TOKIOTA

Securización Acelerador Open AI

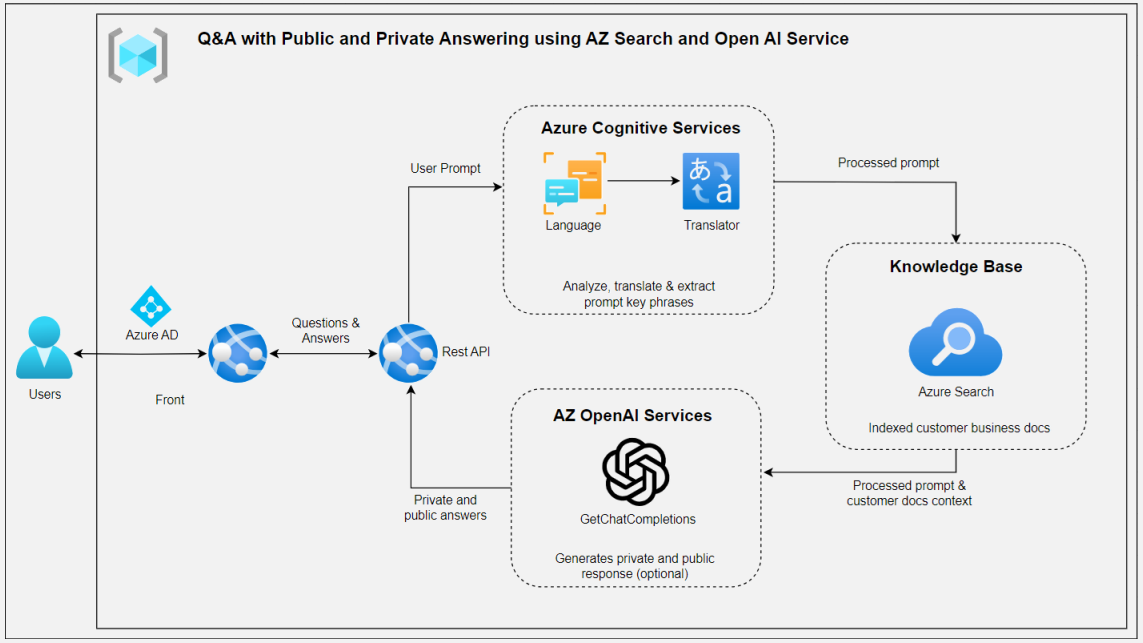
Propuesta de colaboración

Enjoy the journey!

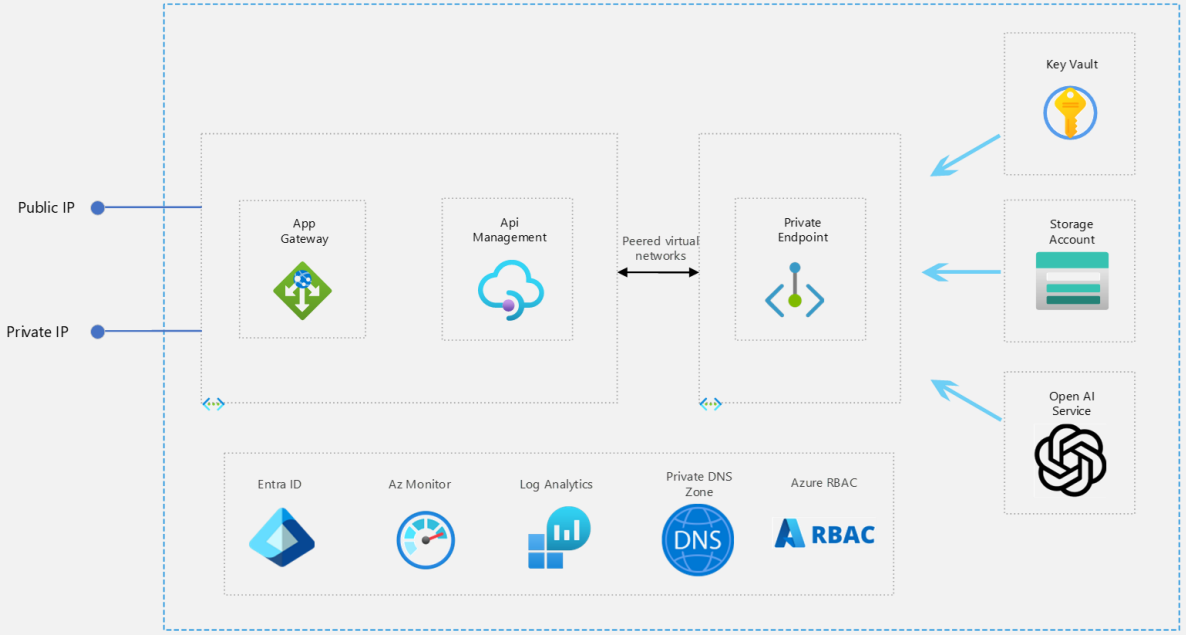
Planteamiento de iniciativa:

Securización infraestructura Acelerador Open AI

Diagrama de flujo



Infraestructura



Securización de la infraestructura del Acelerador de Open AI

1. Conectividad via AppGw con acceso por IP publica y IP Privada
2. Api Management para centralizar la gestión de API's según necesidad
3. Securización con Private Endpoints de los recursos Open AI Service, Storage Accounts y KeyVault
4. Servicios Shared para control de acceso (***RBAC, EntraID***) , monitorización (***Azure monitor***), logs (***Log analytics***) y resolución DNS por zona privada (***PrivateDNS***)

Planteamiento de iniciativa:

Securización plataforma Acelerador Open AI

Securización plataforma OpenAI

1. Eliminar endpoints públicos de los recursos de Azure utilizando private endpoints
2. En las Storage Accounts se activará el infrastructure encryption en el momento de creación
3. Recolección de logs con Log Analytics y análisis con Sentinel (***opcional***)
4. Uso de Keyvault único por despliegue para guardar las credenciales de administración.
5. Hacer uso de Managed identities (***System Assigned***)
6. Configurar el Application Gateway como Load Balancer y WAF

Planteamiento de iniciativa:

Línea Temporal Implementación Securización

Antes

1. Revisión/Configuración del entorno donde se desplegará la solución del Acelerador Open AI
2. Customización del fichero de configuración de Terraform para que incluya los elementos de seguridad y conexiones privadas.

Durante

1. Revisión del estado del despliegue

Después

1. Eliminar endpoints públicos de los recursos de Azure utilizando private endpoints
2. En las Storage Accounts se activará el infrastructure encryption en el momento de creación
3. Recolección de logs con Log Analytics y análisis con Sentinel (***opcional***)
4. Uso de Keyvault único por despliegue para guardar las credenciales de administración.
5. Hacer uso de Managed identities (***System Assigned***)
6. Configurar el Application Gateway como Load Balancer y WAF