# **Simple Storage Service (S3)**

-unlimited storage

-0 bytes to 5 TB

S3 object:

1. Key – object name
2. Value – data itself made of sequence of bytes
3. Version id – object version
4. Metadata – additional information attached to object

S3 bucket: Holds objects; can have folders that hold objects

* universal namespace so bucket names must be unique
* all s3 buckets are PRIVATE by default when created

Access control configured using Bucket Policies (JSON) and Access Control List

S3 storage class: standard (default), intelligent tiering, standard infrequently accessed, one zone IA, glacier, glacier deep archive

S3 encryption

* Traffic between local host and S3 is through SSL/ TLS (secure sockets layer/ transport layer security)
* SSE server-side encryption has 3 types
* SSE-AES Advanced Encryption Standard; uses AES-256 algorithm
* SSE-KMS envelope encryption via AWS KMS (key management service) and you manage keys
* SSE-C customer provided key (you manage keys)
* Client-side encryption where you must encrypt own files before uploading to S3

S3 data consistency

* Read after write: able to read immediately after writing when new s3 object uploaded
* Eventual: when you overwrite or delete object, takes time to replicate to AZ (availability zone)

S3 cross region replication CRR

* Any object uploaded automatically replicated to another region; provides durability and disaster recovery for objects
* Must have versioning turned on both source and destination buckets
* Could replicate to another AWS account as well

S3 versioning

* Store all versions of an object in S3
* Once enabled, can only be suspended; not disabled

S3 life cycle management

* Automate the process of moving objects to storage classes or deleting it altogether
* Can be used in conjunction with versioning (both current and previous version)

S3 transfer acceleration

* Instead of loading into S3 bucket directly, users use distinct URL for an Edge Location that hastens the data transfer; Data arriving Edge Location is automatically routed to S3 over optimized network path known as Amazon Backbone Network

S3 pre-signed URL

* Generate URL that gives temporary access to an object to either upload or download object
* Used to provide access to private objects; for e.g. you have web app that needs to allow users to password protected portion of the app. In this case, web app generates pre-signed URL expiring in 5 seconds within which the user downloads the file

S3 MFA Delete (multi factor authentication)

* Ensures users cannot delete objects from a bucket unless they provide MFA code
* Use AWS CLI to turn on MFA; bucket must have versioning turned on
* Only bucket owner with root access can delete

Aws s3 ls

Aws s3 cp

Bucket policy generator – can be used to prevent from uploading files to the bucket.

S3 replicates data across at least 3 AZs

When a file is uploaded to S3 successfully, you will receive HTTP 200 code

Bucket policies are JSON documents that allows writing complex control access

ACLs are legacy method to grant access to objects and methods