

Экстра возможности агента KUMA

Балансировка трафика

Агент KUMA может поддерживать множество подключений:

The screenshot displays the KUMA agent configuration interface. At the top, there is a tabbed interface with 'Общие параметры' (General parameters) selected. Below this, a red box highlights a section containing two tabs: 'Подключение №1' (Connection #1) and 'Подключение №2' (Connection #2), each with a close button (x). To the right of these tabs is a plus sign (+) button, which is pointed to by a red arrow, indicating the option to add a new connection. Below the tabs, the 'Коннектор:' (Connector) section is visible, showing a dropdown menu with the option 'Создать' (Create). The 'Основные параметры' (Main parameters) section includes fields for '*Название' (Name), '*Тип' (Type), and '*URL'. The 'Тип' dropdown is open, showing a list of connector types: tcp, udp, nats-jetstream, kafka, http, file, 1c-log, 1c-xml, and 1c-... The 'Точки назначения:' (Destinations) section is also visible at the bottom.

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

?

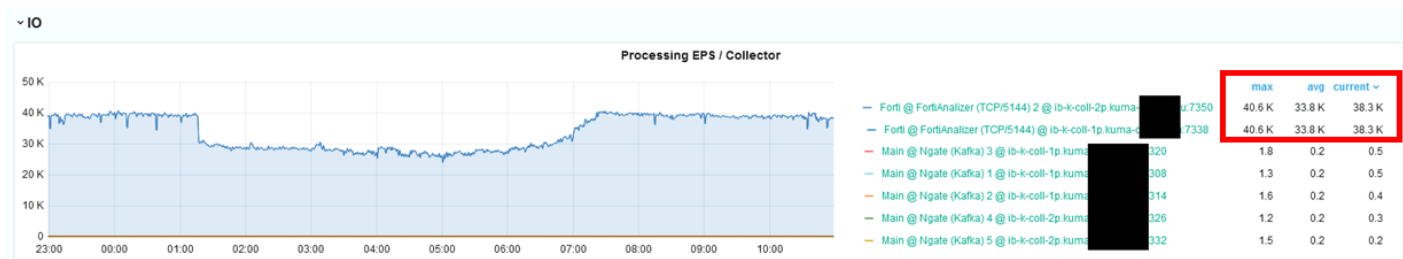
А в дополнительных параметрах точки назначения выбираем Round robin для балансировки:

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 ?

Revision #4

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

Updated 7 July 2024 08:46:37 by Koala