

KWTS 6.0

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/254373.htm>

Настройка передачи событий KWTS в KUMA

Данная инструкция применима для KWTS версии 6.0

Чтобы настроить передачу событий KWTS в KUMA:

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

Перед внесением изменений создайте резервные копии следующих файлов:

- `/opt/kaspersky/kwts/share/templates/core_settings/event_logger.json.template`
- `/etc/rsyslog.conf`

2. Внесите следующие изменения в файл с параметрами экспорта событий

`/opt/kaspersky/kwts/share/templates/core_settings/event_logger.json.template` :

```
"siemSettings":
{
  "enabled": true,
  "facility": "Local5",
  "logLevel": "Info",
  "formatting":
{
```

Прочие параметры оставьте без изменений.

3. Внести изменения в файл `/etc/rsyslog.conf` :

```
$WorkDirectory /var/lib/rsyslog
$ActionQueueFileName ForwardToSIEM
$ActionQueueMaxDiskSpace 1g
$ActionQueueSaveOnShutdown on
$ActionQueueType LinkedList
$ActionResumeRetryCount -1
local5.* @<IP-адрес коллектора KUMA>:<порт коллектора>
```

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

```
local5.* @@<IP-адрес коллектора KUMA>:<порт коллектора>
```

4. Перезапустите сервис rsyslog с помощью следующей команды:

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

5. В веб-интерфейсе приложения в разделе **Параметры** → Syslog включите опцию **Записывать информацию о профиле трафика** и нажмите на кнопку **Сохранить**.

Дополнительный вариант логирования

Так как в CEF могут логироваться не все события, в некоторых случаях целесообразно будет также опрашивать в KUMA лог из `/var/log/kwts-messages`. В этом логге, например, содержится GUID, который позволяет связать события в KATA и KWTS при отправке файлов на проверку в KATA.

Для отправки на KUMA этих событий необходимо в файле `/etc/rsyslog.conf` добавить отправку событий с facility local1 в KUMA. Однако коллектор для этих целей потребует другой, т.к. логи в данном случае будут не в формате CEF, а в kv. Также это потребует и разработки кастомного парсера.

Чтобы настроить отправку local1 в KUMA нужно в конец файла дописать следующее для отправки по UDP:

```
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>
```

После 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 KWTS.

1. На шаге **Транспорт** укажите тип и порт в соответствии с настройками на стороне KWTS.
2. На шаге **Парсинг** событий выберите нормализатор **[OOTB] KWTS syslog CEF**.
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 KWTS (онлайн-справка KUMA):

<https://support.kaspersky.com/help/KUMA/2.1/ru-RU/254373.htm>

Revision #11

Created 11 August 2023 10:39:23 by Koala

Updated 26 November 2024 12:49:49 by Boris RZR