

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 <u>Creating an Amazon EKS Cluster</u> documentation. During setup, on the Configure logging page, enable **Audit logs** then follow the instructions for an existing cluster.

I! LOGPOINT

EKS Cluster Setup (Existing)

- 1. Navigate to the cluster in the <u>Amazon EKS console</u>.
- 2. Click on the **Cluster Name** of the EKS cluster.

Amazon Container X Services	EKS > Clusters		
Amazon ECS Clusters Task definitions	Clusters (1) Info	C Delete	Create cluster
Amazon EKS	Cluster name	Kubernetes version	Status
Clusters	⊖ test	1.17	⊘ Active

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

Cluster configuration Info					
Kubernetes version Info 1.17	Status Ø Active				
Platform version Info eks.3					
Details Compute Networking Logging Update history Tags					
Control Plane Logging Info			Manage logging		
API server Disabled	Audit Enabled	Authenticator Enabled			
Controller manager Disabled	Scheduler Disabled				

CloudWatch log gro	ıp		
Send audit and diag	nostic logs from the Amazon EKS cont	rol plane to CloudWatch Logs.	
API server			
Logs pertaining to API	equests to the cluster.		
Enabled			
Audit			
Logs pertaining to clus	er access via the Kubernetes API.		
C Enabled			
Authenticator			
Logs pertaining to auti	entication requests into the cluster.		
Enabled			
Controller manager			
Logs pertaining to stat	of cluster controllers.		
Enabled			
Scheduler			
Loop portaining to only	tuling decisions.		

I. LOGPOINT

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.

CloudWatch > Log groups					
Log By de	groups (1) Auit, we only load up to 10000 log groups.	Actions View in Logs Insights Start tailing Create log group			
Q	Filter log groups or try prefix search	□ Exact match < 1 > (◎			
0	Log group 🗢 Data protection	∇ Sensitive data count ▼ Retention ▼ Metric filters ▼ Contributor Insights ▼ Sul			
0	/aws/eks/kubedemy/cluster -	- Never expire			
Log s	treams Tags Metric filters Subscription filters Contributor Insights	Data protection			
Log	streams (12)	C Delete Create log stream Search all log streams			
Q	Filter log streams or try prefix search	Exact match Show expired () Info (1 > ())			
	Log stream	▲ Last event time マ			
0	authenticator-24b69d1dfd60a0c0bf45cbbc513bab38	2023-08-13 13:50:01 (UTC+01:00)			
0	authenticator-43d2e98e888b8b1b9629142f4a504403	2023-08-13 13:50:05 (UTC+01:00)			
	cloud-controller-manager-24b69d1dfd60a0c0bf45cbbc513bab38	2023-08-13 13:46:47 (UTC+01:00)			
0	cloud-controller-manager-43d2e98e888b8b1b9629142f4a504403	2023-08-13 13:39:54 (UTC+01:00)			
	kube-apiserver-24b69d1dfd60a0c0bf45cbbc513bab38	2023-08-13 13:50:01 (UTC+01:00)			
	kube-apiserver-43d2e98e888b8b1b9629142f4a504403	2023-08-13 13:50:05 (UTC+01:00)			
	kube-apiserver-audit-24b69d1dfd60a0c0bf45cbbc513bab38	2023-08-13 13:50:00 (UTC+01:00)			
	kube-apiserver-audit-43d2e98e888b8b1b9629142f4a504403	2023-08-13 13:50:01 (UTC+01:00)			
	kube-controller-manager-24b69d1dfd60a0c0bf45cbbc513bab38	2023-08-13 13:39:51 (UTC+01:00)			
0	kube-controller-manager-43d2e98e888b8b1b9629142f4a504403	2023-08-13 13:39:58 (UTC+01:00)			
	kube-scheduler-24b69d1dfd60a0c0bf45cbbc513bab38	2023-08-13 13:47:21 (UTC+01:00)			
0	kube-scheduler-43d2e98e888b8b1b9629142f4a504403	2023-08-13 13:39:53 (UTC+01:00)			