

Kubernetes

클라우드에서 쉽게 사용하자

장현덕 컨설턴트, 클루커스

Cloocus

Gold
Microsoft
Partner


Azure
Expert
MSP

Final Update 2021.09.02 | Produced by Cloocus

Copyright © Cloocus

CONTENTS

- 01 | Docker & Container
- 02 | Kubernetes
- 03 | Azure Kubernetes Service
- 04 | Demo
- 05 | Summary

01

Container & Docker

01. Container & Docker

Container 란?

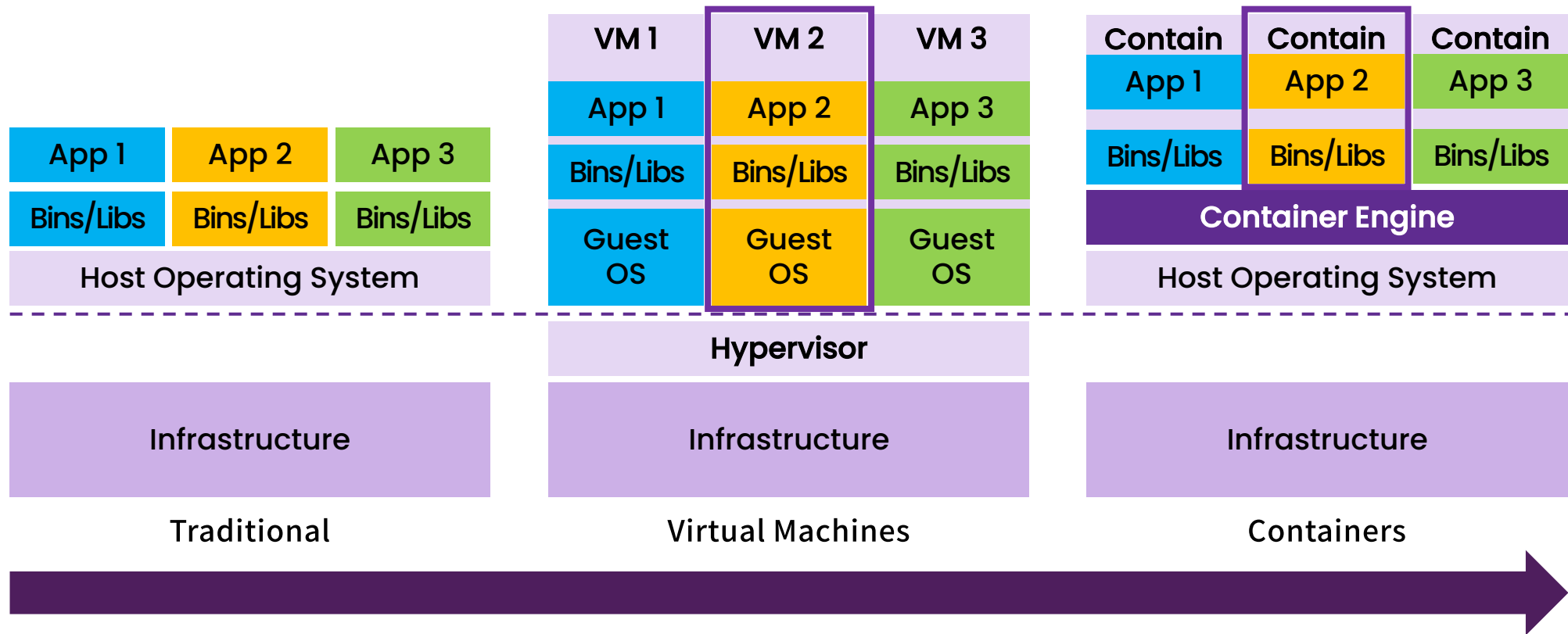
Container

- 소프트웨어 패키지를 빌드하고 실행할 수 있는 격리된 환경



01. Container & Docker

Container로의 시대적 흐름 변화

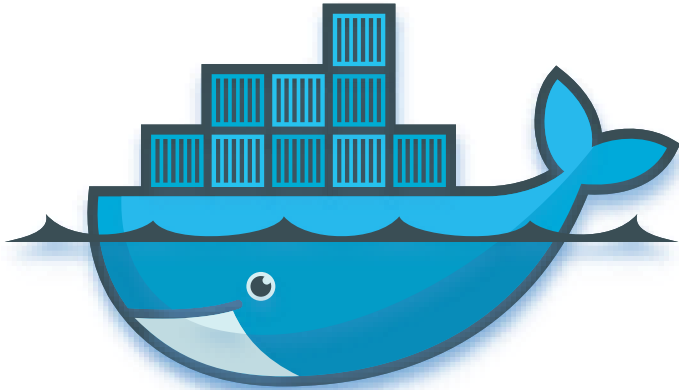


01. Container & Docker

Docker 란

Application을 컨테이너로 쉽게 사용할 수 있는 “ Docker ”

- 컨테이너 생성 및 사용환경을 제공하는 컨테이너화 플랫폼



- 2013년 오픈소스 Docker Engine 출시
- Go 언어
- Linux, Window, MacOS 지원
- Azure를 포함한 많은 클라우드가 Docker를 지원

이미지 및 컨테이너로 구성
이미지로 구성하여 컨테이너에서 실행
한번 생성해 놓은 이미지를 통해 동일한 환경에서 쉽게 재현 가능
Guest OS 없이 실행이 가능.

01. Container & Docker

Docker Container 사용 이점

빠르고 쉬운
배포

이식성 있는
배포 환경

운영 비용
절약

01. Container & Docker

컨테이너 오케스트레이션의 필요성

“Container & Docker
확장성에 대한 문제 제기”



“ 컨테이너 운영 및 관리 필요 ”

많은 수의 컨테이너를 구성, 추가, 제거, 업데이트하는 프로세스



“ 오케스트레이션 ”

01. Container & Docker

컨테이너 오케스트레이션의 필요성

컨테이너 오케스트레이션

자동으로 컨테이너화된 앱을 배포하고 관리하는 시스템

컨테이너 오케스트레이션 기능

- ✓ 컨테이너 자동 배치 및 복제
- ✓ 컨테이너 그룹에 대한 로드 밸런싱
- ✓ 컨테이너 장애 복구
- ✓ 클러스터 외부에 서비스 노출
- ✓ 컨테이너 추가 또는 제거로 확장 및 축소
- ✓ 컨테이너 서비스간의 인터페이스를 통한 연결 및 네트워크 포트 노출 제어



컨테이너 인스턴스 수를
동적으로 조정



실행 중인 인스턴스
자동 업데이트

02



Kubernetes

02. Kubernetes

Kubernetes란



//

컨테이너를 쉽고 빠르게 배포/확장하고

관리를 자동화해주는 오픈소스 플랫폼

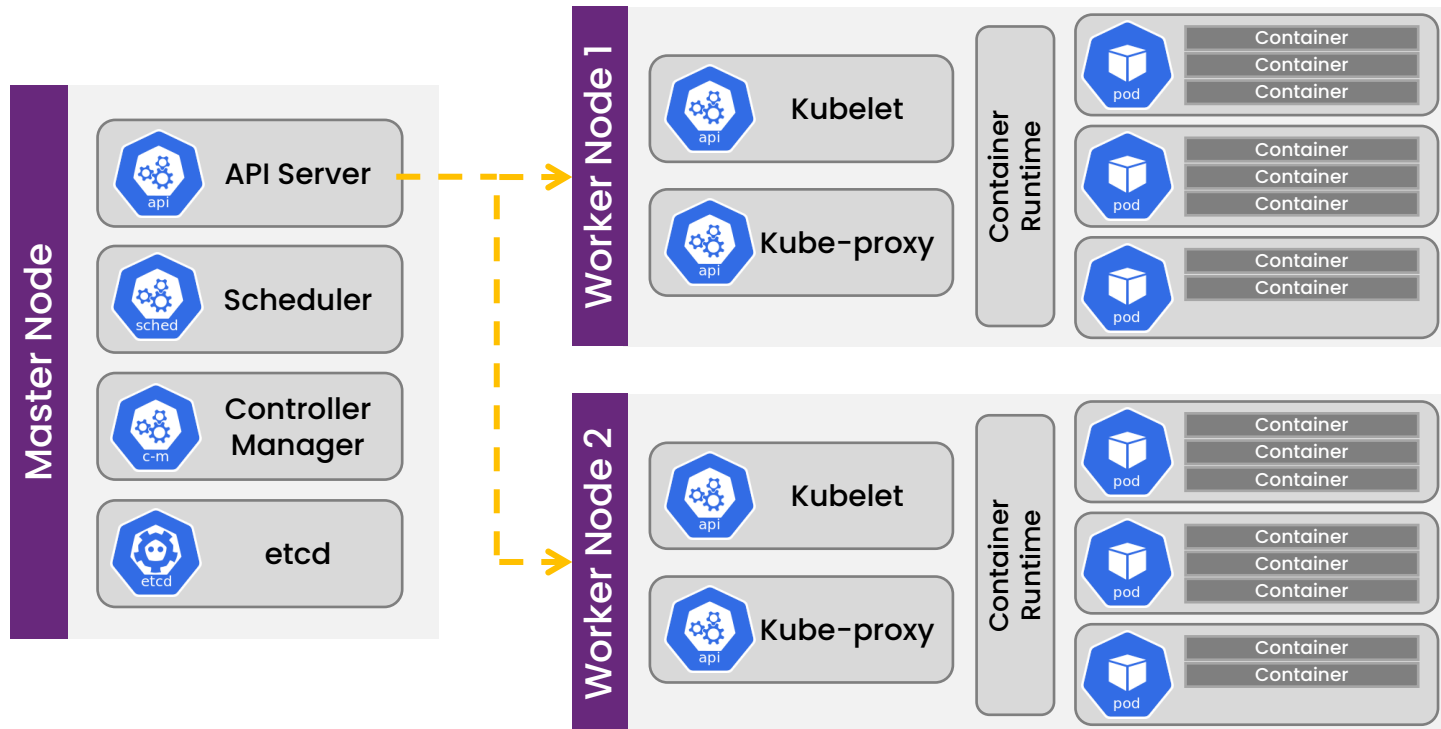
//

- ✓ Google에서 시작 (현재 Microsoft의 Brendan Burns이 공동 제작자)
- ✓ Apache License 2.0, 리눅스 재단 산하 Cloud Native Computing Foundation(CNCF)에서 관리 (오픈 소스)
- ✓ Go 언어로 작성
- ✓ 다양한 환경에서 구축 가능 (Physical, Virtual, Cloud, Hybrid)
- ✓ VM 호스트의 클러스터 간 컨테이너화 된 워크로드의 배포, 확장 및 운영 문제를 자동화
- ✓ 클라우드 네이티브를 위한 운영 체제로 변화

02. Kubernetes

Master Node & Worker Node

Kubernetes Cluster



Master Node

클러스터 운영 • 관리

- ✓ API Server
- ✓ Scheduler
- ✓ Controller Manager
- ✓ etcd

Worker Node

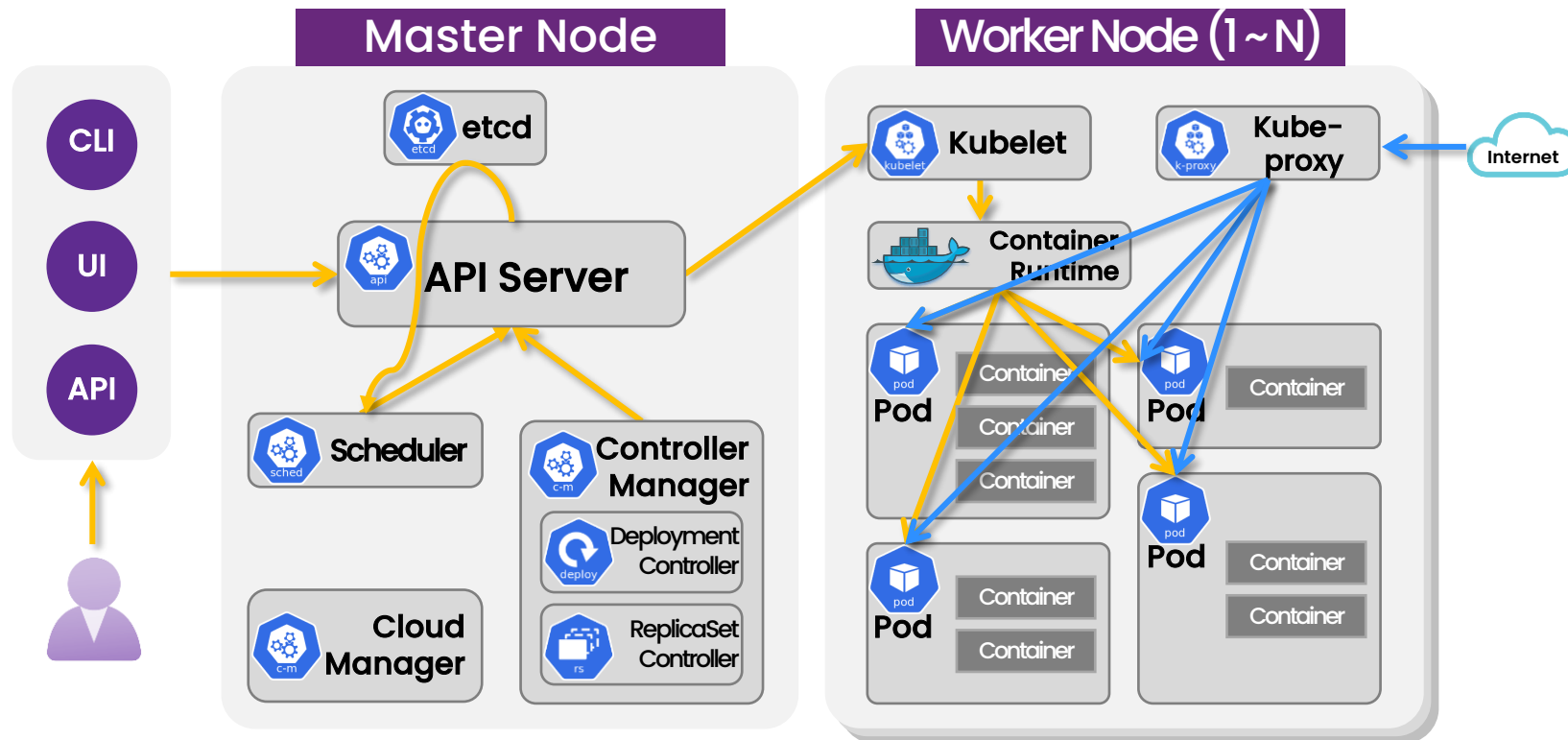
마스터 서버와 통신 및 Pod 생성

- ✓ Kubelet
- ✓ Kube-proxy
- ✓ Container Runtime
- ✓ Pod

02. Kubernetes

Kubernetes Architecture

Kubernetes Cluster



Master Node

API Server

Kubernetes의 오브젝트를 관리/제어하는 마스터의 핵심 모듈

etcd

클러스터의 모든 설정, 상태 데이터를 저장

Scheduler

Node가 배정되지 않은 새로 생성된 Pods를 감지하고 구동될 Node를 할당

Controller Manager

Kubernetes의 Object 상태를 관리

Worker Node

Kubelet

마스터 API 서버와 통신하는 노드 에이전트

Kube-proxy

Pod로 연결되는 네트워크 관리

Container Runtime

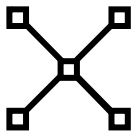
Pod의 컨테이너를 실행

Pod

Container들을 포함하는 기본 배포 단위

02. Kubernetes

Kubernetes 기능



Automatic Binpacking

Worker Node의 가용성을 유지하면서 보유한 리소스를 충분히 활용할 수 있도록 스스로 스케줄링하며 컨테이너를 배치함



Batch Execution

컨테이너 기반의 서비스 관리 뿐 아니라 배치 및 CI 작업 부하를 관리할 수 있어 원하는 경우 실패한 컨테이너 대체 가능



Automatic Rollbacks & Rollouts

컨테이너의 응용 프로그램이나 구성에 대한 변경 사항을 점진적으로 업데이트하고 문제 발생 시 자동으로 롤백 가능



Horizontal Scaling

CPU 사용률과 같은 metric을 기반으로 Pod의 Deployments, Replicaset을 스케줄링하여 수평적 확장 가능

02. Kubernetes

Kubernetes 기능



Secret & Configuration Management

Application 연동 및 접근 제어를 위한 보안 키, 설정 내용을 컨테이너 이미지의 변경 없이 업데이트할 수 있고 외부로 노출하지 않고 사용 가능



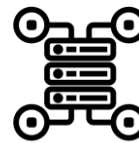
Service Discovery & Load Balancing

컨테이너에 IP 주소를 자동으로 할당하고 클러스터 내 트래픽을 로드 밸런싱할 수 있는 Pod에 단일 DNS 이름을 할당



Self Healing

컨테이너가 실패하거나 노드 장애 시 자동으로 다시 시작하고, 사용자가 정의한 헬스체크에 응답하지 않는 컨테이너를 종료



Storage Orchestration

로컬 저장소를 선택하거나 NFS, iSCSI 등과 같은 공유 네트워크 스토리지를 컨테이너에 할당/마운트하여 사용가능

03

Azure Kubernetes Service

03. Azure Kubernetes Service

Azure Kubernetes Service 란?



“

Azure의 PaaS 서비스로 호스팅되는 완전히 관리되는 Kubernetes 플랫폼

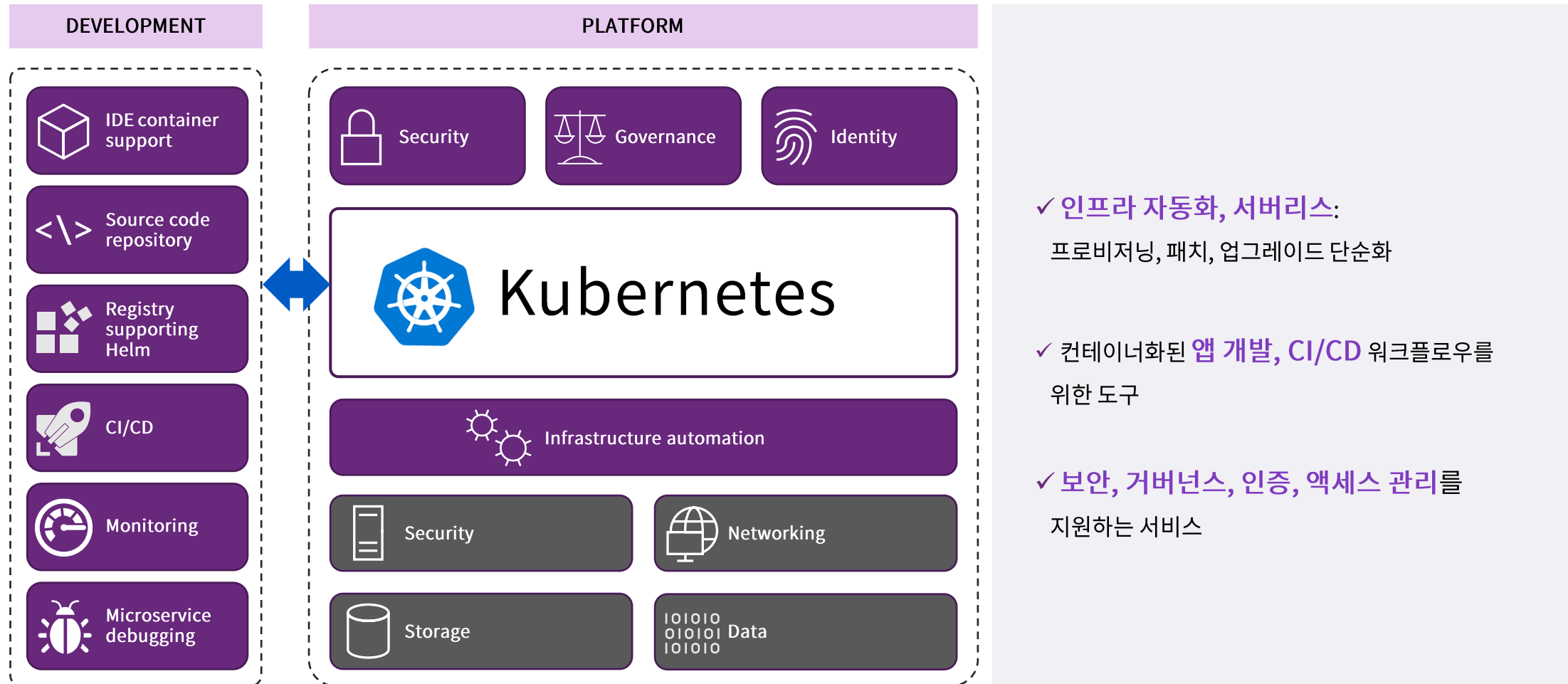
”

- ✓ Azure 클라우드는 퍼블릭 클라우드 공급 업체 중 가장 많은 서비스 지원 리전을 보유 (약 60개 이상)
- ✓ Kubernetes Service 리전 지원 (약 35개 이상), 현재도 확장 중
- ✓ Azure Service와 연계 및 연동 가능 (ACR, ACI, Azure DevOps, Azure Monitor 등)
- ✓ Kubernetes의 Master Node(Control Plane)와 Worker Node의 통합된 프로비저닝 및 관리 기능 제공

“Azure 클라우드에 맞겨, 본연의 **개발**과 **컨테이너화**에 더 집중하자”

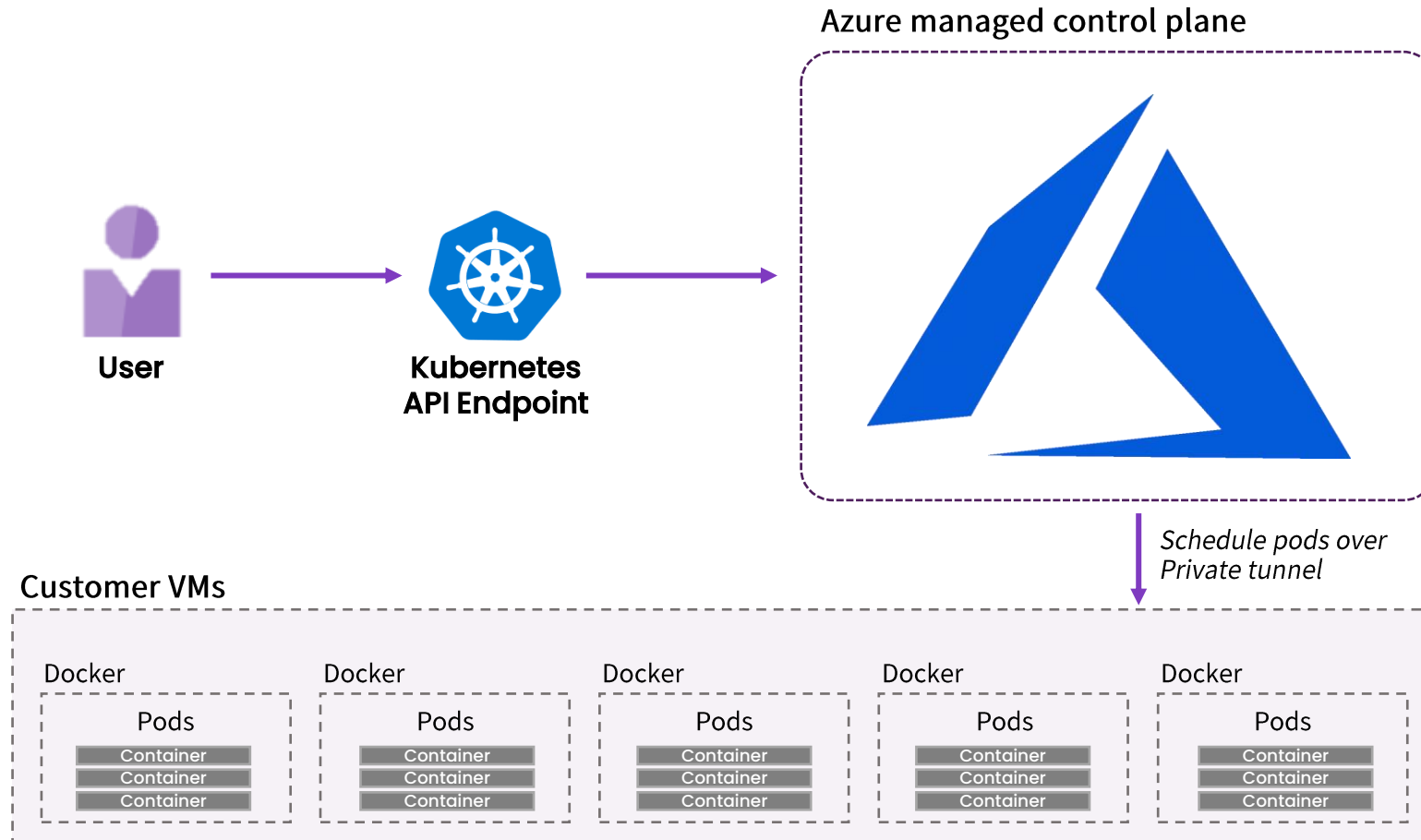
03. Azure Kubernetes Service

Azure Kubernetes Service 란?
















03. Azure Kubernetes Service



Azure Managed Kubernetes Service



03. Azure Kubernetes Service

Responsibilities

Responsibilities	DIY with Kubernetes	Managed Kubernetes on Azure
고려 항목	Containerization	
	Application iteration, debugging	
	CI/CD	
Cluster hosting		
Cluster upgrade		
Patching		
Scaling		
Monitoring and logging		

 Customer
 Microsoft

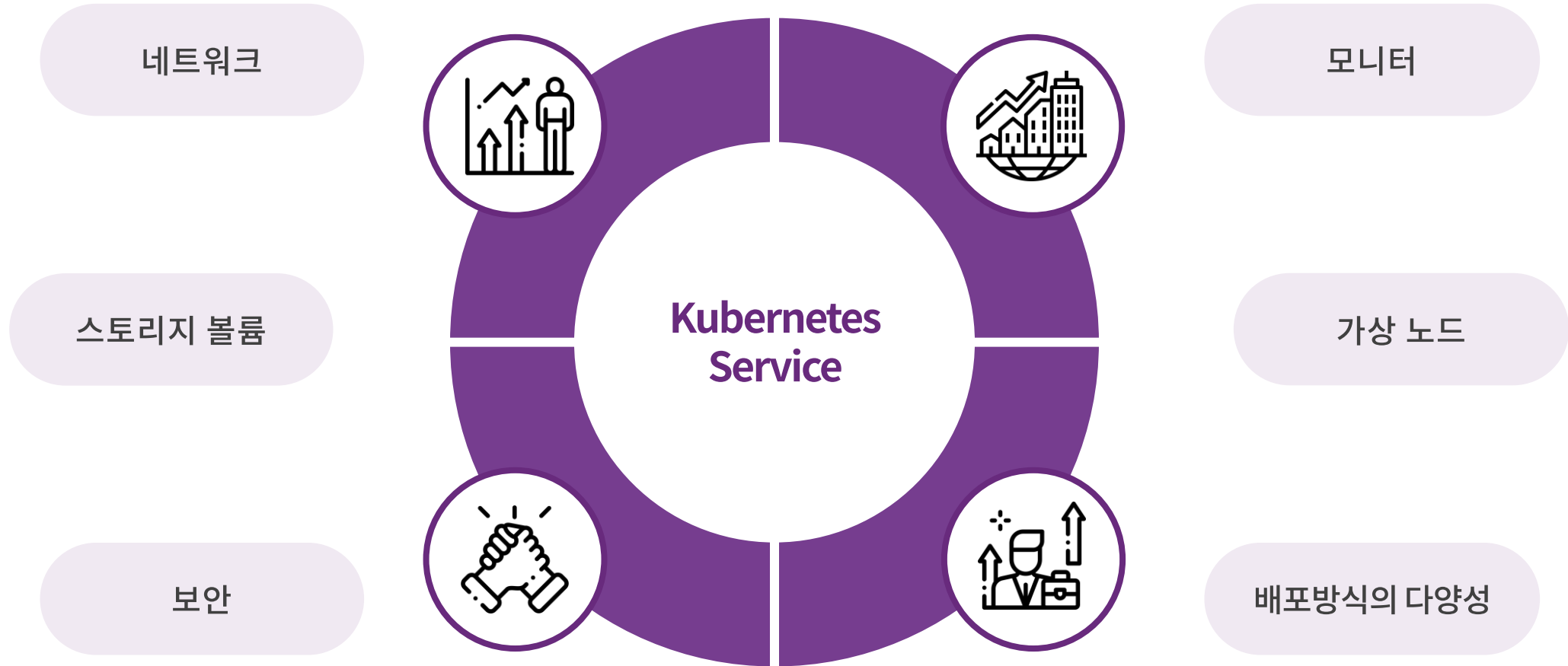
03. Azure Kubernetes Service

Azure Kubernetes Service 란?

- ✓ 서버리스 환경으로 제공
- ✓ 쿠버네티스 API서버의 작동시간을 99.99% 보장
- ✓ 쉽고 안전한 클러스터 Scale in/out
- ✓ Auto-Healing
- ✓ 업그레이드 및 패치가 자동으로 이뤄짐
- ✓ GPU 지원
- ✓ API 서버에 대한 로깅 및 모니터링 제공
- ✓ GitHub Actions, Azure DevOps와 통합지원
- ✓ 하드웨어 및 Master Node 비용 절감

03. Azure Kubernetes Service

Azure Kubernetes Service 기능



03. Azure Kubernetes Service

Azure Kubernetes Service 기능

Network

Kubenet

- Node만 Vnet의 IP 주소를 수신하고, 포드는 직접 통신 불가
- 수동으로 UDR 유지 관리
- NAT를 사용하여 외부 다른 리소스와 통신
- Azure Vnet의 리소스에 연결 가능하도록 NAT 사용
- 클러스터당 최대 노드 수 400개
- 각 노드 당 최대 110개 Pod 지원

AKS CNI(Container Networking Interface)

- Azure Vnet과 Pod간 통신을 연결 시켜주는 Bridge 역할
- Pod는 Subnet에서 IP주소를 할당 받아, 연결된 Vnet의 리소스에 액세스 가능
- Pod 트래픽 속도가 빠름
- 각 노드 당 최대 250개 Pod 지원
- 고급 기능 필요시 사용 (가상 노드, Azure 네트워크 정책 등)
- Vnet 엔드포인트를 사용하여, 프라이빗으로 연결 가능
- IP 주소범위 고갈 문제

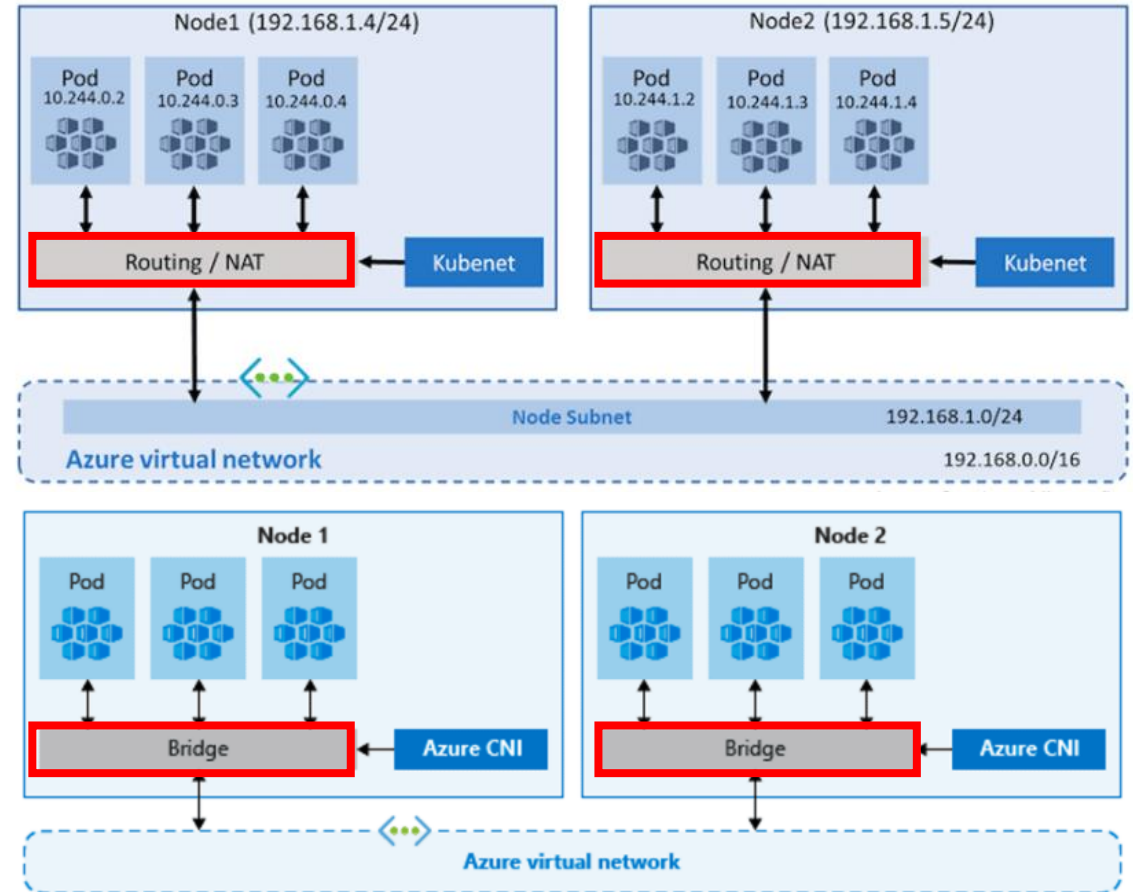


Image Courtesy: Microsoft

03. Azure Kubernetes Service

Azure Kubernetes Service 기능

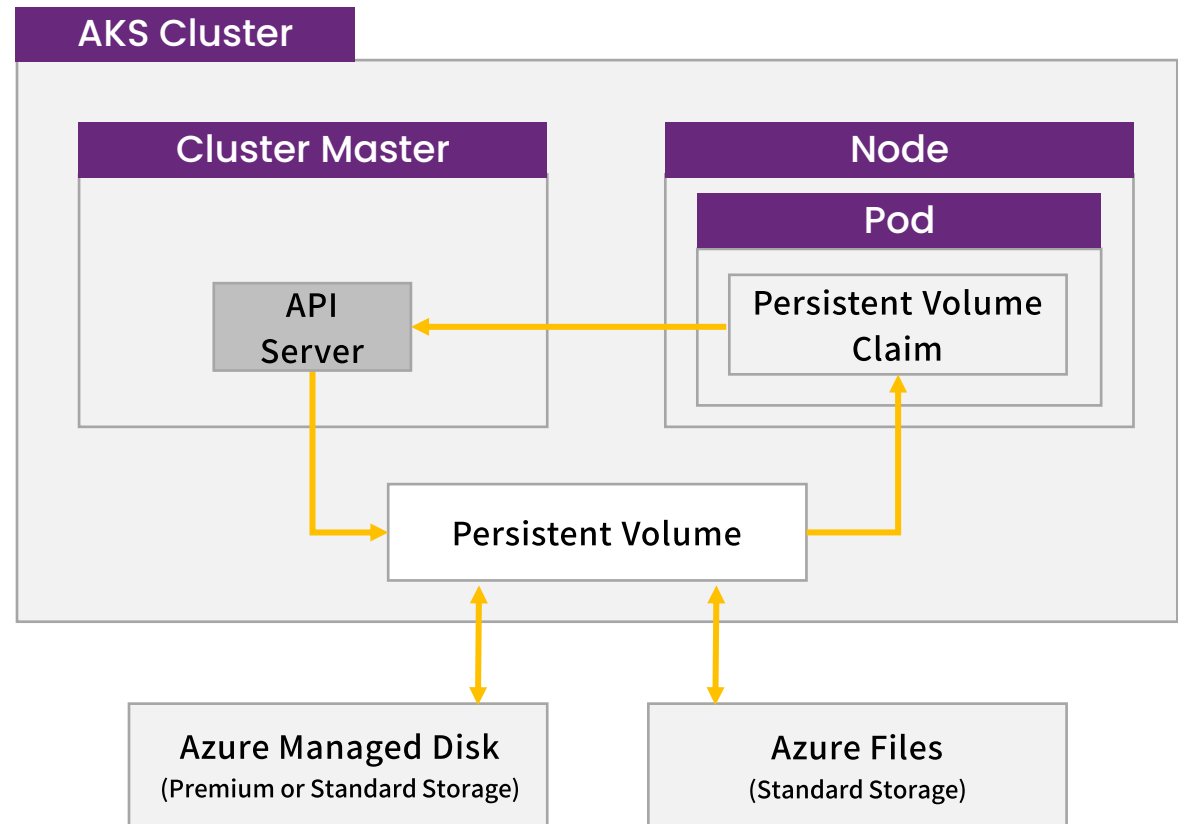
Storage Volume

Azure Disk

- ✓ .yaml 파일 설정만으로 Azure Disk를 볼륨으로 사용 가능
- ✓ HDD와 SSD Disk 제공 (Standard HDD, Premium SSD)
- ✓ 단일 Pod에서 사용 가능, 동시에 여러 Pod에 액세스 불가

Azure Files

- ✓ SMB 3.0 프로토콜을 통해 파일 공유
- ✓ HDD와 SSD Disk 제공 (Standard HDD, Premium SSD)
- ✓ 멀티 노드 및 Pod 간에 데이터를 공유가능



03. Azure Kubernetes Service

Azure Kubernetes Service 기능

Security

Azure Active Directory(AAD)

- ✓ Azure AD와 통합하여, AD에 등록된 사용자 및 사용자 그룹 ID를 기반으로 Kubernetes 액세스 가능
- ✓ Azure AD 인증 토큰으로 AKS 클러스터에 액세스 가능

Kubernetes RBAC (Role-Based Access Control)

- ✓ Kubernetes 클러스터에 대한 액세스 및 권한 제어

Azure Policy

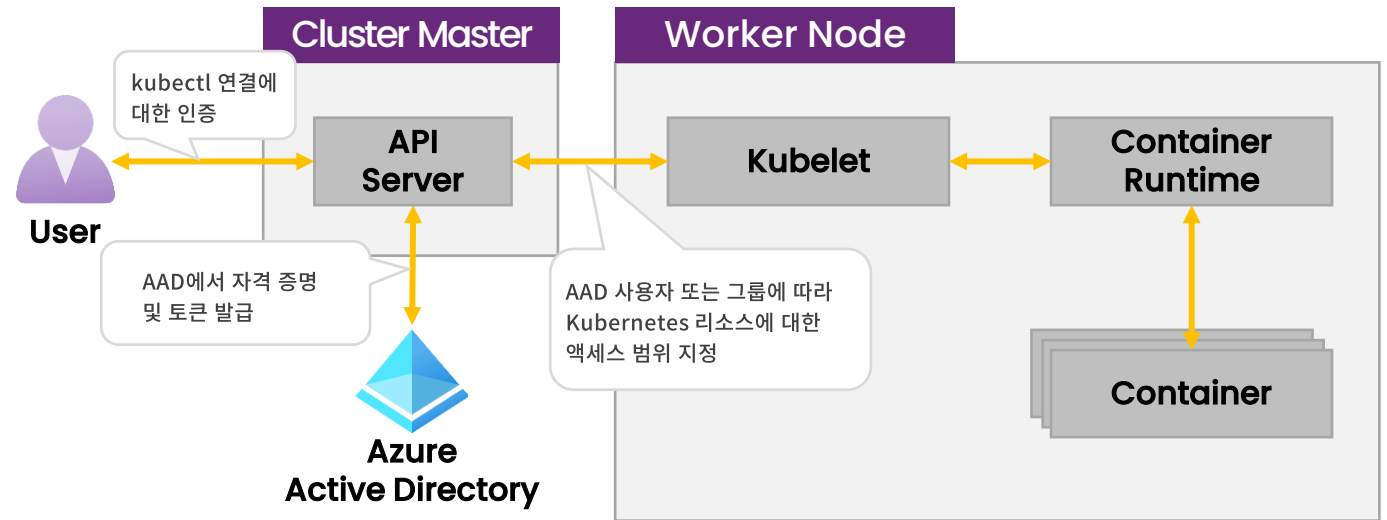
- ✓ Pod 레벨에서의 보안 적용

Azure Security Center

- ✓ 취약점 관리, 위협 탐지 및 모니터링

Azure Private Link

- ✓ Vnet의 프라이빗 엔드포인트로 서비스 간 통신 보호



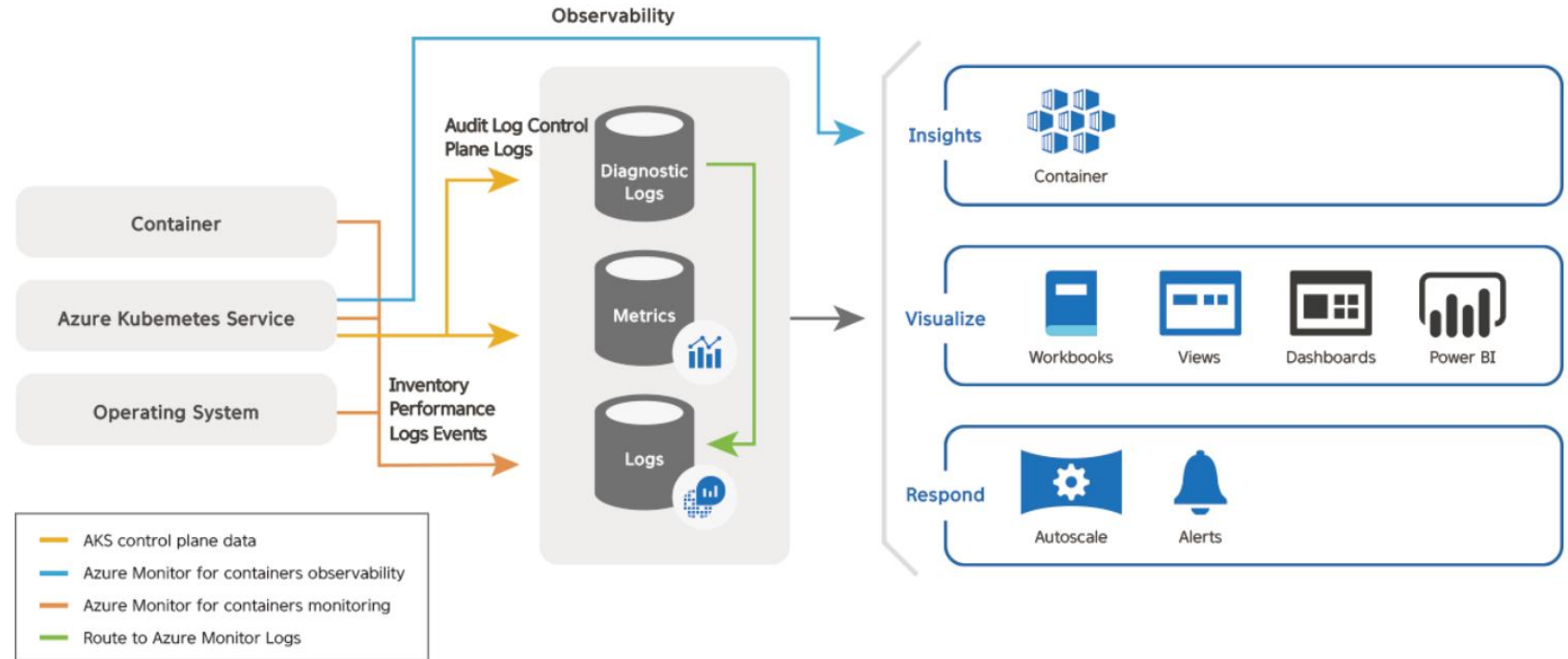
03. Azure Kubernetes Service

Azure Kubernetes Service 기능

Monitor

Container Insight

- ✓ AKS 클러스터 및 배포된 애플리케이션 내의 컨테이너, 노드 및 컨트롤러에서 메모리 및 프로세서 성능 메트릭을 수집하여 시각적으로 표시
- ✓ Azure Log Analytics 작업 영역에 저장
- ✓ Azure Portal, Azure CLI 또는 REST 엔드포인트를 통해 사용 가능



03. Azure Kubernetes Service

Azure Kubernetes Service 기능

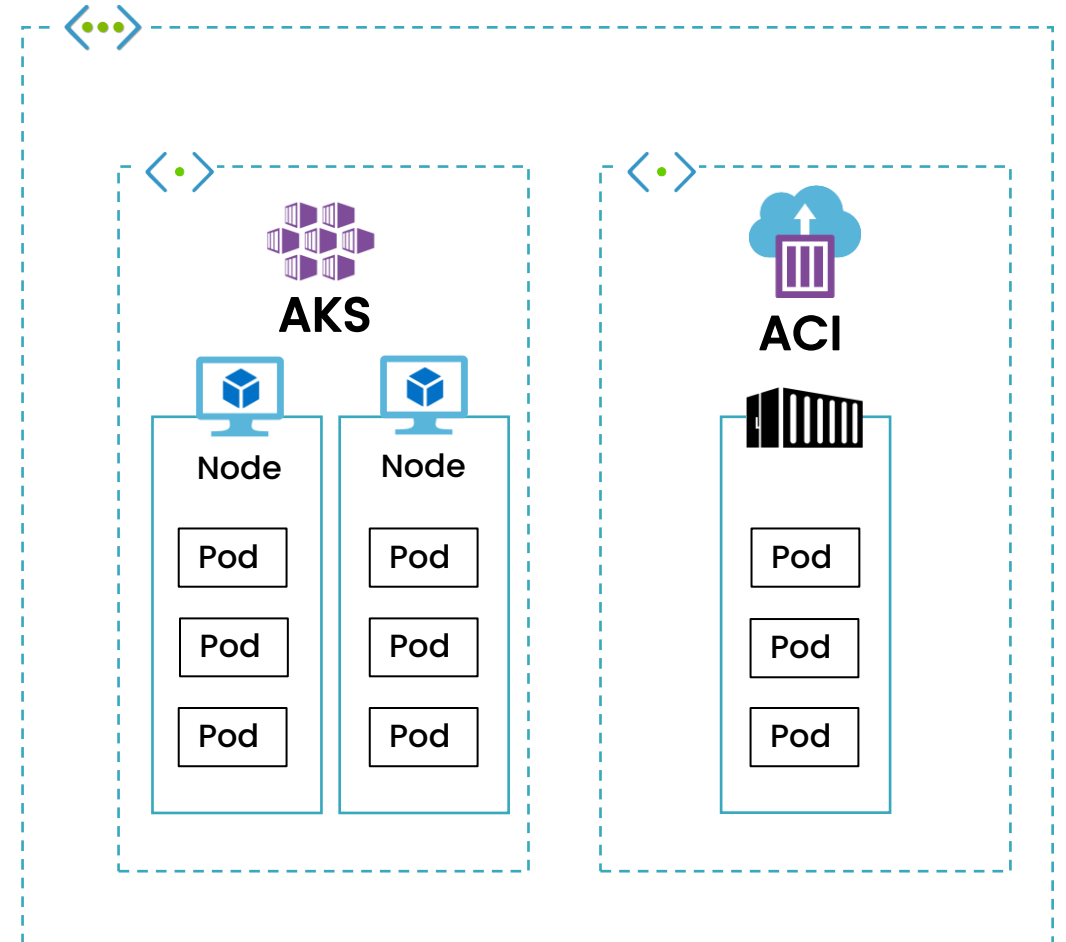
가상노드 (Virtual Node)

Azure Container Instance (ACI)

- ✓ Azure에서 컨테이너를 실행하기 위한 가장 빠르고 간단한 서비스
- ✓ Virtual Node 지원

Virtual Node

- ✓ AKS 클러스터에서 애플리케이션 워크로드를 빠르게 확장하기 위해 사용
- ✓ ACI에 Pod를 빠르게 프로비저닝 가능하며, 실행 시간에 대해서만 비용 지불
- ✓ 동적으로 생성 및 삭제가 가능하며, 관리가 편리
- ✓ 신규 Node가 배포되는 시간보다 ACI를 Node로 배포하는 시간이 훨씬 빠름
- ✓ ACI에서 실행되는 Pod와 AKS 클러스터에서 실행되는 간의 네트워크 통신 가능
- ✓ Azure CNI를 사용하는 클러스터에서 사용 가능
- ✓ Azure Files만 지원

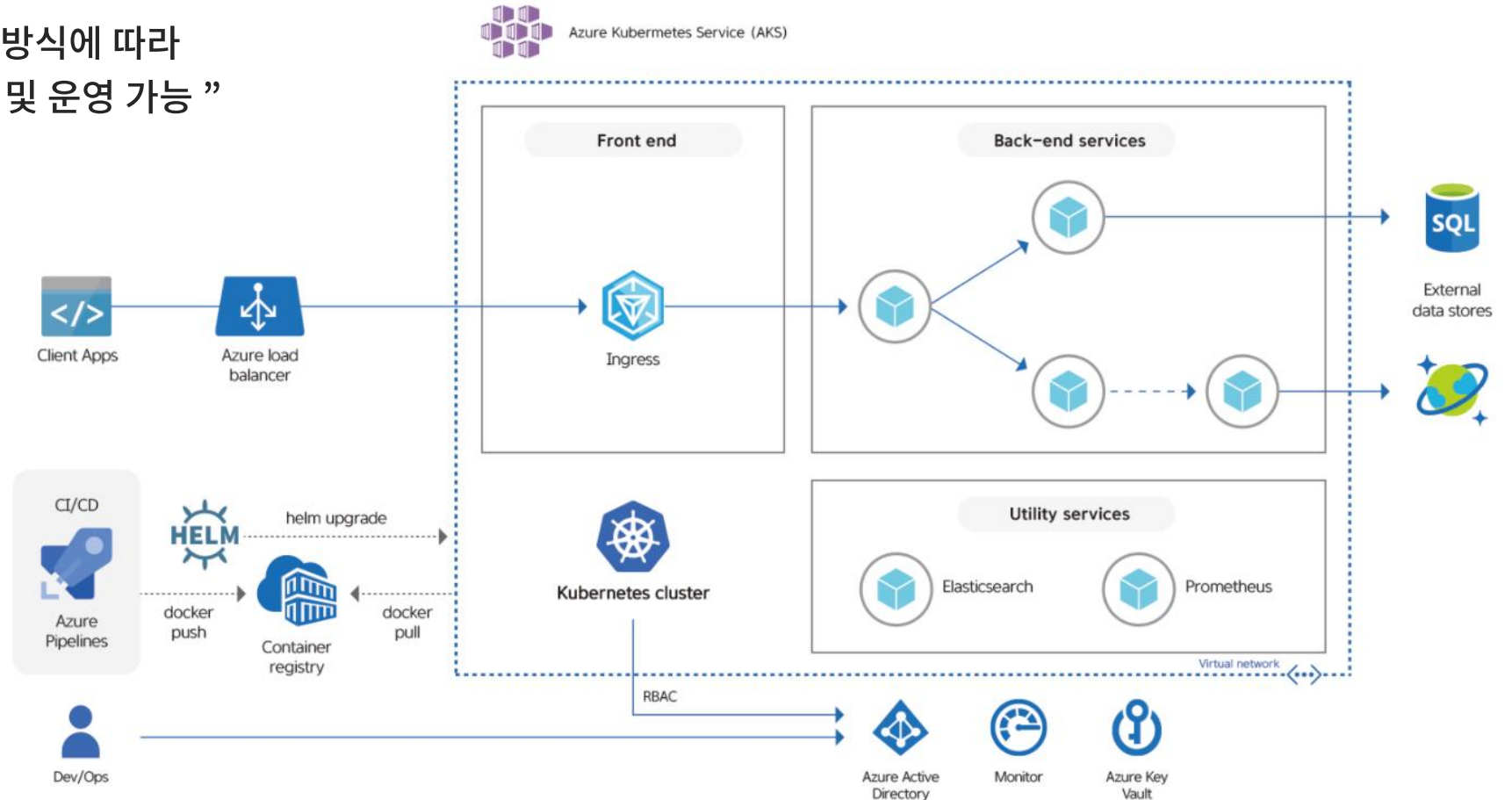


03. Azure Kubernetes Service

다양한 배포 방식

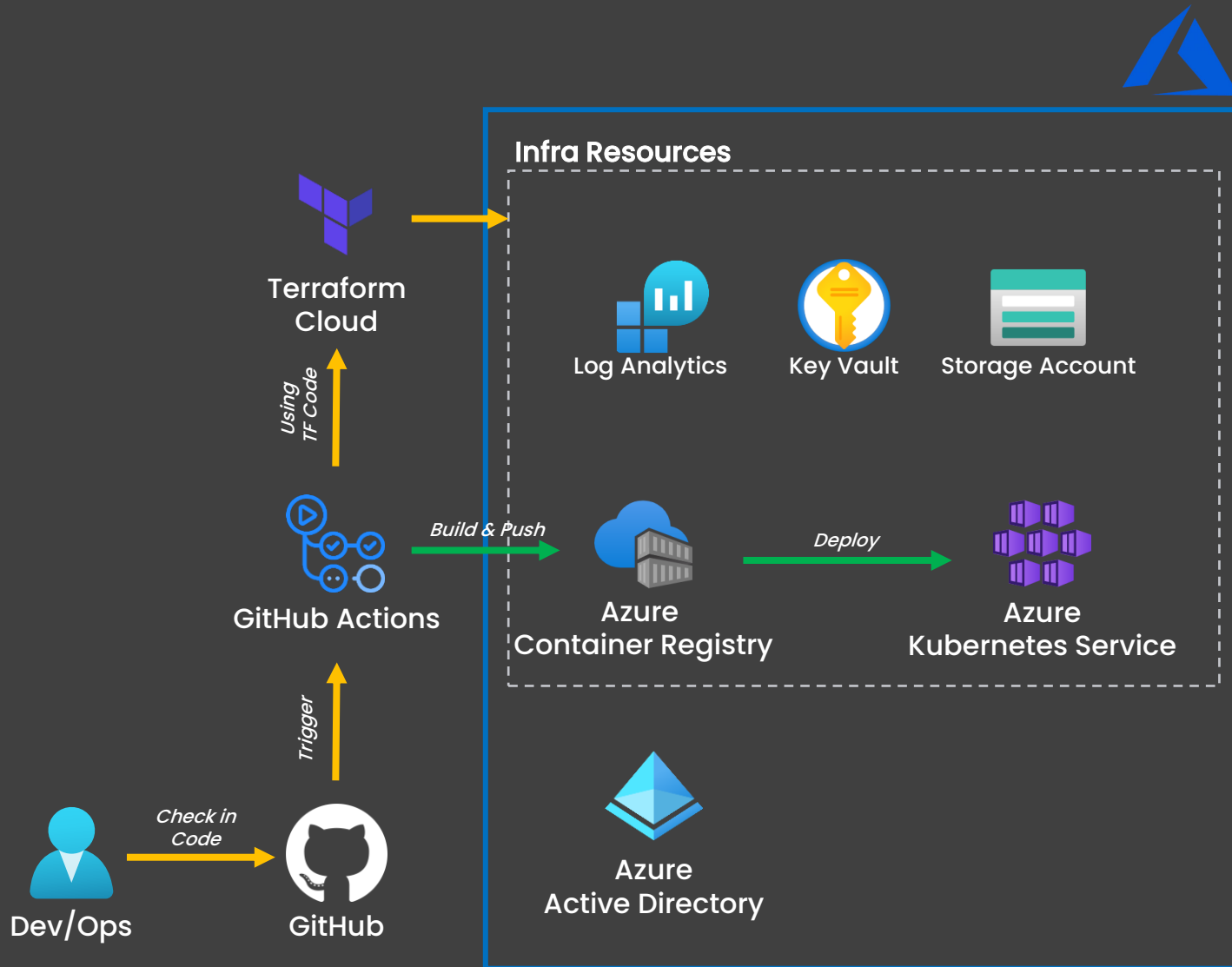
“ AKS를 활용하면 배포 방식에 따라 다양한 아키텍처를 구성 및 운영 가능 ”

- ✓ Azure DevOps 및 GitHub의 Git Actions를 통해 CI/CD로 구성 가능
- ✓ Azure Container Registry에 업로드한 이미지로 Private 환경에서 배포 가능
- ✓ Docker Hub의 Public 이미지 활용 가능



04 / Demo

DEMO



- ✓ Pipeline :
Terraform 인프라 배포 후,
애플리케이션 배포
- ✓ Terraform :
AKS, Vnet, Subnet, ACR, Log Analytics 생성
- ✓ Application :
MS Docs에서 제공하는 Voting App 배포
(Vote-Front와 Vote-Back(Redis)으로 구성)
- ✓ AKS :
VMSS를 사용한 3개의 노드, CNI로 구성
- ✓ ACR, Key Vault, Storage Account

→ : Step 1

→ : Step 2

05 / Summary



KCSP (Kubernetes Certified Service Provider)

//

CNCF 회원사로서 **CKA** (공인 쿠버네티스 관리자) 자격을 갖춘 다수의 엔지니어와

실제 쿠버네티스 **구축 경험**과 구체적인 서비스 모델을 통해 **기술역량과 전문성을 입증**

//



Thank you!

Drive your Digital Transformation with Cloocus

Cloocus

Gold
Microsoft
Partner


Azure
Expert
MSP