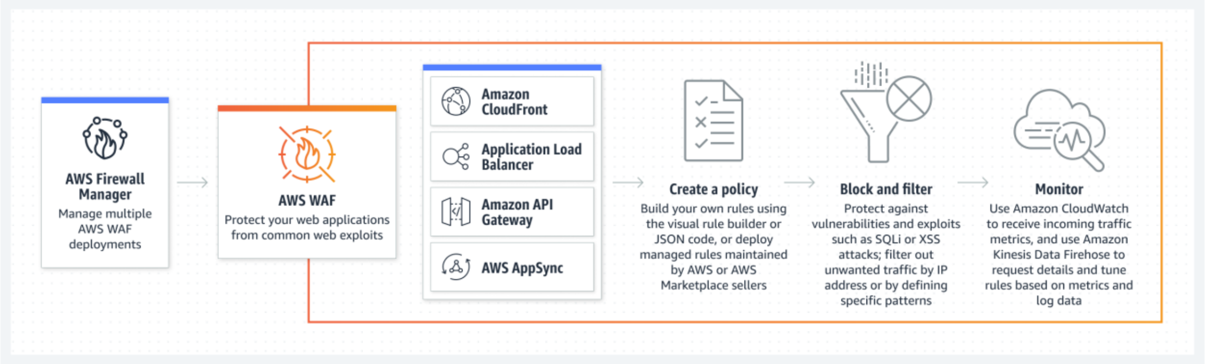
AWS Web Application Firewall (WAF)



AWS Firewall Manager: Manage multiple AWS WAF deployments

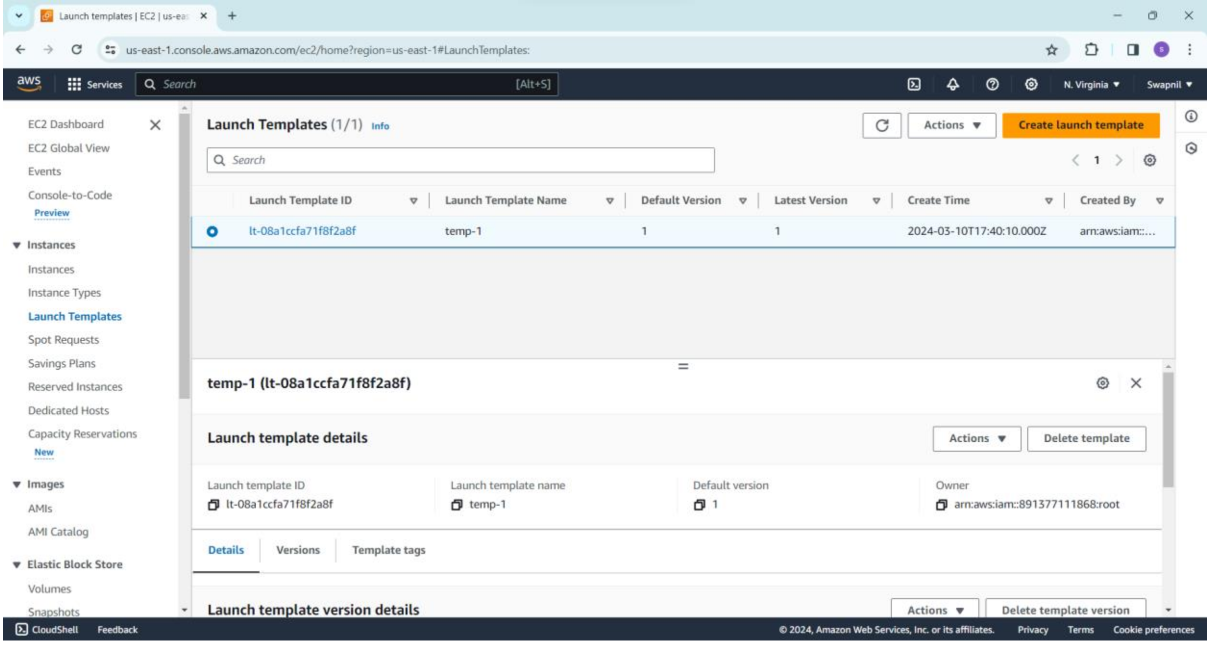
AWS WAF: Protect your web applications from common web exploits

Create a policy: Build your own rules using the visual rule builder or JSON code, or deploy managed rules maintained by AWS or AWS Marketplace sellers

Block and filter: Protect against vulnerabilities and exploits such as SQLi or XSS attacks; filter out unwanted traffic by IP address or by defining specific patterns

Monitor: Use Amazon CloudWatch to receive incoming traffic metrics, and use Amazon Kinesis Data Firehose to request details and tune rules based on metrics and log data

Step 1: Create launch template.



Launch Templates (1/1) Info

	Launch Template ID	Launch Template Name	Default Version	Latest Version	Create Time	Created By
●	lt-08a1ccfa71f8f2a8f	temp-1	1	1	2024-03-10T17:40:10.000Z	arn:aws:iam::...

temp-1 (lt-08a1ccfa71f8f2a8f)

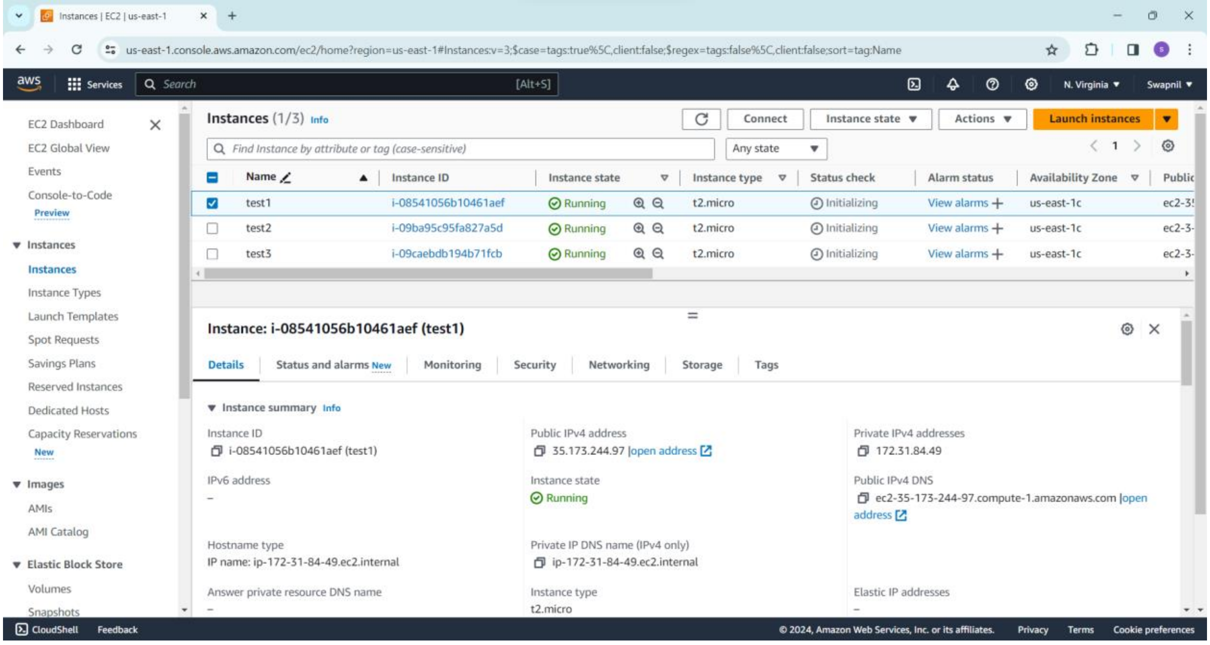
Launch template details — Actions ▾ | Delete template

Launch template ID	Launch template name	Default version	Owner
lt-08a1ccfa71f8f2a8f	temp-1	1	arn:aws:iam::891377111868:root

Details | Versions | Template tags

Launch template version details — Actions ▾ | Delete template version

Step 2: Launch an instance from launch template.



Instances (1/3) Info

	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public
☑	test1	i-08541056b10461aef	Running	t2.micro	Initializing	View alarms +	us-east-1c	ec2-35
□	test2	i-09ba95c95fa827a5d	Running	t2.micro	Initializing	View alarms +	us-east-1c	ec2-3-
□	test3	i-09caebdb194b71fcb	Running	t2.micro	Initializing	View alarms +	us-east-1c	ec2-3-

Instance: i-08541056b10461aef (test1)

Details | Status and alarms New | Monitoring | Security | Networking | Storage | Tags

Instance summary Info

Instance ID: i-08541056b10461aef (test1)

Public IPv4 address: 35.173.244.97 |open address

Private IPv4 addresses: 172.31.84.49

IPv6 address: –

Instance state: Running

Public IPv4 DNS: ec2-35-173-244-97.compute-1.amazonaws.com |open address

Hostname type: IP name: ip-172-31-84-49.ec2.internal

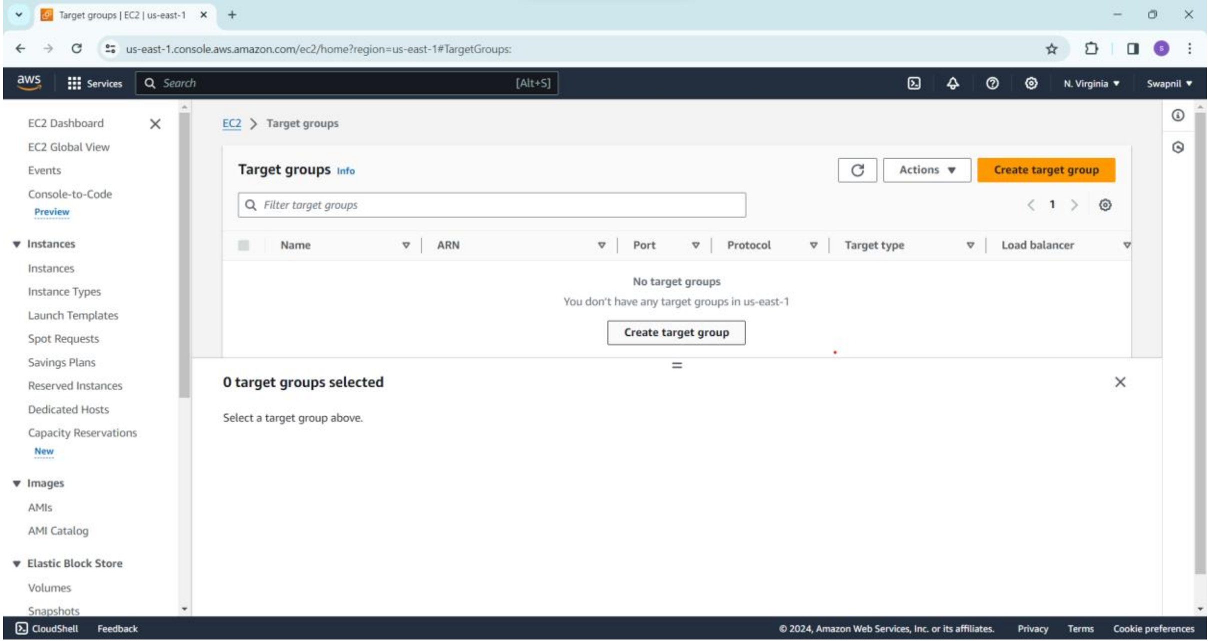
Private IP DNS name (IPv4 only): ip-172-31-84-49.ec2.internal

Answer private resource DNS name: –

Instance type: t2.micro

Elastic IP addresses: –

Step 3: Create a target group



Target groups Info

	Name	ARN	Port	Protocol	Target type	Load balancer

No target groups

You don't have any target groups in us-east-1

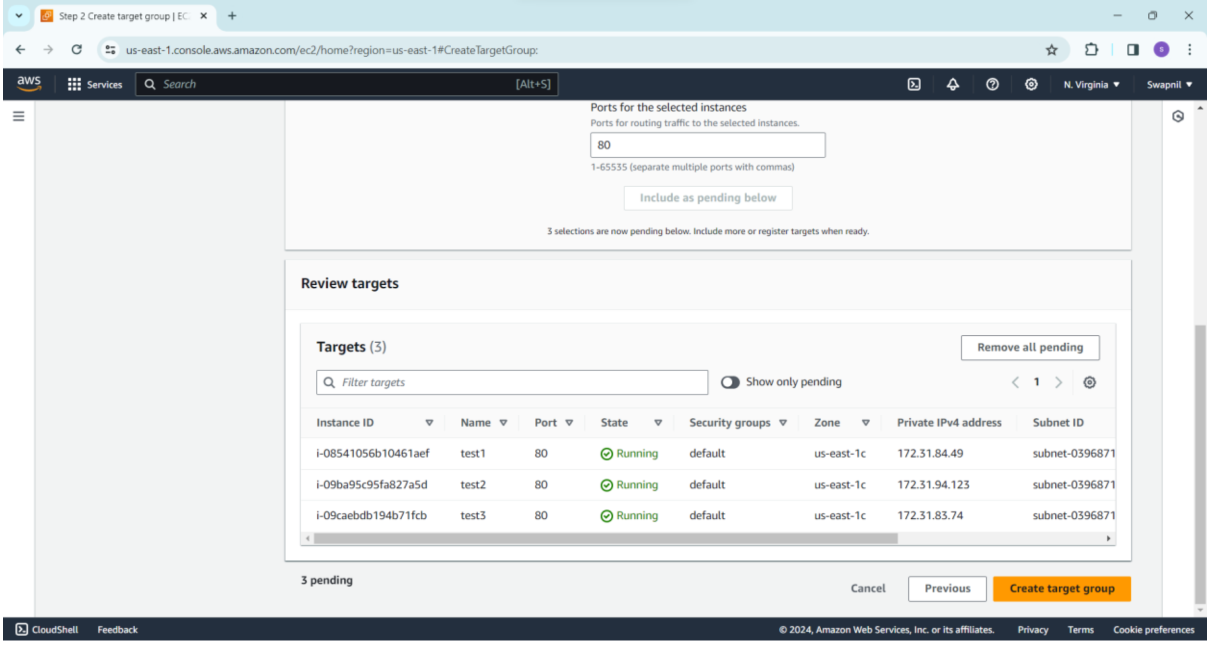
Create target group

0 target groups selected

Select a target group above.

Step 4: Enter the target group detail.

- ➢ Click on create target group.



us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#CreateTargetGroup:

Ports for the selected instances

Ports for routing traffic to the selected instances.

80

1-65535 (separate multiple ports with commas)

3 selections are now pending below. Include more or register targets when ready.

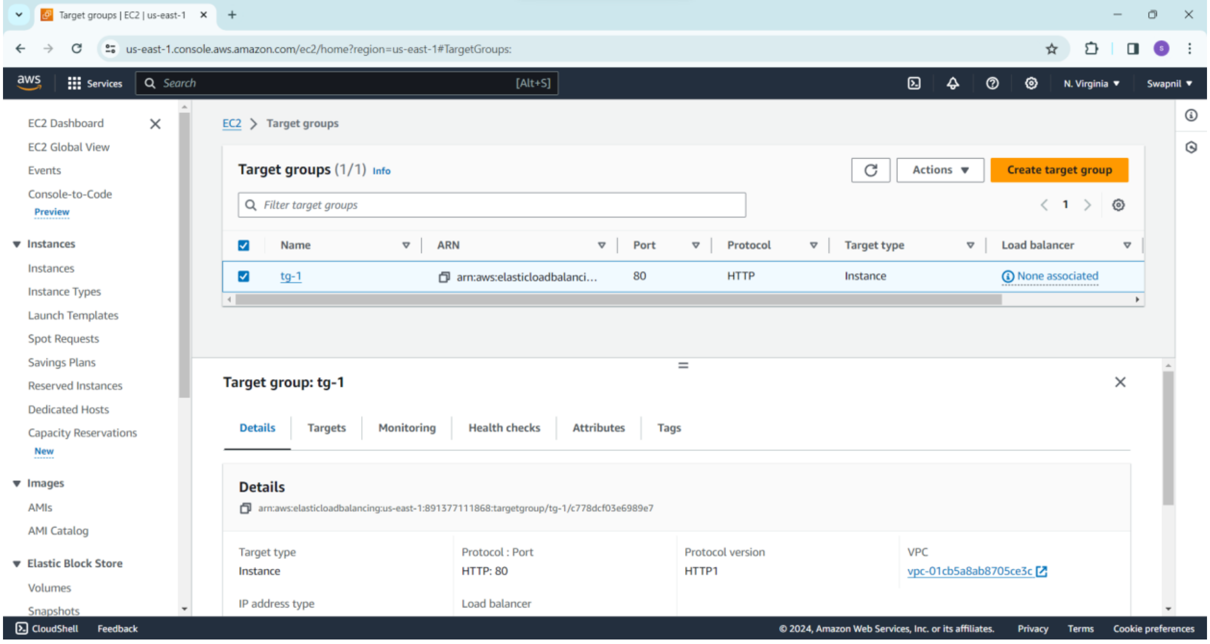
Review targets

Targets (3)

Instance ID	Name	Port	State	Security groups	Zone	Private IPv4 address	Subnet ID
i-08541056b10461aef	test1	80	Running	default	us-east-1c	172.31.84.49	subnet-0396871
i-09ba95c95fa827a5d	test2	80	Running	default	us-east-1c	172.31.94.123	subnet-0396871
i-09caebdb194b71fcb	test3	80	Running	default	us-east-1c	172.31.83.74	subnet-0396871

3 pending

Step 5: Target group is created.



us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#TargetGroups:

EC2 > Target groups

Target groups (1/1)

☑	Name	ARN	Port	Protocol	Target type	Load balancer
☑	tg-1	arn:aws:elasticloadbalanci...	80	HTTP	Instance	None associated

Target group: tg-1

Details

arn:aws:elasticloadbalancing:us-east-1:891377111868:targetgroup/tg-1/c778dcf03e6989e7

Target type: Instance

Protocol : Port: HTTP: 80

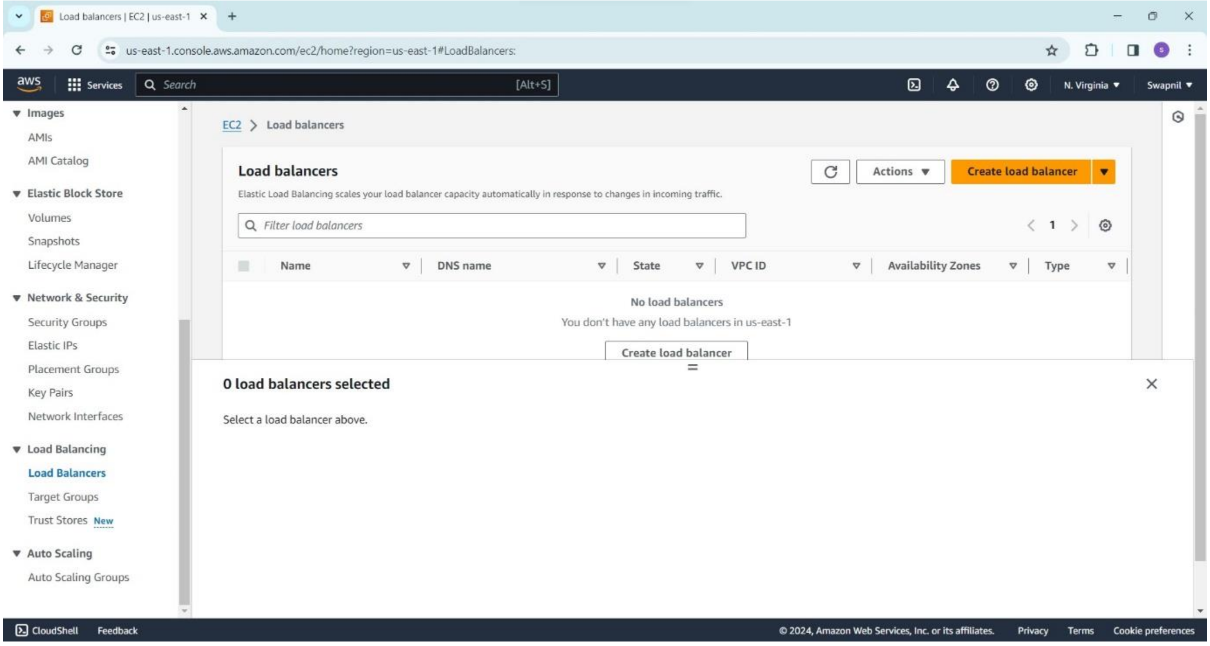
Protocol version: HTTP1

VPC: vpc-01cb5a8ab8705ce3c

IP address type

Load balancer

Step 6: Associated application load balancer to target group



Load balancers | EC2 | us-east-1

us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#LoadBalancers:

Load balancers

Elastic Load Balancing scales your load balancer capacity automatically in response to changes in incoming traffic.

Filter load balancers

Name	DNS name	State	VPC ID	Availability Zones	Type

No load balancers

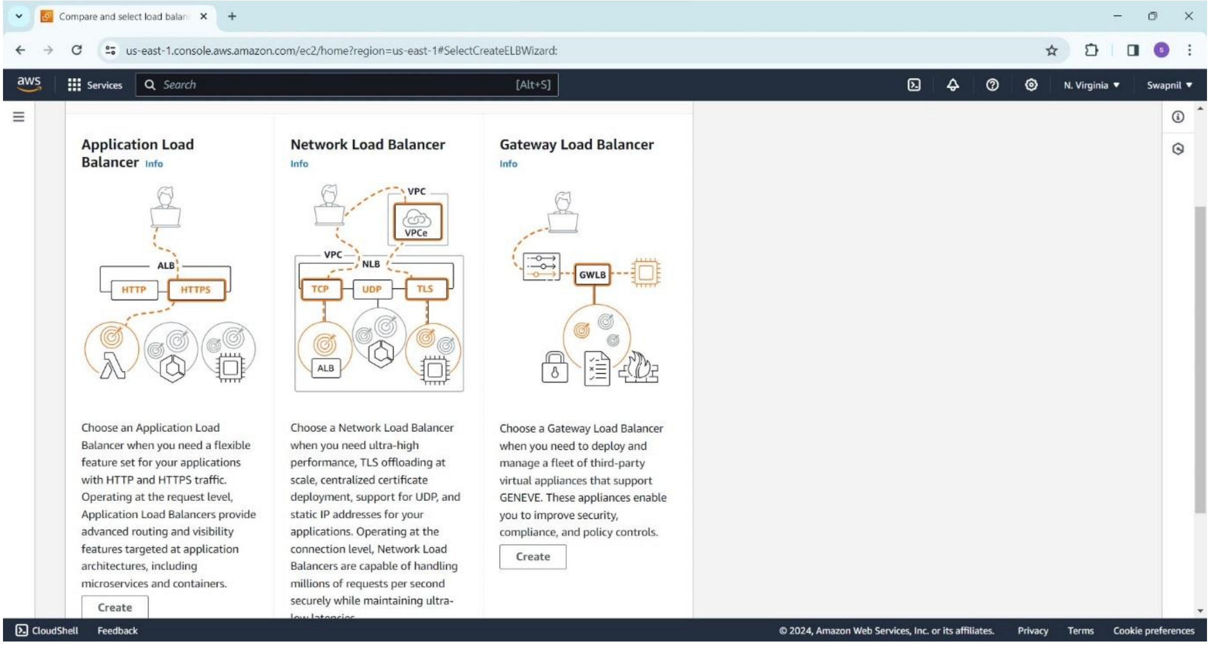
You don't have any load balancers in us-east-1

Create load balancer

0 load balancers selected

Select a load balancer above.

Step 7: Create application load balancer.



Compare and select load balan

us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#SelectCreateELBWizard:

Application Load Balancer Info

Choose an Application Load Balancer when you need a flexible feature set for your applications with HTTP and HTTPS traffic. Operating at the request level, Application Load Balancers provide advanced routing and visibility features targeted at application architectures, including microservices and containers.

Create

Network Load Balancer Info

Choose a Network Load Balancer when you need ultra-high performance, TLS offloading at scale, centralized certificate deployment, support for UDP, and static IP addresses for your applications. Operating at the connection level, Network Load Balancers are capable of handling millions of requests per second securely while maintaining ultra-low latencies.

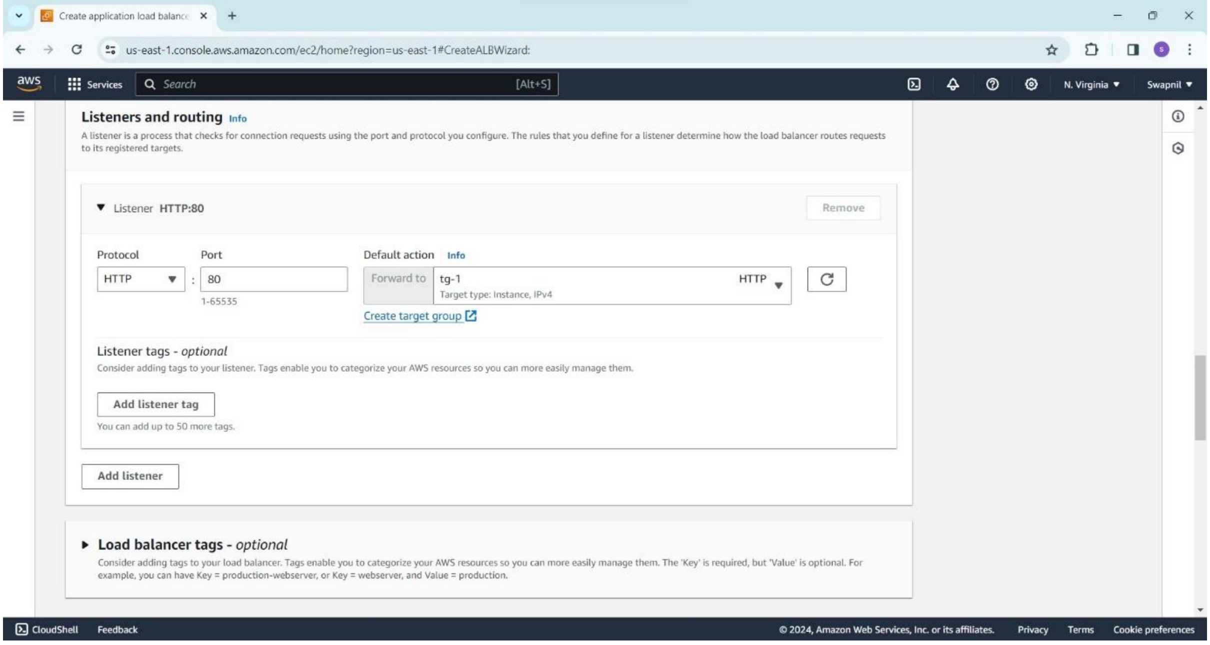
Gateway Load Balancer Info

Choose a Gateway Load Balancer when you need to deploy and manage a fleet of third-party virtual appliances that support GENEVE. These appliances enable you to improve security, compliance, and policy controls.

Create

Step 8: Create load balancer

- ➢ Ente basic detail
- ➢ Add target group
- ➢ Click on create load balancer



Listeners and routing Info

A listener is a process that checks for connection requests using the port and protocol you configure. The rules that you define for a listener determine how the load balancer routes requests to its registered targets.

▼ Listener HTTP:80 — Remove

Protocol: HTTP

Port: 80 (1-65535)

Default action Info: Forward to tg-1 — Target type: Instance, IPv4 — HTTP

Create target group

Listener tags - *optional*

Consider adding tags to your listener. Tags enable you to categorize your AWS resources so you can more easily manage them.

Add listener tag

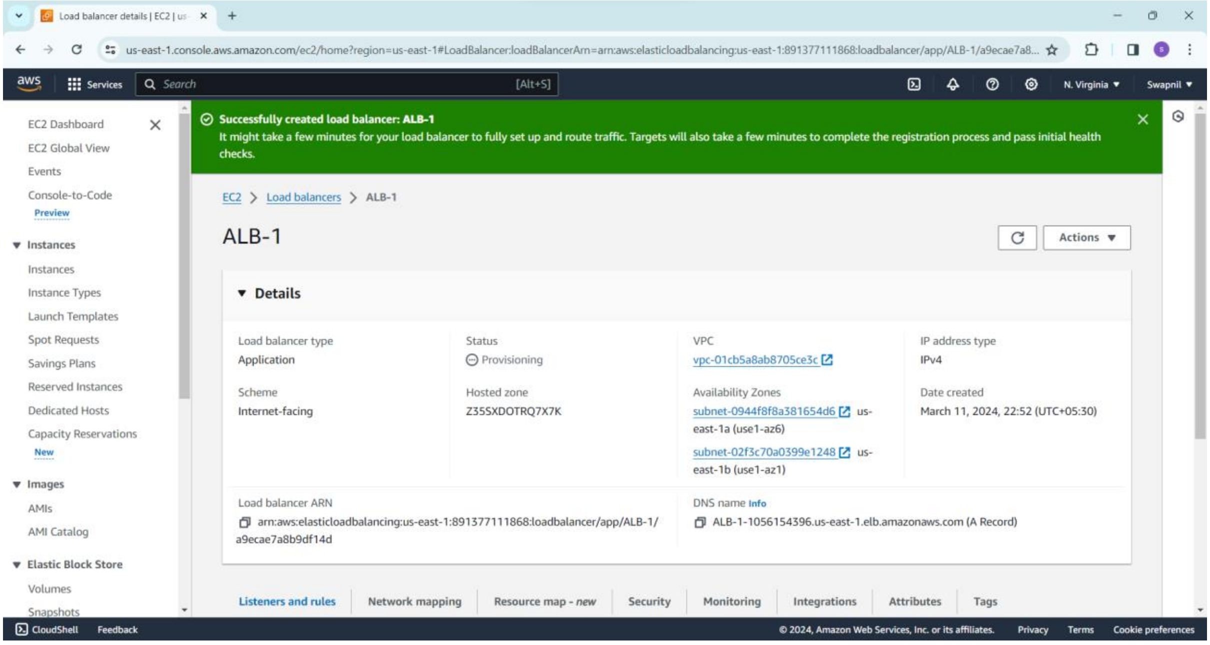
You can add up to 50 more tags.

Add listener

▶ Load balancer tags - *optional*

Consider adding tags to your load balancer. Tags enable you to categorize your AWS resources so you can more easily manage them. The 'Key' is required, but 'Value' is optional. For example, you can have Key = production-webserver, or Key = webserver, and Value = production.

Step 9: Check application load balancer is created.



Successfully created load balancer: ALB-1

It might take a few minutes for your load balancer to fully set up and route traffic. Targets will also take a few minutes to complete the registration process and pass initial health checks.

EC2 > Load balancers > ALB-1

ALB-1

▼ Details

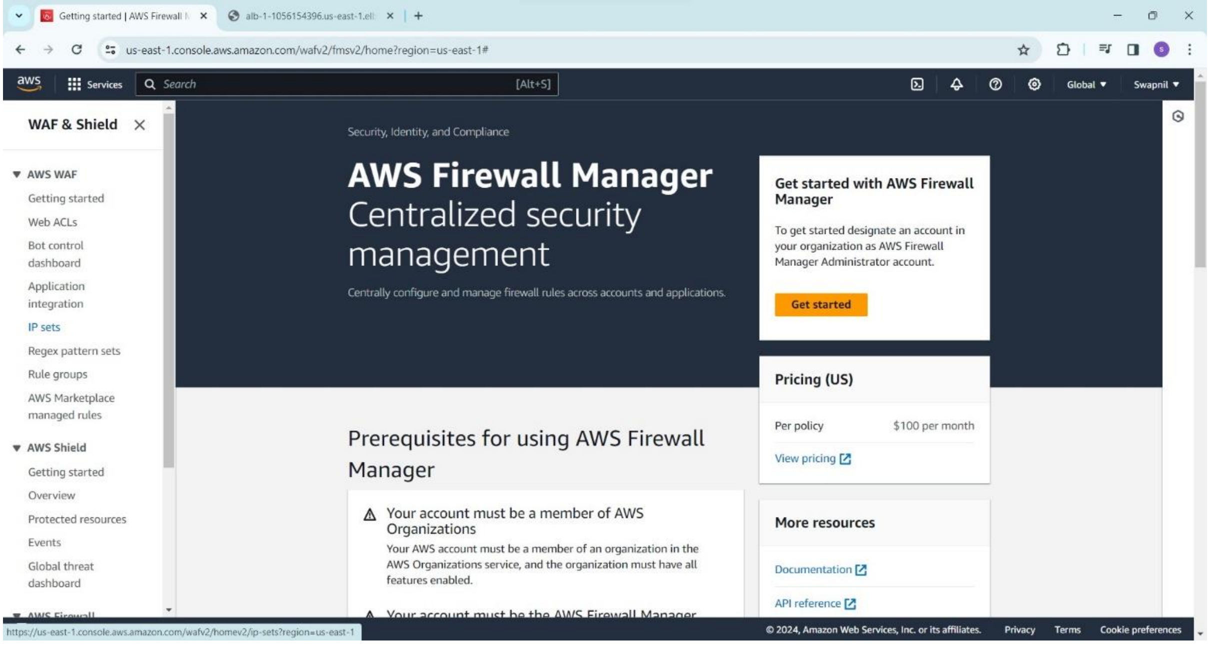
Load balancer type	Status	VPC	IP address type
Application	Provisioning	vpc-01cb5a8ab8705ce3c	IPv4

Scheme	Hosted zone	Availability Zones	Date created
Internet-facing	Z35SXDOTRQ7X7K	subnet-0944f8f8a381654d6 us-east-1a (use1-az6) subnet-02f3c70a0399e1248 us-east-1b (use1-az1)	March 11, 2024, 22:52 (UTC+05:30)

Load balancer ARN: arn:aws:elasticloadbalancing:us-east-1:891377111868:loadbalancer/app/ALB-1/a9ecae7a8b9df14d

DNS name Info: ALB-1-1056154396.us-east-1.elb.amazonaws.com (A Record)

Step 10: Go to the navigation panel and select WAF.



Security, Identity, and Compliance

AWS Firewall Manager
Centralized security management

Centrally configure and manage firewall rules across accounts and applications.

Get started with AWS Firewall Manager

To get started designate an account in your organization as AWS Firewall Manager Administrator account.

Pricing (US)

Per policy	$100 per month

Prerequisites for using AWS Firewall Manager

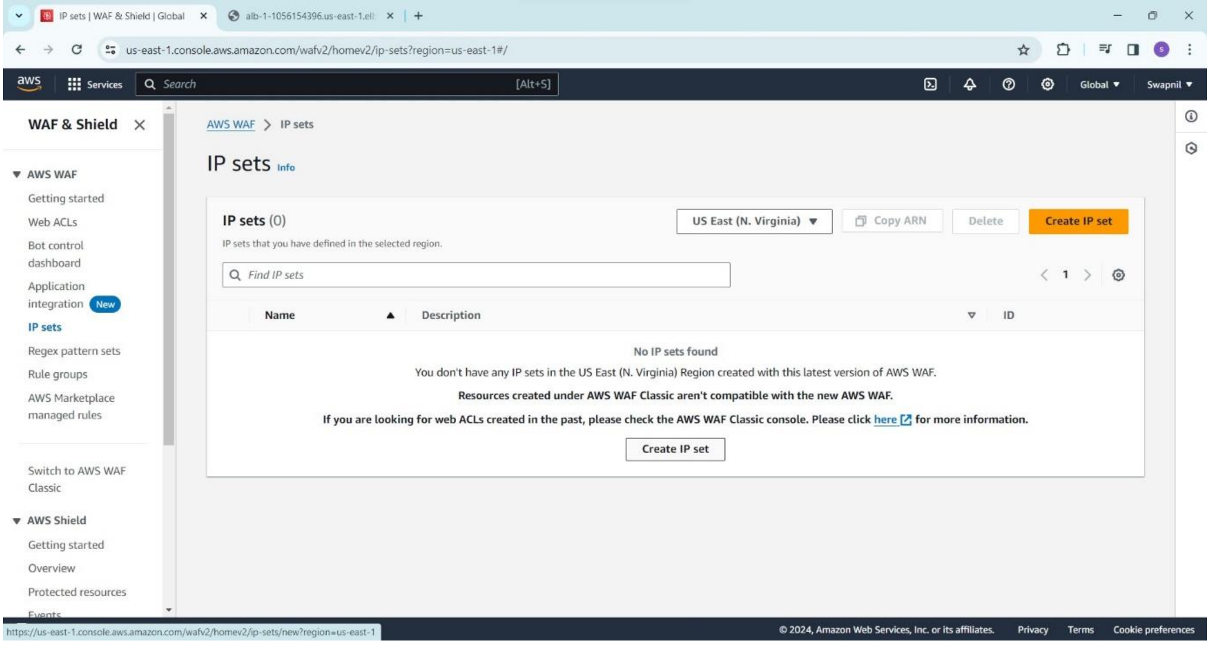
Your account must be a member of AWS Organizations

Your AWS account must be a member of an organization in the AWS Organizations service, and the organization must have all features enabled.

Your account must be the AWS Firewall Manager

More resources

Step 11: Crate IP sets.


IP sets | WAF & Shield | Global
alb-1-1056154396.us-east-1.el
us-east-1.console.aws.amazon.com/wafv2/homev2/ip-sets?region=us-east-1#/
aws
Services
Search
[Alt+S]
Global
Swapnil
WAF & Shield
AWS WAF
Getting started
Web ACLs
Bot control dashboard
Application integration New
IP sets
Regex pattern sets
Rule groups
AWS Marketplace managed rules
Switch to AWS WAF Classic
AWS Shield
Getting started
Overview
Protected resources
Events
AWS WAF > IP sets
Info
US East (N. Virginia)
Copy ARN
Delete
Create IP set
Find IP sets
1
Create IP set
https://us-east-1.console.aws.amazon.com/wafv2/homev2/ip-sets/new?region=us-east-1
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

IP sets

IP sets (0)

IP sets that you have defined in the selected region.

Name	Description	ID

No IP sets found

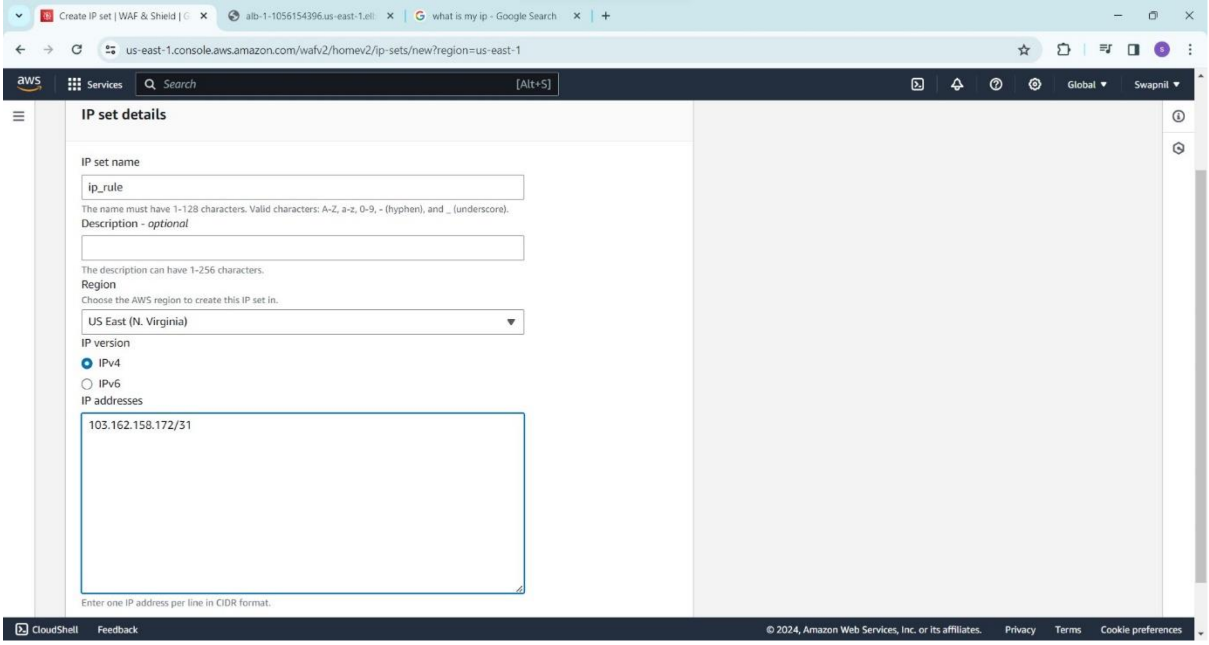
You don't have any IP sets in the US East (N. Virginia) Region created with this latest version of AWS WAF.

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.

Step 12: IP set details.

- ➢ Enter IP set rule name
- ➢ Choose region and IP version
- ➢ Add the IP address list



us-east-1.console.aws.amazon.com/wafv2/homev2/ip-sets/new?region=us-east-1

IP set details

IP set name

ip_rule

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.

Region

Choose the AWS region to create this IP set in.

US East (N. Virginia)

IP version

● IPv4

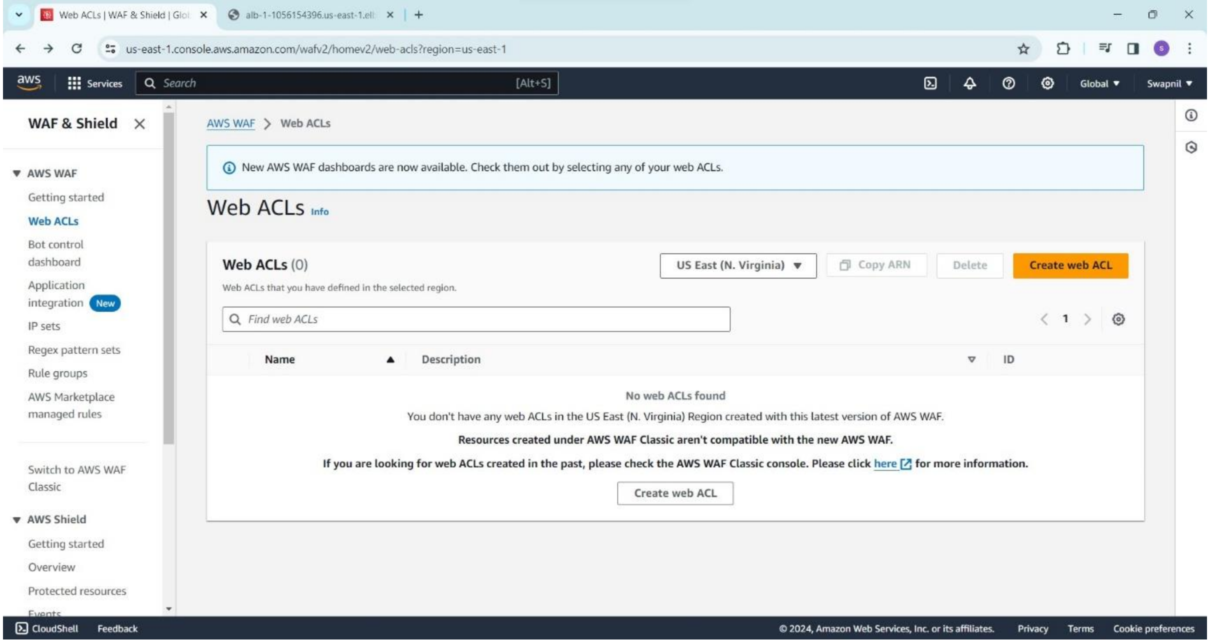
○ IPv6

IP addresses

103.162.158.172/31

Enter one IP address per line in CIDR format.

Step 13: Create web ACL (access control list)



us-east-1.console.aws.amazon.com/wafv2/homev2/web-acls?region=us-east-1

AWS WAF > Web ACLs

New AWS WAF dashboards are now available. Check them out by selecting any of your web ACLs.

Web ACLs Info

Web ACLs (0)

Web ACLs that you have defined in the selected region.

US East (N. Virginia)

Name	Description	ID

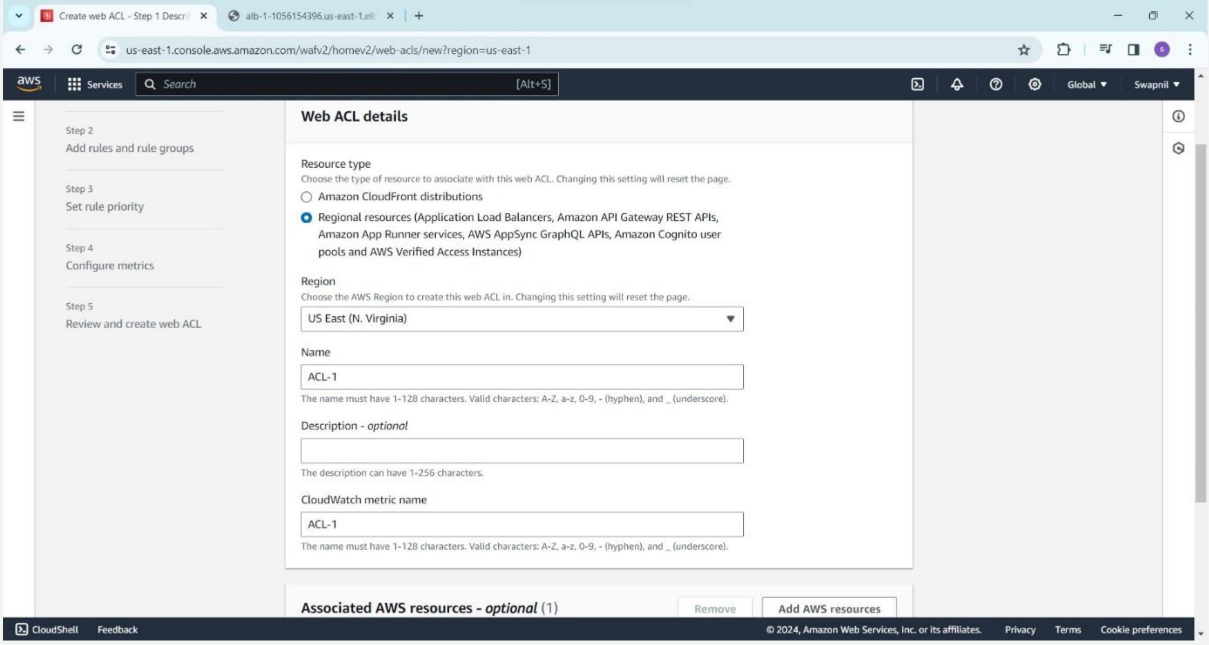
No web ACLs found

You don't have any web ACLs 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.

Step 14: Describe web ACL and associate it to AWS resources



Create web ACL - Step 1 Descri
alb-1-1056154396.us-east-1.ell
us-east-1.console.aws.amazon.com/wafv2/homev2/web-acls/new?region=us-east-1
Services
Search
[Alt+S]
Global
Swapnil
Step 2
Add rules and rule groups
Step 3
Set rule priority
Step 4
Configure metrics
Step 5
Review and create web ACL
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

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, 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.
US East (N. Virginia)

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

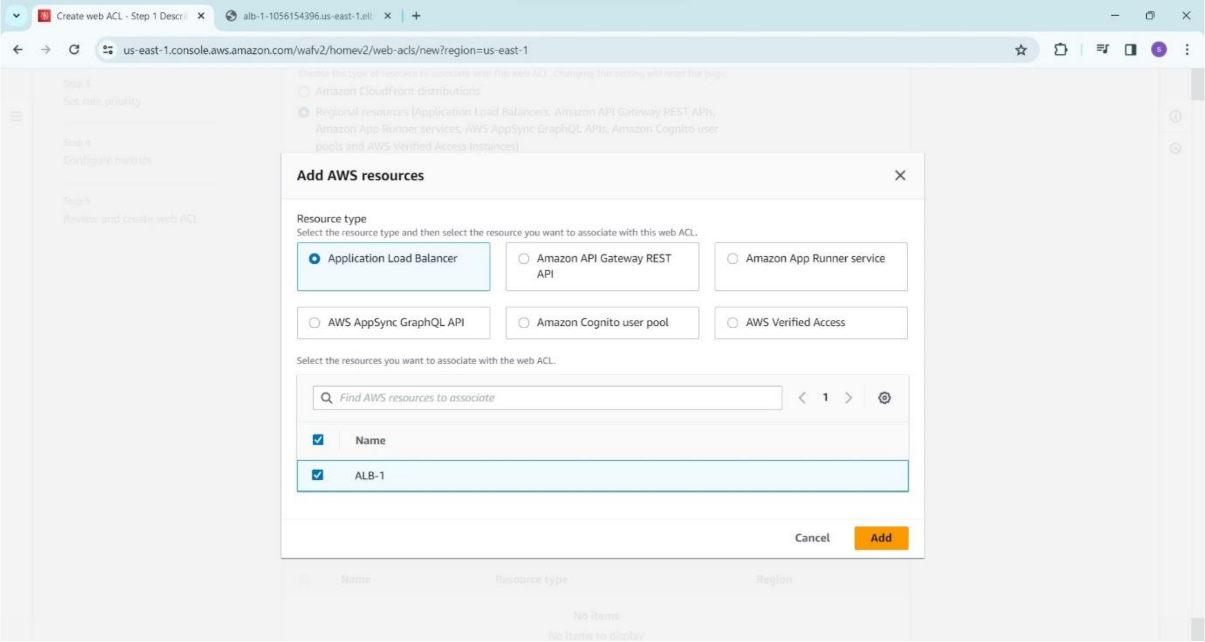
Description - *optional*

The description can have 1-256 characters.

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

Associated AWS resources - *optional* (1)

- Add AWS resources



Create web ACL - Step 1 Descri
alb-1-1056154396.us-east-1.ell
us-east-1.console.aws.amazon.com/wafv2/homev2/web-acls/new?region=us-east-1

Add AWS resources

Resource type
Select the resource type and then select the resource you want to associate with this web ACL.

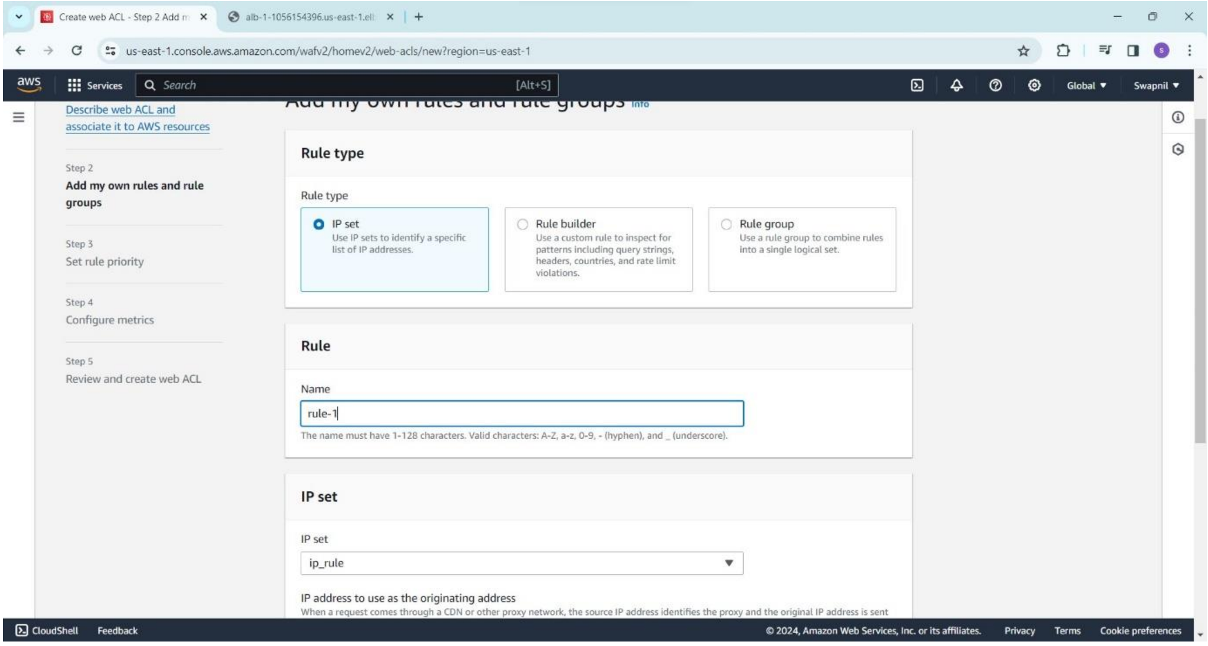
● Application Load Balancer
○ Amazon API Gateway REST API
○ Amazon App Runner service
○ AWS AppSync GraphQL API
○ Amazon Cognito user pool
○ AWS Verified Access

Select the resources you want to associate with the web ACL.

Find AWS resources to associate
1

☑	Name
☑	ALB-1

Step 15: Add rule and rule groups



Create web ACL - Step 2 Add m | alb-1-1056154396.us-east-1.ell

us-east-1.console.aws.amazon.com/wafv2/homev2/web-acls/new?region=us-east-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

Name: rule-1

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

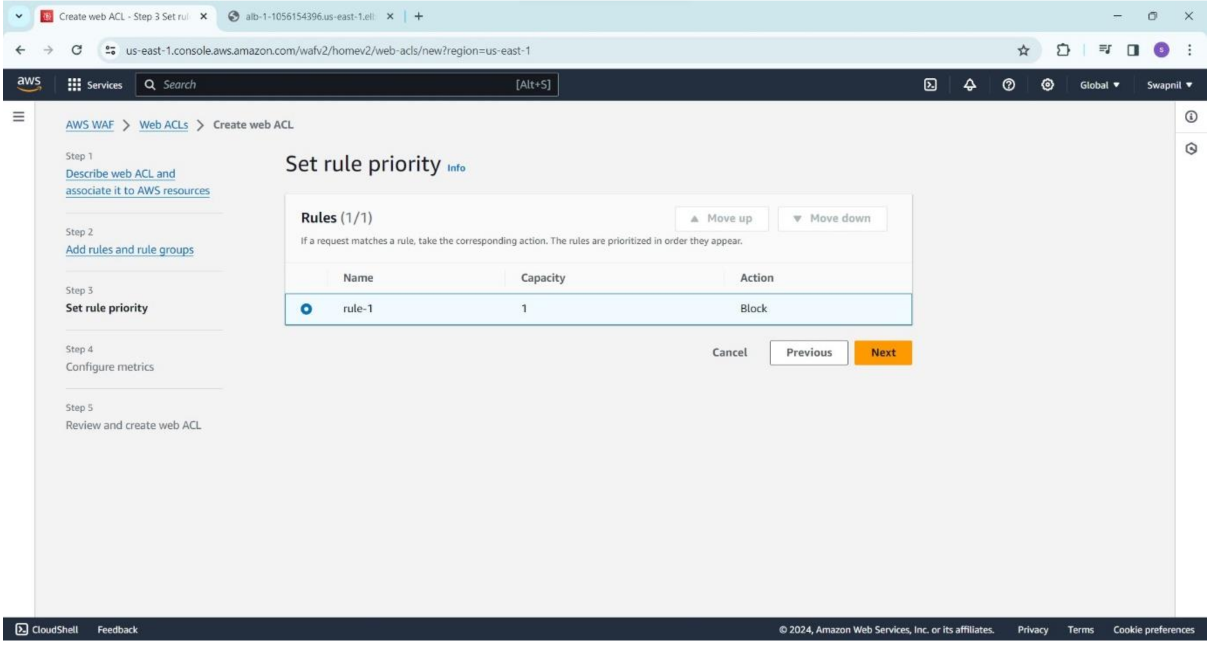
IP set

IP set: ip_rule

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

© 2024, Amazon Web Services, Inc. or its affiliates.

Step 16: Set rule priority.



Create web ACL - Step 3 Set rul | alb-1-1056154396.us-east-1.ell

us-east-1.console.aws.amazon.com/wafv2/homev2/web-acls/new?region=us-east-1

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

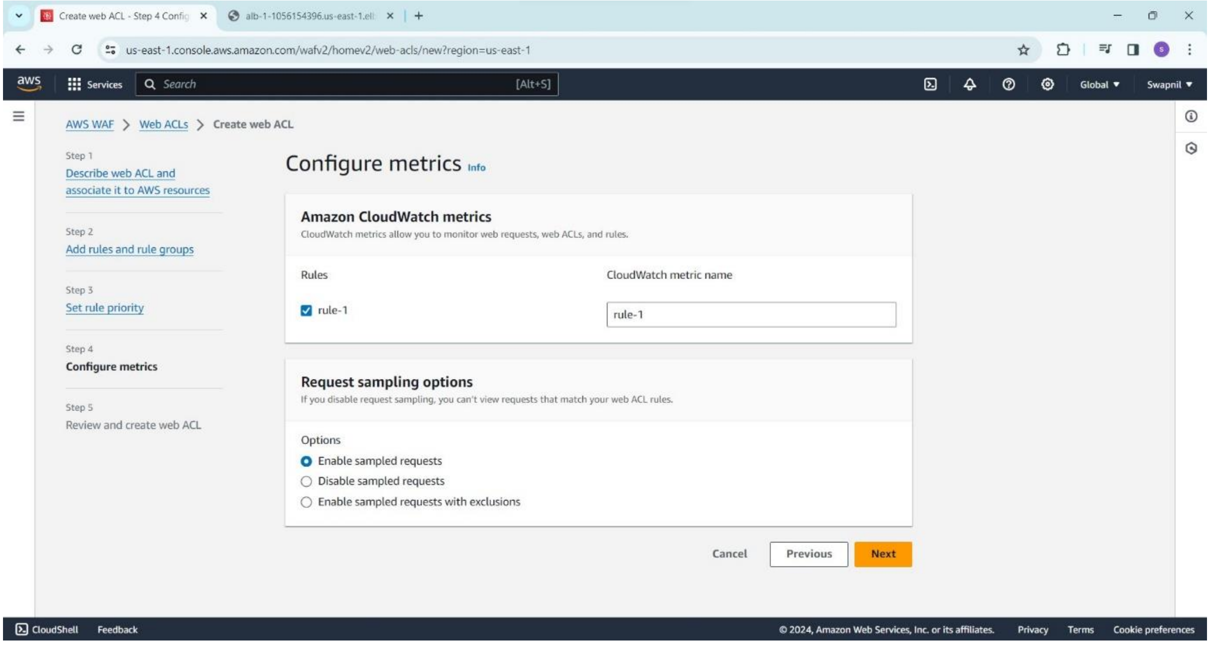
Rules (1/1)

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

	Name	Capacity	Action
●	rule-1	1	Block

© 2024, Amazon Web Services, Inc. or its affiliates.

Step 17: Configure metrics


Create web ACL - Step 4 Config
alb-1-1056154396.us-east-1.elb
us-east-1.console.aws.amazon.com/wafv2/homev2/web-acls/new?region=us-east-1
aws
Services
Search
[Alt+S]
Global
Swapnil
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
Cancel
Previous
Next
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Configure metrics Info

Amazon CloudWatch metrics

CloudWatch metrics allow you to monitor web requests, web ACLs, and rules.

Rules	CloudWatch metric name
☑ rule-1	rule-1

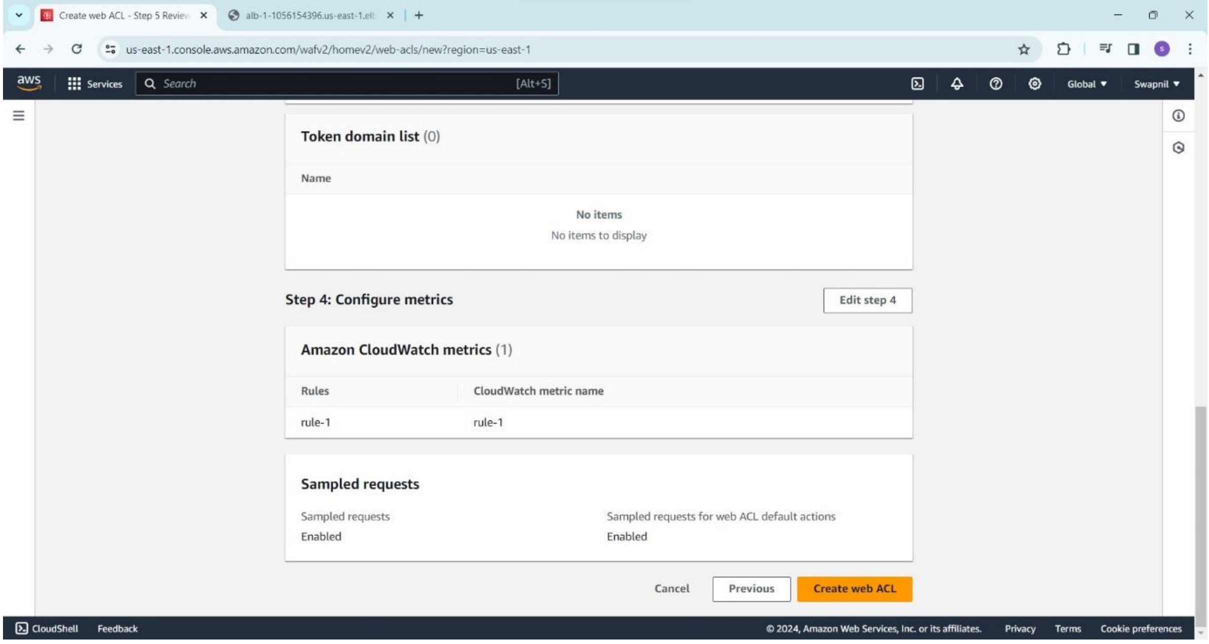
Request sampling options

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

Step 18: Review and create web ACL


Create web ACL - Step 5 Review
alb-1-1056154396.us-east-1.elb
us-east-1.console.aws.amazon.com/wafv2/homev2/web-acls/new?region=us-east-1
aws
Services
Search
[Alt+S]
Global
Swapnil
Edit step 4
Cancel
Previous
Create web ACL
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Token domain list (0)

Name

No items

No items to display

Step 4: Configure metrics

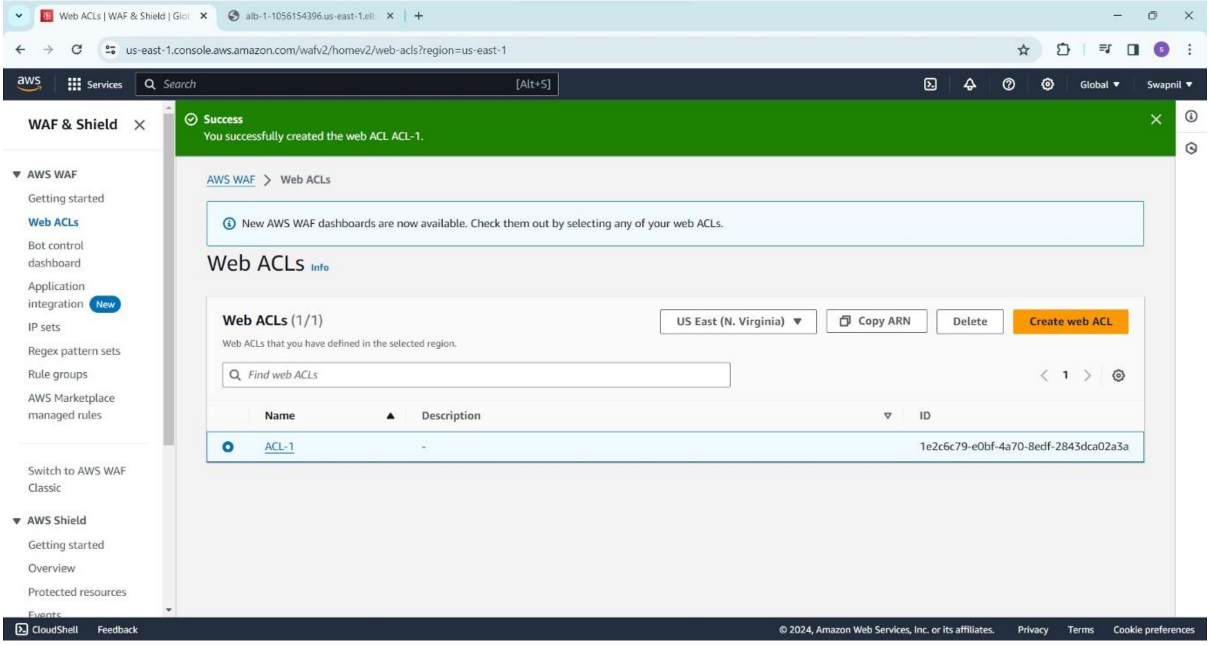
Amazon CloudWatch metrics (1)

Rules	CloudWatch metric name
rule-1	rule-1

Sampled requests

Sampled requests	Sampled requests for web ACL default actions
Enabled	Enabled

Step 19: web ACL is created



Success
You successfully created the web ACL ACL-1.

New AWS WAF dashboards are now available. Check them out by selecting any of your web ACLs.

Web ACLs (1/1)

Web ACLs that you have defined in the selected region.

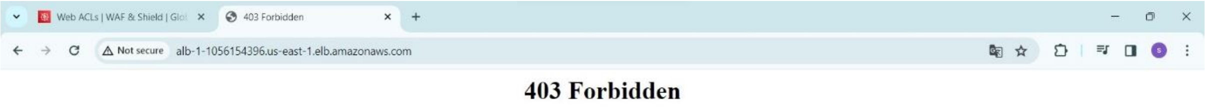
	Name	Description	ID
●	ACL-1	-	1e2c6c79-e0bf-4a70-8edf-2843dca02a3a

Step 20: Check the result

Try to access a load balancer from the IP which is define in the IP sets rules group

We get 403 forbidden message because WAF block that IP.

403 Forbidden error, it means that you do not have permission to view the requested file or resource.

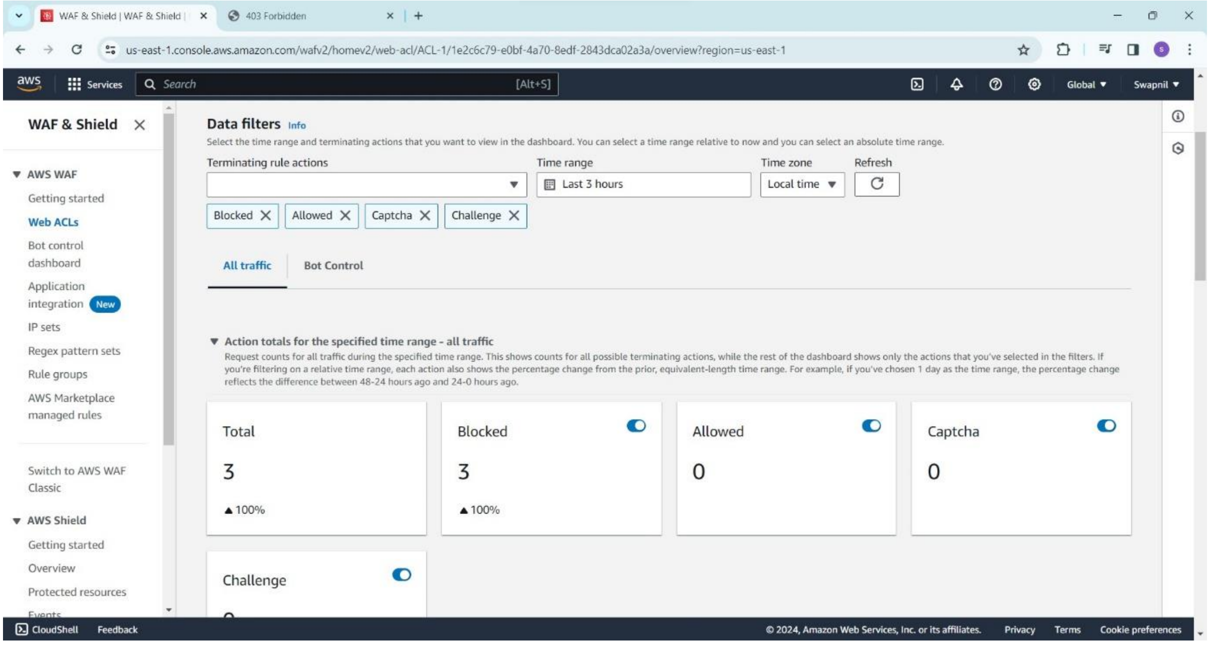

Web ACLs | WAF & Shield | Glo
403 Forbidden
Not secure
alb-1-1056154396.us-east-1.elb.amazonaws.com

403 Forbidden

Step 21:

From WEB ACL we filter the traffic and check all details

Like blocked, allowed IP, Sample of bot detection, client device types, attack type, top 10 countries, etc.



Data filters Info

Select the time range and terminating actions that you want to view in the dashboard. You can select a time range relative to now and you can select an absolute time range.

Terminating rule actions: Blocked, Allowed, Captcha, Challenge

Time range: Last 3 hours

Time zone: Local time

Refresh

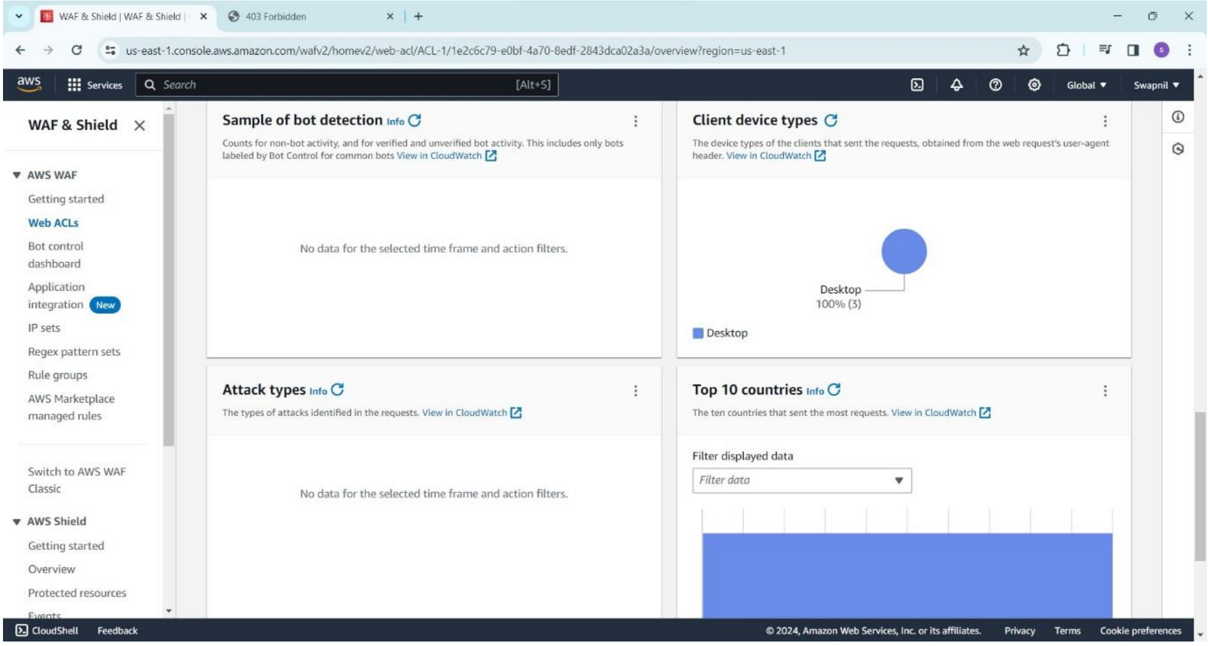
All traffic | Bot Control

Action totals for the specified time range - all traffic

Request counts for all traffic during the specified time range. This shows counts for all possible terminating actions, while the rest of the dashboard shows only the actions that you've selected in the filters. If you're filtering on a relative time range, each action also shows the percentage change from the prior, equivalent-length time range. For example, if you've chosen 1 day as the time range, the percentage change reflects the difference between 48-24 hours ago and 24-0 hours ago.

Total	Blocked	Allowed	Captcha
3	3	0	0
▲100%	▲100%		

Challenge



Sample of bot detection Info

Counts for non-bot activity, and for verified and unverified bot activity. This includes only bots labeled by Bot Control for common bots View in CloudWatch

No data for the selected time frame and action filters.

Client device types

The device types of the clients that sent the requests, obtained from the web request's user-agent header. View in CloudWatch

Attack types Info

The types of attacks identified in the requests. View in CloudWatch

No data for the selected time frame and action filters.

Top 10 countries Info

The ten countries that sent the most requests. View in CloudWatch

Filter displayed data: Filter data