

## Lesson 05 Demo 10

### Configuring Origin Access Identity (OAI)

**Objective:** To block S3 access for the public and restrict access only through the CloudFront using OAI

**Tools required:** AWS

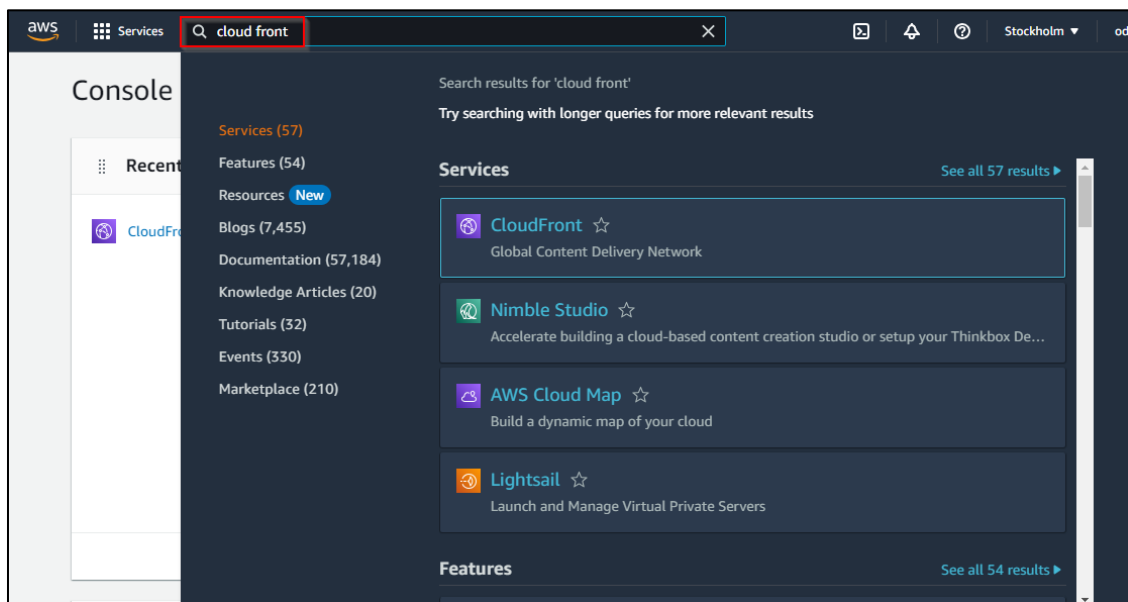
**Prerequisites:** S3 bucket with an object added and an AWS account with CloudFront Distribution created

Steps to be followed:

1. CloudFront access with OAI

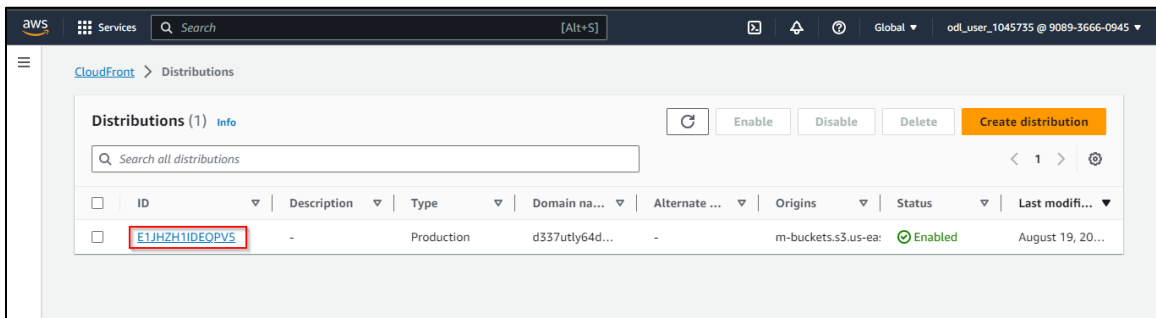
#### Step 1: CloudFront access with OAI

- 1.1 Navigate to the AWS console, search and select **CloudFront**

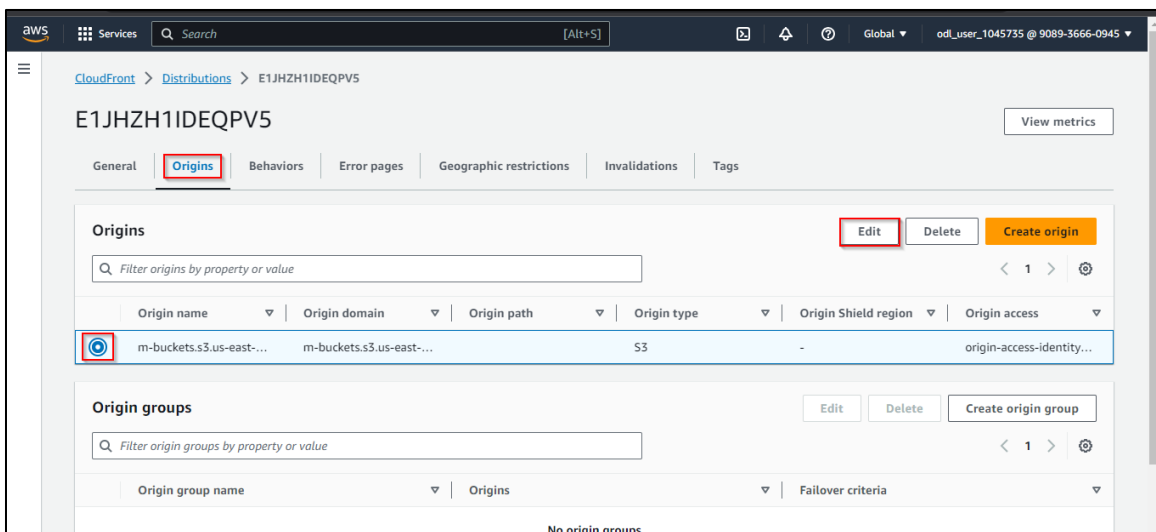


**Note:** Public access needs to be blocked while creating an S3 bucket and uploading any kind of **index.html** file. Refer to the previous demos.

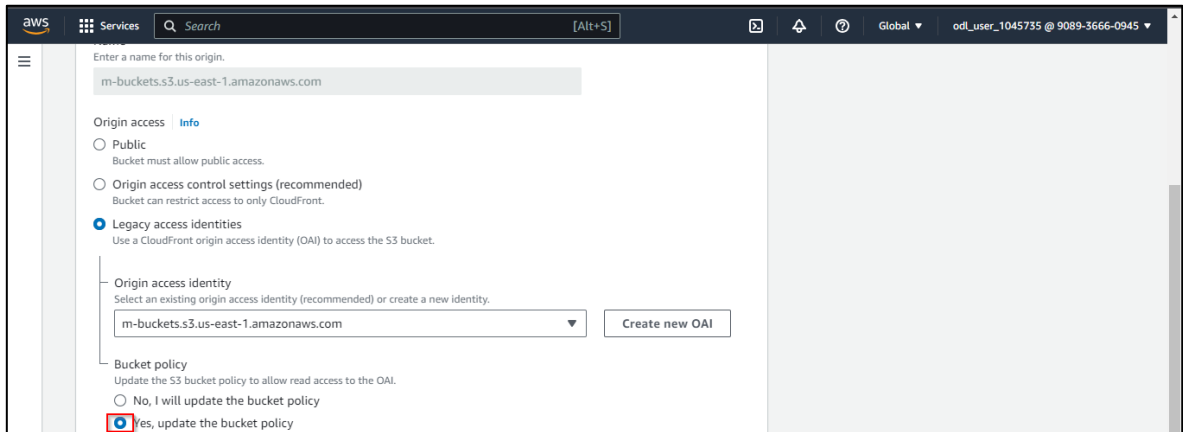
1.2 Navigate to the **CloudFront Distribution** created in previous demos and click on it



1.3 Navigate to **Origins**, select the created bucket, click on the **Edit** button



## 1.4 Click on the **Yes, update the bucket policy**



Enter a name for this origin.  
m-buckets.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.

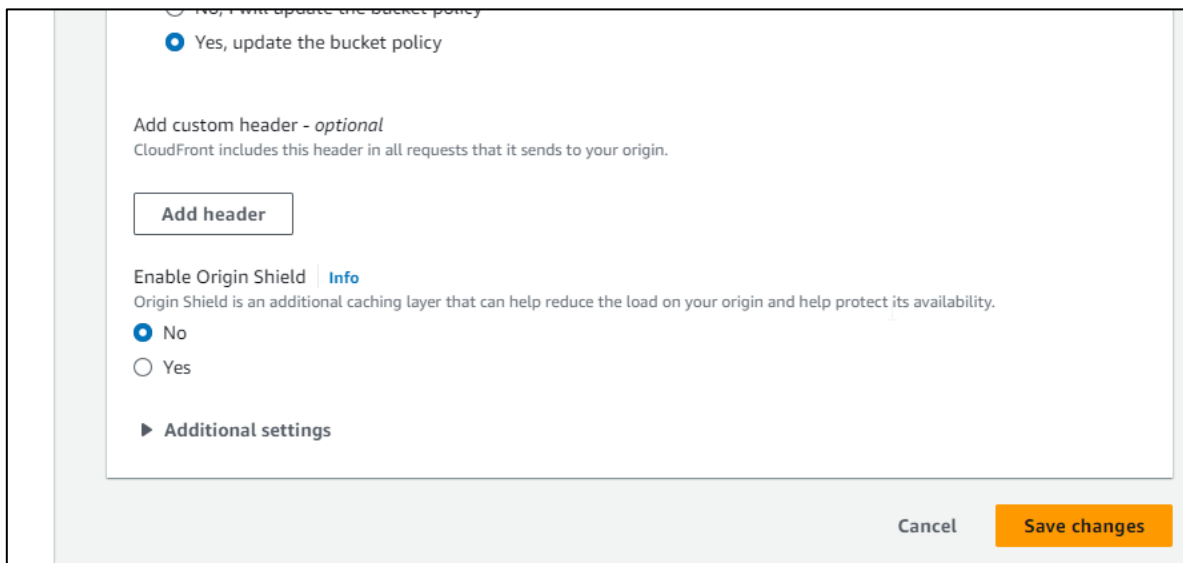
Origin access identity  
Select an existing origin access identity (recommended) or create a new identity.  
m-buckets.s3.us-east-1.amazonaws.com [Create new OAI](#)

Bucket policy  
Update the S3 bucket policy to allow read access to the OAI.

☐ No, I will update the bucket policy

☒ Yes, update the bucket policy

## 1.5 Click on **Save changes**



☐ No, I will update the bucket policy

☒ Yes, update the bucket policy

Add custom header - *optional*  
CloudFront includes this header in all requests that it sends to your origin.

[Add header](#)

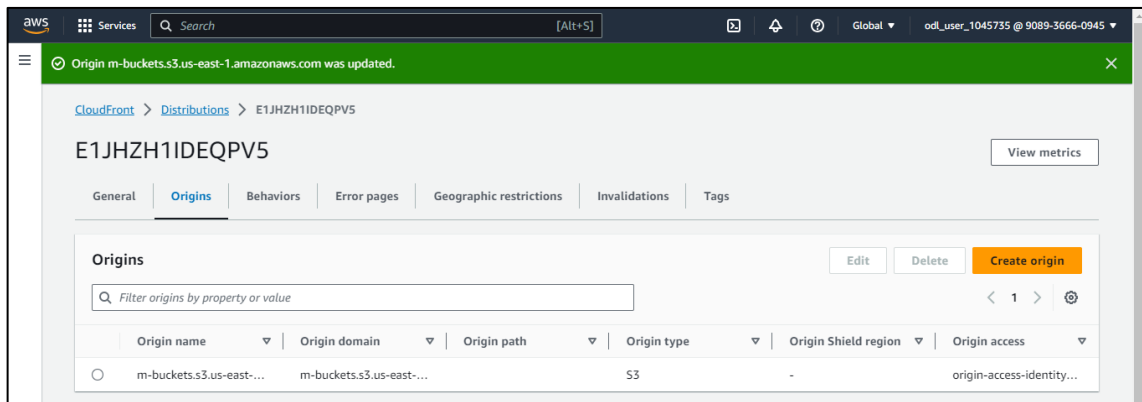
Enable Origin Shield [Info](#)  
Origin Shield is an additional caching layer that can help reduce the load on your origin and help protect its availability.

☒ No

☐ Yes

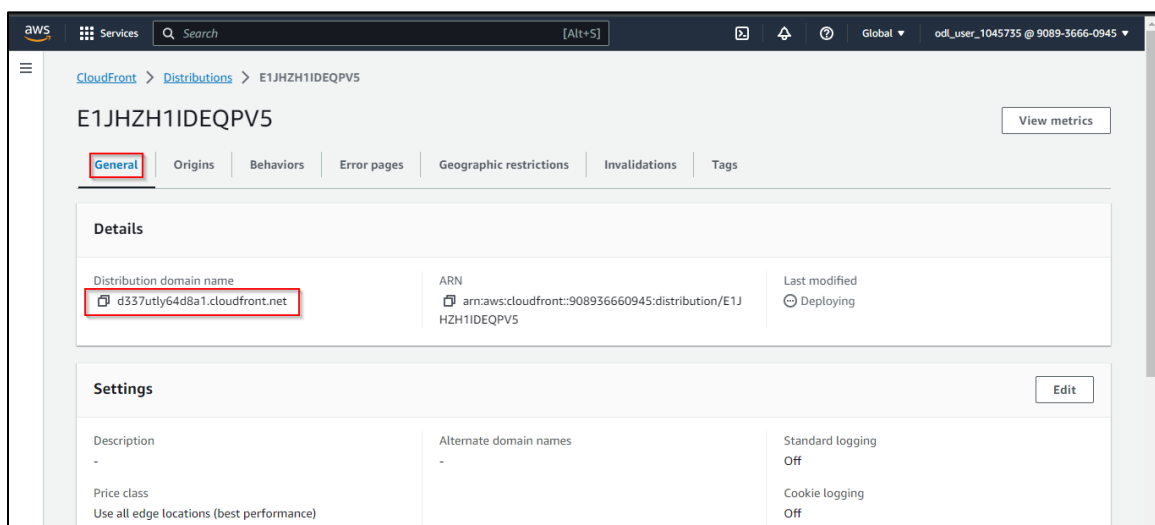
► Additional settings

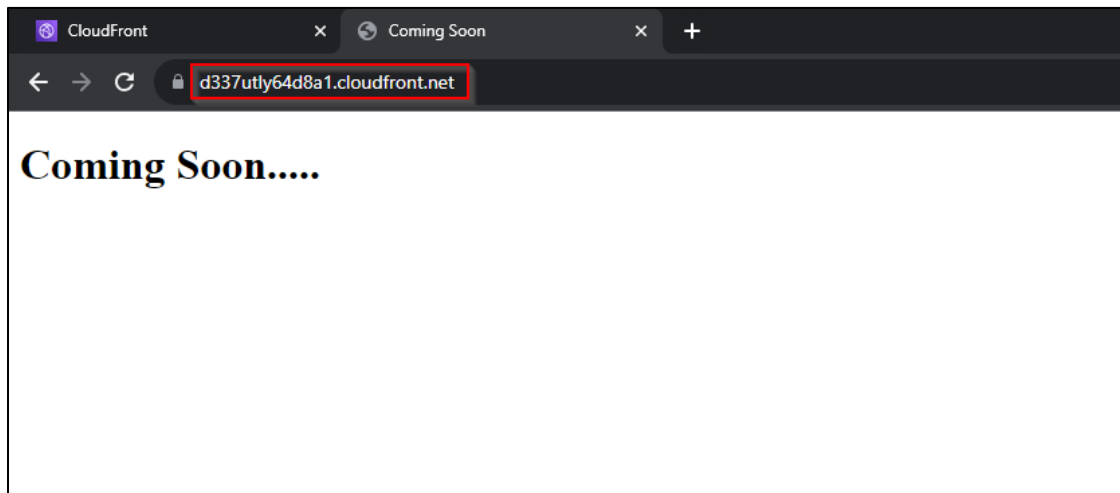
[Cancel](#) [Save changes](#)



The **Origin my-OAI-bucket** has been successfully updated.

#### 1.6 Click on **General** and copy the **Distribution domain name**



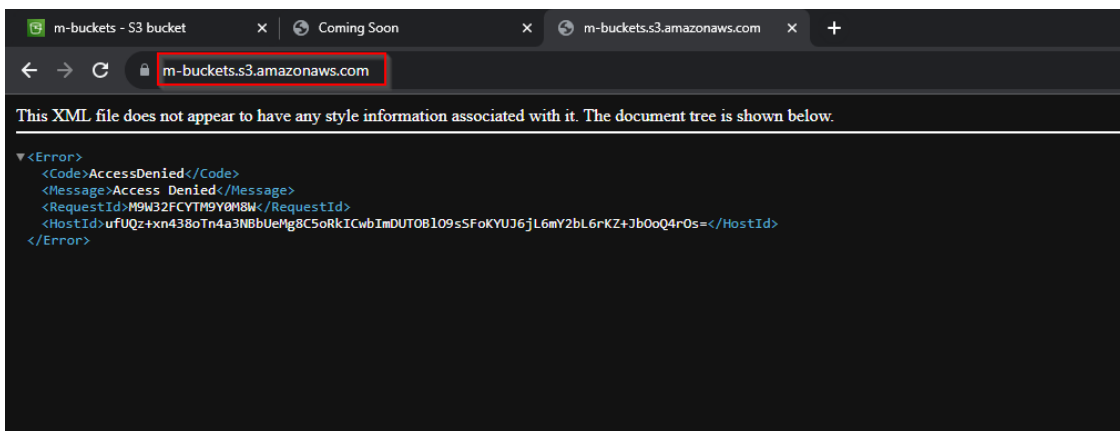


Distribution domain name is successfully deployed in the browser.

The Origin Access Identity has successfully restricted S3 access by blocking public access.

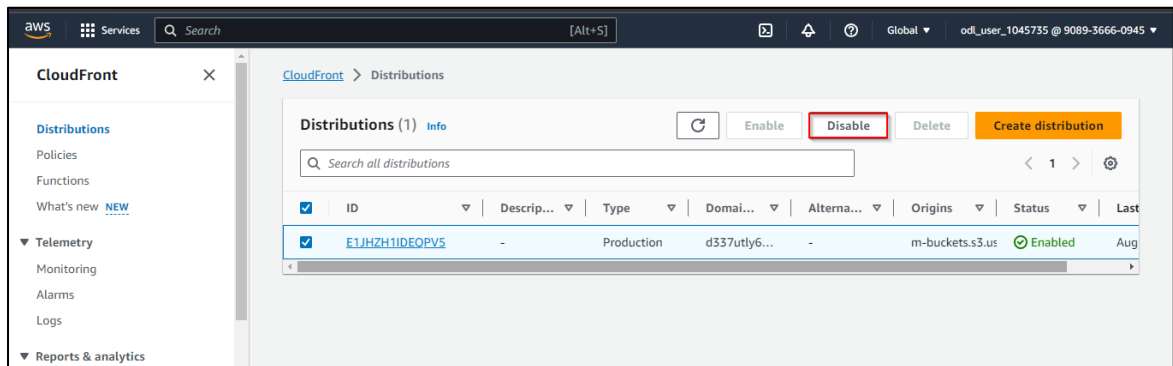
1.7 To verify if public S3 access is blocked, follow this pattern to check the S3 bucket domain link in a browser

**http:// <bucket-name>.s3.amazonaws.com**

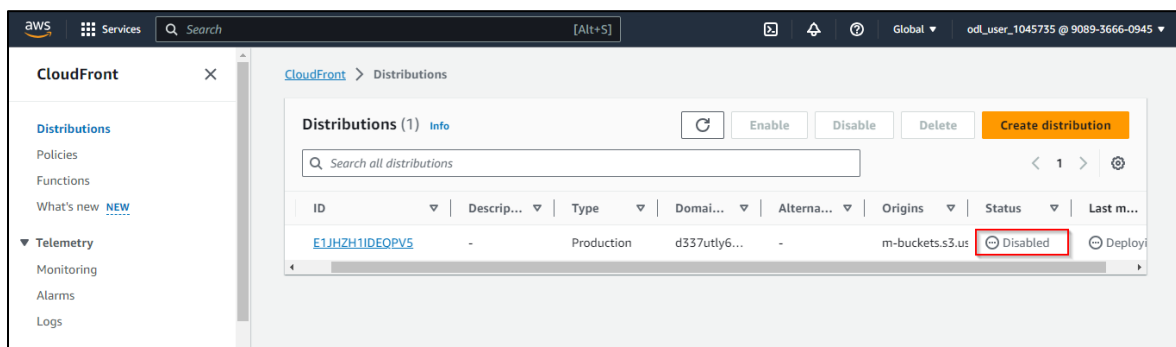
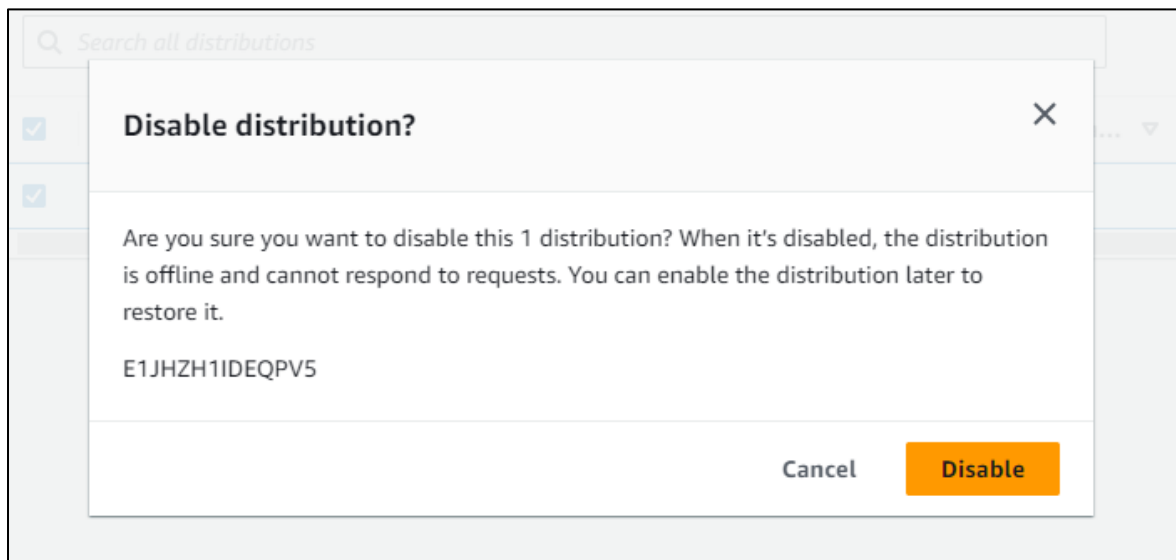


Use the S3 bucket name while creating.

## 1.8 Select the option **Disable**



## 1.9 Click on **Disable**



**CloudFront Distributions** has been successfully disabled.

By following these steps, you have demonstrated the process of configuring an Origin Access Identity to enhance security and restrict public access to an S3 bucket via CloudFront distribution.