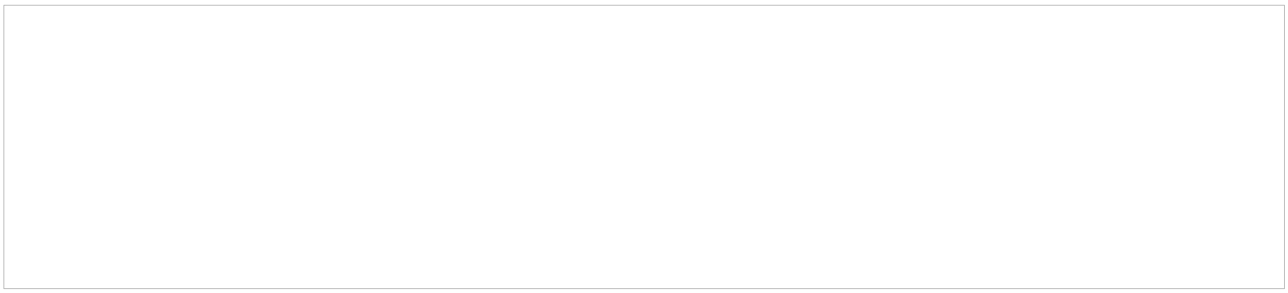
Основы работы с событиями

В рамках данной лабораторной работы мы расскажем какие инструменты поиска существуют в LogIQ, а также как выполнить поиск событий. Длительность выполнения лабораторной работы — 2 часа.

Событиями в рамках данной лабораторной работы называются все поступающие в систему агрегированные данные/сообщения. Для поиска или фильтрации отображаемых в таблице событий используются запросы, основанные на SQL-синтаксисе. Данные запросы вы можете создавать в двух режимах — Конструктор запросов и SQL.

Работа с конструктором запросов

Конструктор является адаптивным режимом сборки SQL-запросов.



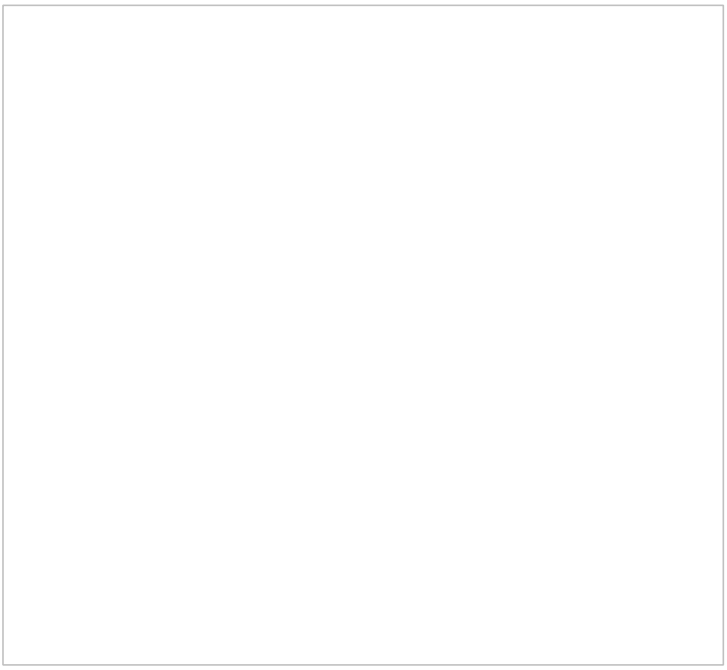
В данном режиме доступен следующий функционал:

1. **Выбор тенанта** — позволяет выбрать тенанты, в которых будет выполняться поиск событий;
2. **Выбор колонок (SELECT)** — позволяет выбрать колонки, которые будут использоваться в запросе;
3. **Выбор фильтров (WHERE)** — позволяет выбрать фильтры, которые будут использоваться в запросе;
4. **Выбор группировки (GROUP BY)** — позволяет настроить группировку в запросе;
5. **Выбор сортировки (ORDER BY)** — позволяет настроить сортировку в запросе;
6. **Ограничение вывода (LIMIT)** — позволяет ограничить количество результатов в выводе запроса;
7. **Определение временных рамок** — позволяет выбрать промежуток времени, за который будут отображаться события.

Выбор колонок (SELECT)

Для упрощения навигации по списку, вы можете выбрать список и порядок отображаемых колонок. Используйте переключатель слева от имени поля, для того, чтобы включить или выключить отображение колонки в таблице. По умолчанию выбраны первые 3 поля.

Для того, чтобы изменить порядок отображения колонок, наведите курсор на иконку сортировки справа от имени колонки, зажмите левую кнопку мыши и перенесите элемент в необходимое место.

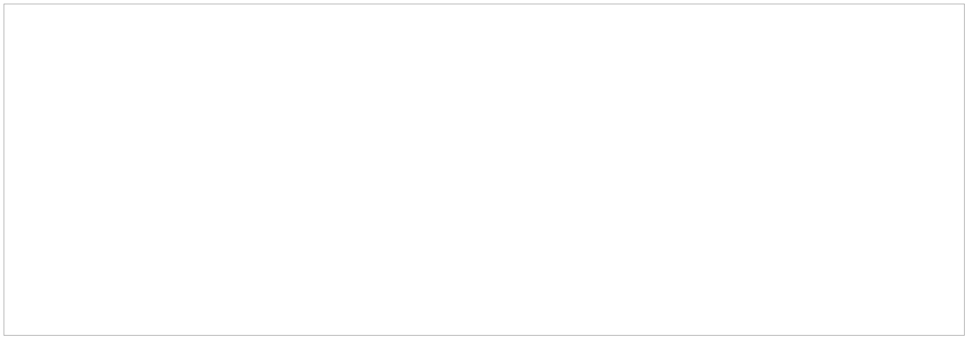


Вы также можете установить псевдонимы для каждой из колонок. Для этого наведите курсор на имя интересующей вас колонки и нажмите на всплывающую иконку карандаша. После этого появится поле для ввода псевдонима. Нажмите на голочку чтобы подтвердить применение псевдонима. После обновления запроса имя колонки будет заменено на установленный псевдоним.

Фильтры (WHERE)

Условия

Для работы с условиями можно использовать функционал фильтров таблицы.



После этого откроется список всех примененных к таблице фильтров. Для того, чтобы добавить условие, нажмите**+ Добавить условие** и заполните всю необходимую информацию:

- **Поле** — поле в базе данных, по которому будет выполняться фильтрация;
- **Оператор** — выбор оператор для фильтрации. Возможные значения **И** и **ИЛИ**;
- **Значение** — значение, по которому будет выполняться фильтрация.

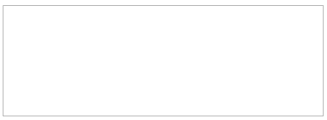
При добавлении двух и более фильтров вы можете построить более сложные выборки с использованием операторов **И** и **ИЛИ**.

Чтобы удалить условие нажмите на иконку корзины справа от него.

Групповые фильтры

Вы также можете добавить группу для условий. Для этого в окне выбора фильтров нажмите**Добавить группу**.

Условия, сформированные в группы, можно использовать для построения сложных выборок с использованием операторов **И** и **ИЛИ**.



Чтобы удалить группу нажмите на иконку корзины справа от нее.

Группировка событий (GROUP BY)

Для того, чтобы сгруппировать события по определенному полю, выберите поле для группировки. Чтобы удалить поле для группировки, нажмите на иконку корзины справа от выбранного поля.

Сортировка (ORDER BY)

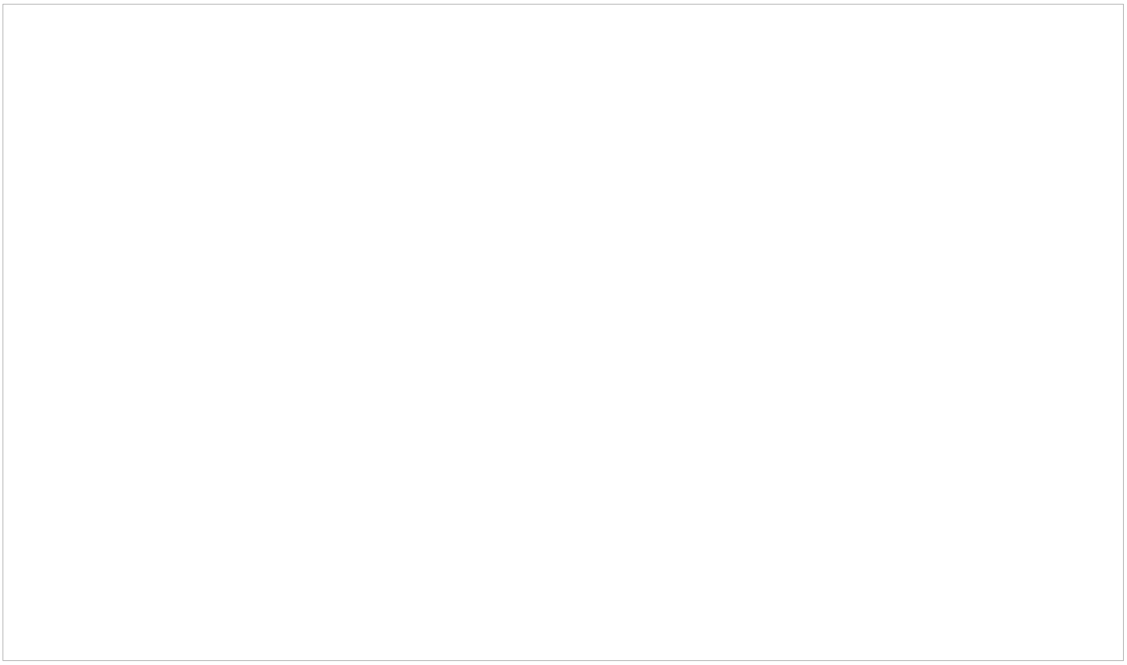
Для того, чтобы отсортировать порядок событий по определенному полю, выберите поле для сортировки и ее направление. Чтобы удалить поле для сортировки, нажмите на иконку корзины справа от выбранного поля.

Ограничение количества (LIMIT)

Для того, чтобы ограничить количество отображаемых результатов выполнения запроса, введите максимальное количество в поле ограничения количества результатов.

Определение временных рамок

Для того, чтобы отфильтровать список событий по времени их регистрации, нажмите **Выберите диапазон** справа от конструктора запроса. Во всплывающем окне вы можете ввести диапазон дат и времени вручную, либо выбрать одно из предустановленных значений.



После того как вы выбрали временной диапазон, нажмите **Выполнить**, чтобы обновить список событий.

Работа с режимом ручного ввода SQL-запросов

При необходимости, вы можете ввести SQL-запрос вручную. Для этого нажмите на поле ввода SQL-запроса и отредактируйте его содержимое под свои нужды.

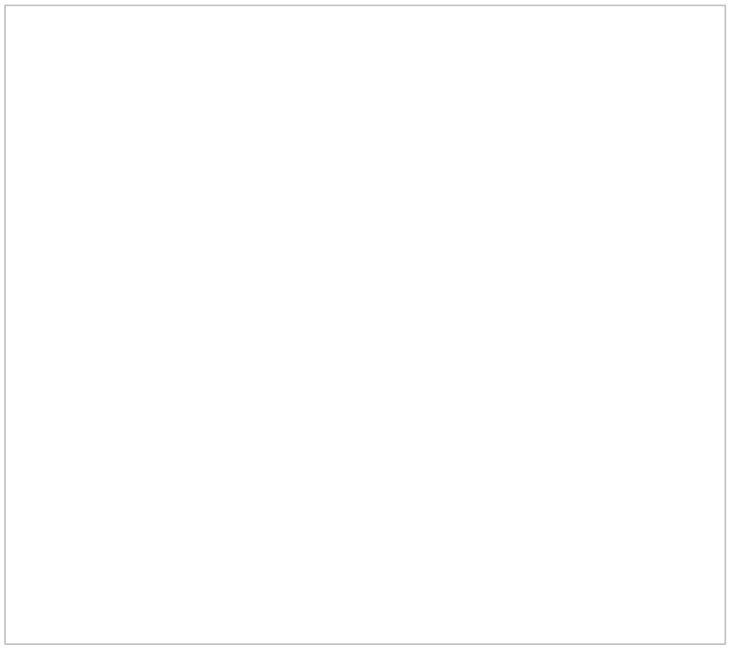
В данном режиме доступен следующий функционал:

1. **Выбор режима** — выбор режима построения запроса;
2. **Автоматическое определение синтаксиса SQL** — подсвечивает синтаксис SQL-запроса в поле для его ввода (параметр активирован по умолчанию);
3. **Выбор тенанта** — позволяет выбрать тенанты, в которых будет выполняться поиск событий;
4. **Выбор колонок (SELECT)** — позволяет выбрать колонки, которые будут использоваться в запросе;
5. **Выбор фильтров (WHERE)** — позволяет выбрать фильтры, которые будут использоваться в запросе;
6. **Только уникальные строки** — позволяет исключить повторяющиеся строки из результатов выполнения запроса;
7. **Определение временных рамок** — позволяет выбрать промежуток времени, за который будут отображаться события.

Выбор колонок (SELECT)

Для упрощения навигации по списку, вы можете выбрать список и порядок отображаемых колонок. Используйте переключатель слева от имени поля, для того, чтобы включить или выключить отображение колонки в таблице. По умолчанию выбраны первые 3 поля.

Для того, чтобы изменить порядок отображения колонок, наведите курсор на иконку сортировки справа от имени колонки, зажмите левую кнопку мыши и перенесите элемент в необходимое место.

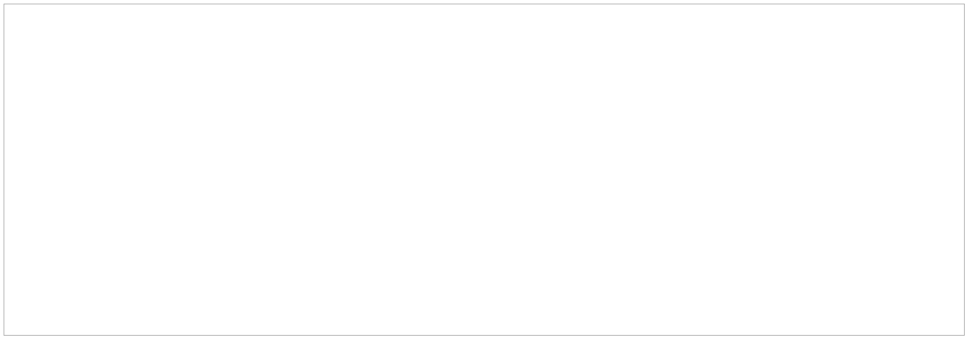


Вы также можете установить псевдонимы для каждой из колонок. Для этого наведите курсор на имя интересующей вас колонки и нажмите на всплывающую иконку карандаша. После этого появится поле для ввода псевдонима. Нажмите на голочку чтобы подтвердить применение псевдонима. После обновления запроса имя колонки будет заменено на установленный псевдоним.

Фильтры (WHERE)

Условия

Для работы с условиями можно использовать функционал фильтров таблицы.



После этого откроется список всех примененных к таблице фильтров. Для того, чтобы добавить условие, нажмите**+ Добавить условие** и заполните всю необходимую информацию:

- **Поле** — поле в базе данных, по которому будет выполняться фильтрация;
- **Оператор** — выбор оператор для фильтрации. Возможные значения **И** и **ИЛИ**;
- **Значение** — значение, по которому будет выполняться фильтрация.

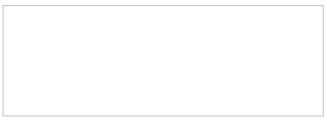
При добавлении двух и более фильтров вы можете построить более сложные выборки с использованием операторов **И** и **ИЛИ**.

Чтобы удалить условие нажмите на иконку корзины справа от него.

Групповые фильтры

Вы также можете добавить группу для условий. Для этого в окне выбора фильтров нажмите**Добавить группу**.

Условия, сформированные в группы, можно использовать для построения сложных выборок с использованием операторов **И** и **ИЛИ**.



Чтобы удалить группу нажмите на иконку корзины справа от нее.

Определение временных рамок

Определение временных рамок выполняется идентично режиму конструктора запросов.

ID статьи: 1361
Последнее обновление: 24 окт., 2025
Обновлено от: Егоров В.
Ревизия: 1
База знаний LogIQ -> Обучающие материалы -> Основы работы с событиями
https://docs.axel.pro/entry/1361/