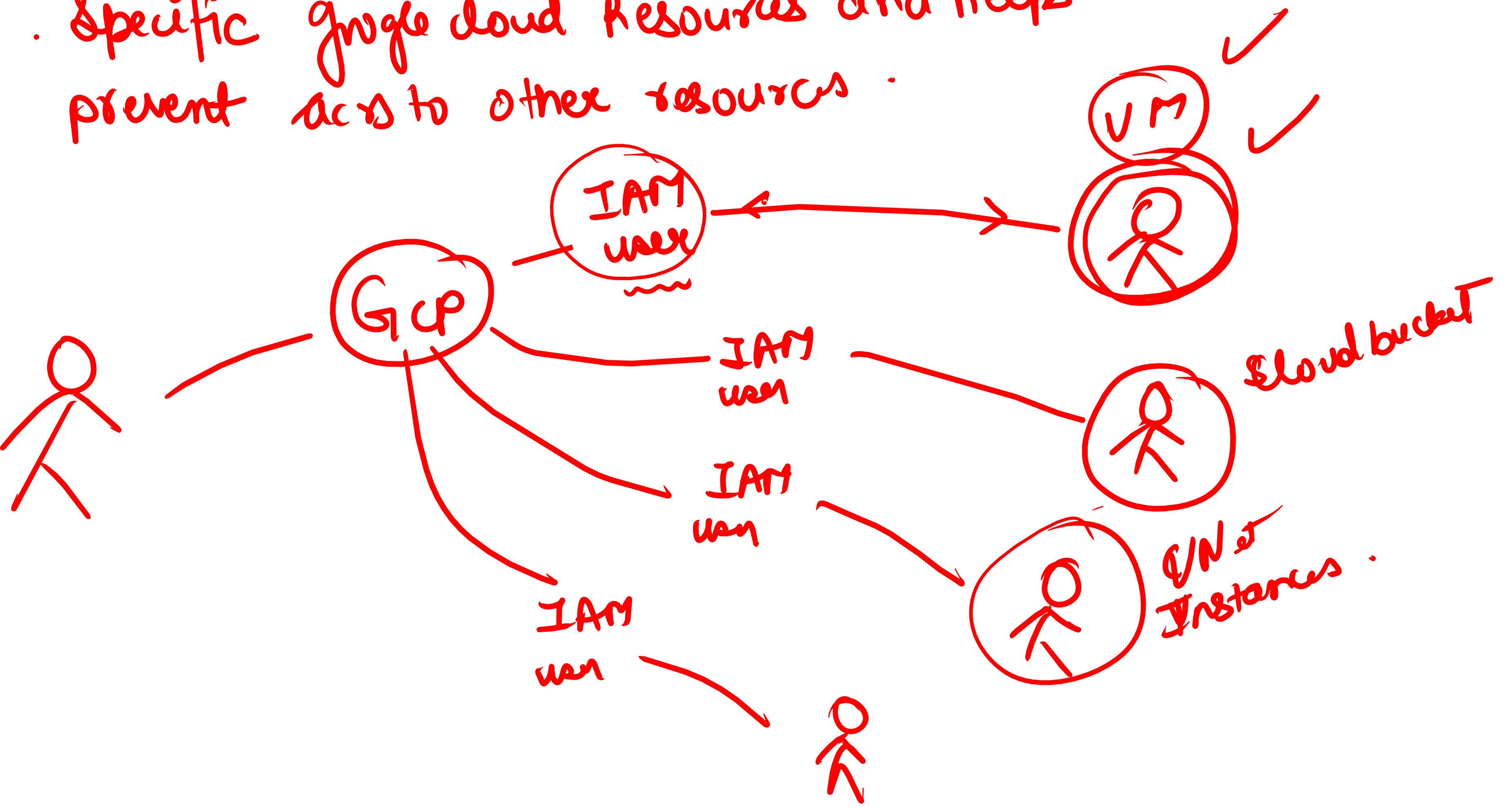
IAM lets you grant granular access to specific google cloud Resources and helps prevent access to other resources.

IAM → Identity & access management.

→ lets us adopt the security principal of least priviledge



features of IAM → who can do what

IAM has three important parts :-

Principal / members

1. google a/c ✓
2. Service a/c ✓
3. Google group
4. Google workspace.
5. cloud identity domain
6. All users.

Roles

Roles is the collection of permissions.

Permission determine what operation are allowed on a Resources.

Role

policy

A policy is a document that binds :-

- who (Principal)
- what (Role)
- where

(Resource : project, bucket, vm)

A policy is a rulebook which tells who gets which role on which resource

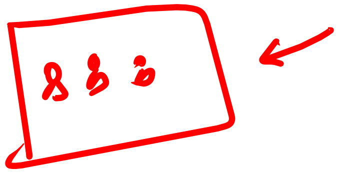
Principals

① Google a/c .

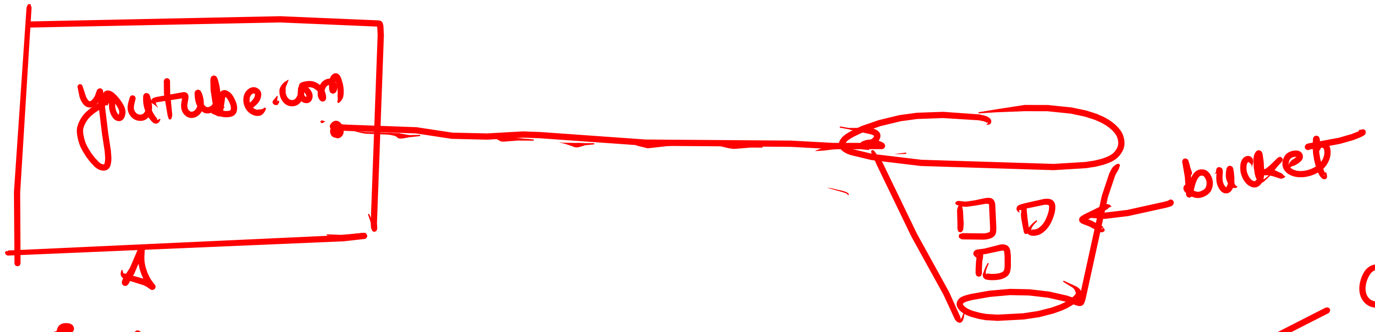
② service a/c . → A service a/c is an a/c for an app or compute workload instead of Individual end user .

google groups

collection of google a/c



Role to the group



Instance

we want VM to access cloud storage

vm-sa@ - - - -

Create a service a/c

Grant Role

roles/storage.objectviewer

attach the service a/c to VM

Principals

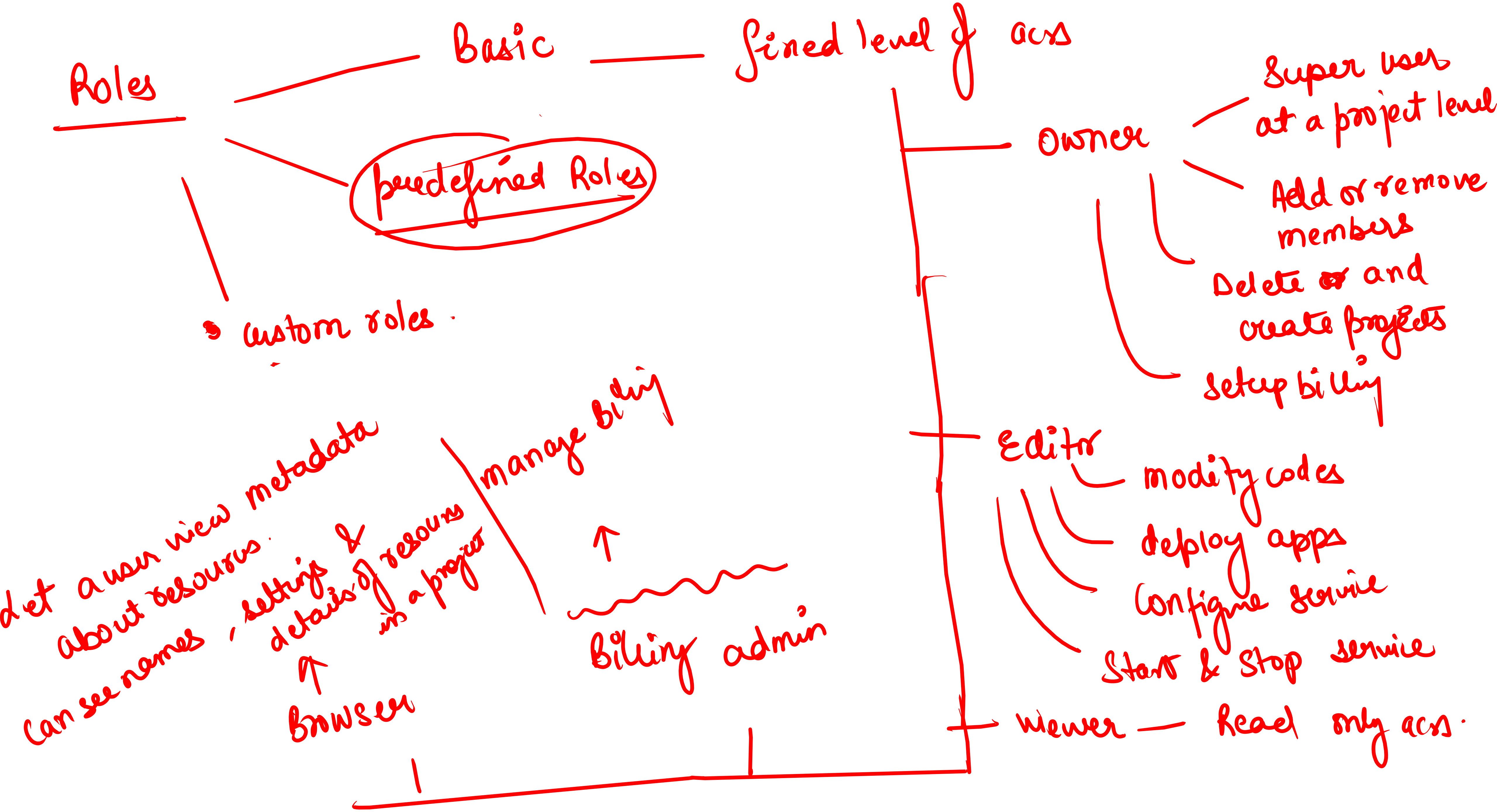
④ Google workspace a/c. ✓

abc@company.com

⑤ All authenticated user ÷ The value allauthenticated user is a special identifier that represents all service a/c and all users on Internet who have authenticated with a google a/c.

⑥ All users ✓

The value alluser is a special identifier that represent anyone who is on internet, including authenticated & unauthenticated user.



Roles

Basic — fined level of acs

predefined Roles

custom roles.

Owner

Super user at a project level

Add or remove members

Delete ~~or~~ and create projects

setup billing

Editor

modify codes

deploy apps

Configure service

Start & stop service

Viewer — Read only acs.

Billing admin

manage billing

Browser

Let a user view metadata about resources

can see names, settings & details of resources in a project

Predefined roles → Google created roles with specific set of permissions designed for common tasks.

They are more fine grained than the Basic roles

e.g
roles/compute.admin → full control over compute engine.

roles/compute.instanceAdmin.v1 → Managed only VM Instances

roles/storage.admin → full control over buckets

Custom roles → A role you create yourself, with only permissions you want.

e.g ÷ Create a role that allows a user to start/stop compute engine Instance, but not delete them.

IAM → Create roles

Name ← vmOperator

Add permission — compute.instance.start

— compute.instance.stop.

Save the role

Bind it to the user.