**Logging and monitoring with AWS EKS**

The diagram shows the following workflow when application logs from Amazon EKS clusters are streamed to Amazon OpenSearch Service:

1. The Fluent Bit service in the Amazon EKS cluster pushes the logs to CloudWatch.
2. The AWS Lambda function streams the logs to Amazon OpenSearch Service using a subscription filter.
3. You can then use Kibana to visualize the logs in the configured indexes.
4. You can also stream logs by using Amazon Kinesis Data Firehose and store them in an S3 bucket for analysis and querying with [Amazon Athena](https://docs.aws.amazon.com/athena/latest/ug/what-is.html).

Diagram

Description automatically generated

Note: diagram shows a logging architecture that automatically streams logs from multiple accounts to a centralized logs server

## Logging and monitoring for Amazon Elastic Kubernetes Service (Amazon EKS) has two categories: the control plane logs and the application logs.

* EKS control plane logging provides audit and diagnostic logs from the control plane to Amazon CloudWatch Logs groups in your AWS account.
* collect application logs you must install a log aggregator, such as [Fluent Bit](https://fluentbit.io/), [Fluentd](https://www.fluentd.org/), or [CloudWatch Container Insights](https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/ContainerInsights.html), in your Amazon EKS cluster.

## You can monitor the Amazon EKS clusters in real time by streaming metrics to [New Relic](https://newrelic.com/) or [Datadog](https://www.datadoghq.com/) for better observability

* New Relic and Datadog provide holistic views of the performance and health of Kubernetes clusters, down to the node, container, and application-level visibility required to identify and troubleshoot performance issues
* - recommend using Fluent Bit as a log collector and using New Relic or Datadog for better observability

##Following list provides three options for logging and monitoring your Amazon EKS clusters:

* **Option 1** – Use Fluent Bit as the log collector and forwarder to send application and cluster logs to CloudWatch. You can then stream the logs to Amazon OpenSearch Service (successor to Amazon Elasticsearch Service) using a subscription filter in CloudWatch. This option is shown in this section's architecture diagram.
* **Option 2** – Use a Datadog agent as the log and metric collector and forwarder to stream logs and metrics to the Datadog UI.
* **Option 3** – Use a New Relic agent as the log and metric collector and forwarder to stream logs and metrics to the New Relic UI.