STATIC WEBSITE

A static website delivers content in the same format in which it is stored. No server-side

code execution is required. For example, if a static website consists of HTML

documents displaying images, it delivers the HTML and images as-is to the browser,

without altering the contents of the files.

Static websites can be delivered to web browsers on desktops, tablets, or mobile

devices. They usually consist of a mix of HTML documents, images, videos, CSS style

sheets, and JavaScript files. Static doesn't have to mean boring—static sites can

provide client-side interactivity as well. Using HTML5 and client-side JavaScript

technologies such as jQuery, AngularJS, React, and Backbone, you can deliver rich

user experiences that are engaging and interactive.

Some examples of static sites include:

• Marketing websites

• Product landing pages

• Microsites that display the same content to all users
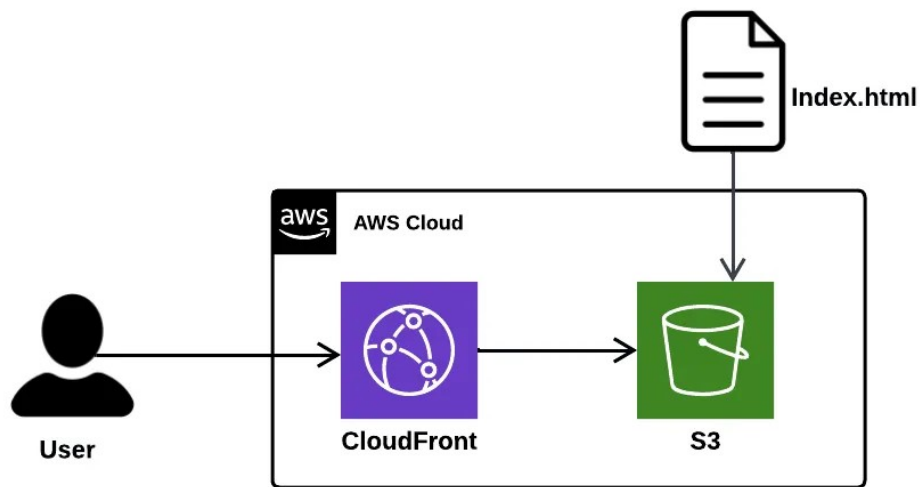
Topics :-

Step 1: Create a bucket

The following instructions provide an overview of how to create your buckets for website hosting. For detailed, step-by-step instructions on creating a bucket.

To create a bucket

- Sign in to the AWS Management Console and open the Amazon S3 console at https://console.aws.amazon.com/s3/.

- Choose **Create bucket**.

- Enter the **Bucket name** (for example, `webbucket`).

- Choose the Region where you want to create the bucket.

  Choose a Region that is geographically close to you to minimize latency and costs, or to address regulatory requirements. The Region that you choose determines your Amazon S3 website endpoint.

- To accept the default settings and create the bucket, choose **Create**.

Step 2: Enable static website hosting

After you create a bucket, you can enable static website hosting for your bucket.

To enable static website hosting

- Sign in to the AWS Management Console and open the Amazon S3 console at https://console.aws.amazon.com/s3/.

- In the **Buckets** list, choose the name of the bucket that you want to enable static website hosting for.

- Choose **Properties**.

- Under **Static website hosting**, choose **Edit**.

- Choose **Use this bucket to host a website**.

- Under **Static website hosting**, choose **Enable**.

- In **Index document**, enter the file name of the index document,
  typically `index.html`.

  The index document name is case sensitive and must exactly match the
  file name of the HTML index document that you plan to upload to your S3
  bucket. When you configure a bucket for website hosting, you must
  specify an index document. Amazon S3 returns this index document when
  requests are made to the root domain or any of the subfolders.

- (Optional) If you want to specify advanced redirection rules,
 in **Redirection rules**, enter JSON to describe the rules.

  For example, you can conditionally route requests according to specific
  object key names or prefixes in the request.

- Choose **Save changes**.

  Amazon S3 enables static website hosting for your bucket. At the bottom
  of the page, under **Static website hosting**, you see the website endpoint
  for your bucket.

- Under **Static website hosting**, note the **Endpoint**.

  The **Endpoint** is the Amazon S3 website endpoint for your bucket. After
  you finish configuring your bucket as a static website, you can use this
  endpoint to test your website.
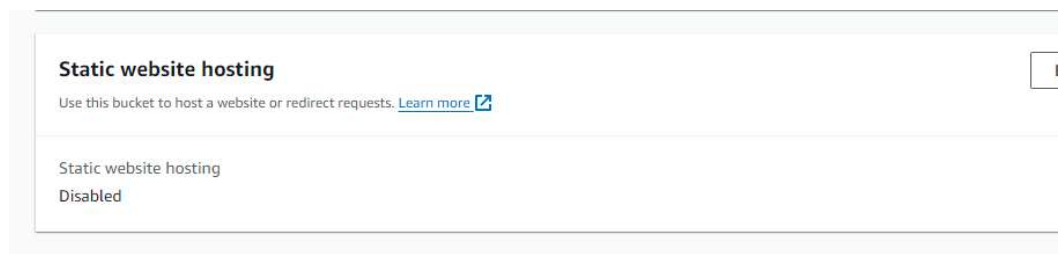
Step 3: Edit Block Public Access settings

By default, Amazon S3 blocks public access to your account and buckets. If you want to use a bucket to host a static website, you can use these steps to edit your block public access settings.

- Open the Amazon S3 console at https://console.aws.amazon.com/s3/.
- Choose the name of the bucket that you have configured as a static website.
- Choose **Permissions**.
- Under **Block public access (bucket settings)**, choose **Edit**.
- Clear **Block *all* public access**, and choose **Save changes**.

  Warning

  Before you complete this step, review Blocking public access to your Amazon S3 storage to ensure you understand and accept the risks involved with allowing public access. When you turn off block public access settings to make your bucket public, anyone on the internet can access your bucket. We recommend that you block all public access to your buckets.

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 c
ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only t
bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings,
that your applications will work correctly without public access. If you require some level of public access to your buckets or objec
within, you can customize the individual settings below to suit your specific storage use cases. **Learn more** ☑

> ⓘ **Account settings for Block Public Access are currently turned on**
> Account settings for Block Public Access that are enabled apply even if they are disabled for this buck

☐ **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 or

  ☐ **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 publi
  ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3
  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 polici**
  S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't ch
  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 pt**
  policies
  S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to bucke
  objects.

Amazon S3 turns off Block Public Access settings for your bucket. To create a public, static website, you might also have to edit the Block Public Access settings for your account before adding a bucket policy.

Step 4: Add a bucket policy that makes your

bucket content publicly available

After you edit S3 Block Public Access settings, you can add a bucket policy to grant public read access to your bucket. When you grant public read access, anyone on the internet can access your bucket.

Important

The following policy is an example only and allows full access to the contents of your bucket.

- Under **Buckets**, choose the name of your bucket.
- Choose **Permissions**.
- Under **Bucket Policy**, choose **Edit**.
- To grant public read access for your website, copy the following bucket policy, and paste it in the **Bucket policy editor**.

```
{

    "Version": "2012-10-17",

    "Statement": [

        {

            "Sid": "PublicReadGetObject",

            "Effect": "Allow",
```

```
          "Principal": "*",

          "Action": [

              "s3:GetObject"

          ],

          "Resource": [

              "arn:aws:s3:::Bucket-Name/*"

          ]

      }

    ]

}
```

- Update the `Resource` to your bucket name.

  In the preceding example bucket policy, `Bucket-Name` is a placeholder for the bucket name. To use this bucket policy with your own bucket, you must update this name to match your bucket name.

- Choose **Save changes**.

  A message appears indicating that the bucket policy has been

successfully added.

If you see an error that says `Policy has invalid resource`, confirm that the bucket name in the bucket policy matches your bucket name.

If you get an error message and cannot save the bucket policy, check your account and bucket Block Public Access settings to confirm that you allow public access to the bucket.

Step 5: Configure an index document

When you enable static website hosting for your bucket, you enter the name of the index document (for example, `index.html`). After you enable static website hosting for the bucket, you upload an HTML file with this index document name to your bucket.

To configure the index document

- Create an `index.html` file.

  If you don't have an `index.html` file, you can use the following HTML to create one:

  ```
  <html xmlns="http://www.w3.org/1999/xhtml" >



  <head>



      <title>My Website Home Page</title>



  </head>



  <body>
  ```

```
<h1>Welcome to my website</h1>

<p>Now hosted on Amazon S3!</p>

</body>

</html>
```

- Save the index file locally.

  The index document file name must exactly match the index document name that you enter in the **Static website hosting** dialog box. The index document name is case sensitive. For example, if you enter `index.html` for the **Index document** name in the **Static website hosting** dialog box, your index document file name must also be `index.html` and not `Index.html`.

- Sign in to the AWS Management Console and open the Amazon S3 console at https://console.aws.amazon.com/s3/.

- In the **Buckets** list, choose the name of the bucket that you want to use to host a static website.

- Enable static website hosting for your bucket, and enter the exact name of your index document (for example, `index.html`).

  After enabling static website hosting, proceed to step 6.

- To upload the index document to your bucket, do one of the following:

  - Drag and drop the index file into the console bucket listing.

  - Choose **Upload**, and follow the prompts to choose and upload the index file.

- (Optional) Upload other website content to your bucket.

Step 6: Configure an error document

When you enable static website hosting for your bucket, you enter the name of the error document (for example, `404.html`). After you enable static website hosting for the bucket, you upload an HTML file with this error document name to your bucket.

To configure an error document

- Create an error document, for example `404.html`.
- Save the error document file locally.

  The error document name is case sensitive and must exactly match the name that you enter when you enable static website hosting. For example, if you enter `404.html` for the **Error document** name in the **Static website hosting** dialog box, your error document file name must also be `404.html`.

- Sign in to the AWS Management Console and open the Amazon S3 console at https://console.aws.amazon.com/s3/.
- In the **Buckets** list, choose the name of the bucket that you want to use to host a static website.
- Enable static website hosting for your bucket, and enter the exact name of your error document (for example, `404.html`).

  After enabling static website hosting, proceed to step 6.

- To upload the error document to your bucket, do one of the following:
  - Drag and drop the error document file into the console bucket listing.
  - Choose **Upload**, and follow the prompts to choose and upload the index file.

Step 7: Test your website endpoint

After you configure static website hosting for your bucket, you can test your website endpoint.

- Under **Buckets**, choose the name of your bucket.

- Choose **Properties**.

- At the bottom of the page, under **Static website hosting**, choose your **Bucket website endpoint**.

  Your index document opens in a separate browser window.

Now you have hosted a website on Amazon S3. This website is available at the Amazon S3 website endpoint. However, you might have a domain, such as `example.com`, that you want to use to serve the content from the website you created.

Step 8: Clean up

If you created your static website only as a learning exercise, delete the AWS resources that you allocated so that you no longer accrue charges. After you delete your AWS resources, your website is no longer available.