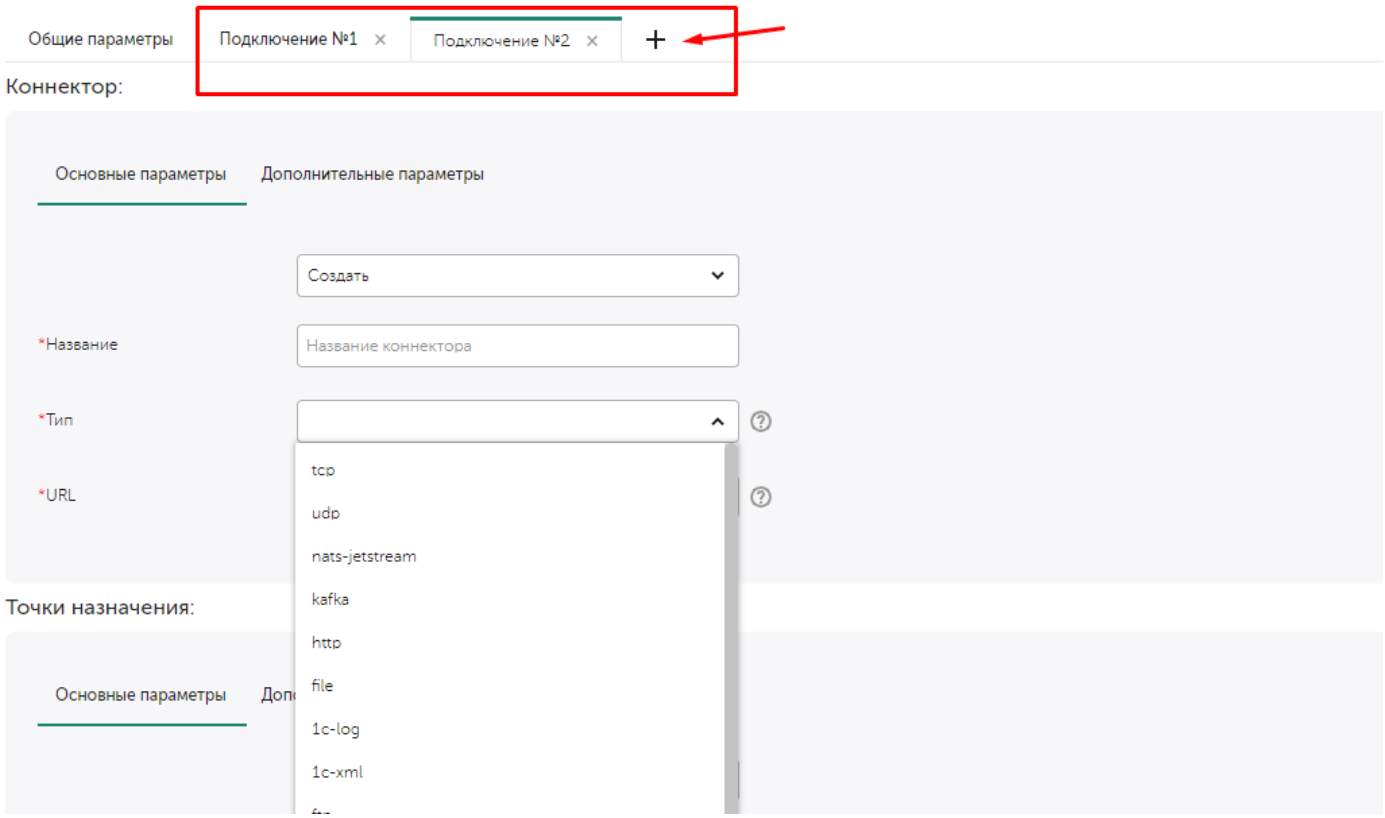
?????? ???????????? ?????? KUMA

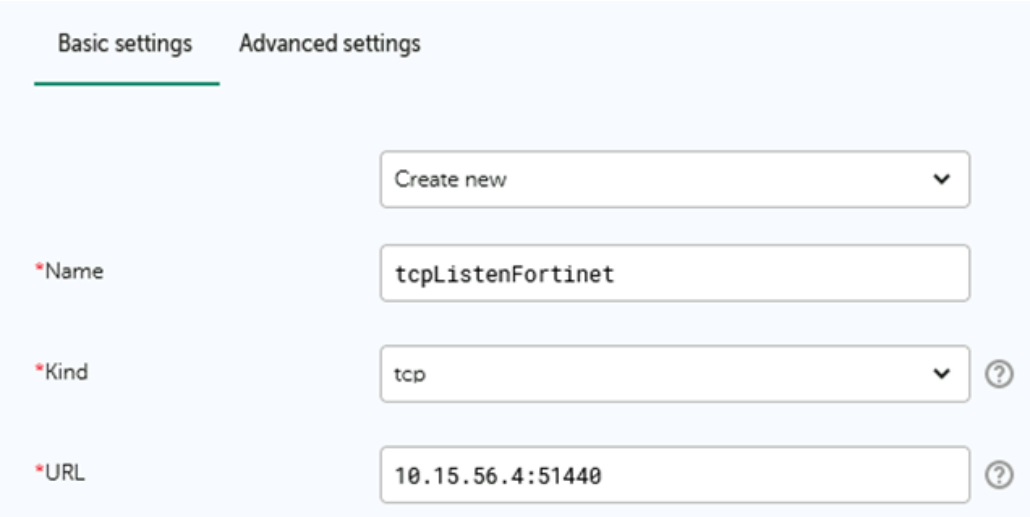
???????????? ???????

Агент KUMA может поддерживать множество подключений:

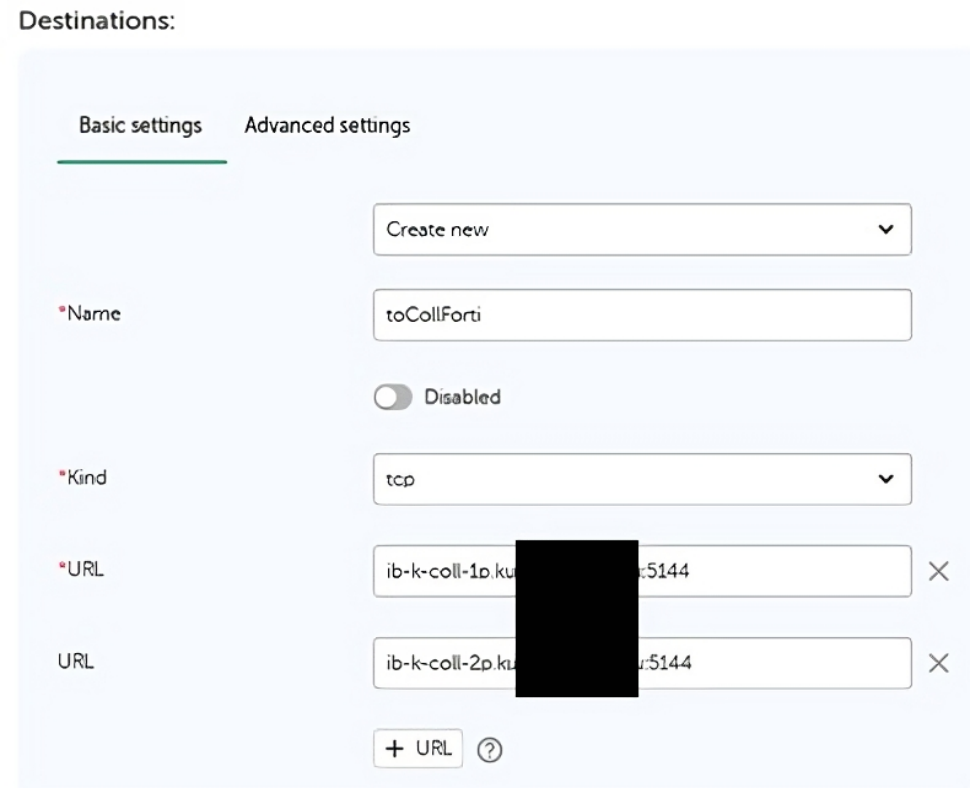


Типы коннекторов у агентов можно посмотреть тут (они отличаются в зависимости от типа ОС например) - https://support.kaspersky.com/KUMA/2.1/ru-RU/217690.htm

Например, в нашей задаче мы поднимаем оди порт 51400:

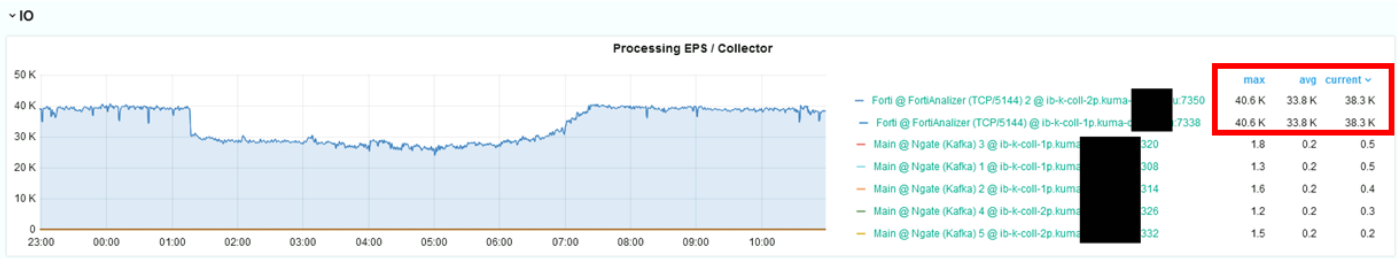


И мы хотим балансировать трафик между двумя коллекторами, для этого в точке назначения агента прописываем:



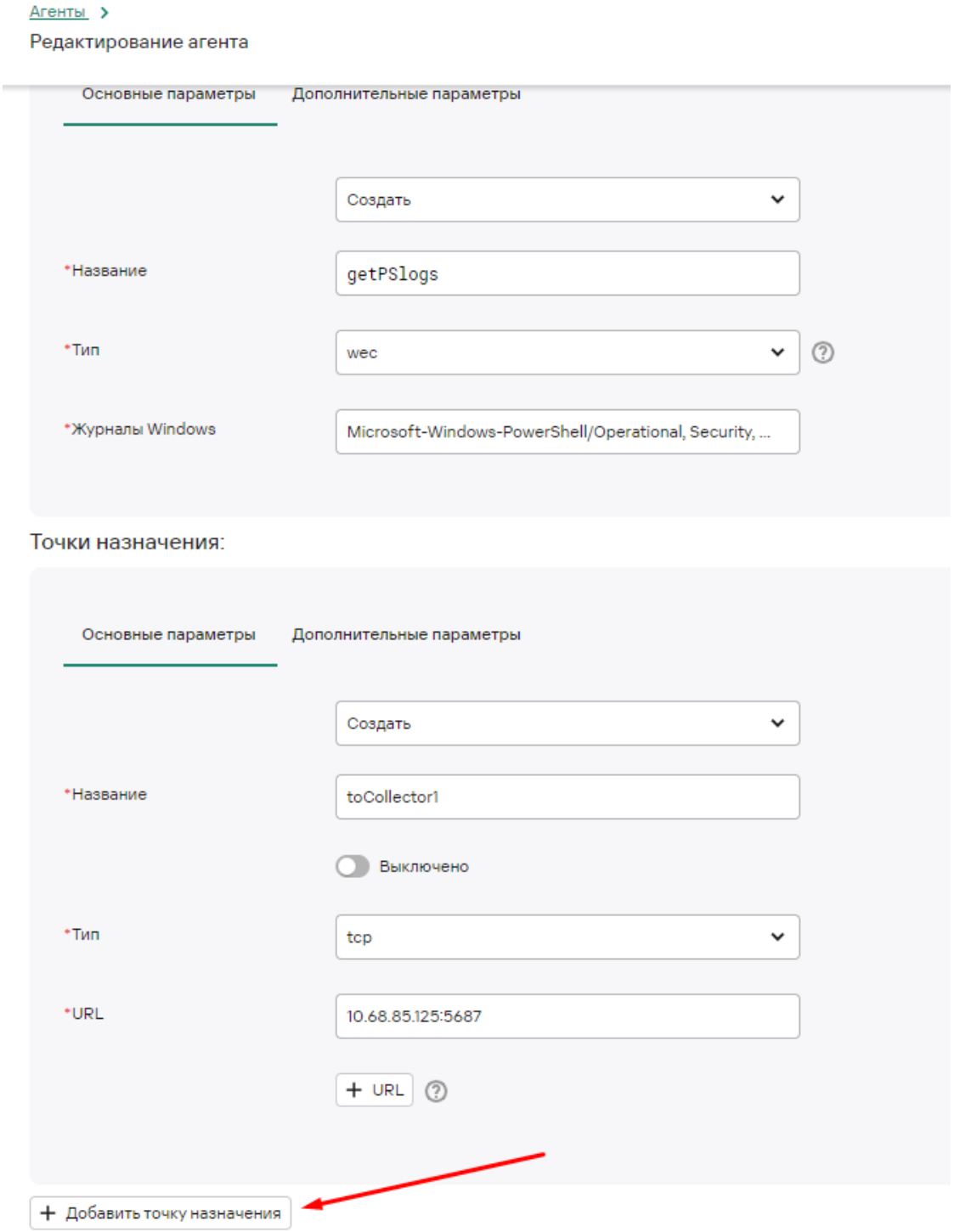
А в дополнительных параметрах точки назначения выбираем Round robin ля балансировки:

В итоге получаем красивую балансировку:

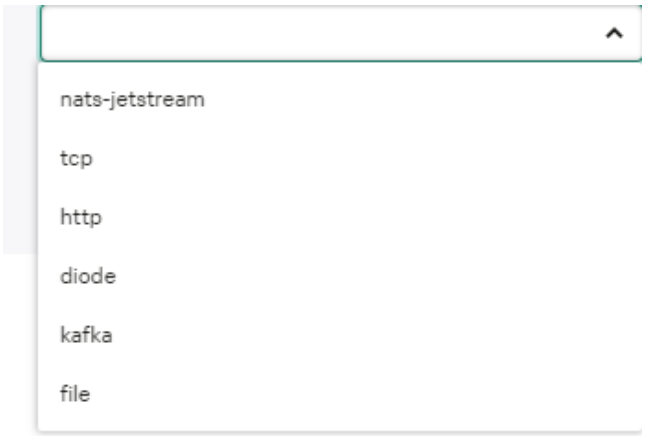


???????? ????? ??????? ? ????????? ?????

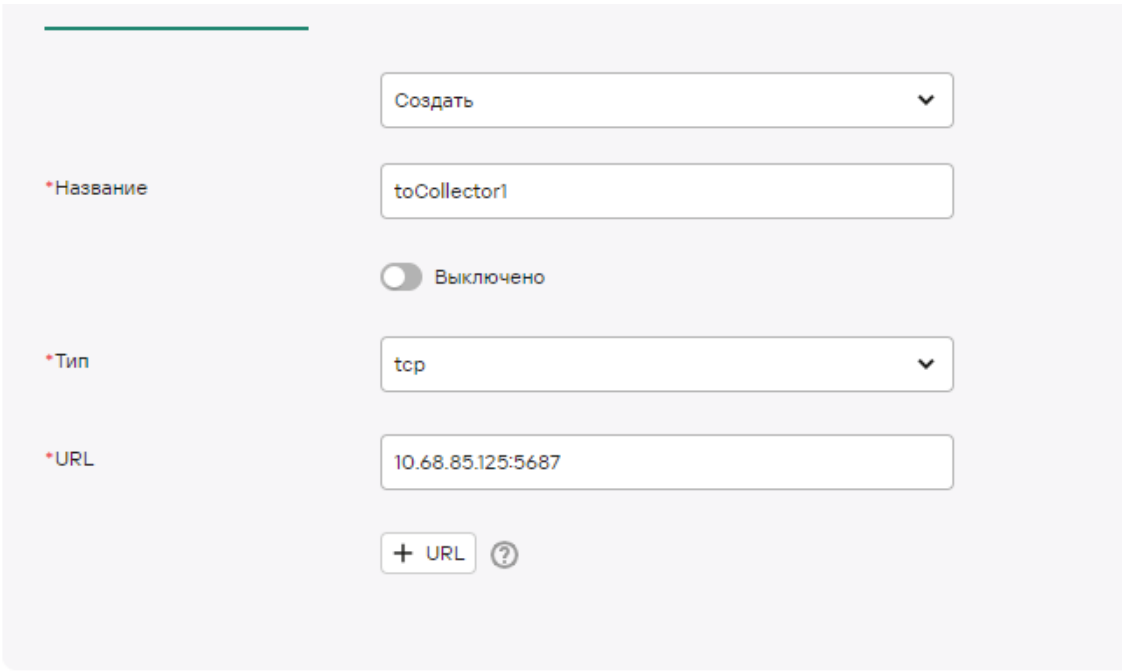
Для решения такой задачи необходимо добавить еще однк точку назначения в конфигурации агента:

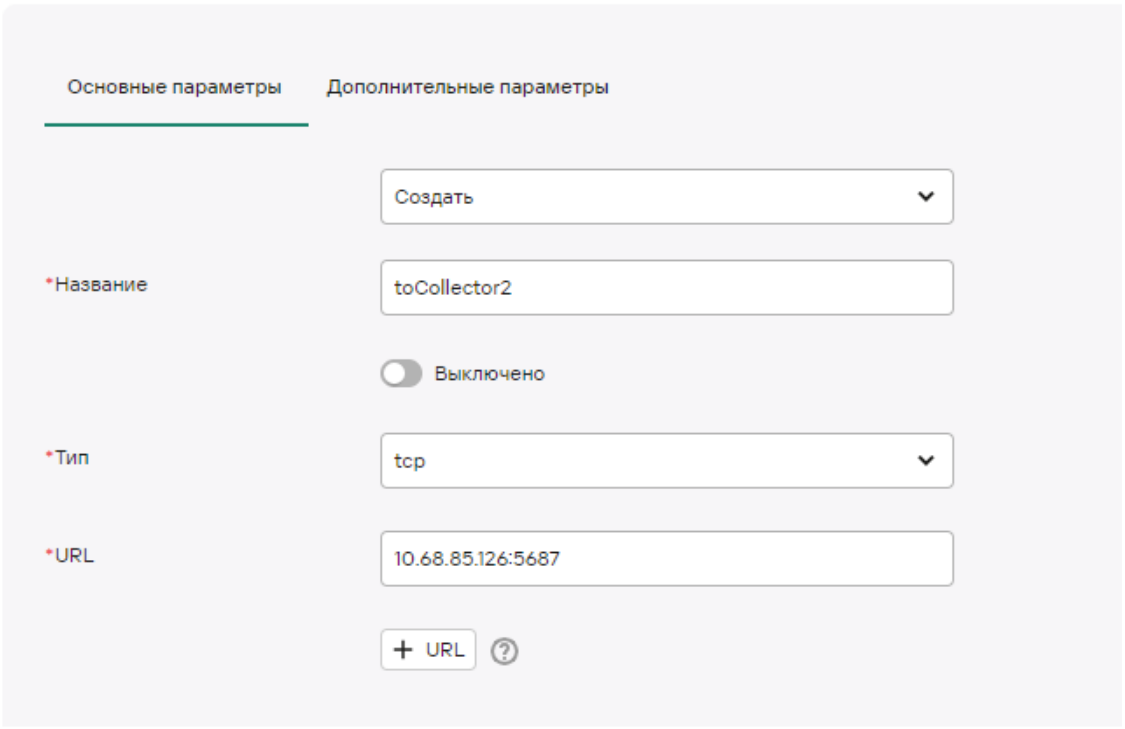


Точки назначения бывают такие:



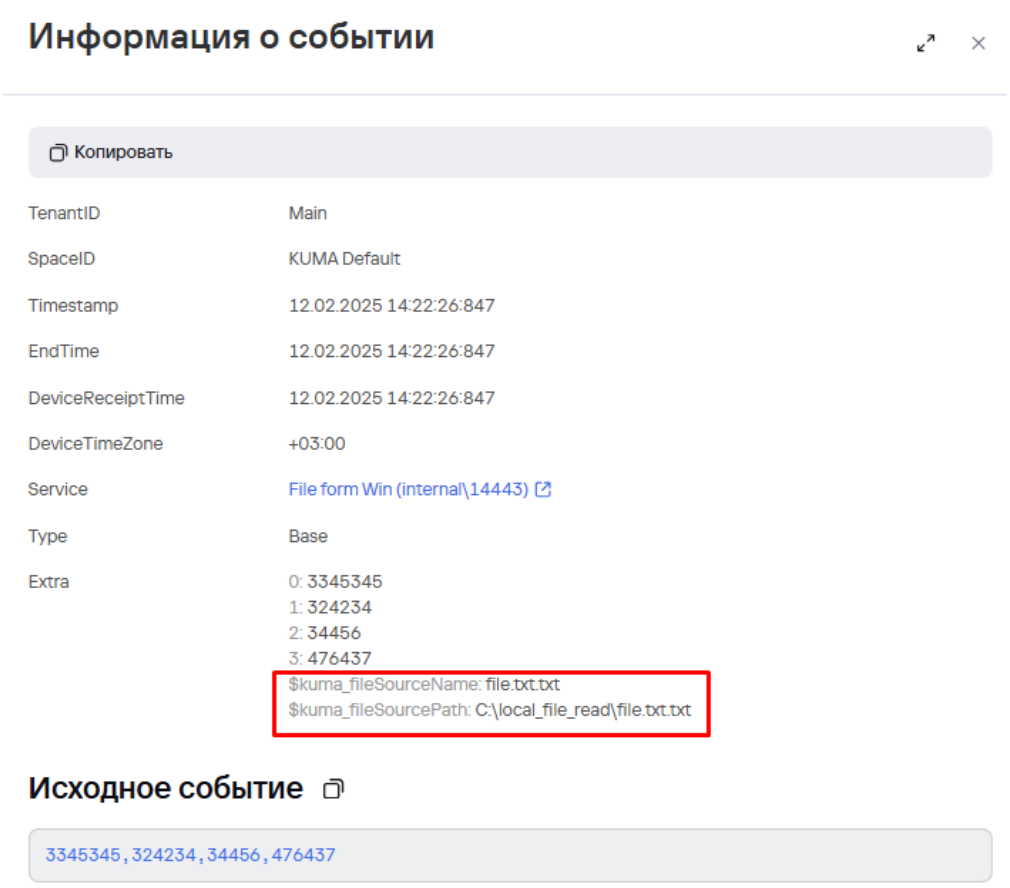
Итого получаем нечто подобное:



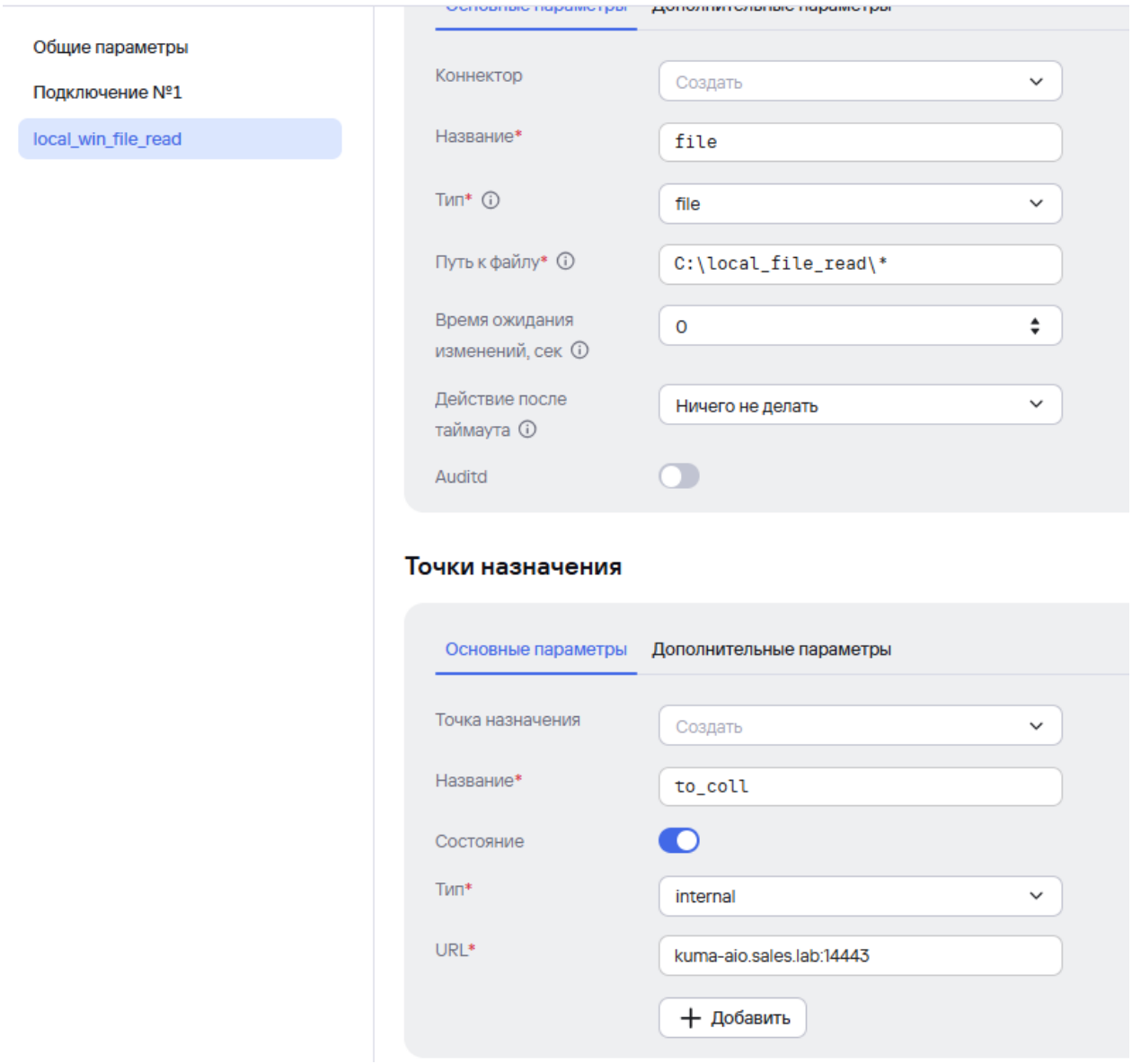


Есть также сторонняя утилита по стресс тестов - [Kraken STT - Kraken Stress Testing Toolkit (kraken-stt.ru)]

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



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

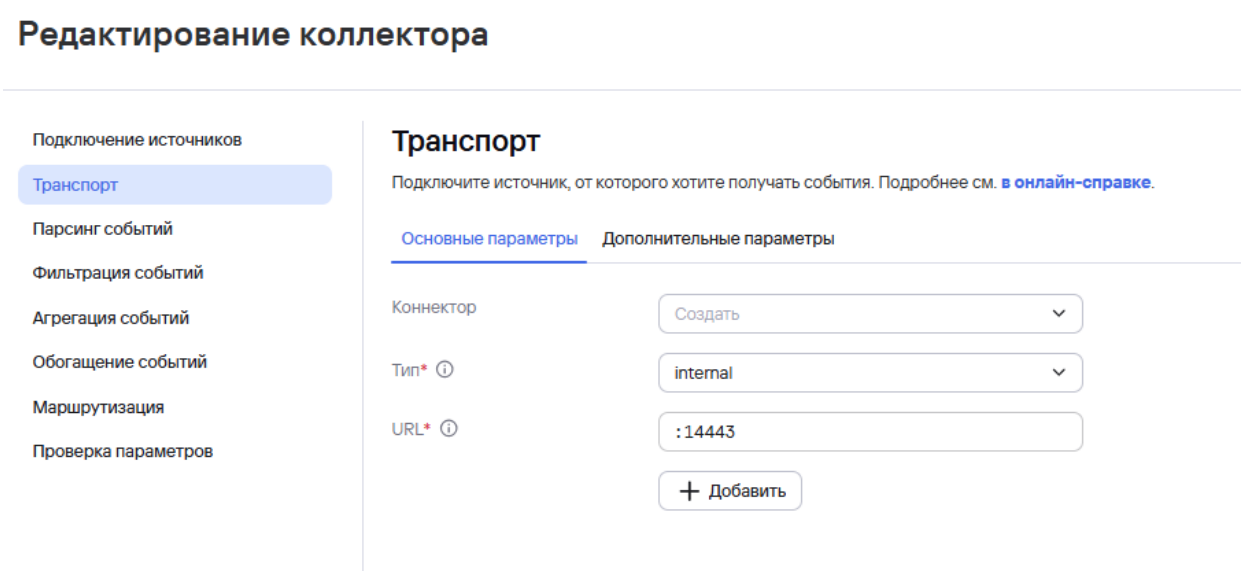


Недопустимо указывать пути, соответствующие следующим регулярным выражениям:

- `(?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`

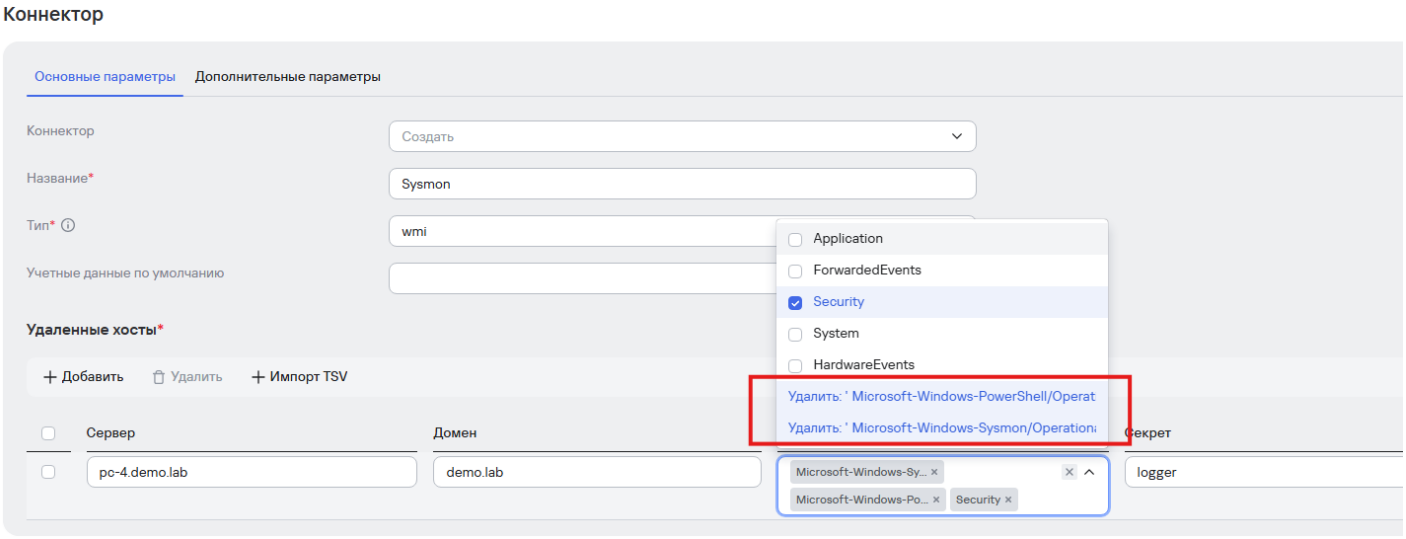
> Однако существует возможность читать файлы из системных директорий через создание символических ссылок: например, `mklink /D "C:\notsecret" "C:\Program Files (x86)\secret"` и в конфигурации агента указать `"C:\notsecret"`.

Соответственно прием на коллекторе тоже должен быть транспортом internal:



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

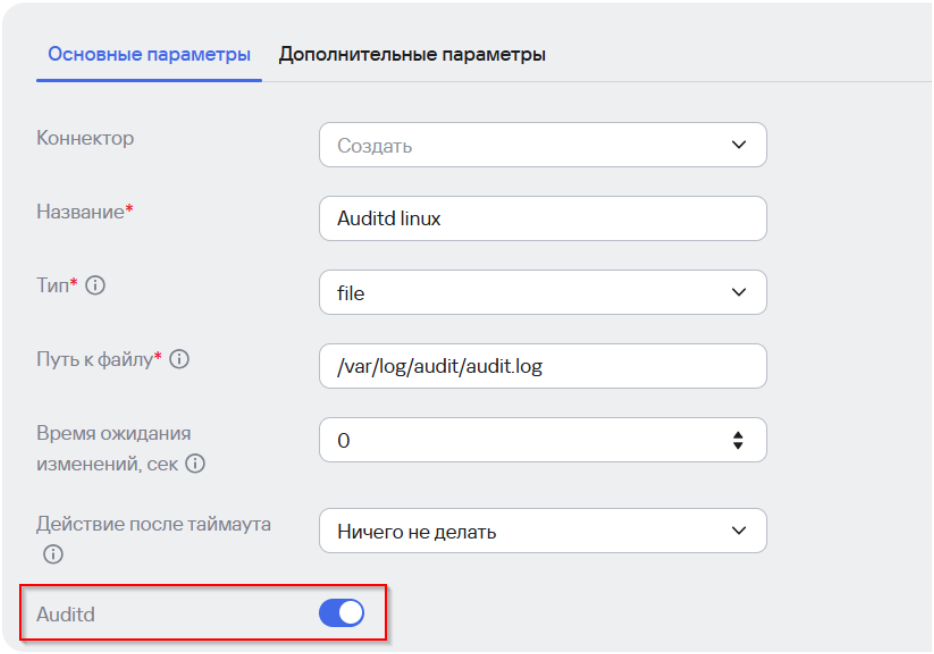
В поле журналов настройки коннектора просто вставьте путь к журналам, пример:



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

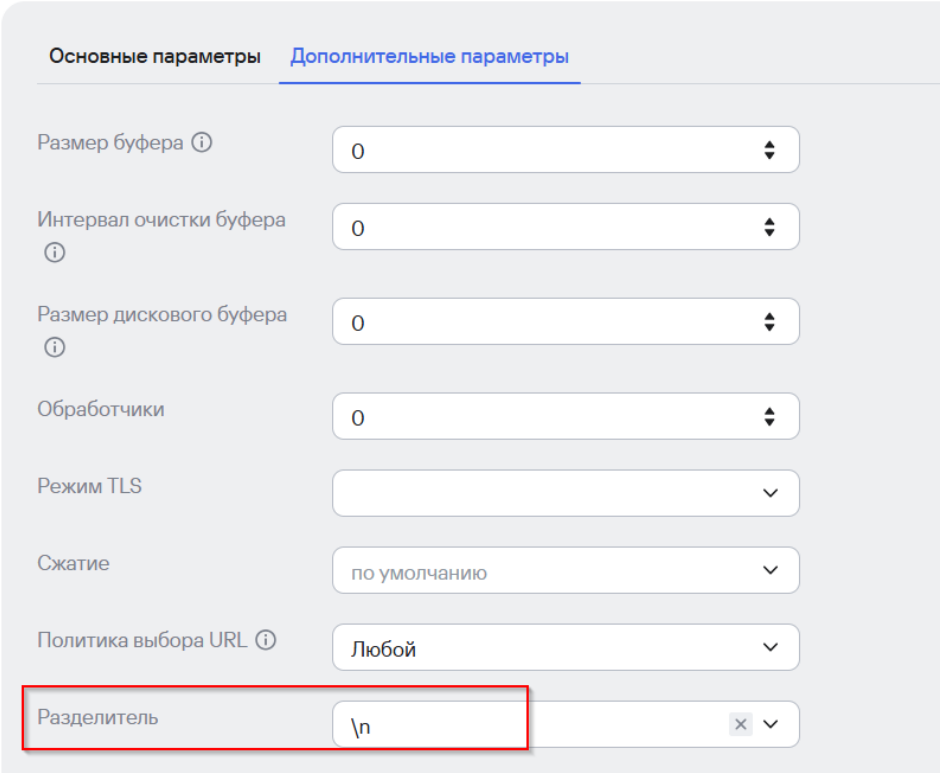
в настройках коннектора агента, поставьте флаг **Auditd**

Коннектор



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



Revision #10
Created 2023-08-14 07:48:21 UTC by Boris Rzr
Updated 2026-02-25 07:28:59 UTC by Koala