AWS SysOps Administrator – Associate Level

TECHNOLOGY

Getting Started with SysOps

simplilearn

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

CloudWatch

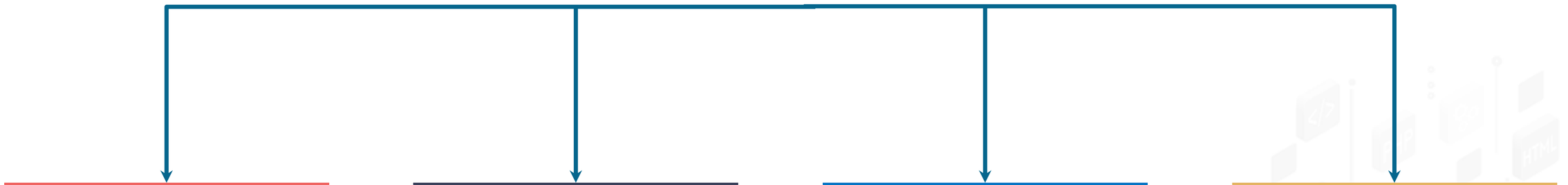
CloudWatch: Overview

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



Compute

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

Storage and Content Delivery

- EBS volumes
- Storage gateways
- CloudFront

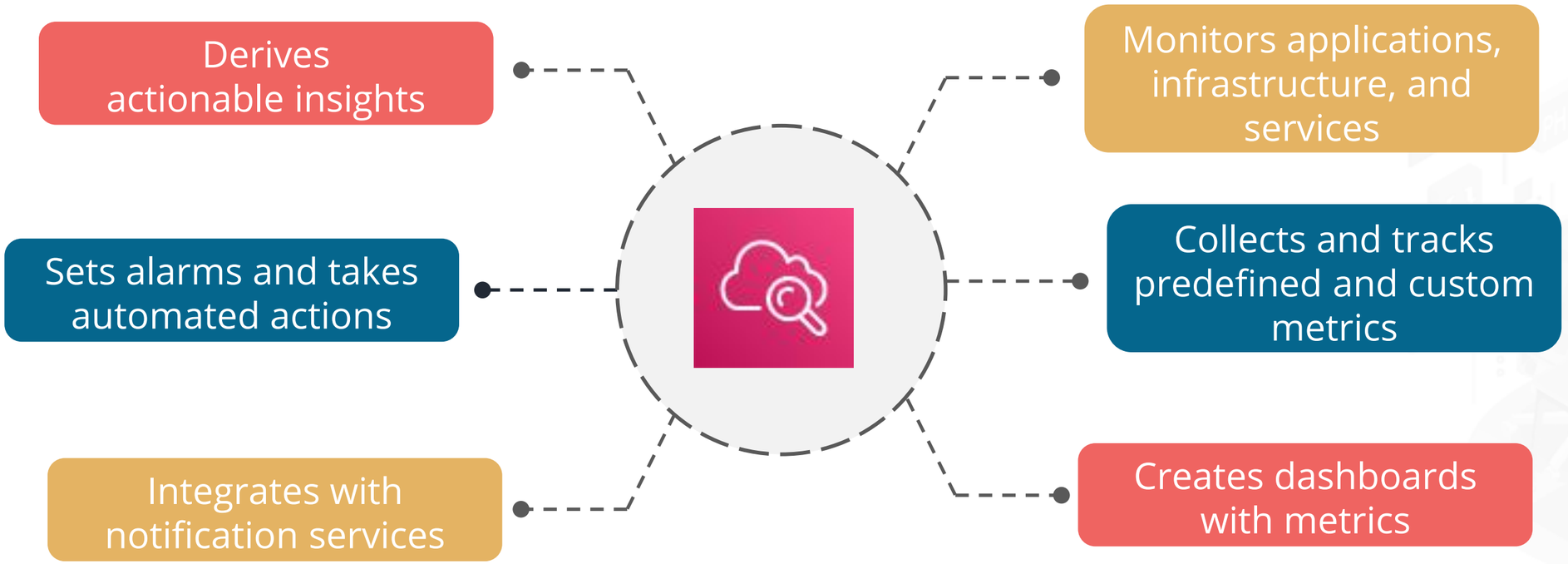
Databases and Analytics

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

Others

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

Features of CloudWatch

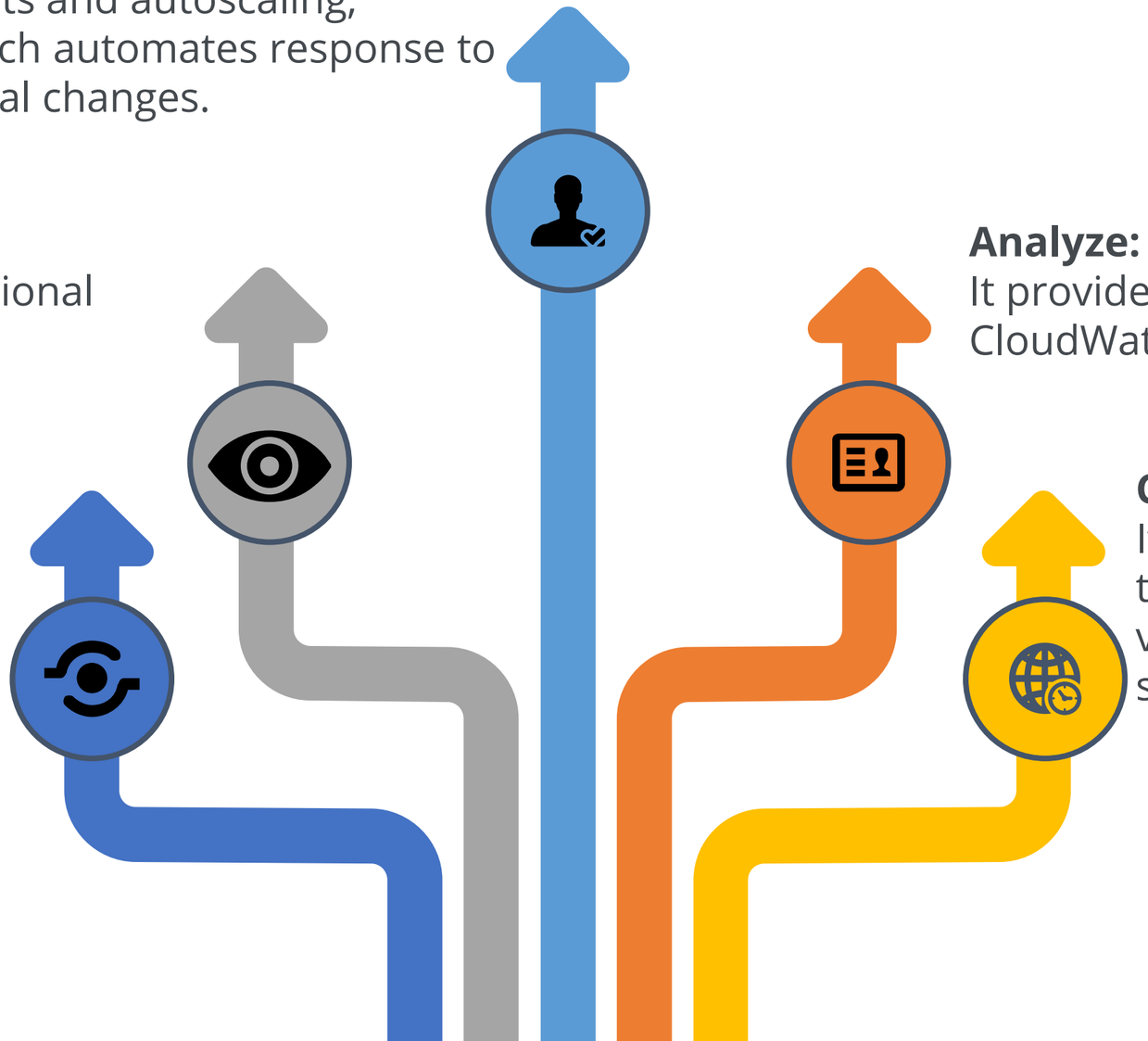


CloudWatch Workflow

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.

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

Create an Alarm Using CloudWatch

Duration: 10 Min.

Problem Statement:

Create an alarm to monitor the Amazon CloudWatch metric in your account.

ASSISTED PRACTICE

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**

Monitoring EC2

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

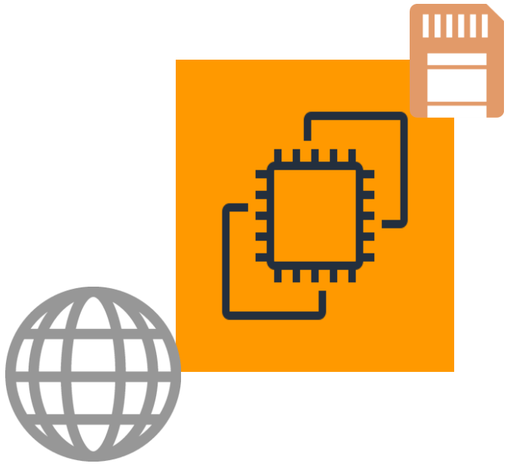
NetworkPacketsOut

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



Monitoring EC2

Duration: 15 Min.

Problem Statement:

Monitor a created EC2 instance with custom metrics.

ASSISTED PRACTICE

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

Monitoring EBS

Introduction: EBS Volume

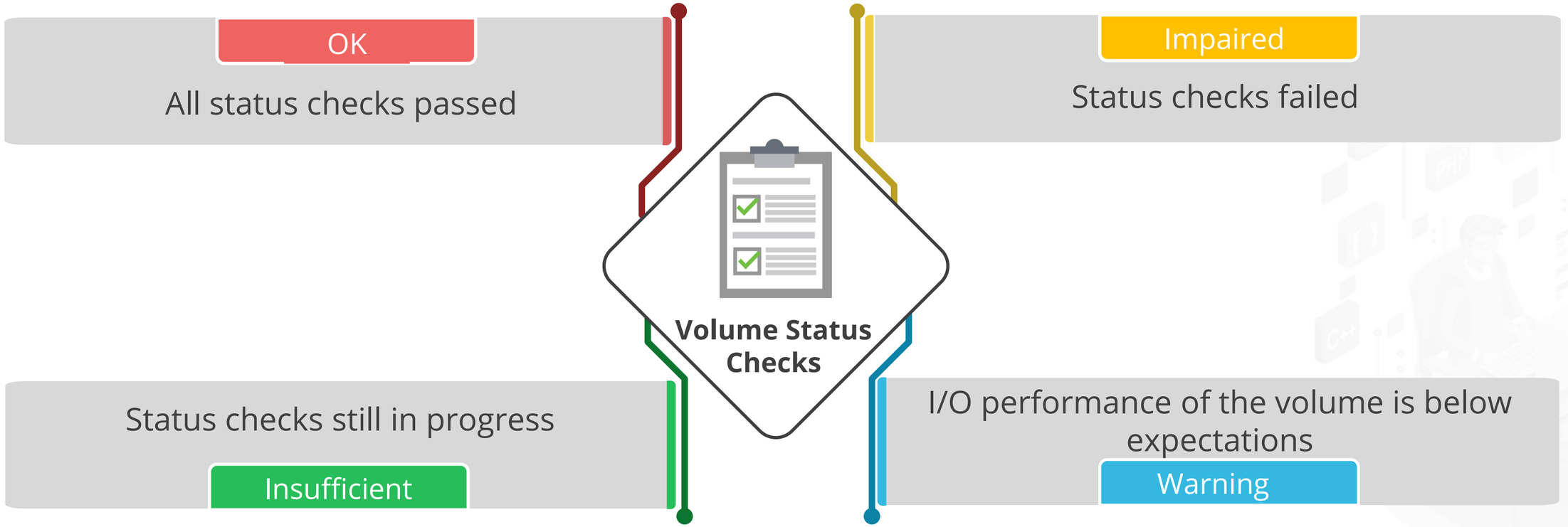
Amazon Elastic Block Store (EBS) is an easy-to-use and high-performance block storage service which allows to attach storage volumes to Amazon EC2 instances.

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



Monitoring EBS

Duration: 20 Min.

Problem Statement:

Monitor an EBS volume using CloudWatch.

ASSISTED PRACTICE

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

Monitoring ELB: Overview

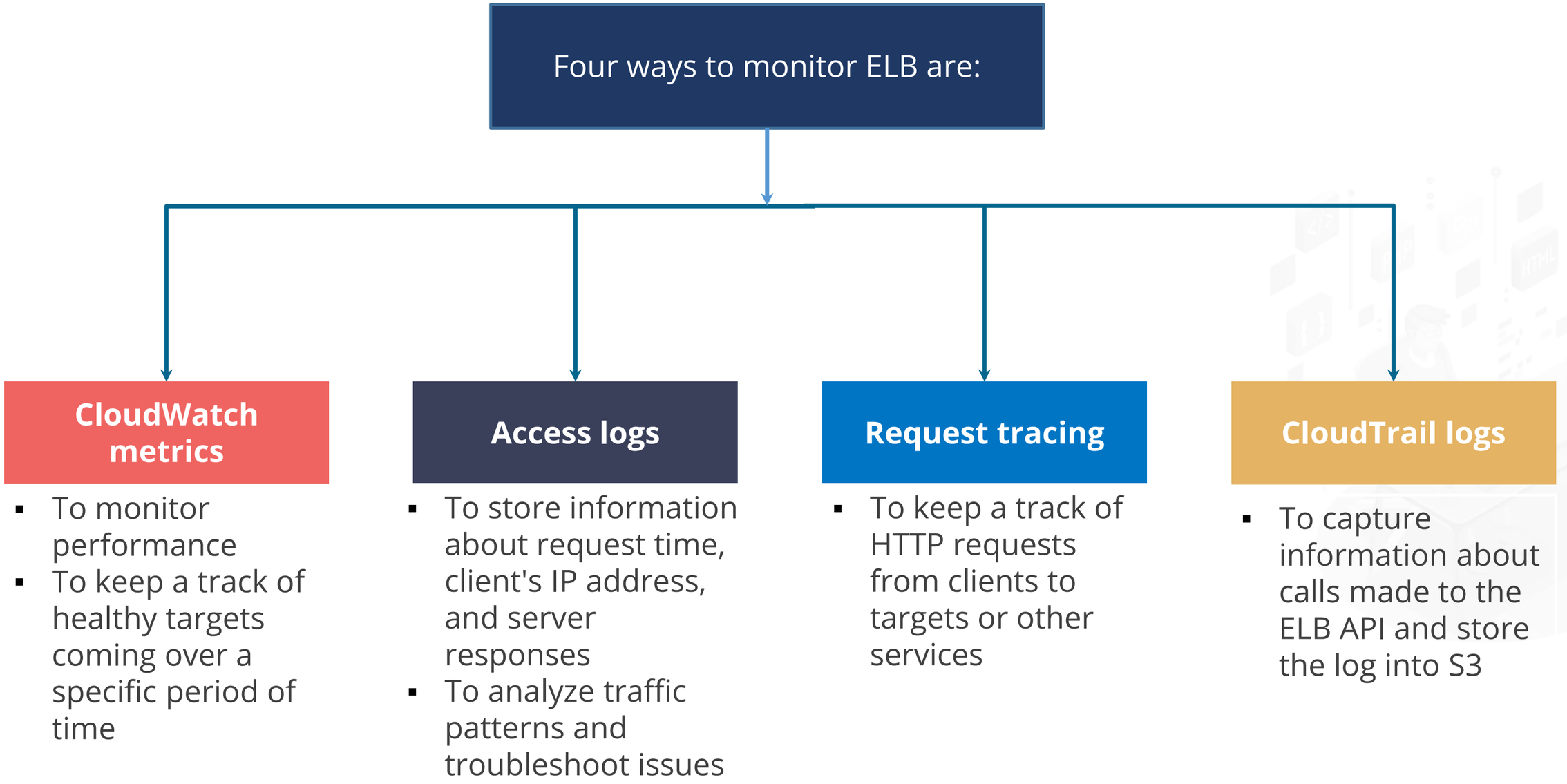
There are three types of ELB: Application Load Balancer, Classic Load Balancer, and Network Load Balancer

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



Monitoring ElastiCache

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.

Monitoring ElastiCache

Duration: 10 Min.

Problem Statement:
Monitor an ElastiCache.

ASSISTED PRACTICE

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**

Metrics from Multiple Regions and Custom Dashboards

Duration: 10 Min.

Problem Statement:

Monitor CloudWatch custom dashboards.

ASSISTED PRACTICE

Assisted Practice: Guidelines

Steps to monitor the CloudWatch custom dashboards:

1. Login to your AWS lab
2. Under **Management Tools** option, select **CloudWatch**
3. Click on **Dashboards**
4. Click on **Create dashboard** and provide a name to the dashboard
5. Select the metrics
6. Select the type of monitoring information
7. Save the dashboards

Create a Billing Alarm

Duration: 15 Min.

Problem Statement:
Create a billing alarm.

ASSISTED PRACTICE

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 Organization

Duration: 10 Min.

Problem Statement:
Set up an AWS organization.

ASSISTED PRACTICE

Assisted Practice: Guidelines

Steps to create an AWS organization:

1. Login to your AWS lab
2. In the **Helpful tips**, click on **Create an organization**
3. Click on **Create organization**
4. Click on **Add accounts** to add different AWS accounts
5. Click on **Organize accounts**
6. Add a policy based on your requirements
7. Attach the created policies to the organization

AWS Resource Groups and Tagging

Duration: 10 Min.

Problem Statement:

Create resource groups and tags.

ASSISTED PRACTICE

Assisted Practice: Guidelines

Steps to create resource groups and tags:

1. Login to your AWS lab
2. Create new EC2 instances
3. Once all the instances are up, go to **Resource Groups**, and click on **Tag Editor**
4. Provide the required information
5. Create tags and attach them to created instances
6. Go to **Resource Groups** and select **Saved Groups**
7. Click on **Create a resource group**

TECHNOLOGY

Cost Explorer and Cost Allocation Tags

simplilearn

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.

Cost Explorer and Cost Allocation Tags

Duration: 15 Min.

Problem Statement:

Set up cost allocation tags and check the status in the cost explorer.

ASSISTED PRACTICE

Assisted Practice: Guidelines

Steps to monitor the cost explorer dashboard:

1. Login to your AWS lab
2. Create an AWS organization
3. Select the created dashboard
4. Click on **Billing** dashboard
5. Click on **Cost allocation tags**
6. Select a tag per your requirement and click on **Activate**
7. Click on **Cost explorer**
8. Select **Launch explorer**
9. Go to **Cost and Usage**

EC2 Pricing Models

EC2 Pricing

On-demand

In this pricing model, you have to pay for compute capacity by the hour or second with no long-term commitments.

Reserved

- It gives a discount up to 75% compared to on-demand instance pricing.
- It provides capacity reservation when used in a specific availability zone.

Spot

These instances are available even at a discount of 90% compared to on-demand instances. They allow you to request spare EC2 computing capacity.

Dedicated hosts

- A physical EC2 server is dedicated for the use.
- It helps to reduce cost by allowing to use existing server-bound software license.

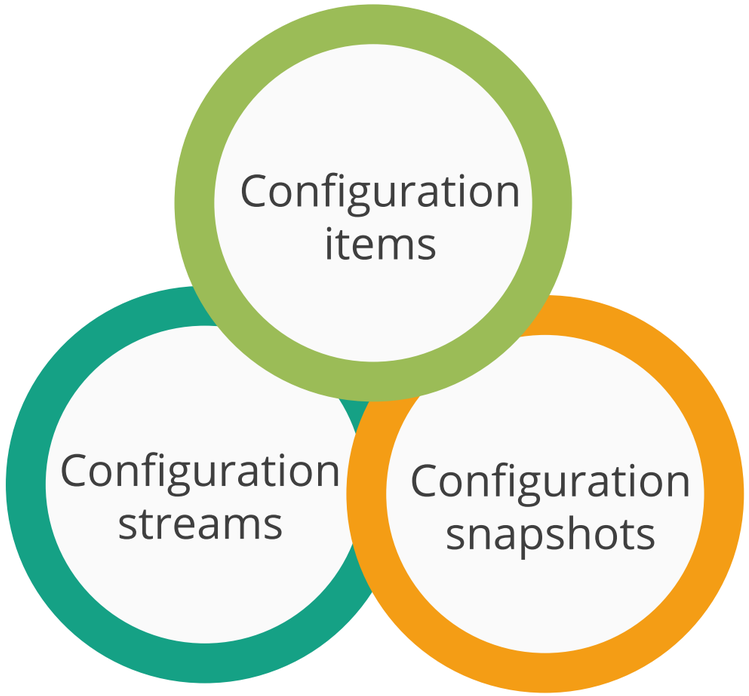
AWS Config

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

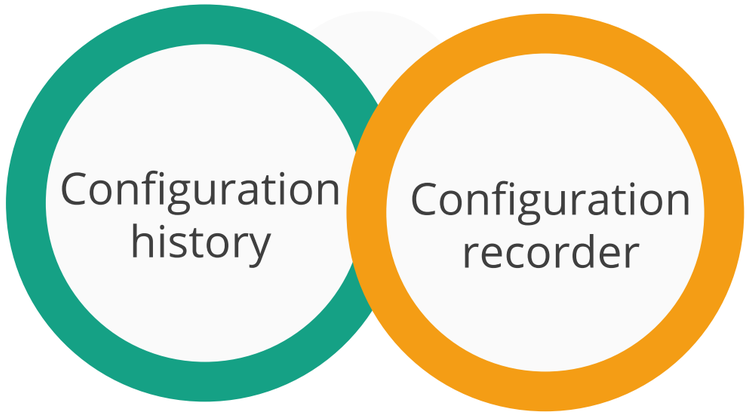


Streams of changed config items

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

AWS Config

Duration: 20 Min.

Problem Statement:
Monitor AWS config.

ASSISTED PRACTICE

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

AWS Config vs. AWS CloudTrail vs. AWS CloudWatch

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

Health Dashboards

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.

Key Takeaways

- CloudWatch is a monitoring and observational service used to monitor resources and applications.
- EBS volumes are created in specific availability zones. From the respective zones, data can be replicated to protect it from failure.
- Elastic load balancer (ELB) automatically distributes incoming application traffic across multiple targets.
- AWS Config continuously monitors and records AWS resource configurations and allows to automate the evaluation of recorded configurations against desired configurations.

.

Create an Application Load Balancer Using EC2

Problem Statement:
Create an application load balancer using EC2, and analyze the CPU utilization by creating an alarm.

Background of the problem statement:
Your manager has assigned a project where you have to create an ELB using an EC2 instance. You also need to create an alarm that sends an email if the CPU utilization is above or equal to 15%.

LESSON-END PROJECT