

# *Hosting A static website with Amazon S3*

---

## **WHAT IS AMAZON S3?**

Amazon S3 (Simple Storage Service) is a service offered by AWS for object storage through a web service interface. It can be used to store or retrieve any amount of data such as documents, images, videos, etc.

**S3 bucket** is a resource in Amazon S3. It is a container where files and folders can be uploaded.

### **What is Amazon CloudFront?**

Amazon CloudFront is a content delivery network (CDN) service offered by AWS. It is used to speed up content delivery and can be integrated with Amazon S3.

### **Benefits of using AWS S3 bucket**

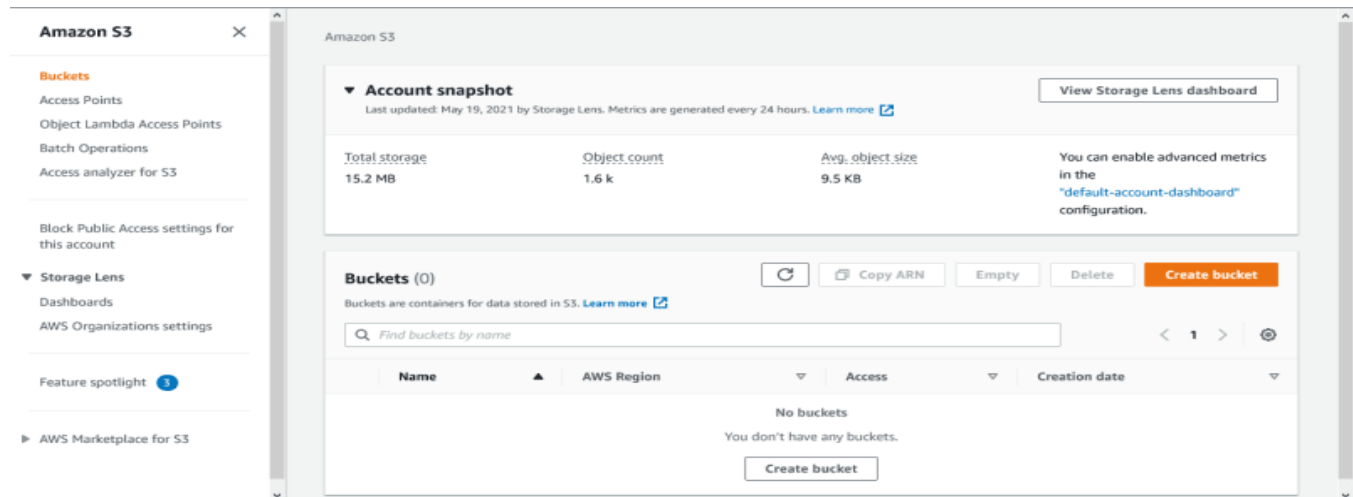
- Each object can contain up to 5TB of data.
  - A resource can only be accessed by the owner until permission is granted to others which makes it more secure.
  - It is cheap.
  - You can enable Multi-Factor Authentication (MFA) delete on an S3 bucket to prevent accidental deletions and unintentional data loss.
-

# HOSTING A STATIC WEBSITE WITH AMAZON S3

## Step 1 — Create an S3 bucket

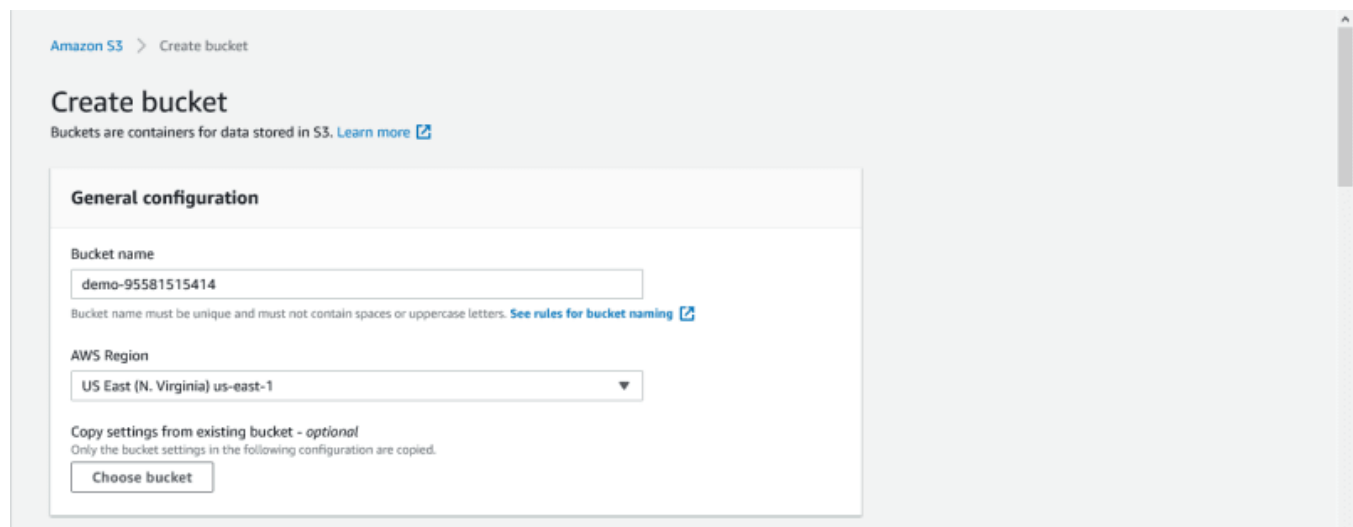
You will need to create an S3 bucket to put your website's files and folders.

To do this, login into your AWS management console and click on **Services** on the top navbar. From the **Services** drop-down, select **S3** from the **Storage** section. This should display the **S3** dashboard.



From the S3 dashboard, click on **Create bucket**. Give the bucket a unique name, the name you choose must be globally unique (for best practice, attach your AWS account ID to the name).

Next, choose your preferred **AWS Region** from the drop-down.




Under **Block Public Access settings for this bucket** section, uncheck the **Block all public access** checkbox and accept the acknowledgement. This is done to make the bucket accessible to the public because you are going to host a website in it.

**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 on **disable** for Bucket Versioning.

You can also **Add tag** to the bucket for easy identification.

Under **Default encryption** section, click on **disable** for Server-side encryption.

**Bucket Versioning**

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. [Learn more](#)

Bucket Versioning

☒ Disable  
☐ Enable

**Tags (1) - optional**

Track storage cost or other criteria by tagging your bucket. [Learn more](#)

| Key  | Value - optional |        |
|------|------------------|--------|
| Name | test             | Remove |

Add tag

**Default encryption**

Automatically encrypt new objects stored in this bucket. [Learn more](#)

Server-side encryption

☒ Disable

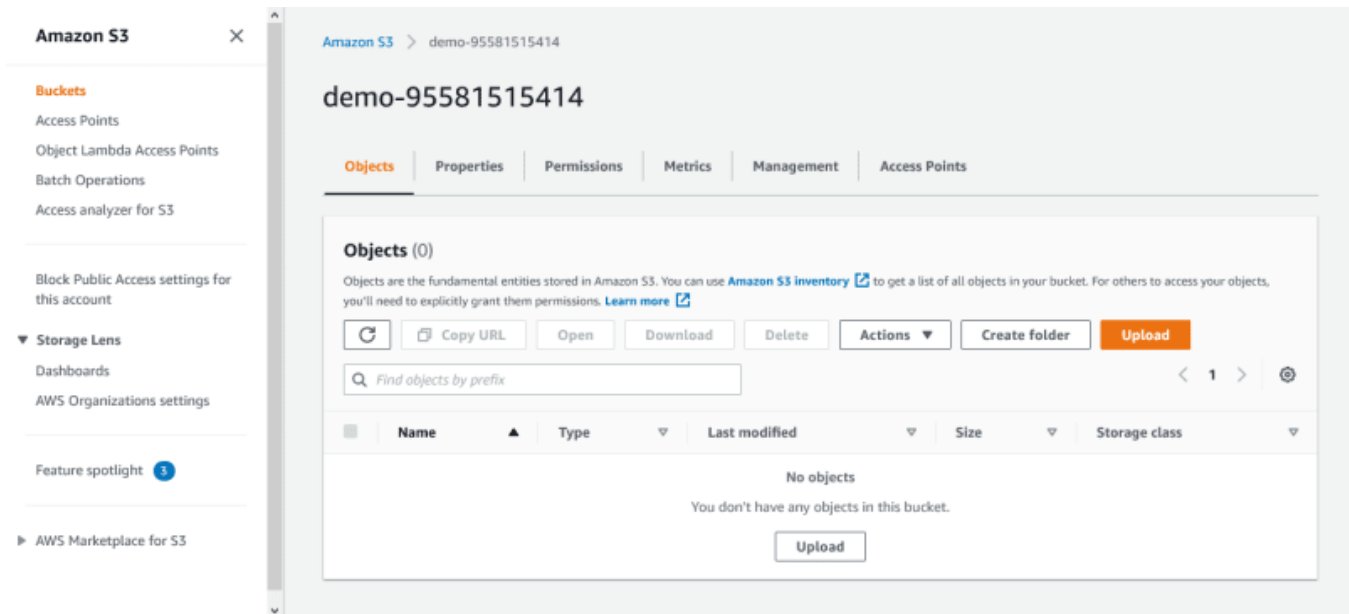
Then click on **Create bucket**.

## Step 2 — Upload web files to S3 bucket

After creating the bucket, you need to upload your website's files and folders into it.

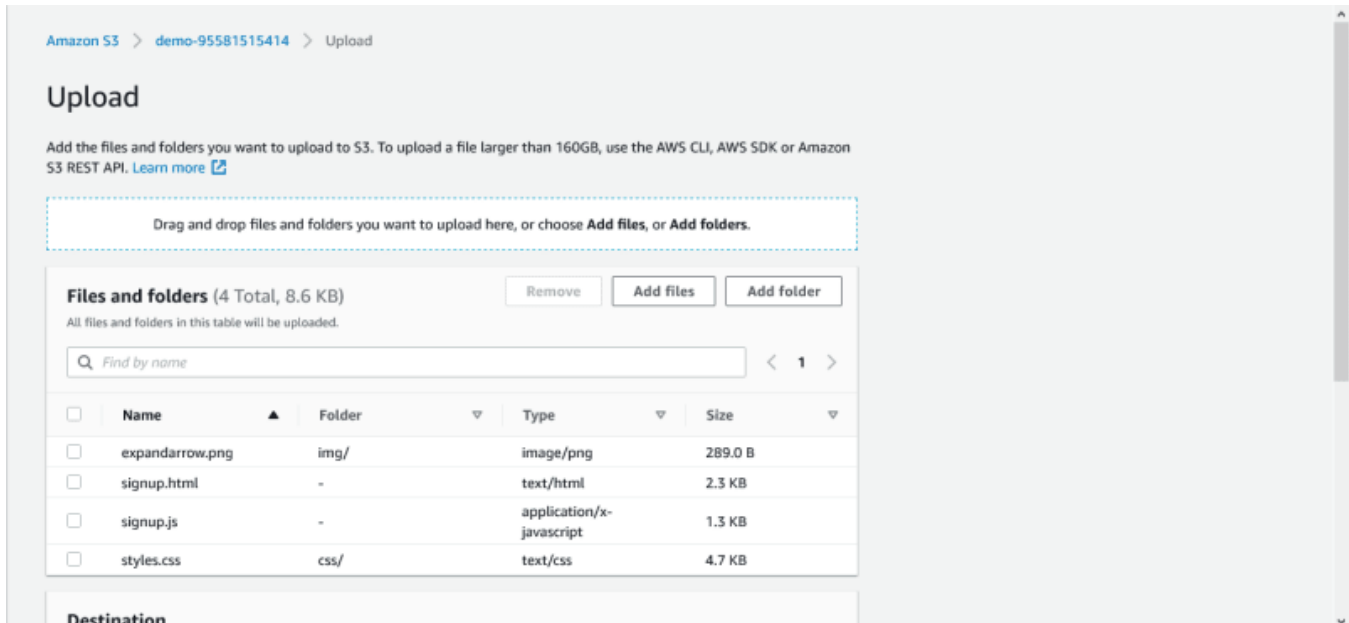
From the **S3** dashboard, click on the **name** of the bucket you just created.

On the **Objects** tab, you can see that the bucket is currently empty, click on the **Upload** button.



This should take you to the **Upload** page. Click **Add files** to add the website files and use **Add folder** to add the website folders.

**Note:** The whole website folder shouldn't be added at once. Instead, add its content one after the other. For example, with the demo project linked up top, I uploaded my **signup.html** as a file, **signup.js** as a file, **css** as a folder and **img** as a folder.



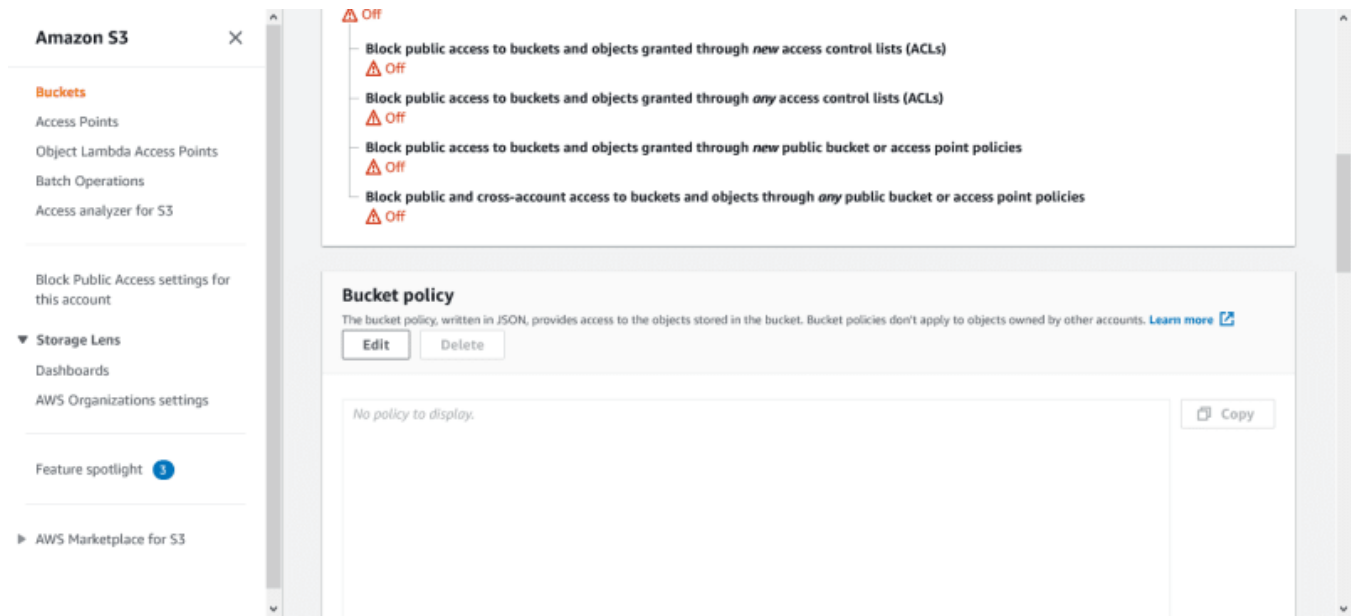
After the necessary files and folders have been added, scroll down and click on **Upload**.

The uploading should be done in a few minutes depending on your network and content size. Also, please do not close the tab while the upload process is going on.

### Step 3 — Secure S3 bucket through IAM policies

Now you need to add some policies to secure your bucket.

From the **S3** dashboard, click on the **name** of the bucket, then click on **Permissions** tab. Scroll down to the **Bucket policy** section and click on its **Edit** button.

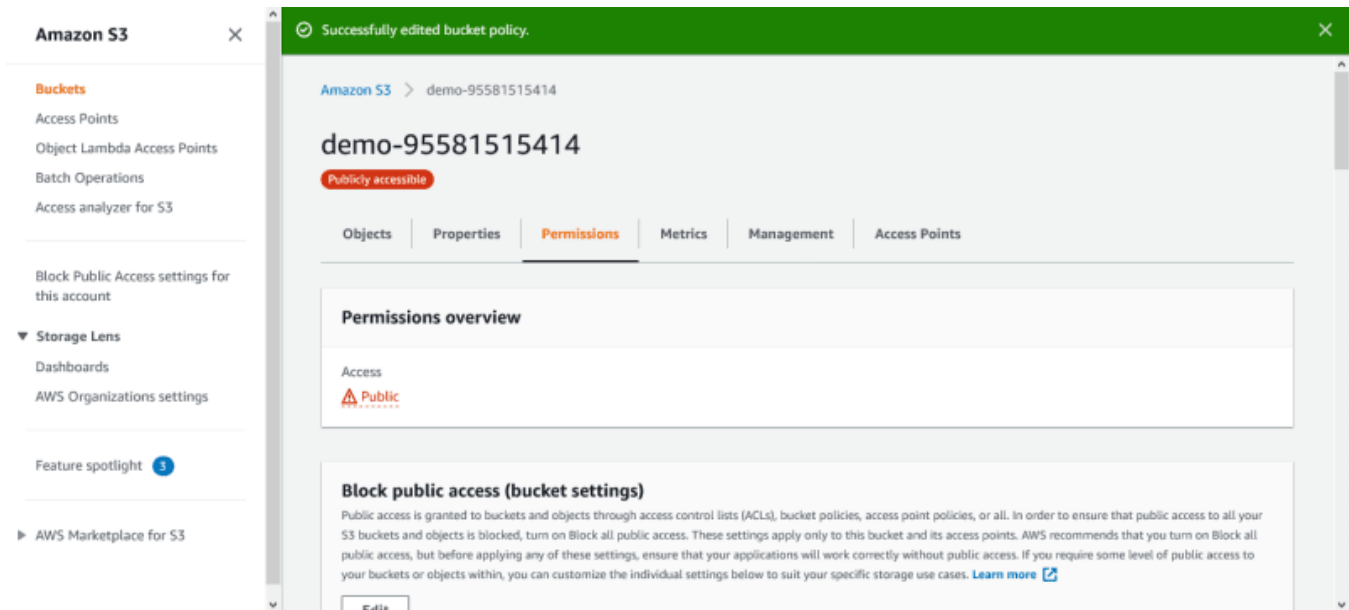


Add the following bucket policy to it and make sure to replace bucket-name with the name of your bucket.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AddPerm",
      "Effect": "Allow",
      "Principal": "*",
      "Action": ["s3:GetObject"],
      "Resource": ["arn:aws:s3:::bucket-name/*"]
    }
  ]
}
```

Then scroll down and click on **Save changes**.

This should change the bucket **access** to public, as shown below.



## Step 4 — Configure S3 bucket

You need to specify the default page and error page for your website.

From the **S3** dashboard, click on the **name** of the bucket, then click on the **Properties** tab.

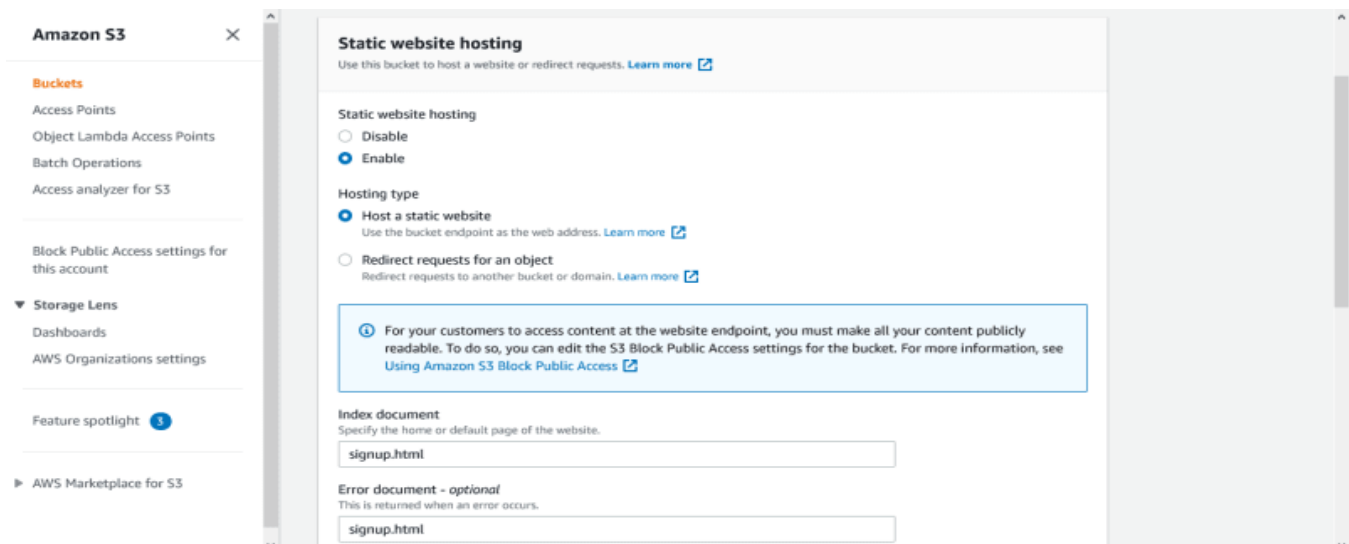
Scroll down to the **Static website hosting** section and click on its **Edit** button.

Select **Enable** for Static website hosting.

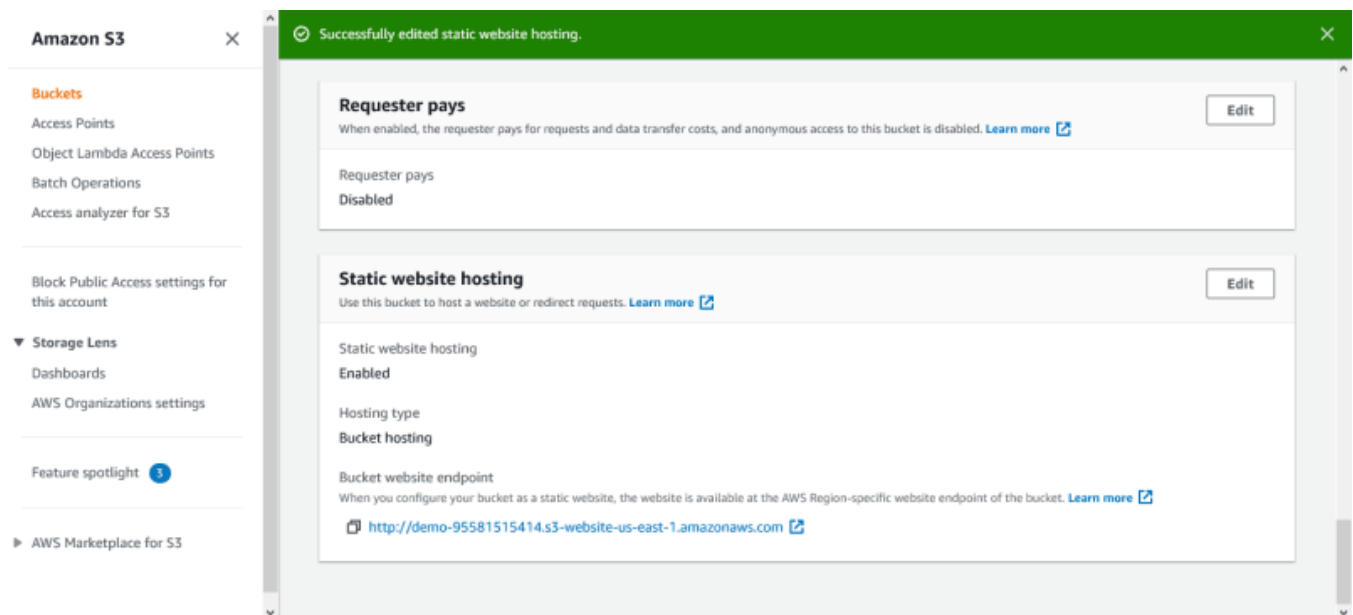
Also, select **Host a static website** for the Hosting type.

Enter the file for your **Index document** and **Error document**. The **Error document** is optional. I used **signup.html** for both **Index document** and **Error document**.

Scroll down and click on **Save Changes**.



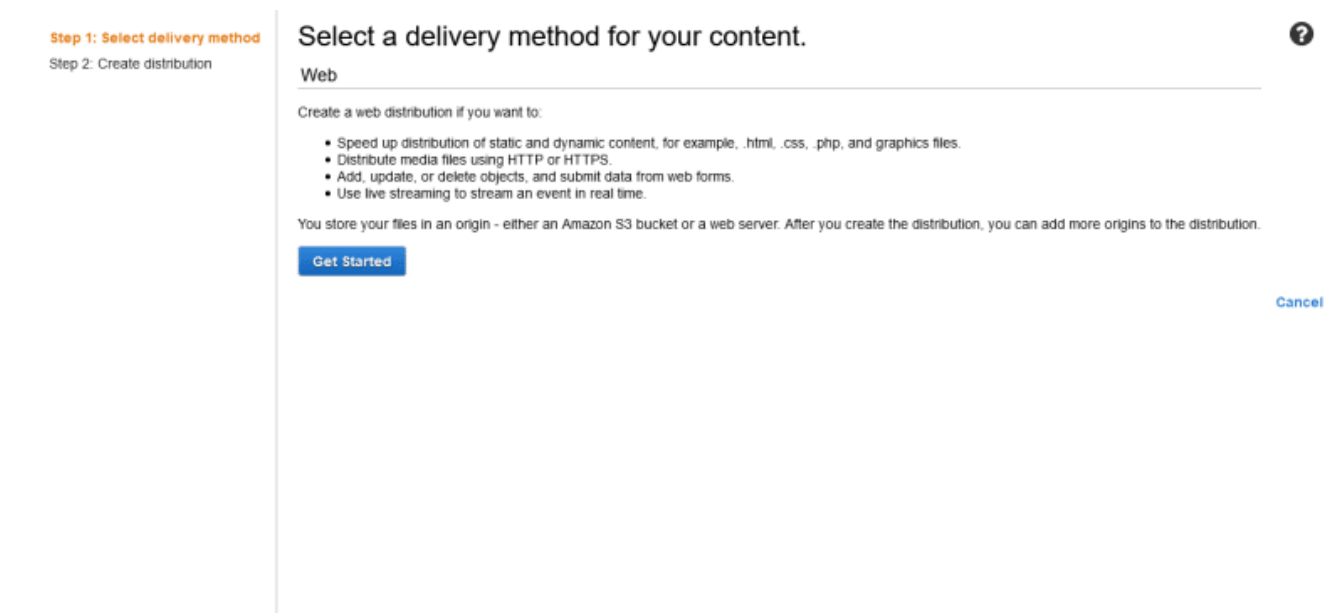
After saving, If you click on the bucket website endpoint, it would display your website.



## Step 5 — Serve content from S3 bucket with CloudFront

From the **Services** drop-down, scroll down to **Networking & Content Delivery** section and click on **CloudFront**. This should take you to the CloudFront dashboard.

Click on **Create Distribution**. On **Select a delivery method for your content** page, click on **Get Started** under the **Web** section.



Under the **Origin Settings** section, click on the **Origin Domain Name** field and select the S3 bucket you created earlier. In the **Origin Path** field, enter **/** to indicate root level.

For **Restrict Bucket Access**, select **Yes**.

For **Origin Access Identity**, select **Create a New Identity**.

For **Grant Read Permissions on Bucket**, select **Yes, Update Bucket Policy**.

[Step 1: Select delivery method](#)

**[Step 2: Create distribution](#)**

### Origin Settings

| Origin Domain Name               | <input type="text" value="demo-95581515414.s3.amazonaws.com"/>  |             |       |                      |                      |  |
|----------------------------------|---|-------------|-------|----------------------|----------------------|--|
| Origin Path                      | <input type="text"/>  |             |       |                      |                      |  |
| Enable Origin Shield             | <input type="radio"/> Yes<br><input checked="" type="radio"/> No  |             |       |                      |                      |  |
| Origin ID                        | <input type="text" value="S3-demo-95581515414"/>  |             |       |                      |                      |  |
| Restrict Bucket Access           | <input checked="" type="radio"/> Yes<br><input type="radio"/> No  |             |       |                      |                      |  |
| Origin Access Identity           | <input checked="" type="radio"/> Create a New Identity<br><input type="radio"/> Use an Existing Identity  |             |       |                      |                      |  |
| Comment                          | <input type="text" value="access-identity-demo-95581515414.s3."/>   |             |       |                      |                      |  |
| Grant Read Permissions on Bucket | <input checked="" type="radio"/> Yes, Update Bucket Policy<br><input type="radio"/> No, I Will Update Permissions   |             |       |                      |                      |  |
| Origin Connection Attempts       | <input type="text" value="3"/>  |             |       |                      |                      |  |
| Origin Connection Timeout        | <input type="text" value="10"/>   |             |       |                      |                      |  |
| Origin Custom Headers            | <table><thead><tr><th>Header Name</th><th>Value</th></tr></thead><tbody><tr><td><input type="text"/></td><td><input type="text"/></td></tr></tbody></table> | Header Name | Value | <input type="text"/> | <input type="text"/> |  |
| Header Name                      | Value   |             |       |                      |                      |  |
| <input type="text"/>             | <input type="text"/>  |             |       |                      |                      |  |

Scroll down to the **Default Cache Behavior Settings** section. For **Viewer Protocol Policy**, select **Redirect HTTP to HTTPS**.

[Step 1: Select delivery method](#)

**[Step 2: Create distribution](#)**

### Default Cache Behavior Settings

|                                   |  |  |
|-----------------------------------|--|--|
| Path Pattern                      | <input type="text" value="Default (*)"/>   |  |
| Viewer Protocol Policy            | <input type="radio"/> HTTP and HTTPS<br><input checked="" type="radio"/> Redirect HTTP to HTTPS<br><input type="radio"/> HTTPS Only                          |  |
| Allowed HTTP Methods              | <input checked="" type="radio"/> GET, HEAD<br><input type="radio"/> GET, HEAD, OPTIONS<br><input type="radio"/> GET, HEAD, OPTIONS, PUT, POST, PATCH, DELETE |  |
| Field-level Encryption Config     | <input type="text" value=""/>  |  |
| Cached HTTP Methods               | <input type="text" value="GET, HEAD (Cached by default)"/>   |  |
| Cache and origin request settings | <input checked="" type="radio"/> Use a cache policy and origin request policy<br><input type="radio"/> Use legacy cache settings                             |  |
| Cache Policy                      | <input type="text" value="Managed-CachingOptimized"/>  |  |
|                                   | <input type="button" value="View policy details"/>   |  |
|                                   | <a href="#">Learn More</a>   |  |
| Origin Request Policy             | <input type="text" value=""/>  |  |
|                                   | <input type="button" value="View policy details"/>   |  |

Next, scroll down to the **Distribution Settings** section. Inside the **Default Root Object** field, enter the filename at the root level, which should be your landing page. I used **signup.html** as my **Default Root Object**.

Leave the rest of the options as default and click on **Create Distribution**.



Step 1: Select delivery method  
Step 2: Create distribution

Supported HTTP Versions ☒ HTTP/2, HTTP/1.1, HTTP/1.0  
☐ HTTP/1.1, HTTP/1.0

Default Root Object

Standard Logging ☐ On  
☒ Off

S3 Bucket for Logs

Log Prefix

Cookie Logging ☐ On  
☒ Off

Enable IPv6 ☒ [Learn more](#)

Comment

Distribution State ☒ Enabled  
☐ Disabled

[Cancel](#) [Back](#) [Create Distribution](#)

Now, you can see the distribution you created from the CloudFront dashboard. It might take a few minutes for it to be deployed.

**CloudFront**

- Distributions
- Policies
- Functions **NEW**
- What's new
- Telemetry
  - Monitoring
  - Alarms
  - Logs **NEW**
- Reports & analytics
  - Cache statistics
  - Popular objects
  - Top referrers
  - Usage
  - Viewers
- Security

How to accelerate your dynamic content with Amazon EC2 as an origin. [Learn more](#)

**Important:** On March 23, 2021, CloudFront will begin migrating the Certificate Authority for the \*.cloudfront.net certificate. For more information, refer to the [AWS Knowledge Center](#).

### CloudFront Distributions

[Create Distribution](#) [Distribution Settings](#) [Delete](#) [Enable](#) [Disable](#)

Viewing: Any Delivery Method Any State

|                          | Delivery Method | ID            | Domain Name   | Comment | Origin   | CNAMEs | Status  | State   | Last Modified   |
|--------------------------|-----------------|---------------|---------------|---------|----------|--------|---------|---------|-----------------|
| <input type="checkbox"/> | Web             | E1BRL41DH5DAF | d34504qtm1w2p | -       | demo-95t | -      | In Prog | Enabled | 2021-05-21 15:1 |

After the CloudFront distribution has been deployed, copy the URI from the Domain Name column and paste it into your browser. Yay! 🎉 That's it!