AWS Cloud Practitioner

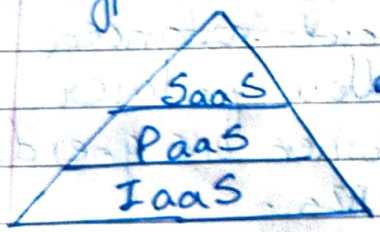
* **Content Outline**
  - Cloud Concept 28%
  - Security 24%
  - Technology 36%
  - Billing & Pricing 12%

* **Exam**
  65 Question 90 mins MCQ (1 of 4 or ~~2 of 5~~)
  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 maintaing data centers
  - Go global in minutes

* Types



eg. Gmail, Ms office
eg. Heroku
Eg. AWS, GCP

* Deployment Models
  - Cloud → Usually → startup
  - Hybrid → used → banks, legacy
  - On-Premise → by → governments, hospitals etc.

* Global Infrastructure

Regions (22) : Physical location with multiple AZ

Availability Zones (AZ) : One or more discrete data centres

Edge (69)

Edge Location : datacenter owned by AWS or trusted partner

Region
- 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 region
- US-EAST-1 is the region where we see all our billing info.

AZ
- 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
- EL serves requests for Cloud Front or S3. Request to these services will be routed to nearest EL automatically
- S3 Transfer Acceleration traffic & API Gateway also used the AWS Edge Network.
- This allows low latency irrespective of geographic location.
- Get or 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 gov.

* Basic Services.

* EC2
  - Server instance, 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 instance terminated.

* Elastic Load Blance (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.

* Cloud front
  - Used as CDN (Content Distribution Network)
  - ~~Takes~~ Copies static content to many edge locations.
  - Needs a S3 bucket.
  - We have similar DNS name 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 place
  - Saving depends on term, offering class & payment options.

Offering class
- Standard → upto 75% discount compared to on demand cannot change RI 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
  - ~~request~~ use 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 ran

* 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

* Free Services

Imp for Exam

1. IAM - Identity Access Management
2. Amazon VPC
3. Auto Scaling
4. Cloud Formation
5. Elastic Beanstalk
6. Ops works
7. Amplify
8. AppSync
9. CodeStar

These services (3 to 9) are free however they can provision AWS services that costs money

10. Organizations & Consolidated Billing
11. AWS Cost Explorer

* Support Plans

Basic	Developer	Business	Enterprise
0$ USD	20 $ USD	100 $	15000$
Email support only for billing & account	Tech support via Email		~24 hrs until reply.
	No third party support	Tech support 24/7	via chat, phone
	General System Guidance Impaired		< 24 hrs < 12 hrs
		Prod System Impaired < 4 hrs Prod System DOWN! < 1 hr	
			Business critical < 15 system down mins
			Personal Concierge TAM - Technical Account Manager
7 Trusted Advisor Check			All Trusted Advisor Check

* AWS Marketplace
Products can be offered as
- AMIs
- AWS Cloud Formation 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, performace, 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 account
- Use cost explorer to visualize the billing
- Feautre is turned on by defaut 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 became 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 EC2, 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 with 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 use.
  - 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 Cloud Formation template that automate & configure deployment.
  3. A deployment guide explaining the arch & implementation in detail.
- Usually take < 1 hr

AWS Cost & Usage Report

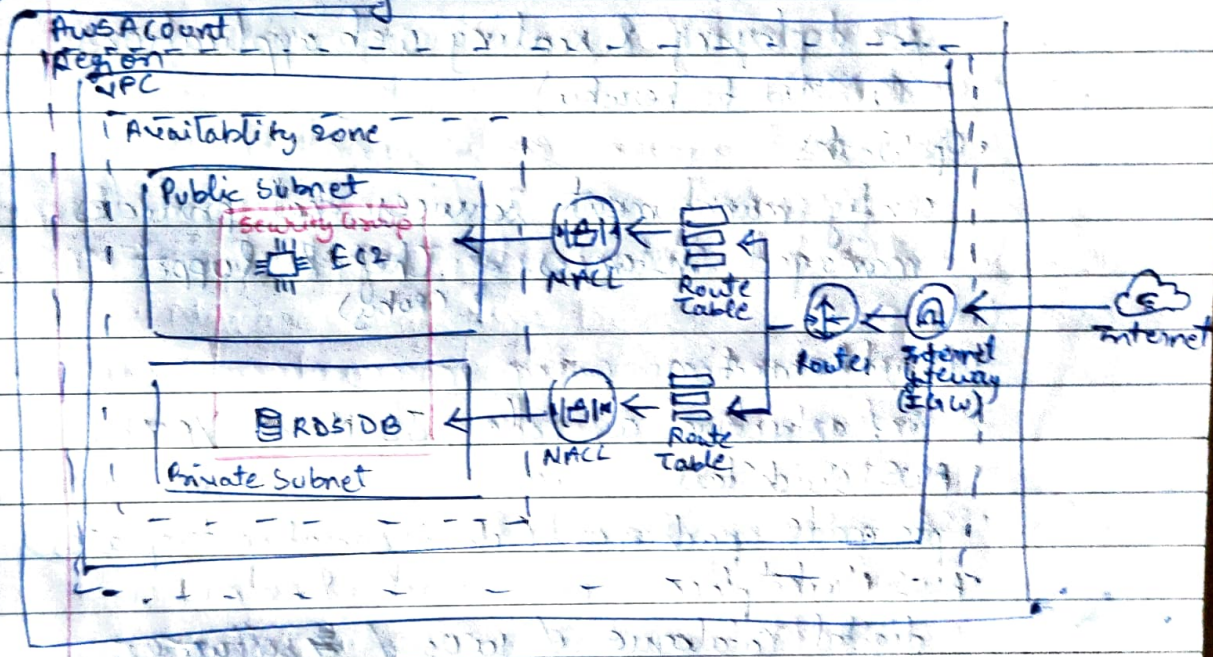
- Generate a detailed spreadsheet of AWS costs.
- Places report into S3
- Use athena to turn report into queryable DB.
- Use QuickSight to visualize the data as graphs.

Technology Overview

★ Organization & Accounts

- Organization Units are group of AWS Accounts, can contain other organizational units.
- Service control policies gives control and 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 manage RDS & we can run MySql & Postgres. Has better performance (5x & 3x respectively) & 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 TB = 1 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)
  - Cloud Formation
    infrastructure as code, JSON or YAML.
  - AWS QuickStart
    pre-made packages (cloud formation templates)
  - AWS Marketplace
    digital catalogue of 1000s of softwares.

* 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.
    (revolution 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

- S3
  - S3 Glacier - low cost storage for archiving & long-term backup
  - Storage Gateway - hybrid cloud storage with local caching
    - File Gateway / Volume —u— / Tape —u—
- EBS - Elastic Block Storage
  hard drive in the cloud you attach to EC2
  SSD, IOPS SSD, Throughput HHD, Cold HHD.
- EFS - Elastic File Storage
  file storage mountable to multiple EC2 simultaneously
- Snowball - physically migrate lots of data via a computer suitcase (50-80 TB)
  - Snowball Edge - better version - 100 TB
  - Snowmobile - shipping container, pulled by semi-trailer truck - 100 PB.

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 & calender service with support for existing desktop & mobile email client application (IMAP).
- Pinpoint
  marketing campaign management system you can use for sending targated email, SMS, push notification & voice message.
- SES - Simple Email Service
  send marketing, notification & email.
- QuickSight
  Business Intelligense (BI) service.
  (similar to power BI).

Note: SMS 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 (SDK/CLI) b/w AWS services
  - CloudWatch
    - collection of services (usually referred to CloudWatch Logs)
    - CloudWatch Logs - perf log of AWS service
    - — " — Metrics - time-ordered set of data points
    - — " — Events - trigger on event based on a condition
    - — " — Alarm - triggers notification based on metrics
    - — " — DashBoard - create visualizations based on metrics

* Know you initialisms

• IAM	• RDS	• TAM	• EBS	• MKS
• S3	• VPC	• ELB	• EFS	• IoT
• SWF	• VPN	• ALB	• EMR	• RI
• SMS	• 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 ——— " ——— of 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 & remidiate 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 AWASP 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 (Shield Standard)
  - route traffic through Route53, CloudFront.
  - Protects against layer 3, 4 & 7 attacks
    (Network) (Transport) (Application)
  - Shield Advanced costs $3000/year
    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	• firewall at subnet level
• implicitly denies all traffic, you create allow rules.	• you create allow & deny rules.
eg Allow an EC2 access on port 22 for SSH	eg. 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.

Page No.
Date

Variation Study :

~~Cloud Formation~~

* Cloud* Services

- Cloud Formation - infra as code (JSON, YML)
- Cloud Trail - logs api calls b/w aws services
- Cloud Front - content distribution
- Cloud Watch - collection of services
  — u— logs / Metrics / Events / Alarms / Dashboard.
- Cloud Search - serch 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	SQS
• pass alongs ~~notifi~~ messages eg. PubSub • sends notifications to subscribers of topics w/ multiple protocol eg. HTTP, Email (plaintext) Sqs, SMS	• Queue Up Messages, Guaranteed Delivery • places messages into a queue. Applications pull queue using AWS SDK.

★★ Inspector (EC2) vs Trusted Advisor (All services) vs Artifact (Get security report for AWS)

ALB	NLB	Classic (OLD)
• Layer 7 req • HTTP & HTTPS	• Layer 4 • TCP & TLS where extreme perf req	• Layer 4 & 7 • intended for applic-ations that were built within EC2-Classic network.
• Routing Rules, more usability from one LB	• capable of handling millions of requests per sec while maintain-ing ultra-low-latency	• doesn't use target groups.
• can attach WAF	• optimized for sudden & volatile traffic patterns while using a single static IP address per AZ	

• Can attach Amazon Certification Manager (ACM) SSL Certificate.

MCQs :

① ★ Elastic Beanstalk | OpsWorks | CFN (Infra as code) | DIY / On Demand

Convenience ←——————————→ Control

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

★ TAM → anything technical
Concierge → 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 Retrival → Archive but quick (millisecond)
Glacier Flexible Retrival → —— " — & time → mins to hrs
Glacier Deep Archive → Archive & retrival time → hours
S3 Outposts → On premise storage

★ Shared controls →
eg. Patch Management · AWS: patching hosts, Customer: & fixing infra patching os, application
eg. Config Management →
& Awareness & Training

Page No.
Date

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

* AWS Health Dashboard provides
  ① Personalized view of AWS service health
  ② Detail trouble shooting guidance to address AWS events impacting your resources.

* IAM user provide & access keys → are long term & secret token is short term to interact with AWS services using AWS CLI, for GUI → ID & password

* AWS MFA → multi factor auth

Page No.
Date

(2) * Instance type & load balancing can effect EC2 cost.

* AWS Transfer Acceleration uses ~~ELs~~ CloudFront's EL's 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 ~~caching~~ caching for read-heavy applications.

* Customers fully inherit Physical & Environmental Control.

* Right-sizing before & after data migration saves cost.

- 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.