Reto Técnico Ingeniero Cloud – GCP

Autor: Axel Giancarlos Moran Murillo

Proveedor de nube: Google Cloud Platform (GCP)

Resumen: Este documento presenta la solución teórica y práctica del reto técnico para Ingeniero Cloud, utilizando los servicios nativos de Google Cloud Platform.

1 Diferencias entre nube pública, privada e híbrida

La nube pública ofrece recursos gestionados por un proveedor externo (como GCP o AWS) y se paga por uso. La nube privada pertenece exclusivamente a una organización, brindando mayor control y seguridad. La nube híbrida combina ambas, permitiendo interoperabilidad entre entornos locales y públicos.

2 Prácticas de seguridad en la nube

- Gestión de identidades y accesos (IAM) bajo el principio de menor privilegio.
- Cifrado de datos en tránsito y en reposo usando KMS.
- Monitoreo activo con Cloud Audit Logs y Security Command Center.

3 Infraestructura como Código (IaC)

IaC permite gestionar la infraestructura como código, garantizando despliegues reproducibles y auditables.
Beneficios: consistencia, versionamiento y automatización.
Herramientas: Terraform (multi-cloud, declarativo) y Ansible (automatización basada en YAML).

4 Métricas esenciales de monitoreo en la nube

- CPU, memoria, disco.
- Latencia y disponibilidad (uptime).
- Errores HTTP 4xx/5xx.
- Costo y consumo de recursos.
- Logs de seguridad.

En GCP se gestionan con Cloud Monitoring y Logging.

5 Docker y sus componentes

Docker es una plataforma de contenedores que facilita la ejecución consistente de aplicaciones.
Componentes: Docker Engine, Dockerfile, Imágenes, Contenedores y Docker Hub.

Caso Práctico: Arquitectura Nativa en GCP

Diseño para una aplicación con frontend web, backend API Microservicios, base de datos y almacenamiento de objetos en Google Cloud Platform.

Componentes:

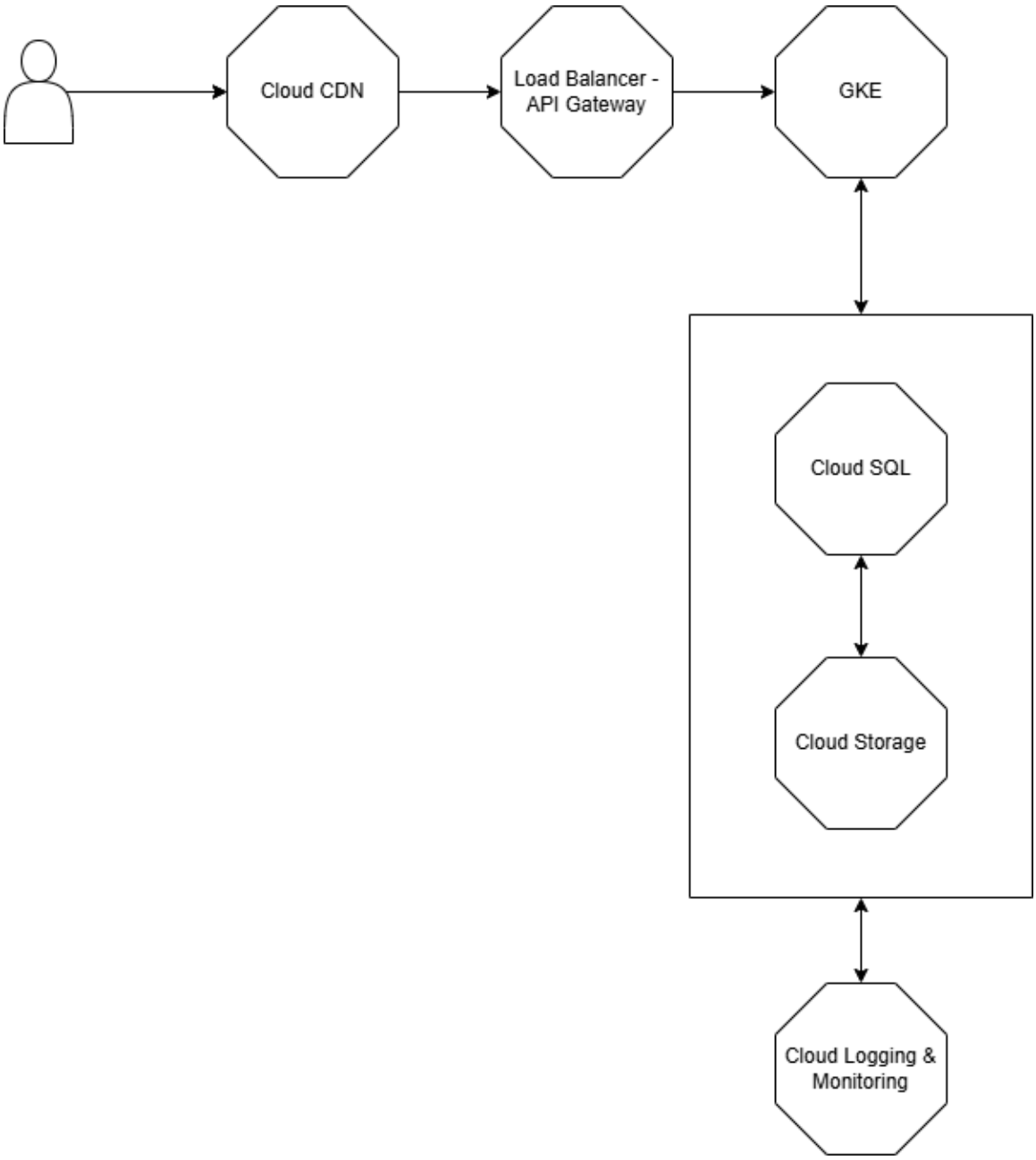
- Frontend: Cloud Storage (sitio estático) + Cloud CDN + HTTPS Load Balancer.
- Backend: GKE con escalado automático a microservicios.
- Base de datos: Cloud SQL (PostgreSQL).
- Almacenamiento: Cloud Storage (objetos e imágenes).
- Monitoreo y seguridad: Cloud Monitoring, Logging, IAM, Secret Manager.

Diagrama de arquitectura (representación textual):

Usuario → Cloud CDN → HTTPS Load Balancer → GKE →Cloud SQL → Cloud Storage → Cloud Logging & Monitoring

Justificación de diseño:

La arquitectura aprovecha los servicios serverless de GCP para minimizar administración y maximizar escalabilidad. GKE maneja la API, Cloud SQL almacena datos críticos, y Cloud Storage junto con Cloud CDN mejoran la entrega global. Toda la solución está monitoreada con Cloud Monitoring y protegida con IAM y VPC Service Controls.


Cloud CDN
Load Balancer - API Gateway
GKE
Cloud SQL
Cloud Storage
Cloud Logging & Monitoring