Docker via syslog

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

Общее

Настройка логирования Docker выполняется путем модификации `/etc/docker/daemon.json`, либо точечно для каждого контейнера через указание соответствующих параметров при запуске. В данной статье будет рассмотрен первый вариант.

Настройка Docker

1. Необходимо подключиться к ноде Docker

2. На ноде создать файл конфигурации `/etc/docker/daemon.json`, либо внести изменения в существующий. Пример файла конфигурации представлен ниже.

```
{
  "log-driver": "syslog",
  "log-opts": {
    "syslog-address": "tcp://10.10.10.10:6688",
    "tag": "{{.ID}}/{{.Name}}",
    "syslog-format": "rfc5424"
  }
}
```

Где, `10.10.10.10` - адрес коллектора KUMA, `66888` - порт коллектора KUMA. При необходимости можно также переопределить протокол передачи, формат логов и тегирование. Подробности см. по ссылке в конце статьи.

3. После внесения изменения в файл необходимо перезапустить службу Docker'а:

```
systemctl restart docker.service
```

В результате внесенных изменений события от Docker будут перенаправляться на сервис коллектора KUMA в соответствии с указанными параметрами.

> Альтернативно можно настроить логирование на стороне Docker в файл и перенаправлять его содержимое через rsyslog или путем монтирования папки/установки агента KUMA.

Настройка коллектора KUMA

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

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

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

> В дальнейшем можно использовать кастомные парсеры в зависимости от приложений, работающих в контейнерах Docker.

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

Документация по настройке syslog в Docker:

https://docs.docker.com/engine/logging/drivers/syslog/

Revision #1
Created 2024-10-24 09:56:33 UTC by Koala
Updated 2024-11-26 12:49:49 UTC by Koala