**1. What is Amazon S3?**

**Answer:** Amazon S3 is an **object storage service** that stores data as objects inside **buckets**.

* **Features:** Unlimited storage, durability (11 9’s), scalability, and availability.
* **Use Cases:** Backup, static websites, data lakes, archiving.

**2. What is the maximum object size in S3?**

**Answer:**

* Maximum object size: **5 TB**.
* For objects >5 GB, use **Multipart Upload**.

**3. What is the difference between S3 Standard and S3 Glacier?**

**Answer:**

* **S3 Standard:** Frequently accessed data, low latency.
* **S3 Glacier:** Long-term archival, retrieval takes minutes to hours, cheaper.

**4. What is an S3 Bucket?**

**Answer:** A **container for storing objects** (files).

* Buckets have **globally unique names**.
* Defined at **region** level.

**5. What is S3 Object Key?**

**Answer:** The **full path** of an object inside a bucket (e.g., images/photo.jpg).

**6. Is S3 storage unlimited?**

**Answer:** Yes. AWS S3 provides **virtually unlimited storage** capacity.

**7. What is the difference between S3 and EBS?**

**Answer:**

* **S3:** Object storage, accessed over HTTP(S).
* **EBS:** Block storage, attached to EC2 instances.

**8. What are S3 Storage Classes?**

**Answer:**

* **S3 Standard** (frequent access)
* **S3 IA** (Infrequent Access)
* **S3 One Zone-IA**
* **S3 Intelligent-Tiering**
* **S3 Glacier / Glacier Deep Archive**

**9. How is data secured in S3?**

**Answer:**

* Encryption (SSE-S3, SSE-KMS, SSE-C)
* IAM policies, bucket policies, ACLs
* MFA delete for versioning

**10. What are S3 Access Control Lists (ACLs)?**

**Answer:** Legacy method for object-level permissions.

* Modern best practice: Use **IAM policies** or **Bucket Policies** instead.

**11. What is S3 Versioning?**

**Answer:** Keeps **multiple versions** of an object to protect against accidental deletion or overwrite.

* Once enabled, cannot be disabled (only suspended).

**12. What is S3 Lifecycle Policy?**

**Answer:** Rules to **automatically transition** objects to cheaper storage (e.g., Glacier) or **expire** (delete) them after a certain time.

**13. What is S3 Cross-Region Replication (CRR)?**

**Answer:** Automatically replicates objects across **different AWS regions** for **disaster recovery** or compliance.

**14. What is S3 Same-Region Replication (SRR)?**

**Answer:** Replicates objects within the same AWS region (useful for compliance or separating workloads).

**15. What is the difference between S3 Bucket Policy and IAM Policy?**

**Answer:**

* **Bucket Policy:** Attached to the bucket, defines who can access it.
* **IAM Policy:** Attached to users, roles, groups to define what they can access.

**16. How to make an S3 bucket public?**

**Answer:**

* Disable **Block Public Access**.
* Attach **Bucket Policy** with "Effect": "Allow" for "Principal": "\*".

**17. What is S3 Transfer Acceleration?**

**Answer:** Speeds up uploads/downloads to S3 using **Amazon CloudFront Edge Locations**.

**18. What is S3 Object Lock?**

**Answer:** Prevents deletion/modification of objects for a retention period (WORM compliance).

**19. What are S3 Event Notifications?**

**Answer:** Trigger events (like Lambda, SQS, SNS) when objects are created, deleted, etc.

**20. What is S3 Pre-Signed URL?**

**Answer:** A temporary URL that allows access to an S3 object without requiring IAM credentials. Example:

aws s3 presign s3://my-bucket/myfile.txt --expires-in 3600

**21. Scenario: You need to host a static website using S3. How?**

**Answer:**

* Enable **Static Website Hosting** on the bucket.
* Make objects public or use CloudFront for distribution.
* Point domain to bucket endpoint via Route 53.

**22. Scenario: Prevent accidental deletion of S3 objects.**

**Answer:**

* Enable **Versioning** + **MFA Delete**.

**23. Scenario: Reduce S3 cost without losing data.**

**Answer:**

* Use **Lifecycle Policies** to transition old data to Glacier.
* Enable **Intelligent-Tiering** for automatic cost optimization.

**24. Scenario: Securely share an S3 file with a third party for 1 hour.**

**Answer:**

* Use a **Pre-Signed URL** with --expires-in 3600.

**25. Scenario: Limit an IAM user to upload only objects with encryption enabled.**

**Answer:** Use a **bucket policy** with condition:

"Condition": { "StringEquals": { "s3:x-amz-server-side-encryption": "AES256" } }

**26. What is the difference between S3 Server-Side Encryption (SSE) types?**

**Answer:**

* **SSE-S3:** AWS manages keys.
* **SSE-KMS:** AWS KMS keys, customer control.
* **SSE-C:** Customer provides encryption keys.

**27. Scenario: You have millions of objects. How to improve S3 performance?**

**Answer:**

* Use **prefix randomization** (e.g., hashing filenames).
* Use **S3 Multipart Upload** for large files.

**28. Can S3 be mounted as a filesystem on EC2?**

**Answer:** Yes, using **s3fs-fuse** or **AWS Storage Gateway**, but it's not native block storage.

**29. Scenario: Detect public access to S3 buckets.**

**Answer:**

* Enable **AWS Config** with **S3 Public Read Prohibited Rule**.
* Use **S3 Block Public Access**.

**30. Scenario: You need to log all access requests to an S3 bucket.**

**Answer:**

* Enable **Server Access Logging** or **CloudTrail data events**.

**31. What is S3 Select?**

**Answer:** Allows **SQL queries** on objects (CSV, JSON, Parquet) without downloading the entire file.

**32. What is S3 Object Lambda?**

**Answer:** Allows you to **transform data** (e.g., watermark images, filter rows) on-the-fly when retrieved via Lambda.

**33. Scenario: You need S3 to integrate with on-prem backup.**

**Answer:** Use **AWS Storage Gateway** (File Gateway or Tape Gateway).

**34. How to replicate encrypted objects between buckets?**

**Answer:**

* Use **SSE-KMS** with proper permissions for both source and destination keys.
* Enable replication with KMS key policy.

**35. What is S3 Intelligent-Tiering and why use it?**

**Answer:** Automatically moves objects between **frequent** and **infrequent** access tiers to optimize cost.

**36. Scenario: You want to prevent objects from being overwritten once uploaded.**

**Answer:**

* Enable **S3 Object Lock (Compliance Mode)**.

**37. What is the difference between S3 Cross-Region Replication and Backup to Glacier?**

**Answer:**

* **CRR:** Replicates objects to another region bucket.
* **Glacier:** Moves objects to archival storage in the same region.

**38. How do you prevent an IAM user from deleting a specific object in a bucket?**

**Answer:** Attach a bucket policy with:

"Effect": "Deny",

"Action": "s3:DeleteObject",

"Resource": "arn:aws:s3:::my-bucket/critical-data/\*"

**39. Scenario: How to enforce all S3 buckets to block public access at the account level?**

**Answer:**

* Use **S3 Block Public Access (Account Settings)**.
* Use **Service Control Policies (SCPs)** in AWS Organizations.

**40. How to ensure data integrity during uploads/downloads?**

**Answer:**

* Use **MD5 checksum** verification.
* Enable **S3 ETag validation**.