1.What is CloudWatch?

A) AWS CloudWatch is a monitoring tool for tracking AWS application health and resource use. It's commonly used to help:

* Monitor and fix operational issues
* Measure and optimize performance through logging
* Monitor AWS applications on-premises or in the cloud
* Troubleshoot AWS infrastructure, and more

2.What are the types of monitoring in CloudWatch? How is pricing different for Detailed Monitoring?

A) Cross-account observability across multiple AWS accounts. ...

* Unified operational view with dashboards. ...
* Composite alarms. ...
* High-resolution alarms. ...
* Logs and metrics correlation. ...
* Application Insights

**Metrics:**

* Basic Monitoring Metrics (at 5-minute frequency)
* 10 Detailed Monitoring Metrics (at 1-minute frequency)
* 1 Million API requests (not applicable to GetMetricData and GetMetricWidgetImage).

**Dashboard:** 3 Dashboards for up to 50 metrics per month

**Alarms:** 10 Alarm metrics (only applicable to Standard resolution alarms that list metrics directly and don’t use a Metrics Insights query)

**Logs:** 5 GB Data (ingestion, archive storage, and data scanned by Logs Insights queries)

**RUM:** First time free trial includes 1 million RUM events per account.

3. What are the CloudWatch metrics that are available for EC2 instance, EBS Volumes, Load Balancers?

A) [Instance metrics](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/viewing_metrics_with_cloudwatch.html#ec2-cloudwatch-metrics)

[CPU credit metrics](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/viewing_metrics_with_cloudwatch.html#cpu-credit-metrics)

[Dedicated Host metrics](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/viewing_metrics_with_cloudwatch.html#dh-metrics)

[Amazon EBS metrics for Nitro-based instances](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/viewing_metrics_with_cloudwatch.html#ebs-metrics-nitro)

[Status check metrics](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/viewing_metrics_with_cloudwatch.html#status-check-metrics)

[Traffic mirroring metrics](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/viewing_metrics_with_cloudwatch.html#traffic-mirroring-metrics)

[Auto Scaling group metrics](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/viewing_metrics_with_cloudwatch.html#autoscaling-metrics)

EBS volume: Pulls CloudWatch metrics for a specific AWS Resource ID (an EBS volume ID or an EC2 instance) Calculates throughput, IOPS, and IO size over a specified period of time

Load Blancers: CloudWatch provides statistics based on the metric data points published by Elastic Load Balancing. Statistics are metric data aggregations over specified period of time. When you request statistics, the returned data stream is identified by the metric name and dimension.

4. What are the Custom metrics in CloudWatch?

A) A custom metric enables you to monitor a specific application binary or runtime. CloudWatch helps you monitor the infrastructure portion of an EC2 instance, such as CPU, hard disk and network.

5. What are CloudWatch Log groups and Log Insights.

A)  A log group is a group of log streams that share the same retention, monitoring, and access control settings. You can define log groups and specify which streams to put into each group.

CloudWatch Logs Insights enables you to interactively search and analyze your log data in Amazon CloudWatch Logs. You can perform queries to help you more efficiently and effectively respond to operational issues.

6. What is SNS. Create an SNS topic with your email as subscriber.

A) Amazon Simple Notification Service (Amazon SNS) is a managed service that provides message delivery from publishers to subscribers (also known as producers and consumers).

SNS topic and receive published messages using a supported endpoint type, such as Amazon Kinesis Data Firehose, Amazon SQS, AWS Lambda, HTTP, email, mobile push notifications, and mobile text messages (SMS).

1. Sign in to the [Amazon SNS console](https://console.aws.amazon.com/sns/home).
2. In the left navigation pane, choose **Subscriptions**.
3. On the **Subscriptions** page, choose **Create subscription**.
4. On the **Create subscription** page, in the **Details** section, do the following:
   1. For **Topic ARN**, choose the Amazon Resource Name (ARN) of a topic.
   2. For **Protocol**, choose **Email**.
   3. For **Endpoint**, enter the email address.
   4. (Optional) To configure a filter policy, expand the **Subscription filter policy** section. For more information, see [Amazon SNS subscription filter policies](https://docs.aws.amazon.com/sns/latest/dg/sns-subscription-filter-policies.html).
   5. (Optional) To enable payload-based filtering, configure Filter Policy Scope to MessageBody. For more information, see [Amazon SNS subscription filter policy scope](https://docs.aws.amazon.com/sns/latest/dg/sns-message-filtering-scope.html).
   6. (Optional) To configure a dead-letter queue for the subscription, expand the **Redrive policy (dead-letter queue)** section. For more information, see [Amazon SNS dead-letter queues (DLQs)](https://docs.aws.amazon.com/sns/latest/dg/sns-dead-letter-queues.html).
   7. Choose **Create subscription**.

7.Create an EC2 alarm for CPU utilization. Install stress (ref 1) utility, increase CPU and make sure you get an alarm on your email.

A) CloudWatch falls under “Management & Governance” service in AWS (Amazon Web Services). CloudWatch is a monitoring and management service which can be used to monitor services on AWS and manage them when a particular condition meets. CloudWatch can be used to collect performance and operational data (CPU, RAM, Network IN, Network Out, etc) of the services available on AWS.

In terms of billing, CloudWatch comes with 2 different options, Free Tier and Paid Tie

8. Create an Autoscaling Group, and scale-in-EC2 instance based on CPU utilization. Increase CPU utilization on EC2 instance using stress utility.

A)  Use predictive scaling directly through AWS Command Line Interface (CLI), EC2 Auto Scaling Management Console, and AWS SDKs similar to how you use other scaling policies, such as Simple Scaling or Target Tracking etc. You don't have to create an AWS Auto Scaling plan just for using predictive scaling.

9. What is AWS Config. What are AWS Config Rules.

A) AWS Config provides a detailed view of the configuration of AWS resources in your AWS account. This includes how the resources are related to one another and how they were configured in the past so that you can see how the configurations and relationships change over time.

AWS Config rules evaluate the configuration settings of your AWS resources. A rule can run when AWS Config detects a configuration change to an AWS resource or at a periodic frequency that you choose (for example, every 24 hours). There are two types of rules: AWS Config Managed Rules and AWS Config Custom Rules.

10.Enable AWS Config to monitor change in security Group. Identity the sequence of events when a security group is modified.

A) Open the CloudTrail console.

Choose Event history.

In Filter, select the dropdown list. ...

In the Enter resource name text box, enter your resource's name (for example, sg-123456789).

For Time range, enter the desired time range.

To change an AWS EC2 instance's security group, open the Amazon EC2 Console and Select “Instances.” Click “Change Security Groups” under “Actions” and select the security group to assign an instance. You can remove pre-existing security groups by choosing “Remove” then save.

11. What is AWS Cloud Trial. Identity the sequence of event when an EC2 instance is created in Cloud Trial.

A) AWS CloudTrail is a service provided by AWS that aids in the governance, compliance, and operational and risk auditing of 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.

12. What are AWS Flow Logs. Enable VPC Flow Logs for a ENI and capture and analyse a VPC Flow log.

A) Virtual Private Cloud (VPC) Flow logging provides built-in power to monitor information about how your network resources are operating in Amazon Web Services.

[VPC](https://www.sumologic.com/glossary/virtual-private-cloud/) Flow logging lets you capture and log data about network traffic in your VPC. VPC Flow logging records information about the IP data going to and from designated network interfaces, storing this raw data in [Amazon CloudWatch](https://www.amazonaws.cn/en/cloudwatch/), where it can be retrieved and viewed.