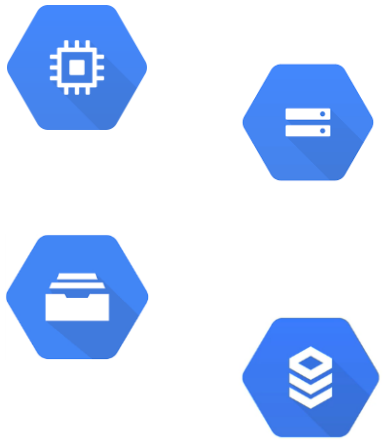
INTRODUCTION TO GOOGLE CLOUD IAM

Members	Permission	Resources
• User 1 • User 2 • . • . • User n	• Owner • Viewer • Editor • Compute.InstanceAdmin • Storage.objectAdmin	

- IAM controls access by defining **roles** (Permissions) for **who** (Members/Identity) on **which** resources
- Permissions determine the operations performed on resources
- Associated with the REST API of resources
- Cloud IAM is developed from the least privilege principle

ROLES & TYPES OF ROLES

- ROLE is a named collection of permissions that provide the ability to perform actions on the resources
- We cannot directly grant users permissions in IAM. Instead, we grant them roles, which bundle one or more permissions
- There are three types of roles in Google Cloud IAM
  - Basic Roles
    - Includes Owner, Editor, and Viewer role
  - Predefined Roles
    - GCP is responsible for updating and adding permissions as necessary
    - **roles/notebooks.admin ; roles/ml.modelUser**
  - Custom Roles
    - Provides granular access according to a user-defined list of permissions
    - We can create a custom IAM role with one or more permissions and then grant that custom role to users or groups
- Multiple roles can be assigned to a user or a group

IAM MEMBERS (IDENTITY)

- Members, also know as Identity can be
  - User account
  - Service account
  - Google group
  - G suite domain
  - Cloud Identity domain
  - alias
    - allauthenticatedUsers
    - allusers