**LAB#6:**

**Kubernetes Audit Logs with AWS**

**CloudWatch**

**\*\*Tasks\*\*:**

**- Set up audit logging in EKS.**

**- Integrate with CloudWatch.**

**- Analyse and monitor logs.**

**- \*\*Documentation\*\*: Explain the**

**importance of monitoring and auditing in**

**Kubernetes security.**

Step1”

Create cluster and node

Add addon

https://www.stacksimplify.com/aws-eks/aws-eks-monitoring/learn-to-enable-monitoring-for-kubernetes-workloads-on-aws-eks/#step-05-generate-load-on-our-sample-nginx-application

apiVersion: v1

kind: Pod

metadata:

name: fluent-bit

namespace: default

spec:

containers:

- name: fluent-bit

image: fluent/fluent-bit:latest

volumeMounts:

- name: config-volume

mountPath: /fluent-bit/config

resources:

requests:

cpu: 100m

memory: 128Mi

volumes:

- name: config-volume

configMap:

name: fluent-bit-config

apiVersion: v1

kind: ConfigMap

metadata:

name: fluent-bit-config

namespace: default

data:

fluent-bit.conf: |

[SERVICE]

Flush 1

Daemon off

Log\_Level info

[INPUT]

Name in\_docker

Tag docker

Path /var/log/pods/\*.log

Buffer\_Size 256k

Mem\_Buf\_Limit 5m

[OUTPUT]

Name out\_cloudwatch

Tag cloudwatch

Match \*

Buffer\_Size 256k

Mem\_Buf\_Limit 5m

Record\_Format multiline

[FILTER]

Name kube\_parser

Match \*.log

Parser kubernetes

After you have created the Fluent Bit manifest file and the ConfigMap, you can deploy them to your worker nodes using the following commands:

kubectl apply -f fluent-bit-pod.yaml

kubectl apply -f fluent-bit-config.yaml