

CLOUDCOMPUTINGWITH AWS SERVICES PROJECT

Deploy a Static Website on AWS



BY:-ANIKET MISHRA

STEP 1: Sign in to AWS Management Console

Click on the **Open Console** button, and you will get redirected to AWS Console in a new browser tab.

STEP 2: Creating a S3 Bucket

In this task, we are going to create a new S3 bucket in the ap-south-1 region with a unique name disabling ACLs, and allowing public access for hosting the static website.

1. Navigate to **S3** by clicking on the **Services** menu at the top, then click on **S3** in the **Storage** section.
2. In the S3 dashboard, click on the **Create Bucket** button.

In the General Configuration, **Bucket name:** Enter **STATICWEB** **Note:** S3 Bucket names are globally unique, choose an available name. Maybe you can enter your name and create one.


1. AWS Region: Select **(MUMBAI) ap-south-1**
2. Object ownership: Select the **ACLs disabled (recommended)** option

In the option of **Block Public Access settings for this bucket**, **Uncheck** the option of **Block all public access**. **Check** the I acknowledge that the current settings might result in this bucket and the objects within becoming public checkboxes.

7. Keep everything default and click on the **Create Bucket** button.

☐ **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.

STEP 3: Enable Static Website Hosting settings

In this task, we will enable static website hosting for our S3 bucket, configure it to use index.html and error.html, copy the provided endpoint, upload two files, and configure the bucket policy by copying its ARN and pasting the provided policy code.

1. To proceed, go to the **S3 bucket name** that you created and click on it. After that, navigate to the **Properties** tab which can be found at the top of the screen.
2. Scroll down to the **Static website hosting** section and click on the **Edit** button.

Static website hosting

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

Edit

Static website hosting

Disabled

1. In the **Static website hosting** dialog box
2. Static website hosting: Select **Enable**
3. Hosting type: Choose **Host a static website**
4. Index document: Type ***index.html***
5. Error document: Type ***error.html***
6. Click on **Save Changes**.

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](#)

 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](#)

Index document

Specify the home or default page of the website.

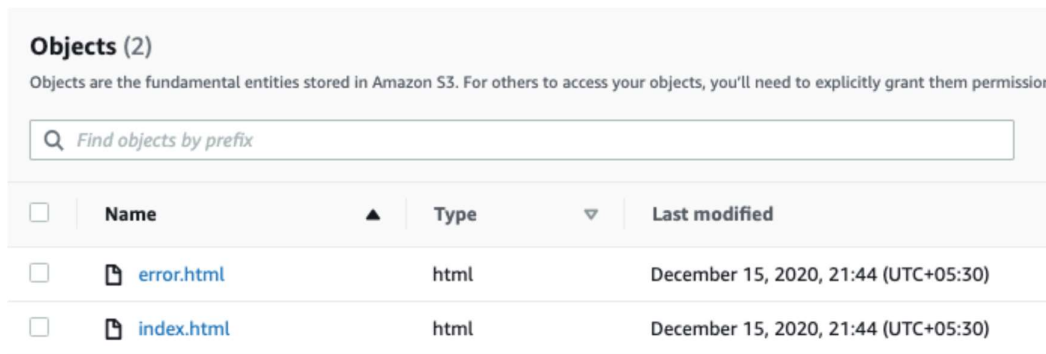
index.html

Error document - *optional*



This is returned when an error occurs.

error.html

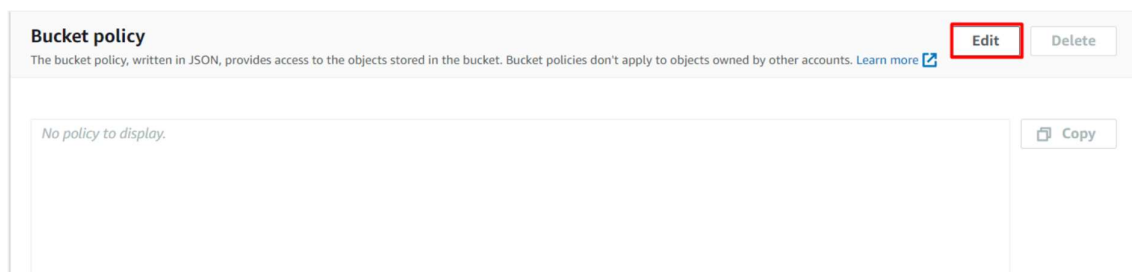
4. Go to the **Properties** tab of your S3 bucket, and find the **Static website hosting** section. **Copy** the Endpoint provided in this section to your clipboard and **save** it for future reference.
5. The next step is to download the zip file by clicking on the [link](#), extract it, and upload two files named **index.html** and **error.html** to the S3 bucket you created earlier.



The screenshot shows the 'Objects (2)' section of an Amazon S3 bucket. It includes a search bar with the placeholder text 'Find objects by prefix'. Below the search bar is a table listing two objects: 'error.html' and 'index.html'. Both objects are of type 'html' and were last modified on 'December 15, 2020, 21:44 (UTC+05:30)'. Each row has a checkbox on the left for selection.

<input type="checkbox"/>	Name	Type	Last modified
<input type="checkbox"/>	 error.html	html	December 15, 2020, 21:44 (UTC+05:30)
<input type="checkbox"/>	 index.html	html	December 15, 2020, 21:44 (UTC+05:30)

6. To configure your S3 bucket, access the **Permissions** tab and make the necessary configurations.
 - In the **Permissions** tab, Click on the **Edit** button beside the **Bucket Policy**.



- You will be able to see a Blank policy editor.
- Before creating the policy, you will need to copy the **ARN** (Amazon Resource Name) of your bucket.

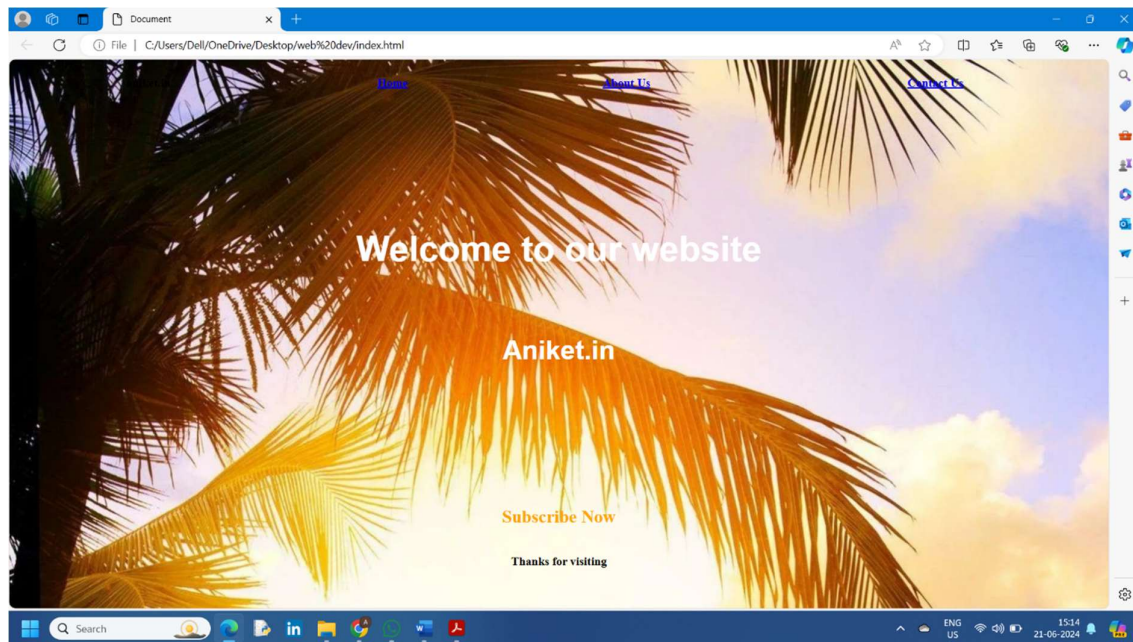
- Copy the **ARN** of your bucket to the clipboard. It is displayed at the top of the policy editor. it will look like **ARN: “arn:aws:s3:::your-bucket-name”**.
- In the policy below, **Update** the bucket ARN on the Resource key value and **paste** the below policy code in the editor.

```
{
    "Id": "Policy1",
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Stmt1",
            "Action": [
                "s3:GetObject"
            ],
            "Effect": "Allow",
            "Resource": "replace-this-string-with-your-bucket-arn/*",
            "Principal": "*"
        }
    ]
}
```

Click on the **Save Changes** button.

STEP 4: Test the website

1. Now copy the **static website URL** (that we saved earlier) and run it in your browser. You will be able to see the index.html file's text. A sample screenshot is attached below:



STEP 5: Test the website's error page

Copy the static website URL (which we saved earlier), but this time, add some random characters to the end of the URL to break it. When satisfied, hit **[Enter]**. You will be redirected to the **error.html** page

