Introduction

This document shows how typically log collection is carried out on Amazon Elastic Kubernetes System (EKS) and how it may be configured to send logs to Logpoint SIEM. This document is provided “as is”. It is highly recommended to practice before trying these instructions in production!

Enabling EKS Cluster for Audit Logs

Log types in Kubernetes environments:

- **Component Logs**: Logs of each Kubernetes component like kube-scheduler.
- **Audit Logs**: Logs of the sequence of actions that happened in the cluster.
- **Event Logs**: Logs of Kubernetes events that occurred in the cluster.
- **Application Logs**: Logs of any individual apps deployed to the cluster.
- **Authenticator Logs**: Logs of communications to EKS through IAM credentials.
- **Worker Logs**: Logs of the worker node, SSH logins, journal, etc.
- **Network Logs**: Logs of network traffic, ingress/egress, in/out of cluster.

EKS supports the following logs in a managed “as a service” manner:

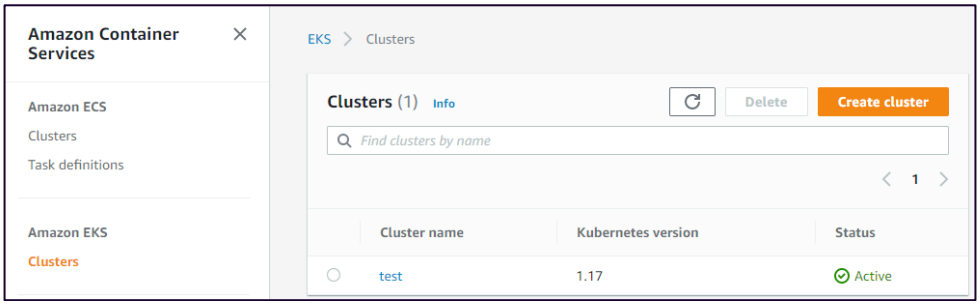
- **Component Logs**: kube-apiserver, kube-scheduler and kube-controller-manager.
- **Audit Logs**: Users, Groups and principals that have affected the cluster.
- **Authenticator Logs**: Accesses that occurred to the cluster using IAM credentials.

EKS Cluster Setup (New)

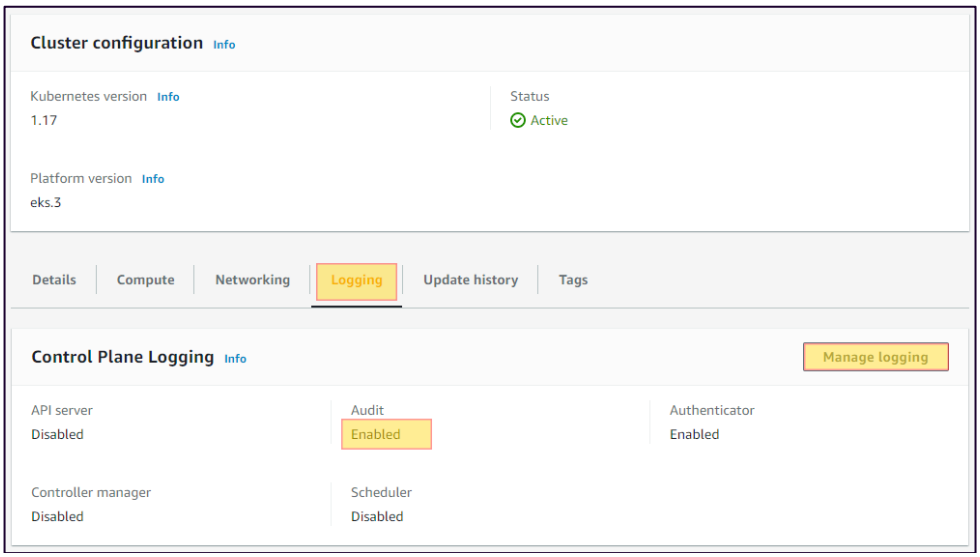
If you do not have an Amazon EKS cluster, create one by following the Creating an Amazon EKS Cluster documentation. During setup, on the Configure logging page, enable **Audit logs** then follow the instructions for an existing cluster.

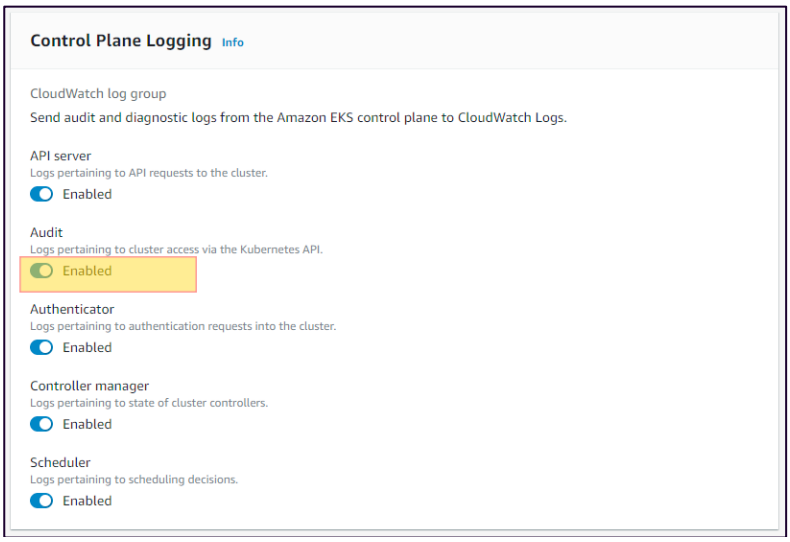
EKS Cluster Setup (Existing)

1. Navigate to the cluster in the Amazon EKS console.
2. Click on the **Cluster Name** of the EKS cluster.



3. Click the **Logging** tab.
4. Click the **Manage logging** button.
5. Toggle the **Audit** option to **Enabled** and click the **Save changes** button.





After **Cluster Audit Logs** has been enabled, each EKS cluster has a separate log group in CloudWatch Logs, and all cluster logs will be sent as log streams to the log group. For each Kubernetes component, there is a separate log stream. Log groups don't have retention by default and must be added by the user after configuring logging for EKS clusters.