Если вы видите что-то необычное, просто сообщите мне.

Как отличать различные типы логов в Logstash

Зачем вообще ризлчать логи?

Если вы собираете два набора логов используя один и тот же источник, вы возможно захотите разделить их таким образом, чтобы обработать каждый по отдельности.

Для примера, вы можете захотеть изменить имя индекса одного типа логов чтобы понимать, что это за лог.

Как разделить логи на два типа?

Деление между типами логов в Logstash может быть получено разыми путями. Если вы используете источники Elastic Beat: Auditbeat, Filebeat or Metricbeat у вас может быть много разделов в вашем конфигурациионном файле, для того, чтобы понять что за тип лога перед вами просто изменив конфигурационный файл и настроив тип с помощью различного именования.

Для примера, ниже мы редактируем Filebeat конфигурационный файл для разделения наших логов на различные типы.

```
filebeat.inputs:

- type: logType1
  enabled: true
  paths:
    - /var/folder_of_logs/*.log

- type: logType2
  enabled: true
  paths:
    - /var/another_folder_of_logs/*.log
  fields_under_root: true
```

В примере выше у нас есть две папки которые содержат лог.

- /var/folder_of_logs/
- /var/another_folder_of_logs/

Чтоб рассказать о разнице между логами которые получаются из этих двух папко, нам нужно добавить `logType1` для одного лога и `logType2` для другого набора логов. Отсюда мы можем использовать Logstash для дальнейшего различения между этих типов логов.

Использование Logstash для разделения логов на типы

Для дальнейшего разделения между типов логов, нам нужно использовать фильтр Logstash. Вы можете иметь доступ к фильтрам Logstash из дашборка для любой вашего Logit Stacks выбирая `View Stack Settings > Logstash Pipelines`.

Вы можете использовать Logstash для отбора типа лога в вашем Logstash фильтре и затем произведем действия основанные на этом условии. Для примера, мы можем захотеть изменить имя появлюящееся под ElasticSearch в Kibana.

```
if [type] == "logType1" {
  mutate {
    add_field => { "[@metadata][beat]" => "YOURINDEXNAME" }
  }
}
else if [type] == "logType2" {
  mutate {
     add_field => { "[@metadata][beat]" => "YOURINDEXNAMETWO" }
  }
}
```

Использование полей для пояснения типа логов.

Вы так же можете выбирать поля вашего лога для проверки типа лога если вы создали поле в вашем логе. Для примера, вы можете создать `mylog.type` поле и затем преобразовать это поле в `iis.logs`.

```
if [mylog][type] == "my-iis-logs" {
  mutate {
     rename => { "[mylog][type]" => "[iis][logs]" }
}
```

Revision #4
Created 29 July 2022 14:57:22 by gasick
Updated 16 April 2023 19:38:12 by gasick