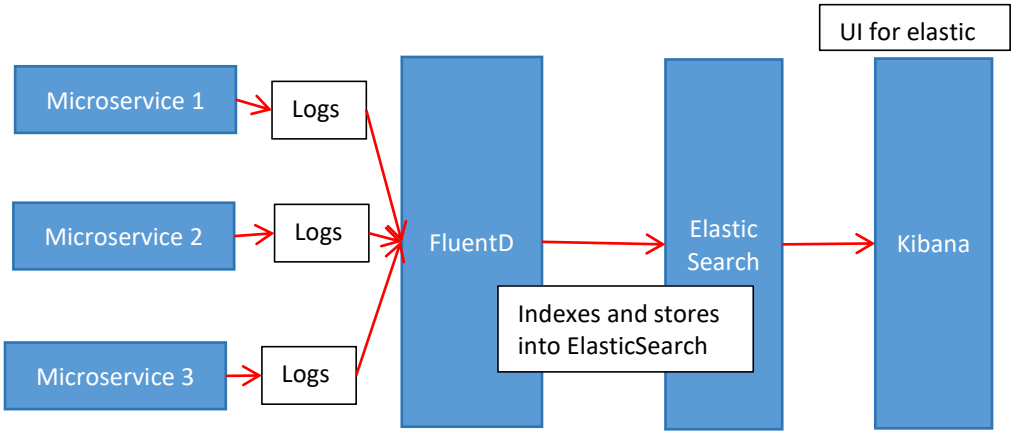
Kubernetes 7
EFK -> Elasticsearch FluentD Kibana

One component we use to read Logs and store into Elasticsearch, it is FluentD



We need Kibana to visualize those Logs

Pod in the end of the day it is our application

Create K8s cluster
eksctl create cluster --name my-eks-cluster --region ca-central-1 --node-type t2.medium --zones ca-central-1a,ca-central-1b

ubuntu@ip-172-31-9-165:~/blue-green-model$ cat blue-deployment.yml

```
---
apiVersion: apps/v1
kind: Deployment
metadata:
 name: javawebbluedeploy
spec:
 replicas: 2
 strategy:
  type: RollingUpdate
 selector:
  matchLabels:
   app: java-web-app
   version: v1
   color: blue
 template:
  metadata:
   labels:
    app: java-web-app
    version: v1
    color: blue
  spec:
   containers:
    - name: javawebappcontainer
      image: hacker123shiva/springbt-in-docker:latest
      imagePullPolicy: Always
      ports:
       - containerPort: 8080
...
```

```
ubuntu@ip-172-31-9-165:~/ElasticSearch$ kubectl apply -f deployment.yml
deployment.apps/javawebbluedeploy created
service/javaappsvc created

---
apiVersion: apps/v1
kind: Deployment
metadata:
  name: javawebbluedeploy
spec:
  replicas: 2
  strategy:
    type: RollingUpdate
  selector:
    matchLabels:
      app: java-web-app
      version: v1
      color: blue
  template:
    metadata:
      labels:
        app: java-web-app
        version: v1
        color: blue
    spec:
      containers:
        - name: javawebappcontainer
          image: hacker123shiva/springbt-in-docker:latest
          imagePullPolicy: Always
          ports:
           - containerPort: 8080
---
apiVersion: v1
kind: Service
metadata:
  name: javaappsvc
spec:
  type: LoadBalancer
  selector:
    app: java-web-app
  ports:
    - port: 80
      targetPort: 8080
...

ubuntu@ip-172-31-9-165:~/ElasticSearch$
ubuntu@ip-172-31-9-165:~/ElasticSearch$ kubectl get pods
NAME                          READY   STATUS    RESTARTS   AGE
javawebbluedeploy-68fc6554d6-lb9tm   1/1     Running   0        82s
javawebbluedeploy-68fc6554d6-zsqkt   1/1     Running   0        82s


ubuntu@ip-172-31-9-165:~/ElasticSearch$ kubectl get all
NAME                              READY   STATUS    RESTARTS   AGE
pod/javawebbluedeploy-68fc6554d6-lb9tm   1/1     Running   0        2m27s
pod/javawebbluedeploy-68fc6554d6-zsqkt   1/1     Running   0        2m27s
```

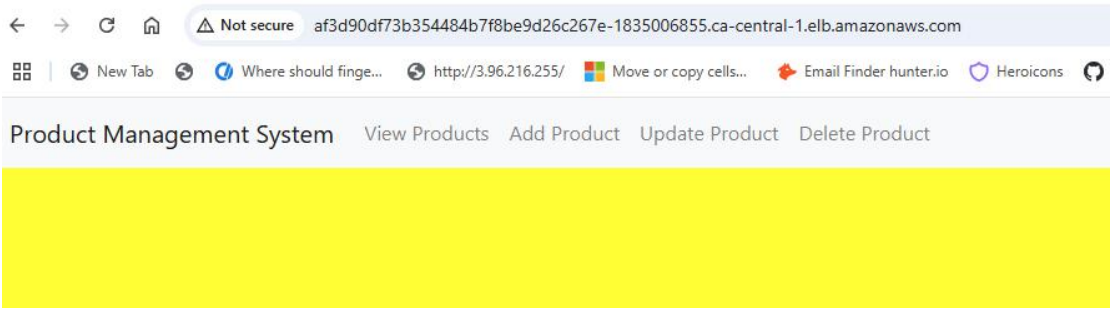
NAME TYPE CLUSTER-IP EXTERNAL-IP PORT(S) AGE
service/javaappsvc LoadBalancer 10.100.252.5 af3d90df73b354484b7f8be9d26c267e-1835006855.ca-central-1.elb.amazonaws.com 80:31177/TCP 2m27s
service/kubernetes ClusterIP 10.100.0.1 <none> 443/TCP 74m

NAME READY UP-TO-DATE AVAILABLE AGE
deployment.apps/javawebbluedeploy 2/2 2 2 2m27s

NAME DESIRED CURRENT READY AGE
replicaset.apps/javawebbluedeploy-68fc6554d6 2 2 2 2m27s

```
ubuntu@ip-172-31-9-165:~/ElasticSearch$
ubuntu@ip-172-31-9-165:~/ElasticSearch$ kubectl apply -f deployment.yml
deployment.apps/javawebbluedeploy created
service/javaappsvc created
ubuntu@ip-172-31-9-165:~/ElasticSearch$ vi deployment.yml
ubuntu@ip-172-31-9-165:~/ElasticSearch$
ubuntu@ip-172-31-9-165:~/ElasticSearch$
ubuntu@ip-172-31-9-165:~/ElasticSearch$ kubectl get pods
NAME                                   READY   STATUS    RESTARTS   AGE
javawebbluedeploy-68fc6554d6-lb9tm   1/1     Running   0          82s
javawebbluedeploy-68fc6554d6-zsqkt   1/1     Running   0          82s
ubuntu@ip-172-31-9-165:~/ElasticSearch$
ubuntu@ip-172-31-9-165:~/ElasticSearch$
ubuntu@ip-172-31-9-165:~/ElasticSearch$ kubectl get all
NAME                                       READY   STATUS    RESTARTS   AGE
pod/javawebbluedeploy-68fc6554d6-lb9tm   1/1     Running   0          2m27s
pod/javawebbluedeploy-68fc6554d6-zsqkt   1/1     Running   0          2m27s

NAME                 TYPE           CLUSTER-IP     EXTERNAL-IP                                                                PORT(S)
service/javaappsvc   LoadBalancer   10.100.252.5   af3d90df73b354484b7f8be9d26c267e-1835006855.ca-central-1.elb.amazonaws.com   80:31177/TCP
service/kubernetes   ClusterIP      10.100.0.1     <none>                                                                     443/TCP

NAME                                   READY   UP-TO-DATE   AVAILABLE   AGE
deployment.apps/javawebbluedeploy   2/2     2            2           2m27s

NAME                                             DESIRED   CURRENT   READY   AGE
replicaset.apps/javawebbluedeploy-68fc6554d6   2         2         2       2m27s
ubuntu@ip-172-31-9-165:~/ElasticSearch$
```

Application URL: af3d90df73b354484b7f8be9d26c267e-1835006855.ca-central-1.elb.amazonaws.com

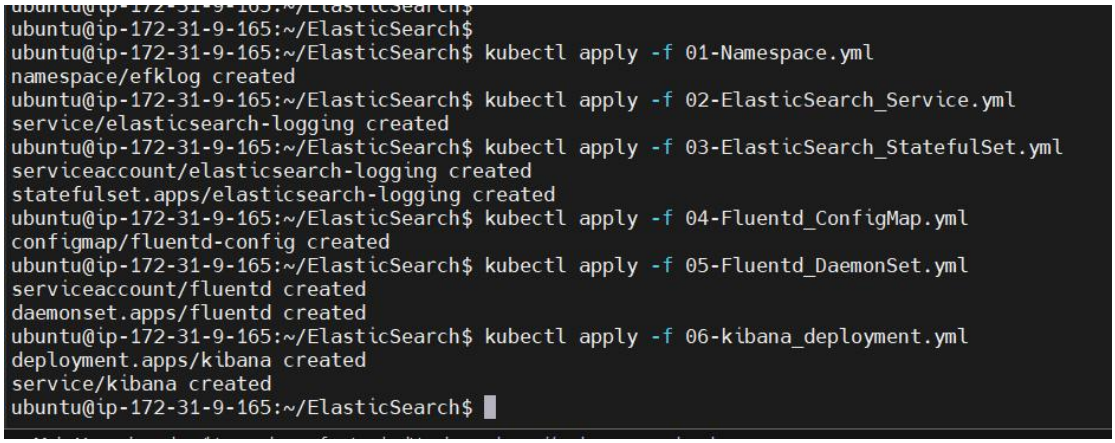


Monitoring application is one part, monitoring cluster is another part

ubuntu@ip-172-31-9-165:~/ElasticSearch$ cat 02-ElasticSearch_Service.yml

```
---
apiVersion: v1
kind: Service
metadata:
  name: elasticsearch-logging
  namespace: efklog
  labels:
    k8s-app: elasticsearch-logging
    kubernetes.io/cluster-service: "true"
    addonmanager.kubernetes.io/mode: Reconcile
    kubernetes.io/name: "Elasticsearch"
spec:
  ports:
```

```
  - port: 9200
    protocol: TCP
    targetPort: db
  selector:
    k8s-app: elasticsearch-logging
...

ubuntu@ip-172-31-9-165:~/ElasticSearch$ ls -l
total 28
-rw-rw-r-- 1 ubuntu ubuntu   65 Jun 15 00:48 01-Namespace.yml
-rw-rw-r-- 1 ubuntu ubuntu  387 Jun 15 01:12 02-ElasticSearch_Service.yml
-rw-rw-r-- 1 ubuntu ubuntu 1466 Jun 15 02:12 03-ElasticSearch_StatefulSet.yml
-rw-rw-r-- 1 ubuntu ubuntu  890 Jun 15 02:18 04-Fluentd_ConfigMap.yml
-rw-rw-r-- 1 ubuntu ubuntu 1495 Jun 15 02:16 05-Fluentd_DaemonSet.yml
-rw-rw-r-- 1 ubuntu ubuntu  737 Jun 15 02:27 Kibana_Deployment.yml
-rw-rw-r-- 1 ubuntu ubuntu  711 Jun 14 22:59 deployment.yml
ubuntu@ip-172-31-9-165:~/ElasticSearch$ mv Kibana_Deployment.yml 06-kibana_deployment.yml
ubuntu@ip-172-31-9-165:~/ElasticSearch$
ubuntu@ip-172-31-9-165:~/ElasticSearch$
ubuntu@ip-172-31-9-165:~/ElasticSearch$ kubectl apply -f 01-Namespace.yml
namespace/efklog created
ubuntu@ip-172-31-9-165:~/ElasticSearch$ kubectl apply -f 02-ElasticSearch_Service.yml
service/elasticsearch-logging created
ubuntu@ip-172-31-9-165:~/ElasticSearch$ kubectl apply -f 03-ElasticSearch_StatefulSet.yml
serviceaccount/elasticsearch-logging created
statefulset.apps/elasticsearch-logging created
ubuntu@ip-172-31-9-165:~/ElasticSearch$ kubectl apply -f 04-Fluentd_ConfigMap.yml
configmap/fluentd-config created
ubuntu@ip-172-31-9-165:~/ElasticSearch$ kubectl apply -f 05-Fluentd_DaemonSet.yml
serviceaccount/fluentd created
daemonset.apps/fluentd created
ubuntu@ip-172-31-9-165:~/ElasticSearch$ kubectl apply -f 06-kibana_deployment.yml
deployment.apps/kibana created
service/kibana created
ubuntu@ip-172-31-9-165:~/ElasticSearch$
```

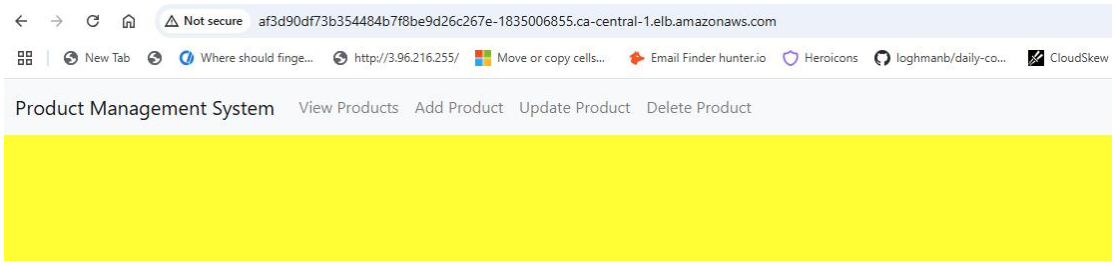


Alternative for EFK is Splunk

```
ubuntu@ip-172-31-9-165:~/ElasticSearch$
ubuntu@ip-172-31-9-165:~/ElasticSearch$ kubectl get all
NAME                                        READY   STATUS    RESTARTS   AGE
pod/javawebbluedeploy-68fc6554d6-lb9tm      1/1     Running   0          3h34m
pod/javawebbluedeploy-68fc6554d6-zsqkt      1/1     Running   0          3h34m

NAME                 TYPE           CLUSTER-IP     EXTERNAL-IP                                                              PORT(S)
service/javaappsvc   LoadBalancer   10.100.252.5   af3d90df73b354484b7f8be9d26c267e-1835006855.ca-central-1.elb.amazonaws.com   80:31177/TCP
service/kubernetes   ClusterIP      10.100.0.1     <none>                                                                   443/TCP

NAME                                   READY   UP-TO-DATE   AVAILABLE   AGE
deployment.apps/javawebbluedeploy      2/2     2            2           3h34m

NAME                                              DESIRED   CURRENT   READY   AGE
replicaset.apps/javawebbluedeploy-68fc6554d6      2         2         2       3h34m
ubuntu@ip-172-31-9-165:~/ElasticSearch$
```

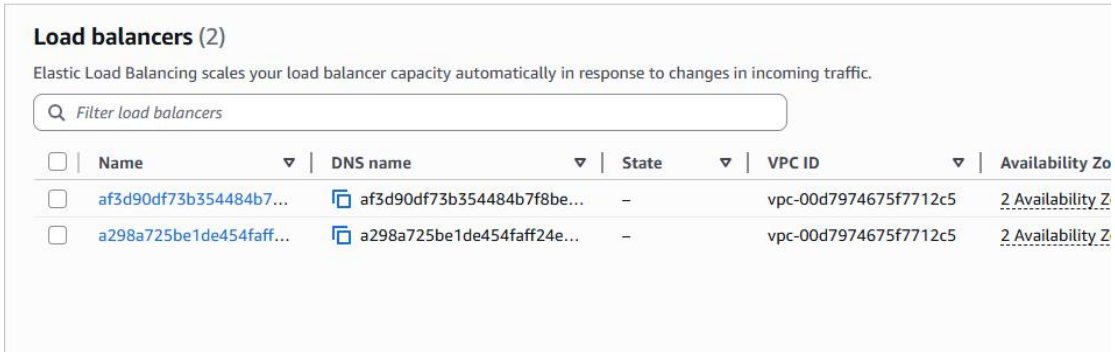
```
ubuntu@ip-172-31-9-165:~/ElasticSearch$
ubuntu@ip-172-31-9-165:~/ElasticSearch$ kubectl get all -n efklog
NAME                                READY   STATUS             RESTARTS   AGE
pod/elasticsearch-logging-0         0/1     Pending            0          4m26s
pod/fluentd-pqvhl                   0/1     ImagePullBackOff   0          4m13s
pod/fluentd-vhx4s                   0/1     ImagePullBackOff   0          4m13s
pod/kibana-78bdcb6988-xx2sq         1/1     Running            0          4m7s

NAME                            TYPE        CLUSTER-IP      EXTERNAL-IP   PORT(S)          AGE
service/elasticsearch-logging   ClusterIP   10.100.41.183   <none>        9200/TCP         4m32s
service/kibana                  NodePort    10.100.58.118   <none>        5601:30601/TCP   4m7s

NAME                        DESIRED   CURRENT   READY   UP-TO-DATE   AVAILABLE   NODE SELECTOR   AGE
daemonset.apps/fluentd      2         2         0       2            0           <none>          4m13s

NAME                        READY   UP-TO-DATE   AVAILABLE   AGE
deployment.apps/kibana      1/1     1            1           4m7s

NAME                                   DESIRED   CURRENT   READY   AGE
replicaset.apps/kibana-78bdcb6988      1         1         1       4m7s

NAME                                     READY   AGE
statefulset.apps/elasticsearch-logging   0/1     4m26s
```

http://af3d90df73b354484b7f8be9d26c267e-1835006855.ca-central-1.elb.amazonaws.com/



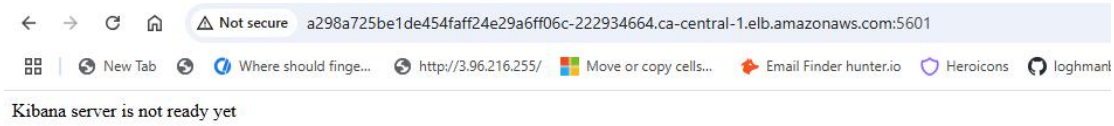
FluentD must be available in every Worker Node and if you want something to be available in all WorkerNodes then DaemonSet comes into picture

We see 2 loadbalancers, second one is for Kibana



```
service/kibana configured
ubuntu@ip-172-31-9-165:~/ElasticSearch$ kubectl get all -n efklog
NAME                          READY   STATUS             RESTARTS   AGE
pod/elasticsearch-logging-0   0/1     Pending            0          19m
pod/fluentd-pqvhl             0/1     ImagePullBackOff   0          19m
pod/fluentd-vhx4s             0/1     ImagePullBackOff   0          19m
pod/kibana-78bdcb6988-xx2sq   1/1     Running            0          19m

NAME                            TYPE           CLUSTER-IP      EXTERNAL-IP                                                                PORT(S)
E
service/elasticsearch-logging   ClusterIP      10.100.41.183   <none>                                                                     9200/TCP
m
service/kibana                  LoadBalancer   10.100.58.118   a298a725be1de454faff24e29a6ff06c-222934664.ca-central-1.elb.amazonaws.com   5601:30601/TCP
m

NAME                    DESIRED   CURRENT   READY   UP-TO-DATE   AVAILABLE   NODE SELECTOR   AGE
daemonset.apps/fluentd   2         2         0       2            0           <none>          19m

NAME                    READY   UP-TO-DATE   AVAILABLE   AGE
deployment.apps/kibana   1/1     1            1           19m

NAME                              DESIRED   CURRENT   READY   AGE
replicaset.apps/kibana-78bdcb6988   1         1         1       19m

NAME                                    READY   AGE
statefulset.apps/elasticsearch-logging   0/1     19m
ubuntu@ip-172-31-9-165:~/ElasticSearch$
```

http://a298a725be1de454faff24e29a6ff06c-222934664.ca-central-1.elb.amazonaws.com:5601/



Kibana server is not ready yet

```
NAME                                    READY   AGE
statefulset.apps/elasticsearch-logging   0/1     19m
ubuntu@ip-172-31-9-165:~/ElasticSearch$ kubectl get svc
NAME         TYPE           CLUSTER-IP      EXTERNAL-IP                                                                PORT(S)
javaappsvc   LoadBalancer   10.100.252.5    af3d90df73b354484b7f8be9d26c267e-1835006855.ca-central-1.elb.amazonaws.com   80:31177/TCP
kubernetes   ClusterIP      10.100.0.1      <none>                                                                     443/TCP
ubuntu@ip-172-31-9-165:~/ElasticSearch$ kubectl get pods -n efklog
NAME                          READY   STATUS             RESTARTS   AGE
elasticsearch-logging-0   0/1     Pending            0          28m
fluentd-pqvhl             0/1     ImagePullBackOff   0          27m
fluentd-vhx4s             0/1     ImagePullBackOff   0          27m
kibana-78bdcb6988-xx2sq   1/1     Running            0          27m
ubuntu@ip-172-31-9-165:~/ElasticSearch$
```

It is not able to connect to ElasticSearch

ubuntu@ip-172-31-9-165:~/ElasticSearch$ kubectl describe -n efklog pod/kibana-c84cb7d7-lcpm9

```
error: You must specify the type of resource to describe. Use "kubectl api-resources" for a complete list of supported resources.
ubuntu@ip-172-31-9-165:~/ElasticSearch$ kubectl describe -n efklog pod/kibana-c84cb7d7-lcpm9
Name:             kibana-c84cb7d7-lcpm9
Namespace:        efklog
Priority:         0
Service Account:  default
Node:             ip-192-168-5-129.ca-central-1.compute.internal/192.168.5.129
Start Time:       Sun, 15 Jun 2025 03:15:33 +0000
Labels:           app=kibana
                  pod-template-hash=c84cb7d7
Annotations:      <none>
Status:           Running
IP:               192.168.22.10
IPs:
  IP:           192.168.22.10
Controlled By:  ReplicaSet/kibana-c84cb7d7
Containers:
  kibana:
    Container ID:   containerd://dd2374fc0c3833ea861885875e0e9e276c55357623a56ab38eb0d30beb3a8d27
    Image:          docker.elastic.co/kibana/kibana:7.17.0
    Image ID:       docker.elastic.co/kibana/kibana@sha256:2673a3599185f4ebf363077580064daa817903ccf9fda3ccf6f4fc0abdf0a6eb
    Port:           5601/TCP
    Host Port:      0/TCP
    State:          Running
      Started:      Sun, 15 Jun 2025 03:22:23 +0000
    Last State:     Terminated
      Reason:       Error
      Exit Code:    137
```

```
ubuntu@ip-172-31-9-165:~/ElasticSearch$
ubuntu@ip-172-31-9-165:~/ElasticSearch$
ubuntu@ip-172-31-9-165:~/ElasticSearch$ kubectl delete all --all
pod "javawebbluedeploy-68fc6554d6-lb9tm" deleted
pod "javawebbluedeploy-68fc6554d6-zsqkt" deleted
service "javaappsvc" deleted
service "kubernetes" deleted
deployment.apps "javawebbluedeploy" deleted
ubuntu@ip-172-31-9-165:~/ElasticSearch$ kubectl delete all --all -n efklog
pod "elasticsearch-logging-0" deleted
pod "fluentd-pqvhl" deleted
pod "fluentd-vhx4s" deleted
pod "kibana-78bdcb6988-xx2sq" deleted
pod "kibana-c84cb7d7-lcpm9" deleted
service "elasticsearch-logging" deleted
service "kibana" deleted
daemonset.apps "fluentd" deleted
deployment.apps "kibana" deleted
statefulset.apps "elasticsearch-logging" deleted
ubuntu@ip-172-31-9-165:~/ElasticSearch$ kubectl apply -f 01-Namespace.yml
namespace/efklog unchanged
ubuntu@ip-172-31-9-165:~/ElasticSearch$ kubectl apply -f 02-ElasticSearch_Service.yml
service/elasticsearch-logging created
ubuntu@ip-172-31-9-165:~/ElasticSearch$ kubectl apply -f 03-ElasticSearch_StatefulSet.yml
serviceaccount/elasticsearch-logging unchanged
statefulset.apps/elasticsearch-logging created
ubuntu@ip-172-31-9-165:~/ElasticSearch$ kubectl apply -f 04-Fluentd_ConfigMap.yml
configmap/fluentd-config unchanged
ubuntu@ip-172-31-9-165:~/ElasticSearch$ kubectl apply -f 05-Fluentd_DaemonSet.yml
serviceaccount/fluentd unchanged
daemonset.apps/fluentd created
ubuntu@ip-172-31-9-165:~/ElasticSearch$ kubectl apply -f 06-kibana_deployment.yml
deployment.apps/kibana created
service/kibana created
ubuntu@ip-172-31-9-165:~/ElasticSearch$
```

```
service "kibana" deleted
daemonset.apps "fluentd" deleted
deployment.apps "kibana" deleted
statefulset.apps "elasticsearch-logging" deleted
ubuntu@ip-172-31-9-165:~/ElasticSearch$ kubectl apply -f 01-Namespace.yml
namespace/efklog unchanged
ubuntu@ip-172-31-9-165:~/ElasticSearch$ kubectl apply -f 02-ElasticSearch_Service.yml
service/elasticsearch-logging created
ubuntu@ip-172-31-9-165:~/ElasticSearch$ kubectl apply -f 03-ElasticSearch_StatefulSet.yml
serviceaccount/elasticsearch-logging unchanged
statefulset.apps/elasticsearch-logging created
ubuntu@ip-172-31-9-165:~/ElasticSearch$ kubectl apply -f 04-Fluentd_ConfigMap.yml
configmap/fluentd-config unchanged
ubuntu@ip-172-31-9-165:~/ElasticSearch$ kubectl apply -f 05-Fluentd_DaemonSet.yml
serviceaccount/fluentd unchanged
daemonset.apps/fluentd created
ubuntu@ip-172-31-9-165:~/ElasticSearch$ kubectl apply -f 06-kibana_deployment.yml
deployment.apps/kibana created
service/kibana created
ubuntu@ip-172-31-9-165:~/ElasticSearch$ vi 07-kibana-service.yml
ubuntu@ip-172-31-9-165:~/ElasticSearch$ kubectl apply -f 07-kibana-service.yml
service/kibana configured
ubuntu@ip-172-31-9-165:~/ElasticSearch$ kubectl apply -f deployment.yml
deployment.apps/javawebbluedeploy created
service/javaappsvc created
```

1:16
eksctl delete cluster --name my-eks-cluster --region ca-central-1

In a week we will have Kibana yml files