PROJECT-2

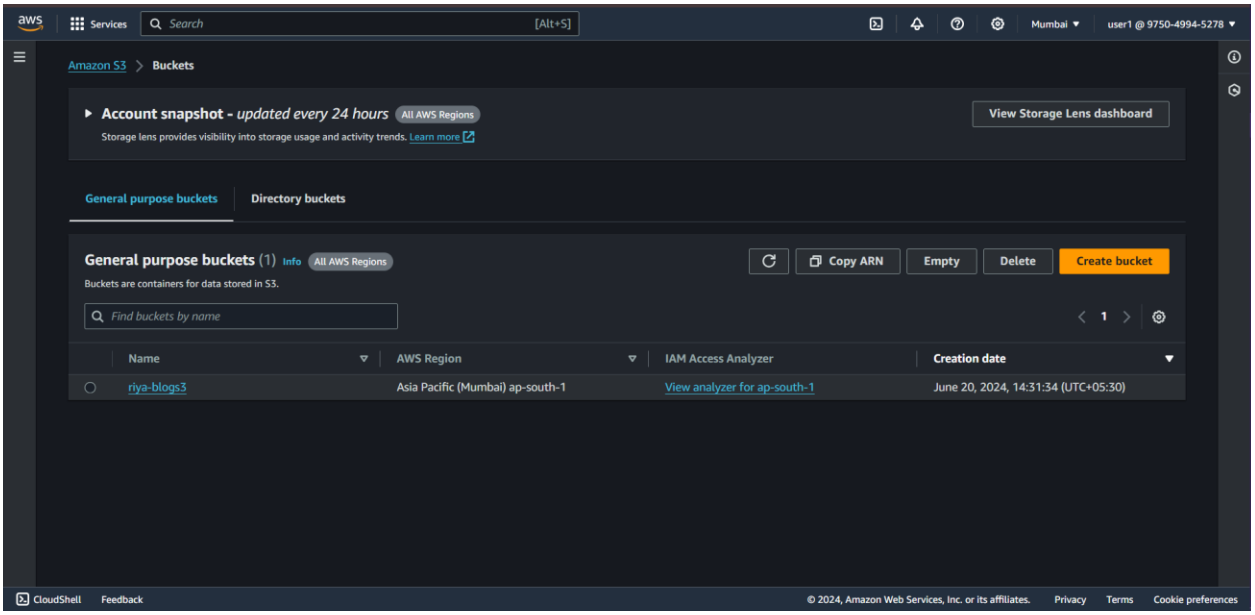
Deploy a static website on AWS

Step 1: Creating a Bucket

First, we have to launch our S3 instance. Follow these steps for creating a Bucket

Open the Amazon S3 console by logging into the AWS Management Console at https://console.aws.amazon.com/s3/.

Click on Create Bucket.



Account snapshot - *updated every 24 hours*

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

General purpose buckets (1)

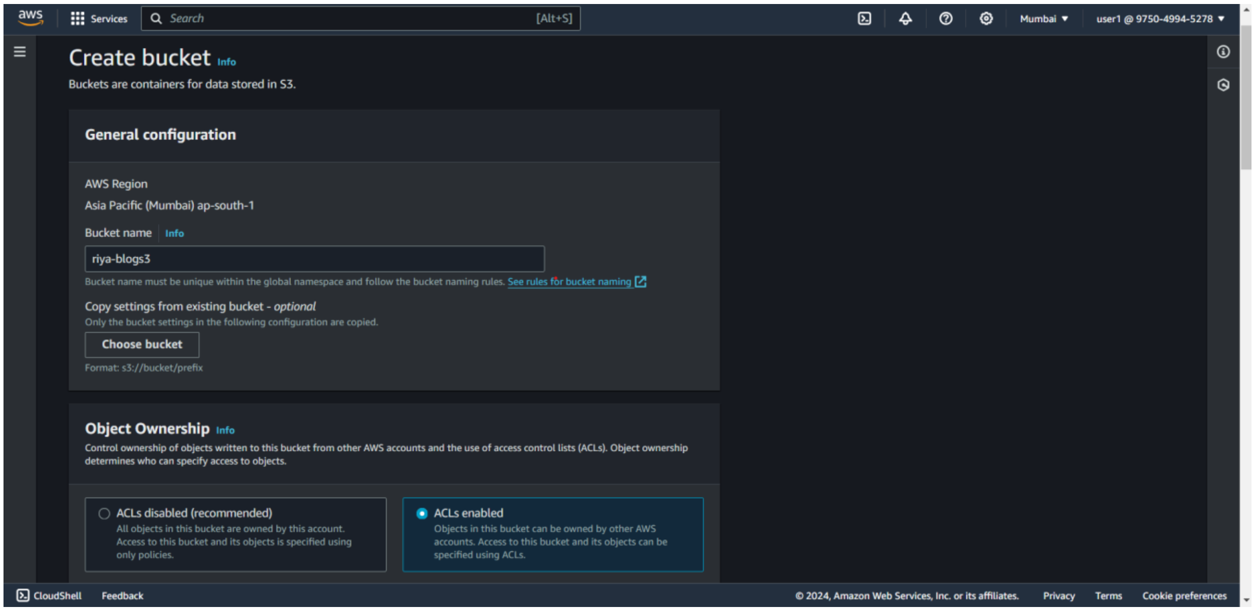
Buckets are containers for data stored in S3.

	Name	AWS Region	IAM Access Analyzer	Creation date
○	riya-blogs3	Asia Pacific (Mumbai) ap-south-1	View analyzer for ap-south-1	June 20, 2024, 14:31:34 (UTC+05:30)

Choose Bucket Name – Bucket Name Should be Unique

AWS Region – Choose a region close to you or the region where you want to create the bucket (Example — Mumbai)

Object Ownership – Enable for making Public, Otherwise disable



Create bucket Info

Buckets are containers for data stored in S3.

General configuration

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

Bucket name Info
riya-blogs3

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

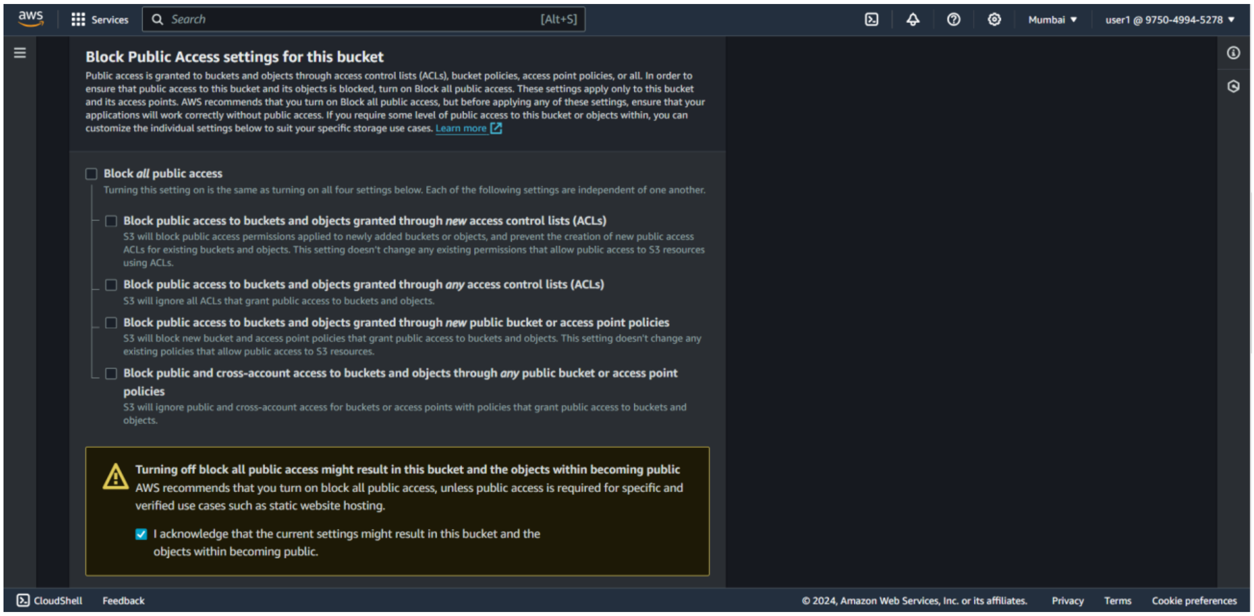
Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.

○ 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.

Step 2: Block Public Access settings for the bucket

Uncheck (Block all public access) for the public, otherwise set default. If you uncheck (Block all public keys).



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.

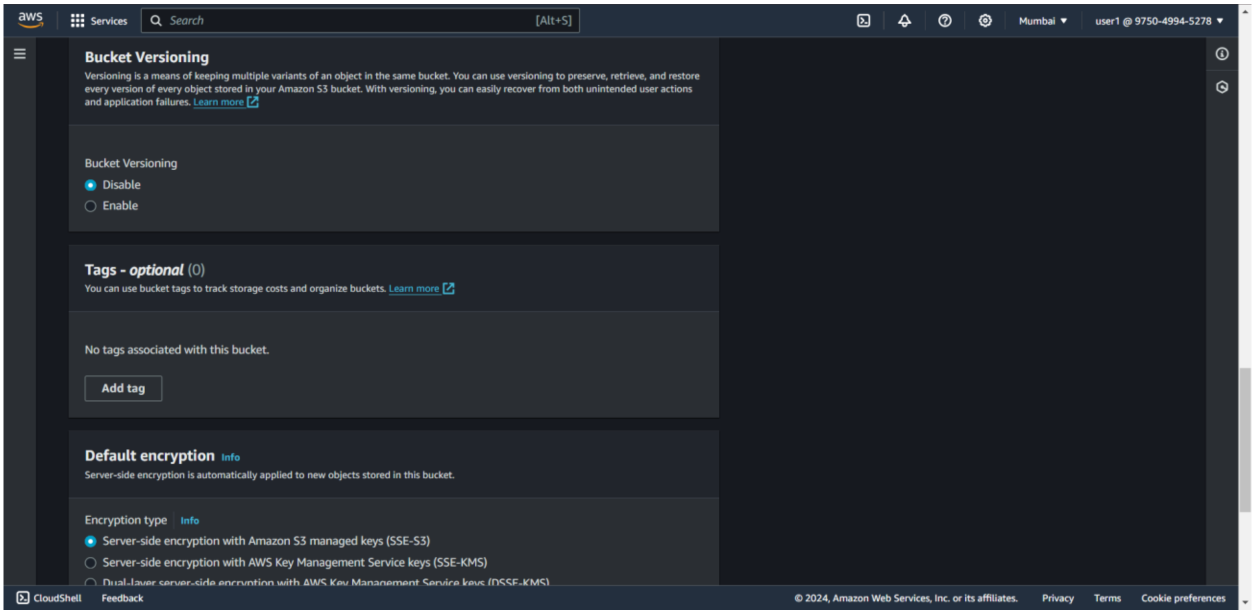
⚠ Turning off block all public access might result in this bucket and the objects within becoming public
AWS recommends that you turn on block all public access, unless public access is required for specific and verified use cases such as static website hosting.

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

Bucket Versioning:- You have to do Nothing (Disable)

Tags(0) : Optional

Default encryption: Disable



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.

Add tag

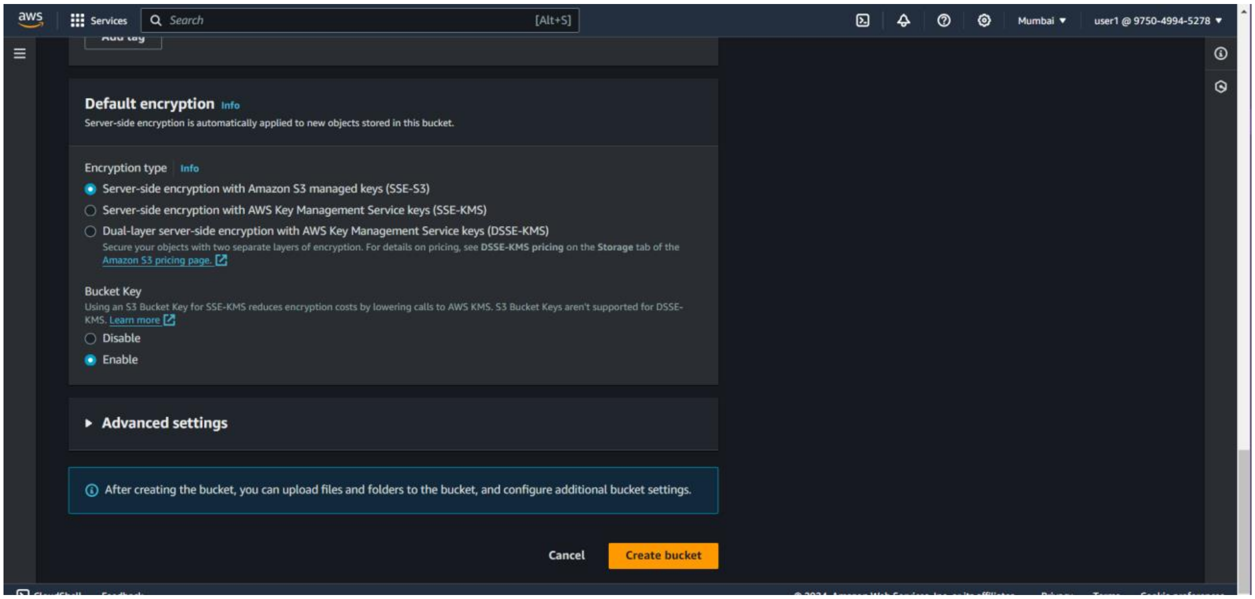
Default encryption Info

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)

Now, click on Create 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

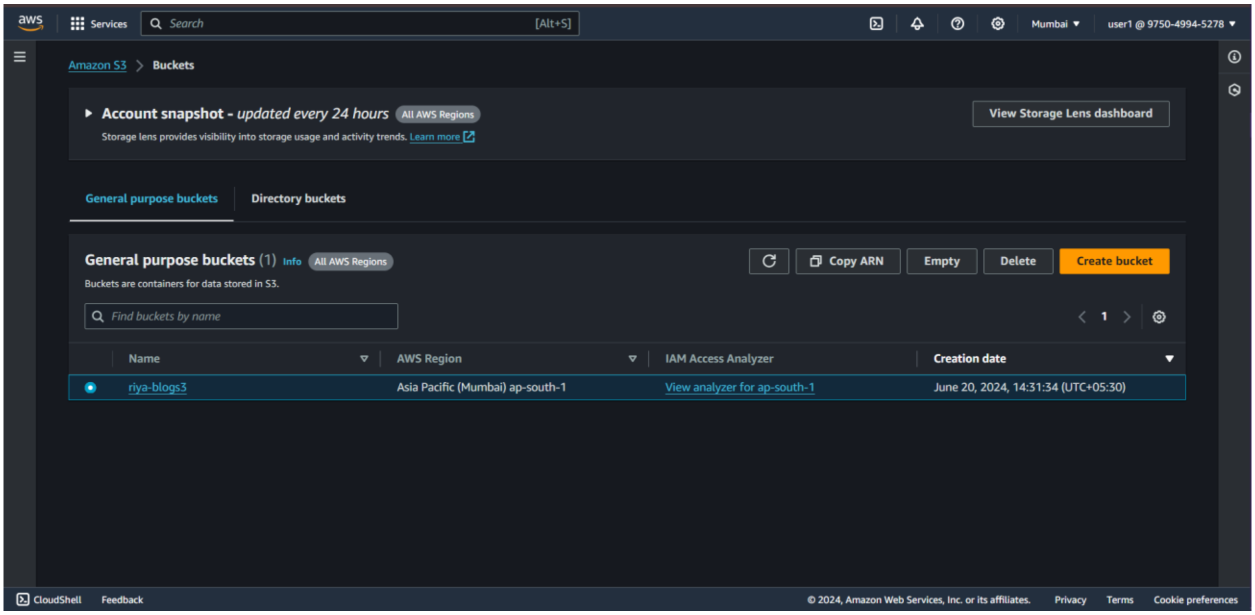
▸ **Advanced settings**

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

Cancel   Create bucket

Step 3: Now upload code files

Select Bucket and Click your Bucket Name.



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

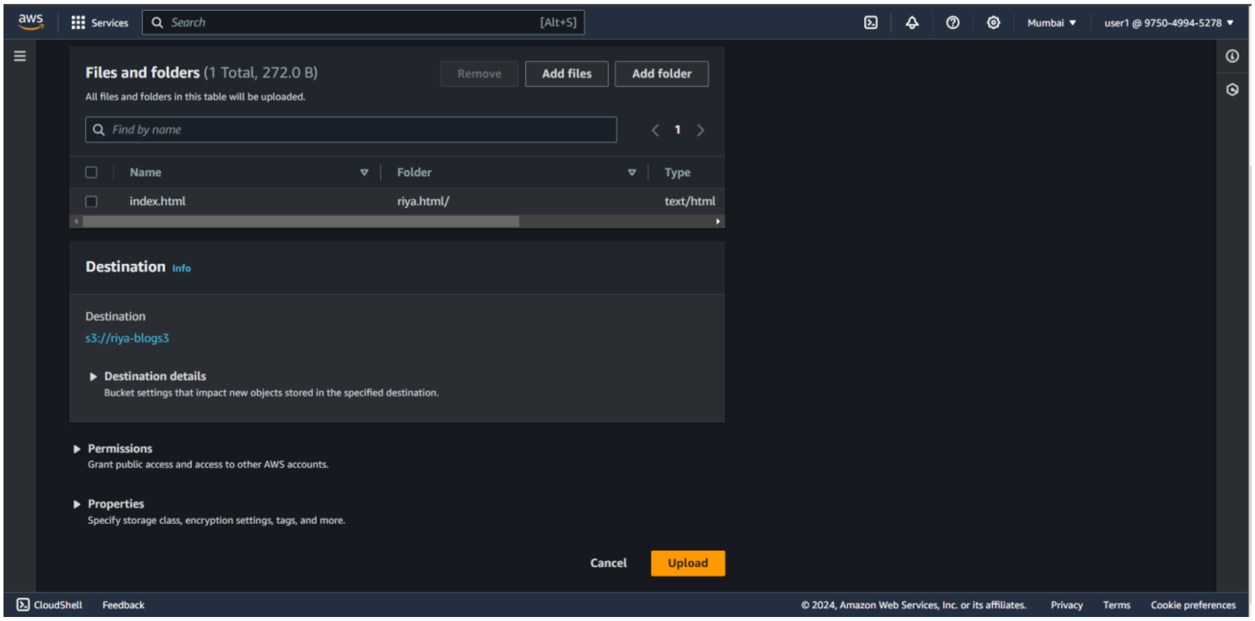
Storage lens provides visibility into storage usage and activity trends. Learn more

General purpose buckets (1)

Buckets are containers for data stored in S3.

	Name	AWS Region	IAM Access Analyzer	Creation date
●	riya-blogs3	Asia Pacific (Mumbai) ap-south-1	View analyzer for ap-south-1	June 20, 2024, 14:31:34 (UTC+05:30)

Now, click on upload (then click add File/folder) and select your HTML code file from your PC/Laptop.



Files and folders (1 Total, 272.0 B)

All files and folders in this table will be uploaded.

□	Name	Folder	Type
□	index.html	riya.html/	text/html

Destination

Destination
s3://riya-blogs3

▸ **Destination details**
Bucket settings that impact new objects stored in the specified destination.

▸ **Permissions**
Grant public access and access to other AWS accounts.

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

After uploading, click on Close.

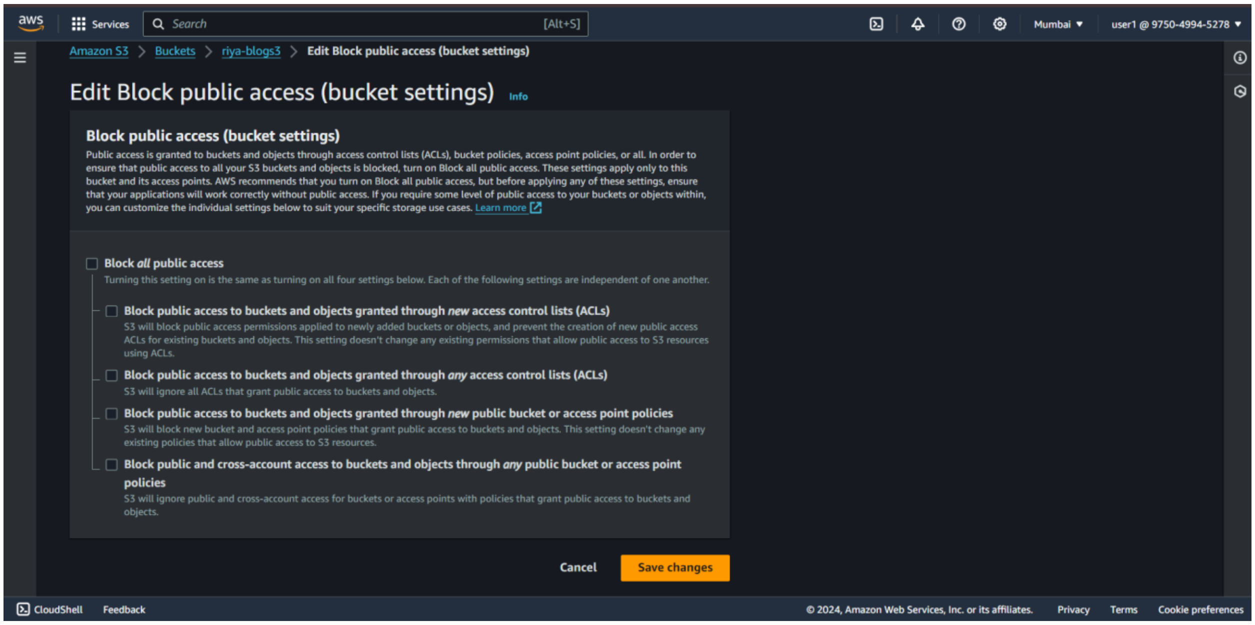
Step 4: Once the Files are uploaded successfully, click on Permissions and now follow this Process –

Block public access:

Click on Edit, under Bucket Policy.

Uncheck Block all public access.

Save changes then type “confirm”.



Amazon S3 > Buckets > riya-blogs3 > Edit Block public access (bucket settings)

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.

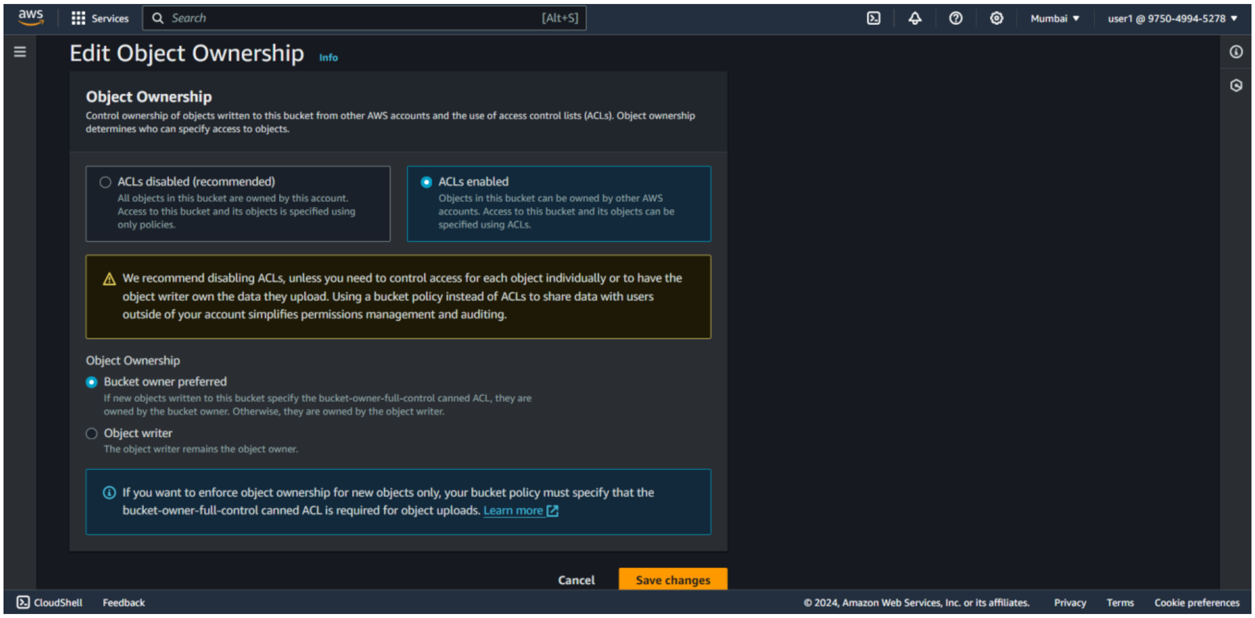
Object Ownership:

Click on Edit.

Click on ACLs Enabled.

Check I acknowledge ….. restored.

Choose Save Changes.



Edit Object Ownership Info

Object Ownership

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

Step 5:- Make public Object

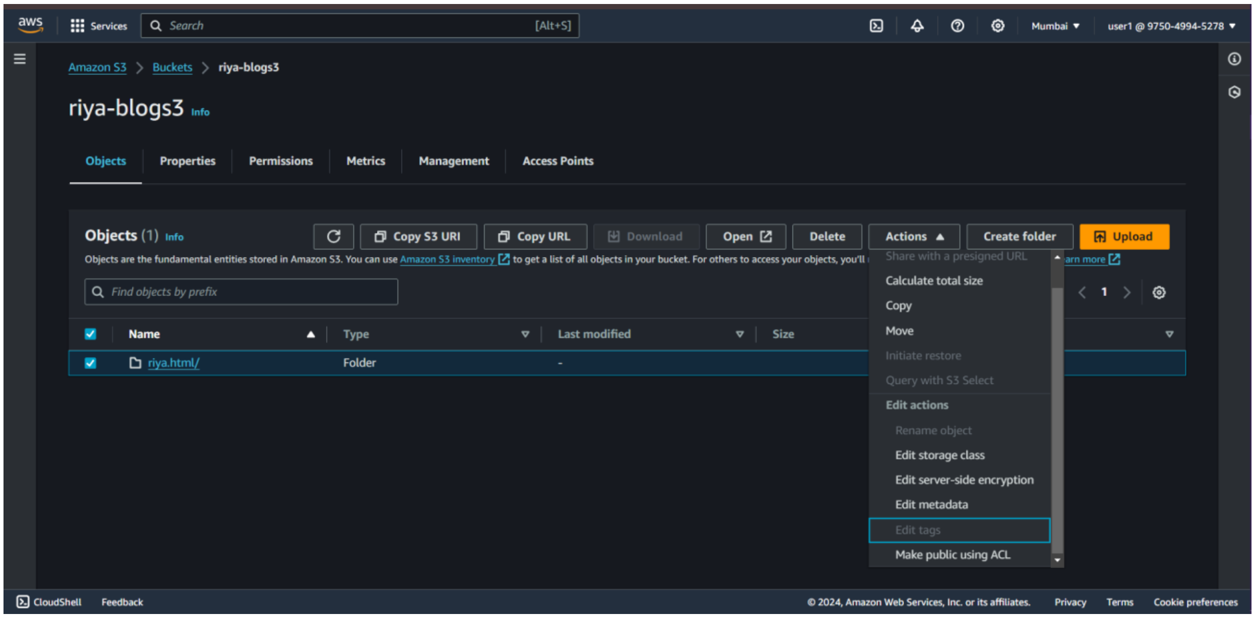
Now, Click on Objects.

Select your All Objects.

Now, Click on Actions.

Select Make Public Using ACL.

Now, Click on Make Public and Close.



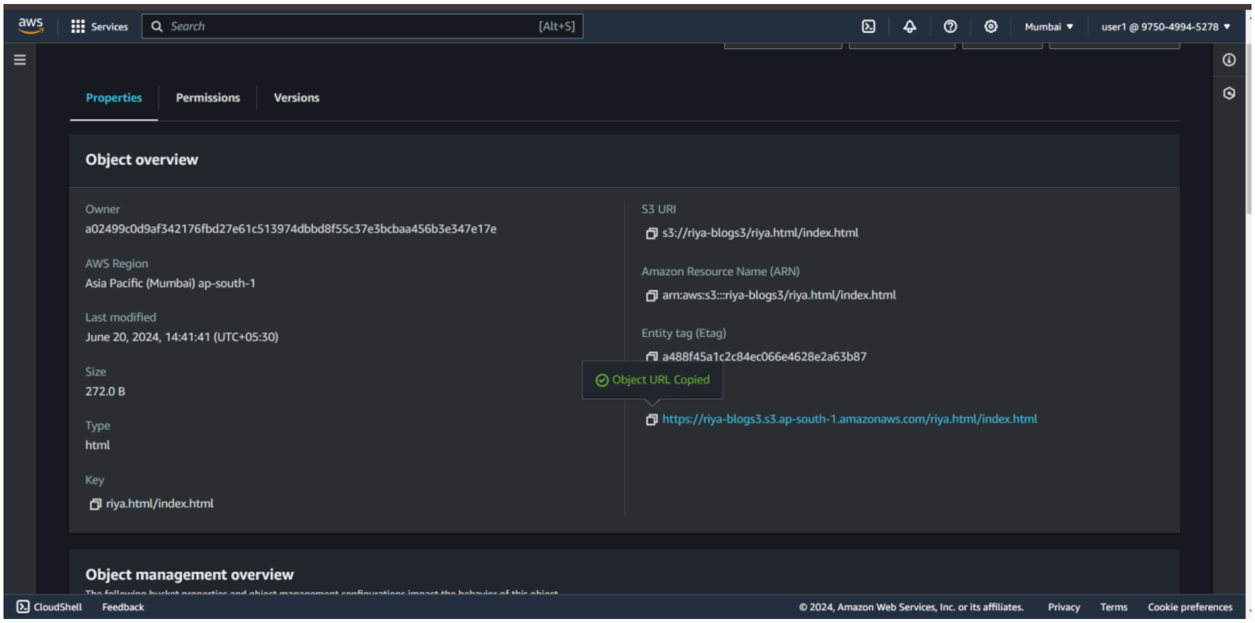
Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll

☑	Name	Type	Last modified	Size
☑	riya.html/	Folder	-	

Step 6: Copy your Object URL

Now, click on your HTML File Object Name.

Copy the Object URL.



Object overview

Owner
a02499c0d9af342176fbd27e61c513974dbbd8f55c37e3bcbaa456b3e347e17e

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

Last modified
June 20, 2024, 14:41:41 (UTC+05:30)

Size
272.0 B

Type
html

Key
riya.html/index.html

S3 URI
s3://riya-blogs3/riya.html/index.html

Amazon Resource Name (ARN)
arn:aws:s3:::riya-blogs3/riya.html/index.html

Entity tag (Etag)
a488f45a1c2c84ec066e4628e2a63b87

https://riya-blogs3.s3.ap-south-1.amazonaws.com/riya.html/index.html

Object management overview

Step 7: Check out your Website!

Directly Paste this URL into the Other Tab or your other System.

Congratulation, Now Your Website is available in the Public.

You Successfully Host Your Website by AWS S3.to