



TechTalk 2023

# 안정적인 11st EKS 운영기

cloud engineering team 이무열

# CONTENTS

1. 팀 소개
2. EKS 현황
3. EKS 이슈
4. EKS 개선
5. 마무리

AWS 기반 **클라우드 인프라 구축** 운영을 담당하는 조직

- 클라우드 엔지니어링에 관련된 전반적인 업무 수행
- 레거시에서 클라우드로 넘어올 때 설계 및 기술적인 내용에 대한 전반적인 부분 지원

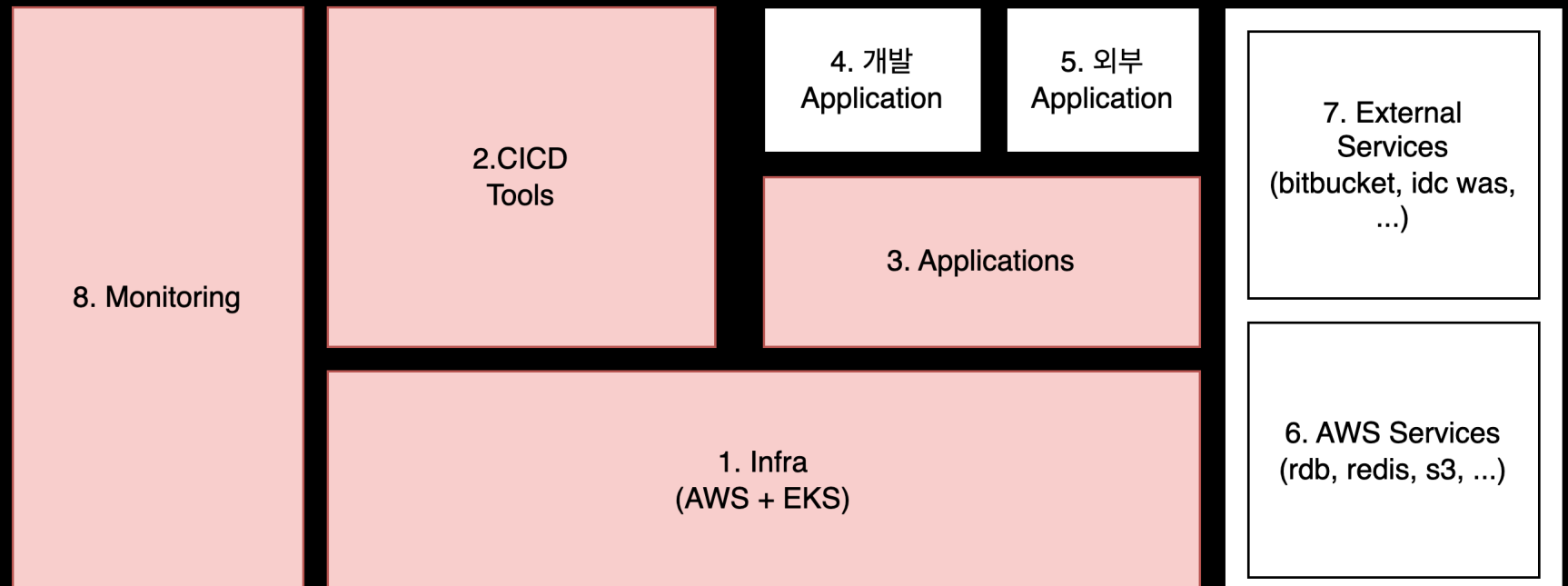
EKS 파트

- 4년차 현재 담당자는 3명
- **안정적인 운영 및 장애 복구**
- EKS기반 서비스 런칭 지원
- 장애 발생 시 개발팀 지원

# EKS 현황 : 외부 관계도 구조

## EKS 구조와 범위 구분

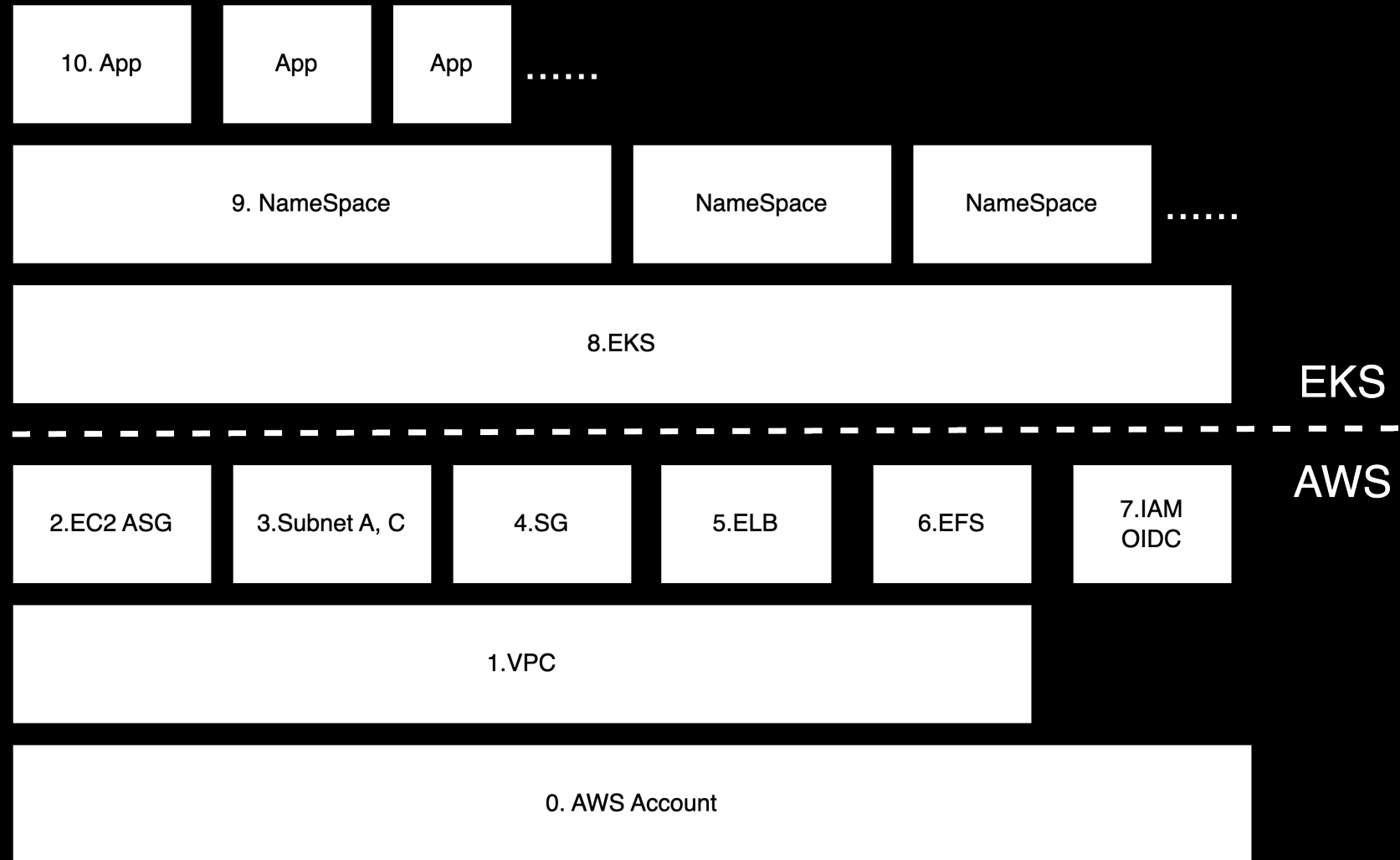
- 8개 범위로 구분
- Cloud Engineering Team에서 모두 관리 중
- EKS Part는 1,2,3,8에 전문적인 역량을 가짐



# EKS 현황 : 내부 구성요소 구조

## EKS 구조 및 구성 요소

- EKS Resource
- AWS Resource



# EKS 현황 : 구축 방법

## 안정적인 인프라 구축

- GitOps기반 **인프라 코드** 관리
- 다양한 팀을 지원하기 위한 **권한 관리 및 보안적용**
- 비용 효율적인 운영 방안 지속적 업데이트
- 클러스터 상황 파악을 위한 **로깅과 모니터링**

## 모든 것이 **예측 가능**하고 **제어 가능**한 인프라 구축 목표

- 예측 가능하고 해결 가능한 이슈
- 대안마련이 가능한 이슈



# EKS 이슈 : 설정과 관리의 복잡성

11 TechTalk 2023

EKS 클러스터는 총 10개

- 모든 클러스터는 중앙집중식으로 관리
- 테라폼 기반 gitops 방식으로 운영
- 다양한 코드 관리 및 다양한 업무 수행
- 타 팀 업무 연계 시 업무 절차를 마련

이를 해결하기 위해 십일번가에 더 특화된 코드와 업무 절차를 만들게 되었습니다

- 모든 설정은 코드로 대응
- git PR 방식을 적극 활용
- 타 팀과 소통 시 PR 위주로 작업 내용 공유



# EKS 이슈 : 권한 관리 및 보안 적용

11 TechTalk 2023

개발팀, 플랫폼 운영팀, 시스템 운영팀, 보안팀등 **다양한 팀과 협업**  
각 팀에 맞는 권한을 나눠서 부여

**AWS SSO**와 **IRSA**를 통한 인증 및 권한 관리 적용

3rdParty. App을 위한 인증 관리 적용

**컨테이너 보안**을 위해 검증된 이미지만 사용

외부 이미지의 내재화 절차 마련

다수의 클러스터를 위한 일괄된 운영 정책 방안 마련

**ISMS-P 보안 심사**를 위한 지침 적용





# EKS 이슈 : 모니터링

## 뚜렷한 목적기반의 모니터링

솔루션과 툴보다는 어떤 **목적**으로 볼지 결정해야함

- EKS 상태 모니터링
- Service on EKS(SoEKS) 모니터링



각 팀마다 원하는 view가 다름

- 각 **업무별** 모니터링 목적이 다름

모니터링 솔루션마다 볼 수 있는 뷰가 다름

- 상용과 무료를 모두 살펴봄
- 가격도 중요 고려 요소

```

! v1/pods error
Kind: Pod
Name: kubernetes-
7b775f7c9c-xcgv
Namespace: kubernetes-event-exporter
Reason: Evicted
Cluster: 11st-vine-prod-amber

Messages
• The node was low on resource: ephemeral-storage. Container
24100Ki, which exceeds its request of 0.
    
```

범위	항목	제목	상세 설명	보호 조치	모니터링
권한	Namespace	Namespace 분리를 통해 과도한 권한을 통제한다	<ul style="list-style-type: none"> <li>개발자 본인의 서비스에 대해서만 전체 권한을 가질 수 있다</li> </ul>	<ul style="list-style-type: none"> <li>ISMS-P: 2.5.1 사용자 계정</li> <li>Namespace 분리</li> </ul>	<ul style="list-style-type: none"> <li>Splunk를 통해 Namespace 현황을 조회한다</li> </ul>

# EKS 이슈 : 비용

비용은 항상 문제가 됨

정확한 서비스별 비용 산정이 어려움

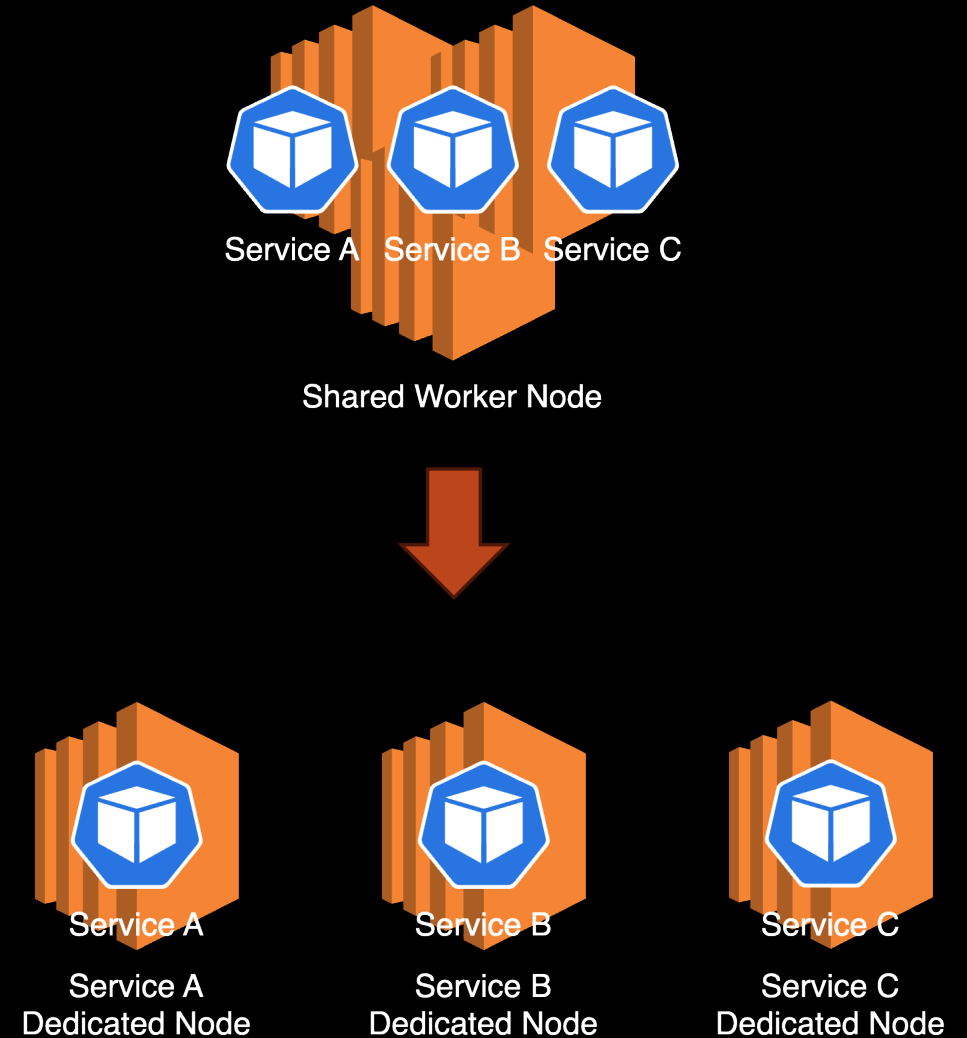
- **쉐어드 노드**
- 컨테이너의 불규칙한 실행과 종료 반복
- ec2의 spot사용에 따른 잦은 변경

운영 비용 가시성 확보 실패

- 효율적 운영의 근거 자료로 부적절
- 예상치 못한 자원 파악을 빠르게 할 수 없음

비용 가시성 확보를 위한 계획

- **서비스별 전용 노드로 분리**



# EKS 이슈 : 업그레이드

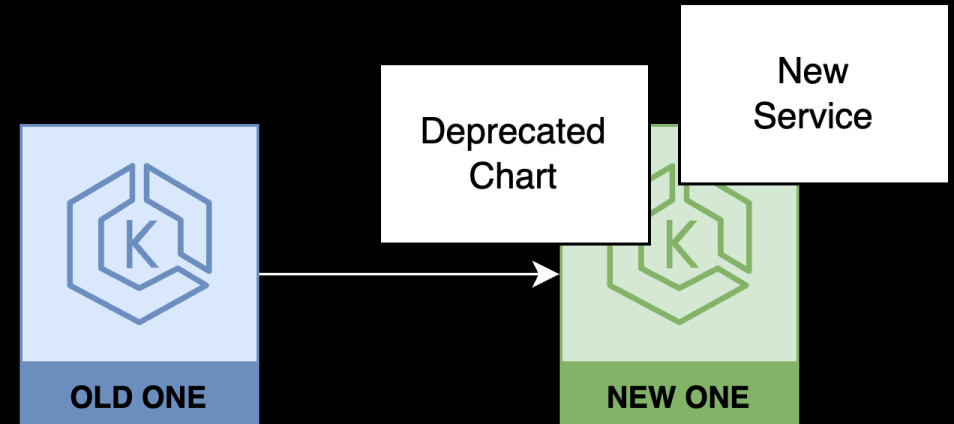
14개월 단위로 지원이 종료되는 EKS

**강제 업그레이드** 난항

K8s 버전업에 따른 변화점 따라가야함

관련 OSS들도 모두 업그레이드 필수

새로운 클러스터를 생성 후 이관 작업을 수행함



Kubernetes 버전	업스트림 릴리스	Amazon EKS 릴리스	표준 지원 종료일
1.28	2023년 8월 15일	2023년 9월 26일	2024년 11월
1.27	2023년 4월 11일	2023년 5월 24일	2024년 7월
1.26	2022년 12월 9일	2023년 4월 11일	2024년 6월
1.25	2022년 8월 23일	2023년 2월 22일	2024년 5월
1.24	2022년 5월 3일	2022년 11월 15일	2024년 1월 31일
1.23	2021년 12월 7일	2022년 8월 11일	2023년 10월 11일

# EKS 이슈 : 사소하지만 중요한 문제들

11 TechTalk 2023

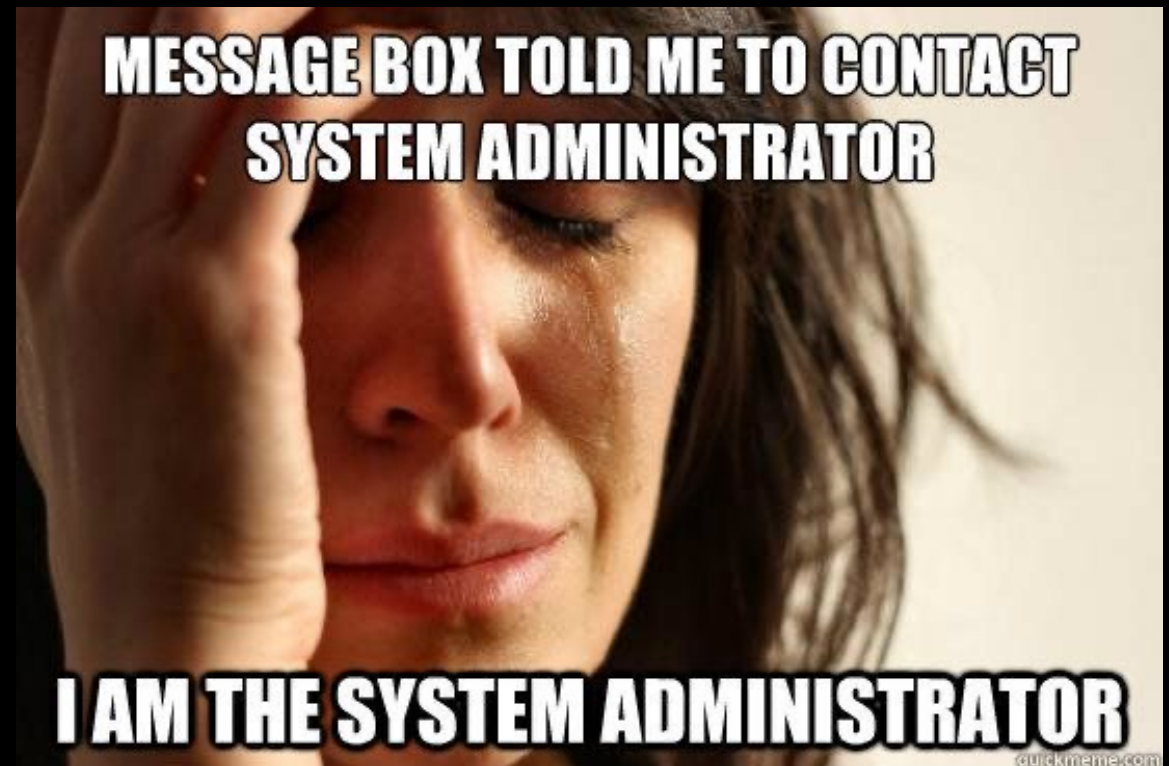
관리 권한의 막강함 - 서비스 중인 POD 삭제

Karpenter 변경 실수로 인한 노드 대량 교체 - live test가 수행됨

ip 부족 - 타이트한 subnet 관리

어제까지 수행되던 POD가 오늘부터 안됨

Node가 ready 상태로 안됨



# EKS 개선 : 십일번가 EKS

11 TechTalk 2023

타 팀과 업무 연계

권한 관리 및 보안 이슈

설정과 관리 복잡성

업무별 다양한 목적의 모니터링

효율적인 운영 비용

정기적인 EKS 업그레이드

부족한 subnet 대응

특화된 EKS 업무 절차

컨테이너 보안 정책 마련

정책 기반 운영 자동화

상용과 OSS를 활용한 모니터링 시스템

서비스 전용 노드 활용

EKS 업그레이드로부터 자유로운 시스템 마련

Secondary subnet 활용 방안 마련



OLD  
Architecture



New  
Architecture

# EKS 개선 : 클러스터 이중화(1/2)

11 TechTalk 2023

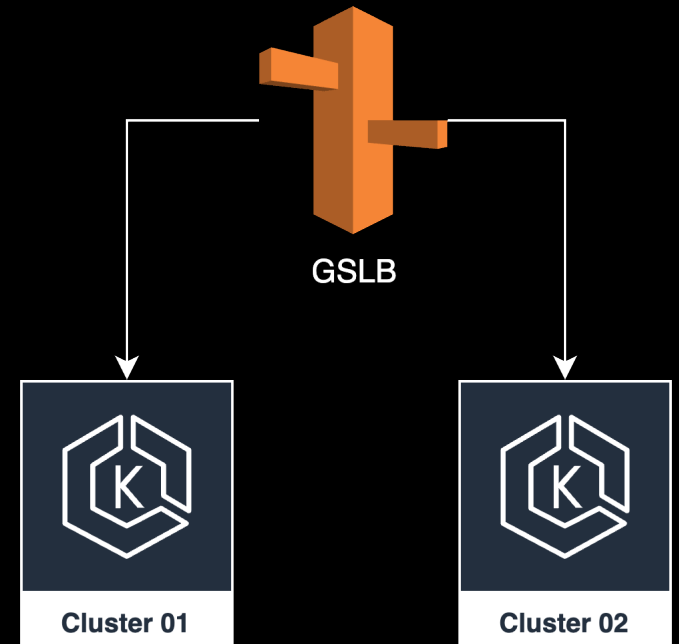
클러스터 이중화를 통한 문제 해결

이중화를 통한 새로운 확장 가능성을 가짐

운영 자동화를 통한 업무 변경

새로운 도전 과제도 함께 발생

- 서비스 네트워크 변경
- 합의된 업무 절차 변경
- 모니터링 방안 마련
- 운영 방침 변경
- 추가 비용 발생 억제



# EKS 개선 : 클러스터 이중화(2/2)

11 TechTalk 2023

**템플릿 기반** 구축할 수 있는 환경 구축

**협업** 가능한 **구조** 적용

운영 방침 변경 및 가이드 작성

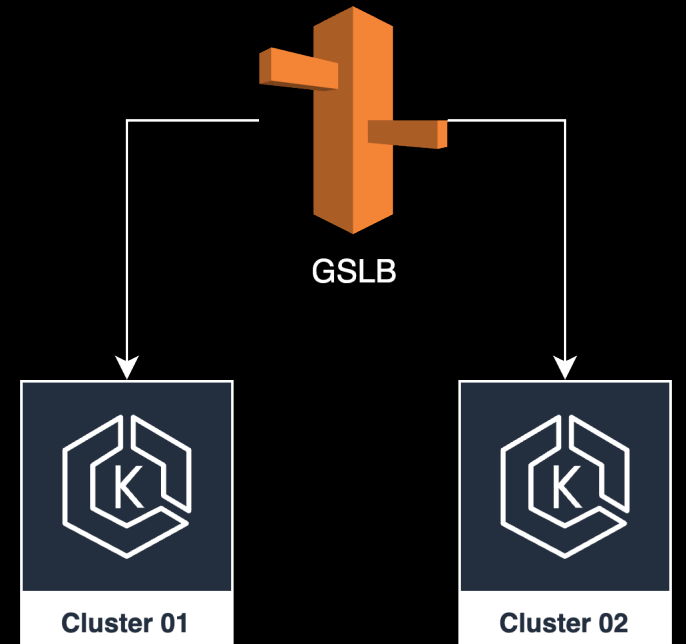
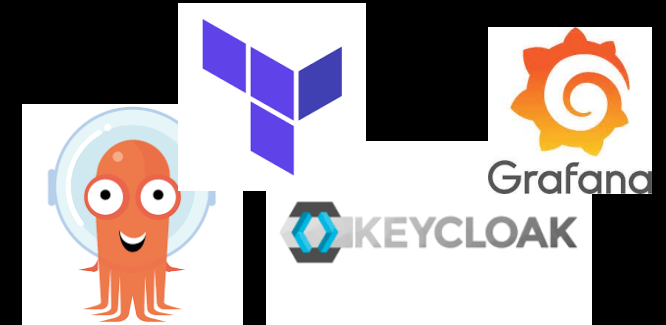
- 타 팀의 참여 환경 구축

**배포 시스템** 변경 : **업무 절차**는 유지

신기능은 새로운 업무 절차를 따름

통합 모니터링 시스템 방안 마련

- 각팀에서 사용중인 모니터링 솔루션 허용 및 연동 방안 마련



# EKS 개선 : 개선된 점

11 TechTalk 2023

EKS 업무 절차 마련 : **업무 절차 개선**

정책 기반 운영 자동화 : **운영 부담 감소**

보안 정책 적용 : **보안성 향상**

모니터링 시스템 지원 : **다양한 목적성 지원**

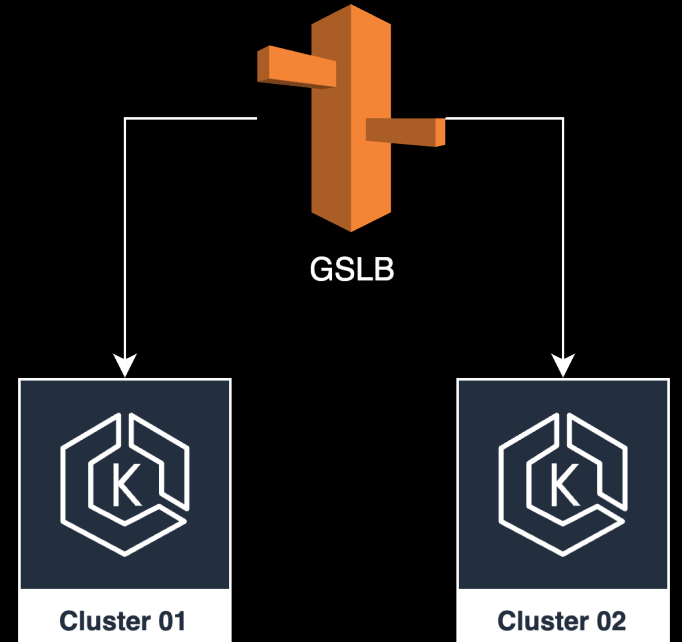
서비스 전용 노드 : **비용, 모니터링 향상**

업그레이드 시점 해방 : **원하는 시점에 업그레이드 가능**

EKS 수준의 서비스 이중화 : **서비스 안정성 확보**

트래픽 제어를 통한 서비스 제어 가능 : **다양한 옵션 제공**

새로운 가능성 제시 : **EKS 이외 k8s와 연동 가능성**





# 마무리

클러스터 이중화로 다양한 환경으로 발전 할 수 있는 환경을 구축함

클러스터 발전을 위한 구성원의 역량 발휘 및 발전

십일번가 특화된 통합 업무 시스템 구축

**안정적 서비스와 업무 효율성 증가 및 업무 시간 단축**

**Thank you**