Project – Create and Host a Static Website on S3

Scenario

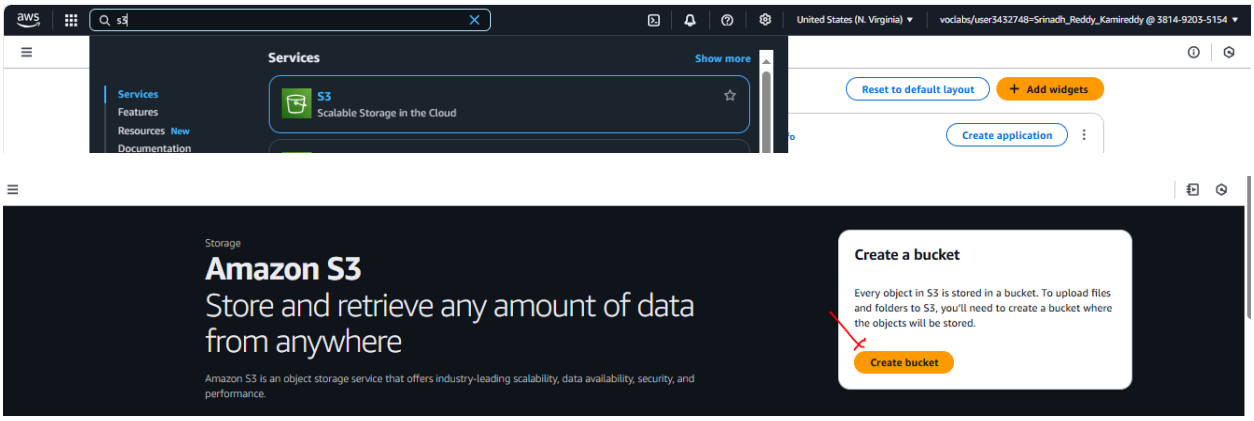
In this project, how to create and host a static website on Amazon S3. You'll create an S3 bucket, configure it for static website hosting, upload website content, and access the website using the S3-generated URL.

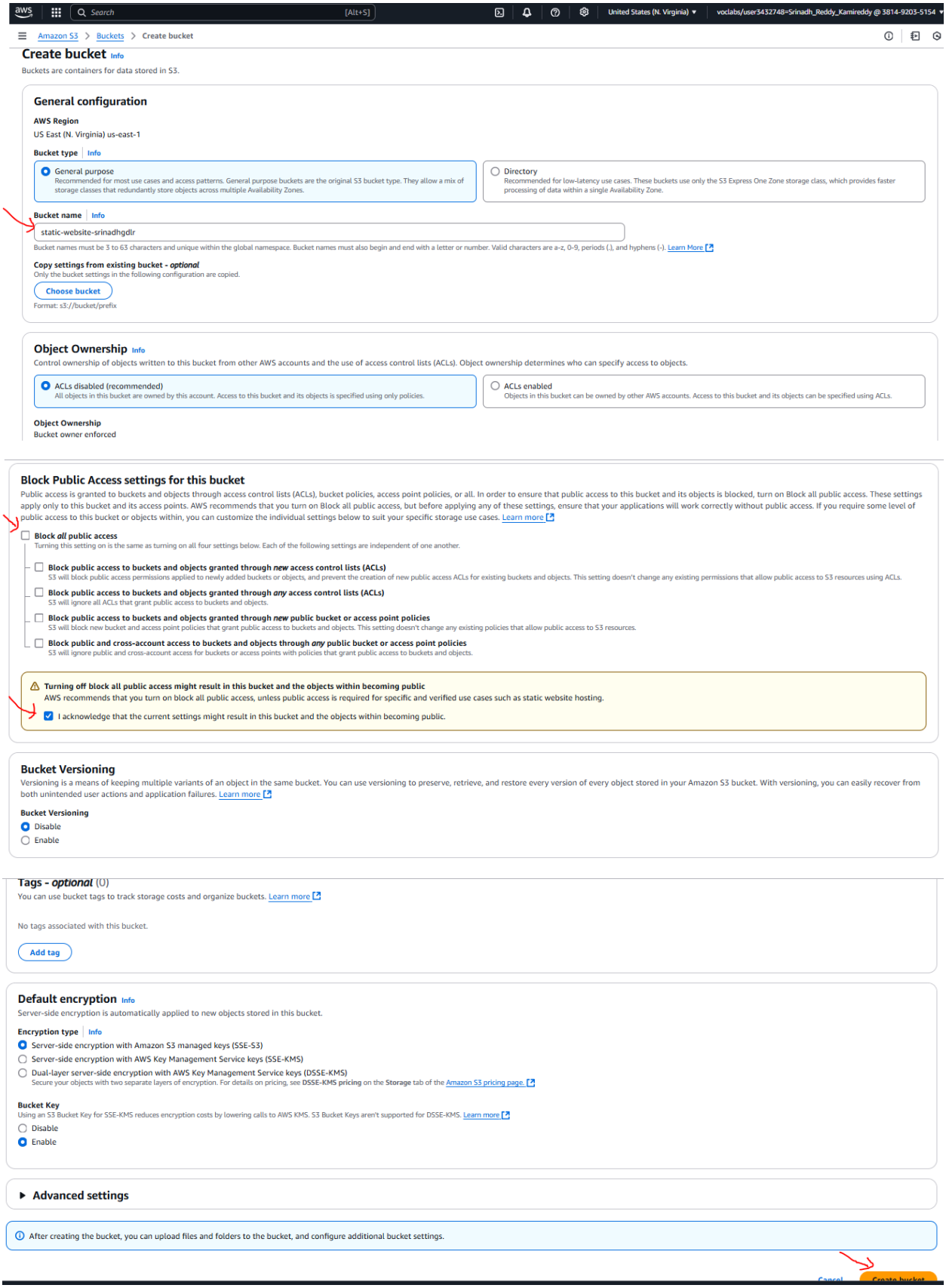
Steps:

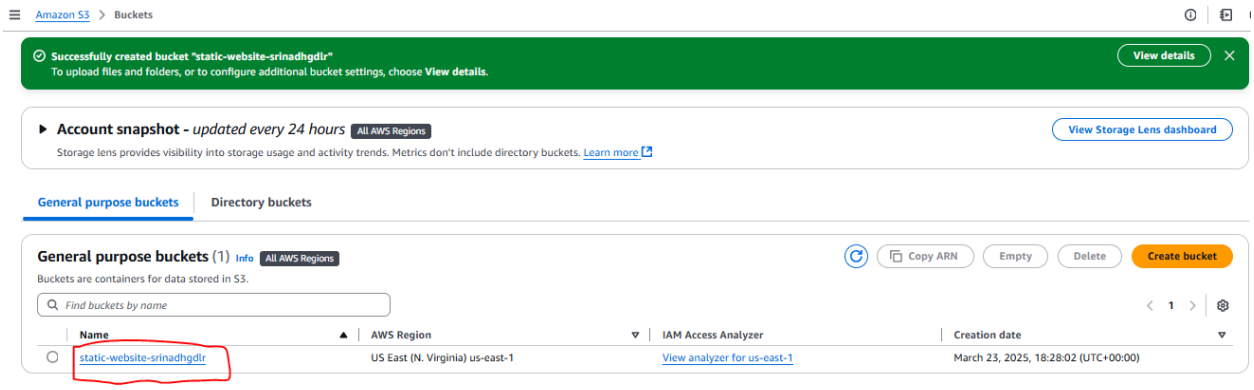
1. Create an S3 bucket static-website-srinadhgdlr in region us-east-1.
2. Set up the S3 bucket for static website hosting with appropriate bucket properties and permission policies.
3. Upload content from the GitHub repository https://github.com/srinadhgdlr/static-website to the bucket root so that index.html shows up on the website root.
4. Access the website over a browser using the S3-generated link.
5. Clean up the resources created.

Task 1 - Create an S3 Bucket

Open the AWS Management Console, Navigate to the S3 service.
Choose Create bucket
Select the region us-east-1
Enter a unique Bucket name: static-website-srinadhgdlr
Disable Block all public access.
Check "I acknowledge that the current settings might result in this bucket and the objects within becoming public."
Choose Create bucket

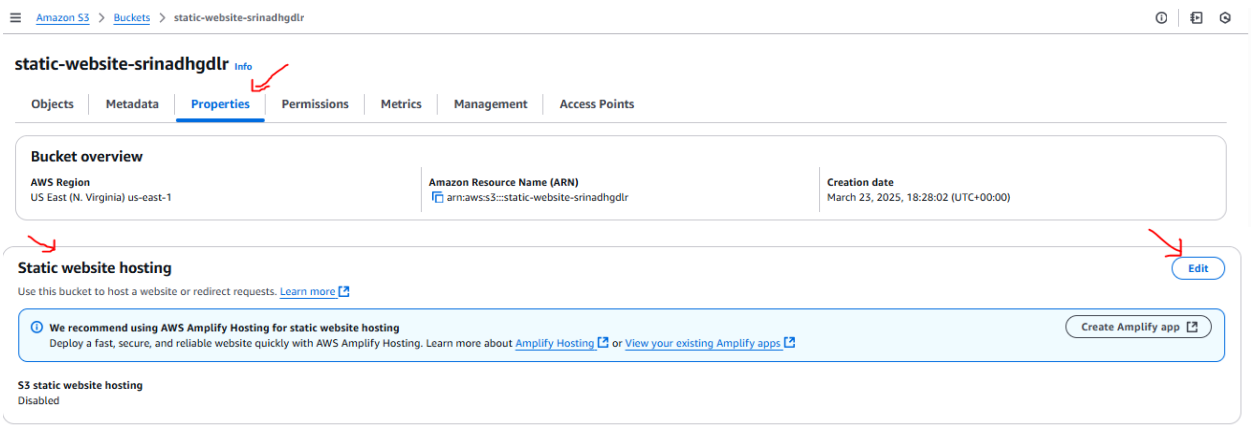


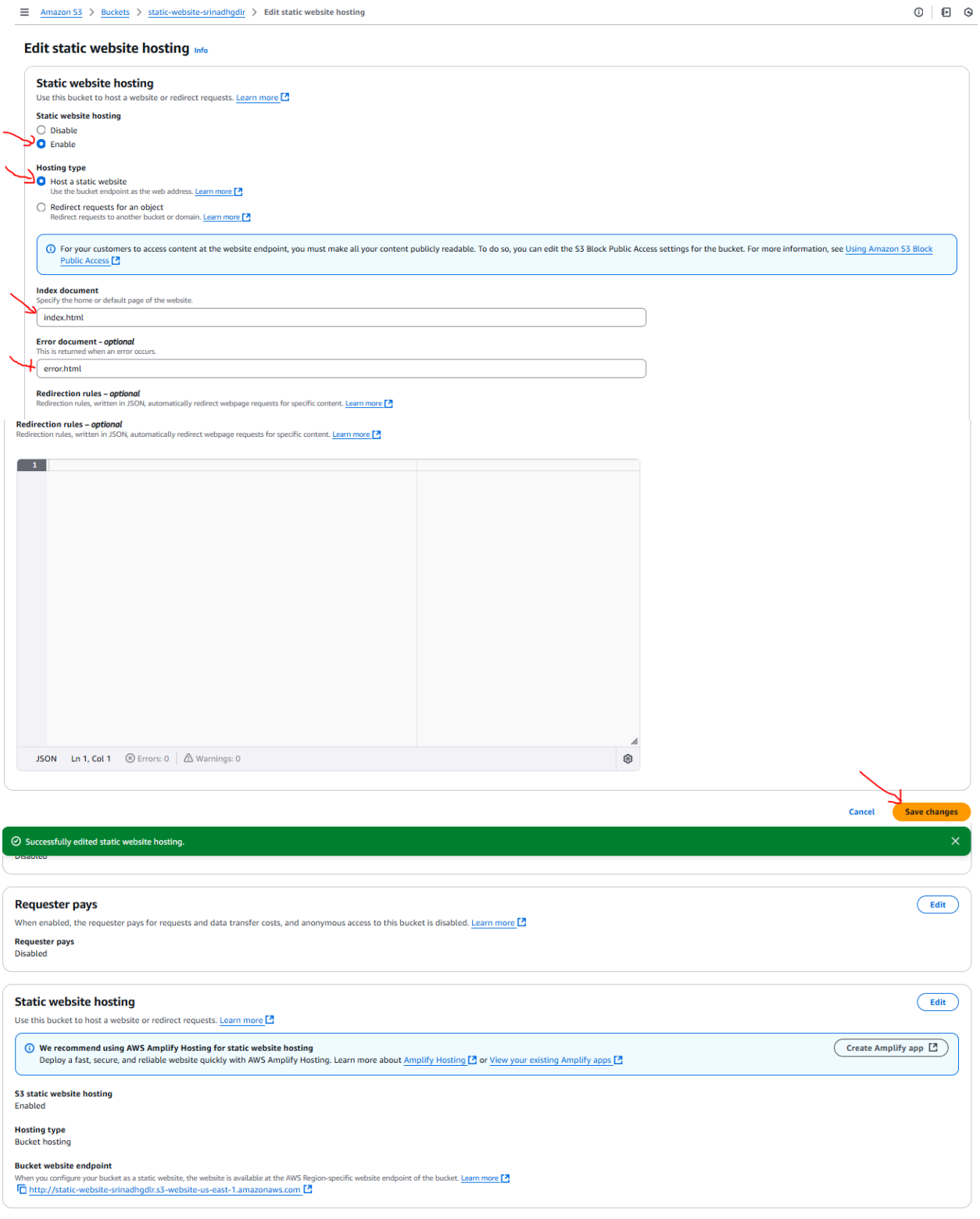

Search [Alt+S]
United States (N. Virginia)
voclabs/user3432748=Srinadh_Reddy_Kamireddy @ 3814-9203-5154
Amazon S3 > Buckets > Create bucket
Create bucket Info
Buckets are containers for data stored in S3.
General configuration
AWS Region
US East (N. Virginia) us-east-1
Bucket type Info
General purpose
Recommended for most use cases and access patterns. General purpose buckets are the original S3 bucket type. They allow a mix of storage classes that redundantly store objects across multiple Availability Zones.
Directory
Recommended for low-latency use cases. These buckets use only the S3 Express One Zone storage class, which provides faster processing of data within a single Availability Zone.
Bucket name Info
static-website-srinadhgdlr
Bucket names must be 3 to 63 characters and unique within the global namespace. Bucket names must also begin and end with a letter or number. Valid characters are a-z, 0-9, periods (.), and hyphens (-). Learn More
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.
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 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.
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 - optional (0)
You can use bucket tags to track storage costs and organize buckets. Learn more
No tags associated with this bucket.
Add tag
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



Task 2 - Set Up Static Website Hosting

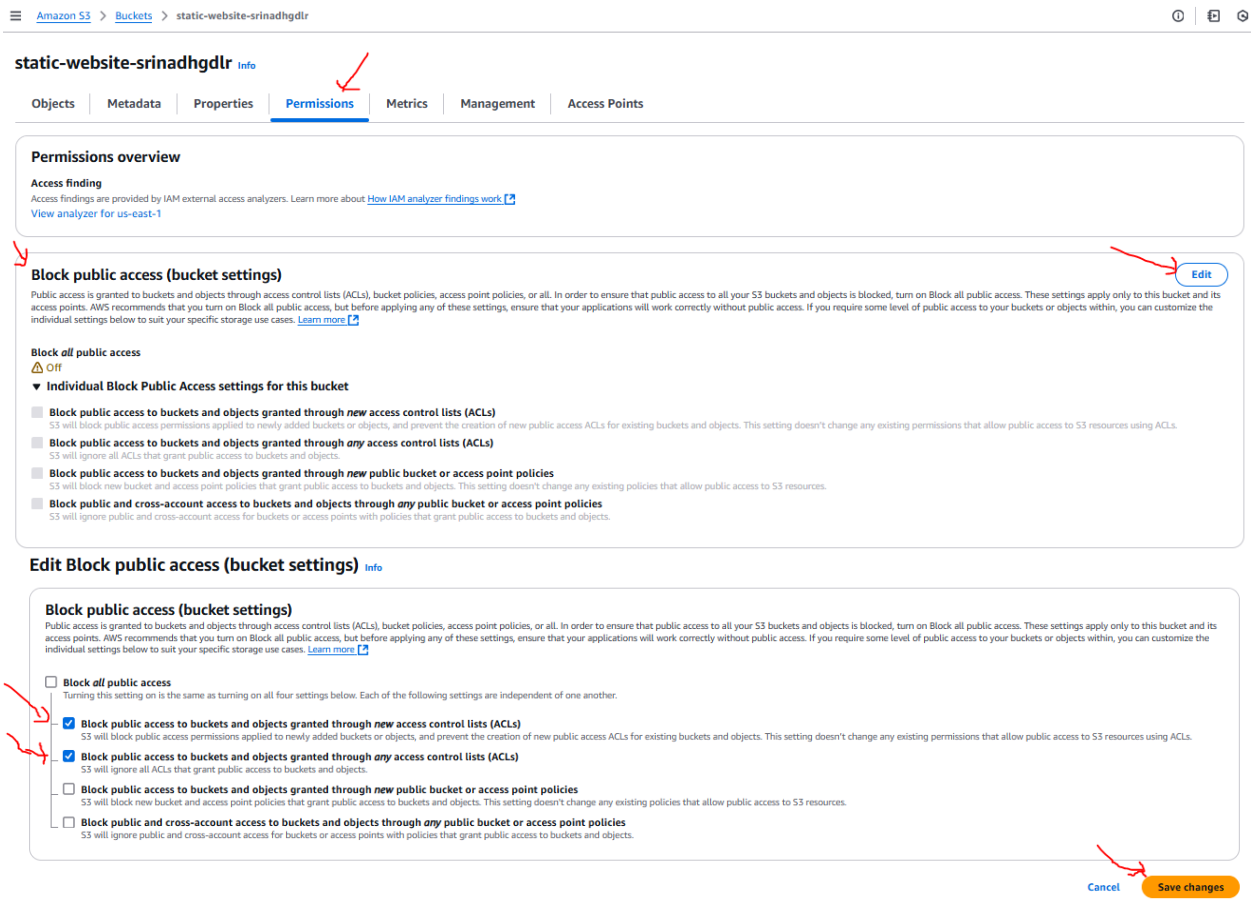
Navigate to the S3 Bucket name static-website-srinadhgdlr and click on Bucket name
Go to the Properties tab.
Scroll down to the Static website hosting section.
Choose Edit.
Select Enable.
In the Index document box, enter index.html.
Choose Save changes.




Amazon S3 > Buckets > static-website-srinadhgdlr > Edit static website hosting
Edit static website hosting Info
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
Redirection rules – optional
Redirection rules, written in JSON, automatically redirect webpage requests for specific content. Learn more
Redirection rules – optional
Redirection rules, written in JSON, automatically redirect webpage requests for specific content. Learn more
1
JSON Ln 1, Col 1 Errors: 0 Warnings: 0
Cancel
Save changes
Successfully edited static website hosting.
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
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://static-website-srinadhgdlr.s3-website-us-east-1.amazonaws.com

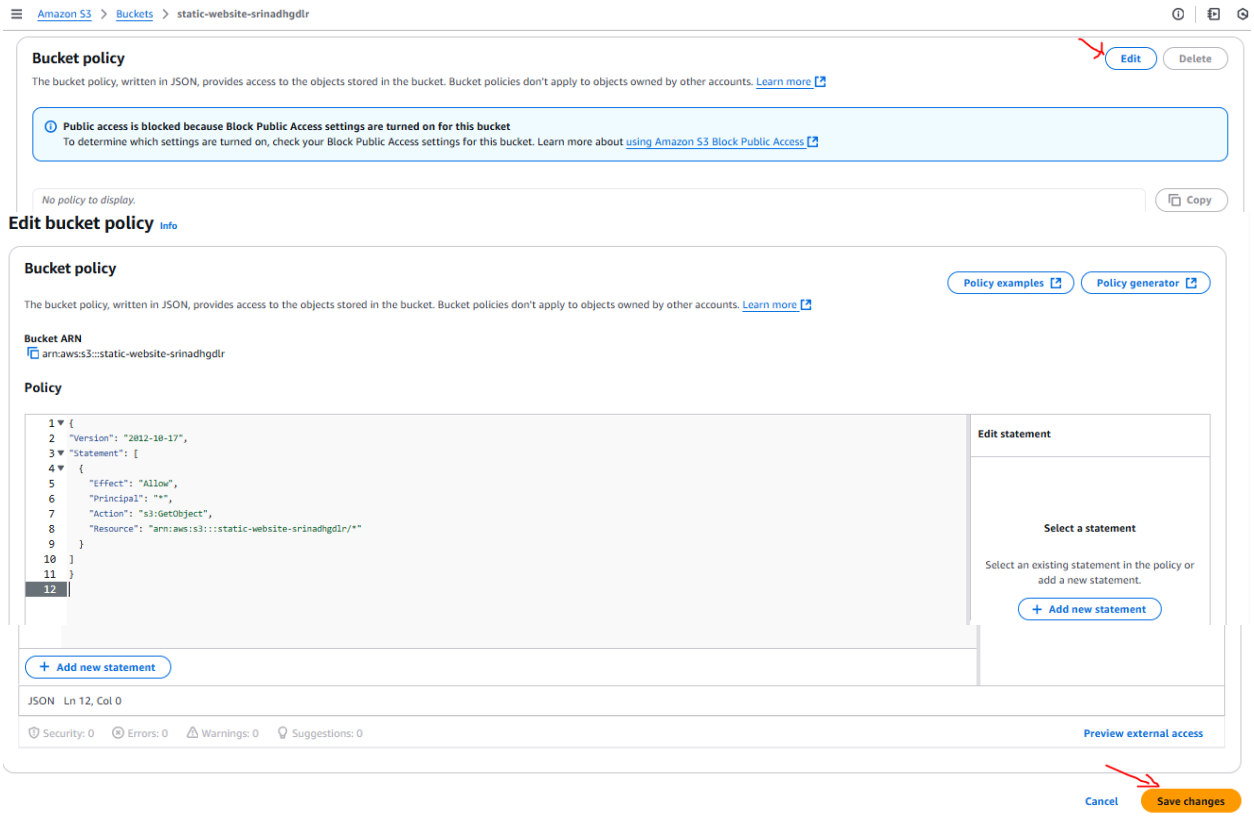
Task 3 - Set Bucket Permissions

Navigate to the Permissions tab.
Under Block public access section, click Edit.
Deselect Block all public access, then select the first two options (ACLs).
Save changes
To confirm the settings, enter *confirm* in the field.



Scroll down to Bucket policy and choose Edit.
Add the following bucket policy to allow public access to the bucket contents.

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



Choose Save changes.

Task 4 - Upload Website Content

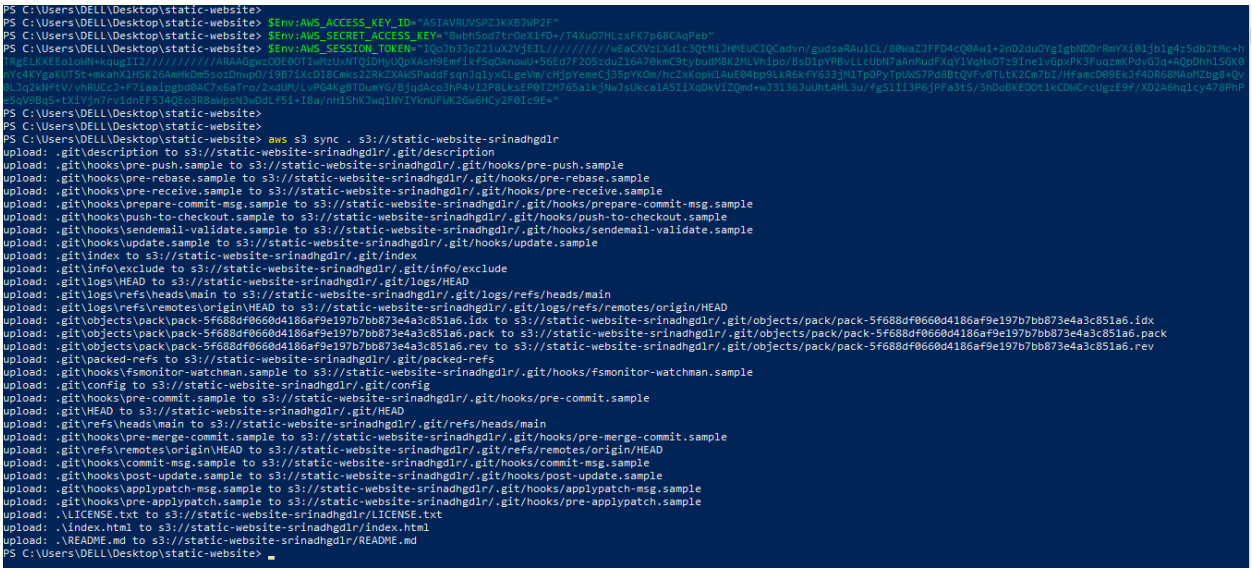
Clone the GitHub Repository Locally:
Open terminal or command prompt. Navigate to directory where you want to save the website project.
Clone the repository using the following command:
git clone https://github.com/srinadhgdlr/static-website.git
Navigate to the cloned repository directory:
cd static-website

```
C:\Users\DELL\Desktop>
C:\Users\DELL\Desktop>git clone https://github.com/srinadhgdlr/static-website.git
Cloning into 'static-website'...
remote: Enumerating objects: 5, done.
remote: Counting objects: 100% (5/5), done.
remote: Compressing objects: 100% (4/4), done.
remote: Total 5 (delta 0), reused 0 (delta 0), pack-reused 0 (from 0)
Receiving objects: 100% (5/5), 5.77 KiB | 1.92 MiB/s, done.

C:\Users\DELL\Desktop>
C:\Users\DELL\Desktop>dir
 Volume in drive C has no label.
 Volume Serial Number is 5699-DF80

 Directory of C:\Users\DELL\Desktop
```

```
C:\Users\DELL\Desktop>
C:\Users\DELL\Desktop>cd static-website

C:\Users\DELL\Desktop\static-website>dir
 Volume in drive C has no label.
 Volume Serial Number is 5699-DF80

 Directory of C:\Users\DELL\Desktop\static-website

23/03/2025  19:09    <DIR>          .
23/03/2025  19:09    <DIR>          ..
23/03/2025  19:09             3,427 index.html
23/03/2025  19:09            11,558 LICENSE.txt
23/03/2025  19:09                41 README.md
               3 File(s)         15,026 bytes
               2 Dir(s)  150,102,220,800 bytes free

C:\Users\DELL\Desktop\static-website>
```

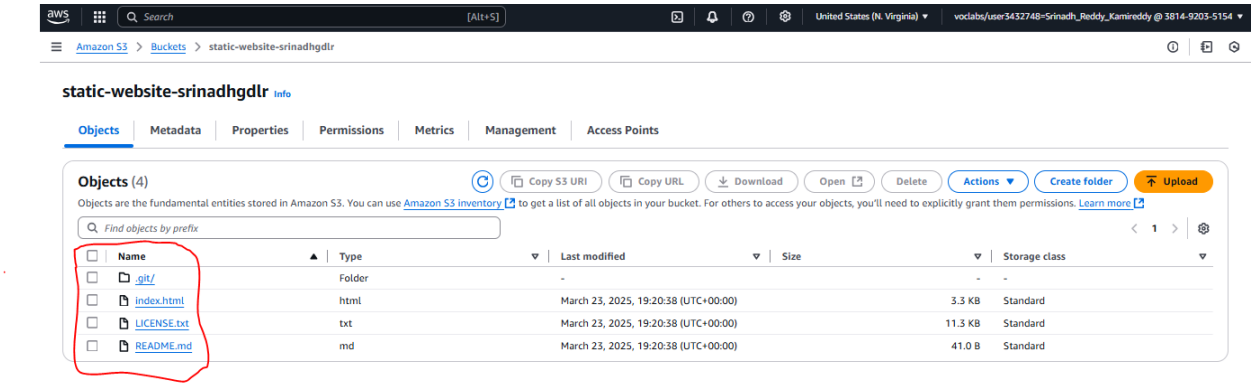
Upload Content to S3 Using AWS CLI:

Ensure that the AWS CLI is installed and configured with the necessary permissions.
Configure the profile settings for your profile or use default one.
Run the following command in to sync the content from the cloned repository to your S3 bucket:
aws s3 sync . s3://static-website-srinadhgdlr



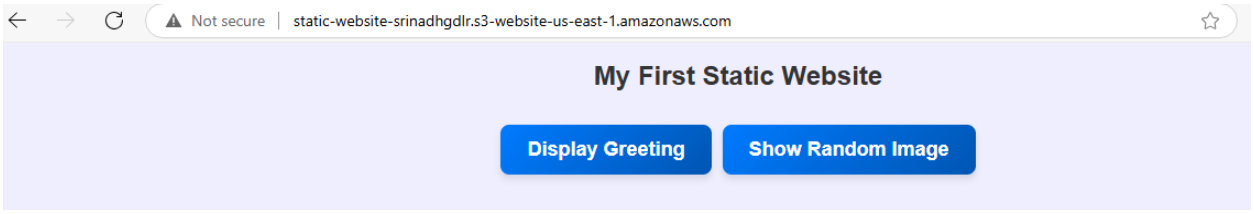
Verify the Upload:

Navigate to the S3 bucket static-website-srinadhgdlr in the AWS Management Console.
Ensure that the content from the GitHub repository has been uploaded successfully to the bucket root.
With this, you will have uploaded the website content to your S3 bucket using AWS CLI commands.



Task 5 - Access the Website

Navigate to the Properties tab of the S3 bucket static-website-srinadhgdlr
Scroll down to the Static website hosting section.
Copy the Bucket website endpoint URL http://static-website-srinadhgdlr.s3-website-us-east-1.amazonaws.com
Open a web browser and paste the copied URL to access the website.
Verify that the website content is displayed correctly.



Task 6 - Clean Up

Navigate to the S3 bucket static-website-srinadhgdlr
Select all the objects in the bucket and choose Delete.
Confirm the deletion.
Delete the S3 bucket static-website-srinadhgdlr