1.From Cloud console, do the following:

Create custom role named "my-custom-role-1" with the following permissions only:

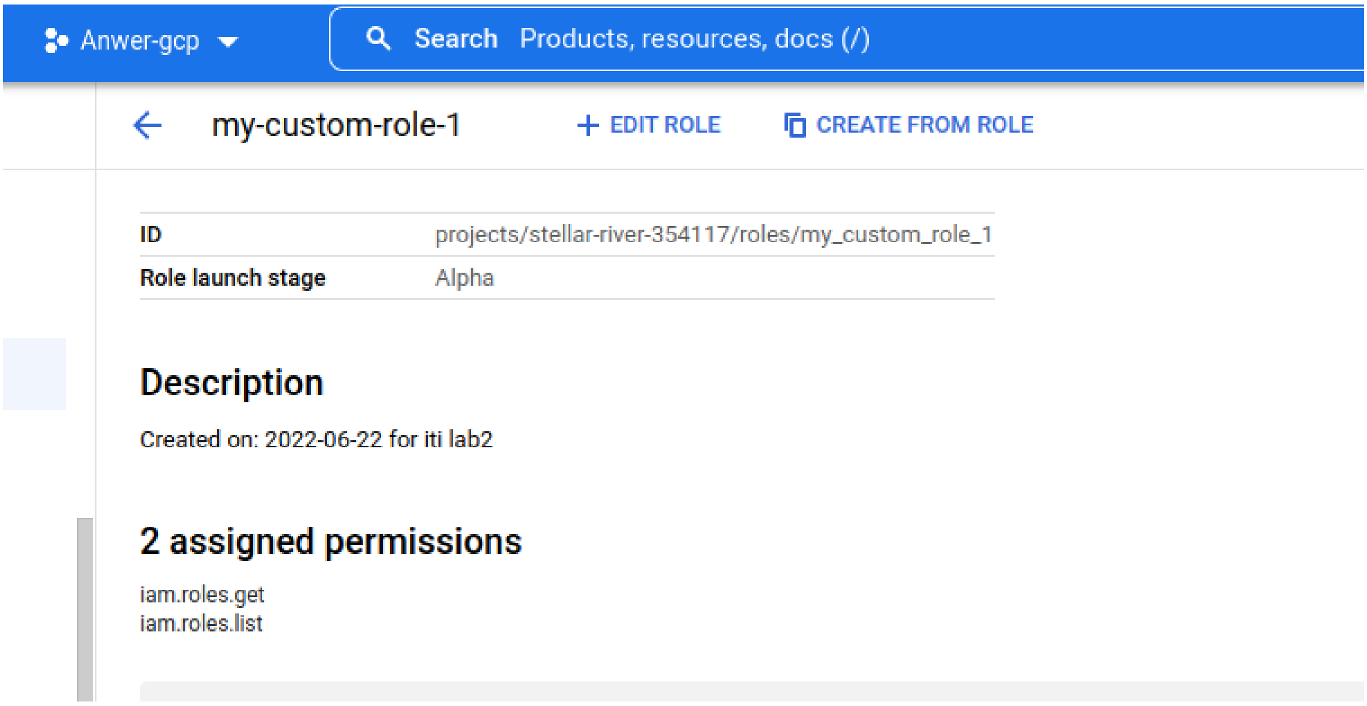
- Iam.roles.get
- Iam.roles.list

what happen in background?

```
- browser send request to google api and return list of roles
- select roles from the list
- browser again will send post request with payload of permissions to iam
api  and  save role
- I think they saved in google databases some where and linked with  the
project ID and account ID
```

why do we need to create custom role?

```
because we need to assign custom role to service account or assign custom
role to user account
so when they try to make request to google api , they will
get error if they don't have permission to do that
```



my-custom-role-1

ID	projects/stellar-river-354117/roles/my_custom_role_1
Role launch stage	Alpha

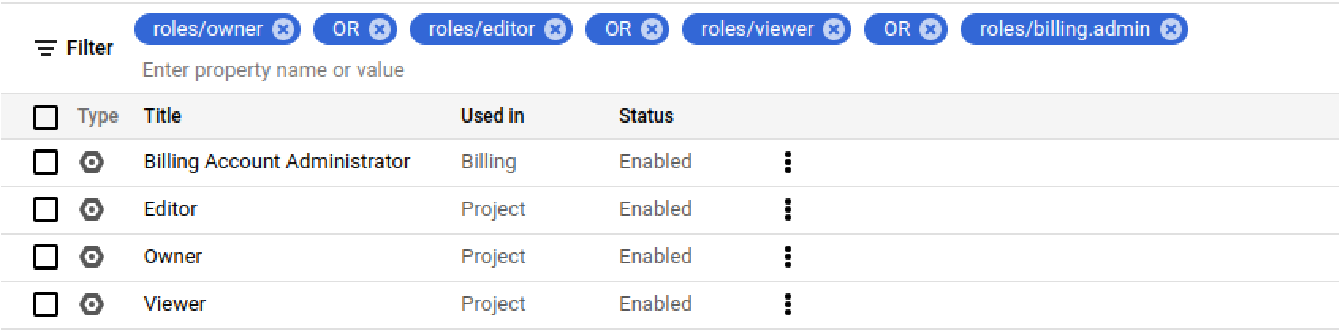
Description

Created on: 2022-06-22 for iti lab2

2 assigned permissions

iam.roles.get
iam.roles.list

2.From Cloud console, Explore primitive and pre-defined roles and their permissions.

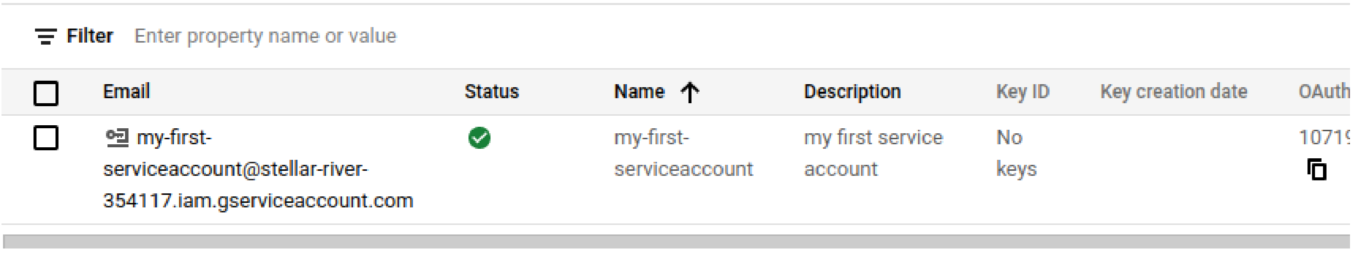


□	Type	Title	Used in	Status	
□	⊙	Billing Account Administrator	Billing	Enabled	⋮
□	⊙	Editor	Project	Enabled	⋮
□	⊙	Owner	Project	Enabled	⋮
□	⊙	Viewer	Project	Enabled	⋮

```
- same as above browser will make request to iam.role.api and  it will
return list of roles

- or using filter we can filter the roles we want
```

3.From Cloud console, Create a service account with id "my-first-serviceaccount".

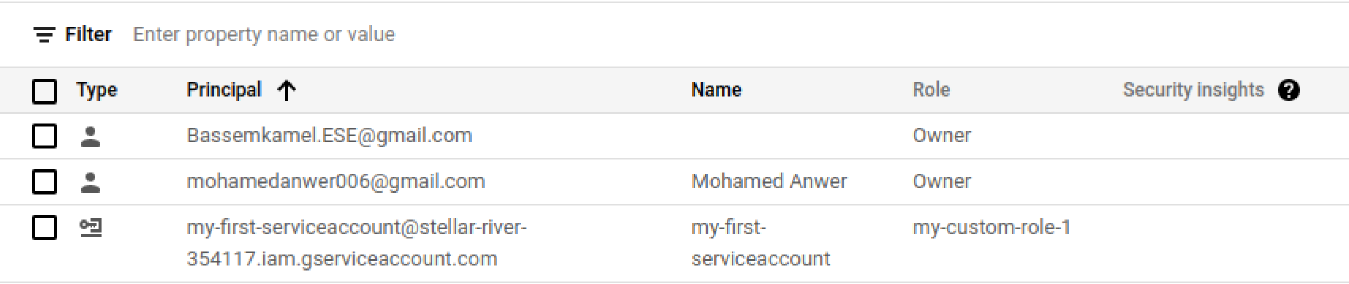
```
why we need to create service account?
    because sometimes we need to call google api from apps like jenkins or
from vms ...


the service account linked with project id and saved in database with its
json-key file
```



□	Email	Status	Name ↑	Description	Key ID	Key creation date	OAuth
□	my-first-serviceaccount@stellar-river-354117.iam.gserviceaccount.com	✓	my-first-serviceaccount	my first service account	No keys		1071

4.From Cloud console, Assign the custom role "my-custom-role-1" to the service account "my-first-serviceaccount"

```
why
we need to assign some permission to service account?
so it can access google api, specifically iam.roles

thats why we attach to it `custom role`
```



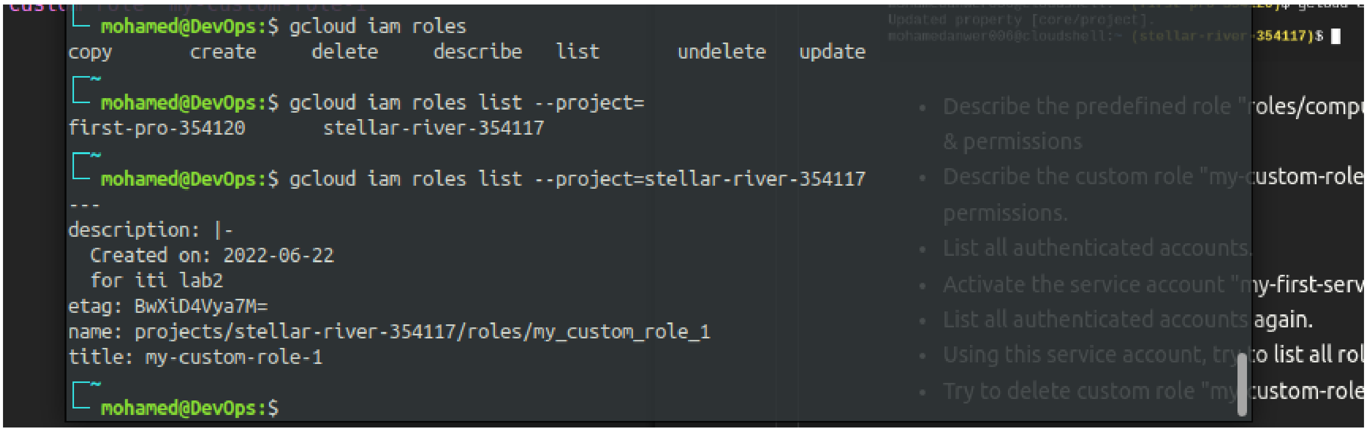
☰ Filter Enter property name or value

□	Type	Principal ↑	Name	Role	Security insights
□	👤	Bassemkamel.ESE@gmail.com		Owner	
□	👤	mohamedanwer006@gmail.com	Mohamed Anwer	Owner	
□		my-first-serviceaccount@stellar-river-354117.iam.gserviceaccount.com	my-first-serviceaccount	my-custom-role-1	

5.Using gcloud

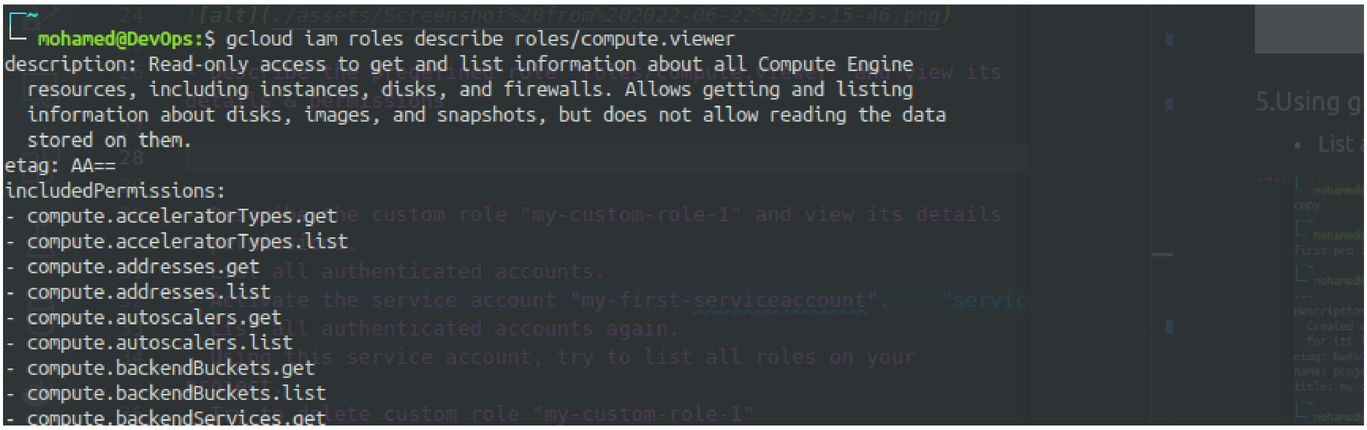
- List all roles on your project.

```
gcloud send get request to iam.roles.list api and it will response with
list of roles
```



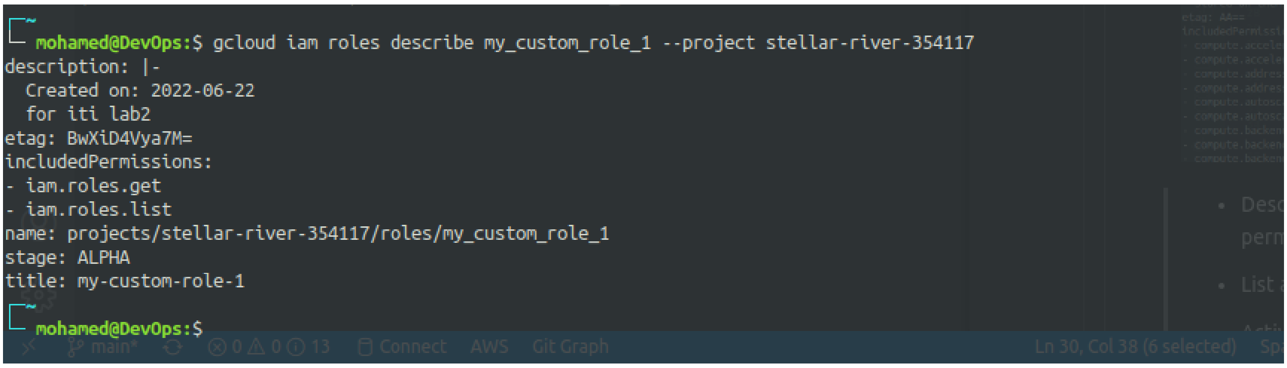
```
└ mohamed@DevOps:$ gcloud iam roles
copy       create     delete     describe    list       undelete    update
┌~
└ mohamed@DevOps:$ gcloud iam roles list --project=
first-pro-354120       stellar-river-354117
┌~
└ mohamed@DevOps:$ gcloud iam roles list --project=stellar-river-354117
---
description: |-
  Created on: 2022-06-22
  for iti lab2
etag: BwXiD4Vya7M=
name: projects/stellar-river-354117/roles/my_custom_role_1
title: my-custom-role-1
┌~
└ mohamed@DevOps:$
```

- Describe the predefined role "roles/compute.viewer" and view its details & permissions



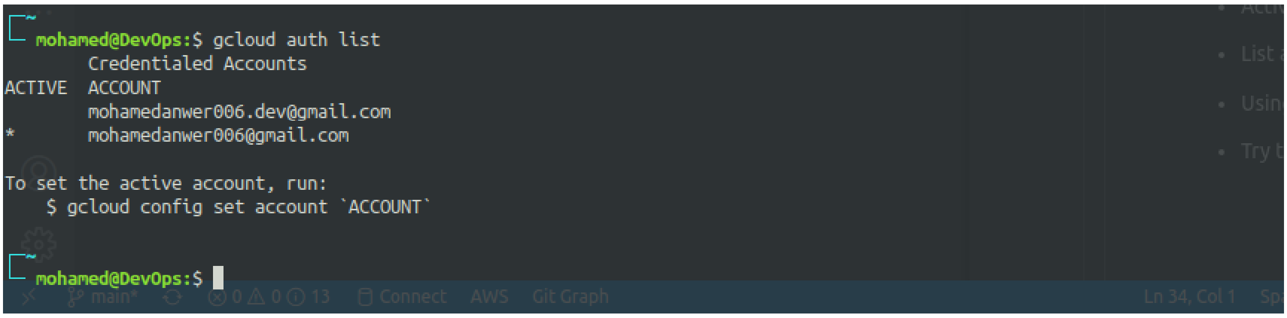
```
┌~
└ mohamed@DevOps:$ gcloud iam roles describe roles/compute.viewer
description: Read-only access to get and list information about all Compute Engine
  resources, including instances, disks, and firewalls. Allows getting and listing
  information about disks, images, and snapshots, but does not allow reading the data
  stored on them.
etag: AA==
includedPermissions:
- compute.acceleratorTypes.get
- compute.acceleratorTypes.list
- compute.addresses.get
- compute.addresses.list
- compute.autoscalers.get
- compute.autoscalers.list
- compute.backendBuckets.get
- compute.backendBuckets.list
- compute.backendServices.get
```

- Describe the custom role "my-custom-role-1" and view its details & permissions.



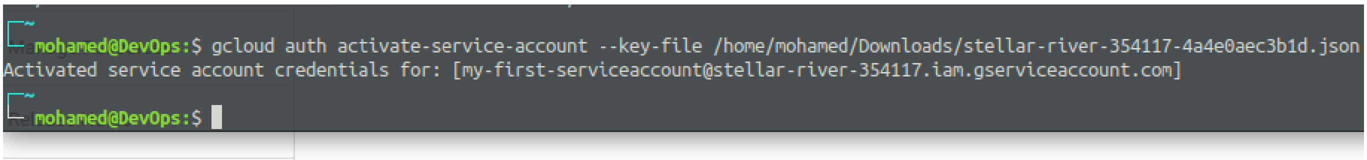
```
┌~
└ mohamed@DevOps:$ gcloud iam roles describe my_custom_role_1 --project stellar-river-354117
description: |-
  Created on: 2022-06-22
  for iti lab2
etag: BwXiD4Vya7M=
includedPermissions:
- iam.roles.get
- iam.roles.list
name: projects/stellar-river-354117/roles/my_custom_role_1
stage: ALPHA
title: my-custom-role-1
┌~
└ mohamed@DevOps:$
```

- List all authenticated accounts.



```
┌~
└ mohamed@DevOps:$ gcloud auth list
        Credentialed Accounts
ACTIVE  ACCOUNT
        mohamedanwer006.dev@gmail.com
*       mohamedanwer006@gmail.com

To set the active account, run:
    $ gcloud config set account `ACCOUNT`


┌~
└ mohamed@DevOps:$
```

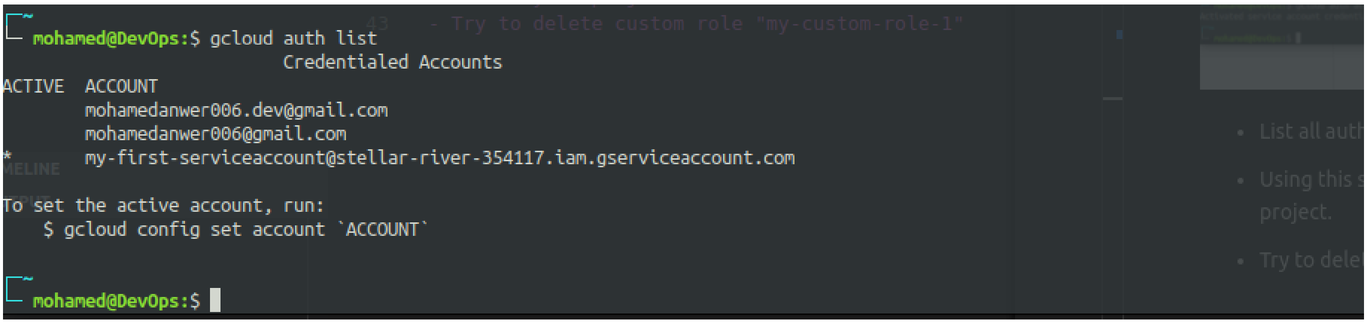
- Activate the service account "my-first-serviceaccount".



```
┌~
└ mohamed@DevOps:$ gcloud auth activate-service-account --key-file /home/mohamed/Downloads/stellar-river-354117-4a4e0aec3b1d.json
Activated service account credentials for: [my-first-serviceaccount@stellar-river-354117.iam.gserviceaccount.com]
┌~
└ mohamed@DevOps:$
```

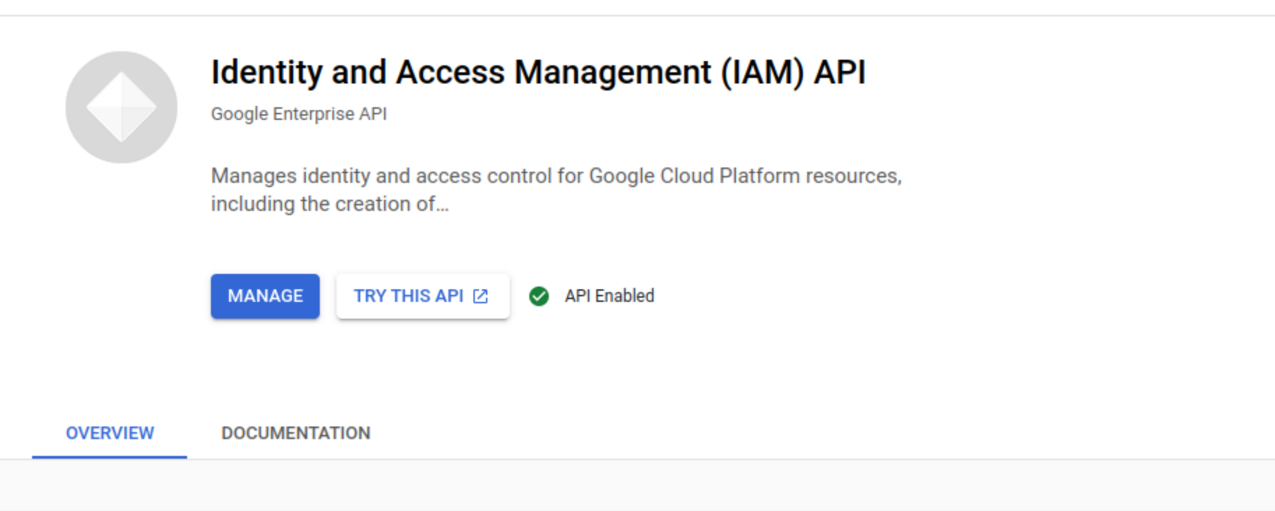
- List all authenticated accounts again.

```
i think here gcloud does not send request to api, it get the authenticated accounts from local machine configuration file
```

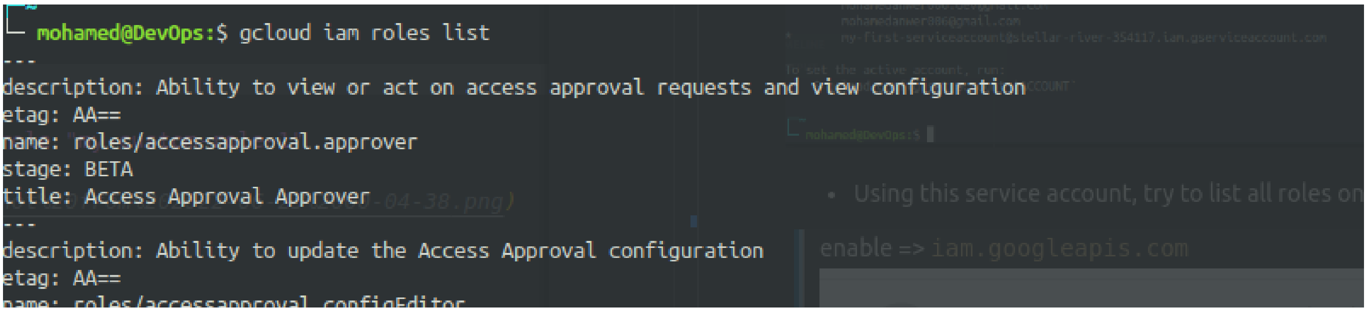


```
┌~
└ mohamed@DevOps:$ gcloud auth list
                Credentialed Accounts
ACTIVE  ACCOUNT
        mohamedanwer006.dev@gmail.com
        mohamedanwer006@gmail.com
*       my-first-serviceaccount@stellar-river-354117.iam.gserviceaccount.com

To set the active account, run:
    $ gcloud config set account `ACCOUNT`


┌~
└ mohamed@DevOps:$
```

- Using this service account, try to list all roles on your project.

> enable => `iam.googleapis.com`
>
> 
>
> Identity and Access Management (IAM) API
>
> Google Enterprise API
>
> Manages identity and access control for Google Cloud Platform resources, including the creation of...
>
>

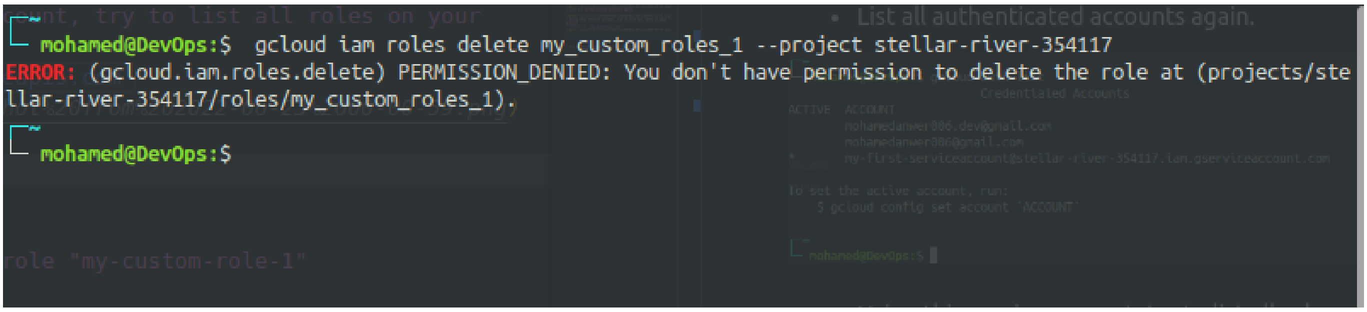
```
gcloud send request to iam.roles.list api with service account key-info

api will check if it have permission to do that
if so it will return list of roles
```



```
└─ mohamed@DevOps:$ gcloud iam roles list
---
description: Ability to view or act on access approval requests and view configuration
etag: AA==
name: roles/accessapproval.approver
stage: BETA
title: Access Approval Approver
---
description: Ability to update the Access Approval configuration
etag: AA==
name: roles/accessapproval.configEditor
```

- Try to delete custom role "my-custom-role-1"

```
same as above
except when the api backend check if it have permission to do that it will
return error

that this service account does not have permission to do that
```



```
└─ mohamed@DevOps:$  gcloud iam roles delete my_custom_roles_1 --project stellar-river-354117
ERROR: (gcloud.iam.roles.delete) PERMISSION_DENIED: You don't have permission to delete the role at (projects/stellar-river-354117/roles/my_custom_roles_1).
┌─~
└─ mohamed@DevOps:$
```