

Работа с событиями в формате JSON

В данной статье описана работа с событиями в формате JSON: как просматривать и фильтровать такие события, а также сохранять запросы фильтрации.

Режим просмотра JSON-событий активируется с помощью внесения изменений в конфигурационные файлы системы. Подробное описание процесса описано в [Руководстве разработчика](#).

Раздел **События** позволяет формировать запрос на выборку событий в формате JSON. Для перехода в раздел нажмите на иконку **События** в левом боковом меню.

События (2 242 645)

06.11.2024 11:25:05 > 06.05.2025 11:25:05

Сохранить Обновить

SELECT `timestamp`, `uuid`, `data` FROM `messages` WHERE `timestamp` BETWEEN

timestamp	uuid	data
16.01.25, 14:29:52	e73d125b-67cf-4d00-8186-...	{ @metadata: { beat: winlogbeat, type: _doc, version: 7.15.0 }, @timesta...
16.01.25, 15:42:58	83fb6623-da1e-4d7f-9532-...	{ @metadata: { beat: winlogbeat, type: _doc, version: 7.15.0 }, @timesta...
16.01.25, 16:27:52	22c6778f-98f9-4e7f-a056-e...	{ @metadata: { beat: winlogbeat, type: _doc, version: 7.15.0 }, @timesta...
16.01.25, 18:26:45	d90a0081-ad01-49ff-84d6-...	{ @metadata: { beat: winlogbeat, type: _doc, version: 7.15.0 }, @timesta...
16.01.25, 21:54:52	d4152e54-67e8-46ff-b7ba-...	{ @metadata: { beat: winlogbeat, type: _doc, version: 7.15.0 }, @timesta...
16.01.25, 23:37:49	d6842adb-f010-4fec-88e9-...	{ @metadata: { beat: winlogbeat, type: _doc, version: 7.15.0 }, @timesta...
17.01.25, 03:37:58	84d092b8-2be9-4e57-9a1b-...	{ @metadata: { beat: winlogbeat, type: _doc, version: 7.15.0 }, @timesta...
04.12.24, 10:56:52	11ab23d0-ddd5-41b6-a054-...	{ @metadata: { beat: winlogbeat, type: _doc, version: 7.15.0 }, @timesta...
04.12.24, 18:02:58	9589a7df-2dbb-402f-bc5b-...	{ @metadata: { beat: winlogbeat, type: _doc, version: 7.15.0 }, @timesta...
04.12.24, 20:08:36	89099bb0-5f0b-4d5b-8876-...	{ @metadata: { beat: winlogbeat, type: _doc, version: 7.15.0 }, @timesta...

Колонки

1 2 3 4 5 ... 112133 > Перейти к 20

На данной странице отображаются все зарегистрированные в Системе события в формате JSON. Здесь вы можете просмотреть список событий, отфильтровать и экспортировать события.

Управление таблицей

По умолчанию на странице отображается 20 записей, однако вы можете выбрать отображение 20, 50, 100 и 500 записей на странице. Для этого нажмите на поле в правом верхнем углу списка и выберите в выпадающем списке необходимое количество для отображения.

Для переключения между страницами используйте блок в левом нижнем углу списка, или введите конкретную страницу и нажмите клавишу **Enter**:

< 1 2 3 4 5 ... 14 > Перейти к

Конфигурация отображения таблицы

Вы можете сконфигурировать отображение таблицы событий. Для этого нажмите на иконку шестеренки в правом верхнем углу таблицы:

Высота строки: Компактная, Нормальная, Расширенная

Автом. опред. синтаксиса SQL: Включено, Выключено

В выпадающем меню вы можете настроить следующие параметры:

- **Высота строки** — высота строк в таблице событий. Доступные значения: **Компактная**, **Нормальная** и **Расширенная**;
- **Автоматическое определение синтаксиса SQL** — данная строка активирует/деактивирует автоматическое определение синтаксиса SQL в содержимом событий.

Автоматическое определение синтаксиса SQL является экспериментальной функцией, в которой могут быть недоступны некоторые действия.

Также вы можете развернуть таблицу в режим полноэкранного отображения. Для этого нажмите на иконку рамок в правом верхнем углу таблицы:



Просмотр событий

Все события отображаются в виде списка в таблице. Для того, чтобы просмотреть содержимое JSON-события, нажмите на его строку. После этого содержимое отобразится в правом сайдбаре.

События (2 242 645)

3

06.11.2024 11:25:05 > 06.05.2025 11:25:05

Q

SELECT `timestamp`, `uuid`, `data` FROM

Колонки

timestamp	uuid
16.01.25, 14:29:52	e73d125b-67cf-4d00-818
16.01.25, 15:42:58	83fb6623-da1e-4d7f-953
16.01.25, 16:27:52	22c6778f-98f9-4e7f-a056
16.01.25, 18:26:45	d90a0081-ad01-49ff-84d
16.01.25, 21:54:52	d4152e54-67e8-46ff-b7b
16.01.25, 23:37:49	d6842adb-f010-4fec-88e
17.01.25, 03:37:58	84d092b8-2be9-4e57-9a
04.12.24, 10:56:52	11ab23d0-ddd5-41b6-a0
04.12.24, 18:02:58	9589a7df-2dbb-402f-bc5
04.12.24, 20:08:36	89099bb0-5f0b-4d5b-887
04.12.24, 21:20:49	a5da26cd-f160-462f-855

Детали события

UUID: d4152e54-67e8-46ff-b7ba-a7399aaae3b6

Q

Название поля или значение

timestamp

16.01.25, 21:54:52

data

{ 10 items

@metadata

{ 3 items

beat

winlogbeat

type

_doc

version

7.15.0

timestamp

"2025-01-16 14:54:52.942337+00:00"

agent

{ 6 items

ephemeral_id

a68337c3-21ea-4855-8d26-99852ee311cb

hostname

is-welf019

id

"7f2643f1-dce0-4b00-a3da-a027fe104549"

name

lt-80.phillips-lopez.com

type

winlogbeat

version

7.15.0

ecs

{ 1 item

1

2

3

4

5

...

112133

Показать типы

Экспорт события

Для быстрого переключения между событиями нажмите на иконки стрелочек в правом верхнем углу сайдбара. Чтобы подсветить определенный элемент в содержимом, нажмите на поле поиска и введите имя данного элемента. Переключатель **Показать типы** активирует/деактивирует отображение типов полей (**Int64**, **string** и т.д.). Вы также можете скопировать содержимое блока в запросе, нажав на иконку копии, которая появляется при наведении курсора на строку.

Фильтрация, сортировка и группировка событий

Для того, чтобы отфильтровать события, можно использовать следующие инструменты:

- Определение временных рамок;
- Поле ввода SQL-запроса;
- Сортировка таблицы с помощью колонок.

Определение временных рамок

Для того, чтобы отфильтровать список событий по времени их регистрации, нажмите на поле выбора даты, расположенное в верхнем левом углу страницы. В модальном окне вы можете ввести диапазон дат и времени вручную, либо выбрать одно из предустановленных значений.

События (2 242 645)

3

Начальная дата > Конечная дата

Сохранить

Диапазон дат, в часовом поясе Etc/GMT-7, UTC + 07:00

Последние
Свой формат
5 минут
15 минут
30 минут
1 час
4 часа
12 часов
24 часа

<< < май 2025 > >>

Пн	Вт	Ср	Чт	Пт	Сб	Вс	Пн	Вт	Ср	Чт	Пт	Сб	Вс
28	29	30	1	2	3	4	26	27	28	29	30	31	1
5	6	7	8	9	10	11	2	3	4	5	6	7	8
12	13	14	15	16	17	18	9	10	11	12	13	14	15
19	20	21	22	23	24	25	16	17	18	19	20	21	22
26	27	28	29	30	31	1	23	24	25	26	27	28	29
2	3	4	5	6	7	8	30	1	2	3	4	5	6

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

Поле ввода SQL-запроса

Для того, чтобы отфильтровать, отсортировать или сгруппировать события, вы можете отредактировать исходный SQL-запрос.

При вводе SQL-запроса необходимо соблюдать следующие правила:

1. Следует использовать только запрос **SELECT**. Попытка обновить таблицу с любым другим запросом приведет к ошибке.
2. В запросе нельзя указывать параметр пагинации **OFFSET**.
3. Наименование полей необходимо указывать в апострофах, например ``event.type``.

Ниже приведены примеры запросов для каждого из действий.

Поиск событий (SELECT)

```
SELECT data.json.computer_name, data.winlog.api FROM `messages`
```

Установка псевдонима (Alias) для поля

```
SELECT data.agent.id AS agid, data.agent.name AS agname, data.json.task AS jtask  
FROM messages  
WHERE (agid LIKE '%0d%') AND (agname LIKE '%-%') AND (jtask LIKE '%else%')
```

Фильтрация событий (WHERE)

```
SELECT data.agent.id, data.agent.name, data.json.task  
FROM messages  
WHERE (data.agent.id LIKE '%0d%') AND (data.agent.name LIKE '%-%') AND (data.json.task LIKE '%else%')
```

Подсчет количества событий (COUNT)

```
SELECT COUNT(*) FROM messages  
WHERE (data.agent.id LIKE '%0d%') AND (data.agent.name LIKE '%-%') AND (data.json.task LIKE '%else%') AND (timestamp != '2025-01-02')  
FORMAT TabSeparated
```

Группировка событий (GROUP BY)

```
SELECT  
  data.json.process.pid::Int64  
FROM messages  
GROUP BY data.json.process.pid::Int64
```

Сортировка событий (ORDER BY)

```
SELECT  
  data.json.process.pid::Int64  
FROM messages  
ORDER BY data.json.process.pid::Int64 DESC
```

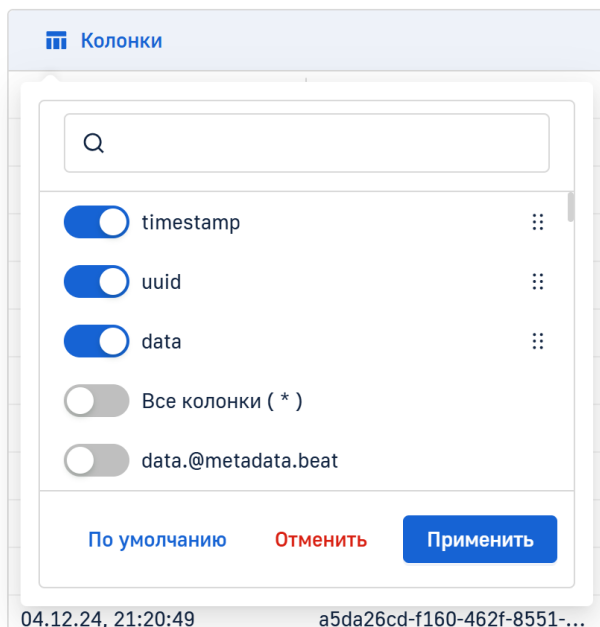
Для корректной работы команд **GROUP BY**, **COUNT** и **ORDER BY** необходимо указать в запросе типы полей в формате **имя_поля.тип_поля**.

Сортировка таблицы с помощью колонок

Данный функционал доступен только при использовании режима **Автоматического определения синтаксиса SQL**.

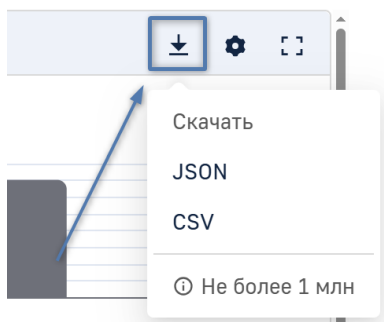
Для упрощения навигации по списку, вы можете выбрать список и порядок отображаемых колонок. Для этого нажмите **Колонки** в левом верхнем углу таблицы. Используйте переключатель слева от имени поля, для того, чтобы включить или выключить отображение колонки в таблице. По умолчанию выбраны первые 3 поля.

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.



Экспорт событий

Для того, чтобы экспортировать список событий нажмите на иконку загрузки в правом верхнем углу таблицы и выберите в выпадающем меню формат файла:

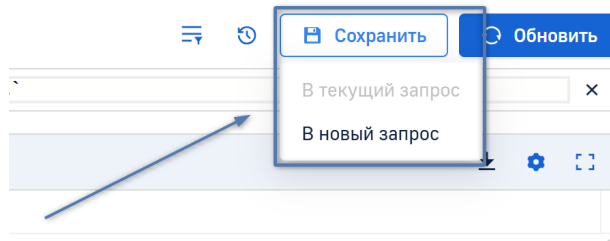


Вы можете экспортировать не более 1 миллиона событий за раз.

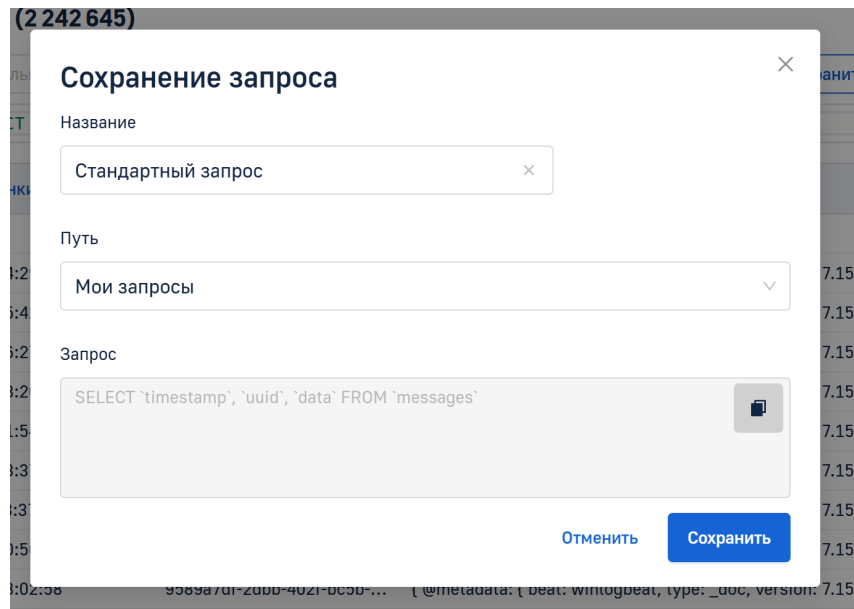
Сохраненные запросы

Сохранение запросов

Для удобства ежедневного использования вы можете сохранить ваши запросы. Для этого нажмите **Сохранить** в правом верхнем углу страницы, затем в выпадающем меню выберите вариант сохранения — в текущий запрос, или в новый.

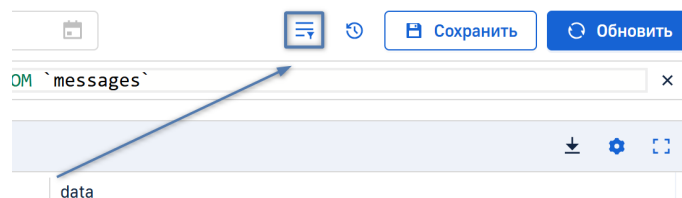


Если вы выбрали **В новый запрос**, откроется новое окно, в котором вы сможете задать имя запроса и указать путь для его сохранения. Для сохранения запроса нажмите **Сохранить**.



Использование сохраненных запросов

Для того, чтобы отфильтровать список событий по ранее сохраненным параметрам, нажмите на иконку сохраненных запросов в правом верхнем углу страницы, затем в правом сайдбаре выберите ранее сохраненный запрос.

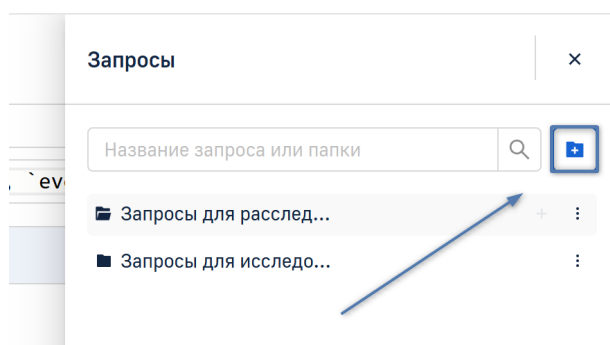


Управление хранилищем сохраненных запросов

Вы можете управлять файловой системой хранения запросов: создавать папки, а также переименовывать, перемещать и удалять папки и сохраненные запросы.

Создание новой папки

Для того, чтобы добавить новую папку, нажмите на иконку добавления в правом верхнем углу дашборда.

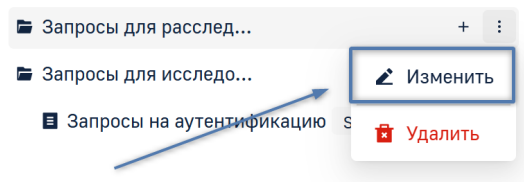


Введите имя для новой папки и нажмите **Создать**.

Если вы хотите создать папку внутри уже существующей, наведите на мышку на корневую папку и нажмите на появившуюся иконку **+**, введите имя для новой папки и нажмите **Создать**.

Редактирование содержимого

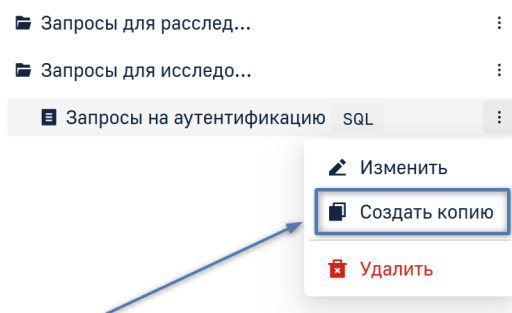
Для того, чтобы отредактировать сохраненный запрос или папку, нажмите на три точки справа от имени и в выпадающем списке выберите **Изменить**.



В открывшемся окне вы можете переименовать и изменить путь к запросу или папке, а также просмотреть содержимое сохраненного запроса. Нажмите **Сохранить** для применения изменений.

Создание копии сохраненного запроса

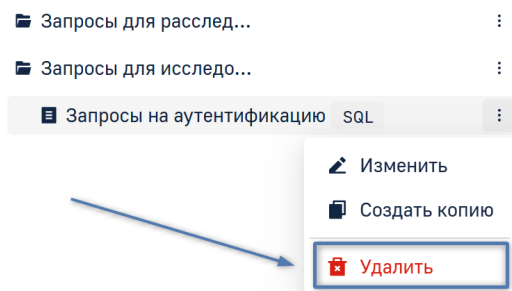
Для того, чтобы создать копию сохраненного запроса, нажмите на три точки справа от имени и в выпадающем списке выберите **Создать копию**.



Выберите путь для сохранения копии запроса и нажмите **Создать копию**.

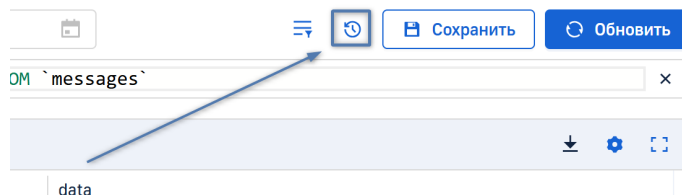
Удаление содержимого

Для того, чтобы удалить сохраненный запрос или папку, нажмите на три точки справа от имени и в выпадающем списке выберите **Удалить**.



Просмотр истории запросов

Для того, чтобы повторить один из ранее использованных запросов, вы можете воспользоваться историей запросов. Для этого нажмите на иконку истории и выберите интересующий вас запрос в правом сайдбаре.



В данном сайдбаре вы можете просмотреть следующую информацию о запросах:

- Дата выполнения запроса;
- Режим выполнения запроса;
- Продолжительность выполнения запроса;
- Содержимое запроса.

Выбор tenants

Для того, чтобы просмотреть события только для определенных tenants, нажмите на иконку базы данных в левом верхнем углу и выберите tenants, для которых вы хотите просмотреть выборку.

События (2 242 645)

3

Начальная дата

>

Конечная дата

Q

SELECT `timestamp`, `uuid`, `data` FROM `message`

Колонки

timestamp	uuid	data
16.01.25, 14:29:52	e73d125b-67cf-4d00-8186-...	{ @metad:
16.01.25, 15:42:58	83fb6623-da1e-4d7f-9532-...	{ @metad:
16.01.25, 16:27:52	22c6778f-98f9-4e7f-a056-e...	{ @metad:
16.01.25, 18:26:45	400~0001~2d01~40ff~84d6	{ @metad: