

# AWS Cloud Practitioner

Difficulty level: Moderate to difficult

## \* Content Outline

- > Cloud Concepts (28%)
- Security 24%
- Technology 36%
- > Billing & Pricing (24%)

## \* Exam

65 questions 90 mins MCQ (1 of 4 or 2 of 25)

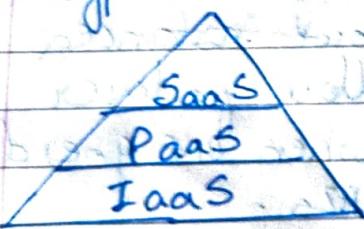
**Hint:** It's 2 of 5 or 3 of 6 many a times.

## Cloud Concepts

### \* 6 Benefits

- Pay On-Demand • Economic Scale Benefit
- Stop guessing capacity • Speed & Agility
- No maintaining data center • go global in minutes

## \* Types



e.g. Gmail, MS office

e.g. Heroku, Node.js

e.g. AWS, Oracle

## \* Deployment Models

Cloud → usually → startup

Hybrid → used → banks, legacy

In-Premise → by → governments, hospitals

## \* Global Infrastructure

~~Regions~~: Physical location with ~~more~~ multiple AZ

~~Availability Zones~~: One or more discrete data centres

~~Edge~~

Edge Location: datacenter owned by AWS or trusted partner

- ~~Notes~~ { most
  - Each region has at least 2 AZ
  - US-EAST is largest region
  - New service usually becomes available first in US-EAST
  - Not all services are available in all regions
  - US-EAST-1 is the region where we use all our billing info.
}
- AZ { most
  - AZs are represented by a Region code followed by an alphabet eg us-east-1a
  - Multi-AZ distributing our instances across multiple AZs allow failover config for handling req when one goes down
  - 10ms latency b/w AZs
}
- EL { most
  - EL servers requests for Cloud Front or RS3. Request to these services will be routed to nearest EL automatically
  - S3 Transfer Acceleration traffic & API gateway also uses the AWS Edge Network.
  - This allows low latency irrespective of geographic location.
  - Get our upload data fast to AWS.
}

## \* Gov Cloud

- Allows to host sensitive controlled Unclassified Information & other regulated work load.
- Only operated by US employees who are US citizens on US soil.
- Only accessible to US entities & root account holder who pass a screening process.
- Can be used by company in business with govt.

## \* Basic Services

### E C2

- Server instances, can choose from processors, OS, etc. Can be accessed using SSH, SSM (Needs IAM) or UI.
- SSM logs the session by default.
- You can also create an image of a running or a stopped instance. (AMI → Amazon Machine Images)
- Auto scaling group can be created using AMIs.
- Auto scaling group automatically replace unhealthy instances. If ASG is deleted, all of its instances terminated.

## \* Elastic Load Balance (ELB)

- Types
- Application LB
  - Network LB
  - Classic LB

ELB gives a DNS name, we need to direct our traffic there.

## \* S3

- S3 doesn't require a region but the bucket does.
- Bucket name is globally unique.

## \* CloudFront

- Used as CDN (Content Distribution Network)
- Takes copies static content to many edge locations.
- Needs a S3 bucket.
- We have similar DNS names as ELB here.

## \* RDS

## \* Lambda

- Can run for up to 15 mins but are usually run for seconds.
- These are just scripts, triggered by other services.

## EC2 Pricing Model.

- \* On demand (least commitment)
    - The low cost & flexibility
    - only pay per hour
    - short term, spiky, unpredictable workload
    - can not be interrupted
    - for first time apps.
  - \* Reserved Instance (RI) upto 75% off (Best long term)
    - steady state or predictable usage
    - commit to EC2 over a 1 or 3 year term
    - can resell unused RI at Reserved Instance Market
    - Saving depends on term, offering class & payment options.
- Offering class
- Standard → upto 75% discount compared to on-demand cannot change AZ attribute
  - Convertible → upto 54% discount allows to change to a larger instance
  - Scheduled → reserve an instance for specific time

Term → 1 or 3 years contract.  
↑ term ↑ saving.

Payment option → All upfront, partial upfront, no upfront  
↑ upfront ↑ saving.

RIs can be shared b/w multiple accounts within an org.

- \* Spot Instances upto 90%. Biggest saving
  - ~~regular~~<sup>wes</sup> spare computing capacity
  - flexible start & end times
  - can handle interruption (server randomly stopping & starting)
  - for non-critical bg jobs
  - Termination condition
    - instance can be terminated by AWS anytime (if an on-demand customer uses it)
    - if AWS terminates we don't get charged for a partial hour of usage
    - If we terminate we pay for hours from
- \* Dedicated Host Instances Most Expensive
  - dedicated servers
  - can be on-demand or reserved (upto 70% off)
  - when you need a guarantee of isolated hardware (enterprise requirement)

# Billing & Pricing

## 7 Free Services

- Imp for Exam
- 1 IAM - Identity Access Management
  - 2 Amazon VPC
  - 3 Auto Scaling
  - 4 CloudFormation
  - 5 Elastic Beanstalk
  - 6 Opsworks
  - 7 Amplify
  - 8 AppSync
  - 9 CodeStar
  - 10 Organizations & Consolidated Billing
  - 11 AWS Cost Explorer
- These services (3 to 9) are free however they can provision AWS services that costs money

## 8 Support Plans

Basic 0 \$ USD	Developer 20 \$ USD	Business 100 \$	Enterprise 1500 \$
Email support only for billing & account	Tech support via Email No third party support	Tech support via Email Tech support via chat, phone 24/7	< 24 hrs reply. < 12 hrs
	General System	Guidance Impaired	< 24 hrs < 4 hrs
		Pocel System Impaired Pocel System DOWN!	< 1 hr
<b>7 Trusted Advisor Check</b>			Business critical system down mins Personal Concierge T+M - Technical Account Manager
<b>All Trusted Advisor Check</b>			

## \* AWS Marketplace

Products can be offered as

- AMIs
- AWS CloudFormation templates
- SaaS
- Web ACL
- AWS WAF rules

## \* We can keep track of the offering we use at AWS Marketplace Subscription

## \* AWS Trusted Advisor

- Advises you on security, saving money, performance, service limits & fault tolerance.
- Think of it as an automatic checklist for best practices on AWS.
- We can see it at AWS Trusted Advisor Dashboard (about 101 checks)

## \* Consolidated Billing

- Offered at no additional cost.
- Master acc pays the bill for all member accounts.
- Use! cost explorer to visualize the billing feature is turned on by default when using AWS Organizations & have multiple member account.
- Cost Explorer can be used to visualize cost.

• Volume Discount - AWS has volume discount for many services. The more we use the cheaper the service becomes thus consolidated billing helps as many user become single user while billing.

#### \* AWS Budgets

- Think of it as billing alarm on steroids.
- Gives the ability to setup alerts if you exceed or are approaching your defined budget.
- Create cost, usage or reservation budget.
- Monthly, quarterly or yearly levels with customizable start/end dates.
- Supports ECS, RDS, Redshift & Elasticache reservations
- Manage via AWS Budget Dashboard or Budget API
- Email or chatbot.

#### \* TCO Calculator

- Total Cost Ownership.
- Used to estimate how much you would save moving to AWS from on-premise.
- Approximation purpose only.
- Steps
  - Describe your environment.
  - View 3 Year Summary of Cost Comparisons
  - Download a full detailed report.

## \* AWS Landing Zone

- Helps enterprise quickly set up a secure AWS multi-account.
- Provides baseline environment
- Does via AVM (AWS Account Vending Machine)
- Login using SSO.

## \* Resource Groups & Tagging

- Tags are words/phrases that act as metadata for organizing AWS resources.
- Resource groups are a collection of resources that share one or more tag.
- They help in monitoring resources that a project uses.
- Can display detail based on
  - Metric / Alarms / Config Settings

## \* AWS Quick Starts

- Prebuilt templates by AWS/AWS Partners to help deploy popular stacks on AWS.
- 3 parts:
  1. A ref arch for deployment
  2. AWS CloudFormation template that automate & configure deployment.
  3. A deployment guide explaining the arch & implementation in detail.
- Usually take < 1 hr

## \* AWS Cost & Usage Report

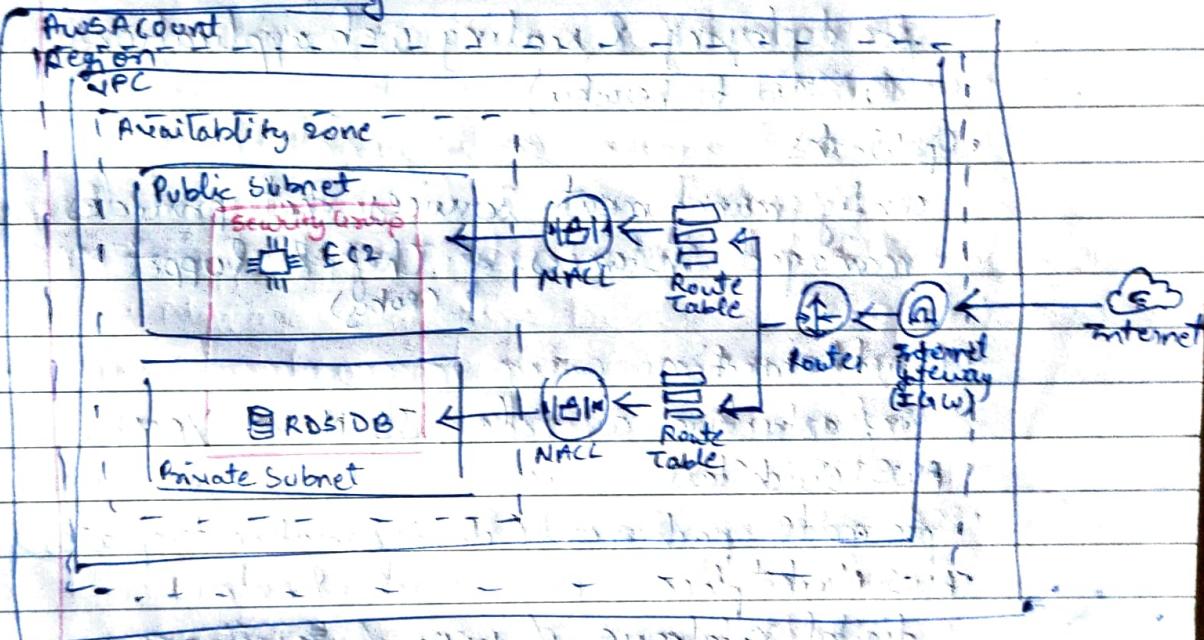
- Generate a detailed spreadsheet of AWS costs.
- Places report into S3
- Use Athena to turn report into queryable DB.
- Use QuickSight to visualize the data as graphs.

# Technology Overview

## \* Organization & Accounts

- Organization Units are group of AWS Accounts, can contain other organizational units.
- Service control policies gives control over the allowed permissions

## \* AWS Networking



- NACL provides firewall at subnet level.
- Security group provides firewall at instance level.
- VPC → logically isolated section of AWS where we can launch services.

## \* DB Services

- DynamoDB - NoSQL key/value (similar to cassandra)
- DocumentDB - NoSQL Document DB, that is MongoDB compatible
- RDS - supports multiple engines
  - Aurora is a fully managed RDS & we can run MySQL & Postgres. Has better performance (5x & 3x respectively). It runs 6 copies of DB across 3 AZ. Highly available & durable.

- Aurora Serverless - only runs when needed like a lambda. (less expensive)
- Neptune - Managed graph DB
- Redshift - columnar database, petabyte warehouse ( $1000\text{ TB} = 1\text{ PB}$ )
- ElastiCache - Redis or Memcached database.

## \* Provisioning

- Elastic Beanstalk - for deploying & scaling web applications (similar to heroku)
- OpsWorks - config management services that provides managed instances of Chef & Puppet (Ruby)
- CloudFormation - infrastructure as code, JSON or YAML
- AWS QuickStart - pre-made packages (CloudFormation templates)
- AWS Marketplace - digital catalogue of thousands of software.

## \* Computing Services

- EC2 (other compute services use EC2 under the hood)
- ECS - Elastic Container Service
  - Docker as Service, container orchestration service, pay for EC2 instances
- Fargate
  - Microservice where you don't think about infrastructure. Pay per task.
  - Evolution of ECS

- EKS

- Kubernetes as a Service

- Lambda

- serverless functions . only pay for compute time

- Elastic Beanstalk

- orchestrates various AWS services like , EC2 , S3 , SNS , CloudWatch , autoscaling , ELB , RDS etc.

- AWS Batch

- plans , schedules , executes batch computing workloads across the full range of AWS services & features.

## \* Storage Options

- S3 Glacier - low cost storage for archiving & long-term backup

- Storage Gateway - hybrid cloud storage with local caching

- file Gateway / Volume / Tape

- EBS - Elastic Block Storage

- hard drive in the cloud you attach to EC2

- SSD , 20GB SSD , Throughput HDD , Cold HDD .

- EFS - Elastic File Storage

- file storage mountable to multiple EC2 simultaneously

- Snowball - physically migrate lots of data via a computer suitcase (50-80TB)

- Snowball Edge - better version - 100TB

- Snowmobile - shipping container , pulled by semi-trailer truck - 100PB .

## \* Business Centric Services

- Amazon Connect

call center

- WorkSpaces

virtual remote desktop

- WorkDocs

content creation & collaboration service

- Chime

platform for online meeting & video conferencing

- WorkMail

managed business mails, contacts & calendar service with support for existing desktop & mobile email client application (ZMAP).

- Pinpoint

marketing campaign management system you can use for sending targeted email, SMS, push notification & voice message.

- SES - Simple Email Service

send marketing, notification & email.

- ClickBright

Business Intelligence (BI) service.

(similar to power BI).

SNS Note: SNS only sends plain text email but SES can have HTML components.

~~Ent~~

## \* Enterprise Integration

- Direct Connect
  - dedicated Gigabit network from your premise to AWS
- VPN
  - secure connection to AWS
  - Site-to-Site - connecting on-premise to AWS
  - Client - connecting a client (a laptop) to AWS network

## \* Storage Gateway

- hybrid storage service that enables your on-premises applications to use AWS cloud storage.

## \* Active Directory

- service for Microsoft AD also known as AWS Managed Microsoft AD.
- enables your directory-aware workloads & AWS resources to use managed Active Directory in AWS.

## \* Logging Service

### \* CloudTrail

- logs all API calls b/w AWS services  
(SDK/CLI)

### \* CloudWatch

- collection of services (usually referred to CloudWatch Logs)
- CloudWatch Logs - perf log of AWS service
  - Metrics - time-ordered set of data points
  - Events - triggers an event based on a condition
  - Alarm - triggers notification based on metrics
  - Dashboard - create visualizations based on metrics

## \* Know your initialisms

- IAM • RDS • TAM • EBS • MKS )
- S3 • VPC • ELB • EFS • IoT )
- SWF • VPN • ALB • EMR • RI )
- SNS • CFN • NLB • EB )
- SQS • WAF • EC2 • ES )
- SES • MQ • ECS • EKS )
- SSM • ASG • ECR • EMS )

## Security

### \* Shared Responsibility Model

- Customer are responsible for security in the cloud (data, config, etc)
- AWS is responsible for the cloud. (hardware, infra)

### \* AWS Compliance Program

- Set of internal policies to comply with laws & uphold reputation.

### \* AWS Artifact

- no cost self service portal for on-demand access to AWS's compliance report.
- only open the pdf (artifact) using Adobe Acrobat.

### \* Amazon Inspector

- hardening is an act of eliminating as many security risks as possible.
- Inspector checks if EC2 is hardened.
- steps. (can perform both Host & Network Assessments)
  - Install AWS agent on EC2
  - Run an assessment for your assessment target
  - Review your findings & remediate security issues

### \* AWS WAF (Web Application Firewall)

- write your own rules to allow/Deny traffic based on the contents of HTTP request.
- or buy a ruleset from marketplace which usually covers AWS Top 10 threats.
- WAF can be attached to either CloudFront or Application Load Balancer.

## \* AWS Shield

- managed DDoS protection service.
- no charge, already turned on when you <sup>(Shield standard)</sup>
- route traffic through Route53, CloudFront.
- Protects against layer 3, 4 & 7 attacks
- Shield Advanced costs \$8000/year <sup>[Network] [Transport] [Application]</sup>  
only available on R53, CloudFront, ELB, Global Accelerator, Elastic IP.

## \* Penetration Testing (PenTesting)

- for some services it is allowed for some we need to request for permission.

## \* Guard Duty

- threat detection service that continuously monitors for suspicious activity & unauthorized behaviour.
- uses ML to analyze following logs: CloudTrail, VPC Flow, DNS.

## \* Key Management Service (KMS)

- multi-tenant HSM (Hardware Security Model)
- uses Envelope Encryption.

## \* Macie

- fully managed service that continuously monitors S3 data access activity & alerts when it detects any risk.
- it has a variety of alerts.
- it can also identify most risked user.

- \* Security Groups & NACL (Network Access Control List)
  - firewall at instance level
  - implicitly denies all traffic, you create allow rules.
  - firewall at subnet level
  - you create allow & deny rules.

e.g. Allow an EC2 access on port 22 for ssh

e.g. Block specific IP address for known abuse.

### \* AWS VPN

- lets you establish a secure & private tunnel from your network or device to the AWS global network.

## Variation Study

### \* Cloud Formation

### \* Cloud Services

- CloudFormation - infra as code (SSON, YML)
- CloudTrail - logs api calls b/w AWS services
- CloudFront - content distribution
- CloudWatch - collection of services
  - u - logs / Metrics / Events / Alarms / Dashboard

### \* Cloud Search - search engine

### \* Connect Services

- Direct Connect - dedicate fiber optic to AWS
- Amazon Connect - call center service
- Media Connect - converts videos to diff video types

### \* Elastic Transcoder

- old way
- transcodes videos to streaming formats

### Media Converter

- new way
- transcodes videos to streaming formats
- overlay images
- insert video clips
- extracts captions data
- Robust UI

## \* SNS

- pass alongs ~~notifi~~ messages  
eg. PubSub
- sends notifications to subscribers of topics via multiple protocol  
eg. HTTP, Email (plaintext)  
SNS, SMS

## SQS

- Queue Up Messages,  
Guaranteed Delivery
- places messages into a queue. Applications pull queue using AWS SDK.

## \* Inspector vs Trusted Advisor vs Artifact (All services) (Get security report for AWS)

### \* ALB

- Layer 7 req
- HTTP & HTTPS

- routing rules, more usability from one LB

- can attach waf

- can attach Amazon Certificate Manager (ACM) SSL certificate.

### NLB

- Layer 4
- TCP & TLS where extreme perf req

- capable of handling millions of requests per sec while maintaining ultra-low-latency

- optimized for sudden & volatile traffic patterns while using a single static IP address per AZ

### Classic (OLD)

- Layer 4 & 7
- intended for applications that were built within E2 - Classic network

- doesn't use target groups.

MCQsInfo as  
↑ codeElastic | OpsWorks | CFN | DIY / OnDemand  
Beanstalk

Convenience → Control

AWS Quick Start reference deployments provide simple / reference CFN templates.

- \* IAM → anything technical  
conierge → helps in account & billing
- \* To keep EBS data safe
  - ① ensure that EBS data is encrypted at rest
  - ② create EBS snapshots.

- \* S3 Standard → Usual needs

Intelligent Tiering → unpredictable access

Standard IA → infrequent access

One Zone IA → \_\_\_\_\_, put data only in 1 AZ rather than 3

Glacier Instant Retrieval → Archive but quick (milliseconds)

Glacier Flexible Retrieval → \_\_\_\_\_ &amp; time → mins to hrs

Glacier Deep Archive → Archive &amp; time → hours

S3 Outposts → On premise storage

- \* Shared controls →

eg. Patch Management • AWS: patching hosts, customer: &amp; fixing infra patchings, application

eg. Config Management →

&amp; Awareness &amp; Training

\* Infra Event Management provides the company with architectural & scaling guidance.

\* AWS Health Dashboard provides

① Personalized view of AWS service health

② Detail troubleshooting guidance to address AWS events impacting your resources.

\* IAM user provides access keys to interact with AWS services using AWS CLI, for ~~API~~ <sup>some long term & secret token</sup> password

\* AWS MFA → multi factor auth

- ②
- \* Instance type & load balancing can effect EC2 cost.
  - \* AWS Transfer Acceleration uses CloudFront's ELBs to transfer files to S3 with ↑ upload speed.
  - \* Service limit: can use Trusted Advisor to monitor service limit, can contact AWS support to increase the limit.
  - \* Hybrid cloud connectivity options : VPN & Direct Connect.
  - \* AWS CloudTrail & Config are change management tools.
  - \* RDS uses EBS primarily.
  - \* Elastic Cache → In-memory data caching for read-heavy applications.
  - \* Customers fully inherit Physical & Environmental Control.
  - \* Right-sizing before & after data migration saves cost.

- ② • To set SSL → IAM or ACM  
IAM works in all regions, but it's good to use IAM only where ACM doesn't work.
- AWS Transit Gateway is used to simplify communication between VPCs.
- AWS provides AWS Professional Services & AWS partners as part of Migration Acceleration Platform (MAP).
- AWS Service Control Policies (SCPs) can be used to what services & actions are allowed in each individual account.
- S3 & Lambda scale automatically.