LFS242 - Cloud Native Logging with Fluentd

Lab 4 – Extending Fluentd with Plugins: Creating Pipelines with Filter Plugins

- What plugins were loaded now?
  - forward, stdout
- What events will the `<filter>` directive capture?
  - All of them, because of the double wildcard (**) pattern in the opening
- How many times did Fluentd report that the worker is now running?
  - Once. It tried to report twice but internal Fluentd events are no longer being captured without a label.
- Using the filter_grep documentation on the Fluentd website, create a configuration that excludes all INFO events

```
<filter>
  @type grep
    <exclude>
      key message
      pattern INFO
    </exclude>
</filter>
```

- Find a pattern that will only print events that mention "file"

```
  @type grep
    <regexp>
      key message
      </regexp>
      pattern file
</filter>
```

- Will the original log message be preserved in this configuration? If so, under what key?
  - Yes, it will be nested under the "report" key.
- Will there be a password key appended to the record?
  - No. There is no "password" parameter being declared under the `<record>` subdirective, so no "password" key will be appended or edited.
- How many events were recorded?
  - Three. Two GET requests and one error.
- Use `cat` to read one of the NGINX log files, and compare how that log is presented in Elasticsearch.
  - NGINX log file

```
ubuntu@labsys:~/lab4$ cat /tmp/lab4/nginx/error.log

2021/07/22 20:04:02 [error] 31#31: *4 open() "/usr/share/nginx/html/404" failed (2: No such file or
directory), client: 172.17.0.1, server: localhost, request: "GET /404 HTTP/1.1", host: "172.17.0.2"
```

- Elasticsearch

```
...
{
```

```
  "_index" : "fluentd",
  "_type" : "_doc",
  "_id" : "ViHRz3oBbInj6EVHmnXs",
  "_score" : 1.0,
  "_source" : {
    "log_level" : "error",
    "pid" : "31",
    "tid" : "31",
    "message" : "*4 open() \"/usr/share/nginx/html/404\" failed (2: No such file or directory),
client: 172.17.0.1, server: localhost, request: \"GET /404 HTTP/1.1\", host: \"172.17.0.2\""
  }

...
```