

Примеры работы с конфигурационными файлами

В данной статье приведена информация о работе с конфигурационными файлами, а также примеры кода, которые будут постоянно дополняться.

Общие сведения

Для обработки событий в Системе используется инструмент Logstash. **Logstash** — это инструмент для сбора, преобразования и доставки логических событий. Он часто используется для агрегации логов с множества машин в централизованное хранилище, например Elasticsearch или MongoDB, для последующего анализа с помощью Kibana или других инструментов.

Подробная информация о написании кода **Logstash** доступна в [официальной документации](#).

Также, конфигурационные файлы можно разрабатывать с помощью языка Ruby.

Подробная информация о написании кода на языке **Ruby** доступна в [официальной документации](#).

Примеры конфигурации

Конфигурация отправки данных во внешние SIEM-системы

Для того, чтобы настроить отправку журналов событий во внешнюю SIEM-систему, необходимо произвести интеграцию LogIQ с этой системой. Для этого выполните следующие действия:

Шаг 1. Подключитесь к серверу, на котором развернута Система и перейдите в директорию **[LogIQ]/services/saturn/**.

Шаг 2. Откройте файл **config.emv** и замените значения полей **MPSIEM_*_ID** на идентификаторы ваших событий.

Вы можете найти идентификаторы в разделе **Служебные события** в MP SIEM.

Шаг 3. При необходимости, включите фильтрацию на основании синхронизированных правил корреляции. Для этого поменяйте значение **MPSIEM_ENABLED** на **true**.

Шаг 4. Откройте конфигурационный файл пайплайна **output** (например, **saturn-pipeline/output_siem/_main.conf**) и отредактируйте его, указав следующие данные:

- **host:** укажите IP-адрес **MPSIEM-Server**;
- **user:** укажите логин учетной записи **rabbitmq**;
- **password:** укажите пароль учетной записи **rabbitmq**.

Ниже приведен пример содержимого конфигурационного файла:

```
output {
  rabbitmq {
    id => "output.siem"
    host => "x.x.x.x"
    user => "Login_rabbitmq_mpsiem"
    password => "Password_rabbitmq_mpsiem"
    exchange => "events"
    exchange_type => "topic"
    key => "normalizerq"
    vhost => "siem"
    batch_publish => true
    batch_size => 200
  }
}
```

Шаг 3. После того, как вы внесли изменения в файл, перезапустите все службы LogIQ.