



# Amazon - S3

## What is Amazon S3 ?

“Amazon S3 (Simple Storage Service) is a scalable, high-speed, low-cost web-based service designed for online backup and archiving of data and application programs.”





# Amazon - S3

## ☰ Amazon - S3 Basics

- Amazon S3 is a Global Service.
- Amazon S3 stores data as an objects within resources called "buckets".
- User can store as many objects as they want within a bucket, and write, read, and delete objects from bucket.
- User can store objects virtually in any kind of format.
- Objects can be up to minimum 0 byte to maximum 5 terabytes in size.





# Amazon - S3

## Amazon - S3 BASICS

- S3 Charges for storage, request, Data transfer and Data Acceleration.
- S3 is a universal namespace, that is name must be unique globally E.g:  
<https://S3-eu-west-1.amazonaws.com/sherdilitacademy>.
- Put primarily means to uploads/updates on an object.
- Get primarily means to download the object.



# Amazon - S3



## Amazon - S3 Object

- **KEY:** The name of the object.
- **Value:** An object value can be any Sequence of the Bytes.
- **Version ID:** Important For versioning.
- **Metadata:** Data about data(object) you are storing.
- **Sub resources:**
  - Access control List



Object



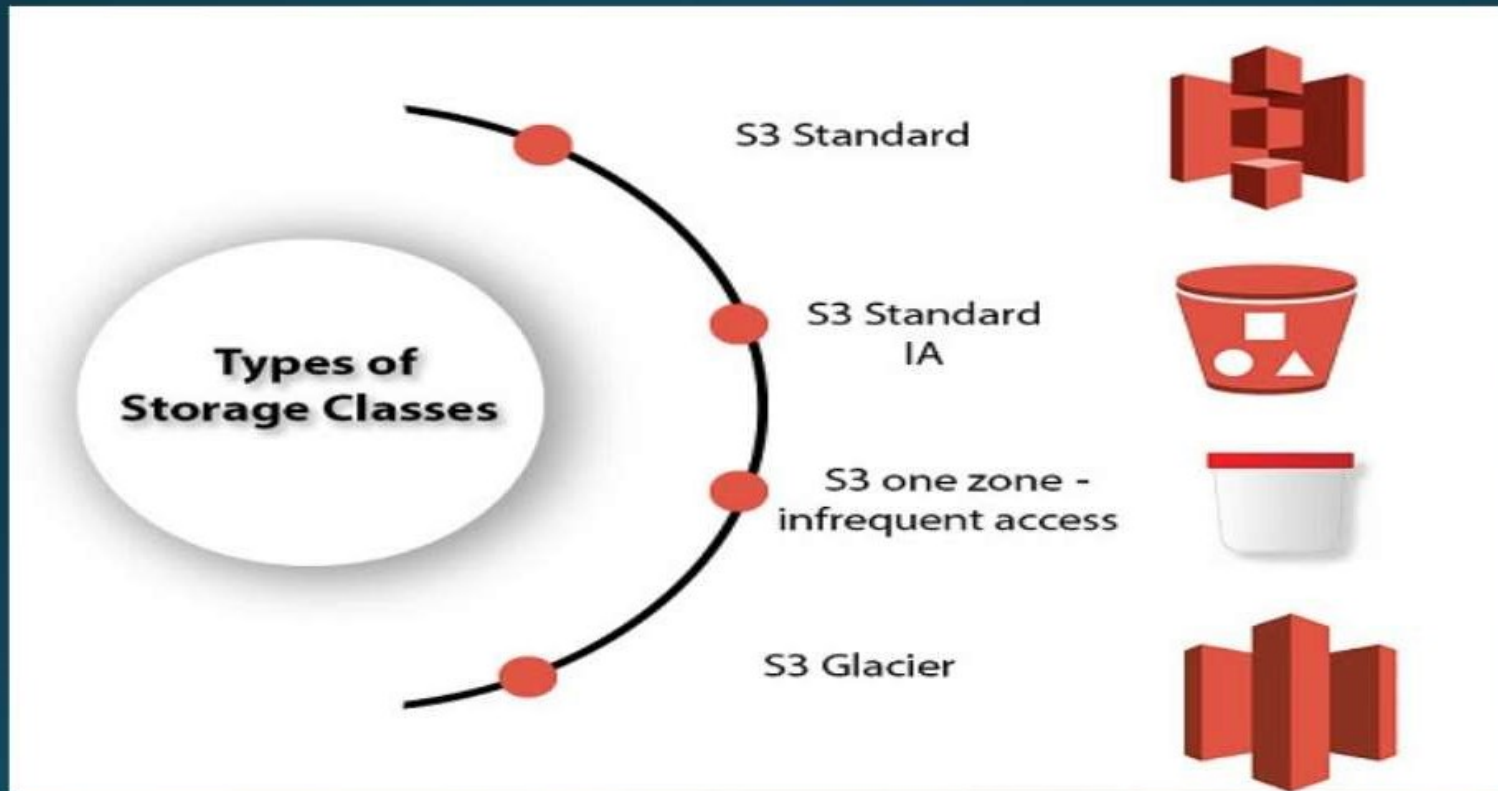
S3 Bucket



S3 bucket with  
Object



# Amazon - S3







# Amazon - S3

## ☰ Features Amazon S3 Storage Classes

Amazon S3 offers a range of storage classes designed for different use cases. These include S3 Standard for general-purpose storage of frequently accessed data, S3 Standard-Infrequent Access and S3 One Zone-Infrequent Access for long-lived.

### GENERAL PURPOSE

**S3 Standard** : S3 Standard offers high durability, availability, and performance object storage for frequently accessed data. Because it delivers low latency and high throughput.





# Amazon - S3

## ≡ Features AMAZON S3 STORAGE CLASSES

### UNKNOWN OR CHANGING ACCES

#### Amazon S3 Intelligent-Tiering:

The S3 Intelligent-Tiering storage class is designed to optimize costs by automatically moving data to the most cost-effective access tier, without performance impact or operational overhead.

It works by storing objects in two access tiers: one tier that is optimized for frequent access and another lower-cost tier that is optimized for infrequent access.





# Amazon - S3

## ≡ Features AMAZON S3 STORAGE CLASSES

### INFREQUENT ACCESS

#### S3 Standard-IA:

\_For Data that is accessed less frequently, but requires rapid access when needed,  
Lower fee than S3, but it will be charged for retrieval fee.

#### S3 One Zone -IA:

Is a Lower cost option for Infrequently accessed data, but do not require multiple  
Availability Zone data resilience.





# Amazon - S3

## ☰ Features AMAZON S3 STORAGE CLASSES

### ARCHIVE

#### Glaciers:

Very cheap but used for archival only, Expedited (1–5 Min), Standard (3–5 Hrs), Bulk (5–12 Hrs) or Provisioned Capacity Unit (fixed up-front fee to expedite retrievals).

#### Glacier Deep Archive :

This new storage class for Amazon Simple Storage Service (S3) is designed for long-term data archival and is the lowest cost storage from any cloud provider, retrieval options are Standard (Within 12 Hrs) or Bulk (Within 48 Hrs).





# Amazon - S3

## ☰ Features AMAZON S3 STORAGE CLASSES

### Storage to your On-Premises

#### S3 on Outposts:

Ideal for workloads that require low latency access to on-premises systems, local data processing, or local data storage. Using the S3 APIs and features available in AWS Regions today, S3 on Outposts makes it easy to store and retrieve data on your Outpost, as well as secure the data, control access, tag, and report on it.





# Amazon - S3

## ☰ Features STORAGE MANAGEMENT

**S3 Batch Operations:** Copies objects between buckets, replace object tag sets, modify access controls, and restore archived objects from Amazon S3 Glacier, with a single S3 API request or a few clicks in the Amazon S3 Management Console.

**S3 Versioning:** You can easily preserve, retrieve, and restore every version of an object stored in Amazon S3, which allows you to recover from unintended user actions and application failures.

**Multi-Factor Authentication Delete:** S3 provides additional security with MFA Delete. When enabled, this feature requires the use of a multi-factor authentication device to delete objects stored in S3 to help protect previous versions of objects.







# Amazon - S3

## ≡ Features STORAGE MANAGEMENT

**S3 Object Lock:** Enforce write-once-read-many (WORM) policies with S3 Object Lock.

**S3 Cross-Region Replication (CRR):** You can replicate objects (and their respective metadata and object tags) into other AWS Regions for reduced latency, compliance, security, disaster recovery, and other use cases. S3 CRR is configured to a source S3 bucket and replicates objects into a destination bucket in another AWS Region.







# Amazon - S3

## ☰ Features STORAGE MONITORING

### AWS Cost Allocation Reports:

You can apply tags to S3 buckets in order to allocate costs across multiple business dimensions (such as cost centres, application names, or owners), and then use AWS Cost Allocation Reports to view usage and costs aggregated by the bucket tags.

### Storage Class Analysis:

Storage Class Analysis observes usage patterns to detect infrequently accessed storage to help transition the right objects from the S3 Standard storage class to the S3 Standard-IA, S3 One Zone-IA classes.





# Amazon - S3



## Features STORAGE MONITORING

### Amazon CloudWatch Metrics for S3:

S3's integration with Amazon CloudWatch helps to improve end-user experience by providing integrated monitoring and alarming on a host of different metrics.

### AWS CloudTrail Management & Data Events for S3:

AWS CloudTrail use to capture bucket-level (Management Events) and object-level API activity (Data Events) on S3 object.

### Event Notifications:

S3 Event Notifications can be sent in response to actions taken on objects uploaded or stored in S3 Bucket through either **Amazon SNS** or **Amazon SQS** or delivered directly to **AWS Lambda** to invoke AWS Lambda functions.





# Amazon - S3

## ☰ Features ACCESS MANAGEMENT

To protect your data in Amazon S3, by default, users only have access to the S3 resources they create. You can grant access to other users by using one or a combination of the following access management features:

### AWS Identity and Access Management:

IAM to create users and manage their respective access.

Access Control Lists: (ACLs) to make individual objects accessible to other AWS Account users

### Bucket policies

To configure permissions for all objects within a single S3 bucket







# Amazon - S3

## ☰ Features SECURITY

### VPC Endpoints:

The data between a VPC and S3 is transferred within the Amazon network, helping protect instances from Internet traffic. User can control what buckets, requests, users, or groups are allowed through a specific VPC endpoint.

### Encryption:

Amazon S3 will automatically encrypt the data on write and decrypt data on retrieval. When Amazon S3 SSE encrypts data at rest.

- It uses Advanced Encryption Standard (AES) 256-bit symmetric keys.
- if user choose server-side encryption with Amazon S3, there are three ways to manage the encryption keys.







# Amazon - S3

## Hands-On Lab

1. Create S3 bucket with unique name.
2. Create & enable Versioning, encryption & tags.
3. Create S3 bucket policy & apply on bucket.
4. Deploy static website hosting & verify.
5. Create life cycle rule.
6. Change S3 storage types

