The information in this presentation is classified:

Google confidential & proprietary

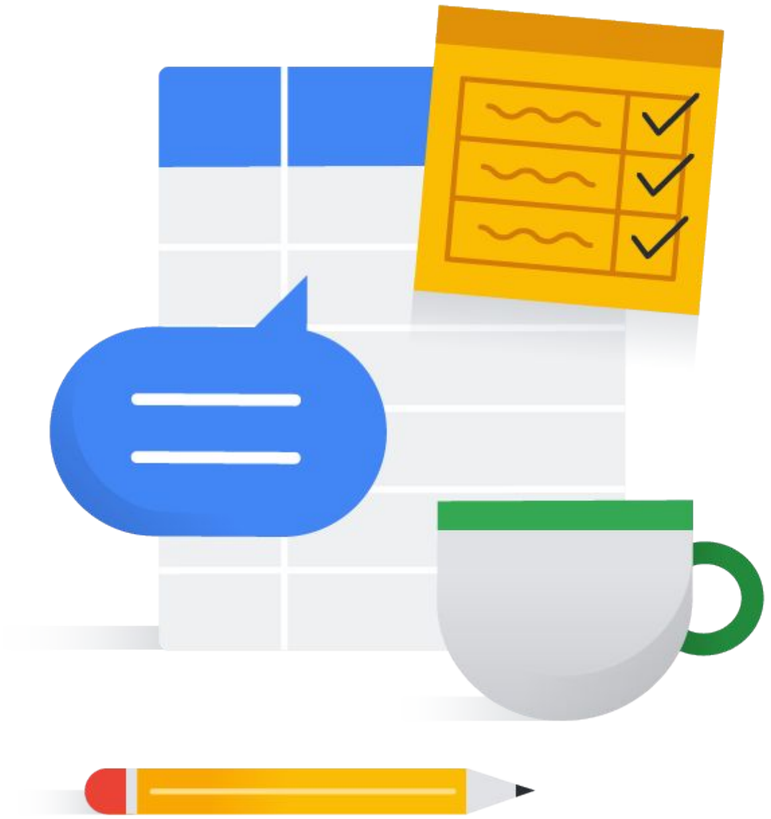
⚠️ This presentation is shared with you under NDA.

- Do **not** record or take screenshots of this presentation.
- Do **not** share or otherwise distribute the information in this presentation with anyone **inside** or **outside** of your organization.

Thank you!

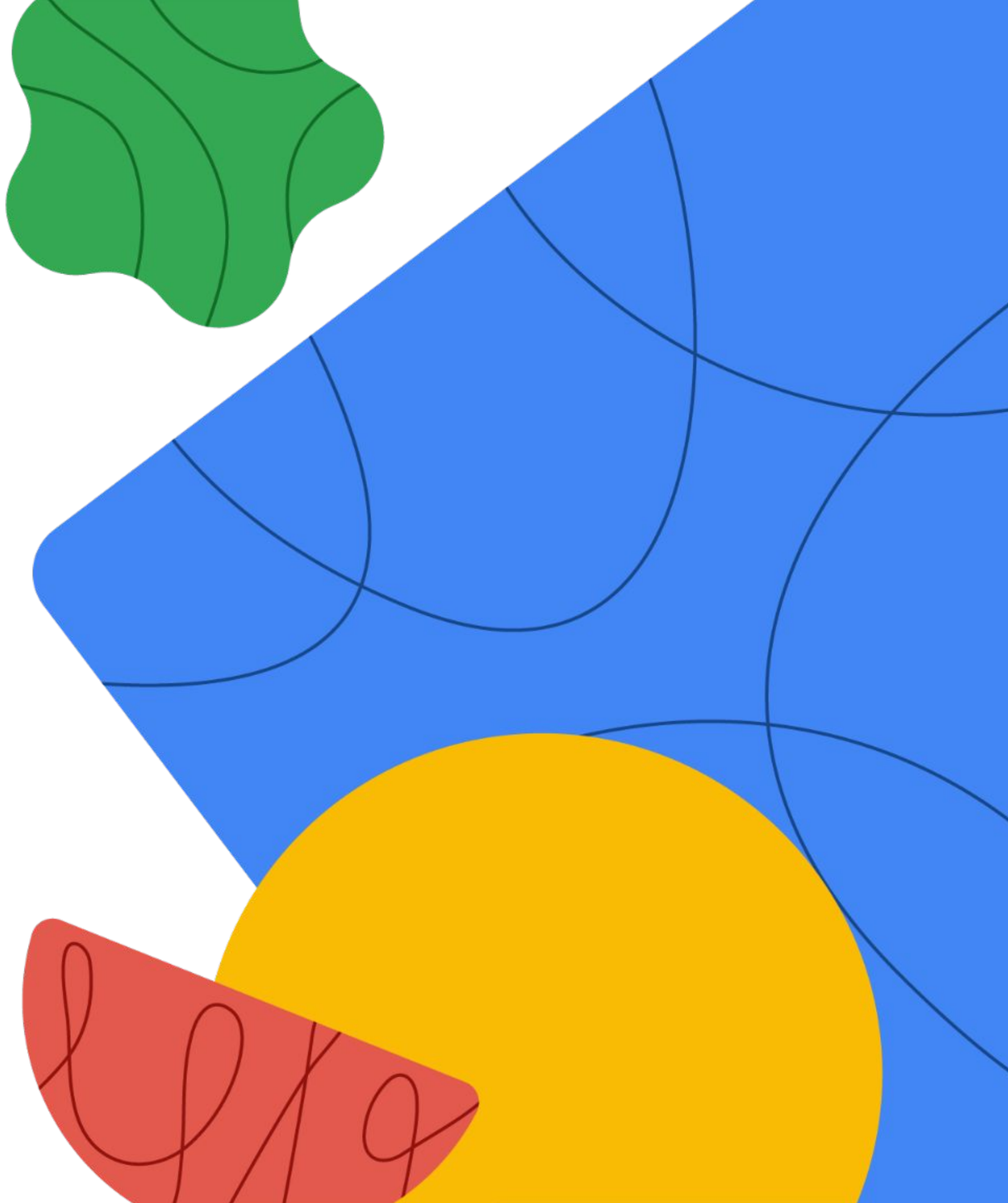
Program issues or concerns?

- Problems with **accessing** Cloud Skills Boost for Partners
  - cloud-partner-training@google.com
- Problems with **a lab** (locked out, etc.)
  - support@qwiklabs.com



Google Cloud

Identity and IAM



Our agenda

01 Cloud Identity

02 Google Cloud Directory Sync

03 Google authentication versus SAML-based SSO

04 Authentication best practices

05 Identity and Access and Management (IAM)

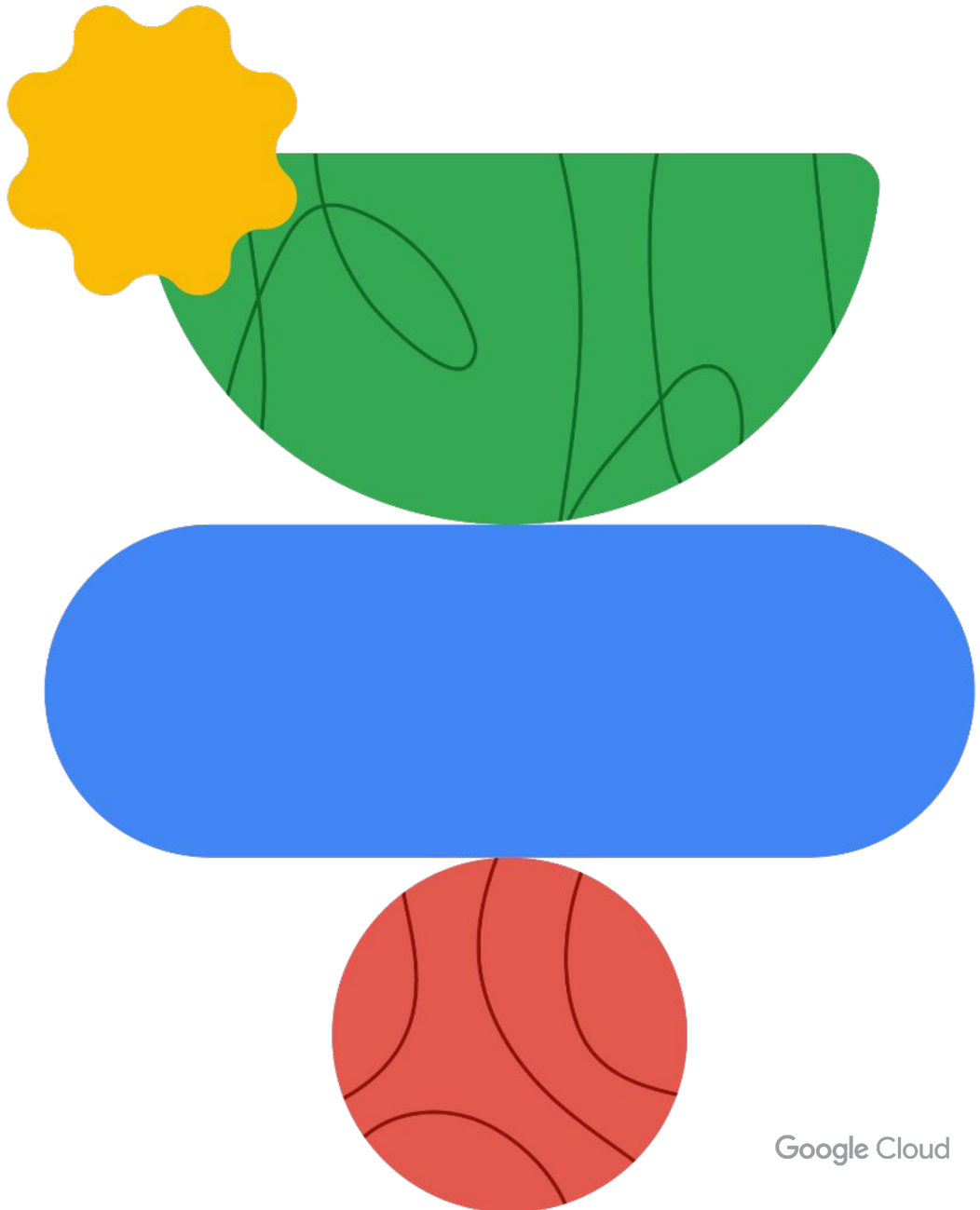
Objectives

01 Explain Cloud Identity.

02 Explain Google Cloud authentication.

02 Discuss access control using Identity and Access Management (IAM).

Cloud Identity



High level overview - service comparison

Service	What it is	Use cases
Cloud Identity	An identity provider (IdP) service that lets you create, manage, and delete identities for authentication purpose. It supports single sign-on, multi factor authentication and mobile device management.	• Cloud-based directory • Authentication (e.g. SSO) & Authorization • User Lifecycle Management • MFA & Endpoint management
Google Cloud Directory Sync	Synchronize the data in your Google Account with your Microsoft Active Directory or LDAP server.	• Syncs users, aliases, groups, and other data with your Google Account from LDAP of Microsoft AD
Managed Microsoft Active Directory	Extend Microsoft Active Directory on-premises service and configuration to your Google Cloud deployments	• Manage authentication and authorization for AD-dependent apps and servers • Automate AD server maintenance and security configuration
Identity Platform	Add identity and access management functionality to your applications	Customer identity and access management (CIAM) system used for: • Multi-tenant SaaS applications • Mobile and web apps • Games, APIs and more

Cloud Identity

Cloud Identity:

- is an Identity as a Services (IDaaS) solution.
- centrally manages users, groups, and domain security.
- is tied to a unique DNS domain that is enabled for receiving email.

Cloud Identity

‘Single pane of glass’

- User lifecycle management
- Account security
- Single sign-on
- Cloud directory
- Device management
- Reporting and analytics
- App management
- Extensible through APIs

Cloud Identity editions

Enable products

Cloud Identity Free

Manage more users and applications to secure your data in the cloud.

Cloud Identity Premium

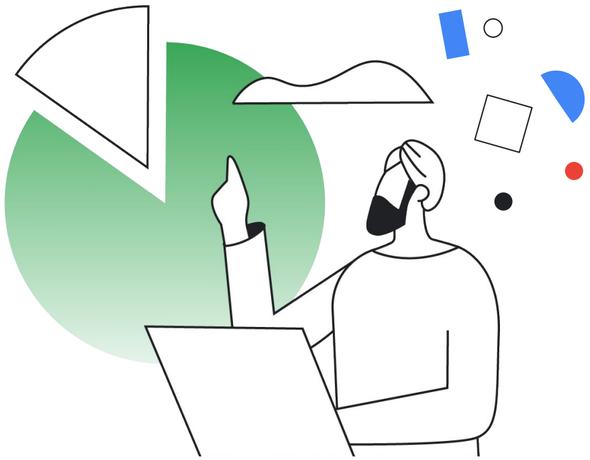
Manage users, devices, and applications to secure your data in the cloud.

Compare Cloud Identity features and editions

https://support.google.com/cloudidentity/answer/7431902

Google Admin Console

- admin.google.com
- Centralized console to manage users, groups, and security settings
- Cloud Identity allows free accounts to be created for each user

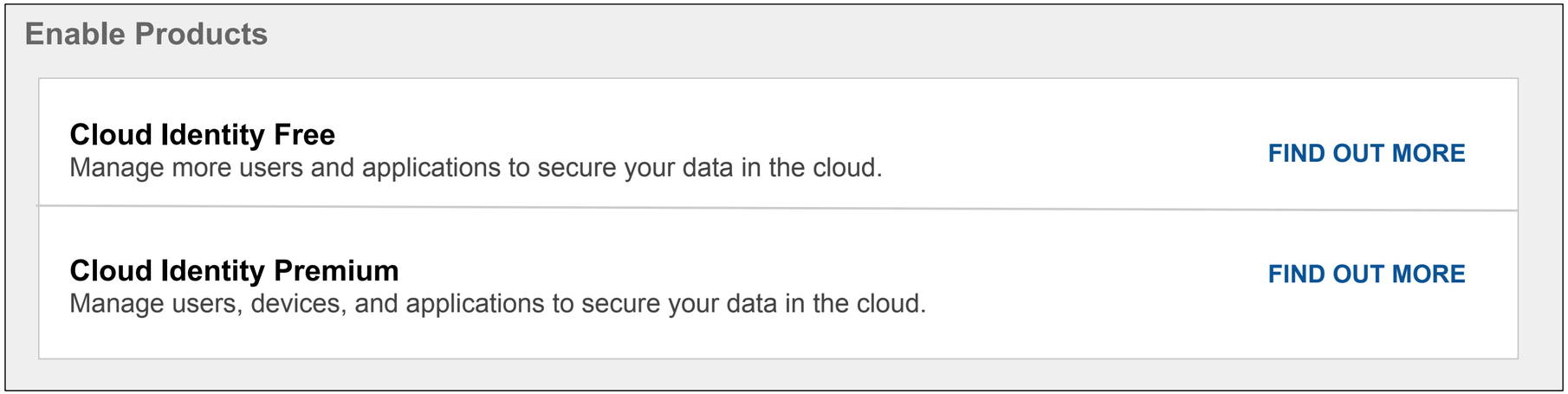


Support for Cloud Identity

- Cloud Identity can be used as a standalone service.
- Cloud Identity can be combined with your Google Workspace services.

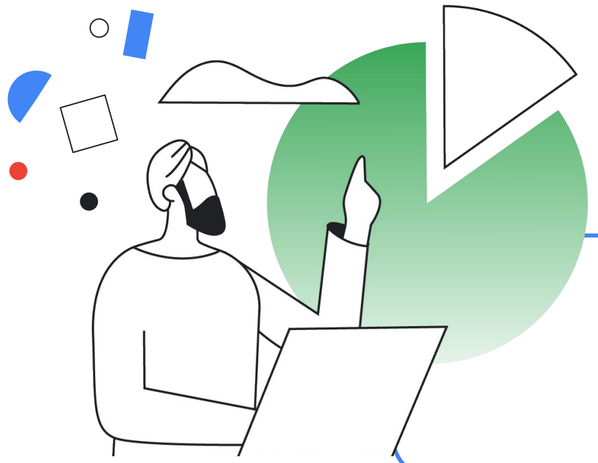
If you are a Google Workspace admin

Sign up for Cloud Identity from the Billing section of the Google Admin console.



Create free Cloud Identity accounts for users who don’t need Google Workspace.

If you are not using Google Workspace



Register your domain as a Cloud Identity domain:

gsuite.google.com/signup/gcpidentity

Then use the Google Admin console to configure users and groups.

Org Admin

Role assignment

Organization Administrator IAM role must be assigned to a user or group.

Resource control

Organization administrators have central control of all resources.

If you are a Google Cloud Admin

Cloud IAM allows you to assign roles to a variety of users and groups, including:

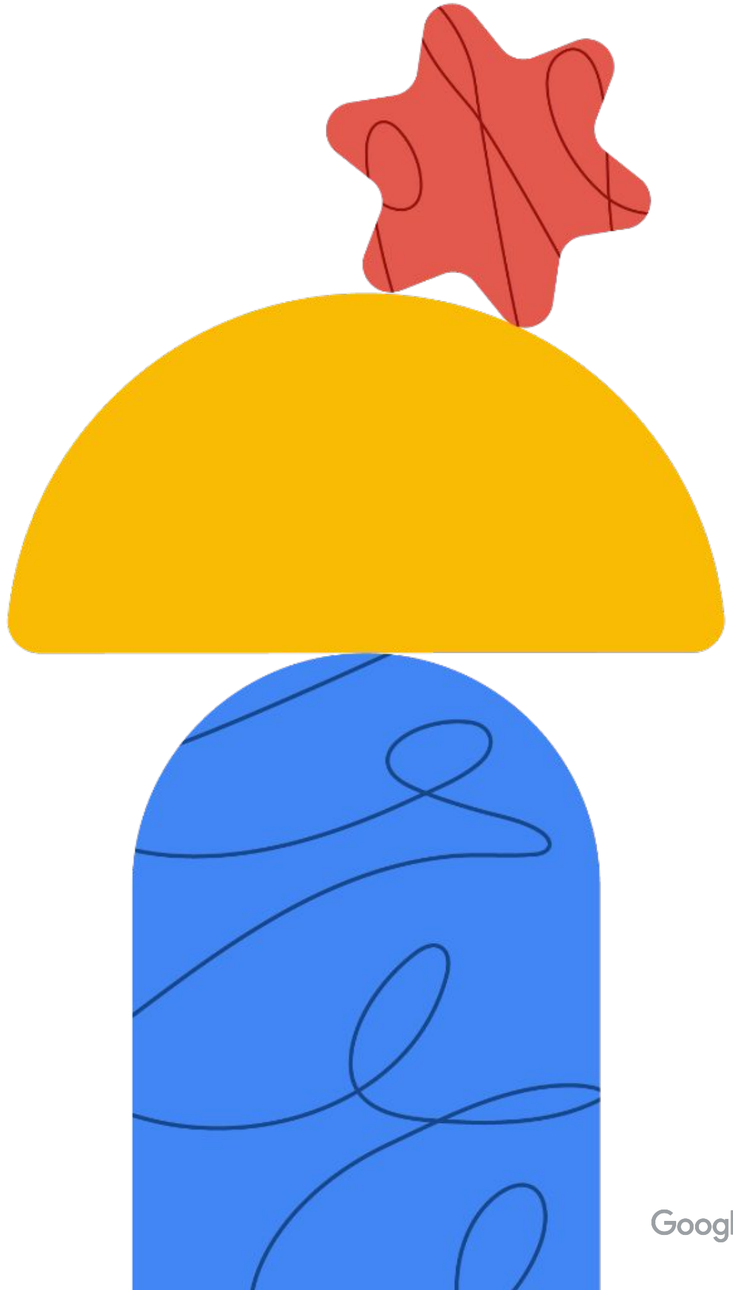
User or group

Any Google Workspace or Cloud Identity user or group

Accounts or group

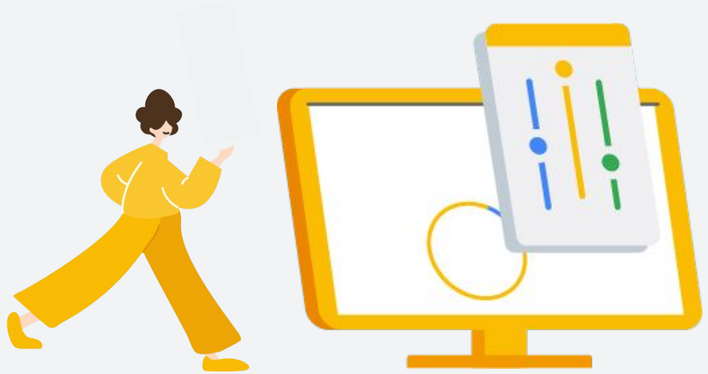
Any Google accounts or group (@gmail, @google)

Google Cloud Directory Sync



Provisioning users

The Admin console allows admins to provision users manually



Different corporate directory

Microsoft Active Directory or LDAP

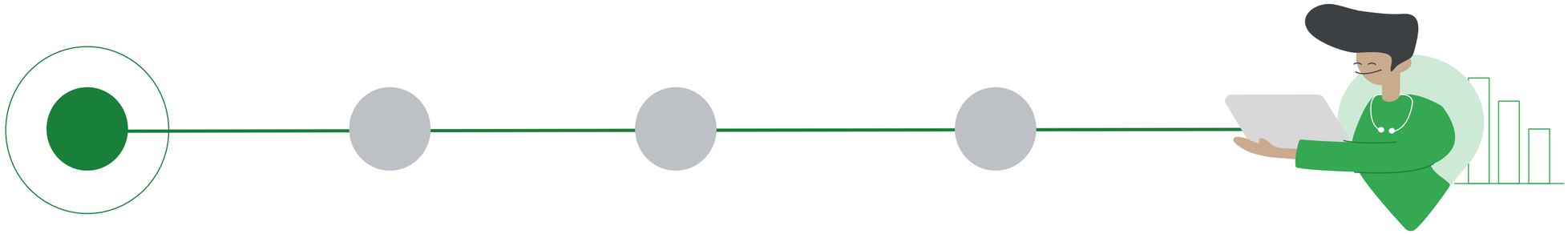
Users and groups in your existing directory service

Google Cloud Directory Sync

Scheduled one-way sync

Users and groups in your Cloud Identity domain

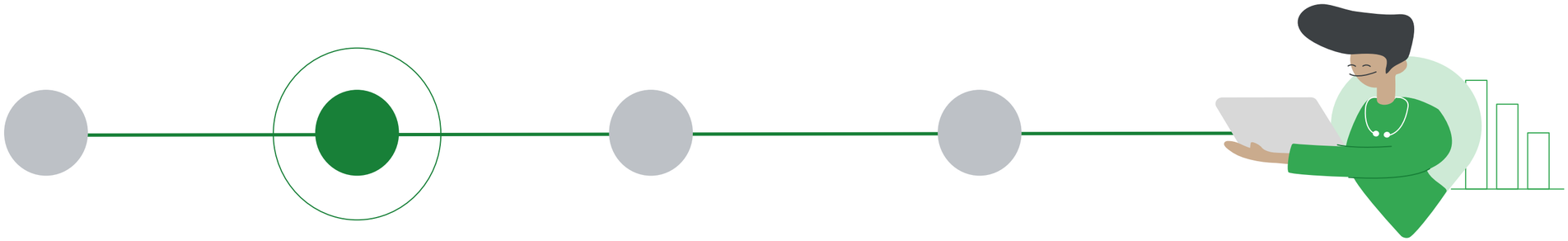
Directory Sync



The Directory Sync process

- Data is exported from your LDAP server or Active Directory.

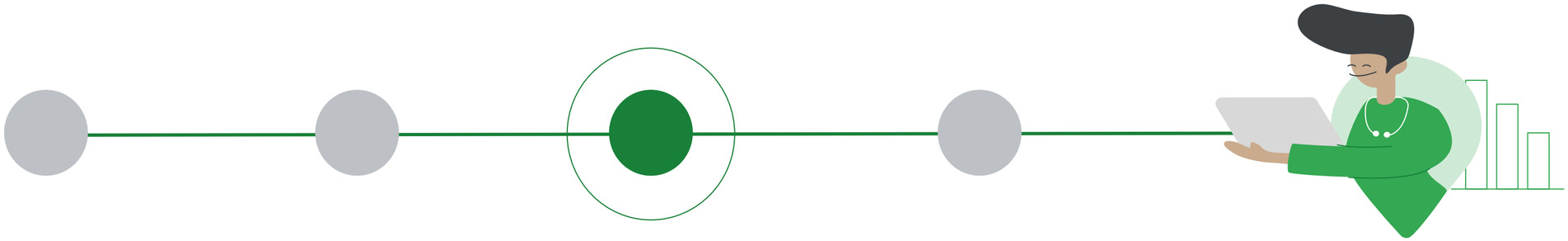
Directory Sync



The Directory Sync process

- Data is exported from your LDAP server or Active Directory.
- Directory Sync connects to the Google domain and generates a list of Google uses, groups, and shared contacts that you specify.

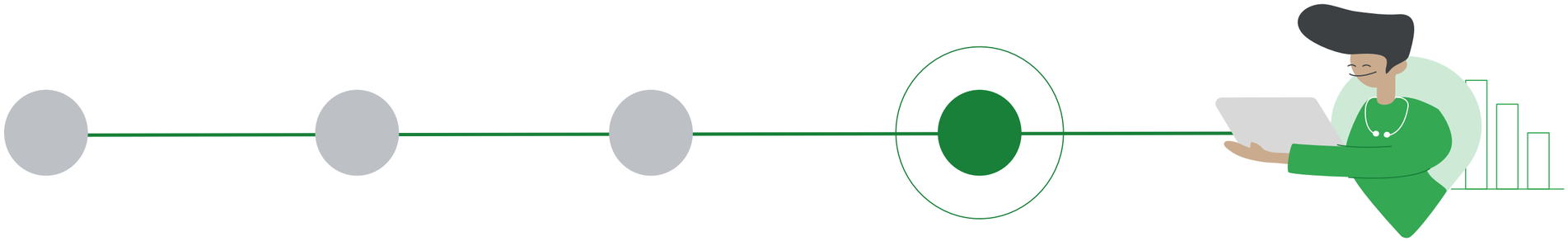
Directory Sync



The Directory Sync process

- Data is exported from your LDAP server or Active Directory.
- Directory Sync connects to the Google domain and generates a list of Google uses, groups, and shared contacts that you specify.
- Directory Sync compares these lists and updates your Google domain to match the data.

Directory Sync



The Directory Sync process

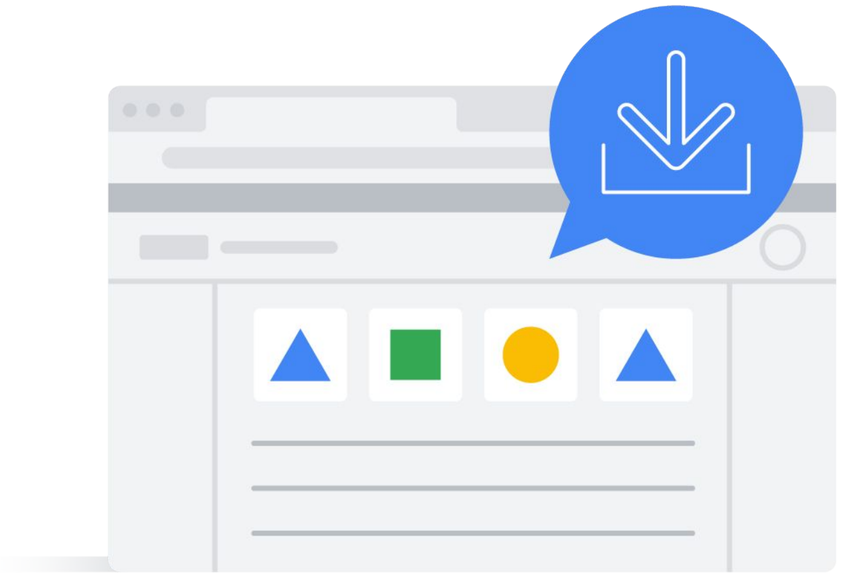
- Data is exported from your LDAP server or Active Directory.
- Directory Sync connects to the Google domain and generates a list of Google uses, groups, and shared contacts that you specify.
- Directory Sync compares these lists and updates your Google domain to match the data.
- When the synchronization is complete, a report is emailed.

One-way synchronization

One-way synchronization; the data in your directory server is never modified or compromised.

Directory Sync runs within the server environment

- Directory Sync operates as a server-based utility, eliminating external access requirements for Active Directory or LDAP servers.
- This ensures sensitive directory data remains within the organization's IT perimeter.



Directory Sync auto-provisioning and deprovisioning

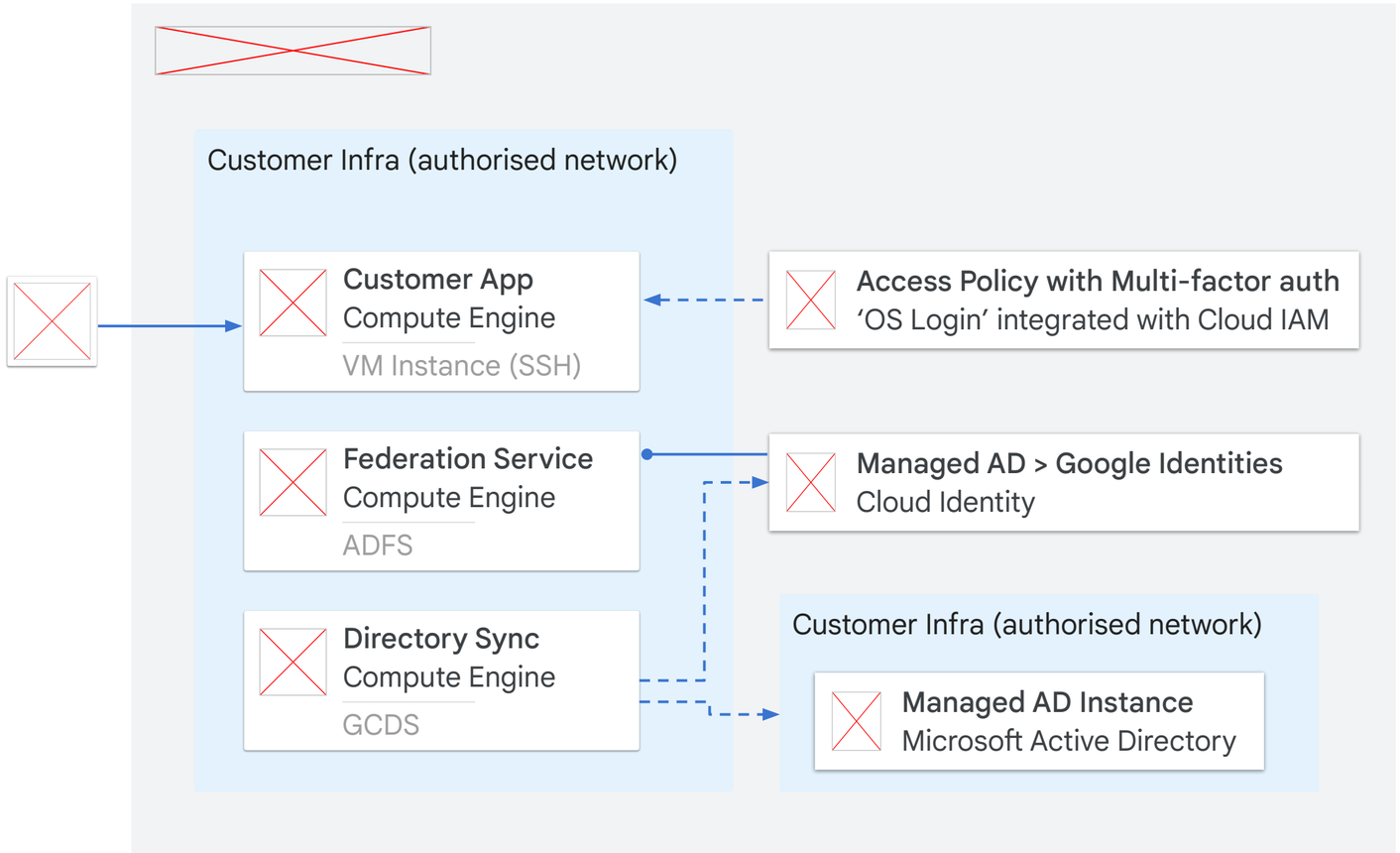
- Directory Sync auto-provisioning and deprovisioning features reduce security risks.
- They remove a user's account and deprovision it from all cloud apps once the user is removed from your directory.
- This eliminates the need for a manual process, reducing operational overhead and security risks.

Managed Microsoft AD

- Managed Microsoft AD allows you to manage cloud-based, AD-dependent workloads.
- Managed Service for Microsoft Active Directory (Managed Microsoft AD):
  - Runs actual Microsoft AD controllers
  - Is virtually maintenance-free
  - Supports both hybrid cloud and standalone cloud domains

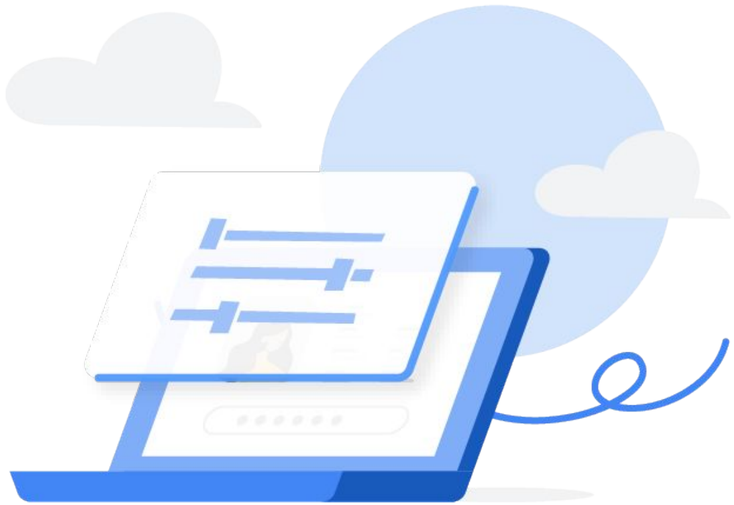
Architecture

That uses Managed Microsoft AD



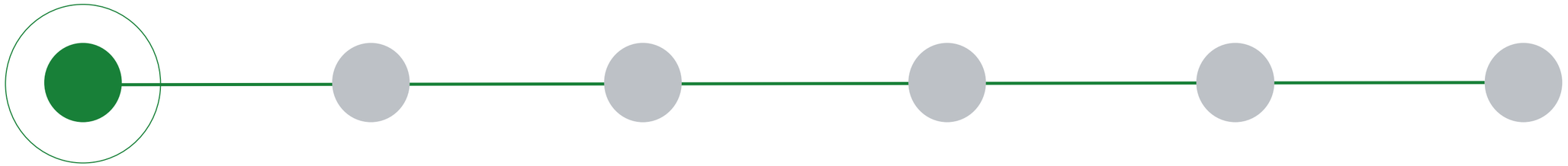
Managed Microsoft AD features

- An actual AD domain
- Familiar tools, such as Group Policy and RSAT
- Highly available configurations
- Hardened servers with snapshots and automated patching
- Flexible, multi-regional deployments



Managed Microsoft AD features

Creating the correct architecture for a domain



Security Zones and Trust Boundaries in Microsoft Active Directory

- In on-premises Active Directory environments, networks are segmented into security zones to establish trust boundaries and contain the impact of attacks.
- All machines within a compromised security zone are considered compromised.

Managed Microsoft AD features

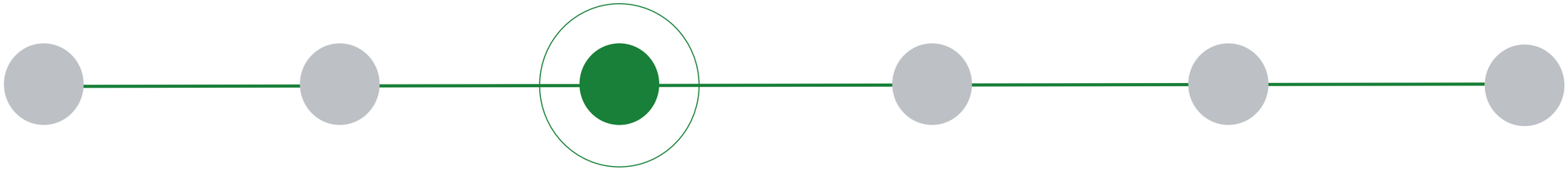
Creating the correct architecture for a domain

Extending Active Directory to Google Cloud

- When deploying Active Directory to Google Cloud, organizations must choose between extending an existing on-premises security zone or creating new security zones for cloud resources.
- The Zero Trust model, where each machine has its own Security Zone, is the preferred networking model for Google Cloud.

Managed Microsoft AD features

Creating the correct architecture for a domain

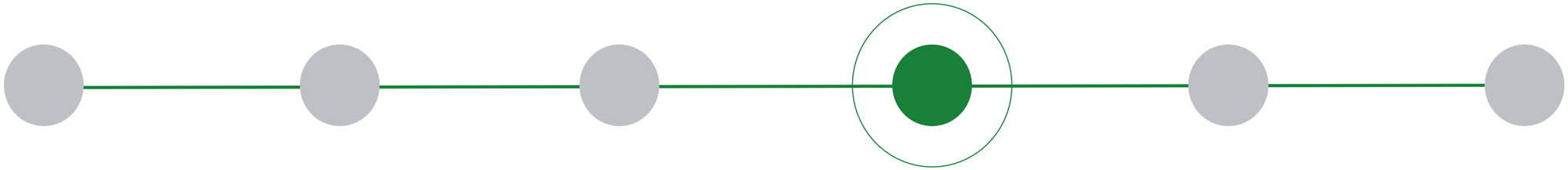


Categorizing Interaction Levels

- Light Interaction: Requires minimal communication between on-premises and cloud resources (e.g., internal administrators accessing cloud servers).
- Moderate Interaction: Involves authentication and communication across trust boundaries (e.g., internal administrators accessing file shares or applications requiring cross-trust authentication).
- Heavy Interaction: Requires near-constant communication between on-premises and cloud resources (e.g., Virtual Desktop Infrastructure environments).

Managed Microsoft AD features

Creating the correct architecture for a domain



Recommendations based on interaction levels

- Light Interaction: Consider separate Active Directory forests without a trust relationship or with a cross-forest trust.
- Moderate Interaction: Recommended to use separate Active Directory forests with a cross-forest trust.
- Heavy Interaction: Recommended to use a single Active Directory forest shared across environments.

Managed Microsoft AD features

Creating the correct architecture for a domain

Administrative autonomy and resource availability

- Granting administrative autonomy to teams can be achieved through delegated administration or separate domains.
- The architecture of your Active Directory deployment can impact resource availability.
- Interacting with multiple domain controllers can decrease resource availability and increase the chance of outages.

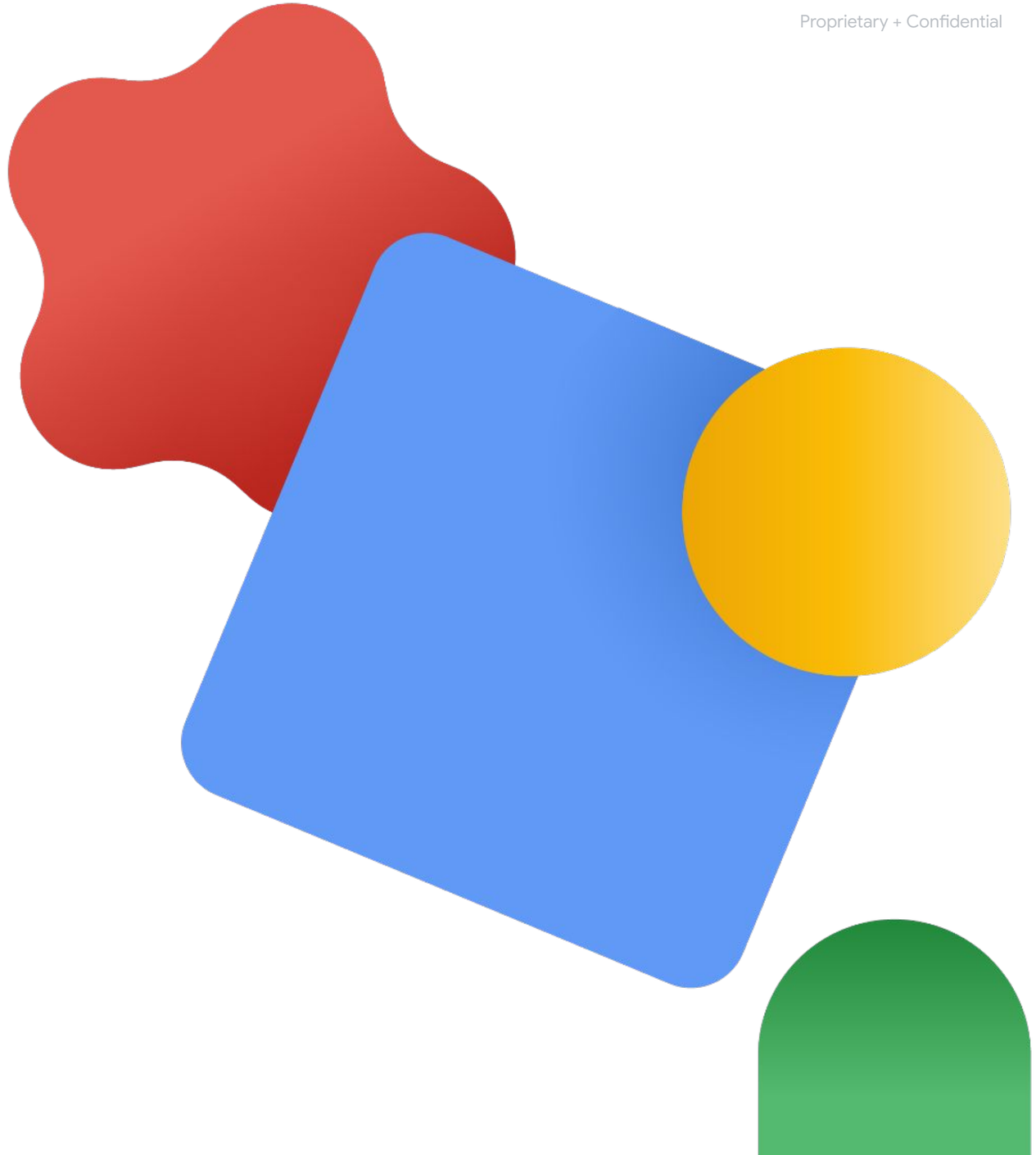
Managed Microsoft AD features

Creating the correct architecture for a domain

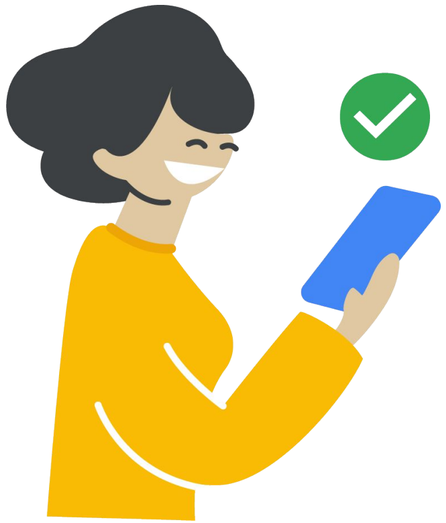
Summary

- Consider interaction levels, administrative needs, and resource availability when extending Active Directory to Google Cloud.
- Aligning your hybrid network topology with application requirements is crucial.

Google authentication versus SAML-based SSO



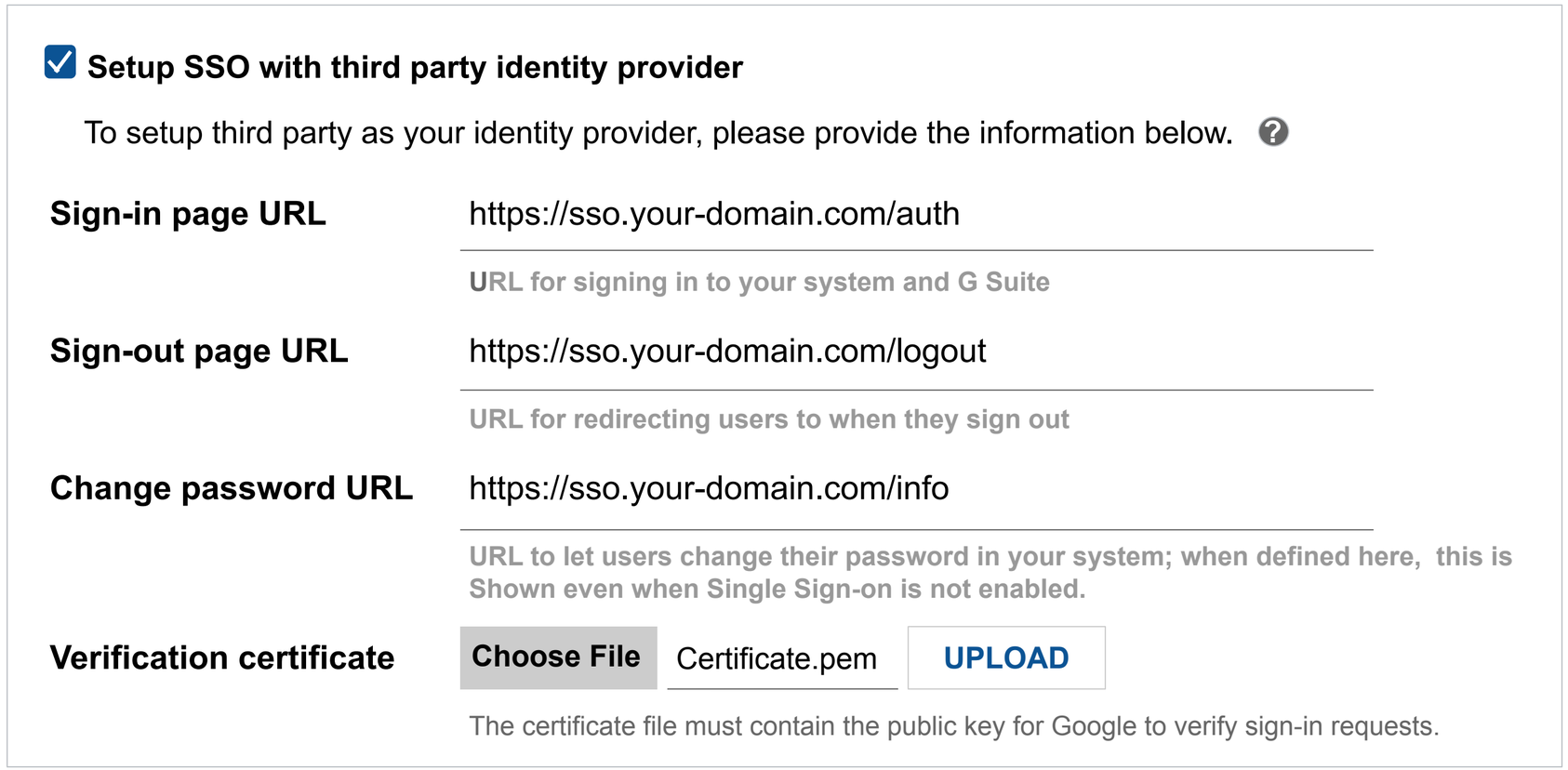
User account authentication



- Google authentication
- Single Sign-On (SSO) authentication

SSO configuration

SSO configuration requires 3 links and a certificate



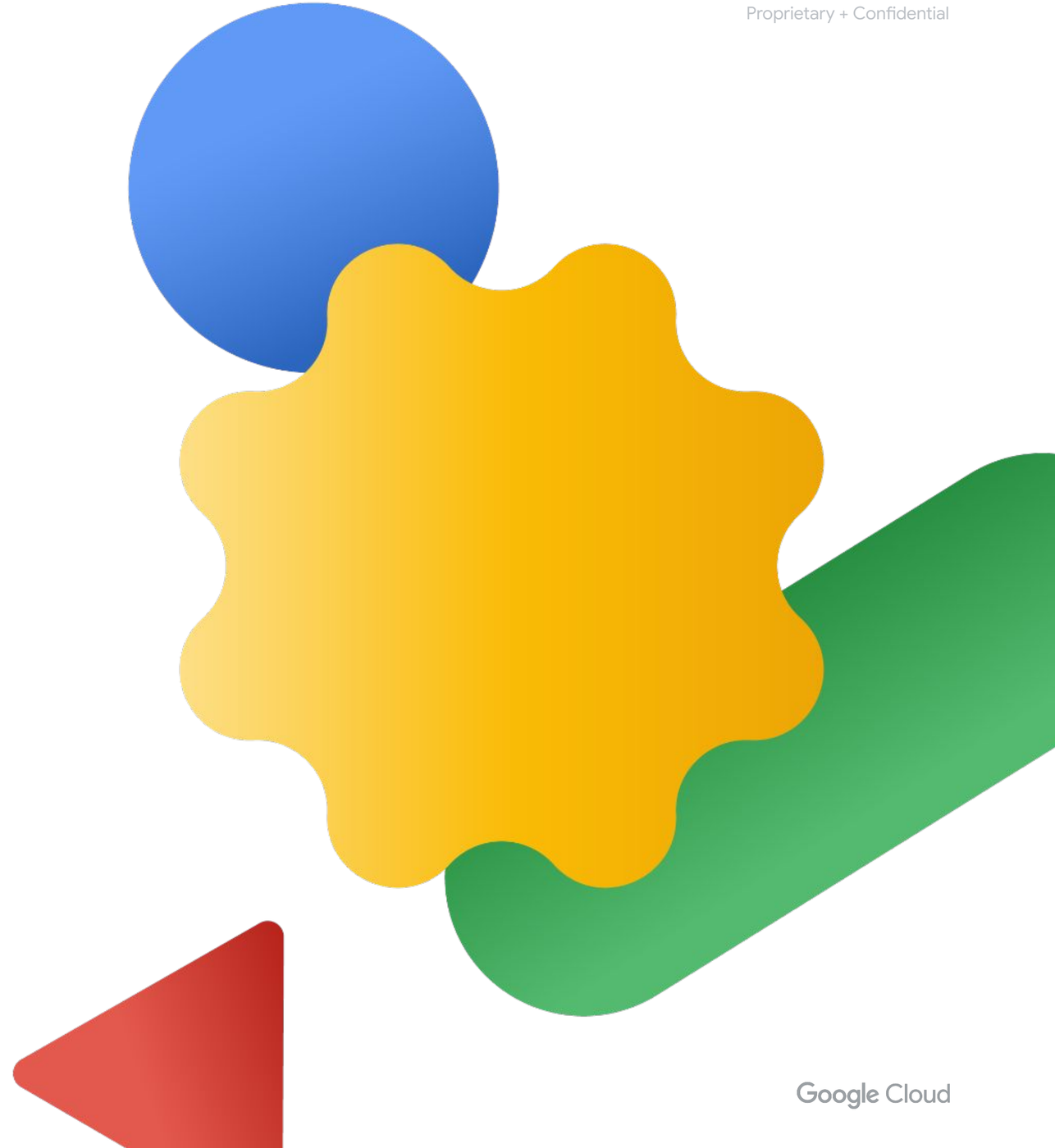
Cloud Identity for SSO

01 Use exitising credentials to authenticate.

02 Existing IdP remains the system for authentication.

03 No need to synchronize passwords to Cloud Identity.

Authentication best practices



Manage Google Cloud permissions with groups

- Avoid managing permissions for individual users in Google Cloud.
- Assign Google Cloud roles to groups instead.
- Google Workspace/Cloud Identity admins manage group
- Group administration occurs in Google Admin Console.
- Changes to group membership do not require IAM changes.
- Exception: High-risk areas may necessitate assigning roles directly to individuals.

Number of Org admins

Redundancy

For redundancy, organizations should have at least two Organization admins in case one admin is unavailable or an account is lost.

Three admins

However, organizations should add no more than three admins.

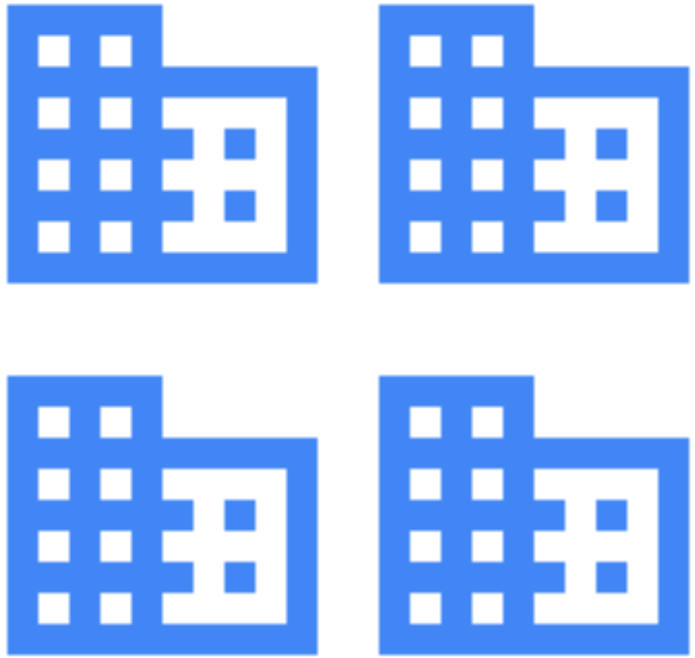
Limit permissions

1. Existing users are granted Project Creator and Billing Account Creator roles.

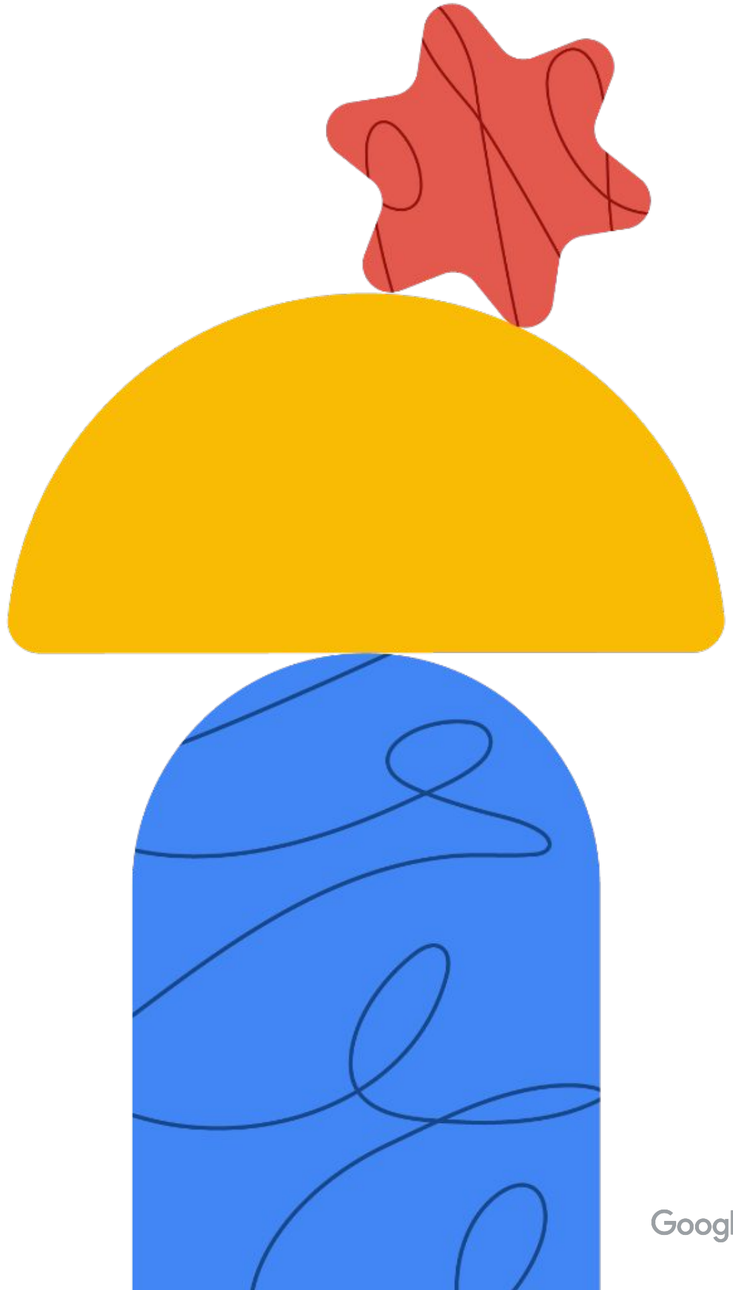
2. Remove these permissions to start locking down access at a finer granularity.

Multiple domains

- Multiple domains can be associated with your organization's account.
- The first domain name becomes the primary domain.
- You must own and verify each additional domain.
- You can add up to 600 domains to your organization's Google account.



Identity and Access Management (IAM)



Identity and Access Management

01 Resource manager

02 IAM roles

03 IAM policies

04 Workload identity federation

05 Policy intelligence

06 IAM troubleshooter

07 IAM recommender

08 IAM audit logs

09 IAM best practices

Identity and Access Management

01 Resource manager

02 IAM roles

03 IAM policies

04 Workload identity federation

05 Policy intelligence

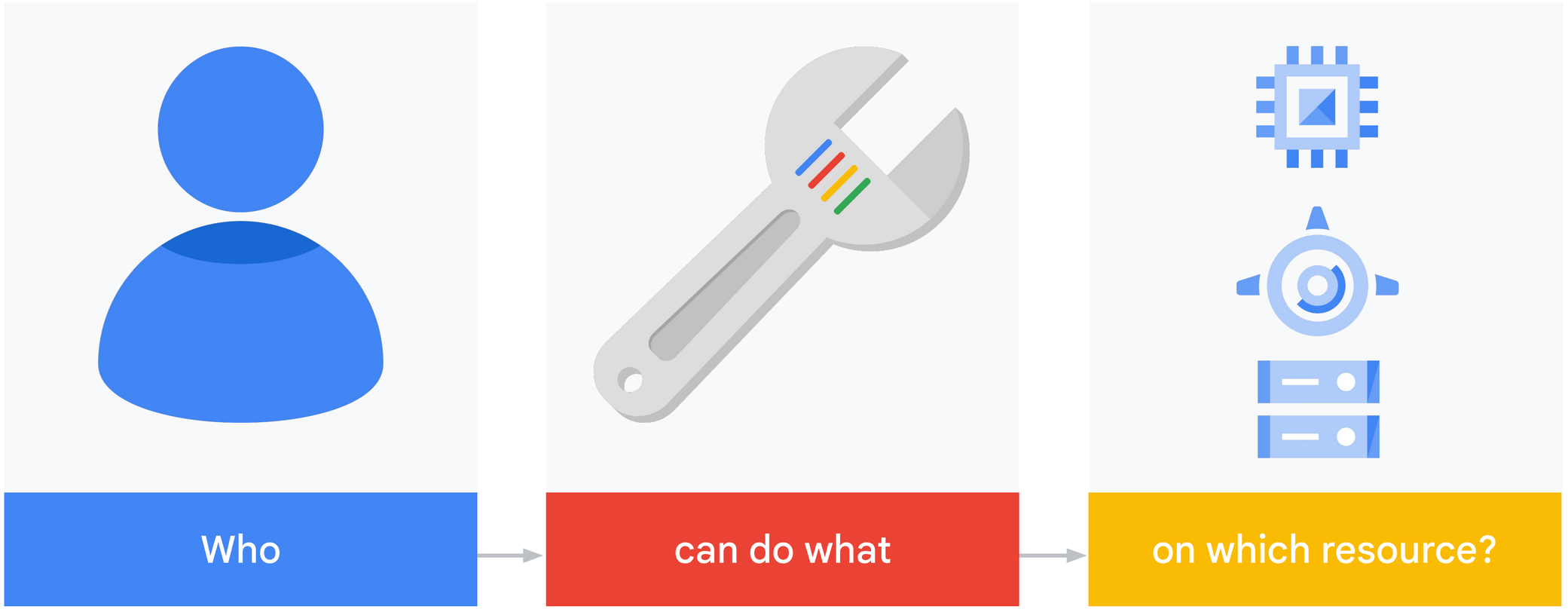
06 IAM troubleshooter

07 IAM recommender

08 IAM audit logs

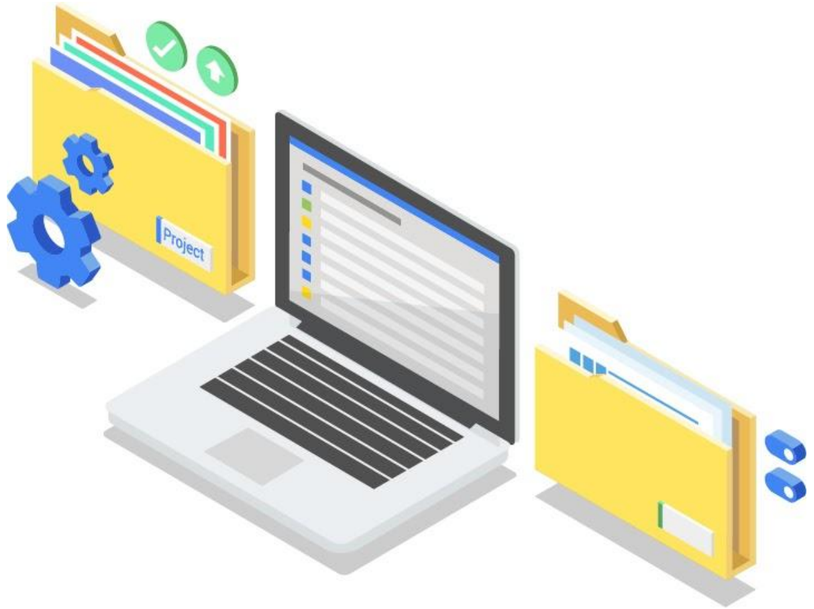
09 IAM best practices

Identity and Access Management



Resource Manager

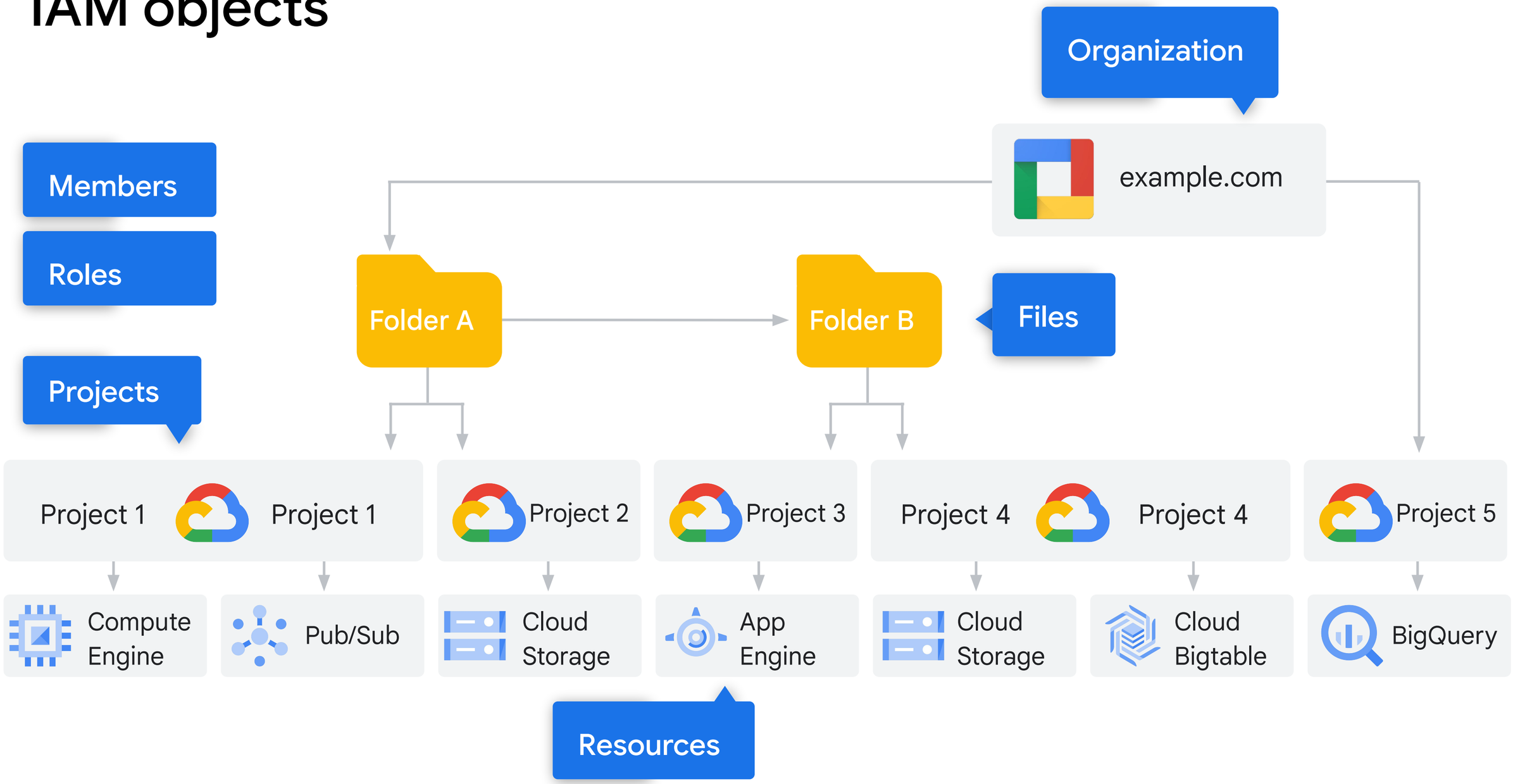
- Resources in Google Cloud are hierarchically managed by organization, folders, and projects.
- Resources Manager enables you to programmatically manage these resource containers.



Google Cloud objects

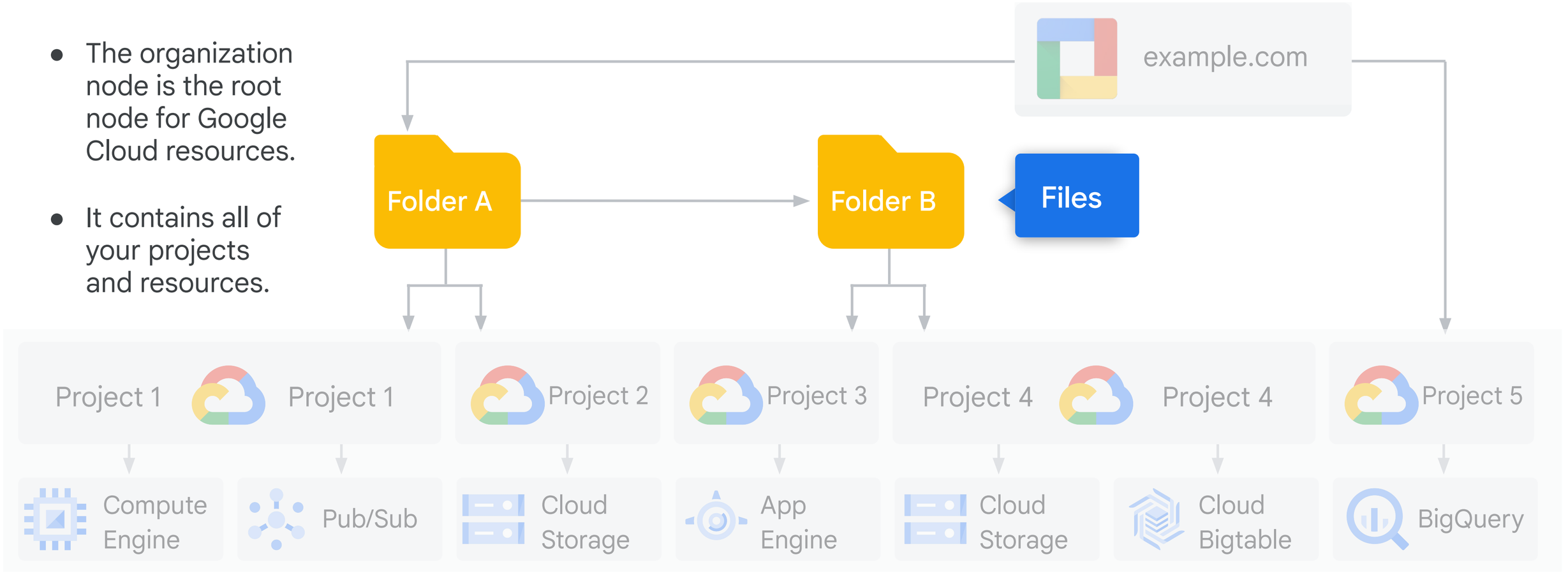
- Objects are the various resources members can access and use on Google Cloud.
- Objects hold data and applications, and also help to organize it and secure it.

IAM objects


Organization
example.com
Members
Roles
Projects
Folder A
Folder B
Files
Project 1
Project 1
Project 2
Project 3
Project 4
Project 4
Project 5
Compute Engine
Pub/Sub
Cloud Storage
App Engine
Cloud Storage
Cloud Bigtable
BigQuery
Resources

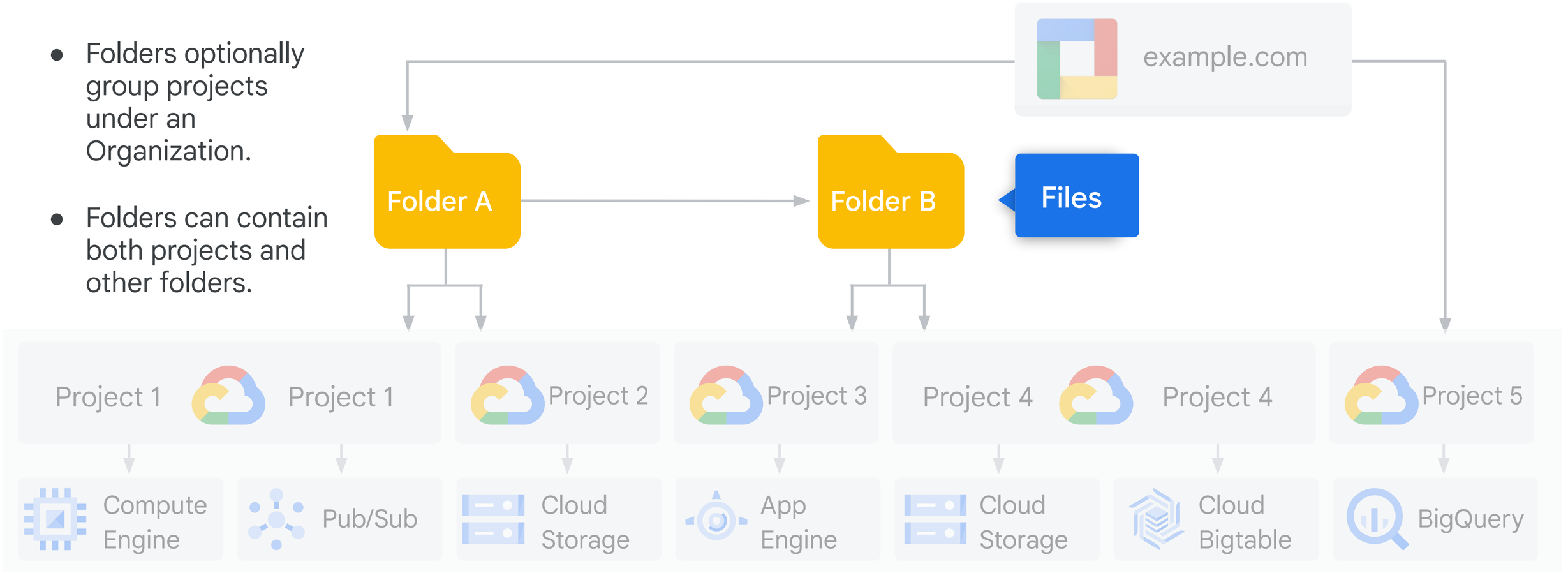
Organization node

- The organization node is the root node for Google Cloud resources.
- It contains all of your projects and resources.



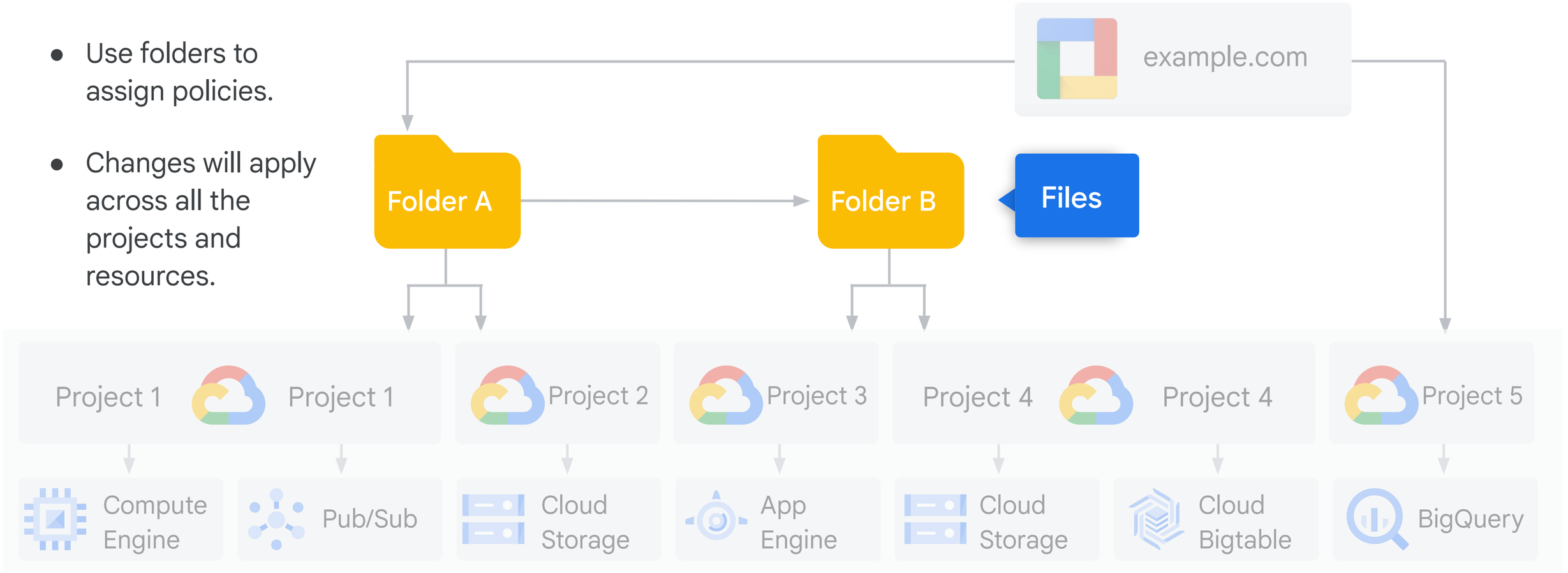
Folders offer flexible management

- Folders optionally group projects under an Organization.
- Folders can contain both projects and other folders.



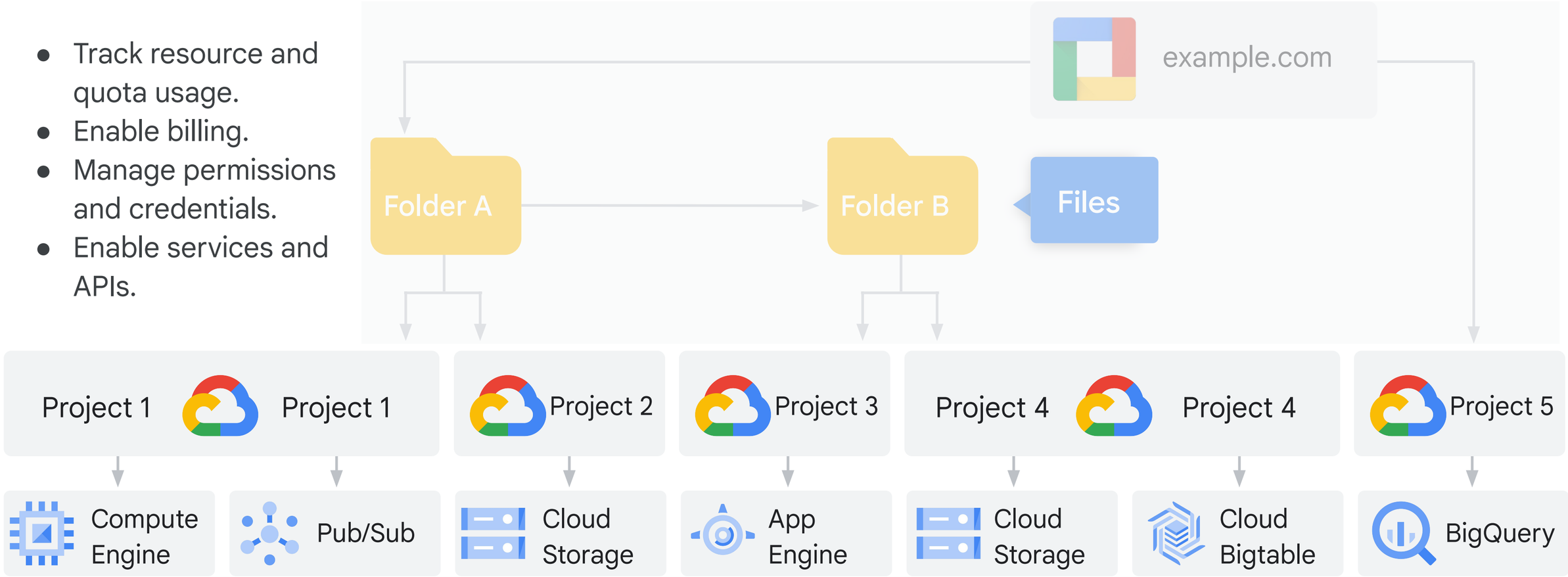
Folders offer flexible management

- Use folders to assign policies.
- Changes will apply across all the projects and resources.



Folders offer flexible management

- Track resource and quota usage.
- Enable billing.
- Manage permissions and credentials.
- Enable services and APIs.



Members

Can be any Google Workspace, or Cloud Identity user or group

Gmail accounts and Google Groups

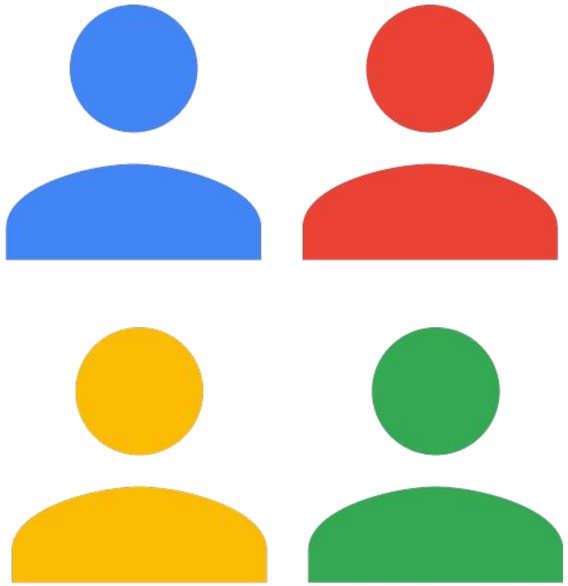
Users and groups in your Google Workspace domain

Users and groups in your Cloud Identity domain

Note: Google Cloud does not create or manage users or groups.

Member roles are collections of permissions

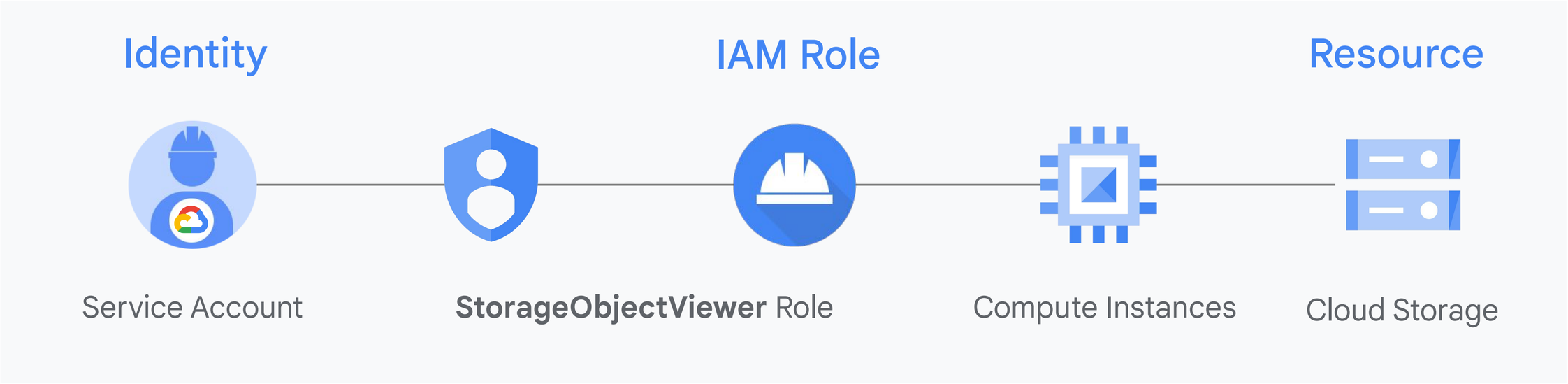
- Permissions are given to members by granting roles.
- Roles define which permissions are granted.
- Google Cloud provides predefined roles and also the ability to create custom roles.



Service accounts

Service accounts control server-to-server interactions:

- Used to authenticate from one service to another
- Used to control privileges used by resources



There are two types of Google Service Accounts

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.

There are two types of Google Service Accounts

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.

There are two types of Google Service Accounts

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.

User-managed keys

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.

Listing keys associated with a service account

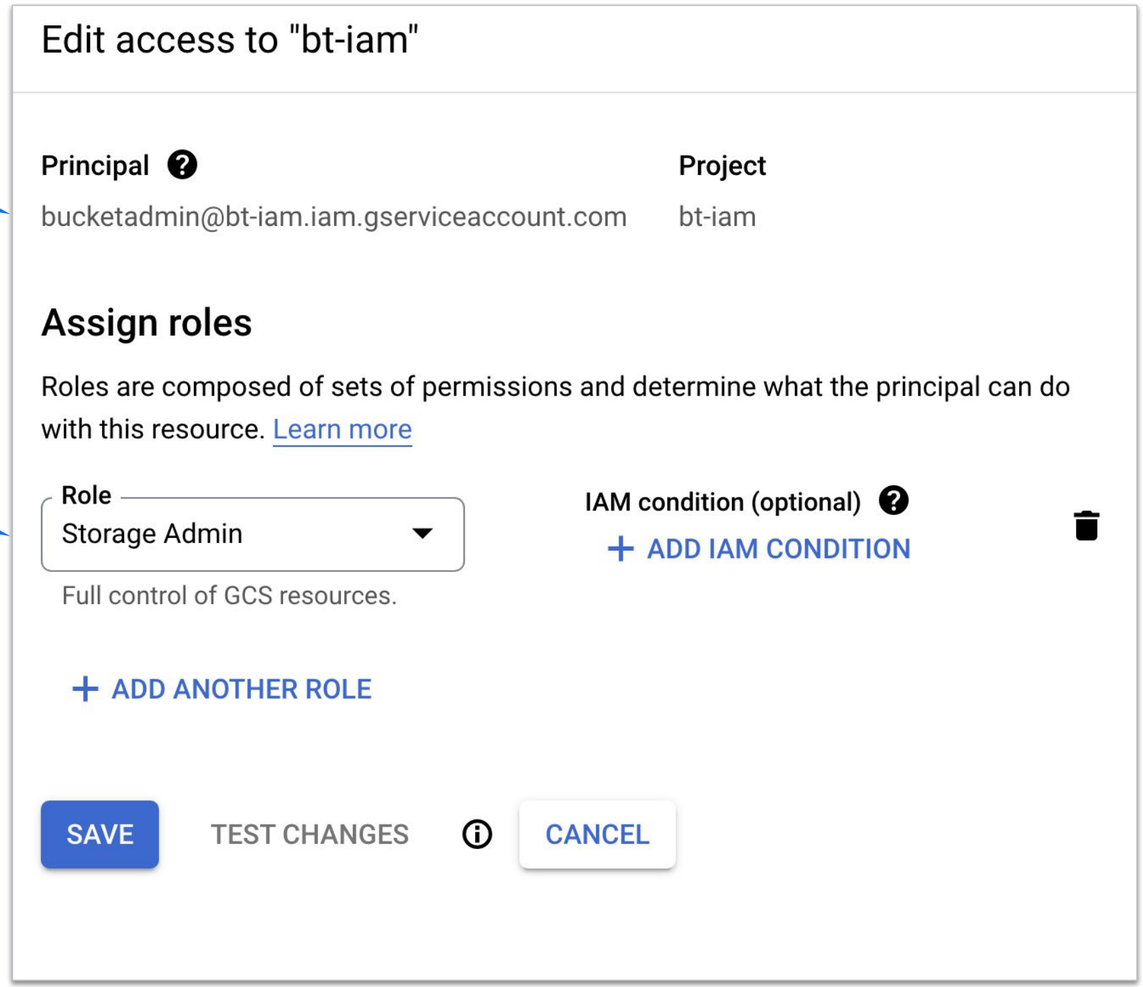
Use the gcloud command-line tool to quickly list all of the keys associated with a service account.

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

Service accounts are both principals and resources

Service Account

Assigned role



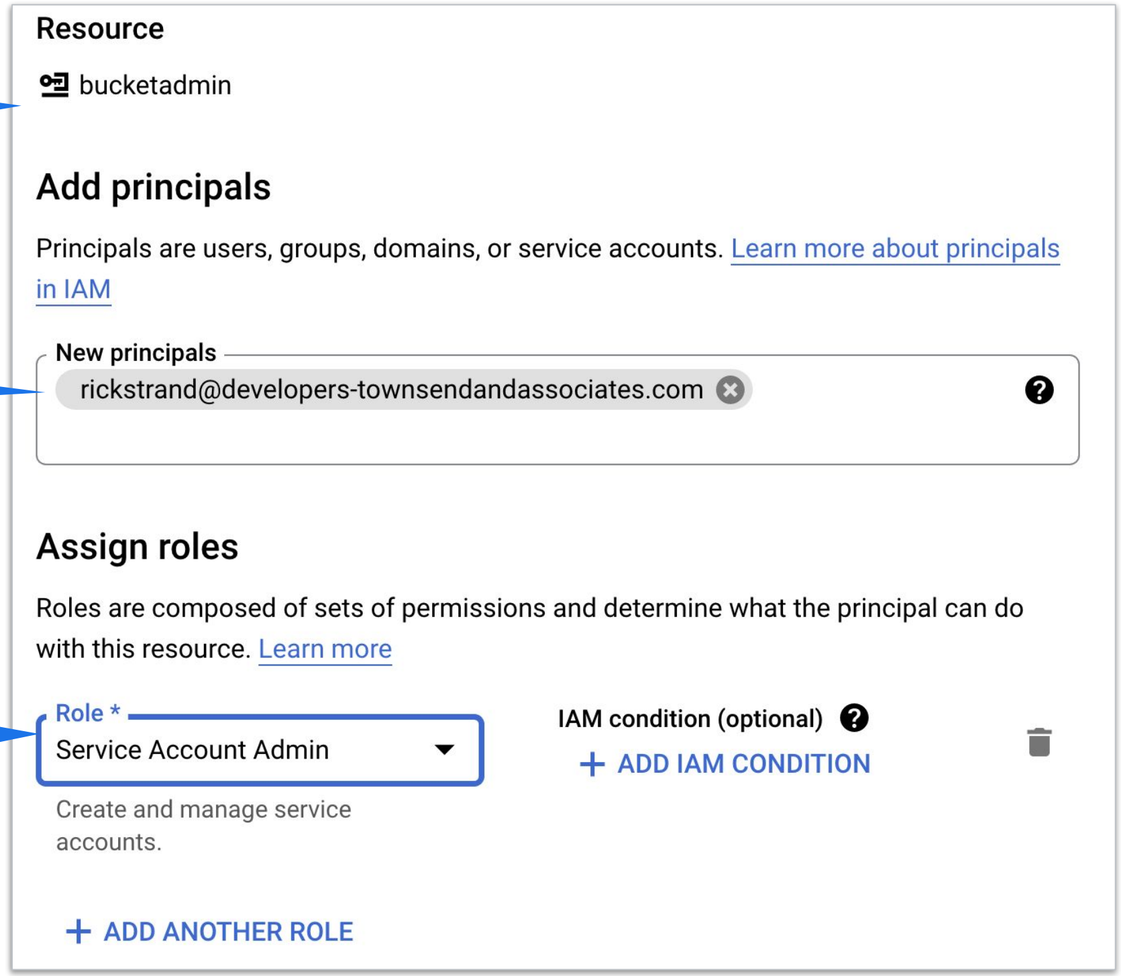
It is a principal when roles are assigned to it.

Service accounts are both principals and resources

Service Account

Principal

Service Account roles



Is a resource when users (principals) are given Service Account IAM roles to manage the service account in some way.

Service account predefined roles (not a complete list)

Assigned to principles

Service account admin

- Create and manage service accounts

Service account predefined roles (not a complete list)

Assigned to principles

Service account user

- Can attach service account to resources (e.g., Compute Engine)
- Can “impersonate” the service account and perform the tasks allowed by IAM given to the service account

Service account predefined roles (not a complete list)

Assigned to principles

Service account key admin

- Create and manage (and rotate) service account keys
- Keys are used by applications external to Google Cloud

Service account predefined roles (not a complete list)

Assigned to principles

Service account token creator

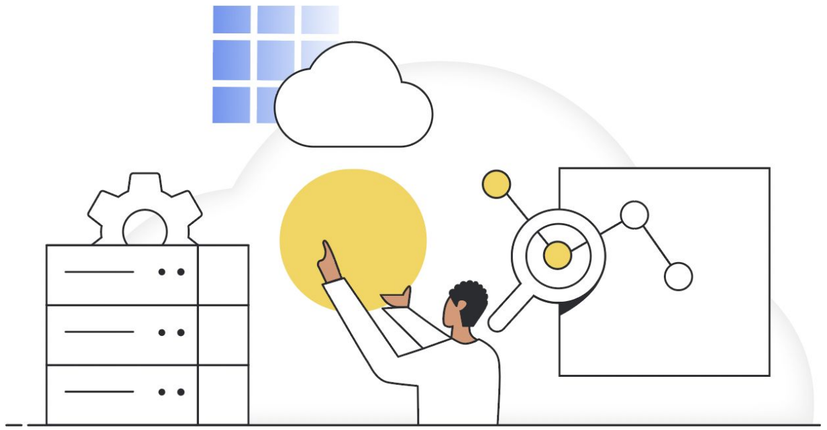
- Short lived credentials represented as OAuth 2.0 access tokens, OpenID Connect ID tokens, self-signed JSON Web Tokens (JWTs), and self-signed binary objects (blobs)

Accessing Google Cloud resources

From an external application

Any user, group, application, etc. must authenticate prior to accessing Google Cloud services*

- This also applies to external (e.g., on-premise) applications
- They use service accounts for this purpose



To authenticate as a service account, applications must use either use

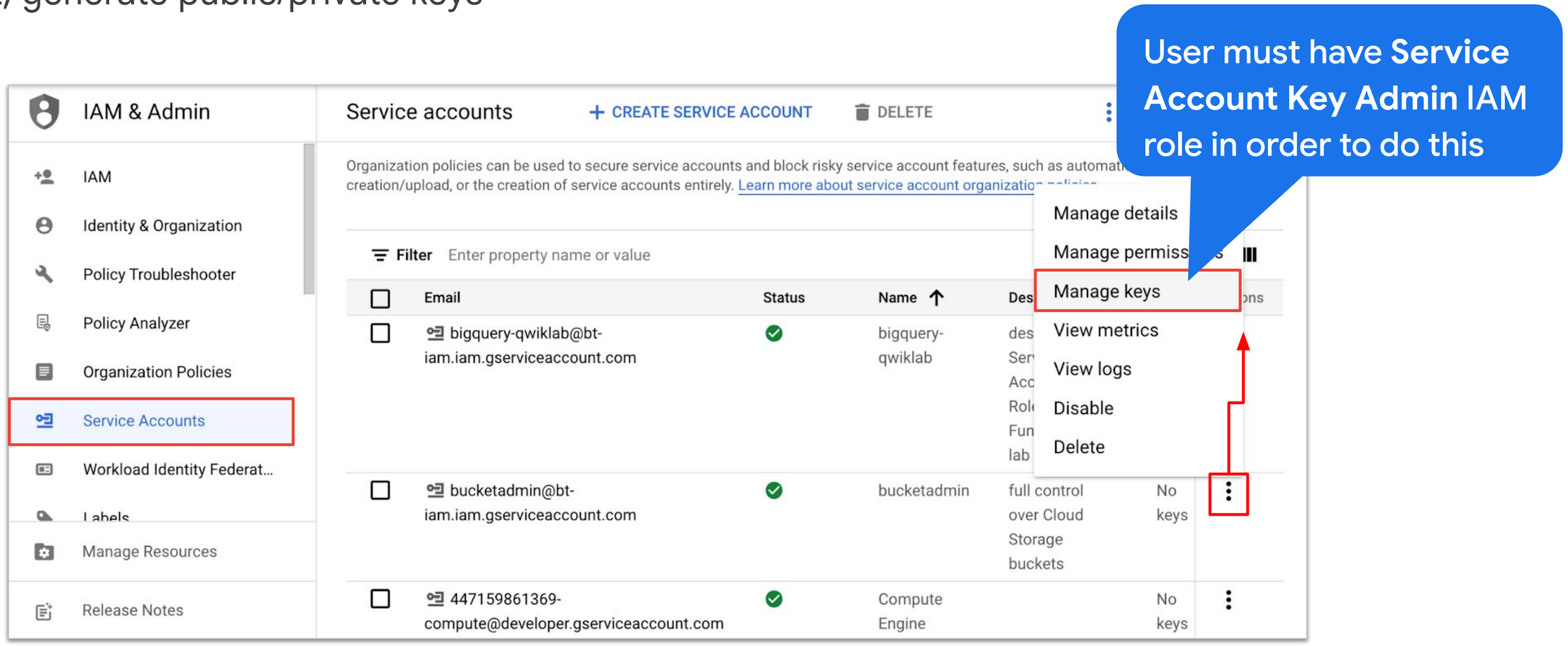
- Service Account Keys
- Service Account Tokens

*Exception: When authentication is not required, e.g., a public website hosted in Google Cloud

Service account keys

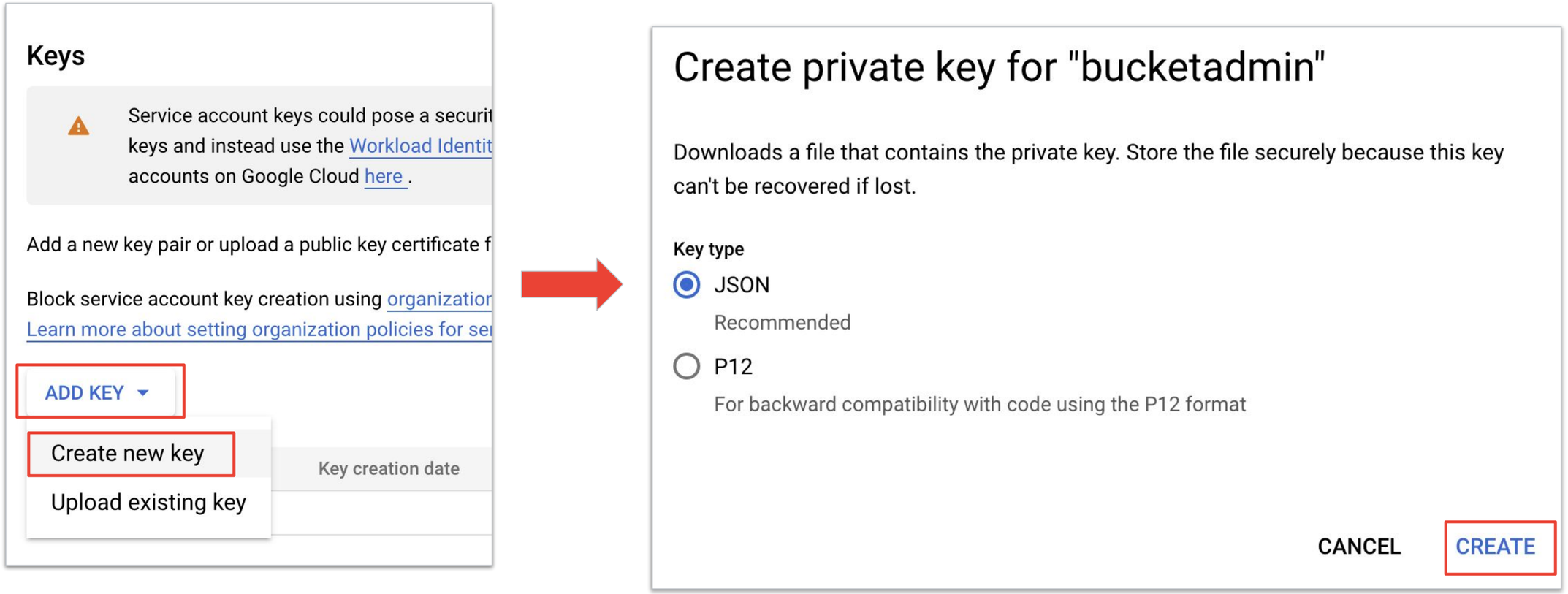
Can be used by external applications when authenticating to Google Cloud

- First, generate public/private keys



Service Account keys stored locally must be secured

- Next, download the private key
  - Public key is kept in Google Cloud
  - The customer is responsible for storing the private key securely



Using a Service Account key with code

To configure gcloud to use a service account:

```
$ gcloud auth activate-service-account \
test-service-account@google.com \
        --key-file=/path/key.json --project=testproject
```

Path where the service account key is stored

To use credentials in your code (Python is this example):

- The SDK will automatically look for the environment variable value

```
import os
from google.cloud.bigquery.client import Client

os.environ['GOOGLE_APPLICATION_CREDENTIALS'] = 'path_to_json_file'
bq_client = Client()
```

Using short-lived credentials with a service account

While service account keys work for application authentication, they are not the preferred method

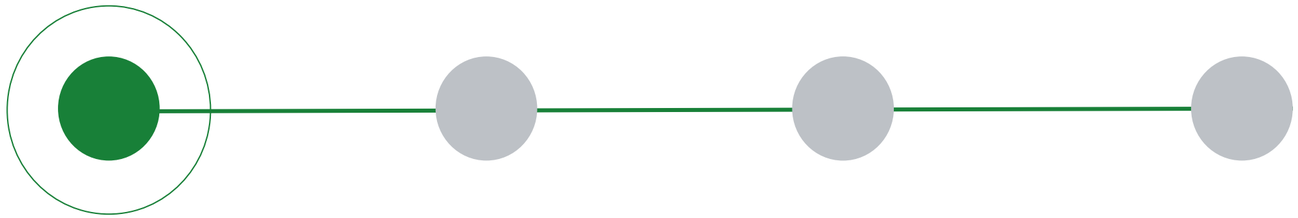
- The private Service Account **key must be secured by the customer** after downloading
  - An unauthorized person with access to the key can authenticate as the Service Account, and do whatever the Service Account's IAM roles allows
- Service account **keys have an unlimited lifetime**

Using short-lived credentials with a service account

The better alternative is to create short-lived credentials via Service Account tokens

- Principals (including service accounts) must have the **Service Account Token Creator** role in order to create tokens
- Different types of token are supported
  - OAuth 2.0 access tokens, OpenID Connect ID tokens, self-signed JSON Web Tokens (JWTs), and self-signed binary objects (blobs)

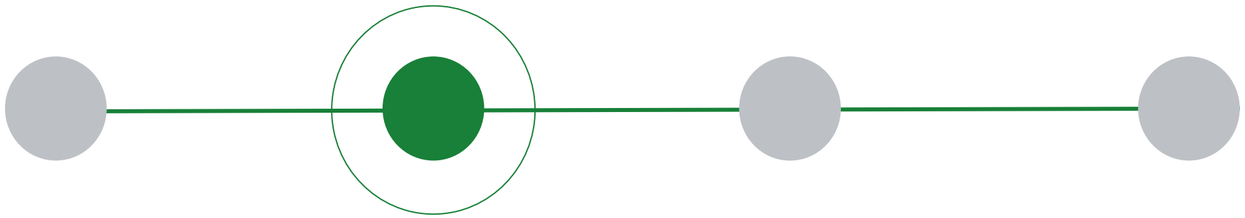
Types of tokens



OAuth 2.0 access tokens

- Used by an application to authenticate to Google APIs

Types of tokens

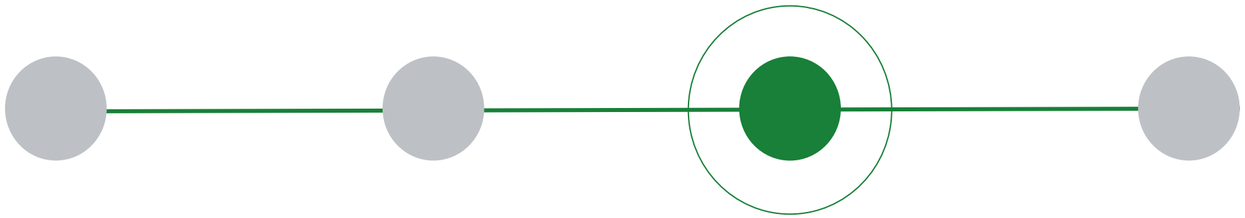


OpenID Connect (OIDC) tokens

Used when:

- Accessing a Cloud Run service
- Invoking a Cloud Function
- Authenticating a user to an application secured by Identity-Aware Proxy (IAP)
- Making a request to an API deployed with API Gateway or Cloud Endpoints

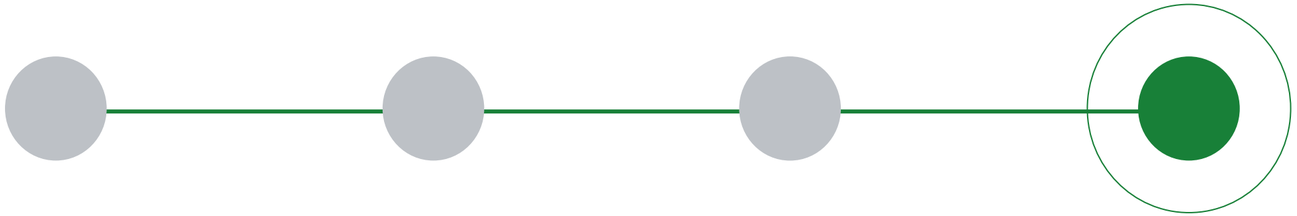
Types of tokens



Self-signed JSON Web Tokens (JWTs)

- Used to authenticate communication between services in a microservices architecture
- Used by an application to authenticate to Google APIs (e.g. FireStore)

Types of tokens



Self-signed binary objects (blobs)

- Used to securely identify the issuer of a request to a Google Cloud Storage bucket

Allowing principals to impersonate service accounts

01

User account user

- This role also allows a principal to attach the service account to a resource, e.g., a VM

Allowing principals to impersonate service accounts

02

Service account token creator

- Can impersonate the service account and create tokens

Allowing principals to impersonate service accounts

03

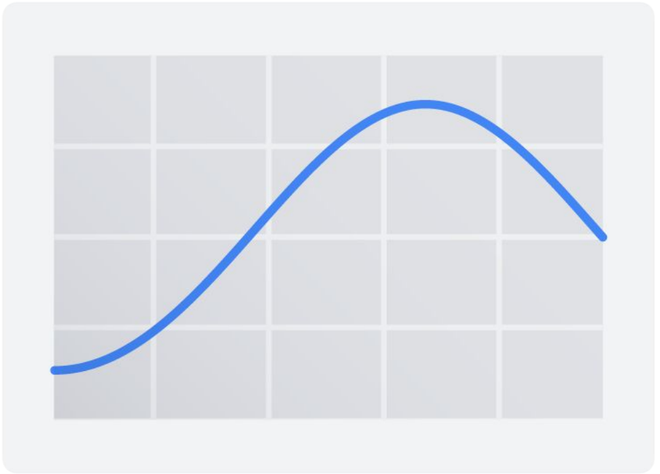
Workload identity user

- Can impersonate service accounts from GKE workloads
  - Kubernetes service accounts are not the same as IAM service accounts
  - Create IAM service accounts with roles to access Google Cloud resources
  - Map the Kubernetes service account to the IAM service account

Organizing Google Cloud instances with labels

Labels in Resource Manager help you organize your Google Cloud instances.

1. Team or cost center labels
2. Component labels
3. Environment or stage labels
4. State labels
5. Virtual machine labels



Label requirements in Resource Manager

1. No more than 64 labels per resource
2. Must be in the form of a key-value pair
3. Keys cannot be empty and must be between 1-63 characters
4. Values may be empty but cannot exceed 63 characters

1. Keys/values can contain only lowercase letters, numeric characters, underscores, and dashes
2. Label keys must be unique, but can be used with multiple resources.
3. Keys must start with a lowercase letter or international character

Google products and services

Currently supporting the use of labels

- BigQuery
- Cloud Bigtable
- Dataflow
- Dataproc
- Cloud Functions
- Cloud Healthcare API
- Cloud Key Management Service
- Pub/Sub

Google products and services

Currently supporting the use of labels

- Cloud Spanner
- Cloud SQL
- Cloud Storage
- Compute Engine
- Google Kuberenetes Engine
- Cloud Run
- Networking
- Resource Manager

Identity and Access Management

01 Resource manager

02 IAM roles

03 IAM policies

04 Workload identity federation

05 Policy intelligence

06 IAM troubleshooter

07 IAM recommender

08 IAM audit logs

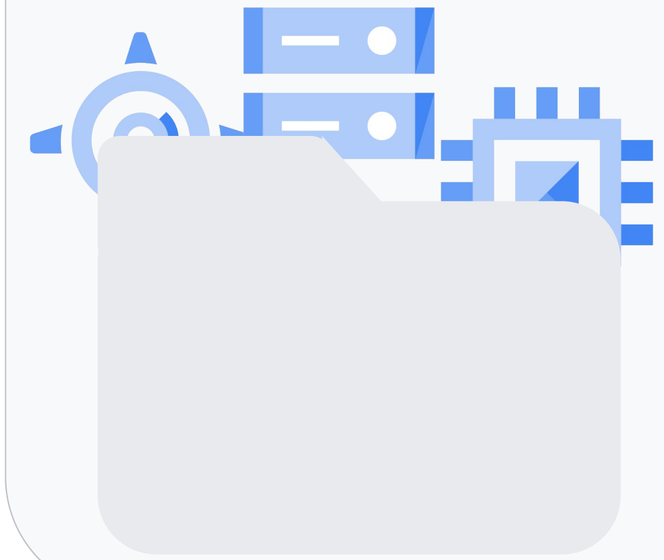
09 IAM best practices

IAM roles in Google Cloud

Basic

Predefined

Custom



IAM basic roles are applied at the project level

Basic roles offer fixed, coarse-grained levels of access

Can do what

on all resources

Basic roles

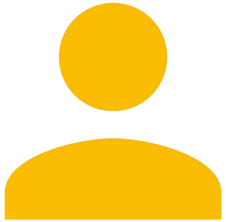
Apply across all Google Cloud services in a project

Owner

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

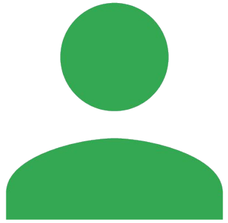
Editor

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



Viewer

- Read-only access



Billing Administrator

- Manage billing
- Add and remove administrators

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

IAM predefined roles

Can do what

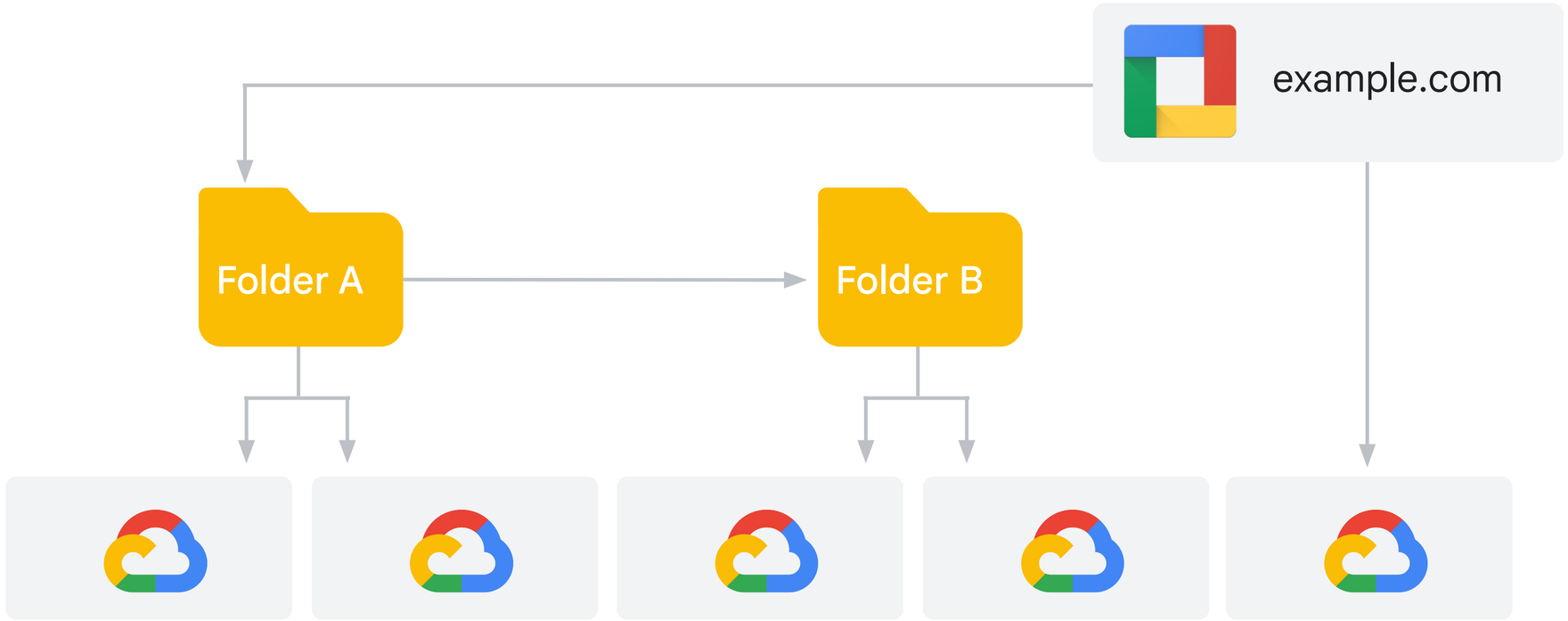
on Compuet Engine resources in this project, folder or org

IAM predefined roles

Offer more fine-grained permissions on particular services

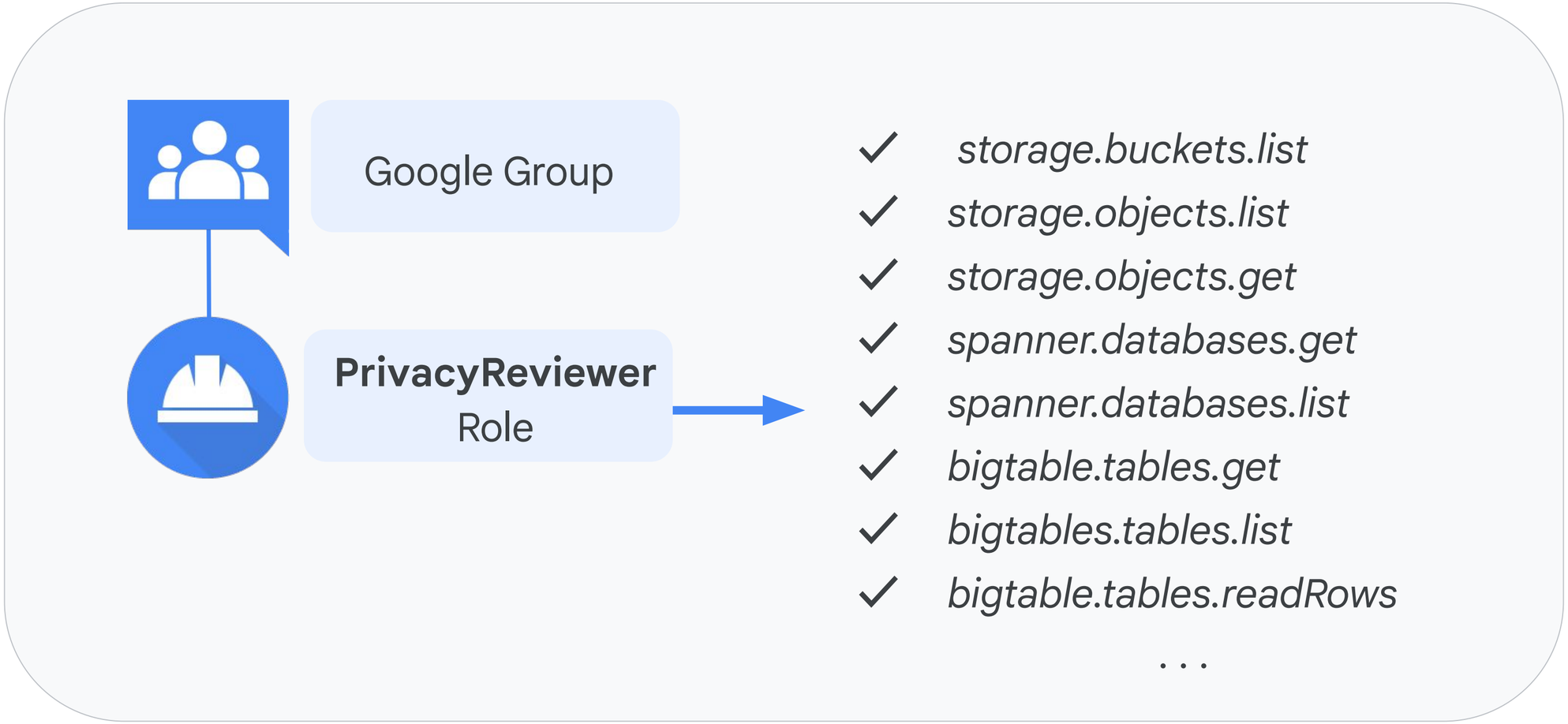
The predefined Browser role

Provides read access to browse the hierarchy for a project, including the organization and folders.



IAM custom roles

Let you define a precise set of permissions



Identity and Access Management

01 Resource manager

02 IAM roles

03 IAM policies

04 Workload identity federation

05 Policy intelligence

06 IAM troubleshooter

07 IAM recommender

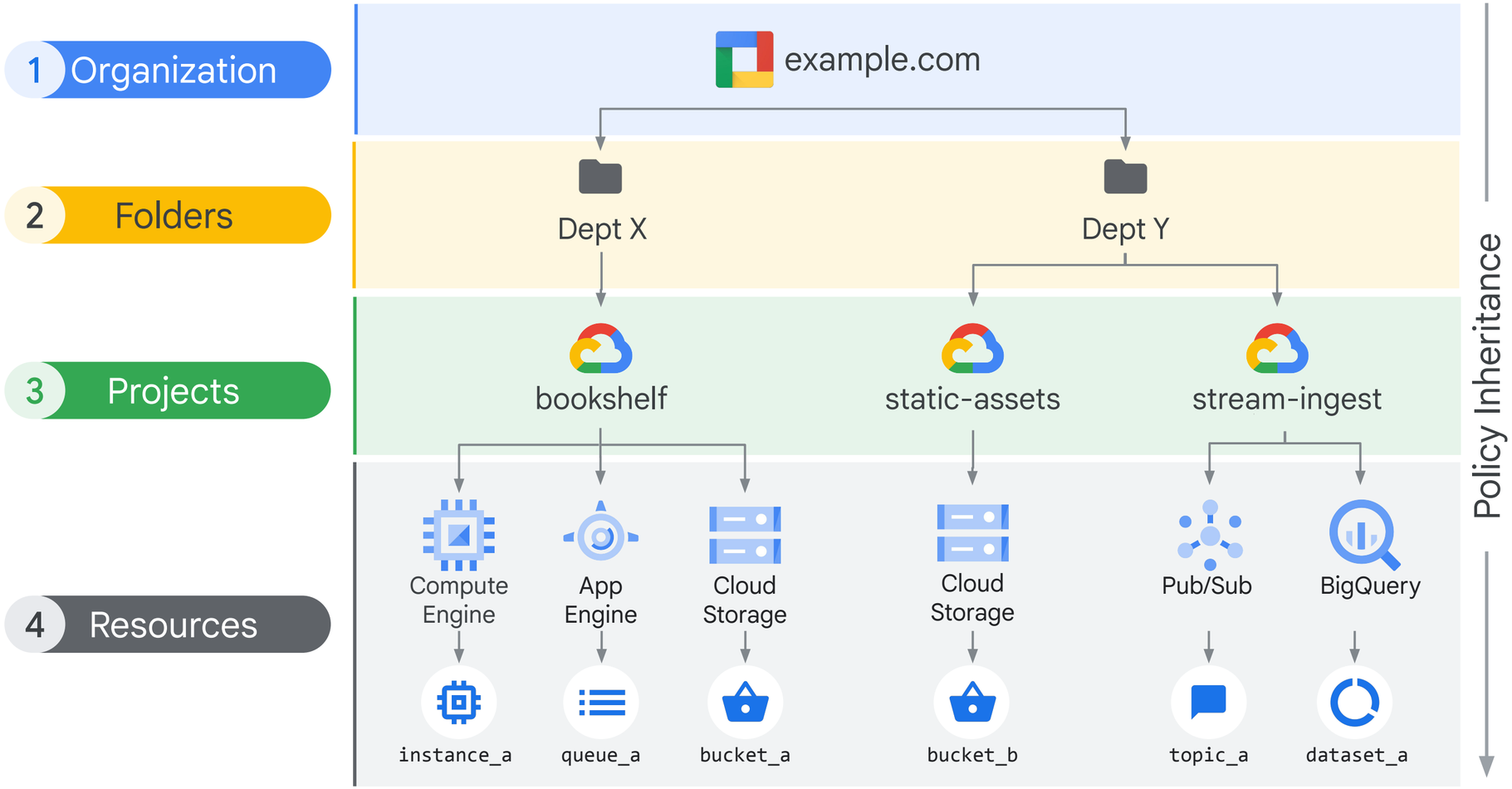
08 IAM audit logs

09 IAM best practices

IAM policies

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

IAM resource hierarchy



IAM policies

- Grant access to Google Cloud resources
- Controls access to the resource itself, as well as 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 conditions

Allow access only to Cloud Storage buckets whose names start with a specified prefix

```
resource.type == "storage.googleapis.com/Bucket" &&
resource.name.startsWith("projects/_/buckets/exampleco-site-assets-")
```

- Specified in the role bindings of a resource's IAM policy
- Enforce conditional, attribute-based access control for Google Cloud resources
- Grant resource access to identities (members) only if configured conditions are met
- Condition attributes
  - Resource attributes
  - Request attributes

Deny policies

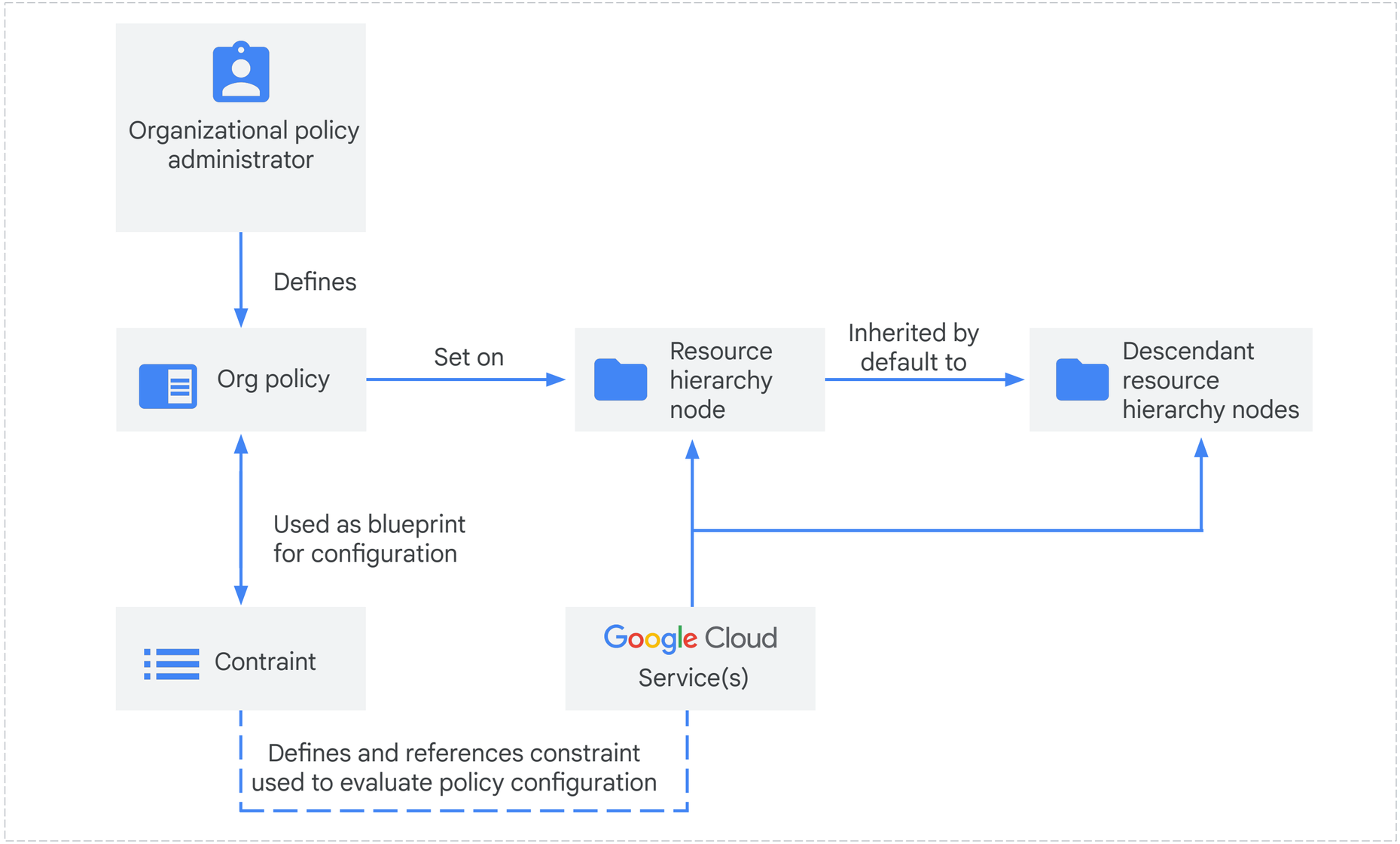
First create a deny policy and store it in a file.

```
{
  "deniedPrincipals": [
    "principalSet://goog/group/dev@example.com"
  ],
  "deniedPermissions": [
    "iam.googleapis.com/serviceAccountKeys.create",
    "Iam.googleapis.com/serviceAccountKeys.delete"
  ]
}
```

Next apply the deny policy.

```
gcloud iam policies create POLICY_ID \
    --attachment-point=[proj-id|folder-id|org-id] \
    --kind=denypolicies \
    --policy-file=POLICY_FILE
```

Organizational policies



Organizational policies contraints

- Configure with constraints
  - Particular type of restriction against either a Google Cloud service or a group of Google Cloud services
- Descendants of the targeted resource hierarchy node inherit the organization policy

```
ADD CODE
```

```
resource: "organizations/ORGANIZATION_ID"
policy: {
  constraint: "constraints/iam.disableServiceAccountCreation"
  booleanPolicy: {
    enforced: true
  }
}
```

Organization policy constraint types

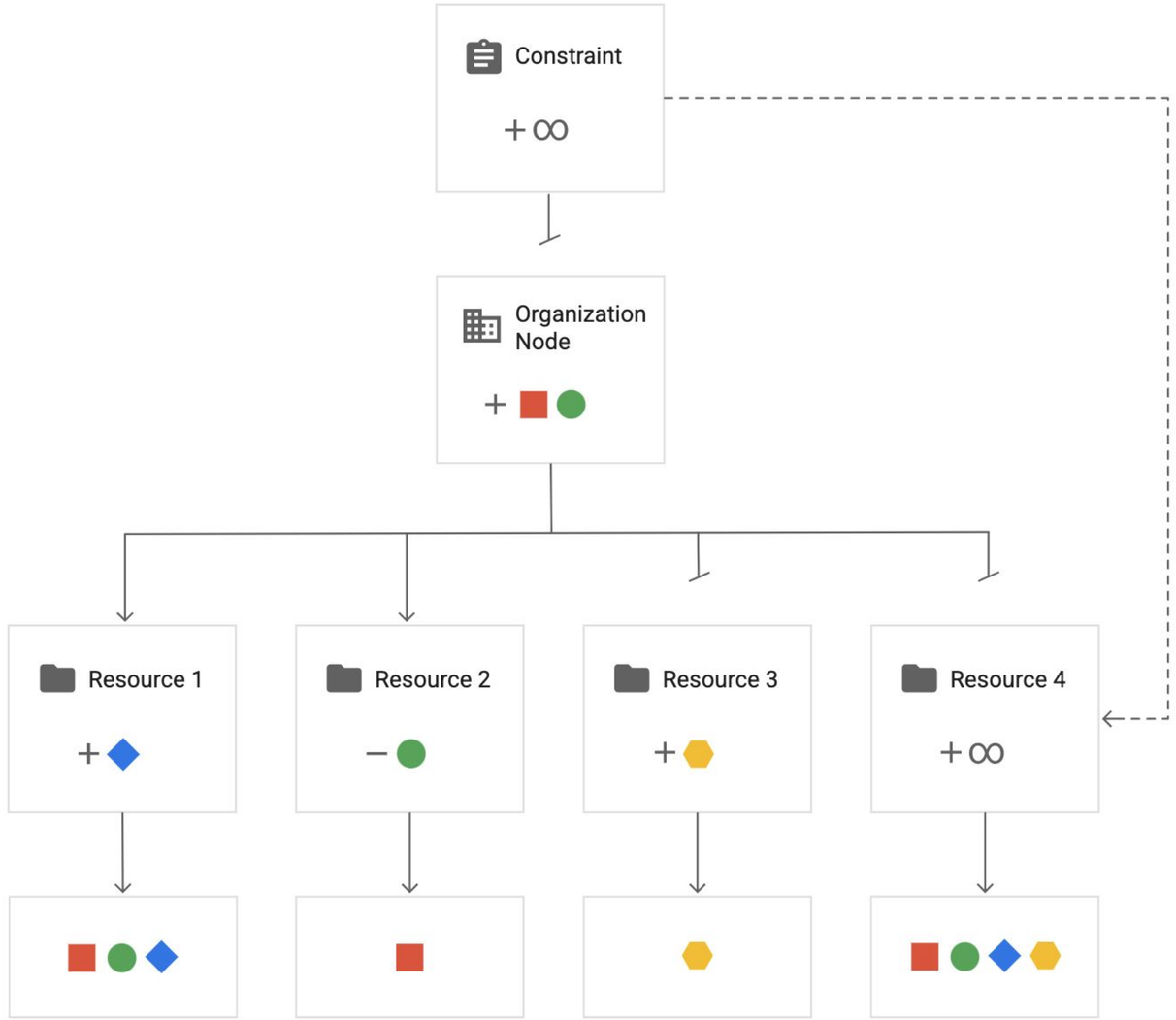
- List constraint type allow or disallow from a list of values
- Example: `compute.vmExternalIpAccess`

- Boolean constraint type turn on or turn off policies
- Example: `compute.disableSerialPortAccess`

Organization policy constraint examples

Service	Constraint
Compute	constraints/compute.disableNestedVirtualization
	constraints/compute.disableSerialPortAccess
	constraints/compute.trustedImageProjects
	constraints/compute.vmExternalIpAccess
IAM	constraints/iam.disableServiceAccountCreation
	constraints/iam.disableServiceAccountKeyCreation
Google Cloud	constraints/serviceuser.services

Organization policies hierarchy



Organization policies versus IAM policies

Organization policies

- These policies focus on **what**.
- Lets the administrator set restrictions on specific resources to determine how they can be configured.

IAM policies

- These policies focus on **who**.
- Lets the administrator authorize who can take action on specific resources based on permissions.

Identity and Access Management

01 Resource manager

02 IAM roles

03 IAM policies

04 Workload identity federation

05 Policy intelligence

06 IAM troubleshooter

07 IAM recommender

08 IAM audit logs

09 IAM best practices

Workload identity federation - overview

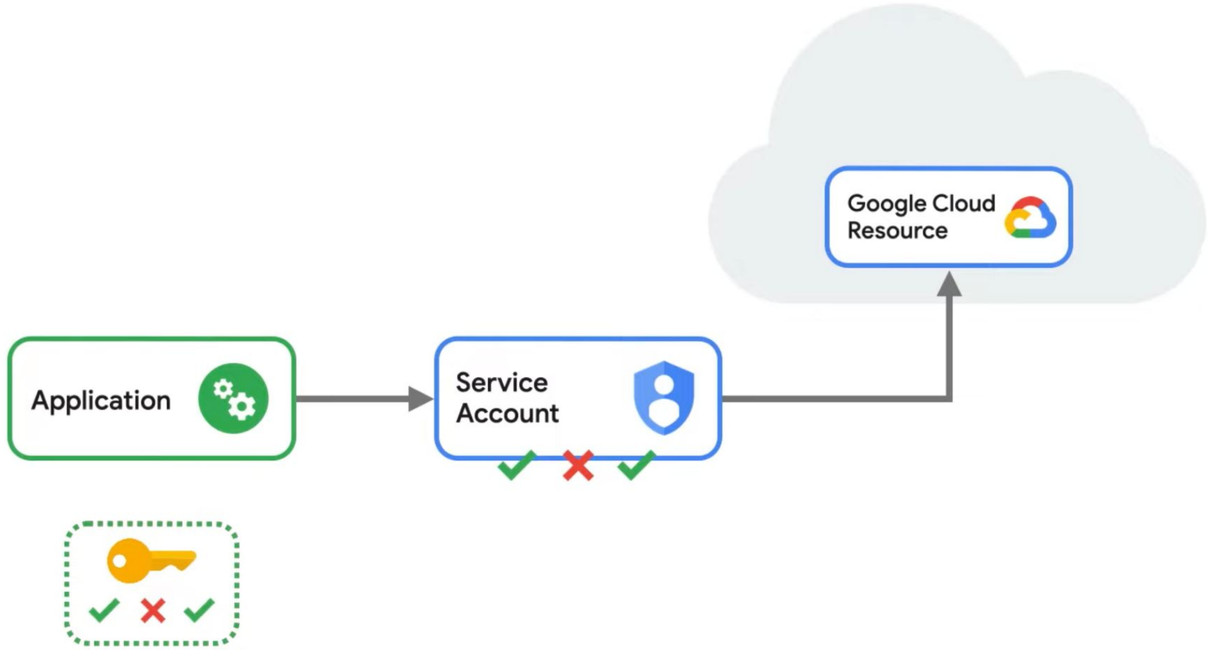
- Grant apps running outside of Google Cloud access to data without service account keys

Problem:

- Service account keys are powerful
  - Security risk if not managed correctly

Solution:

- Grant external identities IAM roles
  - Impersonate service accounts and access resources



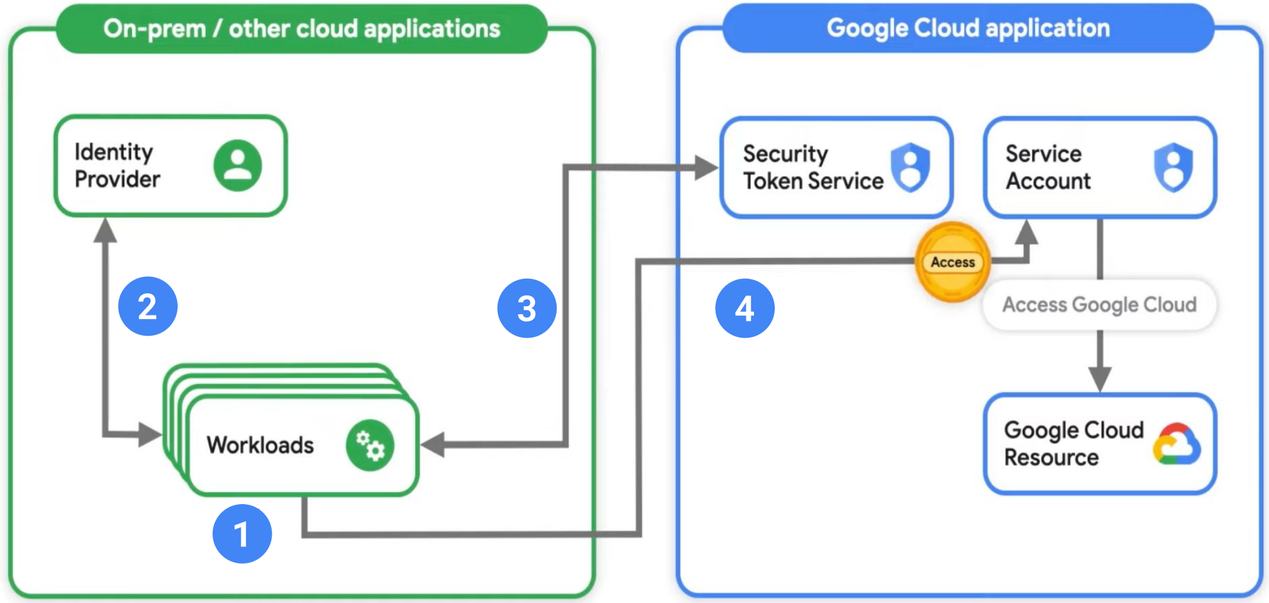
Workload identity federation - how it works

01 Create a workload identity pool in your Google Cloud project

02 App authenticates with identity provider – receives account credentials

03 App calls security token service – get short-lived Google Cloud access token

04 Use token to impersonate service account – access Google Cloud resources



Identity and Access Management

01 Resource manager

02 IAM roles

03 IAM policies

04 Workload identity federation

05 Policy intelligence

06 IAM troubleshooter

07 IAM recommender

08 IAM audit logs

09 IAM best practices

Policy intelligence

Policy Intelligence tools help you understand and manage your policies to proactively improve your security configuration.

1

Troubleshooting tools

Find out what went wrong quickly

2

Analysis tools

Prevent mistakes from happening

3

Actionable recommendations

Make improvements easily

Policy Troubleshooter

Policy Troubleshooter exposes access policies that apply to a particular resources.

01

Policy Troubleshooter requires a member email, a resource name, and a permission check.

02

Policy Troubleshooter examines all IAM policies that apply to that resource.

03

Policy Troubleshooter reports om whether that member’s roles include that permission to that resource.

04

Policy Troubleshooter reports on which policies bind that member to that resource.

Policy Troubleshooter

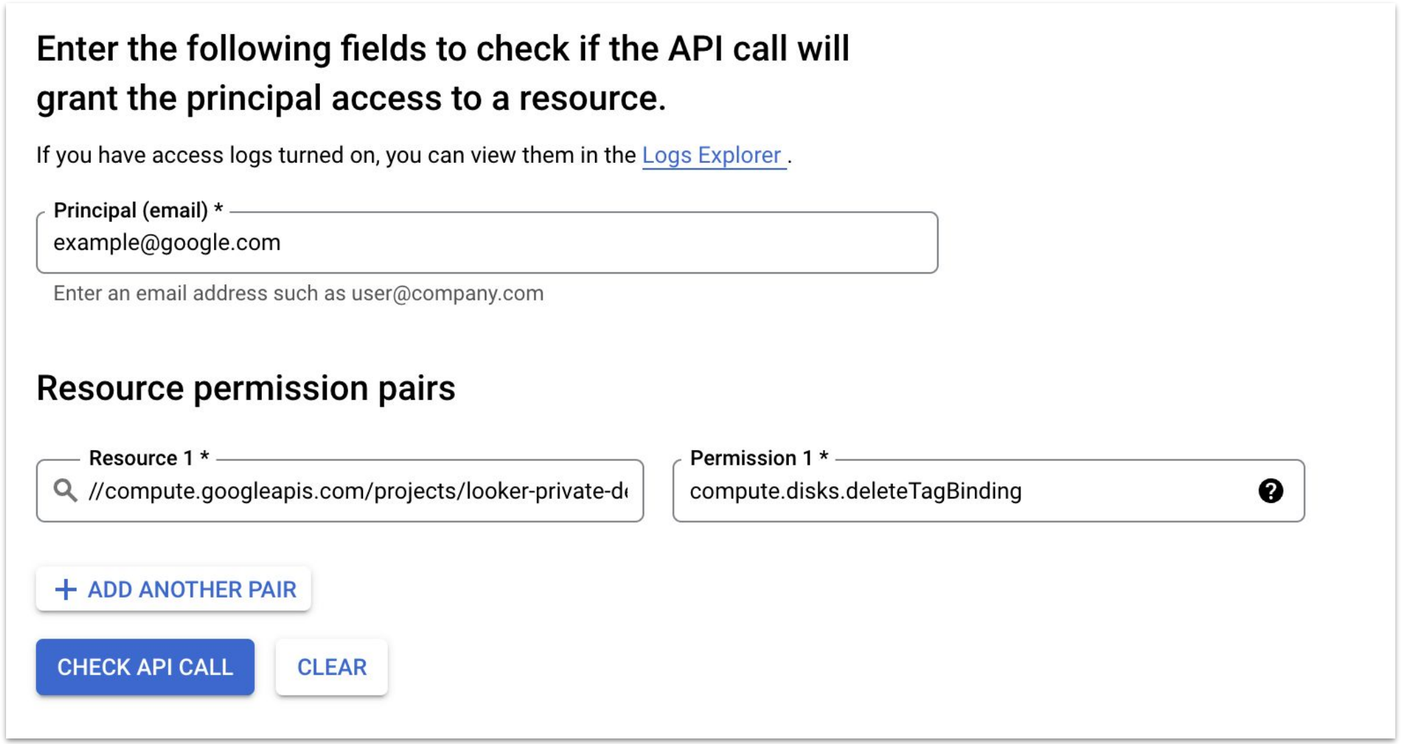
Policy Troubleshooter will only access policies that the user has permissions to view.

- Policy Troubleshooter may not always fully explain resources access.
- If you do not have access to a resource policy, it will not be analyzed.
- Maximum effectiveness requires the Security Reviewer (roles/iam.securityReviewer) role

Policy Troubleshooter

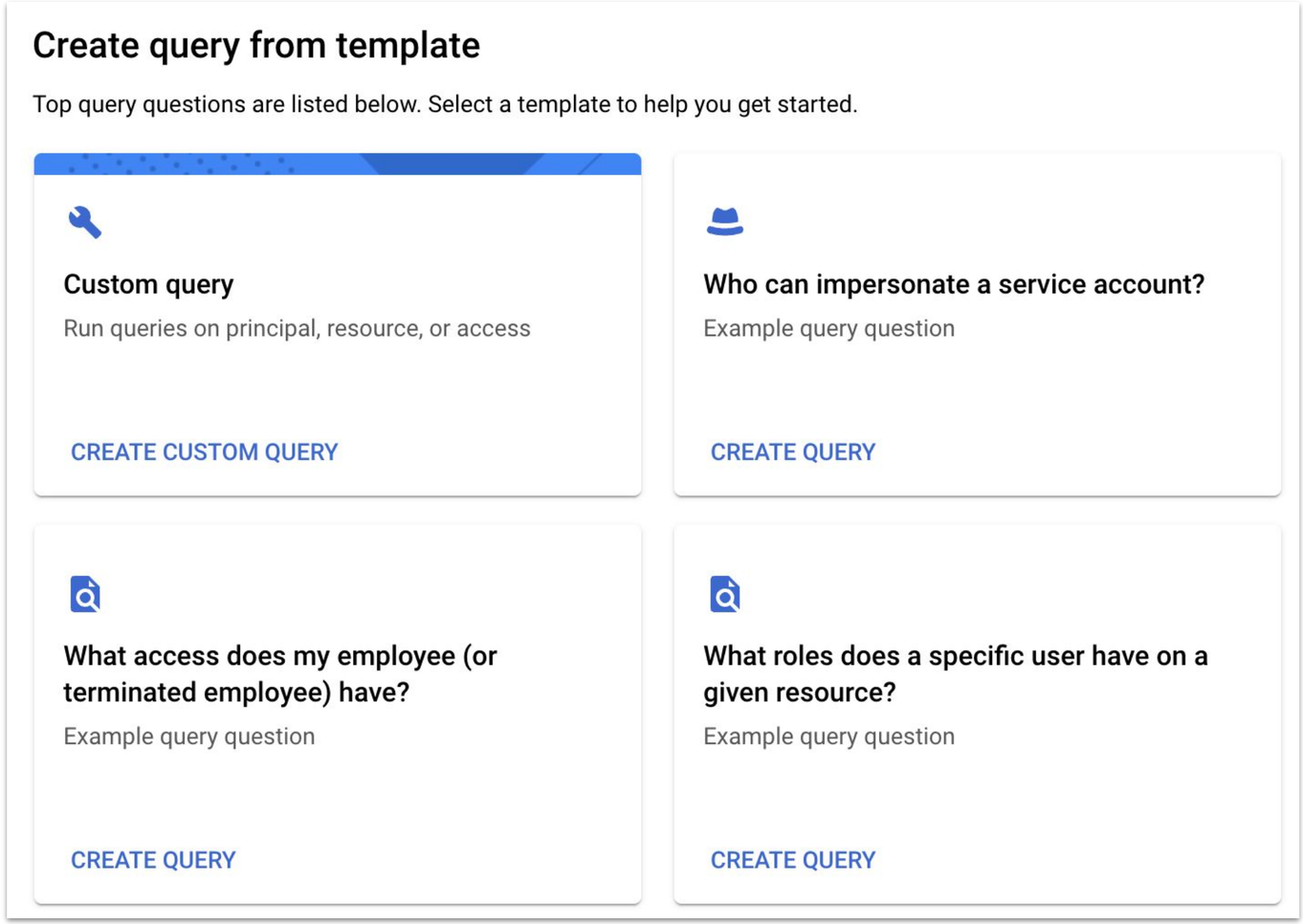
Policy Troubleshooter is accessible through the console, the Google Cloud CLI, or the REST API.

- Console
  - Simple queries
- Google Cloud CLI
  - More complex scenarios
- REST API
  - More complex scenarios



Policy Analyzer

- Which principles have what access to which Google Cloud resources?
- Examples:
  - Who can access IAM service account?
  - Who can read data in BigQuery dataset?
  - Who has access to resources in a project?



Identity and Access Management

01 Resource manager

02 IAM roles

03 IAM policies

04 Workload identity federation

05 Policy intelligence

06 IAM troubleshooter

07 IAM recommender

08 IAM audit logs

09 IAM best practices

Recommender evaluations

- Recommender compares project-level role grants with permissions used within the last 90 days.
- If a permission has not been used within that time, Recommdener will suggest revoking it.
- You have to review and apply recommendation, as they will not be applied automatically.

Recommender

Recommender gives you three types of recommendations:

01 Revoke an existing role

02 Replace an existing role

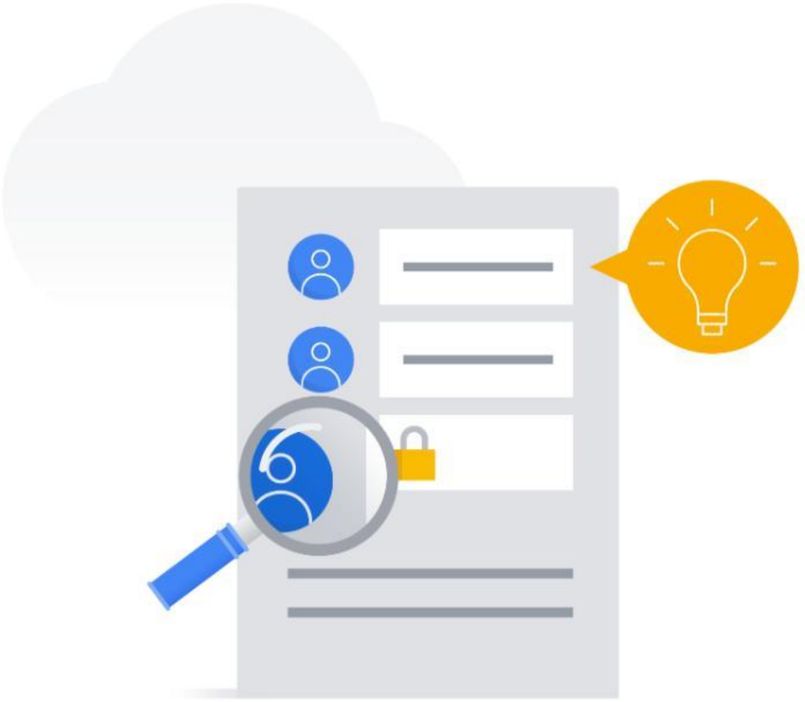
03 Add permissions to an existing role

Recommender creates daily policy recommendations and serves them to you automatically.

Cloud Console

The easiest way to review and apply recommendations is to use the Cloud Console.

- View existing roles by visiting the IAM page.
- Look for the “over-granted permissions” column.
- If there are recommendations you will see a **recommendation available** icon.
- Click the **recommendation available** icon for details.
- Choose to “apply” or to “dismiss” a recommendation.
- You can rever your choice within 90 days.



Identity and Access Management

01 Resource manager

02 IAM roles

03 IAM policies

04 Workload identity federation

05 Policy intelligence

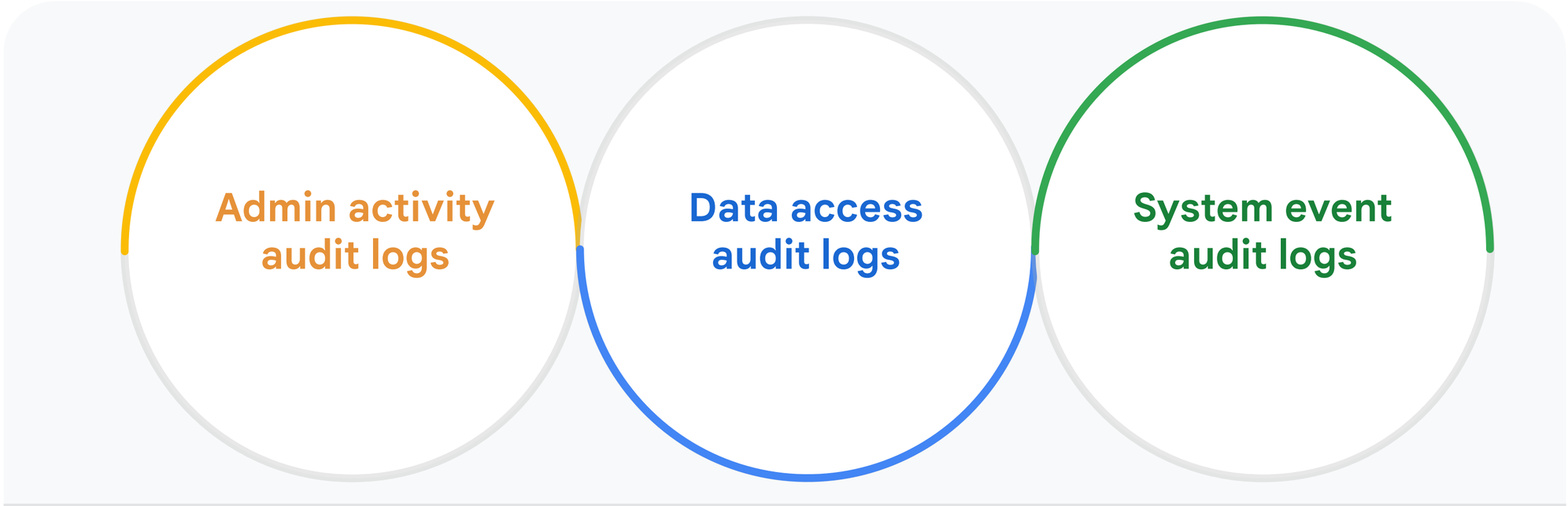
06 IAM troubleshooter

07 IAM recommender

08 IAM audit logs

09 IAM best practices

Cloud Audit Logs



Cloud Audit Logs maintains three logs for each project, folder and organization

Admin Activity Audit Logs

Admin activity audit logs record API calls that modify your resources

01

Created when administrative actions modify configurations or metadata

02

Logs are always written and cannot be disabled

03

Must have IAM role Logging/Logs Viewer or Project/Viewer

System Event Audit Logs

System event audit logs record activity that modifies the configuration of your resources

- Driven by Google system events
- Not triggered by user interaction
- Always written and cannot be disabled

Data Access Audit Logs

Records changes to private cloud resources

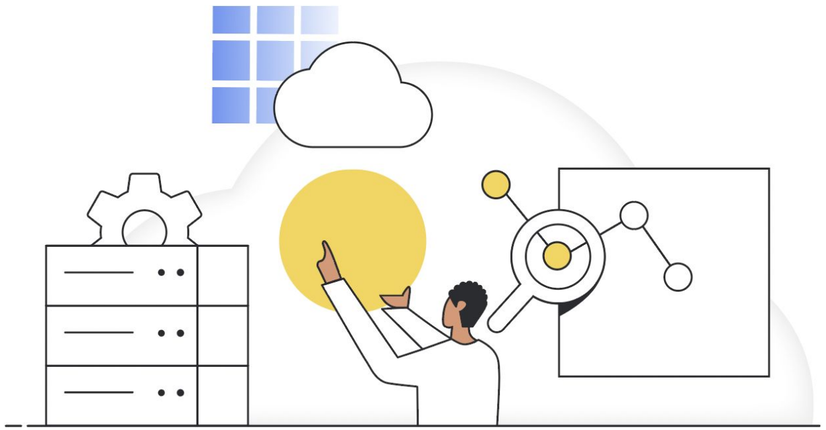
Do not record changes to publicly shared assets

Not enabled by default because they grow quite large

These logs record read, modify, or create activity on your resource metadata or user-provided data

Options for viewing audit logs on Google Cloud

- Basic log viewer
- Advanced log viewer
- gcloud command-line tool
- Audit Logs API



Identity and Access Management

01 Resource manager

02 IAM roles

03 IAM policies

04 Workload identity federation

05 Policy intelligence

06 IAM troubleshooter

07 IAM recommender

08 IAM audit logs

09 IAM best practices

IAM best practices

Principle of Least Privilege

- Adhere to the Principle of Least Privilege.
- This means you should always apply only the minimal access level required to get the job done.

IAM best practices

Using groups for Google access

- Use groups when configuring Google Cloud access.
- Assign roles to the groups instead of individual users

IAM best practices

Pre-defined versus custom roles

- Utilizing predefined roles offers less administrative overhead.
- Predefined roles are managed by Google.
- Custom roles are not maintained by Google.

IAM best practices

Auditing policy changes using audit logs

- Audit logs record project-level permission changes.
- Audit policy changes
- Export audit logs to Cloud Storage to store your logs for long periods of time.


Google Cloud