

School of Computer Science, Engineering and Applications (SCSEA)

B. Tech TY (CCSA)

Subject: Cloud Architecture And Protocol

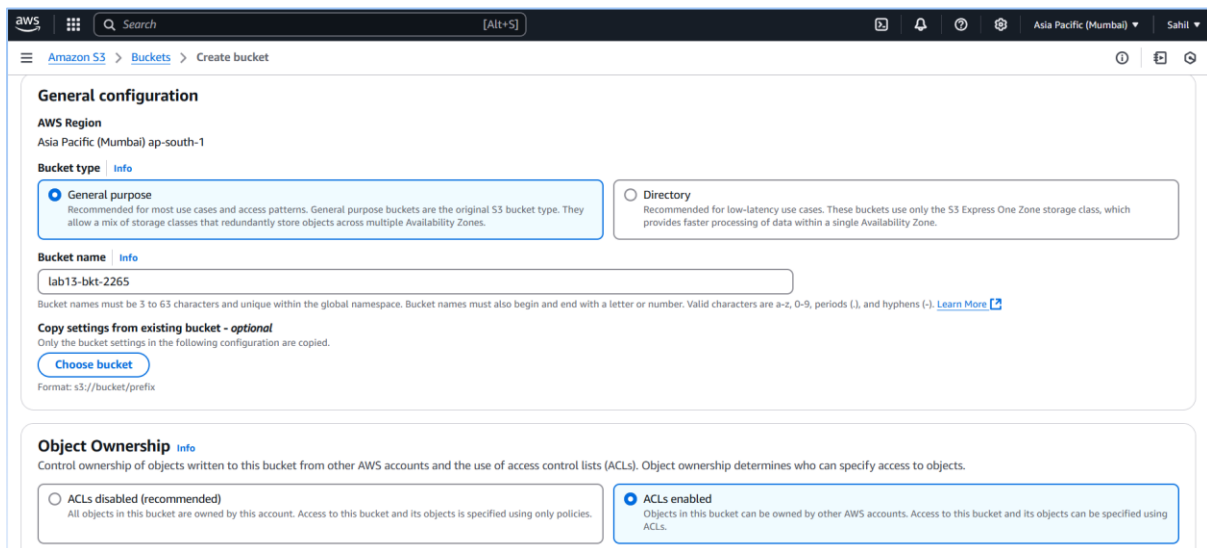
Name of the Student: Sahil S. Mandawgade

PRN: 20220802265

Title of Practical: 13. Architecting Static Web Hosting with Amazon S3 and CloudFront: Access Control, Custom Errors, and Geo-Restriction.

Step 1: Create a bucket in S3 & enable the Static Website Hosting.

- Go to S3 in AWS dashboard.
- Click on 'Create bucket'.
- Select bucket type as 'General purpose'.
- Give proper name to the bucket.
- In 'Object ownership' click on 'ACLs enabled'.



The screenshot shows the AWS S3 'Create bucket' console. Under 'General configuration', the 'AWS Region' is set to 'Asia Pacific (Mumbai) ap-south-1'. The 'Bucket type' is set to 'General purpose'. The 'Bucket name' is 'lab13-bkt-2265'. Under 'Object Ownership', 'ACLs enabled' is selected. The console also shows a 'Copy settings from existing bucket' section with a 'Choose bucket' button.

- Make 'Object ownership' as 'Object writer'.
- Make the bucket public – Untick 'Block all public access' and Tick 'I acknowledge that...'.

School of Computer Science, Engineering and Applications (SCSEA)

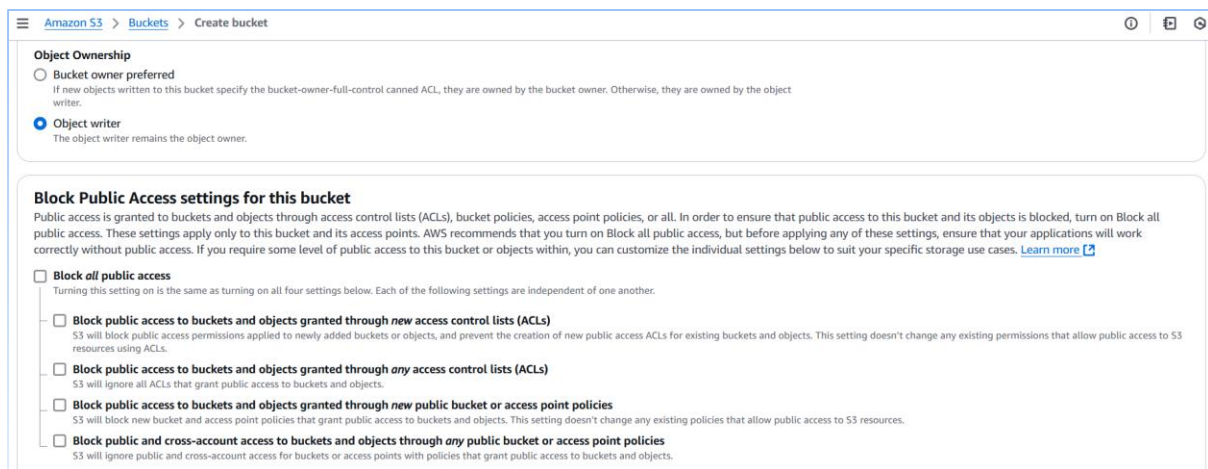
B. Tech TY (CCSA)

Subject: Cloud Architecture And Protocol

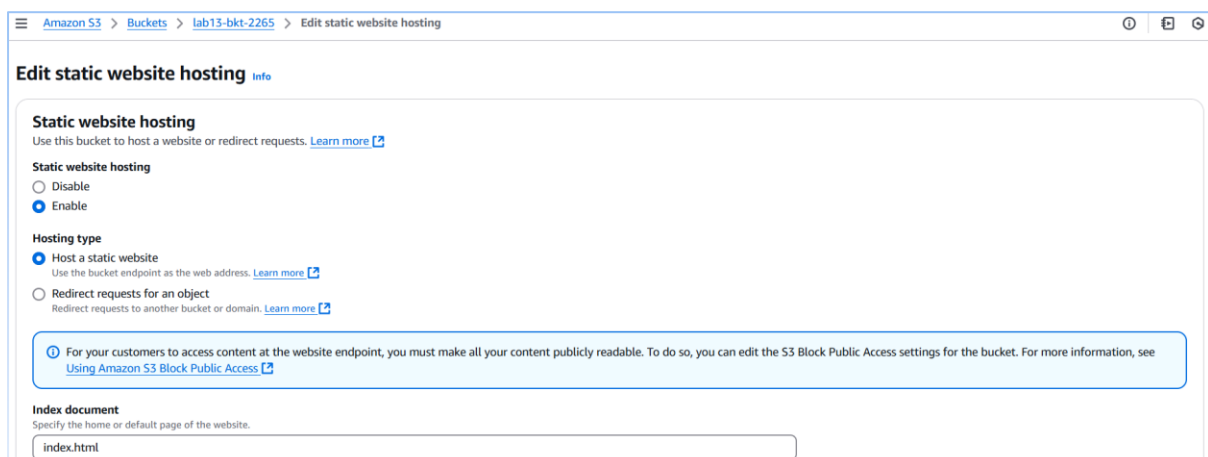
Name of the Student: Sahil S. Mandawgade

PRN: 20220802265

Title of Practical: **13. Architecting Static Web Hosting with Amazon S3 and CloudFront: Access Control, Custom Errors, and Geo-Restriction.**



- Our bucket is created successfully.
- Now, go to 'Properties' tab of bucket and click on edit button of 'Static website hosting'.
- Now, **enable the static website hosting**.
- Select hosting type as 'Host a static website'.
- Select **index document** as 'index.html'.



- Our static website hosting is enabled.

School of Computer Science, Engineering and Applications (SCSEA)

B. Tech TY (CCSA)

Subject: Cloud Architecture And Protocol

Name of the Student: Sahil S. Mandawgade

PRN: 20220802265

Title of Practical: 13. Architecting Static Web Hosting with Amazon S3 and CloudFront: Access Control, Custom Errors, and Geo-Restriction.

Step 2: Upload .html files in our S3 bucket for website hosting and edit the bucket policy.

- In our S3 bucket upload 3 .html files.
 - The index.html file which contains code for the website.
 - The error.html file which contains code to show the error page.
 - The pgnotfound.html file which contains code to show the access blocked page.

Summary

Destination

s3://lab13-bkt-2265

Succeeded

3 files, 1.1 KB (100.00%)

Failed

0 files, 0 B (0%)

Files and folders

Configuration

Files and folders (3 total, 1.1 KB)

Find by name

Name	Folder	Type	Size	Status	Error
block.html	-	text/html	67.0 B	Succeeded	-
index.html	-	text/html	1.0 KB	Succeeded	-
pgnotfound.html	-	text/html	38.0 B	Succeeded	-

- Our files have been uploaded successfully.
- Now, go to 'Permissions' tab of the bucket and edit its bucket policy.
 - Paste this policy :

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Principal": "*",
```



School of Computer Science, Engineering and Applications (SCSEA)

B. Tech TY (CCSA)

Subject: Cloud Architecture And Protocol

Name of the Student: Sahil S. Mandawgade

PRN: 20220802265

Title of Practical: 13. Architecting Static Web Hosting with Amazon S3 and CloudFront: Access Control, Custom Errors, and Geo-Restriction.

```
"Action": [  
    "s3:ListBucket"  
],  
"Resource": "<Bucket ARN>"  
},  
{  
    "Effect": "Allow",  
    "Principal": "*",  
    "Action": [  
        "s3:GetObject",  
        "s3:PutObject"  
    ],  
    "Resource": "<Bucket ARN>/*"  
}  
]  
}
```

- Click on 'Save changes'.

School of Computer Science, Engineering and Applications (SCSEA)

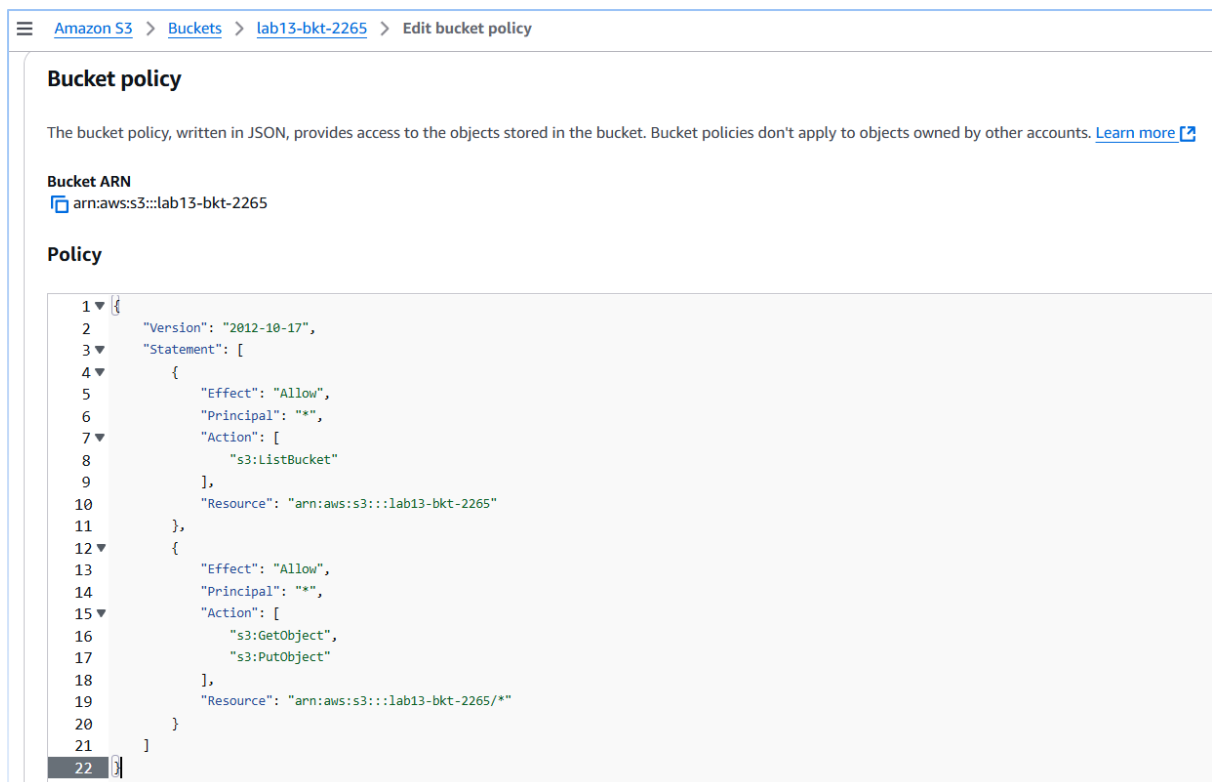
B. Tech TY (CCSA)

Subject: Cloud Architecture And Protocol

Name of the Student: Sahil S. Mandawgade

PRN: 20220802265

Title of Practical: 13. Architecting Static Web Hosting with Amazon S3 and CloudFront: Access Control, Custom Errors, and Geo-Restriction.



```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Principal": "*",
7       "Action": [
8         "s3:ListBucket"
9       ],
10      "Resource": "arn:aws:s3:::lab13-bkt-2265"
11    },
12    {
13      "Effect": "Allow",
14      "Principal": "*",
15      "Action": [
16        "s3:GetObject",
17        "s3:PutObject"
18      ],
19      "Resource": "arn:aws:s3:::lab13-bkt-2265/*"
20    }
21  ]
22 }
```

- Our bucket policy is edited successfully.

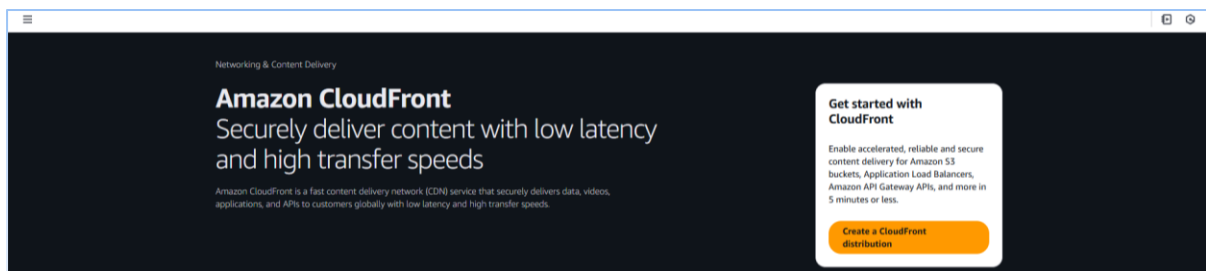
Step 3: Create a Distribution in AWS CloudFront.

- Go to Amazon CloudFront in AWS dashboard.
- Now, click on 'Create a CloudFront distribution'.

School of Computer Science, Engineering and Applications (SCSEA)
B. Tech TY (CCSA)
Subject: Cloud Architecture And Protocol

Name of the Student: Sahil S. Mandawgade **PRN:** 20220802265

Title of Practical: 13. Architecting Static Web Hosting with Amazon S3 and CloudFront: Access Control, Custom Errors, and Geo-Restriction.



- Now, choose 'Origin domain' as our bucket's domain.
- Click on 'Use website endpoint'. (If static website hosting is enabled then it will use the website domain.)
- Set protocol as '**HTTP only**'.

CloudFront > Distributions > Create

Create distribution

Origin

Origin domain
Choose an AWS origin, or enter your origin's domain name. [Learn more](#)

lab13-bkt-2265.s3-website.ap-south-1.amazonaws.com

Enter a valid DNS domain name, such as an S3 bucket, HTTP server, or VPC origin ID.

Protocol | [Info](#)

☒ HTTP only
☐ HTTPS only
☐ Match viewer

HTTP port
Enter your origin's HTTP port. The default is port 80.

80

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.

lab13-bkt-2265.s3-website.ap-south-1.amazonaws.com

- In Web Application Firewall (WAF) click on '**Do not enable security protections**'.

School of Computer Science, Engineering and Applications (SCSEA)

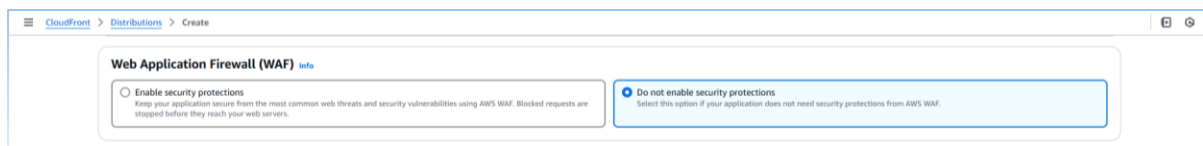
B. Tech TY (CCSA)

Subject: Cloud Architecture And Protocol

Name of the Student: Sahil S. Mandawgade

PRN: 20220802265

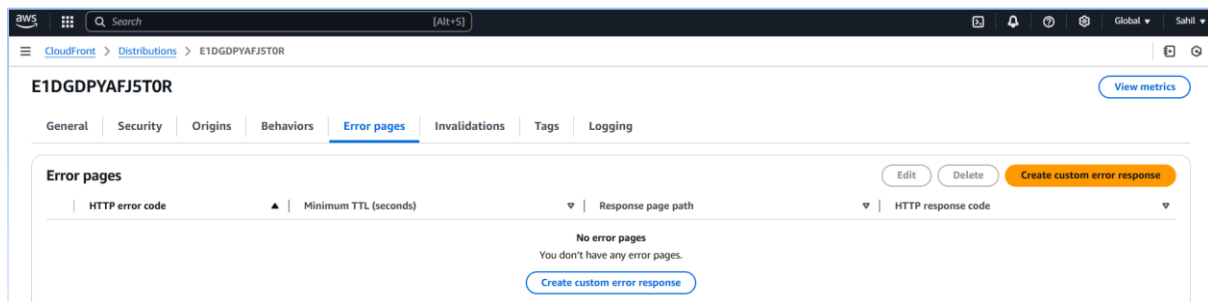
Title of Practical: 13. Architecting Static Web Hosting with Amazon S3 and CloudFront: Access Control, Custom Errors, and Geo-Restriction.



- Click on 'Create distribution'.
- Our CloudFront distribution is created successfully.

Step 4: Create custom error pages in CloudFront distribution.

- In the distribution we created, go to 'Error pages'.
- Click on 'create custom error response'.



- Create first error response for Error page.
- Select HTTP error code as '**404: Not found**'.
- Set 'Error caching minimum TTL' as '10 seconds'.
- In 'Customize error response', click on 'Yes' and in 'Response page path' give path to our error.html file in S3 bucket. – (/error.html)
- Select the HTTP response code as '404: Not found'.
- Click on 'Create custom error response'.

School of Computer Science, Engineering and Applications (SCSEA)

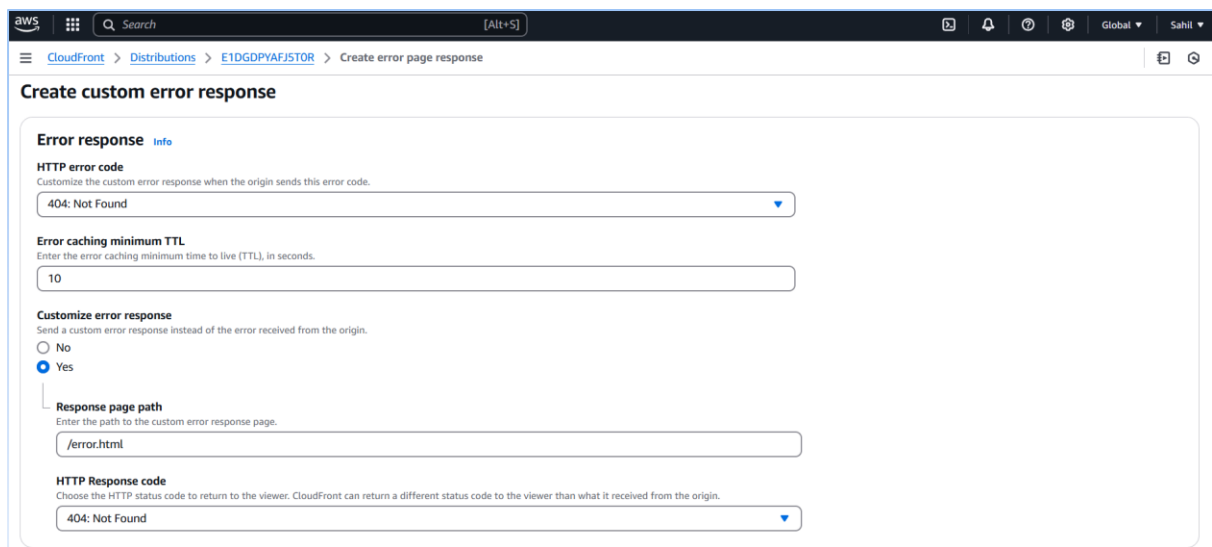
B. Tech TY (CCSA)

Subject: Cloud Architecture And Protocol

Name of the Student: Sahil S. Mandawgade

PRN: 20220802265

Title of Practical: 13. Architecting Static Web Hosting with Amazon S3 and CloudFront: Access Control, Custom Errors, and Geo-Restriction.



aws [Search] [Alt+S] Global Sahil

CloudFront > Distributions > E1DGDPAFJ5TOR > Create error page response

Create custom error response

Error response [Info](#)

HTTP error code
Customize the custom error response when the origin sends this error code.

404: Not Found

Error caching minimum TTL
Enter the error caching minimum time to live (TTL), in seconds.

10

Customize error response
Send a custom error response instead of the error received from the origin.

☐ No
☒ Yes

Response page path
Enter the path to the custom error response page.

/error.html

HTTP Response code
Choose the HTTP status code to return to the viewer. CloudFront can return a different status code to the viewer than what it received from the origin.

404: Not Found

- Create second error response for Block page.
- Select HTTP error code as '**403: Forbidden**'.
- Set 'Error caching minimum TTL' as '10 seconds'
- In 'Customize error response', click on 'Yes' and in 'Response page path' give path to our block.html file in S3 bucket. – (/block.html).
- Select the HTTP response code as '403: Forbidden'.
- Click on 'Create custom error response'.

School of Computer Science, Engineering and Applications (SCSEA)

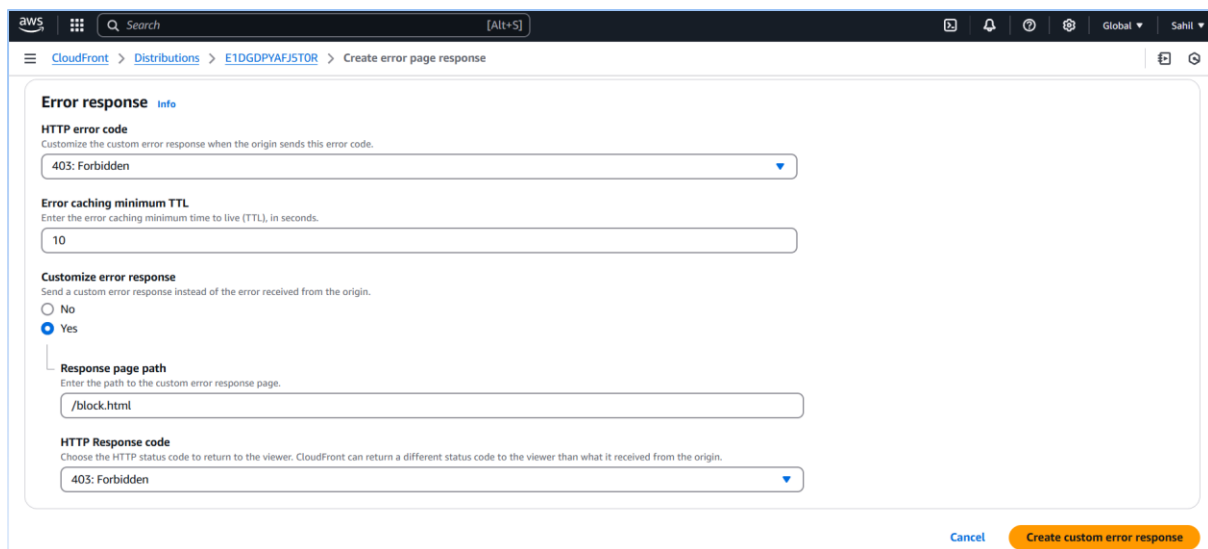
B. Tech TY (CCSA)

Subject: Cloud Architecture And Protocol

Name of the Student: Sahil S. Mandawgade

PRN: 20220802265

Title of Practical: 13. Architecting Static Web Hosting with Amazon S3 and CloudFront: Access Control, Custom Errors, and Geo-Restriction.

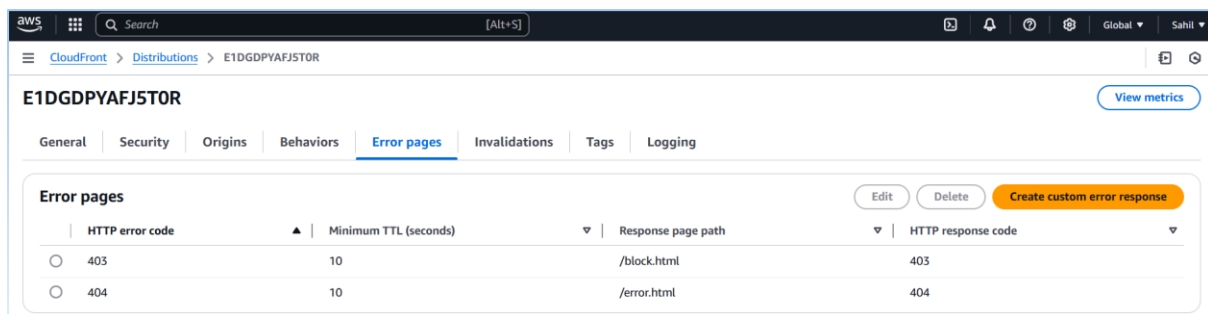


The screenshot shows the AWS CloudFront console interface for creating a custom error response. The breadcrumb navigation is CloudFront > Distributions > E1DGDYPYAFJ5TOR > Create error page response. The form includes the following fields:

- HTTP error code:** A dropdown menu with '403: Forbidden' selected.
- Error caching minimum TTL:** A text input field containing '10'.
- Customize error response:** Radio buttons for 'No' and 'Yes', with 'Yes' selected.
- Response page path:** A text input field containing '/block.html'.
- HTTP Response code:** A dropdown menu with '403: Forbidden' selected.

At the bottom right, there are 'Cancel' and 'Create custom error response' buttons.

- Our custom error pages are created successfully.



The screenshot shows the 'Error pages' tab in the AWS CloudFront console for distribution E1DGDYPYAFJ5TOR. The table lists the configured error responses:

HTTP error code	Minimum TTL (seconds)	Response page path	HTTP response code
403	10	/block.html	403
404	10	/error.html	404

Buttons for 'Edit', 'Delete', and 'Create custom error response' are visible at the top right of the table.

Step 5: Create a Web ACL in WAF with 'SQL Injection' rule in it and attach it to CloudFront distribution.

- Go to WAF & Shield in AWS dashboard.
- Now, click on 'Create web ACL'.

School of Computer Science, Engineering and Applications (SCSEA)

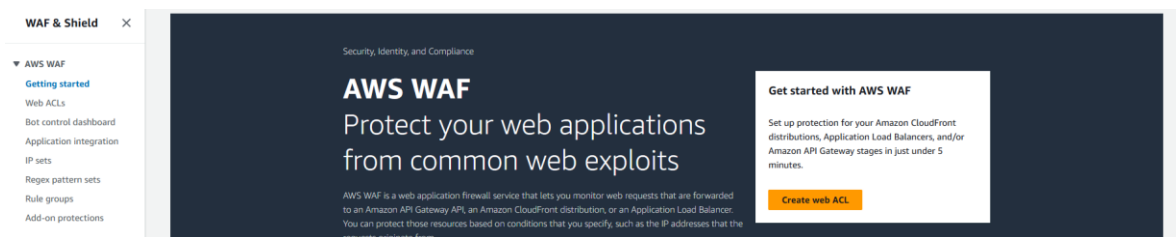
B. Tech TY (CCSA)

Subject: Cloud Architecture And Protocol

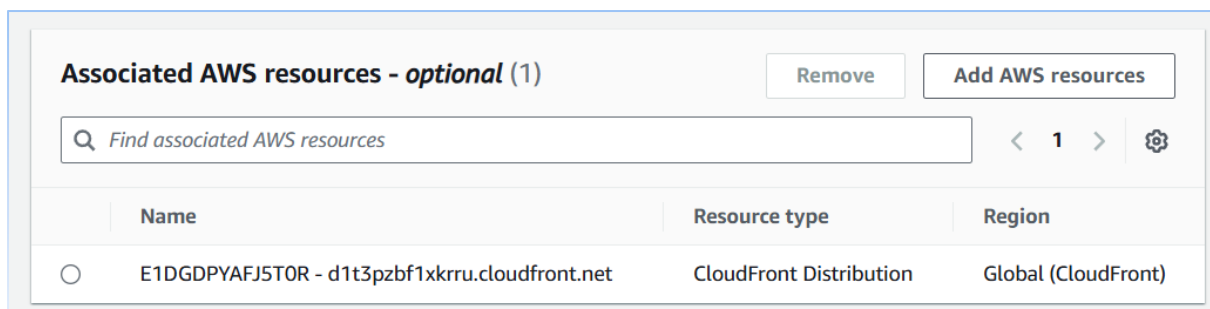
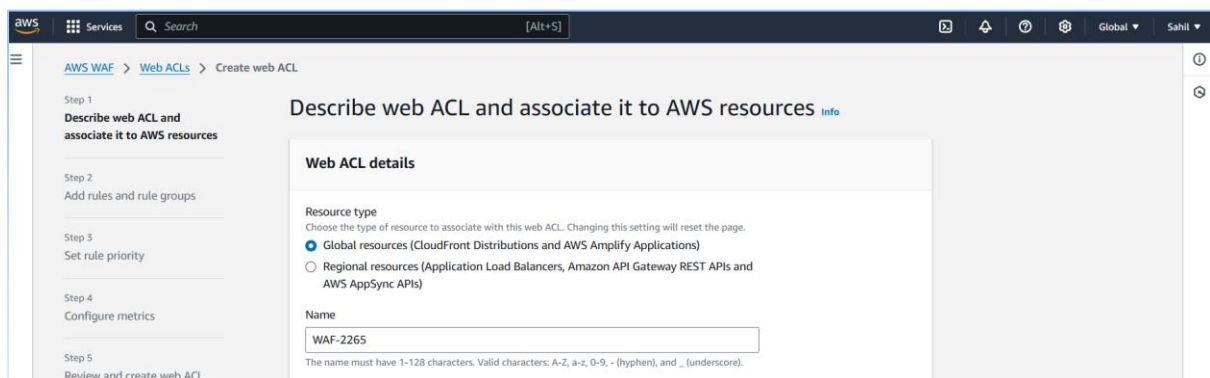
Name of the Student: Sahil S. Mandawgade

PRN: 20220802265

Title of Practical: **13. Architecting Static Web Hosting with Amazon S3 and CloudFront: Access Control, Custom Errors, and Geo-Restriction.**



- Select 'Resource type' as 'Global resources'.
- Give proper name to web ACL as 'WAF-2265'.
- In 'Associated AWS resources' add our CloudFront distribution.



- Select 'Web request body inspection' as 'Default'.
- Now, click on 'Next'.
- Click on 'Add rules' – 'Add managed rule groups' – 'AWS managed rules' – 'Free rule groups' - select the 'SQL Database' rule for protecting against SQL INJECTION.

School of Computer Science, Engineering and Applications (SCSEA)

B. Tech TY (CCSA)

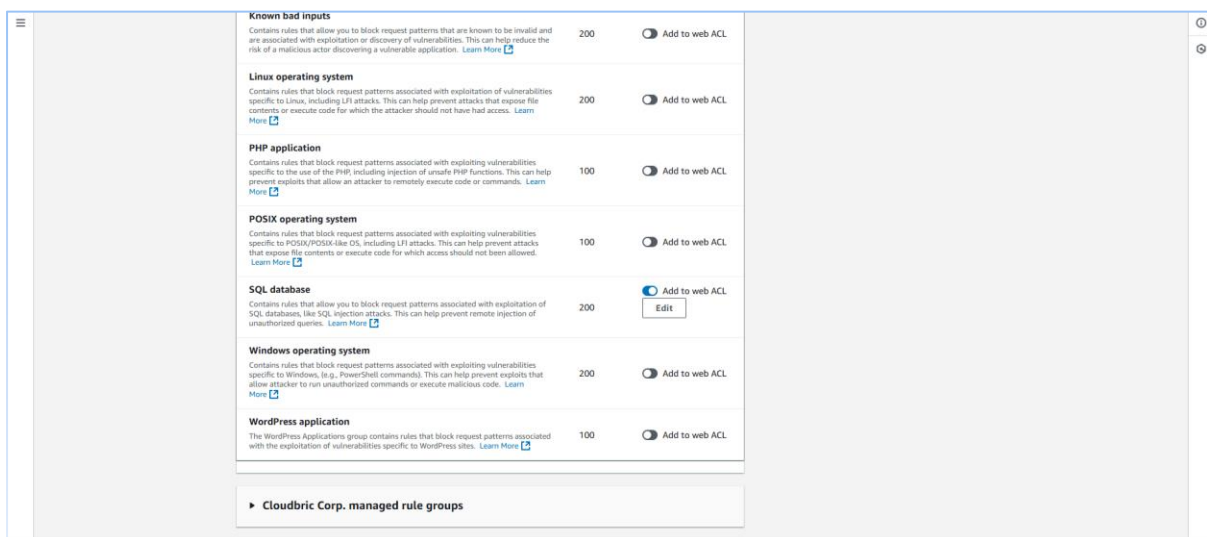
Subject: Cloud Architecture And Protocol

Name of the Student: Sahil S. Mandawgade

PRN: 20220802265

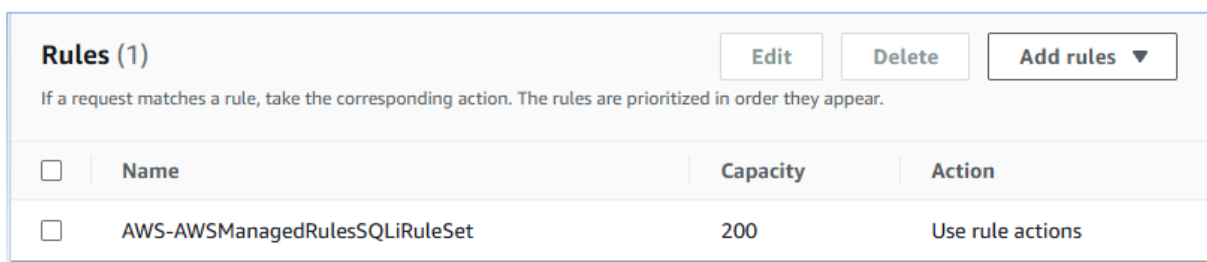
Title of Practical: 13. Architecting Static Web Hosting with Amazon S3 and CloudFront: Access Control, Custom Errors, and Geo-Restriction.

- Click on 'Add rules'.



Rule Group	Rule Name	Capacity	Action
Known bad inputs	Contains rules that allow you to block request patterns that are known to be invalid and are associated with exploitation or discovery of vulnerabilities. This can help reduce the risk of a malicious actor discovering a vulnerable application. Learn More	200	<input type="radio"/> Add to web ACL
Linux operating system	Contains rules that block request patterns associated with exploitation of vulnerabilities specific to Linux, including LFI attacks. This can help prevent attacks that expose file contents or execute code for which the attacker should not have had access. Learn More	200	<input type="radio"/> Add to web ACL
PHP application	Contains rules that block request patterns associated with exploiting vulnerabilities specific to the use of the PHP including injection of unsafe PHP functions. This can help prevent exploits that allow an attacker to remotely execute code or commands. Learn More	100	<input type="radio"/> Add to web ACL
POSIX operating system	Contains rules that block request patterns associated with exploiting vulnerabilities specific to POSIX/POSIX-like OS, including LFI attacks. This can help prevent attacks that expose file contents or execute code for which access should not be allowed. Learn More	100	<input type="radio"/> Add to web ACL
SQL database	Contains rules that allow you to block request patterns associated with exploitation of SQL databases, like SQL injection attacks. This can help prevent remote injection of unauthorized queries. Learn More	200	<input checked="" type="radio"/> Add to web ACL <input type="button" value="Edit"/>
Windows operating system	Contains rules that block request patterns associated with exploiting vulnerabilities specific to Windows, (e.g., PowerShell commands). This can help prevent exploits that allow attacker to run unauthorized commands or execute malicious code. Learn More	200	<input type="radio"/> Add to web ACL
WordPress application	The WordPress Applications group contains rules that block request patterns associated with the exploitation of vulnerabilities specific to WordPress sites. Learn More	100	<input type="radio"/> Add to web ACL

- Our rule is added successfully.



Rules (1)

If a request matches a rule, take the corresponding action. The rules are prioritized in order they appear.

<input type="checkbox"/>	Name	Capacity	Action
<input type="checkbox"/>	AWS-AWSManagedRulesSQLiRuleSet	200	Use rule actions

- Review all the settings of Web ACL.
- Click on 'Create web ACL'.
- Our WAF is created successfully.

Step 6: Check if our Website and CloudFront distribution is working propely.

- Copy the distribution domain name and paste it on the browser.

School of Computer Science, Engineering and Applications (SCSEA)

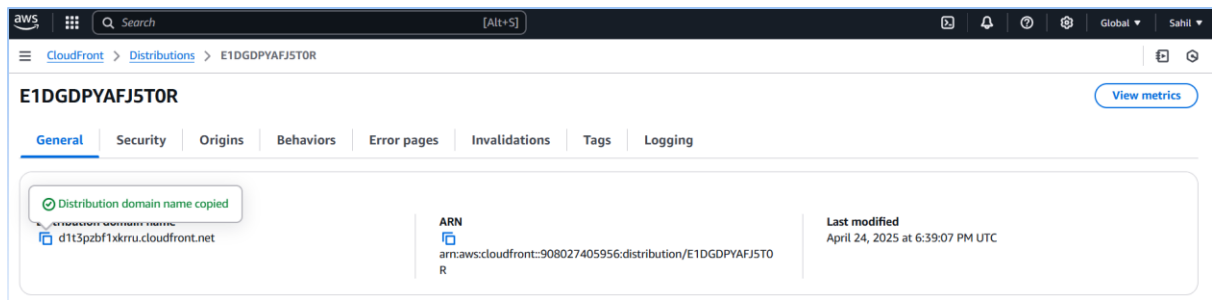
B. Tech TY (CCSA)

Subject: Cloud Architecture And Protocol

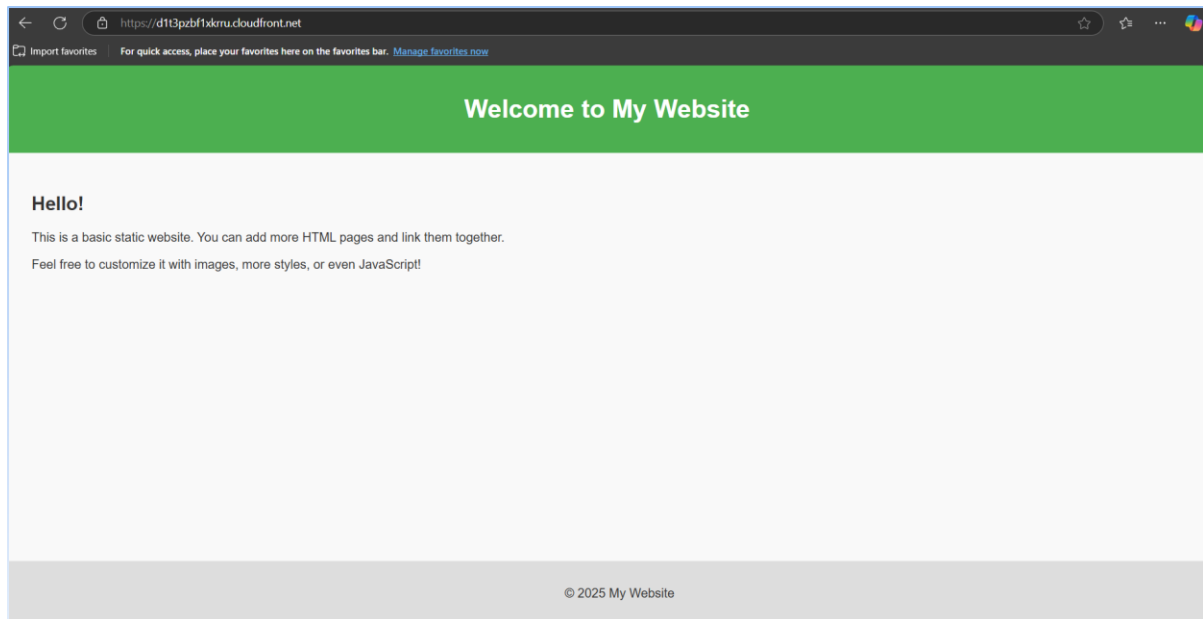
Name of the Student: Sahil S. Mandawgade

PRN: 20220802265

Title of Practical: 13. Architecting Static Web Hosting with Amazon S3 and CloudFront: Access Control, Custom Errors, and Geo-Restriction.



- Our website is working Successfully



Step 7: Add Geo-Restriction security to the CloudFront distribution.

School of Computer Science, Engineering and Applications (SCSEA)

B. Tech TY (CCSA)

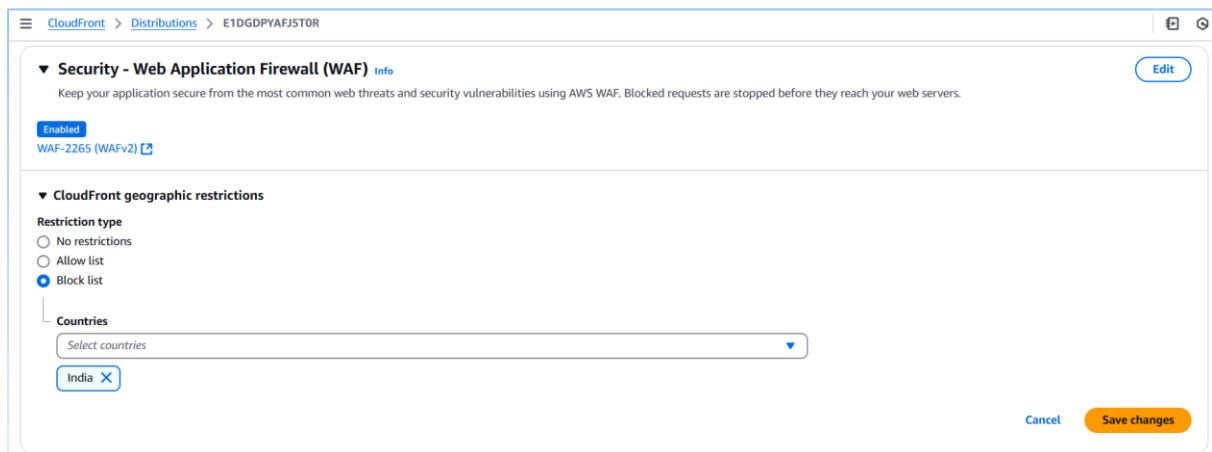
Subject: Cloud Architecture And Protocol

Name of the Student: Sahil S. Mandawgade

PRN: 20220802265

Title of Practical: 13. Architecting Static Web Hosting with Amazon S3 and CloudFront: Access Control, Custom Errors, and Geo-Restriction.

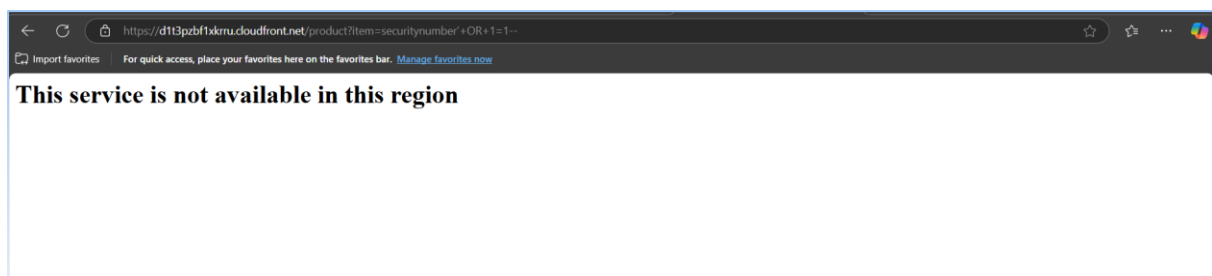
- In the distribution, go to 'Security' tab.
- Go to '**CloudFront geographic restriction**' and click on 'Edit'.
- Click on 'Block list' and select the country where we want to restrict access.
- Click on 'Save changes'.



- We have successfully added the restriction.

Step 8: Check if the WAF and the Geo-restriction enabled on distribution is working or not.

- Copy the distribution domain name and paste it on the browser.
- After pasting add '**/product?item=securitynumber'+OR+1=1--**' to our domain.



School of Computer Science, Engineering and Applications (SCSEA)

B. Tech TY (CCSA)

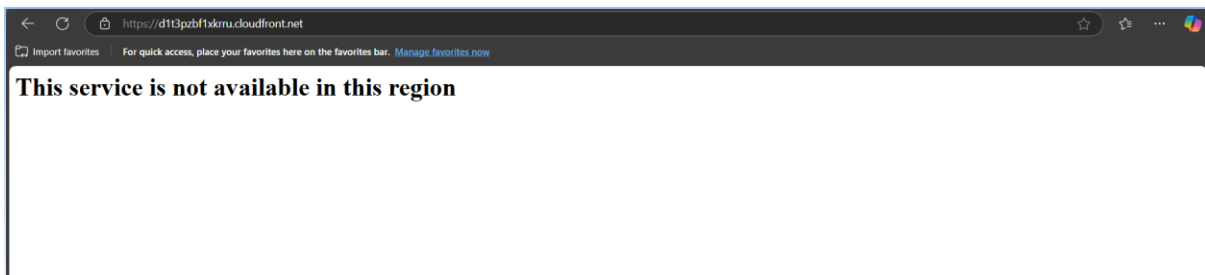
Subject: Cloud Architecture And Protocol

Name of the Student: Sahil S. Mandawgade

PRN: 20220802265

Title of Practical: 13. Architecting Static Web Hosting with Amazon S3 and CloudFront: Access Control, Custom Errors, and Geo-Restriction.

- The '403: Forbidden' error shows that our WAF is working successfully.
- Now try to access our distribution domain name through INDIA.



- The '403: Forbidden' error shows that our Geo-Restriction is working Successfully.

Step 9: Try to access the website by typing something in the distribution domain name and see if the error occurs or not.

- Copy the distribution domain name and paste it on the browser.
- After pasting add '/sahil=2265' to our domain.

[NOTE]: Before checking this step, disable the Geo-restriction access in the security]



The '404 Not found' error shows that our Error Page is working successfully.