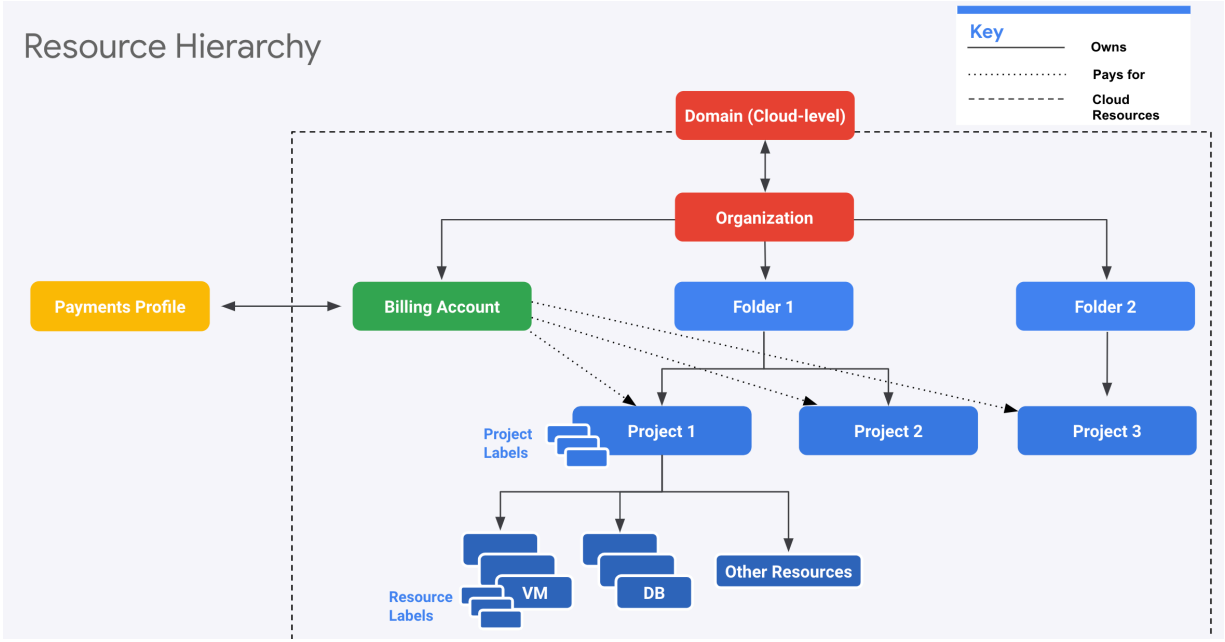
Organizing GCP Resources

Resource Hierarchy in GCP

- **Well defined hierarchy:**
  - Organization > Folder > Project > Resources
- **Resources** are created in projects
- A **Folder** can contain multiple projects
- **Organization** can contain multiple Folders



source: (*https://cloud.google.com*)

Resource Hierarchy - Recommendations for Enterprises

In28 Minutes

- Create **separate projects for different environments**:
  - Complete isolation between test and production environments
- Create **separate folders for each department**:
  - Isolate production applications of one department from another
  - We can create a shared folder for shared resources
- **One project per application per environment**:
  - Let's consider two apps: "A1" and "A2"
  - Let's assume we need two environments: "DEV" and "PROD"
  - In the ideal world you will create four projects: A1-DEV, A1-PROD, A2-DEV, A2-PROD:
    - Isolates environments from each other
    - DEV changes will NOT break PROD
    - Grant all developers complete access (create, delete, deploy) to DEV Projects
    - Provide production access to operations teams only!

Billing Accounts

In 28 Minutes

- **Billing Account** is mandatory for creating resources in a project:
  - Billing Account contains the payment details
  - Every Project with active resources should be associated with a Billing Account
- Billing Account can be associated with one or more projects
- You can have multiple billing accounts in an Organization
- (RECOMMENDATION) Create Billing Accounts representing your organization structure:
  - A startup can have just one Billing account
  - A large enterprise can have a separate billing account for each department
- Two Types:
  - **Self Serve** : Billed directly to Credit Card or Bank Account
  - **Invoiced** : Generate invoices (Used by large enterprises)

Managing Billing - Budget, Alerts and Exports

In28 Minutes

- Setup a **Cloud Billing Budget** to avoid surprises:
  - (RECOMMENDED) Configure **Alerts**
  - Default alert thresholds set at 50%, 90% & 100%
    - Send alerts to Pub Sub (Optional)
    - Billing admins and Billing Account users are alerted by e-mail
- Billing data can be **exported (on a schedule)** to:
  - **Big Query** (if you want to query information or visualize it)
  - **Cloud Storage** (for history/archiving)

IAM Best Practices

- **Principle of Least Privilege** - Give least possible privilege needed for a role!
  - Basic Roles are NOT recommended
    - Prefer predefined roles when possible
  - Use Service Accounts with minimum privileges
    - Use different Service Accounts for different apps/purposes
- **Separation of Duties** - Involve atleast 2 people in sensitive tasks:
  - Example: Have separate deployer and traffic migrator roles
    - AppEngine provides App Engine Deployer and App Engine Service Admin roles
      - App Engine Deployer can deploy new version but cannot shift traffic
      - App Engine Service Admin can shift traffic but cannot deploy new version!
- **Constant Monitoring:** Review Cloud Audit Logs to audit changes to IAM policies and access to Service Account keys
  - Archive Cloud Audit Logs in Cloud Storage buckets for long term retention
- Use Groups when possible
  - Makes it easy to manage users and permissions

User Identity Management in Google Cloud

In 28 Minutes

- Email used to create free trial account => **"Super Admin"**
  - Access to everything in your GCP organization, folders and projects
  - Manage access to other users **using their Gmail accounts**
- However, this is **NOT recommended** for enterprises
- **Option 1**: Your Enterprise is using **Google Workspace**
  - Use Google Workspace to manage users (groups etc)
  - Link Google Cloud Organization with Google Workspace
- **Option 2**: Your Enterprise uses an Identity Provider of its own
  - **Federate** Google Cloud with your Identity Provider

Cloud IAM

Corporate Directory Federation

In 28 Minutes

- **Federate** Cloud Identity or Google Workspace **with your external identity provider (IdP)** such as Active Directory or Azure Active Directory.

- **Enable Single Sign On**:
  - 1: Users are redirected to an external IdP to authenticate
  - 2: When users are authenticated, SAML assertion is sent to Google Sign-In
- **Examples**:
  - Federate Active Directory with Cloud Identity by using Google Cloud Directory Sync (GCDS) and Active Directory Federation Services (AD FS)
  - Federating Azure AD with Cloud Identity

IAM Members/Identities

- **Google Account** - Represents a person (an email address)
- **Service account** - Represents an application account (Not person)
- **Google group** - Collection - Google & Service Accounts
  - Has an unique email address
  - Helps to apply access policy to a group
- **Google Workspace domain**: Google Workspace (formerly G Suite) provides collaboration services for enterprises:
  - Tools like Gmail, Calendar, Meet, Chat, Drive, Docs etc are included
  - If your enterprise is using Google Workspace, you can manage permissions using your Google Workspace domain
- **Cloud Identity domain** - Cloud Identity is an Identity as a Service (IDaaS) solution that centrally manages users and groups.
  - You can use IAM to manage access to resources for each Cloud Identity account

IAM Members/Identities - Use Cases

In28 Minutes

Scenario	Solution
All members in your team have G Suite accounts. You are creating a new production project and would want to provide access to your operations team	Create a Group with all your operations team. Provide access to production project to the Group.
All members in your team have G Suite accounts. You are setting up a new project. You want to provide a one time quick access to a team member.	Assign the necessary role directly to G Suite email address of your team member If it is not a one time quick access, the recommended approach would be to create a Group
You want to provide an external auditor access to view all resources in your project BUT he should NOT be able to make any changes	Give them roles/viewer role (Generally basic roles are NOT recommended BUT it is the simplest way to provide view only access to all resources!)
Your application deployed on a GCE VM (Project A) needs to access cloud storage bucket from a different project (Project B)	In Project B, assign the right role to GCE VM service account from Project A

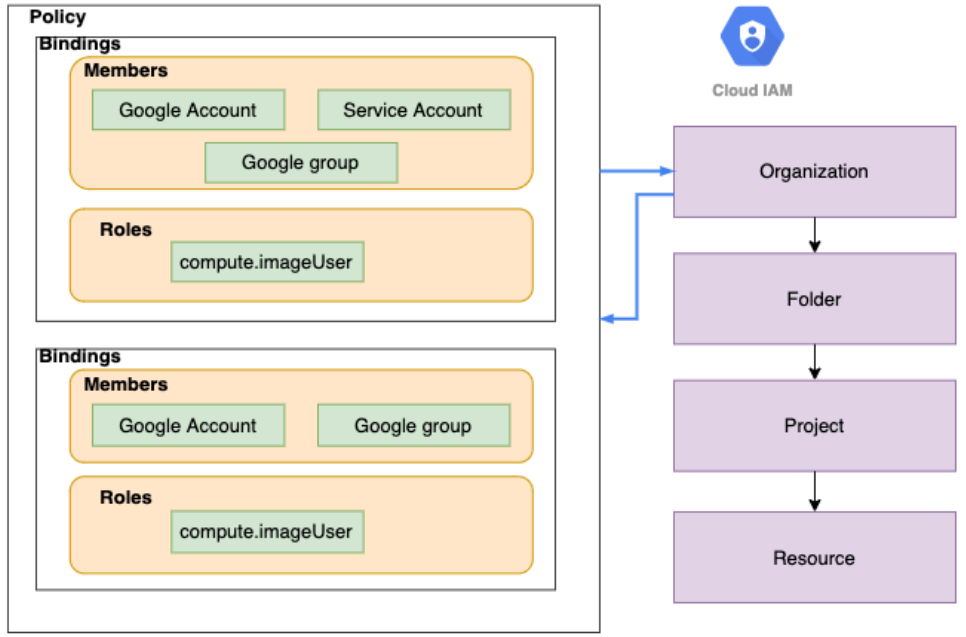
Organization Policy Service

In28 Minutes

- How to enable **centralized constraints** on all resources created in an Organization?
  - Configure **Organization Policy**
  - Example: Disable creation of Service Accounts
  - Example: Allow/Deny creation of resources in specific regions
- Needs a Role - Organization Policy Administrator
- (Remember) **IAM** focuses on **Who**
  - Who can take specific actions on resources?
- (Remember) Organization Policy focuses on **What**
  - What can be done on specific resources?

Resource Hierarchy & IAM Policy

- IAM Policy can be set at any level of the hierarchy
- Resources inherit the policies of **All parents**
- The effective policy for a resource is the union of the policy on that resource and its parents
- Policy inheritance is transitive:
  - For example: Organization policies are applied at resource level
- You can't restrict policy at lower level if permission is given at an higher level



Cloud BigQuery Roles

In28 Minutes

- Cloud BigQuery IAM Roles
  - **BigQuery Admin** - bigquery.*
  - **BigQuery Data Owner** - bigquery.datasets.*, bigquery.models.*, bigquery.routines.*, bigquery.tables.* (**Does NOT have access to Jobs!**)
  - **BigQuery Data Editor** - bigquery.tables.(create/delete/export/get/getData/getIamPolicy/list/update/updateData/updateTag), bigquery.models.*, bigquery.routines.*, bigquery.datasets.(create/get/getIamPolicy/updateTag)
  - **BigQuery Data Viewer** - get/list bigquery.(datasets/models/routines/tables)
  - **BigQuery Job User** - bigquery.jobs.create
  - **BigQuery User** - BigQuery Data Viewer + get/list (jobs, capacityCommitments, reservations etc)
- To see data, you need either BigQuery User or BigQuery Data Viewer roles
  - You CANNOT see data with BigQuery Job User roles
- BigQuery Data Owner or Data Viewer roles do NOT have access to jobs!

Corporate Directory Federation

- **Federate** Cloud Identity or Google Workspace **with your external identity provider(IdP)** such as Active Directory or Azure AD
- **Enable Single Sign On:**
  - 1: Users are redirected to an external IdP to authenticate
  - 2: When users are authenticated, SAML assertion is sent to Google Sign-In
- **Examples:**
  - Use Identity as a service (IDaaS) such as Okta as IdP (identity provider)
    - Use IDaaS (like Okta) for single sign-on
  - Use Active Directory as IdP
    - Use Active Directory Federation Services (AD FS) for single sign-on
    - Use Google Cloud Directory Sync to synchronize users and groups from Active Directory to Cloud Identity
  - Use Azure AD as IdP
    - Use Azure AD for single sign-on
    - Azure AD can be integrated with on-premises Active Directory