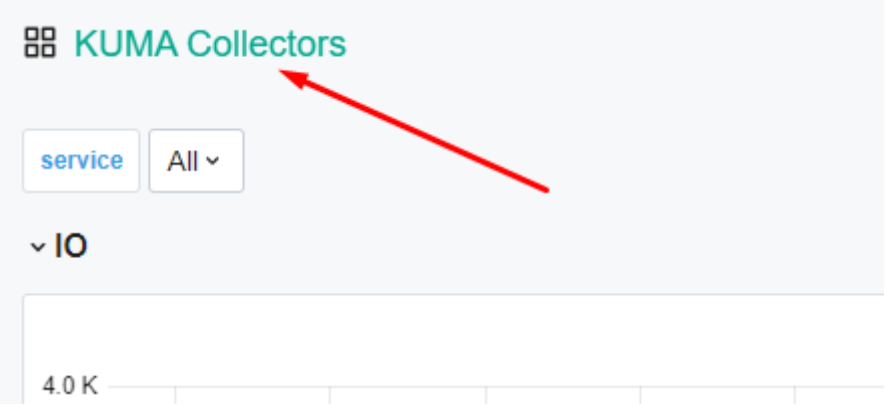
???????? ?????? ? KUMA

> Официальная документация по данному разделу приведена в Онлайн-справке на продукт: https://support.kaspersky.ru/help/KUMA/3.2/ru-RU/218035.htm

> По умолчанию данные о работе KUMA хранятся 3 месяца. Этот срок можно изменить, см. справку.

В KUMA роль системы мониторинга выполняет **Victoria Metrics**. Информация по всем микросервисам обновляется каждые 5 секунд по HTTP-интерфейсу. А **Grafana** отвечает за отображение метрик, собранных с помощью Victoria Metrics.

Для просмотра всех наборов графиков щелкните сюда (на имя подсвеченное зеленым) в разделе KUMA "Метрики":



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

Следующие метрики извлекаются из всех микросервисов KUMA

- Process — Общие метрики процесса
- Memory — Утилизация оперативной памяти, оценивается резидентная память (RSS - Resident set size)
- DISK BPS — Количество байт в секунду прочитанных/записанных на диск
- Network BPS — Количество байт в секунду полученных/отправленных в сеть
- Network Packet Loss — Количество утраченных сетевых пакетов в секунду
- GC Latency — Время (медиана), затраченное на цикл Garbage Collector'a GO
- Goroutines — Текущее количество активных Go-рутин (потоки в Golang)

OS (????? ?????? ???????????? ???????)

- Load — Load average (средняя нагрузка) на ЦП. Обычно да 1, 5 и 15 минут, если число нагрузки за 15 минут более количества ядер (включая виртуальные) системы, то это не нормально
- CPU — Общая утилизация ЦП
- Memory — Общая утилизация оперативной памяти (RSS). В норме, когда число не доходит до 100%
- Disk — Утилизация дискового пространства

??????? Collectors

IO (Input-Output)

- Processing EPS — Количество обрабатываемых событий в секунду
- Output EPS — Количество отправляемых в точку назначения событий в секунду
- Output Latency — Время, затраченное на передачу пачки событий точке назначения и на получения ответа от нее
- Output Errors — Количество ошибок отправки пачки событий точке назначения в секунду. Ошибки отправки по сети и ошибки записи в дисковый буффер отображаются отдельно
- Output Event Loss — Количество потерянных событий в секунду. Потеря может произойти, если их не удалось отправить ни в сеть, ни записать в дисковый буффер
- Output Disk Buffer Size — Текущий размер дискового буффера точки назначения. Ноль означает, что ни одна пачка событий не буферизирована, и это хорошо, не копится очередь

Normalization

- Raw & Normalized event size — Размер (медиана) оригинального лога источника и размер нормализованной формы этого лога (события)
- Errors — Количество ошибок нормализации в секунду

Filtration

- EPS — Количество событий в секунду, отбрасываемых фильтром коллектора

Aggregation

- EPS — Количество событий, входящих и выходящих из правила агрегации в секунду. Позволяет оценить эффективность правил агрегации
- Buckets — Текущее количество бакетов в правиле агрегации

Enrichment

- Cache RPS — Количество обращений к локальному кешу в секунду
- Source RPS — Количество обращений к источнику обогащения в секунду
- Source Latency — Время (медиана), затраченное на отправку запроса и получение ответа от источника обогащения
- Queue — Размер очереди запросов на обогащение. Позволяет оценить, является ли данное правило обогащения узким местом
- Errors — Количество ошибок обращений к источнику обогащения, обозреваемых в секунду

??????? Correlator

IO (Input-Output)

- Processing EPS — Количество обрабатываемых событий в секунду
- Output EPS — Количество событий, отправляемых в точку назначения в секунду
- Output Latency — Время (медиана), затраченное на передачу пачки событий точке назначения и на получения ответа от нее
- Output Errors — Количество ошибок отправки пачки событий точке назначения в секунду. Ошибки отправки в сеть и ошибки записи в дисковый буффер отображаются отдельно
- Output Event Loss — Количество потерянных событий в секунду. Потеря может произойти, если их не удалось отправить ни в сеть, ни записать в дисковый буффер
- Output Disk Buffer Size — Текущий размер дискового буффера точки назначения. Ноль означает, что ни одна пачка событий не буферизирована, и это хорошо, не копится очередь

Correlation

- EPS — Количество корреляционных событий, порождаемых правилом корреляции в секунду
- Buckets — Текущее количество бакетов внутри правила корреляции (только для правил Standard)
- Rate Limiter Hits — Превышение лимита срабатываний правилом корреляции в секунду
- Active Lists OPS — Количество обращений к активному листу в секунду, с указанием операции
- Active Lists Records — Текущее количество записей в активном листе
- Active Lists On-Disk Size — Текущий размер активного листа на диске

Enrichment

- Cache RPS — Количество обращений к локальному кешу в секунду
- Source RPS — Количество обращений к источнику обогащения в секунду

- Source Latency — Время (медиана), затраченное на отправку запроса и получение ответа от источника обогащения
- Queue — Размер очереди запросов на обогащение. Позволяет оценить, является ли данное правило обогащения узким местом
- Errors — Количество ошибок обращений к источнику обогащения, обозреваемых в секунду

Response

- RPS — Количествово запусков/активаций правил реагирования (response) в секунду.

??????? Storage

Clickhouse / General

- Active Queries — Общее кол-во запросов к кластеру Clickhouse, выполняемых в данный момент. Метрика отображается по каждому инстансу Clickhouse
- QPS — Общее количество запросов в секунду
- Failed QPS — Общее количество неуспешных запросов в секунду
- Allocated memory — Количество памяти (RAM), выделенное процессу Clickhouse

Clickhouse / Insert

- Insert EPS — Количество событий, вставляемых за одну секунду в инстанс Clickhouse
- Insert QPS — Количество запросов на вставку в секунду
- Failed Insert QPS — Количество неуспешных запросов на вставку в секунду
- Delayed Insert QPS — Количество запросов на вставку (в секунду), которые были отложены нодой Clickhouse по превышению soft лимита активных слияний.
- Rejected Insert QPS — Количество запросов на вставку (в секунду), которые были отвергнуты нодой Clickhouse по превышению hard лимита активных слияний.
- Active Merges — Количество активных слияний
- Distribution queue — Количество файлов, в которые сохранены временно эвенты в кластере Clickhouse. Эвенты предназначены для инсерта в тот или иной шард, но не попали из-за того, что шард был недоступен. Эти события недоступны в поиске

Clickhouse / Select

- Select QPS — Количество запросов на выборку данных в секунду
- Failed Select QPS — Количество неуспешных запросов на выборку данных в секунду

Clickhouse / Replication

- Active Zookeeper Connections — Количество активных подключений к нодам кластера Zookeeper. В норме должно быть равным количеству нод в кластере Zookeeper

- Read-only Replicas — Количество нод-реплик Clickhouse, находящихся в режиме read-only. В норме таких реплик быть не должно (равно нулю)
- Active Replication Fetches — Количество активных процессов репликации данных в настоящий момент (скачивание данных с ноды)
- Active Replication Sends — Количество активных процессов репликации данных в настоящий момент (отправка данных ноде)
- Active Replication Consistency Checks — Количество текущих проверок консистентности данных на репликах

Clickhouse / Networking

- Active HTTP Connections — Количество активных подключений к HTTP серверу Clickhouse
- Active TCP Connections — Количество активных подключений к TCP серверу Clickhouse
- Active Interserver Connections — Количество активных служебных подключений между нодами Clickhouse

??????? Core

IO (Input-Output)

- RPS — Количество запросов в секунду
- Latency — Время (медиана), затраченное на обработку одного запроса
- Errors — Количество ошибок оборабоки запросов в секунду

Notification Feed

- Subscriptions — Количество клиентов, подключенных к Core с помощью SSE для получения сообщений от сервера в реальном времени. Обычно равно количеству клиентов, использующих Web-console
- Errors — Количество ошибок отправки оповещений в секунду

Schedulers

- Active — Текущее количество активных системных повторяющихся задач. Фоновые задачи, запущенные пользователем, не учитываются
- Latency — Время (медиана), затраченное на выполнение задачи
- Errors — Количество ошибок выполнения задач, обозреваемых в секунду

С KUMA версии 3.2:

Raft

- Lookup RPS — Количество вызовов процедур чтения в секунду. С указанием процедуры
- Lookup Latency — Длительность выполнения процедур чтения, с указанием процедуры. (99 percentile)
- Propose RPS — Количество вызовов процедур обновления состояния Raft (SQLITE) в секунду. С указанием процедуры
- Propose Latency — Длительность выполнения процедур обновления состояния Raft (SQLITE), с указанием процедуры. (99 percentile)

API

- RPS — Количество запросов в секунду
- Latency — Время, затраченное на обработку одного запроса. Медиана
- Errors — Количество ошибок оборабоки запросов, обозреваемых за 1 секунду

С KUMA версии 3.4:

Tasks

- Active tasks — Число выполняемых задач за единицу времени, в шт.
- Task Execution latency — Время выполняемых задач, в сек
- Errors — Ошибки при выполнении задач, в шт

Data Mining

- Executing Rules — Суммарное количество Data Mining правил, которые сейчас выполняются
- Execution Latency — Продолжительность выполнения Data Mining правил (сколько время занял сам запрос в БД от момента запуска, до передачи в коррелятор)
- Queued Rules — Суммарное количество правил в очереди. Очередь появляется тогда, когда запланировано на одно время больше правил, чем разрешено параметром конкурентности (по умолчанию = 1)
- Execution Errors — Количество ошибок при выполнении Data Mining правил

? KUMA ?????? 3.2

??????? KUMA Agent

> Для сбора доступ в ядро по порту 8429/tcp

IO (Input-Output)

- Processing EPS — Количество обрабатываемых событий за 1 секунду

- Output EPS — Количество отправляемых в точку назначения событий за 1 секунду
- Output Latency — Время, затраченное на передачу пачки событий точке назначения и на получения ответа от нее. Иными словами - продолжительность round-trip. Медиана
- Output Event Loss — Количество потерянных событий за 1 секунду. Потеря может произойти, если их не удалось ни отправить в сеть, ни записать в дисковый буффер. Кроме того, если точка назначения ответила кодом, означающим, к примеру, некорректно сформированный запрос - события также будут утеряны
- Output Errors — Количество ошибок отправки пачки событий точке назначения, обозревамое за 1 секунду. Ошибки отправки в сеть и ошибки записи в дисковый буффер отображаются отдельно
- Output Disk Buffer Size — Текущий размер дискового буффера destination. Ноль означает, что ни одна пачка событий не буферизирована, все в порядке
- Write Network BPS — Количество байт отправленных в сеть за 1 секунду

??????? EventRouter

IO (Input-Output)

- Processing EPS — Количество обрабатываемых событий за 1 секунду
- Output EPS — Количество отправляемых в точку назначения событий за 1 секунду
- Output Latency — Время, затраченное на передачу пачки событий точке назначения и на получения ответа от нее. Иными словами - продолжительность round-trip. Медиана
- Output Event Loss — Количество потерянных событий за 1 секунду. Потеря может произойти, если их не удалось ни отправить в сеть, ни записать в дисковый буффер. Кроме того, если точка назначения ответила кодом, означающим, к примеру, некорректно сформированный запрос - события также будут утеряны
- Output Errors — Количество ошибок отправки пачки событий точке назначения, обозревамое за 1 секунду. Ошибки отправки в сеть и ошибки записи в дисковый буффер отображаются отдельно
- Output Disk Buffer Size — Текущий размер дискового буффера destination. Ноль означает, что ни одна пачка событий не буферизирована, все в порядке
- Write Network BPS — Количество байт отправленных в сеть за 1 секунду
- Connector Errors — Количество ошибок в логах коннектора

Revision #6
Created 2024-01-12 07:52:31 UTC by Boris Rzr
Updated 2025-01-10 12:13:53 UTC by Boris Rzr