

SESSION 13

Activate Windows
Go to Settings to activate Windows.

AWS MONITORING

Activate Windows
Go to Settings to activate Windows.

AWS Monitoring

Amazon Web Services (AWS) monitoring is a set of practices you can use to verify the security and performance of your AWS resources and data. These practices rely on various tools and services to collect, analyze, and present data insights. You can then use these insights to identify vulnerabilities and issues, predict performance, and optimize configurations.

Activate Windows
Go to Settings to activate Windows.

Amazon CloudWatch Metrics

- Metrics are data about the performance of your systems.
- CloudWatch provides metrics for every services in AWS
- Metrics have timestamps
- example:
- CloudWatch billing metrics(only in us-east-1), every month end it will set back to 0
- EC2 instances: CPU utilization, Status Checks, Network
- EBS Volume: Disk Read/Writes
- S3 buckets: BucketSizeBytes, NumberOfObjects, AllRequests
- Custom metrics

Amazon CloudWatch Alarm

- Alarms are used to trigger notification for any metric
- AWS CloudWatch Alarms, as the name suggests, allows you to create alarms to monitor different AWS Resources and AWS Services with certain conditions. These alarms can be configured to alert you or your team when the specified conditions are met. AWS CloudWatch Alarms can be used for simple use cases like monitoring the CPU Usage of an AWS EC2 Instance to more complex ones like anomaly detection using past metric data.
- Alarm actions:
 - AutoScaling: increase or decrease EC2 instances desired count
 - EC2 Actions: stop, terminate, reboot or recover EC2 instance
 - SNS notification: send a notification into an SNS topic
- metric alarm can have the following possible states:
 - OK: The metric is within the defined threshold
 - ALARM: The metric is outside of the defined threshold
 - INSUFFICIENT_DATA: The metric is not available or not enough data is available for the metric to determine the alarm state

Activate Windows
Go to Settings to activate Windows.

Amazon CloudWatch Logs

- Enables realtime monitoring of 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. You can then easily view them, search them for specific error codes or patterns, filter them based on specific fields, or archive them securely for future analysis. CloudWatch Logs enables you to see all of your logs, regardless of their source, as a single and consistent flow of events ordered by time.
- They can collect logs from: Elastic Beanstalk, ECS, AWS Lambda, CloudTrail, AWS Lambda
- Query your log data :you can use CloudWatch Logs Insights to interactively search and analyze your log data. You can perform queries to help you more efficiently and effectively respond to operational issues.
- Monitor logs from Amazon EC2 instances – You can use CloudWatch Logs to monitor applications and systems using log data.(need to run CloudWatchlogs agent, IAM permissions Go to Settings to activate Windows.)
- Log retention – By default, logs are kept indefinitely and never expire

Amazon EventBridge(CloudWatch Events)

- Amazon EventBridge is a serverless, fully managed, and scalable event bus that enables integrations between AWS services, Software as a services (SaaS), and your applications.
- EventBridge makes it easier to connect applications. You can ingest, filter, transform and deliver events without writing custom code.
- Schedule: sheduled scripts(Schedule every hour)
- Event pattern: Event rules
- <https://intellipaat.com/blog/aws-amazon-eventbridge/>

Activate Windows
Go to Settings to activate Windows.

AWS CloudTrail

- AWS CloudTrail is a service offered by AWS that enables operational and risk auditing as well as governance and compliance for your AWS account.
- Events in CloudTrail are the actions that a user, role, or an AWS service has performed.
- The AWS Management Console, AWS Command Line Interface, and AWS SDKs and APIs are just a few examples of the events that can occur.
- Can put logs from CloudTrail into CloudWatch logs or S3

AWS X-Ray

- Debugging in Production
- Visual analysis of your application, what is happening for each service.
- Troubleshooting performance
- Understand dependencies in microservice architecture
- service issue
- Users that are impacted

Amazon CodeGuru

- An ML - powered service for automated code reviews and application performance recommendation
- CodeGuru Reviewer: automated code reviews for static code analysis
Built in reviews with actionable recommendations(development)
- CodeGuru Profiler: visibility/recommendations about application performance during runtime. (production)
Detect and optimize the expensive lines of code (in- prod and post-production_
- It identifies critical issues, security vulnerabilities and hard to find bugs
- common coding best practices, resource leaks, security detection, input validation
- Supports java and python

AWS Health Dashboard

- The AWS Health Dashboard is the single place to learn about the availability and operations of AWS services.
- Shows all regions, all services health
- Shows historical information for each day
- Previously called AWS Service Health Dashboard

AWS Health Dashboard- Your Account

- Provides alerts and remediation guidance when AWS experiencing events that may impact you
- Gives you relevant and timely information to help you manage in progress and to provide proactive notification to help you plan for scheduled activities

CloudWatch

- **Metrics:** monitor the performance of AWS services and billing metrics
- **Alarms:** automate notification, perform EC2 action, notify SNS based on metric
- **Logs:** collect log files from EC2 instances, lambda functions etc
- **Events(EventBridge):** react to events, or trigger a rule on a schedule

CloudTrail: audit API calls made within your AWS account

CloudTrail Insights: automate analysis of your CloudTrail Events

X-Ray: trace requests made through distributed applications

AWS Health Dashboard: status of all AWS services across all regions

AWS Account Health Dashboard: AWS events that impact your infrastructure

Amazon CodeGuru: automated code reviews and application performance recommendation

Go to Settings to activate Windows.

Questions

1. Which CloudWatch feature would you use to trigger notifications when a metric reached a threshold you specify
2. Which AWS service would help developers analyze and debug production as well as distributed application
3. Which AWS Service provides alerts and remediation guidance when AWS is experiencing events that may impact you?
4. You need to set up metrics monitoring for every service in AWS. Which service would you use?
5. Which service allows you to inspect, audit, and record events and API calls made within your AWS account
6. Which AWS service automatically analyze code and provides performance recommendations?
7. If a service is deleted in AWS, which service should you use to investigate first?

Activate Windows

Go to Settings to activate Windows.

1. CloudWatch Alarms
2. X-Ray
3. AWS Health Dashboard
4. CloudWatch
5. CloudTrail
6. CodeGuru
7. CloudTrail