AWS Web Application Firewall

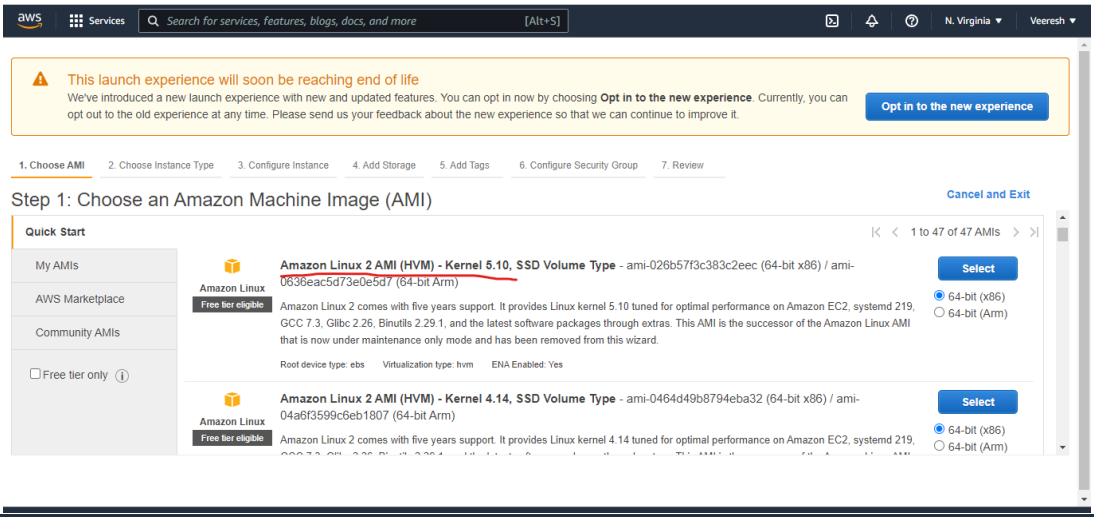
AWS Web Application Firewall (WAF) is a security tool that helps you to protect the application against web attacks. WAF monitors and controls unusual bot traffic, blocks common attack patterns, such as SQL Injection or Cross-site scripting, etc. It also lets you monitor the HTTP and HTTPS requests that are forwarded to an Amazon API Gateway API, Amazon CloudFront or an Application Load Balancer.

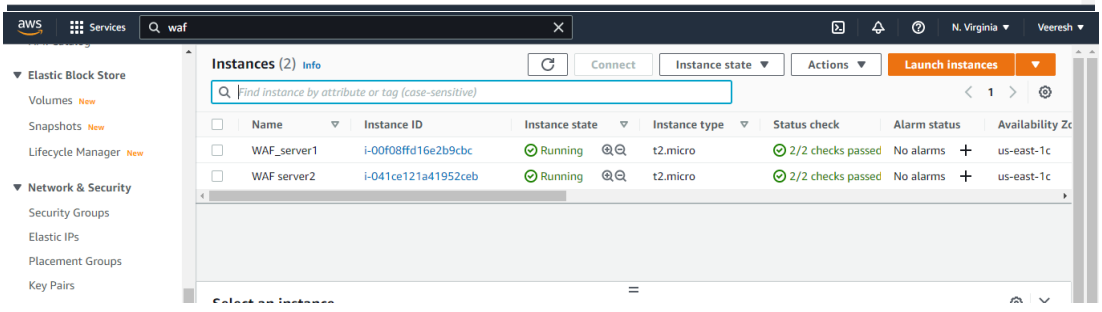
- Amazon WAF allows you to control your content by using an IP address from where the request originates.
- Three things make Amazon WAF work – Access control lists (ACL), Rules and Rule Group.
- Amazon WAF manages Web ACL capacity units (WCU) for rules, rule groups and web ACLs.
- Amazon WAF includes a full-featured API that you can use to automate the creation, deployment, and maintenance of security rules.

Step by step Handson WAF:

Step 1 : Create Load balancer and attach it to the Working Ec2 instances.

- Launch the Ec2 instances which are contains httpd running application with static webpage.
- Create load balancer and target group attach above two instances to that Target group.
- When the health checks are health then take DNS name and run in browser it will work.



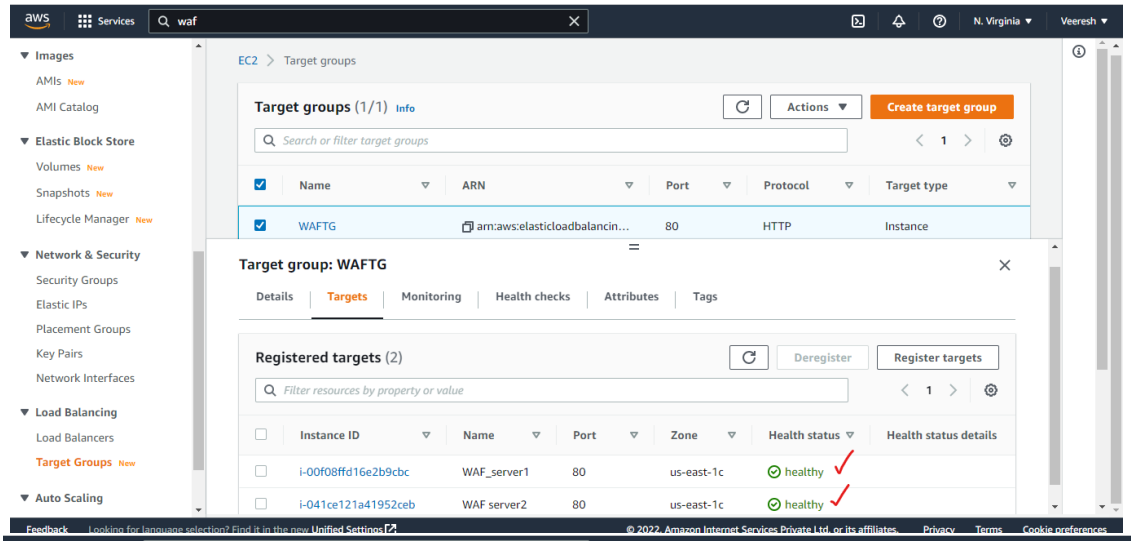


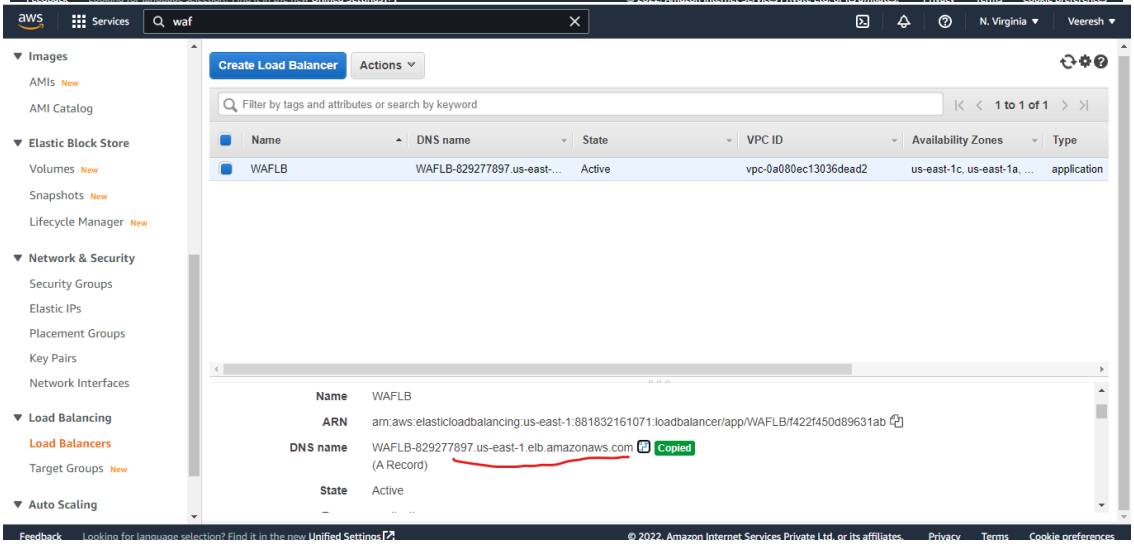
Not secure | 54.144.246.202

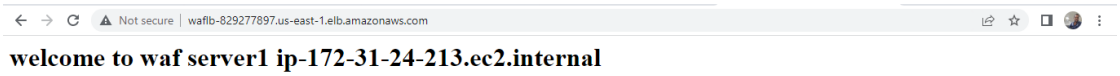
welcome to waf server1 ip-172-31-24-213.ec2.internal

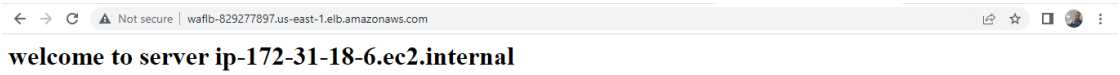
Not secure | 3.83.236.9

welcome to server ip-172-31-18-6.ec2.internal



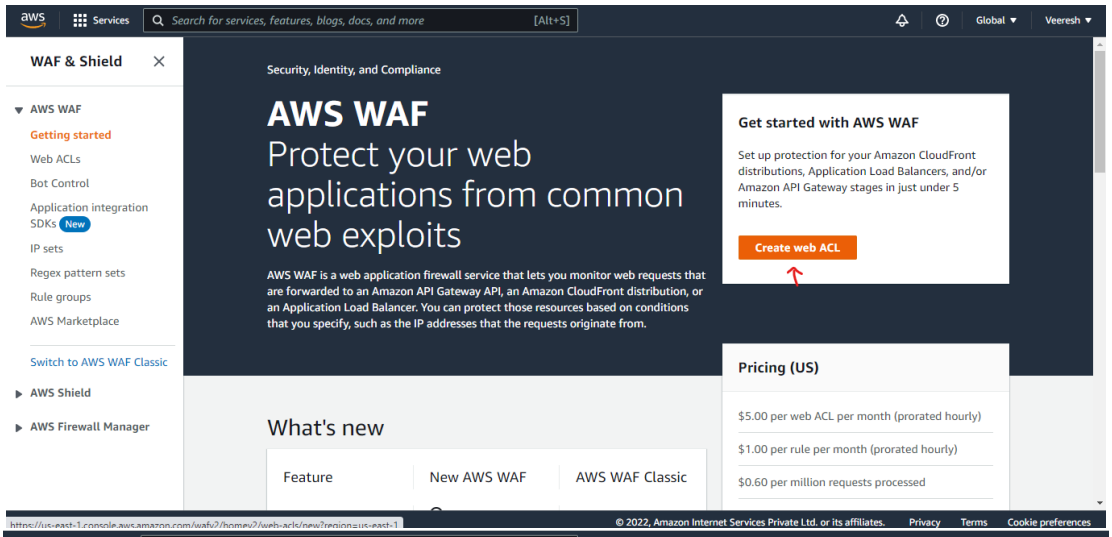


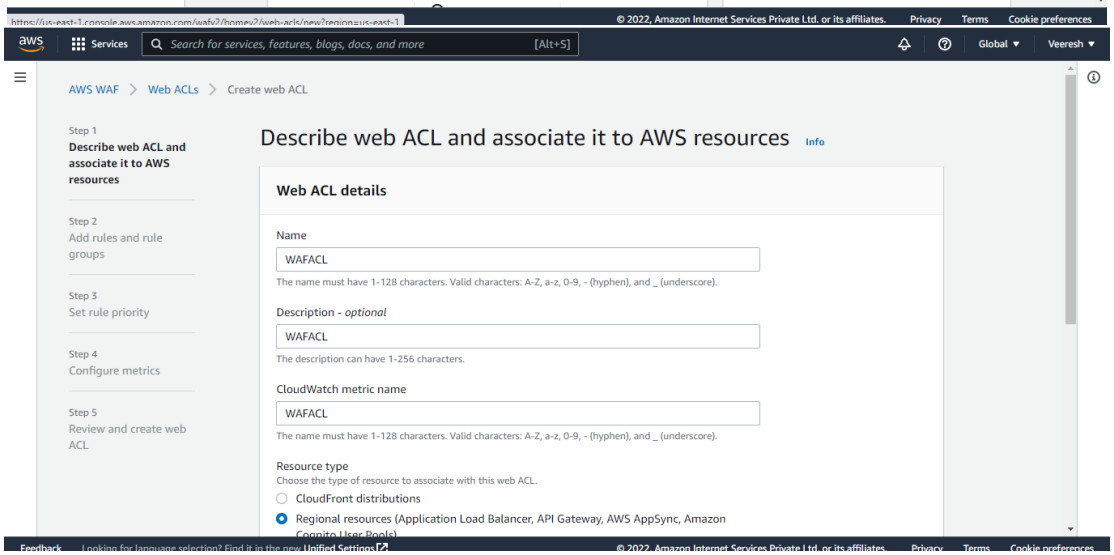


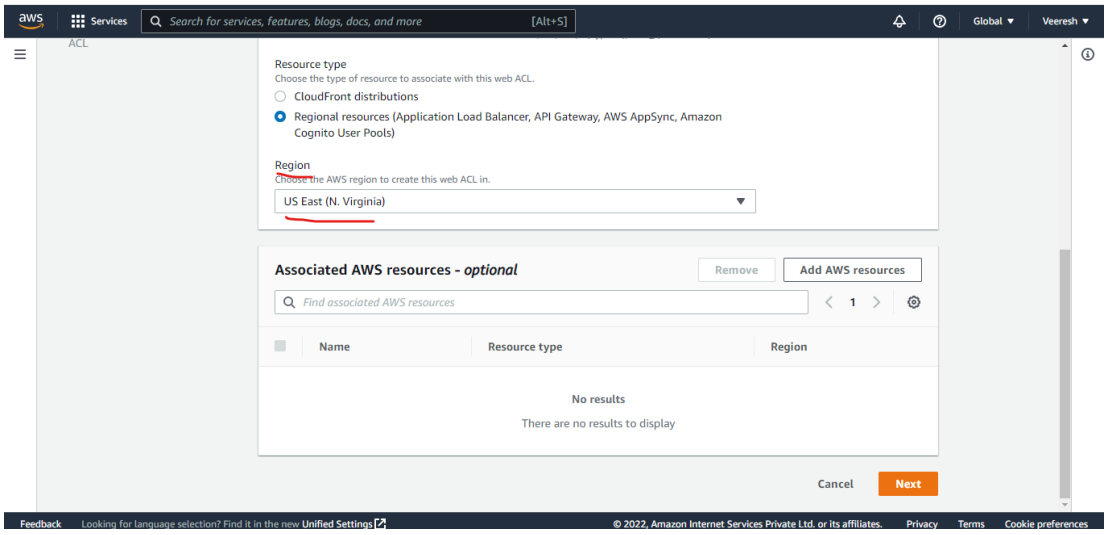


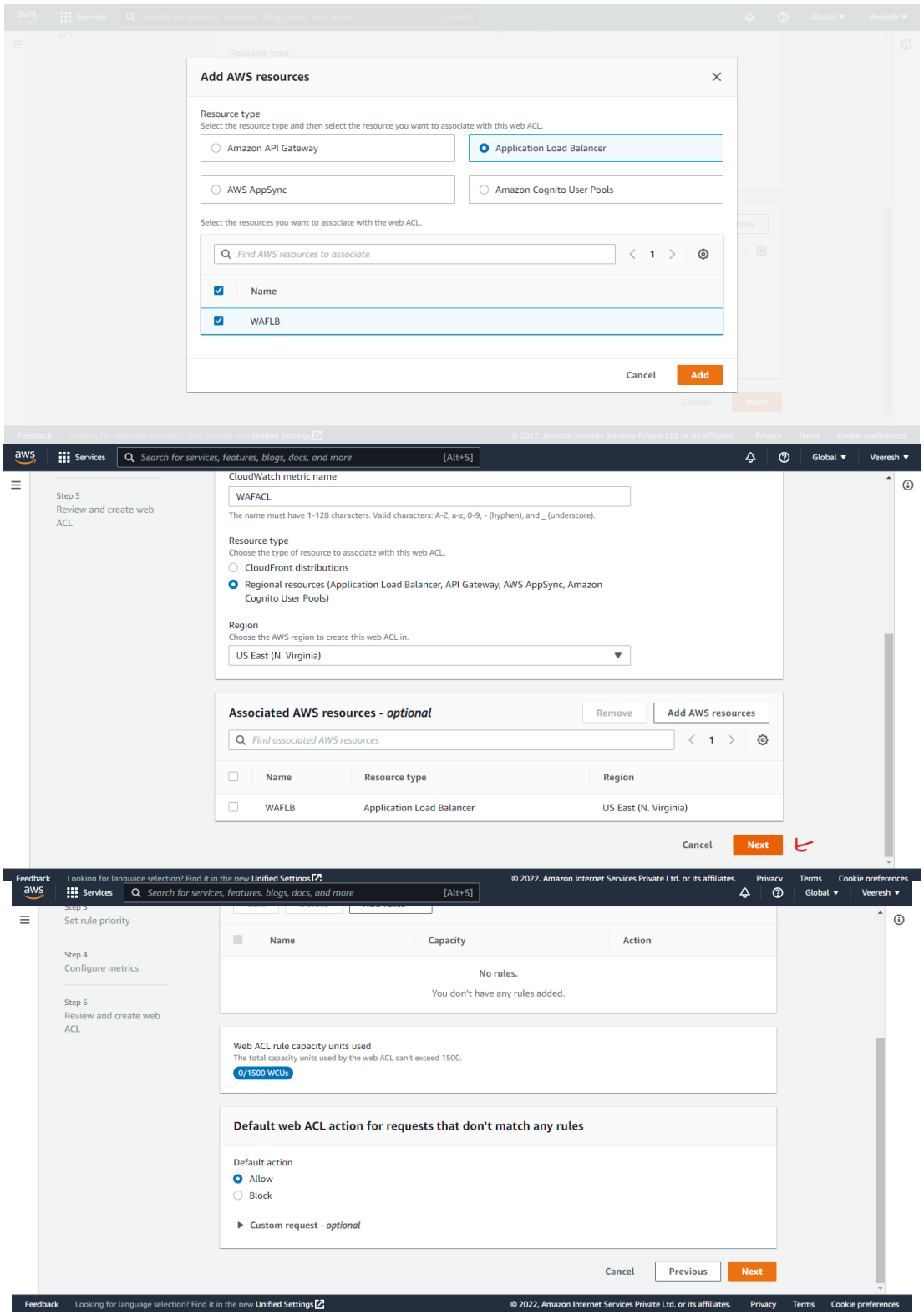
Step 2: Now create Web application firewall.

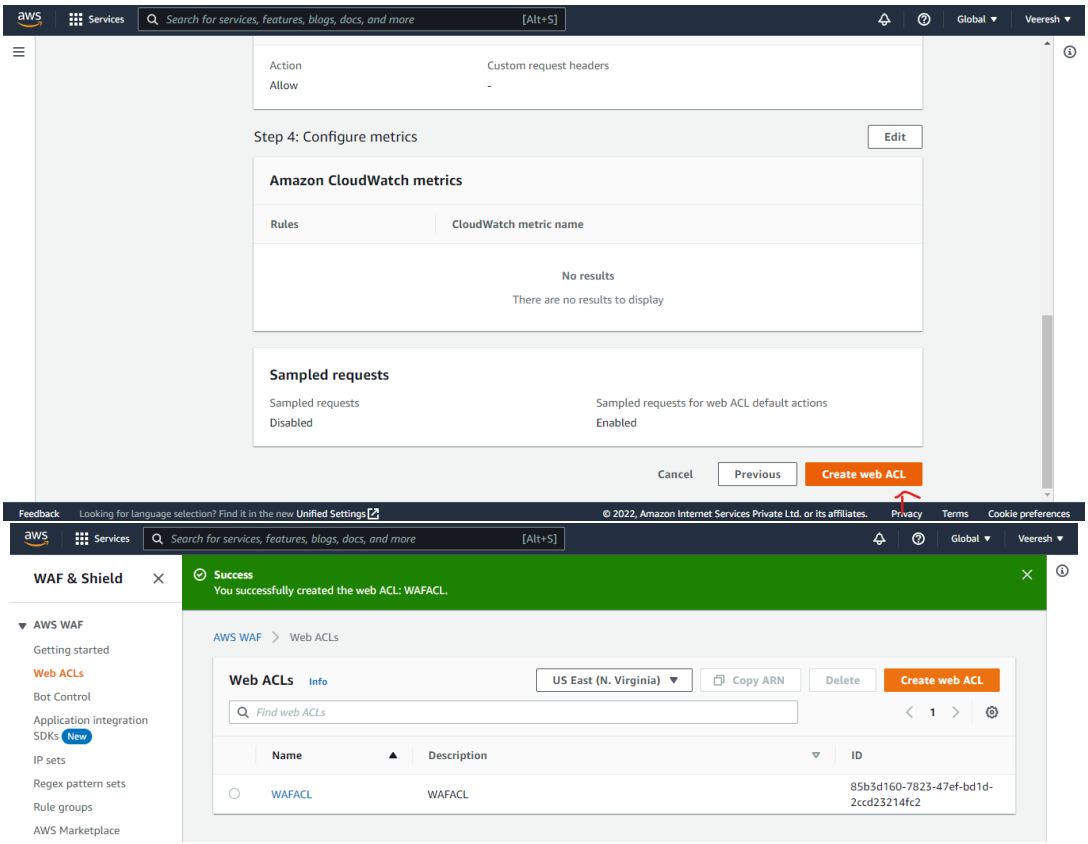
- Goto the AWS WAF dashboard, click create web ACL.
- WEB ACL details – >name - WAFACL, Region select the where the load balancer and TG are available. And make evarything default and create it.
- After creating web ACL in overview there will data available regarding hits of loadbalancer url.


aws
Services
Search for services, features, blogs, docs, and more
[Alt+S]
Global
Veeresh
WAF & Shield
AWS WAF
Getting started
Web ACLs
Bot Control
Application integration SDKs
New
IP sets
Regex pattern sets
Rule groups
AWS Marketplace
Switch to AWS WAF Classic
AWS Shield
AWS Firewall Manager
Security, Identity, and Compliance
AWS WAF
Protect your web applications from common web exploits
AWS WAF is a web application firewall service that lets you monitor web requests that are forwarded to an Amazon API Gateway API, an Amazon CloudFront distribution, or an Application Load Balancer. You can protect those resources based on conditions that you specify, such as the IP addresses that the requests originate from.
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
Pricing (US)
$5.00 per web ACL per month (prorated hourly)
$1.00 per rule per month (prorated hourly)
$0.60 per million requests processed
What's new
Feature
New AWS WAF
AWS WAF Classic
© 2022, Amazon Internet Services Private Ltd. or its affiliates.
Privacy
Terms
Cookie preferences

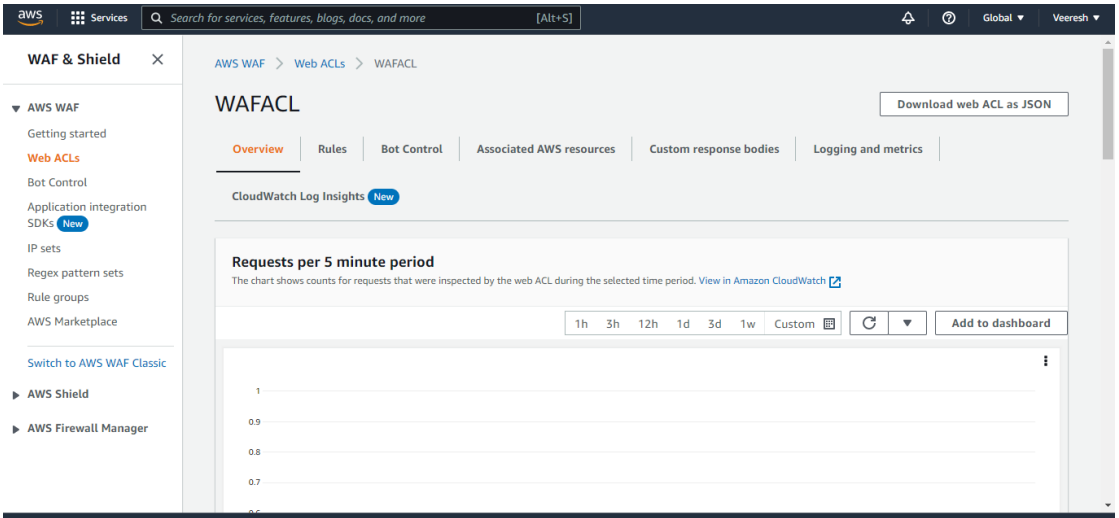

aws
Services
Search for services, features, blogs, docs, and more
[Alt+S]
Global
Veeresh
AWS WAF
Web ACLs
Create web ACL
Step 1
Describe web ACL and associate it to AWS resources
Step 2
Add rules and rule groups
Step 3
Set rule priority
Step 4
Configure metrics
Step 5
Review and create web ACL
Describe web ACL and associate it to AWS resources
Info
Web ACL details
Name
WAFACL
The name must have 1-128 characters. Valid characters: A-Z, a-z, 0-9, - (hyphen), and _ (underscore).
Description - optional
WAFACL
The description can have 1-256 characters.
CloudWatch metric name
WAFACL
The name must have 1-128 characters. Valid characters: A-Z, a-z, 0-9, - (hyphen), and _ (underscore).
Resource type
Choose the type of resource to associate with this web ACL.
CloudFront distributions
Regional resources (Application Load Balancer, API Gateway, AWS AppSync, Amazon
Feedback
Looking for language selection? Find it in the new Unified Settings
© 2022, Amazon Internet Services Private Ltd. or its affiliates.
Privacy
Terms
Cookie preferences

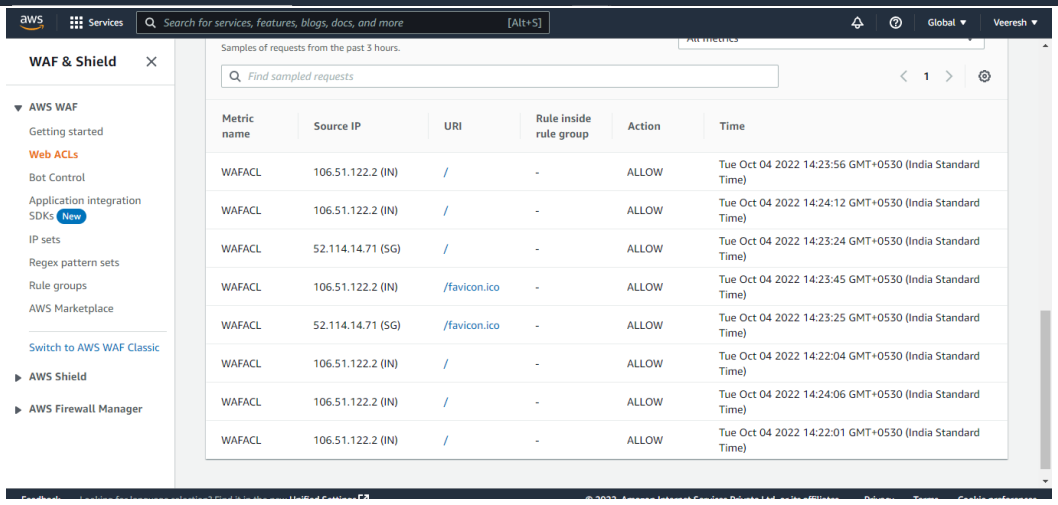

aws
Services
Search for services, features, blogs, docs, and more
[Alt+S]
Global
Veeresh
ACL
Resource type
Choose the type of resource to associate with this web ACL.
CloudFront distributions
Regional resources (Application Load Balancer, API Gateway, AWS AppSync, Amazon Cognito User Pools)
Region
Choose the AWS region to create this web ACL in.
US East (N. Virginia)
Associated AWS resources - optional
Remove
Add AWS resources
Find associated AWS resources
1
Name
Resource type
Region
No results
There are no results to display
Cancel
Next
Feedback
Looking for language selection? Find it in the new Unified Settings
© 2022, Amazon Internet Services Private Ltd. or its affiliates.
Privacy
Terms
Cookie preferences


Add AWS resources
Resource type
Select the resource type and then select the resource you want to associate with this web ACL.
Amazon API Gateway
Application Load Balancer
AWS AppSync
Amazon Cognito User Pools
Select the resources you want to associate with the web ACL.
Find AWS resources to associate
Name
WAFLB
Cancel
Add
Step 5
Review and create web ACL
CloudWatch metric name
WAFACL
The name must have 1-128 characters. Valid characters: A-Z, a-z, 0-9, - (hyphen), and _ (underscore).
Resource type
Choose the type of resource to associate with this web ACL.
CloudFront distributions
Regional resources (Application Load Balancer, API Gateway, AWS AppSync, Amazon Cognito User Pools)
Region
Choose the AWS region to create this web ACL in.
US East (N. Virginia)
Associated AWS resources - optional
Remove
Add AWS resources
Find associated AWS resources
Name
Resource type
Region
WAFLB
Application Load Balancer
US East (N. Virginia)
Cancel
Next
Step 3
Set rule priority
Step 4
Configure metrics
Step 5
Review and create web ACL
Name
Capacity
Action
No rules.
You don't have any rules added.
Web ACL rule capacity units used
The total capacity units used by the web ACL can't exceed 1500.
0/1500 WCUs
Default web ACL action for requests that don't match any rules
Default action
Allow
Block
Custom request - optional
Cancel
Previous
Next
Feedback
Looking for language selection? Find it in the new Unified Settings
© 2022, Amazon Internet Services Private Ltd. or its affiliates.
Privacy
Terms
Cookie preferences


Services
Search for services, features, blogs, docs, and more
[Alt+S]
Global
Veeresh
Action
Allow
Custom request headers
-
Step 4: Configure metrics
Edit
Amazon CloudWatch metrics
Rules
CloudWatch metric name
No results
There are no results to display
Sampled requests
Sampled requests
Disabled
Sampled requests for web ACL default actions
Enabled
Cancel
Previous
Create web ACL
Feedback
Looking for language selection? Find it in the new Unified Settings
© 2022, Amazon Internet Services Private Ltd. or its affiliates.
Privacy
Terms
Cookie preferences

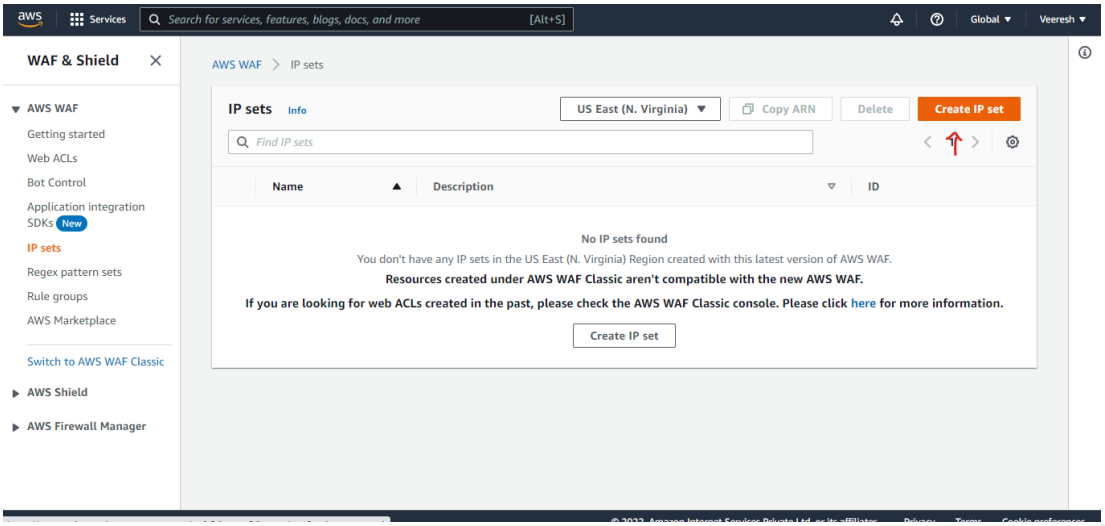
Services
Search for services, features, blogs, docs, and more
[Alt+S]
Global
Veeresh
WAF & Shield
AWS WAF
Getting started
Web ACLs
Bot Control
Application integration SDKs
New
IP sets
Regex pattern sets
Rule groups
AWS Marketplace
Success
You successfully created the web ACL: WAFACL.
AWS WAF
Web ACLs
Web ACLs
Info
US East (N. Virginia)
Copy ARN
Delete
Create web ACL
Find web ACLs
1
Name
Description
ID
WAFACL
WAFACL
85b3d160-7823-47ef-bd1d-2ccd23214fc2

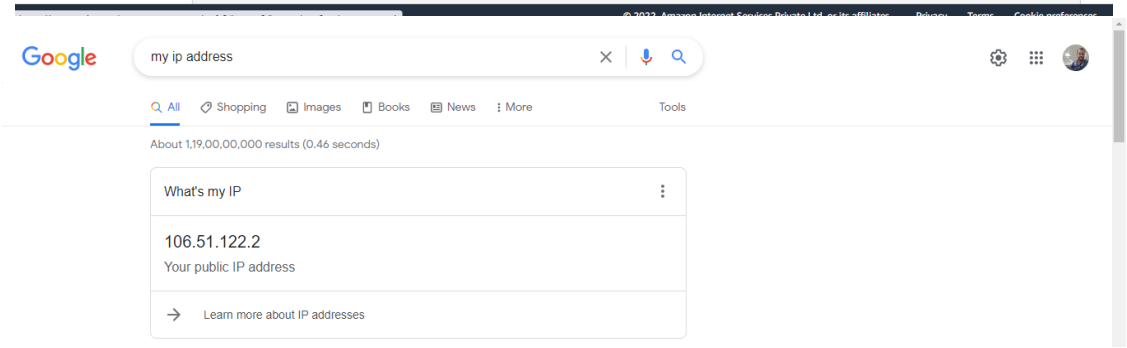


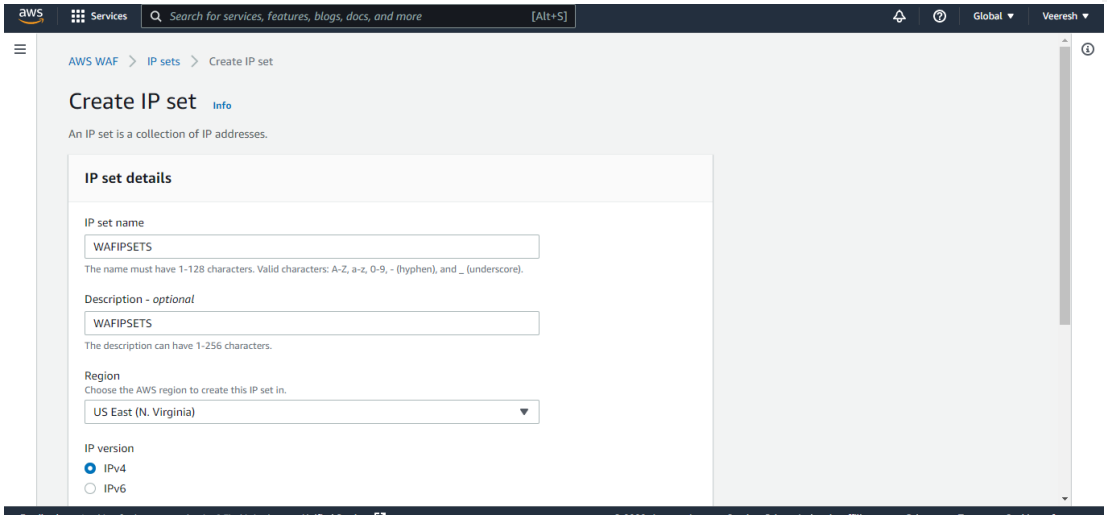


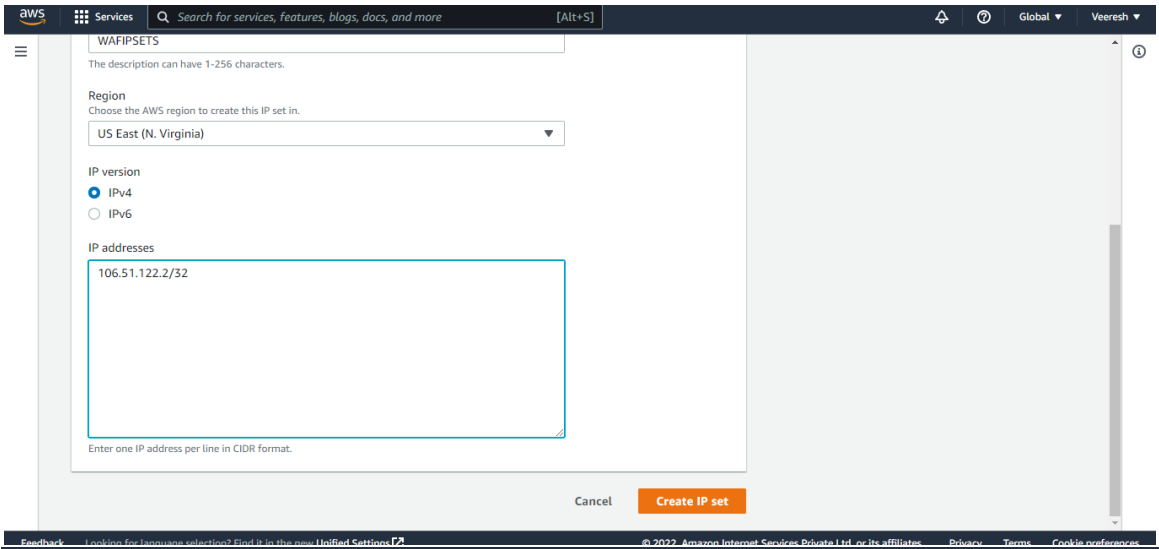
Step 3 : Amazon WAF allows you to control your content by using an IP address from where the request originates.By using the IP sets.

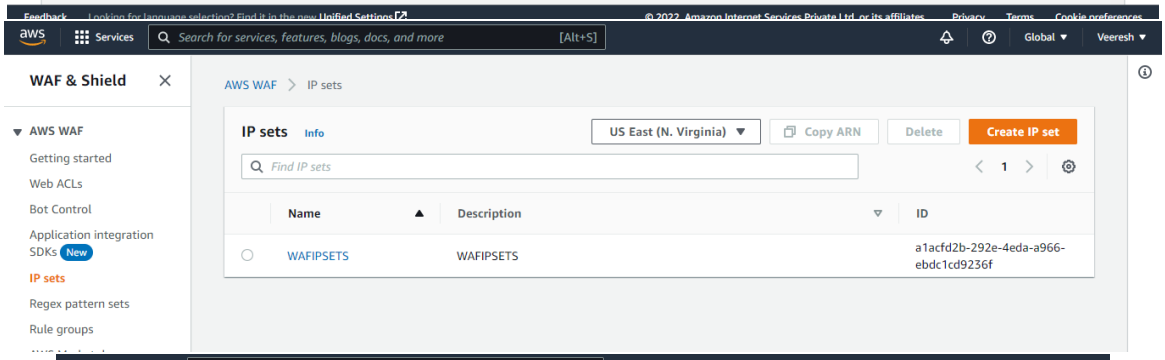
- Goto the AWS WAF dashboard click create IP set.
- IP setname and region select it , IP adress im giving my present IP adress with 32 mask bit.
- And create it.
- Now goto the web acl rules, add a rule.
- Rule type – IP sets , IP set – give the IP set which are previously created.
- In actions select Block option and add rule and save it.
- Now take the load balancers DNS name and hit it in this related IP adress then the website will not work.

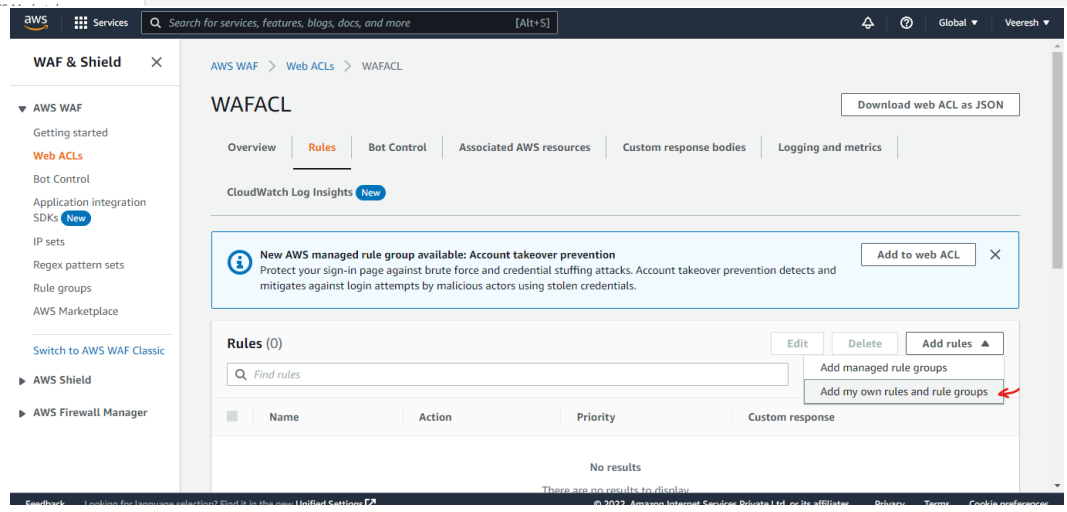

aws
Services
Search for services, features, blogs, docs, and more
[Alt+S]
Global
Veeresh
WAF & Shield
AWS WAF
Getting started
Web ACLs
Bot Control
Application integration SDKs
New
IP sets
Regex pattern sets
Rule groups
AWS Marketplace
Switch to AWS WAF Classic
AWS Shield
AWS Firewall Manager
AWS WAF > IP sets
IP sets Info
US East (N. Virginia)
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 US East (N. Virginia) Region created with this latest version of AWS WAF.
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

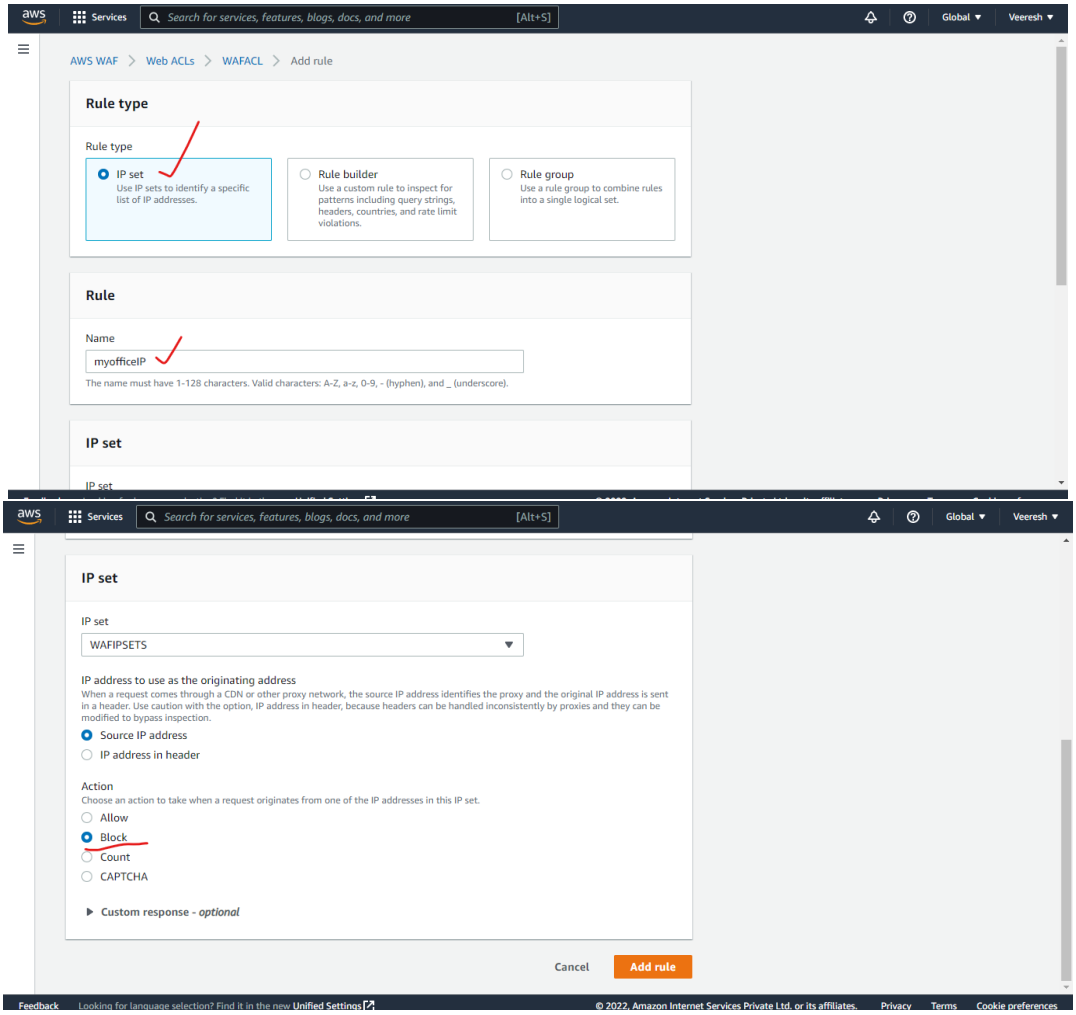

Google
my ip address
All
Shopping
Images
Books
News
More
Tools
About 1,19,00,00,000 results (0.46 seconds)
What's my IP
106.51.122.2
Your public IP address
Learn more about IP addresses


aws
Services
Search for services, features, blogs, docs, and more
[Alt+S]
Global
Veeresh
AWS WAF > IP sets > Create IP set
Create IP set Info
An IP set is a collection of IP addresses.
IP set details
IP set name
WAFIPSETS
The name must have 1-128 characters. Valid characters: A-Z, a-z, 0-9, - (hyphen), and _ (underscore).
Description - optional
WAFIPSETS
The description can have 1-256 characters.
Region
Choose the AWS region to create this IP set in.
US East (N. Virginia)
IP version
IPv4
IPv6

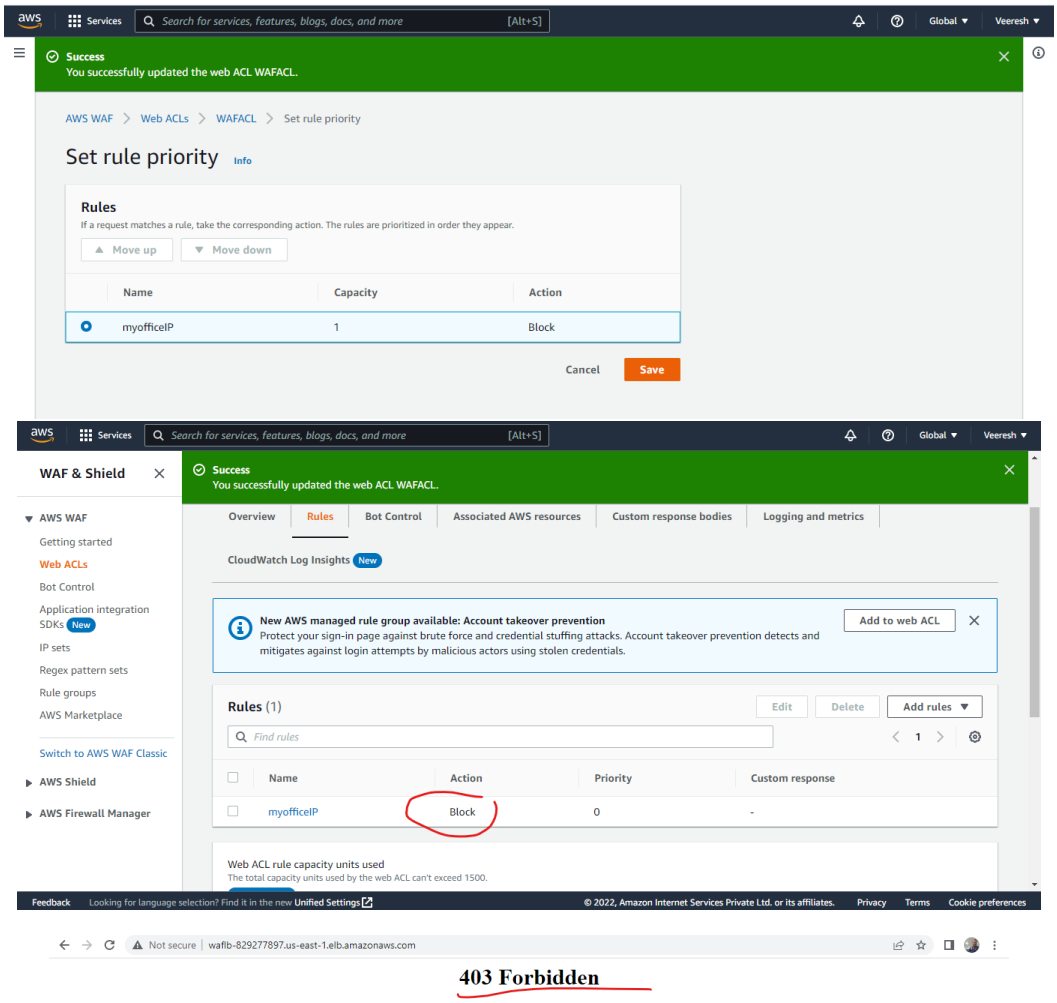

Services
Search for services, features, blogs, docs, and more
[Alt+S]
Global
Veeresh
WAFIPSETS
The description can have 1-256 characters.
Region
Choose the AWS region to create this IP set in.
US East (N. Virginia)
IP version
IPv4
IPv6
IP addresses
106.51.122.2/32
Enter one IP address per line in CIDR format.
Cancel
Create IP set


Services
Search for services, features, blogs, docs, and more
[Alt+S]
Global
Veeresh
WAF & Shield
AWS WAF
Getting started
Web ACLs
Bot Control
Application integration SDKs
New
IP sets
Regex pattern sets
Rule groups
AWS WAF > IP sets
IP sets
Info
US East (N. Virginia)
Copy ARN
Delete
Create IP set
Find IP sets
1
Name
Description
ID
WAFIPSETS
WAFIPSETS
a1acfd2b-292e-4eda-a966-ebdc1cd9236f

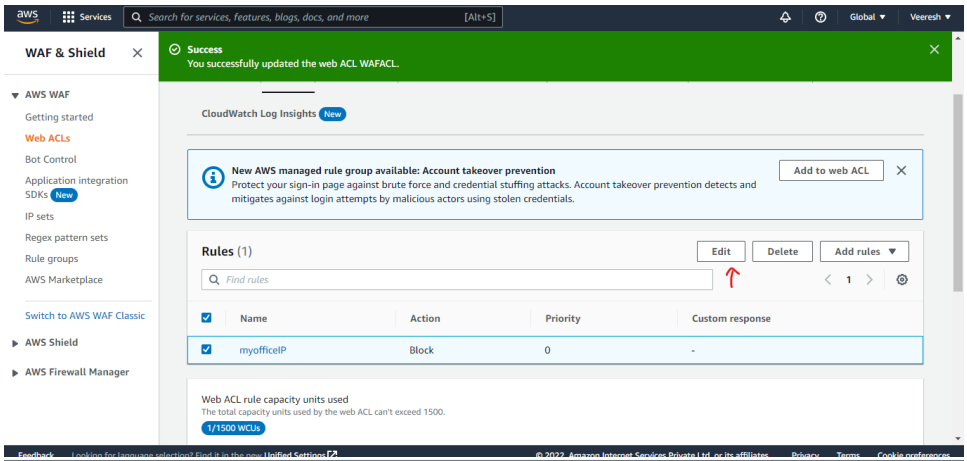

Services
Search for services, features, blogs, docs, and more
[Alt+S]
Global
Veeresh
WAF & Shield
AWS WAF
Getting started
Web ACLs
Bot Control
Application integration SDKs
New
IP sets
Regex pattern sets
Rule groups
AWS Marketplace
Switch to AWS WAF Classic
AWS Shield
AWS Firewall Manager
AWS WAF > Web ACLs > WAFACL
WAFACL
Download web ACL as JSON
Overview
Rules
Bot Control
Associated AWS resources
Custom response bodies
Logging and metrics
CloudWatch Log Insights
New
New AWS managed rule group available: Account takeover prevention
Protect your sign-in page against brute force and credential stuffing attacks. Account takeover prevention detects and mitigates against login attempts by malicious actors using stolen credentials.
Add to web ACL
Rules (0)
Edit
Delete
Add rules
Find rules
Add managed rule groups
Add my own rules and rule groups
Name
Action
Priority
Custom response
No results

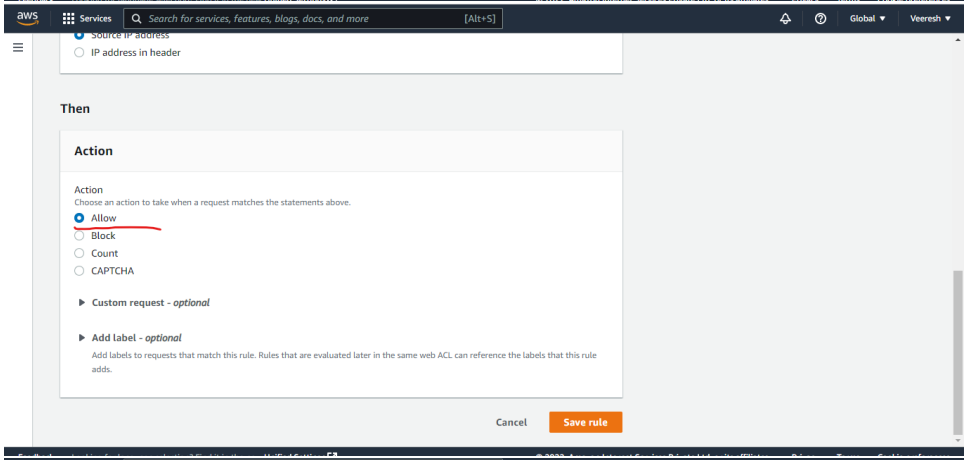

aws
Services
Search for services, features, blogs, docs, and more
[Alt+S]
Global
Veeresh
AWS WAF > Web ACLs > WAFACL > Add rule
Rule type
Rule type
IP set
Use IP sets to identify a specific list of IP addresses.
Rule builder
Use a custom rule to inspect for patterns including query strings, headers, countries, and rate limit violations.
Rule group
Use a rule group to combine rules into a single logical set.
Rule
Name
myofficeIP
The name must have 1-128 characters. Valid characters: A-Z, a-z, 0-9, - (hyphen), and _ (underscore).
IP set
IP set

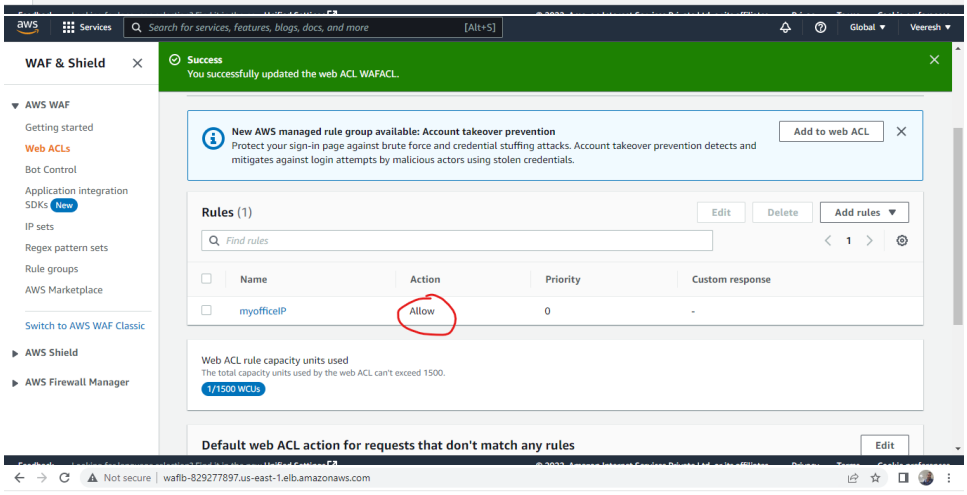
aws
Services
Search for services, features, blogs, docs, and more
[Alt+S]
Global
Veeresh
IP set
IP set
WAFIPSETS
IP address to use as the originating address
When a request comes through a CDN or other proxy network, the source IP address identifies the proxy and the original IP address is sent in a 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
Custom response - optional
Cancel
Add rule
Feedback
Looking for language selection? Find it in the new Unified Settings
© 2022, Amazon Internet Services Private Ltd. or its affiliates.
Privacy
Terms
Cookie preferences



Step 4 : Again allow and check the rule of web acl is it working or not.







welcome to waf server1 ip-172-31-24-213.ec2.internal