SK 주식회사 AX

AI Landing Zone in Azure

Security, Governance를 고려해 Azure 환경에서 AI 도입

2026.02

SK 주식회사 AX

Contents

기업의 AI 모델을 빠르고 쉽게 생성하고 관리하기 위한 전사 AI 플랫폼 (AI Landing Zone in Azure)

AI 구성을 위한 빠른 클라우드 구성

- 생성형 AI 모델을 빠르게 배포
  - 기업 환경에서 생성형 AI 모델을 빠르게 배포 및 관리
- Landing Zone 기반 클라우드 서비스
  - Landing Zone 기반으로 Cloud 자원을 빠르게 배포 지원
  - 기업의 보안, Compliance 정책에 반영
- IaC를 활용한 인프라 구성
  - Infra as Code를 활용해 프로그래밍 코드로 인프라 구성/관리

Landing Zone 기반 생성형 AI 모델 배포
IaC를 활용한 프로그래밍 코드로 빠른 구성 가능

주요 AI 서비스를 위한 표준 플랫폼

- 기업 환경에 맞는 다양한 AI 기반 Use Case 적용 가능
  - Gen AI, Agent, RAG, ML workload를 안전하게 구축/운영
  - Responsible AI 내재화
  - Well-Architected Framework 기반 구현
- 오픈소스 LLM 적용 지원
  - 상용 LLM 및 오픈소스 LLM 적용 가능한 환경 제공
  - 기업 특성에 맞는 다양한 오픈소스 LLM 적용 지원
- 주요 AI 서비스 활용 가능한 플랫폼
  - Azure 외 AWS, GCP, NCP에서 제공하는 AI 서비스 활용

주요 AI 서비스를 활용할 수 있는 플랫폼으로
기업 환경에 맞는 다양한 AI 서비스 구현 가능

보안·컴플라이언스 표준을 내재화해, AI 서비스를 빠르고 일관되게 배포·운영할 수 있도록 신규 AI Landing Zone 구축 또는 기존 Azure Landing Zone을 Upgrade 지원

AI를 위한 Landing Zone이 없다면...

Gen. AI 서비스를 개발할 때마다,
수많은 유사한 작업을 진행해야 합니다

- Identity and Auth Control
  . IAM, RBAC, Source, Open AI Studio, Users ...
- Network 구성
  . Private Endpoint? External Access? Reginal Traffic?
- API 관리와 모니터링 구성
  . One for Use Case, Multiple Use Case, 개별 모니터링?
- 기업 Data 보관, 보호
  . Cloud 환경의 Storage 구조? 암호화 적용?
  . 개인정보 보호를 위한 구현?
- API Service, Function의 Fronting/Backing Call 구성
  . APIM 구성은 어떻게 할 것인지, Managed Service?
- 기존 서비스 연결 구성 vs 신규 구독 독립 구성

AI Landing Zone Concept

IAM
(Net/Sec/DevOps...)

Policy
(보안 Baseline : No Public IP, 암호화)

Management & Monitoring
(Metric, Logs and Alerts)

AI Application
AI Application
AI Application

Application Template
- App. Resources (VM, K8S)
- IAM, Policy, Keys
- Monitoring

Shared Service
- SSO, Auth : AD
- Firewall
- Storage, 암호 Key 관리

Networking
- DNS, Endpoint
- In/outbound,
- Corp Connectivity

AI 도입에 필요한 사항을 고려하여 Azure Landing Zone 설계/구현

Checklist 예시

구분	세부 항목	구현 방안
Network 보안	외부망 접근을 제한하고, 내부망에서만 접근하도록 구현이 필요합니까?	A 전용선/VPN 구성
	Gen.AI API 호출 Endpoint를 Private Network로 구성해야 합니까?	B Private Endpoint 생성
Data 보안	데이터 활용 및 저장을 금지해야 합니까?	C Opt-Out 설정
	API 호출을 위한 Key 관리를 해야 합니까?	D Key 관리 서비스 사용
Monitoring/ Logging	Prompt/Completion 값을 모니터링해야 합니까?	E API Management 사용
	호출하는 Client IP 식별을 해야합니까?	
	Gen.AI 리소스 사용량에 대한 모니터링이 필요합니까?	F 비용 관리 기능 활용
Func.	특정 글자를 필터링하는 등 컨텐츠 필터링 기능이 필요합니까?	G 컨텐츠 필터링 기능
	입력 글자를 제한해야하는 요건이 있습니까?	H 특정 라이브러리 활용
Responsible AI	AI 시스템 구축의 평가부터 개발, 배포까지 프레임워크가 필요합니까?	I Responsible AI 방법론
Compliance	입력 데이터가 개인정보 보호법/산업기술보호법 및 저작권법에 해당될 수 있습니까?	J 개인정보 마스킹

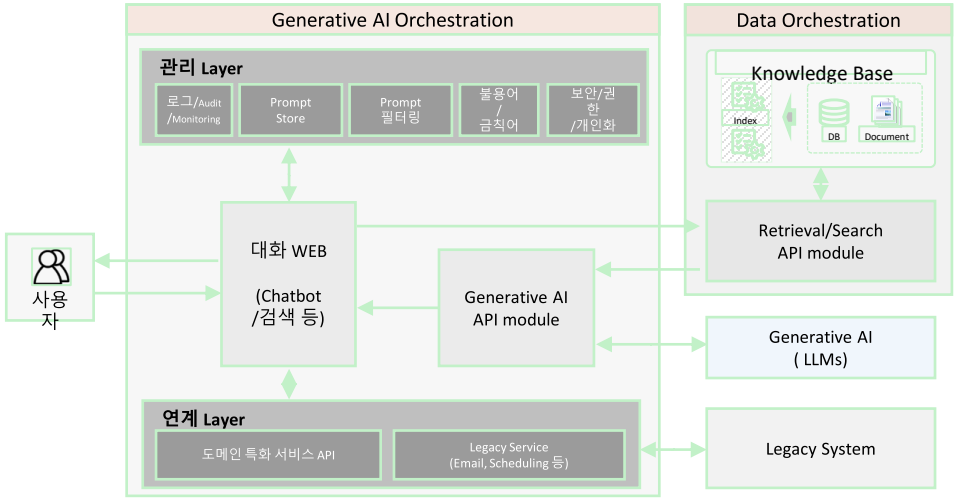
Azure Services

다양한 Azure Native Service 활용

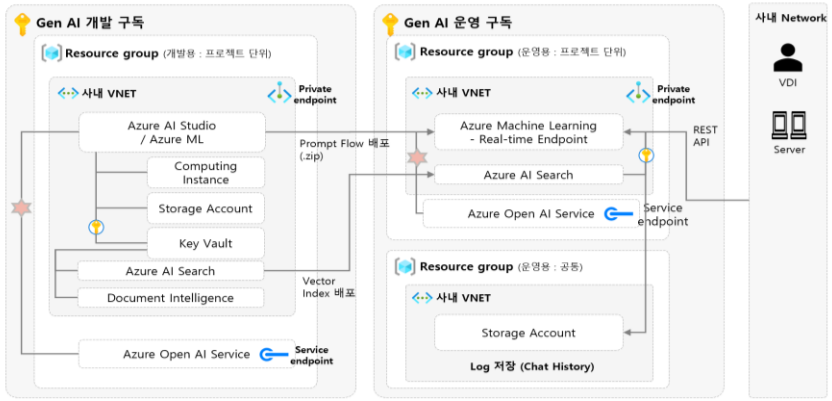
- Azure Policy
- Entra ID
- Key vault
- Azure Firewall
- Cost Management
- Azure Monitoring
- Defender for Cloud (AI Service, DB, VM...)
- Purview
- DDos Protection
- ...

AI 서비스 구현을 위한 사용자, App 통합 관리, Azure AI 개발을 위한 App Arch. 및 Azure Landing Zone에 보안·권한·모니터링이 내재된 개발 플랫폼을 제공

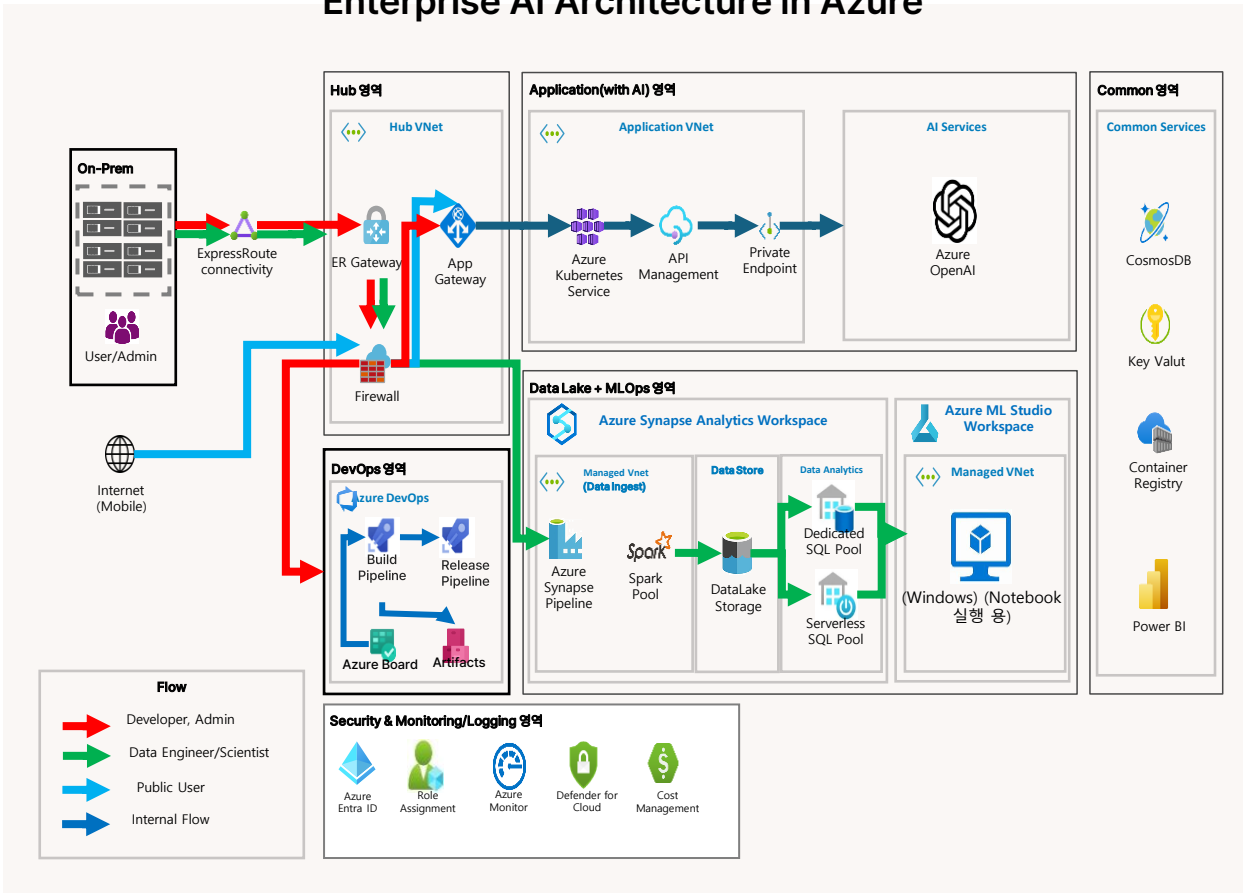
Enterprise AI App *(Chatbot)*. Architecture



Microsoft AI Service 기반 Azure AI Architecture



Enterprise AI Architecture in Azure



전사 차원의 Data 보안, Compliance, Governance를 확보하면서, 분산된 AI 통합, AI 확산을 AI Landing Zone을 통해 빠르게 구현

통합 AI 환경 구축

- Data 보안/Governance
- 생성형 AI 개발 환경
- 계열사로 확산

Landing Zone for AI in Enterprise

	A사 고객 Benefits
분산된 AI/ML 프로젝트 통합	• 즉시 활용할 수 있는 AI/ML과 프롬프트 템플릿을 식별/표준화 • 프로젝트로 인한 시간과 비용 낭비를 최소화 • 데이터 사이언티스트 배치를 효과적으로 관리, 비용을 최적화
AI/ML 프로젝트 모니터링	• 기업 전반에 걸친 AI/ML 프로젝트를 실시간으로 모니터링 • 데이터 사이언티스트 배치를 효과적으로 관리, 비용을 최적화
MLOps/LLMOps를 통한 프로세스 통합	• 데이터 과학자가 인프라 구축 걱정 없이 모델 개발에 집중
전사적인 Gen.AI 프롬프트 개발 환경 배포	• 표준화된 GPT 개발 환경을 구축 • 비데이터 과학자도 빠르게 GPT 솔루션을 개발/배포 가능

Enterprise 요건을 맞춰 Azure CAF, WAF 기반으로 보안/Compliance를 준수, 향후 다양한 Use Case 확장과 운영까지 고려

Discovery & Assessment

~ 2주

✓ 현황 분석
- Landing Zone 유/무
- Data
- LLMs

✓ 요구 사항 파악
- Compliance
- Contents 요구사항
- Security Guideline
- etc

Design

~ 3주

✓ Ref. Architecture Customized
- Azure Landing Zone
- AI Governance
- 표준 Ref. Template

✓ 주요 Policy 설계
- Data
- User
- Access/API

Build & Pilot

~ 4주

✓ 환경 구축
- DevOps
- SecOps
- IaC Template

✓ Workload 검증
- Chatbot
- RAG

Rollout & Scale

~ 지속

✓ 운영체계 연계
- Playbook/Runbook

✓ Use Case On-boarding
- 컨텐츠 생성
- Assistance
- Agent AI
- New Documents
- Knowledge Center/마이닝
- etc

표준·보안 내재 Azure AI Landing Zone으로 자동화·확장·비용 최적화
리스크 최소, 자산 재사용을 통해 비즈니스 가치를 빠르게 실현

자동화 및 유연성

- MIops/LLMops 자동화
- OpenAI, OSS, Agent 등 멀티모델, 멀티 시나리오(Use Case) 수용

표준화 & 보안

- IaC 템플릿과 모듈 설계로 팀별 독립 환경 구축문제를 해소하는 표준화된 AI 플랫폼
- CAF, WAF기반정책, 암호화, ID관리, 컨텐츠 필터링 등 보안 및 거버넌스 내재화

확장성 및 비용 최적화

- PoC/Pilot에서 전사규모 확대로 확장 용이
- 기존 Landing Zone 활용 가능

비즈니스 Value 혁신 집중

- 인프라 준비 시간 최소화
- 비즈니스 Use Case 발굴 집중

AI 도입에 대한 Risk 최소화

- Responsible AI
- 정보자산 보호
- 중앙관리 체계 강화

AI 자산 내재화

- 재사용 가능한 AI 자산 지속 확보
- 프롬프트, 모델, 파이프라인 등
- Chatbot, Agent AI 등

SK 주식회사 AX

THANK YOU