Simple Static Website with AWS S3

Ibrahim S
s.ibrahim1581@gmail.com

Overview

This documentation will guide you through creating a basic static website hosted on Amazon S3.

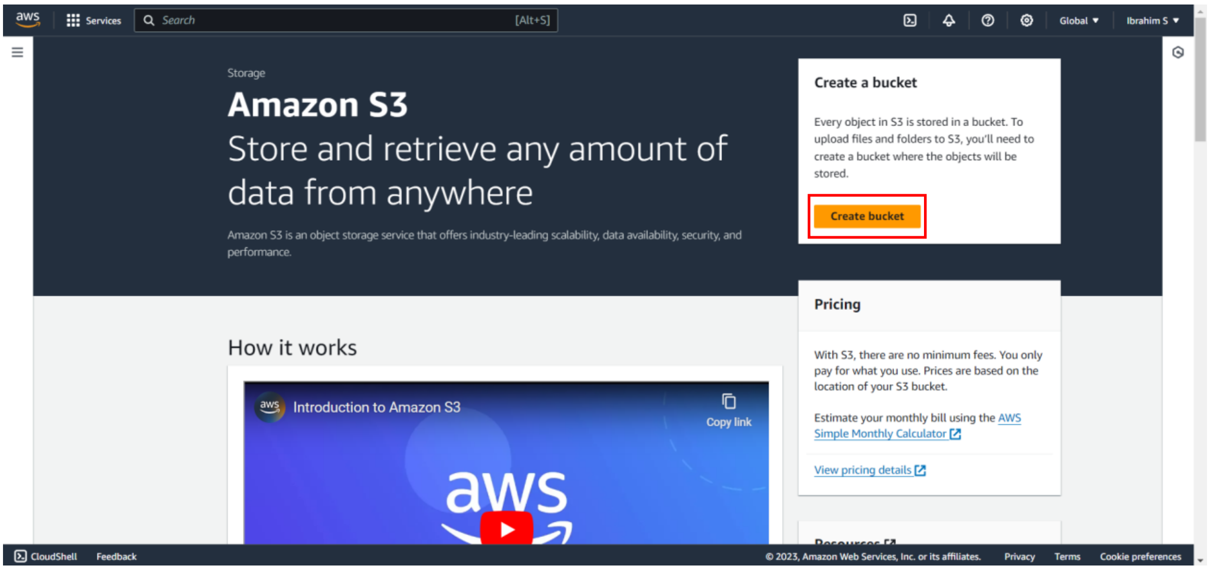
Table of Contents

1. Prerequisites

Before you begin, make sure you have an AWS account

2. Create an S3 Bucket

1. Go to the [Amazon S3 Console] (https://s3.console.aws.amazon.com/s3/).
2. Click on the "Create bucket" button.
3. Choose a globally unique name for your bucket (e.g., my-static-website-bucket).
4. Click through the default settings and click "Create bucket."



Storage

Amazon S3

Store and retrieve any amount of data from anywhere

Amazon S3 is an object storage service that offers industry-leading scalability, data availability, security, and performance.

Create a bucket

Every object in S3 is stored in a bucket. To upload files and folders to S3, you'll need to create a bucket where the objects will be stored.

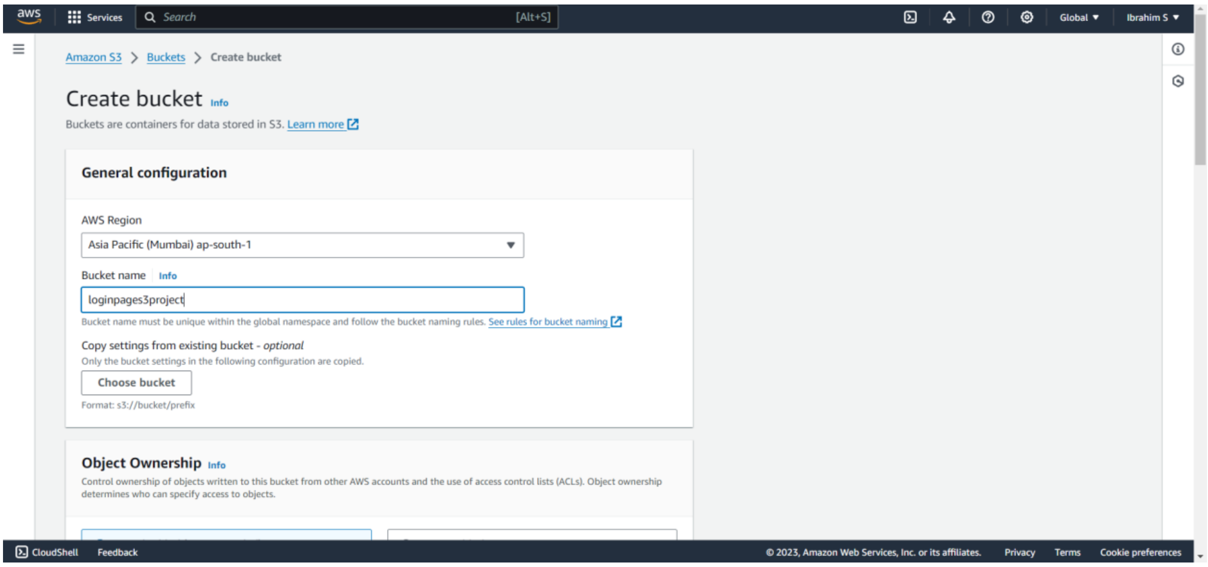
Pricing

With S3, there are no minimum fees. You only pay for what you use. Prices are based on the location of your S3 bucket.

Estimate your monthly bill using the AWS Simple Monthly Calculator

How it works

© 2023, Amazon Web Services, Inc. or its affiliates.



Amazon S3 > Buckets > Create bucket

Create bucket Info

Buckets are containers for data stored in S3. Learn more

General configuration

AWS Region

Asia Pacific (Mumbai) ap-south-1

Bucket name Info

loginpages3project

Bucket name must be unique within the global namespace and follow the bucket naming rules. See rules for bucket naming

Copy settings from existing bucket - *optional*

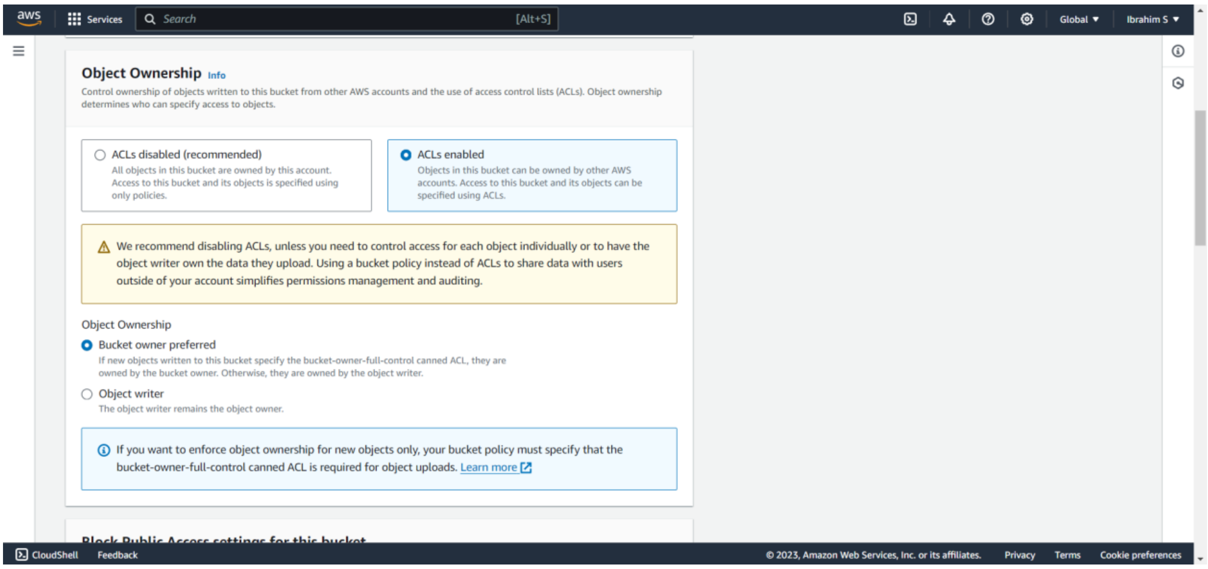
Only the bucket settings in the following configuration are copied.

Choose bucket

Format: s3://bucket/prefix

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.



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.

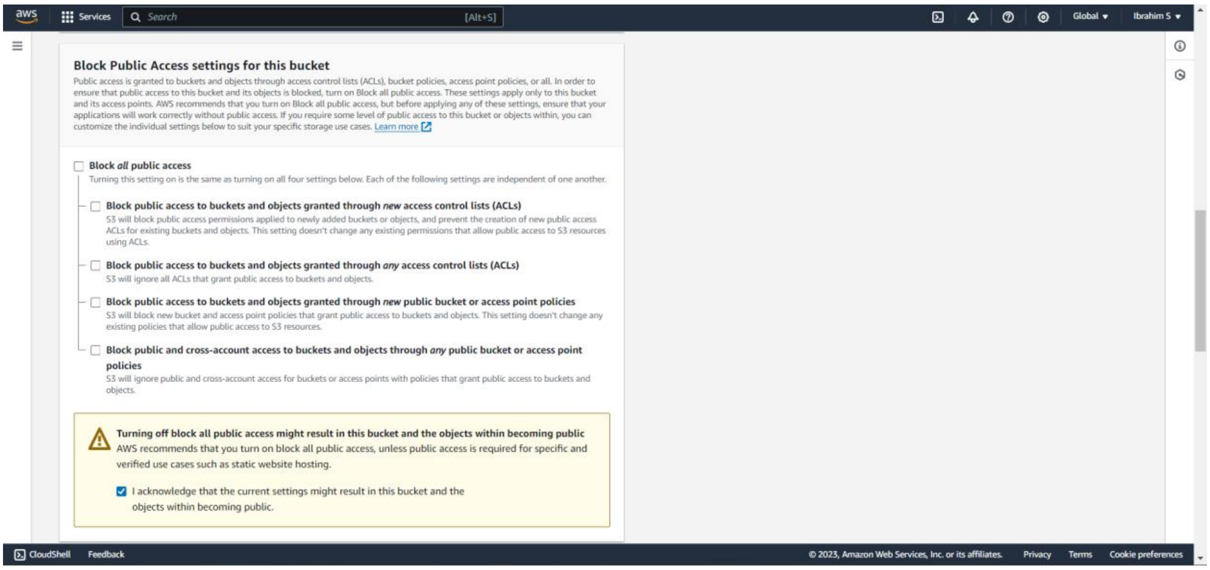
Object Ownership

● 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.

ⓘ 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

Block Public Access settings for this bucket



Block Public Access settings for this bucket

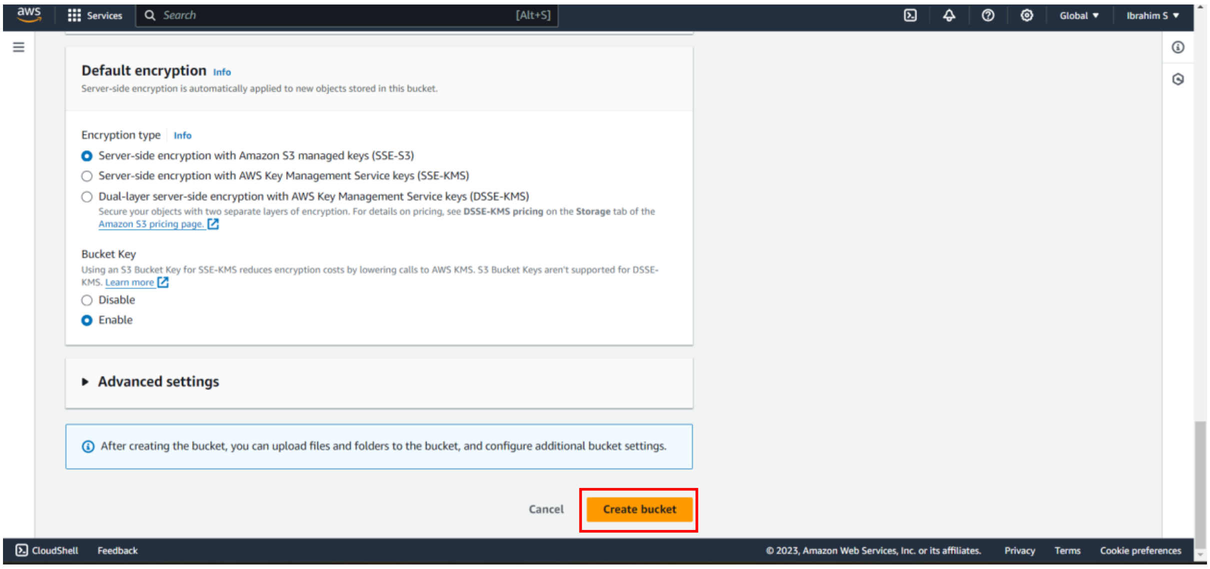
Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to this bucket and its objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access 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.



Default encryption Info

Server-side encryption is automatically applied to new objects stored in this bucket.

Encryption type Info

● 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)
Secure your objects with two separate layers of encryption. For details on pricing, see **DSSE-KMS pricing** on the **Storage** tab of the Amazon S3 pricing page.

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

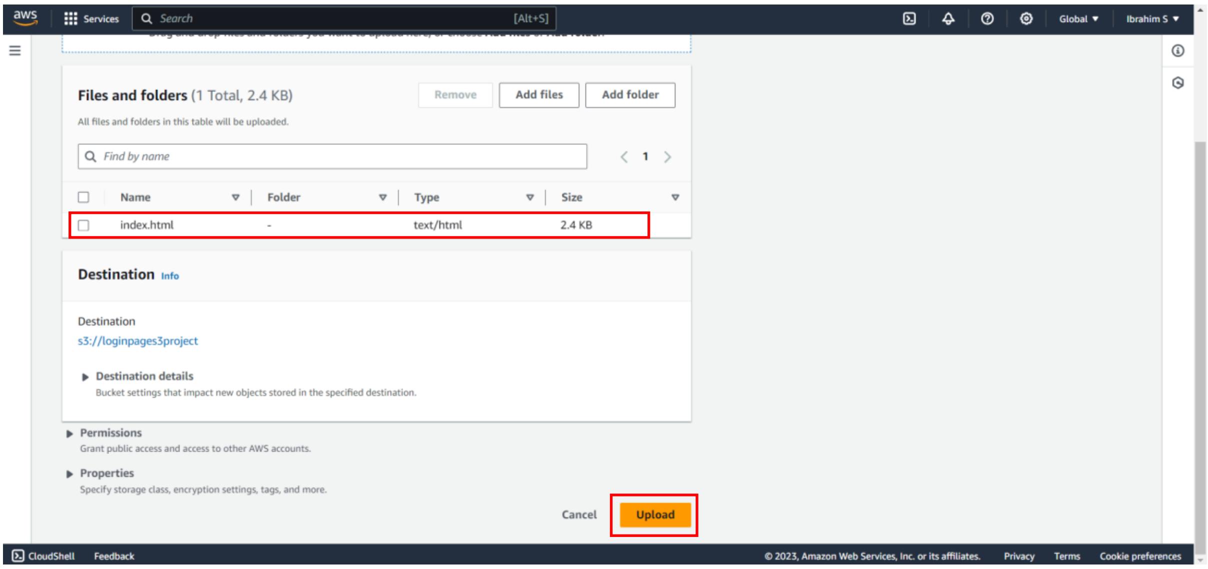
▸ **Advanced settings**

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

Cancel | **Create bucket**

3. Upload HTML and Image Files

1. Select your bucket.
2. Click on the "Upload" button.
3. Upload your HTML file (e.g., `index.html`) and any image files.
4. Ensure that your images are in the same folder as your HTML file.



Files and folders (1 Total, 2.4 KB)

Remove | Add files | Add folder

All files and folders in this table will be uploaded.

Find by name

□	Name	Folder	Type	Size
□	index.html	-	text/html	2.4 KB

Destination Info

Destination
s3://loginpages3project

▸ **Destination details**
Bucket settings that impact new objects stored in the specified destination.

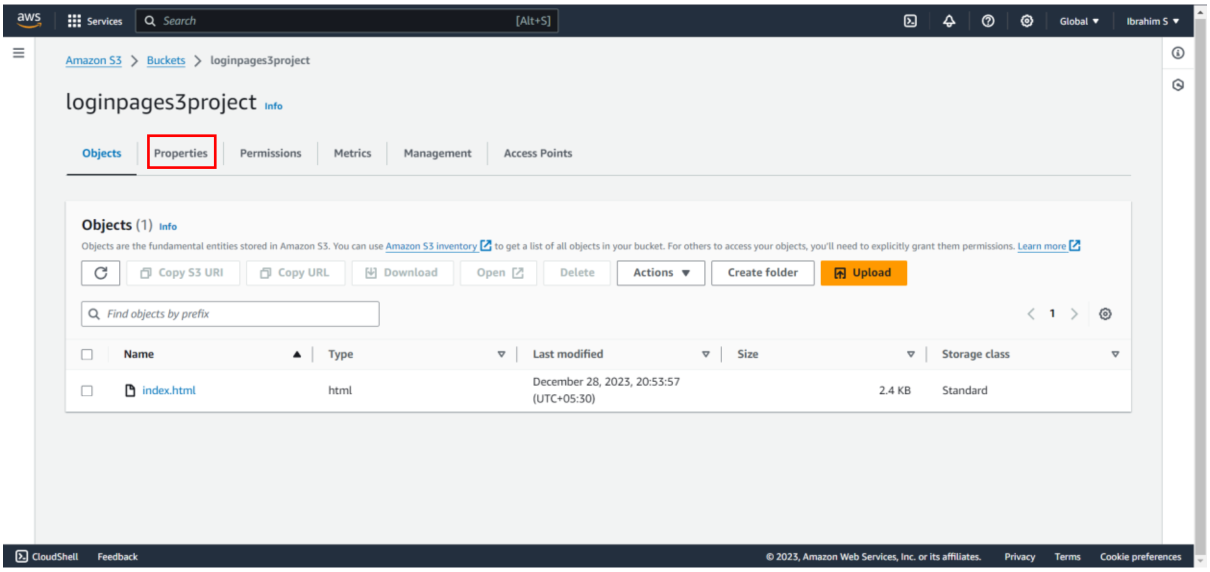
▸ **Permissions**
Grant public access and access to other AWS accounts.

▸ **Properties**
Specify storage class, encryption settings, tags, and more.

Cancel | **Upload**

4. Configure Bucket for Website Hosting

1. Go to the "Properties" tab.
2. Click on "Static website hosting."
3. Choose "Use this bucket to host a website."
4. Set the index document to your HTML file (e.g., `index.html`).
5. Optionally, set an error document.
6. Click "Save changes."



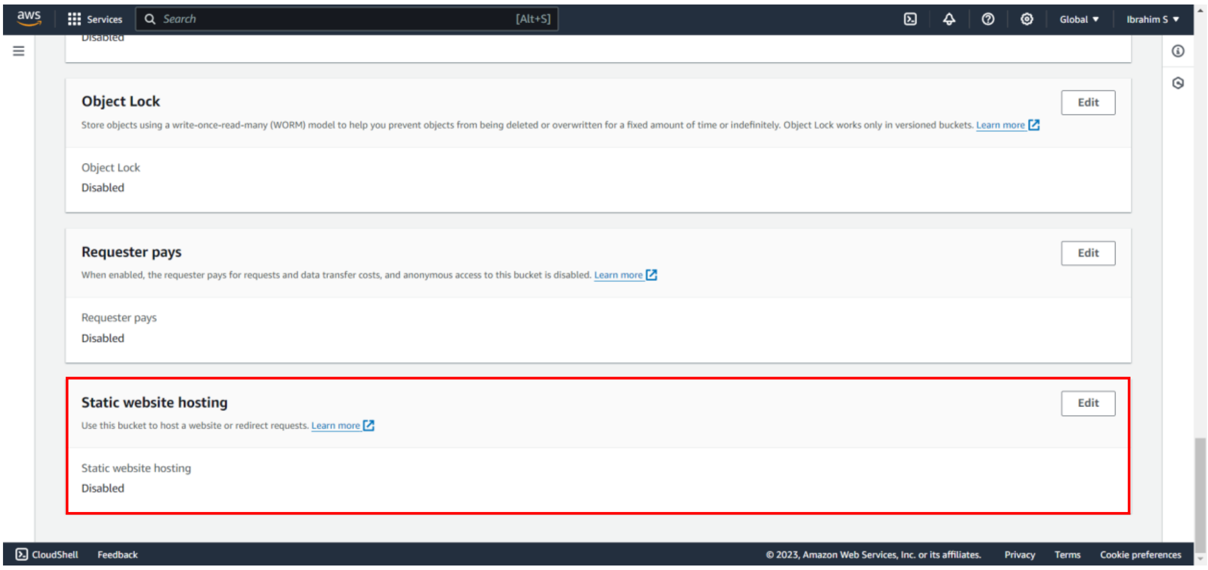
Amazon S3 > Buckets > loginpages3project

loginpages3project Info

Objects (1) Info

Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

□	Name	Type	Last modified	Size	Storage class
□	index.html	html	December 28, 2023, 20:53:57 (UTC+05:30)	2.4 KB	Standard



Object Lock

Store objects using a write-once-read-many (WORM) model to help you prevent objects from being deleted or overwritten for a fixed amount of time or indefinitely. Object Lock works only in versioned buckets. Learn more

Object Lock
Disabled

Requester pays

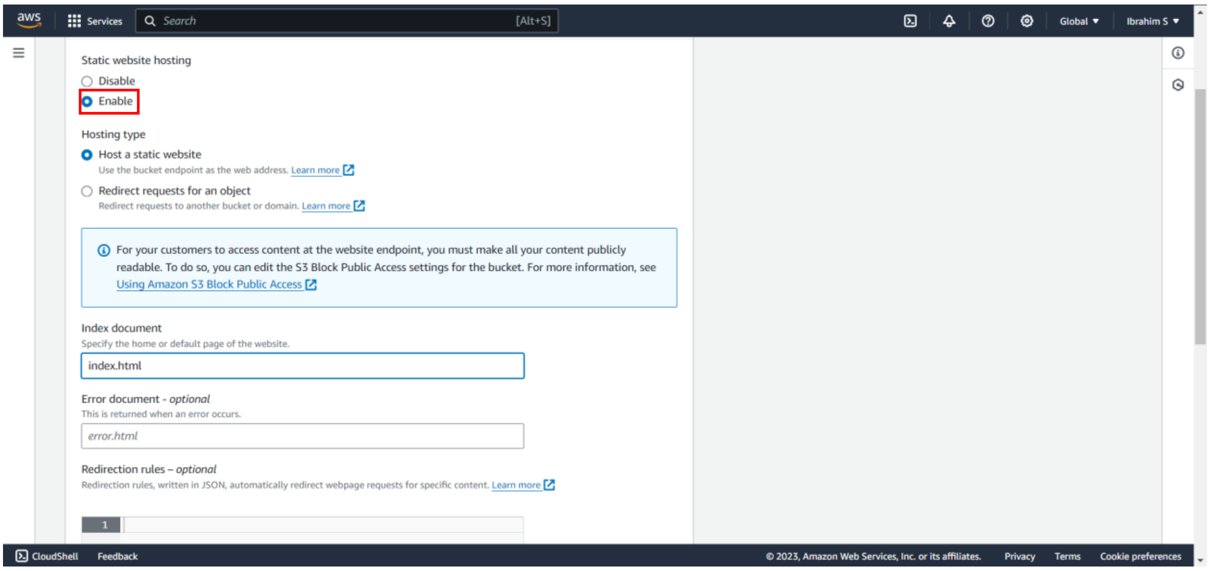
When enabled, the requester pays for requests and data transfer costs, and anonymous access to this bucket is disabled. Learn more

Requester pays
Disabled

Static website hosting

Use this bucket to host a website or redirect requests. Learn more

Static website hosting
Disabled



Static website hosting
○ Disable
● Enable

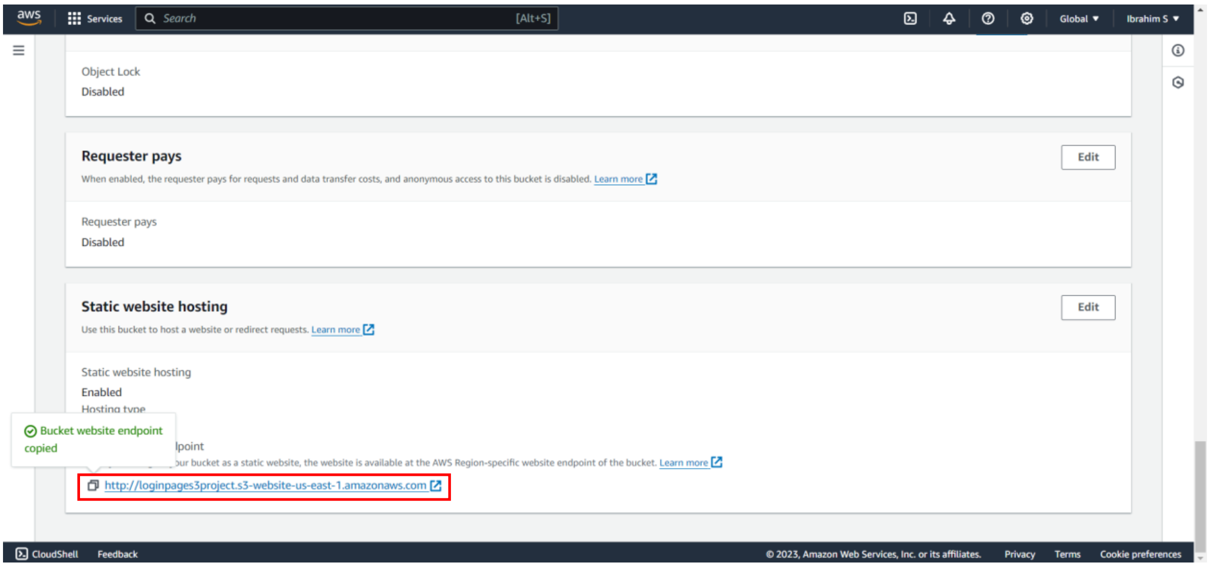
Hosting type
● Host a static website
Use the bucket endpoint as the web address. Learn more
○ Redirect requests for an object
Redirect requests to another bucket or domain. Learn more

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

Redirection rules – *optional*
Redirection rules, written in JSON, automatically redirect webpage requests for specific content. Learn more



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

Static website hosting
Enabled
Hosting type

Bucket website endpoint copied

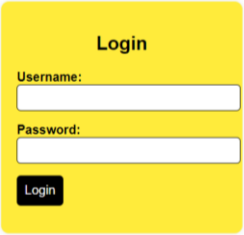
lpoint

our bucket as a static website, the website is available at the AWS Region-specific website endpoint of the bucket. Learn more

http://loginpages3project.s3-website-us-east-1.amazonaws.com

5. Access Your Website

1. in the "Static website hosting" section, note the "Endpoint" URL.
   - It will look like: http://loginpages3project.s3-website-us-east 1.amazonaws.com/?username=asd&password=asd
2. Open this URL in a web browser to view your static website.


Login
Username:
Password:
Login