**IAM**

1. What are users, groups, roles and policies?

Users – Entity created in AWS IAM used to access AWS by any user or an application  
groups – Collection of users  
roles - Temporary access given to users or services to access AWS services  
policies – Permissions or rule written in JSON to provide access to IAM user or roles

1. What is the principle of least privilege, and why should it be followed in IAM?

Provide only required permissions to user, It will improve the security.

1. What is the difference between an identity-based policy and a resourcebased policy?  
   Identity-based policy - Attached to users, groups, or roles  
   Resource-based policy - Attached to AWS resources
2. What are AWS-managed policies and customer-managed policies?  
   AWS-managed policies – Created and managed by aws  
   customer-managed policies – created and managed by user
3. What is multi-factor authentication (MFA), and how does it enhance security?

Two or more verification methods are used to authenticate the user

1. What is a service-linked role, and how is it different from a standard IAM role?  
   Service-linked role – Created by aws services and managed by aws  
   standard IAM role – created and managed by user according to the user need.
2. How do you audit IAM activity using AWS CloudTrail?  
   AWS cloudtrail records all the API logs, Using cloudtrail we can audit all the actions taken.

**EC2 & Lambda**

1. What are the different EC2 instance types, and how do they differ?  
   General Purpose, Compute Optimized, Memory Optimized, Storage Optimized, Accelerated Computing, High Performance Computing (HPC)
2. What are the key components of an ASG?  
   Launch template, AMI, Instance type.
3. How do scaling policies work in ASG, and what are the different types?  
   Auto scale based on utilization, scheduled, manual  
   Step Scaling: add 1 EC2 if CPU > 70%, add 2 if > 90%
4. What are the different types of AWS load balancers, and when should you use each?  
   ALB - HTTP/HTTPS  
   NLB - high performance, TCP/UDP  
   CLB - Old generation, basic Layer 4 and Layer 7 support.
5. How does an ALB distribute traffic across multiple EC2 instances?  
   Distributes traffic based on the rules to target groups.
6. What are target groups, and how do they work with ALB?  
   Group of EC2 instances or Lambda functions as targets, We can attach Target Groups to ALB.
7. How can you configure host-based and path-based routing in ALB?  
   We can configure this using the add rule feature in the listeners, we can write a condition in new rule and use host-header for host based and path for path based routing. If no rules were added, LB will use default rule in the listener.
8. What are AWS Security Groups, and how do they function?  
   Virtual firewalls for EC2, and are stateful.
9. How do Security Groups differ from Network ACLs?  
   stateful and stateless
10. How do you allow only SSH traffic from a specific IP range?  
    allow port 22 to specific ip in SG
11. What is the impact of deleting a Security Group associated with an active EC2 instance?  
    AWS will show an error saying resource is associated.
12. What are the different types of EBS volumes, and when should you use each?  
    GP - Default, balanced performance.  
    Provisioned - High-performance and io operation, R/W operation  
    Throughput Optimized – data transfer per sec ex- GB/s  
    Cold HDD - cheap storage, less accessed
13. How do you resize an EBS volume without downtime?  
    Resize the ebs volume and run below commands in the ec2 which is using the resized ebs.  
    sudo growpart <device name> <partition number>  
    sudo xfs\_growfs -d <mount-point>
14. What is an EBS snapshot, and how can it be used for backup and recovery?  
    Snapshot is an incremental backup of ebs volumes. We can use this restore data or transfer data to other egion.
15. How do you encrypt an EBS volume, and what are the benefits?  
    Encrypt ebs using KMS keys, We need to enable encryption while creating the EBS
16. What is the difference between EBS & EFS?  
    Main diff is how the data is stored, Cost, Use cases.
17. What is AWS Lambda, and how does it enable serverless computing?  
    Lambda is an serverless service where user runs the code and servers and other things managed by aws. Depends on runtimes, package size
18. What are the key factors that impact AWS Lambda cold start times, and how can they be minimized?  
    Cold start – delay in lambda function execution of the code when starts from inactive state or when first start.  
    Reduce cold start  
    Warm-Up Strategies – Regularly invoke your Lambda functions to keep them warm  
    Provisioned concurrency **-** keeps a number of Lambda environments ready
19. What is an EC2 Savings Plan, and how does it help reduce costs?  
    Pre commitment for the instances for 1 or 3 year period will get upto 70% discounts on on-demand instances.
20. What is the difference between Compute Savings Plans and EC2 Instance Savings Plans?  
    Compute Savings Plans - flexibility and up to 66% discounts, Works across ec2, fargate, lambda.

EC2 Instance Savings Plans - up to 72% discounts and only applies to ec2. Less flexibility

1. How do Savings Plans compare to Reserved Instances in terms of flexibility?  
   Savings plan are more flexible compare to RI’s as RI’s more tied to specific instance types, regions. and savings plan specially compute savins plans are flexible in changing region, instance families etc

**EKS & ECR**

1. What are the core components of an EKS cluster?  
   Master nodes, worker nodes, kubelet, api-server, controllers etc
2. How does EKS integrate with the AWS networking model (VPC, Subnets, Security Groups)?  
   Eks are created inside VPC, Nodes are created inside Subnets with SG as firewalls.  
   Uses CNI to assign the ip to pods from VPC cidr
3. What is the difference between managed node groups and self-managed node groups?  
   AWS manages lifecycle, updates, scaling.  
   User mangers the node lifecycle.
4. What role does IAM play in EKS authentication and authorization?  
   Iam manages EKS authentication  
   RBAC manages the autorisation inside the cluster
5. How does EKS handle high availability and scaling?  
   Control plane is managed by aws and highly available.  
   User can use Auto scaling and multi AZ for worker nodes.
6. How do you expose services running in EKS to the internet?  
   K8s LoadBalancer service type  
   Ingress Controllers  
   Node-port service
7. What is the Amazon VPC CNI plugin, and why is it important for EKS networking?  
   Container network interface – Used by conainer runtimes to attach IP’s to pod
8. What is Kubernetes RBAC, and how is it used in EKS?  
   Role Based Access Control - authorization like what actions users or service accounts can perform inside EKS
9. How do you enforce network policies in an EKS cluster?  
   Creating kind: NetworkPolicy configs with rules. To control pod to pod traffic.  
   Calico – Network plugin in eks supports network policies.
10. What is Amazon ECR, and how does it differ from Docker Hub?  
    Elastic Container Registry – AWS managed private container registry  
    Docker hub - public container image registry managed by docker.
11. What is the difference between ECR Public and ECR Private?  
    ECR Public - Public registry and anyone can access it  
    ECR Private - Private registry and only autorised users can access.

**Route 53**

1. What is Amazon Route 53, and what are its key features?  
   AWS Domain Name System service  
   Supports domain registration, DNS routing
2. What are the different types of DNS records supported by Route 53 (A, CNAME, ALIAS, etc.)?

A – Maps domain to IPv4

AAAA – Maps domain to IPv6

CNAME – Maps domain to another domain

ALIAS – AWS-specific, works at root domain

MX – Mail exchange

Etc

1. What is the difference between a public and a private hosted zone in Route 53?  
   public hosted zone - Public internet, Global Access  
   private hosted zone - Within VPC only, Restricted to VPC
2. How does Route 53 handle routing policies (Simple, Weighted, Latencybased, Geolocation, Failover, Multi-value)?

Simple – default

Weighted – Split traffic using weights

Latency-based – Route to nearest region

Geolocation – Route based on user's location

Failover – Switch to backup if primary is unhealthy

Multi-value – Return multiple healthy IPs

1. What is an Alias record, and how does it differ from a CNAME record in Route 53?  
   Alias Record -   
   Maps a domain name to AWS resources  
   Resolved internally by AWS, making it faster and seamless.  
   AWS specific DNS record type  
   DNS queries to AWS resources using Alias are not charged  
     
   CNAME Record -   
   Maps one domain name to another domain name.  
   Cannot be used at the root domain  
   Charged as a normal DNS query  
   Used for external DNS mappings
2. How does Route 53 integrate with AWS services like ALB, CloudFront, and S3?  
   Use Alias record to point domain to ALB, CF or S3
3. How can Route 53 help in setting up a multi-region disaster recovery solution?  
   Automated failover and DR solutions - **Failover routing** - Define primary and secondary records and If the primary is unhealthy, traffic is routed to the secondary

**S3 & Cloudfront**

1. How does Amazon CloudFront work with S3 to deliver content efficiently?  
   CloudFront is an CDN  
   S3 is a object storage type in AWS

Store the data in s3 as origin and create a cloudfront distribution to delivery the s3 content to end user using edge locations.  
User traffic first goes to the edge locations and then if cache data is not present then CF will fetch it from the S3.

1. What is an S3 bucket policy, and how can it be used to allow CloudFront access to private S3 content?  
   S3 bucket policy – It is a aws resource based policy to manage S3 bucket access.  
   Create a s3 bucket policy to only allow required access to the bucket from the CF distribution and block all other actions.
2. What is the difference between a CloudFront distribution and an S3 static website hosting setup?  
   CloudFront distribution –   
   S3 bucket can stay private  
   Edge caching improves performance and reduces S3 load  
   Advanced features: signed URLs, geo-restrictions, compression.  
   better performance and security.  
     
   S3 static website hosting -   
   Content served directly from the S3 bucket  
   Bucket must be public for access.  
   Limited customization
3. How does CloudFront caching work, and how can you invalidate cached objects when updating S3 content?  
   CloudFront caches content at **edge locations** (close to users)  
   If it's **in the cache**, CloudFront serves it immediately or If not it fetches from the origin.  
   Invalidation is used to **force CloudFront to remove cached content** before its TTL expires
4. IMP: What are signed URLs and signed cookies in CloudFront, and how do they secure private S3 content?  
   Signed URLs and signed cookies restrict access to private CloudFront content  
   Used with private S3 buckets  
   Provide secure, time-limited, and optionally IP-restricted access

**VPC & Networking**

1. What is the difference between a public and private subnet in a VPC?  
   subnet that has a route to the internet – Public subnet  
   A subnet that does NOT have a direct route to the internet – Private subnet
2. How does a route table work in AWS VPC, and how do you associate it with subnets?  
   route table in AWS defines how network traffic is directed within a VPC  
   Target, Destination CIDR block.  
   AWS automatically adds a “local” route for communication within the VPC  
   Using Subnet Associations option in route table
3. What is the purpose of an Internet Gateway (IGW), and how does it enable internet access for VPC resources?  
   IGW - A **managed AWS resource** that connects a VPC to the public internet  
   Allows instances in a public subnet to Send and Receive requests to the internet.  
   Acts as a bridge between the VPC and the external internet.
4. What is a NAT Gateway, and how does it differ from an Internet Gateway?  
   Network Address Translation  
   Allows instances in private subnets to access the internet, but prevents the internet from initiating connections back  
     
   IGW -   
   Full internet access for public subnets  
   Inbound + outbound internet access
5. How does VPC Peering work, and when should you use it instead of a Transit Gateway?  
   A network connection between two VPCs that enables private communication using private IP addresses  
     
   TGW - A central hub to connect multiple VPCs and on-premises networks.  
   Choose VPC Peering for small setups, and Transit Gateway for large, complex networks
6. Can VPC Peering be established between different AWS accounts and regions? How?  
   Yes  
   Initiate VPC Peering (Account A) – choose source VPC - Peering VPC ID - Enter the Account ID of the other AWS account - Select region - Create Peering Connection - Accept Peering Request (Account B) - Configure Route Tables in Both VPCs - Update Security Groups & NACLs.
7. How can you ensure high availability and fault tolerance when using NAT Gateway?  
   Create NAT Gateways in Multiple AZs  
   Route Private Subnets to that subnet AZ NAT Gateway
8. What are the security best practices when configuring route tables, NAT Gateways, and Internet Gateways?  
   route tables -   
   Only add routes that are **absolutely necessary**Use Separate Route Tables for separate private/public subnets  
     
   NAT Gateways  
   Place NAT Gateway in Each AZ  
   Restrict Outbound Access  
     
   IGW -   
   Attach IGW Only When Needed  
   Control Access via Security Groups and NACLs  
   Avoid Public IPs in Private Subnets
9. How can you troubleshoot connectivity issues in a VPC using VPC Flow Logs?  
   **VPC Flow Logs** capture IP traffic going to and from **network interfaces** in your VPC

Key Fields in Flow Logs -

Field Description

srcaddr Source IP address

dstaddr Destination IP address

action ACCEPT or REJECT

protocol Protocol used (6 = TCP, 17 = UDP, etc.)

srcport Source port

dstport Destination port

log-status OK / NODATA / SKIPDATA

Check -

Is the traffic being accepted or rejected?

Are security group or NACL rules blocking the traffic?

Is the route table correct?

Is the target reachable

**Cloudwatch (Metrics & Logs)**

1. What are CloudWatch metrics, logs, and alarms, and how do they help in monitoring AWS resources?  
   CloudWatch Metrics -   
   Ex- CPUUtilization (EC2), NetworkIn/NetworkOut, RequestCount (API Gateway)  
   **Numerical data points** representing the performance of resources.  
     
   CloudWatch Logs - **Log data storage and analysis** service  
   Collects logs from aws services  
   Logs are stored in **log groups** → divided into **log streams**CloudWatch Alarms - **Monitors metrics and triggers actions** based on thresholds.  
   Alarms can - Send SNS notifications, Auto-scale EC2 instances, Stop/start/reboot EC2 instances  
     
   Metrics Real-time performance tracking

Logs Detailed event and error tracking

Alarms Automated alerts and proactive responses

1. How can you set up a CloudWatch alarm to trigger an action when an EC2 instance CPU usage exceeds a threshold?

Step Description

Select Metric - EC2 CPUUtilization

Set Condition - Threshold (e.g., > 80% for 5 mins)

Choose Action - SNS alert, auto-scale, stop/reboot EC2

Create Alarm Name and confirm

1. IMP : What is CloudWatch Logs Insights, and how can it be used to analyze log data efficiently?  
   **CloudWatch Logs Insights** is an **interactive log analytics tool** in AWS  
   Allows us to **query and analyze log data** stored in CloudWatch Logs.  
   Filter logs using keywords to narrow results.

Extract key fields like timestamp, status, and message for clarity.

Sort and limit results to find recent or top entries.

Use stats and bin() to aggregate data