

# AKS 아키텍처 가이드

Cloud\_서비스/세일즈 툴킷

Exported on 06/19/2023

## Table of Contents

<b>1 AKS 1. 테스트 아키텍처 .....</b>	<b>5</b>
1.1 AKS 개요.....	5
1.2 아키텍처 구성 .....	5
1.3 AKS 기반의 Microservice CI/CD 아키텍처 .....	5
1.4 AKS vs. ACI vs. Container Services.....	6
1.4.1 AKS(Azure Kubernetes Services) .....	7
1.4.2 ACI(Azure Container Instances) .....	7
1.4.3 Container Services .....	7
1.4.4 Service Fabric Clusters.....	7
1.4.5 App Services .....	7
1.5 AKS와 Kubernetes 비교.....	8
<b>2 AKS 2. 플랫폼 테스트 결과 .....</b>	<b>10</b>
2.1 테스트 결과 요약.....	10
2.2 테스트 결과 상세 .....	10
<b>3 AKS 3. 어플리케이션 테스트 결과.....</b>	<b>17</b>
3.1 테스트 결과 요약 .....	17
3.2 테스트 결과 상세 .....	17
<b>4 AKS 4. 도입/구축 시 고려사항 .....</b>	<b>24</b>
4.1 서비스 리전 .....	24
4.1.1 Region .....	24
4.1.2 Geographies .....	25
4.1.3 Availability Zones .....	27
4.2 AKS(Azure Kubernetes Service) 제공 Region .....	28
4.3 비용 산정 .....	29
4.3.1 Container Registry .....	29
4.3.2 SKU 상세 서비스 .....	30
4.3.3 AKS(Azure Kubernetes Service) .....	30
4.4 AKS 클러스터 네트워크 옵션 .....	30
4.4.1 Basic 네트워킹 .....	31
4.4.2 Advanced 네트워킹 .....	31

4.5 Cloud shell 소개.....	33
4.5.1 기본 제공되는 유틸리티 목록 .....	34
4.5.2 프로그래밍 언어 지원 .....	35
4.6 Resource Group.....	35

**Public Cloud**에서 컨테이너 형태로 어플리케이션을 개발 및 운영하고자 하는 경우 활용할 수 있는 방법을 정리합니다.  
각 **Cloud Service Provider**가 제공하는 관리형 **Kubernetes** 서비스를 대상으로 플랫폼 관리 영역과 어플리케이션 개발 영역으로 나눠 서비스의 기능을 비교하고  
어플리케이션을 개발 및 관리하는 방법을 가이드합니다.

AKS 1.테스트 아키텍처(see page 5)

AKS 2.플랫폼 테스트 결과(see page 4)

AKS 3.어플리케이션 테스트 결과(see page 4)

AKS 4.도입/구축 시 고려사항(see page 4)

# 1 AKS 1. 테스트 아키텍처

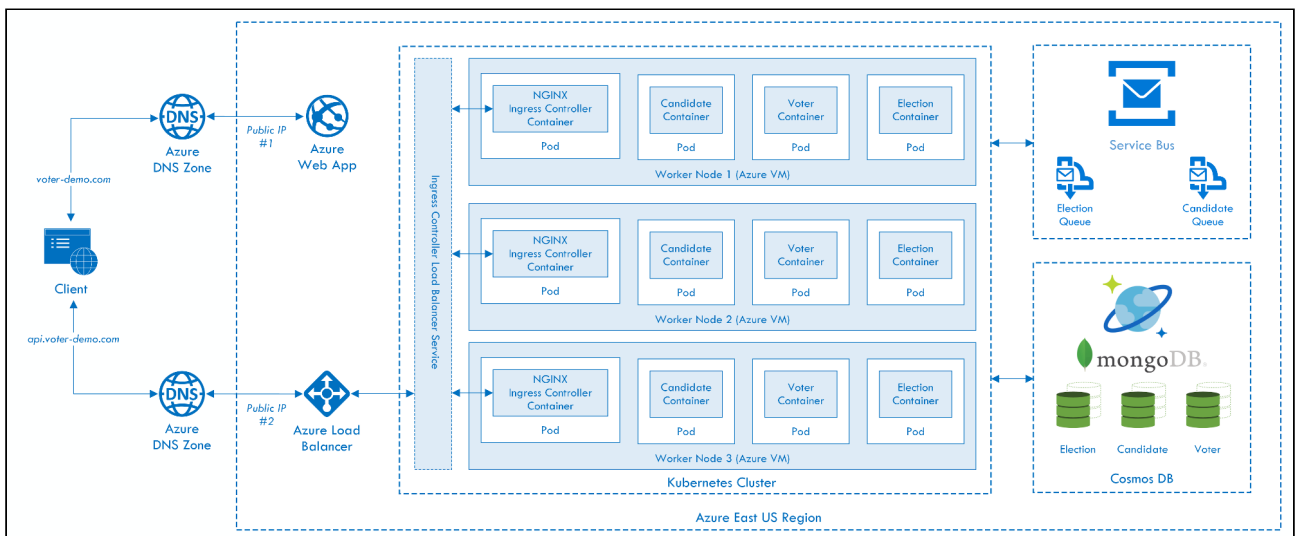
Microsoft Azure AKS(Azure Kubernetes Service)를 활용하여 어플리케이션을 개발하고 관리할 때 주로 활용하게 되는 Azure Cloud Platform의 서비스와 아키텍처 구성에 대해 개괄적으로 설명합니다.

## 1.1 AKS 개요

AKS(Azure Kubernetes Service)는 Azure Cloud Platform 기반에 컨테이너식 애플리케이션 배포를 위한 관리형 환경입니다. AKS 클러스터는 Kubernetes 명령 및 Resource를 사용하여 응용 프로그램을 배포 및 관리 하고 자동 배포를 위한 배포 정책 설정과 어플리케이션 상태 모니터링 서비스를 제공합니다.

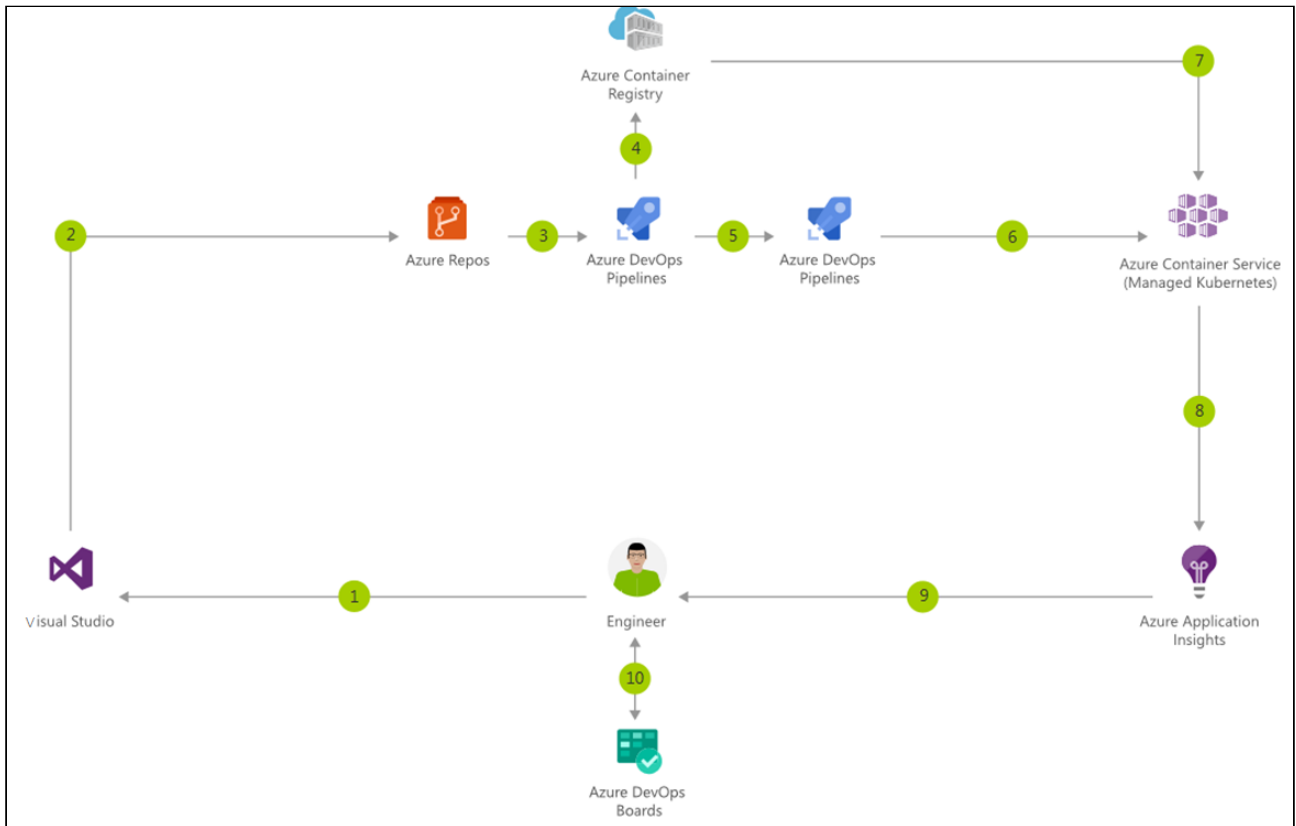
## 1.2 아키텍처 구성

형상관리, CI/CD, 컨테이너 레지스트리, 런타임 어플리케이션, 데이터베이스, 로깅/모니터링 등을 어플리케이션 라이프 사이클 관점에서 구성하는 방법을 정의한다.



## 1.3 AKS 기반의 Microservice CI/CD 아키텍처

Container 서비스를 통해 매우 손쉽게 응용 프로그램을 지속적으로 빌드 및 배포할 수 있습니다. AKS(Azure Kubernetes Service)에서 Kubernetes를 사용하여 해당 컨테이너의 배포를 오케스트레이션하는 방식으로 컨테이너를 복제 가능하고 관리 가능한 클러스터를 구성 할 수 있습니다.



## 1.4 AKS vs. ACI vs. Container Services

Microsoft Azure에서는 다양한 종류의 Container Service를 제공하고 있습니다. 최종 목적은 컨테이너 서비스에 Microservice 기반 애플리케이션을 개발/배포하기 위한 편리한 환경을 제공하는것이지만 비용/용도/개발환경에 따라 다양한 기능과 기술지원이 필요하기 때문에 사용자가 목적에 맞게 선택 할 수 있도록 다양한 컨테이너 환경을 지원하고 있습니다.

- AKS(Azure Kubernetes Services)
- ACI(Azure Container Instances)
- Container Services
- Service Fabric Clusters
- App Services

### 1.4.1 AKS(Azure Kubernetes Services)

AKS(Azure Kubernetes Service)는 완벽한 관리형 Kubernetes 환경 제공하며 Container 오케스트레이션에 대한 전문 지식 없이 컨테이너화된 응용 프로그램을 빠르고 쉽게 배포하고 관리할 수 있는 클러스터 구성 환경을 제공합니다. 또한 응용 프로그램을 오프라인으로 변경하지 않고 온라인으로 클러스터 추가 리소스를 프로비전하고, 업그레이드하고, 크기 조정하여 진행 중인 작업 및 유지 관리를 간편하게 할 수 있습니다. 또한 사용자 요구사항에 맞도록 VPC Network을 구성하거나 다른 Azure 서비스와 연계가능한 Container 서비스 환경을 만들 수 있습니다.

### 1.4.2 ACI(Azure Container Instances)

Container Instances는 클라우드 응용 프로그램을 패키지, 배포 및 관리하기 위한 기본 환경을 제공합니다. ACI는 컨테이너 서비스를 제공하는 가상 머신을 직접 관리하지 않고 Azure에서 컨테이너를 실행하는 가장 빠르고 간단한 방법을 제공합니다. Azure Container Instances는 간단한 응용 프로그램, 작업 자동화 및 빌드 작업 등 간단하게 격리된 컨테이너 실행 환경이 필요한 경우에 적합한 솔루션입니다. 여러 컨테이너 간 서비스 검색, 자동 크기 조정 및 조정된 응용 프로그램 업그레이드를 포함하여 전체 컨테이너 오케스트레이션이 필요한 환경에는 AKS(Azure Kubernetes Service)가 좀더 적합합니다.

### 1.4.3 Container Services

Azure Container Service는 Azure Portal, Azure 명령줄 도구 및 Azure API의 기능이 포함된 SLA 기반 Azure 서비스입니다. 이 서비스는 몇가지 구성 옵션을 통해 표준 컨테이너 오케스트레이션 도구(DC/OS, Docker Swarm, Kubernetes)를 선택하고 실행하는 클러스터를 신속하게 구현하고 관리할 수 있습니다. ACS Engine은 고급 사용자가 모든 수준의 클러스터 구성을 사용자가 변경하여 사용할 있는 오픈 소스 프로젝트입니다. 인프라 및 소프트웨어 양쪽의 구성을 변경하는 기능이 있기 때문에 ACS Engine용 SLA는 Azure에서 제공되지 않으며 운영자 담당자가 직접 모든 서비스를 관리하는 환경에 사용할 수 있습니다. 현재 Container Service는 서비스 종료 예정입니다.

### 1.4.4 Service Fabric Clusters

Azure Service Fabric은 손쉽게 패키징하고 배포하며 확장 가능하고 안정성이 뛰어난 마이크로 서비스 및 컨테이너를 관리하도록 배포된 시스템 플랫폼입니다. 또한 Service Fabric은 클라우드 네이티브 응용 프로그램 개발 및 인프라 관리를 간편하게 제공할 수 있습니다. 개발자와 관리자가 복잡한 인프라 문제를 피하고 업무 수행에 필수적인 까다로운 어플리케이션을 확장 가능하고 안정적인 서비스를 제공하므로 개발자는 어플리케이션을 구현하는 데 집중할 수 있습니다. Service Fabric은 컨테이너에서 실행되는 엔터프라이즈급 Level1 클라우드 규모의 응용 프로그램을 빌드 및 관리하기 위한 차세대 플랫폼 서비스입니다.

### 1.4.5 App Services

Windows와 Linux에서 사용할 수 있는 Azure Web App을 통해 개발자는 인프라 관리에 대해 걱정할 필요 없이 다양한 언어로 작성되고 다수의 서비스와 통합된 엔터프라이즈급 웹 응용 프로그램을 손쉽게 배포하고 확장할 수 있습니다. Web App for Containers 을 통해 개발자는 고유한 Docker 형식의 컨테이너 이미지를 가져와서 Azure에서 대규모로 쉽게 배포하고 실행할 수 있습니다. Azure Functions는 기존 Azure App Service 플랫폼을 확장하는, 서버를 사용하지 않는 이벤트 구동 환경입니다. 매우 작은 리소스를 사용하는 어플리케이션에 적합하며 크기를 조정할 수 있으므로 사용한 리소스에

대해서만 비용을 지불합니다. Azure API Apps를 사용하여 다양한 언어로 작성된 API를 쉽게 빌드, 호스팅 서비스를하는 데 이용할 수 있습니다.

구분	AKS(Azure Kubernetes Services)	ACI(Azure Container Instances)	Web App for Containers
비용	<ul style="list-style-type: none"> <li>- VM Instance 사용료 기준와 스토리지/네트워킹 리소스 사용료</li> <li>- Kubernetes 클러스터 마스터 노드를 제외한 worker node 및 Infra resource 사용료</li> </ul>	<ul style="list-style-type: none"> <li>- 컨테이너 그룹의 CPU/Memory 사용량 기준(초)</li> <li>- vCPU당 0.000014\$ / Memory 1GB 0.000005\$</li> </ul>	<ul style="list-style-type: none"> <li>- 어플리케이션 요금제 기반 사용료 지불(시간)</li> <li>- Free and Shared(Preview), Basic/Standard/Premium 서비스 요금제</li> <li>- vCPU/Memory/Storage에 따른 시간당 단가 차이가 있음.</li> </ul>
스케일링	<ul style="list-style-type: none"> <li>- VM 인스턴스 확장 방식</li> <li>- 컨테이너 배포 상태에 따라 VM 인스턴스 확장 축소 가능</li> <li>- 클러스터 VM 인스턴스는 수동으로 확장/축소 가능하며 Pods는 Kubernetes 자체 기능으로 auto scaling 구성 가능함.</li> </ul>	<ul style="list-style-type: none"> <li>- 컨테이너 그룹은 동일한 호스트 시스템내에서 예약된 컨테이너 자원임.</li> <li>- 컨테이너 그룹은 lifecycle, network, storage volume을 공유하며 Kubernetes의 Pods와 유사함.</li> <li>- 가용성 확보를 위해서는 멀티 컨테이너 그룹을 구성해야 하며 현재 멀티 컨테이너 그룹은 Linux 컨테이너만 지원함.</li> </ul>	<ul style="list-style-type: none"> <li>- 어플리케이션 사용상태에 따라 다양한 조건의 auto scaling 정책 적용이 가능함.</li> <li>- CPU/Memory 사용량 같은 자원사용 기준뿐 아니라 날짜/시간등의 auto scaling 설정도 가능함.</li> </ul>
모니터링 지원 도구	<ul style="list-style-type: none"> <li>- Azure VM 인스턴스에서 제공하는 다양한 모니터링 서비스 및 Kudu 제공</li> </ul>	<ul style="list-style-type: none"> <li>- 컨테이너 로그 및 Alert 로그 제공하는 수준으로 프로덕션 서비스로 제공하기에는 부족함.</li> <li>- 호스트 자체 장애시 로그 제공 불가함.</li> </ul>	<ul style="list-style-type: none"> <li>- 어플리케이션 분석을 위한 Kudu 및 서비스 요금제 등급에 따른 다양한 모니터링 서비스 제공</li> </ul>
기타 기능	<ul style="list-style-type: none"> <li>- 공인 아이피, DNS 및 SSL 구성 가능</li> </ul>	<ul style="list-style-type: none"> <li>- 공인 아이피, DNS 제공하나 SSL 구성 불가능함.</li> </ul>	<ul style="list-style-type: none"> <li>- 공인 아이피, DNS(서비스 요금제에 따라 다름) 및 SSL 구성 가능</li> </ul>

## 1.5 AKS와 Kubernetes 비교

오픈소스 Kubernetes 대비 AKS(Azure Kubernetes Service)가 제공하는 차별적인 기능에 대해 소개한다.



- 액세스 관리 : Azure 포털의 Identity 카테로그의 서비스를 활용하여 계정 및 역할 권한으로 클러스터의 액세스 권한을 관리함
  - 네트워킹 : AKS Advanced 네트워크 옵션을 이용해 컨테이너 클러스터에 하이브리드 네트워킹을 구성이 가능함
  - 보안 및 규정 : AKS 보안팀이 Kubernetes Engine을 지원하며 HIPAA 및 PCI DSS 3.1 규정을 모두 준수
  - 통합 로깅 및 모니터링 : Monitoring 카테고리의 Logs, Metrics, Insights(Preview) 기능을 사용 설정하면 애플리케이션 실행 상태를 손쉽게 확인이 가능함
  - 자동 업그레이드 : Kubernetes의 최신 출시 버전으로 클러스터를 자동으로 최신 상태로 유지 할수 있으며 N-4 버전까지 지원함.
  - 완전 관리형 서비스 : AKS Kubernetes Engine을 완전하게 관리하므로 클러스터의 가용성이 보장되고 최신 상태로 유지됨
  - Private Container Registry : Azure Container Registry와 통합하면 손쉽게 Private Docker 이미지를 저장하고 액세스가 가능함
  - 신속한 빌드 : DevOps 서비스를 사용하여 Kubernetes Engine에서 안정적으로 컨테이너를 배포 및 CI/CD 구성이 가능함.
  - 사용 편의성 : 콘솔 화면 내에 터미널 접속 기능이 있어, 별도의 CLI 설치 작업 없이 손쉽게 사용이 가능함
- 
- [AKS 개요](#)(see page 5)
  - [아키텍처 구성](#)(see page 5)
  - [AKS 기반의 Microservice CI/CD 아키텍처](#)(see page 5)
  - [AKS vs. ACI vs. Container Services](#)(see page 6)
    - [AKS\(Azure Kubernetes Services\)](#)(see page 7)
    - [ACI\(Azure Container Instances\)](#)(see page 7)
    - [Container Services](#)(see page 7)
    - [Service Fabric Clusters](#)(see page 7)
    - [App Services](#)(see page 7)
  - [AKS와 Kubernetes 비교](#)(see page 8)

## 2 AKS 2. 플랫폼 테스트 결과

### 2.1 테스트 결과 요약

Microsoft Azure에서 서비스중인 AKS(Azure Kubernetes Service) 플랫폼 서비스는 전체적으로 Google GKE 플랫폼과 유사하지만 세부적인 기능 옵션 및 자동화 관련 기능에서 일부 부족한 부분이 있는것으로 보인다. 그러나 모니터링 통합 기능 및 서비스들의 카테고리별 재그룹핑등은 사용자가 직관적으로 사용하기에 편리한 구성으로 보인다. 그리고 다른 퍼블릭 클라우드 서비스에서 사용하는 Region 및 AZ(Availability Zone) 개념이 일부 차이가 있으므로 플랫폼 가용성 확보를 위한 아키텍처 설계시 검토가 필요할 것으로 보인다.

### 2.2 테스트 결과 상세

구분	항목	설명	배점	가중치	Azure Kubernetes Service	
					평가결과	평가의견
설치/변경	Host OS 설치/구성 자동화	VM의 OS 설치 및 구성이 자동화 되는가	20	1	2	<ul style="list-style-type: none"> <li>- 기능 지원</li> <li>- CLI 및 GUI로 클러스터 생성이 가능하며 최신버전에서 N-4 버전까지 설치 버전 선택 가능</li> <li>- 한국 Region에는 현재 서비스 지원 안됨.</li> <li>- 설치되는 호스트 OS는 Linux(Ubuntu)이며 별도 버전 선택은 할 수 없음.</li> <li>- 클러스터 생성시 노드 수 및 노드 스펙(CPU,Memory)선택 및 변경이 가능하며 클러스터 노드 auto scaler 기능은 없음.</li> <li>- 클러스터 노드가 배치되는 AZ 또는 Region 선택할 수 없음.</li> </ul>
	Host OS 업그레이드 자동화	VM의 OS Upgrade가 플랫폼 중단 없이 자동화 되는가		1	0	<ul style="list-style-type: none"> <li>- 지원 안됨</li> <li>- 제공되는 host cluster OS 버전은 선택 불가함</li> <li>- Ubuntu LTS 버전이 설치되며 GEK와 달리 제공되는 별도의 customized 된 OS는 없음.</li> </ul>

구분	항목	설명	배점	가중치	Azure Kubernetes Service	
					평가결과	평가의견
	Host OS 다운그레이드 자동화	VM의 OS Downgrade가 플랫폼 중단 없이 자동화 되는가		1	0	- 지원 안됨 - 제공되는 host cluster OS 버전 선택 및 다운그레이드 기능은 제공 되지 않음
	플랫폼 설치	플랫폼 최초 설치 (플랫폼 권장하는 버전으로) 되는가		3	3	- 기능 지원 - AKS 플랫폼 default 버전 및 최신 버전 및 N-4 버전 설치/업그레이드 가능 버전 제공
	플랫폼 설치 정의서	정의서(예: Manifest YAML)를 통해 설치가 자동화 되는가.		2	2	- 기능 지원 - YAML 또는 등록된 플랫폼 템플릿을 통한 설치 기능 지원
	플랫폼 설치 정의서의 민감정보 분리 보관	정의서에서 민감한 정보 (예: 계정, 비번, 인증서, Private Key)을 분리 보관할 수 있는가.		2	2	- 기능 지원 - Access Control(IAM) 계정 및 역할 권한으로 클러스터의 액세스 권한을 관리합니다.
	플랫폼 설치 정의서의 민감정보 암호화	분리된 민감 정보를 안전하게 보관하는 메커니즘이 제공되는가		2	2	- 기능 지원 - Access Control(IAM) 계정 및 역할 권한으로 클러스터의 액세스 권한을 관리합니다.
	설치 정의서의 템플릿화	정의서의 변경을 통해 설정 변경이 가능한가.		2	2	- 기능 지원 - Cluster 생성시 "Download a template for automation" 메뉴를 통해 생성되는 클러스터 템플릿 다운로드가 가능함. - Terraform 등을 사용하여 최초 설치 자동화 구성도 지원함.
	설치/관리 GUI 조회 제공 여부	설치된 플랫폼의 구성 정보를 확인하기 위한 GUI가 제공되는가		2	2	- 기능 지원 - Azure Portal 콘솔을 통해 기능 제공
	설치/관리 GUI 변경 제공 여부	GUI에서 Ansible Inventory 정보 수정/배포 기능이 있는가		2	2	- 기능 지원 - Azure Portal 콘솔을 통해 기능 제공

구분	항목	설명	배점	가중치	Azure Kubernetes Service	
					평가결과	평가의견
	플랫폼 검증 자동화	설치후 시스템 정상 여부 확인 자동화가 가능한가		2	0	- 지원 안됨 - 클러스터 생성 후 완료 상태 이외에 정상 여부 확인하는 verify 기능 없음.
업그레이드	플랫폼 업그레이드	호환성 유지 버전 업그레이드 기능 확인이 가능한가	15	4	4	- 기능 지원 - 수동/자동 Upgrade를 지원하나 최신 버전은 적용할 수 없음 - Master/Worker node 업그레이드 각각 동일 버전으로 업그레이드 - 업그레이드 되는 동안 해당 node에서 서비스 및 클러스터 구성 변경 불가 - 업그레이드 수행 완료 후 정상적으로 수행 됐는지 cli를 통해 유효성 확인 가능
	롤백	업그레이드 도중 장애 발생시 롤백될 수 있는가		4	0	- 지원 안함 - 플랫폼에서 자체 제공되는 기능 없음
	플랫폼 다운그레이드	호환성 유지 버전 다운그레이드 기능 확인이 가능한가		4	0	- 지원 안됨 - 플랫폼에서 지원되는 다운그레이드 기능 없음
	자동 플랫폼 업그레이드	자동 버전 업그레이드 기능을 제공하는가		3	2	- 기능 지원 - 원하는 버전 선택후 Manual 하게 업그레이드 수행 시 각 노드별 rolling 업그레이드 수행
내결함성	Master Node 장애	마스터 노드 장애시 플랫폼 가용성 확인이 가능한가	15	3	3	- 기능 지원 - AZ 수준의 가용성 보장 지원
	Worker Node 장애	워커 노드 장애시 플랫폼 가용성 확인이 가능한가		3	3	- 기능 지원 - 호스트 장애 상황 확인이 어려우나 가용존 이중화로 무중단 서비스 구성 가능
	Infra Node(운영관리 Node) 장애	인프라 노드 장애시 플랫폼 가용성 확인이 가능한가		2	2	- 기능 지원 - 호스트 장애 상황 확인이 어려우나 가용존 이중화로 무중단 서비스 구성 가능

구분	항목	설명	배점	가중치	Azure Kubernetes Service	
					평가결과	평가의견
	Router Node 장애	라우터 노트 장애시 플랫폼 가용성 확인이 가능한가		3	3	- 기능 지원 - 호스트 장애 상황 확인이 어려우나 가용존 이중화로 무중단 서비스 구성 가능
	PV 스토리지 내결함성	스토리지 장비 또는 서비스 장애시 플랫폼 내결함성 범위 확인이 가능한가		2	2	- 기능 지원 - 디스크 장애 확인은 불가하나 HDD/SSD 및 Block/File 타입 스토리지 서비스 기능 제공
	자동 노드 복구	Worker Host 장애를 자동 인지하고 자동 복구 기능을 제공하는가		2	0	- 지원 안함 - Worker node는 현재 있는 기능상으로는 자동 재시작되지는 않음. Worker node 장애는 Portal에 VM을 수동 재시작 수행하는 방식필요
백업 / 복구	플랫폼 백업/복구	플랫폼 삭제 및 동일 버전 재설치 후 데이터 복구 가능 여부 확인이 가능한가	5	5	1	- 지원 안됨 - AKS 플랫폼에서 제공되는 별도의 백업 서비스 없음.
스케일링	Master Node 스케일링	운영자원 효율화를 위해 마스터 노드를 증설하거나 감소할 수 있는가	5	1	1	- 기능 지원 - Master node는 AKS 플랫폼에서 관리함
	Worker Node 스케일링	운영자원 효율화를 위해 워커 노드를 증설하거나 감소할 수 있는가		2	2	- 기능 지원 - cluster node 확장하는 방식으로 지원 가능
	Infra Node(운영관리 Node) 스케일링	운영자원 효율화를 위해 인프라 노드를 증설하거나 감소할 수 있는가		1	1	- 기능 지원 - cluster node 확장하는 방식으로 지원 가능
	Router Node 스케일링	운영자원 효율화를 위해 라우터 노드를 증설하거나 감소할 수 있는가		1	1	- 기능 지원 - Master node는 AKS 플랫폼에서 관리함

구분	항목	설명	배점	가중치	Azure Kubernetes Service	
					평가결과	평가의견
플랫폼 관리	운영자 관리 GUI 제공	운영자가 PaaS 플랫폼을 관리 할 수 있는 GUI 관리 화면을 제공하는가	20	4	4	<ul style="list-style-type: none"> <li>- 기능 지원</li> <li>- 웹 형태의 Console 및 cloud shell 제공하며 cloud shell은 반드시 저장소 연결 및 비용 charge</li> <li>- Cloud Shell은 Root 권한을 제공하지 않는다. 추가적인 Package 설치가 되지 않음</li> </ul>
	운영자 계정 관리	LDAP 계정과 연계한 운영자 계정 관리가 가능한가		4	4	<ul style="list-style-type: none"> <li>- 기능 지원</li> <li>- Kubernetes를 Azure AD와 연동 가능하며 Azure의 사용자 및 그룹을 Kubernetes내 RBAC 과 연동 가능</li> </ul>
	유관시스템 계정 연계(모니터링/로그/미터링)	LDAP 계정과 연계한 모니터링/미터링 계정 관리가 가능한가		5	5	<ul style="list-style-type: none"> <li>- 기능 지원</li> <li>- 서비스에서 사용자 및 권한 통합 관리 가능하며 AD 연동 가능</li> </ul>
	Maintenance Window 지정	업무 부하가 작은 시간대를 정하여 Maintenance 가능한가		3	0	<ul style="list-style-type: none"> <li>- 지원 안함.</li> <li>- 플랫폼에서 제공하는 Maintenance Window 설명 기능 없음</li> </ul>
	PV 스토리지 자원 관리 기능	PV 자원의 할당 / 회수 자동화 기능이 가능한가		4	3	<ul style="list-style-type: none"> <li>- 기능 지원</li> <li>- 디스크 장애 확인은 불가하나 HDD/SSD 및 Block/File 타입 스토리지 서비스 기능 제공</li> </ul>
모니터링	Host 자원 모니터링	각 VM의 자원 모니터링을 통합하여 제공하는가	10	2	2	<ul style="list-style-type: none"> <li>- 기능 지원</li> <li>- Cluster의 모니터링 기능으로 제공하며, Insight, Metrics(preview), Logs 기능으로 확인 가능, 로그는 90일동안 보관됨</li> <li>- Cluster/Worker Nodes/Controllers/Containers 각각 모니터링 및 로깅 기능제공</li> </ul>
	컨테이너 배치 모니터링	각 컨테이너의 자원 모니터링을 통합하여 제공하는가		3	3	<ul style="list-style-type: none"> <li>- 기능 지원</li> <li>- 모니터링 Metrics기능에서 컨테이너 CPU/Memory 기반 리소스 모니터링 가능</li> </ul>

구분	항목	설명	배점	가중치	Azure Kubernetes Service	
					평가결과	평가의견
	데이터 보관기간 설정	모니터링 데이터 보관 기능을 조정할 수 있는가		2	1	- 기능 지원 - Cluster의 모니터링 기능으로 제공하며, Insight, Metrics(preview), Logs 기능으로 확인 가능, 로그는 90일동안 보관됨 - Cluster/Worker Nodes/Controllers/Containers 각각 모니터링 및 로깅 기능제공
	알람 기능 제공	플랫폼 운영자 관점에서 알람기능을 제공하는가		3	3	- 기능 지원 - Alert 서비스에서 리소스별 alert 설정 가능
로그 통합	Host 로그통합	각 VM의 로그를 통합하여 제공하는가	10	2	2	- 기능 지원 - Cluster의 모니터링 기능으로 제공하며, Insight, Metrics(preview), Logs 기능으로 확인 가능, 로그는 90일동안 보관됨 - Cluster/Worker Nodes/Controllers/Containers 각각 모니터링 및 로깅 기능제공
	컨테이너 로그 통합	컨테이너 Lifecycle 및 Event 로그를 통합하여 제공하는가		2	2	- 기능 지원 - Monitor 서비스에서 컨테이너 로그 통합 기능 제공
	데이터 보관기간 설정	로그 데이터 보관 기능을 조정할 수 있는가		2	1	- 부분 기능 지원 - 최대 90일까지 로그 보관 기능을 제공하며 날짜별 시간별 필터/쿼리 기능 제공
	Audit 로그 제공	보안 관점에서 분석 가능한 audit logs를 제공하는가		1	1	- 기능 제공 - Activity log 기능 제공
미터링	사용자 과금 정책 적용	사용자 정의 과금정책 적용 가능한가		1	0	- 지원 안함 - 플랫폼에서 제공하는 별도의 과금 정책 기능 없음
	인스턴스 단위 미터링	컨테이너수 단위 미터링 가능한가		1	1	- 부분 기능 지원 - 모니터 서비스를 사용해 로깅은 가능하나 별도의 과금 체계 개발 필요

구분	항목	설명	배점	가중치	Azure Kubernetes Service	
					평가결과	평가의견
	자원사용량 단위 미터링	CPU, MEMORY, Storage 사용량 단위 미터링 가능한가		1	1	- 부분 기능 지원 - 모니터 서비스를 사용해 로깅은 가능하나 별도의 과금 체계 개발 필요

- [테스트 결과 요약](#)(see page 10)
- [테스트 결과 상세](#)(see page 10)



## 3 AKS 3. 어플리케이션 테스트 결과

### 3.1 테스트 결과 요약

AKS는 전체적으로 Kubernetes를 효과적으로 관리할 수 있는 다양한 기능을 제공해주고 있다.

개발자용 클러스터인 Azure Dev Spaces를 제공하고 VS Code를 사용하는 개발자가 로컬환경을 쉽게 구성할 수 있게 해주며, Insight, Log Analytics 등 로그 분석 및 리소스 모니터링 기능을 효과적으로 사용할 수 있다.

전체적으로 서비스를 보면, 기능 및 콘솔에서 제공해주는 Cloud Shell 등 GCP와 유사한 부분이 많으며, 다양한 서비스 기능들이 현재 추가가 되고 있는 상태이다. 한 예로 인사이트 경우 Preview 단계에서 테스트를 진행하는 동안 정식 서비스로 Release가 되며 기능이 추가된 것을 확인할 수 있었다. 하지만, 콘솔을 이용할 경우 서비스 속도와 안정성 등에서는 아직은 부족하게 느껴진다.

### 3.2 테스트 결과 상세

구분	항목	설명	배점	가중치	Azure Kubernetes Service	
					평가결과	평가의견
컨테이너 빌드/배포	소스코드 빌드/배포	소스 코드를 이용한 빌드/배포 기능	15	5	0	- 제공되지 않음
	DockerHub, 사용자 개발 컨테이너 이미지 배포	컨테이너 이미지를 이용한 빌드/배포 기능		5	5	- Container Registry를 이용하여 이미지 배포 및 관리가 가능함
	Recreate 배포기능 확인	Recreate 배포 방식 지원		1	1	- latest가 retry를 계속하다가 정해진 횟수가 초과되면 fail되며 이전 버전이 다시 올라옴
	Rolling 배포기능 확인	Rolling 배포 방식 지원		1	1	- Deployment config 베이스로 배포정책이 설정되고 수행됨

구분	항목	설명	배점	가중치	Azure Kubernetes Service	
					평가결과	평가의견
	Rollback 배포기능 확인	Rollback 기능 지원		1	1	-Kubernetes 기능을 이용해 가능함 kubectl rollout undo deployment/hello
	BlueGreen 배포기능 확인	BlueGreen 배포 방식 지원		1	0	- 기본제공 하지 않으며 spinnaker를 활용하여 제공 가능
	Canary 배포기능 확인	Canary 배포 방식 지원		1	0	- 기본제공 하지 않으며 spinnaker를 활용하여 제공 가능
컨테이너 레지스트리 관리	Container Registry Service 확인	Container Registry 제공 여부, 설치 편의성	5	2	2	- Azure Container Registry를 제공함 - CLI를 통해 생성하거나 웹콘솔 > 마켓플레이스에서 생성하면 사용이 가능함
	Container Registry 내 이미지 관리 편의성	이미지 버전 관리 편의성		1	1	- 이미지 버전 관리 가능하며 사용이 편리함
	이미지 관리를 위한 추가 기능 확인	별도의 관리 Portal 제공여부, 웹취약점, Docker signed 확인 기능		2	1	- AWS 콘솔 내 별도 관리 Page가 존재함
컨테이너 관리	컨테이너 자원할당 지정	CPU, Memory, storage 지정	25	3	3	- Kubernetes의 기능으로 cpu, memory의 Request, Limit 값을 yaml에 설정하여 배포할 수 있음

구분	항목	설명	배점	가중치	Azure Kubernetes Service	
					평가결과	평가의견
	컨테이너 이미지 관리(버전 관리)	컨테이너 이미지, 버전 관리 기능		3	3	- ACR (Azure Container Registry)를 이용하여 Private Registry를 사용할 수 있으며 컨테이너 이미지 관리가 가능함 - namespace, tag등을 docker hub와 동일하게 사용할 수 있음
	컨테이너 확장 시 자동식별 및 부하 분산	컨테이너 수동/ 자동 으로 확장 시 부하 분산 기능		5	5	- CLI를 통해 수동확장이 가능함 (az aks scale --resource-group myResourceGroup --name myAKSCluster --node-count 3) - 자동확장은 CLI로 설정한 CPU 사용량을 기준으로 가능함 (kubectl autoscale deployment php-apache --cpu-percent=50 --min=1 --max=10) - node의 최소, 최대 개수를 정할 수 있음
	컨테이너 확장 시 부하조정	컨테이너 확장 시 부하 비중 비율 조정 가능 여부		4	4	- service와 label selector를 이용하여 가능하게 함
	Container to Container 통신	컨테이너 간 통신 설정		3	0	- 서비스 단위로 통신 가능
	route 관리	사용자 정의 route 등록/변경/삭제		2	2	- Azure DNS 사용하여 Route 관리가 가능함 - az aks create --resource-group myResourceGroup --name myAKSCluster --enable-addons http_application_routing

구분	항목	설명	배점	가중치	Azure Kubernetes Service	
					평가결과	평가의견
	사용자 인증서 추가	사용자가 Route에 별도의 인증서 등록, 관리 기능		3	2	- Helm을 이용해 nginx ingress를 설치 후 Kubernetes secret 생성 -> 어플리케이션 배포 후 YAML에 tls 정의하여 사용가능 - AKS에서 클러스터 생성시 Load Balancer가 생성되며, 인증서는 컨테이너 내부에서 관리를 함
	어플리케이션 health check	http/port/process 기반의 Health Check 기능		2	2	- Kubernetes의 LivenessProbe, ReadinessProbe를 설정하여 Pod의 Health Check가 가능함
어플리케이션 개발	로컬에서 Eclipse Plug-in을 이용한 개발	이클립스 기반의 개발자 도구가 제공 여부	15	2	0	- 제공되지 않음
	로컬에서 원격 debugging	로컬 환경에서 원격 디버깅 지원 여부		3	3	- AKS Cluster에 Azure Dev Spaces를 설치 후 VS Code용 Azure Dev Space 확장을 설치하여 컨테이너 디버그 가능
	컨테이너 실시간 로그 분석	컨테이너(Pod) 내 실시간 로그 확인		3	3	- CLI를 통해 확인이 가능함
	컨테이너 SSH 접속	컨테이너(Pod)에 SSH 접속 가능 여부 확인		3	3	- 기능확인함 (CLI를 통해 확인이 가능함)
	파이프라인 생성/수정	파이프라인 생성/수정 확인 (Jenkins, Spinnaker, Concourse 등 활용 가능 여부 확인)		4	2	- Azure Devops를 이용하여 Devops 프로젝트를 생성 후 파이프라인 구성이 가능함 - Jenkins 연동하여 사용이 가능함

구분	항목	설명	배점	가중치	Azure Kubernetes Service	
					평가결과	평가의견
어플리케이션 성능/장애 분석	컨테이너 과거 로그 분석	프로젝트/Pod/서비스 단위의 로그 분석 기능	15	3	3	- Azure Log Analytics 설정 후 모니터링 > 로그 메뉴를 통해 로그 분석이 가능함
	Java 분석 기능 (Jconsole, Dump 수집)	Jconsole을 이용한 모니터링 가능 여부 Java의 Heap, Thread Dump 생성 및 추출 가능 여부		2	2	- Java에서 제공해주는 기본 분석 기능 사용이 가능함
	컨테이너 자원 모니터링	Pod별 CPU, 메모리, 디스크 사용량에 대한 모니터링		5	5	- Azure Log Analytics 설정 후 모니터링 > 인사이트 메뉴를 통해 클러스터, 노드, 컨트롤러, 컨테이너의 자원 정보 모니터링이 가능함
	어플리케이션 호출 분석	MSA 서비스간 call trace 분석 가능 여부		2	0	- 지원하지 않음 - 사용자 zipkin을 추가적으로 설치하고 구성해야 함
	사용자를 위한 알람 기능 제공	플랫폼 사용자 관점의 알람 기능 제공 여부		3	3	- Azure portal에서 모니터 > 경고를 설정하여 리소스별 알람 설정이 가능함
프로젝트 관리	개발자 사용을 위한 GUI 제공	개발자용 웹콘솔 확인	15	1	1	- 웹콘솔이 제공됨
	CLI 설치 편의성	CLI 환경 구성 시 설치 편의 및 자동화 여부		1	1	- 별도의 설치 없이 Cloud Shell을 통해 CLI 사용이 가능함
	사용자 관리	사용자 관리 기능 및 편의성 LDAP, SSO 등과의 연동을 통한 외부 사용자 정보를 이용해 일괄 사용자 등록이 가능한지에 대한 확인		2	2	- IAM을 이용하여 사용자 관리가 가능함

구분	항목	설명	배점	가중치	Azure Kubernetes Service	
					평가결과	평가의견
	권한 관리	리소스별/ 사용자별 권한 관리		3	3	- Azure Active Directory를 이용해 권한 관리가 됨 - AKS Cluster에 대한 서비스 계정을 생성하여 사용하며, 다른 Azure 리소스에 대한 권한이 필요할 경우 권한을 위임하여 사용함
	프로젝트 생성/ 삭제	프로젝트 생성 및 프로젝트 관리자 할당		2	1	- 리소스그룹의 Tag를 이용하여 Department, Environment등을 추가하여 관리 할 수 있음 - 리소스그룹별로 접근 권한을 사용할 수 있음
	프로젝트 내에서 하위그룹 관리	개발, 테스트, 운영 등 개발단계별 관리		1	0	- 제공되지 않음
	Quota 관리	CPU, MEMORY, Container수, Route 수 제한		2	2	- Kubernetes 기능으로 Quota 설정이 가능함 Compute Resource - CPU, Memory, Pod 개수와 Object 개수 - configmap, PVC, secrets, services, LB 수를 설정할 수 있음
	Instance App Template 생성	사용자 정의 Application Template 생성이 가능한가 이미지와 템플릿 사이의 workflow 차이 확인		3	2	- Helm을 이용하여 가능함
보안/네트워킹	프로젝트 단위 보안 설정	프로젝트간 통신 설정이 가능한지 확인 (Multi tenancy Enabled)	10	2	1	- Namespace를 이용하여 프로젝트 개념으로 사용이 가능함

구분	항목	설명	배점	가중치	Azure Kubernetes Service	
					평가결과	평가의견
	컨테이너 그룹 단위 보안 설정	컨테이너 그룹을 정의하고 그룹간 통신 설정이 가능한지 확인		2	0	- 지원안됨
	지정 컨테이너 단위 보안 설정	컨테이너별 통신 설정이 가능한지 확인		2	1	- Istio를 사용하여 Service 단위로 보안 설정을 제어할 수 있음
	특정 Role로 통신 제한(inbound)	특정 APP 이 외부의 정해진 IPs, PORT 에 대해서만 inbound 설정 가능한지 확인		2	0	- 지원안됨 - 방화벽을 통해서 차단하거나, istio를 사용하여 Cookie 정보를 이용하여 접근 권한을 제어할 수 있음
	특정 Role로 통신 제한(outbound)	특정 APP 이 외부 연계를 위해 특정 IPs, PORT 로 outbound 가능하도록 설정 가능한지 확인		2	2	- Network Policy를 지원함

- [테스트 결과 요약](#)(see page 17)
- [테스트 결과 상세](#)(see page 17)

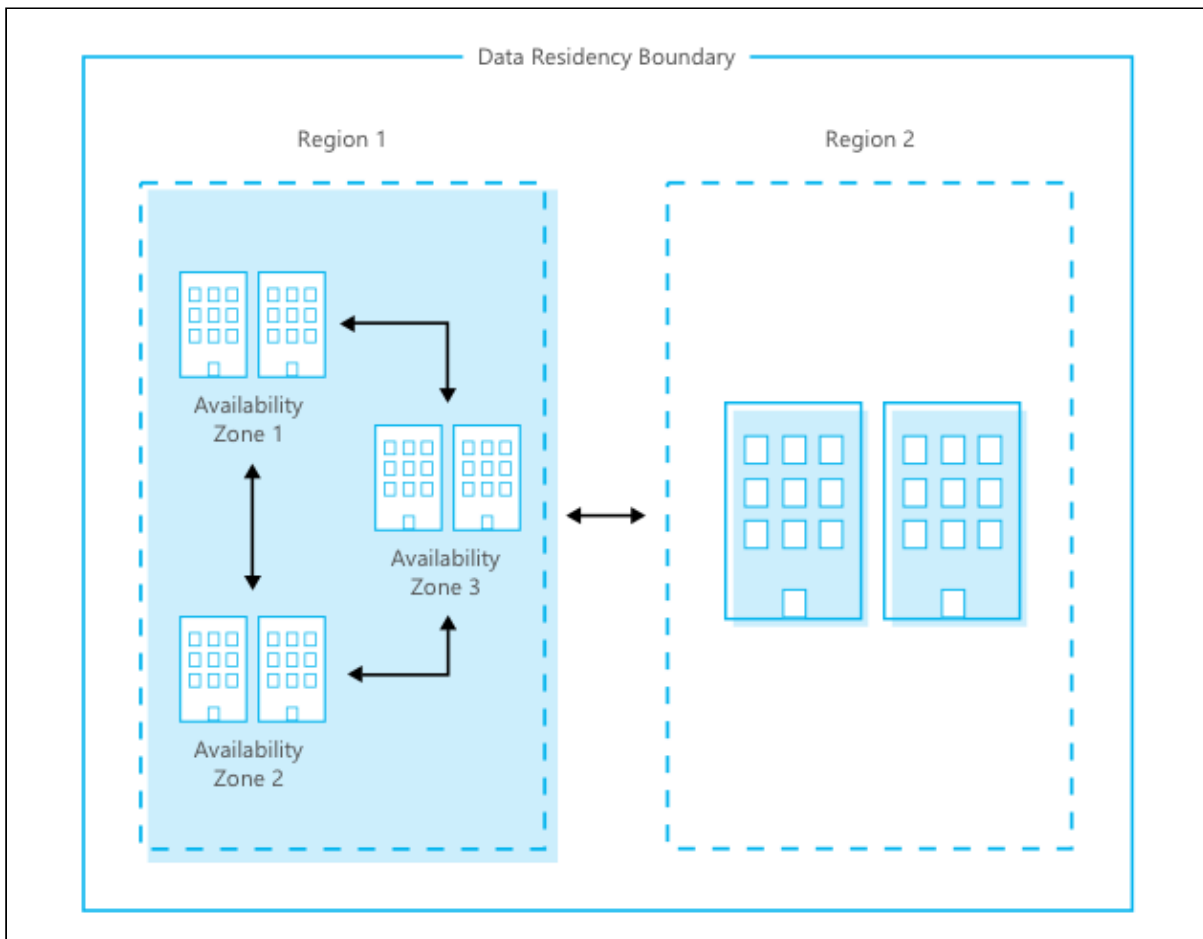
## 4 AKS 4. 도입/구축 시 고려사항

### 4.1 서비스 리전

Azure는 현재 시점('18년 12월)에 전세계 54개 Region과 140국가에 서비스 중이며 한국에는 중부리전과 남부리전이 서비스 중이다. 한국 리전에는 AKS 서비스는 제공되고 있지 않다. Azure에서 사용하는 Global Infra는 다른 퍼블릭 클라우드 서비스에서는 사용하는 Region, AZ(Availability Zones) 용어의 개념이 약간 차이가 있다.

#### 4.1.1 Region

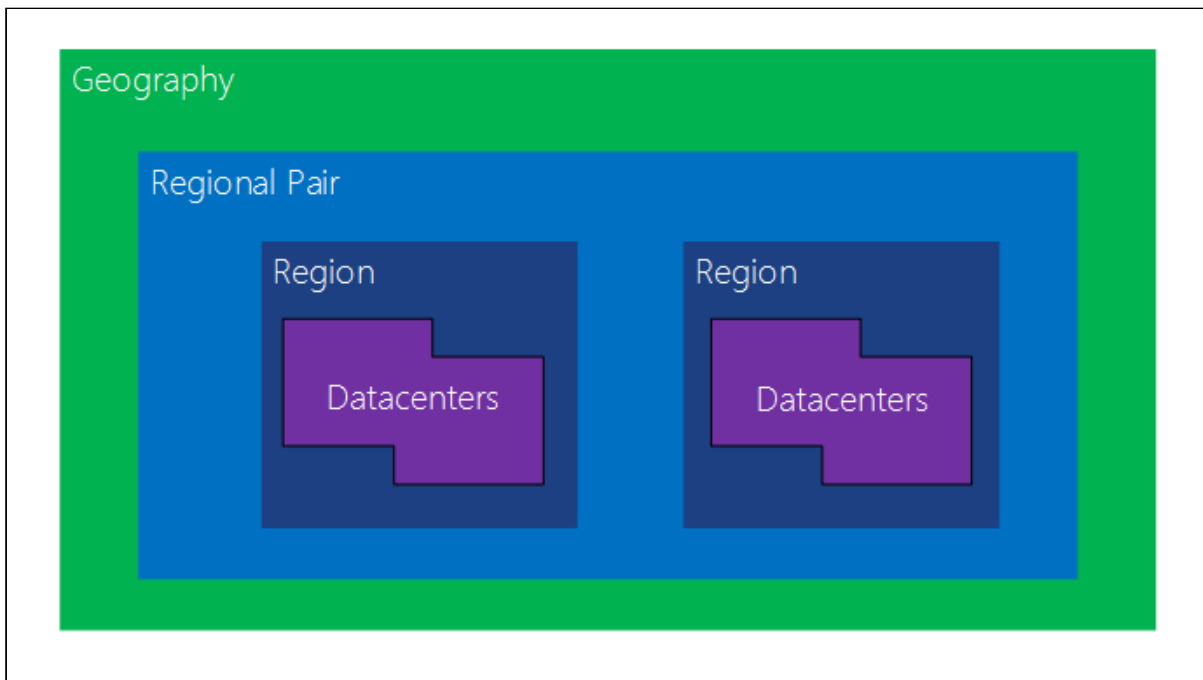
Region은 정해진 latency 내에 배치된 데이터 센터의 집합으로 Low-latency 네트워크로 연결되어 있습니다.





## 4.1.2 Geographies

Geographies는 일반적으로 두개 이상의 리전을 포함하는 별개의 Market 입니다. 그러나 Geographies는 동일한 규정 및 데이터 레지던시를 보장합니다. 특정 데이터 레지던시 및 규정 요구 사항이 있는 고객은 Geographies를 통해 Region에 발생하는 장애에 대비하여 데이터와 응용 프로그램의 가용성을 보장할 수 있습니다.



Geography	쌍을 이루는 지역	
아시아	동아시아	동남아시아
오스트레일리아	오스트레일리아 동부	오스트레일리아 남동부
오스트레일리아	오스트레일리아 중부	오스트레일리아 중부 2
브라질	브라질 남부 2	미국 중남부
캐나다	캐나다 중부	캐나다 동부
중국	중국 북부	중국 동부
중국	중국 북부 2	중국 동부 2
유럽	북유럽	서유럽
프랑스	프랑스 중부	프랑스 남부
독일	독일 중부	독일 북동부
인도	인도 중부	인도 남부
인도	인도 서부(1)	인도 남부
일본	일본 동부	일본 서부
한국	한국 중부	한국 남부
북아메리카	미국 동부	미국 서부
북아메리카	미국 동부 2	미국 중부
북아메리카	미국 중북부	미국 중남부
북아메리카	미국 서부 2	미국 중서부

### 4.1.3 Availability Zones

AZ는 Azure Region내에 물리적으로 분워된 위치를 말합니다. 각 AZ 영역은 독립된 전원, 냉각 및 네트워킹을 갖춘 하나 이상의 데이터 센터로 구성 됩니다.

## 4.2 AKS(Azure Kubernetes Service) 제공 Region

모든 Azure 서비스에는 리소스와 기능에 대한 제약 사항이 있습니다. AKS 서비스의 기본 리소스 제한과 서비스 가능한 지역을 설명합니다.

### AKS 기본 서비스 및 제약 사항

리소스	기본 제한
구독당 최대 클러스터	100
클러스터당 최대 노드	100
노드당 최대 포드: Kubelet과 기본 네트워킹	110
노드당 최대 포드: Azure CNI와 고급 네트워킹	Azure CLI 배포: 30 <sup>1</sup> Resource Manager 템플릿: 30 <sup>1</sup> 포털 배포: 30

#### Azure CLI 배포

Azure CLI 또는 Resource Manager 템플릿을 사용하여 POD를 AKS 클러스터에 배포할 때 이 값은 네트워크 설정에 따라 최대 배포할 수 있는 최대값이 달라질 수 있습니다.

AKS 서비스 제공 Region(2018/12월 기준)

- 오스트레일리아 동부
- 캐나다 중부
- 캐나다 동부
- 미국 중부
- 미국 동부
- 미국 동부2
- 일본 동부
- 북유럽
- 동남아시아
- 인도 남부
- 영국 남부
- 영국 서부
- 서유럽
- 미국 서부
- 미국 서부 2

## 4.3 비용 산정

### 4.3.1 Container Registry

ACR(Azure Container Registry)은 다중 서비스 계층(즉, SKU)에서 사용 가능합니다. SKU는 예측 가능한 가격 책정과 Azure에서 개인 Docker 레지스트리의 용량 및 사용량 패턴에 맞추기 위한 여러 옵션을 제공합니다.

SKU	관리	설명
Basic	yes	개발자가 Azure Container Registry에 대해 배울 수 있는 비용 최적화된 진입점입니다. Basic 레지스트리는 Standard 및 Premium(Azure Active Directory 인증 통합, 이미지 삭제 및 웹 후크)과 동일한 프로그래밍 성능을 갖습니다. 그렇지만 포함된 저장소 및 이미지 처리량은 더 낮은 사용량 시나리오에 가장 적합합니다.
Standard	yes	Standard 레지스트리는 Basic과 동일한 성능을 제공하되, 포함된 저장소 제한과 이미지 처리량은 더 높습니다. Standard 레지스트리는 대부분의 프로덕션 시나리오 요구를 충족합니다.
Premium	yes	Premium 레지스트리는 포함된 저장소 및 동시 작업 수가 가장 높으며 고용량 시나리오를 지원합니다. Premium은 많은 이미지 처리량을 제공하는 것 외에도, 여러 지역 전반에서 단일 레지스트리를 관리하기 위한 <a href="#">지역에서 복제</a> 및 이미지 태그 서명을 위한 <a href="#">콘텐츠 신뢰(미리 보기)</a> 와 같은 기능을 추가적으로 제공합니다.
클래식 <sup>1</sup>	아니 요	SKU는 Azure에서 Azure Container Registry 서비스의 초기 릴리스를 지원했습니다. Classic 레지스트리는 사용자 구독에서 Azure가 만드는 저장소 계정에서 지원하며 ACR가 처리량 증가 및 지역에서 복제 등의 더 높은 수준의 기능을 제공할 수 있는 기능을 제한합니다.

**❗ 클래식**

클래식 SKU는 더 이상 사용되지 않으며 2019년 3월 이후에는 사용할 수 없습니다. 모든 새 레지스트리에는 기본, 표준 또는 프리미엄을 사용해야 합니다.

### 4.3.2 SKU 상세 서비스

리소스	Basic	Standard	Premium
Storage <sup>1</sup>	10GiB	100GiB	500GiB
최대 이미지 계층 크기	20GiB	20GiB	50GiB
분당 ReadOps <sup>2,3</sup>	1,000	3,000	10,000
분당 WriteOps <sup>2,4</sup>	100	500	2,000
다운로드 대역폭 MBps <sup>2</sup>	30	60	100
업로드 대역폭 MBps <sup>2</sup>	10	20	50
Webhook	2	10	100
지역에서 복제	해당 없음	해당 없음	지원됨
콘텐츠 신뢰(미리 보기)	해당 없음	해당 없음	지원됨

- [Container Registry 비용](#)<sup>1</sup>

### 4.3.3 AKS(Azure Kubernetes Service)

AKS(Azure Kubernetes Service)는 Kubernetes의 배포, 관리 및 작업을 완전히 관리되는 Kubernetes 컨테이너 오케스트레이터 서비스로 간소화하는 무료 컨테이너 서비스입니다. 사용된 가상 머신과 연결된 저장소 및 네트워킹 리소스에 대한 요금만 결제한다면 AKS가 출시 제품 중 가장 효율적이고 비용 효과적인 Container Service입니다. Kubernetes Master node는 무료이며 Worker Node 사용료만 과금 됩니다.

- [Azure Pricing Calculator](#)<sup>2</sup>

## 4.4 AKS 클러스터 네트워크 옵션

AKS 클러스터 생성 시 네트워크 옵션은 Basic/Advanced 2가지 방식으로 선택하여 구성이 가능합니다. Advanced 방식은 GCP의 VPC-native(alias IP) 기능과 유사 합니다.

- Basic 네트워킹 - AKS 클러스터가 배포될 때 네트워크 리소스가 만들어지고 구성됩니다.

1 <https://azure.microsoft.com/ko-kr/pricing/details/container-registry/>

2 <https://azure.microsoft.com/ko-kr/pricing/calculator/?service=kubernetes-service>

- Advanced 네트워킹 - AKS 클러스터가 기존 가상 네트워크 리소스 및 구성에 연결됩니다.

#### 4.4.1 Basic 네트워킹

Basic 네트워킹 옵션은 AKS 클러스터 생성시 기본 구성입니다. Azure 플랫폼은 클러스터와 Pod의 네트워크 구성을 관리합니다. Basic 네트워킹은 사용자가 직접 가상 네트워크 구성이 필요하지 않은 배포에 적합합니다. Basic 네트워킹에서는 AKS 클러스터에 할당된 서브넷 이름 또는 IP 주소 범위와 같은 네트워크 구성을 선택할 수 없습니다. Basic 네트워킹에 대해 구성된 AKS 클러스터의 노드에는 [kubenet](#)<sup>3</sup> Kubernetes 플러그인이 구성됩니다.

- Azure Load Balancer를 통해 외부 또는 내부로 Kubernetes 서비스를 제공합니다.
- Pod는 공용 인터넷의 리소스에 액세스할 수 있습니다.

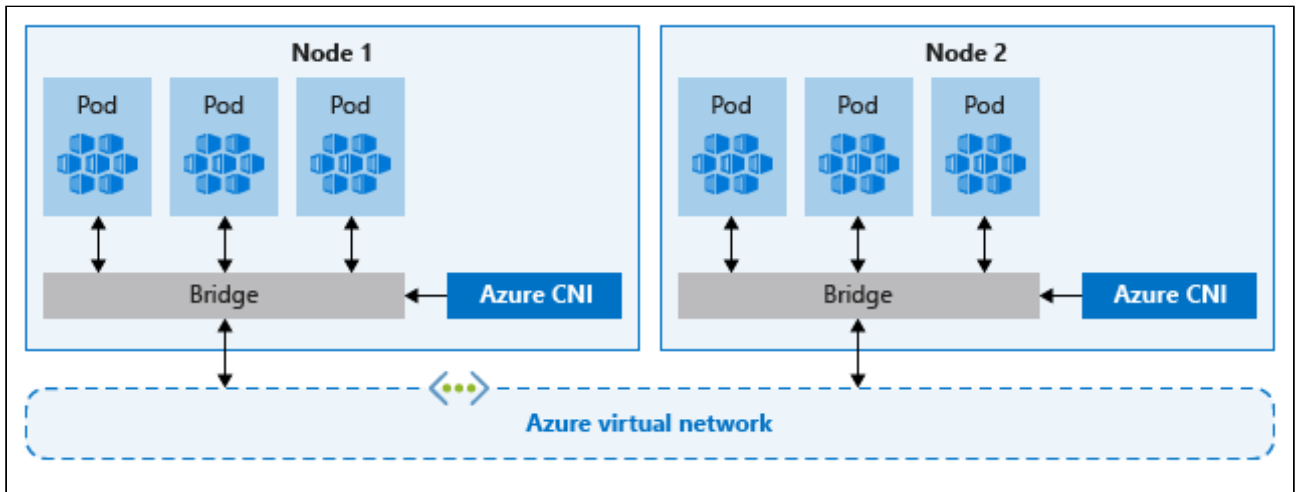
DEVICE	TYPE	IP ADDRESS	SUBNET
aks-agentpool-31294957-nic-2	Network interface	10.240.0.4	aks-subnet
aks-agentpool-31294957-nic-1	Network interface	10.240.0.5	aks-subnet
aks-agentpool-31294957-nic-0	Network interface	10.240.0.6	aks-subnet
aks-agentpool-31294957-nic-3	Network interface	10.240.0.7	aks-subnet

#### 4.4.2 Advanced 네트워킹

Advanced 네트워킹은 구성된 Azure VPC에 Pod를 직접 연결합니다. VPC 네트워크는 다른 Azure 리소스에 대한 자동 연결 및 다양한 기능을 제공합니다. Advanced 네트워킹은 기존 서브넷 연결 사용과 같은 특정 가상 네트워크 구성이 필요한 배포에 적합합니다. Advanced 네트워킹을 사용하면 이러한 서브넷 이름과 IP 주소 범위를 지정할 수 있으며 구성된 AKS 클러스터의 노드에는 [Azure CNI\(컨테이너 네트워킹 인터페이스\)](#)<sup>4</sup> Kubernetes 플러그인이 구성됩니다.

<sup>3</sup> <https://kubernetes.io/docs/concepts/cluster-administration/network-plugins/#kubenet>

<sup>4</sup> <https://github.com/Azure/azure-container-networking/blob/master/docs/cni.md>



- AKS 클러스터를 기존 Azure 가상 네트워크에 배포하거나 클러스터에 대한 새 가상 네트워크와 서브넷을 만듭니다.
- 클러스터의 모든 Pod에 VPC 네트워크의 IP 주소가 할당됩니다. Pod에서 클러스터의 다른 Pod 및 VPC 네트워크의 다른 노드와 직접 통신할 수 있습니다.
- Pod는 ER(ExpressRoute)와 S2S(사이트 간) VPN 연결을 통한 On-premise 네트워크를 포함하여 피어링된 VPC 네트워크의 다른 서비스에 연결할 수 있습니다.
- 서비스 엔드포인트를 사용하도록 설정된 서브넷의 Pod는 Azure 서비스(예: Azure Storage 및 SQL DB)에 안전하게 연결될 수 있습니다.

Dashboard > Virtual networks > lgcns-paas-dev01-vnet

Virtual networks  
simloknaver (Default Directory)

lgcns-paas-dev01-vnet  
Virtual network

Filter by name...

NAME

aks-vnet-31294957

lgcns-paas-dev01-vnet

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Address space

Connected devices

Subnets

DDoS protection

Firewall

DNS servers

Peerings

Service endpoints

Properties

Locks

Automation script

Monitoring

Connection monitor

Diagram

Support + troubleshooting

Connection troubleshoot

New support request

Refresh Move Delete

Resource group (change)  
lgcns-paas-dev01

Location  
East US

Subscription (change)  
Azure PoC 7th

Subscription ID  
fcb1b913-a597-4f0b-bc6f-f81f20be4e3

Tags (change)  
Click here to add tags

Address space  
10.0.0.0/8

DNS servers  
Azure provided DNS service

Connected devices

Search connected devices

DEVICE	TYPE	IP ADDRESS	SUBNET
aks-agentpool-25001505-nic-0	Network interface	10.240.0.4	default
aks-agentpool-25001505-nic-0	Network interface	10.240.0.5	default
aks-agentpool-25001505-nic-0	Network interface	10.240.0.6	default
aks-agentpool-25001505-nic-0	Network interface	10.240.0.7	default
aks-agentpool-25001505-nic-0	Network interface	10.240.0.8	default
aks-agentpool-25001505-nic-0	Network interface	10.240.0.9	default
aks-agentpool-25001505-nic-0	Network interface	10.240.0.10	default
aks-agentpool-25001505-nic-0	Network interface	10.240.0.11	default
aks-agentpool-25001505-nic-0	Network interface	10.240.0.12	default
aks-agentpool-25001505-nic-0	Network interface	10.240.0.13	default
aks-agentpool-25001505-nic-0	Network interface	10.240.0.14	default
aks-agentpool-25001505-nic-0	Network interface	10.240.0.15	default
aks-agentpool-25001505-nic-0	Network interface	10.240.0.16	default



### ① Advanced 네트워킹 고려사항

필요한 IP 주소 수에는 업그레이드 및 Scale 작업에 대해 검토되어야 합니다. 고정 노드 수만 지원하는 IP 주소 범위를 설정할 경우 클러스터의 업그레이드나 노드 확장 계획을 반영해야 합니다.

- AKS 클러스터를 업그레이드할 경우 새 노드가 클러스터에 배포됩니다. 서비스 및 워크로드가 새 노드에서 실행되기 시작하고 기존 노드가 클러스터에서 제거됩니다. 이 업그레이드 배포 프로세스를 위해서 최소 하나 이상의 추가 IP 주소 블록을 사용할 수 있어야 합니다.
- AKS 클러스터를 확장할 경우 새 노드가 클러스터에 배포됩니다. 서비스 및 워크로드가 새 노드에서 실행되기 시작하며 IP 주소 범위에서는 클러스터가 지원할 수 있는 노드 및 Pod 수가 변경될 여유 IP 주소를 가지고 있어야 합니다. 업그레이드 작업에 대한 추가 노드 하나도 포함되어야 합니다.

## 4.5 Cloud shell 소개

Azure에서도 Google Cloud에서와 마찬가지로 시스템 관리 콘솔화면을 통해 브라우저 기반의 CLI 환경을 제공하는 Cloud Shell을 사용 할 수 있습니다. Google Cloud Shell은 30GB 정도의 용량에 cloud shell에 대한 root 권한까지 부여함에 따라 기본적으로 설치되어 있는 유틸리티 외에 사용자가 필요한 유틸리티의 추가 설치가 가능하고 무료서비스로 제공됩니다. Azure Cloud Shell의 경우 cloud shell을 사용하기 위해서는 반드시 디스크를 연결해야 하며 디스크 비용은 유료이며 cloud shell의 일반 유저 권한만 부여하여 제공되는 기본 유틸리티 이외에 추가로 사용자가 필요한 유틸리티를 설치 할 수 없습니다.

### 4.5.1 기본 제공되는 유틸리티 목록

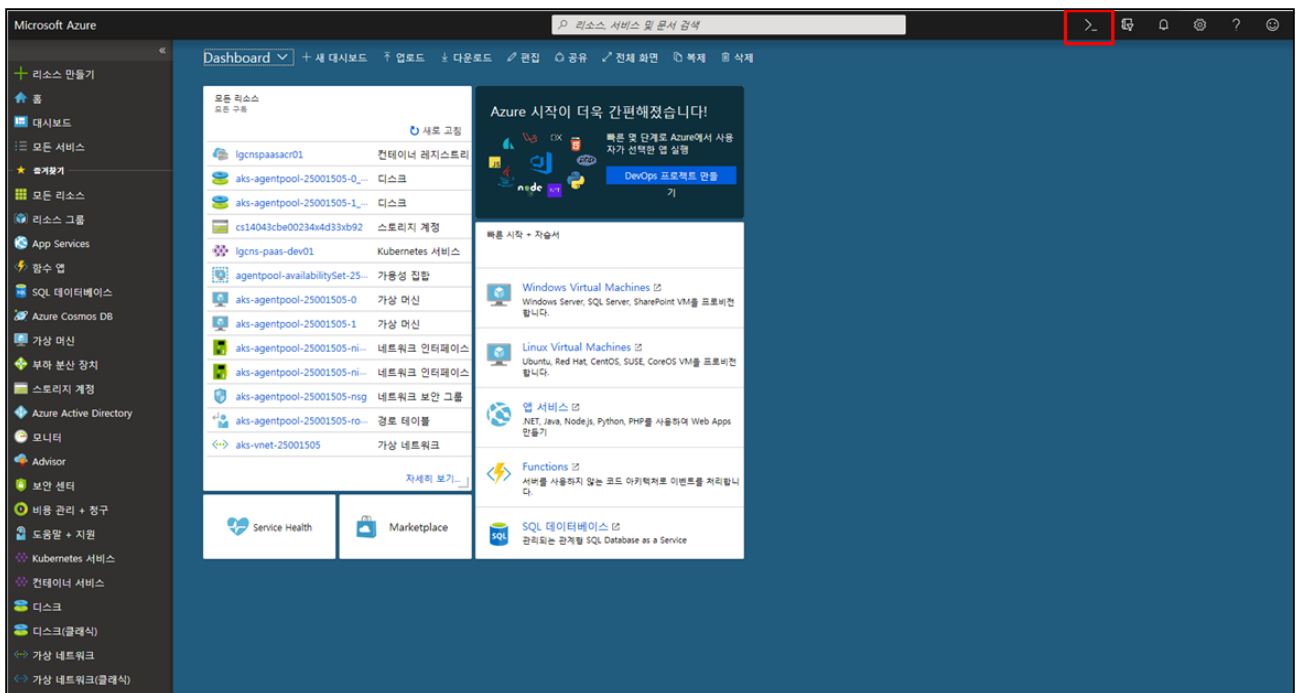
도구	
Category	이름
Linux 도구	bash zsh sh tmux dig
Azure 도구	<a href="#">Azure CLI</a> 및 <a href="#">Azure 클래식 CLI</a> <a href="#">AZCopy</a> <a href="#">Service Fabric CLI</a> <a href="#">Batch Shipyard</a> <a href="#">blobxfer</a>
텍스트 편집기	vim nano emacs 코드
소스 제어	git
빌드 도구	make maven npm pip
컨테이너	<a href="#">Docker 컴퓨터</a> <a href="#">Kubectl</a> <a href="#">Helm</a> <a href="#">DC/OS CLI</a>
데이터베이스	MySQL 클라이언트 PostgreSQL 클라이언트 <a href="#">sqlcmd 유틸리티</a> <a href="#">mssql-scripter</a>
기타	<a href="#">iPython 클라이언트</a> <a href="#">Cloud Foundry CLI</a> <a href="#">Terraform</a> <a href="#">Ansible</a> <a href="#">Chef InSpec</a>

## 4.5.2 프로그래밍 언어 지원

### 언어 지원

언어	버전
.NET Core	2.0.0
Go	1.9
자바	1.8
Node.js	8.9.4
PowerShell	6.1.0
Python	2.7 및 3.5(기본값)

Azure Portal 화면 우측 상단의 아이콘을 클릭하면 Cloud shell에 접속이 가능하다.

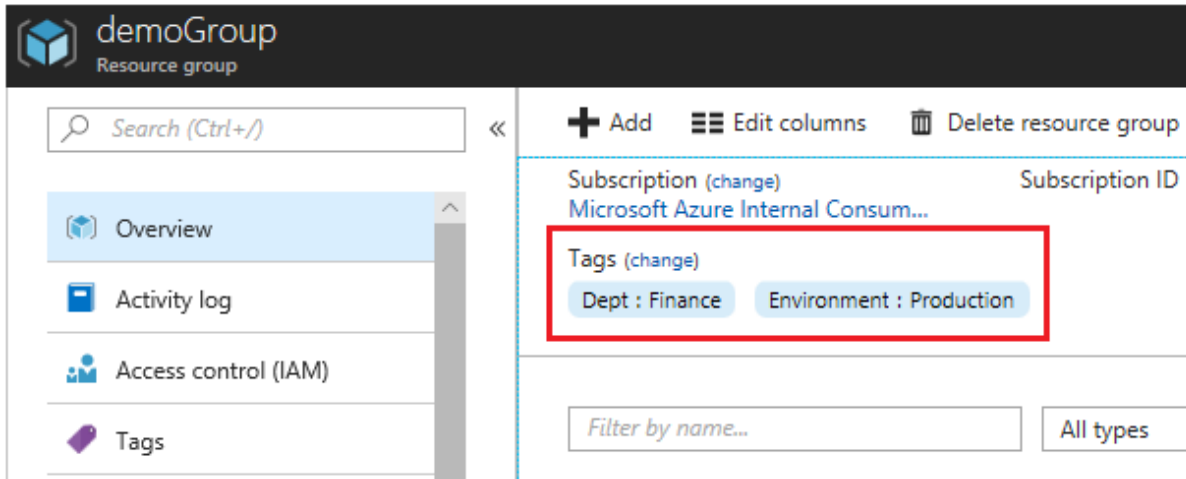


## 4.6 Resource Group

Azure에는 Resource Group을 사용할 수 있다. Resource group이란 Azure에 포함된 리소스를 관리하는 그룹이다. 사용자는 Resource Group을 이용하여 사용자 조직에 가장 적합한 리소스를 할당하고 관리할 수 있다.

일반적으로 함께 배포, 업데이트 하는 리소스들을 한 그룹에 추가하여 동일한 수명주기를 가질 수 있도록 관리한다.

리소스그룹 내에 Tag 기능을 사용하여 부서, 환경 등의 값을 설정하여 해당 리소스 그룹을 관리할 수 있다. 부서별로 리소스 그룹을 분리하여 관리하거나, 개발-Stage-QA-Production 으로 환경을 분리하여 리소스를 관리할 때 Tag 기능을 유용하게 사용할 수 있다.



리소스 그룹은 다른 구독, 다른 리소스 그룹으로 이동이 가능하며, 리소스별 Lock을 설정하여 실수로 리소스가 삭제, 수정되는 것을 예방할 수 있다. 또한, 그룹별로 전체 리소스그룹을 일괄 삭제할 수 있다.

사용자별 역할을 할당할 때, 리소스 그룹, 리소스, 구독에 따라 역할 부여가 가능하므로 특정 사용자가 특정 Resource Group에만 접속할 수 있도록 권한을 관리 할 수 있다.

- 서비스 리전(see page 24)
  - Region(see page 24)
  - Geographies(see page 25)
  - Availability Zones(see page 27)
- AKS(Azure Kubernetes Service) 제공 Region(see page 28)
- 비용 산정(see page 29)
  - Container Registry(see page 29)
  - SKU 상세 서비스(see page 30)
  - AKS(Azure Kubernetes Service)(see page 30)
- AKS 클러스터 네트워크 옵션(see page 30)
  - Basic 네트워킹(see page 31)
  - Advanced 네트워킹(see page 31)
- Cloud shell 소개(see page 33)
  - 기본 제공되는 유틸리티 목록(see page 34)
  - 프로그래밍 언어 지원(see page 35)
- Resource Group(see page 35)