Apache Access Syslog

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

????????? Apache

Для настройки пересылки access-лога веб-сервера apache в KUMA необходимо выполнить следующие действия:

1. Подключитесь к веб-серверу Apache

2. Создайте конфигурационный файл `/etc/rsyslog.d/apache-access.log.conf` и добавьте в него следующие строки:

```
$ModLoad imfile
$InputFileName /var/log/apache2/access.log
$InputFileTag apache_access:
$InputFileStateFile stat-apache-access
$InputFileSeverity info
$InputFileFacility local3
$InputRunFileMonitor
$InputFilePollInterval 10
local3.* @<IP-адрес коллектора KUMA>:<порт коллектора>
```

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

```
local3.* @@<IP-адрес коллектора KUMA>:<порт коллектора>
```

3. Перезапустите службу rsyslog. Для этого выполните команду:

```
systemctl restart rsyslog
```

????????? KUMA

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

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

2. На шаге **Парсинг** событий выберите нормализатор **[OOTB] Apache Access Syslog (Common or Combined Log Format)**.

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.

Revision #4
Created 2023-08-16 07:22:33 UTC by Koala
Updated 2024-07-07 08:50:37 UTC by Koala