

PROJECT-2

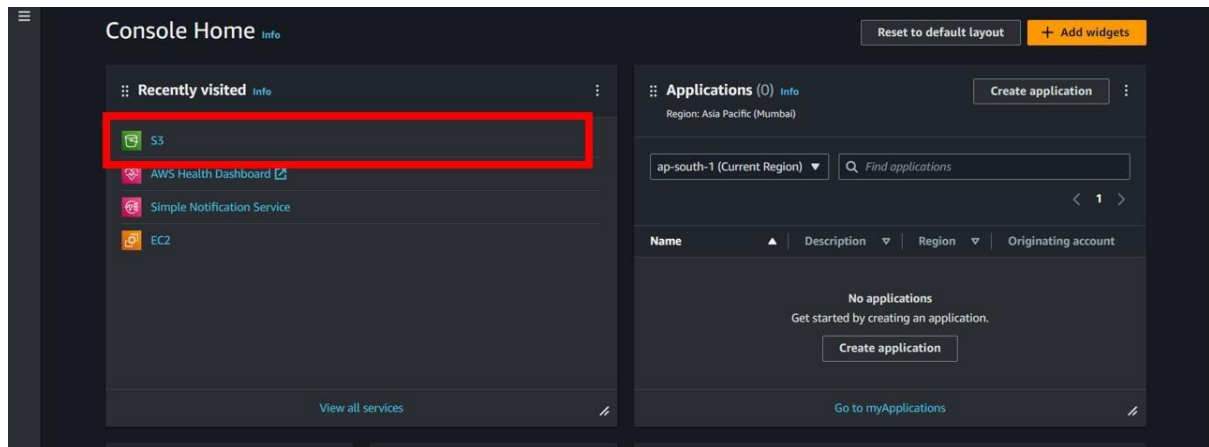
Deploy a Static Website on AWS

- In this project, we will learn how to create a static website and deploy it using AWS services.
- A static website is a site that consists of HTML, CSS, and JavaScript files, and it doesn't require server-side processing or a database.

Sign in to AWS Management Console

1. Click on the Open Console button, and you will get redirected to AWS Console in a new browser tab.
2. On the AWS sign-in page,
 - Leave the Account ID as default. Never edit/remove the 12-digit Account ID present in the AWS Console. otherwise, you cannot proceed with the lab.
 - Now copy your User Name and Password in the Lab Console to the IAM Username and Password in AWS Console and click on the Sign in button.

3. Once Signed in to the AWS Management Console, Make the default AWS Region as US East (N. Virginia) us-east-1.

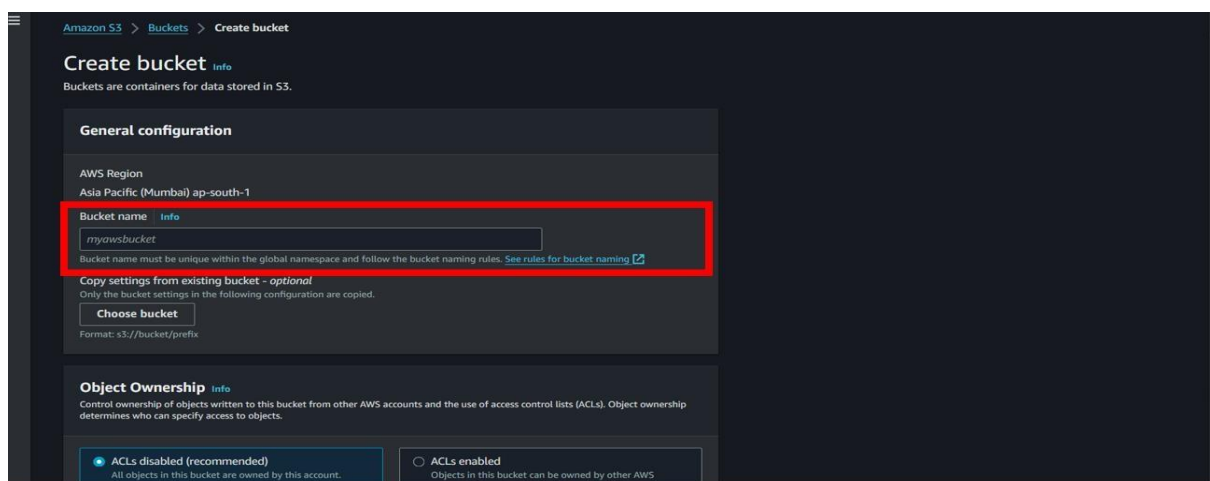
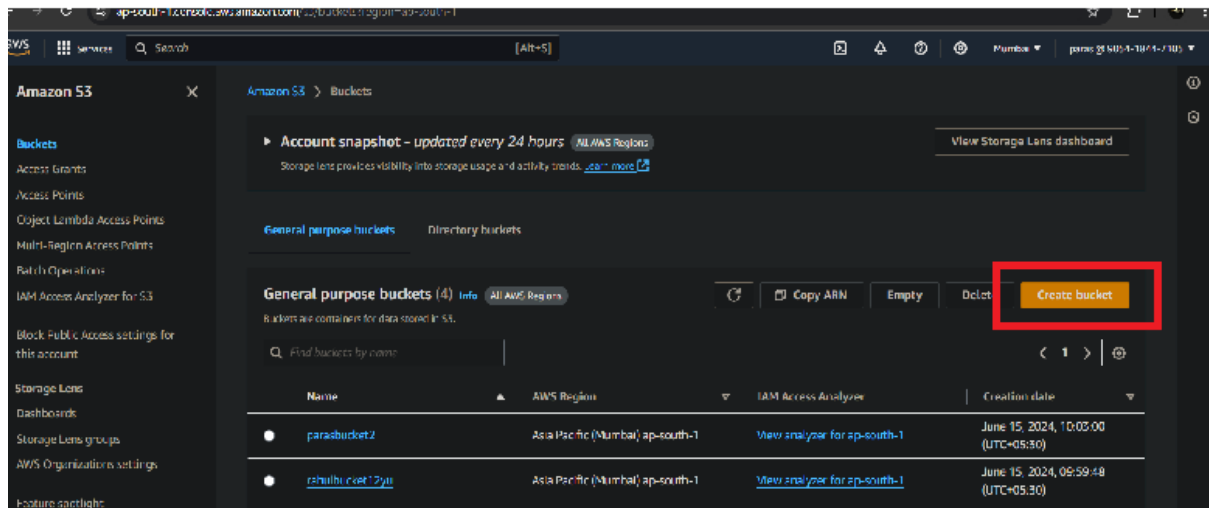


S3 BUCKET:

Amazon S3 (Simple Storage Service) is a cloud-based storage service provided by AWS, it allows users to store and retrieve data over the Internet. It provides a scalable, reliable, and highly available storage infrastructure for a variety of data types, including object storage, files, documents, and multimedia content.

1. Creating an S3 Bucket for Static Website Hosting

On your AWS console, search for S3, and on the S3 dashboard "Create bucket".



NOTE:

- 1.S3 Bucket names are globally unique, choose a name that is available. Maybe you can enter your name and create one.
- 2.In my case it is *"Parasbucket2"*
- 3.AWS Region: Select US East (N. Virginia) us-east-1
- 4.Select ACLs enabled option

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.

☒ **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.

Object Ownership
Bucket owner enforced

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

then uncheck the "block all public access" and check the acknowledgment, then leave the rest of the configuration as default.

☐ **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.

NOTE: Keep everything default and click on Create Bucket button.

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

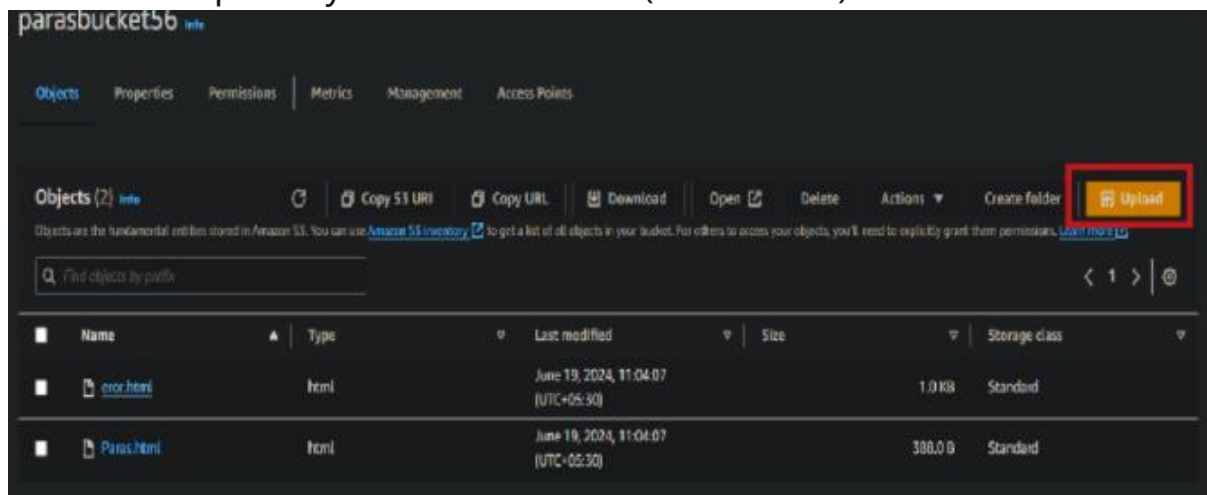
► Advanced settings

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

Cancel
Create bucket

2. Uploading Website Content to S3

Click on your S3 bucket, click on Upload, then click on " **Add files**",
Select and upload your website files (HTML files).



3. Configuring S3 Bucket Permissions for Website Access

Click on the permission tab in your S3 bucket, click on edit permission, and paste the this Json configuration:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AddPerm",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3::: parasbucket56/*"
    }
  ]
}
```

Replace the "*parasbucket56*" in the configuration with your bucket name and click on save

4. Enabling Static Website Hosting on S3

Click on the properties tab in your S3 bucket, scroll down , and click on "static hosting", *by default it is disabled*, click on enable static hosting, follow the configuration in the snapshot, and save.

The screenshot displays the AWS S3 console interface. The top navigation bar shows the bucket name 'parasbucket56' and the 'Properties' tab is selected and highlighted with a red box. Below the navigation bar, the 'Objects (2)' section shows a list of objects: 'error.html' and 'Paras.html'. The 'Static website hosting' section is visible, showing that static website hosting is enabled. The 'Requester pays' section is also visible, showing it is disabled. The 'Edit' button for the 'Static website hosting' section is highlighted with a red box.

Name	Type	Last modified	Size	Storage class
error.html	html	June 19, 2024, 11:04:07 (UTC+05:30)	1.0 KB	Standard
Paras.html	html	June 19, 2024, 11:04:07 (UTC+05:30)	388.0 B	Standard

Static website hosting

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

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://rahuibucket12yu.s3-website-ap-south-1.amazonaws.com>

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](#)

Index document
Specify the home or default page of the website.

Static website hosting
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](#)

Static website hosting
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](#)

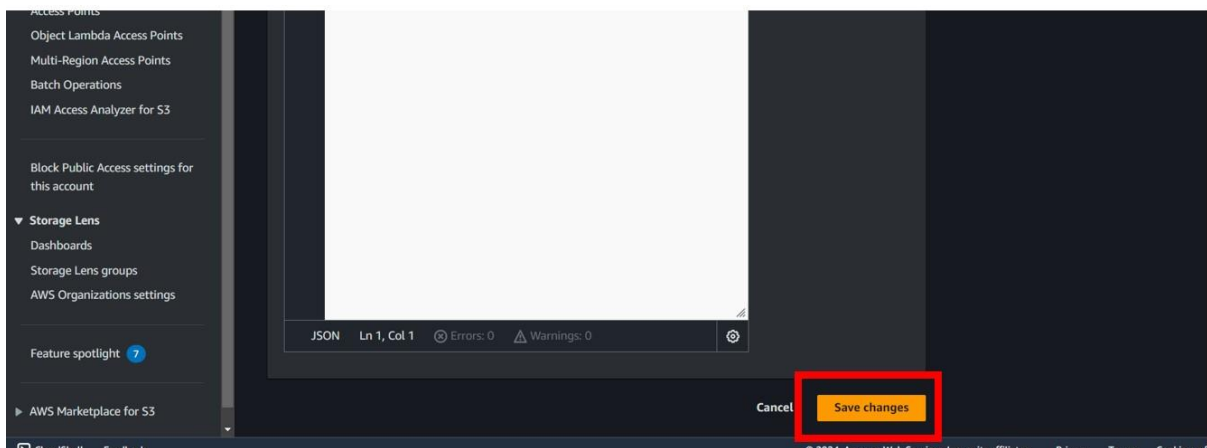
Index document
Specify the home or default page of the website.

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

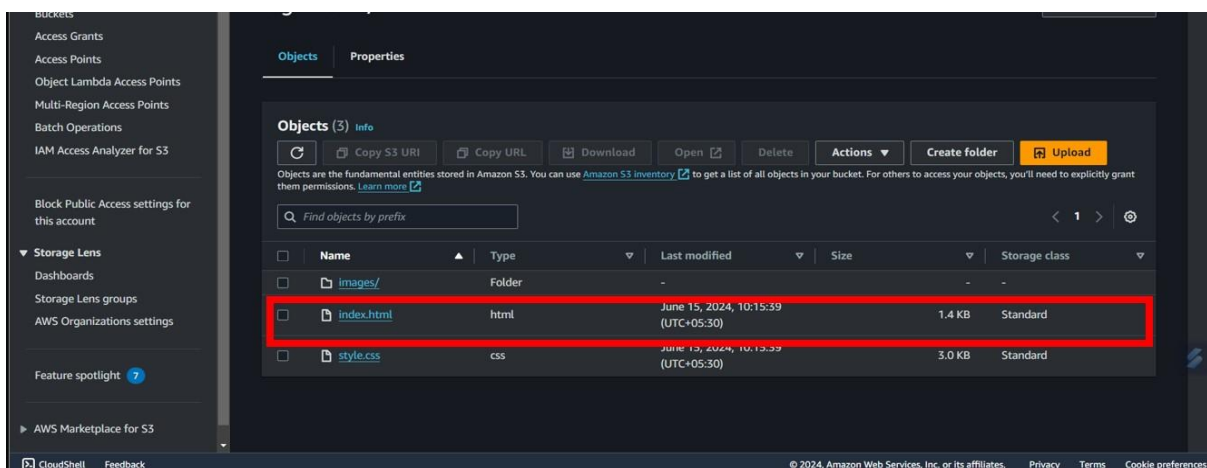
Redirection rules - optional
Redirection rules, written in JSON, automatically redirect webpage requests for specific content. [Learn more](#)

1

In INDEX DOCUMENT provide your html file name.
And the error document is not necessary it is optional, then scroll down and click on SAVE CHANGES .



Then inside your bucket locate your html file and open it.



Then open your html file and copy its object url , and search it in new tab.

