

Huawei (Syslog ? NetFlow)

Информация, приведенная на данной странице, является разработкой команды pre-sales и/или community KUMA и **НЕ** является официальной рекомендацией вендора.

???????? Syslog

Настройка может выполняться через командную строку под учетной записью с правами администратора.

```
#Настройка syslog
info-center channel 6 name Syslog_KUMA
info-center source default channel 6 log level informational
info-center loghost source <Название интерфейса, с которого будет происходить отправка
событий>
info-center loghost <IP-адрес коллектора KUMA> port <Порт коллектора KUMA> facility local7
severity warning
#Включение регистрации событий ввода команд
info-center command-log enable
info-center command-log size 100
info-center command-log timestamp
quit
save
```

???????? NetFlow

Настройка может выполняться через командную строку под учетной записью с правами администратора.

```
#Укажите интерфейс, из которого будут экспортироваться данные о потоке. Замените цифру «3»
фактическим номером интерфейса , если он отличается.
slot 3 (Replace "3" with your actual slot number if different.)
ip netstream sampler fix-packets 500 inbound
ip netstream sampler fix-packets 500 outbound
#Настройка параметров экспорта NetStream. Задайте параметры экспорта NetStream, включая версию,
исходный IP-адрес и IP-адрес хоста.
```

```
ip netstream timeout active 1
ip netstream timeout inactive 15
ip netstream export version 9 #вариативно, 5 или 9 версия
ip netstream export index-switch 32
ip netstream export template timeout-rate 1
ip netstream export source <адрес устройства>
ip netstream export host <IP-адрес KUMA коллектора> 2055 #порт по умолчанию - 2055, при
необходимости меняем
ip netstream export template option sampler
ip netstream export template option timeout-rate 1
ip netstream as-mode 32
#Включите NetFlow на интерфейсах, которые будут экспортировать данные о потоке.
ip netstream inbound
quit
save
```

????????? KUMA

После того как параметры передачи событий настроены, требуется создать коллекторы в веб-интерфейсе KUMA для событий Huawei. Отдельно - коллектор для Syslog и отдельный коллектор для приёма NetFlow.

Создание коллектора для приёма Syslog:

1. На шаге **Транспорт** укажите тип и порт в соответствии с настройками Syslog на стороне Huawei.
2. На шаге **Парсинг** событий выберите нормализатор [ООТВ] Huawei USG Basic (либо другой нормализатор, подходящий под Ваше устройство).
3. На шаге **Маршрутизация** проверьте, что в набор ресурсов коллектора добавлены следующие точки назначения:
 - **Хранилище**. Для отправки обработанных событий в хранилище.
 - **Коррелятор**. Для отправки обработанных событий в коррелятор.

Если точки назначения **Хранилище** и **Коррелятор** не добавлены, создайте их.

4. На шаге **Проверка параметров** нажмите **Сохранить и создать сервис**.

5. Скопируйте появившуюся команду для установки коллектора KUMA.

Создание коллектора для приёма NetFlow:

1. На шаге **Транспорт** укажите тип и порт в соответствии с настройками Netflow на стороне Huawei.

Задаём:

Тип netflow

url :2055 (либо порт - который был задан на этапе настройки со стороны Huawei)

2. На шаге **Парсинг** событий выберите нормализатор [OOTB] NetFlow v5 или [OOTB] NetFlow v9, в зависимости от выбранной версии на этапе настройки Huawei.

3. На шаге **Маршрутизация** проверьте, что в набор ресурсов коллектора добавлены следующие точки назначения:

- **Хранилище**. Для отправки обработанных событий в хранилище.
- **Коррелятор**. Для отправки обработанных событий в коррелятор.

Если точки назначения **Хранилище** и **Коррелятор** не добавлены, создайте их.

4. На шаге **Проверка параметров** нажмите **Сохранить и создать сервис**.

5. Скопируйте появившуюся команду для установки коллектора KUMA.

Revision #9

Created 2025-08-12 09:36:40 UTC by Anton

Updated 2025-08-15 14:26:15 UTC by Anton