

Developing Storage Solutions

AMAZON S3 · BUCKETS & OBJECTS · OBJECT OPERATIONS · VERSIONING · ENCRYPTION · ACCESS CONTROL · SDK STUDY & REVIEW DEVELOPMENT

01 MUST KNOW

if you remember five things, remember these

- 01 Object storage, 11 nines: Amazon S3** is an object storage service built for scalability, availability, security, and performance, and **designed for 99.999999999% (11 nines) of durability** — store 10,000,000 objects and on average you might lose one every 10,000 years. Capacity is virtually unlimited, and S3 can fire **event notifications** to **AWS Lambda**, **Amazon SNS**, or **Amazon SQS**.
- 02 Bucket · object · key:** A **bucket** is a **Regional** container whose name is **globally unique** across every AWS account (3–63 chars; lowercase letters, numbers, hyphens). An **object** is object data plus **metadata**; the **object key** uniquely identifies it — each object has exactly **one** key. Neither the bucket name nor its Region can change after creation.
- 03 PUT · GET · DELETE (+ SELECT):** **PUT** writes an entire object (single upload ≤ 5 GB; **multipart required above 5 GB**, up to 5 TB, and recommended past 100 MB). **GET** reads a whole object or a **byte range**. **DELETE** removes objects by key. **SELECT** queries object contents with SQL. PUT needs write permission; GET needs read access.
- 04 Versioning protects objects:** **Versioning** keeps multiple variants of an object under one key, each with a **version ID**, so you recover from accidental overwrites and deletes. It is **off by default**, and once enabled it can only be **suspended** — **never disabled**. A DELETE with only a key adds a **delete marker** (retrieval then returns 404) instead of erasing prior versions.
- 05 Private by default:** Every bucket and object is **private to the creating account** until you grant access. Share with **identity-based policies** (on IAM users, groups, roles) or **resource-based policies (bucket policies and ACLs)**; a **presigned URL** grants temporary **PUT or GET** on a single object using the creator's own permissions.

02 KEY TERMS

TERM	DEFINITION
Amazon S3	Amazon Simple Storage Service — an object storage service offering scalable, durable, secure, high-performance storage; designed for 11 nines of durability
Bucket	A Regional container for objects; organizes the S3 namespace, identifies the billing account, and is the unit of access control and usage aggregation
Object	The fundamental entity stored in S3 — any kind of file — made up of the object data and its metadata
Object key	The string that uniquely identifies an object within a bucket; every object has exactly one key
Prefix	A shared leading string on object keys; implies a folder structure and limits query results to matching keys
Object metadata	Key-value pairs describing an object; either system-defined (S3-controlled) or user-defined (x-amz-meta- prefix)
Multipart upload	Uploading one object as a set of independently uploaded, resumable parts; required above 5 GB and allowing objects up to 5 TB
Versioning	Keeping multiple variants of an object in one bucket, each with a version ID; can be suspended but never disabled once enabled
Delete marker	The placeholder S3 makes the current version when you delete by key alone in a versioned bucket; retrieval then returns 404 Not Found
Server-side encryption	S3 encrypting objects at rest at the object level — SSE-S3, SSE-KMS, or SSE-C, depending on who manages the keys

TERM	DEFINITION
Bucket policy	A resource-based IAM policy attached to a bucket that grants granular, cross-account permissions on the bucket and its objects
Presigned URL	A time-limited URL (max 1 week) that grants a single PUT or GET on one object using the permissions of the user who created it

03 S3 OBJECT OPERATIONS

PUT/GET/DELETE are the core three; SELECT queries content

OPERATION	WHAT IT DOES	KEY DETAILS
PUT	Uploads an entire object to a bucket (no partial updates)	Needs write permission · single upload ≤ 5 GB · multipart required above 5 GB (max 5 TB)
GET	Retrieves an object from a bucket	Needs read access · fetch the whole object or a byte range
DELETE	Removes one or more objects	By key; in a versioned bucket, target a version ID or drop a delete marker
SELECT	Queries object contents with a SQL expression	Needs s3:GetObject · input as CSV, JSON, or Apache Parquet

04 MANAGING ACCESS: TWO POLICY TYPES

both grant permissions that are private by default

IDENTITY-BASED POLICIES <i>attached to identities</i> — Attached to IAM users, groups, and roles in your account — Grant those identities permission to act on AWS resources — Managed on the IAM side of the account	RESOURCE-BASED POLICIES <i>attached to the S3 resource</i> — Attached directly to your buckets and objects — Bucket policies grant granular, cross-account permissions on a bucket and its objects — ACLs grant basic read/write to other AWS accounts at bucket or object level
---	--

05 SERVER-SIDE ENCRYPTION AT REST

difference is who manages the keys

OPTION	KEYS MANAGED BY	REMEMBER
SSE-S3	Amazon S3	Unique per-object key; AES-256; the key itself is encrypted with a regularly rotated root key
SSE-KMS	AWS KMS	Envelope key needs extra permissions; adds an audit trail of key use; use a default or your own key
SSE-C	You (customer-provided)	You supply the keys; S3 encrypts on write and decrypts on access

06 CREATING A PRESIGNED URL

01 Supply your **security credentials** → **02** Name the **bucket** and **object key** → **03** Pick the **HTTP method** — PUT to upload, GET to download → **04** Set an **expiration** date and time (max 1 week) → **05** Share it — grants only that one action, with your permissions

- × “Bucket names only need to be unique in my account or Region.” — They are **globally unique across every AWS account**; once a bucket exists, no other account can reuse the name in any Region until it is deleted.
- × “I can rename a bucket or move it to another Region.” — Neither is possible: **the bucket name and Region are fixed at creation**, so choose carefully.
- × “Versioning can be switched back off.” — Once enabled, it can only be **suspended, never disabled** — and every stored version keeps incurring standard S3 charges.
- × “Deleting an object by key in a versioned bucket erases it.” — It only adds a **delete marker** as the new current version (the object returns **404**); earlier versions remain until you delete each **version ID**.
- × “Turning on encryption encrypts everything already in the bucket.” — S3 encrypts **only objects added after** encryption is enabled; existing objects are left unchanged.
- × “User-defined metadata can be named anything.” — Keys must begin with the **x-amz-meta-** prefix, and S3 **stores but does not process** user-defined metadata.
- × “Anything over 100 MB requires multipart upload.” — Past 100 MB multipart is **recommended**; it is **required only above 5 GB** (the single-PUT limit) and raises the max object size to 5 TB.
- × “A presigned URL is permanent and grants broad access.” — It is valid **only until its expiration (max 1 week)** and permits **just the one PUT or GET**, bounded by the creator's permissions.

08 SELF-QUIZ

answers are upside-down below

- Q1** For how many “nines” of durability is Amazon S3 designed?
- Q2** What two rules govern the length and character set of an S3 bucket name?
- Q3** What uniquely identifies an object within a bucket, and how many does each object have?
- Q4** What is the maximum size for a single-PUT upload, and above what size is multipart upload required?
- Q5** In a versioning-enabled bucket, what does a DELETE that specifies only the key create?
- Q6** Once versioning is enabled on a bucket, what is the only state change still available?
- Q7** Name the three server-side encryption options by who manages the keys.
- Q8** What prefix must every user-defined object-metadata key begin with?
- Q9** Which S3 object operation queries an object's contents using a SQL expression?
- Q10** What is the maximum length of time a presigned URL can remain valid?

ANSWER KEY (rotate the page)

Q1 11 nines — 99.999999999999999% **Q2** 3–63 characters; only lowercase letters, numbers, and hyphens (no uppercase or underscores) **Q3** the object key; exactly one per object **Q4** 5 GB single PUT; multipart required above 5 GB (max object 5 TB) **Q5** a delete marker (it becomes the current version; retrieval returns 404) **Q6** suspending it — versioning can never be disabled **Q7** SSE-S3 (S3-managed), SSE-KMS (KMS-managed), SSE-C (customer-provided) **Q8** x-amz-meta- **Q9** SELECT (SelectObjectContent) **Q10** one week