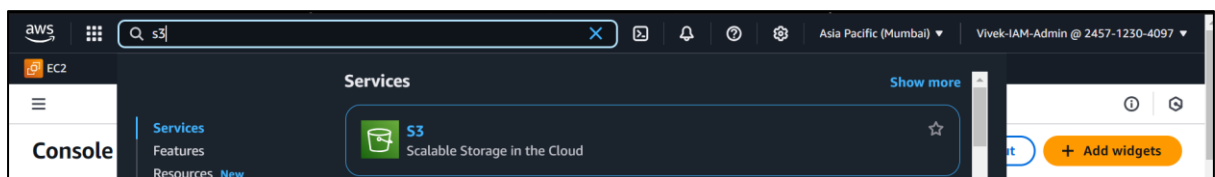


# Host a Website on Amazon S3

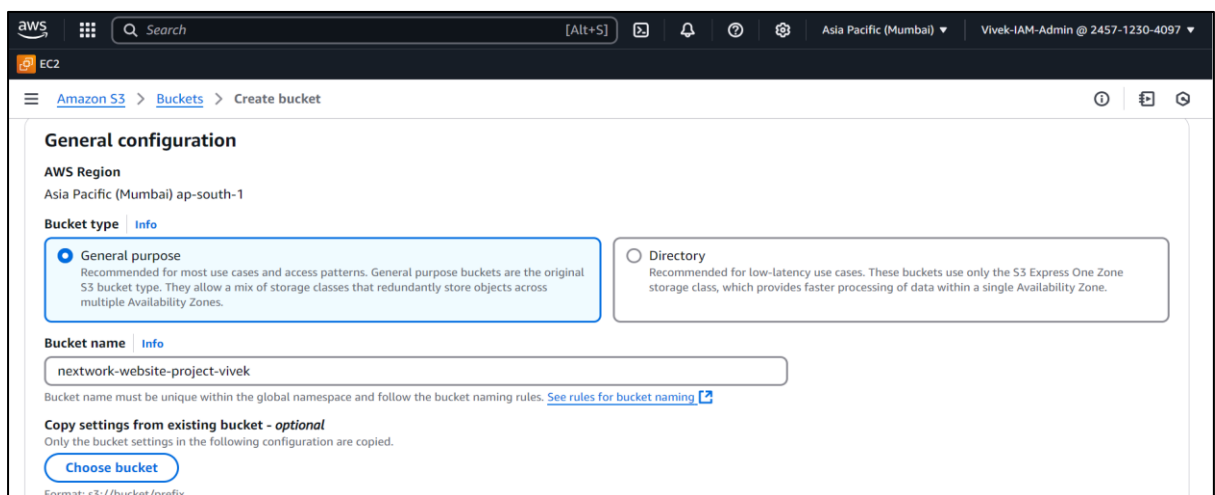
In this project, we'll use Amazon S3 (which stands for Amazon Simple Storage Service) to host a website.

## Create a bucket in Amazon S3

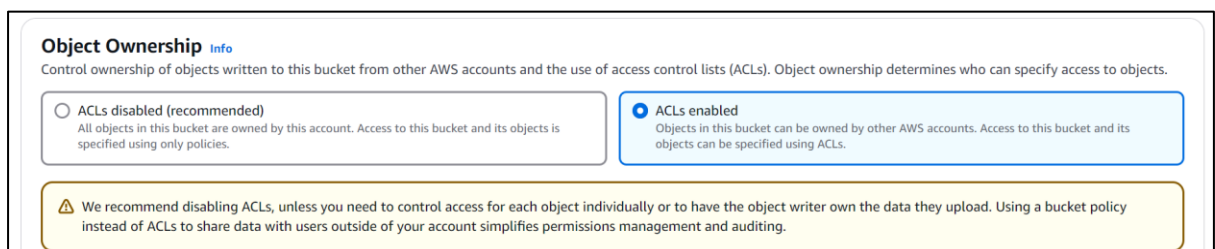
- Open Amazon S3.
- Create a storage space for your website files.
- **Log in to AWS.**
- In the AWS Management Console, search for **S3**.



- Select the **AWS Region** closest to you. You can find this at the top right corner of your AWS Management console, right next to your name!
- Choose **Create bucket**.
- For **Bucket name**, enter **nextwork-website-project-name**
- Make sure to **replace name with your name**.



- For **Object Ownership**, choose **ACLs enabled**.



- Choose **Bucket owner preferred**.
- For **Block Public Access settings for this bucket**, clear the check box for **Block all public access**.
- Check the box that says “**I acknowledge that the current settings might result in this bucket and the objects within becoming public.**”

**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.

- For **Bucket Versioning**, choose **Enable**.
- Choose **Create bucket**.

**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

**Successfully created bucket "network-website-project-vivek"**  
To upload files and folders, or to configure additional bucket settings, choose [View details](#).

Storage lens provides visibility into storage usage and activity trends. Metrics don't include directory buckets. [Learn more](#)

**General purpose buckets** | Directory buckets

**General purpose buckets (4)** [Info](#) [All AWS Regions](#)

Buckets are containers for data stored in S3.

Name	AWS Region	IAM Access Analyzer	Creation date
<a href="#">network-website-project-vivek</a>	Asia Pacific (Mumbai) ap-south-1	<a href="#">View analyzer for ap-south-1</a>	January 3, 2025, 13:29:25 (UTC+05:30)

## Upload website content to your bucket

your S3 bucket all created.

Time to get those website's files inside your bucket.

### In this step, get ready to:

- Download an HTML file that sets up your website.
- Download a zip file of images for your website.
- Upload both files into your S3 bucket.

the links for html file and images are as follows:

HTML File:

[https://storage.googleapis.com/nextwork\\_course\\_resources/courses/aws/AWS%20Project%20People%20projects/Project%203A%20Host%20a%20Static%20Website%20on%20Amazon%20S3/index.html](https://storage.googleapis.com/nextwork_course_resources/courses/aws/AWS%20Project%20People%20projects/Project%203A%20Host%20a%20Static%20Website%20on%20Amazon%20S3/index.html)

Images Zip File:

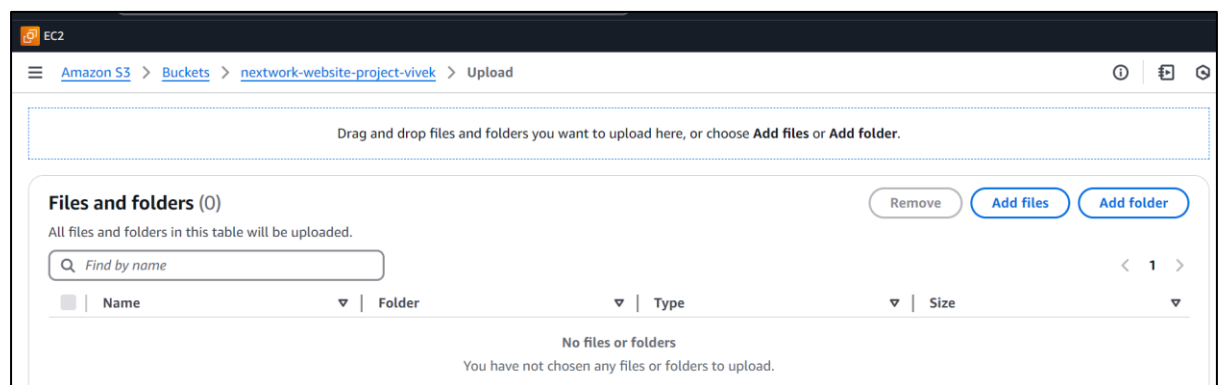
[https://storage.googleapis.com/nextwork\\_course\\_resources/courses/aws/AWS%20Project%20People%20projects/Project%203A%20Host%20a%20Static%20Website%20on%20Amazon%20S3/NextWork%20-%20Everyone%20should%20be%20in%20a%20job%20they%20love\\_files.zip](https://storage.googleapis.com/nextwork_course_resources/courses/aws/AWS%20Project%20People%20projects/Project%203A%20Host%20a%20Static%20Website%20on%20Amazon%20S3/NextWork%20-%20Everyone%20should%20be%20in%20a%20job%20they%20love_files.zip)

Download these files and save in your local computer before uploading to the bucket

Make sure you unzip the Images Zip File, inside the zip file you will find the folder **“NextWork - Everyone should be in a job they love\_files”**

You have to upload that folder along with html file to your S3 Bucket

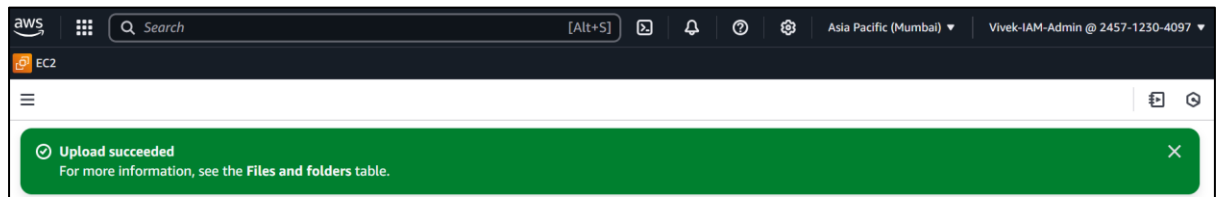
- In the **Buckets** section, choose the name of your new bucket.
- Upload these files into your bucket
- In Amazon S3 console with your bucket page open. Choose the **Objects** tab.
- Choose **Upload**.



- Choose **Add files**.
- Choose **index.html**.
- Choose **Add folder**.

Choose the unzipped folder “**NextWork - Everyone should be in a job they love\_files**” - NOT the zip file itself!

- You might get a popup that tells you that all files in that folder will be uploaded.
- Choose **Upload**.
- S3 will get to work right away!



## Configure a static website on Amazon S3

S3 bucket? Created.

Website files? Uploaded.

Next up, let's make your website available on the internet by setting up **static website hosting**!

**In this step, get ready to:**

- Configure your S3 bucket for static website hosting
- Visit your public website link.
- Make sure you're back in your bucket's page. If you're not sure, choose **Buckets** on the left-hand side navigation bar, and then choose the bucket you created for this project.
- Choose the **Properties** tab.
- Scroll all the way down to the **Static website hosting** panel.
- Choose **Edit**.
- Configure the following settings:
  - **Static web hosting:** Choose **Enable**.
  - **Hosting type:** Choose **Host a static website**.
  - **Index document:** Enter index.html

**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.

**Error document - optional**  
This is returned when an error occurs.

- Choose **Save changes**.
- In the **Static website hosting** panel, click on the URL under **Bucket website endpoint**.

Amazon S3 > Buckets > nextwork-website-project-vivek

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

We recommend using AWS Amplify Hosting for static website hosting  
 Deploy a fast, secure, and reliable website quickly with AWS Amplify Hosting. Learn more about [Amplify Hosting](#) or [View your existing Amplify apps](#) [Create Amplify app](#)

**S3 static website hosting**  
Enabled

**Hosting type**  
Bucket hosting

**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://nextwork-website-project-vivek.s3-website.ap-south-1.amazonaws.com>

**An error!** While accessing that URL

## 403 Forbidden

- Code: AccessDenied
- Message: Access Denied
- RequestId: QFJ0FVERWNPBBCVJ
- HostId: +Mt+euVoItM/1rXSNx9LavUinTAnujXTiF4DSOIofilWVmFBGygZH8kvhEGqur6lzxX6e1m8jCU=

### Why did I get this error?

Objects (in this case, the HTML and images files you uploaded) are private by default. This default setting helps keep your account's data secure.

The error message you're seeing is telling you that your static website is being hosted by S3, but the actual HTML/image files you've uploaded are still private. It's kind of like having a bucket on display, so everyone can see the bucket - but the contents are covered up, preventing anyone from seeing what's inside.

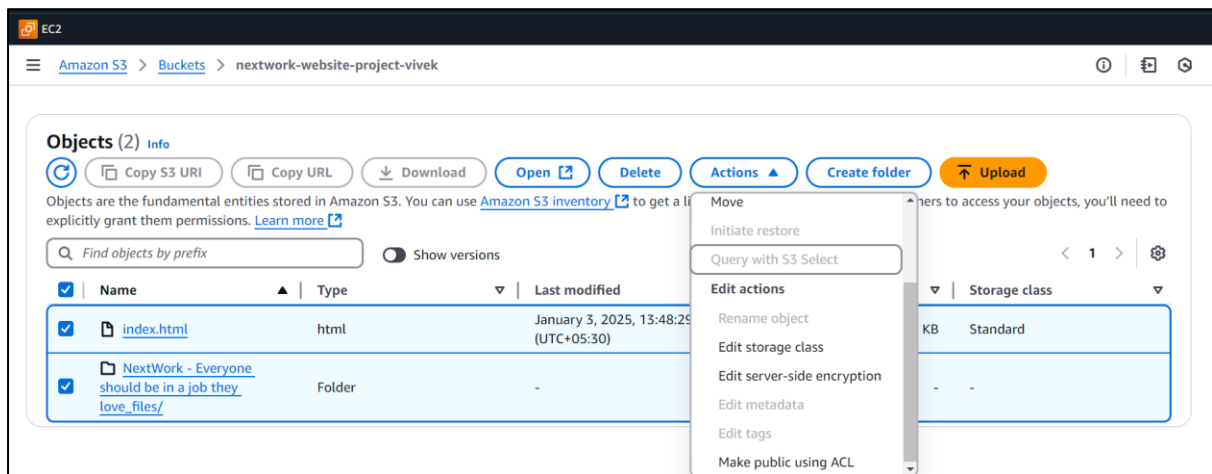
To solve this error, we need to set the permission of the objects to public - this is why we enabled ACLs

## Make objects in your S3 bucket public

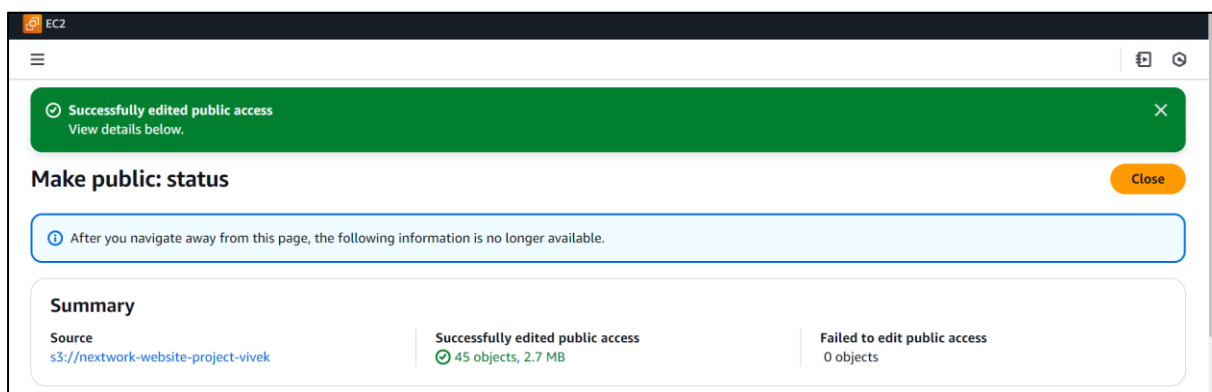
The only missing ingredient is to make your website files **publicly accessible**, so everyone has permission to view your website.

**In this step, get ready to:**

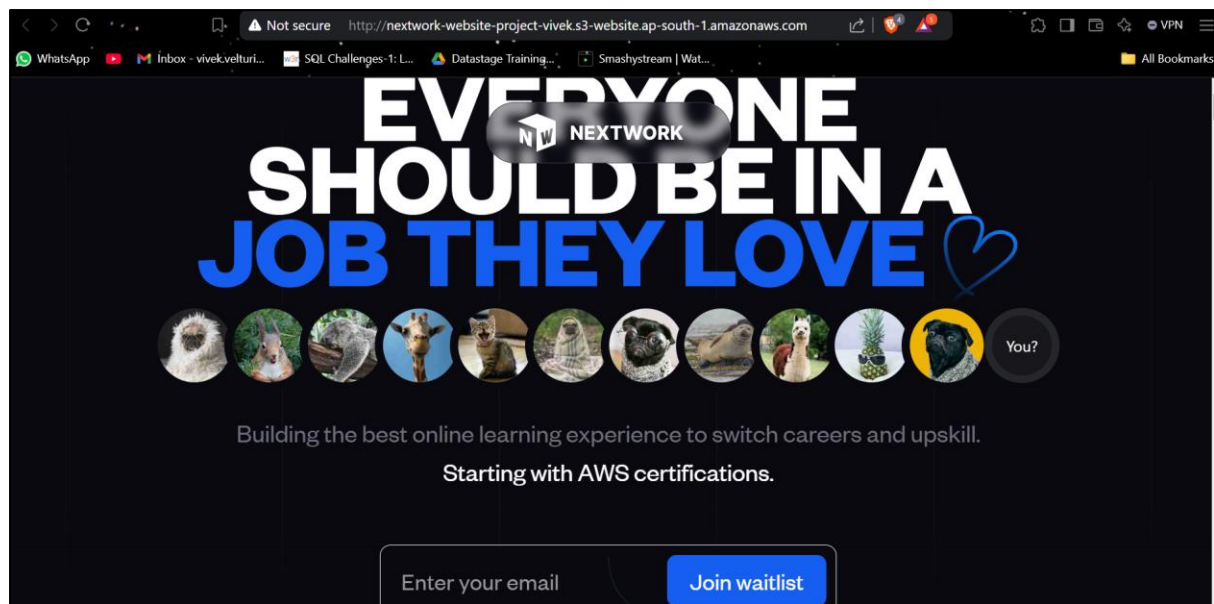
- Make your website files in S3 publicly accessible.
- See your website live on the internet!
- Keep the error message tab open and switch back to the Amazon S3 console tab.
- Would you still remember how to view your S3 bucket's objects? Try finding your bucket's **Objects** page and making your objects public using ACLs.
- Head to the **Objects** tab.
- Select the checkboxes next to your **index.html** file and the folder of website assets.
- In the **Actions** dropdown, choose **Make public using ACL**.



- Choose **Make public**.
- Once the green banner pops up, choose **Close**.



- Return to the web browser tab that has the **403 Forbidden** message.
- Refresh the tab.



**We have successfully hosted your very own static website on Amazon S3.**