

NAVER CLOUD PLATFORM X HASHICORP

네이버 클라우드 플랫폼
DevSecOps X MultiCloud
하시코프 Consul

네이버 클라우드 플랫폼 테크 에반젤리스트 | 송 창 안
하시코프 시니어 솔루션즈 엔지니어 | 이 규 석



2021.04.07

Contents

네이버 클라우드 플랫폼 DevSecOps 구현 하기

네이버 클라우드 플랫폼 소개

DevSecOps 이란?

DevSecOps 서비스 소개

네이버 클라우드 플랫폼 Kubernetes Service 소개

네이버 클라우드 플랫폼에서 DevSecOps를 이용하여 서비스 배포 하기

Contents

네이버 클라우드 플랫폼과 멀티 클라우드 서비스 연결

하시코프 소개

네이버 클라우드 플랫폼과 하시코프의 멀티 클라우드 전략

Consul - 서비스 잇기

Consul - Service Mesh

Consul Federation Demo : NCP - GCP

네이버 클라우드 플랫폼 소개



NAVER CLOUD PLATFORM

매출, 상품 수, 고객 규모 모두 매년 2배 이상 성장하며
가장 빠르게 발전하는 NAVER Cloud의 퍼블릭 클라우드 서비스입니다.

네이버 클라우드 플랫폼 서비스맵



Compute

탄탄한 인프라와 오랜 운영 경험에 기반한
최상의 컴퓨팅 자원 제공



Network

언제 어디서나 빠르고 안정적인 네트워크 환
경으로 막힘 없는 서비스 구현



Security

세계적 수준의 보안 기술로 외부
위협으로부터 서비스를 안전하게 보호



Management

인프라와 서비스를 실시간 모니터링 및 관
리하여 안정적인 서비스 제공



Business Application

성장하는 기업을 위한 클라우드 기반 기업
정보 시스템 및 협업툴 제공



Media

쉽고 빠르게 고품질의 미디어 콘텐츠 변환
및 서비스 플랫폼 구축 가능



Game

게임 서비스를 위한 SDK 제공 및
다양한 필수 부가 서비스 연동 지원



Hybrid & Private Cloud

기업의 필요에 맞춰 다양한 형태의하이브
리드 클라우드 환경 제공



Database

서비스 특성에 맞는 다양한 데이터 플랫폼
제공, 관계형, NoSQL, 캐시 등



Global

전 세계 주요 거점에 구축한 안정적 인프라를
통해 글로벌 서비스 지원



Analytics

서비스 및 시스템 데이터의 효과적인수집
및 통합 분석 서비스 제공



Storage

안전하고 유연한 스토리지 상품 제공,아카
이빙, 객체 스토리지, 백업 등



AI Service

네이버의 풍부한 데이터를 기반으로 학습
된 경쟁력 있는 AI 서비스 활용 가능



Application Service

지도부터 캡차까지 네이버의 기술과서비
스를 손쉽게 사용할 수 있도록 제공



IoT

수백만 대의 디바이스와 클라우드를연결
하여 쉽고 안전한 인사이트 확보



Dev Tools

DevOps를 적용하여 신속하고 안전하게
S/W 개발 환경 구축 및 배포



Blockchain

프라이빗 블록체인에서 블록체인 기반 서
비스까지 클라우드에 구현

네이버 클라우드 플랫폼 장점

네이버의 기술과 노하우가
집약된 기술 플랫폼

기업의 성장과 각 산업에
맞는 상품, 솔루션 제시

24시간 365일 고객 지원
및 친근한 인터페이스

세계적으로 인정받은
엄격한 보안 기술력

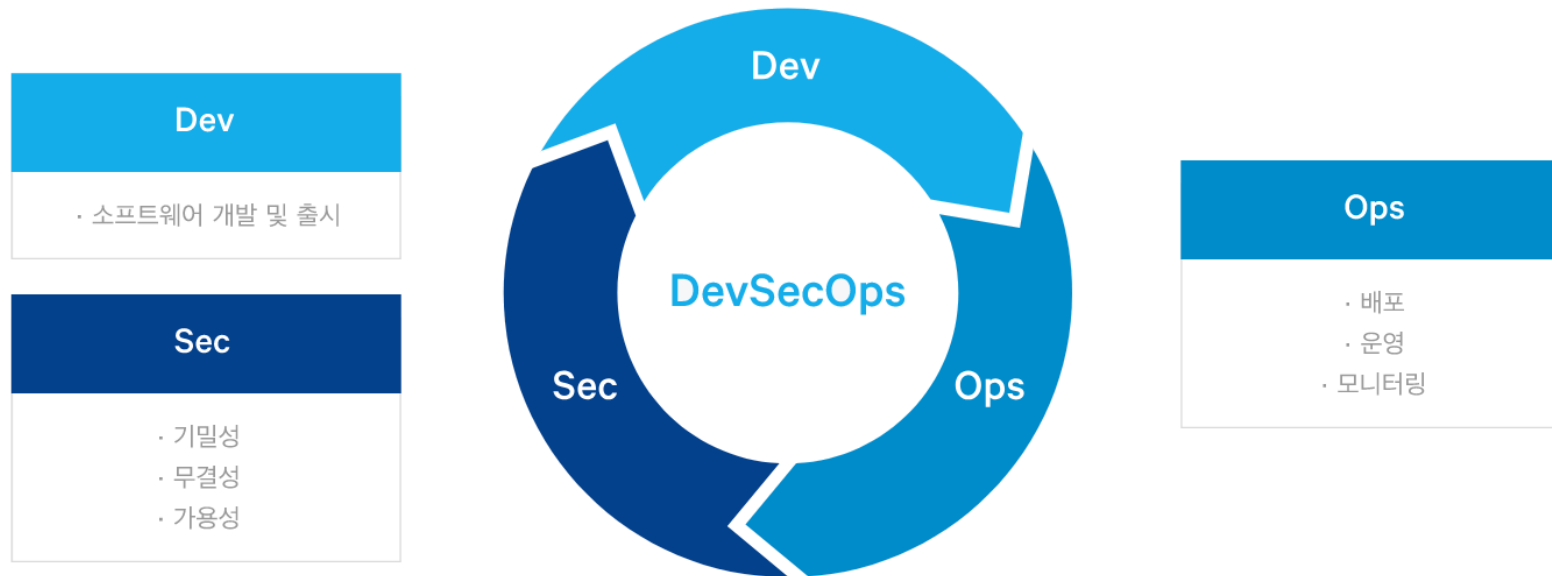
자체 데이터센터
및 글로벌 리전 보유

DevSecOps 이란?

DevSecOps 이란?

데브섹옵스(DevSecOps) 이란?

“데브섹옵스(DevSecOps)는 개발, 보안, 운영을 위한 줄임말이라고 간단하게 정의”

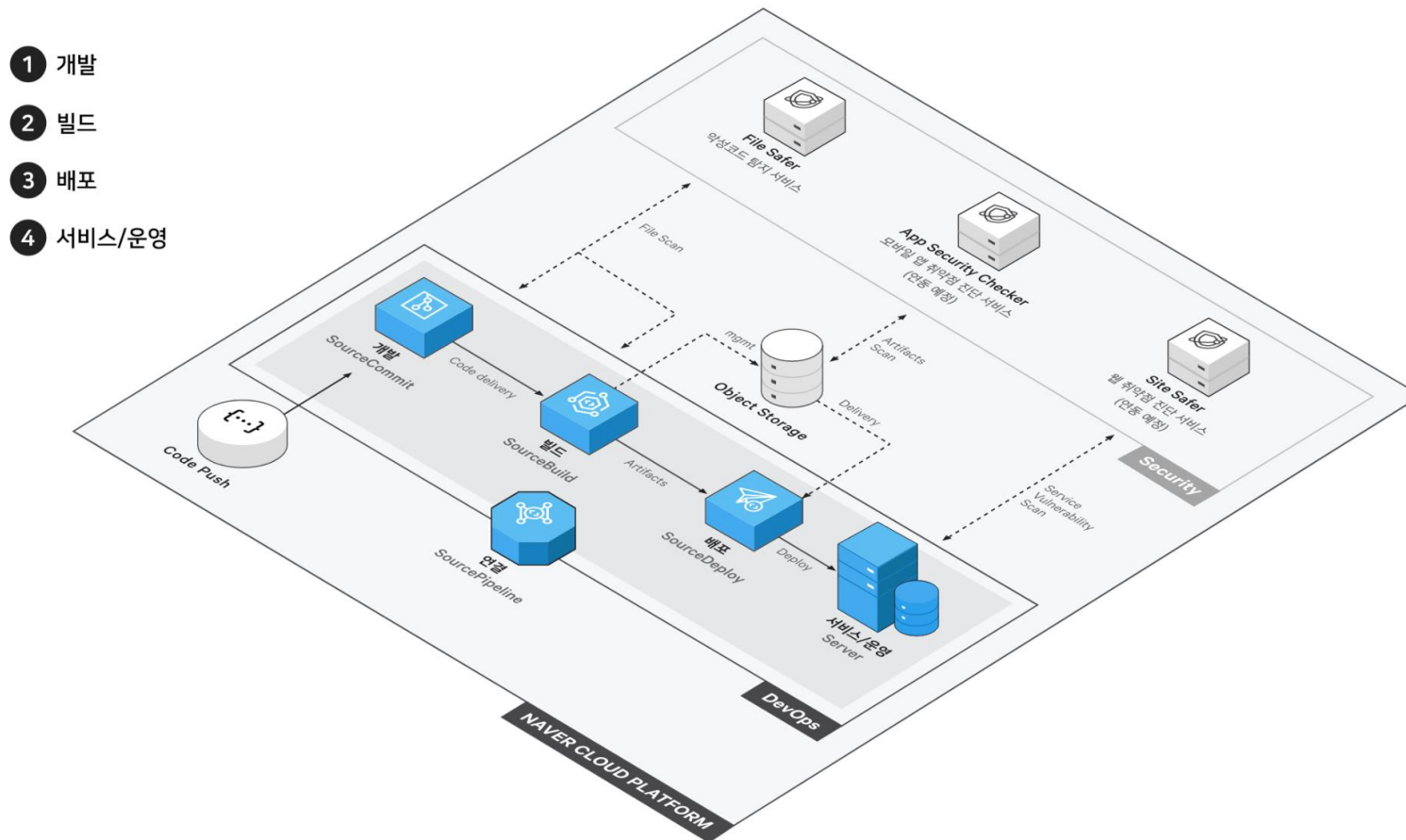


설계부터 개발, 테스트, 생산 및 운영까지의 어플리케이션 라이프 사이클 전반에 보안을 통합

네이버 클라우드 플랫폼의 Dev Tools

안정성과 유연성과 보안성을 갖춘 개발 환경

- ✓ DevOps 의 SourceCommit, SourceBuild, SourceDeploy, SourcePipeline 상품을 제공하여 개발 편의성을 향상
- ✓ DevOps의 각 단계별로 Security 상품들 과의 연동을 통해서 보안을 고려한 서비스 개발 흐름을 설계 및 적용 할 수 있어 매우 효과적



DevSecOps 서비스 소개

DevSecOps tool 소개

Dev Tools



Jenkins



SourceBuild



SourceCommit



SourceDeploy



SourcePipeline

Security



App Safer



App Security
Checker



File Safer



Site Safer



System Security
Checker



Web Security
Checker

SourceCommit 서비스 소개

SourceCommit (소스커밋 서비스)

높은 성능과 뛰어난 확장성

- ✓ 고성능 인프라 및 이중화 아키텍처를 제공 및 대용량 저장소를 사용 가능
- ✓ 저장소에는 소스코드뿐 아니라 모든 파일 형태를 안전하게 저장 가능

편리한 사용

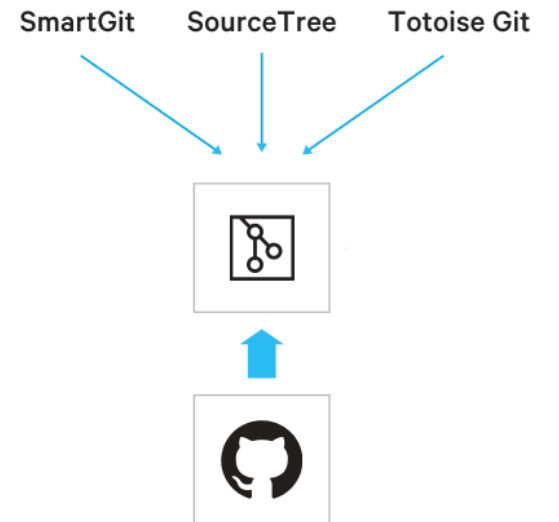
- ✓ 외부에서 사용하던 Git 저장소는 URL만 입력하면 손쉽게 가져올 수 있음.
- ✓ 기존 저장소를 그대로 사용하기 위해 필요한 복잡한 과정을 소스커밋 서비스에서는 자동으로 수행

모든 Git 클라이언트 사용

- 모든 GIT 명령어를 지원하므로, 기존에 사용하던 모든 Git 클라이언트와 연동 가능
- 기존 개발 환경과 동일한 환경에서 편리하고 안전하게 저장소를 사용

보안성 강화

- ✓ 로컬 클라이언트와 통신할 때 HTTPS 프로토콜을 사용해 파일을 안전하게 전송
- ✓ 범용적인 Git 클라이언트를 통해 소스커밋에 접근하기 위해서는 클라이언트 전용 비밀번호를 사용
- ✓ 이러한 보안 장치를 통해 안전하지 않은 클라이언트에 의한 계정 유출 사고를 방지 가능



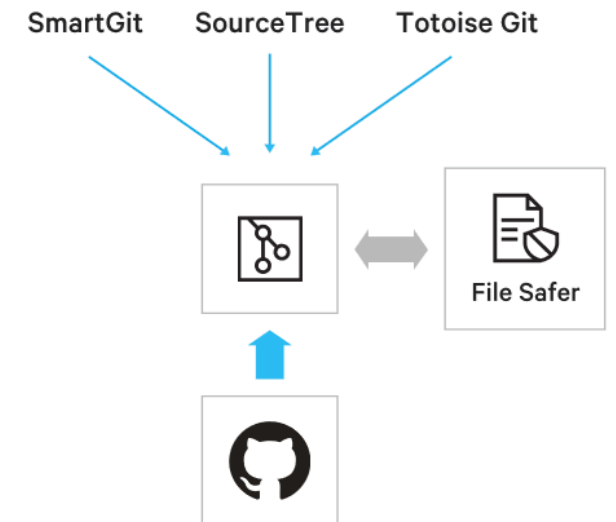
SourceCommit (소스커밋 서비스)

편리한 보안 검사

- ✓ 파일 세이퍼 (File Safer) 서비스와 연동해, 소스커밋 서비스에 업로드하는 다양한 파일의 악성코드 감염 여부를 쉽고 빠르게 확인 가능
- ✓ 저장소에 존재하는 스크립트 및 바이너리 파일의 악성 여부도 확인 가능

파일 세이퍼 연계를 통한 보안 강화

- ✓ 코드 커밋 성공 시, 자동으로 결과물을 파일 세이퍼에 검사를 요청
- ✓ 빌드 결과물에 대한 악성 여부를 확인



SourceBuild 서비스 소개

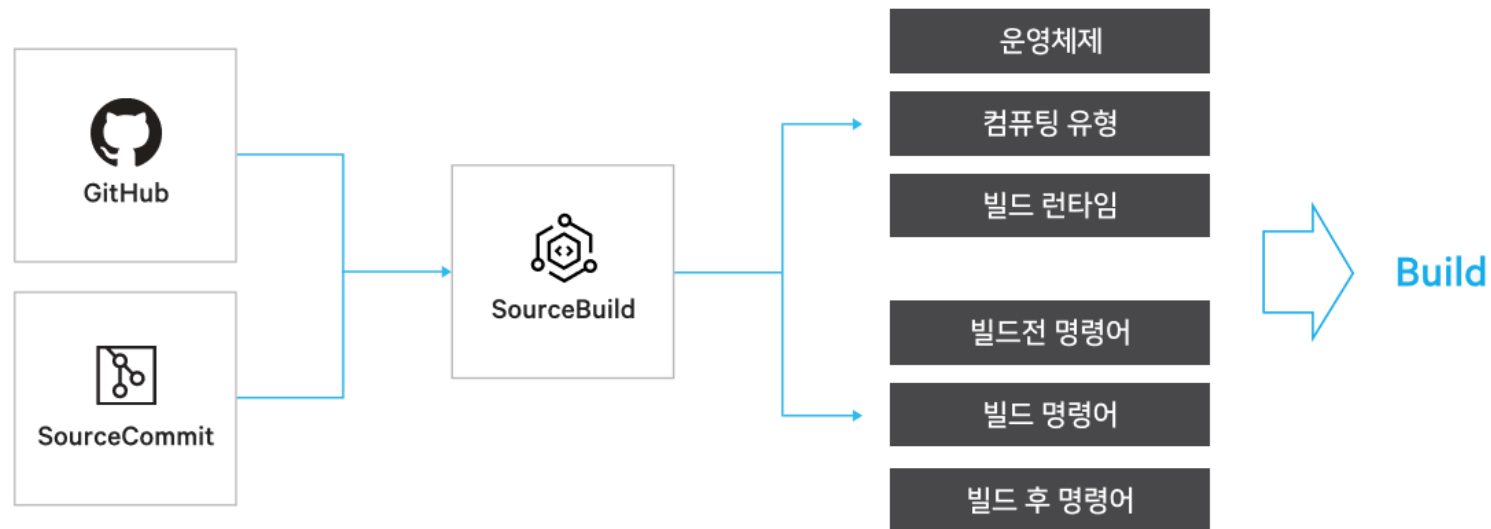
SourceBuild (소스빌드 서비스)

빠른 프로비저닝

- 자체 빌드 서버를 운영할 필요 없이 빌드 작업을 요청하면 빌드 서버가 빠르게 프로비저닝을 제공
- 매번 빌드 작업을 할 때마다 동일한 환경에서 안전하고 빠르게 빌드를 진행 가능

선택 가능한 빌드 서버 리소스

- 소스코드 빌드 및 테스트 케이스에 따라 효과적인 컴퓨팅 유형을 선택해 빌드를 진행 가능
- 매번 빌드 작업을 할 때마다 동일한 환경에서 안전하고 빠르게 빌드를 진행 가능



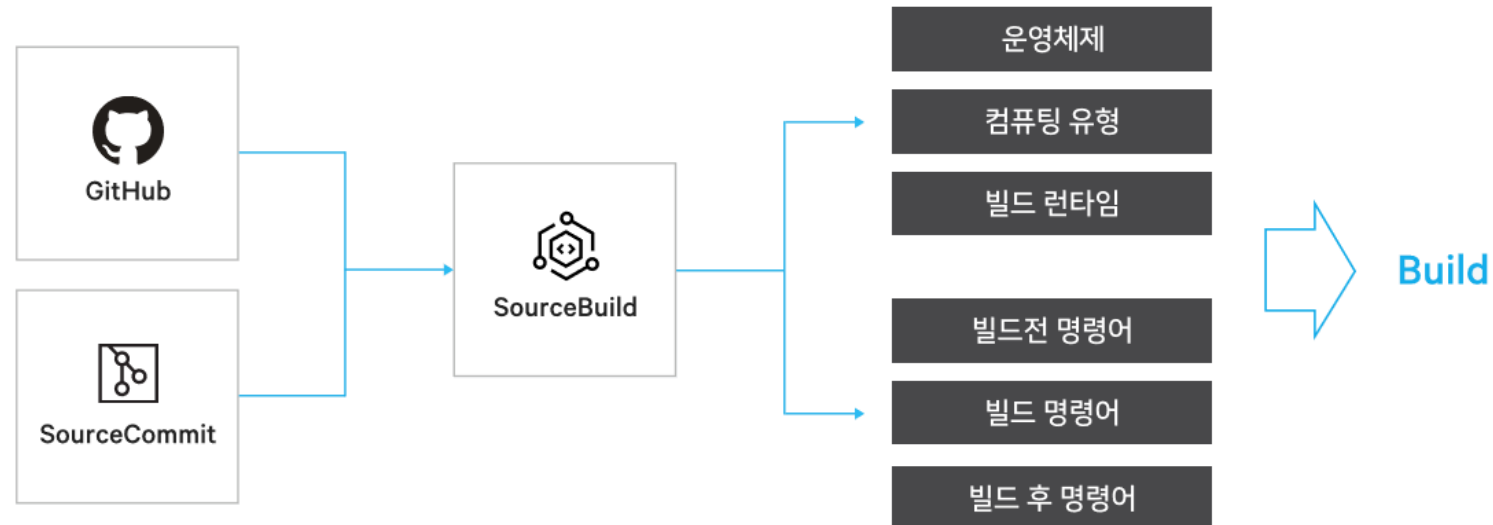
SourceBuild (소스빌드 서비스)

미리 구성된 다양한 빌드 환경 제공

- 개발자가 주로 이용하는 라이브러리와 툴을 미리 구성한 운영체제 및 빌드 런타임을 제공
- 자신에게 맞는 환경을 선택해 쉽고 빠르게 프로젝트를 생성하고 빌드 작업 가능

사용자가 원하는 커스텀 환경 제공 가능

- 사용자가 도커 허브(Docker Hub) 및 퍼블릭 저장소(Public Repository)에서 제공하는 커스텀 도커 이미지를 사용을 통해 사용자가 원하는 빌드 환경에 대해 빠르게 구성 가능



SourceBuild (소스빌드 서비스)

쉽고 빠른 결과물 배포

- 간단한 설정으로 쉽고 빠르게 결과물을 오브젝트 스토리지(Object Storage)에 배포
- 백업 기능을 이용하면 과거 빌드 결과물도 안전하게 보관 가능

파일 세이퍼 연계를 통한 보안 강화

클라우드 로그 애널리틱스 사용

- 발생하는 로그 이력을 저장하고 분석할 수 있는 서비스



SourceDeploy 서비스 소개

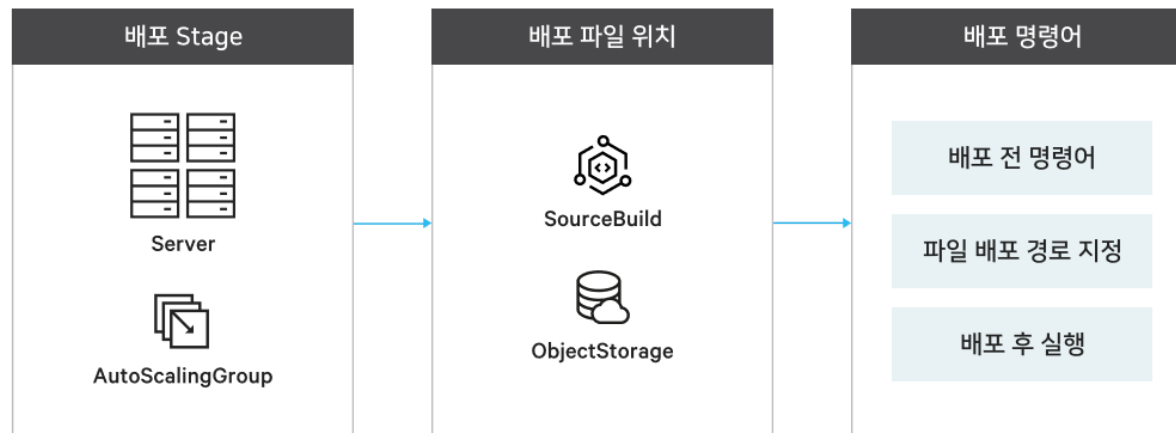
SourceDeploy (소스배포 서비스)

배포 프로젝트별 다양한 환경 및 배포 시나리오 구성

- ✓ 배포 스테이지(Stage)에서 하나의 배포 프로젝트 안에 여러 환경을 구성하고
각 환경마다 배포 시나리오를 다수 생성 가능
- ✓ 이런 구성을 하나의 프로젝트 내에서 한눈에 확인할 수 있어, 배포 관리를 손쉽게 가능

오브젝트 스토리지 및 소스빌드 서비스 연계를 통한 배포 파일 선택

- ✓ 배포하고자 하는 파일 위치는 오브젝트 스토리지 및 소스빌드 서비스 중에서 선택 가능
- ✓ 오브젝트 스토리지에 압축 형태로 소스를 업로드 해두면, 배포 시 자동으로 해당 파일을 다운로드해 배포
- ✓ 소스빌드 서비스를 선택한 경우에는 빌드 프로젝트에서 가장 마지막으로 성공한 결과물을 조회해 해당 결과물을 자동으로 배포
- ✓ 매번 빌드 작업을 할 때마다 동일한 환경에서 안전하고 빠르게 빌드를 진행 가능



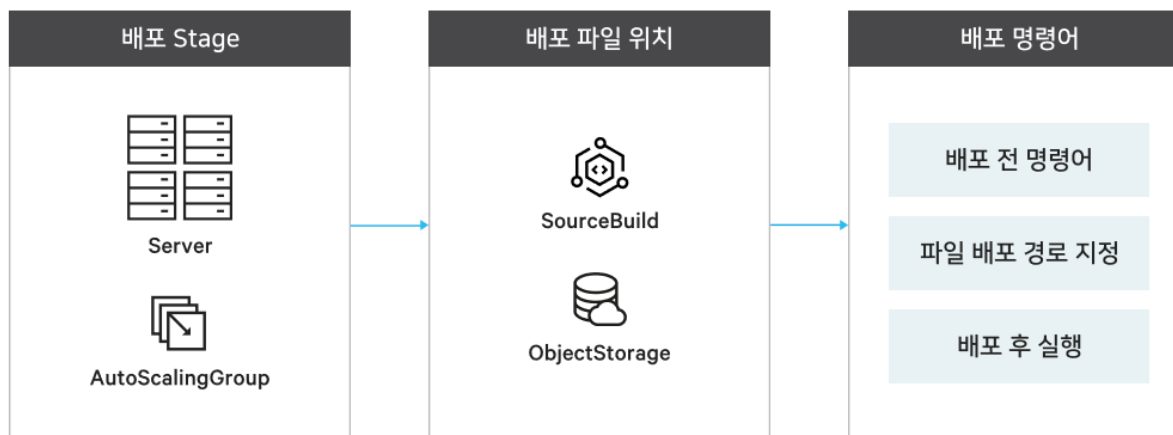
SourceDeploy (소스배포 서비스)

꼭 필요한 배포만 실행 가능

- ✓ 배포 실행 관리자를 별도로 두어 승인을 받아야만 배포가 실행될 수 있도록 배포 제어 기능을 제공.
- ✓ 배포가 실행되기 전 관리자로부터 해당 배포에 대한 검증을 통해 잘못된 배포 실수를 줄일 수 있음.
- ✓ 이런 구성을 하나의 프로젝트 내에서 한눈에 확인할 수 있어, 배포 관리를 손쉽게 가능.

배포 단계별로 필요한 명령어 실행 가능

- ✓ 배포 명령어 단계에서 서버에 배포할 때, 배포 전후로 필요한 명령어를 설정해 서버에서 실행 가능.
- ✓ 돌고 있는 서비스 재실행 또는 필요한 스크립트 실행 등 해당 명령어를 통해 배포 프로세스를 좀 더 유연하게 확장 가능.

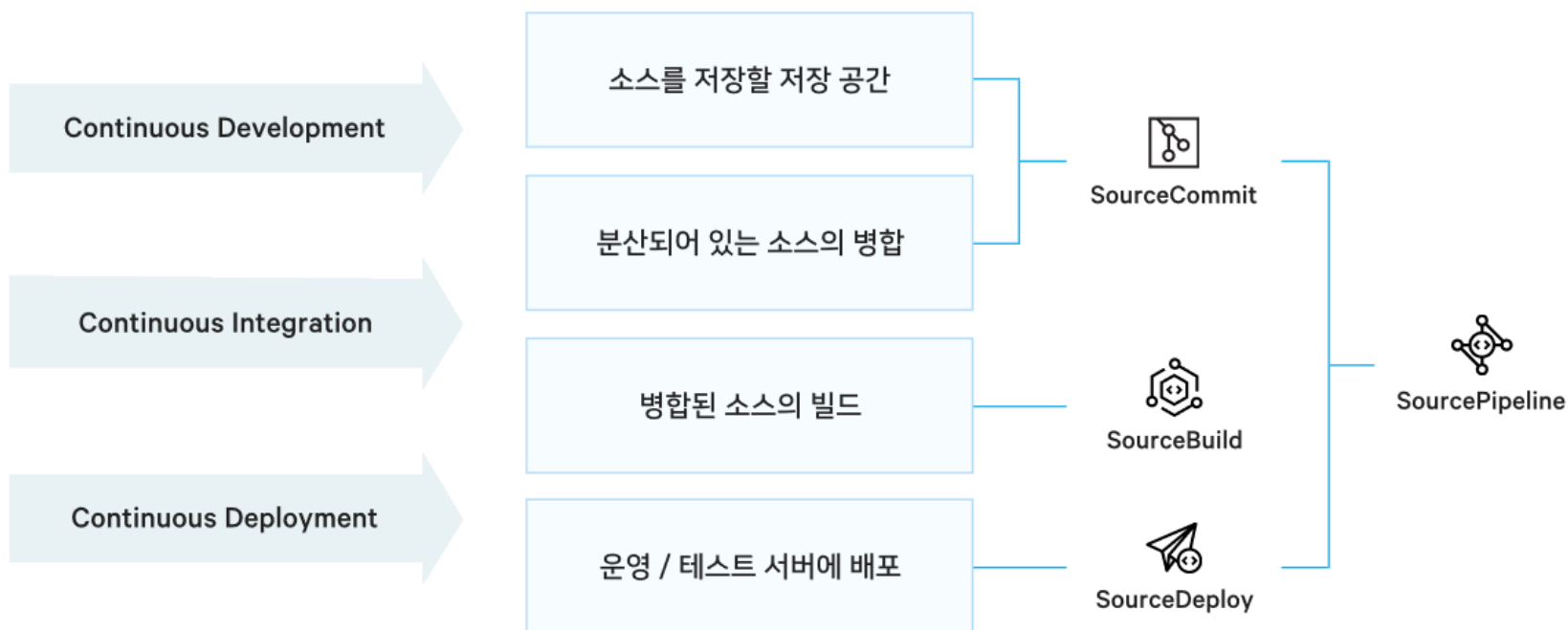


SourcePipeline 서비스 소개

SourceDeploy (소스배포 서비스)

저장소, 빌드, 배포 통합 프로세스 제공

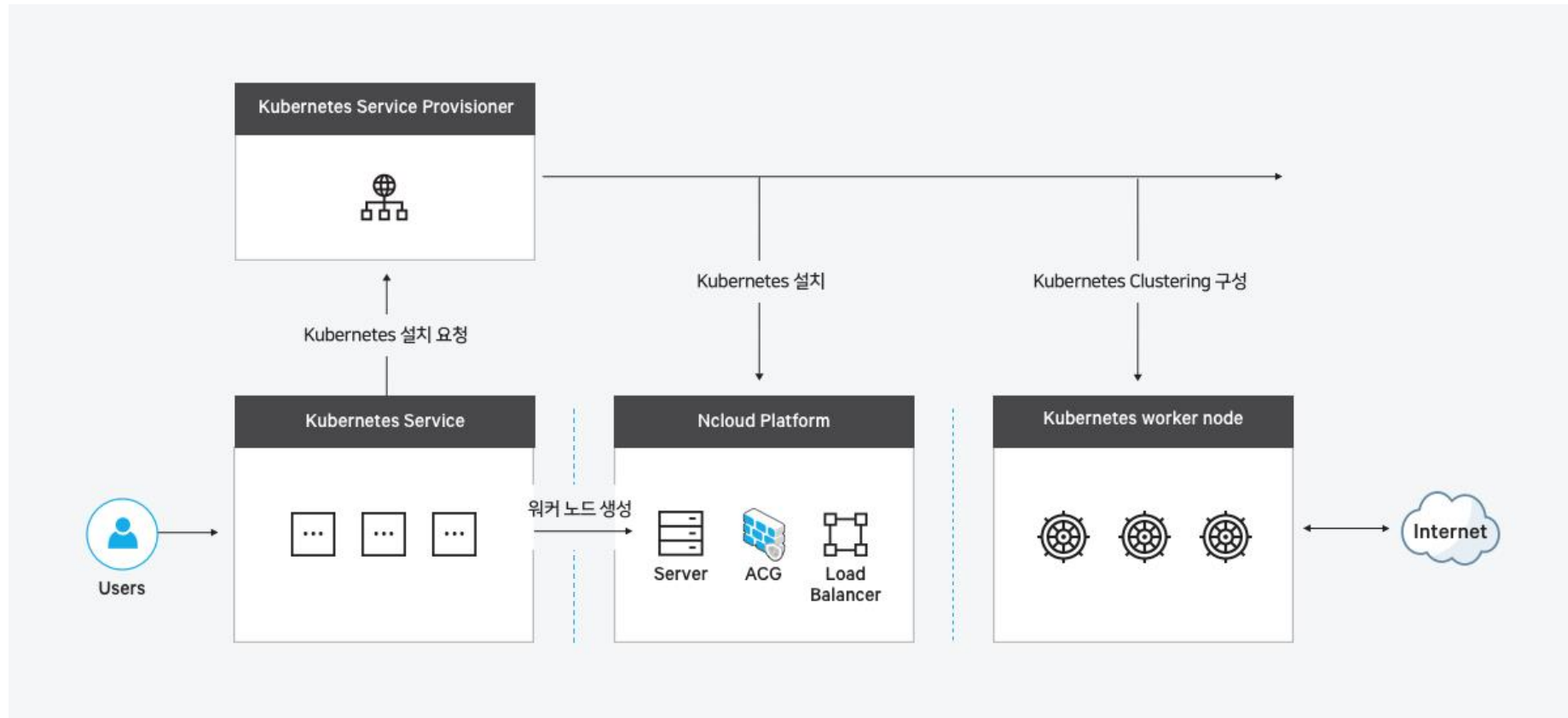
- ✓ 소스 파이프라인은 소스커밋 서비스, 소스빌드 서비스 서비스, 소스 배포 서비스를 통합해 저장소, 빌드, 배포의 과정을 자동화
- ✓ 변경하는 사항을 매번 빌드하고 배포하는 과정을 자동화해 신속하고 빠르게 소프트웨어를 출시 가능
- ✓ 저장소, 빌드, 배포 과정을 통합해 작은 규모의 버그와 오류에 신속하게 대응.



네이버 클라우드 플랫폼 Kubernetes Service 소개



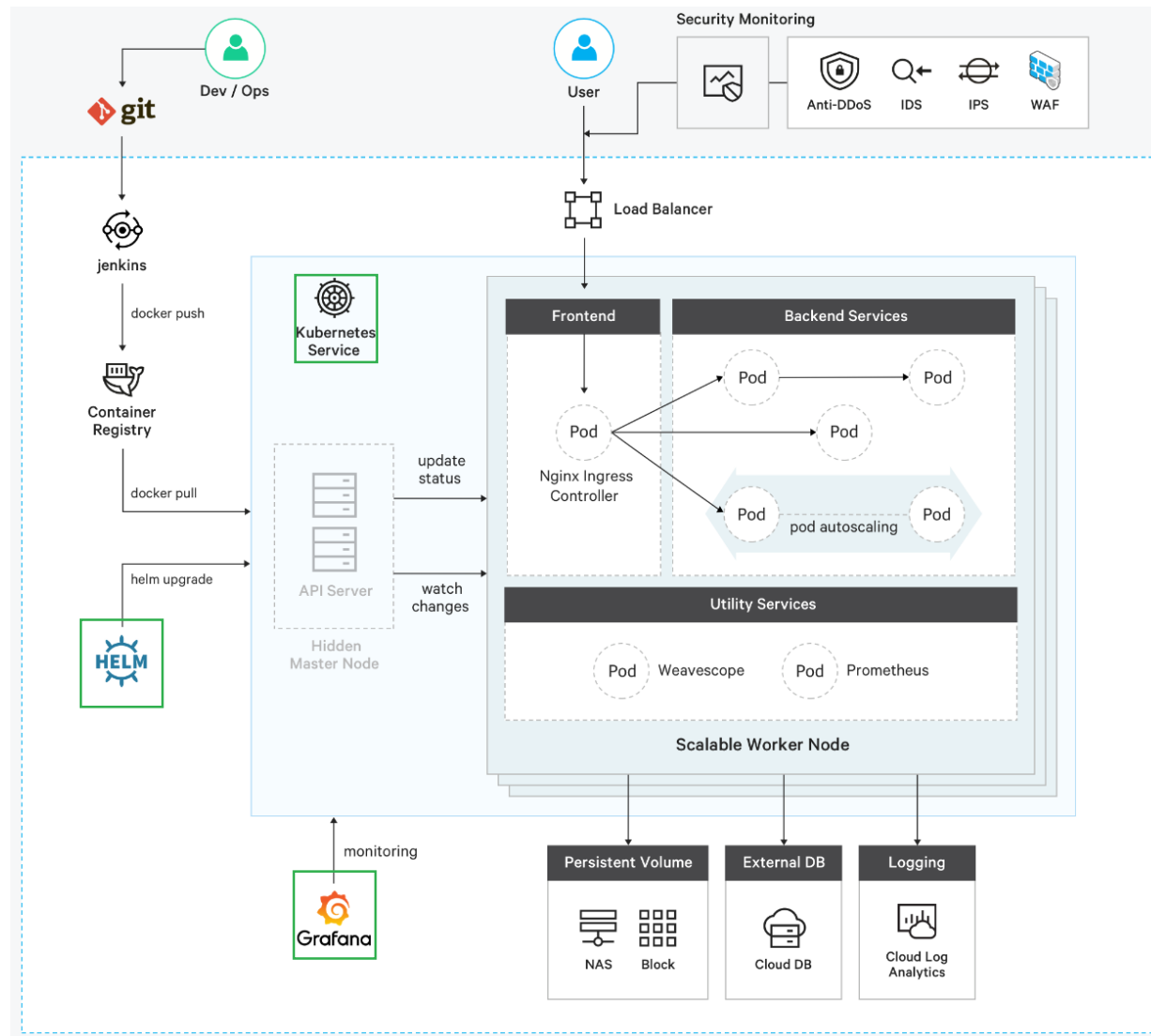
Kubernetes Service Provisioner



Kubernetes Service Provisioner의 제공 범위

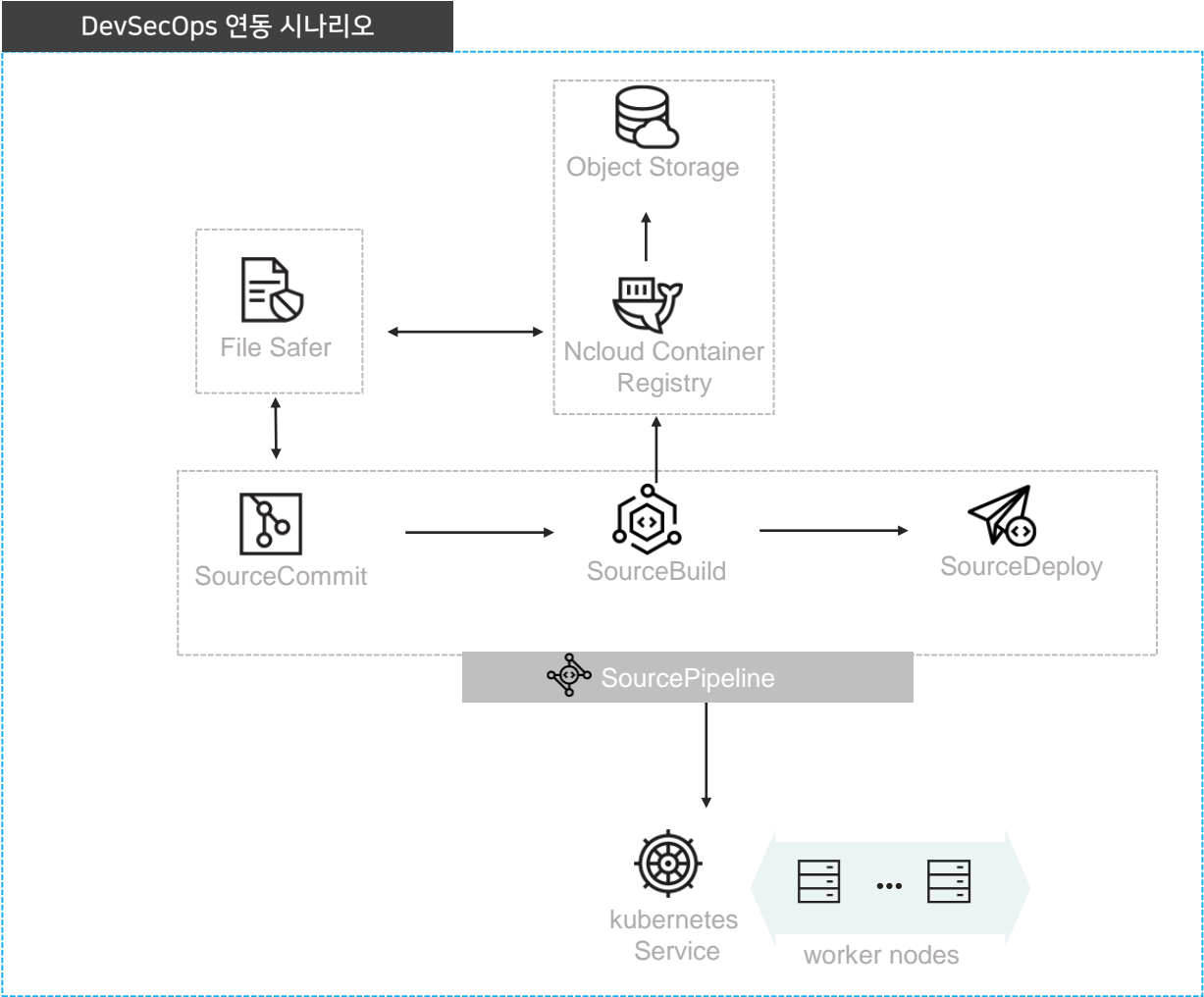


NAVER CLOUD PLATFORM 의 Kubernetes service 구조



네이버 클라우드 플랫폼에서 DevSecOps를 이용하여 서비스 배포 하기

DevSecOps를 이용하여 서비스 연동 시나리오



하시코프 소개



세계적으로 인정 받고 가장 많은 사람들이 동참하고 있는
클라우드 인프라 자동화 도구를 제공합니다.

나스닥에서 발표한 #EnterpriseTech30 목록에서
가장 유망한 엔터프라이즈 기술 회사로 선정되었습니다.

하시코프 솔루션

온프레미스와 클라우드 전반의
인프라 프로비저닝과 자동화



서비스 디스커버리와 서비스 메시로 네트워
크 자동화



로컬 개발환경을 위한 VM 프로비저닝 자동
화와 관리



인증/인가 기반으로
서버와 서비스에 대한 접근관리



민감한 정보의 관리와 접근에
중앙화된 관리 서비스



애플리케이션 배포와 실행을 위한
오케스트레이터



다양한 플랫폼에 대한 이미지 생성과 컨테이
너 이미지를 생성



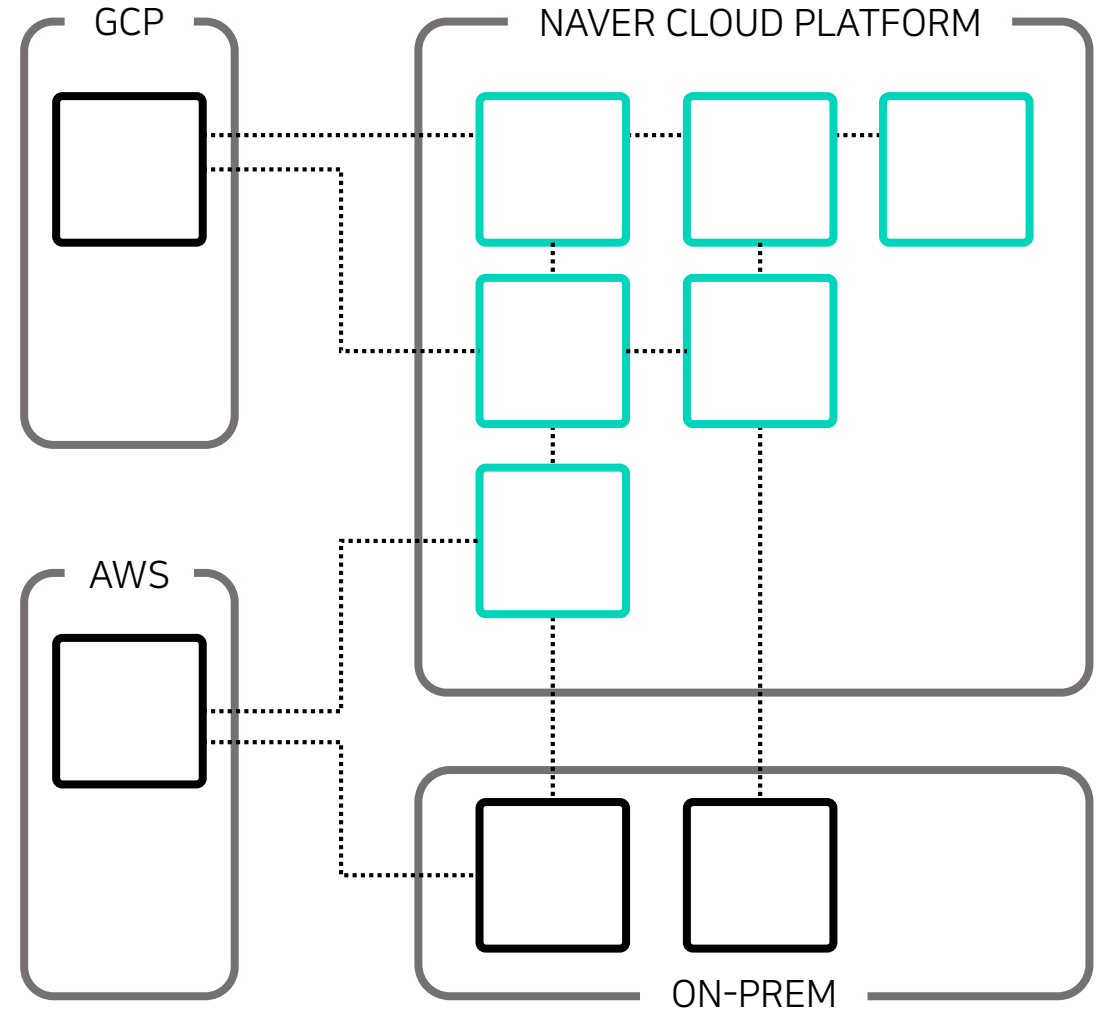
단일 구성으로 컨테이너 환경에
애플리케이션 빌드 및 배포

네이버 클라우드 플랫폼과 하시코프의 멀티 클라우드 전략

멀티 클라우드 - 필요성과 장점

멀티 클라우드란 같은 형태의 클라우드 서비스를 의도적으로 여러 클라우드 제공 기반으로부터 받아 사용하는 것

- 특정 클라우드 서비스에 종속을 방지
- 적합한 조건이나 규정에 따라 필요한 클라우드 환경을 선택
- 기존 데이터센터의 클라우드화에 따라 온프레미스 환경과 퍼블릭 클라우드를 혼용하여 비용 최적화
- 비용, 서비스 측면에서 유연성을 확보



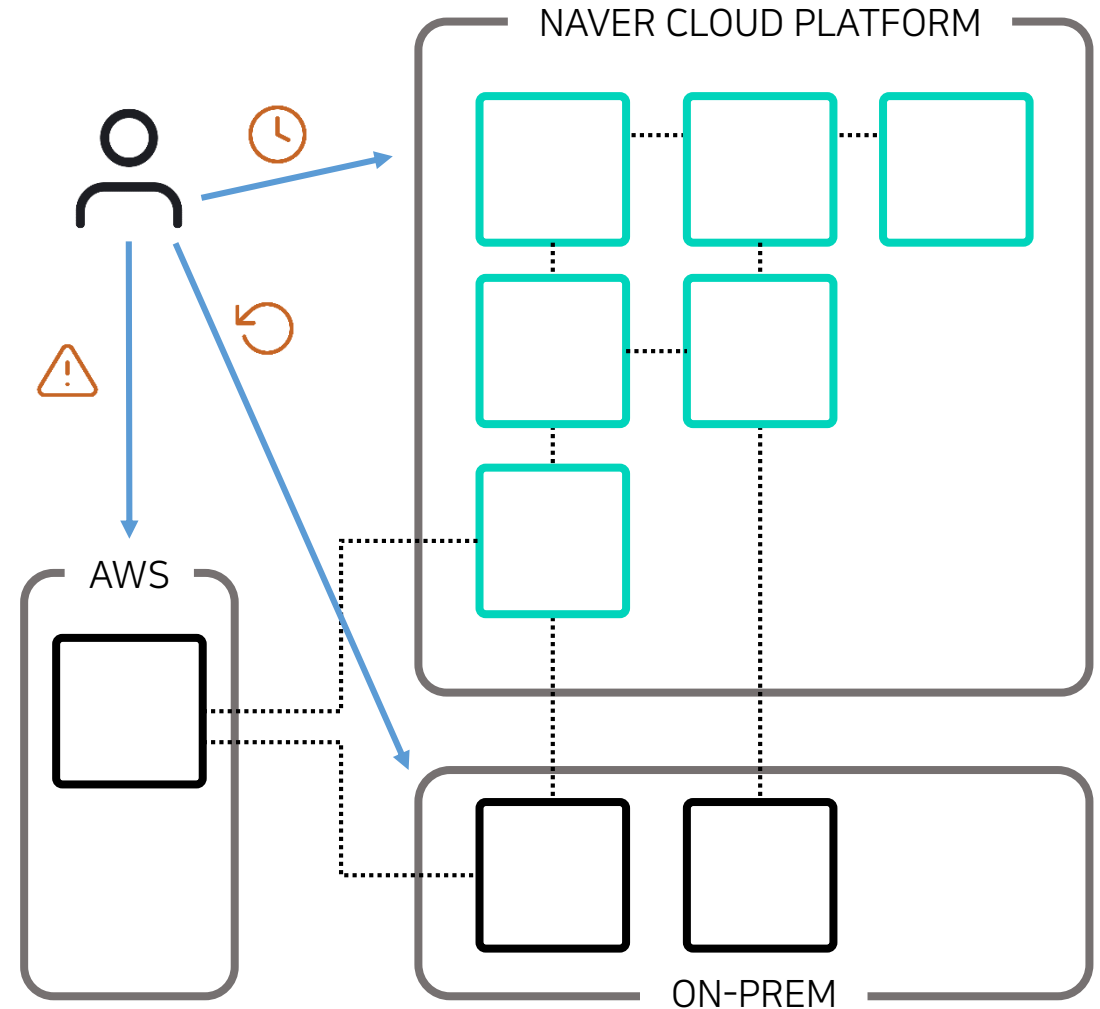
멀티 클라우드 - 단점과 과제

단점

- 멀티 클라우드 전환 시 비용 통제가 어려움
- 이기종 클라우드 환경을 컨트롤 하기 위한 복잡성이 증가
- 클라우드 간 서비스 연결에 보안 위협 증가

과제

- 멀티 클라우드 구축을 위한 전략적 파트너
- 현업에 대한 클라우드 서비스 교육
- 서비스를 위한 애플리케이션 워크로드 정책 수립
- CI/CD와 더불어 클라우드를 위한 DevOps 팀과 협업
- 클라우드 간 이식성 향상



멀티클라우드 전략



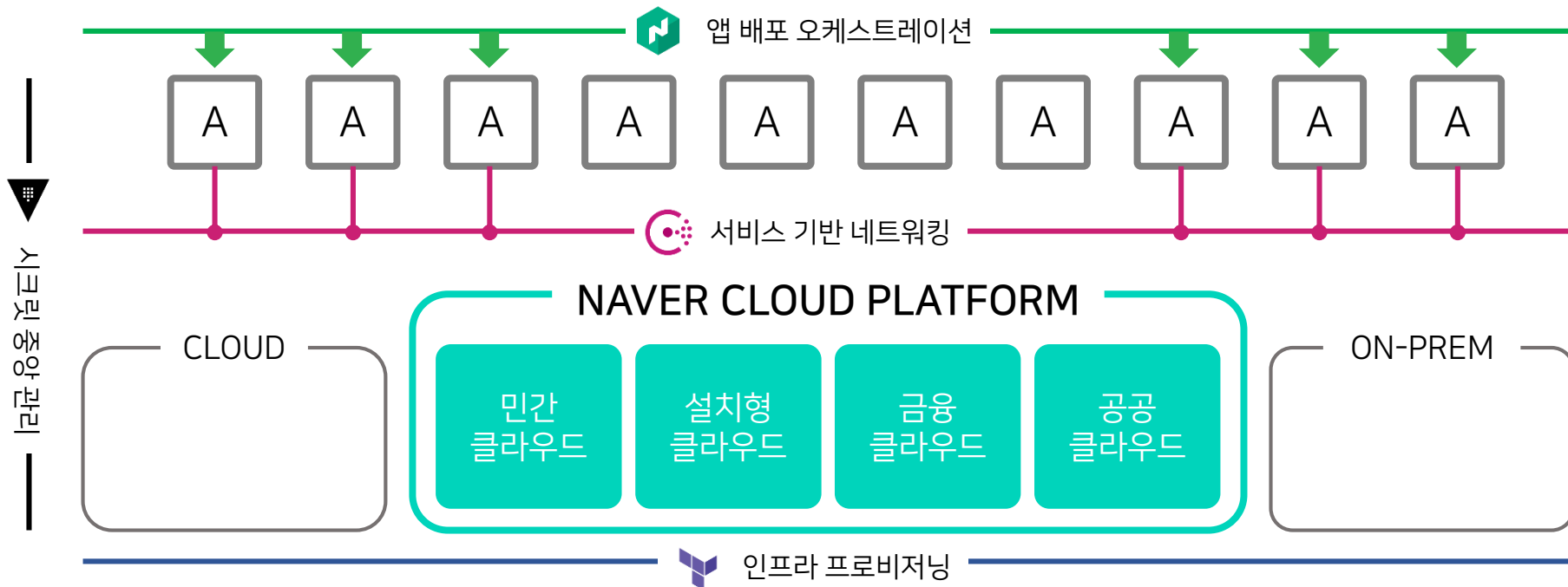
NAVER
CLOUD PLATFORM

- 안정적인 클라우드 환경 제공
- 직관적인 UI/UX와 서비스 구조로 편리한 사용성
- 검증된 클라우드 교육 시스템으로 현업 역량 강화
- 규제 산업 클라우드 도입을 위한 공공, 금융 클라우드 환경 제공



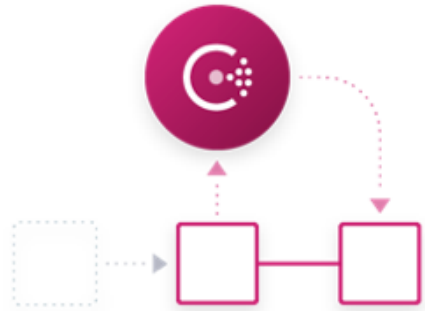
HashiCorp

- 클라우드 운영 모델을 통한 일관된 워크플로우 생성
- 멀티 클라우드 간의 서비스 연계와 배포
- 퍼져있는 민감 정보의 중앙관리
- 온프레미스와 클라우드 전반에 걸친 사용성 제공



Consul – 서비스 찾기

Consul의 기능



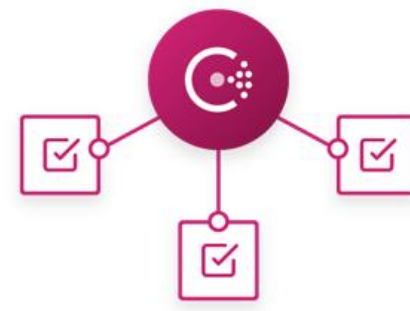
Service Discovery

서비스를 자동으로 등록하고 찾아주는
동적 레지스트리



Service Segmentation & Mesh

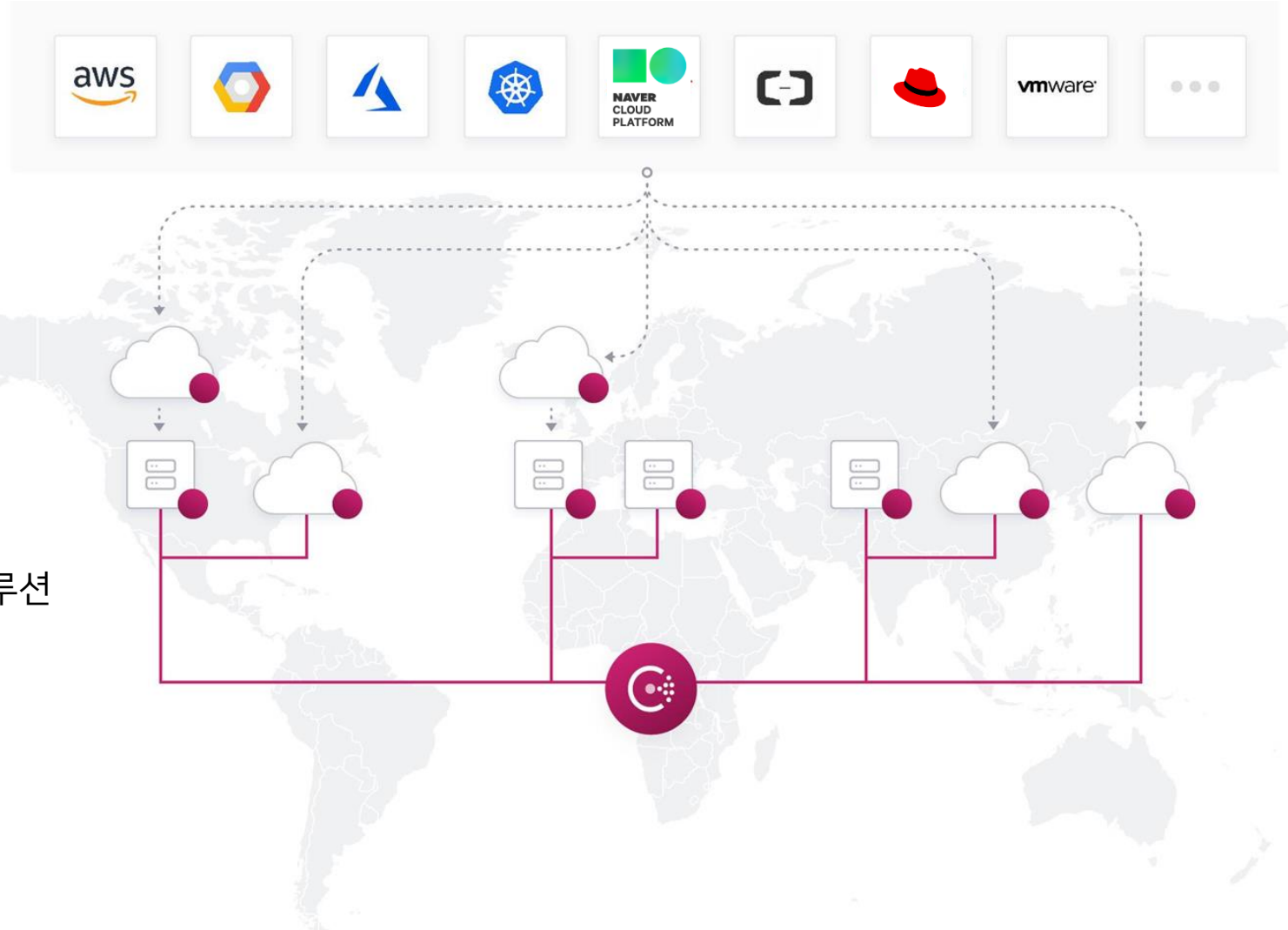
안전한 서비스 연결과 서비스 간 정책



Service Configuration

중앙화된 설정 관리 레지스트리

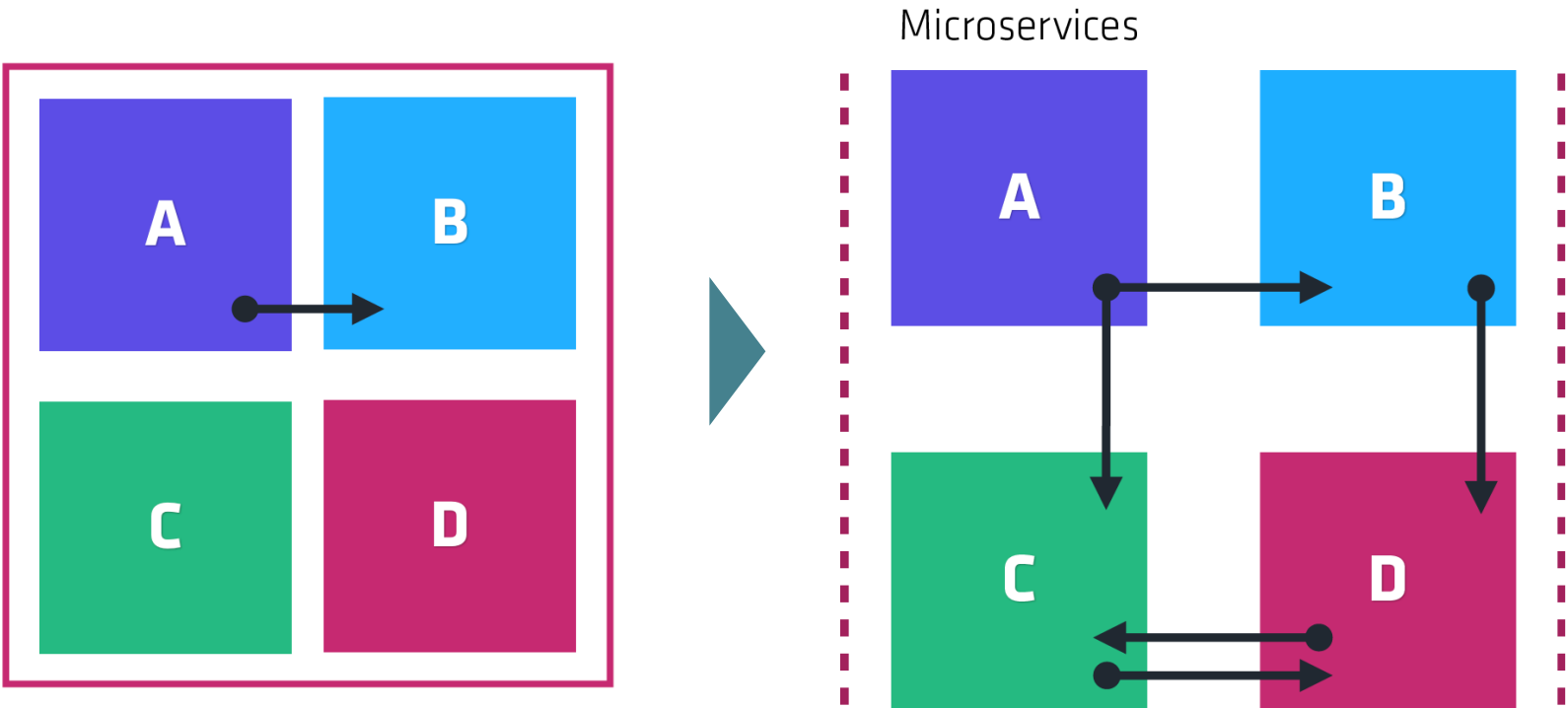
Consul - WAN Federation



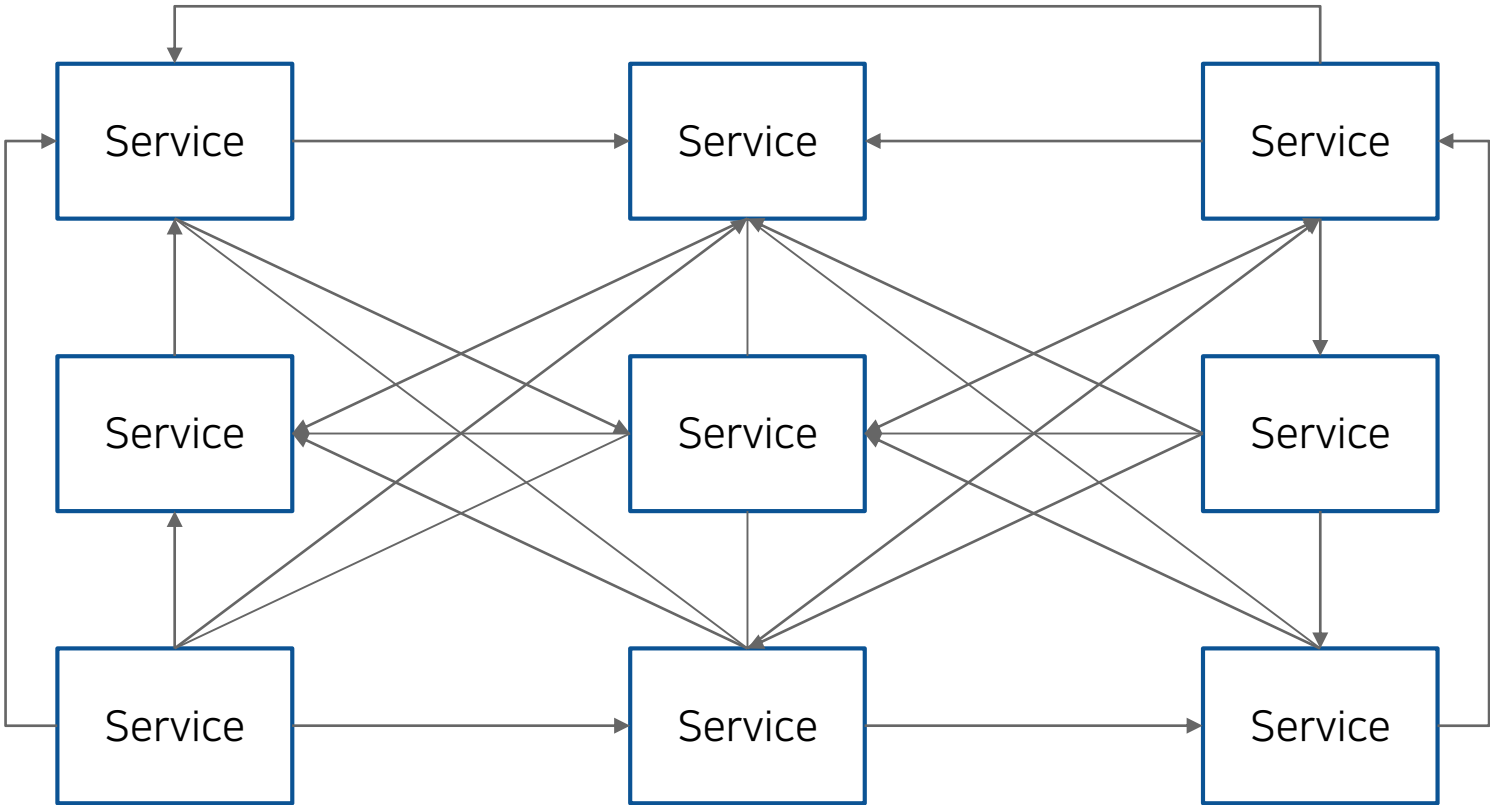
- 멀티 클라우드 환경을 위한 네트워킹 솔루션
- 기존 데이터센터와 클라우드를 포함한 타 데이터 센터의 서비스 통합 관리

Consul – Service Mesh

Micro Services Architecture



DISTRIBUTION Microservices Architecture

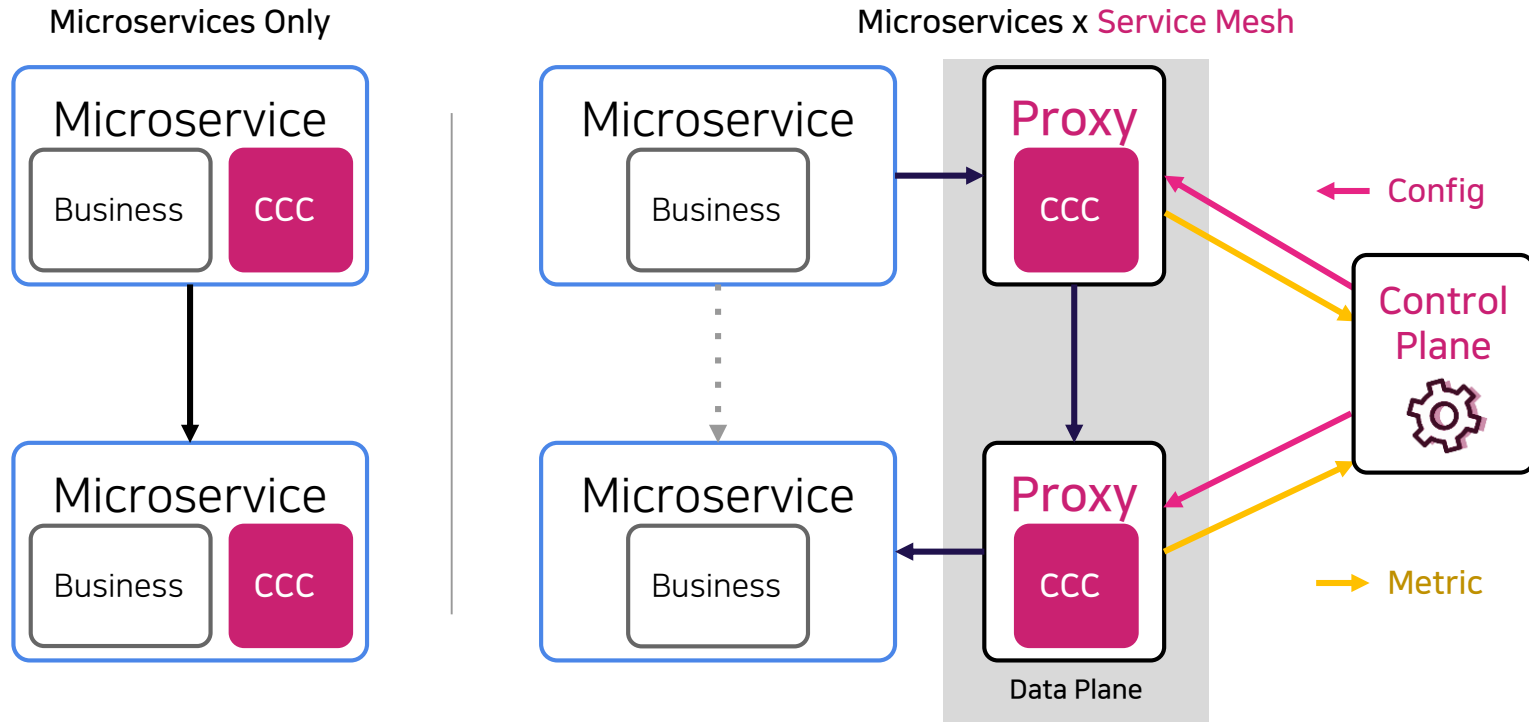


MSA의 도전 과제



CCC - Cross Cutting Concern (횡단 관심사)
: 애플리케이션의 주요 목적 외에 로깅, 인증 연동, 장애 처리, 서비스 찾기 등의 상호작용 처리

MSA의 도전 과제



CCC - Cross Cutting Concern (횡단 관심사)
: 애플리케이션의 주요 목적 외에 로깅, 인증 연동, 장애 처리, 서비스 찾기 등의 상호작용 처리

Consul – Service Mesh

지원되는 프로토콜

TCP, HTTP/1.1+, HTTP/2, gRPC

사이드카

Envoy proxy, Consul proxy

플랫폼 지원

BM, VM, Nomad, Kubernetes

멀티/하이브리드 서비스 메시

Kubernetes, VM, BM - x86, ARM, FreeBSD 등

SaaS 서비스

AWS, Azure

모니터링 기능

- 액세스 로그
- Prometheus 통합
- Grafana 통합
- Path 기반 메트릭
- UI
- 호환 백엔드
 - Datadog
 - Jaeger
 - Zipkin
 - OpenTracing
 - Honeycomb

보안 기능

- mTLS
- 외부 CA인증서 적용
- 외부 CA 키 플러그인
- 동적 트래픽 통제

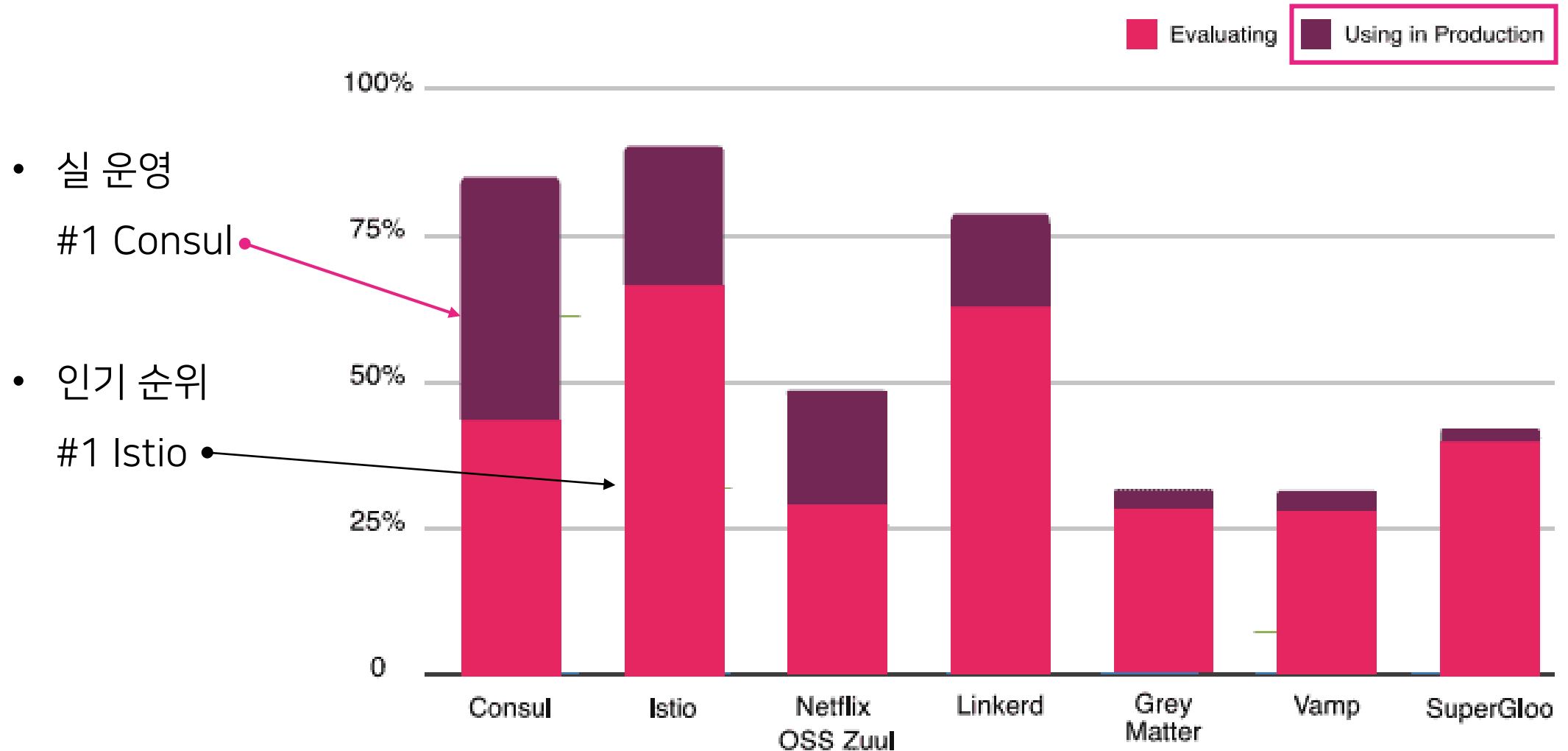
라우팅 기능

- 부하 분산
 - Round Robin
 - Random
 - Weighted
 - Least Request
 - Consistent Hash
- 백분율 기반 분산
- 헤더 및 경로 기반 분산

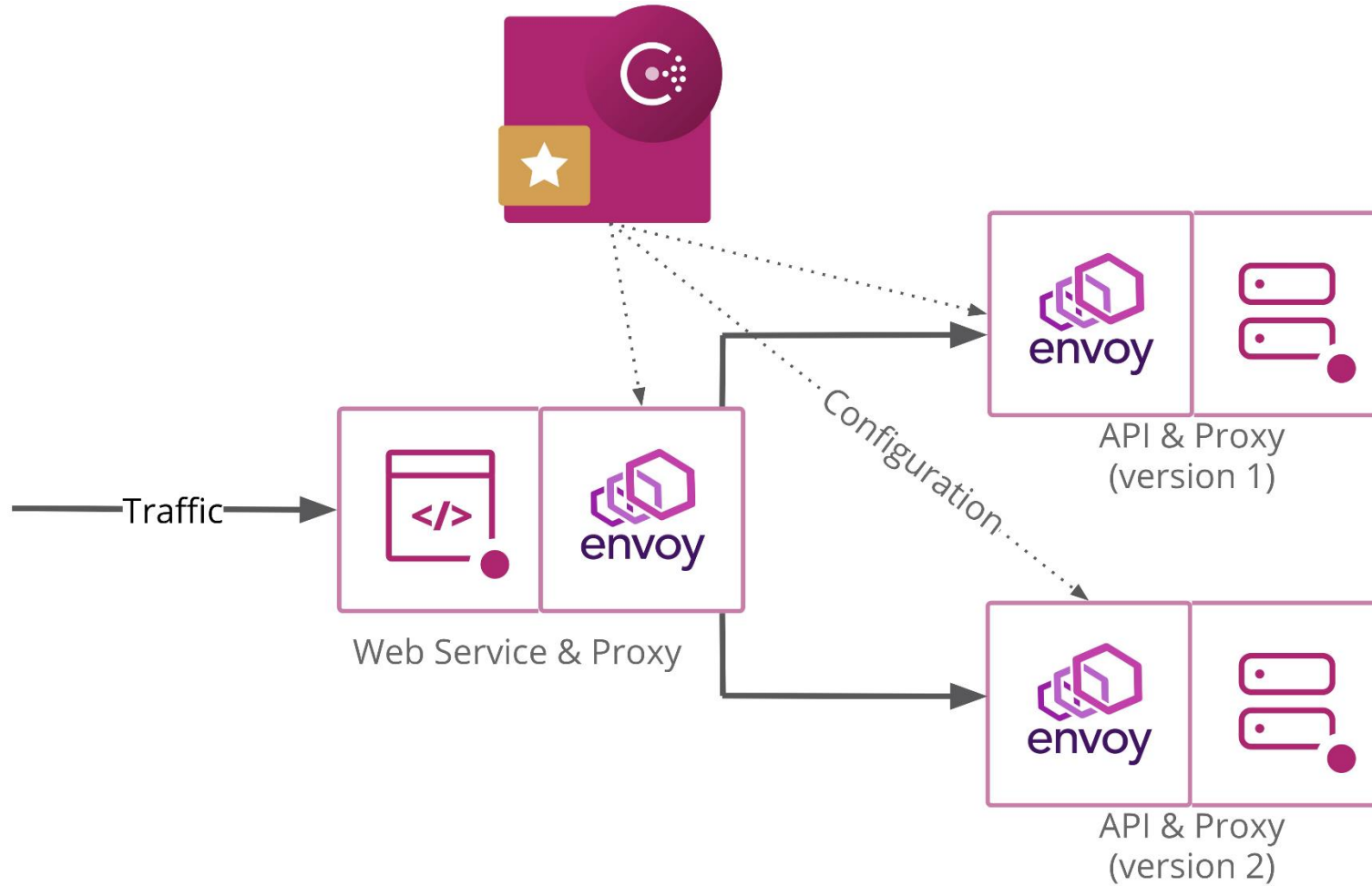
탄력성 기능

- 회로 차단
- 재시도 및 시간 초과
- 경로 기반 재시도 및 시간 초과

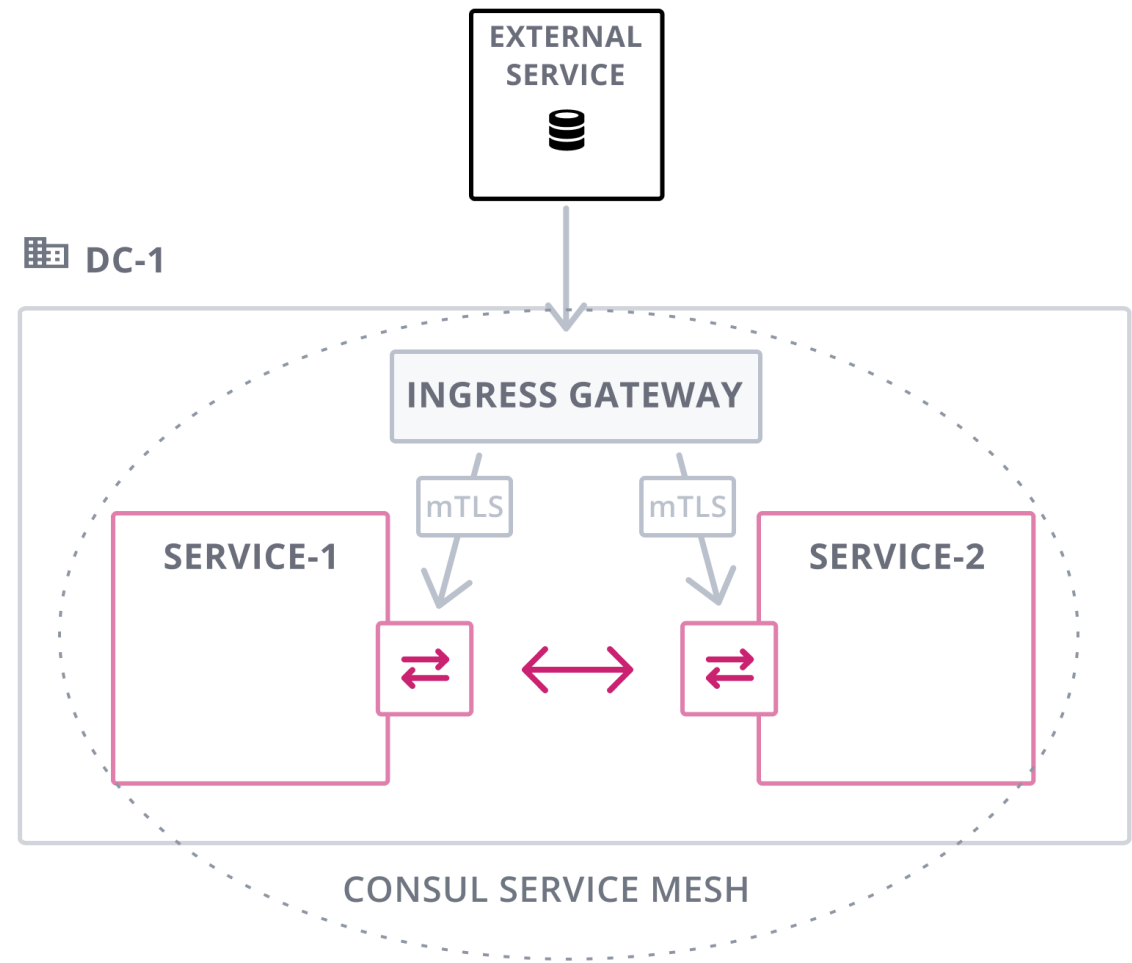
Consul – Service Mesh



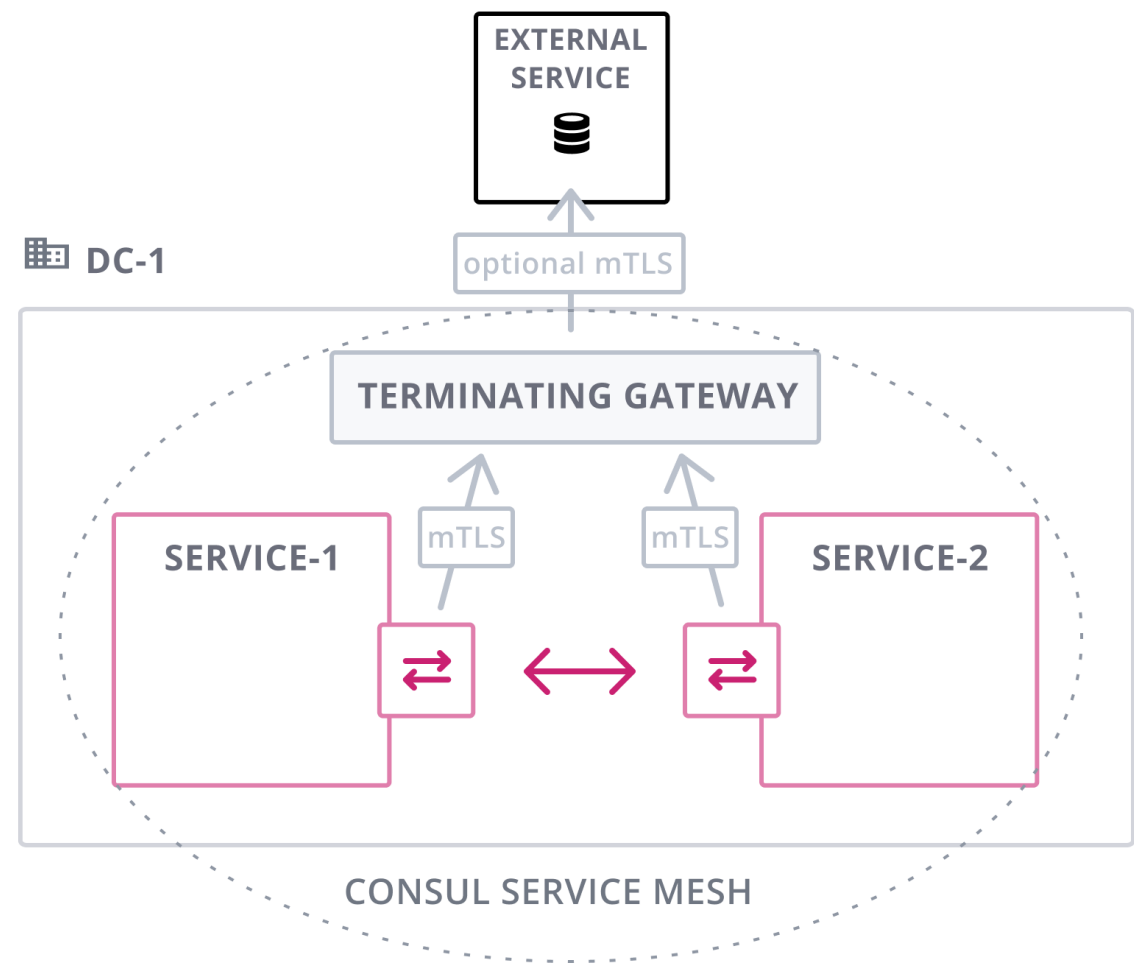
"Sidecar" proxy



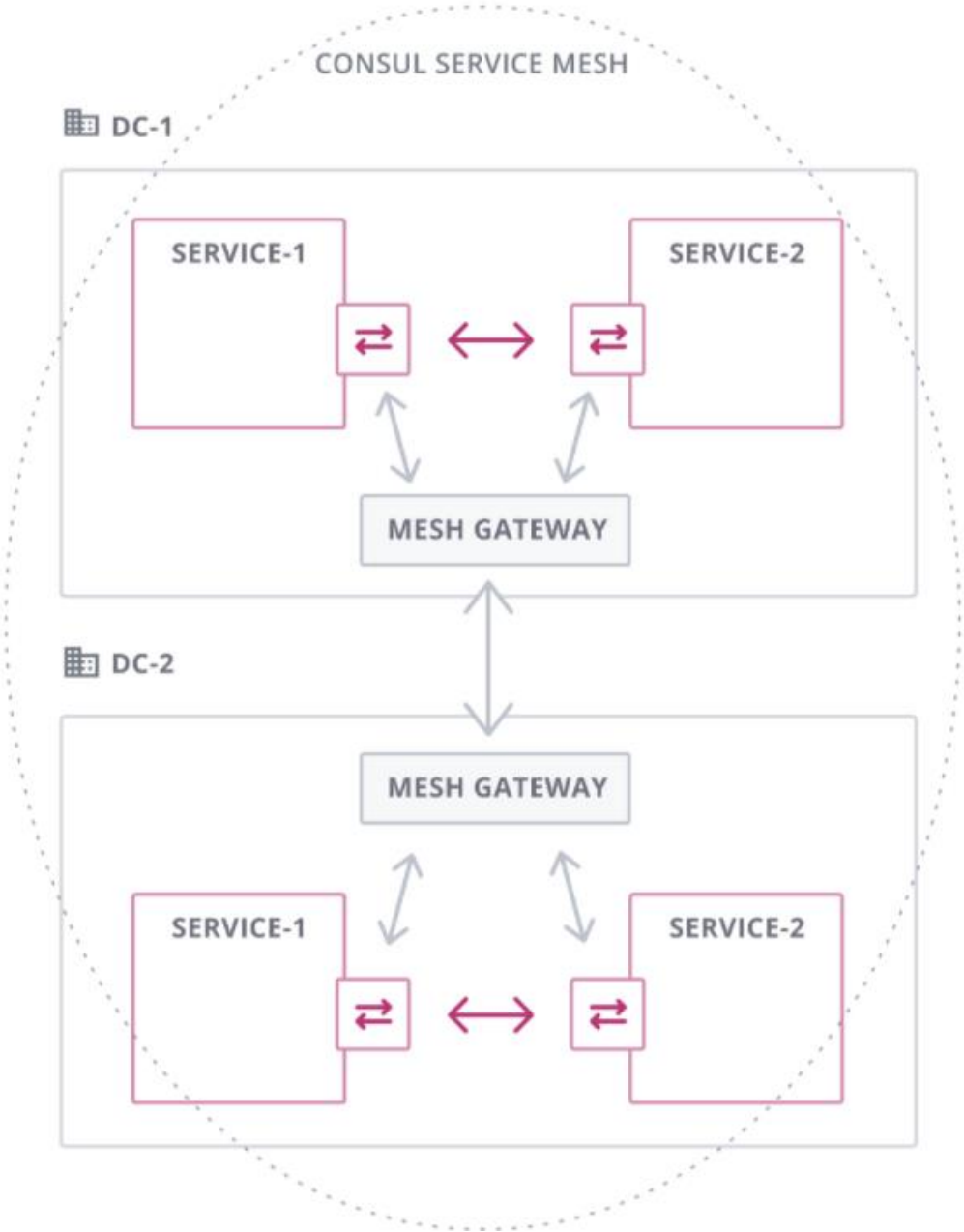
"Ingress" gateway



"Terminating" gateway

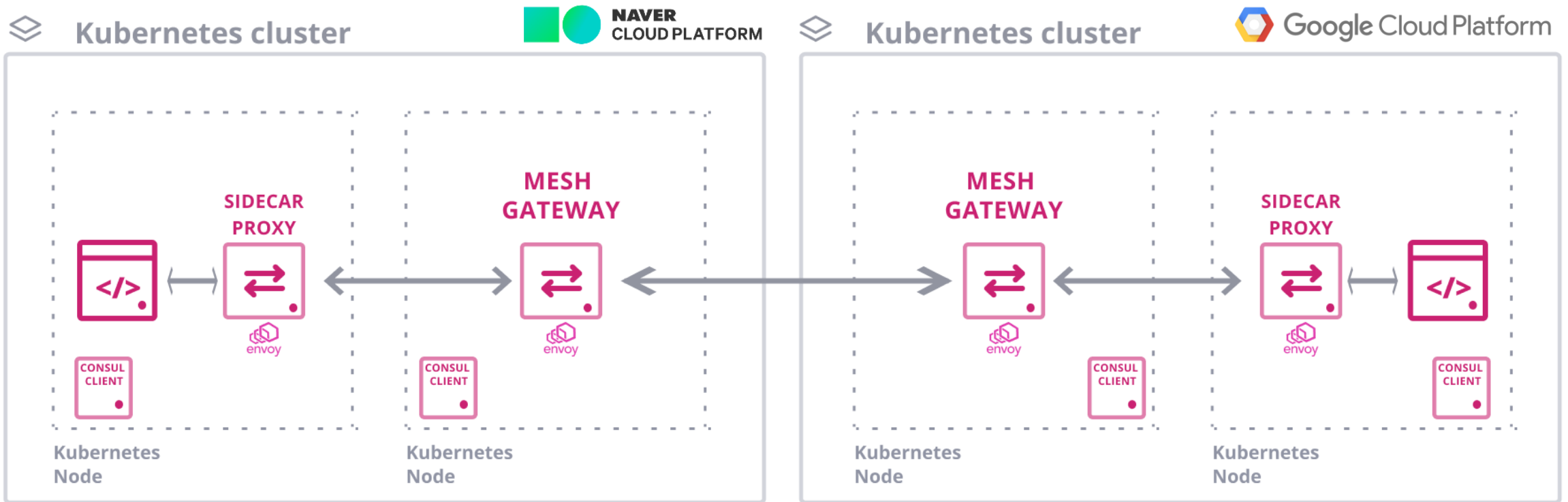


"Mesh" gateway



Consul Federation Demo : NCP - GCP

Overview



어떻게 서로를 찾을 수 있을까요?

```
Deployment or Pod
...
metadata:
  annotations:
    consul.hashicorp.com/connect-inject: 'true'
    consul.hashicorp.com/connect-service: 'dashboard-http'
    consul.hashicorp.com/connect-service-upstreams: 'counting:9001:dc-gcp'
```

Consul Sidecar
(=Consul connect)
사용 여부

Service Discovery에
등록될 서비스 이름

연결 대상 서비스 이름

"[service-name].[service-namespace]:[port]:[optional datacenter]"

Resource

- <https://youtube.com/c/NAVERCLOUDPLATFORM>
- https://blog.naver.com/n_cloudplatform
- <https://www.ncloud.com/guideCenter>
- https://github.com/Planet15/ncloud_infra_example
- https://blog.naver.com/n_cloudplatform/221829343597

-
- <https://www.consul.io/>
 - <https://learn.hashicorp.com/collections/consul/kubernetes-deploy>
 - <https://github.com/hashicorp/consul-helm>

금일 데모 코드로

지금 바로 경험해보시죠!

<https://me2.do/5ncburlj>