API de Gerenciamento de Workloads - Plataforma de Dados

Políticas IAM GCP

1. Introdução

Este documento traz exemplos de políticas IAM no GCP que suportam as políticas definidas no projeto.

1. Políticas IAM

Controle de Acesso Baseado em Funções (RBAC)

Permite conceder permissões a usuários por meio de funções, ou seja, não concedemos permissões diretamente para os usuários. Dentre os exemplos que suportam a política adotada, temos:

1. Princípio do Privilégio Mínimo: o IAM permite conceder privilégios em granularidades bem pequenas, como, por exemplo, conceder apenas permissão para a leitura de uma tabela em um dataset do BigQuery.
2. Funções Customizadas: com o IAM é possível criar funções específicas para determinadas tarefas por meio da combinação de diferentes permissões. Por conta da granularidade, é possível dar permissão apenas para o que se precisa.

Controle de Acesso Baseado em Recursos

1. Hierarquia de Recursos: por conta da hierarquia de projetos, pastas e organização do Google Cloud, é possível aplicar permissionamento específico para todo um departamento dentro da Cloud, por exemplo, forçando a política a todos os usuários relacionados.

Auditoria e Compliance

1. Registros de Auditoria: é possível habilitar *logging* na cloud, permitindo registrar e analisar quem estava fazendo o que e em que horário;
2. Relatórios para Análise: é possível utilizar recursos como o Cloud Security Command Center para gerar relatórios dos acessos e verificar conformidade.

Política de Acesso Condicional

Além de permitir acessos granulares e baseado em funções, é possível adicionar condições para a concessão.

1. Funções com Condições: ao atribuir uma permissão em uma função, é possível restringir IPs, horários e tipos de recursos.
2. Contas de Serviço: ao atribuir funções a uma aplicação, como uma API, é possível criar contas de serviços que possuem apenas os privilégios necessários.