Static Web Hosting

In this documentation we have been discussing about the project details, Architecture Diagram, Technologies Stack and how its further implemented.

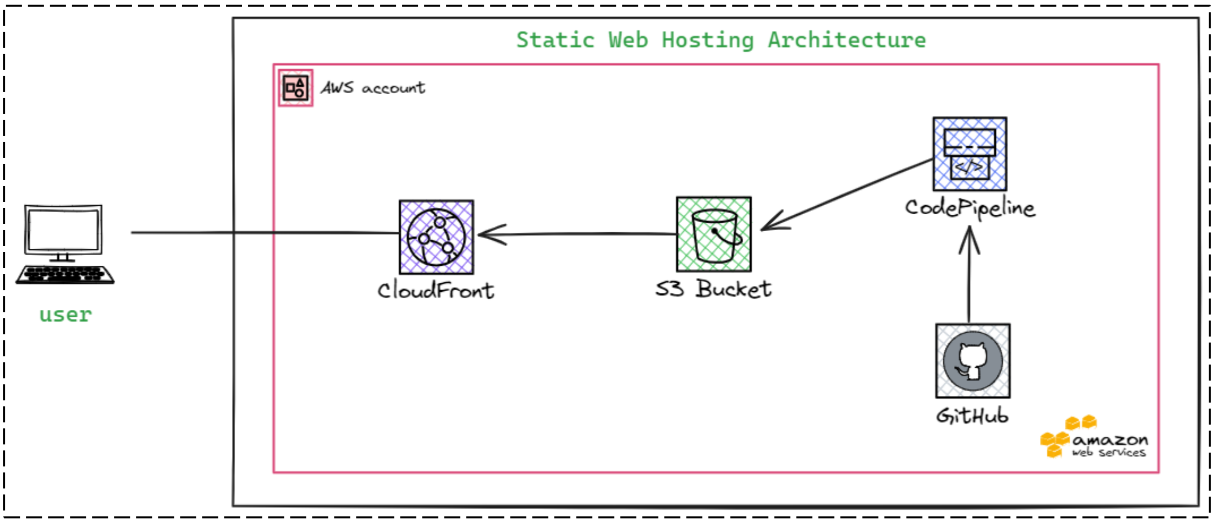
Project Details:

❖ Prerequisites: Create your free-tier AWS account.

❖ Task: Set Up a Simple Static Website on Amazon S3.

❖ Description: Create a static website hosted on Amazon S3. Create a simple portfolio website using HTML and CSS, and host it on Amazon S3. Configure the necessary buckets, enable website hosting, and upload a basic HTML/CSS website.

Architecture Design:



Portfolio Url: https://d31oejfrtk45jt.cloudfront.net/week1/index.html

Technology Stack:

- S3 Bucket
- Cloud Front
- Code Pipeline
- Git hub

Azhar Sheriff I

Why this Services Used?

Aws S3 Bucket:

S3 is Object based storage services where all the files are respected to objects only S3 supports any of files mp3,mp4,jpeg,csv,psx etc.. Its globally accessed. The role of the s3 in this project where you can store the web files like html css are stored in it without public access no one can access the bucket.

Aws Cloud front:

Cloud front is concept of CDN Content Delivery Network this service allows the user to access the files easily from where ever without buffering because its cached memory where store the data to nearest edge-location of the user. Three main benefits of using CDN Low Latency, Security, cost efficient.

AWS Code Pipeline:

Code Pipeline is a service CI/CD where its used for any updates in the website even though it's a static website. In future we can update the website without re doing the whole process.

Git Hub:

In git hub the source code of the Website have been stored in the repository.

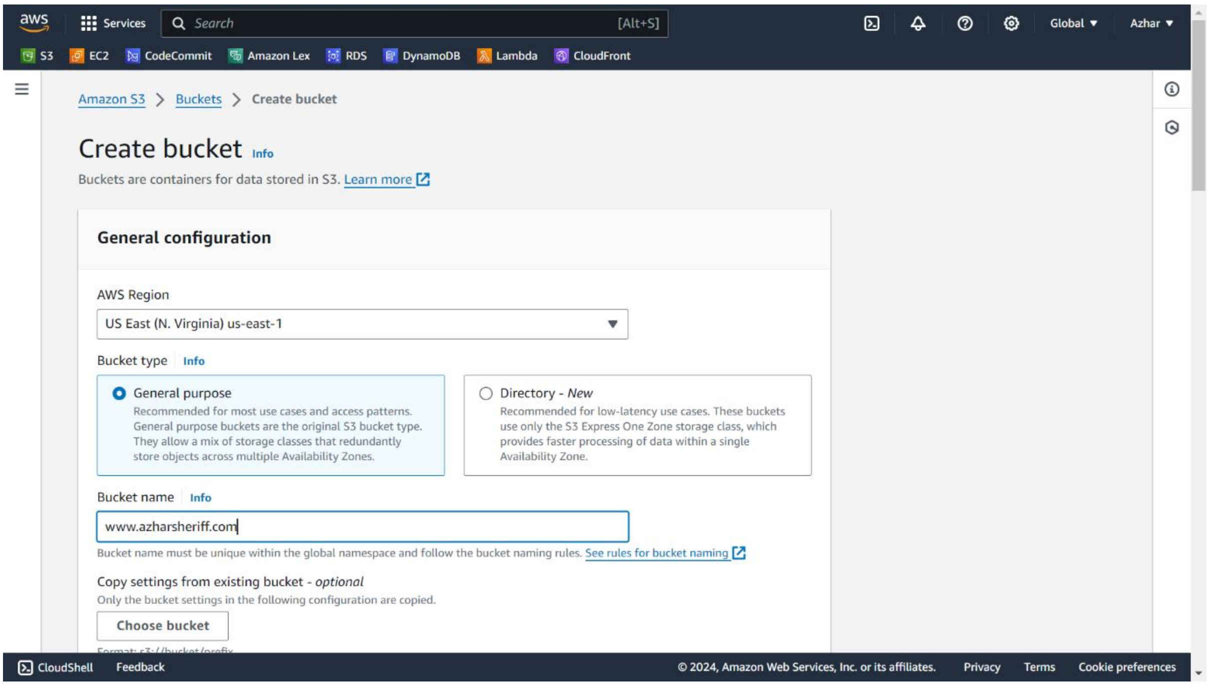
Steps of implementation:-

1. Creation of Bucket S3
2. Configuration of Code pipeline
3. Cloud front Distribution

Step1: Creating S3 Bucket

Go to Aws Console > S3 > Create bucket

Select the aws region where you want to store data, give the bucket name which is globally unique name.



aws
Services
Search [Alt+S]
Global ▾
Azhar ▾
S3 EC2 CodeCommit Amazon Lex RDS DynamoDB Lambda CloudFront
CloudShell Feedback
© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Amazon S3 > Buckets > Create bucket

Create bucket Info

Buckets are containers for data stored in S3. Learn more

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 - *New*
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

www.azharsheriff.com

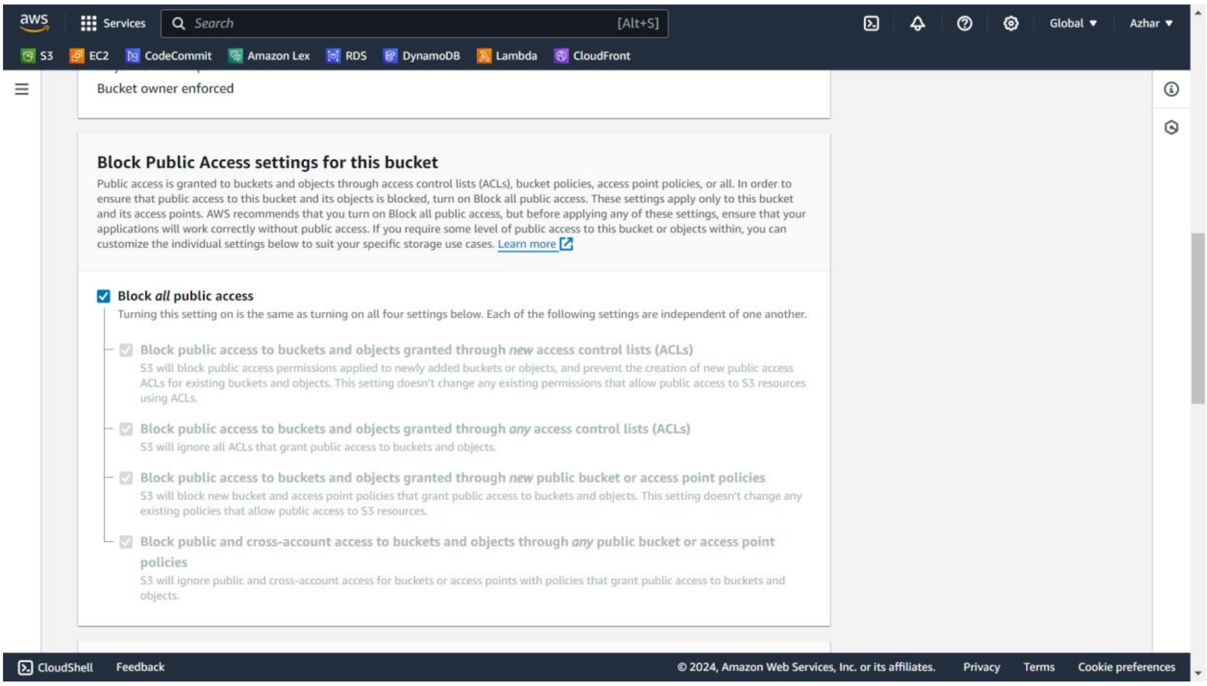
Bucket name must be unique within the global namespace and follow the bucket naming rules. See rules for bucket naming

Copy settings from existing bucket - *optional*

Only the bucket settings in the following configuration are copied.

Choose bucket

Check the all-public access has been blocked. Important point to remember.



aws
Services
Search [Alt+S]
Global ▾
Azhar ▾
S3 EC2 CodeCommit Amazon Lex RDS DynamoDB Lambda CloudFront
CloudShell Feedback
© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Bucket owner enforced

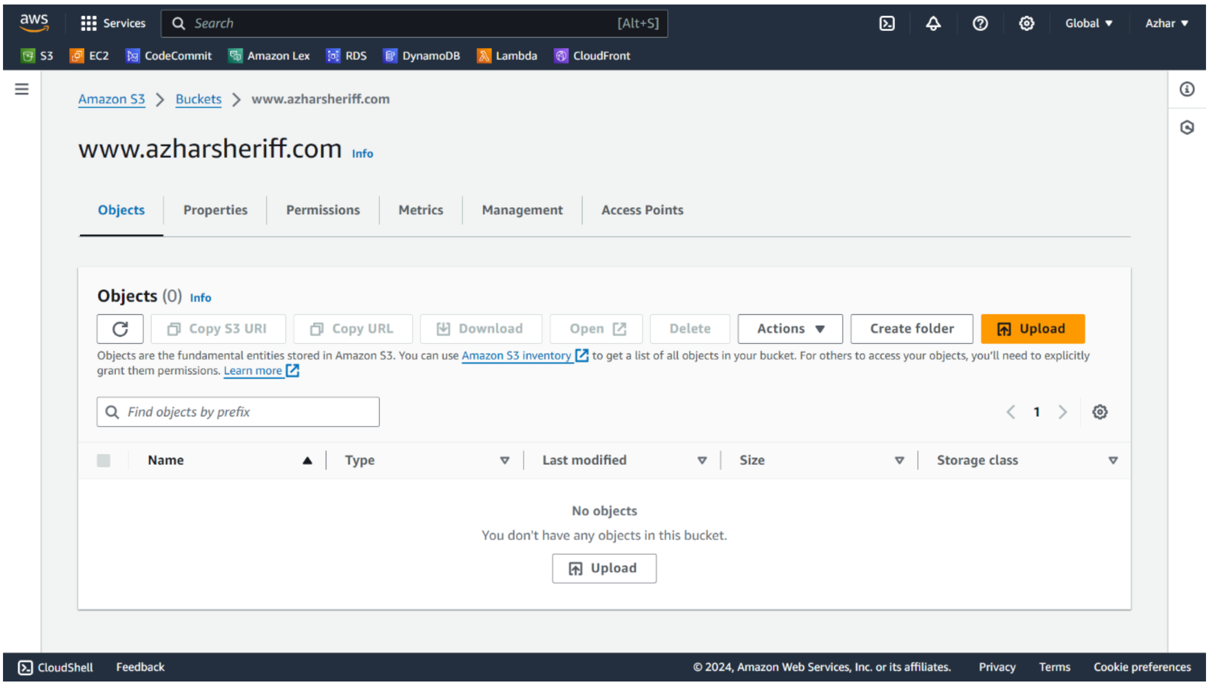
Block Public Access settings for this bucket

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.

Acknowledge whether the bucket created, for now don’t upload any objects.


aws
Services
Search [Alt+S]
Global ▾
Azhar ▾
S3 EC2 CodeCommit Amazon Lex RDS DynamoDB Lambda CloudFront
Amazon S3 > Buckets > www.azharsheriff.com

www.azharsheriff.com Info

Objects (0) 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

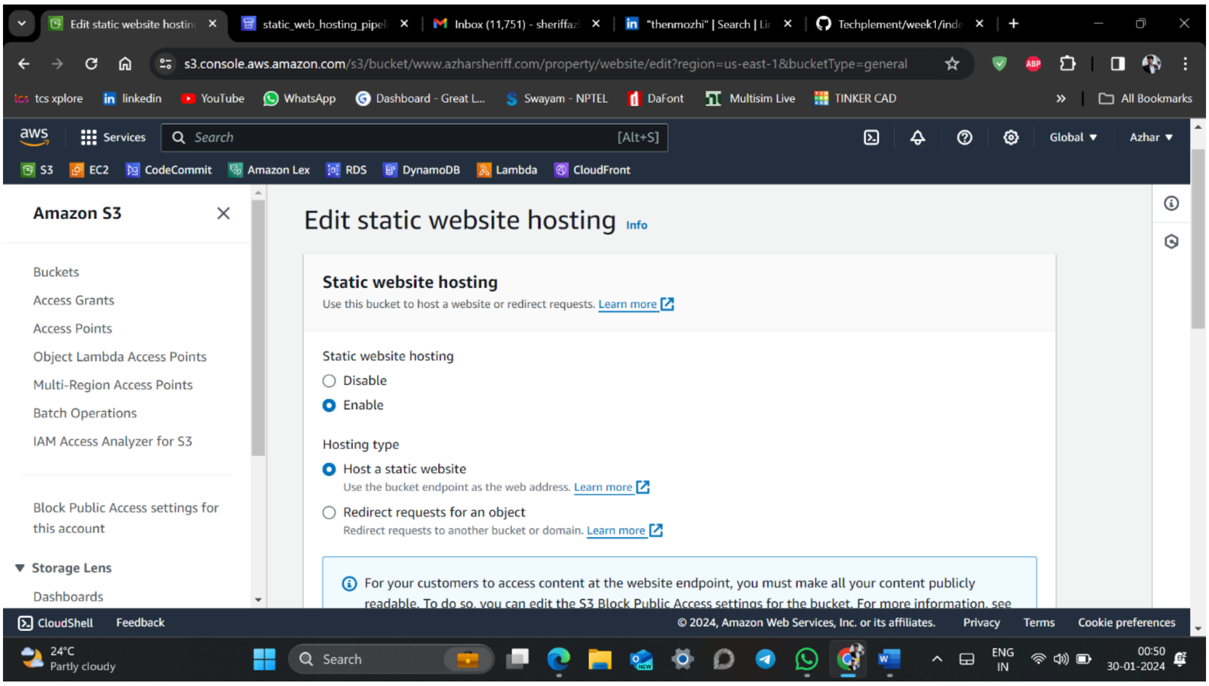
Name ▲	Type	Last modified	Size	Storage class

No objects

You don't have any objects in this bucket.

Go the specific bucket > Properties > Static web hosting

Enable the static web hosting option and give the root as your html page name like index.html and save the changes.


Edit static website hostin
static_web_hosting_pipel
Inbox (11,751) - sheriffa
"thenmozhi" | Search | Li
Techplement/week1/inde
s3.console.aws.amazon.com/s3/bucket/www.azharsheriff.com/property/website/edit?region=us-east-1&bucketType=general
tcs xplore
linkedin
YouTube
WhatsApp
Dashboard - Great L...
Swayam - NPTEL
DaFont
Multisim Live
TINKER CAD
All Bookmarks
aws
Services
Search [Alt+S]
Global ▾
Azhar ▾
S3 EC2 CodeCommit Amazon Lex RDS DynamoDB Lambda CloudFront
Amazon S3
Buckets
Access Grants
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
▼ Storage Lens
Dashboards

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

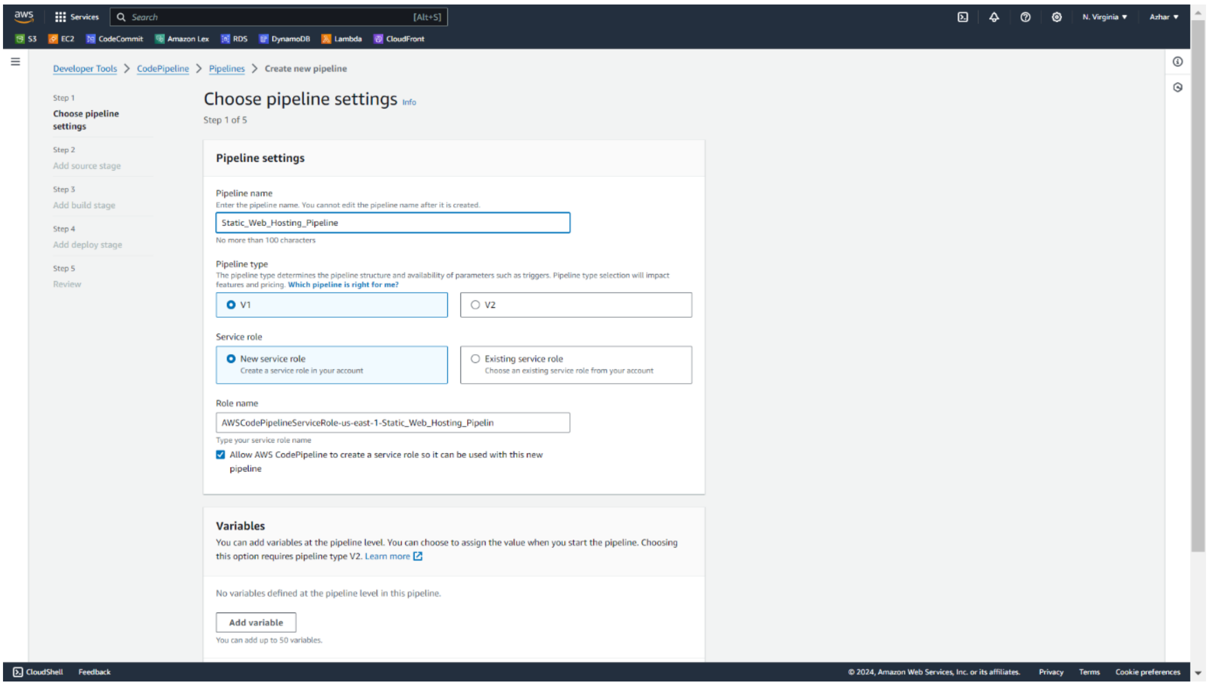
Redirect requests to another bucket or domain. Learn more

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

Step 2: Code Pipeline Configuration

Aws Console > Code Pipeline > Create

Give the pipeline name, select the v1.Click Next



Developer Tools > CodePipeline > Pipelines > Create new pipeline

Step 1 Choose pipeline settings

Step 2 Add source stage

Step 3 Add build stage

Step 4 Add deploy stage

Step 5 Review

Choose pipeline settings Info

Step 1 of 5

Pipeline settings

Pipeline name

Enter the pipeline name. You cannot edit the pipeline name after it is created.

Static_Web_Hosting_Pipeline

No more than 100 characters

Pipeline type

The pipeline type determines the pipeline structure and availability of parameters such as triggers. Pipeline type selection will impact features and pricing. Which pipeline is right for me?

● V1 ○ V2

Service role

● New service role
Create a service role in your account

○ Existing service role
Choose an existing service role from your account

Role name

AWSCodePipelineServiceRole-us-east-1-Static_Web_Hosting_Pipelin

Type your service role name

☑ Allow AWS CodePipeline to create a service role so it can be used with this new pipeline

Variables

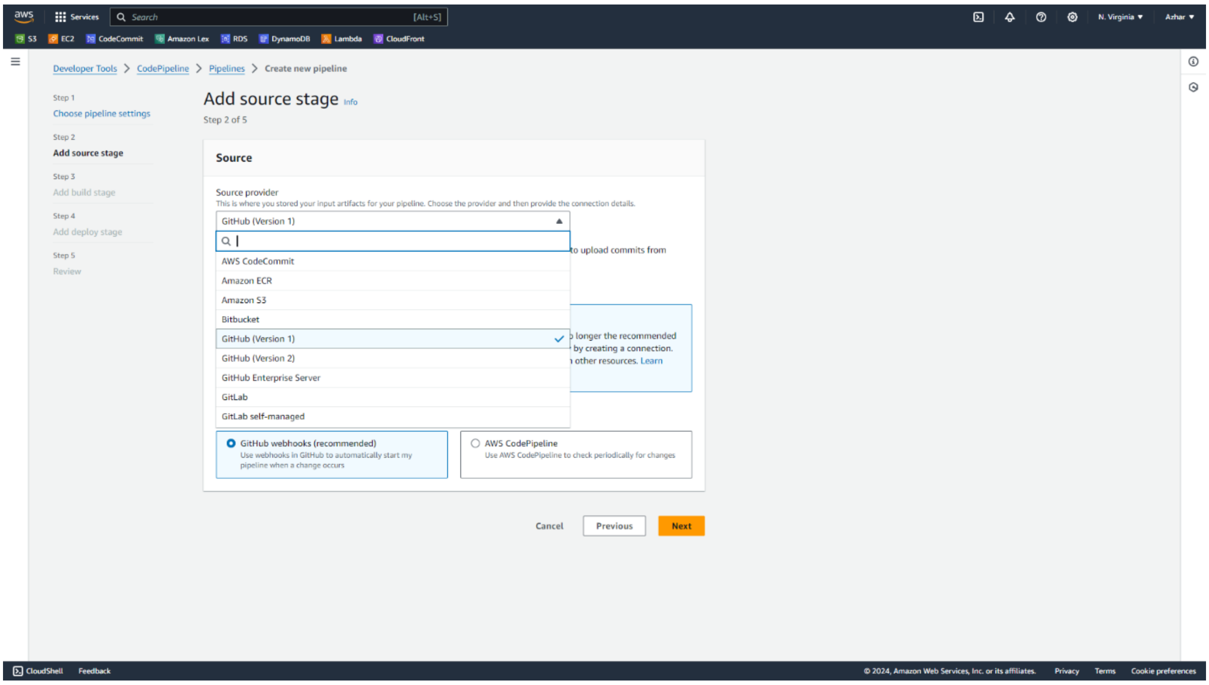
You can add variables at the pipeline level. You can choose to assign the value when you start the pipeline. Choosing this option requires pipeline type V2. Learn more

No variables defined at the pipeline level in this pipeline.

Add variable

You can add up to 50 variables.

Click the source as github version1. Click the connect to github option.



Developer Tools > CodePipeline > Pipelines > Create new pipeline

Step 1 Choose pipeline settings

Step 2 Add source stage

Step 3 Add build stage

Step 4 Add deploy stage

Step 5 Review

Add source stage Info

Step 2 of 5

Source

Source provider

This is where you stored your input artifacts for your pipeline. Choose the provider and then provide the connection details.

GitHub (Version 1)

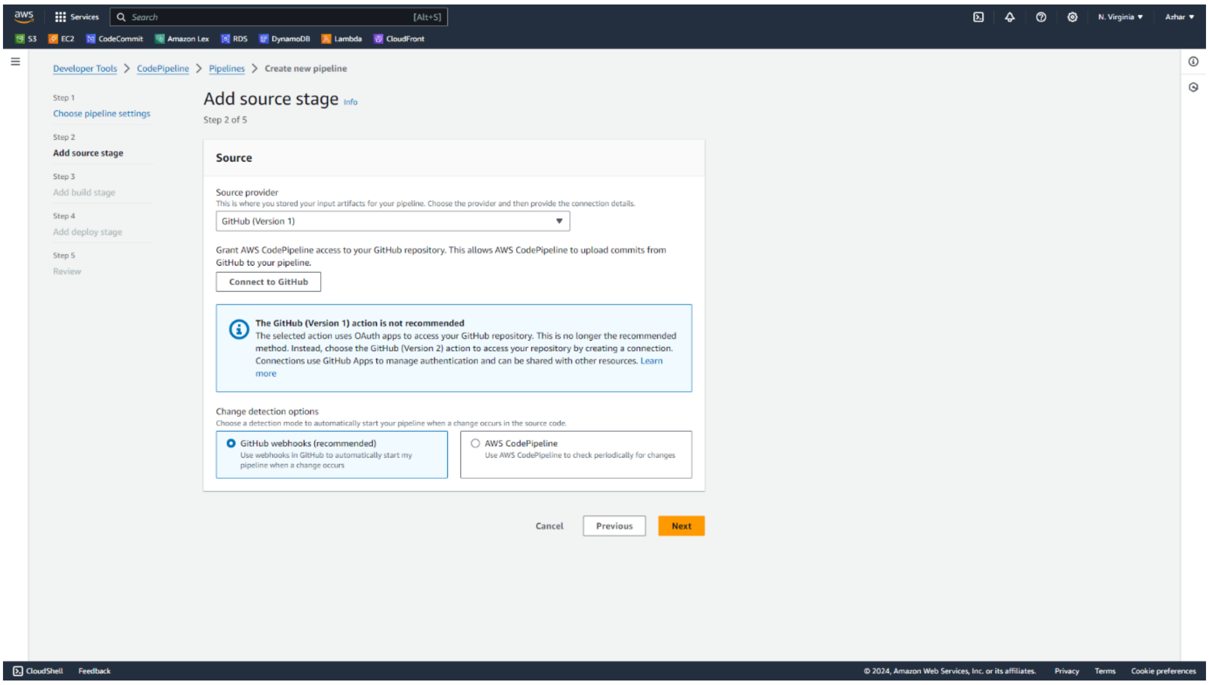
- AWS CodeCommit
- Amazon ECR
- Amazon S3
- Bitbucket
- GitHub (Version 1) ✓
- GitHub (Version 2)
- GitHub Enterprise Server
- GitLab
- GitLab self-managed

to upload commits from

longer the recommended by creating a connection. other resources. Learn

● GitHub webhooks (recommended)
Use webhooks in GitHub to automatically start my pipeline when a change occurs

○ AWS CodePipeline
Use AWS CodePipeline to check periodically for changes



Developer Tools > CodePipeline > Pipelines > Create new pipeline

Step 1 Choose pipeline settings
Step 2 Add source stage
Step 3 Add build stage
Step 4 Add deploy stage
Step 5 Review

Add source stage

Step 2 of 5

Source

Source provider
This is where you stored your input artifacts for your pipeline. Choose the provider and then provide the connection details.
GitHub (Version 1)

Grant AWS CodePipeline access to your GitHub repository. This allows AWS CodePipeline to upload commits from GitHub to your pipeline.

Connect to GitHub

The GitHub (Version 1) action is not recommended
The selected action uses OAuth apps to access your GitHub repository. This is no longer the recommended method. Instead, choose the GitHub (Version 2) action to access your repository by creating a connection. Connections use GitHub Apps to manage authentication and can be shared with other resources. Learn more

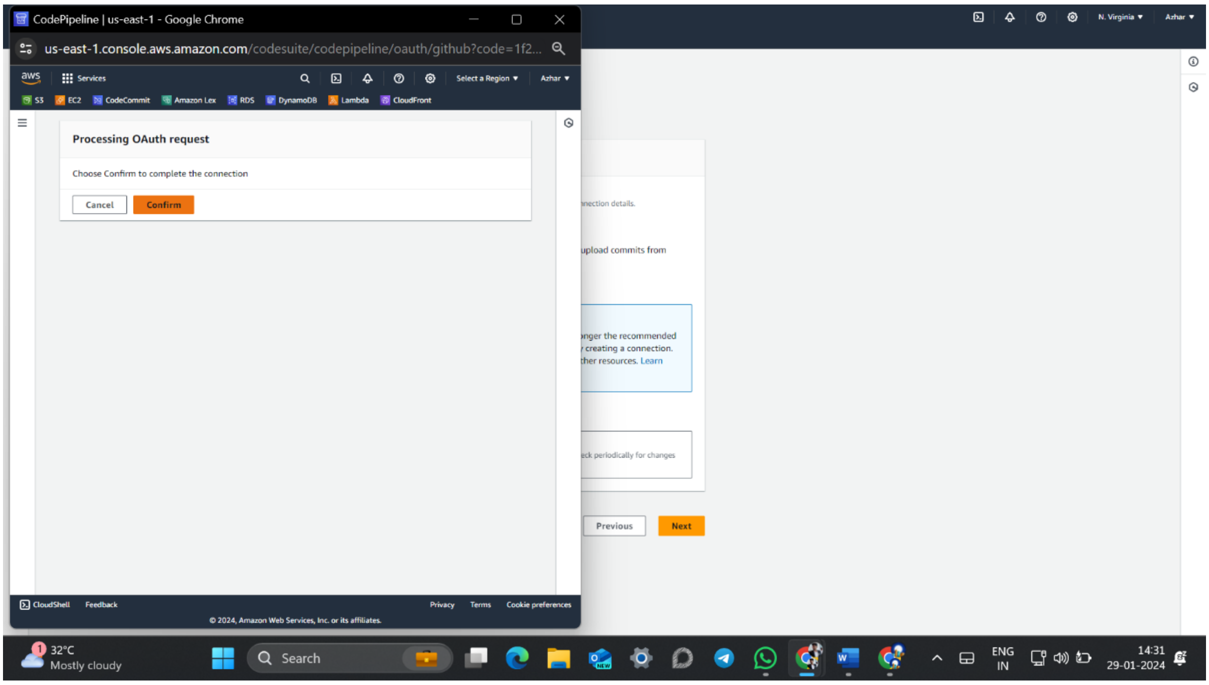
Change detection options
Choose a detection mode to automatically start your pipeline when a change occurs in the source code.

● GitHub webhooks (recommended)
Use webhooks in GitHub to automatically start my pipeline when a change occurs

○ AWS CodePipeline
Use AWS CodePipeline to check periodically for changes

Cancel | Previous | Next

Click confirm option.



CodePipeline | us-east-1 - Google Chrome
us-east-1.console.aws.amazon.com/codesuite/codepipeline/oauth/github?code=1f2...

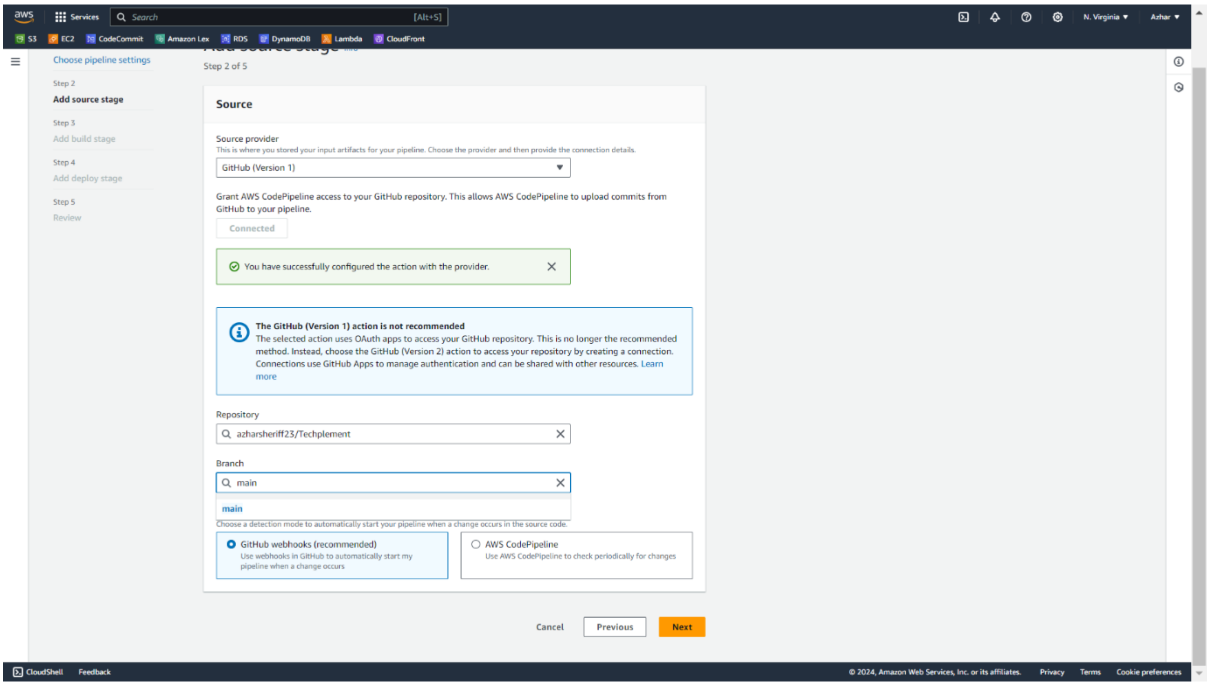
Processing OAuth request

Choose Confirm to complete the connection

Cancel | Confirm

After confirming, the repository are can be access by the aws account you can select the directory which you want.

Azhar Sheriff I



Step 2 of 5

Source

Source provider
This is where you stored your input artifacts for your pipeline. Choose the provider and then provide the connection details.
GitHub (Version 1)

Grant AWS CodePipeline access to your GitHub repository. This allows AWS CodePipeline to upload commits from GitHub to your pipeline.

You have successfully configured the action with the provider.

The GitHub (Version 1) action is not recommended
The selected action uses OAuth apps to access your GitHub repository. This is no longer the recommended method. Instead, choose the GitHub (Version 2) action to access your repository by creating a connection. Connections use GitHub Apps to manage authentication and can be shared with other resources. Learn more

Repository: azharsheriff23/Techplement

Branch: main

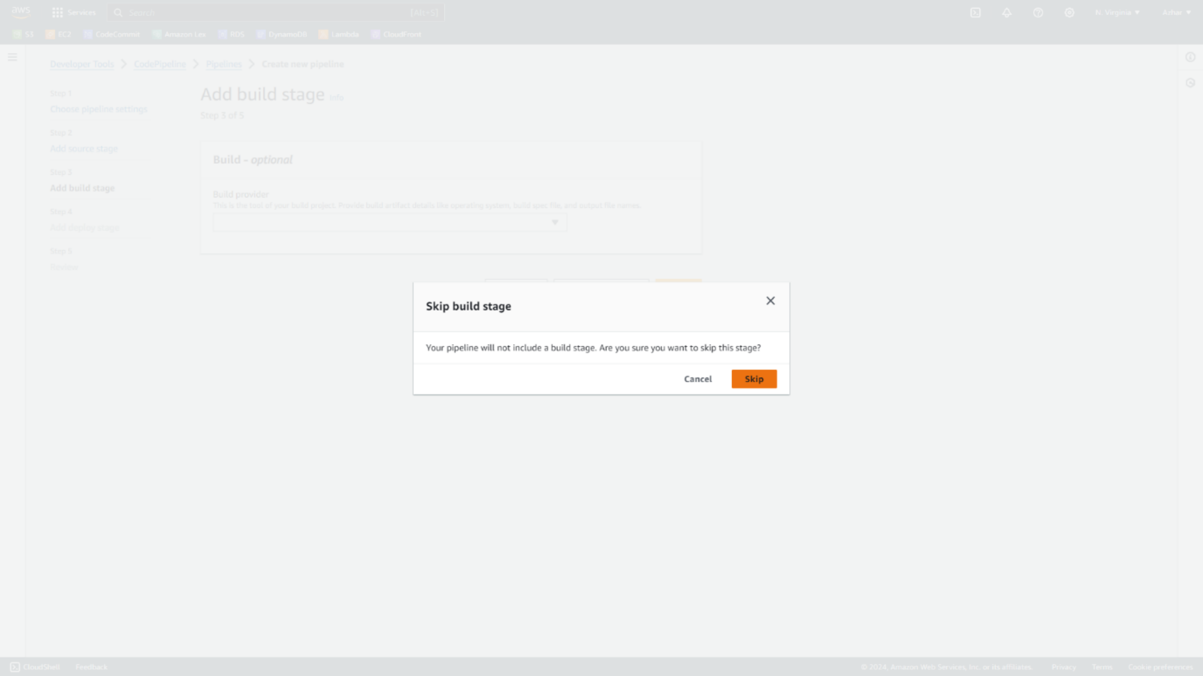
Choose a detection mode to automatically start your pipeline when a change occurs in the source code.

● GitHub webhooks (recommended)
Use webhooks in GitHub to automatically start my pipeline when a change occurs

○ AWS CodePipeline
Use AWS CodePipeline to check periodically for changes

Click the branch as main

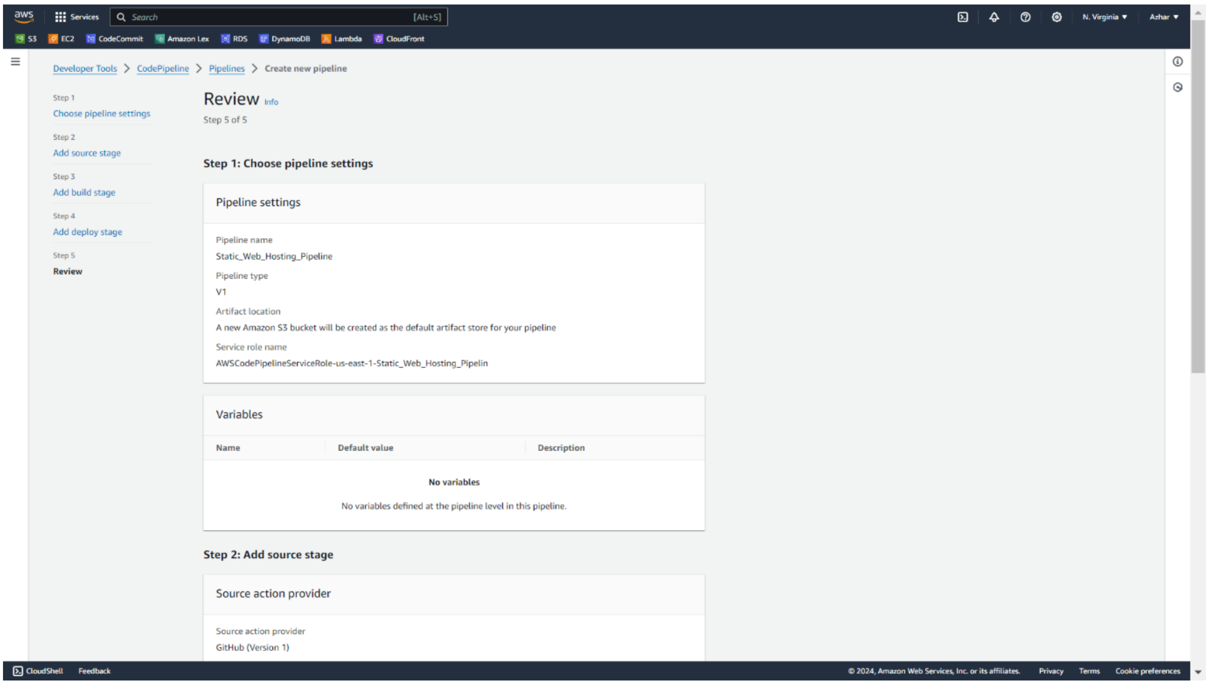
Skip the build stage process for now. In deployment stage select the s3 bucket to store the data files.



Skip build stage

Your pipeline will not include a build stage. Are you sure you want to skip this stage?

Review the Process:



Developer Tools > CodePipeline > Pipelines > Create new pipeline

Step 1
Choose pipeline settings
Step 2
Add source stage
Step 3
Add build stage
Step 4
Add deploy stage
Step 5
Review

Review Info

Step 5 of 5

Step 1: Choose pipeline settings

Pipeline settings

Pipeline name
Static_Web_Hosting_Pipeline

Pipeline type
V1

Artifact location
A new Amazon S3 bucket will be created as the default artifact store for your pipeline

Service role name
AWSCodePipelineServiceRole-us-east-1-Static_Web_Hosting_Pipelin

Variables

Name	Default value	Description

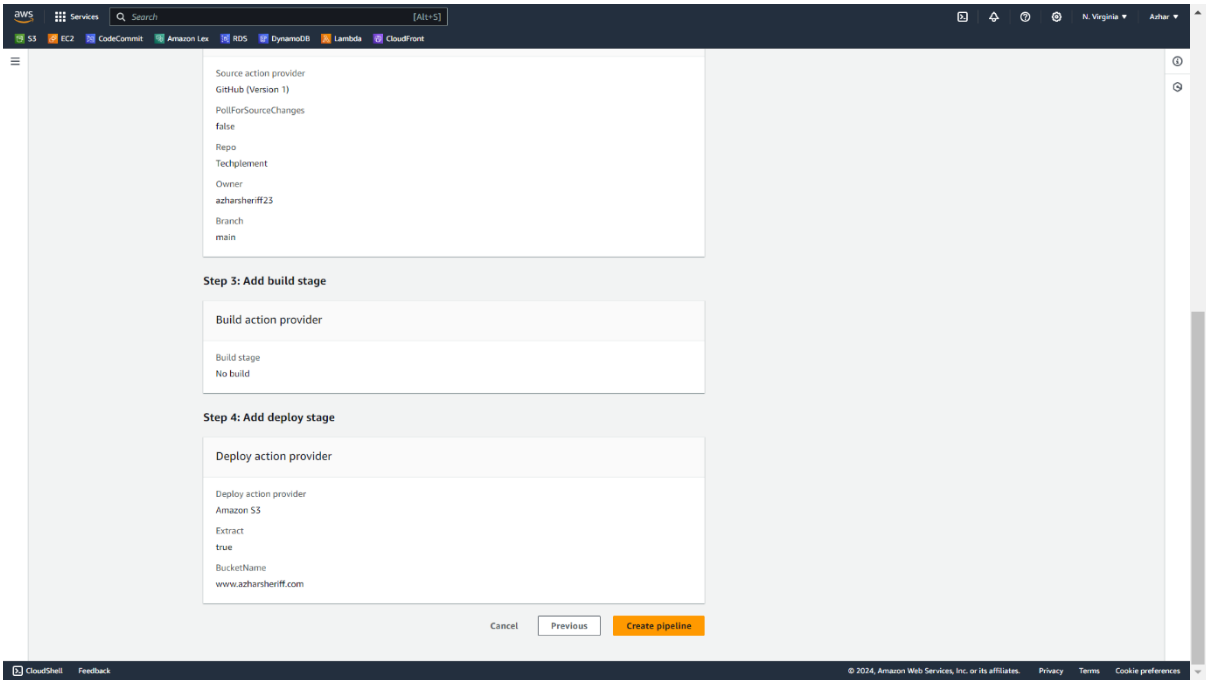
No variables

No variables defined at the pipeline level in this pipeline.

Step 2: Add source stage

Source action provider

Source action provider
GitHub (Version 1)



Source action provider
GitHub (Version 1)

PollForSourceChanges
false

Repo
Techplement

Owner
azharsheriff23

Branch
main

Step 3: Add build stage

Build action provider

Build stage
No build

Step 4: Add deploy stage

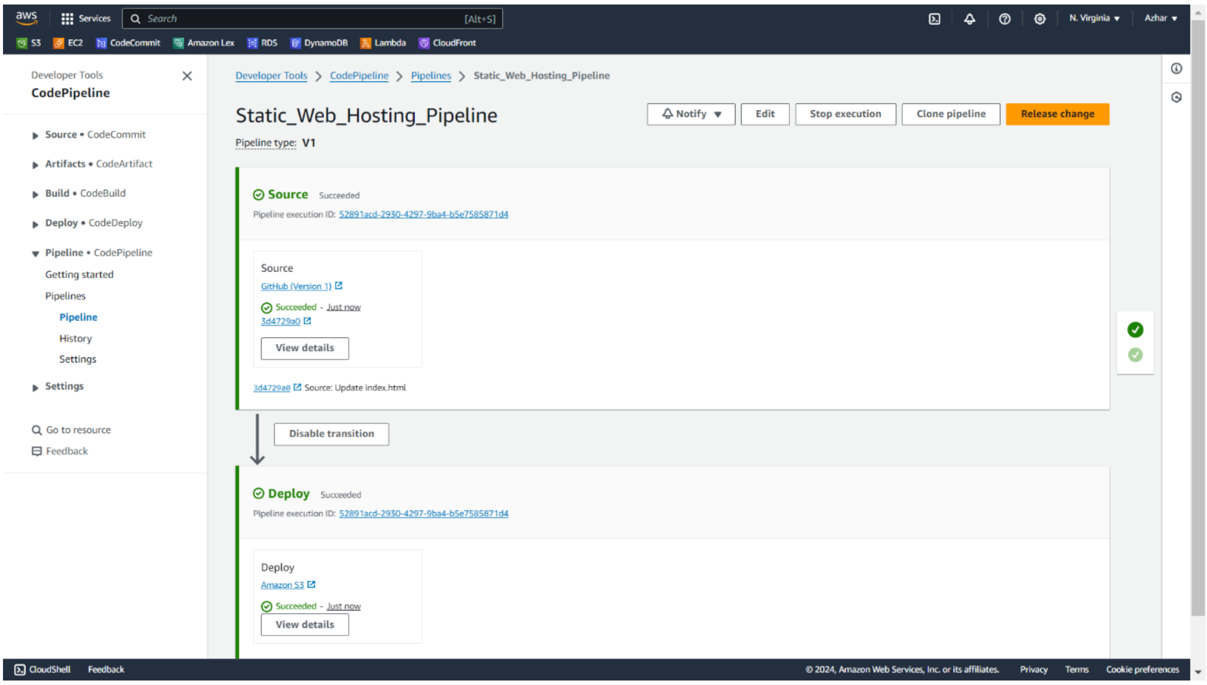
Deploy action provider

Deploy action provider
Amazon S3

Extract
true

BucketName
www.azharsheriff.com

After successfully creating the bucket, you can see this.



Developer Tools > CodePipeline > Pipelines > Static_Web_Hosting_Pipeline

Static_Web_Hosting_Pipeline

Pipeline type: V1

Source Succeeded

Pipeline execution ID: 52891acd-2930-4297-9ba4-b5e7585871d4

Source

GitHub (Version 1)

Succeeded - Just now

3d4729a0

3d4729a0 Source: Update index.html

Deploy Succeeded

Pipeline execution ID: 52891acd-2930-4297-9ba4-b5e7585871d4

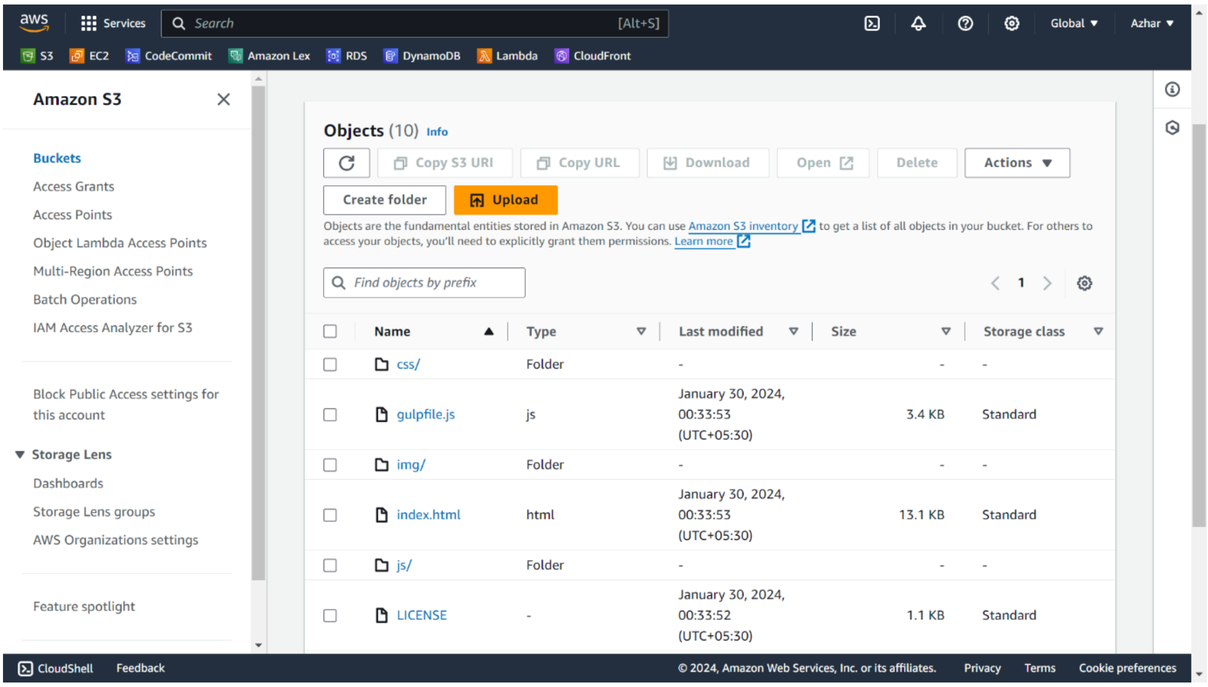
Deploy

Amazon S3

Succeeded - Just now

© 2024, Amazon Web Services, Inc. or its affiliates.

Now You can check the s3 bucket the objects are automatically uploaded in bucket.



Objects (10)

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

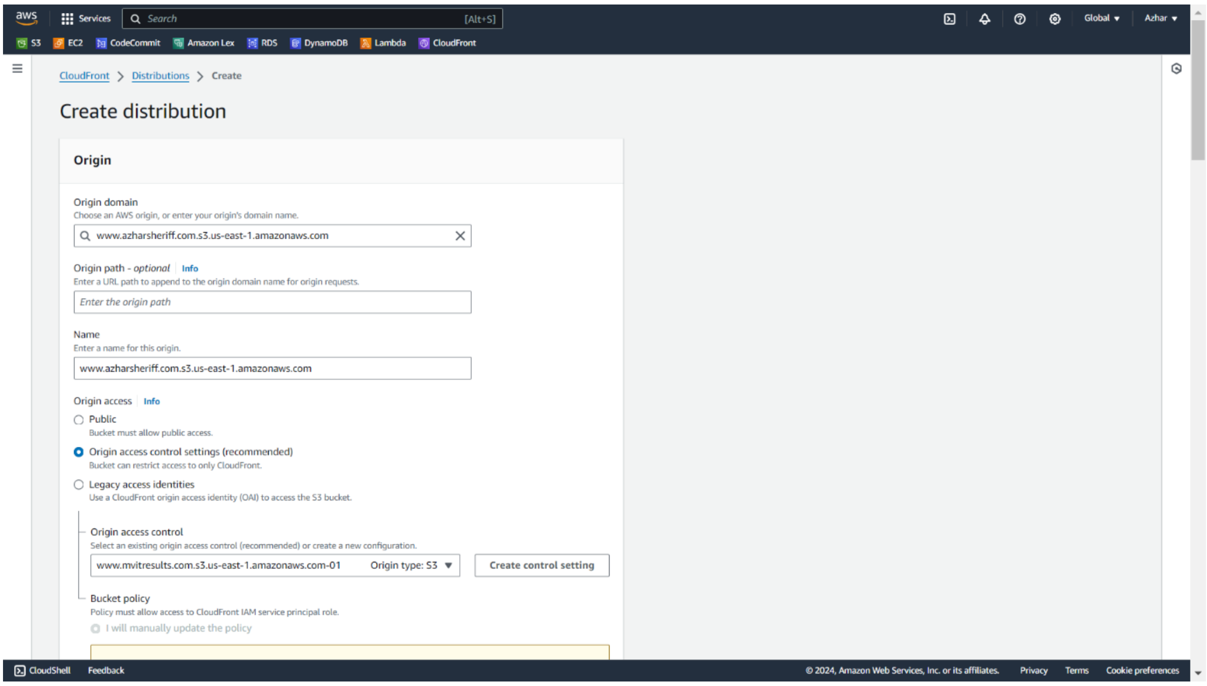
□	Name	Type	Last modified	Size	Storage class
□	css/	Folder	-	-	-
□	gulpfile.js	js	January 30, 2024, 00:33:53 (UTC+05:30)	3.4 KB	Standard
□	img/	Folder	-	-	-
□	index.html	html	January 30, 2024, 00:33:53 (UTC+05:30)	13.1 KB	Standard
□	js/	Folder	-	-	-
□	LICENSE	-	January 30, 2024, 00:33:52 (UTC+05:30)	1.1 KB	Standard

© 2024, Amazon Web Services, Inc. or its affiliates.

Step3: Cloud front Creation

Aws console > Cloud Front > Create Distribution

Select the origin domain from where you want to fetch the data and select the correct resource.



CloudFront > Distributions > Create

Create distribution

Origin

Origin domain
Choose an AWS origin, or enter your origin's domain name.
www.azharsheriff.com.s3.us-east-1.amazonaws.com

Origin path - *optional* Info
Enter a URL path to append to the origin domain name for origin requests.
Enter the origin path

Name
Enter a name for this origin.
www.azharsheriff.com.s3.us-east-1.amazonaws.com

Origin access Info

○ Public
Bucket must allow public access.

● Origin access control settings (recommended)
Bucket can restrict access to only CloudFront.

○ Legacy access identities
Use a CloudFront origin access identity (OAI) to access the S3 bucket.

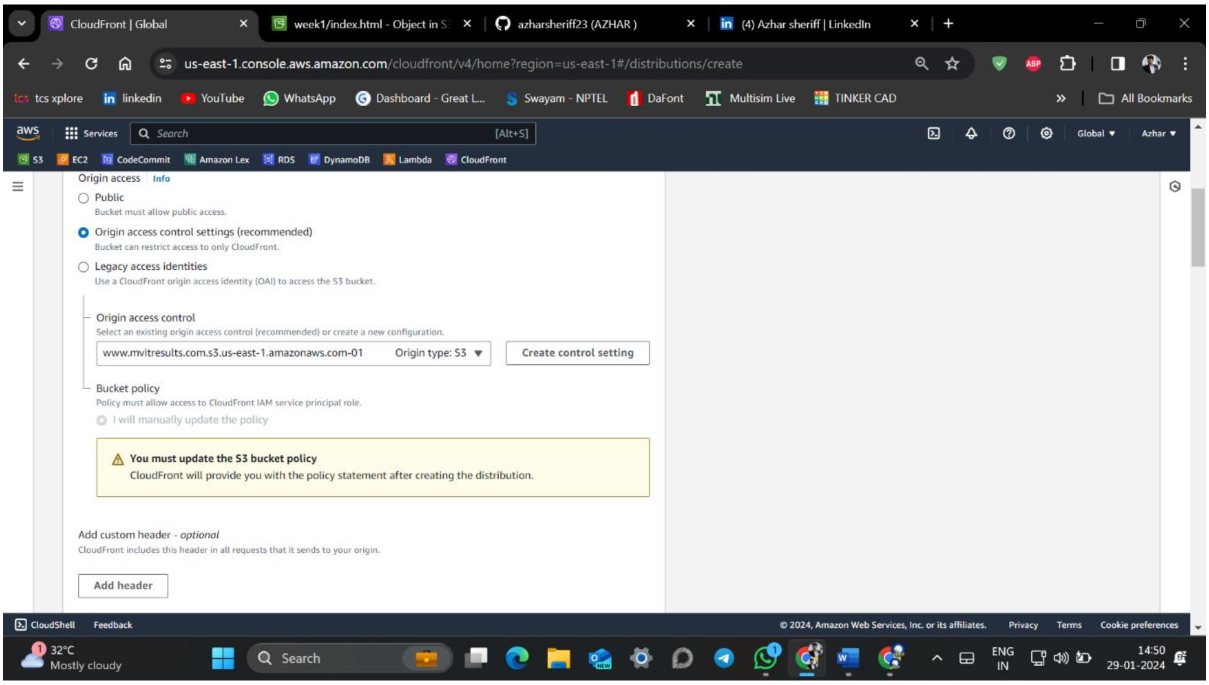
Origin access control
Select an existing origin access control (recommended) or create a new configuration.
www.mvitresults.com.s3.us-east-1.amazonaws.com-01 Origin type: S3

Bucket policy
Policy must allow access to CloudFront IAM service principal role.
○ I will manually update the policy

Origin Access:

Select the origin access should be Origin access control settings (or) legacy access identifiers. Should not be public.

Its important step where you want to update the bucket policy also.



us-east-1.console.aws.amazon.com/cloudfront/v4/home?region=us-east-1#/distributions/create

Origin access Info

○ Public
Bucket must allow public access.

● Origin access control settings (recommended)
Bucket can restrict access to only CloudFront.

○ Legacy access identities
Use a CloudFront origin access identity (OAI) to access the S3 bucket.

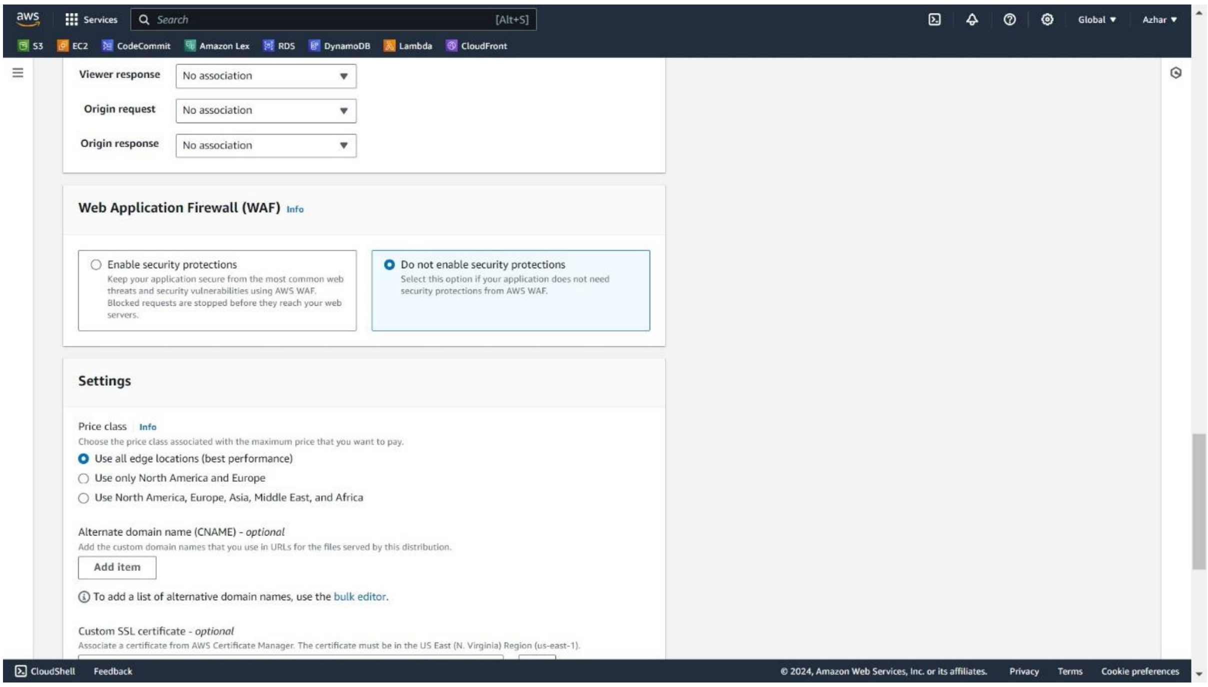
Origin access control
Select an existing origin access control (recommended) or create a new configuration.
www.mvitresults.com.s3.us-east-1.amazonaws.com-01 Origin type: S3

Bucket policy
Policy must allow access to CloudFront IAM service principal role.
○ I will manually update the policy

⚠ **You must update the S3 bucket policy**
CloudFront will provide you with the policy statement after creating the distribution.

Add custom header - *optional*
CloudFront includes this header in all requests that it sends to your origin.

Do the following Configuration:



Viewer response: No association

Origin request: No association

Origin response: No association

Web Application Firewall (WAF) Info

○ Enable security protections
Keep your application secure from the most common web threats and security vulnerabilities using AWS WAF. Blocked requests are stopped before they reach your web servers.

● Do not enable security protections
Select this option if your application does not need security protections from AWS WAF.

Settings

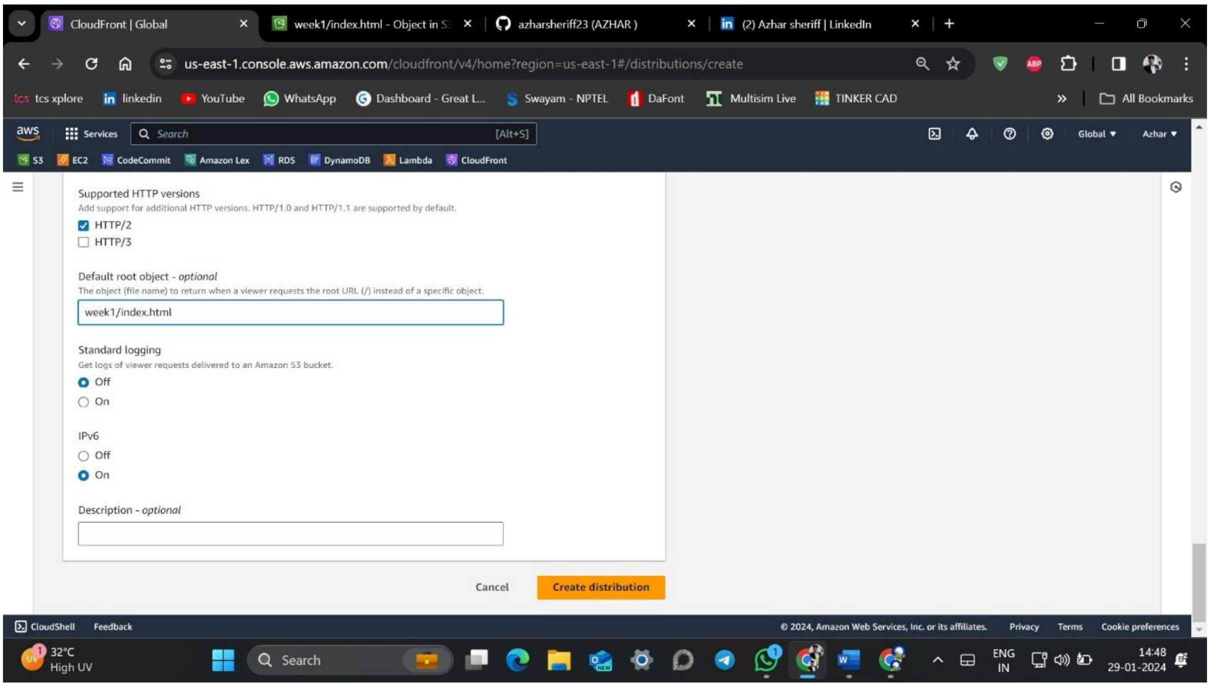
Price class Info
Choose the price class associated with the maximum price that you want to pay.
● Use all edge locations (best performance)
○ Use only North America and Europe
○ Use North America, Europe, Asia, Middle East, and Africa

Alternate domain name (CNAME) - *optional*
Add the custom domain names that you use in URLs for the files served by this distribution.
Add item

ⓘ To add a list of alternative domain names, use the bulk editor.

Custom SSL certificate - *optional*
Associate a certificate from AWS Certificate Manager. The certificate must be in the US East (N. Virginia) Region (us-east-1).

Set the default root object of the object where its stored and click create Distribution.



us-east-1.console.aws.amazon.com/cloudfront/v4/home?region=us-east-1#/distributions/create

Supported HTTP versions
Add support for additional HTTP versions. HTTP/1.0 and HTTP/1.1 are supported by default.
☑ HTTP/2
□ HTTP/3

Default root object - *optional*
The object (file name) to return when a viewer requests the root URL (/) instead of a specific object.
week1/index.html

Standard logging
Get logs of viewer requests delivered to an Amazon S3 bucket.
● Off
○ On

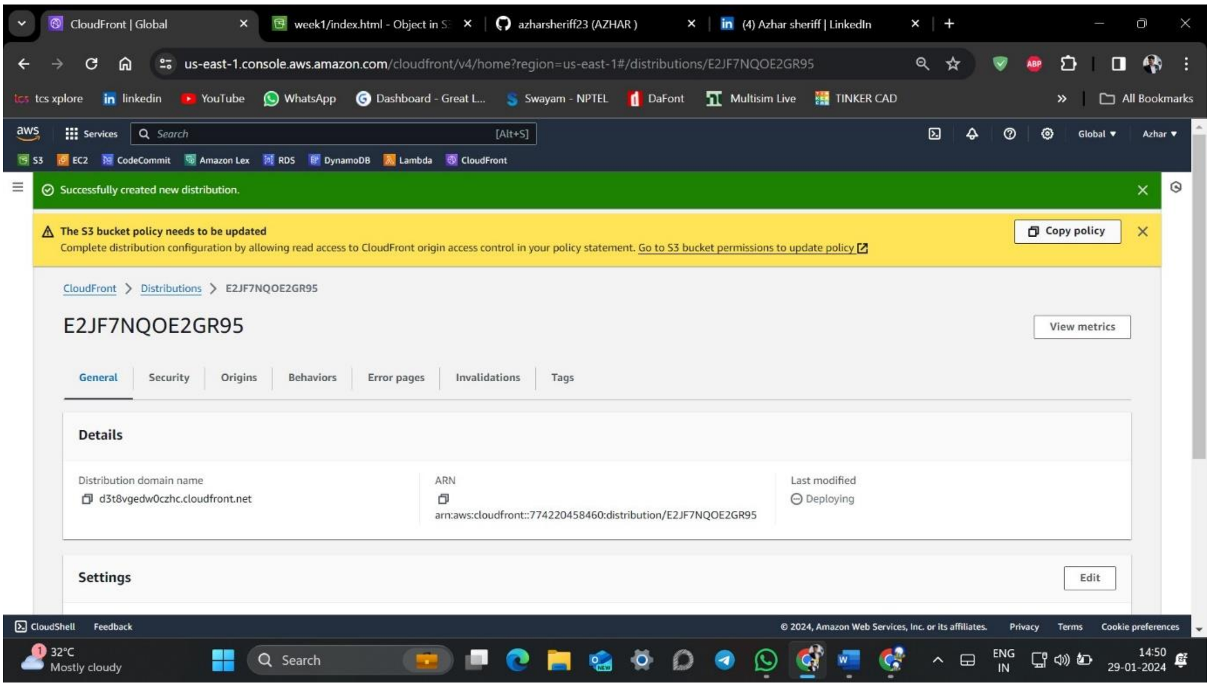
IPv6
○ Off
● On

Description - *optional*

Cancel | Create distribution

Azhar Sheriff I

Copy the bucket policy and paste in the s3 bucket:


CloudFront | Global
week1/index.html - Object in S
azharsheriff23 (AZHAR)
(4) Azhar sheriff | LinkedIn
us-east-1.console.aws.amazon.com/cloudfront/v4/home?region=us-east-1#/distributions/E2JF7NQOE2GR95
Services
Search
S3
EC2
CodeCommit
Amazon Lex
RDS
DynamoDB
Lambda
CloudFront
Global
Azhar

Successfully created new distribution.

The S3 bucket policy needs to be updated
Complete distribution configuration by allowing read access to CloudFront origin access control in your policy statement. Go to S3 bucket permissions to update policy

E2JF7NQOE2GR95

Details

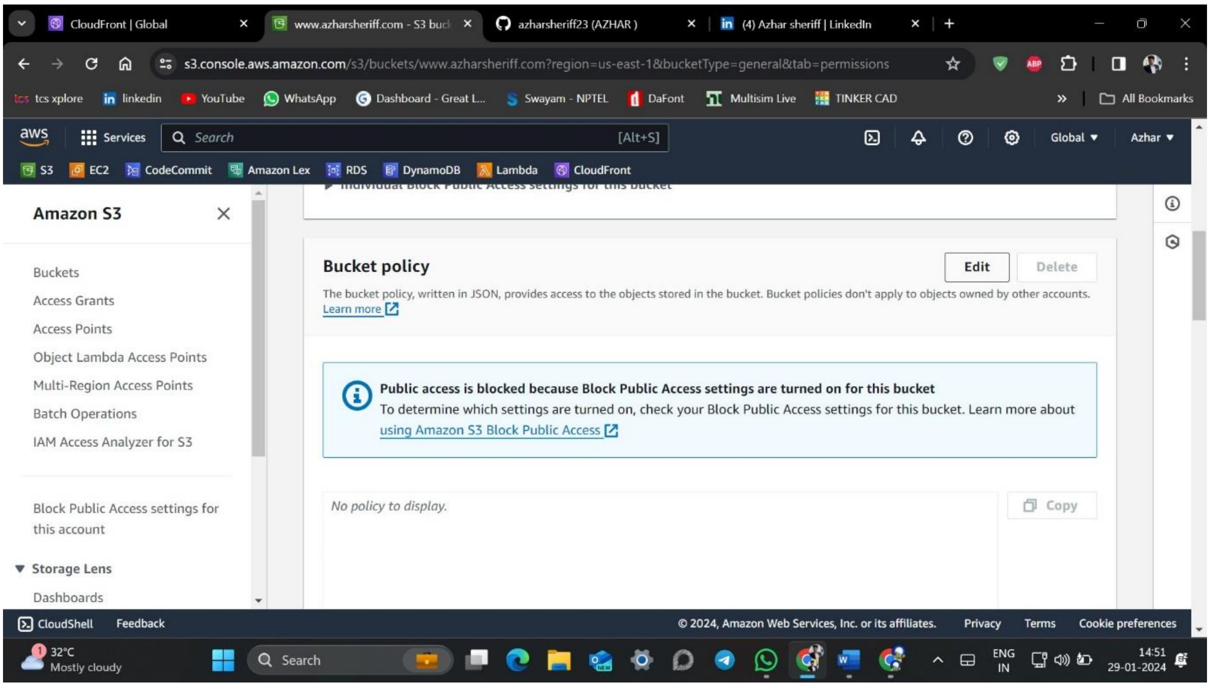
Distribution domain name
d3t8vgedw0czhc.cloudfront.net

ARN
arn:aws:cloudfront::774220458460:distribution/E2JF7NQOE2GR95

Last modified
Deploying

Settings

S3 > Select the bucket > Permissions > Bucket Policy


CloudFront | Global
www.azharsheriff.com - S3 buc
azharsheriff23 (AZHAR)
(4) Azhar sheriff | LinkedIn
s3.console.aws.amazon.com/s3/buckets/www.azharsheriff.com?region=us-east-1&bucketType=general&tab=permissions
Amazon S3
Buckets
Access Grants
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards

Bucket policy

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. Learn more

Public access is blocked because Block Public Access settings are turned on for this bucket
To determine which settings are turned on, check your Block Public Access settings for this bucket. Learn more about using Amazon S3 Block Public Access

No policy to display.

Now you can check with the cloud front after deployment it takes farther max 10 mins for deployment. Happy learning.

Azhar Sheriff I