1. What do you know about AWS Region?

Answer: An AWS Region is a completely independent entity in a geographical area. There are two more Availability Zones in an AWS Region.

Within a region, Availability Zones are connected through low-latency links.

Since each AWS Region is isolated from another Region, it provides very high fault tolerance and stability.

For launching an EC2 instance, we have to select an AMI within the same region.

2. What are the important components of IAM?

Answer: The important components of IAM are as follows:

IAM User: An IAM user is a person or service that will interact with AWS. User can sign in to AWS Management Console for performing tasks in AWS.

IAM Group: An IAM Group is a collection of IAM users. We can specify permission to an IAM Group. This helps in managing a large number of IAM users. We can simply add or remove an IAM User to an IAM Group to manage the permissions.

IAM Role: An IAM Role is an identity to which we give permissions. A Role does not have any credentials (password or access keys). We can temporarily give an IAM Role to an IAM User to perform certain tasks in AWS.

IAM Permission: In IAM we can create two types of Permissions. Identity-based and Resource-based. We can create a Permission to access or perform an action on an AWS Resource and assign it to a User, Role or Group. We can also create Permissions on resources like S3 bucket, Glacier vault etc and specify who has access to the resource.

IAM Policy: An IAM Policy is a document in which we list permissions to specify Actions, Resources, and Effects. This document is in JSON format. We can attach a policy to an IAM User or Group.

3. What are the important features of Amazon S3?

Answer: Some of the important features of Amazon S3 are as follows:

- **Amazon S3 provides unlimited storage for files.**
- **File size in Amazon S3 can vary from 0 Bytes to 5 Terabytes.**
- **We have store files in Buckets in Amazon S3.**
- **In Amazon S3, names of buckets have to be unique globally.**
- **Amazon S3 is Object-Based storage.**

4. What is the scale of durability in Amazon S3 ?

Answer: Amazon S3 supports durability at the scale of 99.999999999% of the time. This is 9 nines after the decimal.

5. What are the Consistency levels supported by Amazon S3?

Answer: Amazon S3 supports Read after Write consistency when we create a new object by PUT. It means as soon as we Write a new object, we can access it.

Amazon S3 supports Eventual Consistency when we overwrite an existing object by PUT. Eventual Consistency means that the effect of overwriting will not be immediate but will happen after some time.

For deletion of an object, Amazon S3 supports Eventual Consistency after DELETE.

6. What are the different tiers in Amazon S3 storage?

Answer: Different Storage tiers in Amazon S3 are as follows:

S3 Standard: In this tier, S3 supports durable storage of files that become immediately available. This is used for frequently used files.

S3 Standard -Infrequent Access (IA): In this tier, S3 provides durable storage that is immediately available. But in this tier files are infrequently accessed.

S3 Reduced Redundancy Storage (RRS): In this tier, S3 provides the option to customers to store data at lower levels of redundancy. In this case data is copied to multiple locations but not on as many locations as standard S3.

7. What is Lambda@Edge in AWS?

Answer: In AWS, we can use Lambda@Edge utility to solve the problem of low network latency for end-users.

In Lambda@Edge there is no need to provision or manage servers. We can just upload our Node.js code to AWS Lambda and create functions that will be triggered on CloudFront requests.

When a request for content is received by CloudFront edge location, the Lambda code is ready to execute.

This is a very good option for scaling up the operations in CloudFront without managing servers.

8. What are the different types of events triggered by Amazon CloudFront?

Answer: Different types of events triggered by Amazon CloudFront are as follows:

Viewer Request: When an end-user or a client program makes an HTTP/HTTPS request to CloudFront, this event is triggered at the Edge Location closer to the end-user.

Viewer Response: When a CloudFront server is ready to respond to a request, this event is triggered.

Origin Request: When CloudFront server does not have the requested object in its cache, the request is forwarded to the origin server. At this time this event is triggered.

Origin Response: When CloudFront server at an Edge location receives the response from the origin server, this event is triggered.

9. What is Geo-Targeting in Amazon CloudFront ?

Answer: In Amazon CloudFront we can detect the country from where end users are requesting our content. This information can be passed to our Origin server by Amazon CloudFront. It is sent in a new HTTP header.

Based on different countries we can generate different content for different versions of the same content. These versions can be cached at different Edge Locations that are closer to the end-users of that country.

In this way, we are able to target our end-users based on their geographic locations.

10. What are the main features of Amazon CloudFront ?

Answer: Some of the main features of Amazon CloudFront are as follows: Device Detection Protocol Detection Geo-Targeting Cache Behavior Cross-Origin Resource Sharing Multiple Origin Servers HTTP Cookies Query String Parameters Custom SSL.

11. What are the security mechanisms available in Amazon S3?

Answer: Amazon S3 is a very secure storage service. Some of the main security mechanisms available in Amazon S3 are as follows:

• Access: When we create a bucket or an object, only the owner get access to the bucket and objects.

• Authentication: Amazon S3 also support user authentication to control who has access to a specific object or bucket.

• Access Control List: We can create Access Control Lists (ACL) to provide selective permissions to users and groups.

• HTTPS: Amazon S3 also supports HTTPS protocol to securely upload and download data from the cloud.

• Encryption: We can also use Server Side Encryption (SSE) in Amazon S3 to encrypt data.

12. What are the benefits of AWS Storage Gateway?

Answer: We can use AWS Storage Gateway (ASG) service to connect our local infrastructure for files etc with Amazon cloud services for storage.

Some of the main benefits of AWS Storage Gateway are as follows:

Local Use: We can use ASG to integrate our data in multiple Amazon Storage Services like- S3, Glacier etc with our local systems. We can continue to use our local systems seamlessly.

Performance: ASG provides better performance by caching data in local disks. Though data stays in the cloud, the performance we get is similar to that of local storage.

Easy to use: ASG provides a virtual machine to use it by an easy to use interface. There is no need to install any client or provision rack space for using ASG. These virtual machines can work in the local system as well as in AWS.

Scale: We get the storage at a very high scale with ASG. Since backend in ASG is Amazon cloud, it can handle large amounts of workloads and storage needs.

Optimized Transfer: ASG performs many optimizations, due to which only the changes to data are transferred. This helps in minimizing the use of bandwidth.

13. What are the main use cases for AWS Storage Gateway ?

Answer: AWS Storage Gateway (ASG) is very versatile in its usage. It solves a variety of problems at an enterprise. Some of the main use cases of ASG are as follows:

Backup systems: We can use ASG to create backup systems. From local storage, data can be backed up into cloud services of AWS. On-demand, we can also restore the data from this backup solution. It is a replacement for Tape based backup systems.

Variable Storage: With ASG, we can grow or shrink our Storage as per our needs. There is no need to add racks, disks etc to expand our storage systems. We can manage the fluctuations in our storage needs gracefully by using ASG.

Disaster Recovery: We can also use ASG for a disaster recovery mechanism. We can create snapshots of our local volumes in Amazon EBS. In the case of a local disaster, we can use our applications in the cloud and recover from the snapshots created in EBS.

Hybrid Cloud: At times we want to use our local applications with cloud services. ASG helps in implementing Hybrid cloud solutions in which we can utilize cloud storage services with our on-premises local applications.

14. What is AWS Snowball?

Answer: AWS provides a very useful service called Snowball for transporting very large amounts of data at the scale of petabytes.

With Snowball, we can securely transfer data without any network cost.

It is a physical data transfer solution to store data in the AWS cloud.

Once we create a Snowball job in AWS console, Amazon ships a physical storage device to our location. We can copy our data to this storage device and ship it back. Amazon services will take the Snowball device and transfer the data to Amazon S3.

15. What are the different types of load balancing options provided by Amazon Elastic Load Balancing (ELB)?

Answer: Amazon Elastic Load Balancing (ELB) provides two types of load balancers:

Classic Load Balancer: This Load Balancer uses application or network load information to route traffic. It is a simple way of load balancing to divide load among multiple EC2 instances.

Application Load Balancer: This Load Balancer uses advanced application-level information to route the traffic among multiple EC2 instances. It can even use the content of the request to make routing decisions.

16. What is the difference between Volume and Snapshot in Amazon Web Services?

Answer: In Amazon Web Services, a Volume is a durable, block-level storage device that can be attached to a single EC2 instance. In plain words, it is like a hard disk on which we can write or read from.

A Snapshot is created by copying the data of a volume to another location at a specific time. We can even replicate the same Snapshot to multiple availability zones. So Snapshot is a single point in time view of a volume.

We can create a Snapshot only when we have a Volume. Also from a Snapshot, we can create a Volume.

In AWS, we have to pay for storage that is used by a Volume as well as the one used by Snapshots.

17. What are the two main types of Volume provided by Amazon EBS?

Answer: Amazon EBS provides the following two main types of Volume:

Solid State Drive (SSD): This type of Volume is backed by a Solid State Drive. It is suitable for transactional work in which there are frequent reads and writes. It is generally more expensive than the HDD based volume.

Hard Disk Drive (HDD): This type of Volume is backed by Hard Disk Drive. It is more suitable for large streaming workload in which throughput is more important than transactional work. It is a cheaper option compared with SSD Volume.

18. What is the difference between Instance Store and EBS?

Answer: Some of the Amazon EC instances types provide the option of using a directly attached block-device storage. This kind of storage is known as Instance Store. In other Amazon EC2 instances, we have to attach an Elastic Block Store (EBS).

Persistence: The main difference between Instance Store and EBS is that in Instance Store data is not persisted for long-term use. If the Instance terminates or fails, we can lose the Instance Store data.

Any data stored in EBS is persisted for a longer duration. Even if an instance fails, we can use the data stored in EBS to connect it to another EC2 instance.

Encryption: EBS provides full-volume encryption of data stored in it. Whereas Instance Store is not considered good for encrypting data.

19. What is an Elastic IP Address?

Answer: Amazon provides an Elastic IP Address with an AWS account. An Elastic IP address is a public and static IP address based on IPv4 protocol. It is designed for dynamic cloud computing.

This IP address is reachable from the Internet. If we do not have a specific IP address for our EC2 instance, then we can associate our instance to the Elastic IP address of our AWS account. Now our instance can communicate on the Internet with this Elastic IP Address.

20. What are the main options available in Amazon CloudWatch?

Answer: Amazon CloudWatch is a monitoring service by Amazon for cloud-based AWS resources. Some of the main options in Amazon CloudWatch are as follows:

Logs: We can monitor and store logs generated by EC2 instances and our application in CloudWatch. We can store the log data for the time period convenient for our use.

Dashboard: We can create visual Dashboards in the form of graphs to monitor our AWS resource in CloudWatch.

Alarms: We can set alarms in CloudWatch. These alarms can notify us by email or text when a specific metric crosses a threshold. These alarms can also detect the event when an Instance starts of shuts down.

Events: In CloudWatch we can also set up events that are triggered by an Alarm. These events can take automated action when a specific Alarm is triggered.

21. What are the main use cases for AWS Lambda?

Answer: Some of the main use cases in which AWS Lambda can be used are as follows:

Web Application: We can integrate AWS Lambda with other AWS services to create a web application that can scale up or down with zero administrative effort for server management, backup or scalability.

Internet of Things (IoT): In the Internet of Things applications, we can use AWS Lambda to execute a piece of code on the basis of an event that is triggered by a device.

Mobile Backend: We can create Backend applications for Mobile apps by using AWS Lambda.

Real-time Stream Processing: We can use AWS Lambda with Amazon Kinesis for processing real-time streaming data.

ETL: We can use AWS Lambda for Extract, Transform, and Load (ETL) operations in data warehousing applications. AWS Lambda can execute the code that can validate data, filter information, sort data or transform data from one form to another form.

Real-time File processing: AWS Lambda can also be used for handling any updates to a file in Amazon S3. When we upload a file to S3, AWS Lambda can create thumbnails, index files, new formats etc in real-time.

22. How does AWS Lambda handle failure during event processing?

Answer: In AWS Lambda we can run a function in synchronous or asynchronous mode.

In synchronous mode, if AWS Lambda function fails, then it will just give an exception to the calling application.

In asynchronous mode, if AWS Lambda function fails then it will retry the same function at least 3 times.

If AWS Lambda is running in response to an event in Amazon DynamoDB or Amazon Kinesis, then the event will be retried till the Lambda function succeeds or the data expires. In DynamoDB or Kinesis, AWS maintains data for at least 24 hours.

23. What are the different routing policies available in Route 53?

Answer: Route 53 provides multiple options for creating a Routing policy. Some of these options are as follows:

Simple Routing: In this option, Route 53 will respond to DNS queries based on the values in the resource recordset.

Weighted Routing: In this policy, we can specify the weight according to which multiple resources will handle the load. E.g. If we have two web servers, we can divide load in 40/60 ration on these servers.

Latency Routing: In this option, Route 53 will respond to DNS queries with the resources that provide the best latency.

Failover Routing: We can configure active/passive failover by using this policy. One resource will get all the traffic when it is up. Once the first resource is down, all the traffic will be routed to second resource that is active during failover.

Geolocation Routing: As the name suggests, this policy works on the basis of the location of end-users from where requests originate.

24. When will you incur costs with an Elastic IP address (EIP)?

Answer: You are not charged if only one Elastic IP address is attached with your running instance. But you do get charged in the following conditions:

- **When you use more than one Elastic IPs with your instance.**
- **When your Elastic IP is attached to a stopped instance.**
- **When your Elastic IP is not attached to any instance.**