

3. Cloud Shell

Created a New Cloud Project GCP-Project-1 for the lab

The screenshot shows the 'New Project' creation interface. At the top, there is a warning message: 'You have 23 projects remaining in your quota. Request an increase or delete projects. [Learn more](#)'. Below this is a 'MANAGE QUOTAS' button. The main form fields include:

- Project name ***: GCP-Project-1
- Project ID**: gcp-project-1-290213 (cannot be changed later)
- Organization ***: g.syr.edu
- Location ***: g.syr.edu

At the bottom are 'CREATE' and 'CANCEL' buttons.

The screenshot shows the Google Cloud Platform dashboard for the project 'My First Project'. The left sidebar includes sections for Project info, Resources, Trace, and Getting Started. The main area displays monitoring dashboards for Compute Engine, RPI APIs, and Error Reporting. A notifications sidebar on the right shows an activity log entry: 'Create Project: GCP-Project-1' (Just now). The dashboard also features a 'SEE ALL ACTIVITIES' button.

GCP-Project-1 Cloud Project Created

This screenshot shows the Google Cloud Platform dashboard for the project 'GCP-Project-1'. The dashboard includes sections for Project info, API APIs, Google Cloud Platform status, Billing, Monitoring, and Error Reporting. The API APIs section shows requests per second over time. The Google Cloud Platform status section indicates all services are normal. The Billing section shows estimated charges of USD \$0.00 for the period from Sep 1 to Sep 21, 2020.

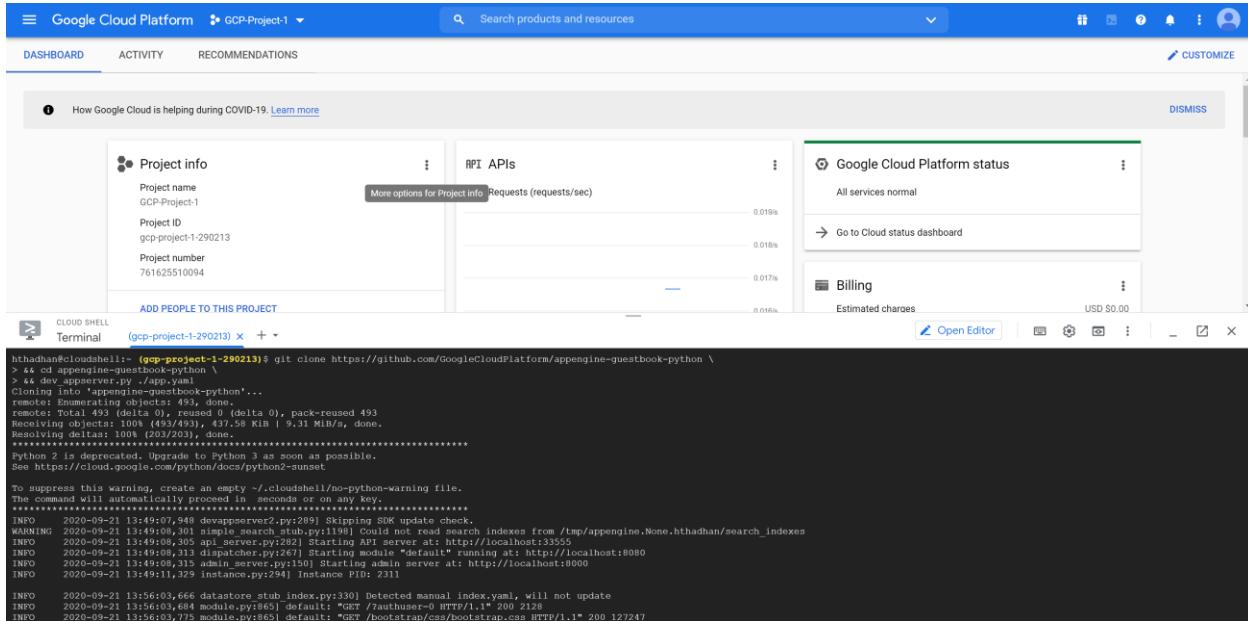
Started the gcloud shell using the Activate Cloud Shell option on the top-right

This screenshot shows the Google Cloud Platform dashboard with a terminal window open in the Cloud Shell. The terminal window displays the user's session information, including the project ID 'gcp-project-1-290213' and a list of gcloud command versions such as alpha 2020.09.11, app-engine-go 1.7.1, app-engine-java 1.9.82, app-engine-python 1.9.91, app-engine-python-extras 1.9.91, beta 2020.09.11, bigtable, bq 2.0.60, cbt 0.9.0, cloud-build-local 0.5.0, cloud-datastore-emulator 2.1.0, core 2020.09.11, dataflow 20190610, gauth 4.33, kubectl 0.27, kpt 0.33.0, kubectl 1.15.11, minikube 1.4.0, podman-emulator 0.1.0, skafold 1.14.0, and hthadhan@cloudshell:~ (gcp-project-1-290213) ~ |

Preview and Deploy an App Engine application

Cloned the github repository containing a sample app and locally running it using the App Deployment server. This local running of the app is being viewed in the web browser using the

Web Preview button on the port 8080 so that before deploying this App online on the internet we can view and make any final changes.



```
htthadhan@CloudShell: ~ (gcp-project-1-290213) + ~
htthadhan@CloudShell: ~ (gcp-project-1-290213) $ git clone https://github.com/GoogleCloudPlatform/appengine-guestbook-python \
> && cd appengine-guestbook-python \
> && dev_appserver.py ./app.yaml
Cloning into 'appengine-guestbook-python'...
remote: Enumerating objects: 493, done.
remote: Total 493 (delta 0), reused 0 (delta 0), pack-reused 493
Receiving objects: 100% (493/493), 437.58 KiB | 9.31 MiB/s, done.
Resolving deltas: 100% (203/203), done.
*****
***** Python 2 is deprecated. Upgrade to Python 3 as soon as possible.
See https://cloud.google.com/python/docs/python2-sunset

To suppress this warning, create an empty ~/.cloudshell/no-python-warning file.
The command will automatically proceed in seconds or on any keypress.
*****
INFO 2020-09-21 13:49:07.948 devappserver2.py:289] Skipping SDK update check.
WARNING 2020-09-21 13:49:08.301 simple_search_stub.py:1198] Could not read search indexes from /tmp/appengine.Nom...htthadhan/search_indexes
INFO 2020-09-21 13:49:08.301 devappserver2.py:150] Starting module "default" running at: http://localhost:8080
INFO 2020-09-21 13:49:08.313 dispatcher.py:267] Starting module "default" running at: http://localhost:8080
INFO 2020-09-21 13:49:08.315 admin_server.py:150] Starting admin server at: http://localhost:8000
INFO 2020-09-21 13:49:11.329 instance.py:294] Instance PID: 2311

INFO 2020-09-21 13:56:03.666 datastore_stub_index.py:330] Detected manual index.yaml, will not update
INFO 2020-09-21 13:56:03.684 module.py:865] default: "GET /authuser=0 HTTP/1.1" 200 2128
INFO 2020-09-21 13:56:03.775 module.py:865] default: "GET /bootstrap/css/bootstrap.css HTTP/1.1" 200 127247
```

Web Preview on the port 8080 for the app.



Attached the App Engine to the project created earlier for the lab.

The screenshot shows the Google Cloud Platform dashboard for project "GCP-Project-1". The "Project info" section displays details like Project name (GCP-Project-1), Project ID (gcp-project-1-290213), and Project number (761625510094). The "API APIs" section shows requests per second. The "Google Cloud Platform status" section indicates all services are normal. The "Billing" section shows estimated charges of USD \$0.00. A terminal window in the foreground shows the command `gcloud app deploy ./index.yaml ./app.yaml` being run, resulting in the creation of an App Engine application named "gcp-project-1-290213" in the "us-central" region.

- Deployed the App using App Deployment server to be accessible from the internet. After the app is deployed, the web browser link to access the app is shown in the target url along with the project name.

```
htthadhan@cloudshell:~/appengine-guestbook-python (gcp-project-1-290213)$ gcloud app deploy ./index.yaml ./app.yaml
Services to deploy:
descriptor:  [/home/htthadhan/appengine-guestbook-python/app.yaml]
source:      [/home/htthadhan/appengine-guestbook-python]
target project: [gcp-project-1-290213]
target service: [default]
target version: [20200921t140812]
target url:   [https://gcp-project-1-290213.uc.r.appspot.com]

Configurations to update:
descriptor:  [/home/htthadhan/appengine-guestbook-python/index.yaml]
type:        [datastore indexes]
target project: [gcp-project-1-290213]

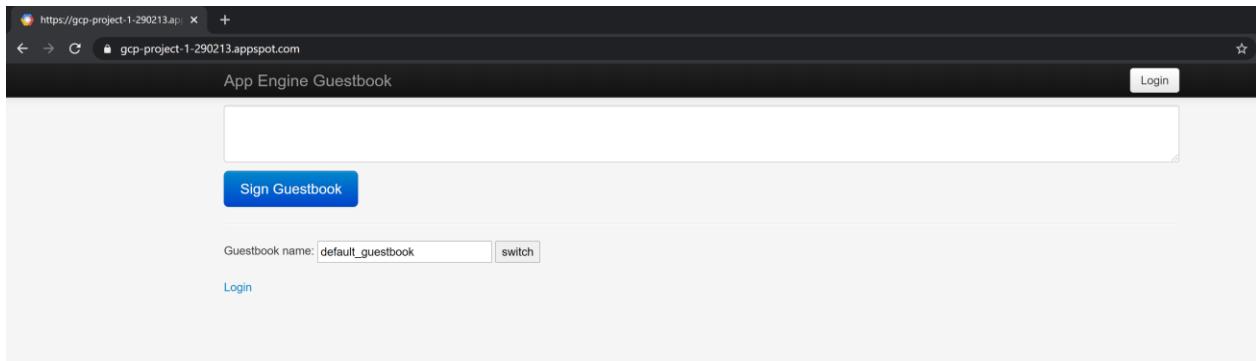
Do you want to continue (Y/n)? y
Beginning deployment of service [default]...
Uploading 21 files to Google Cloud Storage
File upload done.
Updating service [default]...done.
Setting up auto split for service [default]...done.
Deploying service [default] to [https://gcp-project-1-290213.uc.r.appspot.com]
.... 100%...done.
Updating config [index]...done.

Indexes are being rebuilt. This may take a moment.

You can stream logs from the command line by running:
  $ gcloud app logs tail --service default

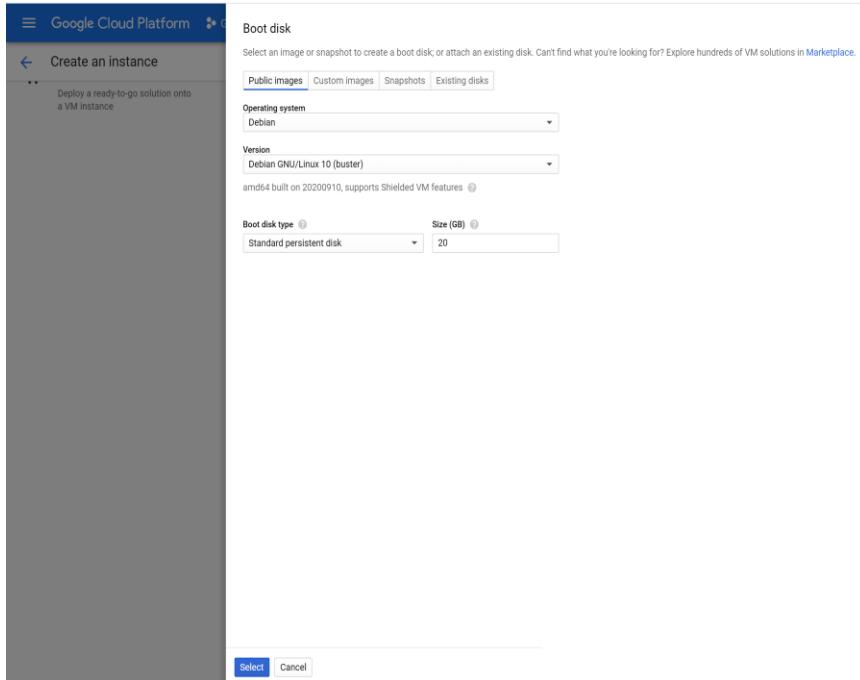
To view your application in the web browser run:
  $ gcloud app browse
htthadhan@cloudshell:~/appengine-guestbook-python (gcp-project-1-290213)$
```

- Previewing the application deployed on the GCP for this project using the Web Browser using the target url with the ProjectID included in it.



Section 4: Creating VM instances

A. Creating an instance from a public image



There are multiple public OS images available including Linux flavors like Debian along with Windows flavors SQL Server for Windows Operating systems. I selected Public Image of Debian Linux and boot disk space of 20GB is selected from the available OS images. These public images are available for everyone to use with all the preconfigured settings and it consists of all the required files to boot the OS.

The screenshot shows the 'Create an instance' wizard in the Google Cloud Platform. On the left, there are four main options: 'New VM instance' (selected), 'New VM instance from template', 'New VM instance from machine image', and 'Marketplace'. The 'New VM instance' section is detailed below:

- Name:** public-image-instance-gcp
- Labels:** (Optional) + Add label
- Region:** us-central1 (Iowa)
- Zone:** us-central1-a
- Machine configuration:**
 - Machine family:** General-purpose (selected)
 - Series:** E2
 - Machine type:** e2-medium (2 vCPU, 4 GB memory)
 - Processor:** 1 vCPU (shared core)
 - Memory:** 4 GB
 - GPUs:** -
- Boot disk:** New 20 GB standard persistent disk (selected)

On the right side of the screen, there is a sidebar with account information:

- This account is managed by g.syr.edu. Learn more
- Hitesh Chandrakumar Thadhani (Profile picture)
- hthadhan@g.syr.edu
- Privacy
- Google Accounts
- Add account
- Sign out

Additional Disk is selected for Temporary Trial purpose of 100GB with Read/Write configuration for allowing data to be written on this hard disk to be used as an additional hard disk for the VM and using Google Managed Key for the encryption to be managed by Google. The data before being written to the disk is encrypted by Google when Google Managed key option is selected and is automatically decrypted when reading the data. All this encryption and decryption of the data is taken care of by Google to maintain the security. The temporary disk of 100GB would be deleted by default when the VM instance is deleted using the Delete Role Delete Disk so that the disk is deleted to free up space automatically when the VM is deleted.

The screenshot shows the 'Create an instance' page in the Google Cloud Platform. The 'Disks' tab is selected. A new disk is being created with the following details:

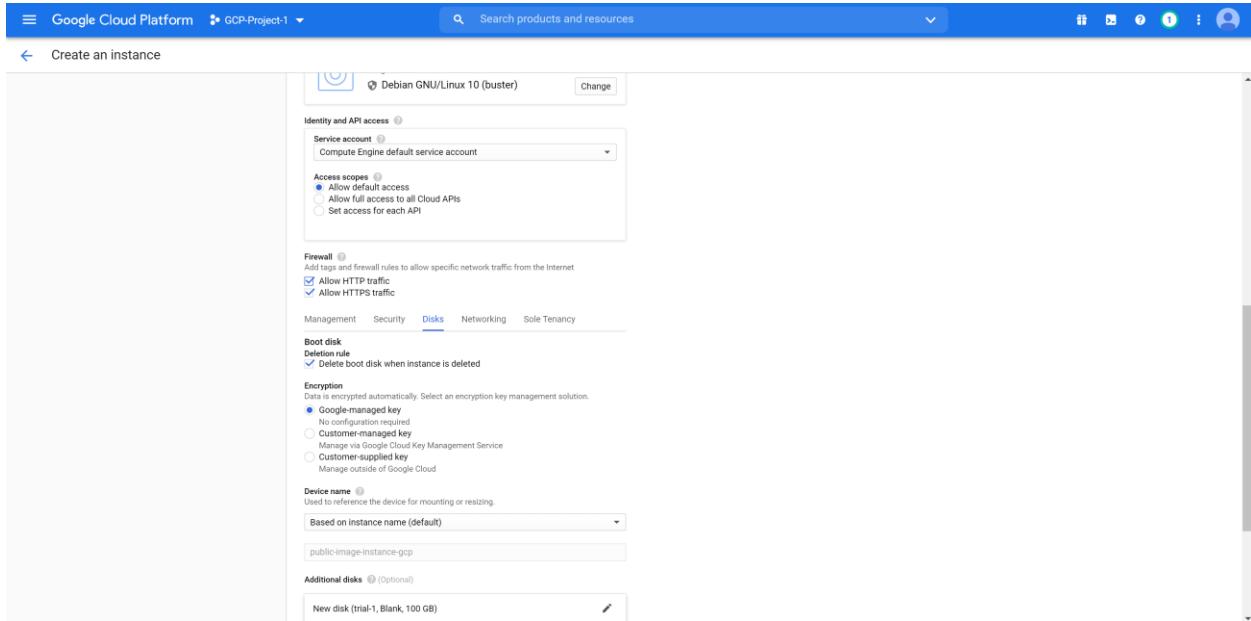
- Name:** trial-1
- Description:** Temporary Trial Disk
- Type:** Standard persistent disk
- Snapshot schedule:** No schedule

The screenshot shows the 'Create an instance' page in the Google Cloud Platform. The 'Disks' tab is selected. A new disk is being created with the following details:

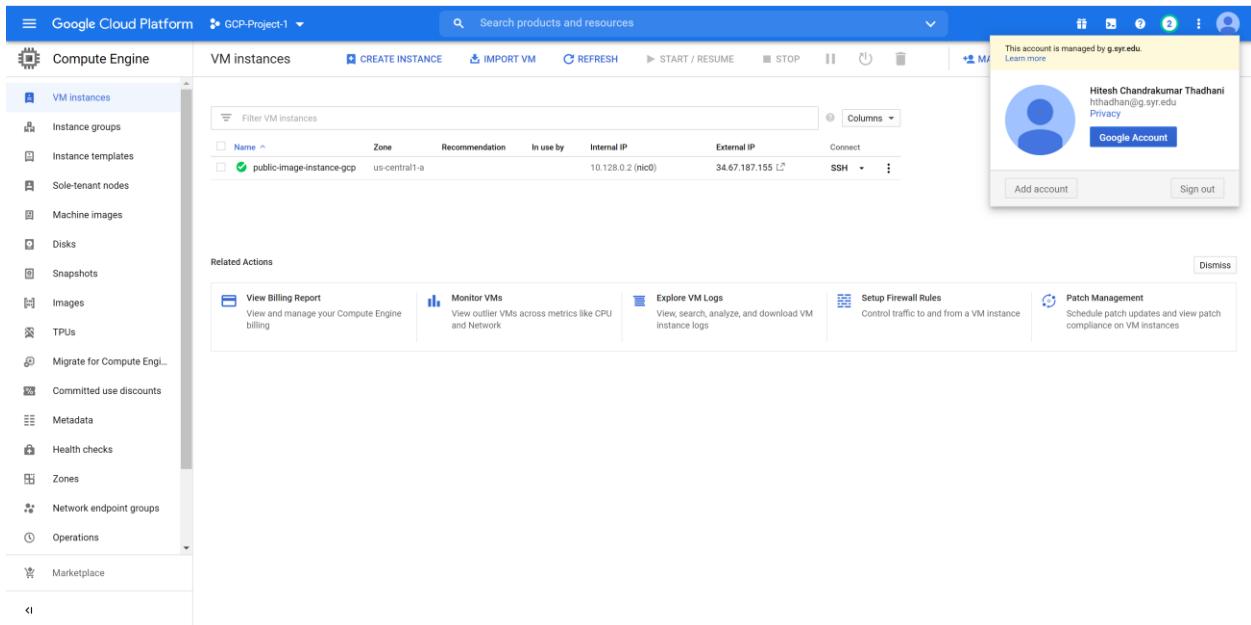
- Source type:** Blank disk
- Mode:** Read/write
- Deletion rule:** Delete disk
- Size (GB):** 100
- Estimated performance:** Sustained random IOPS limit: 75.00, Write: 150.00; Sustained throughput limit (MB/s): 12.00, Write: 12.00
- Encryption:** Google-managed key
- Device name:** trial-1

A note at the bottom states: "You're creating an unformatted disk. Format the disk after you attach it to your VM instance. [Formatting and mounting a zonal persistent disk](#)"

Allow HTTP and HTTPS traffic is selected so that the VM can communicate over the default port 80 for HTTP and 443 for HTTPS. To access the instance over the internet, HTTP and HTTPS protocols would be used. All the traffic coming to the instance would be coming to this port 80 and port 443. This creates a rule to allow the HTTP and HTTPS traffic coming to the VM over the internet.

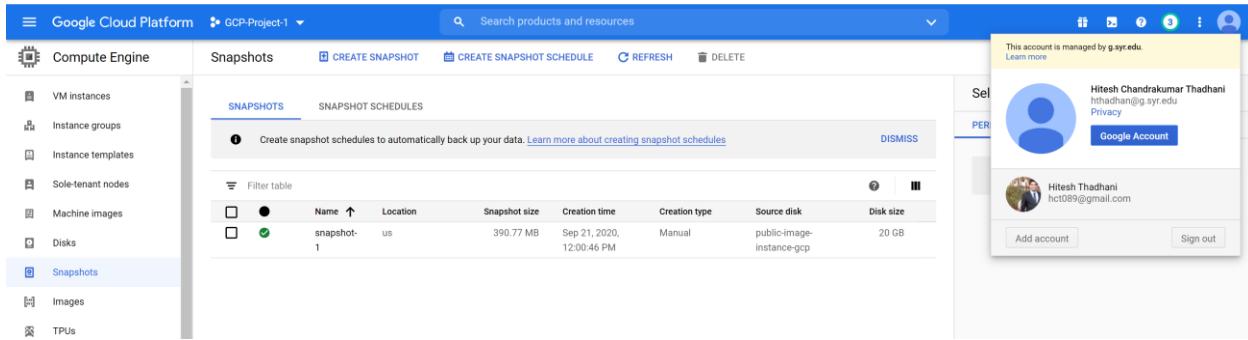


The instance created using the Public image of the OS is up and running which is seen below.



- B. Creating an instance from a snapshot
- Create a snapshot before creating an instance from it –

Created a snapshot of the public instance image to be used as a source for creating a new VM. Snapshot are of incremental nature i.e. snapshot taken at the very 1st time takes the whole point in time snapshot of the instance persistent disk and next time the snapshot is created only the modified data since the last snapshot would be captured. This incremental nature of snapshot makes them faster and easy to transport to restore the data as only the modified data is captured instead of taking the whole image of the instance every time thereby reducing the size of the snapshot.



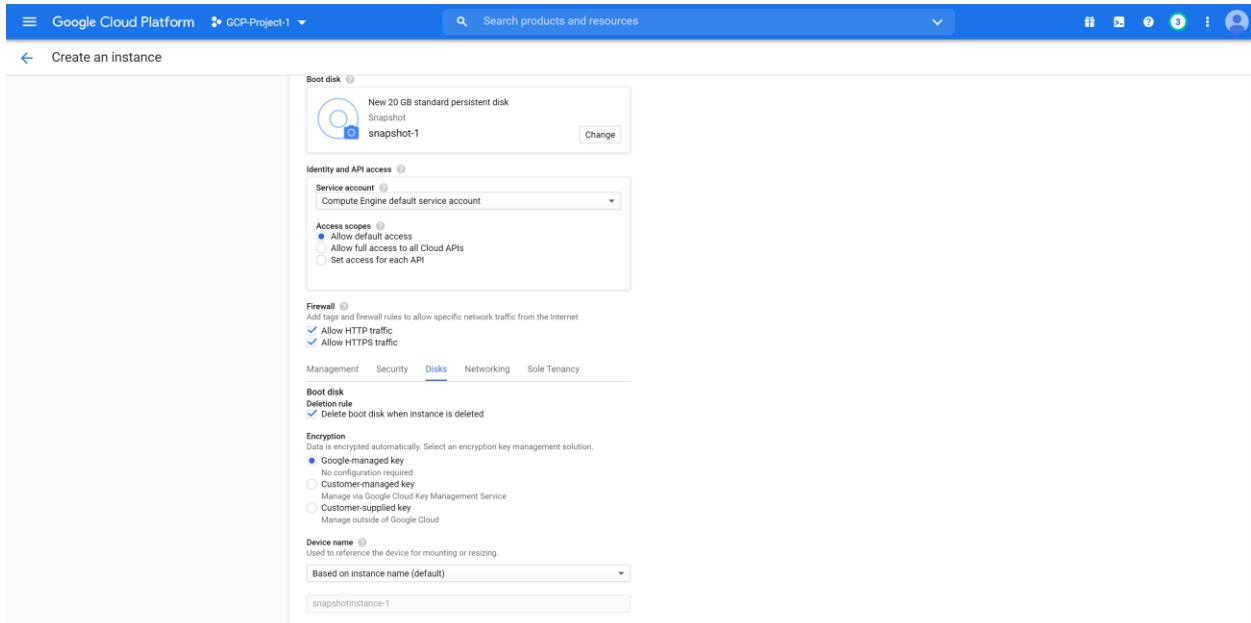
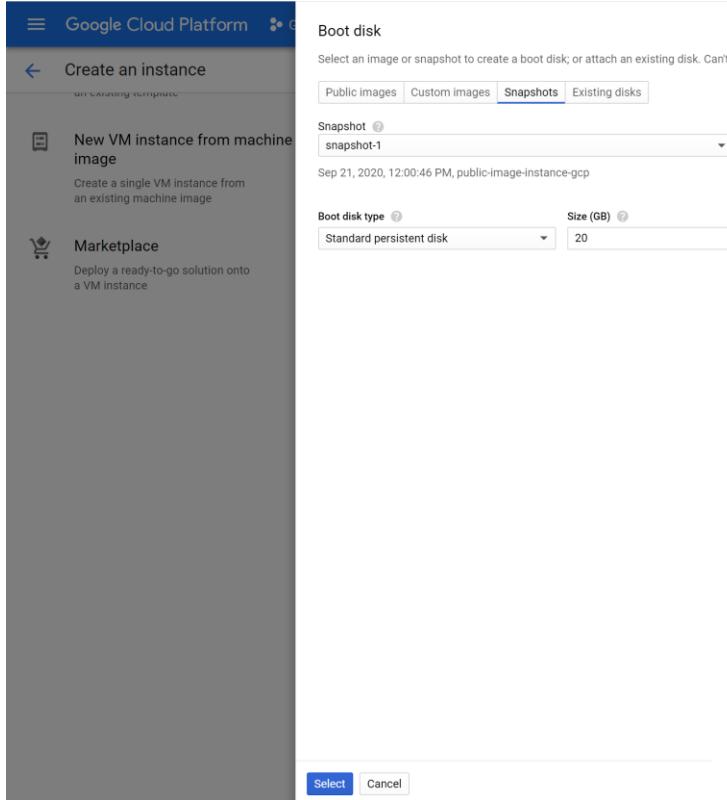
The screenshot shows the Google Cloud Platform interface for the Compute Engine Snapshots page. The left sidebar lists various Compute Engine resources: VM instances, Instance groups, Instance templates, Sole-tenant nodes, Machine images, Disks, and Snapshots (which is selected). The main content area displays a table titled 'SNAPSHOTS' with one entry:

	Name	Location	Snapshot size	Creation time	Creation type	Source disk	Disk size
<input type="checkbox"/>	snapshot-1	us	390.77 MB	Sep 21, 2020, 12:00:46 PM	Manual	public-image-instance-gcp	20 GB

A modal window on the right side of the screen shows account details for 'Hitesh Chandrakumar Thadhani' (hthadhan@g.syr.edu) and 'Hitesh Thadhani' (hct089@gmail.com), along with options to 'Add account' and 'Sign out'.

ii. Creating a new Instance from the Snapshot taken earlier

A new instance is created by using the snapshot as the boot disk taken earlier of the public image instance.



Allow HHTP and HTTPS traffic makes the VM use internet for the access allowing the traffic to be directed to the VM over the HTTPS and HTTP protocol. Delete the disk when instance is deleted allows to release the disk space whenever the instance is deleted.

This account is managed by g.syr.edu.
Learn more

Hitesh Chandrakumar Thadhani
hthadhan@g.syr.edu
Privacy

Google Account

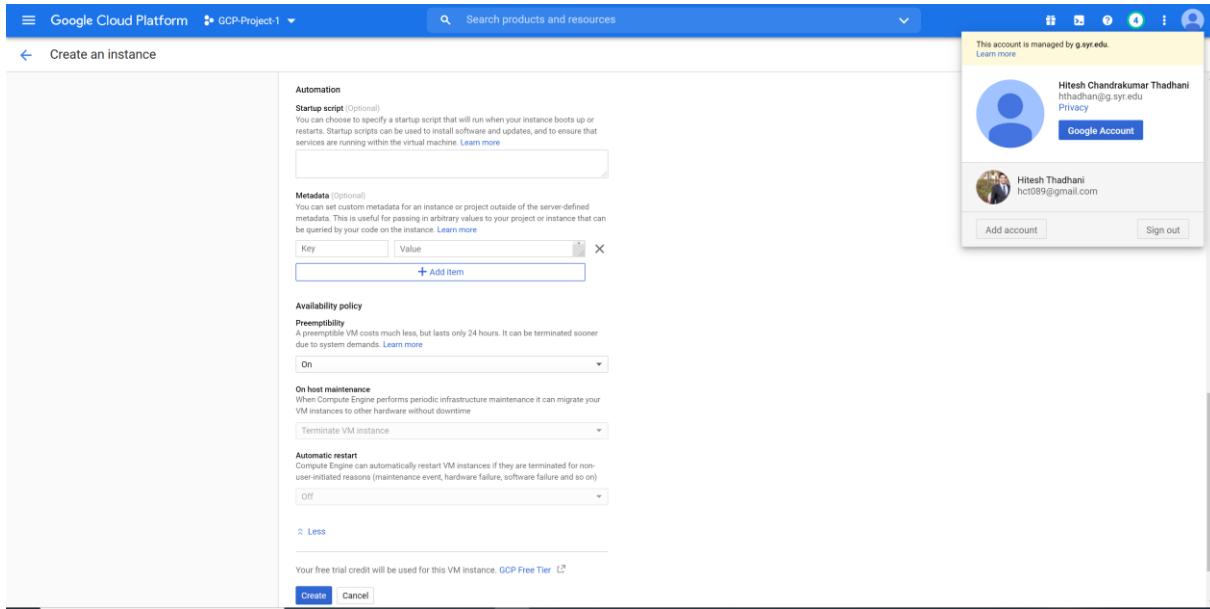
Hitesh Thadhani
hct089@gmail.com

Add account Sign out

C. Complete the following sub-modules in ***Creating and Starting a Preemptible VM Instance***

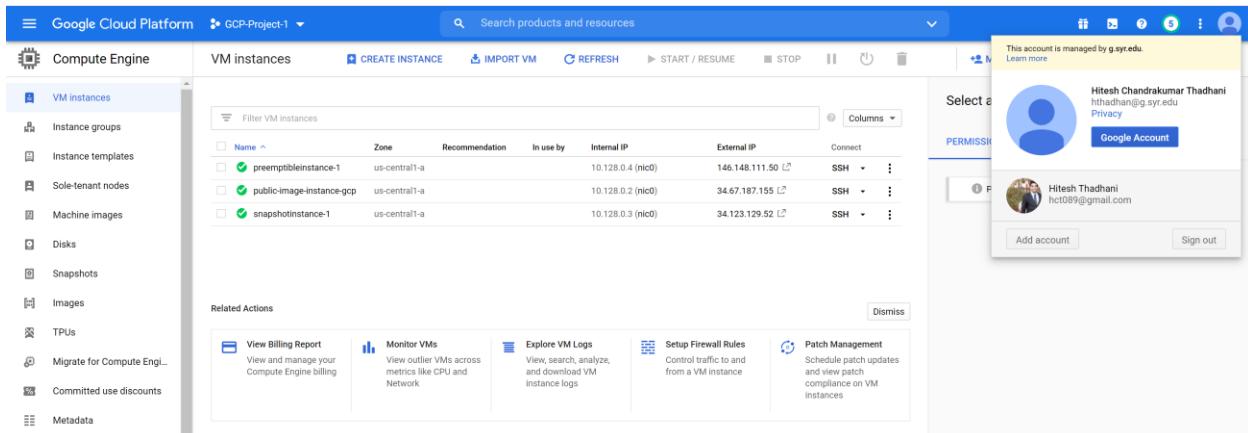
i. Creating a preemptible instance

Preemptible instance is a temporary instance which is available only for 24 hours to use at a very low price as compared to normal instances. These instances are not covered under any SLA. The compute resources can preempt or stop at any time if the load to the normal instances increases and it needs more compute power. These instances are useful for some batch processing tasks which are not so critical that if the instance is pre-empted there would be a business impact.



When the Preemptibility setting is turned on to create the preemptible instance, automatic restart of the instance is turned off and sets the On Host maintenance to Terminate VM instance.

Preemptible instance is successfully created and up and running as shown below.



ii. Checking if an instance is preemptible

The instance is preemptible can be checked using 2 ways Console and Gcloud command line shell.

The screenshot shows the 'VM instance details' page for a preemptible instance named 'preemptibleinstance-1'. The 'Preemptibility' setting is listed as 'On'. Other settings include 'On host maintenance' set to 'Terminate VM Instance' and 'Automatic restart' set to 'Off'. The 'Cloud API access scopes' section shows 'Allow default access' selected.

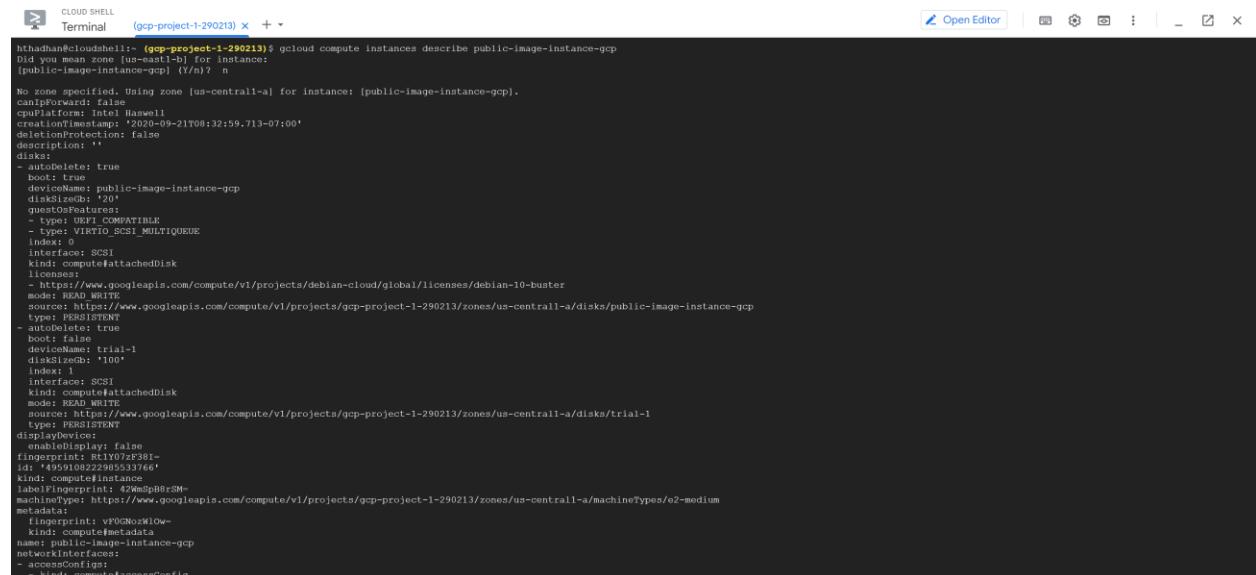
To check for the instance type if it is a preemptible instance or not, clicked on the instance and in the VM details, Availability policies shows that **Preemptibility is On** meaning that the instance is preemptible using the Console.

D. Check status of any instance you created earlier (Check any instance that you created earlier)

\$ gcloud compute instances list – To list all the instances within a project. Also, for the preemptible instance created above, it shows PREEMPTIBLE to be true to show that this instance is preemptible.

```
Welcome to Cloud Shell! Type "help" to get started.
Your Cloud Platform project in this session is set to gcp-project-1-290213.
Use "gcloud config set project [PROJECT_ID]" to change to a different project.
hthadhan@cloudshell:~ (gcp-project-1-290213)$ gcloud compute instances list
NAME          ZONE      MACHINE_TYPE  PREEMPTIBLE INTERNAL_IP  EXTERNAL_IP    STATUS
preemptibleinstance-1  us-central1-a  e2-medium    true        10.128.0.4   146.148.111.50  RUNNING
public-image-instance-gcp  us-central1-a  e2-medium    true        10.128.0.2   34.67.187.155  RUNNING
snapshotinstance-1       us-central1-a  e2-medium    true        10.128.0.3   34.123.129.52   RUNNING
```

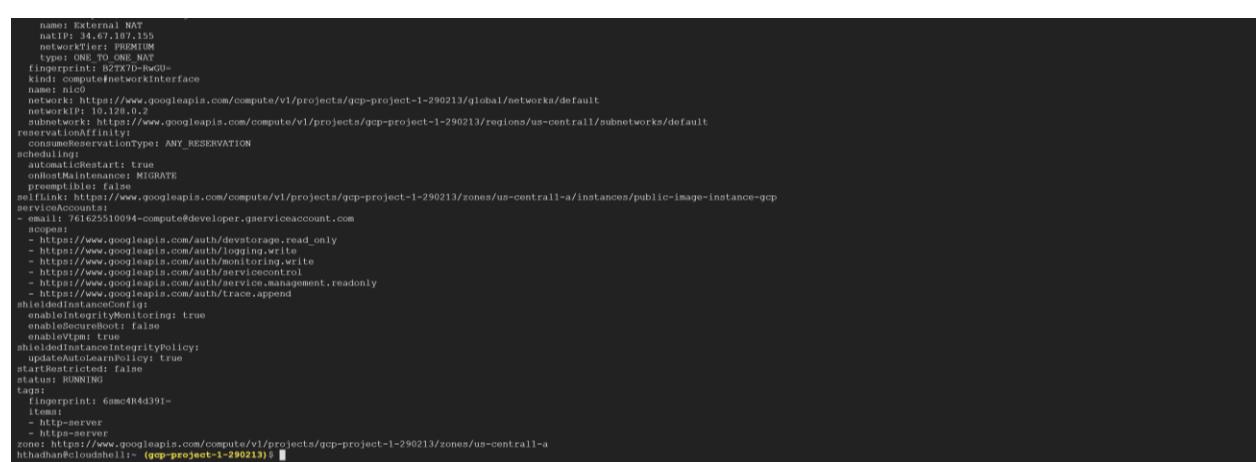
\$ gcloud compute instances describe public-image-instance-gcp – This command describes a specific instance in a very detail giving all the information about the particular instance such as disksize, mode like Read/Write, network interface details like the External Public IP, Service Account details etc along with displaying the instance status if it is running, terminated, stopped etc.



```

hthadhan@cloudshell:~ (gcp-project-1-290213) ~ + 
Did you mean zone [us-central1-a] for instance: [public-image-instance-gcp]?
[public-image-instance-gcp] (y/n)? n
No zone specified. Using zone [us-central1-a] for instance: [public-image-instance-gcp].
canIpForward: false
cpuPlatform: Intel Haswell
creationTimestamp: "2020-05-21T08:32:59.713-07:00"
deletionProtection: false
description: ""
disks:
  autoDelete: true
  boot: true
  deviceName: public-image-instance-gcp
  diskSizeGb: 120
  diskType:
    - type: UNDEFINED
    - type: VIRTIO SCSI MULTIQUEUE
    - type: VIRTIO SCSI
      index: 0
    - interface: SCSI
  kind: compute#attachedDisk
  licenses:
    - https://www.googleapis.com/compute/v1/projects/debian-cloud/global/licenses/debian-10-buster
  mode: READ_WRITE
  name: public-image-instance-gcp
  source: https://www.googleapis.com/compute/v1/projects/gcp-project-1-290213/zones/us-central1-a/disks/public-image-instance-gcp
  type: PERSISTENT
  - autoboot: true
  boot: false
  diskType: trial-1
  diskSizeGb: '100'
  index: 1
  interface: SCSI
  kind: compute#attachedDisk
  mode: READ_WRITE
  source: https://www.googleapis.com/compute/v1/projects/gcp-project-1-290213/zones/us-central1-a/disks/trial-1
  type: PERSISTENT
  displayDevice: false
  enableBootPriority: false
  fingerprint: RTIY0zF38I-
  id: '4959108229855373661'
  kind: compute#disk
  labelFingerprint: 42XeSp8r+SM-
  machineType: https://www.googleapis.com/compute/v1/projects/gcp-project-1-290213/zones/us-central1-a/machineTypes/e2-medium
  metadata:
    items:
      - key: vpcNetwork
        value: compute#metadata
  name: public-image-instance-gcp
  networkInterfaces:
    - accessConfigs:
        - kind: compute#accessConfig
          name: External NAT
          natIP: 34.67.187.155
          networkTier: PREMIUM
        type: ONE_TO_ONE_NAT
      fingerprint: BZxJ0jDpp
      kind: compute#networkInterface
      name: nic0
      network: https://www.googleapis.com/compute/v1/projects/gcp-project-1-290213/global/networks/default
      networkTier: PREMIUM
      subnetwork: https://www.googleapis.com/compute/v1/projects/gcp-project-1-290213/regions/us-central1/subnetworks/default
      reservationPriority: 0
      consumeReservationType: ANY_RESERVATION
      scheduledMaintenance:
        automaticRestart: true
        onionMaintenance: MIGRATE
      preemptible: false
      selfLink: https://www.googleapis.com/compute/v1/projects/gcp-project-1-290213/zones/us-central1-a/instances/public-image-instance-gcp
      serviceAccount: hthadhan@cloudshell.gserviceaccount.com
      email: 761625510094-compute-developer.gserviceaccount.com
      scopes:
        - https://www.googleapis.com/auth/devstorage.read_only
        - https://www.googleapis.com/auth/logging.write
        - https://www.googleapis.com/auth/monitoring.write
        - https://www.googleapis.com/auth/servicecontrol
        - https://www.googleapis.com/auth/service.management.readonly
        - https://www.googleapis.com/auth/trace.append
      shieldedInstanceConfig:
        enableIntegrityMonitoring: true
        enableSecureBoot: false
        enableVtpm: true
      shieldedInstanceIntegrityPolicy:
        updateAutoLearnPolicy: true
      startRestricted: false
      status: RUNNING
      tags:
        items:
          - fingerprint: 6mcRH4d39I-
            items:
              - https-server
              - http-server
            zones: https://www.googleapis.com/compute/v1/projects/gcp-project-1-290213/zones/us-central1-a
hthadhan@cloudshell:~ (gcp-project-1-290213) ~

```



```

name: External NAT
natIP: 34.67.187.155
networkTier: PREMIUM
type: ONE_TO_ONE_NAT
fingerprint: BZxJ0jDpp
kind: compute#networkInterface
name: nic0
network: https://www.googleapis.com/compute/v1/projects/gcp-project-1-290213/global/networks/default
networkTier: PREMIUM
subnetwork: https://www.googleapis.com/compute/v1/projects/gcp-project-1-290213/regions/us-central1/subnetworks/default
reservationPriority: 0
consumeReservationType: ANY_RESERVATION
scheduledMaintenance:
  automaticRestart: true
  onionMaintenance: MIGRATE
preemptible: false
selfLink: https://www.googleapis.com/compute/v1/projects/gcp-project-1-290213/zones/us-central1-a/instances/public-image-instance-gcp
serviceAccount: hthadhan@cloudshell.gserviceaccount.com
email: 761625510094-compute-developer.gserviceaccount.com
scopes:
  - https://www.googleapis.com/auth/devstorage.read_only
  - https://www.googleapis.com/auth/logging.write
  - https://www.googleapis.com/auth/monitoring.write
  - https://www.googleapis.com/auth/servicecontrol
  - https://www.googleapis.com/auth/service.management.readonly
  - https://www.googleapis.com/auth/trace.append
shieldedInstanceConfig:
  enableIntegrityMonitoring: true
  enableSecureBoot: false
  enableVtpm: true
shieldedInstanceIntegrityPolicy:
  updateAutoLearnPolicy: true
startRestricted: false
status: RUNNING
tags:
  items:
    - fingerprint: 6mcRH4d39I-
      items:
        - https-server
        - http-server
      zones: https://www.googleapis.com/compute/v1/projects/gcp-project-1-290213/zones/us-central1-a
hthadhan@cloudshell:~ (gcp-project-1-290213) ~

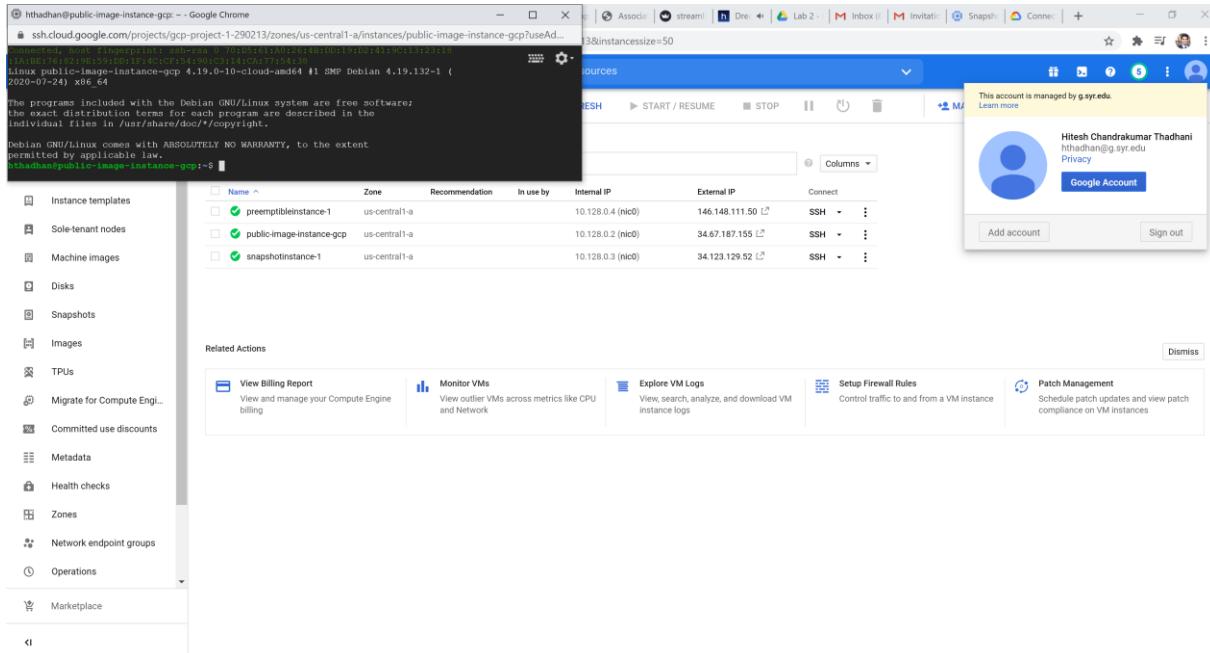
```

E. Complete the following sub-modules in *Connecting to instances*:

1. Connecting to Linux instances

- i. The public image VM instance is accessed through the use of ssh using browser

By clicking on ssh option next to the instance, a new SSH connection is created on the port 22 which is by default the port on which ssh runs. This creates a secure connection to the instance. When we connect to the instance using the ssh in a new browser window, it automatically transfers the required keys to make the secured connection to the instance.



ii. The public image VM instance is being accessed by using the gcloud command-line tool

When connecting to the instance using the ssh using the Gcloud command line, public/private key pairs are generated, the project metadata is updated and these key pairs are used to authenticate the connection request to the instance.

```
CLOUD SHELL (gcp-project-1-290213) + ▾ Open Editor

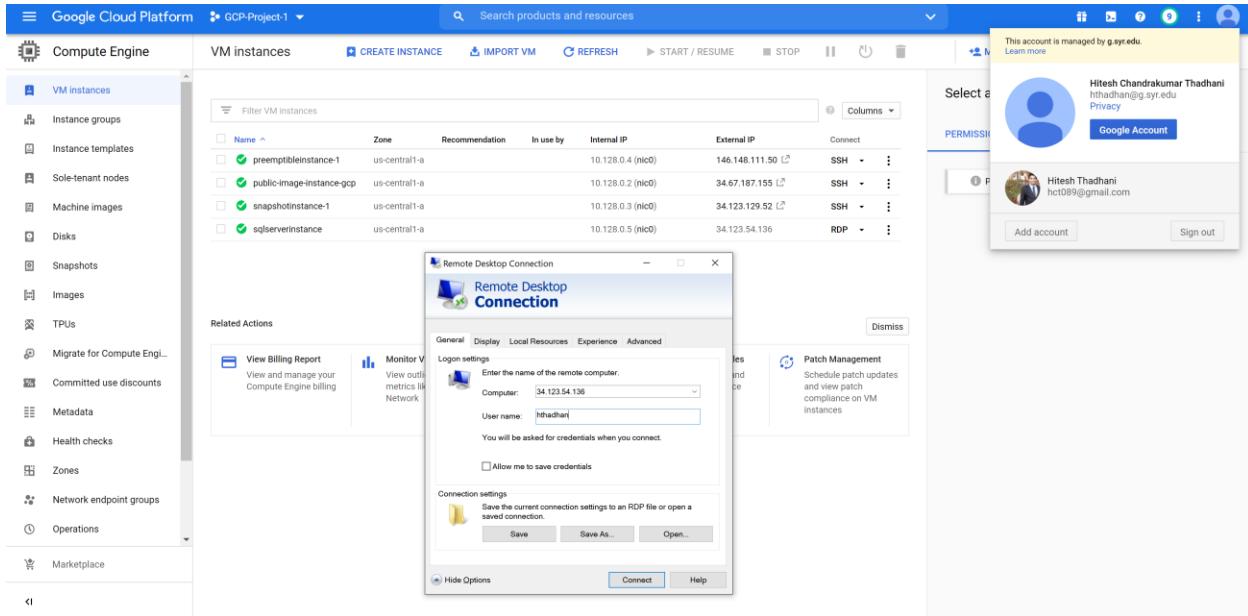
status: RUNNING
Terminal
fingerprint: 6smc4R4d39I-
items:
- http-server
- https-server
zone https://www.googleapis.com/compute/v1/projects/gcp-project-1-290213/zones/us-central1-a
hthadhan@hthadhan-OptiPlex-5090: ~ (gcp-project-1-290213)$ gcloud compute ssh --project "gcp-project-1-290213" --zone "us-central1-a" "public-image-instance-gcp"
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.
This tool needs to create the directory [/home/hthadhan/.ssh] before being able to generate SSH keys.

Do you want to continue (Y/n)? y
Generating public/private rsa key pair.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/hthadhan/.ssh/google_compute_engine.
Your public key has been saved in /home/hthadhan/.ssh/google_compute_engine.pub.
The key fingerprint is:
SHA256:nAFkC4d901tA7yaplogbQccBzRG189xP+b9qclips hthadhan@cs-462143076026-default-default-hw2rx
The key's randomart image is:
+---[20x20v1]---+
| ..++++.++o |
| .o...o+oo..o |
| .o...o+oo..o |
| .o...+.-.+
| .o...+ S ..o |
| .o...+ . .
| .o...+ . .
| .o...+ o+o |
| . . . E..o+o |
+---[SHA256]---+
Updating project metadata... Updated [https://www.googleapis.com/compute/v1/projects/gcp-project-1-290213].
Updating project ssh metadata...done.
Waiting for SSH key to propagate.
Warning: Permanently added 'compute.4959108222985533767' (ECDSA) to the list of known hosts.
Linux public-image-instance-gcp 4.19.0-10-cloud-amd64 #1 SMP Debian 4.19.132-1 (2020-07-24) x86_64

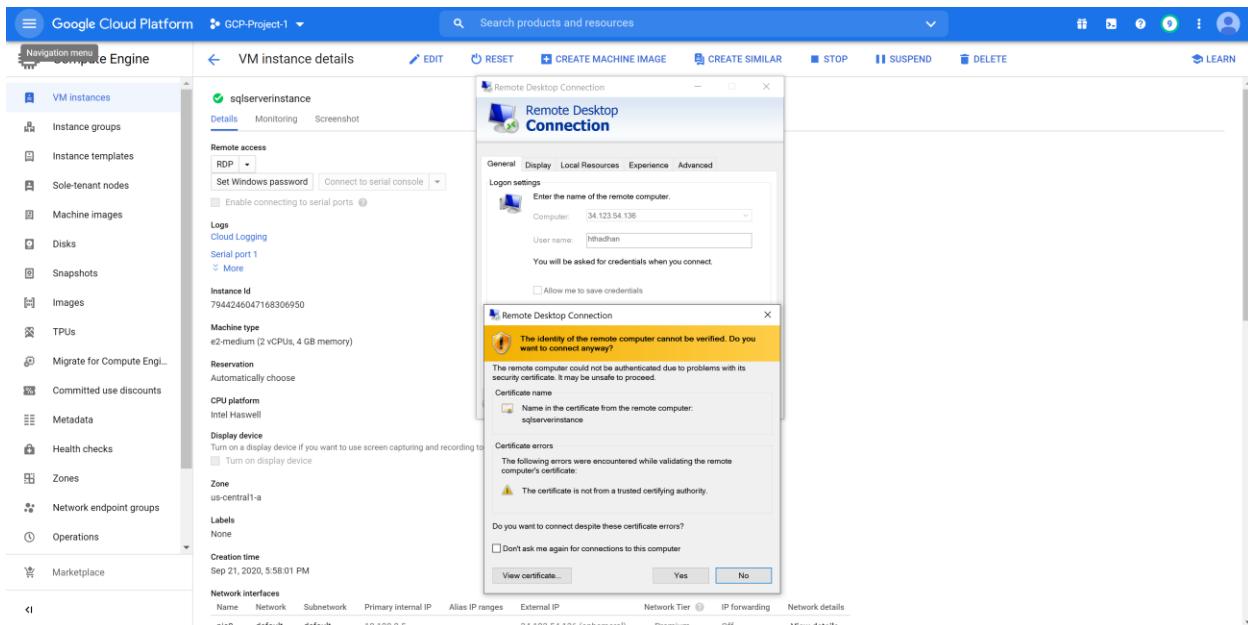
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Sep 21 16:55:41 2020 from 35.235.246.0
hthadhan@public-image-instance-gcp:~$
```

2. Connecting to Windows Instances



For connecting to the Windows instance, SQL server VM instance was created named sqlserverinstance. To connect to the windows instance with a public IP address, RDP (Remote Desktop Protocol) can be used. RDP will be used to login to the instance using the TCP traffic enabled on the port 1433. hthadhan is the username used to connect to the windows instance. Any SQL server using the Windows Operating System can be connected using RDP.



The screenshot shows the Google Cloud Platform Compute Engine interface. A VM instance named 'sqlserverinstance' is selected. The 'Remote access' section is open, showing the 'RDP' tab selected. An 'RDP Connection' window is displayed, showing the progress of connecting to the instance at IP 34.123.54.136. Below it, a 'Remote Desktop Connection' dialog box shows the connection settings, including the IP and port. The 'Network interfaces' table at the bottom lists the instance's network configuration.

Successful connection to the SQL server Windows instance is seen below using the RDP.

The screenshot shows the Microsoft Server Manager Dashboard. The main area displays the 'WELCOME TO SERVER MANAGER' message and the 'Configure this local server' wizard, step 1. It lists five steps: Add roles and features, Add other servers to manage, Create a server group, and Connect this server to cloud services. On the left, a navigation pane shows 'Dashboard', 'Local Server', 'All Servers', and 'File and Storage Services'. The 'File and Storage Services' section is expanded, showing 'File and Storage Services' with 1 role, 'Local Server' with 1 role, and 'All Servers' with 1 role. Each role has a 'Manageability' link.

3. Special Administrative Console - Connecting to an instance through the command line
(Connect to any instance that you created earlier)

Connecting to the Windows Instance using the Special Administrative Console enables interactive interface to the Windows Server using the SAC> command prompt for managing Windows. This enables the connectivity to the Windows instance through a serial interactive console.

cmd - SAC command creates a new channel to be able to login to the Windows using the username and password.

Ch -sn cmd0001 – Switch the channel to the newly created channel to login to the Windows machine using this channel with a valid username and password.

The screenshot shows a terminal window titled "sh-serialport.googleapis.com ~ PuTTY". Inside, the SAC command is run, creating a new channel named "Cmd0001". The user then switches to this channel using "ch -sn cmd0001". Finally, they run "gcloud compute connect-to-serial-port sqlserverinstance --port=2" to establish a connection to the SQL Server instance.

```
Computer is booting, SAC started and initialized.
Use the "ch -?" command for information about using channels.
Use the "?" command for general help.

SAC>
EVENT: The CMD command is now available.
SAC>cmd
The Command Prompt session was successfully launched.
SAC>
EVENT: A new channel has been created. Use "ch -?" for channel help.
Channel: Cmd0001
SAC>ch -sn cmd0001
new channel. SAC returns the channel name, for example... Cmd0001

Google Cloud Shell - gcloud compute connect-to-serial-port sqlserverinstance --port=2
Welcome to the Google Cloud SDK! Run "gcloud -h" to get the list of available commands.
...
C:\Users\hites\AppData\Local\Google\Cloud SDK>gcloud compute instances add-metadata sqlserverinstance --zone us-central1-a --metadata=serial-port-enable=1
Updated [https://www.googleapis.com/compute/v1/projects/gcp-project-1-290213/zones/us-central1-a/instances/sqlserverinstance].
C:\Users\hites\AppData\Local\Google\Cloud SDK>gcloud compute connect-to-serial-port sqlserverinstance --port=2
C:\Users\hites\AppData\Local\Google\Cloud SDK>gcloud compute instances add-metadata sqlserverinstance --zone us-central1-a --metadata=serial-port-enable=1
Updated [https://www.googleapis.com/compute/v1/projects/gcp-project-1-290213/zones/us-central1-a/instances/sqlserverinstance].
C:\Users\hites\AppData\Local\Google\Cloud SDK>gcloud compute connect-to-serial-port sqlserverinstance --port=2
```

```
ssh-serialport.googleapis.com - PuTTY
SAC>cmd
The Command Prompt session was successfully launched.
SAC>
EVENT: A new channel has been created. Use "ch -?" for channel help.
Channel: Cmd0004
SAC>ch -sn cmd0004
<?xml version="1.0"?>
<channel-switch>
<name>Cmd0004</name>
<description>Command Prompt</description>
<type>VT-UTF8</type>
<guid>c3cf5f5c-fd06-11ea-80c0-823db9c8123e</guid>
<application-type>63d02271-8aa4-11d5-bccf-00b0d014a2d0</application-type>
</channel-switch>

Name: Cmd0004
Description: Command
Type: VT-UTF8
Channel GUID: c3cf5f5c-fd06-11ea-80c0-823db9c8123e
Application Type GUID: 63d02271-8aa4-11d5-bccf-00b0d014a2d0

Press <esc><tab> for next channel.
Press <esc><tab>0 to return to the SAC channel.
Use any other key to view this channel.
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . : c.gcp-project-1-290213.internal
Link-local IPv6 Address . . . . . : fe80::547f:7e4e:6292:4d7c%12
IPv4 Address . . . . . : 10.128.0.31
Subnet Mask . . . . . : 255.255.240.0
Default Gateway . . . . . : 10.128.0.1

Tunnel adapter isatap.c.gcp-project-1-290213.internal:

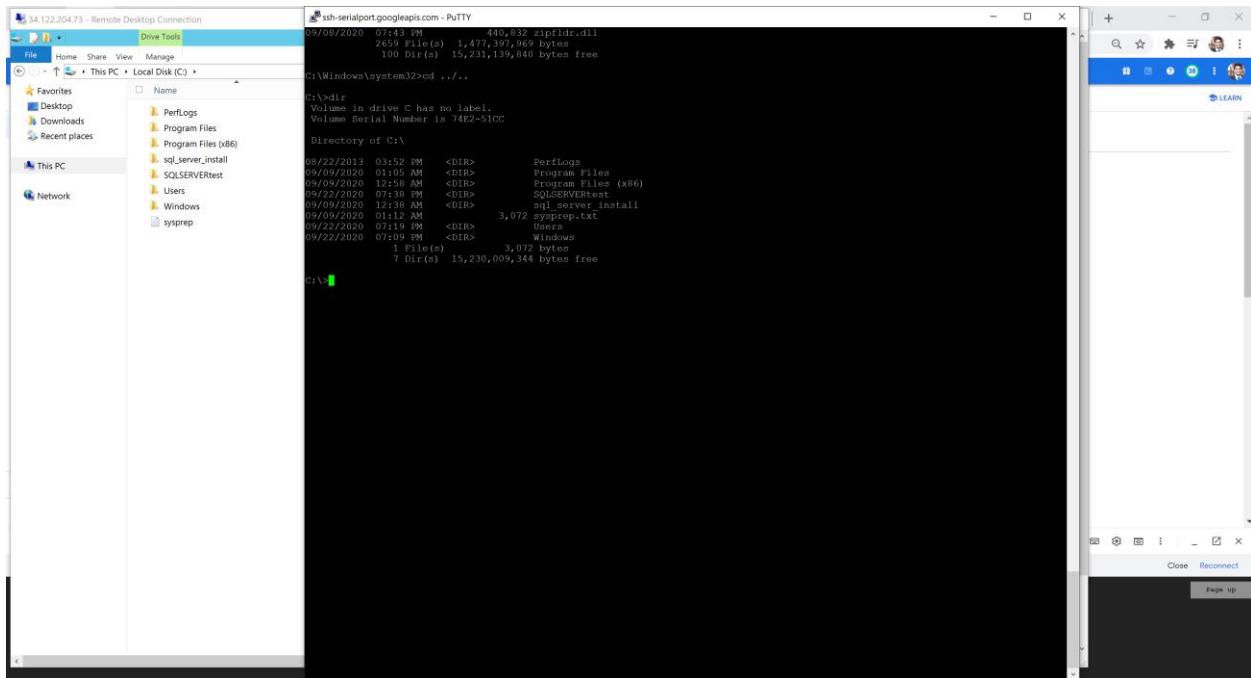
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . : c.gcp-project-1-290213.internal
```

The screenshot shows the Google Cloud Platform Compute Engine interface. On the left, a sidebar lists various Compute Engine resources: VM instances, Instance groups, Instance templates, Sole-tenant nodes, Machine images, Disks, Snapshots, Images, TPUs, Migrate for Compute En..., Committed use discounts, Metadata, Health checks, Zones, Network endpoint groups, Operations, Marketplace, and CLOUD SHELL.

The main pane displays the 'VM instance details' for a VM named 'sqlserverinstance'. The instance is currently running. It is located in the 'us-central1-a' zone. The network interface information includes:

Name	Network	Subnetwork	Primary Internal IP	Alias IP ranges	External IP	Network Tier	IP Forwarding	Network details
nic0	default	default	10.128.0.31	-	34.122.204.73 (ephemeral)	Premium	Off	View details

At the bottom of the screen, there is a terminal window titled 'CLOUD SHELL' with the command 'cloudshell' entered.



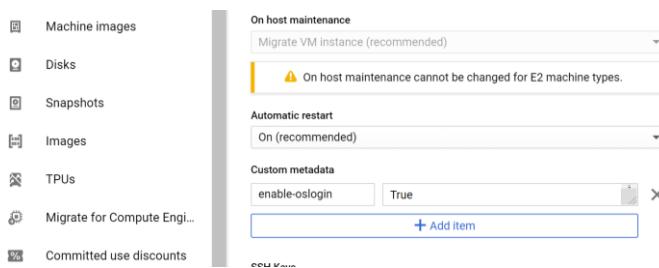
The SAC command prompt shows the directory structure of the windows OS instance using the interactive console.

F. Complete the following sub-modules in ***Connecting to instances using advanced methods:***

Connecting to the instance requires authentication for the secure connection using ssh. This authentication would come by using public and private key pair used to make a secure connection.

1. Providing public SSH keys to instances

To connect securely to the instance from outside, we need to get authenticated which is done by using public/private key pairs. Public and private keys are generated and public key is transferred to the VM instance. So, to provide the SSH key to the instance, we enabled OS Login for the instance which provides these keys through the Google Account to avoid hassle of managing the keys by us. The screenshot shows that the key pairs generated would be assigned to the instance as OS login is enabled.



The screenshot shows the Google Cloud Platform interface for a VM instance. The left sidebar navigation includes Compute Engine, VM instances, Instance groups, Instance templates, Sole-tenant nodes, Machine images, Disks, Snapshots, Images, TPUs, Migrate for Compute Engine, Committed use discounts, Metadata, Health checks, Zones, Network endpoint groups, Operations, and Marketplace. The main content area displays the 'VM instance details' for 'public-image-instance-gcp'. It lists the Boot disk (public-image-instance-gcp, debian-10-buster-v20200910, 20 GB) and Additional disks (trial-1, 100 GB). Under Availability policies, Preemptibility is set to Off (recommended), On host maintenance is set to Migrate VM instance (recommended), and Automatic restart is set to On (recommended). Other sections include Custom metadata (enable-oslogin: True), SSH Keys (None), Service account (761625510094-compute@developer.gserviceaccount.com), and Cloud API access scopes (Allow default access). The URL in the browser bar is https://console.cloud.google.com/compute/instanceTemplates/list?cloudshell=true&organizationId=68... .

Now we create the key pairs which would be used to authenticate the login. The public/private key pairs are generated using the keygen of the type RSA. The file containing the public keys is stored as hitesh.pub and private key file is named as hitesh. The value after -C is the google account to which these keys would be provided to enable the authentication. These public/private key pairs are now stored locally.

```
Google Cloud SDK Shell
C:\Users\hites\AppData\Local\Google\Cloud SDK>ssh-keygen -t rsa -f hitesh -C hthadhan@g.syr.edu
Generating public/private rsa key pair.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in hitesh.
Your public key has been saved in hitesh.pub.
The key fingerprint is:
SHA256:9WCWUOgan/BDVipv1C9z2TugCC1FpE1WM8g0366CsDI hthadhan@g.syr.edu
The key's randomart image is:
+---[RSA 2048]---+
| +B== |
| ==+= |
| .o.+B . |
| + B++ |
| . #S. .oo |
| o+.O o.= . |
| E . .+o.= . . |
| o . . . o |
| . |
+-----[SHA256]----+
```

The public keys are transferred to the instance for the instance to authenticate the login. The ttl is optional parameter which gives the time to live and is set to 1000 for the request to go the instance and live for some time before expiration.

2. Connecting using third-party tools (SSH)

Now that the public keys are transferred to the VM instance for authentication, we use the private key to be able to allow the access as these are key pairs. The format to login to the instance is

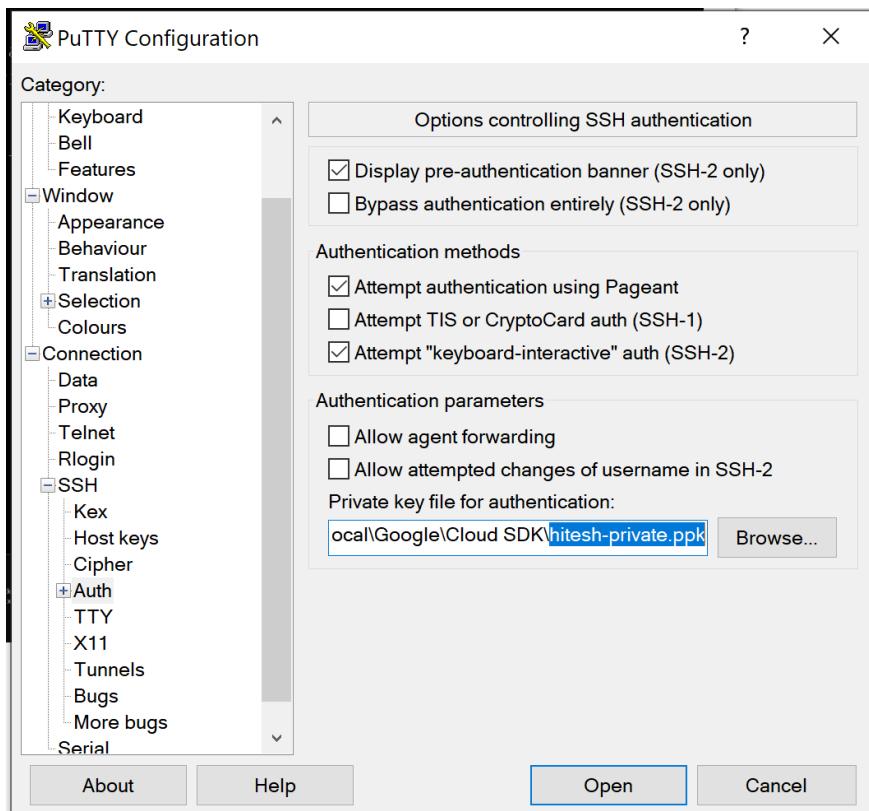
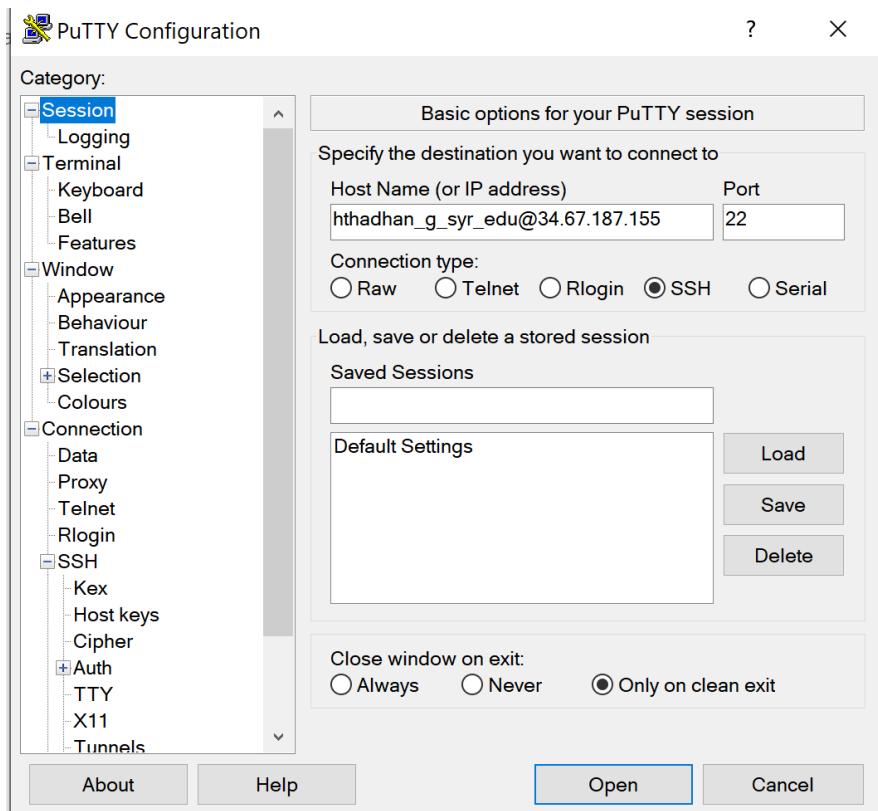
```
ssh -i [PRIVATE_KEY_PATH] [USERNAME]@[EXTERNAL_IP_ADDRESS]
```

The authentication is successful and we do not have any error related to authentication like public key error only connection timed out. Successfully created secured ssh connection to the instance using the public/private key pairs transferred to the VM instance for the authentication.

```
[Google Cloud Shell] C:\Users\hitesh\AppData\Local\Google\Cloud SDK>ssh -i hitesh-private.ppk hthadhan_g_syr_edu@34.57.187.155  
ssh: connect to host 34.57.187.155 port 22: Connection timed out  
C:\Users\hitesh\AppData\Local\Google\Cloud SDK>
```

Below shows how we can use Putty to connect to the VM instance with the Username we mentioned while generating the public/private key pairs using keygen.

Private key path is provided in the putty at SSH -> Auth and username along with External IP address of the instance to login specified in the IP Address.



Successful authentication and login to the instance from the putty is shown below using the third-party tools (SSH) connection.

The screenshot shows a terminal window with the following text output:

```
hthadhan_g_syr_edu@public-image-instance-gcp: ~
Using username "hthadhan_g_syr_edu".
Authenticating with public key "imported-openssh-key"
Linux public-image-instance-gcp 4.19.0-10-cloud-amd64 #1 SMP Debian 4.19.132-1 (2020-07-24) x86_64

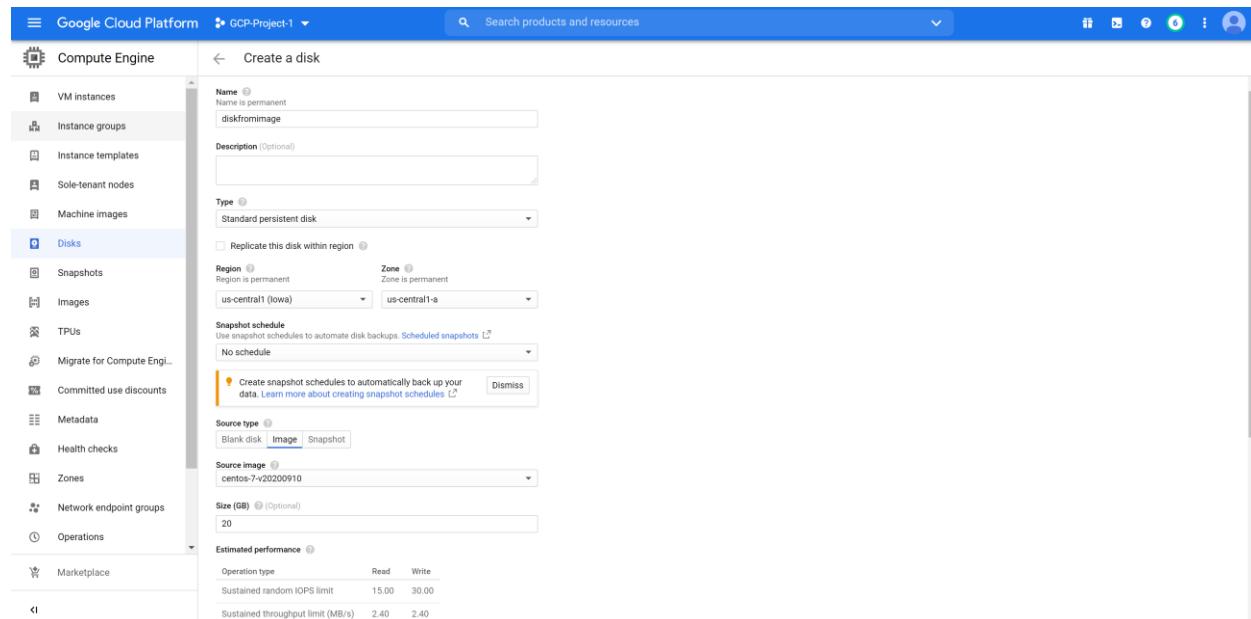
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Sep 22 01:44:16 2020 from 35.235.240.0
hthadhan_g_syr_edu@public-image-instance-gcp:~$
```

G. Complete the following sub-modules in *Creating Customized Boot Disks*:

1. Creating a standalone boot persistent disk from an image:

A standalone disk is created with a size of 20GB which can be used later to be attached to any VM instance as an additional storage hard disk to store additional files or operating system files when the storage is almost full.



Standalone persistent boot disk creation is successful with a 20GB disk size is shown below.

Name	Status	Type	Size	Zone(s)	In use by	Snapshot schedule	Actions
diskfromimage	✓	Standard persistent disk	20 GB	us-central1-a		None	⋮
preemptibleinstance-1	✓	Standard persistent disk	20 GB	us-central1-a	preemptibleinsta...	None	⋮
public-image-instance-gcp	✓	Standard persistent disk	20 GB	us-central1-a	public-image-ins...	None	⋮
snapshotinstance-1	✓	Standard persistent disk	20 GB	us-central1-a	snapshotinstance-1	None	⋮
trial-1	✓	Standard persistent disk	100 GB	us-central1-a	public-image-ins...	None	⋮

H. Creating an SQL Server Instance

SQL Server instance is created using the SQL server 2012 Windows OS with a configuration for better performance like 2CPUS's etc. Firewall rule is created to enable the TCP traffic coming to the instance on the port 1433. This rule allows us to connect to the instance to be able to manage the SQL server database hosted on the Windows instance.

Create a firewall rule

Action on match: Allow Deny

Targets: Specified target tags

Target tags: *

Source filter: IP ranges

Source IP ranges: *

Second source filter: None

Protocols and ports:

- Allow all
- Specified protocols and ports

tcp: 1433

udp: all

Other protocols: protocols, comma separated, e.g. ah, sctp

CREATE CANCEL

Successful creation of Windows instance is shown below.

The screenshot shows the Google Cloud Platform Compute Engine VM instances page. On the left sidebar, under 'Compute Engine', there are several options: VM instances, Instance groups, Instance templates, Sole-tenant nodes, Machine images, Disks, Snapshots, Images, TPUs, Migrate for Compute Engine, Committed use discounts, Metadata, Health checks, Zones, Network endpoint groups, Operations, and Marketplace. The main area displays a table of VM instances:

Name	Zone	Recommendation	In use by	Internal IP	External IP	Connect
preemptibleinstance-1	us-central1-a			10.128.0.4 (nic0)	146.148.111.50	SSH
public-image-instance-gcp	us-central1-a			10.128.0.2 (nic0)	34.67.187.155	SSH
snapshotinstance-1	us-central1-a			10.128.0.3 (nic0)	34.123.129.52	SSH
sqlserverinstance	us-central1-a			10.128.0.5 (nic0)	34.123.54.136	RDP

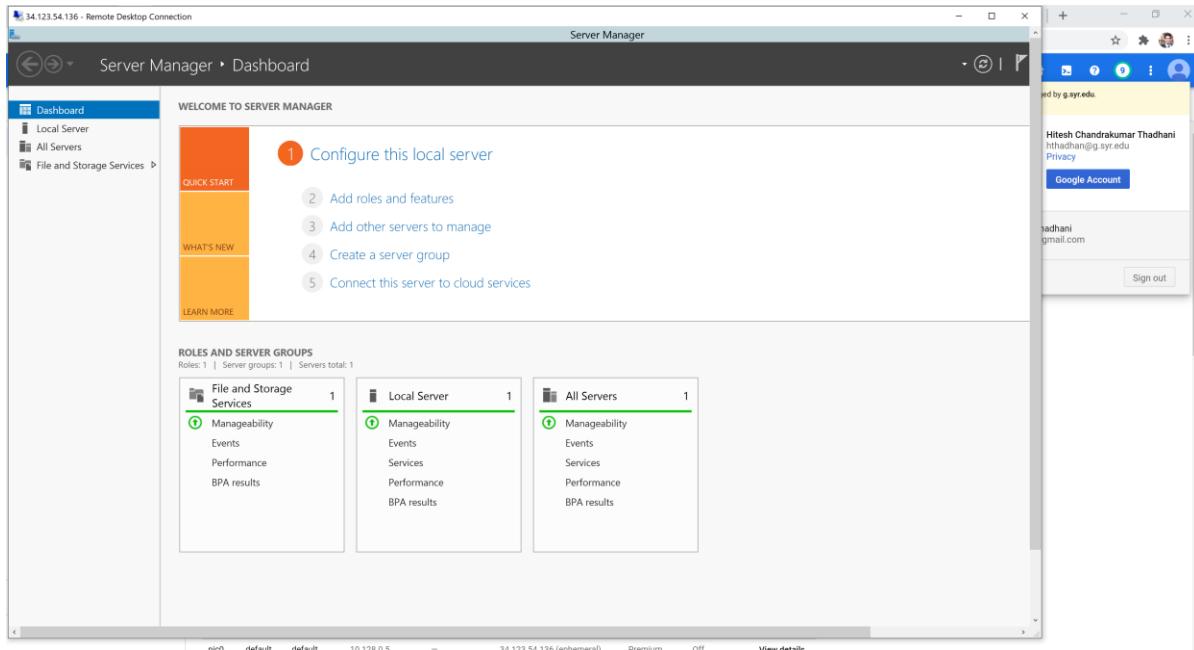
Below the table, there are 'Related Actions' buttons: View Billing Report, Monitor VMs, Explore VM Logs, Setup Firewall Rules, and Patch Management. To the right, a 'Select an instance' panel is open, showing tabs for PERMISSIONS, LABELS, and MONITORING, with a message: 'Please select at least one resource.'

The Windows instance with SQL server 2012 running is accessed using the RDP (Remote Desktop Protocol). RDP is used to connect to any Windows instance from outside to manage the instance and the database running on the Windows Machine.

The screenshot shows the Microsoft Server Manager Dashboard. On the left, there's a navigation bar with icons for Home, Local Server, All Servers, and File and Storage Services. The main area has a 'WELCOME TO SERVER MANAGER' section with a 'QUICK START' button and a numbered list: 1. Configure this local server, 2. Add roles and features, 3. Add other servers to manage, 4. Create a server group, 5. Connect this server to cloud services. Below this, there's a 'ROLES AND SERVER GROUPS' section with three boxes:

- File and Storage Services**: Manageability, Events, Performance, BPA results.
- Local Server**: Manageability, Events, Services, Performance, BPA results.
- All Servers**: Manageability, Events, Services, Performance, BPA results.

At the bottom, there's a taskbar with icons for Start, File Explorer, Task View, and Taskbar settings, along with system status information: 10:16 PM, 9/21/2020.

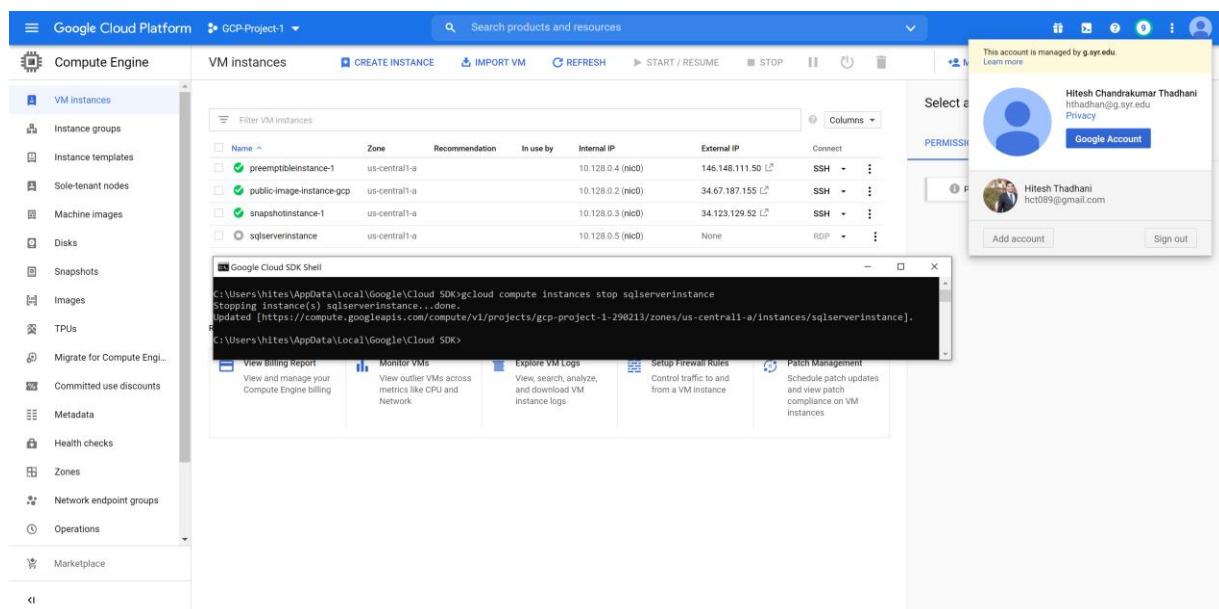


Section 5: Managing your instances

A. Stopping an Instance

1. Stopping an instance (GCloud)

Stopping the sqlserverinstance using the Gcloud command line to save the cost when not using it.



B. Deleting an Instance

Complete the following sub-modules in ***Deleting an Instance***:

1. Delete an Instance (GCloud)

Deleting the sqlserverinstance using the Gcloud command line.

```

a317e330053f4648b89c1102f7570b7e2e7292VaGeroVRbr
vcRZFAuPHUP2tlnGMAK5Kf1y1EFGqgtfB857n0BT1QwP3Va0xFXgU+POABje
mzbBlnHhkpVJNB5FM2zJnpSP104A3sF3TEFW1kWtIrg6JN)==
---- END PUBLIC KEY ----
name: users/hthadhan@syu.edu sshPublicKeys/29859aca0d90215c51f32ff588de08fb9e7da138545d881583d6a4d5f1e86c11

C:\Users\hitesh\AppData\Local\Google\Cloud SDK>gcloud compute instances stop sqlserverinstance
Stopping instance(s) sqlserverinstance...done.
Updated [https://compute.googleapis.com/compute/v1/projects/gcp-project-1-290213/zones/us-central1-a/instances/sqlserverinstance].

C:\Users\hitesh\AppData\Local\Google\Cloud SDK>gcloud compute instances delete sqlserverinstance
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.
- [sqlserverinstance] in [us-central1-a]

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

Deleted [https://www.googleapis.com/compute/v1/projects/gcp-project-1-290213/zones/us-central1-a/instances/sqlserverinstance].
C:\Users\hitesh\AppData\Local\Google\Cloud SDK>

```

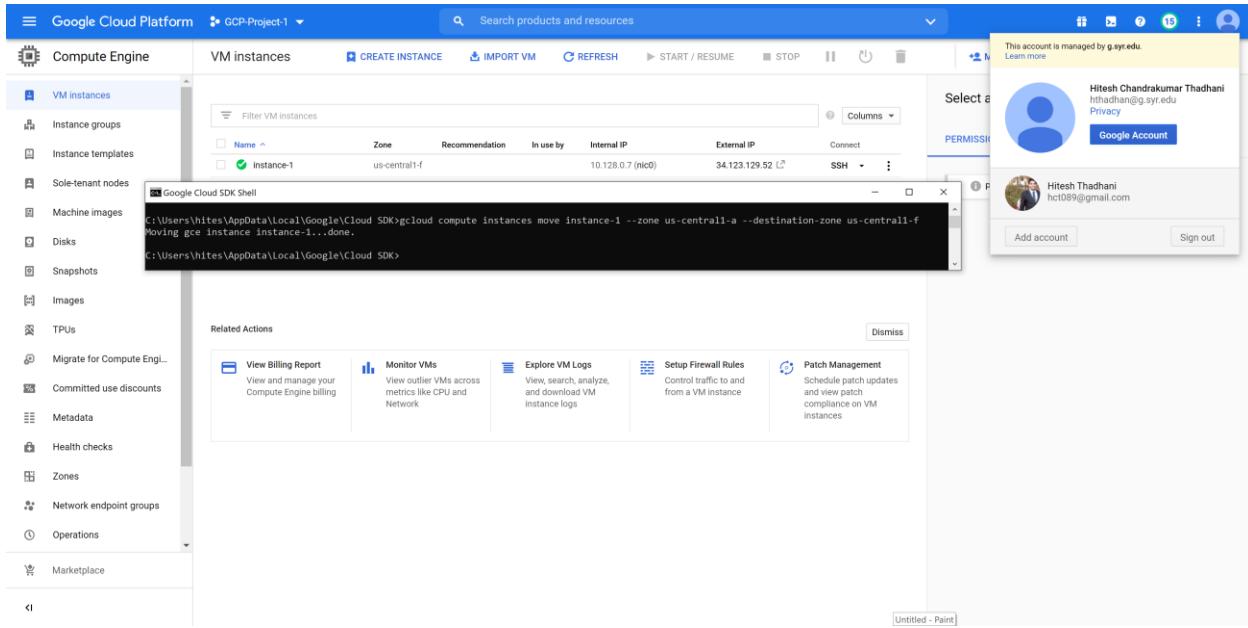
C. Moving an instance

Complete the following sub-module in ***Moving an instance between zones***:

1. Moving an instance automatically (GCloud)

The instance-1 which was in the Zone us-central1-a is being moved to us-central1-f using the Gcloud command line

Name	Network	Subnetwork	Primary Internal IP	Alias IP ranges	External IP	Network Tier	IP forwarding	Network details
nic0	default	default	10.128.0.6	—	34.123.129.52 (ephemeral)	Premium	Off	View details



D. Complete the following sub-module in ***Performing Other Tasks With Your Instances***:

1. Copy files between an instance and local computer

Copying data from Local Machine to GCP Cloud Instance:

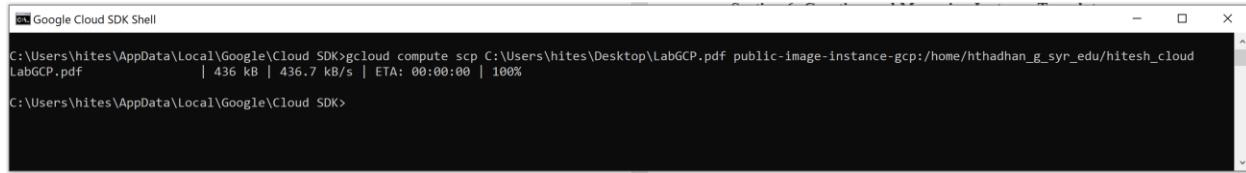
LabGCP pdf file was copied using gcloud scp command from the local machine to the instance. The below shows a new folder created with the name hitesh_cloud for the file to reside inside this folder.

```
hthadhan_g_syr_edu@public-image-instance-gcp: ~/hitesh_cloud - Google Chrome
ssh.cloud.google.com/projects/gcp-project-1-290213/zones/us-central1-a/instances/public-image-instance-gcp?useAdminProxy=true&a...
Connected, host fingerprint: ssh-rsa 0 70:D5:61:A0:26:4B:DD:19:D2:41:9C:13:23:18
:1A:BE:76:82:9E:59:DD:1F:4C:CF:54:90:C3:14:CA:77:54:38
Linux public-image-instance-gcp 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.

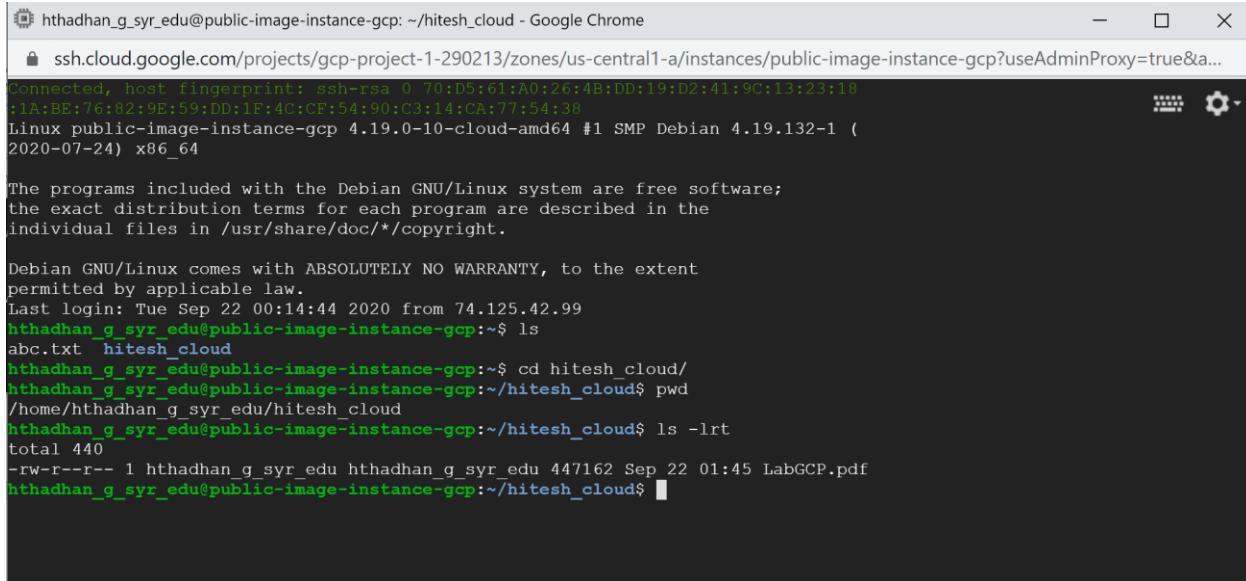
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Sep 22 00:14:44 2020 from 74.125.42.99
hthadhan_g_syr_edu@public-image-instance-gcp:~$ ls
abc.txt  hitesh_cloud
hthadhan_g_syr_edu@public-image-instance-gcp:~$ cd hitesh_cloud/
hthadhan_g_syr_edu@public-image-instance-gcp:~/hitesh_cloud$ pwd
/home/hthadhan_g_syr_edu/hitesh_cloud
hthadhan_g_syr_edu@public-image-instance-gcp:~/hitesh_cloud$
```

The pdf file is copied successfully from the Local Machine to the hitesh_cloud folder in the VM as shown below.



```
C:\Users\hites\AppData\Local\Google\Cloud SDK>gcloud compute scp C:\Users\Desktop\LabGCP.pdf public-image-instance-gcp:/home/hthadhan_g_syr_edu/hitesh_cloud  
LabGCP.pdf | 436 kB | 436.7 kB/s | ETA: 00:00:00 | 100%
```

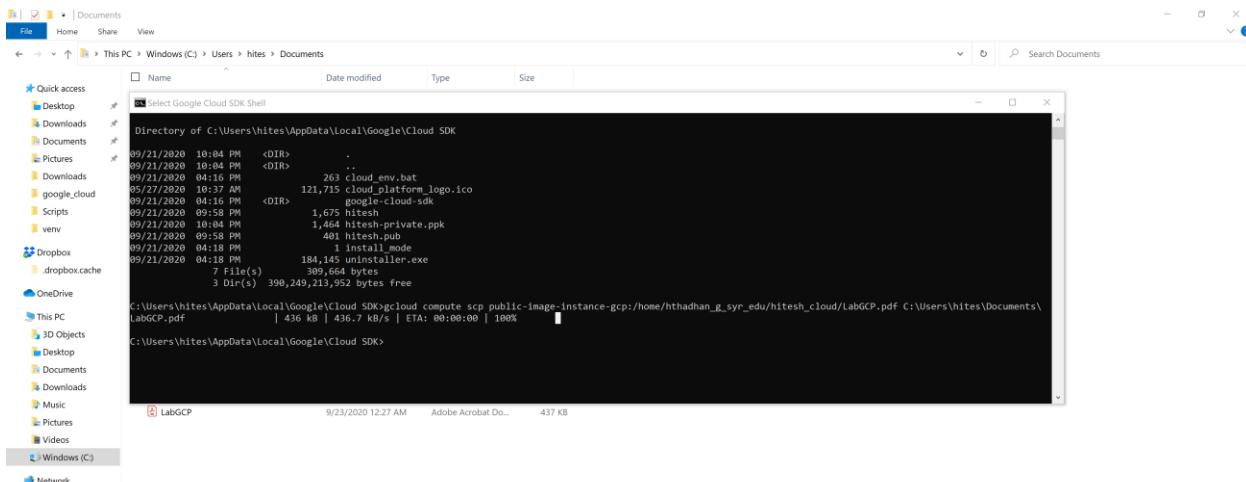
File is successfully residing inside the hitesh_cloud folder on the VM.



```
Connected, host fingerprint: ssh-rsa 0 70:D5:61:A0:26:4B:DD:19:D2:41:9C:13:23:18  
:1A:BE:76:82:9E:59:DD:1F:4C:C8:54:90:C3:14:CA:77:54:38  
Linux public-image-instance-gcp 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.  
Last login: Tue Sep 22 00:14:44 2020 from 74.125.42.99  
hthadhan_g_syr_edu@public-image-instance-gcp:~$ ls  
abc.txt hitesh_cloud  
hthadhan_g_syr_edu@public-image-instance-gcp:~$ cd hitesh_cloud/  
hthadhan_g_syr_edu@public-image-instance-gcp:~/hitesh_cloud$ pwd  
/home/hthadhan_g_syr_edu/hitesh_cloud  
hthadhan_g_syr_edu@public-image-instance-gcp:~/hitesh_cloud$ ls -lrt  
total 440  
-rw-r--r-- 1 hthadhan_g_syr_edu hthadhan_g_syr_edu 447162 Sep 22 01:45 LabGCP.pdf  
hthadhan_g_syr_edu@public-image-instance-gcp:~/hitesh_cloud$
```

Copying data from GCP instance to Local Machine

The same file was copied from the VM instance to the Local Machine in the Documents folder which didn't have the file earlier. After the successful copy using the gcloud scp command, the file LabGCP.pdf is found in the Documents folder as shown below.

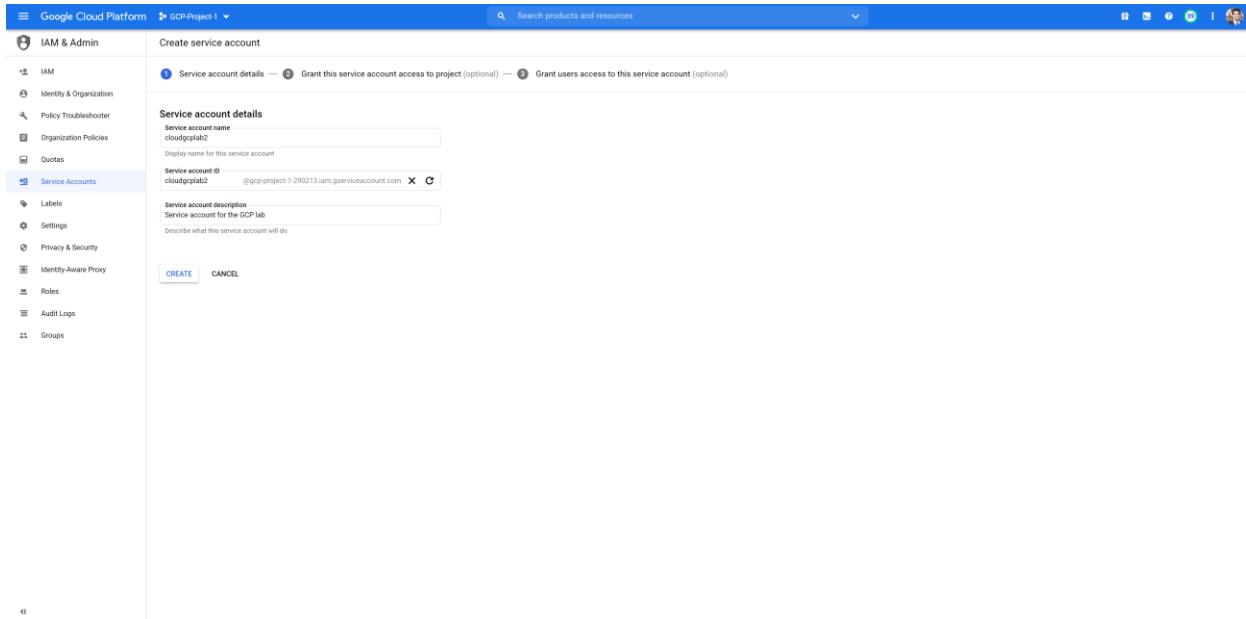


E. Setting Access Control

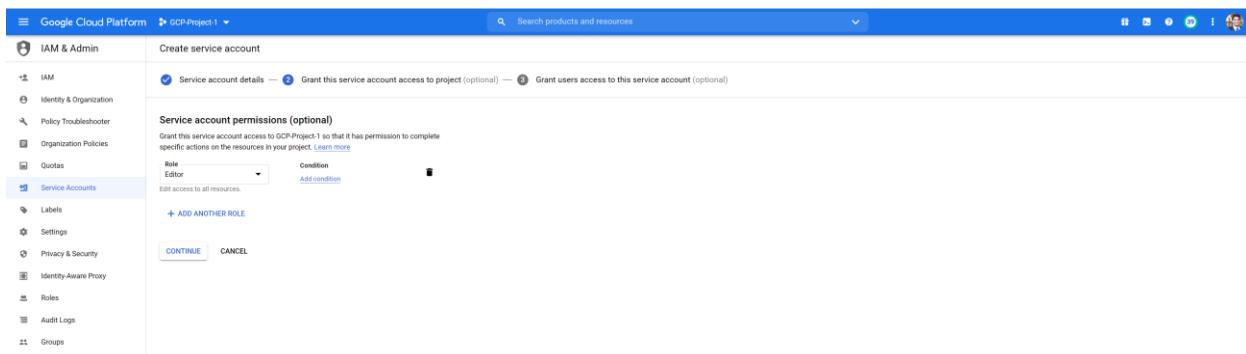
Complete the following sub-modules in ***Creating and enabling service accounts for instances:***

1. Creating a new service account

Service account is created to authenticate and run the applications using this service account instead of the user account. Service account is intended to represent a non-human user account which is authenticated and is authorized to access data. So, now we do not need to have every user authenticated to access the data by giving it privileges.



Service account is created with Editor role to be able to edit the resources of the VM.



Service account is created successfully as shown below.

2. Setting up a new instance to run as a service account (Console and GCloud)

Console:

A new instance is created using the Console with the service account specified created earlier.

The screenshot shows two pages from the Google Cloud Platform Compute Engine interface.

VM instance details:

- General:** Instance name is 'None', created on Sep 22, 2023, at 4:52:02 PM.
- Network interfaces:** One interface named 'n10' with network 'default' and subnet 'default'. Internal IP is 10.128.0.32, external IP is 34.122.204.73 (ephemeral). Network tier is Premium, IP forwarding is Off.
- Public DNS PTR Record:** None.
- Firewall:** Allow HTTP traffic and Allow HTTPS traffic are checked.
- Network tags:** http-server, https-server.
- Deletion protection:** Enabled.
- Confidential VM service:** Disabled.
- Boot disk:** Name is 'service-account-instance-console', image is 'debian-9-stretch-v20200910', size is 20 GB, device name is 'service-account-instance-console', type is Standard persistent disk, encryption is Google managed, mode is Boot, read/write, and when deleting instance is Delete disk.
- Additional disks:** None.
- Local disks:** None.
- Shielded VM:** A note says 'Select a shielded image to use shielded VM features. Turn on all settings for the most secure configuration.' Options include Turn on Confidential Compute, Turn on TPM, and Turn on Integrity Monitoring.
- Availability policies:**
 - Preemptibility: Off (recommended)
 - On host maintenance: Migrate VM instance (recommended)
 - Automatic restart: On (recommended)
- Custom metadata:** None.
- SSH Keys:** Block project-wide SSH keys is checked.
- Service account:** 'cloudsql@gcp-project-1:290213.iam.gserviceaccount.com' is selected.

VM Instances list:

- Shows a table of VM instances with columns: Name, Zone, Recommendation, In use by, Internal IP, External IP, and Connect.
- Instances listed:
 - Instance-1 (us-central1-f)
 - preemptibleinstance-1 (us-central1-a)
 - public-image-instance-gcp (us-central1-a)
 - service-account-instance-console (us-central1-a)
 - snapshothost-1 (us-central1-a)
 - sqlinstance-1 (us-central1-a)

Gcloud:

A new instance is created and assigned the service account using the Gcloud command line.

The screenshot shows the Google Cloud Platform Compute Engine interface and a terminal window.

VM Instances list:

- Shows a table of VM instances with columns: Name, Zone, Recommendation, In use by, Internal IP, External IP, and Connect.
- Instances listed:
 - Instance-1 (us-central1-f)
 - preemptibleinstance-1 (us-central1-a)
 - public-image-instance-gcp (us-central1-a)
 - service-account-instance-console (us-central1-a)
 - service-account-instance-gcloud (us-central1-a)

Terminal Window (Google Cloud SDK Shell):

```

Welcome to the Google Cloud SDK! Run "gcloud -h" to get the list of available commands.
...
C:\Users\hitesh\AppData\Local\Google\Cloud SDK>gcloud compute instances create service-account-instance-gcloud --service-account cloudsql@gcp-project-1:290213.iam.gserviceaccount.com
Created [https://www.googleapis.com/compute/v1/projects/gcp-project-1-290213/zones/us-central1-a/instances/service-account-instance-gcloud].
NAME          ZONE        MACHINE_TYPE PREEMPTIBLE INTERNAL_IP  EXTERNAL_IP   STATUS
service-account-instance-gcloud us-central1-a n1-standard-1    PREEMPTIBLE 10.128.0.33  35.238.13.213  RUNNING
  
```

This service account with the Editor Roles allows to edit or modify the resources of the VM. All the instances with this service account linked to them would be able to edit the VM due to this Editor Role.

3. Changing the service account and access scopes for an instance

The service account for the instance is changed to the default Compute Engine service account and allowed full access to the Cloud API's so that there is a high degree of flexibility for the access which may be required to access the applications.

This screenshot shows the 'VM instance details' page for a VM named 'service-account-instance-console'. The 'Service account' dropdown is set to 'Compute Engine default service account'. Under 'Access scopes', the 'Allow full access to all Cloud APIs' option is selected. The 'Save' button is visible at the bottom.

This screenshot shows the same 'VM instance details' page after changes. The 'Service account' dropdown now lists '76162551094-compute@developer.gserviceaccount.com'. The 'Cloud API access scopes' dropdown is set to 'Allow full access to all Cloud APIs'. The 'Save' button is visible at the bottom.

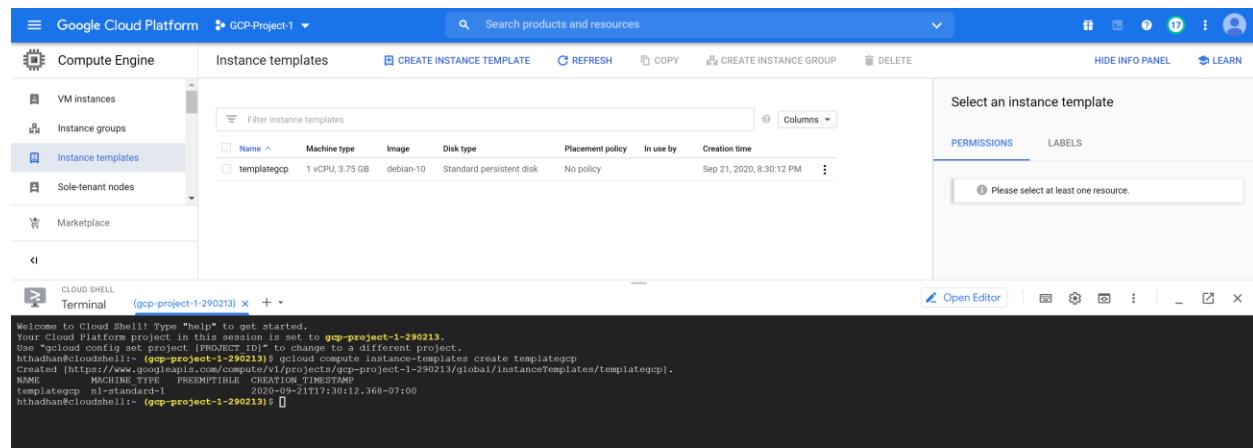
Section 6: Creating and Managing Instance Templates

Complete the following sub-modules in *Creating Instance Templates*:

A. Creating a new instance template (GCloud)

An instance template lets us define the machine type, boot disk image, network properties to create an instance later on using this template. These instance templates can be used to create a single individual instance or a group of managed instances. An instance template cannot be edited once created so for a modification we need to create a new template. These templates ease the creation process as we can define the parameters in the template to be used later on for the instance creation.

Instance template created using the Gcloud command line is shown below.



The screenshot shows the Google Cloud Platform Compute Engine Instance templates page. The left sidebar has 'Compute Engine' selected under 'Instance templates'. The main area displays a table of instance templates with one entry:

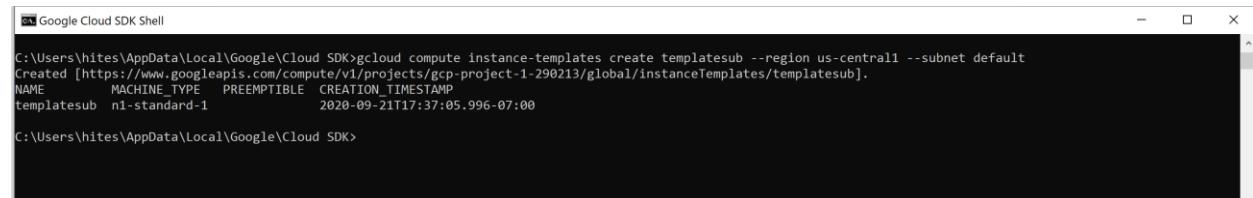
Name	Machine type	Image	Disk type	Placement policy	In use by	Creation time
templategcp	1 vCPU, 3.75 GB	debian-10	Standard persistent disk	No policy		Sep 21, 2020, 8:30:12 PM

To the right of the table is a sidebar titled 'Select an instance template' with tabs for 'PERMISSIONS' and 'LABELS'. Below the table is a message: 'Please select at least one resource.' At the bottom left is a 'CLOUD SHELL' terminal window showing GCloud command output:

```
Welcome to Cloud Shell! Type "help" to get started.  
Your Cloud Platform project in this session is set to gcp-project-1-290213.  
The "gcloud config" project setting is set to a different project:  
hthadhan@cloudshell:~ (gcp-project-1-290213)$ gcloud config set project gcp-project-1-290213  
Created [https://www.googleapis.com/compute/v1/projects/gcp-project-1-290213/global/instanceTemplates/templategcp].  
NAME MACHINE_TYPE PREEMPTIBLE CREATION_TIMESTAMP  
templategcp n1-standard-1 2020-09-21T17:30:12.368-07:00  
hthadhan@cloudshell:~ (gcp-project-1-290213)$ ]
```

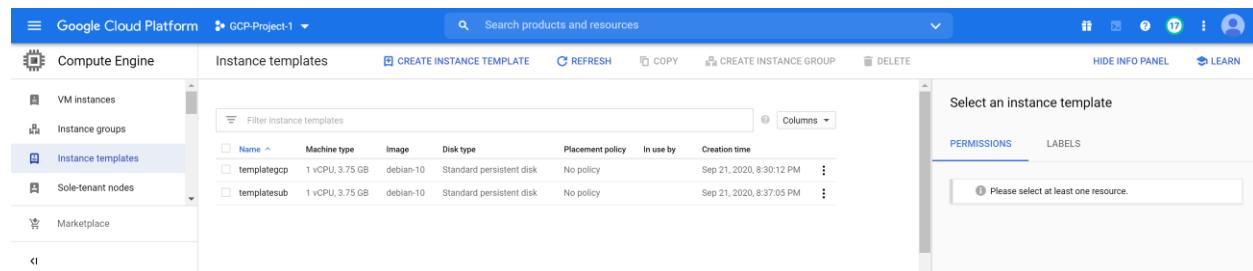
B. Creating an instance template that specifies a subnet

Now creating an instance template using a subnet. This allows to have an instance within a specified subnet or sub network which is defined earlier in the subnet and not on a global network.



The screenshot shows a terminal window titled 'Google Cloud SDK Shell'. The command entered is:

```
C:\Users\hites\AppData\Local\Google\Cloud SDK>gcloud compute instance-templates create templatesub --region us-central1 --subnet default  
Created [https://www.googleapis.com/compute/v1/projects/gcp-project-1-290213/global/instanceTemplates/templatesub].  
NAME MACHINE_TYPE PREEMPTIBLE CREATION_TIMESTAMP  
templatesub n1-standard-1 2020-09-21T17:37:05.996-07:00  
C:\Users\hites\AppData\Local\Google\Cloud SDK>
```



Section 7: Creating and Managing Groups of Instances

A. Complete the following sub-modules in *Creating managed instance groups*:

1. Creating a managed instance group (Console and GCloud)

Managed instance group of instances are a group of managed instances which are managed as a single entity and not as an individual instance. Any change would be applied to all the instances of the managed group.

Console:

Created a Managed group of instances with the template templatesub created earlier using the Console.

To create an instance group, select one of the options:

- New managed instance group (stateless)**
Use for stateless serving and batch workloads.
Supports:
 - autoscaling
 - autohealing, updating, regional deployments
 - load balancing
- New managed instance group (stateful)**
Use for workloads that require persistent data or configuration such as databases or legacy monolithic applications.
Supports:
 - preserving the state of disks and metadata
 - autohealing, updating, regional deployments
 - load balancing
- New unmanaged instance group**
Use for load balancing across a group of VMs that you manage yourself.
Supports:
 - load balancing

Name (Optional)
Name is permanent
instance-group-console

Description (Optional)
Managed Group created using Console

Location
To ensure higher availability, select a multiple zone location for an instance group.
Learn more

Region (Optional)
Region is permanent
us-central1 (Iowa)

Zone (Optional)
Zone is permanent
us-central1-a

Specify port name mapping (Optional)

Instance template (Optional)
templatesub

Number of instances
Based on autoscaling configuration

Autoscaling
Use autoscaling to allow automatic resizing of this instance group for periods of high and low load. [Autoscaling groups of instances](#)

Autoscaling mode
Autoscale

Autoscaling metrics
Use metrics to determine when to autoscale the group. [Autoscaling policy and target utilization](#)

CPU utilization: 60% (default)

Compute Engine

VM instances

Instance groups

Instance templates

Sole-tenant nodes

Machine images

Disks

Snapshots

Instance groups

[CREATE INSTANCE GROUP](#) [REFRESH](#) [DELETE](#)

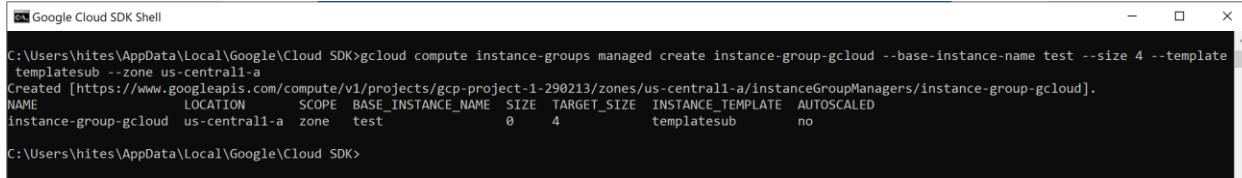
Instance groups are collections of VM instances that use load balancing and automated services, like autoscaling and autohealing. [Learn more](#)

Filter resources

Name	Zone	Instances	Template	Group type	Creation time	Recommendation	Autoscaling	In use by
instance-group-console	us-central1-a	1	templatesub	Managed	Sep 21, 2020, 8:44:17 PM		On: Target CPU utilization 60%	

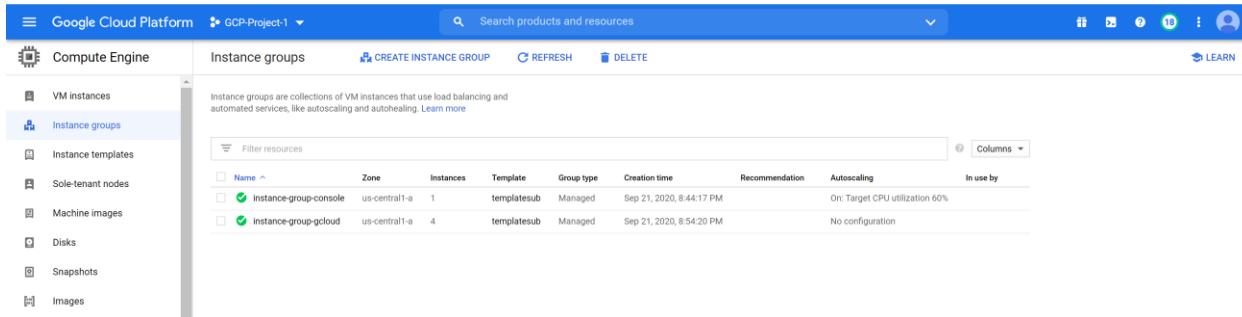
Gcloud:

Managed group of instances is created using the Gcloud command line with managed as the word after instance-groups indicating the instances are managed group along with templatesub as the template to create the Managed Group of instances.



```
C:\Users\hites\AppData\Local\Google\Cloud SDK>gcloud compute instance-groups managed create instance-group-gcloud --base-instance-name test --size 4 --template templatesub --zone us-central1-a
Created [https://www.googleapis.com/compute/v1/projects/gcp-project-1-290213/zones/us-central1-a/instanceGroupManagers/instance-group-gcloud].
NAME          LOCATION      SCOPE   BASE_INSTANCE_NAME  SIZE  TARGET_SIZE INSTANCE_TEMPLATE  AUTOSCALED
instance-group-gcloud  us-central1-a  zone    test            0      4           templatesub        no

C:\Users\hites\AppData\Local\Google\Cloud SDK>
```

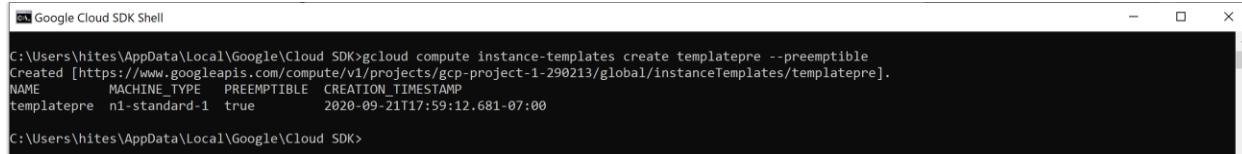


The screenshot shows the Google Cloud Platform interface for managing instance groups. The left sidebar is collapsed. The main area displays the 'Instance groups' section with a table. The table has columns: Name, Zone, Instances, Template, Group type, Creation time, Recommendation, and Autoscaling. Two entries are listed:

Name	Zone	Instances	Template	Group type	Creation time	Recommendation	Autoscaling
instance-group-console	us-central1-a	1	templatesub	Managed	Sep 21, 2020, 8:44:17 PM	On: Target CPU utilization 60%	No configuration
instance-group-gcloud	us-central1-a	4	templatesub	Managed	Sep 21, 2020, 8:54:20 PM		

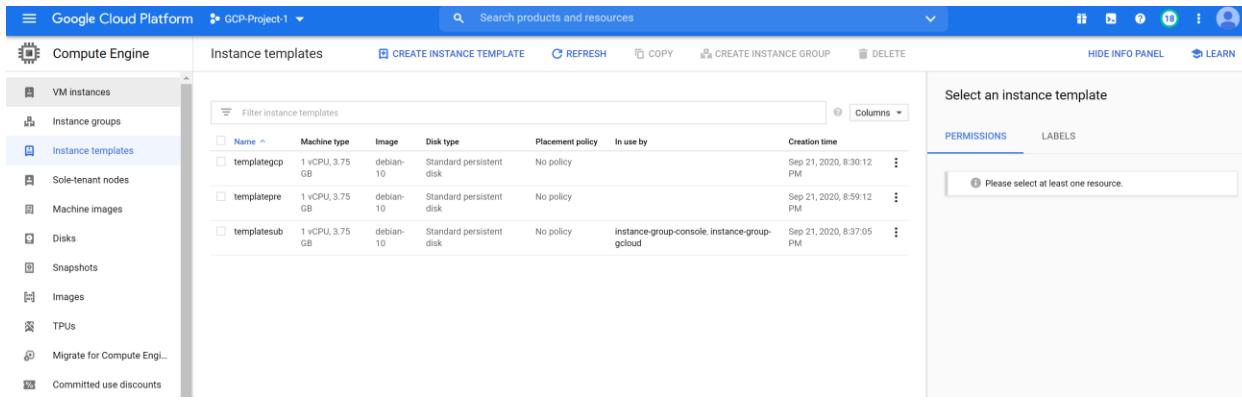
2. Creating groups of preemptible instances

Preemptible instance template is created first for it to be used as a template to create a Preemptible Group of managed instances using the Gcloud command line.



```
C:\Users\hites\AppData\Local\Google\Cloud SDK>gcloud compute instance-templates create templatepre --preemptible
Created [https://www.googleapis.com/compute/v1/projects/gcp-project-1-290213/global/instanceTemplates/templatepre].
NAME      MACHINE_TYPE  PREEMPTIBLE  CREATION_TIMESTAMP
templatepre  n1-standard-1  true        2020-09-21T17:59:12.681-07:00

C:\Users\hites\AppData\Local\Google\Cloud SDK>
```



The screenshot shows the Google Cloud Platform interface for managing instance templates. The left sidebar is collapsed. The main area displays the 'Instance templates' section with a table. The table has columns: Name, Machine type, Image, Disk type, Placement policy, In use by, and Creation time. Three entries are listed:

Name	Machine type	Image	Disk type	Placement policy	In use by	Creation time
templategcp	1 vCPU, 3.75 GB	debian-10	Standard persistent	No policy		Sep 21, 2020, 8:30:12 PM
templatepre	1 vCPU, 3.75 GB	debian-10	Standard persistent	No policy		Sep 21, 2020, 8:59:12 PM
templatesub	1 vCPU, 3.75 GB	debian-10	Standard persistent	No policy	instance-group-console, instance-group-gcloud	Sep 21, 2020, 8:37:05 PM

A new Managed Instance group is created with the template templatepre as the preemptible instance template.

To create an instance group, select one of the options:

New managed instance group (stateless)
Use for stateless serving and batch workloads.
Supports:

- autoscaling
- autohealing, updating, regional deployments
- load balancing

New managed instance group (stateful)
Use for workloads that require persistent data or configuration such as databases or legacy monolithic applications.
Supports:

- preserving the state of disks and metadata
- autohealing, updating, regional deployments
- load balancing

New unmanaged instance group
Use for load balancing across a group of VMs that you manage yourself.
Supports:

- load balancing

Organize VM instances in a group to manage them together. [Instance groups](#)

Name Name is permanent

Description (Optional)

Location To ensure higher availability, select a multiple zone location for an instance group. [Learn more](#)

Region Region is permanent Zone Zone is permanent

Specify port name mapping (Optional)

Instance template

⚠ An instance group created from a template with a preemptible VM will not behave like other instance groups. [Learn more](#)

Number of instances

Autoscaling Use autoscaling to allow automatic resizing of this instance group for periods of high and low load. [Autoscaling groups of instances](#)

Autoscaling mode

Autoscaling metrics Use metrics to determine when to autoscale the group. [Autoscaling policy and target utilization](#)

Preemptible instance group creation is successful as shown below.

Compute Engine Instance groups [CREATE INSTANCE GROUP](#) [REFRESH](#) [DELETE](#) [LEARN](#)

VM instances Instance groups Instance templates Sole-tenant nodes Machine images Disks Snapshots Images TPUs Migrate for Compute Eng... Committed use discounts Metadata Health checks Zones Network endpoint groups Operations Marketplace

Instance groups are collections of VM instances that use load balancing and automated services, like autoscaling and autohealing. [Learn more](#)

Name	Zone	Instances	Template	Group type	Creation time	Recommendation	Autoscaling	In use by
instance-group-console	us-central1-a	1	templatesub	Managed	Sep 21, 2020, 8:44:17 PM	On: Target CPU utilization 60%		
instance-group-gcloud	us-central1-a	4	templatesub	Managed	Sep 21, 2020, 8:54:20 PM	No configuration		
instance-group-pre	us-central1-a	1	templatepre	Managed	Sep 21, 2020, 11:50:02 PM	On: Target CPU utilization 60%		

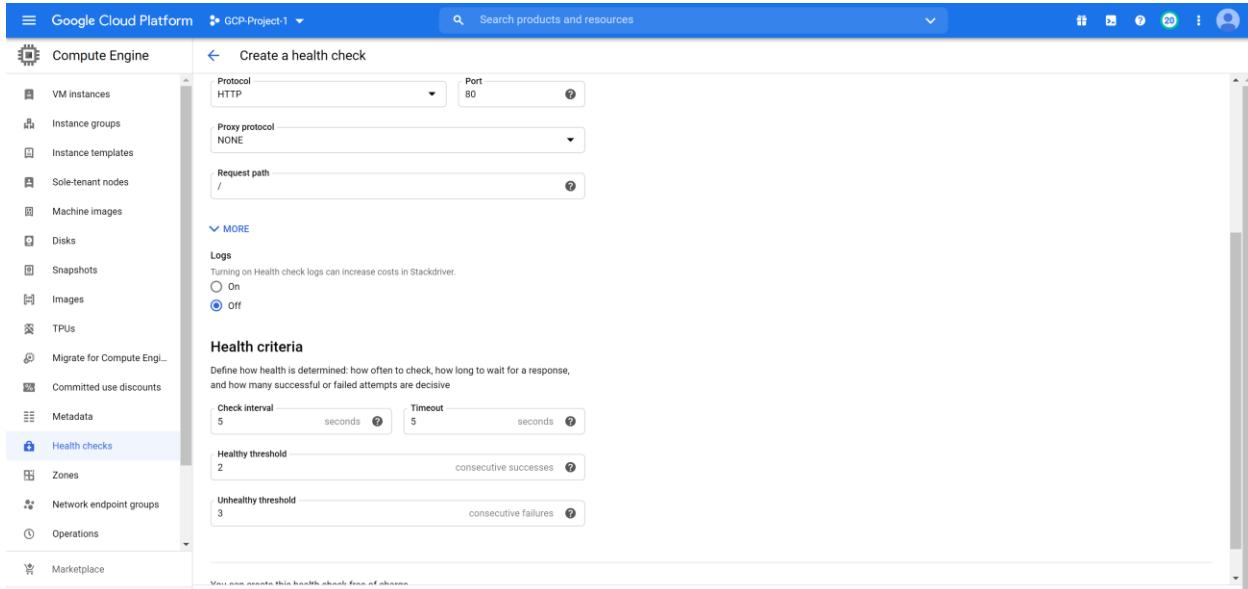
The screenshot shows the Google Cloud Platform Compute Engine interface. The left sidebar is titled 'Compute Engine' and includes options like VM instances, Instance groups, Instance templates, Sole-tenant nodes, Machine images, Disks, Snapshots, Images, TPU, and Migrate for Compute Engine. The main content area is titled 'Instance groups' and shows a single instance group named 'instance-group-pre'. A warning message states: 'This instance group uses preemptible instances, which have a lifespan of 24 hours or less. Learn more'. Below this, there are tabs for Members, Details, Monitoring, and Errors. The 'Members' tab displays a table with one row: 'instance-group-pre-x0r9'. The table columns include Name, Creation time, Template, Per instance config, Health check status, Internal IP, External IP, and Connect. The 'Health check status' column indicates 'Autohealing needs to be configured to get instances health.' The 'Autoscaling' section shows 'On' with 'CPU utilization 60%'.

B. Complete the following sub-module in ***Setting up health checking and autohealing:***
Setting up a health check and an autohealing policy (Console and GCloud)

Here we are setting up a health check policy to look for any issues with the instance health, responding within a specified amount of time to detect any failure and automatically heal this failure. This health check rule is configured on the port 80 for checking the health of the instance with health check setting set below.

The screenshot shows the 'Create a health check' page. The left sidebar is identical to the previous screenshot. The main form has a title 'Create a health check'. It includes fields for 'Name' (set to 'health-check-test'), 'Scope' (set to 'Global'), 'Protocol' (set to 'HTTP' with port '80'), 'Proxy protocol' (set to 'NONE'), and 'Request path' (set to '/'). Below this, there's a 'MORE' section with a 'Logs' toggle switch set to 'Off'. At the bottom, there's a 'Health criteria' section.

Health check setting is set with 5 sec intervals to check for the health. If there are 2 consecutive success responses on the port 80 from the instance it is considered to be healthy. If there are 3 consecutive failures of responses, the instance is considered UNHEALTHY and needs to be fixed to make it healthy again using the Console.



Setting up the health check using Gcloud command line with health check interval set to be 30sec to check the health every 30sec on the port 80 specified. Healthy threshold is set to 1 and 3 consecutive failures result in unhealthy state of the instance.

```
C:\Users\hites\AppData\Local\Google\Cloud SDK>gcloud compute health-checks create http check-gcloud-test --port 80 --check-interval 30s --healthy-threshold 1 --timeout 10s --unhealthy-threshold 3
Created [https://www.googleapis.com/compute/v1/projects/gcp-project-1-290213/global/healthChecks/check-gcloud-test].
NAME          PROTOCOL
check-gcloud-test  HTTP
C:\Users\hites\AppData\Local\Google\Cloud SDK>
```

Firewall rule is created to allow the health-check-rule created earlier to connect to the application with the mentioned IP addresses where the IP Addresses are inspected for checking the health.

```
C:\Users\hites\AppData\Local\Google\Cloud SDK>gcloud compute firewall-rules create allow-health-check --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/gcp-project-1-290213/global火walls/allow-health-check].
Creating firewall...done.
NAME          NETWORK DIRECTION PRIORITY ALLOW    DENY    DISABLED
allow-health-check  default  INGRESS   1000    tcp:80    False
C:\Users\hites\AppData\Local\Google\Cloud SDK>
```

The screenshot shows the Google Cloud Platform Compute Engine Health checks interface. On the left, there's a sidebar with options like VM instances, Instance groups, Instance templates, Sole-tenant nodes, Machine images, Disks, Snapshots, Images, and TPUs. The main area is titled 'Health checks' and contains a table with two rows:

Name	Scope	Region	Host	Path	Protocol	Port	In use by
check-gcloud-test	Global		/	HTTP	80		
health-check-test	Global		/	HTTP	80		

Health-check-rule created shows the IP Addresses to be checked for health of the instances in this range of the VM IP's.

The screenshot shows the Google Cloud Platform Firewall rules interface. The left sidebar lists VPC network, VPC networks, External IP addresses, Firewall (selected), Routes, VPC network peering, Shared VPC, Serverless VPC access, and Packet mirroring. The main panel displays the configuration for the 'allow-health-check' rule:

- Logs:** Off (view)
- Network:** default
- Priority:** 1000
- Direction:** Ingress
- Action on match:** Allow
- Source filters:**
 - IP ranges:** 130.211.0.0/22, 35.191.0.0/16
- Protocols and ports:** tcp:80
- Enforcement:** Enabled
- Insights:** None
- Hit count monitoring:** -
- Applicable to instances:** (Table showing VM instances)

A note at the bottom states: "The following table shows only the VM instances that you have permission to view. The 'default' network might contain other instances that aren't being displayed."

Assigning the Health checks created to the instances using the Console. In the Health Check, I mention the health check created earlier as the way of checking the health of the instance.

The screenshot shows the 'Edit instance-group-gcloud' configuration. Key settings include:

- Zone:** us-central1-a
- Instance template:** templatesub
- Number of instances:** 4
- Autoscaling:** Enabled, configured to allow automatic resizing for periods of high and low load.
- Health check:** Set to 'health-check-test (HTTP)' with port: 80, timeout: 5s, check interval: 5s, and unhealthy threshold: 3 attempts.
- Initial delay:** 300 seconds.

The screenshot shows the configuration of a managed instance group named 'Stackover Logging'. Key settings include:

- Description:** Managed Group created using Console
- Zone:** us-central1-a (1 instance)
- Creation time:** Sep 21, 2020, 8:44:17 PM
- Port name mapping:** None
- Instance template:** templatesub (1 out of 1 (100%) 1 instance)
- Autoscaling:** Turned on.
- Autoscaling metrics:** Metric: CPU utilization, Value: 60%.
- Update parameters:** Minimum number of instances: 1, Maximum number of instances: 10, Cool-down period: 60 seconds.
- Scale In Controls:** Disabled.
- Autorealing:** Health check: 'health-check-test', Initial delay (seconds): 300.

Updated the Managed Group created earlier with Health checks using Gcloud command line

```
C:\Users\hites\AppData\Local\Google\Cloud SDK>gcloud compute instance-groups managed update instance-group-gcloud --health-check check-gcloud-test --initial-delay 300 --zone us-central1-a
Updated [https://www.googleapis.com/compute/v1/projects/gcp-project-1-290213/zones/us-central1-a/instanceGroupManagers/instance-group-gcloud].
```

The instance group is updated with the health check so that if the instance is UNHEALTHY to be able to find such Unhealthy instances.

The screenshot shows the Google Cloud Platform Compute Engine interface. The left sidebar is collapsed. The main area is titled 'Instance groups' under 'Compute Engine'. A sub-menu for 'instance-group-gcloud' is open, showing tabs for 'Members', 'Details', 'Monitoring', and 'Errors'. The 'Details' tab is selected. It displays information about the zone ('us-central1-a (4 instances)'), creation time ('Sep 21, 2020, 8:54:20 PM'), port name mapping ('None'), and the instance template ('templatesub'). Below this, the 'Autoscaling' section shows 'No configuration' and the 'Number of instances' set to '4'. The 'Autohealing' section shows a 'Health check' named 'check-gcloud-test' with an 'Initial delay (seconds)' of '300'. At the bottom, there are 'Update parameters', 'Logs' (Stackdriver Logging), and 'Equivalent REST' links.

Section 8: Virtual Private Cloud (VPC)

A. Complete the following sub-modules in ***Using VPC networks***

1. Creating networks

i. Creating an auto mode network (Console)

We are creating a VPC (Virtual Private Network) using the Auto mode Network. A VPC is a virtual version of the physical network implemented to create an isolated virtual network partition. In the Auto mode, all the regions are selected and 1 subnet each for each region is selected. As the new regions are added, subnet from these regions is added automatically.

The screenshot shows the Google Cloud Platform VPC network interface. The left sidebar is collapsed. The main area is titled 'Create a VPC network' under 'VPC network'. A 'Name' field is filled with 'auto-mode-network'. Below it is a 'Description' field. The 'Subnets' section contains a note: 'Subnets let you create your own private cloud topology within Google Cloud. Click Automatic to create a subnet in each region, or click Custom to manually define the subnets.' A link 'Learn more' is provided. The 'Subnet creation mode' section has two options: 'Custom' (radio button) and 'Automatic' (radio button, selected). A warning message states: 'These IP address ranges will be assigned to each region in your VPC network. When an instance is created for your VPC network, it will be assigned an IP from the appropriate region's address range.' A table lists IP address ranges for various regions:

Region ↑	IP address range
asia-east1	10.140.0.0/20
asia-northeast1	10.146.0.0/20
asia-south1	10.160.0.0/20
asia-southeast1	10.148.0.0/20
australia-southeast1	10.152.0.0/20
europe-west1	10.132.0.0/20
europe-west2	10.154.0.0/20
europe-west3	10.156.0.0/20
europe-west4	10.164.0.0/20

Selected some firewall rules to allow routing to happen regionally.

The screenshot shows the 'Create a VPC network' page under the 'Firewall rules' section. A table lists several firewall rules:

Name	Type	Targets	Filters	Protocols / ports	Action	Priority
auto-mode-network-allow-icmp	Ingress	Apply to all	IP ranges: 0.0.0.0/0	icmp	Allow	65,534
auto-mode-network-allow-internal	Ingress	Apply to all	IP ranges: 10.128.0.0/9	all	Allow	65,534
auto-mode-network-allow-rdp	Ingress	Apply to all	IP ranges: 0.0.0.0/0	tcp:3389	Allow	65,534
auto-mode-network-allow-ssh	Ingress	Apply to all	IP ranges: 0.0.0.0/0	tcp:22	Allow	65,534
auto-mode-network-deny-all-ingress	Ingress	Apply to all	IP ranges: 0.0.0.0/0	all	Deny	65,535
auto-mode-network-allow-all-egress	Egress	Apply to all	IP ranges: 0.0.0.0/0	all	Allow	65,535

Below the table, there is a 'Dynamic routing mode' section with a radio button for 'Regional' selected, indicating Cloud Routers will learn routes only in the region where they were created.

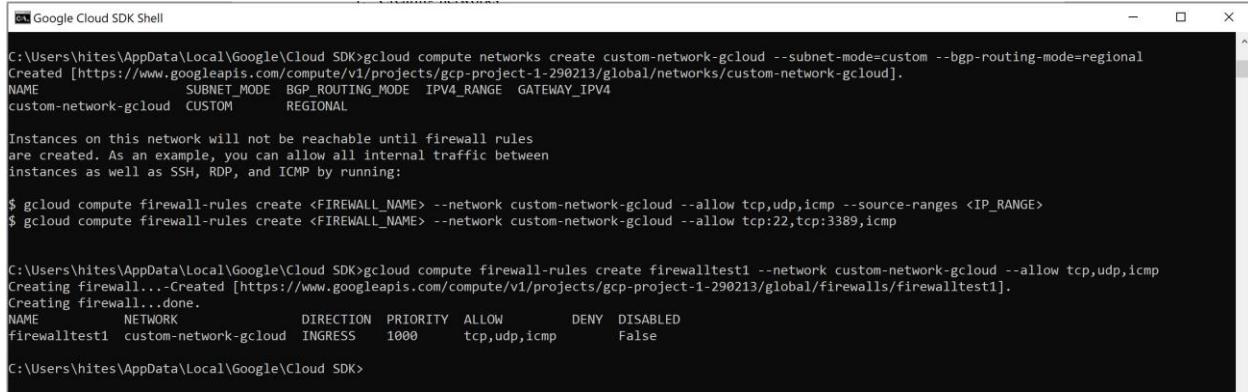
New auto mode network is created with 1 subnet from the each of the regions as shown below.

The screenshot shows the 'VPC networks' list page. It displays a table of auto-mode networks, each with 24 subnets and set to 'Auto' mode. The table includes columns for Name, Region, Subnets, Mode, IP address ranges, Gateways, Firewall Rules, Global dynamic routing, and Flow logs.

Name	Region	Subnets	Mode	IP address ranges	Gateways	Firewall Rules	Global dynamic routing	Flow logs
auto-mode-network	us-central1	24	Auto	10.128.0.0/20	10.128.0.1	2 Off	Off	
	europe-west1			10.132.0.0/20	10.132.0.1		Off	
	us-west1			10.138.0.0/20	10.138.0.1		Off	
	asia-east1			10.140.0.0/20	10.140.0.1		Off	
	us-east1			10.142.0.0/20	10.142.0.1		Off	
	asia-northeast1			10.146.0.0/20	10.146.0.1		Off	
	asia-southeast1			10.148.0.0/20	10.148.0.1		Off	
	us-east4			10.150.0.0/20	10.150.0.1		Off	
	australia-southeast1			10.152.0.0/20	10.152.0.1		Off	
	europe-west2			10.154.0.0/20	10.154.0.1		Off	
	europe-west3			10.156.0.0/20	10.156.0.1		Off	
	southamerica-east1			10.158.0.0/20	10.158.0.1		Off	
	asia-south1			10.160.0.0/20	10.160.0.1		Off	
	northamerica-northeast1			10.162.0.0/20	10.162.0.1		Off	
	europe-west4			10.164.0.0/20	10.164.0.1		Off	
	europe-north1			10.166.0.0/20	10.166.0.1		Off	
	us-west2			10.168.0.0/20	10.168.0.1		Off	
	asia-east2			10.170.0.0/20	10.170.0.1		Off	
	europe-west6			10.172.0.0/20	10.172.0.1		Off	
	asia-northeast2			10.174.0.0/20	10.174.0.1		Off	
	asia-northeast3			10.178.0.0/20	10.178.0.1		Off	
	us-west3			10.180.0.0/20	10.180.0.1		Off	
	us-west4			10.182.0.0/20	10.182.0.1		Off	

ii. Creating a custom mode network (GCloud)

Created a custom network manually by setting subnet-mode as Custom along with Regional Routing enabled using the bgp-routing-mode=regional. This custom network created is set to allow the TCP, UDP and ICMP traffic after the creation.



```

Google Cloud SDK Shell

C:\Users\hites\AppData\Local\Google\Cloud SDK>gcloud compute networks create custom-network-gcloud --subnet-mode=custom --bgp-routing-mode=regional
Created [https://www.googleapis.com/compute/v1/projects/gcp-project-1-290213/global/networks/custom-network-gcloud].
NAME          SUBNET_MODE  BGP_ROUTING_MODE  IPV4_RANGE  GATEWAY_IPV4
custom-network-gcloud  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 custom-network-gcloud --allow tcp,udp,icmp --source-ranges <IP_RANGE>
$ gcloud compute firewall-rules create <FIREWALL_NAME> --network custom-network-gcloud --allow tcp:22,tcp:3389,icmp

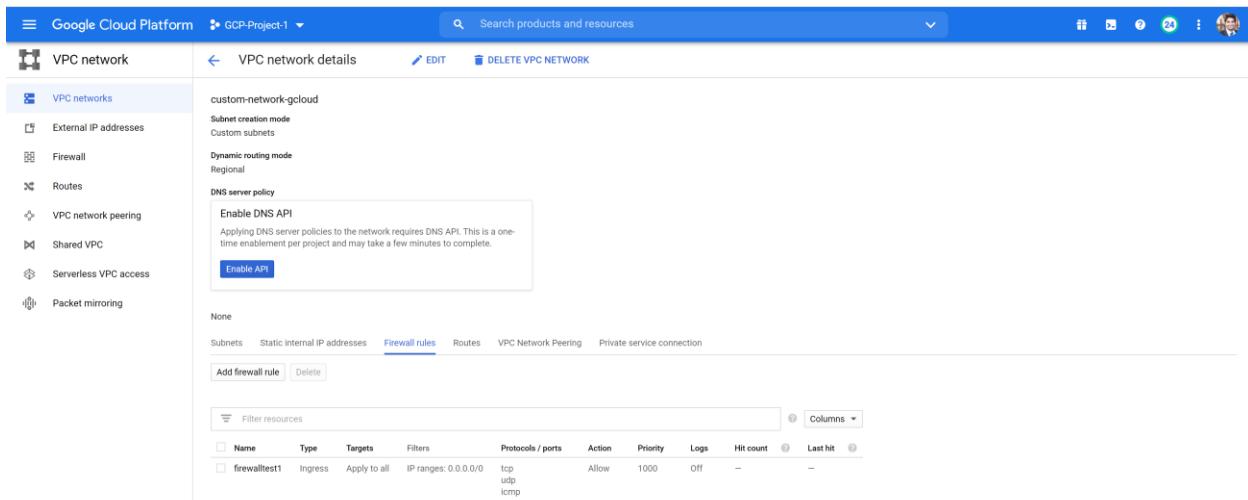
C:\Users\hites\AppData\Local\Google\Cloud SDK>gcloud compute firewall-rules create firewalltest1 --network custom-network-gcloud --allow tcp,udp,icmp
Creating firewall...Created [https://www.googleapis.com/compute/v1/projects/gcp-project-1-290213/global/firewalls/firewalltest1].
Creating firewall...done.

NAME          NETWORK        DIRECTION  PRIORITY ALLOW    DENY    DISABLED
firewalltest1  custom-network-gcloud  INGRESS    1000     tcp,udp,icmp  False

C:\Users\hites\AppData\Local\Google\Cloud SDK>

```

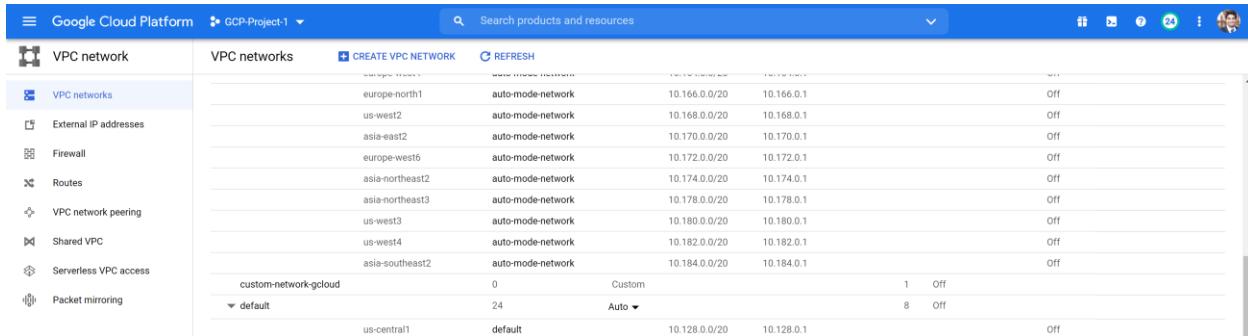
Creation of the manual custom mode network with the required firewall rules is successful.



The screenshot shows the 'VPC network' section of the Google Cloud Platform interface. Under 'VPC networks', it lists 'custom-network-gcloud' with 'Subnet creation mode' set to 'Custom subnets' and 'Dynamic routing mode' set to 'Regional'. In the 'Firewall' tab, a single firewall rule named 'firewalltest1' is listed:

Name	Type	Targets	Filters	Protocols / ports	Action	Priority	Logs	Hit count	Last hit
firewalltest1	Ingress	Apply to all	IP ranges: 0.0.0.0/0	tcp udp icmp	Allow	1000	Off	-	-

This shows the custom mode network with all the firewall rules and the region.



The screenshot shows the 'VPC networks' section of the Google Cloud Platform interface. It lists various networks across different regions:

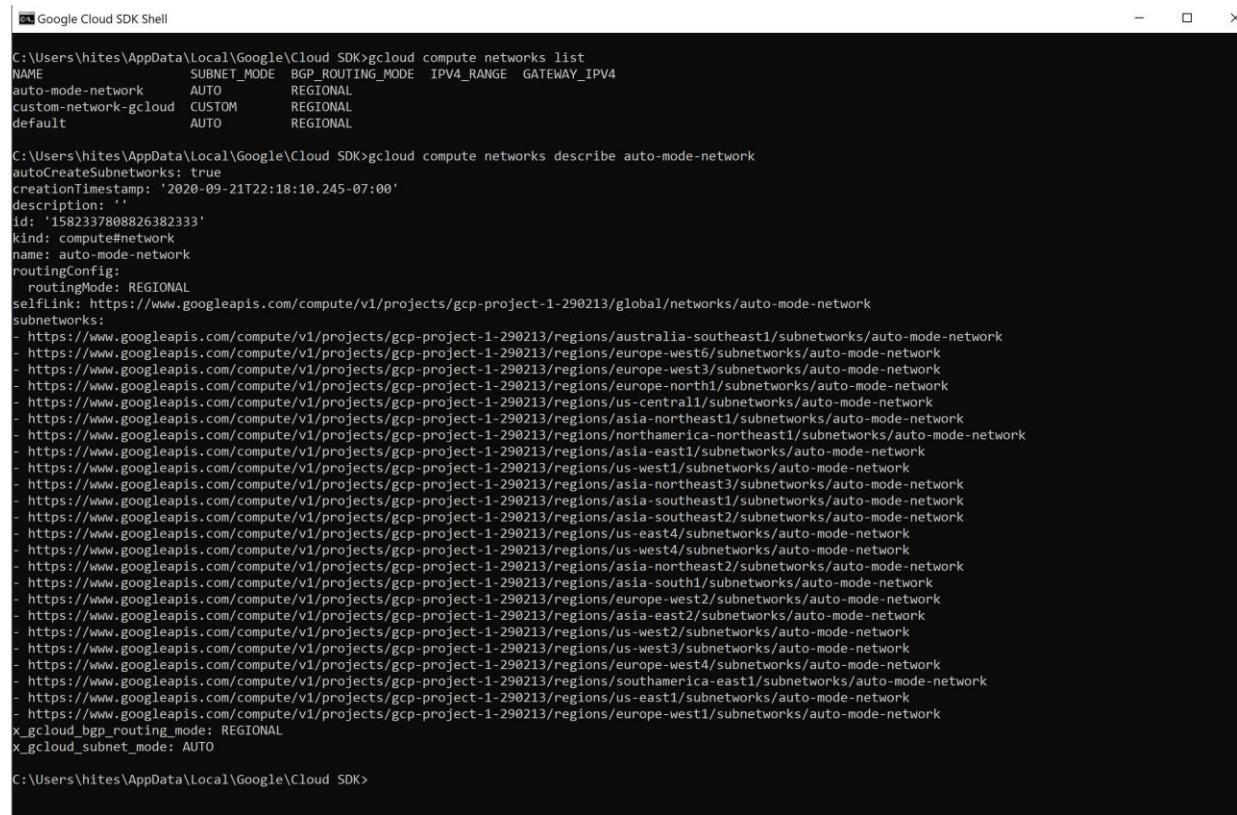
Region	Network Name	Subnet Creation Mode	IP Range	Last Hit
europe-north1	auto-mode-network	auto-mode-network	10.166.0.0/20	10.166.0.1
us-west2	auto-mode-network	auto-mode-network	10.168.0.0/20	10.168.0.1
asia-east2	auto-mode-network	auto-mode-network	10.170.0.0/20	10.170.0.1
europe-west6	auto-mode-network	auto-mode-network	10.172.0.0/20	10.172.0.1
asia-northeast2	auto-mode-network	auto-mode-network	10.174.0.0/20	10.174.0.1
asia-northeast3	auto-mode-network	auto-mode-network	10.178.0.0/20	10.178.0.1
us-west3	auto-mode-network	auto-mode-network	10.180.0.0/20	10.180.0.1
us-west4	auto-mode-network	auto-mode-network	10.182.0.0/20	10.182.0.1
asia-southeast2	auto-mode-network	auto-mode-network	10.184.0.0/20	10.184.0.1
default	0	Custom		1 Off
us-central1	default	Auto	10.128.0.0/20	10.128.0.1

2. Viewing networks

Viewing the VPC's and legacy network in the projects. For VPC's, we can view the information of the subnets and their subnet creation mode.

gcloud compute networks list – lists all the networks created. Here there are 3 networks with 1 default network and the other 2 networks being the auto mode and custom mode network created earlier.

gcloud compute networks describe auto-mode-network – describes a single network in detail showing the creation time, routing configuration and the subnetwork details for that network.



```
Google Cloud SDK Shell

C:\Users\hites\AppData\Local\Google\Cloud SDK>gcloud compute networks list
NAME          SUBNET_MODE  BGP_ROUTING_MODE  IPV4_RANGE   GATEWAY_IPV4
auto-mode-network  AUTO        REGIONAL
custom-network-gcloud  CUSTOM      REGIONAL
default        AUTO        REGIONAL

C:\Users\hites\AppData\Local\Google\Cloud SDK>gcloud compute networks describe auto-mode-network
autoCreateSubnetworks: true
creationTimestamp: '2020-09-21T22:18:10.245-07:00'
description: ''
id: '1582337808826382333'
kind: compute#network
name: auto-mode-network
routingConfig:
  routingMode: REGIONAL
selfLink: https://www.googleapis.com/compute/v1/projects/gcp-project-1-290213/global/networks/auto-mode-network
subnetworks:
- https://www.googleapis.com/compute/v1/projects/gcp-project-1-290213/regions/australia-southeast1/subnetworks/auto-mode-network
- https://www.googleapis.com/compute/v1/projects/gcp-project-1-290213/regions/europe-west6/subnetworks/auto-mode-network
- https://www.googleapis.com/compute/v1/projects/gcp-project-1-290213/regions/europe-west3/subnetworks/auto-mode-network
- https://www.googleapis.com/compute/v1/projects/gcp-project-1-290213/regions/europe-north1/subnetworks/auto-mode-network
- https://www.googleapis.com/compute/v1/projects/gcp-project-1-290213/regions/us-central1/subnetworks/auto-mode-network
- https://www.googleapis.com/compute/v1/projects/gcp-project-1-290213/regions/us-northeast1/subnetworks/auto-mode-network
- https://www.googleapis.com/compute/v1/projects/gcp-project-1-290213/regions/northamerica-northeast1/subnetworks/auto-mode-network
- https://www.googleapis.com/compute/v1/projects/gcp-project-1-290213/regions/asia-east1/subnetworks/auto-mode-network
- https://www.googleapis.com/compute/v1/projects/gcp-project-1-290213/regions/us-west1/subnetworks/auto-mode-network
- https://www.googleapis.com/compute/v1/projects/gcp-project-1-290213/regions/asia-northeast3/subnetworks/auto-mode-network
- https://www.googleapis.com/compute/v1/projects/gcp-project-1-290213/regions/asia-southeast1/subnetworks/auto-mode-network
- https://www.googleapis.com/compute/v1/projects/gcp-project-1-290213/regions/asia-southeast2/subnetworks/auto-mode-network
- https://www.googleapis.com/compute/v1/projects/gcp-project-1-290213/regions/us-east4/subnetworks/auto-mode-network
- https://www.googleapis.com/compute/v1/projects/gcp-project-1-290213/regions/us-west4/subnetworks/auto-mode-network
- https://www.googleapis.com/compute/v1/projects/gcp-project-1-290213/regions/asia-northeast2/subnetworks/auto-mode-network
- https://www.googleapis.com/compute/v1/projects/gcp-project-1-290213/regions/asia-south1/subnetworks/auto-mode-network
- https://www.googleapis.com/compute/v1/projects/gcp-project-1-290213/regions/europe-west2/subnetworks/auto-mode-network
- https://www.googleapis.com/compute/v1/projects/gcp-project-1-290213/regions/asia-east2/subnetworks/auto-mode-network
- https://www.googleapis.com/compute/v1/projects/gcp-project-1-290213/regions/us-west2/subnetworks/auto-mode-network
- https://www.googleapis.com/compute/v1/projects/gcp-project-1-290213/regions/us-west3/subnetworks/auto-mode-network
- https://www.googleapis.com/compute/v1/projects/gcp-project-1-290213/regions/europe-west4/subnetworks/auto-mode-network
- https://www.googleapis.com/compute/v1/projects/gcp-project-1-290213/regions/southamerica-east1/subnetworks/auto-mode-network
- https://www.googleapis.com/compute/v1/projects/gcp-project-1-290213/regions/us-east1/subnetworks/auto-mode-network
- https://www.googleapis.com/compute/v1/projects/gcp-project-1-290213/regions/europe-west1/subnetworks/auto-mode-network
X_gcloud_bgp_routing_mode: REGIONAL
X_gcloud_subnet_mode: AUTO

C:\Users\hites\AppData\Local\Google\Cloud SDK>
```

3. Working with subnets

a. Listing subnets (GCloud)

Listing all the subnets which are part of a project to know the range of IP Addresses which we can use for the instance in a particular subnet as each VPC is sub-divided into subnets. It also gives the details about the names and the regions of the existing subnets i.e. in which region which VPC has what range of IP addresses.

```
C:\Users\hites\AppData\Local\Google\Cloud SDK>gcloud compute networks subnets list
NAME          REGION      NETWORK      RANGE
auto-mode-network us-central1 auto-mode-network 10.128.0.0/20
default        us-central1 default       10.128.0.0/20
auto-mode-network europe-west1 auto-mode-network 10.132.0.0/20
default        europe-west1 default       10.132.0.0/20
auto-mode-network us-west1   auto-mode-network 10.138.0.0/20
default        us-west1   default       10.138.0.0/20
auto-mode-network asia-east1  auto-mode-network 10.140.0.0/20
default        asia-east1  default       10.140.0.0/20
auto-mode-network us-east1   auto-mode-network 10.142.0.0/20
default        us-east1   default       10.142.0.0/20
auto-mode-network asia-northeast1 auto-mode-network 10.146.0.0/20
default        asia-northeast1 default       10.146.0.0/20
auto-mode-network asia-southeast1 auto-mode-network 10.148.0.0/20
default        asia-southeast1 default       10.148.0.0/20
auto-mode-network us-east4   auto-mode-network 10.150.0.0/20
default        us-east4   default       10.150.0.0/20
auto-mode-network australia-southeast1 auto-mode-network 10.152.0.0/20
default        australia-southeast1 default       10.152.0.0/20
auto-mode-network europe-west2   auto-mode-network 10.154.0.0/20
default        europe-west2   default       10.154.0.0/20
auto-mode-network europe-west3   auto-mode-network 10.156.0.0/20
default        europe-west3   default       10.156.0.0/20
auto-mode-network southamerica-east1 auto-mode-network 10.158.0.0/20
default        southamerica-east1 default       10.158.0.0/20
auto-mode-network asia-south1  auto-mode-network 10.160.0.0/20
default        asia-south1  default       10.160.0.0/20
auto-mode-network northamerica-northeast1 auto-mode-network 10.162.0.0/20
default        northamerica-northeast1 default       10.162.0.0/20
auto-mode-network europe-west4   auto-mode-network 10.164.0.0/20
default        europe-west4   default       10.164.0.0/20
auto-mode-network europe-north1  auto-mode-network 10.166.0.0/20
default        europe-north1  default       10.166.0.0/20
auto-mode-network us-west2   auto-mode-network 10.168.0.0/20
default        us-west2   default       10.168.0.0/20
auto-mode-network asia-east2  auto-mode-network 10.170.0.0/20
default        asia-east2  default       10.170.0.0/20
auto-mode-network europe-west6   auto-mode-network 10.172.0.0/20
default        europe-west6   default       10.172.0.0/20
auto-mode-network asia-northeast2 auto-mode-network 10.174.0.0/20
default        asia-northeast2 default       10.174.0.0/20
auto-mode-network asia-northeast3 auto-mode-network 10.178.0.0/20
default        asia-northeast3 default       10.178.0.0/20
auto-mode-network us-west3   auto-mode-network 10.180.0.0/20
default        us-west3   default       10.180.0.0/20
auto-mode-network us-west4   auto-mode-network 10.182.0.0/20
default        us-west4   default       10.182.0.0/20
auto-mode-network asia-southeast2 auto-mode-network 10.184.0.0/20
default        asia-southeast2 default       10.184.0.0/20
C:\Users\hites\AppData\Local\Google\Cloud SDK>
```

b. Describing a subnet (GCloud)

Describing a subnet gives detail information about the subnet such as primary IP Range, name of the network, region and any secondary IP ranges.

```
C:\Users\hites\AppData\Local\Google\Cloud SDK>gcloud compute networks subnets describe auto-mode-network --region=us-central1
creationTimestamp: '2020-09-21T22:18:18.978-07:00'
fingerprint: 3vPn4YkQJ5c=
gatewayAddress: 10.128.0.1
id: '5885204198223788021'
ipCidrRange: 10.128.0.0/20
kind: compute#subnetwork
name: auto-mode-network
network: https://www.googleapis.com/compute/v1/projects/gcp-project-1-290213/global/networks/auto-mode-network
privateIpGoogleAccess: false
purpose: PRIVATE
region: https://www.googleapis.com/compute/v1/projects/gcp-project-1-290213/regions/us-central1
selfLink: https://www.googleapis.com/compute/v1/projects/gcp-project-1-290213/regions/us-central1/subnetworks/auto-mode-network
C:\Users\hites\AppData\Local\Google\Cloud SDK>
```

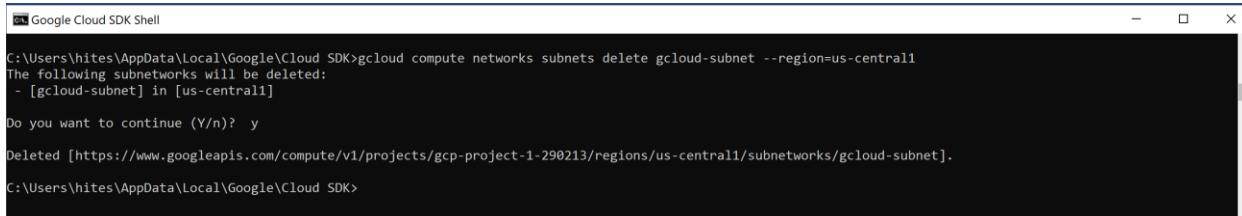
c. Adding subnets (GCloud)

We can create a new subnet in the given network with the name and Primary IP address range.

```
C:\Users\hites\AppData\Local\Google\Cloud SDK>gcloud compute networks subnets create gcloud-subnet --network=default --range=100.64.0.0/10 --region=us-central1
Created [https://www.googleapis.com/compute/v1/projects/gcp-project-1-290213/regions/us-central1/subnetworks/gcloud-subnet].
NAME      REGION      NETWORK      RANGE
gcloud-subnet us-central1 default 100.64.0.0/10
C:\Users\hites\AppData\Local\Google\Cloud SDK>
```

d. Deleting subnets (GCloud)

Deleting the subnets manually requires all the resources using these subnets to be deleted first such as delete VM's, internal firewall rules etc. Here there are no resources which are using this subnet so we can directly delete this subnet without requiring to delete any dependencies before deleting the subnet.

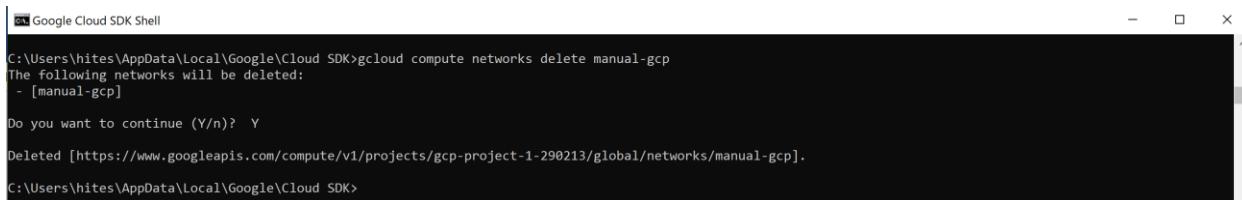


```
Google Cloud SDK Shell
C:\Users\hites\AppData\Local\Google\Cloud SDK>gcloud compute networks subnets delete gcloud-subnet --region=us-central1
The following subnetworks will be deleted:
- [gcloud-subnet] in [us-central1]
Do you want to continue (Y/n)?
Deleted [https://www.googleapis.com/compute/v1/projects/gcp-project-1-290213/regions/us-central1/subnetworks/gcloud-subnet].
C:\Users\hites\AppData\Local\Google\Cloud SDK>
```

4. Modifying networks

a. Deleting a network (GCloud)

If a network is not being used, we can delete it. If there are certain resources using this network, we would need to delete all the resources using this network first in order to be able to delete the network.



```
Google Cloud SDK Shell
C:\Users\hites\AppData\Local\Google\Cloud SDK>gcloud compute networks delete manual-gcp
The following networks will be deleted:
- [manual-gcp]
Do you want to continue (Y/n)?
Deleted [https://www.googleapis.com/compute/v1/projects/gcp-project-1-290213/global/networks/manual-gcp].
C:\Users\hites\AppData\Local\Google\Cloud SDK>
```

B. Complete the following sub-modules in *Using firewall rules*:

1. Creating Firewall Rules (Console)

An example of the firewall rule created with the configuration to allow Ingress traffic from the selected IP's.

The screenshot shows the 'Create a firewall rule' dialog in the Google Cloud Platform. The 'Name' field is set to 'firewalltest'. Under 'Logs', 'On' is selected. The 'Network' dropdown is set to 'default'. The 'Priority' is set to '600'. Under 'Direction of traffic', 'Ingress' is selected. The 'Action on match' is set to 'Allow'. The 'Targets' section shows 'All instances in the network'. The 'Source filter' is set to 'IP ranges' with a value of '0.0.0.0/0'. The 'Protocols and ports' section has 'Allow all' selected.

The screenshot shows the 'Firewall' list page in the Google Cloud Platform. It displays a table of existing firewall rules. One rule, 'firewalltest1', is visible with the following details: Type: Ingress, Targets: Apply to all, IP ranges: 0.0.0.0/0, Action: Allow, Priority: 1000, Network: custom-network-gcloud, Log: Off. Other rules listed include 'allow-health-check', 'default-allow-ssh', 'default-allow-internal', etc.

2. Configuration examples - Recreate sample network configurations in the scenarios listed below

- Example 1: Deny all ingress TCP connections except those to port 80 from subnet1

Firewall rule denies all the ingress traffic coming to port 80 from the subnet1 with a priority of 1000 using the Gcloud Command line.

```
C:\Users\hites\AppData\Local\Google\Cloud SDK>gcloud compute firewall-rules create example1-deny-access-subnet1 --network auto-mode-network --action deny
--direction ingress --rules tcp --source-ranges 0.0.0.0/0 --priority 1000 --target-tags webserver
Creating firewall...Created [https://www.googleapis.com/compute/v1/projects/gcp-project-1-290213/global/firewalls/example1-deny-access-subnet1].
Creating firewall...done.
NAME          NETWORK      DIRECTION  PRIORITY ALLOW DENY DISABLED
example1-deny-access-subnet1  auto-mode-network  INGRESS    1000     tcp  False
```

Firewall to accept the TCP Ingres traffic on the port 80 from subnet1 with priority 50 using Gcloud Command line. This implementation will allow TCP Ingres traffic to port 80 from subnet1 as a result of the priorities set for the rules created. This links these firewall rules created to the specified network auto-mode-network.

```
C:\Users\hites\AppData\Local\Google\Cloud SDK>gcloud compute firewall-rules create example1-allow-access-port80-from-subnet1-ingress --network auto-mode-network --action allow --direction ingress --rules tcp:80 --source-ranges 10.240.10.0/24 --priority 50 --target-tags webserver
Creating firewall...Created [https://www.googleapis.com/compute/v1/projects/gcp-project-1-290213/global/firewalls/example1-allow-access-port80-from-subnet1-ingress].
Creating firewall...done.
NAME          NETWORK      DIRECTION  PRIORITY ALLOW  DENY  DISABLED
example1-allow-access-port80-from-subnet1-ingress  auto-mode-network  INGRESS    50       tcp:80  False
C:\Users\hites\AppData\Local\Google\Cloud SDK>
```

b. Example 2: Deny all egress TCP connections except those to port 80 of vm1

Firewall rule denies all the egress traffic coming to port 80 from the vm1 with a priority of 1000 using the Gcloud Command line.

```
C:\Users\hites\AppData\Local\Google\Cloud SDK>gcloud compute firewall-rules create example2-deny-all-access-egress --network auto-mode-network --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/gcp-project-1-290213/global/firewalls/example2-deny-all-access-egress].
Creating firewall...done.
NAME          NETWORK      DIRECTION  PRIORITY ALLOW  DENY  DISABLED
example2-deny-all-access-egress  auto-mode-network  EGRESS     1000    tcp   False
C:\Users\hites\AppData\Local\Google\Cloud SDK>
```

Firewall to accept the TCP Egress traffic on the port 80 from vm1 with priority 60 using Gcloud Command line. This implementation will allow TCP egress traffic to port 80 from vm1 as a result of the priorities set for the rules created. This links these firewall rules created to the specified network auto-mode-network.

```
C:\Users\hites\AppData\Local\Google\Cloud SDK>gcloud compute firewall-rules create example2-vm1-allow-egress-port80-tcp --network auto-mode-network --action allow --direction egress --rules tcp:80 --destination-ranges 192.168.1.2/32 --priority 60
Creating firewall...Created [https://www.googleapis.com/compute/v1/projects/gcp-project-1-290213/global/firewalls/example2-vm1-allow-egress-port80-tcp].
Creating firewall...done.
NAME          NETWORK      DIRECTION  PRIORITY ALLOW  DENY  DISABLED
example2-vm1-allow-egress-port80-tcp  auto-mode-network  EGRESS     60       tcp:80  False
C:\Users\hites\AppData\Local\Google\Cloud SDK>
```

c. Example 3: Allow egress TCP connections to port 443 of an external host

Firewall rule created to allow all the TCP egress traffic to port 443 from an external host using the Console. This links this firewall rule to the network auto-mode-network with the priority as 70 as specified in the below Console configurations.

d. Example 4: Allow SSH connections from vm2 to vm1

Firewall rule created to allow SSH connection traffic from vm2 to vm1 on the default port of SSH which is 22 for the auto-mode-network using the gcloud command line.

```
C:\Users\hites\AppData\Local\Google\Cloud SDK>gcloud compute firewall-rules create example4-vm1-tcp-ssh-to-vm2-ingress --network auto-mode-network --action allow --direction ingress --rules tcp:22 --source-tags database --priority 80 --target-tags webserver
Creating firewall...[https://www.googleapis.com/compute/v1/projects/gcp-project-1-290213/global/firewalls/example4-vm1-tcp-ssh-to-vm2-ingress].
Creating firewall...done.
NAME          NETWORK      DIRECTION  PRIORITY ALLOW DENY DISABLED
example4-vm1-tcp-ssh-to-vm2-ingress  auto-mode-network  INGRESS    80     tcp:22  False

C:\Users\hites\AppData\Local\Google\Cloud SDK>
```

Name	Type	Targets	Filters	Protocols / ports	Action	Priority	Network	Logs	Hit count	Last hit	insights
example1-allow-access-port80-from-subnet1-ingress	Ingress	webservice	IP ranges: 10.240.10.0/24	tcp:80	Allow	50	auto-mode-network	Off	—	—	
example2-vm1-allow-egress-port80-tcp	Egress	Apply to all	IP ranges: 192.168.1.2/32	tcp:80	Allow	60	auto-mode-network	Off	—	—	
example3-vm1-allow-egress-tcp-443-to-192.0.2.5	Egress	webservice	IP ranges: 192.0.2.5/32	tcp:443	Allow	70	auto-mode-network	Off	—	—	
example4-vm1-tcp-ssh-to-vm2-ingress	Ingress	webservice	Tags: database	tcp:22	Allow	80	auto-mode-network	Off	—	—	
firewalltest	Ingress	Apply to all	IP ranges: 0.0.0.0/0	all	Allow	600	default	Off	—	—	
example1-deny-all-access-egress	Egress	Apply to all	IP ranges: 0.0.0.0/0	tcp	Deny	1000	auto-mode-network	Off	—	—	
example1-deny-all-access-ingress	Ingress	webservice	IP ranges: 0.0.0.0/0	tcp	Deny	1000	auto-mode-network	Off	—	—	
example1-deny-access-subnet1	Ingress	Apply to all	IP ranges: 0.0.0.0/0	tcp	Allow	1000	custom-network:gcloud	Off	—	—	
allow-health-check	Ingress	Apply to all	IP ranges: 130.211.0.0/22, 35.191.0.0/16	tcp:80	Allow	1000	default	Off	—	—	
default-allow-https	Ingress	http-server	IP ranges: 0.0.0.0/0	tcp:80	Allow	1000	default	Off	—	—	
default-allow-https	Ingress	https-server	IP ranges: 0.0.0.0/0	tcp:443	Allow	1000	default	Off	—	—	
sqlservermale	Ingress	Apply to all	IP ranges: 0.0.0.0/0	tcp:1433	Allow	1000	default	Off	—	—	
auto-mode-network-allow-icmp	Ingress	Apply to all	IP ranges: 0.0.0.0/0	icmp	Allow	65534	auto-mode-network	Off	—	—	
auto-mode-network-allow-ssh	Ingress	Apply to all	IP ranges: 0.0.0.0/0	tcp:22	Allow	65534	auto-mode-network	Off	—	—	
default-allow-icmp	Ingress	Apply to all	IP ranges: 0.0.0.0/0	tcp:65535	Allow	65534	default	Off	—	—	
default-allow-internal	Ingress	Apply to all	IP ranges: 10.128.0.0/9	tcp:65535	Allow	65534	default	Off	—	—	
default-allow-icmp	Ingress	Apply to all	IP ranges: 0.0.0.0/0	tcp:3389	Allow	65534	default	Off	—	—	
default-allow-rdp	Ingress	Apply to all	IP ranges: 0.0.0.0/0	tcp:22	Allow	65534	default	Off	—	—	
default-allow-ssh	Ingress	Apply to all	IP ranges: 0.0.0.0/0	tcp:22	Allow	65534	default	Off	—	—	