S3, Cloudfront & Cognito Doc

Steps involved in s3 and Cloudfront:

1, S3
2, Cloudfront
3, Cognito

Simple Storage Service(S3):

- Go to s3 link from the AWS Console https://go.aws/3wgy93z
- Click Create bucket
- Enter a bucket name
- Choose AWS region where you want to host, here I have chosen Mumbai region
- Leave the default settings in Block Public Access settings for this bucket
- Enable Bucket Versioning
- Other settings leave as it is and click Create bucket
- Now click the bucket and go to the permission tab
- Scroll down to Cross-origin resource sharing (CORS), now copy the below code
-

```
[
{
    "AllowedHeaders": [
        "*"
    ],
    "AllowedMethods": ["PUT",
        "POST", "GET", "DELETE"
    ],
    "AllowedOrigins": [
        "*"
    ],
    "ExposeHeaders": [],
    "MaxAgeSeconds": 3000
}
]
```

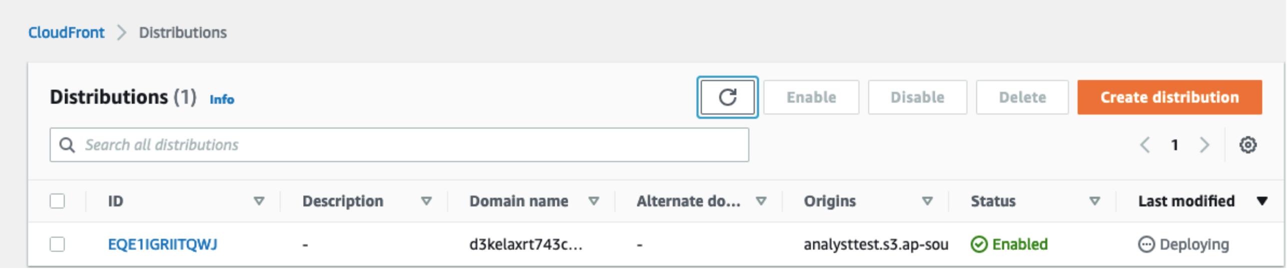
- Click edit and paste the copied code
- Now Click save changes

Cloudfront:

- Go to cloud front dashboard in AWS console https://go.aws/3jTHqJU
- Click Create a CloudFront distribution
- Under Origin domain choose the bucket which you have created earlier
- Now under S3 bucket access choose ***Yes use OAI (bucket can restrict access to only CloudFront)***
- Now in Origin access identity click create new OAI
- Under bucket policy choose ***Yes, update the bucket policy***
- Now scroll down to Default cache behavior
- In viewer section choose Redirect HTTP to HTTPS other options leave as it is
- Now in **Cache key and origin requests** click create policy under Cache policy, now it redirects to another tab.
- Give the name of your desire
- In TTL settings enter 5184000 for all (5184000 = 60 days)
- Scroll down and click Create
- Close the tab and go back to the previous tab
- Click refresh button under Cache policy
- Click the dropdown and choose the cache policy which you have created
- Leave other settings as it is and click Create distribution

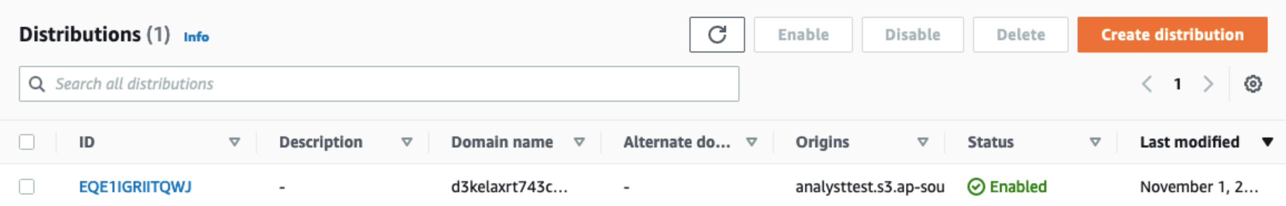
Wait for few minutes for the cloud front distribution to deploy

Before deploy:



□	ID	Description	Domain name	Alternate do...	Origins	Status	Last modified
□	EQE1IGRIITQWJ	-	d3kelaxrt743c...	-	analysttest.s3.ap-sou	✓ Enabled	Deploying

After deploy:

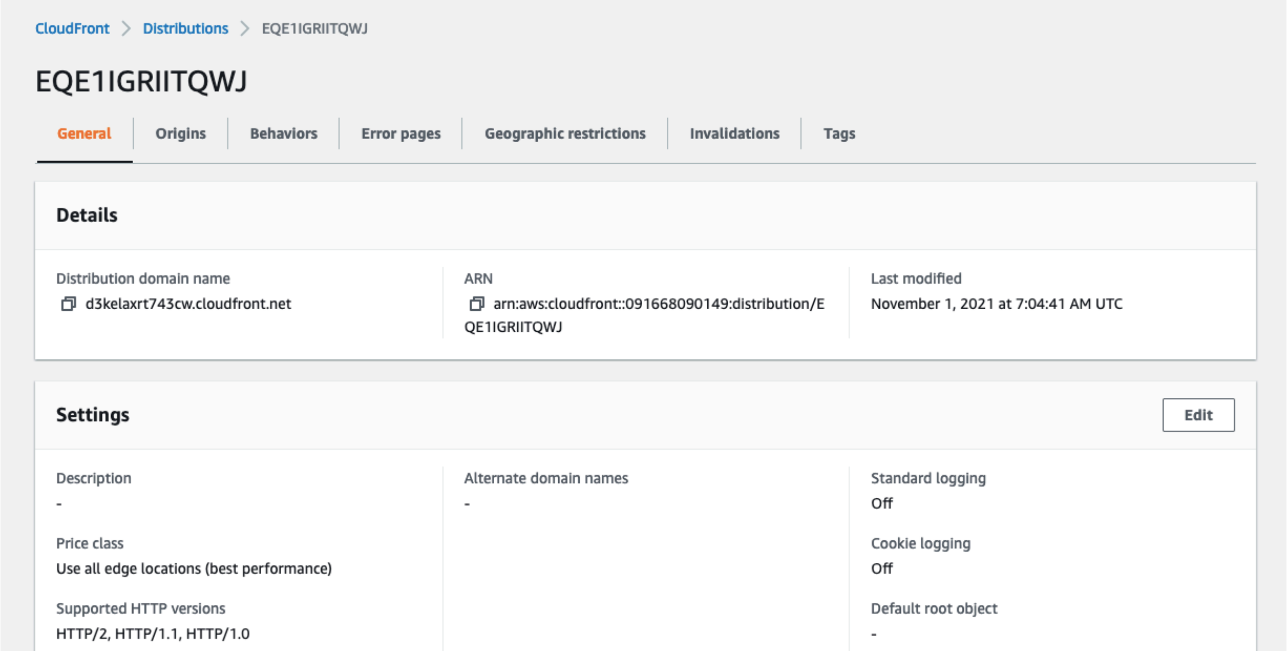


□	ID	Description	Domain name	Alternate do...	Origins	Status	Last modified
□	EQE1IGRIITQWJ	-	d3kelaxrt743c...	-	analysttest.s3.ap-sou	✓ Enabled	November 1, 2...

Test:

- Now in the S3 bucket upload an image or a video
- In cloud front copy the cloud front domain name
- Paste the copied domain name and type a slash and type the object name of the s3 and enter in the web browser

Cloudfront Dashboard:



EQE1IGRIITQWJ

Details

Distribution domain name
d3kelaxrt743cw.cloudfront.net

ARN
arn:aws:cloudfront::091668090149:distribution/EQE1IGRIITQWJ

Last modified
November 1, 2021 at 7:04:41 AM UTC

Settings

Description
-

Price class
Use all edge locations (best performance)

Supported HTTP versions
HTTP/2, HTTP/1.1, HTTP/1.0

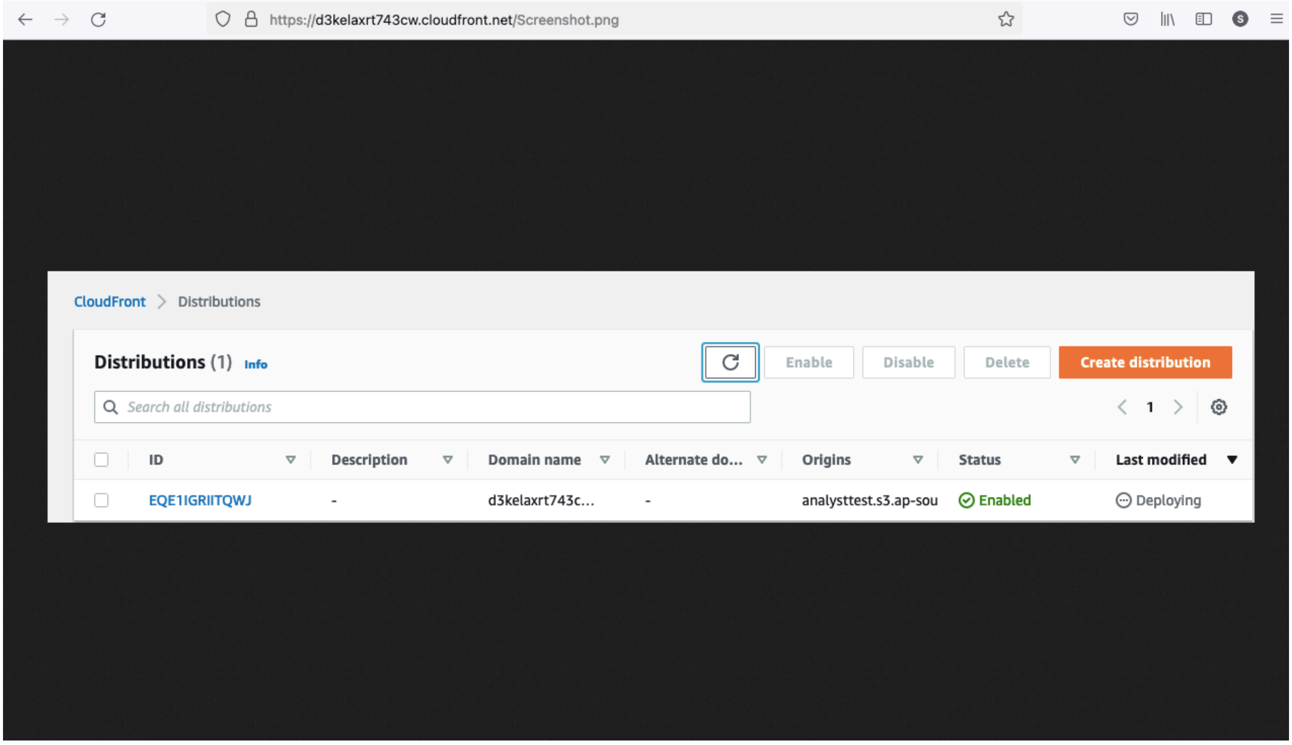
Alternate domain names
-

Standard logging
Off

Cookie logging
Off

Default root object
-

Test Result:



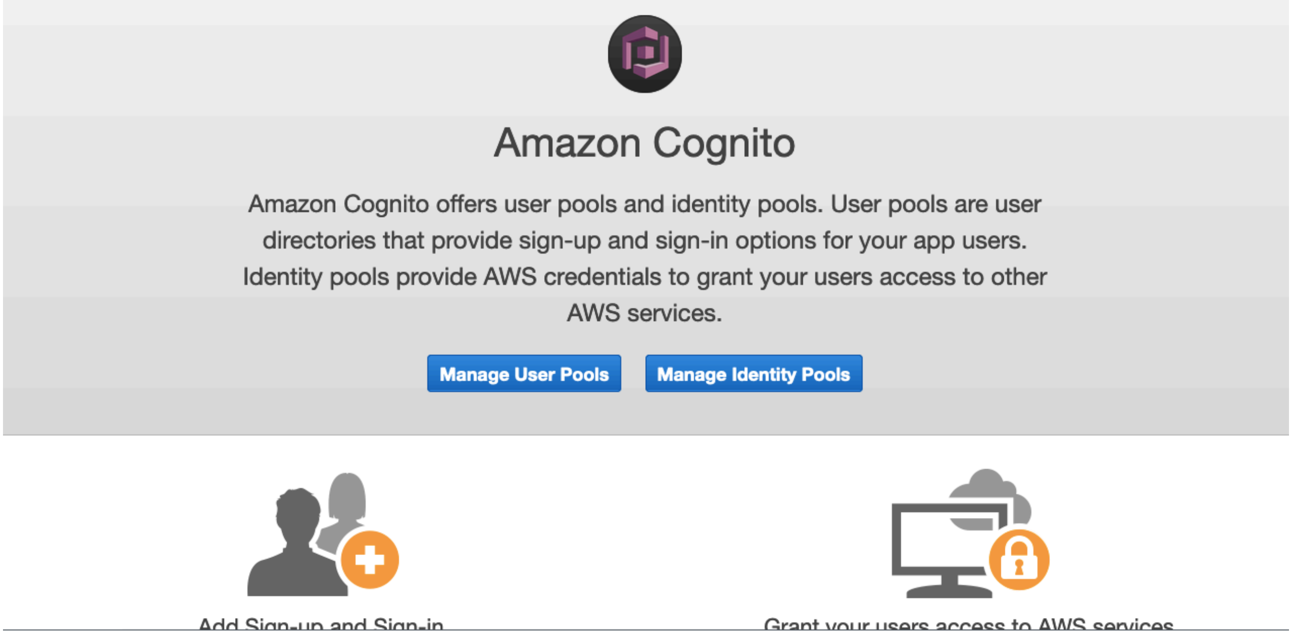
https://d3kelaxrt743cw.cloudfront.net/Screenshot.png

Distributions (1)

□	ID	Description	Domain name	Alternate do...	Origins	Status	Last modified
□	EQE1IGRIITQWJ	-	d3kelaxrt743c...	-	analysttest.s3.ap-sou	✓ Enabled	Deploying

Cognito:

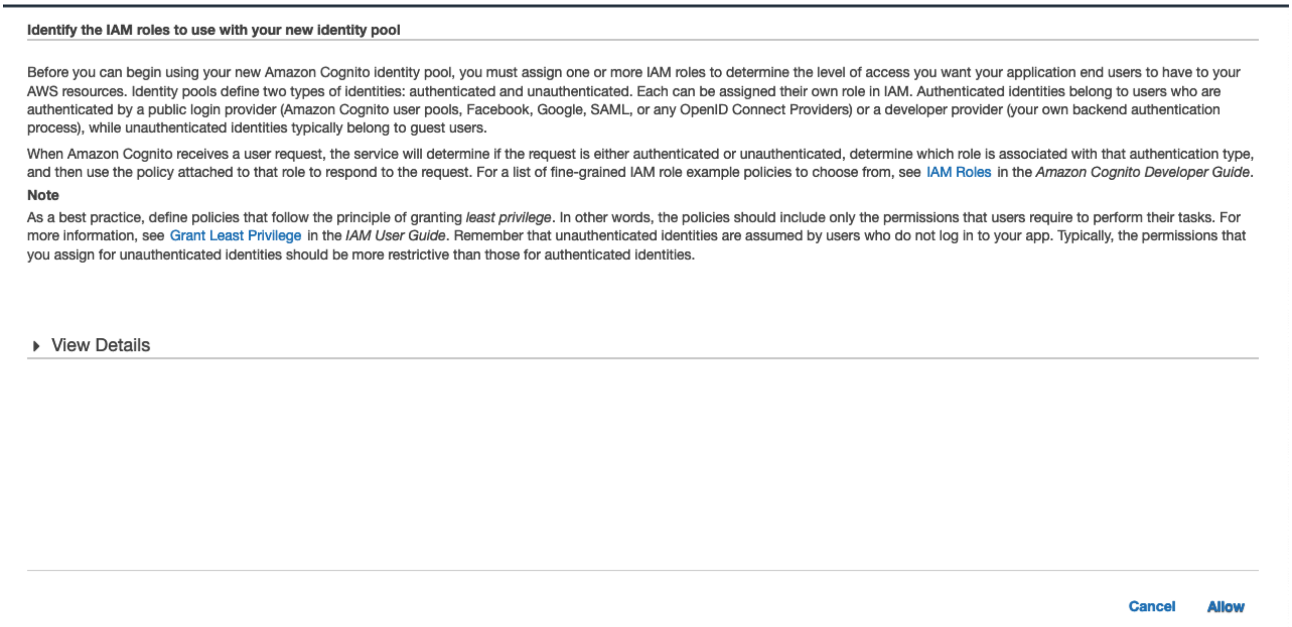
- Go to Cognito services in the AWS console https://go.aws/3pWPkWn
- Select the region which you want to use, here I have selected Mumbai region



Amazon Cognito

Amazon Cognito offers user pools and identity pools. User pools are user directories that provide sign-up and sign-in options for your app users. Identity pools provide AWS credentials to grant your users access to other AWS services.

- Click Manage Identity Pools
- Give a name to Identity pool name
- Under Unauthenticated identities select Enable access to unauthenticated identities
- Scroll down and click create pool



Identify the IAM roles to use with your new identity pool

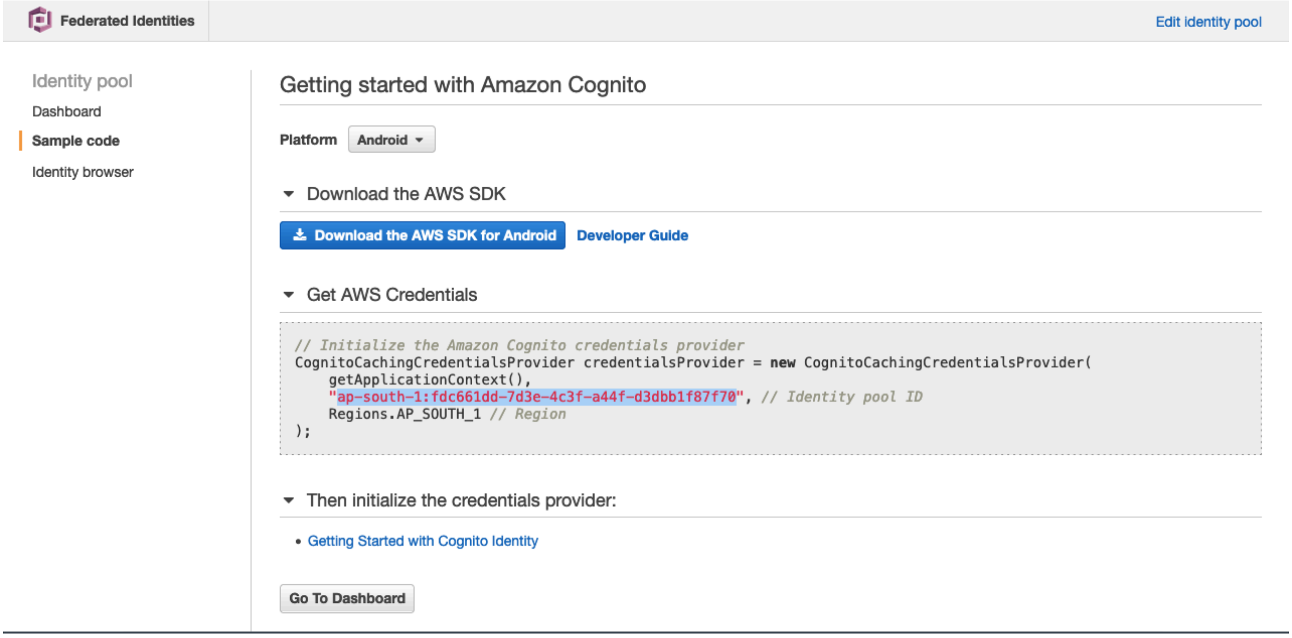
Before you can begin using your new Amazon Cognito identity pool, you must assign one or more IAM roles to determine the level of access you want your application end users to have to your AWS resources. Identity pools define two types of identities: authenticated and unauthenticated. Each can be assigned their own role in IAM. Authenticated identities belong to users who are authenticated by a public login provider (Amazon Cognito user pools, Facebook, Google, SAML, or any OpenID Connect Providers) or a developer provider (your own backend authentication process), while unauthenticated identities typically belong to guest users.

When Amazon Cognito receives a user request, the service will determine if the request is either authenticated or unauthenticated, determine which role is associated with that authentication type, and then use the policy attached to that role to respond to the request. For a list of fine-grained IAM role example policies to choose from, see IAM Roles in the *Amazon Cognito Developer Guide*.

Note

As a best practice, define policies that follow the principle of granting *least privilege*. In other words, the policies should include only the permissions that users require to perform their tasks. For more information, see Grant Least Privilege in the *IAM User Guide*. Remember that unauthenticated identities are assumed by users who do not log in to your app. Typically, the permissions that you assign for unauthenticated identities should be more restrictive than those for authenticated identities.

- Click view details, here an automated IAM role is created on your behalf by the AWS
- Scroll down and click Allow
- Copy the identity pool id and save it in your notes to share the Pool id to developers



Getting started with Amazon Cognito

Download the AWS SDK

Get AWS Credentials

```
// Initialize the Amazon Cognito credentials provider
CognitoCachingCredentialsProvider credentialsProvider = new CognitoCachingCredentialsProvider(
    getApplicationContext(),
    "ap-south-1:fdc661dd-7d3e-4c3f-a44f-d3dbb1f87f70", // Identity pool ID
    Regions.AP_SOUTH_1 // Region
);
```

Then initialize the credentials provider:

- Now go to the IAM console and click roles
- You can find the roles created by the AWS on behalf of you
- For the Two created unauth & Auth Cognito roles attach S3 Full access in permission tab of the respective roles
- Once attached share the credentials to the developers

Example:

Pool id: ap-south-1:fdc661dd-7d3e-4c3f-a44f-d3dbb1f87f70
Bucket name: Training
Cloudfront url: https://d1b158pa2btie3.cloudfront.net