

Para resolver estos problemas mis pasos fueron:

Acceder a GCP: `gcloud auth login`

Habilitar las API a usar en GCP

Crear la cuenta de servicio: `app-272@azjtp4imscisnfy8crfrxe12x2ln4.iam.gserviceaccount.com`

Crear el bucket en cloud storage para el terraform.state y darle permisos de acceso: `https://storage.cloud.google.com/bucket-terraform-test/terraform-state/default.tfstate`

Crear el cluster K8 en GCP usando terraform: `my-gke-cluster`

Configurar GCP cloud-build con repositorio externo para hacer build del Dockerfile y guardar la imagen en artifacts/GCR- configurar aceptación de cloud build

Seguido de lo anterior se despliega una imagen en el cluster de kubernetes con sus correspondientes replicas, HPA y loadbalancer.

La imagen fue tomada del Dockerfile del repositorio github que clone, pero le hice cambios como agregar un nginx al final para mas seguridad.

Configurar GCP Artifact: `gcr.io/azjtp4imscisnfy8crfrxe12x2ln4`

Configurar implementación carga de trabajo con GKE – para que tome la imagen de docker

Mi usuario no tenía permisos suficientes para crear un repositorio en GCP

Logre implementar el CI sin problemas, pero el CD no lo logre con el usuario que tenía.

Para el CI/CD cree el pipeline que despliega la nueva imagen al cluster de kubernetes con github action pero el plugin no está vigente, por lo tanto lo hice un poco apurado y de otra forma (quizá menos segura pero se puede mejorar cuando uno tiene una cuenta con más permisos a los recursos de GCP) sin embargo funciona. IP publica `http://34.72.59.122/`

En el repo están todos los archivos usados, no hice el de Docker-compose.yaml porque me parece que es un archivo que sobra, no veo necesidad si vamos a usar kubernetes.

Pregunta IAM:

Si MediaMarkt quiere almacenar información sensible en Google Cloud Platform (GCP) y utiliza el principio de mínimo privilegio en la asignación de roles. Supongamos que estoy a cargo de asignar roles en GCP como administrador de la organización. Mi tarea es decidir qué rol sería apropiado para cada grupo de personas: el equipo de DevOps para crear clústeres en Kubernetes y el equipo de

Finanzas para gestionar la facturación en GCP. Puntualizo qué roles deben aplicarse y los pasos que se aplicaron en la consola IAM de GCP.

Respuesta:

Para el equipo de DevOps que crea clústeres en Kubernetes, se puede asignar el rol "Kubernetes Engine Admin" (roles/container.admin). Este rol les permitirá crear, gestionar y eliminar clústeres y nodos en Kubernetes.

Para el equipo de Finanzas encargado de gestionar la facturación en GCP, se puede asignar el rol "Billing Account Administrator" (roles/billing.admin). Este rol les permitirá administrar y configurar las cuentas de facturación y asociar proyectos a cuentas de facturación.

Pasos en la consola IAM de GCP:

Iniciar sesión en la consola de GCP (<https://console.cloud.google.com/>).

Navegar hasta "IAM y administración" y luego hacer clic en "IAM".

Hacer clic en "Añadir" para asignar un nuevo rol a un miembro.

Ingresar el correo electrónico del miembro y seleccionar el rol adecuado para cada equipo (Kubernetes Engine Admin para DevOps, Billing Account Administrator para Finanzas).

Hacer clic en "Guardar" para confirmar la asignación del rol.