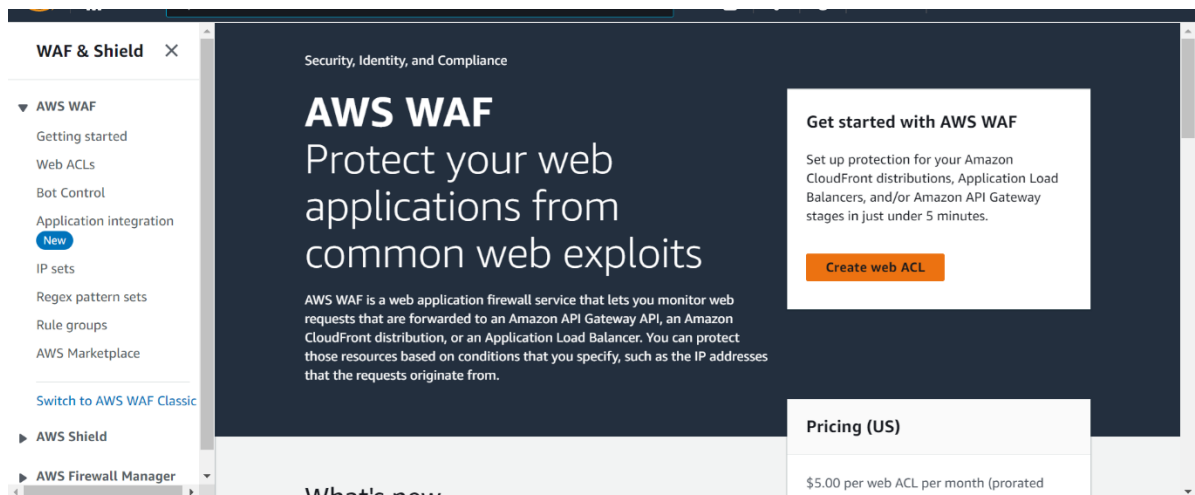


AWS APPLICATION WAF

- ❖ **WAF AWS** monitors all the web incoming and outgoing requests that are forwarded to API Gateway, Amazon CloudFront, and Application Load Balancer. We will see how to get started with WAF and create web ACL in some steps.
- ✓ **Create web ACL:** First, [sign-up](#) for an AWS account, then go to AWS Console and search for Web Application Firewall. You will land on the WAF home page, and choose to **Create Web ACL**.



- ✓ **Give a Name:** Type the name you want to use to identify this web ACL. After that, enter Description if you want (optional) and then hit **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

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

Web ACL details

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

Description - optional
for training purpose
The description can have 1-256 characters.

CloudWatch metric name
test-waf
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)

Region
Choose the AWS region to create this web ACL in.

Step 5
Review and create web ACL

CloudWatch metric name
test-waf
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)

Region
Choose the AWS region to create this web ACL in.
Global (CloudFront)

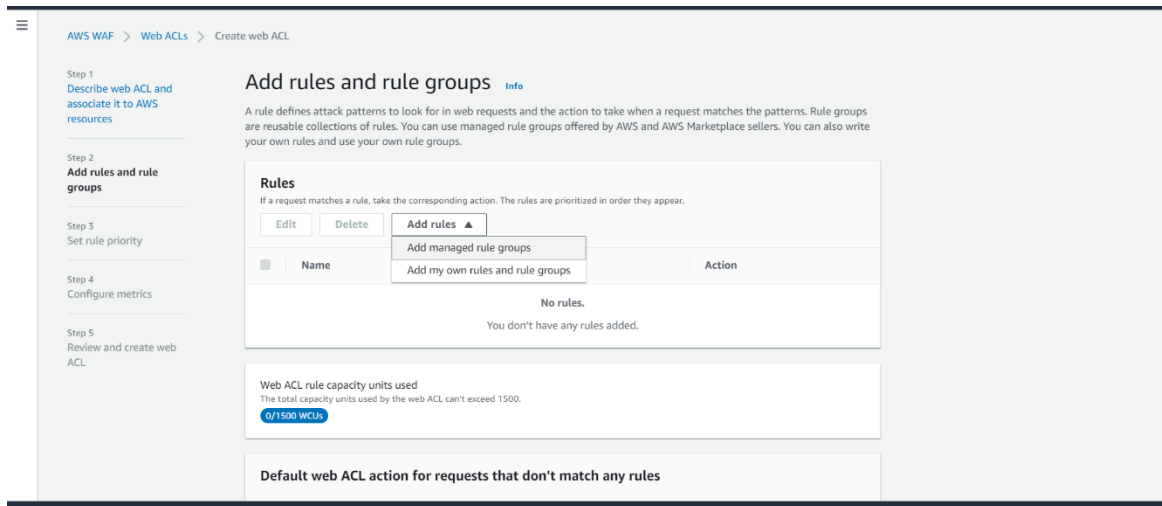
Associated AWS resources - optional [Remove](#) [Add AWS resources](#)

< 1 >

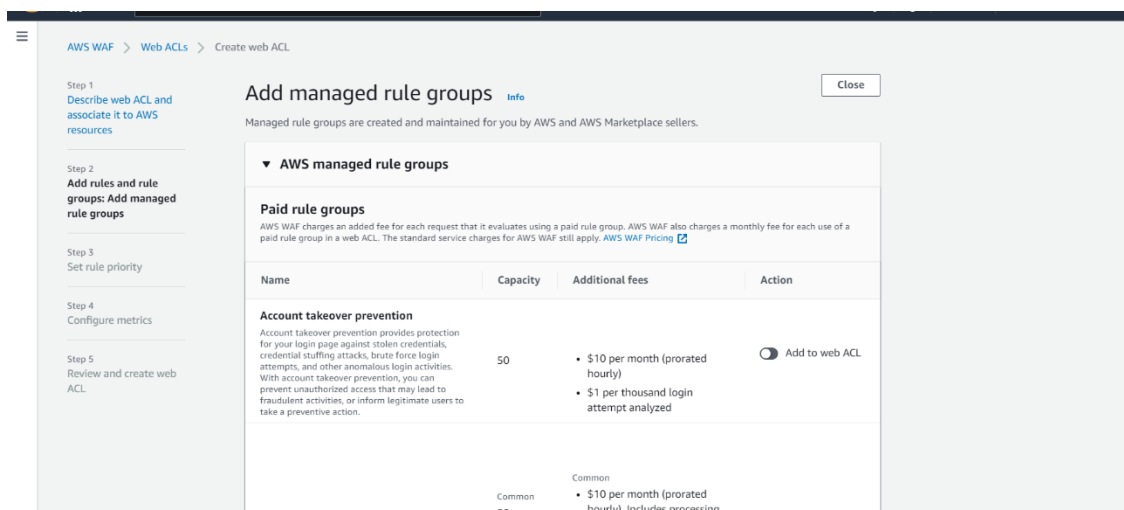
	Name	Resource type	Region
No results There are no results to display			

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

- ✓ **Add an AWS Managed Rules rule group:** In the next step, you need to add rules and rule groups. Click on **Add managed rule groups**. You will land on a new page to manage the ruling group.



- ✓ AWS Managed Rules provides you with a collection of managed rule groups. The majority of these are free for Amazon WAF users. After adding managed rule group, choose to save the rule



- ✓ The rules we're going to create will define the patterns we want to allow/block. We'll add 2 rules only.
 - ◆ **Regular rule:** This rule protects the application from SQL injection attacks. It will check if the URI path contains an SQL injection.
 - ◆ **Rate-based rule:** This rule blocks the requests made from the same IP address after they exceed a certain limit in a time period.

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	<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.	25	<input type="radio"/> Add to web ACL
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	<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.	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.	200	<input type="radio"/> Add to web ACL
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	<input type="radio"/> Add to web ACL

✓ Click on ADD RULES.

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

- ▶ Cloudbric Corp. managed rule groups
- ▶ Cyber Security Cloud Inc. managed rule groups
- ▶ F5 managed rule groups
- ▶ Fortinet managed rule groups
- ▶ GeoGuard managed rule groups
- ▶ Imperva managed rule groups
- ▶ ThreatSTOP managed rule groups

Cancel

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.

<input type="checkbox"/>	Name	Capacity	Action
<input type="checkbox"/>	AWS-AWSManagedRulesAnonymousIpList	50	Use rule actions
<input type="checkbox"/>	AWS-AWSManagedRulesCommonRuleSet	700	Use rule actions

Web ACL rule capacity units used
The total capacity units used by the web ACL can't exceed 1500.

750/1500 WCLUs

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

✓ After that, check the added rules and hit **Next**

Step 5
Review and create web ACL

AWS-AWSManagedRulesCommonRuleSet700Use rule actions

Web ACL rule capacity units used

The total capacity units used by the web ACL can't exceed 1500.

750/1500 WCU

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](#)

Add token domain

You can add 10 more domains

Cancel

Previous

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

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-AWSManagedRulesAnomymousIpList	50	Use rule actions
<input type="radio"/>	AWS-AWSManagedRulesCommonRuleSet	700	Use rule actions

Cancel

Previous

Next

✓ Configure CloudWatch Metrics:

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"/> AWS-AWSManagedRulesAnomymousIpList	AWS-AWSManagedRulesAnomymousIpList
<input checked="" type="checkbox"/> AWS-AWSManagedRulesCommonRuleSet	AWS-AWSManagedRulesCommonRuleSet

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

✓ Review Web ACL Configuration:

In the final step, check all the rules and managed groups and hit on create web ACL.

The screenshot shows the 'Review and create web ACL' page in the AWS WAF console. The left sidebar contains a navigation menu with steps: 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), and Step 5 (Review and create web ACL). The main content area is titled 'Review and create web ACL' and includes an 'Info' link. It is divided into two sections: 'Step 1: Describe web ACL and associate it to AWS resources' and 'Steps 2 and 3: Add rules and set rule priority'. The 'Web ACL details' section shows the Name 'test-waf', Description 'for training purpose', CloudWatch metric name 'test-waf', Scope 'CLOUDFRONT', and Region 'global'. The 'Rules' section shows a table with columns 'Name', 'Capacity', and 'Action'. The table contains two rows: 'AWS-AWSManagedRulesAnonymousList' with a capacity of 50 and action 'Use rule actions', and 'AWS-AWSManagedRulesCommonRuleSet' with a capacity of 300 and action 'Use rule actions'.

Step 1: Describe web ACL and associate it to AWS resources

Web ACL details

Name	test-waf	Scope	CLOUDFRONT
Description	for training purpose	Region	global
CloudWatch metric name	test-waf		

Steps 2 and 3: Add rules and 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-AWSManagedRulesAnonymousList	50	Use rule actions
AWS-AWSManagedRulesCommonRuleSet	300	Use rule actions

The screenshot shows the 'Configure metrics' step in the AWS WAF console. The left sidebar contains a navigation menu with steps: 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), and Step 5 (Review and create web ACL). The main content area is titled 'Configure metrics' and includes an 'Edit' link. It is divided into two sections: 'Amazon CloudWatch metrics' and 'Sampled requests'. The 'Amazon CloudWatch metrics' section shows a table with columns 'Rules' and 'CloudWatch metric name'. The table contains two rows: 'AWS-AWSManagedRulesAnonymousList' with metric name 'AWS-AWSManagedRulesAnonymousList', and 'AWS-AWSManagedRulesCommonRuleSet' with metric name 'AWS-AWSManagedRulesCommonRuleSet'. The 'Sampled requests' section shows a table with columns 'Sampled requests' and 'Sampled requests for web ACL default actions'. The table contains two rows: 'Enabled' and 'Enabled'. At the bottom, there are buttons for 'Cancel', 'Previous', and 'Create web ACL'.

Step 4: Configure metrics

Amazon CloudWatch metrics

Rules	CloudWatch metric name
AWS-AWSManagedRulesAnonymousList	AWS-AWSManagedRulesAnonymousList
AWS-AWSManagedRulesCommonRuleSet	AWS-AWSManagedRulesCommonRuleSet

Sampled requests

Sampled requests	Sampled requests for web ACL default actions
Enabled	Enabled

Cancel Previous Create web ACL

The screenshot shows the AWS WAF console 'Web ACLs' page. The left sidebar contains a navigation menu with 'AWS WAF' and 'Web ACLs' (highlighted). The main content area is titled 'Web ACLs' and includes an 'Info' link. It shows a table with columns 'Name', 'Description', and 'ID'. The table contains one row: 'test-waf' with description 'for training purpose' and ID '161aab06-a16b-48e5-8222-454a0c97cd04'. At the top, there are buttons for 'Global (CloudFront)', 'Copy ARN', 'Delete', and 'Create web ACL'. At the bottom, there is a button for 'Switch to AWS WAF Classic'.

WAF & Shield

Success

You successfully created the web ACL: test-waf.

AWS WAF > Web ACLs

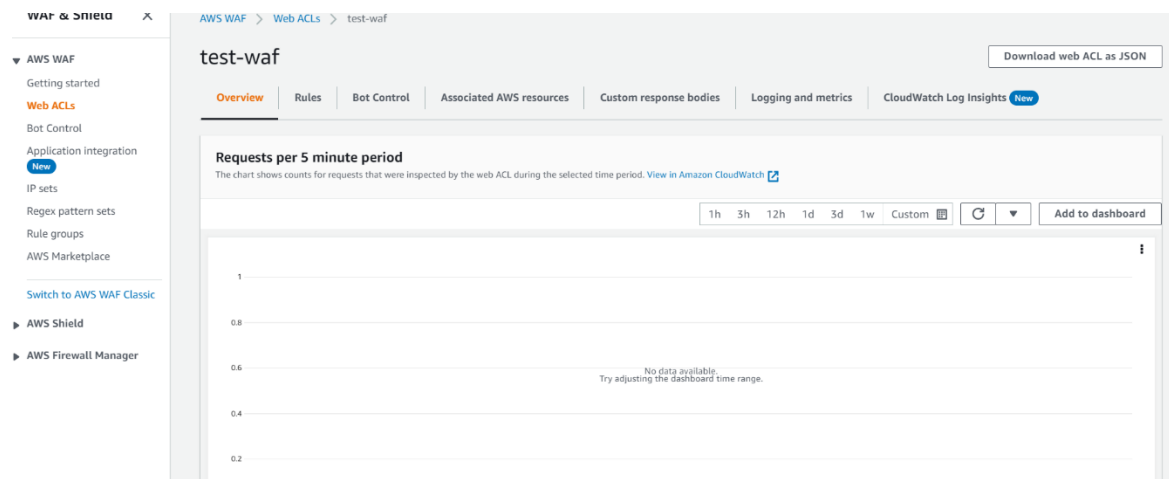
Web ACLs

Global (CloudFront) Copy ARN Delete Create web ACL

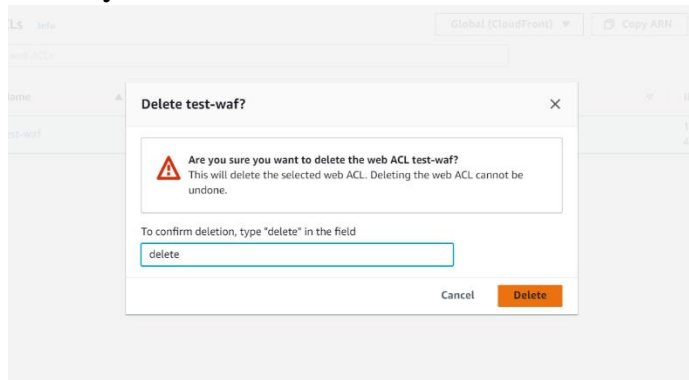
Find web ACLs

Name	Description	ID
test-waf	for training purpose	161aab06-a16b-48e5-8222-454a0c97cd04

Switch to AWS WAF Classic



✓ Once you done with the resources remember to delete them.



END