

# EKS 기반 병원 애플리케이션 개발 환경 구축 프로젝트

---

General Hospital의 IT 인프라 현대화 및 효율성 향상을 위한 전략적 접근

---

# 목차

## 프로젝트 개요

- 클라우드 전환 및 인프라 확장
- 운영 자동화 및 고가용성 확보
- 장애 대응 시스템 구축
- 비용 절감 및 유지보수 효율화

## 프로젝트 배경

- 수행업체 및 엔지니어 소개
- 발주처 소개
- 기존 아키텍처 분석 및 문제점
- 수행업체의 솔루션
- 개선된 아키텍처 구성

## 클라우드 구축 계획

- 단계별 구축 계획
- EKS 도입 배경
- DB 이전 배경
- AWS RDS 선택 이유
- 모니터링 시스템

## 단계별 구축 과정

- 네트워크 및 인프라 설정
- EKS & DB 및 CI/CD 설정
- 모니터링 및 보안 강화

## 향후 계획 및 결론

- 최종 토폴로지
- 기대효과
- 서비스 분리 및 MSA 전환
- 결론

# 프로젝트 개요



## 클라우드 전환 및 인프라 확장

- 온프레미스 → 클라우드 전환
- 클라우드 기반 인프라 확장성 확보

## 운영 자동화 및 고가용성 확보

- 자동화된 배포 및 관리
- 고가용성 시스템 설계

## 장애 대응 시스템 구축

- 실시간 모니터링 및 알림
- 자동화된 장애 복구 프로세스

## 비용 절감 및 유지보수 효율화

- 비용 최적화
- 자동화된 리소스 관리 및 모니터링

# Muhan Cloud 소개



## 보유 기술

- Ubuntu / MySQL / PHP
- AWS (EC2, RDS, S3, CloudWatch 등)
- Docker & Kubernetes
- Git Hub



## 전문 분야

- 클라우드 인프라 설계 및 최적화
- 실시간 모니터링 및 운영 효율화
- 고가용성 시스템 구축 및 장애 복구 설계
- 컨테이너 기반 오케스트레이션 및 자동화 운영

# Muhan Cloud 엔지니어 소개



한동희 엔지니어

- 인프라 구축 기술 보유
- Linux (Cent OS, Ubuntu)
- PHP, Python
- MySQL
- AWS
- Docker & Kubernetes



최우재 엔지니어

- 인프라 구축 기술 보유
- Linux (Cent OS, Ubuntu)
- PHP, Python
- MySQL
- AWS
- Docker & Kubernetes



김동욱 엔지니어

- 인프라 구축 기술 보유
- Linux (Cent OS, Ubuntu)
- PHP, Python
- MySQL
- AWS
- Docker & Kubernetes



# 기존 아키텍처 분석 및 문제점

01

온프레미스 환경에서 서버 운영

- 서버 관리 및 유지보수에 부담
- 단일 서버 구조로 고가용성 부족

02

고객 증가로 인한 서버 용량 확장 부담

- 서버 용량 확장이 어려움
- 급격한 트래픽 증가에 대한 대응 한계

03

서버 관리 인력 부족 및 운영 비용 증가

- 관리 인력 부족으로 효율적 운영 어려움
- 높은 인건비 및 운영비용 발생

# 기존 아키텍처 분석 및 문제점

04

높은 트래픽 대응의 어려움

- 트래픽 급증 시 서버 과부하 발생
- 서비스 성능 저하

05

장애 발생 시 신속한 복구 어려움

- 장애 복구에 긴 시간 소요
- 서비스 가용성 저하

# Muhan Cloud의 솔루션

## 비용 효율화 및 모니터링

- CloudWatch 기반 실시간 모니터링 및 알림
- 자원 최적화로 비용 절감

## 고가용성 및 장애 대응력 향상

- EKS 자동 복구 기능으로 서비스 신뢰성 향상
- RDS로 안정적 데이터베이스 운영

### 확장성 및 고가용성 강화 시스템

## 스케일링 및 트래픽 최적화

- 로드 밸런서로 안정적 트래픽 분산
- Auto Scaling으로 유연한 수요 대응

## 클라우드 전환 및 유연성 확보

- EKS 기반 컨테이너 환경으로 효율적 배포 및 운영
- 관리형 Kubernetes로 서버 관리 자동화 및 리소스 최적화



# 개선된 아키텍처 구성

## EKS 기반 컨테이너 관리

- Kubernetes로 애플리케이션 자동 배포 및 확장
- 관리형 서비스로 서버 운영 부담 감소

## CI/CD 통합 자동화

- IAM 기반 보안 설정으로 안전한 운영 환경
- CodeBuild로 배포 자동화 및 빌드 관리

## RDS 활용 및 데이터 안정성 강화

- 자동 백업 및 복구 기능으로 안정성 확보
- Read Replica로 읽기 성능 향상 및 부하 분산

## 모니터링 및 비용 최적화

- CloudWatch 기반 실시간 모니터링
- Auto Scaling으로 리소스 최적화 및 비용 절감

# 단계별 구축 계획

## 1. 요구사항 분석 & 아키텍처 설계

온프레미스 분석, 클라우드 환경 설계

## 3. 인프라 환경 구축

VPC, Subnet, NAT, IAM, 보안 설정

## 5. CI/CD 구성

Git 연동, Docker 빌드/배포 자동화

## 2. 컨테이너 마이그레이션

Docker 이미지화, ECR 업로드, 경량화

## 4. EKS & DB 구성

EKS 클러스터, NodeGroup, RDS, 스토리지

## 6. 모니터링 및 보안 강화

CloudWatch, SNS, WAF, 로깅 시스템

# EKS 도입 배경

컨테이너 운영의 유연성

Kubernetes로 다양한 워크로드 지원, 확장성 강화

벤더 종속 최소화

오픈소스 Kubernetes로 툴 호환성 제공



강화된 보안 관리

IAM, VPC, Security Group으로 세밀한 보안 설정

## Amazon EKS

고가용성 및 자동화

Auto Scaling, 장애 복구로 안정적 운영 보장

배포 자동화 및 CI/CD

CodeBuild로 효율적 빌드 및 배포

# DB 이전 배경

## 초기 투자 및 운영 비용 절감

- 물리 장비 구매 없이 클라우드 기반으로 효율적 운영
- 관리형 서비스로 DBA 및 유지보수 부담 감소

## 고가용성 및 데이터 보호 강화

- 자동 백업 및 시점 복구(PITR)로 데이터 안정성 확보
- 장애 발생 시 빠른 복구로 서비스 연속성 유지



## 확장성과 유연한 운영

- 자동 스토리지 확장으로 운영 간소화
- 서버 업그레이드 없이 인스턴스 크기 조정으로 유연한 확장

## 운영 자동화 및 모니터링

- 자동 패치 및 장애 복구 기능 제공
- CloudWatch 연계로 실시간 성능 모니터링 가능

# AWS RDS 선택 이유

## 관계형 데이터베이스 요구사항 충족

다양한 DB 엔진 지원

- MySQL, PostgreSQL, Oracle 등

관리형 서비스 제공

- 자동 패치 및 백업
- 모니터링 및 알림

고가용성 및 확장성

- Multi-AZ 배포
- Read Replica 지원

보안 및 규정 준수

- 암호화 및 접근 제어
- 규제 준수 지원





# 모니터링 시스템 구축



## AWS 모니터링 서비스 활용

### AWS CloudWatch

- 리소스 및 애플리케이션 모니터링
- 로그 수집 및 분석
- 사용자 정의 대시보드 생성

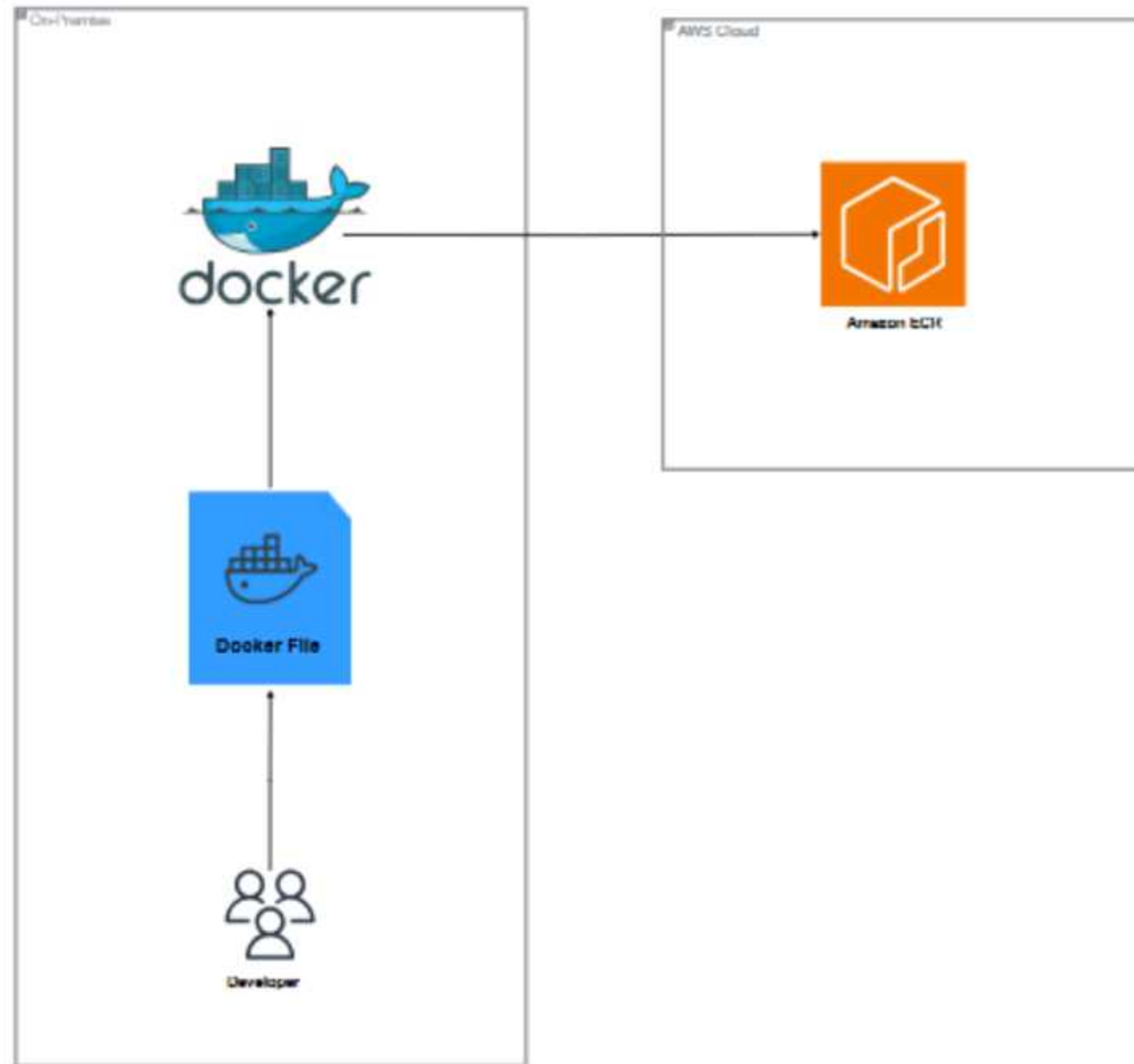
### AWS SNS (Simple Notification Service)

- 실시간 알림 시스템
- 다양한 알림 채널 지원 (이메일, SMS 등)
- 임계값 기반 자동 알림



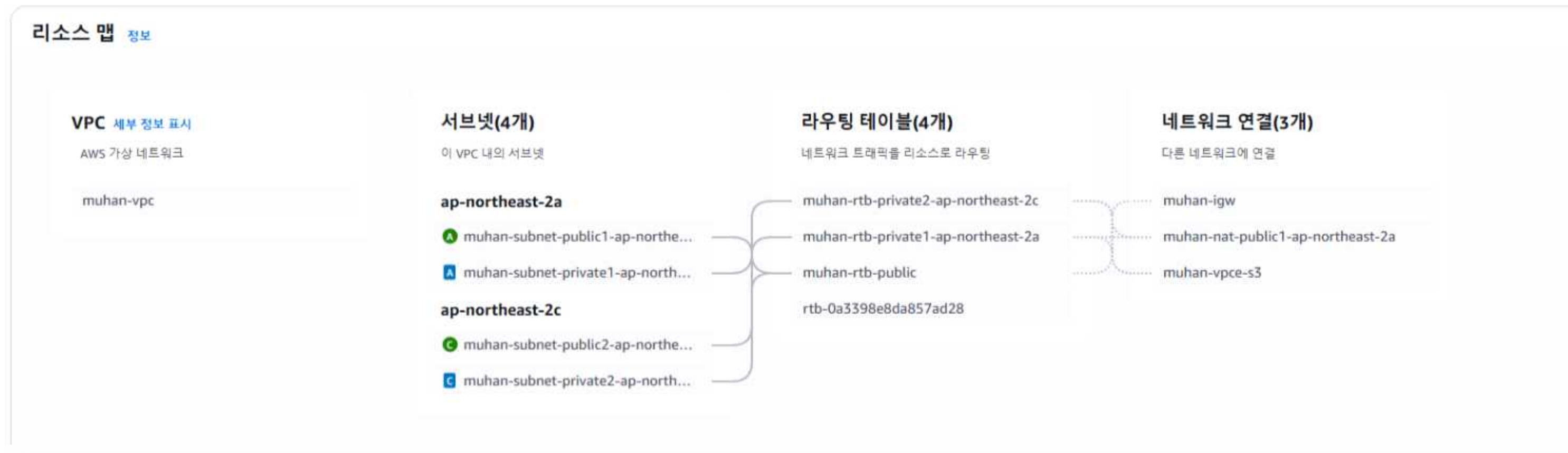
# 네트워크 및 인프라 설정

## 마이그레이션 아키텍처 - Application



# 네트워크 및 인프라 설정

## VPC



# 네트워크 및 인프라 설정

## 서브넷 CIDR 설정

### ap-northeast-2a 퍼블릭 서브넷 CIDR 블록

10.0.0.0/24

256 IPs

### ap-northeast-2c 퍼블릭 서브넷 CIDR 블록

10.0.1.0/24

256 IPs

### ap-northeast-2a 프라이빗 서브넷 CIDR 블록

10.0.2.0/24

256 IPs

### ap-northeast-2c 프라이빗 서브넷 CIDR 블록

10.0.3.0/24

256 IPs

# EKS & DB 및 CI/CD

## EKS Cluster

muhanEKS

클러스터 삭제

대시보드 보기

▼ 클러스터 정보

정보

상태

🟢 활성

Kubernetes 버전

정보

1.32

지원 기간

📅 2026년 3월 21일까지 표준 지원

공급자

EKS

클러스터 상태 문제

🟢 0

업그레이드 인사이트

🟢 0

노드 상태 문제

🟢 0

개요

리소스

컴퓨팅

네트워킹

추가 기능

액세스

관찰성

업데이트 기록

태그

세부 정보

API 서버 엔드포인트

🔗

https://1D003C543885CEFE2648E795461E1A6A.gr7.ap-northeast-2.eks.amazonaws.com

인증 기관

🔗

LS0tLS1CRUdJTiBDRVJUSUZJQ0FUR50tLS0tCk1JSURCVENDQWUyZ0F3SUJBZ0UxVnRDSFUycXd3RFFZSktvWklodmNOQVFFTEJRQXdGVEVUTUJFR0ExVUUKQXhNS2EzVmlaWEp1WlhSbGN6QWV

OpenID Connect 공급자 URL

🔗

https://oidc.eks.ap-northeast-2.amazonaws.com/id/1D003C543885CEFE2648E795461E1A6A

클러스터 IAM 역할 ARN

🔗

arn:aws:iam::183631310061:role/MuhanEKSCluster

[IAM에서 보기](#)

생성됨

🕒

18분 전

클러스터 ARN

🔗

arn:aws:eks:ap-northeast-2:183631310061:cluster/muhanEKS

플랫폼 버전

정보

eks.4

EKS 자율 모드

정보

EKS는 컴퓨팅, 스토리지, 네트워킹에 대한 일상적인 클러스터 작업을 자동화하여 애플리케이션 컴퓨팅 요구 사항을 충족합니다.

EKS 자율 모드

활성화됨

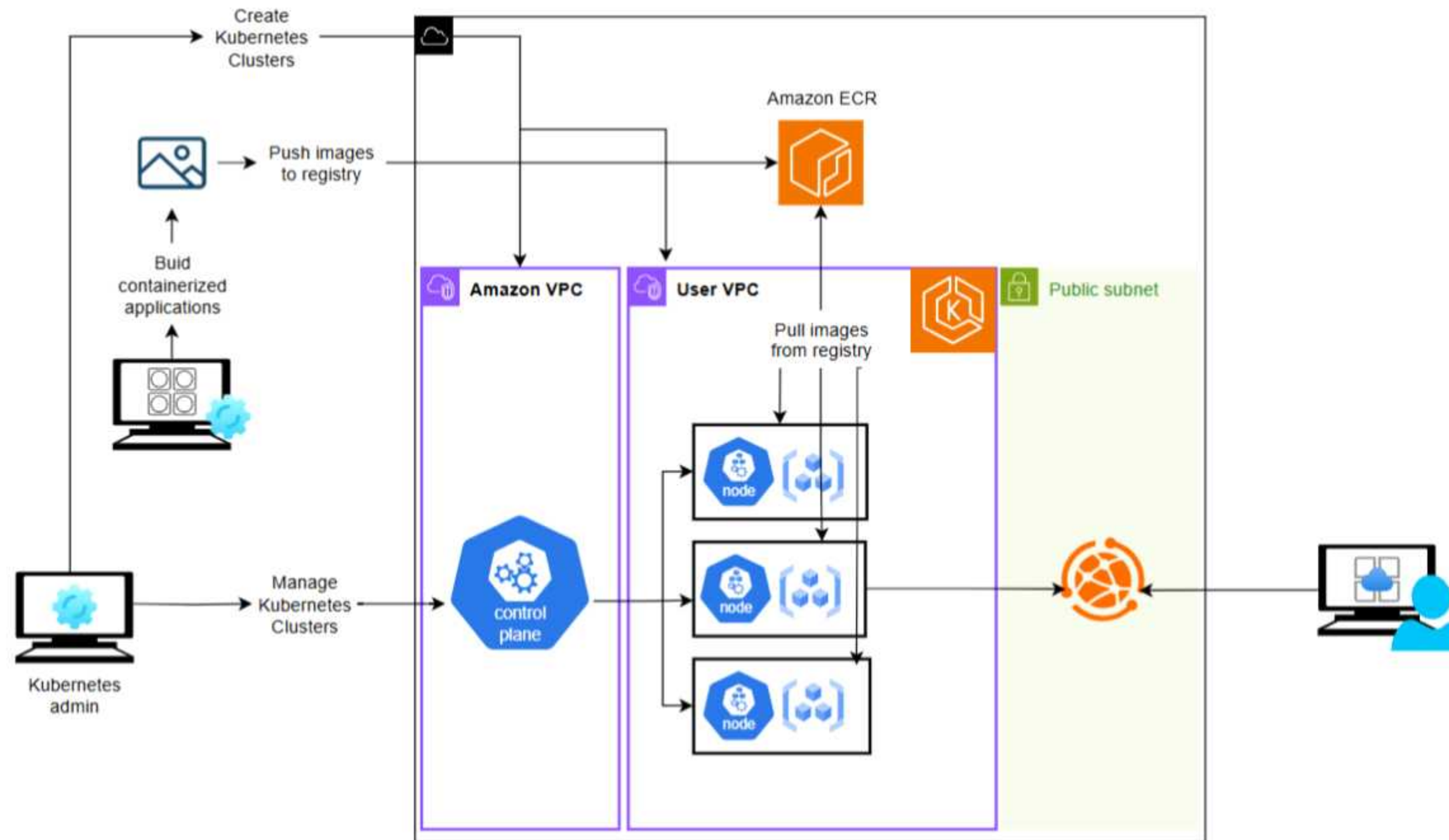
노드 IAM 역할

arn:aws:iam::183631310061:role/muhanEKSThroughNode

관리

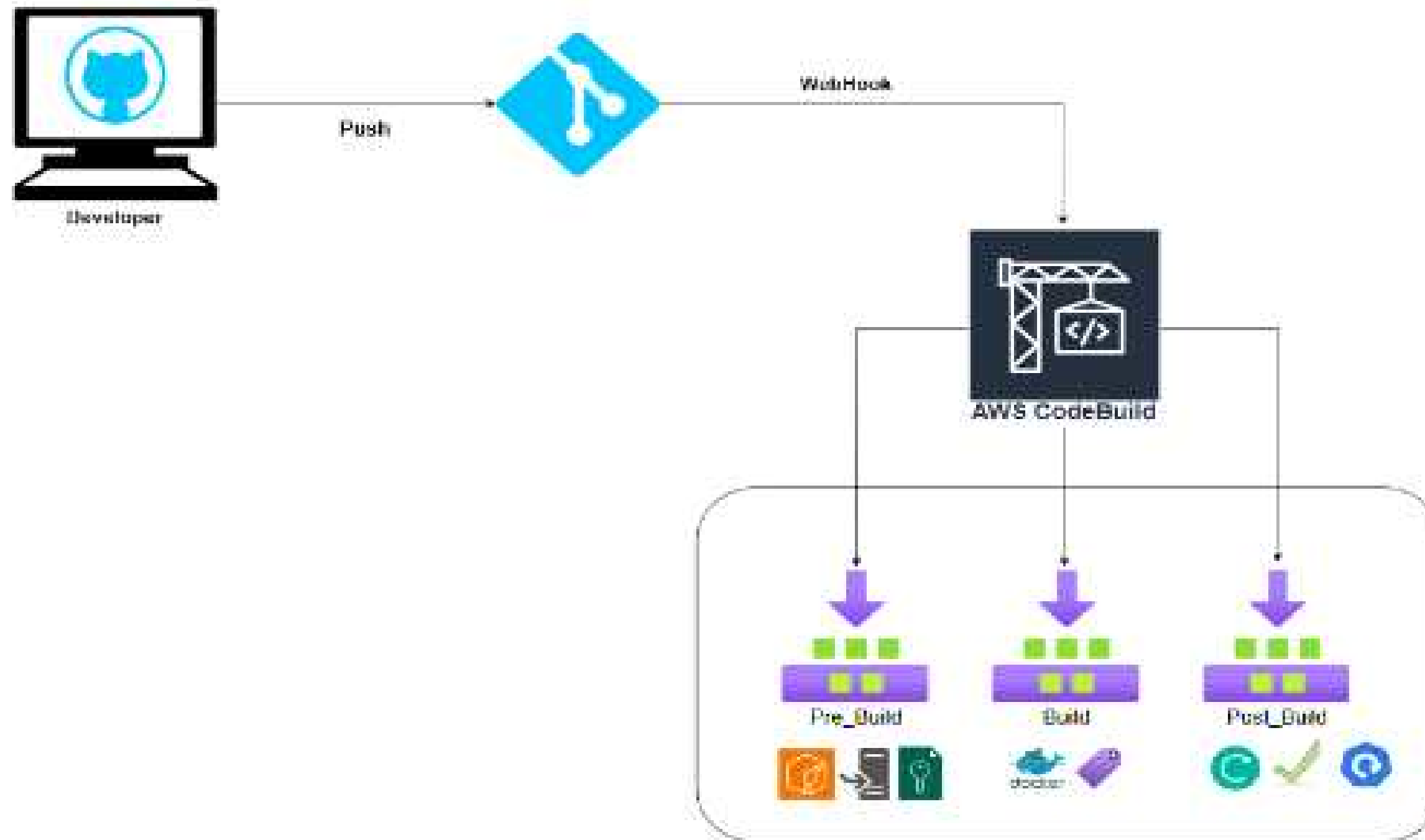
# EKS & DB 및 CI/CD

## EKS Cluster In Action



# EKS & DB 및 CI/CD

## CI/CD 구조





# EKS & DB 및 CI/CD

## Code Build

### HospitalUpdate

작업 ▼트리거 생성편집복제디버그 빌드재정의로 빌드 시작빌드 시작

구성

소스 공급자 GitHub	기본 리포지토리 choiwoojae1547/hospital	아티팩트 업로드 위치 -	서비스 역할 arn:aws:iam::183631310061:role/service-role/codebuild-HospitalUpdate-choiwoojae
퍼블릭 빌드 비활성			

빌드 기록배치 이력프로젝트 세부 정보빌드 트리거지표

프로젝트 구성

편집

이름 HospitalUpdate	설명 -
프로젝트 ARN arn:aws:codebuild:ap-northeast-2:183631310061:project/HospitalUpdate	빌드 배치 비활성
동시 빌드 제한 -	
▶ 태그	

# EKS & DB 및 CI/CD

## Code Build - 소스

소스

편집

소스 공급자	소스 식별자	리포지토리	소스 버전
GitHub	-	<a href="#">choiwoojae1547/hospital</a>	-
Git clone 깊이	Git 하위 모듈		
1	false		

▼ 기본 소스 Webhook 이벤트

Webhook	Webhook Status	Webhook Status Message
<a href="https://github.com/choiwoojae1547/hospital/settings/hooks/534354019">https://github.com/choiwoojae1547/hospital/settings/hooks/534354019</a>	ACTIVE	-

# EKS & DB 및 CI/CD

## Code Build - 세부정보

HospitalUpdate:90506b45-a512-4968-b3bb-87cefb9aba45

빌드 중지

빌드 재시도

### 빌드 상태

상태 ✅ 성공함	시작한 사용자 GitHub-Hookshot/1226e46	빌드 ARN arn:aws:codebuild:ap-northeast-2:183631310061:build/HospitalUpdate:90506b45-a512-4968-b3bb-87cefb9aba45	해결된 소스 버전 2ab161e005496594b3b73644fd185598d14a1066
시작 시간 3월 11, 2025 3:24 오후 (UTC+9:00)	종료 시간 3월 11, 2025 3:26 오후 (UTC+9:00)	빌드 번호 40	

빌드 로그 단계 세부 정보 보고서 환경 변수 빌드 세부 정보 리소스 사용률

이름	상태	컨텍스트	기간	시작 시간	종료 시간
SUBMITTED	✅ 성공함	-	<1 sec	3월 11, 2025 3:24 오후 (UTC+9:00)	3월 11, 2025 3:24 오후 (UTC+9:00)
QUEUED	✅ 성공함	-	1 sec	3월 11, 2025 3:24 오후 (UTC+9:00)	3월 11, 2025 3:24 오후 (UTC+9:00)
PROVISIONING	✅ 성공함	-	30 secs	3월 11, 2025 3:24 오후 (UTC+9:00)	3월 11, 2025 3:25 오후 (UTC+9:00)
DOWNLOAD_SOURCE	✅ 성공함	-	5 secs	3월 11, 2025 3:25 오후 (UTC+9:00)	3월 11, 2025 3:25 오후 (UTC+9:00)
INSTALL	✅ 성공함	-	<1 sec	3월 11, 2025 3:25 오후 (UTC+9:00)	3월 11, 2025 3:25 오후 (UTC+9:00)
PRE_BUILD	✅ 성공함	-	13 secs	3월 11, 2025 3:25 오후 (UTC+9:00)	3월 11, 2025 3:25 오후 (UTC+9:00)
BUILD	✅ 성공함	-	40 secs	3월 11, 2025 3:25 오후 (UTC+9:00)	3월 11, 2025 3:26 오후 (UTC+9:00)
POST_BUILD	✅ 성공함	-	14 secs	3월 11, 2025 3:26 오후 (UTC+9:00)	3월 11, 2025 3:26 오후 (UTC+9:00)
UPLOAD_ARTIFACTS	✅ 성공함	-	<1 sec	3월 11, 2025 3:26 오후 (UTC+9:00)	3월 11, 2025 3:26 오후 (UTC+9:00)
FINALIZING	✅ 성공함	-	<1 sec	3월 11, 2025 3:26 오후 (UTC+9:00)	3월 11, 2025 3:26 오후 (UTC+9:00)
COMPLETED	✅ 성공함	-	-	3월 11, 2025 3:26 오후 (UTC+9:00)	-

# EKS & DB 및 CI/CD

## Code Build - 정책

권한 정책 (13) 정보

최대 10개의 관리형 정책을 연결할 수 있습니다.



시뮬레이션

삭제

권한 추가

검색		필터링 기준 유형		< 1 > ⚙	
<input type="checkbox"/> 정책 이름	유형	연결된 엔터티			
<input type="checkbox"/> <a href="#">AdministratorAccess</a>	AWS 관리형 - 직무	5			
<input type="checkbox"/> <a href="#">AmazonEKS_CNI_Policy</a>	AWS 관리형	3			
<input type="checkbox"/> <a href="#">AmazonEKSClusterPolicy</a>	AWS 관리형	2			
<input type="checkbox"/> <a href="#">AmazonEKSFargatePodExecutionRolePolicy</a>	AWS 관리형	1			
<input type="checkbox"/> <a href="#">AmazonEKSServicePolicy</a>	AWS 관리형	2			
<input type="checkbox"/> <a href="#">AmazonEKSVPCResourceController</a>	AWS 관리형	2			
<input type="checkbox"/> <a href="#">AWSCodeCommitFullAccess</a>	AWS 관리형	1			
<input type="checkbox"/> <a href="#">AWSCodePipeline_FullAccess</a>	AWS 관리형	1			
<input type="checkbox"/> <a href="#">CodeBuildBasePolicy-codebuild-HospitalUpdate-Choiwoojae-ap...</a>	고객 관리형	1			
<input type="checkbox"/> <a href="#">CodeBuildCodeConnectionsSourceCredentialsPolicy-HospitalUp...</a>	고객 관리형	1			
<input type="checkbox"/> <a href="#">eksAccessKubernetesApi</a>	고객 인라인	0			
<input type="checkbox"/> <a href="#">EKSDescribecluster</a>	고객 인라인	0			
<input type="checkbox"/> <a href="#">stsAssumeRole</a>	고객 인라인	0			

# 모니터링 및 보안 강화

## 보안 그룹 - EKS Cluster 보안그룹

sg-00341a3c1c44e5bee - MuhanEKSCluster

작업 ▼

### 세부 정보

보안 그룹 이름

MuhanEKSCluster

보안 그룹 ID

sg-00341a3c1c44e5bee

설명

SG for MuhanEKSCluster

VPC ID

vpc-0a1a03635eaa38c5a

소유자

183631310061

인바운드 규칙 수

2 권한 항목

아웃바운드 규칙 수

0 권한 항목

인바운드 규칙

아웃바운드 규칙

공유 - 신규

VPC 연결 - 신규

태그

### 인바운드 규칙 (2)



태그 관리

인바운드 규칙 편집

< 1 > ⚙

🔍 검색

<input type="checkbox"/>	Name ▼	보안 그룹 규칙 ID ▼	IP 버전 ▼	유형 ▼	프로토콜 ▼	포트 범위 ▼	소스 ▼	설명 ▼
<input type="checkbox"/>	Control Plane ENI	sgr-0e80e070dead2adea	-	사용자 지정 TCP	TCP	1025 - 65535	sg-08d89aa96bedcf688 / EKSWorkerNodeSG	Worker NodeSG
<input type="checkbox"/>	Control Plane ENI	sgr-069139b26874e166b	-	HTTPS	TCP	443	sg-08d89aa96bedcf688 / EKSWorkerNodeSG	Worker NodeSG



# 모니터링 및 보안 강화

## 보안 그룹 - EKS Worker Nodes 보안그룹

sg-08d89aa96bedcf688 - EKSWorkerNodeSG

작업 ▼

### 세부 정보

보안 그룹 이름 EKSWorkerNodeSG	보안 그룹 ID sg-08d89aa96bedcf688	설명 SG for EKSWorkerNode	VPC ID vpc-0a1a03635eaa38c5a
소유자 183631310061	인바운드 규칙 수 4 권한 항목	아웃바운드 규칙 수 1 권한 항목	

인바운드 규칙 | 아웃바운드 규칙 | 공유 - 신규 | VPC 연결 - 신규 | 태그

### 인바운드 규칙 (4)

태그 관리 | 인바운드 규칙 편집

Q 검색

< 1 > ⚙

<input type="checkbox"/>	Name ▼	보안 그룹 규칙 ID ▼	IP 버전 ▼	유형 ▼	프로토콜 ▼	포트 범위 ▼	소스 ▼	설명 ▼
<input type="checkbox"/>	All traffic	sgr-0b97722e86053dd32	-	모든 트래픽	전체	전체	<a href="#">sg-08d89aa96bedcf688 / EKSWorkerNodeSG</a>	WorkerNode Self Traffic Allow
<input type="checkbox"/>	SSH	sgr-02638f6771fbb7fa5	IPv4	SSH	TCP	22	43.201.83.133/32	Admin EC2 IP
<input type="checkbox"/>	Kubernetes API	sgr-0c5030306eab2c408	-	HTTPS	TCP	443	<a href="#">sg-00341a3c1c44e5bee / MuhanEKSCluster</a>	EKSClusterSG
<input type="checkbox"/>	NodePort	sgr-0ebd4926281984f1a	IPv4	사용자 지정 TCP	TCP	30000 - 32767	10.0.0.0/16	VPC CIDR



# 모니터링 및 보안 강화

## 보안 그룹 - EKS Worker Node의 아웃바운드 규칙

sg-08d89aa96bedcf688 - EKSWorkerNodeSG

작업 ▼

### 세부 정보

보안 그룹 이름 EKSWorkerNodeSG	보안 그룹 ID sg-08d89aa96bedcf688	설명 SG for EKSWorkerNode	VPC ID vpc-0a1a03635eaa38c5a
소유자 183631310061	인바운드 규칙 수 2 권한 항목	아웃바운드 규칙 수 1 권한 항목	

인바운드 규칙   아웃바운드 규칙   공유 - 신규   VPC 연결 - 신규   태그

### 아웃바운드 규칙 (1)



태그 관리

아웃바운드 규칙 편집

< 1 > ⚙

검색

<input type="checkbox"/>	Name ▼	보안 그룹 규칙 ID ▼	IP 버전 ▼	유형 ▼	프로토콜 ▼	포트 범위 ▼	대상 ▼	설명 ▼
<input type="checkbox"/>	-	sgr-0abe09a32a4583663	IPv4	모든 트래픽	전체	전체	0.0.0.0/0	-

# 모니터링 및 보안 강화

## Amazon WAF & SHIELD

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)

☒ Regional resources (Application Load Balancers, Amazon API Gateway REST APIs, AWS AppSync GraphQL 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) ▼

**Name**

muhanWAF

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

**Description - optional**

generalhospital 인프라에 대한 전체적인 보호

The description can have 1-256 characters.

**CloudWatch metric name**

muhanWAF

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

**Associated AWS resources - optional (1)** [Remove](#) [Add AWS resources](#)

Find associated AWS resources

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

### SQL 인젝션 공격 방지

SQL 인젝션 시도를 차단

### DDoS 보호

Shield Advanced로 대규모 DDoS 공격 방어

CloudWatch를 통해 대역폭 사용량 초과를 탐지하여 알림 설정

# 모니터링 및 보안 강화

## Amazon WAF & SHIELD

<b>Admin protection</b> Contains rules that allow you to block external access to exposed admin pages. This may be useful if you are running third-party software or would like to reduce the risk of a malicious actor gaining administrative access to your application. <a href="#">Learn More</a>	100	<input checked="" type="checkbox"/> Add to web ACL <a href="#">Edit</a>
<b>Amazon IP reputation list</b> This group contains rules that are based on Amazon threat intelligence. This is useful if you would like to block sources associated with bots or other threats. <a href="#">Learn More</a>	25	<input checked="" type="checkbox"/> Add to web ACL <a href="#">Edit</a>
<b>Anonymous IP list</b> 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. <a href="#">Learn More</a>	50	<input checked="" type="checkbox"/> Add to web ACL <a href="#">Edit</a>
<b>Core rule set</b> 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. <a href="#">Learn More</a>	700	<input type="checkbox"/> Add to web ACL
<b>Known bad inputs</b> 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. <a href="#">Learn More</a>	200	<input checked="" type="checkbox"/> Add to web ACL <a href="#">Edit</a>
<b>Linux operating system</b> 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. <a href="#">Learn More</a>	200	<input type="checkbox"/> Add to web ACL
<b>PHP application</b> 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. <a href="#">Learn More</a>	100	<input checked="" type="checkbox"/> Add to web ACL <a href="#">Edit</a>
<b>POSIX operating system</b> 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 been allowed. <a href="#">Learn More</a>	100	<input type="checkbox"/> Add to web ACL
<b>SQL database</b> 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. <a href="#">Learn More</a>	200	<input checked="" type="checkbox"/> Add to web ACL <a href="#">Edit</a>

### Admin protection

- 노출된 관리자 페이지에 대한 외부 액세스를 차단할 수 있는 규칙

### Amazon IP reputation list

- 봇이나 다른 위협과 관련된 소스를 차단

### Anonymous IP list

- 애플리케이션에서 신원을 숨기려는 사용자를 필터링

### Known bad inputs

- 악용이 알려진 비정상 요청 패턴 차단
- 취약점 탐지 또는 공격 시도 방지

### PHP application

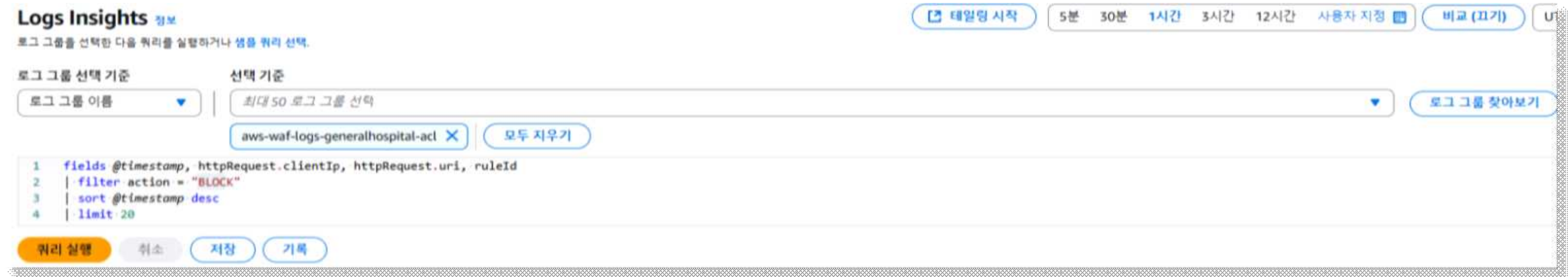
- PHP 기반 애플리케이션 취약점 악용 차단
- 원격 코드 실행(RCE) 등 공격 방지

### SQL database

- 허가되지 않은 쿼리의 원격 주입을 방지

# 모니터링 및 보안 강화

## Amazon WAF & SHIELD Test



The screenshot shows the Amazon WAF Logs Insights console. At the top, there's a 'Logs Insights' header with a '정보' (Info) link. Below it, a sub-header says '로그 그룹을 선택한 다음 쿼리를 실행하거나 샘플 쿼리 선택.' (Select a log group, then run a query or select a sample query.). On the right, there are buttons for '테일링 시작' (Start Tailing), time range filters (5분, 30분, 1시간, 3시간, 12시간), '사용자 지정' (Custom), '비교 (끄기)' (Compare (Toggle)), and 'U'. Below these, there's a '로그 그룹 선택 기준' (Log group selection criteria) dropdown set to '로그 그룹 이름' (Log group name) and a '선택 기준' (Selection criteria) dropdown set to '최대 50 로그 그룹 선택' (Select up to 50 log groups). A search bar contains 'aws-waf-logs-generalhospital-acl' with a close button 'X' and a '모두 지우기' (Clear all) button. A '로그 그룹 찾아보기' (Find log groups) button is on the right. Below the search bar, a query editor shows a sample query: 

```
1 fields @timestamp, httpRequest.clientIp, httpRequest.uri, ruleId
2 | filter action = "BLOCK"
3 | sort @timestamp desc
4 | limit 20
```

 At the bottom, there are buttons for '쿼리 실행' (Run query), '취소' (Cancel), '저장' (Save), and '기록' (Log).

### Amazon WAF Logs Insights Query

차단된 요청 쿼리 입력

- 차단된 요청을 보기위한 쿼리문을 입력

```
fields @timestamp, httpRequest.clientIp, httpRequest.uri, ruleId
| filter action = "BLOCK"
| sort @timestamp desc
| limit 20
```

# 모니터링 및 보안 강화

## Amazon WAF & SHIELD Test

```
[muhancloudse@localhost] ~ % curl -X GET "http://www.g-hospital.com?id=' OR '1'='1'"
```

### SQL Injection Simulation

데이터베이스에서 비정상적인 쿼리를 실행하여 민감한 정보를 탈취하거나 권한을 우회

- id=' OR '1'='1' -> '1'='1' 조건은 항상 참(True)이 되므로, 데이터베이스의 모든 레코드를 반환하도록 유도



# 모니터링 및 보안 강화

## Amazon WAF & SHIELD Test



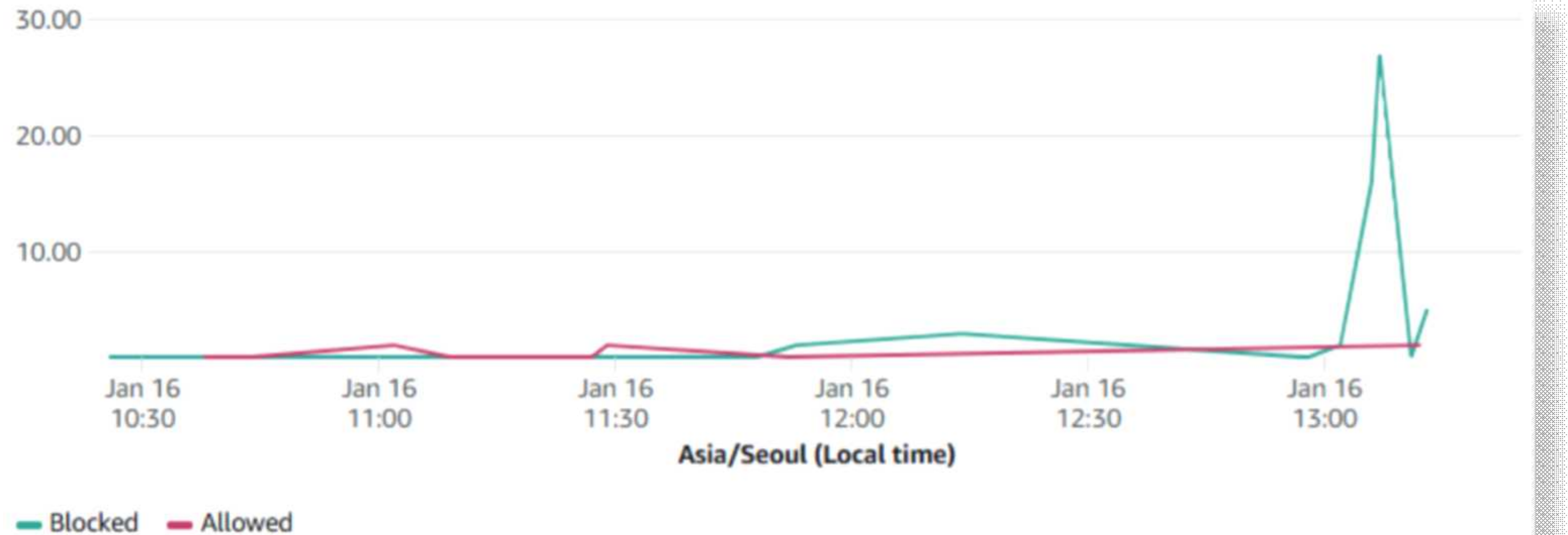
### SQL Injection Simulation\_Log

timestamp	httpRequest.clientIp	httpRequest.uri
- 요청이 발생한 시간	- 요청을 보낸 클라이언트의 IP 주소	- 요청된 URI
- 로그에서 요청이 발생한 시점	- IP가 요청을 보냈고, 차단	- REDACTED로 표시된 것은 WAF 설정에서 URI 또는 기타 민감한 데이터를 마스킹 처리



# 모니터링 및 보안 강화

## Amazon WAF & SHIELD Test



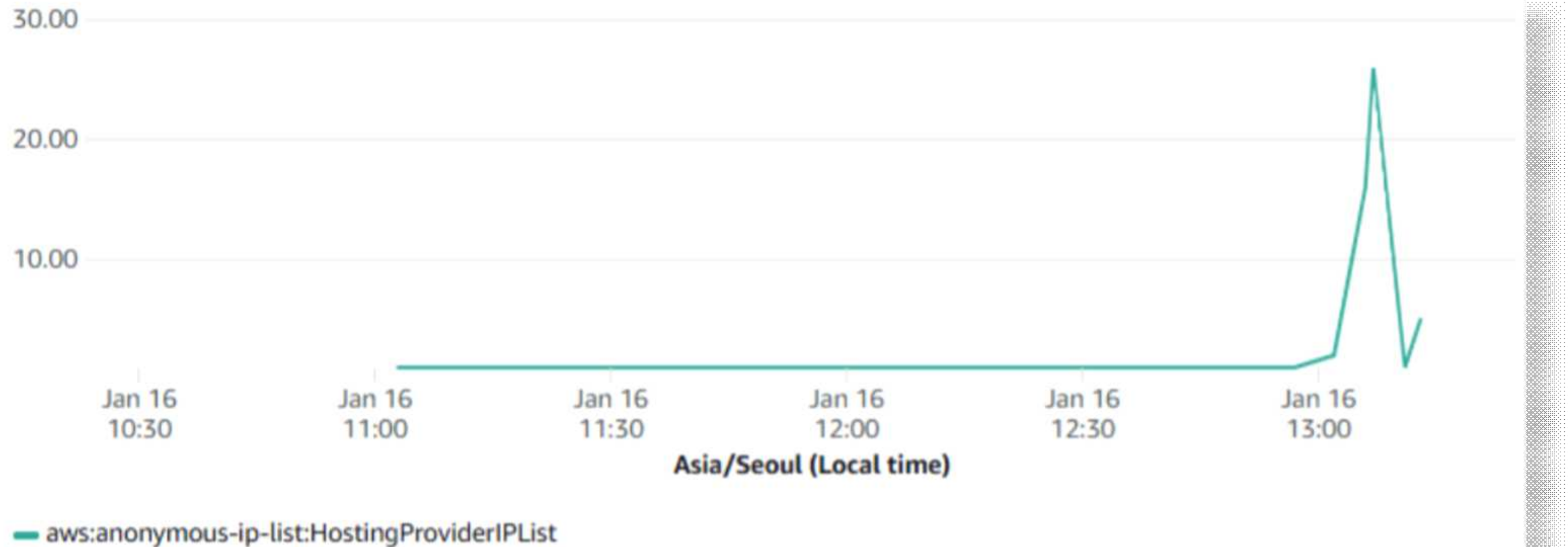
### SQL Injection Simulation\_Log

시각화 데이터

- 차단된 요청과 허용된 요청 비교 데이터 시각화

# 모니터링 및 보안 강화

## Amazon WAF & SHIELD Test



### SQL Injection Simulation\_Log

시각화 데이터

- 익명 연결에 대한 로그 데이터 시각화

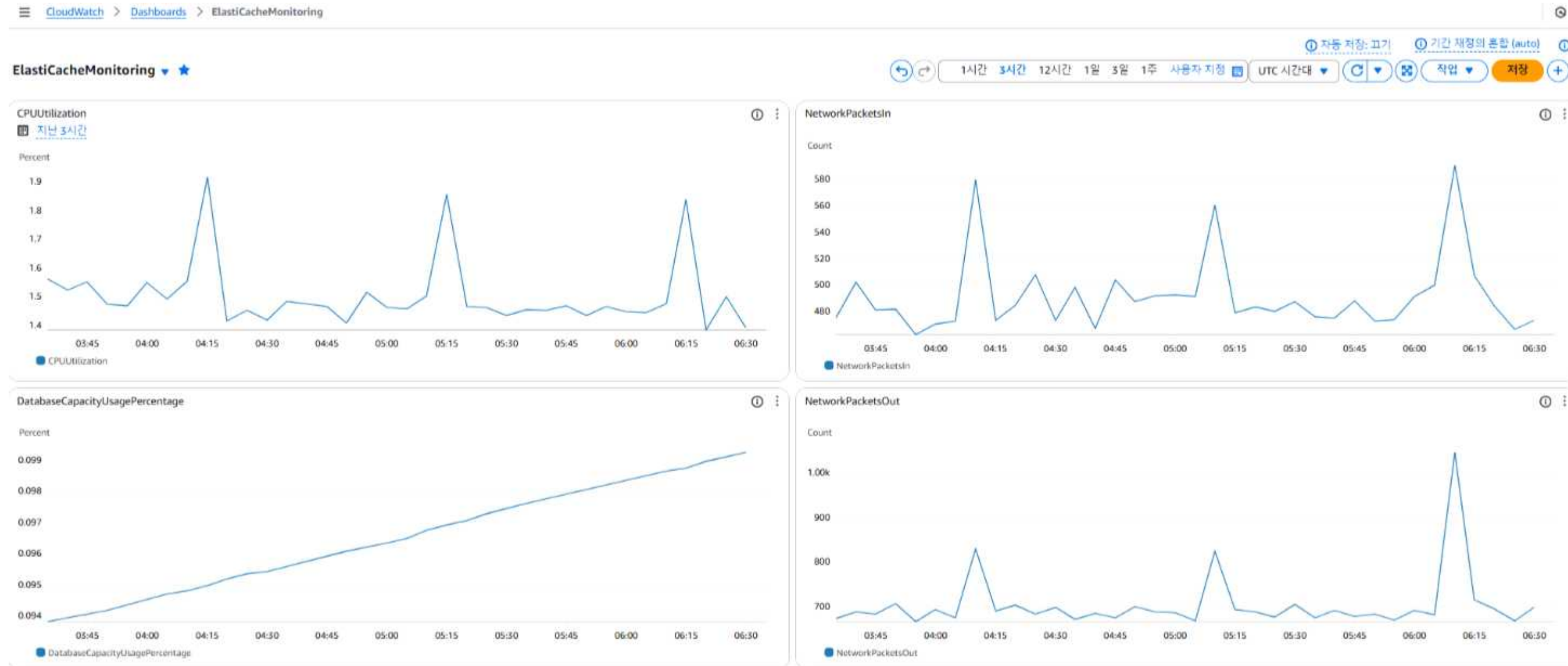
# 모니터링 및 보안 강화

## CloudWatch - EKS Cluster 모니터링




# 모니터링 및 보안 강화

## CloudWatch - ElastiCache 모니터링



# 모니터링 및 보안 강화

## Amazon Simple Notification Service (SNS)

 **AWS Notifications** <no-reply@sns.amazonaws.com>  
나에게 ▾

오후 1:14 (4시간 전) ☆ 😊 ↩ ⋮

You are receiving this email because your Amazon CloudWatch Alarm "BuildFailAlarm" in the Asia Pacific (Seoul) region has entered the ALARM state, because "Threshold Crossed: 1 out of the last 1 datapoints [1.0 (11/03/25 04:04:00)] was greater than or equal to the threshold (0.5) (minimum 1 datapoint for OK -> ALARM transition)." at "Tuesday 11 March, 2025 04:09:00 UTC".

View this alarm in the AWS Management Console:  
<https://ap-northeast-2.console.aws.amazon.com/cloudwatch/deeplink.js?region=ap-northeast-2#alarmsV2:alarm/BuildFailAlarm>

Alarm Details:

- Name: BuildFailAlarm
- Description: Build Fail!!
- State Change: OK -> ALARM
- Reason for State Change: Threshold Crossed: 1 out of the last 1 datapoints [1.0 (11/03/25 04:04:00)] was greater than or equal to the threshold (0.5) (minimum 1 datapoint for OK -> ALARM transition).
- Timestamp: Tuesday 11 March, 2025 04:09:00 UTC

## Amazon Simple Notification Service

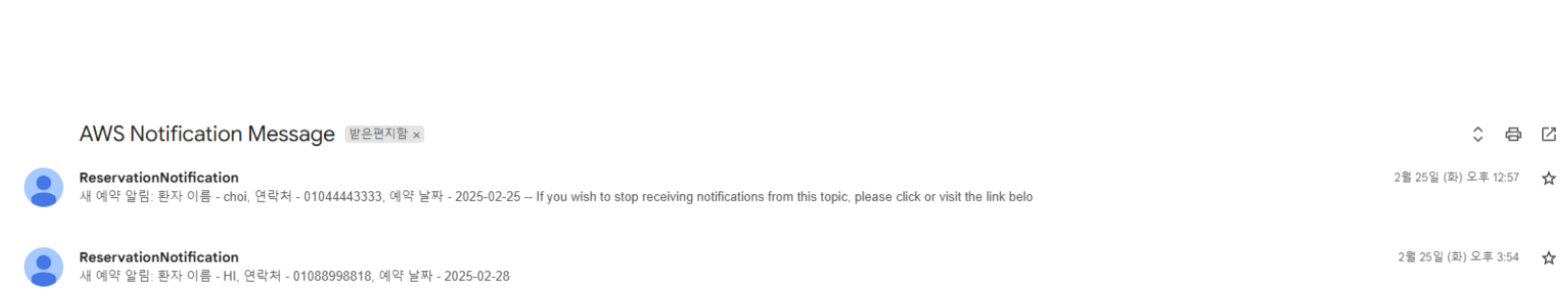
E-mail (CodeBuild Fail 알람)

알림을 구독되어있는 이메일로 수신하여 사용자에게 알림 기능 제공



# 모니터링 및 보안 강화

## Amazon Simple Notification Service (SNS)

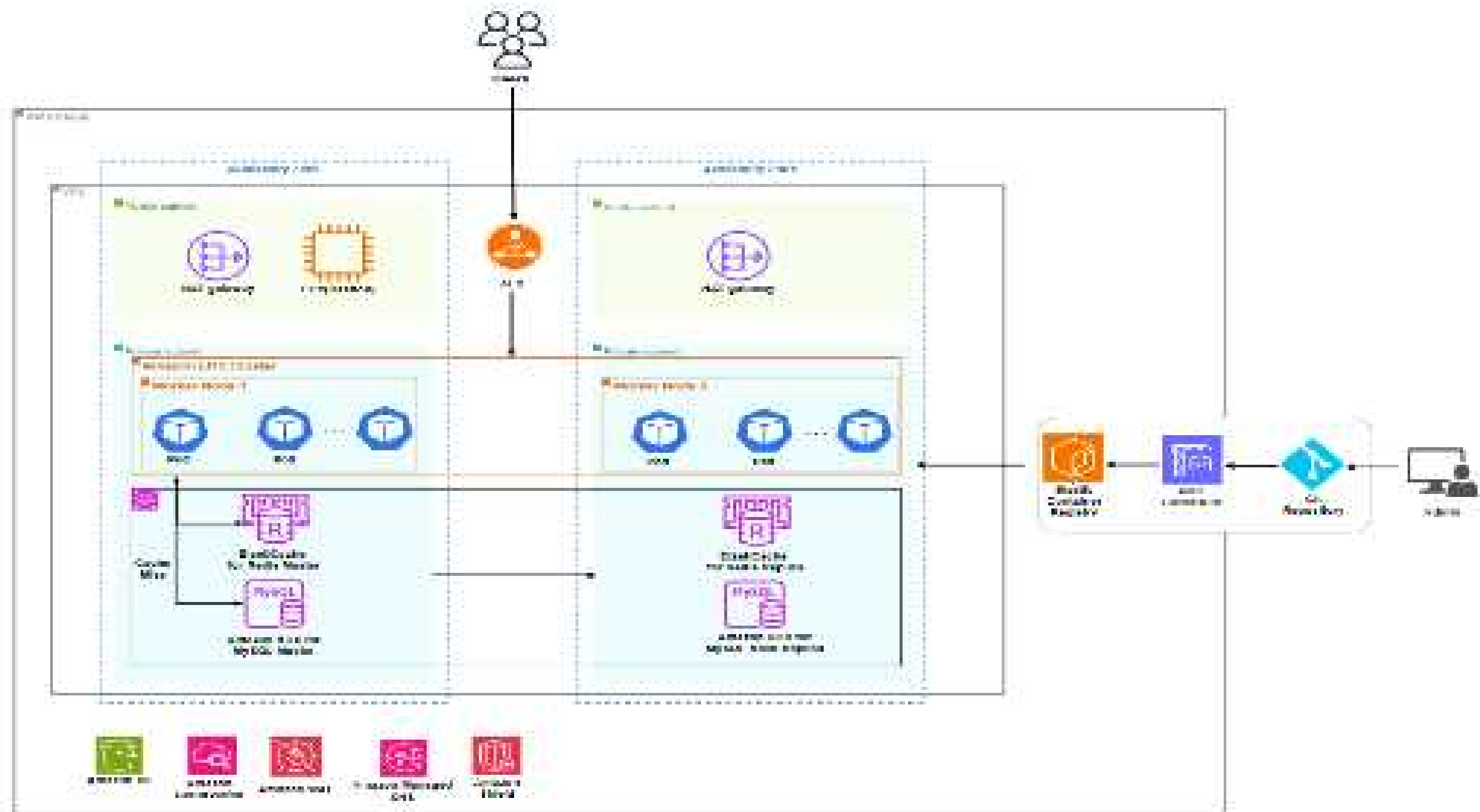


## Amazon Simple Notification Service

E-mail (예약 성공 알람)

알림을 구독되어있는 이메일로 수신하여 사용자에게 알림 기능 제공

# 최종 아키텍처



# 기대 효과



## 확장성 및 운영 효율성

- EKS 자동 확장 & CI/CD로 유연한 대응
- 서버 운영 부담 감소, 표준화된 환경 구축
- 마이크로서비스 전환 기반 마련

## 비용 최적화 및 서비스 가용성

- 리소스 최적화로 비용 절감
- Auto Healing으로 장애 대응
- 실시간 모니터링으로 안정성 향상

# 서비스 분리 및 MSA 전환

## 예약 시스템

- 의사별 스케줄 관리
- 예약 변경 및 취소
- 온라인 예약 기능
- 알림 서비스 연동

## 진료 기록 관리

- 전자의무기록(EMR) 관리
- 의료영상저장전송시스템
  - 환자 이력 조회 기능
  - 데이터 보안 강화

### MSA 전환 주요 서비스

## 결제 시스템

- 환불 처리 기능
- 보험 청구 자동화
- 영수증 발행 시스템
- 다양한 결제 방식 지원

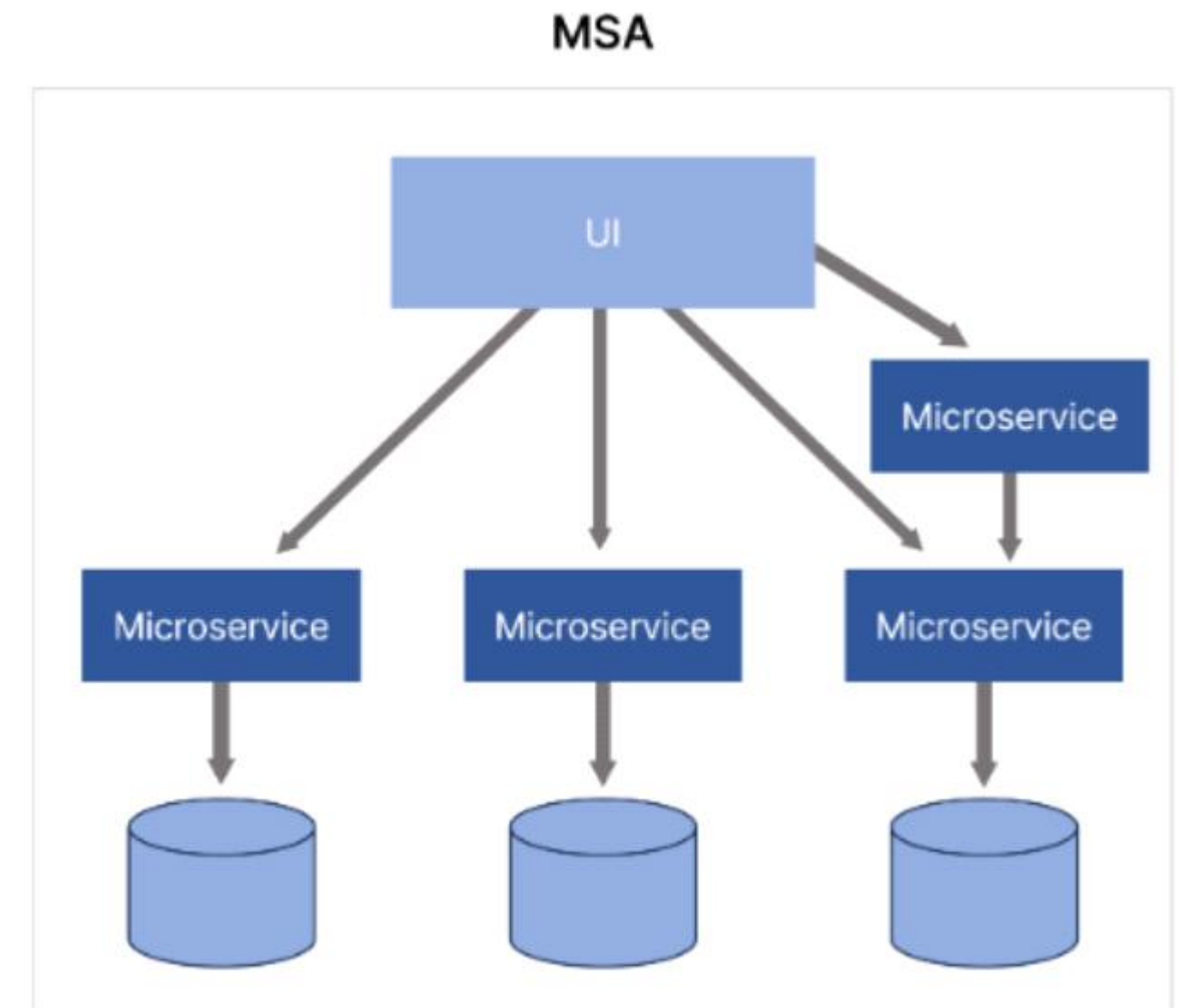
## 기타 서비스

- 의료기기 관리
- 약국 관리 시스템
- 직원 관리 시스템
- 재고 관리 시스템


# 결론

## 클라우드 전환 및 최적화를 통한 병원 IT 서비스 혁신

- 서비스 확장성 및 효율성 강화: 클라우드 전환으로 운영 최적화
- 안정성 강화: 자동 확장 및 자가 복구 도입
- 운영 부담 경감: CodeBuild로 배포 자동화
- 시스템 유연성 향상: 향후 MSA 도입 예정
- 리스크 최소화: 모니터링 및 최적화로 가용성 향상
- 효율성 증대: 서비스 개별화로 독립성 및 효율성 강화







---

# Q & A