

???????????????? ?????,
????????, ??????

????? ????????????

Контекстные таблицы и активные листы:

- живут на корреляторе;
- по большей части наполняются им же, реже - вручную и через API;
- используются для корреляционной логики и обогащения на корреляторе.

Важно! Содержимое активного листа/контекстной таблицы **РАЗНОЕ** на каждом корреляторе.

Словарь / таблица - это ключ и значение, который можно задать один раз и ручками править (можно через API), этот словарь доступен в коллекторах и на корреляторах, причем он один может быть доступен сразу всем. Поле значение не обязательно использовать, можно его пустым сделать, можно "-", "0" написать туда, как удобно. Особенности словарей и таблиц:

- живут на ядре, но транслируются на все сервисы, где они указаны;
- наполняются только вручную или через API, более статичны;
- используются в основном для обогащения на коллекторах/корреляторах, реже для корреляционной логики.

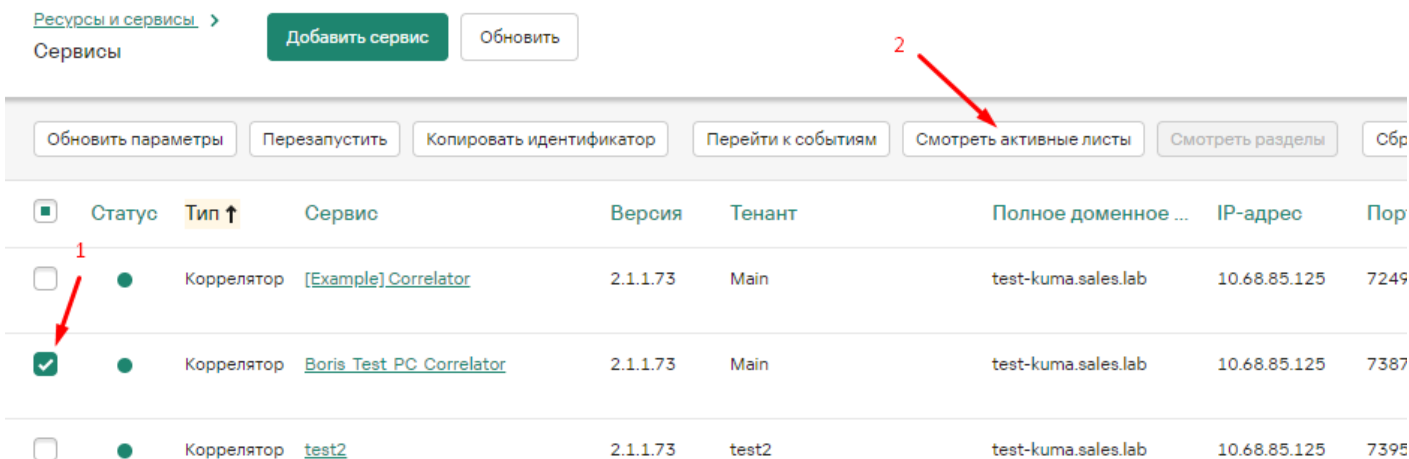
Если словарь содержит более 5000 записей, тогда KUMA в веб-интерфейсе не отображает содержимое словаря. Чтобы изменить содержимое словаря, отредактируйте CSV-файл и загрузите его в KUMA.

Важно! Содержимое словаря/таблицы **ОДИНАКОВОЕ** для всех сервисов, где он используется.

????????? ??????? / ?????

Активный лист (AL) - это контейнер для данных (представляет собой структуру ключ и значение), предназначенный для быстрой записи/чтения динамических данных, доступных всем фильтрам и корреляционным правилам в рамках одного сервиса Коррелятора. Чтобы

их посмотреть, нужно из активных сервисов нажать кнопку **Смотреть активные листы**.



Взаимодействовать с активным листом могут не только компоненты коррелятора, но и пользователи, с помощью Web-консоли и API. Пользователь KUMA имеет возможность работы с данными AL:

- выполнять поиск по именам записей (выполняться по полному вхождению указанной пользователем подстроки);
- удалить записи;
- открыть содержимое записи.

Производительность активных листов комфортна (максимальна) с десятками тысяч записей.

Активные листы работают в памяти коррелятора, также при работе активного листа используется Write-Ahead Log (WAL), который предполагает сохранение каждого изменения состояния в виде двоичного файла на жестком диске. Каждой записи журнала присваивается уникальный идентификатор, позволяющий выполнять дополнительные операции с журналом, такие как сегментация журнала и очистка. Уникальность записей журнала также помогает применять обновления журнала с использованием единой очереди обновлений, обеспечивая последовательные и согласованные обновления.

Примеры использования [тут](#).

Синхронизация активного листа между несколькими корреляторами. **ВАЖНО это не поддерживаемый и не официальный сценарий.** Можно попробовать сделать так: WAL записывается на сетевую папку, примонтированную к двум корреляторам. И если один из корреляторов упал, скрипт (заранее написанный) запускает службу второго коррелятора. Второй коррелятор перечитывает WAL и импортирует данные в лист.

?????????? ????????

Контекстная таблица - это тот же лист, только с дополнительными возможностями по хранению в разных полях разных структур данных. Существует только в рамках конкретного коррелятора, в который она была добавлена либо через фильтры, либо через действия в корреляционных правилах.

Функциональные возможности контекстных таблиц:

- список ключевых полей определяется пользователем;
- данные в контекстных таблицах типизированы (целые числа, числа с плавающей точкой, строки, логический тип, timestamp, IP);
- поддерживаются массивы для всех типов данных, перечисленных выше;
- в корреляции, для полей с массивами возможны подсчеты уникальных значений, вычисление длины массива, обращение к определенному элементу массива.

Примеры использования [тут](#).

Revision #9

Created 2023-08-09 13:05:45 UTC by Boris RZR

Updated 2026-05-20 12:40:54 UTC by Boris RZR