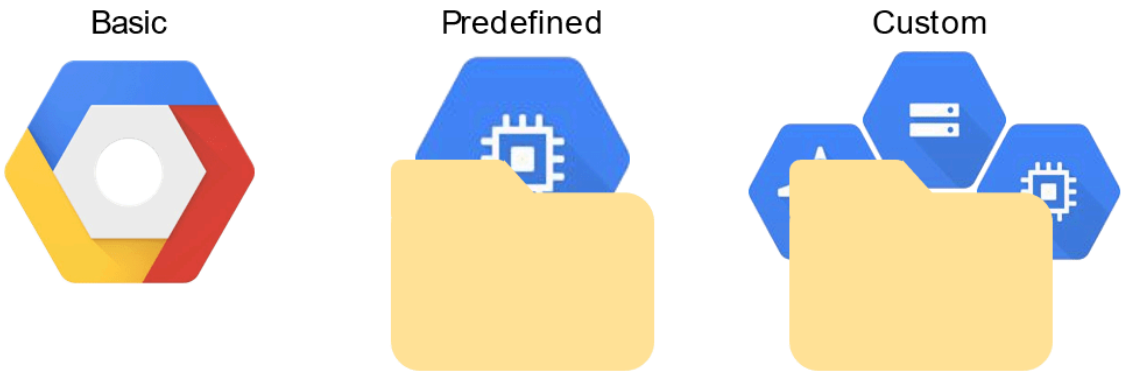
IAM

Identity and Access Management

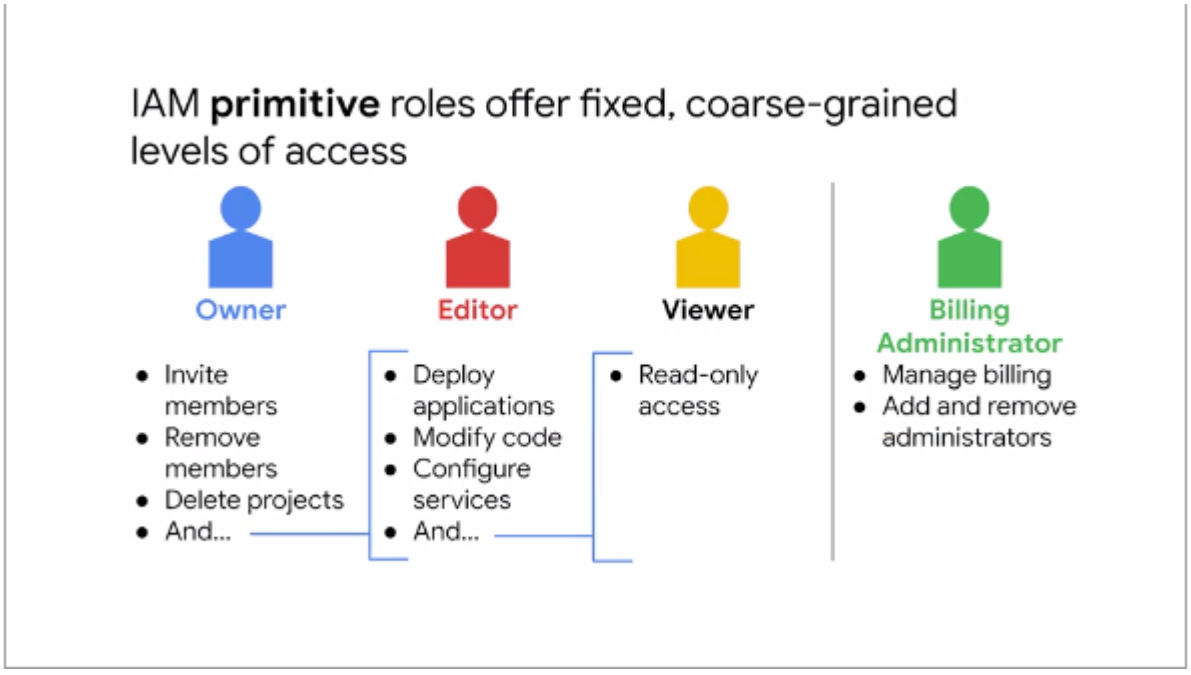
GCP 보안 주체(Who)

Google 계정		서비스 계정
Google 계정	개인 계정(Gmail 계정)	
Google 그룹	GCP를 가입할 수 없지만 IAM 정책은 가능	GCP에성 생성
Cloud ID 또는 Google Workspace 도메인	조직 계정	

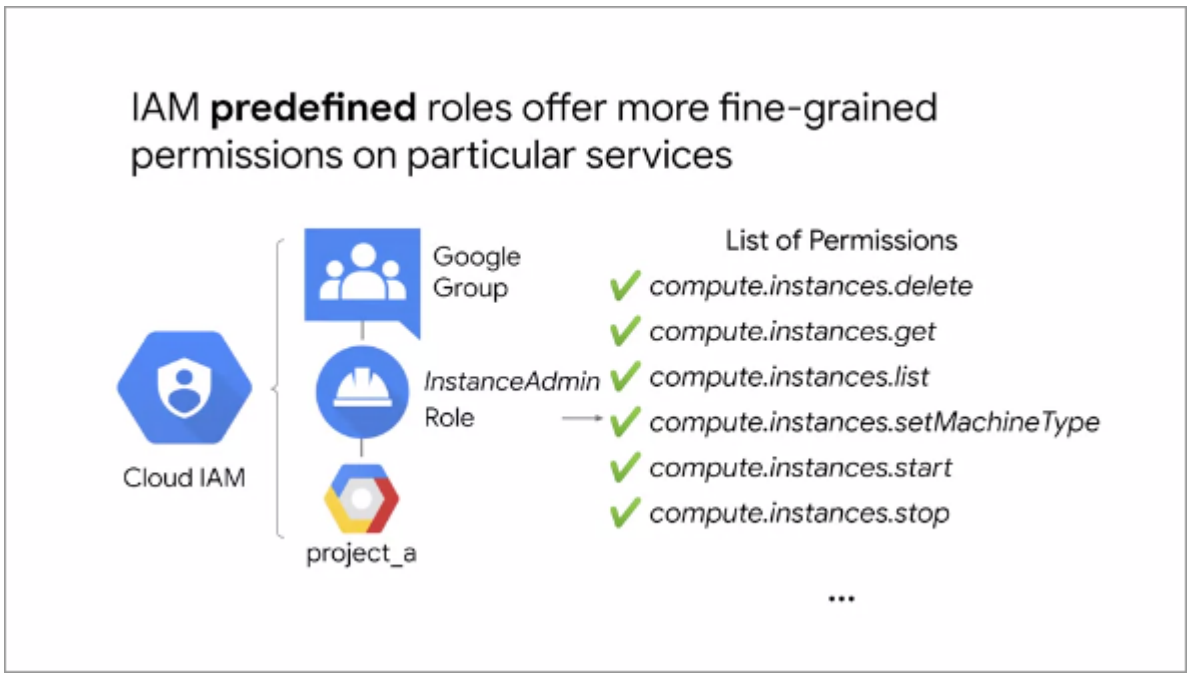
Role



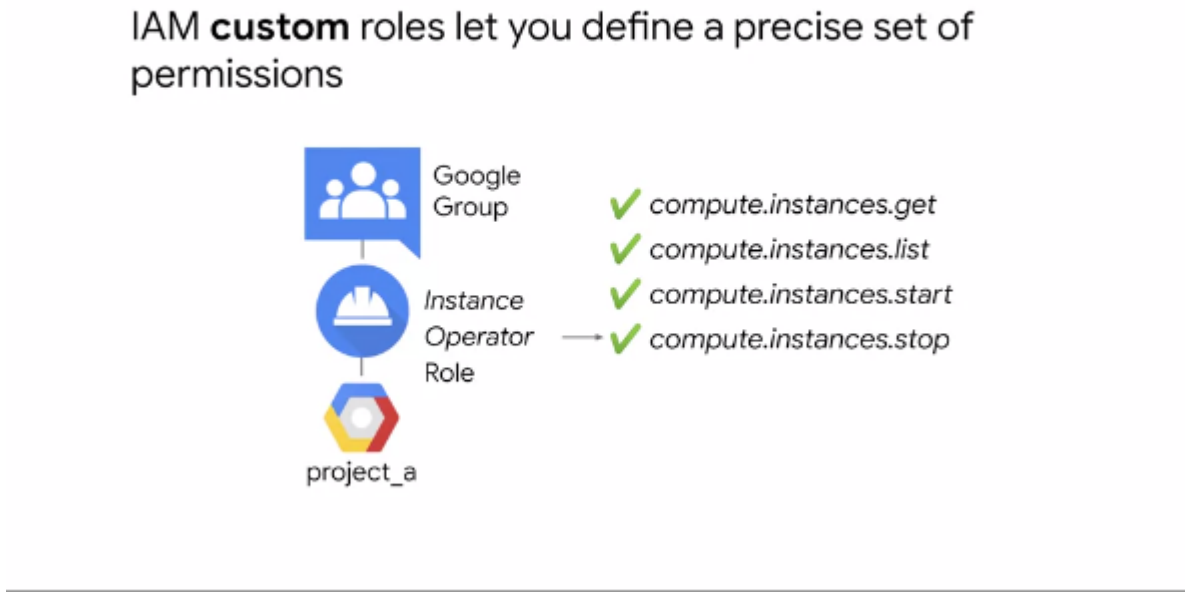
기본 역할



사전 정의된 역할

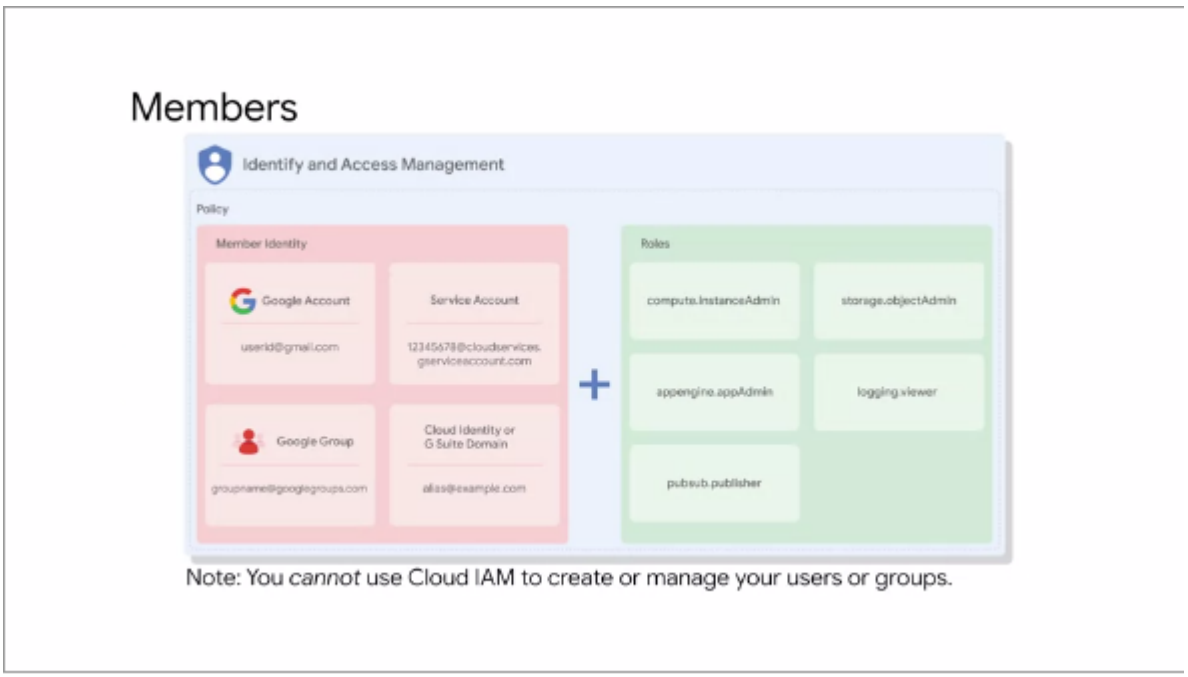

IAM **predefined** roles offer more fine-grained permissions on particular services
Google Group
InstanceAdmin Role
Cloud IAM
project_a
List of Permissions
compute.instances.delete
compute.instances.get
compute.instances.list
compute.instances.setMachineType
compute.instances.start
compute.instances.stop
...

커스텀 역할

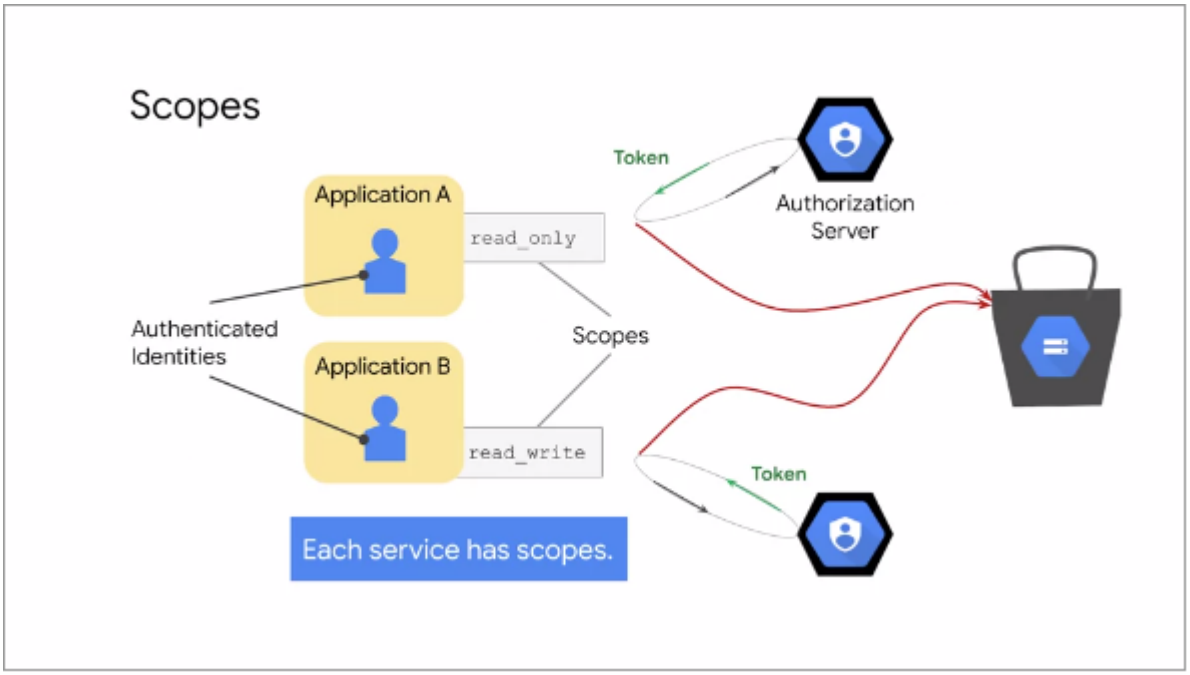

IAM **custom** roles let you define a precise set of permissions
Google Group
Instance Operator Role
project_a
compute.instances.get
compute.instances.list
compute.instances.start
compute.instances.stop

정책

- 정책은 바인딩의 목록으로 구성되고, 역할은 IAM에 의해 정의되는 명명된 권한 목록이다.
- 바인딩은 구성원의 목록을 역할에 바인딩한다. 구성원은 사용자 계정, 구글 그룹, 구글 도메인, 서비스 계정이 될 수 있다.

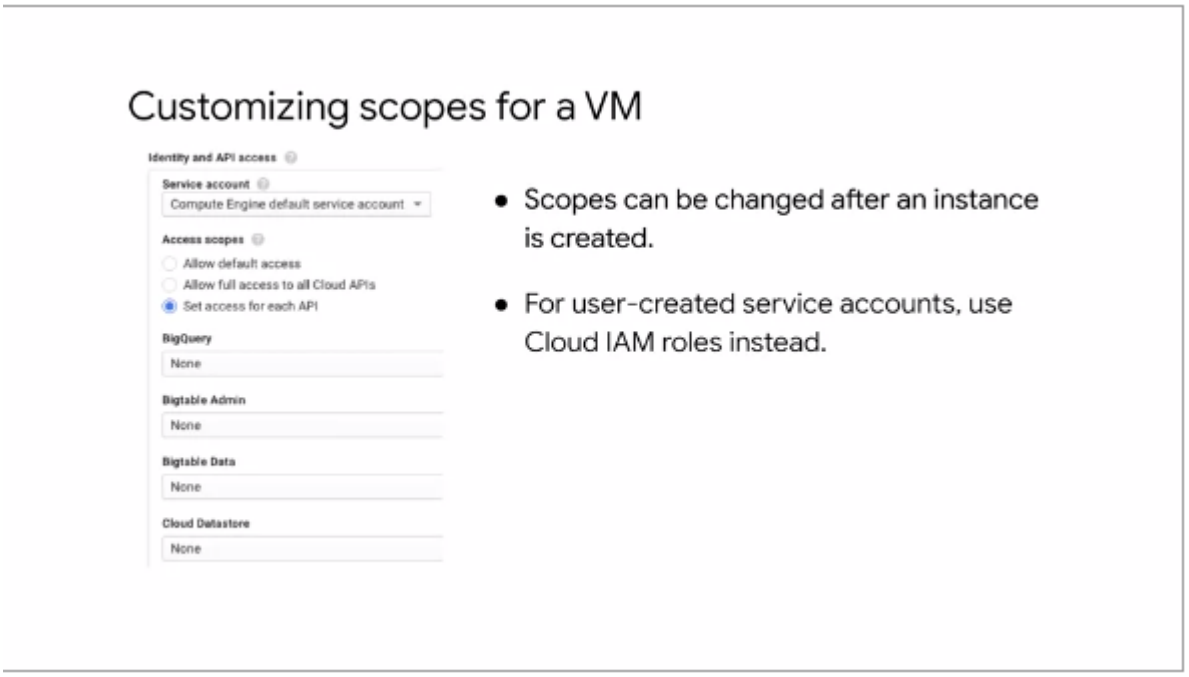


범위



범위 지정

- 범위는 인스턴스가 생성된 후에 변경할 수 있다.
- 사용자가 만든 서비스 계정의 경우 대신 IAM 역할을 사용한다.



- 새 Compute Engine 인스턴스를 만들면 자동으로 다음 액세스 범위가 구성된다.
  - Cloud Storage에 대한 읽기 전용 액세스
  - Compute Engine 로그를 작성할 수 있는 쓰기 액세스
  - Google Cloud 프로젝트에 측정항목 데이터를 게시할 수 있는 쓰기 액세스
  - Google CloudEndpoints에 필요한 서비스 관리 기능에 대한 읽기 전용 액세스
  - Google CloudEndpoints에 필요한 서비스 제어 기능에 대한 읽기 또는 쓰기 액세스
  - VM에서 실행되는 애플리케이션이 프로젝트에 trace 데이터를 쓸 수 있는 Cloud Trace에 대한 쓰기 액세스 권한

서비스 계정 vs 액세스 범위

- GCP에서 서비스 어카운트 권한과 액세스 범위는 서로 다른 두 가지 계층의 권한 제어라서, 둘 중 하나라도 허용하지 않으면 요청이 거부된다.
- 즉, IAM 역할(서비스 어카운트 권한)은 '무엇을 할 수 있는가'를 결정하고, 액세스 범위는 '어떤 API 리소스에 접근할 수 있는가'를 2차적으로 제한한다.
- 즉 서비스 계정이 GCP 리소스에서 수행할 수 있는 작업을 IAM을 통해서 부여하는 것이라면 액세스 범위는 해당 인스턴스가 호출할 수 있는 API 종류와 범위를 제한하는 추가 필터이다.

서비스 계정

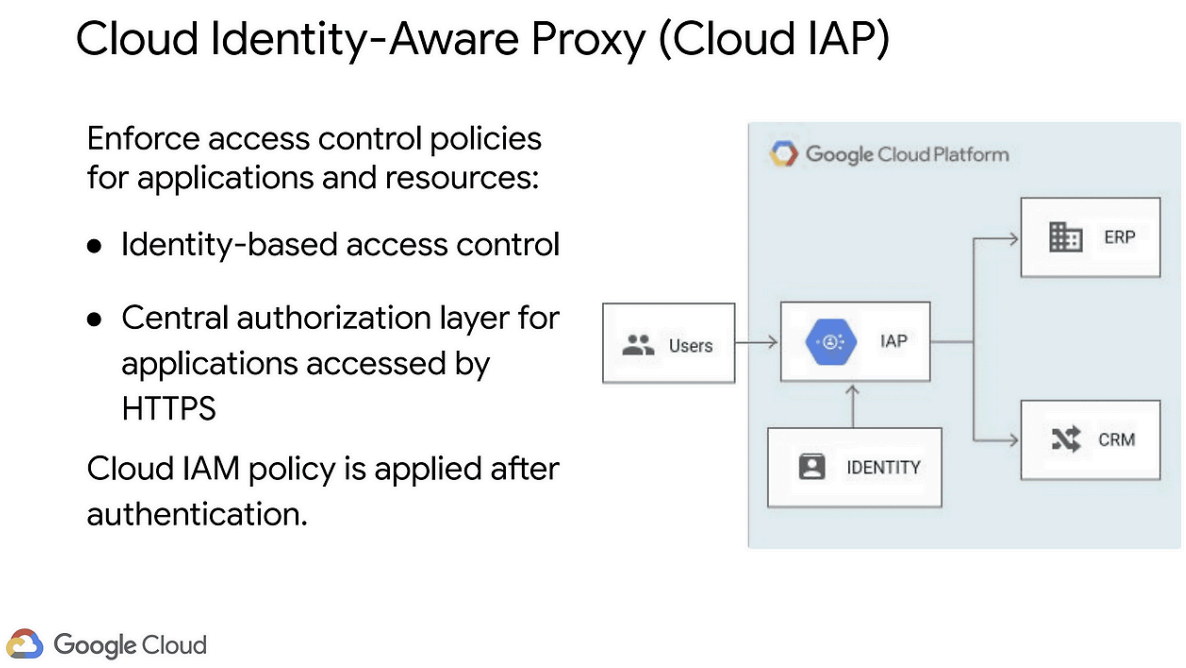
- 서비스 계정을 만들어 VM을 Cloud Storage에 인증

IAP(Identity-Aware Proxy)

애플리케이션 및 리소스에 대한 액세스 제어 정책 시행

- ID 기반의 액세스 제어
- HTTPS로 액세스할 수 있는 애플리케이션을 위한 중앙 승인 레이어

IAM 정책은 인증 후 적용된다.



서비스 계정

Key differences between IAM concepts in Google Cloud and AWS

IAM concept	Google Cloud	AWS
Programmatic identity	Cloud IAM service account	IAM role and instance profile
User identity	Managed outside Cloud IAM. Identity federated to external identity management system.	Managed in IAM. Identity federated to external identity management system.
Policy	A list of bindings. A binding binds a list of members to a role.	A document that explicitly lists permissions.
Permission collection	Role	Policy
Predefined set of permissions	Predefined roles	Managed policies