

Quiz

Section 3: What is Cloud Computing ?.

- Manage only applications and data : PaaS
Pricing model of cloud computing - Pay-as-you-go pricing
- Availability zone: Global Infrastructure identity
Composed of one or more discrete data centers with redundant power, networking, and connectivity, and are used to deploy infrastructure.
- Characteristics of Cloud Computing:
 - 1) Rapid elasticity
 - 2) Scalability
 - 3) Multi-tenancy & Resource pooling
 - 4) On-demand self service
- 3 pricing fundamentals of AWS cloud
 - 1) Compute
 - 2) Storage
 - 3) Data Transfer out of the AWS cloud
- Points of considerations when choosing an AWS region:
 - 1) Compliance with data governance and legal requirements
 - 2) Proximity to customers
 - 3) Available services and features within a Region
 - 4) Pricing.
- Advantage of CC
 - 1) CAPEX for OPEX
 - 2) Go global in minutes
 - 3) Stop spending money running and maintaining data centers.

- AWS regions - Two or more AZs.
- IAM is a global service
- Cloud Computing : On-demand availability of computer system resources, especially data storage (cloud storage) and computing power, without direct active management by the user.
- The Shared Responsibility Model defines who is responsible for what in the AWS cloud.
- Hybrid cloud: Flexible, scalable, on-demand storage access, security, performance

Section 4: Identity and Access Management (IAM)

- IAM roles: An IAM entity that defines a set of permissions for making AWS service requests, that will be used by AWS services.
- - 1) IAM security Tool
 - 2) IAM credentials Report
 - 3) IAM Access Report
- IAM best practice: Don't use the root user account
- IAM Policies: JSON Documents to define Users, Groups or Role's permissions.
- ← → AWS CLI - Using commands
AWS SDK - Programmatically
- Principle regarding IAM permissions - Grant least privilege.
- Increase root account security - Enable MFA.

Section 5:

Elastic Compute Cloud (EC2)

- Convertible instances:
 - 1) Long workloads
 - 2) Flexible instances
- Spot instances: Short workloads, but are less reliable.
- Scheduled instances:
 - 1) Fraction of a day / week / month
- Dedicated Hosts: Strong compliance needs / software that have complicated licensing models.
- Traffic in and out of EC2 instance: Security groups
- OS patches, updates on EC2 instances: The customer
- EC2 Reserved Instances: 1 or 3 years
- EC2 Instance purchasing options:
 - 1) Spot instances
 - 2) Reserved instances
 - 3) On-demand instances
- EC2 instance running continuously for a year - Reserved instances.

Section 6:

EC2 Instance Storage

- EFS: Shared network file system. Set-up, scale, and cost-optimize file storage in the Amazon Cloud.
- Automate image management processes: EC2 Image Builder.
- Microsoft Windows File System: FSx
- EBS volumes can be attached to only one EC2 instance at a time, but EC2 can be attached to or can have multiple EBS volumes attached to them.
- EBS volume is a network drive attached to your instances, data persists even after their termination.
- EC2 instance store: Better I/O performance, but data is lost if EC2 is terminated.
- EBS Snapshot - Backup of your EBS vol. at a point in time.
- Third Party AMI - AWS Marketplace AMI
- EBS volumes are tied to only one availability zone.

Section

7 :

Elastic Load Balancing & Auto Scaling Group (ELB & ASG)

→ High availability means applications running at least in two AZs to survive a data center loss.

→ Hundreds of thousands of connections with low latency - Network load Balancer.

→ ASG - Scale in & out to match the changing load on your applications & websites.

→ Application load Balancers - HTTP & HTTPS.

→ Auto Scaling Strategy:

1) Manual Scaling

2) Dynamic "

3) Predictive

→ Easy horizontal scaling - ASG

→ Load Balancers features:

1) Handle failures of downstream instances

2) Do regular health checks to your instances

3) Spread load across multiple downstream instances.

Simple Storage Service (S3)

→ Amazon Glacier Deep Archive is the most cost-effective option if you want to archive data and do not have a retrieval time requirement - You can retrieve data in 12 or 48 hrs.

→ Policy will not change - S3 Glacier Vault lock.

AWS Storage Gateway is a hybrid cloud storage service that gives you on-premises access to virtually unlimited cloud storage.

→ Snowmobile - Exabytes

Storage optimized → Snowball Edge - Petabytes

TB → Snowcone - Small, portable, rugged and secure edge computing & data transfer device.

→ Objects consists of key, value, metadata.

→ Buckets store objects.

Lifecycle rules: Used to define when S3 objects should be transitioned to another storage class or when objects should be deleted after some time.

→ S3 Standard Infrequent access:

1) Less frequent accessed data

2) Rapid access when needed

3) High durability

4) Allowing an availability zone failure.

Section
9:

Databases & Analytics

- Decentralized block chain: Managed Block chain
 - Hyperledger Fabric
 - Ethereum
- Redshift: Petabyte-scale data warehouse service in the cloud.
- Athena - Serverless + SQL capabilities
- Glue - ETL service that makes it easy for customers to prepare and load their data for analytics.
- Aurora - MySQL + PostgreSQL
- Migrate databases to AWS while still being able to use the database during the migration - Database migration service.
- EMR: Create Hadoop clusters to analyze and process a vast amount of data.
- In-memory AWS DB to reduce the load off databases and has high performance, low-latency: Elasticache
- Central repository to store structural and operational metadata for data assets in AWS Glue - Glue Data Catalog.
- RDS: SQL + setup, operate and scale a relational db in the cloud. OLTP workload.

- Immutable ledger dB - QLDB
- DynamoDB - Fast, flexible non-relational dB for any scale. Scale with no downtime, can process millions of requests per second, fast and consistent in performance.
- Neptune - Graph database. Used for knowledge graphs, fraud detection, recommendation engines, social networking
- Quicksight - Fast, cloud-powered BI service that makes it easy for you to deliver insights to everyone in your organization. Can create and publish interactive dashboard.
- DocumentDB - MongoDB compatible, fast, capable, highly available and fully managed document database service.
- DynamoDB Accelerator: In-memory cache, delivers 10x performance improvement
- RDS Multi-AZ Deployment: High availability
- RDS Read Replica - Scalability

Section
g:

Databases & Analytics

→ Section

10:

ECS, Lambda, Batch, Lightsail.

Charging in AWS Lambda: Per call, per duration.

Serverless service to launch Docker containers with no infrastructure to provision - Fargate

Event-driven: Functions are invoked when needed.

ECS: Launch Docker containers, but provision and maintain the infrastructure.

AWS Lambda:

Integration with the whole AWS suite of services

Virtual functions

Automated and continuous scaling.

Elastic Container Registry: Store Docker image so that they can be run by ECS or Fargate.

API Gateway: Serverless + Easy for developers to create, publish, maintain, monitor, and secure APIs at any scale.

Section 10:

ECS, Lambda, Batch, Lightsail.

Section 11:

Deployments & Managing Infrastructure at Scale.

→ Codestar: Develop, Build and deploy applications on AWS.

→ Elastic Beanstalk: Monitor and to check the health of an environment.

→ AWS CodeDeploy: Automates code deployments.

→ CodeCommit: Secure, highly scalable, managed source control service. Provides software version control.

→ AWS Systems Manager: Visibility & control of your infrastructure. Patching systems at scale.

→ AWS OpsWorks: Configuration management service that provides managed instances of Chef and Puppet.

→ AWS CDK: Open source software development framework to define your cloud application resources using familiar programming languages.

→ CloudFormation: Deploy Iaas.

→ Cloud9: Cloud based IDE

→ Elastic Beanstalk: Paas.

→ CloudFormation Templates: JSON or YAML text files. They are declaration of the AWS resources that make up a stack.

- CodeArtifact: Store code dependencies.
- CodeBuild: Serverless, build code & run tests
- CloudFormation, Elastic Beanstalk are free of use. You do pay for the resources created

Section
12:

Leveraging the AWS Global Infrastructure.

- Weighted Routing Policy - Used to route traffic to multiple resources in proportions that you specify.
- Wavelength: Deploy ultra-low latency applications to 5G devices. Optimized for mobile edge computing applications.
- S3 Transfer Acceleration: Fast, easy and secure transfers of files over long distances on S3.
- AWS CloudFront uses Caching Content in Edge locations to improve read performance.
- Outposts: Run AWS infrastructure and services on-premises for a hybrid cloud model.
- Route 53 features: Domain registration, DNS, Health checks, Routing Policy.
- WAF & Shield - CloudFront integrates to protect against web attacks.

Section 13 :

Cloud Integrations

→ MQ - Managed Message Broker service for Apache MQ and RabbitMQ. Easy to set up and operate message brokers in the cloud.

→ Simple Notification Service - Highly available, durable, secure, fully managed pub/sub messaging service that enables you to decouple microservices, distributed systems, and serverless applications. It is a push-based system.

→ Amazon Kinesis:

Real time analysis from video streams
Timely insights

Four services: Data Firehose, Data Analytics, Data Streams, Video Streams

→ Decouple your applications - Principle applied when using SQS and SNS.

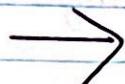
→ Simple Queue Service (SQS) - Send, store, and receive messages between software components at any volume, without losing messages nor requiring other services to be available. It uses pull system.

Section
14:

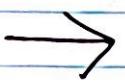
Cloud Monitoring



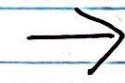
CloudWatch Alarms: Trigger notifications when a metric reaches a threshold you specify.



X-Ray: Helps developers analyze and debug production, distributed applications, such as those built using a microservices architecture.



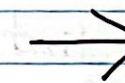
Personal Health Dashboard: Provides alerts and remediation guidance when AWS is experiencing events that may impact you.



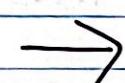
CloudWatch - Monitoring service for AWS cloud resources. Used to collect and track metrics, collect and monitor log files, and set alarms.



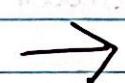
CloudTrail Insights: Helps AWS users identify and detect unusual activity: inaccurate resource provisioning, hitting service limits.



CloudTrail: Inspect, audit, record events and API calls.



Code Guru: Developer tool that provides intelligent recommendations to improve code quality and identify an application's most expensive lines of code.



CloudWatch Logs: A single, highly scalable service that centralizes the logs from all of your systems, applications, and AWS services that you use.

VPC & Networking.

- NAT Gateways: Private subnets to access the internet while remaining private, and managed by AWS.
- Network Access Control List (NACL): Firewall that has both ALLOW and DENY rules and operated at the subnet level.
- Transit Gateway: Connects thousands of VPC and on-premises networks together in a single gateway.
- VPC Peering: Networking connection between two VPC's using AWS network.
- A VPC: Logically isolated section of AWS, where you can launch AWS resources in a private network that you define.
- AWS Direct Connect: Cloud service solution that makes it easy to establish a dedicated private network connection from your premises to AWS.
- Internet Gateway: Horizontally scaled, redundant, and highly available VPC component that allows communication between your VPC and the internet.

Section 16:

Security & Compliance.

- Data at rest: Data stored or archived on a device
- Macie: Security service that uses ML to automatically discover, classify, and protect sensitive data in AWS viz PII or intellectual property.
- Detective: Easy to analyze, investigate, and quickly identify the root cause of potential security issues or suspicious activities.
- WAF: Web Application Firewall. Protect web app or API.
- Artifact: On-demand access to AWS compliance documentation and AWS agreements.
- Config: Enables you to assess, audit, and evaluate the configurations of your AWS resources.
- Certificate Manager (ACM): Secure network communications using SSL & TLS certificates
- Patch Management: AWS & customer.
AWS responsible for patching flaws within the infrastructure.
Customers are responsible for patching their guest OS and applications.
Shared control also includes Configuration Management, Awareness and Training.

→ Security Hub: Comprehensive view of your security state within AWS and your compliance and security standards and best practices.

→ KMS: Used for cryptographic operations.
Manage Encryption Keys.

→ Inspector: Automated Security Assessment
Helps improve the security & compliance of applications
Test the network accessibility of EC2 instances, security state of applications running on the instances.

→ AWS: Security "OF" the cloud
Customer: Security "IN" the cloud.

→ Shield: ONLY used to safeguard running applications from DDoS attacks.

→ GuardDuty: Threat detection service, continuously monitors for malicious activity and unauthorized behavior.

Section
17:

Machine Learning

→ Transcribe: Speech to Text
Polly: Text to Speech

→ Lex:

- 1) Speech to Text
- 2) Building conversational interfaces
- 3) Advanced deep learning
- 4) ASR + NLU
- 5) Build applications with highly engaging user experiences and lifelike conversational interactions.

→ Forecasts:

ML to deliver highly accurate forecasts.

→ Rekognition: Finds objects, people, text, scene in images & videos.
Deep learning technology.

→ Personalize: ML service, makes it easy for developers to create individualized recommendations for customers using their applications.

→ Comprehend: NLP service that uses ML to find meaning and insights in text

→ Translate: Neural Machine Translation service that delivers fast, high-quality, and affordable language translation.

→ SageMaker: Build, train, and deploy a ML model.

→ Kendra: Document search powered by ML

first at design evolution
stage of test & effec

test

BOT at design
specification period
initial job definition
USA & UK
engineering office Washington D.C.
and Estes Park, Colorado, USA
initial design

other cost

of new structure will switch off old

new test design, development
task & cost of
specification period

cost of failure - stored in knowledge
management tool, tribal knowledge, experience
knowledge, task, plan, document, etc.

but also can use feedback from R&D (development)
task of failure has minimum

new test design, initial design cost
initial design, planning, test, initial design
specification period

new design, test design, initial design
specification period

Section 18.

Account Management, Billing & Support

→ Services free in AWS:

1) IAM

2) VPC

3) Consolidated Billing

4) Elastic Beanstalk

→ Inbound data transfer in the S3 region is free.

→ Compute Savings Cost Plans:

Most flexible

Help reduce costs by upto 66%.

Consistent amount of usage for 1/3 yr.

→ With Linux EC2 instances you pay per second of compute capacity. There is also a minimum of 60s of use.

→ Save when you Reserve: Allows you to minimize risks, predictably manage budgets, and comply with long term requirements, and is available for EC2, DynamoDB, ElastiCache, RDS and Redshift.

→ Reserved Instances:

Good and more cost-effective (69% discount).

Can reserve instances for 1 or 3 yrs in RDS.