Руководство пользователя ИндексЛог

СОДЕРЖАНИЕ

1 ВВЕДЕНИЕ

Пользователь системы ИндексЛог – аналитик данных, в его обязанности входит анализ данных, хранящихся в системе, построение визуализаций, создание информационных панелей – дашбордов – из этих визуализаций. Для выполнения этих обязанностей ему предоставляется доступ к чтению данных и доступ к построению визуализаций. Также пользователь в соответствии со своей должностью и областью ответственности может иметь доступ к встроенным информационным панелям приложений APM, Инфраструктурного мониторинга, Мониторинга доступности и приложениям Безопасности. Краткие инструкции по пользованию этими приложениями включены в решение, поэтому в данном Руководстве будет рассмотрено использование возможностей визуализации ИндексЛог_Аналитика.

2 ПРИНЦИП РАБОТЫ ВИЗУАЛИЗАЦИЙ В ИНДЕКСЛОГ_АНАЛИТИКА

Решение ИндексЛог_Аналитика представляет собой фронтэнд приложение стека ИндексЛог. Его основные функции – упрощение отправки в ИндексЛог_Поиск REST API-запросов и визуализация результатов, возвращаемых ИндексЛог_Поиск.

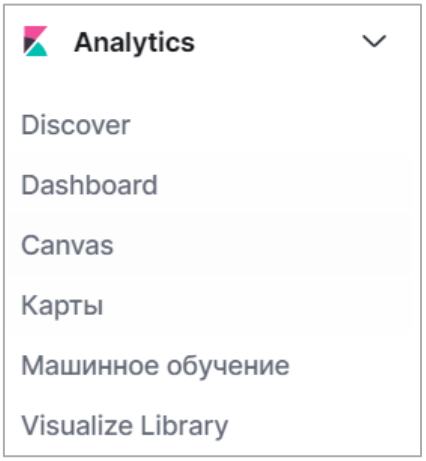
Поисковые запросы ИндексЛог_Поиск имеют два типа: search и aggregation. Запросы типа aggregation используются для распределения на группы, суммирования и проведения математических и статистических операций над ними. Агрегации разбивают данные на bucket'ы и возвращают их в формате JSON. На основе bucket'ов и строятся все визуализации в ИндексЛог_Аналитика. Визуализации можно затем сохранить и добавить на информационную панель (далее - дашборд) для создания представления данных, удобного для анализа данных пользователя.

3 СОЗДАНИЕ ВИЗУАЛИЗАЦИИ В ИНДЕКСЛОГ_АНАЛИТИКА

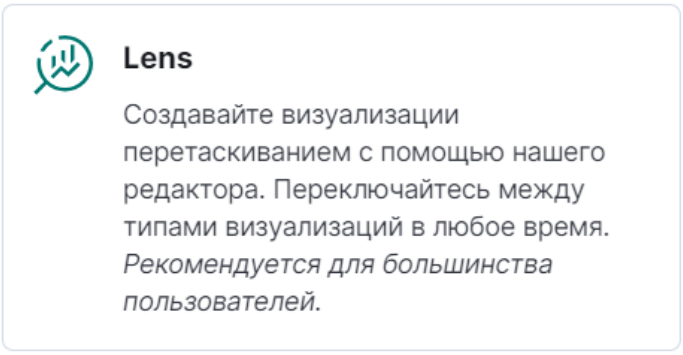
Вкладка Visualize позволяет создавать визуализации на основе запросов ИндексЛог_Поиск без необходимости создавать запрос вручную. Визуализации создаются в удобном интерфейсе и имеют широкие возможности настройки.

Для создания визуализации:

1. Откройте левую боковую панель навигации и кликните на вкладку «Visualize Library».

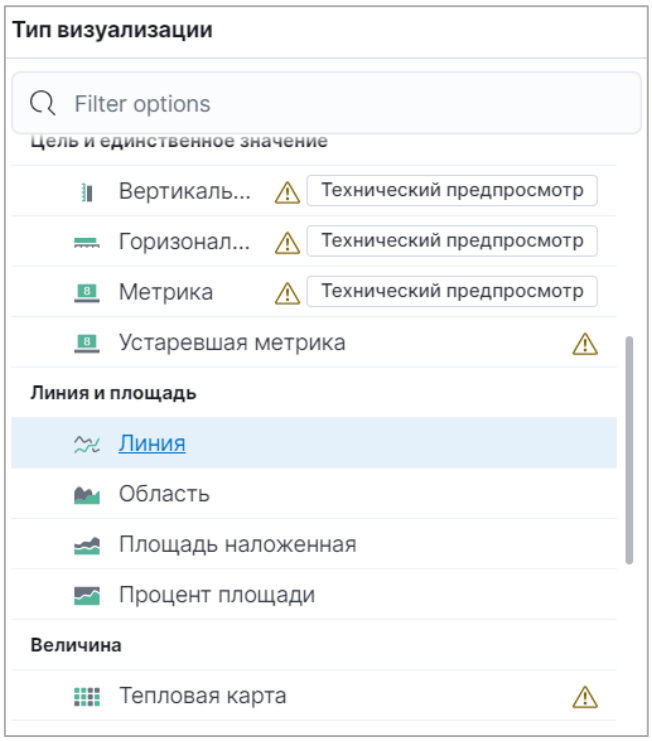


2. Нажмите кнопку «Создать визуализацию».
3. Выберите стандартный инструмент создания визуализаций «Lens».

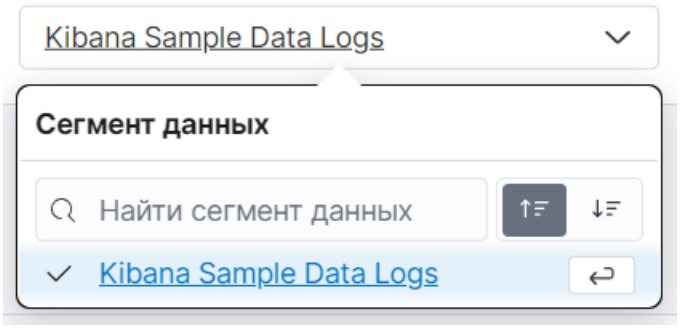


4. Выберите тип визуализации:

- таблица;
- гистограммы: вертикальные, вертикальные складываемые, процентные гистограммы вертикальные, горизонтальные, горизонтальные складываемые, процентные гистограммы горизонтальные;
- метрики и шкалы: вертикальные и горизонтальные шкалы, метрика;
- графики и области: графики, областные диаграммы, процентные областные диаграммы;
- тепловые карты;
- географические карты;
- пропорции: вафельные диаграммы, древовидные карты, кольцевые диаграммы, круговые диаграммы, мозаики.



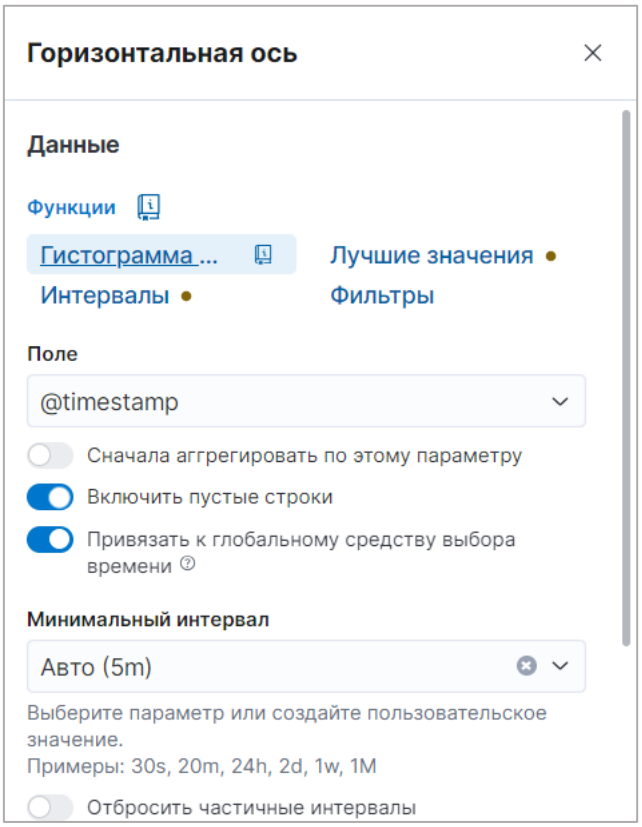
5. Выберите сегмент данных для визуализации.



6. Добавьте данные на вертикальную ось. Выберите метрику агрегации для оси Y визуализации:

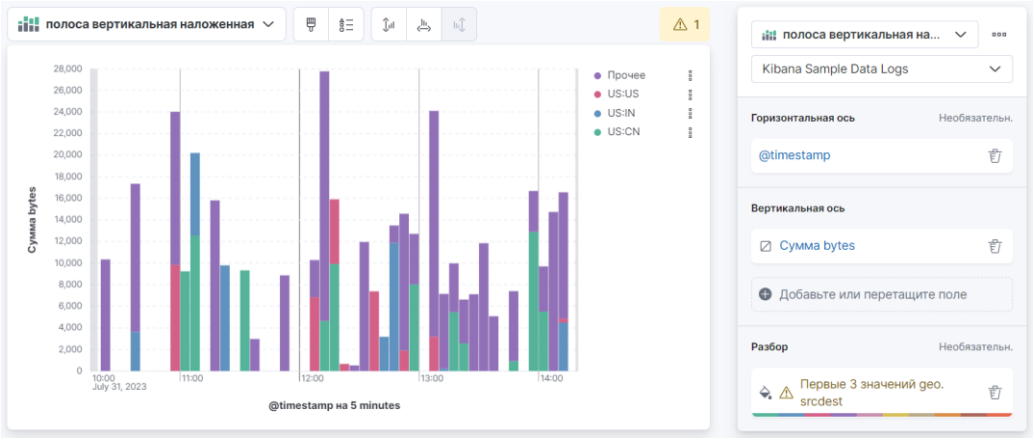
- метрические агрегации: подсчет, среднее, сумма, минимум, максимум, стандартное отклонение, количество уникальных значений, медиана (50%), процентные ряды, топ значений;
- агрегации родительских источников информации: производная, кумулятивная сумма, скользящее среднее, последовательный дифференциал;
- агрегации родственного источника: среднее по bucket'у, сумма по bucket'у, минимум и максимум по bucket'у.

7. Добавьте данные на горизонтальную ось. Выберите для оси X агрегацию по bucket'у: гистограмма дат, спектр, выражения, фильтры, знаковые выражения.



8. При необходимости добавьте данные для разбивки

В качестве примера построена агрегация типа «складываемая вертикальная гистограмма» на сегменте данных логов. Визуализация предоставляет количество байтов лога, полученные за выбранный период времени с разбивкой по направлению передачи данных.



Обзор параметров визуализаций в ИндексЛог.

Графики, диаграммы и областные диаграммы строятся по двум осям.

Для оси Y (вертикальной) доступны следующие агрегации:

- **Подсчет**. Агрегация подсчета возвращает чистый подсчет элементов в выбранном шаблоне индекса.
- **Среднее**. Данная агрегация возвращает среднее значение по числовому полю. Выбирайте поле из выпадающего списка.
- **Сумма**. Возвращает общую сумму по числовому полю. Выбирайте поле из выпадающего списка.
- **Минимум**. Возвращает минимальное значение по числовому полю. Выбирайте поле из выпадающего списка.
- **Максимум**. Возвращает максимальное значение по числовому полю. Выбирайте поле из выпадающего списка.
- **Кол-во уникальных значений**. Кардинальная агрегация возвращает число уникальных значений в поле. Выбирайте поле из выпадающего списка.
- **Стандартное отклонение**. Агрегация общей статистики возвращает стандартное отклонение данных в числовом поле. Выбирайте поле из выпадающего списка.
- **Лучшие значения**. Агрегация топовых значений возвращает один или больше топовых значений из специального поля в вашем документе. Выбирайте поле из выпадающего списка, тип сортировки документов, количество значений, которые нужно вернуть.
- **Процентиль**. Агрегация процентов разделяет значения числового поля на заданные диапазоны. Выбирайте поле из выпадающего списка, затем определите одну или больше областей в полях Процентили.
- **Процентильный ранг.** Агрегация процентного ранга возвращает процентное ранжирование по выбранному числовому полю. Выбирайте поле из выпадающего списка, затем определите один или больше значений процентного ранга в полях Значения.
- **Производная**. Агрегация производной подсчитывает производную определенных метрик.
- **Кумулятивная сумма**. Агрегация накопительной суммы подсчитывает накопительную сумму определенных метрик в родительской гистограмме.
- **Скользящее среднее**. Агрегация скользящего среднего будет вставлять окно сквозь данные и писать среднее значение этого окна.
- **Последовательное дифференцирование**. Последовательное дифференцирование — это метод, где значения во временном ряде отнимаются от самых себя в другой временной период или задержки.
- **Среднее по bucket'у**. Среднее сегмента вычисляет среднее значение определенных метрик в агрегации родственных источников.
- **Сумма по bucket'у**. Высчитывает сумму значений определенной метрики в агрегации родственного источника.
- **Минимум по bucket'у**. Возвращает минимальное значение определенной метрики в агрегации родственного источника.
- **Максимум по bucket'у**. Возвращает максимальное значение определенной метрики в агрегации родственного источника.

По горизонтальной оси доступны следующие агрегации:

- **Временная гистограмма**. Временная гистограмма построена на основе числового поля и организована по дате. Вы можете определить временные рамки для интервалов в секундах, минутах, часах, днях, неделях, месяцах или годах.

Вы также можете определить интервал по умолчанию, выбрав Польз. в качестве интервала и указав число и единицу времени в текстовом поле. По умолчанию единицами временного интервала являются: s для секунд, m для минут, h для часов, d для дней, w для недель, y для лет. Различные единицы поддерживают различные уровни точности, вплоть до одной секунды. Интервалы подписываются в начале интервала, используя ключ-дату, который возвращается из ИндексЛог_Поиск. Для примера, на всплывающей подсказке для месячного интервала будет отображаться первый день месяца.

- **Гистограмма**. Стандартная гистограмма строится на основе числового поля. Определите целочисленный интервал для этого поля. Range. С помощью агрегации рангов вы можете определить ранги для значений числового поля. Кликните «Добавить диапазон» для добавления набора конечных точек ранга. Кликните красный символ (x), чтобы удалить ранг.
- **Диапазон дат**. Агрегация временного ранга сообщает значения, которые находятся в указанном диапазоне дат. Вы можете указать диапазоны дат, используя математические выражения даты. Кликните «Добавить диапазон», чтобы добавить набор конечных точек ранга
- **IPv4 Range**. Агрегация IPv4 ранга позволяет вам определить диапазоны IPv4 адресов. Кликните Add Range, чтобы добавить набор конечных точек ранга. Кликните красный символ (x), чтобы удалить ранг.
- **Термины**. Агрегация значений позволяет вам определить верхние или нижние n элементов данного поля для отображения, упорядоченные по количеству или пользовательской метрике.
- **Фильтры**. Вы можете определить набор фильтров для данных. Возможно указать фильтр как строку запроса или в формате JSON, так же как и в поисковой вкладке Discover. Кликните «Добавить фильтр», чтобы добавить другой фильтр. Кликните кнопку сноска, чтобы открыть поле подписи, где вы можете напечатать имя для отображения на визуализации.
- **Важные термины**. Выводит результаты экспериментальной агрегации знаковых значений.