

Serving a static Website which is Uploaded in S3 through CDN and route 53

Summary

- 1.Host a static website in S3
- 2.Buy a SSL certificate for your subdomain(us-east-1)
- 3.Map your S3 domain name in CDN and choose your certificate there
- 4.Create a subdomain in Route 53 and map your CDN against the subdomain

Host a static website in S3

Note: Give bucket name as subdomain name which you want to create
(eg:john.gradiouslabs.click)

- 1.Go to S3 and create a bucket, Choose your region, ACLs disabled and allow public access, Bucket versioning enable and leave the rest as default

A:

The screenshot shows the 'Create bucket' wizard in the AWS Management Console. The top navigation bar includes 'Services', a search bar, and user information ('gujjapranaykumar @ 6281-3291-6033'). The breadcrumb path is 'Amazon S3 > Buckets > Create bucket'. The main section is titled 'Create bucket' with a 'Info' link. It contains fields for 'Bucket name' (set to 'pranay.gradiouslabs.click') and 'AWS Region' (set to 'Asia Pacific (Mumbai) ap-south-1'). Below these are sections for 'General configuration', 'Copy settings from existing bucket - optional', and 'Block all public access'. A warning message at the bottom states that turning off block all public access might result in the bucket becoming public.

General configuration

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

Bucket name: [Info](#)
pranay.gradiouslabs.click

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

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.

⚠ Turning off block all public access might result in this bucket and the objects within becoming public
AWS recommends that you turn on block all public access, unless public access is required for specific and verified use cases such as static website hosting.

I acknowledge that the current settings might result in this bucket and the objects within becoming public.

Bucket Versioning

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. [Learn more](#)

Bucket Versioning

Disable

Enable

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
- Storage Lens groups
- AWS Organizations settings

Services

Search [Alt+S]

Global ▾ gujjapranaykumar @ 6281-3291-6035

Policy

```
1▼ {  
2  "Version": "2012-10-17",  
3▼  "Statement": [  
4▼    {  
5      "Effect": "Allow",  
6      "Principal": "*",  
7      "Action": "s3:GetObject",  
8      "Resource": "arn:aws:s3:::pranay.gradiouslabs.click/*"  
9    }  
10  ]  
11 }  
12 }
```

Edit statement

Select a statement

Select an existing statement in the policy or add a new statement.

+ Add new statement

2.Extract the below file and upload it to your s3 bucket

Squadfree.zip

A:

3. Go to bucket -> properties -> static website hosting -> Enable, and give html file name and save

4.Grab the url and access it in the browser

A:

The screenshot shows the 'Static website hosting' configuration for an S3 bucket. The 'Enable' radio button is selected for static website hosting. Under 'Hosting type', the 'Host a static website' option is selected, with a note explaining that the bucket endpoint will be used as the web address. A callout box provides information about making content publicly readable via S3 Block Public Access settings. The 'Index document' field is set to 'index.html'. There is also an 'Error document - optional' field.

Buy SSL certificate for your subdomain(us-east-1)

1. Navigate to aws certificate Manager -> request certificate and give your domain name eg(john.gradiouslabs.click)

2. Leave everything else default

A:

The screenshot shows the 'Certificates' page in AWS Certificate Manager. It displays one certificate entry:

Certificate ID	Domain name	Type	Status	In use	Renewal eligibility	Key algorithm
4a3cf05f-9861-4be1-8d42-3b8d38964031	pranay.gradio.uslabs.click	Amazon Issued	Pending validation	No	Ineligible	RSA 2048

3.Create a record for route 53

A:

▼ Record 1

Delete

Record name Info	Record type Info
_8175cee9e2b09b0b46bcd50950d2	.gradiouslabs.click
Keep blank to create a record for the root domain.	
<input checked="" type="radio"/> Alias	CNAME – Routes traffic to another domain name and to some AWS reso...
Value Info	<input type="text" value="82ae938d7686ad5128f62a2828d69c55.mhbtsbpndt.acm-validations.aws."/>
Enter multiple values on separate lines.	
TTL (seconds) Info	Routing policy Info
<input type="text" value="300"/>	<input type="button" value="1m"/> <input type="button" value="1h"/> <input type="button" value="1d"/> Simple routing
Recommended values: 60 to 172800 (two days)	

Creating Cloudfront Distribution

1.Navigate to cloudfont, create Distribution

2.Click Use website endpoint option

3.Leave protocol as http

4.Choose your SSL certificate in Settings and give your domain name in alternate domain name

5.Click create Distribution

6.Go to your Cloudfront Distribution and copy your CDN Domain name and access it in Browser

A:

aws Services Search [Alt+S] Global gujjapranaykumar @ 6281-3291-6033 ▾

CloudFront > Distributions > Create

Create distribution

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.

HTTPS port
Enter your origin's HTTPS port. The default is port 443.

Services Search [Alt+S] Global ▾ gujjapranaykumar @ 6281-3291-6033 ▾

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).

pranay.gradiouslabs.click (4a3cf05f-9861-4be1-8d42-3b8d38964031) [Request certificate](#)

pranay.gradiouslabs.click [Request certificate](#)

Legacy clients support - \$600/month prorated charge applies. Most customers do not need this.
CloudFront allocates dedicated IP addresses at each CloudFront edge location to serve your content over HTTPS.

Enabled

Security policy
The security policy determines the SSL or TLS protocol and the specific ciphers that CloudFront uses for HTTPS connections with viewers (clients).

TLSv1.2_2021 (recommended)

TLSv1.2_2019

TLSv1.2_2018

TLSv1.1_2016

[Alt+S] Global ▾ gujjapranaykumar @ 6281-3291-6033 ▾

Details

Distribution domain name	ARN	Last modified
d285u96es9qoa.cloudfront.net	arn:aws:cloudfront::628132916033:distribution/E27BQY80XQW648	January 20, 2024 at 10:40:47 AM UTC

Settings

[Edit](#)

Description	Alternate domain names	Standard logging
-	pranay.gradiouslabs.click	Off
Price class	Custom SSL certificate	Cookie logging
Use all edge locations (best performance)	pranay.gradiouslabs.click	Off
Supported HTTP versions	Security policy	Default root object
HTTP/2, HTTP/1.1, HTTP/1.0	TLSv1.2_2021	-

