

Web Hosting (Static)

Introduction

Amazon S3 can be used not just for storage but also for **static website hosting**. You can upload HTML, CSS, JavaScript, and images to an S3 bucket, enable static website hosting, and access your site via an S3 URL or custom domain.

Benefits:

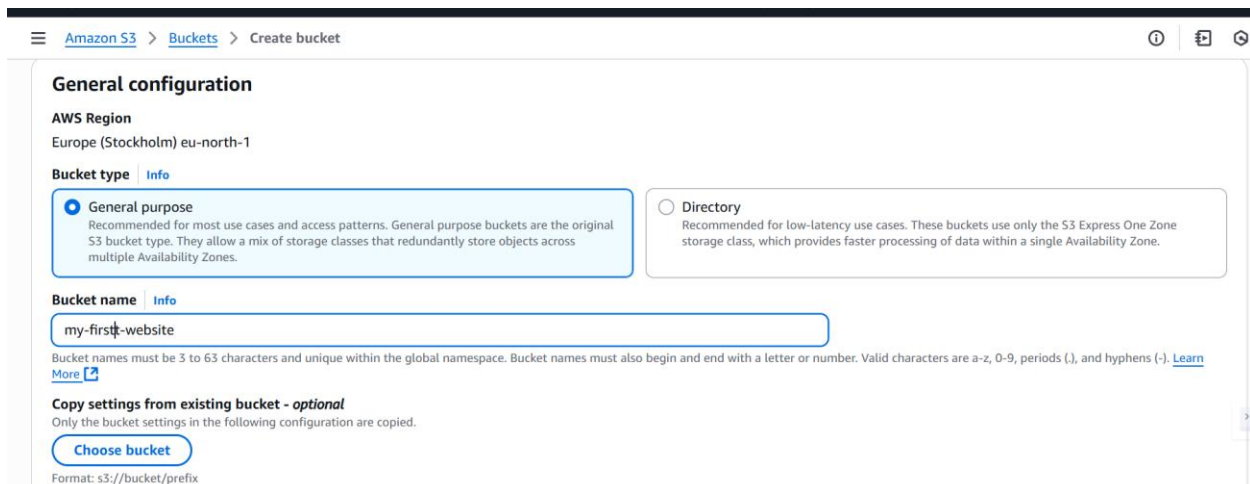
- Scalable and highly durable
- Low-cost, pay-as-you-go
- Secure with IAM and bucket policies

It's ideal for **static websites, portfolios, and app frontends**.

Project Execution

For creating static website, we use S3 service in AWS.

Step 1: Create Bucket



The screenshot shows the 'Create bucket' page in the Amazon S3 console. The breadcrumb navigation at the top reads 'Amazon S3 > Buckets > Create bucket'. The page is titled 'General configuration'. Under 'AWS Region', it shows 'Europe (Stockholm) eu-north-1'. The 'Bucket type' section has two options: 'General purpose' (selected with a radio button) and 'Directory'. The 'General purpose' option is described as '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.' The 'Directory' option is described as '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.' Below this, the 'Bucket name' field contains 'my-first-website'. A note states: '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](#)'. At the bottom, there is a section for 'Copy settings from existing bucket - optional' with a 'Choose bucket' button and a format example 's3://bucket/prefix'.

By default, Bucket is private so In object ownership I will enabled ACLs because it will help me to inside object(data) is public.

Amazon S3 > Buckets > Create bucket

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.

⚠ 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.

Object Ownership

☒ **Bucket owner preferred**
If new objects written to this bucket specify the bucket-owner-full-control canned ACL, they are owned by the bucket owner. Otherwise, they are owned by the object writer.

☐ **Object writer**
The object writer remains the object owner.

ℹ If you want to enforce object ownership for new objects only, your bucket policy must specify that the bucket-owner-full-control canned ACL is required for object uploads. [Learn more](#)

In Block Public Access will uncheck the box to get Public access of the bucket.

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

Secure your objects with two separate layers of encryption. For details on pricing, see DSSE-KMS pricing on the Storage tab or the [Amazon S3 pricing page](#).

☒ **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)

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**

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

Cancel Create bucket

Step 2: for Upload I will use sample website template to host

Amazon S3 > Buckets > my-firstt-website > Upload

Upload

Info

Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDKs or Amazon S3 REST API. [Learn more](#)

Drag and drop files and folders you want to upload here, or choose **Add files** or **Add folder**.

Files and folders (5 total, 137.9 KB)

Remove

Add files

Add folder

All files and folders in this table will be uploaded.

Find by name

< 1 >

<input type="checkbox"/>	Name	Folder	Type	Size
<input type="checkbox"/>	index.html	-	text/html	31.0 KB
<input type="checkbox"/>	listing.html	-	text/html	51.5 KB
<input type="checkbox"/>	contact.html	-	text/html	8.2 KB
<input type="checkbox"/>	category.html	-	text/html	25.2 KB
<input type="checkbox"/>	prepros.config	-	application/xml	22.0 KB

Destination

Info

Destination

[s3://my-firstt-website](#)

Click on Upload

Amazon S3 > Buckets > my-firstt-website > Upload

Upload

Info

All files and folders in this table will be uploaded.

Find by name

< 1 2 3 4 5 6 >

<input type="checkbox"/>	Name	Folder	Type	Size
--------------------------	------	--------	------	------

Destination

Info

Destination

[s3://my-firstt-website](#)

Destination details

Bucket settings that impact new objects stored in the specified destination.

Permissions

Grant public access and access to other AWS accounts.

Properties

Specify storage class, encryption settings, tags, and more.

Cancel

Upload

Step 3: In properties edit static website option

Amazon S3 > Buckets > my-firstt-website

Object Lock

Disabled

Requester pays

Edit

When enabled, the requester pays for requests and data transfer costs, and anonymous access to this bucket is disabled. [Learn more](#)

Requester pays

Disabled

Static website hosting

Edit

Use this bucket to host a website or redirect requests. [Learn more](#)

We recommend using AWS Amplify Hosting for static website hosting

Create Amplify app

Deploy a fast, secure, and reliable website quickly with AWS Amplify Hosting. Learn more about [Amplify Hosting](#) or [View your existing Amplify apps](#)

S3 static website hosting

Disabled

Enable it and write index document name and save changes

The screenshot shows the 'Edit static website hosting' page in the AWS console. The 'Static website hosting' section has the 'Enable' radio button selected. The 'Hosting type' section has 'Host a static website' selected. A blue information box states: 'For your customers to access content at the website endpoint, you must make all your content publicly readable. To do so, you can edit the S3 Block Public Access settings for the bucket. For more information, see Using Amazon S3 Block Public Access'. The 'Index document' field contains 'index.html' and the 'Error document - optional' field contains 'error.html'.

Step 4: to make my object public. In Action I will choose Make Public using ACL

The screenshot shows the 'Objects' page in the AWS console for bucket 'my-firstt-website'. A table lists objects: assets/, category.html, contact.html, index.html, listing.html, prepros.config, and vendor/. The 'index.html' object is selected, and the 'Actions' dropdown menu is open, showing the option 'Make public using ACL' at the bottom.

Name	Type	Last modified	Size
assets/	Folder	-	-
category.html	html	September 8, 2025, 14:13:22 (UTC+05:30)	-
contact.html	html	September 8, 2025, 14:13:21 (UTC+05:30)	-
index.html	html	September 8, 2025, 14:13:19 (UTC+05:30)	-
listing.html	html	September 8, 2025, 14:13:20 (UTC+05:30)	-
prepros.config	config	September 8, 2025, 14:13:22 (UTC+05:30)	-
vendor/	Folder	-	-

Now copy URL and paste in browser and you will get your hosted website.

Bucket website endpoint

When you configure your bucket as a static website, the website is available at the AWS Region-specific website endpoint of the bucket. [Learn more](#)

<http://my-firstt-website.s3-website.eu-north-1.amazonaws.com>

<http://my-firstt-website.s3-website.eu-north-1.amazonaws.com>

