보안 위협 대응 클라우드 기반 보안 엔지니어

AWS 기반 보안형 아키텍처 숙소 예약 시스템 구축 프로젝트

2025.07.14-2025.07.21

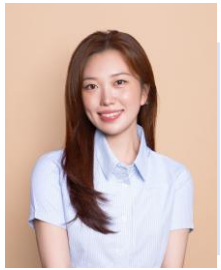
netfort

팀원 소개

김민성

김현수

김혜수



신영민

신지혜

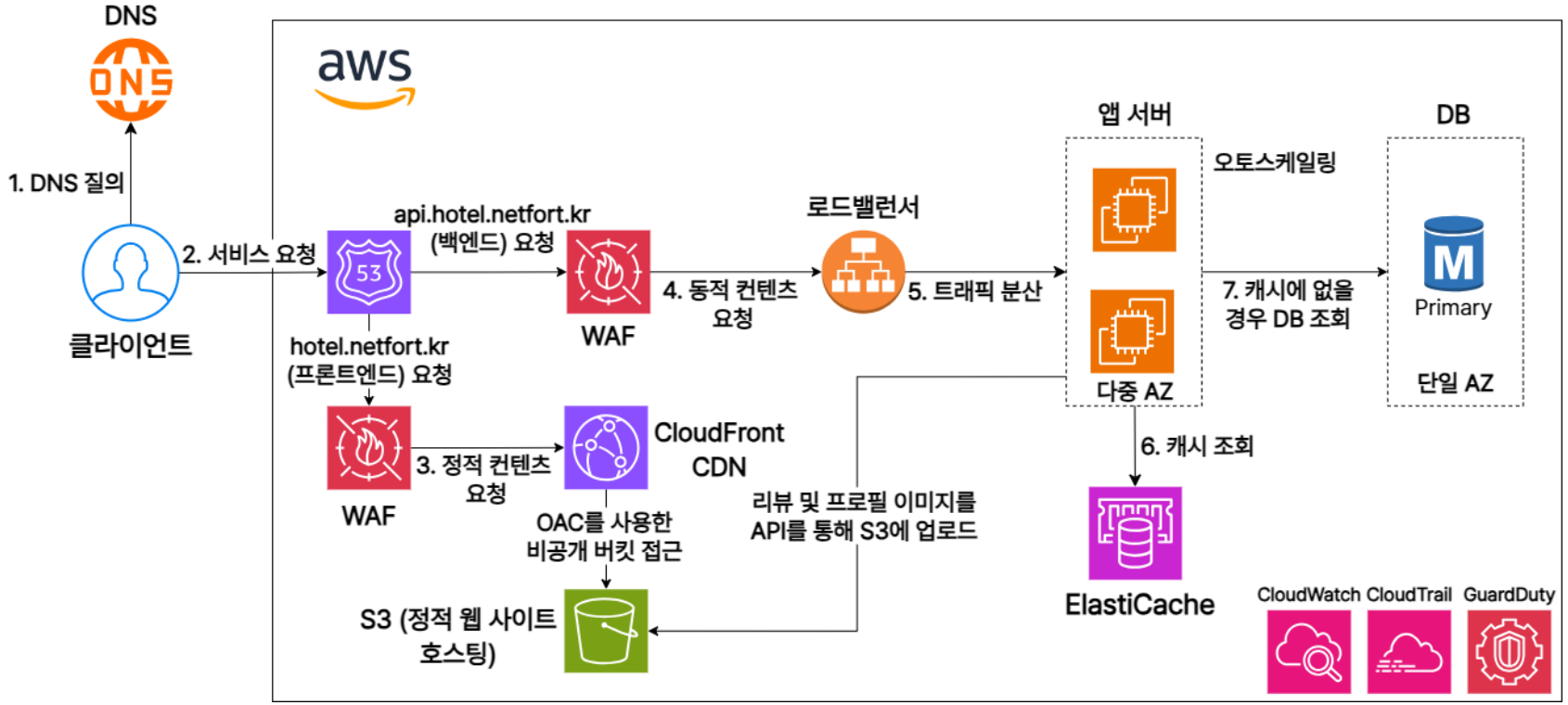
조준한

netfort

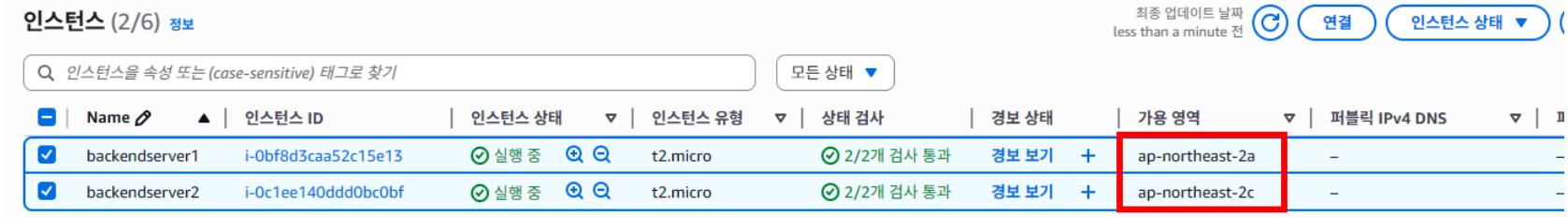
목차

netfort

구성도


DNS
1. DNS 질의
클라이언트
2. 서비스 요청
aws
api.hotel.netfort.kr
(백엔드) 요청
hotel.netfort.kr
(프론트엔드) 요청
WAF
WAF
3. 정적 컨텐츠
요청
CloudFront
CDN
OAC를 사용한
비공개 버킷 접근
S3 (정적 웹 사이트
호스팅)
4. 동적 컨텐츠
요청
로드밸런서
5. 트래픽 분산
앱 서버
다중 AZ
오토스케일링
7. 캐시에 없을
경우 DB 조회
DB
Primary
단일 AZ
6. 캐시 조회
ElastiCache
리뷰 및 프로필 이미지를
API를 통해 S3에 업로드
CloudWatch
CloudTrail
GuardDuty

인프라 - EC2

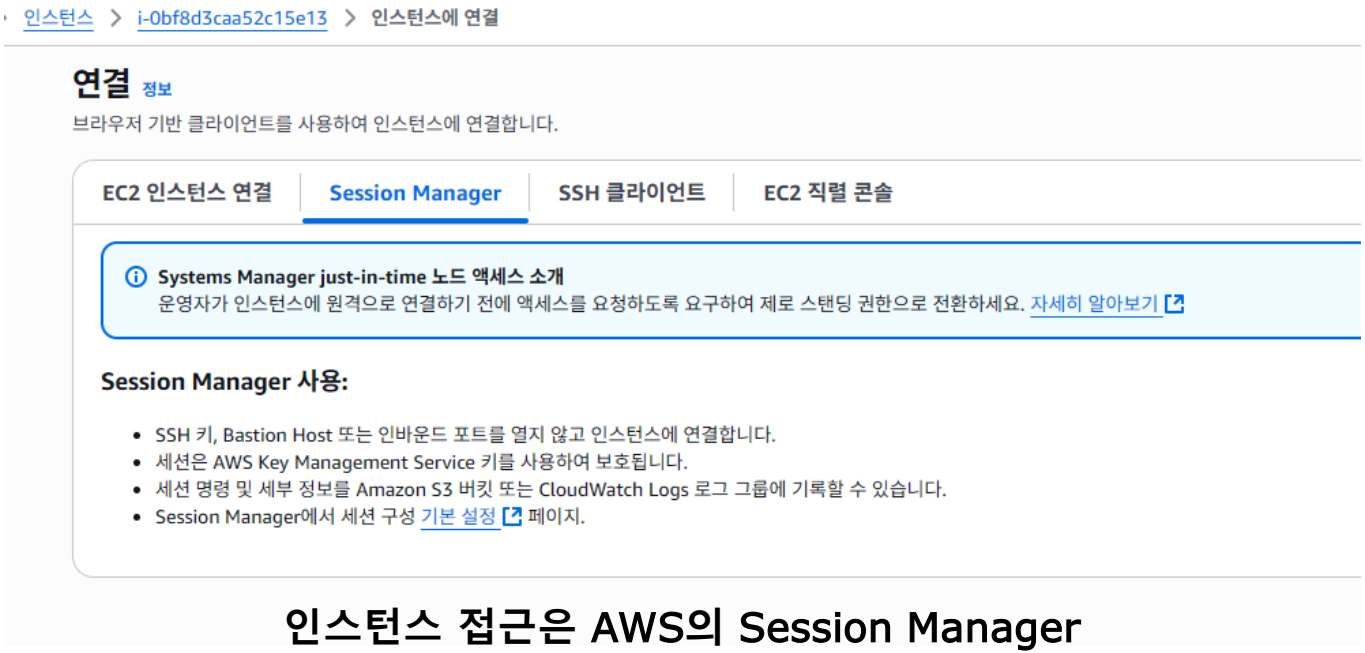


다중 가용영역에 구성된 백엔드 인스턴스

- FastAPI로 개발된 백엔드 애플리케이션
- Docker 컨테이너로 패키징되어 EC2 인스턴스에서 실행

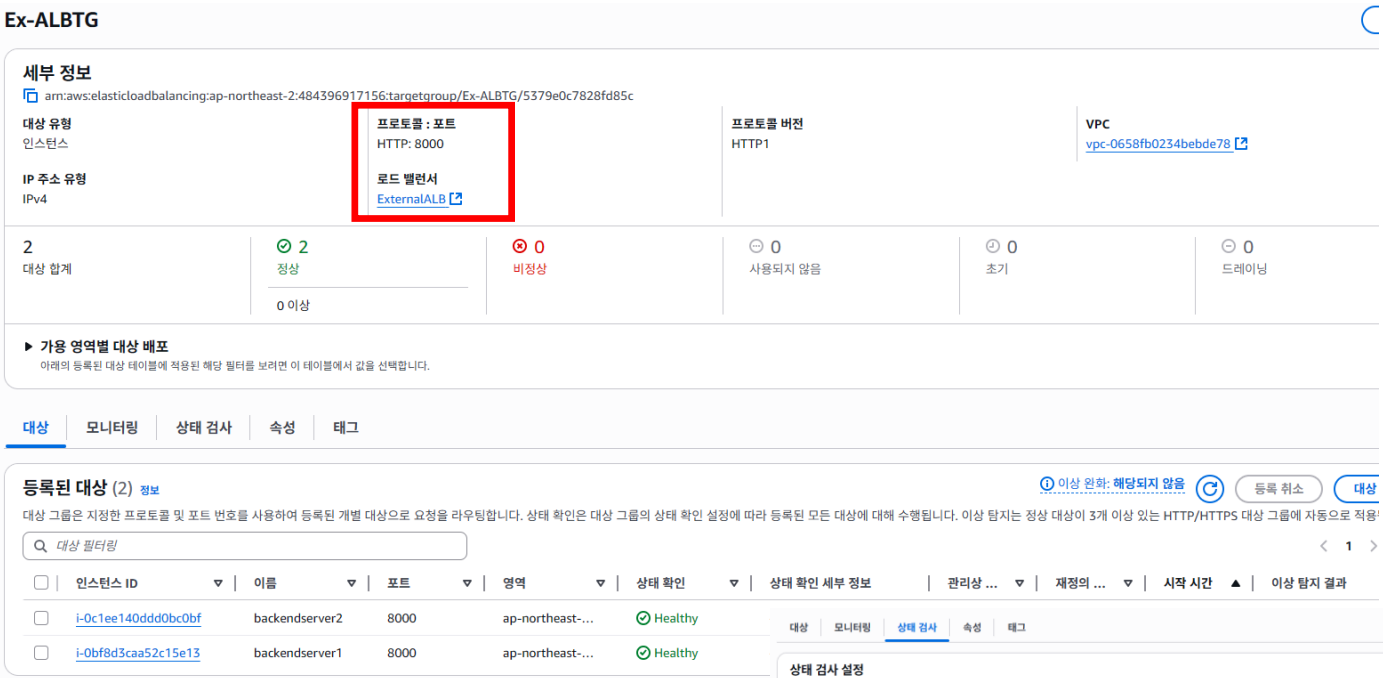
```
[root@ip-172-31-43-4 ~]# tree
.
├── backend
│   ├── Dockerfile
│   ├── auth.py
│   ├── crud.py
│   ├── database.py
│   ├── email_utils.py
│   ├── main.py
│   ├── models.py
│   ├── requirements.txt
│   ├── schemas.py
│   └── seed.py
└── docker-compose.yml

1 directory, 11 files
[root@ip-172-31-43-4 ~]# docker ps
CONTAINER ID   IMAGE          COMMAND                  CREATED         STATUS         PORTS                                       NAMES
05230f9f9986   root-backend   "gunicorn -k uvicorn…"   38 minutes ago   Up 38 minutes   0.0.0.0:8000->8000/tcp, :::8000->8000/tcp   root-backend-1
```

인프라 - EC2



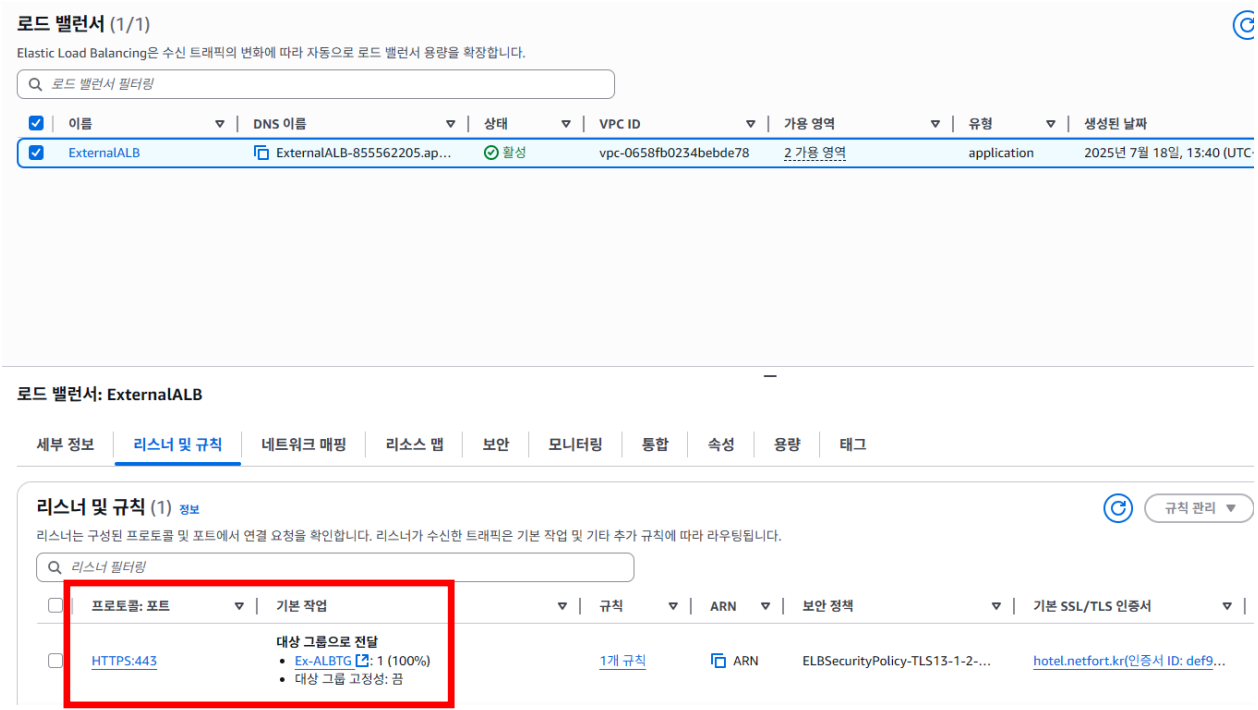
인스턴스 접근은 AWS의 Session Manager 를 통해 접속할 수 있으며 외부 접속은 차단

인프라 - Load Balancer



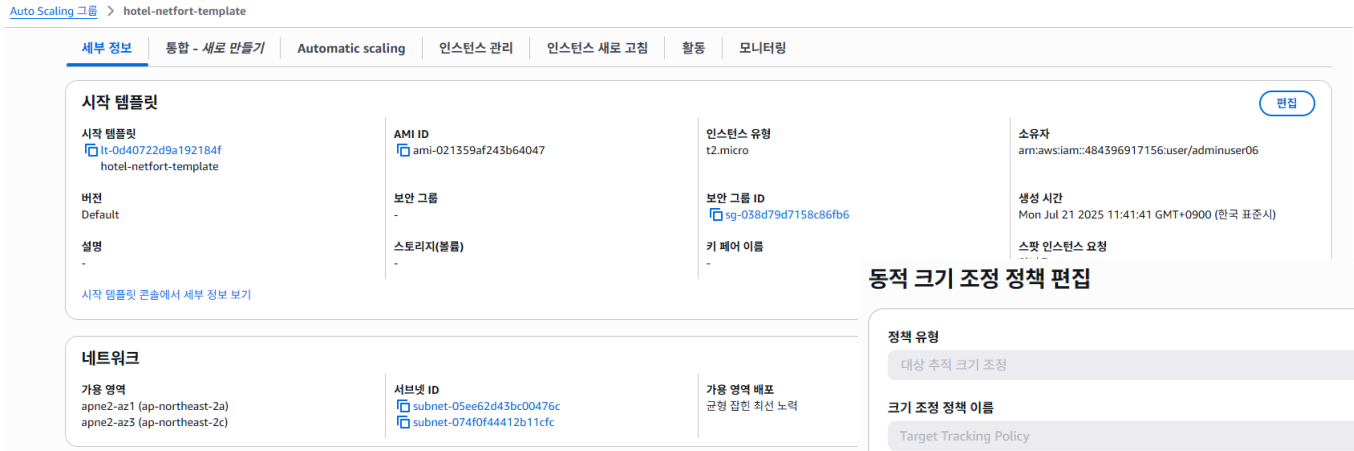
대상 그룹에 백엔드 인스턴스가 등록되어
백엔드가 사용 중인 포트 8000의 상태를

인프라 - Load Balancer



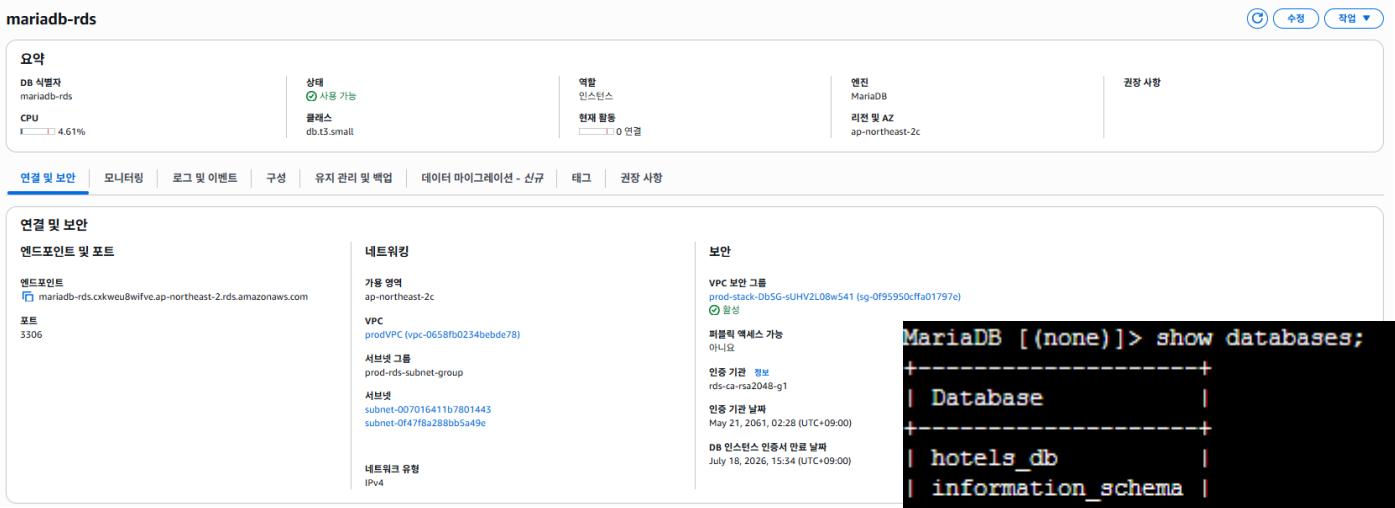
로드 밸런서에서 HTTPS로 접속 시 대상 그룹(포트 8000)로 전달

인프라 - Auto Scaling



- 시작 템플릿을 이용하여 Auto Scaling 그룹 생성
- 그룹 내 인스턴스가 평균 CPU 사용률이 70% 이상일 경우 인스턴스 추가

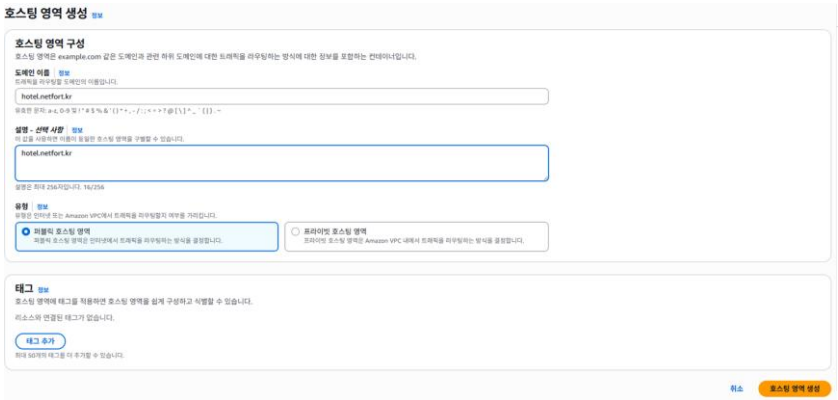
인프라 - RDS

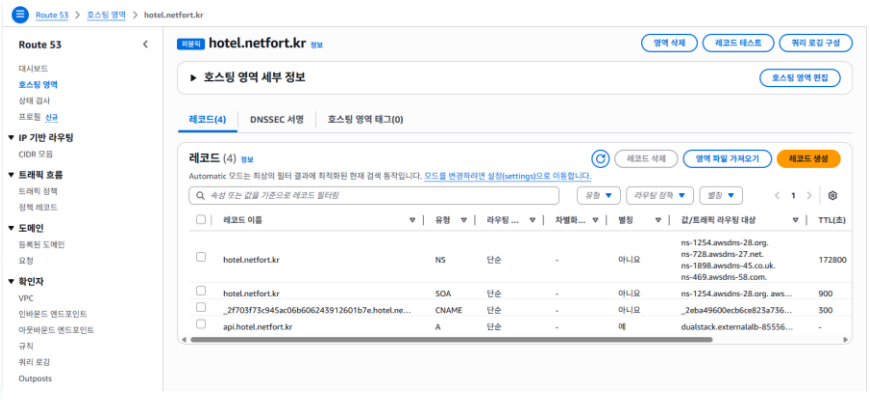



```
MariaDB [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| hotels_db          |
| information_schema |
| innodb             |
| mysql              |
| performance_schema |
| sys                |
+--------------------+
6 rows in set (0.003 sec)

MariaDB [(none)]>
```

서비스의 모든 데이터는 완전 관리형 데이터베이스 서비스인 Amazon RDS를 통해 안전하게 관리

인프라 - Route 53



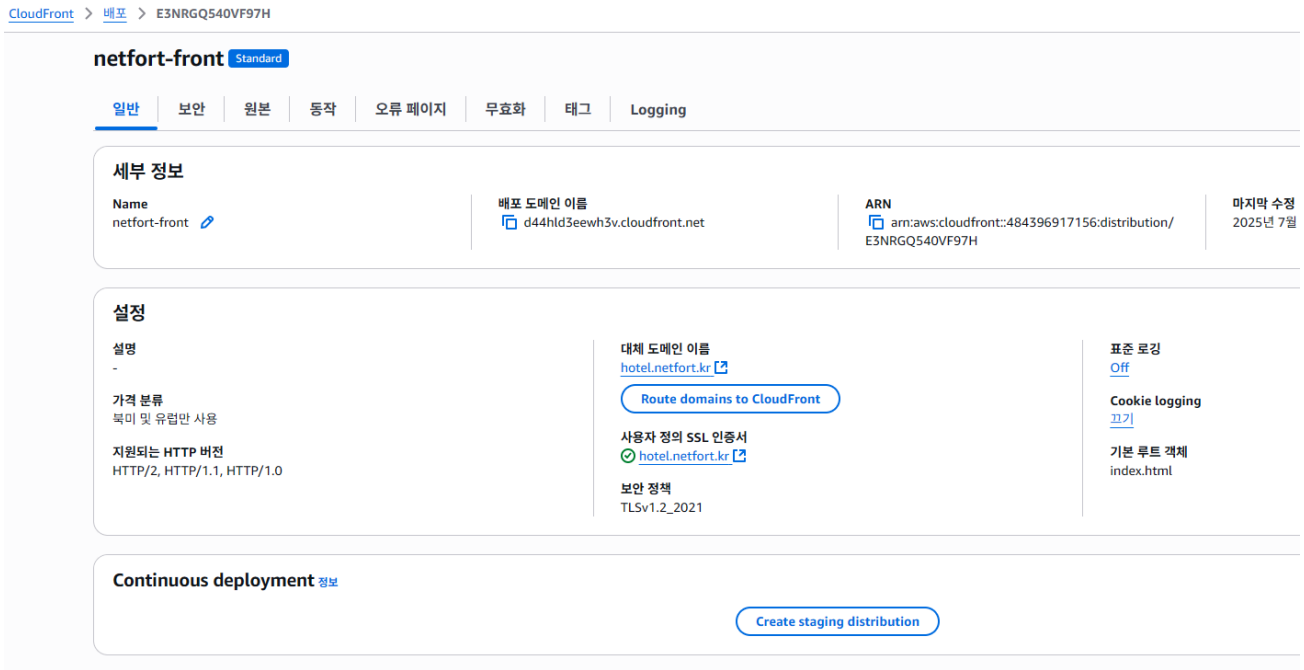


도메인 hotel.netfort.kr 을 퍼블릭 호스팅 영역 유형으로 생성하여 외부에서 접근 가능하도록 설정

backend(api.hotel.netfort.kr) 를 로드 밸런서로 연결

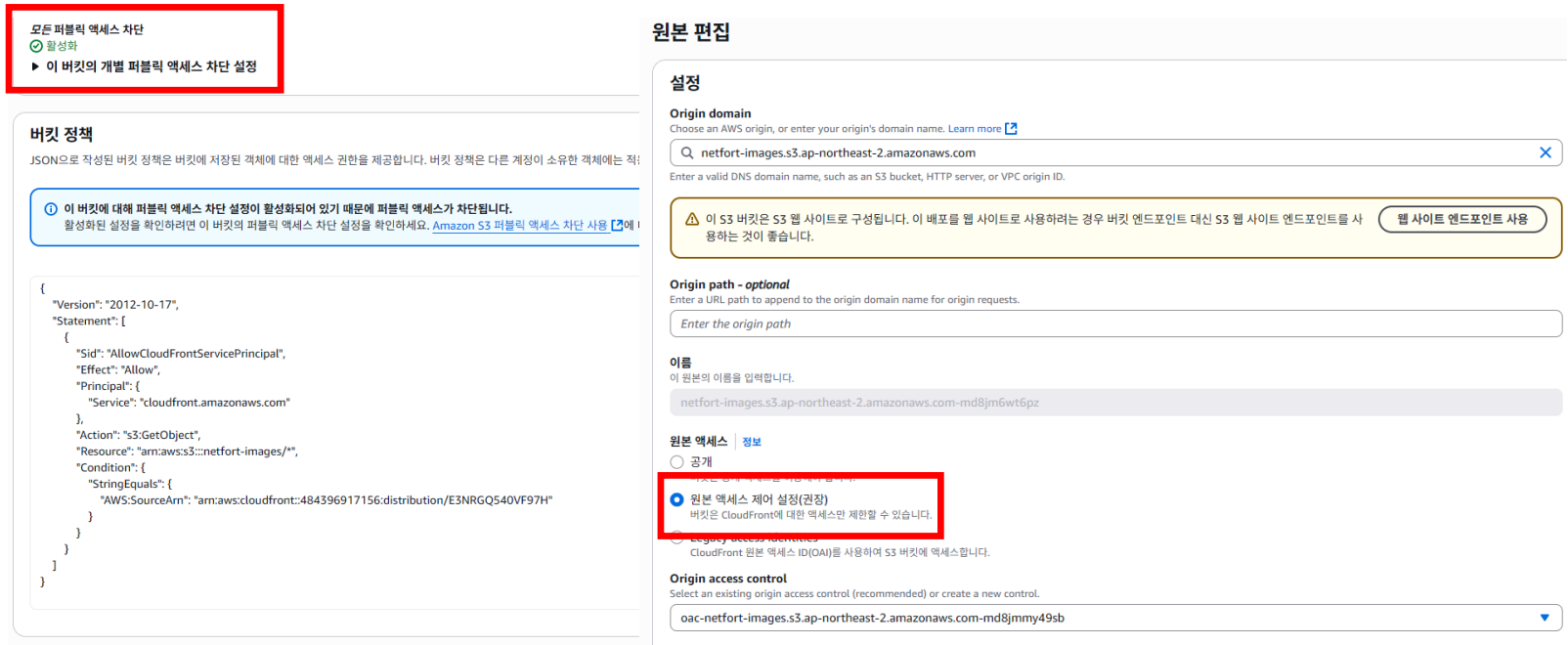
netfort

인프라 - CloudFront



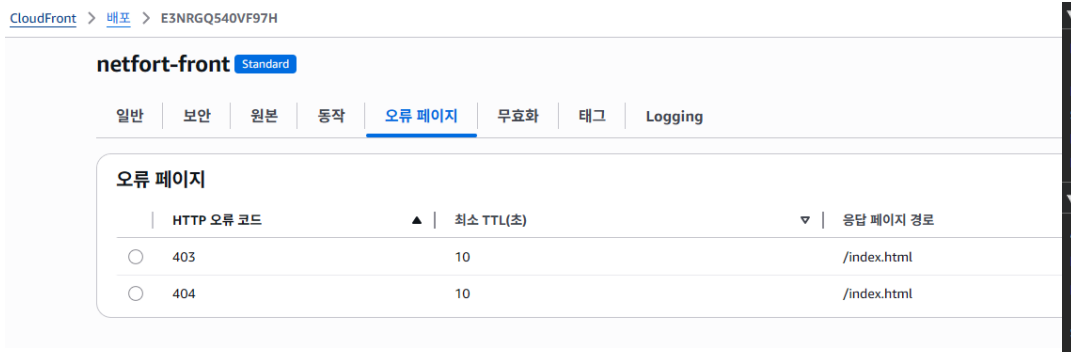
S3에 저장된 모든 콘텐츠는 Amazon CloudFront를 통해 사용자에게 제공

인프라 - CloudFront

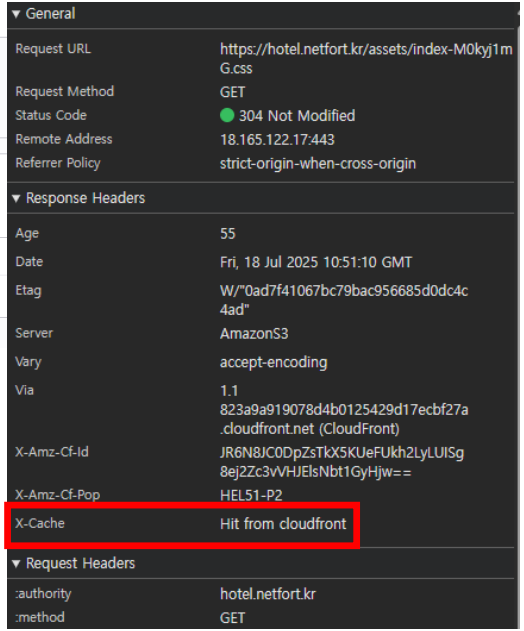


- S3의 웹 사이트를 CloudFront 를 통해 접속
- 보안을 위해 웹 사이트 엔드포인트는 사용하지 않고, 원본 액세스 제어 설정을 하여 S3 버킷을 CloudFront 에서만 액세스

인프라 - CloudFront

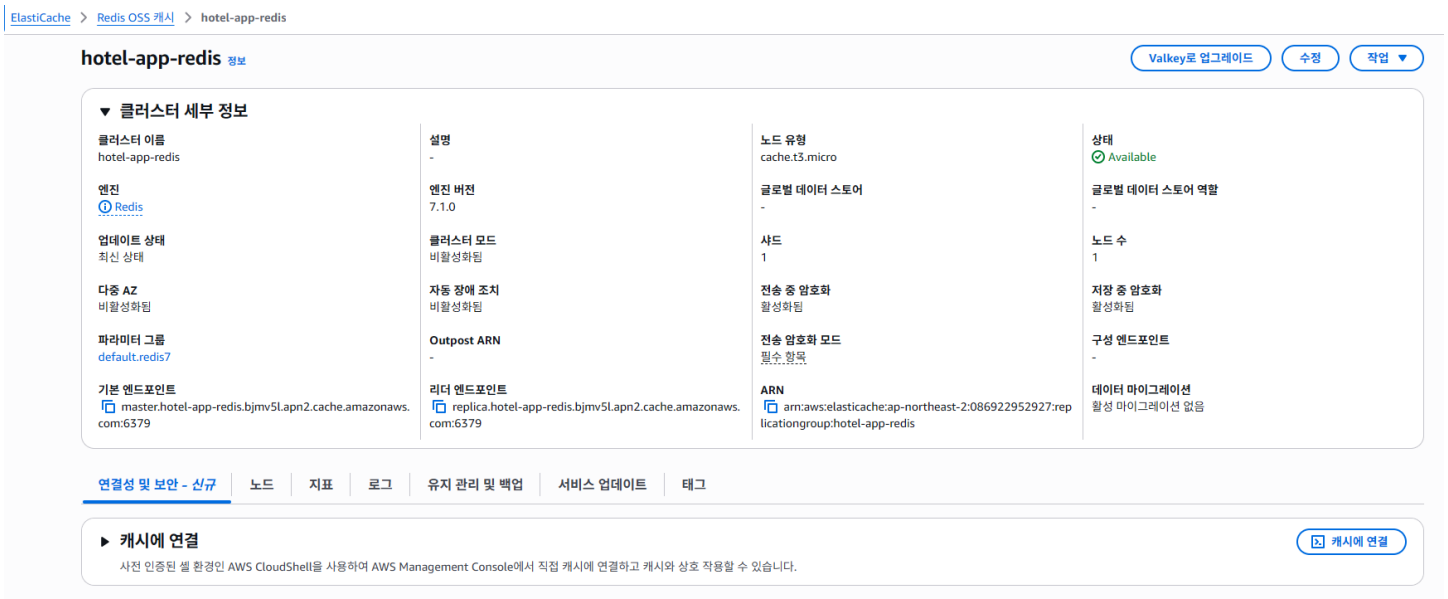


Single Page Application (SPA) 라우팅 문제 해결을 위해 403, 404 에러 페이지를 index.html로 반환



헤더 X-Cache를 확인하여 동적 콘텐츠는 캐싱 되는 것을 확인

인프라 - ElastiCache



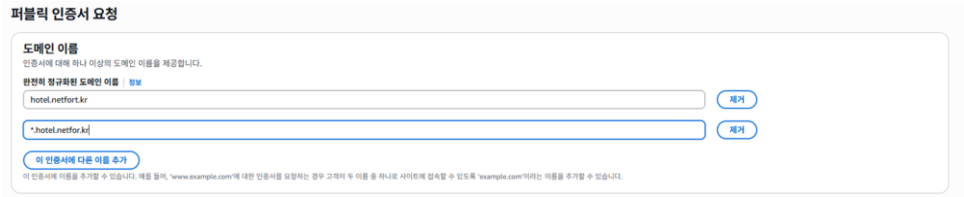
ElastiCache의 Redis를 사용하여 데이터를 캐싱,사용자에게 더 빠른 응답 속도를 제공

인프라 - ElastiCache

```
master.hotel-app-redis.bjmv5l.apn2.cache.amazonaws.com:6379> KEYS *
1) "hotels:skip=0:limit=100"
2) "login_attempts:admin@netfort.kr"
master.hotel-app-redis.bjmv5l.apn2.cache.amazonaws.com:6379> GET login_attempts:admin@netfort.kr
"1"
master.hotel-app-redis.bjmv5l.apn2.cache.amazonaws.com:6379> GET hotels:skip=0:limit=100
(nil)
master.hotel-app-redis.bjmv5l.apn2.cache.amazonaws.com:6379> GET hotels:skip=0:limit=100
"[{\"name\": \"\\ub9ac\\uc561\\ud2b8 \\ud638\\ud154 \\uc11c\\uc6b8\", \"location\": \"\\uc11c\\uc6b8, \\uac15\\ub0a8\\uad6c\", \"rating\": 5.0, \"images\
9-6a8506099945?w=500\", \"https://images.unsplash.com/photo-1582719508461-905c673771fd?w=500\", \"https://images.unsplash.com/photo-1596394516093-501ba68
c\\uc6b8\\uc758 \\uc911\\uc2ec, \\uac15\\ub0a8\\uc5d0 \\uc704\\uce58\\ud55c 5\\uc131\\uae09 \\ud638\\ud154\\uc785\\ub2c8\\ub2e4. \\ucd5c\\uc0c1\\uc758 \\
778 \\uc2dc\\uc124\\ub85c \\ube44\\uc988\\ub2c8\\uc2a4 \\ubc0f \\ub808\\uc800 \\uc5ec\\ud589\\uac1d \\ubaa8\\ub450\\uc5d0\\uac8c \\uc644\\ubcbd\\ud55c \\
2e4.\", \"price\": 250000, \"amenities\": [\"\\ubb34\\ub8cc Wi-Fi\", \"\\uc218\\uc601\\uc7a5\", \"\\ud53c\\ud2b8\\ub2c8\\uc2a4 \\uc13c\\ud130\", \"\\ub80
ub2a5\"]}, {\"name\": \"\\ubdf0 \\ud638\\ud154 \\uc81c\\uc8fc\", \"location\": \"\\uc81c\\uc8fc, \\uc11c\\uadc0\\ud3ec\\uc2dc\", \"rating\": 4.5, \"image
287-417002075841?w=500\", \"https://images.unsplash.com/photo-1571003123894-1f0594d2b5d9?w=500\", \"https://images.unsplash.com/photo-1563911302283-d2bc1
81c\\uc8fc\\ub3c4\\uc758 \\uc544\\ub984\\ub2e4\\uc6b4 \\ud574\\uc548\\uac00\\uc5d0 \\uc790\\ub9ac \\uc7a1\\uc740 \\ubdf0 \\ud638\\ud154\\uc785\\ub2c8\\ub
d658\\uc0c1\\uc801\\uc778 \\uc624\\uc158\\ubdf0\\ub97c \\uac10\\uc0c1\\ud560 \\uc218 \\uc788\\uc73c\\uba70, \\uc790\\uc5f0\\uacfc \\ud568\\uaed8\\ud558\\
b2c8\\ub2e4.\", \"price\": 180000, \"amenities\": [\"\\ubb34\\ub8cc Wi-Fi\", \"\\ud574\\ubcc0 \\uc811\\uadfc\\uc131\", \"\\uc2a4\\ud30c\", \"\\uc870\\uc2
ub10c\\ud2b8 \\ube44\\uce58 \\ub9ac\\uc870\\ud2b8\", \"location\": \"\\ubd80\\uc0b0, \\ud574\\uc6b4\\ub300\\uad6c\", \"rating\": 4.0, \"images\": [\"http
69f7?w=500\", \"https://images.unsplash.com/photo-1590073242678-70ee3fc28e8e?w=500\", \"https://images.unsplash.com/photo-1551882547-ff40c63fe5fa?w=500\"
574\\uc6b4\\ub300 \\ud574\\uc218\\uc695\\uc7a5 \\ubc14\\ub85c \\uc55e\\uc5d0 \\uc704\\uce58\\ud55c \\ub9ac\\uc870\\ud2b8\\uc785\\ub2c8\\ub2e4. \\uac00\\u
```

캐싱된 호텔 목록 및 로그인 실패 이력 데이터

인프라 - ACM



퍼블릭 인증서 요청

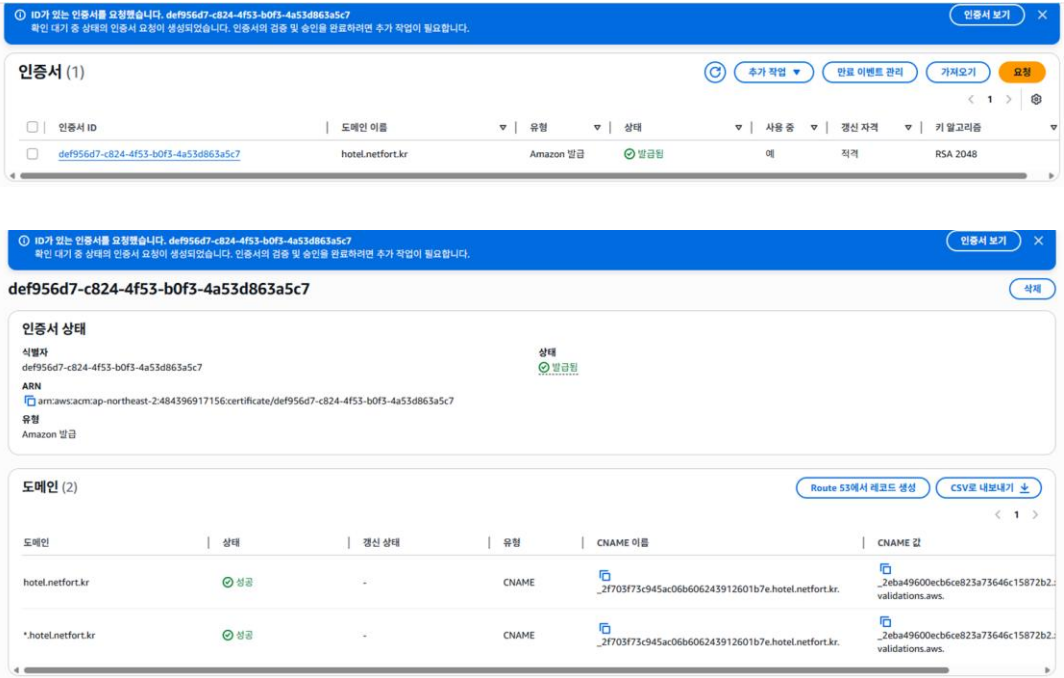
- 웹 브라우저나 공개적으로 사용가능한 인증서를 Amazon으로부터 발급받는 과정
- HTTPS 프로토콜로 안전하게 통신할 수 있도록 해줌

도메인 이름

- 메인 도메인과 서브 도메인을 하나의 인증서로 함께 보호할 수 있게 해줌

netfort

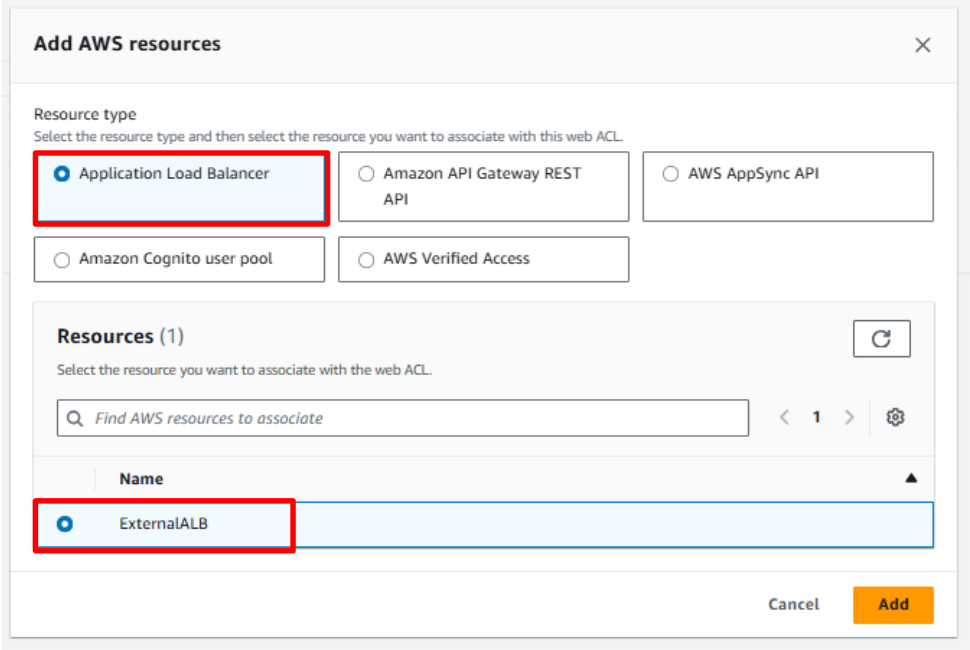
인프라 - ACM



ACM 인증서 생성 및 발급 상태 확인 후, 호스팅 영역에서 CNAME 확인

netfort

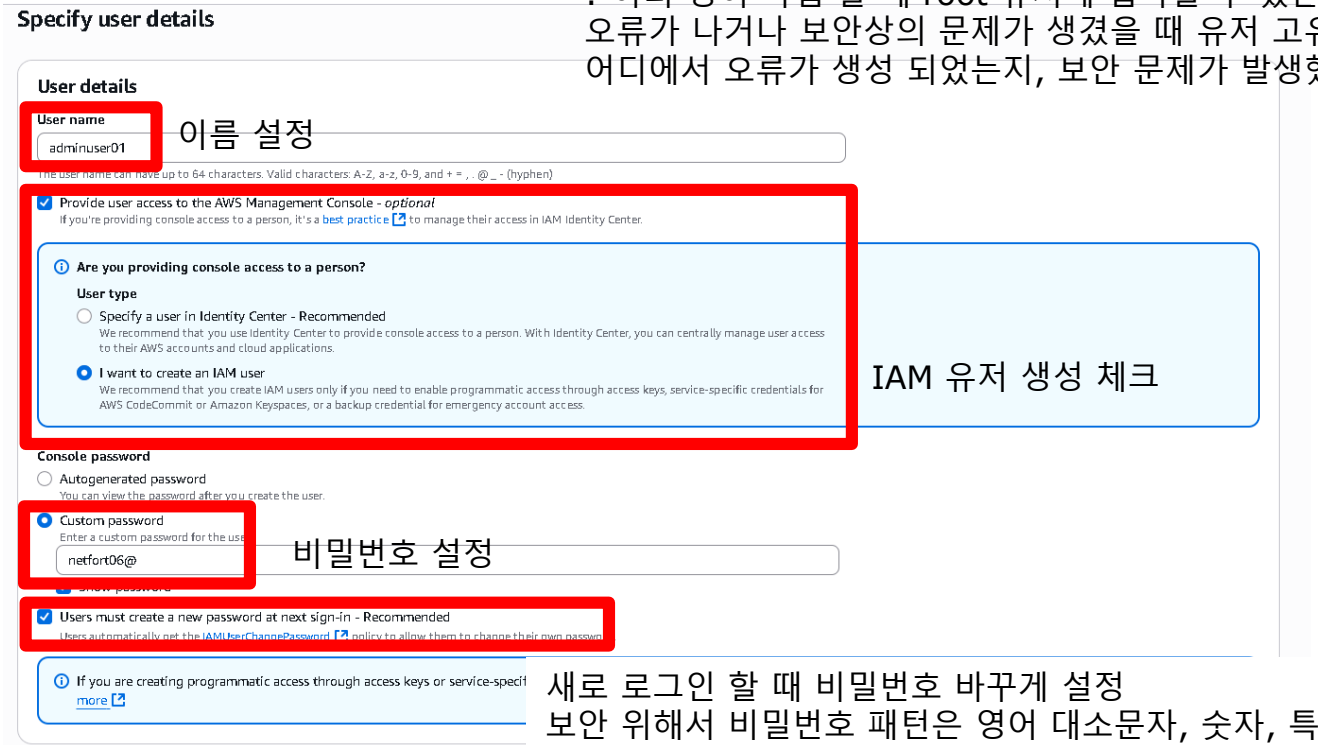
WAF 설정



WAF를 ALB에 연동하여 보안 규칙에 따라 요청을 허용 또는 차단하도록 설정

IAM 유저 생성 - adminuser

Admin 유저 생성 이유
: 여러 명이 작업 할 때 root 유저에 접속할 수 있는 인원 제한 有
오류가 나거나 보안상의 문제가 생겼을 때 유저 고유의 식별 번호를 통해
어디에서 오류가 생성 되었는지, 보안 문제가 발생했는지 쉽게 식별 가능



새로 로그인 할 때 비밀번호 바꾸게 설정
보안 위해서 비밀번호 패턴은 영어 대소문자, 숫자, 특수문자 포함하게 설정

IAM 유저 생성 - adminuser

Set permissions

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. Learn more

Permissions options

- Add user to group
  Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.
- Copy permissions
  Copy all group memberships, attached managed policies, and inline policies from an existing user.
- **Attach policies directly** (권한 설정)
  Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

Permissions policies (1/1378)

Choose one or more policies to attach to your new user.

Create policy

Filter by Type

Search | All types

1 2 3 4 5 6 7 ... 69

Policy name	Type	Attached entities
AccessAnalyzerServiceRolePolicy	AWS managed	0
AdministratorAccess	AWS managed - job function	0
AdministratorAccess-Amplify	AWS managed	0

Admin 권한 주기

IAM 유저 생성 - adminuser

Review and create

Review your choices. After you create the user, you can view and download the autogenerated password, if enabled.

User details

User name	Console password type	Require password reset
adminuser01	Custom password	Yes

Permissions summary

최종 정보 확인

AdministratorAccess	AWS managed - job function	Permissions policy
IAMUserChangePassword	AWS managed	Permissions policy

Tags - *optional*

Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.

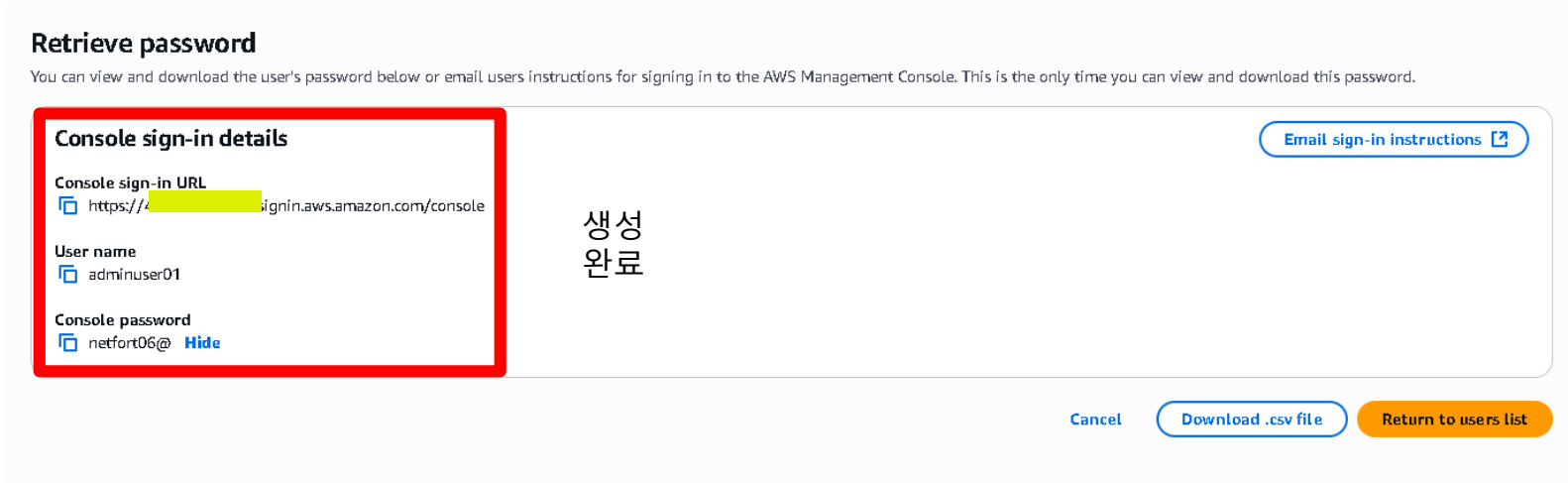
No tags associated with the resource.

Add new tag

You can add up to 50 more tags.

Cancel Previous Create user

IAM 유저 생성 - adminuser



IAM 유저 생성 - cloudwatch

Specify user details

User details

User name

clodwatch 이름 설정

The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (hyphen)

☐ Provide user access to the AWS Management Console - *optional*

If you're providing console access to a person, it's a best practice to manage their access in IAM Identity Center.

ⓘ If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, you can generate them after you create this IAM user. Learn more

Cancel Next

IAM 유저 생성 - cloudwatch

Set permissions

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. Learn more

Permissions options

- Add user to group
  Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.
- Copy permissions
  Copy all group memberships, attached managed policies, and inline policies from an existing user.
- **Attach policies directly**
  Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

권한 설정

Permissions policies (6/1378)

Choose one or more policies to attach to your new user.

권한 선택

Create policy

Filter by Type

cloudwatch | All types | 52 matches | 1 2 3

Policy name	Type	Attached entities
AmazonAPIGatewayPushToCloudWatchLogs	AWS managed	0
AmazonCloudWatchEvidentlyFullAccess	AWS managed	0
AmazonCloudWatchEvidentlyReadOnlyAccess	AWS managed	0
AmazonCloudWatchEvidentlyServiceRolePolicy	AWS managed	0
AmazonCloudWatchRUMFullAccess	AWS managed	0

IAM 유저 생성 - cloudwatch

Review and create

Review your choices. After you create the user, you can view and download the autogenerated password, if enabled.

User details

User name	Console password type	Require password reset
clodwatch	None	No

Permissions summary

1

Name	Type	Used as
AmazonCloudDirectoryFullAccess	AWS managed	Permissions policy
AmazonCloudWatchEvidentlyFullAccess	AWS managed	Permissions policy
AmazonCloudWatchRUMFullAccess	AWS managed	Permissions policy
CloudWatchFullAccess	AWS managed	Permissions policy
CloudWatchFullAccessV2	AWS managed	Permissions policy
CloudWatchLogsFullAccess	AWS managed	Permissions policy

최종 정보 확인

Tags - *optional*

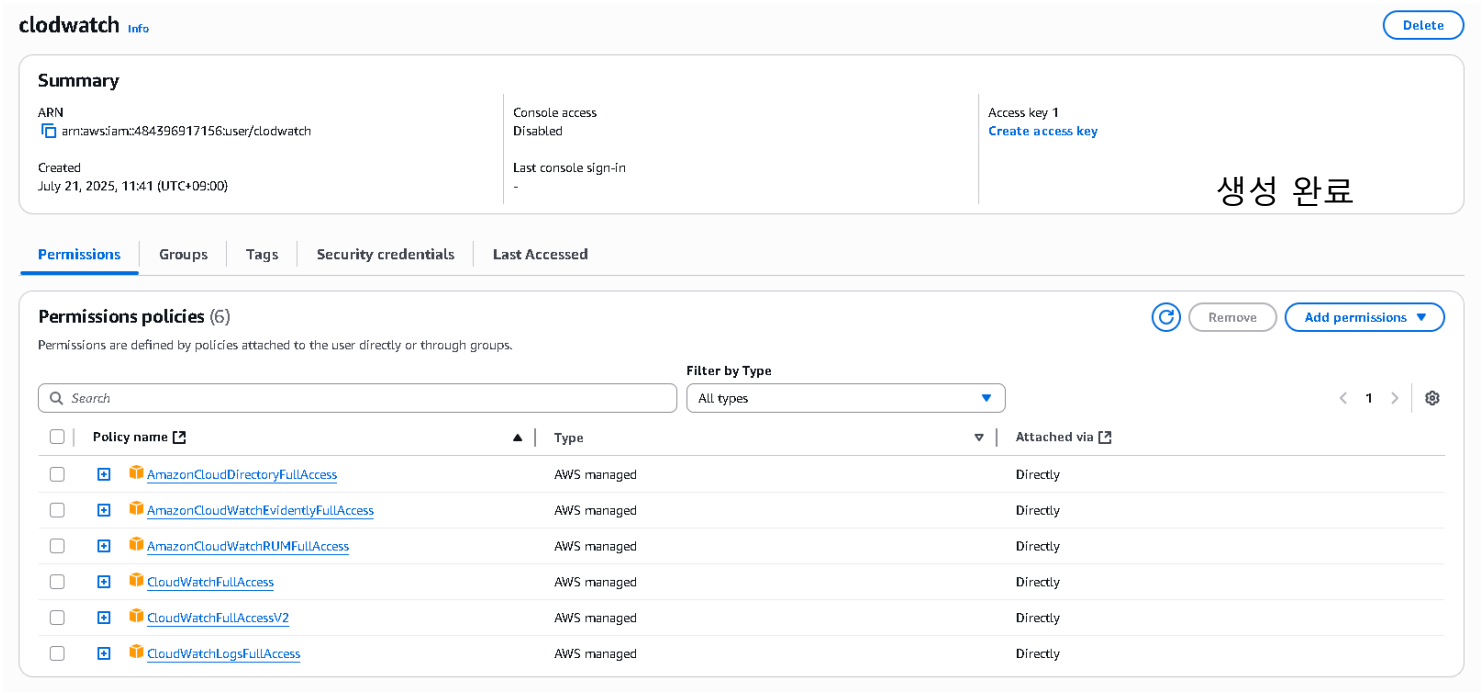
Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.

No tags associated with the resource.

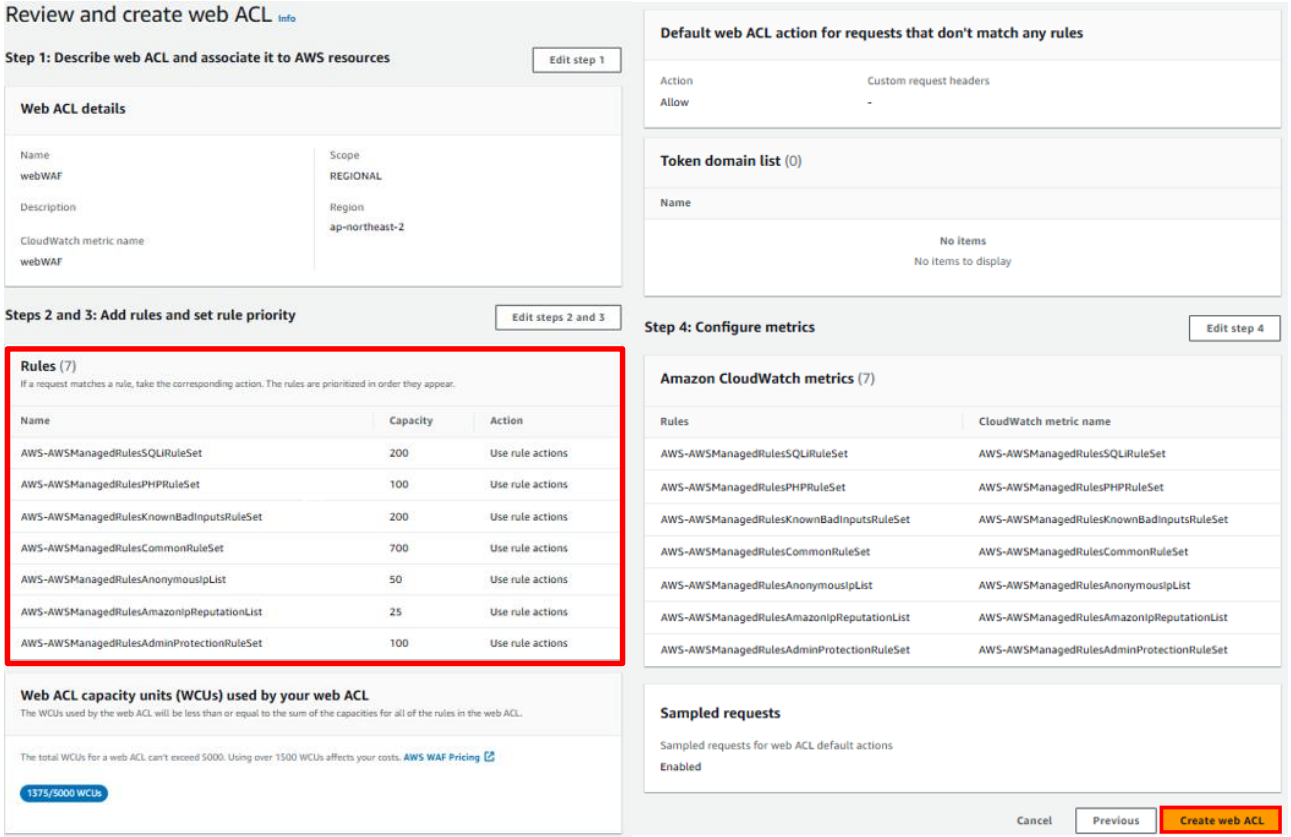
Add new tag

You can add up to 50 more tags.

IAM 유저 생성 - cloudwatch



WAF 설정



Review and create web ACL Info

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

Web ACL details

Name	Scope
webWAF	REGIONAL
Description	Region
	ap-northeast-2
CloudWatch metric name	
webWAF	

Steps 2 and 3: Add rules and set rule priority — Edit steps 2 and 3

Rules (7)

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

Name	Capacity	Action
AWS-AWSManagedRulesSQLiRuleSet	200	Use rule actions
AWS-AWSManagedRulesPHPRuleSet	100	Use rule actions
AWS-AWSManagedRulesKnownBadInputsRuleSet	200	Use rule actions
AWS-AWSManagedRulesCommonRuleSet	700	Use rule actions
AWS-AWSManagedRulesAnonymousIpList	50	Use rule actions
AWS-AWSManagedRulesAmazonIpReputationList	25	Use rule actions
AWS-AWSManagedRulesAdminProtectionRuleSet	100	Use rule actions

Web ACL capacity units (WCUs) used by your web ACL

The WCUs used by the web ACL will be less than or equal to the sum of the capacities for all of the rules in the web ACL.

The total WCUs for a web ACL can't exceed 5000. Using over 1500 WCUs affects your costs. AWS WAF Pricing

1375/5000 WCUs

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

Action	Custom request headers
Allow	-

Token domain list (0)

Name

No items

No items to display

Step 4: Configure metrics — Edit step 4

Amazon CloudWatch metrics (7)

Rules	CloudWatch metric name
AWS-AWSManagedRulesSQLiRuleSet	AWS-AWSManagedRulesSQLiRuleSet
AWS-AWSManagedRulesPHPRuleSet	AWS-AWSManagedRulesPHPRuleSet
AWS-AWSManagedRulesKnownBadInputsRuleSet	AWS-AWSManagedRulesKnownBadInputsRuleSet
AWS-AWSManagedRulesCommonRuleSet	AWS-AWSManagedRulesCommonRuleSet
AWS-AWSManagedRulesAnonymousIpList	AWS-AWSManagedRulesAnonymousIpList
AWS-AWSManagedRulesAmazonIpReputationList	AWS-AWSManagedRulesAmazonIpReputationList
AWS-AWSManagedRulesAdminProtectionRuleSet	AWS-AWSManagedRulesAdminProtectionRuleSet

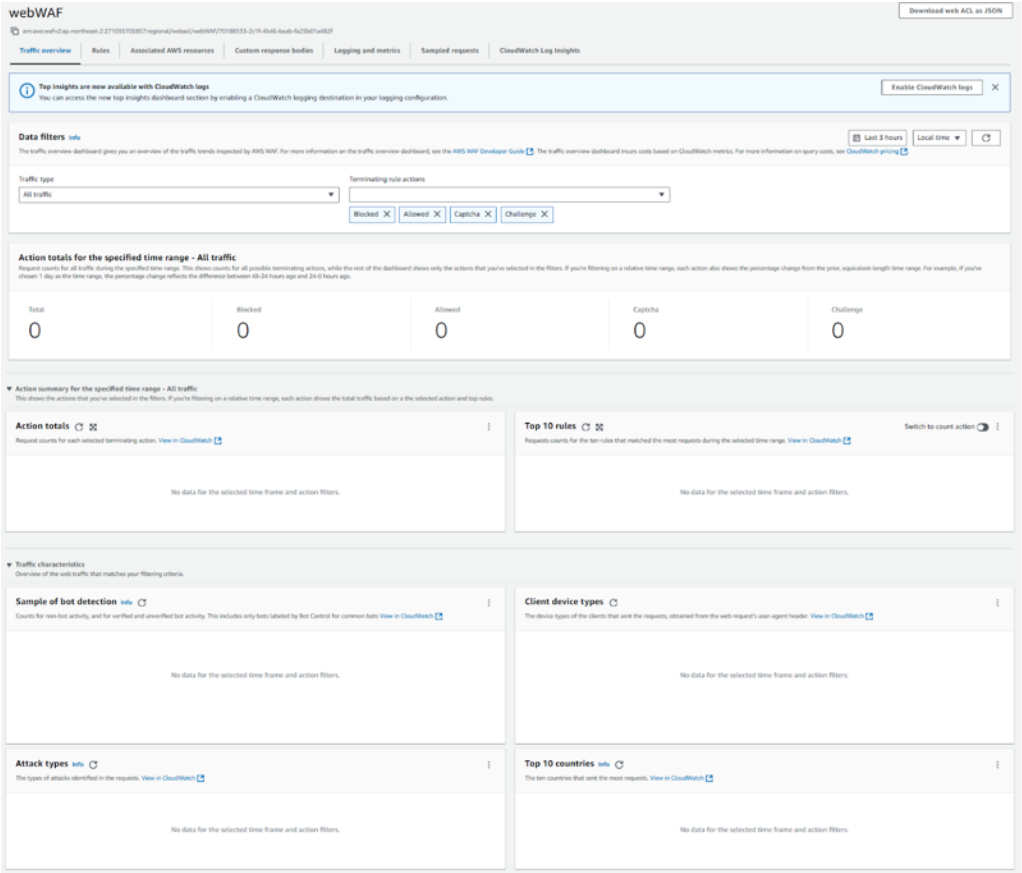
Sampled requests

Sampled requests for web ACL default actions

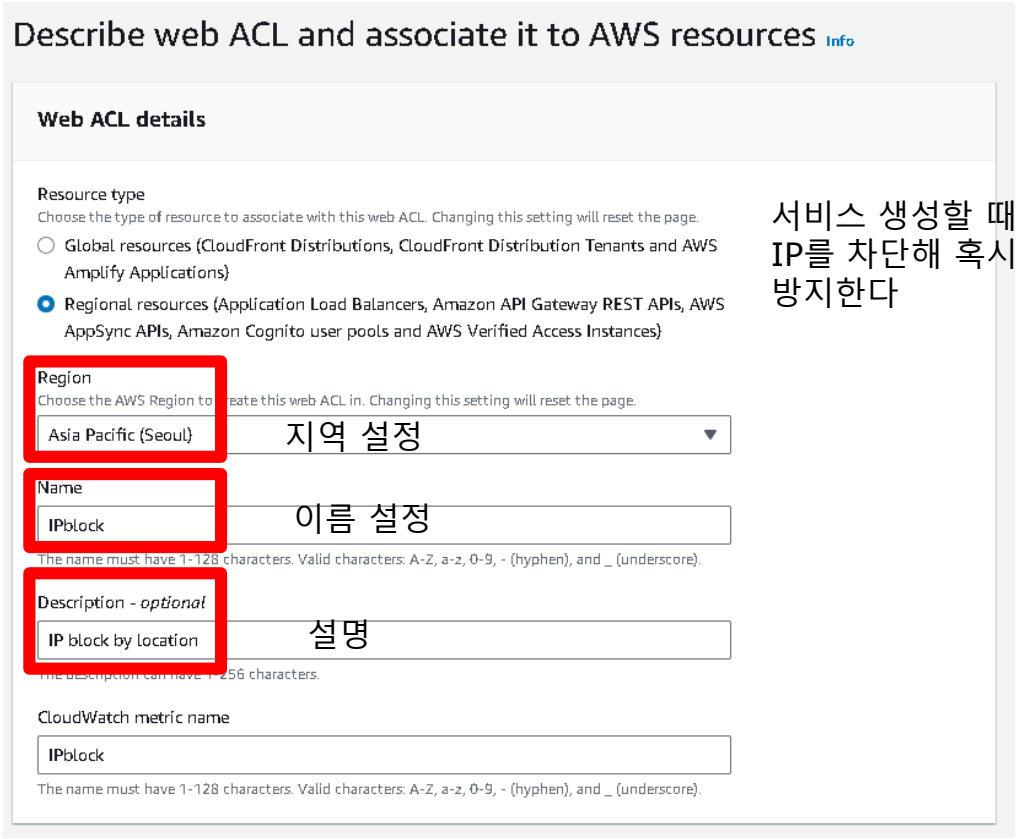
Enabled

Cancel | Previous | Create web ACL

WAF 설정


webWAF
Download web ACL as JSON
Traffic overview
Rules
Associated AWS resources
Custom response bodies
Logging and metrics
Sampled requests
CloudWatch Log insights
Top insights are now available with CloudWatch logs
You can access the new top insights dashboard section by enabling a CloudWatch logging destination in your logging configuration.
Enable CloudWatch logs
Data filters
Last 3 hours
Local time
Traffic type
All traffic
Terminating rule actions
Blocked
Allowed
Captcha
Challenge
Action totals for the specified time range - All traffic
Total
0
Blocked
0
Allowed
0
Captcha
0
Challenge
0
Action summary for the specified time range - All traffic
Action totals
No data for the selected time frame and action filters.
Top 10 rules
Switch to count action
No data for the selected time frame and action filters.
Traffic characteristics
Sample of bot detection
No data for the selected time frame and action filters.
Client device types
No data for the selected time frame and action filters.
Attack types
No data for the selected time frame and action filters.
Top 10 countries
No data for the selected time frame and action filters.

IP 차단 - WAF



서비스 생성할 때 지역기반으로 IP를 차단해 혹시나 있을 공격을 방지한다

IP 차단 - WAF

Add rules and rule groups Info

A rule defines attack patterns to look for in web requests and the action to take when a request matches the patterns. Rule groups are reusable collections of rules. You can use managed rule groups offered by AWS and AWS Marketplace sellers. You can also write your own rules and use your own rule groups.

Rules (0)

Edit | Delete | Add rules ▲

If a request matches a rule, take the corresponding action. The rules a

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

Name	Capacity

No rules.

You don't have any rules added.

내 규칙 추가하기

Add my own rules and rule groups Info

Rule type

Rule type

- **IP set** — Use IP sets to identify a specific list of IP addresses.
- **Rule builder** — Use a custom rule to inspect for patterns including query strings, headers, countries, and rate limit violations.
- **Rule group** — Use a rule group to combine rules into a single logical set.

Rule Builder

Rule builder

Rule visual editor | Rule JSON editor

You can use the JSON editor for complex statement nesting, for example to nest two OR statements inside an AND statement. The visual editor handles one level of nesting. For web ACLs and rule groups with complex nesting, the visual editor is disabled.

Rule

Validate

Name

blockChina

이름 설정

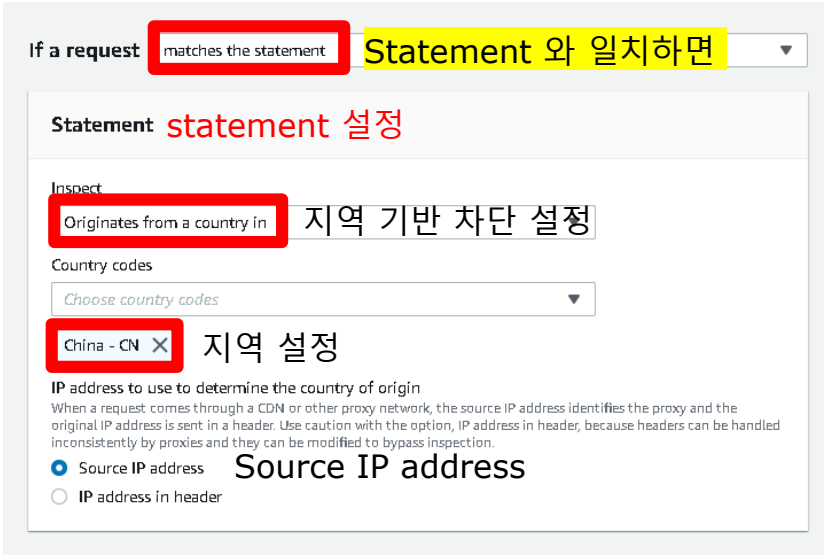
The name must have 1- 8 characters. Valid characters: A-Z, a-z, 0-9, - (hyphen), and _ (underscore).

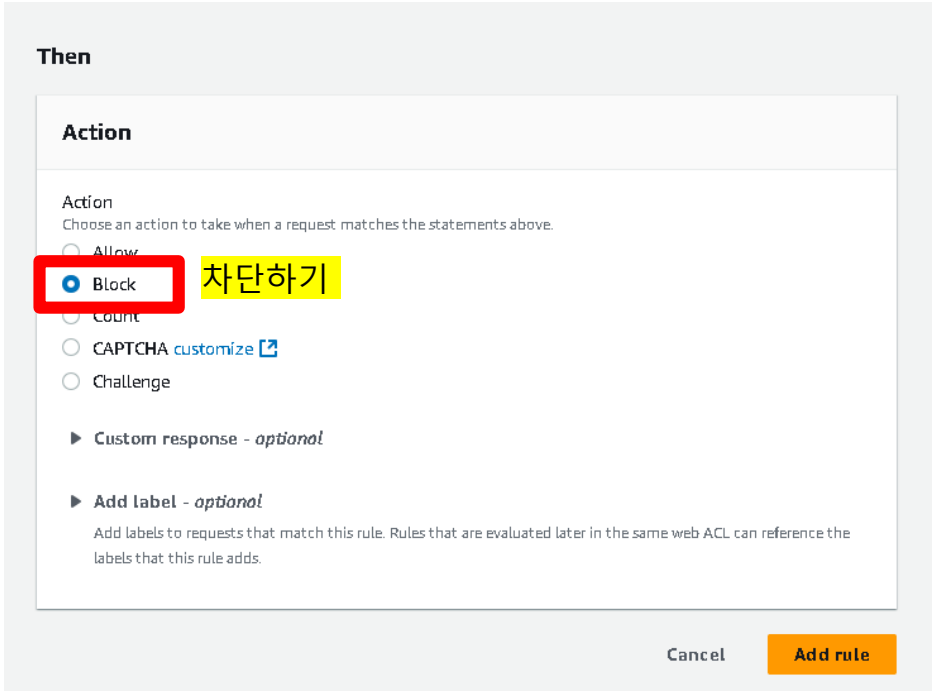
Type

- Regular rule
- Rate-based rule

Limits request rates for requests that match your criteria. Applies the action to matching requests when the limit is reached, and removes the action when the rate falls below the limit.

IP 차단 - WAF


If a request
matches the statement
Statement 와 일치하면
Statement
statement 설정
Inspect
Originates from a country in
지역 기반 차단 설정
Country codes
Choose country codes
China - CN
지역 설정
IP address to use to determine the country of origin
When a request comes through a CDN or other proxy network, the source IP address identifies the proxy and the original IP address is sent in a header. Use caution with the option, IP address in header, because headers can be handled inconsistently by proxies and they can be modified to bypass inspection.
Source IP address
Source IP address
IP address in header


Then
Action
Action
Choose an action to take when a request matches the statements above.
Allow
Block
차단하기
Count
CAPTCHA customize
Challenge
Custom response - optional
Add label - optional
Add labels to requests that match this rule. Rules that are evaluated later in the same web ACL can reference the labels that this rule adds.
Cancel
Add rule

IP 차단 - WAF

Add rules and rule groups Info

A rule defines attack patterns to look for in web requests and the action to take when a request matches the patterns. Rule groups are reusable collections of rules. You can use managed rule groups offered by AWS and AWS Marketplace sellers. You can also write your own rules and use your own rule groups.

Rules (1)

Edit | Delete | Add rules

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

Name	Capacity	Action
blockChina	1	Block

완성

Add rules and rule groups Info

A rule defines attack patterns to look for in web requests and the action to take when a request matches the patterns. Rule groups are reusable collections of rules. You can use managed rule groups offered by AWS and AWS Marketplace sellers. You can also write your own rules and use your own rule groups.

Rules (7)

Edit | Delete | Add rules

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

Name	Capacity	Action
blockChina	1	Block
blockRussia	1	Block
blockIsrael	1	Block
blockIran	1	Block
blockIraq	1	Block
captchaIndia	1	CAPTCHA
captchaUS	1	CAPTCHA

같은 방법으로 규칙 더 생성하기

IP 차단 - WAF

Set rule priority Info

우선순위 설정

Rules (7)

Move up | Move down

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

	Name	Capacity	Action
○	blockChina	1	Block
○	blockRussia	1	Block
○	blockIsrael	1	Block
○	blockIran	1	Block
○	blockIraq	1	Block
○	captchaIndia	1	CAPTCHA
○	captchaUS	1	CAPTCHA

Cancel | Previous | Next

Configure metrics Info

Amazon CloudWatch metrics

CloudWatch metrics allow you to monitor web requests, web ACLs, and rules.

Rules	CloudWatch metric name
☑ blockChina	blockChina
☑ blockRussia	blockRussia
☑ blockIsrael	blockIsrael
☑ blockIran	blockIran
☑ blockIraq	blockIraq
☑ captchaIndia	captchaIndia
☑ captchaUS	captchaUS

Request sampling options

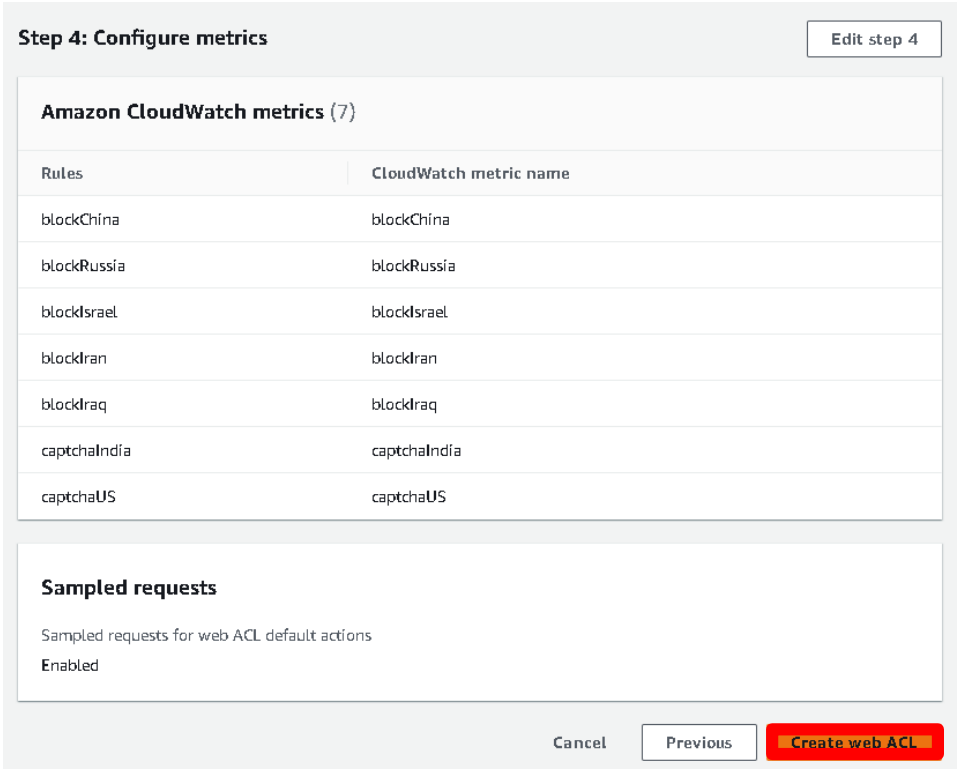
If you disable request sampling, you can't view requests that match your web ACL rules.

◉ Enable sampled requests

Enable sampled requests

○ Enable sampled requests with exclusions

IP 차단 - WAF



Create web ACL

IP 차단 - Web ACLs

2025-07-24T11:29:32.343+09:00 {"timestamp":1753324172343,"formatVersion":1,"webaclId":"arn:aws:wafv2:ap-northeast-2:4

```
{
    "timestamp": 1753324172343,
    "formatVersion": 1,
    "webaclId": "arn:aws:wafv2:ap-northeast-2:484396917156:regional/webacl/webWAF/596e81c8-55e8-4c8a-9b78-444d729665f5",
    "terminatingRuleId": "AWS-AWSManagedRulesCommonRuleSet",
    "terminatingRuleType": "MANAGED_RULE_GROUP",
    "action": "BLOCK",
    "terminatingRuleMatchDetails": [
        {
            "conditionType": "XSS",
            "location": "BODY",
            "matchedData": [
                "onerror",
                "alert('XSS')"
            ],
            "matchedFieldName": ""
        }
    ],
    "httpSourceName": "ALB",
    "httpSourceId": "484396917156-app/ExternalALB/1769f93447726f9c",
    "ruleGroupList": [
        {
            "ruleGroupId": "AWS#AWSManagedRulesAdminProtectionRuleSet",
            "terminatingRule": null,
            "nonTerminatingMatchingRules": [],
            "excludedRules": null,
            "customerConfig": null
        },
        {
            "ruleGroupId": "AWS#AWSManagedRulesAmazonIpReputationList",
            "terminatingRule": null,
            "nonTerminatingMatchingRules": [],
            "excludedRules": null,
            "customerConfig": null
```

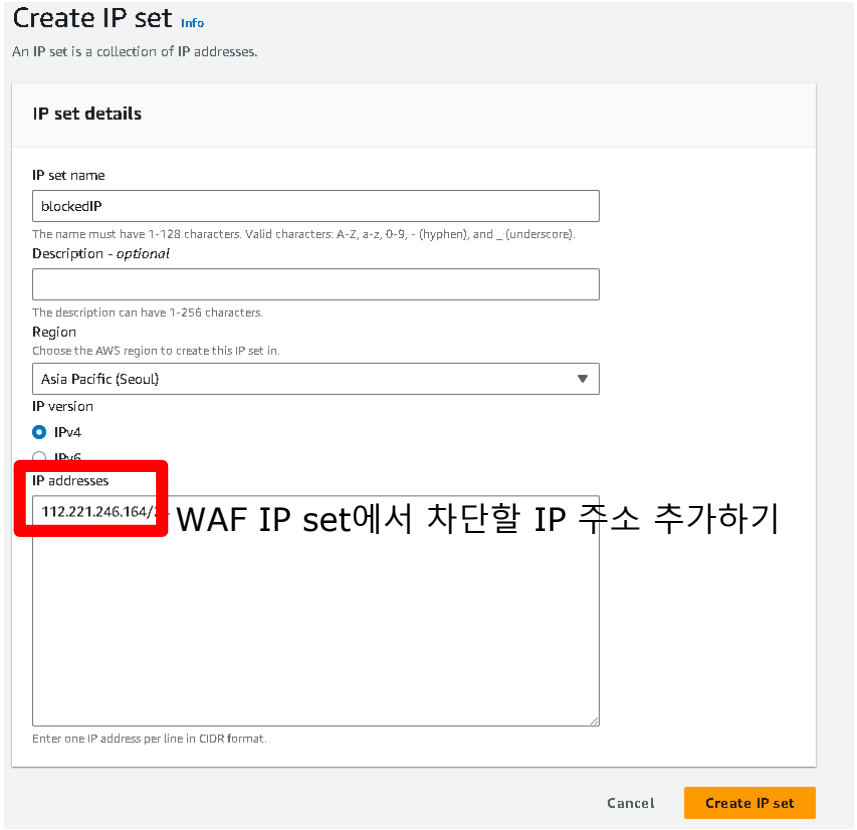

XSS 공격 차단한 로그가 뜸

IP 차단 - Web ACLs


```
"rateBasedRuleList": [],
"nonTerminatingMatchingRules": [],
"requestHeadersInserted": null,
"responseCodeSent": null,
"httpRequest": {
    "clientIp": "112.221.246.164"
    "country": "KR",
    "headers": [
        {
            "name": "host",
            "value": "api.hotel.netfort.kr"
        },
        {
            "name": "content-length",
            "value": "277"
        },
        {
            "name": "sec-ch-ua-platform",
            "value": "\"Windows\""
        },
        {
            "name": "authorization",
            "value": "Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiJ0ZXN0QHRlc3QuY29tIiwiZXhwIjoxNzUzNDEwNTA4fQ.1taT7fhFjEADPhL
        },
        {
            "name": "user-agent",
            "value": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36"
        },
        {
            "name": "accept",
            "value": "application/json, text/plain, */*"
        },
        {
            "name": "sec-ch-ua",
            "value": "\"Not)A;Brand\";v=\"8\", \"Chromium\";v=\"138\", \"Google Chrome\";v=\"138\""
```

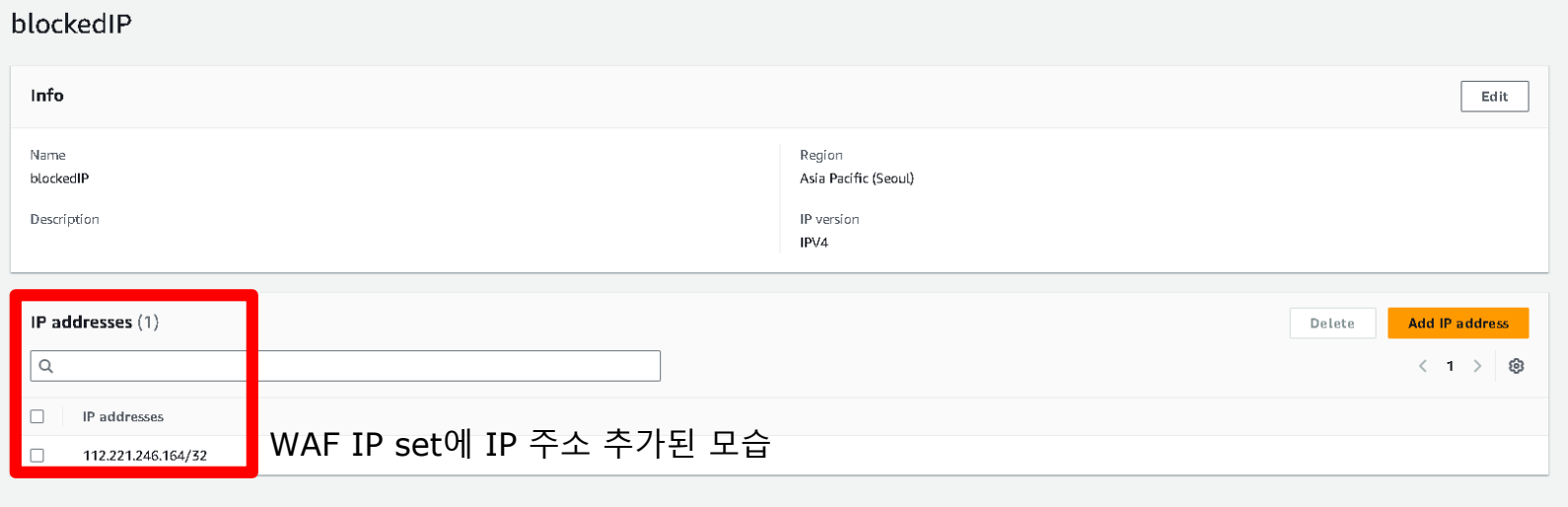

위 공격을 한 IP 주소 112.221.246.164

IP 차단 - Web ACLs



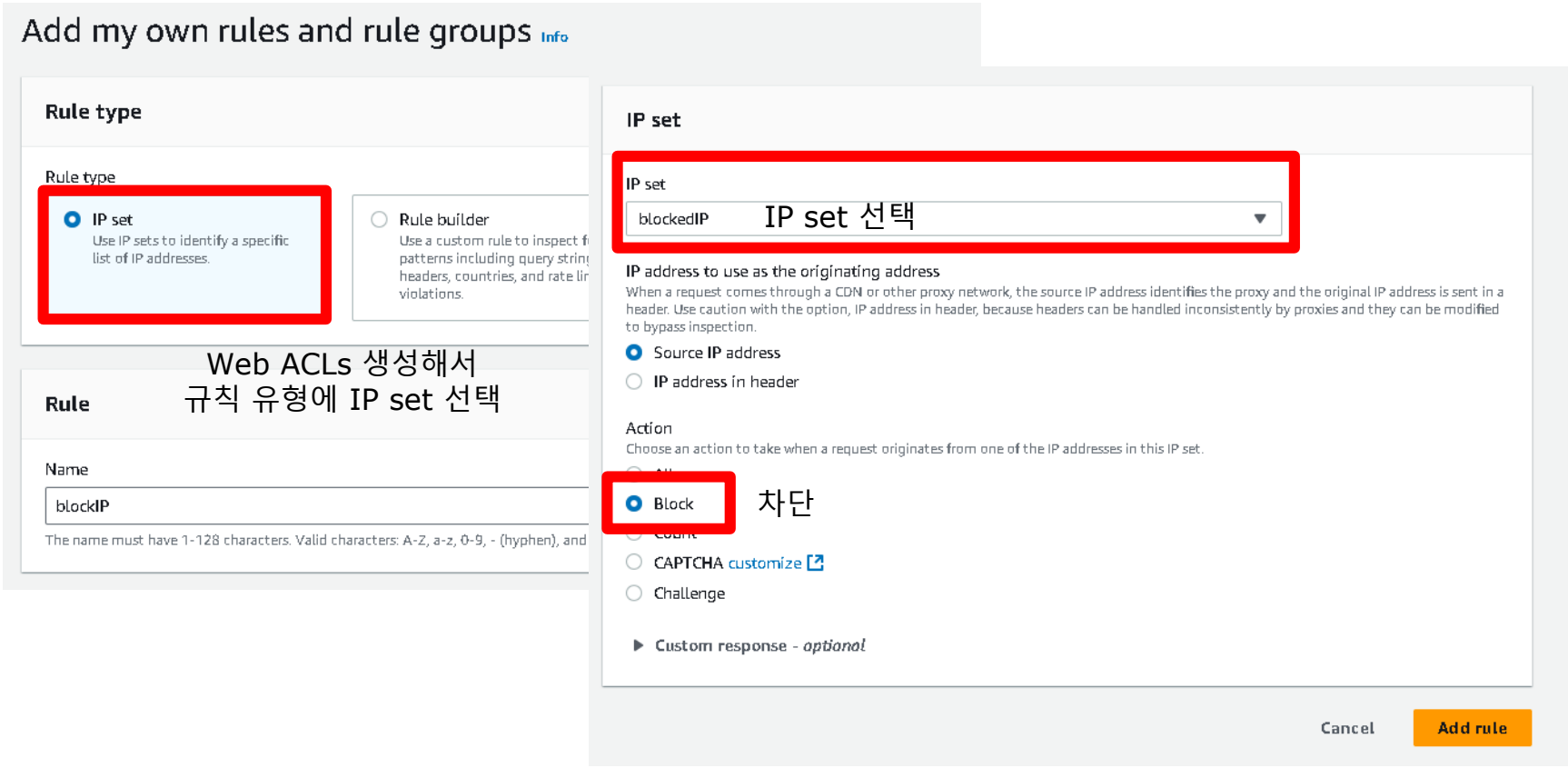
WAF IP set에서 차단할 IP 주소 추가하기

IP 차단 - Web ACLs

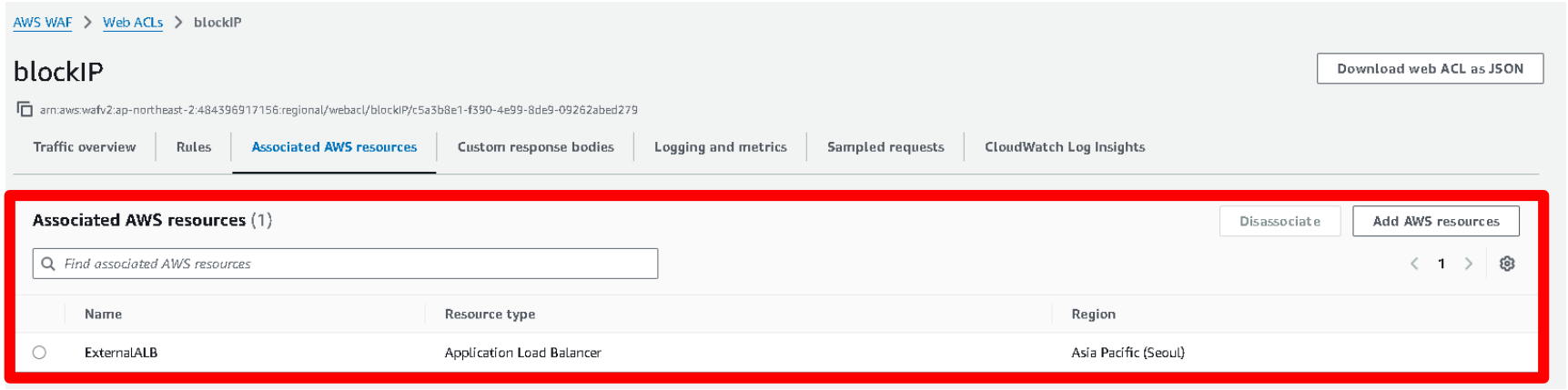


WAF IP set에 IP 주소 추가된 모습

IP 차단 - Web ACLs

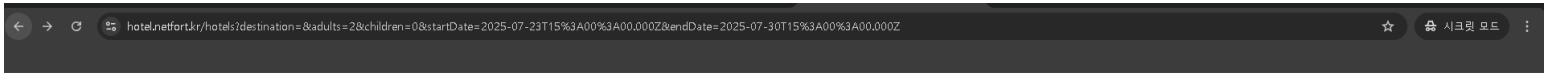


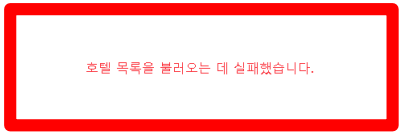
IP 차단 - Web ACLs



웹페이지 EC2에 연결된 ALB와 연결하기

IP 차단 - Web ACLs





성공적으로 차단된 모습

IP 차단 - Network ACLs

2025-07-24T13:26:05.913+09:00 {"timestamp":1753331165913,"formatVersion":1,"webaclId":"arn:aws:wafv2:ap-northeast-


```
{
    "timestamp": 1753331165913,
    "formatVersion": 1,
    "webaclId": "arn:aws:wafv2:ap-northeast-2:484396917156:regional/webacl/webWAF/596e81c8-55e8-4c8a-9b78-444d729665f5",
    "terminatingRuleId": "AWS-AWSManagedRulesSQLiRuleSet",
    "terminatingRuleType": "MANAGED_RULE_GROUP",
    "action": "BLOCK",
    "terminatingRuleMatchDetails": [
        {
            "conditionType": "SQL_INJECTION",
            "location": "BODY",
            "matchedData": [
                "------WebKitFormBoundaryh5HrAjBuoz2UQYaq\nContent-Disposition: f",
                "OR",
                "1",
                "=",
                "1 ORDER BY 8122-- eGeQ\n------WebKitFormBoundaryh5HrAjBuoz2UQYaq"
            ],
            "matchedFieldName": "",
            "sensitivityLevel": "LOW"
        }
    ],
```

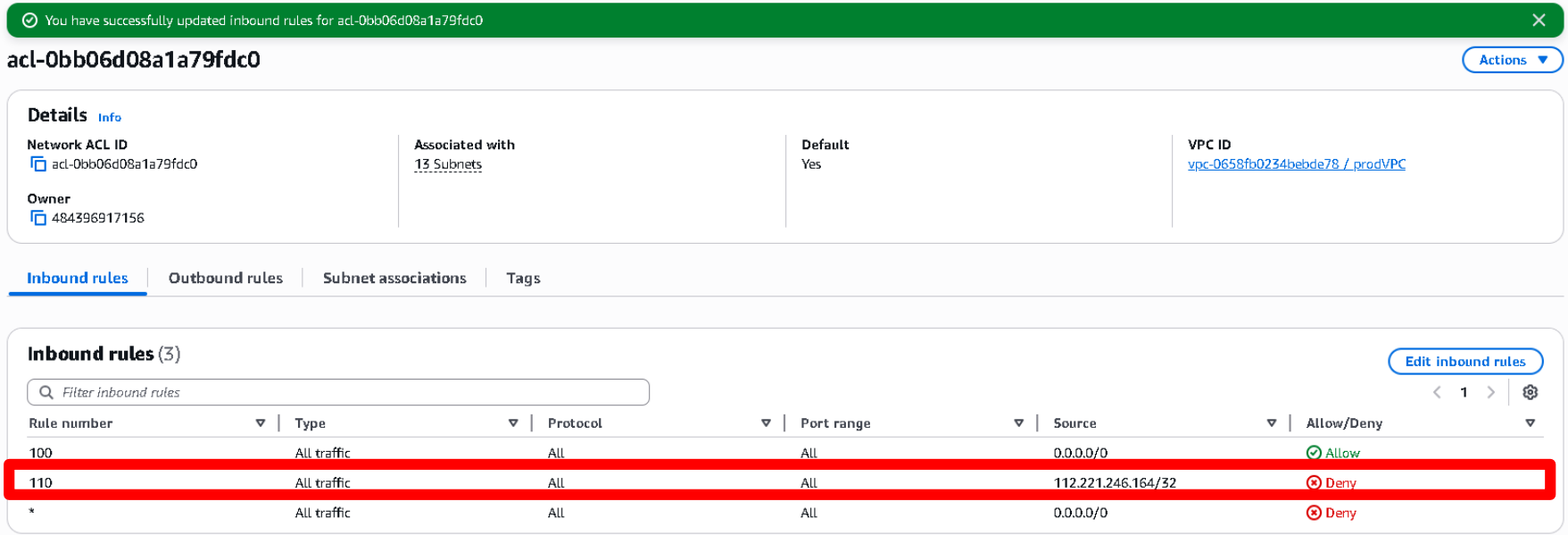

SQLi 공격 차단한 로그가 뜸

IP 차단 - Network ACLs


```
"rateBasedRuleList": [],
"nonTerminatingMatchingRules": [],
"requestHeadersInserted": null,
"responseCodeSent": null,
"httpRequest": {
    "clientIp": "112.221.246.164"
    "country": "KR",
    "headers": [
        {
            "name": "Accept-Encoding",
            "value": "identity"
        },
        {
            "name": "Content-Length",
            "value": "257"
        },
        {
            "name": "Host",
            "value": "api.hotel.netfort.kr"
        },
        {
            "name": "Authorization",
            "value": "Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiO
        },
        {
            "name": "Accept",
            "value": "application/json, text/plain, */*"
        },
```

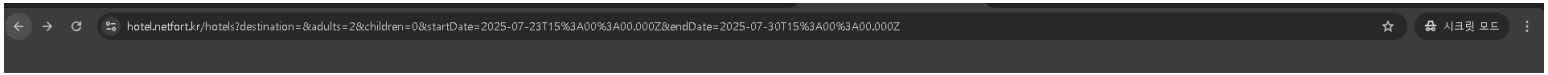

위 공격을 한 IP 주소 112.221.246.164

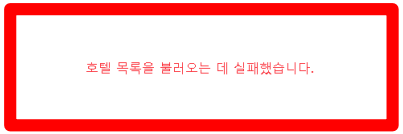
IP 차단 - Network ACLs



Network ACLs의 규칙에 IP 주소 추가하고 Deny 설정

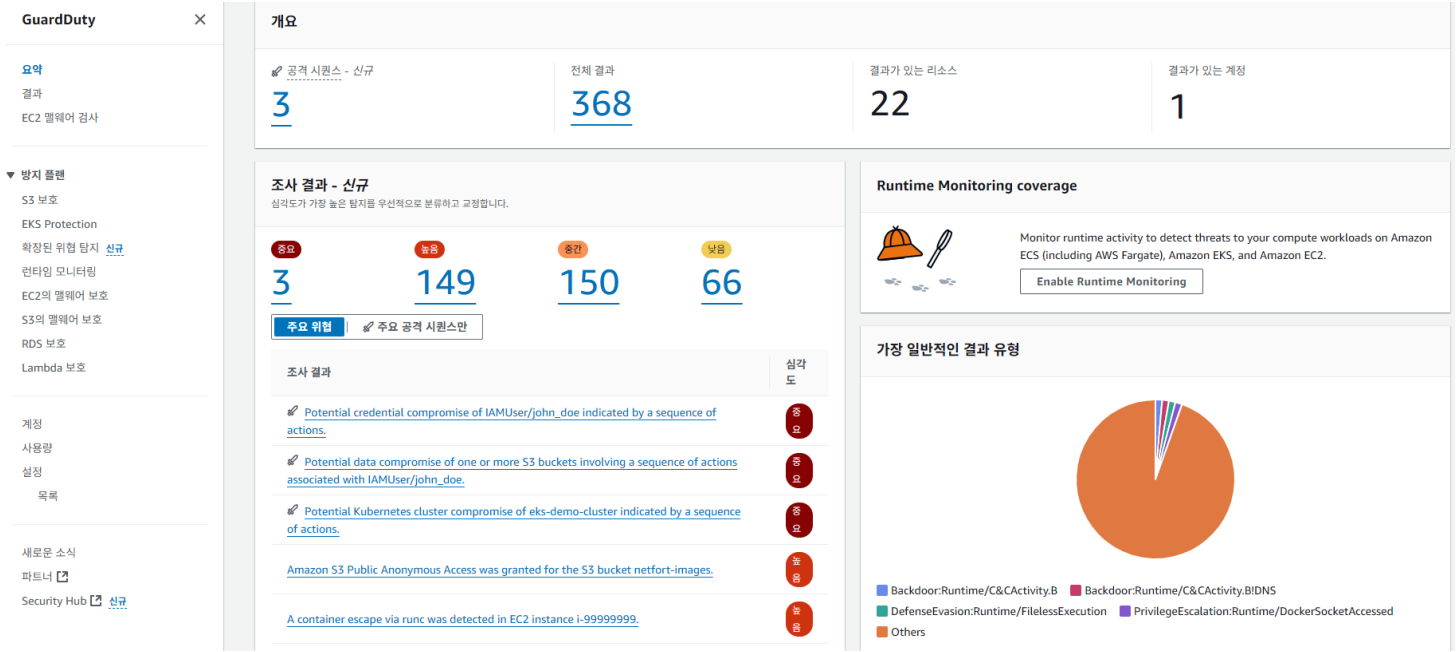
IP 차단 - Network ACLs





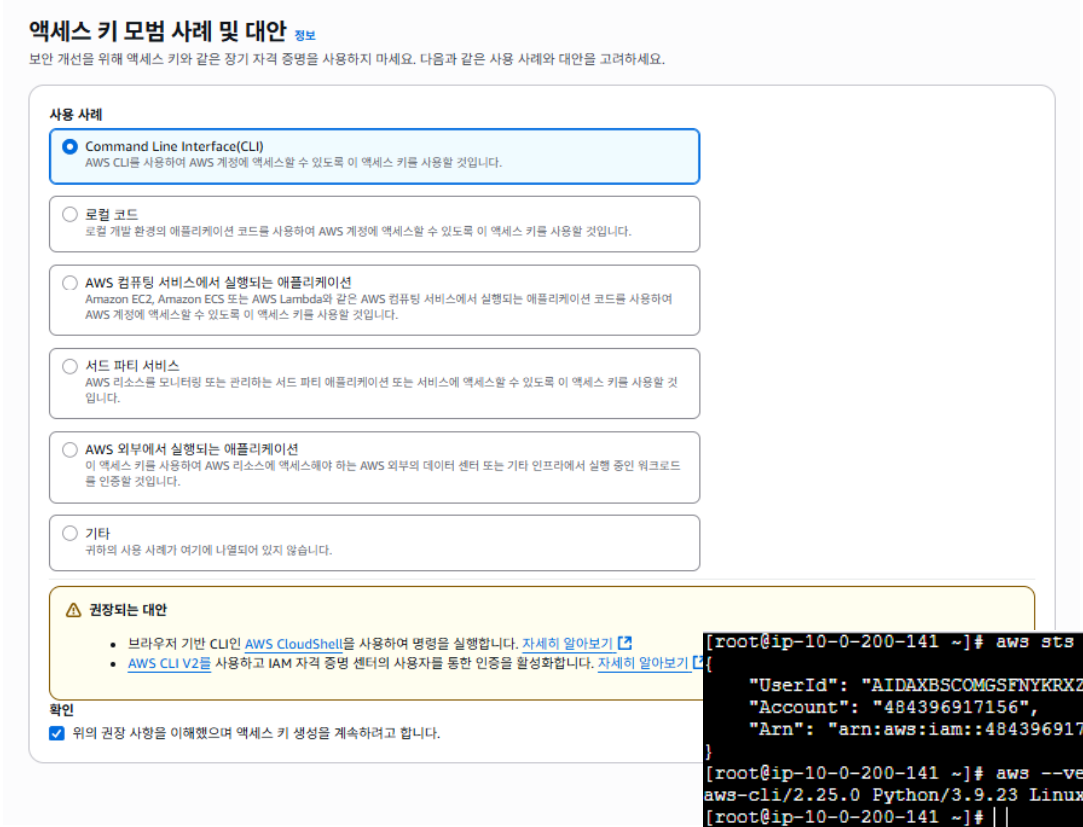
성공적으로 차단된 모습

보안 - GuardDuty



악의적인 활동이나 비정상적인 행위를 자동으로 탐지

모니터링 - Zabbix에 CLI 설치 및 구성




```
[root@ip-10-0-200-141 ~]# aws sts get-caller-identity
{
    "UserId": "AIDAXBSCOMGSFNYKRXZXW",
    "Account": "484396917156",
    "Arn": "arn:aws:iam::484396917156:user/zabbix-monitor"
}
[root@ip-10-0-200-141 ~]# aws --version
aws-cli/2.25.0 Python/3.9.23 Linux/6.1.141-165.249.amzn2023.x86_64 source/x86_64.amzn.2023
[root@ip-10-0-200-141 ~]#
```

- Zabbix에 AWS CLI를 구성
- 인증 검증 완료, CLI를 활용한 모니터링 자동화 환경 구축

CloudWatch 메트릭 수집 스크립트 준비

```
[root@ip-10-0-200-141 ~]# /etc/zabbix/scripts/cloudwatch_attack_monitor.sh
cpu_utilization=0.897925349634157
disk_write_bytes=0.0
disk_write_ops=0.0
network_in=605242.0
status_check_failed=0.0
[root@ip-10-0-200-141 ~]#
```

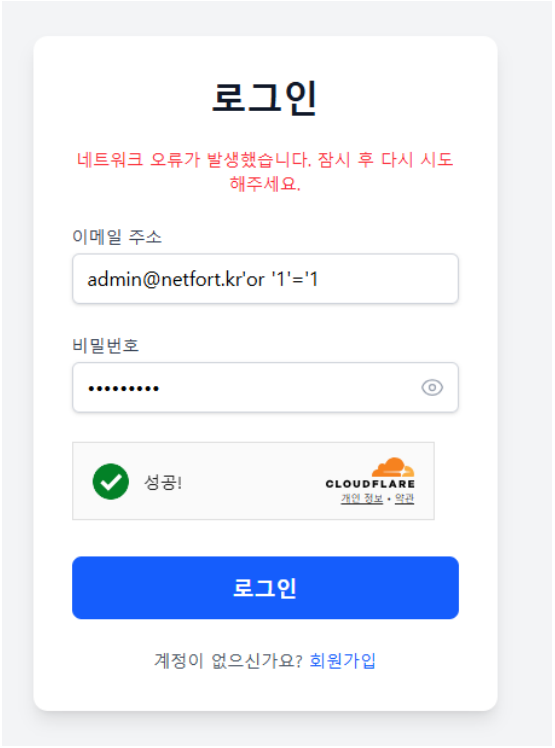
CloudWatch의 주요 시스템 메트릭을 수집하는 스크립트를 작성하고, Zabbix 서버의 외부 스크립트 디렉터리와 연동

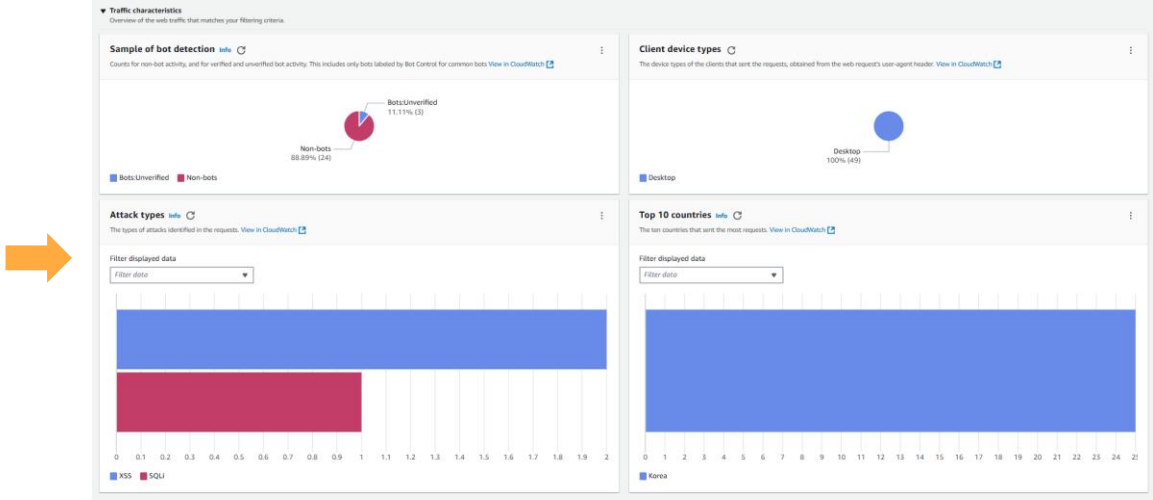
스크립트 실행시 실시간으로 데이터를 수집하여 공격시나리오에 대비

수집 메트릭

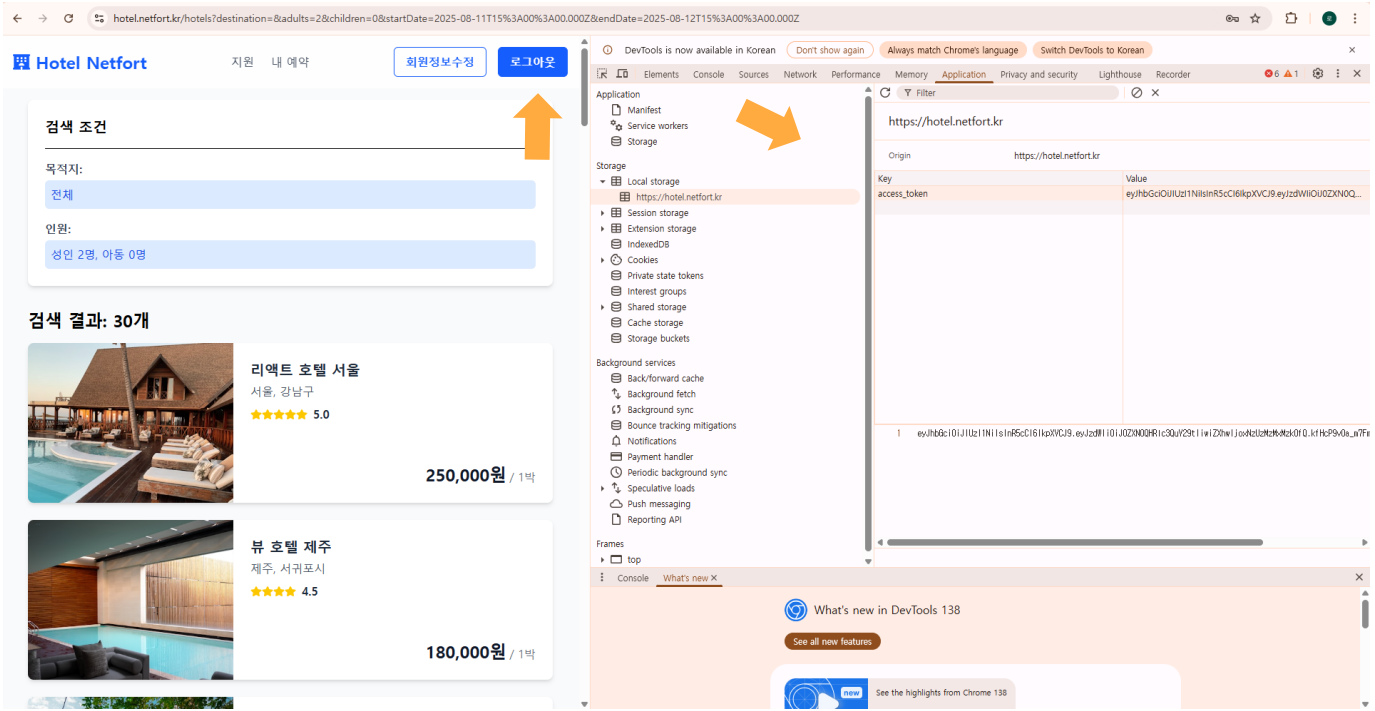
- CPU 사용률
- 디스크 쓰기 바이트
- 디스크 쓰기 작업
- 네트워크 트래픽
- 인스턴스 상태

다양한 SQLi 취약점 테스트



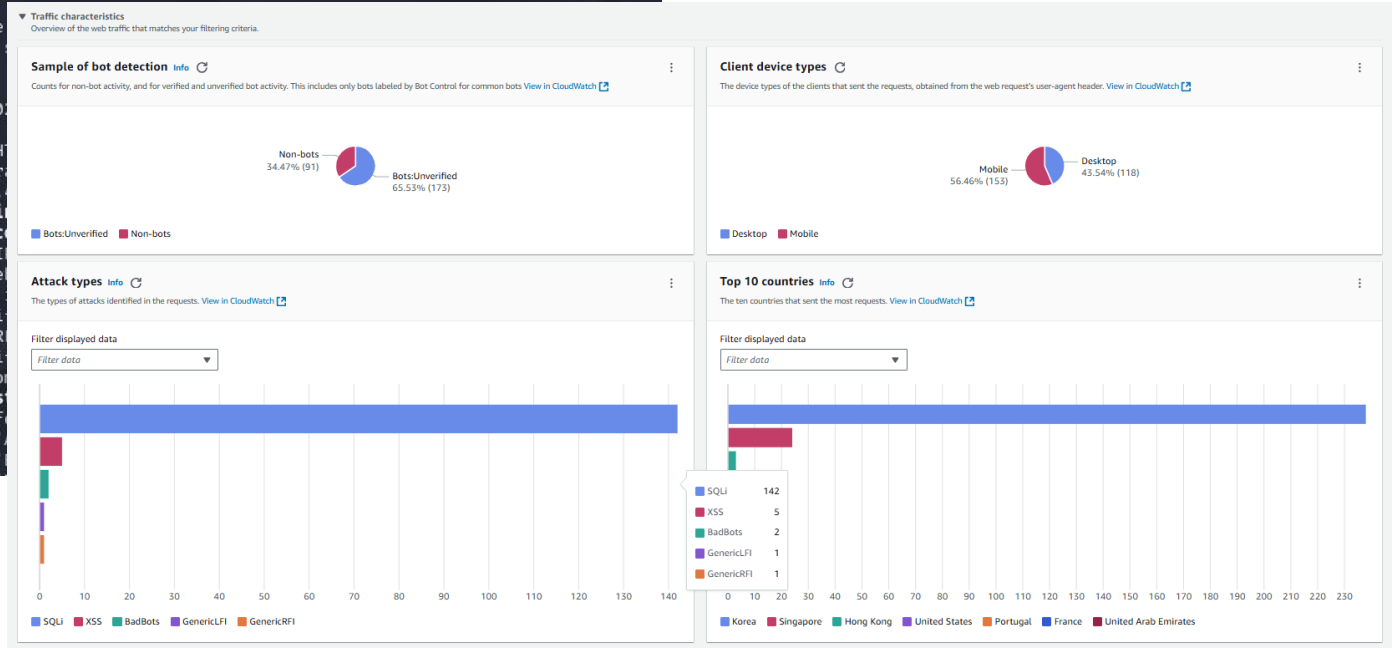


다양한 SQLi 취약점 테스트

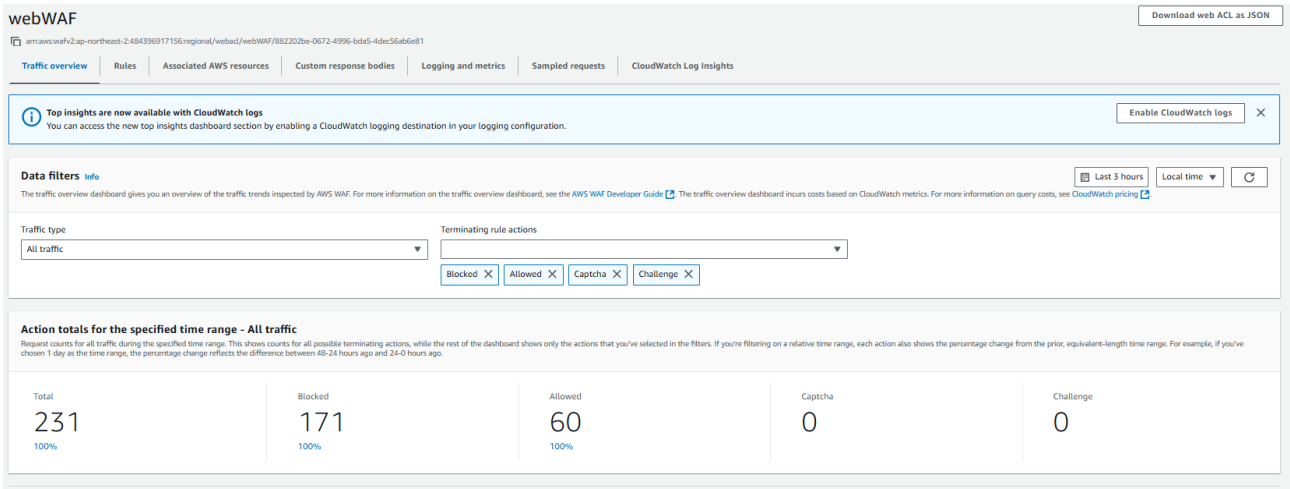


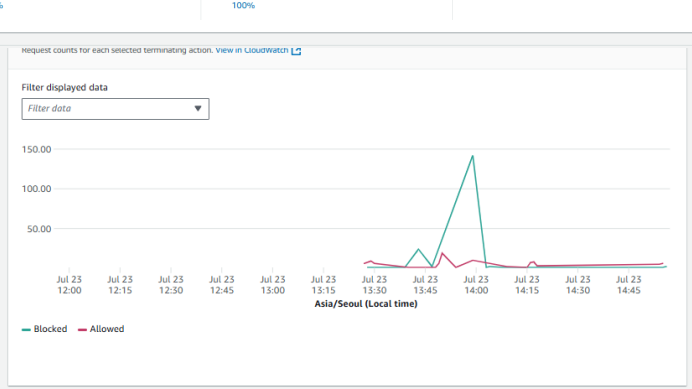
다양한 SQLi 취약점 테스트

```
┌──(root㉿kali)-[~]
└─# sqlmap -r request.txt --force-ssl --random-agent --batch --dbs

                {1.9.2#stable}
https://sqlmap.org

[!] legal disclaimer: Usage
obey all applicable local,
 this program

[*] starting @ 00:59:14 /20

[00:59:14] [INFO] parsing H
[00:59:14] [INFO] fetched r
ebKit/886; U; en) Presto/2.
Multipart-like data found i
[00:59:14] [INFO] testing c
[00:59:14] [CRITICAL] WAF/I
[00:59:14] [WARNING] the we
[00:59:14] [INFO] checking
[00:59:14] [INFO] testing i
[00:59:14] [INFO] target UR
[00:59:15] [INFO] testing i
[00:59:15] [WARNING] (custo
[00:59:15] [WARNING] heuris
[00:59:15] [INFO] testing f
[00:59:15] [INFO] testing '
[00:59:15] [INFO] testing '
```



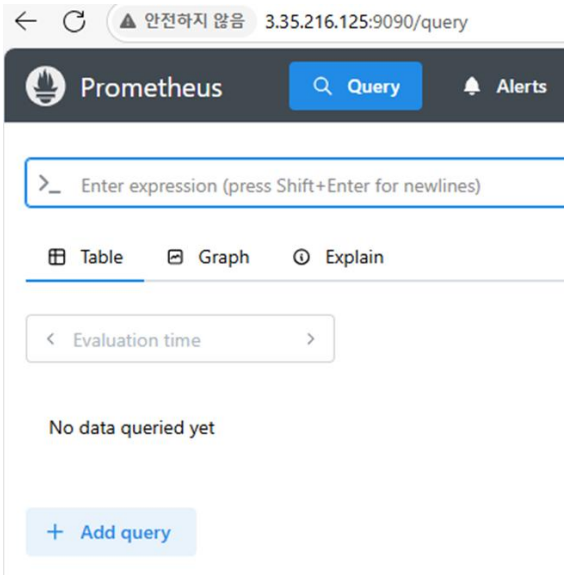
다양한 SQLi 취약점 테스트





Prometheus 설치

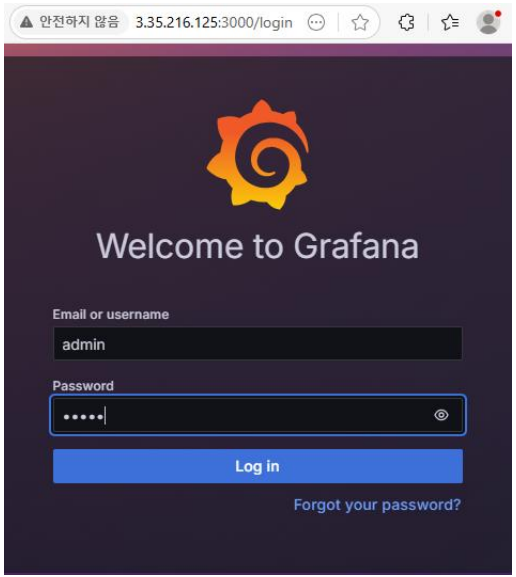

```
root@ip-10-0-100-85:~# ls
get-docker.sh  snap
root@ip-10-0-100-85:~#
root@ip-10-0-100-85:~# docker run -itd --name prometheus -p 9090:9090 prom/prometheus
Unable to find image 'prom/prometheus:latest' locally
latest: Pulling from prom/prometheus
9fa9226be034: Pull complete
1617e25568b2: Pull complete
097a69c6efe6: Pull complete
2ee6cb77bebd: Pull complete
a4e782810d03: Pull complete
76619c1908eb: Pull complete
2dfc70ad9941: Pull complete
fd1d3a5a5f79: Pull complete
5e4c02bc6754: Pull complete
208063e2dcbb: Pull complete
Digest: sha256:63805ebb8d2b3920190daf1cb14a60871b16fd38bed42b857a3182bc621f4996
Status: Downloaded newer image for prom/prometheus:latest
2125c407de61da6c59050c48d421ce1efcc46ef0ea611b798929752a4d1e1a43
root@ip-10-0-100-85:~#
root@ip-10-0-100-85:~#
```



netfort

Grafana 설치 및 Prometheus 연동

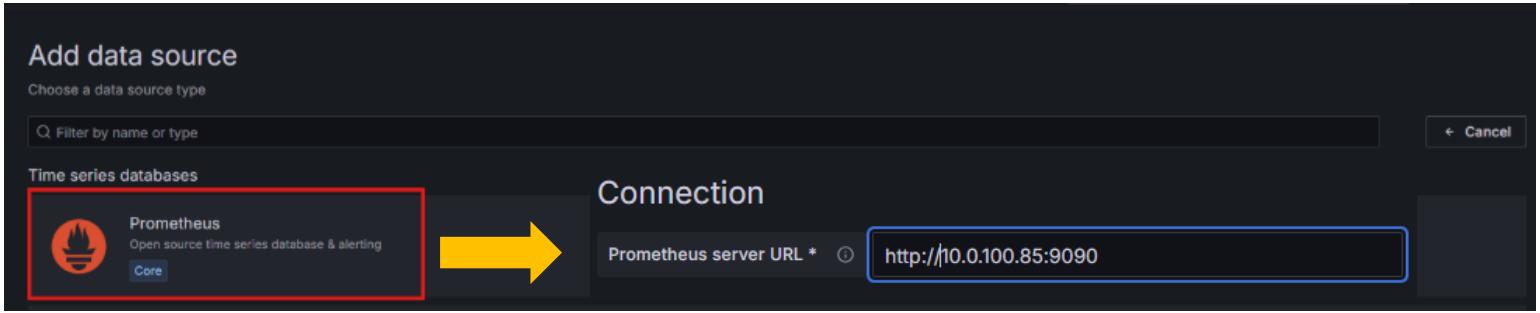
```
root@ip-10-0-100-85:~# docker ps
CONTAINER ID   IMAGE          COMMAND                  CREATED         STATUS         PORTS                                       NAMES
2125c407de61   prom/prometheus   "/bin/prometheus --c…"   4 minutes ago   Up 4 minutes   0.0.0.0:9090->9090/tcp, [::]:9090->9090/tcp   prometheus
root@ip-10-0-100-85:~#
root@ip-10-0-100-85:~# docker run -itd --name=grafana -p 3000:3000 grafana/grafana
Unable to find image 'grafana/grafana:latest' locally
latest: Pulling from grafana/grafana
f18232174bc9: Pull complete
9183b65e90ee: Pull complete
3f8d5c908dcc: Pull complete
30bb92ff0608: Pull complete
807a2e881ecd: Pull complete
4a4d0948b0bf: Pull complete
04f6155c873d: Pull complete
85dde7dceb0a: Pull complete
7009d5001b77: Pull complete
538deb30e80c: Pull complete
Digest: sha256:b5b59bfc7561634c2d7b136c4543d702ebcc94a3da477f21ff26f89ffd4214fa
Status: Downloaded newer image for grafana/grafana:latest
a0bf3cb52ac533829e3e411d4194aa082809116b7054efdd4bed9c1c8ba9832f
root@ip-10-0-100-85:~#
root@ip-10-0-100-85:~#
```

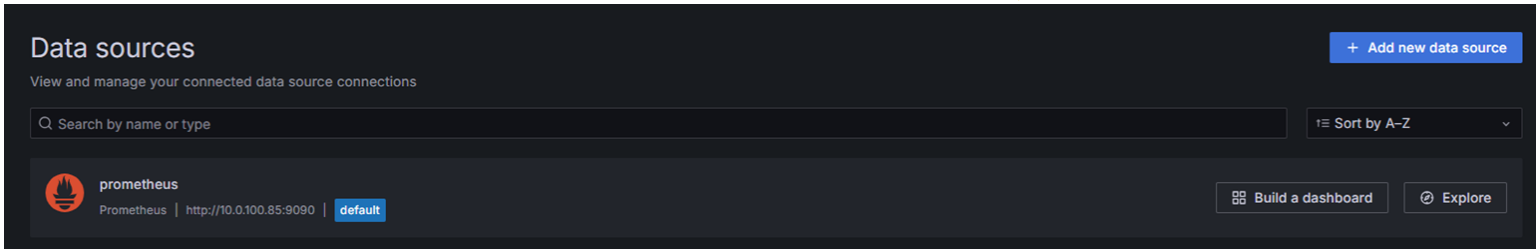


Grafana 컨테이너 구동 및 페이지 접속

netfort

Grafana 설치 및 Prometheus 연동





Prometheus 서버에 접속하여 수집된 모든 메트릭 데이터를 읽어오고 사용자는 데이터를 활용,
다양한 모니터링 대시보드를 만들 수 있음

netfort

Node Exporter 설치

```
[root@ip-10-0-110-244 ~]#
[root@ip-10-0-110-244 ~]# docker run -itd --name node-exporter --net="host" --pid="host" -v "/:/host:ro,rslave" quay.io/prometheus/node-exporter:latest --path.rootfs=/host
48d981368f2668eb6ba03760fe904a31dc4e05695ed9c3aaaad28b209e2ab281
[root@ip-10-0-110-244 ~]#
[root@ip-10-0-110-244 ~]# docker ps
CONTAINER ID   IMAGE                                  COMMAND                  CREATED         STATUS         PORTS     NAMES
48d981368f26   quay.io/prometheus/node-exporter:latest   "/bin/node_exporter …"   5 seconds ago   Up 4 seconds             node-exporter
[root@ip-10-0-110-244 ~]#
[root@ip-10-0-110-244 ~]#
```

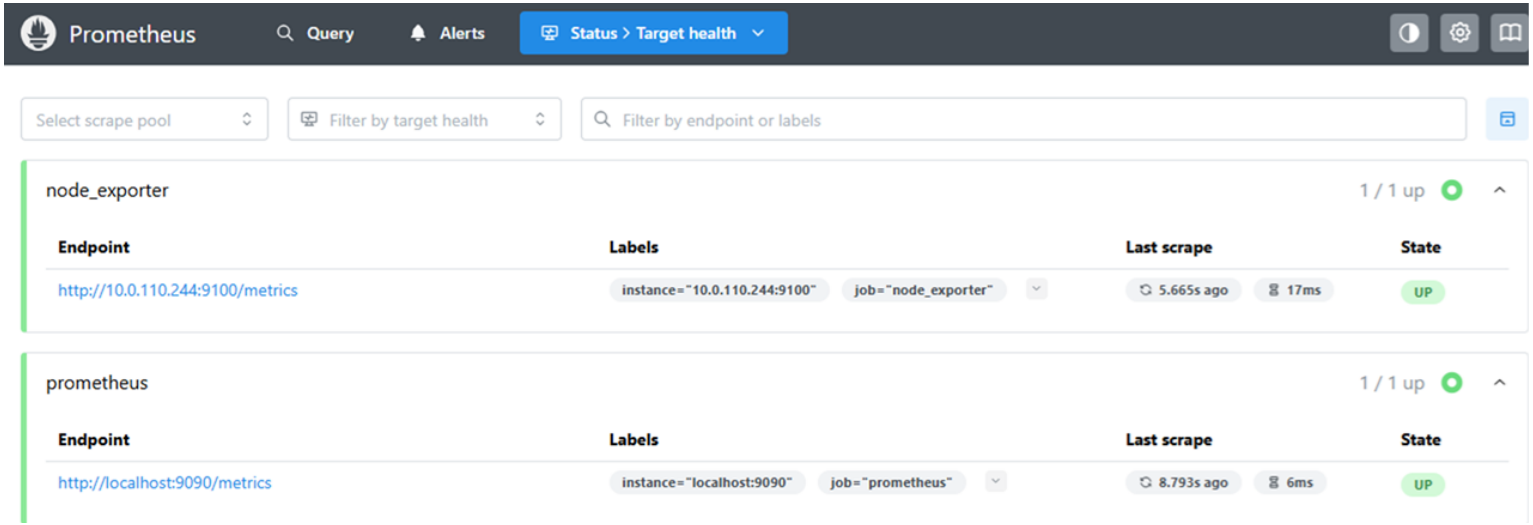
- Node-exporter 컨테이너 구동.
  > 네트워크 모드를 호스트로 사용.

```
root@ip-10-0-100-85:~# nano prometheus.yml
  GNU nano 7.2                                                  prometheus.yml *
global:
  scrape_interval: 15s # 기본 수집 주기를 15초로 설정.
  evaluation_interval: 15s # 규칙 평가 주기를 15초로 설정.

scrape_configs:
  - job_name: 'prometheus'
    static_configs:
      - targets: ['localhost:9090']

  # Node Exporter를 모니터링하기 위한 job
  - job_name: 'node_exporter'
    static_configs:
      - targets: ['10.0.110.244:9100']
```

- Node Exporter를 모니터링하여 해당 서버의 시스템 정보를 수집
- 15초마다 설정된 모든 대상에서 데이터를 수집 및 알림 규칙 평가

netfort

Node Exporter 설치



Prometheus에서 node_exporter 메트릭 서버 수집 확인

netfort

Alert Manager 설치

```
root@ip-10-0-100-85:~# nano alert-manager.yml
 GNU nano 7.2                                  alert-manager.yml *
global:
  resolve_timeout: 5m

route:
  receiver: 'telegram-notifier'
  group_by: ['alertname', 'instance']
  group_wait: 30s
  group_interval: 5m
  repeat_interval: 1h

receivers:
  - name: 'telegram-notifier'
    telegram_configs:
      - bot_token: '7741206539:AAEv8szu-CrjCQisislt1tK8voNPiTTfLzM'
        chat_id: 8039038339
        send_resolved: true
        parse_mode: 'HTML'
```

```
root@ip-10-0-100-85:~# docker run -d \
  --name alertmanager \
  -p 9093:9093 \
  -v $(pwd)/alert-manager.yml:/etc/alertmanager/alertmanager.yml \
  --restart unless-stopped \
  prom/alertmanager:latest \
  --config.file=/etc/alertmanager/alertmanager.yml
Unable to find image 'prom/alertmanager:latest' locally
latest: Pulling from prom/alertmanager
9fa9226be034: Already exists
1617e25568b2: Already exists
545c14a5a415: Pull complete
6fcbfeb5877c: Pull complete
a9c7f41169bf: Pull complete
5759234535c5: Pull complete
4f4fb700ef54: Pull complete
Digest: sha256:27c475db5fb156cab31d5c18a4251ac7ed567746a2483ff264516437a39b15ba
Status: Downloaded newer image for prom/alertmanager:latest
0bdf29f2fb91e5b83a124eb9873c7003e21f7f0af7573733a42d9d417441a9b9
root@ip-10-0-100-85:~#
root@ip-10-0-100-85:~#
```

alert-manager.yml 파일 작성

alertmanager 컨테이너 구동

netfort

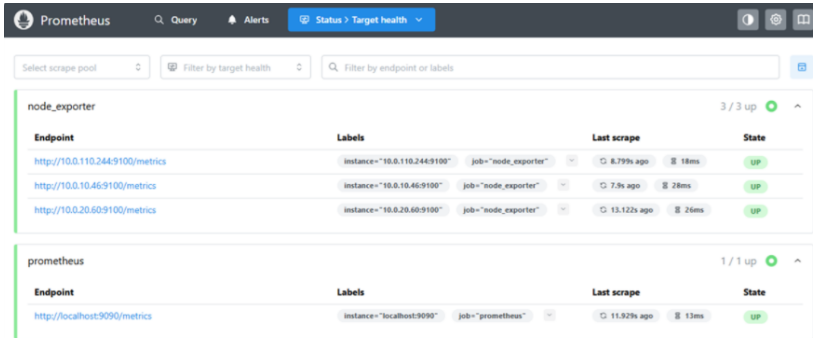
경고 발생 시 자동 알림 전송 구성

```
root@ip-10-0-100-85:~# nano alert-rules.yml
 GNU nano 7.2                                  alert-rules.yml
groups:
  - name: cpu_alert_rules
    rules:
      - alert: HighCpuUsage
        # 1분 동안 CPU 사용량이 70%를 초과하면 알림을 보냅니다.
        expr: 100 * (1 - avg by(instance) (rate(node_cpu_seconds_total{mode="idle"}[5m]))) > 70
        # 이 조건이 1분 동안 지속될 경우에만 알림을 트리거.
        for: 5m
        labels:
          severity: critical
        annotations:
          summary: "인스턴스 {{ $labels.instance }} CPU 사용량 높음"
          description: "호스트 {{ $labels.instance }}의 CPU 사용량이 5분 동안 70%를 초과했습니다. 현재 값: {{ $value | printf \"%.2f\" }}%"
```

alert-rules.yml 파일 작성

```
root@ip-10-0-100-85:~# nano prometheus.yml
global:
  scrape_interval: 15s # 기본 수집 주기를 15초로 설정.
  evaluation_interval: 15s # 규칙 평가 주기를 15초로 설정.

rule_files:
  - 'alert-rules.yml'

alerting:
  alertmanagers:
    - static_configs:
        - targets: ['10.0.100.85:9093']

scrape_configs:
  - job_name: 'prometheus'
    static_configs:
      - targets: ['localhost:9090']

  # Node Exporter를 모니터링하기 위한 job
  - job_name: 'node_exporter'
    static_configs:
      - targets: ['10.0.110.244:9100','10.0.10.46:9100','10.0.20.60:9100']
```

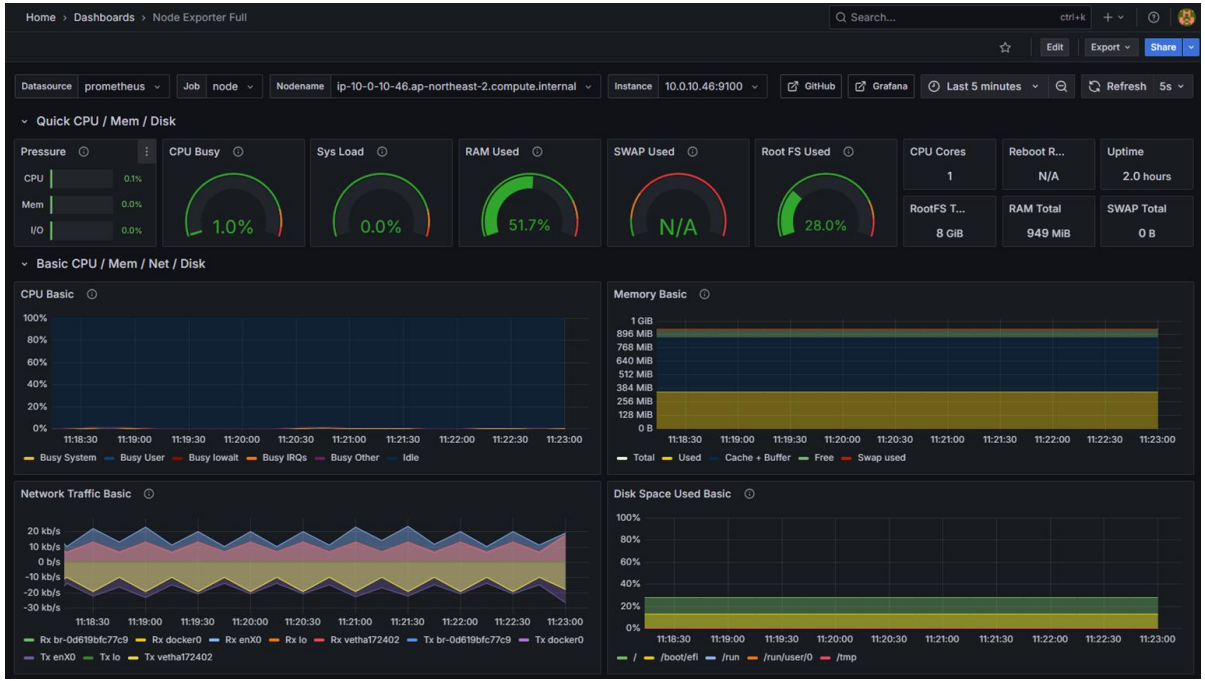
prometheus.yml 파일 작성



Prometheus에서 node_exporter, backendserver1, backendserver2의 메트릭
서버 수집

netfort

grafana 그래프 생성



grafana에서 backendserver1의 그래프 확인

netfort

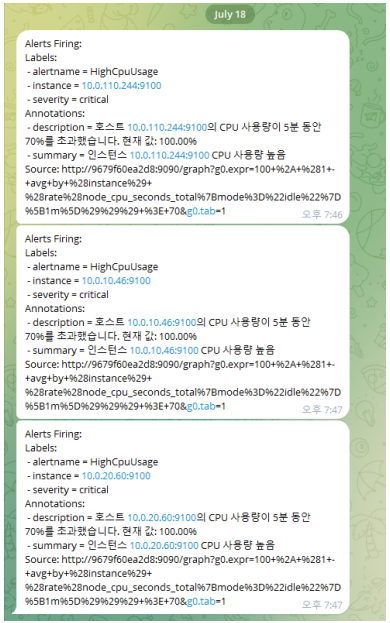
경고 발생 시 자동 알림 전송 구성

```
[root@ip-10-0-110-244 ~]# stress -c 1
stress: info: [30954] dispatching hogs: 1 cpu, 0 io, 0 vm, 0 hdd
```

```
[root@ip-10-0-10-46 ~]# stress -c 1
stress: info: [42533] dispatching hogs: 1 cpu, 0 io, 0 vm, 0 hdd
```

```
[root@ip-10-0-20-60 ~]# stress -c 1
stress: info: [40906] dispatching hogs: 1 cpu, 0 io, 0 vm, 0 hdd
```

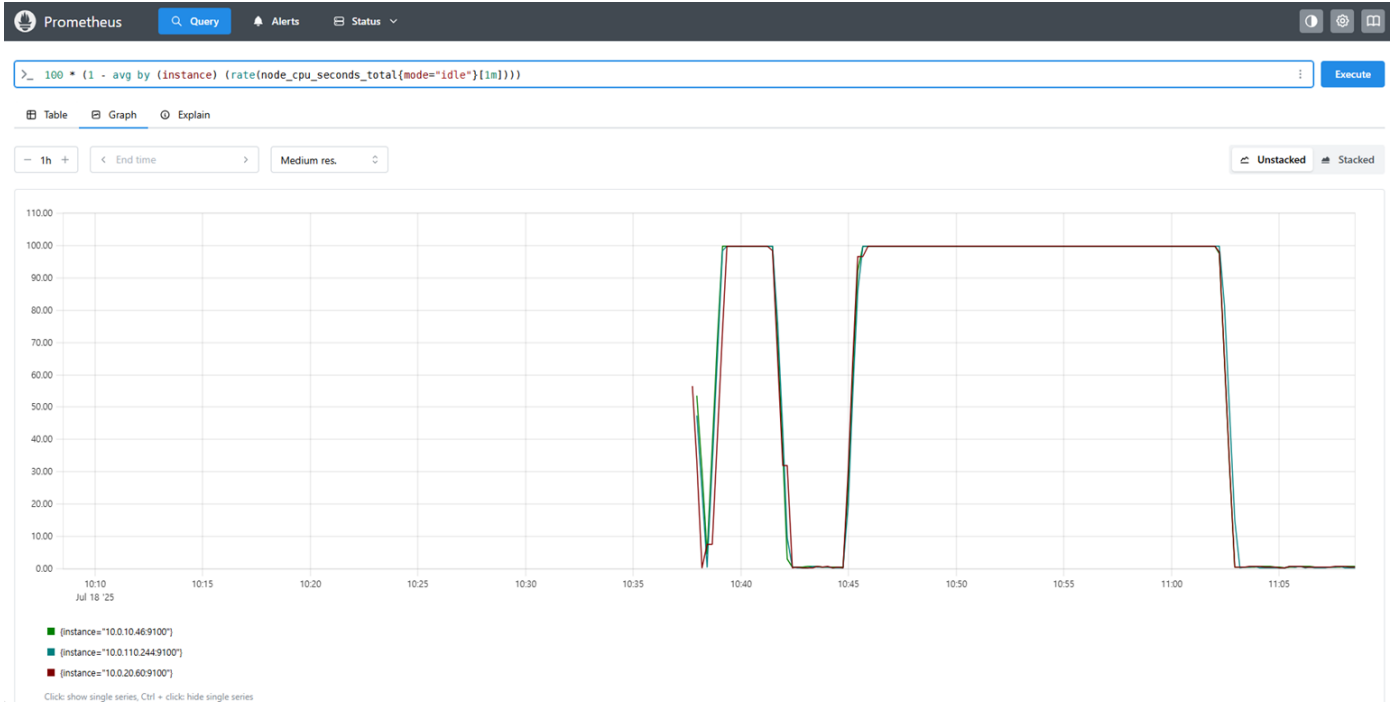
NodeExport, backendserver1, backendserver2 에게 CPU 과부하 적용



telegram 에서 메시지 전송 확인

netfort

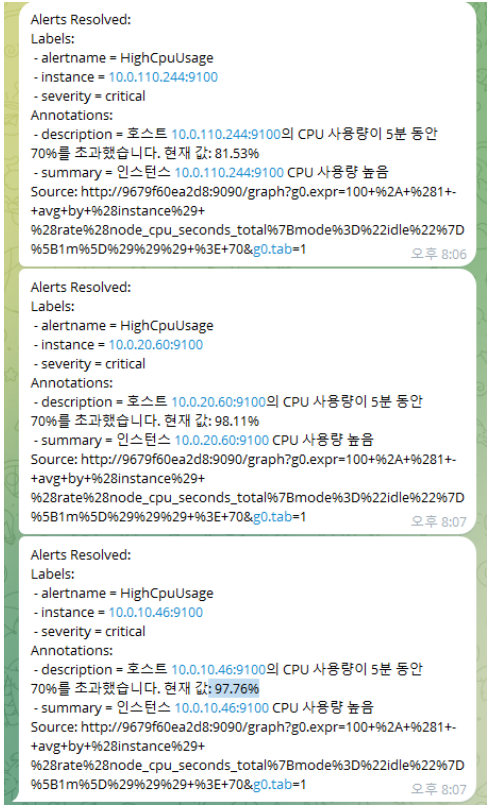
경고 발생 시 자동 알림 전송 구성



Prometheus에서 그래프 확인

netfort

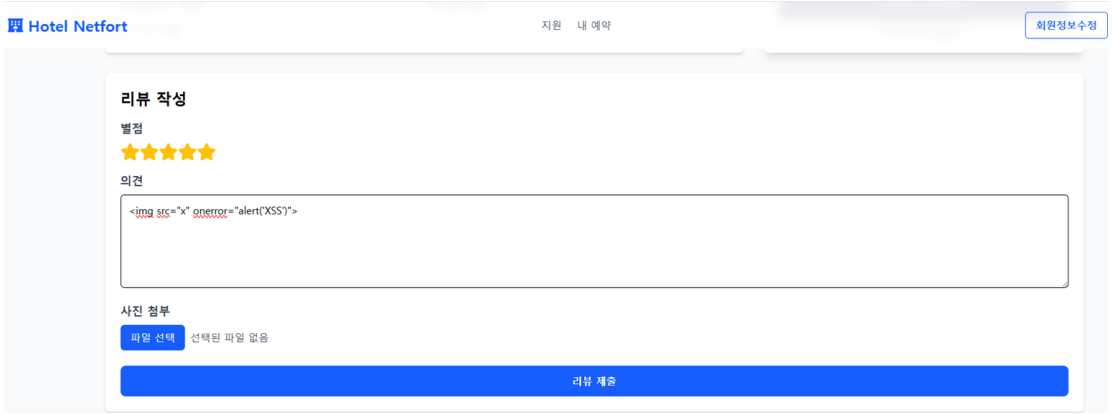
경고 발생 시 자동 알림 전송 구성



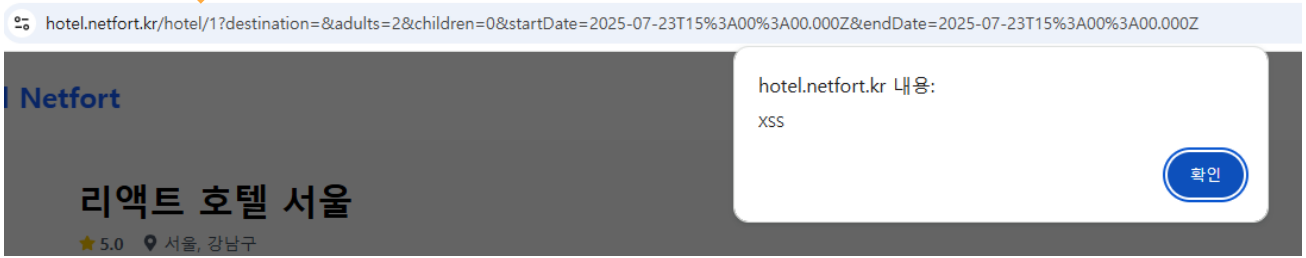
NodeExporter, backendserver1, backendserver2에 적용된 CPU 과부하를 종료시킨 후, telegram에서 해결 문자 전송 확인

netfort

XSS 공격 검증

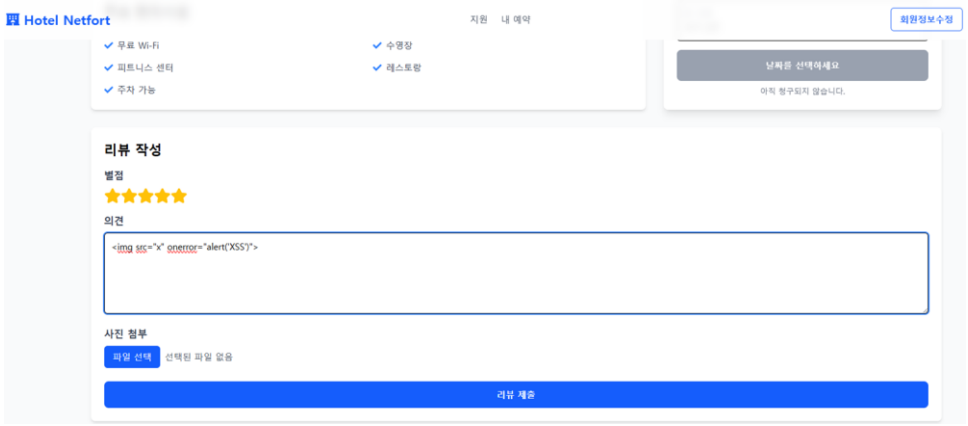


리뷰창에서 공격 시도 및 공격 성공.

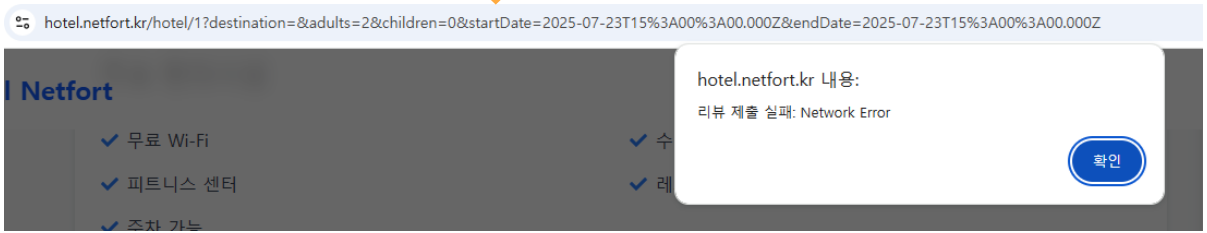


netfort

XSS 공격 검증



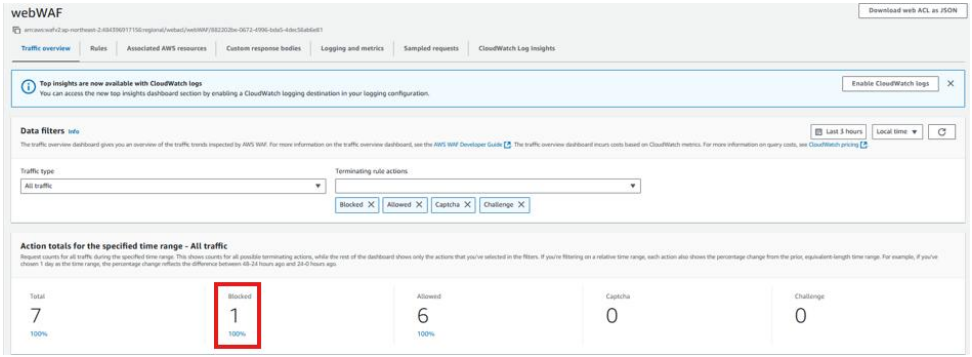
리뷰창에서 다시 한 번 공격 시도

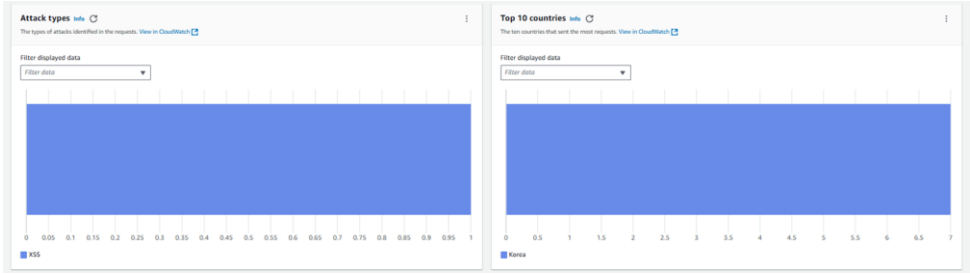


공격 실패

netfort

xss 공격 검증



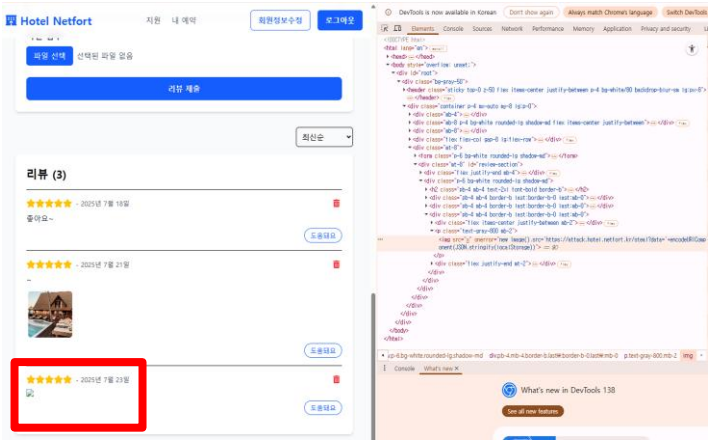


- WAF에서 확인한 결과, xss 공격 시도에 대
  해 차단 확인.
  - 방금 전 공격 시도에 실패한 이유 : WAF
    에서 xss에 대한 공격을 탐지하고, 차단.

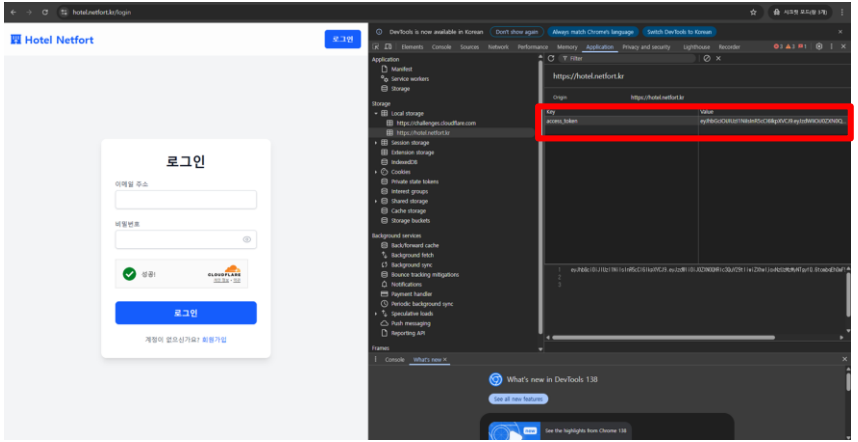
- xss 공격 유형에 대해 WAF에서 탐지한 부분을 그래프로도 확인 가능.

netfort

XSS 공격 검증 - token 취득 및 로그인 시도



리뷰창으로 token을 취득하기 위해 공격 시도 및 공격 성공.



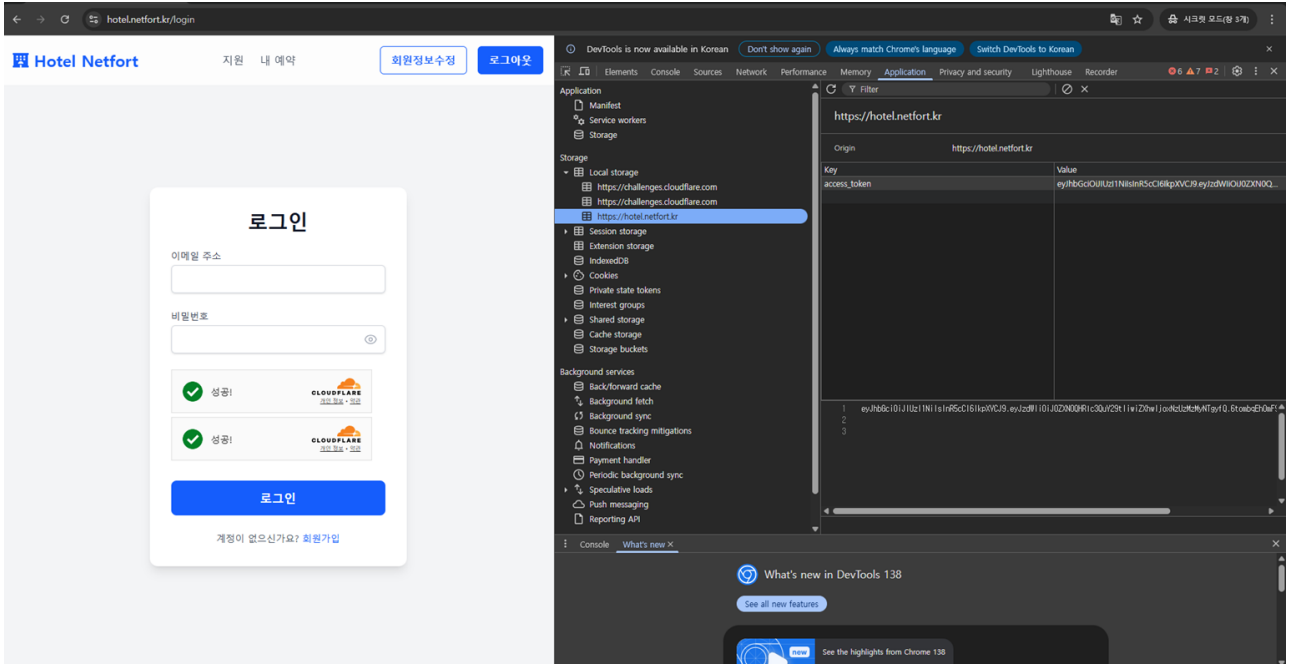
개발자 창에서 취득한 토큰 값으로 변경하여 로그인 시도.

```
10.0.1.91 - attack.hotel.netfort.kr [23/Jul/2025:05:44:27 +0000] "GET /steal?data=%7B%22access_token%22%3A%22eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiJ0ZXN0QHRlc3QuY29tIiwiZXhwIjoxNzUzMzMyNTgyfQ.6tombqEhOmF9Ttjh-CPZyv5dSnXuZVR_EajXZRkdhmw%22%7D HTTP/1.1" status=404 uri=/steal?data=%7B%22access_token%22%3A%22eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiJ0ZXN0QHRlc3QuY29tIiwiZXhwIjoxNzUzMzMyNTgyfQ.6tombqEhOmF9Ttjh-CPZyv5dSnXuZVR_EajXZRkdhmw%22%7D args=- ua="Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36"
```

Token 값 취득

netfort

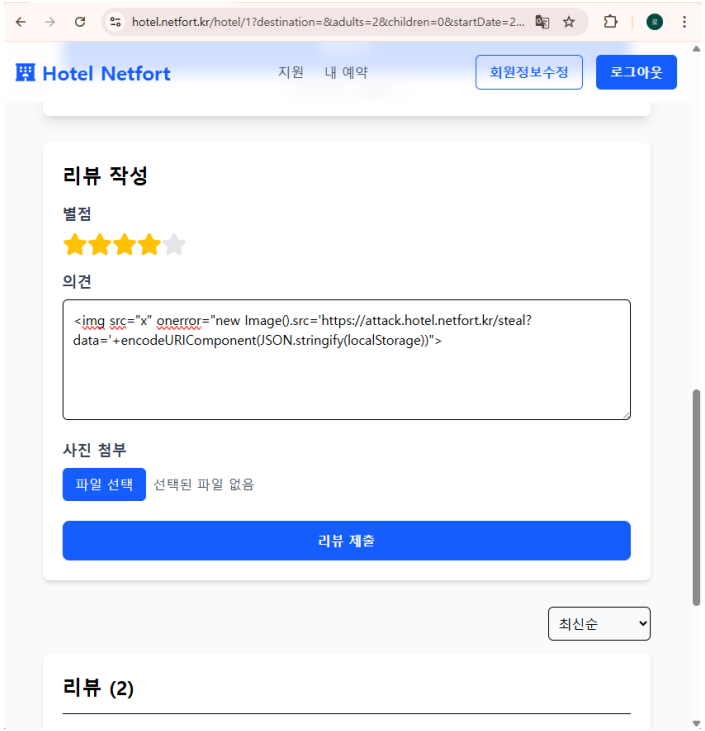
XSS 공격 검증 - token 취득 및 로그인 시도



취득한 token으로 로그인 성공.

netfort

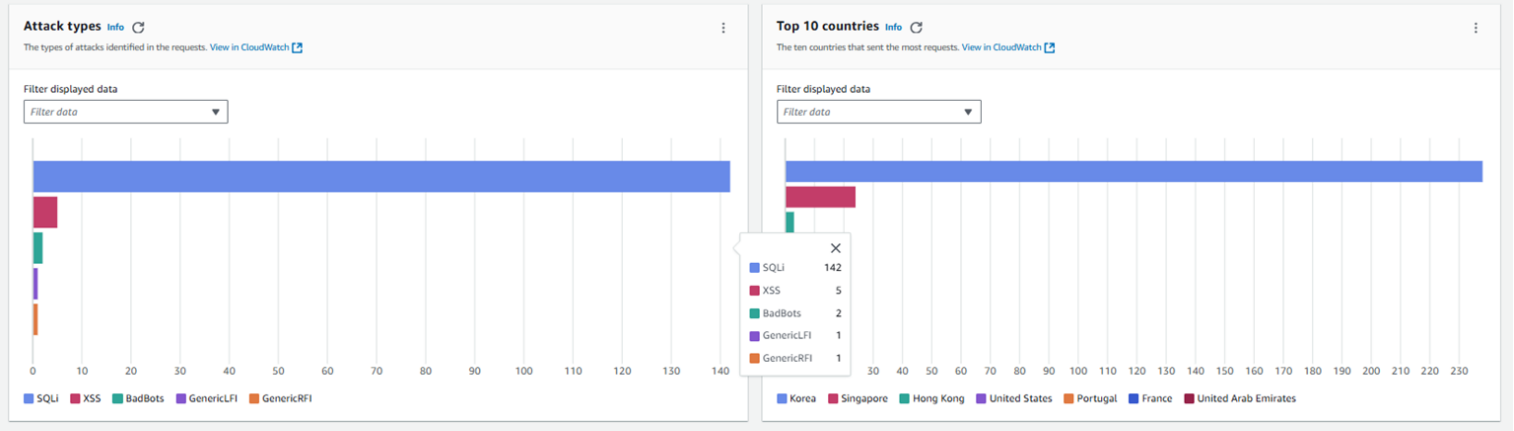
XSS 공격 - token 취득 및 로그인 시도



WAF 를 실행한 상태에서 같은 스크립트로 다시 한 번 공격 시도 및 공격 실패 확인.

netfort

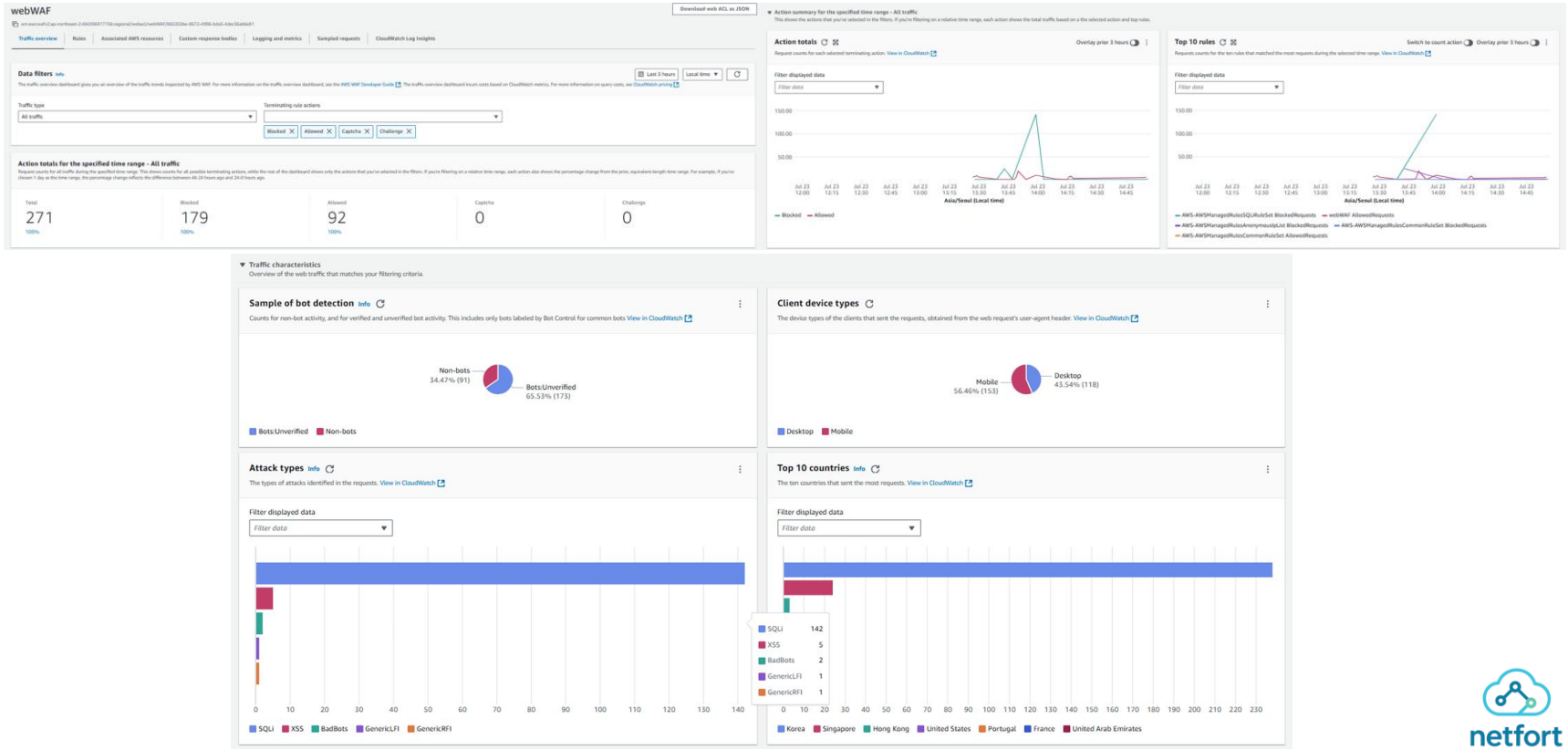
XSS 공격 - token 취득 및 로그인 시도



WAF 에서 XSS 공격 유형에 대해 차단한 부분을 그래프로 확인 가능.

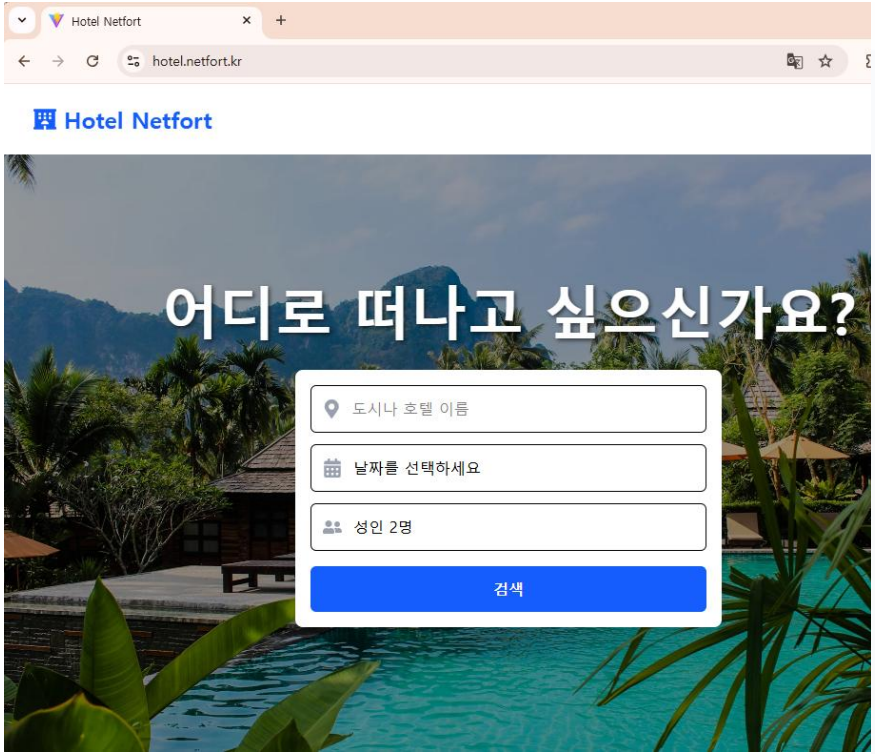
netfort

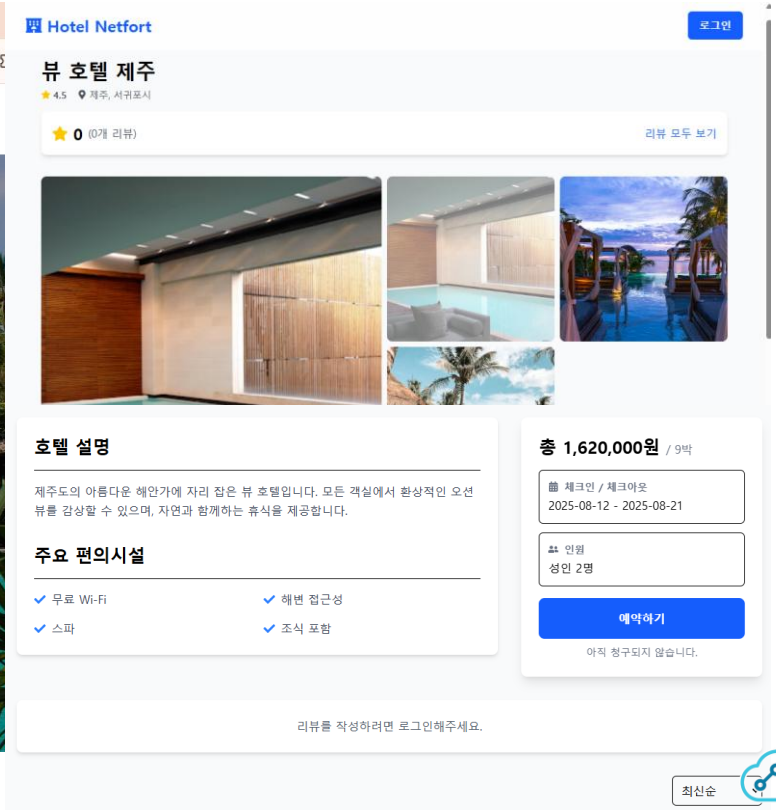
모든 공격 확인



netfort

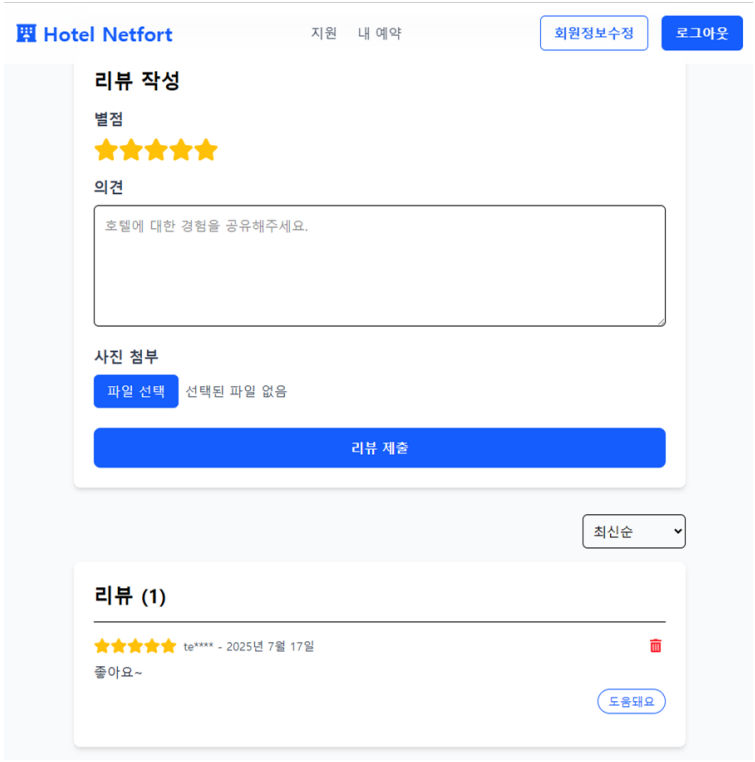
결과

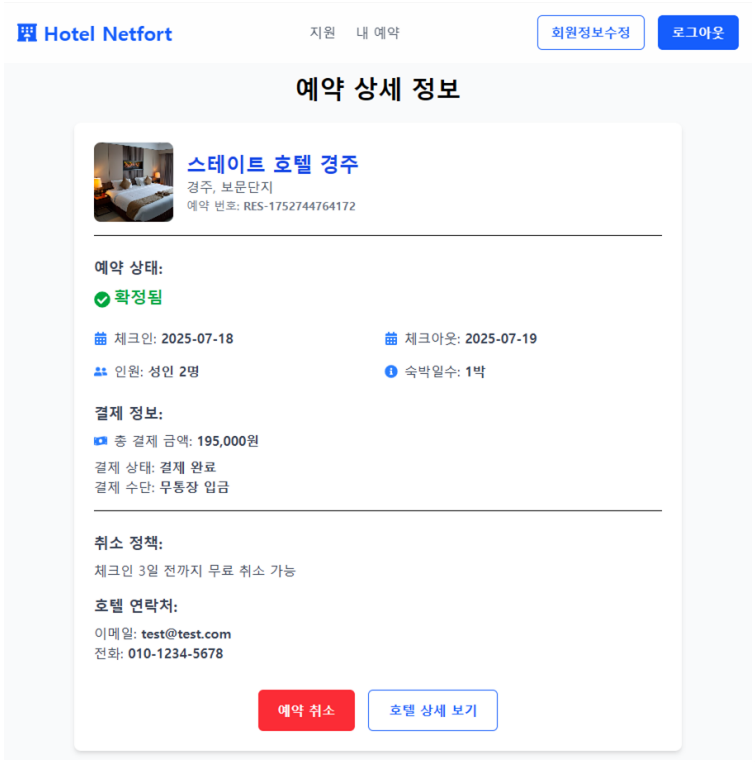

Hotel Netfort
hotel.netfort.kr
Hotel Netfort
어디로 떠나고 싶으신가요?
도시나 호텔 이름
날짜를 선택하세요
성인 2명
검색


Hotel Netfort
로그인
뷰 호텔 제주
4.5
제주, 서귀포시
0 (0개 리뷰)
리뷰 모두 보기
호텔 설명
제주도의 아름다운 해안가에 자리 잡은 뷰 호텔입니다. 모든 객실에서 환상적인 오션 뷰를 감상할 수 있으며, 자연과 함께하는 휴식을 제공합니다.
주요 편의시설
무료 Wi-Fi
해변 접근성
스파
조식 포함
총 1,620,000원 / 9박
체크인 / 체크아웃
2025-08-12 - 2025-08-21
인원
성인 2명
예약하기
아직 청구되지 않습니다.
리뷰를 작성하려면 로그인해주세요.
최신순

netfort

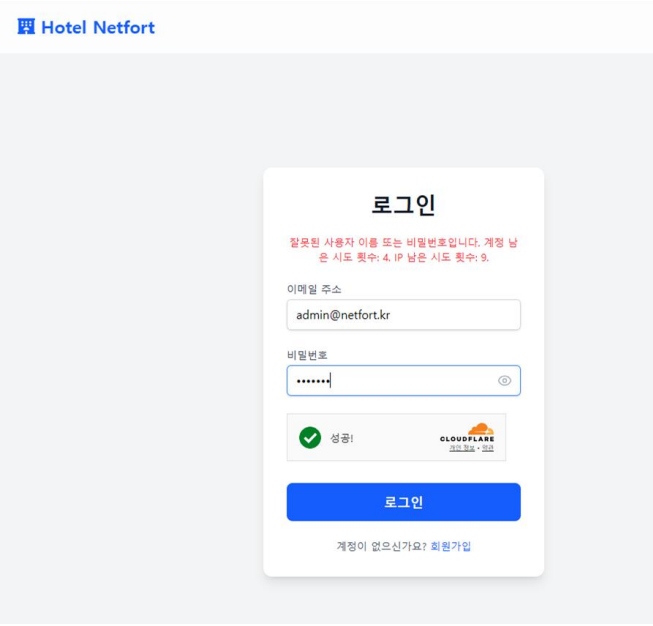
결과

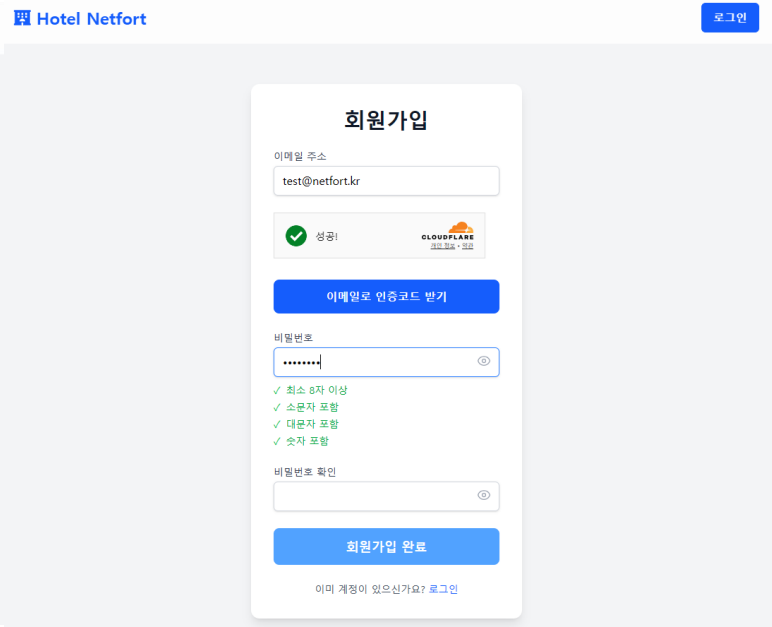

Hotel Netfort
지원
내 예약
회원정보수정
로그아웃
리뷰 작성
별점
의견
호텔에 대한 경험을 공유해주세요.
사진 첨부
파일 선택
선택된 파일 없음
리뷰 제출
최신순
리뷰 (1)
te**** - 2025년 7월 17일
좋아요~
도움돼요


Hotel Netfort
지원
내 예약
회원정보수정
로그아웃
예약 상세 정보
스테이트 호텔 경주
경주, 보문단지
예약 번호: RES-1752744764172
예약 상태:
확정됨
체크인: 2025-07-18
체크아웃: 2025-07-19
인원: 성인 2명
숙박일수: 1박
결제 정보:
총 결제 금액: 195,000원
결제 상태: 결제 완료
결제 수단: 무통장 입금
취소 정책:
체크인 3일 전까지 무료 취소 가능
호텔 연락처:
이메일: test@test.com
전화: 010-1234-5678
예약 취소
호텔 상세 보기

netfort

결과


Hotel Netfort
로그인
잘못된 사용자 이름 또는 비밀번호입니다. 계정 남은 시도 횟수: 4, IP 남은 시도 횟수: 9.
이메일 주소
admin@netfort.kr
비밀번호
성공!
CLOUDFLARE
로그인
계정이 없으신가요? 회원가입


Hotel Netfort
로그인
회원가입
이메일 주소
test@netfort.kr
성공!
CLOUDFLARE
이메일로 인증코드 받기
비밀번호
✓ 최소 8자 이상
✓ 소문자 포함
✓ 대문자 포함
✓ 숫자 포함
비밀번호 확인
회원가입 완료
이미 계정이 있으신가요? 로그인

netfort

결과

Hotel Netfort 회원가입 이메일 인증 받은편지함 ×

noreply@netfort.kr 수신거부
나에게

안녕하세요, 사용자님!
Hotel Netfort에 가입해 주셔서 감사합니다.
다음 인증 코드를 입력하여 회원가입을 완료해주세요:

인증 코드: 633815

이 코드는 5분간 유효합니다.

Hotel Netfort 예약이 완료되었습니다! 받은편지함 ×

noreply@netfort.kr 수신거부
나에게

안녕하세요, mail.com님!
Hotel Netfort 예약이 성공적으로 완료되었습니다.

호텔: 리액트 호텔 서울
체크인: 2025-08-12 00:00:00
체크아웃: 2025-08-13 00:00:00
총 결제 금액: 250000원
예약 번호: RES-1753148441156

즐거운 여행 되세요!

netfort