



Azure Landing Zone

Cloocus

Focus on Cloud

Microsoft Azure Consulting Expert Group

Cloocus

Gold
Microsoft
Partner


Azure
Expert
MSP

Contents

01 Azure Landing Zone이란?

1-1. Overview

1-2. Key word

02 주요 서비스(Azure)

2-1. 계정 권한 관리(Azure Active Directory, Identity and Access Management)

2-2. 시스템 운영 정책(Compliance, Key Management)

2-3. 보안 관리(Network Security Group, Azure Security Center)

2-4. 로그 관리(Azure Log Analytics)

03 Azure Blueprint

3-1. 배포 방식 (Custom Deployment, Azure Blueprint)

3-2. Blueprint 살펴보기



Azure

Landing Zone이란? 어떻게?

Key word



계정 권한 관리

- Azure Active Directory
- Identity and Access Management



보안 관리

- Azure Security Center
- (참고)시스템 취약점 진단 서비스



운영정책 관리

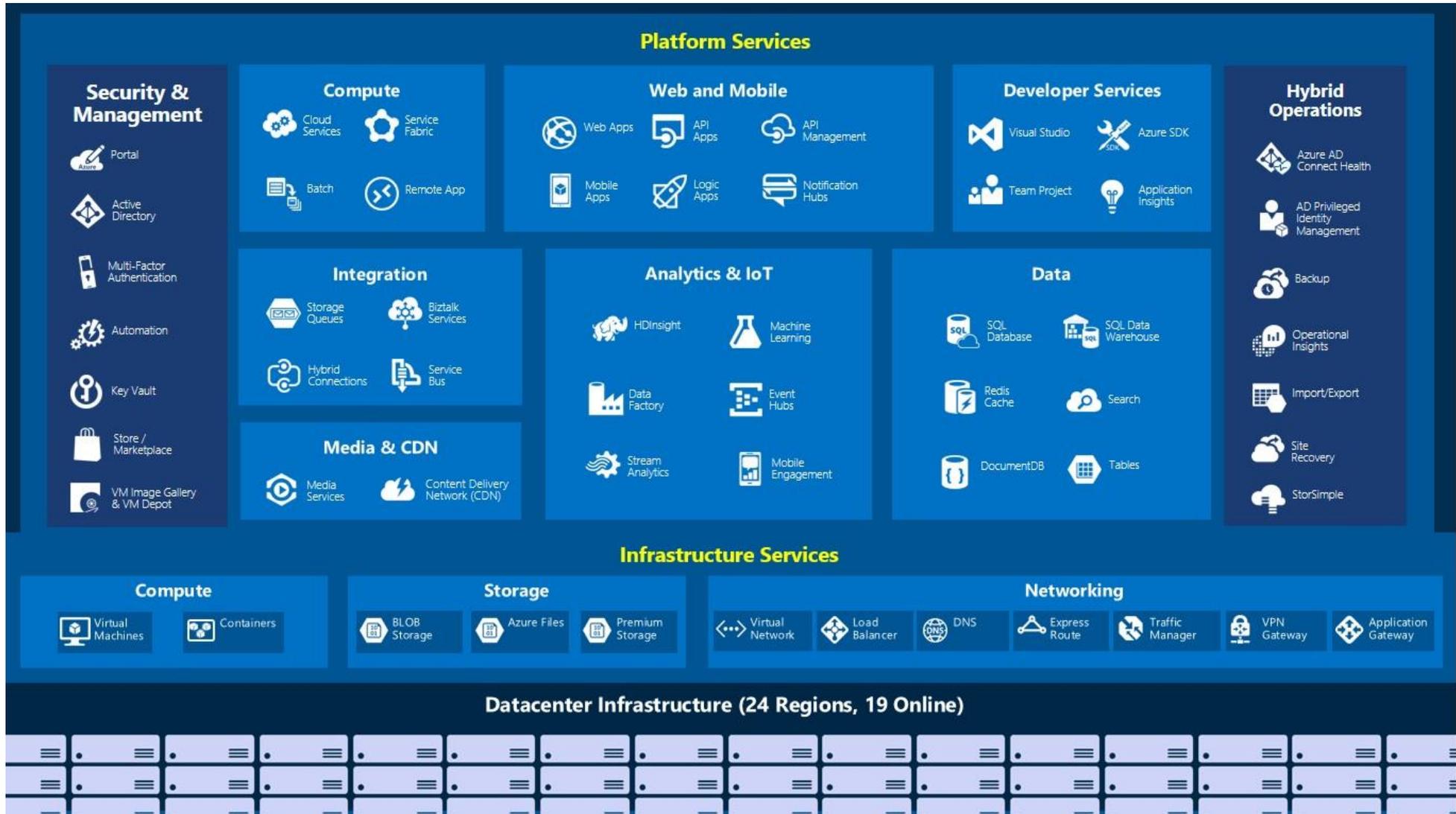
- Azure Policy
- Azure Key Vault(암호/키/인증서)
- (참고)Compliance Solutions



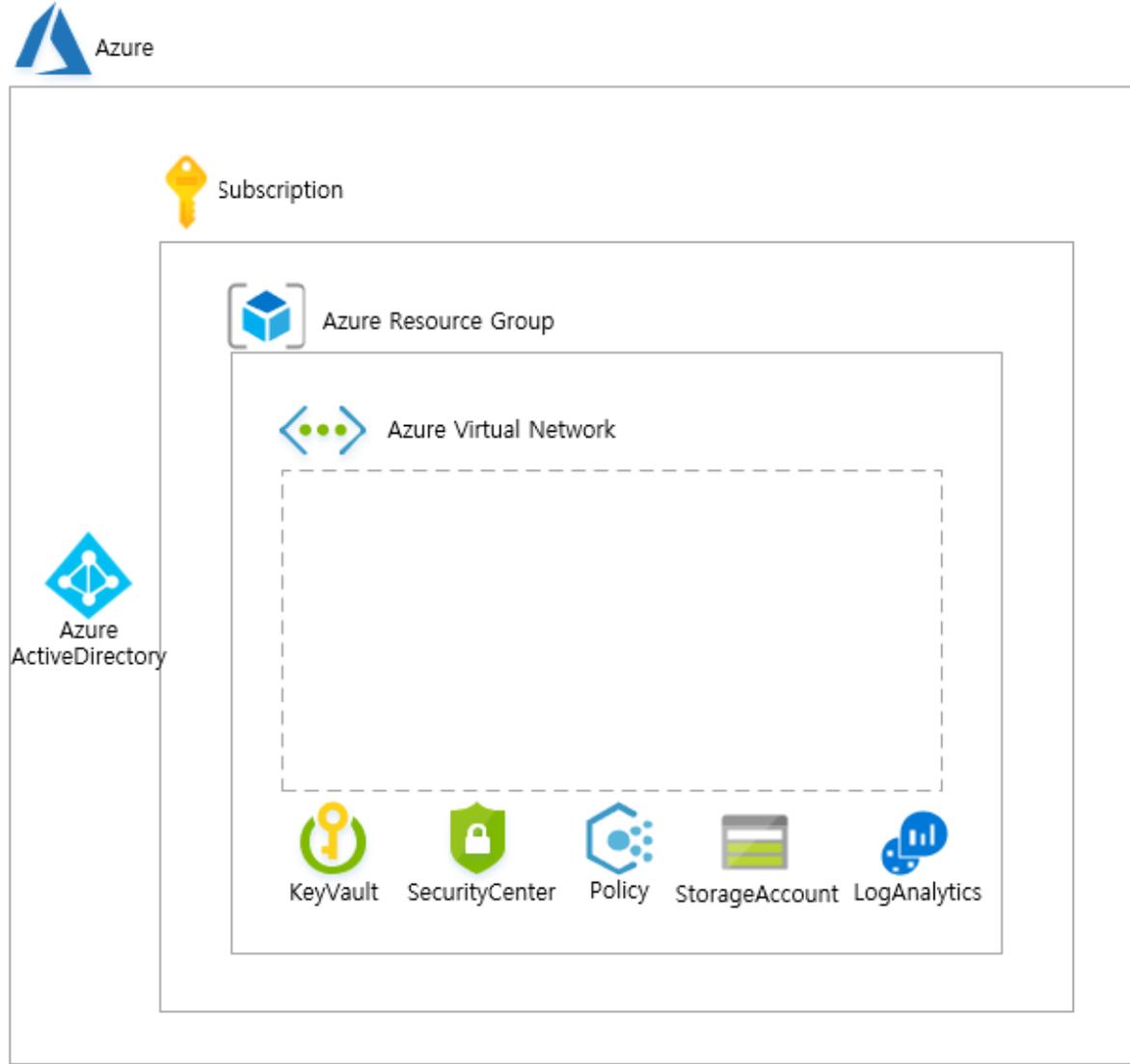
로그 중앙화

- Azure Log Analytics
- (참고)로그 관리 시스템

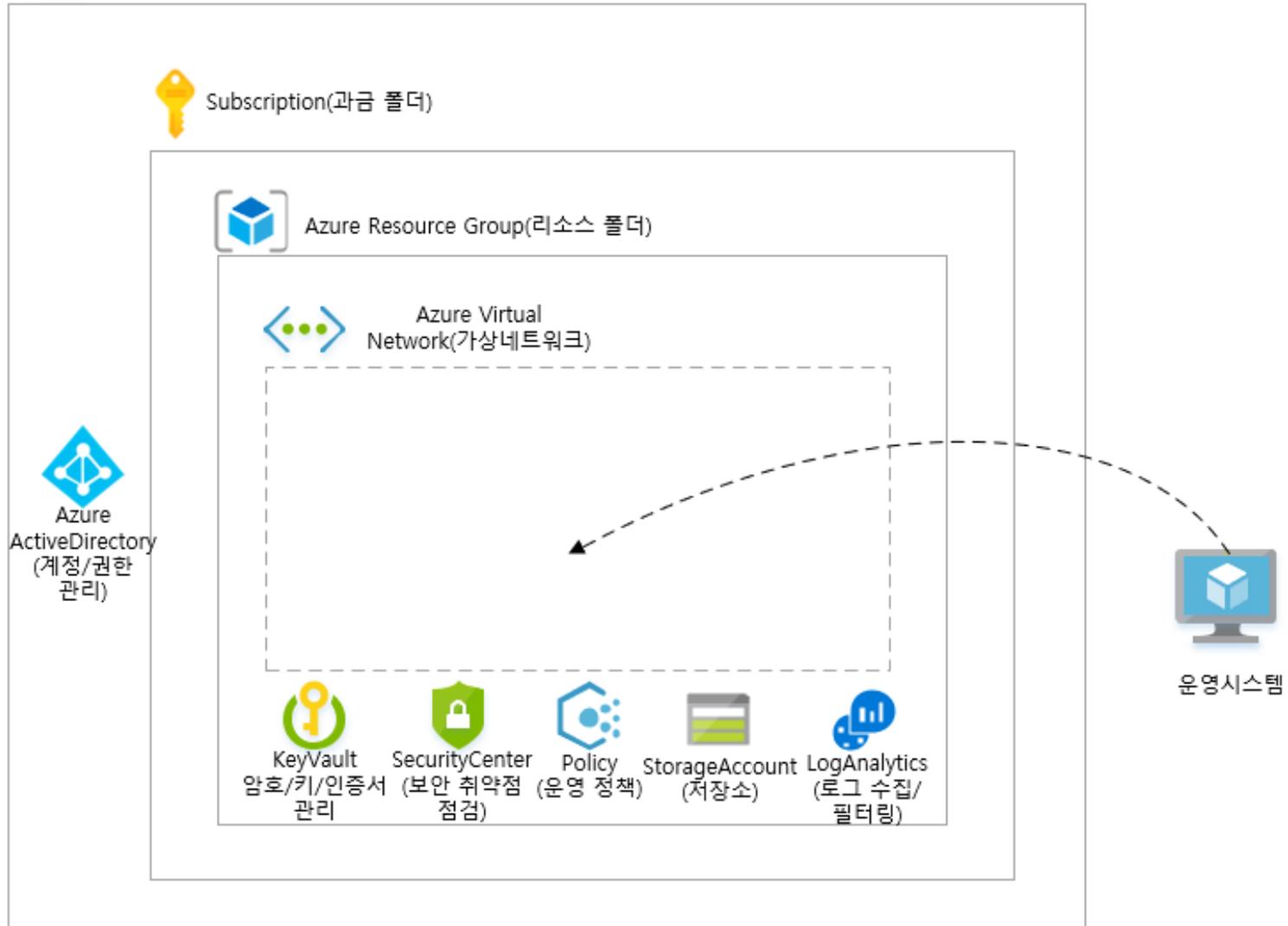
Azure Services



Overview



Overview





Azure Landing Zone 설계

1. 계정 권한 관리

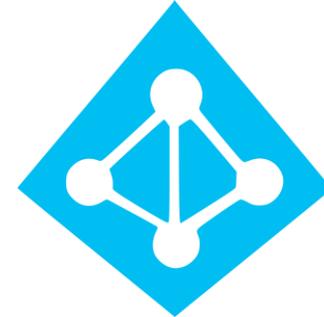
Azure Active Directory

[주요 기능]

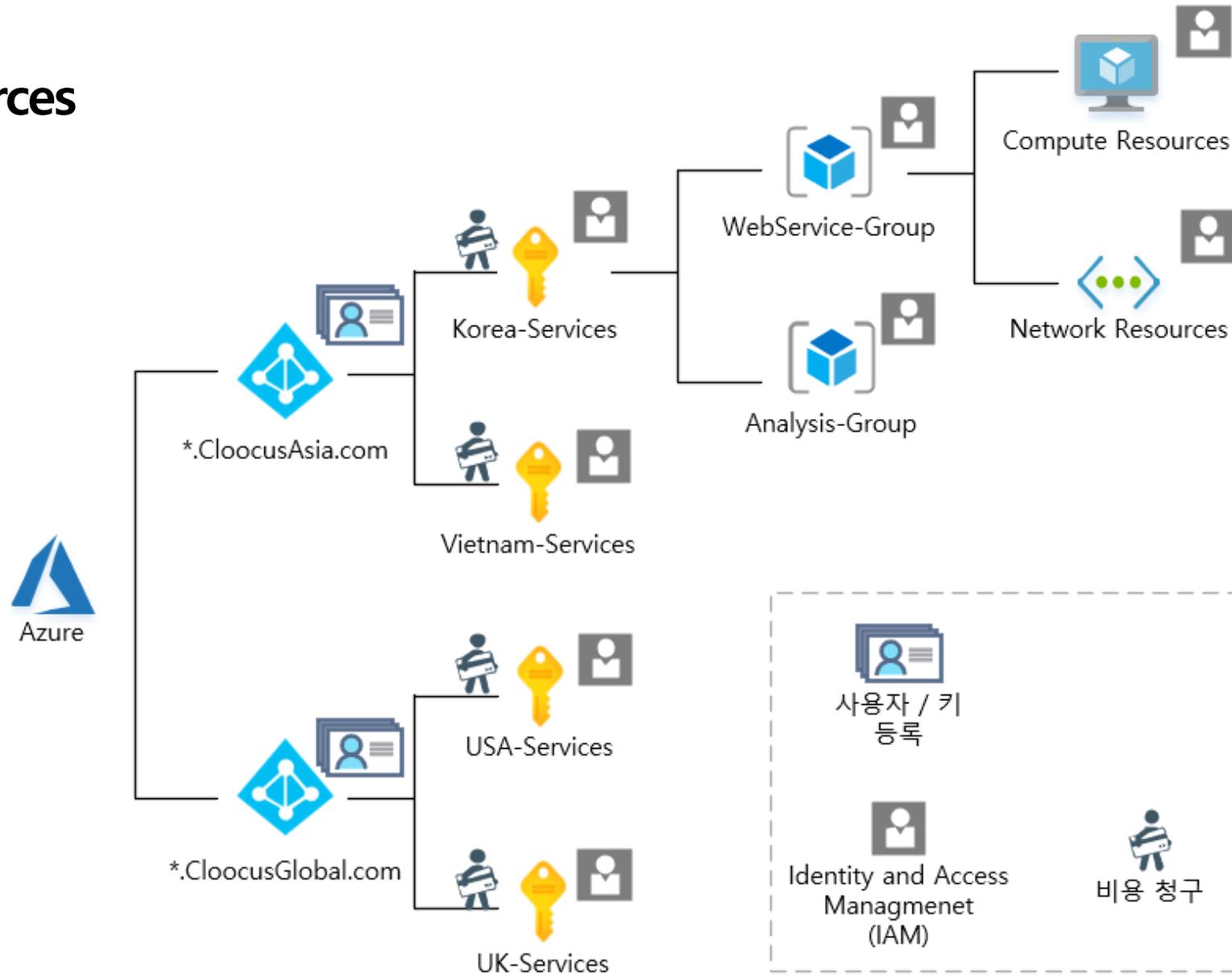
- 계정 생성 / 그룹 생성
- 액세스 키 생성 (앱 등록)
- 계정 별 역할 관리
- 외부 도메인 계정 추가 ex) cloocus@outlook.com
- 사용자 별 정책 기능은 Azure Policy 사용
- 네가지 등급의 기능 별 과금 체계 ex) 조건부 액세스, Just-In-Time 액세스

[장점]

- Multi-factor Authentication 기본 제공
- 등록된 계정으로 모든 Azure 리소스 관리
- Single-Sign-On (클라우드 지원 SaaS Apps, On-pre to Azure)



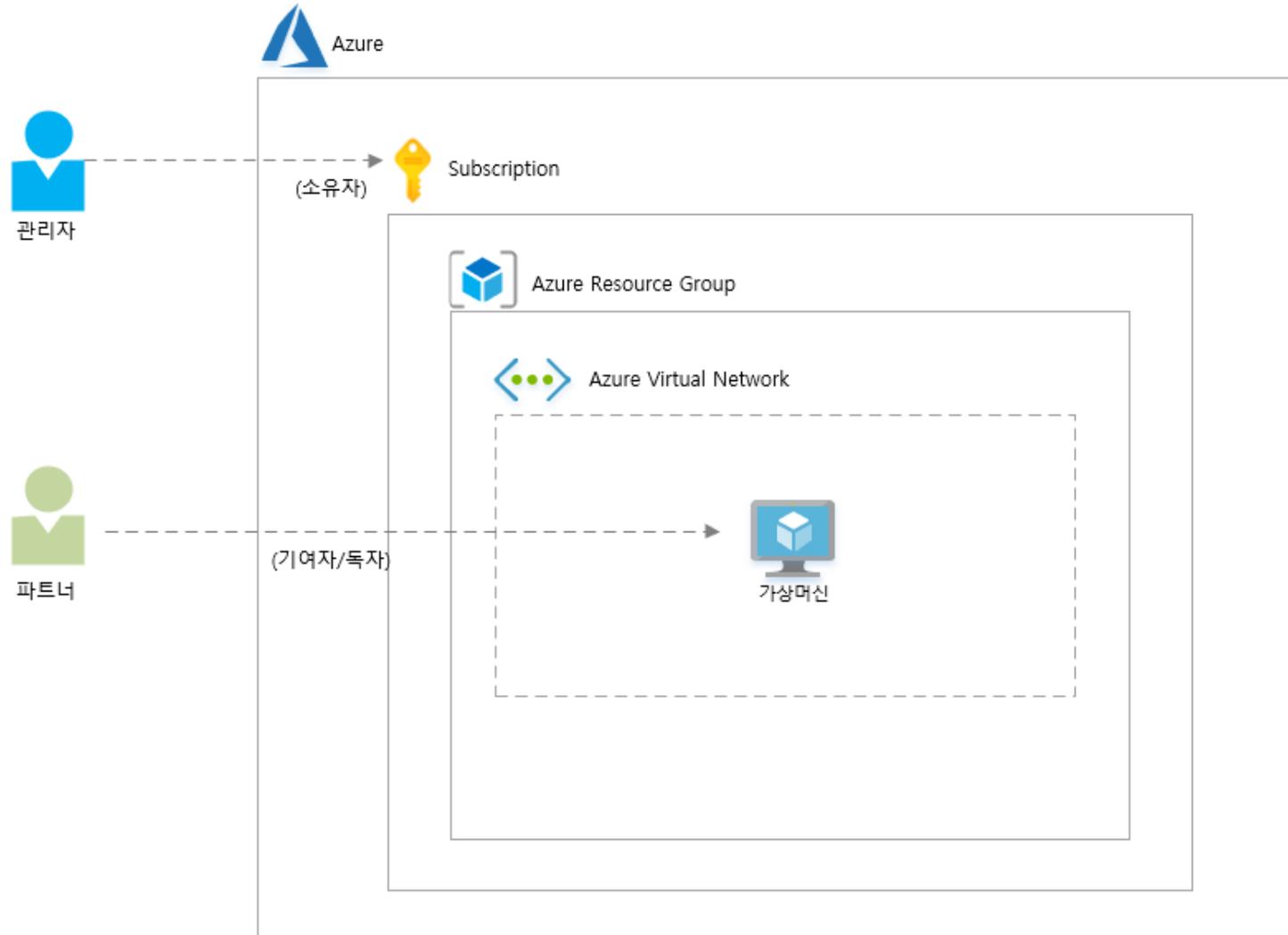
Azure Resources



자료 출처 : <https://docs.microsoft.com/ko-kr/azure/event-grid/overview>

Landing Zone 이란?

Overview





Azure Landing Zone 설계

2. 운영 정책

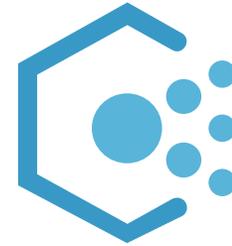
Azure Policy

[주요 기능]

- 정책 감사
- 그룹 별 정책 관리(이니셔티브)
- 커스텀 정책 생성(Json)

[장점]

- 국제 표준 운영 정책 패키지 제공(ISO27001:2013, PCI v3.2.1:2018 등)



Overview

매개 변수 포함 ⓘ

템플릿 매개 변수 스크립트

> ⚙ 매개 변수(3)
 📄 변수(0)
 ✓ 📦 리소스(1)
 🖥 [parameters('virtualMachines_spiderDB_name')]
 (Microsoft.Compute/virtualMachines)

```
17     },
18     "variables": {},
19     "resources": [
20       {
21         "type": "Microsoft.Compute/virtualMachines",
22         "apiVersion": "2019-07-01",
23         "name": "[parameters('virtualMachines_spiderDB_name')]",
24         "location": "koreacentral",
25         "properties": {
26           "hardwareProfile": {
27             "vmSize": "Standard_D2s_v3"
28           }
29       }
30     ]
31   }
32 }
```

정책 규칙

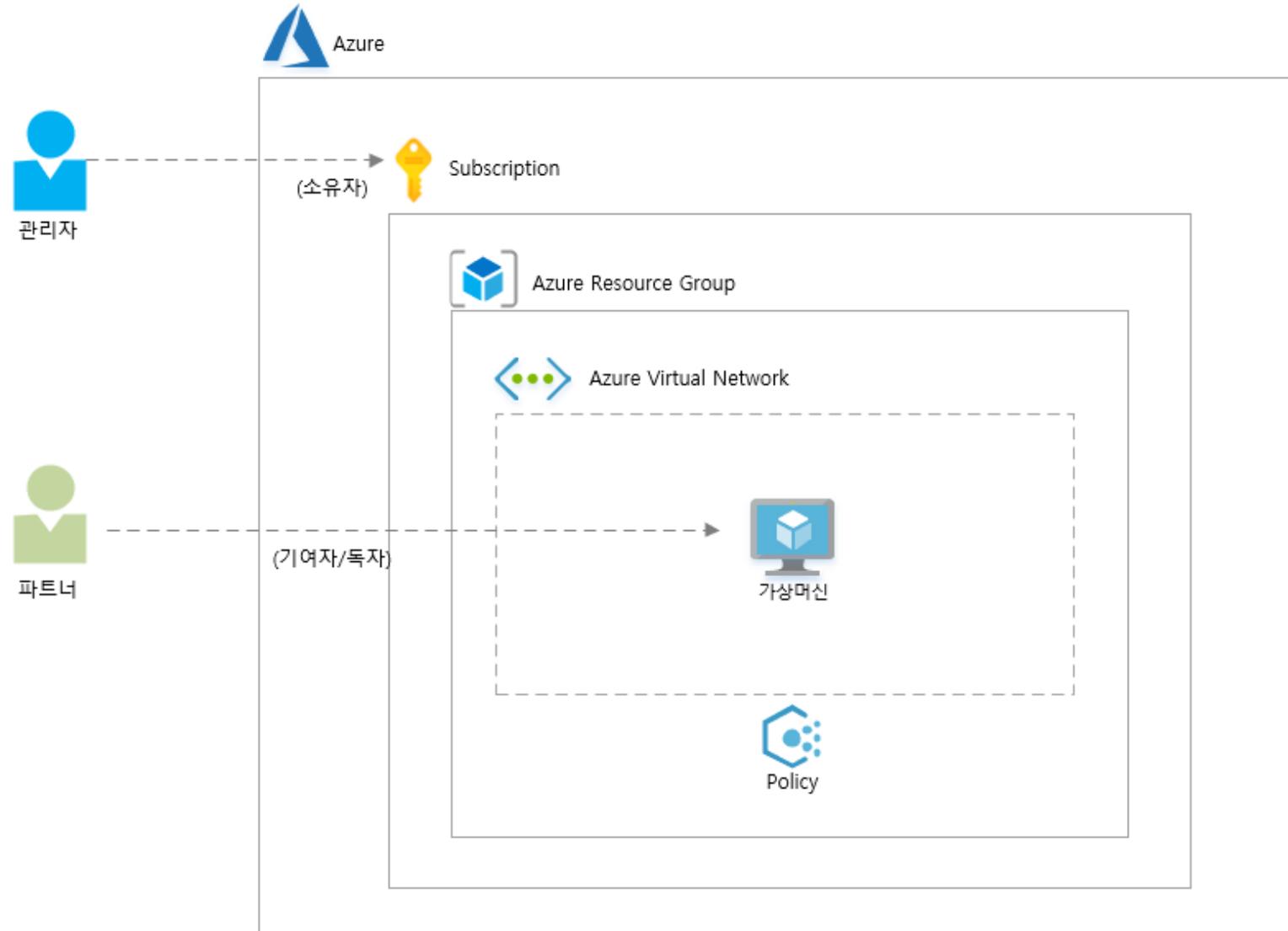
↓ [GitHub에서 샘플 정책 정의 가져오기](#)

🔗 [정책 정의 구조에 대한 자세한 정보](#)

```
1 {
2   "mode": "All",
3   "policyRule": {
4     "if": {
5       "allOf": [
6         {
7           "field": "type",
8           "equals": "Microsoft.Network/networkSecurityGroups/securityRules"
9         }
10      ]
11     }
12   }
13 }
```

Landing Zone 이란?

Overview



Azure Key Vault

[주요 기능]

- Key 관리 (생성, 권한, 유효기간)
- Secret 관리 (생성, 권한, 유효기간)
- 인증서 관리
- Azure Disk 암호화
- Azure SQL DB 암호화
- Azure Active Directory를 통한 역할 기반 액세스 정책

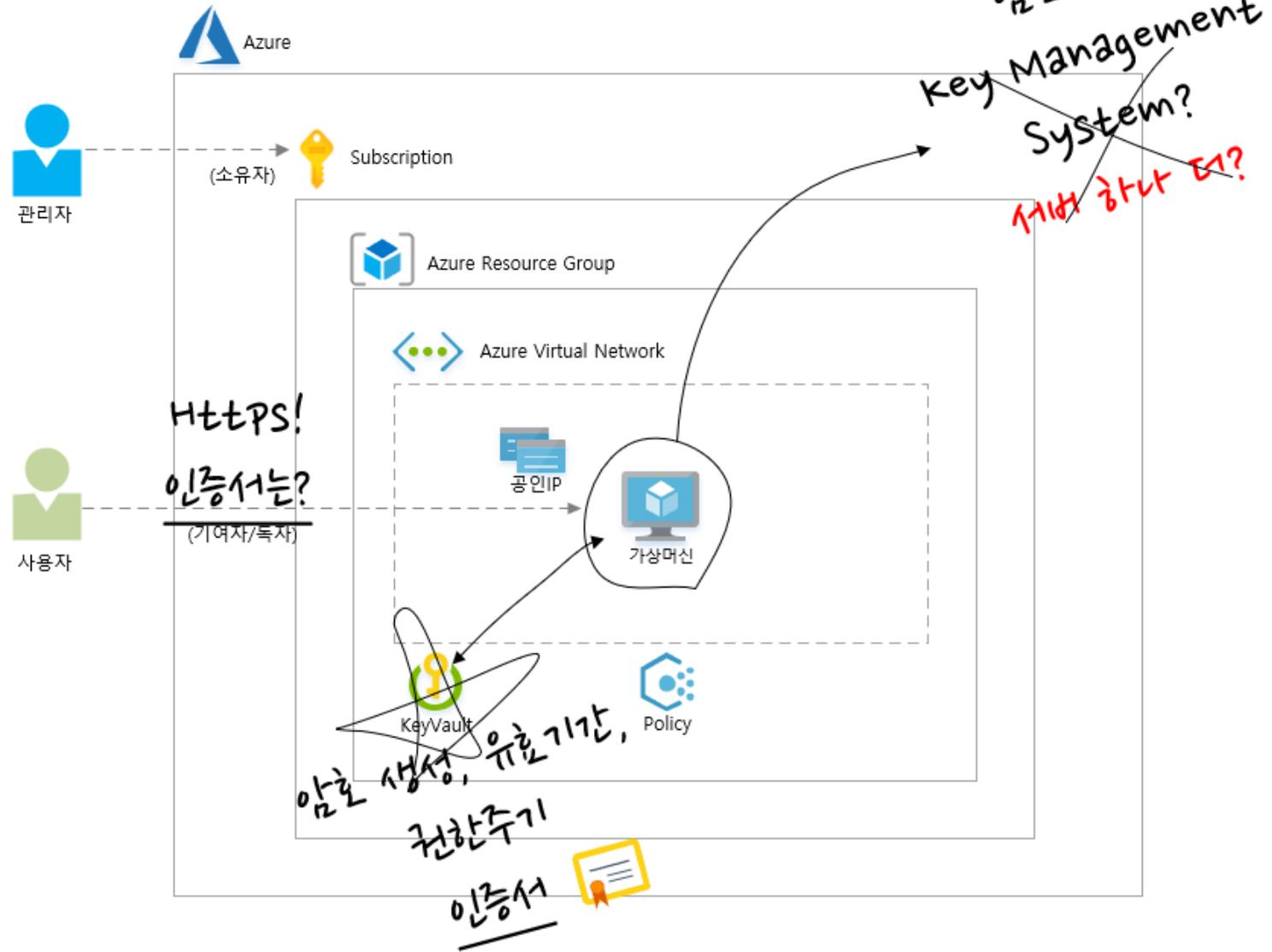
[장점]

- Azure 서비스와의 편리한 연동
- Transaction 당 과금



Landing Zone 이란?

Overview





Azure Landing Zone 설계

3. 보안 관리

- 네트워크
- 보안 정책

Azure Network Security Group(NSG)

[주요 기능]

- IP / Port 방화벽
- Subnet에 연결됨
- Network Interface (NIC)에 연결됨
- 최대 1000개 까지 정책 등록
- Azure 서비스에 대한 Tag 제공

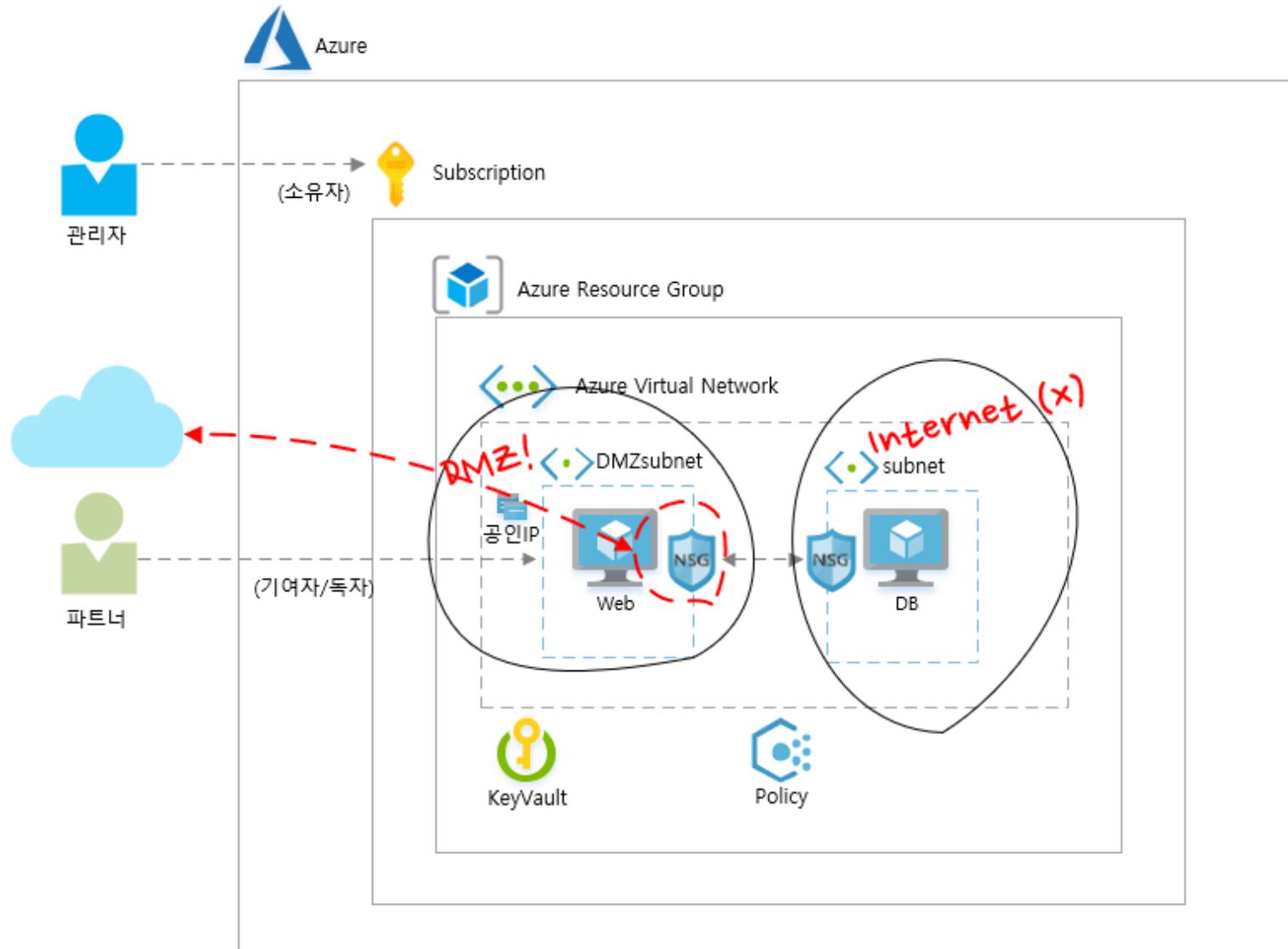
[장점]

- 무료
- 트래픽 로그 수집(추가 기능)



Landing Zone 이란?

Overview



Azure Security Center

[주요 기능]

- 클라우드 리소스 보안 감사
- 분석된 내용을 보안 점수로 평가
- 보안 기능 적용 방법 안내
- 국제 표준 패키지 (업계 표준 정책 제공 : ISO27001, PCI DSS 3.2.1 등)
- 사용자 지정 보안 점검 기준 작성(Preview)

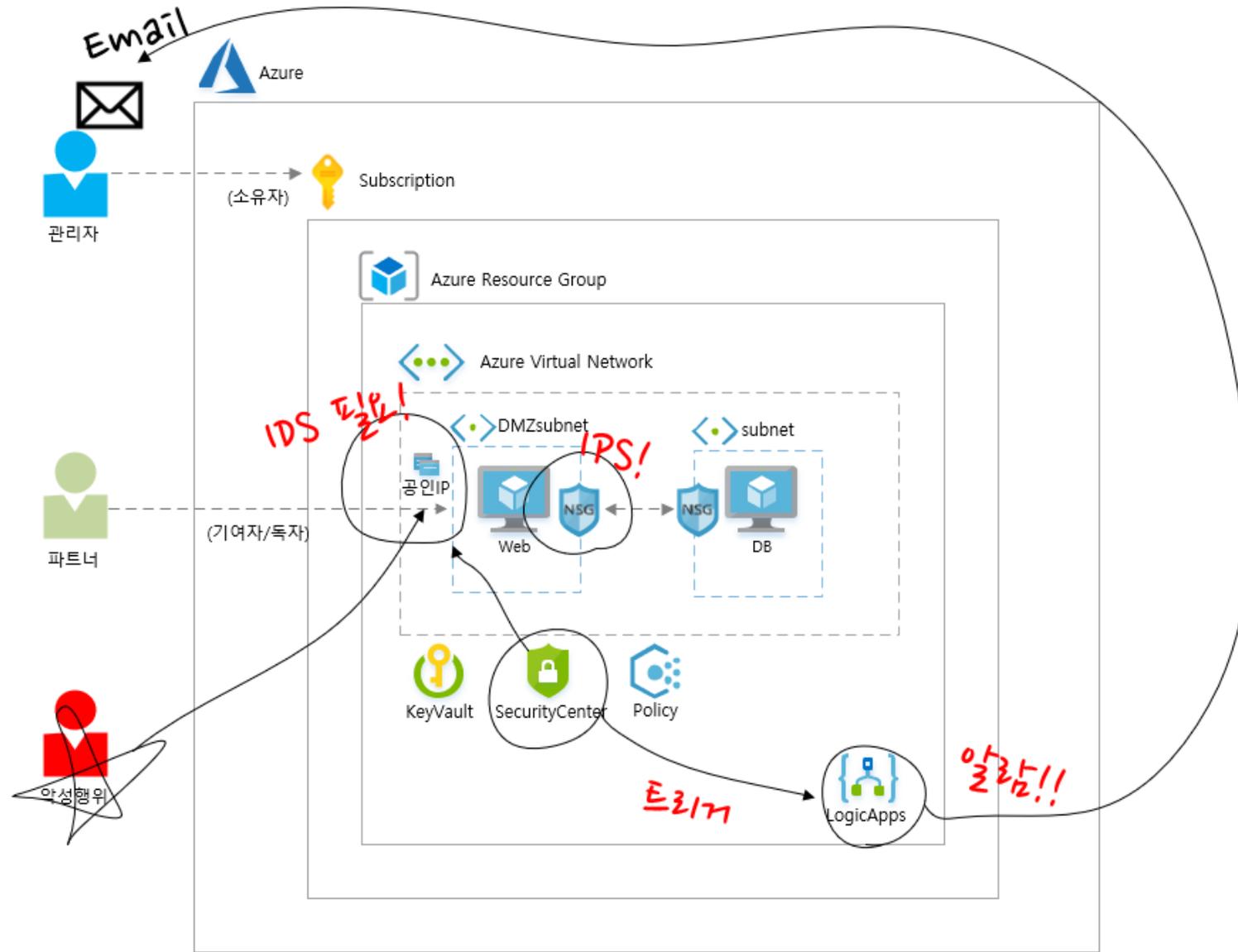
[장점]

- 보안 경고 발생 시 알람
- 업무 자동화 구축 가능 (Azure Logic Apps)
- Azure Defender 보안 경고 설정 (IDS/악성 행위 탐지)
- 리소스 별 과금



Landing Zone 이란?

Overview





Azure Landing Zone 설계

4. 로그 관리

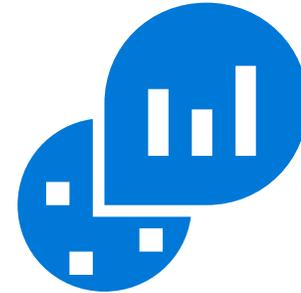
Azure Log Analytics

[주요 기능]

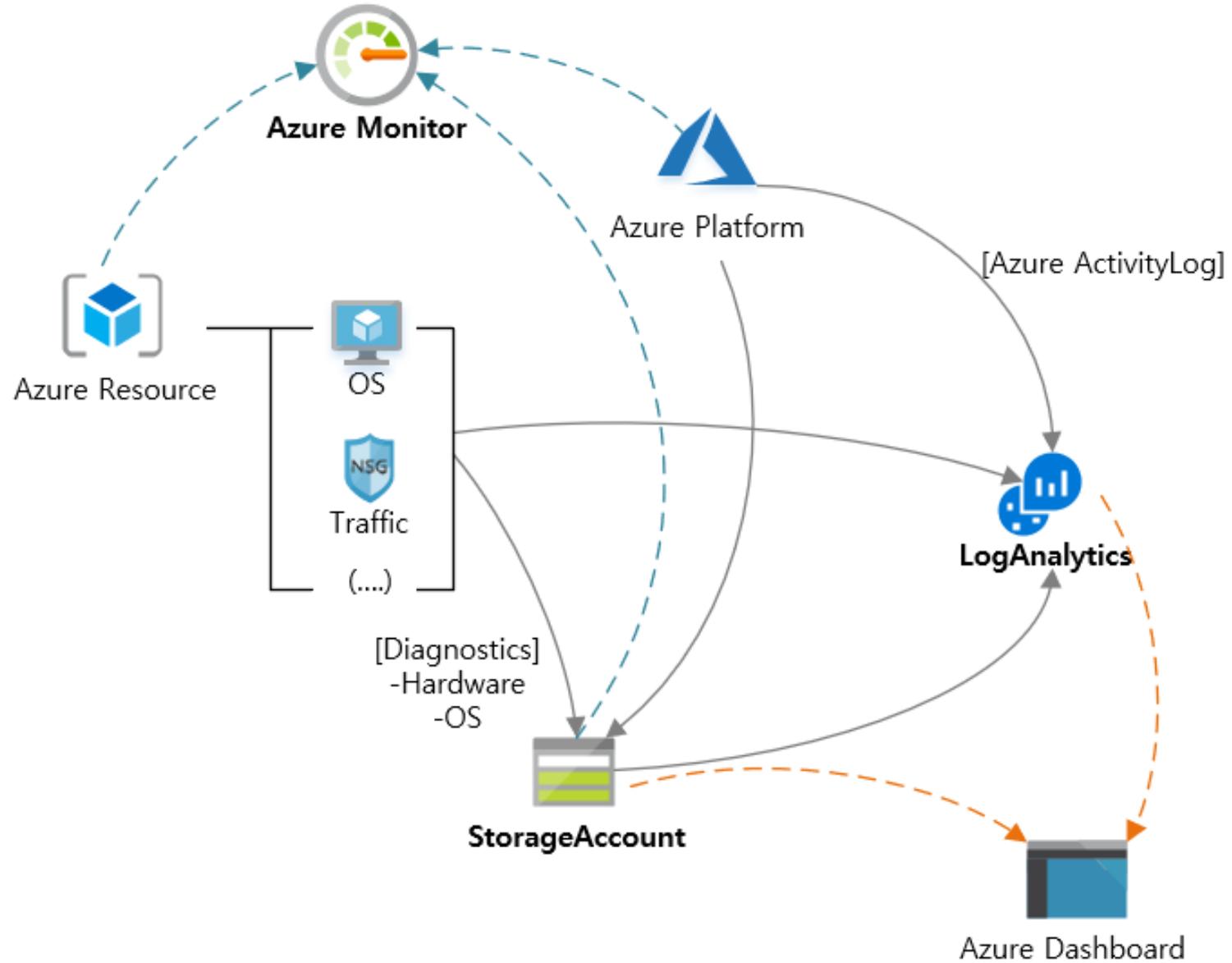
- 로그 수집(최소 10초)
- 로그 저장
- 로그 필터링(Kusto) / 차트 생성
- Azure Dashboard 연동 (Refresh 최소 5초)

[장점]

- Azure Platform + Operation System + Application Log 중앙 관리
- 무료 과금 구간

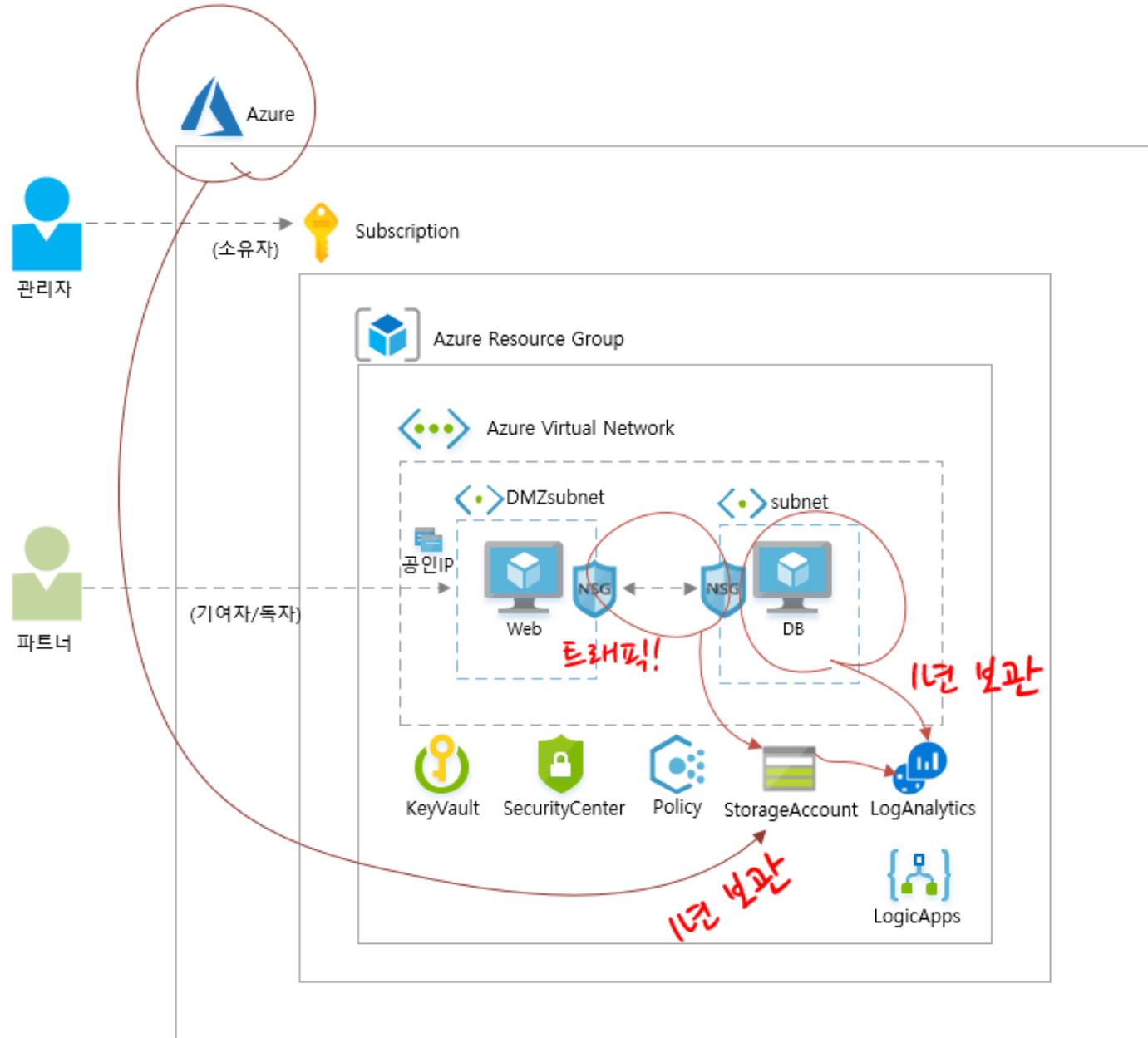


Overview



Landing Zone 이란?

Overview





Azure Landing Zone 설계

5. Azure Blueprint

Custom Deployment

[개념]

- 원하는 기능을 선별하여 배포
- Azure Resources 선택
- 자사 운영 정책에 맞는 커스텀 배포

[제안 기준]

- Azure 클라우드 운영에 필요한 특정 기능이 있을 경우.

Azure Blueprint

[개념]

- 국제 표준을 준수할 수 있도록 관리 기능을 패키지 형태로 제공

[제안 기준]

- 국제 표준 및 Azure 표준으로 운영 관리를 원하는 경우.

[제공된 패키지]

Azure 클라우드 채택 프레임워크

ISO27001 (정보보호관리체계)

일반 정책 (자주 사용되는 기능)

PCI-DSS (신용카드 데이터 보안 기준)

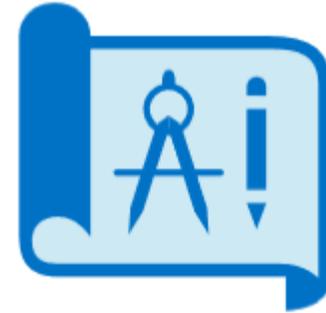
Azure Blueprint

[주요 기능]

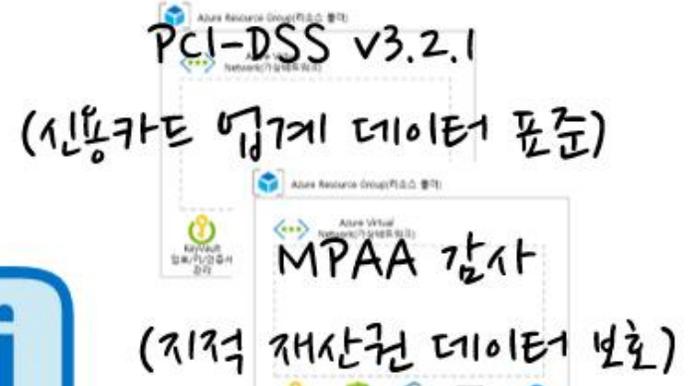
- 시스템 운영에 대한 국제 표준 패키지 제공(ISO27001, MPAA 등)
- Landing Zone 관련 리소스 배포
- Azure Policy 정책 활용
- 정책 패키지(청사진) 버전 관리

[장점]

- Cloud Landing Zone 버전 관리
- 자사 운영 환경에 맞는 커스텀 Landing Zone 구성



Overview

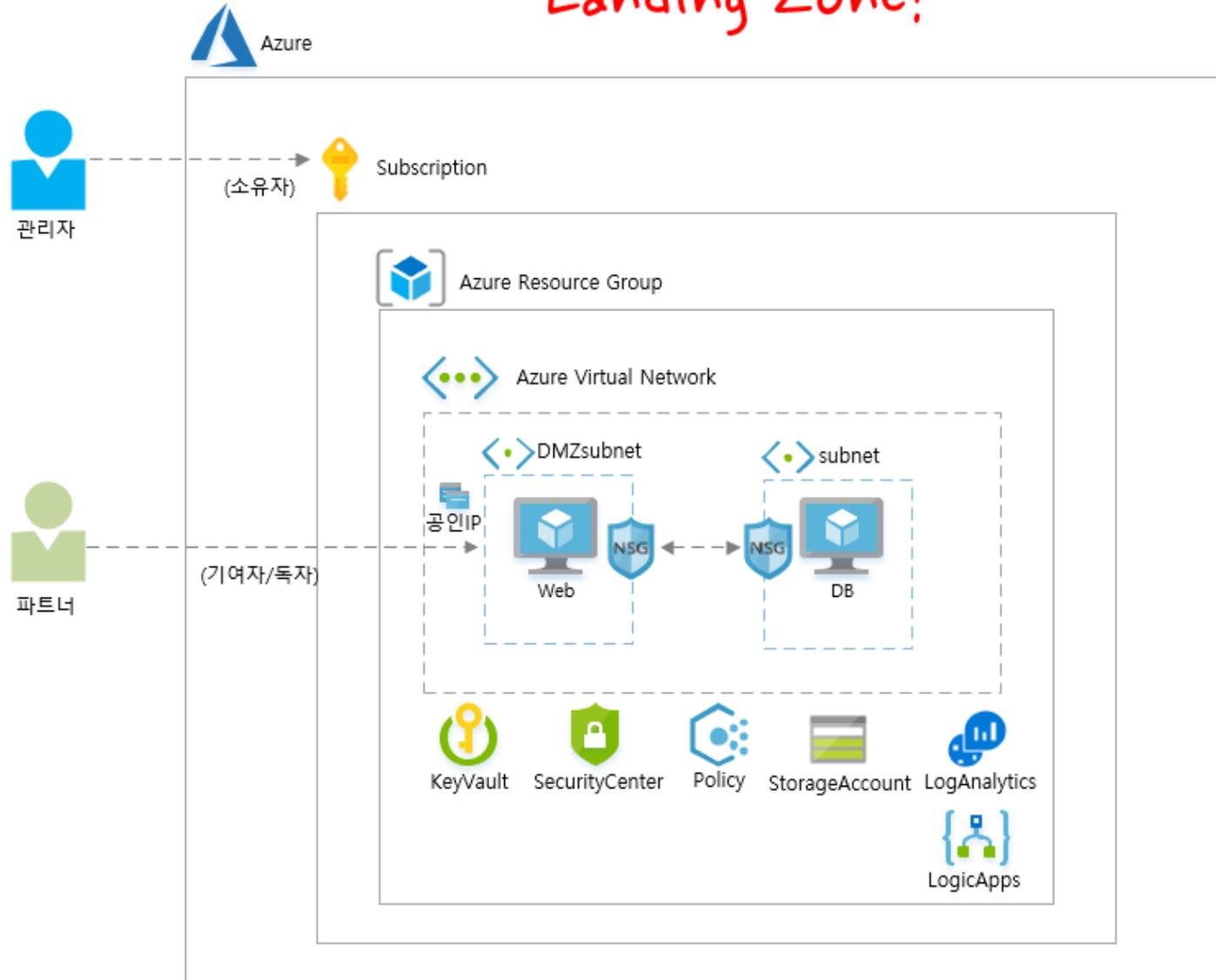


Azure Blueprint



Landing Zone 이란?

Overview





감사합니다.