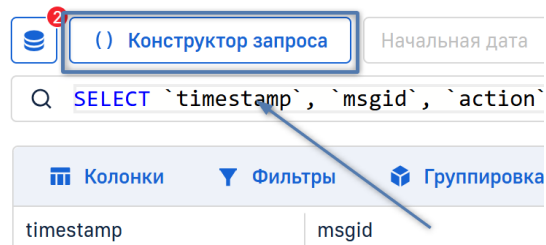


Конструктор запроса

Для фильтрации событий может быть использован функционал конструктора SQL-запросов. Данный инструмент является агрегатором функций по поиску событий — каждый из блоков (колонки, условия, группировка, сортировка и лимит) может быть детально настроен, после чего результат будет отображен в разделе **Пreview запроса**.

Для доступа к данному инструменту нажмите **Конструктор SQL** в левом верхнем углу страницы.

События (≥ 78)



2

() Конструктор запроса

Начальная дата

Q SELECT `timestamp`, `msgid`, `action`

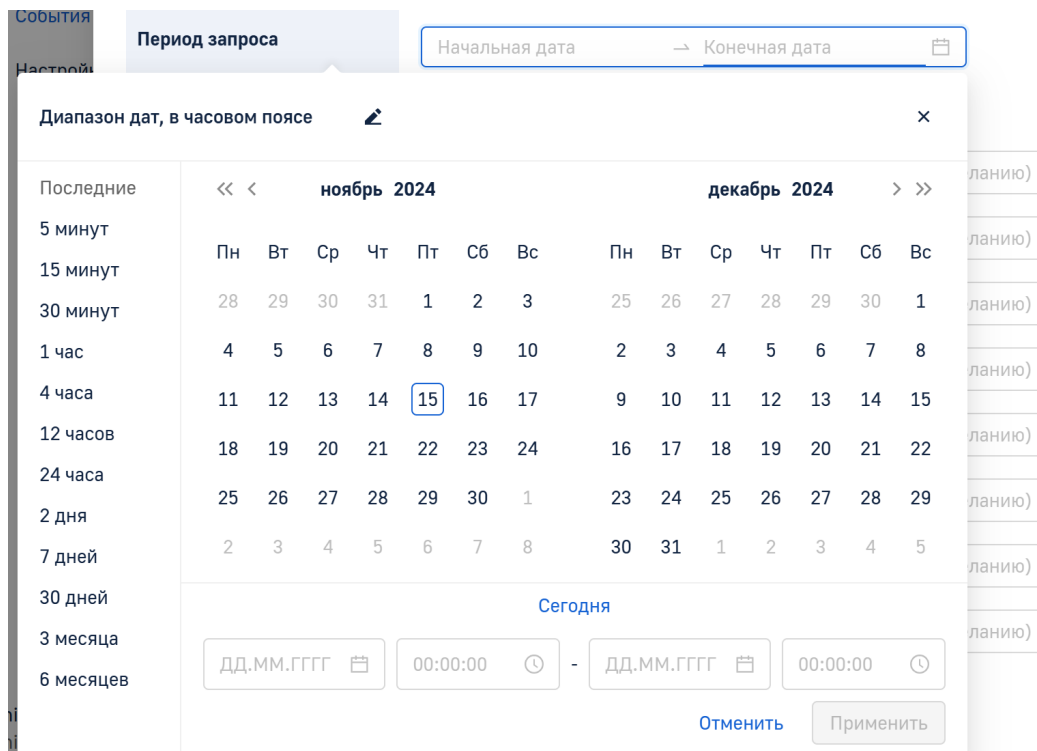
Колонки Фильтры Группировка

timestamp msgid

Ниже приведено описание блоков конструктора SQL.

Период запроса

В данном блоке вы можете настроить фильтрацию по времени события. Для этого нажмите на окно выбора даты и укажите даты для фильтрации, либо выберите одно из предложенных значений.



События

Период запроса

Начальная дата → Конечная дата

Диапазон дат, в часовом поясе

Последние

5 минут

15 минут

30 минут

1 час

4 часа

12 часов

24 часа

2 дня

7 дней

30 дней

3 месяца

6 месяцев

ноябрь 2024 декабрь 2024

Пн Вт Ср Чт Пт Сб Вс Пн Вт Ср Чт Пт Сб Вс

28 29 30 31 1 2 3 25 26 27 28 29 30 1

4 5 6 7 8 9 10 2 3 4 5 6 7 8

11 12 13 14 15 16 17 9 10 11 12 13 14 15

18 19 20 21 22 23 24 16 17 18 19 20 21 22

25 26 27 28 29 30 1 23 24 25 26 27 28 29

2 3 4 5 6 7 8 30 31 1 2 3 4 5

Сегодня

ДД.ММ.ГГГГ 00:00:00 - ДД.ММ.ГГГГ 00:00:00

Отменить Применить

Колонки (Оператор SELECT)

Данный блок используется для определения колонок, которые будут отображаться в таблице со списком событий.

Колонки

☐ Выбрать всё

Скрыть блок

timestamp

msgid

action

event_src_title

event_src_vendor

event_src_hostname

event_src_ip

message

+ Добавить

Здесь вы можете выбрать колонки из списка, а также задать им пользовательские имена для отображения. Вы также можете выбрать все колонки для запроса, нажав **Выбрать все** под названием блока.

Для того, чтобы добавить больше колонок, нажмите **Добавить**. Для того, чтобы удалить колонки, нажмите на иконку корзины справа от полей конфигурации колонок.

Условия (Оператор WHERE)

Данный блок используется для настройки фильтрации таблицы со списком событий.

Условия

☒

Скрыть блок

Группа 1 ...

Подгруппа 1.1 ...

message

Равно

REJECT

и

uuid

Не равно

0

или

Подгруппа 1.2 ...

message

Равно

ACCEPT

и

uuid

Не равно

0

и

action_name

Содержит

%login%

+ Условие

Группа

Подробное описание конфигурации фильтров приведено в статье [Работа с событиями](#).

Группировка (Оператор GROUP BY)

Данный блок используется для настройки группировки колонок таблицы со списком событий.

Группировка

☒

event_type

action_id

Для того, чтобы удалить атрибуты, нажмите **X** справа от имени атрибута. Чтобы добавить атрибут, нажмите на иконку стрелочки справа от поля выбора.

Сортировка (Оператор ORDER BY)

Данный блок используется для сортировки событий в таблице

Сортировка

timestamp

Сначала старые

Сначала новые

msgid

А-Я

Я-А

action

А-Я

Я-А

event_src_title

А-Я

Я-А

+ Добавить

Для этого выберите атрибут по которому будут сортироваться события, затем выберите порядок сортировки.

Лимит (Оператор LIMIT)

Данный блок используется для конфигурации ограничения на количество событий в таблице.

Лимит

150000

Ограничение на количество строк в таблице Событий

Пreview запроса

В данном блоке отображается предпросмотр запроса, который был создан с помощью конструктора.

Пreview запроса

Скрыть блок

```
SELECT
`timestamp`,
`msgid`,
`action`,
`event_src_title`,
`event_src_vendor`,
`event_src_hostname`,
`event_src_ip`,
`message`
FROM
`messages`
WHERE
(
(
`message` = 'REJECT'
AND `uuid` != '0'
)
OR (
`message` = 'ACCEPT'
AND `uuid` != '0'
)
)
```

Управление запросом

После того, как вы сформировали запрос, вы можете применить его. Для этого нажмите **Применить**. Для того, чтобы вернуть запрос к состоянию до использования конструктора SQL, нажмите **Вернуть исходный запрос**. Если вы хотите сбросить запрос, нажмите **Очистить все**.

Для обновления списка событий после конфигурирования запроса обновите список событий, нажав **Обновить**.

ID статьи: 213

Последнее обновление: 28 дек., 2024

Обновлено от: Егоров В.

Ревизия: 4

База знаний LogIQ -> Документация -> Система хранения и обработки данных «LogIQ». Версия 2.3.0 -> LogIQ. Руководство пользователя -> Раздел «События» -> Конструктор запроса

<https://docs.axel.pro/entry/213/>