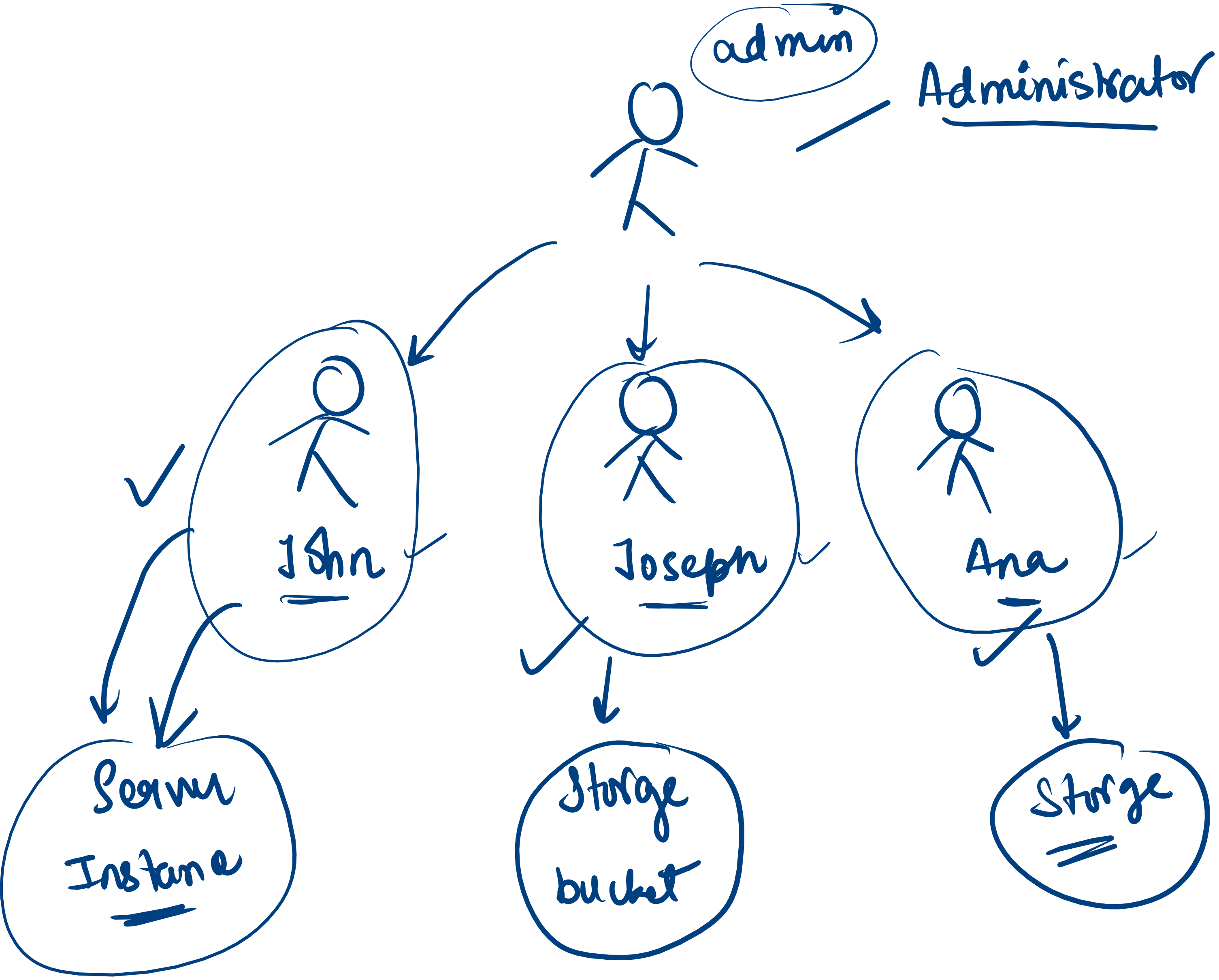
IAM (IDENTITY and ACCESS management)



IAM is a service in GCP that lets u control who (identity) can do what (role/permission) on which resource

It helps you securely manage access to your gcp resources

IAM lets you adopt the security principle of least priviledge , which states that no body should have more permissions then they actually need

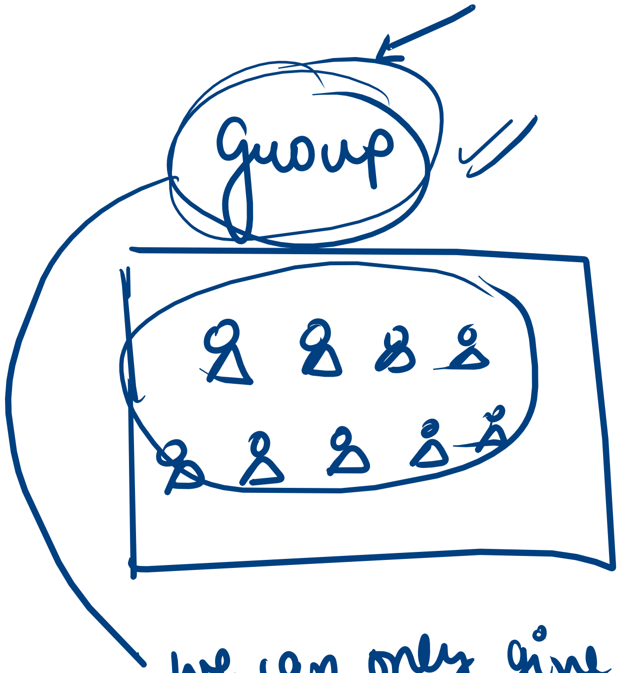
MAIN COMPONENTS :

1) Identities (Who?)

These are the users or the services that need the access

Examples:

> google account (your personal or work email)
> Service account (used by apps or VPms)
> google group



we can only give permission to Group we do not have to give it individualy

2. Roles (what can they do ?)

A collection of permissions (like read , write and delete) that allows you to perform specific actions on google cloud

Types:
Basic role: Owner, Editor , Viewer
Predefined roles: Storage admin , compute viewer
Custom roles: you create your own combination of permissions

OWNER: Superuser at a project level , Add and remove the users, Delete and crrate project , Setup billing for projects

EDITOR: Modify codes, Deploy apps , Configure services, Start and stop and services

Viewer: Read only access

Billing admin : Manage billing

Predefined role :

>Provides granular access for specific services and is managed and defined by google cloud

> Prevents unwanted access to other resources

like instance read permission

>Custom role :

Provides granualar acces according to user defined list of permissions
you can create a custom iam role with one or more permissiosn and then grant that custom role to user or group

Principal : The identity (user/service) who is doing something

Role: What they are allowed to do

Resources : what they are acting on