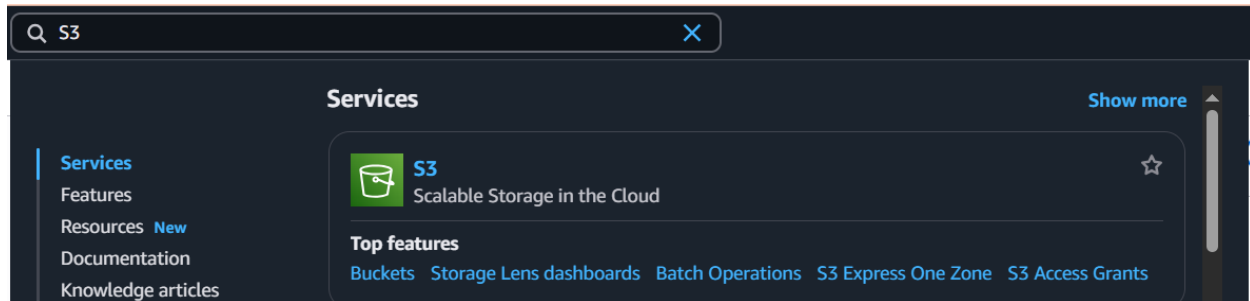


## AWS Static Web Hosting S3:

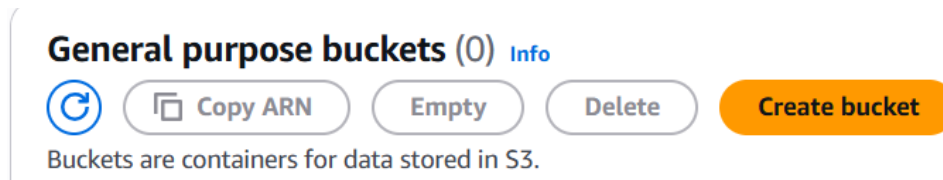
### Steps:

Login to your AWS account.

Search S3 in search bar > Click on Services > Buckets

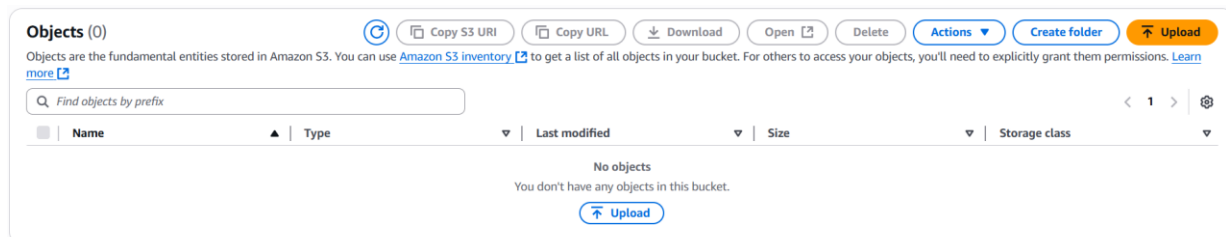


Create a bucket.

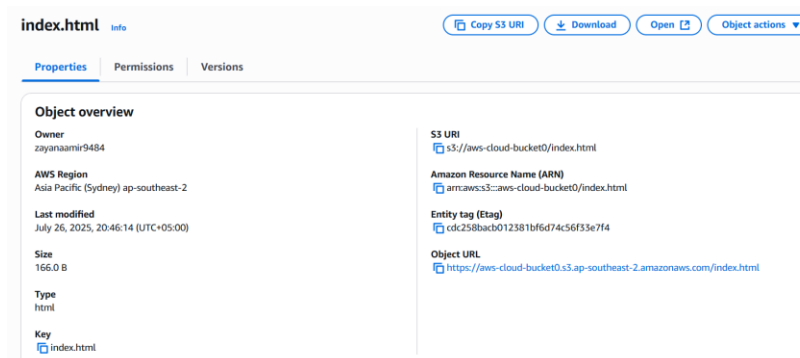


Give it a name, scroll down and click on Create bucket. The bucket will be created.

Click on your bucket & upload files i.e., web file



After upload, click on the uploaded file name and it will open a page like this where you can see the URL of your web under Object URL.



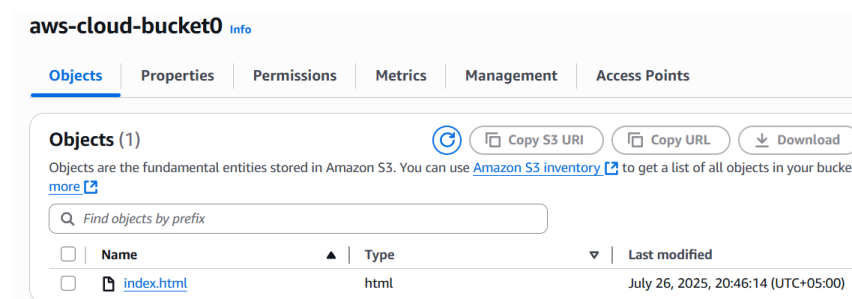
When you copy and paste this URL in your browser, it will give your error message like this.

```
This XML file does not appear to have any style information associated with it. The document tree is shown below.

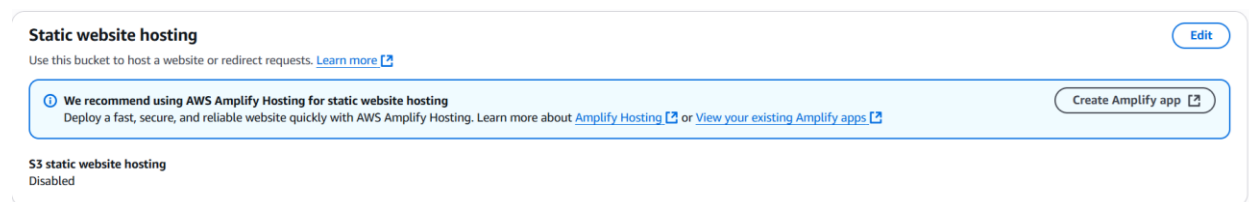
<?xml version="1.0" encoding="UTF-8" ?>
<Error>
  <Code>AccessDenied</Code>
  <Message>Access Denied</Message>
  <RequestId>FPCX9K06JEEH845V</RequestId>
  <HostId>GSdnksxJFKRQIQcf2ZG66WhGfjVBwMIM/mdGiOTqGXPwmHD7e19RuEzirT16I0gKLfuy0yk3ToQ=</HostId>
</Error>
```

To resolve this, we have to enable Static Web Hosting and some permissions.

Go to your bucket and click on Properties.

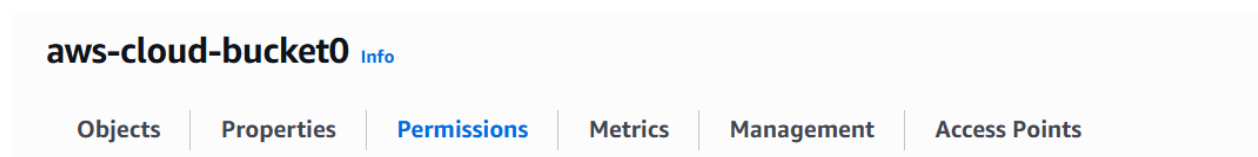


Scroll and enable Static Web Hosting by clicking on Edit.



Enable it, write the name of your web file (like index.html) & save changes.

Now to make it publicly accessible, go to the Permissions tab of your bucket.



Click on edit Block Public Access and “uncheck block all public access”

## 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](#)

Now, we need to make it public via ACL (Access Control List).

Scroll after saving changes and edit Object Ownership.

### 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.

## 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.

#### ⚠ Enabling ACLs turns off the bucket owner enforced setting for Object Ownership

Once the bucket owner enforced setting is turned off, access control lists (ACLs) and their associated permissions are restored. Access to objects that you do not own will be based on ACLs and not the bucket policy.

☒ I acknowledge that ACLs will be restored.

Save changes.

Now open your bucket > Select it > Actions > Make public using ACL > Make Public

## aws-cloud-bucket0 [Info](#)

[Objects](#) | [Properties](#) | [Permissions](#) | [Metrics](#) | [Management](#) | [Access Points](#)

### Objects (1/1)

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, [permissions](#). [Learn more](#)

Find objects by prefix

<input checked="" type="checkbox"/>	Name	Type	Last modified	Size
<input checked="" type="checkbox"/>	<a href="#">index.html</a>	html	July 26, 2025, 20:46:14 (UTC+05:00)	

Share with a presigned URL

Calculate total size

Copy

Move

Initiate restore

Query with S3 Select

Edit actions

Rename object

Edit storage class

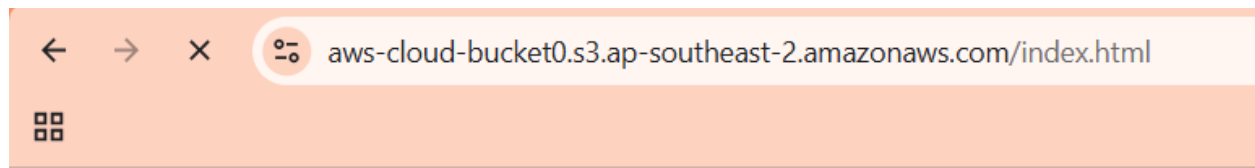
Edit server-side encryption

Edit metadata

Edit tags

Make public using ACL

Now refresh that web URL that was giving error. Your website will be loaded.



# Welcome to AWS

This is static web hosting.