Amazon Cloudwatch

❖ AMAZON CLOUDWATCH:

- Monitoring is an important part of maintaining the reliability, availability, and performance of AWS Audit Manager and your other AWS solutions.
- It is a monitoring service for AWS cloud services, resources and applications you run on AWS.
- CloudWatch is a monitoring and observability service built for DevOps engineers, developers, site reliability engineers (SREs), IT managers, and product owners.
- CloudWatch to detect anomalous behaviour in your environments, set alarms, visualize logs and metrics side by side, take automated actions, troubleshoot issues, and discover insights to keep your applications running smoothly.
- It provides centralized logging and performance metrics for AWS resources.
- It is used to collect and track metrics, collect and monitor log files, set alarms, and automatically react to changes in your AWS resources.
- Cloud watch Alarms can be used as "Triggers".
- Metric is a variable to monitor (CPU utilization, Networkin….).

BENEFITS:

- Use a single platform for observability
- Collect metrics on AWS and on premises
- Improve operational performance and resource optimization
- Get operational visibility and insight
- Derive actionable insights from logs

➢ MONITORING LEVELS:

BASIC:

- Data is available automatically in **5-minute periods** at no charge.
- By default, your instance enabled with basic monitoring.

DETAILED:

- Data is available in **1-minute periods** for an additional cost.
- AWS free tier allows us to have 10 detailed monitoring metrics.

➢ STATUS CHECKS:

SYSTEM STATUS CHECKS: (Things that outside of our control)

- Loss of system power and network Connectivity.
- Software issues on the physical host.
- Hardware issues on the physical host

How to solve: Generally stopping and restarting the instance will fix the issues. This causing the instance to launch on a different physical hardware device.

INSTANCE STATUS CHECKS: (Software issues that we do control)

- Mis configured networking or start-up configuration.
- Exhausted memory.
- Corrupted file system.
- Incompatible kernel.

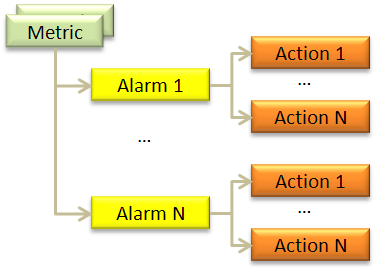
How to solve: Generally, a reboot or resolving the file system configuration issue.

➢ DASHBOARDS:

- Great way to setup dashboard for quick access to keys metrics.
- Dashboards are Global, which includes graphs from different regions.
- **Pricing:** 3 dashboards (up to 50 metrics) for free.

➢ ALARMAS:

- The new CloudWatch Alarms feature allows you to watch CloudWatch metrics and to receive notifications when the metrics fall outside of the levels (high or low thresholds) that you configure.
- We can attach multiple Alarms to each metric and each one can have multiple actions.
- Alarms are used to **trigger notifications** of any metric.
- **Alarms states are:** OK, INSUFFICIENT_DATA, ALARM.



➢ LOGS:

- CloudWatch Logs enables you to centralize the logs from all of your systems, applications, and AWS services that you use, in a single, highly scalable service.
- To collect logs from EC2 instances and on-premises servers into CloudWatch Logs.
- To send logs to CloudWatch, make sure IAM permissions are correct.
- Logs can use filter expressions.
- Log's insights can be used to query logs and add queries to CloudWatch Dashboards.

➢ EVENTS:

- CloudWatch Events delivers a near real-time stream of system events that describe changes in AWS resources.
- Events becomes aware of operational changes as they occur.
- Event creates a small JSON document to give information about the change.
- CloudWatch Events supports **cron expressions** and **rate expressions**.

CRON EXPRESSIONS:

- Cron expressions have six required fields, which are separated by white space.
- **Syntax: cron(fields)**

Field	Values	Wildcards
Minutes	0-59	, - * /
Hours	0-23	, - * /
Day-of-month	1-31	, - * ? / L W
Month	1-12 or JAN-DEC	, - * /
Day-of-week	1-7 or SUN-SAT	, - * ? L #
Year	1970-2199	, - * /

RATE EXPRESSIONS:

- A rate expression starts when you create the scheduled event rule, and then runs on its defined schedule.
- Rate expressions have two required fields. Fields are separated by white space.

SYNTAX: rate (value unit)

VALUE:

- A positive number.

UNIT:

- The unit of time. Different units are required for values of 1, such as minute, and values over 1, such as minutes.
- Valid values: minute | minutes | hour | hours | day | days

➢ SERVICE LENS:

- ServiceLens enables you to visualize and analyze the health, performance, and availability of your applications in a single place.
- It ties together CloudWatch metrics and logs, as well as traces from AWS X-Ray.
- It enables you to gain visibility into your applications in two main areas:
  - Infrastructure monitoring
  - Transaction monitoring

➢ SYNTHETICS:

- CloudWatch Synthetics allows you to monitor application endpoints more easily.
- CloudWatch now collects canary traffic, which can continually verify your customer experience.
- It supports monitoring of your REST APIs, URLs, and website content, checking for unauthorized changes from phishing, code injection and cross-site scripting.
- It runs tests on your endpoints every minute, 24x7, and alerts you when your application endpoints don’t behave as expected.

➢ CLOUDWATCH VS CLOUDTRAIL

CLOUDWATCH:

- It is a monitoring tool used for real-time monitoring of AWS resources and applications. It provides a report on the basis of monitoring which can be used to analyze the performance of the system. It monitors various AWS resources like Amazon EC2, Amazon RDS, Amazon S3, Elastic Load Balancer, etc.

CLOUDTRAIL:

- It is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. It continuously logs and monitors the activities and actions across your AWS account. It also provides the event history of your AWS account including information about who is accessing your AWS services.

CloudWatch	CloudTrail
Performance monitoring (operations)	Auditing (security)
Log events across AWS services – think operations	Log API activity across AWS services – think activities
Higher-level comprehensive monitoring and eventing	More low-level granular
Log from multiple accounts	Log from multiple accounts
Logs stored indefinitely	Logs stored to S3 or CloudWatch indefinitely
Alarms history for 14 days	No native alarming; can use CloudWatch alarms

NOTE:

- CloudWatch **monitors performance**, whereas CloudTrail **monitors actions** in your AWS environment.