STATIC WEBSITE USING S3 BUCKET CLOUD FRONT (CND-CONTENT DELIVERY NETWORK)

CONTENT:

To serve a static website hosted on Amazon S3, you can deploy a CloudFront distribution using one of these configurations:

Using a REST API endpoint as the origin, with access restricted by an origin access control (OAC) or origin access identity (OAI)

Note: It's a best practice to use origin access control (OAC) to restrict access. Origin access identity (OAI) is a legacy method for this process.

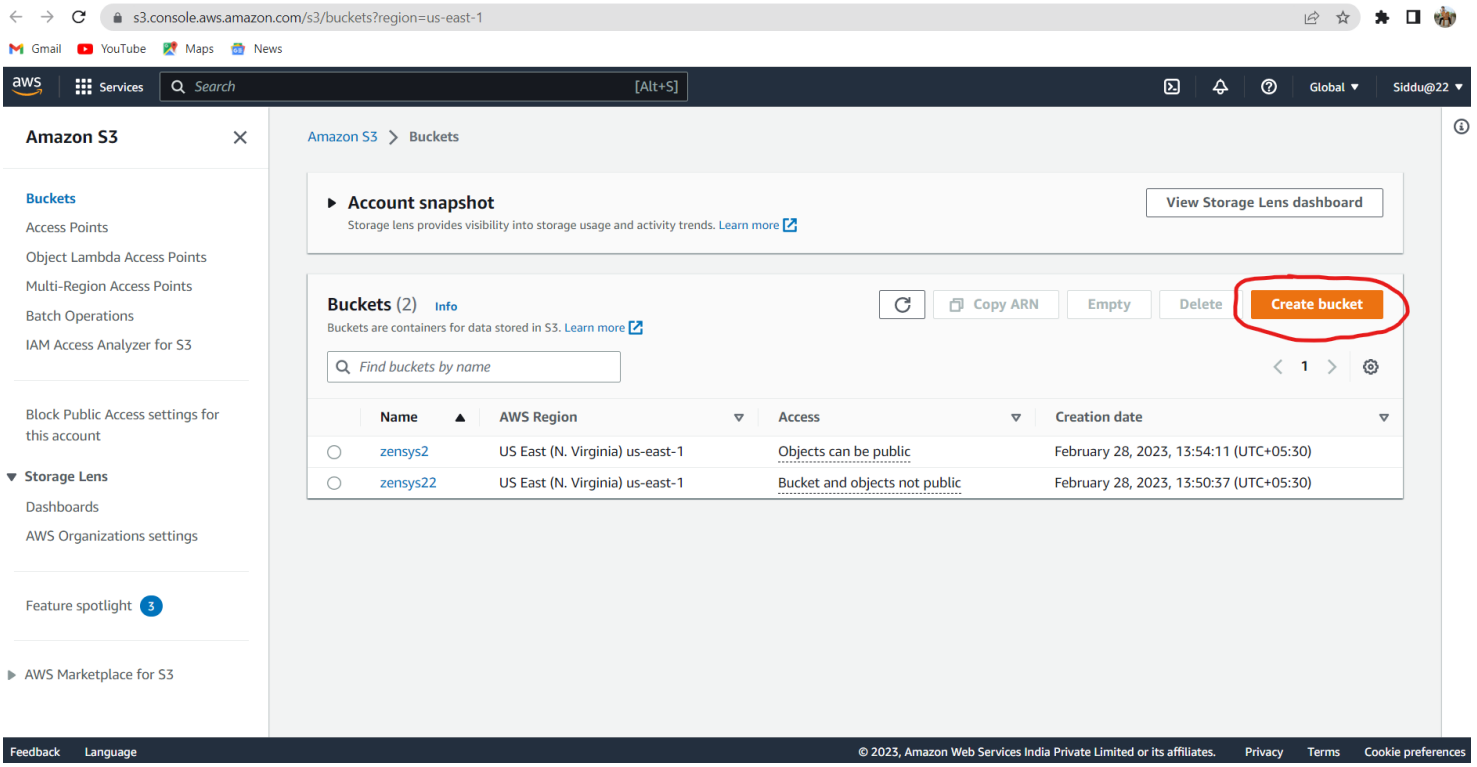
Using a website endpoint as the origin, with anonymous (public) access allowed

Using a website endpoint as the origin, with access restricted by a Referer header

Using CloudFormation to deploy a static website endpoint as the origin, and custom domain pointing to CloudFront

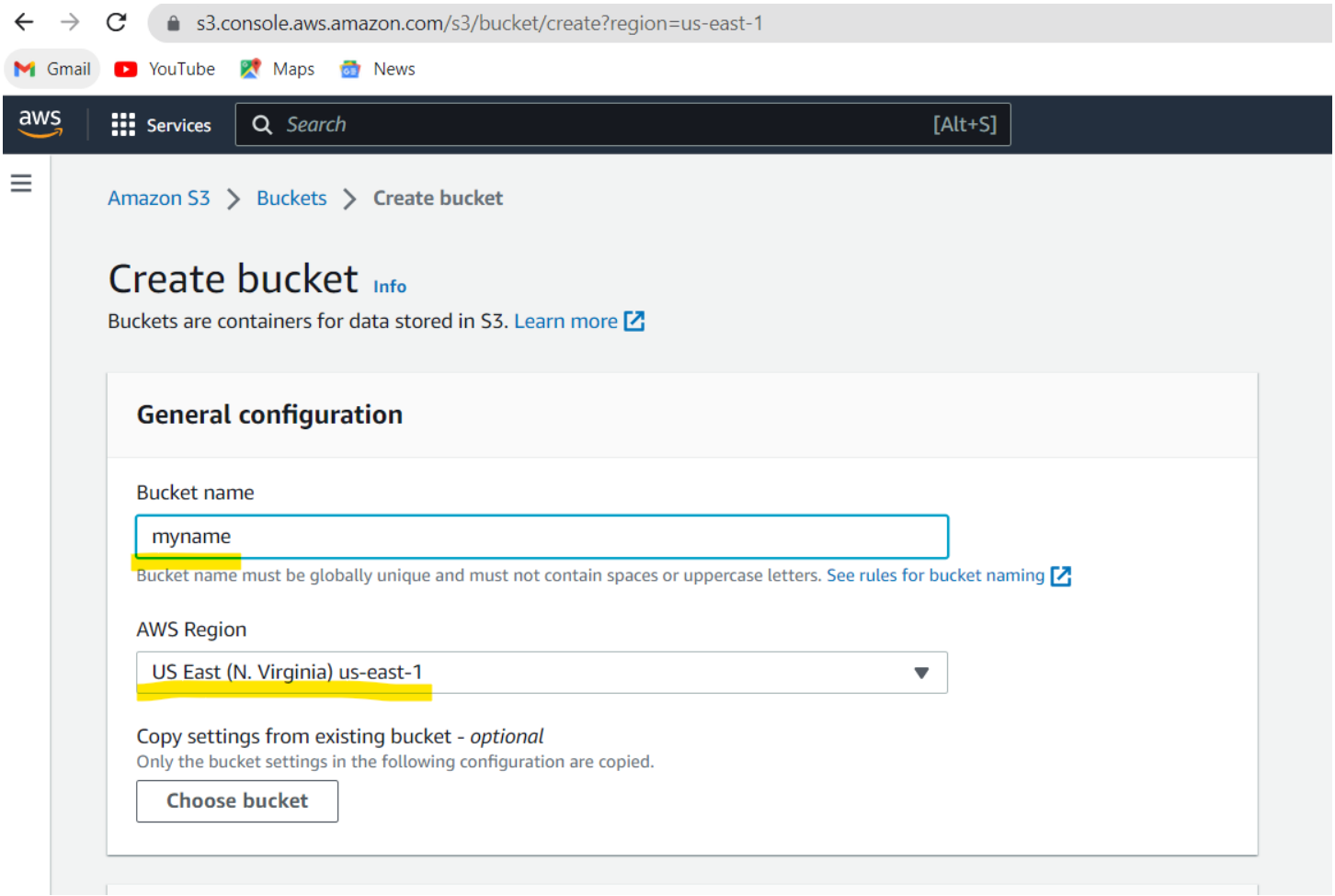
“NOW WE SEE STEP BY STEP PROCESS TO CREATE A STATIC WEBSITE USING S3 BUCKET”

- Open AWS console and login in to the account using the Gmail id and password.
- Type S3 Bucket in search bar open it in a new tab.
- Now click on create bucket.

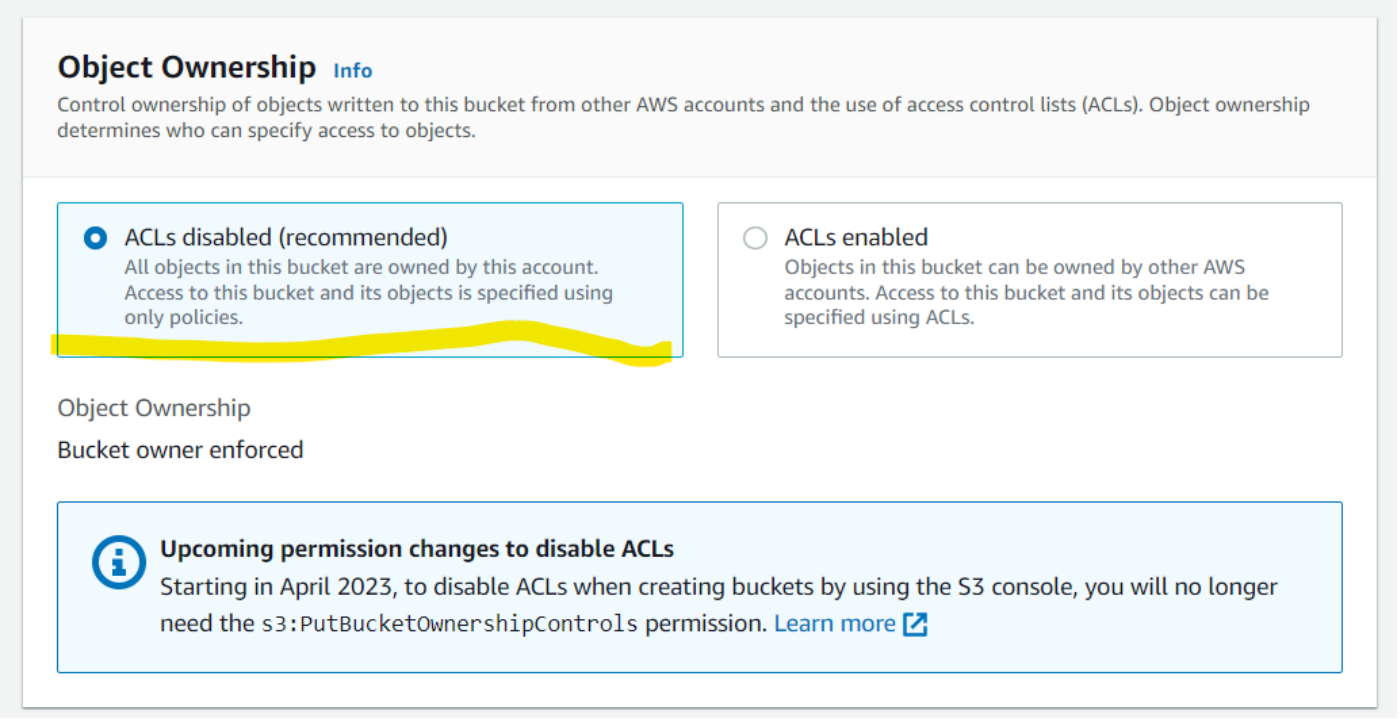


Now we are going to create a new bucket to upload some of the files of website what we have going to be launch a website.

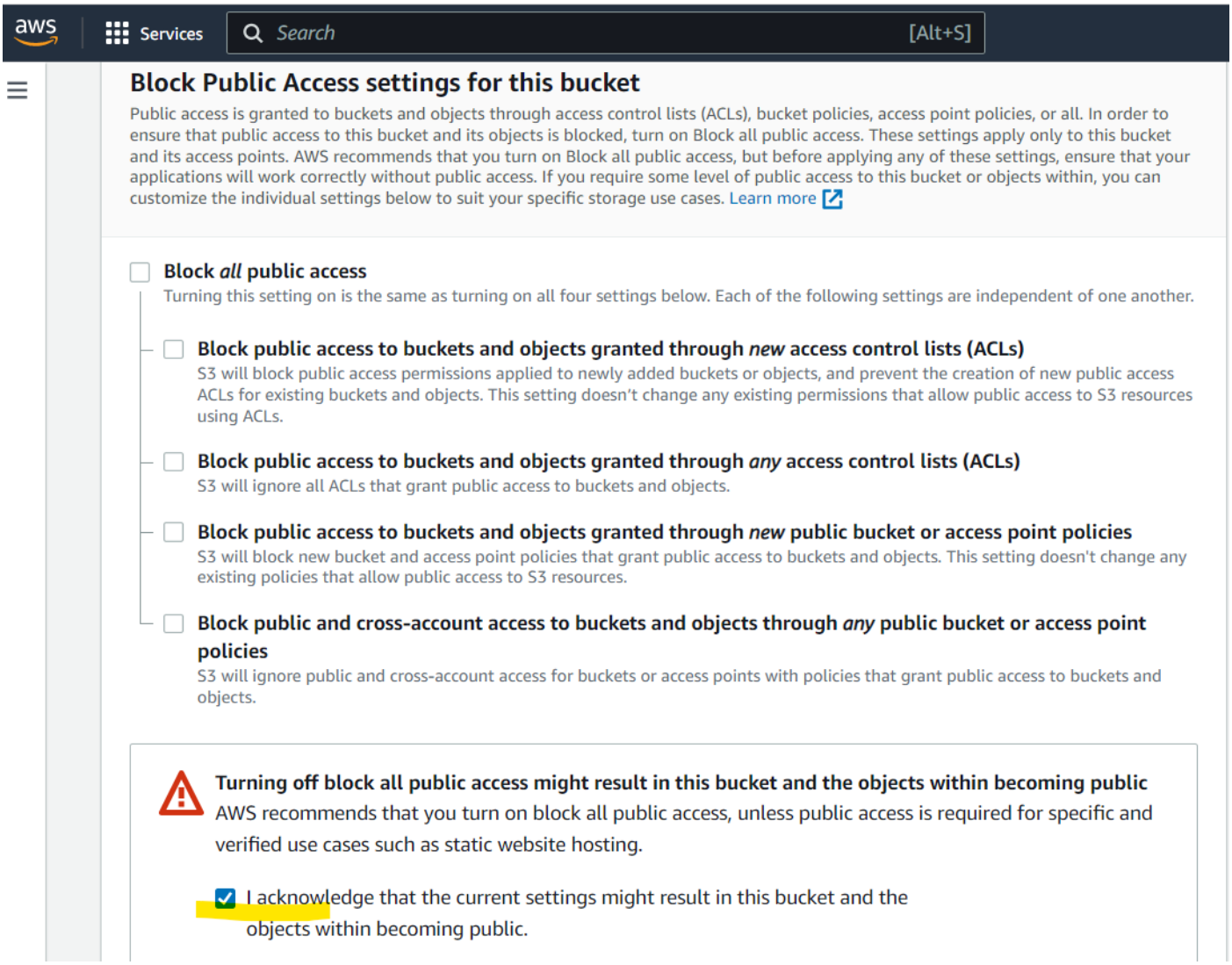
- Now title a name to the bucket we are going to create. then,
- Select the region



- Now select the ACL(access control list) it should be disabled.

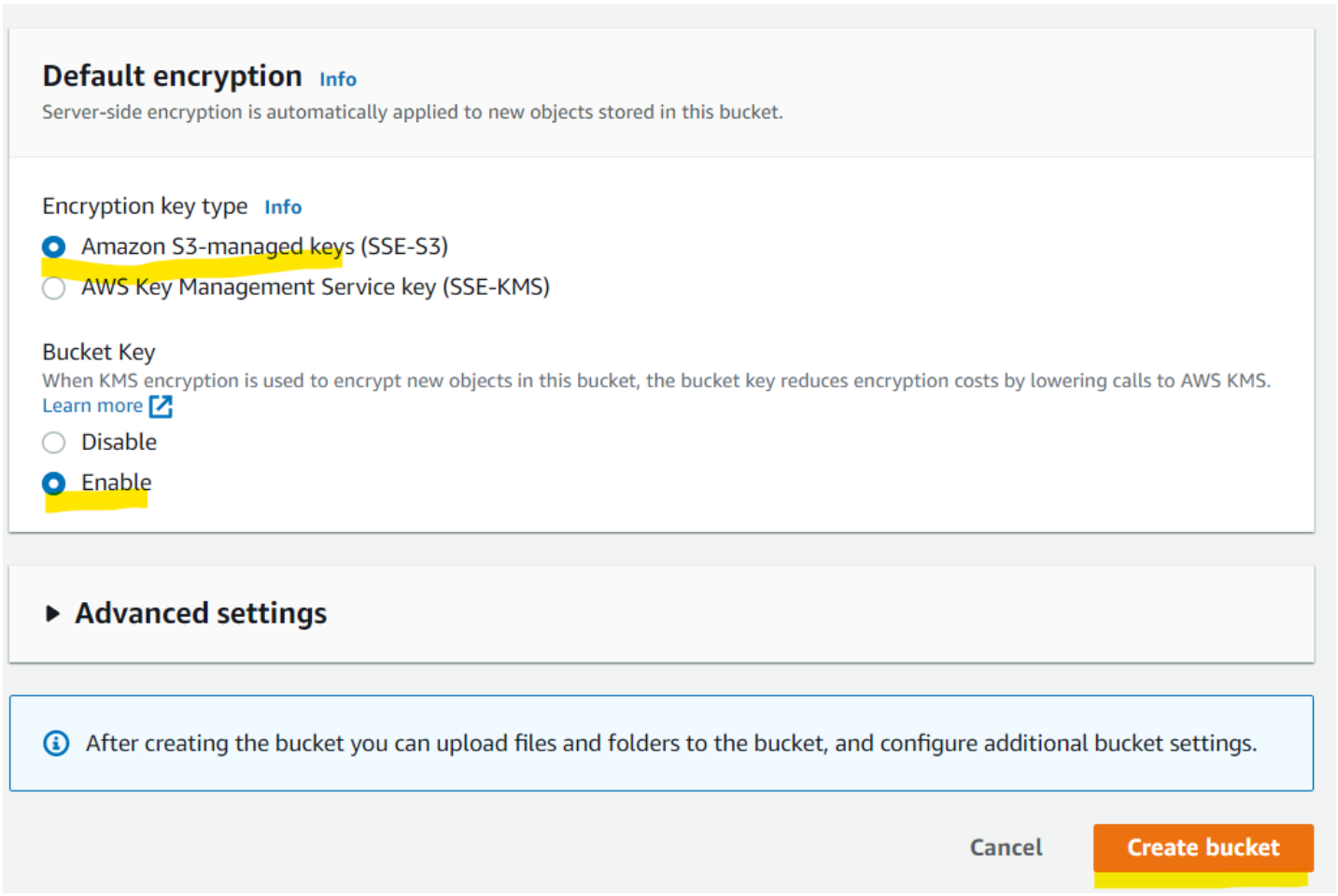


- Now click on Block all public access because we are creating the private access. Below we can see the acknowledge part of the access clock on it the we can create by public access.

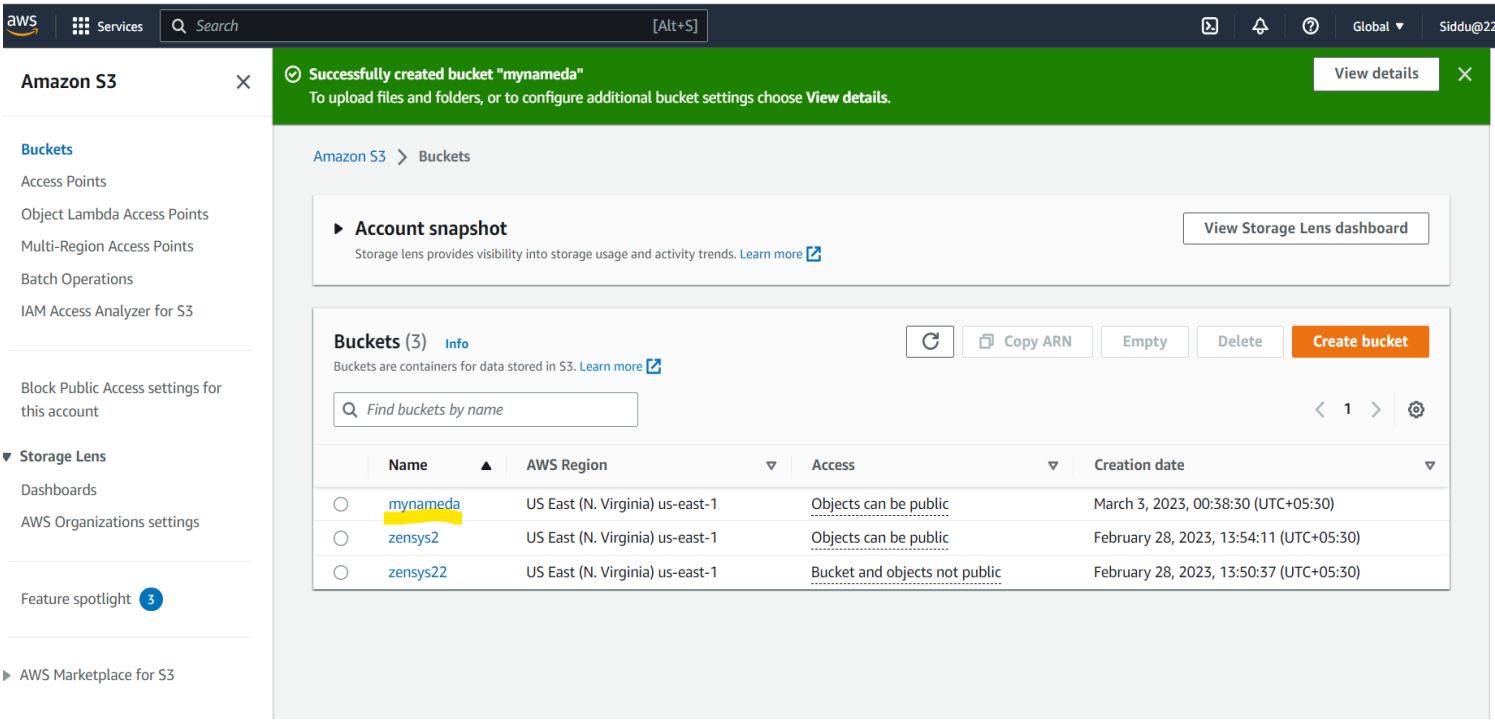


- Bucket version and key management are default selected.

Then, now click on the create bucket.

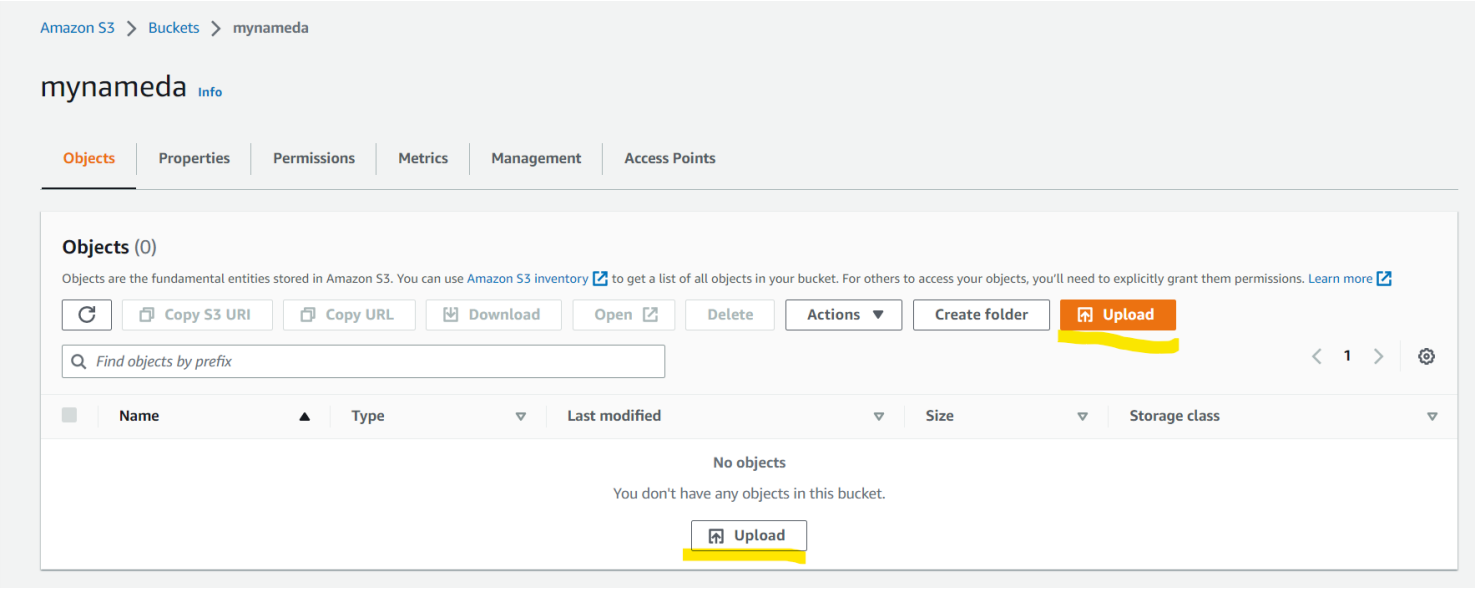


Now we can see bucket is created.

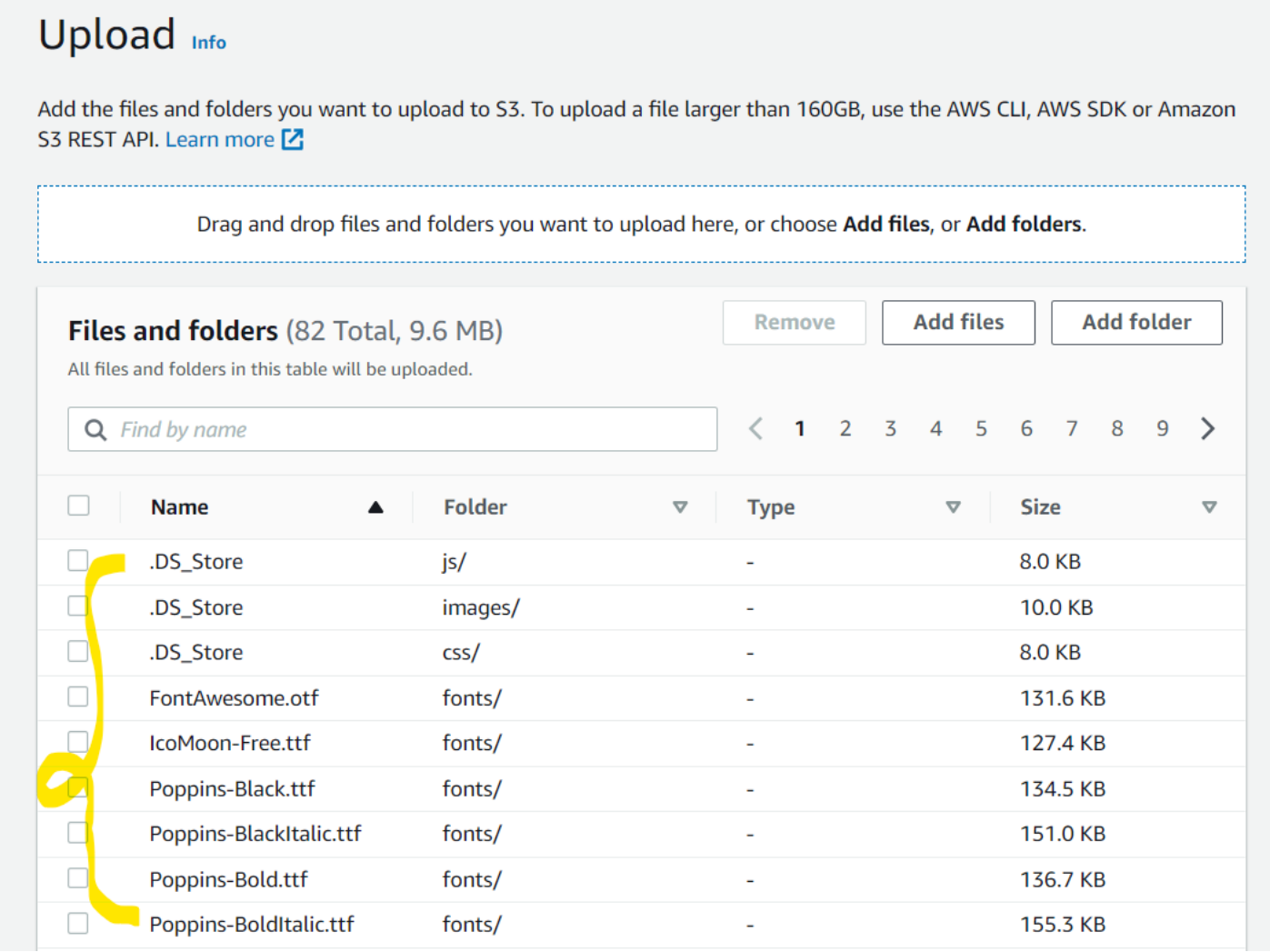


Now we click on the name of the S3 bucket. Then you can see the properties and fundamentals of the created S3 bucket.

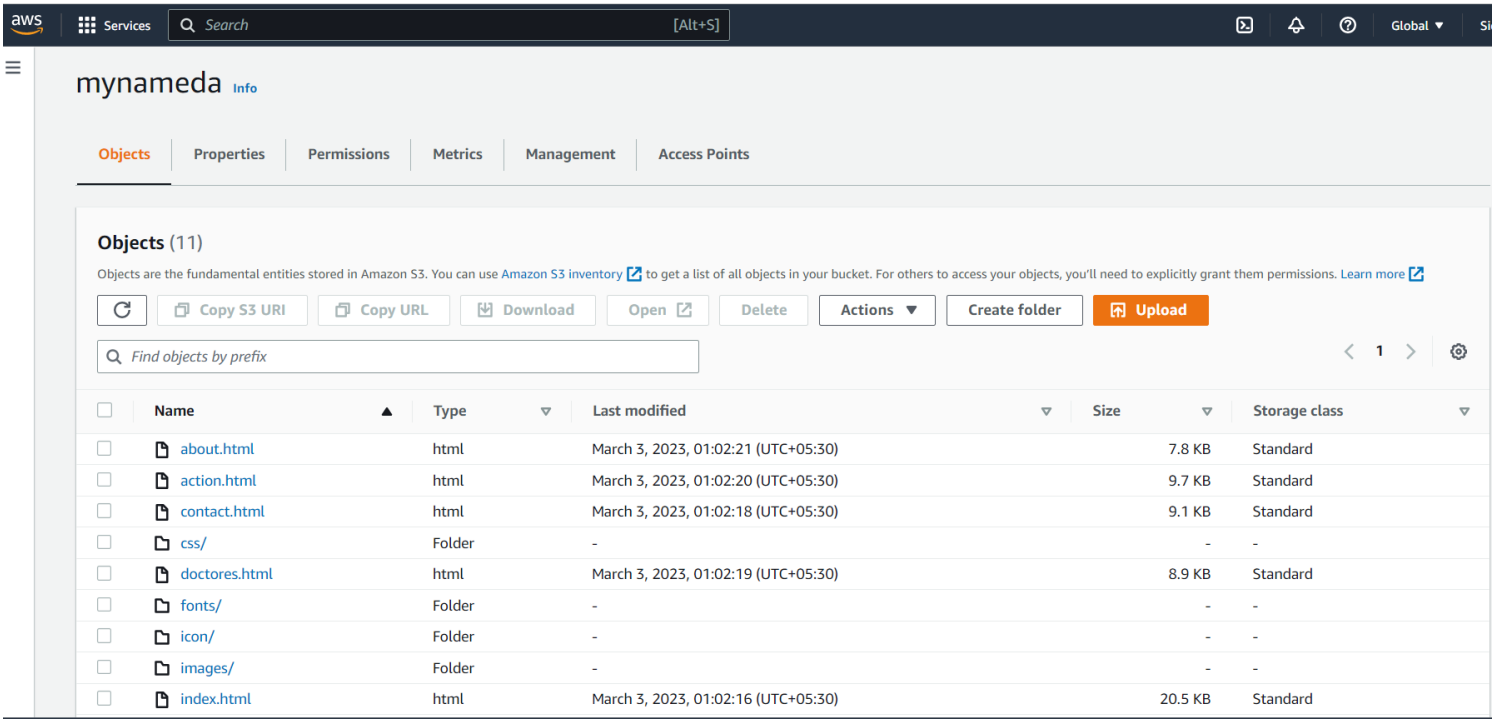
Now click on the upload button and upload the files which we are going to launch the website.



Now add files and click on upload button



Now click on the bucket name then we can see the files what we have uploaded in the properties of the regarding bucket.



Now click on properties the bucket then scroll down till end then click on the edit button of static website hosting.

Now click on enable button of static website hosting.

Then give a name to index documentation. Type this in the index document(/index.html)

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

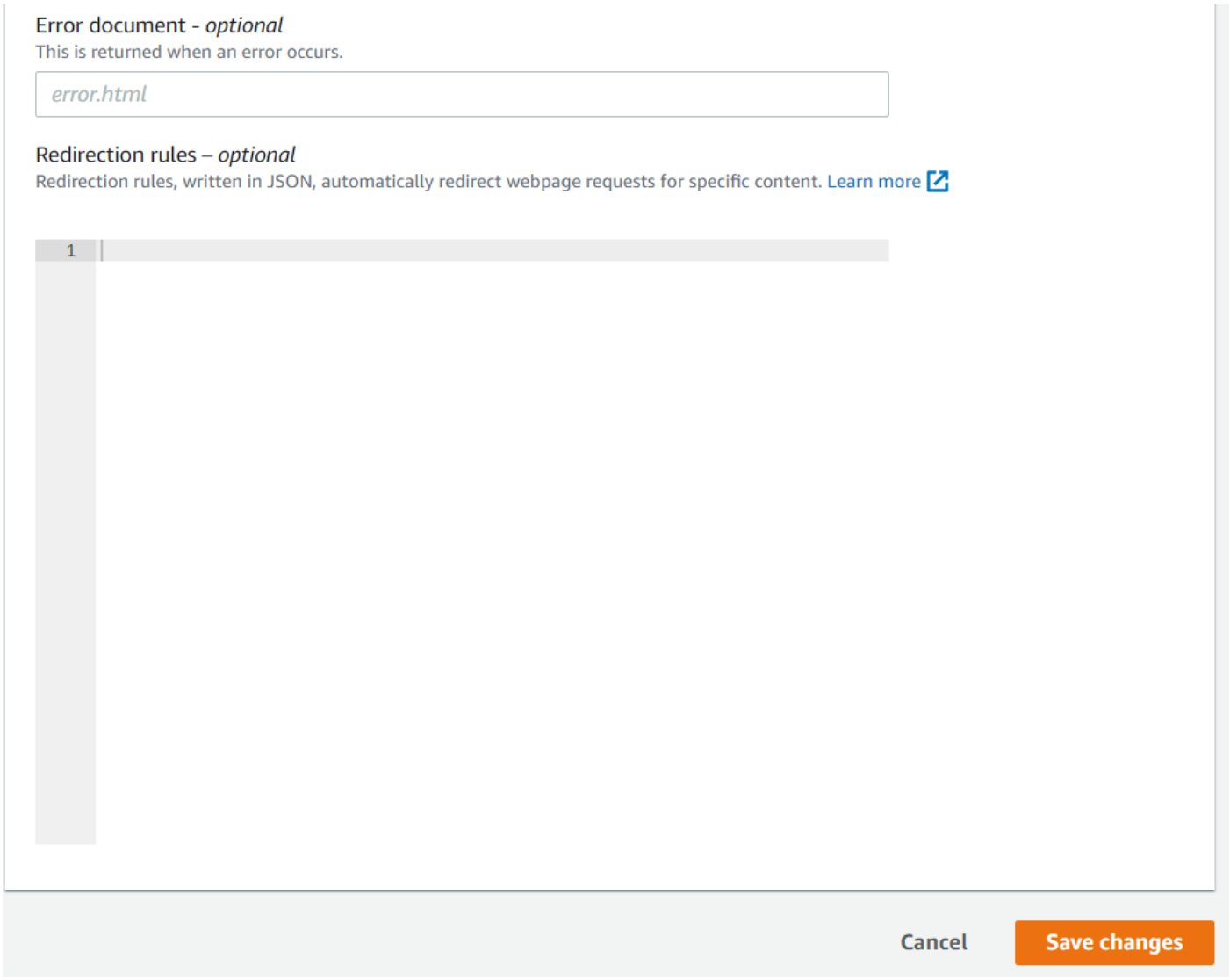
- ◉ Host a static website
  Use the bucket endpoint as the web address. Learn more
- ○ Redirect requests for an object
  Redirect requests to another bucket or domain. Learn more

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

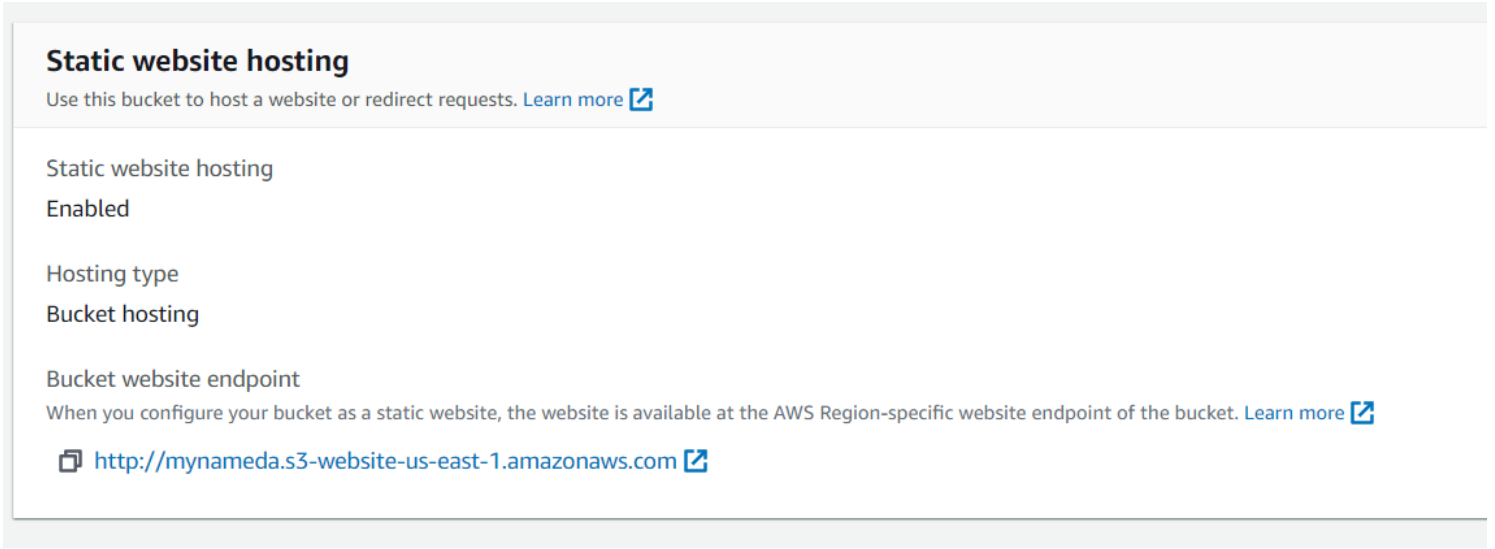
Specify the home or default page of the website.

index.html

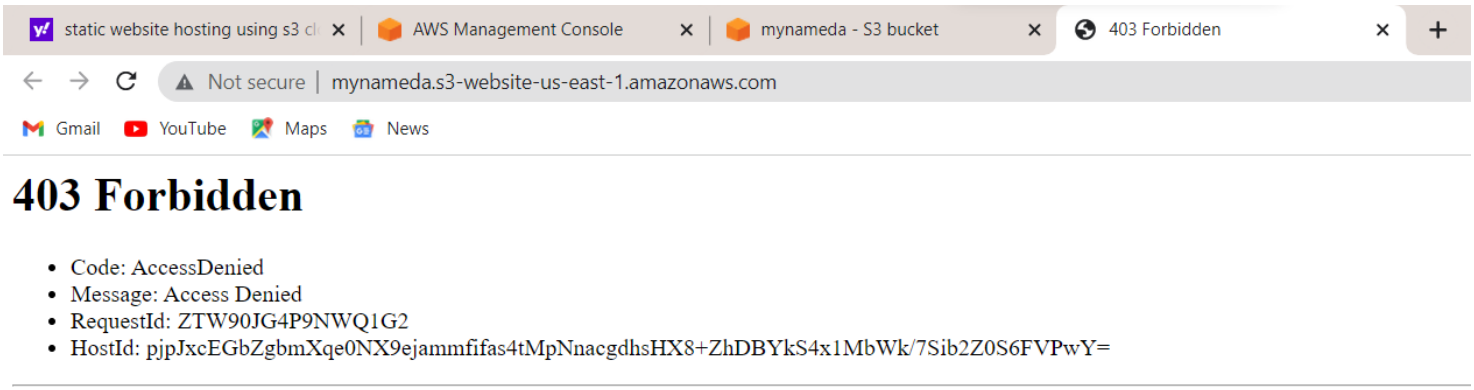


Now click on the save changes. Then it will be saved

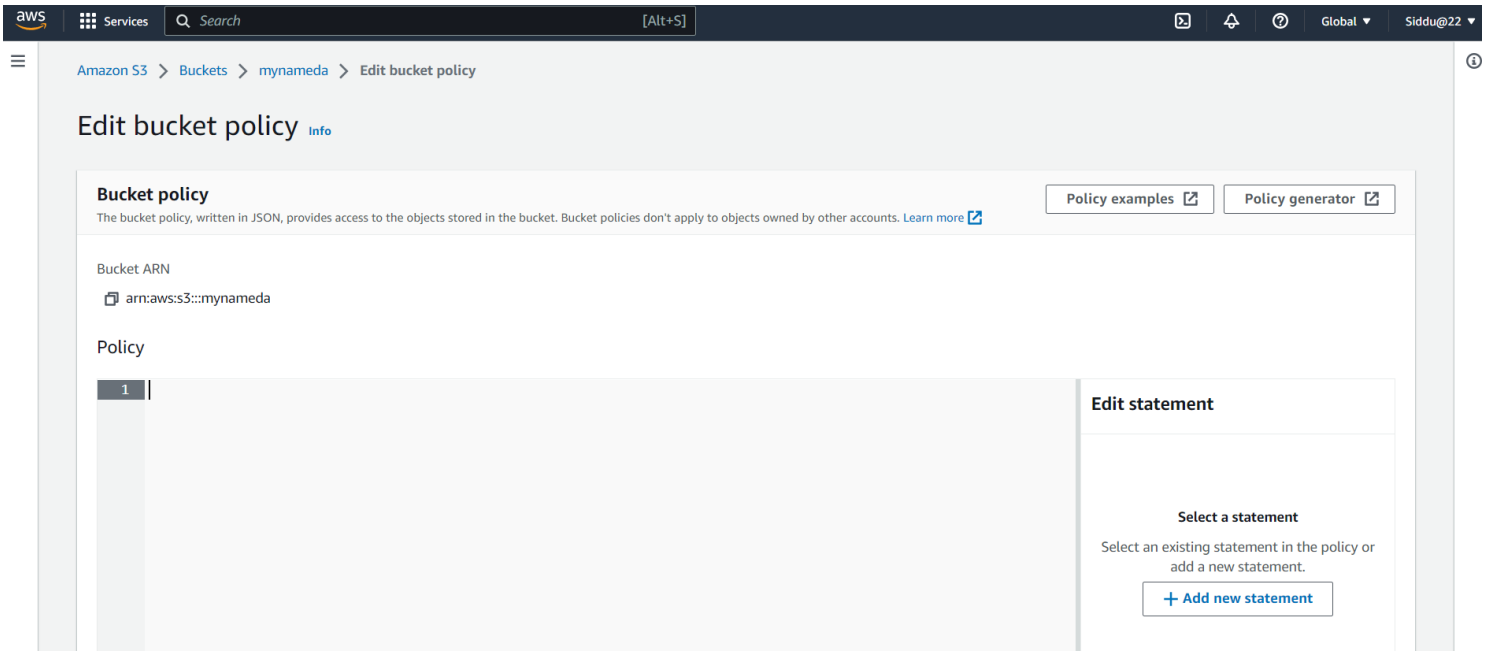
Now scroll down the you can see the URL it is just a bucket static website



If we click on the URL, as shown below it will be displayed,



Now open permission tab in S3 bucket and edit Bucket policy to allow public access for bucket.



Then click on policy generator.

1.select type policy, choose S3 bucket policy.

2.select the principle to (*) it defines to select total coding for the policy generator.

3.AWS service will default selected when we gave (*) to the principle.

4.click on all actions

5. copy amazon resource name from bucket ARN paste it in policy generator ARN.

6.now click on add statment

AWS Policy Generator

The AWS Policy Generator is a tool that enables you to create policies that control access to Amazon Web Services (AWS) products and resources. For more information about creating policies, see key concepts in Using AWS Identity and Access Management. Here are sample policies.

Step 1: Select Policy Type

A Policy is a container for permissions. The different types of policies you can create are an IAM Policy, an S3 Bucket Policy, an SNS Topic Policy, a VPC Endpoint Policy, and an SQS Queue Policy.

Select Type of Policy SQS Queue Policy

Step 2: Add Statement(s)

A statement is the formal description of a single permission. See a description of elements that you can use in statements.

Effect Allow Deny

Principal

Use a comma to separate multiple values.

AWS Service Amazon SQS All Services ('*')

Use multiple statements to add permissions for more than one service.

Actions -- Select Actions -- All Actions ('*')

Amazon Resource Name (ARN)

ARN should follow the following format: arn:aws:sqs:${Region}:${Account}:${QueueName}.
Use a comma to separate multiple values.

Add Conditions (Optional)

Add Statement

Now you can see the generated policy.

Policy JSON Document

Click below to edit. To save the policy, copy the text below to a text editor.
Changes made below will **not be reflected in the policy generator tool.**

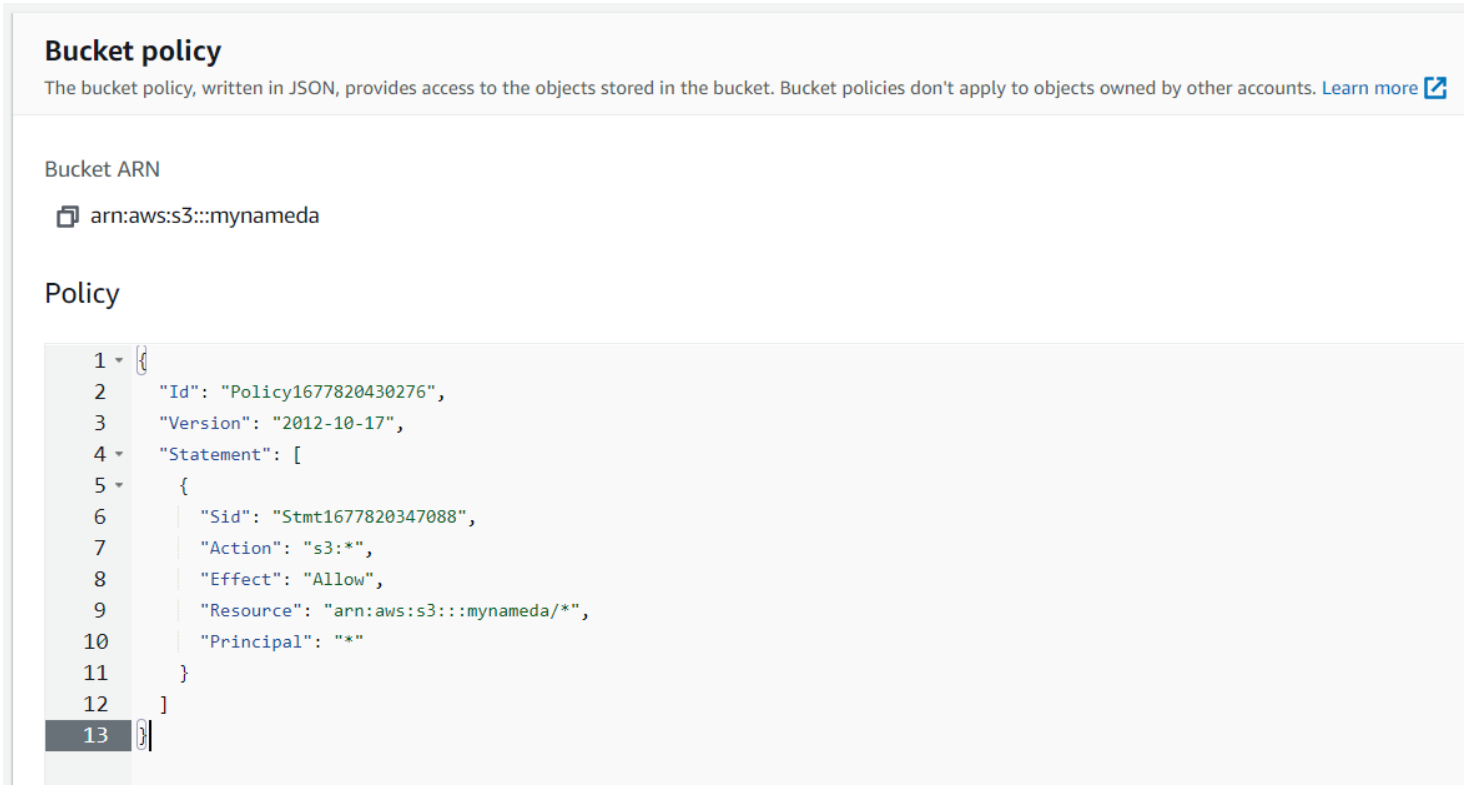
```
{
  "Id": "Policy1677820430276",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1677820347088",
      "Action": "s3:*",
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::mynameda/*",
      "Principal": "*"
    }
  ]
}
```

This AWS Policy Generator is provided for informational purposes only, you are still responsible for your use of Amazon Web Services technologies and ensuring that your use is in compliance with all applicable terms and conditions. This AWS Policy Generator is provided as is without warranty of any kind, whether express, implied, or statutory. This AWS Policy Generator does not modify the applicable terms and conditions governing your use of Amazon Web Services technologies.

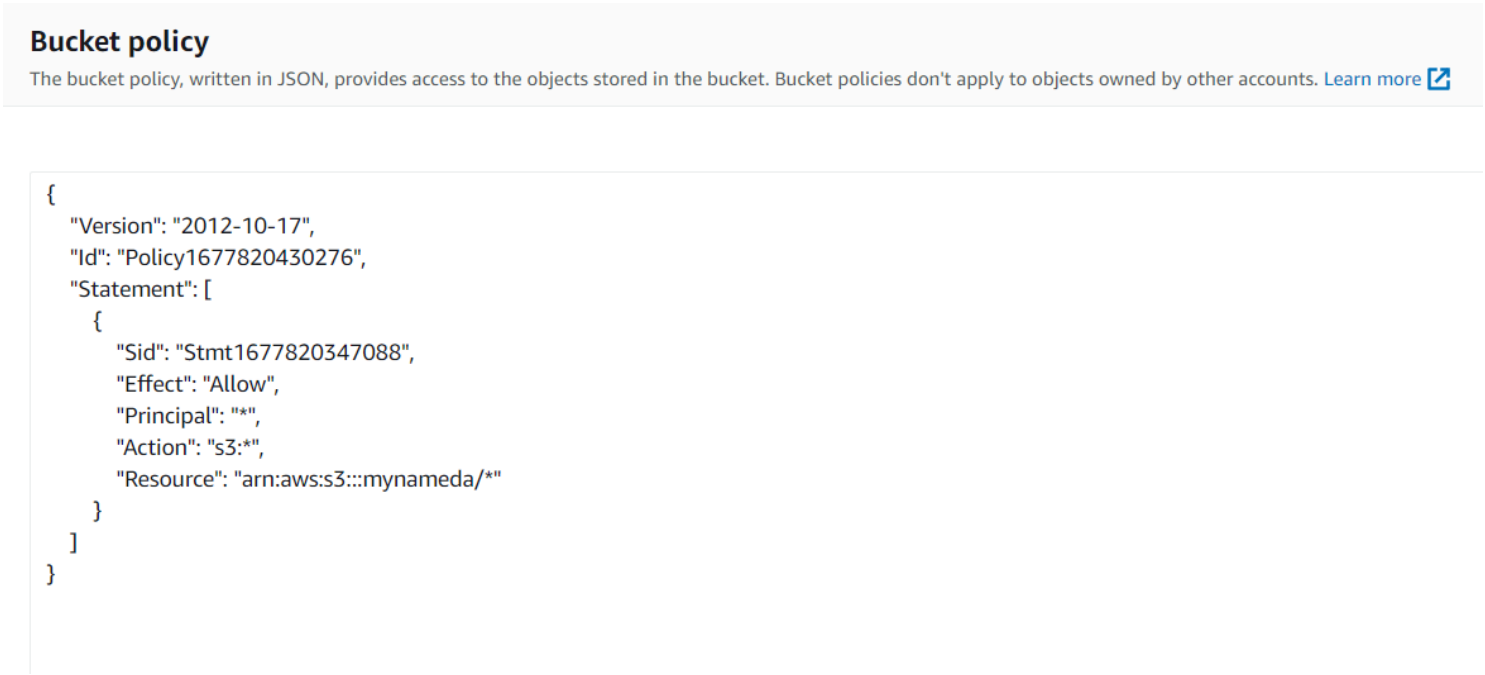
Close

Now do change near bucket name to /*.

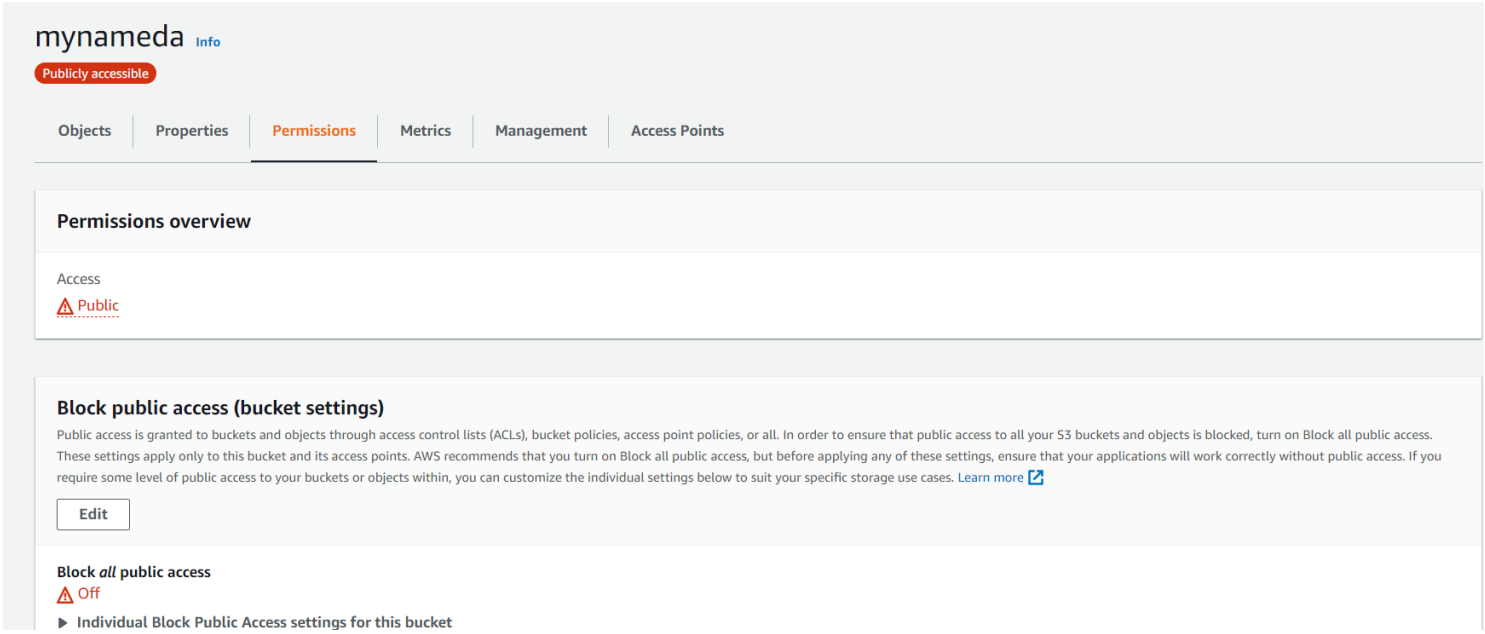
Now copy the policy and paste it in bucket policy.



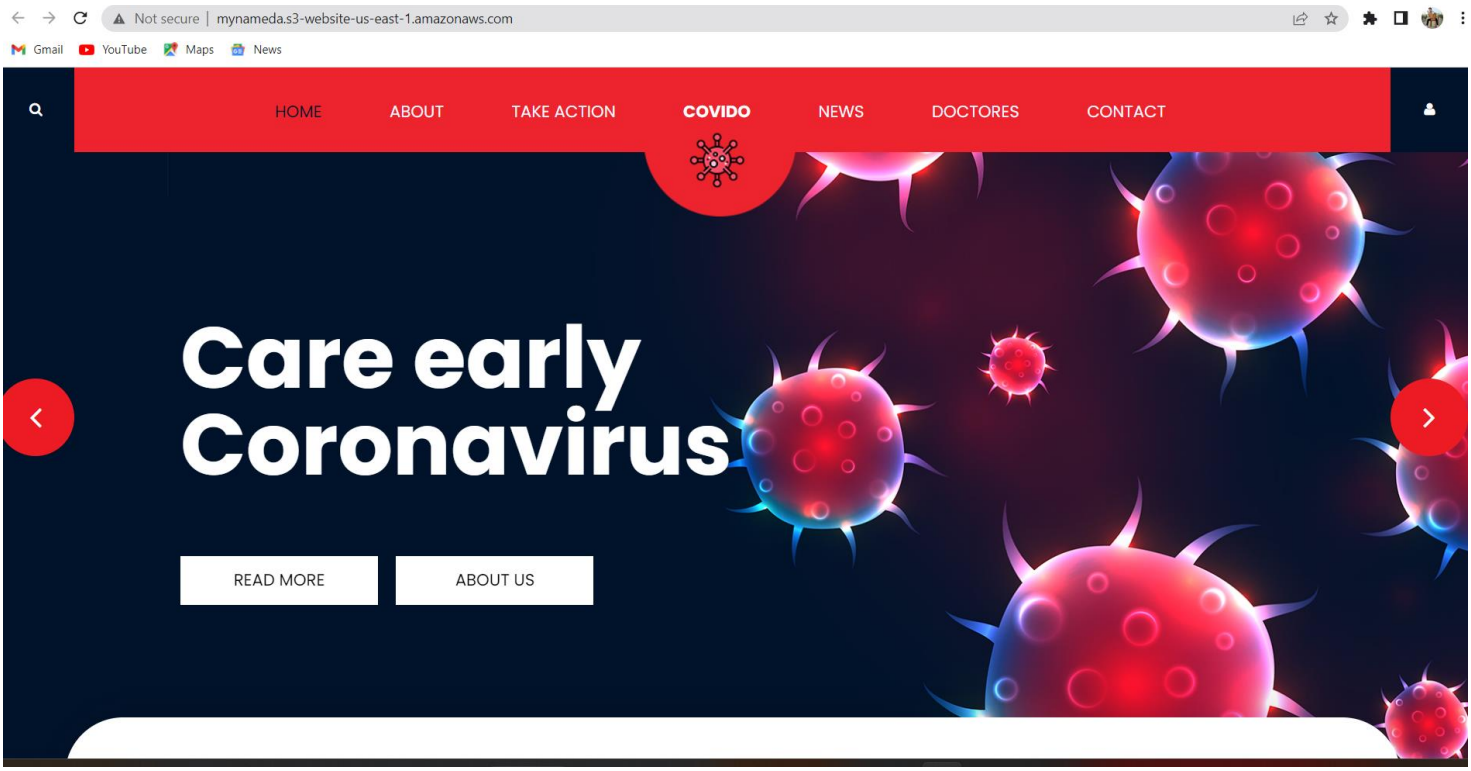
Then click on save changes. It will be updated and shown in bucket policy.



Now access permission will be overview int to public access.



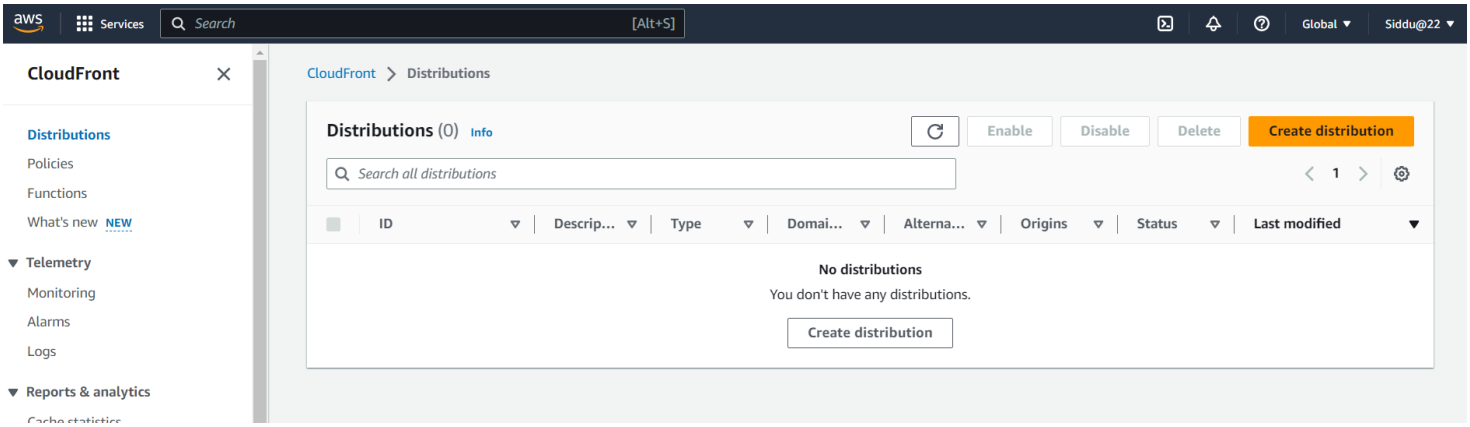
Now click on URL.



Now we can see the website what we have launched through S3 bucket.

Now we create it in a cloudfront distribution

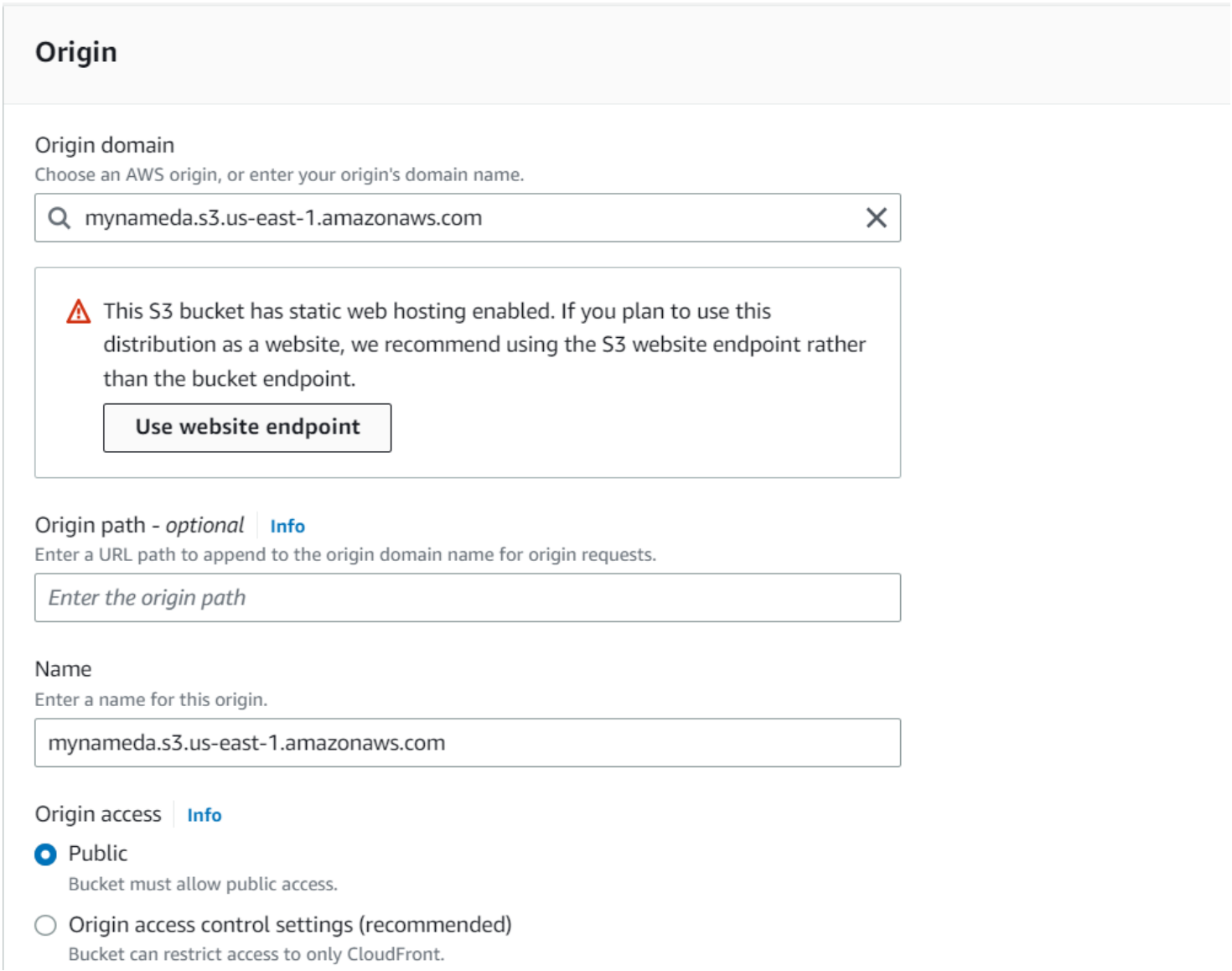
Go to search bar and type cloudfront, open it in a tab.



Now click on create distribution to create a distribution origin.

1. select the name of the origin domain

2. origin access must be public because we are disturbuting from the S3 bucket

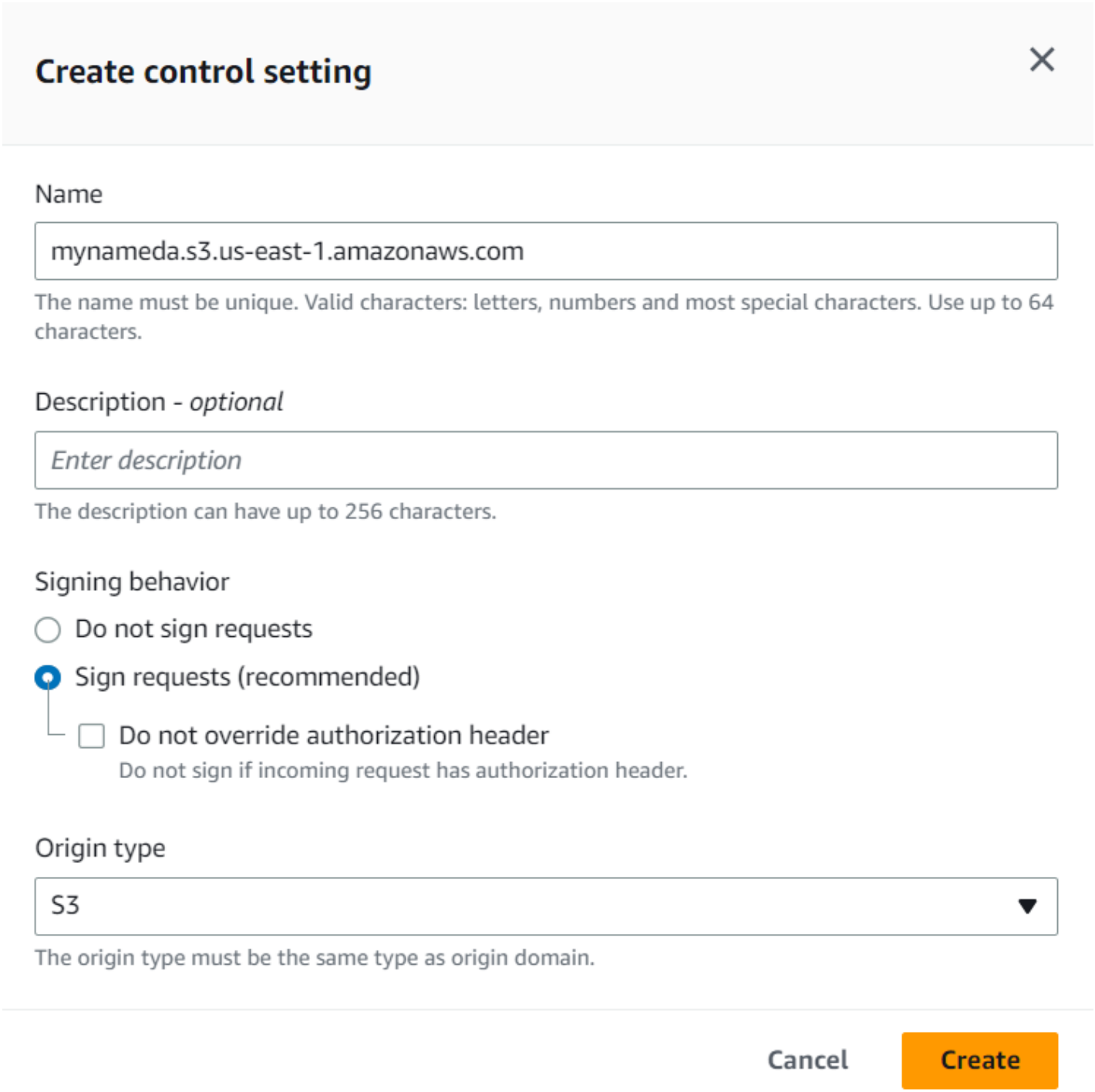


Click on origin access and change to origin access control settings.

Click on create control settings.

Select the name.

Select origin type to S3

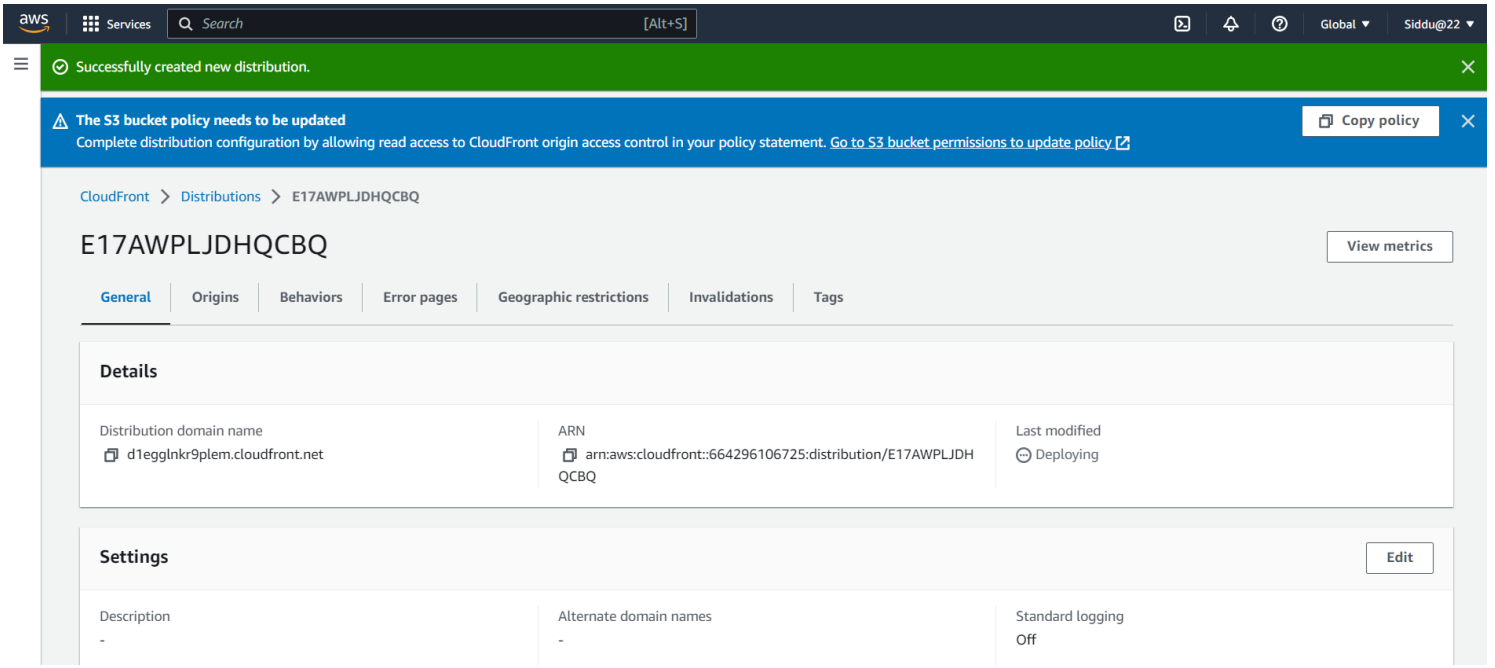


Click on create button.

It will create origin access

Remaining all behaviours are default selected no need of any changes

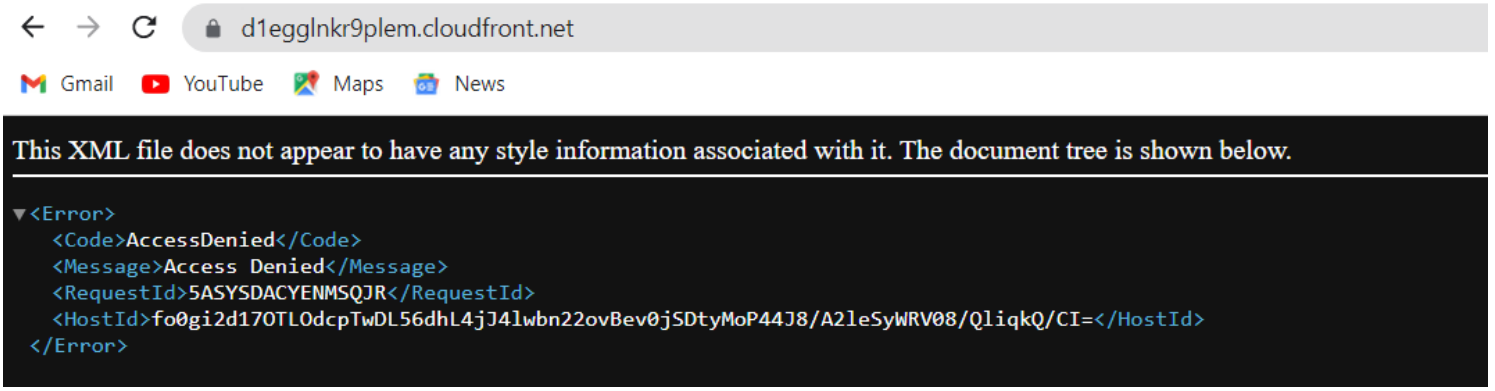
Finally click on the create distribution button.



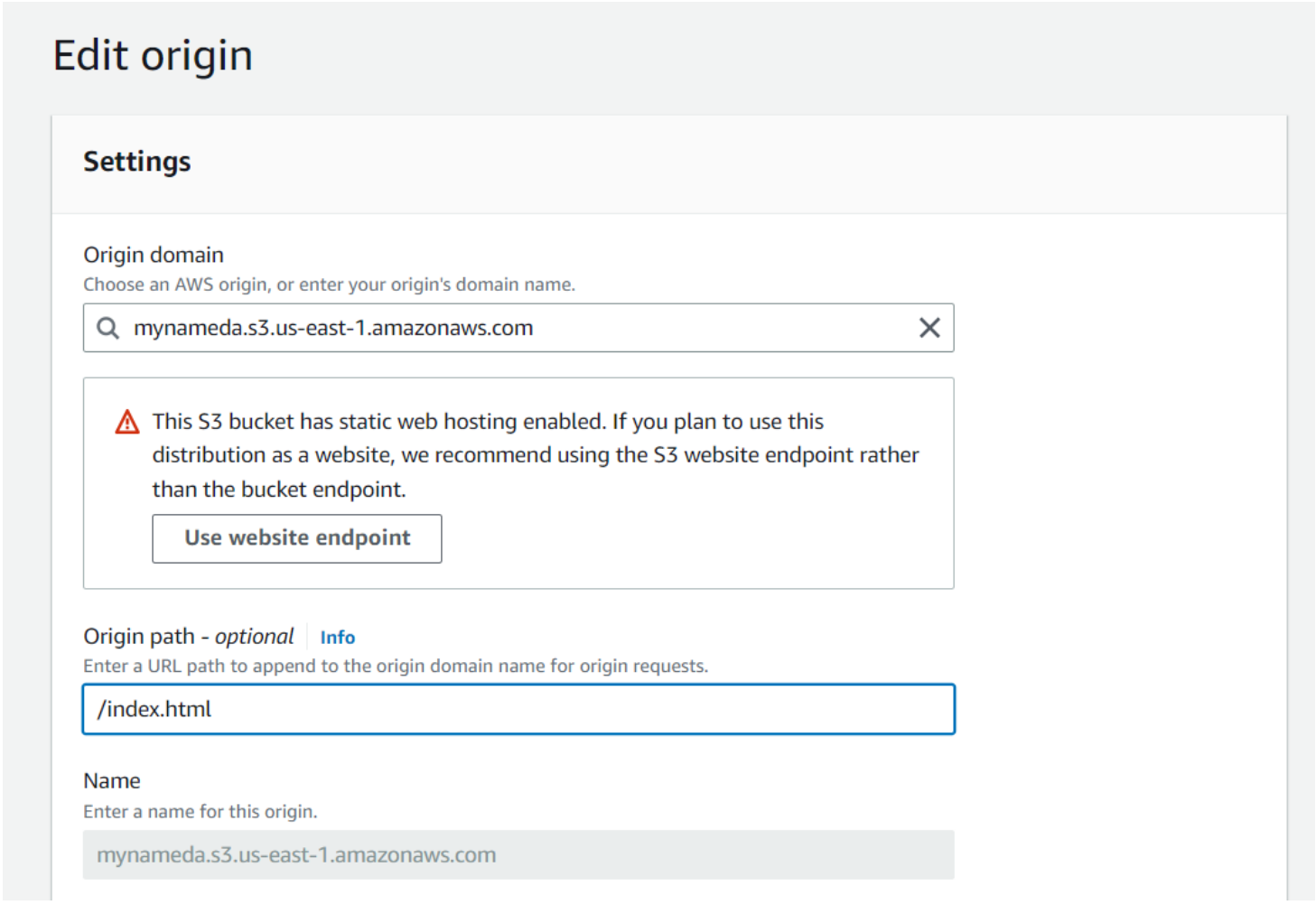
Now click on the cloudfront distribution.

Click on the URL of distribution domain name and copy it.

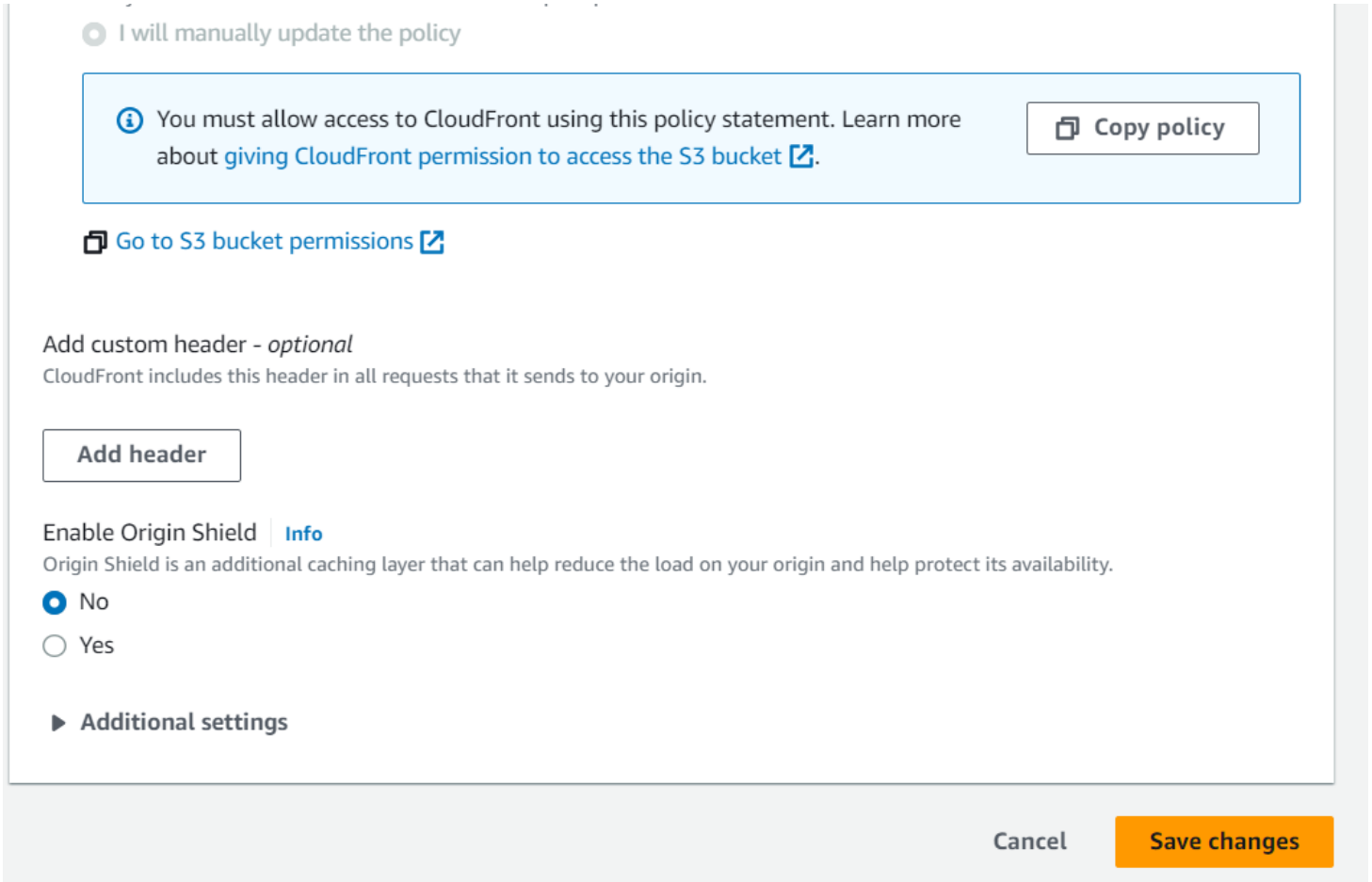
Paste the URL in a new tab.



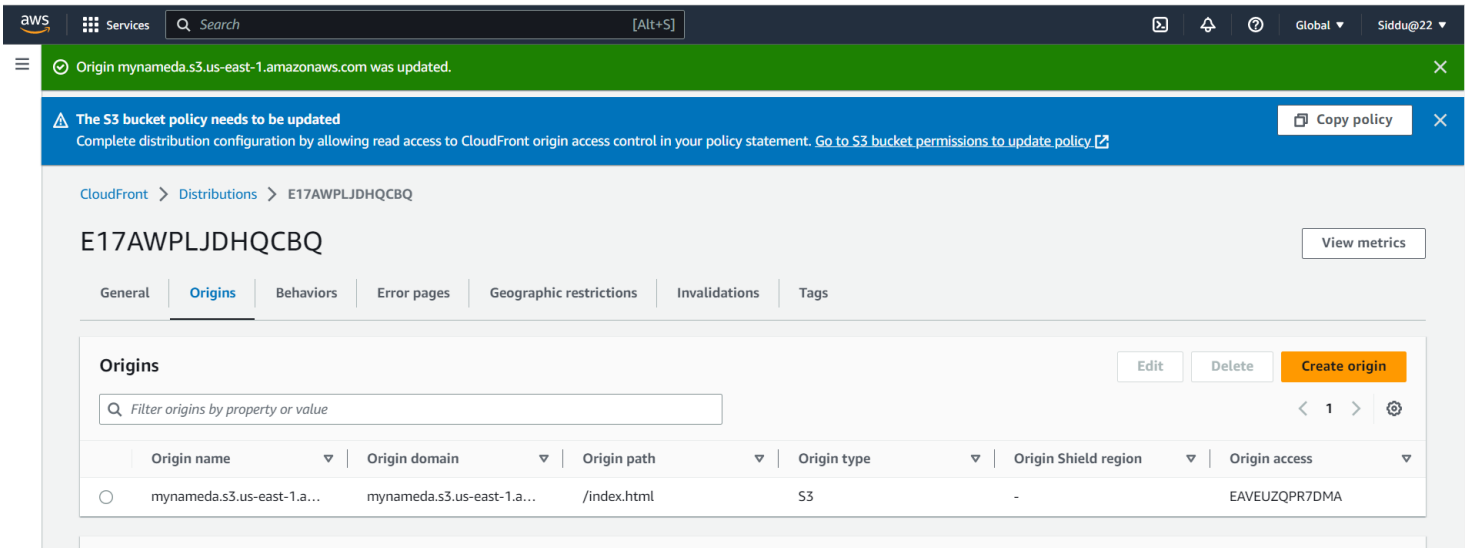
Now go to origin tab and edit the origin path into “/index.html”



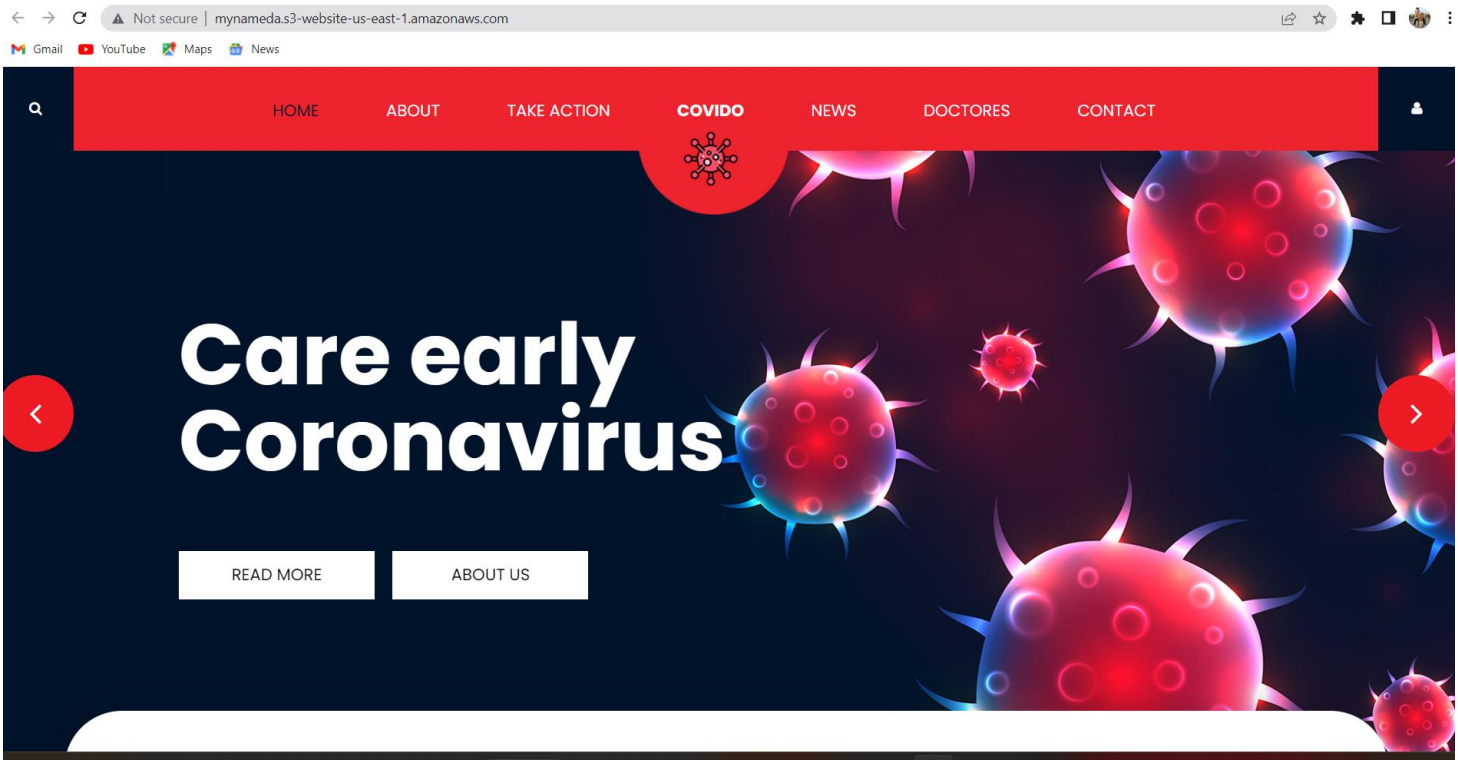
Now click on save changes



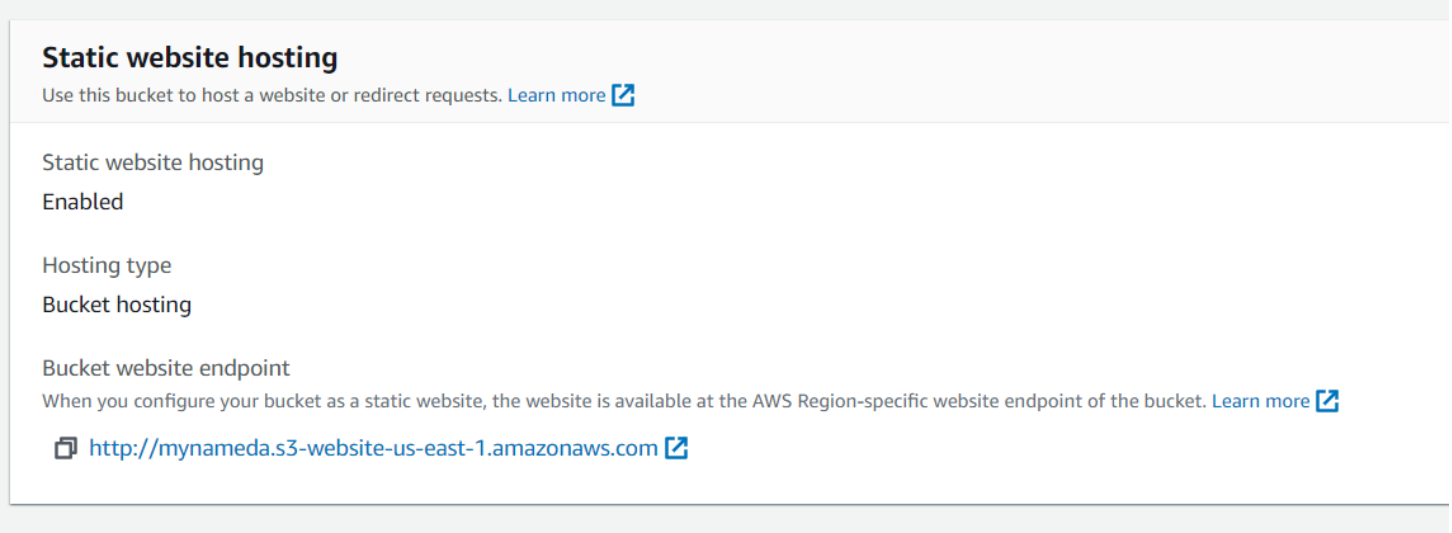
Now it will be update the origin path.



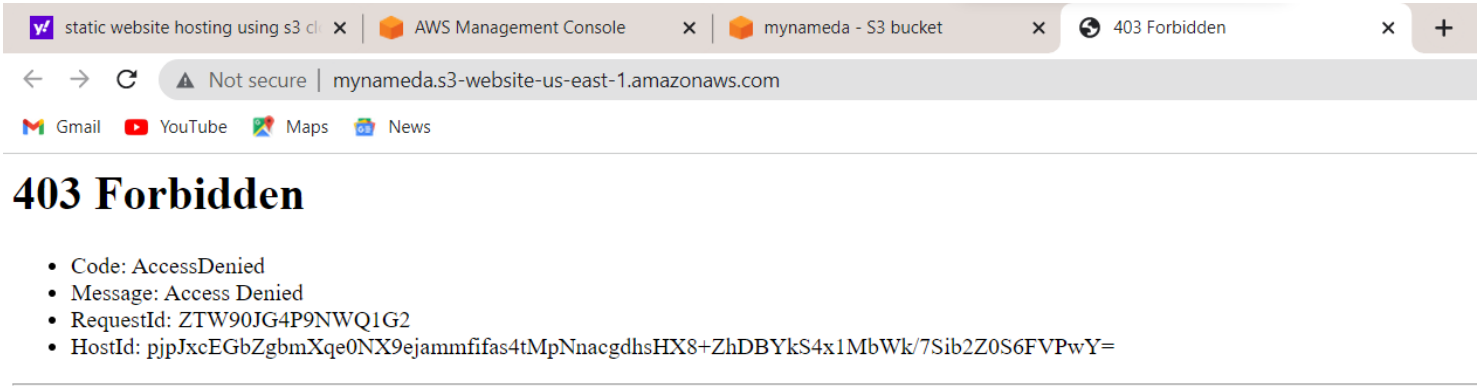
Now copy the URL and “/index.html”



Now if we open S3 bucket URL will not open.



It will show 403 forbidden error:



This are steps to launch a static website using S3 bucket cloudfront.

We can launch it in both S3 bucket as well as cloudfront.

By changing their origin paths as well the change of URl.