## Logging with EFK Stack (Elasticsearch, Fluent Bit, Kibana) on Amazon EKS

### 🔍 Why Logging?

**Debugging**: Identify application issues.

**Auditing**: Track user actions and access.

**Performance Monitoring**: Detect bottlenecks.

**Security**: Spot unauthorized/malicious activity.

## 🧰 Tools Used

**Elasticsearch** – log storage and search

**Fluent Bit** – log collection and forwarding

**Kibana** – data visualization

## 🏗️ Centralized Architecture

**Multiple clusters send logs to one EFK stack**

**Fluent Bit in each cluster pushes logs to central Elasticsearch**

**Kibana connected to that Elasticsearch instance**

## EFK Stack Architecture(with EBS)

+-----------------------------------------------------------+

| Amazon EKS Cluster |

| |

| +-----------------+ +----------------------+ |

| | Fluent Bit | ---> | Elasticsearch (ES) | |

| | (DaemonSet) | | StatefulSet + EBS | |

| +-----------------+ +----------------------+ |

| ↑ ↑ |

| +-----------------+ +----------------------+ |

| | Node Logs | | Kibana (Deployment) | |

| | /var/log/... | +----------------------+ |

| +-----------------+ | |

| ↓ |

| Kibana Dashboard (UI) |

+-----------------------------------------------------------+

### **1) Create IAM Role for Service Account**

eksctl create iamserviceaccount \

--name ebs-csi-controller-sa \

--namespace kube-system \

--cluster observability \

--role-name AmazonEKS\_EBS\_CSI\_DriverRole \

--role-only \

--attach-policy-arn arn:aws:iam::aws:policy/service-role/AmazonEBSCSIDriverPolicy \

--approve

* This command creates an IAM role for the EBS CSI controller.
* IAM role allows EBS CSI controller to interact with AWS resources, specifically for managing EBS volumes in the Kubernetes cluster.
* We will attach the Role with service account

### **2) Retrieve IAM Role ARN**

ARN=$(aws iam get-role --role-name AmazonEKS\_EBS\_CSI\_DriverRole --query 'Role.Arn' --output text)

* Command retrieves the ARN of the IAM role created for the EBS CSI controller service account.

### **3) Deploy EBS CSI Driver**

eksctl create addon --cluster observability --name aws-ebs-csi-driver --version latest \

--service-account-role-arn $ARN --force

* Above command deploys the AWS EBS CSI driver as an addon to your Kubernetes cluster.
* It uses the previously created IAM service account role to allow the driver to manage EBS volumes securely.

### **4) Create Namespace for Logging**

kubectl create namespace logging

### **5) Install Elasticsearch on K8s**

helm repo add elastic https://helm.elastic.co

helm install elasticsearch \

--set replicas=1 \

--set volumeClaimTemplate.storageClassName=gp2 \

--set persistence.labels.enabled=true elastic/elasticsearch -n logging

* Installs Elasticsearch in the logging namespace.
* It sets the number of replicas, specifies the storage class, and enables persistence labels to ensure data is stored on persistent volumes.

### **6) Retrieve Elasticsearch Username & Password**

# for username

kubectl get secrets --namespace=logging elasticsearch-master-credentials -ojsonpath='{.data.username}' | base64 -d# for password

kubectl get secrets --namespace=logging elasticsearch-master-credentials -ojsonpath='{.data.password}' | base64 -d

* Retrieves the password for the Elasticsearch cluster's master credentials from the Kubernetes secret.
* The password is base64 encoded, so it needs to be decoded before use.
* 👉 ****Note****: Please write down the password for future reference

### **7) Install Kibana**

helm install kibana --set service.type=LoadBalancer elastic/kibana -n logging

* Kibana provides a user-friendly interface for exploring and visualizing data stored in Elasticsearch.
* It is exposed as a LoadBalancer service, making it accessible from outside the cluster.

### **8) Install Fluentbit with Custom Values/Configurations**

* ****Note****: Please update the HTTP\_Passwd field in the fluentbit-values.yml file with the password retrieved earlier in step 6: (i.e NJyO47UqeYBsoaEU)"

helm repo add fluent https://fluent.github.io/helm-charts

helm install fluent-bit fluent/fluent-bit -f fluentbit-values.yaml -n logging

## **✅ Conclusion**

* We have successfully installed the EFK stack in our Kubernetes cluster, which includes Elasticsearch for storing logs, Fluentbit for collecting and forwarding logs, and Kibana for visualizing logs.
* To verify the setup, access the Kibana dashboard by entering the `LoadBalancer DNS name followed by :5601 in your browser.
  + http://LOAD\_BALANCER\_DNS\_NAME:5601
* Use the username and password retrieved in step 6 to log in.
* Once logged in, create a new data view in Kibana and explore the logs collected from your Kubernetes cluster.

## **Clean Up**

helm uninstall monitoring -n monitoring

helm uninstall fluent-bit -n logging

helm uninstall elasticsearch -n logging

helm uninstall kibana -n logging

kubectl delete -k kubernetes-manifest/

kubectl delete -k alerts-alertmanager-servicemonitor-manifest/

eksctl delete cluster --name observability