Cloud

Module 3

[2:00:00]
lecture 8

IAM → Identity and access management

↳ Who can perform What actions on Which resources

* Who (Identity)
* What (Roles)
* Which

Pricing :- All use of Identity and Access Management API is free of charge

* Types of Identities in Google Cloud (Who)

1. Google account (user) → only a/c able to login to console.
2. Service account (Applicatn component)
3. G-Suite Domain (All members of a specified domain)
4. Cloud Identity Domain (——do——)
5. Google Group (All members of the group)

* Types of Roles (What)

1. Primitive Roles :- Broad Access Spans across services.
   - Three Roles :- Owner
     Editor
     Viewer

2. Predefined Roles :- Narrow Access Permission to a single service Hundreds of roles:
   - Service Admin
   - Service Viewer
   - So on

3. Custom Roles :- Customized Access, create from scratch or from existing.
   e.g. compute instance admin without permission to assign external IPs.

LAB :-

#1 ↳ go to IAM & admin → +Add
   - New members (gmail)
   - Select a role (e.g Project - Editor) - Save

#2 ↳ go to another browser and select the project and switch.
   as editor i can create VM but not add IAM.

#1 ↳ again go to IAM for predefined Roles.
   - Select a role - Compute Engine - Compute Admin
   - Save

#2 ↳ go and create VM if not done

#1 ↳ add one more Role - Service a/c - Service a/c user.
   Now try.

Dt. _____ Pg. _____

to add bucket you add Role
– Storage – Storage Admin
Now able to create Bucket

Custom Role :– to combine Roles.

#1 ↳ go to IAM – Roles – ~~Create~~ Search Compute Engine – create Role –
Name and ID should be different.
↳ Add permission
Search Storage Admin – select All – Add – create
↳ Now go to IAM
edit that user – remove all – add another – custom – Custom created Role

#2 Try to create VM only nothing else work.

~~~

* Represents a set of fined grained permission
e.g
Service . Resource type, verb
storage . buckets . create
iam . service account . delete
compute . disk , list
bigquery . tables . update
~~~

By using command line.

↳ Search 'owner' → click Cloud Shell
→ type :- gcloud iam roles describe roles/owner
:- clear
:- gcloud iam roles describe roles/owner | less

Policy and Bindings

↳ Policies connect the resource, roles and members via bindings

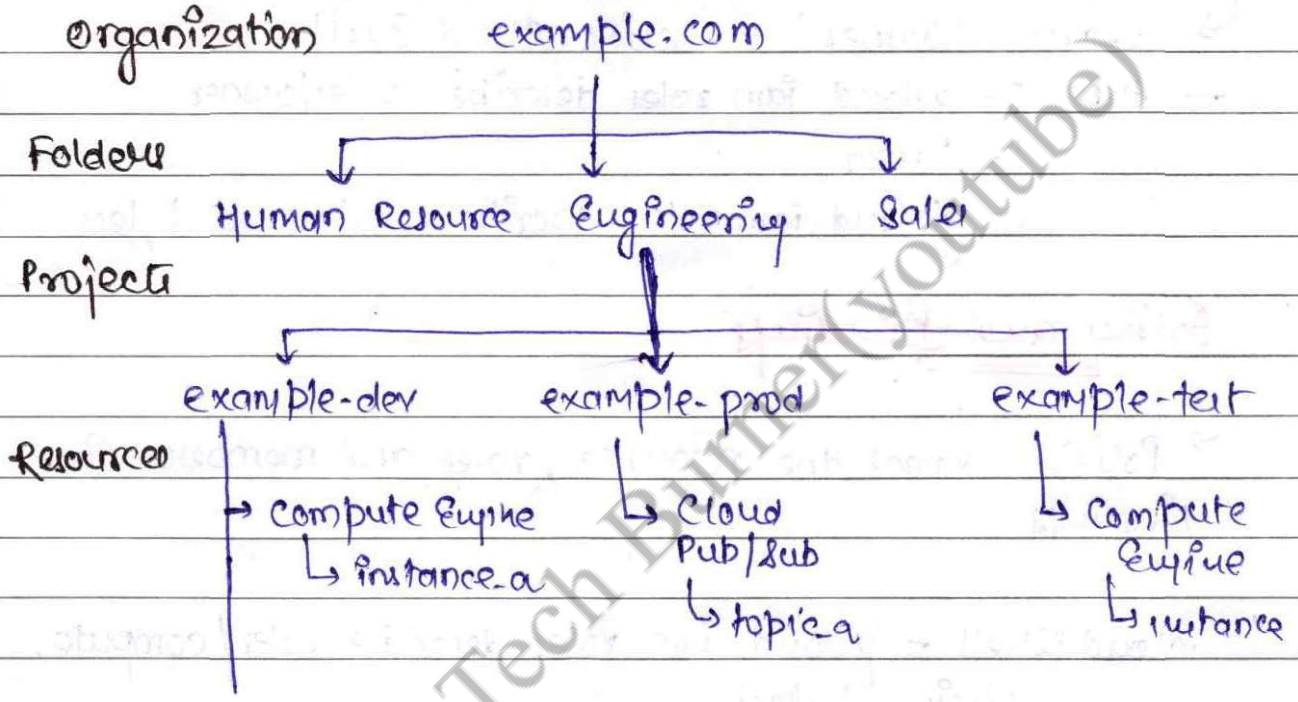
↳ cloud shell - gcloud iam roles describe roles/compute.admin | less

to filter the owner/editor/viewer so on.

↳ go to filter - Role: owner or.
↳ go to cloud shell
- gcloud projects get-iam-policy [Proj. ID] --format json > demo.json
- echo $DEVSHELL_PROJECT_ID → $DEVSHELL_PROJECT_ID

Dt. _____ Pg. _____

Resource Hierarchy



* Policy inheritance is transitive. (slide)

Service Account

- Identity of a Service
- Compute Engine can have only one service a/c.
- Multiple GCE instances can use the same service a/c.
- Normal user a/c can use password or key to authenthic but service a/c ~~or~~ use only key. Upto 10 service a/c keys per service a/c can be created.
- Two types of Service Account
  - → Google Managed service Account
  - → User Managed Service Account
- Upto 100 service accounts per project (including the default compute Engine service a/c and the App Engine service a/c) can be created.

Create Service A/c :-

↳ go to IAM – Service a/c → create
Name – service account-webconsole
ID – ~~do~~
Descrip – Service a/c created in web console.
– create –
Role – ~~Project~~ Compute Engine : Compute Admin
– Add –
Now we will use this identity and create a VM

can we upload a file to a bucket.

Dt. _____ Pg. _____

↳ go to VM — create
— Name : svc-demo
—
— Identity and API — select your service a/c
— create — ssh

↳ go to storage — create bucket
Name — learniy-svc-gcs
— create

↳ SSH — gcloud auth list
— vi test.txt
— gsutil cp test.txt gs://learniy-svc-gcs

doesn't have permission go back to IAM

↳ select that created one — edit — Add role
— Storage : Storage object creator
admin

— we write command:
gsutil cp test.txt ....
— cat gs://learniy-svc-gcs

Hiiy command live —DONE—
?