Top 20 AWS Interview Questions & Answers (DevOps Focus)

Q: What is AWS, and what are its core services?

A: AWS is Amazon Web Services — a cloud computing platform offering compute (EC2, Lambda, ECS, EKS), storage (S3, EBS, EFS), networking (VPC, Route53), and managed services (RDS, DynamoDB, etc.).

Q: What is the difference between EC2, Lambda, and ECS/EKS?

A: EC2 provides virtual servers, Lambda is serverless compute triggered by events, ECS/EKS are container orchestration services for running Docker containers.

Q: What is IAM, and how does it help in AWS security?

A: IAM (Identity and Access Management) manages users, groups, roles, and permissions to securely control access to AWS resources.

Q: What are Security Groups vs NACLs?

A: Security Groups are stateful firewalls at the instance level. NACLs are stateless filters at the subnet level.

Q: Explain EC2 instance types. How do you choose the right one?

A: Instance types include General Purpose, Compute Optimized, Memory Optimized, Storage Optimized, and Accelerated Computing. Choice depends on workload type.

Q: What is Auto Scaling, and how does it work?

A: Auto Scaling adjusts the number of EC2 instances automatically based on load to ensure availability and cost-efficiency.

Q: Difference between ECS and EKS? When to use which?

A: ECS is AWS's native container orchestration, easier to start with. EKS runs Kubernetes, useful if you want portability and Kubernetes ecosystem tools.

Q: What is AWS Lambda, and what are its limitations?

A: Lambda is a serverless compute service. Limitations: 15-minute execution timeout, limited memory (10GB), cold starts, and limited execution environment.

Q: Difference between S3, EBS, and EFS?

A: S3 is object storage, EBS is block storage for EC2, and EFS is a shared file system for multiple instances.

Q: What are S3 storage classes?

A: Standard, Intelligent-Tiering, Standard-IA, One Zone-IA, Glacier Instant, Glacier Flexible, and Glacier Deep Archive — each optimized for cost and access frequency.

Q: How do you secure data in S3?

A: Use IAM policies, bucket policies, block public access, server-side encryption (SSE-S3, SSE-KMS), and versioning.

Q: Explain VPC, Subnets, Route Tables, IGW, and NAT Gateway.

A: VPC = private network. Subnets = divide VPC. Route Tables = control routing. IGW = internet access for public subnets. NAT Gateway = internet access for private subnets.

Q: Difference between Public and Private Subnets?

A: Public subnets have internet access via IGW, private subnets do not — they use NAT for outbound access.

Q: What is VPC Peering and Transit Gateway?

A: VPC Peering connects two VPCs directly. Transit Gateway connects multiple VPCs and on-premises networks centrally.

Q: How do you build a CI/CD pipeline in AWS?

A: Use CodeCommit (repo), CodeBuild (build), CodeDeploy (deploy), and CodePipeline (orchestration). Can also integrate with GitHub/Jenkins.

Q: What are AWS CloudFormation and Terraform? Differences?

A: Both are Infrastructure as Code (IaC). CloudFormation is AWS-native. Terraform is multi-cloud, community-driven, and more flexible.

Q: How does Elastic Beanstalk compare to ECS/EKS?

A: Elastic Beanstalk is a PaaS for simple app deployment. ECS/EKS are container orchestration for microservices and complex workloads.

Q: How do you monitor AWS resources?

A: Use CloudWatch (metrics, logs, alarms), CloudTrail (API auditing), and X-Ray (distributed tracing).

Q: What are some AWS best practices for cost optimization?

A: Use Reserved Instances, Spot Instances, right-size resources, use auto-scaling, S3 lifecycle policies, and monitor with Cost Explorer.

Q: How do you secure credentials in AWS?

A: Use IAM roles instead of hardcoding keys, store secrets in AWS Secrets Manager or Parameter Store, and enable MFA.