Google Cloud IAM Use Case

Use Case: Enhancing Security and Access Control with Google Cloud IAM

GENERAL CHARACTERISTICS

Intent	To enhance security and manage access control across Google Cloud resources using Google Cloud IAM.
Scope	Implementation of Identity and Access Management (IAM) to enforce least privilege access policies.
Level	System-level.
Client	Confidential (Technology Company).
Last Update	03/12/2024
Status	Finalized.
Stage	Implementation and Monitoring.

ACTORS

Primary Actor	Cloud Security Engineer.
Secondary Actors	IT Operations Team, Compliance Officers, Developers.

PREREQUISITES

Static Preconditions	- Google Cloud Project set up with Cloud IAM API enabled. - Roles and permissions matrix defined based on organizational requirements.
Dynamic Preconditions	- Cloud resources identified and grouped for access management. - Policies reviewed and validated for compliance with security standards.
Assumptions	- Client requires granular access control to manage user roles effectively. - Security compliance with standards such as SOC 2, ISO 27001, or HIPAA is mandatory.

TRIGGERS

Trigger Event	The client required a secure and scalable solution to manage user access across multiple Google Cloud projects.

EXPECTED OUTCOME

Success Postcondition	- Access is securely managed with granular IAM policies. - Compliance requirements are met with

Google Cloud IAM Use Case

	detailed audit logs.
Failed Postcondition	- Unauthorized access or privilege escalation compromises data security.

OPERATIONS AND CONCEPTS

Operations	1. Defined a roles and permissions matrix to align with least privilege principles. 2. Assigned predefined roles such as Viewer, Editor, and Owner to users based on their responsibilities. 3. Created custom roles for specific use cases requiring granular permissions. 4. Set up IAM policies to enforce organization-wide access controls. 5. Enabled audit logging to monitor access and ensure compliance. 6. Periodically reviewed and updated IAM policies to reflect organizational changes.
Concepts	- IAM Policies: Manage access control by assigning roles to users or service accounts. - Audit Logs: Track and monitor access to cloud resources for compliance. - Least Privilege Principle: Restrict user access to only the resources required for their role.

MAIN SUCCESS SCENARIO

Step 1	Analyzed the client's access control requirements across their cloud environment.
Step 2	Created a roles and permissions matrix to enforce least privilege principles.
Step 3	Assigned predefined roles to users and service accounts.
Step 4	Developed custom roles for specific use cases requiring fine-grained permissions.
Step 5	Enabled audit logging to track access and detect unauthorized activities.
Step 6	Reviewed and optimized IAM policies to align with organizational changes and compliance standards.
Step 7	Monitored IAM activity regularly to ensure ongoing security and compliance.