

NAME – VICKY SHARMA

AIM-CONCEPT OF CLOUDFRONT

\*( ATTACH CLOUD FRON TO A STATIC WEBSITE HOST IN S3 )

STEP1

CREATE A S3 BUCKET ]

Account snapshot

View Storage Lens dashboard

Storage lens provides visibility into storage usage and activity trends. [Learn more](#)

General purpose buckets

Directory buckets

General purpose buckets (1) Info

Refresh

Copy ARN

Empty

Delete

Create bucket

Buckets are containers for data stored in S3.

Find buckets by name

< 1 > ⚙

Name	AWS Region	Access	Creation date
wxewfdfer	US East (N. Virginia) us-east-1	Public	March 24, 2024, 13:40:56 (UTC+05:30)

STEP2 – UPLOAD YOUR HTML FILE TO HOST A WBESITE

Objects (1) Info

Refresh

Copy S3 URI

Copy URL

Download

Open

Delete

Actions

Create folder

Upload

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](#)

Find objects by prefix

< 1 > ⚙

<input type="checkbox"/>	Name	Type	Last modified	Size	Storage class
<input type="checkbox"/>	index.html	html	March 24, 2024, 13:56:57 (UTC+05:30)	14.0 B	Standard

STEP-3

ENABLE YOUR STATIC WEBSITE IN PROPERTIES SECTION

### Static website hosting

Use this bucket to host a website or redirect requests. [Learn more](#)

Edit

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://wxewfdfer.s3-website-us-east-1.amazonaws.com>

NOW CREATE A CLOUD FRONT AND ATTACH YOUR S3 BUCKET THERE

Choose an AWS origin, or enter your origin's domain name.

Q wxewfdfer.s3.us-east-1.amazonaws.com X

**⚠** This S3 bucket has static web hosting enabled. If you plan to use this distribution as a website, we recommend using the S3 website endpoint rather than the bucket endpoint.

Use website endpoint

#### Origin path - optional

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.

wxewfdfer.s3.us-east-1.amazonaws.com

#### Origin access [Info](#)

Enter a name for this origin.

wxewfdfer.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 control.

Select an origin access control ▼

Create new OAC

**⚠** This field cannot be empty

HERE DON'T ALLOW PUBLIC ACCESS INSTEAD OF THAT ALLOW ORGIN ACCESS CONTROL

**Name**  
The name must be unique. Valid characters: letters, numbers and most special characters. Use up to 64 characters.

wxewfdfer.s3.us-east-1.amazonaws.com

**Description - optional**  
The description can have up to 256 characters.

Enter description

**Signing behavior**

☒ Do not sign requests  
☐ Sign requests (recommended)

**Origin type**


S3 ▼

The origin type must be the same type as origin domain.

Cancel Create

Here in signing behavior please got with recommend one mean sign request

wxewfdfer.s3.us-east-1.amazonaws.com ▼ Create new OAC

 **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.

STEP 4- NOW TO GO S3 PERMISSION AND UPDATE THE BUCKET POLICY

Compress objects automatically [Info](#)

- ☐ No
- ☒ Yes

### Viewer

Viewer protocol policy

- ☐ HTTP and HTTPS
- ☒ Redirect HTTP to HTTPS
- ☐ HTTPS only

Allowed HTTP methods

- ☒ GET, HEAD
- ☐ GET, HEAD, OPTIONS
- ☐ GET, HEAD, OPTIONS, PUT, POST, PATCH, DELETE

Restrict viewer access

If you restrict viewer access, viewers must use CloudFront signed URLs or signed cookies to access your content.

- ☒ No
- ☐ Yes

## 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.

### 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.

index.html

### Standard logging

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

☒ Off

☐ On

### IPv6

☐ Off

☒ On

EC2 VPC S3 AWS Auto Scaling Simple Queue Service Simple Notification Service Key Management Service CloudTrail Amazon EventBridge RDS IAM

☑ Successfully created new distribution. X

⚠ 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 X

CloudFront > Distributions > E11MX4Y5OSCT0K

E11MX4Y5OSCT0K View metrics

General Security Origins Behaviors Error pages Invalidations Tags

Now here distribution itself provide us a bucket policy so just copy and paste the bucket policy and attach to bucket

### 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](#)

```
{
  "Version": "2012-10-17",
  "Id": "Policy1711268376177",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": "*"
    }
  ]
}
```

EditDelete

Copy

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

Successfully edited bucket policy.

Amazon S3 > Buckets > wxewfdfer

wxewfdfer

Info Publicly accessible

Objects

Properties

Permissions

Metrics

Management

Access Points

Permissions overview

Access

Public

Now also block all public access

## Block public access (bucket settings)

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

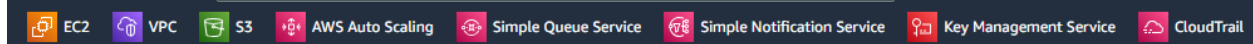
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

#### ☒ 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.



## CloudFront

### Distributions

Policies

Functions

What's new [NEW](#)

#### ▼ Telemetry

Monitoring

Alarms

Logs

#### ▼ Reports & analytics

Cache statistics

Popular objects

[CloudFront](#) > [Distributions](#) > E1J1W9N552QY1K

## E1J1W9N552QY1K

General

Security

Origins

Behaviors

Error pages

Invalidations

Tags

### Details

✓ Distribution domain name copied

Distribution domain name  
d23bhcf59ao97m.cloudfront.net

ARN

arn:aws:cloudfront::905418179079:distribution/E1J1W9N552QY1K

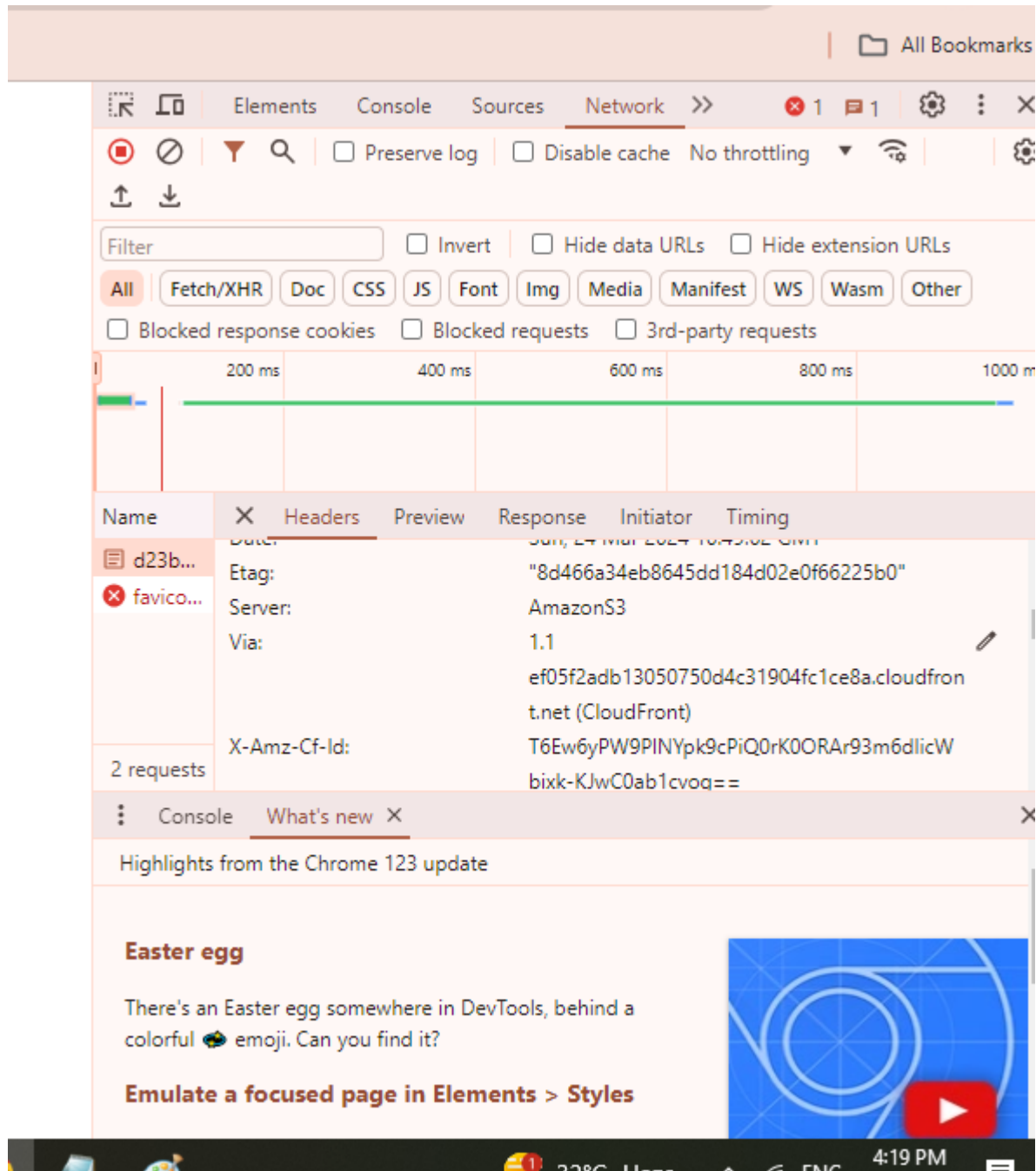
Last  
Mar

### Settings



Gmail YouTube

hii vicky here



Here successfully we attach our static website in s3 to cloudfront