**Basic-Level AWS Interview Questions:**

1. What is AWS?

AWS (Amazon Web Services) is a comprehensive and widely adopted cloud platform offering over 200 fully featured services from global data centers. It supports Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS), allowing businesses to deploy scalable applications with high availability, security, and performance.

2. What are the main services provided by AWS?

AWS provides services tailored to different business needs:

* Website Hosting: EC2, S3, Route 53
* Data Storage & Backup: S3, Glacier
* App Development: Lambda, API Gateway
* Databases: RDS for SQL, DynamoDB for NoSQL
* Machine Learning: SageMaker

These services allow businesses to scale operations, reduce costs, and increase flexibility.

3. What is EC2?

EC2 (Elastic Compute Cloud) is a service from AWS that lets you rent virtual machines to run applications in the cloud. You can choose the size, memory, and operating system, and pay only for what you use. It's like having a computer in the cloud that you control.

4. What is S3 and what are its storage classes?

Amazon S3 is an object storage service that offers 99.999999999% durability and scales for any size of data.  
Its main storage classes are:

* S3 Standard: General-purpose, frequent access
* S3 Intelligent-Tiering: Auto-optimizes costs by moving data between tiers
* S3 Standard-IA: Infrequent access, lower cost
* S3 One Zone-IA: IA storage in a single zone
* S3 Glacier / Glacier Deep Archive: Archival and long-term backups

5. What is the difference between an EC2 instance and a Lambda function?

* EC2 is like a virtual server—you manage everything, including OS and updates.
* Lambda runs code in response to events without managing servers (serverless).

6. What is IAM and why is it used?

IAM (Identity and Access Management) helps you control who can do what in your AWS account. You can create users and assign permissions to keep things secure.

7. How does AWS VPC work?

An AWS VPC is a logically isolated section of AWS Cloud where you define your own network topology (CIDR block, route tables, subnets, internet gateways). It’s the foundation for deploying secure AWS resources like EC2, RDS, and load balancers.

8. What is the difference between public and private subnets in a VPC?

* Public Subnet: Has internet access via an Internet Gateway.
* Private Subnet: No direct internet access—used for internal services.

9. What is an Elastic Load Balancer (ELB)?

Elastic Load Balancer ensures high availability by distributing network or application traffic across multiple targets (EC2, Lambda, IPs). It supports 3 types:

* Application Load Balancer (ALB) – Layer 7, for HTTP/HTTPS
* Network Load Balancer (NLB) – Layer 4, high performance
* Gateway Load Balancer (GWLB) – For third-party appliances

10. What is Auto Scaling in AWS?

Auto Scaling automatically adds or removes servers (EC2 instances) based on traffic. It helps you save cost and maintain performance.

**Intermediate-Level AWS Questions:**

1. What are the different types of EC2 instance types?

* Use t-series for low-cost web apps
* Use c-series for gaming or compute-heavy tasks
* Use r/x-series for in-memory DBs like SAP HANA
* Use i/d-series for high-speed storage needs
* Use g/p-series for AI/ML and graphics-intensive apps

2. What is the difference between EBS and S3?

* EBS is like a hard disk for EC2 virtual machines
* S3 is like an online folder to store and retrieve files from anywhere

3. How does Route 53 work in AWS?

Amazon Route 53 handles domain registration, DNS routing (A, AAAA, CNAME, etc.), and health checks. It supports routing policies like latency-based, failover, geolocation, and weighted routing to control traffic globally with low latency.

4. Explain the concept of security groups and NACLs.

* Security Groups: Work like firewalls at the instance level
* NACLs (Network Access Control Lists): Act as firewalls at the subnet level

5. What is CloudWatch and how does it differ from CloudTrail?

* Use CloudWatch for real-time metrics, alarms, dashboards
* Use CloudTrail for auditing, compliance, and forensic analysis (e.g., “Who deleted this resource?”)

6. What is the difference between AWS RDS and DynamoDB?

* RDS is for SQL databases (like MySQL, PostgreSQL)
* DynamoDB is a NoSQL key-value and document database

7. Explain AWS Lambda's cold start issue.

Cold starts occur when a new container is initialized to run a Lambda—causing a delay (100ms to several seconds). It affects performance, especially for APIs. To reduce cold starts, use Provisioned Concurrency or keep functions warm with scheduled invocations.

8. What are AWS Availability Zones and Regions?

AWS Regions are isolated geographic areas. Each region contains multiple AZs—physically separate but interconnected data centers—to ensure high availability, fault tolerance, and disaster recovery.

9. How do you secure data in transit and at rest in AWS?

* In transit: Use SSL/TLS encryption
* At rest: Use AWS KMS-managed or customer-managed encryption keys

10. Explain the Shared Responsibility Model of AWS.

AWS manages the security *of* the cloud (hardware, networking), and you manage what’s *in* the cloud (your data, apps, configurations).

**Advanced-Level AWS Questions:**

1. How would you design a fault-tolerant architecture on AWS?

To architect a highly fault-tolerant AWS application:

* Compute Layer:
  + Deploy EC2 instances in an Auto Scaling Group across multiple AZs.
  + Use Elastic Load Balancer (ALB/NLB) to distribute traffic.
* Database Layer:
  + Use Amazon RDS with Multi-AZ replication or Aurora with cross-region replication.
  + For NoSQL, use DynamoDB with global tables.
* Storage:
  + Use Amazon S3 with versioning and cross-region replication for critical files.
  + Use EFS (Elastic File System) for shared file storage across AZs.
* DNS and Routing:
  + Use Route 53 with health checks and failover routing policies.
* Monitoring and Recovery:
  + Enable CloudWatch, CloudTrail, and AWS Config.
  + Set up AWS Lambda functions or SNS notifications to automate recovery actions.
* Backup & DR:
  + Automate snapshots and backups using AWS Backup.
  + Implement a disaster recovery plan using pilot light or warm standby in a different region.