



AMITY SCHOOL OF ENGINEERING & TECHNOLOGY

(Academic Year 2022-23)

LAB-4

Student Name: Mohammad Faraz M Khan

Class: B.Tech(CSE) Semester: 7

Enrollment Number: A70405219039

Faculty In-charge

Department of CSE

ASET, AUM

AIM: a) Create Bucket, upload text file and image file b)

Enable the public access of object

c) Create version of text file and image file and check for deletion process.

d) Explore S3 storage classes.

1(a). Creating a Bucket

Sign in to the AWS Management Console and open the Amazon S3 console.

2. Choose Create bucket.

The Create bucket wizard opens.

3. In Bucket name, enter a DNS-compliant name for your bucket.

The bucket name must:

Be unique across all of Amazon S3.

Be between 3 and 63 characters long.

Not contain uppercase characters.

Start with a lowercase letter or number.

4. After you create the bucket, you cannot change its name.

5. In Region, choose the AWS Region where you want the bucket to reside.

6. Under Object Ownership, to disable or enable ACLs and control ownership of objects uploaded in your bucket, choose one of the following settings:

ACLs disabled

Bucket owner enforced – ACLs are disabled, and the bucket owner automatically owns and has full control over every object in the bucket. ACLs no longer affect permissions to data in the S3 bucket. The bucket uses policies to define access control.

ACLs enabled

Bucket owner preferred – The bucket owner owns and has full control over new objects that other accounts write to the bucket with the bucket-owner-full-control canned ACL.

Object writer – The AWS account that uploads an object owns the object, has full control over it, and can grant other users access to it through ACLs.

7. In Bucket settings for Block Public Access, choose the Block Public Access settings that you want to apply to the bucket.

8. Choose Create bucket.

Create bucket [Info](#)

Buckets are containers for data stored in S3. [Learn more](#)

General configuration

Bucket name

Bucket name must be globally unique and must not contain spaces or uppercase letters. [See rules for bucket naming](#)

AWS Region

US East (N. Virginia) us-east-1

Copy settings from existing bucket - *optional*

Only the bucket settings in the following configuration are copied.

Choose bucket

Object Ownership [Info](#)

Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.

☒ **ACLs disabled (recommended)**

All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.

☐ **ACLs enabled**

Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.

Object Ownership

Bucket owner enforced

Block Public Access settings for this bucket

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to this bucket and its objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to this bucket or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

☒ Block *all* public access

Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

☒ Block public access to buckets and objects granted through *new* access control lists (ACLs)

S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.

☒ Block public access to buckets and objects granted through *any* access control lists (ACLs)

S3 will ignore all ACLs that grant public access to buckets and objects.

☒ Block public access to buckets and objects granted through *new* public bucket or access point policies

S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.

☒ Block public and cross-account access to buckets and objects through *any* public bucket or access point policies

S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

Bucket Versioning

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. [Learn more](#)

Bucket Versioning

- ☐ Disable
- ☒ Enable

Tags (0) - optional

Track storage cost or other criteria by tagging your bucket. [Learn more](#)

No tags associated with this bucket.

Add tag

Default encryption

Automatically encrypt new objects stored in this bucket. [Learn more](#)

Server-side encryption

- ☒ Disable
- ☐ Enable

► Advanced settings

 After creating the bucket you can upload files and folders to the bucket, and configure additional bucket settings.

Cancel

Create bucket

Account snapshotStorage lens provides visibility into storage usage and activity trends. [Learn more](#)[View Storage Lens dashboard](#)**Buckets (3)** [Info](#)Buckets are containers for data stored in S3. [Learn more](#)

Copy ARN

Empty

Delete

Create bucket

< 1 >

	Name ▲	AWS Region ▼	Access ▼	Creation date ▼
<input type="radio"/>	faraz1bucket	Asia Pacific (Mumbai) ap-south-1	Objects can be public	October 19, 2022, 15:23:52 (UTC+05:30)
<input type="radio"/>	faraz2bucket	Asia Pacific (Mumbai) ap-south-1	Bucket and objects not public	October 19, 2022, 15:47:29 (UTC+05:30)
<input type="radio"/>	gfhfhg	Asia Pacific (Mumbai) ap-south-1	Public	October 19, 2022, 16:33:01 (UTC+05:30)

1(b).Uploading Files

After creating a bucket in Amazon S3, you're ready to upload an object to the bucket. An object can be any kind of file: a text file, a photo, a video, and so on.

To upload an object to a bucket

- 1.Open the Amazon S3 console.
- 2.In the Buckets list, choose the name of the bucket that you want to upload your object to.
- 4.On the Objects tab for your bucket, choose Upload.
- 5.Under Files and folders, choose Add files.
- 6.Choose a file to upload, and then choose Open.
- 7.Choose Upload.

Uploading an Image file

The screenshot shows the Amazon S3 console interface. The breadcrumb navigation is Amazon S3 > Buckets > gfhfhg > apple/ > preview.jpg. The file name 'preview.jpg' is displayed with an 'Info' link. Action buttons include 'Copy S3 URI', 'Download', 'Open', and 'Object actions'. Below this, there are tabs for 'Properties', 'Permissions', and 'Versions'. The 'Object overview' section displays the following details:

Owner 1d039ec82cbeceac7c9f26a022ad886fe3b4704452bddcd1b138d04776d07c27	S3 URI s3://gfhfhg/apple/preview.jpg
AWS Region Asia Pacific (Mumbai) ap-south-1	Amazon Resource Name (ARN) arn:aws:s3::gfhfhg/apple/preview.jpg
Last modified November 21, 2022, 13:18:23 (UTC+05:30)	Entity tag (Etag) 0d6e6cebb7147443dc7dcc72c458bc8b
Size 345.6 KB	Object URL https://gfhfhg.s3.ap-south-1.amazonaws.com/apple/preview.jpg
Type jpg	

At the bottom of the console, there is a footer with 'Feedback', a language selection prompt, copyright information for 2023, and links for 'Privacy', 'Terms', and 'Cookie preferences'.

Object management overview

The following bucket properties and object management configurations impact the behavior of this object.

Bucket properties

Bucket Versioning

When enabled, multiple variants of an object can be stored in the bucket to easily recover from unintended user actions and application failures.

Enabled

Object Lock

When enabled, this object will be prevented from being deleted or overwritten until the hold is explicitly removed.

Disabled

Object Lock retention mode

In governance mode, users can't overwrite or delete this object or alter its lock settings unless they have special permissions. In compliance mode the object can't be overwritten or deleted by any user, including the root user in your AWS account.

Disabled

Default retention period

Objects will be prevented from being overwritten or deleted for the duration of the retention period.

-

Management configurations

Replication status

When a replication rule is applied to an object the replication status indicates the progress of the operation.

-

[View replication rules](#)

Expiration rule

You can use a lifecycle configuration to define expiration rules to schedule the removal of this object after a pre-defined time period.

-

Expiration date

The object will be made noncurrent and generate a delete marker on this date.

-

Storage class

Amazon S3 offers a range of storage classes designed for different use cases. [Learn more](#) or see [Amazon S3 pricing](#)

Edit

Storage class

Standard

Server-side encryption settings

Server-side encryption protects data at rest. [Learn more](#)

Edit

Default encryption

Disabled

Server-side encryption

None

Additional checksums

Checksum functions are used for additional data integrity verification of new objects. [Learn more](#)

Additional checksums

Off

Tags (0)

Track storage cost of other criteria by tagging your objects. [Learn more](#)

Edit

Key

Value

No tags associated with this resource.

Metadata (1)

Metadata is optional information provided as a name-value (key-value) pair. [Learn more](#)

Edit

Type

Key

Value

System defined

Content-Type

image/jpeg

Object Lock

Store objects using a write-once-read-many (WORM) model to help you prevent objects from being deleted or overwritten for a fixed amount of time or indefinitely. [Learn more](#)

Object Lock

Disabled

Amazon S3 currently does not support enabling Object Lock after a bucket has been created. To enable Object Lock for this bucket, contact [Customer Support](#)

Enabling Public Access

1. Open the Amazon S3 console.
2. From the list of buckets, choose the bucket with the objects that you want to update.
3. Navigate to the folder that contains the objects.
4. From the object list, select all the objects that you want to make public.
5. Choose Actions, and then choose Make public.
6. In the Make public dialog box, confirm that the list of objects is correct.
7. Choose Make public.

Before enabling public access

Objects

Properties

Permissions

Metrics

Management

Access Points

Permissions overview

Access

Bucket and objects not public

Block public access (bucket settings)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

Edit

Block all public access

On

Individual Block Public Access settings for this bucket

Bucket policy

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. [Learn more](#)

EditDelete

Public access is blocked because Block Public Access settings are turned on for this bucket

To determine which settings are turned on, check your Block Public Access settings for this bucket. [Learn more about using Amazon S3 Block Public Access](#)

No policy to display.

Copy

Object Ownership [Info](#)

[Edit](#)

Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.

Object Ownership

Bucket owner enforced

ACLs are disabled. All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.

Access control list (ACL) [Edit](#)

Grant basic read/write permissions to other AWS accounts. [Learn more](#)



This bucket has the bucket owner enforced setting applied for Object Ownership

When bucket owner enforced is applied, use bucket policies to control access. [Learn more](#)

Grantee	Objects	Bucket ACL
Bucket owner (your AWS account) Canonical ID: b1f2c8b707fa4e51eed66c527e588d3b03eb7013e6872f9d10f4ca932d509164	List, Write	Read, Write
Everyone (public access) Group: http://acs.amazonaws.com/groups/global/AllUsers	-	-
Authenticated users group (anyone with an AWS account) Group: http://acs.amazonaws.com/groups/global/AuthenticatedUsers	-	-
S3 log delivery group Group: http://acs.amazonaws.com/groups/s3/LogDelivery	-	-

Cross-origin resource sharing (CORS) [Edit](#)

The CORS configuration, written in JSON, defines a way for client web applications that are loaded in one domain to interact with resources in a different domain. [Learn more](#)

No configurations to display

Copy

Block all public access is enabled for the bucket

Edit Block public access (bucket settings) [Info](#)

Block public access (bucket settings)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

☐ Block all public access

Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

☐ Block public access to buckets and objects granted through *new* access control lists (ACLs)

S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.

☐ Block public access to buckets and objects granted through *any* access control lists (ACLs)

S3 will ignore all ACLs that grant public access to buckets and objects.

☐ Block public access to buckets and objects granted through *new* public bucket or access point policies

S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.

☐ Block public and cross-account access to buckets and objects through *any* public bucket or access point policies

S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

Cancel

Save changes

Edit Block public access (bucket settings)



Updating the Block Public Access settings for this bucket will affect this bucket and all objects within. This may result in some objects becoming public.

To confirm the settings, enter *confirm* in the field.

Cancel

Confirm

Block public access (bucket settings)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

Edit

Block all public access

Off

► Individual Block Public Access settings for this bucket

Adding Bucket Policy

We need to add bucket policy by making it

Step 1: Select Policy Type

A Policy is a container for permissions. The different types of policies you can create are an IAM Policy, an S3 Bucket Policy, an S VPC Endpoint Policy, and an SQS Queue Policy.

Select Type of Policy S3 Bucket Policy ▾

Step 3: Generate Policy

A *policy* is a document (written in the Access Policy Language) that acts as a container for one or more statements.

Add one or more statements above to generate a policy.

Amazon S3 > Buckets > gfhfhg

gfhfhg Info

Publicly accessible

Objects

Properties

Permissions

Metrics

Management

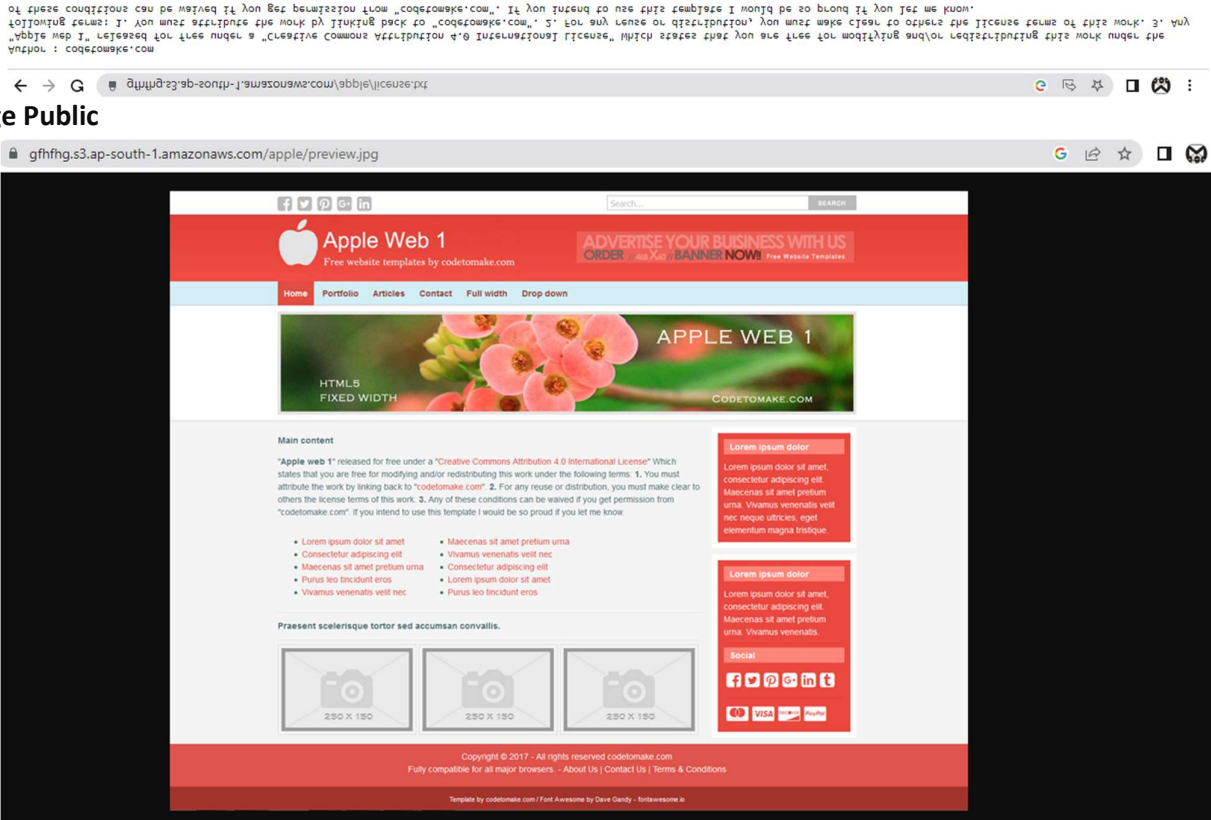
Access Points

Permissions overview

Access

 Public

Both text and image files can now be accessed using Object URL Text
Public



Versioning

Versioning in Amazon S3 is a means of keeping multiple variants of an object in the same bucket. You can use the S3 Versioning feature to preserve, retrieve, and restore every version of every object stored in your buckets. With versioning you can recover more easily from both unintended user actions and application failures.

Enabling/Disabling Versioning

To enable or disable versioning on an S3 bucket

1. Sign in to the AWS Management Console and open the Amazon S3 console.
2. In the Buckets list, choose the name of the bucket that you want to enable versioning for.
3. Choose Properties.
4. Under Bucket Versioning, choose Edit.
5. Choose Suspend or Enable, and then choose Save changes.

Edit Bucket Versioning [Info](#)

Bucket Versioning

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. [Learn more](#)

Bucket Versioning

☐ Suspend

This suspends the creation of object versions for all operations but preserves any existing object versions.

☒ Enable

Multi-factor authentication (MFA) delete

An additional layer of security that requires multi-factor authentication for changing Bucket Versioning settings and permanently deleting object versions. To modify MFA delete settings, use the AWS CLI, AWS SDK, or the Amazon S3 REST API. [Learn more](#)

Disabled

Cancel

Save changes

Amazon S3 > Buckets > gfhfhg

gfhfhg [Info](#)

Publicly accessible

Objects

Properties

Permissions

Metrics

Management


Access Points

Bucket overview

AWS Region

Asia Pacific (Mumbai) ap-south-1

Amazon Resource Name (ARN)

 arn:aws:s3:::gfhfhg

Creation date

October 19, 2022, 16:33:01 (UTC+05:30)

After enabling bucket versioning

Reuploading the same image file creates adds a new version object

Uploaded text file gets a version after enabling bucket versioning

Deleting Files

1. Sign in to the AWS Management Console and open the Amazon S3 console.
2. In the Bucket name list, choose the name of the bucket that you want to delete an object from.

3. To delete an object in a versioning-enabled bucket with versioning:

- **Off:** Amazon S3 creates a delete marker. To delete the object, select the object, and choose delete and confirm your choice by typing delete in the text field.
- **On:** Amazon S3 will permanently delete the object version. Select the object version that you want to delete, and choose delete and confirm your choice by typing permanently delete in the text field.

Deleting image file

The screenshot shows the AWS Management Console interface for deleting objects. At the top, the AWS logo and navigation bar are visible. Below the navigation bar, a message states: "same name that are uploaded before the delete action is completed will also be deleted." with a "Learn more" link. A blue information box contains the text: "Deleting the specified objects adds delete markers to them. If you need to undo the delete action, you can delete the delete markers. Learn more". Below this, the "Specified objects" section features a search bar with the placeholder "Find objects by name" and a table with one object: "preview.jpg" (jpg, 345.6 KB, last modified November 21, 2022, 13:18:23 (UTC+05:30)). The "Delete objects?" section prompts the user to "To confirm deletion, type delete in the text input field." and shows a text input field containing the word "delete". At the bottom right, there are "Cancel" and "Delete objects" buttons.

same name that are uploaded before the delete action is completed will also be deleted. [Learn more](#)

Deleting the specified objects adds delete markers to them
If you need to undo the delete action, you can delete the delete markers. [Learn more](#)

Specified objects

< 1 >

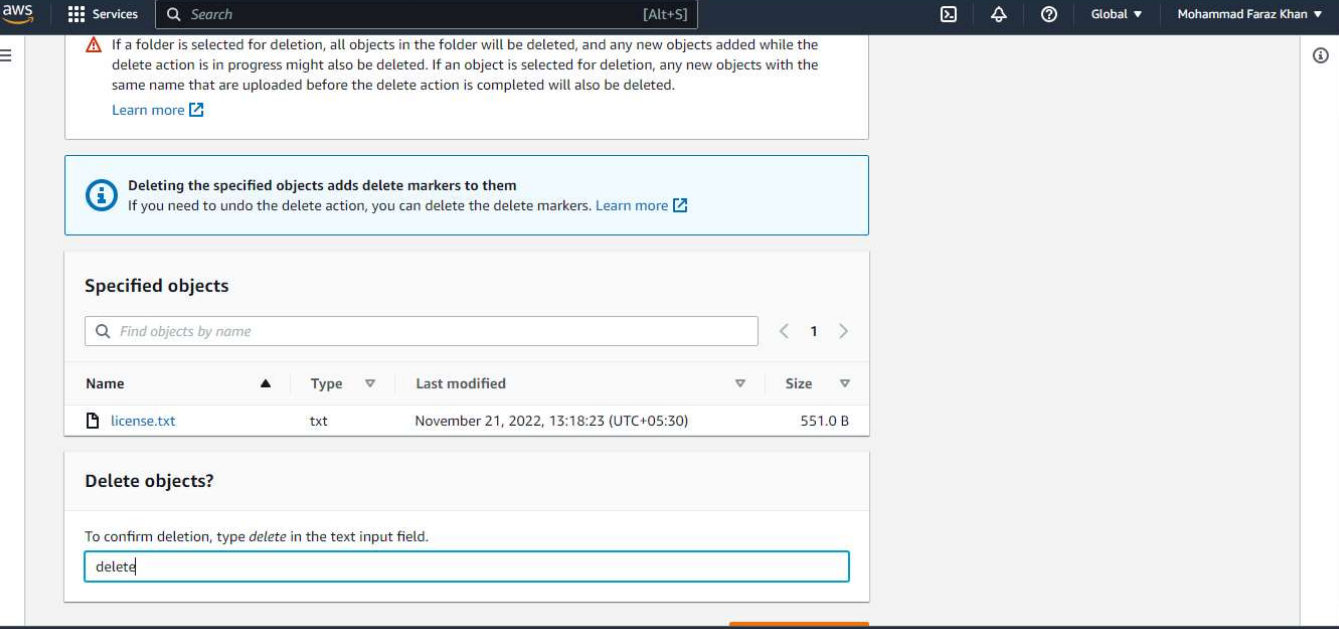
Name	Type	Last modified	Size
preview.jpg	jpg	November 21, 2022, 13:18:23 (UTC+05:30)	345.6 KB

Delete objects?

To confirm deletion, type *delete* in the text input field.

Cancel **Delete objects**

Deleting text file

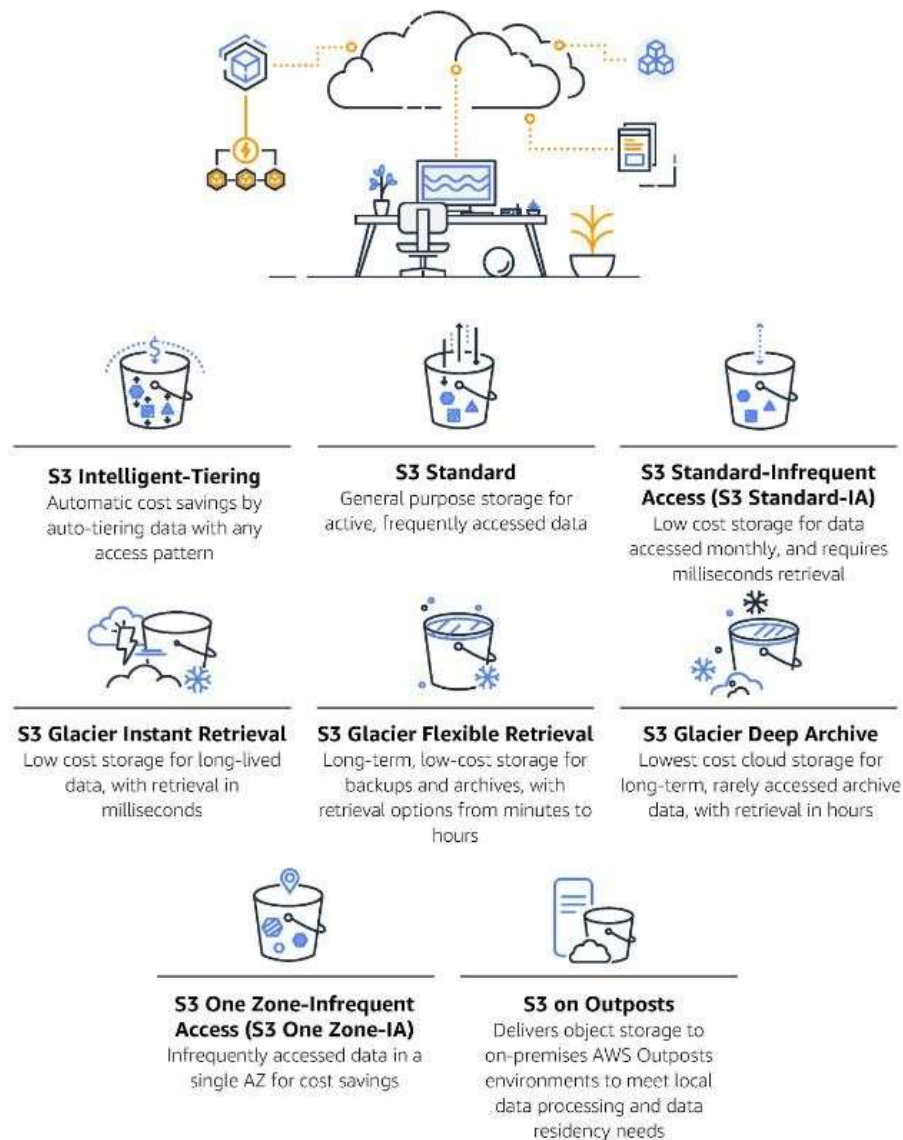


S3 Storage Classes

Amazon S3 offers a range of storage classes that you can choose from based on the data access, resiliency, and cost requirements of your workloads. S3 storage classes are purpose-built to provide the lowest cost storage for different access patterns. S3 storage classes are ideal for virtually any use case, including those with demanding performance needs, data residency requirements, unknown or changing access patterns, or archival storage.

The Amazon S3 Storage Classes

Purpose-built to provide the lowest cost storage for different access patterns, and virtually any use case



The S3 storage classes include S3 Intelligent-Tiering for automatic cost savings for data with unknown or changing access patterns, S3 Standard for frequently accessed data, S3 Standard-Infrequent Access (S3 Standard-IA) and S3 One Zone-Infrequent Access (S3 One Zone-IA) for less frequently accessed data, S3 Glacier Instant Retrieval for archive data that needs immediate access, S3 Glacier Flexible Retrieval (formerly S3 Glacier) for rarely accessed long-term data that does not require immediate access, and Amazon S3 Glacier Deep Archive (S3 Glacier Deep Archive) for long-term archive and digital preservation with retrieval in hours at the lowest cost storage in the cloud. If you have data residency requirements that can't be met by an existing AWS Region, you can use the S3 Outposts storage class to store your S3 data on premises. Amazon S3 also offers capabilities to manage your data throughout its lifecycle. Once an S3 Lifecycle policy is set, your data will automatically transfer to a different storage class without any changes to your application.

General purpose

Amazon S3 Standard (S3 Standard)

S3 Standard offers high durability, availability, and performance object storage for frequently accessed data. Because it delivers low latency and high throughput, S3 Standard is appropriate for a wide variety of use cases, including cloud applications, dynamic websites, content distribution, mobile and gaming applications, and big data analytics.

Key Features:

- Low latency and high throughput performance
- Designed for durability of 99.99999999% of objects across multiple Availability Zones
- Resilient against events that impact an entire Availability Zone
- Designed for 99.99% availability over a given year
- Supports SSL for data in transit and encryption of data at rest
- S3 Lifecycle management for automatic migration of objects to other S3 Storage Classes

Unknown or changing access

Amazon S3 Intelligent-Tiering (S3 Intelligent-Tiering)

Amazon S3 Intelligent-Tiering (S3 Intelligent-Tiering) is the first cloud storage that automatically reduces your storage costs on a granular object level by automatically moving data to the most cost-effective access tier based on access frequency, without performance impact, retrieval fees, or operational overhead. S3 Intelligent-Tiering delivers milliseconds latency and high throughput performance for frequently, infrequently, and rarely accessed data in the Frequent, Infrequent, and Archive Instant Access tiers. You can use S3 Intelligent-Tiering as the default storage class for virtually any workload, especially data lakes, data analytics, new applications, and user-generated content.

Key Features:

- Frequent, Infrequent, and Archive Instant Access tiers have the same low-latency and high-throughput performance of S3 Standard
- The Infrequent Access tier saves up to 40% on storage costs
- The Archive Instant Access tier saves up to 68% on storage costs
- Opt-in asynchronous archive capabilities for objects that become rarely accessed
- Deep Archive Access tier has the same performance as Glacier Deep Archive and saves up to 95% for rarely accessed objects
- Designed for durability of 99.99999999% of objects across multiple Availability Zones and for 99.9% availability over a given year
- Small monthly monitoring and auto tiering charge
- No operational overhead, no lifecycle charges, no retrieval charges, and no minimum storage duration
- Objects smaller than 128KB can be stored in S3 Intelligent-Tiering but will always be charged at the Frequent Access tier rates, and are not charged the monitoring and automation charge.

Infrequent access

Amazon S3 Standard-Infrequent Access (S3 Standard-IA)

S3 Standard-IA is for data that is accessed less frequently, but requires rapid access when needed. S3 StandardIA offers the high durability, high throughput, and low latency of S3 Standard, with a low per GB storage price and per GB retrieval charge. This combination of low cost and high performance make S3 Standard-IA ideal for long-term storage, backups, and as a data store for disaster recovery files.

Key Features:

- Same low latency and high throughput performance of S3 Standard
- Designed for durability of 99.999999999% of objects across multiple Availability Zones
- Resilient against events that impact an entire Availability Zone
- Data is resilient in the event of one entire Availability Zone destruction
- Designed for 99.9% availability over a given year
- Supports SSL for data in transit and encryption of data at rest
- S3 Lifecycle management for automatic migration of objects to other S3 Storage Classes

Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA)

S3 One Zone-IA is for data that is accessed less frequently, but requires rapid access when needed. Unlike other S3 Storage Classes which store data in a minimum of three Availability Zones (AZs), S3 One Zone-IA stores data in a single AZ and costs 20% less than S3 Standard-IA. S3 One Zone-IA is ideal for customers who want a lower-cost option for infrequently accessed data but do not require the availability and resilience of S3 Standard or S3 Standard-IA.

Key Features:

- Same low latency and high throughput performance of S3 Standard
- Designed for durability of 99.999999999% of objects in a single Availability Zone
- Designed for 99.5% availability over a given year
- Supports SSL for data in transit and encryption of data at rest
- S3 Lifecycle management for automatic migration of objects to other S3 Storage Classes

Archive

The [Amazon S3 Glacier storage classes](#) are purpose-built for data archiving, and are designed to provide you with the highest performance, the most retrieval flexibility, and the lowest cost archive storage in the cloud. You can choose from three archive storage classes optimized for different access patterns and storage duration. For archive data that needs immediate access, such as medical images, news media assets, or genomics data, choose the S3 Glacier Instant Retrieval storage class, an archive storage class that delivers the lowest cost storage with milliseconds retrieval. For archive data that does not require immediate access but needs the flexibility to retrieve large sets of data at no cost, such as backup or disaster recovery use cases, choose S3 Glacier Flexible Retrieval (formerly S3 Glacier), with retrieval in minutes or free bulk retrievals in 5—12 hours. To save even more on long-lived archive storage such as compliance archives and digital media preservation, choose S3 Glacier Deep Archive, the lowest cost storage in the cloud with data retrieval from 12—48 hours.

Amazon S3 Glacier Instant Retrieval

Amazon S3 Glacier Instant Retrieval is an archive storage class that delivers the lowest-cost storage for longlived data that is rarely accessed and requires retrieval in milliseconds. With S3 Glacier Instant Retrieval, you can save up to 68% on storage costs compared to using the S3 Standard-Infrequent Access (S3 Standard-IA) storage class, when your data is accessed once per quarter. S3 Glacier Instant Retrieval delivers the fastest access to archive storage, with the same throughput and milliseconds access as the S3 Standard and S3 Standard-IA storage classes.

Key Features:

- Data retrieval in milliseconds with the same performance as S3 Standard
- Designed for durability of 99.999999999% of objects across multiple Availability Zones
- Data is resilient in the event of the destruction of one entire Availability Zone
- Designed for 99.9% data availability in a given year
- 128 KB minimum object size
- S3 PUT API for direct uploads to S3 Glacier Instant Retrieval, and S3 Lifecycle management for automatic migration of objects

Amazon S3 Glacier Flexible Retrieval (Formerly S3 Glacier)

S3 Glacier Flexible Retrieval delivers low-cost storage, up to 10% lower cost (than S3 Glacier Instant Retrieval), for archive data that is accessed 1—2 times per year and is retrieved asynchronously. For archive data that does not require immediate access but needs the flexibility to retrieve large sets of data at no cost, such as backup or disaster recovery use cases, S3 Glacier Flexible Retrieval (formerly S3 Glacier) is the ideal storage class.

Key Features:

- Designed for durability of 99.999999999% of objects across multiple Availability Zones
- Data is resilient in the event of one entire Availability Zone destruction
- Supports SSL for data in transit and encryption of data at rest
- Ideal for backup and disaster recovery use cases when large sets of data occasionally need to be retrieved in minutes, without concern for costs
- Configurable retrieval times, from minutes to hours, with free bulk retrievals
- S3 PUT API for direct uploads to S3 Glacier Flexible Retrieval, and S3 Lifecycle management for automatic migration of objects

Amazon S3 Glacier Deep Archive

S3 Glacier Deep Archive is Amazon S3's lowest-cost storage class and supports long-term retention and digital preservation for data that may be accessed once or twice in a year. It is designed for customers—particularly those in highly-regulated industries, such as financial services, healthcare, and public sectors—that retain data sets for 7—10 years or longer to meet regulatory compliance requirements. S3 Glacier Deep Archive can also be used for backup and disaster recovery use cases, and is a cost-effective and easy-to-manage alternative to magnetic tape systems, whether they are on-premises libraries or off-premises services.

Key Features:

- Designed for durability of 99.999999999% of objects across multiple Availability Zones
- Lowest cost storage class designed for long-term retention of data that will be retained for 7-10 years
 - Ideal alternative to magnetic tape libraries
- Retrieval time within 12 hours
- S3 PUT API for direct uploads to S3 Glacier Deep Archive, and S3 Lifecycle management for automatic migration of objects

S3 on Outposts

S3 Outposts

Amazon S3 on Outposts delivers object storage to your on-premises AWS Outposts environment. 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. The S3 Outposts storage class is ideal for workloads with local data residency requirements, and to satisfy demanding performance needs by keeping data close to on-premises applications.

Key Features:

- S3 Object compatibility and bucket management through the S3 SDK
- Designed to durably and redundantly store data on your Outposts
- Encryption using SSE-S3 and SSE-C
- Authentication and authorization using IAM, and S3 Access Points
- Transfer data to AWS Regions using AWS DataSync □ S3 Lifecycle expiration actions