

# SETTING UP A SIMPLE STATIC WEBSITE ON AMAZON S3

## STEP 1 : Create an S3 Bucket on AWS

Navigate to the Amazon S3 service in the AWS Management Console, and click on the "Create Bucket" button. Enter a unique name for your bucket (bucket names must be globally unique across all AWS accounts) and click "Create".

## STEP 2 : Enabling and Configuring Static Website Hosting

After creating the bucket, click on its name to go to the bucket details page. Click on the "Properties" tab, then enable the "Static website hosting". Enter the index document name (e.g., "index.html") and optionally the error document name (e.g., "error.html") if you want to provide a custom error page. Click "Save changes."

## STEP 3 : Upload Website Content to the S3 Bucket

Upload your website files, such as HTML, CSS, JavaScript, and any other assets, into the S3 bucket. You can use the AWS Management Console, AWS CLI, or any S3-compatible tools to upload your files.

## STEP 4 : Setting up Permissions in S3 Bucket

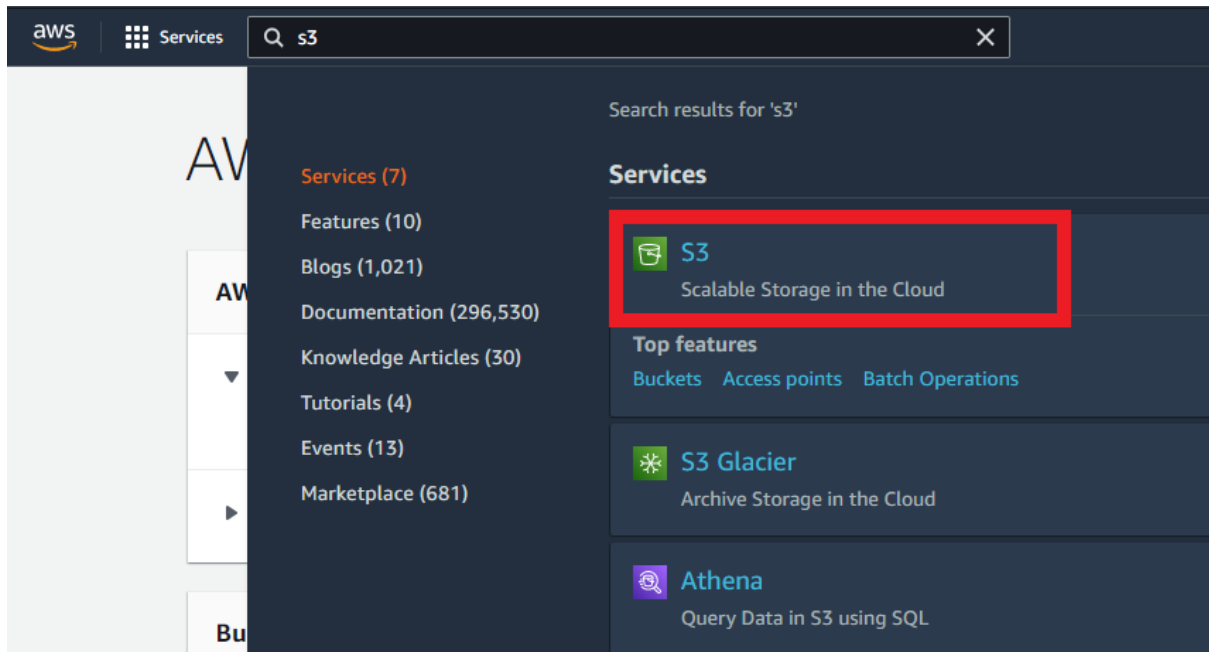
Ensure that the objects you uploaded have appropriate permissions so that the public can access them. Select the bucket and Configure a bucket policy to allow public access to objects within the bucket.

## STEP 5 : Accessing the Website Through URL

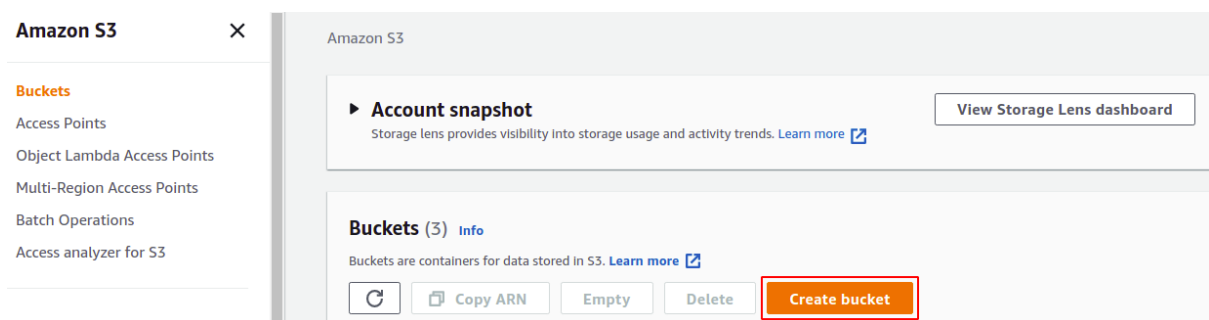
Open a web browser and enter the endpoint URL of the index.html file. You should be able to see your static website hosted on Amazon S3.

## STEP 1 : Create an S3 Bucket on AWS

The first step to hosting a static website on AWS S3 is to create an S3 bucket in your AWS account. Login to your AWS management console and go to the search bar and search for **S3** there. This will lead you to your S3 dashboard:

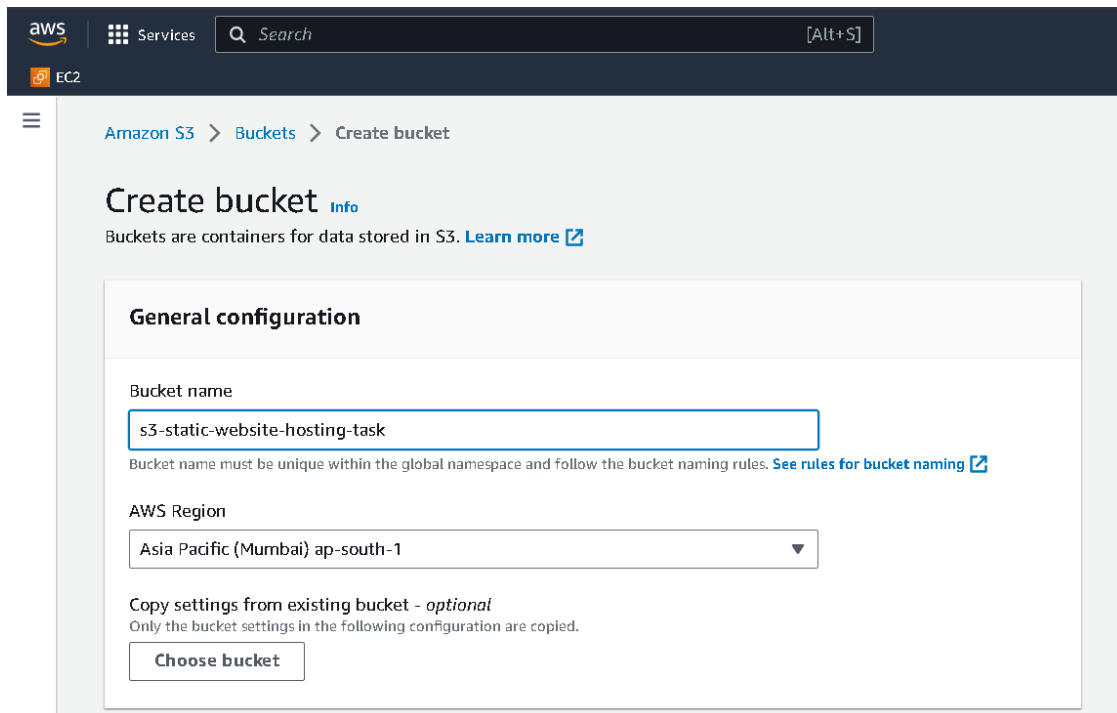


Click on Create Bucket at the right corner of the S3 console:



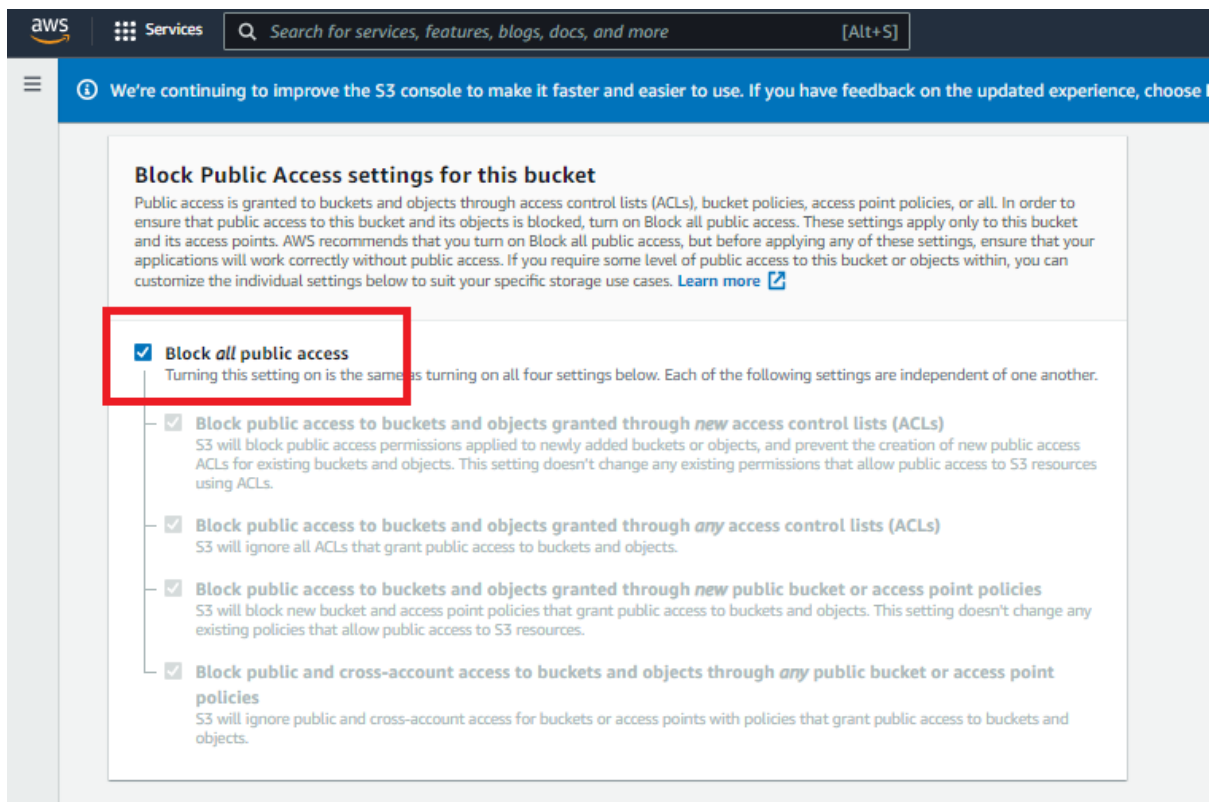
Next, you need to provide your S3 bucket name, the region where you want your bucket to be created.

The bucket name should be unique for all AWS accounts around the world:



The screenshot shows the AWS 'Create bucket' page. The breadcrumb navigation is 'Amazon S3 > Buckets > Create bucket'. The main heading is 'Create bucket' with an 'Info' link. Below it, a note states 'Buckets are containers for data stored in S3. [Learn more](#)'. The 'General configuration' section contains a 'Bucket name' input field with the value 's3-static-website-hosting-task', an 'AWS Region' dropdown menu set to 'Asia Pacific (Mumbai) ap-south-1', and a 'Copy settings from existing bucket - optional' section with a 'Choose bucket' button. A note indicates that only bucket settings from the chosen configuration are copied.

Since we wanted the website to be accessible to the audience, we had to grant the public access to the objects of this S3 bucket. For that, uncheck the Block all public access checkbox in the “Block Public Access setting for this bucket” section:



The screenshot shows the 'Block Public Access settings for this bucket' section. It includes an introductory paragraph about public access and a 'Learn more' link. Below this, there is a red-bordered box containing a checked checkbox labeled 'Block all public access' with the text 'Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.' Below the red box, there are four other settings, each with a checked checkbox and a description: 'Block public access to buckets and objects granted through new access control lists (ACLs)', 'Block public access to buckets and objects granted through any access control lists (ACLs)', 'Block public access to buckets and objects granted through new public bucket or access point policies', and 'Block public and cross-account access to buckets and objects through any public bucket or access point policies'.

After configuring the public access settings, a section will appear to acknowledge the S3 bucket and its content being made public. Check the box to acknowledge it:

### 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**

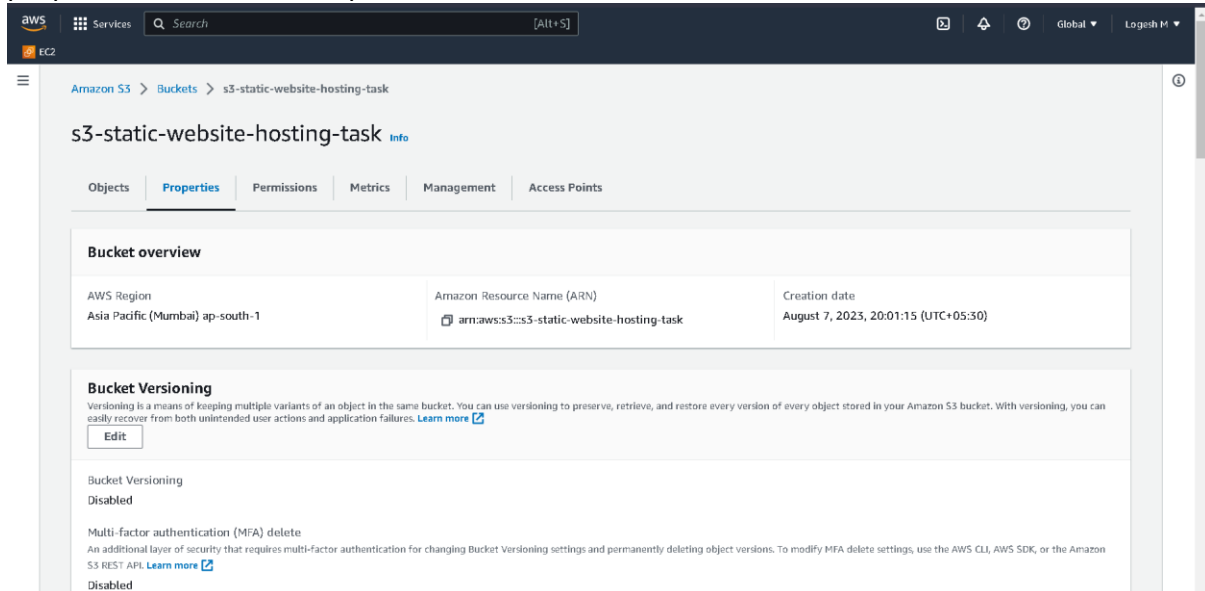
AWS recommends that you turn on block all public access, unless public access is required for specific and verified use cases such as static website hosting.

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

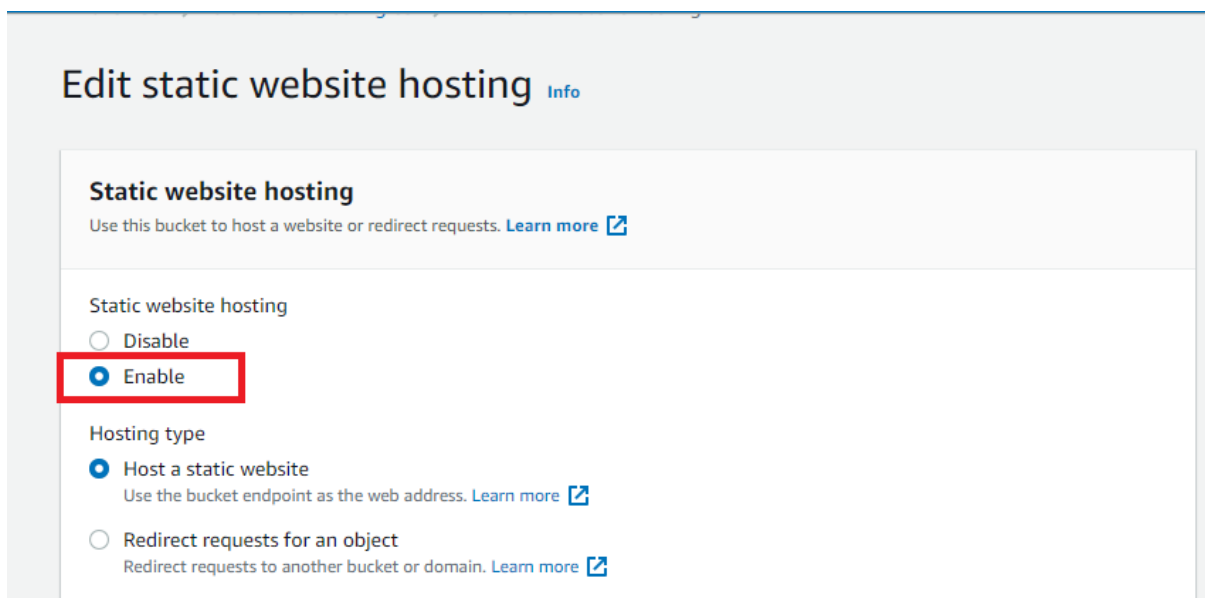
If the bucket name you specified is unique, the S3 bucket will be created. Otherwise, you will get an error, and you have to change the bucket name.

## STEP 2 : Enabling and Configuring Static Website Hosting

In order to allow static website hosting on your S3 bucket, Select bucket & go to the properties tab from the top menu in the S3 bucket:



Scroll down in properties tab and look for the Static Website Hosting section and Click on the Edit button in the Static website hosting section and enable the hosting:



After enabling static website hosting, specify the index file of your project (the opening page of your website or web application). In this case, it is index.html:

Index document

Specify the home or default page of the website.

index.html

Error document - optional

This is returned when an error occurs.

error.html

Also, if there is an error file in your project, you must specify it in the error document field. This will appear in case your actual web page is not reachable & save it. Now, our S3 bucket is hosting the website content uploaded to it and is publicly accessible.

### STEP 3 : Upload Website content to the S3 Bucket

Upload your website files, such as HTML, CSS, JavaScript, and any other assets, into the S3 bucket. You can use the AWS Management Console, AWS CLI, or any S3-compatible tools to upload your files.

Amazon S3

Buckets

Access Points

Object Lambda Access Points

Multi-Region Access Points

Batch Operations

IAM Access Analyzer for S3

Block Public Access settings for this account

Storage Lens

Dashboards

AWS Organizations settings

Feature spotlight

AWS Marketplace for S3

Amazon S3 > Buckets > s3-static-website-hosting-task

s3-static-website-hosting-task

Publicly accessible

Objects Properties Permissions Metrics Management Access Points

Objects (7)

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](#)

Copy S3 URI

Copy URL

Download

Open

Delete

Actions

Create folder

Upload

Find objects by prefix

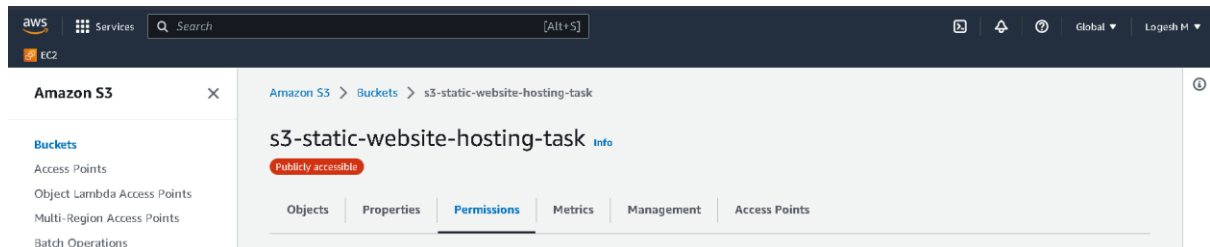
	Name	Type	Last modified	Size	Storage class
	css/	Folder	-	-	-
	guide.md	md	August 7, 2023, 20:35:29 (UTC+05:30)	30.3 KB	Standard
	img/	Folder	-	-	-
	index.html	html	August 7, 2023, 20:35:30 (UTC+05:30)	17.3 KB	Standard
	js/	Folder	-	-	-
	README.md	md	August 7, 2023, 20:35:31 (UTC+05:30)	172.0 B	Standard
	screenshot.png	png	August 7, 2023, 20:35:33 (UTC+05:30)	2.9 MB	Standard

Feedback Language

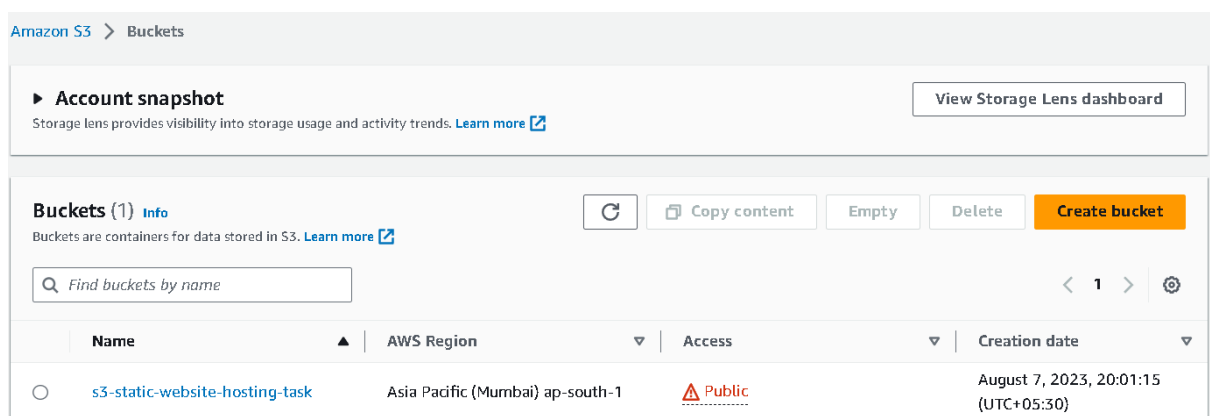
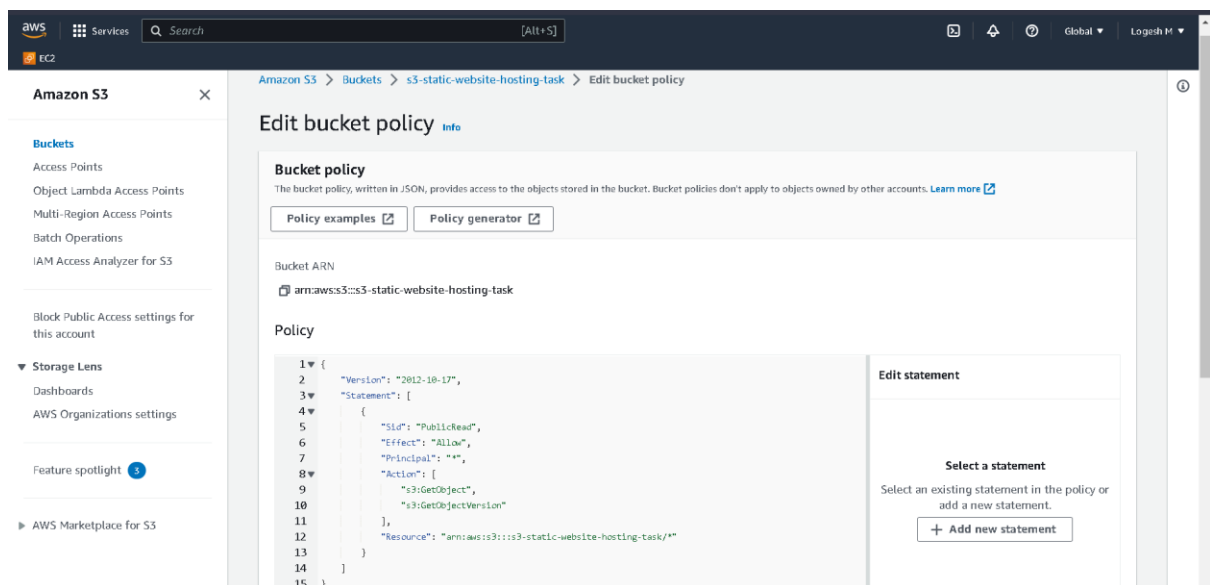
© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

## STEP 4 : Setting up Permissions in S3 Bucket

To make our content accessible publicly, we need to add a bucket policy for which we have to go to the permissions tab of our S3 bucket to make some changes to the permissions of our S3 bucket:

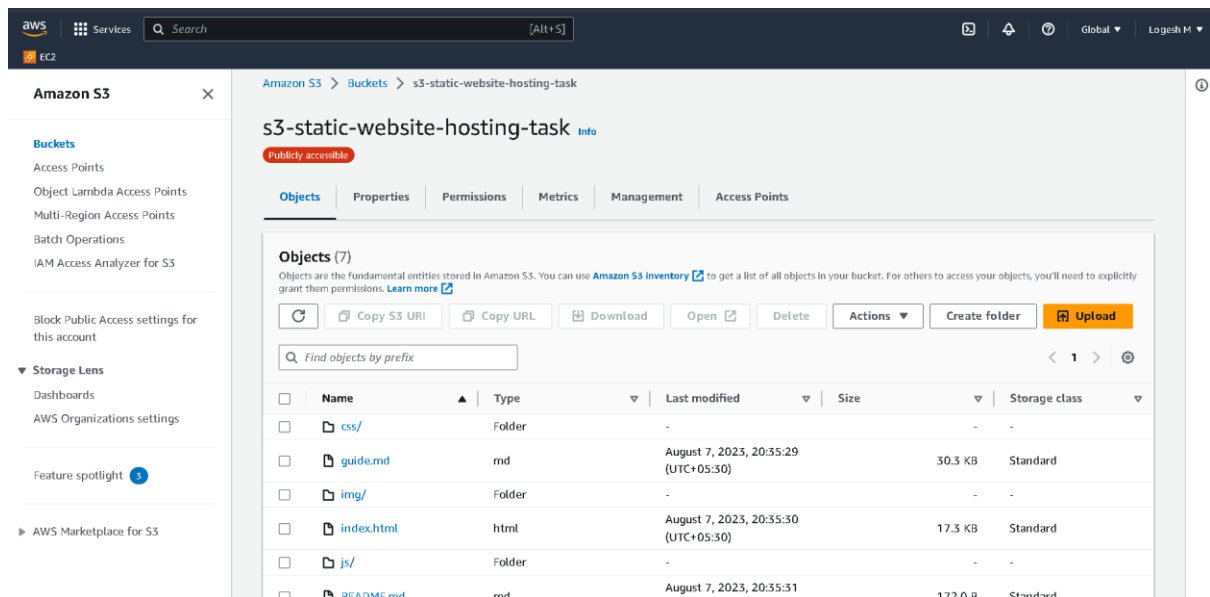


Now, move to the bucket policy section and click on the **Edit** button and update the bucket policy. After updating bucket policy bucket must be shown as public access.

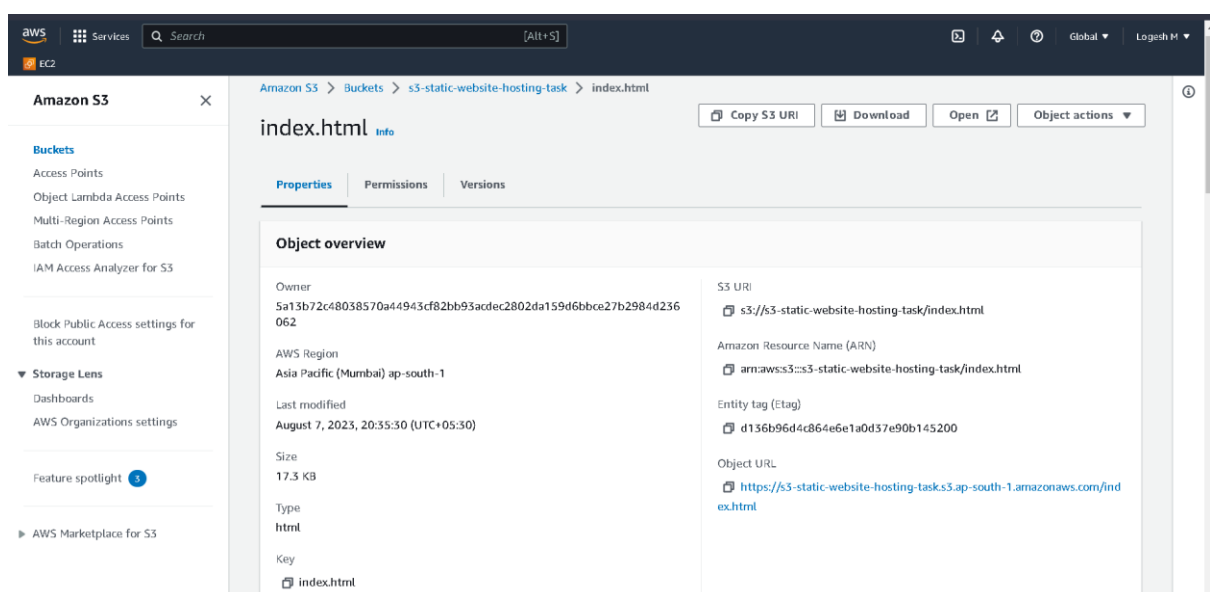


## STEP 5 : Accessing the Website Through URL

After setting the permissions for the bucket, it's time to access the webpage through the URL. Look for the index.html file, which you defined as the index document for this project. Click on the index.html file:



Now, in the object overview section under the properties tab, you can find the URL of the static website:





Go to this URL, and the static website hosted on the AWS S3 bucket will be accessible via browser:

