AWS CLOUD PRACTIOTIONER

WHAT IS CLOUD COMPUTING?

- Traditional IT setup. (problems)
- on-demand, pay as you go, instant
- public, private and hybrid cloud.
- 5 characteristics.
  1. on demand self service.
  2. Broad network access.
  3. Multi-tenancy and resource pooling.
  4. Rapid elasticity and scalability.
  5. Measured service / pay-as-you-go.
- Six Advantages.
  1. Opex over capex.
  2. massive economies of scale.
  3. No need to guess capacity.
  4. Increased speed and agility.
  5. No money spend on data centers.
  6. Go global in minutes.
- IAAS, PAAS and SAAS.

→ application]
→ data] PAAS]
→ runtime] – IAAS.

→ middleware
→ O/S
→ virtualization
→ storage
→ servers/hardware.
→ networking

- pricing models -
  - compute
  - storage
  - data out of the cloud.
- AWS Global Infrastructure.
  - 30 regions - cluster of data centers.
  - 96 AZ.
  - 2-6 AZ in each region.
  - 216 points of presence
    - 205 edge locations.
    - 11 regional caches.
- Global and Local services.
- AWS Shared Responsibility.
- AWS Acceptable Use Policy (AUP)

IDENTITY AND ACCESS MANAGEMENT (IAM)

- Global service.
- users, groups, permissions, policies.
  least privilege principle policy.
- IAM policy inheritance
- MFA for extra security.
- AWS management console, CLI, SDK.

- IAM Roles for Services:
  - EC2 instance roles.
  - Lambda function roles.
  - Roles for Cloudformation.

  ] Assign policies to roles.

- IAM security tools
  - IAM Credentials Report (account-level)
  - IAM Access Advisor (user-level)

ELASTIC COMPUTE CLOUD (EC2)

- OS
- Compute - CPU & RAM
- Storage
  - EBS, EFS and EC2 instance store
- Firewall rules.
- EC2 user data - startup script.

- EC2 Instance Types:
  1. General Purpose.
  2. Compute optimized.
  3. memory optimized.
  4. storage optimized.

- Security Group.
  - for SSH, HTTP access.

  → never enter access keys within EC2 instance connect, use IAM role instead.

- EC2 instance connect within browser

- EC2 Purchasing options:
  1. On-demand instances.
  2. Reserved (1 & 3 years)
  3. Savings Plan.
  4. Spot instances. → cheapest / cost effective.
  5. Dedicated Hosts. → most expensive.
  6. Dedicated instances.
  7. Capacity Reservation.

EC2 INSTANCE STORAGE

- EBS Volume
  - Network drive
  - persist data.
  - one instance at a time
  - bound to specific AZ → create snapshots to move to different AZ.
- EBS Snapshots.
- Amazon Machine Image (AMI)
  - bound to region.
- EC2 Image Builder.
- EC2 Instance Store
  - ephemeral.
  - high performance.
- Elastic File System (EFS)
  - can be mounted to 100s of EC2.
  - EFS works multi-AZ.
  - highly available, scalable and expensive.
- Amazon FSx.
  - for windows file server
  - for Lustre (Linux cluster)
    - ↳ HPC.
    - ⇒ ML, Video etc.

ELASTIC LOAD BALANCING & AUTO SCALING GROUPS.

- Vertical Scalability
  - increase size of an instance
  - non-distributed systems.

- Horizontal
  - Elastic / increase # of instances.
  - High Availability
  - Distributed systems
    - ASGs / Load Balancer.

- HA can be achieved by:-
  - ASG with multi AZ
  - Load Balancer with multi AZ.

- Scalability v/s Elasticity v/s Agility.

- Load Balancing.
  - manage traffic

1. Application Load Balancer → HTTP (HTTPS) gRPC
   → Static IPs.
   → Layer 7.

2. Network Load Balancer → TCP | UDP
   → Layer 4
   → high performance.
   → Elastic IP.

3. Gateway Load Balancer
   - Layer 3
     - Intrusion detection
     - GENEVE protocol.

- Auto Scaling Groups (ASGs).
  - scale in / out.
  - ensure min/max instance running.
  - automatically register new instances to load balancer.

-- Strategies:
  - Manual Scaling.
  - Dynamic
    - Simple - CPU based
    - Target tracking - CPU at 40%.
    - Scheduled. - known usage patterns.
    - Predictable - ML based.

AMAZON S3

- buckets at regional level.
- naming convention.

- S3 security.
  - User-based.
  - Resource-Based
    - bucket-policies.
    - object ACLs.
    - Bucket ACLs.

- Public Access - Bucket policy.
- User Access - IAM permissions.
- EC2 instance access - IAM roles.

- Cross-Account Access - Use Bucket Policy.

- Replication.
  - Cross-Region Replication (CRR)
  - Same-Region Replication (SRR)

- S3 Storage Classes.

1. General Purpose - 99.99% HA, low latency high throughput.
2. Infrequent Access.
   - Standard IA - 99.9% HA, backups
   - One-zone Infrequent Access → secondary backups → 99.5% HA.
3. Glacier Storage
   - archival/backup
   - Instant Retrieval - instant/min. 90 days
   - Flexible Retrieval - mins to hours. min 90 days.
   - Deep Archieve - 12 to 48 hours, min 180 days.

- AWS Snow Family.
  - Snowball Edge (TBs/PBs).
  - Snowcone (8TBs).
  - Snowmobile (1EB)
- AWS OpsHub.
- AWS Storage Gateway for hybrid cloud.

DATABASES

I) RDS - Relational Database Service.

P - PostgreSQL
O - oracle
M - MySQL
M - MariaDB
M - Microsoft SQL server
A - Aurora (AWS proprietary)

- Multi A2, Scaling, EBS storage, read replicas.

① Aurora.
- Postgresql and MySQL

Read-Replicas = Scale
Multi-AZ = Failover.

⇒ Amazon Elasticache
- Redis or memcached
- managed service.
- in-memory cache

] also NoSQL.

II) NoSQL

① DynamoDB.
- HA, 3AZ.
- NoSQL, serverless
- single-digit milliseconds latency.
- key/value database

- DAX accelerator of 10x more performance
- DAX only for DynamoDB whereas ElastiCache for other DBs.
- DynamoDB Global Tables - Active Active replication.

OTHERS:

1. Redshift - Postgres
   - OLAP, not OLTP
   - Columnar Storage
2. EMR - Hadoop
   - Big data.
3. Athena - serverless
   - Columnar Data
   - data stored in S3
4. Quicksight - BI tool
5. DocumentDB
   - MongoDB, for JSON data.
   - noSQL database
6. Neptune
   - Graph DB
   - HA - 3AZs.
7. QLDB
   - Quantum ledger DB.
   - HA, 3AZs.
   - no decentralization component
8. Amazon Manged Blockchain
   - Blockchain
   - Ethereum
   - has a decentralization component
9. Glue
   - managed ETL.
   - serverless.

⇒ Database Migration service (DMS)

- source DB to target DB.
- Homogeneous and Hetero.

OTHER SERVICES - ECS, LAMBDA, FARGATE, LIGHTSAIL.

(1) Docker
- containers
- DockerHub.
- Amazon ECR.

(2) ECS
- managed container service.
- must provision infra beforehand.

(3) Fargate
- serverless.
- launch docker containers.
- no need to provision infra beforehand

- ECR to register images for ECS or Fargate.

(4) Serverless
- function as a service.
- Lambda
- S3, DynamoDB, Fargate, Lambda, Athena, Glue.

- LAMBDA
  - functions for server management.
  - short execution
  - on-demand
  - scaling is automated.
  - Event driven
  - pricing on calls and duration.

⇒ Amazon API Gateway
- managed
- serverless
- Restful and websocket APIs.

(5) Batch
- fully managed batch processing. , no-time limit.
- will provision EC2 on its own

- Docker image and run on ECS.

ε Lambda v/s Batch

⑥ Lightsail
- simpler alternative to EC2, EBS... etc
- for people with little cloud experience.
- simple web apps, websites, dev/test environment.
- HA but no auto-scaling.

DEPLOYING AND MANAGING INFRASTRUCTURE AT SCALE.

① Cloudformation (AWS only)
- declarative templates. - JSON/YAML.
- Infrastructure as code.
- Easily estimate costs.
- Automated generation of diagrams.

② CDK
- Cloud infra in your own language.
- Python/Java etc.

③ Beanstalk (AWS only)
- developer centric view of deploying applications
- PAAS.
- managed service.
- health monitoring.

④ CodeDeploy (hybrid)
- hybrid service
- EC2 and on-premises servers.
- servers/instances must be provisioned beforehand.

⑤ CodeCommit.
- AWS product for Github.
- Code repository.

⑥ Code Build
- Compile, test, produces packages.
- works with CodeCommit to deploy your app.

(7) CodePipeline
- CI/CD like pipeline
- works with CodeCommit, CodeBuild & CodeDeploy.

(8) CodeArtifact.
- software depend on each other.
- maven, gradle, npm, yarn etc can work with.
- Artifact management system.

(9) CodeStar.
- Unified UI for (5) to (8)
- AWS Cloud9 for editing.

(10) AWS Cloud9
- IDE for code directly in the cloud.
- works with the browsers.

(11) AWS SSM (Systems Manager) (hybrid)
- manage EC2 & on prem systems at scale
- hybrid AWS service.
- patch automation

- Session Manager
  - without SSH access and keys, can use session manager
  - need to create the right IAM role.

(12) OpsWorks. (hybrid)
- = managed chef & puppet.
- alternative to AWS SSM.

AWS GLOBAL INFRASTRUCTURE

why?
- Global application - geographies / region / AZ.
- Decreased Latency.
- Disaster Recovery.
- Attack protection.

(1) Global DNS: Route 53.

- managed DNS.
  - simple routing policy
    - no health checks.
  - weighted routing policy.
    - load balancing.
  - Latency routing policy.
    - minimize latency
  - failover routing policy.
    - Disaster Recovery
    - Health checkup.

(2) Global CDN - Cloudfront.

- improves read performance, content is cached at the edge.
- Improves user experience.
- 216 Point of presence.
- DDoS protection.
- Origins :- S3 bucket, ALB, EC2, HTTP backend.
  - Great for static content that must be available everywhere.

(3) S3 Transfer Acceleration.

- Increase transfer speed.
  - good web app to check how much faster is S3 Tranfer.

(4) AWS Global Accelerator.

- improve availability and performance.
- 2 Anycast IP
- good for regions far from you.

(5) AWS Outposts.

- Physical racks by AWS to mimic cloud behaviour on your on-prem setup.
- Low latency, local data processing.

(6) AWS Wavelength.

- 5G networks, embed at edge for telecom.
- Ultra-low latency.
- Smart cities, connected vehicles etc. usecase.

(7) AWS Local Zones.

- Places AWS resources closer to end-user.
- Extend VPC to more location.

- eg:- create a Boston local zone.

(8) Global Application Architecture.

- Single Region, single AZ
- Single Region, Multi AZ.
- Multi-Region, Active-Passive.
- Multi-Region, Active-Active.

CLOUD INTEGRATIONS

- Synchronous
- Async / Event based. - queue.

(1) AWS Simple Queue Service (SQS)

- Producer send message to SQS.
- Consumer poll messages from SQS.
- oldest offering.
- fully managed, serverless.
- used to decouple applications.

(2) Kinesis:

- real time big data streaming.

(3) SNS (simple notification service)

- pub/sub
- event publishers.
- emails, sms & notif., http endpoints.

(4) Amazon MQ

- alternative to SQS & SNS.
- message broker service
- managed service for RabbitMQ and active mq
- MQ doesn't scale.
- mq runs on servers
- MQTT, AMQP, STOMP, WSS, Openwire.

CLOUD MONITORING

① Cloudwatch metrics
- EC2 - CPU utilization, no RAM
- EBS volumes.
- S3 buckets.
- billing.
- service limits
- custom limits.

⇒ Cloudwatch Alarms.
- Billing alarm only available in us-east-1.

⇒ Cloudwatch Logs
- EBS, ECS, Lambda, Cloudtrail, Route 53.
- EC2 can send logs to Cloudwatch.
- Need to install Cloudwatch logs agent on EC2.

② Event Bridge
- Cron jobs
- Event patterns

③ Cloud Trail
- governance, audit, compliance
- enabled by default.
- history of everything within your AWS account.
- can send the trail to Cloudwatch logs or S3.
- monitors SDK, CLI, console, IAM etc.

④ X-Ray
- Debugging in production.
- log analysis is hard.
- visual analysis using service graph.

⑤ Code Guru.
- automated code reviews, ML-powered.
- Reviewer and Profiler.

⑥ service Health Dashboard. & Personal Health Dashboard.

VPC & NETWORKING

① Virtual Private Cloud.

- Linked to a region.
- subnet allow you to partition your VPC
  - subnet associated with an AZ.
  - public subnet = internet accessible
  - private subnet = not openly accessible.
  - access to the internet & between subnets is by RouteTables.

- Internet Gateway will help VPC instances connect with the internet.
- Public Subnet have a route to the internet gateway
- NAT Gateway will allow instances in private Subnet to access the internet while remaining private.
- NAT Gateway is created in the public subnet.

② Network Security

① - NACL - stateless
- A firewall that controls traffic from and to subnet.
- NACL is on a subnet level. ALLOW & DENY rules.
- Rules only include IP addresses.

② Security Groups - stateful
- firewall for EC2 instance
- only ALLOW rules

③ VPC Flow Logs

- VPC, subnet, ENI
- monitor & troubleshoot.
- can integrate with S3 and Cloudwatch logs.
- VPC peering is not transitive

④ VPC Endpoints

- Connect access AWS services from private network.
- endpoints help in the above.

⑤ PrivateLink

- secure & seculable way to expose a service to 1000's of VPCs.
- alternative to VPC peering.
- requires network load balancer (service end) and ENI (customer end)

(6) Site to Site VPN and Direct Connect

- for hybrid cloud.
- connect on-prem data center to AWS VPC. - goes over the internet.
- Direct connect is a physical connection.
  - goes over private network. (1 month)
- Site-to-site VPN
  - On prem: must use a Customer Gateway (CGW)
  - AWS: must use a Virtual Private Gateway (VGW)

(7) AWS Client VPN

- allows your personal computer to connect to EC2 over a private IP.
- uses openVPN
- goes over public network

(8) Transit Gateway

- for peering 1000s of VPC & on-prem using a hub and spoke (star) connection.

SECURITY & COMPLIANCE

(1) AWS Shared Responsibility Management.

(2) DDoS Protection.

- AWS Shield Standard (free)
- " " Advanced (paid)
- AWS WAF - Web Application Firewall. (Layer 7)
- Cloudfront & Route 53.
- Ready to scale - AWS Auto Scaling.

(3) Penetration Testing.

(4) Encryption with KMS

- At rest: } encryption keys.
- In transit: }
- Key management service -> AWS manages.

- Cloud HSM (HSM is a physical device)
  - AWS provisions encryption hardware.
  - We manage it on our own.

- Customer Master Keys (CMK)
  - customer managed CMK
  - AWS managed CMK
  - AWS owned CMK
  - Cloud HSM keys.

(5) AWS Certificate Manager (ACM)
- SSL / TLS certificates.
- in-flight encryption for websites.
- Free public TLS certificates.

(6) AWS Secrets Manager
- Rotation of secrets every x days.
- Integration with Amazon RDS.

(7) AWS Artifact.
- on-demand access to AWS compliance documentation.
- SOC, PCI, third-party auditors.
- BAA, HIPAA
- used for internal audit and compliance.

(8) Guard Duty
- intelligent threat discovery using ML.
- Takes all logs as input
- Protects against cryptocurrency attacks.

(9) Inspector
- Automated security Assessments.
- For EC2, ECR, Lambda Functions.

(10) Config.
- Auditing and recording compliance of AWS resources.
- record config changes over time.

(11) Macie
- sensitive data check in AWS.
- Uses ML and pattern matching.

(12) AWS security Hub.

- Central security tool to manage security across several AWS accounts.
- Interactive dashboard.

(13) **Amazon Detective**
- used to find root cause of security issues.
- collects data from all logs.

(14) **AWS Abuse**
- Report suspected AWS resources used for abusive purposes.
- You can report any activity to AWS abuse team.

(15) **Root user privileges.**
- Account Owner.
- Do not use root user for everyday tasks.
- Change account settings, close your AWS account, change or cancel AWS support plan, register as seller in the Reserved instance marketplace } only root user can do this.

MACHINE LEARNING

(1) **Amazon Rekognition**
- Image / video
- Text
- face detection.
- Pathing / Person counting.

(2) **Transcribe**
- speech to text.
- Automatically remove PII using Redaction.
- multi-lingual.

(3) **Polly**
- Text to speech.
- create applications that talk.

(4) **Translate**
- language translation

(5) **Lex & Connect**
- lex = powers Amazon Alexa.
- ASR

- NLU, intents.
- chatbots.
- Connect = virtual contact center
  - can integrate with CRM

⑥ **Comprehend**
- NLP
- serverless
- text = language, sentiment, tokenization, topic etc.

⑦ **Sagemaker**
- Machine learning., build models
- end to end ML

⑧ **Forecast**
- used for time series forecasting.
- upload data to S3 and forecast service will read it.

⑨ **Kendra.**
- Document search service by ML.
- Creates its own knowledge index for search.

⑩ **Personalize**
- for real-time personalized recommendation.
- data stored in S3.

⑪ **Textract**
- OCR tool from Amazon
- Images, PDF etc.

ACCOUNT MANAGEMENT, BILLING & SUPPORT

① **AWS Organizations.**
- Global service.
- manage multiple AWS accounts.
- Cost benefits.
- API available for creating sandbox accounts.
- Restrict account privileges using SCP (Service Control Policies)

- Multi Account Strategies.

- dev / test / prod.
  - per department, per cost center.
- By Business unit, by environment, by project-based.

- service control policies (SCP)
  - Applied at the OU or account level.
  - Does not apply to master account. ← ⭐⭐
  - applied to user and roles of the account, including Root
  - SCP should have explicit ALLOW.
    - used to restrict certain service
    - Enforce PCI Compliance.

- Consolidated Billing.
  - combined usage, reserved instances.

(2) AWS Control Tower
- easy to use and setup a multi-account AWS environment based on best practices.
- Control Tower runs on top of AWS organizations.
- Automatically sets up AWS organizations and applies SCP.

(3) Pricing Models. - 4.
- Pay as you go.
- Save when you reserve.
- Pay less by using more. - volume based discounts.
- Pay less as AWS grows.

- Free = IAM, VPC, Billing, Beanstalk, Cloudformation, ASGs.
  EC2 = t2.micro free for a year

EC2:
- on-demand instances.
- Reserved instances (75%)
- Spot instances (90% discount)
- Dedicated hosts.

Lambda / ECS
- API calls, pay per duration.

S3:
- as per storage class
- based on volume.
- number & type of requests.
- Data transfer OUT of S3.
- S3 Transfer Accelerations.
- EFS also the same pricing.

EBS :
- volume type
- Storage volume in GB provisioned (not pay per use)
- IOPS :, snapshots.
- Data transfer OUT.

RDS :
- per hour billing.
- engine, size, memory class.
- on-demand or reserved instances.
- Backup storage
- # of input/output requests per month.
- Deployment type.
- Data Transfer OUT.

Cloudfront
- Global service so pricing is region based.
- Data Transfer OUT.
- # of HTTP/HTTPS requests.

Networking Costs
- 1 cent for private IP communication
- 2 cents for public IP communication.
} use private.

(4) Savings Plan.
- Commit Certain $ of 1 or 3 year.
- EC2 (72% discount) regardless of AZ, size, OS etc.
- tied to instance family and a region.
- Compute Savings plan
  - 66% discount
  - regardless of instance family or region.
- ML Savings Plan. for Sagemaker.

(5) AWS Compute Optimizer
- ML powered service by AWS to choose optimal config.
- EC2, ASG, Lambda, volumes.

(6) Billing and costing tools.
- Pricing calculator (Estimating)
- Billing Dashboard, (Tracking)
  - free tier dashboard.
  - Cost allocation tags.
  - Cost Usage Reports - most extensive.
  - Cost explorer - visual tool → allows 12 month forecasting.

- Billing Alarms (Monitoring)
  - us-east-1 only.
  - actual cost. not projected.
- Budget.
  - for Reserved Instances.

(7) AWS Trusted Advisor

- high level AWS account assessment
- provides recommendation on 5 categories
  - Cost optimization
  - Performance
  - Security
  - Fault tolerance
  - Service limits

  ⭐⭐

- Support Plans
  - 7 core checks ← ⭐⭐ } learn the name.
  - Full checks ← ⭐⭐
- support Plan pricing. ← ⭐⭐

ADVANCED IDENTITY

(1) AWS Security Token Service (STS)

- temporary, limited-privileged credentials.
- short-term credentials.
- Identity federation.
- IAM roles for cross/same account access.
- IAM roles for EC2.

(2) Cognito

- Identity for your web and Mobile application users.
- for web apps; you don't create IAM roles for end-users of your app.

(3) Directory Services.

- Microsoft Active Directory (AD)
- centralized account management.

- AWS managed Microsoft AD.
- AD connector.
- Simple AD

④ IAM Identity Center.

- provides Single sign on
- AWS accounts, Business cloud apps, SAML2.0, EC2.

OTHER SERVICES

① Amazon workspaces.

- provisim Windows or Linux desktops.
- eliminate management of on-premises VDI.

② Appstream 2.0

- like bluestacks for apps.
- can be accessed through browsers.

③ Sumerian

- AR/VR, 3D models.
- directly through browsers.

④ IoT Core

- Connect IoT devices to AWS cloud
- IoT Core acts as a pub-sub.

⑤ Elastic Transcoder

- convert media files in S3 to formats by consumer playback devices.

⑥ AppSync

- backend for mobile and web apps
- makes use of GraphQL by Facebook.

⑦ Amplify.

- develop and deploy scalable full stack web & mobile apps.

⑧ Device Farm

- test mobile & web apps against desktop browsers and real devices.

(9) AWS Backup.
- Backup, Point in Time Recovery.

(10) Disaster Recovery Strategies.
- Backup and Restore is the cheapest.
- Pilot Light.
- Warm standby

(11) Elastic Disaster Recovery (DRS)
- service from AWS for DRS.

(12) AWS DataSync
- move large amount of data from on-prem to AWS.
- incremental after the first full load.

(13) App Discovery & Migration service
- ADS helps you plan your migration to AWS.
  - Agentless discovery
  - Agent-based discovery.
- AMS or MGN helps you lift and shift and perform migration.

(14) Fault Injection Simulator (FIS)
- Chaos Engineering. / run faulty experiments.
- stress testing

(15) Step Functions
- serverless workflow for Lambda functions.

(16) Ground station
- for satellite communications
- download satellite data to a VPC.

(17) AWS Pinpoint.
- 2-way marketing communication service.
- support push SMS, run campaigns etc.
- better than SNS / SES.

AWS ARCHITECTING & ECOSYSTEM

(1) Design Principles.

- Scalability - vertical & horizontal
- Disposable Resources
- Automation - serverless, Iaac,
- Loose Coupling. - No monolith.
- Servicy, not servers

6 pillars :-

i) Operational Excellence
- deliver business value, continually improve.
- Iaac ← most important → CloudFormation
- Annotate documentation
- make frequent, small, reversible changes.
- Refine operations
- anticipate failures → learn

ii) Security
- principal of least privilege - IAM
- Traceability
- vpc, subnet, LB
- encryption, tokenization, ACLs.

iii) Reliability

iv) Performance efficiency

v) Cost optimization.

vi) Sustainability.
- environmental impacts.

Practice Tests

Test 1 - 70%

- AWS Direct Connect
- ~~AWS Connect~~
- block-level storage
- Reliability
- devices MFA
- ECS vs Fargate
- Support plans detail
- AWS Systems Manager
- well-architected framework
- ECS benefits.
- Local zone vs edge
- list of serverless servies.
- list of Global servies.
- Amazon Inspector
- AWS Compute optimizer

Test 2 - 80%

- how credits work
- encryption by default.
- support plan details.
- VPC endpoint gateway.
  S3 and DynamoDB
- SQS and SNS
- Shared responsibility models.
- S3 encryption.
- Reliability pillar.
- variable expense = opex.
- AWS shield.

Test 3 - 84%

Test 4 - 75%

Test 5 - 81%