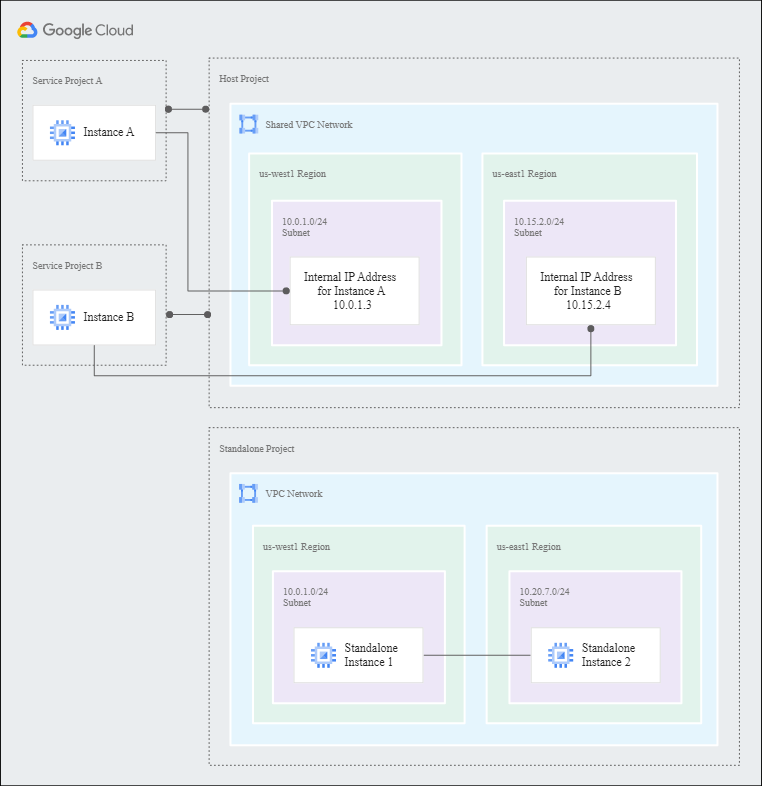
**SHARED-VPC on GCP**

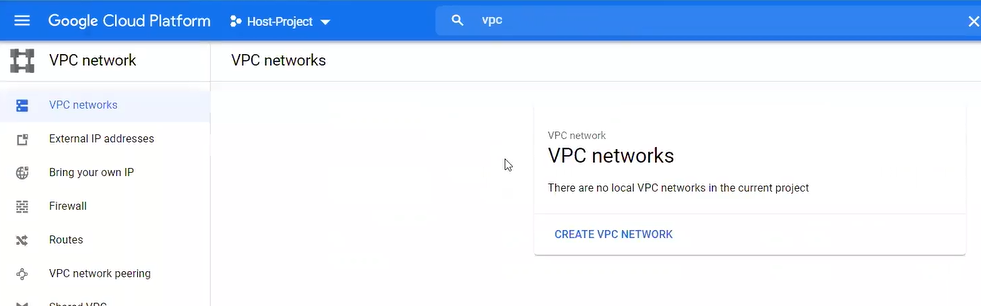
To implement Shared-VPC both n/w should be on that organisation, shared VPC Admin role should be there who are going to enable/XPN also called as shared VPC, Network User permissions also.

**host project**: which can capable to create shared VPC (only Organisation)

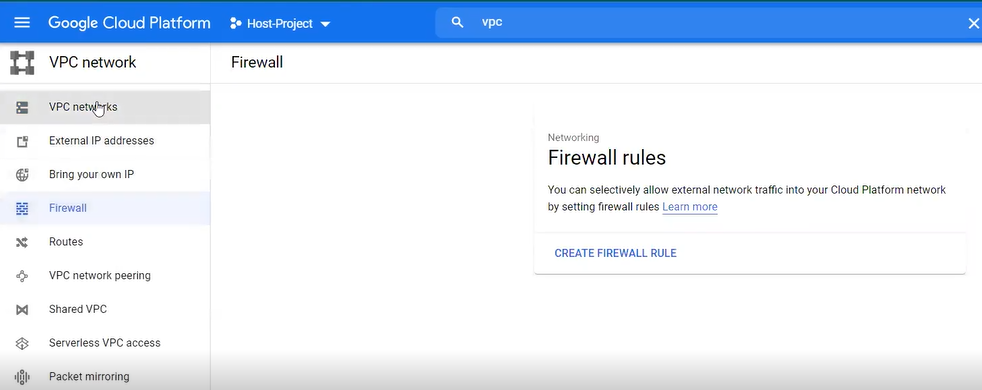
who can create shared VPC he should be having Shared VPC Admin, Anyone using Shared VPC he (service user) need: Compute Network User Role



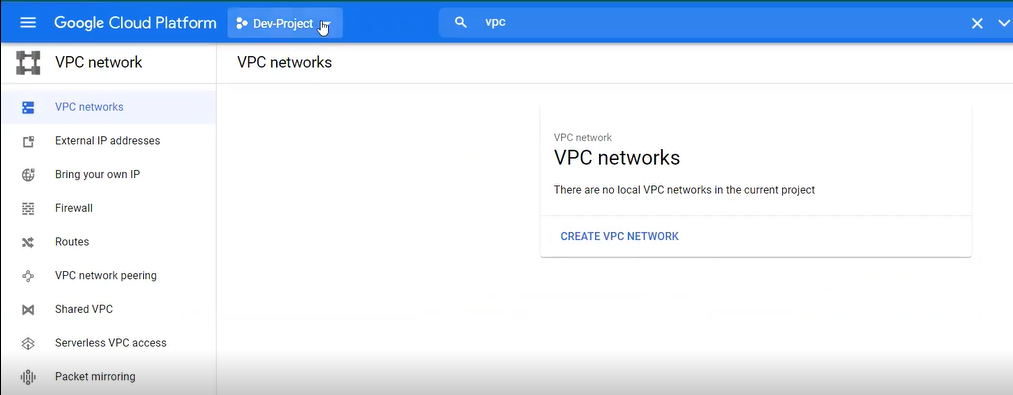
on host project no VPC’s



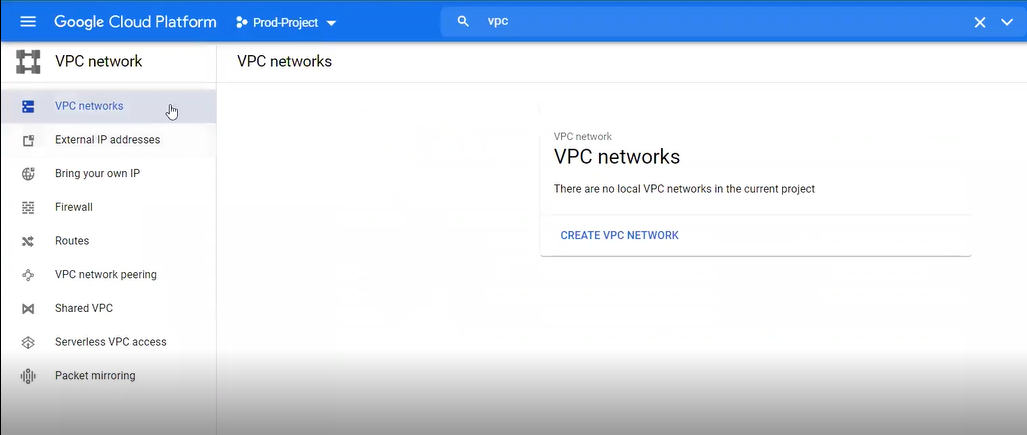
No firewalls



Dev project

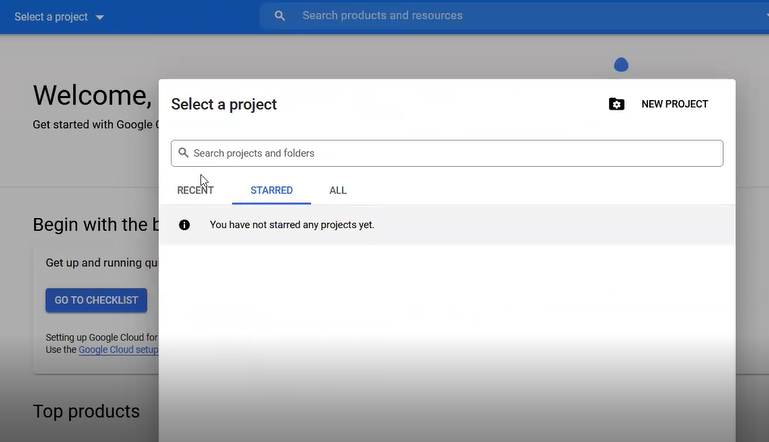


Prod Project

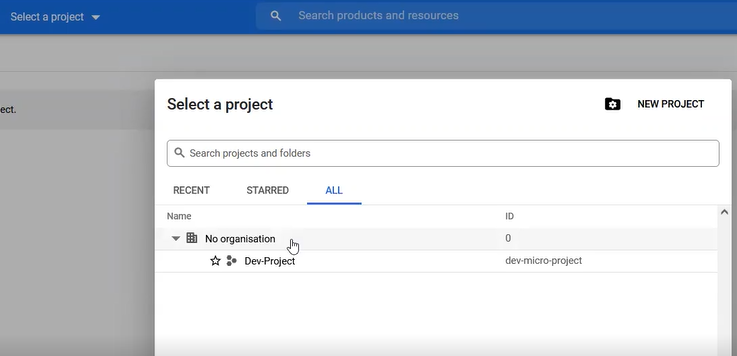


Service user:

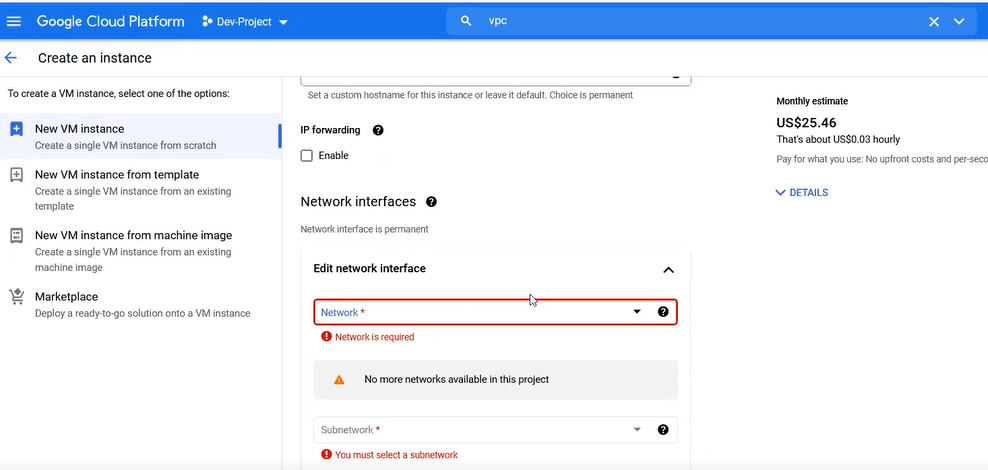
No project access, provide access to Dev-Project to service user like compute admin role



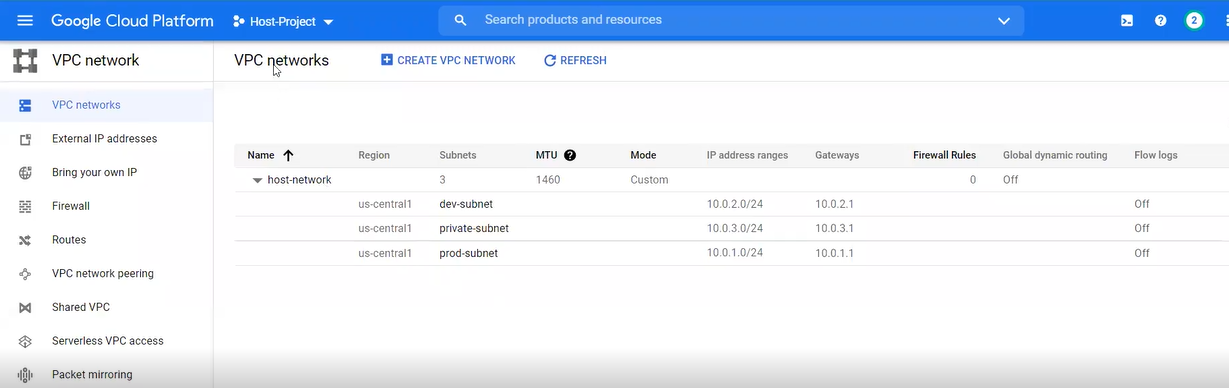
Now Service user having access to Dev-Project, like any normal user and to see organisation he need organisation viewer role



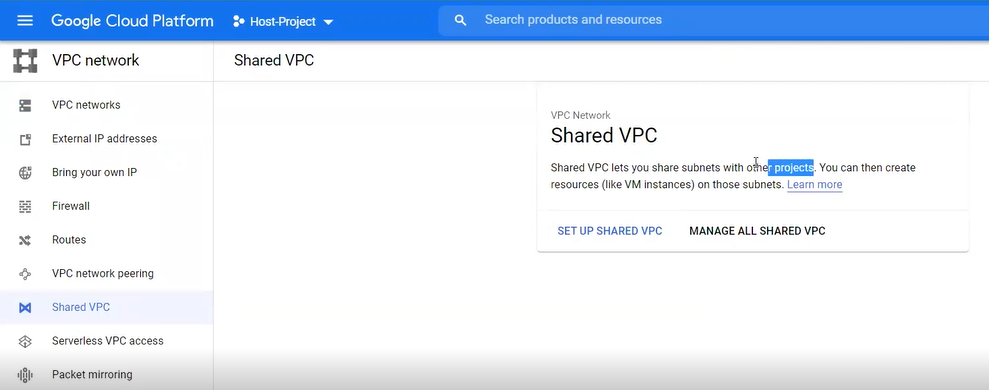
To create a VM, service user don’t have to create a n/w, he need n/w and that is going to be inherited from Host-Project.



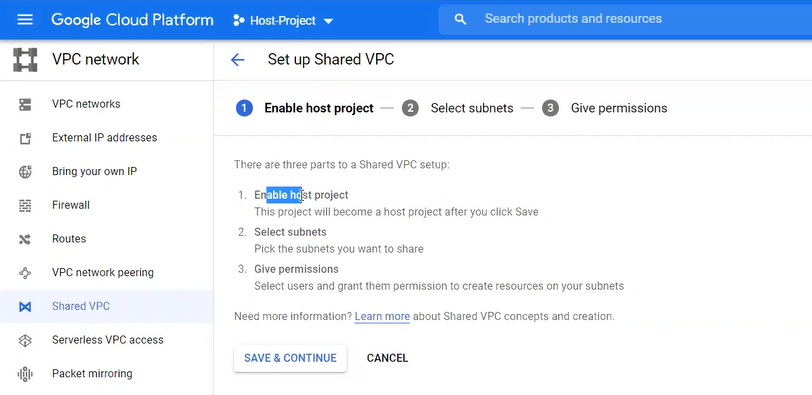
Create VPC network from Host-Project



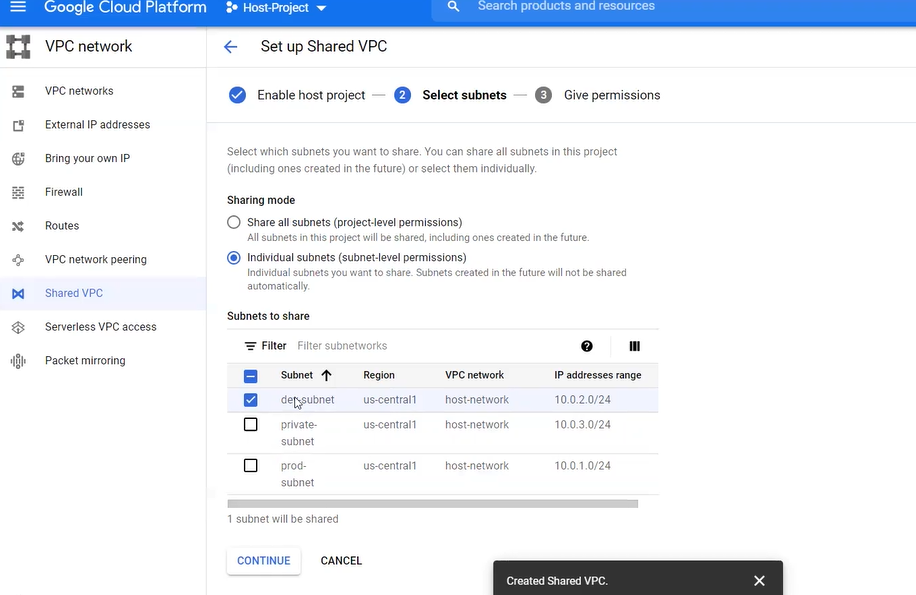
From Host-Project it will be enabled Shared-VPC to all the projects or required projects



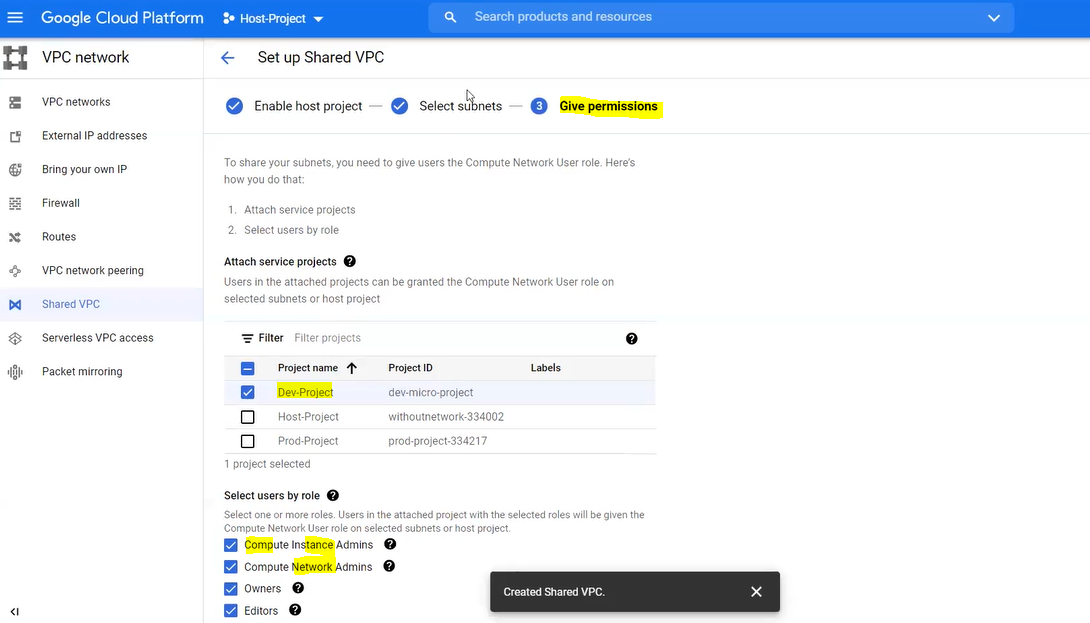
Enable Host-Project, and share projects as needed



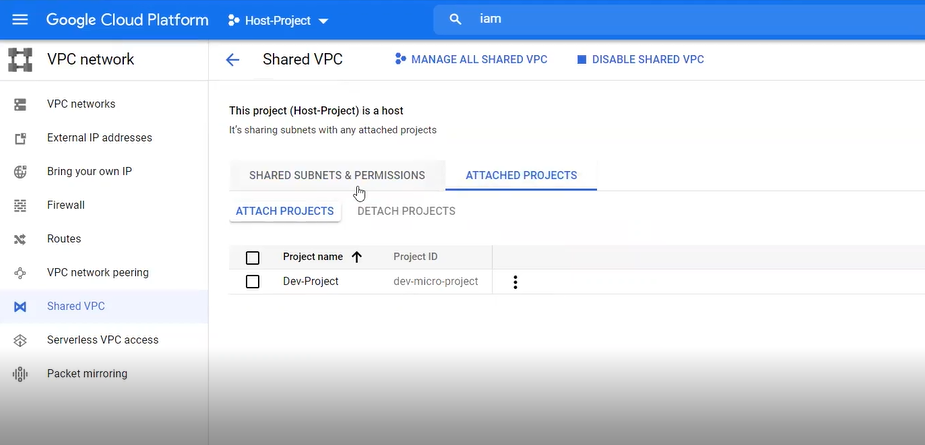
Select required subnet for the users which you want to share like here Dev-Subnet



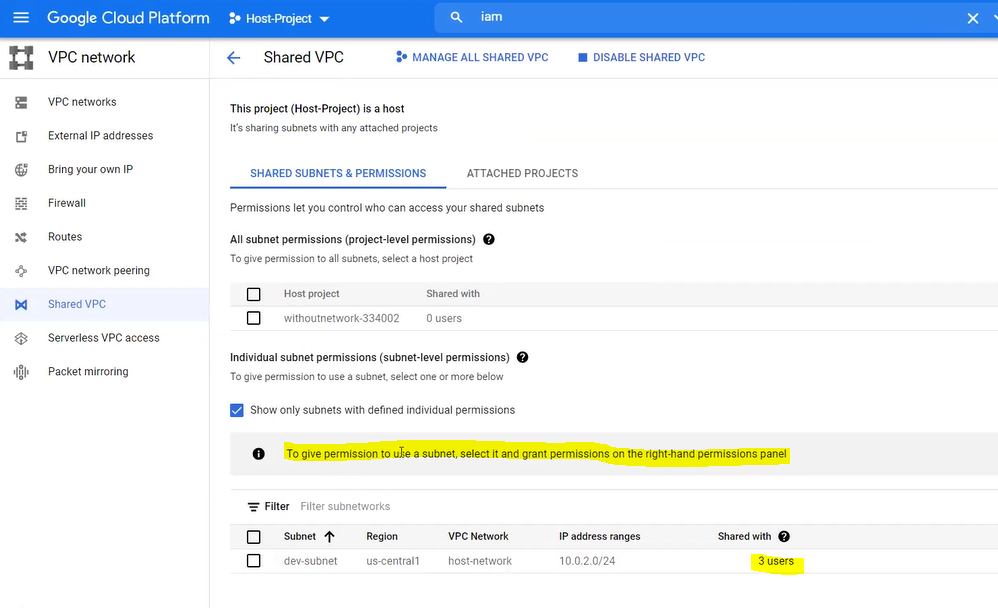
Select permissions for the project and save what service users can do actions

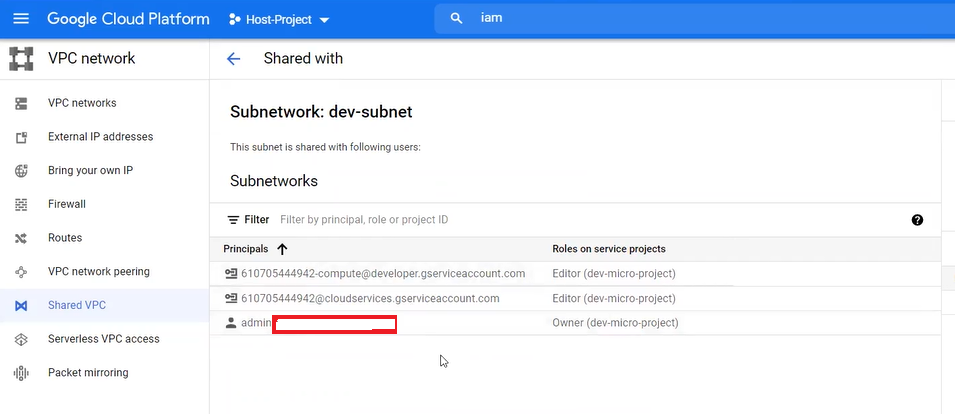


If need you can attach projects also in future

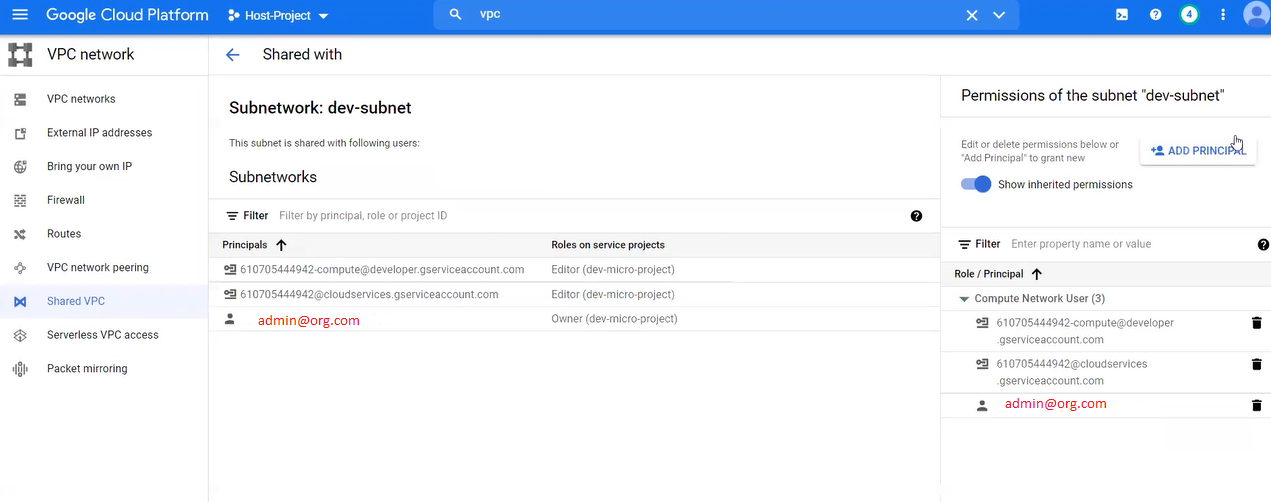


By default, service accounts and admin of organisation will have access by default

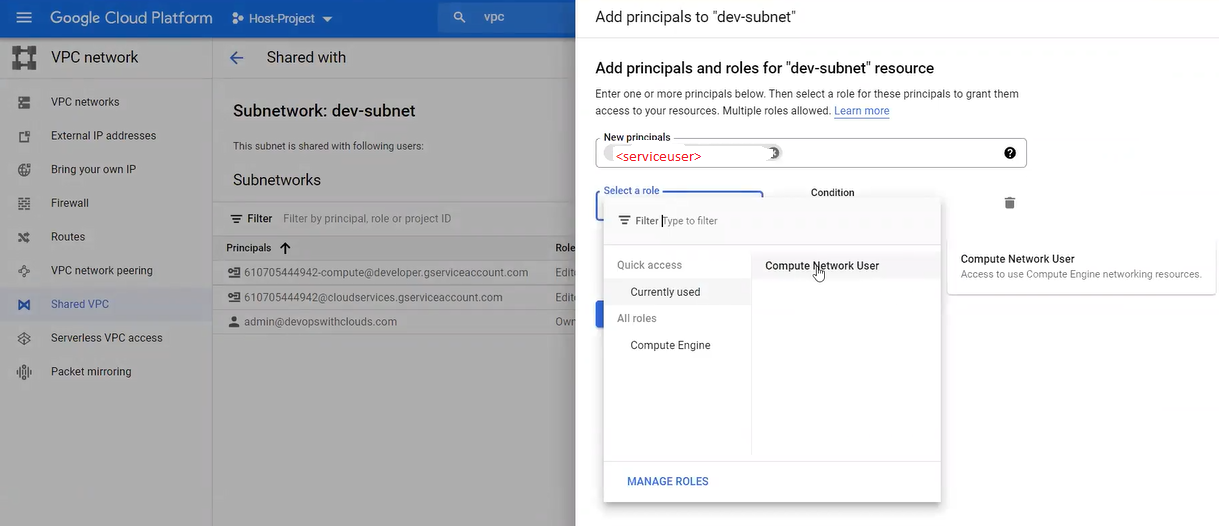




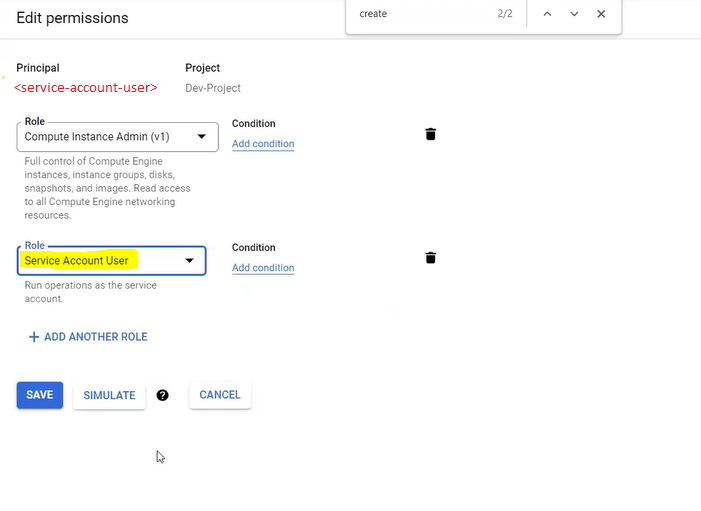
ADD PRINCIPAL for service account user



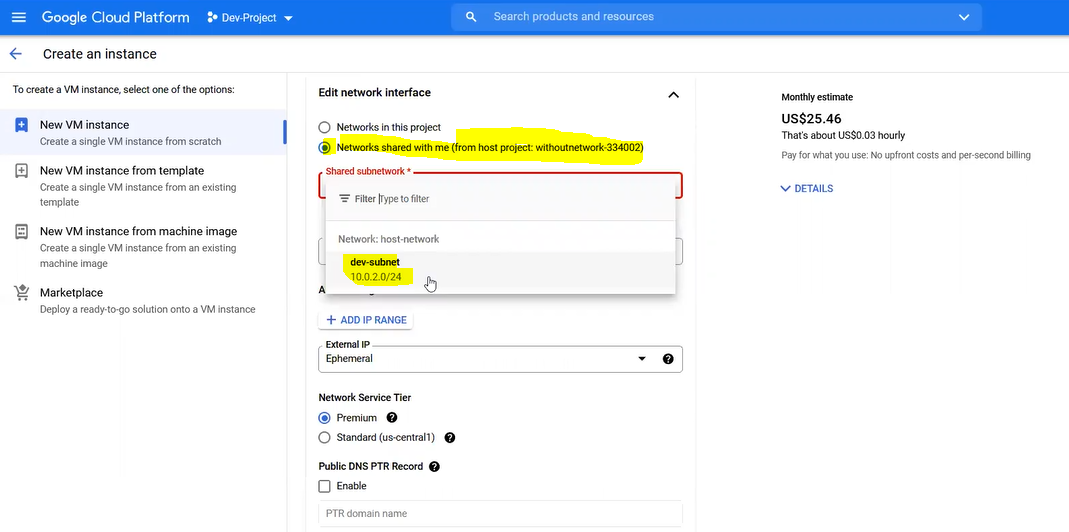
Provide service user email, assign Compute Network User role and service account user must have Service Account User Role.



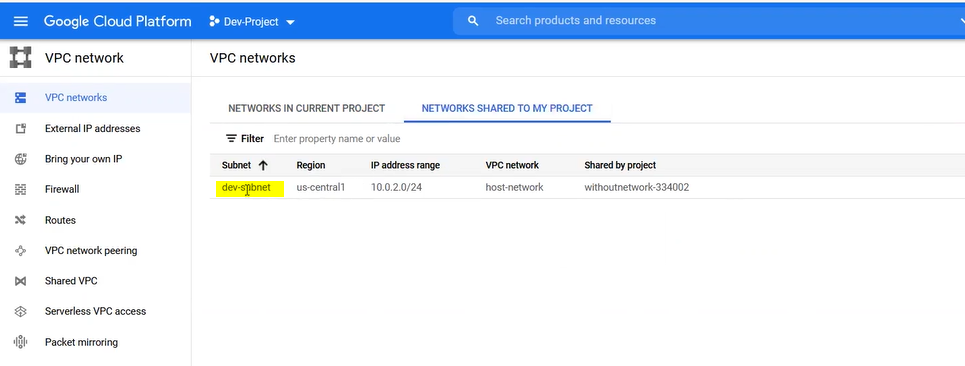
Service account user must need Service Account Permissions to create instances:



Now Service user will be able to select the subnet what is required based on region.

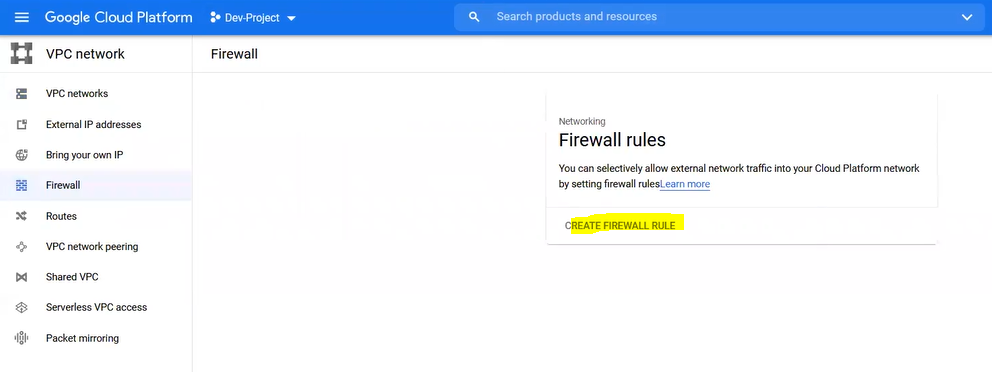


Now on Dev-Project for Service User you will able to see dev-subnet

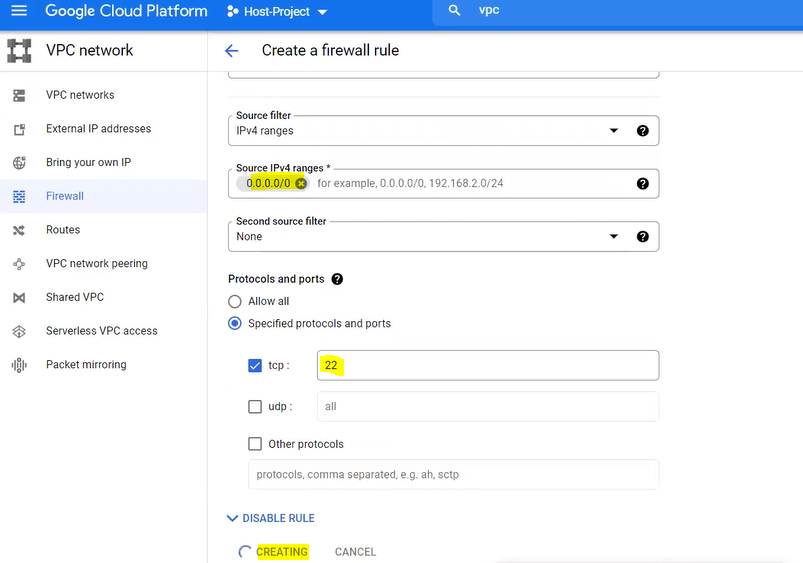


To access or connect VM’s(like ssh) you will not for a new shared VPC bcoz you will not have firewalls defined, you cannot create firewalls only N/w Admins will create them at org level.

Note: Generally, organisation level firewalls will be configured that will be used



N/w admins will create org level Firewalls at Host-Project a

Now you will able to login or access VM’s

