Функциональное описание Q.ScribeR

Exported on Jul 08, 2019

Программное решение **Q.ScribeR** позволяет осуществлять поиск любой сложности по всем данным, проиндексированным программой **Q.KeepeR**. Для точного поиска по полям объектов, точного полнотекстового поиска, нечёткого поиска по полям, нечёткого полнотекстового поиска (независимо от его атрибутного состава), получения данных версии объекта (независимо от его атрибутного состава) используется удобный графический интерфейс в любом браузере. Также одним из важнейших преимуществ **Q.ScribeR** является возможность построения графических отчетов, диаграмм, таблиц любой сложности на основе данных в **Q.KeepeR**.
Функциональность программы легко расширяется с помощью различных плагинов.
Для знакомства с интерфейсом **Q.ScribeR** и чтобы попробовать полнотекстовый неточный поиск, необходимо наполнить **Q.KeepeR** тестовой информацией (см. Инструкцию по установке **Q.ScribeR**).

Интерфейс Q.ScribeR содержит четыре основных раздела:

- Discover (просмотр доступных данных)
- Visualize (визуализация собранных данных)
- Dashboard (управление дашбордами)
- Settings (настройки)

1 Раздел Discover

Предположим, что в Q.KeepeR собрано большое количество логов (файлов - журналов бизнес приложения). При первом подключении к Q.ScribeR вы попадёте на страницу Discover, которая изначально показывает список логов, записанных последними. Здесь есть возможность отфильтровать сообщения логов по времени и получить необходимые данные.

Страница Discover содержит следующие элементы:

- Строка поиска: находится прямо под главным меню. С помощью нее возможен поиск по всем логам.
- Фильтрация по времени (Time Filter): расположена в правом верхнем углу. Эта функция используется для применения различных фильтров к логам на основе относительных и абсолютных временных диапазонов.
- Список полей: находится слева, под строкой поиска. Здесь можно выбирать поля для визуализации и поиска.
- Гистограмма: график, который находится в центре страницы под строкой поиска. По умолчанию в нём отображается количество всех логов в зависимости от времени (ось x).
- Просмотр логов: список под гистограммой, который содержит сообщения логов и данные, отфильтрованные по полям. В случае если поле не установлено, сообщение отображается полностью.

1.1 Синтаксис поиска

Поисковая строка позволяет быстро найти необходимый набор сообщений. Синтаксис поиска достаточно прост и поддерживает логические операторы, шаблоны и фильтры полей. Например, чтобы найти логи доступа Nginx, которые были созданы пользователями Google Chrome, нужно ввести:

type: "nginx-access" agent: "chrome"

Также поиск можно выполнять по хостам, диапазонам IP-адресов и другим данным, которые содержатся в логах.

Вы можете сохранять поисковые запросы, которые часто используете. Для этого нажмите Save Search (кнопка справа от поисковой строки) и выберите Save.

Чтобы открыть сохранённый поиск, нажмите Load Saved Search. Позже эти данные можно использовать для визуализации.

Попробуйте сохранить запрос type: «nginx-access» и создать его визуализацию.

2 Раздел Visualize

На странице интерфейса Visualize вы можете создавать, редактировать и просматривать пользовательские визуализации. Q.ScribeR предлагает несколько видов визуализации: вертикальные и секторные диаграммы, отображение данных на карте, таблицы данных. Визуализацией можно поделиться с другими пользователями, которые имеют доступ к Q.ScribeR.

Если вы используете визуализацию Q.ScribeR впервые, перезапустите список полей.

Примечание: Об этом и других настройках можно прочитать в разделе о странице Settings данного руководства.

2.1 Создание вертикальной диаграммы

Чтобы создать визуализацию, откройте страницу Visualize.

Выберите тип визуализации. Например, чтобы создать вертикальную диаграмму, нужно выбрать Vertical bar chart.

Теперь нужно выбрать источник поиска. Вы можете создать новый или использовать сохраненный поиск. Если вы создали поиск type nginx access, как предлагалось ранее, используйте его.

Сначала появится график для предварительного просмотра. Если поисковой запрос обнаружил логи, вертикальная диаграмма будет состоять только из оси Y, которая отображает количество логов.

Вы можете расширить диаграмму с помощью меню слева, buckets. К примеру, вы можете добавить ось X, затем открыть выпадающее меню Aggregation, выбрать Date Histogram и нажать Apply. После этого в диаграмме появятся новые вертикали: количество логов распределится по оси X, которая отображает время.

Попробуйте выполнить следующее:

- Кликните Add Sub Aggregation и выберите тип Split Bars.
- Откройте выпадающее меню Sub Aggregation и выберите Significant Term.
- Откройте выпадающее меню Field и выберите clientip.raw.
- В поле Size введите 10.
- Нажмите Apply, чтобы сформировать новый график.

Если отображаемые логи сформированы на основе нескольких IP-адресами (т.е., ваш сайт посетил не один пользователь), вы увидите, что каждая вертикаль в графике разделена на несколько разноцветных сегментов. Каждый такой сегмент отображает количество логов, сформированных тем или иным IP-адресом. Максимальное количество сегментов – 10 (указано в Size).

Чтобы сохранить визуализацию, нажмите Save Visualization в верхнем меню, выберите название и нажмите Save.

2.2 Создание других визуальных отображений

Прежде чем приступить к работе над дашбордом, нужно создать хотя бы ещё одну диаграмму. Ознакомьтесь с остальными функциями страницы Visualize самостоятельно, выберите тип визуализации, создайте и сохраните график.

К примеру, вы можете создать круговую диаграмму из пяти самых распространённых типов логов. Для этого:

- Откройте Visualize и выберите Pie chart.
- В строку поиска введите запрос «» (чтобы вывести все логи).

- В меню buckets выберите *Split Slices**.
- В выпадающем меню Aggregation выберите Significant Terms.
- В выпадающем меню Field выберите type.raw.
- В поле Size введите 5.
- Чтобы отобразить диаграмму, нажмите Apply.

Примечание: Количество сегментов в круговой диаграмме может быть меньше, если запрашиваемых данных недостаточно для построения всех сегментов (например, если типов логов у вас всего 2).

3 Раздел Dashboard

Страница Dashboard позволяет создавать, изменять и просматривать пользовательские дашборды. Дашборды объединяют несколько визуализаций в одну страницу и могут фильтровать их. Дашборды помогают получить полный обзор логов и сравнить несколько визуализаций.

3.1 Создание дашборда

Чтобы создать дашборд, перейдите в раздел Dashboard.

Для создания дашборда необходимо иметь хотя бы две диаграммы. Если ранее вы не создавали дашбордов и на данный момент у вас недостаточно диаграмм, на экране появится почти пустая страница и надпись:

Ready to get started?

Если у вас достаточно данных для создания дашборда, нажмите New Dashboard (справа от строки поиска).

Чтобы создать дашборд, нажмите Add Visualization и добавьте созданные ранее диаграммы.

Когда диаграммы появятся на экране, вы сможете поменять их местами или изменить их размеры с помощью мыши.

Чтобы сохранить дашборд, кликните Save Dashboard, выберите имя для дашборда и нажмите Save.

3.2 Работа с дашбордами

Вы можете фильтровать данные в дашборде, изменив фильтр времени или кликая на элементы визуализации.

К примеру, кликнув на один из сегментов диаграммы, вы можете получить подробные данные о нём.

Чтобы отфильтровать данные, нужно нажать кнопку Apply Now. Все фильтры работают так же, как на странице Discover, но в дашборде они применяются только к определённому набору данных.

4 Раздел Settings

Страница Settings позволяет изменять настройки Q.ScribeR.

4.1 Перезагрузка списка полей

Добавляя в Q.SaveR (данная программа идет в комплекте с Q.ScribeR) новое поле (например, фильтр для нового типа логов), вы должны проиндексировать заново список полей, чтобы в нем появились новые поля.

Также список полей необходимо перезагрузить в случае, если вы не можете найти отфильтрованные поля в Q.ScribeR (они хранятся в кэше временно).

Чтобы обновить список полей:

- Откройте Settings и кликните по надписи "Index Patterns."
- Нажмите жёлтую пиктограмму с круглыми стрелками (при наведении мыши на эту пиктограмму, появится надпись "Refresh Field List").

4.2 Редактирование сохранённых объектов

Раздел Objects позволяет редактировать, просматривать и удалять сохранённые дашборды, поиски и диаграммы.

Чтобы открыть эту страницу, выберите Settings → Objects. Здесь вы можете управлять созданными ранее объектами.