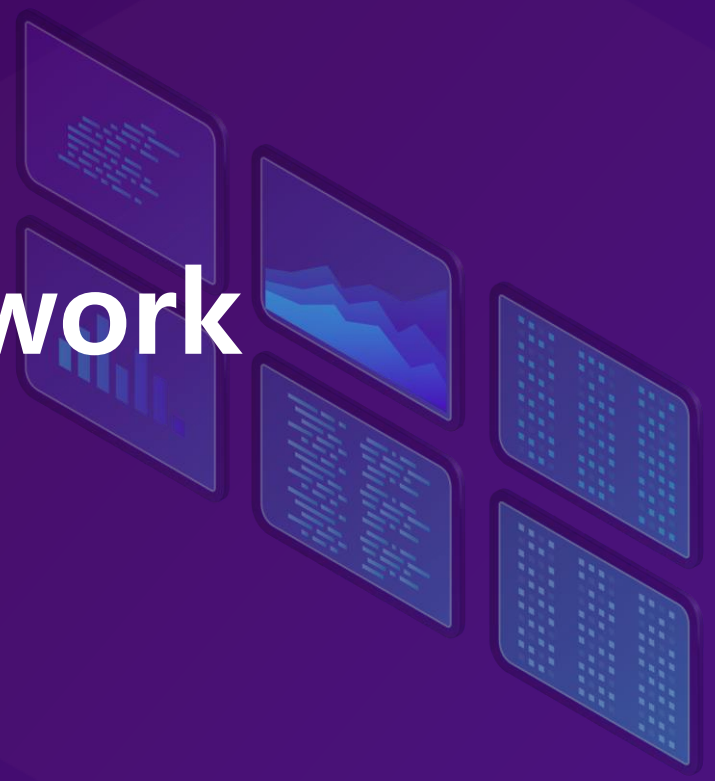
클라우드 환경 구현의 시작점

클라우드 랜딩존 with Cloud Adoption Framework



클루커스, 박항서 컨설턴트 (그룹 리드)

Cloocus Gold Microsoft Partner Azure Expert MSP

Final Update 2021.10.14 I Produced by Cloocus

Main Contents

01

Landing Zone 이란?

Landing Zone 이란?

개요

노트북 구매 전략

전략 정의

전략 정의

"동영상 강의 시청으로 영어 성적 20% 향상 "

계획

계획

노트북 모델 선정

노트북 관리자(큰아들)

Windows 10 학습 계획

무선 공유기 학습 계획

준비

(Landing Zone)

- 노트북 사용 시간
- 안티 바이러스 프로그램 구매
- Azure에 데이터 백업

채택

(마이그레이션)

노트북 설치

자동 종료 설정

성인 사이트 차단

(최적화)

OS 성능 최적화

게임을 위한 관리 방안

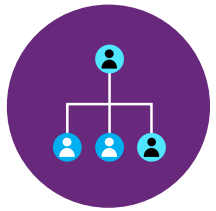
관리 방법 개선

Keyword

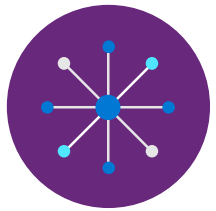
Landing Zone은 클라우드 리소스 마이그레이션 및 배포를 고려하는데 있어서 최적화된 운영을 위한 정책이자 관리 시스템 입니다.

엔터프라이즈 등록

Identity

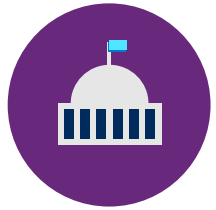


리소스 조직



네트워크 토폴로지
& 연결성

비즈니스 연속성
& 재해 복구



거버넌스 원칙

배포 옵션

운영 기준

02

거버넌스란(Governance)?

Landing Zone 개요

클라우드 거버넌스 방법론

클라우드 거버넌스 방법론을 통해 지속 가능한 운영 기준을 정의합니다. 클라우드에서는 정의된 운영 기준을 관리 시스템으로 배포하여 운영 효율성을 극대화 합니다.

거버넌스 방법론

거버넌스

비즈니스 위험

데이터 분류와 애플리케이션 중요도를 기반으로 진화하는 비즈니스 위험과 비즈니스 위험 허용 범위를 문서화

기업 정책 정의

정책 & 컴플라이언스

클라우드 채택 경계를 설정하기 위해 위험 결정을 정책 설명으로 변환

프로세스 운영

프로세스

기업 정책에 대한 위반 및 준수를 모니터링하는 프로세스 설정

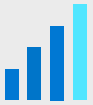
클라우드 거버넌스의 5가지 분야

비용 관리

비용을 평가 및 모니터링, IT 지출을 제한, 필요에 맞게 확장, 비용 책임감을 생성

보안 기준

모든 채택 노력에 보안 기준을 적용하여 IT 보안 요구 사항 준수를 보장



리소스 일관성

리소스 구성의 일관성을 보장.

온보딩, 복구, 검색에 대한 관행을 적용.

Identity 기준

역할 정의와 할당을 일관적으로 적용하여 Identity 및 액세스 기준이 적용되도록 보장

배포 가속화

템플릿 배포 전반에 걸쳐 중앙 집중화, 일관성 및 표준화를 통해 배포를 가속화

Landing Zone 개요

Azure Policy – 비용관리

비즈니스 단위 전체에 적절한 비용 할당을 보장하기 위해 제어와 프로세스를 설정하고 애플리케이션의 비용을 분석

☑ 정의

- 비용 관리 예산 및 경고 + RACI
- 비용 관리 RBAC 모델

☑ 비용 관리 정책 정의

- 태깅
- **허용되는 VM SKU**
- 허용되는 스토리지 SKU
- 허용되는 네트워킹 SKU
- 허용되는 데이터베이스 SKU

* RACI (Responsible, Accountable, Consulted, Informed)

Cloocus

Azure 도구 및 서비스

Azure Policy

Azure 마켓플레이스의 Azure 비용 관리 FBI 애플리케이션

Azure Advisor

Azure 포털

Azure EA 컨텐츠 팩

Azure Policy – 비용관리

Allowed virtual machine size SKUs

Policy definition

Assign | Edit definition | Duplicate definition | Delete definition | Export definition

Essentials

Name	: Allowed virtual machine size SKUs	Definition location	
Description	: This policy enables you to specify a set of virtual machine size SKUs that your organization can deploy.	Definition ID	
Available Effects	: Deny	Type	
Category	: Compute	Mode	

Definition | Assignments (0) | Parameters

```
{
  "properties": {
    "displayName": "Allowed virtual machine size SKUs",
    "policyType": "BuiltIn",
    "mode": "Indexed",
    "description": "This policy enables you to specify a set of virtual machine size SKUs that your organization can deploy.",
    "metadata": {
      "version": "1.0.1",
      "category": "Compute"
    },
    "parameters": {
      "listOfAllowedSKUs": {
        "type": "Array",
        "metadata": {
          "description": "The list of size SKUs that can be specified for virtual machines.",
          "displayName": "Allowed Size SKUs",
          "strongType": "VMSKUs"
        }
      }
    },
    "policyRule": {
      "if": {
        "allOf": [
          {
            "field": "type",
            "equals": "Microsoft.Compute/virtualMachines"
```

Landing Zone 개요

Azure Policy – 보안 기준

네트워크, 자산 및 데이터를 보호하기 위한 정책 설정

☑ 보안과 관련된 위험, 비즈니스 허용 범위, 완화 전략을 문서화:

- 데이터 및 자산: 가장 중요한 데이터 자산을 식별하고 보호하고 모니터링하기 위해 명확한 가이드라인을 개발
- 네트워크: 온-프레미스 환경과 클라우드 워크로드간 허용되는 모든 커뮤니케이션을 제어하고 모니터링

☑ 기업 정책에 대한 모범 사례를 구현:

- **네트워크 요구 사항: 권한이 부여되지 않은 액세스로부터 보호**
- 하이브리드 Identity 전략: 클라우드 기반 Identity와 기존 온-프레미스 Identity의 통합
- 암호화: 비밀과 키가 저장되고 관리되는 방식 정의
- 보안 기준 정책: 보안 정책 업데이트를 관리하는 프로세스 정의 (예, 초기 위험 평가 및 계획, 배포 계획 및 테스트, 분기별 검토 및 계획)

Azure 도구 및 서비스

Azure Policy

Azure Security Center

Azure Sentinel

구독 디자인

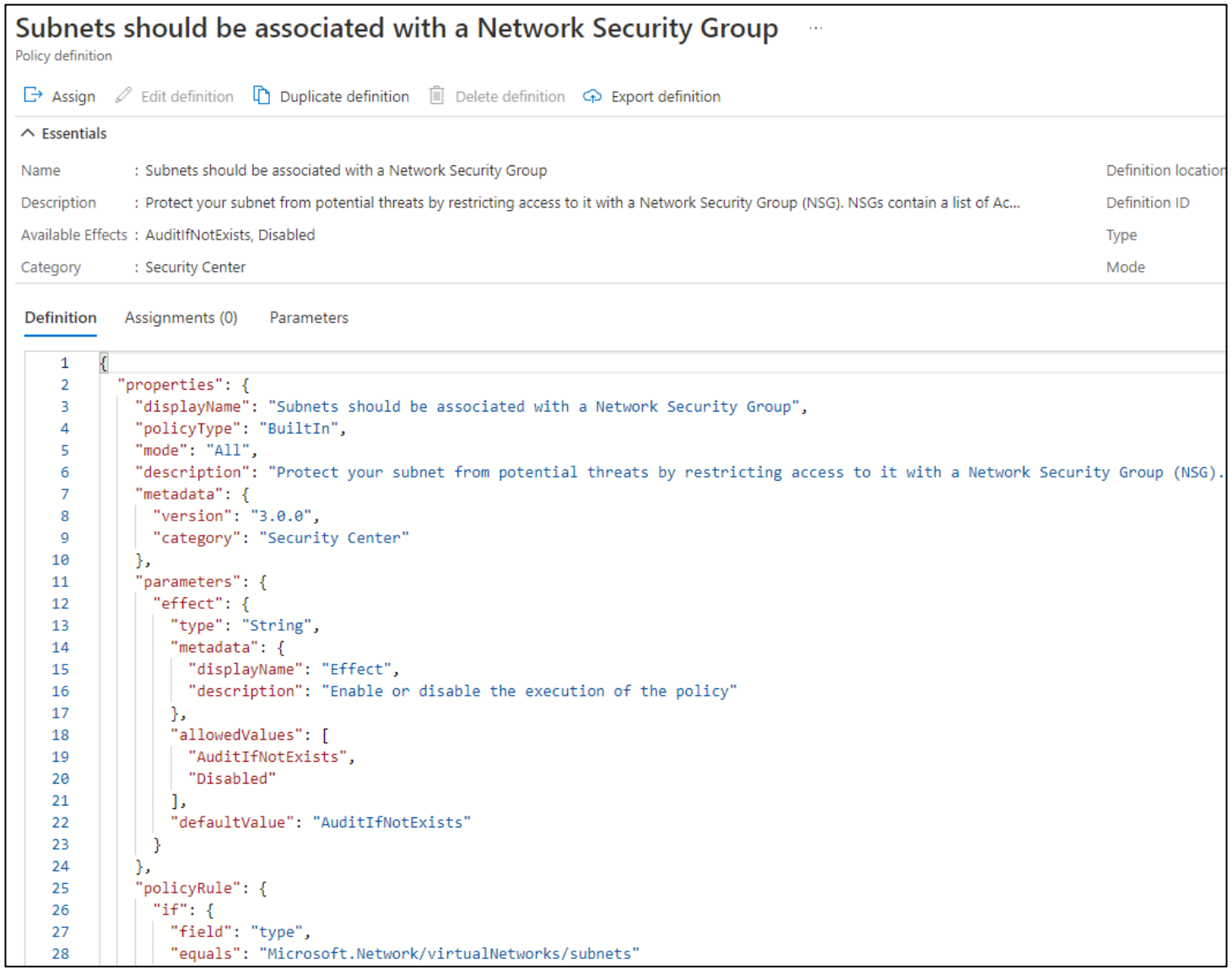
암호화

하이브리드 Identity

Azure 네트워킹

Azure Automation

Azure Policy – 보안 기준



Subnets should be associated with a Network Security Group

Policy definition

Assign | Edit definition | Duplicate definition | Delete definition | Export definition

Essentials

Name	: Subnets should be associated with a Network Security Group	Definition location	
Description	: Protect your subnet from potential threats by restricting access to it with a Network Security Group (NSG). NSGs contain a list of Ac...	Definition ID	
Available Effects	: AuditIfNotExists, Disabled	Type	
Category	: Security Center	Mode	

Definition | Assignments (0) | Parameters

```
{
  "properties": {
    "displayName": "Subnets should be associated with a Network Security Group",
    "policyType": "BuiltIn",
    "mode": "All",
    "description": "Protect your subnet from potential threats by restricting access to it with a Network Security Group (NSG).
    "metadata": {
      "version": "3.0.0",
      "category": "Security Center"
    },
    "parameters": {
      "effect": {
        "type": "String",
        "metadata": {
          "displayName": "Effect",
          "description": "Enable or disable the execution of the policy"
        },
        "allowedValues": [
          "AuditIfNotExists",
          "Disabled"
        ],
        "defaultValue": "AuditIfNotExists"
      }
    },
    "policyRule": {
      "if": {
        "field": "type",
        "equals": "Microsoft.Network/virtualNetworks/subnets"
```

Azure Policy – 리소스 일관성

클라우드 리소스에 대한 일관성 구현

☑ Azure 관리 그룹 & 구독 모델 및 RACI 정의

- 보안, 운영 및 비즈니스/회계 계층 구조를 반영
- 유사한 리소스를 논리적 컬렉션으로 그룹화

☑ 리소스 일관성 역할 & 책임을 정의

- 애플리케이션 혹은 워크로드를 배포 및 운영 단위로 그룹화

☑ 리소스 일관성 정책 정의

- 명명 규칙
- 태깅
- **허용되는 위치**
- 허용되는 리소스 유형
- 허용되는 확장
- 감사

Azure 도구 및 서비스

Azure Policy

Azure Monitor

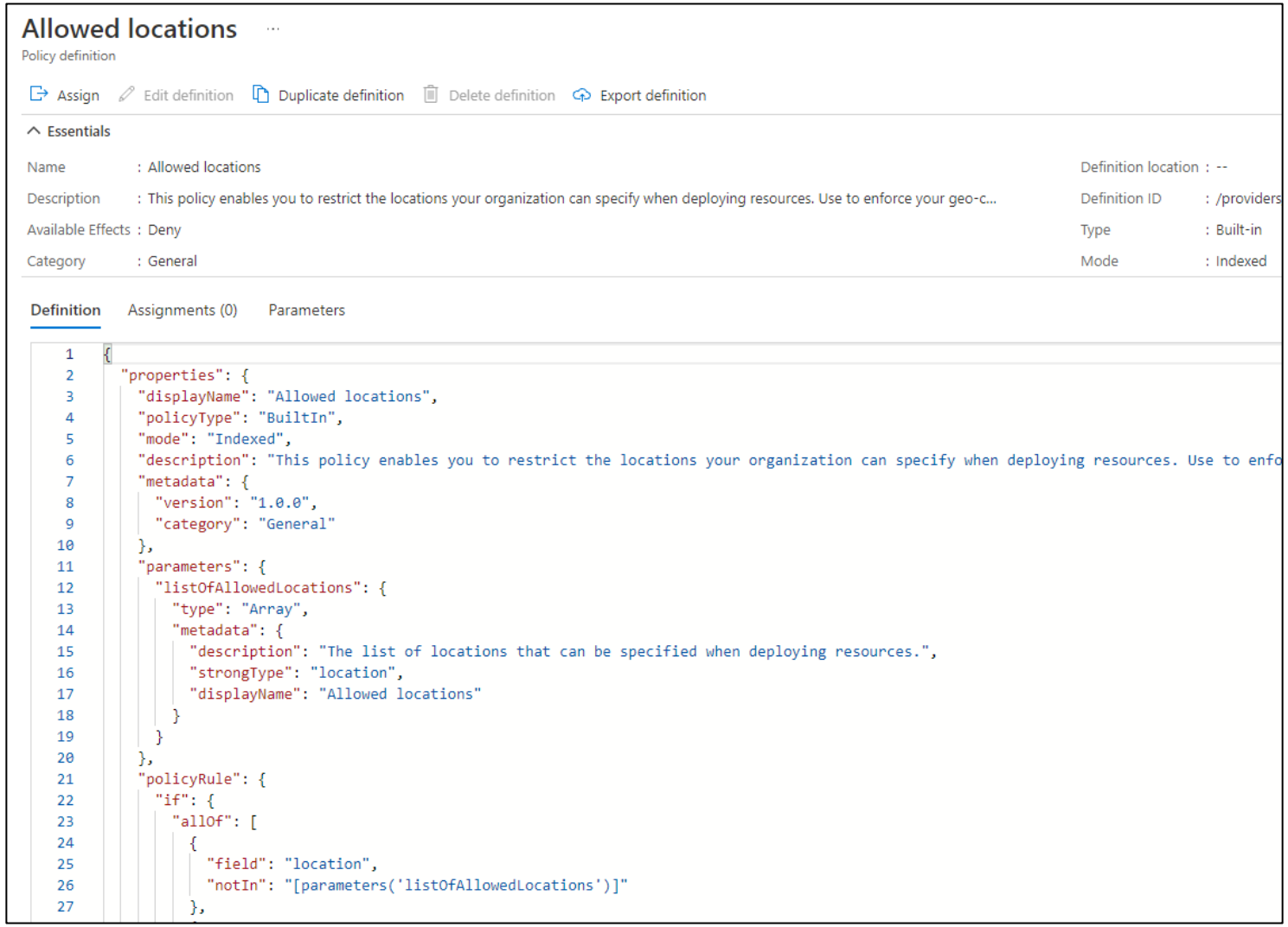
Azure Advisor

리소스 관리자 템플릿

Resource Graph

관리 그룹

Azure Policy – 리소스 일관성



Azure RBAC – Identity

Identity 관리와 액세스 제어를 구현

☑ Azure RBAC 모델 정의

- RBAC을 사용하여 팀 내의 책임을 분리
- 하고 작업을 수행하는데 필요한 사용자에게만 권한을 부여

☑ Azure 액세스 관리 프로세스와 RACI 정의

- 비용과 복잡성이 다양한 클라우드 환경에서 Identity를 관리

☑ Azure 권한 있는 Identity 관리 운영operationalize

- 클라우드 기반 Identity는 반복적인 관리 프로세스로 운영됨

Azure 도구 및 서비스

RBAC

Azure AD

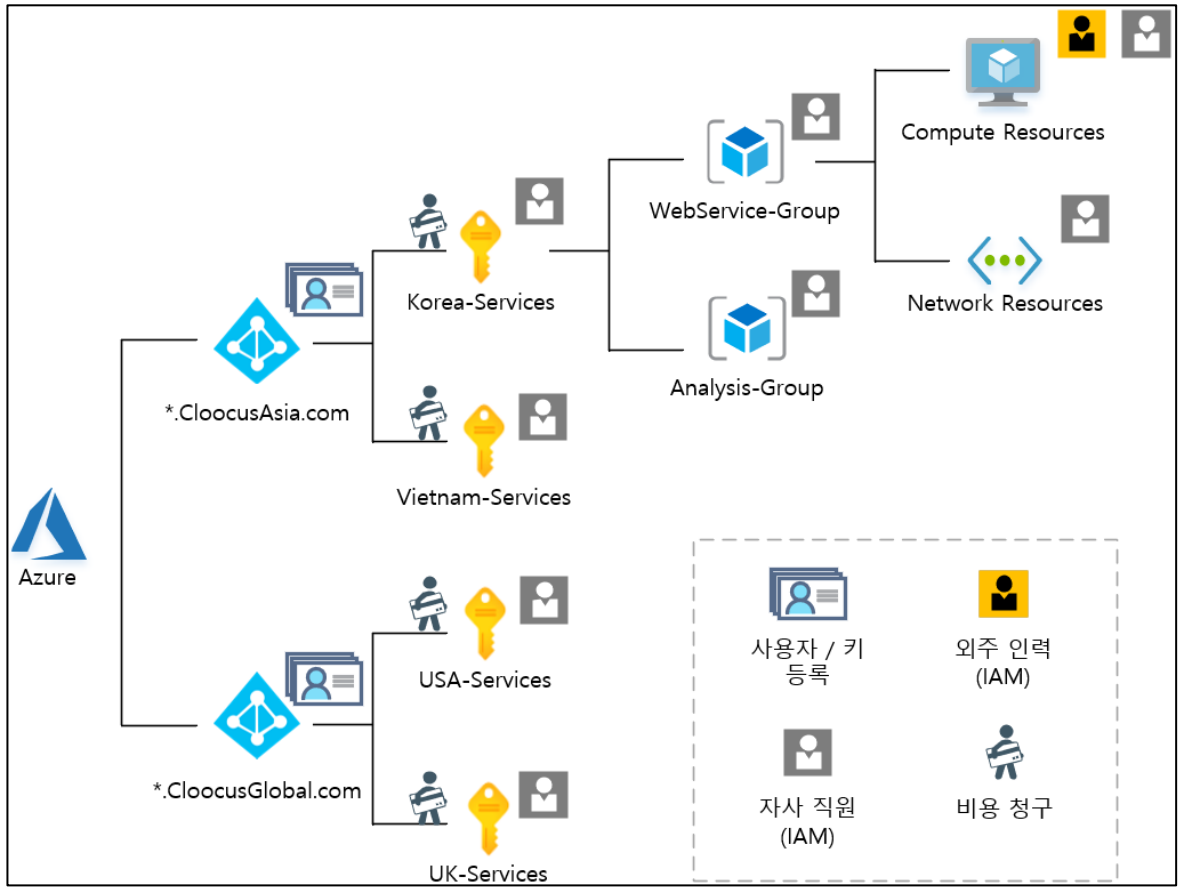
Azure AD B2B

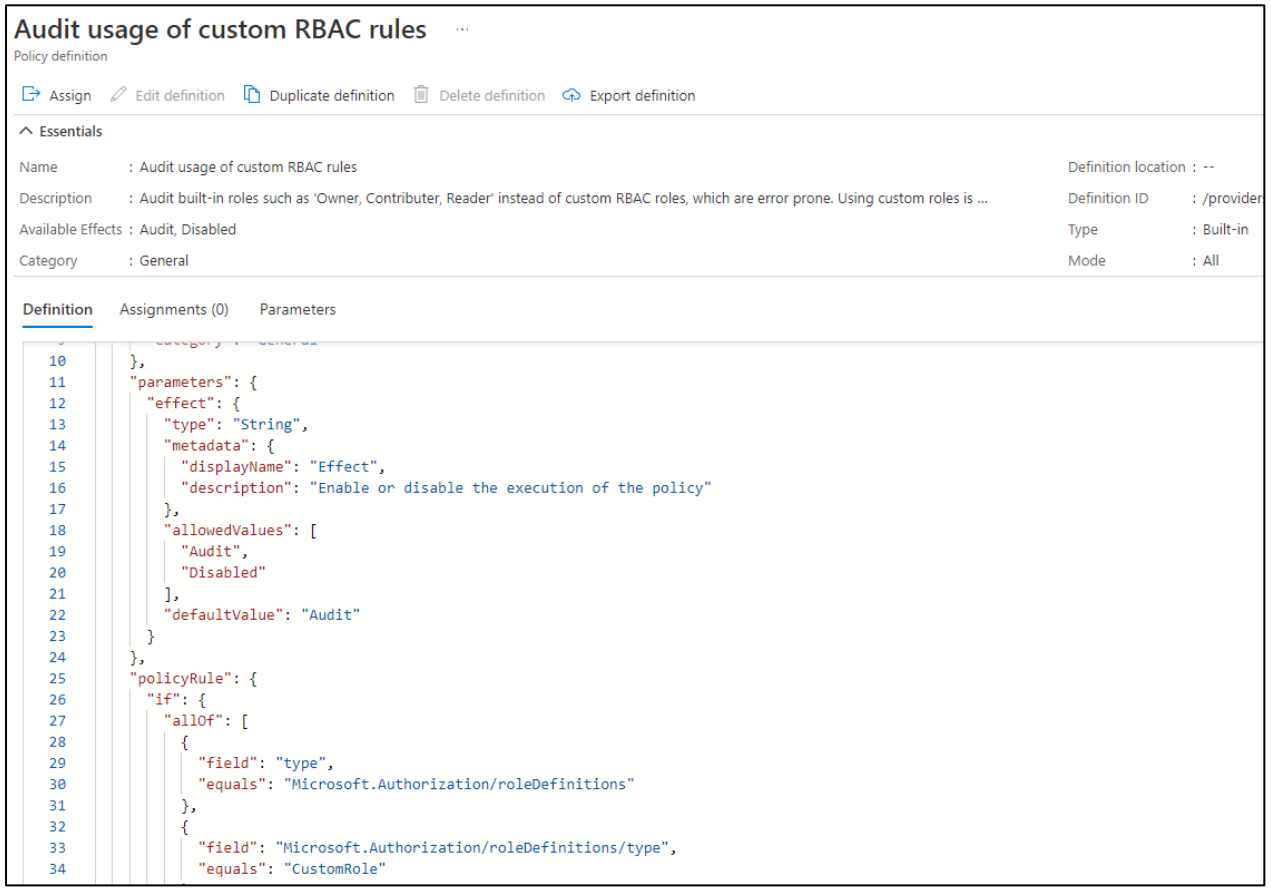
Azure AD B2C

디렉터리 페더레이션

디렉터리 복제

Azure RBAC – Identity





Audit usage of custom RBAC rules

Policy definition

Assign | Edit definition | Duplicate definition | Delete definition | Export definition

Essentials

Name	: Audit usage of custom RBAC rules	Definition location	: --
Description	: Audit built-in roles such as 'Owner, Contributer, Reader' instead of custom RBAC roles, which are error prone. Using custom roles is ...	Definition ID	: /provider
Available Effects	: Audit, Disabled	Type	: Built-in
Category	: General	Mode	: All

Definition | Assignments (0) | Parameters

```
10      },
11      "parameters": {
12        "effect": {
13          "type": "String",
14          "metadata": {
15            "displayName": "Effect",
16            "description": "Enable or disable the execution of the policy"
17          },
18          "allowedValues": [
19            "Audit",
20            "Disabled"
21          ],
22          "defaultValue": "Audit"
23        }
24      },
25      "policyRule": {
26        "if": {
27          "allOf": [
28            {
29              "field": "type",
30              "equals": "Microsoft.Authorization/roleDefinitions"
31            },
32            {
33              "field": "Microsoft.Authorization/roleDefinitions/type",
34              "equals": "CustomRole"
```

Landing Zone 개요

Azure Devops – 배포가속화

DevOps 통해 CI/CD 구현

☑ Infrastructure as code

- 신속한 환경 구축
- 인적 요소를 제거하고 신뢰할 수 있고 반복적인 방법으로 배포
- 환경 가시성과 개발자 효율성을 개선
- 인프라 정의를 애플리케이션 코드와 함께 저장

☑ 코드 통합 및 지속적인 배포 (CI & CD)

- 자동화를 통해 배포 가속화
- 클라우드 운영과 DevOps의 통합
- ex) Terraform, Azure ARM template

Azure 도구 및 서비스

리소스 관리자 템플릿

Azure PowerShell

Azure CLI

Azure Policy

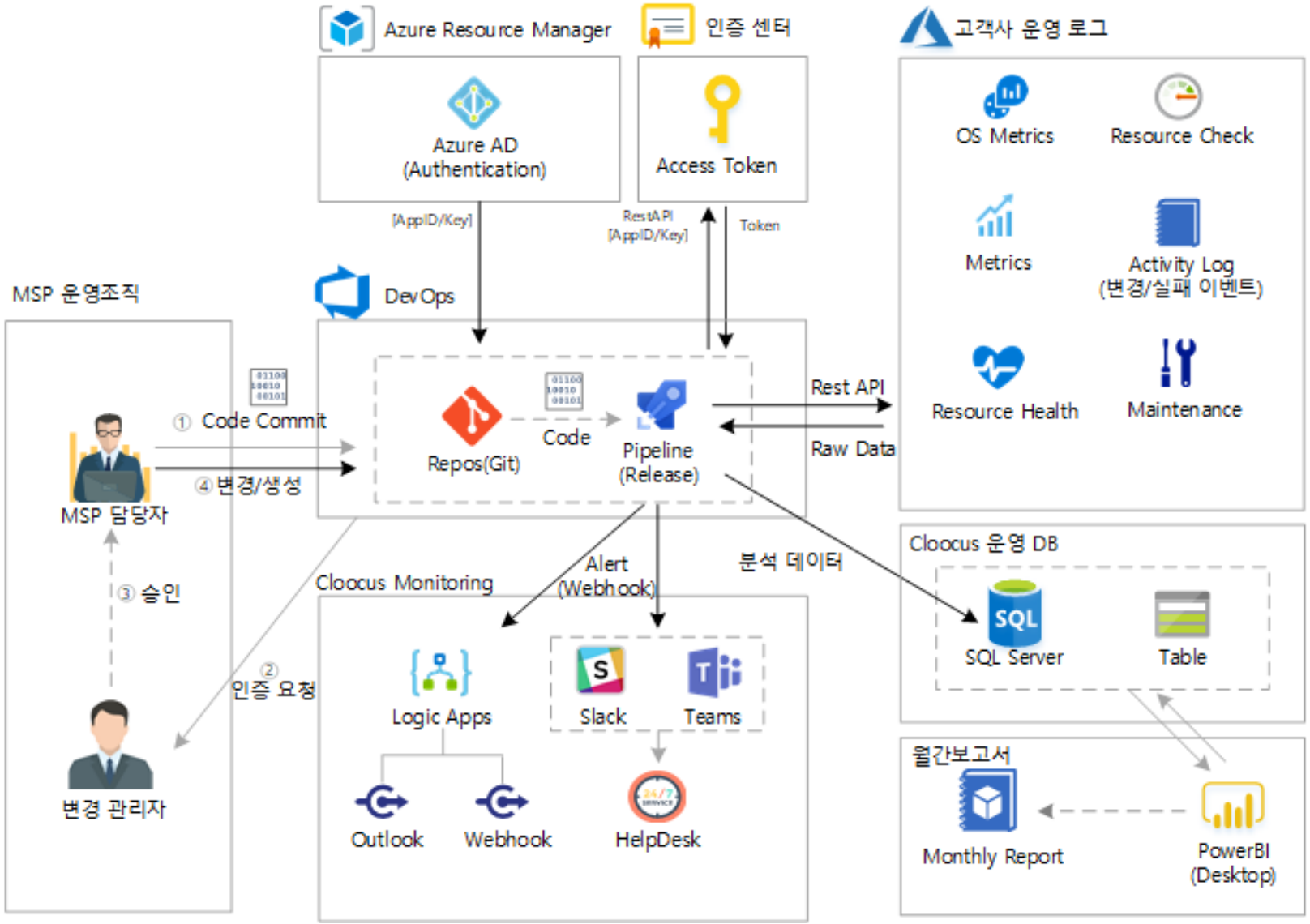
리소스 그룹화 & 태깅

Azure DevOps

GitHub – Azure GitHub Actions

Azure Automation

Azure Devops – 배포가속화



Cloocus

Microsoft

클라우드 네이티브 도구

참고) Azure 는 거버넌스 관리를 위하여 다음과 같은 도구를 제공하고 있습니다.

클라우드 네이티브 도구

비용 관리

Azure Blueprint
Azure Policy
Azure Cost Management
Azure Advisor

보안 기준

Azure Blueprint
Azure Policy
Azure Security Center
Azure Sentinel
위협 보호

Identity 기준

Azure Blueprint
Azure RBAC
Azure AD
Azure AD B2B
Azure AD B2C
디렉터리 페더레이션
디렉터리 복제

리소스 일관성

Azure Blueprint
Azure Policy
Azure Monitor
변경 추적
DSC
업데이트 관리
자동화

배포 가속화

Azure Blueprint
Azure Policy
리소스 태깅
ARM 템플릿
Azure DevOps
Azure Site Recovery
Azure Backup
Azure Automation

클라우드와 IaC

Json

{

Activity Log

Deployment Template

}

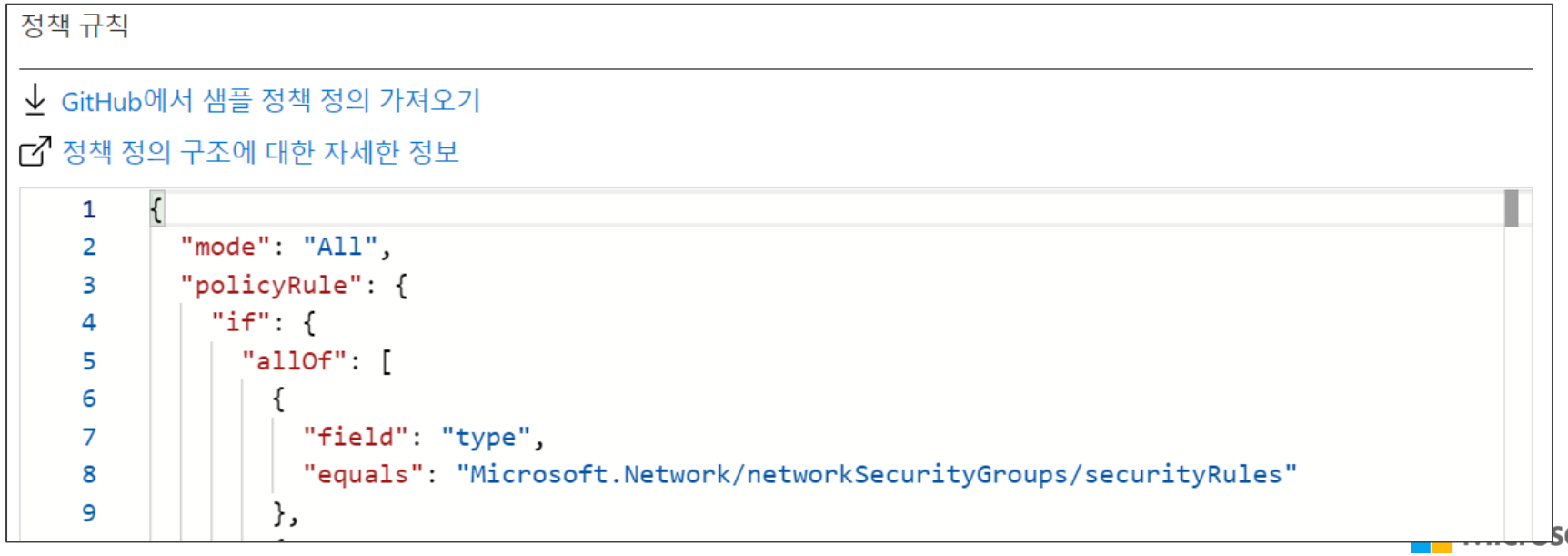
Json

{

Activity Log : Audit

Deployment Log : Deny

}



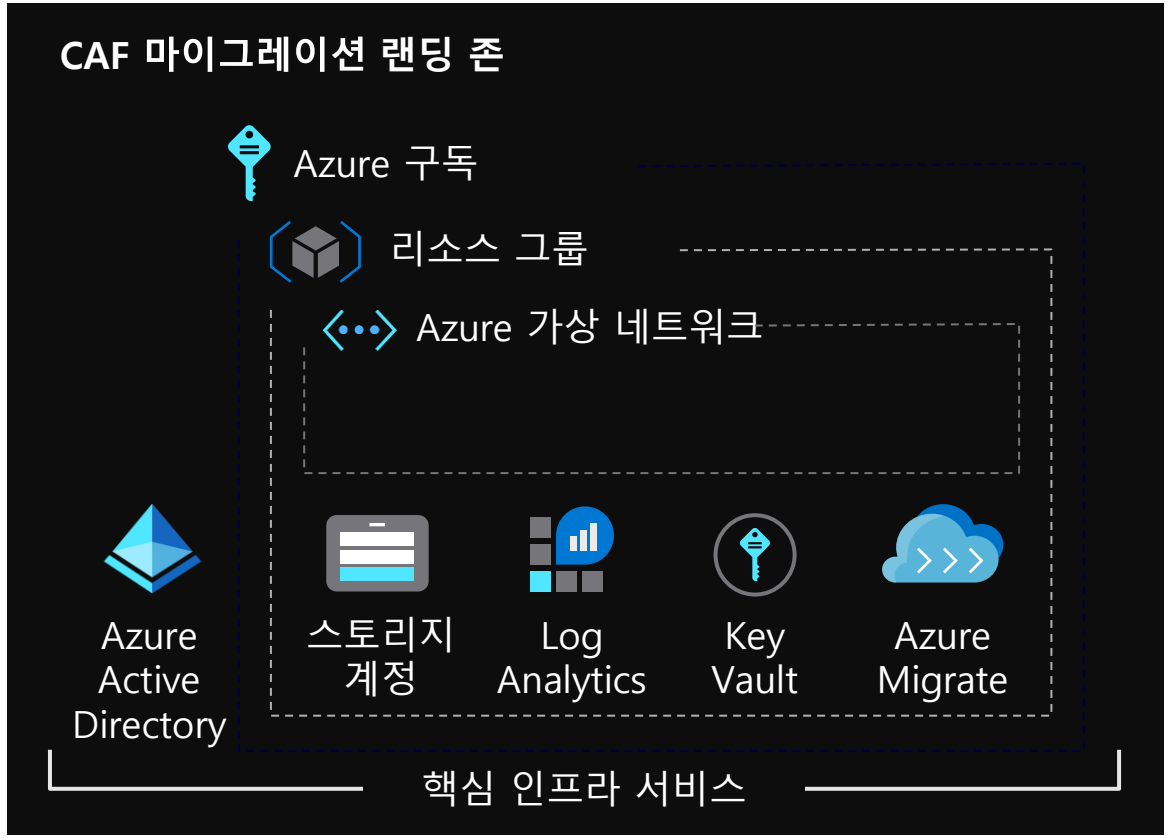
03

Landing Zone 구현

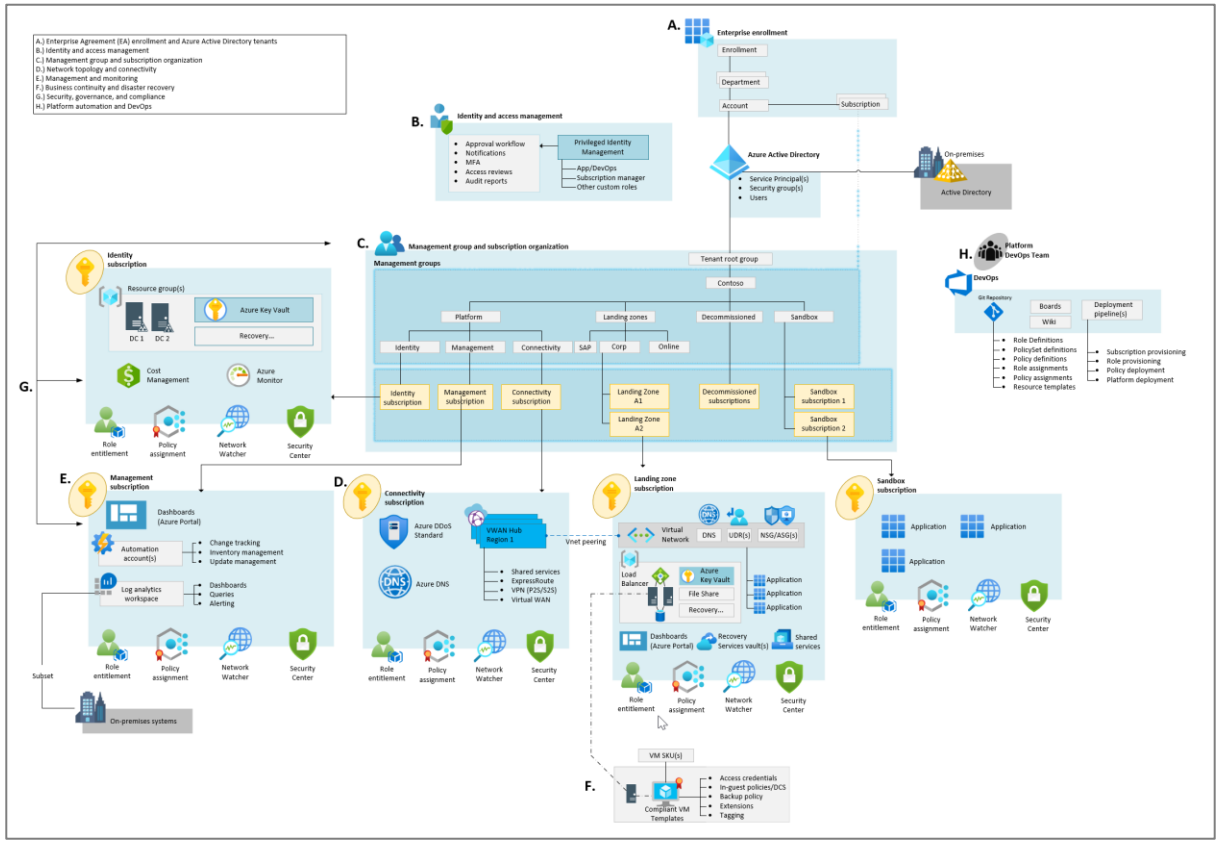
Landing Zone 구현

Landing Zone 접근 방법

- MVP(a minimum viable product)



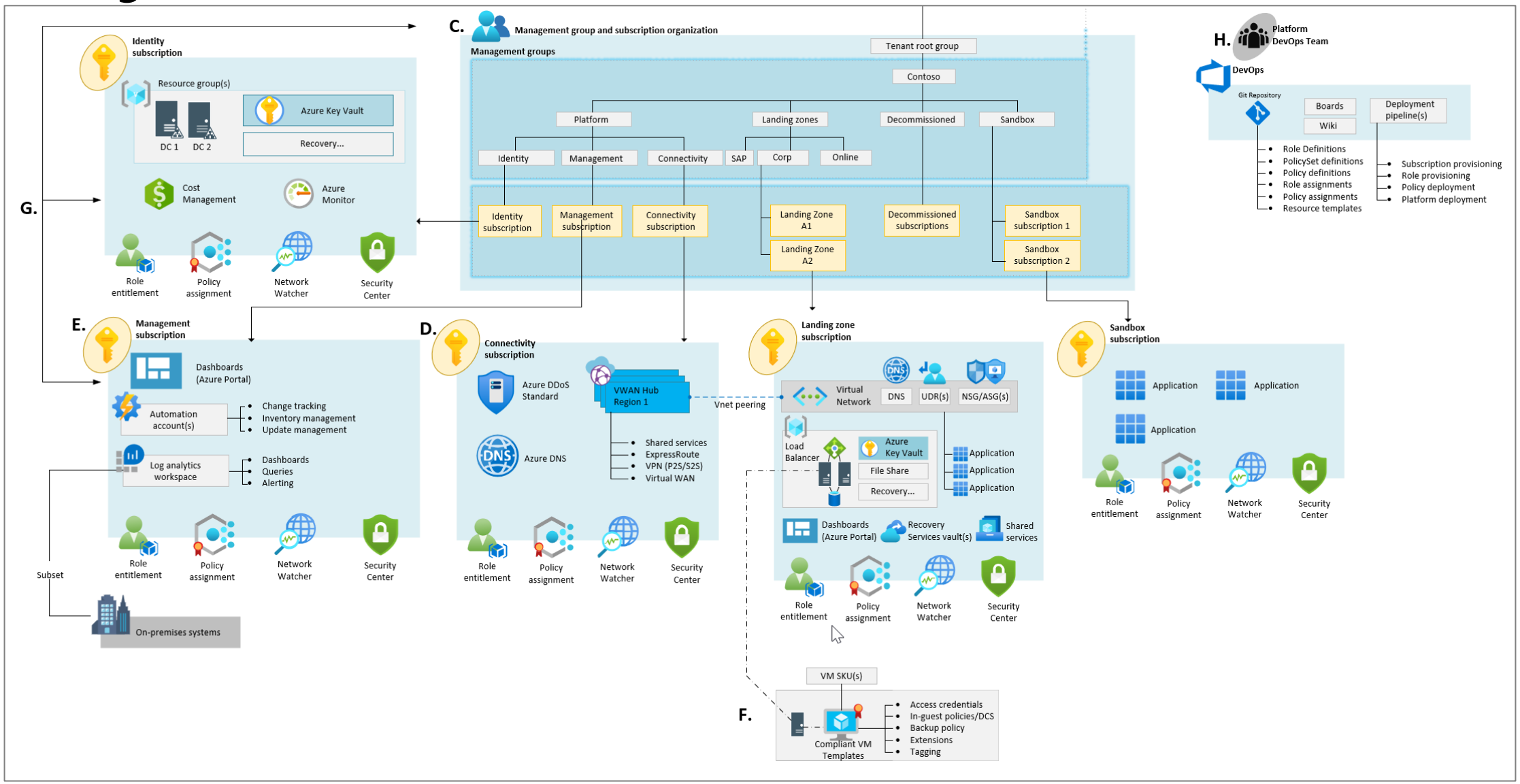
- 엔터프라이즈 규모로 시작



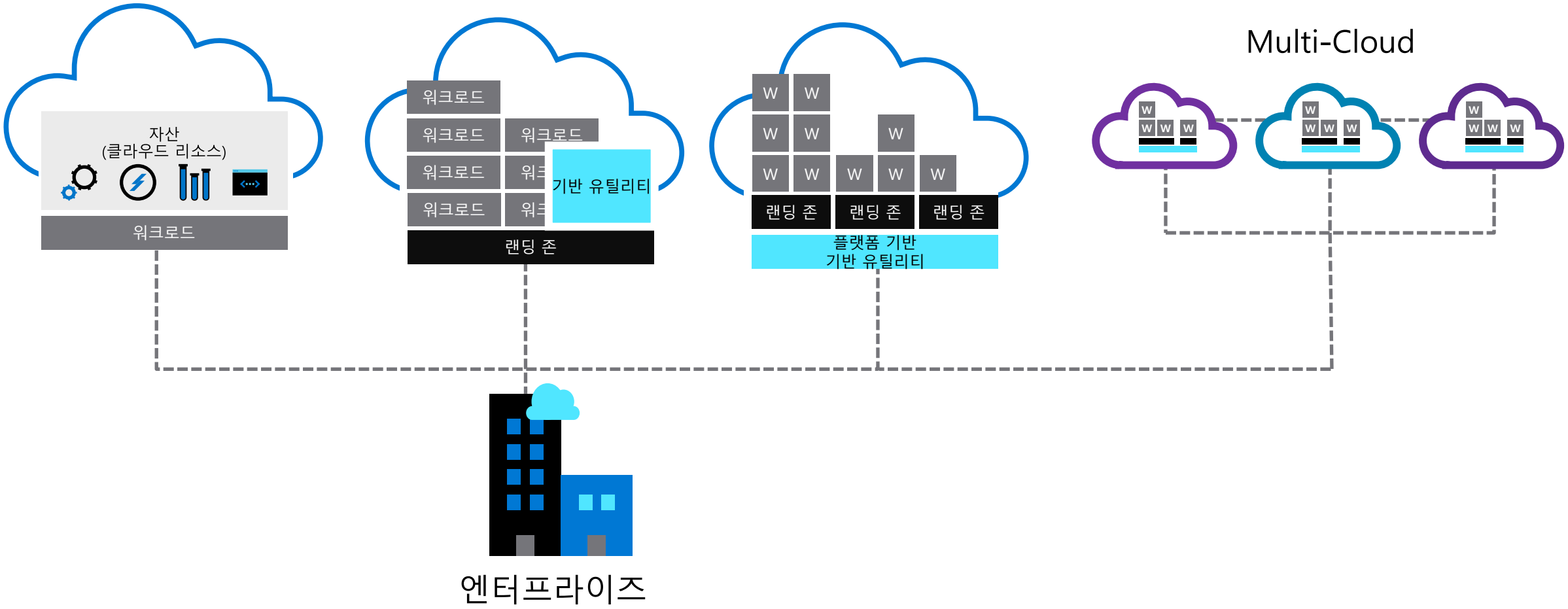
Cloocus

Microsoft

Landing Zone 접근 방법 – 엔터프라이즈 규모



Landing Zone 운영 모델



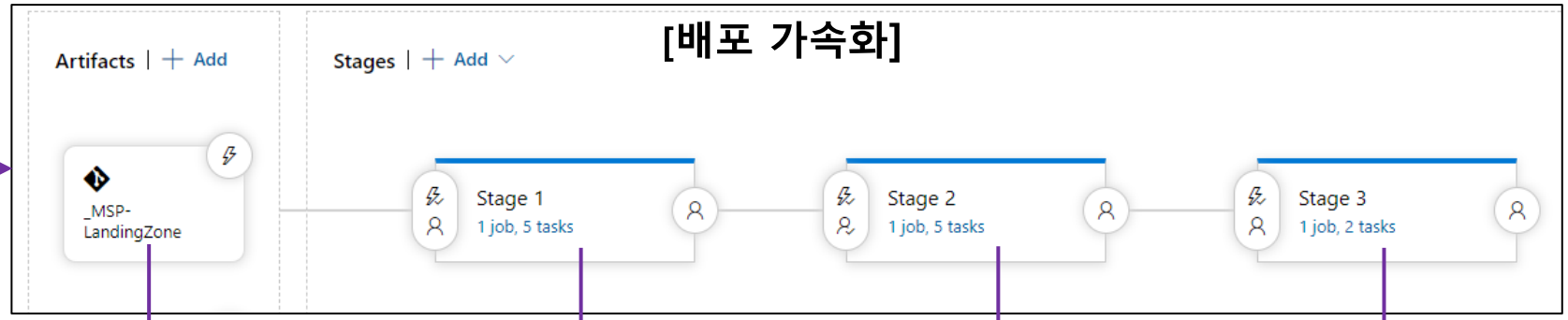
Landing Zone 구현 방법

DevOps를 활용하면 Landing Zone 템플릿을 효율적으로 배포 및 관리할 수 있으며, Terraform 으로 리소스 일관성을 유지할 수 있습니다.

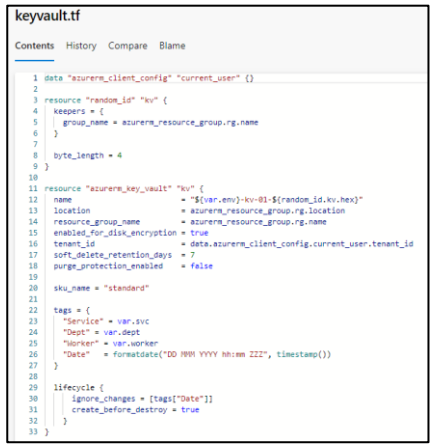
Azure DevOps

[Cloud Adoption Frameworks]

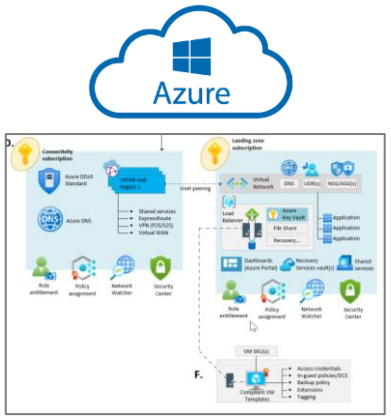
ID	Title
1	Cloud Adoption Strategy
2	Cloud Adoption Plan
3	Cloud Ready
5	Cloud Migration
6	First Workload
7	First Host
8	Workload Template
9	Landing zone creation
10	Define the Cloud Adoption Plan
11	Define Adoption Strategy

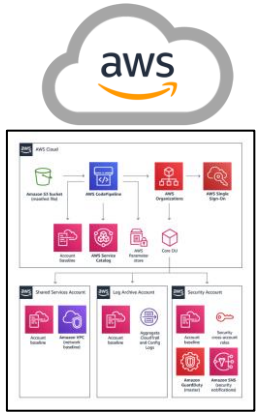


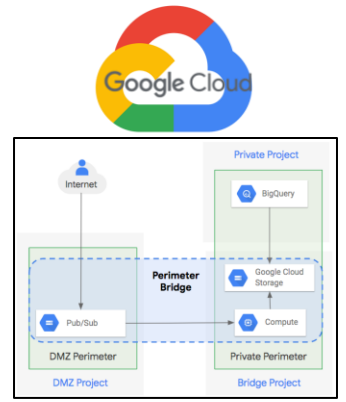
Terraform



[Deployment]







04

CAF 란?
(Cloud Adoption Frameworks)

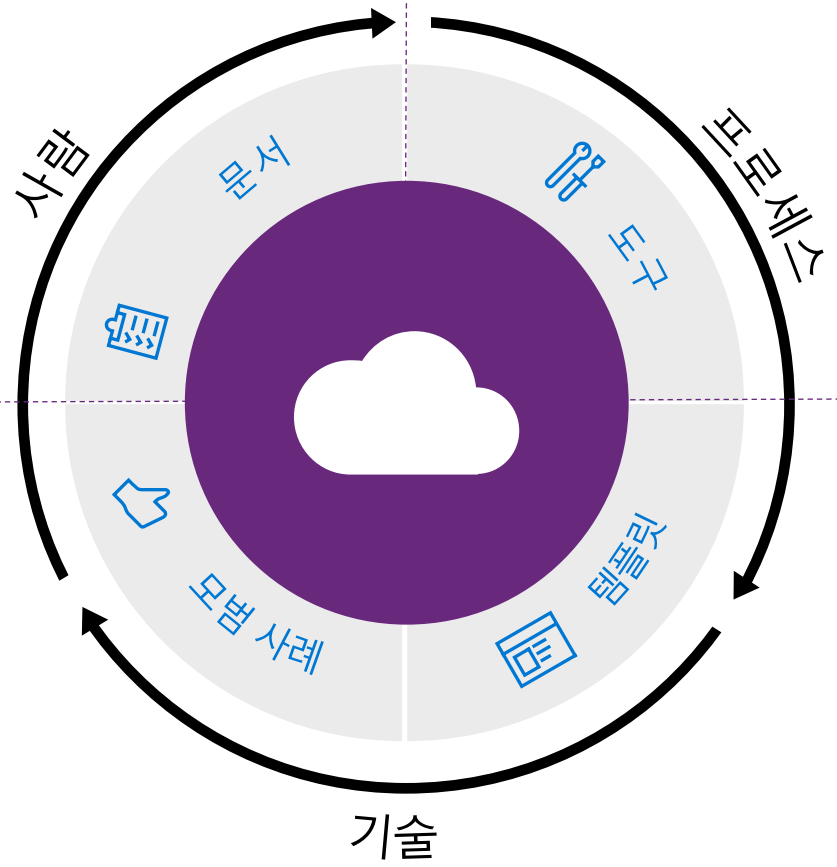
Cloud Adoption Frameworks 개요

CAF란?

고객이 클라우드에서 성공하기 위해 필요한 비즈니스 및 기술 전략을 만들고 구현하는데 도움이 되는 입증된 비즈니스 및 기술 지침입니다.

프로세스 기획/운영

기술 구현



Cloud Journey Tracker

SMART

(Strategic Migration Assessment and Readiness Tool)

Governance Benchmark

Landing Zone

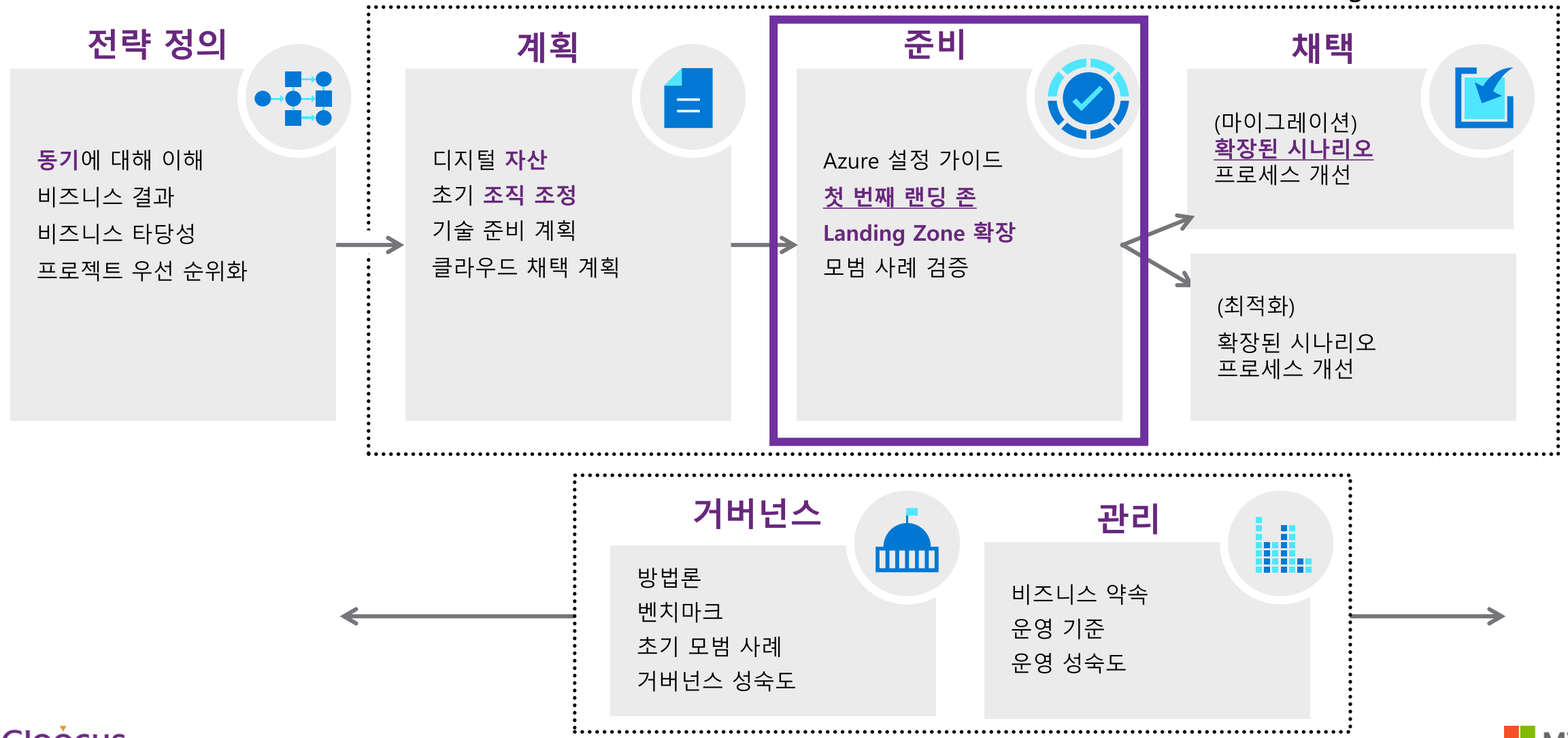
IaC (Terraform, Arm template)

DevOps

Landing Zone 개요

CAF 를 활용한 랜딩존 접근 방안

고객사 비즈니스에 대한 이해를 바탕으로 클라우드 운영 방안을 정의하고 이를 효율적으로 관리하기 Landing Zone을 구성합니다.

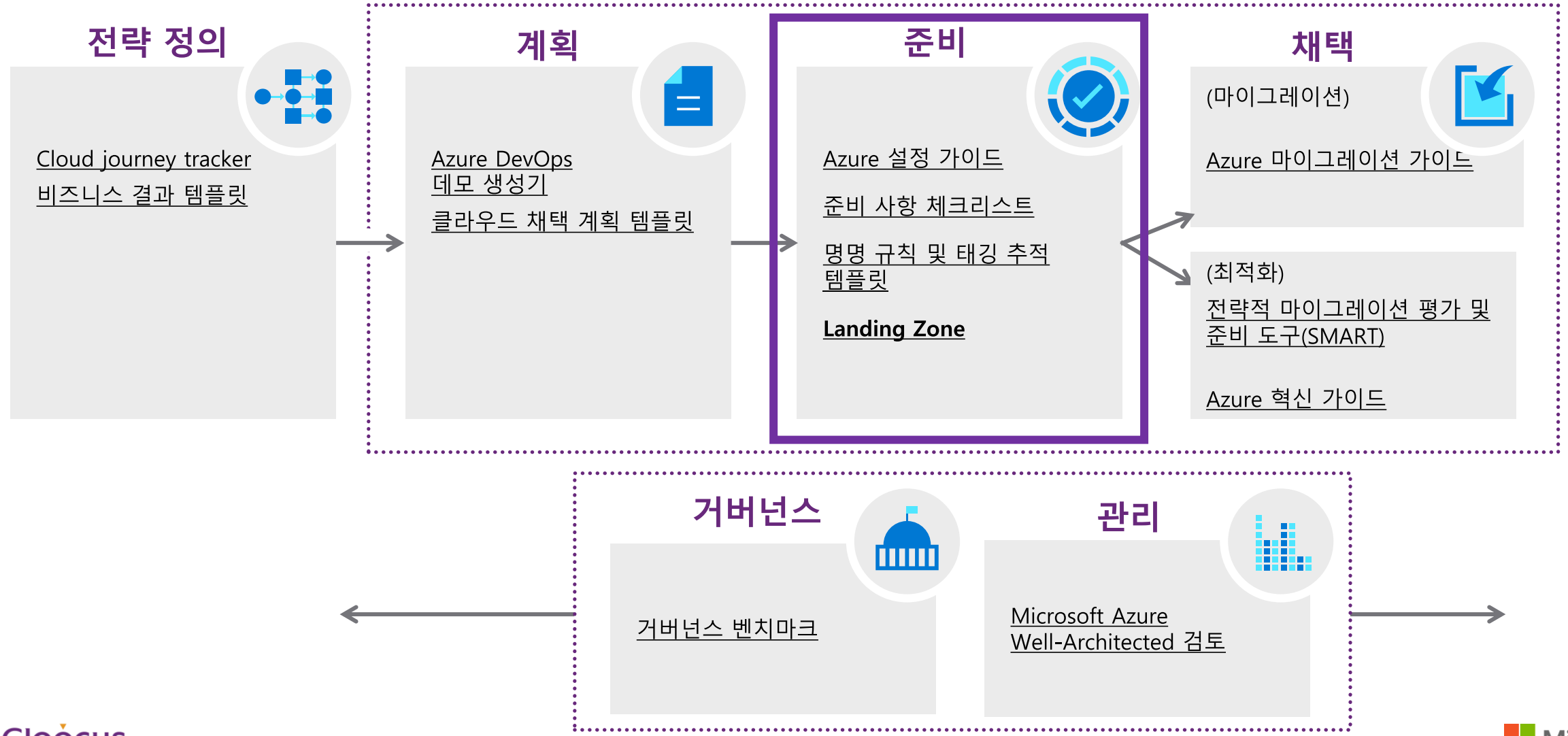


Cloocus

Microsoft

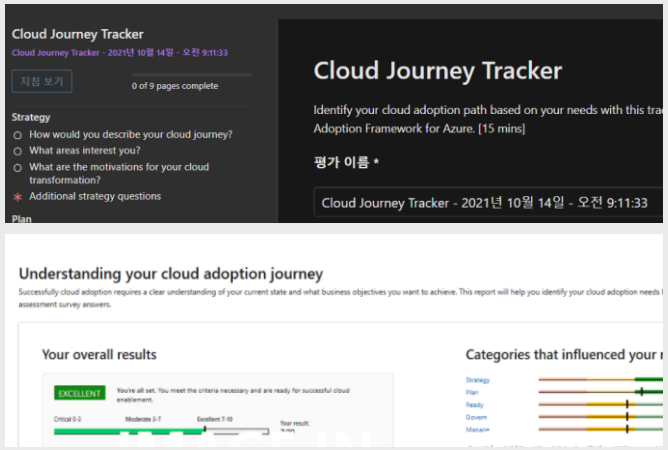
CAF 를 활용한 랜딩존 접근 방안

참고) Azure 는 거버넌스 관리를 위하여 다음과 같은 도구를 제공하고 있습니다.



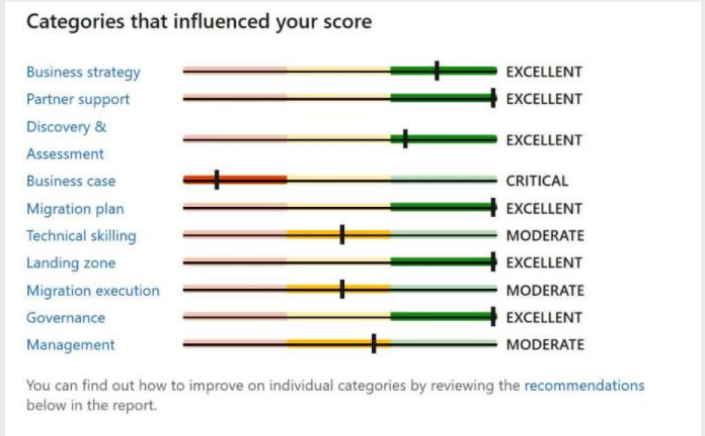
사례) CAF 구현을 위한 도구

참고) Azure는 CAF를 구현을 위하여 단계별로 도구를 제공하며 수집된 데이터는 운영 관리를 최적화 하는데 활용됩니다.



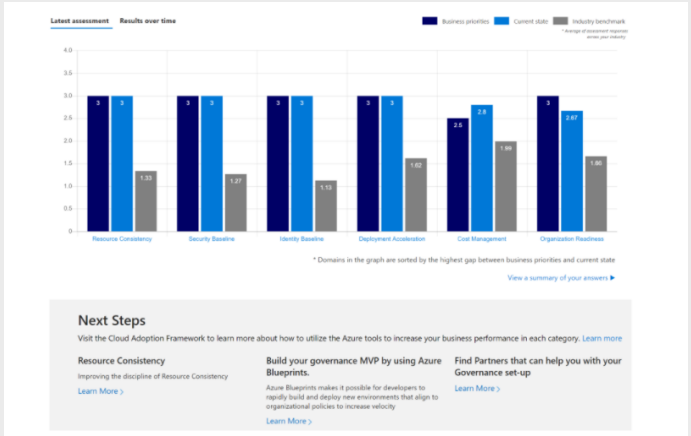
Cloud Journey Tracker

클라우드 채택 요구 사항을
식별하고 고유한 클라우드 여정을
위한 권장 사항을 확인



전략적 마이그레이션 평가 & 준비 도구

대규모 클라우드 마이그레이션을
구현하기 위한 조직의 준비
상태를 이해



거버넌스 벤치마크

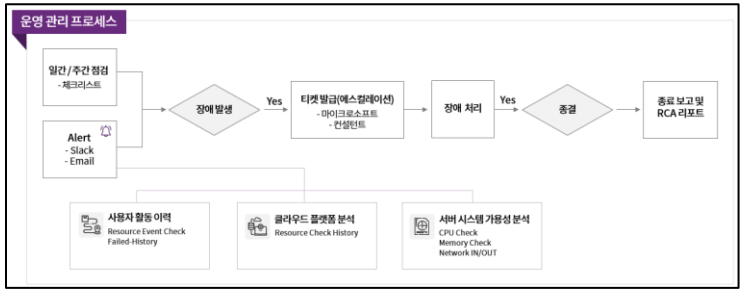
조직의 현재 거버넌스 상태의 차이를
식별하고 시작 방법에 대한 선별된
지침을 확인

Cloud Adoption Frameworks 개요

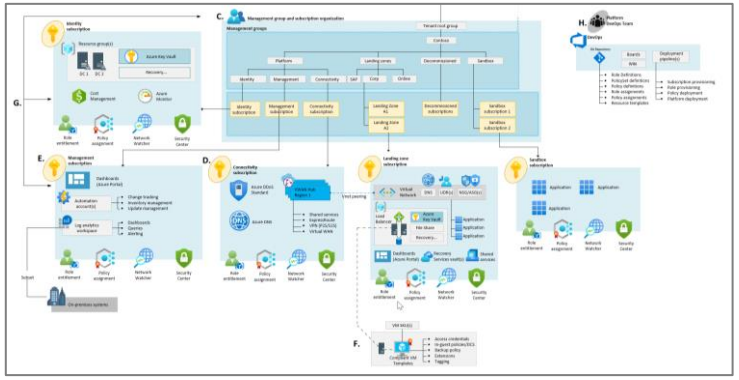
CAF 관리 방안과 Landing Zone

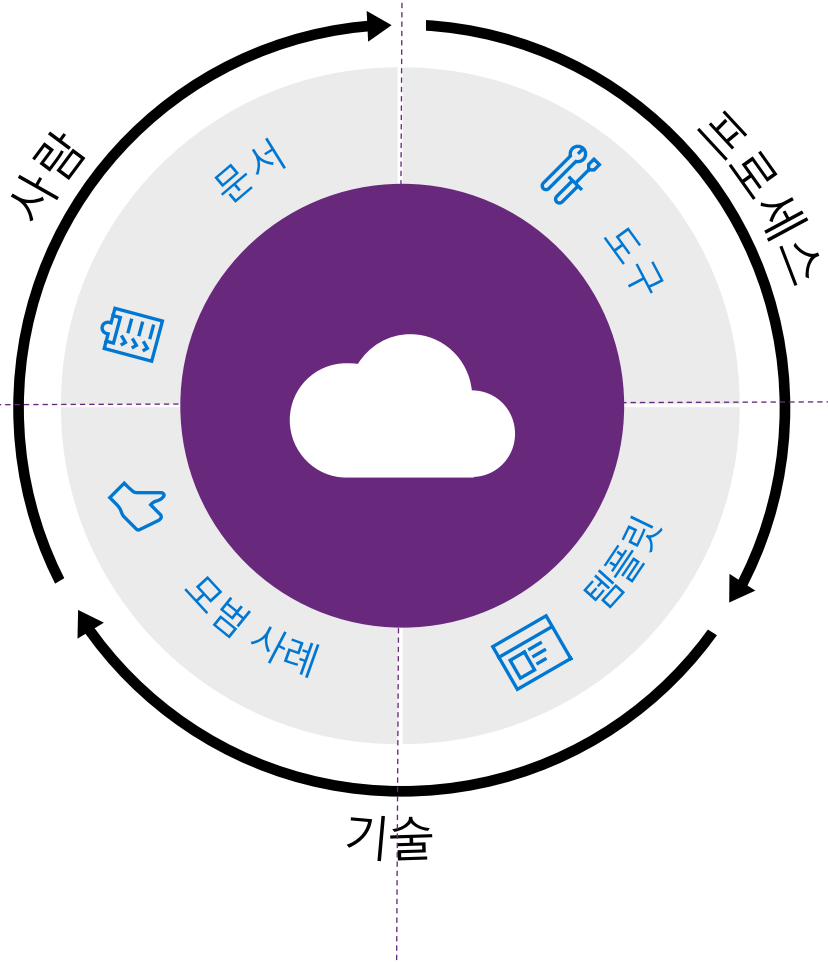
CAF 를 기반으로 지속적인 운영 방안과 절차를 정의하고 이를 시스템으로 구성하여 효율적인 클라우드 관리를 수행합니다.

운영 관리 절차

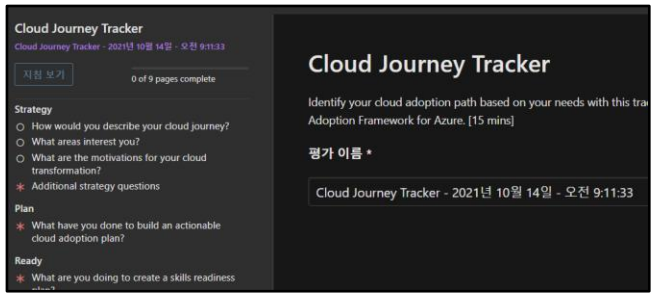


운영 시스템(Landing Zone)

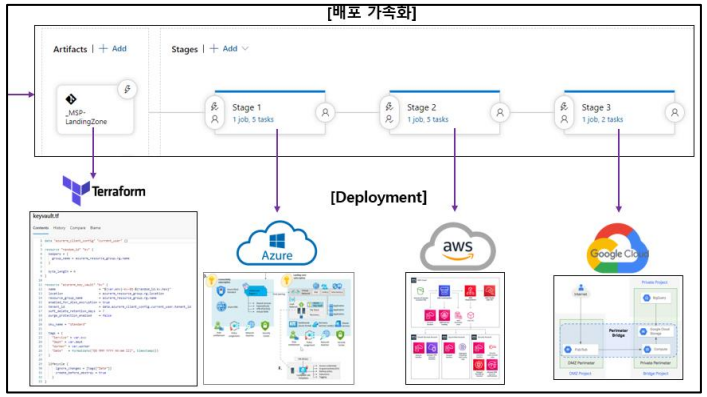




CAF 관리 도구 (지속적인 운영)



DevOps (배포관리)



Cloocus

Microsoft

Thank you

Cloud Navigator, Cloocus

Cloocus Gold Microsoft Partner Azure Expert MSP

Final Update 2021.10.14 I Produced by Cloocus