

Lesson 07 Demo 04

Creating and Configuring AWS WAF

Objective: To configure AWS WAF to protect your web applications and APIs hosted on AWS environment

Tools required: AWS Management Console

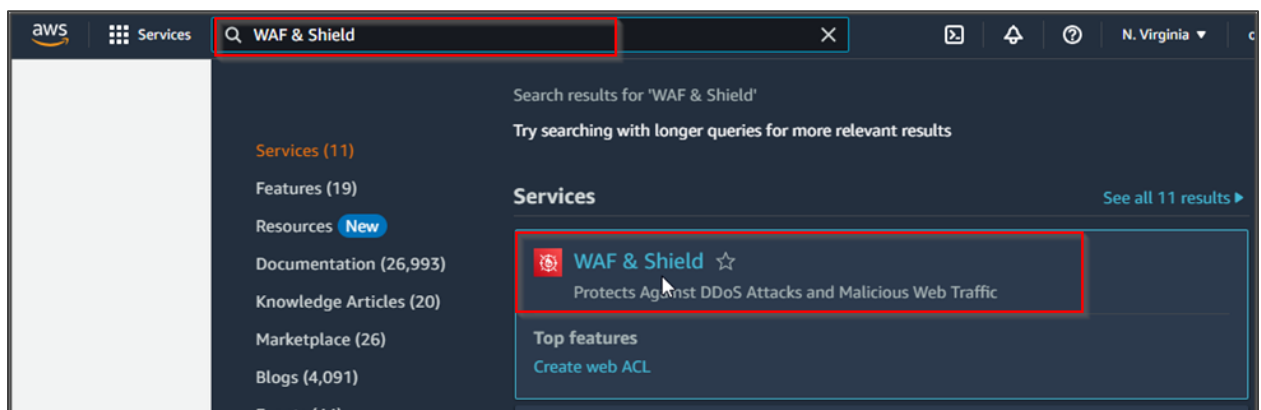
Prerequisites: None

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

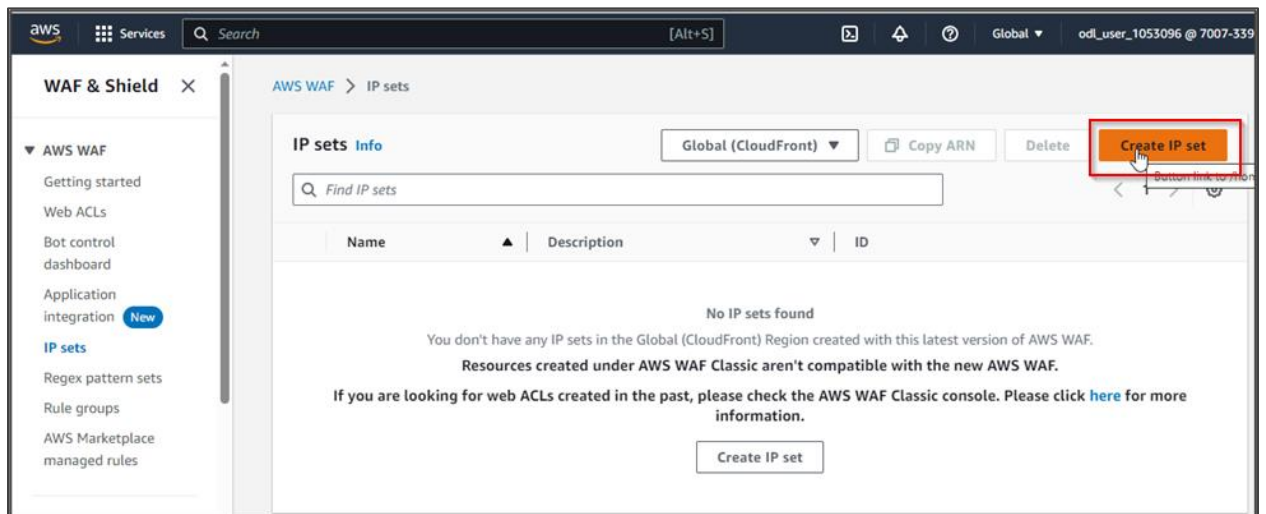
1.1 Navigate to the AWS Management Console, search for and select **WAF & Shield**



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



1.3 Click on **Create IP set**



- 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**

aws Services Search [Alt+S]

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.

Cancel Create IP set

aws Services Search [Alt+S] Global od_user_1053096 @ 7007-3391-168

WAF & Shield

Success

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

AWS WAF > IP sets

IP sets Info Global (CloudFront) Copy ARN Delete Create IP set

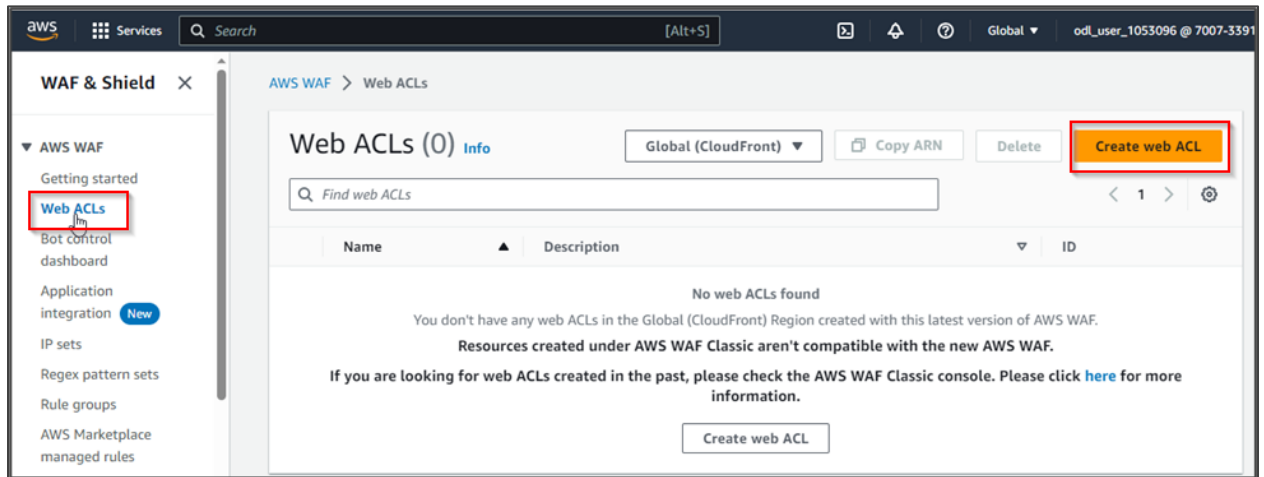
Find IP sets

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

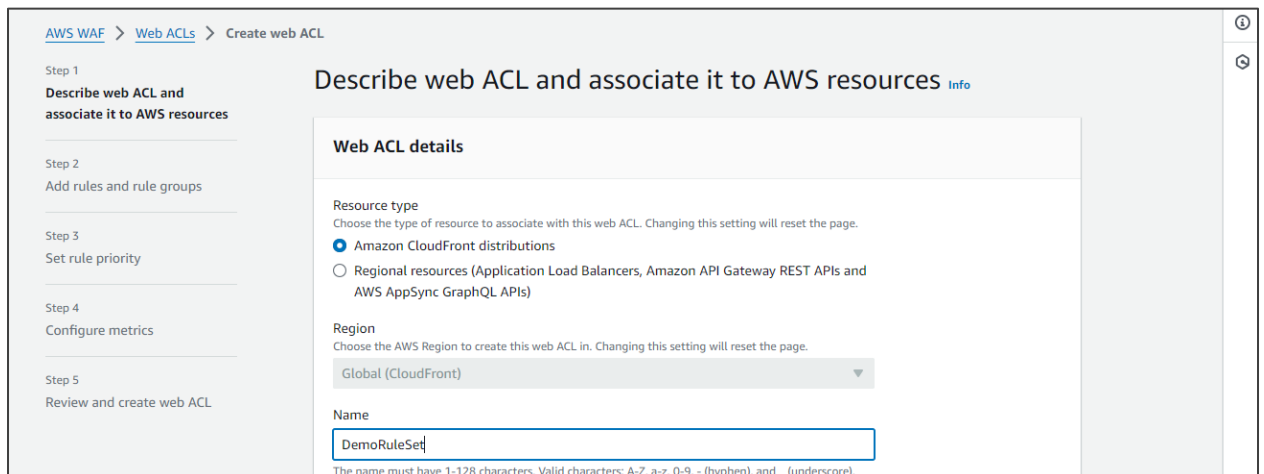
The IP set has been created successfully.

Step 2: Create Web ACL

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



2.2 Choose the **Resource type** as **Amazon CloudFront distributions**, provide a name, scroll down and click on **Next**



No items to display

Web request body inspection - optional [Info](#)

By default, rules that inspect the web request body are limited to the first 16 KB of content. You can increase this size for additional costs. [AWS WAF Pricing](#)

Body size limit
The AWS WAF default limit is 16 KB. Settings over 16 KB incur additional costs. [Learn more](#)

CloudFront distributions

☒ Default

☐ 16 KB

☐ 32 KB

☐ 48 KB

☐ 64 KB

[Cancel](#)
[Next](#)

2.3 In the **Add rules and rule groups** page, click on **Add rules** and 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) [Edit](#) [Delete](#)

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

	Name	Capacity	Action
<p>No rules.</p> <p>You don't have any rules added.</p>			

Add rules ▲

Add managed rule groups

Add my own rules and rule groups

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

[AWS WAF](#) > [Web ACLs](#) > Create web ACL

Step 1
[Describe web ACL and associate it to AWS resources](#)

Step 2
Add managed rule groups

Step 3
Set rule priority

Step 4
Configure metrics

Step 5
Review and create web ACL

Add managed rule groups [Info](#)

Managed rule groups are created and maintained for you by AWS and AWS Marketplace sellers. Any fees that a managed rule group provider charges for using a managed rule group are in addition to the standard service charges for AWS WAF. [AWS WAF Pricing](#)

▼ **AWS managed rule groups**

Paid rule groups

AWS WAF charges subscription and usage fees for paid managed rule groups. These are in addition to the standard service charges for AWS WAF. [AWS WAF Pricing](#)

Name	Capacity	Additional fees	Action
Account creation fraud prevention - new Provides protection against the creation of fraudulent accounts on your site. Fraudulent accounts can be used for activities such as	50	See pricing details	<input type="checkbox"/> Add to web ACL

aws Services [Alt+S] Global od_user_1053096 @

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	<input type="checkbox"/> 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	<input checked="" type="checkbox"/> 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	<input checked="" type="checkbox"/> 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	<input checked="" type="checkbox"/> Add to web ACL Edit

aws Services Search [Alt+S]				Global	odl_user_1053096 @
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	<input type="radio"/> 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	<input checked="" type="radio"/> Add to web ACL <input type="button" value="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	<input checked="" type="radio"/> Add to web ACL <input type="button" value="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	<input checked="" type="radio"/> Add to web ACL <input type="button" value="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	<input checked="" type="radio"/> Add to web ACL <input type="button" value="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 More	200	<input checked="" type="radio"/> Add to web ACL <input type="button" value="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

aws Services Search [Alt+S]				Global	odl_user_1053096 @
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	<input type="radio"/> 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	<input checked="" type="radio"/> Add to web ACL <input type="button" value="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	<input checked="" type="radio"/> Add to web ACL <input type="button" value="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	<input checked="" type="radio"/> Add to web ACL <input type="button" value="Edit"/>			

Override all rule actions

Override to Count

Remove all overrides

<div>GenericRFI_URI_PATH_RC_COUNT</div> <div>Rule action: Count</div> <div>Override to Count</div>	<div>GenericRFI_BODY_RC_COUNT</div> <div>Rule action: Count</div> <div>Override to Count</div>	<div>GenericRFI_QUERYARGUMENTS_RC_COUNT</div> <div>Rule action: Count</div> <div>Override to Count</div>
<div>RestrictedExtensions_QUERYARGUMENTS_RC_COUNT</div> <div>Rule action: Count</div> <div>Override to Count</div>	<div>RestrictedExtensions_URI_PATH_RC_COUNT</div> <div>Rule action: Count</div> <div>Override to Count</div>	<div>GenericRFI_BODY_RC_COUNT</div> <div>Rule action: Count</div> <div>Override to Count</div>
<div>GenericRFI_URI_PATH_RC_COUNT</div> <div>Rule action: Count</div> <div>Override to Count</div>	<div>GenericRFI_QUERYARGUMENTS_RC_COUNT</div> <div>Rule action: Count</div> <div>Override to Count</div>	<div>EC2MetadataSSRF_QUERYARGUMENTS_RC_COUNT</div> <div>Rule action: Count</div> <div>Override to Count</div>
<div>EC2MetadataSSRF_URI_PATH_RC_COUNT</div> <div>Rule action: Count</div> <div>Override to Count</div>	<div>EC2MetadataSSRF_COOKIE_RC_COUNT</div> <div>Rule action: Count</div> <div>Override to Count</div>	<div>EC2MetadataSSRF_BODY_RC_COUNT</div> <div>Rule action: Count</div> <div>Override to Count</div>
<div>UserAgent_BadBots_HEADER_RC_COUNT</div> <div>Rule action: Count</div> <div>Override to Count</div>	<div>NoUserAgent_HEADER</div> <div>Rule action: Block</div>	<div>UserAgent_BadBots_HEADER</div> <div>Rule action: Block</div>

2.6 Click on **Save rule**

► Override rule group action - optional

Cancel

Save rule

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

<input checked="" type="checkbox"/> AWS-AWSManagedRulesAmazonIpReputationList	AWS-AWSManagedRulesAmazonIpReputationList
<input checked="" type="checkbox"/> AWS-AWSManagedRulesAnonymousIpList	AWS-AWSManagedRulesAnonymousIpList
<input checked="" type="checkbox"/> AWS-AWSManagedRulesCommonRuleSet	AWS-AWSManagedRulesCommonRuleSet
<input checked="" type="checkbox"/> AWS-AWSManagedRulesKnownBadInputsRuleSet	AWS-AWSManagedRulesKnownBadInputsRuleSet
<input checked="" type="checkbox"/> 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**

2.10 Review the settings, scroll down and click on **Create web ACL**

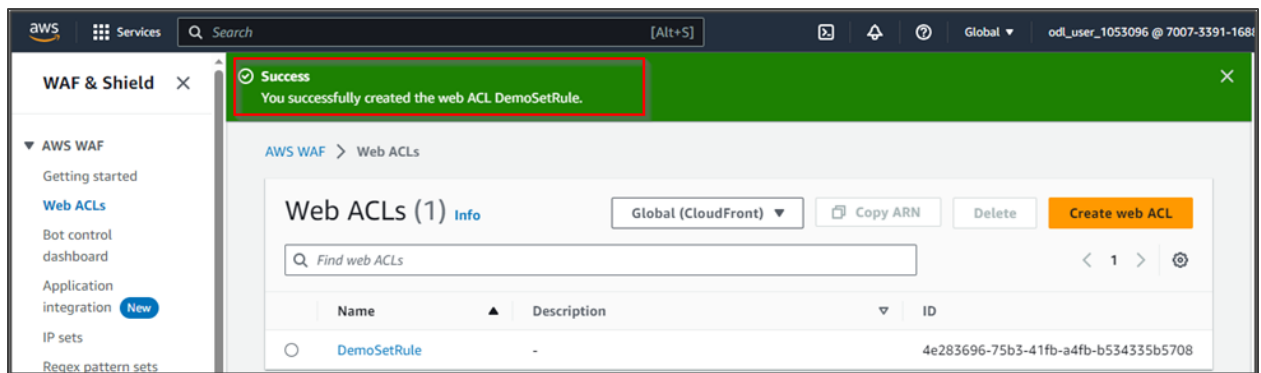
Amazon CloudWatch metrics (5)

Rules	CloudWatch metric name
AWS-AWSManagedRulesAmazonIpReputationList	AWS-AWSManagedRulesAmazonIpReputationList
AWS-AWSManagedRulesAnonymousIpList	AWS-AWSManagedRulesAnonymousIpList
AWS-AWSManagedRulesCommonRuleSet	AWS-AWSManagedRulesCommonRuleSet
AWS-AWSManagedRulesKnownBadInputsRuleSet	AWS-AWSManagedRulesKnownBadInputsRuleSet
AWS-AWSManagedRulesLinuxRuleSet	AWS-AWSManagedRulesLinuxRuleSet

Sampled requests

Sampled requests	Sampled requests for web ACL default actions
Enabled	Enabled

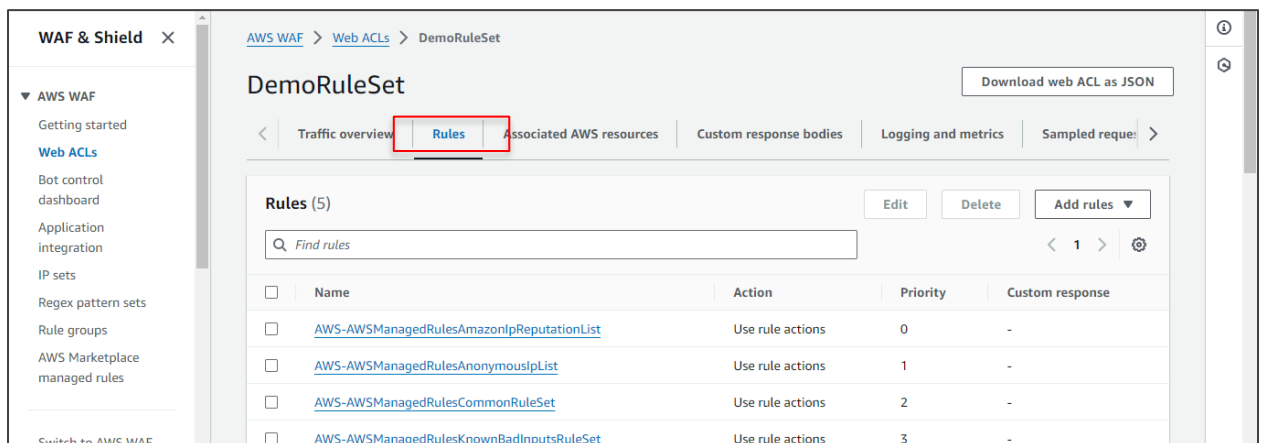
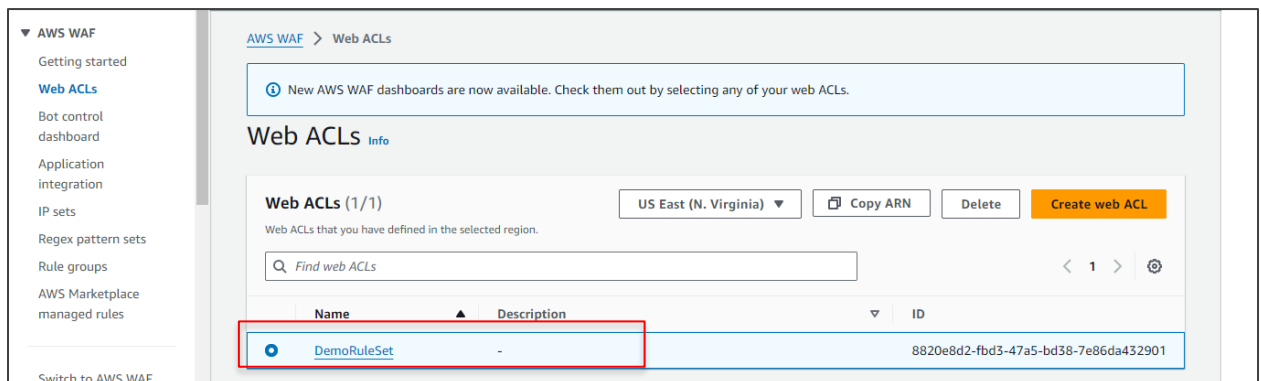
Cancel Previous **Create web ACL**



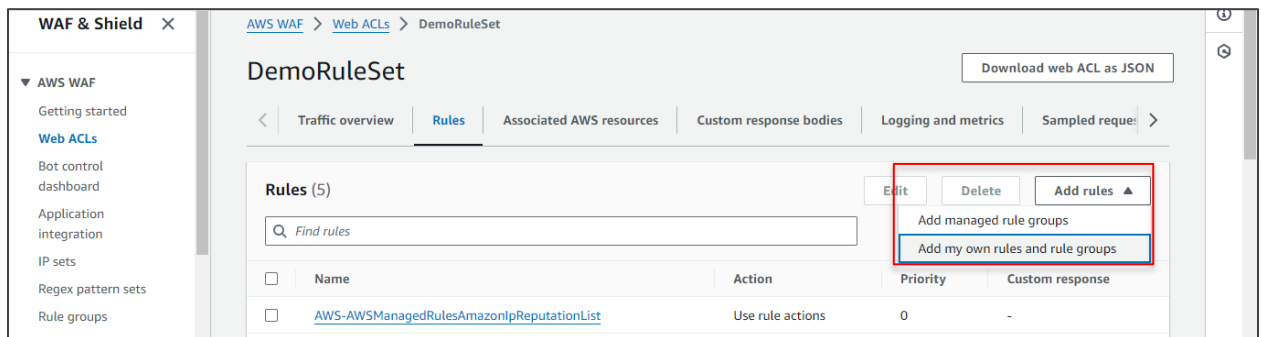
The Web ACL has been successfully created.

Step 3: Create a custom rule in Web ACL

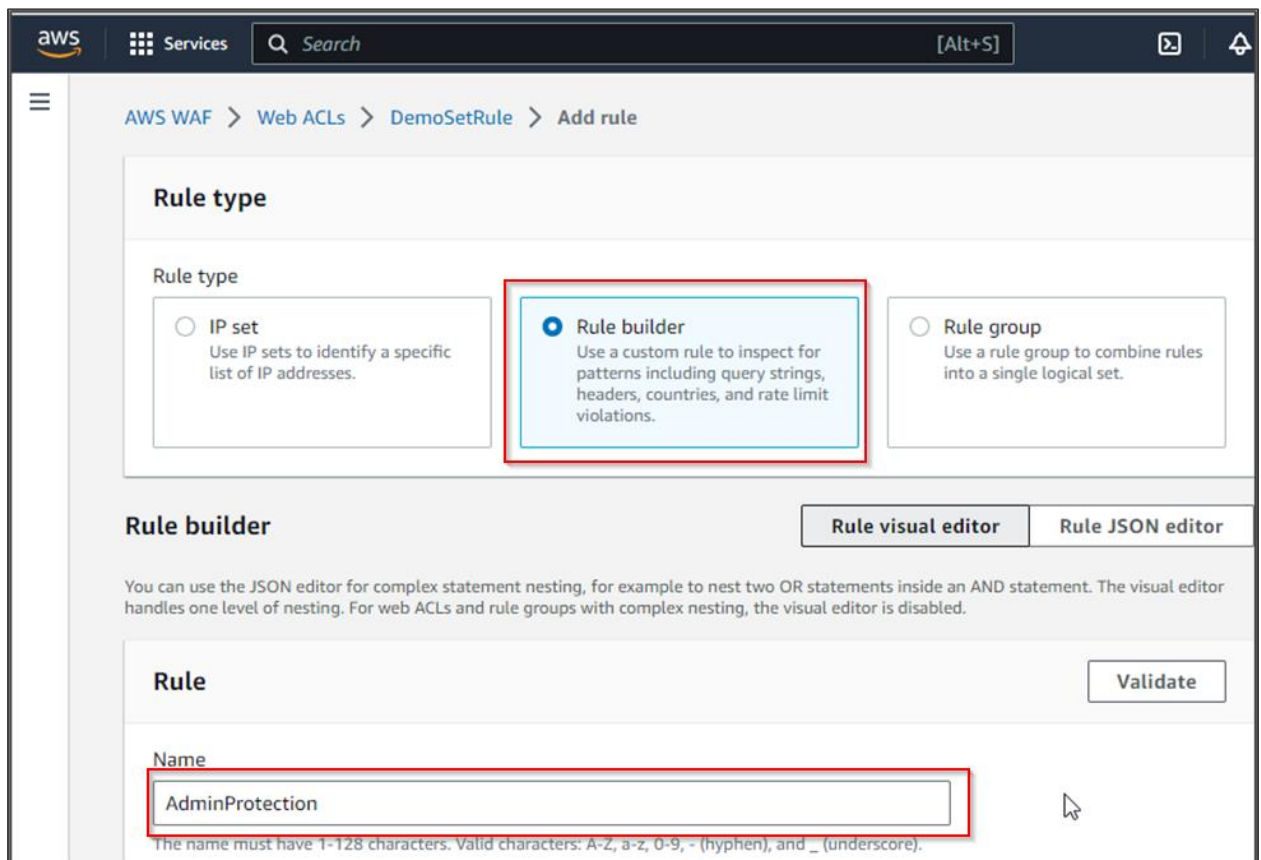
3.1 Select the Web ACL that you created and then click on **Rules**



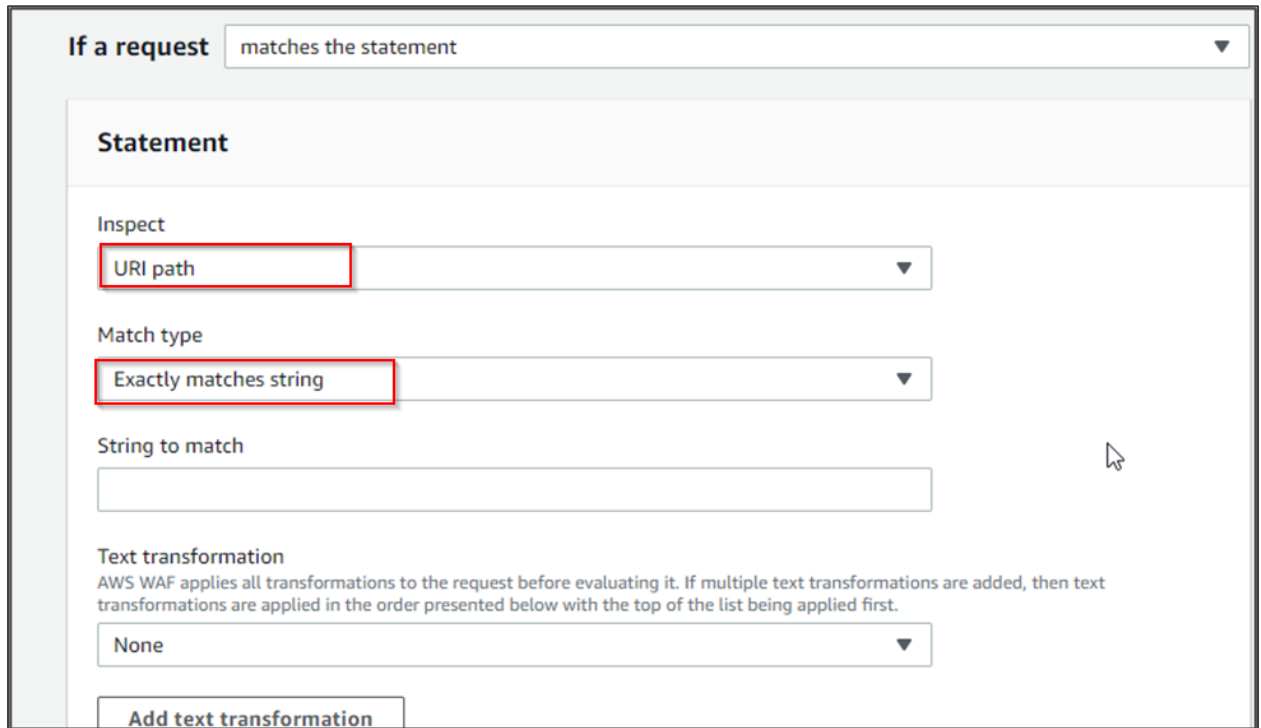
3.2 Click on **Add rules** and select **Add my own rule and rule groups**



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



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



If a request matches the statement ▼

Statement

Inspect
URI path ▼

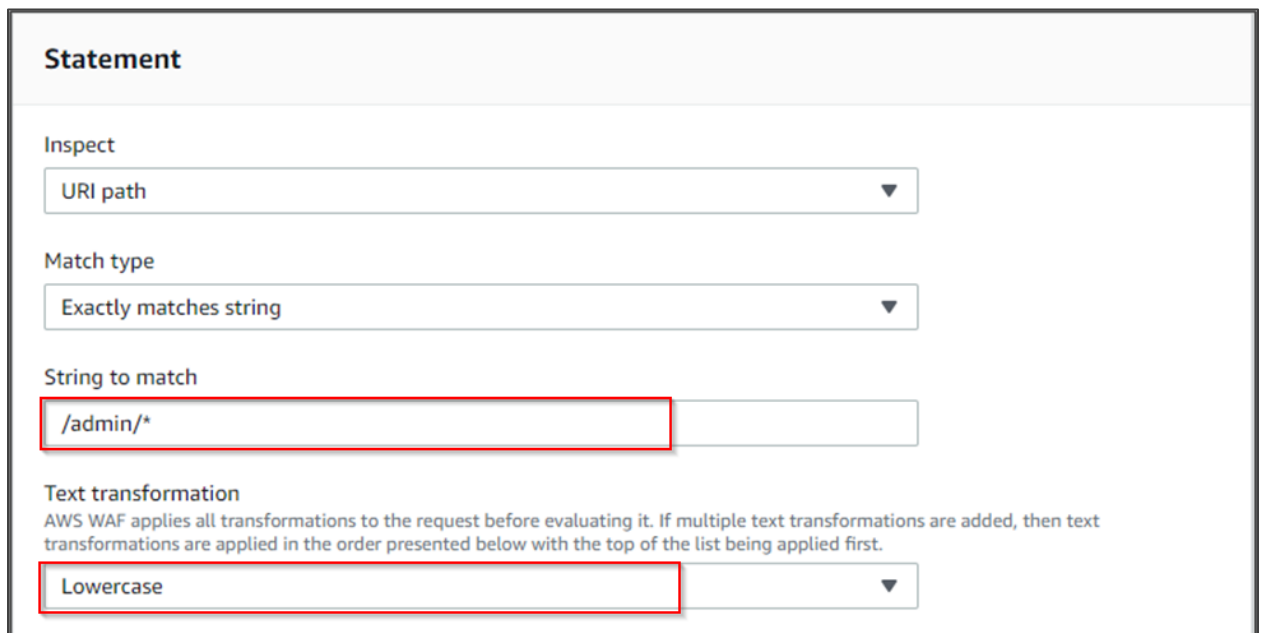
Match type
Exactly matches string ▼

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 ▼

[Add text transformation](#)

- 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**

aws Services Search [Alt+S]

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.

Cancel Add rule

3.7 Click on **Save**

AWS WAF > Web ACLs > DemoSetRule > Set rule priority

Set rule priority [Info](#)

Rules (6)
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
<input type="radio"/>	AWS-AWSManagedRulesAmazonIpReputationList	25	Use rule actions
<input type="radio"/>	AWS-AWSManagedRulesAnonymousIpList	50	Use rule actions
<input type="radio"/>	AWS-AWSManagedRulesCommonRuleSet	700	Use rule actions
<input type="radio"/>	AWS-AWSManagedRulesKnownBadInputsRuleSet	200	Use rule actions
<input type="radio"/>	AWS-AWSManagedRulesLinuxRuleSet	200	Use rule actions
<input type="radio"/>	AdminProtection	12	Block

Cancel **Save**

aws Services Search [Alt+S] Global odl_user_1053096 @ 7007-3391-1688

WAF & Shield ×

Success
You successfully updated the web ACL DemoSetRule.

AWS WAF > Web ACLs > DemoSetRule

DemoSetRule

Download web ACL as JSON

aws Services Search [Alt+S] Global odl_user_1053096 @ 7007-3391-1688

WAF & Shield ×

AWS WAF
Getting started
Web ACLs
Bot control dashboard
Application

<input type="checkbox"/>	AWS-AWSManagedRulesAmazonIpReputationList	Use rule actions	0	-
<input type="checkbox"/>	AWS-AWSManagedRulesAnonymousIpList	Use rule actions	1	-
<input type="checkbox"/>	AWS-AWSManagedRulesCommonRuleSet	Use rule actions	2	-
<input type="checkbox"/>	AWS-AWSManagedRulesKnownBadInputsRuleSet	Use rule actions	3	-
<input type="checkbox"/>	AWS-AWSManagedRulesLinuxRuleSet	Use rule actions	4	-
<input type="checkbox"/>	AdminProtection	Block	5	-

The custom rule has been successfully added.

By following these steps, you have successfully configured AWS WAF to protect your web applications and APIs hosted on AWS environment.