

2024.11.25~2024.12.10  
2차 팀프로젝트

# Istio 기반의 Canary Deployment와 CI/CD 파이프라인 구현



팀명: EchoCloud  
팀장: 김선호  
팀원: 강대영, 김시내, 박다은

# LIST

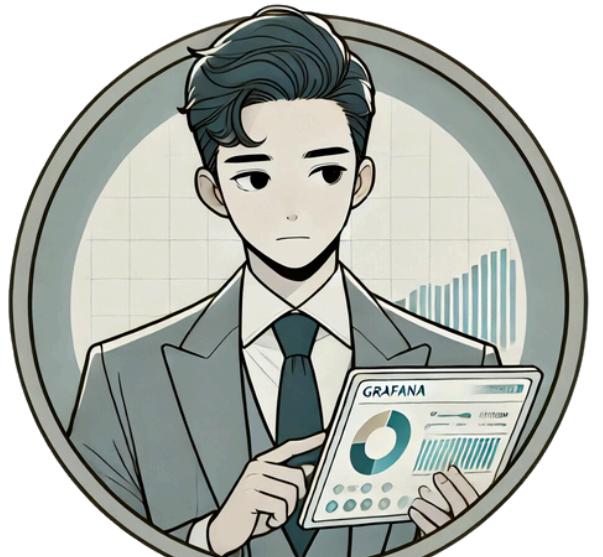
1. 팀 소개
2. 프로젝트 주제 및 선정 배경
3. 개발 환경
4. 기술 소개
5. 활용방안 및 기대효과

# 1. Team Info



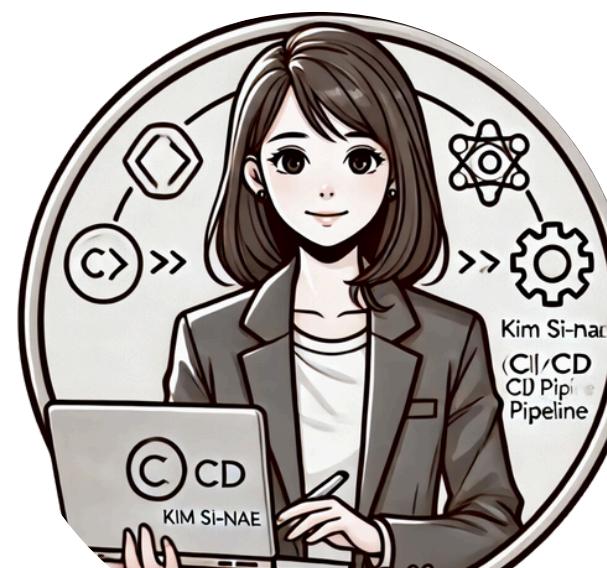
김선호

**Team Leader**  
**PM**  
**Istio**



강대영

**Team Member**  
**Grafana & Slack**  
**Multi-Master**



김시내

**Team Member**  
**CI/CD (SonarQube)**  
**Python**



박다은

**Team Member**  
**CI/CD (Harbor)**  
**Python**

# “EchoCloud”

## 2. 프로젝트 선정 배경

### 경기공유서비스 서비스 일시 중단 안내

경기공유서비스 메인화면 개편 및  
서비스 안정화 작업으로 인해 서비스 접속이  
일시 중단됩니다.  
이용에 불편을 끼쳐드려 죄송합니다.

보다 나은 서비스 제공을 위해  
항상 노력하겠습니다.



중단일시

2022년 8. 25.(목) 19시 ~ 24시

중단사유

메인화면 개편 및 서비스 안정화 작업

중단업부

경기공유서비스 전체

중단 시간은 작업 상황에 따라 변경될 수 있습니다.

매출 손실

서비스 복구  
비용 증가

신뢰도 하락

## 2. 프로젝트 소개

### 무중단 배포

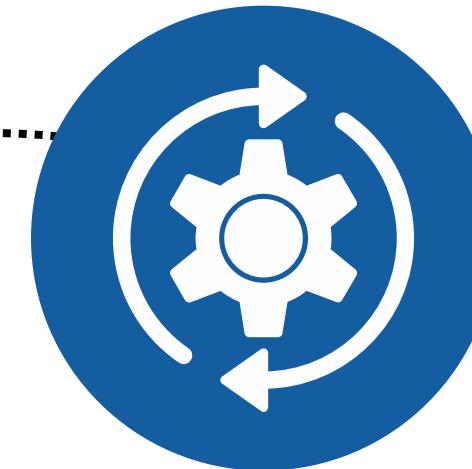
서비스 중단 없는 신뢰있  
고 안정적인 Canary  
Deployment

“환경 구축”

## 2. 프로젝트 목표

### 실시간 알림

문제 해결 자동화 및 실시간 Slack 알림 연동



### 자동화

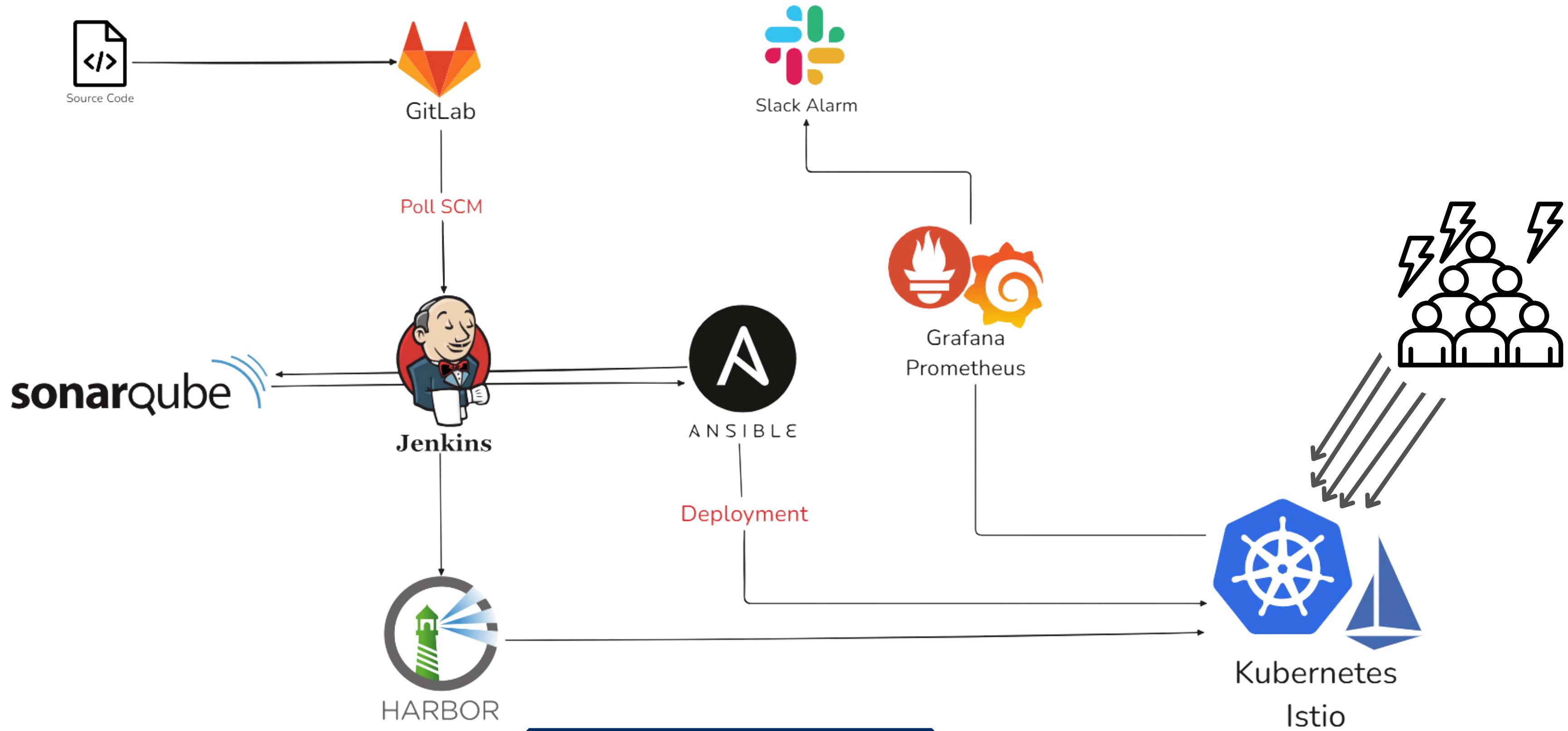
CI/CD 자동화를 통해 효율적인 배포와 관리체계 확립



### 무중단 배포

Istio의 트래픽 라우팅으로 무중단배포 구현  
배포 신뢰성 향상

# 3. Architecture



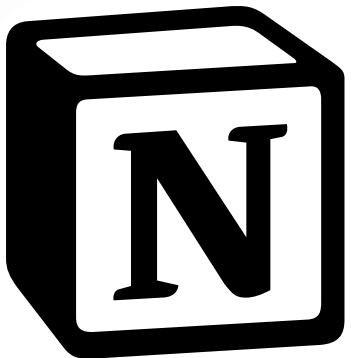
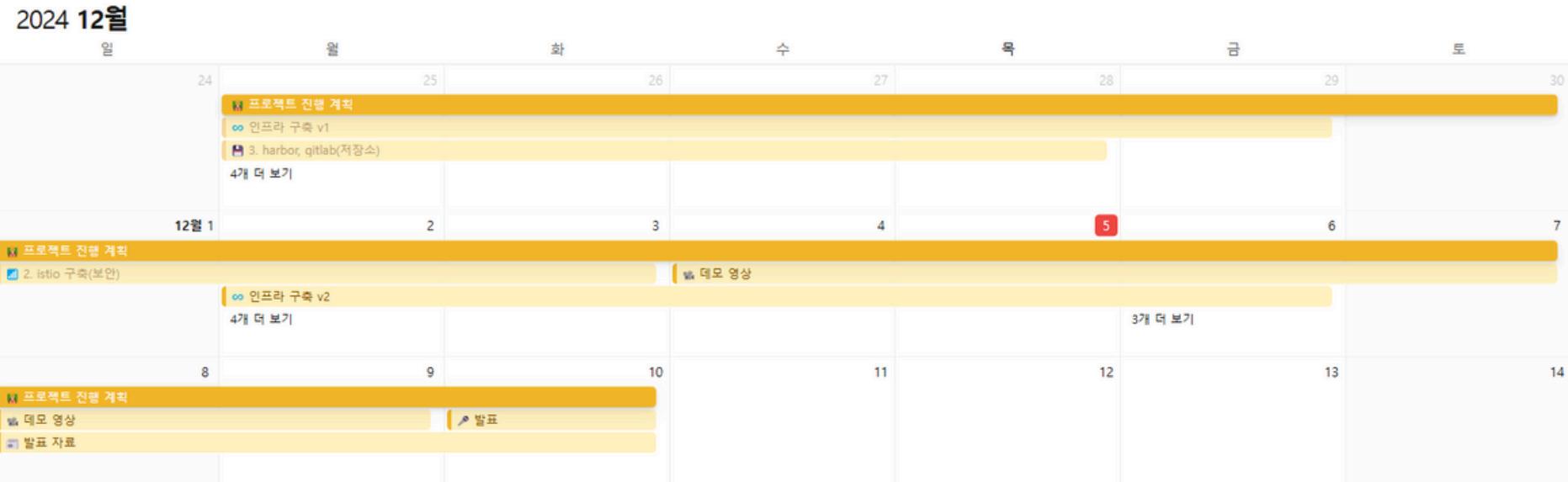
### 3. 개발 환경

## Bridge 네트워크를 통한 효율적인 리소스 관리

추가적인 네트워크 리소스가 필요할 때 손쉽게 확장 가능

	MASTER	WORKER	JENKINS	HARBOR	GITLAB	DEV
RAM	8 GB			4 GB		
CPU	8			4		
DISK	80 GB			40 GB		
IMAGE	ubuntu 22.04					

# 3. 협업 도구



KAKAO TALK

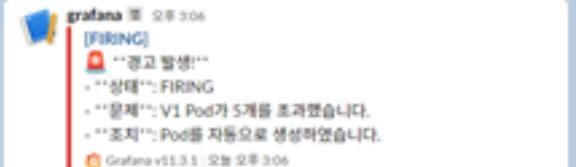
김선호 10.8.0.151 오후 12:26

강대영 istio-ingressgateway.istio-system.svc.cluster.local

<https://echocloud-09628b3db6d1.herokuapp.com/>

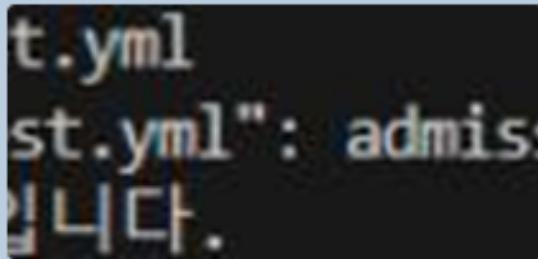
김선호 mysql.default.svc.cluster.local 오후 1:5

강대영





김선호



김시내 https://10.10.100.110/harbor/projects/3/repositories/harbor 오후 7:30

## 4. 기술 소개

**Multi-Master & LoadBalancer**

**CI/CD Harbor/SonarQube**

**Istio**

**Grafana & Slack**

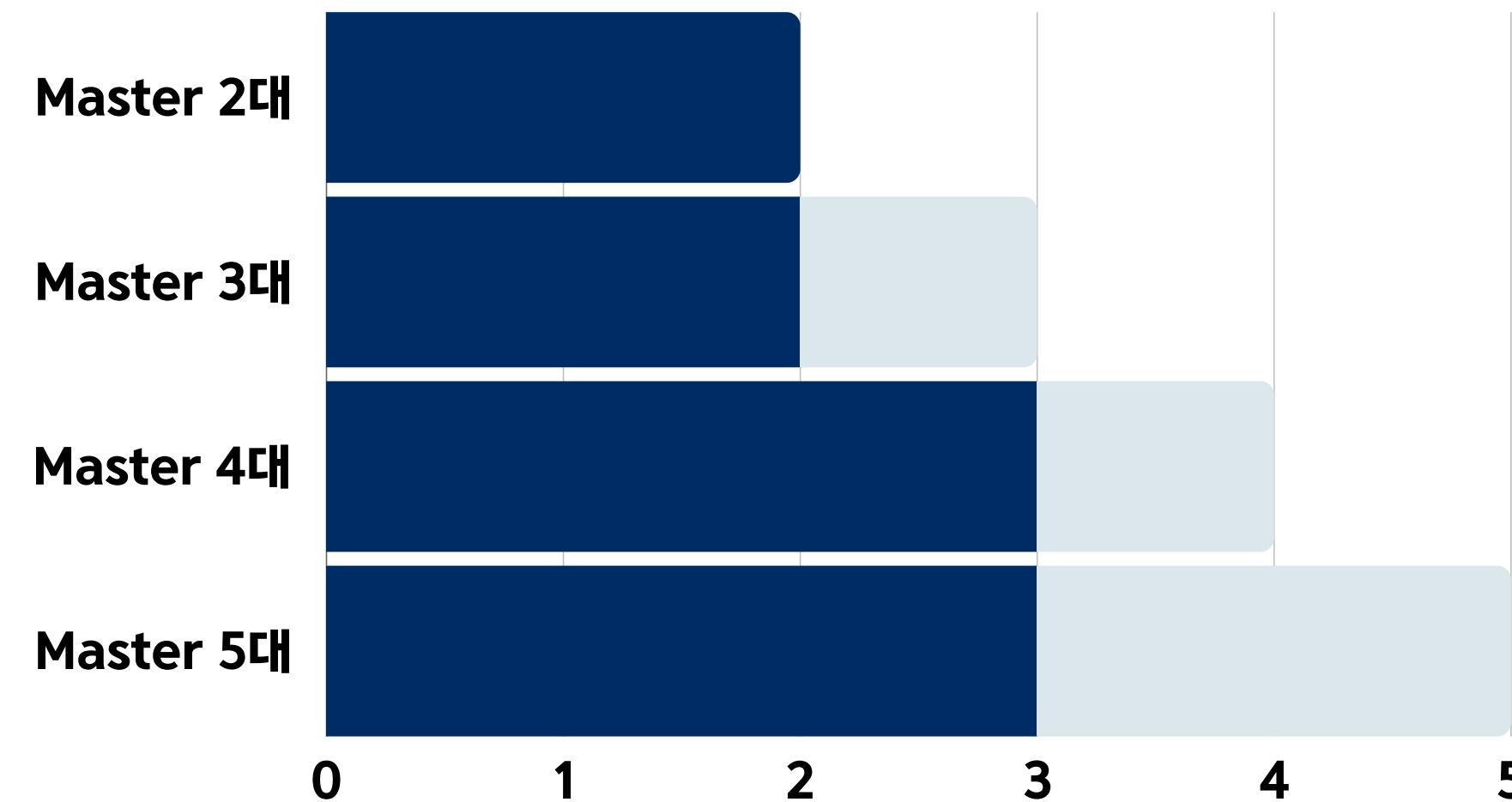
# 4. Multi-Master

## Multi-Master Cluster Down 방지

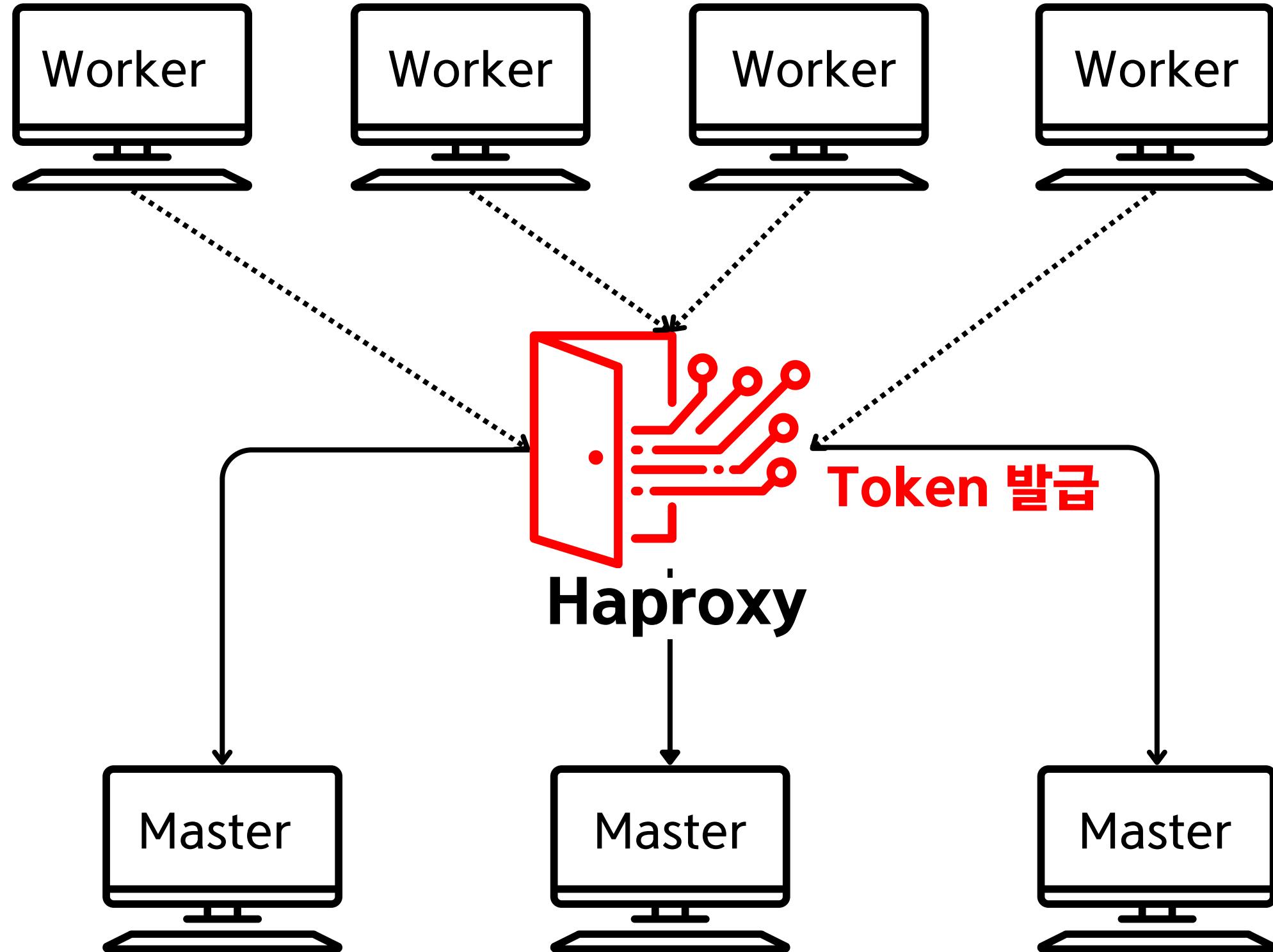
### 3대의 Master Node Quorum(정족수)를 고려하여 3대로 구성

## Quorum(정족수)

분산 시스템에서 다수결의 원칙에 따라 의사결정을 할 때,  
**동의해야 하는 최소한의 노드 수**



# 4. Load Balancer & Multi-Master



## Health Check

down 된 master에게 불필요한  
트래픽 전송 방지

## 부하분산

요청을 균등하게 분배해  
클러스터 제어 성능 최적화

# 4. Gitlab+Jenkins, Ansible

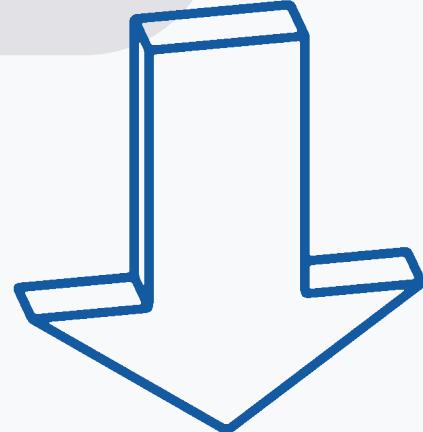
유연한 플러그인 기반 CI 자동화 도구로,  
빌드와 테스트 프로세스를 간단히 설정 가능



Jenkins

JenkinsFile

코드 저장소와 이슈 추적, 협업 기능을  
통합적으로 제공하여 팀 생산성을 높임



에이전트리스 방식의 간단하고 강력한 CD 도구  
서버 구성 및 배포를 효율적으로 처리.

Playbook

# 4. Repository

The screenshot shows the Harbor UI interface. On the left, there's a sidebar titled 'Administration' with options like 'Users', 'Robot Accounts', 'Registries', 'Replications', 'Distributions', and 'Labels'. The main area has a navigation bar with tabs: 'Summary', 'Repositories', 'Members', 'Labels', 'Scanner', 'P2P Preheat', 'Policy', 'Robot Accounts', 'Webhooks', 'Logs' (which is currently selected), and 'Configuration'. Below the navigation is a table with columns: 'Username', 'Resource', 'Resource Type', 'Operation', and 'Timestamp'. The table contains two rows: one for 'admin' creating a 'test/harbor:blue' artifact and another for 'admin' creating a 'test' project. A large white lighthouse icon is centered above the table.

Username	Resource	Resource Type	Operation	Timestamp
admin	test/harbor:blue	artifact	create	11/21/24,
admin	test	project	create	11/21/24,

# Harbor

## 컨테이너 이미지 저장소

관리 편의

- 프로젝트별로 이미지 저장소 구분

비용 절감

- 오픈소스
- 저장 공간 및 요청 횟수에 제한 X

보안 강화

- CA 인증서를 지원해 데이터 암호화

RBAC

- 역할 기반 접근 제어(RBAC)로 사용자 권한을 세밀하게 관리

# 4. sonarQube

The screenshot shows the SonarQube interface for a project named 'echoCloud' in the 'main' branch. The top navigation bar includes 'Overview', 'Issues', 'Security Hotspots', 'Measures', 'Code', and 'Activity'. A prominent red box on the left indicates a 'Failed' status with '2 conditions failed'. Below this, under 'MEASURES', it shows 'New Code' coverage at 0.0% and 'Overall Code' coverage at 0.0%. It also lists 12 bugs, 0 vulnerabilities, 18 security hotspots, and a duration of 1h 25min. A detailed view of the 'hello.py' file shows several code smells and errors:

```
# 오류 2: 끝없는 변수 사용 (변수 이름 오류)
area = 3.14 * radius**2 # 'radius'의 오류가 있음: 'radius'로 잘못 썼음.

# 오류 3: 미사용 변수 선언
unused_variable = "I am never used"

❸ Remove the unused local variable "unused_variable".

return area

❹ def divide_numbers(a, b):
❺     # 오류 4: ZeroDivisionError
❻     result = a / b # b가 0이면 ZeroDivisionError 발생

❾     # 오류 5: 잘못된 문자 비교
❿     if isinstance(a, str) and isinstance(b, str): # 숫자 비교가 아님 문자열 비교
```



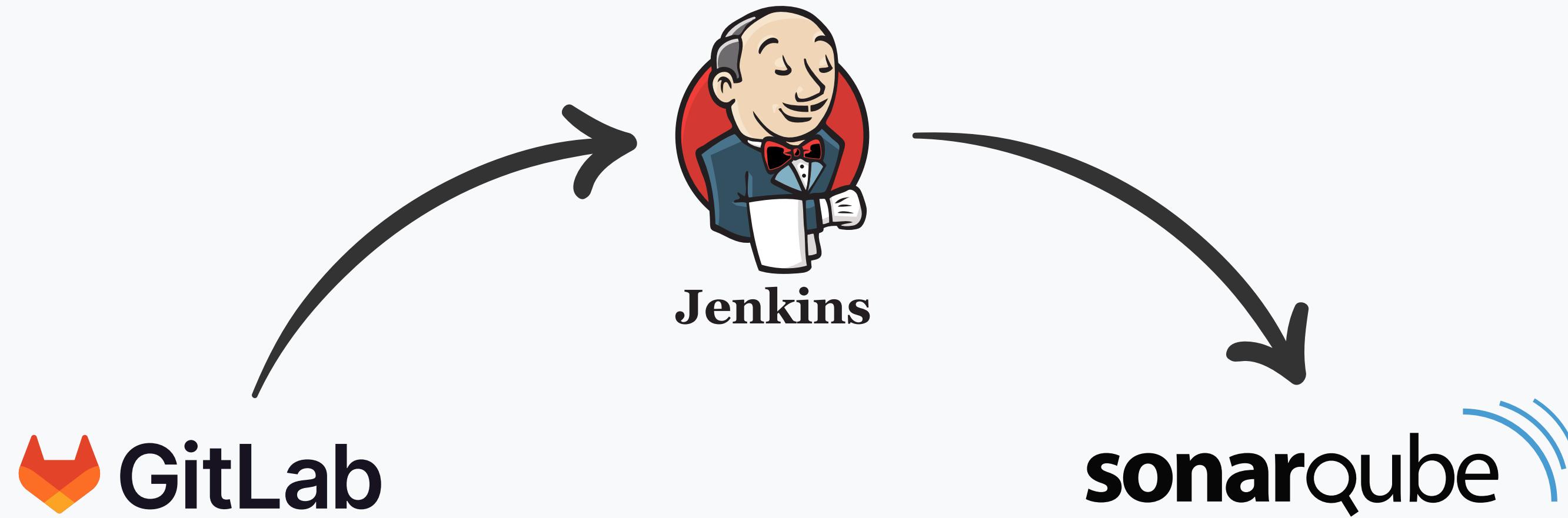
## 코드 품질 관리 및 정적 분석 도구

### # 정적 코드 분석

### # 코드 스멜

### # 품질 게이트

## 4. sonarQube + Jenkins



SonarQube는 Jenkins의 workspace를 스캔해,  
Git에서 가져온 코드를 분석

# 4. Python + Django



# Python과 Django 프레임워크 기반 프로젝트를  
SonarQube로 정적 분석하여 코드 품질 평가

# 4. Istio

사용 기업



Istio는 서비스 메쉬(Service Mesh)를 구현하는 오픈소스 플랫폼으로,  
Kubernetes 클러스터에서 애플리케이션의 서비스 간 통신을 관리



트래픽 관리



보안



가시성



서비스 정책 대응



확장성



비바리퍼블리카

HYPERCONNECT

하이퍼커넥트

ABLEY

에이블리

DEVSISTERS

데브시스터즈

Bagelcode

베이글코드

kakaostyle

카카오스타일

Gmarket

지마켓

SK텔레콤

두들린

Greeting

퀀타랩

ABLEY

에이블리

DEVSISTERS

데브시스터즈

Bagelcode

베이글코드

kakaostyle

카카오스타일

Gmarket

지마켓

SK텔레콤

두들린

RAPPORT LABS

라포랩스

FACIAL COMMERCE

엔에이치엔커머스

CJ

두들린

퀀타랩

카리스쉐어테크

카카오화재

카카오뱅크

# 4. Envoy Proxy

Envoy  
Proxy

Application

NAME	READY	STATUS	RESTARTS	AGE
v1-dp-6fc7fb4bbd-ftqhb	2/2	Running	0	53s
v2-dp-5b9d68864d-srmsb	2/2	Running	0	53s

# Pod 배포시 자동으로 SideCar 생성

# 로드 밸런싱

# 장애 복구 효율적

# 트래픽 라우팅

# TLS 암호화

# 데이터 전송 암호화

# 4. CANARY UPDATE



소수 배포로 문제  
발생 시 영향 최소화

리스크 최소화



일부 배포로 실시간  
피드백과 문제 해결

빠른 피드백



점진적 트래픽 증가  
로 안정성 보장

안정성

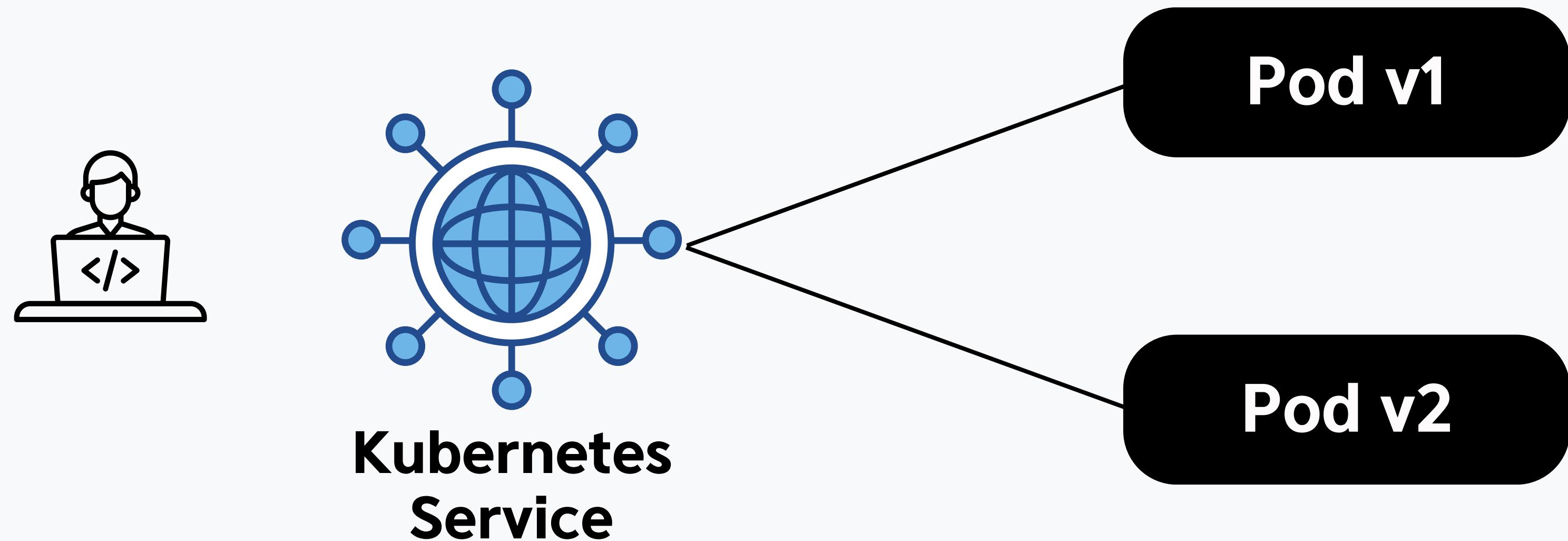


Istio와  
Kubernetes로 배포  
전략 구현 용이

유연성

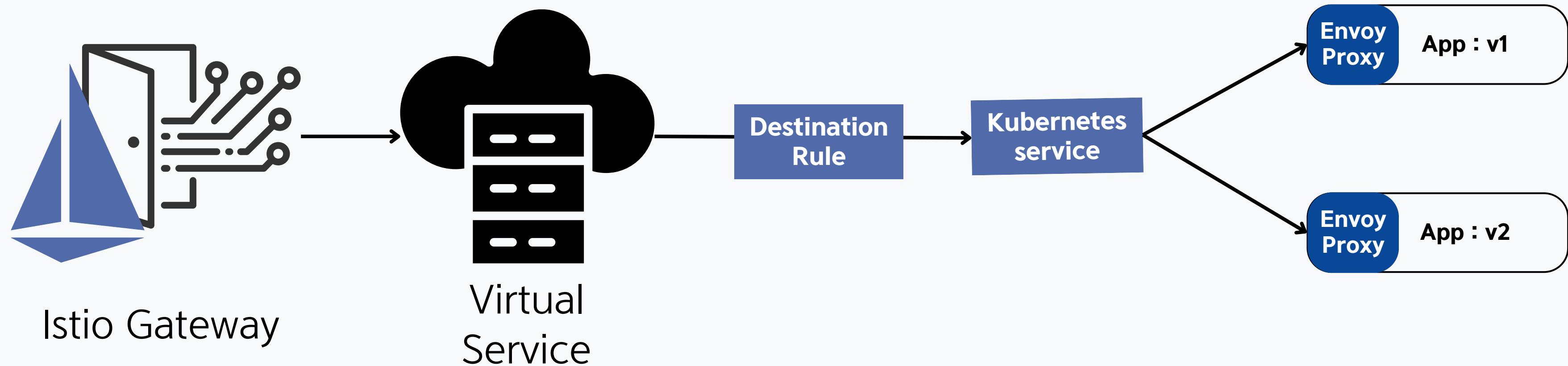
## 4. 기존 버전의 서비스

### 기존 배포



# 4. 새로운 버전의 서비스

## Istio를 이용한 배포



# 4. 새로운 버전의 서비스

```
apiVersion: networking.istio.io/v1beta1
kind: Gateway
metadata:
  name: canary-gateway
spec:
  selector:
    istio: ingressgateway
  servers:
    - port:
        number: 80
        name: http
        protocol: HTTP
      hosts:
        - "*"
        apiVersion: networking.istio.io/v1beta1
        kind: VirtualService
        metadata:
          name: canary-virtualservice
        spec:
          hosts:
            - "*"
          gateways:
            - canary-gateway
          http:
            - match:
                - headers:
                    x-forwarded-for:
                      exact: "10.5.6.2" # 특정 IP를 v2로 라우팅
                - headers:
                    x-forwarded-for:
                      exact: "10.5.6.10" # 특정 IP를 v2로 라우팅
                - headers:
                    x-forwarded-for:
                      exact: "10.5.6.11" # 특정 IP를 v2로 라우팅
              route:
                - destination:
                    host: canary-svc
                    subset: v2
                - route:
                    - destination:
                        host: canary-svc
                        subset: v1
            apiVersion: networking.istio.io/v1beta1
            kind: DestinationRule
            metadata:
              name: canary-destinationrule
            spec:
              host: canary-svc # svc에서 설정했던 name
              subsets:
                - name: v1
                  labels:
                    ver: v1
                - name: v2
                  labels:
                    ver: v2
```

```
apiVersion: v1
kind: Service
metadata:
  name: canary-svc
  labels:
    service: canary
apiVersion: apps/v1
kind: Deployment
metadata:
  name: v1-dp
spec:
  replicas: 1
  selector:
    matchLabels:
      app: canary
      ver: v1
  template:
    metadata:
      labels:
        app: canary
        ver: v1
```

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: v2-dp
spec:
  replicas: 1
  selector:
    matchLabels:
      app: canary
      ver: v2
  template:
    metadata:
      labels:
        app: canary
        ver: v2
```

```
root@Master3:~# k get svc istio-ingressgateway -n istio-system -o yaml | grep externalTrafficPolicy
externalTrafficPolicy: Local
```

# 4. 새로운 버전의 서비스

## Canary 배포

Menu  
ECHO CLOUD  
Welcome, test100 [Log out](#)

**GO! TEAM ECHO CLOUD!!**

Explore the innovative solutions provided by our team at EchoCloud.  
Stay connected and empowered.

- [Get Started](#)

**Innovative Solutions**

Experience cutting-edge technology and expertise to help you grow.

**Reliable Team**

Trust in our dedicated team to provide unparalleled support and service.



**Future Ready**

Prepare for the challenges of tomorrow with solutions designed for today.

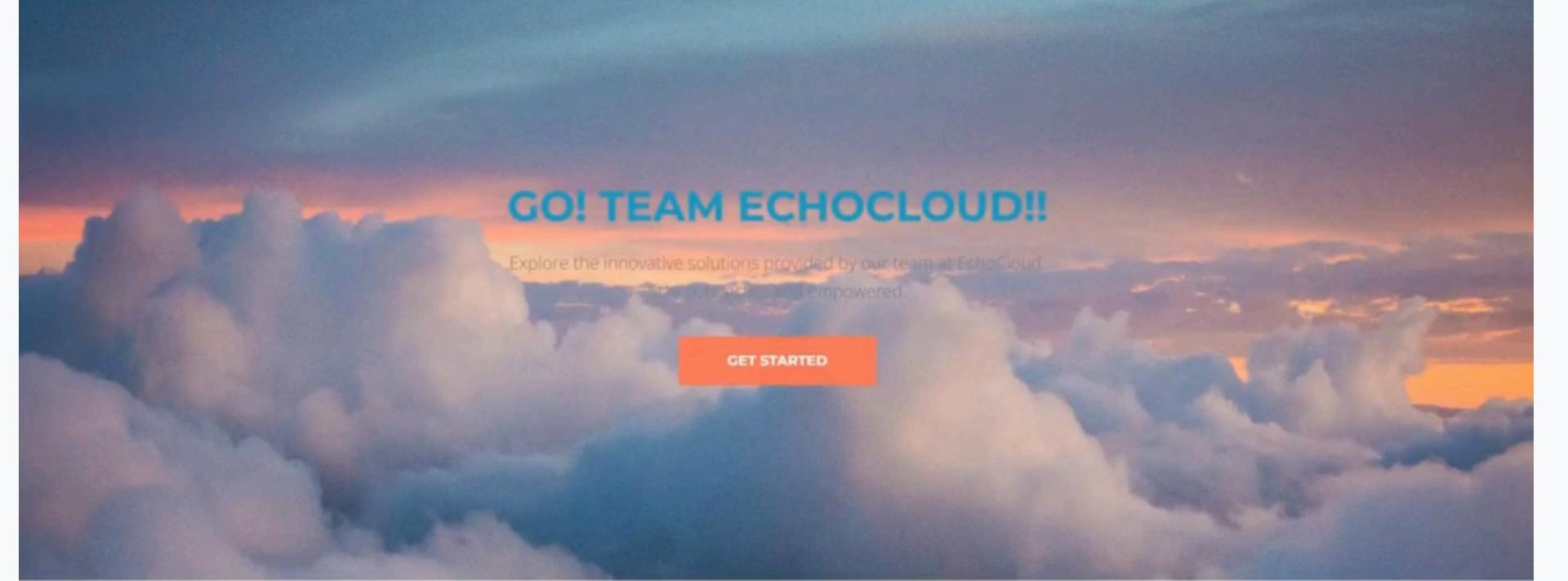
**v1**

ECHO CLOUD

**GO! TEAM ECHO CLOUD!!**

Explore the innovative solutions provided by our team at EchoCloud.  
Stay connected and empowered.

[GET STARTED](#)



**v2 – 정상 페이지**

10.8.0.151



# 4. Monitoring(Grafana)



# 4. Monitoring(Slack Alert)

## Settings

### Basic Information

Collaborators  
Socket Mode  
Install App  
Manage Distribution

### Features

App Home  
Agents & Assistants...  
Workflow Steps NEW  
Org Level Apps  
Incoming Webhooks  
Interactivity & Short...  
Slash Commands  
Steps from Apps LEGACY

### OAuth & Permissions

### Event Subscriptions

### User ID Translation

### App Manifest

### Beta Features

### Submit to Slack Marketplace

### Review & Submit

## App Credentials

These credentials allow your app to access the Slack API. They are secret. Please don't share your app credentials with anyone, include them in public code repositories, or store them in insecure ways.

### App ID

A082Y95F36U

### Date of App Creation

November 24, 2024

### Client ID

8070895776614.8100311513232

### Client Secret

ce5531704a920516b7202722d8f91e09

Show

Regenerate

You'll need to send this secret along with your client ID when making your `oauth.v2.access` request.

### Signing Secret

b3b5fe2360296f574bb88b5f422ce3ab

Show

Regenerate

Slack signs the requests we send you using this secret. Confirm that each request comes from Slack by verifying its unique signature.

### Verification Token

iry9lqhM1FVwDmndvi883FGj

Regenerate

This deprecated Verification Token can still be used to verify that requests come from Slack, but we strongly recommend using the above, more secure, signing secret instead.

# Slack에서 API를 위한 토큰 발급

A Prometheus Metrics browser > count(kube\_pod\_info{namespace="default", pod=~"v1-dp-.\*"}) Options ▾ 10 minutes, MD = 43200, Min. Interval = 1s Set as alert condition

Kick start your query Explain

Add query

Rule type Select where the alert rule will be managed. Need help?

Grafana-managed Data source-managed

The alert rule type cannot be changed for an existing rule.

Expressions Manipulate data returned from queries with math and other operations.

C Threshold  Alert condition

Takes one or more time series returned from a query or an expression and checks if any of the series match the threshold condition.

Input B  IS ABOVE  5  Custom recovery threshold

B Reduce

Takes one or more time series returned from a query and reduces them using a specified function.

Input A  Function Max

# Grafana에서 Alert 설정

# 4. Monitoring(Slack Alert)

grafana 앱 오후 3:06

[FIRING]

🚨 \*\*경고 발생!\*\*

- \*\*상태\*\*: FIRING
- \*\*문제\*\*: V1 Pod가 5개를 초과했습니다.
- \*\*조치\*\*: Pod를 자동으로 생성하였습니다.

Grafana v11.3.1 | 오늘 오후 3:06

---

grafana 앱 오후 3:21

[RESOLVED]

✓ \*\*경고 해결!\*\*

- \*\*상태\*\*: RESOLVED
- \*\*설명\*\*: 안정되어 V1 Pod 개수가 정상 값으로 복구되었습니다.

Grafana v11.3.1 | 오늘 오후 3:21

# Slack에서 alarm 확인

# 5. 활용 방안 및 기대 효과

## 보안 강화

Harbor로 배포 보안성 향상  
Istio로 서비스 간 통신 보호

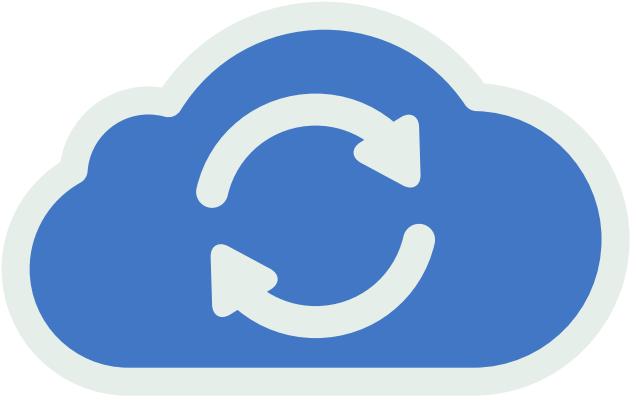
## 운영의 효율성

CI/CD 자동화로 배포 시간 단축  
소나큐브를 사용해 개발자 코드  
유효성 검사

## 배포 신뢰성 향상

Canary update로  
배포의 신뢰성 향상

## 5. 보완점



### 추가하고 싶은 점

#### VPN

#### Istio

#### DataBase

OpenVPN을 이용한  
외부 네트워크 차단

Gatekeeper를 이용해  
보안성 쟁기기

한 개의 Pod가 아닌  
DB Pod를 두고 PVC를 통해  
데이터 유지하기

# Q & A

2024.11.25~2024.12.10

2차 팀프로젝트

Thank You

ECHO CLOUD