

Экстра возможности агента KUMA

Балансировка трафика

Агент KUMA может поддерживать множество подключений:

The screenshot displays the KUMA agent configuration interface. At the top, there are tabs for 'Общие параметры' (General parameters) and two active connection tabs: 'Подключение №1' and 'Подключение №2'. A red box highlights the '+' button next to these tabs, with a red arrow pointing to it, indicating the option to add more connections. Below the tabs, the 'Коннектор:' (Connector) section is visible. It has two sub-tabs: 'Основные параметры' (Main parameters) and 'Дополнительные параметры' (Additional parameters). Under 'Основные параметры', there is a 'Создать' (Create) dropdown menu, a text field for '*Название' (Name) with the placeholder 'Название коннектора', and a dropdown menu for '*Тип' (Type). The '*Тип' dropdown is open, showing a list of connector types: tcp, udp, nats-jetstream, kafka, http, file, 1c-log, 1c-xml, and 1c-... There are also question mark icons next to the '*Тип' and '*URL' fields.

Типы коннекторов у агентов можно посмотреть тут (они отличаются в зависимости от типа ОС например) - <https://support.kaspersky.com/KUMA/2.1/ru-RU/217690.htm>

Например, в нашей задаче мы поднимаем оди порт 51400:

Basic settings

Advanced settings

Create new

*Name

tcpListenFortinet

*Kind

tcp

*URL

10.15.56.4:51440

И мы хотим балансировать трафик между двумя коллекторами, для этого в точке назначения агента прописываем:

Destinations:

Basic settings

Advanced settings

Create new

*Name

toCollForti

☐ Disabled

*Kind

tcp

*URL

ib-k-coll-1p.ku...:5144

URL

ib-k-coll-2p.ku...:5144

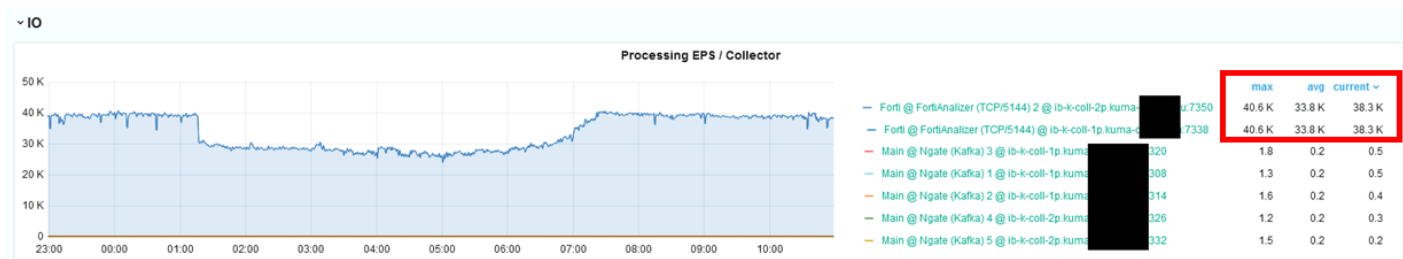
+ URL

А в дополнительных параметрах точки назначения выбираем Round robin для балансировки:

URL selection policy

Round robin

В итоге получаем красивую балансировку:



Отправка копии трафика в несколько точек

Для решения такой задачи необходимо добавить еще одну точку назначения в конфигурации агента:

[Агенты](#) >

Редактирование агента

Основные параметры	Дополнительные параметры
	<div>Создать</div>
*Название	<div>getPSlogs</div>
*Тип	<div>wec</div>
*Журналы Windows	<div>Microsoft-Windows-PowerShell/Operational, Security, ...</div>

Точки назначения:

Основные параметры	Дополнительные параметры
	<div>Создать</div>
*Название	<div>toCollector1</div>
	<div><input type="checkbox"/> Выключено</div>
*Тип	<div>tcp</div>
*URL	<div>10.68.85.125:5687</div>
	<div>+ URL</div>

+ Добавить точку назначения

Точки назначения бывают такие:

nats-jetstream
tcp
http
diode
kafka
file

Итого получаем нечто подобное:

Создать

*Название

toCollector1

☐ Выключено

*Тип

tcp

*URL

10.68.85.125:5687

+ URL ?

Основные параметры

Дополнительные параметры

Создать

*Название

toCollector2

☐ Выключено

*Тип

tcp

*URL

10.68.85.126:5687

+ URL ?

Есть также сторонняя утилита по стресс тестов - [Kraken STT - Kraken Stress Testing Toolkit](http://kraken-stt.ru) (kraken-stt.ru)

Файловая интеграция с указанием файла и пути в событии

Информация о событии



Копировать

TenantID	Main
SpaceID	KUMA Default
Timestamp	12.02.2025 14:22:26:847
EndTime	12.02.2025 14:22:26:847
DeviceReceiptTime	12.02.2025 14:22:26:847
DeviceTimeZone	+03:00
Service	File form Win (internal\14443)
Type	Base
Extra	0: 3345345 1: 324234 2: 34456 3: 476437 \$kuma_fileSourceName: file.txt.txt \$kuma_fileSourcePath: C:\local_file_read\file.txt.txt

Исходное событие

3345345, 324234, 34456, 476437

Для этого в агенте в коллектор необходимо указать транспорт internal в точке назначения:

Редактирование агента

Общие параметры

Подключение №1

local_win_file_read

Основные параметры

Дополнительные параметры

Коннектор

Создать

Название*

file

Тип* ⓘ

file

Путь к файлу* ⓘ

C:\local_file_read*

Время ожидания изменений, сек ⓘ

0

Действие после таймаута ⓘ

Ничего не делать

Auditd

☐

Точки назначения

Основные параметры

Дополнительные параметры

Точка назначения

Создать

Название*

to_coll

Состояние

☒

Тип*

internal

URL*

kuma-aio.sales.lab:14443

+ Добавить

Соответственно прием на коллекторе тоже должен быть транспортом internal:

Редактирование коллектора

Подключение источников

Транспорт

Парсинг событий

Фильтрация событий

Агрегация событий

Обогащение событий

Маршрутизация

Проверка параметров

Транспорт

Подключите источник, от которого хотите получать события. Подробнее см. [в онлайн-справке](#).

Основные параметры

Дополнительные параметры

Коннектор

Создать

Тип* ⓘ

internal

URL* ⓘ

:14443

+ Добавить

Revision #5

Created 14 August 2023 07:48:21 by Boris RZR

Updated 13 February 2025 13:21:00 by Boris RZR