

Simple Storage Service (S3) – REGIONAL

- Regional: All data
- Global: bucket names
- Supports BitTorrent for object smaller than 5gb
Object storage
- Traffic Acceleration from around the world

Buckets

- container for objects
- names are global and unique
- data is stored in regions
- bucket name max 63 lowercase letters, numbers, hyphens, periods

Objects

- stores data (bytes) and metadata
- max size 5TB (min 0b)
- metadata: system and user (specified at creation)

Keys

- max 1024 UTF-8 chars.
- unique within a bucket

Important

- No folders, key can contain backslashes:
bucket/some/di rectory/x.com – file name
- No hierarchy just prefixes and delimiters

Durability & Availability

Standard:

- 99.99999999% (11 9s) durability
- 99.99% (4 9s) availability

RRS:

- 99.99% (4 9s) durability
- 99.99% (4 9s) availability

Standard IA

- 99.99999999% (11 9s) durability
- 99.9% (3 9s) availability

Glacier

- 99.99999999% (11 9s) durability

Consistency

- eventual
- Read-After-Write on PUTS new objects
- Eventual for the rest
- You might see file after DELETE

Access Control

- ACL on object – does not allow to make all object publicly available (only single object)
- Bucket policy, restriction on AWS account, Ip Address, time
- MFA for delete
- pre-signed url for GET and PUT

Lifecycle Management

- Change storage class after some time
- Can delete files after expiring

Encryption

- In transit – SSL
- At rest:
 - SSE (server side encryption) s3 – managed by s3
 - SSE KMS – managed by s3 with additional controls over master key and access control
 - SSE C – customer provided keys
 - Client side encryption
- Encryption on Object/Version level
- You can encrypt object which already exists – go to properties and click encrypt

Versioning

- Can be enabled, but can only be suspended
- Multi Factor Delete – only from root account

Pre Signed Url

- time based access url to resource

Multipart upload

- recommended above 100 MB
- required above 5GB

Range get

- You can read only range of bytes from object

Cross region replication

- replicate only user initiated actions (can't chain cross region replications), it will not replicate files deleted by lifecycle
- Will only replicate new objects, not existing ones
- Metadata and ACLs are replicated

Event notifications

- setup on bucket level
- Targets:
 - SNS
 - SQS
 - Lambda
- Can be used to replace lost object in RRS

Logs

- contain ip, bucket, time, action, response
- delivered on a best-effort basis
- might be delayed

Performance

- You may need to randomize object names above 100 req/s

Static Website Hosting

- You can host static website
- You can have custom 404 error page
- CORS configuration for different domain
- bucket name has to be the same as your custom domain to set up CNAME

Glacier – Regional

Data is stored in Archives (think tar files) and organized in vaults (think folders)

Archives

- data stored in archives
- max size 40 TB
- unique archive ID - service generated
- immutable, can't be changed

Vaults

- containers for archives
- max 1000 vaults

Vault Locks

- for compliance
- you can specify WORM (Write Once Read Many) policy
- Once locked policy can no longer be changed

Encryption

- Encrypted by default