Google Cloud Platform

Getting Started with Google Cloud Platform

Google Cloud Platform Fundamentals

V2.0

Agenda

1. Google Cloud Platform Projects
2. Identity and Access Management (IAM)
3. Interacting with Google Cloud Platform
4. Quiz & Lab

Projects (1 of 2)

- All Google Cloud Platform services are associated with a project that is used to:
  - Track resource and quota usage
  - Enable billing
  - Manage permissions and credentials
  - Enable services and APIs

Projects (2 of 2)

- Projects use three identifying attributes:
  - Project Name
  - Project Number
  - Project ID
    - Also known as Application ID
- Interact with projects using the Cloud Console or the Cloud Resource Manager API Alpha

Project Permissions - Primitive Roles

Owner

Invite members
Remove members
Can delete project
Includes Editor rights

Editor

Deploy applications
Modify code
Configure services
Includes Viewer rights

Viewer

Read-only access

Billing administrator

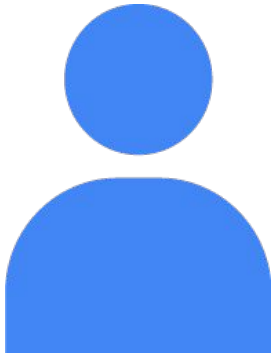
Manage billing
Add administrators
Remove administrators

A project can have multiple owners, editors, viewers and billing administrators.

Agenda

1. Google Cloud Platform Projects
2. Identity and Access Management (IAM)
3. Interacting with Google Cloud Platform
4. Quiz & Lab

Identity and Access Management



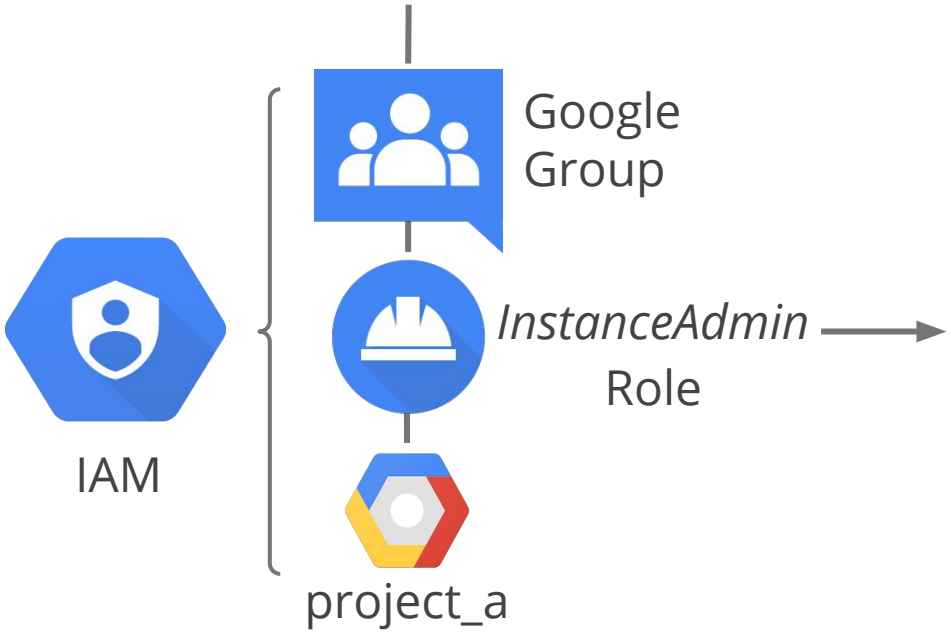
Who

can do what

on which resource

IAM Roles - Curated Roles

- *Google Account* (test@gmail.com)
- *Service Account* (test@project_id.iam.gserviceaccount.com)
- *Google Group* (test@googlegroups.com)
- *Google Apps Domain* (test@example.com)



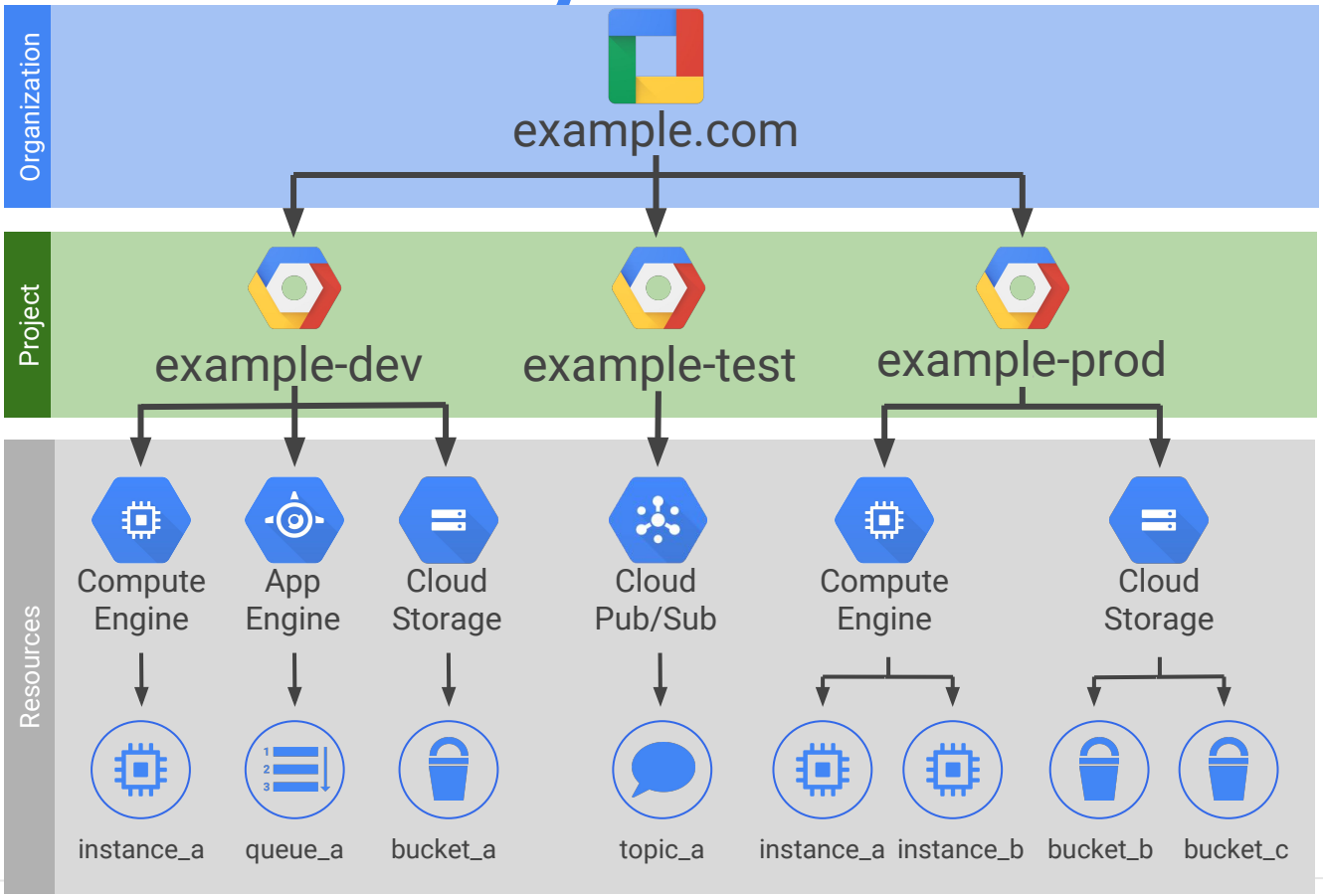
List of Permissions

- ✔ *compute.instances.delete*
- ✔ *compute.instances.get*
- ✔ *compute.instances.list*
- ✔ *compute.instances.setMachineType*
- ✔ *compute.instances.start*
- ✔ *compute.instances.stop*

. . .

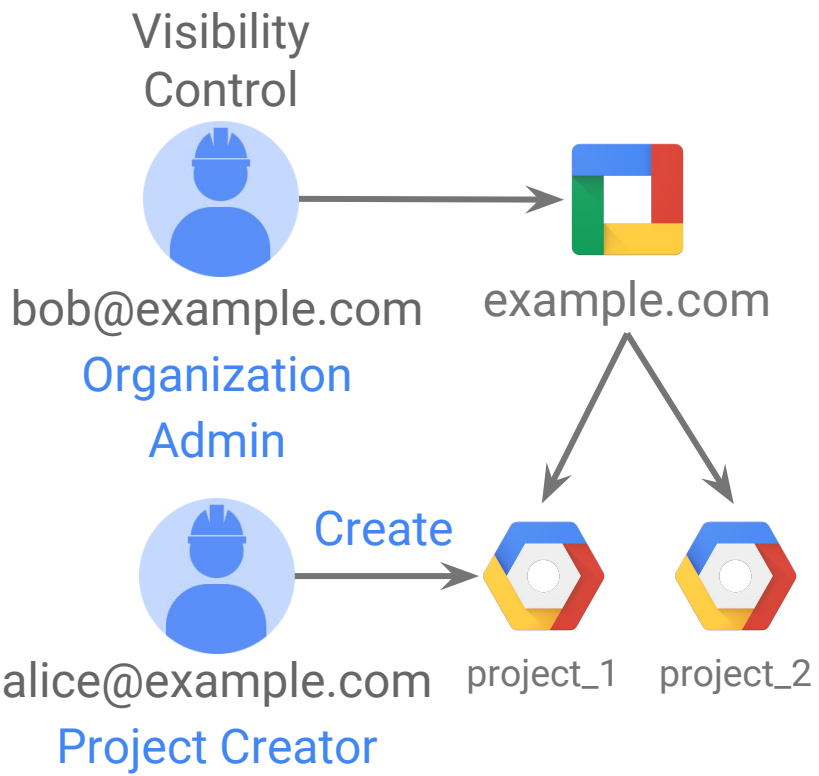
IAM Resource Hierarchy

- A policy is set on a resource
  - Each policy contains: Set of roles, role members
- Resources inherit policies from parent
  - Resource policies are a union of parent and resource
- If parent policy less restrictive, overrides more restrictive resource policy



Organization Node Beta

- Organization node is root node for Google Cloud resources
- 2 organization roles:
  - *Organization Admin* - Control over all cloud resources
  - *Project Creator* - Controls project creation



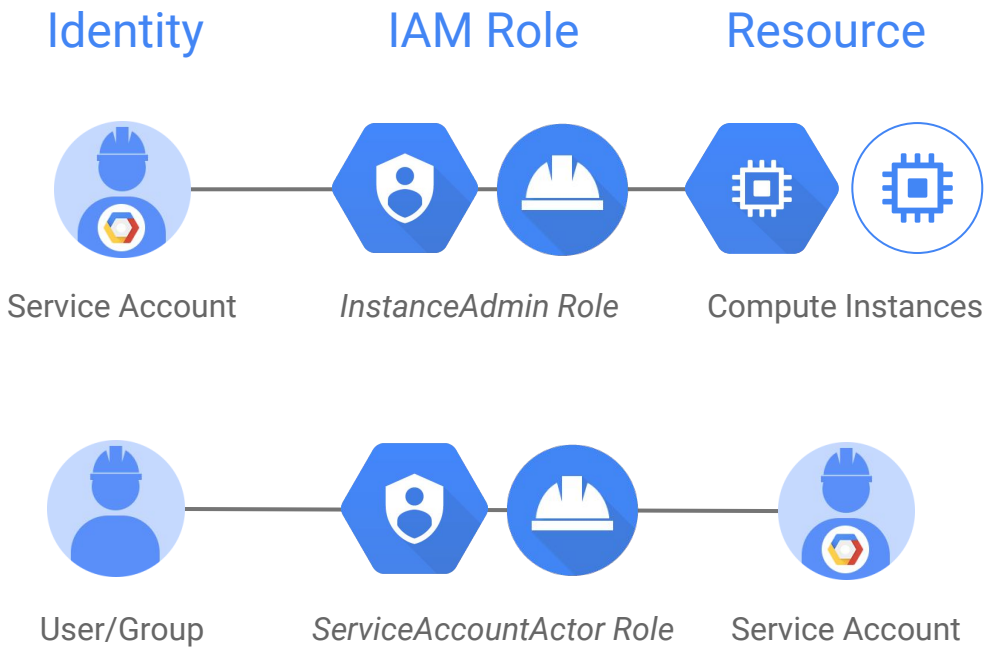
Service Accounts

- Provide an identity for carrying out **server-to-server** interactions in a project
- Used to **authenticate** from one service to another
- Can be used with primitive and curated roles
- Identified with an **email** address:

```
<project_number>@developer.gserviceaccount.com
<project_id>@developer.gserviceaccount.com
```

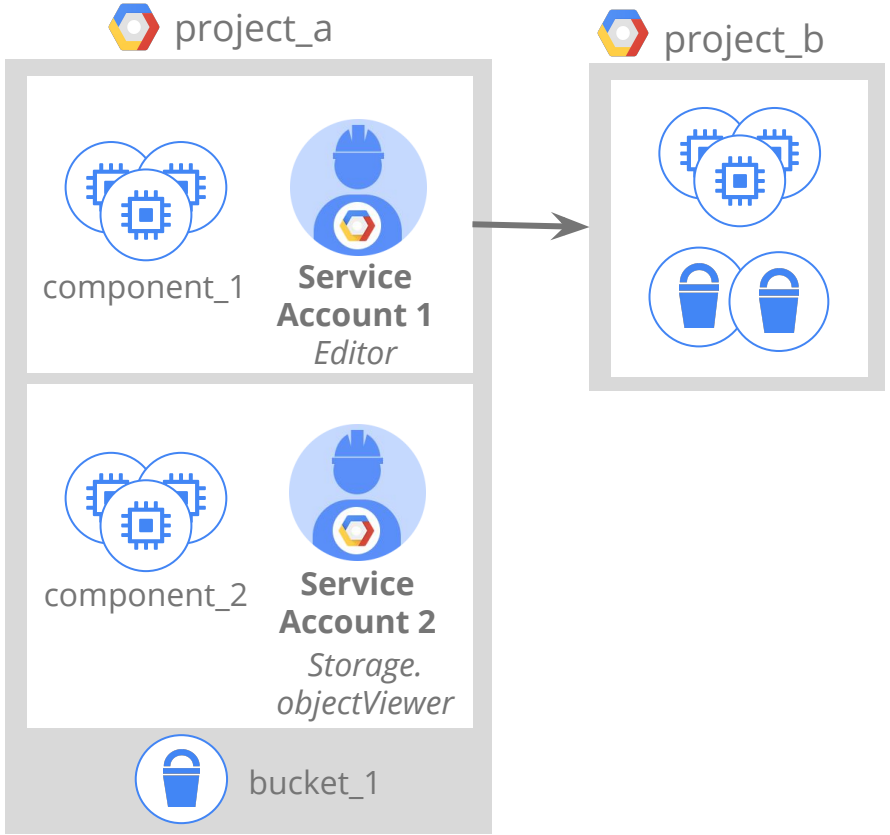
Service Accounts and IAM

- Service accounts authenticate with keys
  - Google manages keys, key rotation for Compute Engine and App Engine
- Can assign an IAM role to the service account
- Can also assign ServiceAccountActor role to users/groups



Example: Service Accounts and IAM

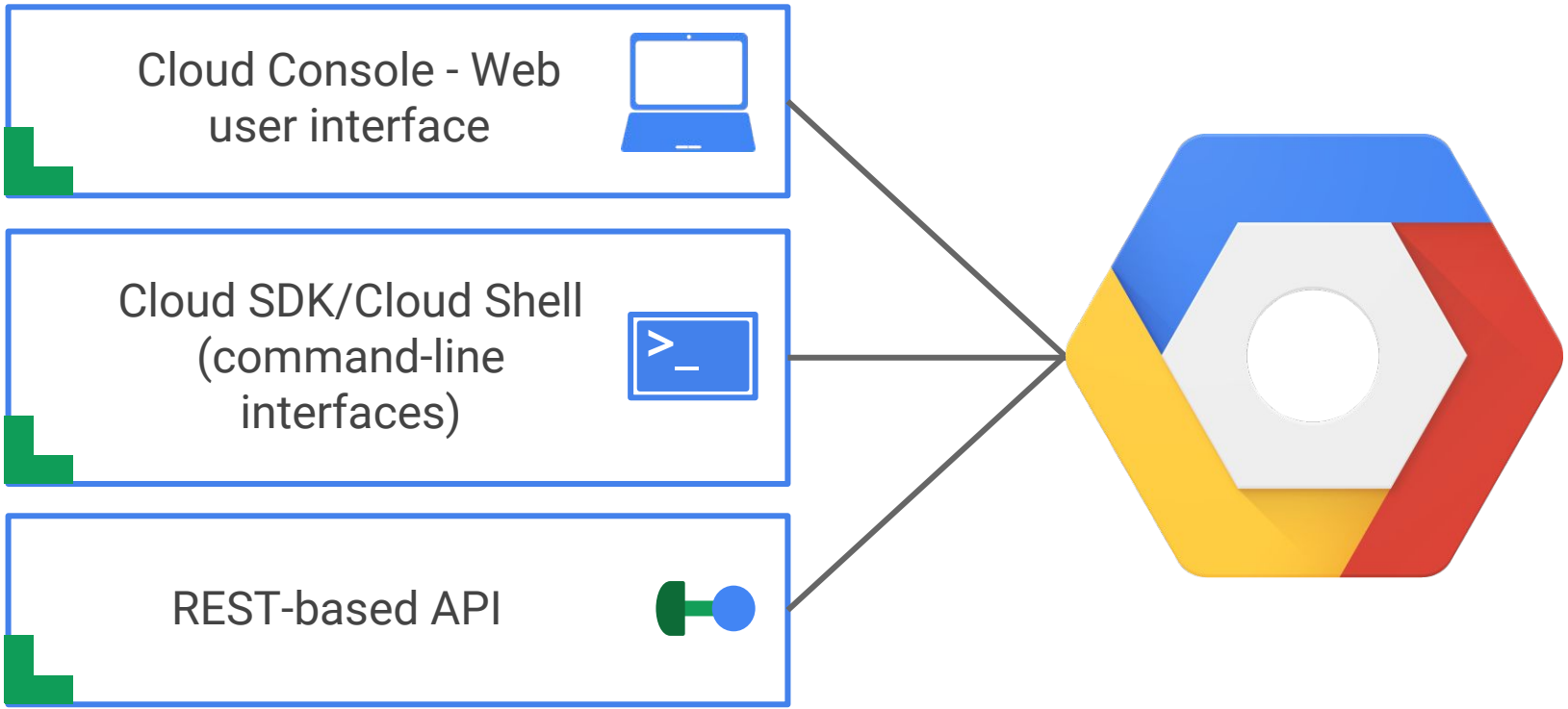
- VMs running component_1 are granted Editor access to project_b using *Service Account 1*
- VMs running component_2 are granted objectViewer access to bucket_1 using *Service Account 2*
- Service account permissions can be changed without recreating VMs



Agenda

1. Google Cloud Platform Projects
2. Identity and Access Management (IAM)
3. Interacting with Google Cloud Platform
4. Quiz & Lab

Interacting with Google Cloud Platform



Google Cloud Platform Console

- Centralized console for all project data
- Developer tools
  - Cloud Source Repositories
  - Cloud Shell
- Access to product APIs
- Manage, create projects

Google Cloud SDK

- SDK includes CLI tools for Cloud Platform products and services
  - gcloud, gsutil (Cloud Storage), bq (BigQuery)
- Available as Docker image
- Available via Cloud Shell
  - Containerized version of Cloud SDK running on Compute Engine instance

RESTful APIs

- Programmatic access to products and services
  - Typically use JSON as an interchange format
  - Use OAuth 2.0 for authentication and authorization
- Enabled through the Google Cloud Platform Console
- Most APIs include daily quotas and rates (limits) that can be raised by request
  - Important to **plan ahead** to manage your required capacity
- Experiment with APIs Explorer

APIs Explorer

- The APIs Explorer is an interactive tool that lets you easily try Google APIs using a browser
- With the APIs Explorer, you can:
  - Browse quickly through available APIs and versions.
  - See methods available for each API and what parameters they support along with inline documentation.
  - Execute requests for any method and see responses in real time.
  - Make authenticated and authorized API calls with ease.

Client Libraries

- Google Cloud Client Libraries
  - Community-owned, hand-crafted client libraries
- Google APIs Client Libraries
  - Open source, generated
  - Support various languages
    - Java, Python, JavaScript, PHP, .NET, Go, Node.js, Ruby, Objective-C, Dart

Agenda

1. Google Cloud Platform Projects
2. Identity and Access Management (IAM)
3. Interacting with Google Cloud Platform
4. Quiz & Lab

Quiz (1 of 2)

1. *True or False*: In Google Cloud IAM, if a policy gives you Owner permissions at the project level, your access to an individual resource in the project may be restricted to Viewer by applying a more restrictive policy to that resource.
2. *True or False*: All Google Cloud Platform resources are associated with a project.

Quiz Answers (1 of 2)

1. *False*: Policies are a union of the parent and the resource. If a parent policy is less restrictive, it overrides a more restrictive resource policy.
2. *True*: All Google Cloud Platform resources are associated with a project.

Quiz (2 of 2)

Service accounts are used to provide which of the following?

- ❑ Authentication between Google Cloud Platform services
- ❑ Key generation and rotation when used with App Engine and Compute Engine
- ❑ A way to restrict the actions a resource (such as a VM) can perform
- ❑ A way to allow users to act with service account permissions
- ❑ All of the above

Quiz Answers (2 of 2)

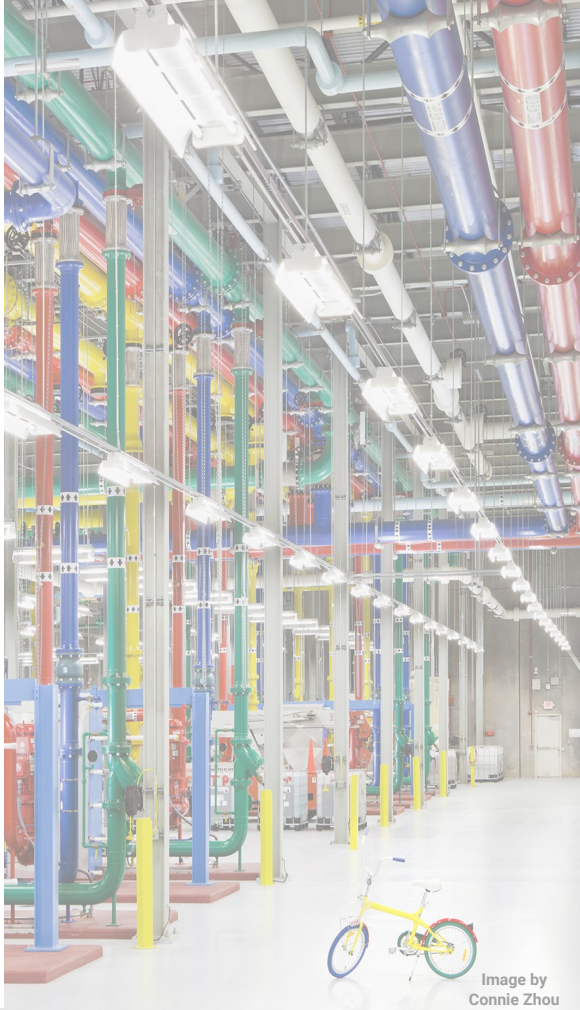
Service accounts are used to provide which of the following?

- ❑ Authentication between Google Cloud Platform services
- ❑ Key generation and rotation when used with App Engine and Compute Engine
- ❑ A way to restrict the actions a resource (such as a VM) can perform
- ❑ A way to allow users to act with service account permissions
- ✓ All of the above

Lab

Deploy a virtual development environment using Google Cloud Launcher.

1. Deploy a Bitnami LAMP stack to Compute Engine using Cloud Launcher
2. Verify the deployment



Resources

- Cloud SDK installation and quick start
  https://cloud.google.com/sdk/#Quick_Start
- ‘gcloud’ tool guide
  https://cloud.google.com/sdk/gcloud/
- IAM
  https://cloud.google.com/iam/
- Configuring permissions on Google Cloud Platform
  https://cloud.google.com/docs/permissions-overview
- Google Cloud Platform security
  https://cloud.google.com/security/


cloud.google.com