Identity Aware Proxy (IAP)

IAP

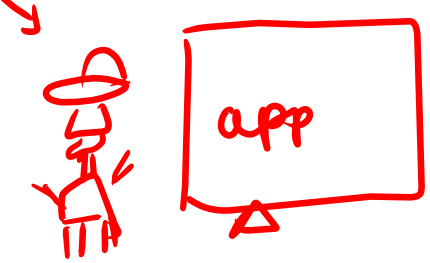
It is a security feature in GCP that helps control accs to your web application & VM based on Identity of the user.

IAP sits in front of your app. and only allows accs to users who are authenticated & authorized.

Think IAP, like a security guard at the gate

It checks → who is the person

Then ask → 'Are they allowed to enter''



How IAP works ?

① user request accss to a protected Resource (e.g https:// my-app.com)

② IAP Intercepts the request.

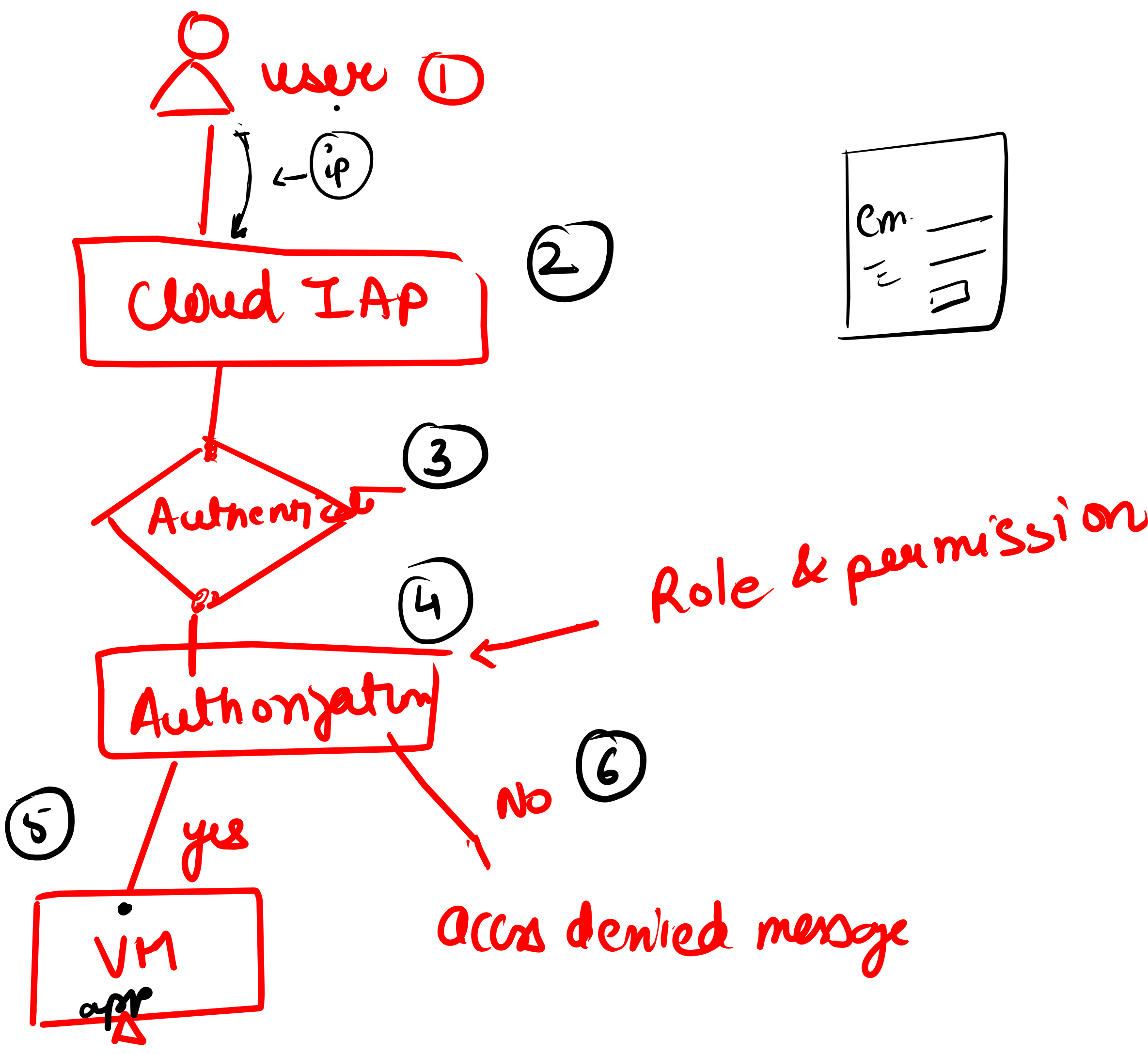
③ IAP checks:

→ Is the user authenticated ?
(If no, it redirects to google login)

④ Does the user have right IAM role? (permission)

⑤ If yes, the request is forwarded to your app

⑥ If No, the user get accss denied msg



where is it used?

→ web app hosted on App Engine, compute Engine, GKE or cloud Run.

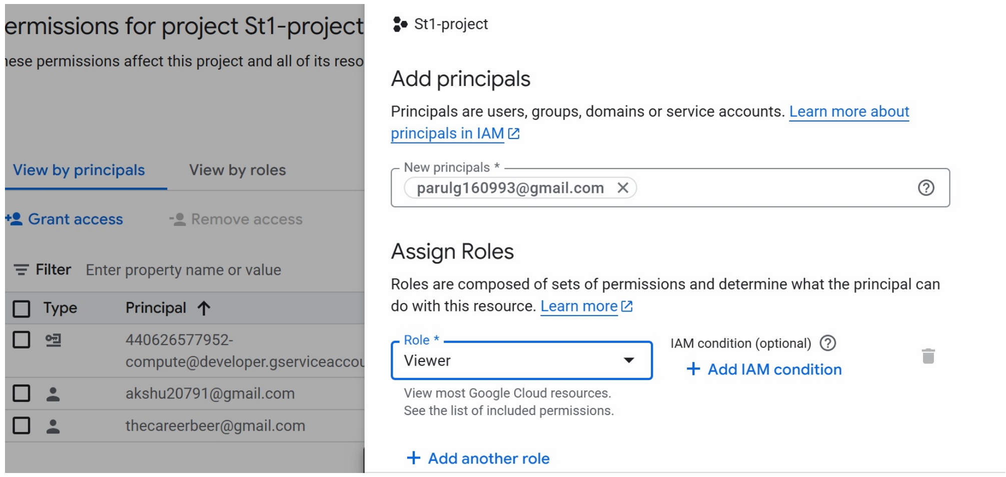
→ Internal admin dashboards, internal tools etc . . .

AGENDA FOR LAB: restrict a specific user to perform ssh to my private machine. for this we need to give the intercept permissionn via iap

1) create a VM(private VM) . to create private vm in networking disable external ip address : none
create

2) Install GCP CLI if it is not already installed in ur laptop
https://cloud.google.com/sdk/docs/install
After installation command prompt will open ...u can select ur existing project

3) Go to IAM -> GRand access -> New principle :parulg160993@gmail.com (u use ur other mail id)
role -> basic -> viewer



ermissions for project St1-project

iese permissions affect this project and all of its reso

View by principals   View by roles

Grant access   Remove access

Filter   Enter property name or value

	Type	Principal ↑
□		440626577952-compute@developer.gserviceaccou
□		akshu20791@gmail.com
□		thecareerbeer@gmail.com

St1-project

Add principals

Principals are users, groups, domains or service accounts. Learn more about principals in IAM

New principals *
parulg160993@gmail.com ✕

Assign Roles

Roles are composed of sets of permissions and determine what the principal can do with this resource. Learn more

Role *
Viewer

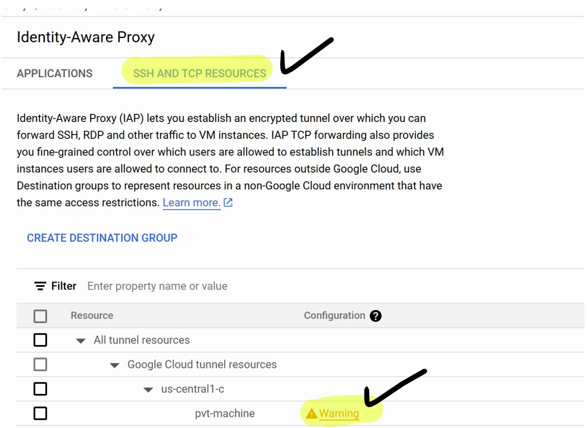
View most Google Cloud resources.
See the list of included permissions.

IAM condition (optional)

+ Add IAM condition

+ Add another role

4) Search for IAP from gcp console



Identity-Aware Proxy

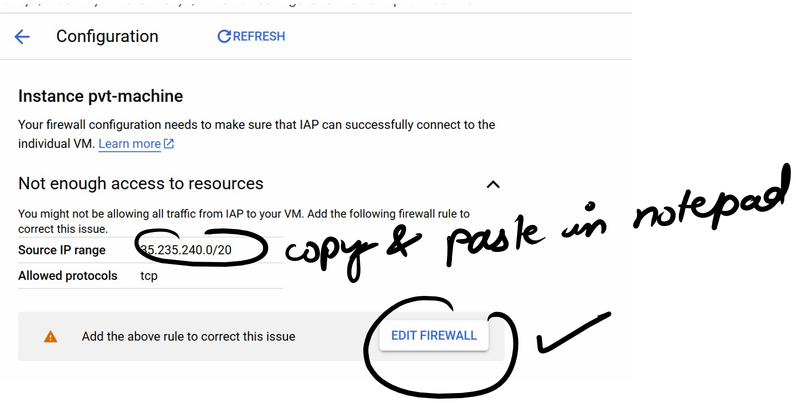
APPLICATIONS | SSH AND TCP RESOURCES ✓

Identity-Aware Proxy (IAP) lets you establish an encrypted tunnel over which you can forward SSH, RDP and other traffic to VM instances. IAP TCP forwarding also provides you fine-grained control over which users are allowed to establish tunnels and which VM instances users are allowed to connect to. For resources outside Google Cloud, use Destination groups to represent resources in a non-Google Cloud environment that have the same access restrictions. Learn more.

CREATE DESTINATION GROUP

Filter Enter property name or value

	Resource	Configuration
□	All tunnel resources	
□	Google Cloud tunnel resources	
□	us-central1-c	
□	pvt-machine	⚠ Warning ✓



Configuration REFRESH

Instance pvt-machine

Your firewall configuration needs to make sure that IAP can successfully connect to the individual VM. Learn more

Not enough access to resources

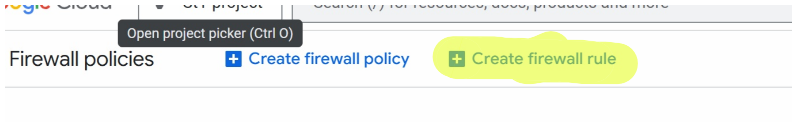
You might not be allowing all traffic from IAP to your VM. Add the following firewall rule to correct this issue.

Source IP range	35.235.240.0/20
Allowed protocols	tcp

copy & paste in notepad

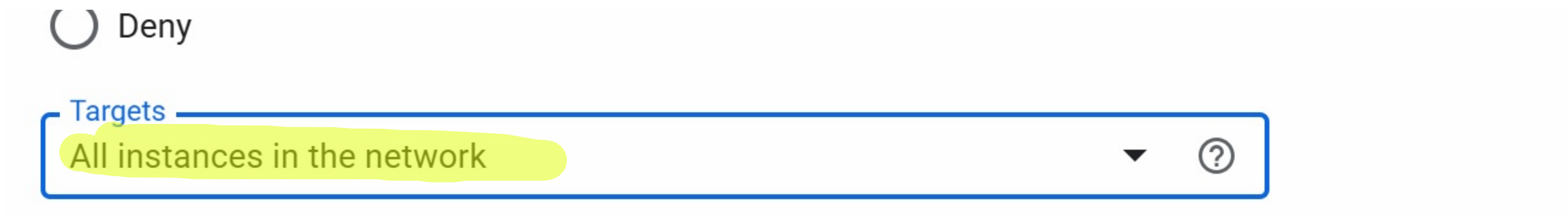
⚠ Add the above rule to correct this issue EDIT FIREWALL ✓

click on edit firewall



Create firewall rule

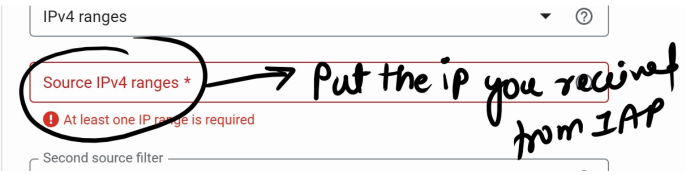
Give name as : iaprules



○ Deny

Targets: All instances in the network

in source ip range put the ip range u received from iap



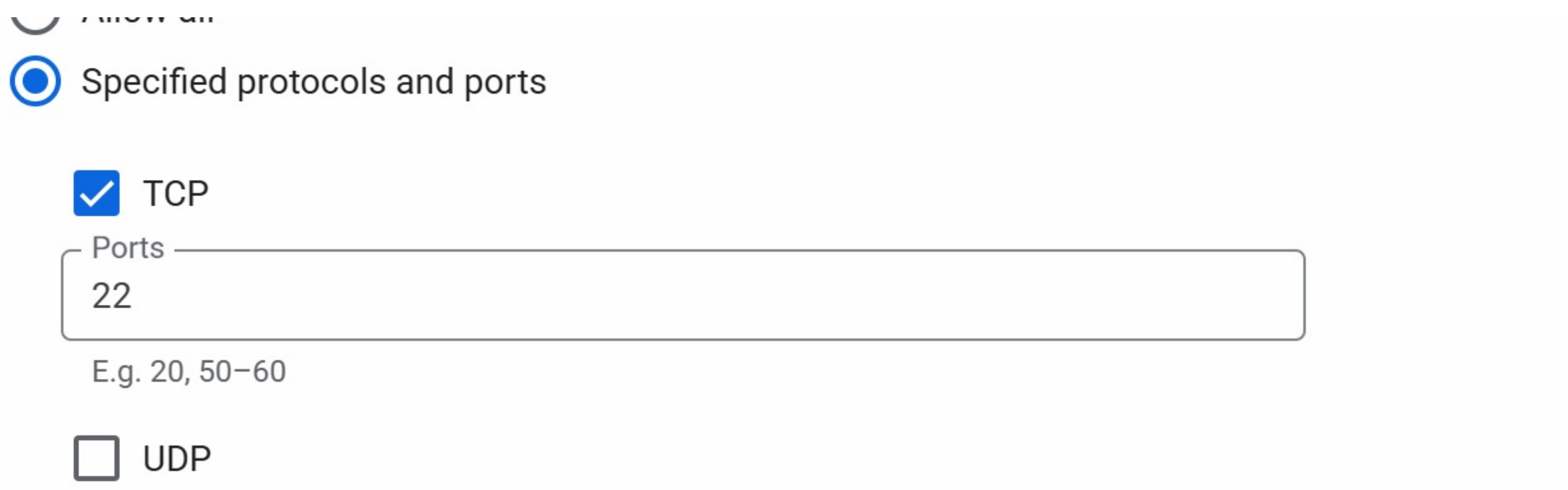
IPv4 ranges

Source IPv4 ranges *

At least one IP range is required

Second source filter

Put the ip you recived from IAP



● Specified protocols and ports

☑ TCP

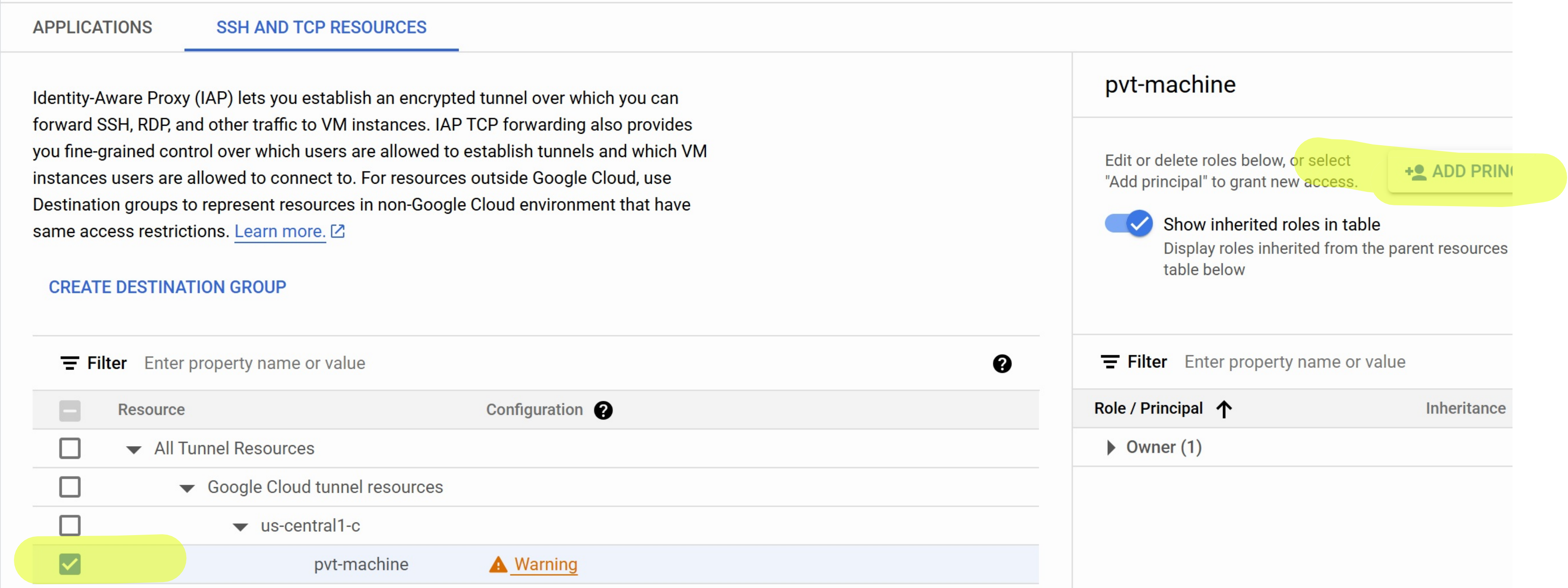
Ports: 22

E.g. 20, 50–60

□ UDP

Create

We need to authenticate via iap ...so need the user as iap as well
go to iap -> ssh and tunner resources



APPLICATIONS | SSH AND TCP RESOURCES

Identity-Aware Proxy (IAP) lets you establish an encrypted tunnel over which you can forward SSH, RDP, and other traffic to VM instances. IAP TCP forwarding also provides you fine-grained control over which users are allowed to establish tunnels and which VM instances users are allowed to connect to. For resources outside Google Cloud, use Destination groups to represent resources in non-Google Cloud environment that have same access restrictions. Learn more.

CREATE DESTINATION GROUP

Filter Enter property name or value

	Resource	Configuration
□	All Tunnel Resources	
□	Google Cloud tunnel resources	
□	us-central1-c	
☑	pvt-machine	⚠ Warning

pvt-machine

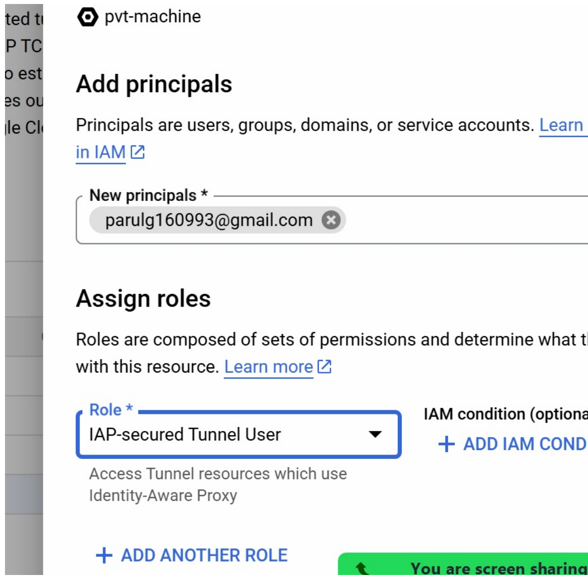
Edit or delete roles below, or select "Add principal" to grant new access.

ADD PRIN

☑ Show inherited roles in table
Display roles inherited from the parent resources table below

Filter Enter property name or value

Role / Principal ↑	Inheritance
Owner (1)	



pvt-machine

Add principals

Principals are users, groups, domains, or service accounts. Learn in IAM

New principals *
parulg160993@gmail.com

Assign roles

Roles are composed of sets of permissions and determine what t with this resource. Learn more

Role *
IAP-secured Tunnel User
Access Tunnel resources which use Identity-Aware Proxy

IAM condition (optiona
+ ADD IAM COND

+ ADD ANOTHER ROLE

You are screen sharing

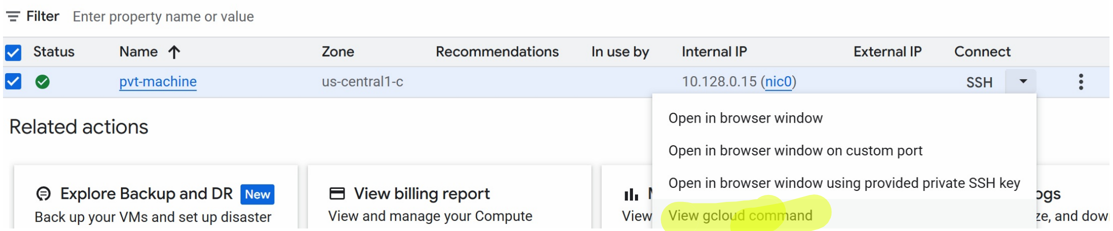
Add

Now the open the CMD which opened when u downloaded the GCP CLI

gcloud auth login

it will open the browser . here select the mail which u want to give access..in our case if parulg160993@gmail.com

>>> LETS NOW START TRYING CONNECTING WITH THE MACHINE>>>>>



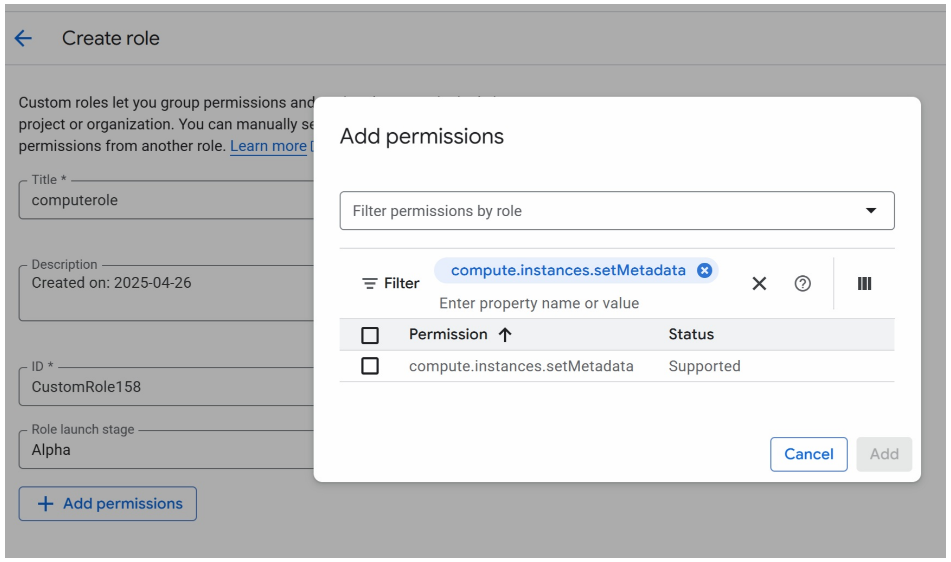
Filter   Enter property name or value

☑ Status	Name ↑	Zone	Recommendations	In use by	Internal IP	External IP	Connect
☑ ✓	pvt-machine	us-central1-c			10.128.0.15 (nic0)		SSH ▾

Open in browser window
Open in browser window on custom port
Open in browser window using provided private SSH key
View gcloud command
Related actions
Explore Backup and DR New
Back up your VMs and set up disaster
View billing report
View and manage your Compute
View
ogs
ze, and dow

copy the command which comes in front of u
and paste it in the cmd

You will get some errors while doing ssh to the machines
In IAM -> ROLES -> CREATE A NEW ROLE
Title : compute-roles
+ Add permission -> compute.istances.setMetadata



Create role

Custom roles let you group permissions and project or organization. You can manually se permissions from another role. Learn more

Title *
computerole

Description
Created on: 2025-04-26

ID *
CustomRole158

Role launch stage
Alpha

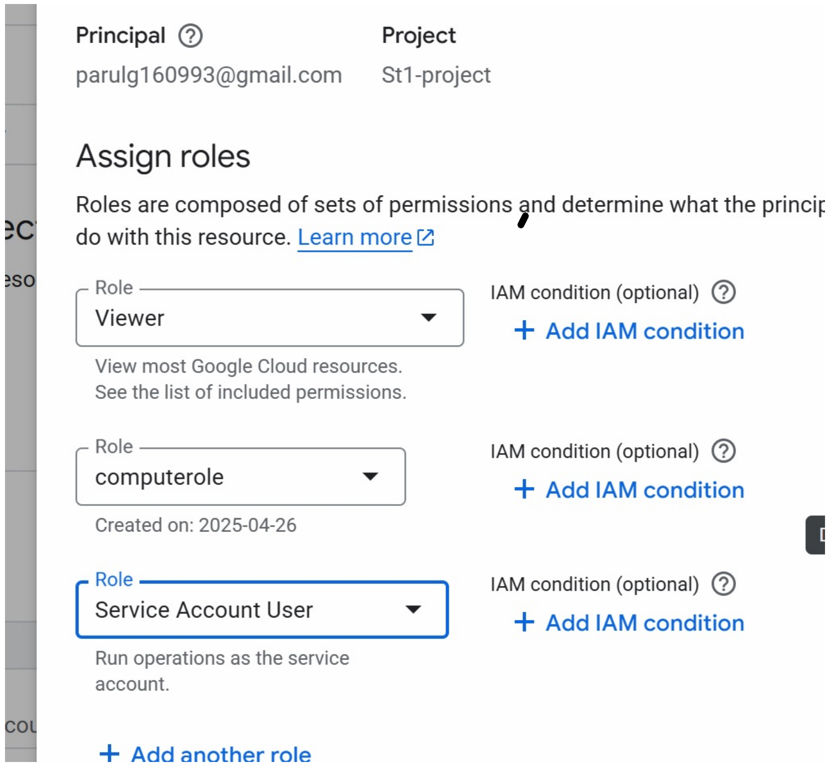
Add permissions

Filter permissions by role

Filter compute.instances.setMetadata
Enter property name or value

☐	Permission ↑	Status
☐	compute.instances.setMetadata	Supported

Go back to iam -> select the user -> Click on pencil button to edit in front of user



Principal ⓘ parulg160993@gmail.com

Project St1-project

Assign roles

Roles are composed of sets of permissions and determine what the princip do with this resource. Learn more

Role: Viewer — IAM condition (optional) ⓘ + Add IAM condition

View most Google Cloud resources. See the list of included permissions.

Role: computerole — IAM condition (optional) ⓘ + Add IAM condition

Created on: 2025-04-26

Role: Service Account User — IAM condition (optional) ⓘ + Add IAM condition

Run operations as the service account.

+ Add another role

Save

now if you try to do ssh again you will able to connect