# Identity Management

Memi Lavi
www.memilavi.com

# Identity Management

- Usually there are more than one user in the cloud
- Very important to set who can do what
- Remember: You created the project so you can do everything
- This is not the best practice
- Users should be allowed to do JUST what they need to do

# Identity Management

- Examples:

| User role | Should be able to… | Should not be able to… |
|---|---|---|
| Infrastructure engineer | • Deploy and access VMs<br>• Deploy GKE clusters<br>• Deploy Cloud SQL | • Upload code to App Engine<br>• Create or delete Projects |
| Developer | • Upload code to Cloud Run<br>• View logs<br>• Access VMs | • Deploy VMs<br>• Create or delete Projects |
| Organization admin | • Create or delete projects<br>• Add or remove users<br>• View all resources | • Deploy or remove VMs<br>• Deploy BigTable |
| Budget admin | • View all resources<br>• Set budget | • Anything else… |

- "The Least Privilege Principle"

# Identity Management

- In GCP this is done using Cloud IAM

# Cloud IAM

- IAM = Identity and Access Management
- Defines:

| | |
|---|---|
| Who | → Principal |
| Can do What | → Role |
| With which Resource | → Allow Policy |

# Principal

- Identity in GCP
- Can access resources
- Can be assigned roles
- Not necessarily a human

# Principal

- Principal types:

Google Account

Service Account

Google group

Google workspace account

Cloud Identity domain

All authenticated users

All users

# Principal

Google Account

- A person who interacts with Google Cloud
- Having email address associated with Google Account
- Can be `gmail.com` or anything else
- This is the type of account you have and the most common one

# Principal

Service Account

- Represents an application or a compute workload
- Used to grant code running on Google Cloud permissions to access and work with other resources in the cloud
- Created automatically when creating various resources (ie. VM)
- Can be created manually and attached to a workload

# DEMO

- Let's take a quick look on VM service account
- Go to Compute engine and start creating a new instance
- Scroll down and show the service account
- This sets whether the VM can access and work with other resources

# Principal

Google group

- A collection of Google accounts and Service accounts
- Has a unique email address
- A convenient way to apply access controls to a collection of users
- Requires organization – we won't be able to use it

# Principal

Google Workspace account

- A virtual group of all the Google Accounts in the organization
- Contains all the accounts with the organization's domain name
- Requires organization – we won't be able to use it

# Principal

Cloud identity domain

- Similar to Google Workspace account
- Users don't have access to Google Workspace applications
  - ie. Docs, Sheets, Slides etc.
- Requires organization – we won't be able to use it

# Principal

All authenticated users

- Represents all the Google accounts and Service accounts
- Useful if you want all the cloud users to have a unified permissions on a specific resource

# Principal

All users

- Represents all the users on the internet
- Useful if you want to make a specific resource public on the internet
- We used it with the Cloud Storage Bucket

# Principal

- You will usually work with:
  - Google Accounts
  - Service Accounts
  - Groups (when available)

# Synchronizing with Active Directory

- One of the common requirements in the cloud is to synchronize user in on-premises Active Directory with the cloud
- This can be achieved using Federation

# Federating Users

- Two steps process:
  - Provisioning users
  - Single sign-on

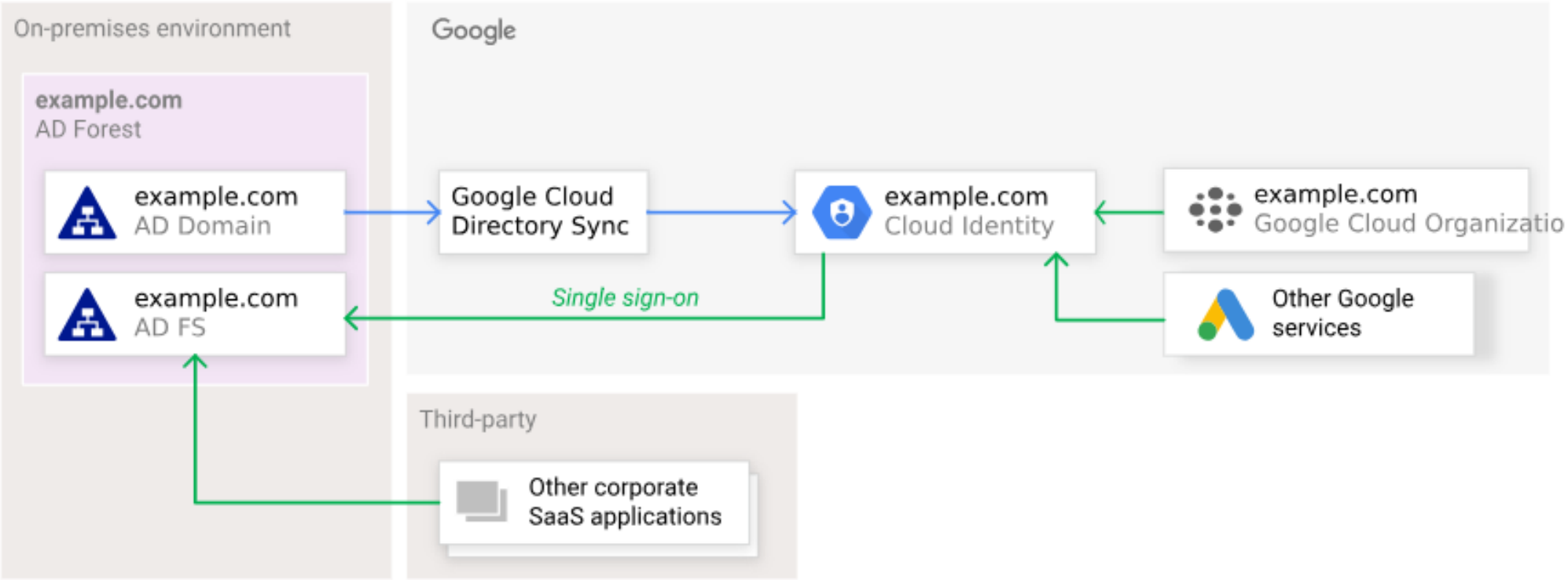
# Provisioning Users

- Users and groups are periodically synchronized with the cloud
- One-way sync – only to the cloud
- Credentials are not synchronized
- Implemented using Google Cloud Directory Sync
- A free tool to synchronize the users and groups

# Single sign-on

- When a synchronized user logs into the cloud – the cloud delegates the user to the Active Directory for signing in
- Using the SAML protocol
- Can be implemented using Active Directory Federation Services or other federation services

# Federating Users



# Roles

- One of the most important security aspects in GCP is Roles
- Roles allow assigning pre-defined permissions to users
- You should be VERY CAREFUL when assigning roles
- Many security breaches are caused by too permissive role assignments

# Role Types in GCP

- There are two types of roles in GCP:

Use THIS!

| Basic Roles | Predefined Roles |
| --- | --- |
| - Highly permissive | - Provide granular access to specific GCP resource |
| - Legacy – existed prior to IAM | - Updated by Google |
| - Should be avoided | - Should be used |

# Basic Roles

Viewer (roles/viewer)

- Read-only actions
- Does not change state
- Example: viewing VM instance

Editor (roles/editor)

- All Viewer permissions plus…
- Permissions to change state (create, change, delete resources)
- Example: Creating VM instance

Owner (roles/Owner)

- All Editor permissions plus…
- Completing sensitive tasks (ie. Canceling BigQuery jobs)
- Managing roles and permissions for a project
- Setting up billing for a project

Not Recommended!

# Predefined Roles

- Provide granular access to specific GCP resources
- Roles per service
- Examples:

| | |
|---|---|
| Compute Admin (`roles/compute.admin` | Full control of all Compute Engine resources |
| Cloud SQL Instance User (`roles/cloudsql.instanceUser` | Allows access to a Cloud SQL instance |
| Storage Object Creator (`roles/storage.objectCreator` | Allows users to create objects in Cloud Storage |

# Permissions

- A role is a collection of permissions
- Permission: A (very!) granular permission for a specific action in a specific service
- Represented in a form of: `service.resource.verb`
- Examples: `cloudsql.databases.list`

  `appengine.applications.create`

# Permissions

- Permissions are assigned to roles
- Cannot be assigned directly to principals
- Can view the permissions of each role

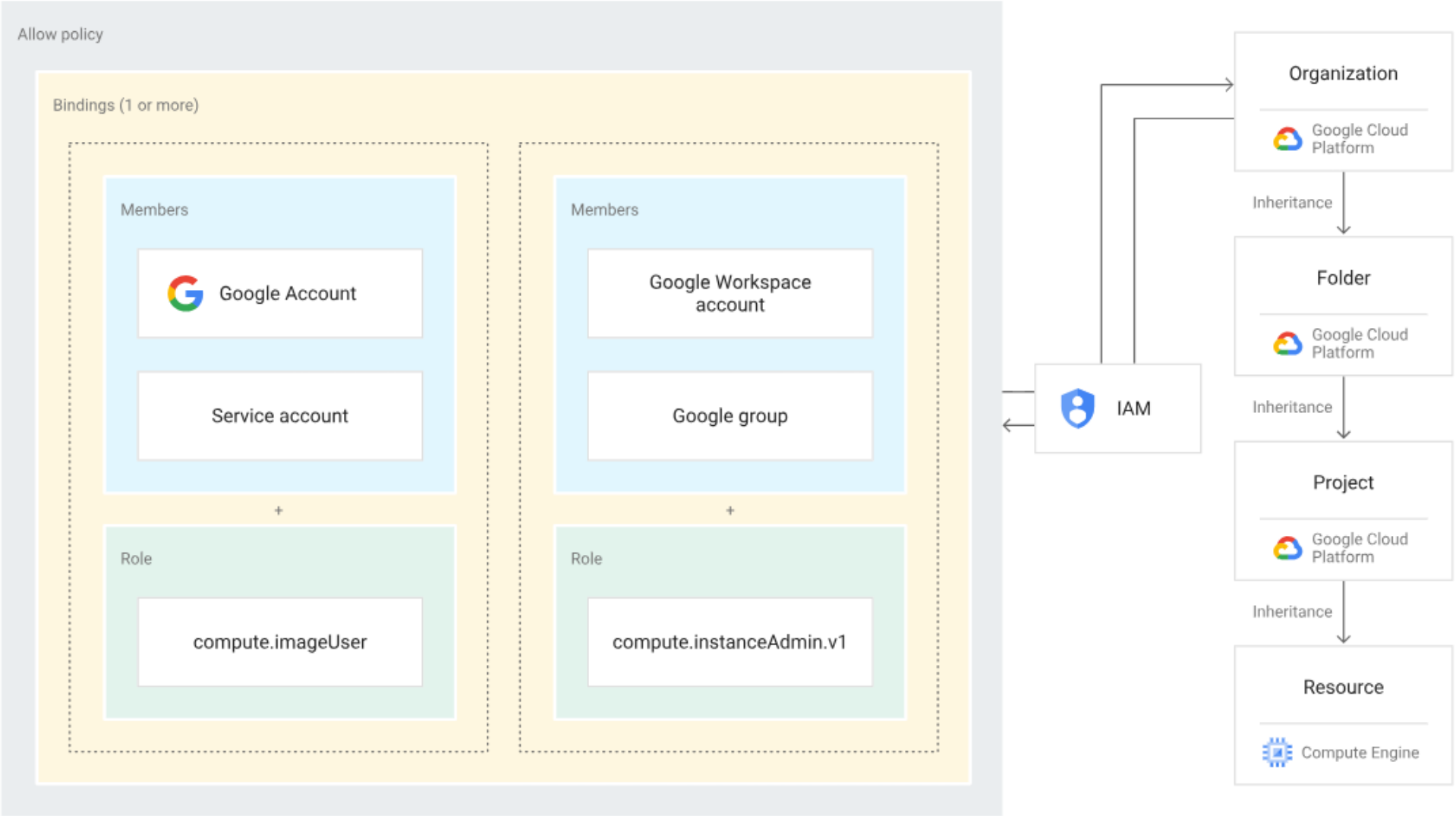
# Custom Roles

- User-defined roles
- Good for bundling permissions for specific needs
- Created in a project (or organization)
- Not all permissions can be included in custom roles

# Allow Policy

- Grants roles to principals for specific resources
- Can be set on an organization, folder, project or resource level

# Allow Policy



# Quotas

- GCP uses quotas to restrict use of its resources
- Helps in preventing spikes in resource usage, creating overload
- Almost every resource type has a quota
- When running out of quota, you can submit increase request
- Quota alerts help in following quota usage

# Quotas in Free Account

- Quotas are quite low
  - Example: Only 5 networks can be created
- Cannot submit increase requests
- Quota alerts can be created

# Identity Platform

- With Cloud IAM we control access to the cloud resources
- The cloud offers another identity management capability
- Allowing identity management to apps we develop
- This is done using Identity Platform

# Identity Platform

- Customer identity and access management (CIAM) platform
- Scale automatically as needed
- Global service
- SLA: 99.95%
- Support multiple protocols (OpenID, SAML and more)

# Identity Platform

- Built-in support for various social providers:
  - Facebook
  - Microsoft
  - Apple
  - Google
  - And more…

# Identity Platform

- Support for Multi-Factor Authentication (MFA)
- Using phone

# Identity Platform Pricing

- Based on:
  - Monthly Active Users (MAU)
    - The first 50K are free
  - SMS sent (price changes per country)

# Identity Platform Pricing

Identity Platform

MAU from Social, Anonymous, Email+Password and Phone : 80,000

**USD 165.00**

**Total Estimated Cost: USD 165.00 per 1 month**

Estimate Currency

USD - US Dollar

# ReadIt!

## Architecture: ReadIt Cloud System