Secure First
Then Connect

cloudbric

Cloudbric Rule Set for AWS WAF Setting Guide v1.1 2023.05

FOR ENDUSER(PUBLIC)

CHANGE HISTORY

Date	Author	Revision Description	Page no.	Comment
2022.12	Park. Junhyung	Initial documentation		v 1.0
2023.05	Park. Junhyung	Added details regarding the Rule override using Labels.	15, 17, 22, 26	v 1.1

CONTENTS

1. Overview

This document was made to explain how to subscribe to「Cloudbric Rule Set」, the Managed Rule for AWS WAF, listed in AWS Marketplace by Cloudbric Corp., and how to add the Rule Set to the Web ACL.

What is Managed Rule Group of AWS Marketplace?

Cloudbric Rule Set is an AWS WAF Managed Rules developed by Cloudbric. Cloudbric is the first and only AWS WAF Ready Program Launch Partner of South Korea that has passed the strict technical evaluations of Amazon Web Services (AWS). Cloudbric Rule Set was developed based on the technical capabilities of Cloudbric's core team which is consisted of some of the best security experts in the field with over 20 years of experience and is continuously updated and managed to maintain a stable level of security.

1.1 Cloudbric Rule Set Overview:

Cloudbric Rule Set is a threat intelligence-based Managed Rule Groups for AWS WAF, able to be extensively applied for IP reputation list and OWASP Top 10 protection.

Cloudbric Rule Set was developed based on expert knowledge of Cloudbric's core team with over 20 years of experience and technology accumulated over 16 years by a company specializing in security. Cloudbric Rule Set is continuously updated and maintained by security experts through Threat DB provided by Cloudbric Labs and latest attack trends research to promptly detect new security threats and maintain stable security.

1.2 Cloudbric Rule Set Types:

Name	Details
OWASP Top 10 Rule Set *Continue to Subscribe*	Based on Cloudbric's logic engine which has the leading market share in the APAC market for five consecutive years, The intelligent logic-based rules analyze millions of traffic and detect abnormal patterns and behaviors defined by the OWASP Top 10 Vulnerabilities such as SQL injections and Cross-site scripting (XSS).
Malicious IP Reputation Rule Set *Continue to Subscribe*	Provides a list of IPs with a high threat index compiled by Cloudbric Labs via analyzing data collected from over 700,000 sites in 95 countries over a daily basis to reduce the time it takes to detect various threats and proactively block high-risk IPs.

2. How to configure Cloudbric Rule Set

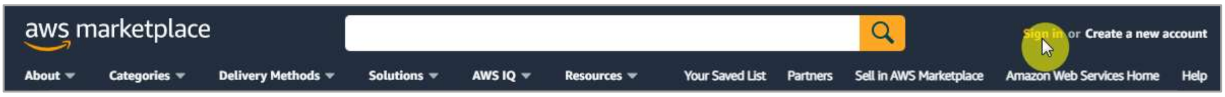
You must subscribe to Cloudbric Rule Set through AWS Marketplace prior to configuring the Cloudbric Rule Set for AWS WAF. Cloudbric Rule Set can be added to the Web ACL on the AWS WAF console after the subscription.

2.1 Subscribing to Cloudbric Rule Set

- **Step 1**

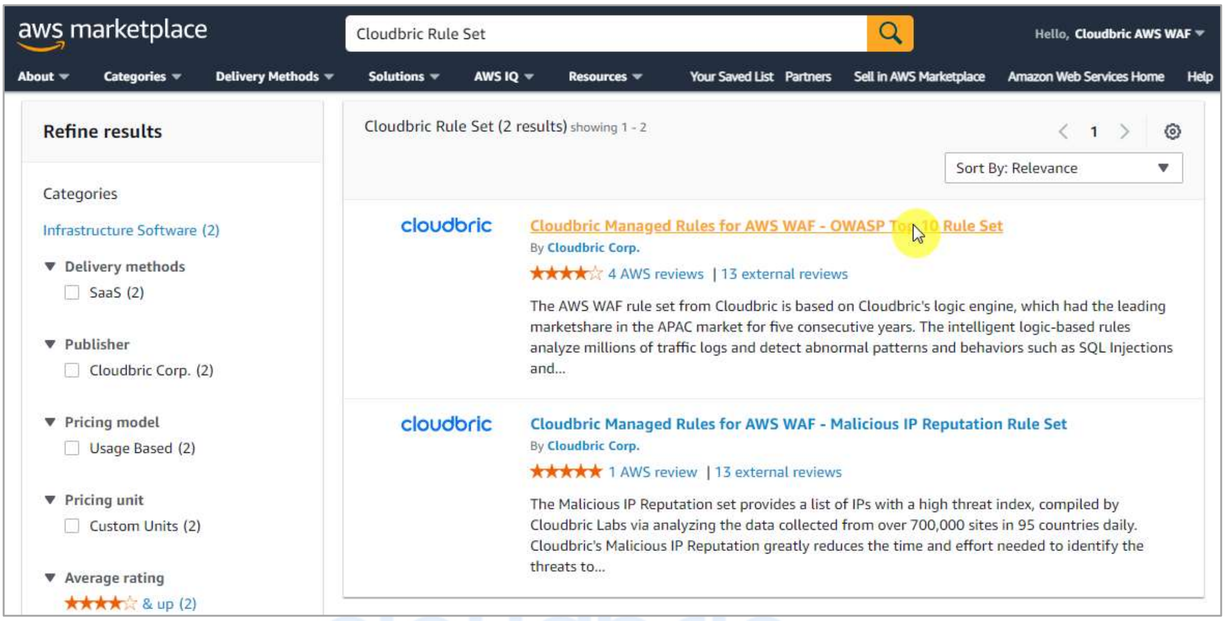
  Log in with AWS account in AWS Marketplace.

  ※ *AWS Marketplace:* https://aws.amazon.com/marketplace/



- **Step 2**

  Search for **'Cloudbric Rule Set'** and select the name of the product to subscribe.



Cloudbric Rule Set

Cloudbric Rule Set (2 results) showing 1 - 2

Sort By: Relevance

Refine results

Categories
Infrastructure Software (2)

Delivery methods
□ SaaS (2)

Publisher
□ Cloudbric Corp. (2)

Pricing model
□ Usage Based (2)

Pricing unit
□ Custom Units (2)

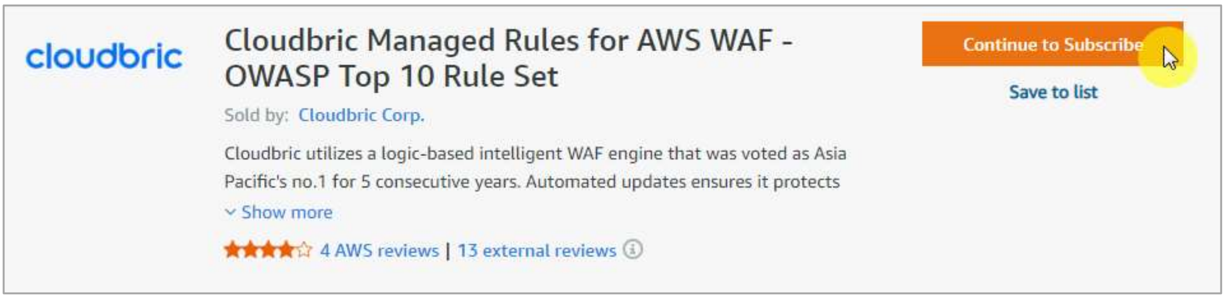
Average rating
★★★★☆ & up (2)

Cloudbric Managed Rules for AWS WAF - OWASP Top 10 Rule Set
By Cloudbric Corp.
★★★★☆ 4 AWS reviews | 13 external reviews
The AWS WAF rule set from Cloudbric is based on Cloudbric's logic engine, which had the leading marketshare in the APAC market for five consecutive years. The intelligent logic-based rules analyze millions of traffic logs and detect abnormal patterns and behaviors such as SQL Injections and...

Cloudbric Managed Rules for AWS WAF - Malicious IP Reputation Rule Set
By Cloudbric Corp.
★★★★★ 1 AWS review | 13 external reviews
The Malicious IP Reputation set provides a list of IPs with a high threat index, compiled by Cloudbric Labs via analyzing the data collected from over 700,000 sites in 95 countries daily. Cloudbric's Malicious IP Reputation greatly reduces the time and effort needed to identify the threats to...

- **Step 3**

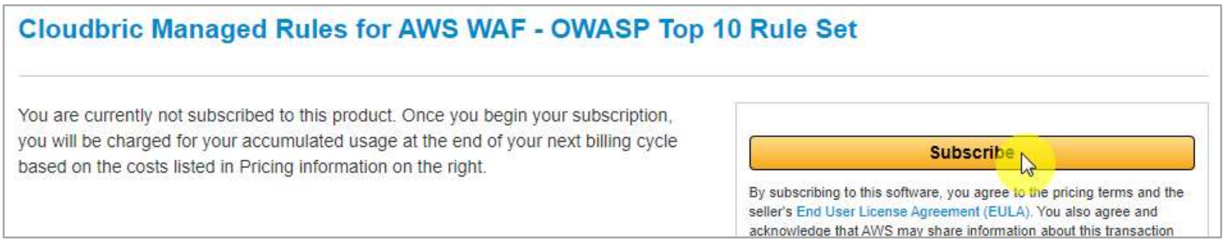
  Go over the details of the selected product, then select **[Continue to Subscribe]**.



Cloudbric Managed Rules for AWS WAF - OWASP Top 10 Rule Set
Sold by: Cloudbric Corp.
Cloudbric utilizes a logic-based intelligent WAF engine that was voted as Asia Pacific's no.1 for 5 consecutive years. Automated updates ensures it protects
★★★★☆ 4 AWS reviews | 13 external reviews

- **Step 4**

  Go over the terms and pricing information, then select **[Subscribe]** to complete the subscription.



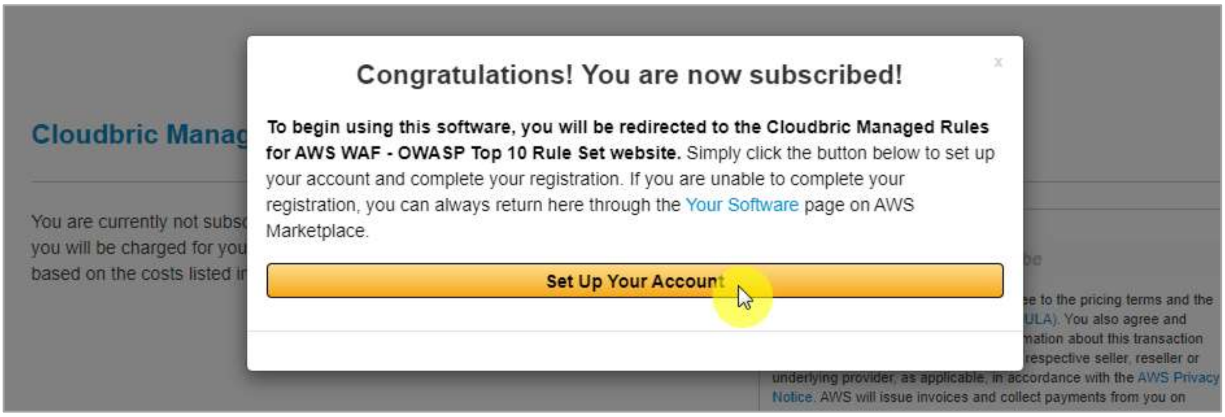
Cloudbric Managed Rules for AWS WAF - OWASP Top 10 Rule Set

You are currently not subscribed to this product. Once you begin your subscription, you will be charged for your accumulated usage at the end of your next billing cycle based on the costs listed in Pricing information on the right.

By subscribing to this software, you agree to the pricing terms and the seller's End User License Agreement (EULA). You also agree and acknowledge that AWS may share information about this transaction

- **Step 5**

  You are now subscribed to Cloudbric Rule Set. To use Cloudbric Rule Set, select **[Set Up Your Account]** and go to AWS WAF console.



Congratulations! You are now subscribed!

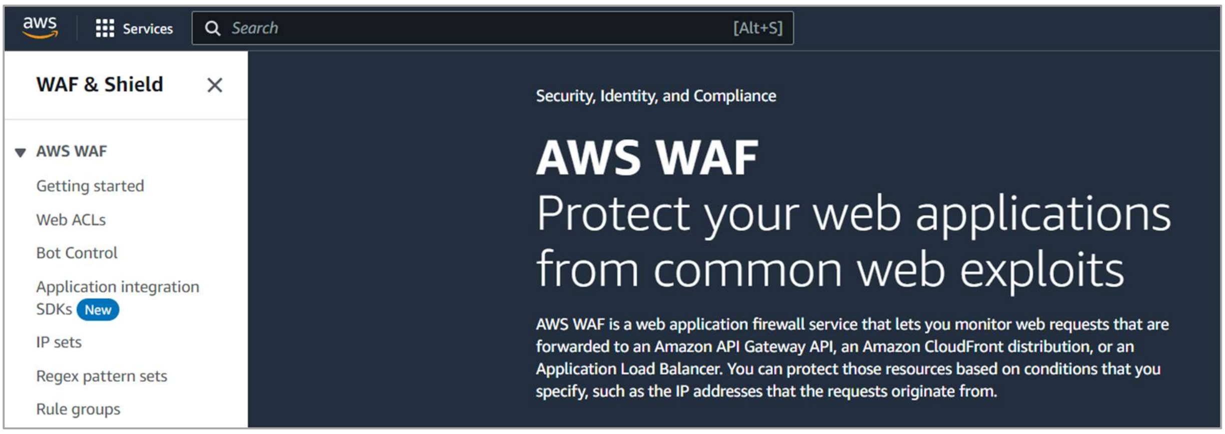
To begin using this software, you will be redirected to the Cloudbric Managed Rules for AWS WAF - OWASP Top 10 Rule Set website. Simply click the button below to set up your account and complete your registration. If you are unable to complete your registration, you can always return here through the Your Software page on AWS Marketplace.

2.2 Adding Cloudbric Rule Set

- **Step 1**

  Go to AWS WAF console.

  ※ *AWS WAF console :* https://console.aws.amazon.com/wafv2/



Security, Identity, and Compliance

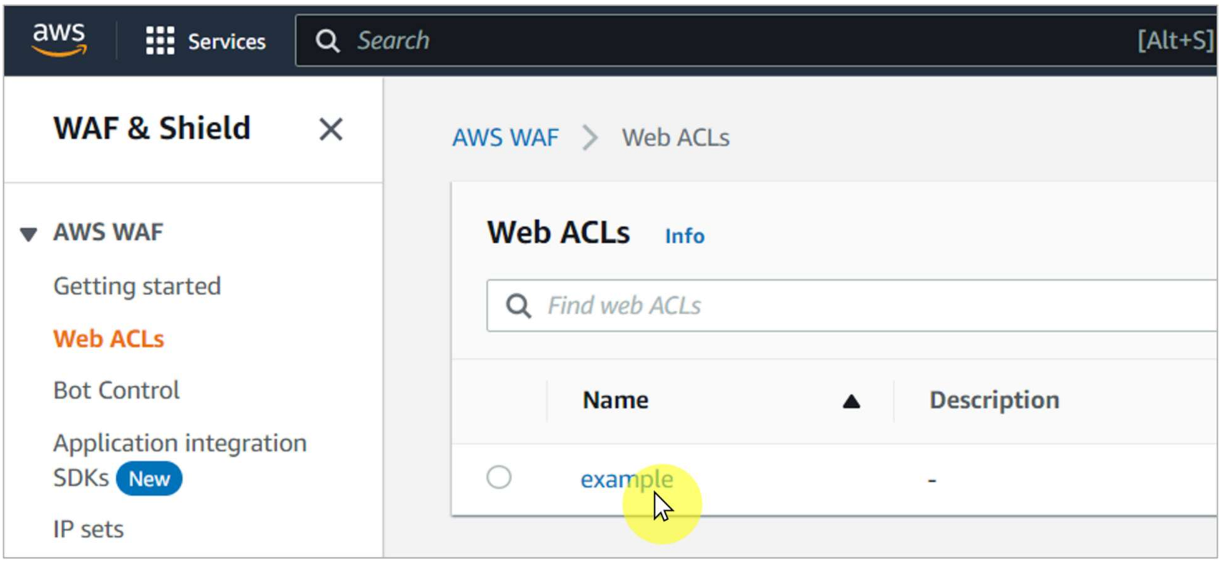
AWS WAF

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.

- **Step 2**

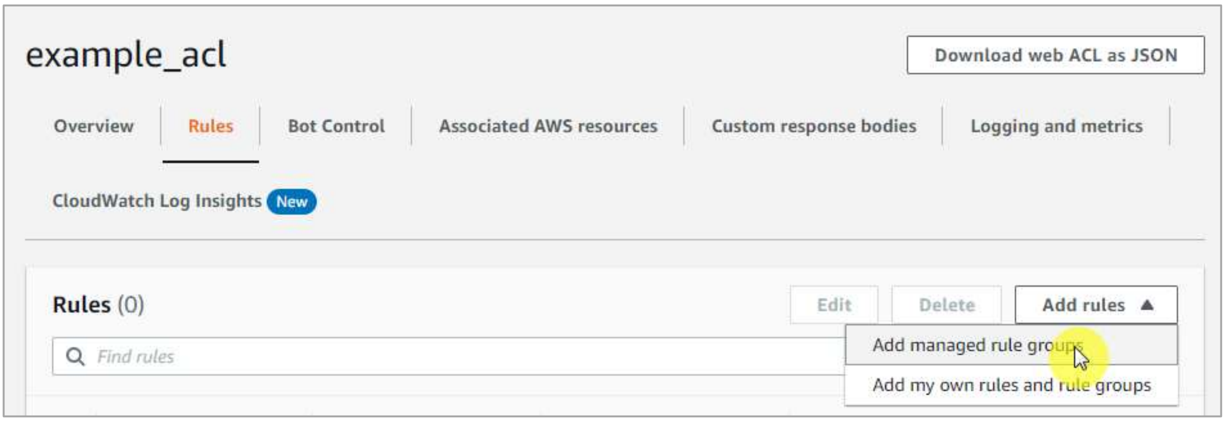
  Go to the Web ACL menu and select the Web ACL to add the Cloudbric Rule Set.



	Name	Description
○	example	-

- **Step 3**

  Select the **[Rules]** tab and select **[Add managed rule group]** from the **[Add rules]** drop down menu.



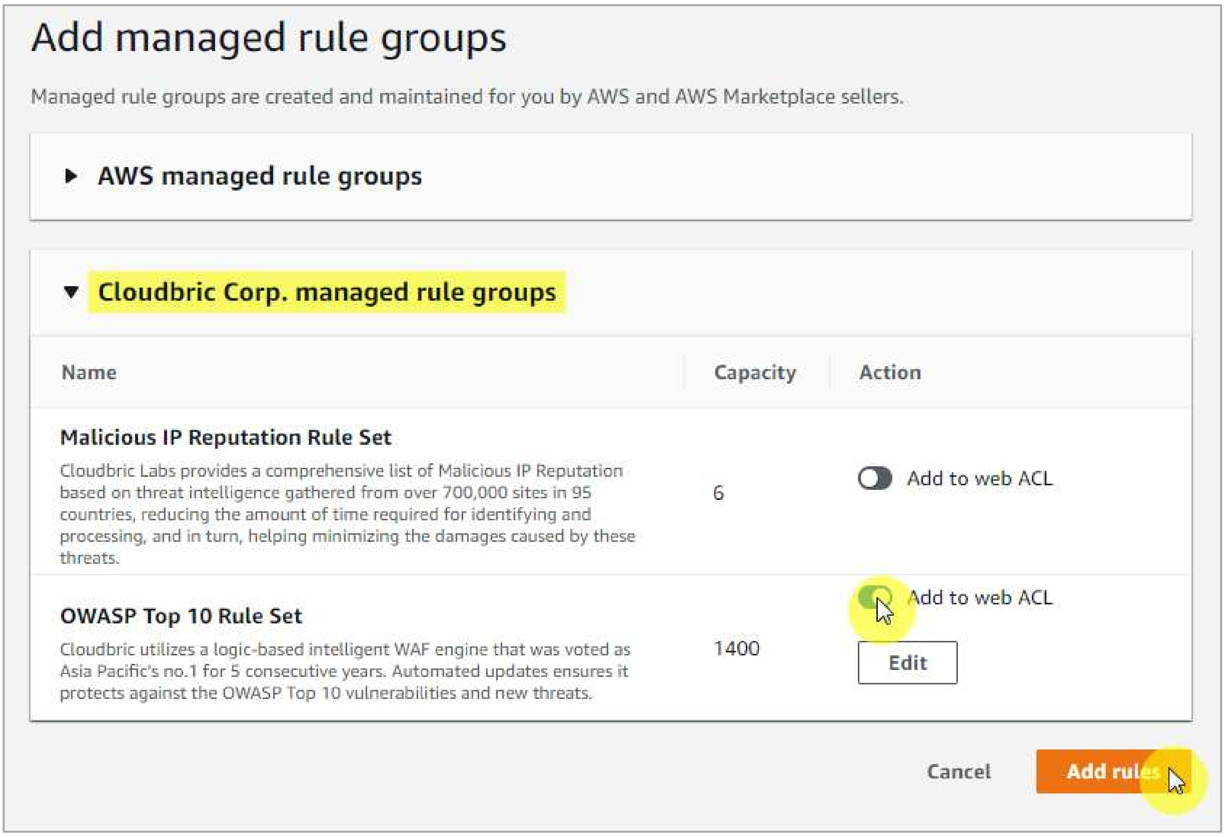
example_acl

Rules (0)

- **Step 4**

  Enable the 'Add to web ACL' of the subscribed Cloudbric Rule Set, then select **[Add rules]**.

  ※ *To test the Rules Set first, select [Edit] and change the Action of the Rule to 'count'.*



Add managed rule groups

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

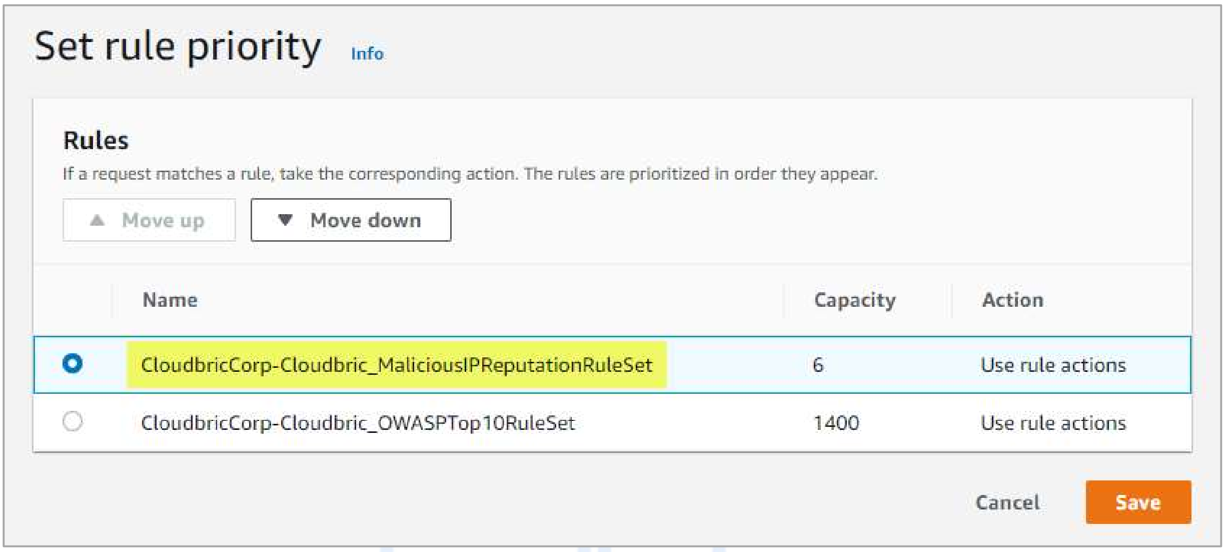
▶ AWS managed rule groups

▼ Cloudbric Corp. managed rule groups

Name	Capacity	Action
Malicious IP Reputation Rule Set Cloudbric Labs provides a comprehensive list of Malicious IP Reputation based on threat intelligence gathered from over 700,000 sites in 95 countries, reducing the amount of time required for identifying and processing, and in turn, helping minimizing the damages caused by these threats.	6	Add to web ACL
OWASP Top 10 Rule Set Cloudbric utilizes a logic-based intelligent WAF engine that was voted as Asia Pacific's no.1 for 5 consecutive years. Automated updates ensures it protects against the OWASP Top 10 vulnerabilities and new threats.	1400	Add to web ACL Edit

- **Step 5**

  When adding both Cloudbric Rule Sets, set **Malicious IP Reputation Rule Set** as priority, then select **[Save]** to complete applying the Rules.



Set rule priority Info

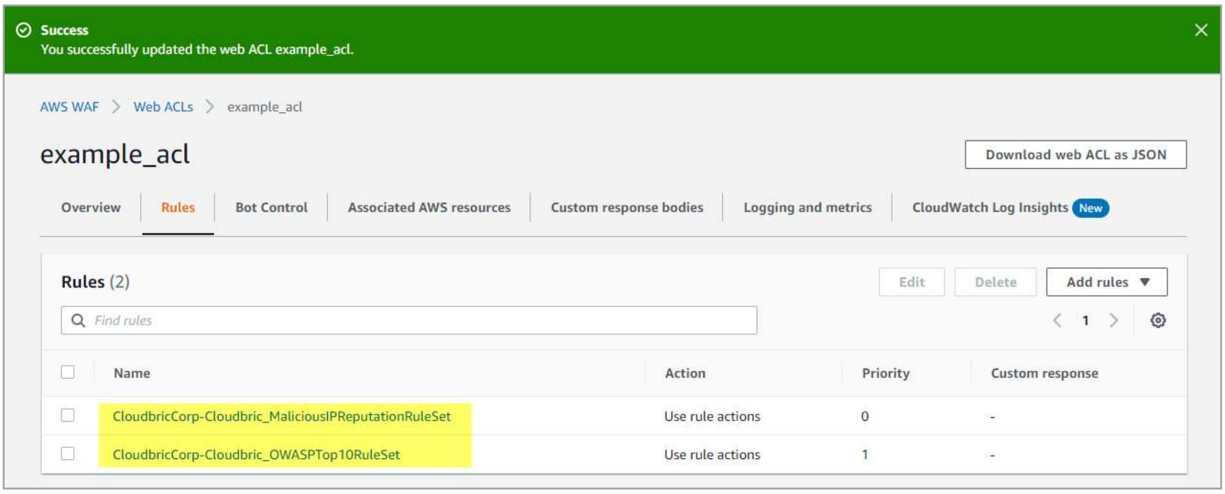
Rules

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

	Name	Capacity	Action
●	CloudbricCorp-Cloudbric_MaliciousIPReputationRuleSet	6	Use rule actions
○	CloudbricCorp-Cloudbric_OWASPTop10RuleSet	1400	Use rule actions

- **Step 6**

  Confirm that the **Cloudbric Rule Set** has been applied from the **[Rules]** tab of the Web ACL.



Success
You successfully updated the web ACL example_acl.

AWS WAF > Web ACLs > example_acl

example_acl

Rules (2)

□	Name	Action	Priority	Custom response
□	CloudbricCorp-Cloudbric_MaliciousIPReputationRuleSet	Use rule actions	0	-
□	CloudbricCorp-Cloudbric_OWASPTop10RuleSet	Use rule actions	1	-

3. How to remove Cloudbric Rule Set

If Cloudbric Rule Set is no longer in use, in addition to cancelling Cloudbric Rule Set subscription, all Cloudbric Rule Sets must be deleted from all Web ACLs of the AWS WAF console to avoid being billed from subscribing to the Rule Sets.

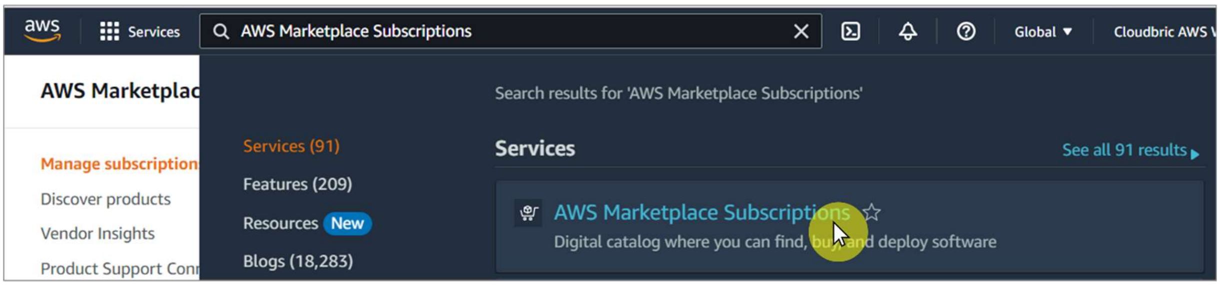
※ You will be continued to be billed if you only unsubscribe Cloudbric Rule Set without deleting the Cloudbric Rule Set added to the Web ACL.

3.1 Cancelling Cloudbric Rule Set subscription

- **Step 1**

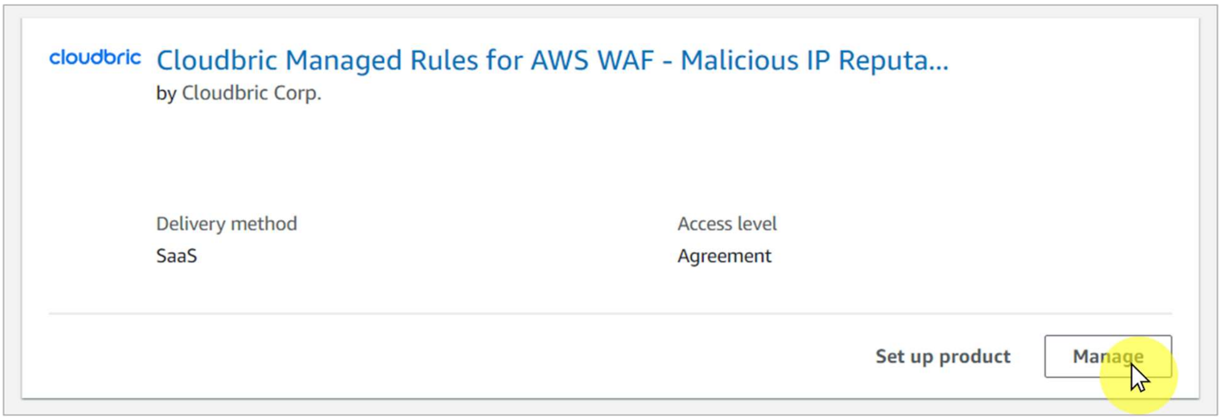
  Go to AWS Marketplace subscriptions management console.

  ※ *AWS WAF console :* https://console.aws.amazon.com/marketplace/home#/subscriptions



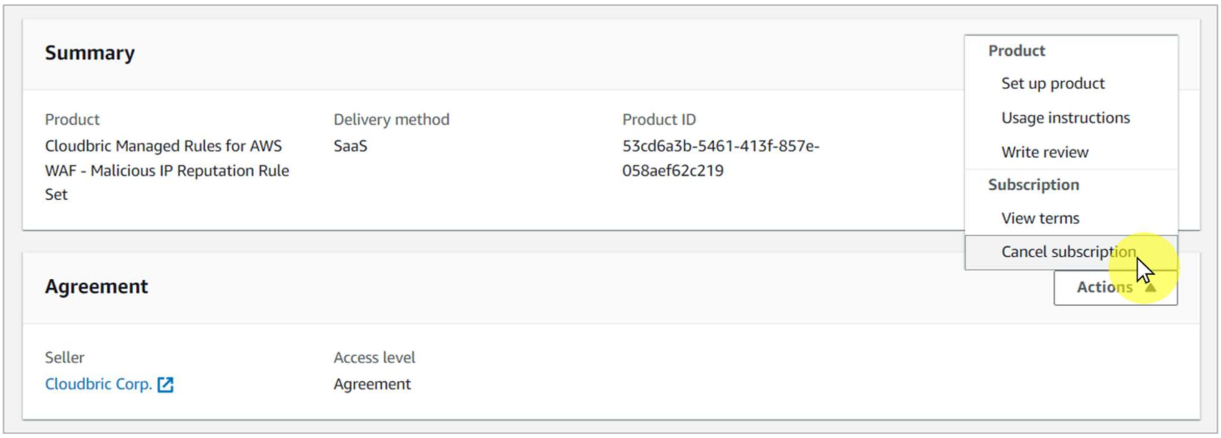
- **Step 2**

  Select **[Manage]** of the Cloudbric Rule Set to unsubscribe from the **[Manage subscriptions]** menu.



- **Step 3**

  Select **[Cancel subscription]** from **[Actions]** drop down menu in **'Agreement.'**



Summary

Product
Cloudbric Managed Rules for AWS WAF - Malicious IP Reputation Rule Set

Delivery method
SaaS

Product ID
53cd6a3b-5461-413f-857e-058aef62c219

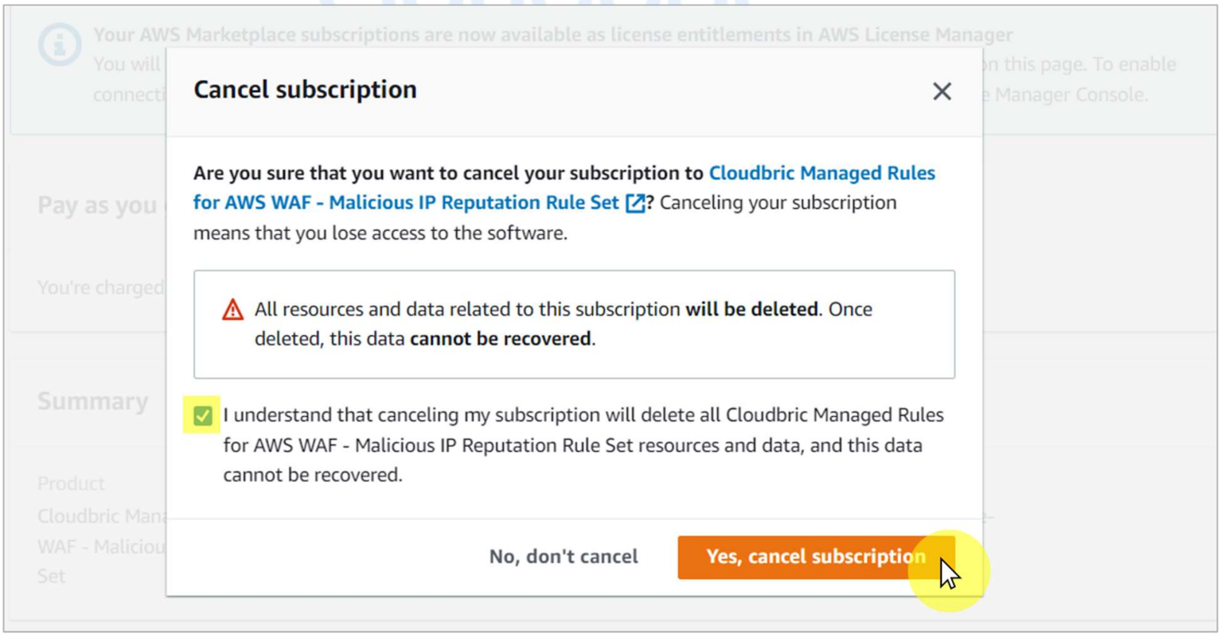
Agreement

Seller
Cloudbric Corp.

Access level
Agreement

- **Step 4**

  Complete the cancellation of subscription by selecting **[Yes, cancel subscription]** after selecting the checkbox for the disclaimer regarding the recoverability of data.



Your AWS Marketplace subscriptions are now available as license entitlements in AWS License Manager
Pay as you
Summary
Product
No, don't cancel
Yes, cancel subscription

Cancel subscription

Are you sure that you want to cancel your subscription to Cloudbric Managed Rules for AWS WAF - Malicious IP Reputation Rule Set? Canceling your subscription means that you lose access to the software.

⚠ All resources and data related to this subscription **will be deleted**. Once deleted, this data **cannot be recovered**.

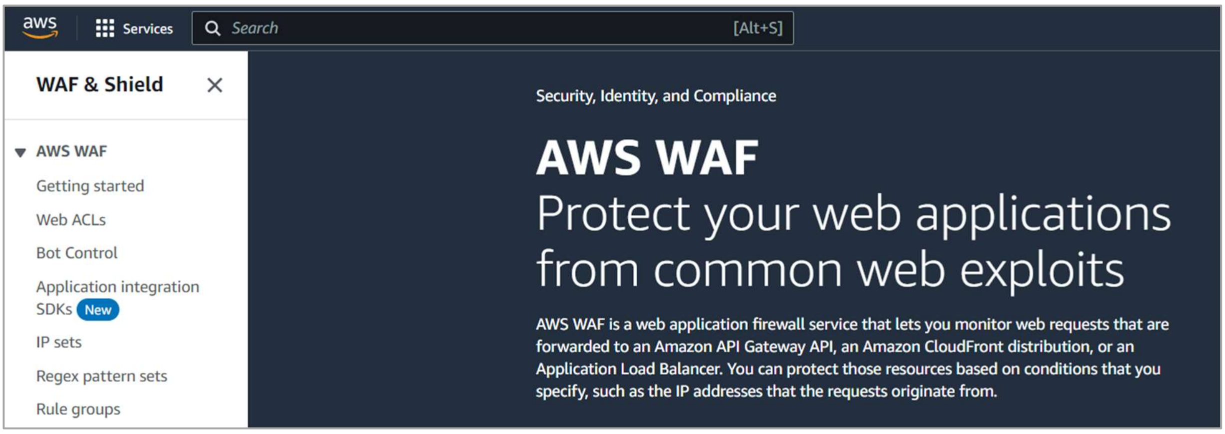
☑ I understand that canceling my subscription will delete all Cloudbric Managed Rules for AWS WAF - Malicious IP Reputation Rule Set resources and data, and this data cannot be recovered.

3.2 Deleting Cloudbric Rule Set

- **Step 1**

  Go to AWS WAF console.

  ※ *AWS WAF console :* https://console.aws.amazon.com/wafv2/



Security, Identity, and Compliance

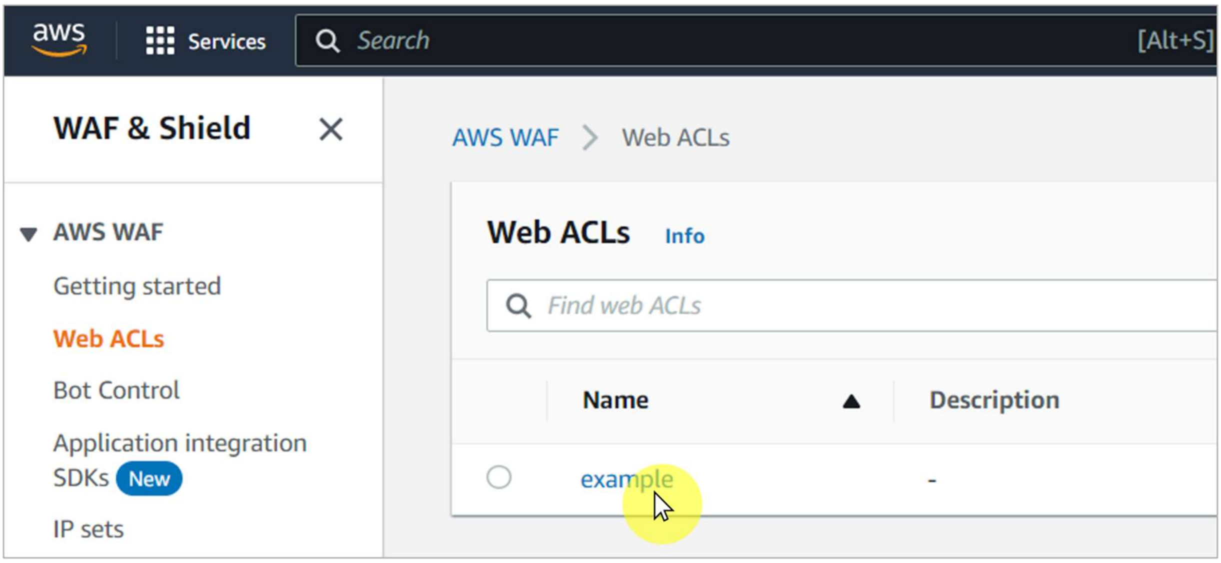
AWS WAF

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.

- **Step 2**

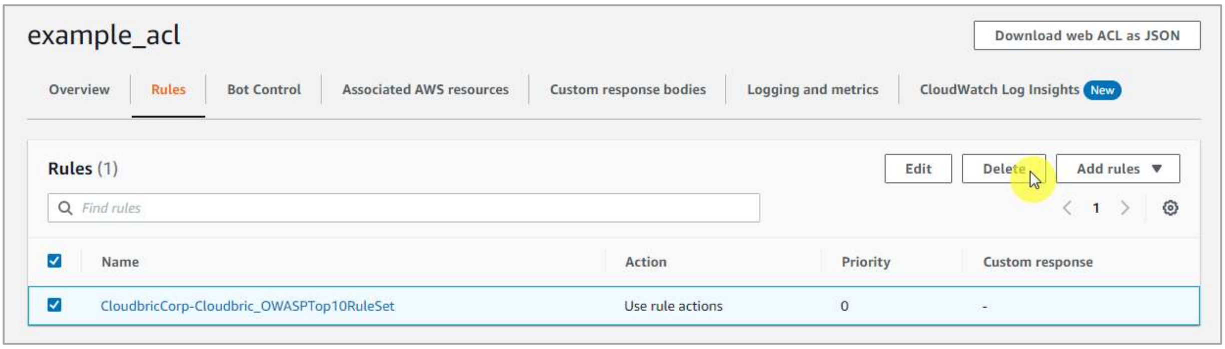
  Go to the Web ACL menu and select the Web ACL to add the Cloudbric Rule Set.



	Name	Description
○	example	-

- **Step 3**

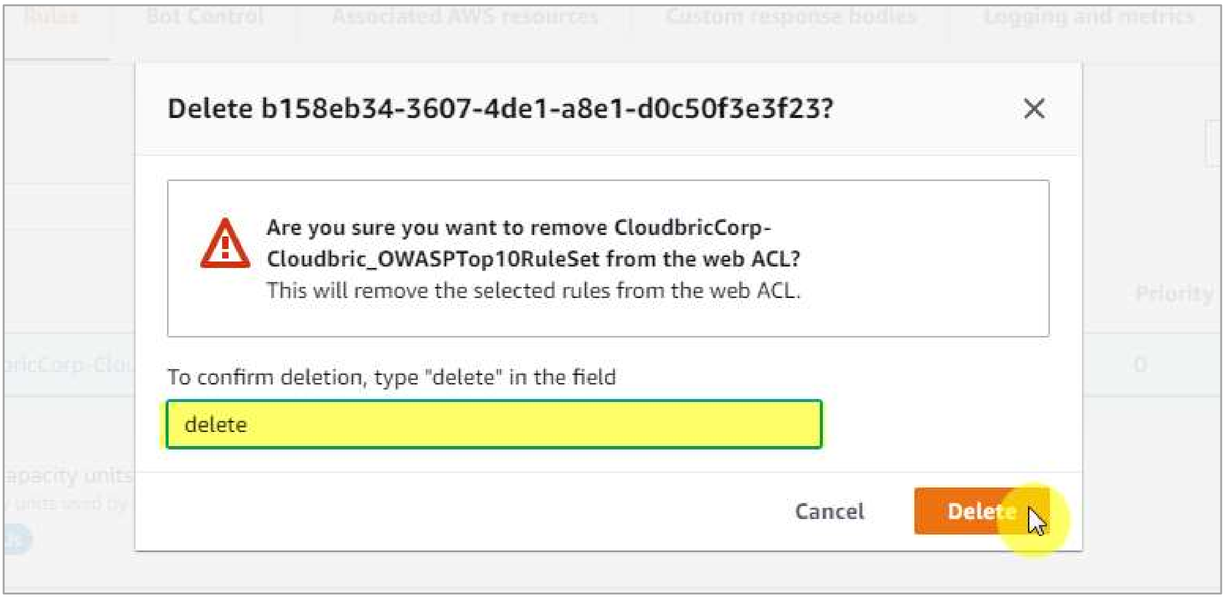
  Select the Cloudbric Rule Set to delete from **[Rules]** tab and select **[Delete]**.



☑	Name	Action	Priority	Custom response
☑	CloudbricCorp-Cloudbric_OWASPTop10RuleSet	Use rule actions	0	-

- **Step 4**

  Type in **'delete,'** and select **[Delete]** to complete the deletion.



Delete b158eb34-3607-4de1-a8e1-d0c50f3e3f23?

Are you sure you want to remove CloudbricCorp-Cloudbric_OWASPTop10RuleSet from the web ACL?
This will remove the selected rules from the web ACL.

To confirm deletion, type "delete" in the field

delete

4. Cloudbric Rule Set Override

When a false-positive is detected in which a legitimate request has been blocked by the Cloudbric Rule Set, the Action for the Rule with the false-positive must be re-defined as ‘Count’ to override and avoid the block. However, this could also lead to instances in which a malicious request is also permitted. To maintain the functions of the Rules as much as it was before the Rule Override and apply the Override on a specific pattern that the false-positive has occurred, the Override Rule must be re-defined by adding a label-based, user-defined Rule.

※ *All Rules in Cloudbric OWASP Top 10 Rule Set is configured with Labels.*

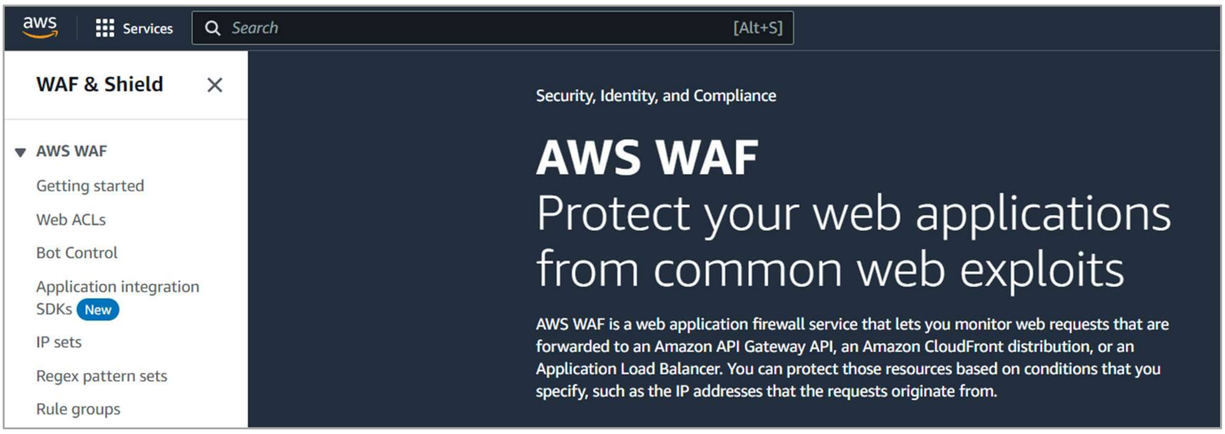
※ *The IP based Cloudbric Rule Sets are not configured with any other Labels due to the dynamic nature of the IP List. If an IP requires an Override, a Rule allowing the IP should be created.*

4.1 Configuring Rule Action ‘Count’

- **Step 1**

  Go to AWS WAF console.

  ※ *AWS WAF console :* https://console.aws.amazon.com/wafv2/



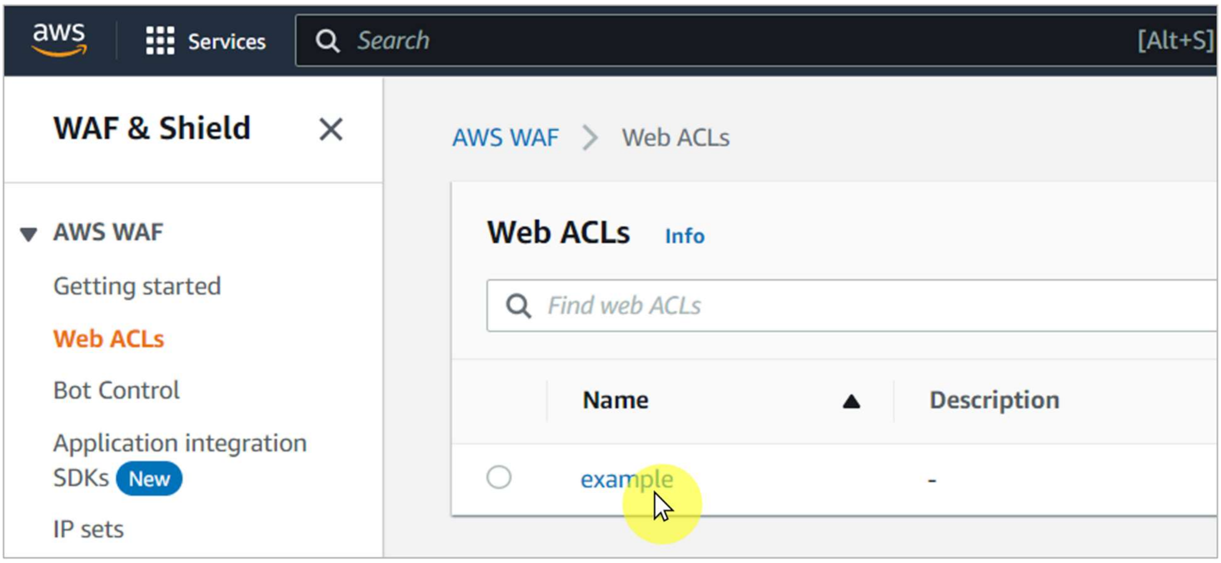
AWS WAF

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.

- **Step 2**

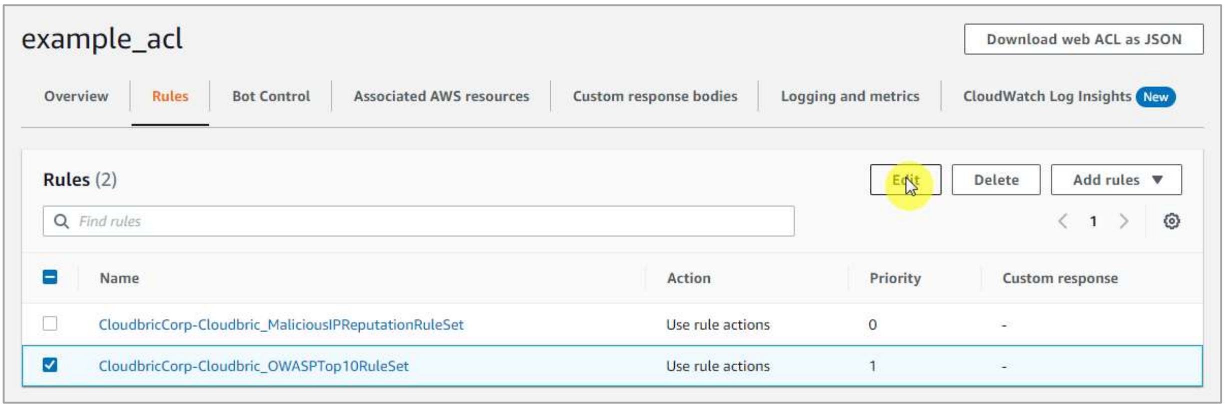
  Go to the Web ACL menu and select the Web ACL applied with the Cloudbric Rule Set.



	Name ▲	Description
○	example	-

- **Step 3**

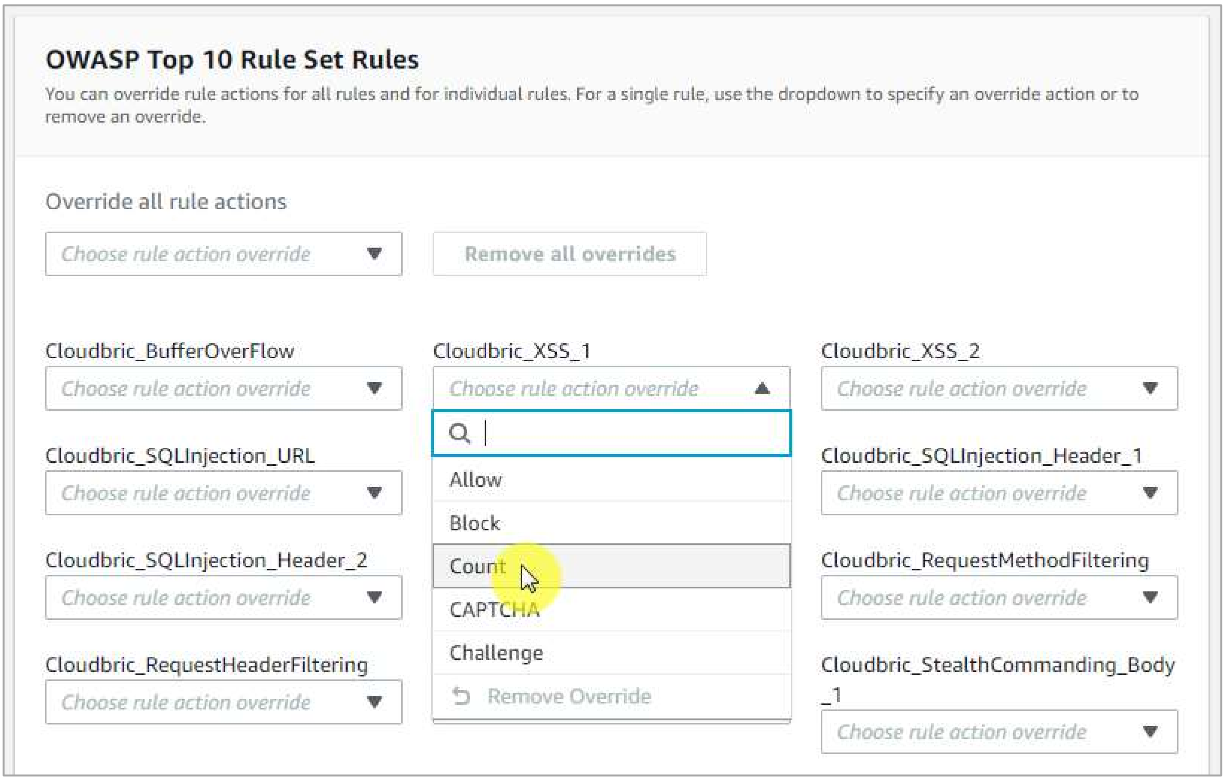
  Go to **[Rules]** tab, then select the Checkbox for all the Rule Sets to override and select **[Edit]**.



	Name	Action	Priority	Custom response
□	CloudbricCorp-Cloudbric_MaliciousIPReputationRuleSet	Use rule actions	0	-
☑	CloudbricCorp-Cloudbric_OWASPTop10RuleSet	Use rule actions	1	-

- **Step 4**

  Redefine the Action of the Rule to override to 'Count' and select **[Save rule]** to complete the override.



OWASP Top 10 Rule Set Rules

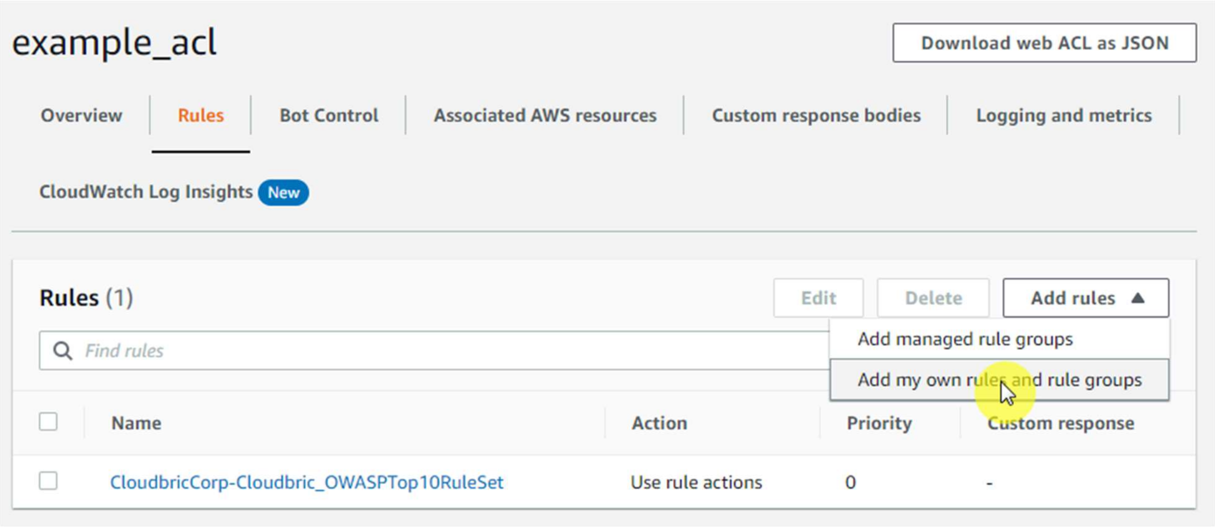
You can override rule actions for all rules and for individual rules. For a single rule, use the dropdown to specify an override action or to remove an override.

Override all rule actions
Choose rule action override
Remove all overrides
Cloudbric_BufferOverFlow
Choose rule action override
Cloudbric_XSS_1
Choose rule action override
Allow
Block
Count
CAPTCHA
Challenge
Remove Override
Cloudbric_XSS_2
Choose rule action override
Cloudbric_SQLInjection_URL
Choose rule action override
Cloudbric_SQLInjection_Header_1
Choose rule action override
Cloudbric_SQLInjection_Header_2
Choose rule action override
Cloudbric_RequestMethodFiltering
Choose rule action override
Cloudbric_RequestHeaderFiltering
Choose rule action override
Cloudbric_StealthCommanding_Body_1
Choose rule action override

4.2 Adding Override Rules based on Labels

- **Step 1**

  Go to **[Rules]** tab from Web ACL and select **[Add my own rules and rule groups]** from the drop down menu that appears by clicking **[Add rules]** to create a new Rule.



example_acl

Download web ACL as JSON

Overview | Rules | Bot Control | Associated AWS resources | Custom response bodies | Logging and metrics | CloudWatch Log Insights New

Rules (1)

Edit | Delete | Add rules ▲

Find rules

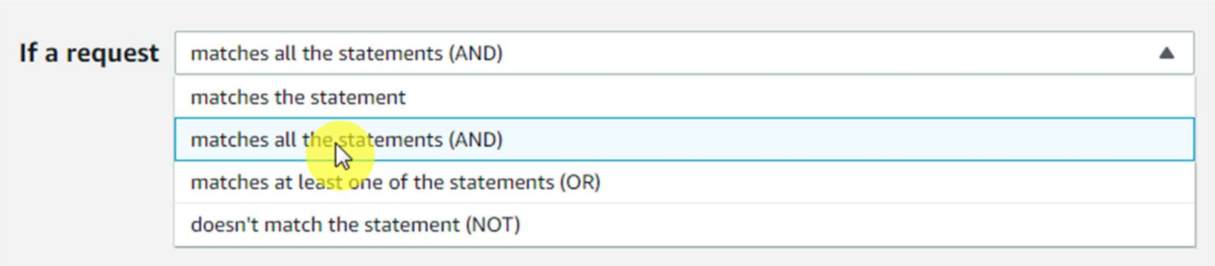
- Add managed rule groups
- Add my own rules and rule groups

□	Name	Action	Priority	Custom response
□	CloudbricCorp-Cloudbric_OWASPTop10RuleSet	Use rule actions	0	-

- **Step 2**

Select the overlapping 'AND' option for the request to match the rule when it fulfills 2 statements.

- If a request: matches all the statements (AND)



If a request: matches all the statements (AND) ▲

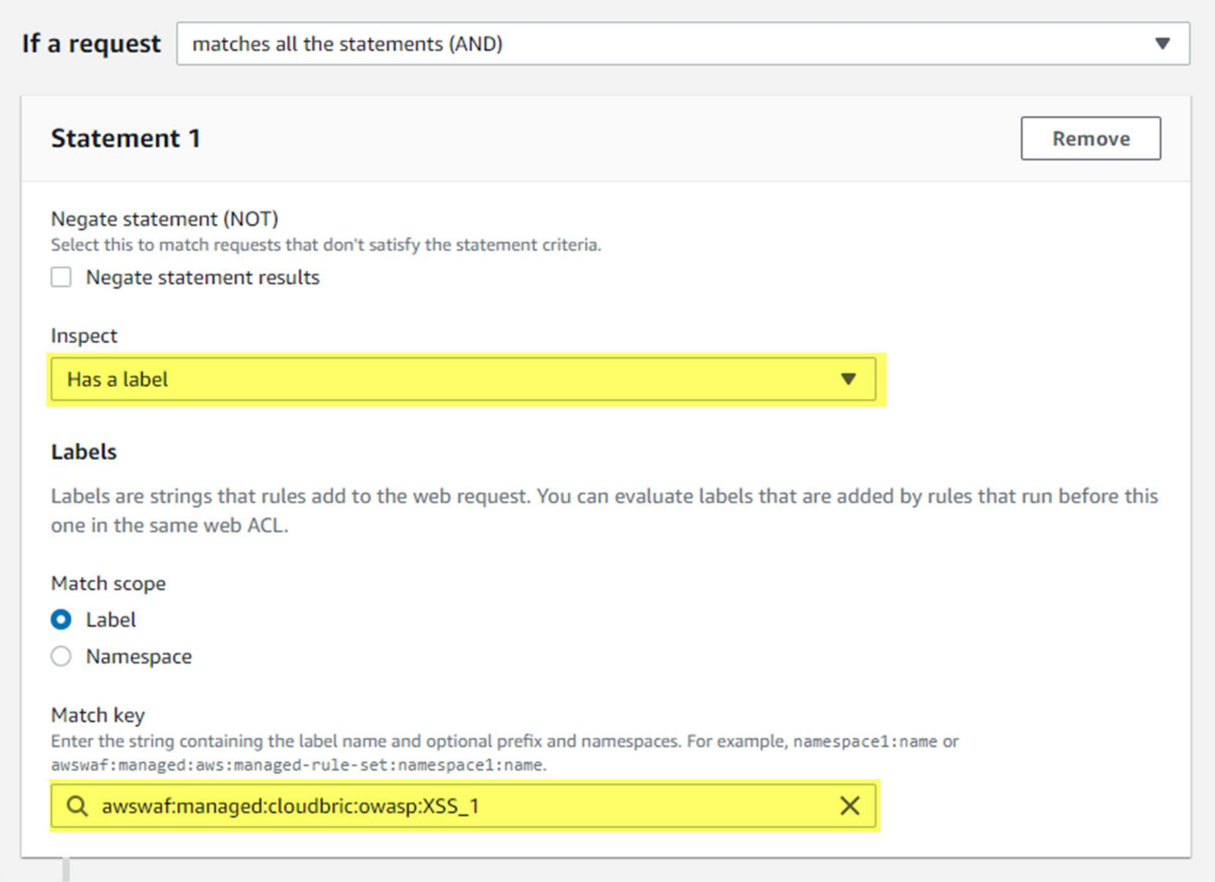
- matches the statement
- matches all the statements (AND)
- matches at least one of the statements (OR)
- doesn't match the statement (NOT)

- **Step 3**

  Statement 1 is defined to inspect the request that matches the Rule configured to Override in「4.1」.

  - Inspect: Has a label

  - Match key: Enter 'Label Name' for the Rule configured to Override



If a request: matches all the statements (AND)

Statement 1

Negate statement (NOT)

Select this to match requests that don't satisfy the statement criteria.

□ Negate statement results

Inspect: Has a label

Labels

Labels are strings that rules add to the web request. You can evaluate labels that are added by rules that run before this one in the same web ACL.

Match scope

● Label

○ Namespace

Match key

Enter the string containing the label name and optional prefix and namespaces. For example, namespace1:name or awswaf:managed:aws:managed-rule-set:namespace1:name.

awswaf:managed:cloudbric:owasp:XSS_1

※ *The structure of Label Name for Cloudbric OWASP Top 10 Rule Set :*

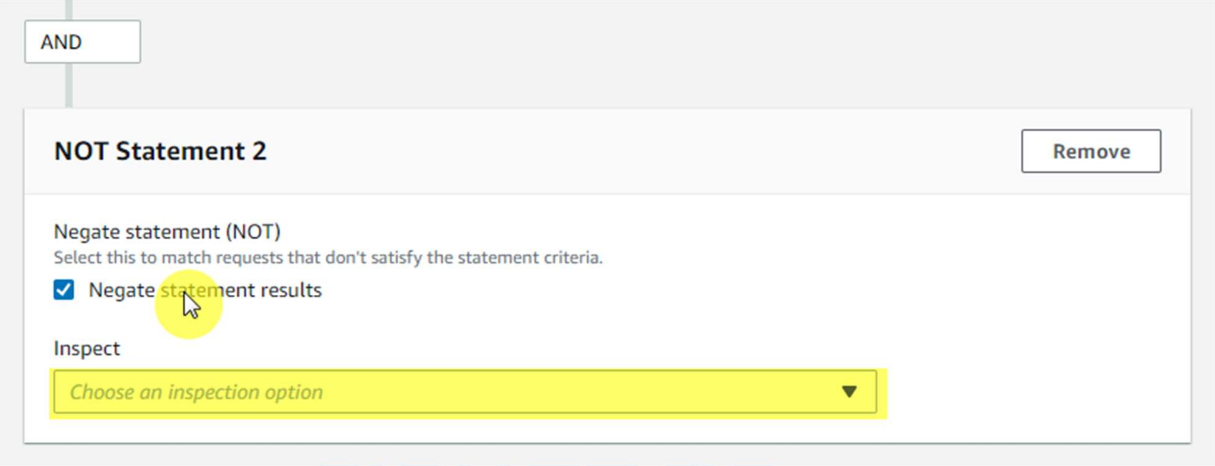
*awswaf:managed:cloudbric:owasp:**[Rule Name]***

*- Example: If the Rule Name is 'Cloudbric_XXS_1,' the label is created as: 'awswaf:managed:cloudbric:owasp:**XSS_1**'*

- **Step 4**

  Statement 2 is defined to override the inspection option for the request with the false-positive occurrence from the Rule configured to Override in「4.1」.

  - Negate statement results: Configured to check to Override the inspection option defined in the statement.
  - Inspect: Configures the inspection option with the false-positive occurrences.



AND

NOT Statement 2

Negate statement (NOT)

Select this to match requests that don't satisfy the statement criteria.

☑ Negate statement results

Inspect

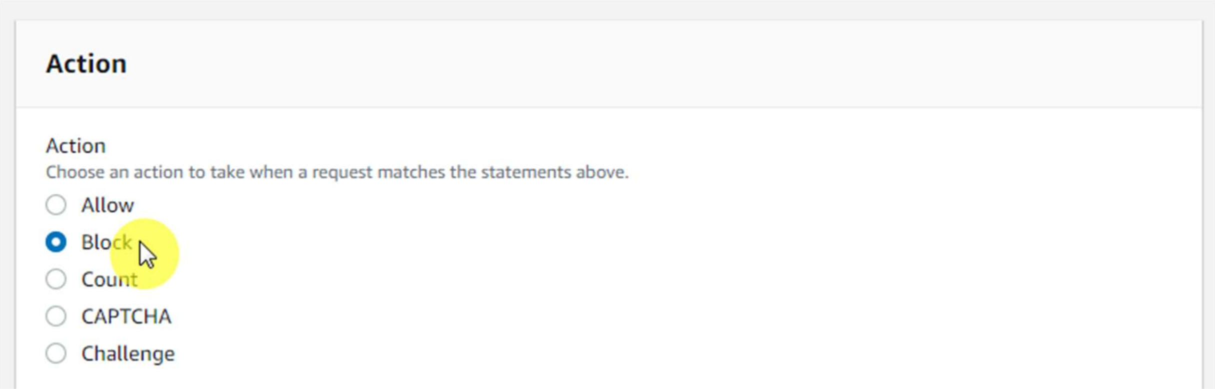
Choose an inspection option ▼

※ *The inspection option that matched the request can be reviewed from AWS WAF 'ruleMatchDetails' Log field, limited to Rules that detect SQL injection and Cross Site Scripting (XSS) attacks.*

※ *Please contact awsmkp@cloudbric.com and provide the Log information if any false-positives occurred in the other Rules.*

- **Step 5**

  Select the Action of the Rule as Block to block the request when it matches the Rule and click **[Add rule]** to add Rule.



Action

Action

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

○ Allow

● Block

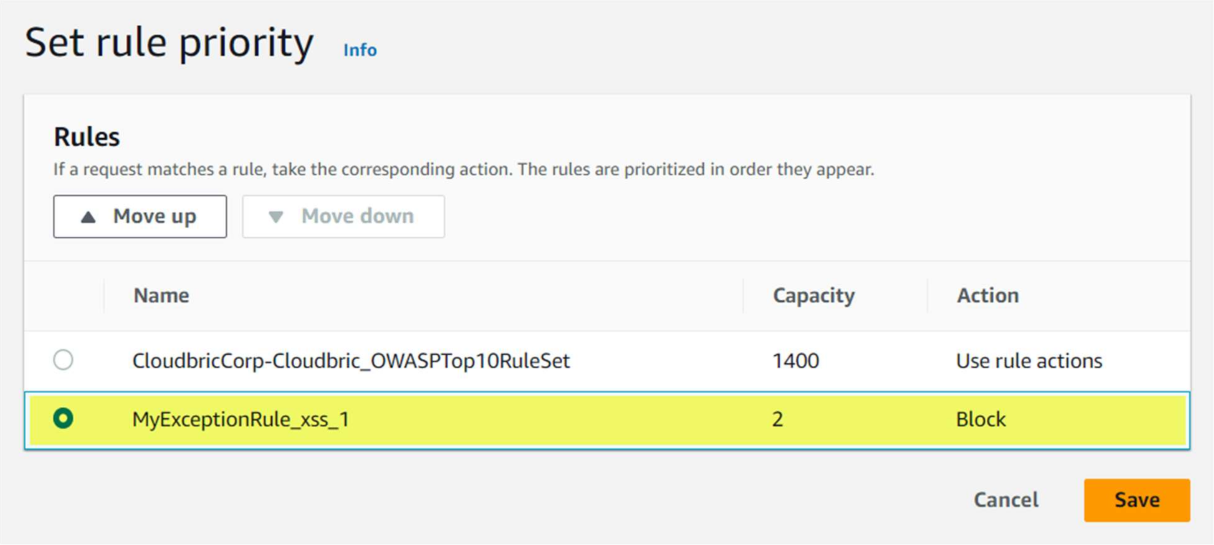
○ Count

○ CAPTCHA

○ Challenge

- **Step 6**

  Set the priority of the Rule to be applied after the Rule configured to Override in「4.1」and click **[Save]** to complete the configuration of the Override Rule.



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
○	CloudbricCorp-Cloudbric_OWASPTop10RuleSet	1400	Use rule actions
●	MyExceptionRule_xss_1	2	Block

5. Appendix

5.1. Frequently Asked Questions

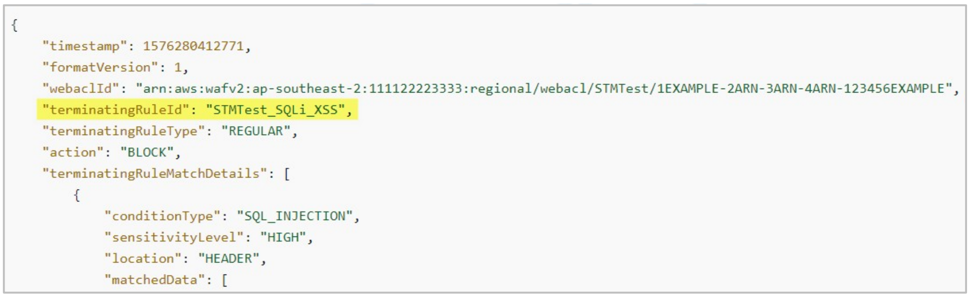
Q. How do I find the Rule ID that blocked the request?

You can find the Rule ID from **[Sampled requests] > [Rule inside rule group]** from the Web ACL, or if the Web ACL is configured, it can be found from the **[RuleID]** Log field.

※ *You can view up to 100 logs of requests from the last 3 hours for Sampled requests.*
For details, refer to Viewing a sample of web requests from the AWS Developer Guide.
https://docs.aws.amazon.com/waf/latest/developerguide/web-acl-testing-view-sample.html

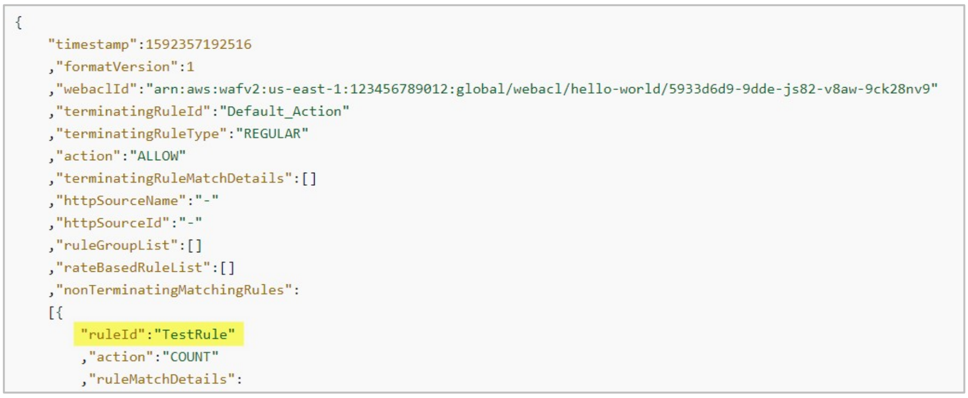
The following are Log examples to see the Rule ID.

- **terminatingRuleId**: Rule ID that terminated the request.
  Value is set to Default_Action if there is no rule to terminate the request.
  ex)



```
{
    "timestamp": 1576280412771,
    "formatVersion": 1,
    "webaclId": "arn:aws:wafv2:ap-southeast-2:111122223333:regional/webacl/STMTest/1EXAMPLE-2ARN-3ARN-4ARN-123456EXAMPLE",
    "terminatingRuleId": "STMTest_SQLi_XSS",
    "terminatingRuleType": "REGULAR",
    "action": "BLOCK",
    "terminatingRuleMatchDetails": [
        {
            "conditionType": "SQL_INJECTION",
            "sensitivityLevel": "HIGH",
            "location": "HEADER",
            "matchedData": [
```

- **RuleId**: Rule ID of the nonterminatingMatchingRules that matches the request but has not been terminated.
  ex)



```
{
    "timestamp":1592357192516
    ,"formatVersion":1
    ,"webaclId":"arn:aws:wafv2:us-east-1:123456789012:global/webacl/hello-world/5933d6d9-9dde-js82-v8aw-9ck28nv9"
    ,"terminatingRuleId":"Default_Action"
    ,"terminatingRuleType":"REGULAR"
    ,"action":"ALLOW"
    ,"terminatingRuleMatchDetails":[]
    ,"httpSourceName":"-"
    ,"httpSourceId":"-"
    ,"ruleGroupList":[]
    ,"rateBasedRuleList":[]
    ,"nonTerminatingMatchingRules":
    [{
        "ruleId":"TestRule"
        ,"action":"COUNT"
        ,"ruleMatchDetails":
```

※ *Refer to the example of Log Examples from AWS Developer Guide for more information.*

Log examples: https://docs.aws.amazon.com/waf/latest/developerguide/logging-examples.html

Q. Is there a way to check if the Cloudbric Rule Set was properly added?

When the request matches the Rule that was set as Block, AWS WAF returns a 403 Forbidden error as default. You can check if the Rule Set was properly added by entering a simplified XSS attack example on the browser.

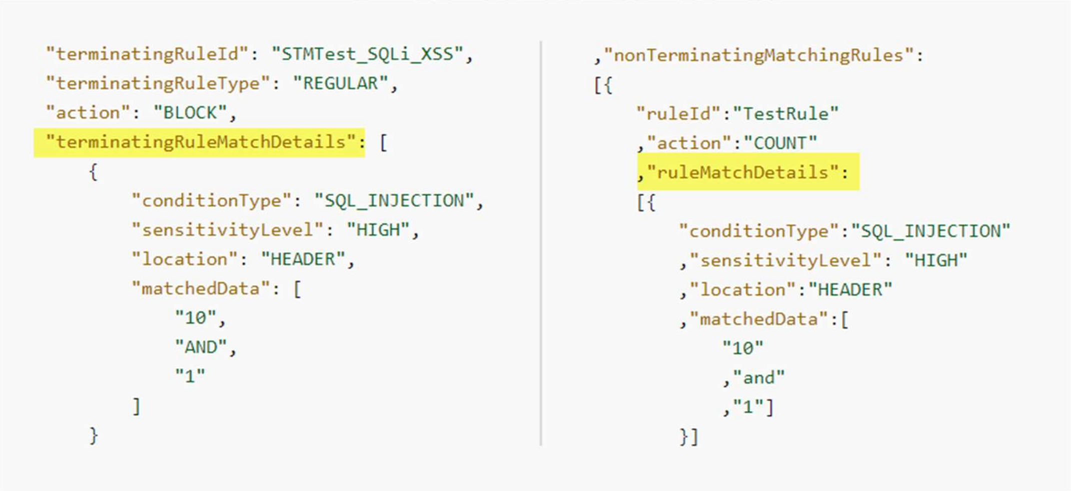
- http://your-domain/<script>alert('XSS')</script>

Q. Can I view the inspection criteria of Cloudbric Rule Set?

As a default, the details of the inspection location or pattern of AWS WAF Managed Rules is not disclosed, as it is an intellectual property of the AWS Marketplace vendor, and disclosing the detection criteria may be exploited to for hacking such as bypassing the Rule.

However, the inspection option that matched the request can be reviewed from AWS WAF 'ruleMatchDetails' Log field, limited to Rules that detect SQL injections and Cross Site Scripting (XSS) attacks.

Log example of inspection option of the Rule matched with SQL injection attacks:



```
"terminatingRuleId": "STMTest_SQLi_XSS",
"terminatingRuleType": "REGULAR",
"action": "BLOCK",
"terminatingRuleMatchDetails": [
    {
        "conditionType": "SQL_INJECTION",
        "sensitivityLevel": "HIGH",
        "location": "HEADER",
        "matchedData": [
            "10",
            "AND",
            "1"
        ]
    }
```

```
,"nonTerminatingMatchingRules":
[{
    "ruleId":"TestRule"
    ,"action":"COUNT"
    ,"ruleMatchDetails":
    [{
        "conditionType":"SQL_INJECTION"
        ,"sensitivityLevel": "HIGH"
        ,"location":"HEADER"
        ,"matchedData":[
            "10"
            ,"and"
            ,"1"]
        }]
```

(Left)When the Rule terminated the request / (Right)When the Rule did not terminate the request

Q. Can the inspection option be changed when a false-positive or over detection occurs?

AWS does not provide any features to change inspection options for Managed Rules.

However, as AWS WAF Managed Rules are written based on the threats generally observed from majority of clientele, false-positives and over detections may occur according to the environment. Therefore, it is recommended that Cloudbric Rule Set applied after being configured to Override as stated in「4. Cloudbric Rule Set Override」according to the operating environment through 2~4 weeks of monitoring before actual application to your environment.

If you have any difficulties in optimizing the Rule configuration according to the user environment, we recommend using Cloudbric WMS, a security Rule operation and management service for AWS WAF.

- Cloudbric WMS Overview page: https://www.cloudbric.com/cloudbric-wms/
- Cloudbric WMS Service Inquiry: https://cloudbric.zendesk.com/hc/en-us/requests/new

Q. Where can I view the changes made to the Cloudbric Rule Set?

Since Nov 12th, 2021, changes made on Cloudbric Rule Sets are notified on Cloudbric official homepage.

※ Due to the variability of the IP address list, the changes made on the IP address list applied to Malicious IP Reputation Rule Set are not notified on the Cloudbric official homepage.

Cloudbric Managed Rule Set for AWS WAF Release note URL

- KR: https://www.cloudbric.co.kr/cloudbric-managed-rules-for-aws-waf-releas-notes/
- EN: https://www.cloudbric.com/cloudbric-managed-rules-for-aws-waf-release-notes/
- JP: https://www.cloudbric.jp/managed-rules-for-aws-waf-release-notes/

Q. What is the pricing for Cloudbric Rule Set each month?

The cost for the AWS WAF Managed Rule is estimated by two cost dimensions based on the Web ACLs with Cloudbric Rule Set applied as stated as follows.

① **Region**: Number of Regions with Web ACL deployed.

② **Requests**: Number of Requests received by Web ACL per region by units of 1million requests.

Example of estimating cost for Cloudbric OWASP Top 10 Rule Set:

- OWASP Top 10 Rule Set cost information:

Units	Cost
Per Region	$25/Month (Pro-rated by the hour)
Per million requests in each region	$1/Month

- Case A:

2 Web ACL with added Cloudbric Rule Set created for a single region(ex: us-east-1)
Total number of Web requests the Web ACL received was 10million for a month for 2 Web ACLs
Estimate)
<u>us-east-1 Region</u>
① **Region Cost**: $25.00 * 1 = $25.00
② **Requests Cost**: $1.00(Per million) * 10 Requests(Total of 10million) = $10.00

= Total Cost(①+②): $35.00

- Case B:

2 Web ACL with added Cloudbric Rule Set created for 2 regions(ex: us-east-1, us-west-2)
Total number of requests for 2 Web ACL in each region received was 10million
Estimate)
<u>us-east-1 Region</u>
① **Region Cost**: $25.00 * 1 = $25.00
② **Requests Cost**: $1.00(Per million) * 10 Requests(Total of 10million) = $10.00
<u>us-west-2 Region</u>
③ **Region Cost**: $25.00 * 1 = $25.00
④ **Requests Cost**: $1.00(Per million) * 10 Requests(Total of 10million) = $10.00

= Total Cost(①+②+③+④): $70.00

5.2 Cloudbric OWASP Top 10 Rule Types Description

Rule Types	Details
Buffer Overflow	Blocks Request sentence including a volume of data that exceeds the limit which a memory Buffer Overflow attack on the web server.
Cross Site Scripting (XSS)	Blocks malicious script code deployed from the client's side.
SQL Injection	Blocks requests attempting to inject SQL Query.
Directory Traversal	Blocks requests attempting to access directories or files using vulnerabilities of the web server.
Request Method Filtering	Blocks against unsafe HTTP Request Methods.
Request Header Filtering	Detects requests as an abnormal request (for instance sent by an automated attack tool) for requests that lack essential elements in the header or cause an error, unlike normal HTTP Request sentences sent from the web browser.
Stealth Commanding	Blocks requests attempting to execute a particular command within the web server through an HTTP Request.
File Upload	Blocks the upload of the file that can be opened from the web server.
XXE Injection	Blocks attacks that cause the browsing of local files using the External entity of XML documents.