# Google Cloud IAM, Policies, and Service Accounts: A Quick Guide

## Introduction

Google Cloud Identity and Access Management (IAM) is a central component for managing access to resources on the Google Cloud platform. This document provides a concise overview of essential concepts, commands, and best practices related to IAM, policies, and service accounts.

## IAM Basics

- Principle of Least Privilege: Assign the minimum necessary permissions for users or service accounts.
- Policy Architecture: IAM policies define relationships between members, roles, and resources.
- Roles: Primitive, predefined, and custom roles bundle permissions for access control.
- Conditions: Add an extra layer of security with conditions based on time, IP address, etc.

## IAM Commands

- `gcloud projects get-iam-policy`: Retrieve IAM policy for a Google Cloud project.
- `gcloud resource-manager folders get-iam-policy`: Similar to project command but for folders.
- `gcloud organization get-iam-policy`: Retrieve IAM policy for a Google Cloud organization.
- Policy Inheritance: Policies are inherited down the resource hierarchy.
- Policy Versions and Limitations: IAM policies have versions and certain limitations.
- Time-Based and Resource-Based Conditions: Granular control with conditions.

## Cloud IAM Best Practices

Principle of Least Privilege: Grant minimum necessary permissions.
Regular Review and Audit: Periodically review and adjust IAM policies.
Use Predefined Roles: Minimize custom roles; leverage Google Cloud's predefined roles.
Implement Conditions: Enhance security by adding conditions to IAM policies.
Service Account Key Rotation: Regularly update service account keys for security.

## Service Accounts

- Service Account Types: User-managed and Google-managed service accounts.
- Creating Service Accounts with Permissions: Use `gcloud` commands to create and grant permissions.

```
gcloud iam service-accounts create <service-account-name> --description="<description>"
--display-name="<display-name>"

gcloud projects add-iam-policy-binding <project-id>
--member="serviceAccount:<service-account-email>" --role="<role>"
```

## Conclusion

Understanding and effectively managing Google Cloud IAM, policies, and service accounts are essential for maintaining a secure cloud environment. Regularly applying best practices, reviewing policies, and using IAM commands will contribute to a robust security posture and efficient resource management on the Google Cloud platform.

Check out the detailed blog:-https://medium.com/@srivastavayushmaan1347/google-cloud-iam-policies-and-service-accounts-4acf099c8983