

Настройка отправки событий с FortiGate (CEF)

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

Настройка коллектора KUMA

Создание коллектора KUMA

Для приема и обработки событий с FortiGate необходимо создать сервис коллектора в KUMA. Для этого в веб-интерфейсе перейдите на вкладку **Ресурсы** и нажмите на кнопку

Подключить источник. В появившемся окне **Создание коллектора**:

- На шаге **Подключение источников** укажите **Имя коллектора** и **Тенант**, к которому будет принадлежать создаваемый коллектор

Создание коллектора

Подключение источников

Транспорт

Парсинг событий

Фильтрация событий

Агрегация событий

Обогащение событий

Маршрутизация

Проверка параметров

Подключение источников

Коллекторы используются для получения данных из источников событий, а также преобразования их в нормализованные события, понятные KUMA. С помощью коллектора можно также отсеивать ненужные события, объединять похожие события и обогащать события информацией из сторонних источников. Чтобы создать коллектор, следуйте шагам мастера. Подробнее см. [в онлайн-справке](#).

Название коллектора*

FortiGate UDP/5205 **1**

Тенант*

Main **2**

Обработчики

0

Отладка



Описание

Создать

Отмена

- На шаге **Транспорт** укажите **Тип** и **Порт** (данные параметры должны соответствовать настройкам на стороне FortiGate: **set mode** и **set port** соответственно)

Для распределенной инсталляции укажите hostname:port сервера коллектора в поле **URL**

Создание коллектора

Подключение источников

Транспорт

Парсинг событий

Фильтрация событий

Агрегация событий

Обогащение событий

Маршрутизация

Проверка параметров

Транспорт

Подключите источник, от которого хотите получать события. Подробнее см. [в онлайн-справке](#).

Основные параметры

Дополнительные параметры

Коннектор

Тип* ⓘ

URL* ⓘ

Разделитель

Создать

udp ⓘ 1

:5205 ⓘ 2

Создать

Отмена

- На шаге **Парсинг событий** укажите нормализатор. Рекомендуется использовать предустановленный нормализатор **[OOTB] Syslog-CEF** (<https://support.kaspersky.com/help/KUMA/3.0.3/ru-RU/255782.htm>).
- Если планируете использовать правила корреляции для FortiGate из Community-Pack необходимо использовать нормализатор **[2024-04-22] FortiGate Syslog-CEF**, также доступный в Community-Pack

Нормализатор

[OOTB] Syslog-CEF 1

Название*

[OOTB] Syslog-CEF

Метод парсинга*

syslog

Сохранить исходное событие*

При возникновении ошибок

Сохранить дополнительные поля*

Нет

+ Загрузить из файла

Ошибка коннектора. Невозможно скачать файл.

Примеры событий

Сопоставление

+ Добавить строку

Удалить

Применить сопоставление по умолчанию

Исходные данные		Поле KUMA	Подпись	Примеры
app	⇅⇅⇅	DeviceProcessName		
facility	⇅⇅⇅	DeviceFacility		

OK

Отмена

- Шаги мастера настройки с четвертого по шестой можно пропустить и вернуться к их настройке позднее.
- На седьмом шаге **Маршрутизация** задайте точки назначения. Для хранения событий добавьте точку назначения типа **Хранилище**. В случае если предполагается также корреляция по событиям добавьте точку назначения типа **Коррелятор**.

- Подключение источников
- Транспорт
- Парсинг событий
- Фильтрация событий
- Агрегация событий
- Обогащение событий
- Маршрутизация
- Проверка параметров

Маршрутизация

Укажите, куда следует отправлять полученные события. Подробнее см. [в онлайн-справке](#).

+ Добавить

Удалить

<input type="checkbox"/>	Название	Тип	URL
<input type="checkbox"/>	[OOTB] Storage 1	storage	localhost:7230
<input type="checkbox"/>	[OOTB] Correlator 2	correlator	localhost:7231

Создать

Отмена

- На завершающем шаге **Проверка параметров** нажмите на кнопку **Сохранить и создать сервис**. После чего появится команда установки сервиса, которую необходимо скопировать для дальнейшей установки.

- Подключение источников
- Транспорт
- Парсинг событий
- Фильтрация событий
- Агрегация событий
- Обогащение событий
- Маршрутизация
- Проверка параметров

Проверка параметров

Настройка коллектора завершена, сервис добавлен в KUMA. Подробнее см. [в онлайн-справке](#).
Чтобы начать получать события, сервис этого коллектора необходимо установить на сервере, предназначенном для сбора событий (см. пример команды установки ниже). Обратите внимание, что должна быть обеспечена сетевая связность компонентов системы и открыты порты.
Подробнее см. [в онлайн-справке](#).

Сервисы, использующие этот коллектор

Тип	Название
collector	FortiGate UDP/5205

- Сохранить и перезапустить сервисы
- Сохранить и обновить параметры сервисов

Рекомендуемая команда для установки коллектора

```
/opt/kaspersky/kuma/kuma collector --core https://kuma-aio.kaspersky.ru:7210 --id 9a9b81f9-50ae-4d8b-a833-d22ab08c7ecd --api.port 7249 --install
```

- Сохранить
- Отмена

Также после выполнения вышеуказанных действий на вкладке **Ресурсы > Активные сервисы** появится созданный сервис коллектора.

Ресурсы и сервисы / Сервисы

Сервисы

+ Добавить сервис

Обновить

Обновить параметры

Перезапустить

Сбросить сертификат

Удалить

⋮

fortigate udp

🔍

⚙️

<input type="checkbox"/>	Статус	Тип	Сервис	Версия	Тенант	Полное доменное имя	IP-адрес	Порт API	Время работы	Создан
<input type="checkbox"/>	<div>●</div>	Коллектор	FortiGate UDP/5205		Main					01.04.2024 18:45:21

Установка коллектора KUMA

Выполните подключение к CLI KUMA (установка коллектора выполняется с правами root).

Перед установкой рекомендуется выполнить из командной строки команду, скопированную на прошлом шаге без ключа **--install**, чтобы убедиться в отсутствии ошибок.

```
[root@kuma-aio ~]# /opt/kaspersky/kuma/kuma collector --core https://kuma-aio.kaspersky.ru:7210 --id 9a9b81f9-50ae-4d8b-a833-d22ab08c7ecd --api.port 7249
```

В случае отсутствия ошибок в выводе командной строки, прервите исполнение в командной строке, после чего можно переходить к установке.

Для установки сервиса коллектора в командной строке выполните команду, скопированную на прошлом шаге.

```
[root@kuma-aio ~]# /opt/kaspersky/kuma/kuma_collector --core https://kuma-aio.sail.m.lan:7218 --id 9a9b81f9-50ae-4d8b-a833-d22ab08c7ecd --api.port 7249 --install
Created symlink /etc/systemd/system/multi-user.target.wants/kuma-collector-9a9b81f9-50ae-4d8b-a833-d22ab08c7ecd.service → /usr/lib/systemd/system/kuma-collector-9a9b81f9-50ae-4d8b-a833-d22ab08c7ecd.service.
[root@kuma-aio ~]#
```

При необходимости добавьте порт коллектора в исключения фаервола и обновите параметры службы.

```
firewall-cmd --add-port=<порт, выбранный для коллектора>/udp --permanent
firewall-cmd --reload
```

После успешной установки сервиса его в статус в веб-интерфейсе KUMA изменится на **зеленый**.

Ресурсы и сервисы / Сервисы

Сервисы

+ Добавить сервис

Обновить

Обновить параметры

Перезапустить

Сбросить сертификат

Удалить

fortigate udp

<input type="checkbox"/>	Статус	Тип	Сервис	Версия	Тенант	Полное доменное имя	IP-адрес	Порт API	Время работы	Создан
<input type="checkbox"/>	<div></div>	Коллектор	FortiGate UDP/5205	2.0.0.0	Main	kuma-collector-9a9b81f9-50ae-4d8b-a833-d22ab08c7ecd	10.40.0.115	7249	38 секунд	01.04.2024 18:45:21

Настройка FortiGate

Для настройки отправки событий в формате CEF с FortiGate в KUMA выполните следующие действия:

- Подключитесь к CLI FortiGate по SSH
- Перейдите в секцию настройки параметров Syslog:

```
config log syslogd setting
```

- Выполните настройку параметров Syslog:

```
set status enable # включить отправки событий на удаленный Syslog-сервер
set server <IP-адреса сервера-коллектора KUMA>
set mode udp # отправлять события по UDP
set port <порт, заданный в параметрах коллектора KUMA>
set source-ip <IP-адрес FortiGate> # IP-адрес, который будет использоваться в качестве Source IP при
```

end

В открывшемся окне **События** убедитесь, что присутствуют события с FortiGate.

Kaspersky

Unified Monitoring and Analysis Platform

Выбрано tenants: 4

Панель мониторинга

Алерты

Инциденты

События

Активы

Отчеты

Ресурсы

Диспетчер задач

Параметры

Состояние источников

Метрики

borisov

События

Не обновлять

SELECT * FROM `events` WHERE ServiceID = '9a9b81f9-58ae-4d8b-a833-d22ab08c7ecd' ORDER BY Timestamp DESC LIMIT 10

Timestamp ↓	TenantID	DeviceProduct	DeviceVendor	DestinationUserNa...	Dest
01.04.2024 18:51:13	Main	Fortigate	Fortinet	admin	
01.04.2024 18:50:16	Main	Fortigate	Fortinet		

Информация о событии

TenantName	Main
Timestamp	01.04.2024 18:51:13.716
Name	eventsystem login success
EndTime	01.04.2024 18:51:22.000
Message	Administrator admin logged in successfully from ssh[IP]
DeviceAction	login
DeviceAddress	[IP]
DeviceAssetID	FortiGate-VM64
DeviceEventCategory	eventsystem
DeviceEventClassID	32001
DeviceExternalID	FGVMEVWMA2YKBF5A
DeviceFacility	23
DeviceHostName	FortiGate-VM64
DeviceProduct	Fortigate
DeviceReceiptTime	01.04.2024 18:51:22.000
DeviceTimeZone	+03:00
DeviceVendor	Fortinet
DeviceVersion	v6.4.15
SourceAddress	[IP]
SourceAssetID	[IP]
SourceProcessName	ssh([IP])
DestinationAddress	[IP]
DestinationAssetID	FortiGate-VM64

Полезные ссылки

Отправка событий в формате CEF - <https://community.fortinet.com/t5/FortiGate/Technical-Note-FortiGate-Logs-can-be-sent-to-syslog-servers-in/ta-p/190617>

Revision #7

Created 1 April 2024 15:30:24 by Dmitry Borisov

Updated 7 July 2024 08:51:49 by Koala