Exploring Logs Collection and Shipping

In this lesson, we will explore two different contestants which we can use to explore logs collection and shipping.

WE'LL COVER THE FOLLOWING

Logstash & Fluentd

For a long time now, there have been two major contestants for the “logs collection and shipping” throne. Those are Logstash and Fluentd. Both are open-source, and both are widely accepted and actively maintained. While both have their pros and cons, **Fluentd** turned up to have an edge with cloud-native distributed systems. It consumes fewer resources and, more importantly, it is not tied to a single destination (**Elasticsearch**). While **Logstash** can push logs to many different targets, it is primarily designed to work with **Elasticsearch**. For that reason, other logging solutions adopted **Fluentd**. As of today, no matter which logging product you embrace, the chances are that it will support **Fluentd**. The culmination of that adoption can be seen by **Fluentd’s** entry into the list of Cloud Native Computing Foundation projects. Even **Elasticsearch** users are adopting **Fluentd** over **Logstash**. What was previously commonly referred to as ELK (*Elasticsearch*, **Logstash**, **Kibana**) stack, is now called EFK (**Elasticsearch**, **Fluentd**, **Kibana**).

We’ll follow the trend and adopt **Fluentd** as the solution for collecting and shipping logs, no matter whether the destination is **Papertrail**, **Elasticsearch**, or something else.

We’ll install **Fluentd** soon. But, since **Papertrail** is our first target, we need to create and set up an account. For now, remember that we need to collect logs from all the nodes of the cluster and, as you already know, Kubernetes’ DaemonSet will ensure that a **Fluentd** Pod will run in each of our servers.

Q

While **Logstash** can push logs to many different targets, it is primarily designed to work with **Elasticsearch**.

COMPLETED 0%

1 of 1

In the next lesson, we will explore centralized logging through **Papertrail**.