Caltech | Center for Technology & Management Education

Post Graduate Program in Cloud

simplilearn

Cloud

Caltech | Center for Technology & Management Education

AWS Certified SysOps Administrator

simplilearn

Monitoring, Reporting and Cost optimization

Learning Objectives

By the end of this lesson, you will be able to:

- Discuss features of CloudWatch
- Monitor the deployed application using EC2, EBS, ELB, and ElastiCache
- Describe cost explorer, cost allocation, and EC2 pricing models
- Explain the usability of health dashboards

A Day in the Life of an AWS Administrator

You work for an IT company as a system administrator. The company has several cloud-based applications and is searching for a few monitoring solutions for the services it utilizes on the AWS cloud to host them.
Please find the following requirements from the organization, based on which you will have to propose various solutions:

- You should receive an email notification when any of the metrics fall outside of the levels (high or low thresholds) that you configure for any resource.
- There should be a way to monitor each resource that the company uses to ensure its security and performance.

A Day in the Life of an AWS Administrator

- There should be a way to set up a billing setting based on your organization's budget so that an email notification is sent if your account billing surpasses the level you define.
- Additionally, the organization is searching for a solution that will allow them to review, audit, and evaluate all AWS resources' setups.

To achieve all of the above along with some additional features, you will be learning a few concepts in this lesson that will help you find solutions for the above-given scenario.

AWS Monitoring Tools

CloudWatch: Overview

1. CloudWatch is a monitoring and observational service used to monitor resources and applications you run on AWS.

2. It helps you to collect and access all your performances and operational data in the form of logs and metrics.

3. It provides system-wise visibility into resource utilization, application performance, and operational health.

CloudWatch Monitoring

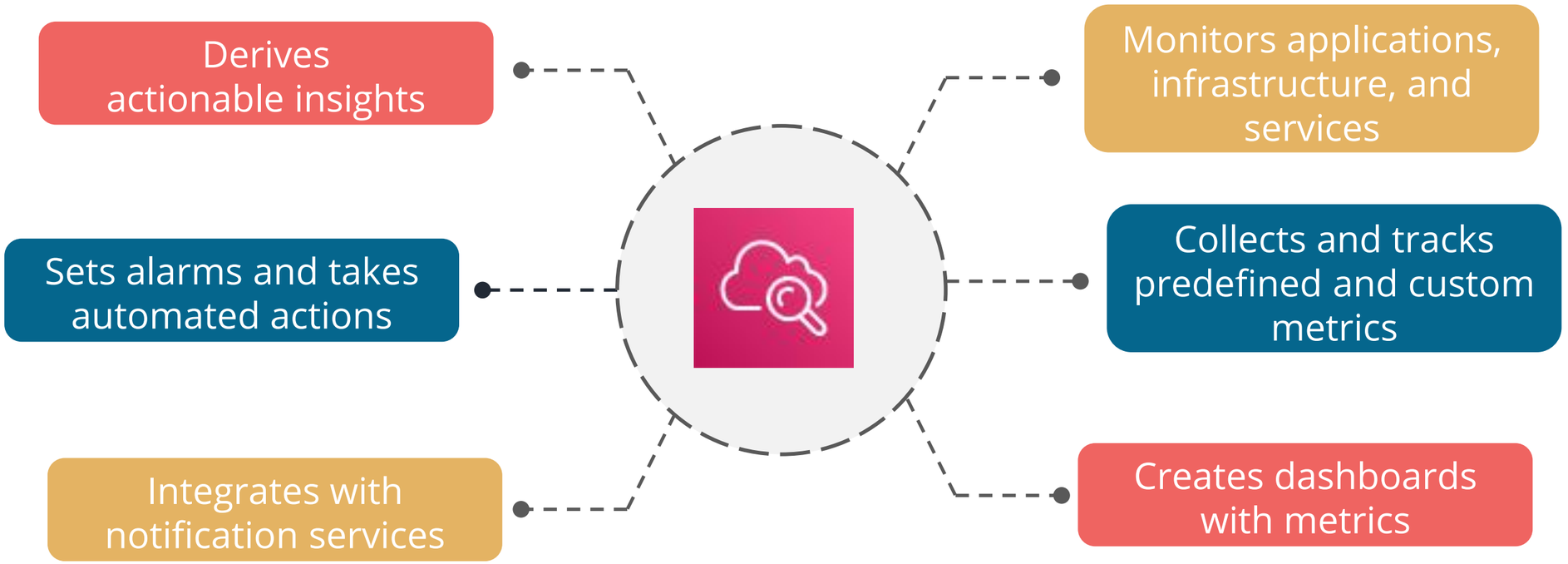
- Autoscaling groups
- Elastic load balancer
- Route 53 health checks

- EBS volumes
- Storage gateways
- CloudFront

- DynamoDB
- ElastiCache nodes
- RDS instances
- Elastic MapReduce job flow
- Redshift

- SNS topics
- SQS queues
- Opsworks
- CloudWatch logs
- Estimated charges on customers' AWS bills

Features of CloudWatch

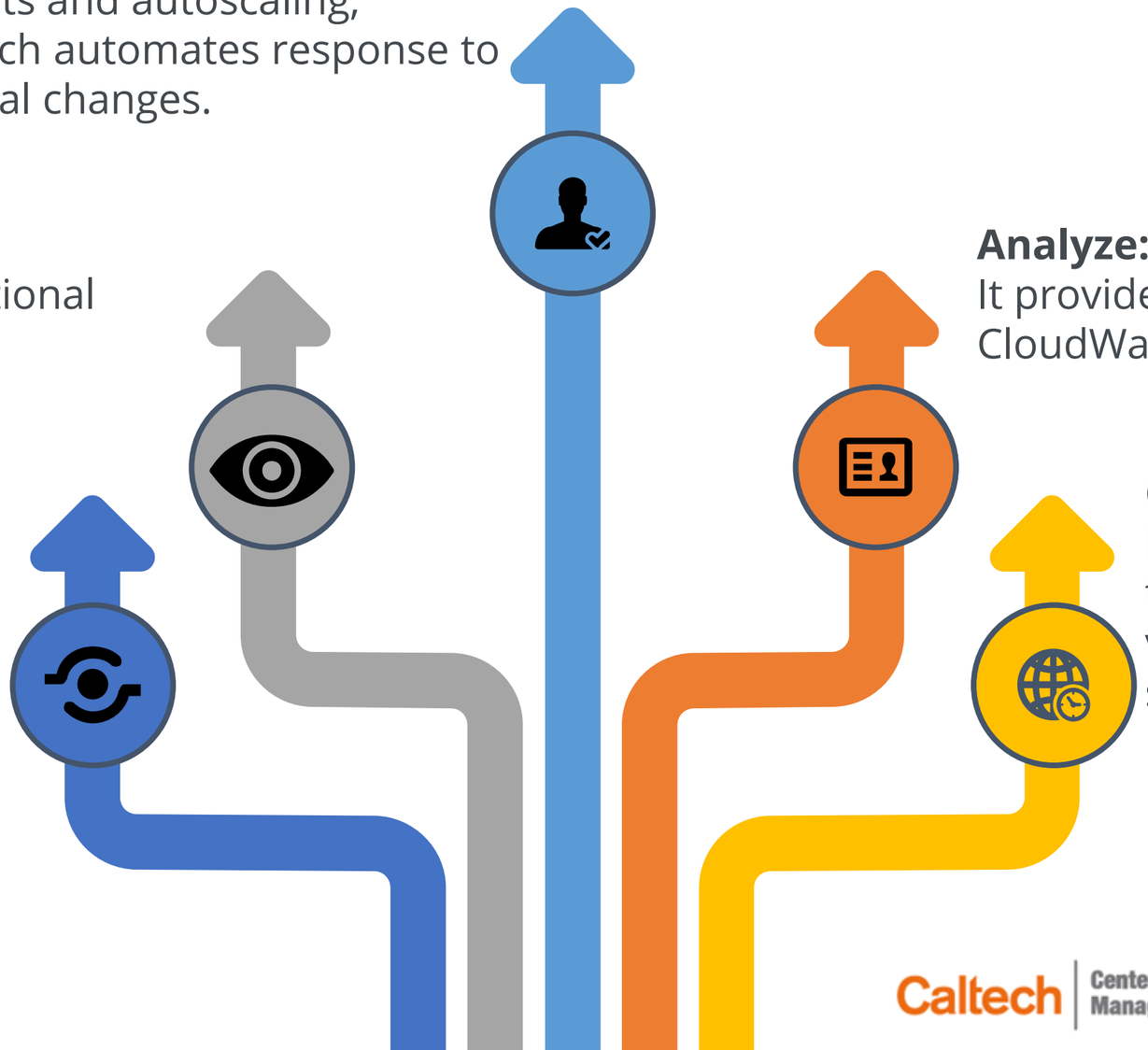


CloudWatch Workflow

Act:
With events and autoscaling, CloudWatch automates response to operational changes.

Monitor:
It provides uniform operational view with dashboards.

Control:
It collects metrics and logs from all AWS resources, applications, and services that run on AWS and on-premises servers.



Analyze:
It provides real-time analysis with CloudWatch Metric Math.

Compliance and Security:
It is integrated with IAM to track a user's activities on various resources and services.

Caltech | Center for Technology & Management Education

simplilearn

CloudWatch Metrics

AWS services provide metrics about performance

- Basic (free)
- Detailed (paid)

Custom metrics are also supported

- Metric data is available for 15 months
- Alarms are set against values for metrics

Metrics can be used for searching and graphing on dashboards

AWS SNS

Amazon Simple Notification Service (Amazon SNS) is a fully managed messaging service for both application-to-application (A2A) and application-to-person (A2P) communication.

Assisted Practice

Create an Alarm Using CloudWatch

Duration: 10 Min.

Problem Statement:

You are given a project to create an alarm using CloudWatch that will allow you to watch CloudWatch metrics and receive notifications when the metrics fall outside the levels (high or low thresholds) that you configure for any resource.

Assisted Practice: Guidelines

Steps to create an alarm using CloudWatch :

1. Login to your AWS lab and open **CloudWatch**
2. In the navigation pane, choose **Alarms**
3. Click on **Create Alarm**
4. Choose the appropriate **Metrics**
5. Provide the required conditions
6. Enter name and description for the alarm
7. Under the **Preview and Create** tab, confirm the provided information
8. Click on **Create**

AWS Health Events

Amazon CloudWatch Events can be used to notice and respond to changes in AWS Health events. Then, when an event meets the values specified in a rule, CloudWatch Events initiates one or more target actions based on the set rules.

A user can send notifications, capture event information, take corrective measures, trigger events, or perform other activities depending on the type of event.

Health Dashboards and Usability

- They consist of service health dashboards and personal health dashboards.
- The service health dashboard shows the health of each AWS service as a whole per region.
- The personal health dashboard notifies you with alerts and remediation guidance when AWS is experiencing few events that may impact you.

CloudTrail

AWS Health is integrated with AWS CloudTrail, a service that monitors all the actions in AWS Health. CloudTrail captures API calls for AWS Health as events.

AWS Health can log the following events in CloudTrail log files:

- Check the request made with root or IAM credentials
- Check the request made with temporary security credentials for a role or federated user
- Check the request made by another AWS service

Monitoring AWS Services

Introduction to EC2

Data can be retrieved from a terminated EC2 instance.

For EC2 monitoring, host level metrics consists of CPU, network, disk, and status check.

By default, CloudWatch logs will store the log data indefinitely.

EC2 monitoring is done every five minutes.

Common EC2 Metrics

CPU Utilization

The percent of EC2 compute units that are used in an instance

NetworkIn

Number of bytes received on all network interfaces by an EC2 instance

NetworkOut

Number of bytes sent out on all network interfaces by an EC2 instance

NetworkPacketsIn

Number of packets received on all network interfaces by an EC2 instance

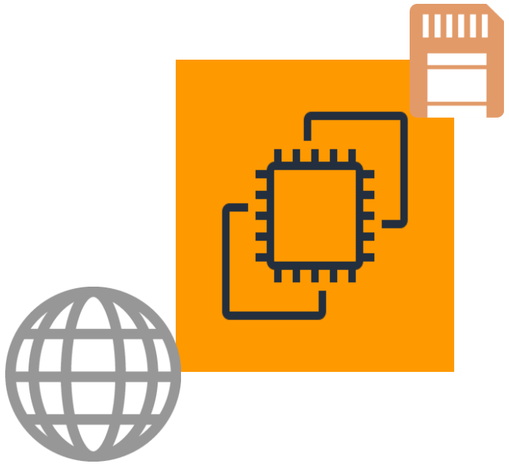
NetworkPacketsOut

Number of packets sent out on all network interfaces by an EC2 instance

Custom EC2 Metrics

You can monitor custom metrics for EC2 instances by:

- Using a CloudWatch agent to collect metrics
- Using a single agent to collect both the system metrics and log files from Amazon EC2 instances
- Installing an agent on your EC2 instance and starting to collect metrics for CPU, disk, memory, and network



Assisted Practice

Monitoring EC2

Duration: 15 Min.

Problem Statement:
You are given a project to set up a monitoring configuration for an EC2 instance that you have launched, to verify the security and performance of your EC2 instance and the data.

Assisted Practice: Guidelines

Steps to monitor an EC2 instance:

1. Login to your AWS lab and search for **IAM**
2. Create a new role for EC2 using CloudWatch
3. Provide the required information and click on **Create**
4. Go to EC2
5. Create a new EC2 instance per your requirements
6. In **IAM role**, select the newly created IAM role
7. Use terminal and connect the EC2 instance using the SSH command
8. In the AWS console, go to CloudWatch
9. Click **Browse Metrics**
10. Select EC2 and check the status of the EC2 instance

Introduction: EBS Volume

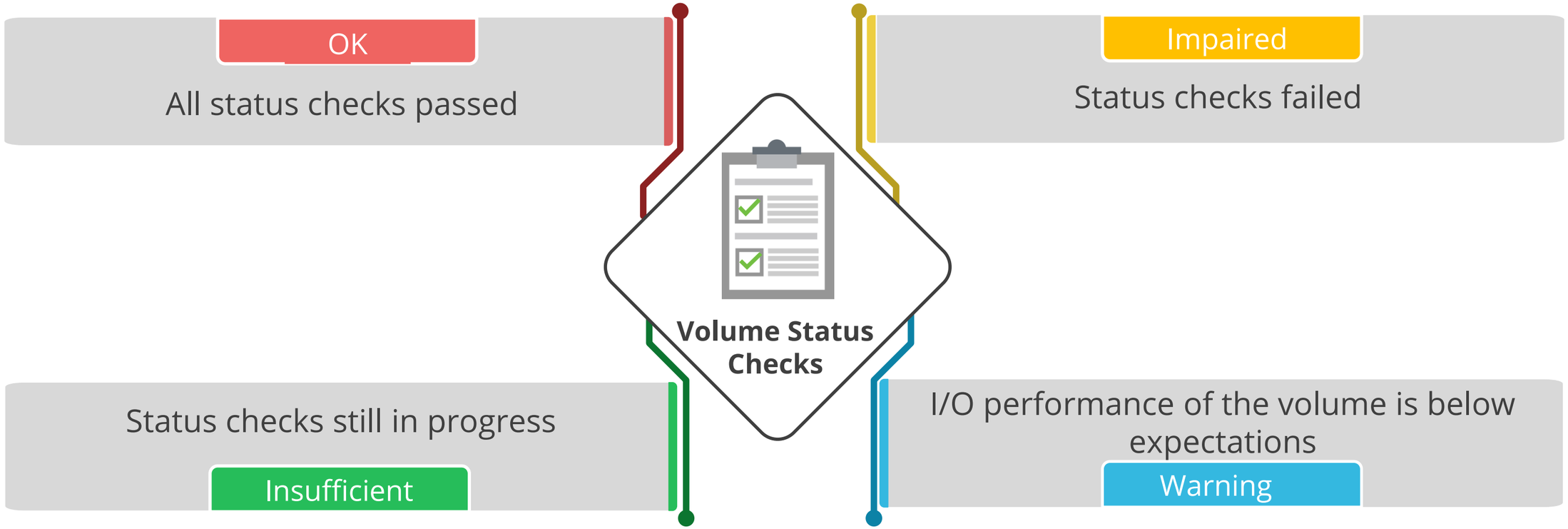
Amazon Elastic Block Store (EBS) is an easy-to-use and high-performance block storage service which allows to attach storage volumes to Amazon EC2 instances.

EBS volumes are highly available, secure, cost-effective, and easy to use.

Elastic volume feature allows to dynamically increase the capacity, tune performance, and change the volume of a live volume.

EBS volumes are created in specific availability zones. From the respective zones, data can be replicated to protect it from failure.

Types of Volume Status Check



Assisted Practice

Monitoring EBS

Duration: 20 Min.

Problem Statement:
You are given a project to set up a monitoring configuration for an EBS Volume that you have created, to verify the security and performance of your EBS Volume.

Assisted Practice: Guidelines

Steps to monitor an EBS volume using CloudWatch:

1. Login to your AWS lab and open **CloudWatch**
2. Click on **Create Alarms** in the navigation pane
3. Click on **Select Metrics**
4. Provide the name and decryption of the alarm
5. Configure the threshold and set up a notification for the alarm
6. Click on **Create Alarm**

Monitoring ELB: Overview

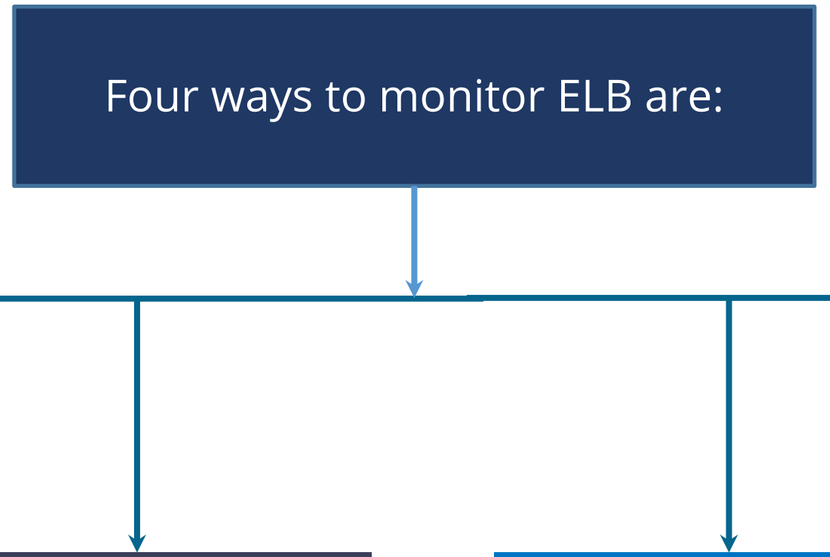
There are three types of ELB: Application Load Balancer, Classic Load Balancer, and Network Load Balancer

Elastic load balancer (ELB) automatically distributes incoming application traffic across multiple targets

ELB is secure, flexible, and elastic and provides robust monitoring

It allows to manage incoming traffic by optimally transferring the traffic to make sure that no instance is overloaded

ELB Monitoring Types



CloudWatch metrics

- To monitor performance
- To keep a track of healthy targets coming over a specific period of time

Access logs

- To store information about request time, client's IP address, and server responses
- To analyze traffic patterns and troubleshoot issues

Request tracing

- To keep a track of HTTP requests from clients to targets or other services

CloudTrail logs

- To capture information about calls made to the ELB API and store the log into S3

Assisted Practice

Monitoring ELB

Duration: 10 Min.

Problem Statement:
You are given a project to set up a monitoring configuration for an ELB that you have created, to verify the security and performance of your ELB.

Assisted Practice: Guidelines

Steps to monitor an ELB:

1. Login to your AWS lab
2. Open the Amazon EC2 console and configure **Load balancers**
3. Open the Cloudwatch console and configure **Metrics**

ElastiCache: Overview

- Amazon ElastiCache is a distributed cache environment which allows to set up, run, and scale popular in-memory data stores on cloud.
- It improves the performance of existing databases by retrieving information from managed in-memory cache.
- It is used in many real-time use cases such as gaming, queuing, and real-time analytics.
- It has fully managed Redis and Memcached engines for in-memory caching.
- To monitor caching engines, one should look at CPU utilization, swap usage, evictions, and concurrent connections.

Assisted Practice

Managing ElastiCache Amazon SNS Notifications

Duration: 10 Min.

Problem Statement:
You are given the task to monitor ElastiCache that provides enhanced visibility via CloudWatch into key performance metrics associated with your resources.

Assisted Practice: Guidelines

Steps to monitor an ElastiCache:

1. Login to your AWS lab and open **CloudTrail**
2. Add an **AWS CloudTrail Source** by providing the required information
3. Configure **Amazon CloudWatch metrics**
4. Collect Amazon ElastiCache events with **AWS SNS**

Assisted Practice

Create a Billing Alarm

Duration: 15 Min.

Problem Statement:
You are given the task to create a billing alarm for your enterprise AWS account so that a notification will trigger whenever your account billing exceeds the threshold you had specified.

Assisted Practice: Guidelines

Steps to create a billing alarm:

1. Login to your AWS lab
2. Under **Management and Governance** option, select **CloudWatch**
3. Click on **Billing**
4. Click on **Create alarm**
5. Fill in the required information to create the alarm
6. Click on **Create alarm**

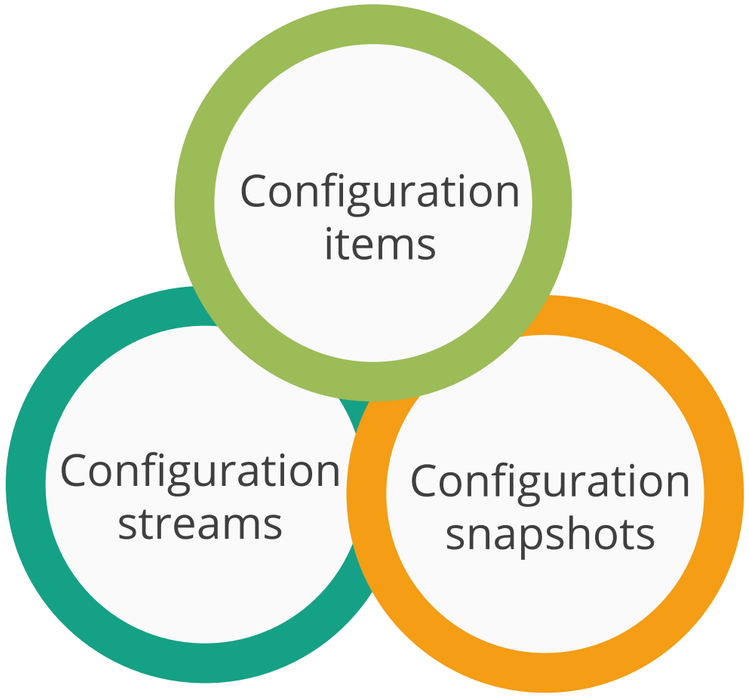
AWS Config

AWS Config

- It is a fully managed service that provides you with an inventory, configuration history, and configuration change notifications to enable security and governance.
- It continuously monitors and records AWS resource configurations and allows to automate the evaluation of recorded configurations against desired configurations.
- AWS config stores everything inside an S3 bucket.

Terminologies Used for AWS Config

Point-in-time attributes of resources

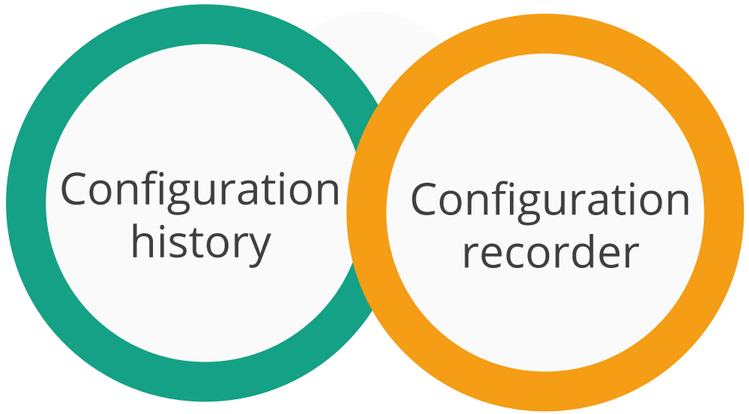


Streams of changed config items

Collection of config items

Terminologies Used for AWS Config

Collection of config items for a resource over time



Records and stores config items

AWS Config: Workflow

When configuration changes occur in your AWS resources

Event

AWS Config

Records and normalizes the changes into a consistent format and stores data in an S3 bucket

AWS Lambda

Uses standard or custom rules

AWS SNS

Alerts you when changes occur

Assisted Practice

Setting Up AWS Config

Duration: 20 Min.

Problem Statement:
You are given a project to create an AWS Config that will enable you to assess, audit, and evaluate the configurations of your AWS resources, and will allow you to automate the evaluation of recorded configurations against desired configurations.

Assisted Practice: Guidelines

Steps to monitor AWS config:

1. Login to your AWS lab
2. Under **Management Tools**, select **Config**
3. Provide the required information for **Settings**
4. Add config rules

Assisted Practice

AWS Config with S3

Duration: 10 Min.

Problem Statement:

Demonstrate the working of AWS Config with S3.

Assisted Practice: Guidelines

Steps to use AWS config with S3:

1. Selecting S3 bucket
2. Creating config rules for S3

Key Differences: AWS Config vs. AWS CloudTrail vs. AWS CloudWatch

AWS Config	AWS CloudTrail	AWS CloudWatch
Monitors and records the state of an AWS environment and notifies users for changes	Monitors API calls in the AWS platform	Monitors performance
Focuses on the configuration of AWS resources and reports with detailed snapshots on how resources have changed	Focuses on the user, application, and activity performed on the system	Focuses on real time stream of system events describing changes to AWS services

Cost and Performance Optimization Tools

Cost Explorer and Cost Allocation

Cost explorer

- It is a tool that enables you to view and analyze cost and usage.
- It allows to view old data up to thirteen months, forecast data for next three months, and get recommendations to purchase reserved instances.

Cost allocation

- After activating the tags applied to the AWS resources in the billing and cost management console, AWS generates a cost allocation report in the .csv format.

Cost allocation tags

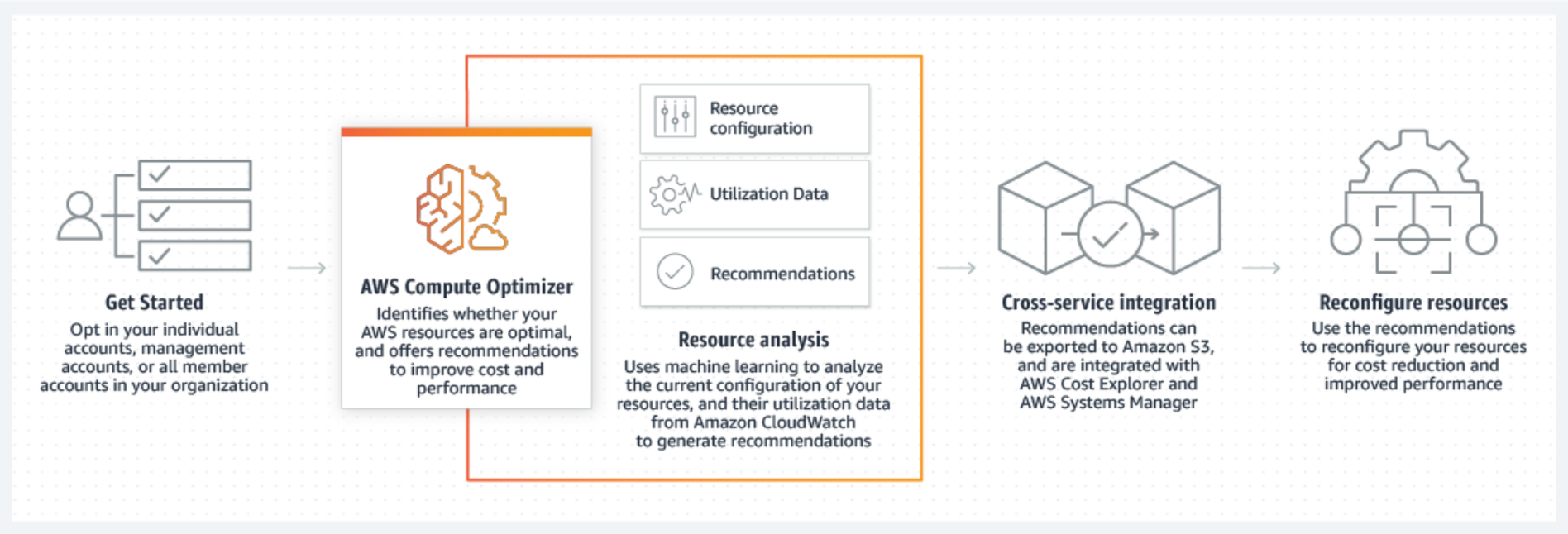
- These are used to track your AWS cost in detail.
- Two types of cost allocation tags are AWS-generated tags and user-defined tags.

AWS Compute Optimizer

AWS Compute Optimizer uses machine learning to examine historical utilization metrics to recommend ideal AWS resources for their workloads in order to minimize costs and enhance performance.

AWS Compute Optimizer

This is the workflow of Compute Optimizer:



Cost Optimization Strategy

Recommend Compute Resources Based on Performance Metrics

Compute Optimizer examines the current instance specifications as well as performance metrics. Then, the gathered data recommends the best-suited Amazon EC2 instance type for the current workload.

Recommendations are provided with per-hour instance cost.

Configure AWS Budgets and Billing Alarms

A user can use AWS Budgets to monitor and manage the AWS costs and usage.
AWS Budgets can be used to track aggregate utilisation and coverage metrics for Reserved Instances (RIs) or Savings Plans.

Users can use AWS Budgets to enable simple-to-complex cost and usage tracking. Some examples include:

- Setting a monthly cost budget with a fixed target amount
- Setting a monthly cost budget with a variable target amount
- Setting a monthly usage budget with a fixed usage amount and forecasted notifications
- Setting a daily utilization or coverage budget

AWS Account Management

AWS Service Catalog

Allows organizations to create and manage catalogs of IT services that are approved for use on AWS

Includes virtual machine images, servers, softwares, and databases to complete a multi-tier architecture

Manages the commonly deployed IT services to achieve consistent governance and meet IT compliance requirements

Enables the users to quickly deploy only the approved IT services they need

Benefits of AWS Service Catalog

1. Ensures compliance with corporate standards
2. Centrally manages an IT service lifecycle
3. Helps employees to quickly find and deploy approved IT services
4. Connects with ITSM/ITOM software

Assisted Practice

AWS Service Catalog Portfolio

Duration: 10 Min.

Problem Statement:

You are given a project to create an AWS Service Catalog that will allow your organization to create and manage catalogs of IT services that are approved for use on AWS.

Assisted Practice: Guidelines

Steps to create a portfolio::

1. Login to the AWS Service Catalog console
2. Choose **Create portfolio**
3. Enter the necessary details and choose **Create**

Key Takeaways

- CloudWatch is a monitoring and observational service used to monitor resources and applications.
- Amazon SNS is a fully managed messaging service for both application-to-application (A2A) and application-to-person (A2P) communication.
- Elasticache has fully managed Redis and Memcached engines for in-memory caching.
- AWS Config continuously monitors and records AWS resource configurations and allows to automate the evaluation of recorded configurations against desired configurations.