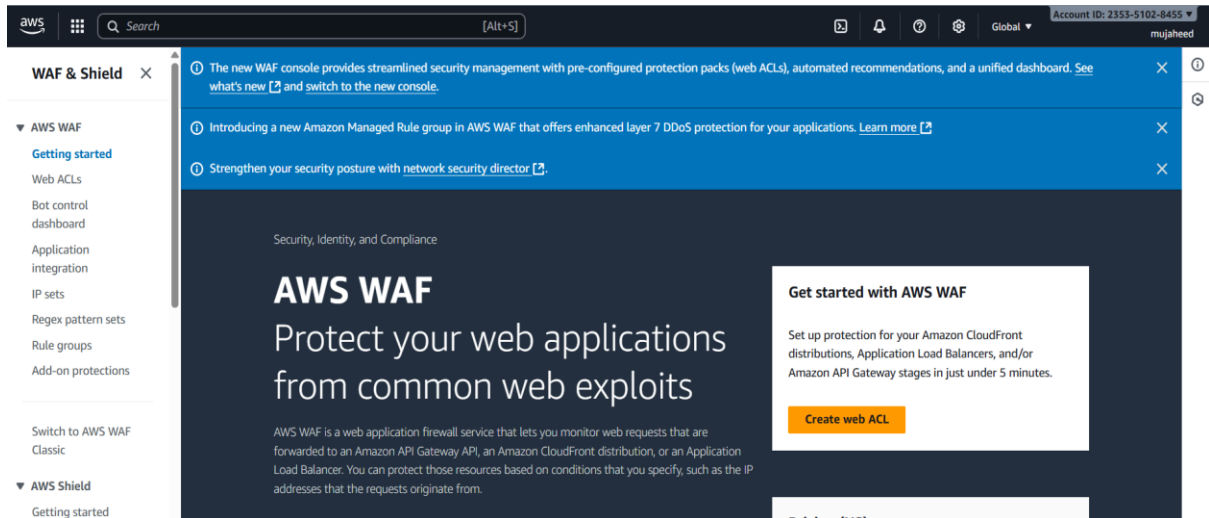
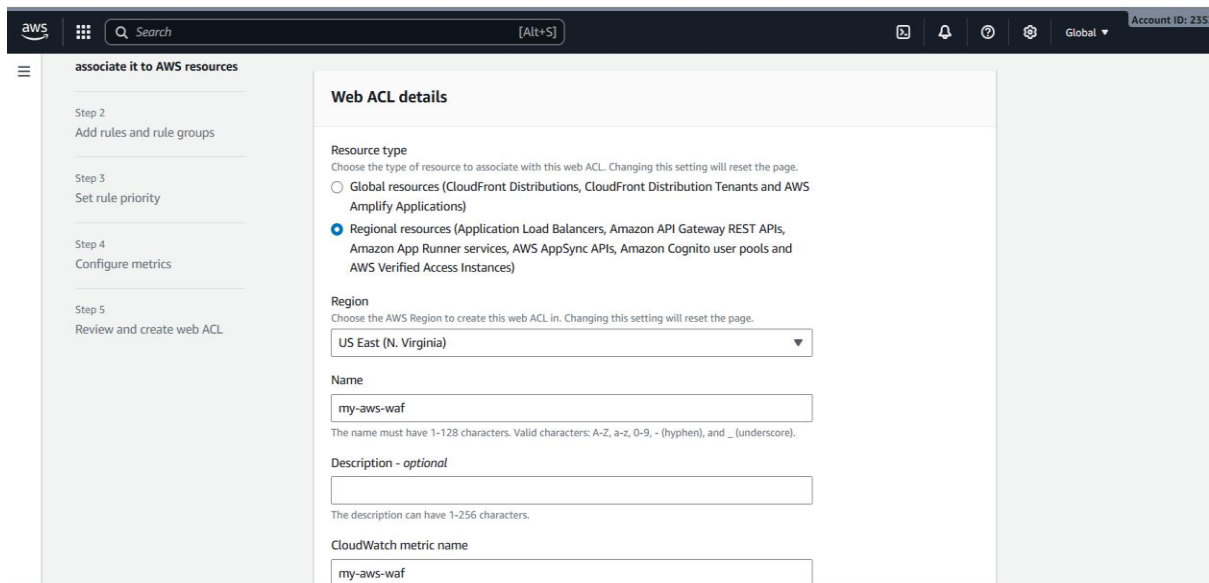


AWS WAF:

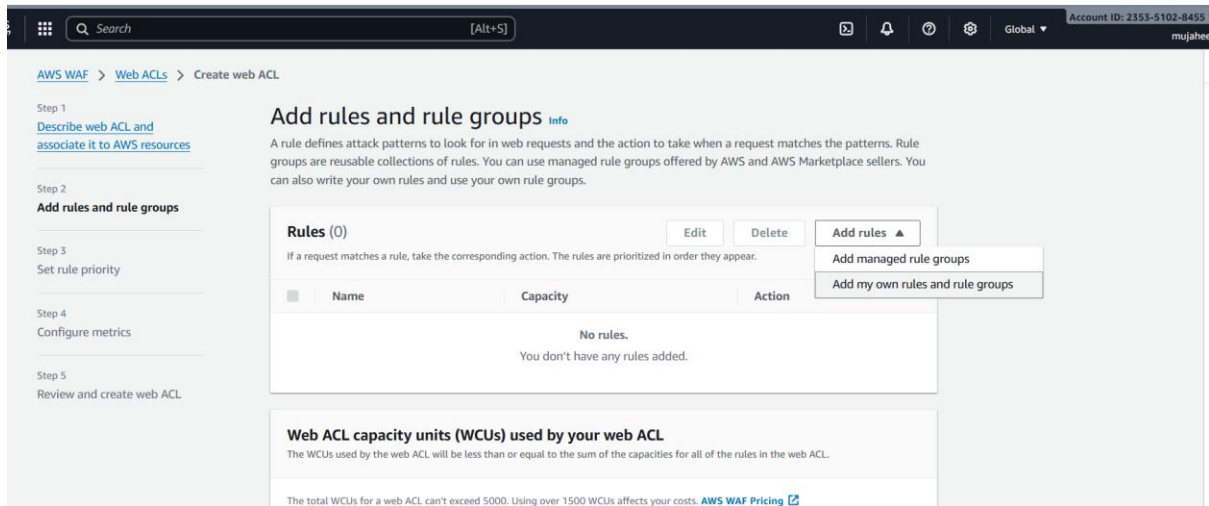
go to aws console and click on search bar as AWS WAF



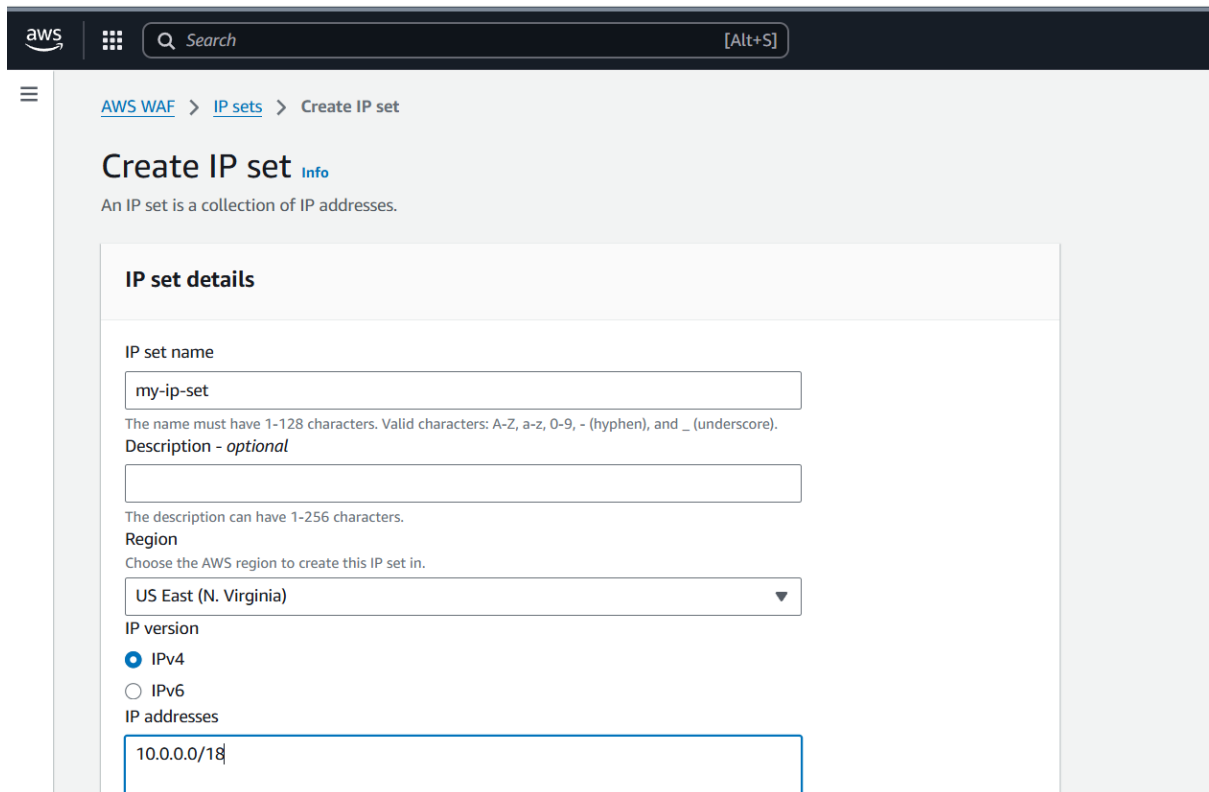
Click on create web ACL and give name for that waf and click on next.



Click on add rules and select add my own rules and rule groups.



In waf console click on create ip set. Give name and select ipv4 and give 1 ip address.



In creation of waf select ip set and give the name and select your created ipset and enable the action to allow or deny and click on add rule.

aws Search [Alt+S]

[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

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

Allow-ipset

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

IP set

IP set

my-ip-set

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

IP set

IP set

my-ip-set

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 customize [?](#)

☐ Challenge

► Custom request - optional

Cancel Add rule

Select you ip-set and choose the action and click on create.

aws

Search

[Alt+S]

Global

Account ID

Step 3
Set rule priority

Step 4
Configure metrics

Step 5
Review and create web ACL

Rules (1/1)

EditDeleteAdd rules

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

	Name	Capacity	Action
<input checked="" type="checkbox"/>	Allow-ipset	1	Allow

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

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

Default action

☒ Allow

☐ Block

☐ Custom request - optional

CloudShellFeedback

© 2025, Amazon Web Services, Inc. or its affiliates. PrivacyTerms

aws

Search

[Alt+S]

Global

Account ID

[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
<input checked="" type="checkbox"/> Allow-ipset	<input type="text" value="Allow-ipset"/>

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

Cancel

Previous

Next

aws

Search

[Alt+S]

WAF & Shield

▼ AWS WAF

Getting started

Web ACLs

Bot control dashboard

Application integration

IP sets

Regex pattern sets

Rule groups

Add-on protections

Switch to AWS WAF Classic

▼ AWS Shield

Getting started

AWS WAF

>

Web ACLs

Web ACLs

Info

Web ACLs (1)

US East (N. Virginia)

Delete

Find web ACLs

	Name	Description	ARN
	my-aws-waf	-	arn:aws:wafv2:us-east-1:235351028455:regional/webacl...