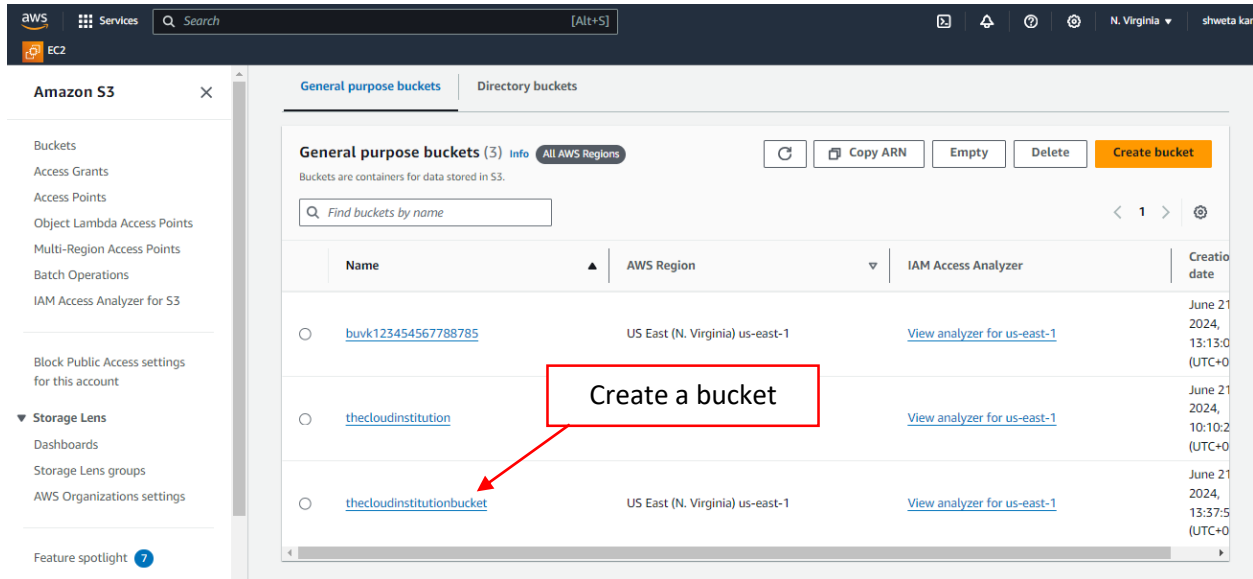
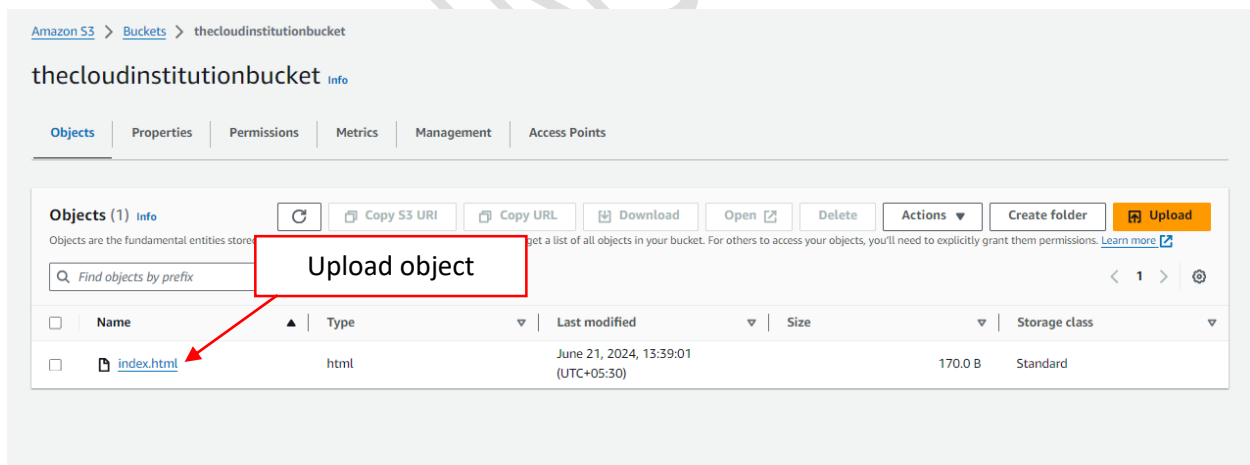


## CLOUDFRONT - SETTING UP CLOUDFRONT WITH S3 AND OAC

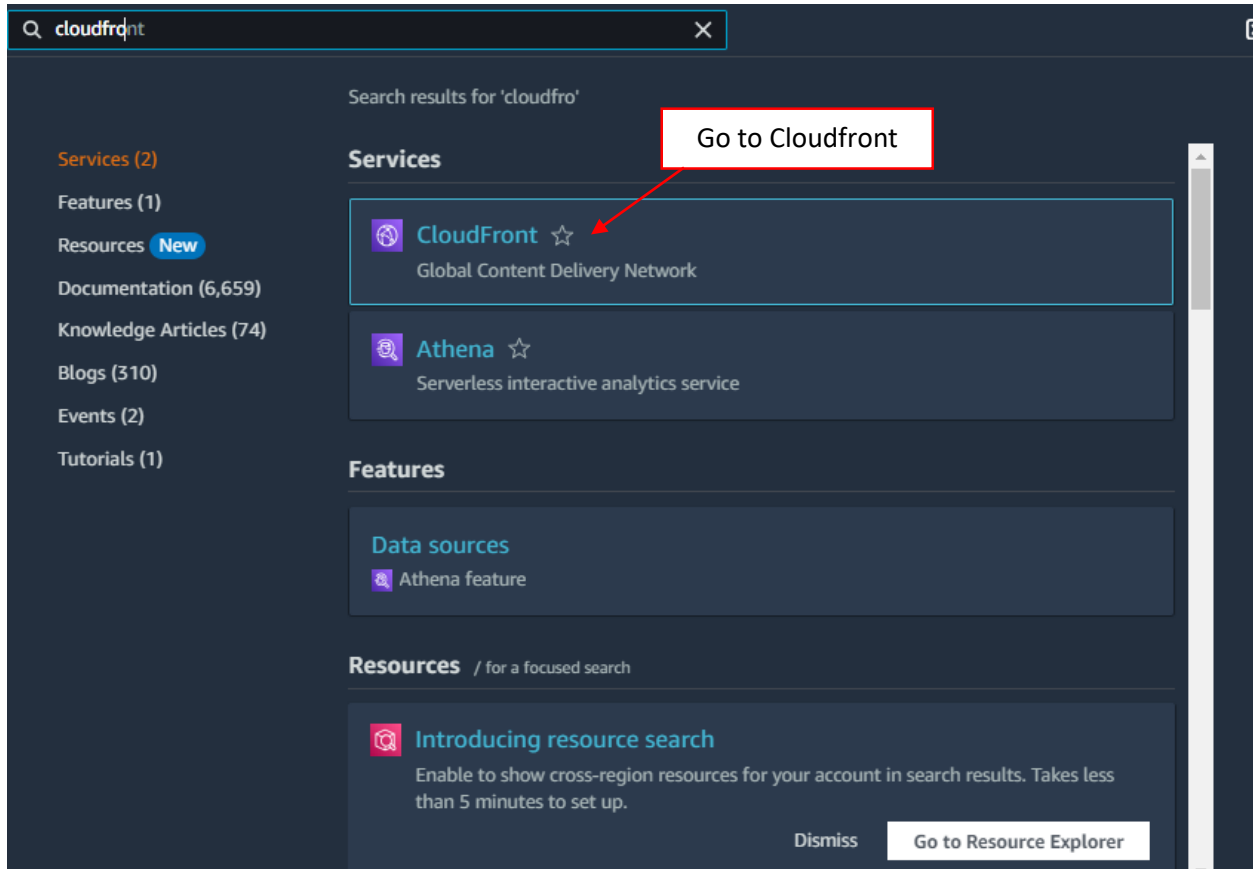
### Step 1: Create and Configure an S3 Bucket



### Upload content to the S3 bucket:



Step 2: Create a CloudFront Distribution with an OAC (Origin Access Control)



Search results for 'cloudfront'

**Services (2)**

- CloudFront** ☆  
Global Content Delivery Network
- Athena** ☆  
Serverless interactive analytics service

**Features**

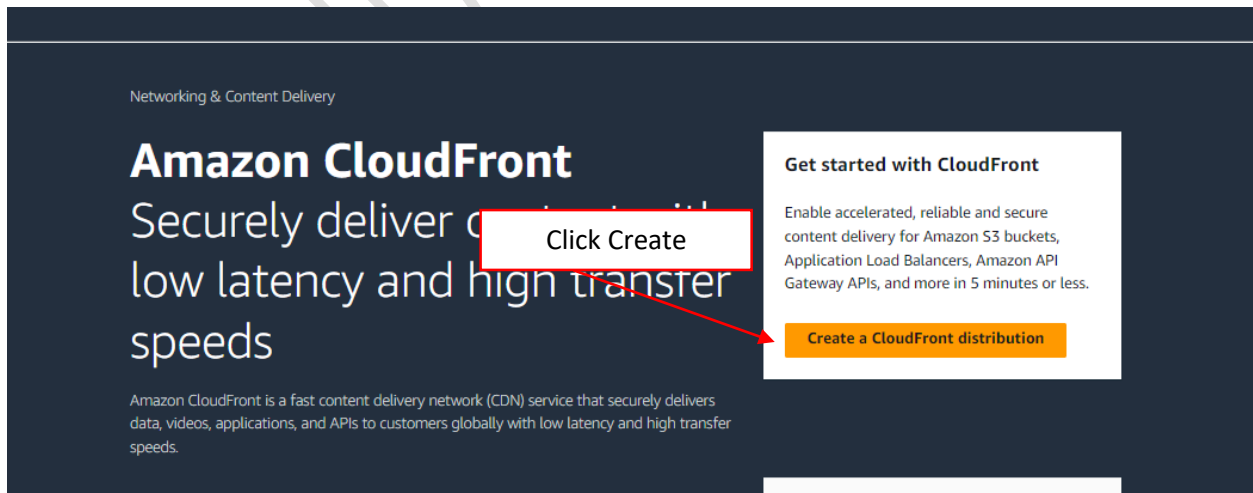
- Data sources**
  - Athena feature

**Resources** / for a focused search

**Introducing resource search**  
Enable to show cross-region resources for your account in search results. Takes less than 5 minutes to set up.

Dismiss [Go to Resource Explorer](#)

**Go to Cloudfront**



Networking & Content Delivery

# Amazon CloudFront

Securely deliver content to your users with low latency and high transfer speeds

Amazon CloudFront is a fast content delivery network (CDN) service that securely delivers data, videos, applications, and APIs to customers globally with low latency and high transfer speeds.

**Click Create**

**Get started with CloudFront**

Enable accelerated, reliable and secure content delivery for Amazon S3 buckets, Application Load Balancers, Amazon API Gateway APIs, and more in 5 minutes or less.

[Create a CloudFront distribution](#)

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

## Create distribution

### Origin

#### Origin domain

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

Q Choose origin domain

#### Amazon S3

buvk123454567788785.s3.amazonaws.com

thecloudinstitution.s3.amazonaws.com

thecloudinstitutionbucket.s3.amazonaws.com

#### Elastic Load Balancer

No origins available.

#### API Gateway

No origins available.

#### Mediastore container

No origins available.

Select the created bucket

### Origin

#### Origin domain

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

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

#### 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.

thecloudinstitutionbucket.s3.us-east-

Click on Origin access control

#### 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

Click Create new OAC

Create new OAC

CloudFront console - Create new OAC

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

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

**Signing behavior**  
☐ Do not sign requests  
☒ Sign requests (recommended)  
☐ Do not override authorization header  
Do not sign if incoming request has authorization header.

**Origin type**  
S3  
The origin type must be the same type as origin domain.

**Buttons:** Cancel, Create

**Annotation:** Click Create (with arrow pointing to the Create button)

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.

▼

**Warning:** 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.

**Enable Origin Shield**  
Origin shield is an additional caching layer that can help reduce the load on your origin and help protect its availability.  
☒ No  
☐ Yes

Let other setting be default

**Default cache behavior**

Path pattern [Info](#)

Default (\*)

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.

## Settings

### Price class [Info](#)

Choose the price class associated with the maximum price that you want to pay.

- ☒ Use all edge locations (best performance)
- ☐ Use only North America and Europe
- ☐ 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](#)

[i](#) 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).

[Choose certificate](#) ▼



[Request certificate](#) [↗](#)

### Supported HTTP versions

Add support for additional HTTP versions. HTTP/1.0 and HTTP/1.1 are supported by default.

- ☒ HTTP/2
- ☐ HTTP/3

### 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](#)

Enter the name of the object uploaded in bucket

### Standard logging

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

- ☒ Off
- ☐ On

### IPv6

- ☐ Off
- ☒ On

### Description - optional

Click Create

Cancel

Create distribution

## Distribution Created

Successfully created new distribution.

**⚠ 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

[CloudFront](#) > [Distributions](#) > E2WDSPIB008O3Y

### E2WDSPIB008O3Y

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

**Details**

Distribution domain name dlsqz9no3cgg6.cloudfront.net	ARN arn:aws:cloudfront::473869189128:distribution/E2WDSPIB008O3Y	Last modified Deploying
--	---	----------------------------

**Copy the policy**

[View metrics](#)

## Step 3: Update the S3 Bucket Policy

Go to bucket permission

[Amazon S3](#) > [Buckets](#) > thecloudinstitutionbucket

### thecloudinstitutionbucket [Info](#)

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

**Go to permissions**

**Permissions overview**

Access finding  
Access findings are provided by IAM external access analyzers. Learn more about [How IAM analyzer findings work](#)  
[View analyzer for us-east-1](#)

**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

**Bucket policy** Edit Delete

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](#)

**Public access is blocked because Block Public Access settings are turned on for this bucket**

To determine which settings are turned on, check your Block Public Access settings for this bucket. [Learn more about using Amazon S3](#)

**Click edit**

No policy to display. Copy

Bucket ARN  
arn:aws:s3:::thecloudinstitutionbucket

Policy

**Paste the policy here**

```
1 {
2   "Version": "2008-10-17",
3   "Id": "PolicyForCloudFrontPrivateContent",
4   "Statement": [
5     {
6       "Sid": "AllowCloudFrontServicePrincipal",
7       "Effect": "Allow",
8       "Principal": {
9         "Service": "cloudfront.amazonaws.com"
10      },
11      "Action": "s3:GetObject",
12      "Resource": "arn:aws:s3:::thecloudinstitutionbucket/*",
13      "Condition": {
14        "StringEquals": {
15          "AWS:SourceArn": "arn:aws:cloudfront::473869189128:distribution/E2W0SPIB00803Y"
16        }
17      }
18    }
19  ]
20 }
```

**Edit statement**

Select a statement

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

+ Add new statement





```
11      "Action": "s3:GetObject",
12      "Resource": "arn:aws:s3:::thecloudinstitutionbucket/*",
13    },
14    "Condition": {
15      "StringEquals": {
16        "AWS:SourceArn": "arn:aws:cloudfront::473869189128:distribution/E2WDSPIB008O3Y"
17      }
18    }
19  ]
20 }
```

add a new statement.

+ Add new statement

+ Add new statement

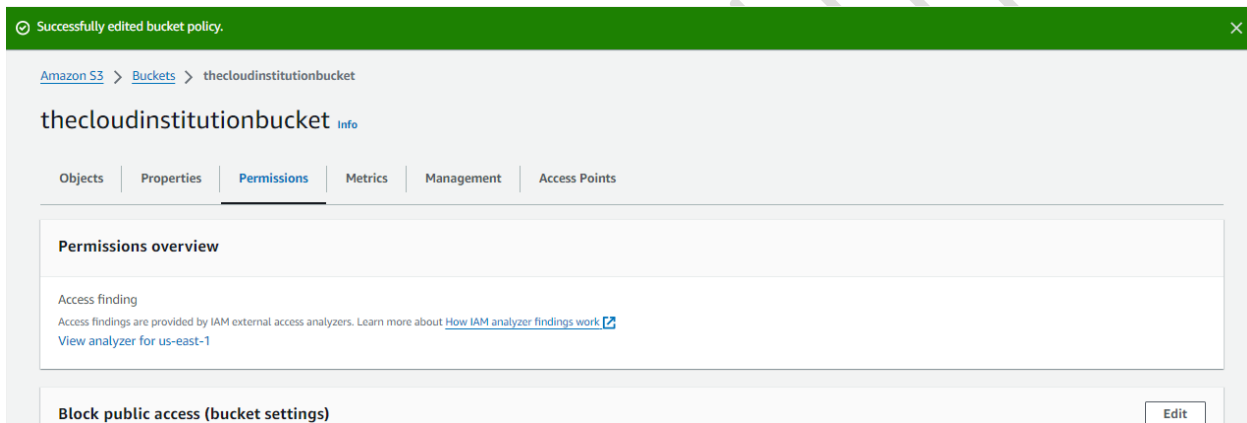
JSON Ln 20, Col 7

Security: 0 Errors: 0 Warnings: 0 Suggestions: 0

Click save

Preview external access

Cancel Save changes



Successfully edited bucket policy.

Amazon S3 > Buckets > thecloudinstitutionbucket

thecloudinstitutionbucket Info

Objects Properties Permissions Metrics Management Access Points

Permissions overview

Access finding

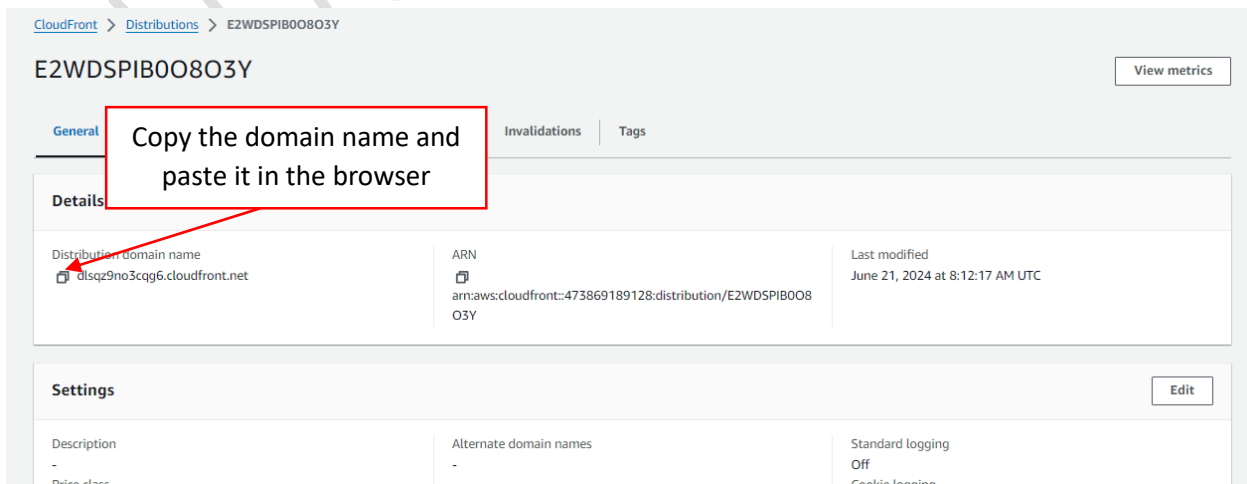
Access findings are provided by IAM external access analyzers. Learn more about [How IAM analyzer findings work](#)

[View analyzer for us-east-1](#)

Block public access (bucket settings) Edit

## Step 4: Test Access

### Go to Cloudfront




CloudFront > Distributions > E2WDSPIB008O3Y

E2WDSPIB008O3Y View metrics

General Invalidations Tags

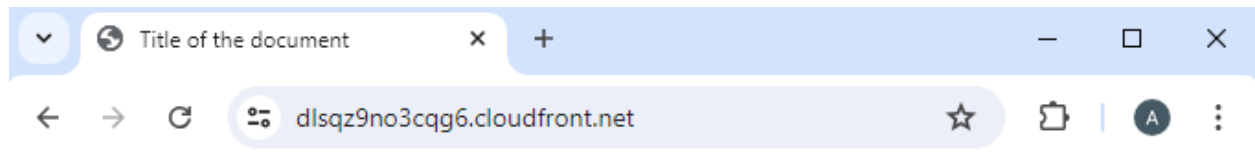
Copy the domain name and paste it in the browser

Details

Distribution domain name	ARN	Last modified
 d1sqz9no3c9g6.cloudfront.net	arn:aws:cloudfront::473869189128:distribution/E2WDSPIB008O3Y	June 21, 2024 at 8:12:17 AM UTC

Settings Edit

Description	Alternate domain names	Standard logging
-	-	Off
Price class		Cookie Invalidation



Hello..This is a sample message from Cloud Institution.....

CLOUDINSTITUTION.COM