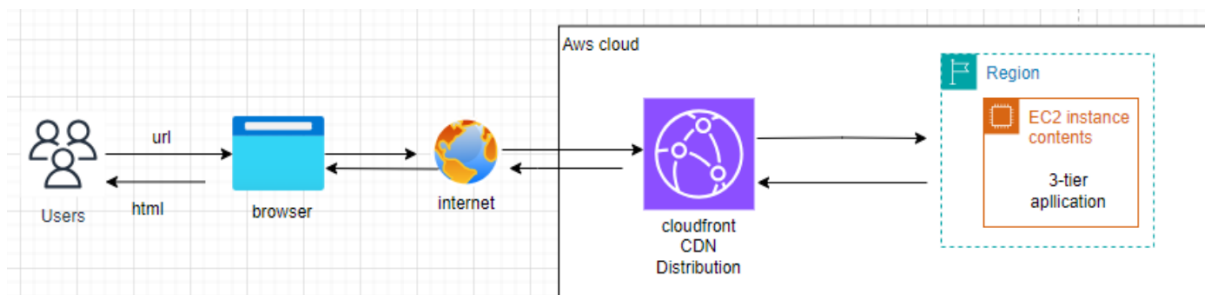


Create a CloudFront (Distribution) service using EC2 Instance & S3 Bucket

AWS CloudFront is a content delivery network service that speeds up the distribution of static (mostly S3) and dynamic web content (EC2 for static/dynamic) to users. It keeps the content on edge locations so that users can retrieve it easily whenever they request it. It delivers the content with the best possible performance by routing the user to the closest edge location. Amazon CloudFront will deliver the web content with low latency and with high transfer speeds.

What is a CDN?

A [Content Delivery Network \(CDN\)](#) is a system of distributed servers that deliver web content to users based on their geographic location. It reduces latency and speeds up load times by caching content closer to users. CDNs improve website performance and reliability, and help handle high traffic volumes efficiently. Examples include [Akamai](#), [Cloudflare](#), and Amazon CloudFront.



Using EC2 Instance-

Create Instance- (SG- SSH & HTTP)

Connect to Instance

```
$ sudo apt install apache2
```

Change dir to /var/www/html and **delete index.html** that has been **already presented**.

```
$ sudo rm index.html
```

Change dir to home

Install Website Template

```
$ wget https://www.free-css.com/assets/files/free-css-templates/download/page288/global.zip
```

```
$ sudo apt install unzip
```

```
$ unzip global.zip
```

Move that unzipped file contains only to /var/www/html

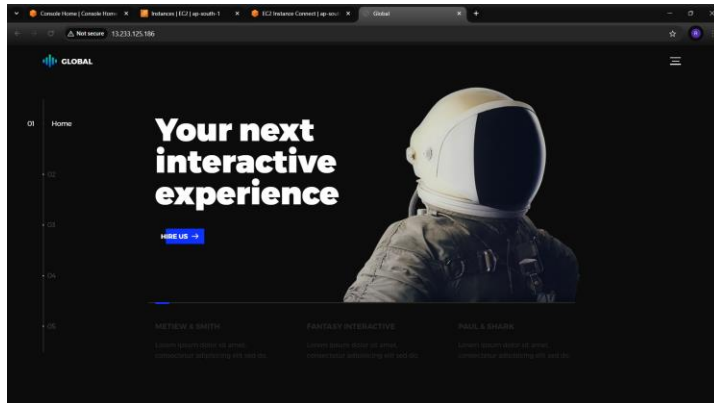
```
ubuntu@ip-172-31-42-7:~$ ls
global-master  global.zip
ubuntu@ip-172-31-42-7:~$ sudo mv global-master/* /var/www/html/
ubuntu@ip-172-31-42-7:~$ cd /var/www/html/
ubuntu@ip-172-31-42-7:/var/www/html$ ls
README.md  assets  index.html
```

```
$ sudo mv global-master/* /var/www/html/
```

Change dir to / var/www/html/ and check the moved files.

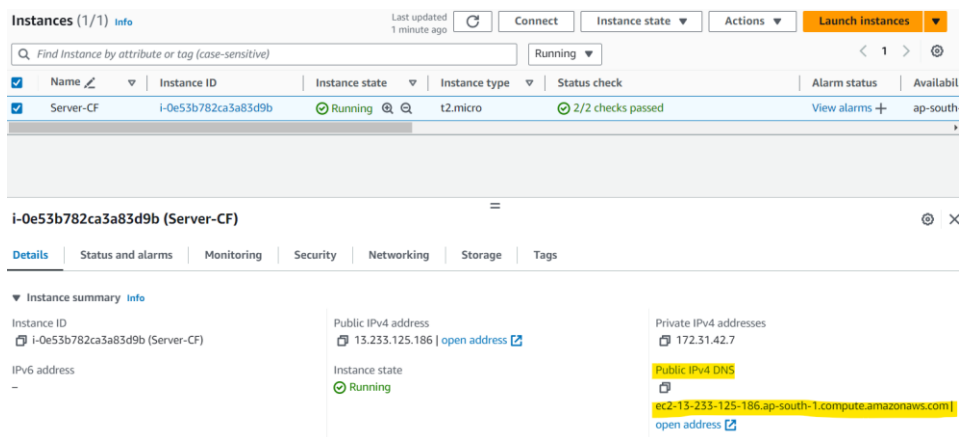
```
$ cd /var/www/html/
```

Check using Public IP that website can accessible

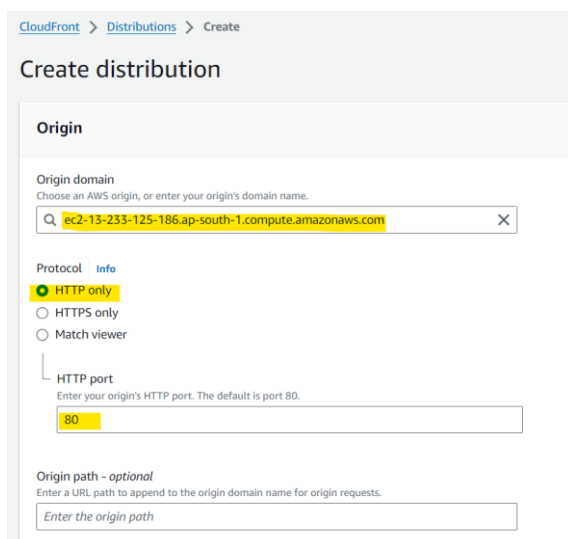


Create CloudFront Distribution-

Copy Public IPv4 DNS



Assign Public IPv4 DNS as an Origin Domain → Select HTTP only Protocol



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.

→ Create Distribution

Wait until its change Deploying Status

The screenshot shows the AWS CloudFront console with a table of distributions. The distribution 'EEF9N99KOZ2YA' is in the 'Deploying' status.

ID	Description	Type	Domain name	Alternate do...	Origins	Status	Last modified
EEF9N99KOZ2YA	-	Production	d3v3qatkxk1x3n...	-	ec2-13-233-125-186...	Enabled	Deploying

The screenshot shows the AWS CloudFront console with the same distribution 'EEF9N99KOZ2YA' now in the 'Enabled' status.

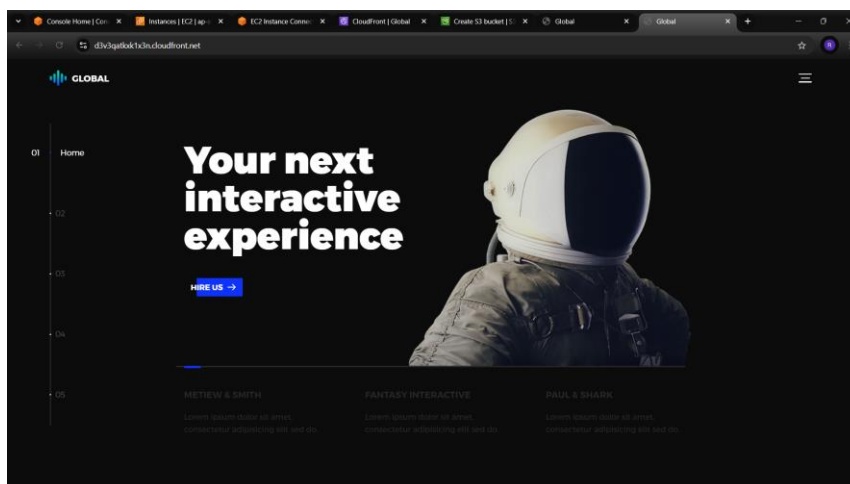
ID	Description	Type	Domain name	Alternate do...	Origins	Status	Last modified
EEF9N99KOZ2YA	-	Production	d3v3qatkxk1x3n...	-	ec2-13-233-125-186...	Enabled	August 26, 2024...

After changing Status

Use Distribution domain name as URL

The screenshot shows the details of the distribution 'EEF9N99KOZ2YA'. The 'Distribution domain name' is highlighted as 'd3v3qatkxk1x3n.cloudfront.net'.

Details	ARN	Last modified
Distribution domain name d3v3qatkxk1x3n.cloudfront.net	arn:aws:cloudfront:905418477144:distribution/EEF9N99KOZ2YA	August 26, 2024 at 8:14:39 PM UTC



NOTE – It is possible with Public IPv4 DNS

Using S3 Bucket

Create S3 Bucket → Give only Bucket Name

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](#)

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.

Format: s3://bucket/prefix

Upload Template files (Drag & Drop)

Amazon S3 > Buckets > myawsbuckeeett

myawsbuckeeett [Info](#)

[Objects](#) [Properties](#) [Permissions](#) [Metrics](#) [Management](#) [Access Points](#)

Objects (3) [Info](#) [Actions](#)

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](#)

<input type="checkbox"/>	Name	Type	Last modified	Size	Storage class
<input type="checkbox"/>	assets/	Folder	-	-	-
<input type="checkbox"/>	index.html	html	August 27, 2024, 02:09:50 (UTC+05:30)	14.9 kB	Standard
<input type="checkbox"/>	README.md	md	August 27, 2024, 02:09:50 (UTC+05:30)	962.0 B	Standard

Change some permission

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

Unblock all public access

Amazon S3 > Buckets > myawsbuckeeett > Edit Block public access (bucket settings)

Edit Block public access (bucket settings) [Info](#)

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.
- ☐ **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.

Object Ownership

Info

Edit

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 specify access to objects.

Object Ownership

Bucket owner enforced

ACLs are disabled. All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.

ACL's Enable-

Amazon S3

>

Buckets

>

myawsbuckeeett

>

Edit Object Ownership

Edit Object Ownership

Info

Object Ownership

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 specify access to objects.

☐ ACLs disabled (recommended)

All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.

☒ ACLs enabled

Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.

We recommend disabling ACLs, unless you need to control access for each object individually or to have the object writer own the data they upload. Using a bucket policy instead of ACLs to share data with users outside of your account simplifies permissions management and auditing.

Enabling ACLs turns off the bucket owner enforced setting for Object Ownership
Once the bucket owner enforced setting is turned off, access control lists (ACLs) and their associated permissions are restored. Access to objects that you do not own will be based on ACLs and not the bucket policy.

☒ I acknowledge that ACLs will be restored.

Edit ACL

Access control list (ACL)

Edit

Grant basic read/write permissions to other AWS accounts. [Learn more](#)

The console displays combined access grants for duplicate grantees
To see the full list of ACLs, use the Amazon S3 REST API, AWS CLI, or AWS SDKs.

Grantee	Objects	Bucket ACL
Bucket owner (your AWS account) Canonical ID: 4207a10e57aec34d71cea6d854d469939c186b87029b6f7a6dec943e46ce566a	List, Write	Read, Write
Everyone (public access) Group: http://acs.amazonaws.com/groups/global/AllUsers	-	-

Give Access List & Read for Everyone

Amazon S3

>

Buckets

>

myawsbuckeeett

>

Edit access control list (ACL)

Edit access control list (ACL)

Info

Access control list (ACL)

Grant basic read/write permissions to other AWS accounts. [Learn more](#)

Grantee	Objects	Bucket ACL
Bucket owner (your AWS account) Canonical ID: 4207a10e57aec34d71cea6d854d469939c186b87029b6f7a6dec943e46ce566a	<input checked="" type="checkbox"/> List <input checked="" type="checkbox"/> Write	<input checked="" type="checkbox"/> Read <input checked="" type="checkbox"/> Write
Everyone (public access) Group: http://acs.amazonaws.com/groups/global/AllUsers	<input checked="" type="checkbox"/> List <input type="checkbox"/> Write	<input checked="" type="checkbox"/> Read <input type="checkbox"/> Write

Changes in Properties

Static website hosting

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

Static website hosting

Disabled

Edit

Enable static website hosting & mention index document (ie. Index.html)

Amazon S3 > Buckets > myawsbuckeeett > Edit static website hosting

Edit static website hosting

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

Error document - optional

Make public using ACL for all Objects in the bucket

Amazon S3 > Buckets > myawsbuckeeett

myawsbuckeeett

Objects | Properties | Permissions | Metrics | Management | Access Points

Objects (3)

Find objects by prefix

	Name	Type	Last modified	Size
<input checked="" type="checkbox"/>	assets/	Folder	-	
<input checked="" type="checkbox"/>	index.html	html	August 27, 2024, 02:09:50 (UTC+05:30)	
<input checked="" type="checkbox"/>	README.md	md	August 27, 2024, 02:09:50 (UTC+05:30)	

Actions

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

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

Name	Type	Last modified	Size
📁 assets/	Folder	-	-
📄 index.html	html	August 27, 2024, 02:09:50 (UTC+05:30)	14.9 KB
📄 README.md	md	August 27, 2024, 02:09:50 (UTC+05:30)	962.0 B

Cancel

Make public

Use endpoint

Static website hosting

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

Static website hosting

Enabled

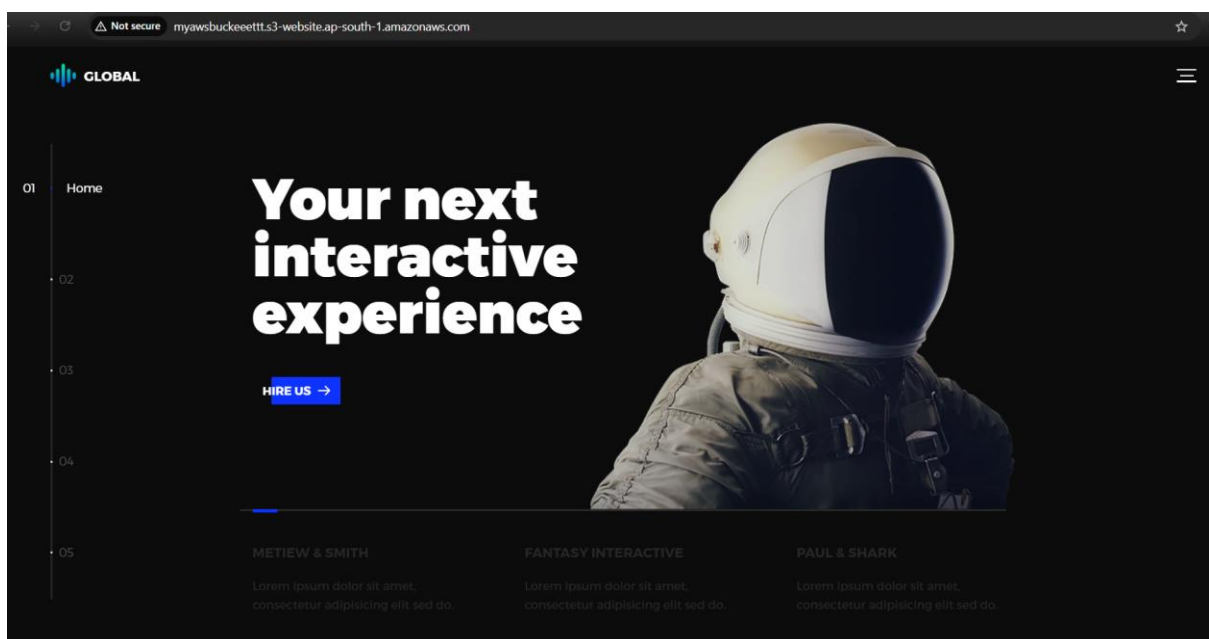
Hosting type

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://myawsbuckeeett.s3-website.ap-south-1.amazonaws.com>



Create CloudFront Distribution-

Select S3 bucket as Origin Domain

CloudFront > Distributions > Create

Create distribution

Origin

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

Amazon S3
myawsbuckeeett.s3.amazonaws.com

Elastic Load Balancer
No origins available.

API Gateway

IMP- Use website endpoint

Origin

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

⚠ 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.

Name
Enter a name for this origin.

Origin access [Info](#)

☒ **Public**
Bucket must allow public access.

Select protocol HTTP only

Origin

Origin domain

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

Protocol [Info](#)

☒ HTTP only

☐ HTTPS only

☐ Match viewer

HTTP port

Enter your origin's HTTP port. The default is port 80.

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.

→ Create Distribution

And, wait until Deploying

Successfully created new distribution.

CloudFront > Distributions > EAGQXIS4Z4NZ

EAGQXIS4Z4NZ [View metrics](#)

[General](#) [Security](#) [Origins](#) [Behaviors](#) [Error pages](#) [Invalidations](#) [Tags](#)

Details

Distribution domain name

db16zjv8dla6v.cloudfront.net

ARN

arn:aws:cloudfront:905418477144:distribution/EAGQXIS4Z4NZ

Last modified

Deploying

CloudFront > Distributions

Distributions (1) [Info](#)

Enable

Disable

Delete

Create distribution

< 1 >

<input type="checkbox"/>	ID	Description	Type	Domain name	Alternate do...	Origins	Status	Last modified
<input type="checkbox"/>	EAGQXIS4Z4NZ	-	Production	db16zjv8dla6v.cl...	-	myawsbuckeeett.s3-v	Enabled	August 26, 2024...

Use Distribution domain name

CloudFront > Distributions > EAGQXIS4Z4NZ

EAGQXIS4Z4NZ

View metrics

General

Security

Origins

Behaviors

Error pages

Invalidation

Tags

Details

Distribution domain name

db16zjv8dla6v.cloudfront.net

ARN

arn:aws:cloudfront::905418477144:distribution/EAGQXIS4Z4NZ

Last modified

August 26, 2024 at 9:06:56 PM UTC

A screenshot of a web browser displaying a landing page for a company named 'GLOBAL'. The browser's address bar shows the URL 'db16zjv8dla6v.cloudfront.net'. The page has a dark theme. On the left, there is a vertical navigation menu with links labeled '01 Home', '02', '03', '04', and '05'. The main content area features a large, bold headline 'Your next interactive experience' in white text. Below the headline is a blue button with the text 'HIRE US' and a right-pointing arrow. To the right of the text is a high-quality image of an astronaut in a white spacesuit, seen from the side, looking towards the right. Below the main content, there are three columns of text, each starting with a name: 'METIEW & SMITH', 'FANTASY INTERACTIVE', and 'PAUL & SHARK'. Each column contains several lines of placeholder text (Lorem Ipsum). The browser's tab bar at the top shows several open tabs, including 'Console Home', 'Instances', 'EC2 Instance Connect', 'CloudFront', and others.

Rushikesh Magar (Cloudblitz)