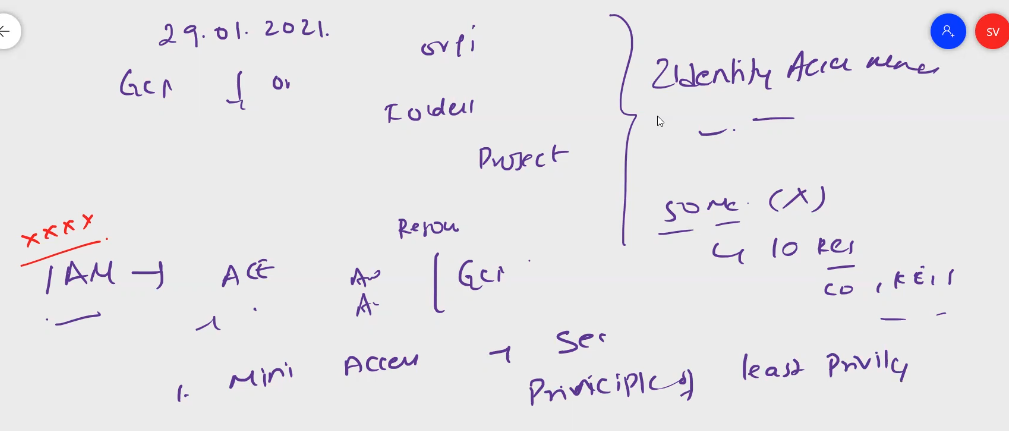
IAM

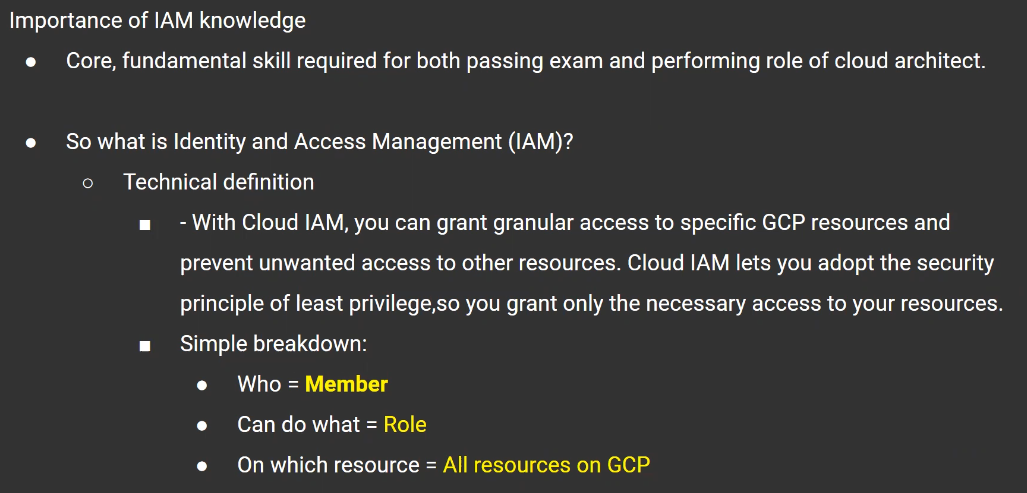
IAM is the one of the core component of the Google cloud platform



Using IAM we can implement Principles of least privileges

We can assign permissions, roles to set the security levels on resoureses

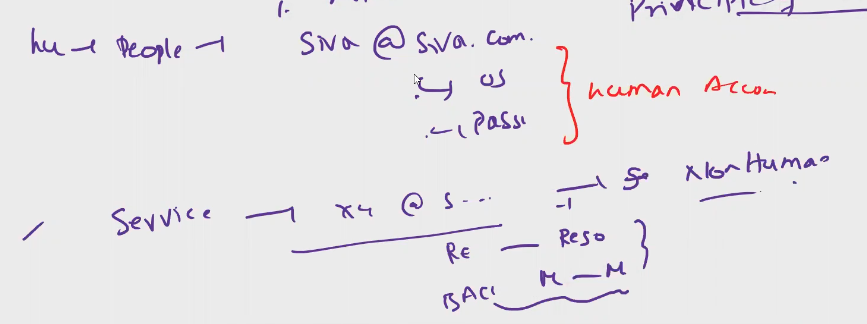
Google defined the below definition for IAM







Who means member identification to set the security permissions to access the google resources



Service accounts are configured for specific service which is running continuously without interruption

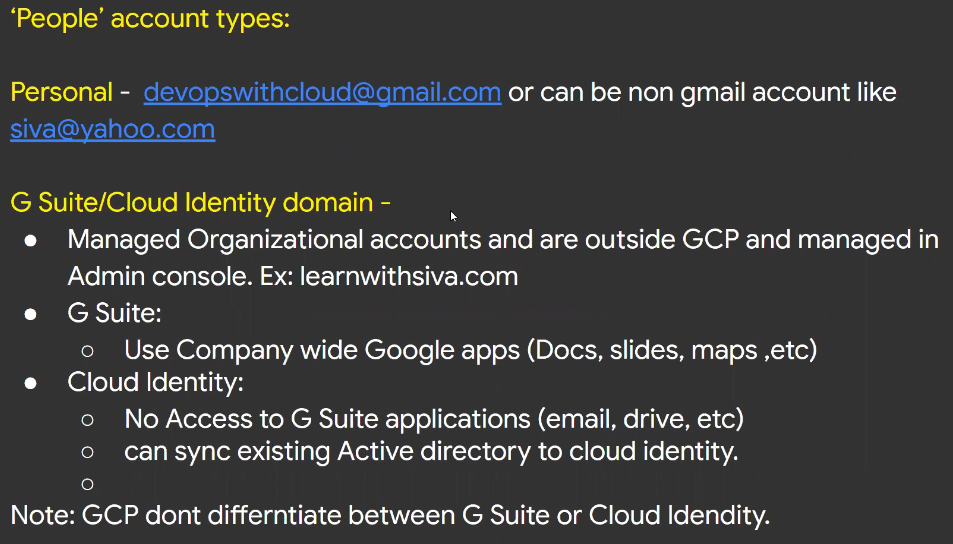
Once created service accounts can not be deleted or removed – non humon accouts

\*int – when new emp comes how to assign access –

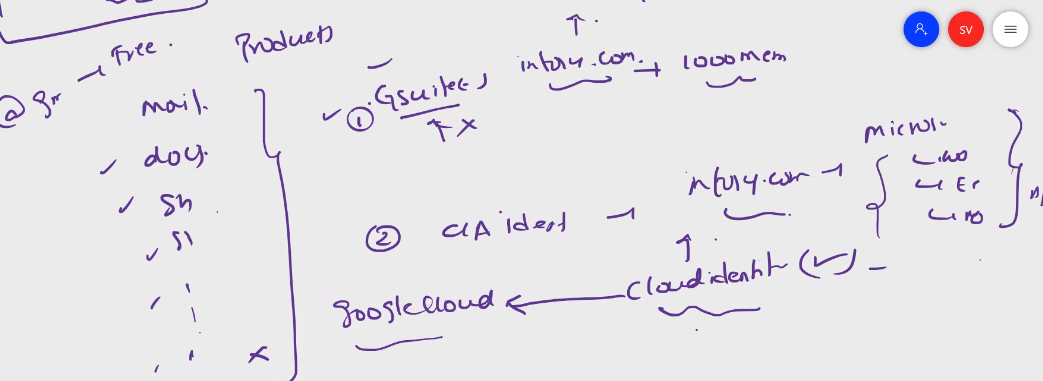
Organization emails never create in google cloud – should create in google cloud admin console

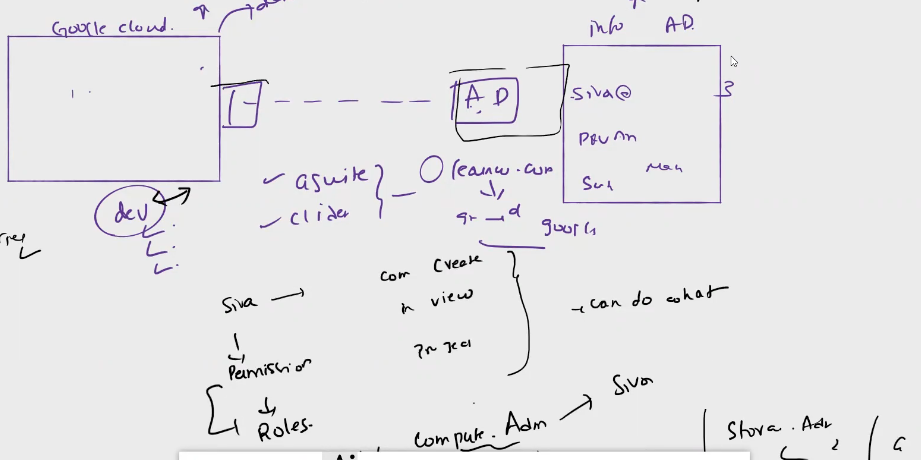
In other clouds ex aws and azure, user creation can be done with in cloud console, but in gcp user creation can be done outside the google cloud

Service accounts only can be created with in the cloud



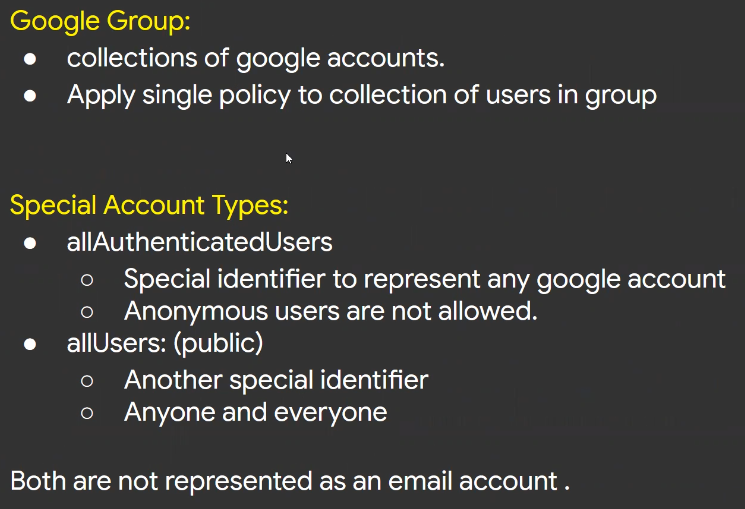
Int- what is gsuite and cloud identity accounts in gcp

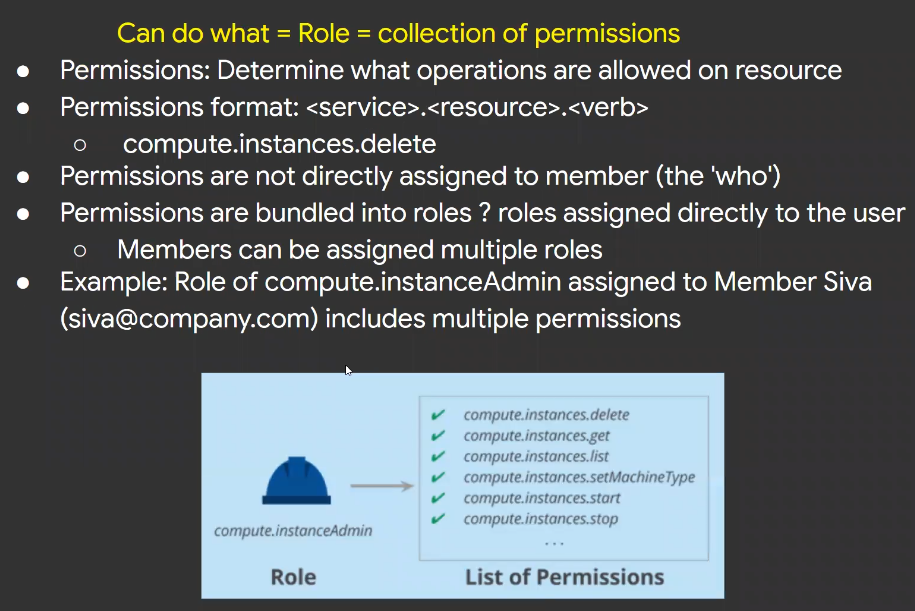


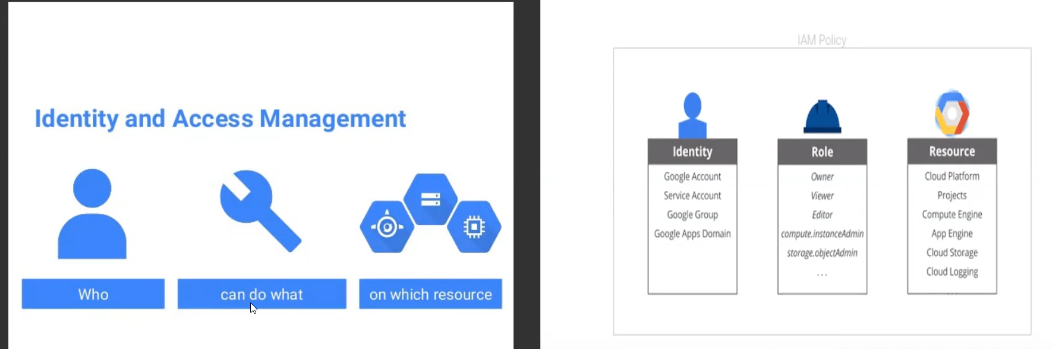


When we want to integrate user accounts from other cloud environments, we need to sync with that domain in gcp to access the google cloud resources (ex. From azure AD to gcp admin console integration), for AD integration need to use ADSync

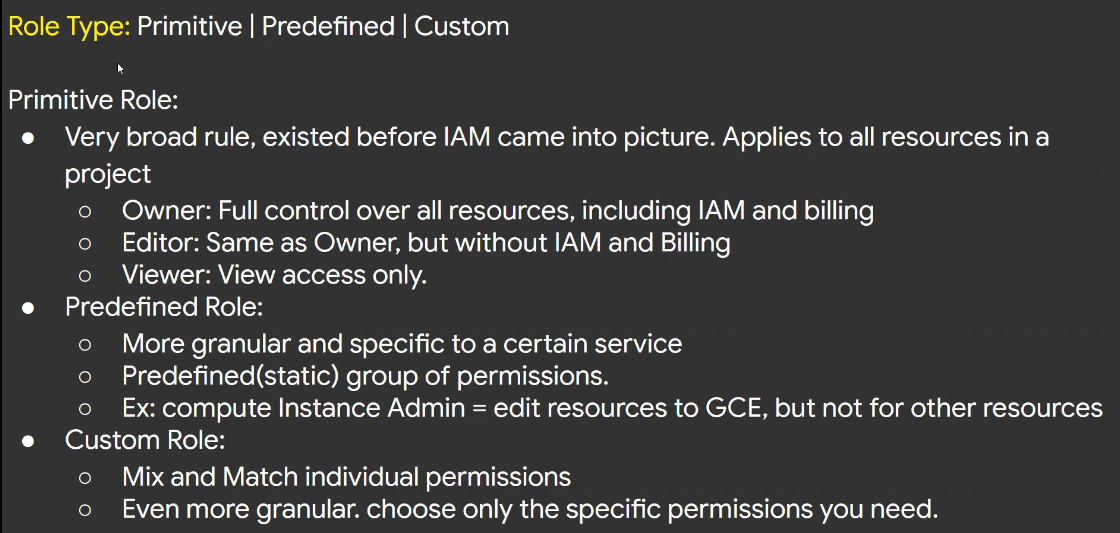
We can use gsuite accounts or cloud identity accounts to access the resources



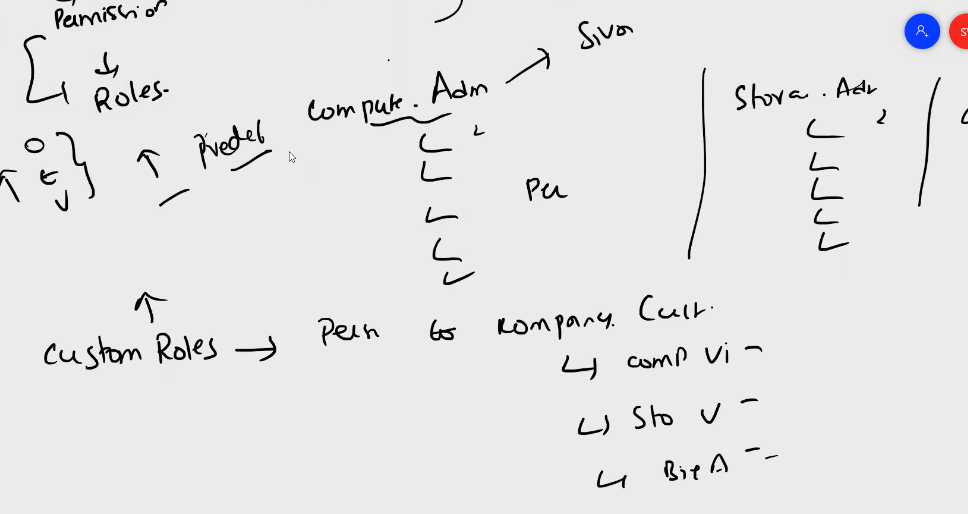




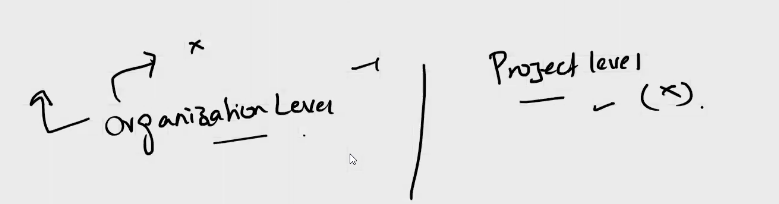
Int - Types of roles, which type of rolls you are using



Rolls are a group of permissions



We can assign permission on organization wide and project wide

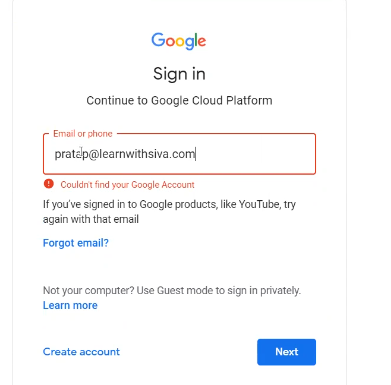


Costume roles to assign permissions on resources level, we can customize the rolls as per the requirement and assign to users

We can assign google wide roles can use primitive rolls

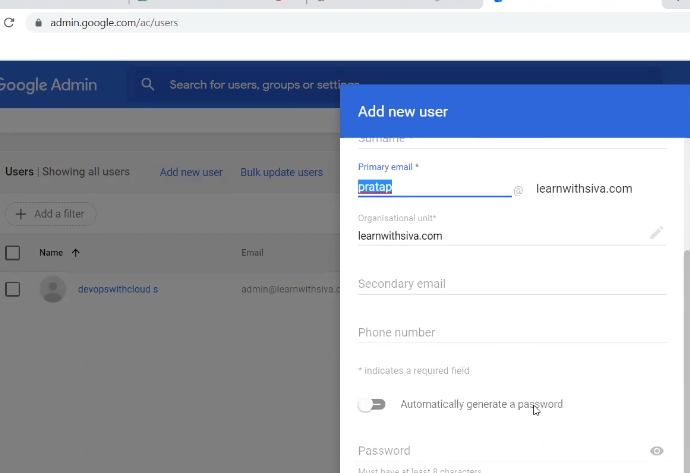
**User account creation**

Create an account named as Pratap

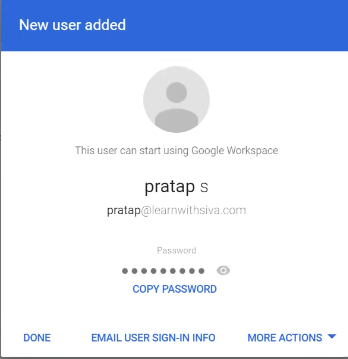


When we give first time any non existing account, we can see above login error

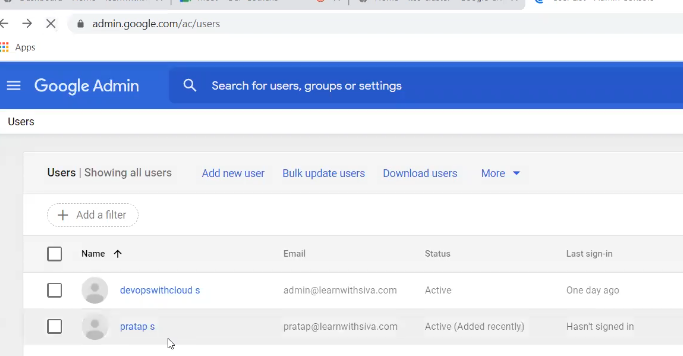
We have to create user accounts in admin account, for access to user we have to use console



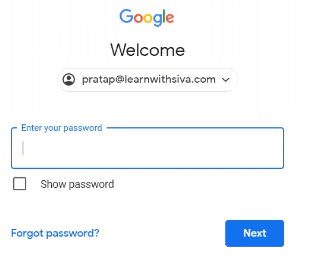
Go to google admin console, click on add new user option and provide required details to create user google cloud account

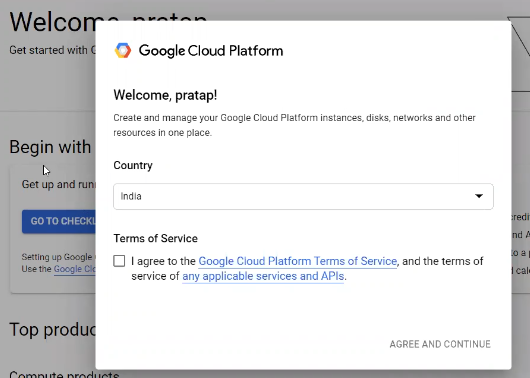


We can user gsuite accounts or google accounts or Microsoft AD to integrate ADsync to create accounts

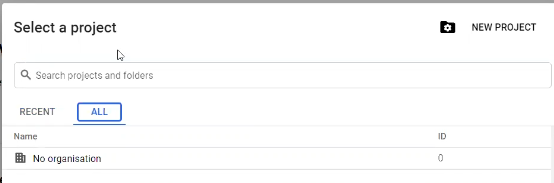


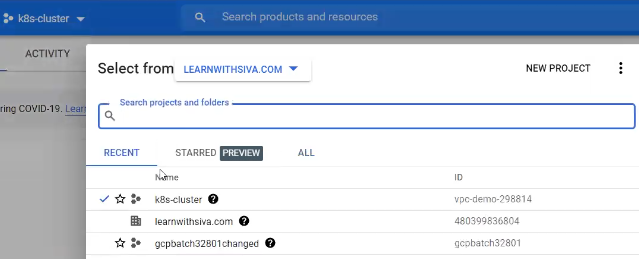
Login to user account



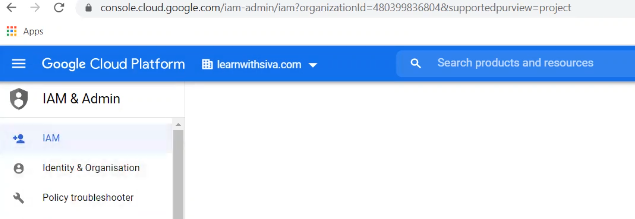


By default new users will not have access to organization or projects, can access once users are added to respective roles on admin cloud console

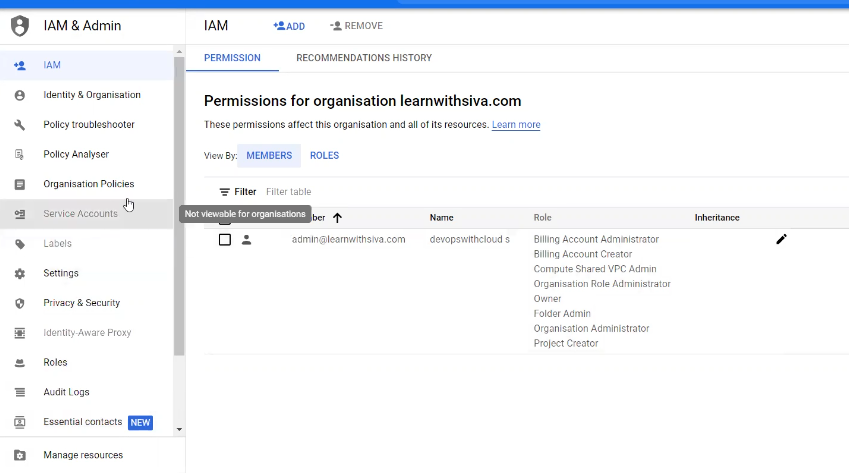




To assign permissions to users we need to go organization level, IAM and Admin option

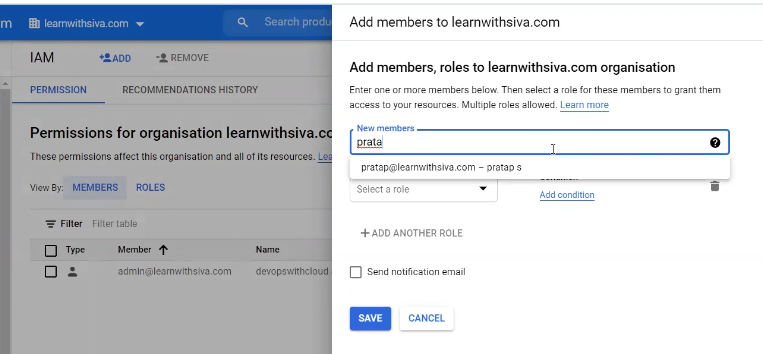


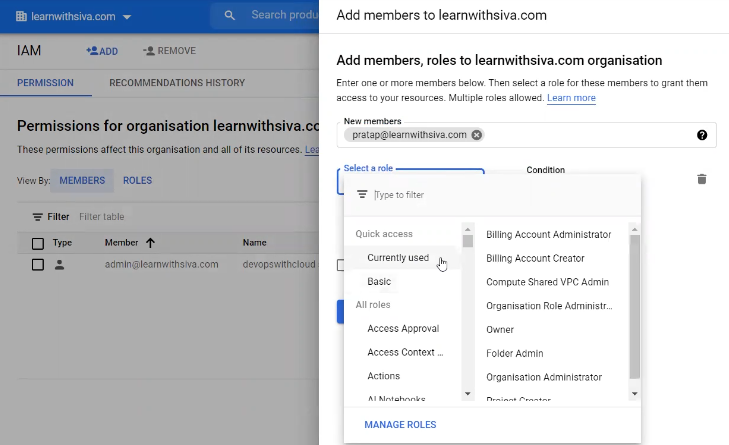
We can create and assign service accounts, assign roles, and security policies

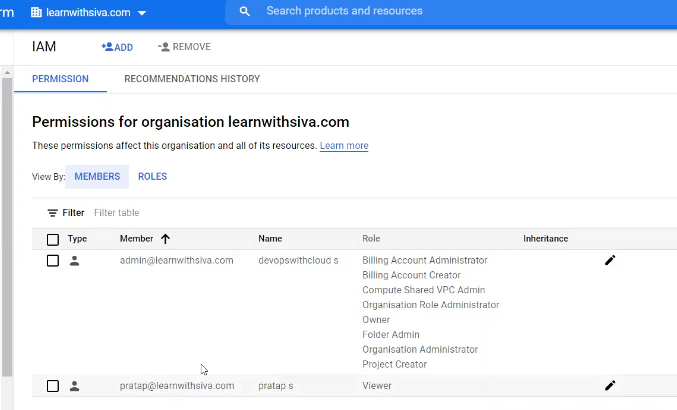


Service accounts can not be created and assigned to organization level, it should be grayed out

In IAM and Admin option need to go ADD to add users and to assign required permissions

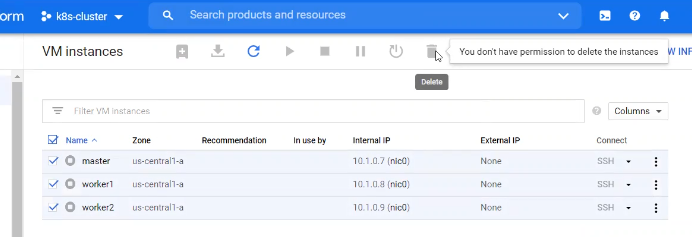






Projects are syncing to user accounts as per the permissions provided in admin console

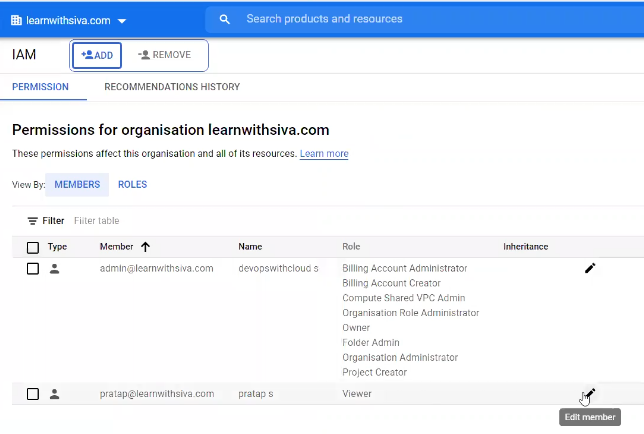
Permissions are applied as per the provided access

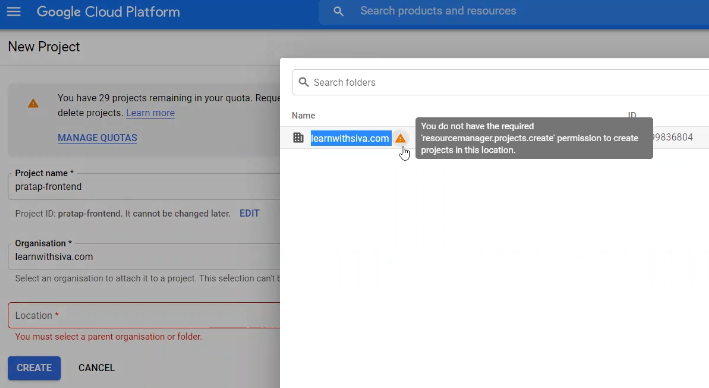


Assigning roles to see organization is depends on roles assigned to user, its not mandate to list the organization domain in users google console, be default users can not see organization domain

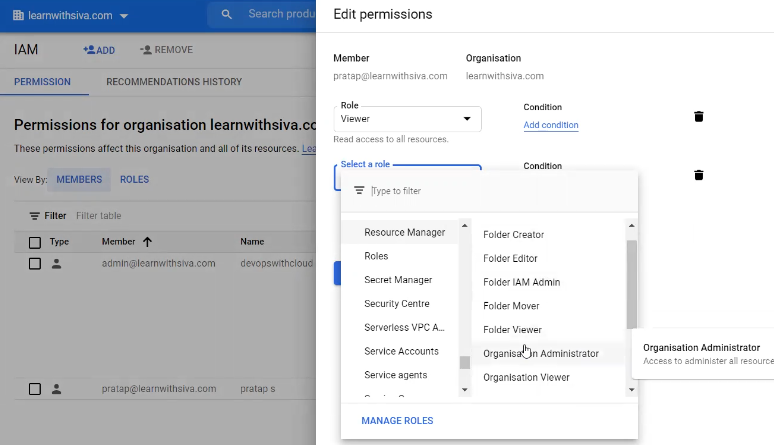
If we want to assign permission to list the organization, need to enable access in admin google console

Go to admin google login console, edit the previously provided access to that user and edit



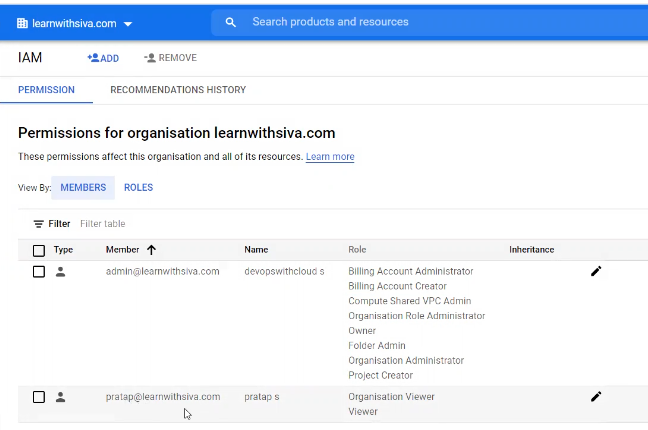


If we want to provide permission in organization level, go to users permissions, resource manager, then select viewer or administrator to manage the resources

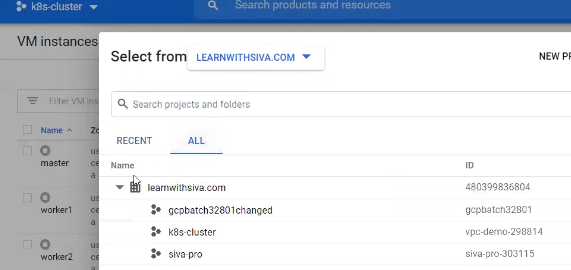


Int – if we are not seeing organization for user account, where can we grant permission, above is the answer

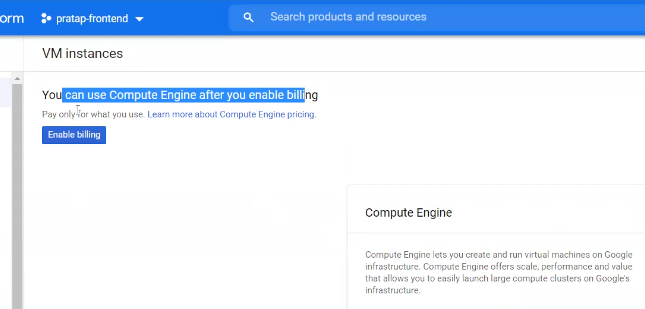
Now Pratap user also can view organization level

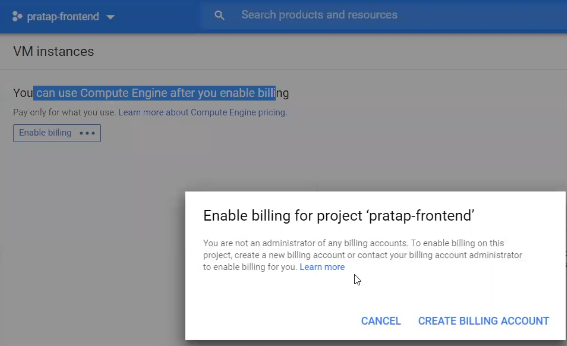


Now we can view organization in console



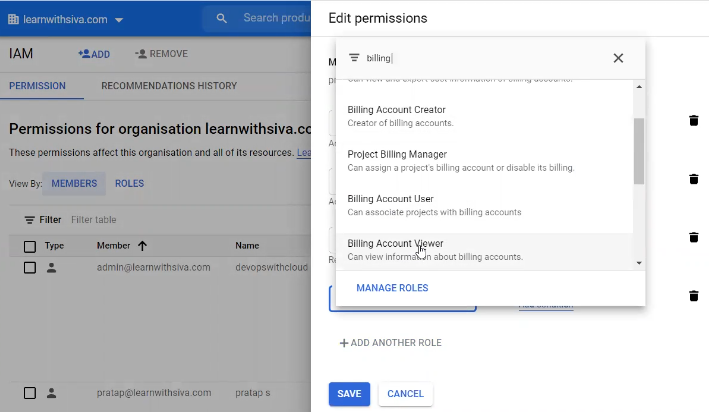
To create projects we need to associate billing account to create resources





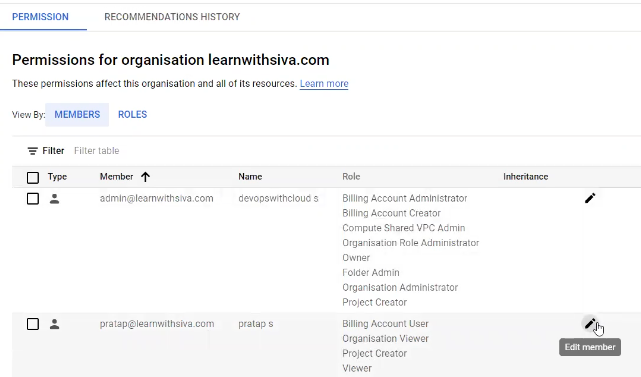
Imp – users never create billing accounts to associate projects to billing accounts, we use only cleated billing accounts in organization billing account

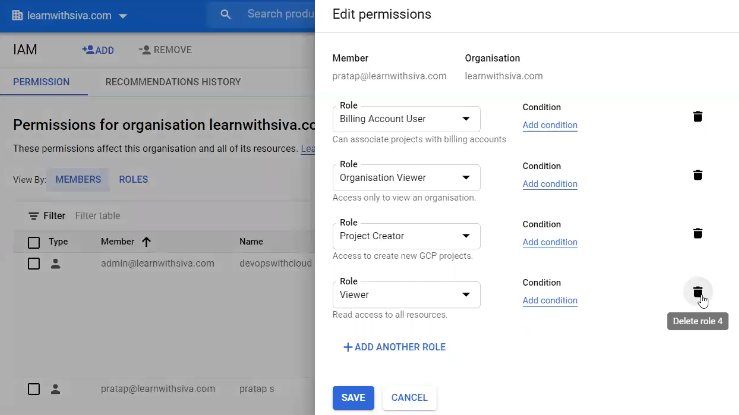
To enable billing we need to assign the below role to user

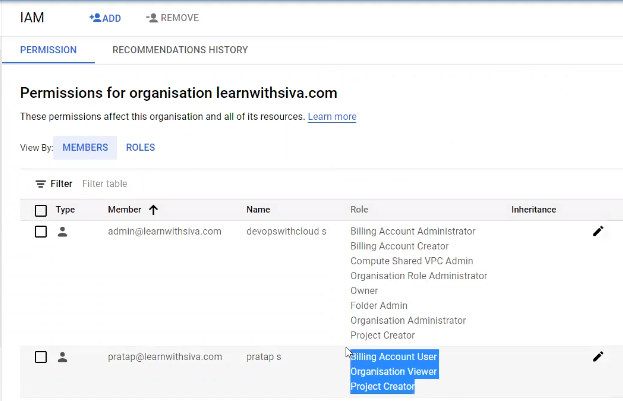


Once billing account is enabled for the project, we can create required resources by enabling API

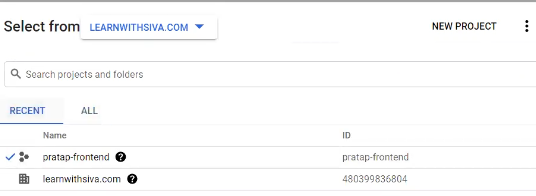
To remove viewer role and check the permissions



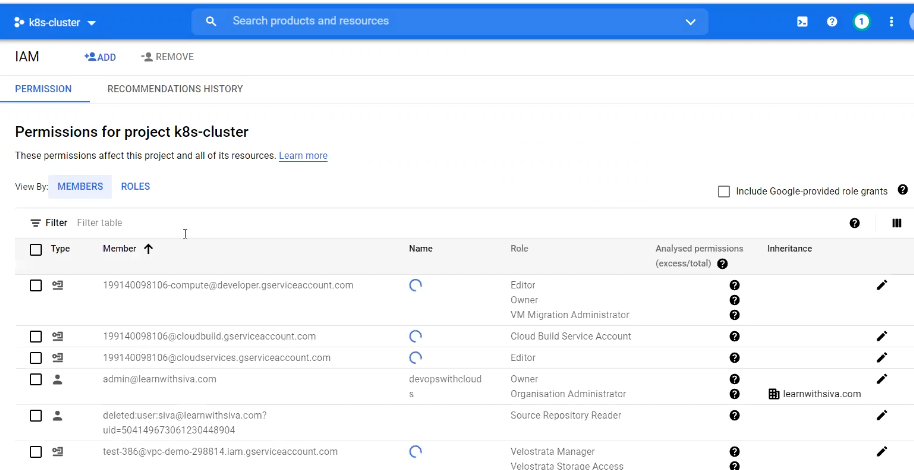


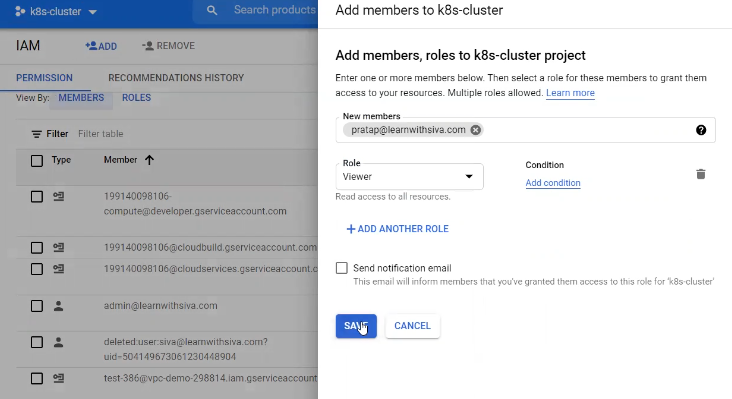


Once removed viewer role to the user, user can not view the projects except user created



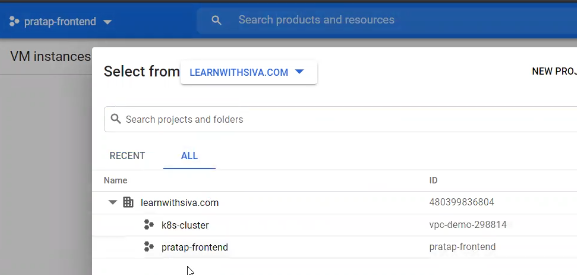
If we want to provide access to particular project, we have to go project level and go to IAM role and add the user to set the required permission



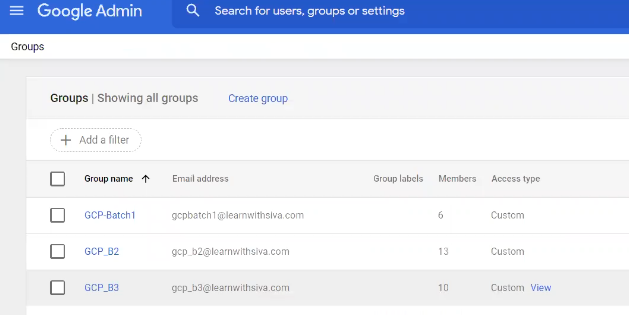


Assign viewer to project to user to view the project in users console

Now pratap can view the respective project to view



We can create groups in admin google cloud console only



<https://cloud.google.com/iam/docs/overview>