

Deploy-static-website-on-S3-bucket-and-configure-CloudFront-distribution

Case Study Problem Statement :

An organization requires a solution for hosting a static web page that ensures firewall protection, failover capabilities, geographical restrictions, and low latency access. The current infrastructure lacks the necessary security measures, redundancy, and global accessibility, leading to potential security breaches, downtime, and slow website performance. To address these concerns, the organization needs a comprehensive hosting solution that can provide robust firewall protection, automatic failover mechanisms, the ability to enforce geographical restrictions for access and ensure low latency access to the web page for users worldwide.

To address the challenges outlined in the problem statement, the following AWS services can be used to create a secure, resilient, and globally accessible hosting solution for a static web page:

Amazon S3: Hosts the static content of the web page and provides high durability and availability

AWS WAF (Web Application Firewall): To protect the web page from common web exploits. Protects against common web attacks by controlling incoming and outgoing traffic

Amazon CloudFront: To distribute the content globally, ensuring low latency and implementing geographical restrictions. A content delivery network (CDN) that caches content at edge locations, ensuring low latency access globally.

The key benefits of using Amazon S3, Amazon CloudFront, and AWS WAF for hosting a static web page include:

Enhanced Security: AWS WAF provides robust protection against web exploits and attacks, ensuring the integrity and confidentiality of the web page.

Improved Performance: CloudFront's global content delivery network ensures low latency and high transfer speeds for users around the world.

Increased Reliability: Amazon S3 offers high durability and availability for stored content, reducing the risk of data loss.

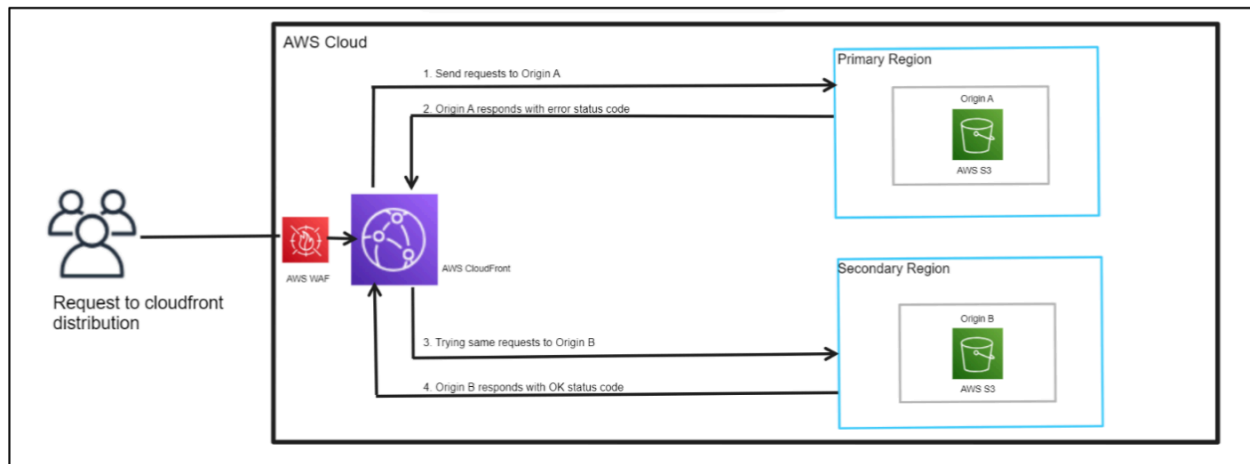
Cost savings are realized through:

Pay-as-you-go Pricing: You only pay for the services you use, without upfront costs, which can lead to significant savings.

Reduced Bandwidth Costs: CloudFront's data transfer efficiency can lower overall bandwidth costs.

No Need for Physical Infrastructure: Eliminating the need to maintain physical servers reduces operational expenses.

Architecture Diagram:



Task 1 - Creating S3 buckets

1. Created two buckets in 2 different regions
2. Capstones3ytask1 - Primary bucket in US East N.Virginia

General purpose buckets

Directory buckets

General purpose buckets (4) Info All AWS Regions

Refresh

Copy ARN

Empty

Delete

Create bucket

Buckets are containers for data stored in S3.

Find buckets by name

< 1 > ⚙

	Name ▲	AWS Region ▼	IAM Access Analyzer	Creation date ▼
<input type="radio"/>	capstones3ytask1	US East (N. Virginia) us-east-1	View analyzer for us-east-1	April 10, 2024, 20:52:31 (UTC+05:30)

3. Capstones3ytask2 -Secondary bucket in US East Ohio

General purpose buckets

Directory buckets

General purpose buckets (5) Info All AWS Regions

Refresh Copy ARN Empty Delete Create bucket

Buckets are containers for data stored in S3.

Find buckets by name

< 1 > ⚙

	Name ▲	AWS Region ▼	IAM Access Analyzer	Creation date ▼
<input type="radio"/>	capstones3ytask1	US East (N. Virginia) us-east-1	View analyzer for us-east-1	April 10, 2024, 20:52:31 (UTC+05:30)
<input type="radio"/>	capstones3ytask2	US East (Ohio) us-east-2	View analyzer for us-east-2	April 10, 2024, 20:55:11 (UTC+05:30)

4. Created an index.html page for the static website and uploaded the same file in 2 buckets

Index

10-04-2024 20:57

Chrome HTML Docu...

Uploaded index.html in both the storage buckets

capstones3ytask1 Info

Objects

Properties

Permissions

Metrics

Management

Access Points

Objects (1) Info


Refresh Copy S3 URI Copy URL Download Open Delete Actions

Create folder Upload

Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

Find objects by prefix

< 1 > ⚙

<input type="checkbox"/>	Name ▲	Type ▼	Last modified ▼	Size ▼	Storage class ▼
<input type="checkbox"/>	 Index.html	html	April 10, 2024, 21:01:20 (UTC+05:30)	25.0 B	Standard

capstones3ytask2 [Info](#)

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

Objects (1) [Info](#)

↻

Copy S3 URI

Copy URL

Download

Open

Delete

Actions ▼


Create folder

Upload

Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

Find objects by prefix

< 1 > ⚙

<input type="checkbox"/>	Name ▲	Type ▼	Last modified ▼	Size ▼	Storage class ▼
<input type="checkbox"/>	 Index.html	html	April 10, 2024, 21:01:48 (UTC+05:30)	25.0 B	Standard

Task -2: Creating a Cloud Front distribution

1. Create distribution

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

Distributions (1) [Info](#)

↻

Enable

Disable

Delete

Create distribution

Search all distributions

< 1 > ⚙

<input type="checkbox"/>	ID	Description	Type	Domain name	Alternate
--------------------------	----	-------------	------	-------------	-----------

2. Choose primary for the origin domain


Create distribution

Origin

Origin domain

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

Q capstones3ytask1.s3.us-east-1.amazonaws.com X

 This S3 bucket has static web hosting enabled. If you plan to use this distribution as a website, we recommend using the S3 website endpoint rather than the bucket endpoint.

Use website endpoint

Origin path - *optional*

Enter a URL path to append to the origin domain name for origin requests.

Enter the origin path

3. In Origin access, Select the OAI option and create a new OAI, Then select Yes, update bucket policy.

Name

Enter a name for this origin.

capstones3ytask1.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.

capstones3ytask1.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

4. Select redirect HTTP and HTTPS

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

5. Change the cache policy to caching disabled

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

Cache policy

Choose an existing cache policy or create a new one.

CachingDisabled

Policy with caching disabled



[Create cache policy](#) [View policy](#)

Origin request policy - optional

Choose an existing origin request policy or create a new one.

Select origin policy



[Create origin request policy](#)

6. DO not enable WAF and leave the remaining by default, save.

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

Task 3 - Configuring CloudFront for failover


Create Origin

[CloudFront](#) > [Distributions](#) > [E2ZBM4UEMWVT5I](#) > Create origin

Create origin

Settings

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

 This S3 bucket has static web hosting enabled. If you plan to use this distribution as a website, we recommend using the S3 website endpoint rather than the bucket endpoint.

[Use website endpoint](#)

Origin path - optional
Enter a URL path to append to the origin domain name for origin requests.

Select Secondary Bucket, select OAI, create OAI and yes, update policy

Name
Enter a name for this origin.

capstones3ytask2.s3.us-east-2.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.

capstones3ytask1.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

Leave rest as default and create Origin

CloudFront > Distributions > E2ZBM4UEMWVT5I

View metrics

E2ZBM4UEMWVT5I

General
Security
Origins
Behaviors
Error pages
Invalidations
Tags

Origins

Edit Delete Create origin

Q Filter origins by property or value

< 1 > ⚙

	Origin name ▼	Origin domain ▼	Origin path ▼	Origin type ▼	Origin Shield re... ▼	Origin access ▼
<input type="radio"/>	capstones3ytask2....	capstones3ytask2....		S3	-	origin-access-ident...
<input type="radio"/>	capstones3ytask1....	capstones3ytask1....		S3	-	origin-access-ident...

Create Origin Group

Capstones3origingroup - Origin Group name

Origins							Edit	Delete	Create origin
<input type="text" value="Filter origins by property or value"/>							< 1 > ⚙️		
	Origin name ▾	Origin domain ▾	Origin path ▾	Origin type ▾	Origin Shield re... ▾	Origin access ▾			
<input type="radio"/>	capstones3task2...	capstones3task2...		S3	-	origin-access-ident...			
<input type="radio"/>	capstones3task1...	capstones3task1...		S3	-	origin-access-ident...			

Origin groups				Edit	Delete	Create origin group
<input type="text" value="Filter origin groups by property or value"/>				< 1 > ⚙️		
	Origin group name ▾	Origins ▾	Failover criteria ▾			
<input type="radio"/>	Capstones3origingroup	capstones3task1.s3.us-east-1.amazonaws.co...	400, 403, 404, 416			

Edit the default behavior, choose the origin group name and save

Origin and origin groups

▾

Compress objects automatically [Info](#)

☐ No
☒ Yes

Viewer

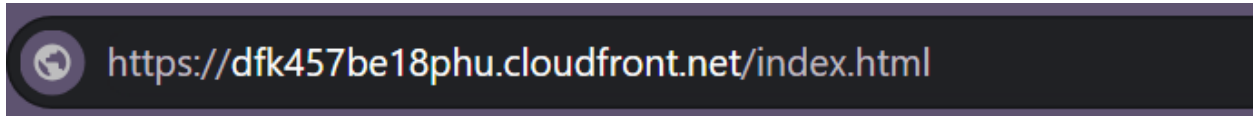
Viewer protocol policy

☐ HTTP and HTTPS
☒ Redirect HTTP to HTTPS
☐ HTTPS only

Task 4: Testing Failover

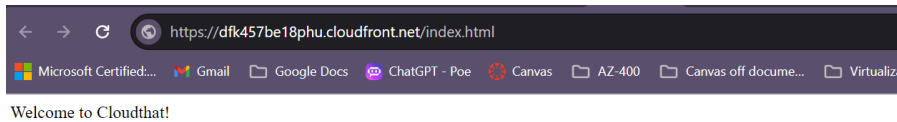
Go to Distribution, copy the Domain name

dfk457be18phu.cloudfront.net

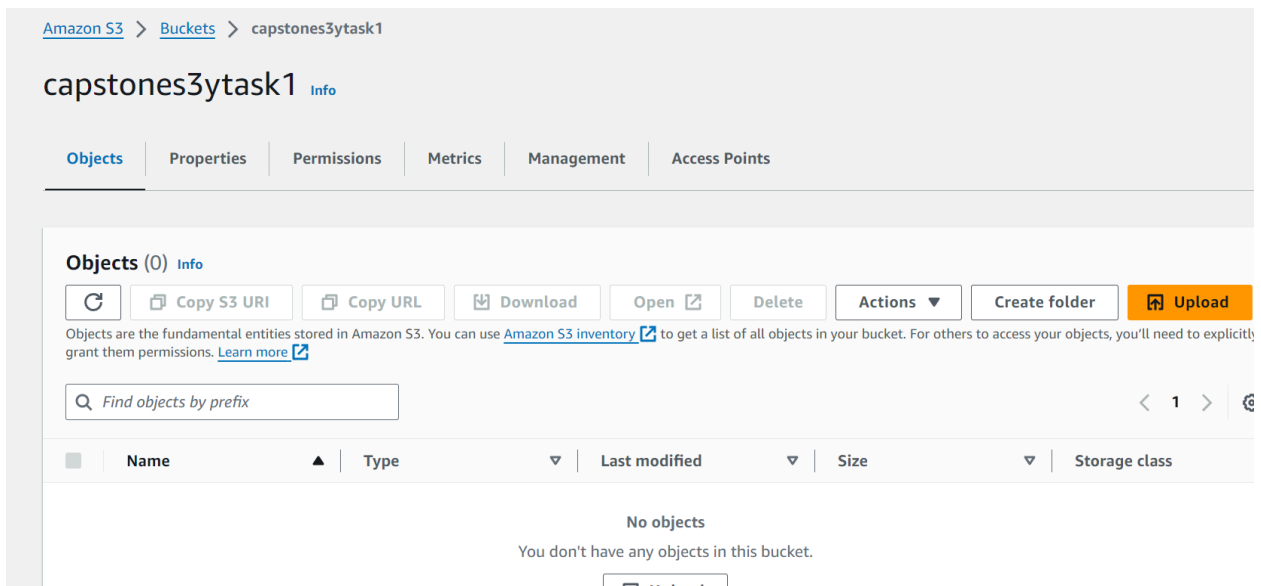


2. Paste domain name in browser and add /index.html in front of domain name.

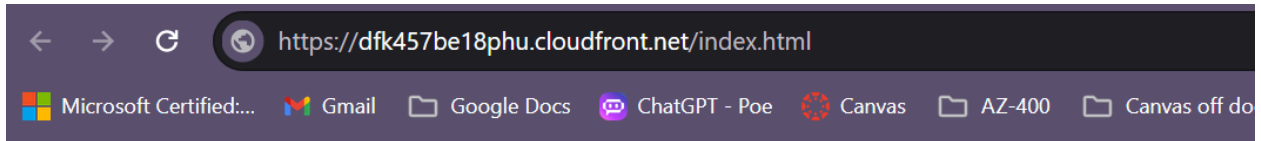
You will observe website



Deleted index file in primary bucket

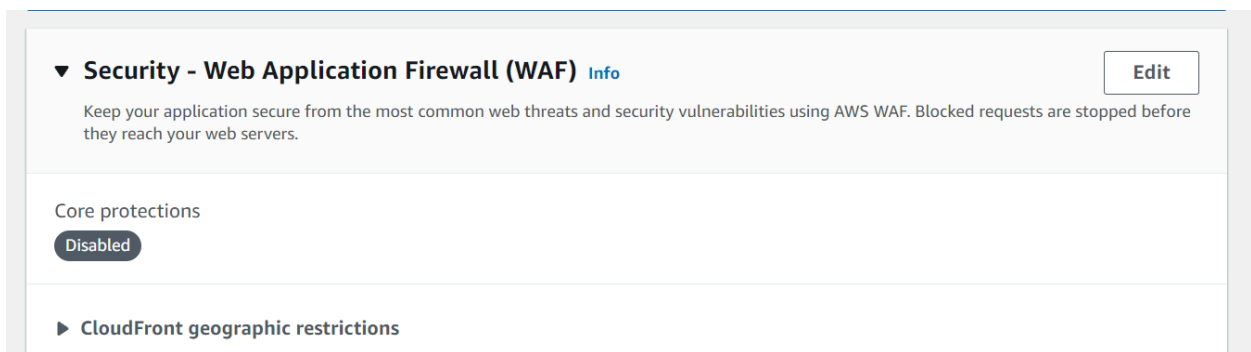


Try accessing the website again and see the results

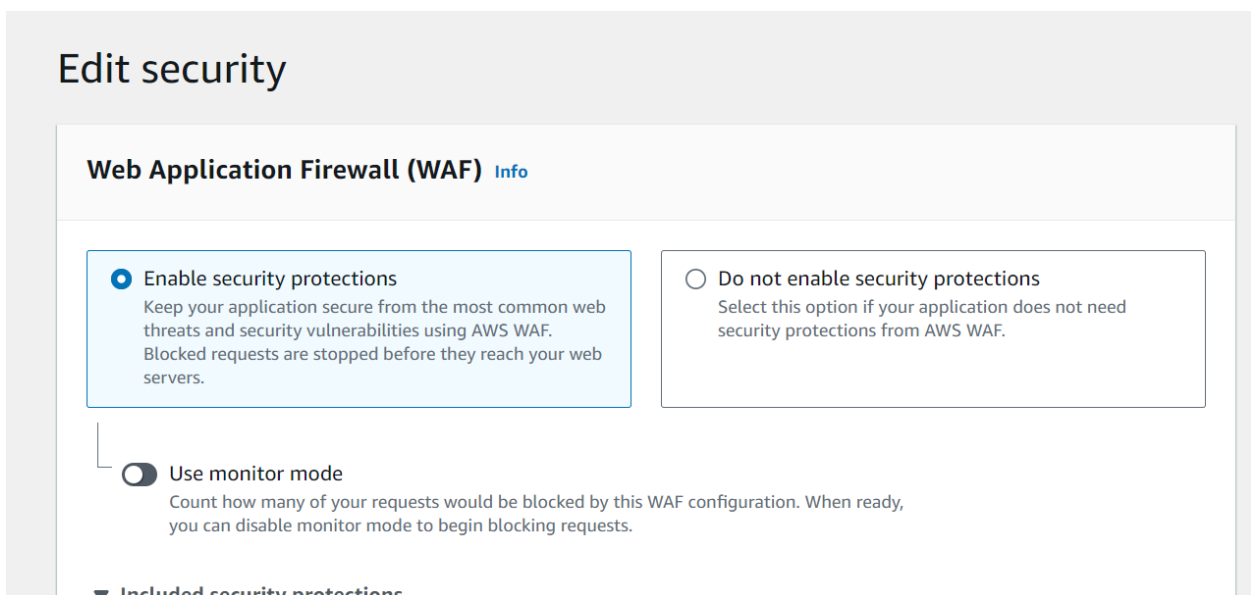


Task 5: Adding WAF to CloudFront

1. In your distribution -> go to the general tab -> In settings, click Edit.

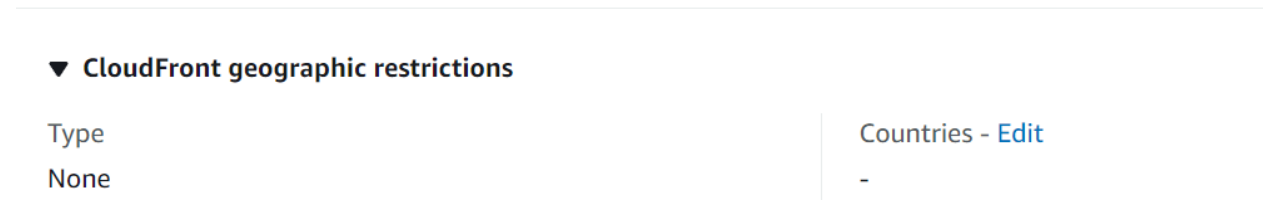


2. Enable WAF then Save changes.



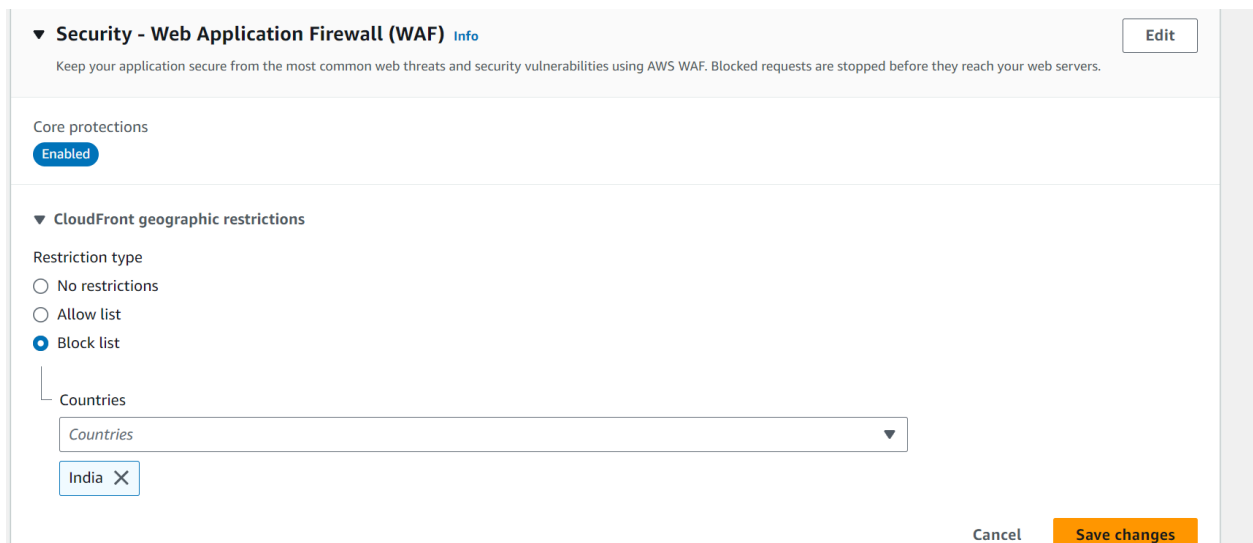
Task 6: Implementing Geo restriction

1. In your distribution -> go to the geographic restriction tab -> click Edit.



The screenshot shows the 'CloudFront geographic restrictions' configuration page. On the left, under 'Type', the value is 'None'. On the right, there is a link 'Countries - Edit' and a minus sign '-' below it.

2. Select the countries which you have to allow or block, -> Save changes. (In my case I have blocked access from India)



The screenshot shows the 'Security - Web Application Firewall (WAF)' configuration page. It includes a section for 'Core protections' with an 'Enabled' button. Below that, under 'CloudFront geographic restrictions', the 'Restriction type' is set to 'Block list'. A 'Countries' dropdown menu is shown with 'India' selected and a minus sign to its left. At the bottom right, there are 'Cancel' and 'Save changes' buttons.

3. Copy the distribution domain name and try to access it from a blocked location (You will get 403 error message)

403 ERROR

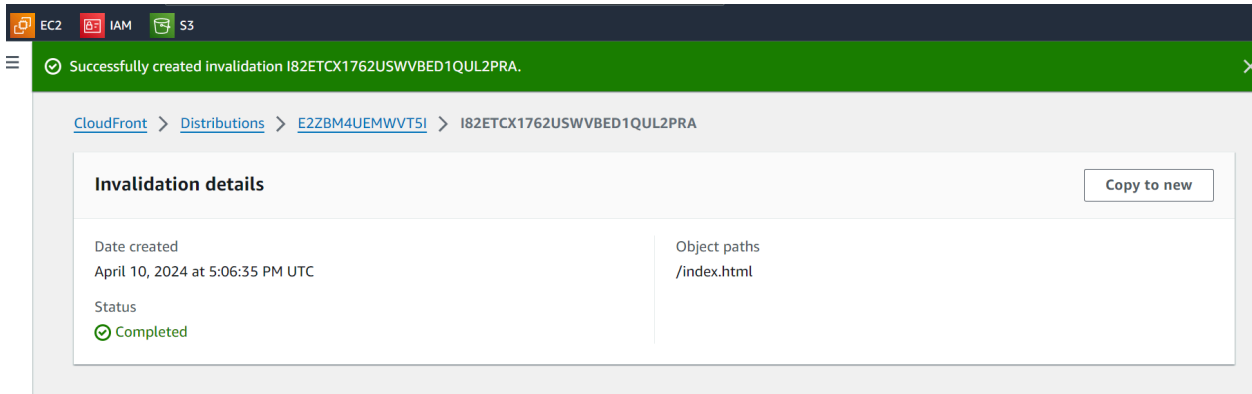
The request could not be satisfied.

The Amazon CloudFront distribution is configured to block access from your country. We can't connect to the server for this app or website at this time. There might be too much traffic or a configuration error. Try again later, or contact the app or website owner. If you provide content to customers through CloudFront, you can find steps to troubleshoot and help prevent this error by reviewing the CloudFront documentation.

Generated by cldfront (CloudFront)
Request ID: 1UCXhs117mDwyYs3yuF4vUDQUSEavhkfsoq_4xOrUOVK4df7sRWqPg==

Task 7: Invalidating data in cache

Created invalidation



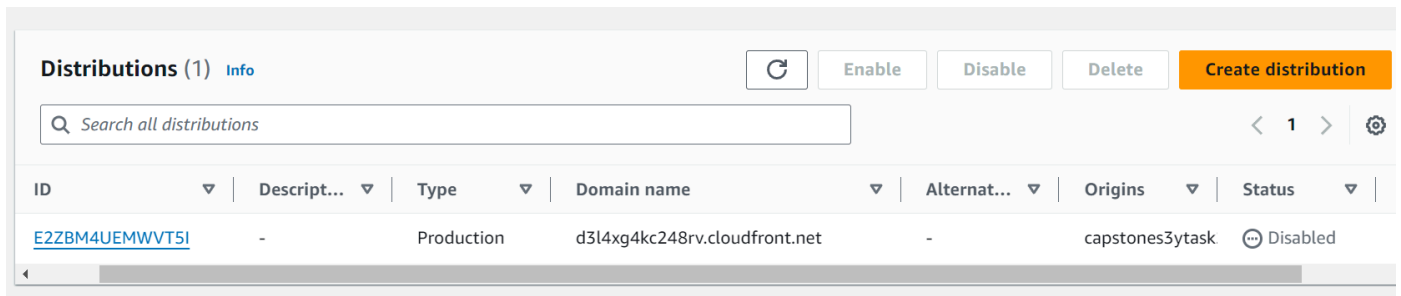
The screenshot shows the AWS CloudFront console with a green success banner at the top stating "Successfully created invalidation I82ETCX1762USWVBED1QUL2PRA." Below the banner, the breadcrumb navigation is "CloudFront > Distributions > E2ZBM4UEMWVT5I > I82ETCX1762USWVBED1QUL2PRA". The main content area is titled "Invalidation details" and contains the following information:

Invalidation details	
Date created	Object paths
April 10, 2024 at 5:06:35 PM UTC	/index.html
Status	
Completed	

A "Copy to new" button is located in the top right corner of the details section.

Task 8: Deleting resources:

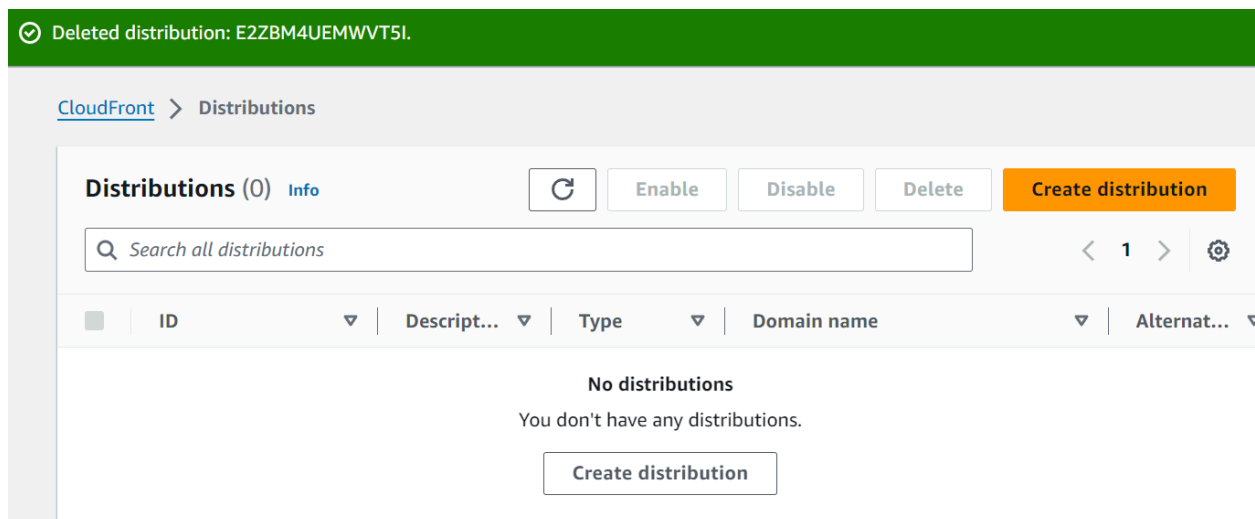
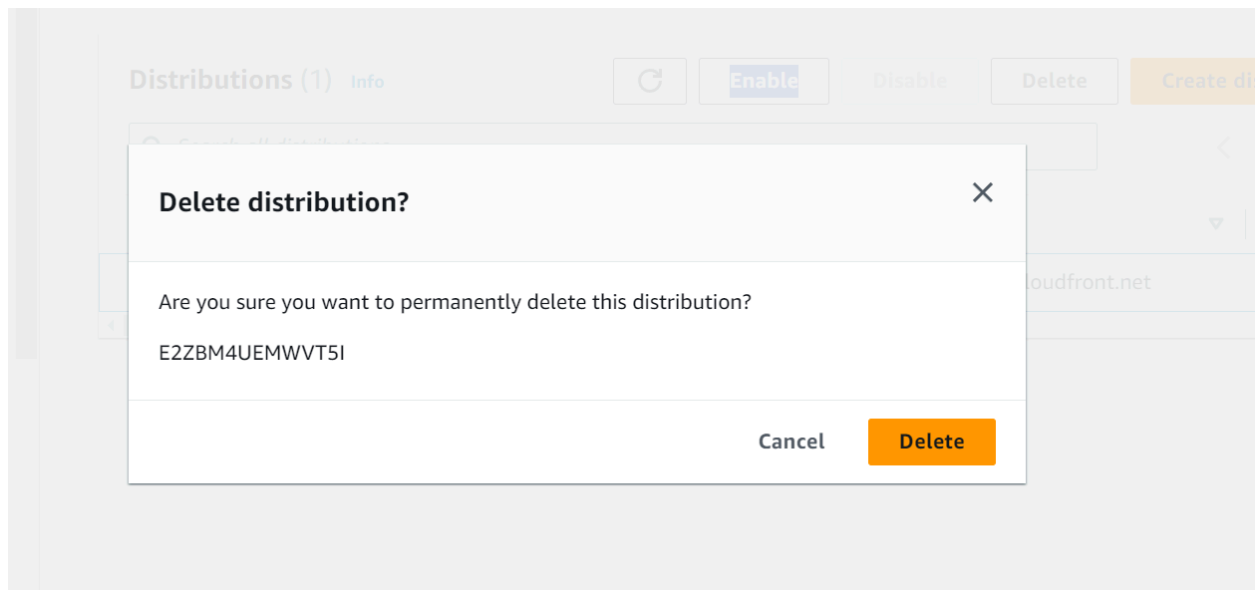
Disable distribution



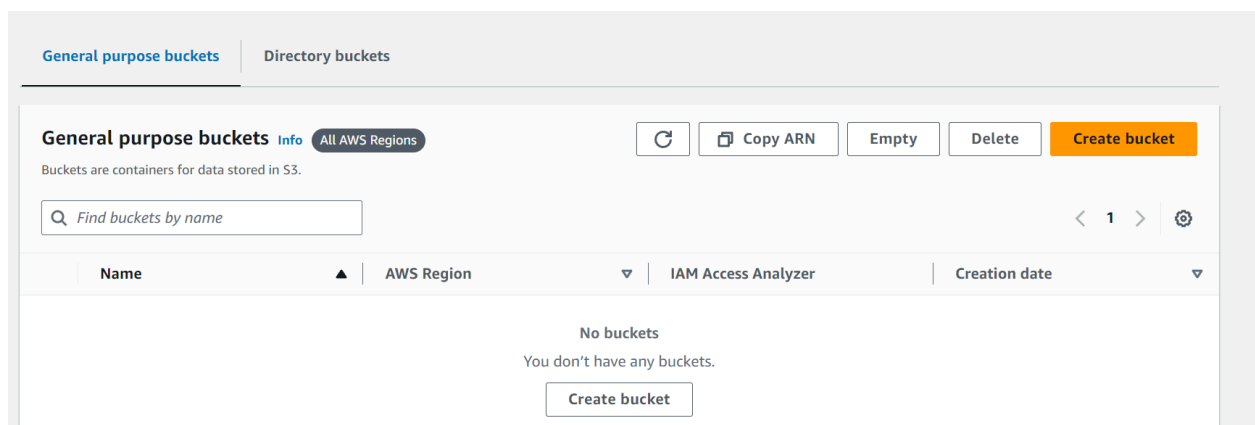
The screenshot shows the AWS CloudFront console with the "Distributions (1)" header. Above the distribution list are buttons for "Enable", "Disable", "Delete", and "Create distribution". A search bar is present with the text "Search all distributions". The distribution list table is as follows:

ID	Descript...	Type	Domain name	Alternat...	Origins	Status
E2ZBM4UEMWVT5I	-	Production	d3l4xg4kc248rv.cloudfront.net	-	capstones3ytask	Disabled

Deleted the distribution



Removed the buckets



Conclusion:

By using Amazon S3 for hosting, Amazon CloudFront for fast content delivery, and AWS WAF for security, the organization has overcome its previous challenges with a secure, reliable, and efficient web hosting solution.