

FAQ

Ниже вы можете найти ответы на часто задаваемые вопросы, а также задать свои в комментариях

Q: ??? ?????? ????? ?????????????? KUMA?

A: Логи всех компонентов находятся по пути

```
/opt/kaspersky/kuma/<component>/<id>/log/<component>
```

<component> - collector, correlator, storage, agent

<id> - id соответствующего сервиса

- Логи core

- KUMA до 3.0 /opt/kaspersky/kuma/core/log/core

- KUMA 3.0 /opt/kaspersky/kuma/core/log/stdout.log и /opt/kaspersky/kuma/core/log/stderr.log

- KUMA 3.2 /opt/kaspersky/kuma/core/00000000-0000-0000-0000-000000000000/log/stdout.log и /opt/kaspersky/kuma/core/00000000-0000-0000-0000-000000000000/log/stderr.log

- Логи агента Windows C:\ProgramData\Kaspersky Lab\KUMA\agent\<id>\agent.log

- Логи mongodb /opt/kaspersky/kuma/mongodb/log/mongod.log

- Логи grafana /opt/kaspersky/kuma/grafana/data/log/grafana.log

Q: ??? ?????????????? id (?????????????????) ??????????

A: В веб-интерфейсе перейти на вкладку **Ресурсы - Активные сервисы**. Поставить галочку слева от нужного сервиса и в верхней части интерфейса выбрать **Копировать идентификатор**. Идентификатор сервиса будет скопирован.

Q: ??? ?????????????? ?????????? ?????????? ?? ??????????????

A: Можно воспользоваться утилитой nc (текстом и из файла):

```
nc <адрес коллектора> <порт коллектора> <<< "тестовое событие"
nc <адрес коллектора> <порт коллектора> < events.txt
```

Для отправки по udp нужно добавить к командам ключ `-u`

Также можно воспользоваться truss способом (для tcp и udp соответственно):

```
echo "тестовое событие" > /dev/tcp/<адрес коллектора>/<порт коллектора>
echo "тестовое событие" > /dev/udp/<адрес коллектора>/<порт коллектора>
```

Еще примеры - [тут](#).

Q: ??? ?????????? ??????? http-???????????

A: Для отправки события на http-коллектор используется POST запрос на URL

```
http://<collector ip/fqdn>:<port>/input
```

Событие помещается в body запроса.

Q: ??? ??????? ?????? ?? ??????????? ??????? KUMA?

A: Используются стандартные команды межсетевых экранов

firewalld (для Oracle Linux):

```
firewall-cmd --add-port=7220/tcp --permanent
firewall-cmd --reload
```

ufw (для Astra Linux):

```
ufw allow 7220/tcp
ufw reload
```

Q: ??? ?????????????????? ????? hosts ? Windows?

A: Запустите cmd.exe от имени администратора и выполните команду:

```
notepad.exe %WINDIR%\System32\drivers\etc\hosts
```

Внесите изменения в файл и сохраните (`Ctrl + S`)

Q: ?????? ?? ?????????????????? ?????????? ?????????? ?? ?????? ??????????

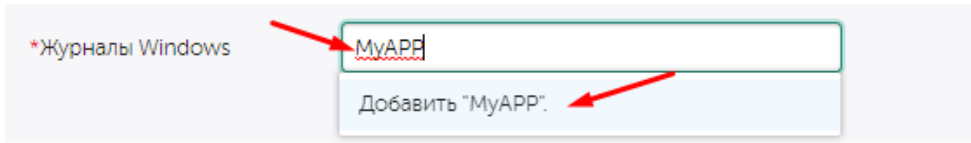
A: Официально, нет. Правильный способ - создавать сервис агента с несколькими Подключениями (Config's).

Q: ??? ?????????? ? URL udp/tcp ??????????????

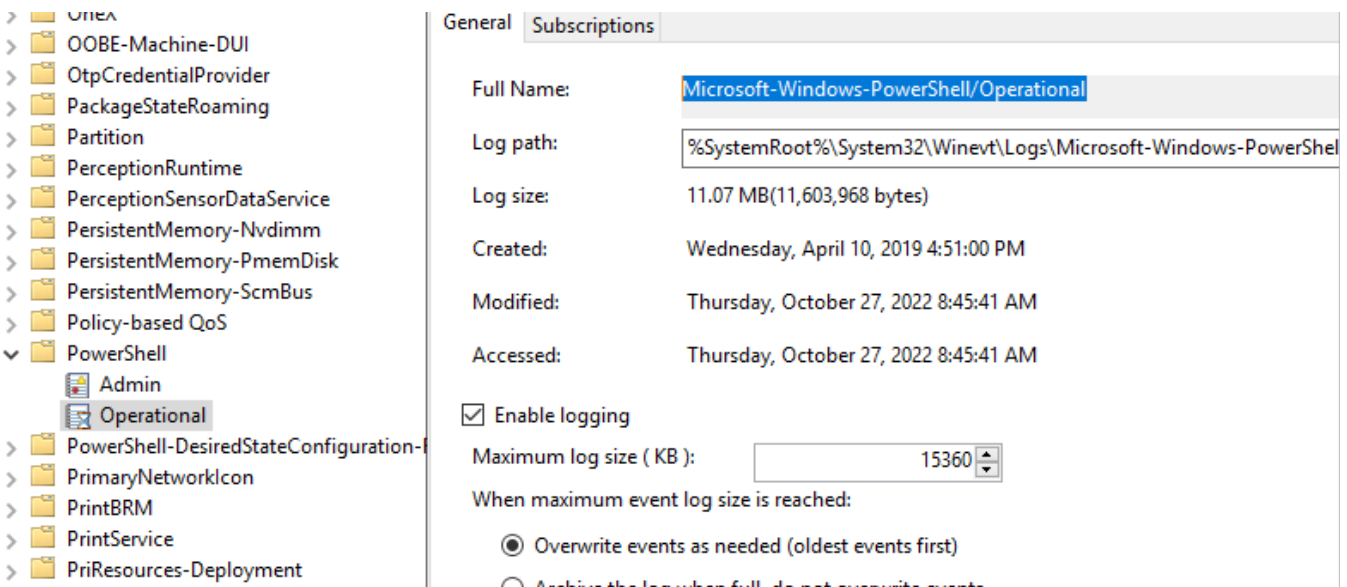
A: Достаточно указать просто порт через двоеточие, например, `:5151`

Q: ????? ???? ?????????? ?????????? ? Windows-????????? KUMA, ?? ????????? Powershell"

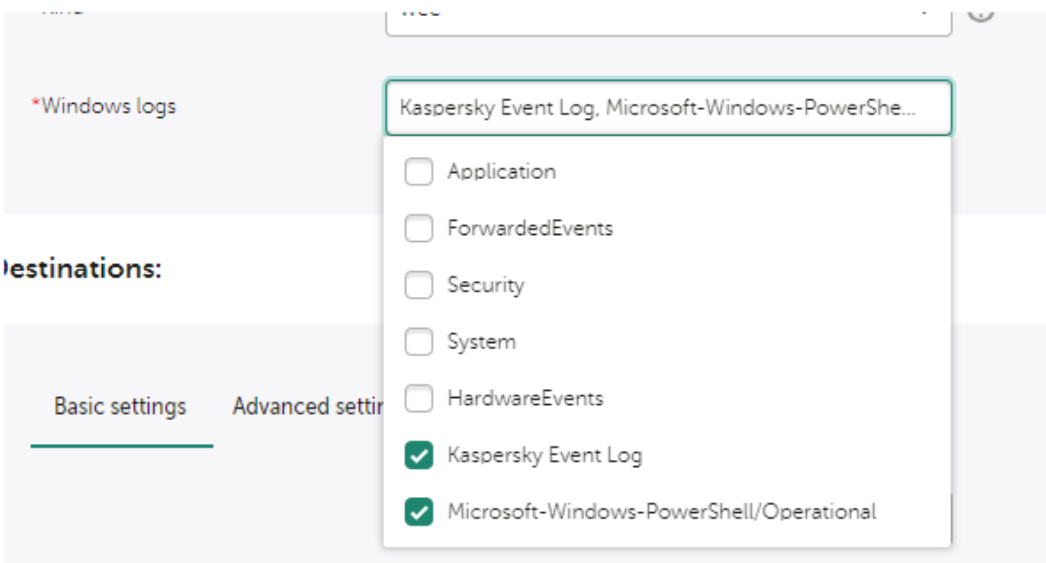
A: Если необходимо анализировать определенные журналы приложений, напишите имя журнала в выпадающем списке и нажмите Добавить.



Пример, с Powershell, сначала смотрим в свойствах журнала в EventViewer полное название:



Добавляем в агент:



Q: ?????? Windows-????????? ??? ?????????????? "No mapping between account names and security IDs was done."

A: Опечатка в логине пользователя, указанного в ключе `--user`

Q: ???????? KUMA ?? 2.1, ?? ????? ?????? kuma-clickhouse.service, ??? ?????????

A: Начиная с версии 2.1 отдельного микросервиса kuma-clickhouse больше нет. Clickhouse теперь дочерний процесс сервиса kuma-storage-`<id>`

Q: ??? ?????????? ?????????? ?????????? ?????????? ? ?????????????? WMI ? ?????????????? ?????????? kuma?

A: Агент обходит все серверы и пытается собрать с них логи. Если какой то сервер не доступен, агент запишет ошибку доступа в лог и перейдёт к следующему серверу в списке. К проблемному серверу в следующий раз придёт через 60 сек. И так до бесконечности. Если проблемный сервер оживет через 10 дней, то логи с него будут собираться автоматом. Это верно для версии 2.1.

Q: ??? ?????????? ???-???? ? ???? Timestamp?

A: Никак. Для записи временных меток пользователем есть поля EndTime, StartTime и другие.

Q: ??? ? ?????????? ?? ?????????? ??????????, ??? ?????? ?????????? ?????? ?????????????

A: `!= ''` для строковых полей и `!=0` для числовых. Пример:

```
SELECT * FROM `events` WHERE Name != '' AND SourcePort != 0
```

Q: ??? ?????????????? ?????????? ?????????? ?????????????? ?????????????? ? ?????????? ?? ?????????

A: Место можно посмотреть в вебе: **Активные сервисы - Хранилище - Смотреть разделы**

Q: ?????? ?????????????? ?????????? ?????????? ?????????????? ?????? KSC?

A: Однозначного ответа нет: сбор из БД не требует дополнительной лицензии; сбор в формате CEF требует лицензию Расширенный и выше; сбор Syslog требует долгой настройки, как на стороне KSC, так и на стороне нормализатора.

Q: ??? ?????????????? ?????????? ?????????????????????? ?????????????????? / ?????????????????????? ?? ??????????????

A: Онлайн-справка: <https://support.kaspersky.com/KUMA/2.1/ru-RU/255782.htm>

Q: ??? ?????????? ? ??? Extra ??? ?????????????? ??????????

A: С помощью конструкции `{{index .Extra "myField1"}}{{index .Extra "myField2"}}`

*Тип источника: шаблон

*Шаблон: `{{index .Extra "myField1"}}{{index .Extra "myField2"}}`

*Целевое поле: DeviceProcessName

Q: ????? ?? ???????????? KUMA ???????? ?? NAT?

A: Да, начиная с версии 2.1 компоненты KUMA умеют находиться за NAT. Для этого при установке сервисов нужно указать дополнительные параметры:

```
--advertise.api.port string  API port to be reported to Core
--advertise.fqdn string      FQDN to be reported to Core
```

Q: ??? ? ?????????????? ?????????????? ? ?????????????? ?????? ?????????????? ???????

A: У активных листов есть следующие служебные поля:

- `_count` (счетчик количества записей)
- `_created` (время создания записи UnixTime, в наносекундах)
- `_updated` (время обновления записи UnixTime, в наносекундах)
- `_expires` (время окончания жизни записи UnixTime, в наносекундах)
- `_key` (значение ключевой записи)

Q: ? ?????? ?????????? ?????????? ?????? ? ?????????? ?????????? ?? REST API?

A: Время задается в теле запроса в блоке `period` (в параметрах `from` и `to`). Для времени в UTC формат должен быть следующим:

```
YYYY-MM-DDThh:mm:ssZ
```

Пример:

```
2022-12-08T17:30:00Z
```

При необходимости, можно также указать таймзону в формате `+/-hh:mm` без пробела после времени и литеры `Z`

Пример:

```
2022-12-08T17:30:00+03:00
```

Q: ?????? ?????? KUMA ?? ???-????????????, ?? ?????? ?????????????? ID ???
????????? ? ?????????, ??? ?????? ID?

A: Можно в поиске событий выполнить запрос:

```
SELECT * FROM `events` WHERE DeviceAction = 'service deleted' AND Type=4 ORDER BY Timestamp  
DESC LIMIT 250
```

В результате поиска можно будет увидеть события удаления сервиса. ID сервиса будет в поле `DeviceExternalID`.

События

```
1 SELECT * FROM `events` WHERE DeviceAction = 'service deleted' AND Type=4 ORDER BY Timestamp DESC LIMIT 250
```

Нажмите Ctrl + Enter, чтобы выполнить запрос

TSV

TenantID	Timestamp	Name	DeviceProduct	DeviceVendor
Main	04.12.2024 11:22:40.793		KUMA	Kaspersky

Информация о событии

Копировать

TenantID	Main
Timestamp	04.12.2024 11:22:40.793
EndTime	04.12.2024 11:22:40.793
DeviceAction	service deleted
DeviceExternalID	<u>fba977e9-04e1-42cd-87e2-d60dd9474710</u>
DeviceFacility	collector
DeviceHostName	kuma-aio.sales.lab
DeviceProcessName	KEDR (API)
DeviceProduct	KUMA

Revision #34

Created 2023-08-11 12:00:42 UTC by Koala

Updated 2024-12-04 08:31:52 UTC by Koala