빅쿼리를 활용한 빅데이터 분석 (6)

서진호

제 6 강 목표

1. 클라우드 IAM
2. IAM 정책과 정책 구조
3. 클라우드 IAM 역할

Cloud IAM

- 구글 클라우드 서비스의 ID 와 접근을 할 수 있도록 제공해주는 서비스
- 누가, 언제, 어떤 리소스에 접근하여 이용하는 지에 대한 제어
- 클라우드 리소스를 중앙에서 쉽게 관리
- 복잡한 조직 구조와 많은 작업 그룹과 프로젝트를 지닌 기업에서도 조직 전체에 적용되는 통합 보기를 제공
- 정책을 만들면 사용자 ID 별로 역할을 줄 수 있음.
- GCP 내의 리소스 별로 개별 설정할 수 있음.

Cloud IAM 에서 사용하는 ID

구글 계정

서비스 계정

G Suite 계정

구글 그룹

액세스 관리과 역할

역할(Role) – compute.instanceAdmin

권한(Permissions)

- compute.instances.get
- compute.instances.stop
- compute.instances.list
- compute.instances.start

IAM 정책(IAM Policy)

정책(Policy)

Bindings (리소스별 역할을 가진 멤버 정의)

역할(Role): 컴퓨트 엔진 인스턴스 관리자

멤버 목록(Members)

j@gmail.com

J 구글 그룹 멤버들
J 서비스 계정에 속한 구성원들

역할(Role): Cloud Storage 관리자

멤버 목록(Members)

j@gmail.com

역할(Role): BigQuery 관리자

멤버 목록(Members)

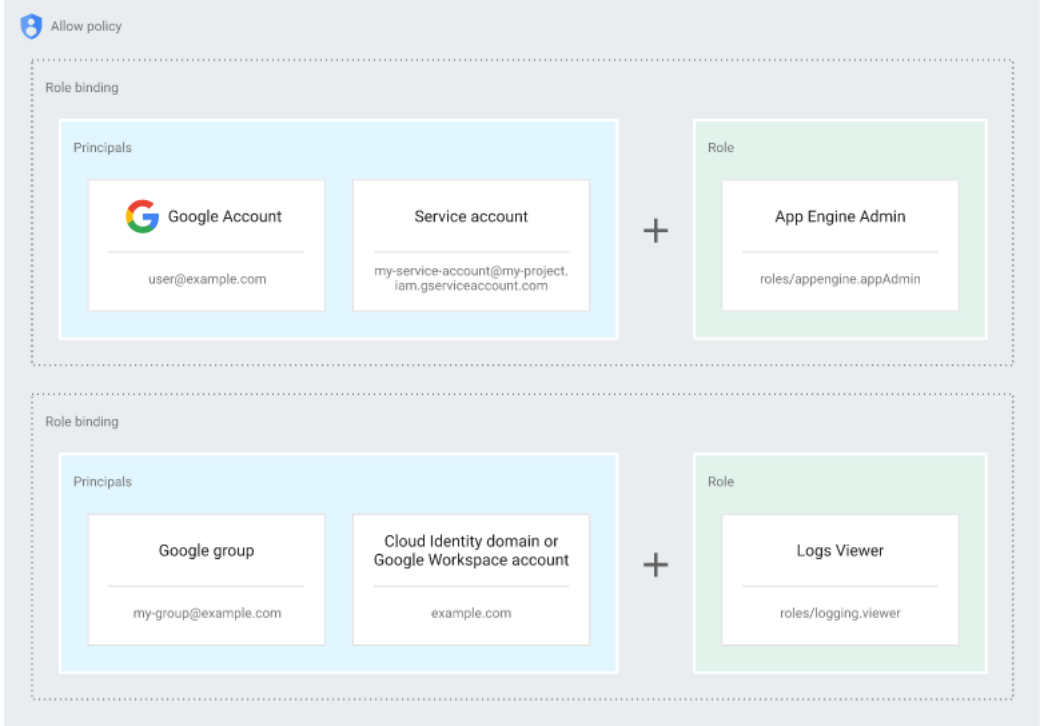
j@gmail.com

데이터 관리 부서 구성원

IAM 정책(IAM Policy) 객체

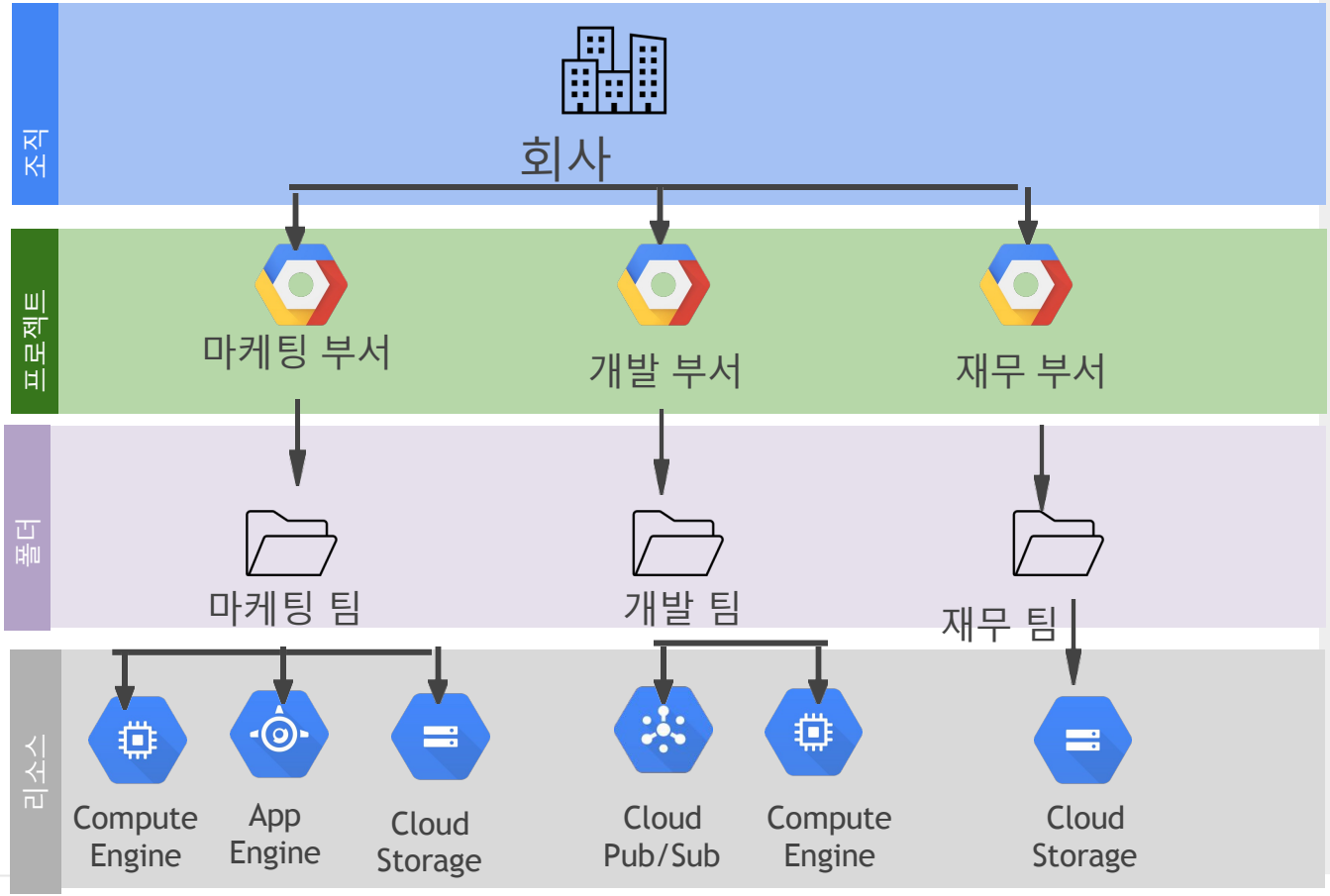
```
{
    "bindings": [
    {
        "role": "roles/storage.objectAdmin",
        "members": [
            "user:synabreu@gmail.com",
            "serviceccount:synabreu-service@appspot.gserviceaccount.com",
            "group:admins@example.com",
            "domain:gmail.com"
        ]
    },
    {
        "role": "roles/storage.objectives",
        "members": ["user:jinho.seo@example.com"]
    }
  ]
{
```

IAM 정책(IAM Policy) 예시



참고: https://cloud.google.com/iam/docs/overview

정책 계층 구조


조직
회사
프로젝트
마케팅 부서
개발 부서
재무 부서
폴더
마케팅 팀
개발 팀
재무 팀
리소스
Compute Engine
App Engine
Cloud Storage
Cloud Pub/Sub
Compute Engine
Cloud Storage

클라우드 IAM 역할 - 기본 역할

소유자
(Owner)

편집자
(Editor)

뷰어(Viewer)

역할 이름	역할 칭호	권한
Roles/owner	소유자	프로젝트 및 프로젝트 내의 모든 리소스에 대한 역할 및 관리 프로젝트에 대한 결제 설정
Roles/editor	편집자	뷰어 권한에 리소스 변경과 같이 상태 변경 작업까지 포함
Roles/Viewer	뷰어	읽기 전용 작업에 대한 권한이 부여함. 기존 리소스 또는 데이터 조회

클라우드 IAM 역할 - 사전 정의된 역할

- 기본 역할보다 더욱 더 세부적인 액세스 제어를 부여하는 역할로 구글에서 만들고 유지와 관리
- 해당 역할의 권한은 GCP에 새로운 기능이나 서비스가 추가될 때와 같이 필요한 경우 자동으로 업데이트

클라우드 IAM 역할 - 커스텀 역할

- 커스텀 역할은 사전 정의된 역할 이상의 세부적인 관리가 필요할 때
- 사용자가 직접 정의하며 하나 이상의 역할을 결합
- 커스텀 역할을 만들기 위해서는 ‘iam.roles.create' 권한이 필요하기 때문에 소유자가 아난 사용자에게는 ‘조직 역할 관리자 역할(roles/iam. organizationRoleAdmin) 또는 ' IAM 역할관리자' 역할(roles/iam.roleAdmin)이 할당

서비스 계정

- 서비스 계정은 서비스의 ID가 되며, 서비스가 액세스할 수 있는 리소스를 제어
- 사용자가 아닌 애플리케이션 또는 가상 머신에 속한 계정
- 애플리케이션은 사용자 계정이 아닌 서비스 계정을 이용하여 GCP API에 접근

- 서비스 계정의 주요 특징
  - ID 사용
  - 리소스 사용

서비스 계정 키

참고 사항 - 리소스

- Cloud IAM
  https://cloud.google.com/iam/docs/overview

- Cloud IAM - Predefined Roles
  https://doud.google.com/ianvdocs/understancling-roles?hl-ko#predefined_roles