--------------------

EFK stack setup LAB

--------------------

First, we need deploy an application in k8s cluster and we do some operations

# kubectl get pods

# kubectl get nodes

We can see two worker nodes are running in our k8s cluster

We have a docker image and the same is stored in the Docker hub and same needs to be used in our application log checking

We have deployment.yml file in machine, using this deployment.yml we can create the application

# vim deployment.yml

---

apiVersion: apps/v1

kind: Deployment

metadata:

name: sbwebappdeplyment

spec:

replicas: 2

strategy:

type: RollingUpdate

selector:

matchLabels:

app: my-web-app

template:

metadata:

name: sbwebapppod

labels:

app: my-web-app

version: v1

color: blue

spec:

containers:

- name: sbwebappcontainer

image: vinodses/my-web-app

---

apiVersion: v1

kind: Service

metadata:

name: sbappsvc

spec:

type: LoadBalancer

selector:

app: my-web-app

ports:

- port: 80

targetPort: 8080

...

# kubectl apply -f deployment.yml

using this deployment.yml my application got created and service also created.

We can verify that using

# kubectl get pods

# kubectl get svc

# kubectl get all

what all the components got created will be listed

first, we need to take that load balancer url and paste in our browser

So that we can see our application url loadbalancer url

http://loadBalancer-url:my-web-app

We perform some operating in my application, then application will generate some logs. Using that logs we will get an idea whether my application is working or not

# kubectl logs <pod name>

can monitor the pod logs

Now we want to install EFK stack in our k8s cluster (fluentd,elastic search,kibana)

We need to clone these yaml files from the git hub repository

# git clone https://github.com/suffixscope/efkstack.git

We have 7 manifest yml file, the first one namespace yml file and next two are elastic search yml file, next two are fluntd yml file and 2 more yaml file for kibana deployment

inside the namespace manifest yml file , can see the efklog as namespace name

Elastic search is displayed as stateful set and its port number 9200

fluentd will be deployed as deamonset - deamonset means a copy of the pod will be created on all the nodes which we have running in our cluster

kibana will be displayed as deployment and kibana pods should be exposed to load balancer service type. So that we can access the kibana dashboard from outside the k8s cluster

# cd efkstack

# kubectl apply -f .

all the manifest.yml file will be executed

# kubectl get all -n efklog

In this namespace we can see what are resources created in our k8s cluster

Now we want to access the kibana dashboard to view the logs of our application

kibana service type as load balancer. Loadbalancer URL is available and that LB is exposing the port number 5601

got to aws load balancer the take LB dns name and poste in our browser

http://kibana loadbalancer url:5601

Then one kibana dashboard will open there you can click explore on my own

click on discover there set the index pattern as \* and in the filter field select @timestamp and same

once we done go to discover again there you can see the application logs

we have filter option through that way we can filter the logs of our application