**130 Mins - 60 Questions**

**Pass mark: 720 (Marks: 100-1000)**

**Qualification valid for 2 years**

**All Scenario based questions**

AWS Cloud Practitioner course

Amazon ES2, S3, EBS, RDS, CloudFront

TCO Calculator

AWS Cloud Infra: Elasticity, Scalability, Reliability

Regions & Availability Zones (AZ)

Edge Locations

Regions – Physical location – Contains multiple AZs

AZ – One or more discrete data centers - housed in separate facilities

Edge Location – Content Delivery Network – Amazon CloudFront – Delivers content to customers from nearest Edge location – Located in highly populated regions (aws.amazon.com/CloudFront/details)

Systems always available (Downtime reduces and upgrades can happen without human intervention)

TAGS: Always important & useful. In case of billing, easy to identify which resource is consuming what easily, if we have TAGS.

# Elasticity

Scale computing resources up or down & pay for only used resource.

AWS Lambda falls under “Compute” category

EC2 – Elastic Compute Cloud

More->Documentation-> All products help available category-wise. No need to login.

Regions-> Not automatically replicated on other regions

# Amazon Virtual Private Cloud (AVPC)

AVPC – Lives in a region and can span across multiple AZs within a region

Subnet- Public/Private/Republic

Republic – Needs an internet gateway to access VPC and update route table of the public subnet

EC2 instances need a public IP address to route to an internet gateway

Classless Inter-Domain Routing (CIDR) block

If a subnet's traffic is routed to an internet gateway, the subnet is known as a public subnet.

If a subnet doesn't have a route to the internet gateway, the subnet is known as a private subnet.

# AWS Compute

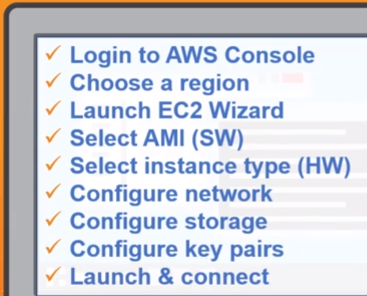
AWS Lightsail – Suitable for building simple e-commerce applications

ECS – Containers – Build, operate own cluster management services

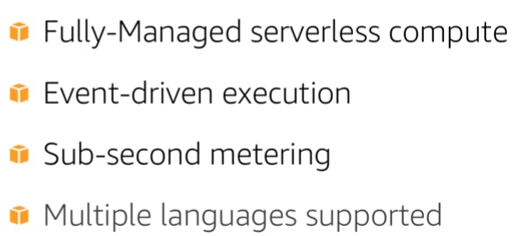
# EC2 – Elastic Compute Cloud

Instance – Pay as you go

AMI – Amazon Machine Image – Software platform for the EC2 instance



# LAMBDA



Executes code only when needed and scales upto 1000s of requests/second

Supports: C#, Java, python

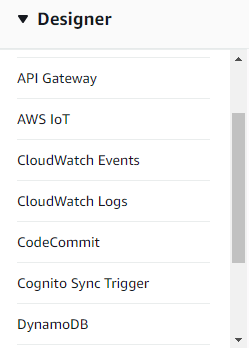
Build serverless micro-services

Event driven: Suitable where code needs to execute based on certain event, e.g. Updation of a

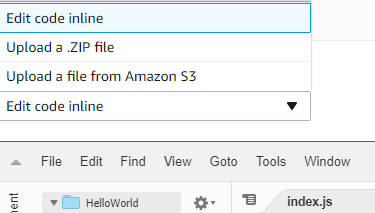
DynamoDB table, change in an S3 bucket

Billed based on no. of times code is triggered and for each millisecond of code execution

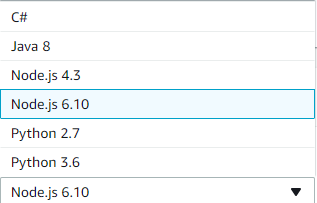
Under Configuration->Designer we can add any kind of trigger E.g,



Under Function code, we can start coding or import from a file:



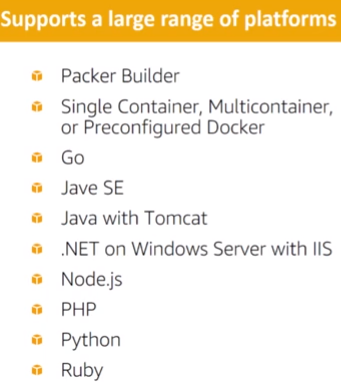
Runtime has following options:



You can configure the memory you need for a function, time for how long it must run (Time out)

# Elastic Beanstalk – Web Application Package

Platform as a Service, Choose our own Instance type (OS), DB, Autoscale



We can create a new environment which includes: (Instance creation/attachment, DB, for which programming language (python, java, node.js,etc)

It will set-up the complete environment and enable us to deploy as soon as our code is ready

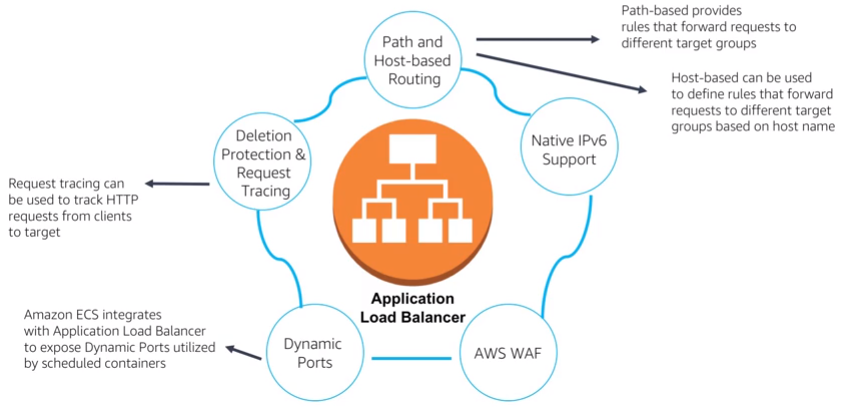
# Application Load Balancer (ALB)

When to use ALB?

When you use Containers to host microservices and route to those applications through single load balancer.

ALB register Targets instead of instances

Target – Destination of traffic based on established listener rules



Applications can be on same EC2 instance but different paths based on the port number.

Demo showed configuring two ports: 80 & 443

When configuring load balancer in EC2, can add multiple listeners (Load balancer protocol & load balancer port)

Then configure security group

Then configure Routing

Then Configure Health Checks

Then register Targets

# Elastic Load Balancer

Classic Load Balancer – Can have both public & private subnet. To isolate any back-end service from public network.



Traffic Distribution:

HTTP request: Round robin

TCP request: Least outstanding requests for the backend instances

**Traffic Distribution based on AZ**: If LB is launched from AWS Console, this is default, else if it is launched through Command line tools or an SDK, we need to associate the LB to an AZ as a separate process

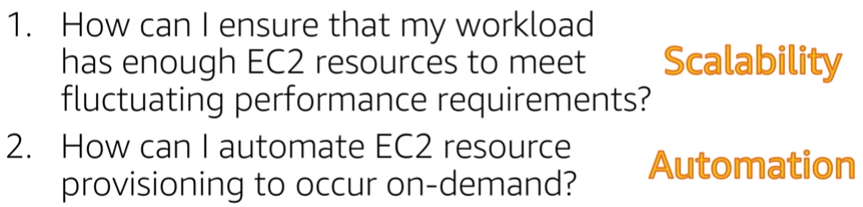
**Monitoring**: Filter metrics based on AZ or LB

**Types of LB:**

Public/Internet facing

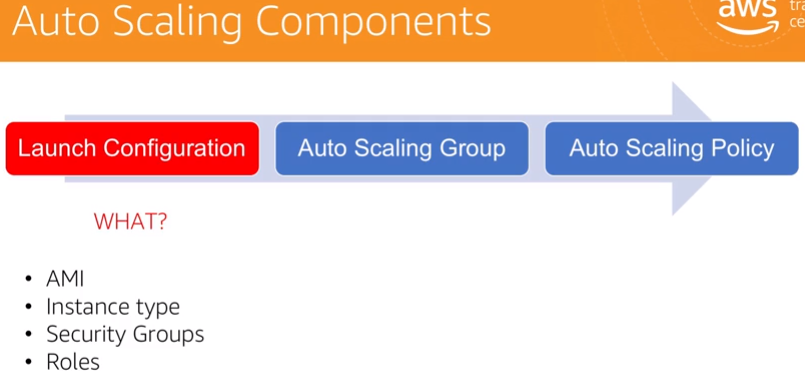
Internal

# Auto Scaling



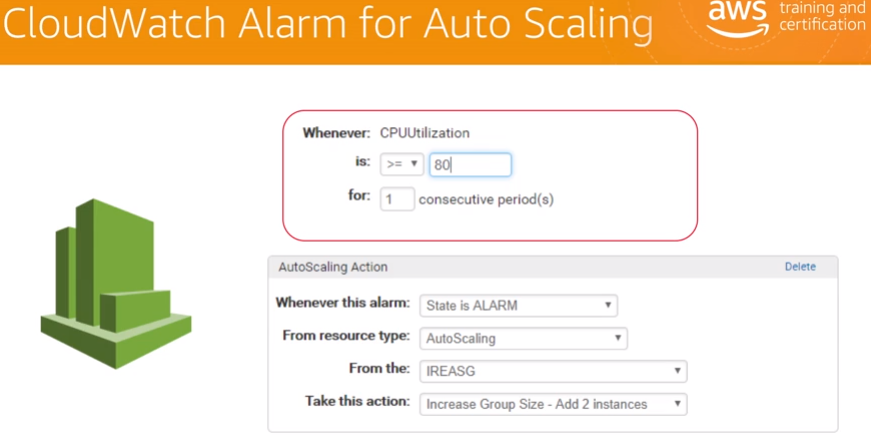
**Scaling Out**: Adding more EC2 instances

**Scaling In:** Terminating EC2 instances



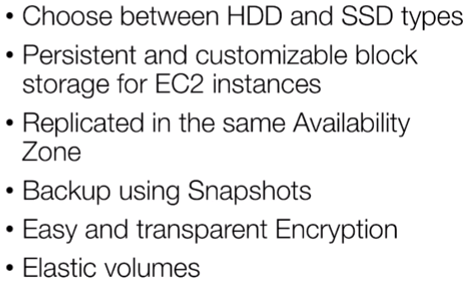






**Default metric interval for CloudWatch: 5 mins (One period = 5 mins)**

# Elastic Block Store (EBS)



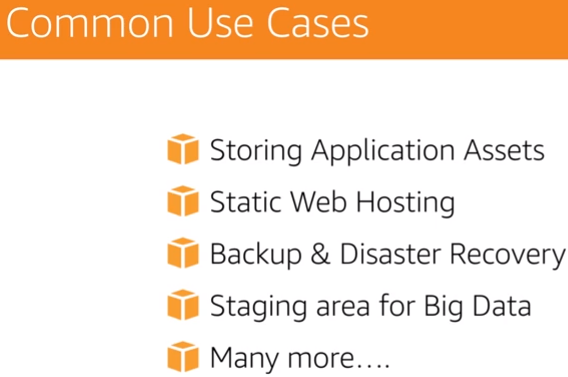
EBS Volume (SSD or HDD)

EBS volume must be created on same AZ where the instance is.

# Simple Storage Services

Amazon S3 – Managed cloud storage device

Stores objects (files,images,videos,etc) – Supports objects of size TB, even DB snapshot can be an object



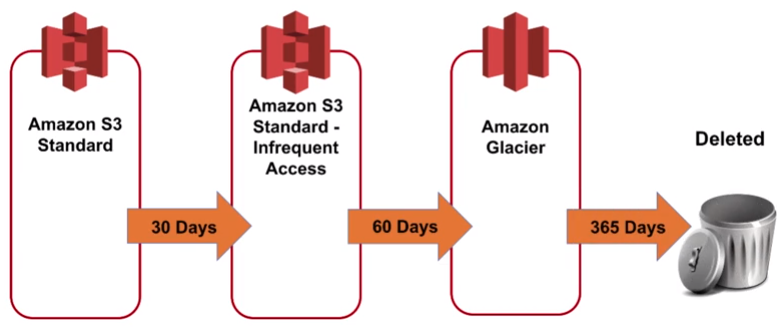
AWS Import/Export device – Snow ball

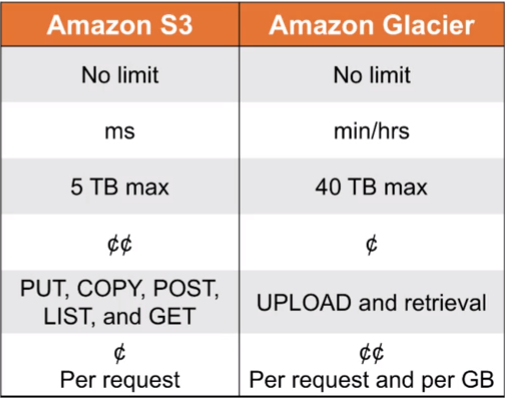
# Amazon Glacier

Data archiving solution

Archive – Basic storage unit – Can be any object

Vault-Vault name and storage region to be specified Access policy



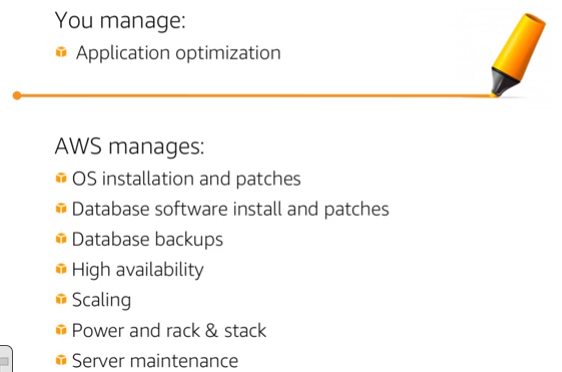


Glacier – More charge for retrieval

Glacier – Encrypts data with AES-256

Glacier – Data archival for long-term analytics

# Amazon Relational Database System (RDS)



DB Instance is the base, currently supports 6 DBs:



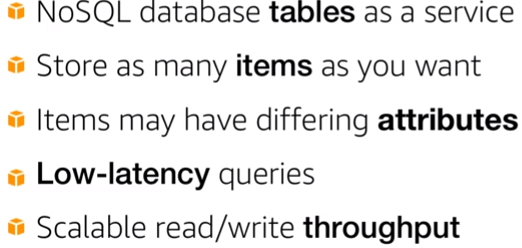
DB Instances usually are hosted in private subnet VPC. Can be accessed only by applications that we specify

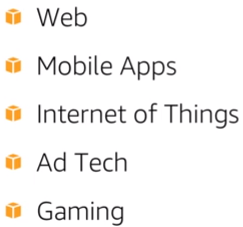
A private subnet is associated with an AZ, so when we select subnet, we select AZ and in turn physical storage location.

**RDS Read Replicas** – Can read from MySQL,MariaDB,Amazon aurora. Can be used when you want a DB nearer to user to save on latency



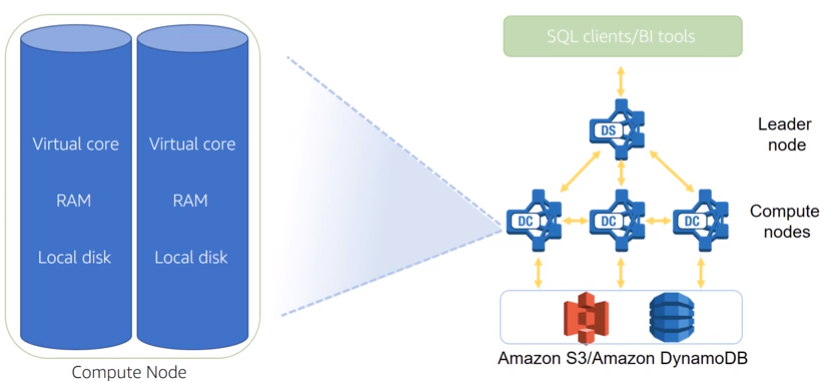
# Amazon DynamoDB





# Amazon RedShift

Data Warehouse Service



Enterprise Data Warehouse, Big Data, SaaS

Create Redshift Cluster

It will have JDBC & ODBC Connection links

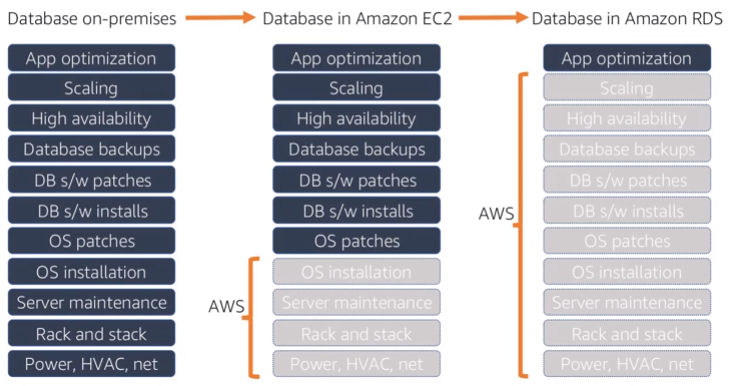
Open SQL WorkBench

Connect to the needed DB and create table.

Use Copy command to upload data from an S3 instance or any external source

# Amazon Aurora

High performance, cost effective, managed RDS



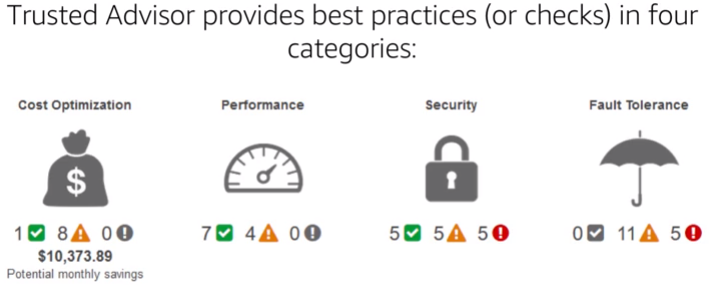
Amazon Aurora Vs Amazon RDS

-High Availability – Available in 3 AZs, Up to 15 Read Replicas can be used

-Resilient Design – Redo Log happens on every read operation – So, after a crash, very easy to recover and start again

# AWS Trusted Advisor

Keep track of your AWS Resources



Trusted Advisor – Integrated with CloudWatch Events

Helps in building Automation of optimization of AWS resources

# AWS Security

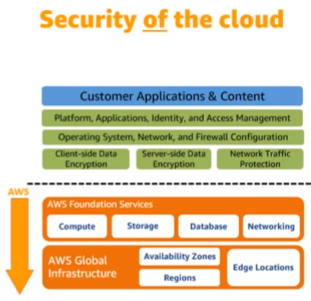
Governance Enabled Features

Inherit AWS security controls

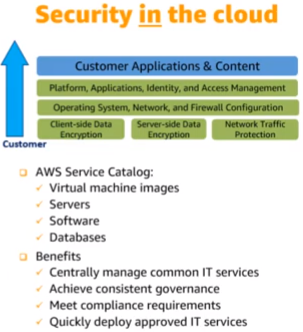
DDOS Mitigation Technology

Monitoring & Logging

Shared Responsibility Model







AWS Security Catalog – To choose and configure security features

# AWS Access Control & Management

Two types of Access: Programmatic & Management Console Access



Both Access Key ID & Secret Access key needed if an IAM user has to access AWS programmatically



# AWS Security Compliance Programs









<https://aws.amazon.com/compliance/>

<https://aws.amazon.com/compliance/hipaa-compliance/>

# AWS Security Resources

AWS Auditor Learning Path

AWS Compliance Solutions Guide

Services In Scope

AWS Security Blog

Case Studies

<https://aws.amazon.com/securiy>

# AWS Architecting Essentials

## Security Pillar

IAM

Detective Controls

Infrastructure Protection

Data Protection

Incident Response



## Reliability Pillar

Before implementing any cloud architecture system, foundational requirements must be in place

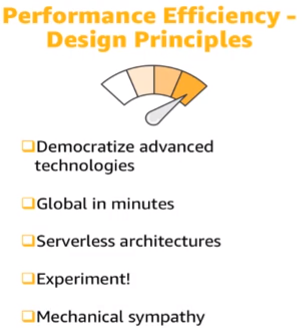


## Performance Efficiency Pillar



Monitoring in AWS – CloudWatch, Simple Queue service, Lambda

Trade off – Consistency Vs Ability in Time Vs Space



## Cost Optimization Pillar



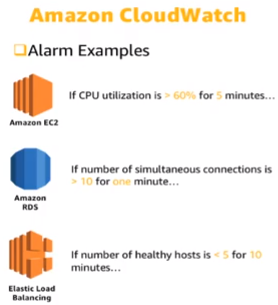


## Operational Excellence Pillar



# Reference Architecture – Fault Tolerance & High Availability



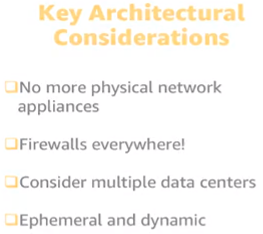




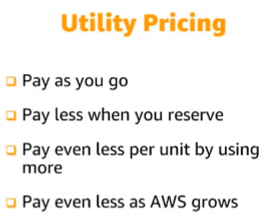
# Reference Architecture – Web Hosting







# Pricing & Support



EC2 instances – Can save up to 75% on reserved capacities when compared to On-demand capacity

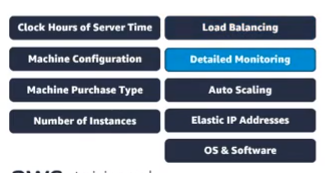


AURI payment – Maximum discount

S3, EC2 – More you use, less you pay – Tiering pricing model.

Data Transfer IN is free







# AWS Total Cost Ownership (TCO) Calculator

# AWS Support

Support Plans: Basic, Developer, Business, Enterprise

# **S3**

Versioning – MFA Delete can be used for having another layer of security – To Delete versioning settings

Versioning can only be suspended, after enabling.

Versioning stores all versions of an object even if it is deleted.

For CrossRegionReplication-> Versioning enabled->Must

Only new objects/objects that are changed will be replicated

After replication: If a version 2 file is deleted and reverted to Version 1 in source, this is not reflected in the destination. Destination still has version 2. We must go and delete the version 2 from destination to have the files in sync across different regions.

Cross region replication can be used for: Crypto-currency, storing wallets

## Lifecycle Management, S3-IA & Glacier:

Can work with

Can be applied to Current and Previous versions

Reduce storage cost – Use LifeCycleManagement Rules.

# CloudFront

**CDN-Content Delivery Network**

Edge Location: Content will be cached (50 Edge locations approx. around the world)

Origin: S3 bucket/EC2 instance/ ELB/Route53

Distribution: Name given to CDN which is a collection of Edge locations

* Web Distribution
* RTMP – Media Streaming

Origin can be a non-AWS server too

Edge location has both Read/Write

TTL (Time To Live) – Object Cached for the life of TTL

Clearing cached objects will be charged

# Creating CDN

A distribution can have multiple origin paths

An origin path can be an S3 bucket for e.g.

Possible to restrict viewer access with Signed URLs/signed cookies

# S3 – Security & Encryption

## Secure using:

* Bucket policies
* Access Control lists

## Encryption

* In Transit
  + SSL/TLS (Https)
* At Rest
  + Server side encryption
    - S3 Managed keys – SSE-S3
    - AWS Key Management Service, Managed Keys – SSE-KMS (Audit Trail)
    - Server side encryption with Customer Provided Keys – SSE-C
  + Client Side Encryption

# Storage Gateway

Connects On-premises software appliance with cloud based storage

* File Gateway (NFS) – Store Flat files in S3
* Volume Gateways (iSCSI block protocol) – Block based storage
  + Stored Volumes – Entire dataset stored on site and asynchronously backed up to S3
  + Cached Volumes – most frequently accessed data is cached in site
* Tape Gateway (Virtual Tape Library) – Backup & Archiving solution – Send to S3 /Glacier

# Snowball

* Snowball
* Snowball Edge
* Snowmobile