Руководство пользователя ПО «Клаудвизор»

Введение

О программном обеспечении

ПО «Клаудвизор» представляет из себя удобный инструмент, позволяющий повысить наблюдаемость и безопасность ИТ- систем, за счёт внедрения быстрой и простой в обслуживании системы поиска и анализа логов, а также позволяющий ускорить доступ к архивным логам для высоконагруженных сервисов.

Функциональные возможности ПО «Клаудвизор»:

- Улучшение наблюдаемости и безопасности ИТ- систем за счёт внедрения быстрой и простой в обслуживании системы поиска и анализа логов.
- Ускорение доступа к архивным логам для высоконагруженных сервисов.
- Полнотекстовый поиск по архивным файлам логов на локальных и внешних хранилищах данных.
- Программный интерфейс для загрузки логов
- Анализ данных: обзорная панель, группировки, выделение полей по запросу
- Быстрый переход от результатов поиска к исходным логам
- Экспорт результатов поиска
- Совместная командная работа над результатами поиска
- Контроль доступа к логам, разделение ролей
- Библиотека поисковых запросов

Системные требования

ПО «Клаудвизор» (далее также – система, ПО) может быть поставлено заказчику в двух форматах:
- облачное решение;
- серверное решение.
Настройка ПО в формате облачного решения и предоставление ресурсов для его функционирования обеспечивается компанией-правообладателем ПО.
При установке серверного решения на локальных серверах заказчика не требуется установка дополнительных компонентов, поскольку ПО для установки включает требуемые компоненты.

Минимальные

- Windows 10 (Home/Pro) или Debian-based Linux, или Windows Server 2012
- 4 vCPU

- 8 Гб RAM
- 300 MB HDD для установки
- 10 GB HDD для поисковых метаданных
- Дисковое пространство для загружаемых файлов логов
    - только при выборе локального жесткого диска для хранения логов
    - не требуется при поиске в логах на внешних хранилищах

Рекомендуемые

- Windows 10 или 11 (Home/Pro) или Ubuntu Linux 20.2 и выше, или Windows Server 2018
- 8-64 vCPU, в зависимости от требований к скорости поиска в логах
- 16-256 GB RAM, в зависимости от требований к скорости поиска в логах
- 300 MB SSD для установки
- 10-100 GB SSD для поисковых метаданных, в зависимости от количества событий в просматриваемых логах.
- Дисковое пространство для загружаемых файлов логов
    - только при выборе локального жесткого диска для хранения логов

Вход в систему

Внутренние пользователи

- Чтобы использовать ПО (систему), распространяемое в формате интернет-сервиса, необходимо зарегистрироваться на сайте https://logpad.cloudvyzor.ru/ ..
- Чтобы войти в систему как внутренний пользователь в локальной инсталляции, такой пользователь должен быть создан администратором ПО «Клаудвизор». Чтобы создать внутреннего пользователя, обратитесь к разделу «Администрирование».
- admin — единственный заранее созданный внутренний пользователь. Чтобы войти в систему как администратор, обратитесь к главе «Администрирование».

Пользователи Active Directory

Не является обязательным функционалом ПО и является альтернативой внутренним пользователям.

Чтобы войти в систему как пользователь Active Directory в локальной версии

- Локальная версия должна быть установлена в домене Windows
- Пользователю должен быть предоставлен доступ к одному или нескольким репозиториям. Информацию о том, как предоставить доступ к репозиториям, см. в разделе «Администрирование».
- Имя пользователя должно быть введено в формате домен\пользователь

Выбор репозитория

Репозиторий - это рабочее пространство пользователя, содержащее набор баз данных с логами.

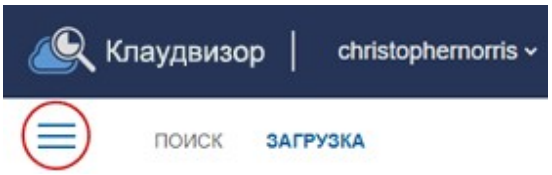
У каждого внутреннего пользователя есть свой собственный репозиторий.

У пользователей Active Directory нет собственных репозиториев, и им может быть предоставлен доступ только к репозиторию внутреннего пользователя.

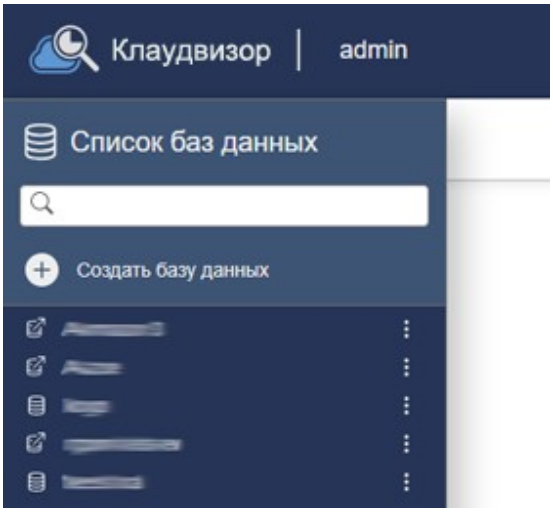
Если пользователю предоставлен доступ к нескольким репозиториям, в заголовке отображается раскрывающийся список с выбором репозитория.

По умолчанию, выбирается собственный репозиторий. Если собственного репозитория нет, выбирается первый предоставленный репозиторий.

Выбор базы данных

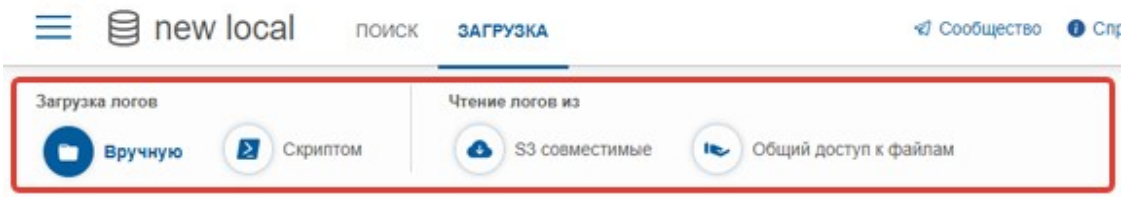


База данных — это контейнер для логов. На левой панели отображается список баз данных их можно создавать, переименовывать и удалять.



Перед началом поиска необходимо создать новую или выбрать существующую базу данных.

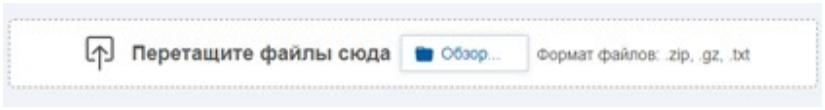
Создание базы данных и доступ к логам



При создании базы данных, необходимо выбрать способ доступа к логам.

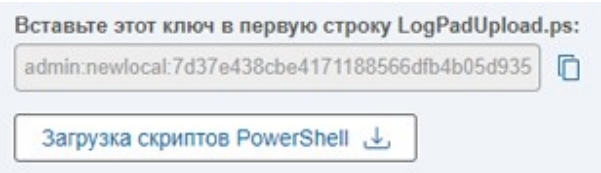
Загрузка вручную

На вкладке «Загрузить» в пользовательском интерфейсе вы можете перетаскивать файлы или выбрать файлы логов и загружать их. Поддерживаются ZIP-файлы и текстовые файлы логов .txt. В этом случае, логи хранятся на сервере ПО «Клаудвизор». Можно загрузить один и тот же файл несколько раз, он будет перезаписан.



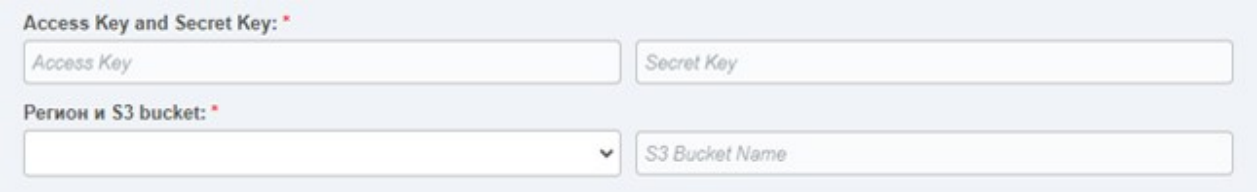
Загрузка скриптом

Файлы можно загружать, вызвав программный интерфейс сервера ПО «Клаудвизор» с ключом агента в качестве параметра. Ключ агента и примеры сценариев PowerShell доступны на вкладке «Скриптом» в разделе «Загрузка».



Хранилище S3

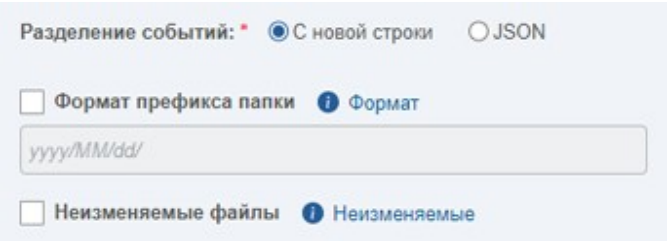
Логи можно искать на внешнем хранилище S3. Вам нужно указать ключ доступа и секретный ключ, а также имя хранилища.



Скорость поиска в логе в бакете S3 сильно зависит от структуры бакета: одни и те же поисковые запросы могут выполняться за секунды или за часы.

Оптимальная производительность достигается если:

1. Сервер ПО «Клаудвизор» устанавливается в том же датацентре, что и сервис S3, желательно в том же регионе, чтобы сетевое подключение было быстрым и бесплатным.
2. В конфигурации базы ПО «Клаудвизор» установлена опция «Неизменяемые». Это означает, что файлы логов считаются неизменяемыми и не могут обновляться на лету, поэтому их метаданные могут кэшироваться и не нуждаются в обновлении.
3. В бакете S3 файлы логов хранятся в папках по годам, месяцам, дням (и, возможно, по часам), и в конфигурации базы ПО «Клаудвизор» параметр «Префикс папки» включён и настроен соответствующим образом.



При записи файлов логов в бакет S3, настоятельно рекомендуется хранить их в папках, содержащих год, месяц и день. Если вы это делаете, пожалуйста, укажите формат префикса, содержащий год, месяц и дату. Это сильно оптимизирует время выполнения поисковых запросов.

Например, если файлы хранятся в вашем хранилище S3 как

*bucket1/**2024/01/01**/service1/log.zip*
*bucket1/**2024/01/01**/service1/log.zip*
*bucket1/**2024/01/02**/service2/log.zip*
*bucket1/**2024/01/02**/service2/log.zip*

то следует указать формат префикса папки: **«yyyy/MM/dd»**

Разделение событий

Поддерживаются два формата лог файлов:

1. **Формат, в котором каждое событие начинается с новой строки** (выбрано по умолчанию)
2. **Формат лог файлов JSON**.
   Для него, необходимо указать формат массива эвентов
   1. Нет массива событий: объекты-события записаны через запятую как {event1},{event2},{event3}
   2. Массив событий без ключа: [{event1},{event2},{event3}]
   3. Массив событий с ключом: {obj1, obj2, "events":[{event1},{event2},{event3}]}
      В этом случае, нужно указать JSON-путь до массива, например $.events.

   Также, поддерживается формат, когда события JSON записаны каждое в отдельной строке. В этом случае, следует выбрать опцию "С новой строки".

Файловое хранилище

Логи можно искать на локальном диске и файловом хранилище. Необходимо указать путь к локальному фолдеру или фолдеру на файловом сервере.

Для ПО «Клаудвизор» сервера на машине Windows:

Для поиска в локальном фолдере, укажите путь к фолдеру в формате например c:\logs\myapplogs
Для поиска в фолдере с общим доступом, укажите путь к фолдеру в формате например \\fileshare\logs\myapplogs
Убедитесь, что права на чтение этой папки предоставлены учетной записи компьютера, на котором установлено ПО «Клаудвизор». Если это не так, то в явном виде укажите имя пользователя и пароль на доступ к папке.

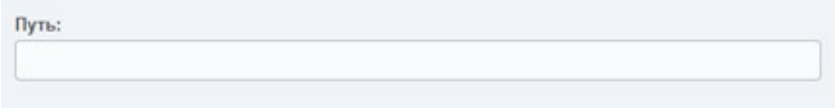
Для ПО «Клаудвизор» сервера на машине Linux:

Для поиска в локальном фолдере, укажите путь к фолдеру в формате file://home/user1/logs/.

Для поиска в фолдере на другом сервере, необходимо выполнить mount внешнего фолдера к локальному фолдеру на сервере ПО «Клаудвизор» и указать путь у фолдеру в формате file://home/user1/mounted_folder

Поиск производится только в указанном фолдере, без сабфолдеров.

Однако, если файлы логов разложены разложены по сабфолдерам вида user1/logs/2024/12/11, то для этого случая поддерживается указание префикса фолдера. Если префикс указан, то поиск будет производиться в сабфолдерах согласно префиксу.



Начало поиска

После выбора или настройки базы данных, можно приступать к поиску логов.

Для локальных баз данных небольшого/среднего размера можно просто ввести ключевые слова и выполнить поиск.

Для больших и внешних баз данных в первую очередь следует подумать о нескольких вещах, чтобы ускорить поиск:

- **Временной фильтр.** По умолчанию он настроен на последний день в логах. Вам следует настроить его на то количество времени, которое вам действительно нужно, но не намного больше.
- **Фильтр по имени файла.** Допустим, ваш бакет S3 с логами имеет такую структуру:

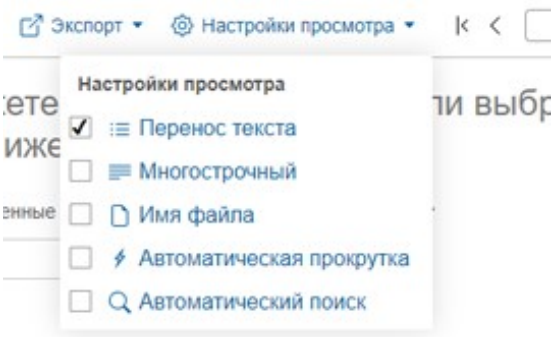
В таком случае, если вы исследуете только проблему с мобильным приложением, введите **“file:mobileapp*”** в поисковый запрос, чтобы ускорить поиск.

Язык поисковых запросов

Шаблон поиска	Пример	Результат
Простой термин	error	Строка лога содержит “error”
Исключенный термин	-OutOfMemory	Строка лога не содержит “OutOfMemory”
Несколько терминов	Exception BadRequest	Строка лога содержит как “Exception” так и “BadRequest”
Полная фраза	“File not found”	Строка лога содержит точную фразу “File not found”
Исключенная фраза	-“File not found”	Строка лога не содержит точной фразы “File not found”
Поиск по шаблону	Err*	Строка лога содержит слово, начинающееся с Err
Полная фраза с подстановочными знаками	"phrase* with* wildcards*"	Строка лога содержит фразу, соответствующую этому шаблону
Экранирование	“\”phrase in quotes\””	Строка лога содержит ”phrase in quotes”
Специальные символы	"special \t symbols"	Строка лога содержит эту фазу с символом табуляции
Временные метки	timestamp>="2017-11-12 13:14:15.667"	Поиск строк лога с отметкой времени, большей или равной указанной
	timestamp>"2017-11-12 13:14:15"	Поиск строк лога с отметкой времени, больше указанной
	timestamp<="2017-11-12"	Поиск строк лога с отметкой времени меньше или равной указанной
	timestamp<”2017-11-12”	Поиск строк лога с отметкой времени меньше указанной
	date=2017-11-12	Найти строки лога с датой, равной указанной
Пути к файлам:	path="path"	Поиск файлов лога с точным путем к файлу
	path:pathSubstring	Поиск файлов лога по пути, содержащему подстроку
	-path:pathSubstring	Поиск файлов лога по пути, НЕ содержащему подстроку

Имена файлов:	file="fileName"	Поиск файлов лога с точным именем файла
	file:fileNameSubstring	Поиск файлов лога по имени файла, содержащему подстроку
	-file:fileNameSubstring	Поиск файлов лога с именем, НЕ содержащим подстроки
Шаблоны:	`Operation {name} done in {time} ms`	Укажите шаблон для преобразования строки лога в таблицу

Режимы просмотра



Перенос текста

- Включение переноса текста должно привести к тому, что длинный текст события поместится на экране
- Отключение переноса текста должно сделать длинный текст события длиной в одну строку с возможностью прокрутки по горизонтали

Многострочный

- Включенный многострочный режим должен отображать текст события в соответствии с символами новой строки в тексте события
- Выключеный многострочный режим должен отображать текст события как один блок, игнорируя символы новой строки в тексте события

Имя файла

- При включении, будет отображаться имя файла слева от даты/времени события
- При выключении, не будет отображаться имя файла слева от даты/времени события

Автоматическая прокрутка

- При отключённой автоматической прокрутке, вертикальная прокрутка должна останавливаться в нижней части страницы
- При включённой автоматической прокрутке, вертикальная прокрутка должна загружать следующую страницу в нижней части страницы

Автоматический поиск

- Функция автоматического поиска должна автоматически запускать поиск при каждом изменении строки запроса или фильтра
- Отключение автоматического поиска НЕ должно приводить к автоматическому запуску поиска, но должно запускать его только при нажатии кнопки «Поиск» или клавиши «Ввод» в строке поиска

Полноэкранный режим

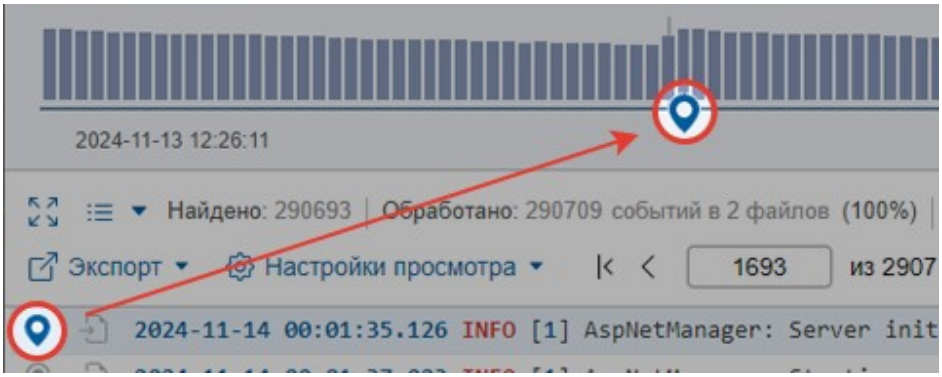
- Нажатие на значок во весь экран должно СКРЫТЬ заголовок и временную шкалу
- Нажатие на значок «Полноэкранный режим» в полноэкранном режиме должно отобразить заголовок и временную шкалу

Флаги

Флаги используются для того, чтобы отметить интересные события и вернуться к ним позже.

При нажатии на значок «Флаг», выделенный серым цветом, должен появиться флаг на событии и на временной шкале.

При нажатии на значок с изображением флага он должен исчезнуть с события и временной шкалы.

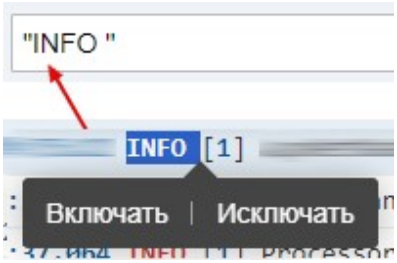


Перейти к позиции в логе

Когда вы найдёте интересное событие, вы можете просмотреть исходный лог-файл, то есть события, которые происходили непосредственно до и после этого события.

При нажатии на значок «Перейти к позиции в логе» открывается ещё одна вкладка браузера с фильтром по файлу лога, к которому относится исходное событие. Исходное событие также помечается флажком.

Включить / Исключить выбор



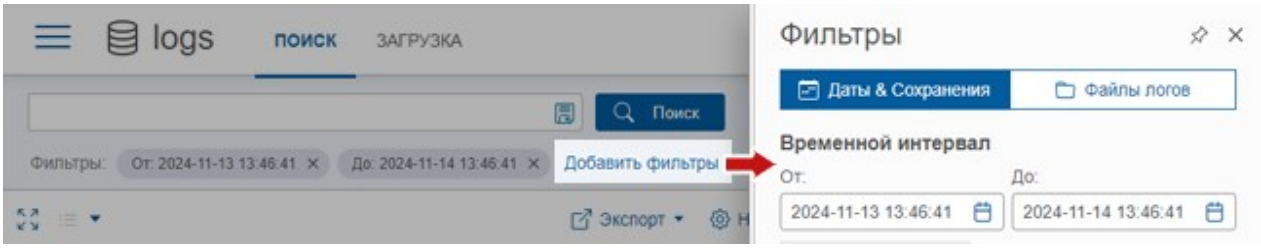
При выборе текста в результатах поиска появляется всплывающее окно «Включить/исключить»:

- При нажатии на «Включить» выбранный текст будет добавлен в поисковый запрос.
- При нажатии на «Исключить» выбранный текст будет добавлен в запрос с оператором «-» (НЕ).
- Щелчок за пределами всплывающего окна скроет всплывающее окно и удалит выделение.

Панель фильтров

Панель «Фильтры» открывается нажатием на ссылку «Добавить фильтры» под строкой поиска. На этой панели находятся:

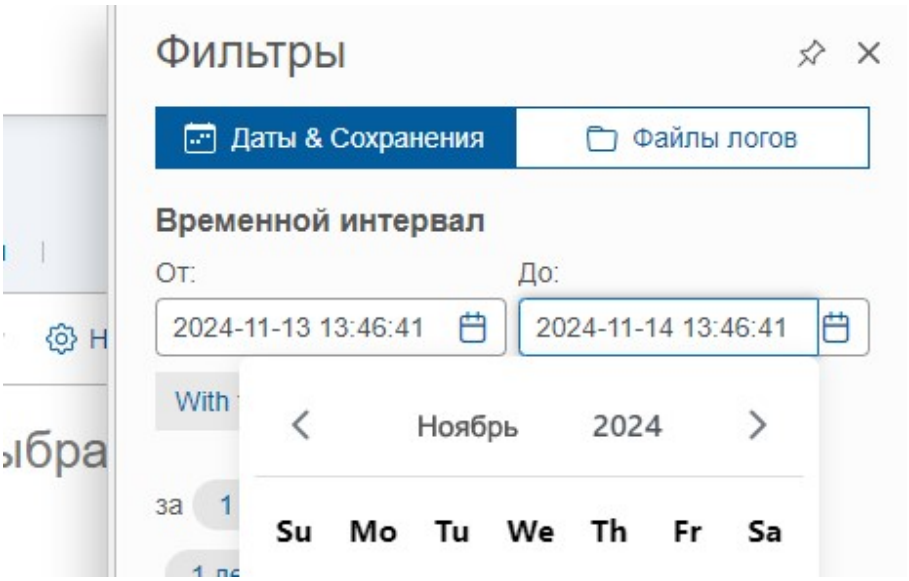
- Фильтр по времени
- Фильтр файлов
- Сохраненные поиски



Фильтр по времени

Фильтр времени позволяет указывать временные метки От и До с помощью:

- элементов управления календарем
- прямым редактированием
- выбор предопределенных интервалов



По умолчанию временная метка «До» устанавливается на временную метку последнего известного события в текущей базе данных.

По умолчанию отметка времени «От» устанавливается на 1 день раньше отметки времени «До».

Скорость поиска во многом зависит от временного фильтра, поэтому установите его на разумное значение, чтобы поиск был быстрее.

Только с метками времени

- Если установлен флажок «Только с метками времени», отображаются только события с обнаруженными метками времени.

Например, если есть файл лога CSV, в котором первая строка содержит заголовки столбцов, то эта строка не будет отображаться.

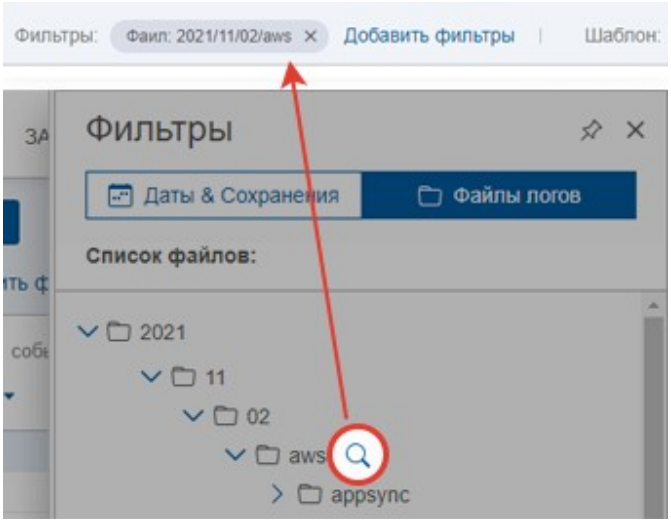
- Если не установлен флажок «Только с метками времени», то события без отметок времени тоже будут отображаться .

Фильтр файлов

Для базы данных, настроенной для ручной или автоматической загрузки логов, на этой панели будет отображаться простой список загруженных файлов логов. Для внешних баз данных — дерево папок и файлов.

- Значок поиска в папке применяет фильтр ТОЛЬКО к этой папке
- Значок поиска в файле применяет фильтр ТОЛЬКО к этому файлу

Фильтр файлов отображается в виде значка под строкой поиска и может быть удалён.

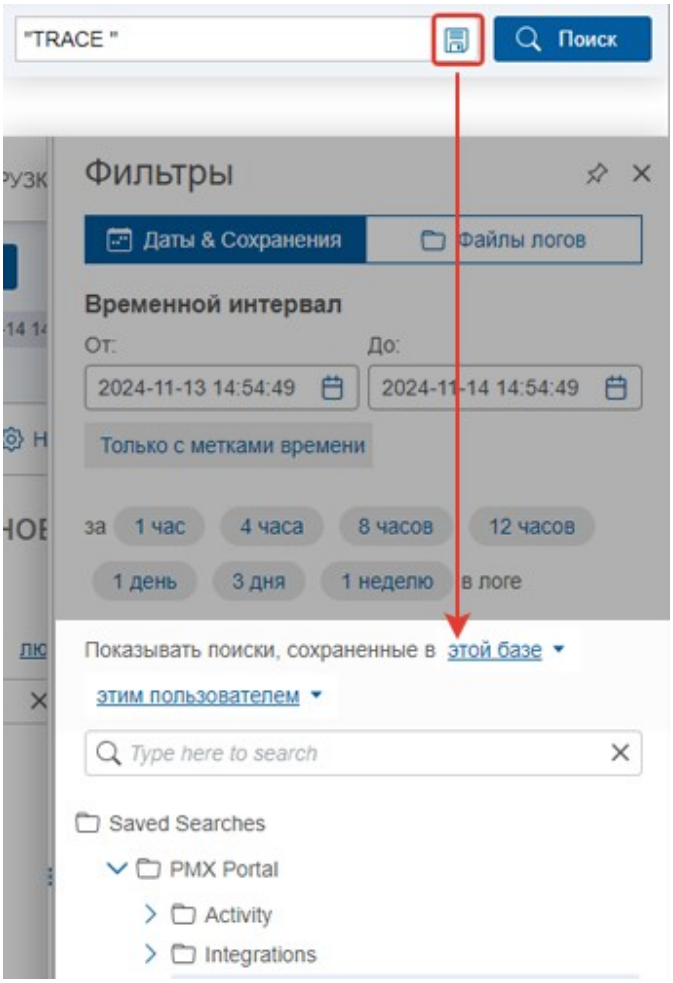


Фильтр файлов также можно указать как часть поискового запроса, например «file:lambda*», см. главу «Синтаксис поискового запроса».

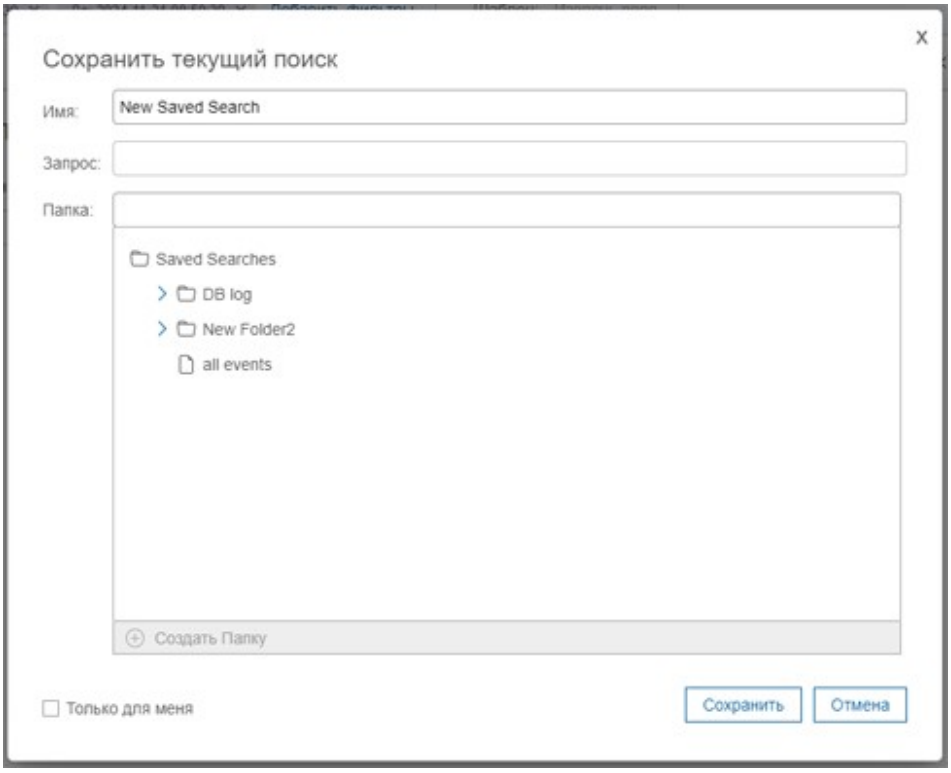
Сохраненные поиски

*Только для роли администратора или автора.

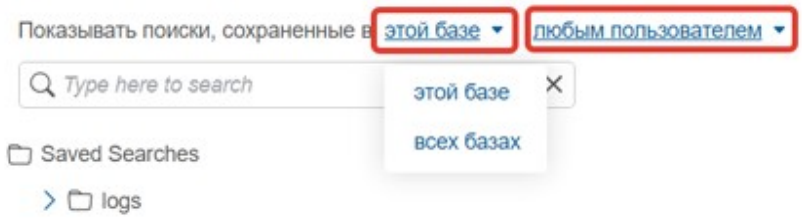
Вы можете сохранить свой поисковый запрос для повторного использования его позже.



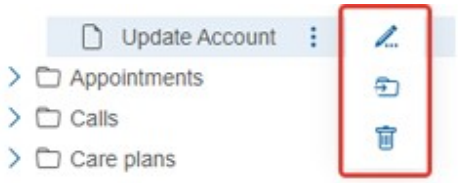
- Чтобы сохранить поиск, нажмите на значок диска в правой части панели поиска. Появится всплывающее окно с сохранением поиска с названием поиска и запросом. Название сохраненного поиска по умолчанию совпадает с запросом, но его можно изменить.
- Пожалуйста, введите путь или выберите папку в дереве, чтобы указать путь к сохранённому поиску.
- Вы также можете установить флажок «Сохранить только для меня», и тогда другие пользователи не увидят его.



- По умолчанию в дереве «Сохранённые поиски» содержатся поисковые запросы для этой базы данных и для всех пользователей. Вы можете изменить это, используя фильтры над деревом.

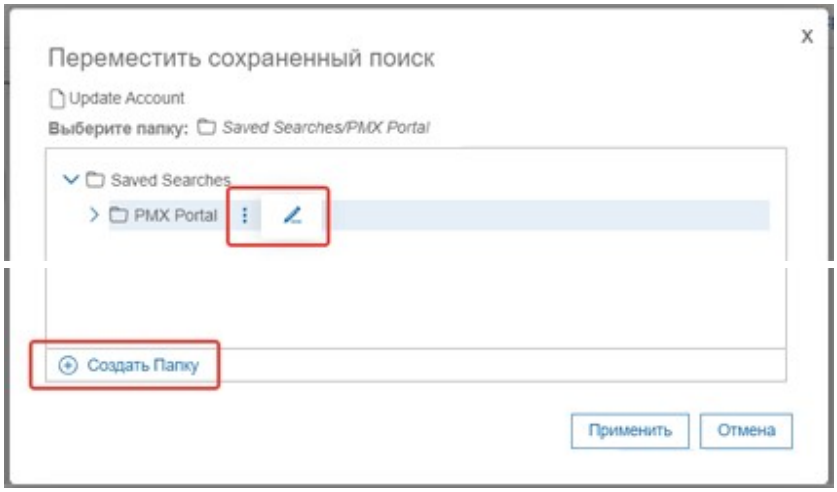


- Запустить сохранённый поиск можно нажав на название в дереве.
  - Если в поисковом запросе были указаны фильтры по времени и по файлам, они будут применены.
  - Если нет, то будут применены текущие фильтры времени и файлов.

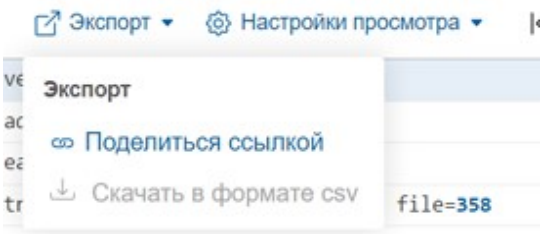


- Чтобы переименовать сохранённый поиск, выберите «Переименовать» в меню, кликнув по трём точкам. Введите новое название в поле.

- Чтобы удалить сохранённый поиск, выберите «Удалить» в меню, кликнув по трём точкам.
- Чтобы переместить сохраненный поиска: выберите «Переместить сохраненный поиск» в меню, кликнув по трём точкам.
    - В открывшемся диалоговом окне «Переместить сохранённый поиск» вы можете выбрать папку назначения, а также добавить новую папку или переименовать существующую.



Меню экспорта

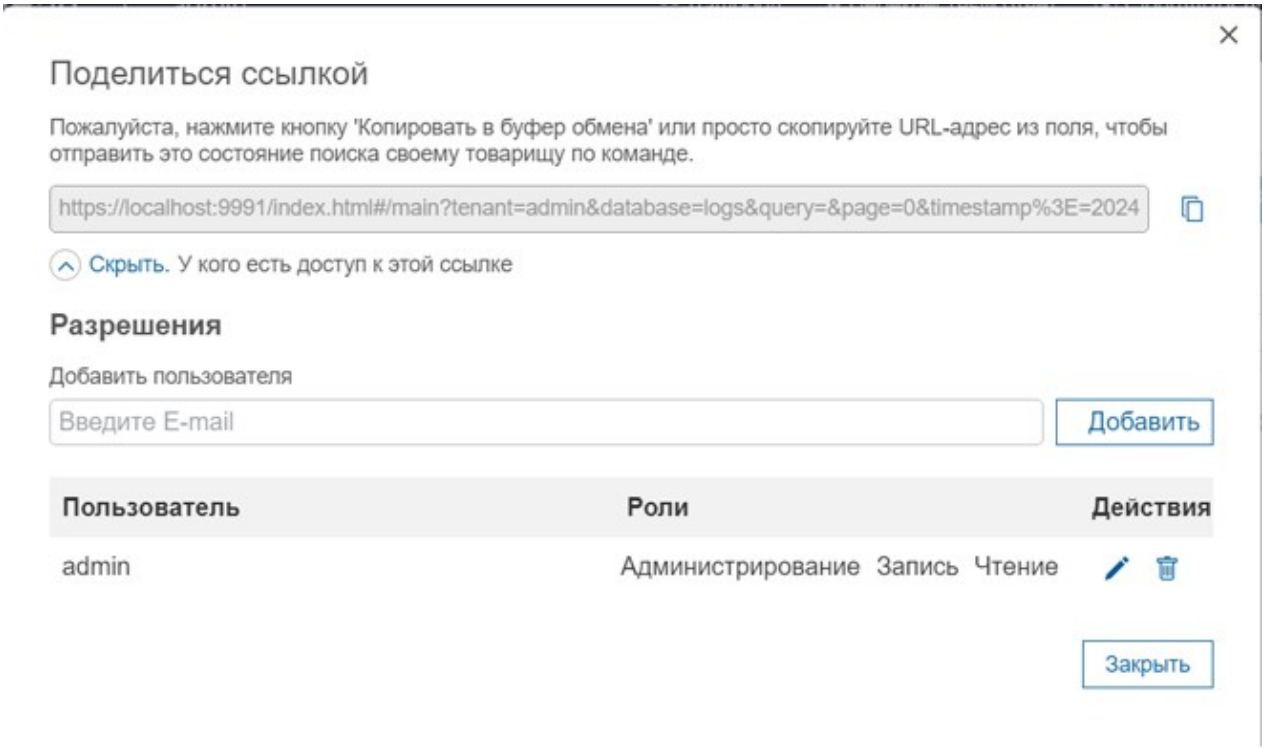


Вы можете экспортировать результаты поиска двумя способами:

- Поделитесь ссылкой для поиска
- Загрузить в формате CSV

Поделиться ссылкой

Команда «Поделиться ссылкой» открывает диалоговое окно с ссылкой для поиска. Ссылка содержит URL-адрес сервера, репозиторий, имя базы данных, поисковый запрос и фильтры, поэтому для запуска поиска достаточно одного клика.



В диалоговом окне "Поделиться ссылкой":

- Щелкните значок Копирования, чтобы скопировать общую ссылку в буфер обмена
- Посмотрите на таблицу ниже, чтобы убедиться, что у предполагаемых получателей есть как минимум разрешение на чтение текущей базы данных. Если у кого-то из них его нет, вы можете прямо там предоставить им разрешение на чтение.

Загрузить в формате CSV

«Скачать как CSV» — загрузит результаты поиска в виде CSV-файла. Для этого необходимо применить шаблон, чтобы результаты поиска были представлены в виде таблицы. См. главу «Применение шаблона».

Применить шаблон

Применение шаблона полезно для преобразования неструктурированных данных лога в формат структурированной таблицы.

Например, если результаты вашего поиска:

2023-10-10 14:26:23.383 INFO [61] Audit: user started search in admin/logs: 'out of memory'
2023-10-10 14:28:52.873 INFO [42] Audit: user started search in admin/logs: 'access denied'

Затем применяем шаблон:

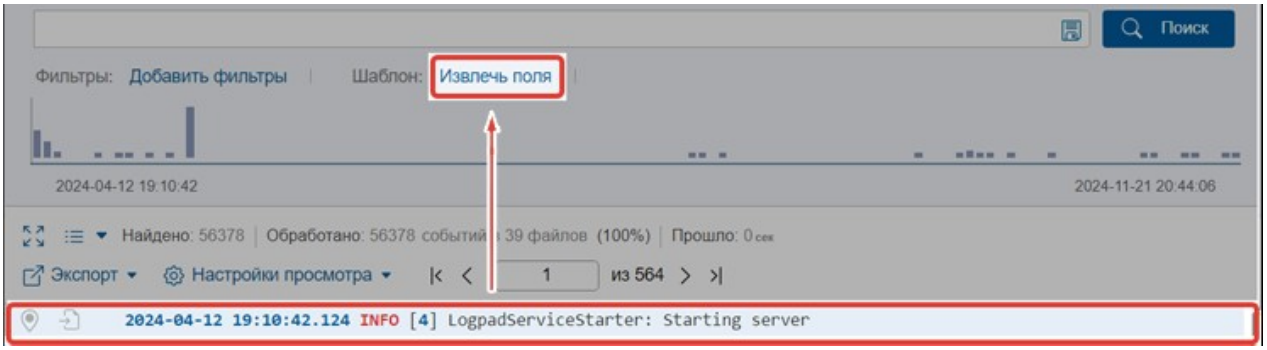
{Date} {Time} INFO [{}] Audit: user started search in admin/logs: {Search}

Это создаст таблицу, подобную:

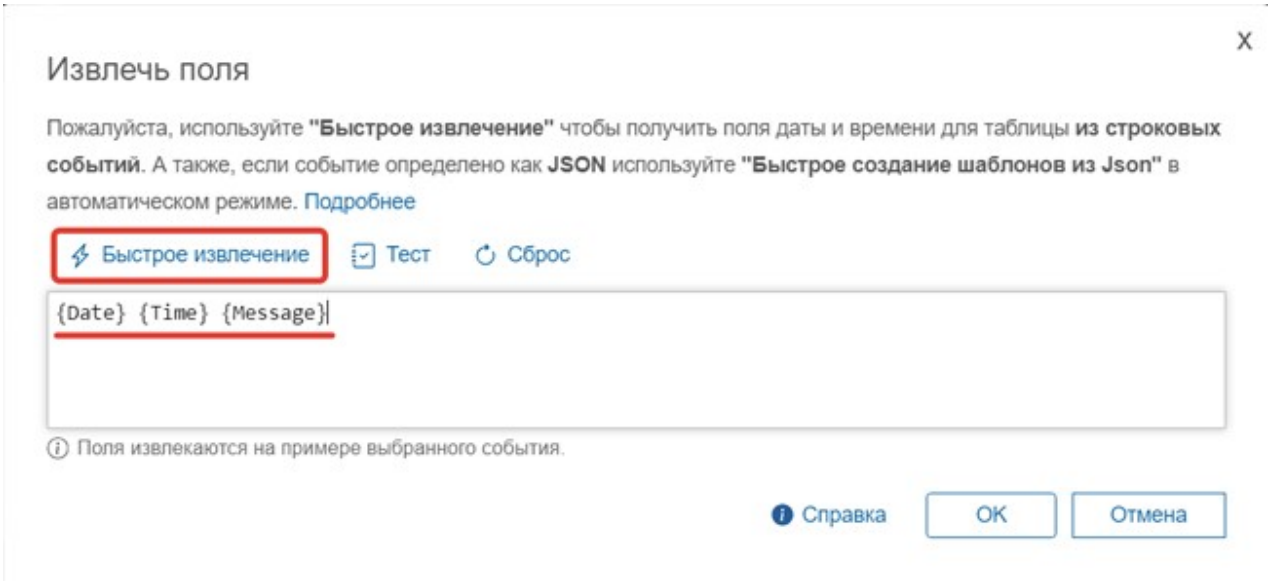
Date	*Time*	*Search*
10.10.2023	*14:26:23.383*	*out of memory*
10.10.2023	*14:28:52.873*	*access denied*

Как применить шаблон

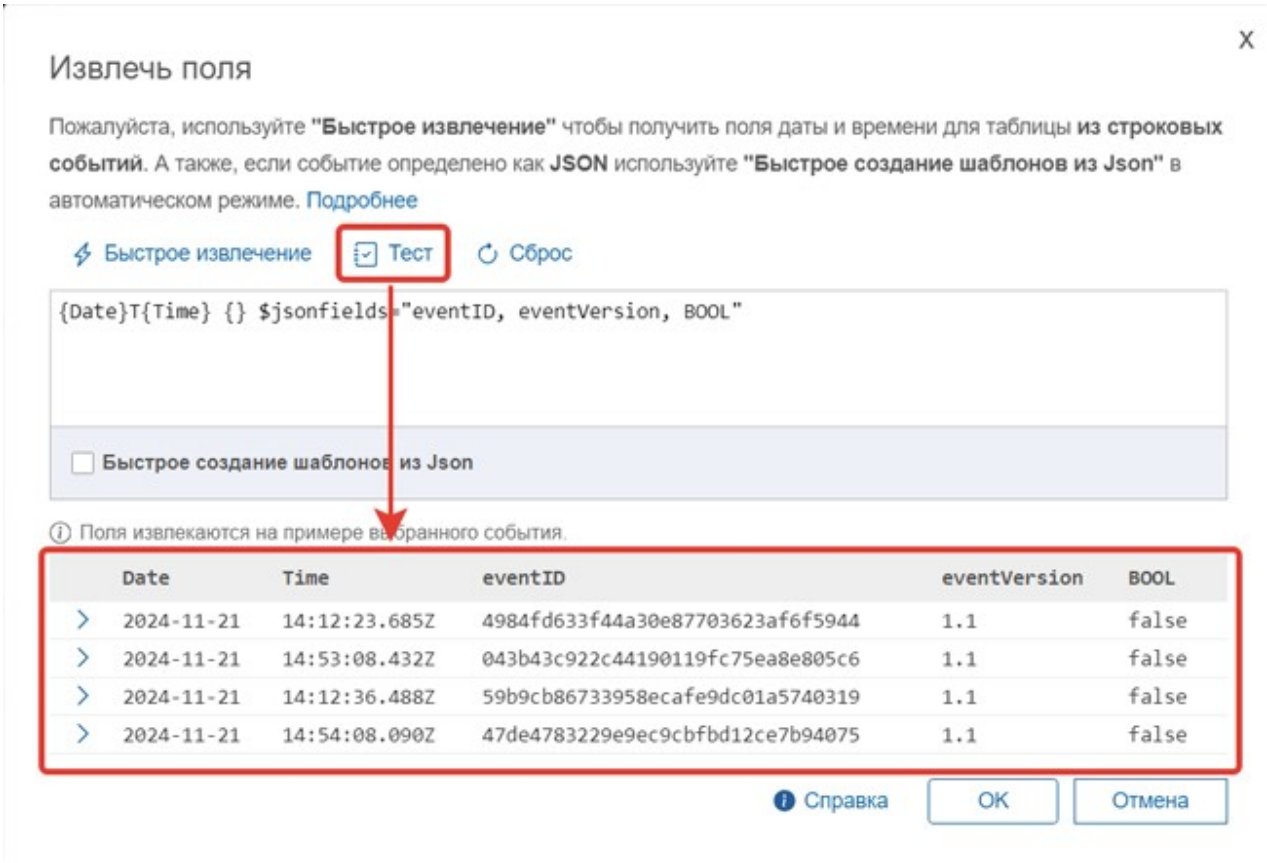
- Убедитесь, что результаты поиска более или менее однородны и соответствуют одному шаблону. Строки, которые не соответствуют шаблону, будут отображаться как пустые. Уточните запрос и добавьте больше фильтров, чтобы получить более однородные результаты.
- Выберите строку и нажмите кнопку «Извлечь поля». Должно появиться диалоговое окно для извлечения.



- **"Быстрое извлечение"** кнопка применяет простой шаблон **{date}{time}{message}**.



- **«Тест»** показывает результат применения шаблона к 1–4 ближайшим событиям.



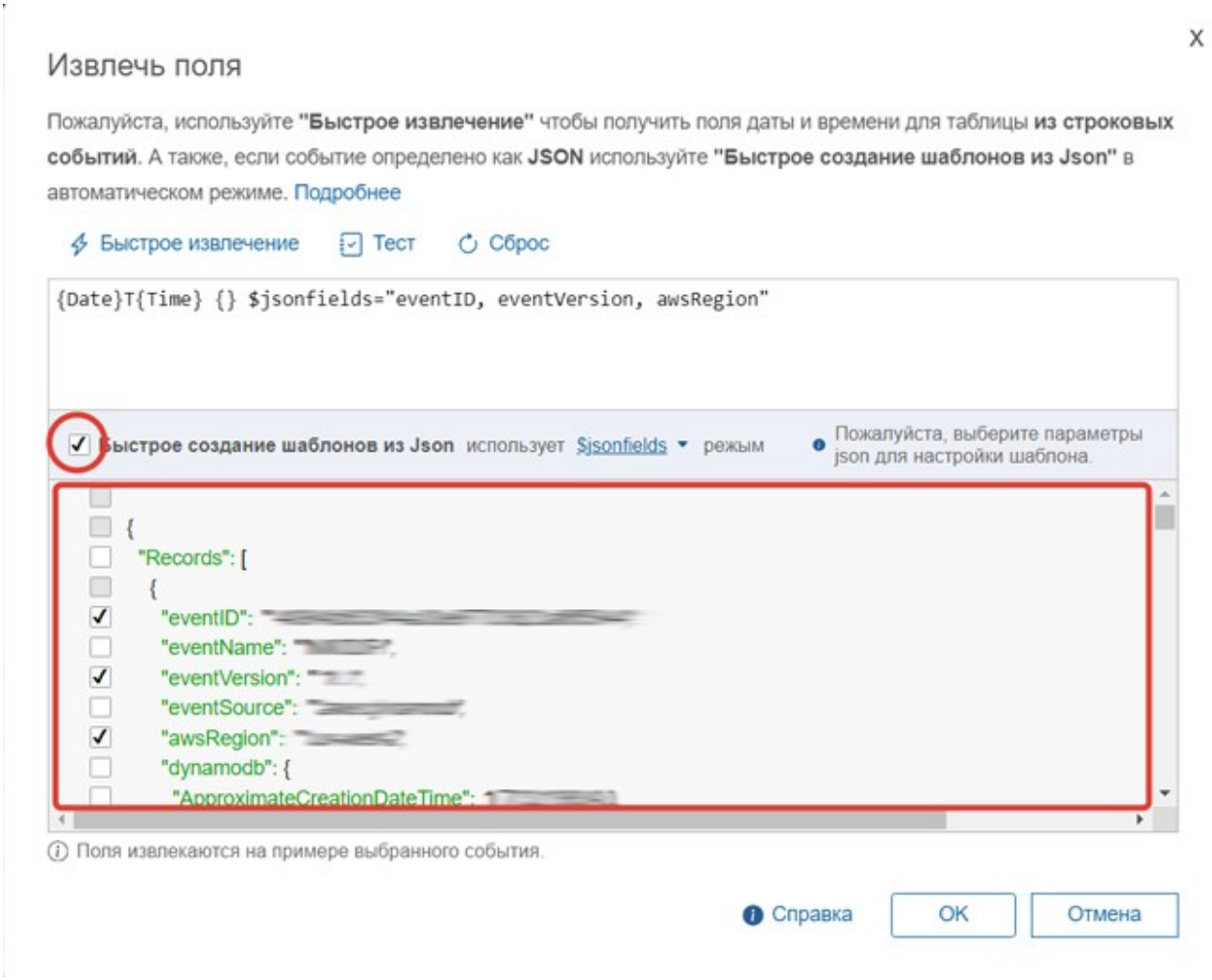
- Если событие распознано как JSON — попробуйте **режим JSON**, у него есть три варианта: **автоматический**, **$jsonfields** и **универсальный** шаблон.

    - В автоматическом режиме тип шаблона выбирается автоматически между «$jsonfields» и «универсальным» в зависимости от выбранных полей JSON.

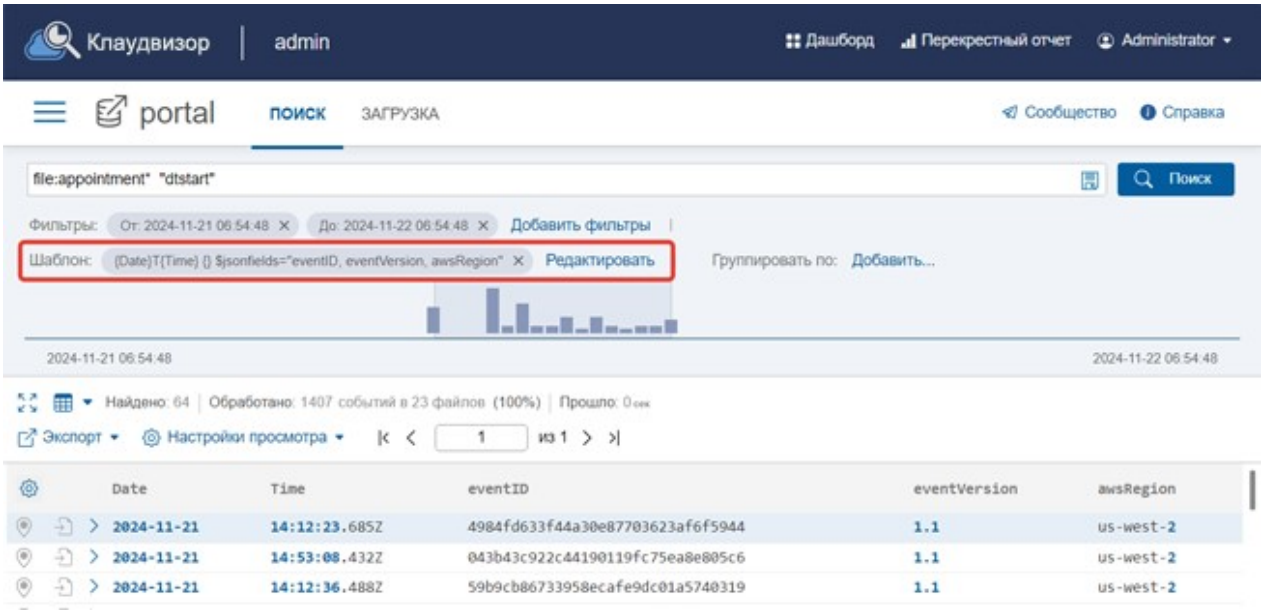
    - Шаблон $jsonfields имеет более простую форму записи, например **$jsonfields="имя_поля_1, имя_поля_2, имя_поля_3, ..."** где перечислены имена полей JSON.
      Примечание: шаблон $Jsonfieds не поддерживает объекты JSON и массивы JSON.

    - Для универсального шаблона замените части, которые нужно извлечь, выражениями **{имя_поля}**. Например, если текст выглядит так: "user=john age=23" то шаблон `**user={user} age={age}**` извлечёт поля **john** and **23**.

      Выберите соответствующие поля JSON, и шаблон изменится соответствующим образом/В активном шаблоне должен отображаться значок (применить шаблон).

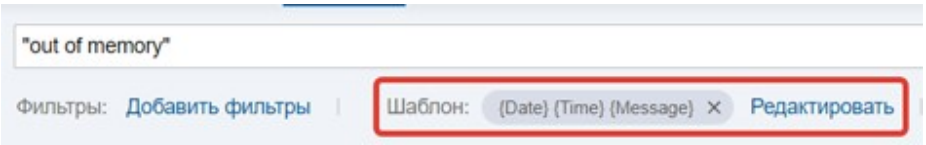


- Нажмите «Применить», чтобы применить шаблон. Будет выполнен ещё один поиск на сервере, но с применением шаблона. Результаты появятся в режиме таблицы. Активный шаблон будет отображаться под строкой поиска.



Редактировать и удалять шаблон

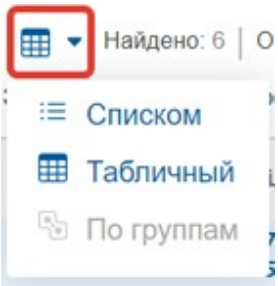
Активный шаблон отображается под строкой поиска. Нажмите на крестик, чтобы удалить его, и результаты вернутся в режим просмотра списка. Нажмите «Изменить», чтобы отредактировать шаблон.



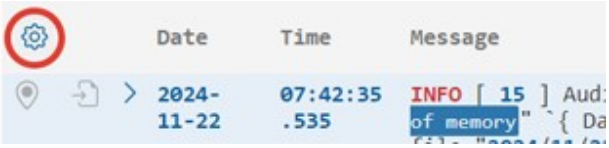
Просмотр таблицы

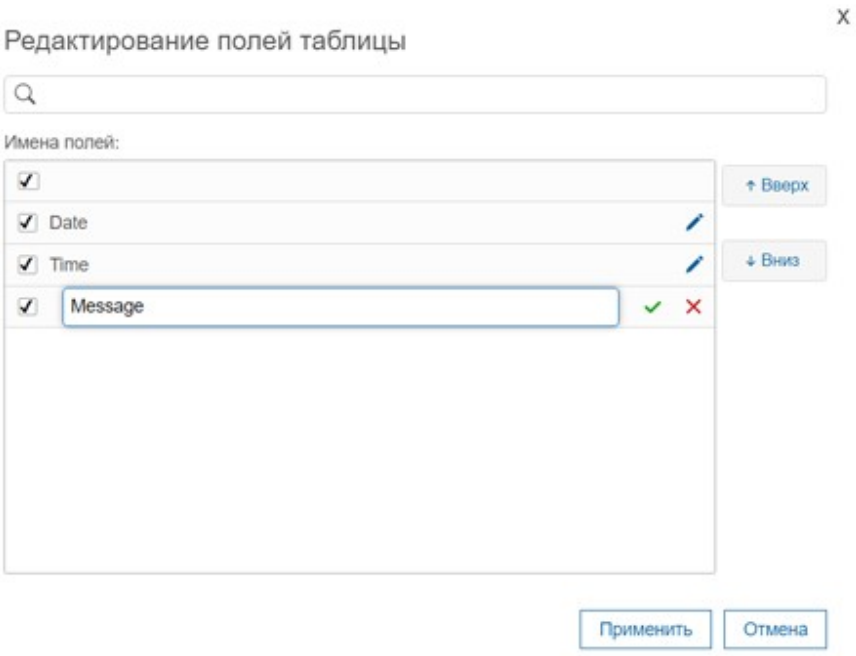
Просмотр таблицы должен включаться автоматически при применении шаблона.

Вы можете переключаться между представлением таблицы и списка, нажав кнопку Переключения вида.



В диалоговом окне "Столбцы" вы можете





- показывать / скрывать столбцы
- изменить порядок столбцов
- переименовывать столбцы

Вы также можете скрывать и переименовывать столбцы, нажимая на заголовки столбцов

Группировать

Команда «Группировать по» полезна для расчёта группировок по результатам поиска. Команда доступна только при использовании шаблона.

Например, если результаты вашего поиска:

Date	*Time*	*User*	*Site*	*Search*
10.10.2023	*14:26:23.383*	*Admin*	*Root*	*out of memory*
10.10.2023	*14:28:52.873*	*User1*	*Landing*	*access denied*
10.10.2023	*14:36:23.383*	*Admin*	*Root*	*out of memory*
10.10.2023	*14:58:52.873*	*Admin*	*Landing*	*bad request*

Вы можете получить такую статистику, сгруппировав данные по различным столбцам, например “user”, “site” или “search”:

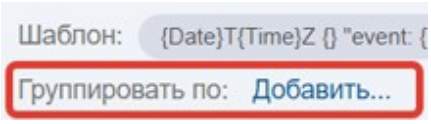
User	*Count*
Admin	3
User1	1

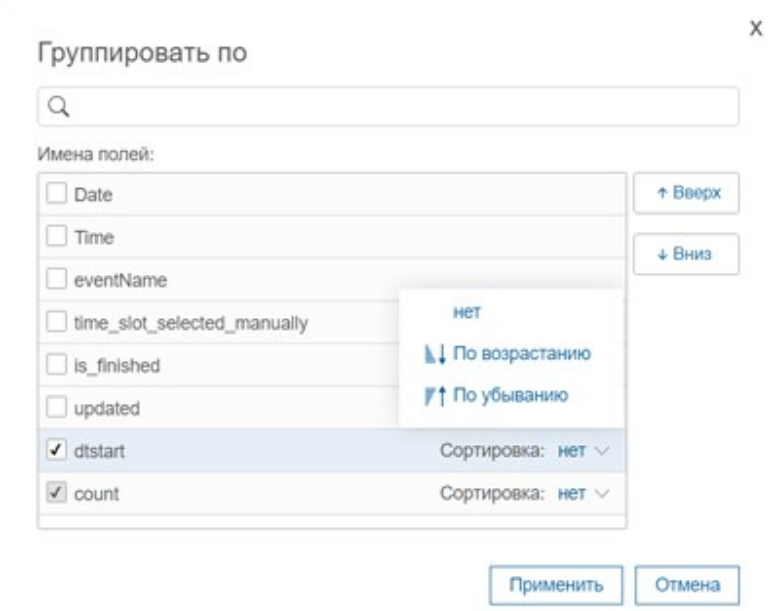
Site	*Count*
Root	2
Landing	2

Search	*Count*
out of memory	2
access denied	1
bad request	1

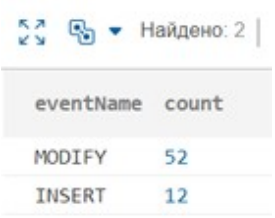
Как применить Группировку

Кнопка «Группировать по: **Добавить**» открывает диалоговое окно «Группировать по». В текущей версии вы можете выбрать только один столбец для группировки и единственную доступную агрегатную функцию «Количество». Вы можете сортировать по выбранному столбцу (по возрастанию/убыванию) или по количеству (по возрастанию/убыванию).



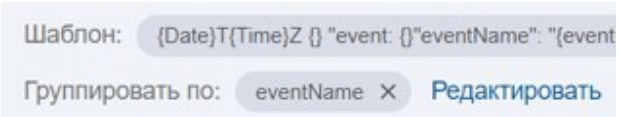


Нажмите «Применить», чтобы запустить агрегированный поиск на сервере и отобразить результаты в виде таблицы с отдельными значениями выбранного столбца и подсчётом для каждого значения этого столбца.



Количество отображается в виде ссылок. При нажатии на ссылку открывается другая вкладка браузера с поиском по отдельным значениям столбца.

«Группировать по» отображается в виде чипса под строкой поиска. При нажатии на ссылку «Изменить» должно открыться диалоговое окно «Группировать». При удалении значка вы вернётесь в режим просмотра таблицы.

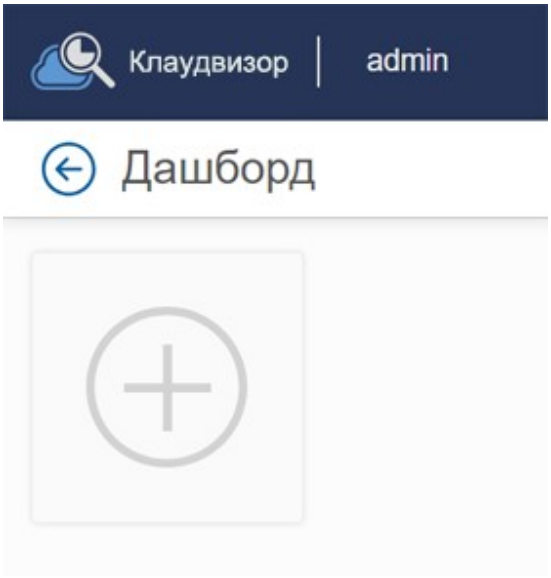


Вы можете переключаться между режимами «Группировка», «Таблица» и «Список» или между режимами одного и того же запроса с помощью кнопки «Режим».

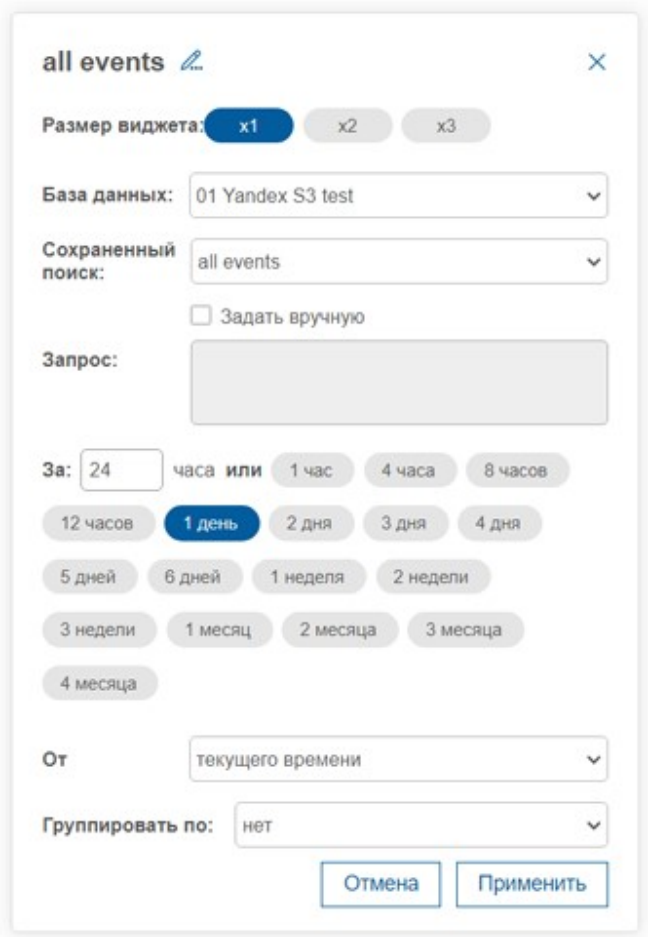
Дашборд

Вы можете использовать сохранённые поисковые запросы для отображения в виде диаграмм на Дашборде. Дашборд создаётся для каждого пользователя.

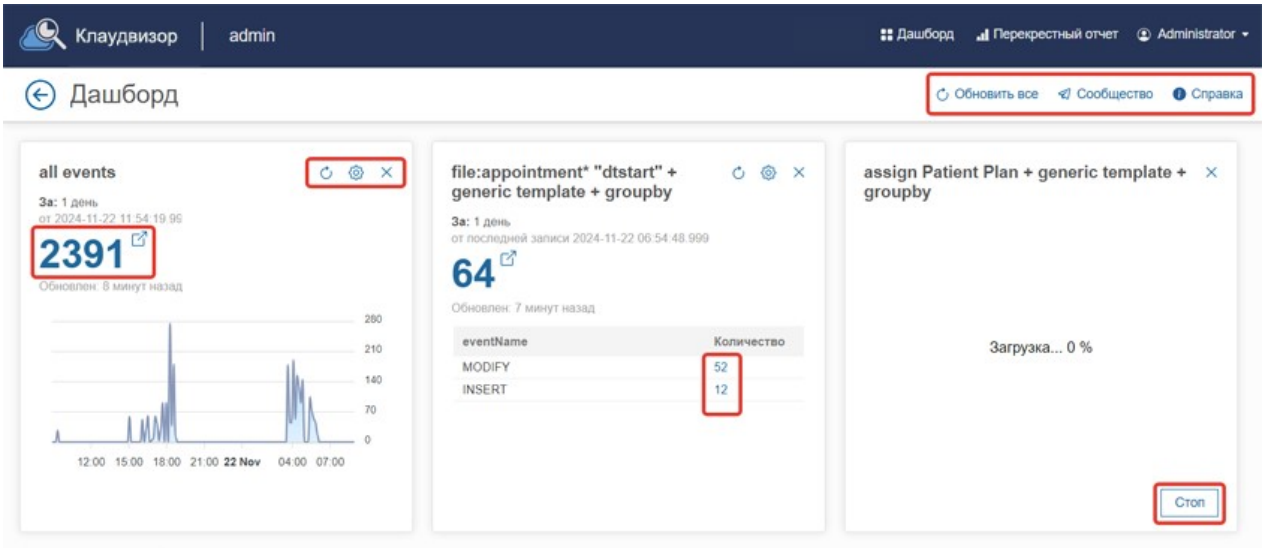
Добавление нового виджета



Нажмите на ссылку «Дашборд» в главной панели, чтобы перейти на Дашборд. Нажмите на значок «+» для создания нового виджета, отобразится страница настроек.



- Выберите ширину виджета: x1, x2 или x3 должны отображать виджет нужного размера.
- Выберите используемую базу данных. По умолчанию выбрана текущая база данных.
- Выберите сохранённый поисковый запрос, который нужно выполнить в этом виджете, или введите новый поисковый запрос.
- Укажите временные рамки в часах или используйте предопределенные временные рамки
- Если в вашем поисковом запросе есть опция «Группировать по», вы сможете указать количество первых N результатов, которые будут отображаться в виджете.
- Если в вашем поисковом запросе не было опции «Группировать по», вы можете указать интервал группировки для отображения диаграммы:
    - Опция “Не группировать” должна отображать график сплошной линией
    - Опция “День” должна отображать столбцы по дням
    - Опция “Неделя” должна отображать столбцы по неделям
    - Опция “Месяц” должен отображать столбцы по месяцам
- Нажмите кнопку «Применить», чтобы запустить запрос. Виджет отобразит ход поиска. Виджет отображает диаграмму (или топ-N) и общее количество найденных событий.
- Вы можете перейти от панели управления к событиям, нажав на номер в виджете или значок в виде квадрата со стрелкой.



Обновление данных

Результаты в виджетах кэшируются до тех пор, пока не будет выполнено ручное обновление. В виджете указано, насколько старые данные отображаются. Вы можете обновить все виджеты одновременно, нажав кнопку «Обновить все». Вы можете обновить виджеты по отдельности, нажав значок «Обновить» в виджете.

Редактирование виджетов

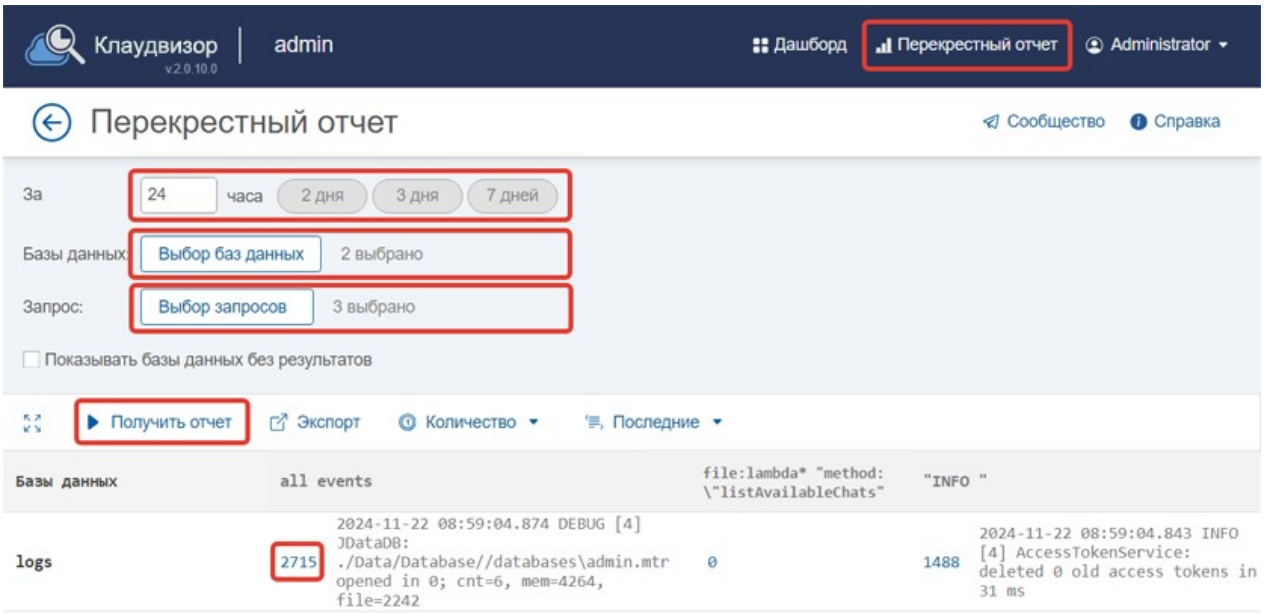
- При нажатии на значок крестика появится запрос на удаление виджета
- При нажатии на значок Настроек откроется панель настроек.

Перекрестный отчет

Отчет по разным базам данных полезен, когда вы используете базы данных в качестве контейнеров для похожих логов, но у разных создателей (разные клиенты, разные местоположения, разные серверы). Например, если вы настроили одну базу данных для каждого клиента и настроили загрузку логов по сценарию от каждого клиента в отдельную базу данных. Затем, если у одного клиента возникла проблема, вы можете увидеть это в логах и вы можете найти, какие другие клиенты сталкиваются с такой же проблемой.

Отчёт по нескольким базам данных выполняет выбранные сохранённые поисковые запросы по указанному количеству баз данных и отображает количество событий, найденных каждым запросом в каждой базе данных.

Запуск Перекрестного отчета



- Нажмите на ссылку "Перекрестный отчет" в главной панели.
- Укажите временной интервал: введите количество часов в поле для ввода или нажмите на значок
- Выберите одну или несколько баз данных для выполнения запроса
- Выберите один или несколько сохраненных поисковых запросов
- Нажмите кнопку Получить отчет

В итоговом отчёте строки будут представлять собой базу данных, а столбцы — поисковые запросы. В ячейках будет отображаться количество найденных событий. Вы можете нажать на число и открыть этот набор данных в отдельной вкладке браузера.

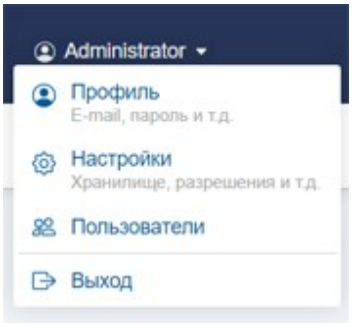
Опция «Показывать базы данных без результатов» позволяет отображать или скрывать базы данных, в которых не найдено ни одного события.

Экспорт данных

Вы можете нажать кнопку «Экспорт», чтобы загрузить CSV-файл с результатами отчета.

Меню профиля

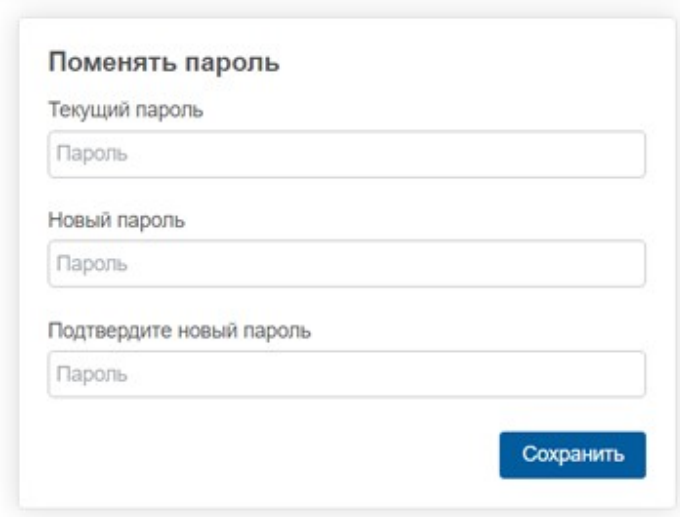
Меню учётной записи пользователя отображается при нажатии на значок профиля в правом верхнем углу. Содержимое меню зависит от роли пользователя.



- Для всех типов пользователей отображается команда выхода из системы.
- Для внутренних пользователей, владеющих репозиторием, также отображаются команды профиля и Настроек.
- Для администратора продукта (пользователя “admin”) – также отображается команда Users

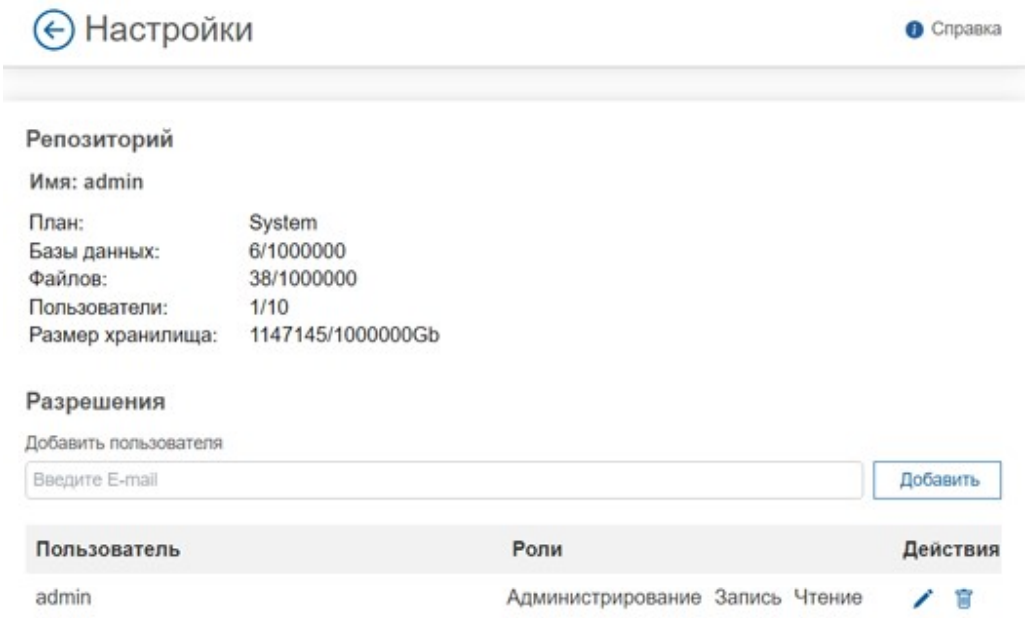
Раздел Профиль

Раздел «Профиль» отображается для внутренних пользователей в меню пользователя. Он открывает экран «Профиль», на котором можно изменить пароль пользователя. Внешние пользователи, например пользователи Active Directory - не имеют профиля.



Раздел Настройки

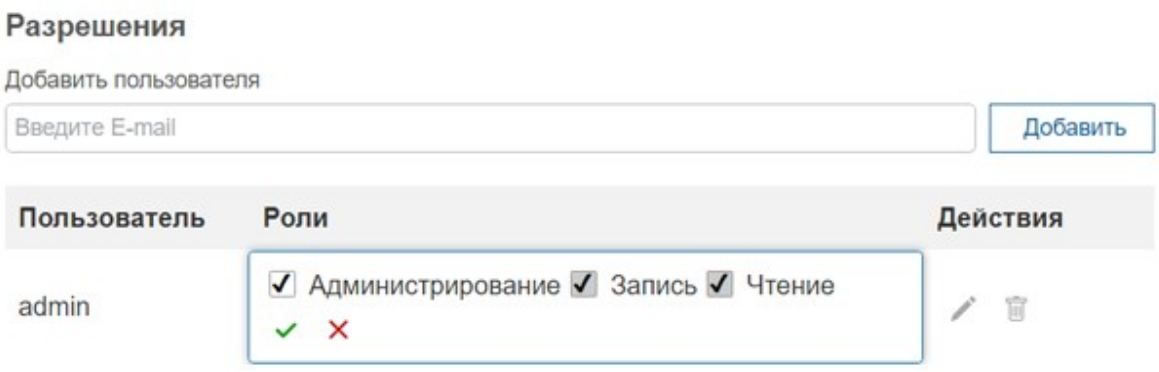
Раздел «Настройки» отображается для внутренних пользователей в меню пользователя. Он открывает экран «Настройки», на котором отображается:



- Лицензионный план (бесплатный, платный и т.д.)
- Собственная статистика хранилища: количество баз данных, файлов, пользователей с доступом, размер хранилища.
- Список пользователей (внутренних и объединённых) с разрешением на доступ к собственному репозиторию.

Предоставление доступа к собственному репозиторию

В разделе «Разрешения» на экране «Настройки» отображается список пользователей, имеющих доступ к собственному репозиторию. Вы можете добавлять/удалять внутренних и внешних пользователей и изменять их роль в собственном репозитории:



- Чтение
  - можно просматривать базы данных, выполнять поиск, просматривать панель управления, просматривать отчёты по нескольким базам данных

    - нельзя создавать/удалять/редактировать базы данных и загружать логи в существующие базы данных, сохранять запросы
    - нельзя предоставить разрешения для репозитория
- Запись
    - можно просматривать базы данных, выполнять поиск, просматривать панель управления, просматривать отчёты по нескольким базам данных
    - можно создавать/удалять/редактировать базы данных и загружать логи в существующие базы данных, сохранять запросы
    - нельзя предоставить разрешения для репозитория
- Администратор
    - можно просматривать базы данных, выполнять поиск, просматривать панель управления, просматривать отчёты по нескольким базам данных
    - можно создавать/удалять/редактировать базы данных и загружать логи в существующие базы данных, сохранять запросы
    - может предоставлять разрешения для репозитория

Администрирование

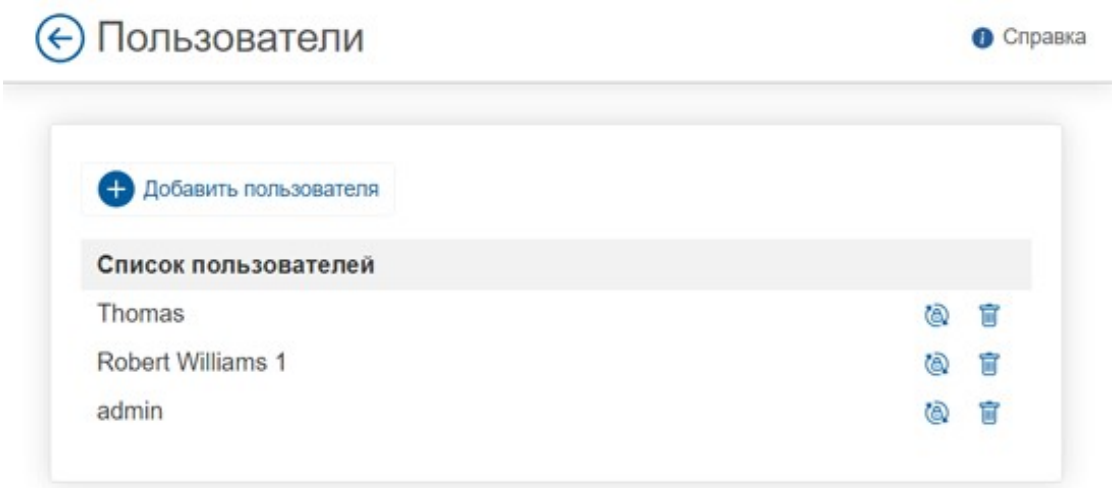
Первый вход в систему

После установки единственным доступным пользователем является «admin» с паролем «admin». Этот пользователь является суперпользователем.

Измените пароль администратора по умолчанию

После первого входа в систему пароль администратора необходимо немедленно изменить. Нажмите на значок «Профиль», выберите команду «Профиль» и измените пароль.

Раздел Пользователи



- Внутренние пользователи могут владеть репозиторием с логами
- Пользователи Active Directory — это «внешние» пользователи, которым может быть предоставлен доступ к репозиториям, принадлежащим внутренним пользователям.

  -->

Только пользователь с правами администратора может добавлять или удалять внутренних пользователей и сбрасывать их пароли. Чтобы добавить внутреннего пользователя, нажмите «Пользователи» в меню «Профиль». Вы можете добавлять и удалять внутренних пользователей и изменять их пароли.

Настройка доступа для пользователей Active Directory

Если ПО «Клаудвизор» установлен в домене Active Directory, пользователям домена можно предоставить доступ к репозиториям. Администратор репозитория должен нажать «Настройки» в меню «Профиль» и ввести «домен\пользователь» при добавлении нового разрешения.