Logging

CloudWatch Logs Terminology

It’s helpful to remember CloudWatch Logs terminology when working with your logs in AWS.

The terminology and concepts that are central to your understanding and use of CloudWatch Logs are described below.

Log events

A log event is a record of some activity recorded by the application or resource being monitored. The log event record that CloudWatch Logs understands contains two properties: the timestamp of when the event occurred, and the raw event message. Event messages must be UTF-8 encoded.

Log streams

A log stream is a sequence of log events that share the same source. More specifically, a log stream is generally intended to represent the sequence of events coming from the application instance or resource being monitored.

Log groups

Log groups define groups of log streams that share the same retention, monitoring, and access control settings. Each log stream has to belong to one log group.

Metric filters

You can use metric filters to extract metric observations from ingested events and transform them to data points in a CloudWatch metric. Metric filters are assigned to log groups, and all of the filters assigned to a log group are applied to their log streams.

Retention settings

Retention settings can be used to specify how long log events are kept in CloudWatch Logs. Expired log events get deleted automatically. Just like metric filters, retention settings are also assigned to log groups, and the retention assigned to a log group is applied to their log streams.

AWS Lambda and CloudWatch Logs

Configuring Lambda to send logs to CloudWatch Logs isn’t a difficult task. In fact, the only step is to make sure that Lambda is allowed to create a Log Group, create a Log Stream and put Log Events. This can easily be done by using the IAM managed policy “AWSLambdaBasicExecutionRole”. Then, it’s only a matter of using the print method or any logging library that writes to stdout or stderr in your code. You can find more information on how to use it here:

https://docs.aws.amazon.com/lambda/latest/dg/python-logging.html

Amazon API Gateway and CloudWatch Logs

Configuring API Gateway to send logs to CloudWatch isn’t difficult either. You configure this at the stage level.

There are two types of API logging in CloudWatch: execution logging and access logging. In execution logging, API Gateway manages the CloudWatch Logs. The process includes creating log groups and log streams, and reporting to the log streams any caller's requests and responses.

The logged data includes errors or execution traces (such as request or response parameter values or payloads), data used by Lambda authorizers (formerly known as custom authorizers), whether API keys are required, whether usage plans are enabled, and so on.

Read more about logging and API Gateway here:

https://docs.aws.amazon.com/apigateway/latest/developerguide/set-up-logging.html