cloudbric

Cloudbric Rule Set for AWS WAF Setting Guide v1.3 2023.08

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
2023.06	Park. Junhyung	Description for Tor IP Detection Rule Set, Rule Set versioning, and update notifications settings added	4, 10-14, 19, 20	v 1.2
2023.08	Park. Junhyung	Added description for Bot Protection Rule Set	4	v 1.3

cloudbric

PUBLIC

CONTENTS

PUBLIC

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.

1.1 Cloudbric Rule Set Overview:

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 to pass the strict technical evaluations of Amazon Web Services (AWS). Cloudbric Rule Set was developed based on the technical capabilities of Cloudbric's core team consists of some of the best security experts in the field with over 20 years of experience. Cloubric Rule Set is continuously updated and managed by the core team to maintain a stable level of security.

What is Managed Rule Group of AWS Marketplace?
Managed Rule Group of AWS Marketplace is a group of pre-defined WAF Security Rules written and maintained by AWS Marketplace vendors for AWS WAF users. By subscribing to the Managed Rule Groups through the AWS Marketplace, AWS WAF users can immediately start protecting their web applications or APIs from general threats without having to write their own rules.

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.
Tor IP Detection Rule Set *Continue to Subscribe*	Reduces the threat towards websites and web applications by preventing any damages caused by illegal use of Tor Browser which anonymizes the source of traffic by routing the internet traffic through distributed relay network.
Bot Protection Rule Set *Continue to Subscribe*	Prevents damage from wide range of attacks caused by Bots such as Account Takeover (ATO), Scraping, and Application DDoS by detecting and blocking the traffic of Bots that perform repeated actions or specific actions with malicious intents.

2. How to configure Cloudbric Rule Set

You must first subscribe to Cloudbric Rule Set through AWS Marketplace to configure the Cloudbric Rule Set for AWS WAF. Once subscribed, Cloudbric Rule Set can be implemented on the Web ACL from the AWS WAF console,

PUBLIC

and the user may change the settings related to the use of Cloudbric Rule Set such as versions and update notifications through Amazon Simple Notification Service (Amazon SNS).

2.1 Subscribing to Cloudbric Rule Set

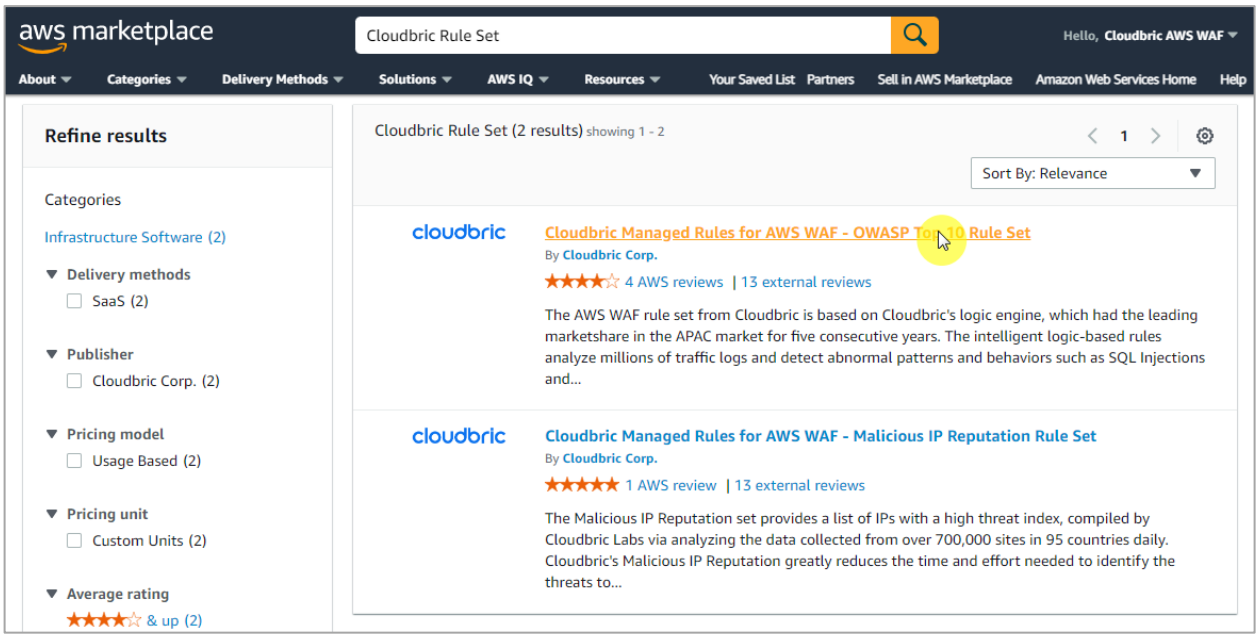
- **Step 1**

  Log in to AWS Marketplace with an AWS Account.

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

- **Step 2**

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



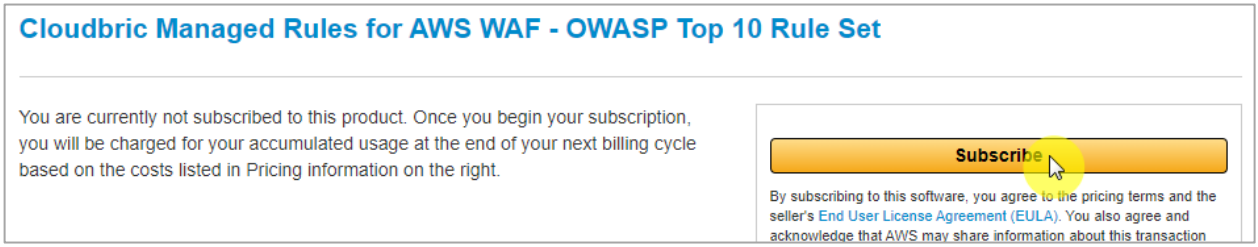
- **Step 3**

  Make sure to read the details of the selected product, then select **[Continue to Subscribe]**.

PUBLIC

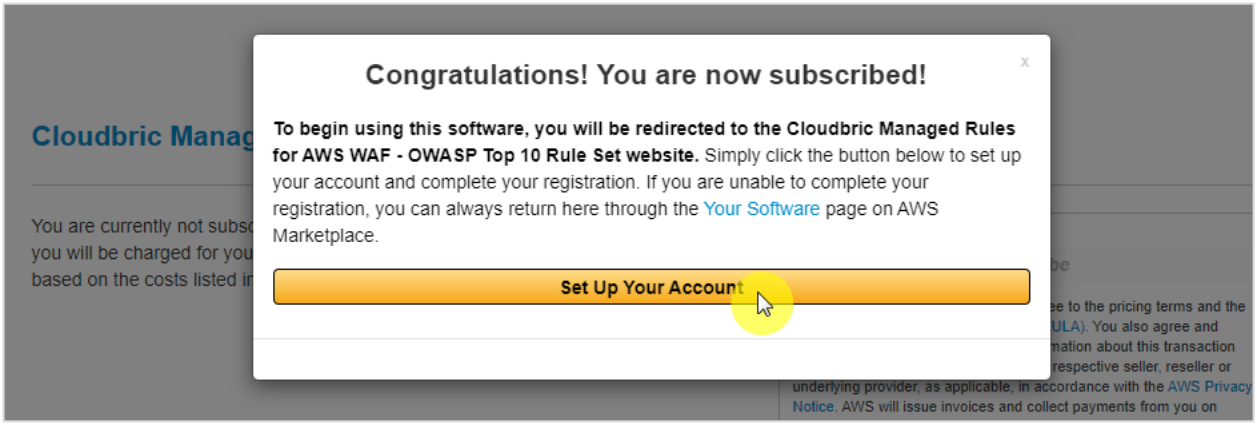
- **Step 4**

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



- **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.



2.2 Adding Cloudbric Rule Set

- **Step 1**

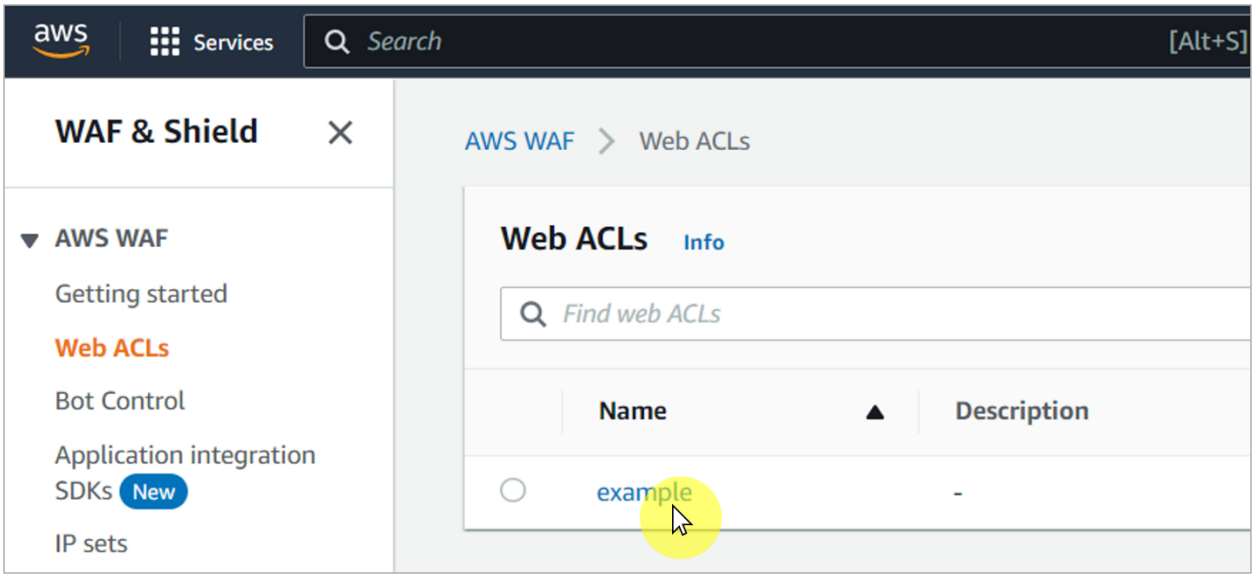
  Go to AWS WAF console.

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

PUBLIC

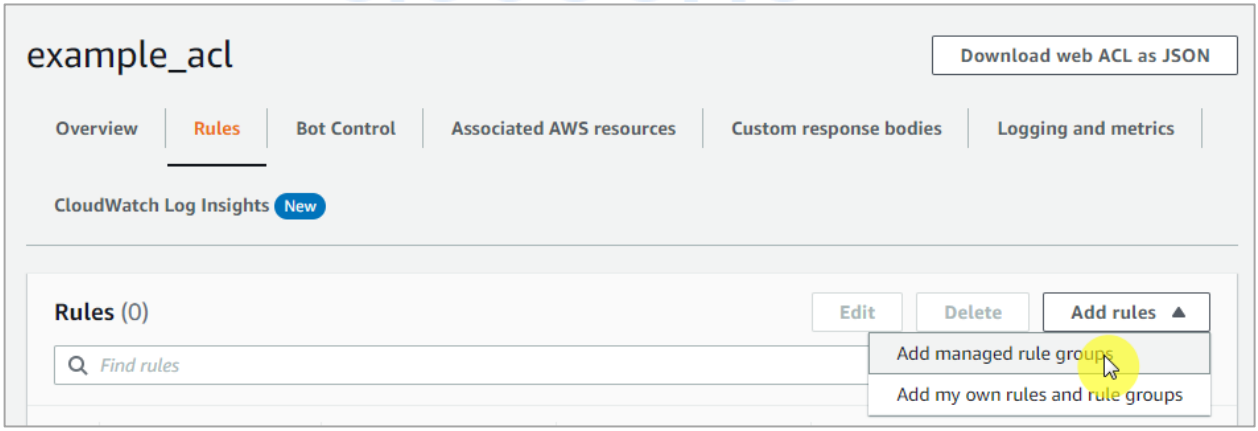
- **Step 2**

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



- **Step 3**

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

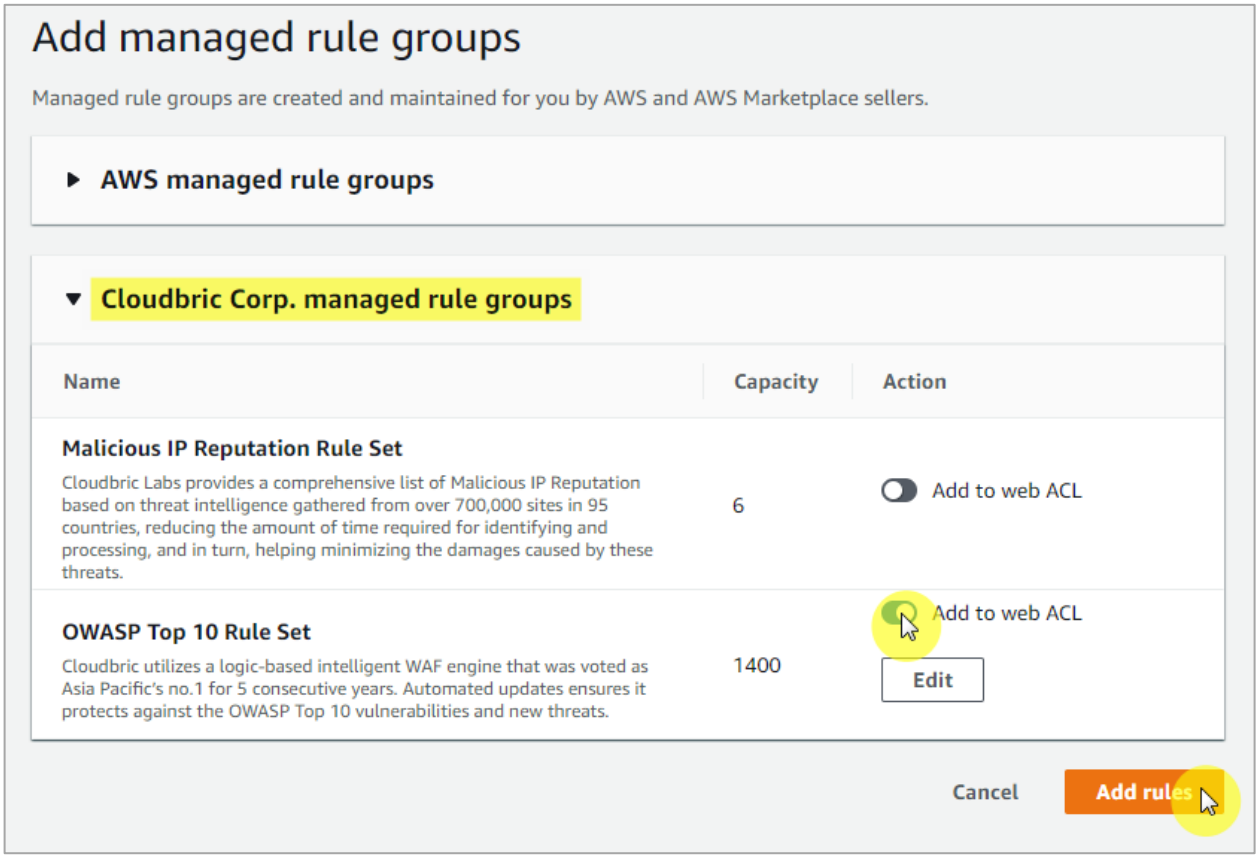


PUBLIC

- **Step 4**

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

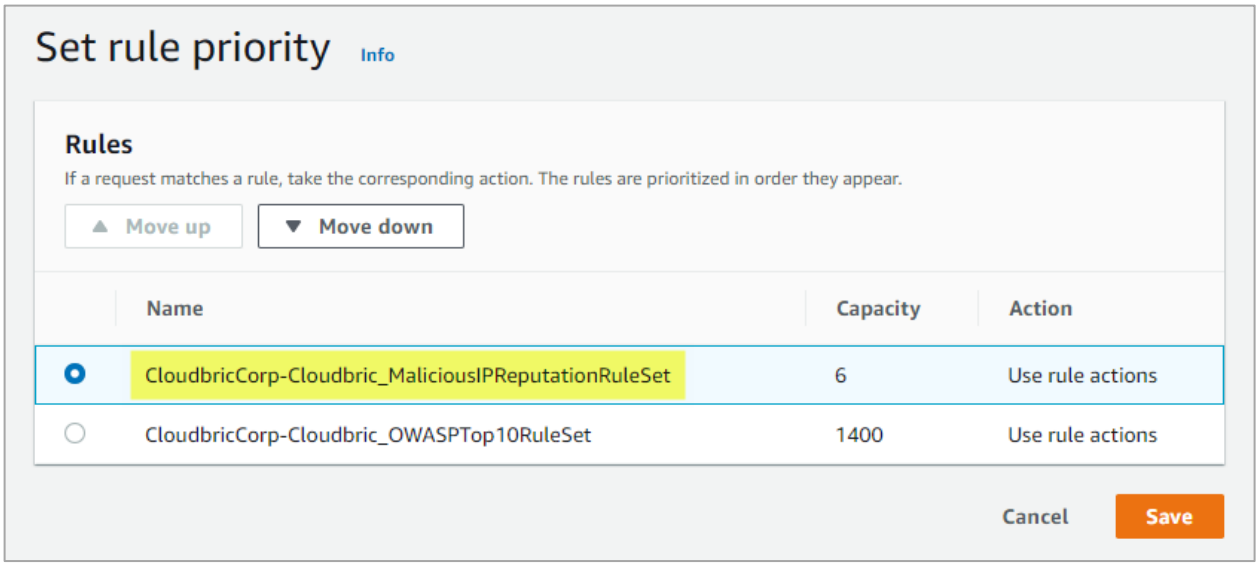
  ※To test the Rules Set first, select [Edit] and change the Action of the Rule to 'count'.



PUBLIC

- **Step 5**

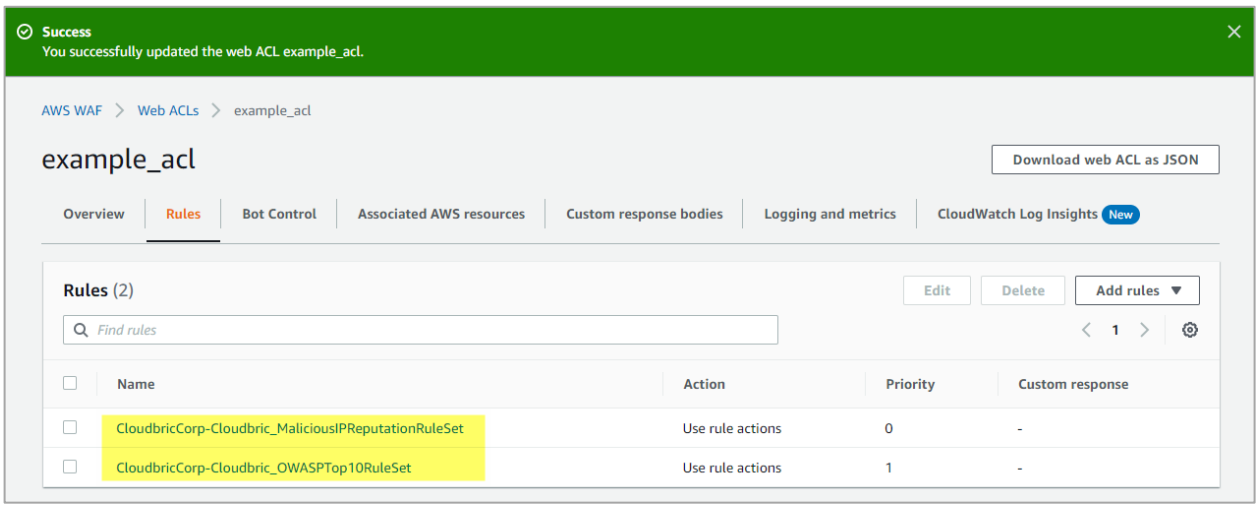
  When adding both Cloudbric Rule Sets, set **Malicious IP Reputation Rule Set** as priority, then select **[Save]** to complete applying the Rules.



cloudbric

- **Step 6**

  Check to see if the **Cloudbric Rule Set** has been properly applied from the **[Rules]** tab of the Web ACL.

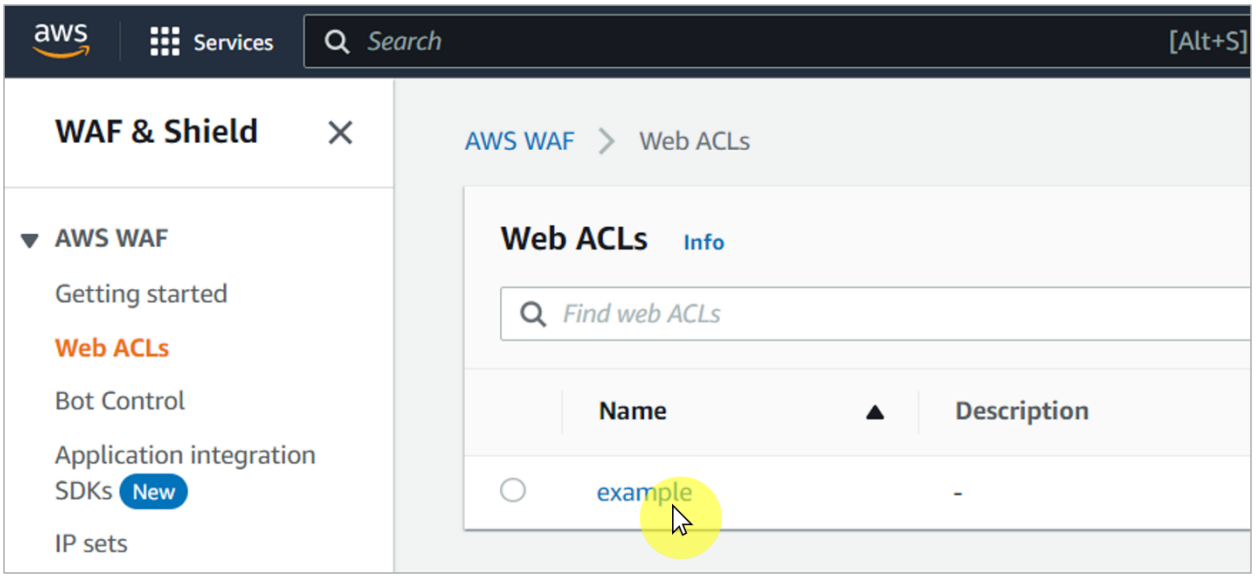


PUBLIC

2.3 Selecting the version of Cloudbric Rule Set

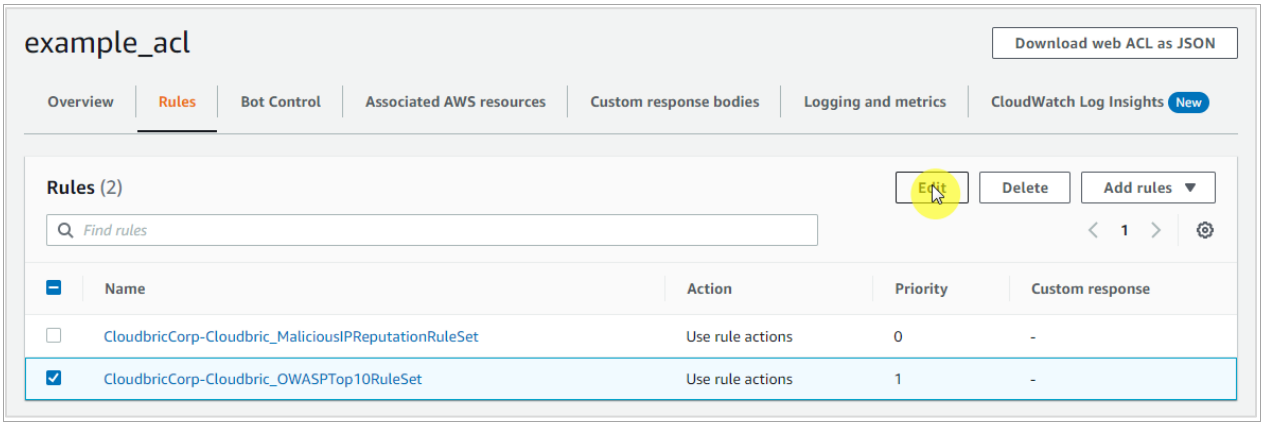
- **Step 1**
  Go to AWS WAF console.
  ※*AWS WAF console :* https://console.aws.amazon.com/wafv2/

- **Step 2**
  Go to the Web ACL menu and select the Web ACL for the Cloudbric Rule Set that the version is to be selected.



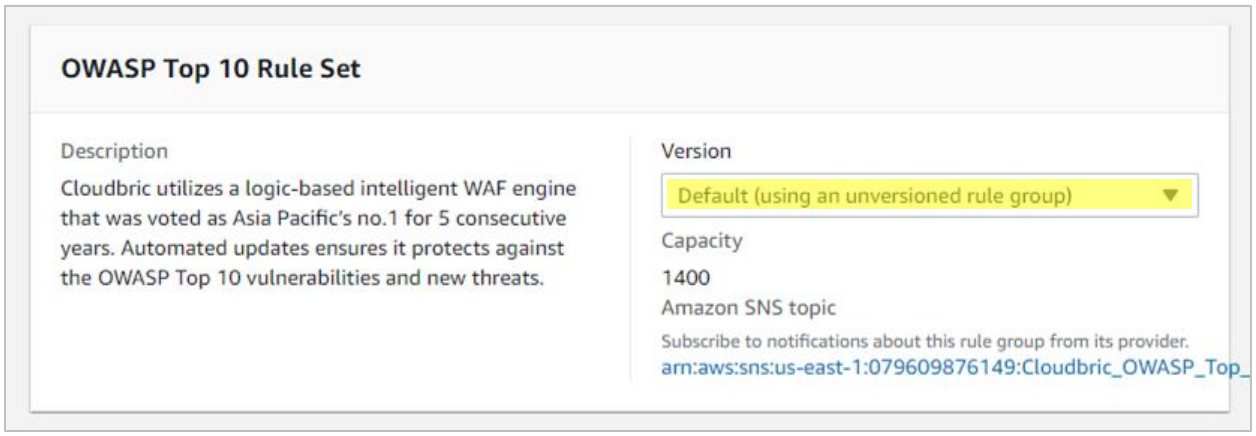
PUBLIC

- **Step 3**
  Select the **[Rules]** tab of the Web ACL, select the Cloudbric Rule Set to edt, and click **[Edit]**.



※Versioning is currently only available for OWASP Top 10 Rule Set.

- **Step 4**
  Select the version of Cloudbric Rule Set to use and click **[Save rule]** to finish the versioning process**.**



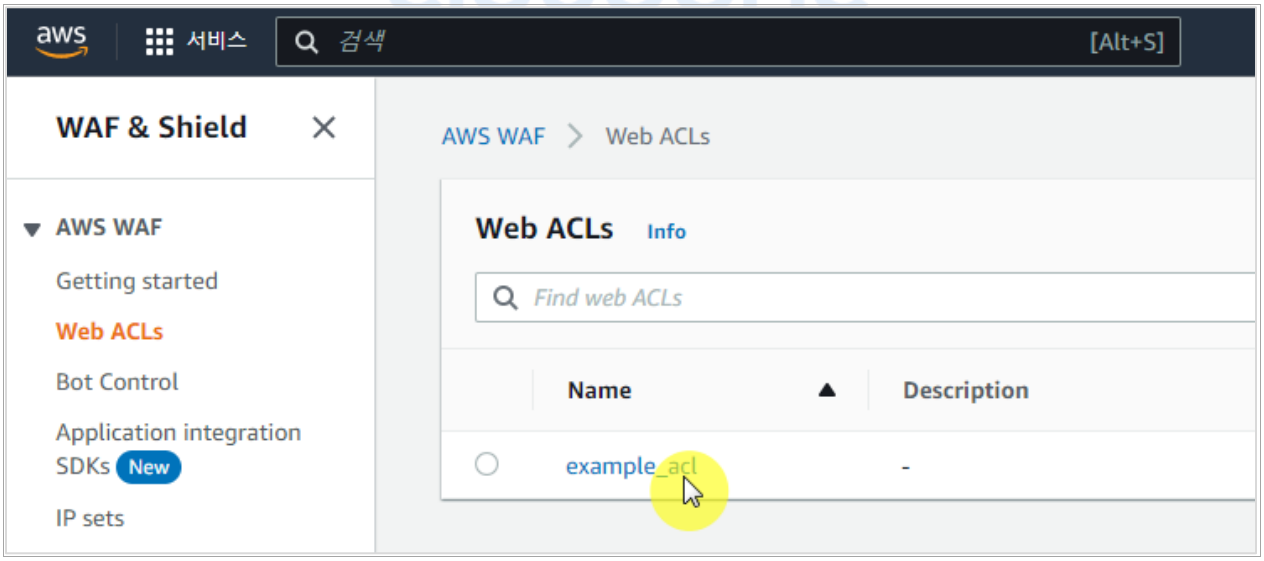
※Only the default version (latest version) is currently available. The current version will be available for use as new updated versions are to be added to the Version.

PUBLIC

2.4 Cloudbric Rule Set update notifications settings

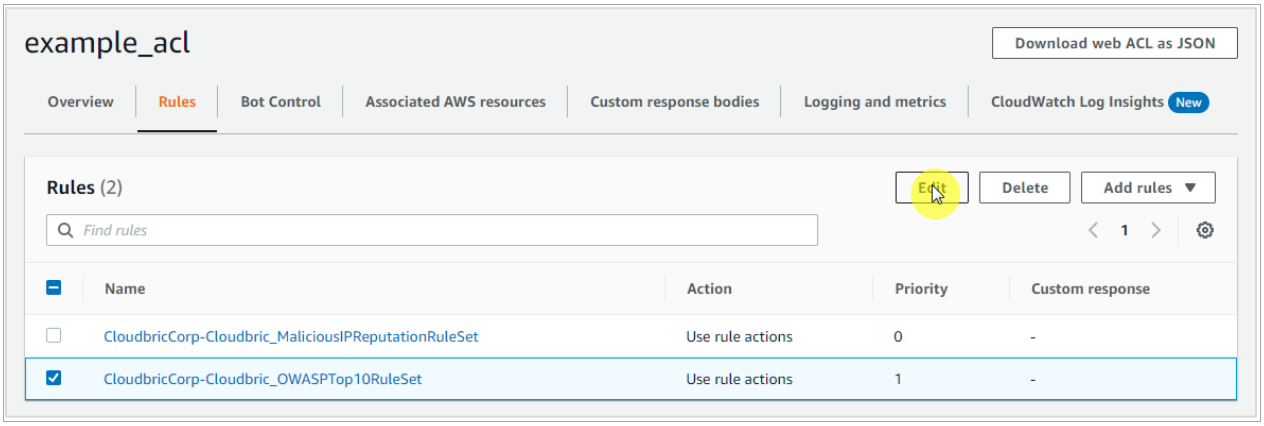
- **Step 1**
  Go to AWS WAF console.
  ※*AWS WAF console :* https://console.aws.amazon.com/wafv2/

- **Step 2**
  Go to the Web ACL menu and select the Web ACL for the Cloudbric Rule Set that the version is to be selected.

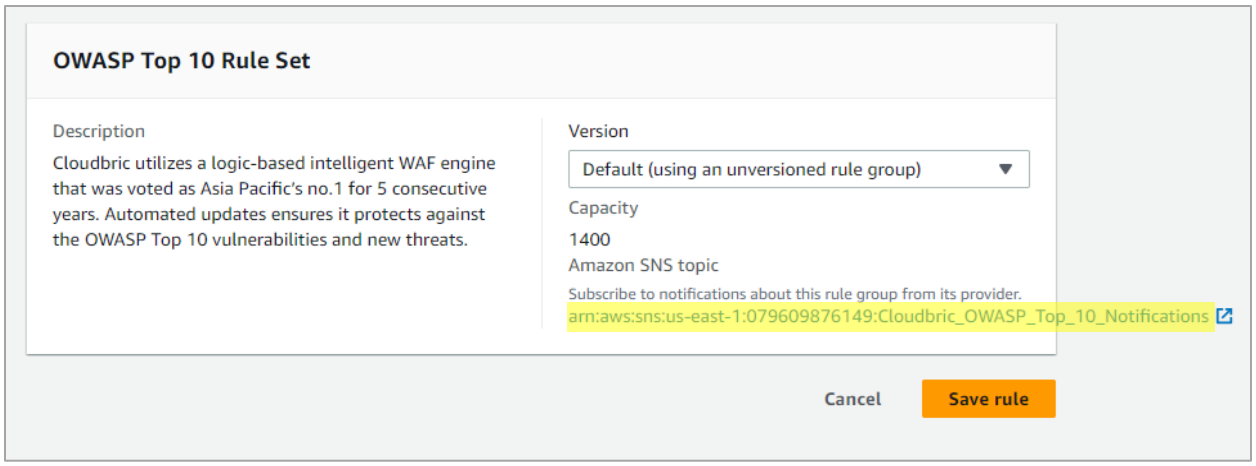


PUBLIC

- **Step 3**
  Select the **[Rules]** tab of the Web ACL, select the Cloudbric Rule Set to edt, and click **[Edit]**.



- **Step 4**
  Copy the Amazon Simple Notification Service (SNS) topic Amazon Resource Name (ARN) of the Cloudbric Rule Set, then click on the Amazon SNS topic ARN to change the settings for the update notifications of Amazon SNS.



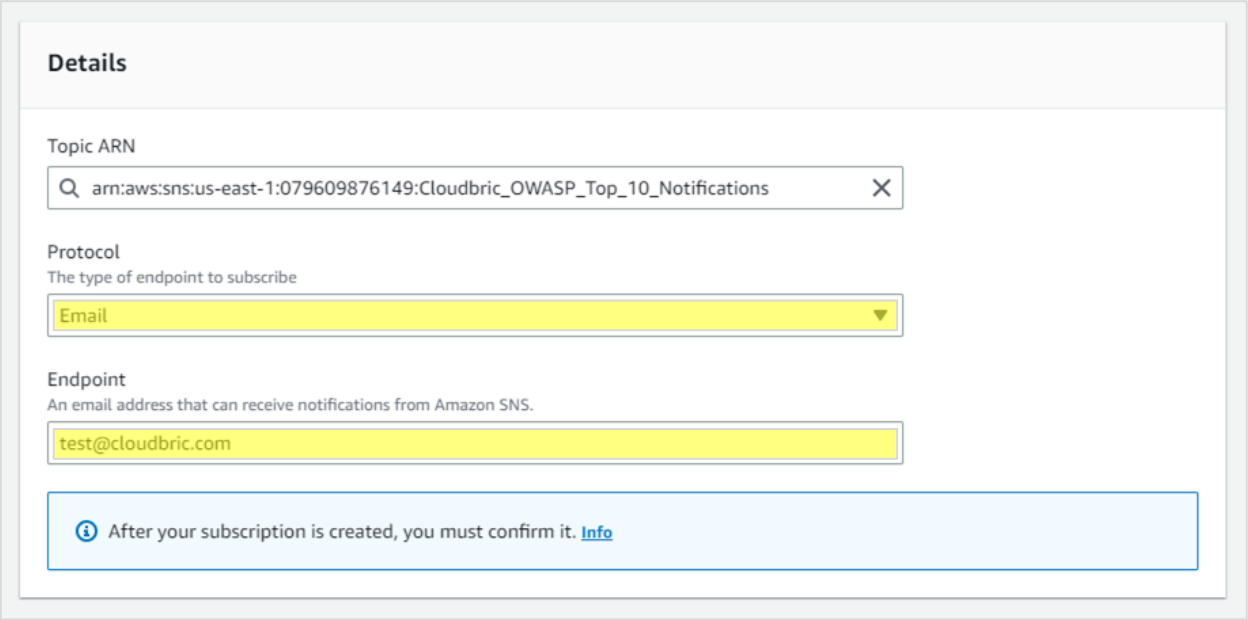
PUBLIC

- **Step 5**
  Enter the Protocol and Endpoint to receive the notifications of the updates.

-Topic ARN: Enter the Amazon SNS topic ARN that was copied from the previous step.

-Protocol: Enter Email.

-Endpoint: Enter an email address to receive notifications of the updates.



※If you wish to receive the update notifications through protocols other than email, please enter the endpoint that matches the protocol.

- **Step 6**
  Complete the process of changing the update notifications settings by clicking the **"Confirm subscription"** from the email sent to the email address you entered by AWS.

3. How to unsubscribe Cloudbric Rule Set

If you do wish to unsubscribe from Cloudbric Rule Set, the Cloudbric Rule Set must be deleted from all Web ACLs in the AWS WAF console, in addition to unsubscribing from the AWS Marketplace to stop the billing for the subscription of the Cloudbric Rule Set.

※You will be continued to be billed for the subscription if the Cloudbric Rule Set has not been deleted from the Web ACLs, even if the Cloudbric Rule Set has been unsubscribed.

※You may be billed for the use of Amazon Simple Notification Service (SNS) if the update notifications for Cloudbric Rule Set, if not deleted.

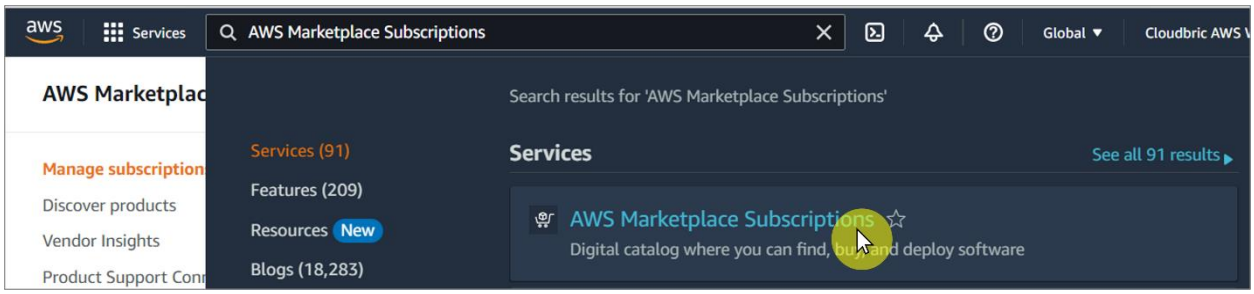
PUBLIC

3.1 Cancelling Cloudbric Rule Set subscription

- **Step 1**

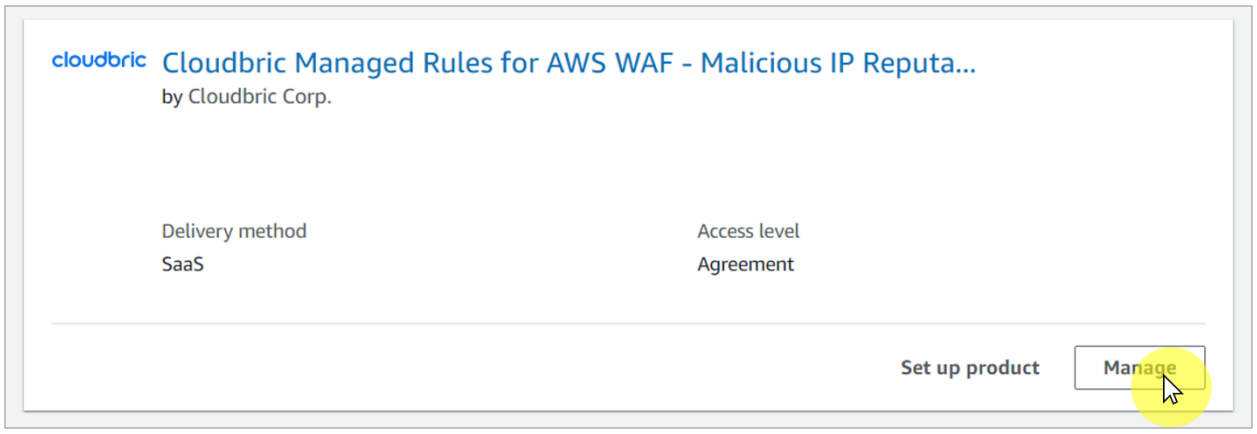
  Go to AWS Marketplace subscriptions management console.

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



- **Step 2**

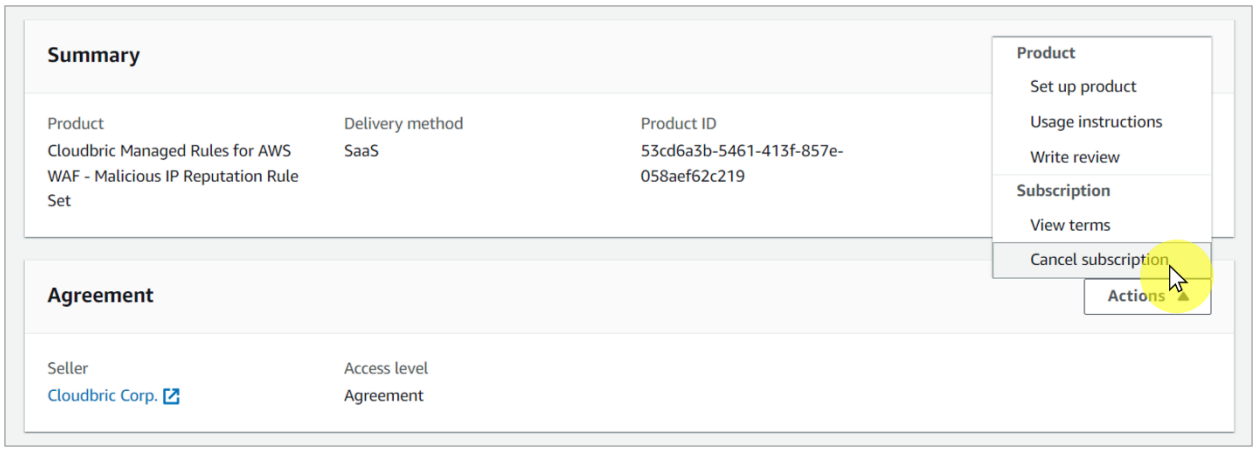
  Select **[Manage]** of the Cloudbric Rule Set to unsubscribe from the **[Manage subscriptions]** menu.



PUBLIC

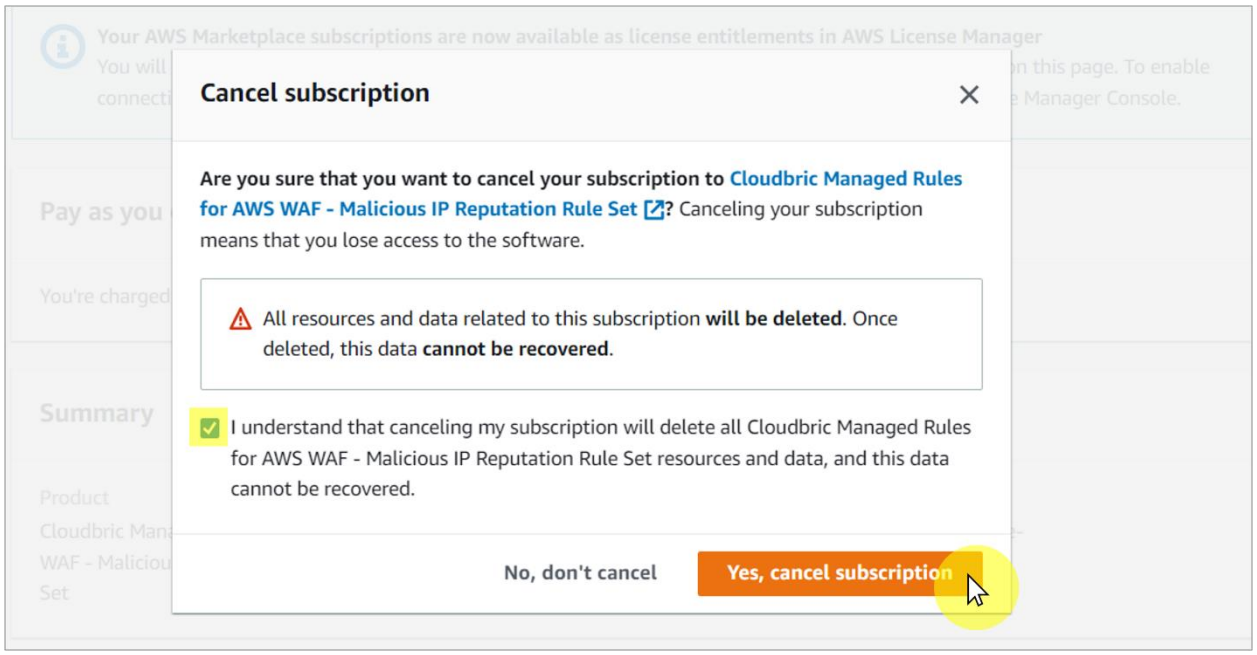
- **Step 3**

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



PUBLIC

3.2 Deleting Cloudbric Rule Set

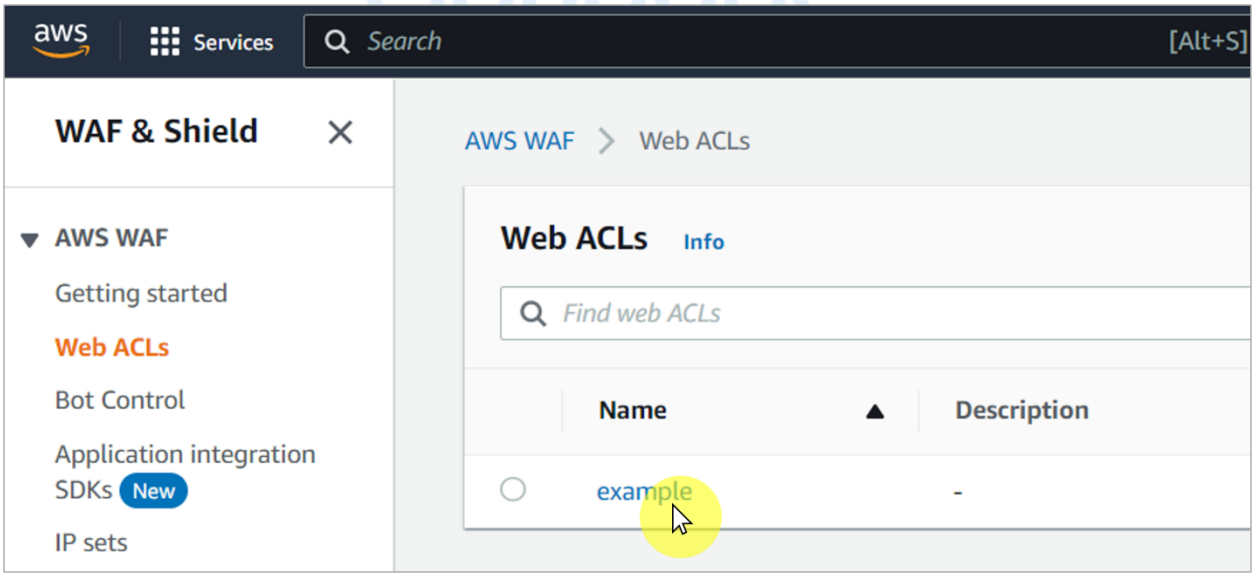
- **Step 1**

  Go to AWS WAF console.

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

- **Step 2**

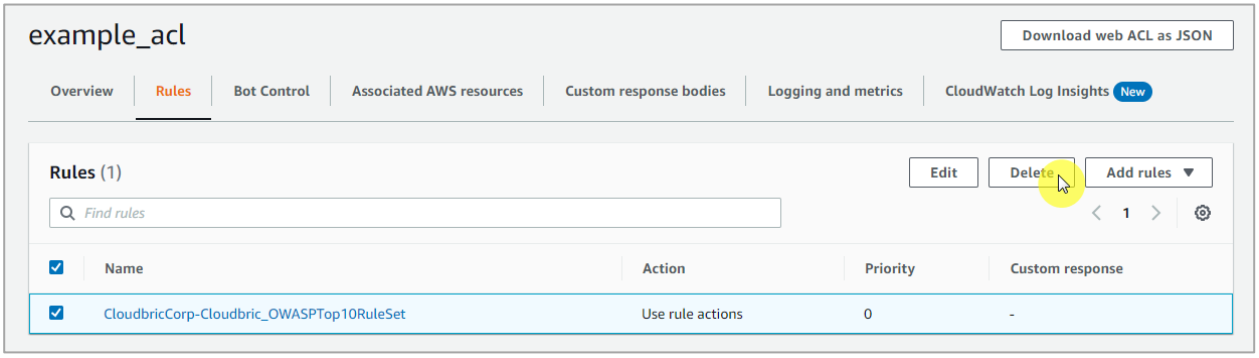
  Go to the Web ACL menu and select the Web ACL to delete the Cloudbric Rule Set.



PUBLIC

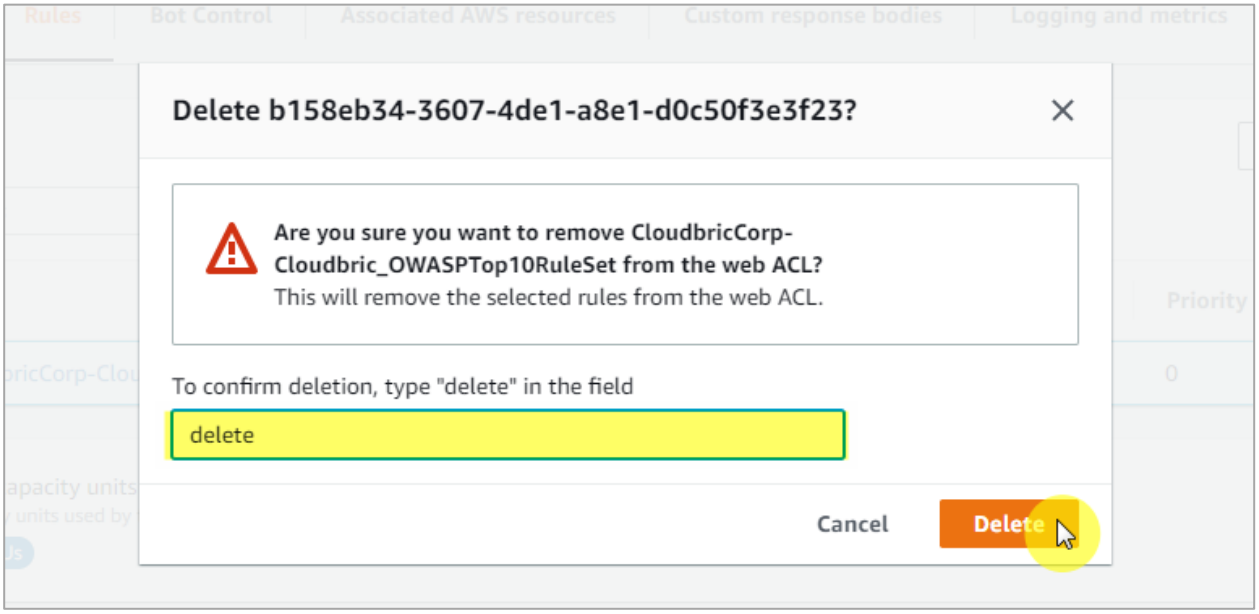
- **Step 3**

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



- **Step 4**

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

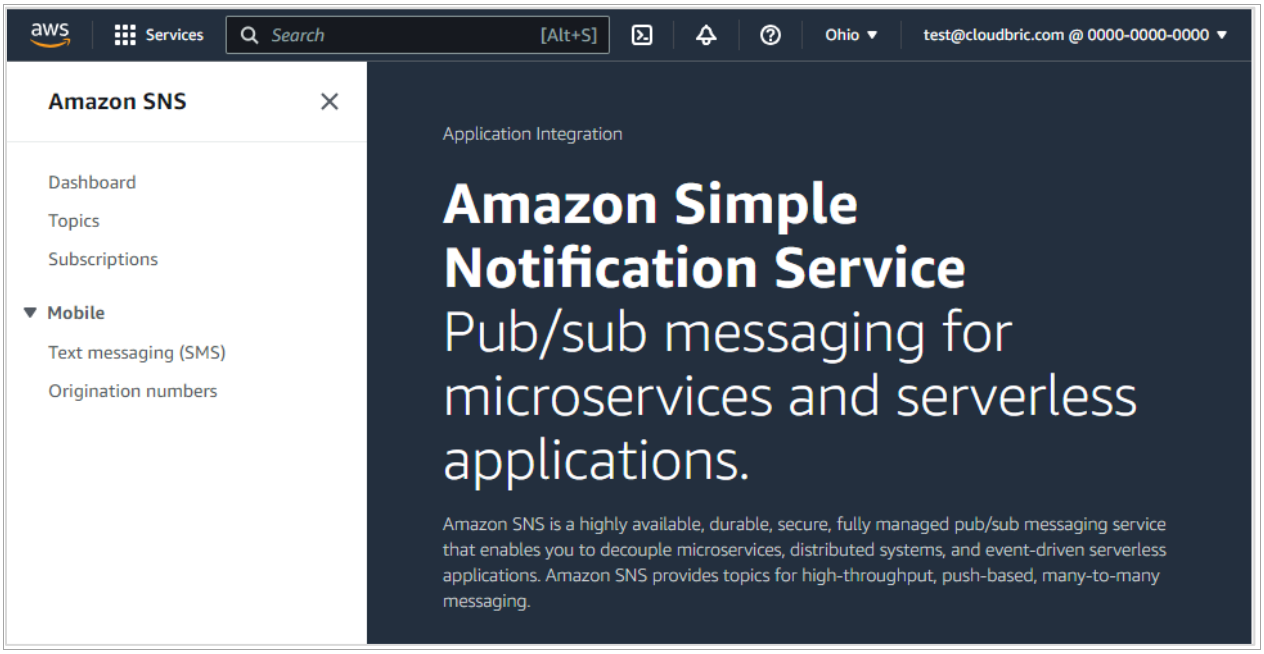


PUBLIC

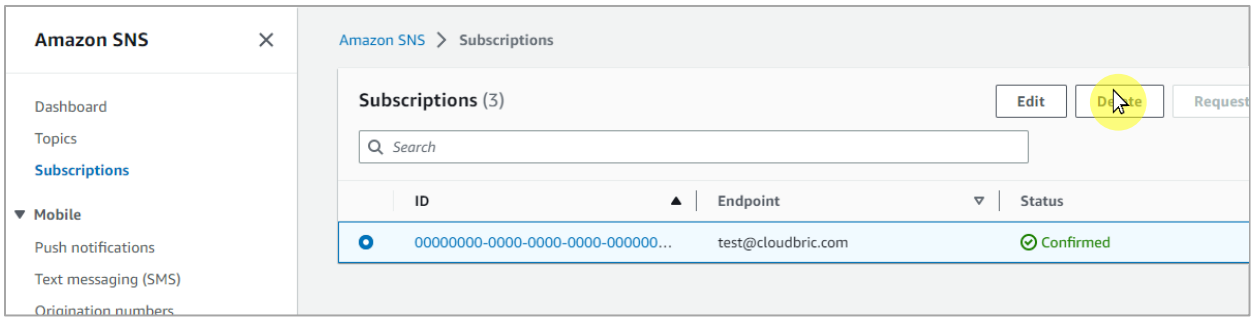
3.3 Deleting the update notifications for Cloudbric Rule Set

- **Step 1**
  Go to Amazon Simple Notification Service (SNS) console.

  ※ *Amazon SNS console:* https://console.aws.amazon.com/sns/home

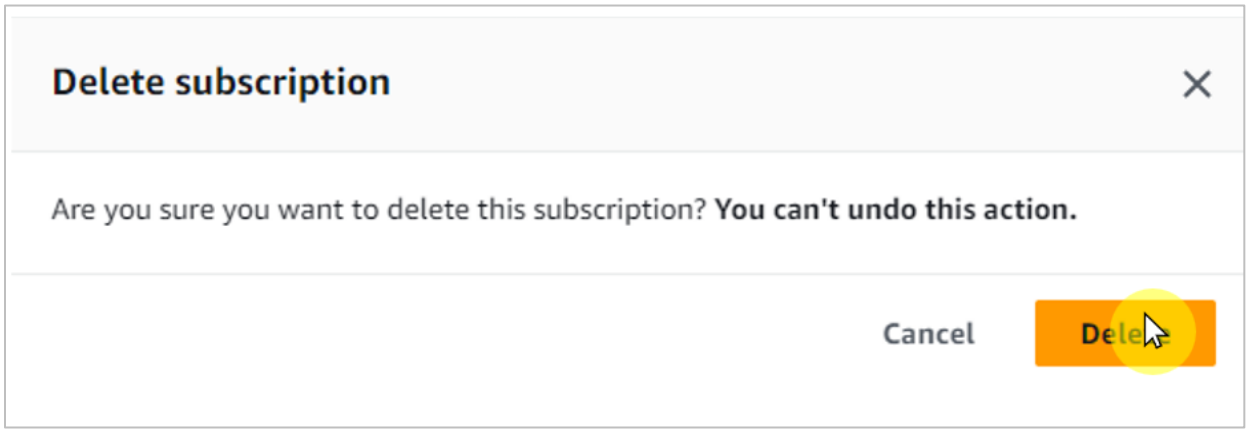


- **Step 2**
  Select the ID that is currently receiving the update notifications for the Cloudbric Rule Set from the Subscriptions menu and click **[Delete]**.



PUBLIC

- **Step 3**
  Click **[Delete]** to confirm the deletion of the update notifications.



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.

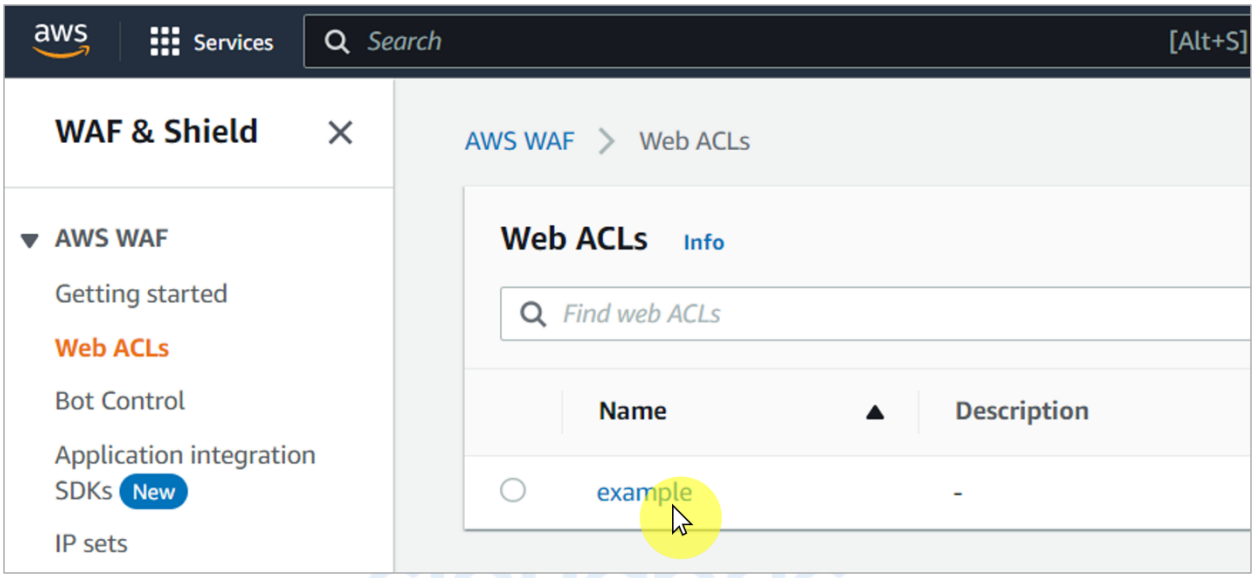
4.1 Configuring Rule Action 'Count'

- **Step 1**
  Go to AWS WAF console.
  ※AWS WAF console : https://console.aws.amazon.com/wafv2/

15 PUBLIC

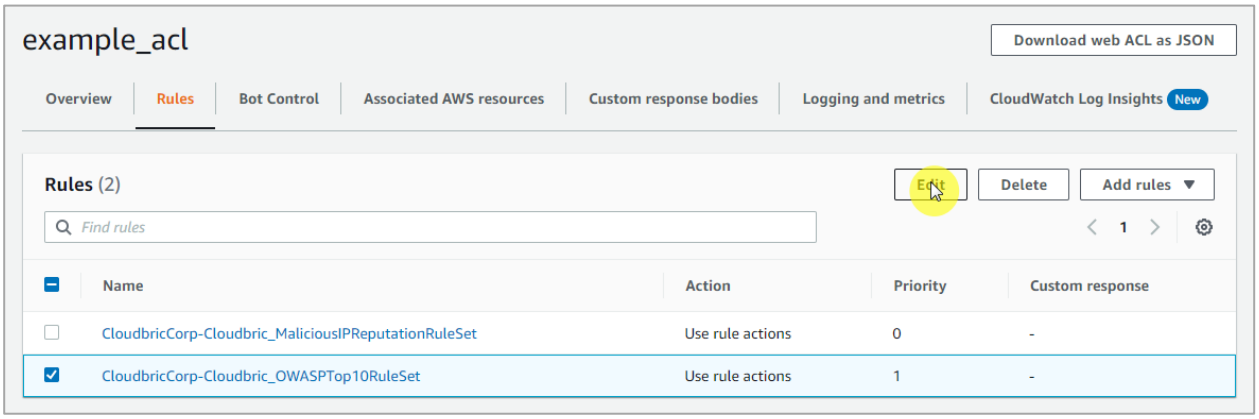
- **Step 2**

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



- **Step 3**

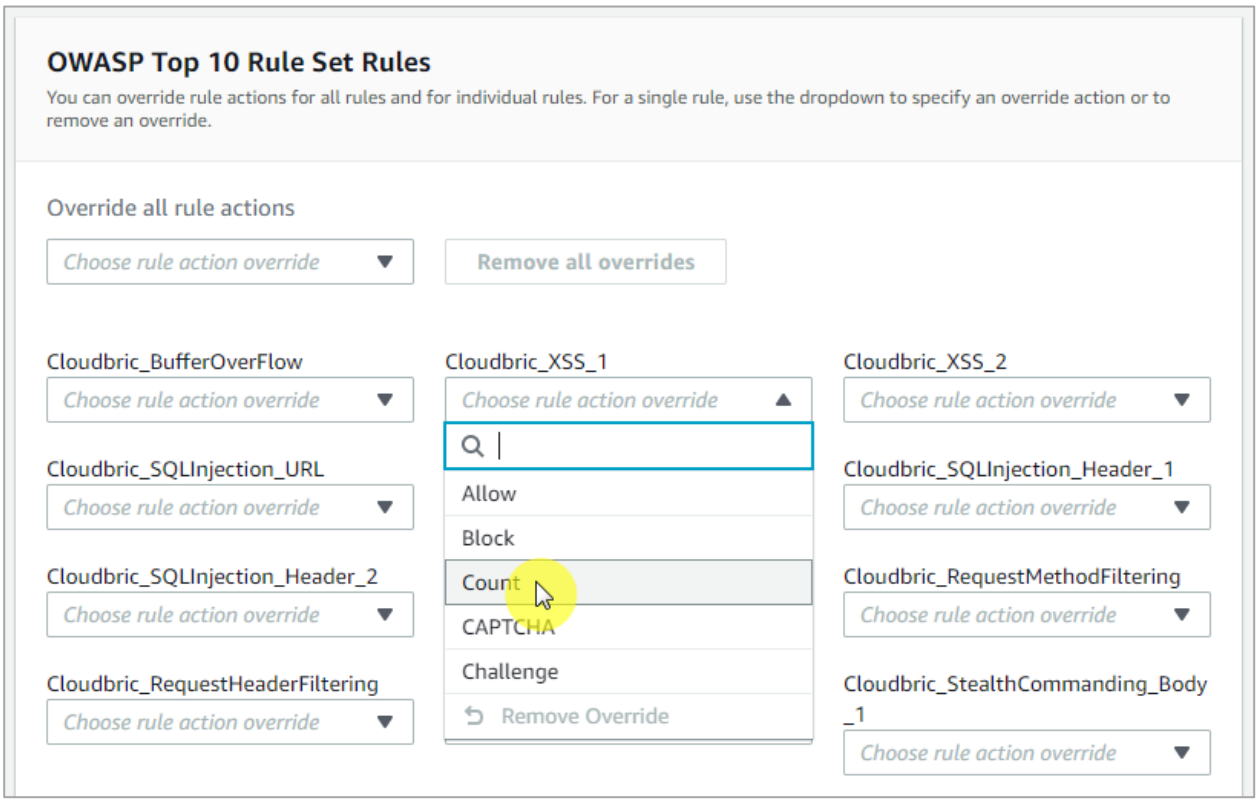
  Go to **[Rules]** tab, then select the Checkbox for all the Rule Sets to override and select **[Edit]**.



PUBLIC

- **Step 4**

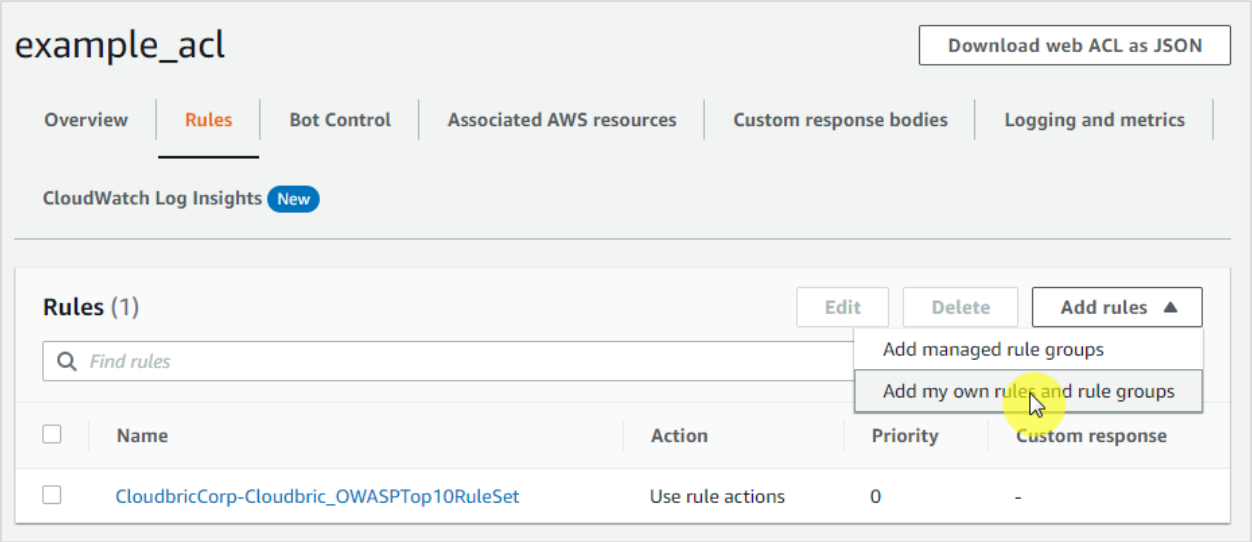
  Redefine the Action of the Rule to override to ‘Count’ and select **[Save rule]** to complete the override.



PUBLIC

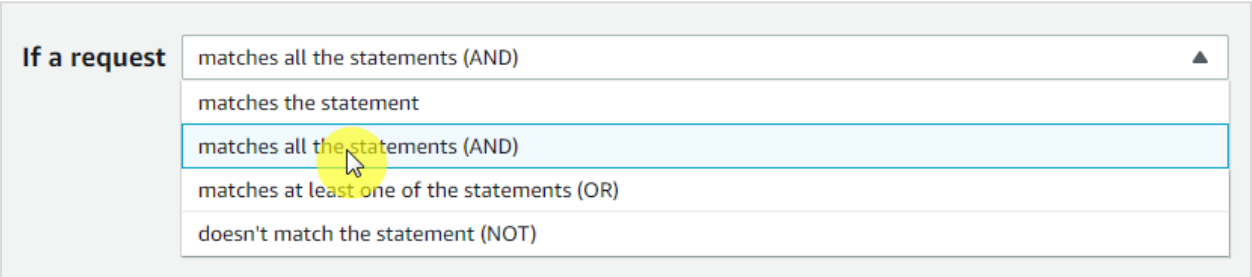
4.2 Adding Override Rules based on Labels

- **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.



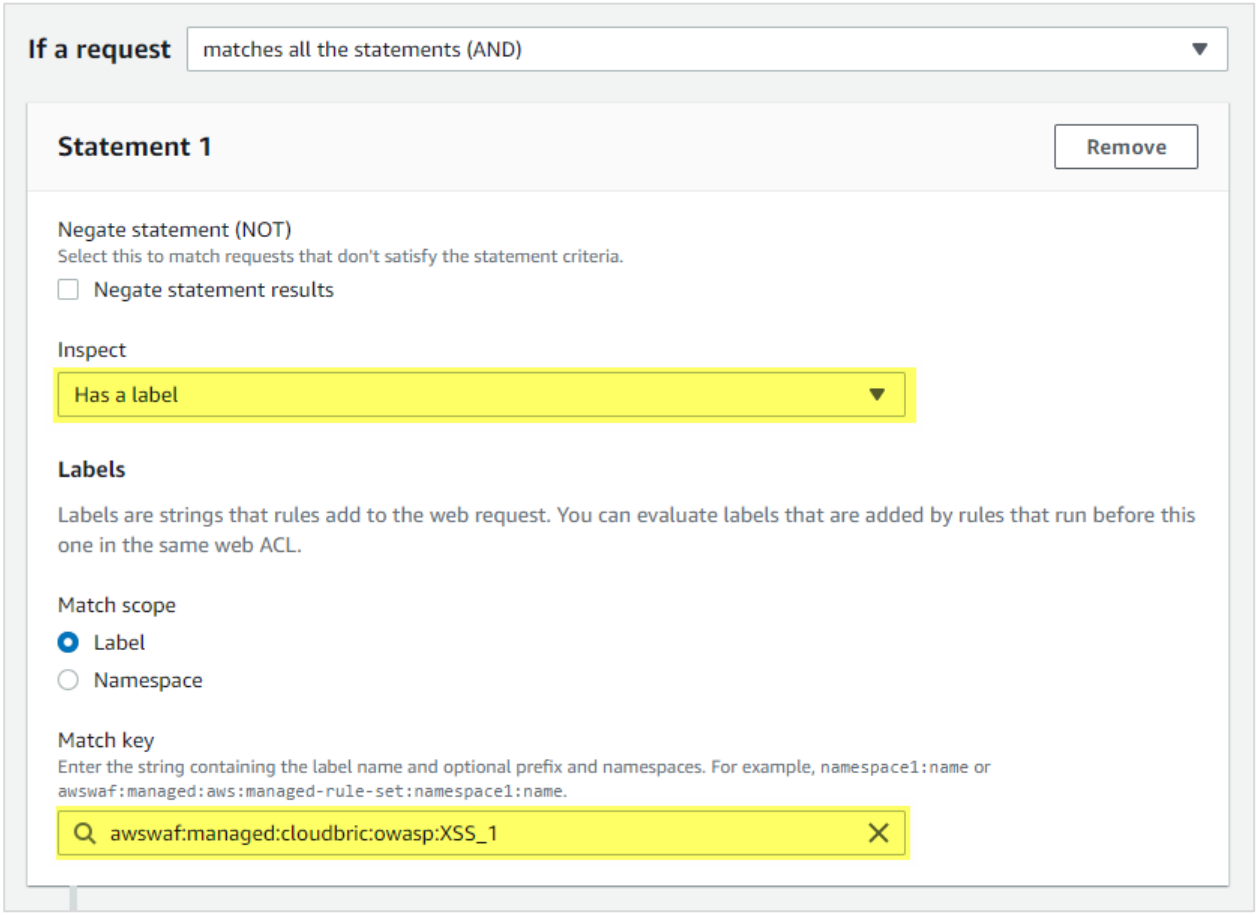
cloudbric

- **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)



15 PUBLIC

- **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

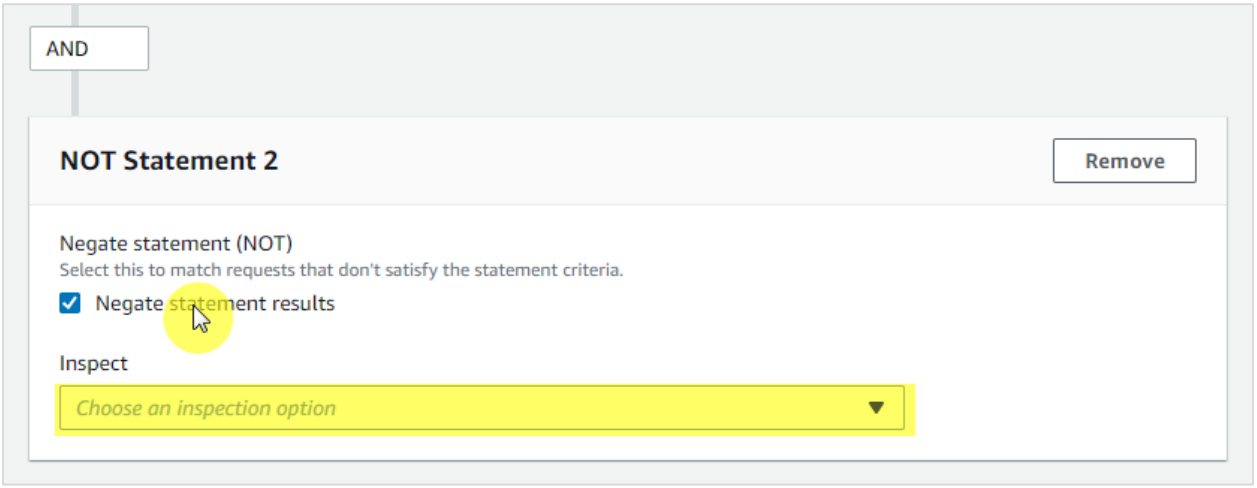


※*The structure of Label Name for Cloudbric OWASP Top 10 Rule Set :*

*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'***

PUBLIC

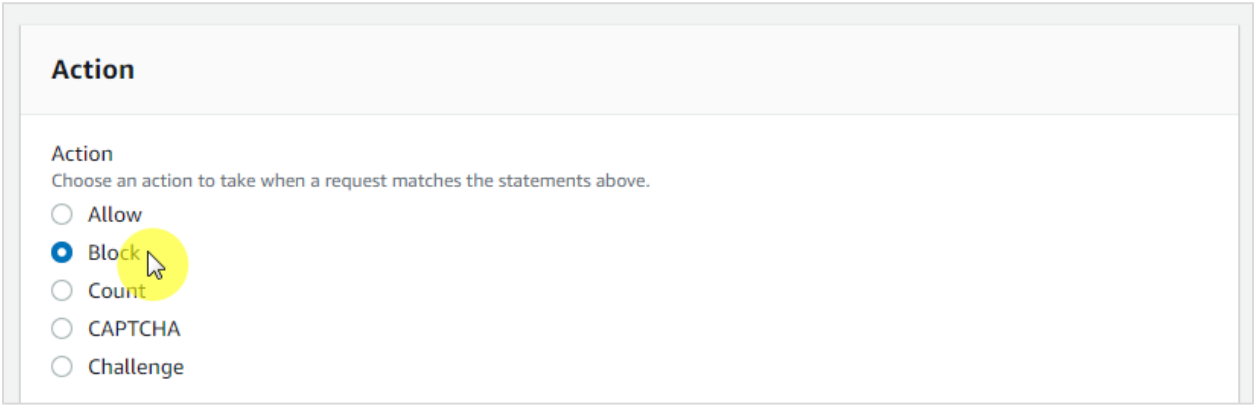
- **Step 4**
  Statement 2 is defined to override the inspection option for the request with the false-positive occurrence from the Rule configured to Override in 「4.1」.
  - Negate statement results: Configured to check to Override the inspection option defined in the statement.
  - Inspect: Configures the inspection option with the false-positive occurrences.



※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.

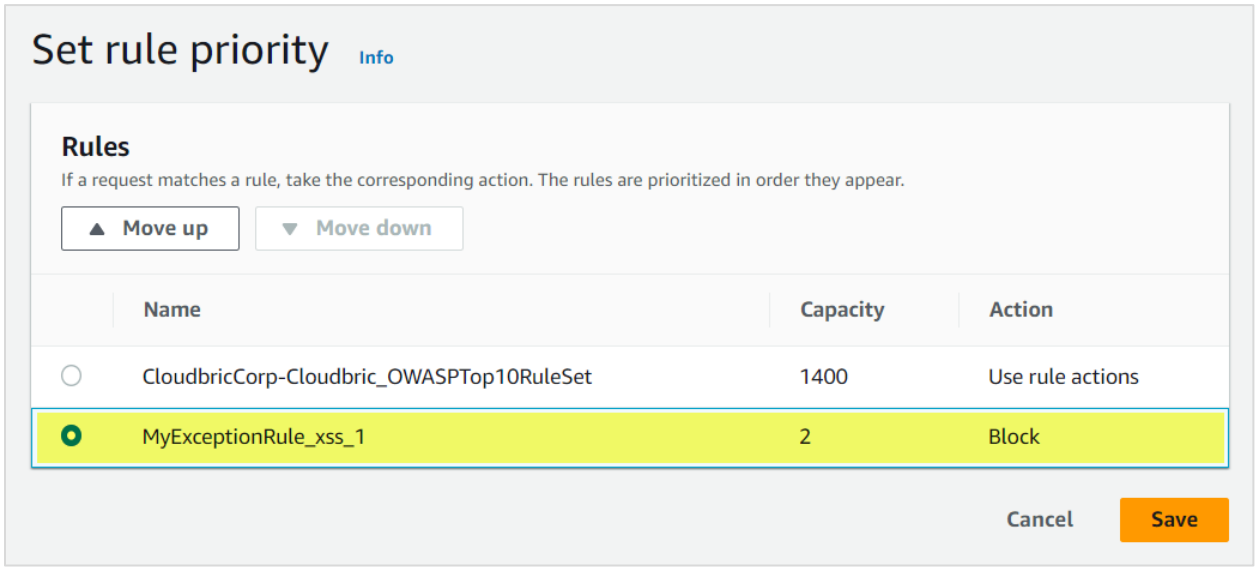
※Please contact awsmkp@cloudbric.com and provide the Log information if any false-positives occurred in the other Rules.

- **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.



PUBLIC

- **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.



cloudbric

PUBLIC

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

PUBLIC

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

PUBLIC

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/

PUBLIC

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)
  us-east-1 Region
  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)
  us-east-1 Region
  ① **Region Cost**: $25.00 * 1 = $25.00
  ② **Requests Cost**: $1.00(Per million) * 10 Requests(Total of 10million) = $10.00
  us-west-2 Region
  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

PUBLIC

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.

PUBLIC