# What is CloudWatch?

You can use Amazon CloudWatch to collect and track metrics, collect and monitor log files, set alarms, and automatically react to changes in your AWS resources. Since CloudWatch is integrated with the majority of AWS services, you can use CloudWatch to get a global view of your infrastructure and applications.

While CloudWatch is a monitoring service, it is billed as “near real-time”. If you are using it for debugging, there may be a lag from the event time until it shows up in the tool. Additional tools, like server logs, may be needed to bridge the gaps.

<https://aws.amazon.com/cloudwatch/>

(Lambda) - <http://docs.aws.amazon.com/lambda/latest/dg/monitoring-functions-logs.html>

<http://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/SettingLogRetention.html>

## Alarms

You can create a CloudWatch alarm that watches a single metric. The alarm performs one or more actions based on the value of the metric relative to a threshold over a number of time periods. Alarms invoke actions for sustained state changes only. CloudWatch alarms do not invoke actions simply because they are in a particular state, the state must have changed and been maintained for a specified number of periods.

<http://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/AlarmThatSendsEmail.html>

# What is CloudTrail?

CloudTrail is a web service that records activity made on your account and delivers log files to your Amazon S3 bucket. It tracks all the details of each change made within an account, including the user who made the request, the services used, the actions performed, and parameters for the action, and the response elements returned.

CloudTrail is designed for those who need to track changes to resources, answer simple questions about user activity, demonstrate compliance, troubleshoot, or perform security analysis.

<https://aws.amazon.com/cloudtrail>

# What is Sumo Logic?

Sumo Logic is only TR-approved 3rd party for log management, aggregation and analysis services. Sumo Logic focuses on logs as opposed to alarms.

https://www.sumologic.com/

# What is Datadog?

Datadog is only TR-approved 3rd party monitoring service for cloud-scale applications, bringing together data from servers, databases, tools, and services to present a unified view of an entire stack. Datadog focuses on alarms as opposed to logs.

<https://www.datadoghq.com/>

Labs Overview - <https://thomsonreuters.webex.com/thomsonreuters/lsr.php?RCID=77410c9a65bf4166b6e352166a77d4c1>

TRTA Overview - <https://thehub.thomsonreuters.com/groups/trta-enterprise-architecture-council/projects/monitoring-and-alerting/blog/2017/07/13/datadog-overview-recording>

TR Overview - Monitoring Containers - <https://tlr.webex.com/tlr/lsr.php?RCID=6a8db1ffbcae4f73a46e0591046938a9>