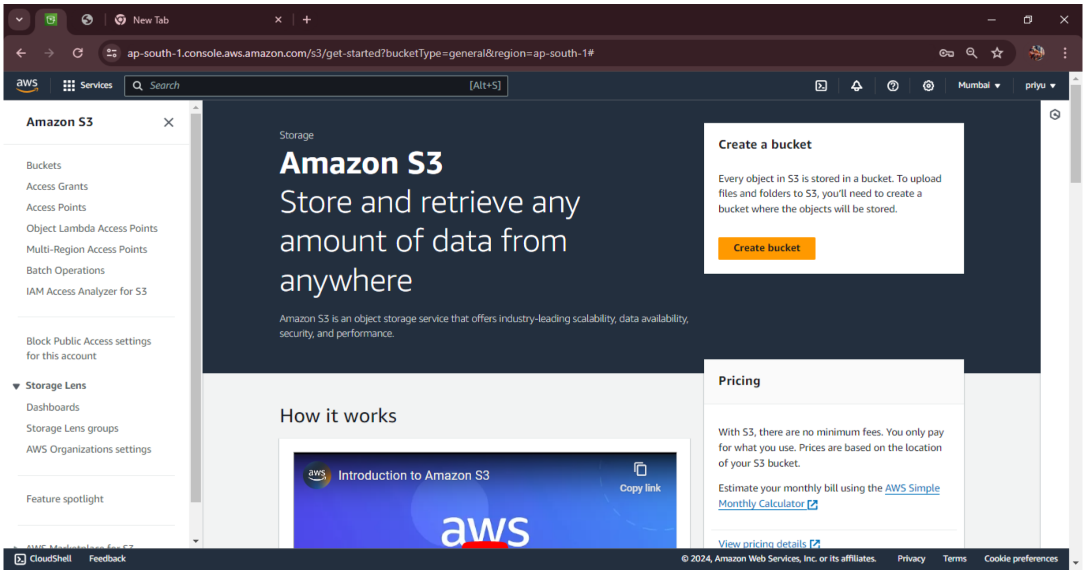
AMAZON S3(SIMPLE STORAGE SECURE)

Buckets are containers for data stored in S3

Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDK or Amazon S3 REST API

Step 1 create a bucket



ap-south-1.console.aws.amazon.com/s3/get-started?bucketType=general&region=ap-south-1#

Storage

Amazon S3

Store and retrieve any amount of data from anywhere

Amazon S3 is an object storage service that offers industry-leading scalability, data availability, security, and performance.

Create a bucket

Every object in S3 is stored in a bucket. To upload files and folders to S3, you'll need to create a bucket where the objects will be stored.

Create bucket

How it works

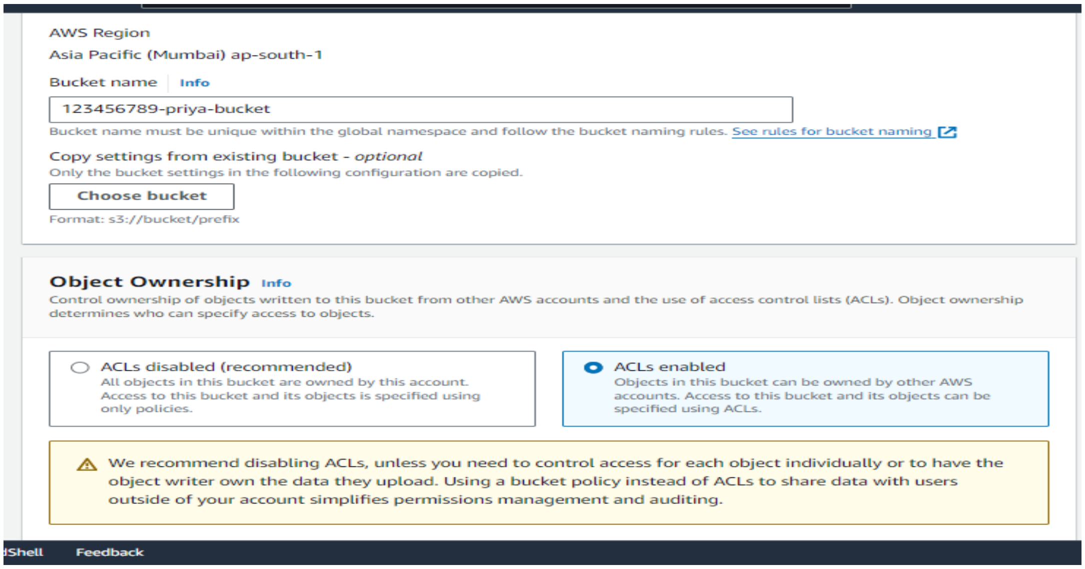
Pricing

With S3, there are no minimum fees. You only pay for what you use. Prices are based on the location of your S3 bucket.

Estimate your monthly bill using the AWS Simple Monthly Calculator

View pricing details

© 2024, Amazon Web Services, Inc. or its affiliates.



AWS Region
Asia Pacific (Mumbai) ap-south-1

Bucket name Info
123456789-priya-bucket
Bucket name must be unique within the global namespace and follow the bucket naming rules. See rules for bucket naming

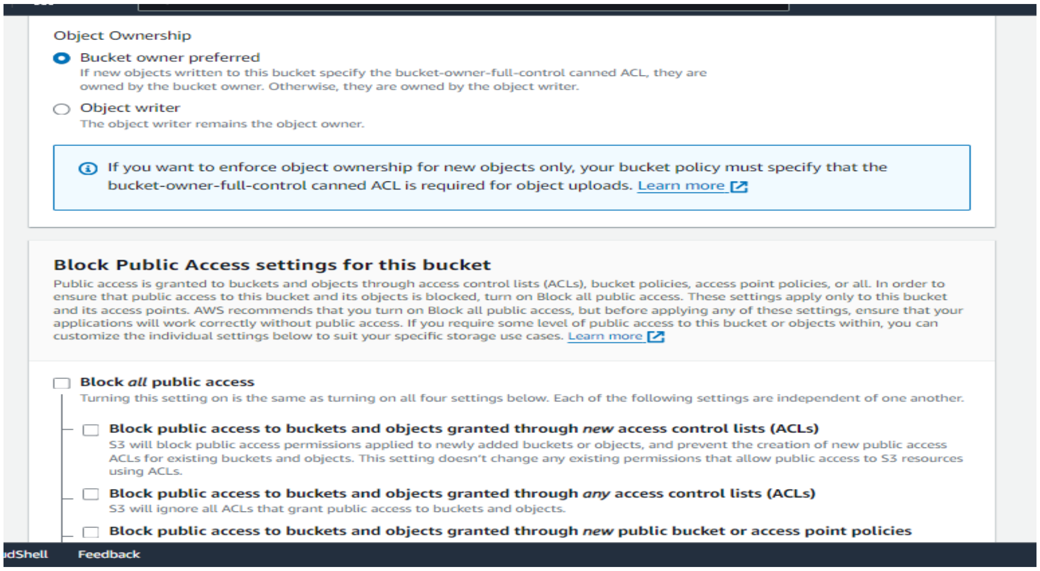
Copy settings from existing bucket - *optional*
Only the bucket settings in the following configuration are copied.
Choose bucket
Format: s3://bucket/prefix

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.

⚠ We recommend disabling ACLs, unless you need to control access for each object individually or to have the object writer own the data they upload. Using a bucket policy instead of ACLs to share data with users outside of your account simplifies permissions management and auditing.



Object Ownership

● Bucket owner preferred
If new objects written to this bucket specify the bucket-owner-full-control canned ACL, they are owned by the bucket owner. Otherwise, they are owned by the object writer.

○ Object writer
The object writer remains the object owner.

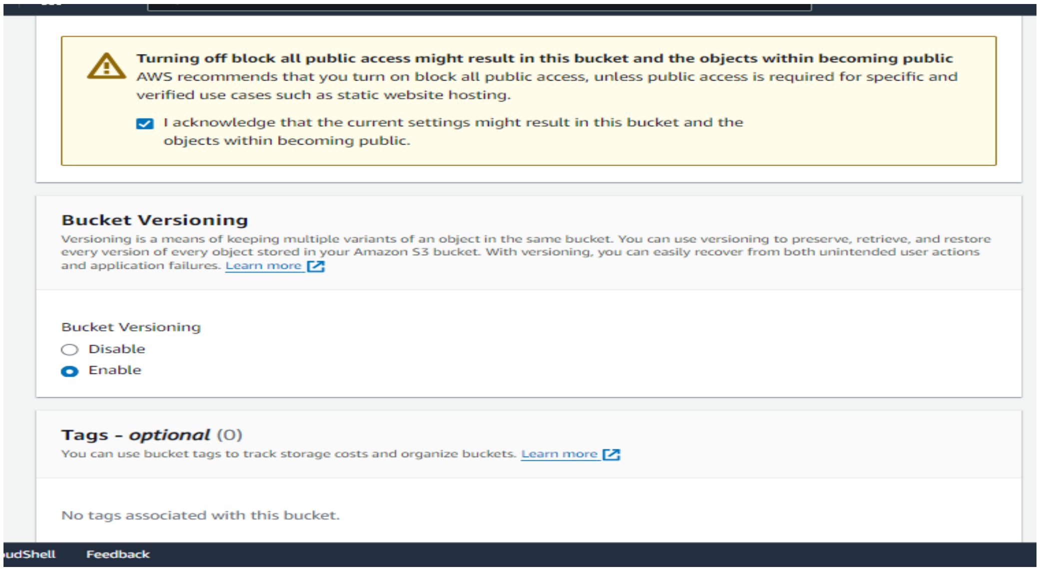
ⓘ If you want to enforce object ownership for new objects only, your bucket policy must specify that the bucket-owner-full-control canned ACL is required for object uploads. Learn more

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**



⚠ **Turning off block all public access might result in this bucket and the objects within becoming public**
AWS recommends that you turn on block all public access, unless public access is required for specific and verified use cases such as static website hosting.

☑ I acknowledge that the current settings might result in this bucket and the objects within becoming public.

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

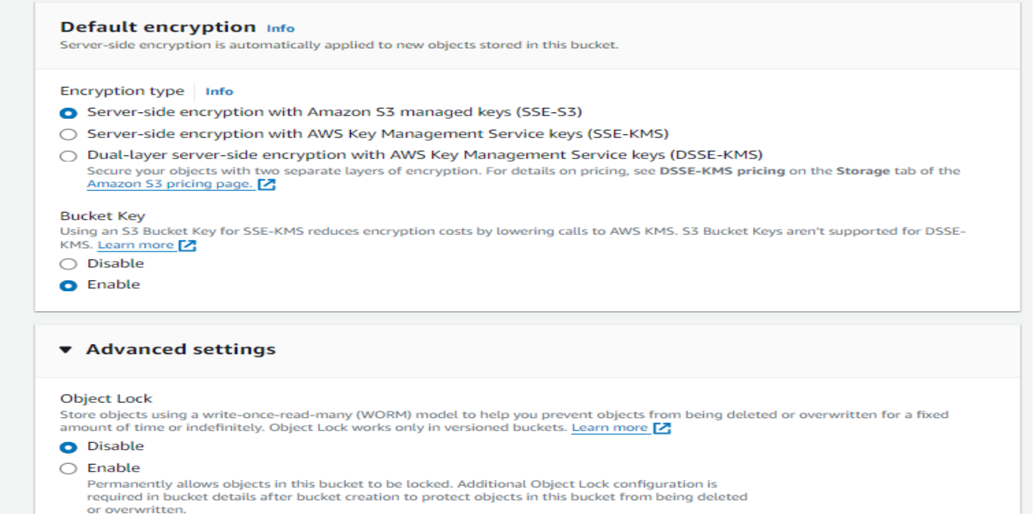
Bucket Versioning

○ Disable
● Enable

Tags - *optional* (0)

You can use bucket tags to track storage costs and organize buckets. Learn more

No tags associated with this bucket.



Default encryption Info

Server-side encryption is automatically applied to new objects stored in this bucket.

Encryption type | Info

● Server-side encryption with Amazon S3 managed keys (SSE-S3)
○ Server-side encryption with AWS Key Management Service keys (SSE-KMS)
○ Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)
Secure your objects with two separate layers of encryption. For details on pricing, see **DSSE-KMS pricing** on the **Storage** tab of the Amazon S3 pricing page.

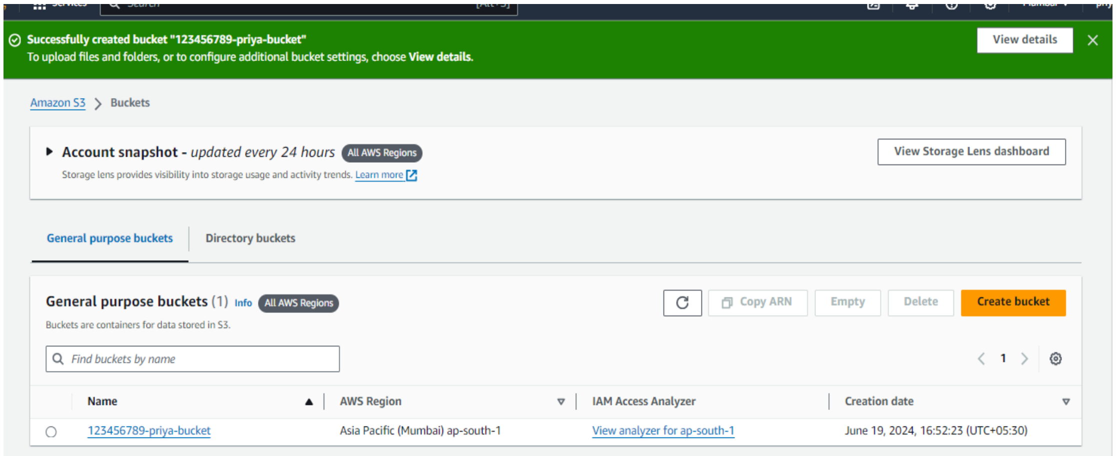
Bucket Key
Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-KMS. Learn more

○ Disable
● Enable

▼ Advanced settings

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. Object Lock works only in versioned buckets. Learn more

● Disable
○ Enable
Permanently allows objects in this bucket to be locked. Additional Object Lock configuration is required in bucket details after bucket creation to protect objects in this bucket from being deleted or overwritten.



Successfully created bucket "123456789-priya-bucket"
To upload files and folders, or to configure additional bucket settings, choose **View details**.

Amazon S3 > Buckets

Account snapshot - *updated every 24 hours* All AWS Regions

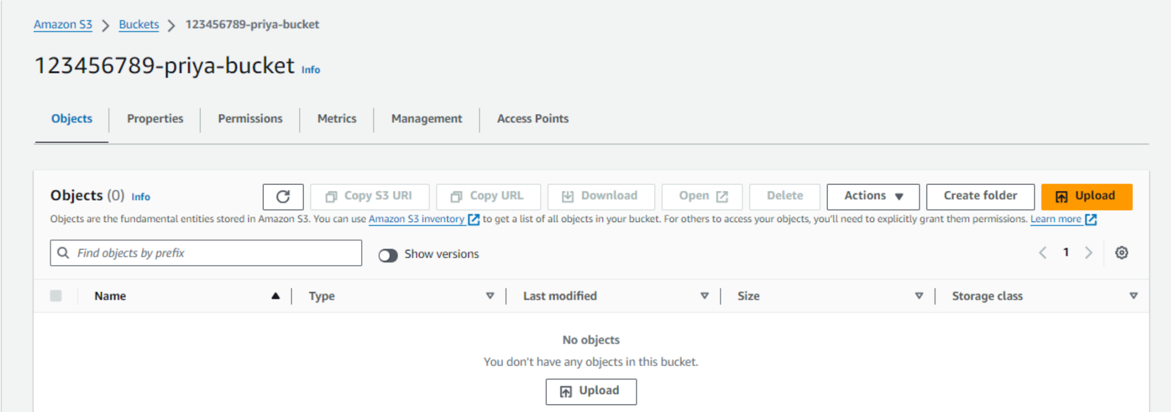
Storage lens provides visibility into storage usage and activity trends. Learn more

General purpose buckets (1) Info All AWS Regions

Buckets are containers for data stored in S3.

Name	AWS Region	IAM Access Analyzer	Creation date
○ 123456789-priya-bucket	Asia Pacific (Mumbai) ap-south-1	View analyzer for ap-south-1	June 19, 2024, 16:52:23 (UTC+05:30)

Step 2 upload files or folders in created bucket



Amazon S3 > Buckets > 123456789-priya-bucket

123456789-priya-bucket Info

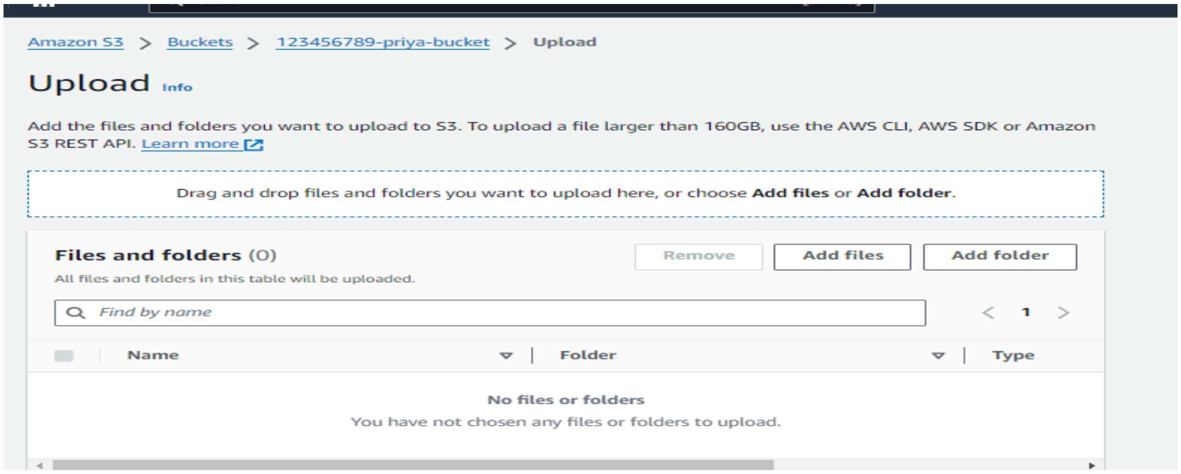
Objects (0) Info

Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

Name	Type	Last modified	Size	Storage class

No objects

You don't have any objects in this bucket.



Amazon S3 > Buckets > 123456789-priya-bucket > Upload

Upload Info

Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDK or Amazon S3 REST API. Learn more

Drag and drop files and folders you want to upload here, or choose **Add files** or **Add folder**.

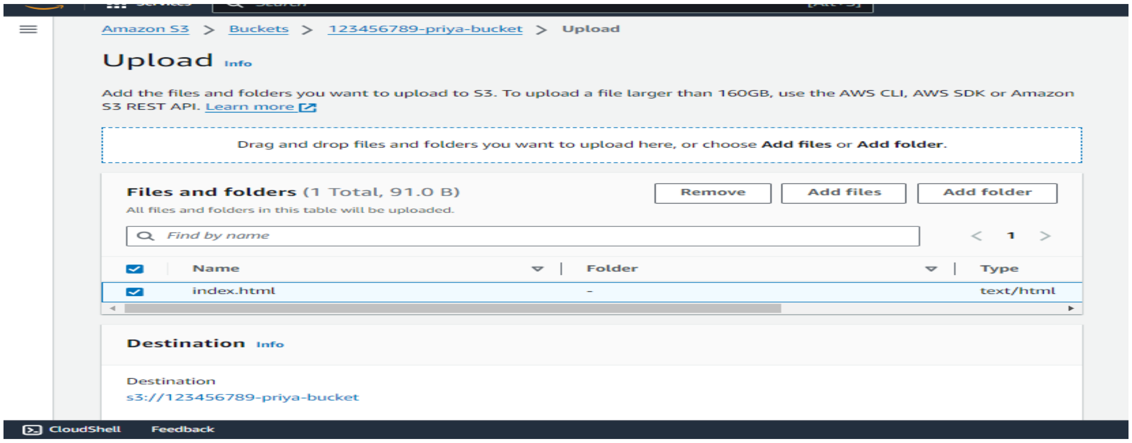
Files and folders (0)

All files and folders in this table will be uploaded.

Name	Folder	Type

No files or folders

You have not chosen any files or folders to upload.



Upload Info

Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDK or Amazon S3 REST API. Learn more

Drag and drop files and folders you want to upload here, or choose **Add files** or **Add folder**.

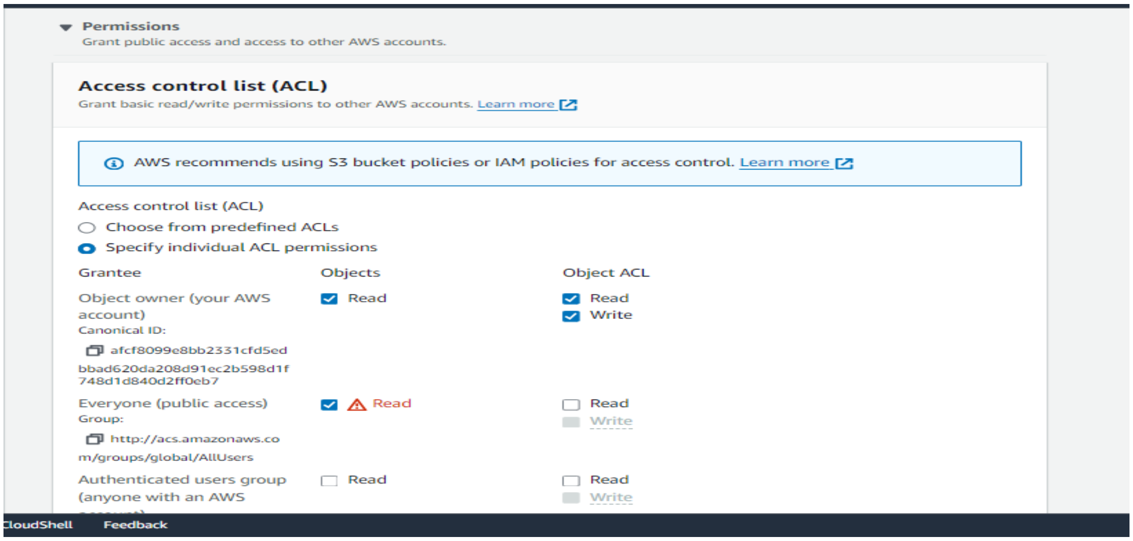
Files and folders (1 Total, 91.0 B)

All files and folders in this table will be uploaded.

☑	Name	Folder	Type
☑	index.html	-	text/html

Destination Info

Destination
s3://123456789-priya-bucket



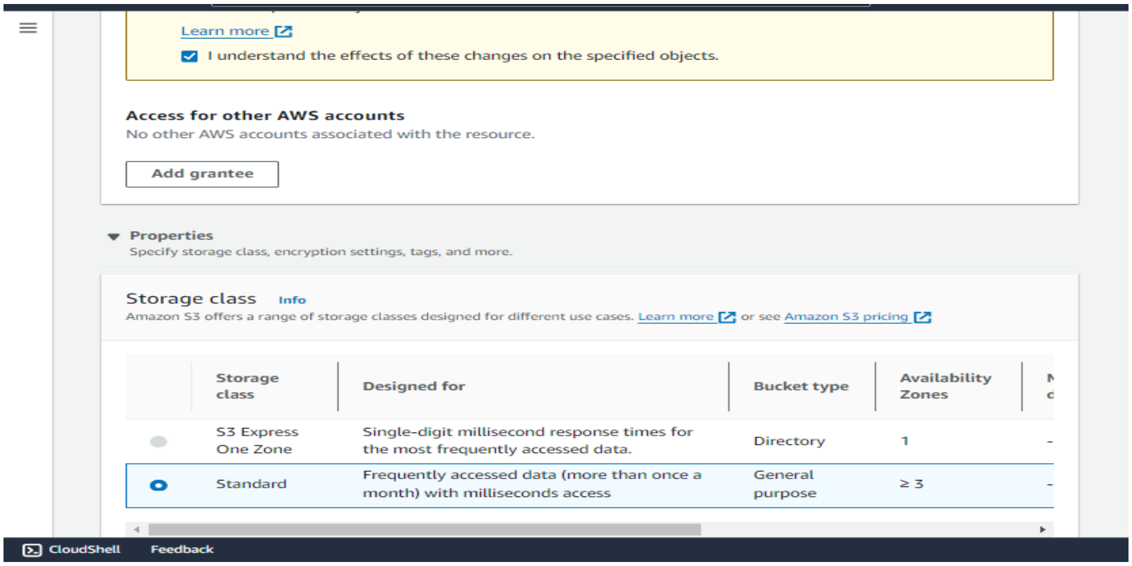
Permissions
Grant public access and access to other AWS accounts.

Access control list (ACL)
Grant basic read/write permissions to other AWS accounts. Learn more

AWS recommends using S3 bucket policies or IAM policies for access control. Learn more

Access control list (ACL)
○ Choose from predefined ACLs
● Specify individual ACL permissions

Grantee	Objects	Object ACL
Object owner (your AWS account) Canonical ID: afcf8099e8bb2331cfd5ed bbad620da208d91ec2b598d1f 748d1d840d2ff0eb7	☑ Read	☑ Read ☑ Write
Everyone (public access) Group: http://acs.amazonaws.com/groups/global/AllUsers	☑ ⚠ Read	□ Read □ Write
Authenticated users group (anyone with an AWS	□ Read	□ Read □ Write



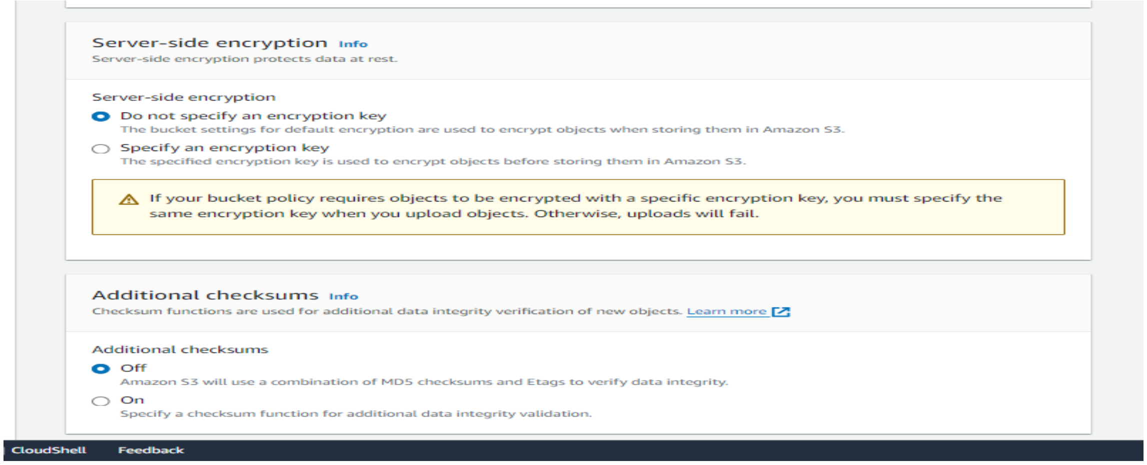
Learn more
☑ I understand the effects of these changes on the specified objects.

Access for other AWS accounts
No other AWS accounts associated with the resource.

Properties
Specify storage class, encryption settings, tags, and more.

Storage class Info
Amazon S3 offers a range of storage classes designed for different use cases. Learn more or see Amazon S3 pricing

	Storage class	Designed for	Bucket type	Availability Zones	M c
○	S3 Express One Zone	Single-digit millisecond response times for the most frequently accessed data.	Directory	1	-
●	Standard	Frequently accessed data (more than once a month) with milliseconds access	General purpose	≥ 3	-



Server-side encryption Info

Server-side encryption protects data at rest.

Server-side encryption

● Do not specify an encryption key

The bucket settings for default encryption are used to encrypt objects when storing them in Amazon S3.

○ Specify an encryption key

The specified encryption key is used to encrypt objects before storing them in Amazon S3.

⚠ If your bucket policy requires objects to be encrypted with a specific encryption key, you must specify the same encryption key when you upload objects. Otherwise, uploads will fail.

Additional checksums Info

Checksum functions are used for additional data integrity verification of new objects. Learn more

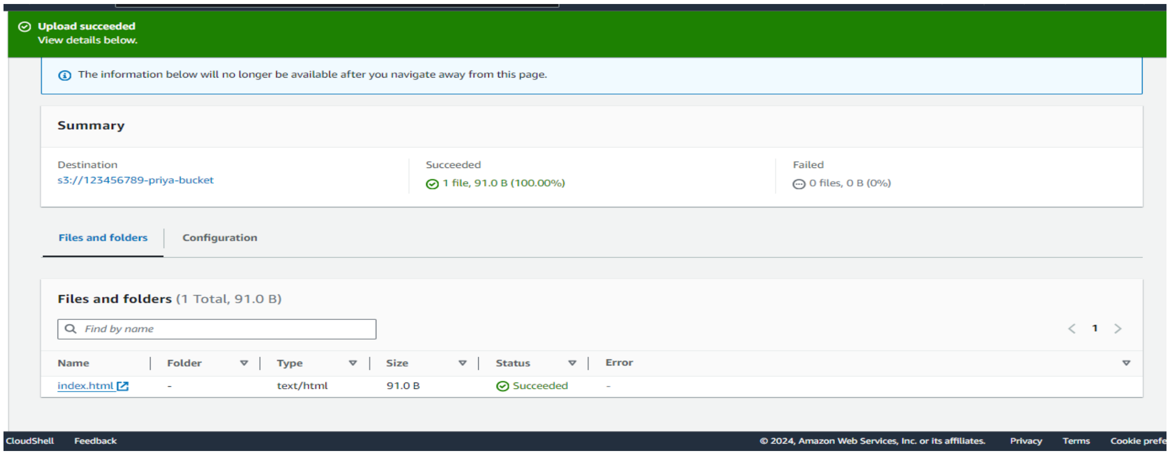
Additional checksums

● Off

Amazon S3 will use a combination of MD5 checksums and Etags to verify data integrity.

○ On

Specify a checksum function for additional data integrity validation.



Upload succeeded

View details below.

The information below will no longer be available after you navigate away from this page.

Summary

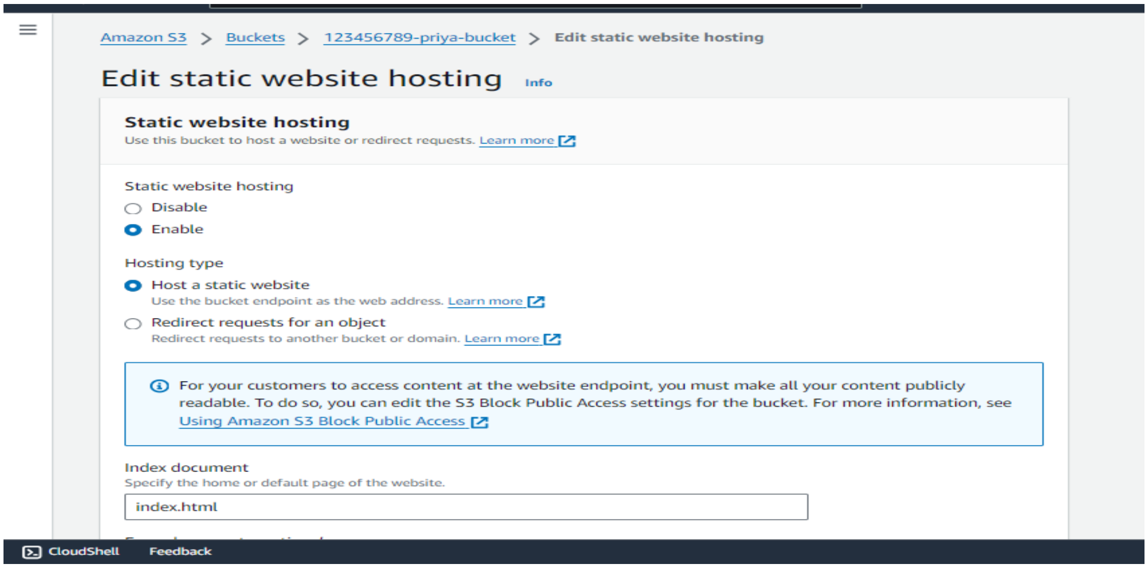
Destination	Succeeded	Failed
s3://123456789-priya-bucket	✓ 1 file, 91.0 B (100.00%)	0 files, 0 B (0%)

Files and folders (1 Total, 91.0 B)

Name	Folder	Type	Size	Status	Error
index.html	-	text/html	91.0 B	✓ Succeeded	-

Step 3 let's share the files

- Properties-> edit static hosting



Amazon S3 > Buckets > 123456789-priya-bucket > Edit static website hosting

Edit static website hosting Info

Static website hosting

Use this bucket to host a website or redirect requests. Learn more

Static website hosting

○ Disable

● Enable

Hosting type

● Host a static website

Use the bucket endpoint as the web address. Learn more

○ Redirect requests for an object

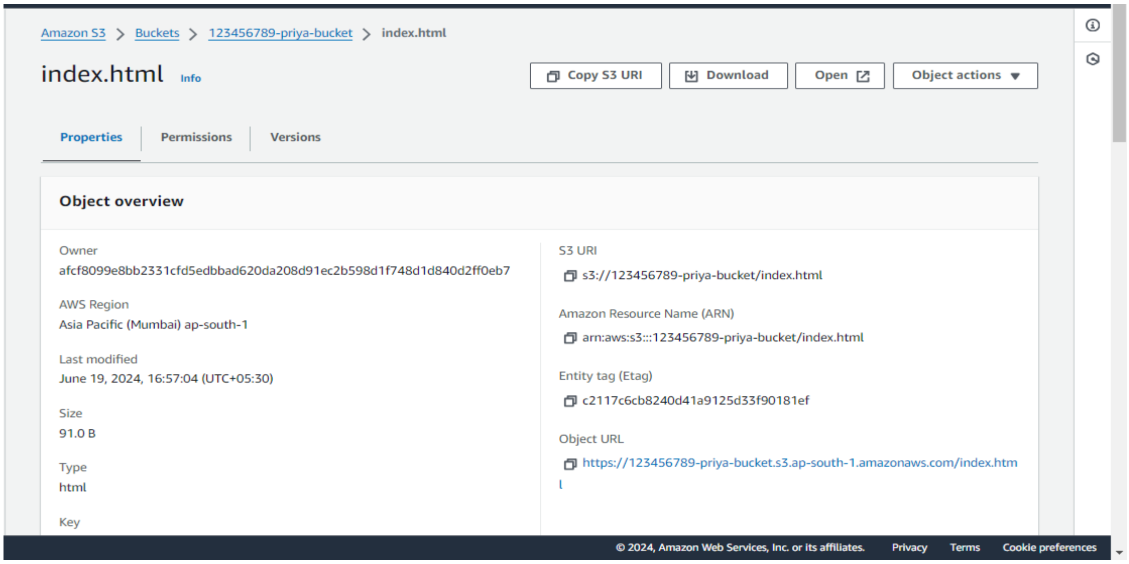
Redirect requests to another bucket or domain. Learn more

For your customers to access content at the website endpoint, you must make all your content publicly readable. To do so, you can edit the S3 Block Public Access settings for the bucket. For more information, see Using Amazon S3 Block Public Access

Index document

Specify the home or default page of the website.

index.html



Object overview

Owner
afcf8099e8bb2331cfd5edbbad620da208d91ec2b598d1f748d1d840d2ff0eb7

AWS Region
Asia Pacific (Mumbai) ap-south-1

Last modified
June 19, 2024, 16:57:04 (UTC+05:30)

Size
91.0 B

Type
html

Key

S3 URI
s3://123456789-priya-bucket/index.html

Amazon Resource Name (ARN)
arn:aws:s3:::123456789-priya-bucket/index.html

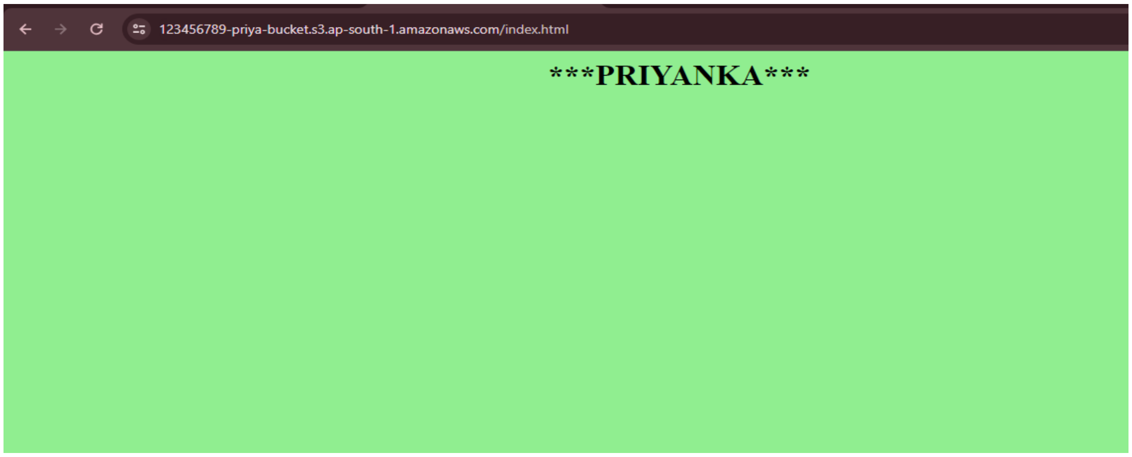
Entity tag (Etag)
c2117c6cb8240d41a9125d33f90181ef

Object URL
https://123456789-priya-bucket.s3.ap-south-1.amazonaws.com/index.html

- Object URL

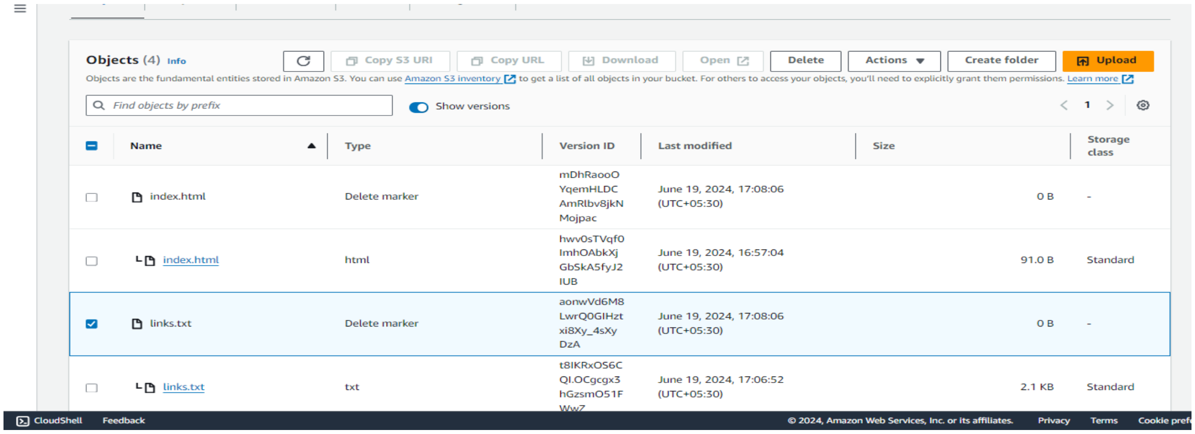
https://123456789-priya-bucket.s3.ap-south-1.amazonaws.com/index.html

Step 4 Paste the link in the browser and check it


123456789-priya-bucket.s3.ap-south-1.amazonaws.com/index.html

PRIYANKA

- After deleting files it can viewed in show versions



Objects (4) Info

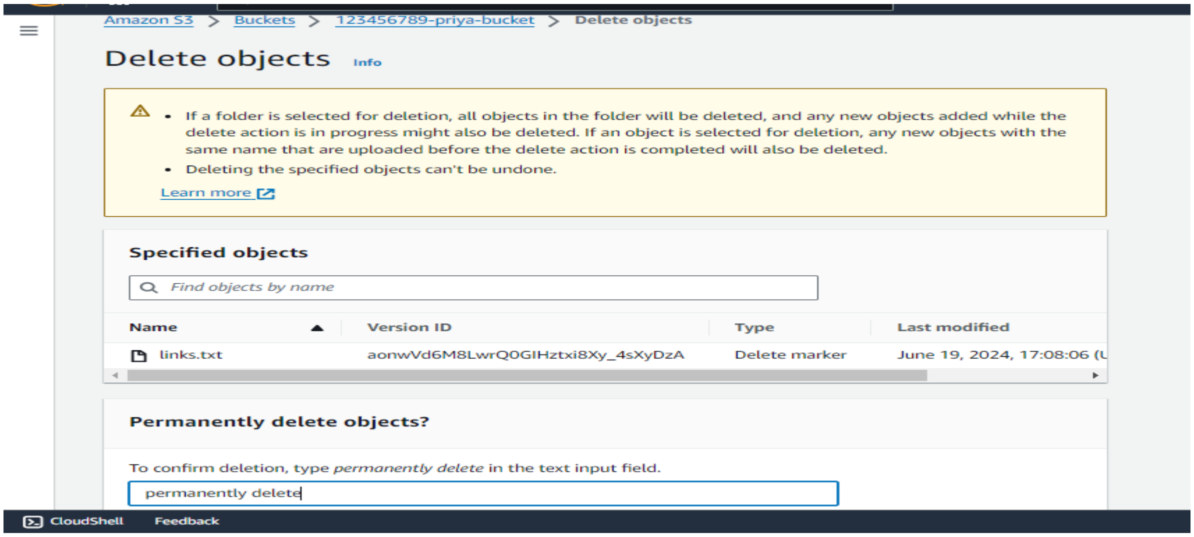
Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

Find objects by prefix

● Show versions

	Name	Type	Version ID	Last modified	Size	Storage class
□	index.html	Delete marker	mDhRaooOYqemHLDCAmRlbv8jkNMojpac	June 19, 2024, 17:08:06 (UTC+05:30)	0 B	-
□	└ index.html	html	hwv0sTVqf0ImhOAbkXjGbSkA5fyJ2IUB	June 19, 2024, 16:57:04 (UTC+05:30)	91.0 B	Standard
☑	links.txt	Delete marker	aonwVd6M8LwrQ0GIHztxi8Xy_4sXyDzA	June 19, 2024, 17:08:06 (UTC+05:30)	0 B	-
□	└ links.txt	txt	t8IKRxOS6CQI.OCgcgx3hGzsmO51FWwZ	June 19, 2024, 17:06:52 (UTC+05:30)	2.1 KB	Standard

- To delete permanently



Amazon S3 > Buckets > 123456789-priya-bucket > Delete objects

Delete objects Info

- If a folder is selected for deletion, all objects in the folder will be deleted, and any new objects added while the delete action is in progress might also be deleted. If an object is selected for deletion, any new objects with the same name that are uploaded before the delete action is completed will also be deleted.
- Deleting the specified objects can't be undone.

Learn more

Specified objects

Find objects by name

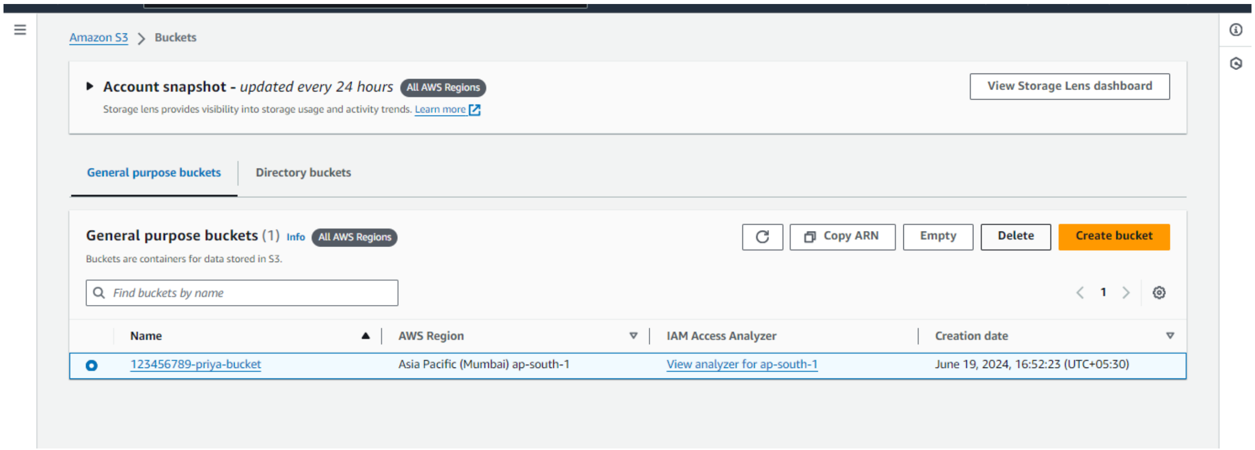
Name	Version ID	Type	Last modified
links.txt	aonwVd6M8LwrQ0GIHztxi8Xy_4sXyDzA	Delete marker	June 19, 2024, 17:08:06 (U

Permanently delete objects?

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

permanently delete

- To delete bucket, first empty the bucket



Account snapshot - *updated every 24 hours* All AWS Regions

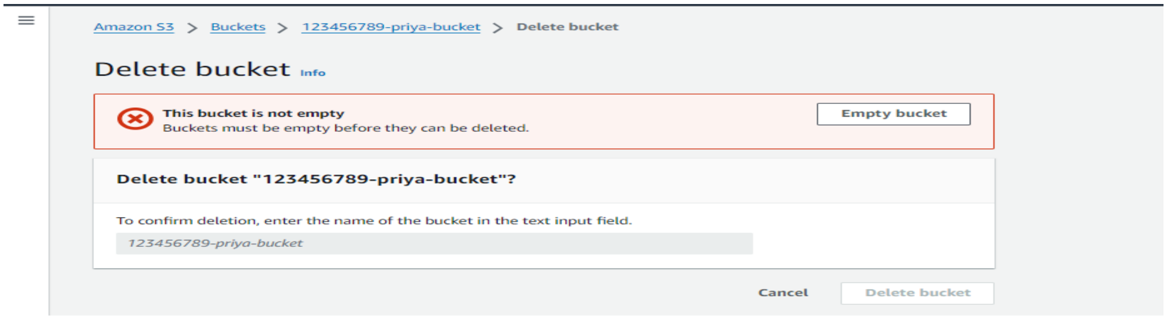
Storage lens provides visibility into storage usage and activity trends. Learn more

General purpose buckets (1) Info All AWS Regions

Buckets are containers for data stored in S3.

Find buckets by name

	Name	AWS Region	IAM Access Analyzer	Creation date
●	123456789-priya-bucket	Asia Pacific (Mumbai) ap-south-1	View analyzer for ap-south-1	June 19, 2024, 16:52:23 (UTC+05:30)


Amazon S3 > Buckets > 123456789-priya-bucket > Delete bucket

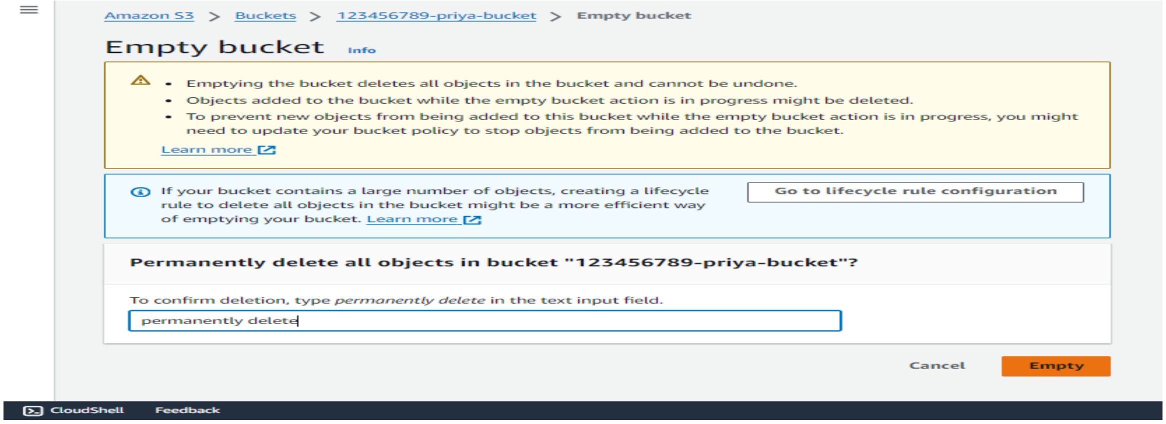
Delete bucket Info

This bucket is not empty
Buckets must be empty before they can be deleted.

Delete bucket "123456789-priya-bucket"?

To confirm deletion, enter the name of the bucket in the text input field.

123456789-priya-bucket


Amazon S3 > Buckets > 123456789-priya-bucket > Empty bucket

Empty bucket Info

- Emptying the bucket deletes all objects in the bucket and cannot be undone.
- Objects added to the bucket while the empty bucket action is in progress might be deleted.
- To prevent new objects from being added to this bucket while the empty bucket action is in progress, you might need to update your bucket policy to stop objects from being added to the bucket.

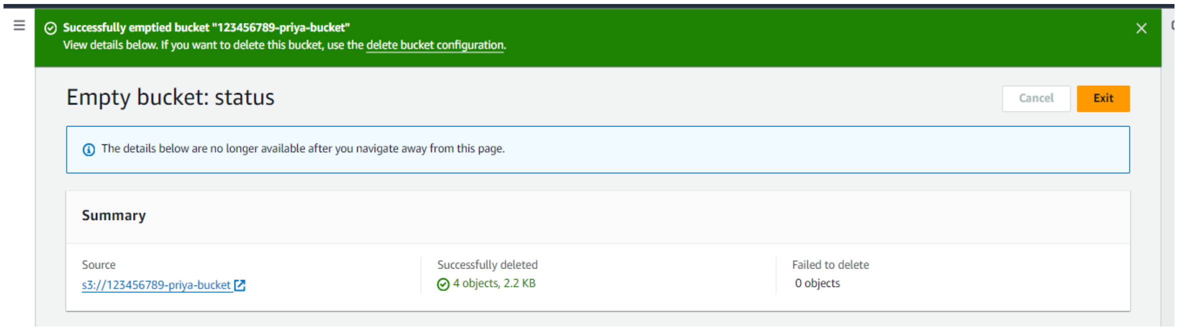
Learn more

If your bucket contains a large number of objects, creating a lifecycle rule to delete all objects in the bucket might be a more efficient way of emptying your bucket. Learn more

Permanently delete all objects in bucket "123456789-priya-bucket"?

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

permanently delete

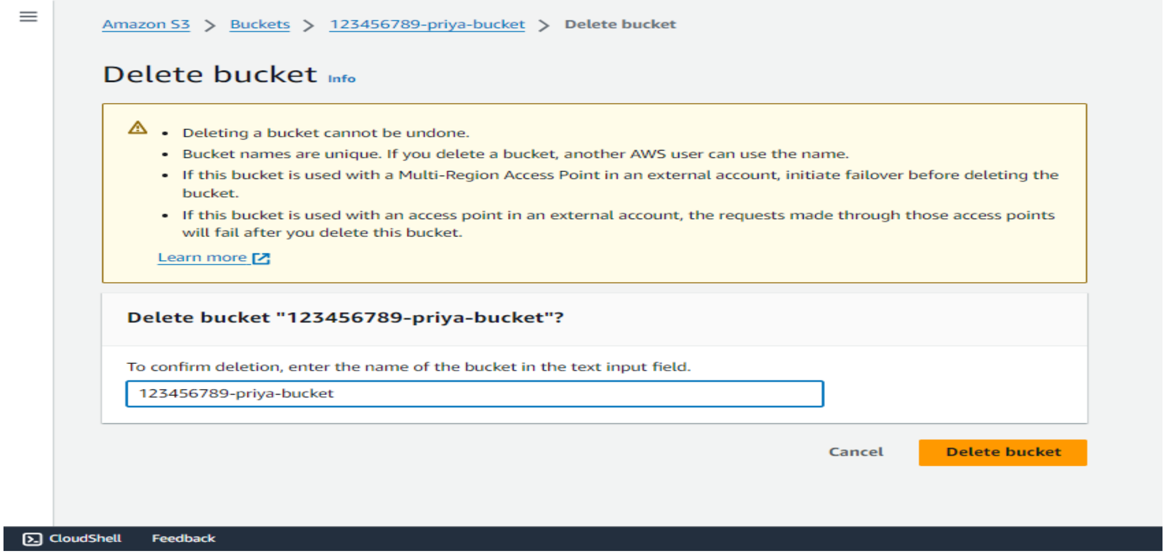

Successfully emptied bucket "123456789-priya-bucket"
View details below. If you want to delete this bucket, use the delete bucket configuration.

Empty bucket: status

The details below are no longer available after you navigate away from this page.

Summary

Source	Successfully deleted	Failed to delete
s3://123456789-priya-bucket	✓ 4 objects, 2.2 KB	0 objects


Amazon S3 > Buckets > 123456789-priya-bucket > Delete bucket

Delete bucket Info

- Deleting a bucket cannot be undone.
- Bucket names are unique. If you delete a bucket, another AWS user can use the name.
- If this bucket is used with a Multi-Region Access Point in an external account, initiate failover before deleting the bucket.
- If this bucket is used with an access point in an external account, the requests made through those access points will fail after you delete this bucket.

Learn more

Delete bucket "123456789-priya-bucket"?

To confirm deletion, enter the name of the bucket in the text input field.

123456789-priya-bucket