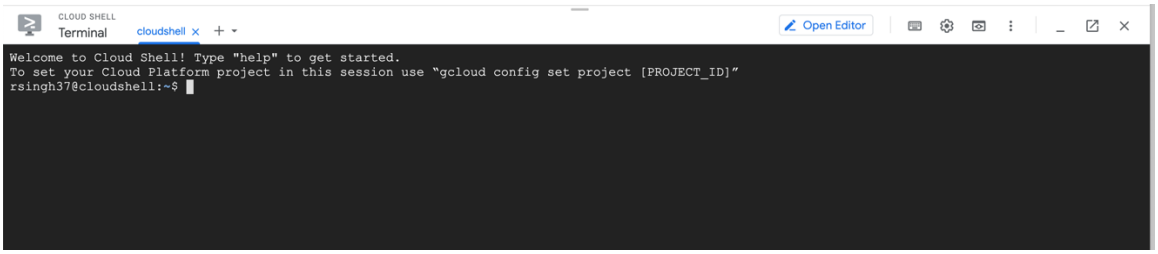
Rashika Pramod Singh
IST 615

Lab 2: Google Cloud Platform

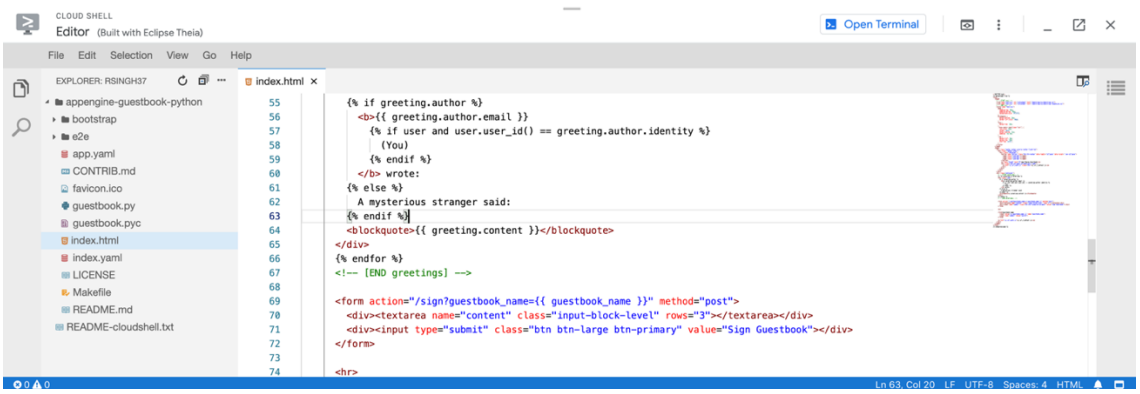
1. Cloud Shell

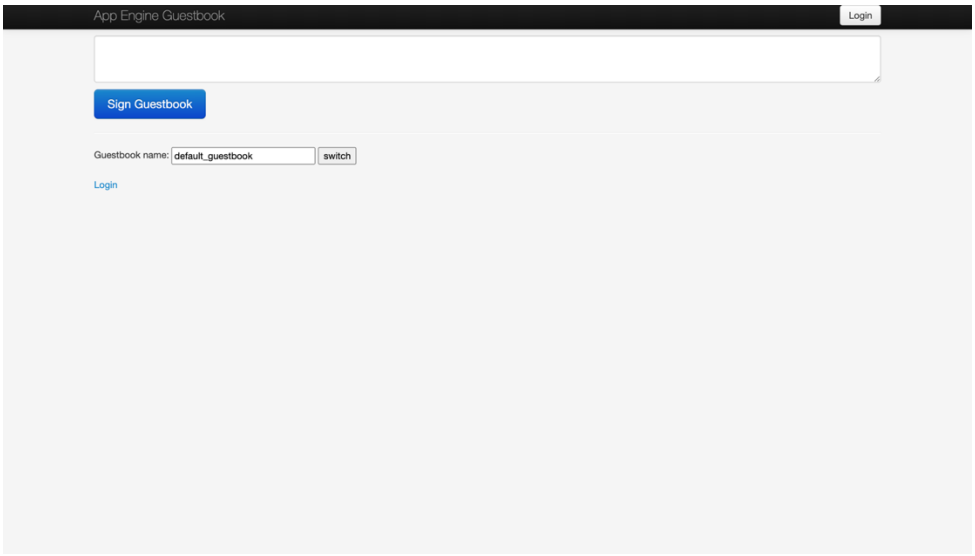
- Preview and deploy an App Engine Application

Google App Engine allows app developers to build web and backend in any programming language and deploy on a serverless program.
First, I created a free account on Google Cloud Platform, created a project and started the cloud shell from the Console.

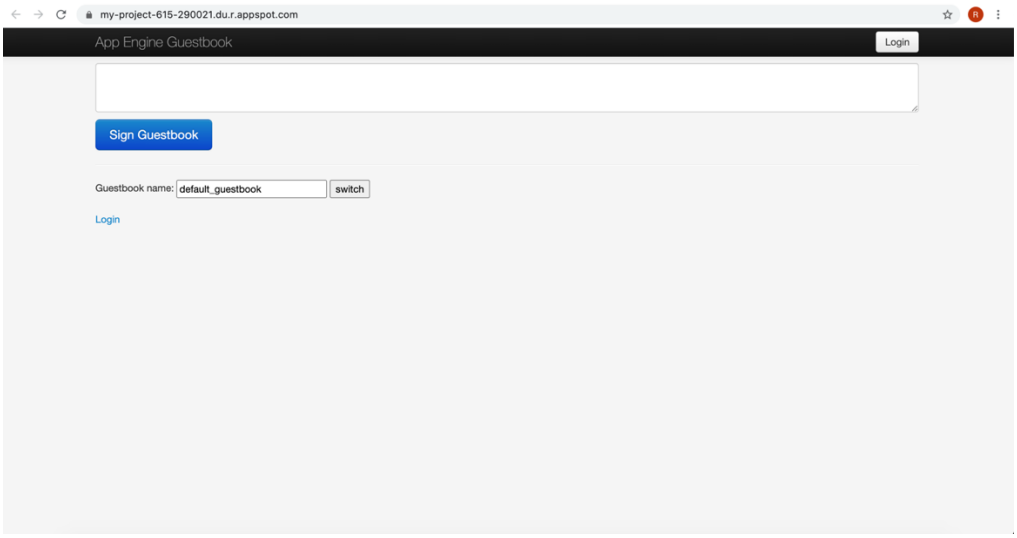


I wrote the code on the shell which cloned the repository from github, cd changed the location of the shell and then runs the app locally. The snippet shows the sample code in the repo and then I previewed the app before hosting it on the internet. The default port is 8080.





Then, I create an app engine using the command and deploy the app to the App Engine using gcloud app deploy. After deployment, I can see the target url which I can use in the search of chrome, the URL also has the project ID for my cloud. The below snippet shows the application created in the URL.

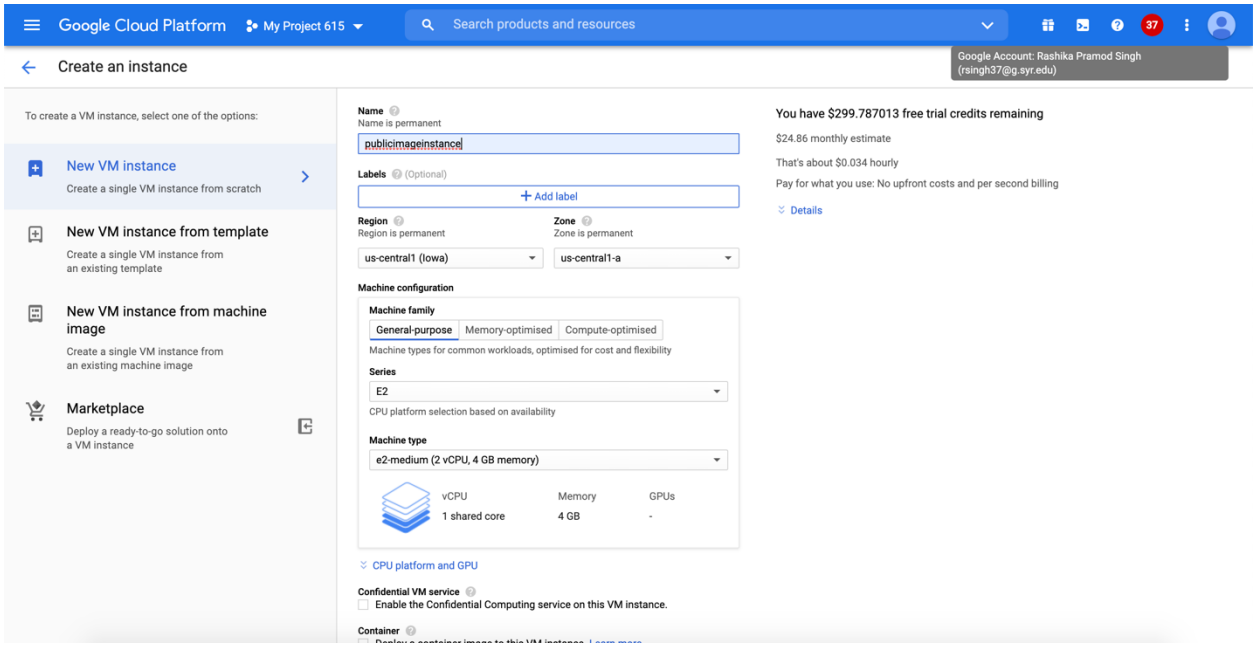


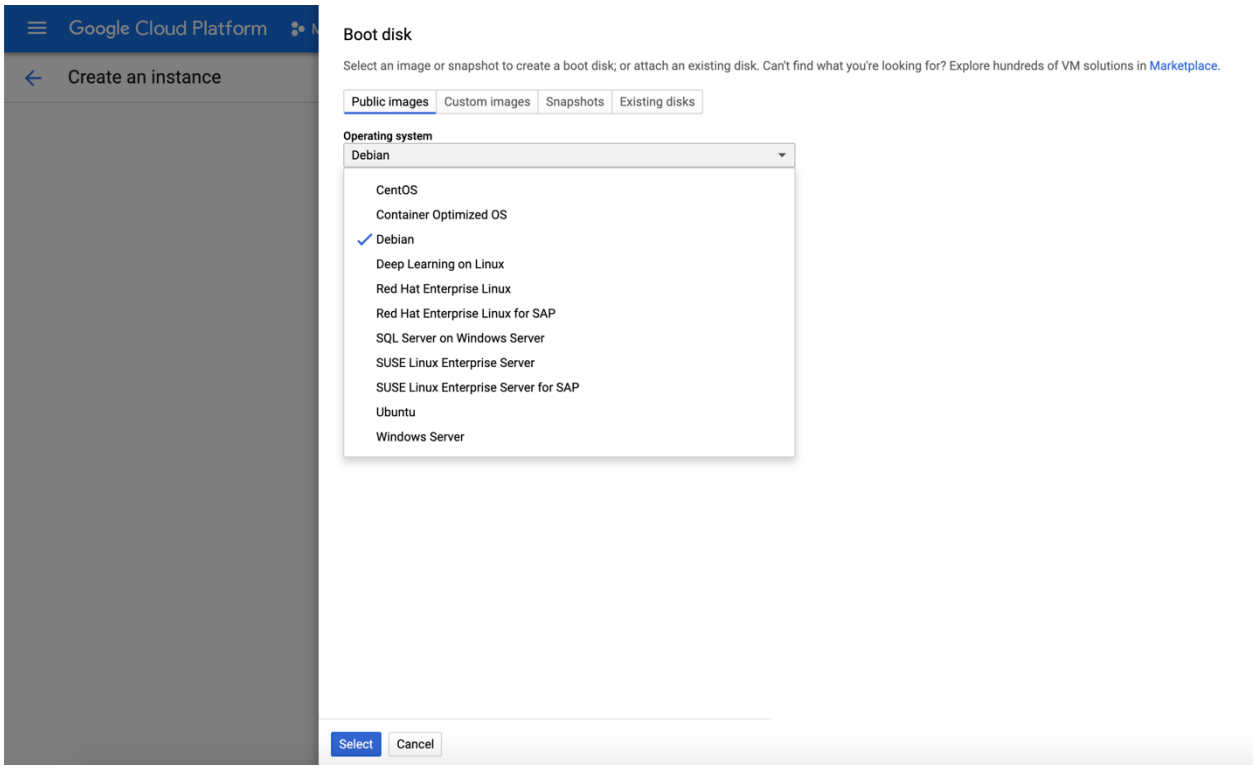
2. Creating VM Instances

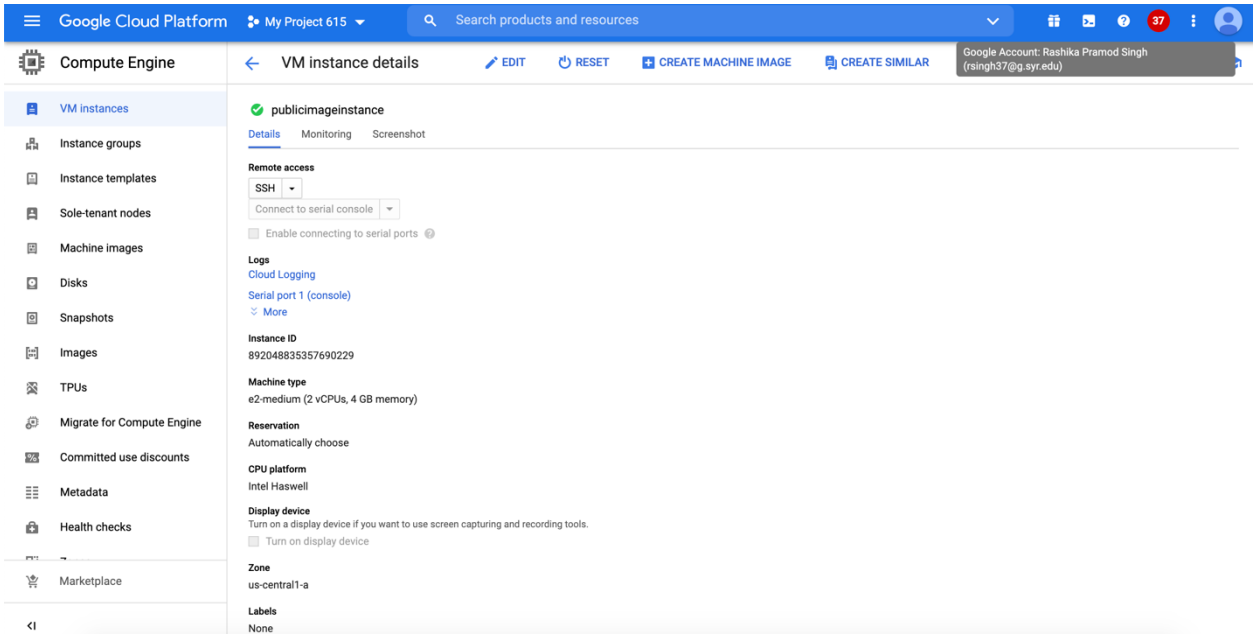
A VM instance is a virtual machine hosted on Google's infrastructure. The instance can be created using gcloud, console or Compute Engine API.

- Creating an instance from public image

Google Cloud provides and maintains many OS public images. All the projects can create VMs using public OS images. I started with creating a new instance and the boot disk allows you to choose from many public images. I selected the Debian GNU which is mounted on a disk size of 20GB.



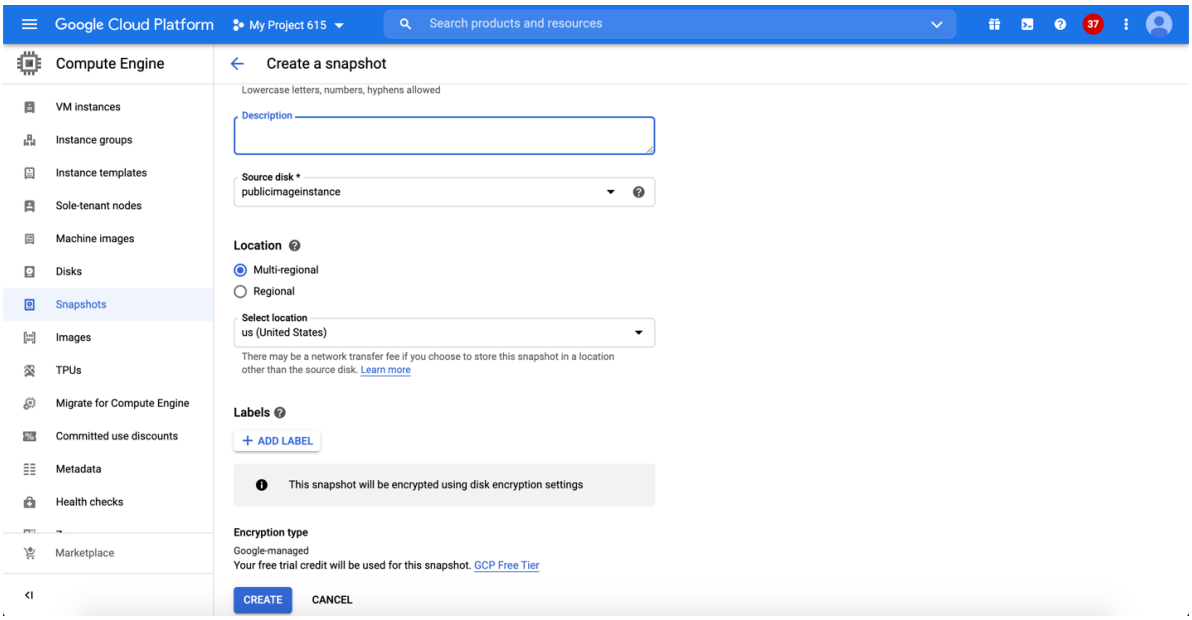




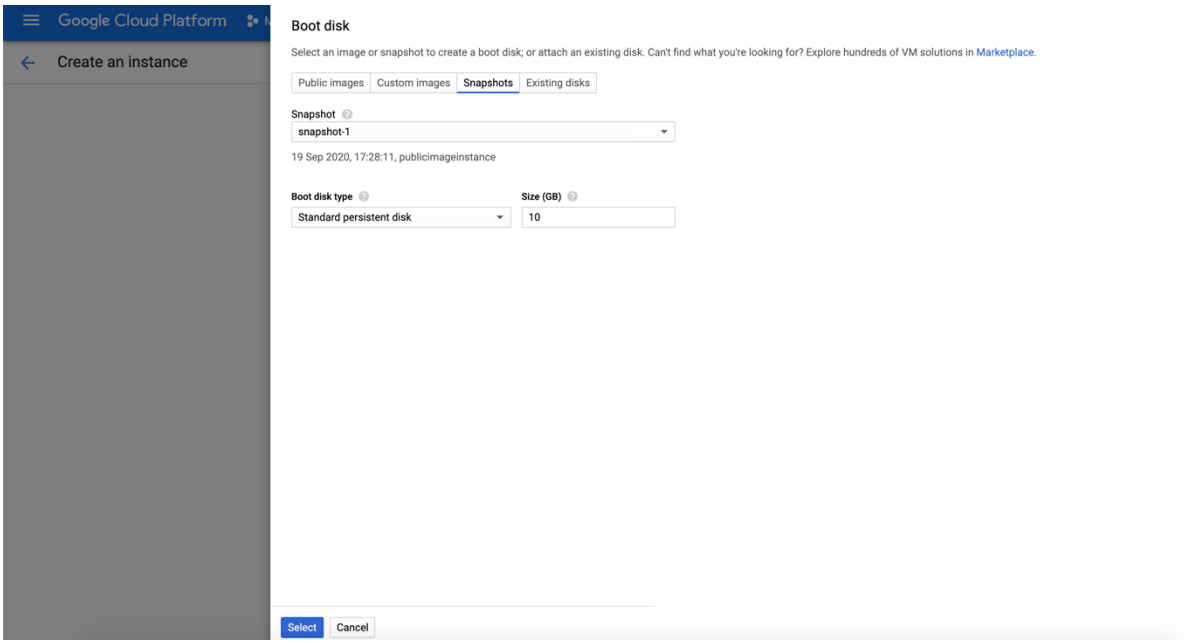
- Creating an instance from a snapshot

  If you have backed a disk with a snapshot, you can use that to create an instance. I have used the snapshot of the previous instance's disk. Snapshots also backup data and are incremental in nature so it contains the modified data from the previous one. It is faster

than an image as it has modified data. Snapshots are global resources and are accessible by any resource in the same project.

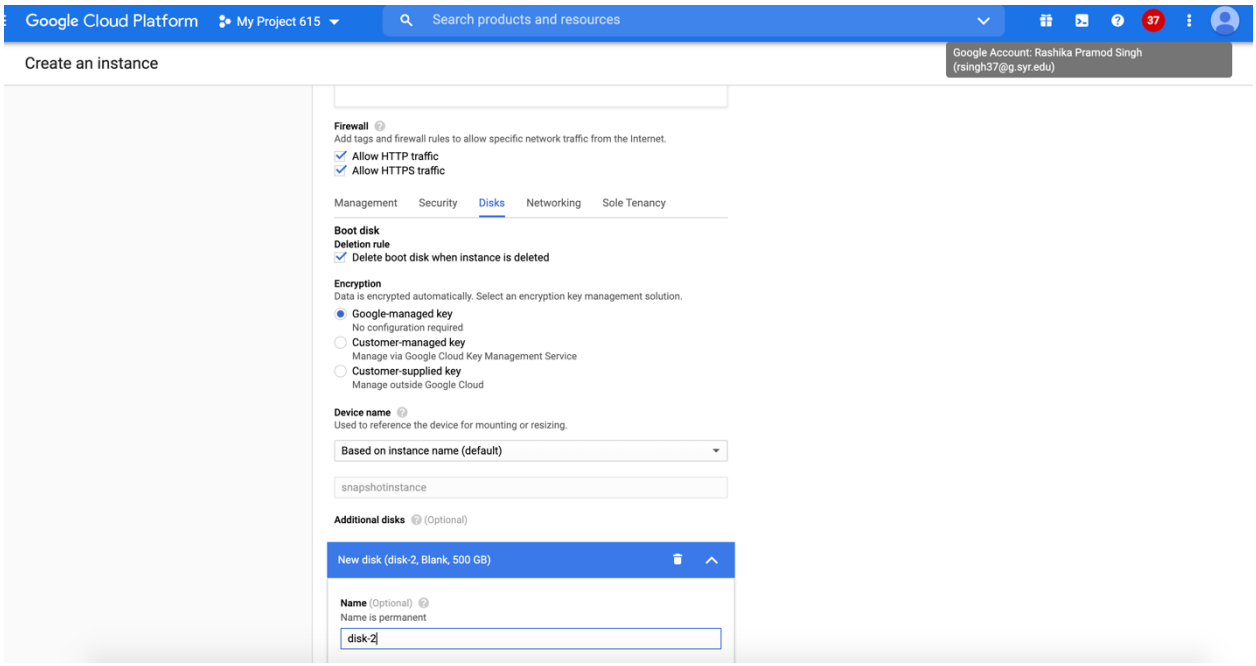


I used a snapshot from the previous instance and used it to create a new VM instance.

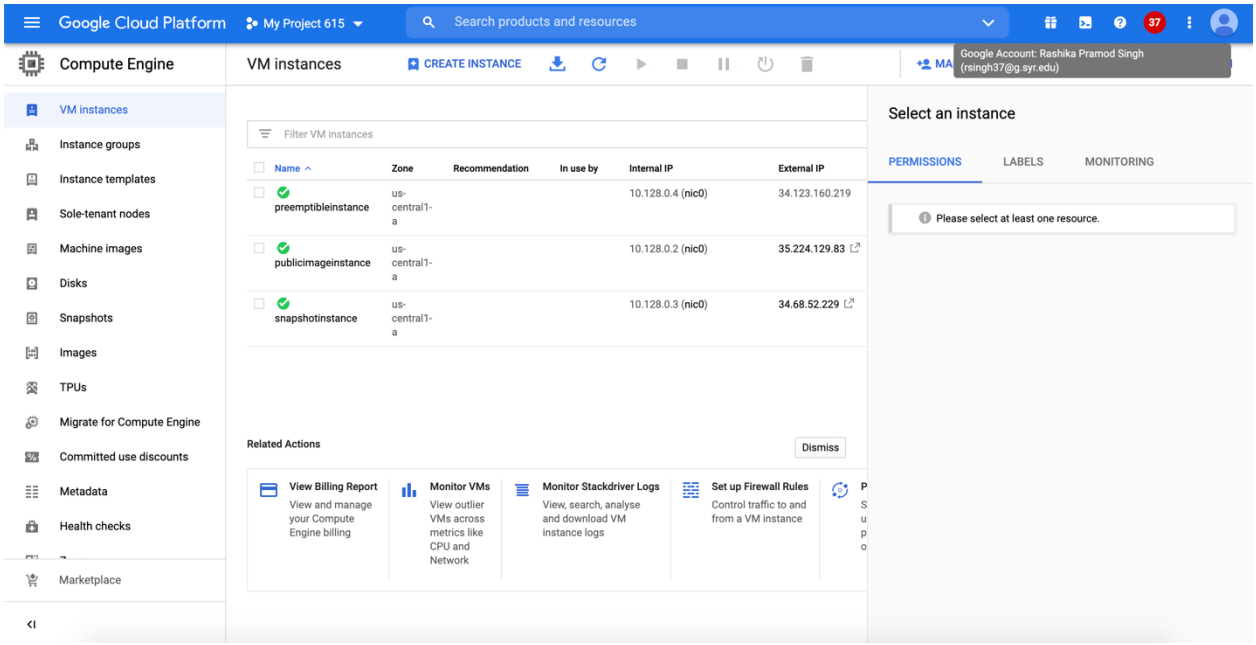


The rules state that whenever instance is deleted the boot disk is also deleted and the firewall rules allow the HTTP traffic and the HTTPS traffic. This adds a network tag to the instance and creates the corresponding ingress rule for the incoming traffic. Configuring instances with

firewall allows them to be accessed even through the internet. I have also added an additional disk to the instance.



The snippet shows that the instance is created.

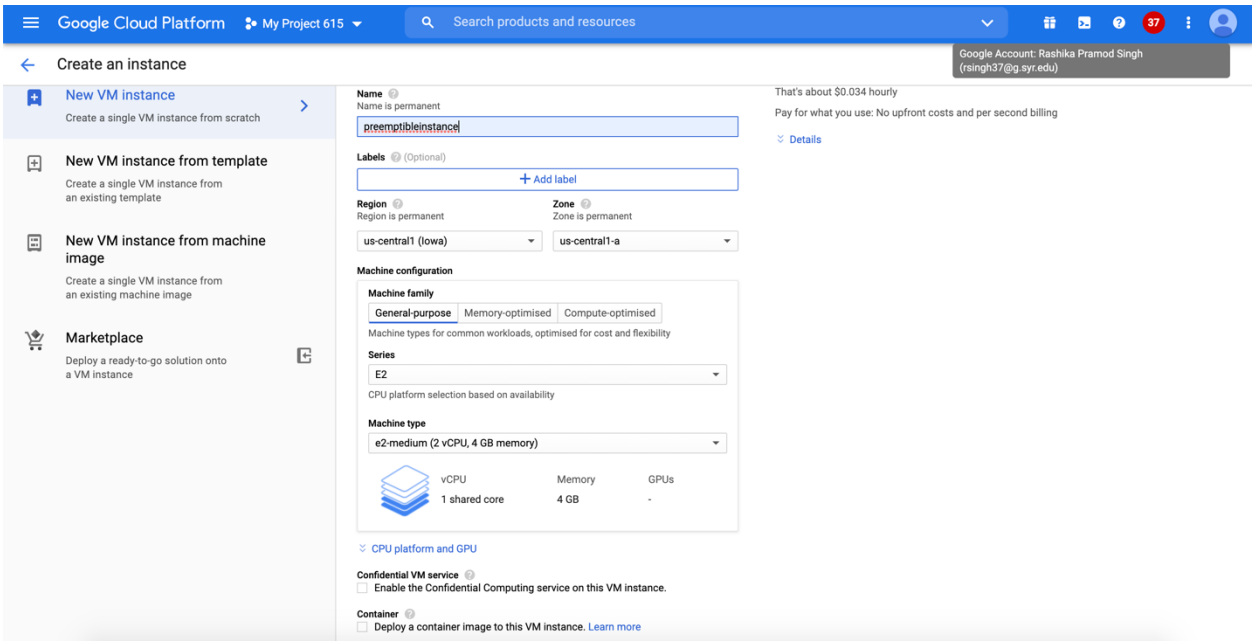


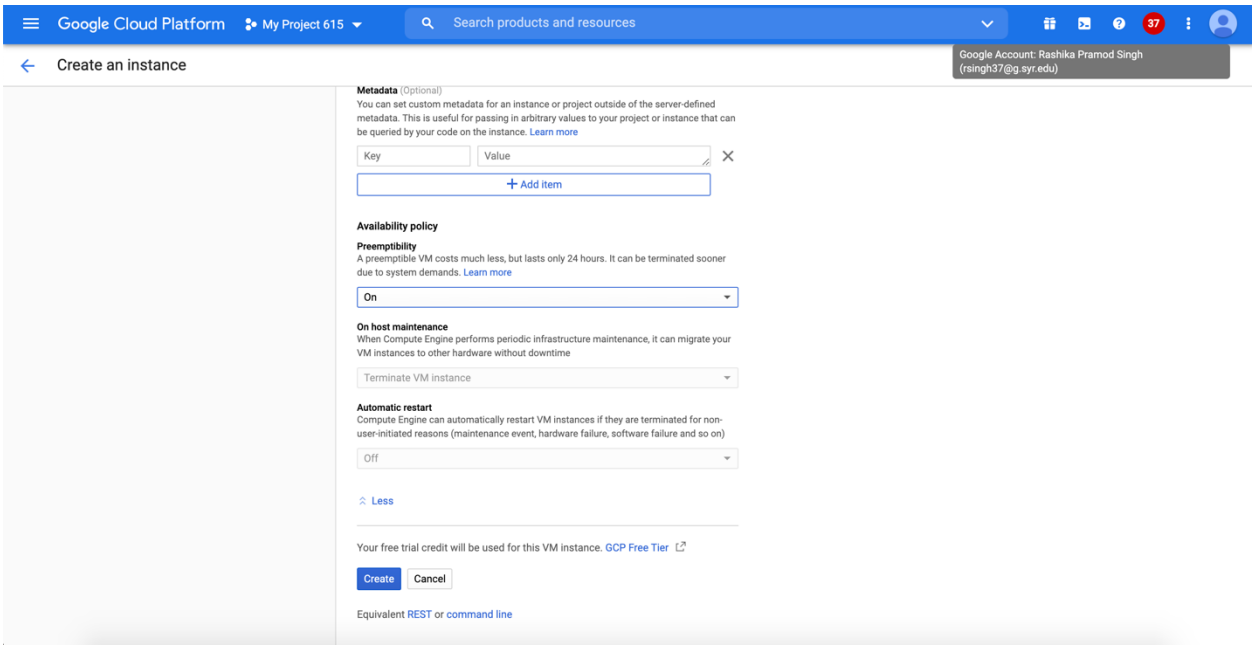
- Creating and starting a preemptible VM instance

A preemptible instance is an instance that you can create and run at lower price than normal ones and the compute engine can stop the instances if resources are required for another task. Preemptible instances will always stop after 24 hours.

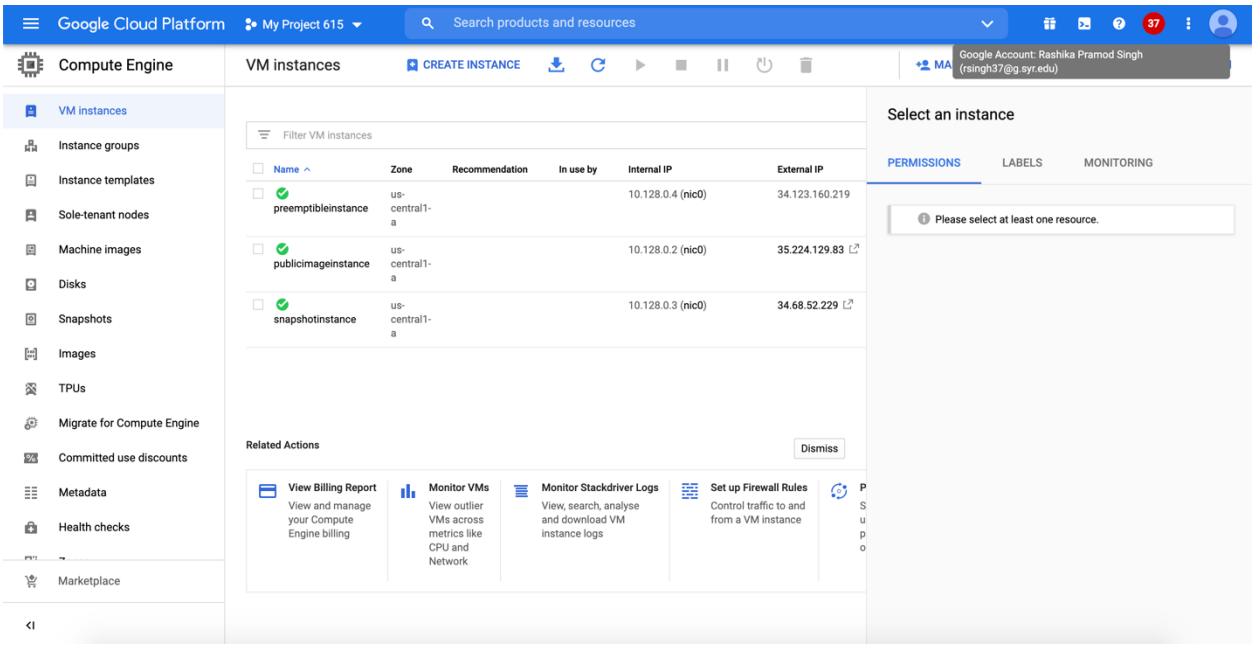
- Checking a preemptible instance

Here I create a preemptible instance where the instances have excess capacity so their availability can vary with usage. I created an instance as preemptible by selecting the preemptible option in the availability policy.



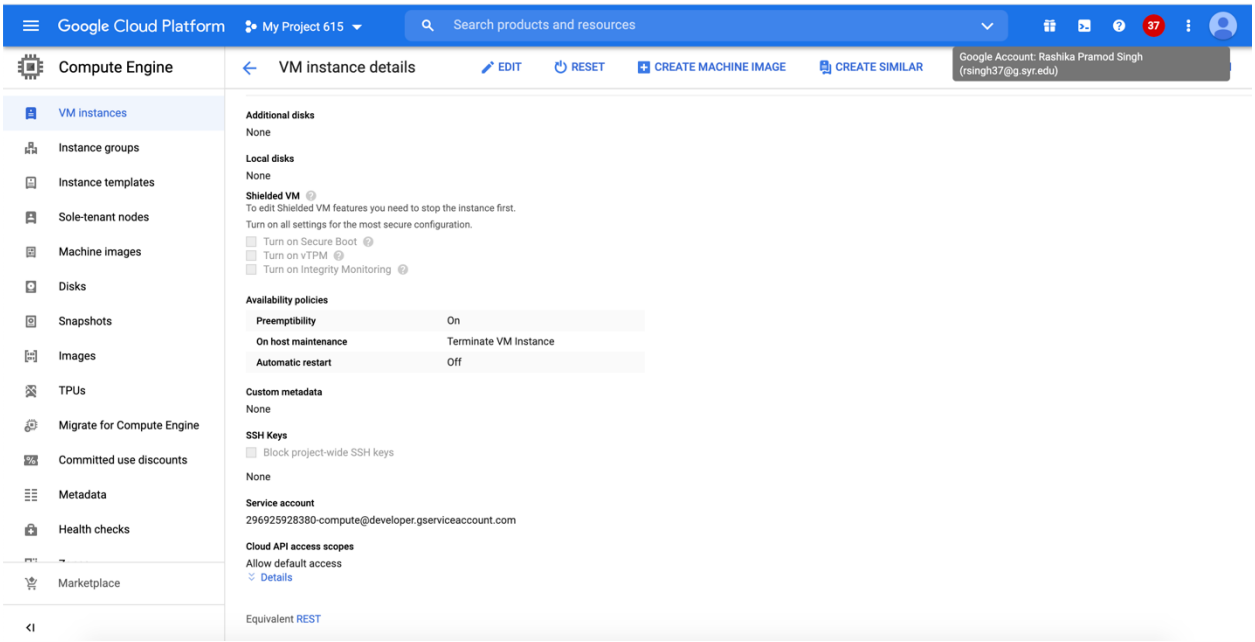


The screenshot shows that the instance is preemptible.



- Checking if an instance is preemptible

Here I am checking if an instance is preemptible or not. I can check this by clicking on the instance and checking the availability option. Here preemptible is on which shows that the instance is preemptible.

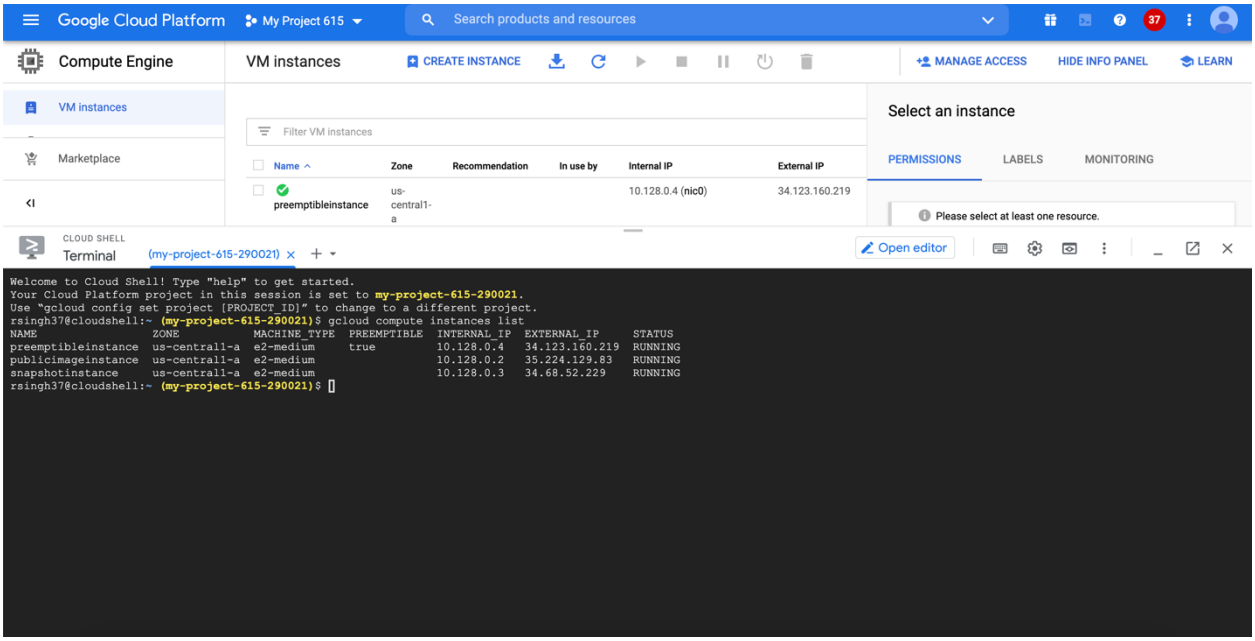


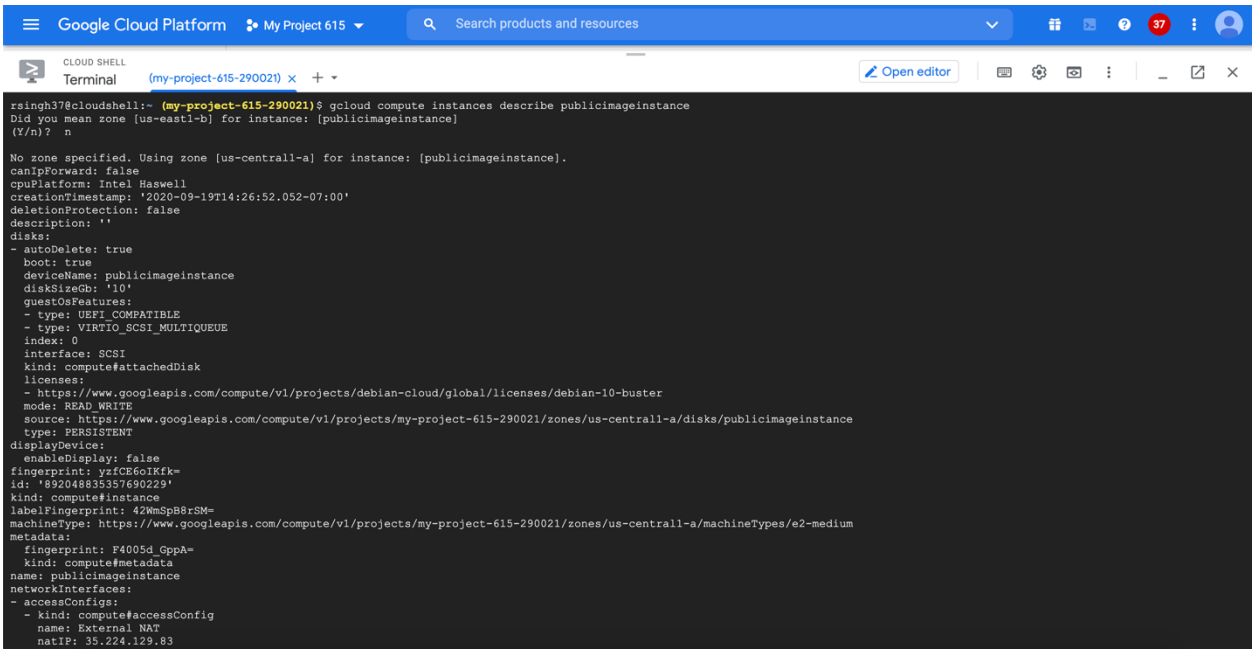
- Checking an instance's status

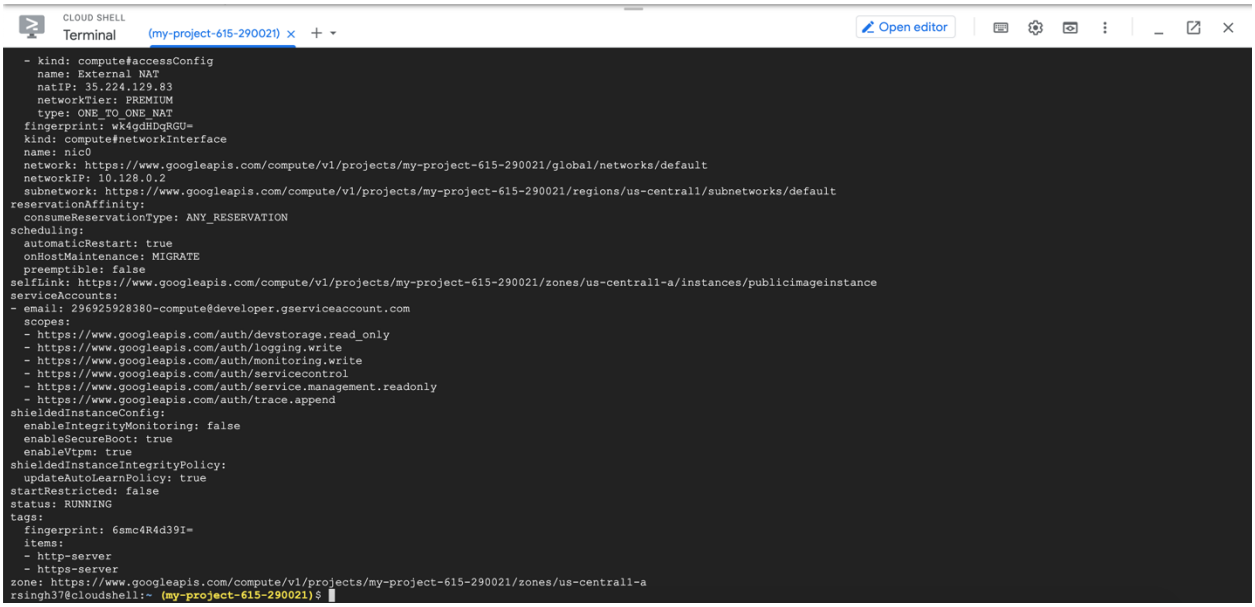
I can check a created instance's status by using gcloud command:

$gcloud compute instances list #This command lists all the instances running on the cloud. I can view more information about a particular instance by using the command:

$gcloud compute instances describe publicimageinstance #This command shows the details of a single instance publicimageinstance.

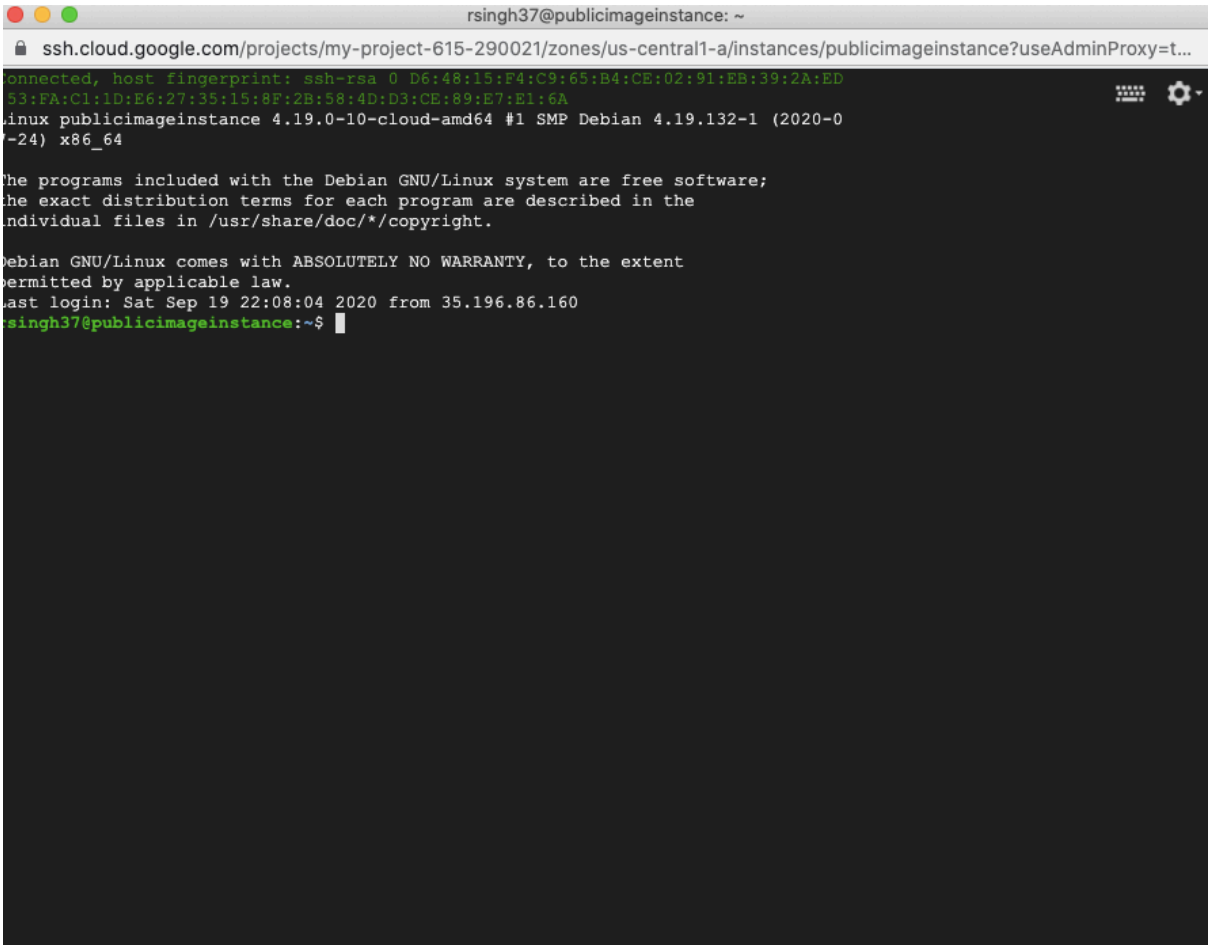




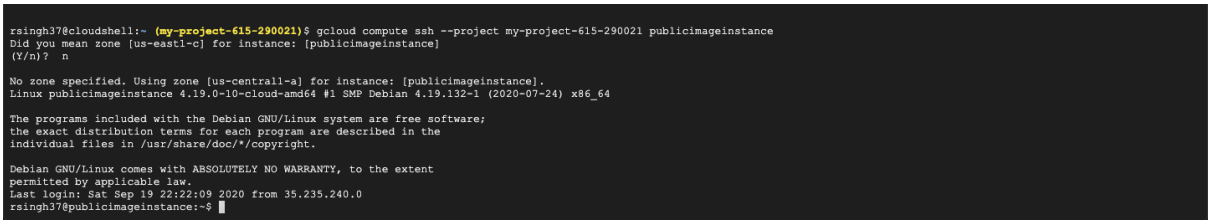


- Connecting to instances
    - Connecting to Linux instances

I can connect to a Linux instance by clicking on the SSH button next in an instance, this will create an SSH connection on the default port. SSH connection are secured due to encryption. Every time a public and private key is created on its own.



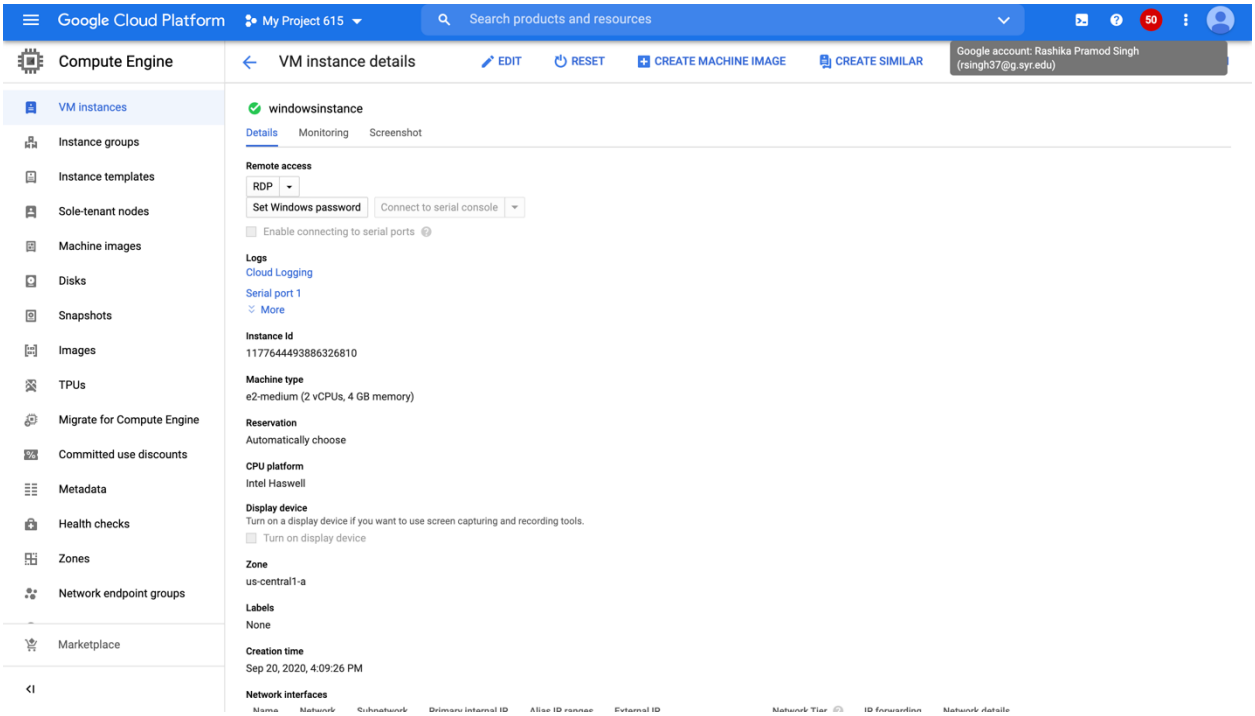
I have also connected to Linux instances using gcloud command:
$gcloud compute ssh –project my-project-615-290021 publicimageinstance #This command connects to instances that I have the permission to connect. Here my-project-615-290021 is the project_id and publicimageinstance is the name of the instance that I want to connect to. This generates a public and private key for the instance

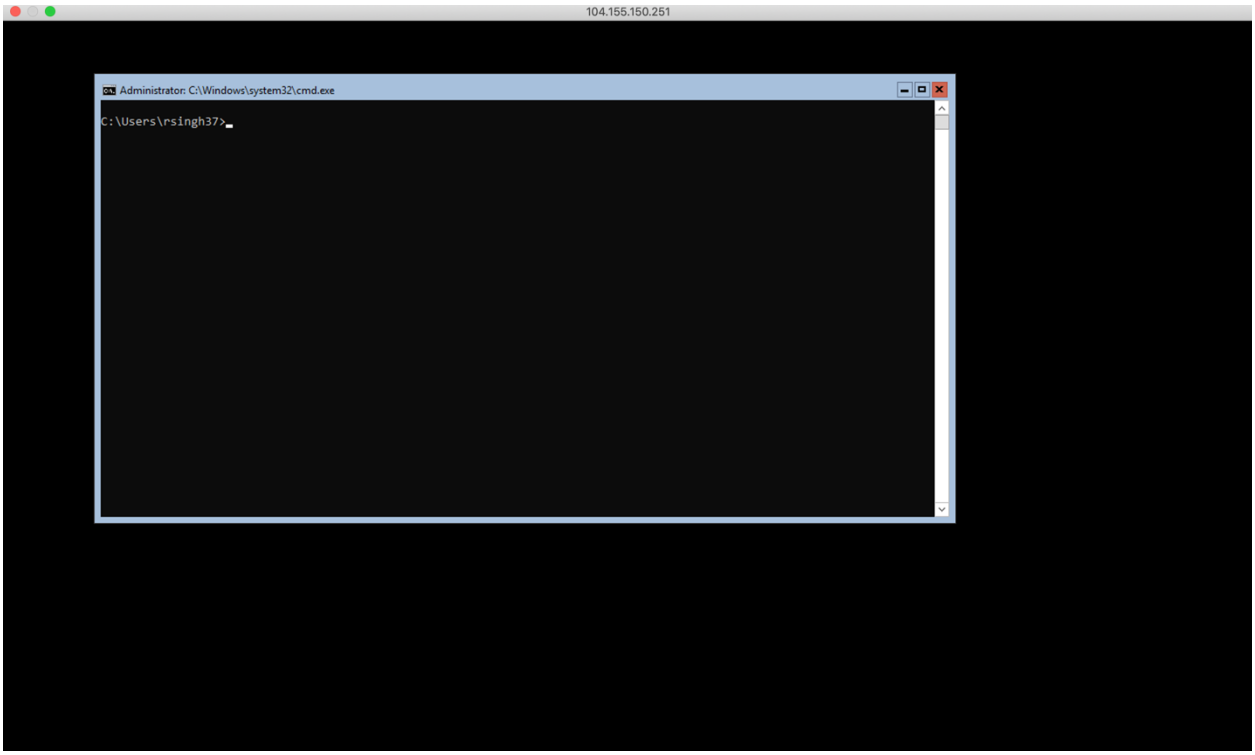


- Connecting to Windows instances

This helps me to connect to a Windows instance. I start by creating a windows instance and creating a password for it. For creating a Windows instance, I change the boot disk as Windows server and note the external IP of the Windows instance that I want to connect to. Then, I use Microsoft Remote Desktop to connect to the instances using the external IP and credentials that I

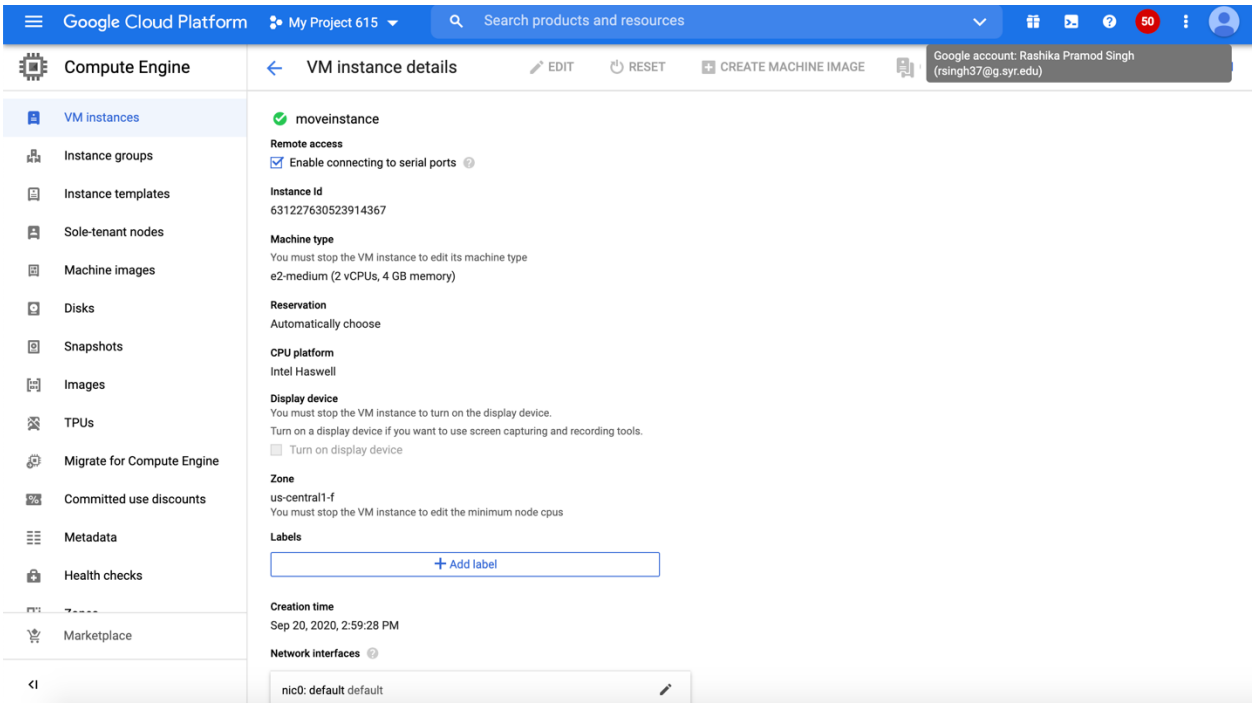
created. The snippet shows creation of a Windows instance and then connecting to it using Remote Desktop.

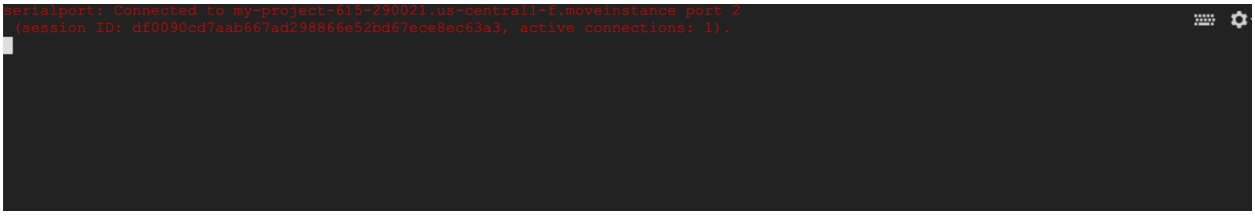




- Special Administrative Console

This is used to connect to an instance using interactive serial console. First you go to the instance you want to establish connection to and edit the instance. Under Remote access, once you enable connecting to serial port, it enables the interactive serial console for the instance. Under remote access, select the connect to serial console and select port 2. You can enable metadata by selecting enable connecting serial ports in the console, this allows the instance to connect to a port.





Using gcloud, I entered the command:
$gcloud compute connect-to-serial-port movieinstance—port=2 #The command connects to the instance moveinstance at port number 2.

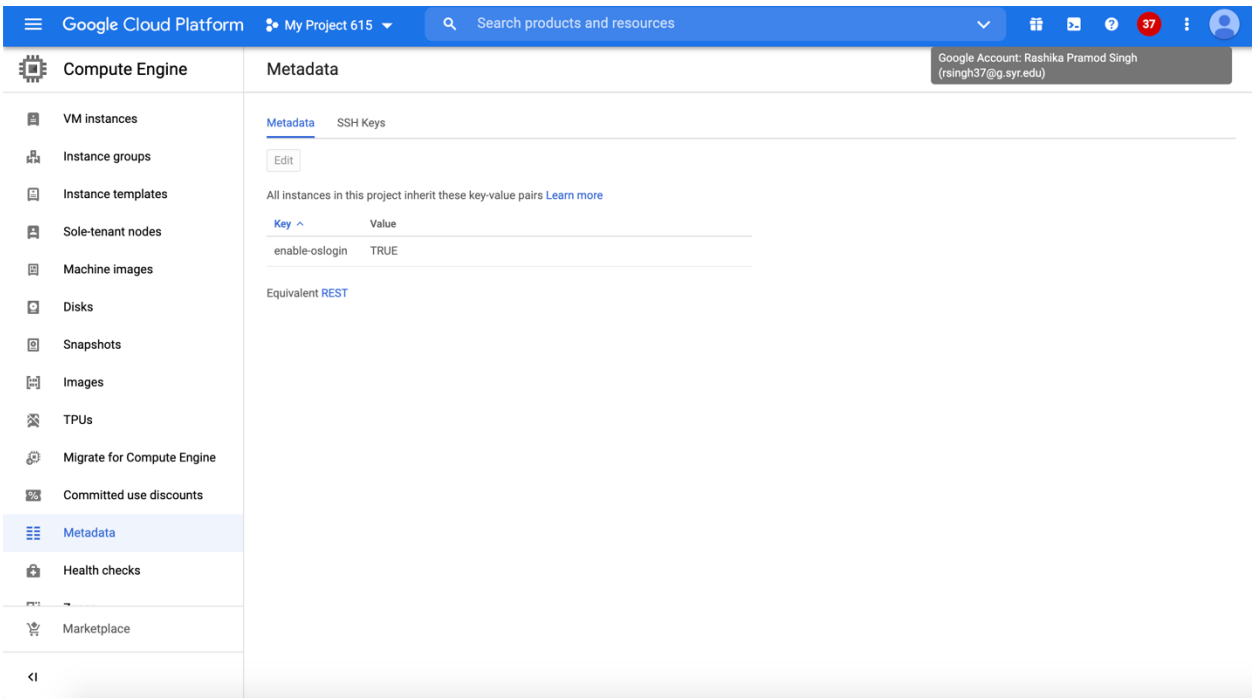
```
Rashikas-Air:~ rashikasingh$ gcloud compute connect-to-serial-port moveinstance
--port=2
No zone specified. Using zone [us-central1-f] for instance: [moveinstance].
serialport: Connected to my-project-615-290021.us-central1-f.moveinstance port 2
 (session ID: 644ffe71fd47a5c83cac5fb7ad29c0ef11583a274c90005122bc68ca3d90c629,
active connections: 1).
```

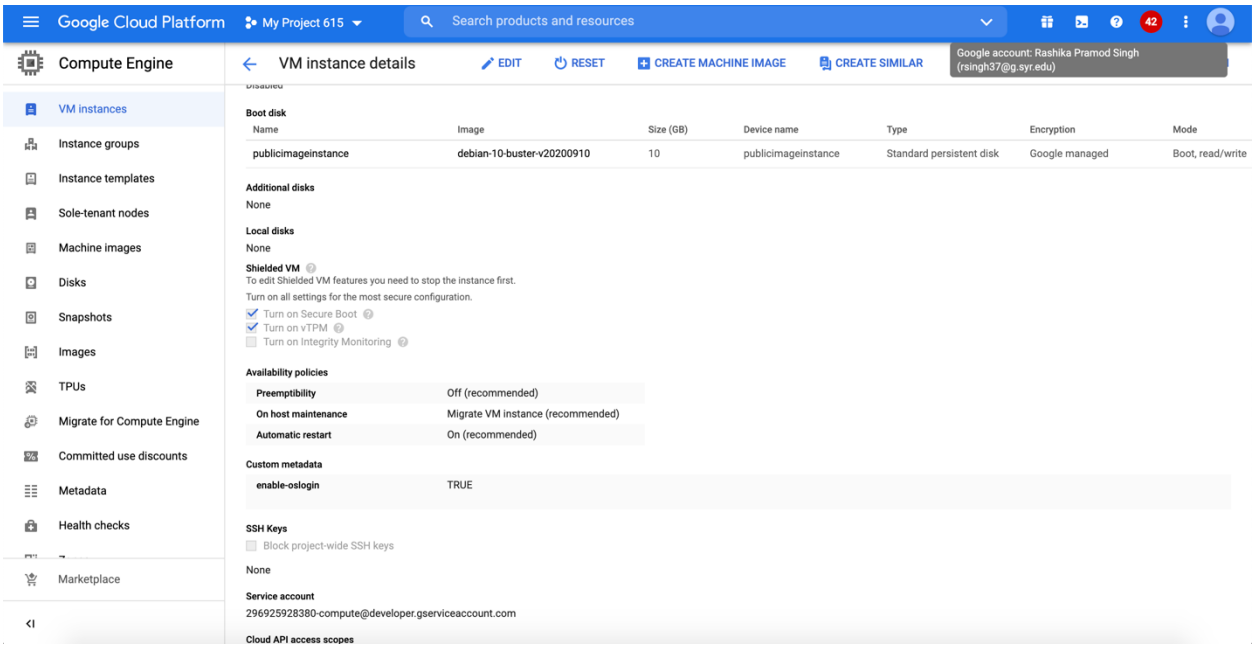
- Connecting to instances using advanced methods
    - Providing public SSH keys to instances

For connecting to instances using advanced methods, you will have to create an SSH key. We create a key-value pair in order to identify the instance from outside. A key-value pair (KVP) is a set of two linked data items: a key which is a unique identifier and value with is the data that is identified to the location of the data. It is used for authentication key pairs for SSH. This is used for automating logins, single sign-on and for authenticating hosts. I create a key-value pair using the command ssh-key-gen where the type is rsa and the key is stored at the location given as gcpkey. The -C is the comment at the text that the username is rsingh37. This generates a public and private key. I enter the paraphrase and then the key is stored to the given location in my local machine.

```
.ssh — -bash — 80×24
The default interactive shell is now zsh.
To update your account to use zsh, please run `chsh -s /bin/zsh`.
For more details, please visit https://support.apple.com/kb/HT208050.
Rashikas-MacBook-Air:~ rashikasingh$ ssh-keygen -t rsa -f ~/.ssh/gcpkey -C rsingh37
Generating public/private rsa key pair.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /Users/rashikasingh/.ssh/gcpkey.
Your public key has been saved in /Users/rashikasingh/.ssh/gcpkey.pub.
The key fingerprint is:
SHA256:i0NZksqNERptXgqGwjmaxeNt6hB2XqU/CJ1UtzM+noY rsingh37
The key's randomart image is:
+---[RSA 3072]----+
|.oo.. .. .       |
|o+*ooo.o. .      |
|o=o*+o* .+       |
|+..+=X +. o      |
|..oo* * So       |
|. .. o +o.o      |
| o    oEo+       |
|  .    ..        |
|                 |
+----[SHA256]-----+
```

The screenshot shows that I have to Enable OS-login as it allows linking the account to the instance. In the custom metadata, I enable-oslogin as TRUE.





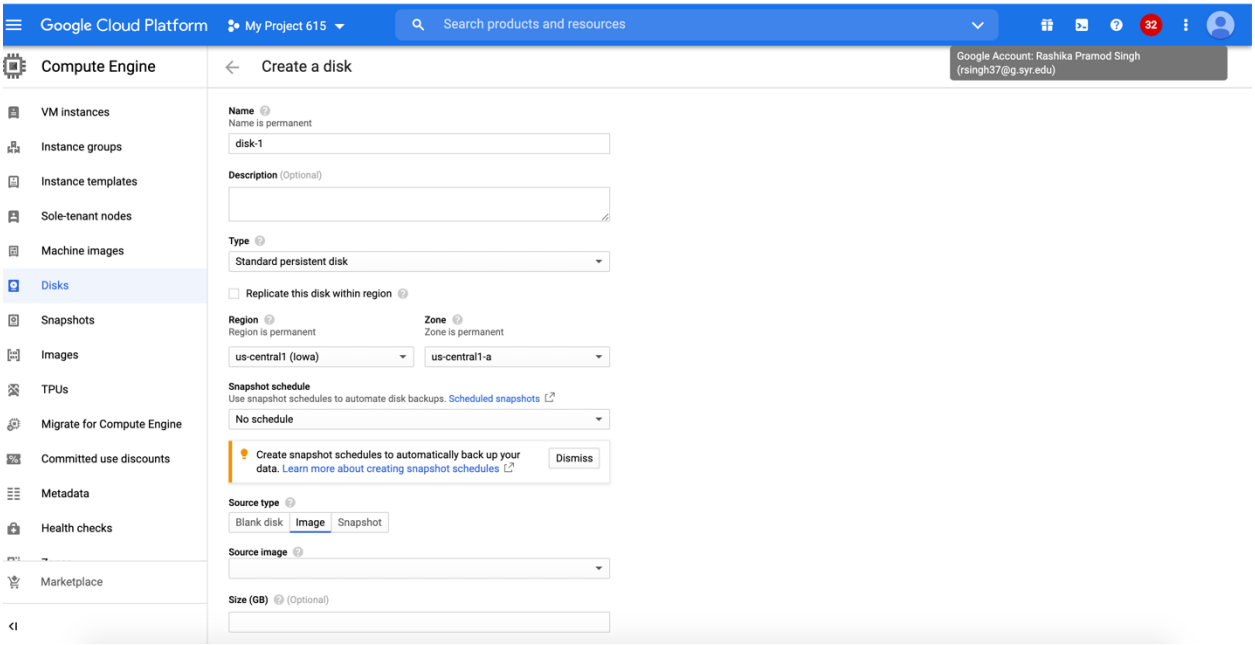
Then in my terminal, I added the public key to the user account using the gcloud command: $gcloud compute os-login ssh-keys add –key-file ~/.ssh/gcpkey.pub –ttl 0 #this command adds the user to the key and sets expiration time to 0. Following that, I check the user profile using gcloud compute os-login describe-profile. I can see that my user key is added with the username. O use the command:

$ ssh -i ~/.ssh/gcpkey rsingh37_g_syr_edu@34.122.40.72 # The command specifies the path, rsingh37_g_syr_edu is the username and after @ is the external IP of the instance that I want to connect to. A successful connection is established, and I can close the connection using exit command.

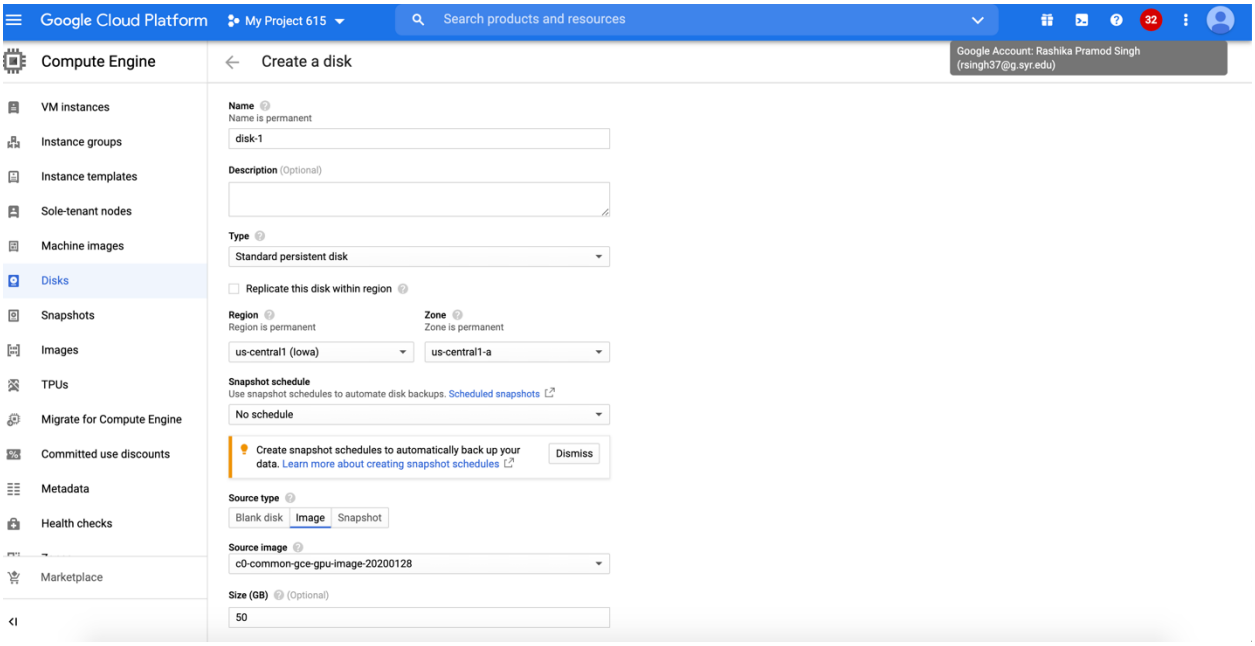
```
Last login: Sun Sep 20 11:18:10 on ttys000

The default interactive shell is now zsh.
To update your account to use zsh, please run `chsh -s /bin/zsh`.
For more details, please visit https://support.apple.com/kb/HT208050.
Rashikas-Air:~ rashikasingh$ gcloud compute os-login describe-profile
name: '104206022127936168550'
posixAccounts:
- gid: '1000127429'
  homeDirectory: /home/rsingh37_g_syr_edu
  operatingSystemType: LINUX
  primary: true
  uid: '1000127429'
  username: rsingh37_g_syr_edu
sshPublicKeys:
  4403965df357448aa30f70e8e9466e4fbdeb7c7a80fd76131037e9347f80c170:
    fingerprint: 4403965df357448aa30f70e8e9466e4fbdeb7c7a80fd76131037e9347f80c170
    key: |
      ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQC4dtHzcMNncum0WmKdKB1aMRC8nmnPilSdxc2ygjBQw0m1s4fcsiVJwh9OOluRHzfbc6k3M07VAecRRe1yrB31mYf8z9ATkjm7E42j+OsOUhG8m6nnPddf4adJ+Lg+hYPi/q3j9Hy7Aipu76+lNN6foXq312gUWn
CBy5gauedffvchPEsyqwuD8A40drbexcWPd5QUuAu0s21RjGpAXlHoouJy54PHPQeojp4kj0+uce4U2mBAQee/GsQzXgtuDXsTytT3byiWJpplm4Yn370vvOklTZdt6eBRhSNj1wVQzgBqwpKqHsUWaPZKMjRiy45O6X6qMFH+mEhzycVDc3pUiaqu3+GxRJy3nrA4PXr6sS
cwBLcZys5YtEquXtwWcxqu1msX27+cHsdj8mhmtuvbpVtL3tmn+6DgRs0y54o+0/alHTVsX2up+TjUiEAv/7diGPRT6dU7xFzUn/nfjqgF8hFP2zFkP5oyVl0ThuMdNX5iLu8AWvvpeEAUFvH2WLE= rsingh37
    name: users/rsingh37@g.syr.edu/sshPublicKeys/4403965df357448aa30f70e8e9466e4fbdeb7c7a80fd76131037e9347f80c170
Rashikas-Air:~ rashikasingh$ ssh -i ~/.ssh/gcpkey rsingh37_g_syr_edu@34.122.40.72
Linux publicimageinstance 4.19.0-10-cloud-amd64 #1 SMP Debian 4.19.132-1 (2020-07-24) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Creating directory '/home/rsingh37_g_syr_edu'.
rsingh37_g_syr_edu@publicimageinstance:~$ exit
logout
Connection to 34.122.40.72 closed.
Rashikas-Air:~ rashikasingh$
```

- Creating customized Boot Disks
  - Creating a standalone boot persistent disk from an image.

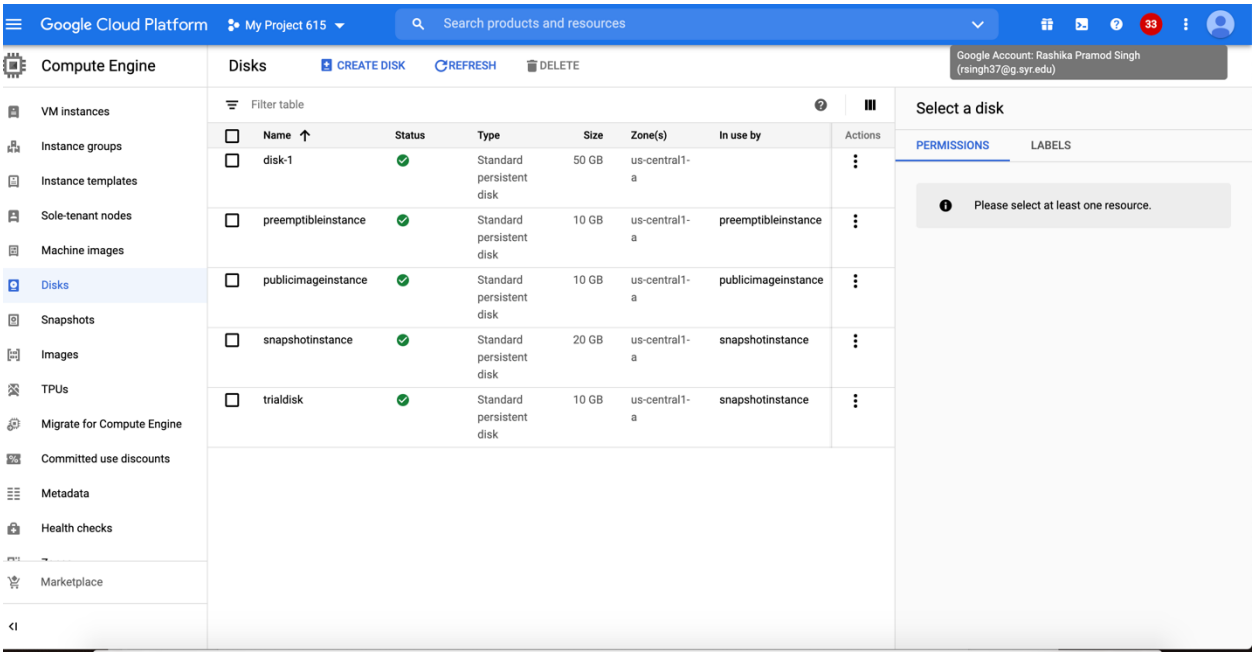
    A boot disk is a digital storage medium from which a computer can load and run an operating system or program. A computer must have a built-in program which will load and execute a program from a boot disk meeting certain standard. When we create a VM we also require a boot disk for the VM. We can create a disk using the following steps in the create instances.



I add a source image as the selected below with size 50GB.

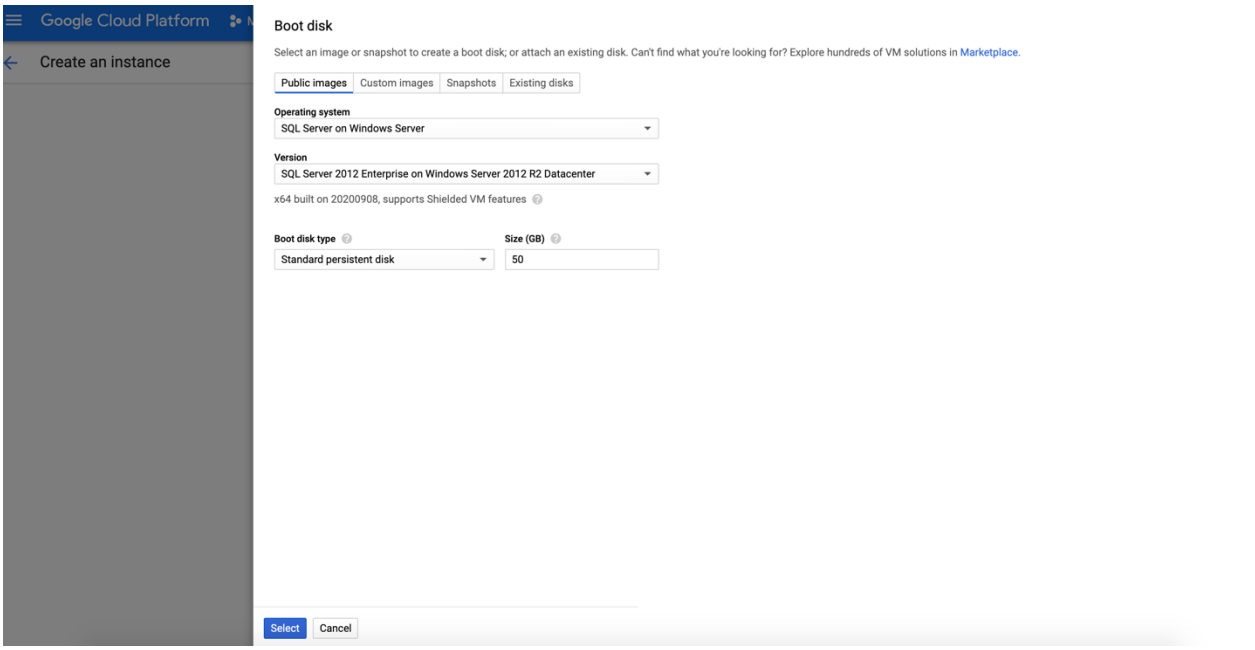


The following snippet shows the successful creation of the boot disk.

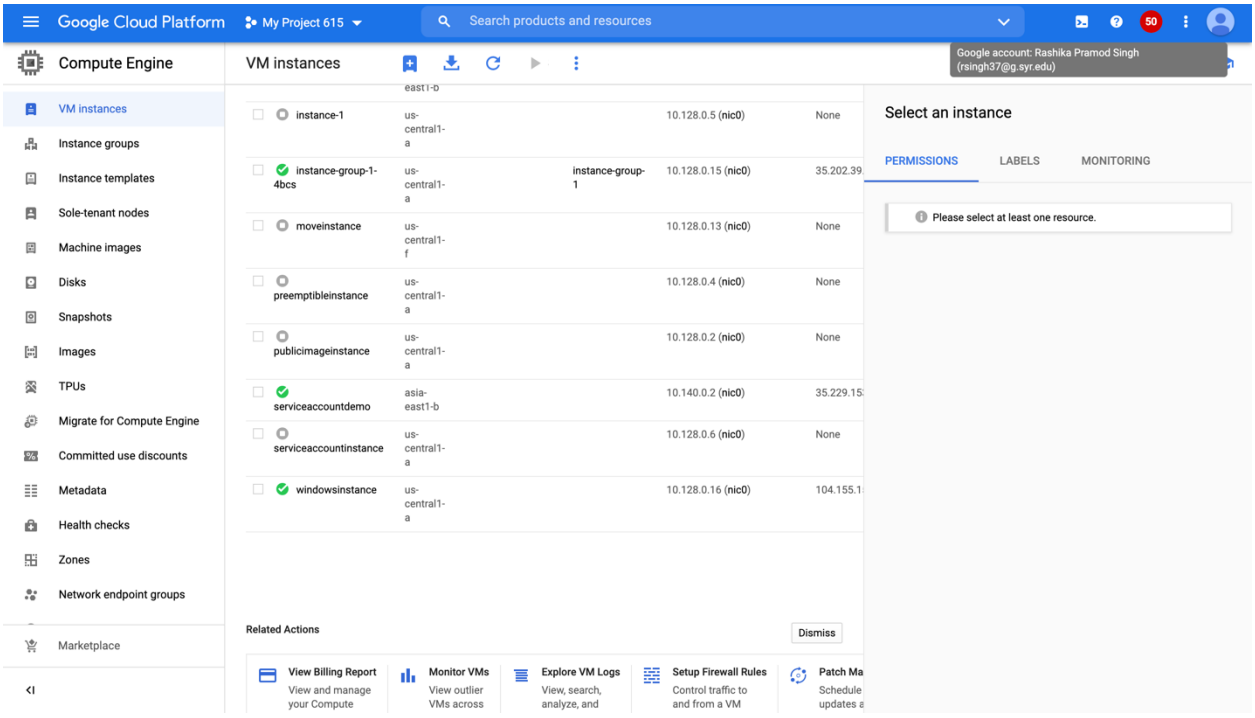


- Creating SQL Server instances

You can also create a VM with a preconfigured SQL Server public image. I make the changes in the create VM, you must enable billing as this is not included in the free version.



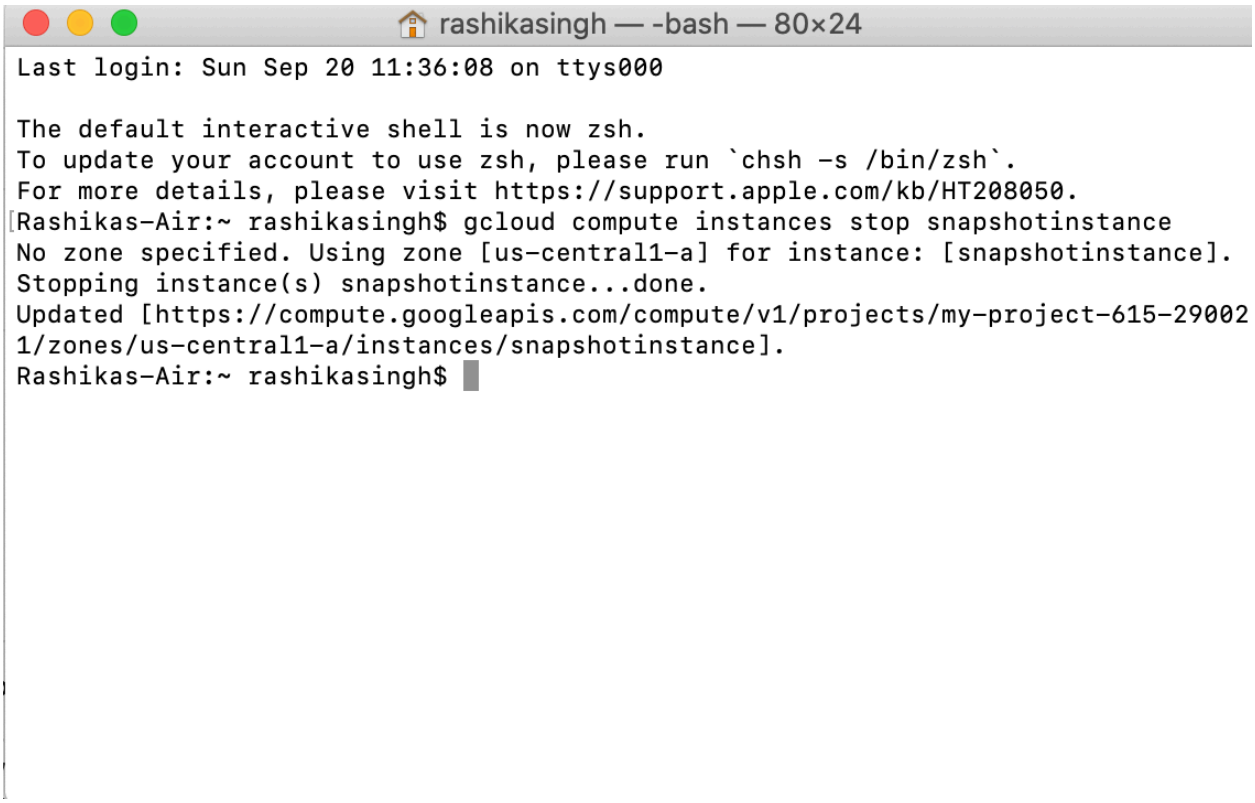
The screenshot shows successful creation of the instance-1 which I later stopped.



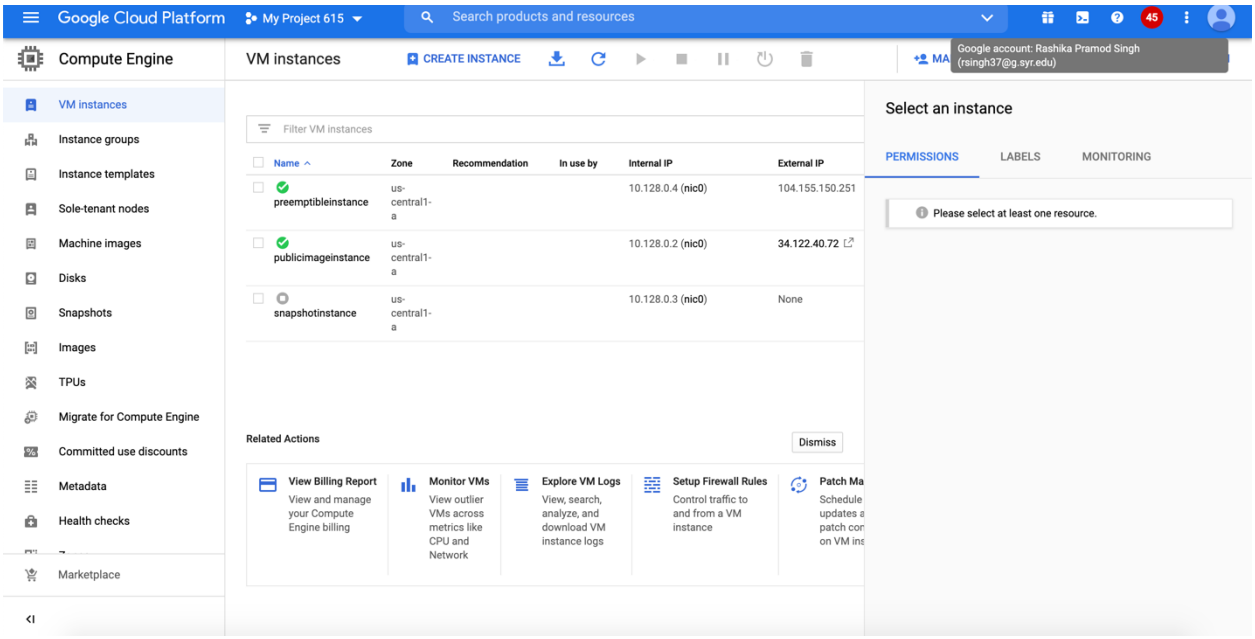
3. Managing your instances

- Stopping an instance (gcloud)

  You can stop an instance using gcloud command, the command has to have the instance name like the snapshotinstance in the screenshot.



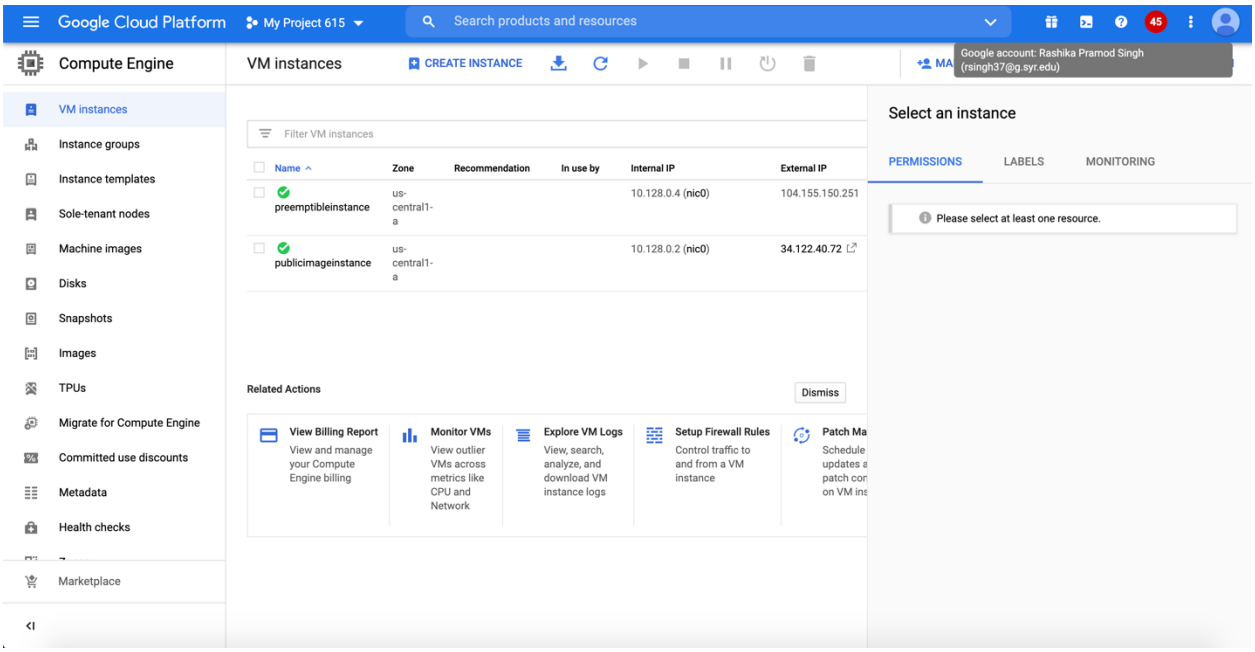
The snapshotinstance is stopped.



- Deleting an instance
  You can delete an instance by specifying the instance name in the gcloud command gcloud delete, I used snapshotinstance.

```
rashikasingh — -bash — 91×26
Last login: Sun Sep 20 11:36:08 on ttys000

The default interactive shell is now zsh.
To update your account to use zsh, please run `chsh -s /bin/zsh`.
For more details, please visit https://support.apple.com/kb/HT208050.
Rashikas-Air:~ rashikasingh$ gcloud compute instances stop snapshotinstance
No zone specified. Using zone [us-central1-a] for instance: [snapshotinstance].
Stopping instance(s) snapshotinstance...done.
Updated [https://compute.googleapis.com/compute/v1/projects/my-project-615-290021/zones/us-
central1-a/instances/snapshotinstance].
Rashikas-Air:~ rashikasingh$ gcloud compute instances delete snapshotinstance
No zone specified. Using zone [us-central1-a] for instance: [snapshotinstance].
The following instances will be deleted. Any attached disks configured
 to be auto-deleted will be deleted unless they are attached to any
other instances or the `--keep-disks` flag is given and specifies them
 for keeping. Deleting a disk is irreversible and any data on the disk
 will be lost.
 - [snapshotinstance] in [us-central1-a]

Do you want to continue (Y/n)?  Y

Deleted [https://www.googleapis.com/compute/v1/projects/my-project-615-290021/zones/us-cent
ral1-a/instances/snapshotinstance].
Rashikas-Air:~ rashikasingh$
```

This screenshot shows that the instance is deleted.



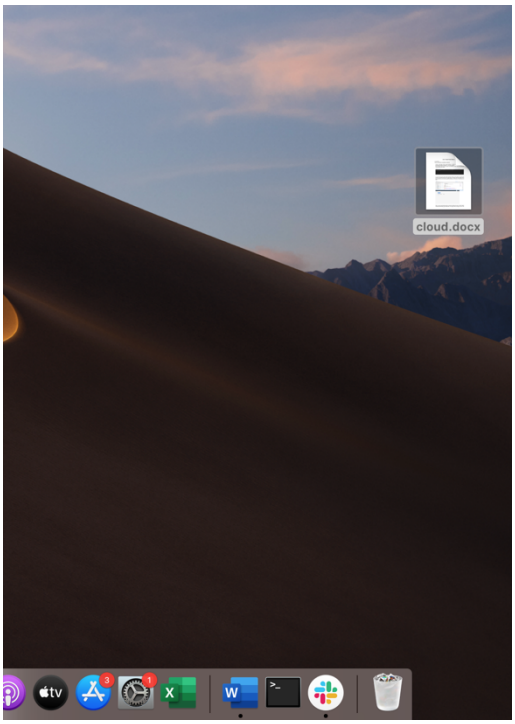
- Moving an instance

You can move an instance from one zone to another using gcloud. You mention the instance name and the current location and the location to be moved. Here the source is us-central1-a and destination zone is us-central1-f.

```
Rashikas-Air:~ rashikasingh$ gcloud compute instances move moveinstance --zone u
s-central1-a --destination-zone us-central1-f
Moving gce instance moveinstance...done.
Rashikas-Air:~ rashikasingh$
```

- Copy files between instance and local computer

Here, I copied a file called cloud.docx from my machine's desktop to the cloud.

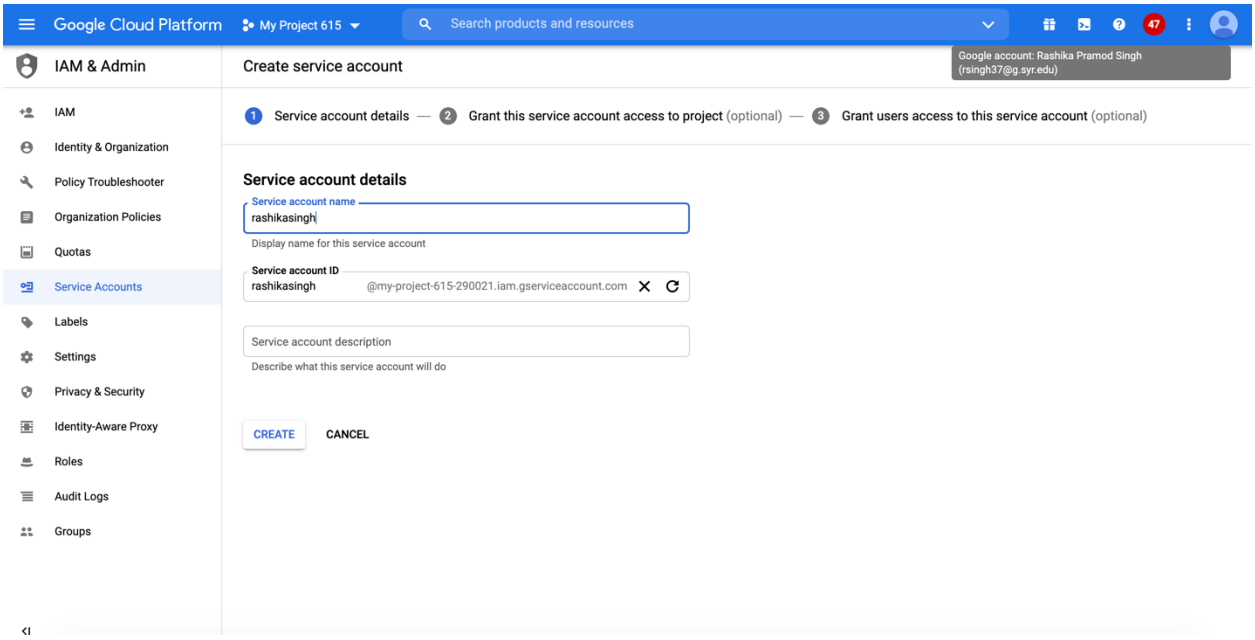


I used the command gcloud compute scp to copy contents from my local computer to the instance publicimageinstance. The screenshot shows that the document is added to the instance.

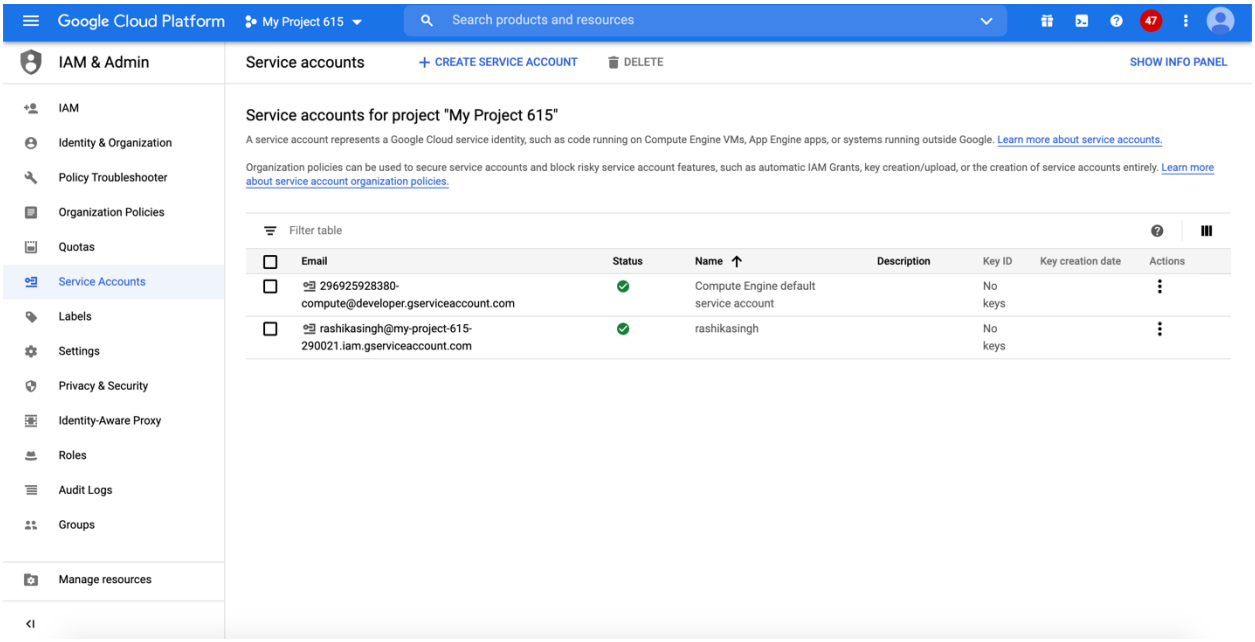
```
rashikasingh — -bash — 129×27
WARNING: The private SSH key file for gcloud does not exist.
WARNING: The public SSH key file for gcloud does not exist.
WARNING: You do not have an SSH key for gcloud.
WARNING: SSH keygen will be executed to generate a key.
Generating public/private rsa key pair.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /Users/rashikasingh/.ssh/google_compute_engine.
Your public key has been saved in /Users/rashikasingh/.ssh/google_compute_engine.pub.
The key fingerprint is:
SHA256:S7un2yRD8RvVdwU9mg/K8qnZsbNGL/aO0YHypn3kuSs rashikasingh@Rashikas-Air.fios-router.home
The key's randomart image is:
+---[RSA 3072]----+
|              .o.|
|             . .o|
|        .   . + +|
|         o ..+ ..|
|        S.+...o  |
|       o +o*.... |
|        = *==..  |
|         *BE==   |
|        +B=*O=o  |
+----[SHA256]-----+
No zone specified. Using zone [us-central1-a] for instance: [publicimageinstance].
Warning: Permanently added 'compute.892048835357690229' (ECDSA) to the list of known hosts.
cloud.docx                                    100% 4462KB   1.0MB/s   00:04
Rashikas-Air:~ rashikasingh$
```

- Setting Access Control
    - Creating a new service account

Service Account is an account linked with an application or VM instead of a user account. I created a service account name rashikasingh and add editor access to the account.

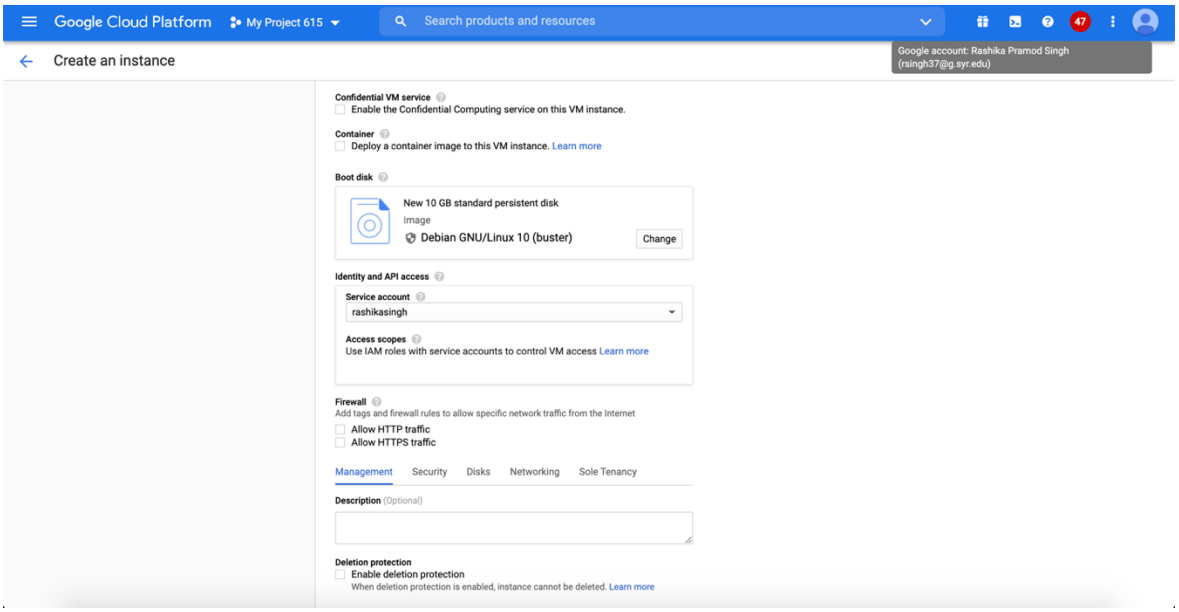


I created a service account rashikasingh for my project 615 which shows in the screenshot.

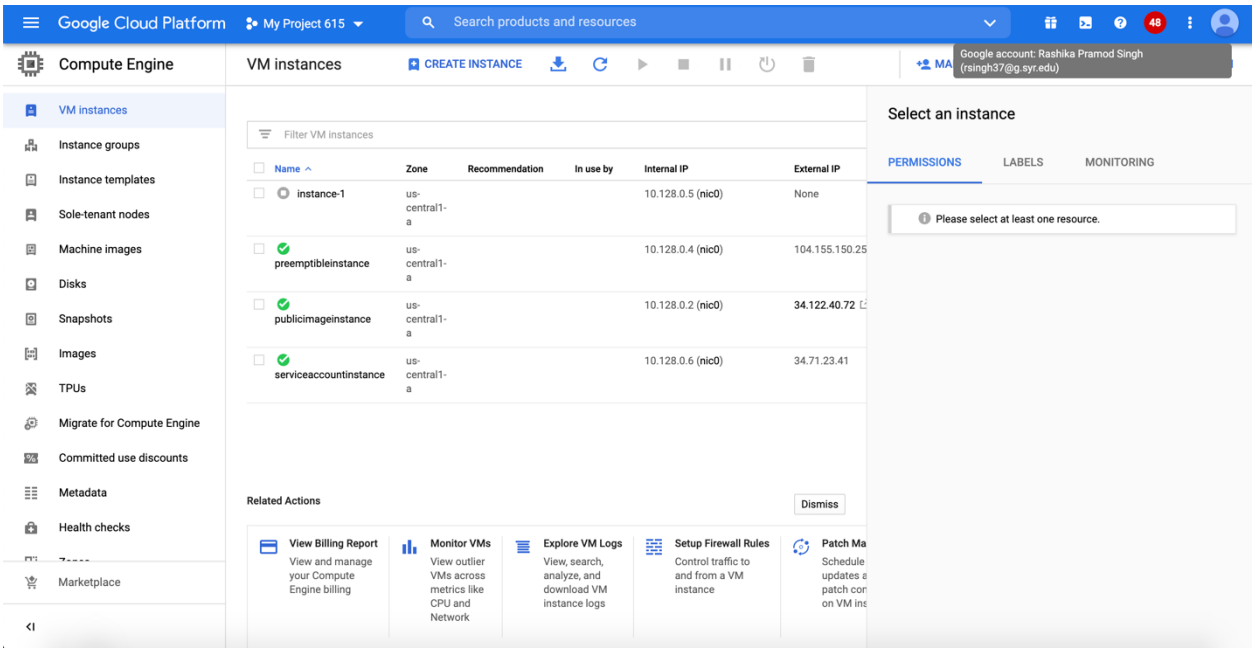


- Setting up a new instance to run as a service account

I created a new instance and, in the identity, and API access added a service account rashikasingh which I created.



The screenshot shows the creation of service account instance using console and gcloud.

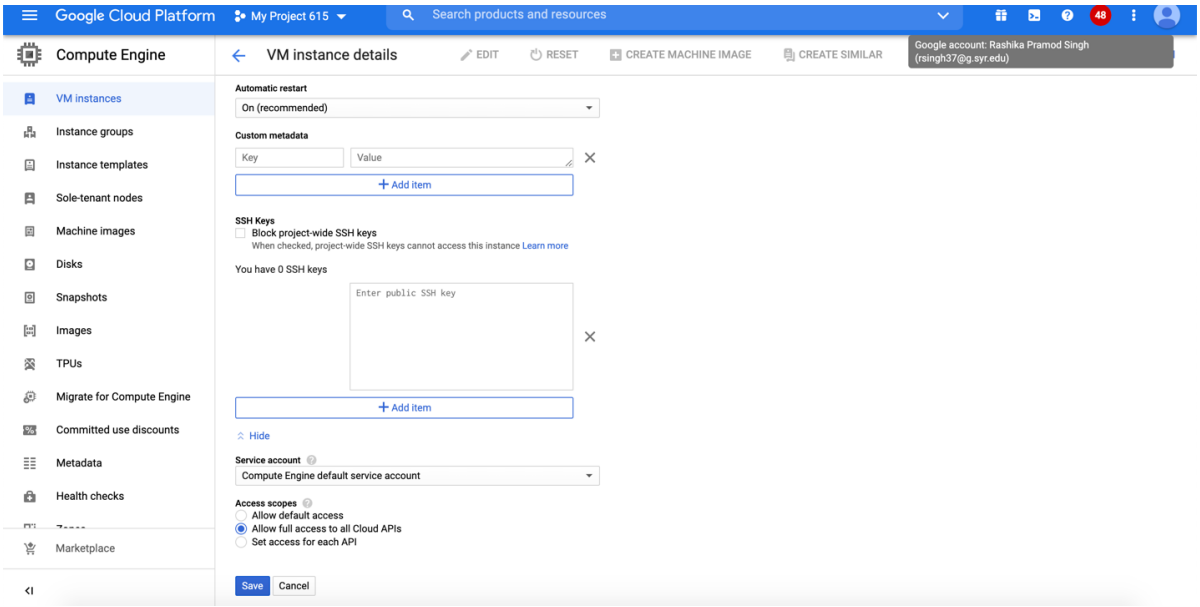


This allows users with the service account to have access to the VM as an editor, the service account email is added in the commandline. One VM can have only one service account.

```
  gcloud compute instances create --help
Rashikas-Air:~ rashikasingh$ gcloud compute instances create serviceaccountdemo --service-account rashikasingh@my-project-615-290021.iam.gserviceaccount.com
For the following instance:
 - [serviceaccountdemo]
choose a zone:
 [1] asia-east1-a
 [2] asia-east1-b
 [3] asia-east1-c
 [4] asia-east2-a
 [5] asia-east2-b
 [6] asia-east2-c
 [7] asia-northeast1-a
 [8] asia-northeast1-b
 [9] asia-northeast1-c
 [10] asia-northeast2-a
 [11] asia-northeast2-b
 [12] asia-northeast2-c
 [13] asia-northeast3-a
 [14] asia-northeast3-b
 [15] asia-northeast3-c
 [16] asia-south1-a
 [17] asia-south1-b
 [18] asia-south1-c
 [19] asia-southeast1-a
 [20] asia-southeast1-b
 [21] asia-southeast1-c
 [22] asia-southeast2-a
 [23] asia-southeast2-b
 [24] asia-southeast2-c
 [25] australia-southeast1-a
 [26] australia-southeast1-b
 [27] australia-southeast1-c
 [28] europe-north1-a
 [29] europe-north1-b
 [30] europe-north1-c
 [31] europe-west1-b
 [32] europe-west1-c
 [33] europe-west1-d
 [34] europe-west2-a
 [35] europe-west2-b
 [36] europe-west2-c
 [37] europe-west3-a
 [38] europe-west3-b
 [39] europe-west3-c
 [40] europe-west4-a
 [41] europe-west4-b
 [42] europe-west4-c
 [43] europe-west6-a
 [44] europe-west6-b
 [45] europe-west6-c
 [46] northamerica-northeast1-a
 [47] northamerica-northeast1-b
 [48] northamerica-northeast1-c
 [49] southamerica-east1-a
 [50] southamerica-east1-b
Did not print [23] options.
Too many options [73]. Enter "list" at prompt to print choices fully.
Please enter your numeric choice:  2

Created [https://www.googleapis.com/compute/v1/projects/my-project-615-290021/zones/asia-east1-b/instances/serviceaccountdemo].
NAME              ZONE          MACHINE_TYPE   PREEMPTIBLE  INTERNAL_IP  EXTERNAL_IP    STATUS
serviceaccountdemo  asia-east1-b  n1-standard-1               10.140.0.2   35.229.153.91  RUNNING
Rashikas-Air:~ rashikasingh$
```

- Changing the service account and access scopes for an instance

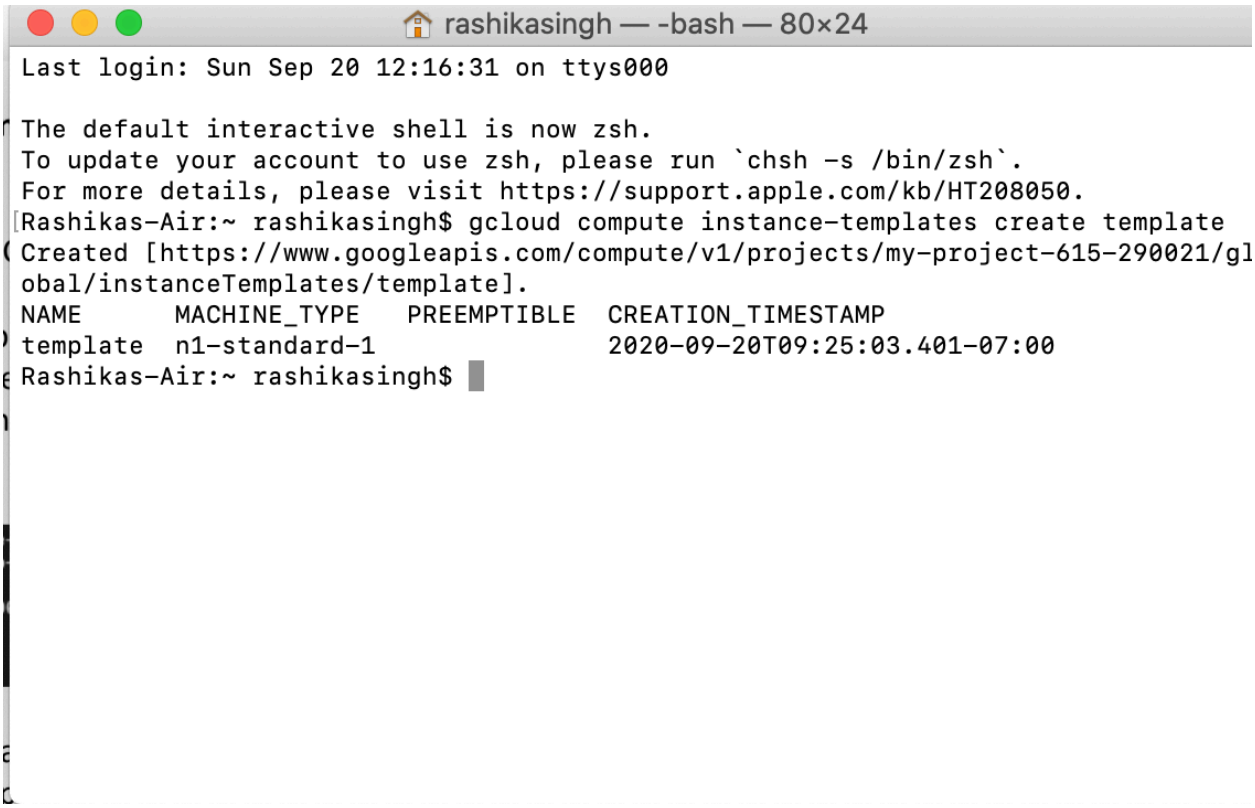
You can change the service account and access scopes for an instance. Here I changed the service account as Compute Engine default account and changed the scope to Allow full access in the console. This allows flexibility if any changes need to be added to the account.



4. Creating and Managing Instance Templates

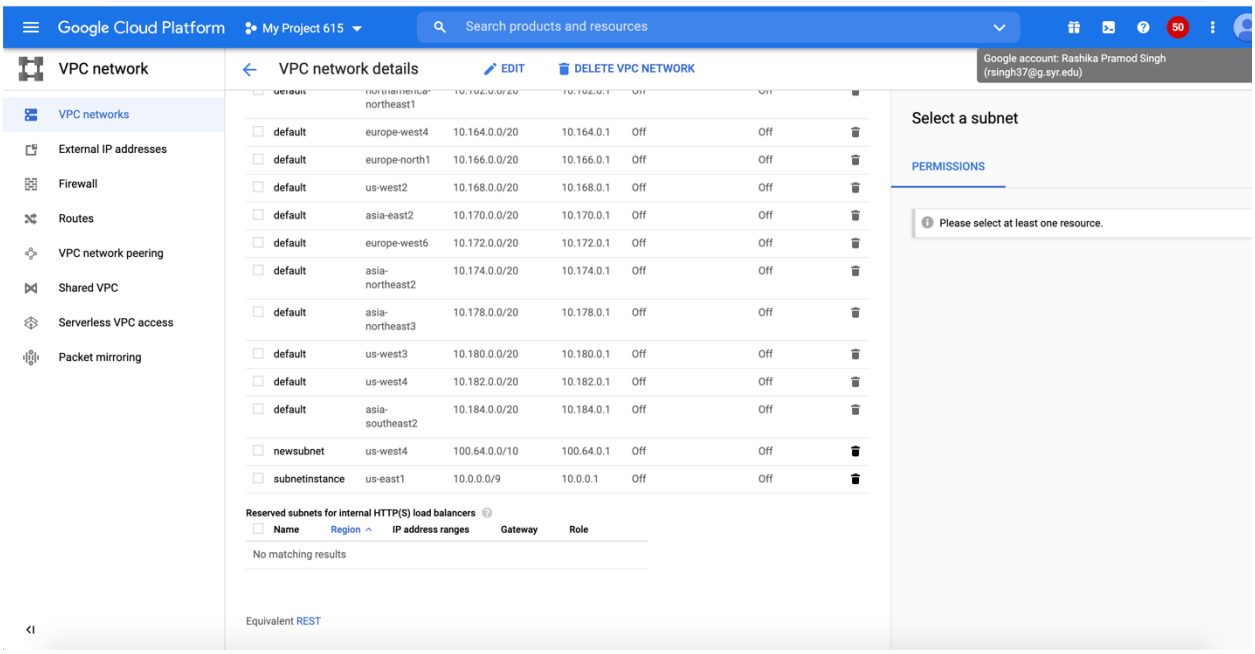
- Creating a new instance template (gcloud)

An instance template is a resource which can be used to created VM instances and managed instance groups. It defines the machine type, boot disk or container image and other properties. This can be used to create a MIG or individual VMs. They are convenient to save a configuration and use late on. I created an instance template using the gcloud command for the project.



- Creating an instance template that specifies a subnet

First, I create a subnet which are regional resources. Each subnet defines range of IP addresses. Traffic to and from instances are controlled by firewall rules. I create a subnetinstance which allows IP ranges mentioned in the creation.



Then, gcloud command creates an instance template in the region with the subnetinstance.

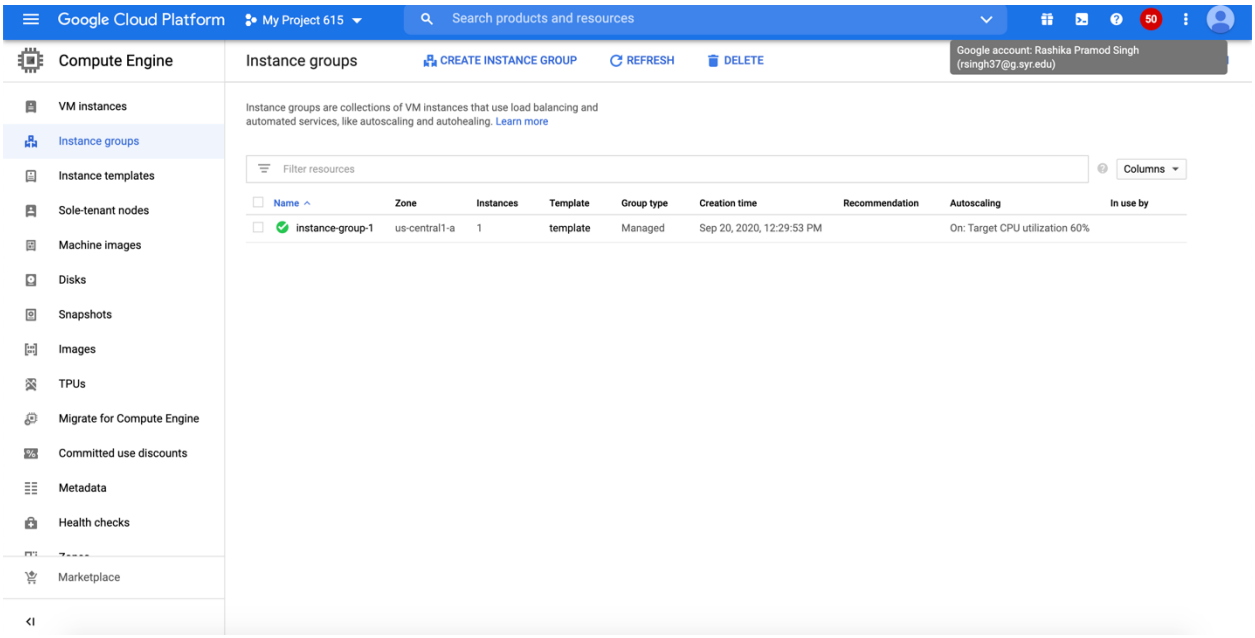
```
Rashikas-Air:~ rashikasingh$ gcloud compute instance-templates create templatesample --region us-east1 --subnet subnetinstance
Created [https://www.googleapis.com/compute/v1/projects/my-project-615-290021/global/instanceTemplates/templatesample].
NAME            MACHINE_TYPE   PREEMPTIBLE  CREATION_TIMESTAMP
templatesample  n1-standard-1               2020-09-20T11:40:14.010-07:00
Rashikas-Air:~ rashikasingh$
```

5. Creating and Managing Groups of Instances

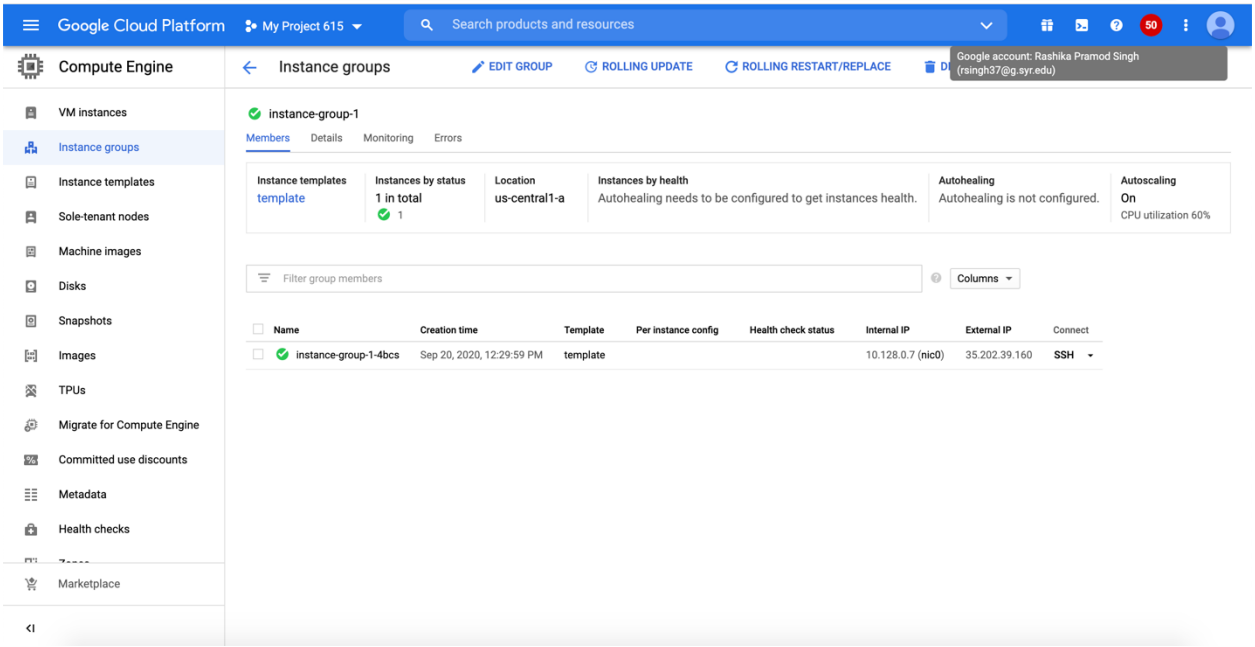
A managed instance group allows you to manage multiple instances together and any change to the configuration affects the group as a whole.

- Creating managed instance groups.
  - Creating a managed instance group

    Here I created a MIG from the console.



This shows specification of the instance group.

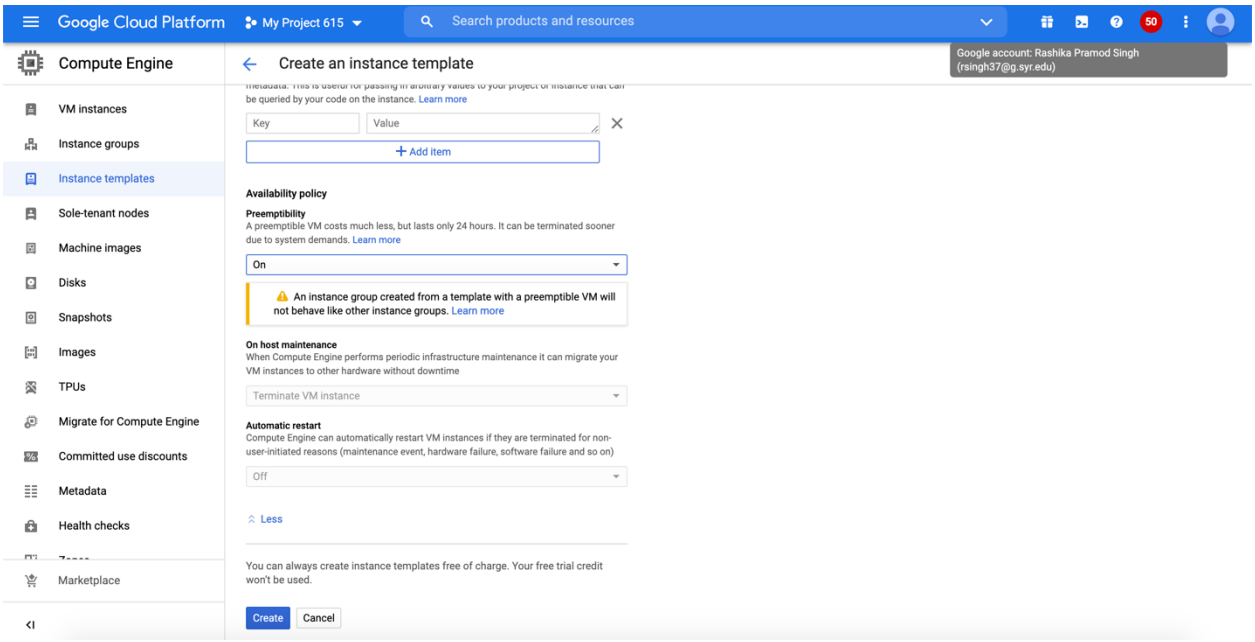


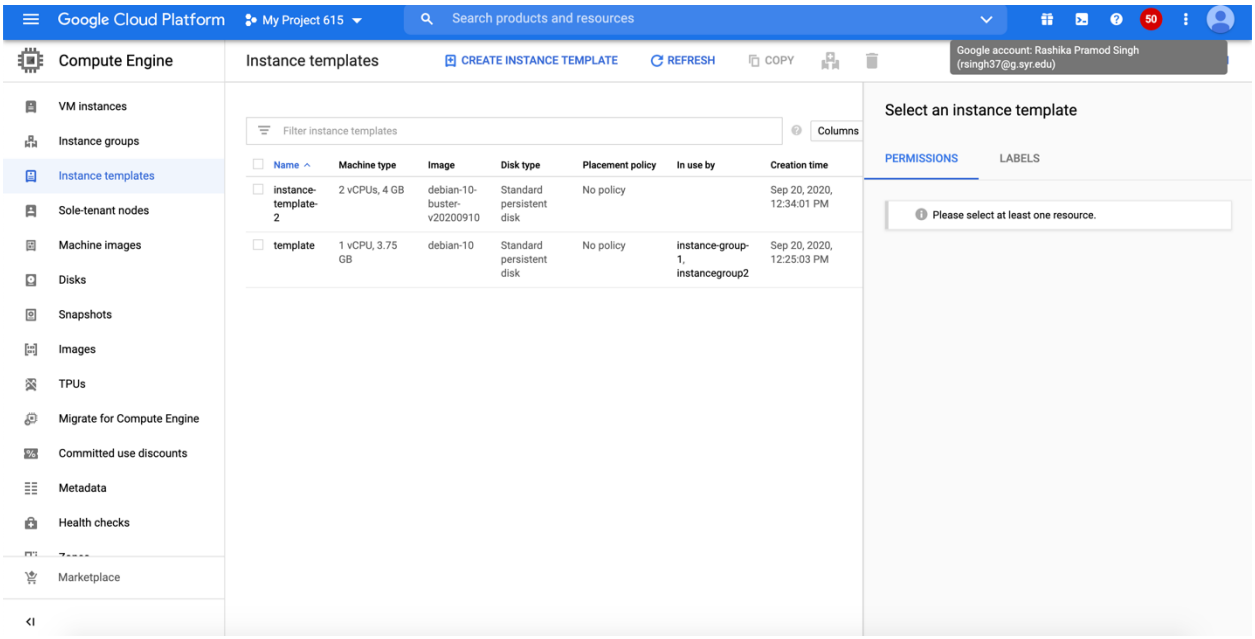
A managed instance group can also be created from the gcloud. Managed is used for creating MIG and the name is given instancegroup2 with a size 5.

```
Rashikas-Air:~ rashikasingh$ gcloud compute instance-groups managed create instancegroup2 --base-instance-name ins --size 5 -
--template template --zone us-east1-b
Created [https://www.googleapis.com/compute/v1/projects/my-project-615-290021/zones/us-east1-b/instanceGroupManagers/instance
group2].
NAME           LOCATION    SCOPE  BASE_INSTANCE_NAME  SIZE  TARGET_SIZE  INSTANCE_TEMPLATE  AUTOSCALED
instancegroup2  us-east1-b  zone   ins                 0     5            template           no
Rashikas-Air:~ rashikasingh$
```

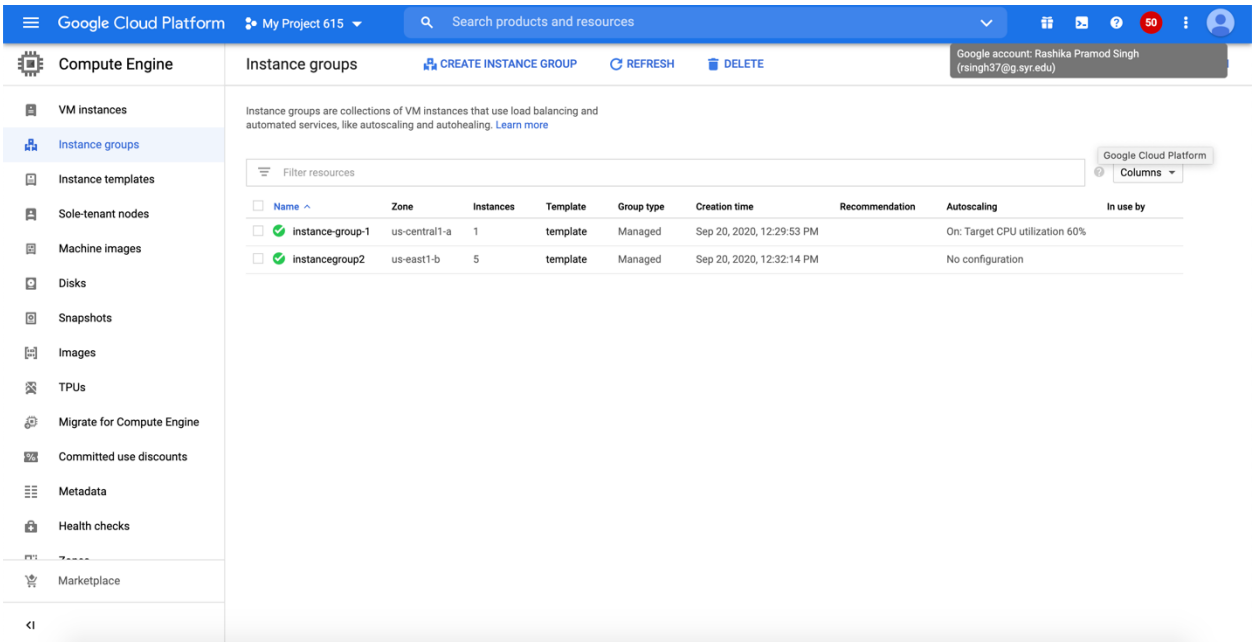
- Creating groups of preemptible instances

For this, first I created an instance template for preemptible instances and then make a group for it.



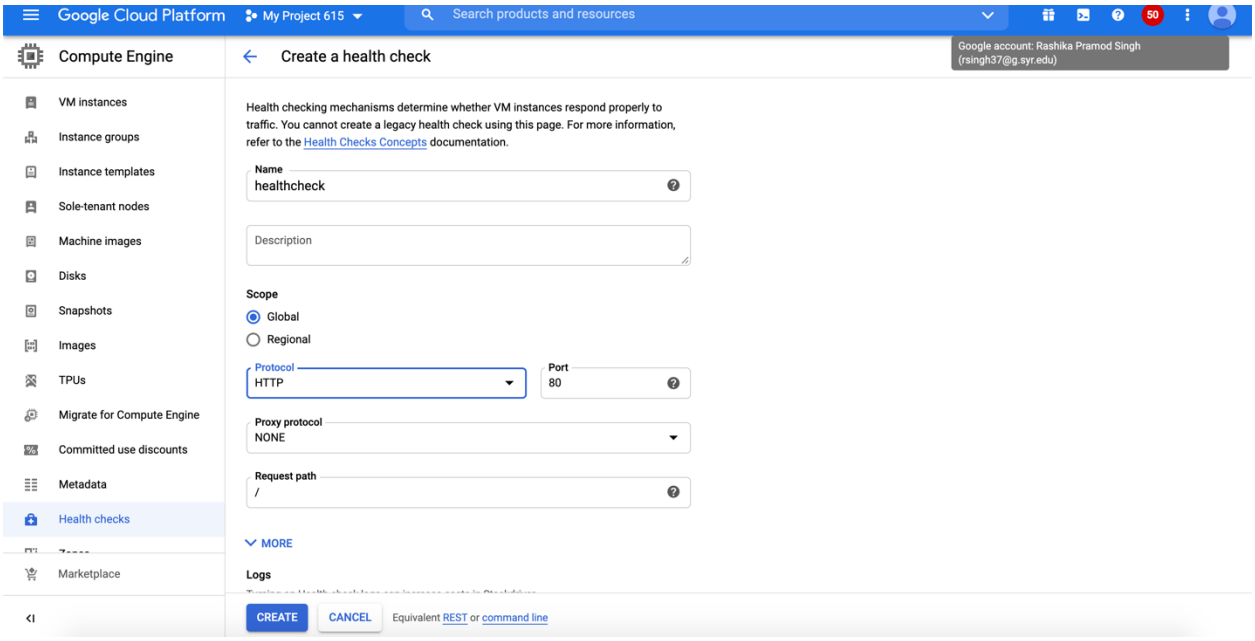


This shows the creation of instance groups.



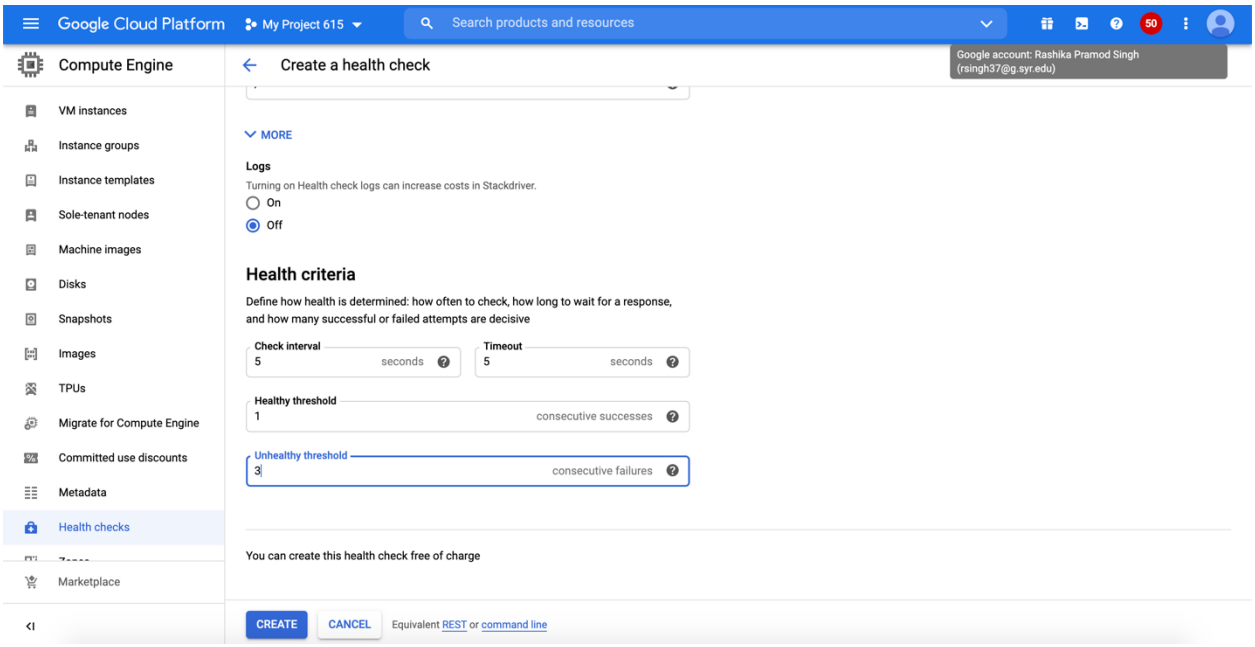
- Setting up health checking and auto healing

Here, I create a health check that looks for protocol HTTP on port 80 and tolerates failure before marking instances as UNHEALTHY.

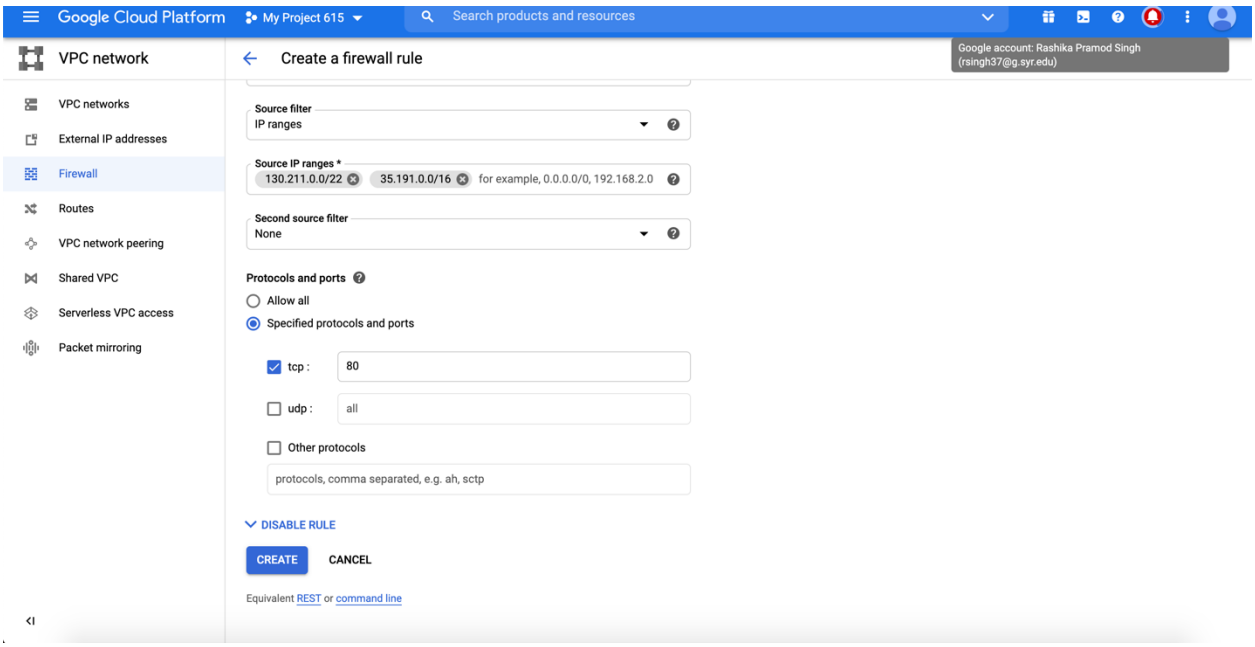


GCP has a UI which provides all information per instance such as protocol, port and health criteria. GCP computes a health state for each instance whose criteria defines how often to check whether an instance is healthy. It includes checks and criteria such as how long to wait for a response, how many successful attempts or unsuccessful attempts are decisive? It defines how many times an instance has to fail before total time period to be considered unhealthy. The health check can even define how many times it has to fail over what total time period before an instance is considered unhealthy.

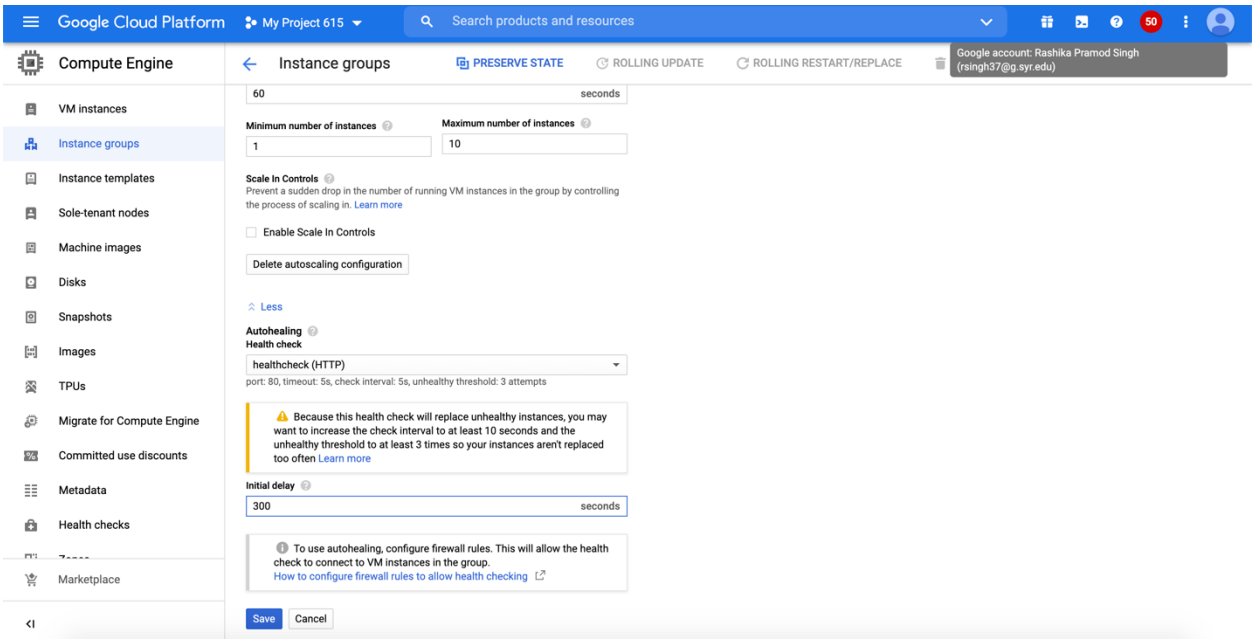
You can set a healthy instance threshold as 1 and unhealthy as 3. If it returns once successfully it is termed healthy and if returns thrice it is UNHEALTHY. This helps to check the health of instances.



I created a firewall rule which will allow the IP ranges with the health checker. This allows incoming traffic only from the mentioned IP.



I enabled the health check in the instance group which was previously created.



The health checker can be created using gcloud it checks on port 80 with an interval of 30s and healthy threshold as 1 and unhealthy as 3.

```
Rashikas-Air:~ rashikasingh$ gcloud compute health-checks create http check2 --port 80 --check-interval 30s --he
althy-threshold 1 --timeout 10s --unhealthy-threshold 3
Created [https://www.googleapis.com/compute/v1/projects/my-project-615-290021/global/healthChecks/check2].
NAME    PROTOCOL
check2  HTTP
Rashikas-Air:~ rashikasingh$
```

This creates firewall rule to allow incoming traffic on tcp:80 with the IP ranges.

```
check2  HTTP
Rashikas-Air:~ rashikasingh$ gcloud compute firewall-rules create allow-health-check2 --allow tcp:80 --source-ranges 130.211.0.0
/22,35.191.0.0/16 --network default
Creating firewall...Created [https://www.googleapis.com/compute/v1/projects/my-project-615-290021/global/firewalls/allow-health
-check2].
Creating firewall...done.
NAME                 NETWORK  DIRECTION  PRIORITY  ALLOW   DENY  DISABLED
allow-health-check2  default  INGRESS    1000      tcp:80        False
Rashikas-Air:~ rashikasingh$
```

This updates the instance group to enable health checker.

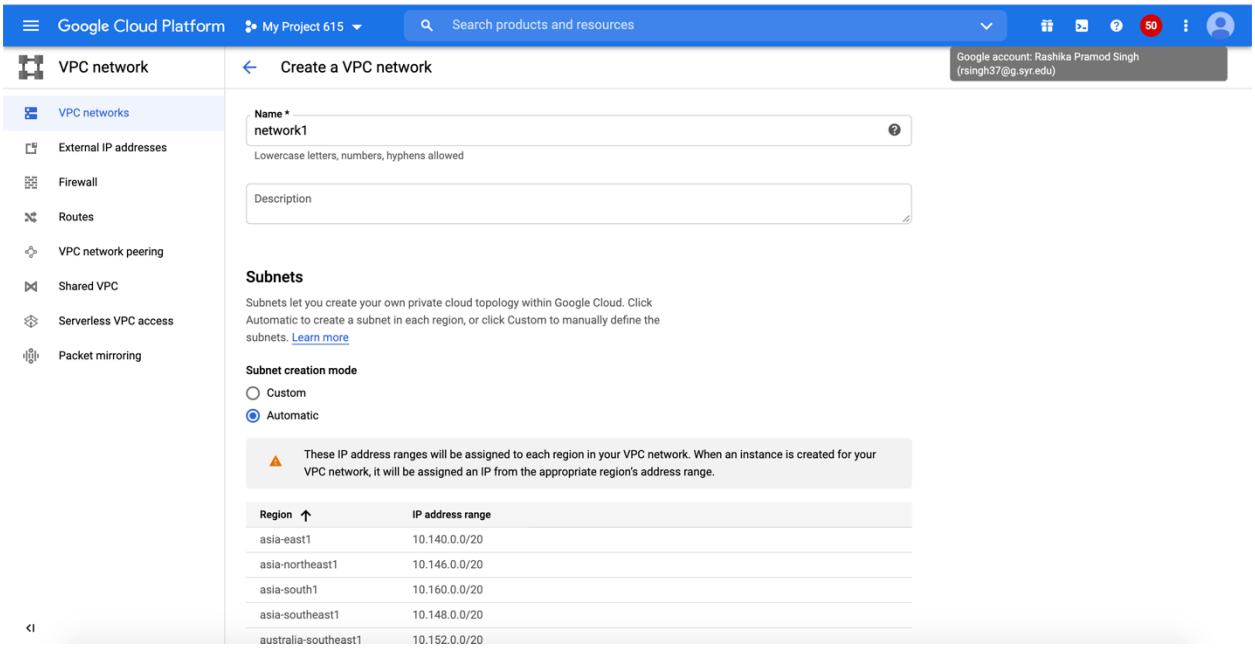
```
Rashikas-Air:~ rashikasingh$ gcloud compute instance-groups managed update instance-group-1 --health-check check2 --initia
l-delay 300 --zone us-central1-a
Updated [https://www.googleapis.com/compute/v1/projects/my-project-615-290021/zones/us-central1-a/instanceGroupManagers/in
stance-group-1].
Rashikas-Air:~ rashikasingh$
```

6. Virtual Private Cloud (VPC)

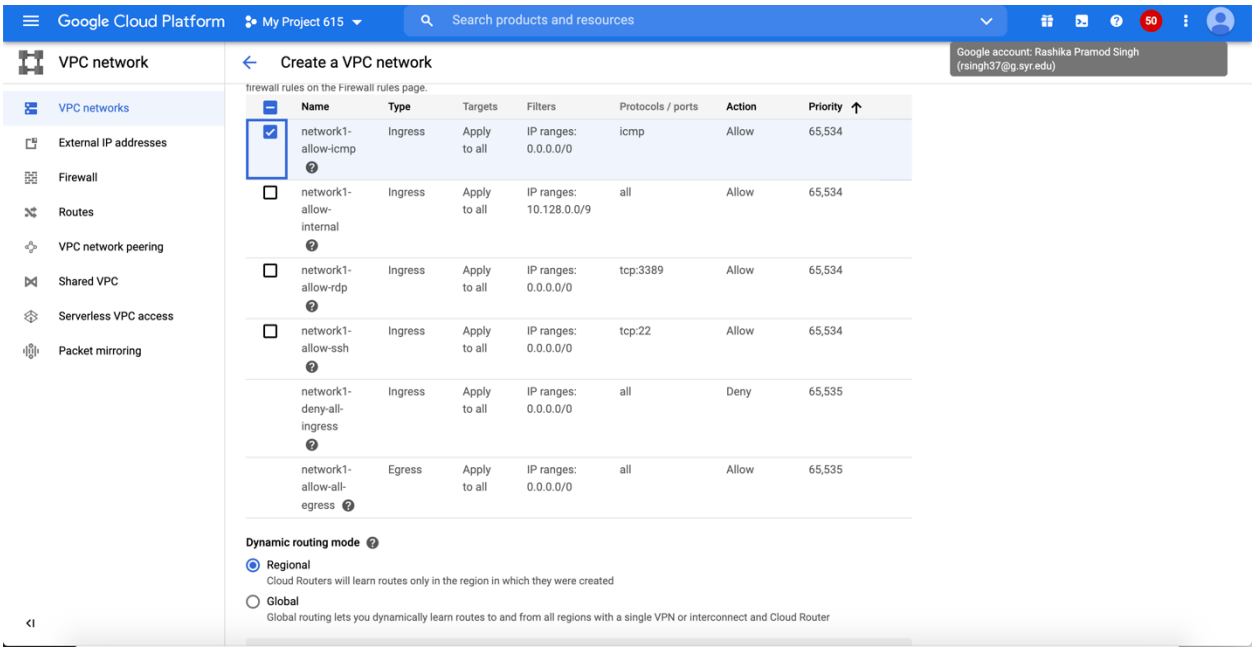
Part 1: A Virtual Private Cloud (VPC) is a global private isolated virtual network partition that provides managed networking functionality for GCP.

- Creating networks
    - Creating an auto mode network

      An auto mode network selects all the regions hence it is automode.



You can also select the firewall rules for the network which allow only certain traffic to pass through.



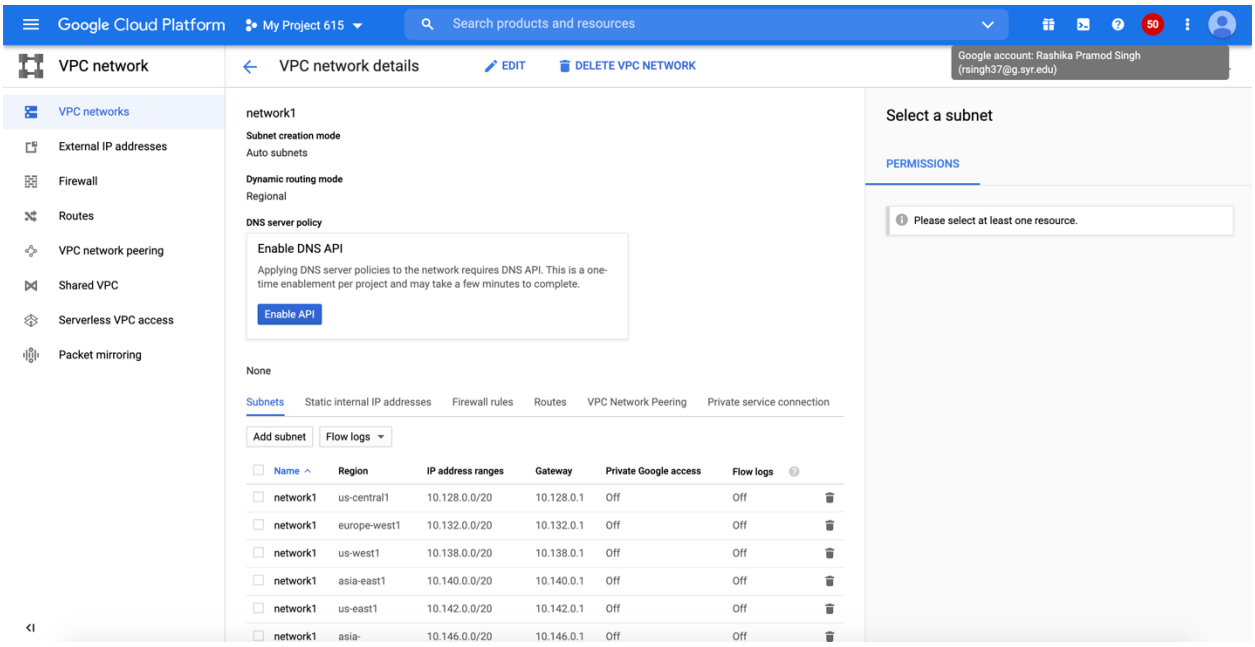
- Creating a custom mode network.
  Here you can select a subnet mode as custom where you can select the mode here I selected regional mode and also selected firewall rules where you can specify which allows tcp, udp and icmp with the source ranges

```
Rashikas-Air:~ rashikasingh$ gcloud compute networks create network2 --subnet-mode=custom --bgp-routing-mode=regional
Created [https://www.googleapis.com/compute/v1/projects/my-project-615-290021/global/networks/network2].
NAME      SUBNET_MODE  BGP_ROUTING_MODE  IPV4_RANGE  GATEWAY_IPV4
network2  CUSTOM       REGIONAL

Instances on this network will not be reachable until firewall rules
are created. As an example, you can allow all internal traffic between
instances as well as SSH, RDP, and ICMP by running:

$ gcloud compute firewall-rules create <FIREWALL_NAME> --network network2 --allow tcp,udp,icmp --source-ranges <IP_RANGE>
$ gcloud compute firewall-rules create <FIREWALL_NAME> --network network2 --allow tcp:22,tcp:3389,icmp

Rashikas-Air:~ rashikasingh$
```

```
$ gcloud compute firewall-rules create <FIREWALL_NAME> --network network2 --allow tcp,udp,icmp --source-ranges <IP_RANGE>
$ gcloud compute firewall-rules create <FIREWALL_NAME> --network network2 --allow tcp:22,tcp:3389,icmp

Rashikas-Air:~ rashikasingh$ gcloud compute networks subnets list
NAME      REGION                   NETWORK   RANGE
default   us-central1              default   10.128.0.0/20
network1  us-central1              network1  10.128.0.0/20
default   europe-west1             default   10.132.0.0/20
network1  europe-west1             network1  10.132.0.0/20
default   us-west1                 default   10.138.0.0/20
network1  us-west1                 network1  10.138.0.0/20
default   asia-east1               default   10.140.0.0/20
network1  asia-east1               network1  10.140.0.0/20
default   us-east1                 default   10.142.0.0/20
network1  us-east1                 network1  10.142.0.0/20
default   asia-northeast1          default   10.146.0.0/20
network1  asia-northeast1          network1  10.146.0.0/20
default   asia-southeast1          default   10.148.0.0/20
network1  asia-southeast1          network1  10.148.0.0/20
default   us-east4                 default   10.150.0.0/20
network1  us-east4                 network1  10.150.0.0/20
default   australia-southeast1     default   10.152.0.0/20
network1  australia-southeast1     network1  10.152.0.0/20
default   europe-west2             default   10.154.0.0/20
network1  europe-west2             network1  10.154.0.0/20
default   europe-west3             default   10.156.0.0/20
network1  europe-west3             network1  10.156.0.0/20
default   southamerica-east1       default   10.158.0.0/20
network1  southamerica-east1       network1  10.158.0.0/20
default   asia-south1              default   10.160.0.0/20
network1  asia-south1              network1  10.160.0.0/20
default   northamerica-northeast1  default   10.162.0.0/20
network1  northamerica-northeast1  network1  10.162.0.0/20
default   europe-west4             default   10.164.0.0/20
network1  europe-west4             network1  10.164.0.0/20
default   europe-north1            default   10.166.0.0/20
network1  europe-north1            network1  10.166.0.0/20
default   us-west2                 default   10.168.0.0/20
network1  us-west2                 network1  10.168.0.0/20
default   asia-east2               default   10.170.0.0/20
network1  asia-east2               network1  10.170.0.0/20
default   europe-west6             default   10.172.0.0/20
network1  europe-west6             network1  10.172.0.0/20
default   asia-northeast2          default   10.174.0.0/20
network1  asia-northeast2          network1  10.174.0.0/20
default   asia-northeast3          default   10.178.0.0/20
network1  asia-northeast3          network1  10.178.0.0/20
default   us-west3                 default   10.180.0.0/20
network1  us-west3                 network1  10.180.0.0/20
default   us-west4                 default   10.182.0.0/20
network1  us-west4                 network1  10.182.0.0/20
default   asia-southeast2          default   10.184.0.0/20
network1  asia-southeast2          network1  10.184.0.0/20
Rashikas-Air:~ rashikasingh$
```

- Viewing networks

  You can view the networks using the console..



- Working with networks
  - Listing subnets

    Subnets are regional resources where each subnet defines a range of IP addresses. Traffic to and from instances can be controlled with network firewall rules. A subnet or subnetwork is a segmented piece of larger network. It is a logical partition of an IP

network into multiple, smaller networks which allows to split a large network into grouping of smaller, interconnected networks to avoid traffic and increase networking speed.

This snippet shows all the subnet networks.

```
$ gcloud compute firewall-rules create <FIREWALL_NAME> --network network2 --allow tcp,udp,icmp --source-ranges <IP_RANGE>
$ gcloud compute firewall-rules create <FIREWALL_NAME> --network network2 --allow tcp:22,tcp:3389,icmp

Rashikas-Air:~ rashikasingh$ gcloud compute networks subnets list
NAME      REGION                   NETWORK   RANGE
default   us-central1              default   10.128.0.0/20
network1  us-central1              network1  10.128.0.0/20
default   europe-west1             default   10.132.0.0/20
network1  europe-west1             network1  10.132.0.0/20
default   us-west1                 default   10.138.0.0/20
network1  us-west1                 network1  10.138.0.0/20
default   asia-east1               default   10.140.0.0/20
network1  asia-east1               network1  10.140.0.0/20
default   us-east1                 default   10.142.0.0/20
network1  us-east1                 network1  10.142.0.0/20
default   asia-northeast1          default   10.146.0.0/20
network1  asia-northeast1          network1  10.146.0.0/20
default   asia-southeast1          default   10.148.0.0/20
network1  asia-southeast1          network1  10.148.0.0/20
default   us-east4                 default   10.150.0.0/20
network1  us-east4                 network1  10.150.0.0/20
default   australia-southeast1     default   10.152.0.0/20
network1  australia-southeast1     network1  10.152.0.0/20
default   europe-west2             default   10.154.0.0/20
network1  europe-west2             network1  10.154.0.0/20
default   europe-west3             default   10.156.0.0/20
network1  europe-west3             network1  10.156.0.0/20
default   southamerica-east1       default   10.158.0.0/20
network1  southamerica-east1       network1  10.158.0.0/20
default   asia-south1              default   10.160.0.0/20
network1  asia-south1              network1  10.160.0.0/20
default   northamerica-northeast1  default   10.162.0.0/20
network1  northamerica-northeast1  network1  10.162.0.0/20
default   europe-west4             default   10.164.0.0/20
network1  europe-west4             network1  10.164.0.0/20
default   europe-north1            default   10.166.0.0/20
network1  europe-north1            network1  10.166.0.0/20
default   us-west2                 default   10.168.0.0/20
network1  us-west2                 network1  10.168.0.0/20
default   asia-east2               default   10.170.0.0/20
network1  asia-east2               network1  10.170.0.0/20
default   europe-west6             default   10.172.0.0/20
network1  europe-west6             network1  10.172.0.0/20
default   asia-northeast2          default   10.174.0.0/20
network1  asia-northeast2          network1  10.174.0.0/20
default   asia-northeast3          default   10.178.0.0/20
network1  asia-northeast3          network1  10.178.0.0/20
default   us-west3                 default   10.180.0.0/20
network1  us-west3                 network1  10.180.0.0/20
default   us-west4                 default   10.182.0.0/20
network1  us-west4                 network1  10.182.0.0/20
default   asia-southeast2          default   10.184.0.0/20
network1  asia-southeast2          network1  10.184.0.0/20
Rashikas-Air:~ rashikasingh$
```

- Describing a subnet

The gcloud command can be used to describe a subnet if we mention the network name and region with details such as creating time, network, region among other details.

```
Rashikas-Air:~ rashikasingh$ gcloud compute networks subnets describe SUBNET_NAME \
>
Rashikas-Air:~ rashikasingh$ gcloud compute networks subnets describe network1 --region us-west3
creationTimestamp: '2020-09-20T09:47:24.945-07:00'
fingerprint: z7WSWdAiba4=
gatewayAddress: 10.180.0.1
id: '8263949363844888947'
ipCidrRange: 10.180.0.0/20
kind: compute#subnetwork
name: network1
network: https://www.googleapis.com/compute/v1/projects/my-project-615-290021/global/networks/network1
privateIpGoogleAccess: false
purpose: PRIVATE
region: https://www.googleapis.com/compute/v1/projects/my-project-615-290021/regions/us-west3
selfLink: https://www.googleapis.com/compute/v1/projects/my-project-615-290021/regions/us-west3/subnetworks/network1
Rashikas-Air:~ rashikasingh$
```

- Adding subnets

This adds subnets using gcloud with the name, network as default and IP range and the region you want the subnet.

```
  gcloud compute networks subnets create --help
Rashikas-Air:~ rashikasingh$ gcloud compute networks subnets create newsubnet --network=default --range=100.64.0.0/10 --region us-west4
Created [https://www.googleapis.com/compute/v1/projects/my-project-615-290021/regions/us-west4/subnetworks/newsubnet].
NAME       REGION    NETWORK  RANGE
newsubnet  us-west4  default  100.64.0.0/10
Rashikas-Air:~ rashikasingh$
```

- Deleting subnets

  This is used to delete an existing subnet with the region mentioned.

```
Rashikas-Air:~ rashikasingh$ gcloud compute networks subnets delete network1 --region=us-central1
The following subnetworks will be deleted:
 - [network1] in [us-central1]

Do you want to continue (Y/n)?  Y

Deleted [https://www.googleapis.com/compute/v1/projects/my-project-615-290021/regions/us-central1/subnetworks/network1].
Rashikas-Air:~ rashikasingh$
```

- Modifying networks
  - Deleting a network

    This deletes an existing network by specifying the existing network name. I also deleted the firewall associated with it to avoid errors.

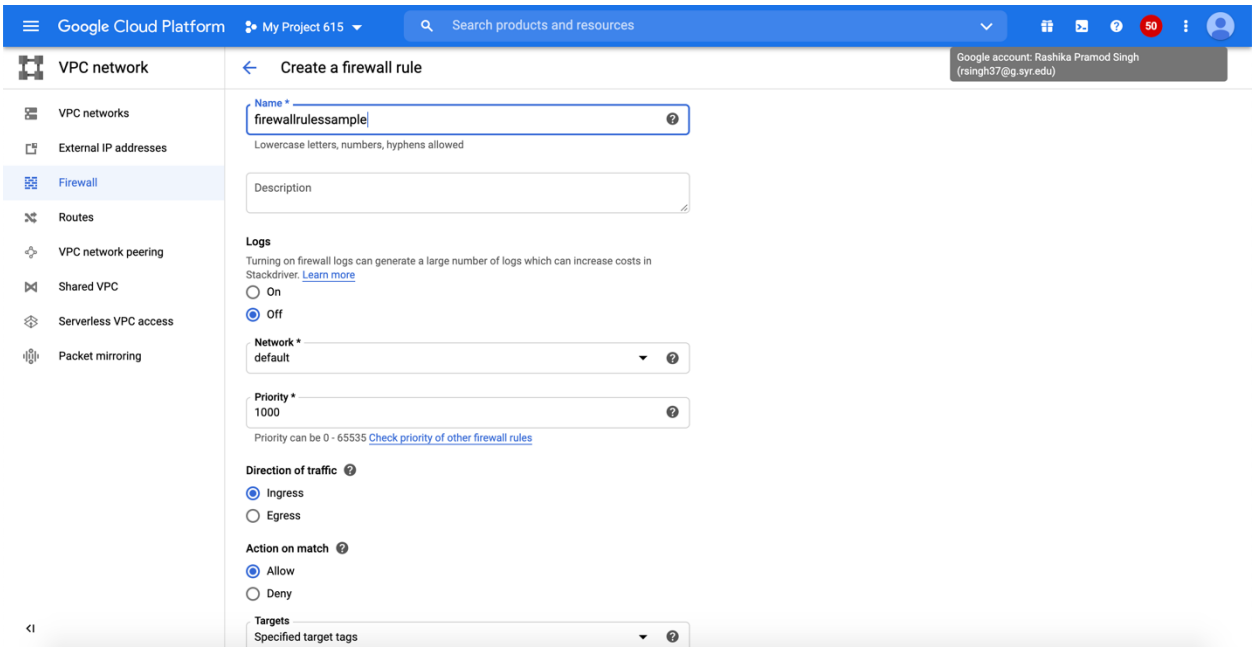
```
Rashikas-Air:~ rashikasingh$ gcloud compute networks delete network2
The following networks will be deleted:
 - [network2]

Do you want to continue (Y/n)?  Y

Deleted [https://www.googleapis.com/compute/v1/projects/my-project-615-290021/global/networks/network2].
Rashikas-Air:~ rashikasingh$
```

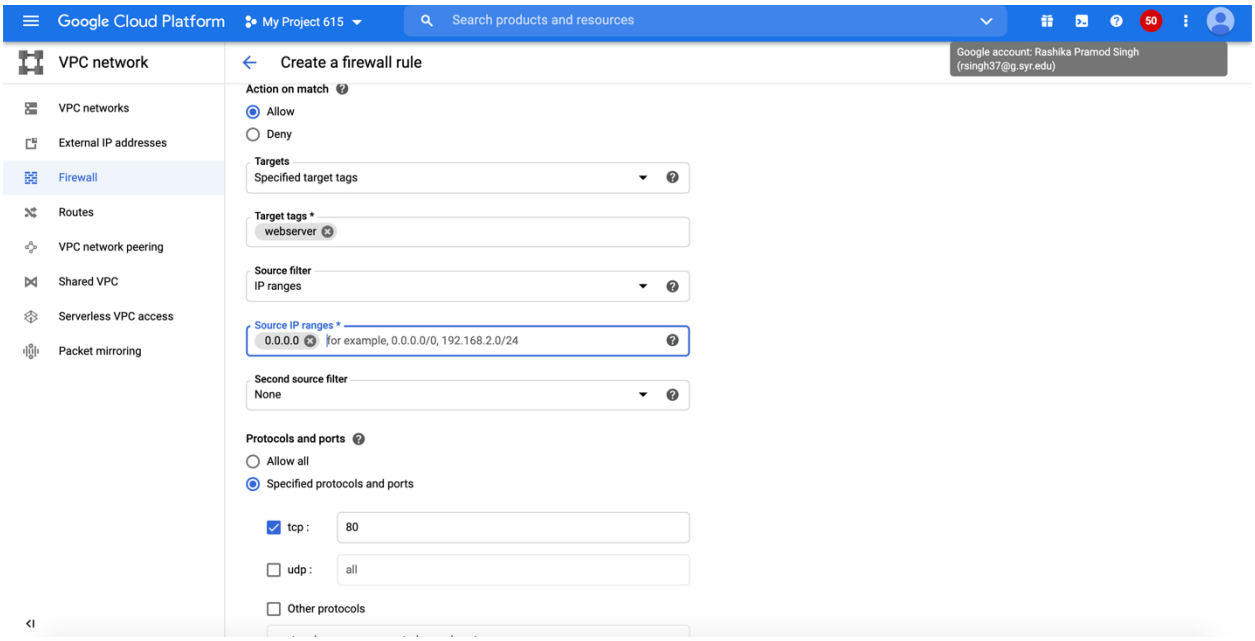
Part 2: Using firewall rules

- Creating firewall rules

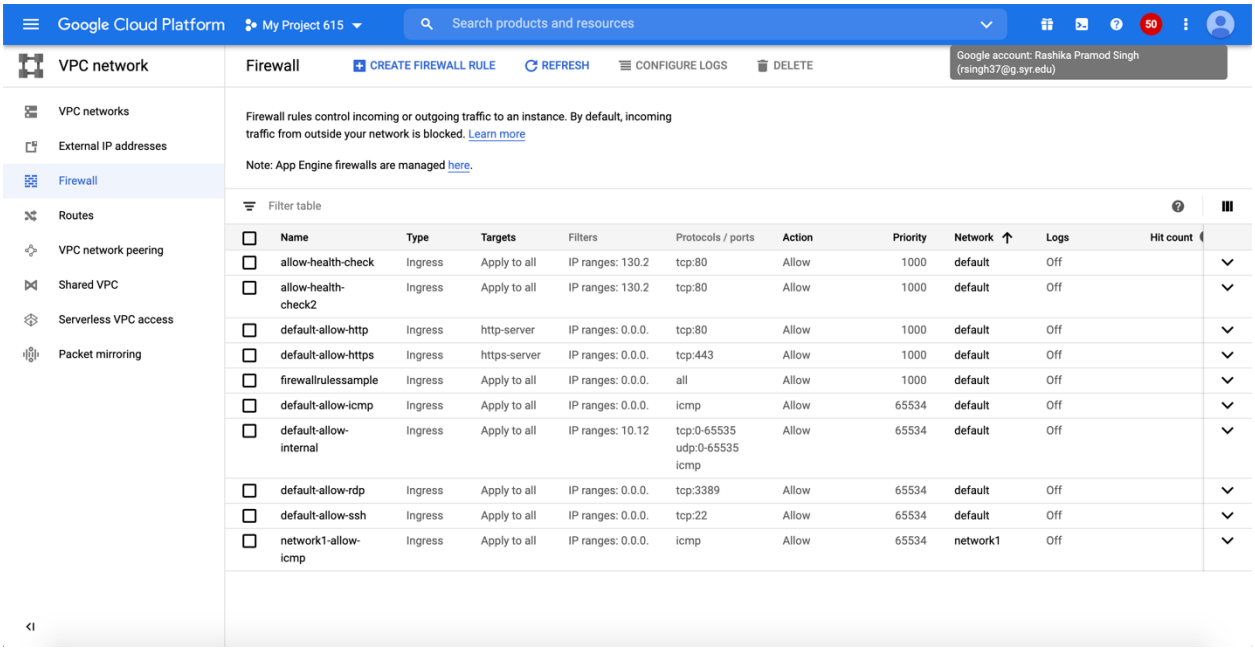
Rashika Pramod Singh
IST 615

Here I create a firewall rule with direction of traffic ingress (ingress is right to enter the property) while egress is the right to exit the property and with the IP ranges.

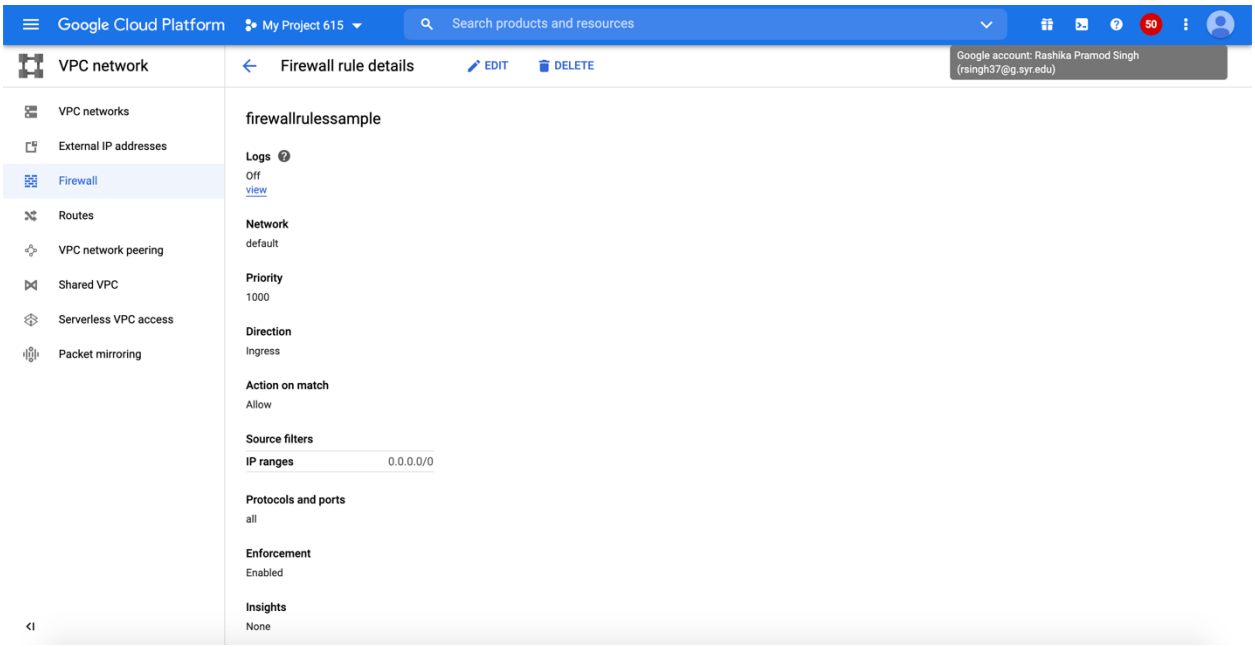




This shows that the firewallrulessample is created.

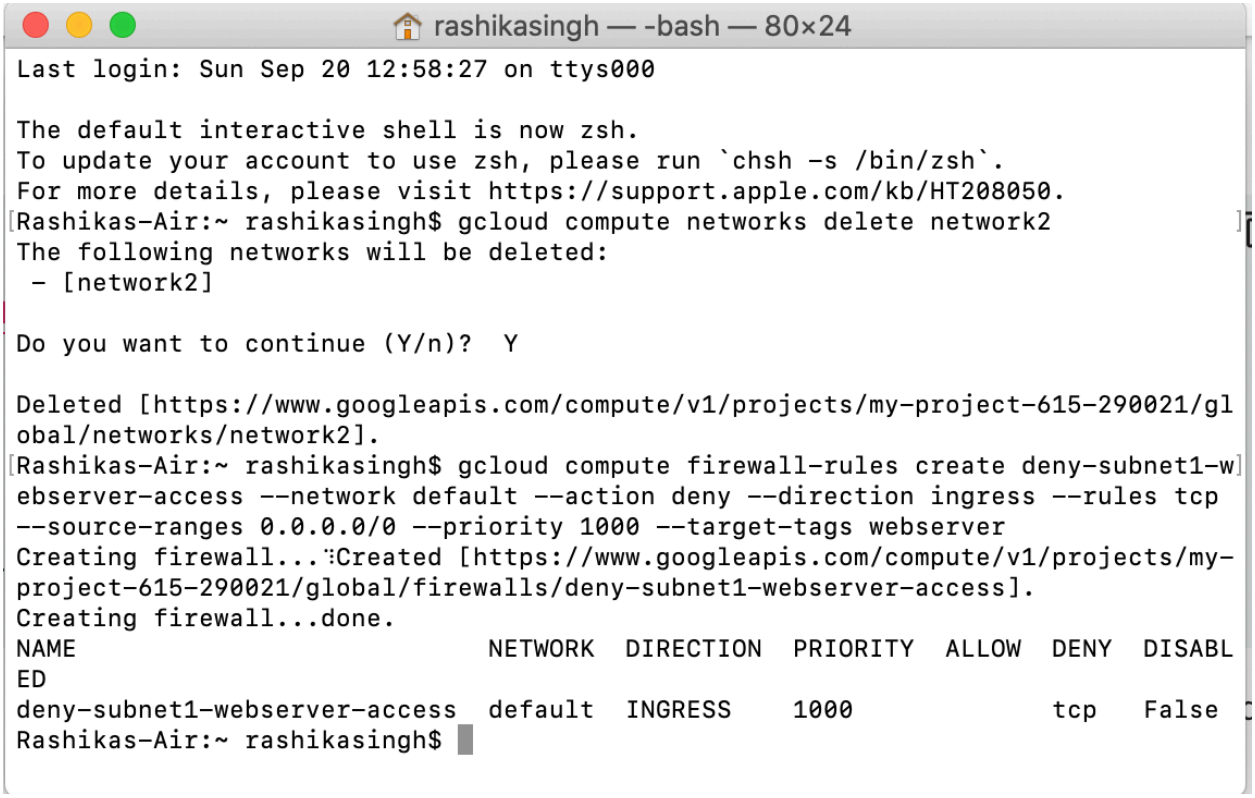


This shows the details of the firewall.



- Configuration examples:
  - Deny all ingress TCP connections except those to port 80 from subnet1

  This denies all the incoming TCP connections except those from port 80 from subnet with priority of 1000 on the default network.



- Deny all egress TCP connections except those to port 80 of vm1

This denies all the outgoing traffic with TCP with priority 1000 except that of port 80 of vml.

```
Rashikas-Air:~ rashikasingh$ gcloud compute firewall-rules create deny-all-acces
s  --network default --action deny --direction egress --rules tcp --destination-
ranges 0.0.0.0/0 --priority 1000
Creating firewall...⠹Created [https://www.googleapis.com/compute/v1/projects/my-
project-615-290021/global/firewalls/deny-all-access].
Creating firewall...done.
NAME             NETWORK  DIRECTION  PRIORITY  ALLOW  DENY  DISABLED
deny-all-access  default  EGRESS     1000             tcp   False
Rashikas-Air:~ rashikasingh$
```

- Allow egress TCP connections to port 443 of an external host

This allows all the exit traffic from TCP connections to port 443 of external host.

```
Rashikas-Air:~ rashikasingh$ gcloud compute firewall-rules create vm1-allow-egress-tcp-port443-to-192-0-2-5 --network default --action allow --direction egress --rules tcp:443 --destination-ranges 192.0.2
.5/32 --priority 70 --target-tags webserver
Creating firewall...⠹Created [https://www.googleapis.com/compute/v1/projects/my-project-615-290021/global/firewalls/vm1-allow-egress-tcp-port443-to-192-0-2-5].
Creating firewall...done.
NAME                                  NETWORK  DIRECTION  PRIORITY  ALLOW    DENY  DISABLED
vm1-allow-egress-tcp-port443-to-192-0-2-5  default  EGRESS     70        tcp:443        False
Rashikas-Air:~ rashikasingh$
```

- Allow SSH connections from vm2 to vm1

This allows all SSH connections from vm2 to vm1 in the network.

```
Rashikas-Air:~ rashikasingh$ gcloud compute firewall-rules create vm1-allow-ingress-tcp-ssh-from-vm2 --network default --action allow --direction ingress --rules tcp:22 --source-tags database --priority 8
0 --target-tags webserver
Creating firewall...⠹Created [https://www.googleapis.com/compute/v1/projects/my-project-615-290021/global/firewalls/vm1-allow-ingress-tcp-ssh-from-vm2].
Creating firewall...done.
NAME                                 NETWORK  DIRECTION  PRIORITY  ALLOW   DENY  DISABLED
vm1-allow-ingress-tcp-ssh-from-vm2  default  INGRESS    80        tcp:22        False
Rashikas-Air:~ rashikasingh$
```

Then, I shut down the instances, project and stop the billing.