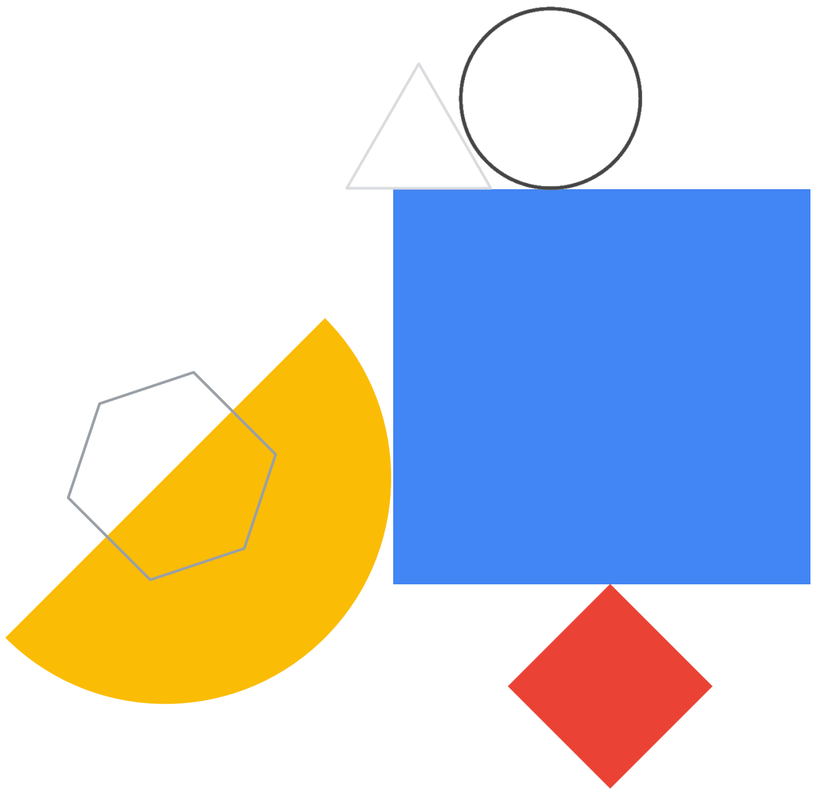
Google Cloud

Identity and Access Management



Agenda

01 Identity and Access Management (IAM)

02 Organization

03 Roles

04 Members

05 Service Accounts

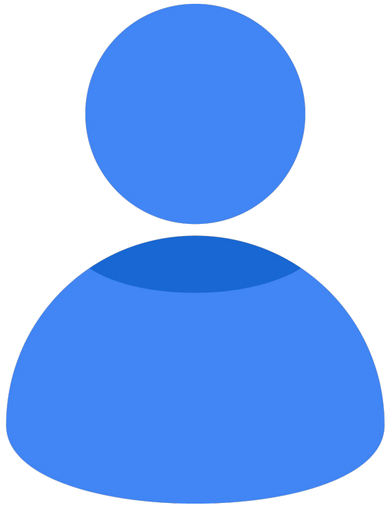
06 IAM Best Practices

Lab: Exploring IAM

01

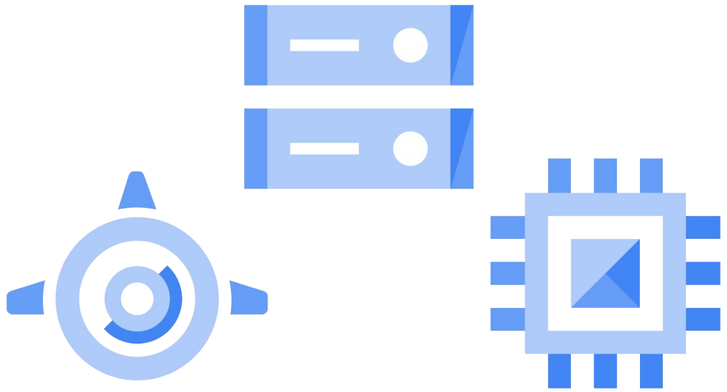
Identity and Access Management (IAM)

Identity and Access Management



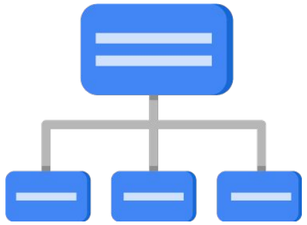
Who

can do what



on which resource

IAM objects



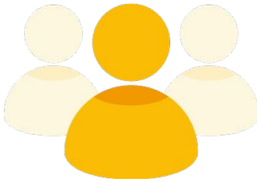
Organization

Folders

Projects

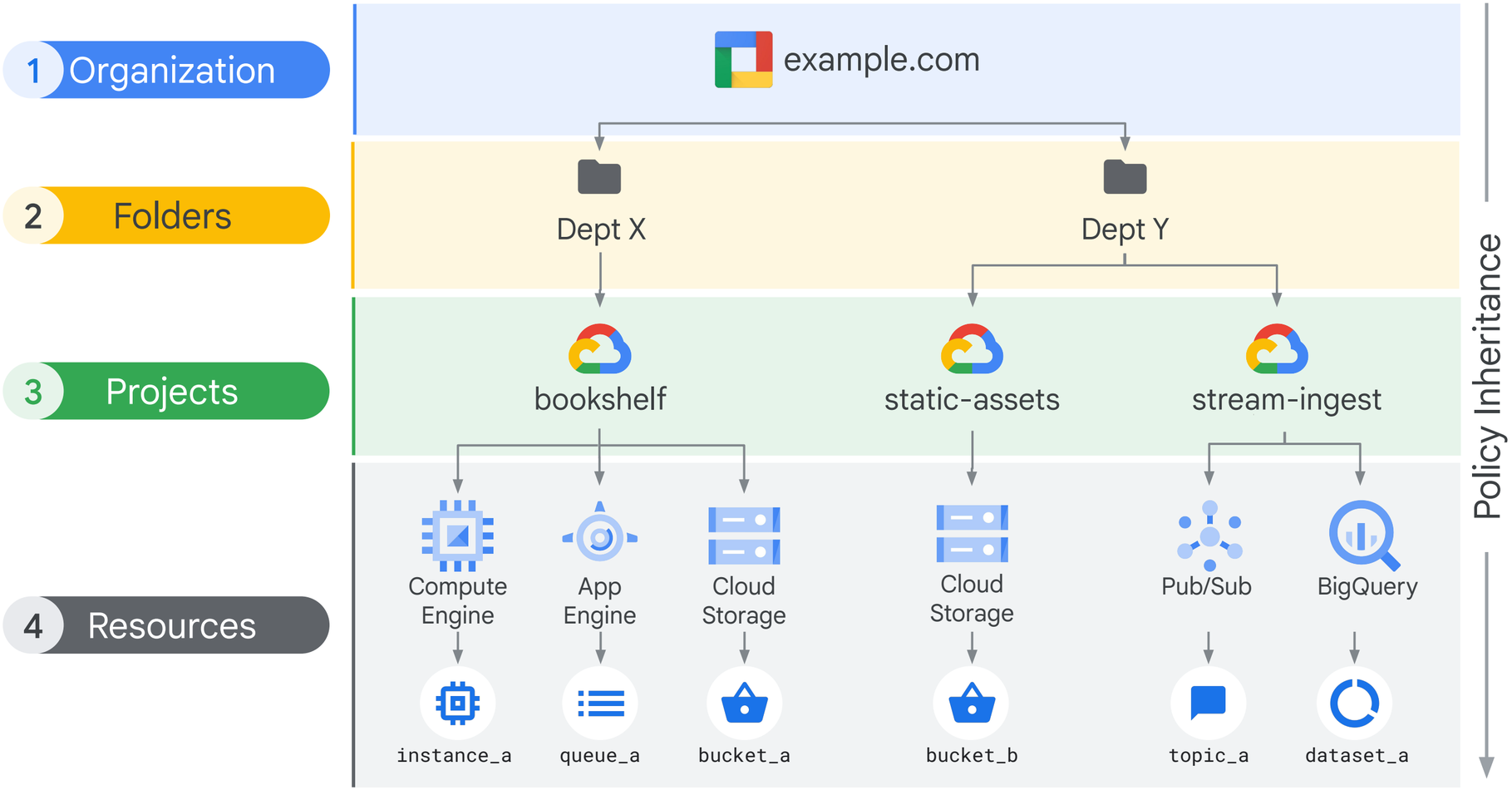
Resources

Roles



Members

IAM resource hierarchy

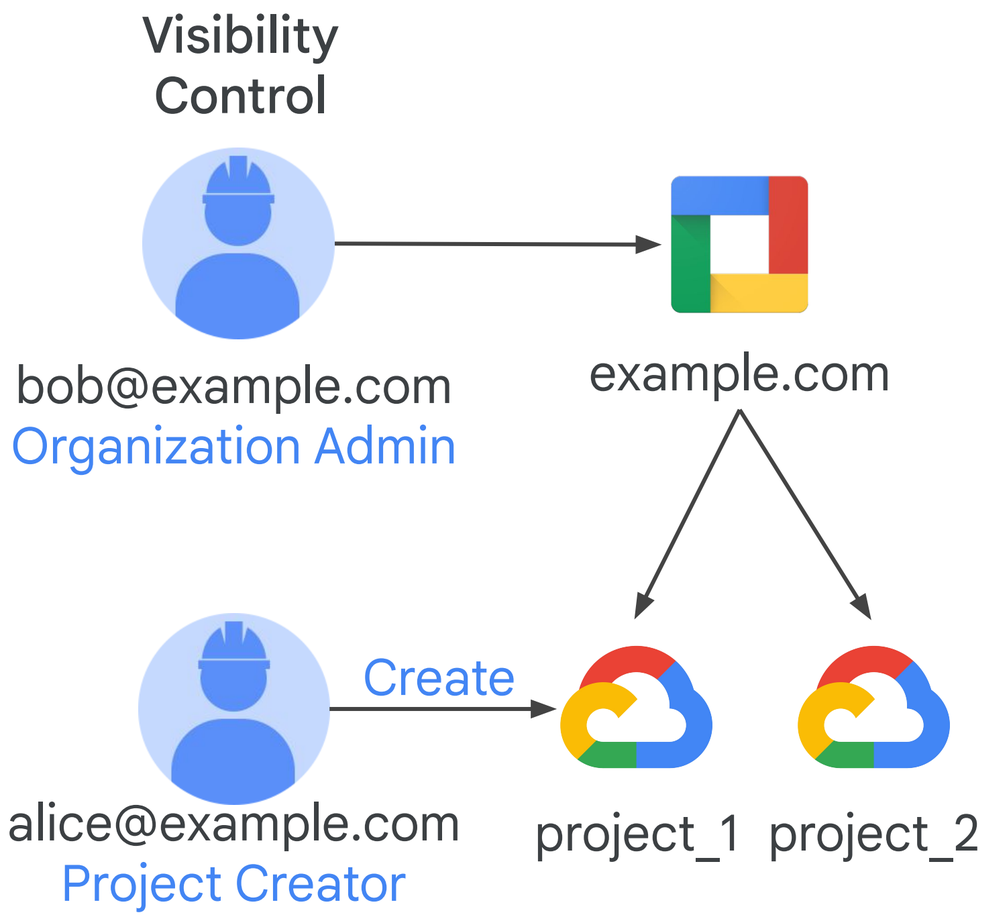


02

Organization

Organization node

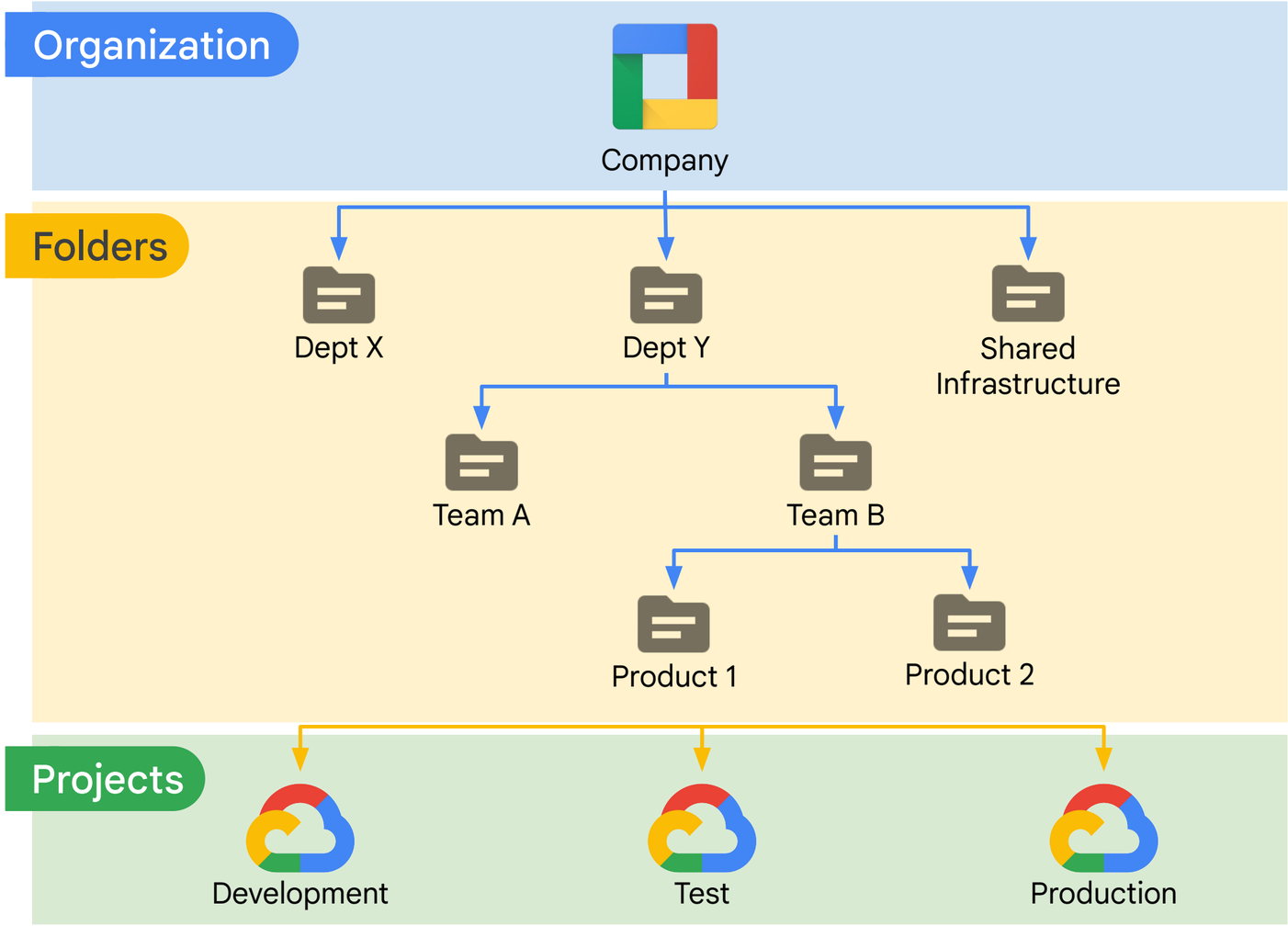
- An organization node is a root node for Google Cloud resources
- Organization roles:
  - **Organization Admin:** Control over all cloud resources; useful for auditing
  - **Project Creator:** Controls project creation; control over who can create projects



Creating and managing organizations

- Created when a **Google Workspace** or **Cloud Identity** account creates a Google Cloud Project
- **Workspace** or **Cloud Identity** super administrator:
  - Assign the **Organization admin** role to some users
  - Be the point of contact in case of recovery issues
  - Control the lifecycle of the Workspace or Cloud Identity account and Organization resource
- **Organization admin:**
  - Define IAM policies
  - Determine the structure of the resource hierarchy
  - Delegate responsibility over critical components such as Networking, Billing, and Resource Hierarchy through IAM roles

Folders



Additional grouping mechanism and isolation boundaries between projects:

- Different legal entities
- Departments
- Teams

Folders allow delegation of administration rights.

Resource manager roles

Organization

- **Admin:** Full control over all resources
- **Viewer:** View access to all resources

Folder

- **Admin:** Full control over folders
- **Creator:** Browse hierarchy and create folders
- **Viewer:** View folders and projects below a resource

Project

- **Creator:** Create new projects (automatic owner) and migrate new projects into organization
- **Deleter:** Delete projects

Policy Inheritance

03

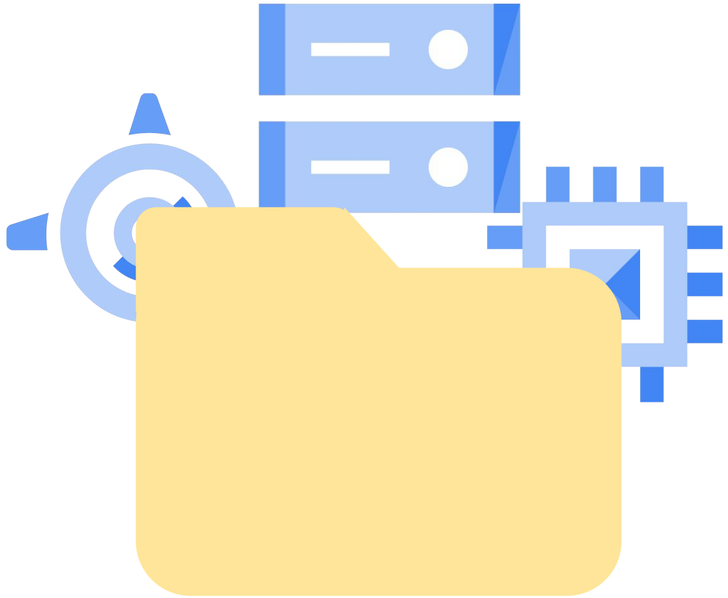
Roles

There are three types of IAM roles

Basic

Predefined

Custom

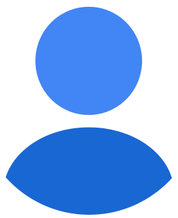


IAM basic roles apply across all Google Cloud services in a project

can do what

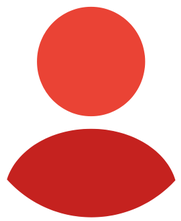
on all resources

IAM basic roles offer fixed, coarse-grained levels of access



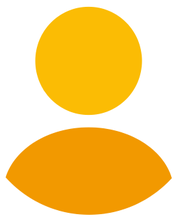
Owner

- Invite members
- Remove members
- Delete projects
- And...



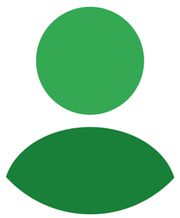
Editor

- Deploy applications
- Modify code
- Configure services
- And...



Viewer

- Read-only access



Billing Administrator

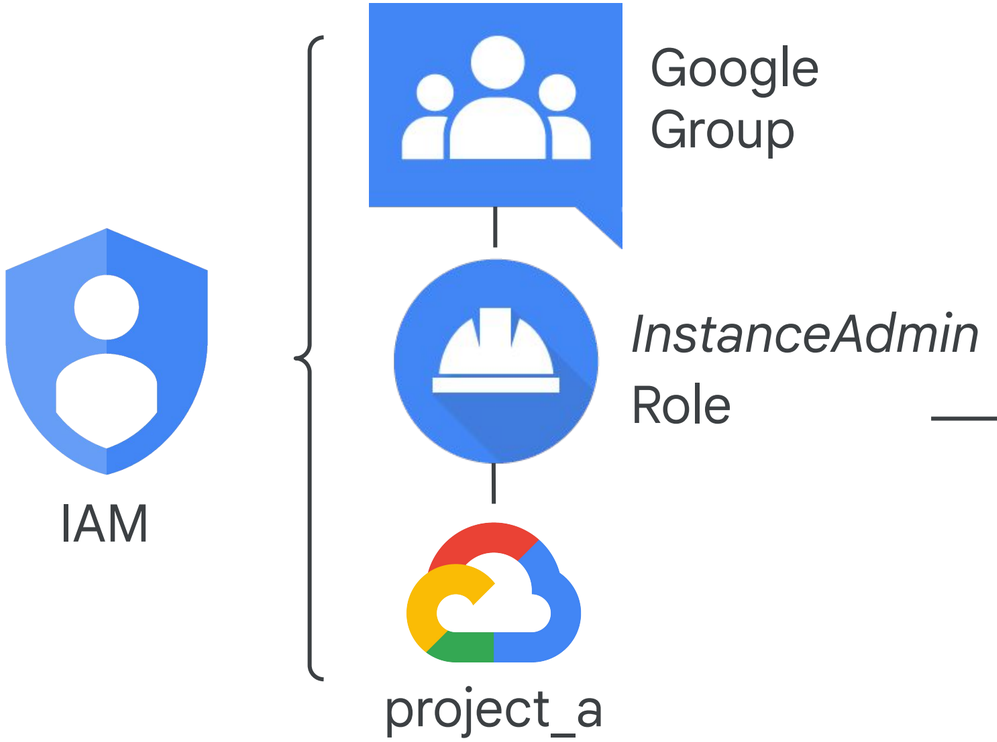
- Manage billing
- Add and remove administrators

IAM **predefined** roles apply to a particular Google Cloud service in a project

can do what

on Compute Engine resources in this project, or folder, or org

IAM **predefined** roles offer more fine-grained permissions on particular services



List of Permissions

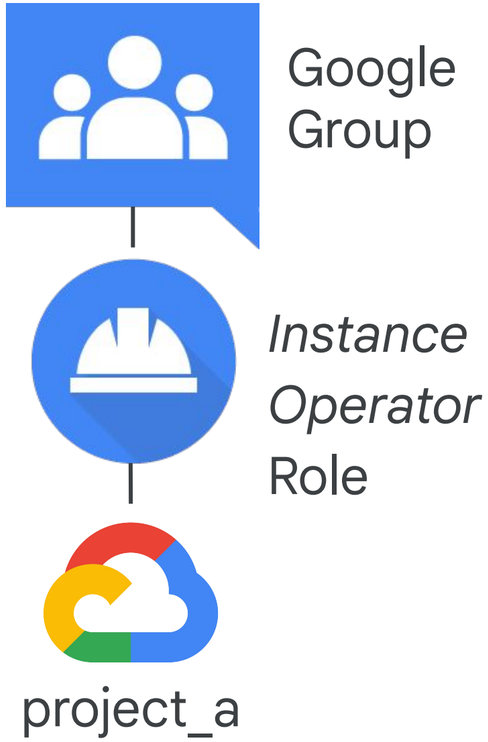
- ✔ `compute.instances.delete`
- ✔ `compute.instances.get`
- ✔ `compute.instances.list`
- ✔ `compute.instances.setMachineType`
- ✔ `compute.instances.start`
- ✔ `compute.instances.stop`

...

Compute Engine IAM roles

Role Title	Description
Compute Admin	Full control of all Compute Engine resources (compute.*)
Network Admin	Permissions to create, modify, and delete networking resources, except for firewall rules and SSL certificates
Storage Admin	Permissions to create, modify, and delete disks, images, and snapshots

IAM **custom** roles let you define a precise set of permissions

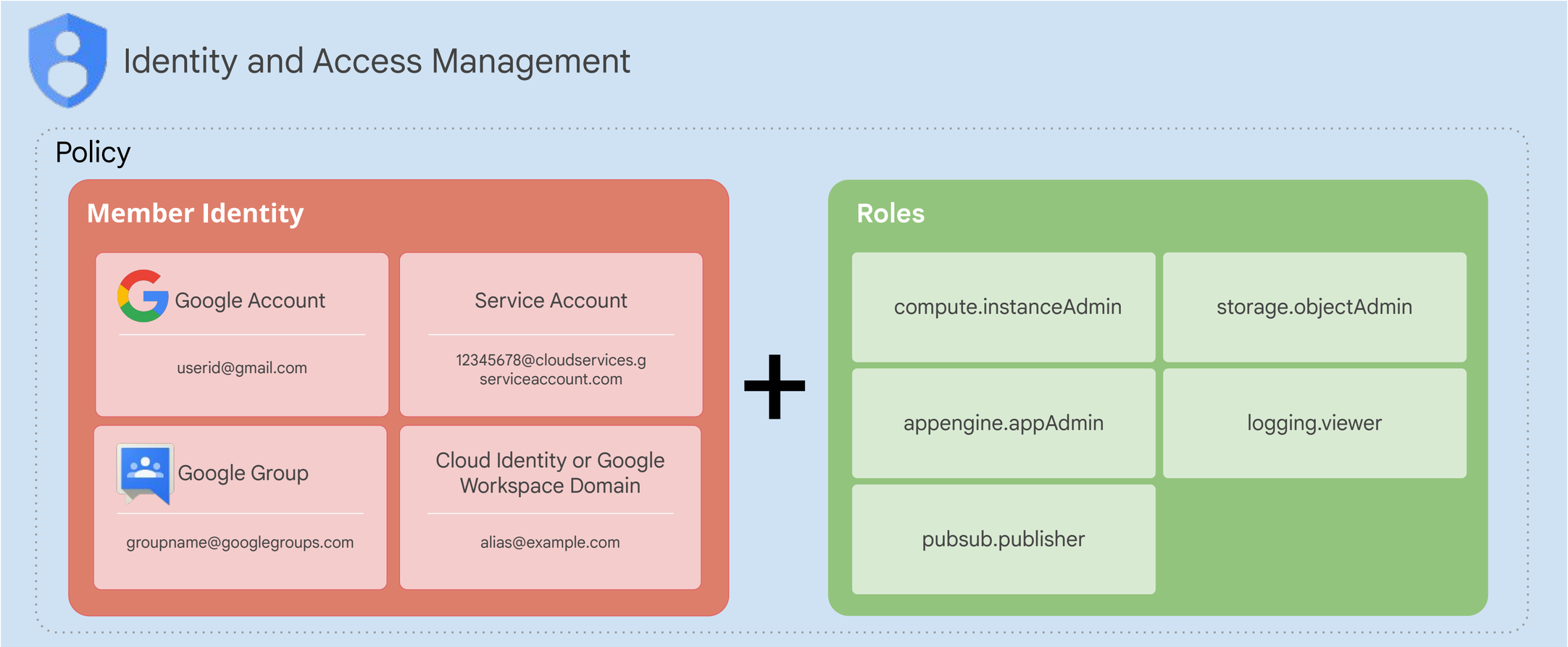


- ✔ `compute.instances.get`
- ✔ `compute.instances.list`
- ✔ `compute.instances.start`
- ✔ `compute.instances.stop`

04

Members

Members

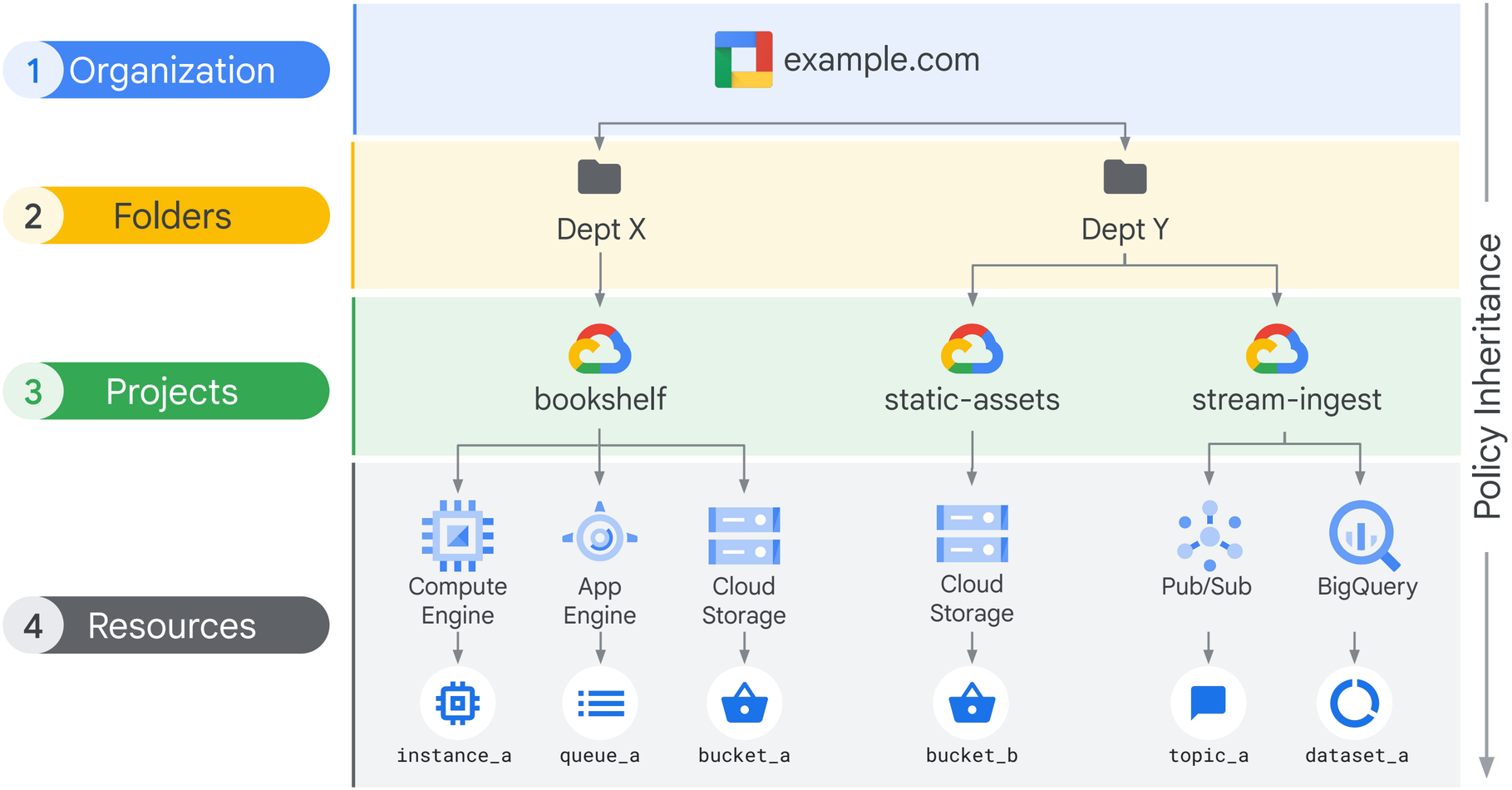


Note: You *cannot* use IAM to create or manage your users or groups.

IAM policies

- A policy consists of a list of bindings.
- A binding binds a list of members to a role.

IAM resource hierarchy



IAM allow policies

- Grant access to Google Cloud resources
- Controls access to the resource itself, as well as any descendants of that resource
- Associates, or binds, one or more principals (also known as a member or identity) with a single IAM role

```
{
  "bindings": [
    {
      "members": [
        "user:jie@example.com"
      ],
      "role": "roles/resourcemanager.organizationAdmin"
    },
    {
      "members": [
        "user:raha@example.com",
        "user:jie@example.com"
      ],
      "role": "roles/resourcemanager.projectCreator"
    }
  ],
  "etag": "BwUjMhCsNvY=",
  "version": 1
}
```

IAM deny policies

Deny rules prevent certain principals from using certain permissions, regardless of the roles they're granted.

Deny policies are made up of deny rules. Each deny rule specifies:

- A set of principals that are denied permissions
- The permissions that the principals are denied, or unable to use
- Optional: The condition that must be true for the permission to be denied

When a principal is denied a permission, they can't do anything that requires that permission.

IAM Conditions

Enforce conditional, attribute-based access control for Google Cloud resources.

- Grant resource access to identities (members) only if configured conditions are met.
- Specified in the role bindings of a resource's IAM policy.

Organization policies

An organization policy is:

- A configuration of restrictions
- Defined by configuring a constraint with desired restrictions.
- Applied to the organization node, folders or projects.

Example to restrict the service account key creation

Cloud Organization Policies let you constrain access to resources at and below this organization, folder or project. You can edit restrictions on the policy detail page.

Filter | Name : Disable service account key creation | Filter by constraint name, ID, or type

Name	ID	Constraint type
Disable service account key creation	constraints/iam.disableServiceAccountKeyCreation	Boolean

What if I already have a different corporate directory?

Microsoft Active Directory or LDAP

Google Cloud Directory Sync

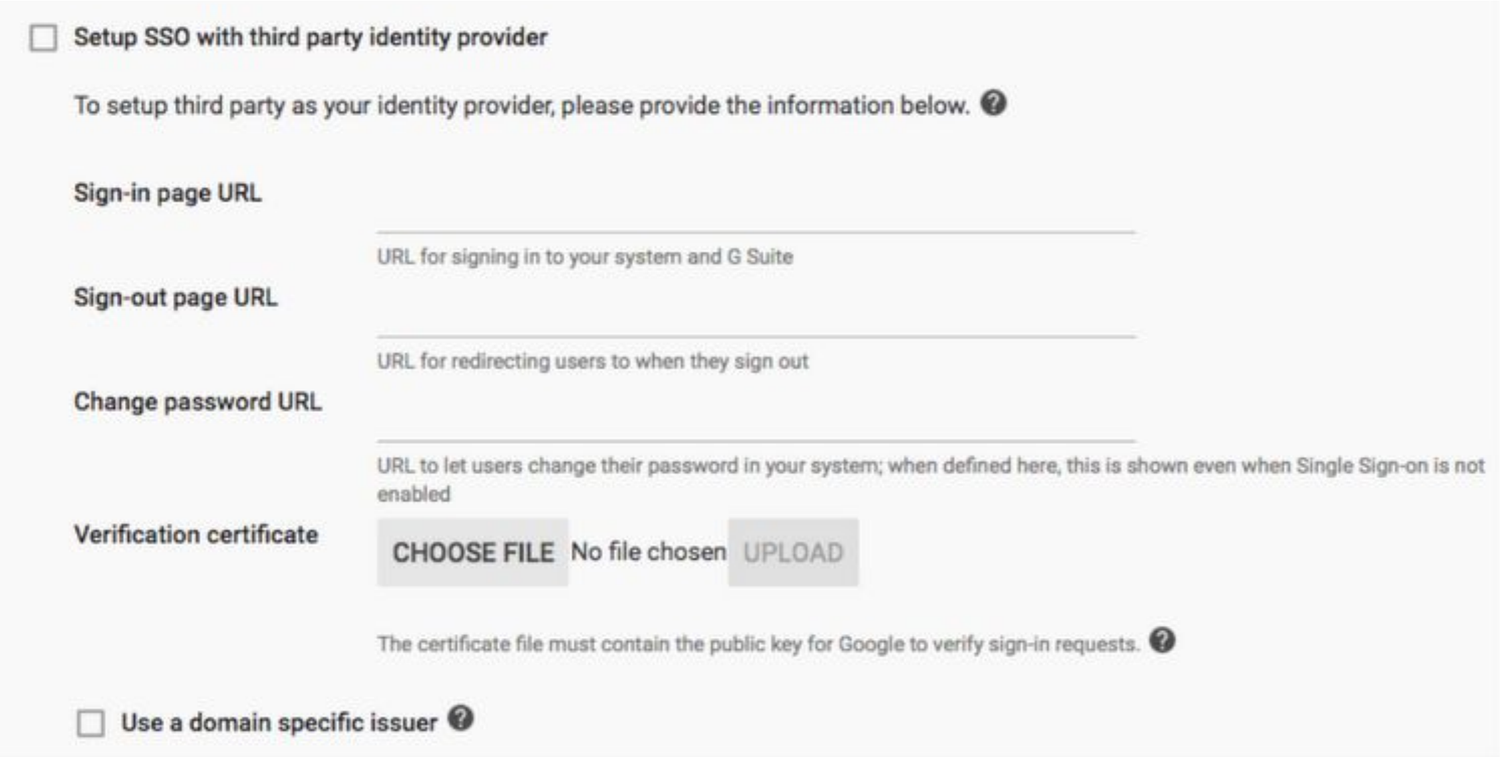
Users and groups in your existing directory service

Scheduled one-way sync

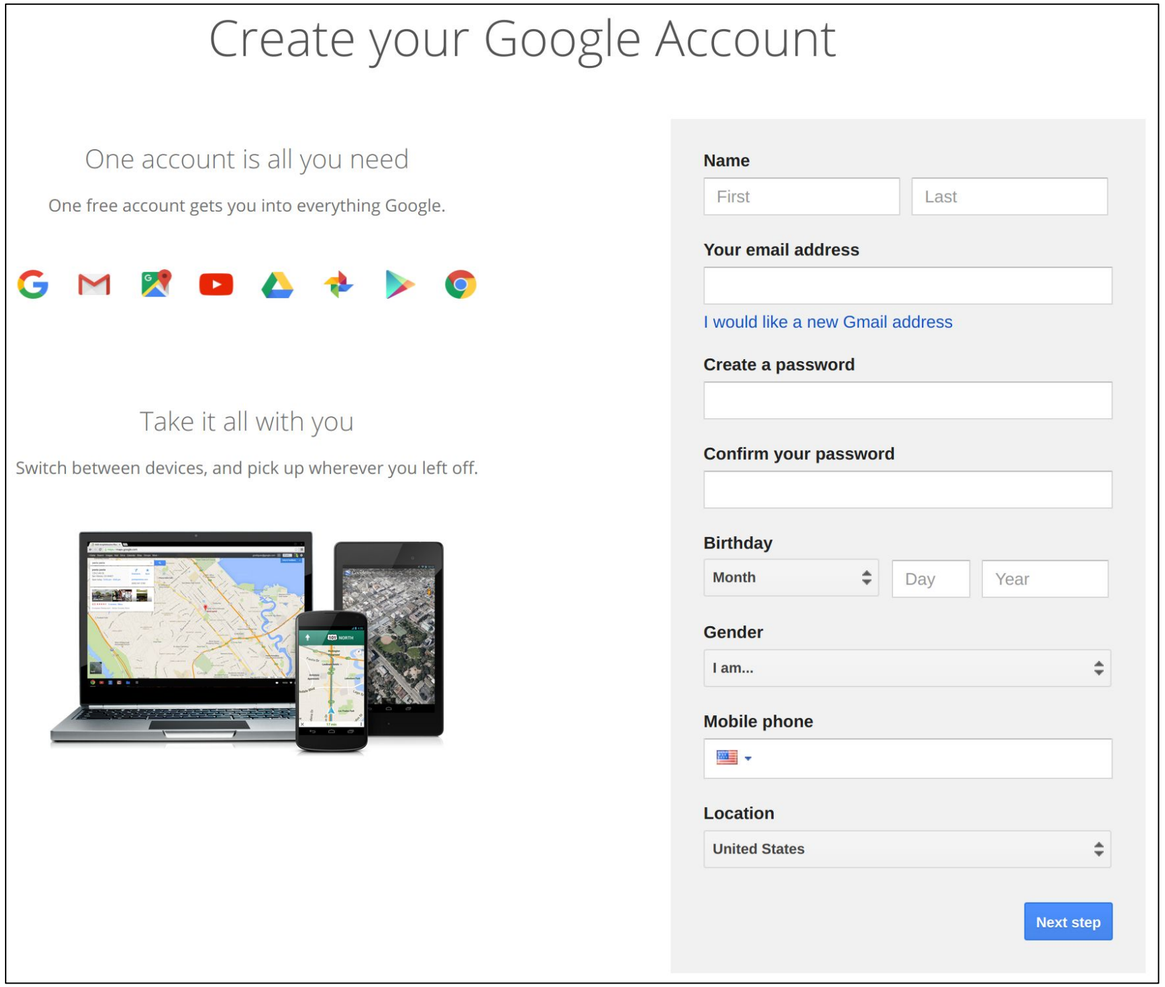
Users and groups in your Cloud Identity domain

Single sign-on (SSO)

- Use Cloud Identity to configure SAML SSO,
- If SAML2 isn’t supported, use a third-party solution (ADFS, Ping, or Okta).



Google Cloud access without Gmail



- You can get a Google password without Gmail.
- There are benefits to having a domain, including group permissions.

05

Service Accounts

Service accounts provide an identity for carrying out service-to-service interactions

- Programs running within Compute Engine instances can automatically acquire access tokens with credentials.
- Tokens are used to access any service API in your project and any other services that granted access to that service account.
- Service accounts are convenient when you're not accessing user data.

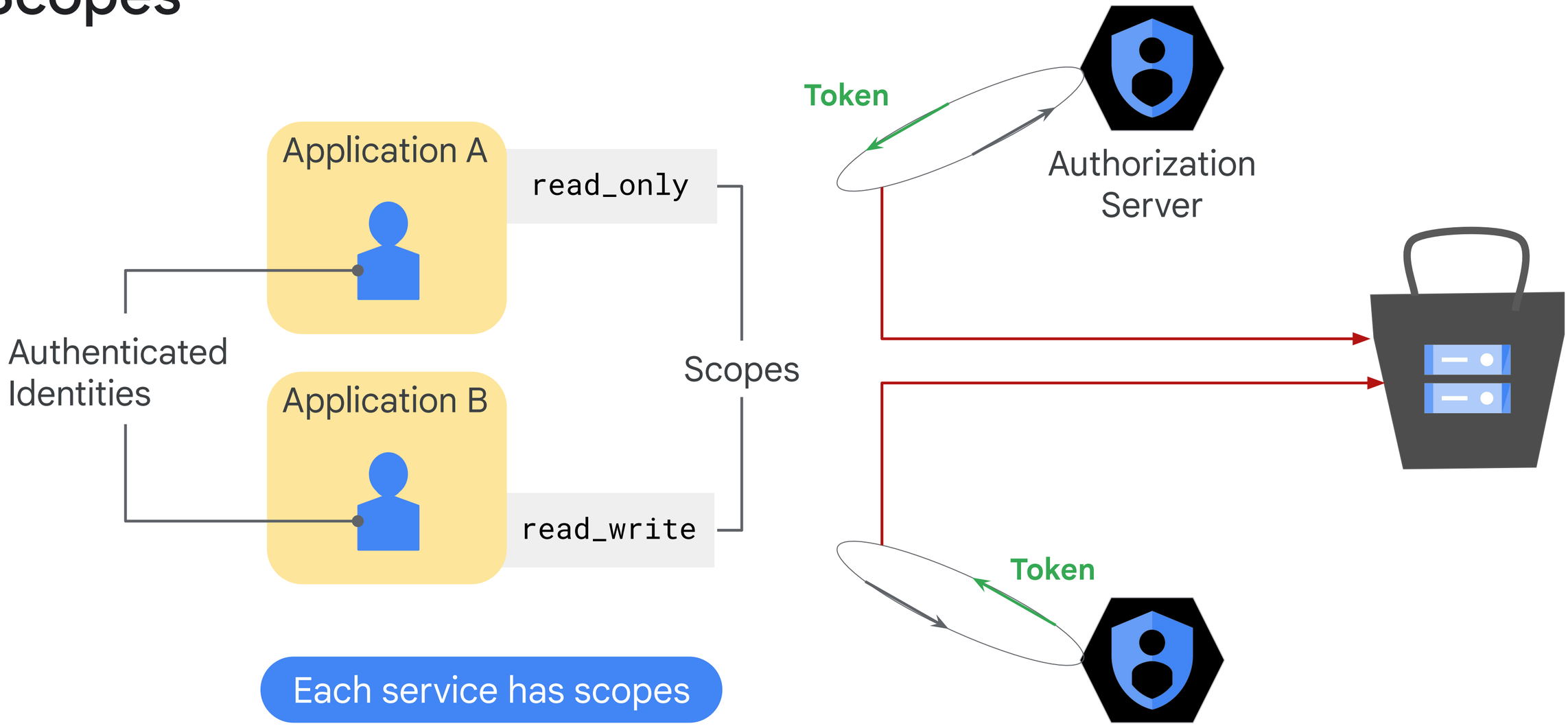
Service accounts are identified by an email address

- `123845678986-compute@project.gserviceaccount.com`
- Three types of service accounts:
  - User-created (custom)
  - Built-in
    - Compute Engine and App Engine default service accounts
  - Google APIs service account
    - Runs internal Google processes on your behalf.

Default Compute Engine service account

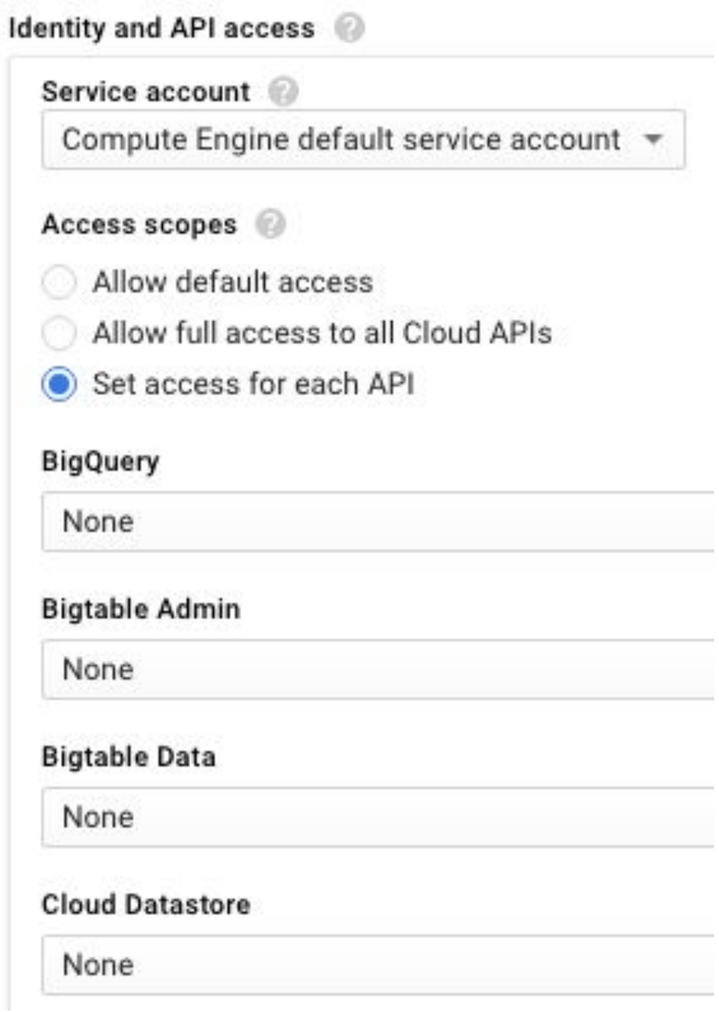
- Automatically created per project with auto-generated name and email address:
  - Name has -compute suffix `39xxxx0965-compute@developer.gserviceaccount.com`
- Automatically added as a project Editor
- By default, enabled on all instances created using `gcloud` or the Google Cloud console

Scopes



Each service has scopes

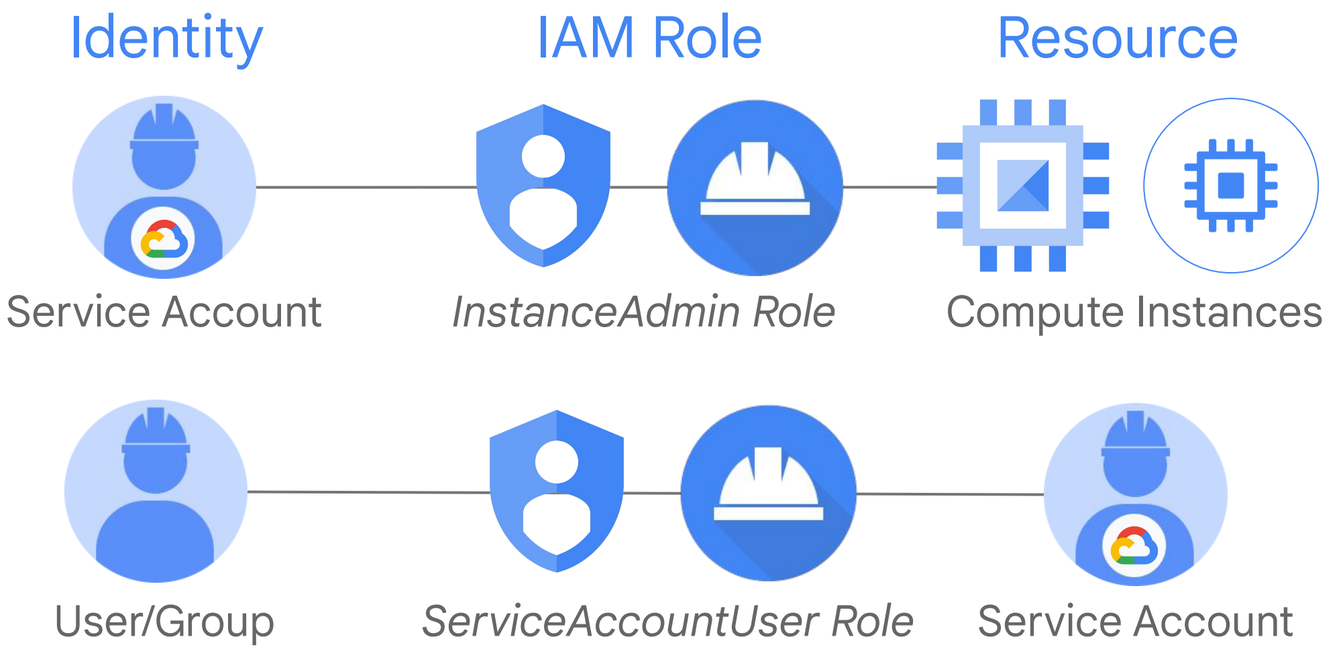
Customizing scopes for a VM



- Scopes can be changed after an instance is created.
- For user-created service accounts, use IAM roles instead.

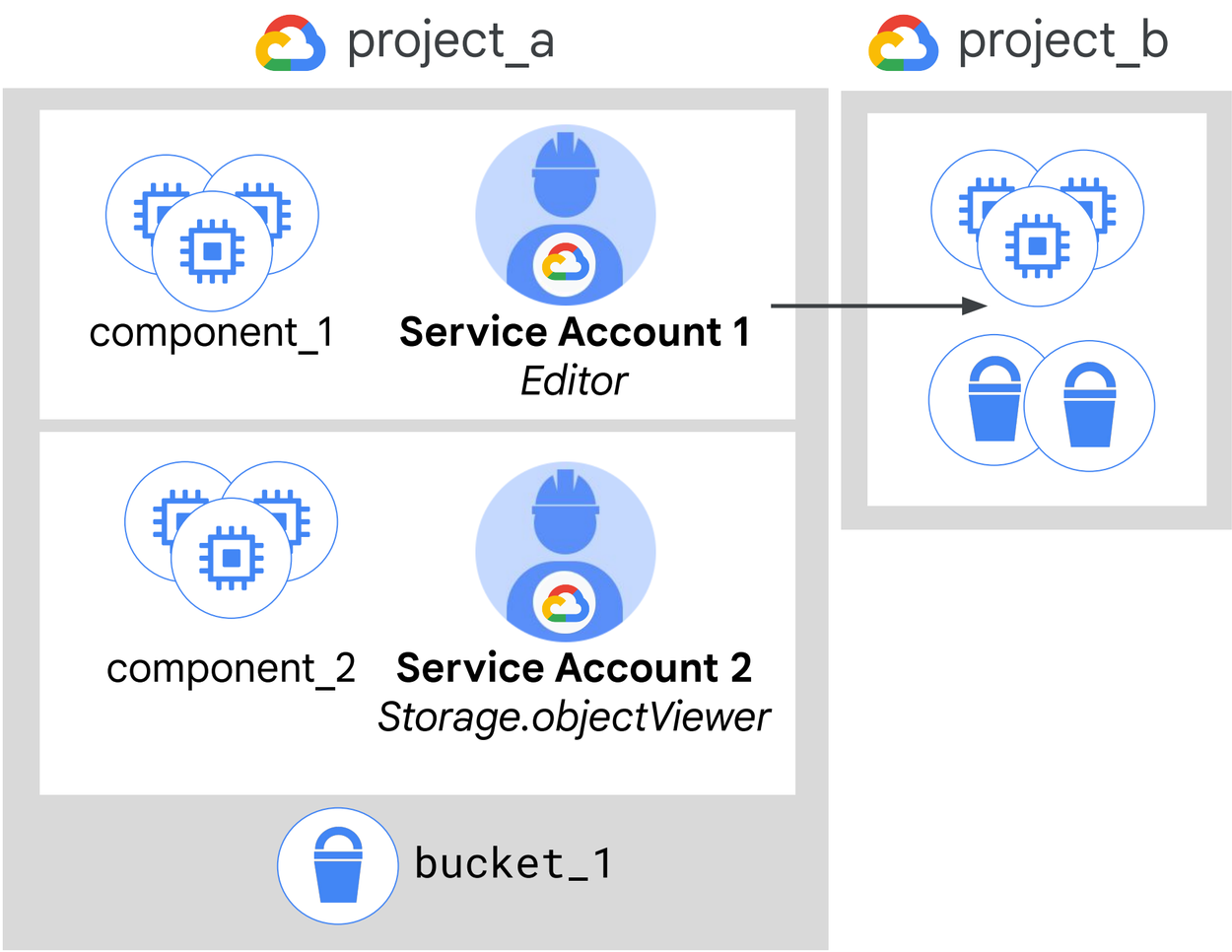
Service account permissions

- Default service accounts: basic and predefined roles
- User-created service accounts: predefined roles
- Roles for service accounts can be assigned to groups or users



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 re-created VMs.



Two types of service account keys

Google-managed service accounts

- All service accounts have Google-managed keys.
- Google stores both the public and private portion of the key.
- Each public key can be used for signing for a maximum of two weeks.
- Private keys are never directly accessible.

User-managed service accounts

- Google only stores the public portion of a user-managed key.
- Users are responsible for private key security.
- Can create up to 10 user-managed service account keys per service.
- Can be administered via the IAM API, `gcloud`, or the console.

Two types of service account keys

Google-managed service accounts

- All service accounts have Google-managed keys.
- Google stores both the public and private portion of the key.
- Each public key can be used for signing for a maximum of two weeks.
- Private keys are never directly accessible.

User-managed service accounts

- Google only stores the public portion of a user-managed key.
- Users are responsible for private key security.
- Can create up to 10 user-managed service account keys per service.
- Can be administered via the IAM API, `gcloud`, or the console.

Two types of service account keys

Google-managed service accounts

- All service accounts have Google-managed keys.
- Google stores both the public and private portion of the key.
- Each public key can be used for signing for a maximum of two weeks.
- Private keys are never directly accessible.

User-managed service accounts

- Google only stores the public portion of a user-managed key.
- Users are responsible for private key security.
- Can create up to 10 user-managed service account keys per service.
- Can be administered via the IAM API, `gcloud`, or the console.

Keeping your user-managed keys safe is vital - and is the creator's responsibility

Remember: Google does not save your user-managed private keys - if you lose them, Google cannot help you recover them.

Use the `gcloud` command-line tool to quickly list all of the keys associated with a Service Account

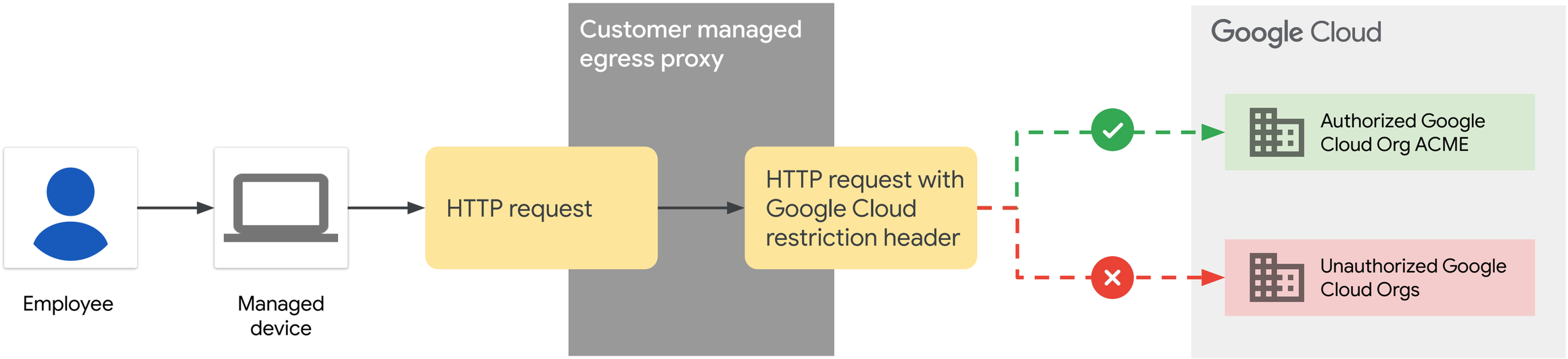
```
gcloud iam service-accounts keys list --iam-account user@email.com
```

06

Organization Restrictions

Organization restrictions let you prevent data exfiltration through phishing or insider attacks.

Organization Restrictions



07

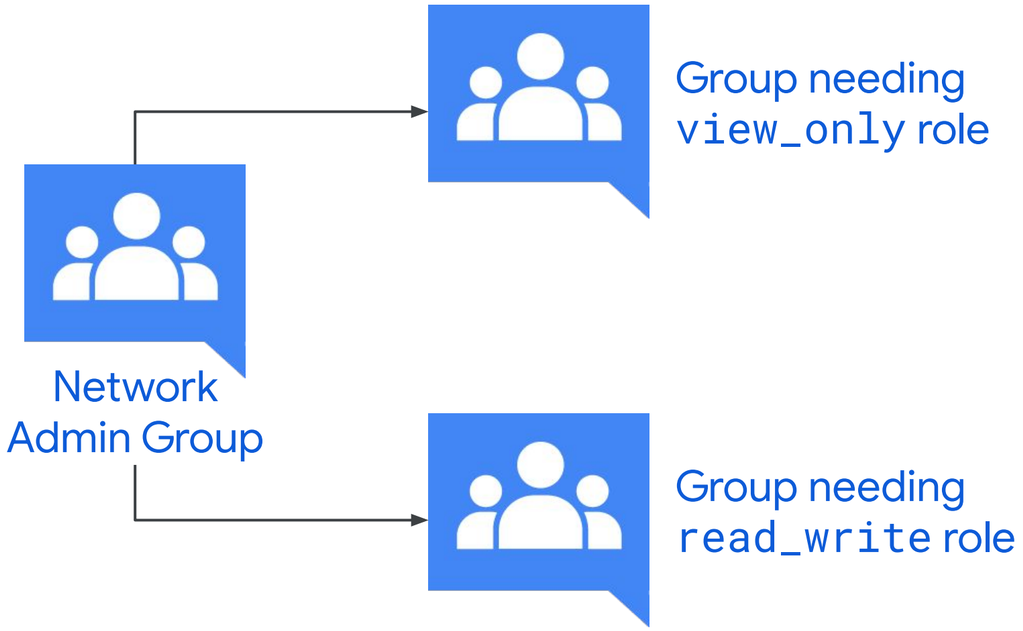
IAM Best Practices

Leverage and understand the resource hierarchy

- Use projects to group resources that share the same trust boundary.
- Check the policy granted on each resource and make sure you understand the inheritance.
- Use “principles of least privilege” when granting roles.
- Audit policies in Cloud Audit Logs: setiampolicy.
- Audit membership of groups used in policies.

Grant roles to Google groups instead of individuals

- Update group membership instead of changing IAM policy.
- Audit membership of groups used in policies.
- Control the ownership of the Google group used in IAM policies.



Service accounts

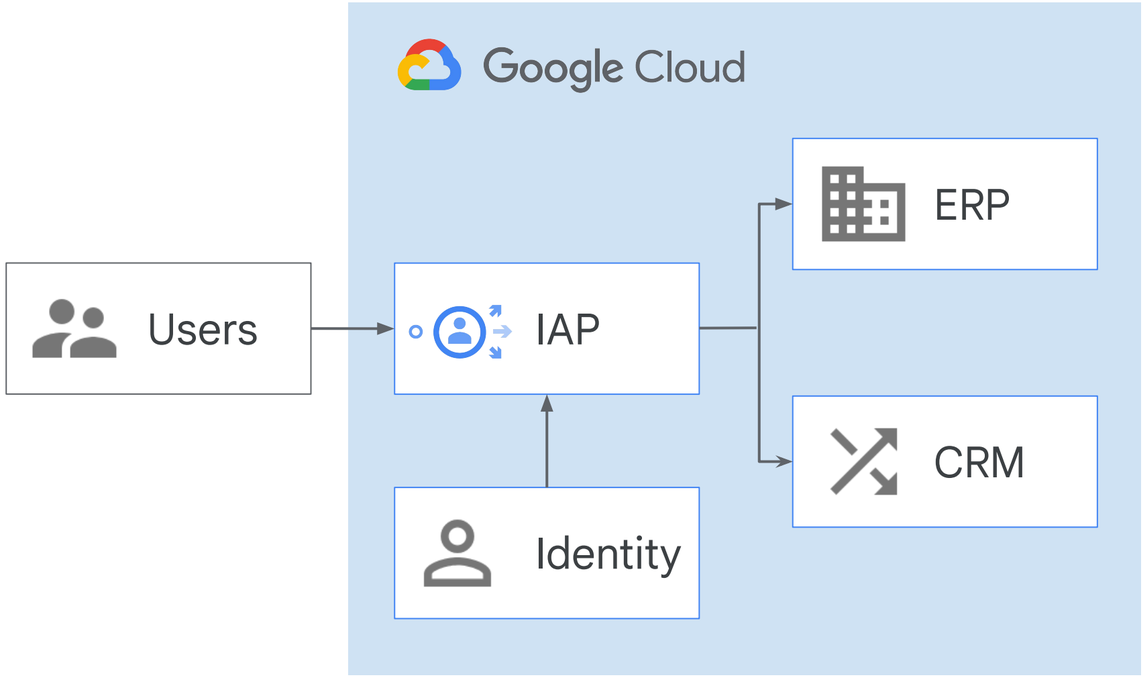
- Be very careful granting `serviceAccountUser` role.
- When you create a service account, give it a display name that clearly identifies its purpose.
- Establish a naming convention for service accounts.
- Establish key rotation policies and methods.
- Audit with `serviceAccount.keys.list()`method.

Identity-Aware Proxy (IAP)

Enforce access control policies for applications and resources:

- Identity-based access control
- Central authorization layer for applications accessed by HTTPS

IAM policy is applied after authentication.



Lab Intro

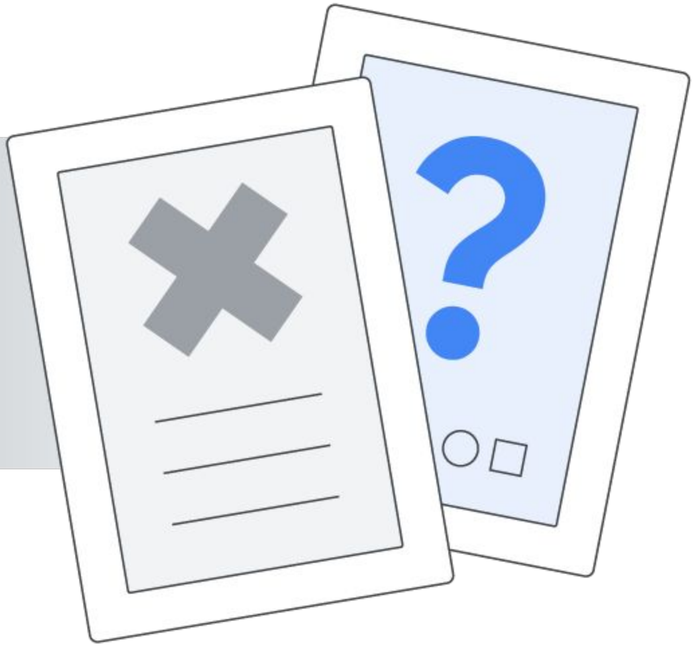
Exploring IAM

Lab objectives

01 Use IAM to implement access control

02 Restrict access to specific features or resources

03 Use the Service Account User role



Quiz

Question #1

Question

What abstraction is primarily used to administer user access in IAM?

A. Leases, an abstraction of periodic entitlements

B. Roles, an abstraction of job roles

C. Credentials, an abstraction of an authorization token

D. Privileges, an abstraction of access rights

Question #1

Answer

What abstraction is primarily used to administer user access in IAM?

A. Leases, an abstraction of periodic entitlements

B. **Roles, an abstraction of job roles**

C. Credentials, an abstraction of an authorization token

D. Privileges, an abstraction of access rights

Question #2

Question

Which of the following is not a type of IAM role?

A. Basic

B. Predefined

C. Custom

D. Advanced

Question #2

Answer

Which of the following is not a type of IAM role?

A. Basic

B. Predefined

C. Custom

D. Advanced

Question #3

Question

Which of the following is not a type of IAM member?

A. Google Account

B. Service Account

C. Google Group

D. Organization Account

E. Cloud Identity domain

F. Google Workspace domain

Question #3

Answer

Which of the following is not a type of IAM member?

A. Google Account

B. Service Account

C. Google Group

D. **Organization Account**

E. Cloud Identity domain

F. Google Workspace domain

Review: Identity and Access Management