THE LINUX FOUNDATION | Training & Certification

KUBERNETES FUNDAMENTALS (LFS258)

SUPPORT SIGN OUT

LOGGING AND TROUBLESHOOTING

Logging and Troubleshooting

Logging Tools

Logging, like monitoring, is a vast subject in IT. It has many tools that you can use as part of your arsenal.

Typically, logs are collected locally and aggregated before being ingested by a search engine and displayed via a dashboard which can use the search syntax. While there are many software stacks that you can use for logging, the Elasticsearch, Logstash, and Kibana Stack (ELK) has become quite common.

In Kubernetes, the kubelet writes container logs to local files (via the Docker logging driver). The **`kubectl logs`** command allows you to retrieve these logs.

Cluster-wide, you can use Fluentd to aggregate logs. Check out the cluster administration logging concepts for a detailed description.

Fluentd is part of the Cloud Native Computing Foundation and, together with Prometheus, they make a nice combination for monitoring and logging.

Setting up Fluentd for Kubernetes logging is a good exercise in understanding DaemonSets. Fluentd agents run on each node via a DaemonSet, they aggregate the logs, and feed them to an Elasticsearch instance prior to visualization in a Kibana dashboard.