

# Task-1

## Deploying a website using aws S3

---

### Introduction

Amazon S3 (Simple Storage Service) is a highly scalable and cost-effective cloud storage solution provided by Amazon Web Services (AWS). In addition to storing files, it can also be used to host static websites. This report will guide you through the process of setting up a simple static website on Amazon S3.

### I. Prerequisites:

Before proceeding with the setup, ensure that you have the following:

An AWS account: Sign up for an AWS account if you don't have one already.

A registered domain name (optional): If you want to use a custom domain for your website, register a domain from a domain registrar.

### II. Steps to Set Up a Simple Static Website on Amazon S3:

#### Step 1: Create an S3 bucket

Log in to the AWS Management Console.

Open the Amazon S3 service.

Click on "Create bucket" to start the bucket creation process.

---

---

Provide a unique bucket name and choose a region.

Click "Next" and keep the default settings for the subsequent screens.

Finally, click "Create bucket" to complete the creation process.

## **Step 2: Enable website hosting**

Select the newly created bucket from the S3 bucket list.

Go to the "Properties" tab and click on "Static website hosting."

Choose the option "Use this bucket to host a website."

Enter the name of the index document (e.g., "index.html") and the error document (optional).

Click "Save" to enable website hosting for the bucket.

## **Step 3: Upload your website files**

Open the "Overview" tab of your bucket.

Click on "Upload" to upload your website files (e.g., HTML, CSS, JS) or drag and drop them into the bucket.

Once the files are uploaded, make sure that the index document is present.

## **Step 4: Configure bucket permissions**

In the "Properties" tab, click on "Permissions."

Under "Block public access," click on "Edit" and disable "Block all public access."

---

Configure the bucket policy and CORS (Cross-Origin Resource Sharing) settings as per your requirements. For a simple website, you can allow public read access to all objects.

Save the changes.

### **Step 5: Test your website**

Go back to the "Static website hosting" section under the "Properties" tab.

Note down the endpoint URL provided under the "Endpoint" field.

Open a web browser and paste the endpoint URL to access your website.

Verify that your website is displayed correctly.

### **Conclusion:**

Setting up a simple static website on Amazon S3 is a straightforward process. By following the steps outlined in this report, you can create an S3 bucket, enable website hosting, upload your website files, configure bucket permissions, and test your website. Amazon S3 provides a reliable and cost-effective solution for hosting static websites, making it a popular choice for many developers and organizations.

## Screenshots:

### 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](#)

Edit

#### Block all public access

Off

Individual Block Public Access settings for this bucket

- ☐ **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.

Amazon S3 > Buckets > demowebapp-dheeraj

## demowebapp-dheeraj [Info](#)

Objects | Properties | Permissions | Metrics | Management | Access Points

### Objects (5)

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](#)

Refresh

Copy S3 URI

Copy URL

Download

Open

Delete

Actions

Create folder

Upload

Find objects by prefix

< 1 > ⚙

<input type="checkbox"/>	Name	Type	Last modified	Size	Storage class
<input type="checkbox"/>	assets/	Folder	-	-	-
<input type="checkbox"/>	images/	Folder	-	-	-
<input type="checkbox"/>	index.html	html	July 6, 2023, 10:54:21 (UTC+05:30)	3.7 KB	Standard
<input type="checkbox"/>	script.js	js	July 6, 2023, 10:54:23 (UTC+05:30)	9.6 KB	Standard