HOSTING A STATIC WEBSITE USING AWS S3 (Simple Storage Service)

What is S3?

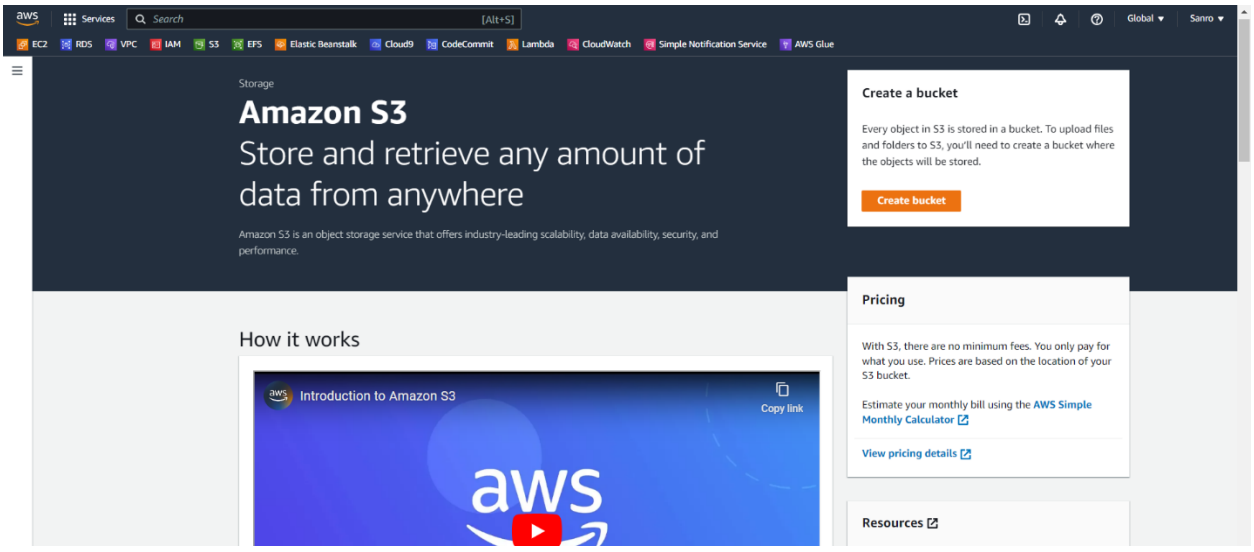
Amazon Simple Storage Service (Amazon S3) is an object storage service that offers industry-leading scalability, data availability, security, and performance. You can use Amazon S3 to store and retrieve any amount of data at any time, from anywhere.

Amazon S3 is a pioneer in cloud data storage and has uncountable benefits, the 5 most prominent ones are

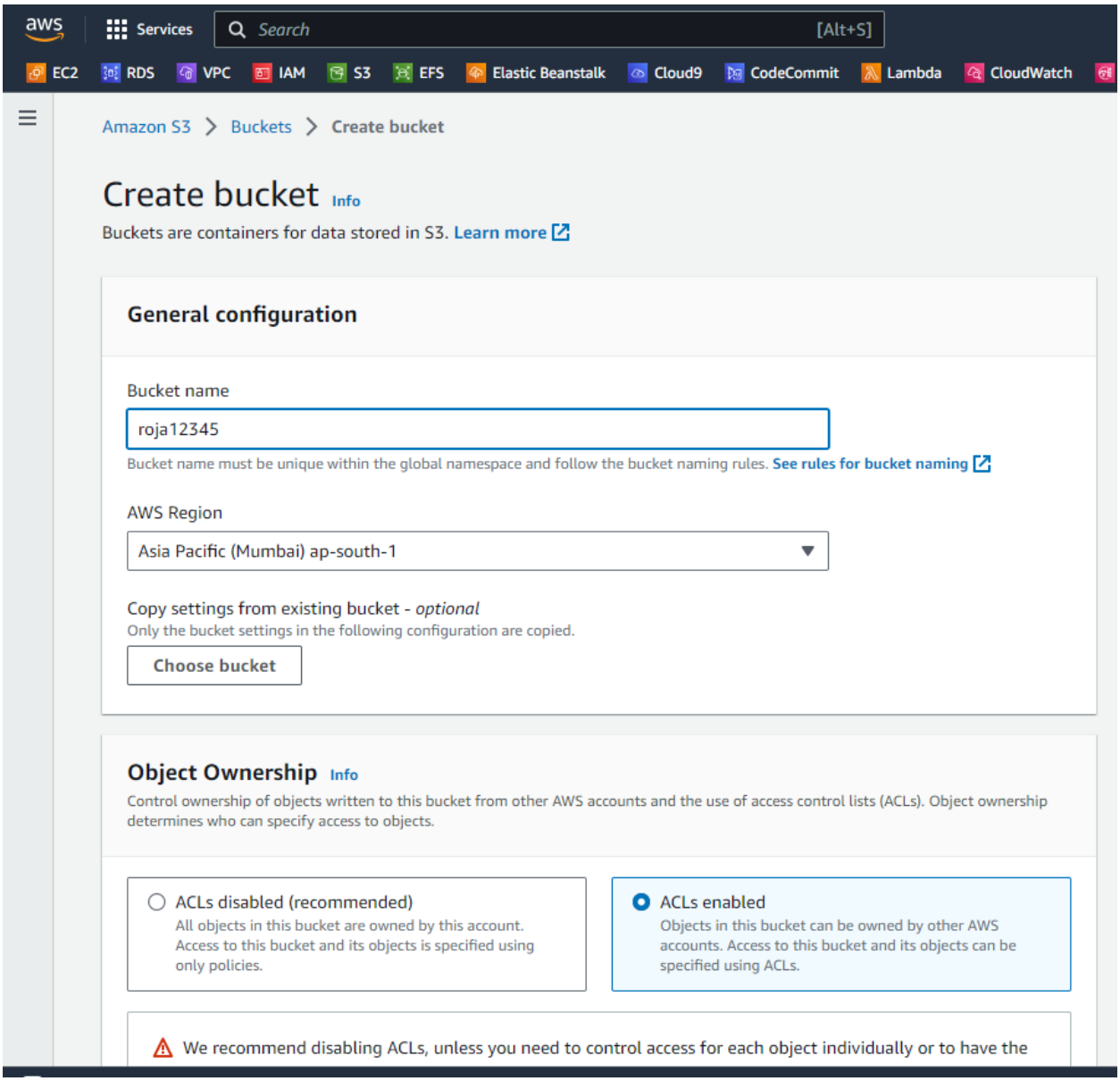
- Reliable Security
- All-time Availability
- Very Low Cost
- Ease if Migration
- The simplicity of Management

Step-by-Step method to store static websites in an S3 bucket.

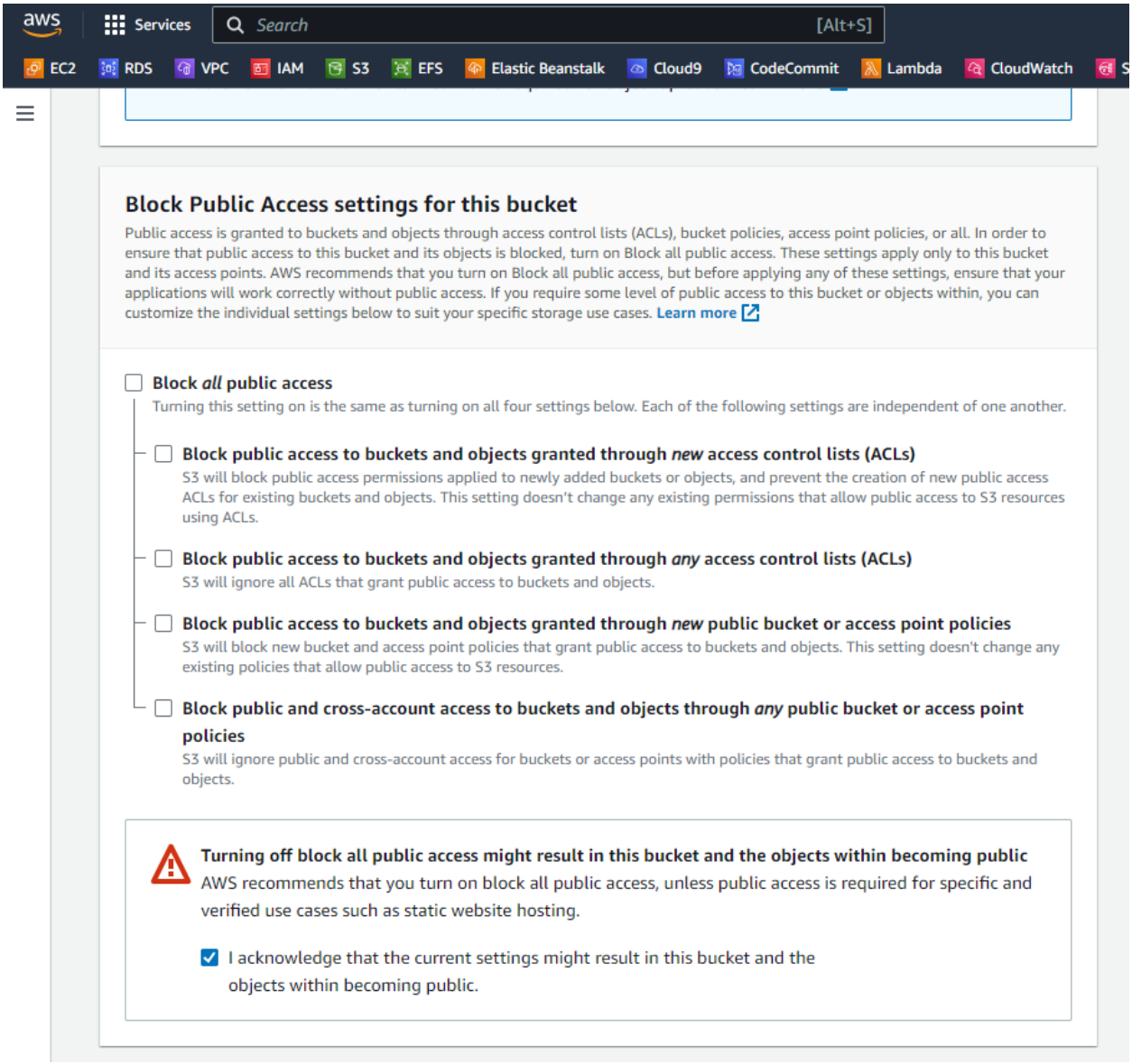
Step 1: Search for s3 service in AWS management console and click on create bucket

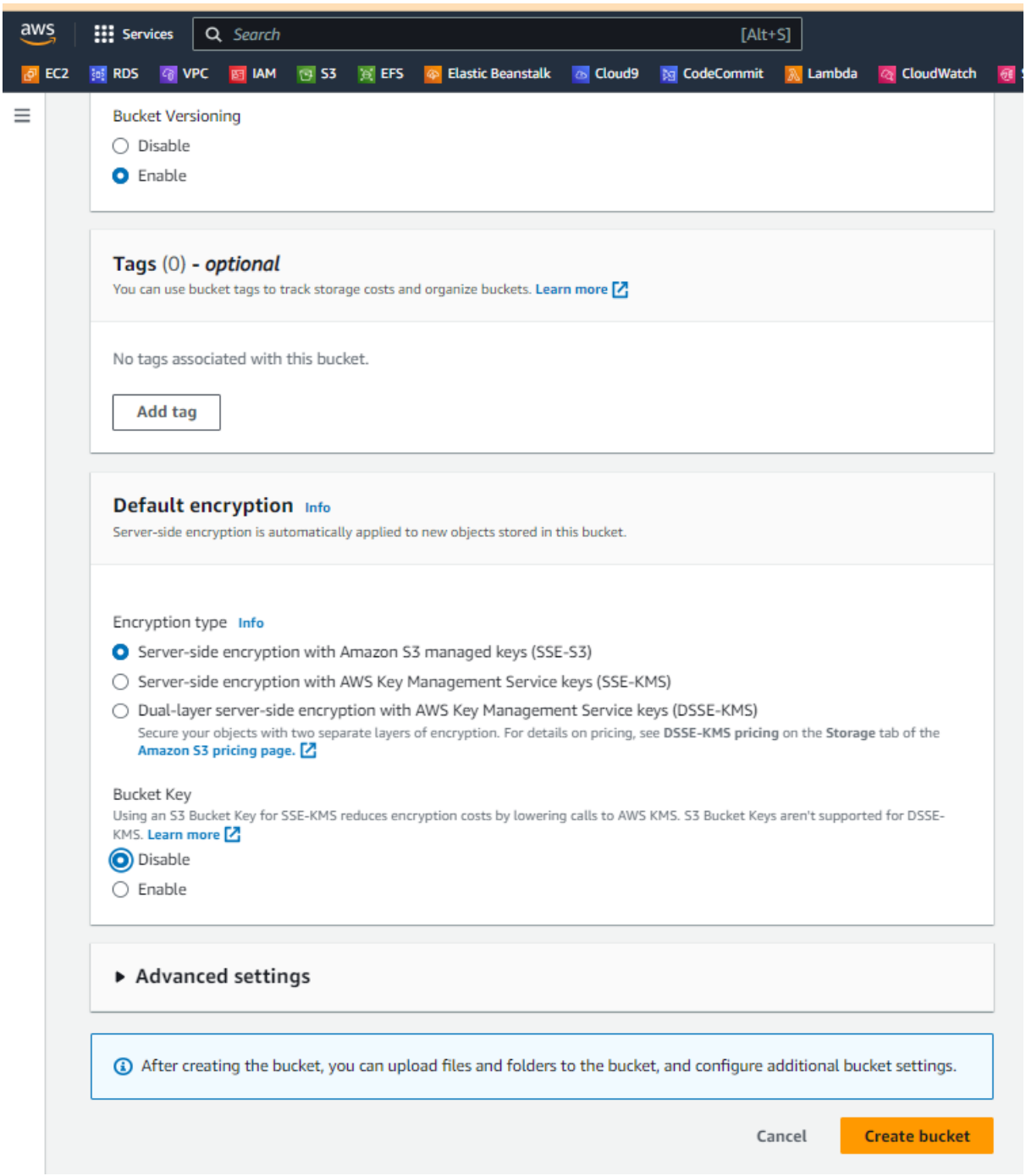


Step 2: Create bucket by providing the details as shown in below pictures

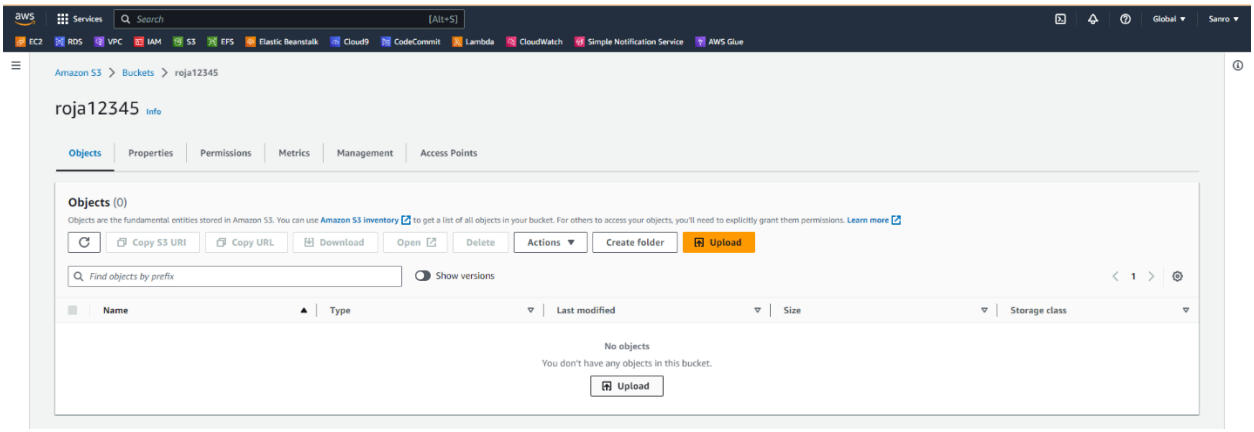


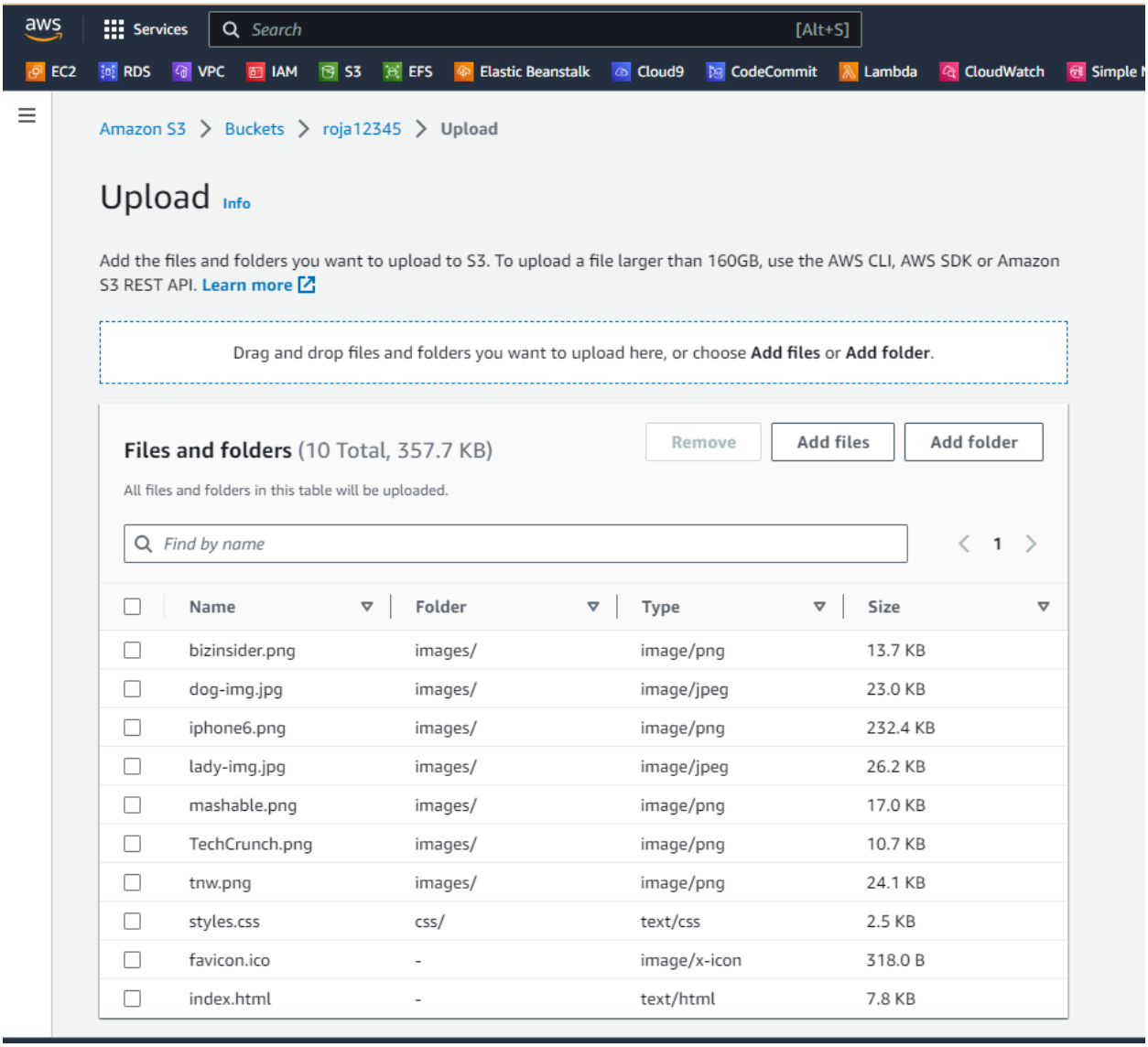
- Make sure to allow public access buy not clicking on the “block public Access settings” for this bucket
- Enable bucket versioning as it helps with tracking the changes in the bucket data and recovery of it when something happens to the data

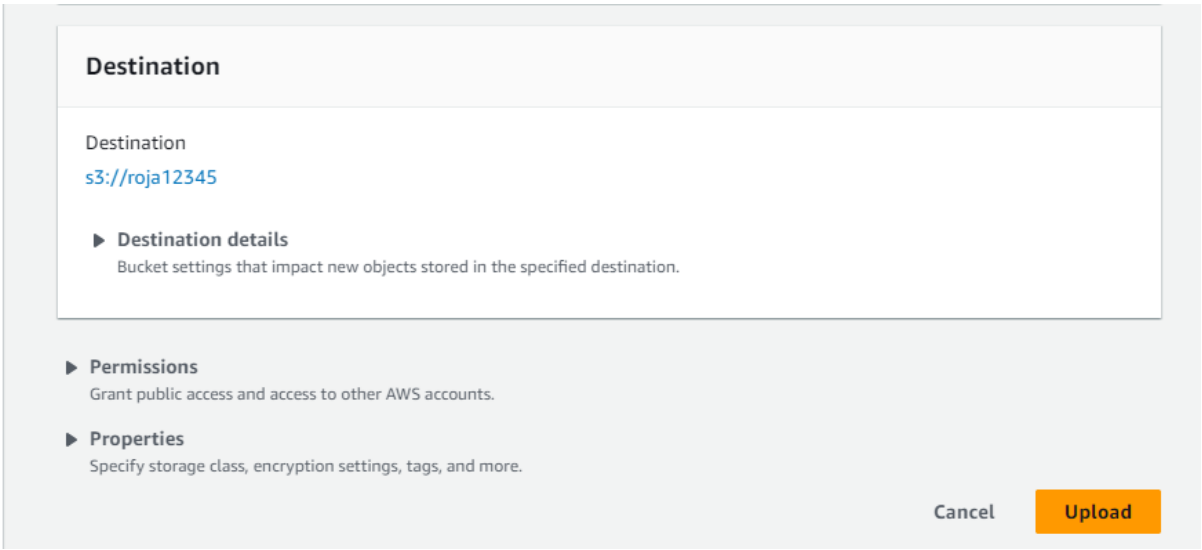

aws
Services
Search
[Alt+S]
EC2
RDS
VPC
IAM
S3
EFS
Elastic Beanstalk
Cloud9
CodeCommit
Lambda
CloudWatch
Block Public Access settings for this bucket
Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure 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.

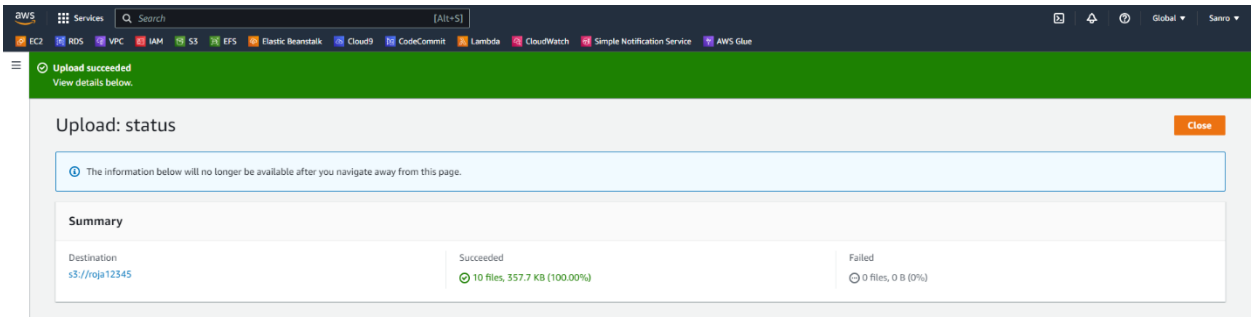


Step 3: Now upload the files of the website that you want to host in AWS into that bucket

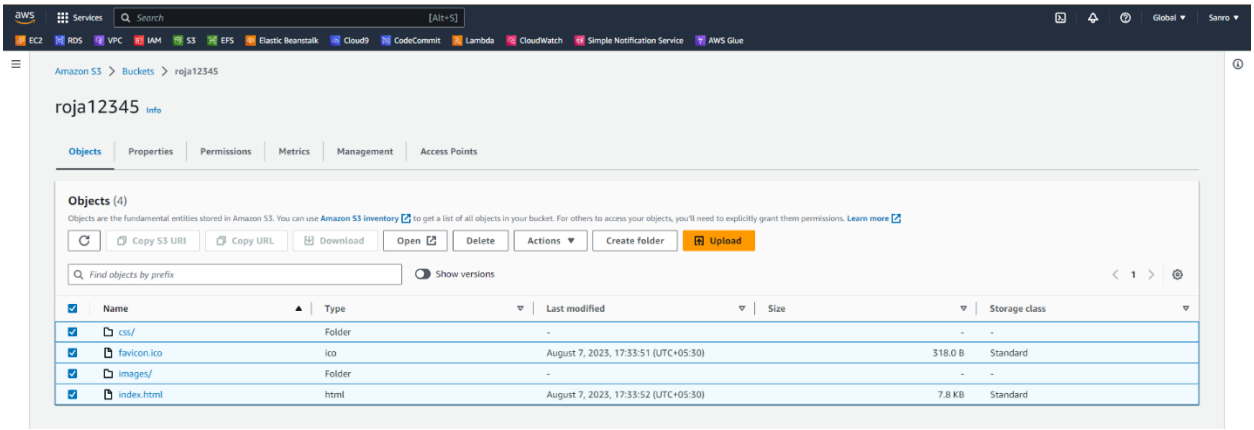

Amazon S3 > Buckets > roja12345
roja12345 Info
Objects
Properties
Permissions
Metrics
Management
Access Points
Objects (0)
Copy S3 URI
Copy URL
Download
Open
Delete
Actions
Create folder
Upload
Find objects by prefix
Show versions
Name
Type
Last modified
Size
Storage class
No objects
You don't have any objects in this bucket.
Upload

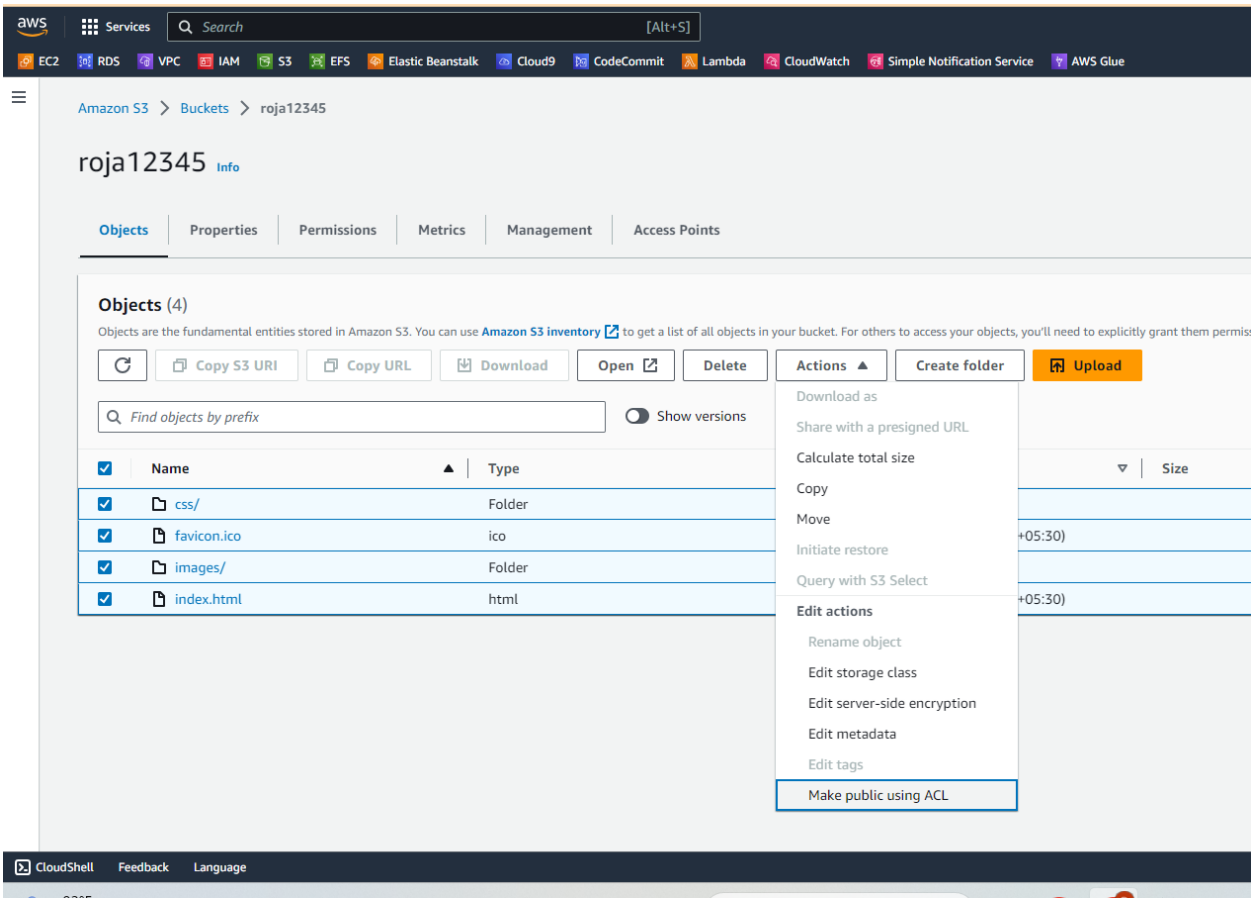

Services
Search
[Alt+S]
EC2
RDS
VPC
IAM
S3
EFS
Elastic Beanstalk
Cloud9
CodeCommit
Lambda
CloudWatch
Amazon S3 > Buckets > roja12345 > Upload
Upload Info
Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDK or Amazon S3 REST API. Learn more
Drag and drop files and folders you want to upload here, or choose Add files or Add folder.
Files and folders (10 Total, 357.7 KB)
Remove
Add files
Add folder
All files and folders in this table will be uploaded.
Find by name
1
Name
Folder
Type
Size
bizinsider.png images/ image/png 13.7 KB
dog-img.jpg images/ image/jpeg 23.0 KB
iphone6.png images/ image/png 232.4 KB
lady-img.jpg images/ image/jpeg 26.2 KB
mashable.png images/ image/png 17.0 KB
TechCrunch.png images/ image/png 10.7 KB
tnw.png images/ image/png 24.1 KB
styles.css css/ text/css 2.5 KB
favicon.ico - image/x-icon 318.0 B
index.html - text/html 7.8 KB

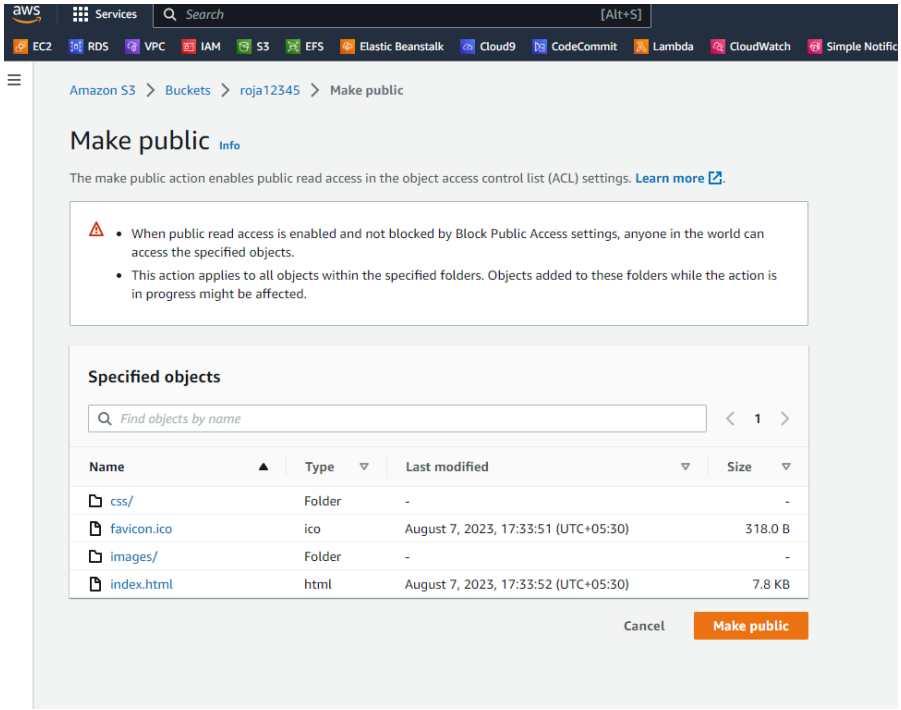




Step 4: After successfully uploading the files into the bucket now select all the files in the bucket and make public access using ACL (Access Control List)

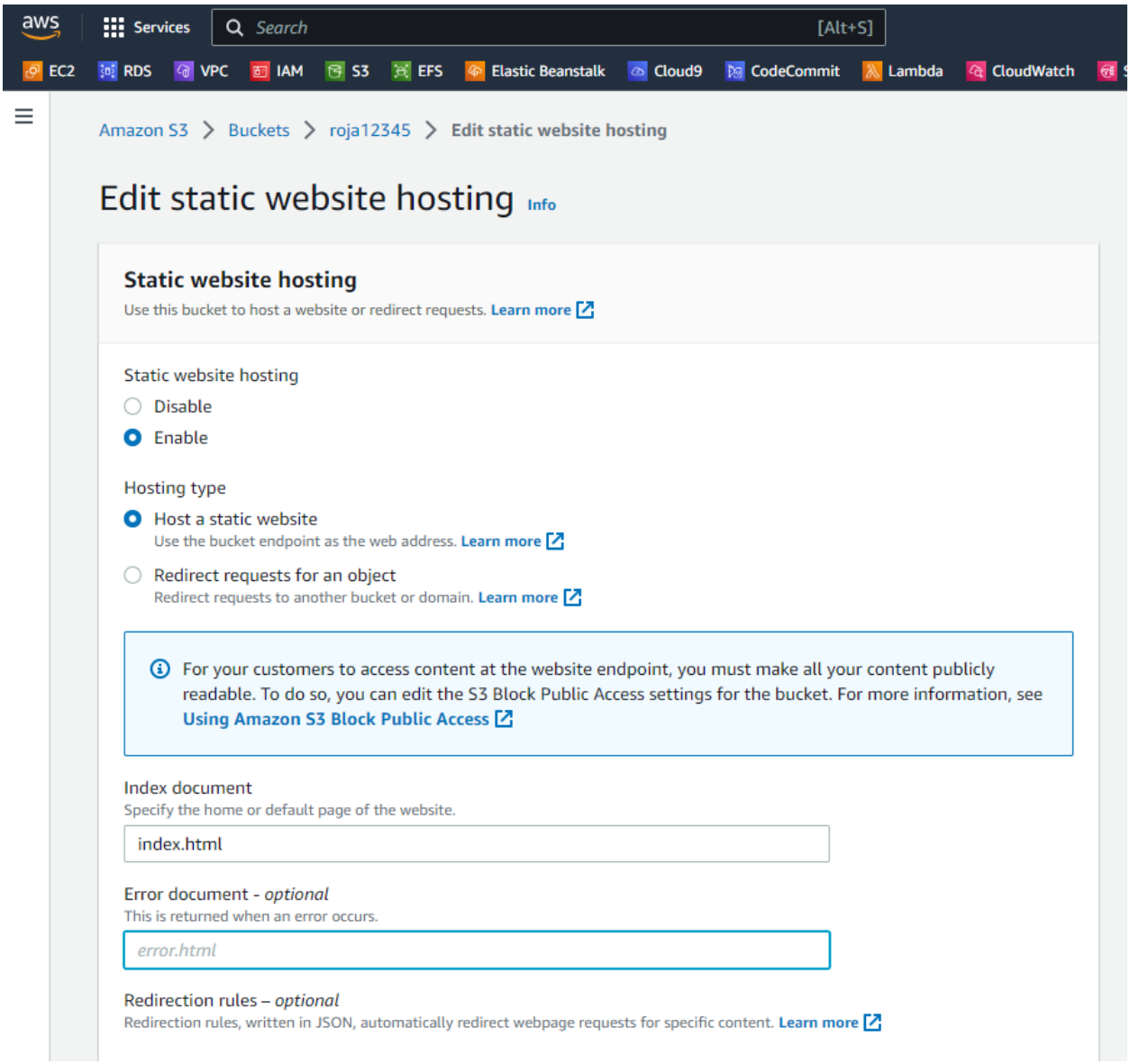



aws
Services
Search
[Alt+S]
EC2
RDS
VPC
IAM
S3
EFS
Elastic Beanstalk
Cloud9
CodeCommit
Lambda
CloudWatch
Simple Notification Service
AWS Glue
Amazon S3 > Buckets > roja12345
roja12345 Info
Objects
Properties
Permissions
Metrics
Management
Access Points
Objects (4)
Objects are the fundamental entities 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 permis
Copy S3 URI
Copy URL
Download
Open
Delete
Actions
Create folder
Upload
Find objects by prefix
Show versions
Name
Type
Size
css/
Folder
favicon.ico
ico
images/
Folder
index.html
html
+05:30)
Download as
Share with a presigned URL
Calculate total size
Copy
Move
Initiate restore
Query with S3 Select
Edit actions
Rename object
Edit storage class
Edit server-side encryption
Edit metadata
Edit tags
Make public using ACL
CloudShell
Feedback
Language


aws
Services
Search
[Alt+S]
EC2
RDS
VPC
IAM
S3
EFS
Elastic Beanstalk
Cloud9
CodeCommit
Lambda
CloudWatch
Amazon S3 > Buckets > roja12345 > Make public
Make public Info
The make public action enables public read access in the object access control list (ACL) settings. Learn more.
When public read access is enabled and not blocked by Block Public Access settings, anyone in the world can access the specified objects.
This action applies to all objects within the specified folders. Objects added to these folders while the action is in progress might be affected.
Specified objects
Find objects by name
1
Name
Type
Last modified
Size
css/
Folder
-
favicon.ico
ico
August 7, 2023, 17:33:51 (UTC+05:30)
318.0 B
images/
Folder
index.html
html
August 7, 2023, 17:33:52 (UTC+05:30)
7.8 KB
Cancel
Make public

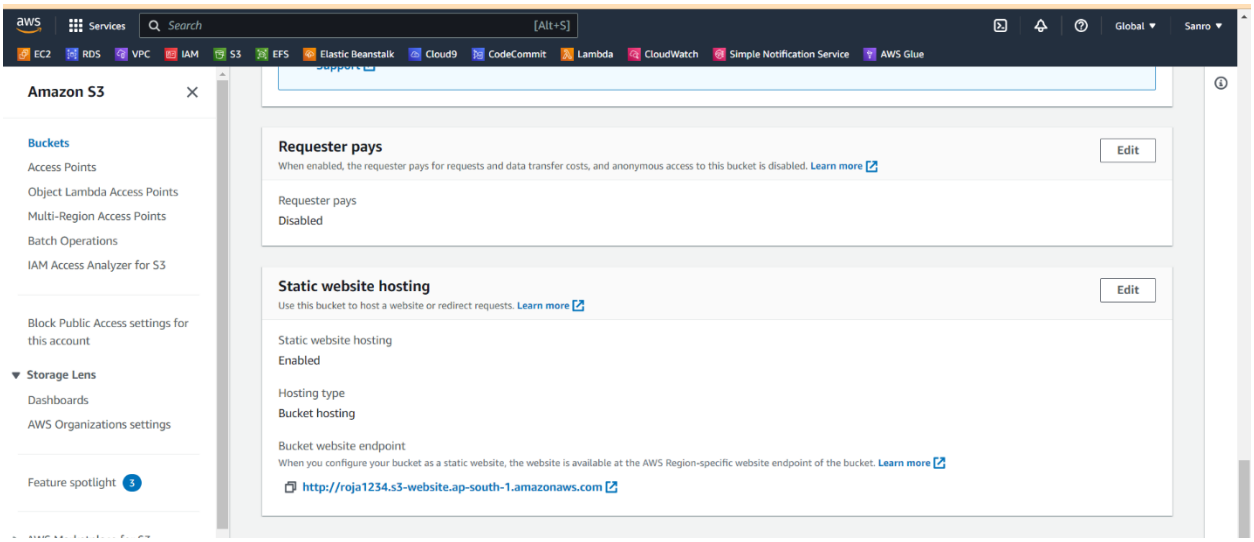
Step 5: Now go to properties and enable static website hosting

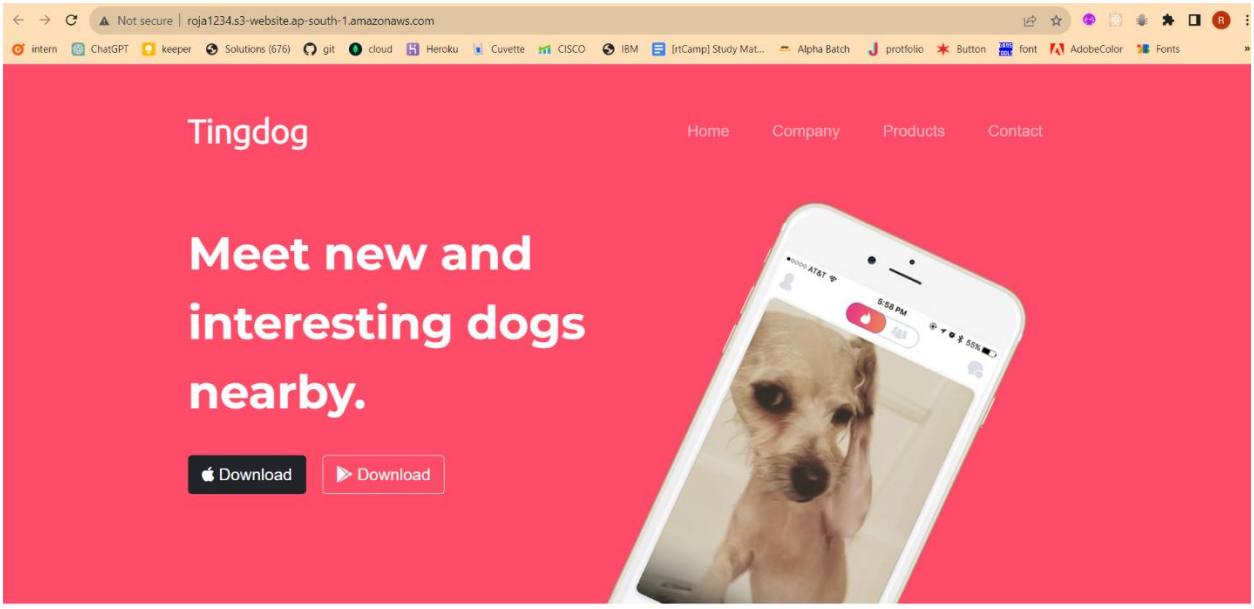
Both step 4 and 5 are permissions for providing the access of our website globally



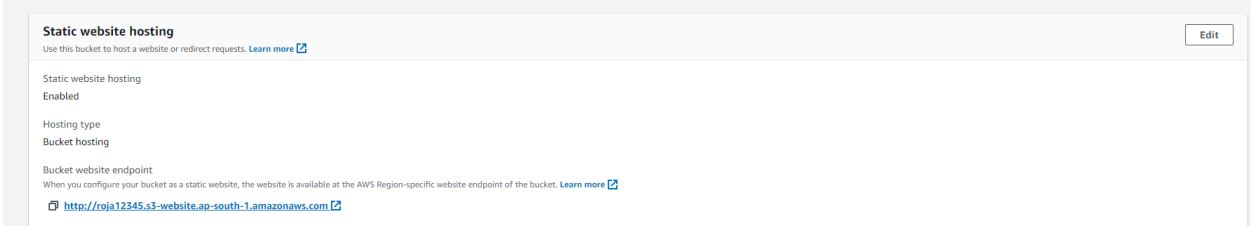
Step 6: Thus, our website is hosted on the AWS Cloud which can be accessed in many ways some of them are provided below

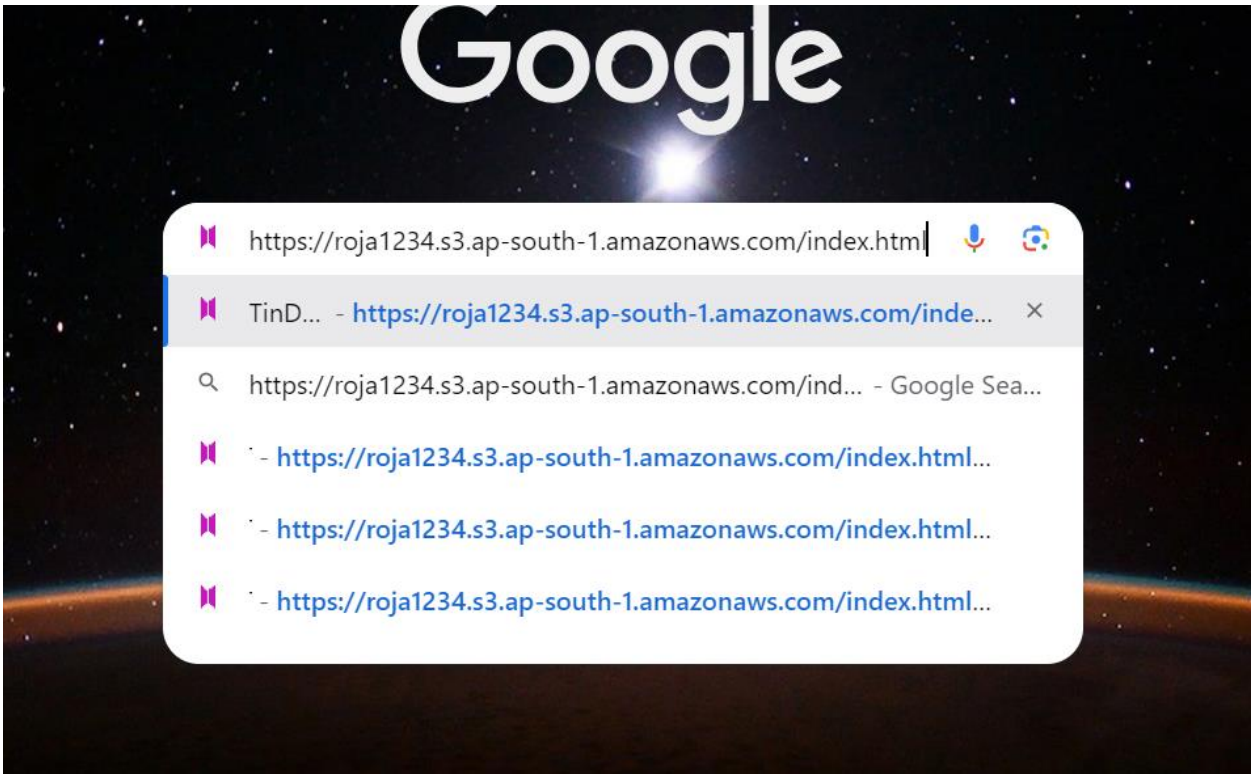
a. We can simply click on the URL that is shown under ‘static website hosting’ in properties

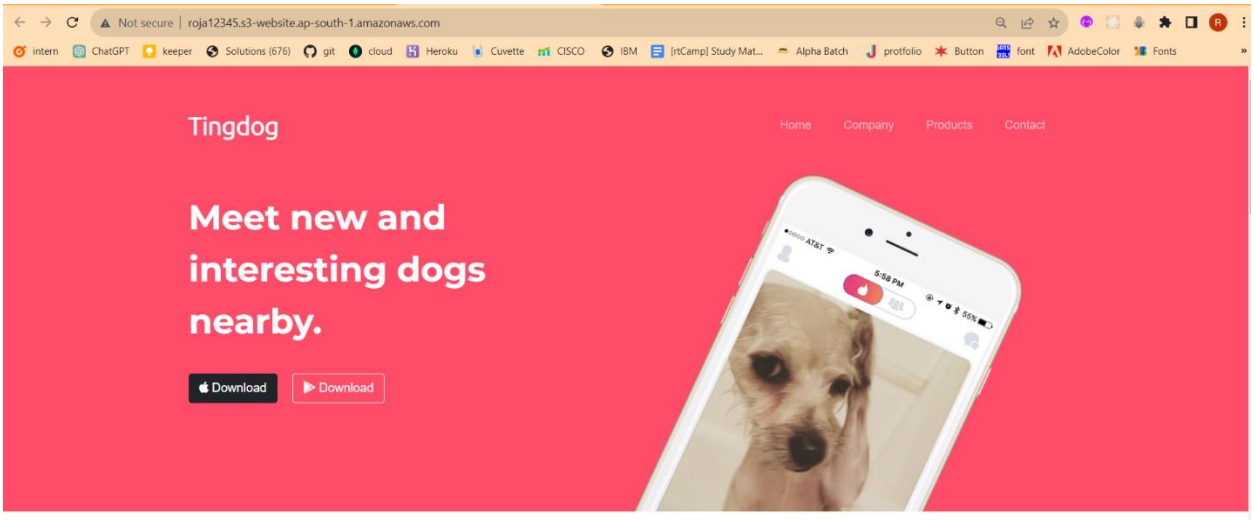




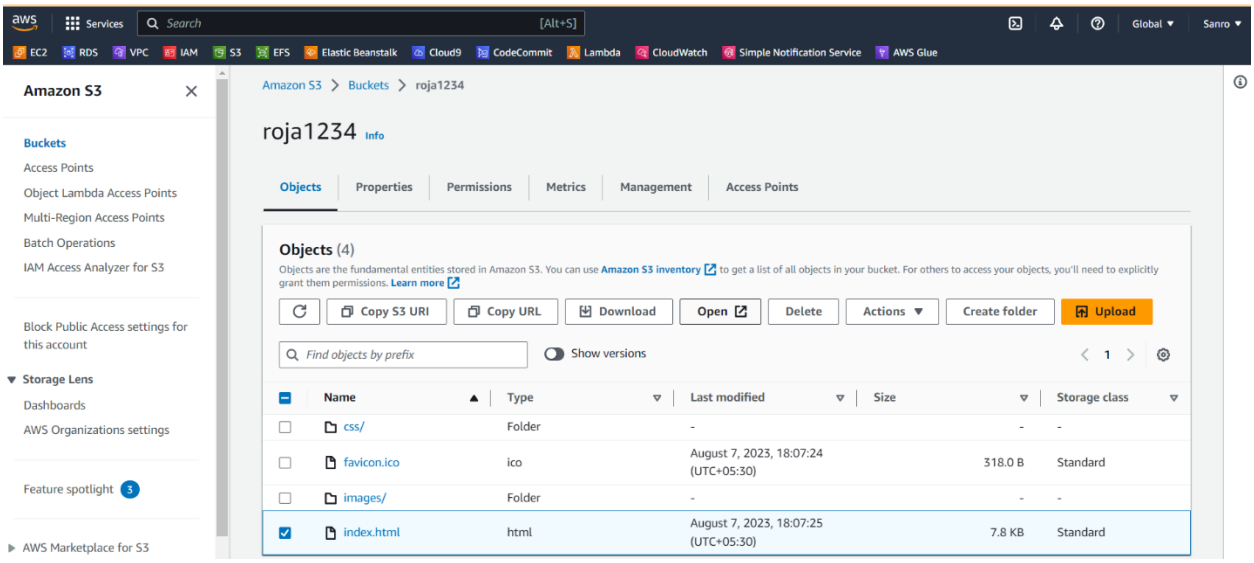
b. We can copy the website URL and paste it on the browser



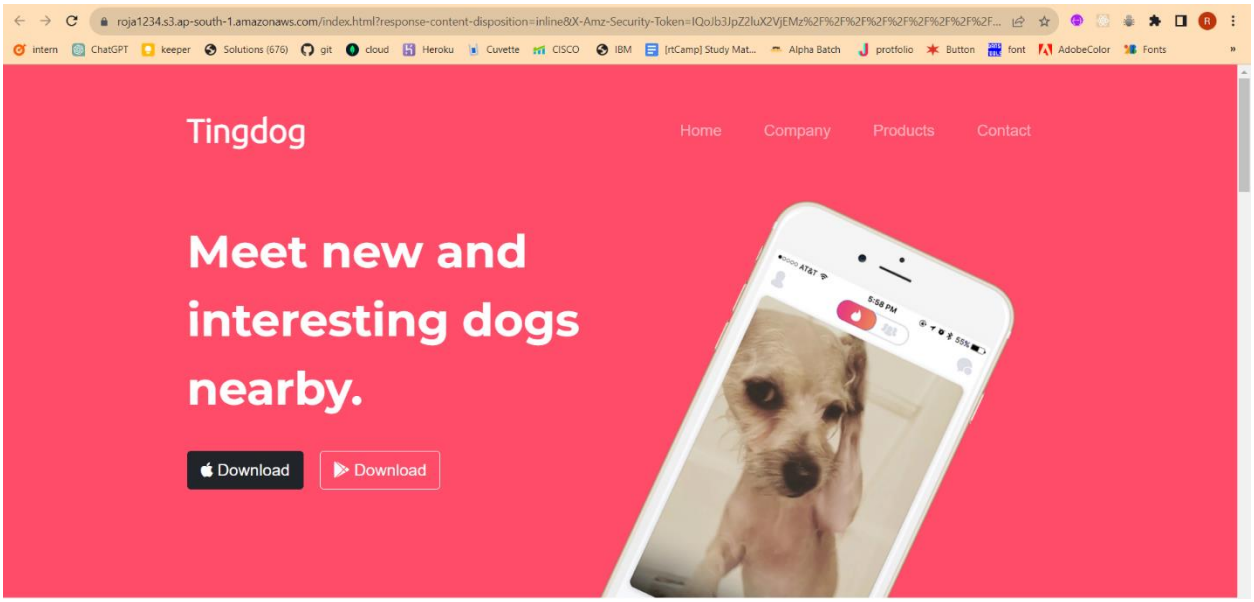




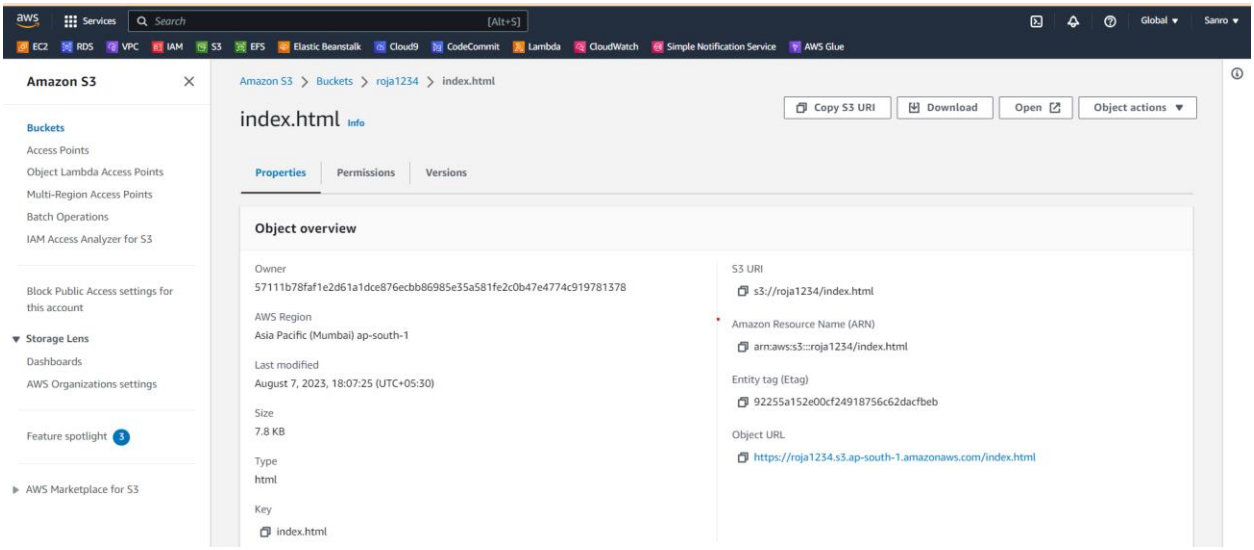
c. Go to the bucket and to the main file of our website which is index.html, select it then we can click on ‘open URL’



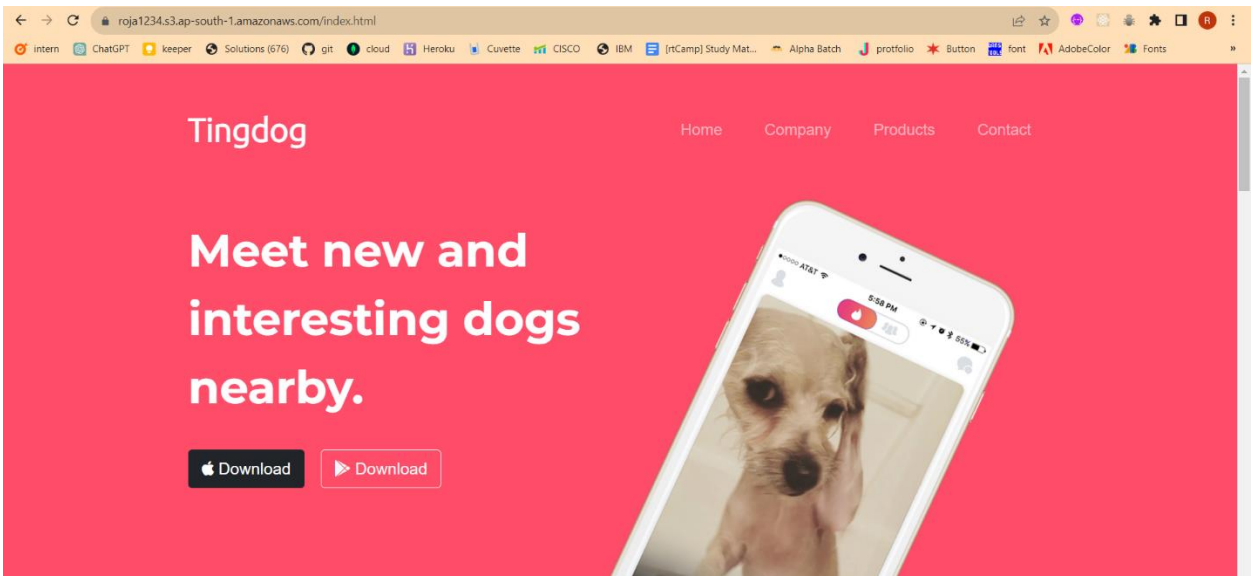
- Observe the URL on the browser to know the change on how we are accessing in different ways



d. The last way is by clicking on the index.html file and then go to properties there we can find a URL , click on it which redirects to the website



- We can observe the URL Path which end point is shown an /index.html



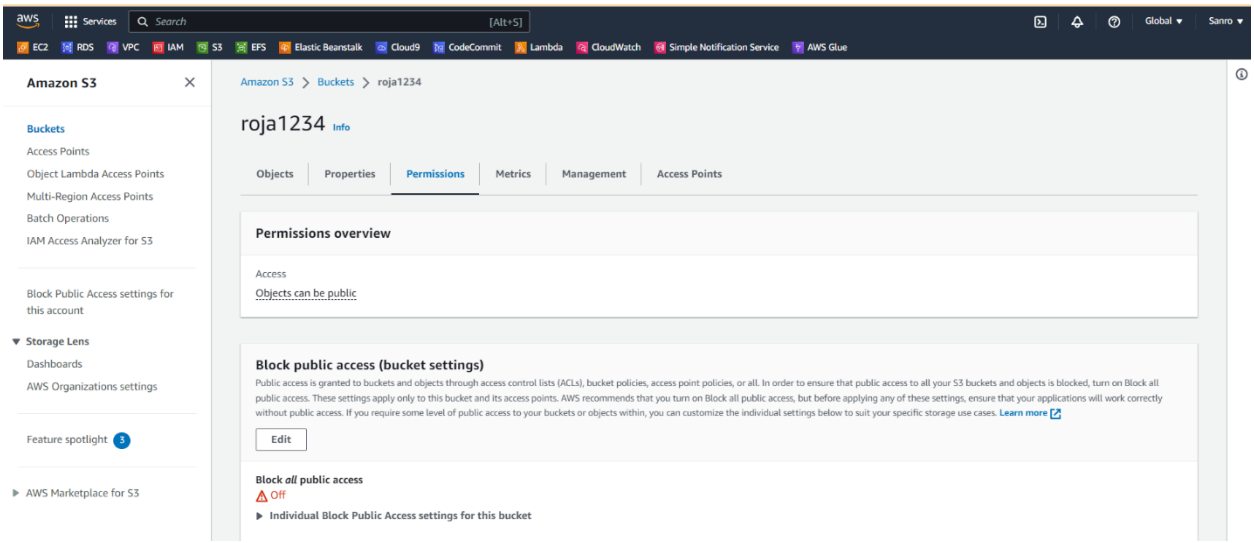
These has been the steps for hosting a static website in AWS s3

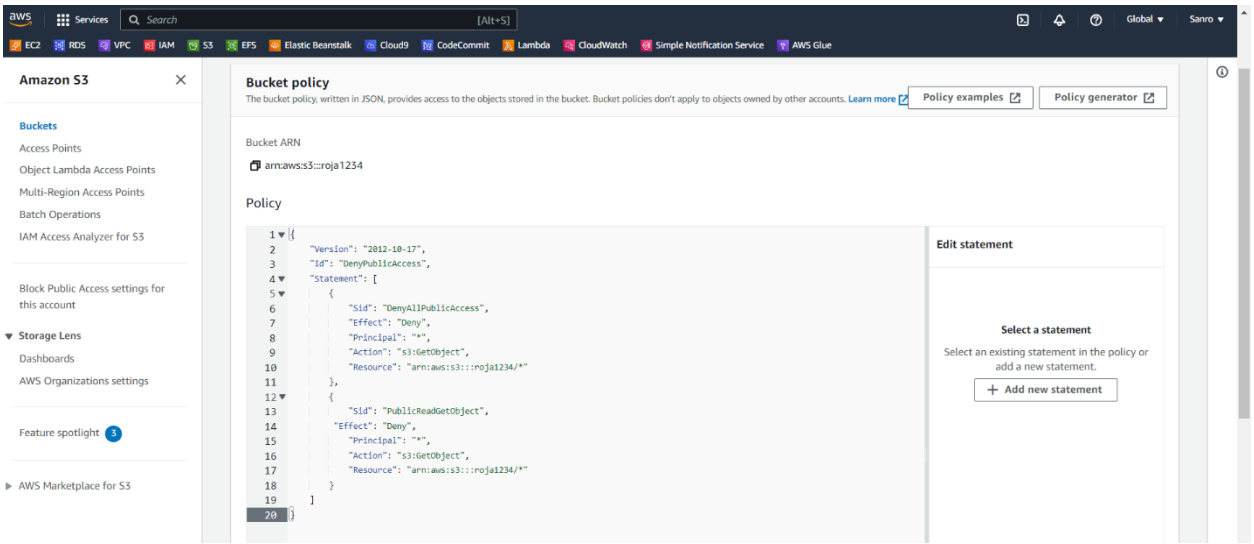
Step 7: Go to permissions and edit bucket policies (optional)

In addition to these we can add few more steps to the above process in order to provide much security and accessibility restrictions through bucket policies . They are

Bucket Policy for Public Access Control: To prevent accidental public access to your static website content, you can use a bucket policy that denies public access by default and then grants access to specific AWS services and resources.

Website Hosting Permissions: Allow public read access to your website's objects so that they can be accessed by visitors.





Done! here's my website http://roja1234.s3-website.ap-south-1.amazonaws.com hosted in AWS s3