Step1: Deploy ES Cluster

Step2: Deploy Kibana

Step3: Deploy FluentD

Step4: Deploy Nginx App

<https://kubernetes.io/docs/concepts/cluster-administration/logging/>

<https://kubernetes.io/docs/tasks/debug-application-cluster/>

**Master**

* /var/log/kube-apiserver.log - API Server, responsible for serving the API
* /var/log/kube-scheduler.log - Scheduler, responsible for making scheduling decisions
* /var/log/kube-controller-manager.log - Controller that manages replication controllers

### **Worker Nodes**

* /var/log/kubelet.log - Kubelet, responsible for running containers on the node
* /var/log/kube-proxy.log - Kube Proxy, responsible for service load balancing

About Elastisearch : <https://www.slideshare.net/richu100/elasticsearch-vs-relational-database>

Kubectl logs <podname> can only provide logs for a single pod. For getting logs for multiple containers, we can use the plug-in **mtail.**

To install mtail, we need the krew plugin manager installed first. Refer to the document “K8S-Tools-Plugins” for further details.