



# Static Website using AWS S3

## Project Description:-

Amazon S3 (*Simple Storage Service*) is a highly scalable and reliable object storage service offered by AWS. It allows you to store and retrieve any amount of data from anywhere on the web. In this project, we will leverage the capabilities of AWS S3 to host a static website. Unlike dynamic websites, which require server-side processing and databases, static websites consist of HTML, CSS, JavaScript, and other client-side files that can be directly served to visitors

**The main objectives of this project are as follows:**

1. Upload the website files to an S3 bucket: We will create a new S3 bucket and upload the static website files to it. These files can include HTML pages, CSS stylesheets, JavaScript scripts, images, and other assets.
2. Configure the S3 bucket as a static website: S3 provides a feature to turn a bucket into a static website by enabling website hosting. Once configured, the bucket will act as a web server, serving the static content directly to visitors.
3. Set up appropriate permissions: We'll define the necessary permissions to ensure public access to the static website. This will allow anyone with the website URL to view the content.
4. Ensure cost-effectiveness and scalability: AWS S3 is known for its cost-effectiveness and scalability, making it an ideal choice for hosting static websites.

Now that we have a clear understanding of the project's objectives, let's proceed with the step-by-step resolution of the projec

# Hands-on Project: Hosting a Static Website on AWS S3

## Step 1: Create an S3 Bucket

1. Log in to your AWS Management Console.
2. Navigate to the S3 service by clicking on “Services” in the top-left corner and selecting “S3” under the “Storage” section.
3. Click on the “Create Bucket” button.
4. Choose a unique bucket name that reflects your website (e.g., my-static-website).
5. Select the appropriate region for your website’s audience (choose the region closest to your target audience for better performance).
6. Leave other settings as default or adjust them as needed.

### Create bucket [Info](#)

Buckets are containers for data stored in S3.

#### General configuration

##### AWS Region

US East (Ohio) us-east-2

##### Bucket type [Info](#)

☒ **General purpose**  
Recommended for most use cases and access patterns. General purpose buckets are the original S3 bucket type. They allow a mix of storage classes that redundantly store objects across multiple Availability Zones.

☐ **Directory**  
Recommended for low-latency use cases. These buckets use only the S3 Express One Zone storage class, which provides faster processing of data within a single Availability Zone.

##### Bucket name [Info](#)

mystatic-website

Bucket names must be 3 to 63 characters and unique within the global namespace. Bucket names must also begin and end with a letter or number. Valid characters are a-z, 0-9, periods (.), and hyphens (-). [Learn More](#)

##### 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.

##### Object Ownership

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.

## 7. Click on “Create Bucket” to create your S3 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**

① After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.

[Cancel](#) [Create bucket](#)

## Step 2: Upload Website Files

### 1. Once the S3 bucket is created, click on its name to open the bucket details.

**irpitjaiswalbucket** [Info](#)

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

**Objects (0)** [Copy S3 URI](#) [Copy URL](#) [Download](#) [Open](#) [Delete](#) [Actions](#) [Create folder](#) [Upload](#)

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

Name	Type	Last modified	Size	Storage class
No objects				
You don't have any objects in this bucket.				

[Upload](#)

### 2. Click on the “Upload” button to upload your website files.

### 3. Drag and drop or choose the files from your local system.

### 4. Make sure to include your HTML, CSS, JavaScript, images, and any other assets required for the website.

**irpitjaiswalbucket** [Info](#)

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

**Objects (1)** [Copy S3 URI](#) [Copy URL](#) [Download](#) [Open](#) [Delete](#) [Actions](#) [Create folder](#) [Upload](#)

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

Name	Type	Last modified	Size	Storage class
<a href="#">Night with hut at river in the moonlight - Premium Vector.html</a>	html	June 24, 2025, 00:35:35 (UTC+05:30)	548.3 KB	Standard

## 5. Step 3: Configure the S3 Bucket for Website Hosting

### 6. In the bucket properties, navigate to the “Static website hosting” section.

7. Select the “Use this bucket to host a website” option.
8. For the “Index document,” enter the filename of your default homepage (usually “index.html”).
9. For the “Error document,” enter the filename of your custom error page (optional, usually “error.html” or “404.html”).
10. Click on “Save changes” to enable website hosting for the bucket.

**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](#)

---

**Index document**  
Specify the home or default page of the website.

**Error document - optional**  
This is returned when an error occurs.

## Step 4: Edit S3 Block Public Access settings and Set Bucket Policy for Public Access

1. In the bucket properties, navigate to the “Permissions” tab.
2. Under Block public access (bucket settings), choose Edit.
3. Clear Block *all* public access, and choose Save changes.

## 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 only you have access 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 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 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.
- ☐ **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.

4. Under Bucket Policy, choose Edit.

5. To grant public read access to your website, copy the following bucket policy, and paste it into the Bucket policy editor.

```
6. {
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PublicReadGetObject",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:s3:::Bucket-Name/*"
      ]
    }
  ]
}
```

Click on “Save” to apply the bucket policy, allowing public read access to

## objects in the bucket

### Policy

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Sid": "PublicReadGetObject",  
6       "Effect": "Allow",  
7       "Principal": "*",  
8       "Action": [  
9         "s3:GetObject"  
10      ],  
11      "Resource": [  
12        "arn:aws:s3:::arpitjaiswalbucket/*"  
13      ]  
14    }  
15  ]  
16 }
```

### Step 5: Test and Verify

Test your website by accessing the S3 bucket endpoint (e.g., [my-static-website.s3.amazonaws.com](http://my-static-website.s3.amazonaws.com)) in a web browser

You should be able to see your static website live and accessible to the public.

## Laptop Wallpaper Vectors

