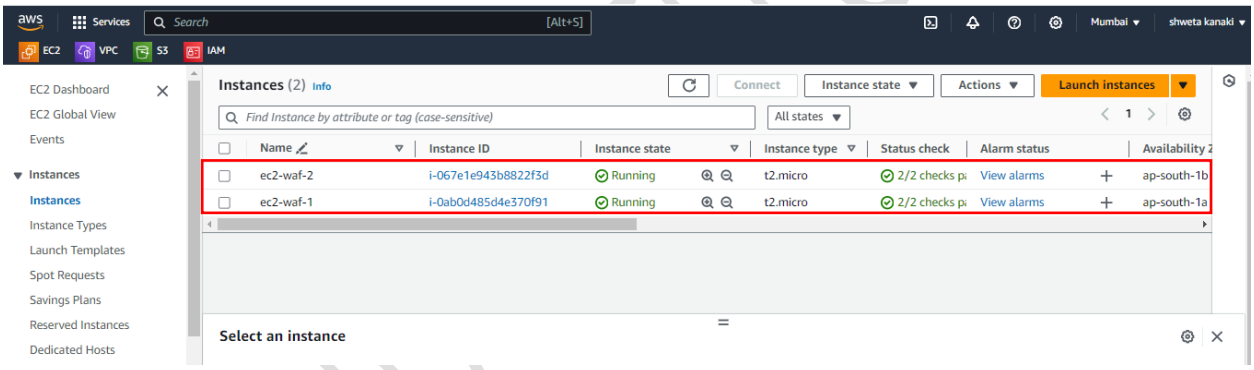
WEB APPLICATION FIREWALL (AWS WAF)

AWS WAF (Web Application Firewall) is a cloud-based firewall service provided by Amazon Web Services (AWS) that helps protect web applications from common web exploits and vulnerabilities. It offers several benefits and features that enhance the security of web applications.

SET UP AWS WAF (WEB APPLICATION FIREWALL) FOR AN EC2 INSTANCE

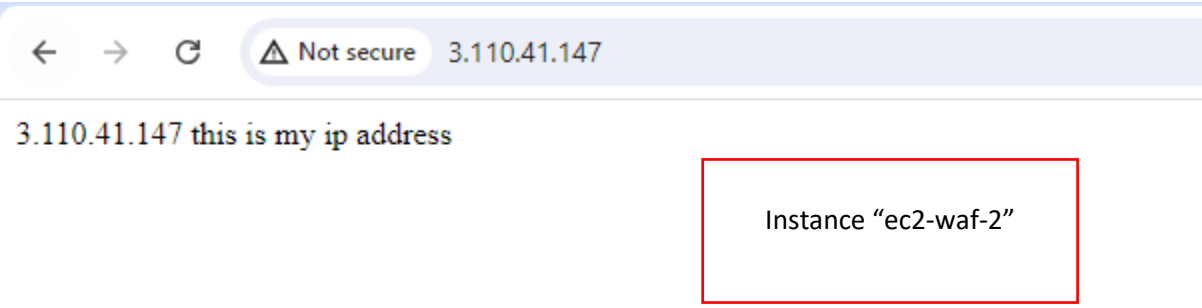
Step 1: Create two EC2 instances



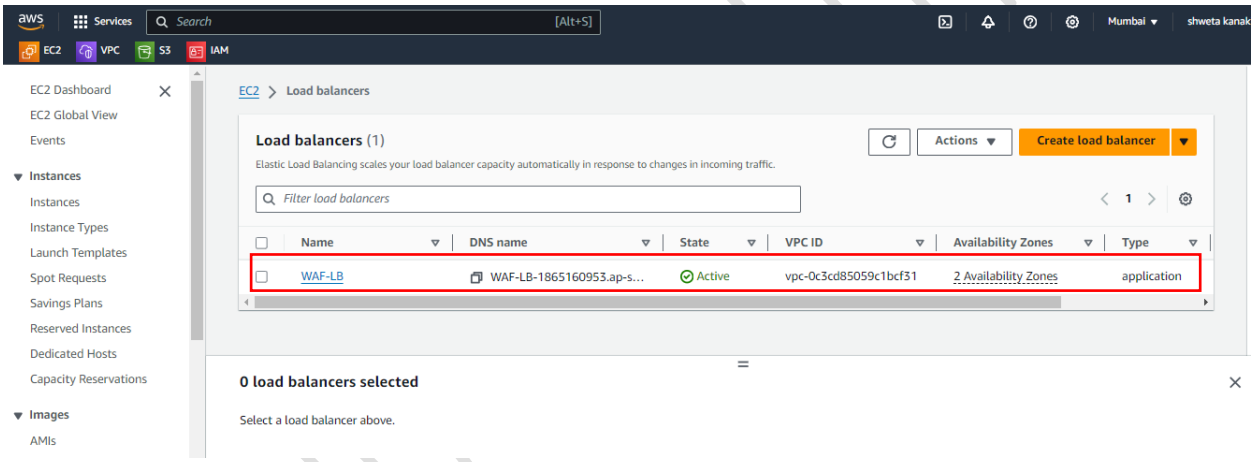
Configure a simple index.html page in both the instances

hii..we are working on Web Application Firewall

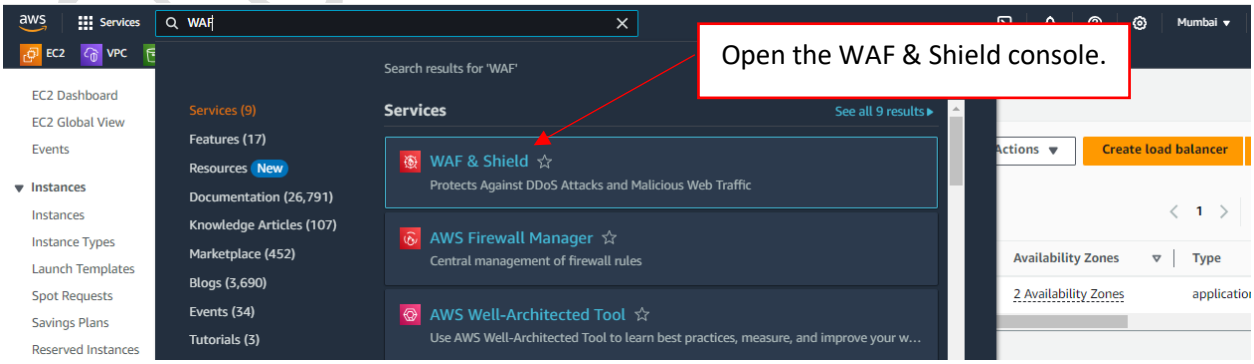
Instance “ec2-waf-1”

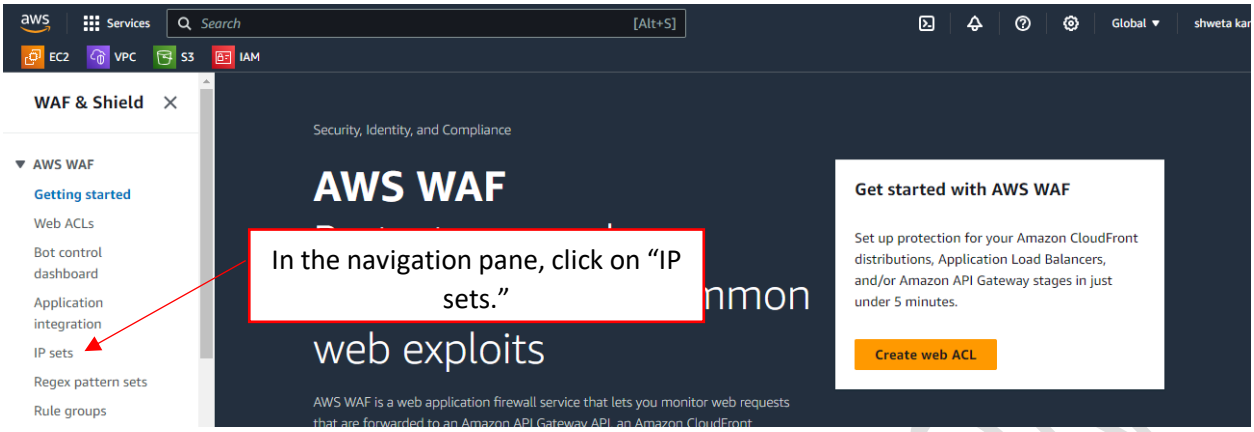


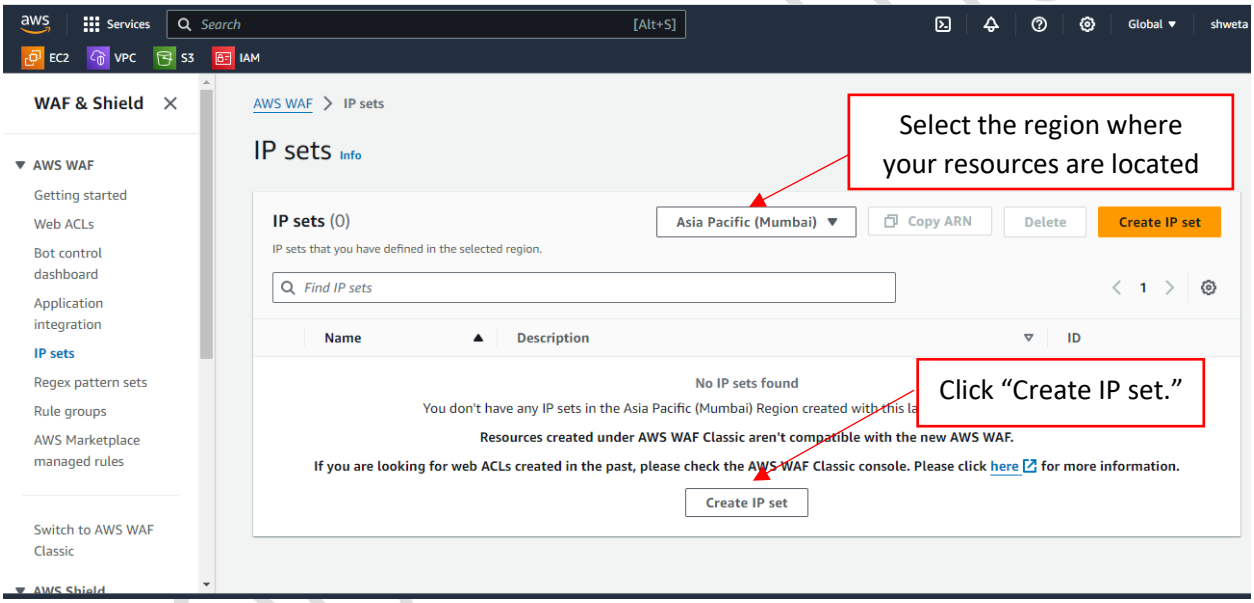
Step 2: Create an Application Load Balancer with the Target Group associated with it.

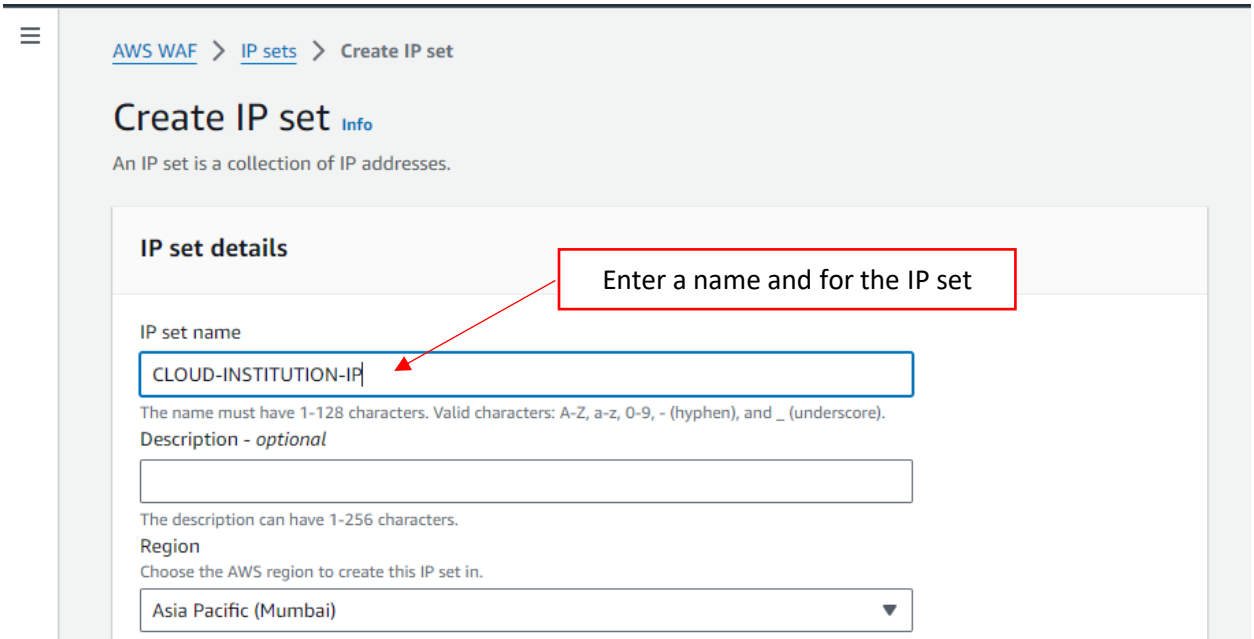


Step 3: Create an IP Set in AWS WAF

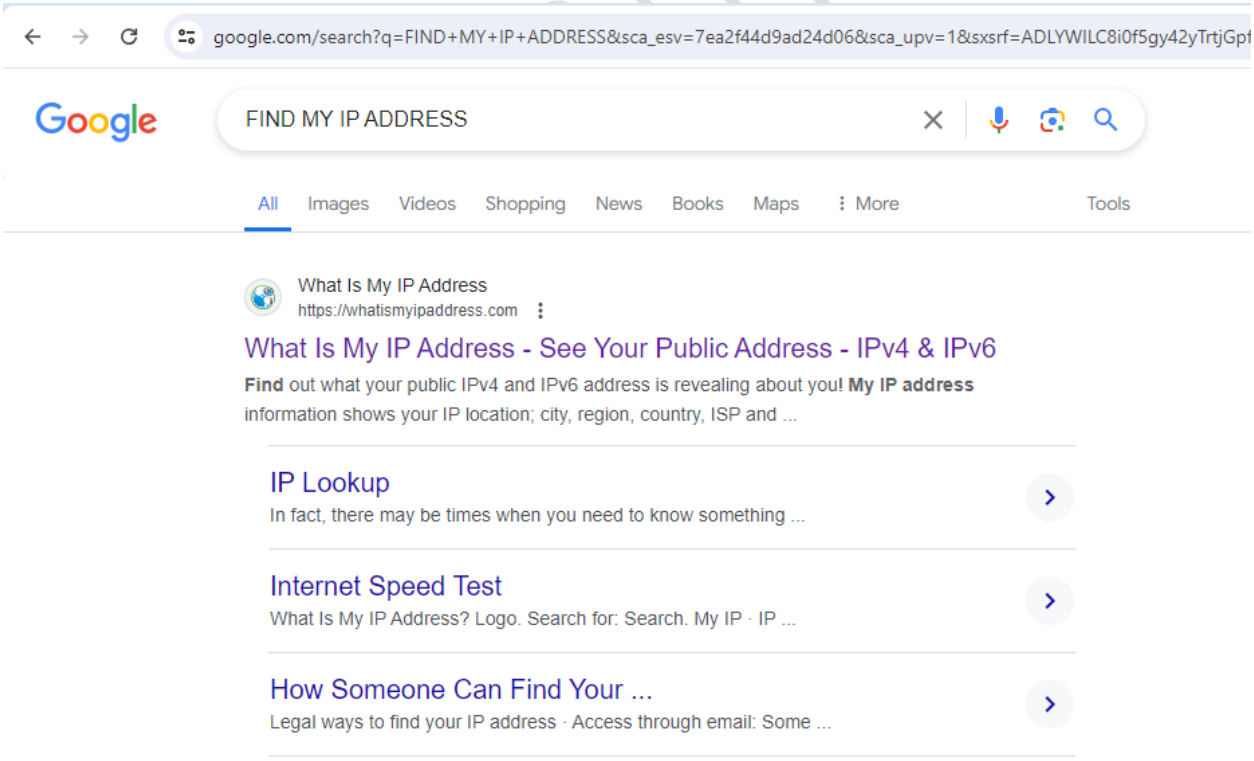


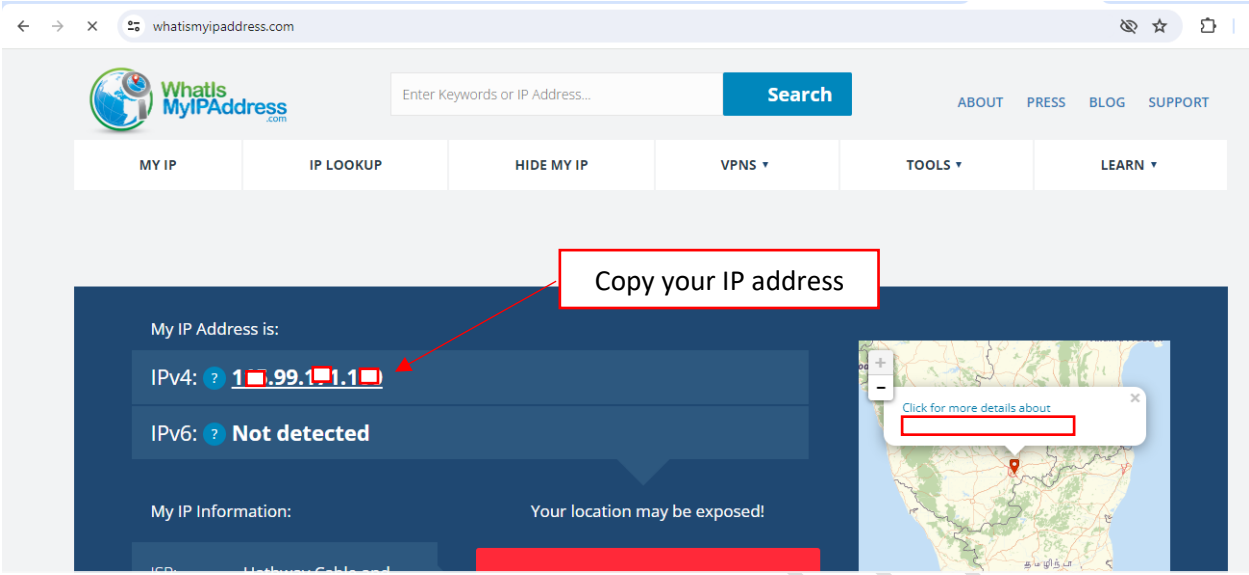

aws
Services
Search
[Alt+S]
Global
EC2
VPC
S3
IAM
WAF & Shield
AWS WAF
Getting started
Web ACLs
Bot control dashboard
Application integration
IP sets
Regex pattern sets
Rule groups
Security, Identity, and Compliance
AWS WAF
In the navigation pane, click on "IP sets."
web exploits
AWS WAF is a web application firewall service that lets you monitor web requests
Get started with AWS WAF
Set up protection for your Amazon CloudFront distributions, Application Load Balancers, and/or Amazon API Gateway stages in just under 5 minutes.
Create web ACL

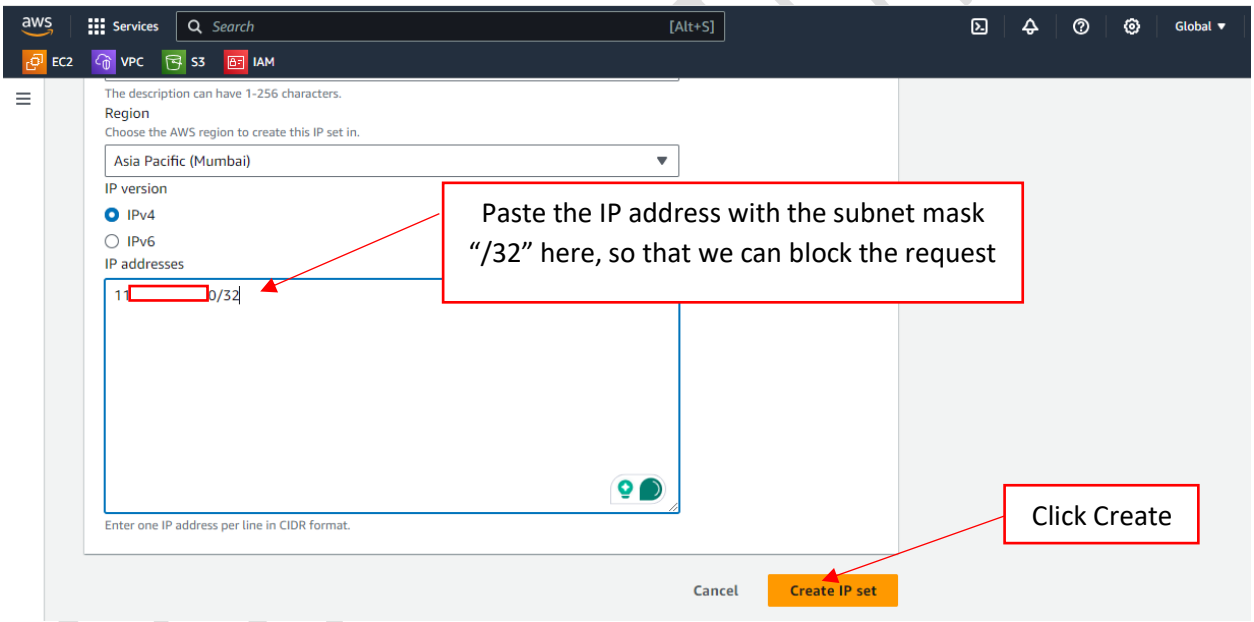

aws
Services
Search
[Alt+S]
Global
EC2
VPC
S3
IAM
WAF & Shield
AWS WAF
Getting started
Web ACLs
Bot control dashboard
Application integration
IP sets
Regex pattern sets
Rule groups
AWS Marketplace managed rules
Switch to AWS WAF Classic
AWS WAF > IP sets
IP sets Info
Select the region where your resources are located
IP sets (0)
IP sets that you have defined in the selected region.
Asia Pacific (Mumbai)
Copy ARN
Delete
Create IP set
Find IP sets
Name
Description
ID
No IP sets found
You don't have any IP sets in the Asia Pacific (Mumbai) Region created with this la
Click "Create IP set."
Resources created under AWS WAF Classic aren't compatible with the new AWS WAF.
If you are looking for web ACLs created in the past, please check the AWS WAF Classic console. Please click here for more information.
Create IP set

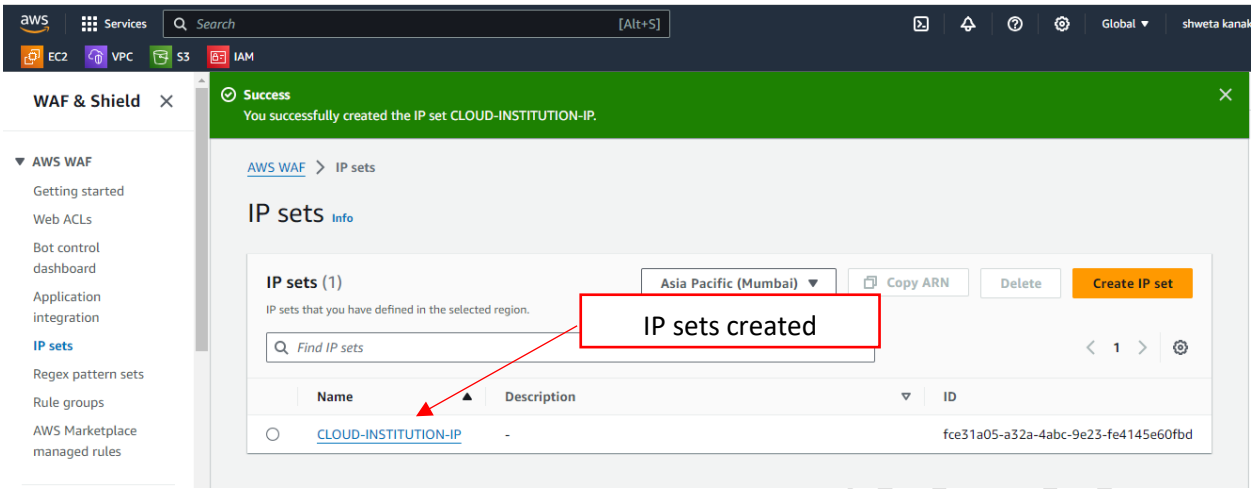


Now go to your browser and check for your systems' IP address.

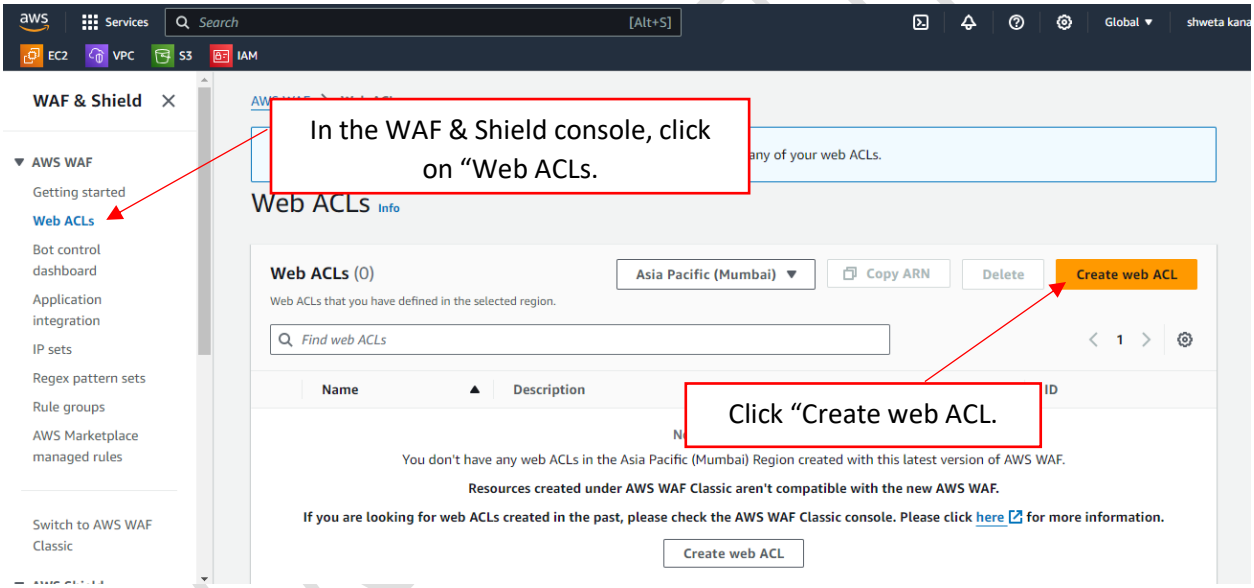


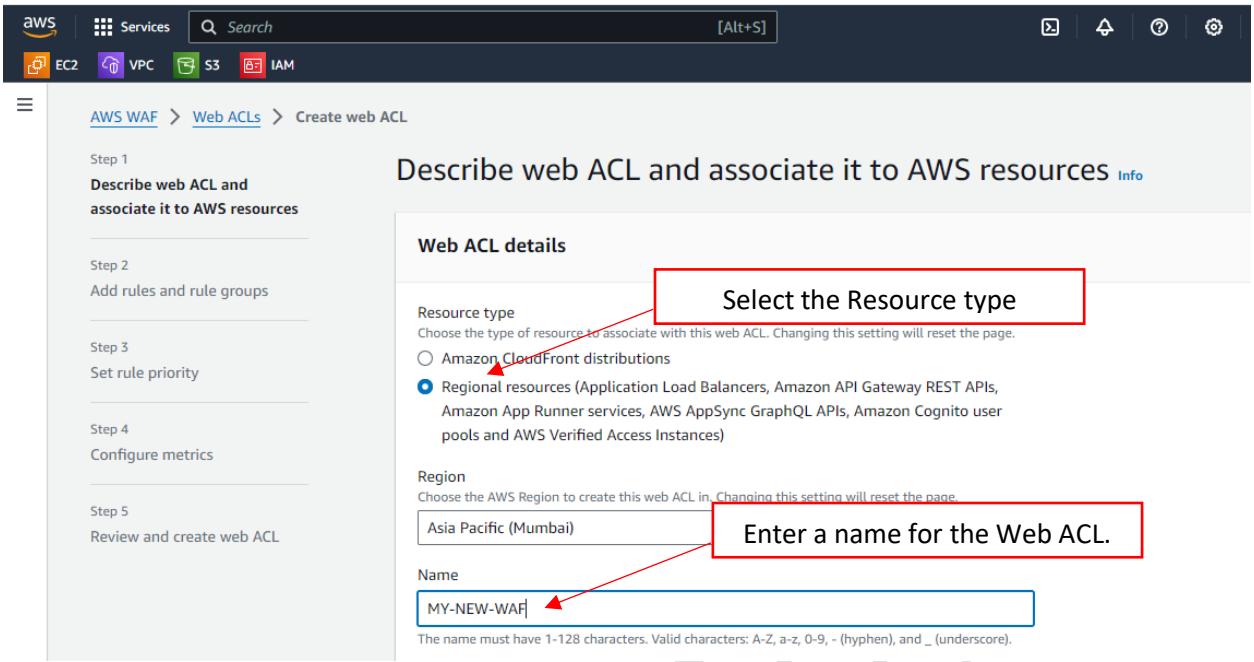

whatismyipaddress.com
WhatIsMyIPAddress.com
Enter Keywords or IP Address...
Search
ABOUT
PRESS
BLOG
SUPPORT
MY IP
IP LOOKUP
HIDE MY IP
VPNS
TOOLS
LEARN
Copy your IP address
My IP Address is:
IPv4: 1[redacted].99.1[redacted]1.1[redacted]
IPv6: Not detected
My IP Information:
Your location may be exposed!
Click for more details about

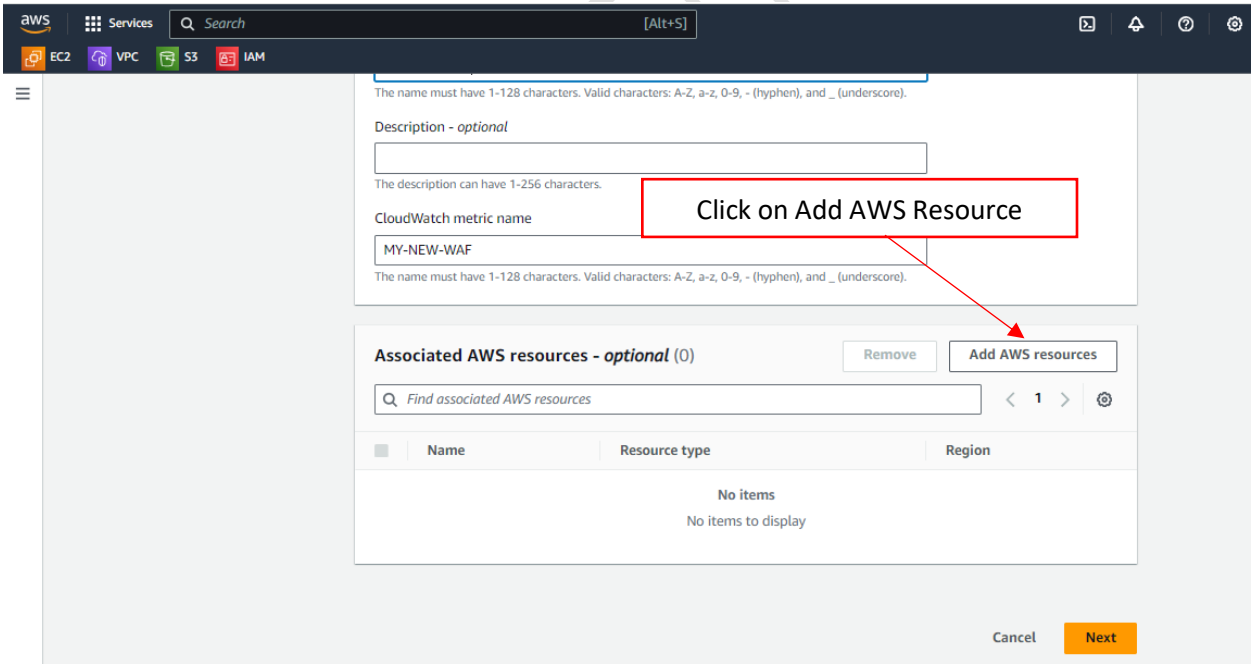

aws
Services
Search
[Alt+S]
Global
EC2
VPC
S3
IAM
The description can have 1-256 characters.
Region
Choose the AWS region to create this IP set in.
Asia Pacific (Mumbai)
IP version
IPv4
IPv6
IP addresses
1[redacted]0/32
Enter one IP address per line in CIDR format.
Paste the IP address with the subnet mask "/32" here, so that we can block the request
Click Create
Cancel
Create IP set

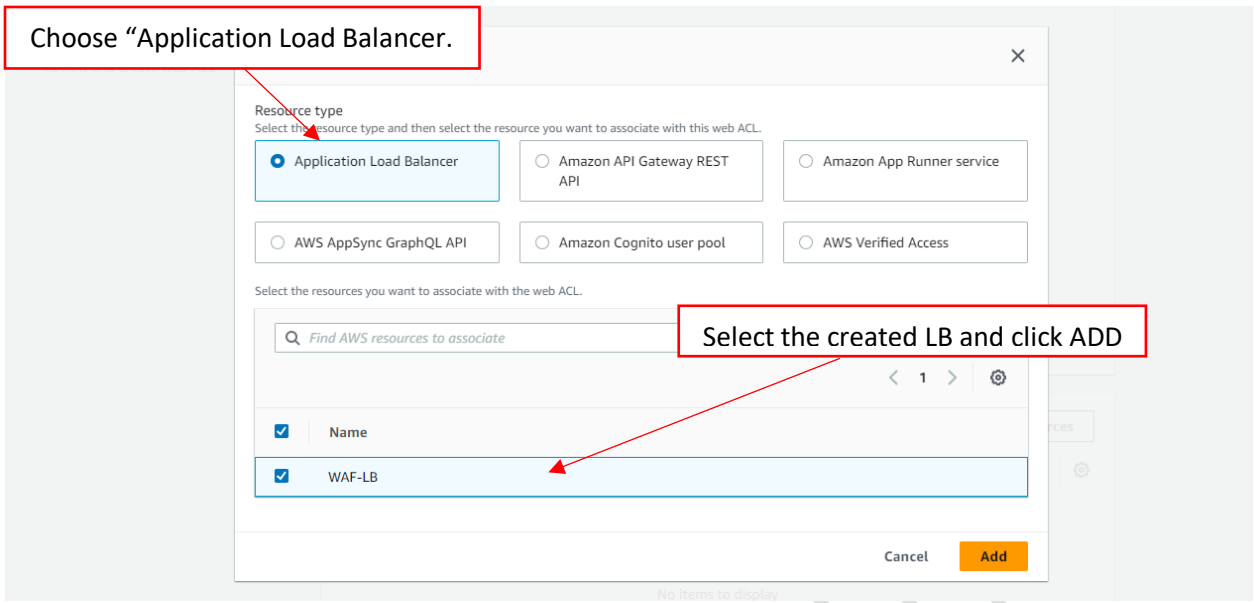


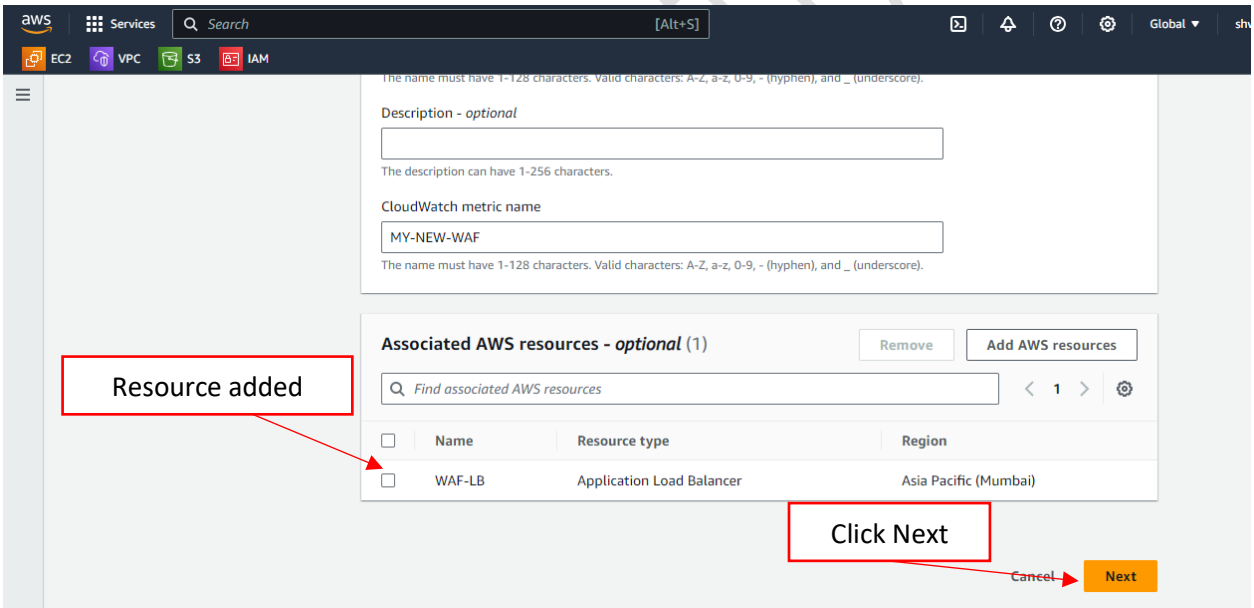
Step 4: Create a Web ACL in AWS WAF.



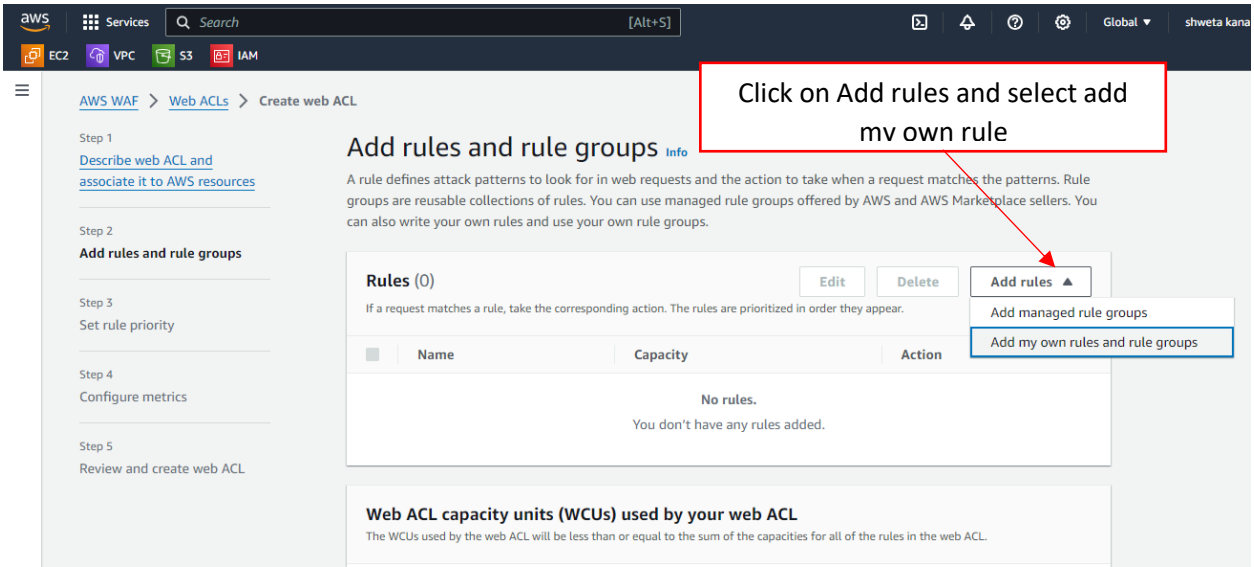

aws
Services
Search
[Alt+S]
EC2
VPC
S3
IAM
AWS WAF > Web ACLs > Create web ACL
Step 1
Describe web ACL and associate it to AWS resources
Step 2
Add rules and rule groups
Step 3
Set rule priority
Step 4
Configure metrics
Step 5
Review and create web ACL
Describe web ACL and associate it to AWS resources Info
Web ACL details
Select the Resource type
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, Amazon App Runner services, AWS AppSync GraphQL APIs, Amazon Cognito user pools and AWS Verified Access Instances)
Region
Choose the AWS Region to create this web ACL in. Changing this setting will reset the page.
Asia Pacific (Mumbai)
Enter a name for the Web ACL.
Name
MY-NEW-WAF
The name must have 1-128 characters. Valid characters: A-Z, a-z, 0-9, - (hyphen), and _ (underscore).

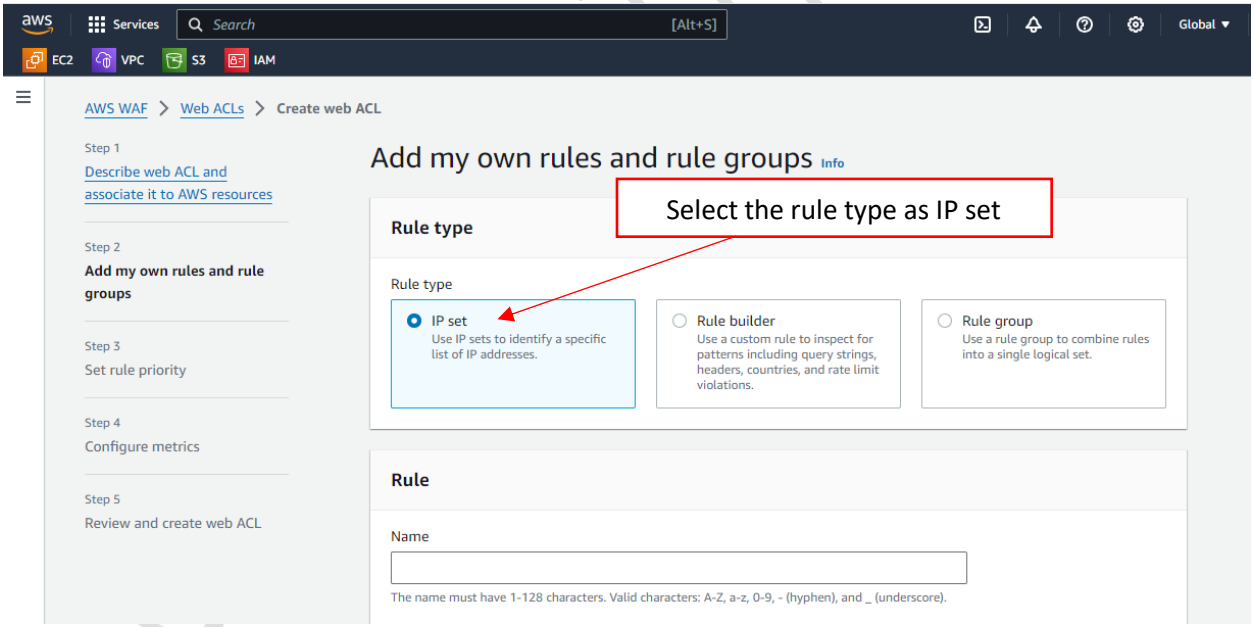

aws
Services
Search
[Alt+S]
EC2
VPC
S3
IAM
The name must have 1-128 characters. Valid characters: A-Z, a-z, 0-9, - (hyphen), and _ (underscore).
Description - optional
The description can have 1-256 characters.
Click on Add AWS Resource
CloudWatch metric name
MY-NEW-WAF
The name must have 1-128 characters. Valid characters: A-Z, a-z, 0-9, - (hyphen), and _ (underscore).
Associated AWS resources - optional (0)
Remove
Add AWS resources
Find associated AWS resources
1
Name
Resource type
Region
No items
No items to display
Cancel
Next

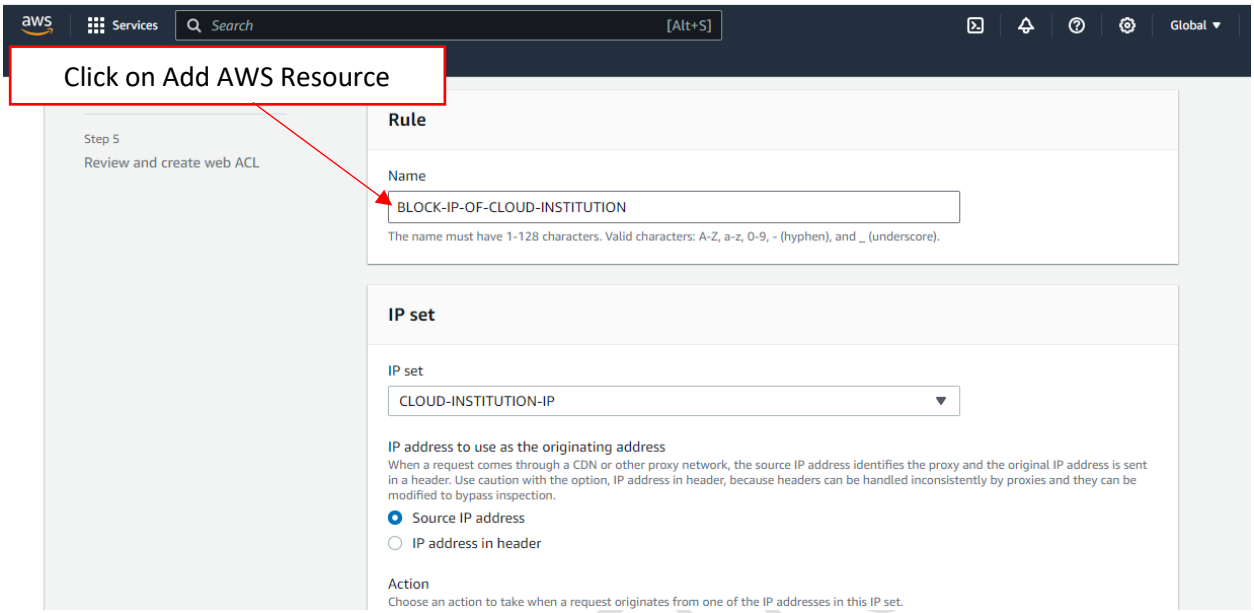

Choose “Application Load Balancer.
Resource type
Select the resource type and then select the resource you want to associate with this web ACL.
Application Load Balancer
Amazon API Gateway REST API
Amazon App Runner service
AWS AppSync GraphQL API
Amazon Cognito user pool
AWS Verified Access
Select the resources you want to associate with the web ACL.
Find AWS resources to associate
Select the created LB and click ADD
Name
WAF-LB
Cancel
Add

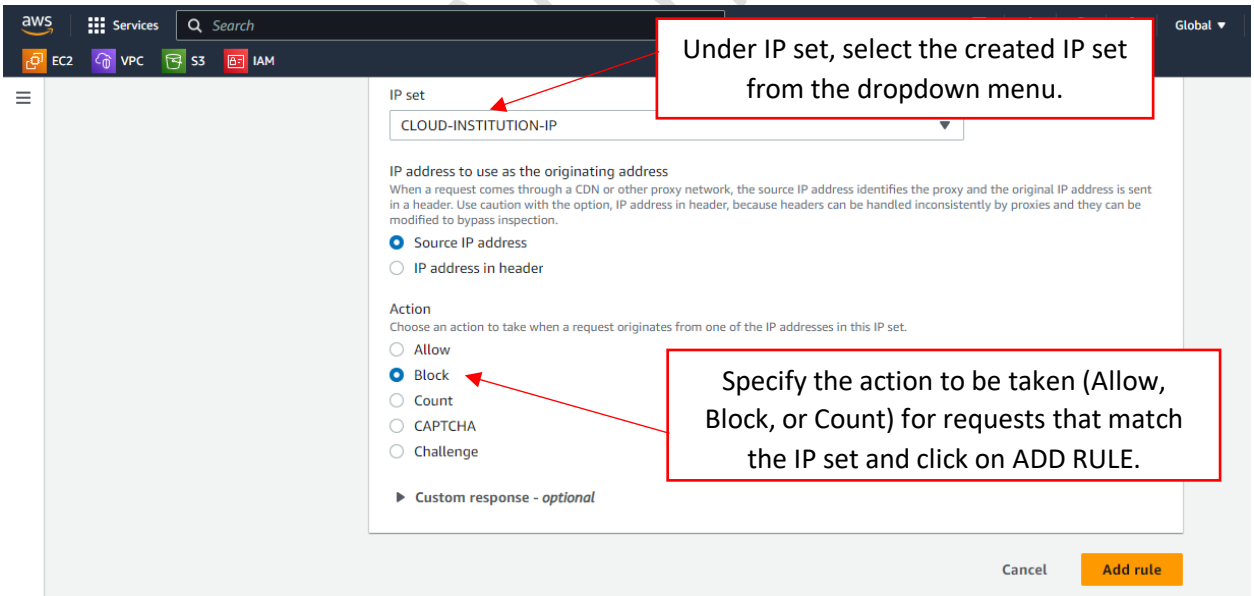

aws
Services
Search
[Alt+S]
Global
EC2
VPC
S3
IAM
Description - optional
The description can have 1-256 characters.
CloudWatch metric name
MY-NEW-WAF
The name must have 1-128 characters. Valid characters: A-Z, a-z, 0-9, - (hyphen), and _ (underscore).
Associated AWS resources - optional (1)
Remove
Add AWS resources
Find associated AWS resources
Resource added
Name
Resource type
Region
WAF-LB
Application Load Balancer
Asia Pacific (Mumbai)
Click Next
Cancel
Next

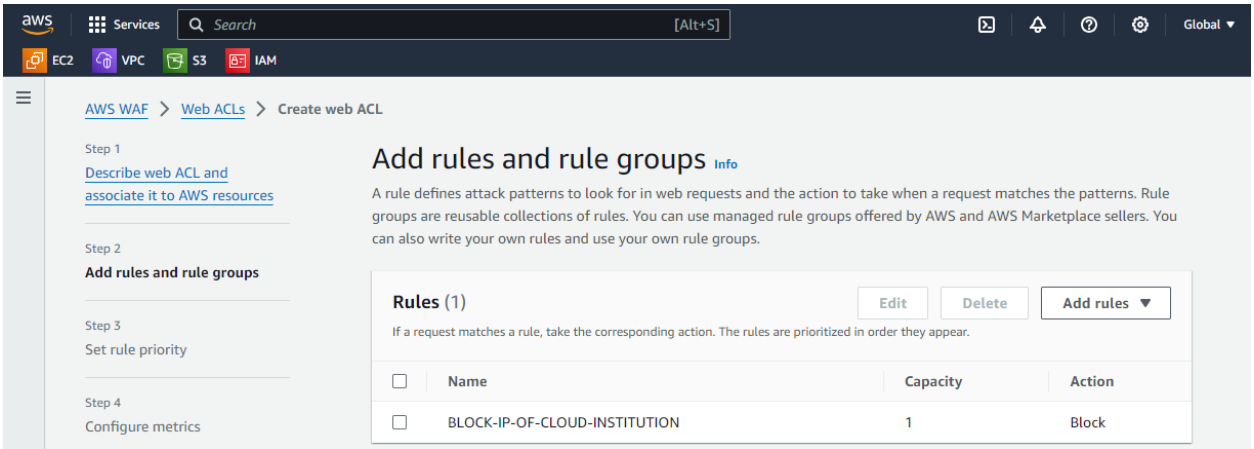
Add Rules to the Web ACL

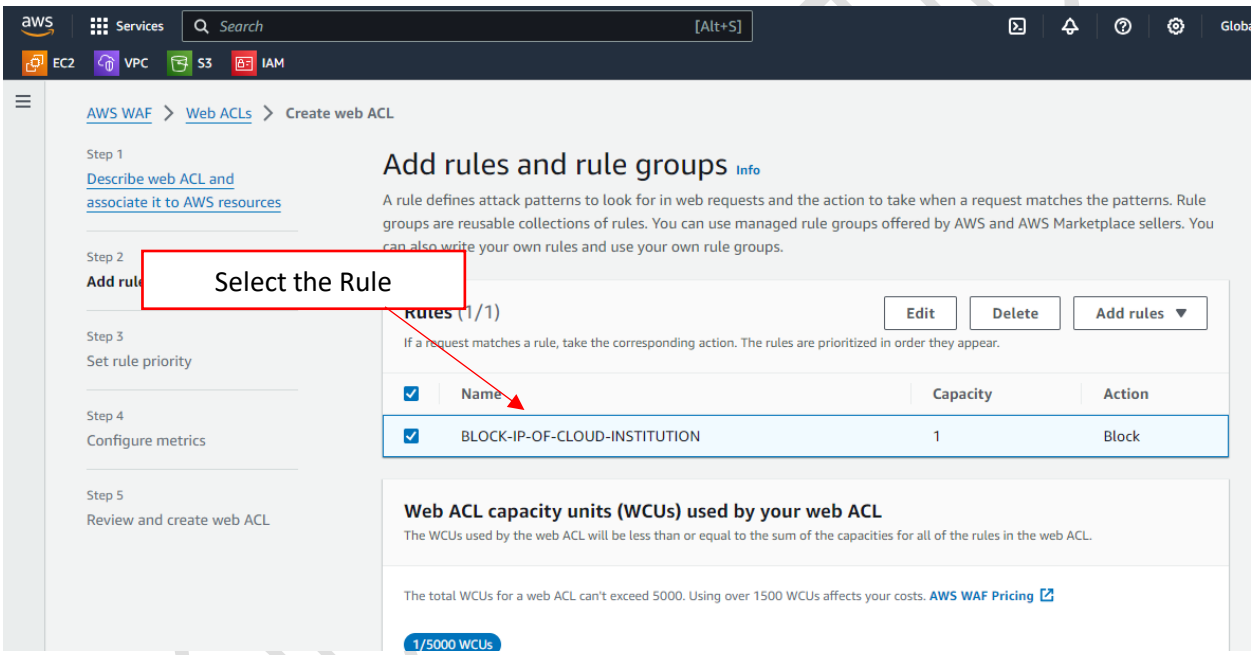


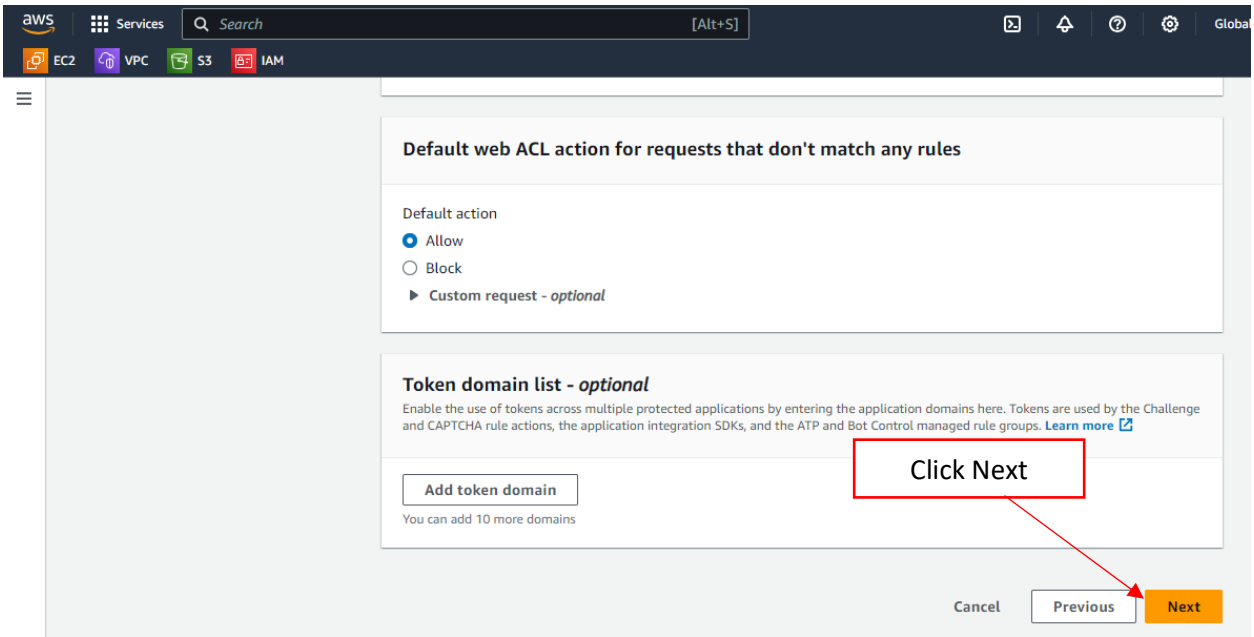


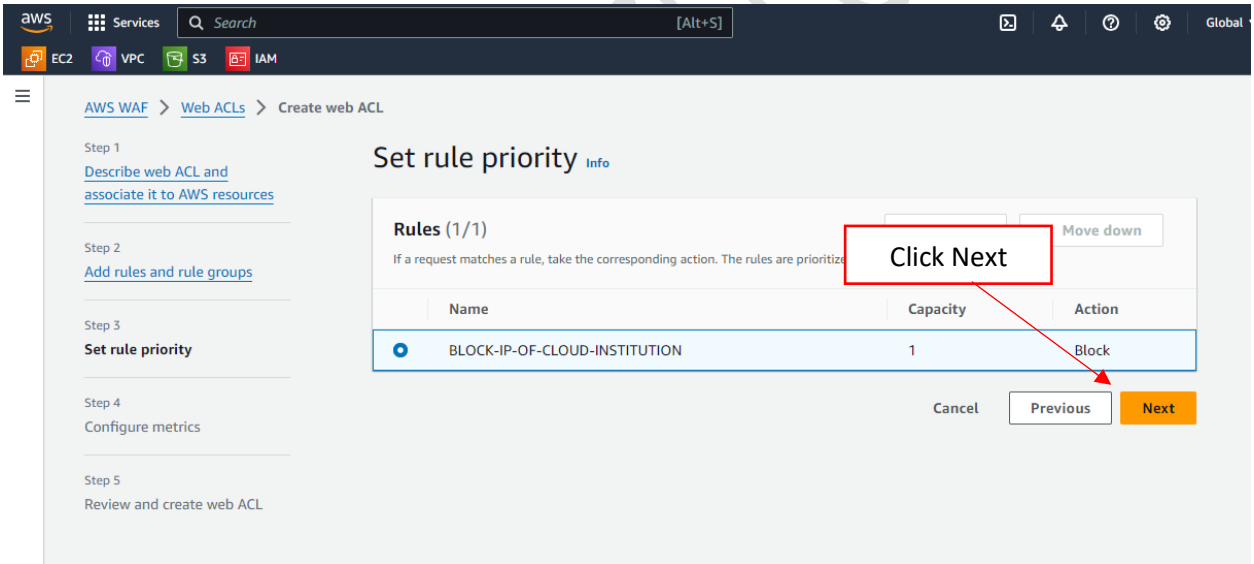

Click on Add AWS Resource
Step 5
Review and create web ACL
Rule
Name
BLOCK-IP-OF-CLOUD-INSTITUTION
The name must have 1-128 characters. Valid characters: A-Z, a-z, 0-9, - (hyphen), and _ (underscore).
IP set
IP set
CLOUD-INSTITUTION-IP
IP address to use as the originating address
When a request comes 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
Action
Choose an action to take when a request originates from one of the IP addresses in this IP set.

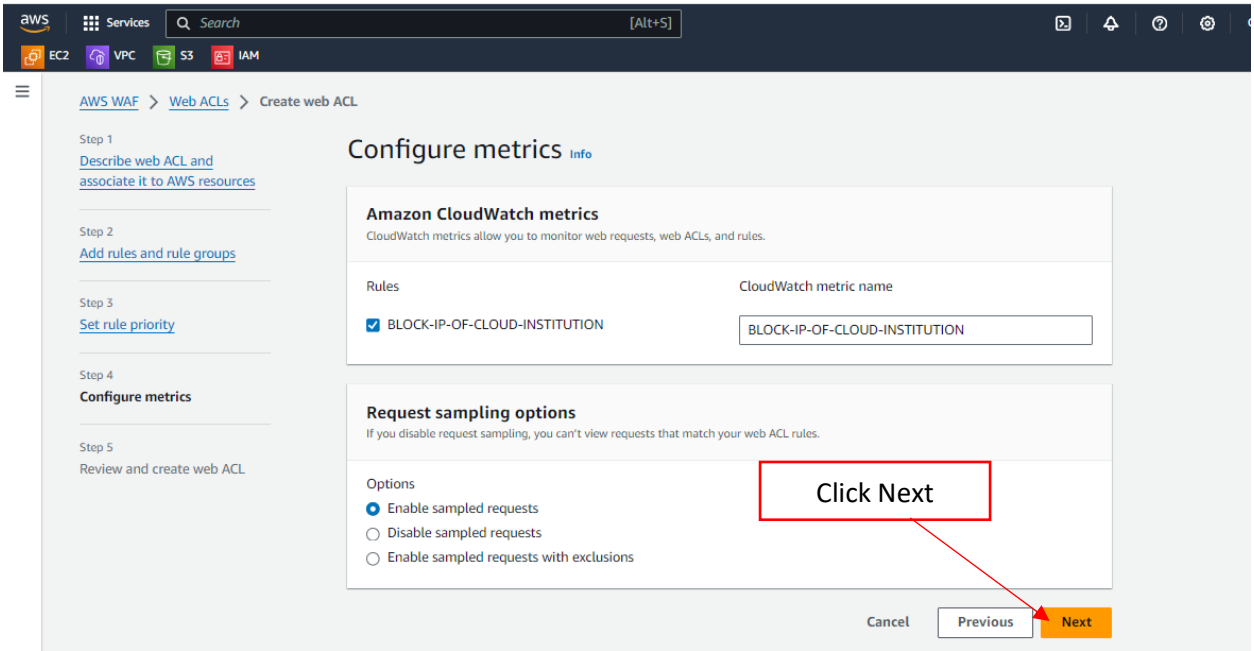

Under IP set, select the created IP set from the dropdown menu.
IP set
CLOUD-INSTITUTION-IP
IP address to use as the originating address
When a request comes through a CDN or other proxy network, the source IP address identifies the proxy and the original IP address is sent in a header. Use caution with 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
Action
Choose an action to take when a request originates from one of the IP addresses in this IP set.
Allow
Block
Count
CAPTCHA
Challenge
Specify the action to be taken (Allow, Block, or Count) for requests that match the IP set and click on ADD RULE.
Custom response - optional
Cancel
Add rule

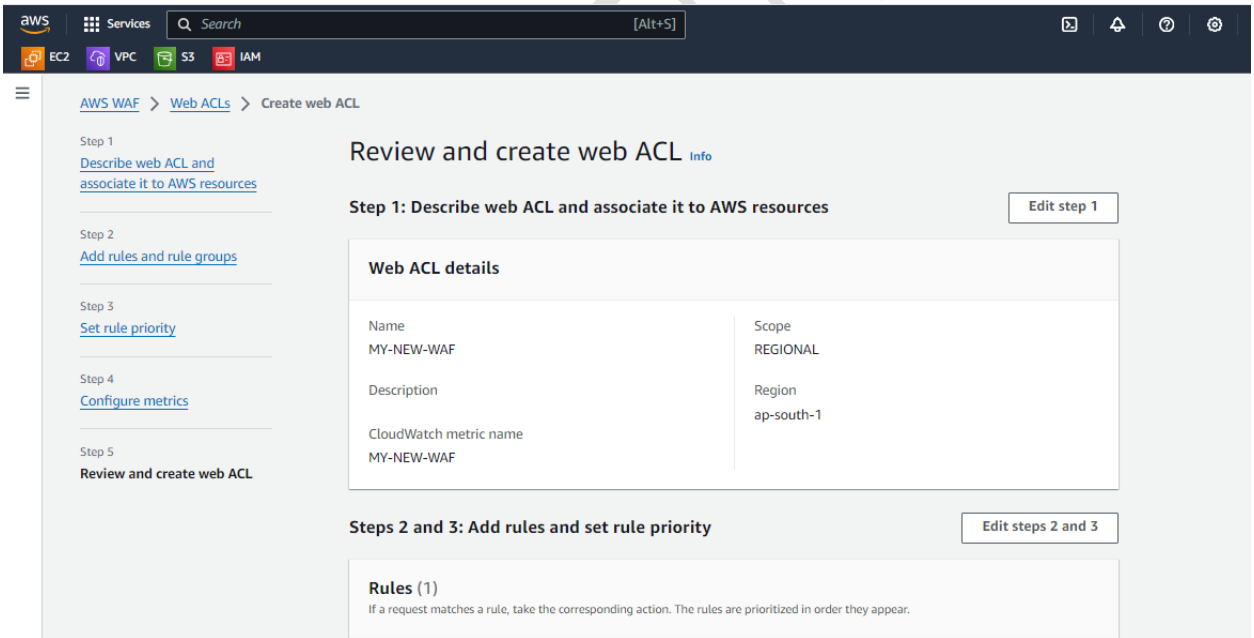

aws
Services
Search
[Alt+S]
Global
EC2
VPC
S3
IAM
AWS WAF > Web ACLs > Create web ACL
Step 1
Describe web ACL and associate it to AWS resources
Step 2
Add rules and rule groups
Step 3
Set rule priority
Step 4
Configure metrics
Add rules and rule groups Info
A rule defines attack patterns to look for 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
BLOCK-IP-OF-CLOUD-INSTITUTION
1
Block

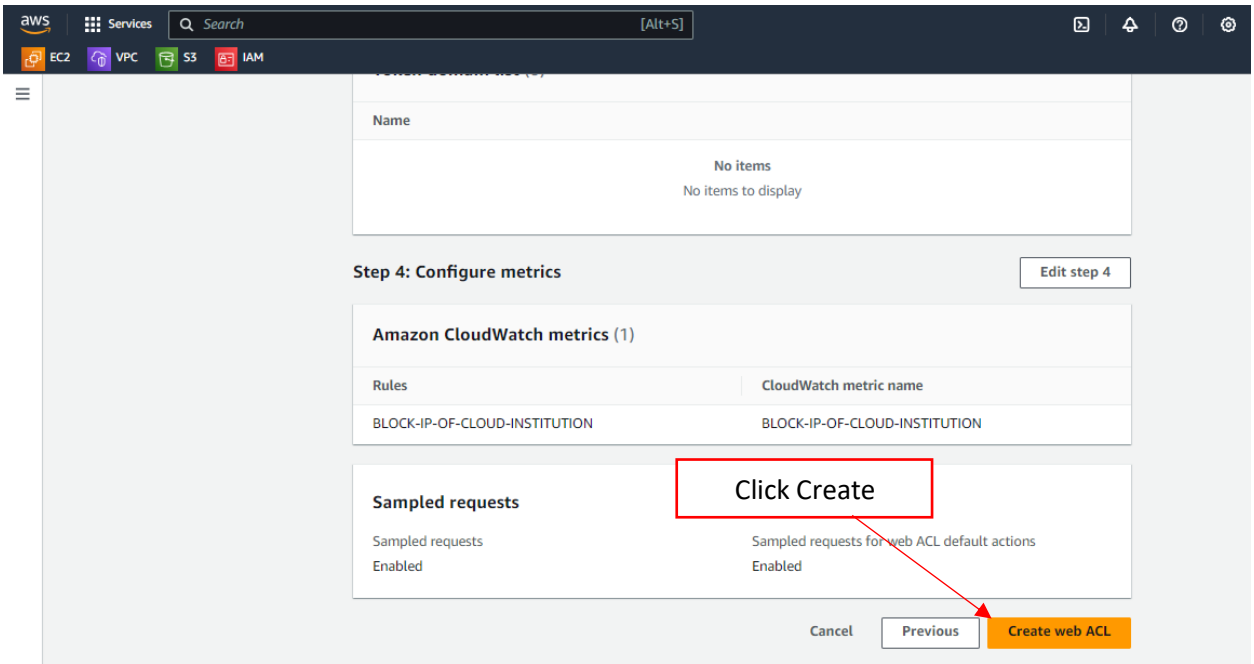

aws
Services
Search
[Alt+S]
EC2
VPC
S3
IAM
AWS WAF > Web ACLs > Create web ACL
Step 1
Describe web ACL and associate it to AWS resources
Step 2
Add rule
Select the Rule
Step 3
Set rule priority
Step 4
Configure metrics
Step 5
Review and create web ACL
Add rules and rule groups Info
A rule defines attack 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 (1/1)
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
BLOCK-IP-OF-CLOUD-INSTITUTION
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

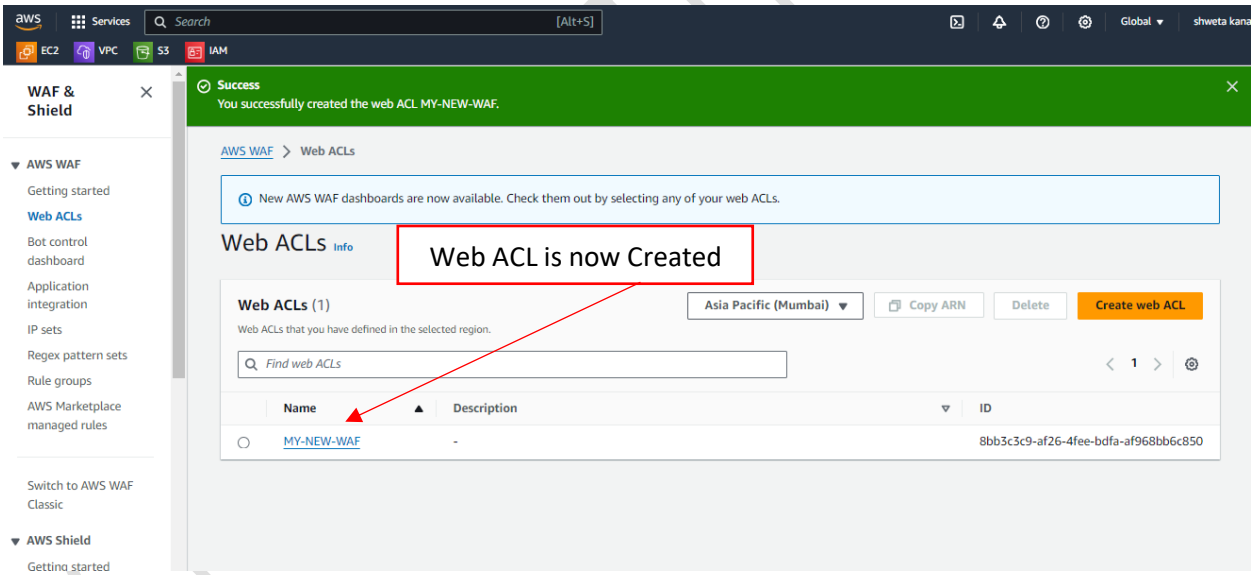

aws
Services
Search
[Alt+S]
EC2
VPC
S3
IAM
Default web ACL action for requests that don't match any rules
Default action
Allow
Block
Custom request - optional
Token domain list - optional
Enable the use of tokens across multiple protected applications by entering the application domains here. Tokens 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
Click Next
Cancel
Previous
Next


aws
Services
Search
[Alt+S]
EC2
VPC
S3
IAM
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 (1/1)
If a request matches a rule, take the corresponding action. The rules are prioritize
Move down
Click Next
Name
Capacity
Action
BLOCK-IP-OF-CLOUD-INSTITUTION
1
Block
Cancel
Previous
Next


aws
Services
Search
[Alt+S]
EC2
VPC
S3
IAM
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
Configure metrics Info
Amazon CloudWatch metrics
CloudWatch metrics allow you to monitor web requests, web ACLs, and rules.
Rules
CloudWatch metric name
BLOCK-IP-OF-CLOUD-INSTITUTION
BLOCK-IP-OF-CLOUD-INSTITUTION
Request sampling options
If you disable request sampling, you can't view requests that match your web ACL rules.
Options
Enable sampled requests
Disable sampled requests
Enable sampled requests with exclusions
Click Next
Cancel
Previous
Next


aws
Services
Search
[Alt+S]
EC2
VPC
S3
IAM
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
MY-NEW-WAF
Scope
REGIONAL
Description
Region
ap-south-1
CloudWatch metric name
MY-NEW-WAF
Steps 2 and 3: Add rules and set rule priority
Edit steps 2 and 3
Rules (1)
If a request matches a rule, take the corresponding action. The rules are prioritized in order they appear.





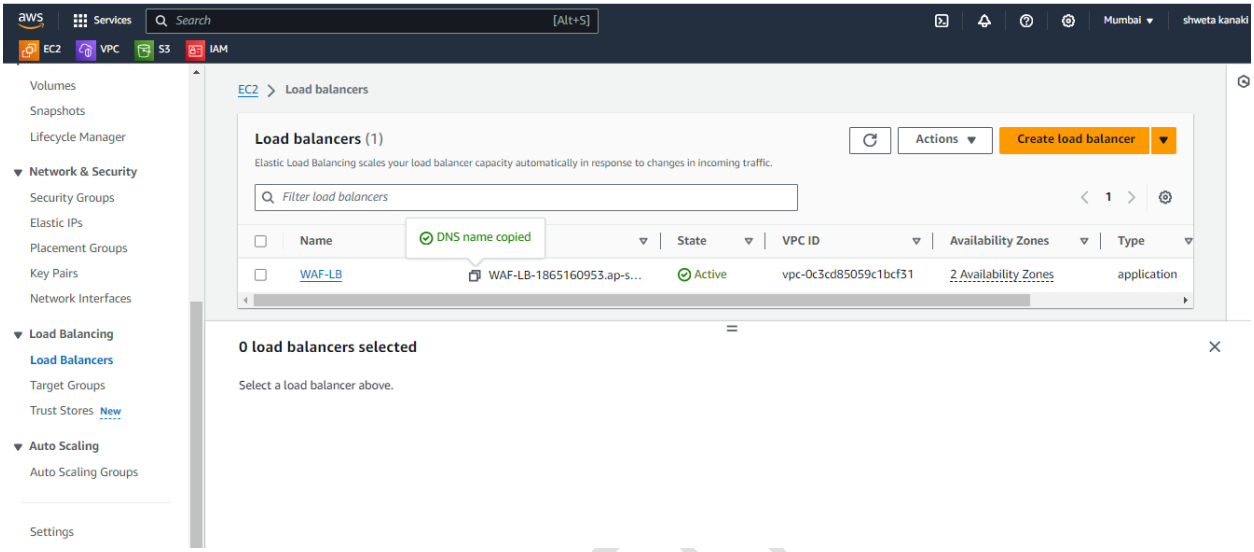
Step 5 : Verify the Configuration

Verify the Association:

- Navigate to the AWS WAF & Shield console.
- Select your Web ACL and check the “Associated AWS resources” tab.
- Ensure your Application Load Balancer is listed.

Step 6: Testing the AWS WAF.

Now go to the Load Balancer and copy the DNS Name and paste it in the browser.



403 Forbidden

It is giving a “403 forbidden” error because the access is blocked.

We can also see from where the requests are coming from.