NEERAJ PANWAR (B7-CEQ545)

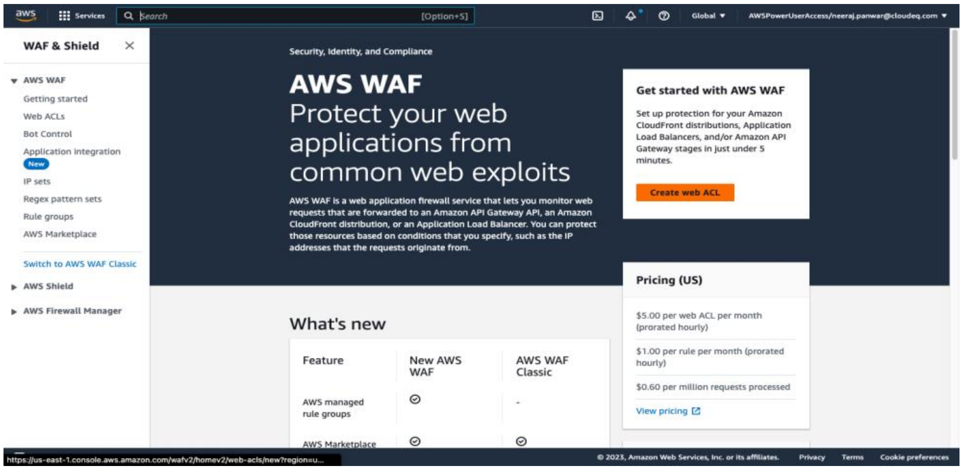
AWS WAF

AWS WAF is a web application firewall that lets you monitor the HTTP and HTTPS requests that are forwarded to your protected web application resources. You can protect the following resource types:

- Amazon CloudFront distribution
- Amazon API Gateway REST API
- Application Load Balancer
- AWS AppSync GraphQL API
- Amazon Cognito user pool
- AWS App Runner service

AWS WAF lets you control access to your content. Based on conditions that you specify, such as the IP addresses that requests originate from or the values of query strings, your protected resource responds to requests either with the requested content, with an HTTP 403 status code (Forbidden), or with a custom response.

Create web ACL(**Access control list):**



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.

Pricing (US)

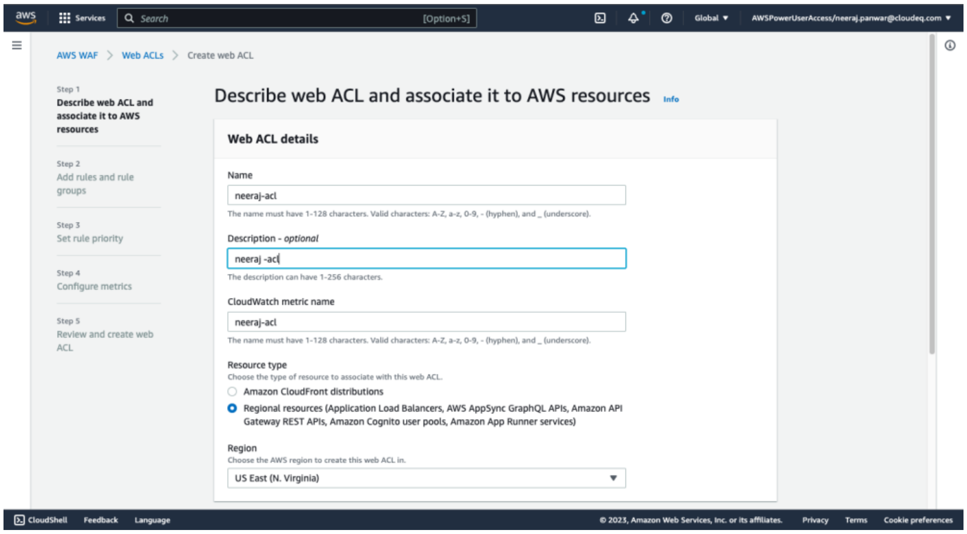
$5.00 per web ACL per month (prorated hourly)

$1.00 per rule per month (prorated hourly)

$0.60 per million requests processed

What's new

Feature	New AWS WAF	AWS WAF Classic
AWS managed rule groups	✓	-
AWS Marketplace	✓	✓


aws
Services
Search
[Option+S]
Global ▾
AWSPowerUserAccess/neeraj.panwar@cloudeq.com ▾
AWS WAF > Web ACLs > Create web ACL
Info
CloudShell
Feedback
Language
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

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

Web ACL details

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

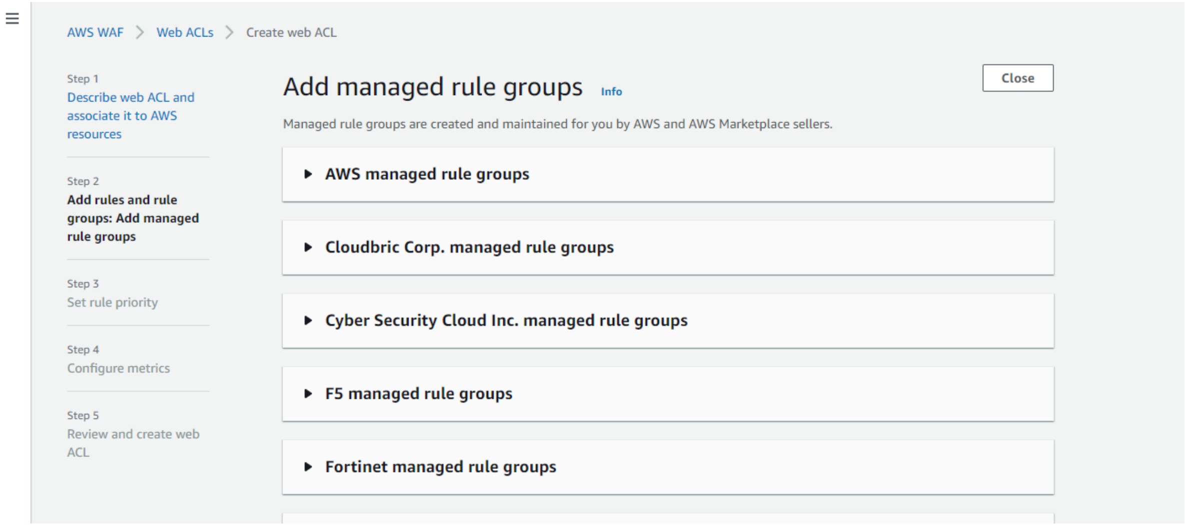
Description - *optional*: neeraj -acl
The description can have 1-256 characters.

CloudWatch metric name: neeraj-acl
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.
○ Amazon CloudFront distributions
● Regional resources (Application Load Balancers, AWS AppSync GraphQL APIs, Amazon API Gateway REST APIs, Amazon Cognito user pools, Amazon App Runner services)

Region
Choose the AWS region to create this web ACL in.
US East (N. Virginia)

Add Managed rule groups:



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: Add managed rule groups

Step 3
Set rule priority

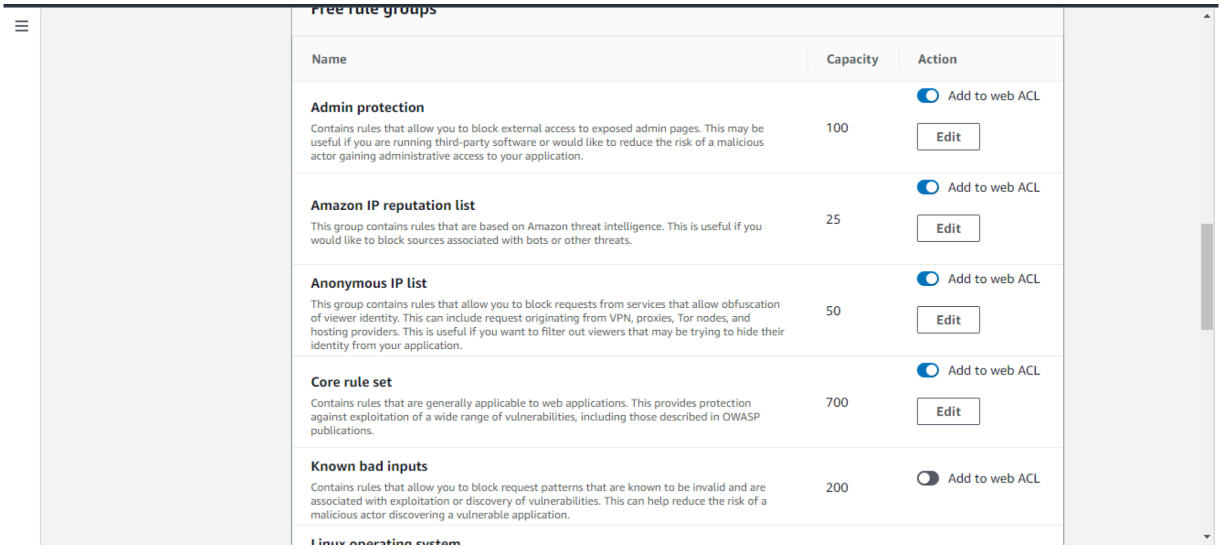
Step 4
Configure metrics

Step 5
Review and create web ACL

Add managed rule groups

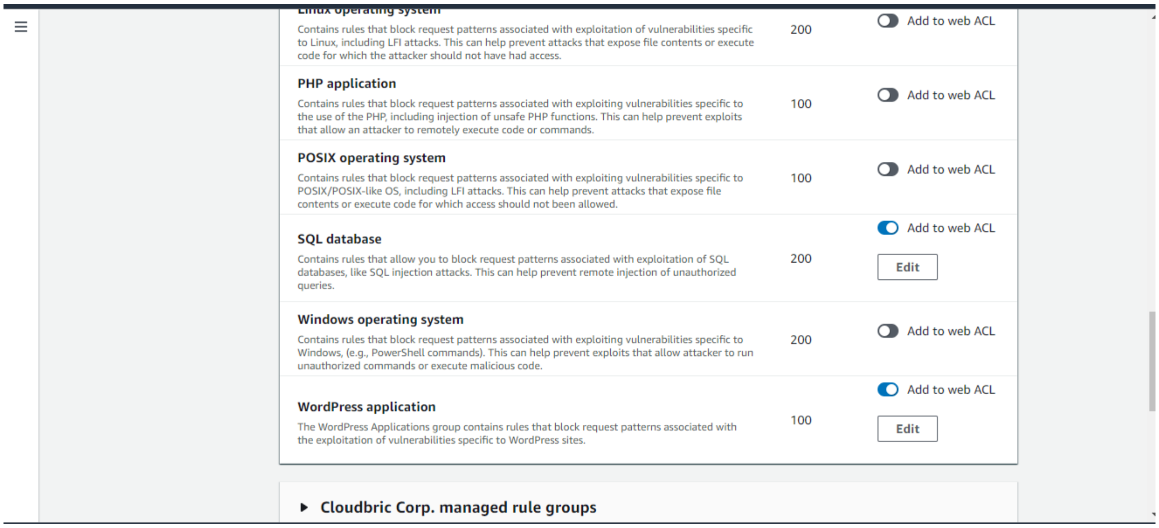
Managed rule groups are created and maintained for you by AWS and AWS Marketplace sellers.

- ▸ **AWS managed rule groups**
- ▸ **Cloudbric Corp. managed rule groups**
- ▸ **Cyber Security Cloud Inc. managed rule groups**
- ▸ **F5 managed rule groups**
- ▸ **Fortinet managed rule groups**



Free rule groups

Name	Capacity	Action
Admin protection Contains rules that allow you to block external access to exposed admin pages. This may be useful if you are running third-party software or would like to reduce the risk of a malicious actor gaining administrative access to your application.	100	● Add to web ACL Edit
Amazon IP reputation list This group contains rules that are based on Amazon threat intelligence. This is useful if you would like to block sources associated with bots or other threats.	25	● Add to web ACL Edit
Anonymous IP list This group contains rules that allow you to block requests from services that allow obfuscation of viewer identity. This can include request originating from VPN, proxies, Tor nodes, and hosting providers. This is useful if you want to filter out viewers that may be trying to hide their identity from your application.	50	● Add to web ACL Edit
Core rule set Contains rules that are generally applicable to web applications. This provides protection against exploitation of a wide range of vulnerabilities, including those described in OWASP publications.	700	● Add to web ACL Edit
Known bad inputs Contains rules that allow you to block request patterns that are known to be invalid and are associated with exploitation or discovery of vulnerabilities. This can help reduce the risk of a malicious actor discovering a vulnerable application.	200	○ Add to web ACL
Linux operating system		



Linux operating system

Contains rules that block request patterns associated with exploitation of vulnerabilities specific to Linux, including LFI attacks. This can help prevent attacks that expose file contents or execute code for which the attacker should not have had access.

200 — Add to web ACL: off

PHP application

Contains rules that block request patterns associated with exploiting vulnerabilities specific to the use of the PHP, including injection of unsafe PHP functions. This can help prevent exploits that allow an attacker to remotely execute code or commands.

100 — Add to web ACL: off

POSIX operating system

Contains rules that block request patterns associated with exploiting vulnerabilities specific to POSIX/POSIX-like OS, including LFI attacks. This can help prevent attacks that expose file contents or execute code for which access should not been allowed.

100 — Add to web ACL: off

SQL database

Contains rules that allow you to block request patterns associated with exploitation of SQL databases, like SQL injection attacks. This can help prevent remote injection of unauthorized queries.

200 — Add to web ACL: on — Edit

Windows operating system

Contains rules that block request patterns associated with exploiting vulnerabilities specific to Windows, (e.g., PowerShell commands). This can help prevent exploits that allow attacker to run unauthorized commands or execute malicious code.

200 — Add to web ACL: off

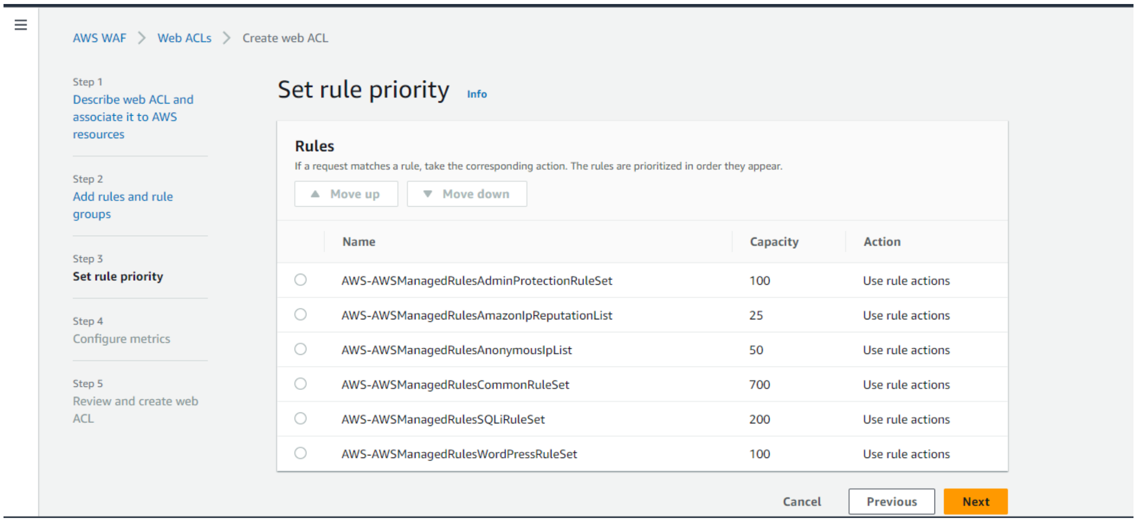
WordPress application

The WordPress Applications group contains rules that block request patterns associated with the exploitation of vulnerabilities specific to WordPress sites.

100 — Add to web ACL: on — Edit

▸ **Cloudbric Corp. managed rule groups**

Set Rule Priority:



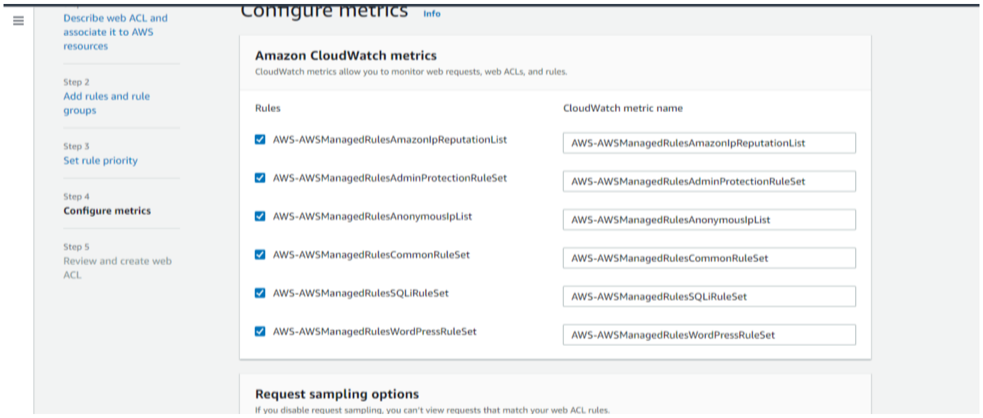
AWS WAF > Web ACLs > Create web ACL
Step 1
Describe web ACL and associate it to AWS resources
Step 2
Add rules and rule groups
Step 3
Set rule priority
Step 4
Configure metrics
Step 5
Review and create web ACL

Set rule priority

Rules

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

	Name	Capacity	Action
○	AWS-AWSManagedRulesAdminProtectionRuleSet	100	Use rule actions
○	AWS-AWSManagedRulesAmazonIpReputationList	25	Use rule actions
○	AWS-AWSManagedRulesAnonymousIpList	50	Use rule actions
○	AWS-AWSManagedRulesCommonRuleSet	700	Use rule actions
○	AWS-AWSManagedRulesSQLiRuleSet	200	Use rule actions
○	AWS-AWSManagedRulesWordPressRuleSet	100	Use rule actions


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

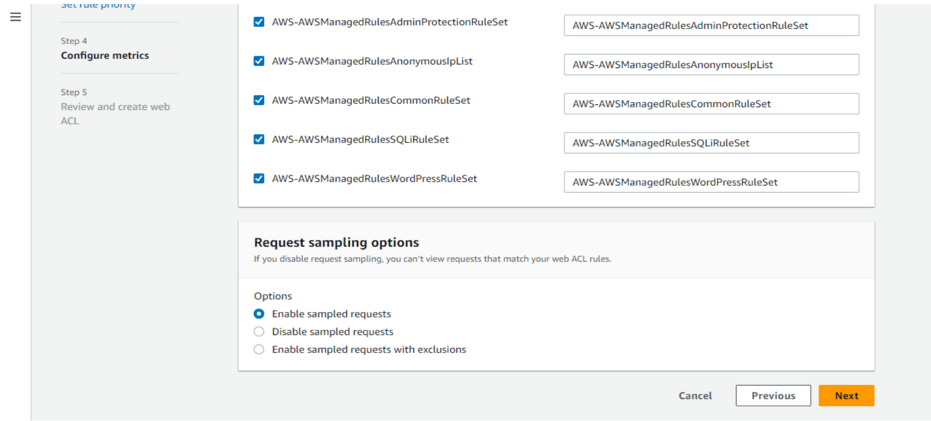
Amazon CloudWatch metrics

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

Rules	CloudWatch metric name
☑ AWS-AWSManagedRulesAmazonIpReputationList	AWS-AWSManagedRulesAmazonIpReputationList
☑ AWS-AWSManagedRulesAdminProtectionRuleSet	AWS-AWSManagedRulesAdminProtectionRuleSet
☑ AWS-AWSManagedRulesAnonymousIpList	AWS-AWSManagedRulesAnonymousIpList
☑ AWS-AWSManagedRulesCommonRuleSet	AWS-AWSManagedRulesCommonRuleSet
☑ AWS-AWSManagedRulesSQLiRuleSet	AWS-AWSManagedRulesSQLiRuleSet
☑ AWS-AWSManagedRulesWordPressRuleSet	AWS-AWSManagedRulesWordPressRuleSet

Request sampling options

If you disable request sampling, you can't view requests that match your web ACL rules.



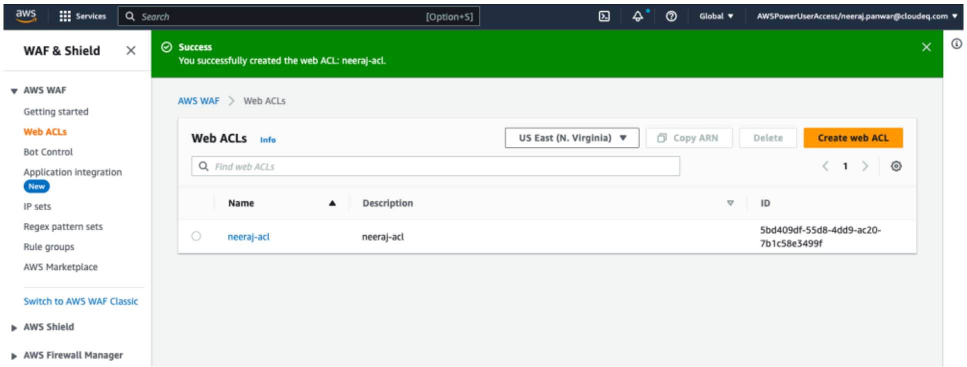
☑ AWS-AWSManagedRulesAdminProtectionRuleSet	AWS-AWSManagedRulesAdminProtectionRuleSet
☑ AWS-AWSManagedRulesAnonymousIpList	AWS-AWSManagedRulesAnonymousIpList
☑ AWS-AWSManagedRulesCommonRuleSet	AWS-AWSManagedRulesCommonRuleSet
☑ AWS-AWSManagedRulesSQLiRuleSet	AWS-AWSManagedRulesSQLiRuleSet
☑ AWS-AWSManagedRulesWordPressRuleSet	AWS-AWSManagedRulesWordPressRuleSet

Request sampling options

If you disable request sampling, you can't view requests that match your web ACL rules.

Options

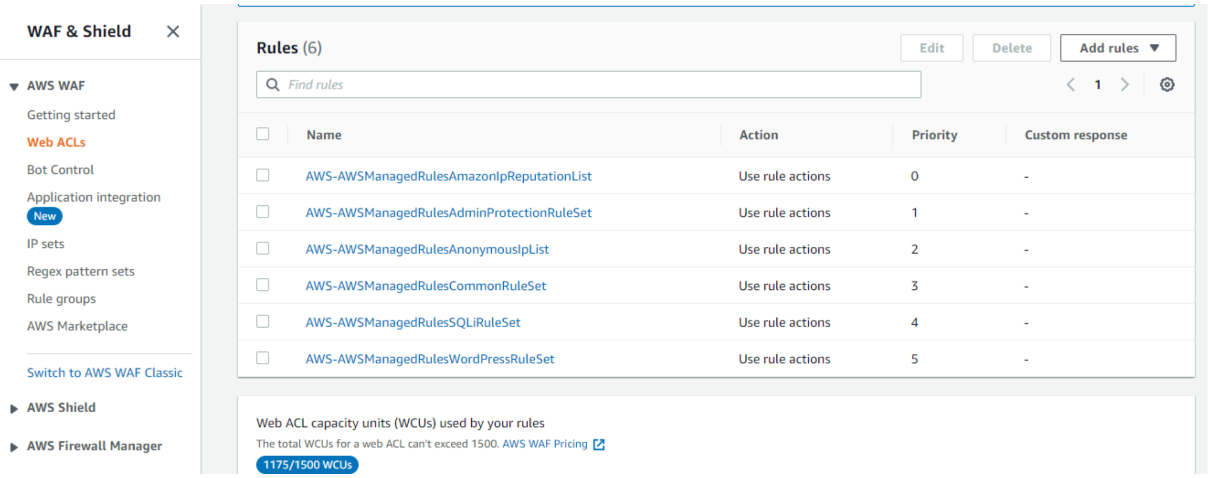
● Enable sampled requests
○ Disable sampled requests
○ Enable sampled requests with exclusions



Success
You successfully created the web ACL: neeraj-acl.

	Name	Description	ID
○	neeraj-acl	neeraj-acl	5bd409df-55d8-4dd9-ac20-7b1c58e3499f

Add Rules:



Rules (6)

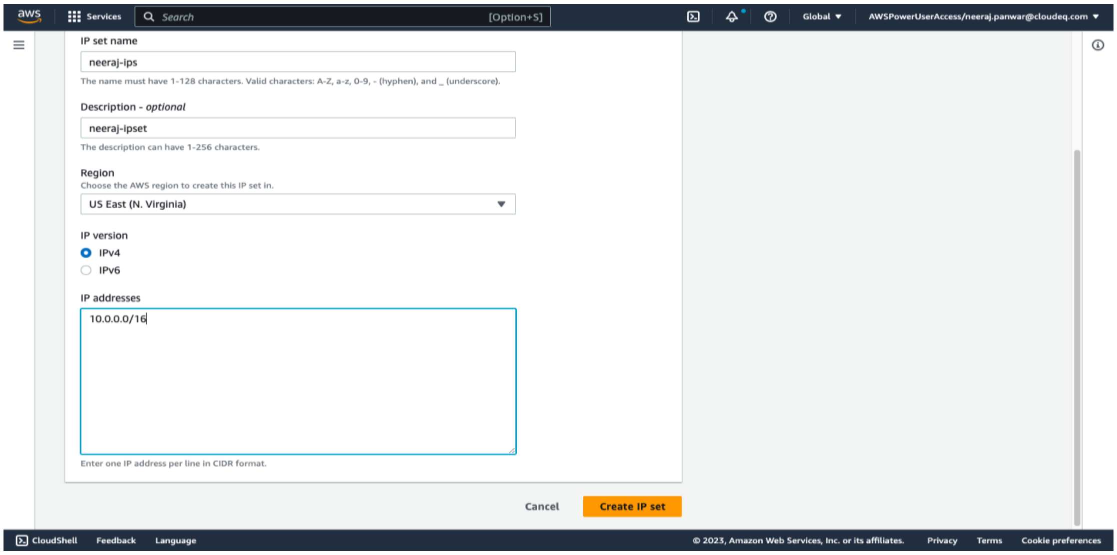
□	Name	Action	Priority	Custom response
□	AWS-AWSManagedRulesAmazonIpReputationList	Use rule actions	0	-
□	AWS-AWSManagedRulesAdminProtectionRuleSet	Use rule actions	1	-
□	AWS-AWSManagedRulesAnonymousIpList	Use rule actions	2	-
□	AWS-AWSManagedRulesCommonRuleSet	Use rule actions	3	-
□	AWS-AWSManagedRulesSQLiRuleSet	Use rule actions	4	-
□	AWS-AWSManagedRulesWordPressRuleSet	Use rule actions	5	-

Web ACL capacity units (WCUs) used by your rules

The total WCUs for a web ACL can't exceed 1500. AWS WAF Pricing

1175/1500 WCUs

Create IP:



IP set name

neeraj-ips

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

Description - *optional*

neeraj-ipset

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

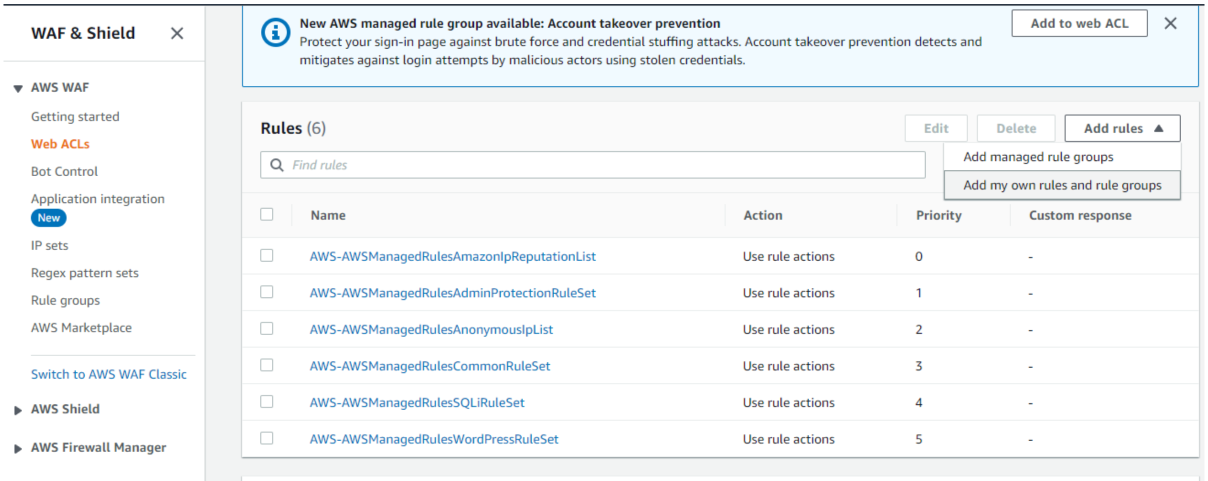
○ IPv6

IP addresses

10.0.0.0/16

Enter one IP address per line in CIDR format.

Add my own rules and rule group:

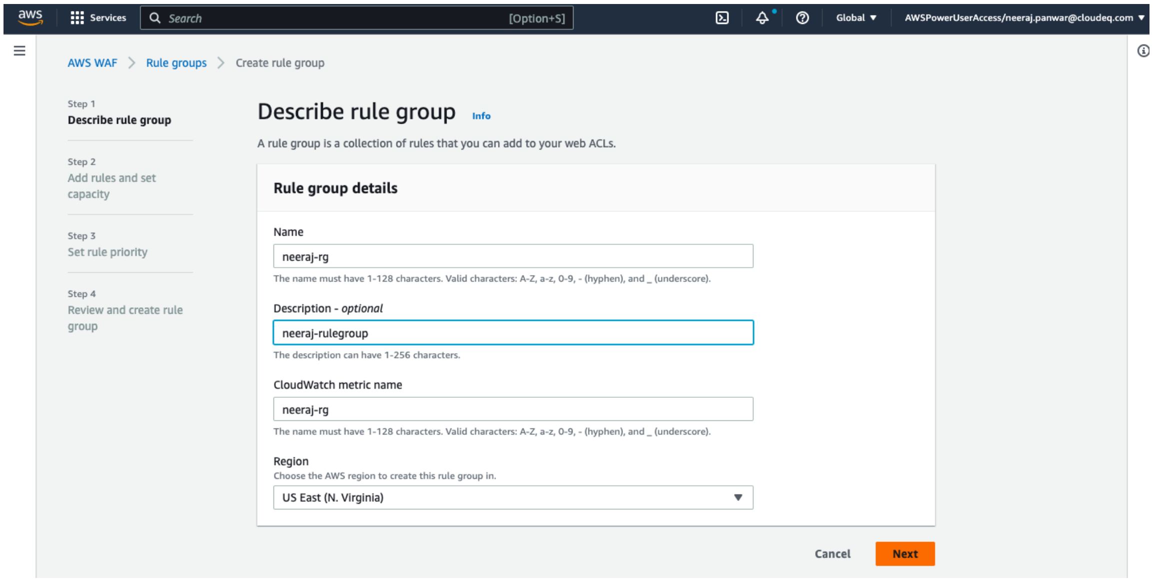


New AWS managed rule group available: Account takeover prevention
Protect your sign-in page against brute force and credential stuffing attacks. Account takeover prevention detects and mitigates against login attempts by malicious actors using stolen credentials.

Rules (6)

Name	Action	Priority	Custom response
AWS-AWSManagedRulesAmazonIpReputationList	Use rule actions	0	-
AWS-AWSManagedRulesAdminProtectionRuleSet	Use rule actions	1	-
AWS-AWSManagedRulesAnonymousIpList	Use rule actions	2	-
AWS-AWSManagedRulesCommonRuleSet	Use rule actions	3	-
AWS-AWSManagedRulesSQLiRuleSet	Use rule actions	4	-
AWS-AWSManagedRulesWordPressRuleSet	Use rule actions	5	-

Create Rule groups:


aws
Services
Search
[Option+S]
Global
AWSPowerUserAccess/neeraj.panwar@cloudeq.com
AWS WAF > Rule groups > Create rule group
Step 1
Describe rule group
Step 2
Add rules and set capacity
Step 3
Set rule priority
Step 4
Review and create rule group
Info
Cancel
Next

Describe rule group

A rule group is a collection of rules that you can add to your web ACLs.

Rule group details

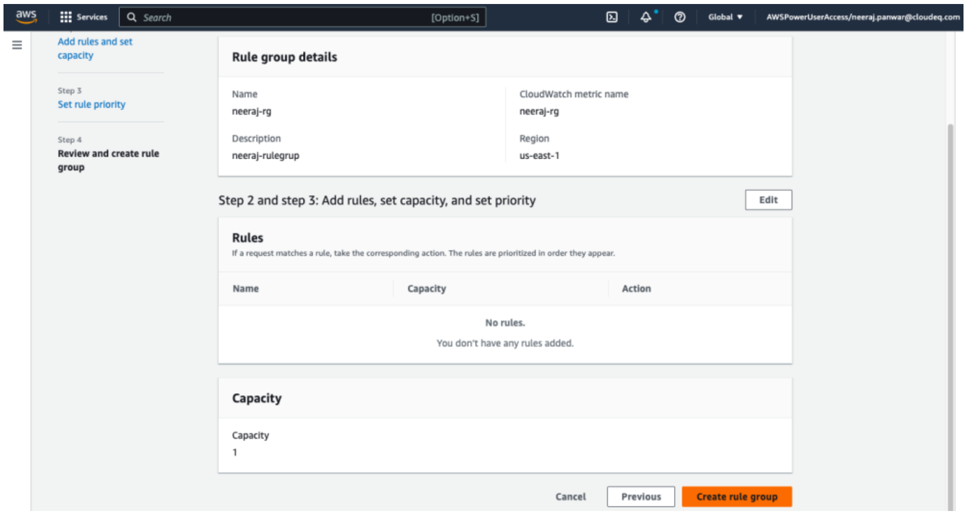
Name: neeraj-rg
The name must have 1-128 characters. Valid characters: A-Z, a-z, 0-9, - (hyphen), and _ (underscore).

Description - *optional*: neeraj-rulegroup
The description can have 1-256 characters.

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

Region
Choose the AWS region to create this rule group in.
US East (N. Virginia)

Add Rule group:



aws
Services
Search
[Option+S]
Global ▼
AWSPowerUserAccess/neeraj.panwar@cloudeq.com
Add rules and set capacity
Step 3
Set rule priority
Step 4
Review and create rule group

Rule group details

Name neeraj-rg	CloudWatch metric name neeraj-rg
Description neeraj-rulegrup	Region us-east-1

Step 2 and step 3: Add rules, set capacity, and set priority

Rules

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

Name	Capacity	Action

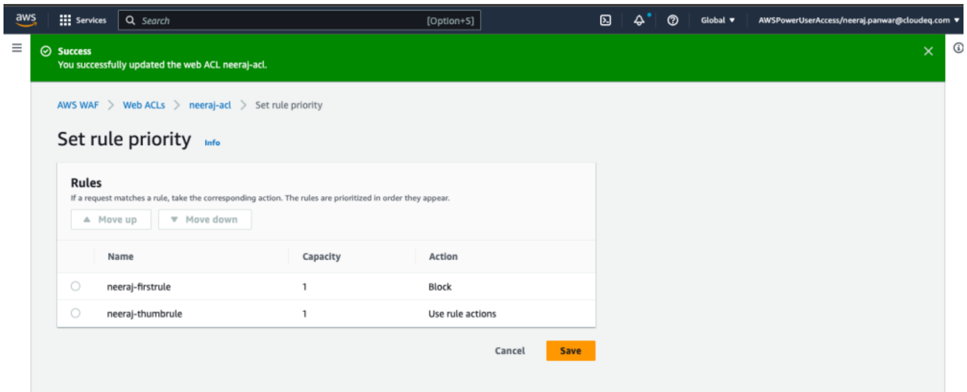
No rules.

You don't have any rules added.

Capacity

Capacity
1

WAF Updated Successfully.



Success
You successfully updated the web ACL neeraj-acl.

AWS WAF > Web ACLs > neeraj-acl > Set rule priority

Set rule priority Info

Rules

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

	Name	Capacity	Action
○	neeraj-firstrule	1	Block
○	neeraj-thumbrule	1	Use rule actions

____________________Thank You____________________________