**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.**

**Prerequisites:**

**Install kubectl**

**Install eks**

**Install awscli**

**Add access key**

**Add roles for cluster and node permissions**

**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 |
| --- |

Documentation of the lab: Importance of Monitoring and Auditing in Kubernetes Security

* Real-time Threat Detection:
  + Visibility into System Behavior: Monitoring provides real-time insights into the behavior of pods, nodes, and the overall Kubernetes cluster, aiding in the early detection of suspicious activities or anomalies.
* Incident Response and Forensics:
  + Rapid Incident Response: Continuous monitoring allows for prompt responses to security incidents or breaches, enabling mitigation measures to be implemented swiftly.
  + Forensic Analysis: Auditing logs facilitates post-incident forensic analysis, helping identify the root cause and prevent similar security incidents in the future.
* Compliance and Governance:
  + Regulatory Compliance: Auditing helps in meeting regulatory compliance requirements by maintaining detailed logs and records of activities within the Kubernetes environment.
  + Policy Enforcement: Monitoring and auditing ensure adherence to security policies and best practices, enabling enforcement and validation of security configurations.
* Continuous Improvement and Optimization:
  + Performance Optimization: Analyzing monitoring data helps in identifying performance bottlenecks and optimizing resource utilization within the Kubernetes cluster.
  + Security Enhancements: Insights gained from audits and monitoring drive improvements in security postures, enabling the implementation of better security controls and practices.

**Conclusion of the lab:**

**Monitoring and auditing are integral components of maintaining a secure Kubernetes environment, ensuring proactive threat detection, compliance adherence, and continuous improvement in security measures.**

* **Proactive Threat Detection and Response: Monitoring provides real-time visibility, enabling proactive threat detection and swift responses to security incidents, reducing the impact of potential breaches.**
* **Compliance and Governance Adherence: Auditing logs and activities ensures compliance with regulations and governance requirements, fostering a secure and accountable environment for Kubernetes deployments.**
* **Continuous Improvement: Insights gained from monitoring and audits drive continuous improvement, allowing for optimization of performance, identification of vulnerabilities, and the implementation of enhanced security controls.**

**The integration of robust monitoring and auditing practices is essential for bolstering the security posture of Kubernetes deployments. Continuous vigilance, regular audits, and leveraging insights obtained from monitoring data are crucial in maintaining a resilient and secure Kubernetes environment.**