

Static Website on AWS S3

- **Objective:**

To demonstrate how to host a basic static website using Amazon S3, including an HTML file and an image file.

- **Technologies Used:**

- HTML
- AWS S3 (Simple Storage Service)

File/Folder	Description
website.html	Main HTML file of the website
image/logo.jpeg	Image used in the web page

- **HTML Code:**

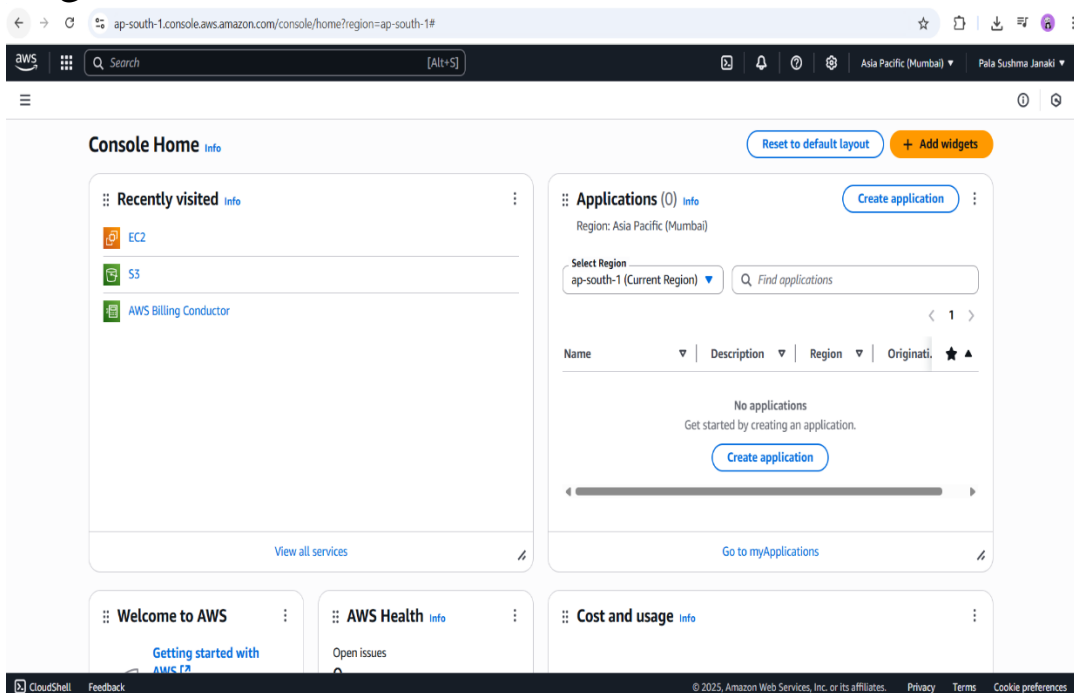
```
<!DOCTYPE html>
<html>
<head>
  <title>AWS Made Easy</title>
</head>
<body>
  <h1>Welcome to AWS Made Easy</h1>
  <p>AWS Services helps us in deploying websites</p>
  
</body>
</html>
```

- **Logo :**

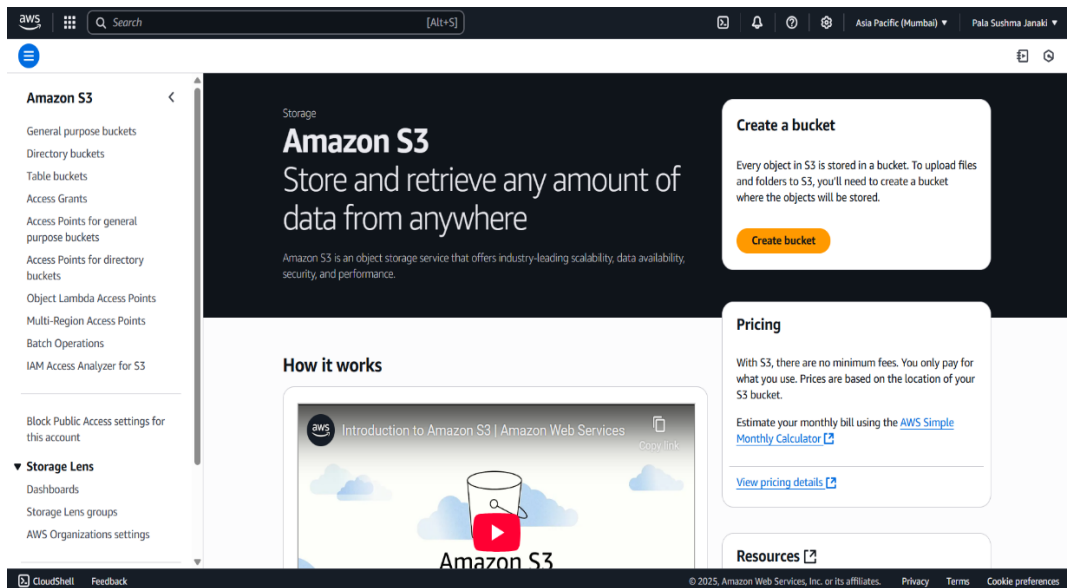


- **Hosting Steps on AWS S3:**

1. Login to AWS Console

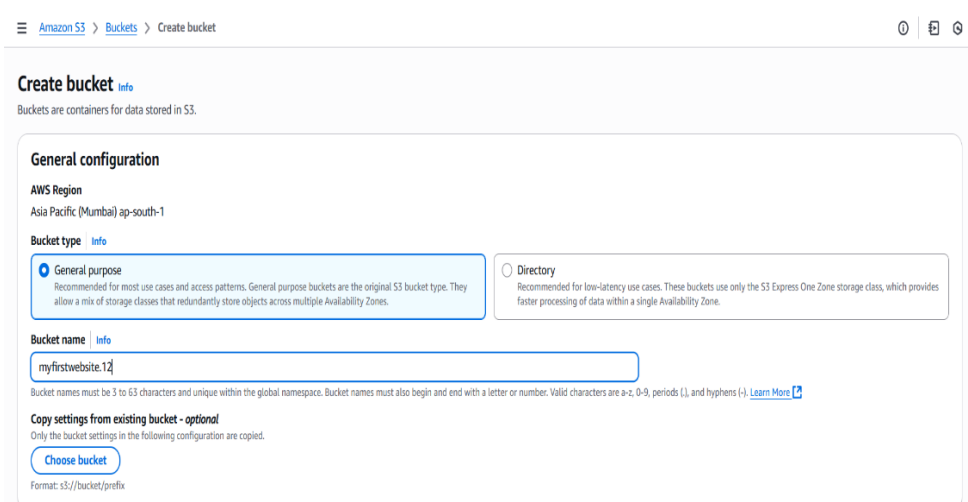


2. Go to **S3** from the services menu



3. Click **Create Bucket**

- Name: myfirstwebsite.12



- Region: (your AWS region)

• Uncheck: “Block all public access”

Amazon S3 > Buckets > Create bucket

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.

⚠ **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.

• Click Create Bucket

Amazon S3 > Buckets > Create bucket

You can add up to 50 tags.

Default encryption

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](#)

aws Search [Alt+S]

Amazon S3 > Buckets

Account snapshot - updated every 24 hours [View Storage Lens dashboard](#)

Storage lens provides visibility into storage usage and activity trends. Metrics don't include directory buckets. [Learn more](#)

General purpose buckets | Directory buckets

General purpose buckets (1) [Info](#) [All AWS Regions](#)

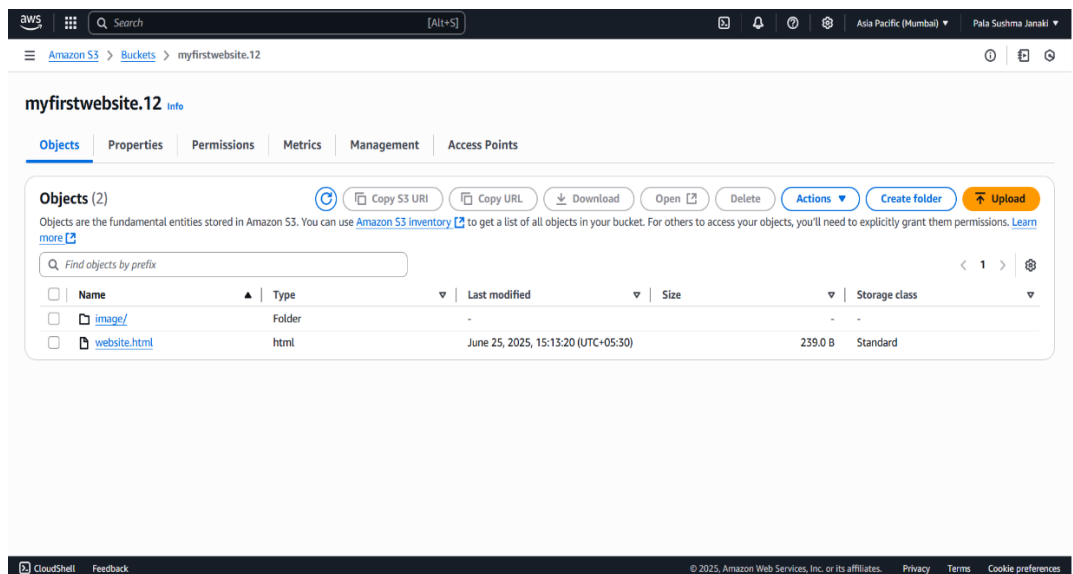
Buckets are containers for data stored in S3.

[Copy ARN](#) [Empty](#) [Delete](#) [Create bucket](#)

Name	AWS Region	IAM Access Analyzer	Creation date
myfirstwebsite.12	Asia Pacific (Mumbai) ap-south-1	View analyzer for ap-south-1	June 25, 2025, 14:43:46 (UTC+05:30)

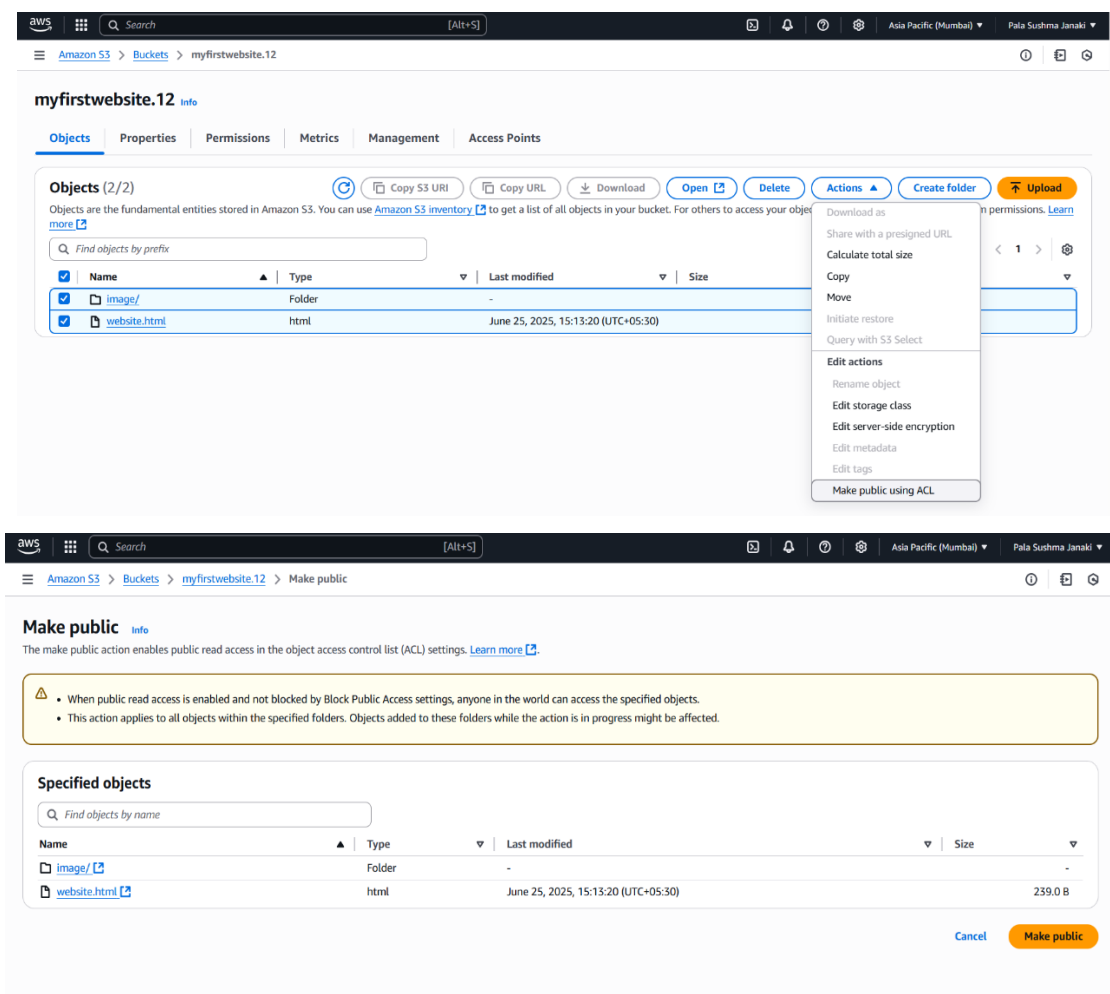
© 2025, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

4. Upload Files



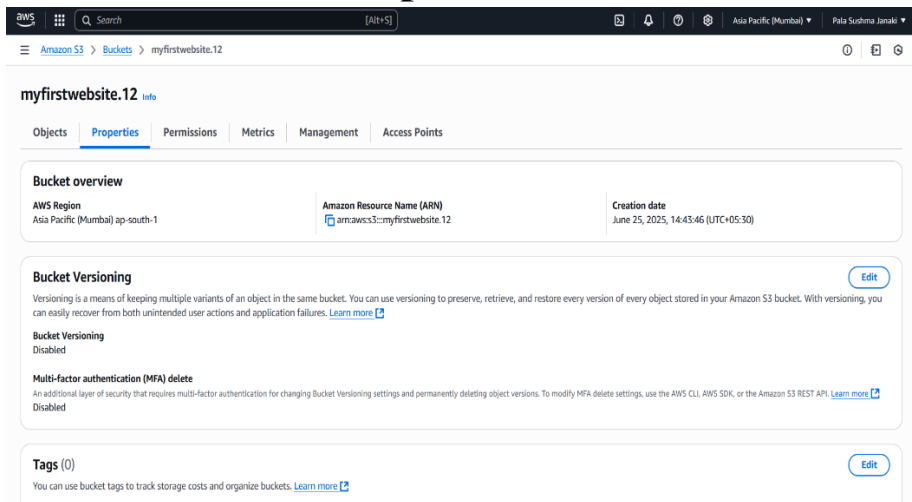
5. Make Files Public

- Select files → Actions → Make public

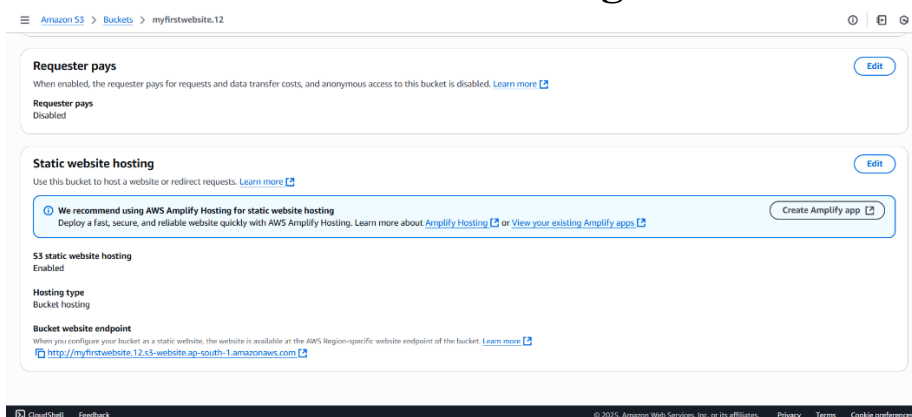


6. Enable Static Website Hosting

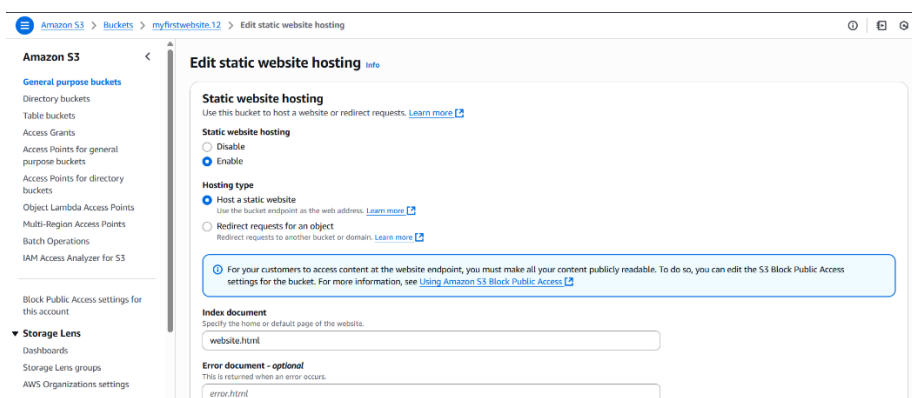
- Go to bucket → **Properties**



- Scroll to **Static website hosting** → Click **Edit**



- Enable hosting
- Index document: website.html



- Save

7. Get the Website URL

- Go to the **S3 Dashboard** on AWS.
- Click on your bucket name → myfirstwebsite.12
- Go to the **Properties** tab.
- Scroll down to the "**Static website hosting**" section.
- After enabling it, you'll see like this:

<http://myfirstwebsite.12.s3-website.ap-south-1.amazonaws.com>

8. Test Your Website

- Open the website **endpoint URL** in a browser.
- Make sure your page loads correctly:
 - a. Heading: ☒
 - b. Paragraph: ☒
 - c. Image: ☒