LFS242 - Cloud Native Logging with Fluentd

Lab 1-A – Installing and configuring Fluentd on Linux

- What types (plugins) are used in the sample config file above?
  - in_forward, in_http, in_unix, monitoring_agent, filter_record_transformer, filter_grep, debug_agent, out_file, out_stdout, out_forward, out_copy, out_null
- What is the path to the config file Fluentd is using?
  - /etc/fluent/fluent.conf
- What port is the Fluentd "forwarding server" using?
  - 24224 by default, used when no `port` parameter is specified
- How many plugins are registered for use? Are all of these mentioned in your config file?
  - Six total are in uncommented directives
- Issue the debug message several more times; what is different about each message?
  - The timestamp, which bears microsecond precision

Lab 1-B – Running Fluentd in a Docker environment

- What logging driver is dockerd using?
  - json_file
- A registry, in docker terms, is a network server from which container images can be downloaded, which "Registry" is docker using as a default?
  - https://index.docker.io/v1/
- The docker daemon (dockerd) is sometimes referred to as the docker server, what is the docker server version?
  - 20.10.7
- In docker, plugins extend the functionality of the basic dockerd services, what log plugins are available?
  - awslogs fluentd gcplogs gelf journald json-file local logentries splunk syslog
- What type of input plugins are being used in this configuration?
  - in_forward and in_http
- What ports will Fluentd be listening on?
  - Port 24220 for HTTP traffic and 24224 for Fluentd traffic
- What type of output plugins are being used in this configuration?
  - out_stdout
- Identify the log lines that report docker downloading the Fluentd container image
  - Lines like `b73585fcd1ae: Pull complete` indicate that parts of the Fluentd container image are being downloaded
- Locate the log output that reports the Fluentd configuration file in use
  - `2021-07-22 18:14:32 +0000 [info]: parsing config file is succeeded path="/fluentd/etc/docker.conf"`
- What version of Fluentd is running in the container?
  - Version 1.13.2

- How did the route in the curl command (`/test`) manifest in the container output?
  - As a plain JSON map, resulting in {"hi":"mom"}
- Try this curl command: `curl -X POST -d 'json={"hi":"mom"}' http://localhost:24220/test/ing`
  - `2021-07-22 18:19:12.022070131 +0000 test.ing: {"hi":"mom"}``
- Try this curl command:
  `curl -X POST -d 'json={"hi":"mom", "severity":"superbad"}' http://localhost:24220/test/ing`
  - `2021-07-22 18:19:29.542448298 +0000 test.ing: {"hi":"mom","severity":"superbad"}`
- Where did the logged event come from?
  - The nginx container.
- What is the actual event text?
  - `172.17.0.1 - - [22/Jul/2021:18:21:54 +0000] \"GET / HTTP/1.1\" 200 612 \"-\" \"curl/7.68.0\" \"-\"`