LFS242 - Cloud Native Logging with Fluentd

Lab 5 – Working with Parser and Formatter plugins, processing Apache2 log data

- Who made the request?
  - The `curl` client
- From where was the request made?
  - A local address, noted as `::1`
- What tag was assigned to the event? Was this something that was set by the user?
  - apache2.access was set by the user as the `tag` parameter for the `<source>` directive tailing the Apache log
- What is the most significant difference between the two logs?
  - There are headers attached to each of the pieces of the log in the Fluentd event that are not present in the original.
- Remove the parse subdirective from the source directive; how did it turn out in Fluentd?
  - Fluentd didn't reload - the `<parse>` subdirective is required for the in_tail plugin
- Where is the container sending httpd logs?
  - The container is sending the httpd logs to the container's standard output, which is then forwarded to Fluentd
- Which part of the Fluentd event for the container has the actual httpd log content?
  - Actual log content is attached to the "log" key.
- How is the time different?
  - The time is formatted in a short date format (YY/MM/DD) without any milliseconds.
- Using the information on https://docs.ruby-lang.org/en/2.4.0/Time.html#method-i-strftime, change the time format.
  - One example being: `time_format %Y%m%dT%H%M%S%z` which will produce the following event:

```
20210722T202032+0000,apache2.access,
{"host":"127.0.0.1","user":null,"method":"GET","path":"/","code":200,"size":11173,"referer":null,"ag
ent":"curl/7.68.0"}
```