

ViPNet Coordinator

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

Настройка ViPNet Coordinator

Для отправки событий ViPNet Coordinator в KUMA выполните следующее:

1. Подключитесь к консоли ViPNet Coordinator локально или через ssh.
2. Перейдите режим в Администратора с помощью следующей команды:

```
enable
```

3. Из командной строки в режиме Администратора выполните команду:

```
machine set loghost <ip-адрес коллектора KUMA>
```

После выполненных настроек ViPNet Coordinator будет отправлять системный журнал на адрес коллектора KUMA по протоколу UDP и 514-му порту.

В случае если коллектор KUMA является открытым узлом по отношению к ViPNet Coordinator, то также необходимо создать фильтр открытой сети, разрешающий исходящий трафик по протоколу UDP на 514-й порт коллектора KUMA.

Настройка KUMA

После того как параметры передачи событий настроены, требуется создать коллектор в веб-интерфейсе KUMA для событий ViPNet Coordinator.

1. На шаге **Транспорт** укажите тип UDP и порт 514.
2. На шаге **Парсинг** событий выберите нормализатор **[OOTB] VipNet Coordinator syslog**.

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.

Дополнительная настройка коллектора

После установки коллектора, необходимо внести изменения в файл сервиса коллектора для того, чтобы коллектор мог слушать входящие соединения на порту 514.

Для этого выполните следующие действия:

1. Остановите выполнение сервиса коллектора командой

```
systemctl stop kuma-collector-<id>
```

2. Откройте на редактирование файл коллектора `/usr/lib/systemd/system/kuma-collector-<id>.service`

3. В разделе **[Service]** добавьте следующую строку

```
AmbientCapabilities=CAP_NET_BIND_SERVICE
```

4. Сохраните полученный файл

5. Обновите параметры сервисов следующей командой

```
systemctl daemon-reload
```

6. Запустите службу коллектора следующей командой

```
systemctl start kuma-collector-<id>
```
