

# Hosting a Resume Website on S3 and Linking with CloudFront

I have developed a portfolio website featuring a cloud resume and an option to download the resume in PDF format. I will now proceed to host the website on AWS by creating an S3 bucket with no public access and linking it with CloudFront to facilitate public access to the site.

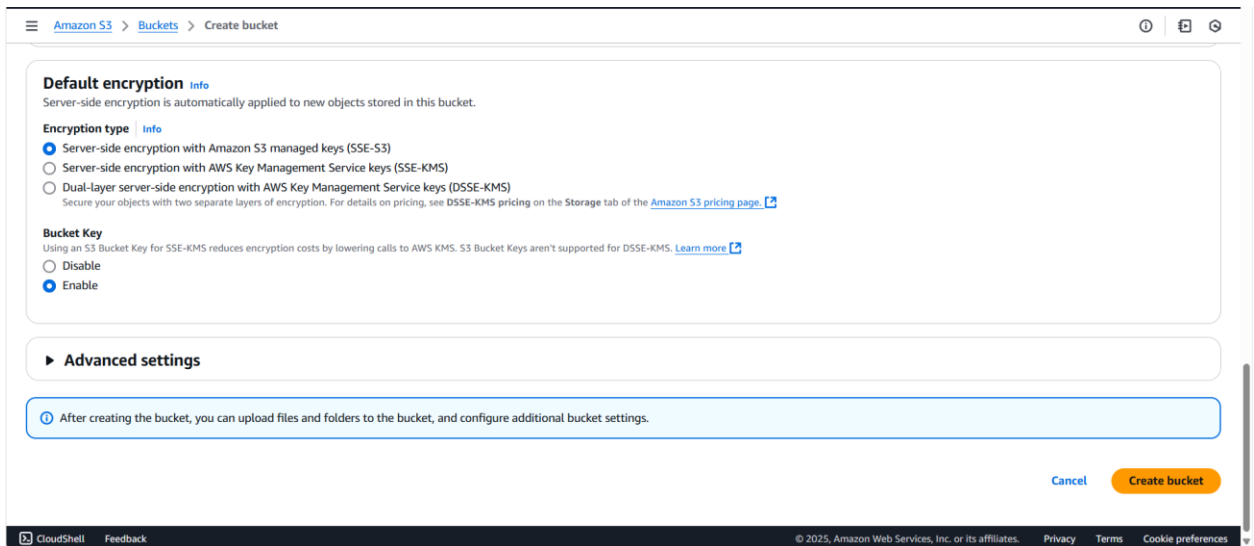
## S3 Bucket Creation

⇒ I have created an S3 bucket as demonstrated in the images below. Please refer to the screenshots for guidance while setting up your own S3 bucket.

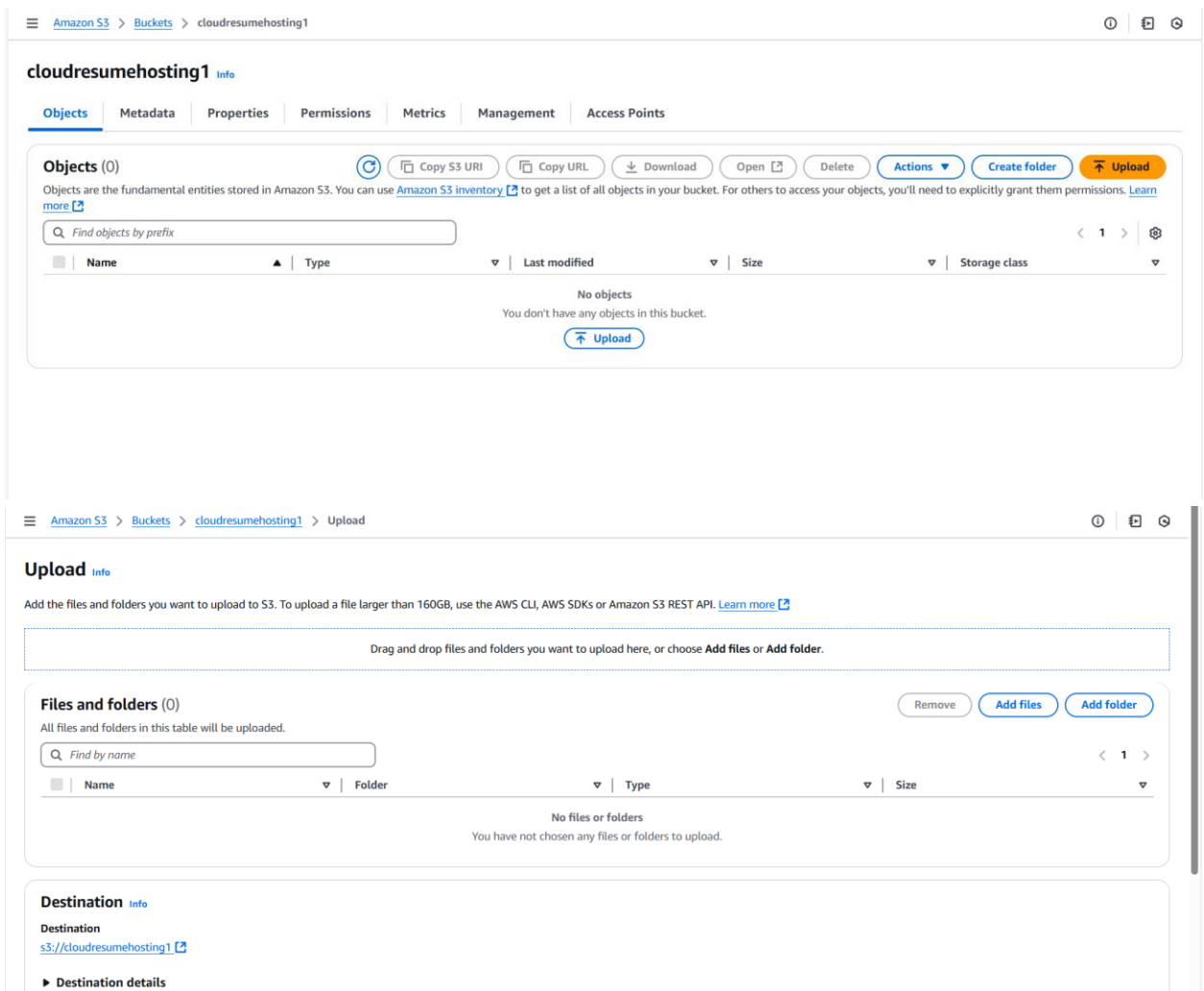
The screenshot shows the 'Create bucket' page in the Amazon S3 console. The breadcrumb navigation at the top reads 'Amazon S3 > Buckets > Create bucket'. The page title is 'Create bucket' with an 'Info' link. Below the title, it states 'Buckets are containers for data stored in S3.' The 'General configuration' section is active. Under 'AWS Region', 'US East (N. Virginia) us-east-1' is selected. Under 'Bucket type', 'General purpose' is selected with a radio button, and 'Directory' is unselected. The 'General purpose' option has a description: 'Recommended for most use cases and access patterns. General purpose buckets are the original S3 bucket type. They allow a mix of storage classes that redundantly store objects across multiple Availability Zones.' The 'Directory' option has a description: 'Recommended for low-latency use cases. These buckets use only the S3 Express One Zone storage class, which provides faster processing of data within a single Availability Zone.' The 'Bucket name' field contains 'cloudresumehosting1'. Below the field, a note states: 'Bucket names must be 3 to 63 characters and unique within the global namespace. Bucket names must also begin and end with a letter or number. Valid characters are a-z, 0-9, periods (.), and hyphens (-). [Learn More](#)'. The 'Copy settings from existing bucket - optional' section has a 'Choose bucket' button and a format example: 'Format: s3://bucket/prefix'.

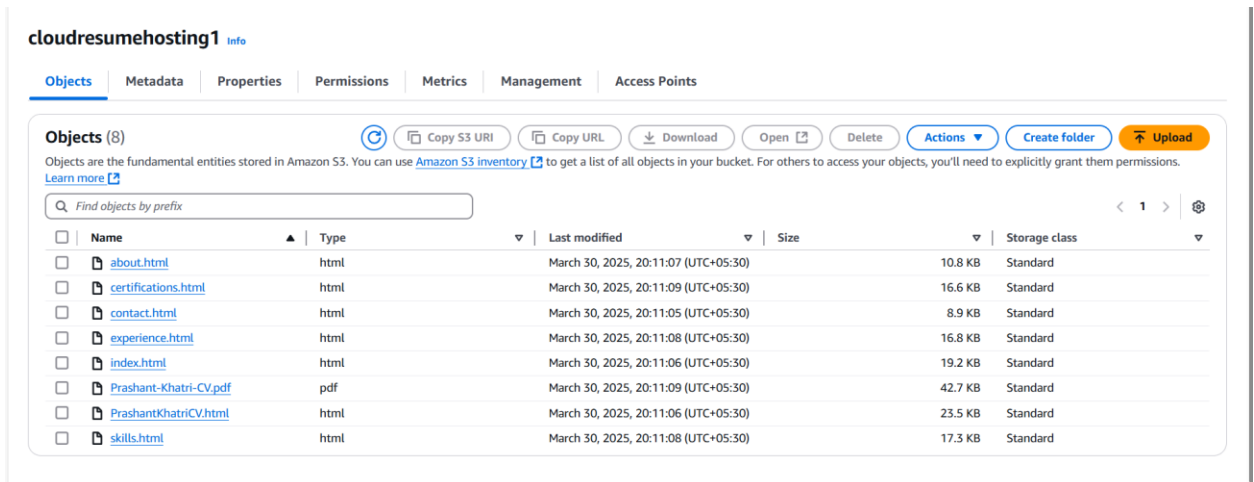
⇒ Public access for this S3 bucket will be blocked.

The screenshot shows the 'Block Public Access settings for this bucket' section of the 'Create bucket' page. The breadcrumb navigation at the top reads 'Amazon S3 > Buckets > Create bucket'. The page title is 'Object Ownership' with a 'Bucket owner enforced' subtitle. The 'Block Public Access settings for this bucket' section is active. It states: '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 this bucket and its 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 this bucket or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)'. The 'Block all public access' checkbox is checked. Below it, a note states: 'Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.' There are four sub-settings, each with a checkbox and a description: 1. 'Block public access to buckets and objects granted through new access control lists (ACLs)' with a description: '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.' 2. 'Block public access to buckets and objects granted through any access control lists (ACLs)' with a description: 'S3 will ignore all ACLs that grant public access to buckets and objects.' 3. 'Block public access to buckets and objects granted through new public bucket or access point policies' with a description: '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.' 4. 'Block public and cross-account access to buckets and objects through any public bucket or access point policies' with a description: 'S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.' The 'Bucket Versioning' section is also visible at the bottom, stating: '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](#)'.



⇒ After creating the S3 bucket, I have uploaded the content for my website as per the images shown below:

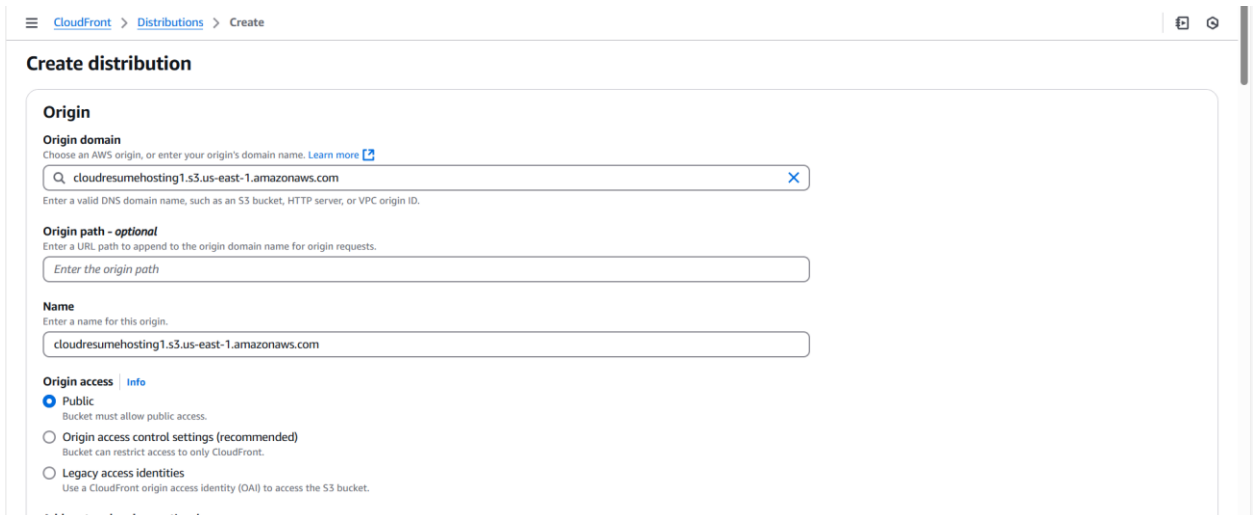




⇒ We have uploaded the required files in our S3 bucket and now this S3 bucket will act as Origin Domain for our Cloud Front Distribution.

## Establishing a CloudFront Distribution

⇒ I have established a CloudFront Distribution. Please refer to the images below for guidance.



I have created a new Origin Access Control and blocked it publicly, as shown below.

CloudFront > Distributions > Create

Name

Enter a name for this origin.

cloudresumehosting1.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 control

Select an existing origin access control (recommended) or create a new control.

Select an origin access control

Create new OAC

Add custom header - optional

CloudFront includes this header in all requests that it sends to your origin.

Add header

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

Additional settings

Create new OAC

Name

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

cloudresumehosting1.s3.us-east-1.amazonaws.com

Description - optional

The description can have up to 256 characters.

no public access

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.

Cancel

Create

CloudFront > Distributions > Create

Name

Enter a name for this origin.

cloudresumehosting1.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 control

Select an existing origin access control (recommended) or create a new control.

cloudresumehosting1.s3.us-east-1.amazonaws.com

Create new OAC

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.

Add header

Enable Origin Shield

Origin shield is an additional caching layer that can help reduce the load on your origin and help protect its availability.

Set Default Cache Behavior:

Viewer protocol policy → Choose Redirect HTTP to HTTPS.

Allowed HTTP methods → Select GET, HEAD (static sites don't need POST).

CloudFront > Distributions > Create

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

**Cache key and origin requests**

We recommend using a cache policy and origin request policy to control the cache key and origin requests.

☒ Cache policy and origin request policy (recommended)  
☐ Legacy cache settings

For the purpose I am disabling WAF (Web Application Firewall)

CloudFront > Distributions > Create

**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**

**Anycast static IP list - optional** [Info](#)

Deliver traffic from a small set of IP addresses

There are no Anycast static IP lists available

[Create an Anycast static IP list](#)

There are no Anycast static IP lists available

**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](#)

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

**Default root object - optional**

The object (file name) to return when a viewer requests the root URL (/) instead of a specific object.

index.html

**IPv6**

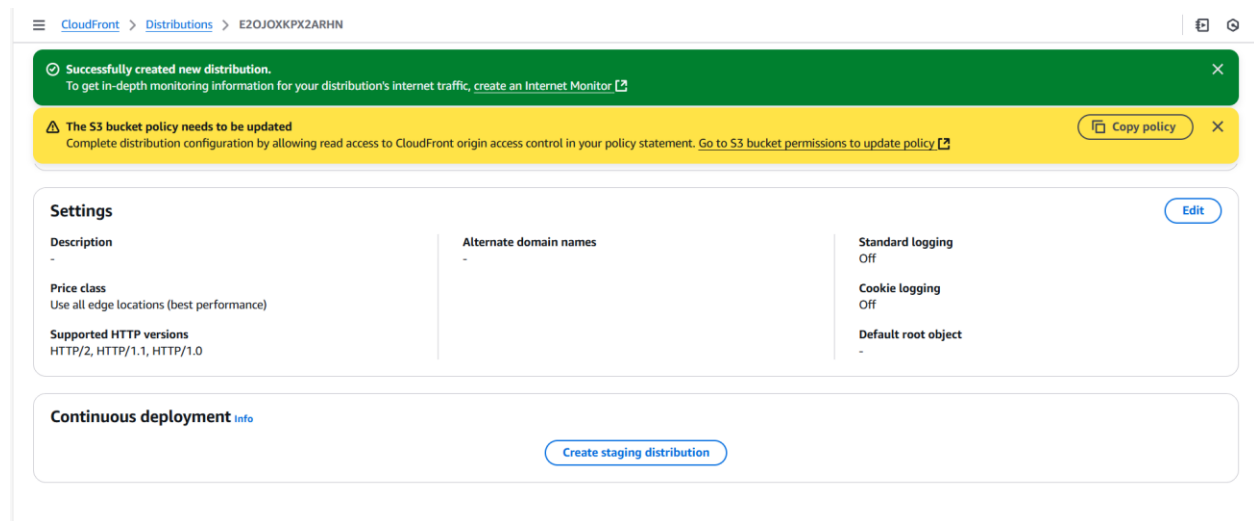
☐ Off  
☒ On

**Description - optional**

**Standard logging** [Info](#)

Additional charges may apply. See Info for more details.

Leave rest other options as default and click on “Create”

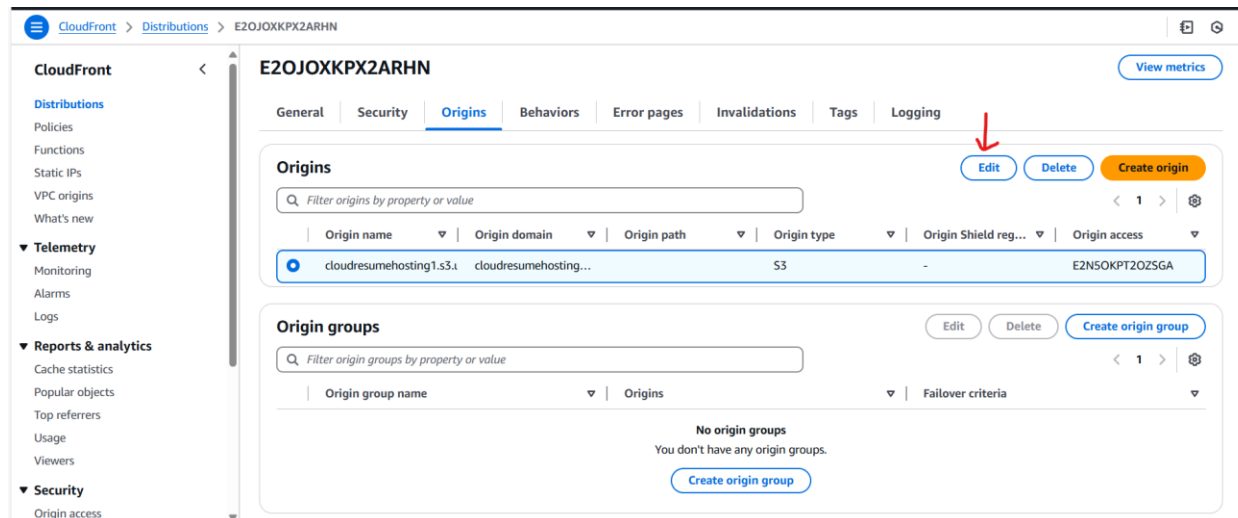


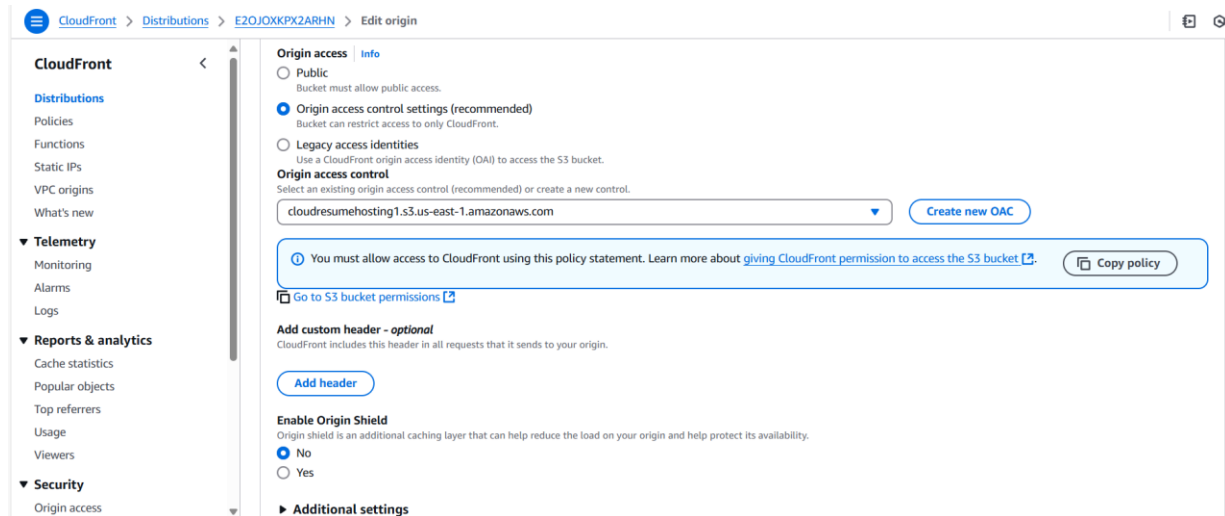
Till the time it is being deployed let's configure the Bucket permission policy so that CloudFront can access files from this private bucket.

## Configuring CloudFront for Public Access

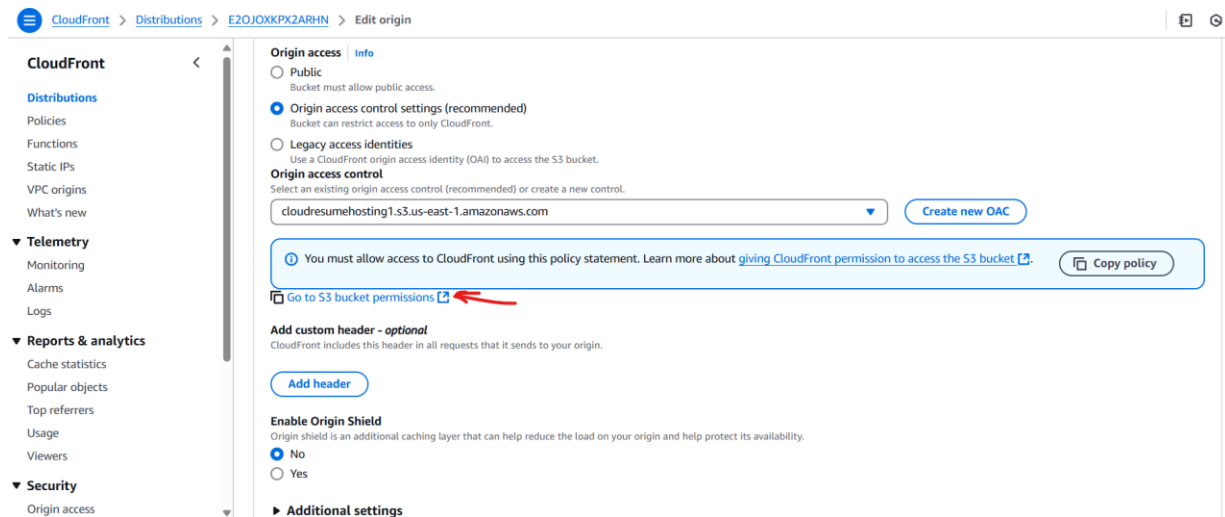
I am going to allow CloudFront to access components inside the S3 bucket while keeping the bucket private.

- ⇒ Launch Origins from the CloudFront Distribution as shown below in the images and then copy the policy under Origin Access Control to allow CloudFront to access components/files inside the S3 bucket.





⇒ Click on “Go to S3 bucket permission and then use copied policy.



⇒ Click on Edit as shown below in the images and then paste the copied policy.  
Once pasted the Json code then click on Save Changes.

Amazon S3

General purpose buckets

Directory buckets

Table 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

Feature spotlight 11

Successfully edited bucket policy.

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

```
{
  "Version": "2008-10-17",
  "Id": "PolicyForCloudFrontPrivateContent",
  "Statement": [
    {
      "Sid": "AllowCloudFrontServicePrincipal",
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudfront.amazonaws.com"
      },
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::cloudresumehosting1/*",
      "Condition": {
        "StringEquals": {
          "AWS:SourceArn": "arn:aws:cloudfront::185705888843:distribution/E2OJ0XKPX2ARHN"
        }
      }
    }
  ]
}
```

Copy

Amazon S3

General purpose buckets

Directory buckets

Table 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

Feature spotlight 11

Bucket policy

EditDelete

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 Block Public Access](#)

No policy to display.

Copy

Amazon S3

General purpose buckets

Directory buckets

Table 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

Feature spotlight 11

Bucket policy

Policy examplesPolicy generator

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](#)

Bucket ARN

arn:aws:s3:::cloudresumehosting1

Policy

```
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:::cloudresumehosting1/*",
13      "Condition": {
14        "StringEquals": {
15          "AWS:SourceArn": "arn:aws:cloudfront::185705888843:distribution/E2OJ0XKPX2ARHN"
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



**Amazon S3**

**General purpose buckets**

- Directory buckets
- Table 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

Feature spotlight 11

**cloudresumehosting1**

Security: 0 Errors: 0 Warnings: 0 Suggestions: 0 [Preview external access](#)

**You need permissions**

User: arn:aws:iam:18570588843:user/odl\_user\_1664712 is not authorized to perform: access-analyzer:ValidatePolicy on resource: arn:aws:access-analyzer:us-east-1:18570588843:\*

[Diagnose with Amazon Q](#)

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

**Successfully edited bucket policy.**

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



```
{
  "Version": "2008-10-17",
  "Id": "PolicyForCloudFrontPrivateContent",
  "Statement": [
    {
      "Sid": "AllowCloudFrontServicePrincipal",
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudfront.amazonaws.com"
      },
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::cloudresumehosting1/*",
      "Condition": {
        "StringEquals": {
          "AWS:SourceArn": "arn:aws:cloudfront:18570588843:distribution/E2OJ0XKPX2ARHN"
        }
      }
    }
  ]
}
```

[Copy](#)

⇒ Now post deployment of the CloudFront distribution copy the distribution name as shown below and access it in a browser

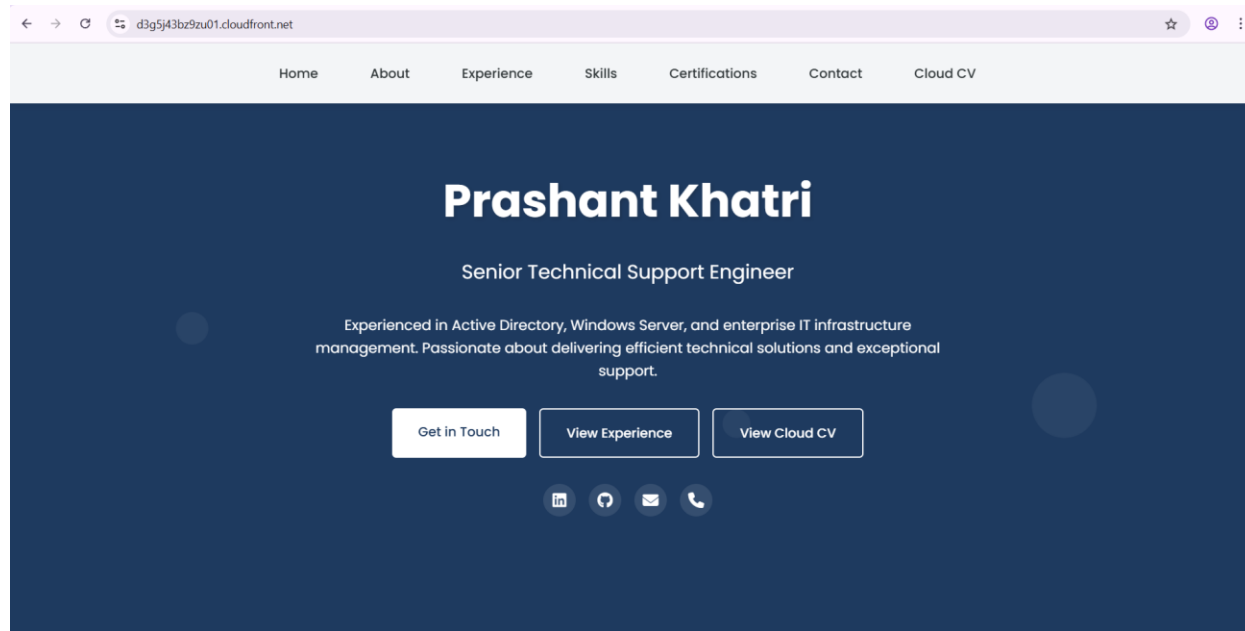
**General** | Security | Origins | Behaviors | Error pages | Invalidations | Tags | Logging

**Details**

<b>Distribution domain name</b>  d3g5j43bz01.cloudfront.net	<b>ARN</b>  arn:aws:cloudfront:961341537881:distribution/EGJKFOR7AR2TT	<b>Last modified</b> March 30, 2025 at 3:39:58 PM UTC
---	--	--

**Settings** [Edit](#)

<b>Description</b> -	<b>Alternate domain names</b> -	<b>Standard logging</b> Off
<b>Price class</b> Use all edge locations (best performance)		<b>Cookie logging</b> Off
<b>Supported HTTP versions</b> HTTP/2, HTTP/1.1, HTTP/1.0		<b>Default root object</b> index.html



Successfully create a CloudFront distribution through which the public users can access my portfolio and website while keeping the S3 bucket access private.

Note: This is all created using AWS Free tier account.