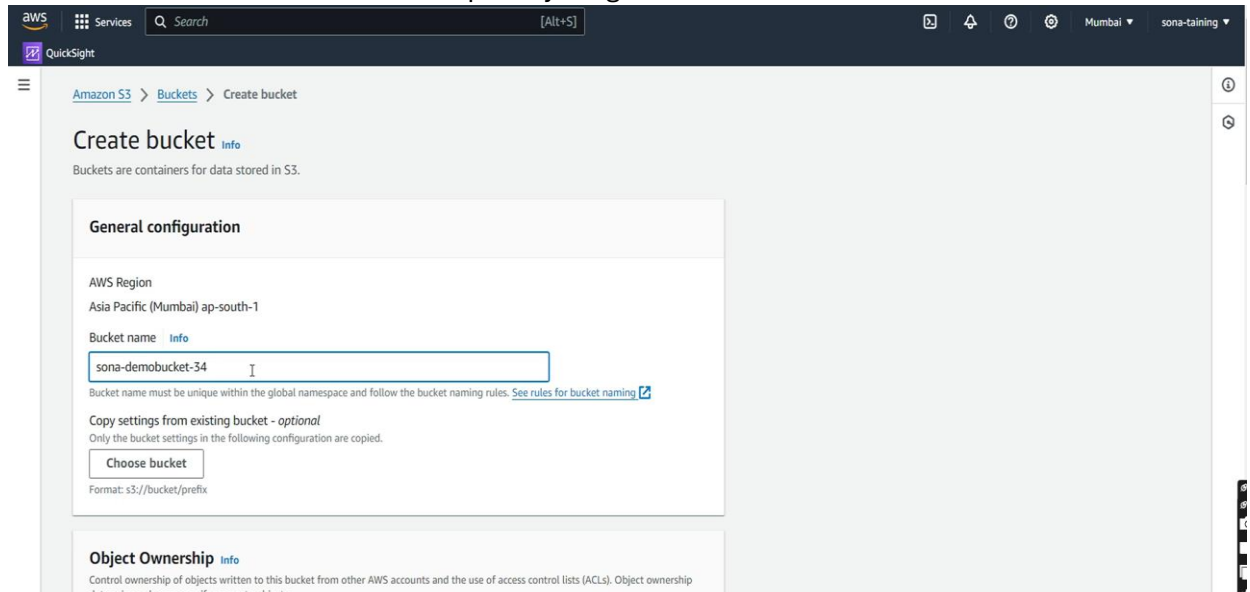


Lab: CloudFront

1. Let's first create a S3 bucket and keep everything as default. Then click on create bucket.



Amazon S3 > Buckets > Create bucket

Create bucket [Info](#)

Buckets are containers for data stored in S3.

General configuration

AWS Region
Asia Pacific (Mumbai) ap-south-1

Bucket name [Info](#)
sona-demobucket-34

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.

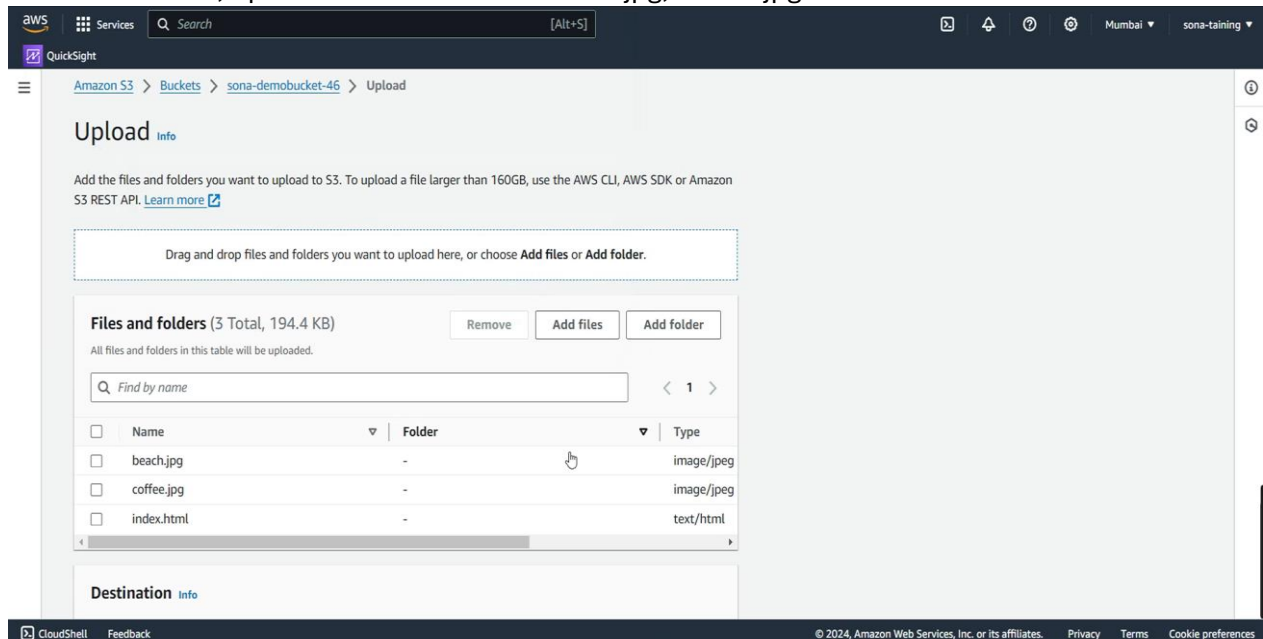
[Choose bucket](#)

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 modify, delete, or restore objects.

2. Inside S3 bucket, upload all three files i.e. coffee.jpg, beach.jpg and index.html.



Amazon S3 > Buckets > sona-demobucket-46 > 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 (3 Total, 194.4 KB)

[Remove](#) [Add files](#) [Add folder](#)

All files and folders in this table will be uploaded.

<input type="checkbox"/>	Name	Folder	Type
<input type="checkbox"/>	beach.jpg	-	image/jpeg
<input type="checkbox"/>	coffee.jpg	-	image/jpeg
<input type="checkbox"/>	index.html	-	text/html

Destination [Info](#)

CloudShell Feedback

© 2024, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

3. Open details of index.html → click on this pre-signed URL for my S3 bucket → don't see the image becoz it is not public
4. So let's see how we can instead use CloudFront to make these files accessible w/o making them public.
4. Search CloudFront (a global service) → Create a distribution → Origin name = Choose my S3 bucket → Origin access = Choose origin access control setting becoz it restrict access to only CloudFront → Create new OAC (leave everything as default and click on create) → WAF = Do not enable (depend on you) → Skip many option → Default root object = index.html → click on create distribution.

QuickSight

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.

Standard logging

Get logs of viewer requests delivered to an Amazon S3 bucket.

☒ Off

☐ On

IPv6

☐ Off

☒ On

Description - optional

Cancel

Create distribution

5. Our distribution may take some time to be created. Wait until the 'Last Modified' status updates. Then, copy the bucket policy and paste it into the S3 bucket policy editor.

aws Services Search [Alt+S]

QuickSight

Successfully created new distribution.
To get in-depth monitoring information for your distribution's internet traffic, [create an Internet Monitor](#)

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](#)

Copy policy

E21GY2XAE44H93

View metrics

General

Security

Origins

Behaviors

Error pages

Invalidation

Tags

Details

Distribution domain name

d244yso5s66cu4.cloudfront.net

ARN

arn:aws:cloudfront::956360599114:distribution/E21GY2XAE44H93

Last modified

Deploying

Settings

Edit

Description

Alternate domain names

Standard logging

off

CloudShell

Feedback

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

aws Services Search cloudfront

QuickSight

Amazon S3 > Buckets > sona-demobucket-46

sona-demobucket-46 Info

Objects

Properties

Permissions

Metrics

Management

Access Points

Permissions overview

Access finding

Access findings are provided by IAM external access analyzers. [Learn more about How IAM analyzer findings work](#)

[View analyzer for ap-south-1](#)

Block public access (bucket settings)

Edit

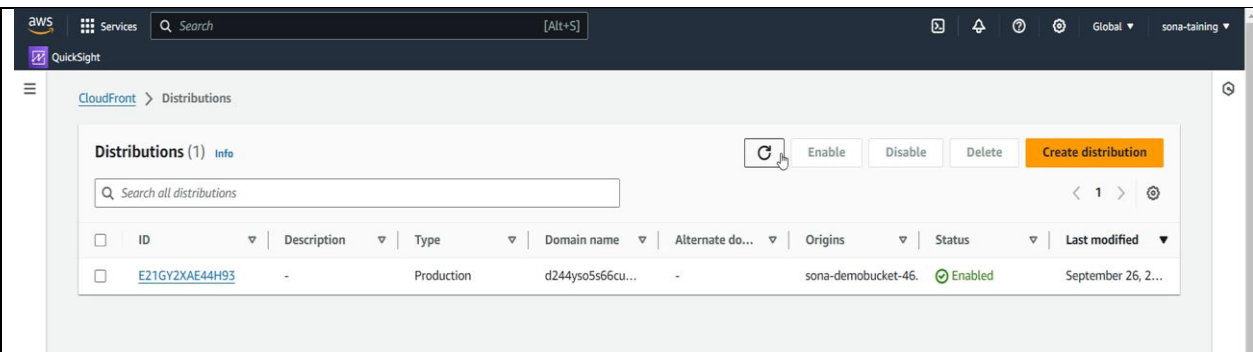
Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access 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 your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

Block all public access

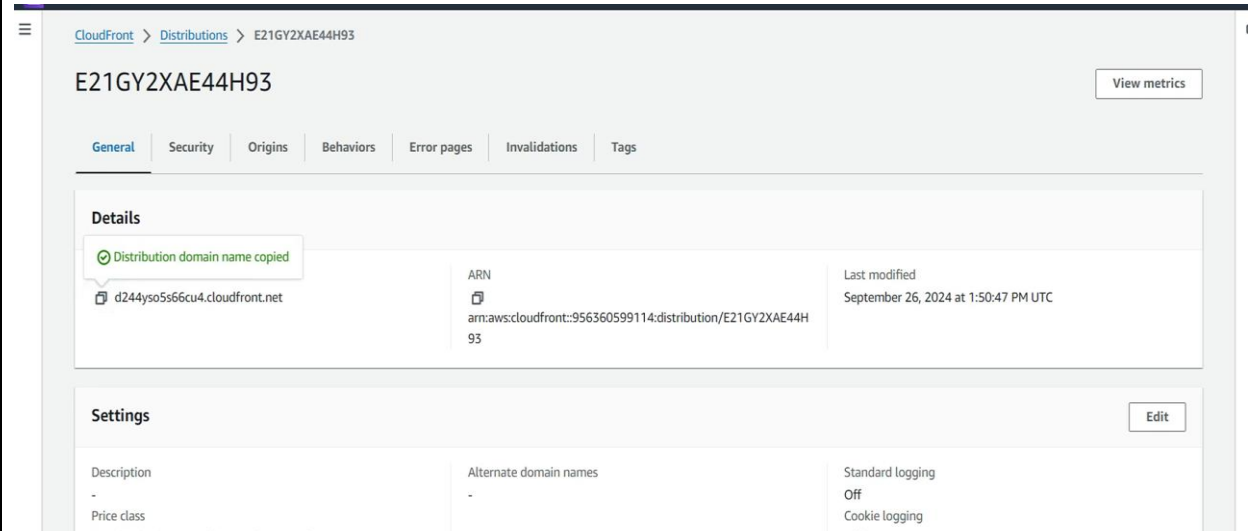
On

Individual Block Public Access settings for this bucket

6. Distribution is successfully created.



7. Go to this distribution, copy the distribution domain name and paste it into any browser. It's working now.



8. It's working now. But the cool thing about this is that now if I refresh this page, this is served from CloudFront cache and not from S3 bucket itself. Hence, the loading is much quicker.

