Lesson 07 Demo 04

Creating and Configuring AWS WAF

Objective: To demonstrate the process of configuring AWS WAF to protect your web applications and APIs hosted on AWS environment

Tools required: AWS Management Console

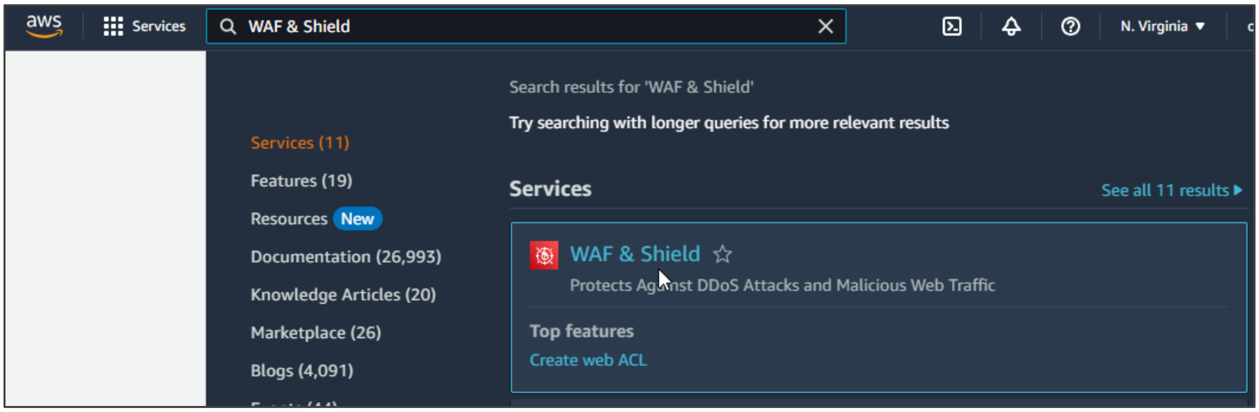
Prerequisites: None

Steps to be followed:

1. Create an IP set
2. Create Web ACL
3. Create a custom rule in Web ACL

Step 1: Create an IP set

1.1 Navigate to the AWS portal, search for and select **WAF & Shield**

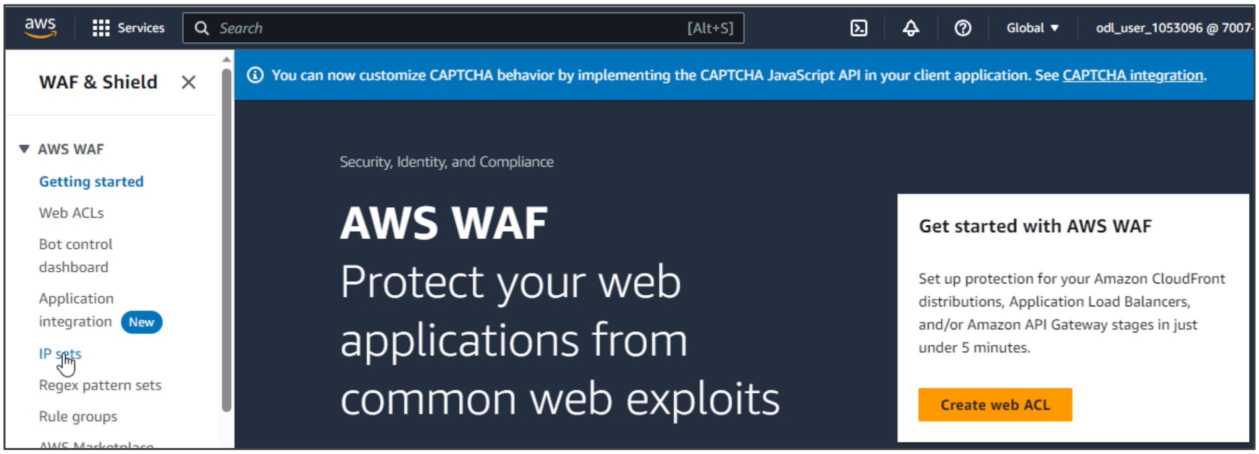


Search results for 'WAF & Shield'

Try searching with longer queries for more relevant results

Protects Against DDoS Attacks and Malicious Web Traffic

1.2 In the WAF & Shield dashboard, select **IP sets** from the left pane



You can now customize CAPTCHA behavior by implementing the CAPTCHA JavaScript API in your client application. See CAPTCHA integration.

Security, Identity, and Compliance

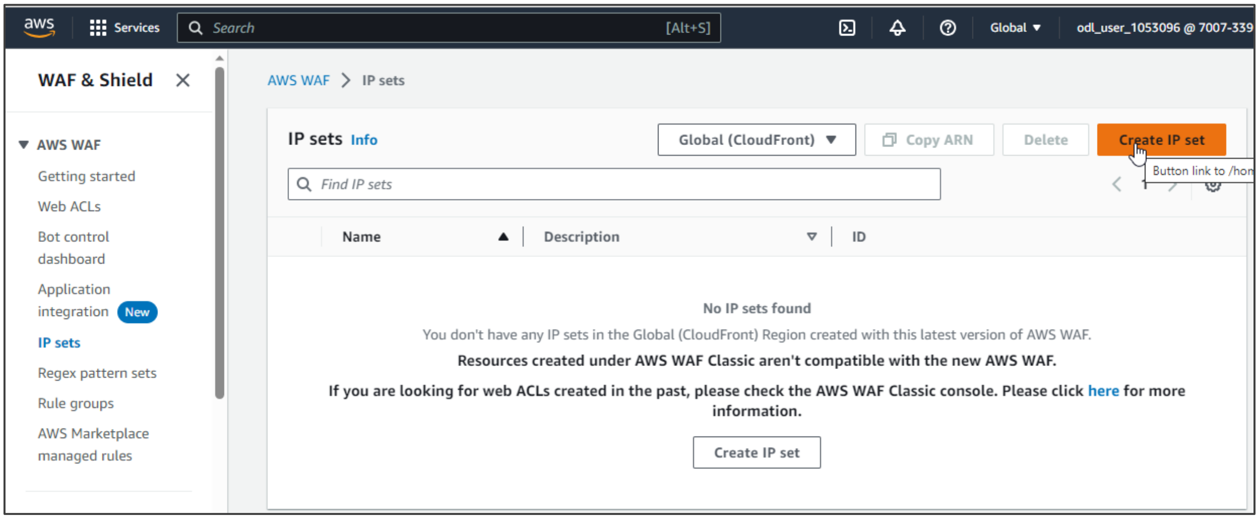
AWS WAF

Protect your web applications from common web exploits

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.

1.3 Click on **Create IP set**



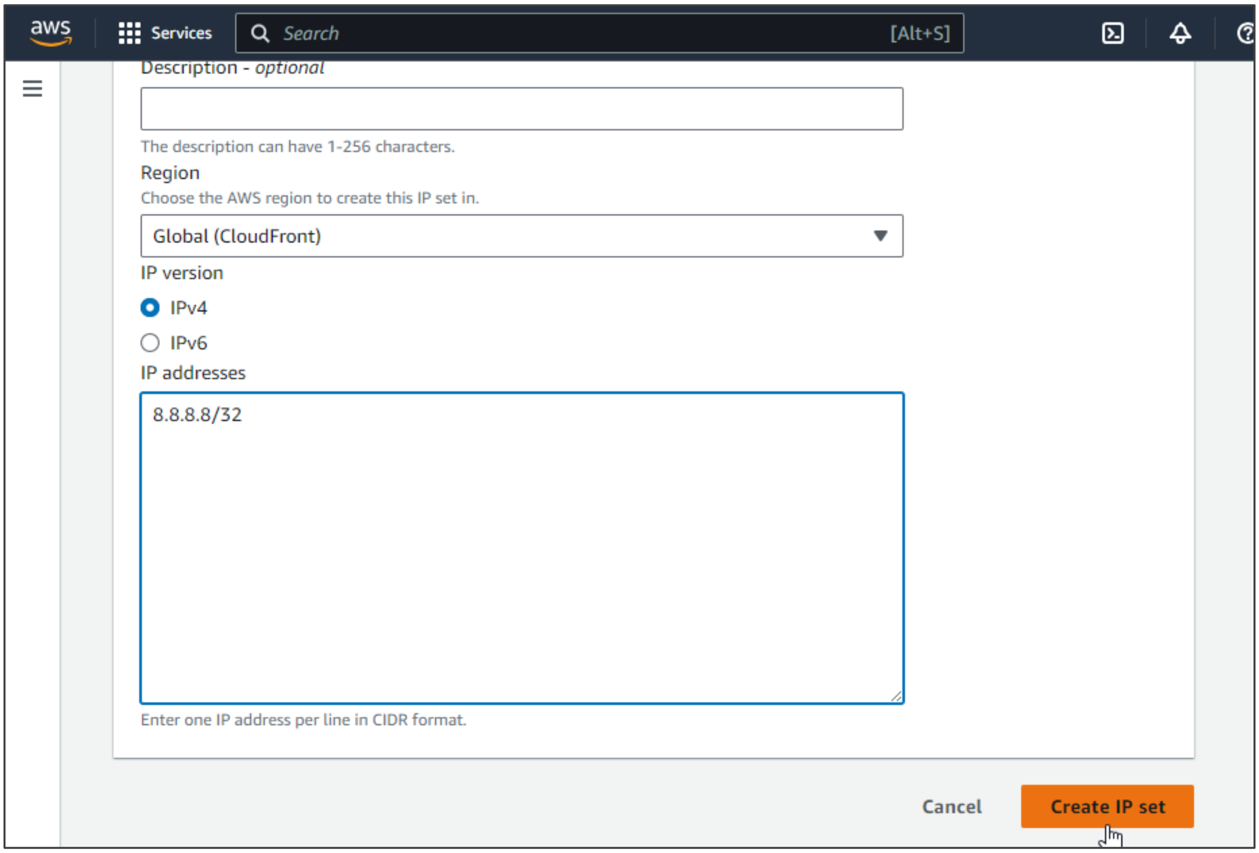
No IP sets found

You don't have any IP sets in the Global (CloudFront) 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.

1.4 Provide a name to the IP set, choose the **Region** as **Global (CloudFront),** select the IP version as **IPv4**, add the IP address as **8.8.8.8/32**, and then click on **Create IP set**



Description - *optional*

The description can have 1-256 characters.

Region

Choose the AWS region to create this IP set in.

Global (CloudFront)

IP version

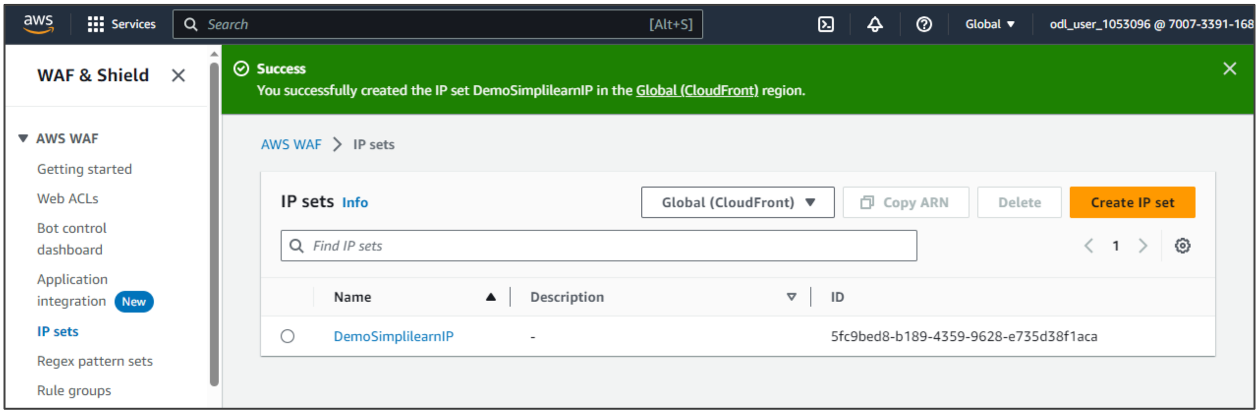
● IPv4

○ IPv6

IP addresses

8.8.8.8/32

Enter one IP address per line in CIDR format.



Success

You successfully created the IP set DemoSimplilearnIP in the Global (CloudFront) region.

AWS WAF > IP sets

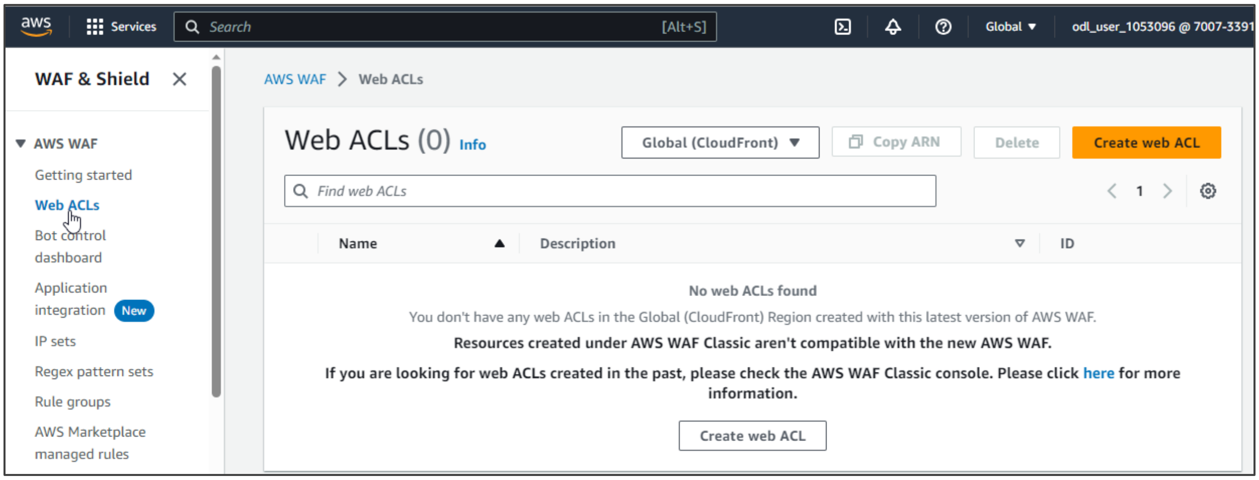
IP sets Info

	Name	Description	ID
○	DemoSimplilearnIP	-	5fc9bed8-b189-4359-9628-e735d38f1aca

The IP set has been created successfully.

Step 2: Create Web ACL

2.1 Navigate back to the WAF & Shield dashboard, select **Web ACLs** from the left pane, and then click on **Create web ACL**



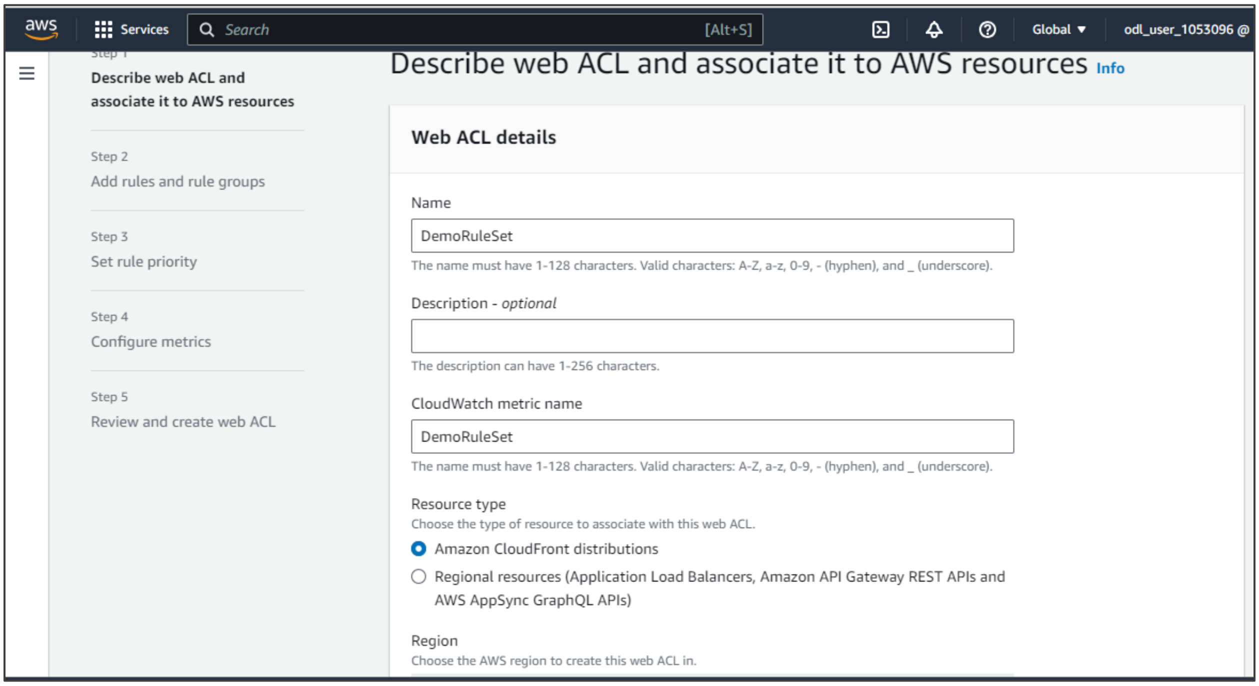
No web ACLs found

You don't have any web ACLs in the Global (CloudFront) 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.

2.2 Provide a name to the Web ACL, choose the **Resource type**, and click on **Next**



Describe web ACL and associate it to AWS resources Info

Web ACL details

Name: DemoRuleSet

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: DemoRuleSet

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.

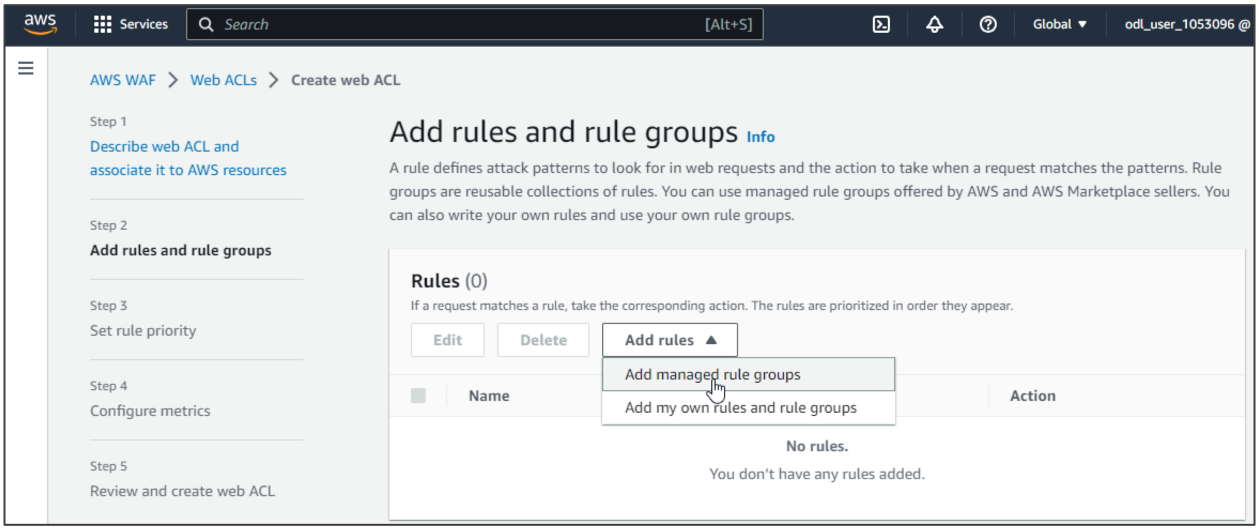
● Amazon CloudFront distributions

○ Regional resources (Application Load Balancers, Amazon API Gateway REST APIs and AWS AppSync GraphQL APIs)

Region

Choose the AWS region to create this web ACL in.

2.3 In the **Add rules and rule groups** page, select **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

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.

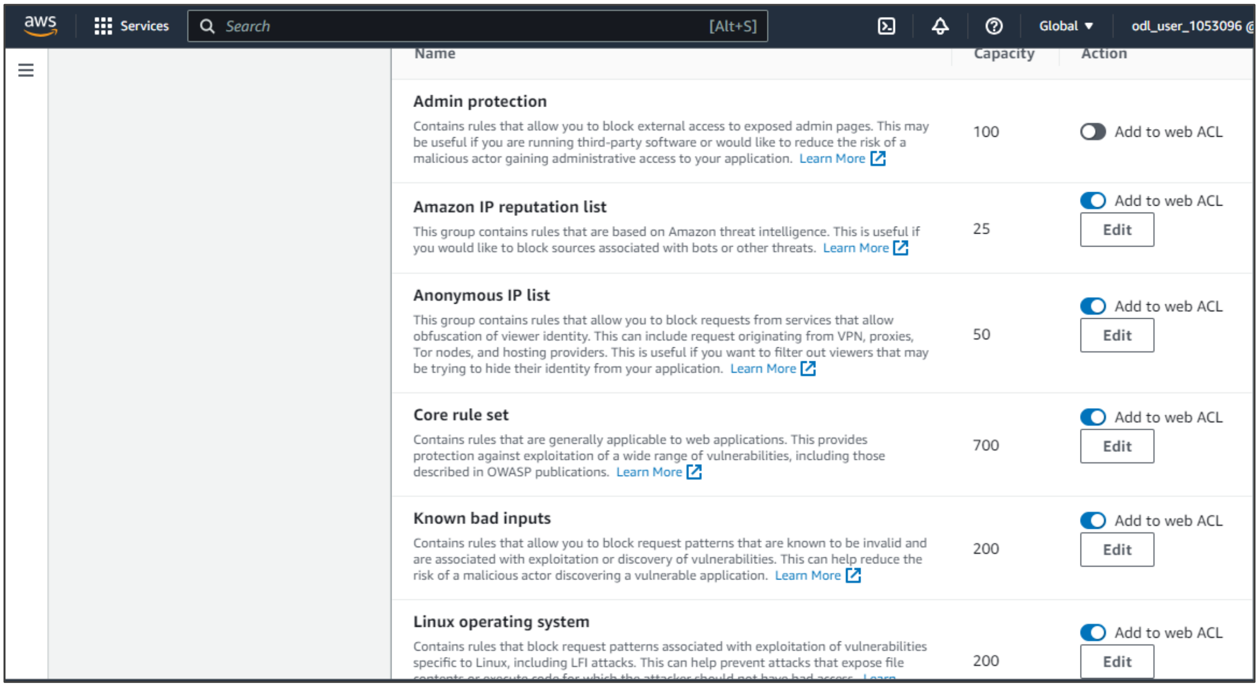
Rules (0)

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

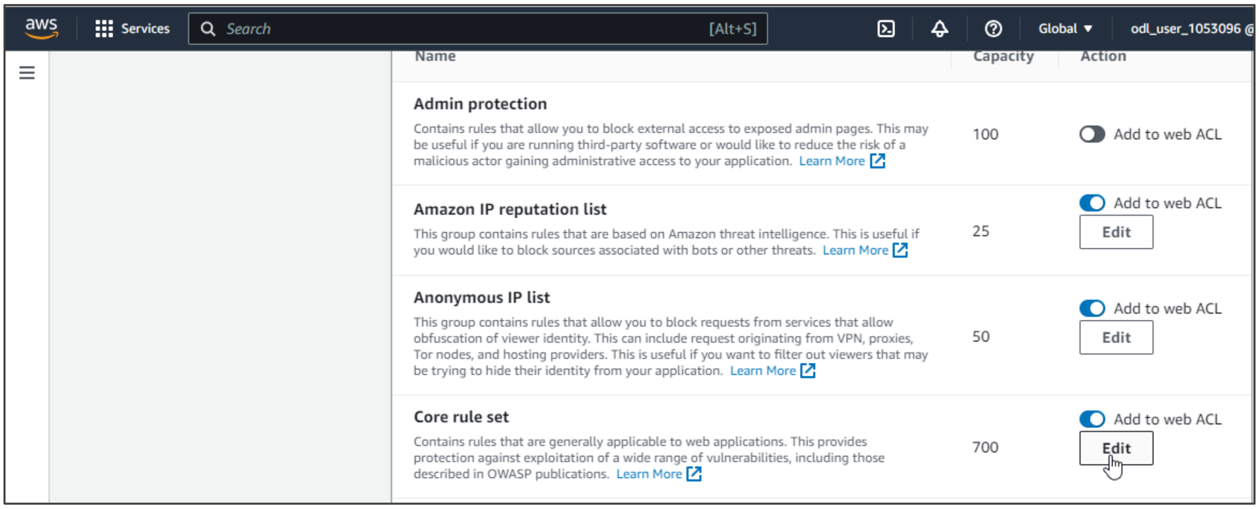
No rules.

You don't have any rules added.

2.4 Select the options in **AWS managed rule groups** as shown here:

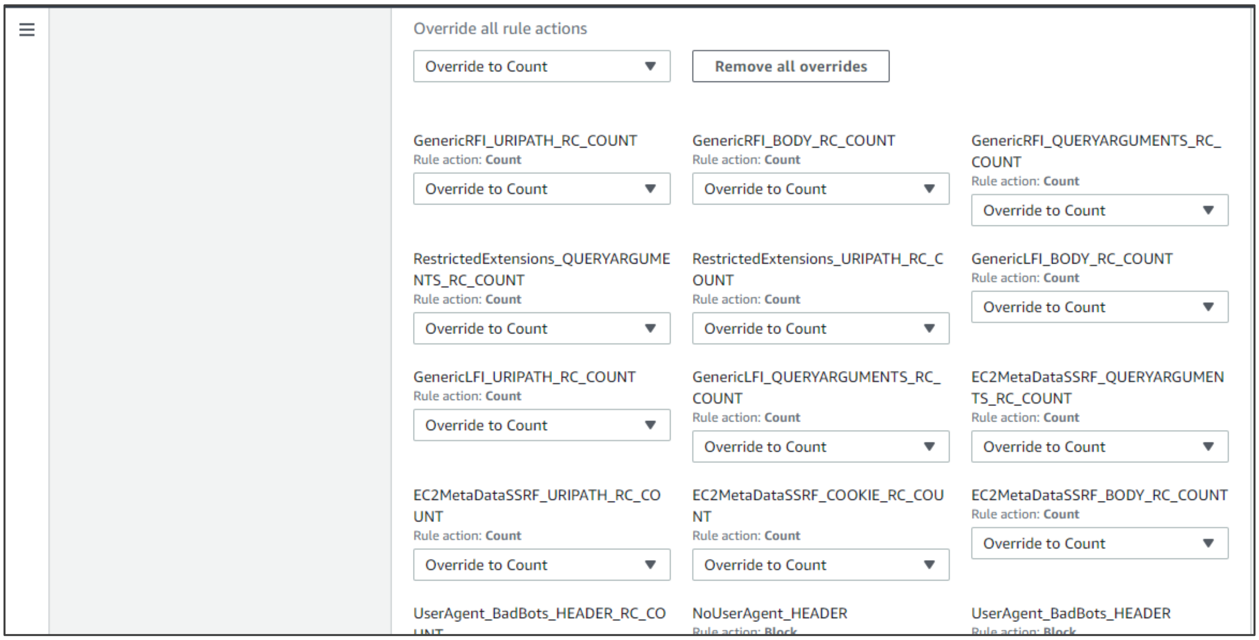


Name	Capacity	Action
Admin protection Contains rules that allow you to block external access to exposed admin pages. This may be useful if you are running third-party software or would like to reduce the risk of a malicious actor gaining administrative access to your application. Learn More	100	○ Add to web ACL
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. Learn More	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. Learn More	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. Learn More	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. Learn More	200	● Add to web ACL Edit
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. Learn	200	● Add to web ACL Edit



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. Learn More	100	○ Add to web ACL
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. Learn More	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. Learn More	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. Learn More	700	● Add to web ACL Edit

2.5 In the **Core rule set** option, click on **Edit**, and then select **Override to Count** from the drop-down menu in the **Override all rule actions** option



Override all rule actions
Override to Count ▼ | Remove all overrides

GenericRFI_URIPATH_RC_COUNT
Rule action: **Count**
Override to Count ▼

GenericRFI_BODY_RC_COUNT
Rule action: **Count**
Override to Count ▼

GenericRFI_QUERYARGUMENTS_RC_COUNT
Rule action: **Count**
Override to Count ▼

RestrictedExtensions_QUERYARGUMENTS_RC_COUNT
Rule action: **Count**
Override to Count ▼

RestrictedExtensions_URIPATH_RC_COUNT
Rule action: **Count**
Override to Count ▼

GenericLFI_BODY_RC_COUNT
Rule action: **Count**
Override to Count ▼

GenericLFI_URIPATH_RC_COUNT
Rule action: **Count**
Override to Count ▼

GenericLFI_QUERYARGUMENTS_RC_COUNT
Rule action: **Count**
Override to Count ▼

EC2MetaDataSSRF_QUERYARGUMENTS_RC_COUNT
Rule action: **Count**
Override to Count ▼

EC2MetaDataSSRF_URIPATH_RC_COUNT
Rule action: **Count**
Override to Count ▼

EC2MetaDataSSRF_COOKIE_RC_COUNT
Rule action: **Count**
Override to Count ▼

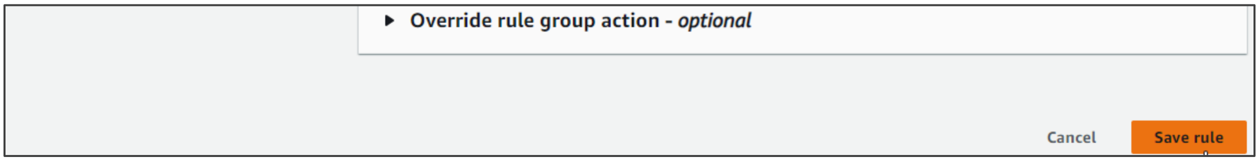
EC2MetaDataSSRF_BODY_RC_COUNT
Rule action: **Count**
Override to Count ▼

UserAgent_BadBots_HEADER_RC_COUNT

NoUserAgent_HEADER
Rule action: **Block**

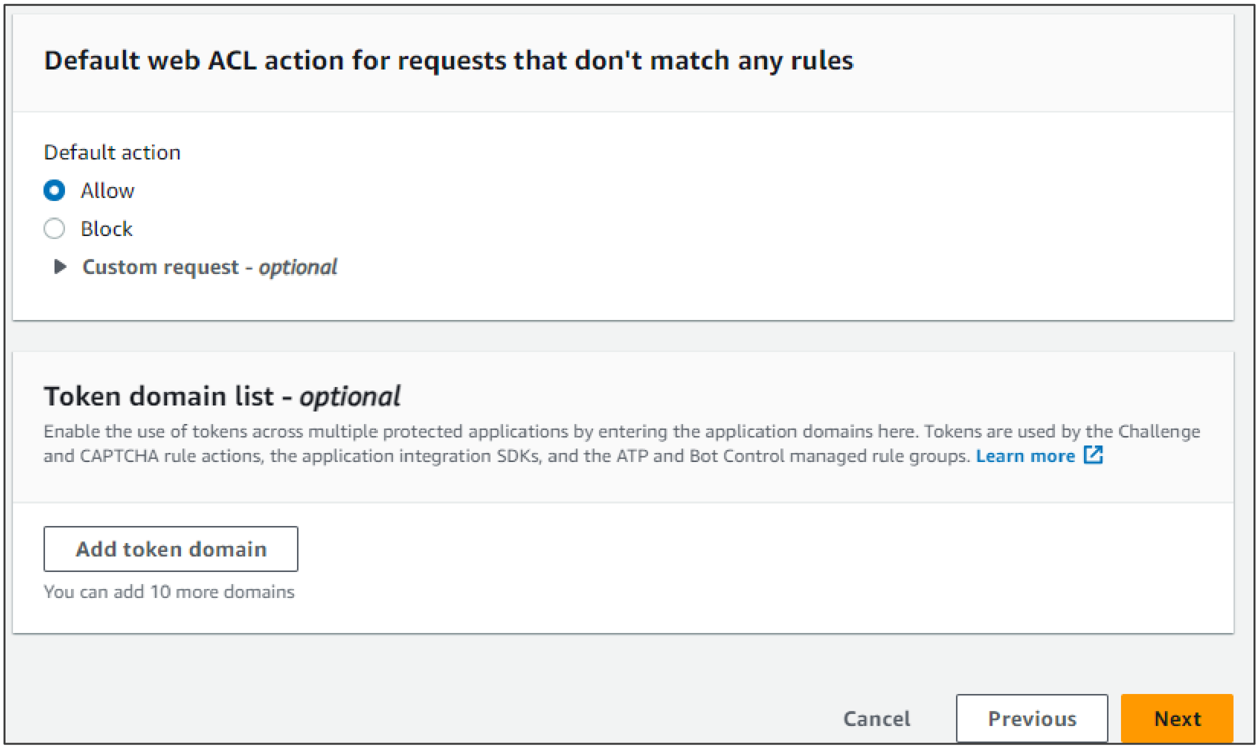
UserAgent_BadBots_HEADER
Rule action: **Block**

2.6 Click on **Save rule**



▶ **Override rule group action** - *optional*

2.7 Now, click on **Next**



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

Default action

● Allow

○ Block

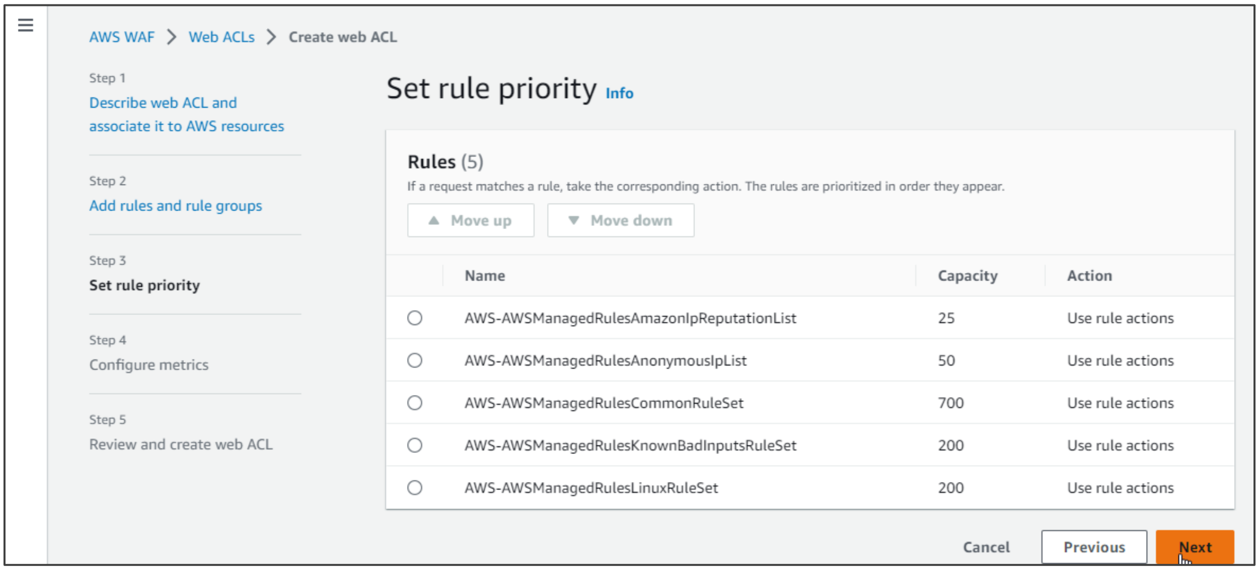
▶ **Custom request** - *optional*

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

You can add 10 more domains

2.8 In the **Set rule priority** page, click on **Next**



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 (5)

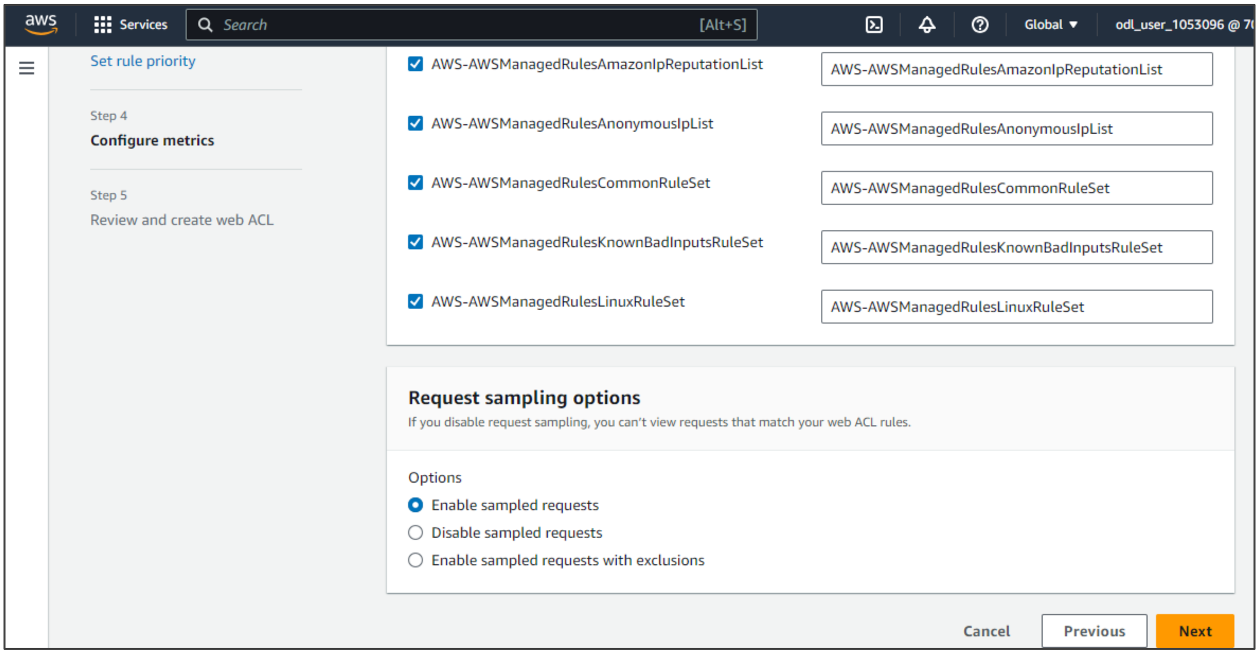
If a request matches a rule, take the corresponding action. The rules are prioritized in order they appear.

▲ Move up ▼ Move down

	Name	Capacity	Action
○	AWS-AWSManagedRulesAmazonIpReputationList	25	Use rule actions
○	AWS-AWSManagedRulesAnonymousIpList	50	Use rule actions
○	AWS-AWSManagedRulesCommonRuleSet	700	Use rule actions
○	AWS-AWSManagedRulesKnownBadInputsRuleSet	200	Use rule actions
○	AWS-AWSManagedRulesLinuxRuleSet	200	Use rule actions

Cancel Previous Next

2.9 In the **Configure metrics** page, choose **Enable sampled requests** in the **Request sampling options**, and then click on **Next**



Set rule priority

Step 4
Configure metrics

Step 5
Review and create web ACL

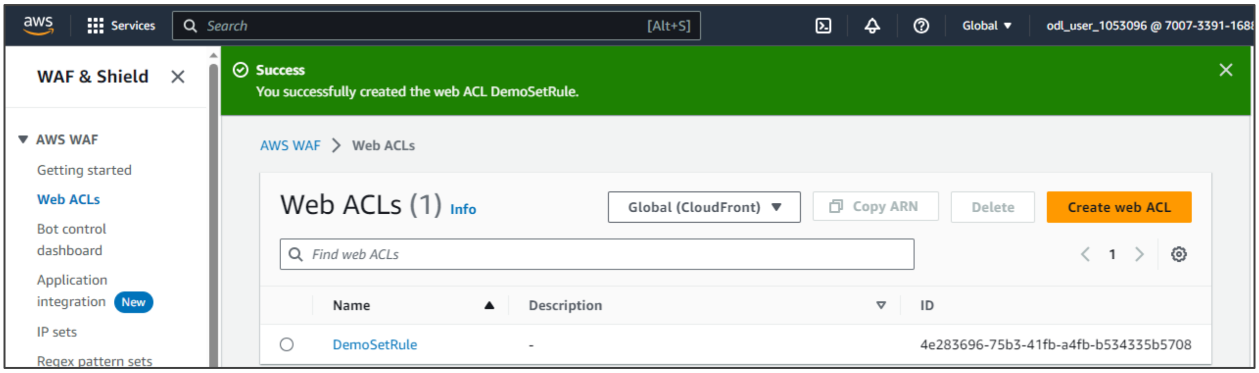
☑ AWS-AWSManagedRulesAmazonIpReputationList	AWS-AWSManagedRulesAmazonIpReputationList
☑ AWS-AWSManagedRulesAnonymousIpList	AWS-AWSManagedRulesAnonymousIpList
☑ AWS-AWSManagedRulesCommonRuleSet	AWS-AWSManagedRulesCommonRuleSet
☑ AWS-AWSManagedRulesKnownBadInputsRuleSet	AWS-AWSManagedRulesKnownBadInputsRuleSet
☑ AWS-AWSManagedRulesLinuxRuleSet	AWS-AWSManagedRulesLinuxRuleSet

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



Success
You successfully created the web ACL DemoSetRule.

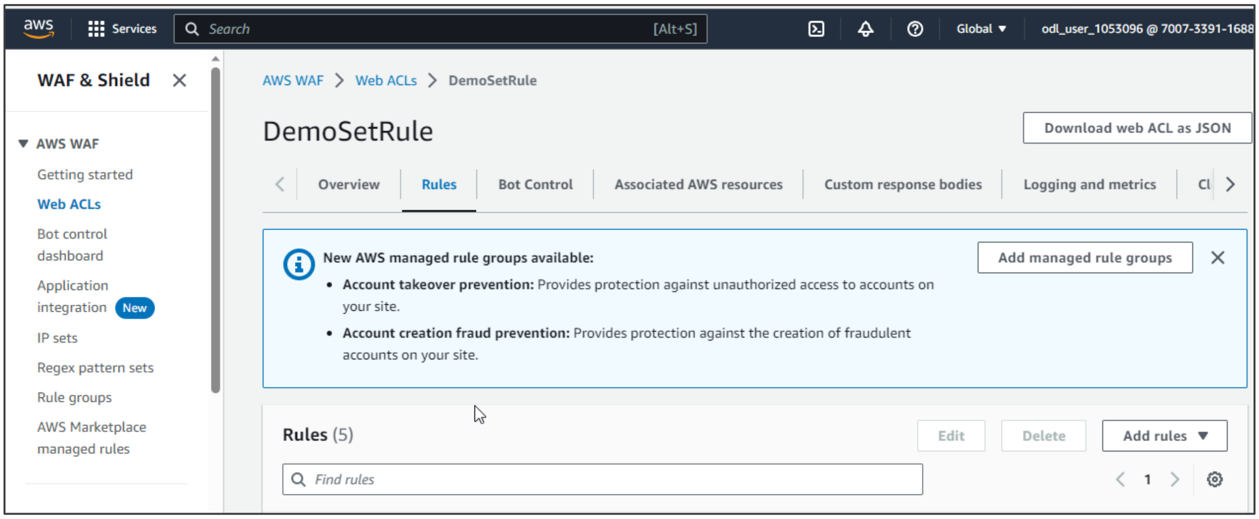
Web ACLs (1)

	Name	Description	ID
○	DemoSetRule	-	4e283696-75b3-41fb-a4fb-b534335b5708

The Web ACL has been created successfully.

Step 3: Create a custom rule in Web ACL

3.1 Select the Web ACL that you created and then click on **Rules**



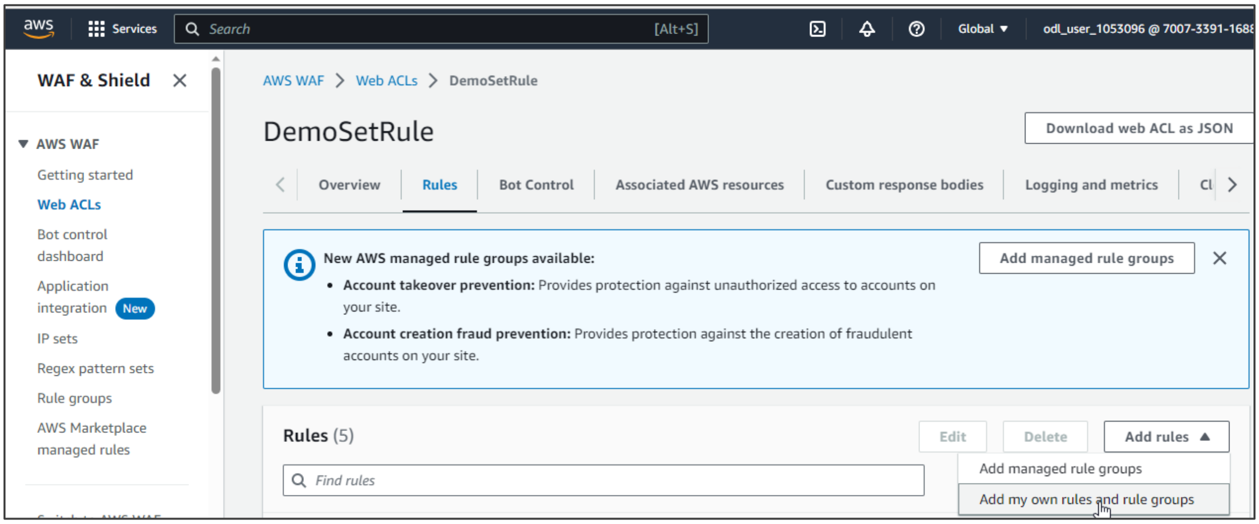
DemoSetRule

New AWS managed rule groups available:

- **Account takeover prevention:** Provides protection against unauthorized access to accounts on your site.
- **Account creation fraud prevention:** Provides protection against the creation of fraudulent accounts on your site.

Rules (5)

3.2 Select **Add my own rule and rule groups** from the **Add rules** option



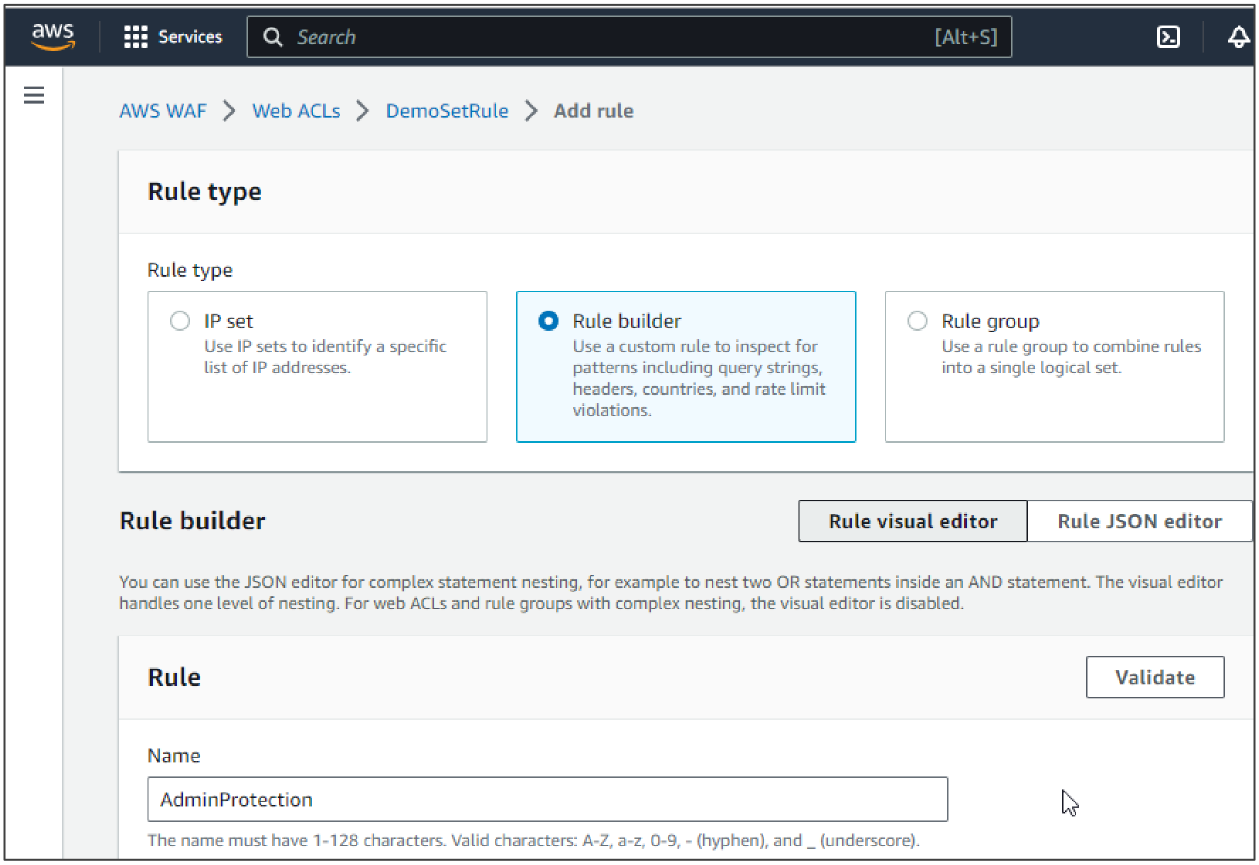
DemoSetRule

New AWS managed rule groups available:

- **Account takeover prevention:** Provides protection against unauthorized access to accounts on your site.
- **Account creation fraud prevention:** Provides protection against the creation of fraudulent accounts on your site.

Rules (5)

3.3 Select **Rule builder** in the **Rule type** option and provide a name to the 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 builder

You can use the JSON editor for complex statement nesting, for example to nest two OR statements inside an AND statement. The visual editor handles one level of nesting. For web ACLs and rule groups with complex nesting, the visual editor is disabled.

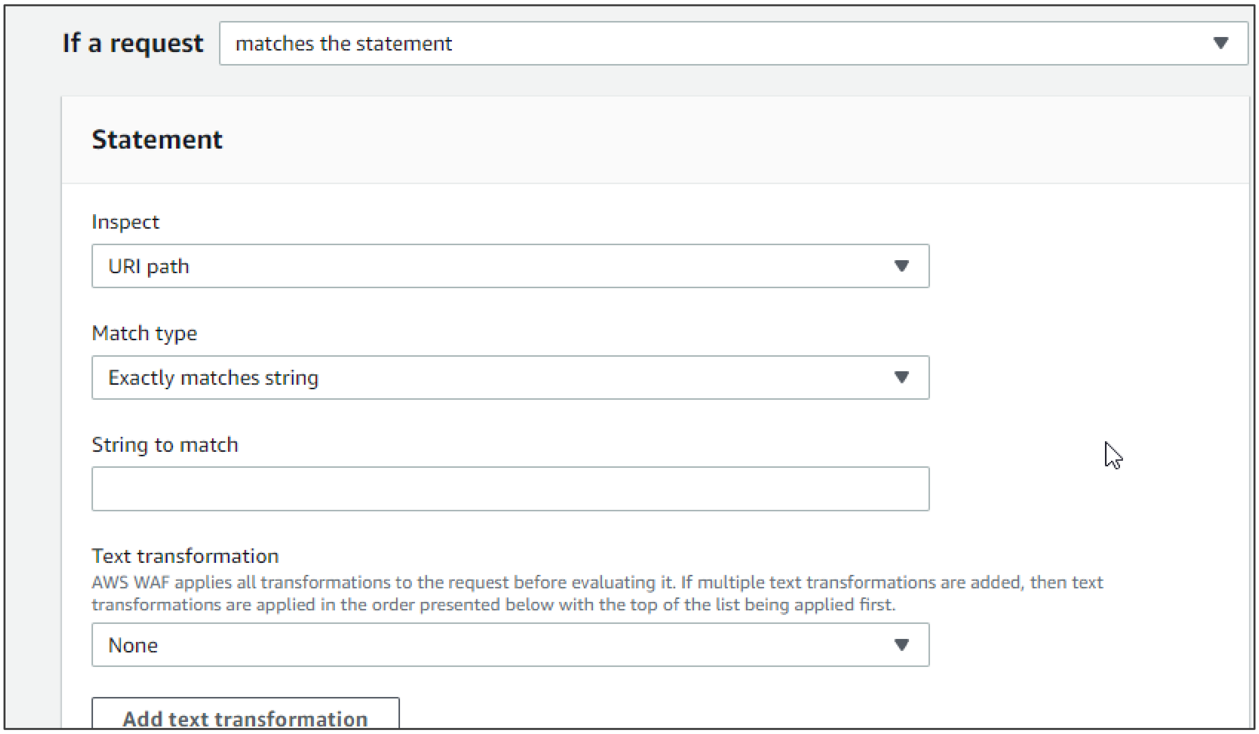
Rule

Name

AdminProtection

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

3.4 In the **Statement** page, choose **URI path** from the drop-down in the **Inspect** option and enter **Exactly matches string** from the drop-down in the **Match type** option



If a request: matches the statement

Statement

Inspect: URI path

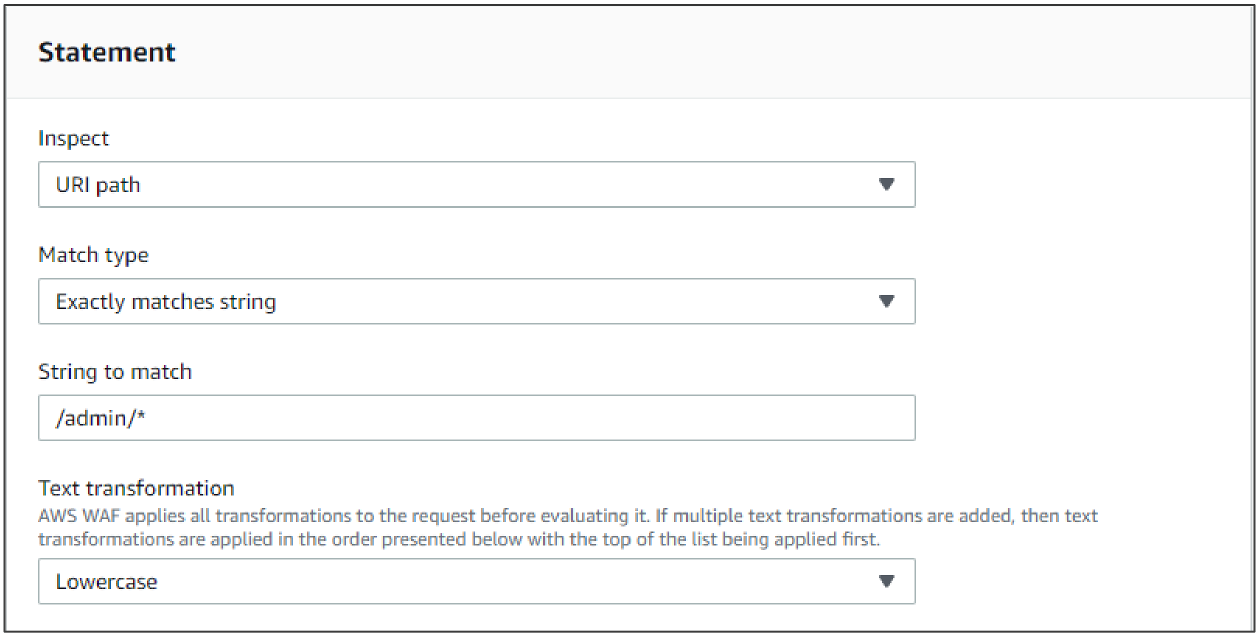
Match type: Exactly matches string

String to match:

Text transformation
AWS WAF applies all transformations to the request before evaluating it. If multiple text transformations are added, then text transformations are applied in the order presented below with the top of the list being applied first.

None

3.5 Enter **/admin/*** in the **String to match** option and choose **Lowercase** in the **Text transformation** option



Statement

Inspect: URI path

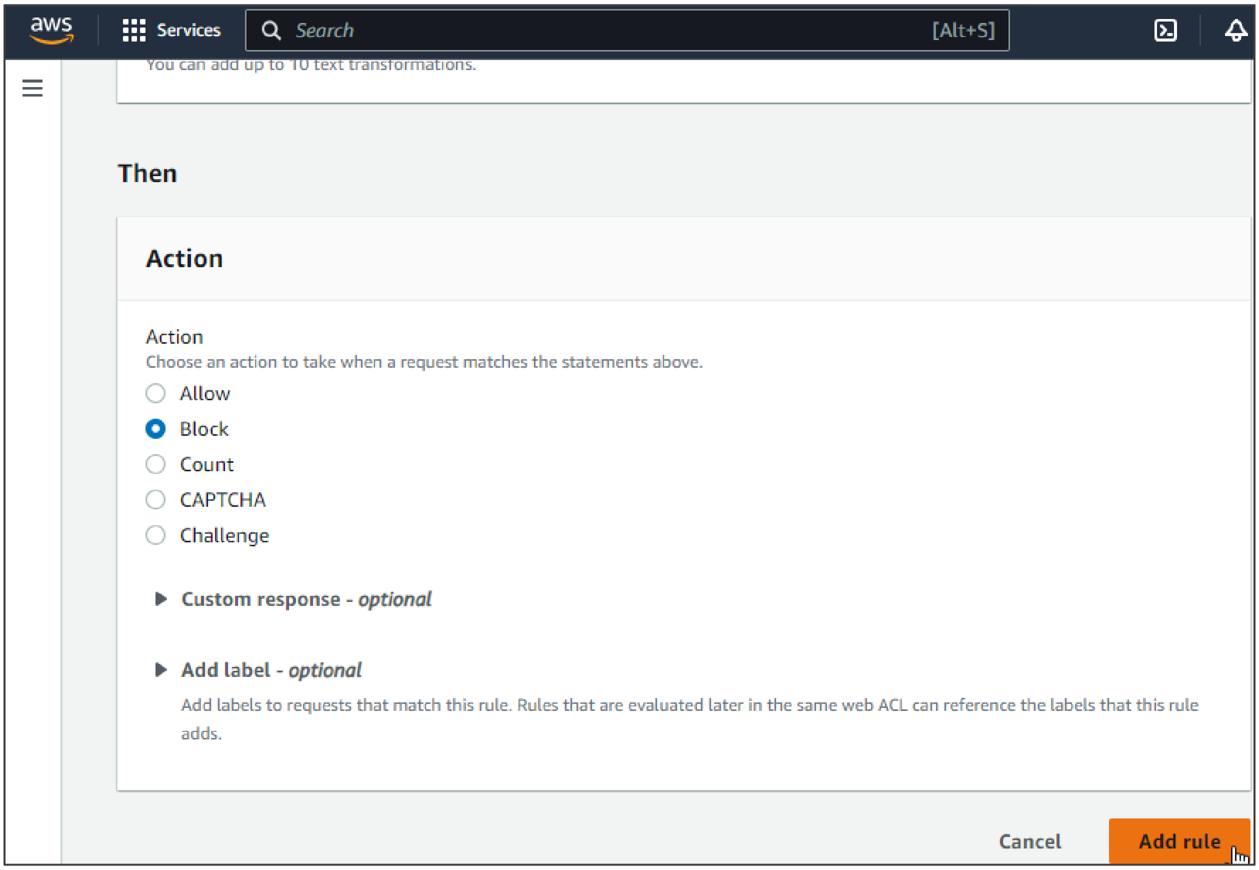
Match type: Exactly matches string

String to match: /admin/*

Text transformation
AWS WAF applies all transformations to the request before evaluating it. If multiple text transformations are added, then text transformations are applied in the order presented below with the top of the list being applied first.

Lowercase

3.6 In the **Action** option, choose **Block**, and then click on **Add rule**



You can add up to 10 text transformations.

Then

Action

Action

Choose an action to take when a request matches the statements above.

○ Allow

● Block

○ Count

○ CAPTCHA

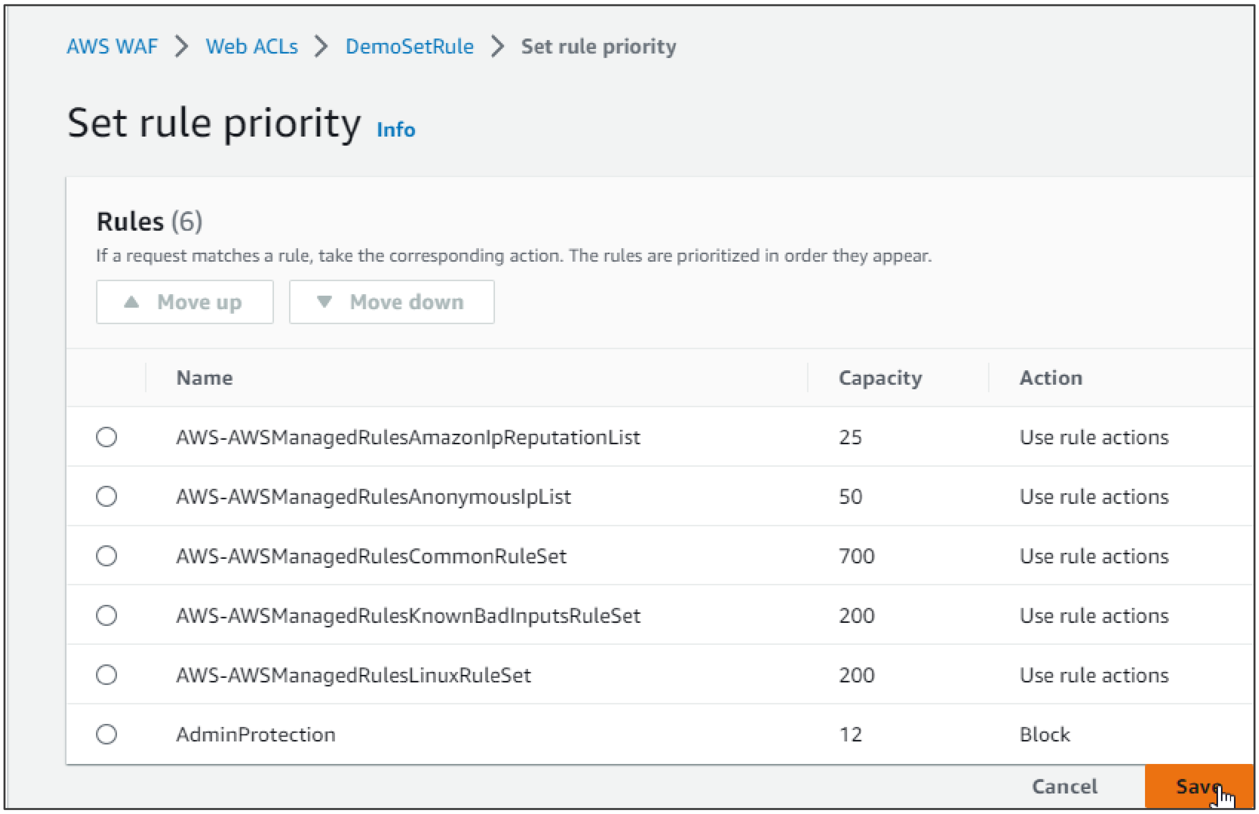
○ Challenge

▶ Custom response - *optional*

▶ Add label - *optional*

Add labels to requests that match this rule. Rules that are evaluated later in the same web ACL can reference the labels that this rule adds.

3.7 Now, click on **Save**

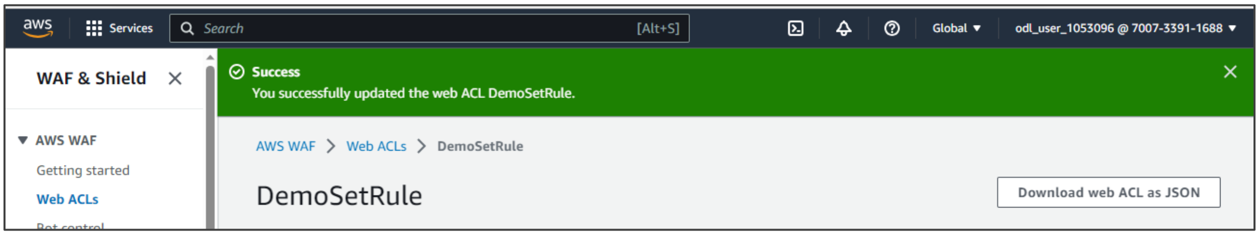


Set rule priority Info

Rules (6)

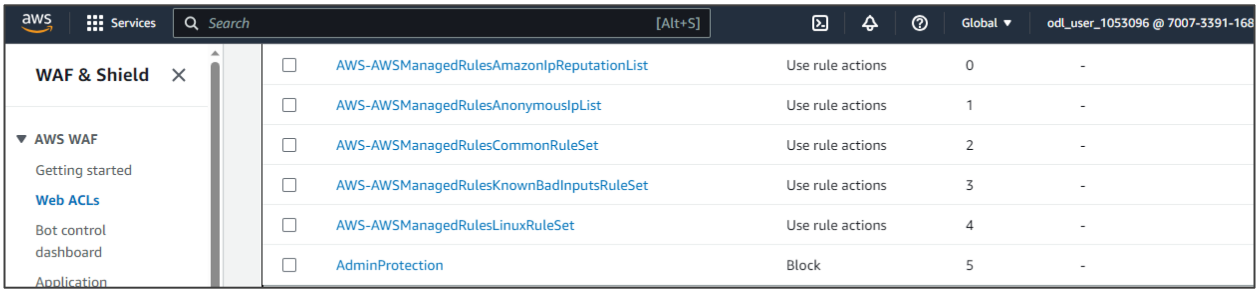
If a request matches a rule, take the corresponding action. The rules are prioritized in order they appear.

	Name	Capacity	Action
○	AWS-AWSManagedRulesAmazonIpReputationList	25	Use rule actions
○	AWS-AWSManagedRulesAnonymousIpList	50	Use rule actions
○	AWS-AWSManagedRulesCommonRuleSet	700	Use rule actions
○	AWS-AWSManagedRulesKnownBadInputsRuleSet	200	Use rule actions
○	AWS-AWSManagedRulesLinuxRuleSet	200	Use rule actions
○	AdminProtection	12	Block



Success
You successfully updated the web ACL DemoSetRule.

DemoSetRule



□	AWS-AWSManagedRulesAmazonIpReputationList	Use rule actions	0	-
□	AWS-AWSManagedRulesAnonymousIpList	Use rule actions	1	-
□	AWS-AWSManagedRulesCommonRuleSet	Use rule actions	2	-
□	AWS-AWSManagedRulesKnownBadInputsRuleSet	Use rule actions	3	-
□	AWS-AWSManagedRulesLinuxRuleSet	Use rule actions	4	-
□	AdminProtection	Block	5	-

The custom rule has been added successfully.

By following these steps, you have successfully implemented the process of creating and configuring AWS WAF.