RUN ELK stack on kubernetes

<https://www.digitalocean.com/community/tutorials/how-to-set-up-an-elasticsearch-fluentd-and-kibana-efk-logging-stack-on-kubernetes>

1 kube-logging.yaml

2 elasticsearch\_statefulset.yaml

3 kibana.yaml

**Elasticsearch** is a real-time, distributed, and scalable search engine which allows for full-text and structured search, as well as analytics.

Elasticsearch is commonly deployed alongside **Kibana**, a powerful data visualization frontend and dashboard for Elasticsearch.

We’ll use **Fluentd** to collect, transform, and ship log data to the Elasticsearch backend. Fluentd is a popular open-source data collector that we’ll set up on our Kubernetes nodes to tail container log files, filter and transform the log data, and deliver it to the Elasticsearch cluster, where it will be indexed and stored.

Important:

KIBANA\_POD=$(kubectl get pods -l app=kibana -o jsonpath='{.items[0].metadata.name}')

​

​

kubectl port-forward $KIBANA\_POD 5601:5601 & //& is used to run it even after it(port forwarding) closes

​

kubectl expose deployment els --type=LoadBalancer --name=eslb

​

ps aux | grep kibana

kill -9 process id//to kill the running kibana aon port where u are able to access it.

kubectl -n kube-logging get all //to get all services

kubectl get namespaces

1 nano kube-logging.yaml

Kubectl apply –f kube-logging.yaml

kubectl -n kube-logging get all

2 nano elasticsearch\_svc.yaml

Kubectl apply –f elasticsearch\_svc.yaml

Note : change

storageClassName: standard

3 kubectl port-forward es-cluster-0 9200:9200 --namespace=kube-logging

4 Then, in a separate terminal window, perform a curl request against the REST API:

* curl http://localhost:9200/\_cluster/state?pretty

5 nano kibana.yaml

kubectl create -f kibana.yaml

kubectl rollout status deployment/kibana --namespace=kube-logging

kubectl get pods --namespace=kube-logging

kubectl port-forward kibana-6c9fb4b5b7-plbg2 5601:5601 --namespace=kube-logging

note port name keeps changing

write an env query to fetch the latest port

kubectl port-forward es-cluster-0 9200:9200 --namespace=kube-logging