# AWS S3: Simple Storage Service

**Amazon S3 (Simple Storage Service)** provides safe, secure, highly-scalable object-based storage on the cloud.

You only pay for what you use, have unlimited storage, and the sizes of individual files can be anywhere between 0 bytes and 5 terabytes.

**S3** is one of the basic and important core systems in AWS.  When an object is successfully uploaded, you will receive a **HTTP 200 Code**.

With S3, you can easily change the storage classes and the encryption policies of the Objects and Buckets.  For redundancy, you can have contents replicated automatically by using [**Cross-Region Replication (CRR)**](https://docs.aws.amazon.com/AmazonS3/latest/dev/crr.html).

# Basic Features

* [**Lifecycle Management**](https://docs.aws.amazon.com/AmazonS3/latest/dev/object-lifecycle-mgmt.html)
* **Versioning**
* **Encryption**
* **Data Security** (using ACLs and Bucket Policies).

## “Objects” go into “Buckets”

When they say **Objects**, think Files – like images, HTML pages, .zip files.  Each individual object can be as large as 5TBs, and you can upload unlimited number of files.

**Buckets** are where you keep the **Objects**. Each Bucket exists in a “global namespace.”

This means that no two buckets in ***ALL*** of AWS can have an identical name.  This includes everyone else in the world who uses S3 – not just within your own account.

For example, I just went ahead and created an S3 Bucket called “awsnewbies.”  This means that no one else using S3 in all of AWS infrastructure has a Bucket called “awsnewbies.”

redundancy, you can have contents replicated automatically by using [**Cross-Region Replication (CR**](https://docs.aws.amazon.com/AmazonS3/latest/dev/crr.html)

The easiest analogy is your computer’s Folder (Bucket) where you keep your Files (Object), and you can’t have 2 Folders with the same name in the same level.

Access permissions can be set by Object level (ACL) or Bucket level (Bucket Policy).

## What’s in an Object?

Objects consist of **object data** and **metadata**.  **Metadata** is a set of name-value pairs that describe the object, such as “Department; Finance,” or “User; John.”

### Parts of an Object:

* [**Key**](https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingMetadata.html#object-keys): Name of object
* **Value**: Data
* **Version ID**: Used for versioning (different iterations of the same file)
* **Metadata**: “Data about data”
* **Subresources**
  + Access Control Lists (ACLs)
  + [Torrent](https://docs.aws.amazon.com/AmazonS3/latest/dev/S3Torrent.html)

# Availability and Durability of S3

Their durability guarantee is **99.999999999%** (commonly referred to as “eleven 9’s of durability“). This is how likely a file is to get corrupted.

Their availability guarantee is **99.99%**.  This is how likely a file is to be accessible or inaccessible.

# Data Consistency Model for S3

* **Read-After-Write Consistency** for [PUTS](https://docs.aws.amazon.com/AmazonS3/latest/API/RESTObjectPUT.html) of new objects(Adds an object to a bucket. You must have WRITE permissions on a bucket to add an object to it.)
  + The changes are immediate when you upload a new file
* **Eventual Consistency** for overwrite PUTS and DELETES
  + Edits and deletions can take time to propagate, which means you might get 2 versions for a while when you try to load the file until update is fully completed

Basically, if you uploaded a new Object, you can immediately see it, but if you edited or deleted an Object, you might get the pre or post edits for a while.

# Storage Classes

## Standard

* Standard: quick retrieval
* Stored redundantly across multiple devices and facilities (AZs)
* Designed to sustain 2 facilities loss at the same time
* 99.99% availability

## Standard-IA (Infrequently Access)

* For infrequently accessed data that require rapid access when necessary (same speed as S3 Standard)
* Lower fee than S3, but charged retrieval fee
* Can exist in the same bucket as S3 Standard
* Data stored in minimum of 3 AZs
* 99.9% availability

## One Zone-IA

* Lower-cost option for infrequently accessed data (same speed as S3 Standard/-IA)
* Only in one AZ – data isn’t resilient, but 20% cheaper than S3 Standard-IA
* Lower per GB storage and retrieval price than S3 Standard/-IA
* Can exist in the same bucket as S3 Standard/-IA
* 99.5% availability

## Glacier

* [Independent AWS service](https://aws.amazon.com/glacier/)
* Low cost and optimal for archival purposes
* Resilient to 1 entire AZ destruction
* 3 retrieval options:
  + Expedited retrieval: few minutes
  + Standard retrieval: 3-5 hours
  + Bulk retrieval: 5-12 hours

## Storage Class Comparison

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Standard** | **Standard-IA** | **One Zone-IA** | **Glacier** |
| **Designed for Durability** | 99.999999999% | 99.999999999% | 99.999999999% | 99.999999999% |
| **Designed for Availability** | 99.99% | 99.9% | 99.5% | N/A |
| **Availability SLA** | 99.9% | 99% | 99% | N/A |
| **Availability Zones** | >3 | >3 | 1 | >3 |
| **Minimum Capacity Charge per Object** | N/A | 128KB | 128KB | N/A |
| **Minimum Storage Duration Charge** | N/A | 30 days | 30 days | 90 days |
| **Retrieval Fee** | N/A | per GB retrieved | per GB retrieved | per GB retrieved |
| **First Byte Latency** | milliseconds | milliseconds | milliseconds | select minutes or hours |
| **Storage Type** | Object | Object | Object | Object |
| **Lifecycle Transitions** | Yes | Yes | Yes | Yes |

(Source: [Amazon S3 Storage Classes](https://aws.amazon.com/s3/storage-classes/))

# Charges and Billing

You can upload unlimited number of files that are up to 5TB in size each.  But that doesn’t mean that everything is free.  Here are some ways you can get charged for using S3

* **Storage:** You pay for storage at rate based on the objects’ sizes, how long they are stored, and the storage class.
* **Requests:** You pay for requests put upon the objects, including lifecycle requests.
* **Retrievals:** You pay for retrieving objects in every storage class except S3 Standard.
* **Early Deletes:** You pay for deleting objects in SA Standard-IA/One Zone-IA/Glacier before the minimum storage commitment
* **Storage Management:** You pay for storage management enabled on the account’s buckets (ie: Amazon S3 inventory, analytics, object tagging)
* **Data Transfer:** Transferring data from one region to another (Cross-Region Replication)
* **Transfer Acceleration:** Fast and secure transfer of files over long distances between end users and S3 bucket using CloudFront
* **Bandwidth:** You pay for bandwidth in/out of S3 and data transferred using [**S3 Transfer Acceleration**](https://docs.aws.amazon.com/AmazonS3/latest/dev/transfer-acceleration.html) EXCEPT:
  + Data transferred in from the internet
  + Data transferred out to [EC2](https://awsnewbies.com/ec2/) instance (when EC2 instance is in same region as S3 Bucket)
  + Data transferred out to [CloudFront](https://awsnewbies.com/cloudfront/)

# Security

## Encryption

* **Client Side Encryption**
* **Server Side Encryption**
  + **SSE-S3:** S3 Managed Keys
  + **SSE-KMS:** Key Management Service
  + **SSE-C:** Customer Provided Keys

## Access Control

By default, all buckets and objects are set to be private.

* **Access Control List:** Bucket and File Level
* **Bucket Policy:** Bucket Level

# Versioning

* Once you enable versioning, you can only suspend; never disable
* S3 will keep the files for every version, so should be cognizant of costs associated with keeping large file versions
* Versioning stores all versions of an object, including all writes and deletes
* MFA Delete Capability: protects against accidental deletion by requiring multi-factor authentication
* Integrates with Lifecycle rules

# Cross-Region Replication

* Versioning must be enabled for both source and destination buckets
* Only for new objects are replicated
* Regions must be different (cross-region)
* Cannot daisy-chain to multiple buckets
* Use [**AWS CLI**](https://aws.amazon.com/cli/)to transfer existing objects
  + aws s3 cp –recursive s3://[source bucket] s3://[destination bucket]
* Deletion marker is replicated, but when the deletion marker or a version is deleted, that action is not replicated

# Host a Static Website

If you have a static website (as opposed to [dynamic](https://rocketmedia.com/blog/static-vs-dynamic-websites)), you can host the whole thing on Amazon Simple Storage Service!

I’ve written an article on a very quick 5 minute process to get your static website up and running:

[**How to Host a Static Website with S3**](https://awsnewbies.com/static-website-s3/)