

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-1b.ku...:5144

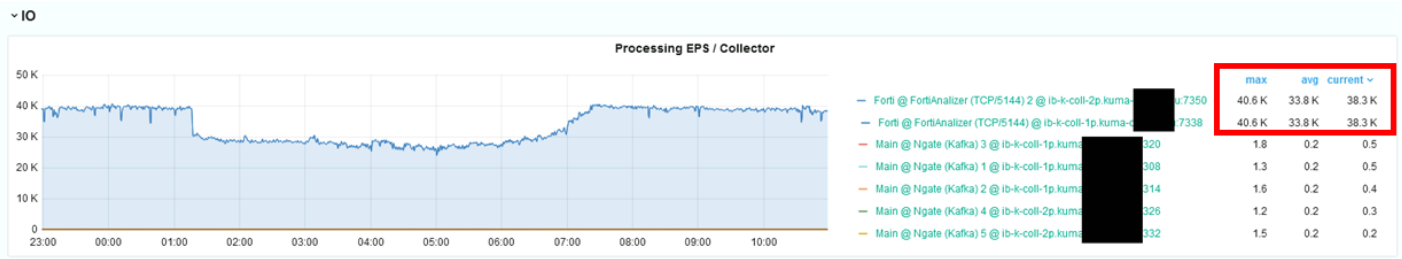
URL ib-k-coll-2p.ku...:5144

+ URL

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

URL selection policy Round robin

В итоге получаем красивую балансировку:



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

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

[Агенты](#) >

Редактирование агента

Основные параметры	Дополнительные параметры
	<input type="text" value="Создать"/>
*Название	<input type="text" value="getPSlogs"/>
*Тип	<input type="text" value="wec"/> ?
*Журналы Windows	<input type="text" value="Microsoft-Windows-PowerShell/Operational, Security, ..."/>

Точки назначения:

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



Точки назначения бывают такие:

Dropdown menu with an upward arrow icon at the top right. The list of items is:

- nats-jetstream
- tcp
- http
- diode
- kafka
- file

Итого получаем нечто подобное:

Form for creating a collector:

Создать ▼

*Название: toCollector1

Выключено

*Тип: tcp ▼

*URL: 10.68.85.125:5687

+ URL ?

Form for creating a collector with tabs:

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 \(kraken-stt.ru\)](http://kraken-stt.ru)

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

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

Название*

Тип*

Путь к файлу*

Время ожидания изменений, сек

Действие после таймаута

Auditd

Точки назначения

Основные параметры

Дополнительные параметры

Точка назначения

Название*

Состояние

Тип*

URL*

Недопустимо указывать пути, соответствующие следующим регулярным выражениям:

- `(?i)^[a-zA-Z]:\\Program Files`
- `(?i)^[a-zA-Z]:\\Program Files\(\x86\)`
- `(?i)^[a-zA-Z]:\\Windows`
- `(?i)^[a-zA-Z]:\\ProgramData\\Kaspersky Lab\\KUMA`

Однако существует возможность читать файлы из системных директорий через создание символических ссылок: например, `mklink /D "C:\notsecret" "C:\Program Files (\x86)\secret"` и в конфигурации агента указать `"C:\notsecret"`.

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

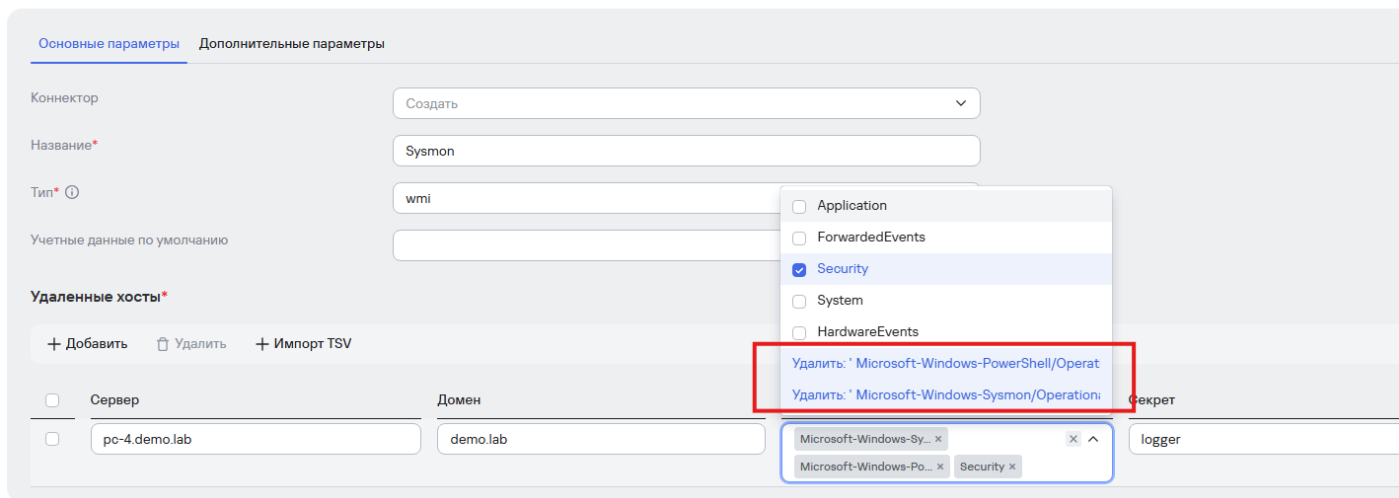
Тип*

URL*

????????? ?????????????????? ?????????? ? ??
Windows ?? ????????? Sysmon / PowerShell

В поле журналов настройки коннектора просто вставьте путь к журналам, пример:

Коннектор



????????? ?????????? Auditd

в настройках коннектора агента, поставьте флаг **Auditd**

Опция auditd на агенте доступна при использовании транспорта: internal, tcp, udp или чтении файла

Коннектор

Основные параметры	Дополнительные параметры
Коннектор	Создать
Название*	Auditd linux
Тип* ⓘ	file
Путь к файлу* ⓘ	/var/log/audit/audit.log
Время ожидания изменений, сек ⓘ	0
Действие после таймаута ⓘ	Ничего не делать
Auditd	<input checked="" type="checkbox"/>

Включите переключатель в параметрах коннектора агента, вам нужно выбрать значение `\n` в раскрывающемся списке. Разделитель в параметрах коннектора коллектора, в который агент отправляет события.

Точки назначения

Основные параметры	Дополнительные параметры
Размер буфера ⓘ	0
Интервал очистки буфера ⓘ	0
Размер дискового буфера ⓘ	0
Обработчики	0
Режим TLS	
Сжатие	по умолчанию
Политика выбора URL ⓘ	Любой
Разделитель	\n

Revision #11

Created 2023-08-14 07:48:21 UTC by Boris RZR

Updated 2026-06-29 14:46:41 UTC by Boris RZR