="text" value="-"/>
Системность	<input type="checkbox"/> True/False
Описание *	<div><div></div><div></div></div>
Дата закрытия	<input type="text"/>
ID пользователя Keycloak, создавшего запись	<input type="text"/>

Ограниченный доступ предполагает новый объект с другим кодом. В поле "Код" продублируем название сущности из п. "Сущности системы" и допишем нужный постфикс (поле, по которому будет происходить разрез данных через знак "/").

Изменять старые записи в админ-панели не рекомендуется, так как значения в системных полях не изменятся.

В коде указываем «rev_exp/type». Приписка /type означает, что это объект ограниченного доступа, type — поле, по которому будет разграничиваться датасет.

В "Названии" продублируем название сущности из п. "Сущности системы".

В выпадающем списке "Название сущности" выбираем датасет, к которому создаём объект — insight.rev_exp.

В Описании указываем, что это объект ограниченного доступа к датасету "insight.rev_exp".

Вводим все параметры и нажимаем кнопку «Сохранить».

Атрибуты доступа

Переходим на вкладку "Атрибуты доступа" и нажимаем кнопку "+ Добавить запись".

ПОКАЗАТЕЛЬ	ДАННЫЕ
ID	<input type="text"/>
Код *	<input type="text"/>
Название *	<input type="text"/>
Схема БД	<input type="text"/>
Наименование подразделения	<input type="text"/>
Системность	<input type="checkbox"/> True/False
Дата создания	<input type="text"/>
Дата закрытия	<input type="text"/>

В поле "Код" указываем «type». type — поле, по которому будет разграничиваться датасет. В поле "Название" указываем, что это разрез по полю type. Остальные поля — это дополнительный функционал на будущее, его не надо использовать.

Вводим все параметры и нажимаем кнопку «Сохранить».

Настройка объектов ограничения

Возвращаемся на страницу “Настройка объектов ограничения” для того, чтобы связать атрибут доступа и объект ограничения.

sur-admin-authority.public.view_entity/entity_id	sur-admin-authority.public.view_entity/entity_id	sur-admin-authority.public.view_entity	sur-admin-authority.public.view_entity	1	Все данные
<input type="text" value="Найти"/>					+ Добавить запись
НАЗВАНИЕ	КОД АТТРИБУТА	НАЗВАНИЕ АТТРИБУТА	СИСТЕМНОСТЬ АТТРИБУТА	СИСТЕМНОСТЬ	
Ограничение по полю entity_id	entity_id	Разрез по полю entity_id	false	false	Все данные

Для этого необходимо раскрыть созданный объект ограничения, нажав на стрелку справа в строке с объектом. Далее нажать на кнопку “+ Добавить запись”.

Добавить

ПОКАЗАТЕЛЬ	ДАННЫЕ
ID	<input type="text"/>
Название ограничения объекта *	<input type="text"/>
ID атрибута *	<input type="text" value="-"/>
Системность *	<input type="checkbox"/> True/False
Код объекта ограничений *	<input type="text" value="sur-admin-authority.public.view_entity/entity_id"/>
Дата закрытия	<input type="text"/>
ID пользователя Keycloak, создавшего запись	<input type="text"/>
Дата создания	<input type="text"/>

В поле “Название ограничения объекта” пишем по какому полю хотим настроить ограничение. В нашем случае запишем “Ограничение по полю type”.

В поле “ID Атрибута” выберем название атрибута - “Разрез по полю type”. Остальные поля заполнять не нужно.

Вводим все параметры и нажимаем кнопку «Сохранить».

Наборы значений

Переходим на страницу "Наборы значений" и нажимаем кнопку "+ Добавить запись".

Добавить

ПОКАЗАТЕЛЬ	ДАННЫЕ
ID	<div></div>
Код *	<div></div>
Название *	<div></div>
Доступ к null *	<div><input type="checkbox"/> True/False</div>
Системность *	<div><input type="checkbox"/> True/False</div>
Описание *	<div><div></div><div></div></div>
Дата закрытия	<div><div></div><div></div></div>
ID пользователя Keycloak, создавшего запись	<div></div>

Наборы значений — это наборы для заполнения ими значениями, а в нашем случае это место, куда мы положим наше значение "Доход".

В поле "Код" указываем поле, по которому будет осуществляться ограничение с постфиксом "_valueset". В нашем случае получится "type_valueset". type — поле, по которому будет разграничиваться датасет.

В поле "Название" дублируем "Код".

Чекбокс "Доступ к null" при включении позволяет пользователю видеть не только поля в датасете, значение атрибута в которых не только соответствует значению набору, но и является null.

В поле "Описание" желательно написать: "набор значений по полю ... сущности ...". В нашем случае напишем - "набор значений по полю type сущности "insight.rev_exp"

Остальные поля — это дополнительный функционал на будущее, его не надо использовать.

Вводим все параметры и нажимаем кнопку «Сохранить».

После создания набора значений необходимо привязать к нему атрибут. Для этого необходимо раскрыть созданный набор значений, нажав на стрелку справа в строке с набором. Далее нажать на кнопку “+ Добавить запись”.

Добавить

ПОКАЗАТЕЛЬ	ДАННЫЕ
ID	<div></div>
ID атрибута *	<div>-</div>
ID набора значений *	<div></div>
Системность *	<div><input type="checkbox"/> True/False</div>
Дата закрытия	<div></div>
ID пользователя Keycloak, создавшего запись	<div></div>
Дата создания	<div></div>
ID пользователя Keycloak, обновившего запись	<div></div>

В поле “ID Атрибута” выберем название атрибута – “Разрез по полю type”.

В поле “ID набора значений” выберем название набора значений – “type_valueset”.

Остальные поля заполнять не нужно.

Вводим все параметры и нажимаем кнопку «Сохранить».

Значения доступа

На страницу “Значения доступа” можно перейти через страницу “Наборы значений” путем нажатия на многоточие на строке с информацией о созданном наборе значений. Затем необходимо нажать кнопку “Открыть значения набора”.

Администрирование > Администрирование

Подсказка для пользователя

Наборы значений

Управление наборами значений для атрибутов доступа

Найти

Сбросить все

+ Добавить запись

КОД #1	НАЗВАНИЕ #1	ДОСТУП К NULL #1	СИСТЕМНОСТЬ #1	ОПИСАНИЕ #1
b84214d9-405a-4f17-ba8b-b714dd8f5dcp.public.object/code	b84214d9-405a-4f17-ba8b-b714dd8f5dcp.public.object/code	false	false	Набор значений для ограничения доступа к b84214d9-405a-4f17-ba8b-b714dd8f5dcp.public.object no code
b84214d9-405a-4f17-ba8b-b714dd8f5dcp.public.object/entity_id	b84214d9-405a-4f17-ba8b-b714dd8f5dcp.public.object/entity_id	false	false	Набор значений для ограничения доступа к b84214d9-405a-4f17-ba8b-b714dd8f5dcp.public.object no entity_id
b84214d9-405a-4f17-ba8b-b714dd8f5dcp.public.object/id	b84214d9-405a-4f17-ba8b-b714dd8f5dcp.public.object/id	false	false	Набор для ограничения доступа к b84214d9-405a-4f17-ba8b-b714dd8f5dcp.public.object no полю id

На этой странице набор заполняется конкретными значениями.

Добавить



ПОКАЗАТЕЛЬ	ДАННЫЕ
ID	<input type="text"/>
Значение *	<input type="text"/>
Название набора значений *	<input type="text" value="-"/>
Системность *	<input type="checkbox"/> True/False
Дата закрытия	<input type="text"/>
ID пользователя Keycloak, создавшего запись	<input type="text"/>
Дата создания	<input type="text"/>
ID пользователя Keycloak, обновившего запись	<input type="text"/>

В поле “Значение” указываем «Доход». В этом поле необходимо указывать конкретное значение из поля датасета, по которому происходит разрез. Пользователь, которому ограничат доступ к датасету, будет видеть только те поля, в которых значение поля соответствует введенному.

В выпадающем списке “Название набора значений” выбираем название набора значений для атрибута type.

Вводим все параметры и нажимаем кнопку «Сохранить».

Полномочия и правила доступа

Переходим на вкладку “Полномочия и правила доступа” и нажимаем кнопку “+ Добавить запись”.

Добавить
✕

ПОКАЗАТЕЛЬ	ДАННЫЕ
ID	<input type="text"/>
Роль *	<input type="text"/>
Код объекта *	- ▼
Включено *	<input type="checkbox"/> True/False
Разрешение на запись *	<input type="checkbox"/> True/False
Системность *	<input type="checkbox"/> True/False
Описание	<input type="text"/> ✎
Дата закрытия	<input type="text"/> 📅
ID пользователя Keycloak,	<input type="text"/> ▼

“Роль” — роль, которую в дальнейшем нужно будет прописать в Keycloak пользователю, которому необходимо предоставить доступ к датасету.

Указываем роль “rev_exp/type_role”.

В выпадающем списке “Код объекта” указываем объект, к которому создаём роль, — «rev_exp/type».

В пункте “Включено” ставим параметр True (ставим галку).

“Разрешение на запись” и “Системность” — это дополнительный функционал на будущее, их не надо использовать.

В Описании указываем, что выдаём разрешение на ограниченный доступ по набору значений к датасету «insight.rev_exp».

Вводим все параметры и нажимаем кнопку «Сохранить».

После создания роли ее необходимо связать с набором значений и объектом ограничения. Для этого необходимо раскрыть созданную роль, нажав на стрелку справа в строке с ролью. Далее нажать на кнопку “+ Добавить запись”.

Добавить

×

ПОКАЗАТЕЛЬ	ДАННЫЕ
ID	<input type="text"/>
Полномочие *	<input type="text" value="qa_join_1/genre_role"/>
Ограничение объекта *	<input type="text" value="-"/>
Набор значений *	<input type="text" value="-"/>
Системность *	<input type="checkbox"/> True/False
Дата закрытия	<input type="text"/>
ID пользователя Keycloak, создавшего запись	<input type="text"/>
Дата создания	<input type="text"/>
ID пользователя Keycloak	<input type="text"/>

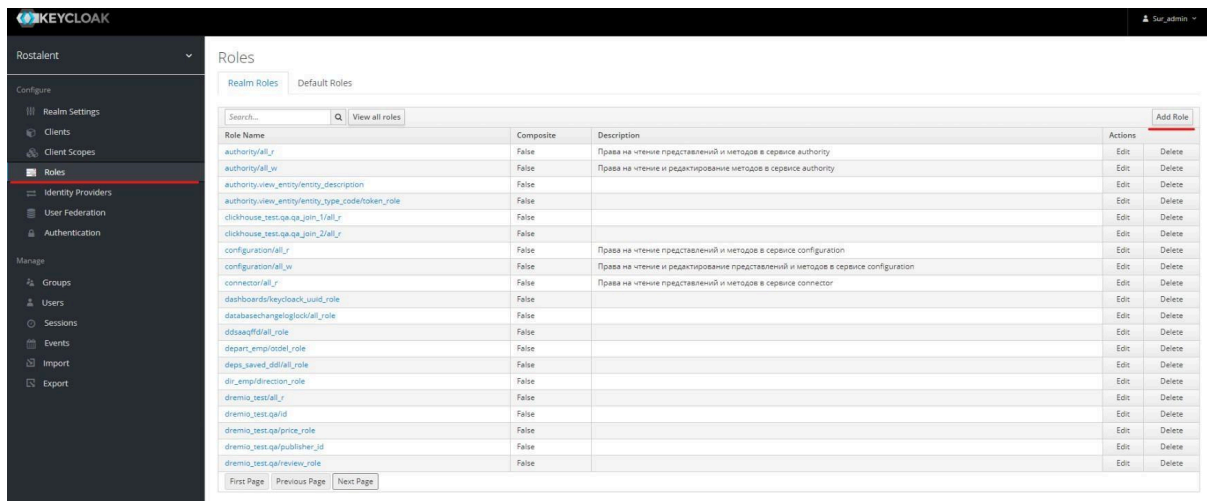
В поле “Ограничение объекта” выберем название соответствующее значению поля “Название ограничения объекта” – “Ограничение по полю type”.

В поле “Набор значений” выберем название набора значений – “type_valueset”. Остальные поля заполнять не нужно.

Вводим все параметры и нажимаем кнопку «Сохранить».

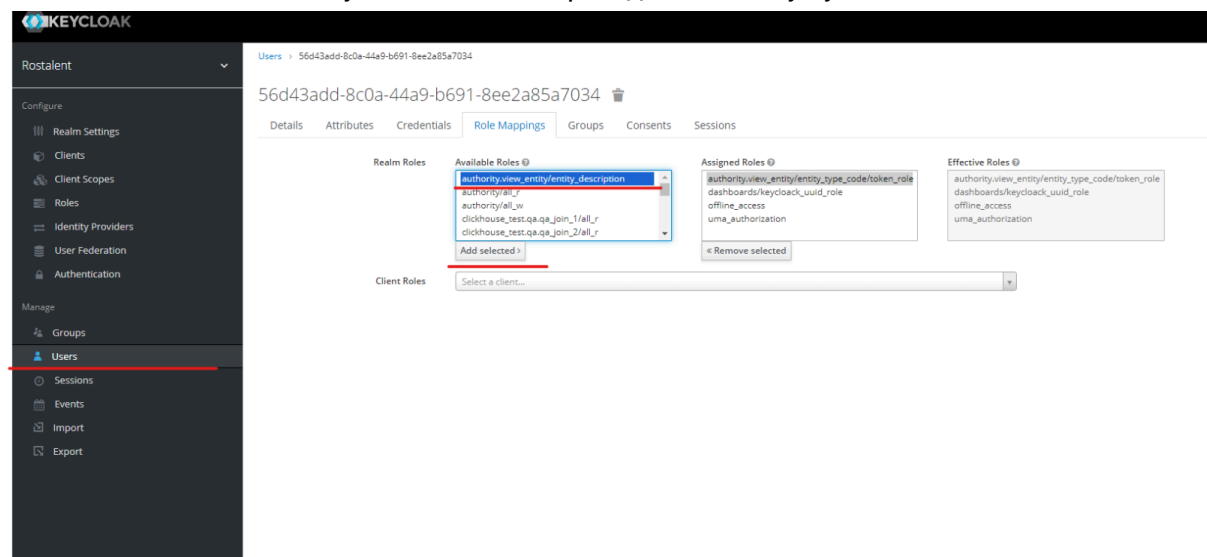
Keycloak

Пользователю необходимо перейти в Keycloak.



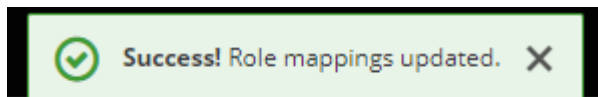
В разделе “Roles” в Keycloak, путём нажатия на «Add role», создаем роль с таким же названием, как в СУРе в п. “Полномочия и правила доступа”. В нашем случае - “rev_exp/type_role”.

После этого кликаем на пункт «Users» и переходим к поиску нужного пользователя.



Кликаем на ID пользователя, переходим в его настройки и выбираем пункт «Role mappings».

Кликаем на роль “rev_exp/type_role”, а дальше на «Add selected». После чего появится надпись «Success!» — роль успешно назначена пользователю.



Если выдаёте новую роль пользователю для доступа к датасету, не забывайте удалять предыдущую.

В нашем случае мы удаляли роль «rev_exp/all_role» через "Remove selected".

Проверка ограниченного доступа без привязки к пользователю

Переходим к проверке доступа. Вернёмся к приложению, в котором мы проверяли полный доступ.

Теперь слева, в подключении без СУРа, видим все строки, а справа - только строки с Доходом.

Без СУРа

list	type	amount
Торговая точка "Мария"	Доход	96920
Торговая точка "Люксор"	Доход	73688
Сдача помещения №1 в аренду	Доход	22000
Сдача авто Nissan в аренду	Доход	12000
Заработная плата	Доход	56000
Аренда торговой площади в ТЦ Нива	Расход	18000
Аренда торговой площади в ТЦ Мир	Расход	13000
Связь (телефон, интернет)	Расход	1000

С СУРом

list	type	amount
Торговая точка "Мария"	Доход	96920
Торговая точка "Люксор"	Доход	73688
Сдача помещения №1 в аренду	Доход	22000
Сдача авто Nissan в аренду	Доход	12000
Заработная плата	Доход	56000

Ограниченный доступ без привязки к пользователю настроен.

Ограниченный доступ по ключевому слову

Такой доступ позволяет делиться с пользователем только частью данных, хранящихся в датасете. В качестве аналогии можно привести датасет, отфильтрованный по полю. Только в случае ограниченного доступа по ключевому слову значения фильтра указываются в Keycloak, а пользователь, для которого отфильтрованы данные, не знает о том, что он видит не весь датасет.

Для настройки этого доступа необходимо:

1. Нужно создать необходимый датасет или представление.
2. Нужно создать объект ограничения, то, как необходимо предоставлять доступ (ко всей таблице, по определенному полю).
3. Нужно создать атрибут доступа. Это поле, по которому будет разграничение. Также необходимо связать атрибут доступа и объект ограничения.

4. Необходимо создать набор значений (Наборы значений — это наборы для заполнения ими значениями). Нужно также привязать атрибут доступа набору значений.
5. Необходимо создать ключевое слово типа token. Оно нужно для использования в Keycloak, поэтому стоит избегать зарезервированных слов Keycloak. Также важно привязать ключ к ключевому слову.
6. В этом разделе нужно привязать созданное ключевое слово к созданному набору значений.
7. В этом разделе нужно создать роль, которую затем необходимо будет прописать пользователю в Keycloak. Прежде чем записать роль в Keycloak ее необходимо связать с набором значений и объектом ограничения.
8. В разделе Roles в Keycloak создаем роль с таким же названием, как в СУРе.
9. В разделе Users в Keycloak переходим к нужному пользователю, находим созданную роль и присваиваем пользователю.
10. В разделе Clients в Keycloak переходим к player, далее к Mappers, создаем Mapper.
11. Необходимо в Keycloak в разделе Users перейти в Attributes, создать новый атрибут.

Например, возникла потребность в ограниченном доступе к таблице dir_emp с направлением «HR»:

direction	emp_count
HR	3
Производство	34
Финансы	1
Маркетинг	7

Сущности системы

Заполнение СУРа начинаем со страницы " Сущности системы". Нажимаем кнопку «+ Добавить запись», после чего откроется окно для ввода данных.

Добавить

ПОКАЗАТЕЛЬ	ДАННЫЕ
ID	
Название *	
Тип *	-
Системность *	<input type="checkbox"/> True/False
Описание *	
Название бизнес-объекта *	
Дата закрытия	
ID пользователя Keycloak, создавшего запись	

В "Названии" указываем название датасета – «insight.dir_emp », тк создаем сущность для виджетов версии 2.1.

Важно!

Если датасет будет использоваться в виджетах версии 2.1 (SDK), то в названии необходимо указать путь к датасету в виде:

3) Если датасет на Dremio - "БД.схема.путь до таблицы, включая папки".

4) Если датасет на PostgreSQL - "БД.путь до таблицы, включая папки".

Если датасет будет использоваться в виджетах с idp (или будет открываться в разделе редактора "Датасеты" или "Библиотека"), то в названии необходимо указать путь к датасету в виде "код подключения.схема.таблица".

В выпадающем списке "Тип" указываем «Объект данных БД – view или table».

«Бизнес-объект» – это дополнительный функционал на будущее, его не надо использовать.

В поле "Системность" флаг ставить не нужно, поле может быть отключено, так и должно быть.

"Описание" в этом пункте, как и в других пунктах далее, лучше заполнять подробностями, иначе будет тяжело ориентироваться.

“Название бизнес-объекта” указываем по аналогии с пунктом “Название”, **если будем просматривать сущность через IDP. Если объект данных будет просматриваться через виджеты версии 2.1**, то в “Название бизнес-объекта” следует вставить только название датасета или выю, которые заносим в систему.
Вводим все параметры и нажимаем кнопку «Сохранить».

Настройка объектов ограничения

Переходим на вкладку “Настройка объектов ограничения” и нажимаем кнопку “+ Добавить запись”.

Добавить

ПОКАЗАТЕЛЬ

ДАННЫЕ

ID

Код *

Название *

Название сущности *

-

Системность

☐ True/False

Описание *

Дата закрытия

ID пользователя Keycloak,
создавшего запись

Ограниченный доступ предполагает новый объект с другим кодом. В поле “Код” продублируем название сущности из п. “Сущности системы” и допишем нужный постфикс (поле, по которому будет происходить разрез данных через знак “/”).

Изменять старые записи в админ-панели не рекомендуется, так как значения в системных полях не изменятся.

В коде указываем «dir_emp/direction». Приписка /direction означает, что это объект ограниченного доступа, direction— поле, по которому будет разграничиваться датасет. В “Названии” продублируем название сущности из п. “Сущности системы”.

В выпадающем списке “Название сущности” выбираем датасет, к которому создаём объект — insight.dir_emp.

В Описании указываем, что это объект ограниченного доступа к датасету “insight.dir_emp”.

Вводим все параметры и нажимаем кнопку «Сохранить».

Атрибуты доступа

Переходим на вкладку “Атрибуты доступа” и нажимаем кнопку “+ Добавить запись”.

Добавить

ПОКАЗАТЕЛЬ	ДАННЫЕ
ID	<div></div>
Код *	<div></div>
Название *	<div></div>
Схема БД	<div></div>
Наименование подразделения	<div></div>
Системность	<div><input type="checkbox"/> True/False</div>
Дата создания	<div></div>
Дата закрытия	<div></div>

В поле “Код” указываем “direction”. direction — поле, по которому будет разграничиваться датасет.

В поле “Название” указываем, что это разрез по полю direction.

Остальные поля — это дополнительный функционал на будущее, его не надо использовать.

Вводим все параметры и нажимаем кнопку «Сохранить».

Настройка объектов ограничения

Возвращаемся на страницу “Настройка объектов ограничения” для того, чтобы связать атрибут доступа и объект ограничения.

sur-admin-authority.public.view_entity/entity_id	sur-admin-authority.public.view_entity/entity_id	sur-admin-authority.public.view_entity	sur-admin-authority.public.view_entity	1	⌕ Все данные
<input type="text" value="Найти"/>					+ Добавить запись
НАЗВАНИЕ #1	КОД АТТРИБУТА #1	НАЗВАНИЕ АТТРИБУТА #1	СИСТЕМНОСТЬ АТТРИБУТА	СИСТЕМНОСТЬ	
Ограничение по полю entity_id	entity_id	Разрез по полю entity_id	⦿ false	⦿ false	⌕ Все данные

Для этого необходимо раскрыть созданный объект ограничения, нажав на стрелку справа в строке с объектом. Далее нажать на кнопку “+ Добавить запись”.

Добавить

ПОКАЗАТЕЛЬ

ДАННЫЕ

ID

Название ограничения объекта *

ID атрибута *

Системность *

Код объекта ограничений *

Дата закрытия

ID пользователя Keycloak, создавшего запись

Дата создания

В поле “Название ограничения объекта” пишем по какому полю хотим настроить ограничение. В нашем случае запишем “Ограничение по полю direction”.

В поле "ID Атрибута" выберем название атрибута - "Разрез по полю direction". Остальные поля заполнять не нужно.

Вводим все параметры и нажимаем кнопку «Сохранить».

Наборы значений

Переходим на страницу "Наборы значений" и нажимаем кнопку "+ Добавить запись".

Добавить

ПОКАЗАТЕЛЬ	ДАННЫЕ
ID	<div></div>
Код *	<div></div>
Название *	<div></div>
Доступ к null *	<div><input type="checkbox"/> True/False</div>
Системность *	<div><input type="checkbox"/> True/False</div>
Описание *	<div><div></div><div></div></div>
Дата закрытия	<div><div></div><div></div></div>
ID пользователя Keycloak, создавшего запись	<div></div>

Наборы значений — это наборы для заполнения ими значениями. В поле "Код" указываем поле, по которому будет осуществляться ограничение с префиксом "valueset_" и постфиксом "_token". В нашем случае получится "valueset_direction_token". direction — поле, по которому будет разграничиваться датасет.

В поле "Название" вписываем "Список direction с keywords token".

Чекбокс "Доступ к null" при включении позволяет пользователю видеть не только поля в датасете, значение атрибута в которых не только соответствует значению набору, но и является null.

В поле "Описание" желательно написать: "набор значений по полю ... сущности ...". В нашем случае напишем - "набор значений по полю type сущности "insight.dir_emp"

Остальные поля — это дополнительный функционал на будущее, его не надо использовать.

Вводим все параметры и нажимаем кнопку «Сохранить».

После создания набора значений необходимо привязать к нему атрибут. Для этого необходимо раскрыть созданный набор значений, нажав на стрелку справа в строке с набором. Далее нажать на кнопку “+ Добавить запись”.

Добавить

ПОКАЗАТЕЛЬ	ДАННЫЕ
ID	<div></div>
ID атрибута *	<div>-</div>
ID набора значений *	<div></div>
Системность *	<div><input type="checkbox"/> True/False</div>
Дата закрытия	<div></div>
ID пользователя Keycloak, создавшего запись	<div></div>
Дата создания	<div></div>
ID пользователя Keycloak, обновившего запись	<div></div>

В поле “ID Атрибута” выберем название атрибута – “Разрез по полю direction”.

В поле “ID набора значений” выберем название набора значений – “valueset_direction_token”. Остальные поля заполнять не нужно.

Вводим все параметры и нажимаем кнопку «Сохранить».

Управление ключевыми словами

Ключевое слово — это набор, который заполняется значением атрибута пользователя в Keycloak.

Переходим на вкладку "Управление ключевыми словами" и нажимаем кнопку "+ Добавить запись".

Добавить

×

ПОКАЗАТЕЛЬ	ДАННЫЕ
ID	<div></div>
Код *	<div></div>
Название *	<div></div>
Описание *	<div></div>
Очищать при загрузке *	<div><input type="checkbox"/> True/False</div>
Время действия в сек., 0-бессрочно *	<div></div>
Ключевое слово *	<div>-</div>
Системность *	<div><input type="checkbox"/> True/False</div>

В качестве "Кода" указываем то же название, что и у атрибута — direction.

В поле "Название" дублируем код. Описание можно продублировать.

"Очищать при загрузке" — это дополнительный функционал на будущее, его не надо использовать.

В поле "Время действия в сек., 0-бессрочно" указываем 0.

В выпадающем списке "Ключевое слово" указываем Value from token. Value from keyword не используем.

Вводим все параметры и нажимаем кнопку «Сохранить».

После создания ключевого слова необходимо привязать к нему ключ. Для этого необходимо раскрыть созданное ключевое слово, нажав на стрелку справа в строке со словом. Далее нажать на кнопку "+ Добавить запись".

Добавить

ПОКАЗАТЕЛЬ	ДАННЫЕ
ID	
Ключ *	
Ключевое слово *	emp_count_key
Системность *	<input type="checkbox"/> True/False
Дата закрытия	
Дата создания	
ID пользователя Keycloak, создавшего запись	
Дата обновления	
ID пользователя Keycloak	

Ключ — значения для ключевого слова, т.е. то, как называется атрибут пользователя в Keycloak, указываем его как "direction".

В выпадающем списке выбираем ключевое слово с описанием "direction".

Вводим все параметры и нажимаем кнопку «Сохранить».

Связанные ключевые слова

Переходим на вкладку "Связанные ключевые слова и нажимаем кнопку "+ Добавить запись".

Добавить

ПОКАЗАТЕЛЬ	ДАННЫЕ
ID	<input type="text"/>
Набор значений *	<div>-</div>
Кодовое слово *	<div>-</div>
Системность *	<input type="checkbox"/> True/False
Дата закрытия	<input type="text"/>
ID пользователя Keycloak, создавшего запись	<input type="text"/>
Дата создания	<input type="text"/>
ID пользователя Keycloak, обновившего запись	<input type="text"/>

Этой связкой мы говорим, что набор значений заполняется значениями из атрибутов пользователя Keycloak.

В выпадающем списке "Набор значений" выбираем "Список direction с keywords token".
В выпадающем списке "Кодовое слово" выбираем "direction".

Вводим все параметры и нажимаем кнопку «Сохранить».

Полномочия и правила доступа

Переходим на вкладку "Полномочия и правила доступа" и нажимаем кнопку "+ Добавить запись".

Добавить
✕

ПОКАЗАТЕЛЬ	ДАННЫЕ
ID	<input type="text"/>
Роль *	<input type="text"/>
Код объекта *	- ▼
Включено *	<input type="checkbox"/> True/False
Разрешение на запись *	<input type="checkbox"/> True/False
Системность *	<input type="checkbox"/> True/False
Описание	<input type="text"/> ✎
Дата закрытия	<input type="text"/> 📅
ID пользователя Keycloak,	<input type="text"/> ▼

“Роль” — роль, которую в дальнейшем нужно будет прописать в Keycloak пользователю, которому необходимо предоставить доступ к датасету.

Указываем роль “rev_exp/type_role”.

В выпадающем списке “Код объекта” указываем объект, к которому создаём роль, — «rev_exp/type».

В пункте “Включено” ставим параметр True (ставим галку).

“Разрешение на запись” и “Системность” — это дополнительный функционал на будущее, их не надо использовать.

В Описании указываем, что выдаём разрешение на ограниченный доступ по набору значений к датасету «insight.rev_exp».

Вводим все параметры и нажимаем кнопку «Сохранить».

После создания роли ее необходимо связать с набором значений и объектом ограничения. Для этого необходимо раскрыть созданную роль, нажав на стрелку справа в строке с ролью. Далее нажать на кнопку “+ Добавить запись”.

Добавить



ПОКАЗАТЕЛЬ	ДАННЫЕ
ID	<input type="text"/>
Полномочие *	<input type="text" value="qa_join_1/genre_role"/>
Ограничение объекта *	<input type="text" value="-"/>
Набор значений *	<input type="text" value="-"/>
Системность *	<input type="checkbox"/> True/False
Дата закрытия	<input type="text"/>
ID пользователя Keycloak, создавшего запись	<input type="text"/>
Дата создания	<input type="text"/>
ID пользователя Keycloak	<input type="text"/>

В поле “Ограничение объекта” выберем название соответствующее значению поля “Название ограничения объекта” – “Ограничение по полю type”.

В поле “Набор значений” выберем название набора значений – “type_valueset”. Остальные поля заполнять не нужно.

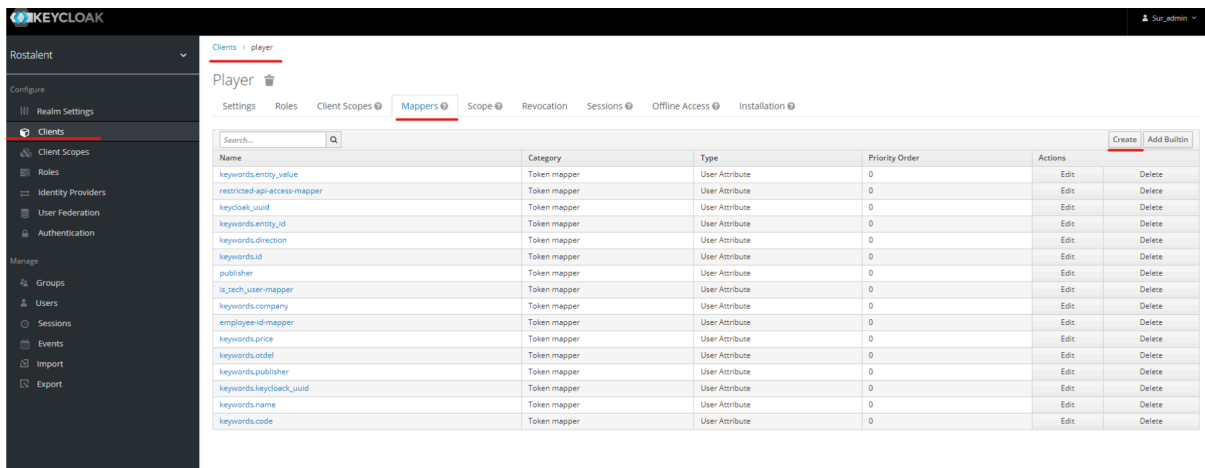
Вводим все параметры и нажимаем кнопку «Сохранить».

Keycloak

Пользователю необходимо перейти в Keycloak. В данном разделе осуществляется переход в Keycloak, где вы создаёте mapper, создаёте атрибут пользователю.

Mapper — это протокол, позволяющий передавать атрибут пользователя в KK в токен. Этот токен потом встраивается в запрос к датасету, по сути в SQL запрос добавляется фильтрация типа WHERE.

В разделе Clients в Keycloak переходим в player, далее в Mappers, создаем Mapper.



Нажимаем "Create" и переключаемся на экран создания mapper.

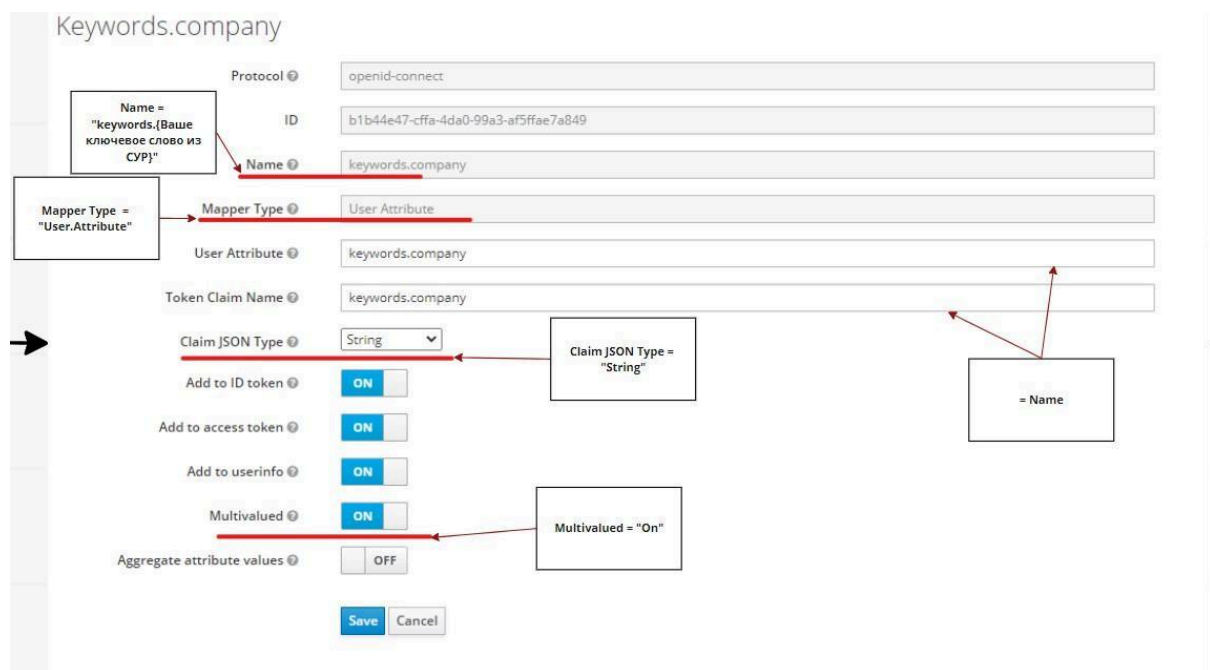
В "Name" пишем "keywords.direction". Обязательно пишем "keywords.".

В выпадающем списке "Mapper Type" выбираем "User Attribute".

В "User Attribute" и "Token Claim Name" указываем "keywords.direction". В выпадающем списке "Claim JSON Type" выбираем "String".

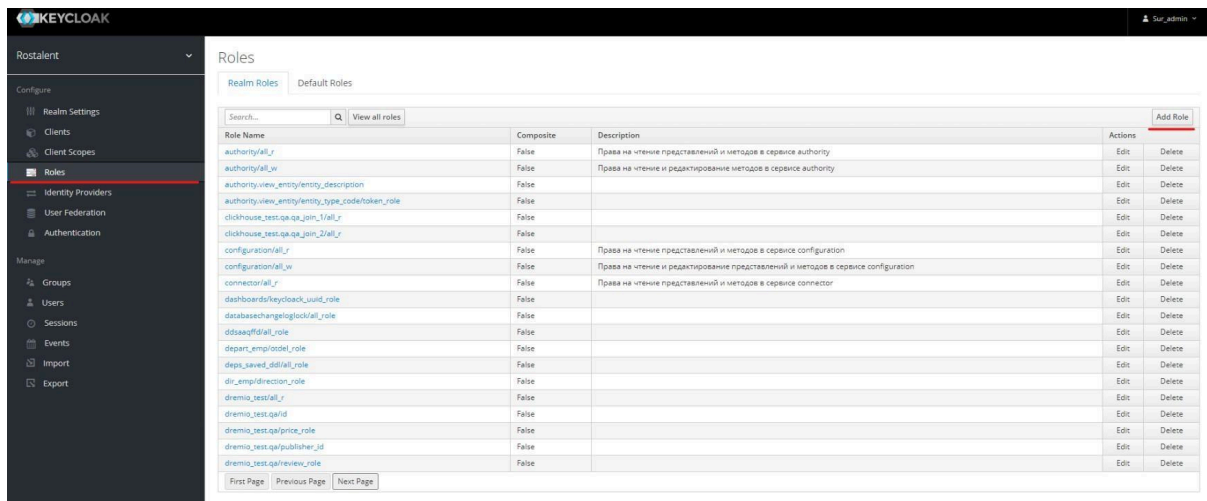
Переключаем свич "Multivalued" в режим "ON".

Вводим все параметры и нажимаем кнопку «Save».



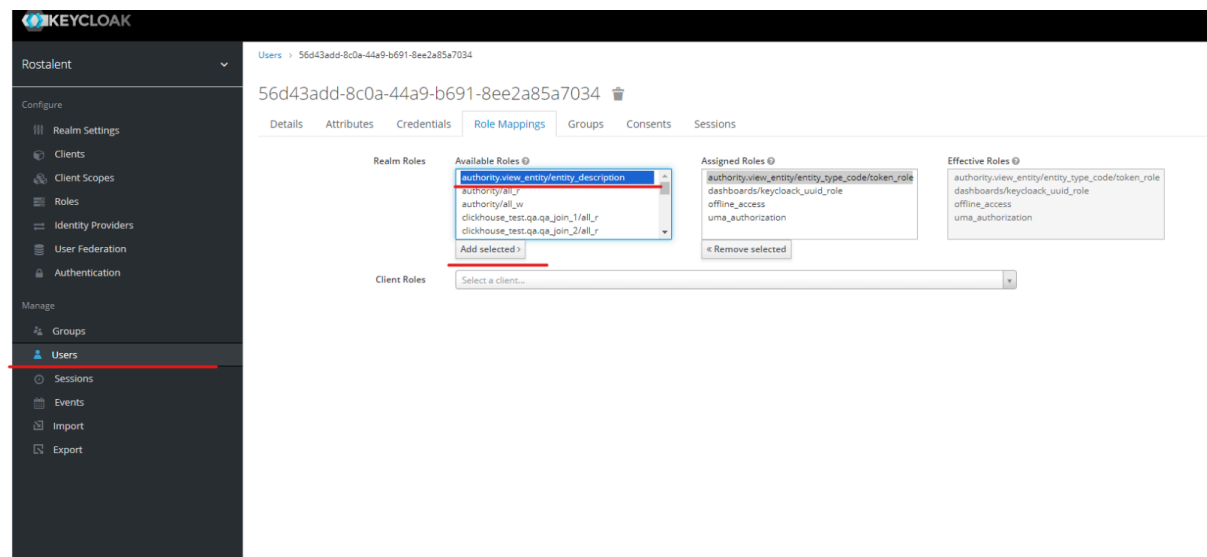
Переходим на вкладку "Роли".

В данном разделе осуществляется переход в Keycloak, где вы создаёте роль и назначаете её пользователю.



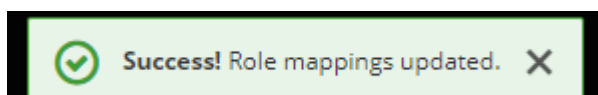
В разделе “Roles” в Keycloak, путём нажатия на «Add role», создаем роль с таким же названием, как в СУРе в п. “Полномочия и правила доступа”. В нашем случае - “dir_emp/direction_role”.

После этого кликаем на пункт «Users» и переходим к поиску нужного пользователя.



Кликаем на ID пользователя, переходим в его настройки и выбираем пункт «Role mappings».

Кликаем на роль “dir_emp/direction_role”, а дальше на «Add selected». После чего появится надпись «Success!» — роль успешно назначена пользователю.



Далее переходим в “Attributes” пользователя.

Details **Attributes** Credentials Role Mappings Groups Consents Sessions

Key	Value	Actions
keywords.direction	HR	Add

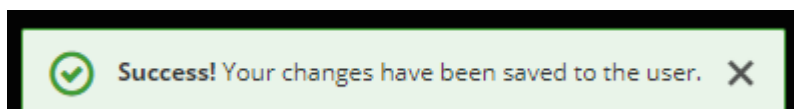
Save Cancel

В "Key" пишем название mapper — "keywords.direction".

В "Value" пишем значение, которым мы хотим фильтровать датасет, — "HR". В этом поле необходимо указывать конкретное значение из поля датасета, по которому происходит разрез. Пользователь, которому ограничат доступ к датасету, будет видеть только те поля, в которых значение поля соответствует введенному.

После этого нажимаем кнопку "Add", после чего становится доступна кнопка "Save".

Нажимаем кнопку "Save", в результате чего появится надпись «Success!» — атрибут успешно добавлен пользователю.



Проверка ограниченного доступа с привязкой к пользователю

Переходим к проверке доступа. Вернёмся к приложению, в котором мы проверяли полный доступ.

Мы скопировали предыдущую страницу и переключили датасеты таблиц на новый источник — dir_emp.

Слева, в подключении без СУРа, видим все строки, а справа - только строки с HR.

Без СУРа

direction	emp_count
HR	3
Производство	34
Финансы	1
Маркетинг	7

С СУРом

direction	emp_count
HR	3

Ограниченный доступ с привязкой к пользователю настроен.