

KSMG 1.1

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

Официальная документация по данному разделу приведена в Онлайн-справке на продукт: <https://support.kaspersky.com/help/KUMA/2.1/ru-RU/254785.htm>

Настройка передачи событий KSMG в KUMA

Данная инструкция применима для KSMG версии 1.1

Чтобы настроить передачу событий KSMG в KUMA:

1. Подключитесь к серверу KSMG по проколу SSH под учетной записью с правами администратора перейдите в меню Technical Support Mode.

2. С помощью утилиты `ksmg-control` выгрузите настройки в файл `settings.xml`:

```
sudo /opt/kaspersky/ksmg/bin/ksmg-control --get-settings EventLogger -n -f /tmp/settings.xml
```

3. Убедитесь, что параметры файла `/tmp/settings.xml` имеют следующие значения, при необходимости внесите изменения:

```
<siemSettings>
<enabled>1</enabled>
<facility>Local1</facility>
```

4. Примените настройки с помощью следующей команды:

```
sudo /opt/kaspersky/ksmg/bin/ksmg-control --set-settings EventLogger -n -f /tmp/settings.xml
```

5. Для отправки событий по протоколу UDP внесите следующие изменения в конфигурационный файл `/etc/rsyslog.conf`.

```
$WorkDirectory /var/lib/rsyslog
$ActionQueueFileName ForwardToSIEM
$ActionQueueMaxDiskSpace 1g
$ActionQueueSaveOnShutdown on
$ActionQueueType LinkedList
$ActionResumeRetryCount -1
local1.* @<IP-адрес коллектора KUMA>:<порт коллектора>
```

Если вы хотите отправлять события по протоколу TCP, последняя строчка должна выглядеть следующим образом:

```
local1.* @@<IP-адрес коллектора KUMA>:<порт коллектора>
```

6. Сохраните внесённые изменения.

7. Перезапустите сервис rsyslog с помощью следующей команды:

```
sudo systemctl restart rsyslog.service
```

Настройка KUMA

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

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

2. На шаге **Парсинг** событий выберите нормализатор **[OOTB] KSMG**.

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.

Полезные ссылки

Настройка получения событий KSMG (онлайн-справка KUMA):

<https://support.kaspersky.com/help/KUMA/2.1/ru-RU/254785.htm>

Публикация событий в SIEM-систему (онлайн-справка KSMG):

<https://support.kaspersky.com/help/KSMG/1.1.3/ru-RU/151504.htm>

Revision #8

Created 11 August 2023 07:36:02 by Koala

Updated 26 November 2024 12:49:49 by Koala