



cloudbric

Cloudbric Rule Set for AWS WAF

세팅 가이드 v1.3 2023.08

FOR ENDUSER(PUBLIC)

변경 이력

갱신일	담당자	갱신내용	페이지	비고
2022.12	강수아	최초 작성		v 1.0
2023.05	강수아	Label 을 사용한 Rule 예외 처리 관련 내용 추가	14, 17, 22, 23	v 1.1
2023.06	배윤비	Tor IP Detection Rule Set 소개, Rule Set 버전 설정, 업데이트 알람 설정/삭제 관련 내용 추가	5, 11-16, 20, 21	v 1.2
2023.08	배윤비	Bot Protection Rule Set 소개	5	v 1.3

CONTENTS

1. Overview	04
- 1.1 Cloudbric Rule Set 이란?	04
- 1.2 Cloudbric Rule Set 종류	05
2. Cloudbric Rule Set 설정 방법	06
- 2.1 Cloudbric Rule Set 구독하기	06
- 2.2 Cloudbric Rule Set 적용하기	08
- 2.3 Cloudbric Rule Set 버전 선택하기	11
- 2.4 Cloudbric Rule Set 업데이트 알람 설정하기	13
3. Cloudbric Rule Set 해제 방법	16
- 3.1 Cloudbric Rule Set 구독 취소하기	16
- 3.2 Cloudbric Rule Set 삭제하기	18
- 3.3 Cloudbric Rule Set 업데이트 알람 삭제하기	20
4. Cloudbric Rule Set 예외 처리	22
- 4.1 Rule Action 'Count' 설정하기	22
- 4.2 Label 기반 예외 처리 Rule 추가하기	25
5. 부록	29
- 5.1 자주 하는 질문 (FAQ)	29
- 5.2 Cloudbric OWASP Top 10 Rule 유형 설명	33

1. Overview

본 문서는 클라우드브릭(주)이 AWS Marketplace 에서 판매하는 AWS WAF 관리형 규칙(Managed Rules)인 「Cloudbric Rule Set」을 구독하고 Web ACL 에 적용하는 방법을 설명하기 위해 작성되었습니다.

1.1 Cloudbric Rule Set 이란?

클라우드브릭에서 개발한 AWS WAF 관리형 규칙(Managed Rules)입니다. 클라우드브릭은 아마존 웹 서비스(AWS, Amazon Web Service)의 엄격한 기술적 평가를 통과한 국내 최초이자 유일한 AWS WAF Ready Program 론칭 파트너입니다. Cloudbric Rule Set 은 20 년 이상의 풍부한 보안 경험과 축적된 노하우로 개발되었으며 안정적인 보안 수준을 유지하기 위해 지속적으로 갱신 및 관리하고 있습니다.

AWS WAF 관리형 규칙(Managed Rules)이란?

AWS Marketplace 판매자가 AWS WAF 사용자를 위해 작성하고 유지 및 관리하는 사전 정의된 WAF 보안 규칙 모음입니다. AWS WAF 사용자는 직접 규칙을 작성할 필요 없이 AWS Marketplace 를 통해 구독만 하면 즉시 사용이 가능하며 일반적인 위협으로부터 웹 애플리케이션 또는 API 를 빠르게 보호할 수 있습니다.

1.2 Cloudbric Rule Set 종류:

이름	설명
OWASP Top 10 Rule Set 구독하러 바로가기	5 년 연속 아시아 태평양 시장 점유율 1 등 웹 방화벽 탐지 엔진을 탑재한 Cloudbric WAF+의 지능형 탐지 모듈을 구현한 구성으로 지능형 탐지 모듈은 수백만 개의 로그에서 비정상적인 패턴과 동작을 정확히 감지하여 OWASP Top 10 에 속한 SQL Injection, Cross Site Scripting(XSS) 등 웹 취약점으로부터 보호합니다.
Malicious IP Reputation Rule Set 구독하러 바로가기	Cloudbric Labs 의 95 개국 700,000 개 이상 사이트에서 매일 수집 및 가공되는 위협 인텔리전스 기반의 IP 평판 데이터를 활용한 구성으로 광범위하고 다양한 위협을 식별하는데 필요한 시간을 줄이고 위험도 높은 IP 를 사전 차단하여 피해를 예방하는데 도움을 줍니다.
Tor IP Detection Rule Set 구독하러 바로가기	분산형 릴레이 네트워크를 통해 인터넷 트래픽을 라우팅하여 트래픽의 출처를 익명화하는 Tor 브라우저가 불법적인 목적으로 사용되는 경우의 피해를 방지하는 데 도움을 주어 웹사이트 및 웹 애플리케이션에 대한 위협을 줄입니다.
Bot Protection Rule Set 구독하러 바로가기	악의성을 지닌 반복 작업 및 특정 작업을 실행하는 악성 Bot 의 트래픽을 탐지하고 차단하여 계정 탈취 (ATO, Account Takeover), 스크래핑, 애플리케이션 DDoS 등 광범위한 악성 Bot 에 의한 공격을 방어하여 피해를 예방합니다.

2. Cloudbric Rule Set 설정 방법

AWS WAF 에서 Cloudbric Rule Set 을 설정하려면 먼저 AWS Marketplace 를 통해 Cloudbric Rule Set 을 구독해야 합니다. 구독이 완료되면 AWS WAF 콘솔에서 Web ACL 에 Cloudbric Rule Set 을 적용할 수 있습니다. 또한 Cloudbric Rule Set 의 버전 선택과 Amazon SNS(Simple Notification Service)을 통한 업데이트 알람을 설정할 수 있습니다.

2.1 Cloudbric Rule Set 구독하기

• Step 1

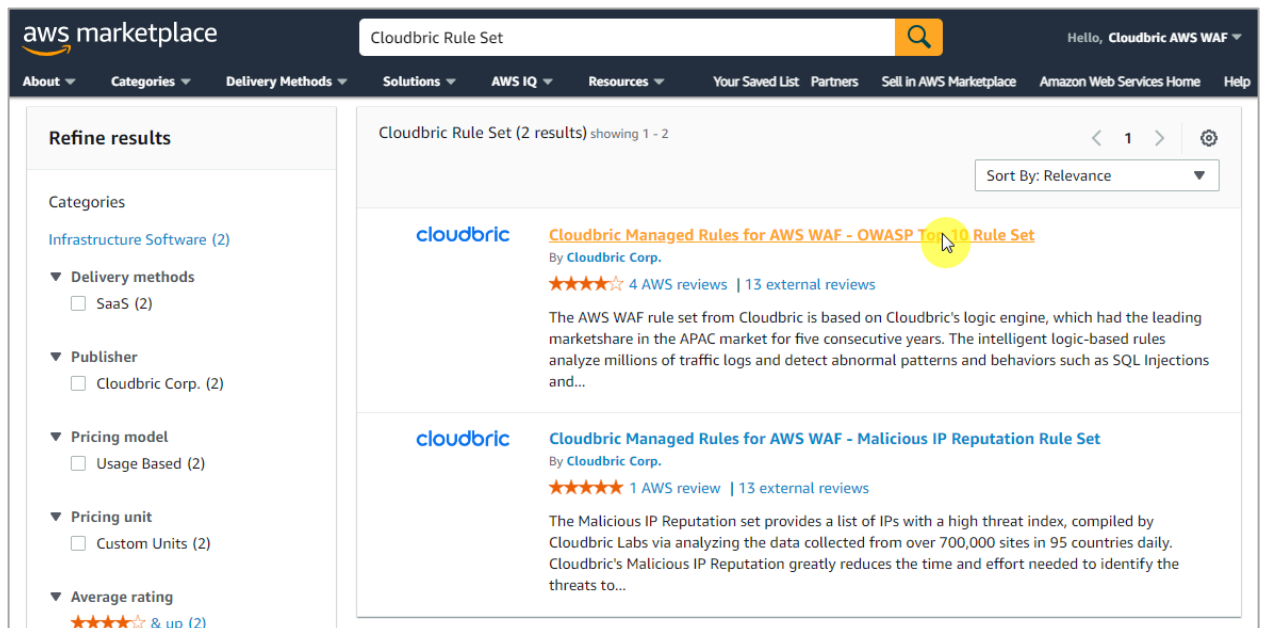
AWS Marketplace 에 접속 후 AWS 계정으로 로그인합니다.

※ AWS Marketplace: <https://aws.amazon.com/marketplace/>



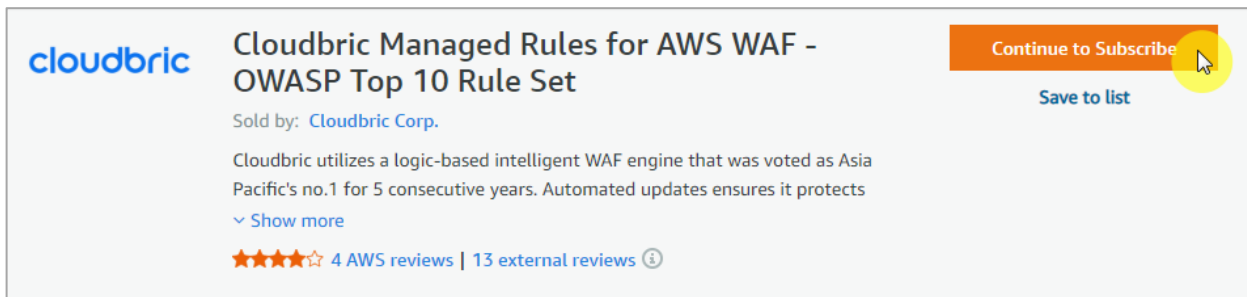
• Step 2

검색창에 'Cloudbric Rule Set'를 검색 후 구독이 필요한 제품 이름을 선택합니다.



- Step 3

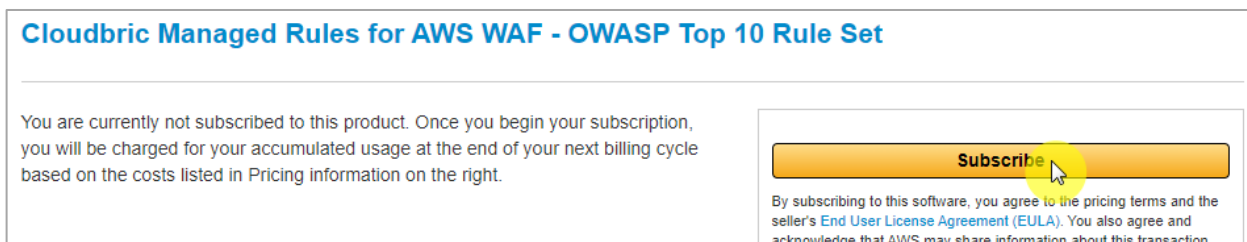
선택한 제품의 세부 정보를 확인 후 **[Continue to Subscribe]** 버튼을 선택합니다.



The screenshot shows the product page for 'Cloudbric Managed Rules for AWS WAF - OWASP Top 10 Rule Set'. The Cloudbric logo is on the left. The product title is in bold. Below it, it says 'Sold by: Cloudbric Corp.' and a description: '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'. There is a 'Show more' link and a star rating with '4 AWS reviews | 13 external reviews'. On the right, there is an orange 'Continue to Subscribe' button with a mouse cursor pointing at it, and a blue 'Save to list' link below it.

- Step 4

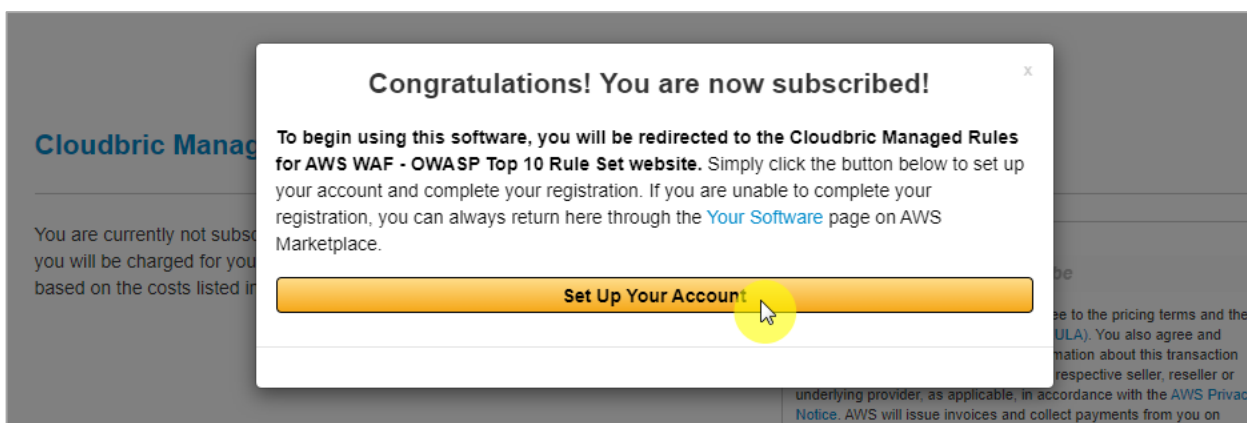
구독 약관과 가격 정보를 확인 후 **[Subscribe]** 버튼을 선택하여 구독을 완료합니다.



The screenshot shows the subscription confirmation page. The title is 'Cloudbric Managed Rules for AWS WAF - OWASP Top 10 Rule Set'. The main text states: '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.' On the right, there is a large orange 'Subscribe' button with a mouse cursor pointing at it. Below the button, there is a disclaimer: '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

Cloudbric Rule Set 구독이 완료되었습니다. 이제 Cloudbric Rule Set 을 적용하기 위해 **[Set Up Your Account]** 버튼을 선택하여 AWS WAF 콘솔로 이동합니다.



The screenshot shows a 'Congratulations! You are now subscribed!' dialog box. The text inside says: '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.' At the bottom of the dialog is a large orange 'Set Up Your Account' button with a mouse cursor pointing at it. The background shows a blurred view of the subscription page.

2.2 Cloudbric Rule Set 적용하기

- Step 1

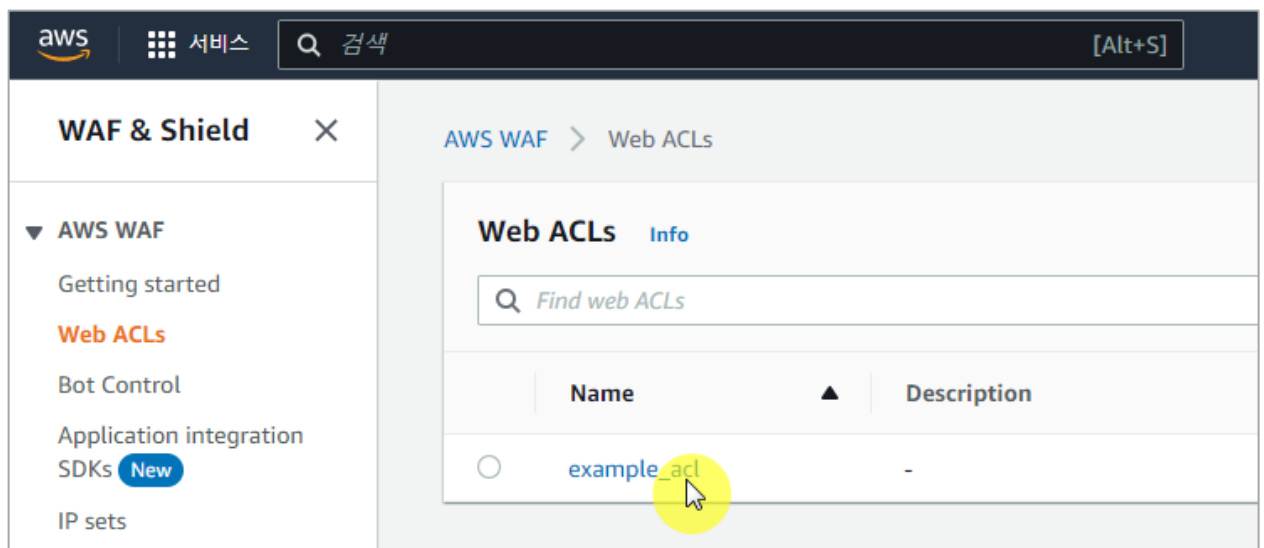
AWS WAF 콘솔에 접속합니다.

※ AWS WAF 콘솔: <https://console.aws.amazon.com/wafv2/>



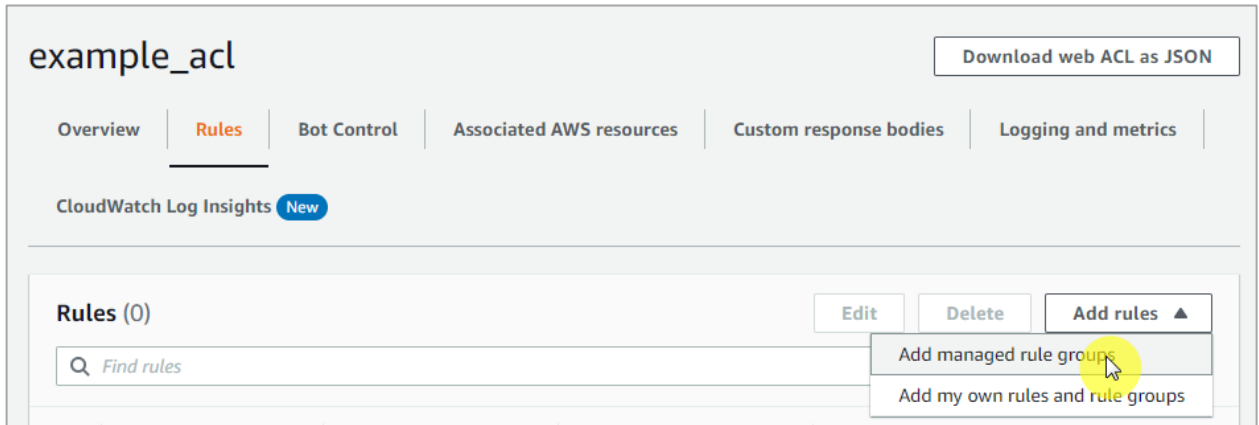
- Step 2

Web ACL 메뉴에서 Cloudbric Rule Set 을 적용할 Web ACL 이름을 선택합니다.



- Step 3

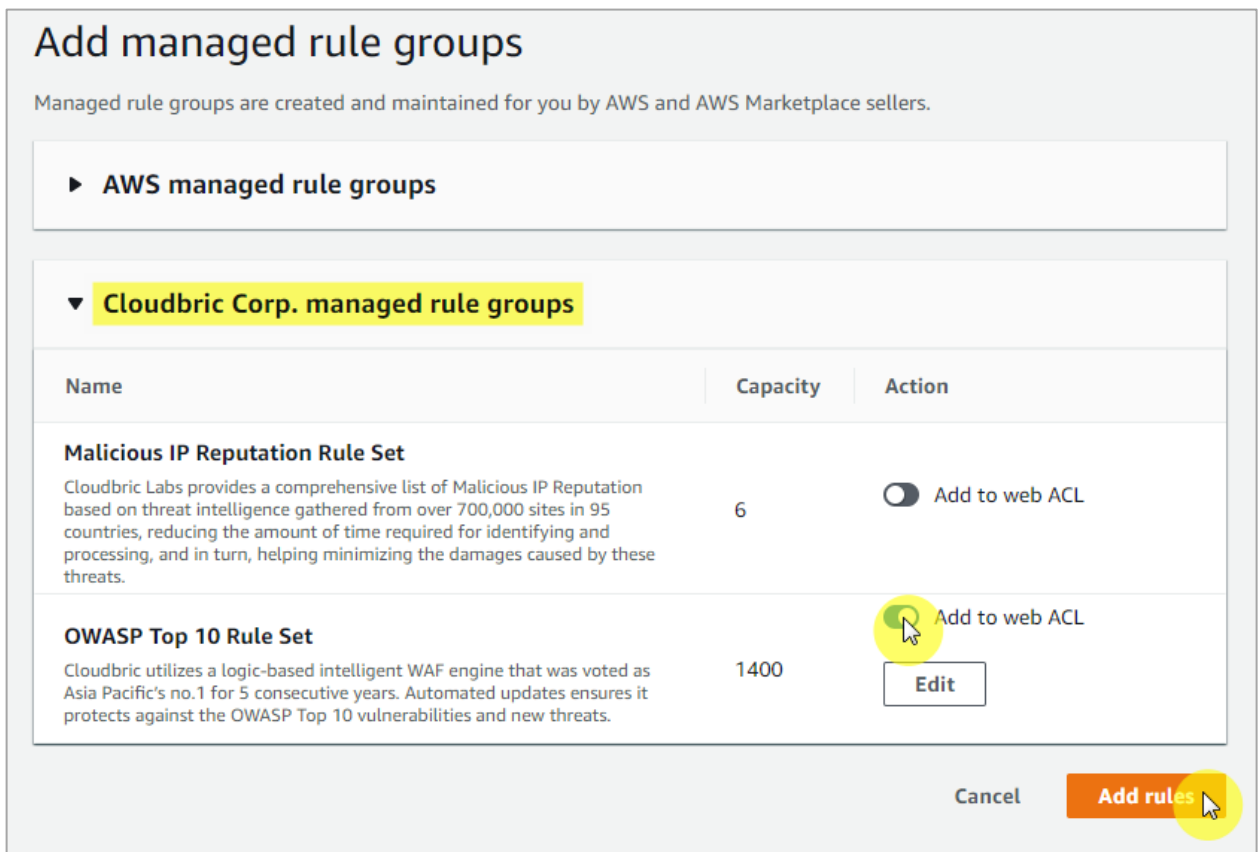
해당 Web ACL 의 **[Rules]** 탭으로 이동한 뒤 **[Add rules]** 버튼에서 **[Add managed rule groups]**을 선택합니다.



- Step 4

구독한 Cloudblic Rule Set 을 활성화한 뒤 **[Add rules]** 버튼을 선택합니다.

※ 테스트를 먼저 진행하려면 **[Edit]** 버튼을 선택한 뒤 Rule 의 Action 을 'count'로 재 정의하시면 됩니다.



- Step 5

Cloudbric Rule Set 을 모두 활성화할 경우 **Malicious IP Reputation Rule Set** 이 먼저 적용되도록 우선순위(Priority)를 설정한 뒤 **[Save]** 버튼을 선택하여 적용을 완료합니다.

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 checked="" type="radio"/>	CloudbricCorp-Cloudbric_MaliciousIPReputationRuleSet	6	Use rule actions
<input type="radio"/>	CloudbricCorp-Cloudbric_OWASPTop10RuleSet	1400	Use rule actions

[Cancel](#) [Save](#)

- Step 6

Web ACL 의 **[Rules]** 탭에서 **Cloudbric Rule Set** 이 적용된 것을 확인합니다.

Success
You successfully updated the web ACL example_acl.

AWS WAF > Web ACLs > example_acl

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 (2) [Edit](#) [Delete](#) [Add rules ▼](#)

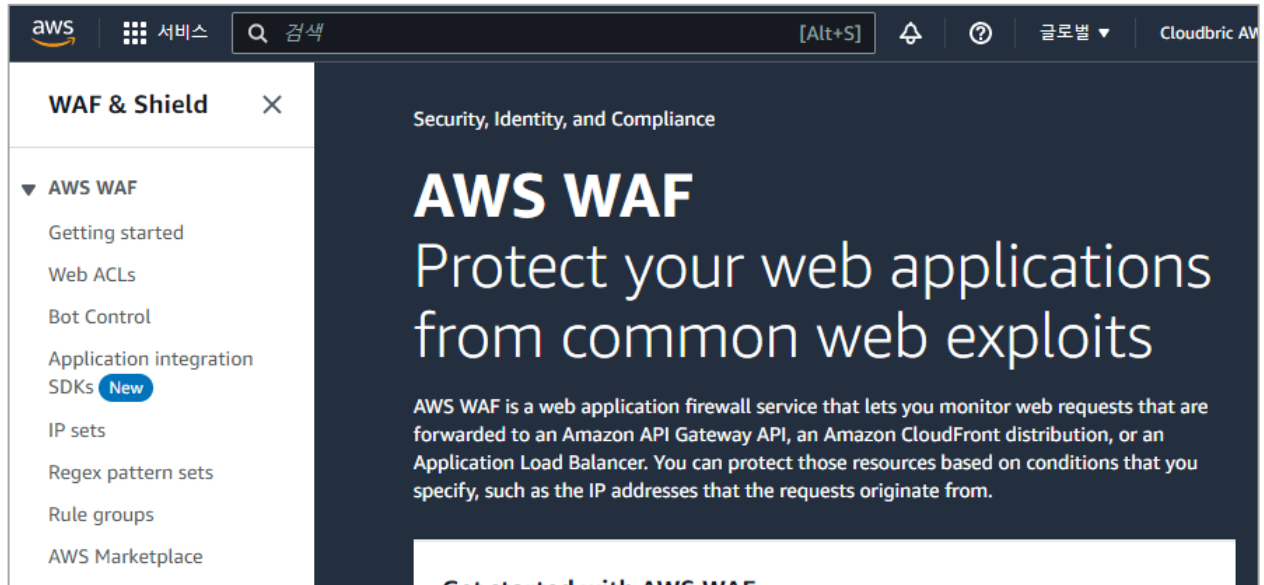
<input type="checkbox"/>	Name	Action	Priority	Custom response
<input type="checkbox"/>	CloudbricCorp-Cloudbric_MaliciousIPReputationRuleSet	Use rule actions	0	-
<input type="checkbox"/>	CloudbricCorp-Cloudbric_OWASPTop10RuleSet	Use rule actions	1	-

2.3 Cloudbric Rule Set 버전 선택하기

- Step 1

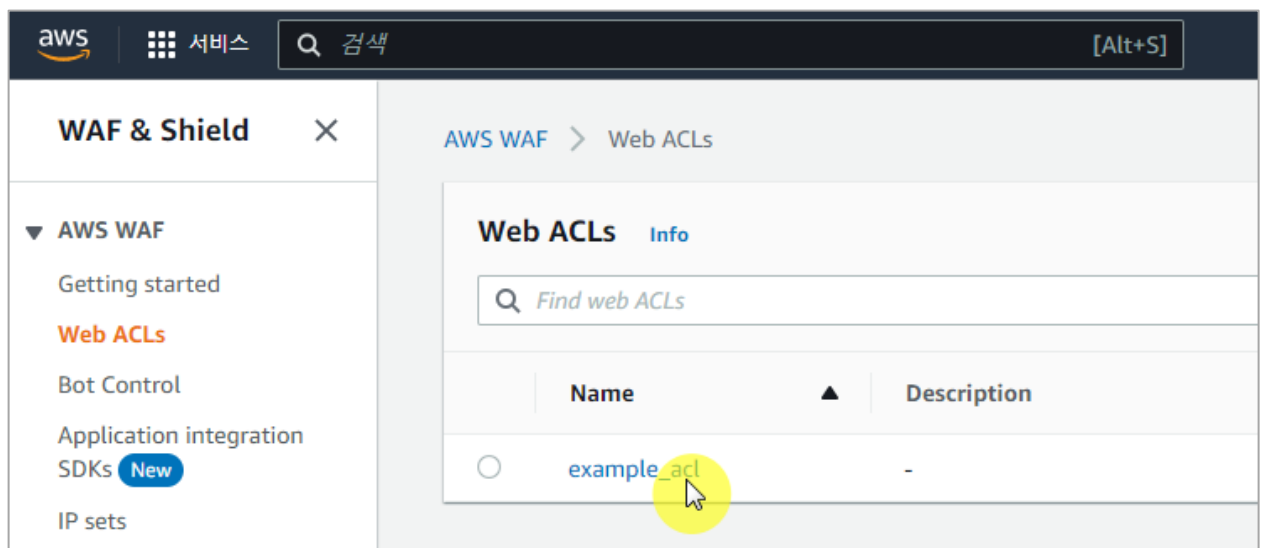
AWS WAF 콘솔에 접속합니다.

※ AWS WAF 콘솔: <https://console.aws.amazon.com/wafv2/>



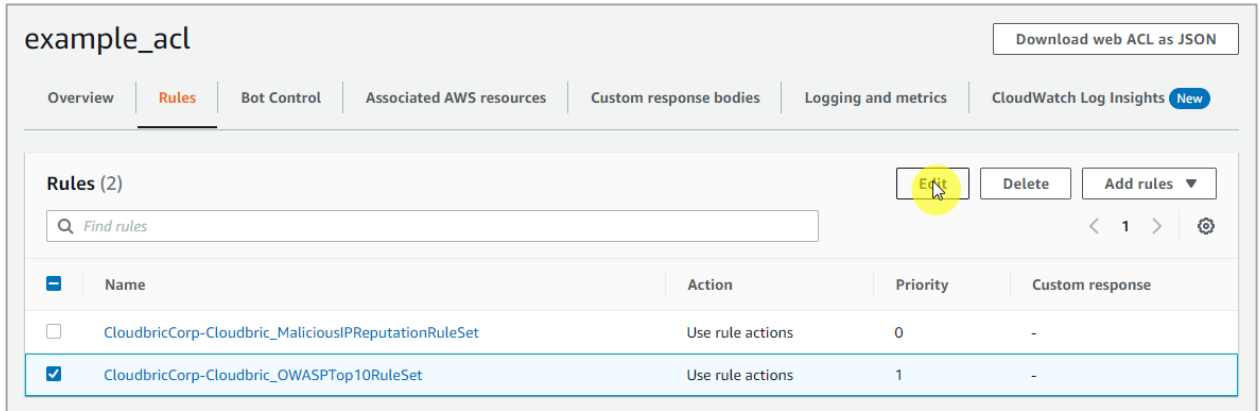
- Step 2

Web ACL 메뉴에서 Cloudbric Rule Set 의 버전을 선택할 Web ACL 이름을 선택합니다.



• Step 3

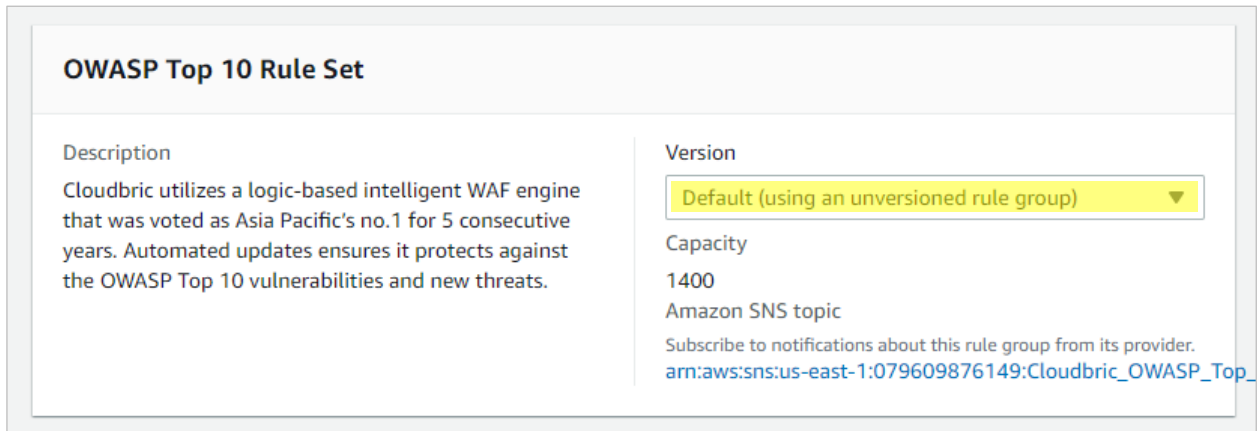
해당 Web ACL 의 **[Rules]** 탭으로 이동한 뒤 Cloudbric Rule Set 을 체크하고 **[Edit]** 버튼을 선택합니다.



※ 현재, 버전 설정 기능은 OWASP Top 10 Rule Set 에 한하여 제공하고 있습니다.

• Step 4

이용하고자 하는 Cloudbric Rule Set 의 버전을 선택 후, **[Save rule]** 버튼을 선택하여 설정을 완료합니다.



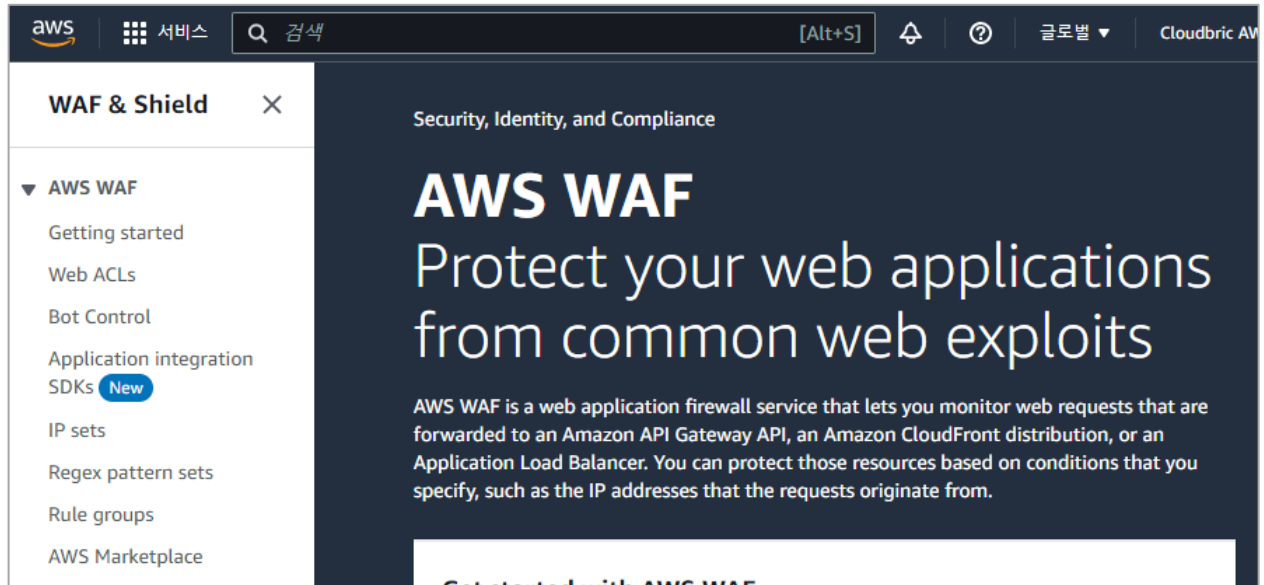
※ 현재는 Default(가장 최신 버전)만을 제공하고 있으며, 추후 Rule 의 주요 업데이트 따라 기존 버전을 제공할 예정입니다.

2.4 Cloudblic Rule Set 업데이트 알람 설정하기

- Step 1

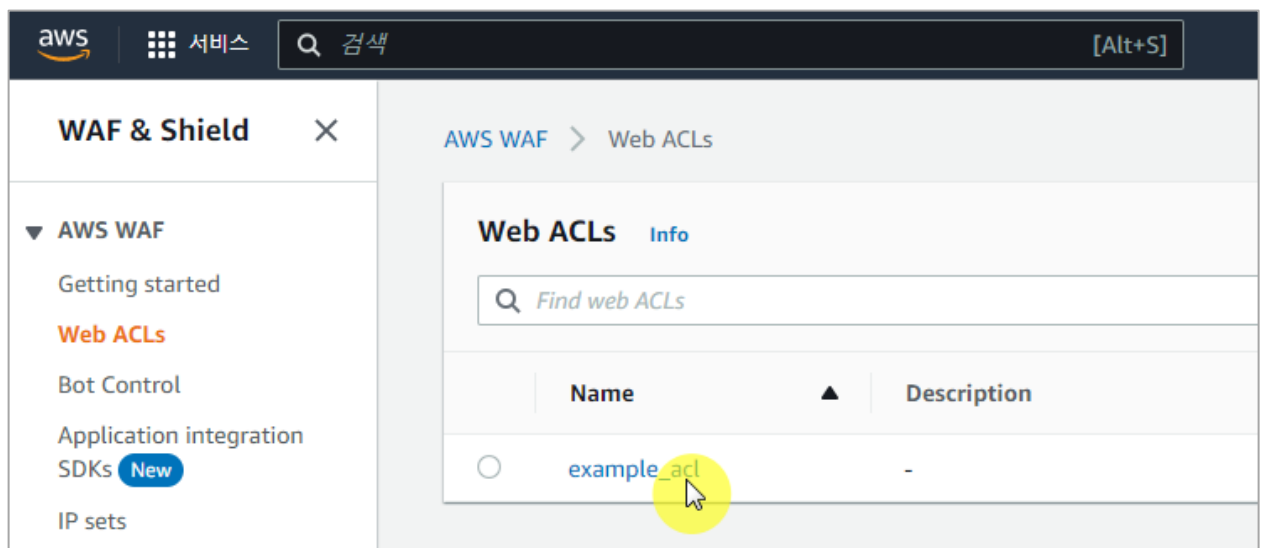
AWS WAF 콘솔에 접속합니다.

※ AWS WAF 콘솔: <https://console.aws.amazon.com/wafv2/>



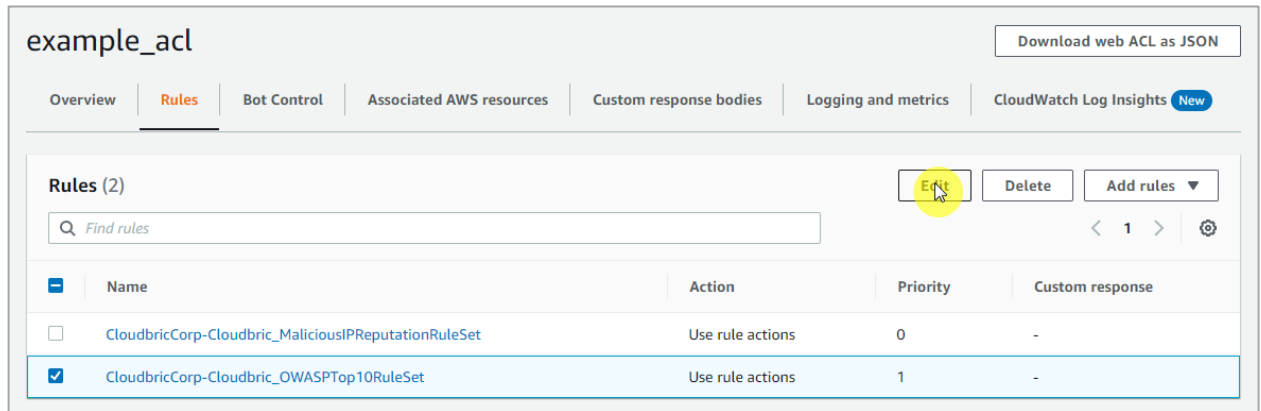
- Step 2

Web ACL 메뉴에서 Cloudblic Rule Set 의 버전을 선택할 Web ACL 이름을 선택합니다.



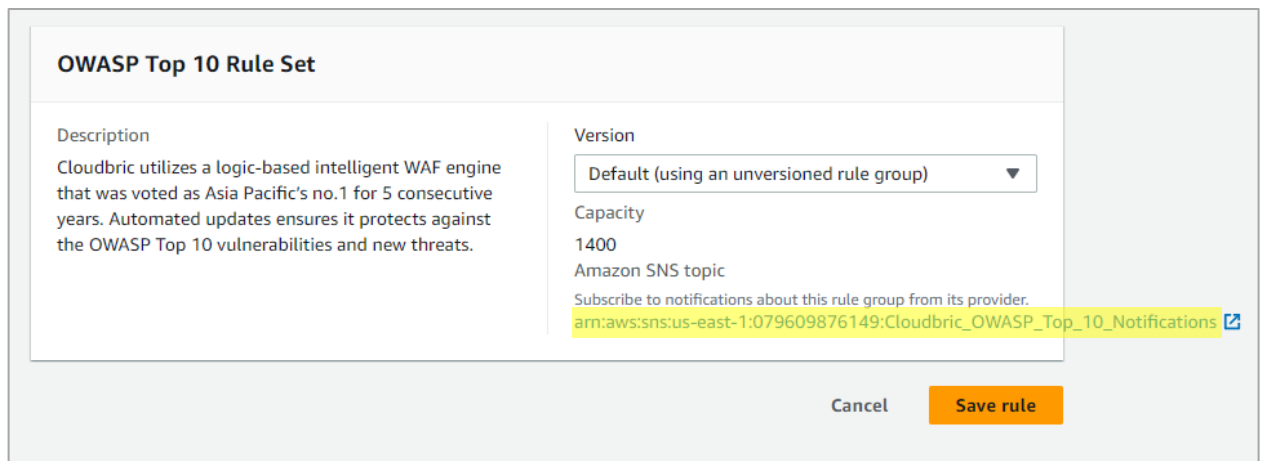
- Step 3

해당 Web ACL 의 [Rules] 탭으로 이동한 뒤 Cloudbric Rule Set 을 체크하고 [Edit] 버튼을 선택합니다.



- Step 4

Cloudbric Rule Set 의 Amazon SNS(Simple Notification Service) topic ARN(Amazon Resource Name)을 드래그 하여 복사한 뒤, Amazon SNS topic ARN 을 선택해 Amazon SNS 의 업데이트 알림 등록 페이지로 이동합니다.



- Step 5

Cloudbric Rule Set 의 업데이트 알람을 받기위한 Protocol 과 Endpoint 를 입력합니다.

-Topic ARN: 복사한 Cloudbric Rule Set 의 Amazon SNS topic ARN 을 입력.

-Protocol: Email 선택.

-Endpoint: 업데이트 알람을 수신할 이메일 주소를 입력.

Amazon SNS

Dashboard
Topics
Subscriptions

▼ Mobile
Push notifications
Text messaging (SMS)
Origination numbers

Details

Topic ARN
arn:aws:sns:us-east-1:079609876149:Cloudbric_OWASP_Top_10_Notifications

Protocol
The type of endpoint to subscribe
Email

Endpoint
An email address that can receive notifications from Amazon SNS.
test@cloudbric.com

After your subscription is created, you must confirm it. Info

※ Email 외의 Protocol 을 통해 업데이트 알람을 이용할 경우, 설정한 Protocol 에 맞는 Endpoint 를 입력해주세요.

- Step 6

입력한 이메일 주소로 전송된 AWS 의 인증 메일에서 'Confirm subscription'을 선택하여 업데이트 알람 설정을 완료합니다.

You have chosen to subscribe to the topic:
arn:aws:sns:us-east-1:000000000000:cloudbric

To confirm this subscription, click or visit the link below (If this was in error no action is necessary):
[Confirm subscription](#)

Please do not reply directly to this email. If you wish to remove yourself from receiving all future SNS subscription confirmation requests please send an email to [sns-opt-out](#)

3. Cloudbric Rule Set 해제 방법

Cloudbric Rule Set 을 더 이상 사용하지 않을 경우 구독 요금이 부과되지 않으려면 AWS Marketplace 구독 취소와 함께 AWS WAF 콘솔의 모든 Web ACL 에서 Cloudbric Rule Set 을 삭제해야 합니다. 또한 Cloudbric Rule Set 의 업데이트 알림을 받고 있다면 알림에 대한 요금이 부과되지 않도록 Amazon SNS(Simple Notification Service)에서 Cloudbric Rule Set 의 업데이트 알림을 삭제해야 합니다.

※ Web ACL 에 적용된 Cloudbric Rule Set 이 남아있고 구독만 취소할 경우 요금이 지속적으로 청구됩니다.

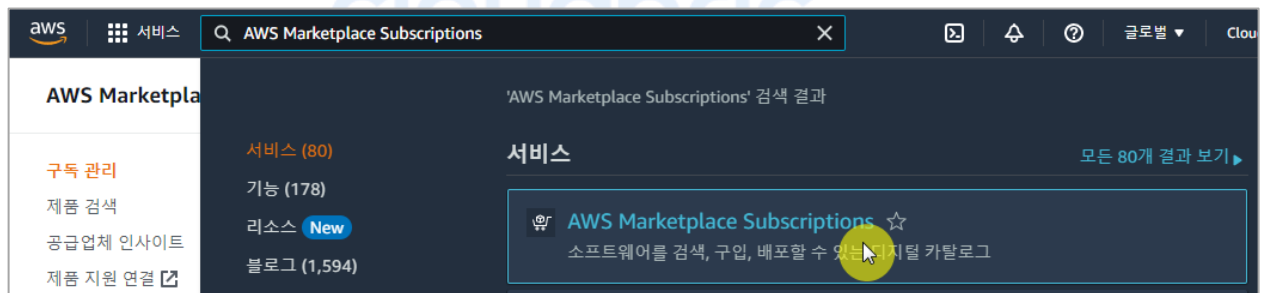
※ Amazon SNS(Simple Notification Service)에서 Cloudbric Rule Set 의 업데이트 알림을 삭제하지 않으면 알림 설정 이용에 대한 요금이 청구될 수 있습니다.

3.1 Cloudbric Rule Set 구독 취소하기

- Step 1

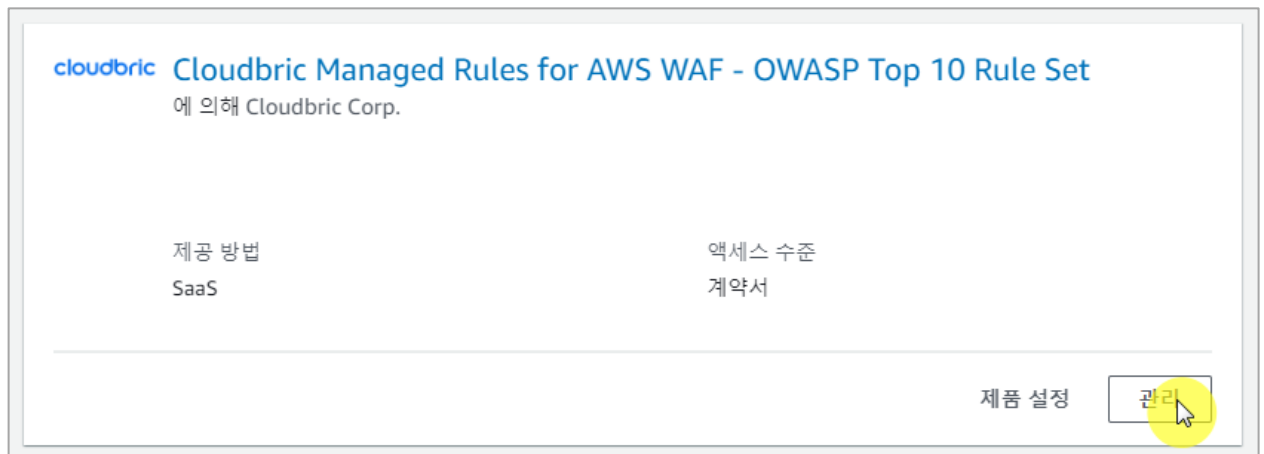
AWS Marketplace 구독 관리 콘솔에 접속합니다.

※ AWS WAF 콘솔: <https://console.aws.amazon.com/marketplace/home#/subscriptions>



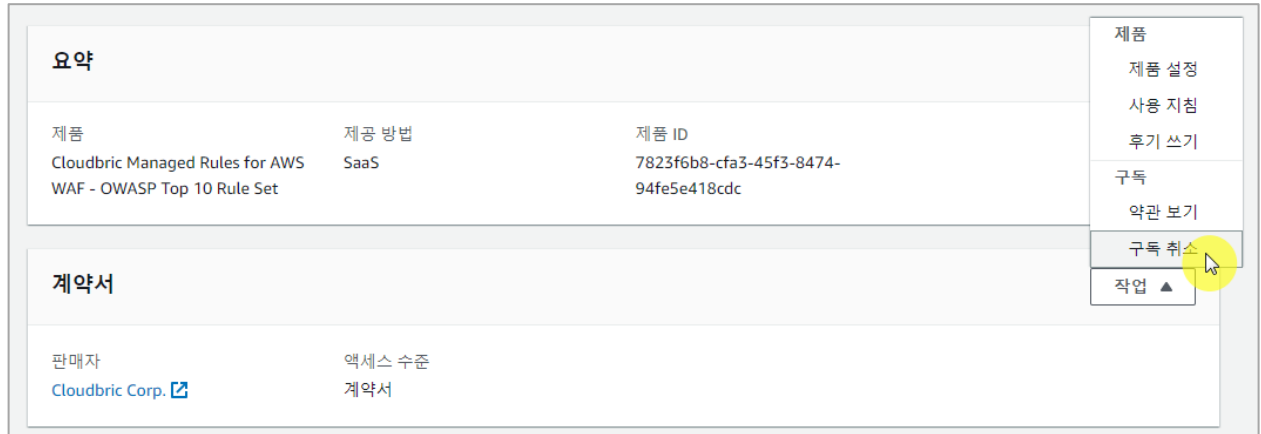
- Step 2

[구독 관리] 메뉴에서 구독을 취소할 Cloudbric Rule Set 의 [관리] 버튼을 선택합니다.



• Step 3

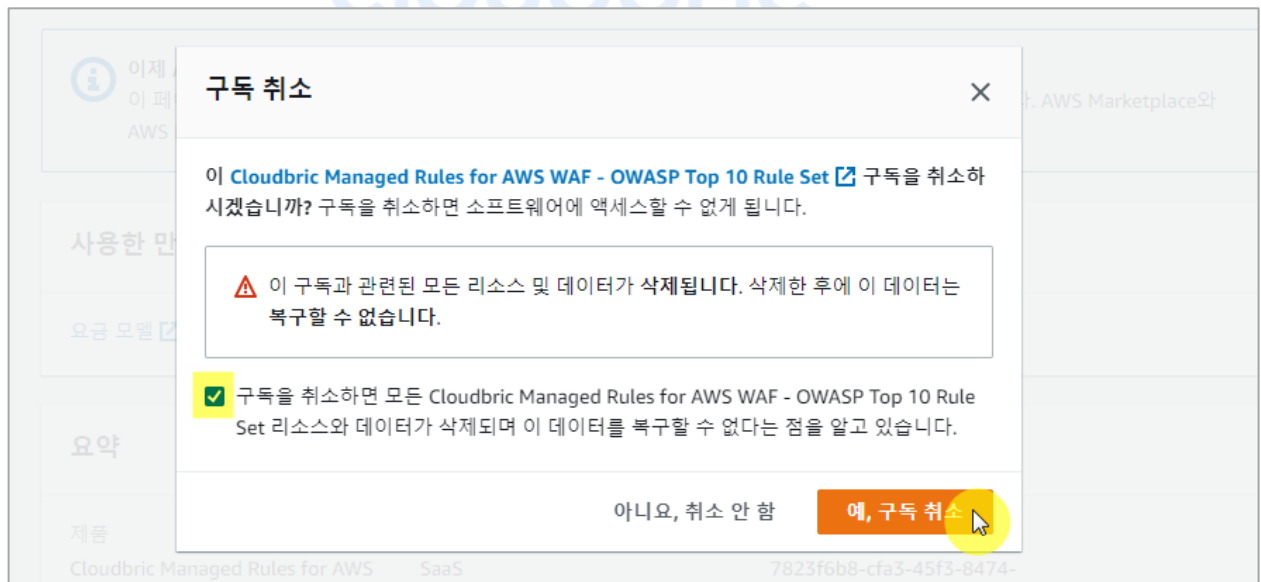
하단의 '계약서' 정보 오른쪽의 [작업]에서 [구독 취소]를 선택합니다.



The screenshot shows a product page for 'Cloudbric Managed Rules for AWS WAF - OWASP Top 10 Rule Set'. The '계약서' (Contract) section is visible, showing the seller as 'Cloudbric Corp.' and the access level as '계약서'. A dropdown menu is open on the right, with '구독 취소' (Cancel Subscription) highlighted by a yellow circle.

• Step 4

데이터 복구 불가 안내 내용 확인에 체크한 뒤 [예, 구독 취소] 버튼을 선택하여 구독 취소를 완료합니다.



The screenshot shows a confirmation dialog box titled '구독 취소' (Cancel Subscription). The dialog contains the following text:

이 [Cloudbric Managed Rules for AWS WAF - OWASP Top 10 Rule Set](#) 구독을 취소하시겠습니까? 구독을 취소하면 소프트웨어에 액세스할 수 없게 됩니다.

⚠ 이 구독과 관련된 모든 리소스 및 데이터가 삭제됩니다. 삭제한 후에 이 데이터는 복구할 수 없습니다.

☒ 구독을 취소하면 모든 Cloudbric Managed Rules for AWS WAF - OWASP Top 10 Rule Set 리소스와 데이터가 삭제되며 이 데이터를 복구할 수 없다는 점을 알고 있습니다.

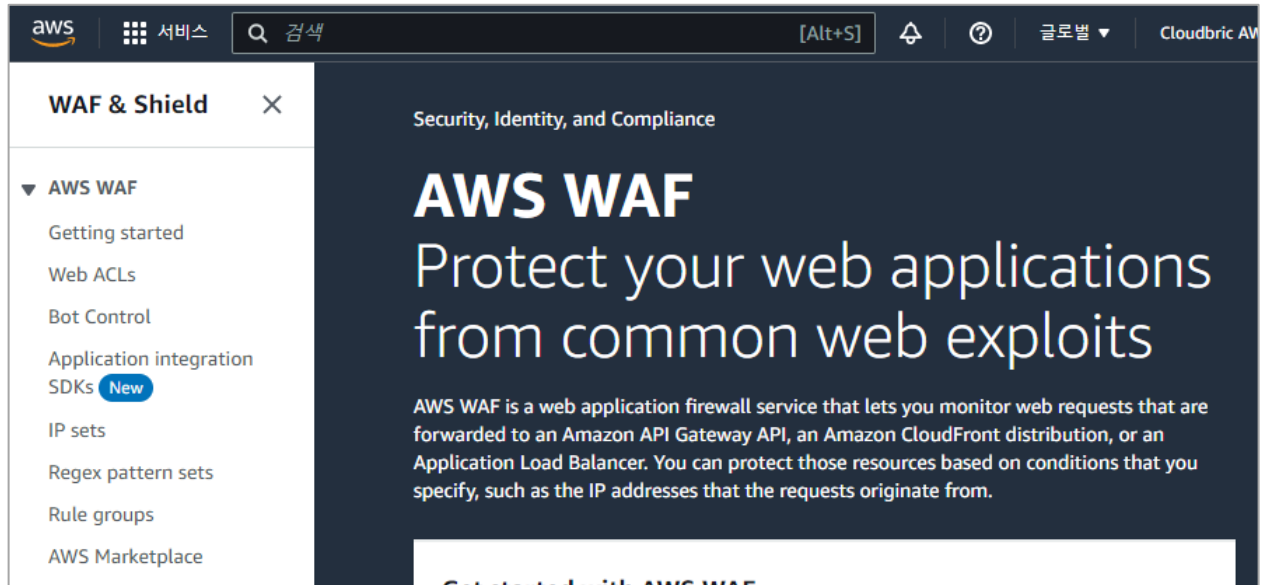
At the bottom, there are two buttons: '아니요, 취소 안 함' (No, I don't want to cancel) and '예, 구독 취소' (Yes, I want to cancel). The '예, 구독 취소' button is highlighted by a yellow circle.

3.2 Cloudbric Rule Set 삭제하기

- Step 1

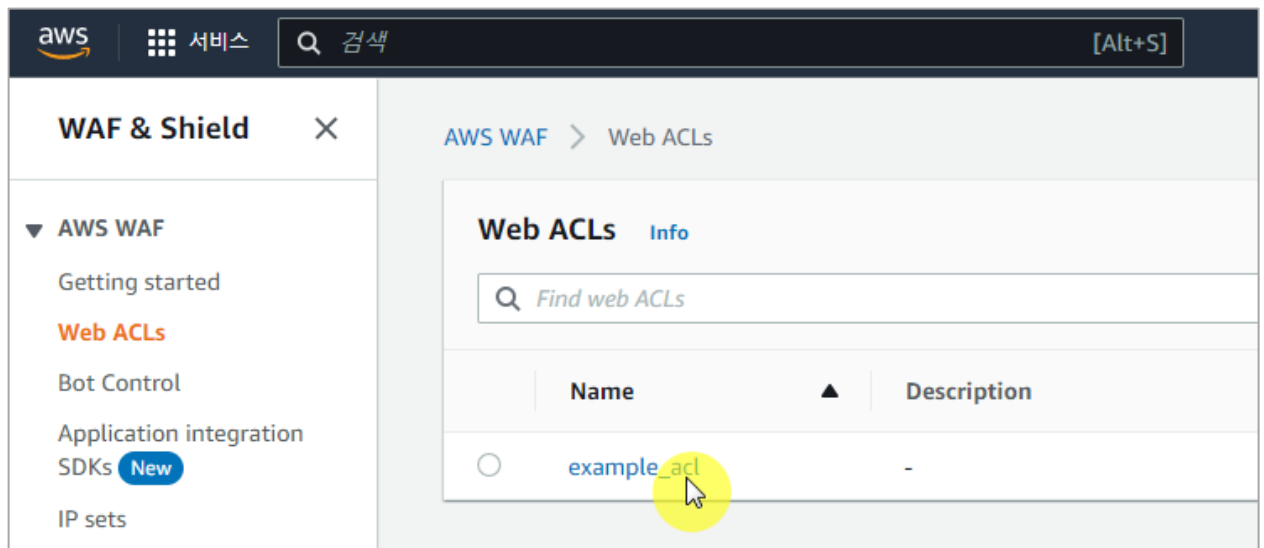
AWS WAF 콘솔에 접속합니다.

※ AWS WAF 콘솔: <https://console.aws.amazon.com/wafv2/>



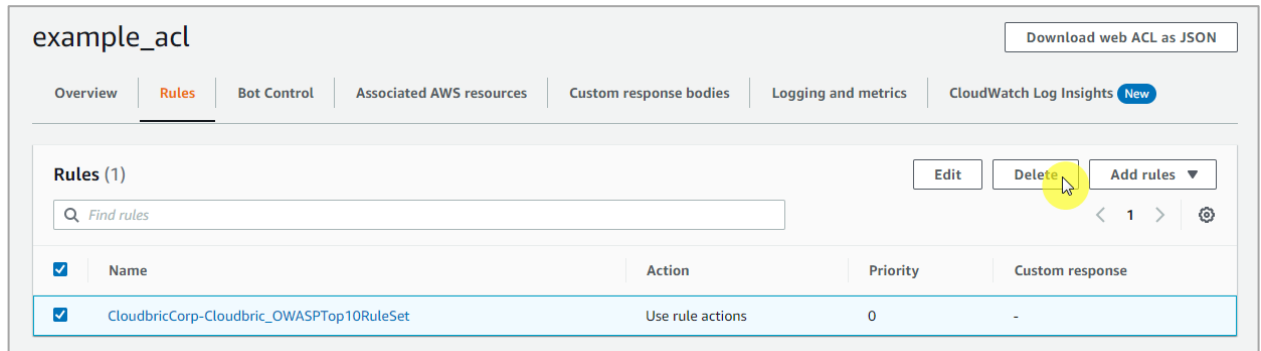
- Step 2

Web ACL 메뉴에서 Cloudbric Rule Set 을 삭제할 Web ACL 이름을 선택합니다.



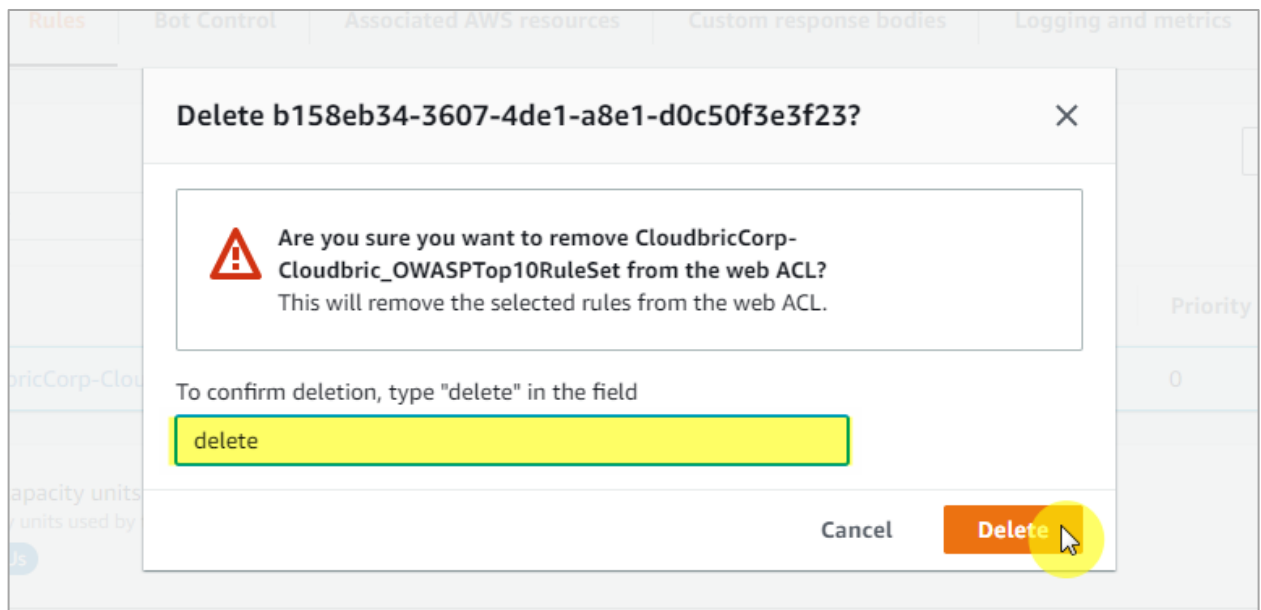
- Step 3

[Rules] 탭으로 이동한 뒤 삭제할 Cloudbric Rule Set 을 체크하고 [Delete] 버튼을 선택합니다.



- Step 4

'delete'를 타이핑한 뒤 [Delete] 버튼을 선택하여 삭제를 완료합니다.

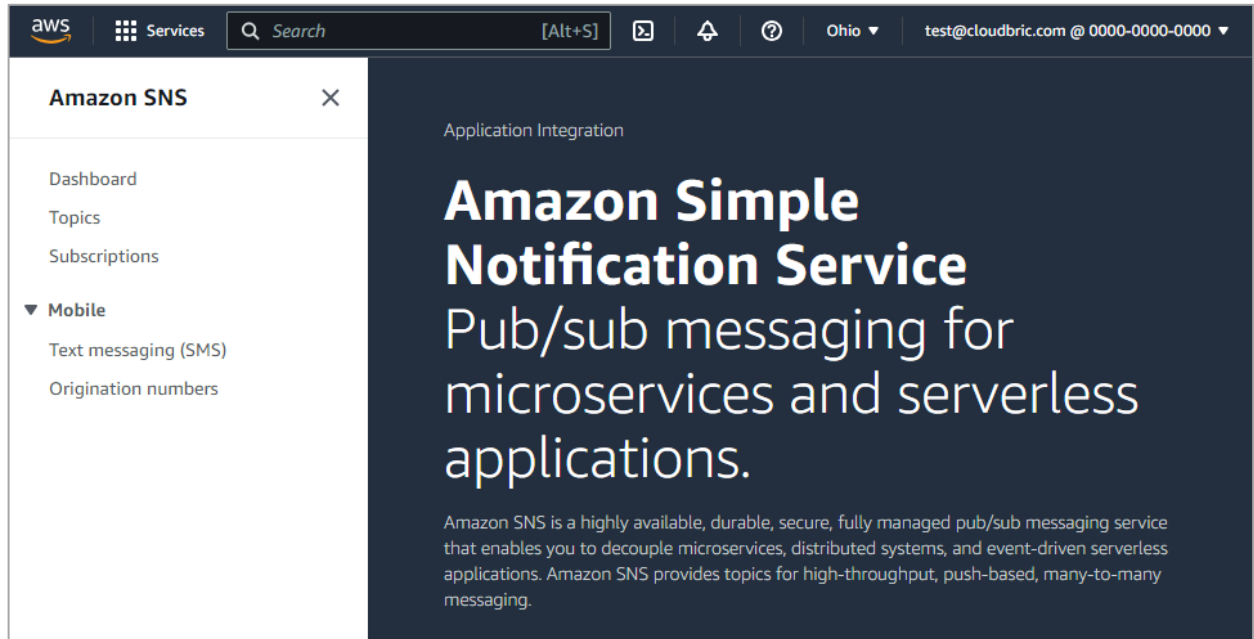


3.3 Cloudbric Rule Set 업데이트 알람 삭제하기

- Step 1

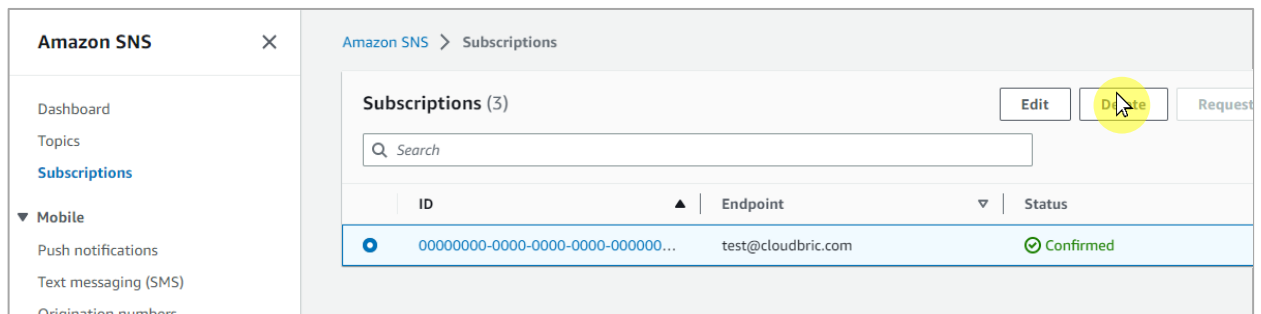
Amazon SNS(Simple Notification Service) 콘솔에 접속합니다.

※ Amazon SNS(Simple Notification Service) 콘솔: <https://console.aws.amazon.com/sns/home>



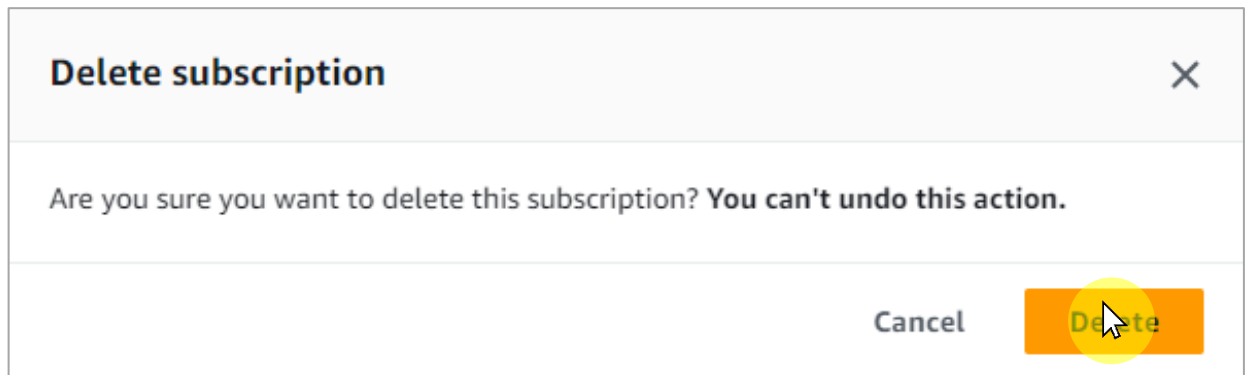
- Step 2

Subscriptions 메뉴에서 Cloudbric Rule Set 의 업데이트 알람을 받고 있는 ID 를 선택 후, [Delete]를 선택합니다.



- Step 3

업데이트 알림 삭제 확인 팝업에서 **[Delete]**를 선택하여 업데이트 알림의 삭제를 완료합니다.



cloudbric

4. Cloudbric Rule Set 예외 처리

Cloudbric Rule Set 에서 정상적인 요청을 차단하는 오탐이 발견되면 오탐이 발생한 특정 Rule 의 Action 을 'Count'로 재 정의하여 차단되지 않도록 예외 처리해야 합니다. 하지만 이로 인해 악의적인 요청 또한 허용되는 상황이 발생할 수 있습니다. Rule 예외 처리 전과 같이 기능을 최대한 유지하고 오탐이 발생한 특정 패턴만 예외 처리하려면 Label 기반의 사용자 정의 Rule 을 추가하여 예외 처리 정책을 재 정의해야 합니다.

※ Cloudbric OWASP Top 10 Rule Set 의 모든 Rule 에는 Label 이 설정되어 있습니다.

※ IP 기반의 Cloudbric Rule Set 은 IP 주소 목록의 동적 특성으로 별도의 Label 이 설정되어 있지 않습니다.

예외 처리가 필요한 IP 가 있는 경우 해당 IP 를 허용하는 Rule 을 생성하시면 됩니다.

4.1 Rule Action 'Count' 설정하기

- Step 1

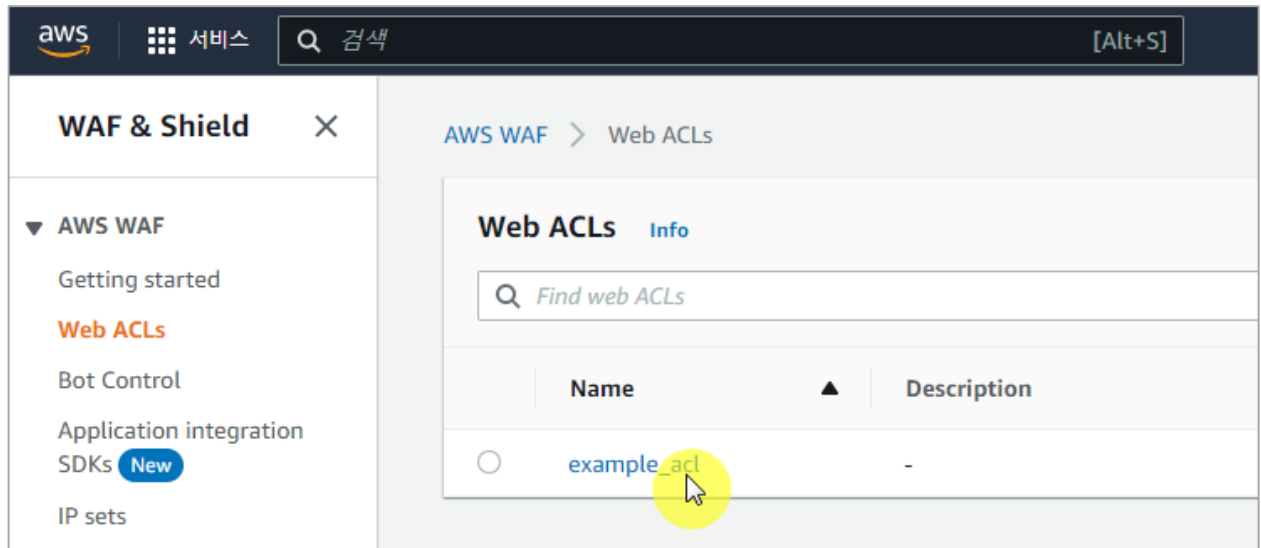
AWS WAF 콘솔에 접속합니다.

※ AWS WAF 콘솔: <https://console.aws.amazon.com/wafv2/>



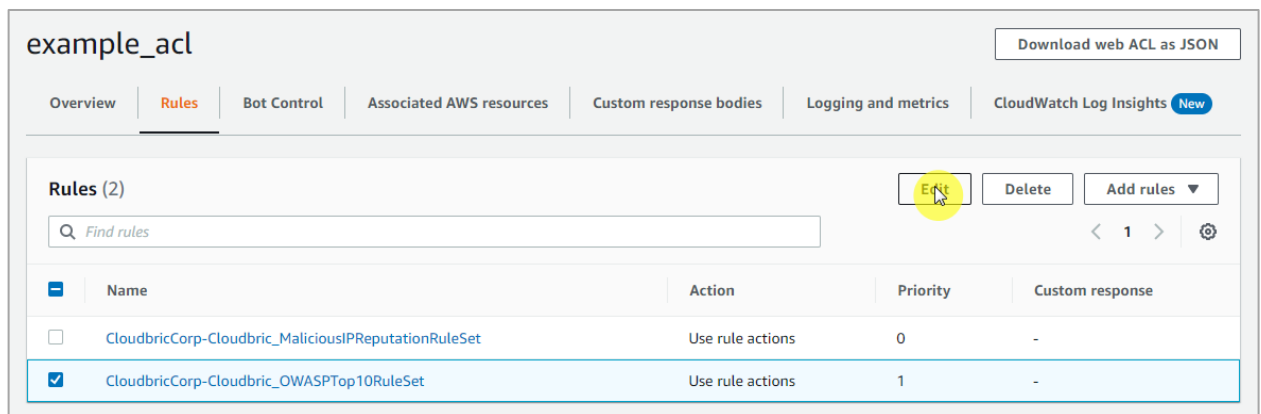
- Step 2

Web ACL 메뉴에서 Cloudbric Rule Set 을 적용한 Web ACL 이름을 선택합니다.



- Step 3

[Rules] 탭으로 이동한 뒤 Cloudbric Rule Set 을 체크하고 [Edit] 버튼을 선택합니다.



- **Step 4**

예외 처리가 필요한 Rule 의 Action 을 'Count'로 재 정의 후 **[Save rule]** 버튼을 선택하여 예외 처리를 완료합니다.

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_SQLInjection_URL

Choose rule action override ▼

Cloudbric_SQLInjection_Header_2

Choose rule action override ▼

Cloudbric_RequestHeaderFiltering

Choose rule action override ▼

Cloudbric_XSS_1

Choose rule action override ▲

Q |

Allow

Block

Count

CAPTCHA

Challenge

↶ Remove Override

Cloudbric_XSS_2

Choose rule action override ▼

Cloudbric_SQLInjection_Header_1

Choose rule action override ▼

Cloudbric_RequestMethodFiltering

Choose rule action override ▼

Cloudbric_StealthCommanding_Body_1

Choose rule action override ▼

15

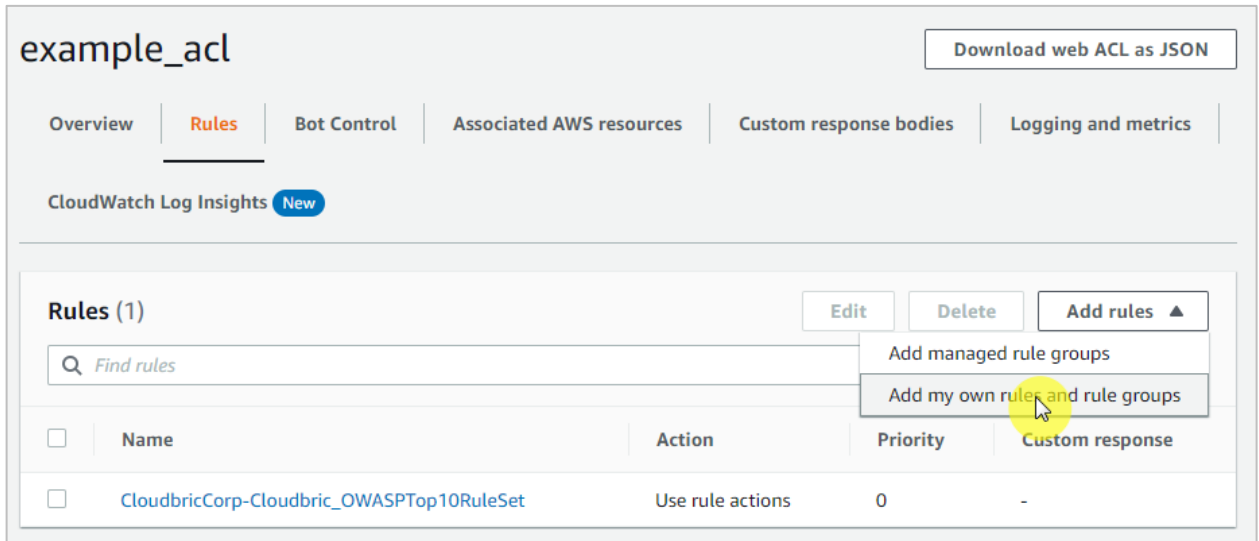
PUBLIC

24

4.2 Label 기반 예외 처리 Rule 추가하기

- Step 1

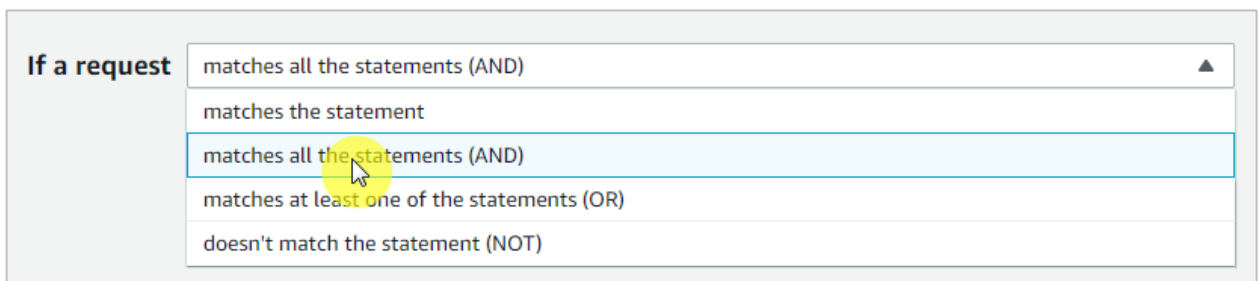
Web ACL 에서 **[Rules]** 탭으로 이동한 뒤 **[Add rules]** 버튼에서 **[Add my own rules and rule groups]**을 선택하여 신규 Rule 을 생성합니다.



- Step 2

2 개의 statement 를 충족하면 일치하도록 중첩 조건을 'AND'로 선택합니다.

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



- Step 3

Statement 1 은 「4.1」에서 예외 처리한 Rule 과 일치하는 요청을 대상으로 검사하도록 정의합니다.

- Inspect: Has a label 선택
- Match key: 예외 처리된 Rule 에 설정한 'Label 이름' 입력

If a request matches all the statements (AND)

Statement 1 Remove

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.
awsfaf.managed:cloudbric:owasp:XSS_1

※ Cloudbric OWASP Top 10 Rule Set 의 Label 이름 구조: awswaf:managed:cloudbric:owasp:[Rule 이름]

- 예제: Rule 이름이 'Cloudbric_XSS_1' 인 경우 'awswaf:managed:cloudbric:owasp:XSS_1'로 생성됩니다.

• Step 4

Statement 2 는 「4.1」에서 예외 처리된 Rule 에서 오탐이 발생한 요청의 탐지 조건을 제외하도록 정의합니다.

- Negate statement results: 해당 구문에 정의된 탐지 조건을 제외하도록 체크 설정
- Inspect: 오탐이 발생한 탐지 조건 설정

AND

NOT Statement 2 Remove

Negate statement (NOT)
Select this to match requests that don't satisfy the statement criteria.

☒ Negate statement results

Inspect
Choose an inspection option ▼

※ SQL injection 및 XSS(Cross Site Scripting) 공격을 탐지하는 Rule 에 한하여 AWS WAF 'ruleMatchDetails' 로그 필드에서 요청이 일치한 탐지 조건을 확인할 수 있습니다.

※ 그 외의 Rule 에서 오탐이 발생한 경우 로그 정보와 함께 awsmkp@cloudbric.com 으로 연락 주세요.

• Step 5

Rule 에 일치하는 경우 차단되도록 Rule 의 Action 을 'Block'으로 설정하고 **[Add rule]** 버튼을 선택하여 Rule 을 추가해 주세요.

Action

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

☐ Allow

☒ Block

☐ Count

☐ CAPTCHA

☐ Challenge

- **Step 6**

「4.1」에서 예외 처리한 Rule 보다 나중에 적용되도록 우선순위(Priority)를 설정한 뒤 **[Save]** 버튼을 선택하여 예외 처리 Rule 설정을 완료합니다.

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"/>	CloudbricCorp-Cloudbric_OWASPTop10RuleSet	1400	Use rule actions
<input checked="" type="radio"/>	MyExceptionRule_xss_1	2	Block

CancelSave

cloudbric

5. 부록

5.1. 자주 하는 질문 (FAQ)

Q. 요청을 차단한 Rule 이름을 확인할 수 있나요?

Web ACL 의 [Sampled requests] > [Rule inside rule group] 정보에서 확인하거나 Web ACL 로깅을 설정했다면 [RuleId] 로그 필드에서 확인할 수 있습니다.

※ Sampled requests 는 지난 3 시간 동안의 요청 중 최대 100 개의 로그를 확인할 수 있습니다.

더 자세한 내용은 AWS 개발자 안내서의 웹 요청 샘플 보기를 참조해 주세요.

https://docs.aws.amazon.com/ko_kr/waf/latest/developerguide/web-acl-testing-view-sample.html

다음은 Rule 이름을 확인할 수 있는 로그 예제입니다.

- **terminatingRuleId**: 요청을 종료한 Rule ID 입니다.
요청을 종료하는 Rule 이 없으면 이 값은 Default_Action 입니다.

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

- **RuleId**: 요청과 일치하고 종료되지 않은 nonTerminatingMatchingRules 의 Rule ID 입니다.

```
"timestamp": 1592357192516
, "formatVersion": 1
, "webaclId": "arn:aws:wafv2:us-east-1:123456789012:global/webacl/hello-world/5933d6d9-9dde-js82-v8"
, "terminatingRuleId": "Default_Action"
, "terminatingRuleType": "REGULAR"
, "action": "ALLOW"
, "terminatingRuleMatchDetails": []
, "httpSourceName": "-"
, "httpSourceId": "-"
, "ruleGroupList": []
, "rateBasedRuleList": []
, "nonTerminatingMatchingRules":
[ {
  "ruleId": "TestRule"
, "action": "COUNT"
, "ruleMatchDetails":
```

※ 더 자세한 내용은 AWS 개발자 안내서의 로그 예제를 참조해 주세요.

로그 예제: https://docs.aws.amazon.com/ko_kr/waf/latest/developerguide/logging-examples.html

Q. Cloudbric Rule Set 이 제대로 적용되었는지 확인할 방법이 있을까요?

AWS WAF 는 Block 으로 설정된 Rule 과 요청이 일치하면, 기본적으로 403 Forbidden 오류를 반환합니다. 간단한 XSS 공격 예제를 브라우저에 입력하여 Cloudbric Rule Set 이 적용되었는지 확인해 보세요.

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

Q. Cloudbric Rule Set 탐지 조건을 볼 수 있는 방법이 있나요?

기본적으로 AWS WAF Managed Rules 의 탐지 위치나 패턴 등의 상세 조건은 AWS Marketplace 판매자의 지적 재산권이며 이를 공개할 경우 Rule 우회 등의 해킹에 악용될 우려가 있어 공개하지 않습니다.

하지만 SQL injection 및 XSS(Cross Site Scripting) 공격을 탐지하는 Rule 에 한하여 AWS WAF 'ruleMatchDetails' 로그 필드에서 요청이 일치한 탐지 조건을 확인할 수 있습니다.

- SQL injection 공격과 일치한 Rule 의 탐지 조건 로그 예제:

<pre> "terminatingRuleId": "STMTTest_SQLi_XSS", "terminatingRuleType": "REGULAR", "action": "BLOCK", "terminatingRuleMatchDetails": [{ "conditionType": "SQL_INJECTION", "sensitivityLevel": "HIGH", "location": "HEADER", "matchedData": ["10", "AND", "1"] }] </pre>	<pre> ,"nonTerminatingMatchingRules": [{ "ruleId": "TestRule" , "action": "COUNT" , "ruleMatchDetails": [{ "conditionType": "SQL_INJECTION" , "sensitivityLevel": "HIGH" , "location": "HEADER" , "matchedData": ["10" , "and" , "1"] }] }] </pre>
--	--

(왼쪽)요청을 종료한 Rule 인 경우 / (오른쪽)요청을 종료하지 않은 Rule 인 경우

Q. 오탐 및 과탐이 발생할 경우 Cloudbric Rule Set 탐지 조건을 변경하는 방법이 있나요?

AWS 에서 Managed Rules 자체 탐지 조건을 변경하는 기능은 제공하지 않습니다.

하지만 AWS WAF Managed Rules 는 일반적으로 많은 고객에게서 관찰된 위협을 기반으로 작성되기 때문에 사용하는 환경에 따라 오탐 및 과탐이 발생할 수 있습니다. 따라서 Cloudbric Rule Set 을 실 환경에 적용하기 전에 약 2~4 주간의 모니터링을 통해 운영 환경에 맞춰 「4. Cloudbric Rule Set 예외 처리」를 참고하여 예외 처리한 뒤 적용하는 것을 권장합니다.

사용자 환경에 맞는 Rule 설정이 어렵다면 클라우드브릭의 AWS WAF 보안 정책 운영 및 관리 서비스인 Cloudbric WMS 를 사용해 보는 것도 방법입니다.

- Cloudbric WMS 소개 페이지: <https://www.cloudbric.co.kr/cloudbric-wms/>
- Cloudbric WMS 도입 문의하기: <https://www.cloudbric.co.kr/문의하기/>

Q. Cloudbric Rule Set 변경 사항은 어디에서 확인할 수 있나요?

클라우드브릭 공식 홈페이지에서 2021.11.12 이후부터 출시된 Cloudbric Rule Set 의 변경 사항을 안내하고 있습니다.

※ IP 기반의 Cloudbric Rule 의 경우 IP 주소 목록의 동적 특성으로 Rule 에 적용된 IP 주소 목록에 대한 변경 사항은 안내하지 않습니다.

Cloudbric Rule Set for AWS WAF 릴리즈 노트 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. Cloudbric Rule Set 월별 요금은 어떻게 계산하나요?

AWS Marketplace 의 AWS WAF Managed Rule 요금은
Cloudbric Rule Set 이 적용된 Web ACL 기준으로 아래 2 개 항목 요금이 부과됩니다.

- ① **Region:** Web ACL 이 배포된 Region 수
- ② **Requests:** 각 Region 별 1 백만 건 단위로 Web ACL 에 수신된 Requests 수

Cloudbric OWASP Top 10 Rule Set 요금 계산 예시:

- OWASP Top 10 Rule Set 가격 정보:

계산 단위	요금
Region 당	\$25/월(시간당 비례 배분)
각 Region 의 1 백만 Requests 당	\$1/월

- 사례 A:

단일 지역(예: us-east-1)에 생성한 2 개 Web ACL 에 Cloudbric Rule Set 을 적용하고
한 달 동안 2 개의 Web ACL 에 수신된 Web Requests 가 1 천만 건인 경우
계산)

us-east-1 Region

- ① **Region 요금:** $\$25.00 * 1 = \25.00
 - ② **Requests 요금:** $\$1.00(1 \text{ 백만 건당}) * 10 \text{ Requests}(1 \text{ 천만 건}) = \10.00
- = 총 요금(①+②):** \$35.00

- 사례 B:

2 개의 지역(예: us-east-1, us-west-2)에 각 2 개씩 생성한 Web ACL 에 Cloudbric Rule Set 을 적용하고
한 달 동안 지역별 2 개의 Web ACL 에 수신된 Web Requests 가 각 1 천만 건인 경우
계산)

us-east-1 Region

- ① **Region 요금:** $\$25.00 * 1 = \25.00
- ② **Requests 요금:** $\$1.00(1 \text{ 백만 건당}) * 10 \text{ Requests}(1 \text{ 천만 건}) = \10.00

us-west-2 Region

- ③ **Region 요금:** $\$25.00 * 1 = \25.00
- ④ **Requests 요금:** $\$1.00(1 \text{ 백만 건당}) * 10 \text{ Requests}(1 \text{ 천만 건}) = \10.00

= 총 요금(①+②+③+④): \$70.00

5.2 Cloudblic OWASP Top 10 Rule 유형 설명

Rule 유형	설명
Buffer Overflow	웹 서버에 메모리 Buffer Overflow 공격을 일으킬 수 있는 제한 값보다 큰 데이터가 포함된 요청문을 차단합니다.
Cross Site Scripting (XSS)	클라이언트 측에서 실행되는 악성 스크립트 코드를 차단합니다.
SQL Injection	SQL Query 구문을 삽입하려는 요청을 차단합니다.
Directory Traversal	웹 서버의 취약점을 이용하여 디렉터리 및 파일에 접속하려는 요청을 차단합니다.
Request Method Filtering	안전하지 않은 HTTP Request Method 에 대하여 차단합니다.
Request Header Filtering	웹 브라우저에서 정상적으로 보내는 HTTP Request 요청문과 달리, 헤더에 필수 요소의 누락이나 오류가 발생한 경우, 해당 요청을 비정상 요청(자동화된 공격 도구 등의 요청)으로 탐지합니다.
Stealth Commanding	HTTP Request 를 통하여 웹 서버 내의 특정 명령어를 실행하려는 요청을 차단합니다.
File Upload	웹 서버에서 실행 가능한 파일의 업로드를 차단합니다.
XXE Injection	XML 문서의 External entity 를 사용하여 로컬 파일의 열람 등을 유발하는 공격을 차단합니다.