Hosting a Static website on S3 and making a Cloud Front distribution and making WAF configuration

Made by: Salma Salah

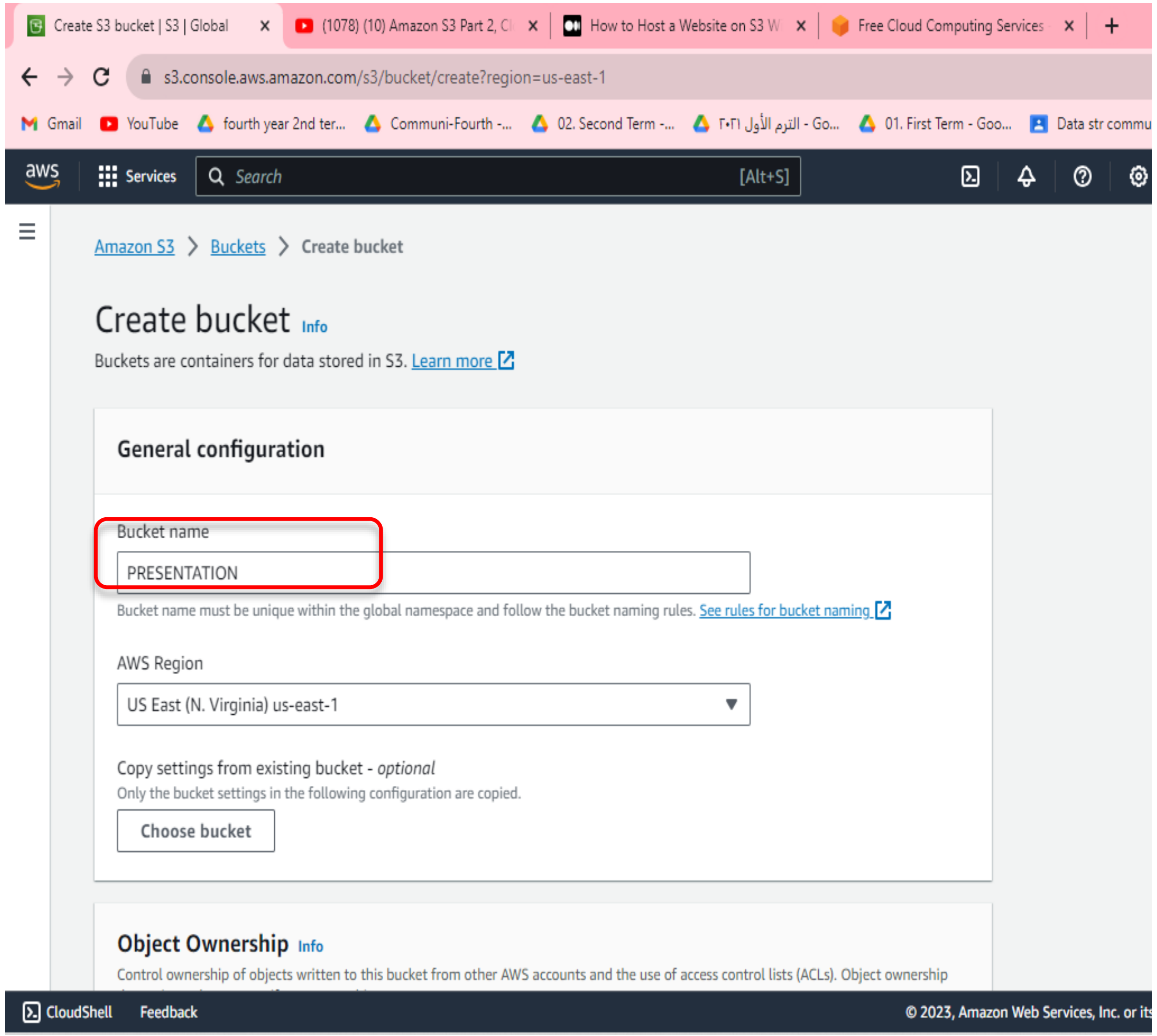
TASK Requirements

1. Create an S3 Bucket & Host a public static web site on S3

2. Make a cloud front distribution and Restrict the access to Static Web Site on S3 Bucket to be only through Cloud Front Using Bucket Policy

3. Deny Access From Egypt using GeoRestrictions in Cloud Front or Through WAF configuration

Part 1 : Create S3 Bucket


Create S3 bucket | S3 | Global
(1078) (10) Amazon S3 Part 2, Cl
How to Host a Website on S3 W
Free Cloud Computing Services
s3.console.aws.amazon.com/s3/bucket/create?region=us-east-1
Gmail
YouTube
fourth year 2nd ter...
Communi-Fourth -...
02. Second Term -...
الترم الأول ٢٠٢١ - Go...
01. First Term - Goo...
Data str commu
aws
Services
Search
[Alt+S]
CloudShell
Feedback
© 2023, Amazon Web Services, Inc. or its

Amazon S3 > Buckets > Create bucket

Create bucket Info

Buckets are containers for data stored in S3. Learn more

General configuration

Bucket name

PRESENTATION

Bucket name must be unique within the global namespace and follow the bucket naming rules. See rules for bucket naming

AWS Region

US East (N. Virginia) us-east-1 ▼

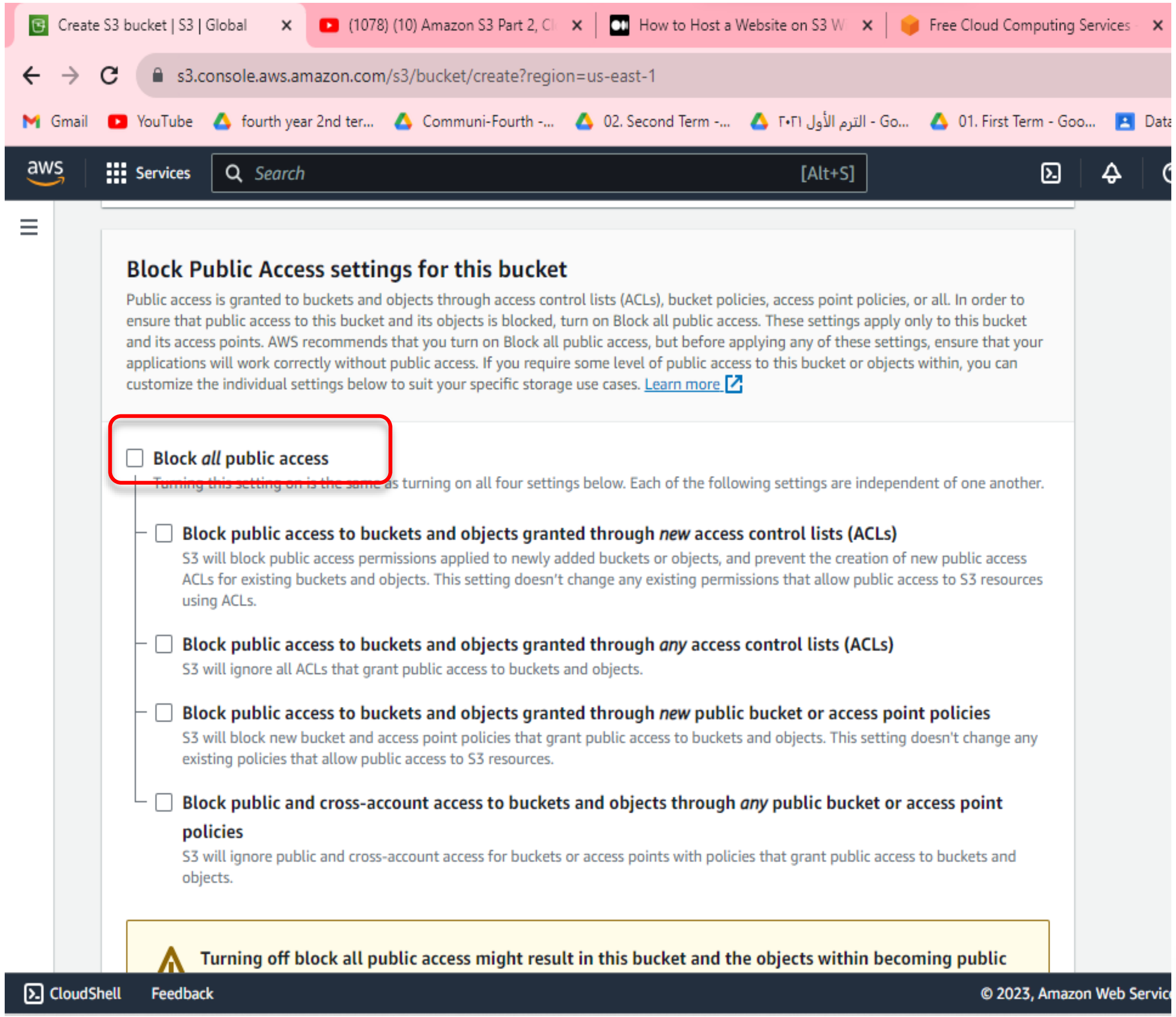
Copy settings from existing bucket - *optional*

Only the bucket settings in the following configuration are copied.

Choose bucket

Object Ownership Info

Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership


Create S3 bucket | S3 | Global
(1078) (10) Amazon S3 Part 2, Cl
How to Host a Website on S3 W
Free Cloud Computing Services
s3.console.aws.amazon.com/s3/bucket/create?region=us-east-1
Gmail
YouTube
fourth year 2nd ter...
Communi-Fourth -...
02. Second Term -...
الترم الأول ٢٠٢١ - Go...
01. First Term - Goo...
Data
aws
Services
Search
[Alt+S]
CloudShell
Feedback
© 2023, Amazon Web Servic

Block Public Access settings for this bucket

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

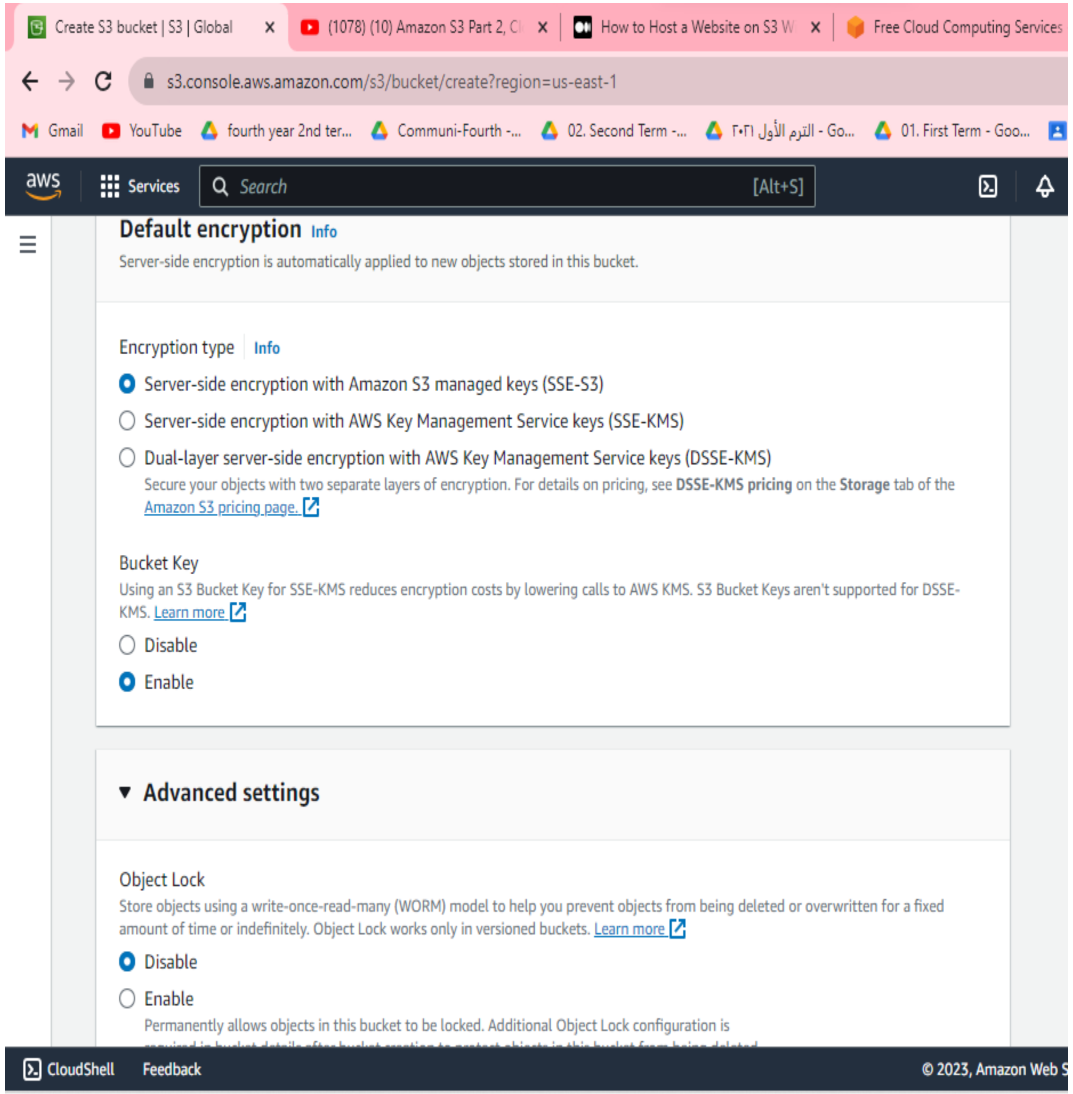
☐ **Block *all* public access**

Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

- ☐ **Block public access to buckets and objects granted through *new* access control lists (ACLs)**
  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.
- ☐ **Block public access to buckets and objects granted through *any* access control lists (ACLs)**
  S3 will ignore all ACLs that grant public access to buckets and objects.
- ☐ **Block public access to buckets and objects granted through *new* public bucket or access point policies**
  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.
- ☐ **Block public and cross-account access to buckets and objects through *any* public bucket or access point policies**
  S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

⚠ **Turning off block all public access might result in this bucket and the objects within becoming public**

Part 1 : Create S3 Bucket



Default encryption Info

Server-side encryption is automatically applied to new objects stored in this bucket.

Encryption type Info

● Server-side encryption with Amazon S3 managed keys (SSE-S3)

○ Server-side encryption with AWS Key Management Service keys (SSE-KMS)

○ Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)
Secure your objects with two separate layers of encryption. For details on pricing, see **DSSE-KMS pricing** on the **Storage** tab of the Amazon S3 pricing page.

Bucket Key

Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-KMS. Learn more

○ Disable

● Enable

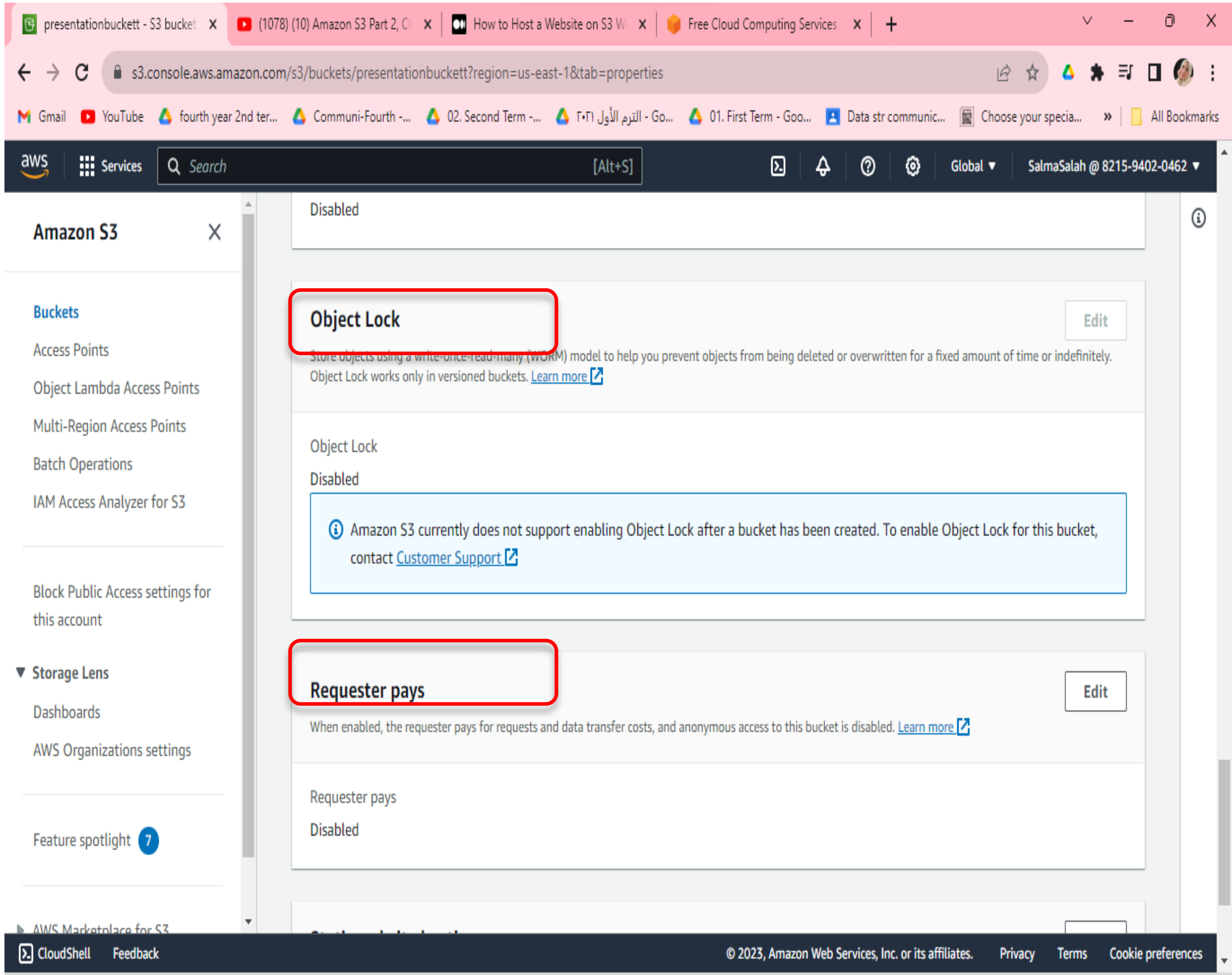
▼ Advanced settings

Object Lock

Store objects using a write-once-read-many (WORM) model to help you prevent objects from being deleted or overwritten for a fixed amount of time or indefinitely. Object Lock works only in versioned buckets. Learn more

● Disable

○ Enable
Permanently allows objects in this bucket to be locked. Additional Object Lock configuration is


presentationbuckett - S3 bucket
(1078) (10) Amazon S3 Part 2, Cl
How to Host a Website on S3 W
Free Cloud Computing Services
s3.console.aws.amazon.com/s3/buckets/presentationbuckett?region=us-east-1&tab=properties
Gmail
YouTube
fourth year 2nd ter...
Communi-Fourth -...
02. Second Term -...
الترم الأول ٢٠٢١ - Go...
01. First Term - Goo...
Data str communic...
Choose your specia...
All Bookmarks
aws
Services
Search
[Alt+S]
Global ▾
SalmaSalah @ 8215-9402-0462 ▾
Amazon S3
Buckets
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
AWS Organizations settings
Feature spotlight 7
AWS Marketplace for S3
Edit
Edit
CloudShell
Feedback
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Disabled

Object Lock

Store objects using a write-once-read-many (WORM) model to help you prevent objects from being deleted or overwritten for a fixed amount of time or indefinitely. Object Lock works only in versioned buckets. Learn more

Object Lock

Disabled

Amazon S3 currently does not support enabling Object Lock after a bucket has been created. To enable Object Lock for this bucket, contact Customer Support

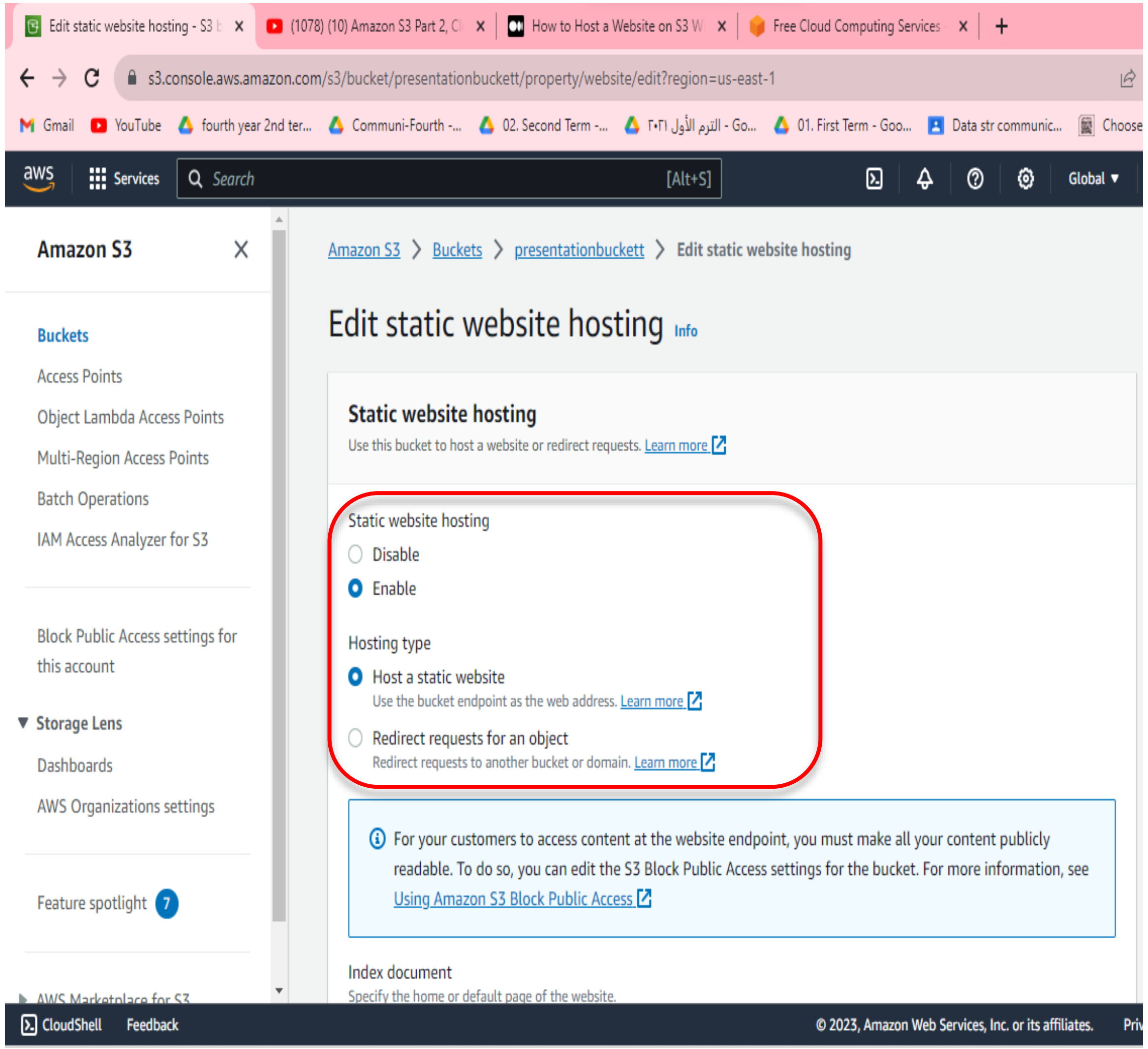
Requester pays

When enabled, the requester pays for requests and data transfer costs, and anonymous access to this bucket is disabled. Learn more

Requester pays

Disabled

Part 1 : Create S3 Bucket


Edit static website hosting - S3
(1078) (10) Amazon S3 Part 2, C
How to Host a Website on S3 W
Free Cloud Computing Services
s3.console.aws.amazon.com/s3/bucket/presentationbuckett/property/website/edit?region=us-east-1
Gmail
YouTube
fourth year 2nd ter...
Communi-Fourth -...
02. Second Term -...
٢٠٢١ الترم الأول - Go...
01. First Term - Goo...
Data str communic...
Choose
aws
Services
Search
[Alt+S]
Global
Amazon S3
Buckets
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
AWS Organizations settings
Feature spotlight 7
AWS Marketplace for S3
CloudShell
Feedback
© 2023, Amazon Web Services, Inc. or its affiliates.
Priv

Amazon S3 > Buckets > presentationbuckett > Edit static website hosting

Edit static website hosting Info

Static website hosting

Use this bucket to host a website or redirect requests. Learn more

Static website hosting

○ Disable

● Enable

Hosting type

● Host a static website

Use the bucket endpoint as the web address. Learn more

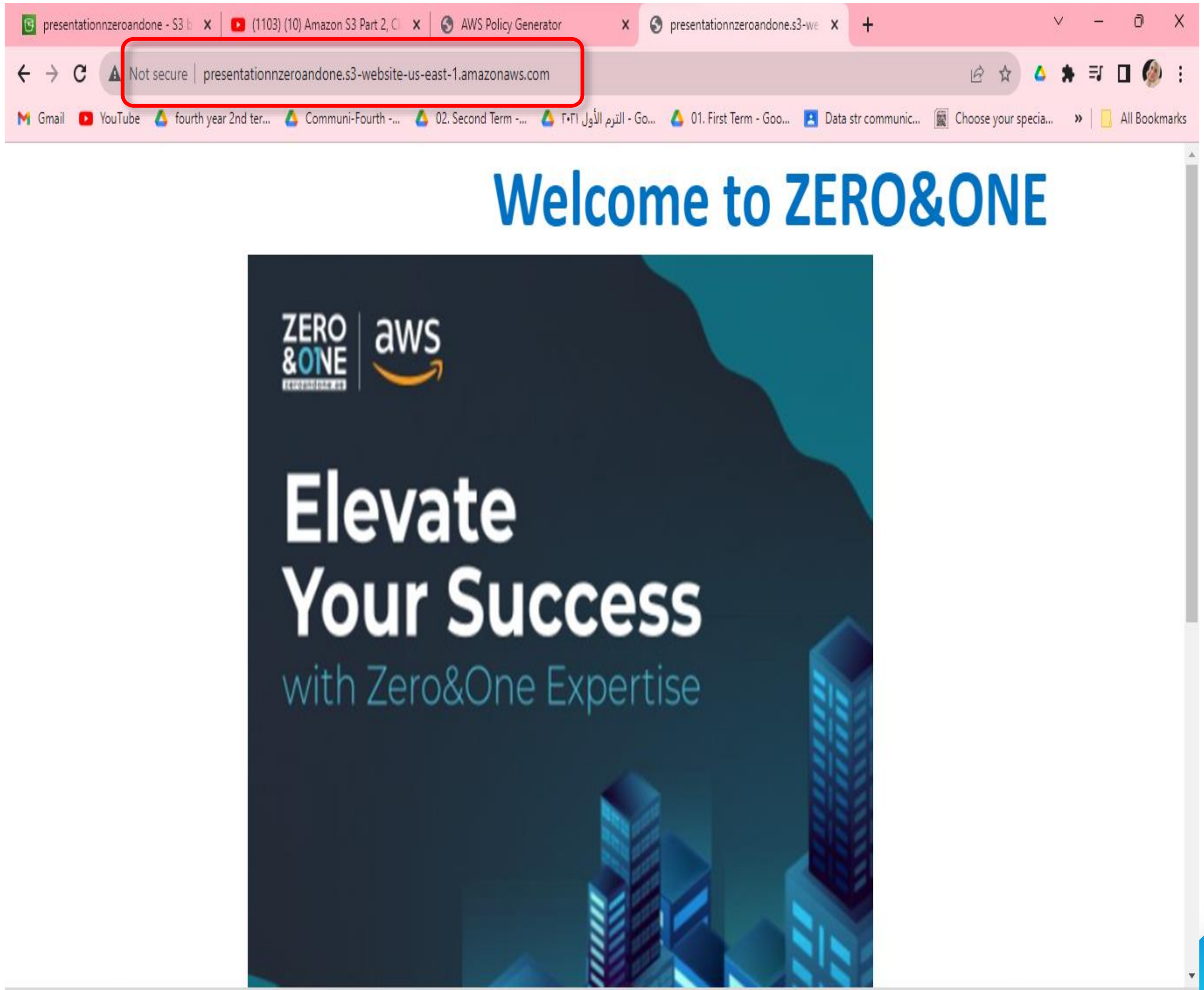
○ Redirect requests for an object

Redirect requests to another bucket or domain. Learn more

For your customers to access content at the website endpoint, you must make all your content publicly readable. To do so, you can edit the S3 Block Public Access settings for the bucket. For more information, see Using Amazon S3 Block Public Access

Index document

Specify the home or default page of the website.

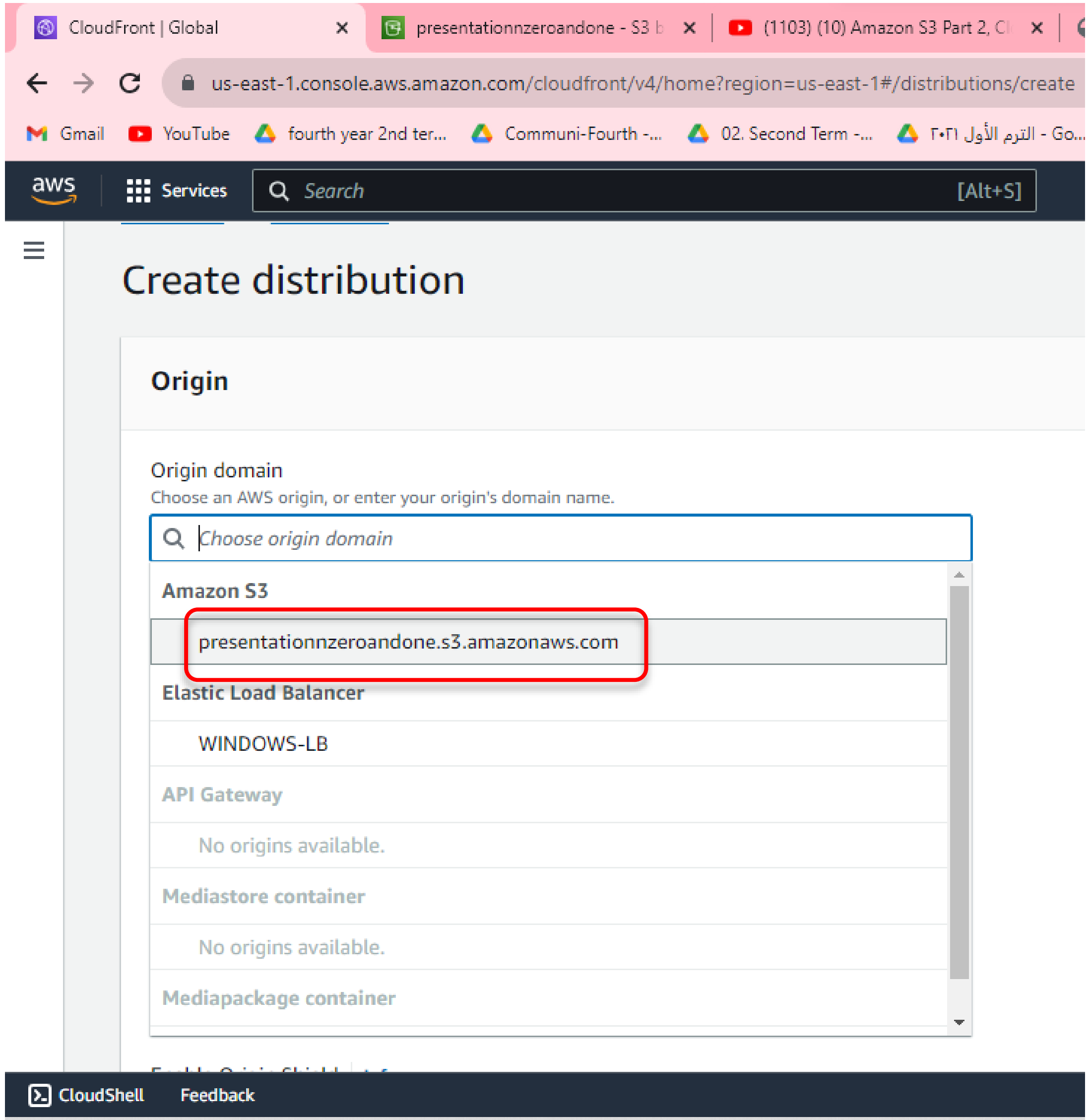


Not secure | presentationnzeroandone.s3-website-us-east-1.amazonaws.com

Welcome to ZERO&ONE

Elevate Your Success with Zero&One Expertise

Part 2 : Create a Cloud Front Distribution



Create distribution

Origin

Origin domain

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

Choose origin domain

Amazon S3

presentationnzeroandone.s3.amazonaws.com

Elastic Load Balancer

WINDOWS-LB

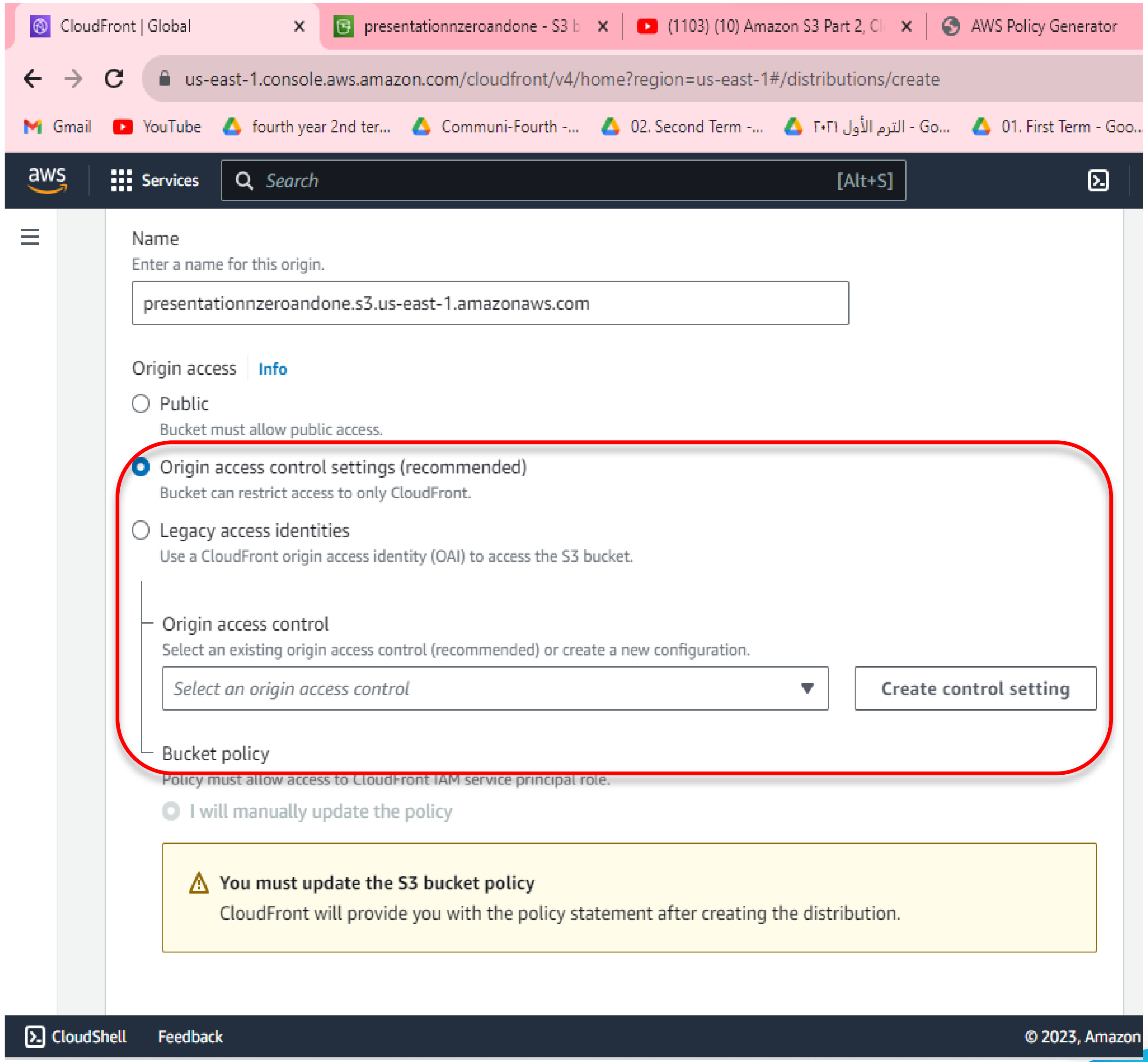
API Gateway

No origins available.

Mediastore container

No origins available.

Mediapackage container



Name

Enter a name for this origin.

presentationnzeroandone.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 configuration.

Select an origin access control ▼ | Create control setting

Bucket policy

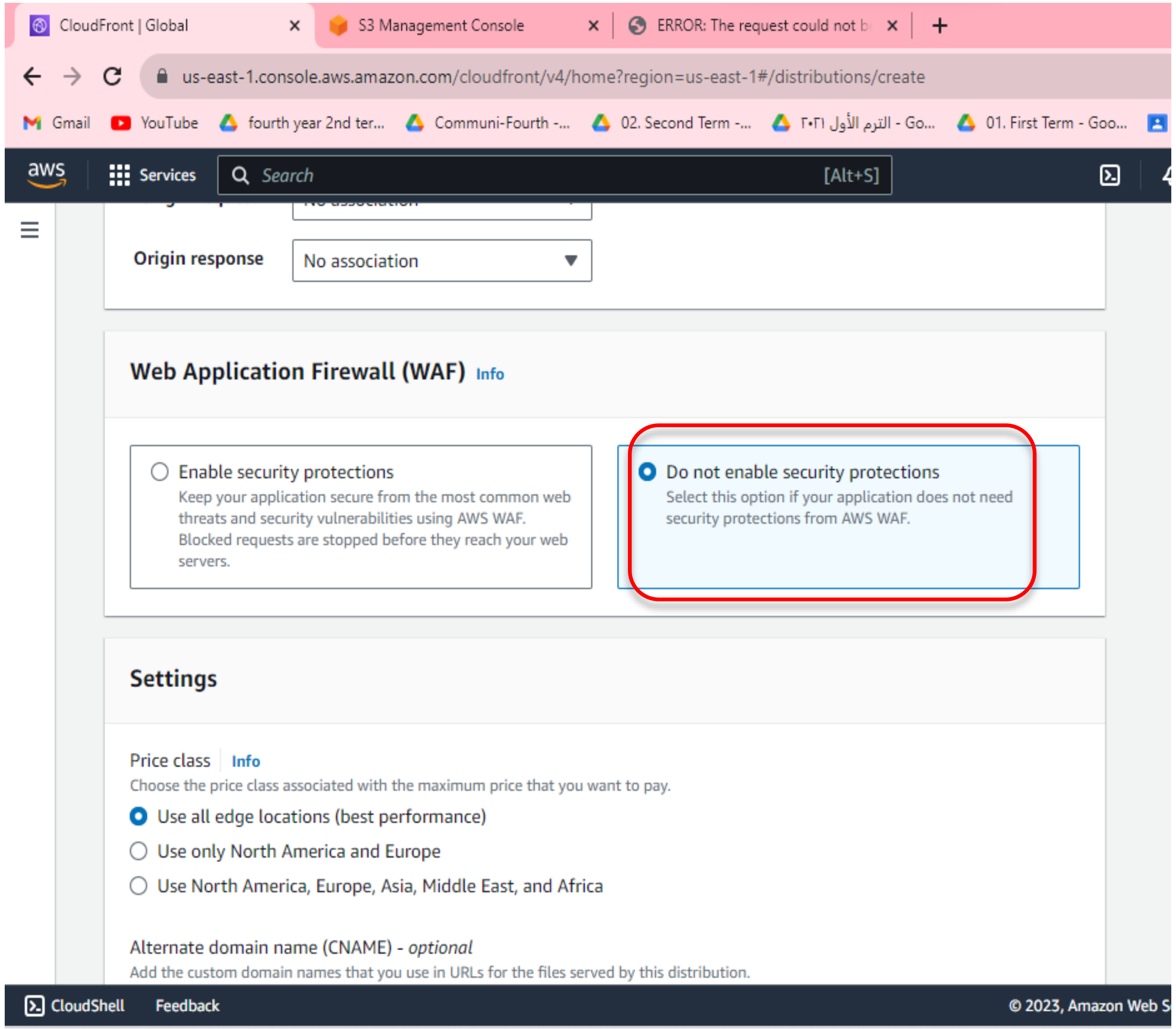
Policy must allow access to CloudFront IAM service principal role.

○ I will manually update the policy

⚠ **You must update the S3 bucket policy**

CloudFront will provide you with the policy statement after creating the distribution.

Part 2 : Create a Cloud Front Distribution



Origin response: No association

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.

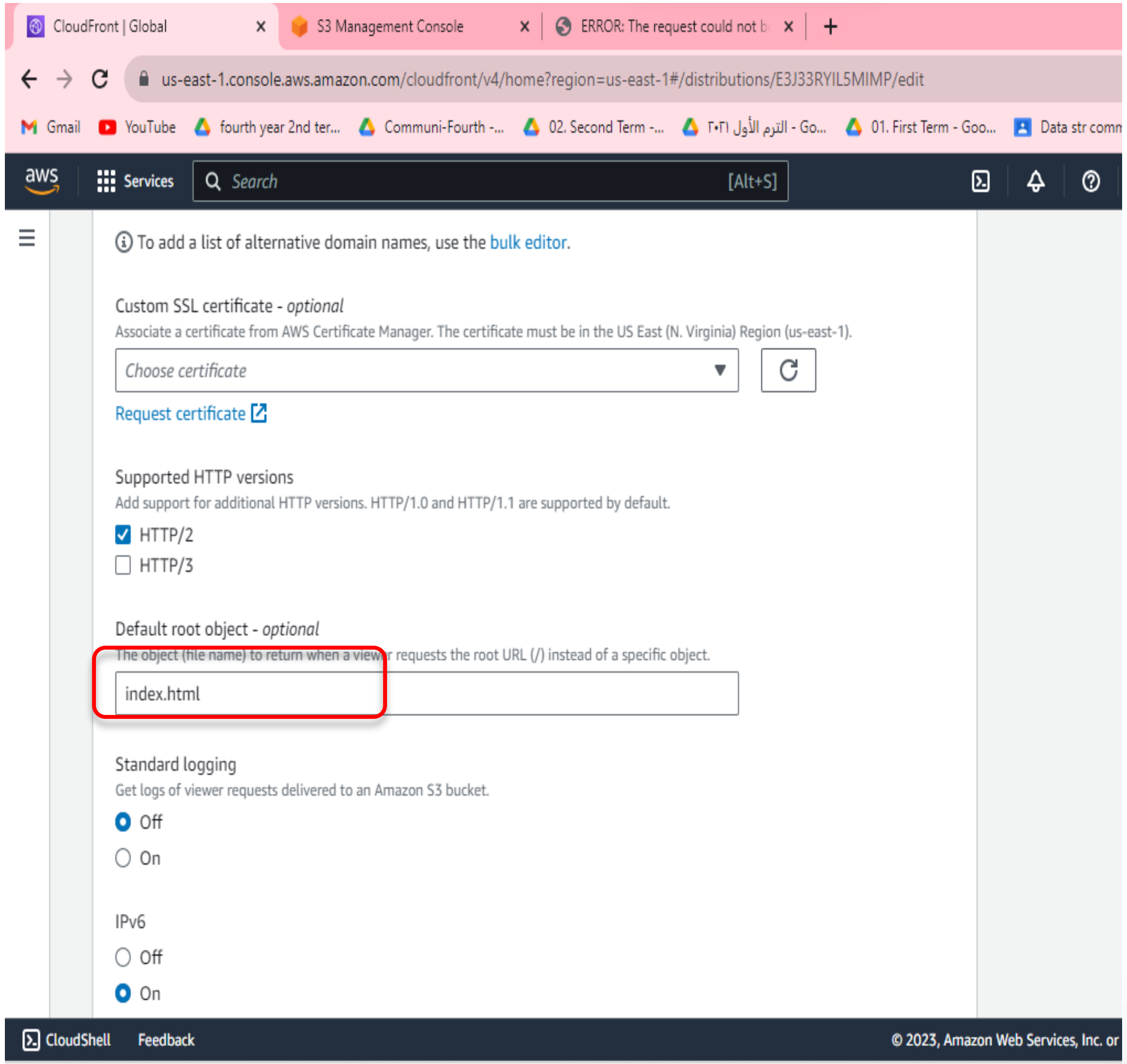
● Do not enable security protections
Select this option if your application does not need security protections from AWS WAF.

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.



ⓘ 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

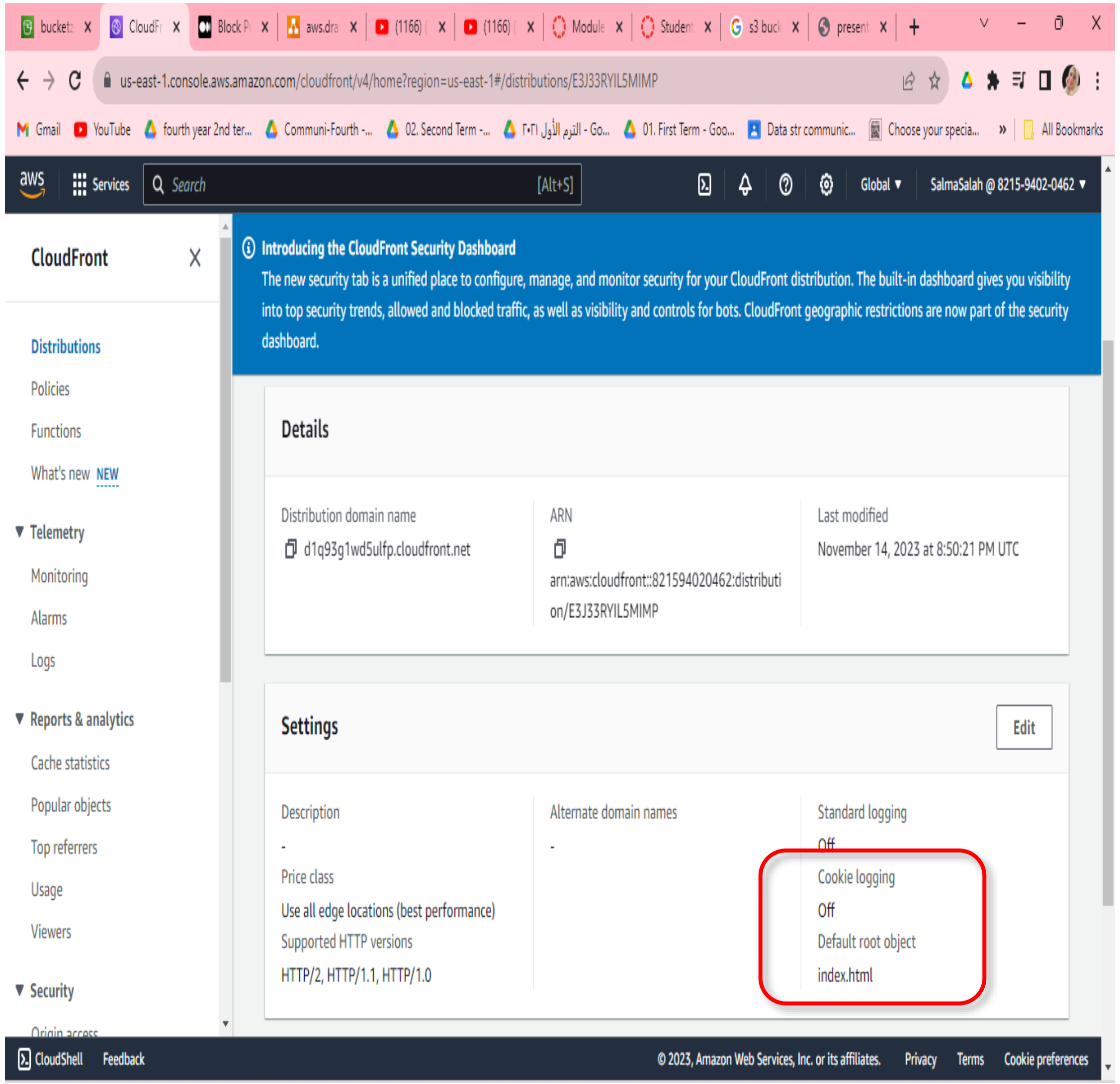
Supported HTTP versions
Add support for additional HTTP versions. HTTP/1.0 and HTTP/1.1 are supported by default.
☑ HTTP/2
☐ HTTP/3

Default root object - *optional*
The object (file name) to return when a viewer requests the root URL (/) instead of a specific object.
index.html

Standard logging
Get logs of viewer requests delivered to an Amazon S3 bucket.
● Off
○ On

IPv6
○ Off
● On

Part 2 : Access Through Cloud Front



us-east-1.console.aws.amazon.com/cloudfront/v4/home?region=us-east-1#/distributions/E3J33RYIL5MIMP

Introducing the CloudFront Security Dashboard

The new security tab is a unified place to configure, manage, and monitor security for your CloudFront distribution. The built-in dashboard gives you visibility into top security trends, allowed and blocked traffic, as well as visibility and controls for bots. CloudFront geographic restrictions are now part of the security dashboard.

Details

Distribution domain name: d1q93g1wd5ulfp.cloudfront.net

ARN: arn:aws:cloudfront::821594020462:distribution/E3J33RYIL5MIMP

Last modified: November 14, 2023 at 8:50:21 PM UTC

Settings Edit

Description: -

Price class: Use all edge locations (best performance)

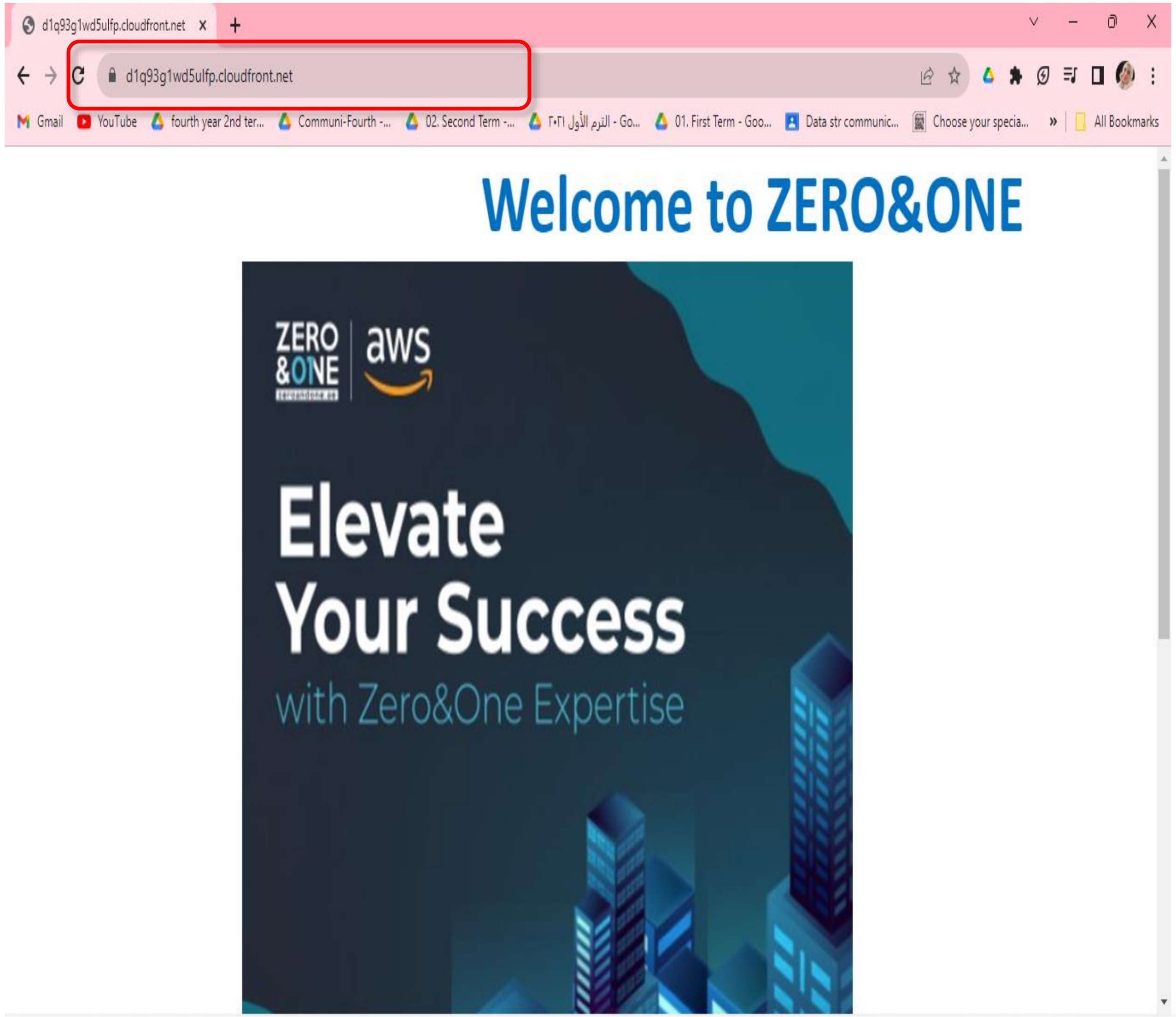
Supported HTTP versions: HTTP/2, HTTP/1.1, HTTP/1.0

Alternate domain names: -

Standard logging: Off

Cookie logging: Off

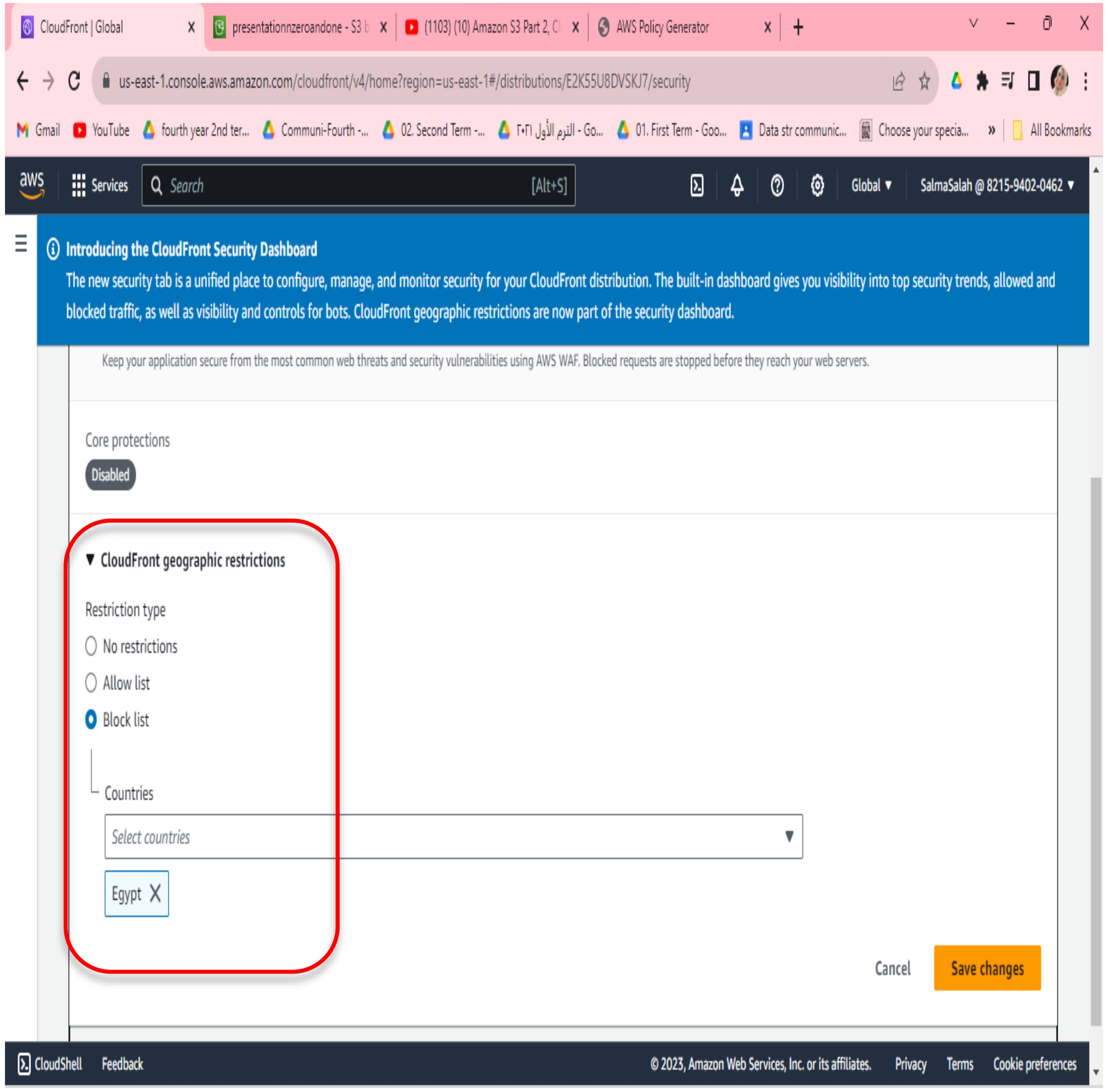
Default root object: index.html



d1q93g1wd5ulfp.cloudfront.net

Welcome to ZERO&ONE

Part 3 : Restrict Access From GeoRestrictions



us-east-1.console.aws.amazon.com/cloudfront/v4/home?region=us-east-1#/distributions/E2K55U8DVSKJ7/security

Introducing the CloudFront Security Dashboard

The new security tab is a unified place to configure, manage, and monitor security for your CloudFront distribution. The built-in dashboard gives you visibility into top security trends, allowed and blocked traffic, as well as visibility and controls for bots. CloudFront geographic restrictions are now part of the security dashboard.

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.

Core protections

Disabled

▾ CloudFront geographic restrictions

Restriction type

○ No restrictions

○ Allow list

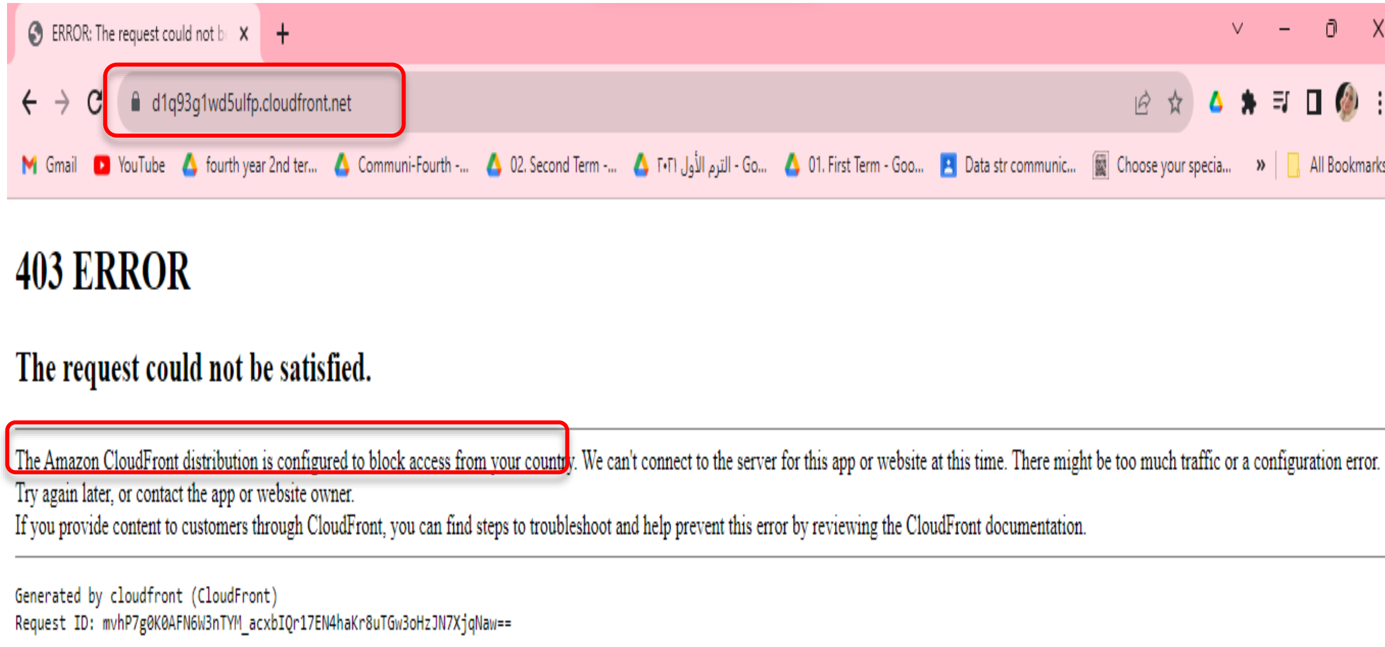
● Block list

Countries

Select countries ▾

Egypt X

Cancel | Save changes



d1q93g1wd5ulfp.cloudfront.net

403 ERROR

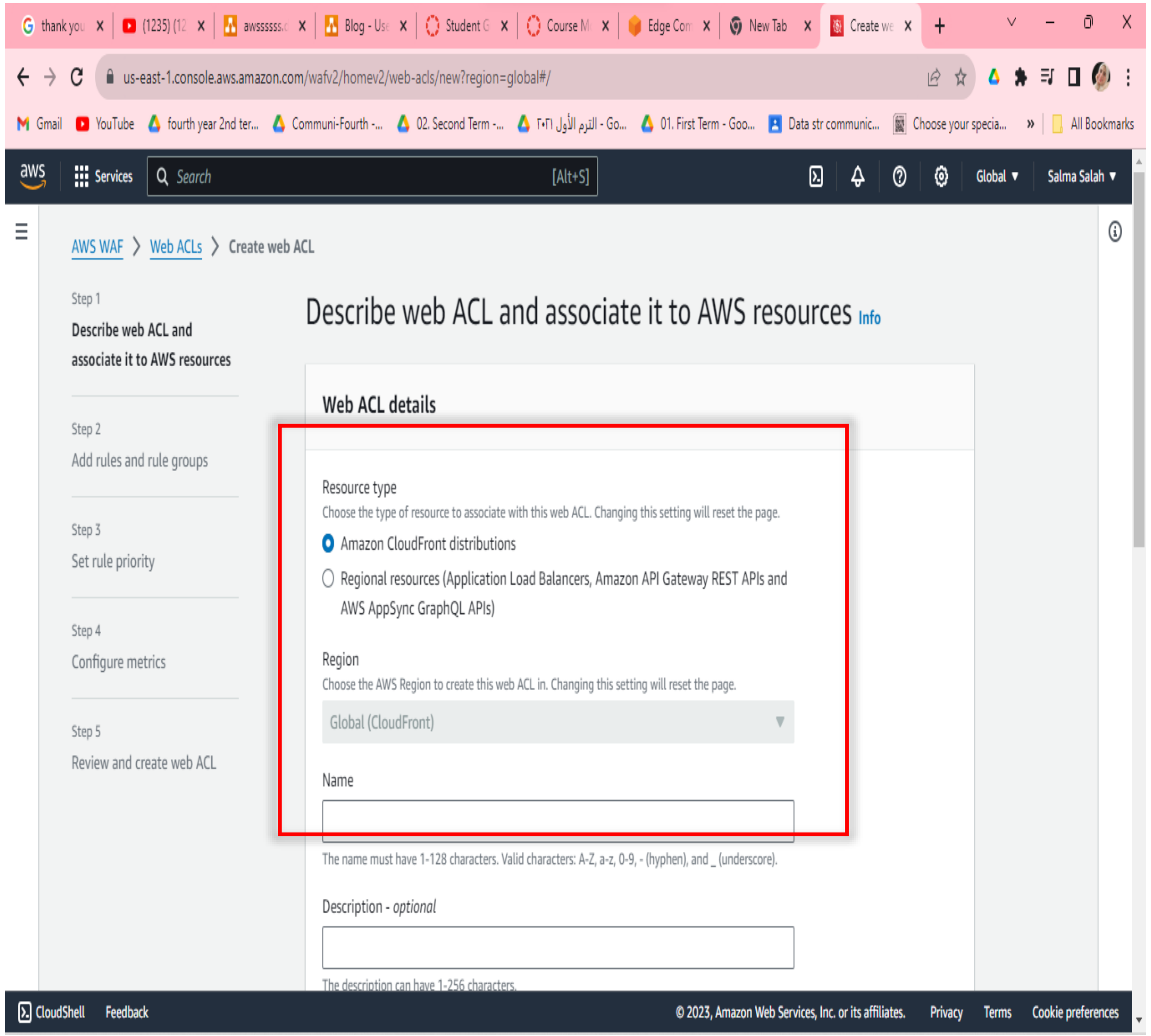
The request could not be satisfied.

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 cloudfront (CloudFront)
Request ID: mvhP7g0K0AFN6W3nTYM_acxbIQr17EN4haKr8uTGw3oHzJN7XjqNaw==
```

Part 4 : WAF



AWS WAF > Web ACLs > Create web ACL

Step 1
Describe web ACL and associate it to AWS resources

Step 2
Add rules and rule groups

Step 3
Set rule priority

Step 4
Configure metrics

Step 5
Review and create web ACL

Describe web ACL and associate it to AWS resources Info

Web ACL details

Resource type
Choose the type of resource to associate with this web ACL. Changing this setting will reset the page.

● Amazon CloudFront distributions

○ Regional resources (Application Load Balancers, Amazon API Gateway REST APIs and AWS AppSync GraphQL APIs)

Region
Choose the AWS Region to create this web ACL in. Changing this setting will reset the page.

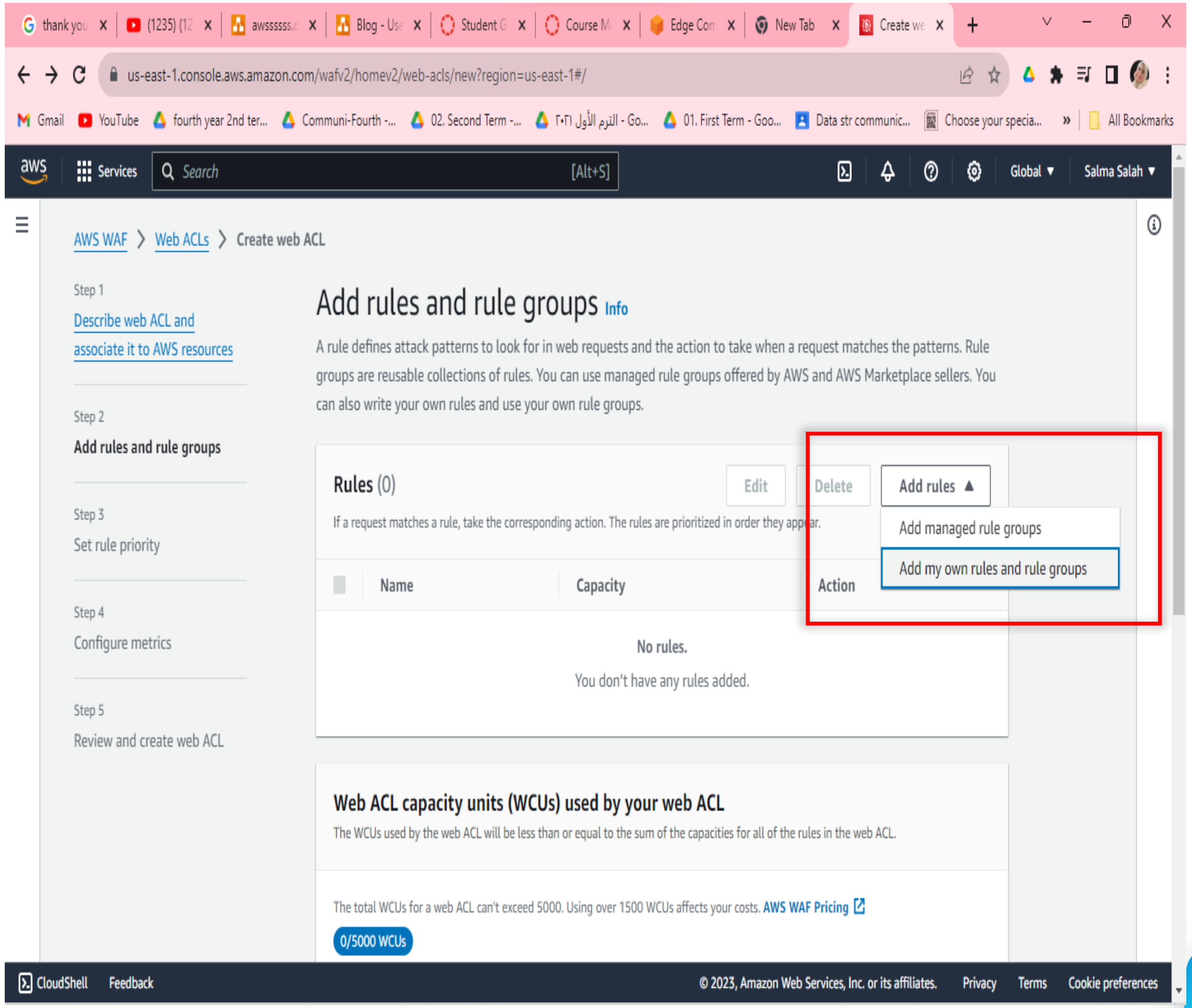
Global (CloudFront) ▾

Name

The name must have 1-128 characters. Valid characters: A-Z, a-z, 0-9, - (hyphen), and _ (underscore).

Description - *optional*

The description can have 1-256 characters.



AWS WAF > Web ACLs > Create web ACL

Step 1
Describe web ACL and associate it to AWS resources

Step 2
Add rules and rule groups

Step 3
Set rule priority

Step 4
Configure metrics

Step 5
Review and create web ACL

Add rules and rule groups Info

A rule defines attack patterns to look for in web requests and the action to take when a request matches the patterns. Rule groups are reusable collections of rules. You can use managed rule groups offered by AWS and AWS Marketplace sellers. You can also write your own rules and use your own rule groups.

Rules (0)

Edit | Delete | Add rules ▲

- Add managed rule groups
- Add my own rules and rule groups

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

	Name	Capacity	Action

No rules.
You don't have any rules added.

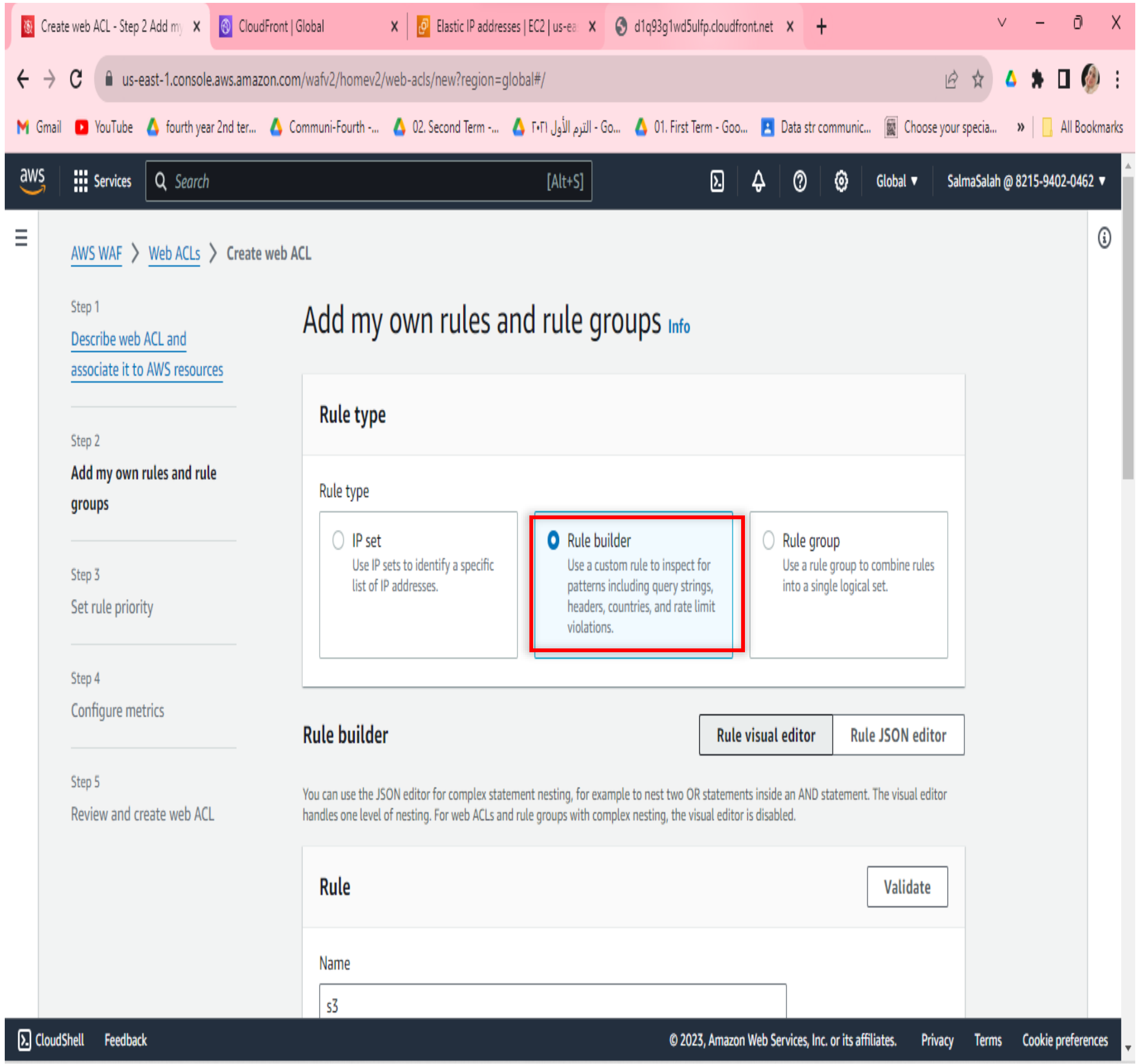
Web ACL capacity units (WCUs) used by your web ACL

The WCUs used by the web ACL will be less than or equal to the sum of the capacities for all of the rules in the web ACL.

The total WCUs for a web ACL can't exceed 5000. Using over 1500 WCUs affects your costs. AWS WAF Pricing

0/5000 WCUs

Part 4 : WAF



AWS WAF > Web ACLs > Create web ACL

Step 1
Describe web ACL and associate it to AWS resources

Step 2
Add my own rules and rule groups

Step 3
Set rule priority

Step 4
Configure metrics

Step 5
Review and create web ACL

Add my own rules and rule groups Info

Rule type

Rule type

○ IP set
Use IP sets to identify a specific list of IP addresses.

● Rule builder
Use a custom rule to inspect for patterns including query strings, headers, countries, and rate limit violations.

○ Rule group
Use a rule group to combine rules into a single logical set.

Rule builder

Rule visual editor | Rule JSON editor

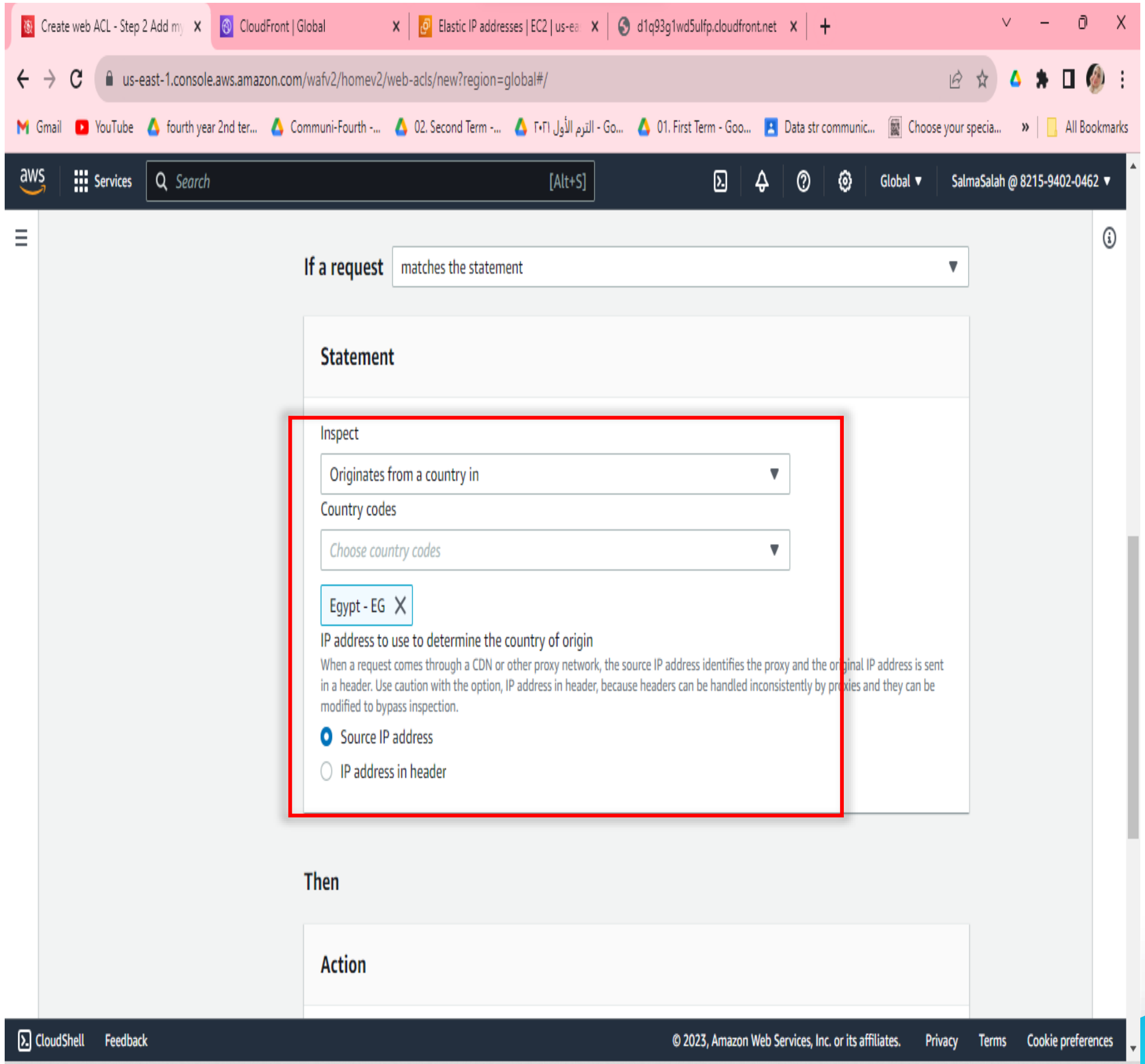
You can use the JSON editor for complex statement nesting, for example to nest two OR statements inside an AND statement. The visual editor handles one level of nesting. For web ACLs and rule groups with complex nesting, the visual editor is disabled.

Rule

Validate

Name

s3



If a request: matches the statement

Statement

Inspect
Originates from a country in

Country codes
Choose country codes

Egypt - EG X

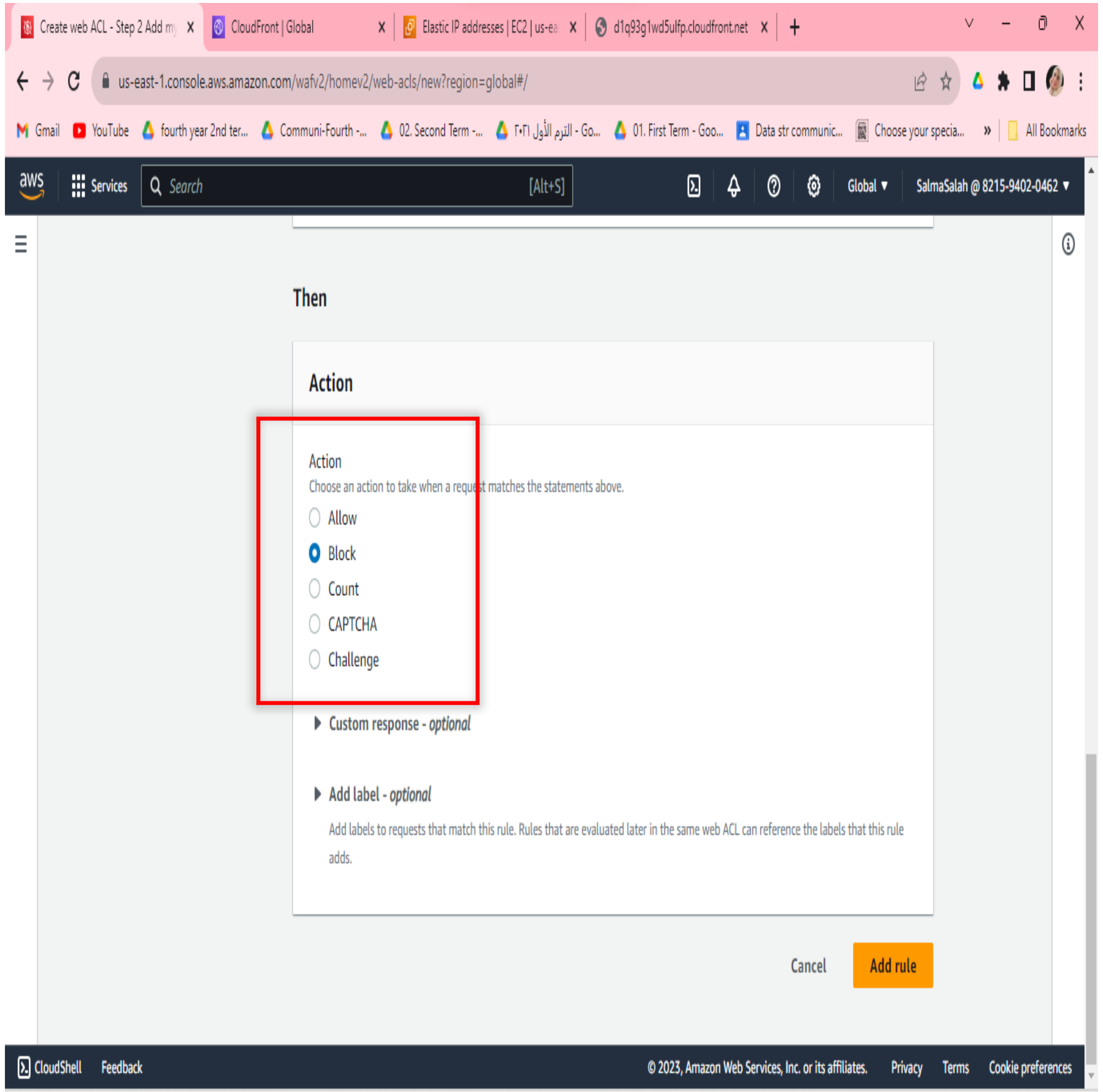
IP address to use to determine the country of origin
When a request comes through a CDN or other proxy network, the source IP address identifies the proxy and the original IP address is sent in a header. Use caution with the option, IP address in header, because headers can be handled inconsistently by proxies and they can be modified to bypass inspection.

● Source IP address
○ IP address in header

Then

Action

Part 4 : WAF


Create web ACL - Step 2 Add my
CloudFront | Global
Elastic IP addresses | EC2 | us-ea
d1q93g1wd5ulfp.cloudfront.net
us-east-1.console.aws.amazon.com/wafv2/homev2/web-acls/new?region=global#/
Gmail
YouTube
fourth year 2nd ter...
Communi-Fourth -...
02. Second Term -...
التيرم الأول ٢٠٢١ - Go...
01. First Term - Goo...
Data str communic...
Choose your specia...
All Bookmarks
aws
Services
Search
[Alt+S]
Global ▾
SalmaSalah @ 8215-9402-0462 ▾
CloudShell
Feedback
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Then

Action

Action

Choose an action to take when a request matches the statements above.

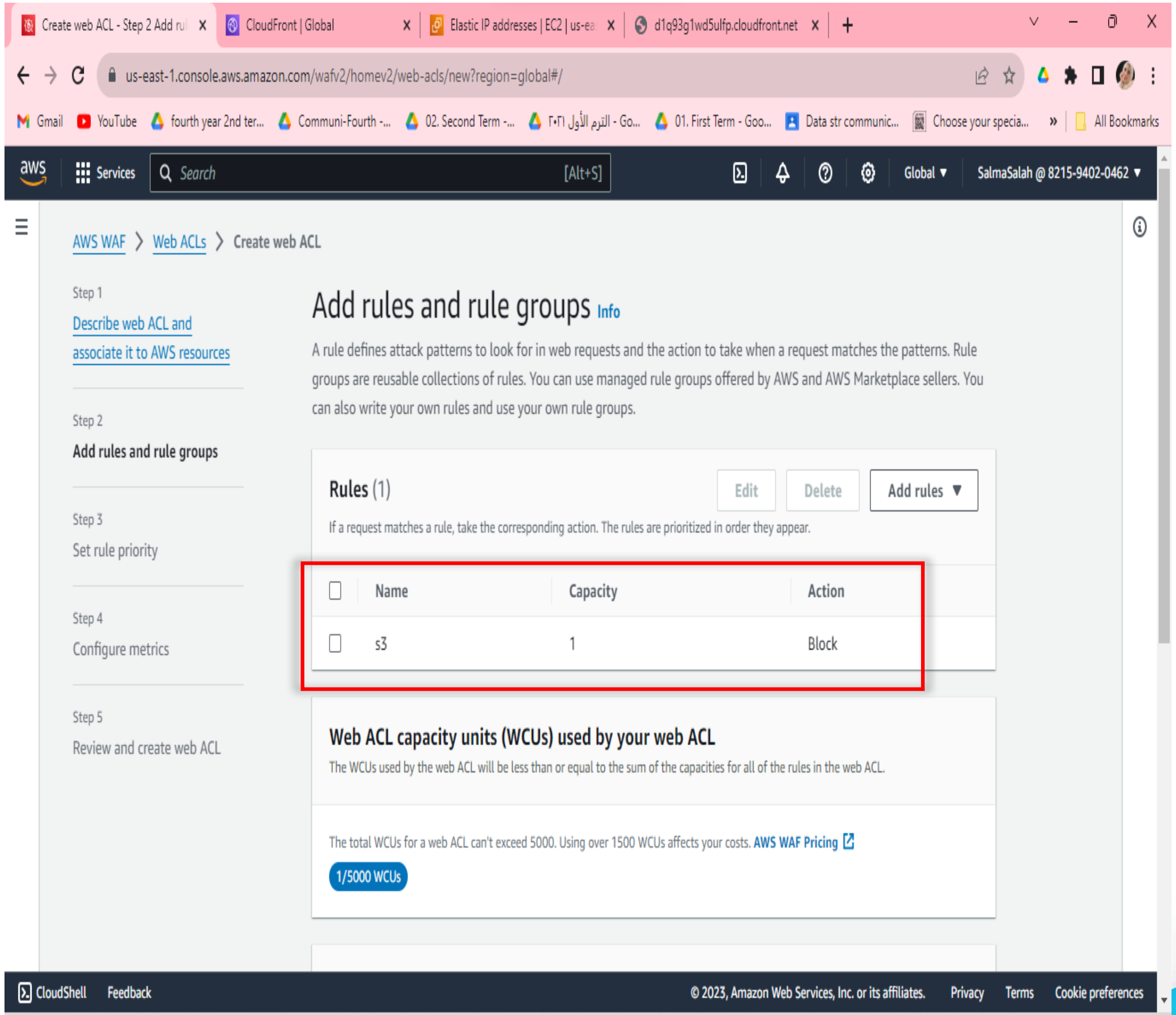
○ Allow
● Block
○ Count
○ CAPTCHA
○ Challenge

▸ Custom response - *optional*

▸ Add label - *optional*

Add labels to requests that match this rule. Rules that are evaluated later in the same web ACL can reference the labels that this rule adds.

Cancel | Add rule


Create web ACL - Step 2 Add ru
CloudFront | Global
Elastic IP addresses | EC2 | us-ea
d1q93g1wd5ulfp.cloudfront.net
us-east-1.console.aws.amazon.com/wafv2/homev2/web-acls/new?region=global#/
Gmail
YouTube
fourth year 2nd ter...
Communi-Fourth -...
02. Second Term -...
التيرم الأول ٢٠٢١ - Go...
01. First Term - Goo...
Data str communic...
Choose your specia...
All Bookmarks
aws
Services
Search
[Alt+S]
Global ▾
SalmaSalah @ 8215-9402-0462 ▾
CloudShell
Feedback
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

AWS WAF › Web ACLs › Create web ACL

Step 1
Describe web ACL and associate it to AWS resources

Step 2
Add rules and rule groups

Step 3
Set rule priority

Step 4
Configure metrics

Step 5
Review and create web ACL

Add rules and rule groups Info

A rule defines attack patterns to look for in web requests and the action to take when a request matches the patterns. Rule groups are reusable collections of rules. You can use managed rule groups offered by AWS and AWS Marketplace sellers. You can also write your own rules and use your own rule groups.

Rules (1) — Edit | Delete | Add rules ▾

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

□	Name	Capacity	Action
□	s3	1	Block

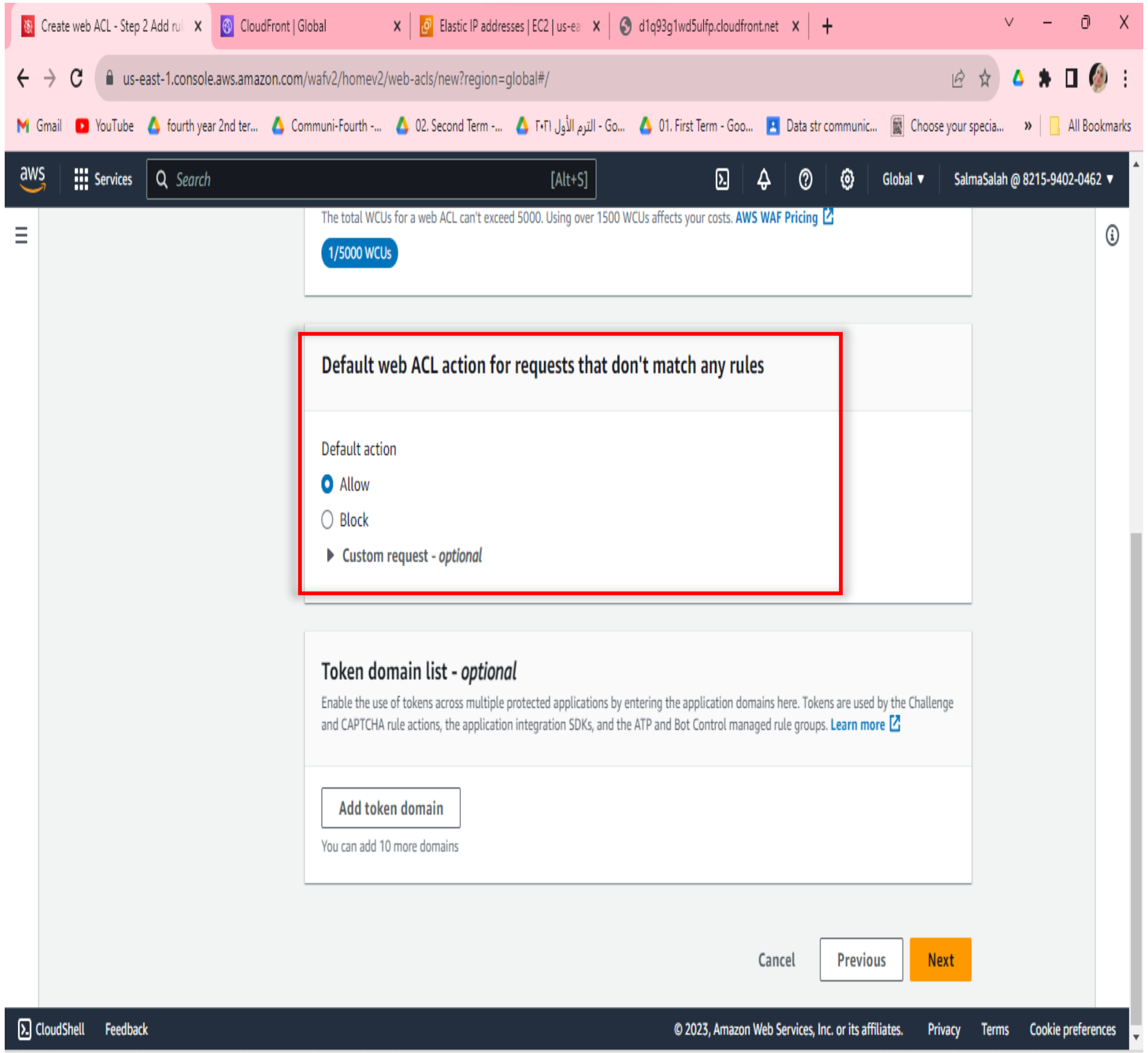
Web ACL capacity units (WCUs) used by your web ACL

The WCUs used by the web ACL will be less than or equal to the sum of the capacities for all of the rules in the web ACL.

The total WCUs for a web ACL can't exceed 5000. Using over 1500 WCUs affects your costs. AWS WAF Pricing

1/5000 WCUs

Part 4 : WAF



The total WCUs for a web ACL can't exceed 5000. Using over 1500 WCUs affects your costs. AWS WAF Pricing

1/5000 WCUs

Default web ACL action for requests that don't match any rules

Default action

● Allow

○ Block

▸ Custom request - *optional*

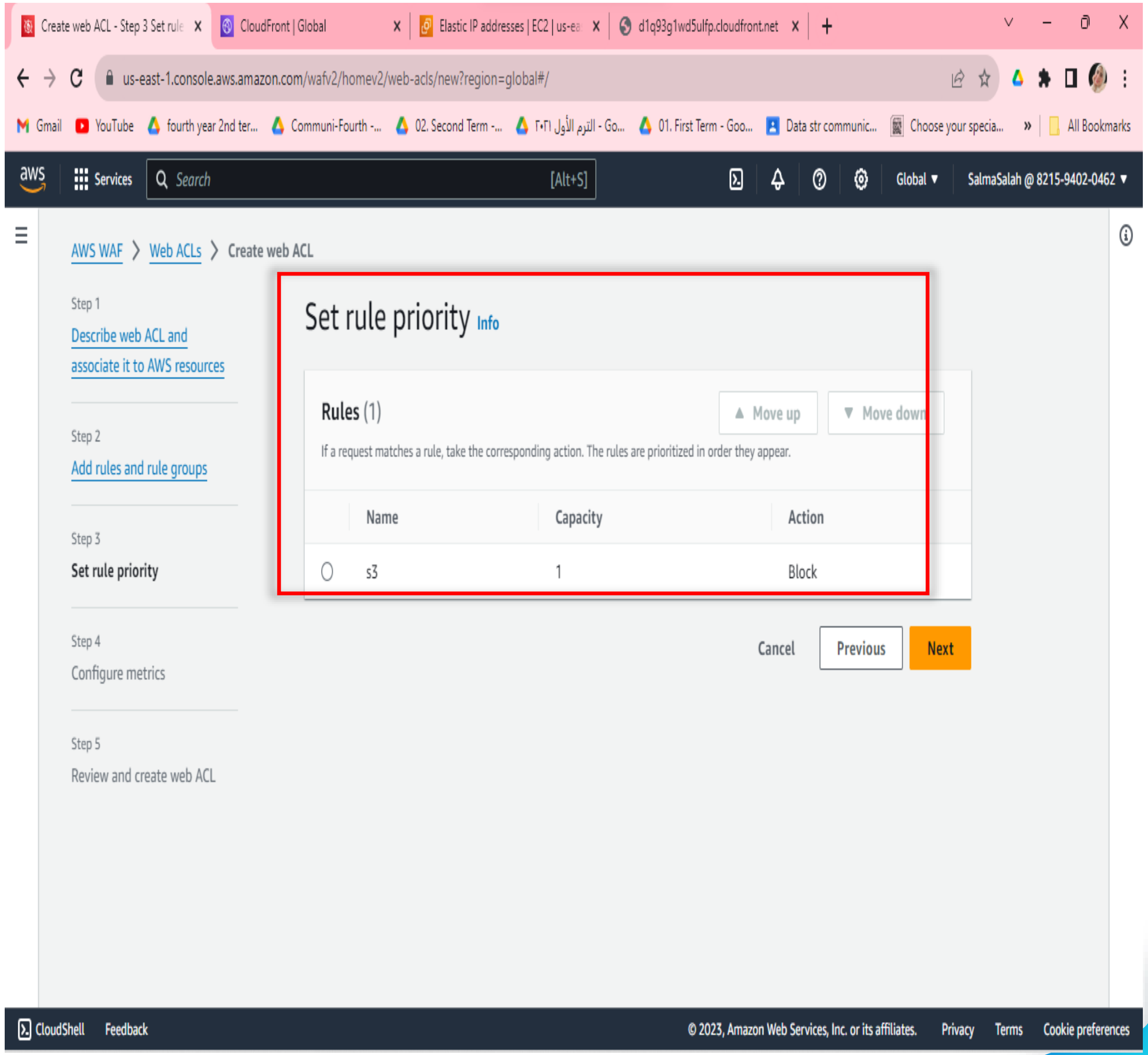
Token domain list - *optional*

Enable the use of tokens across multiple protected applications by entering the application domains here. Tokens are used by the Challenge and CAPTCHA rule actions, the application integration SDKs, and the ATP and Bot Control managed rule groups. Learn more

Add token domain

You can add 10 more domains

Cancel | Previous | Next



AWS WAF > Web ACLs > Create web ACL

Step 1
Describe web ACL and associate it to AWS resources

Step 2
Add rules and rule groups

Step 3
Set rule priority

Step 4
Configure metrics

Step 5
Review and create web ACL

Set rule priority Info

Rules (1)

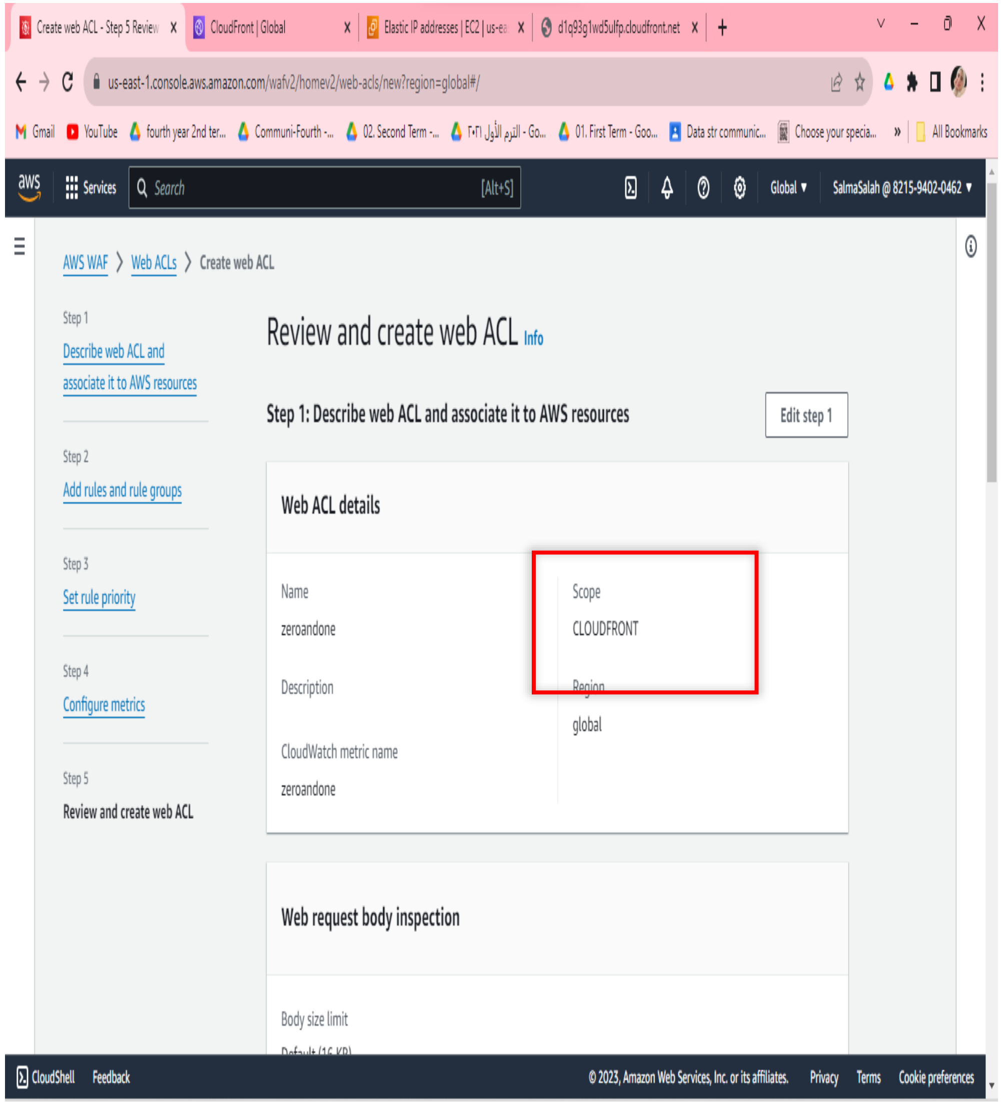
▲ Move up | ▼ Move down

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

	Name	Capacity	Action
○	s3	1	Block

Cancel | Previous | Next

Part 4 : WAF



AWS WAF > Web ACLs > Create web ACL

Step 1
Describe web ACL and associate it to AWS resources

Step 2
Add rules and rule groups

Step 3
Set rule priority

Step 4
Configure metrics

Step 5
Review and create web ACL

Review and create web ACL Info

Step 1: Describe web ACL and associate it to AWS resources

Edit step 1

Web ACL details

Name
zeroandone

Description

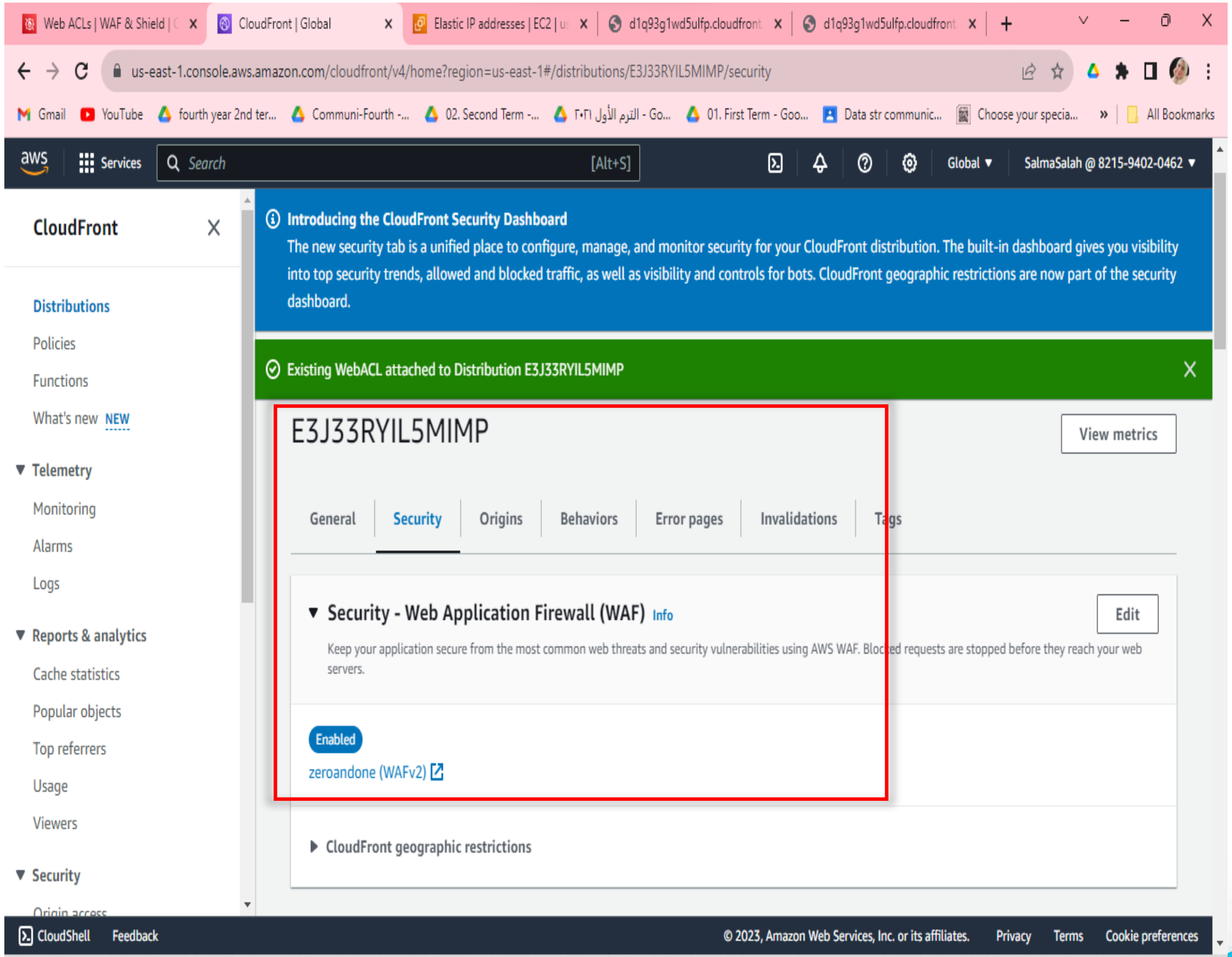
CloudWatch metric name
zeroandone

Scope
CLOUDFRONT

Region
global

Web request body inspection

Body size limit
Default (16 KB)



Introducing the CloudFront Security Dashboard

The new security tab is a unified place to configure, manage, and monitor security for your CloudFront distribution. The built-in dashboard gives you visibility into top security trends, allowed and blocked traffic, as well as visibility and controls for bots. CloudFront geographic restrictions are now part of the security dashboard.

Existing WebACL attached to Distribution E3J33RYIL5MIMP

E3J33RYIL5MIMP

View metrics

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

Security - Web Application Firewall (WAF) Info

Edit

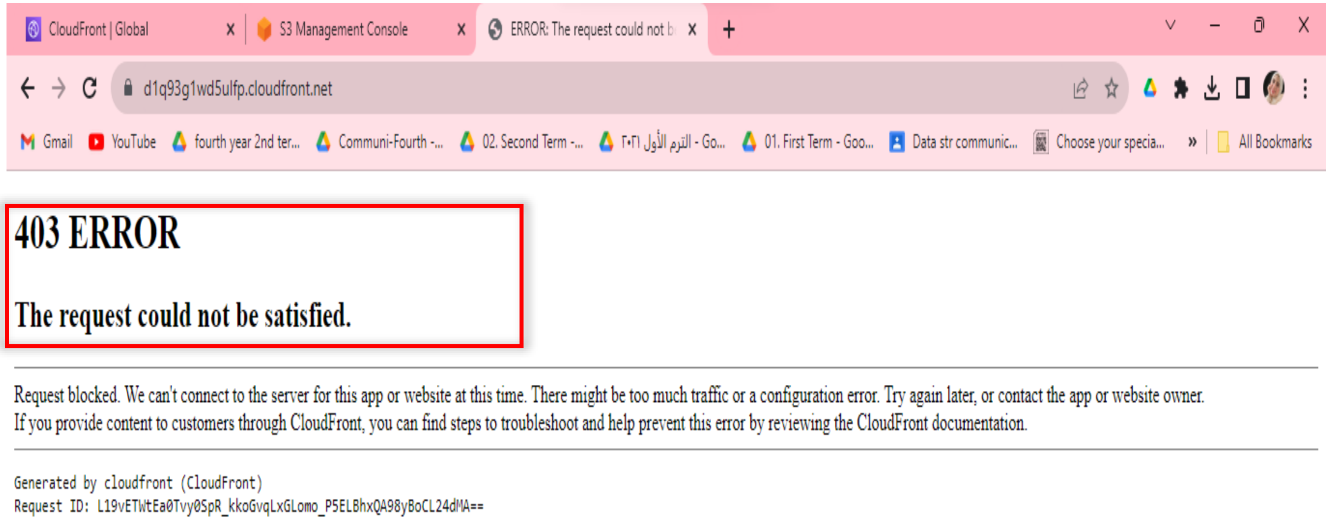
Keep your application secure from the most common web threats and security vulnerabilities using AWS WAF. Blocked requests are stopped before they reach your web servers.

Enabled

zeroandone (WAFv2)

CloudFront geographic restrictions

Part 4 : WAF



403 ERROR

The request could not be satisfied.

Request blocked. 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 cloudfront (CloudFront)
Request ID: L19vETWtEa0Tvy0SpR_kkoGvqLxGLomo_P5ELBhxQA98yBoCL24dMA==
```