

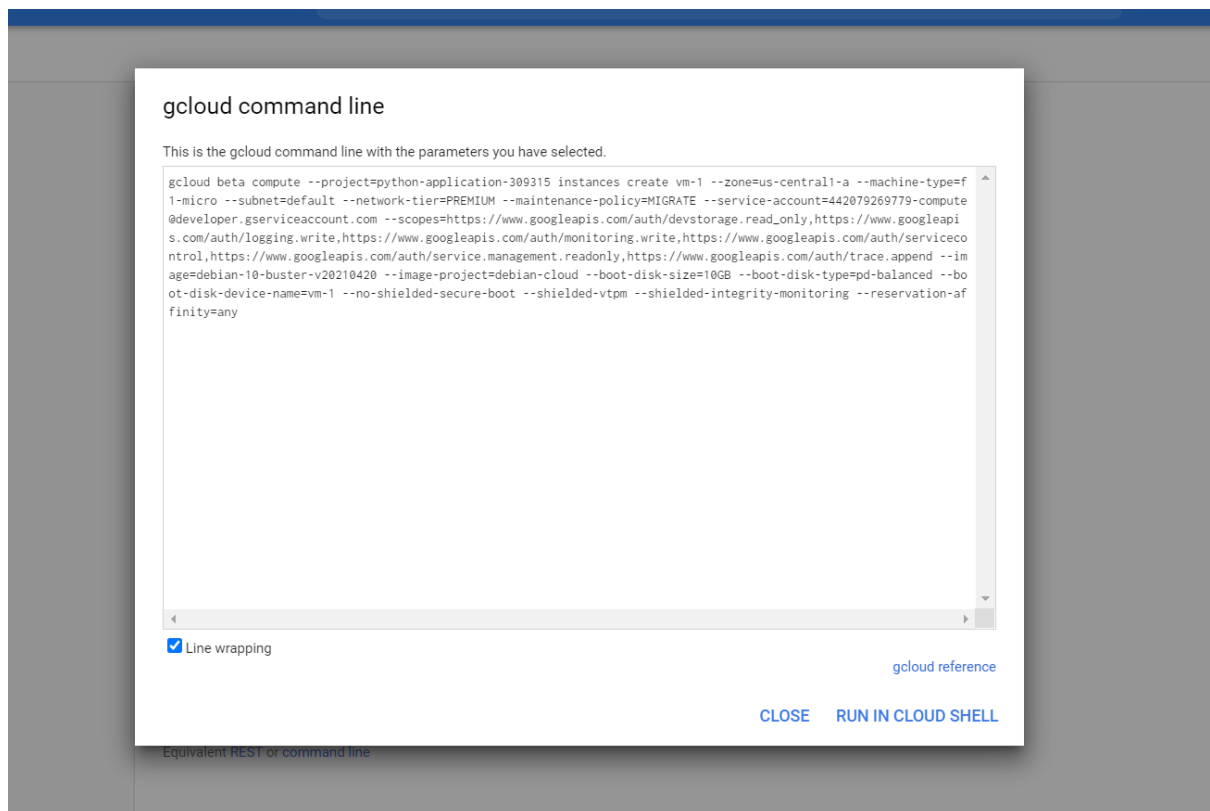
Yogeshwaran s

Case study 9

Module 9: Google Cloud Platform APIs & Development Services

Step 1:

she must find the command to create vm which is from comment line on creation of vm



Step 2:

She must copy the line to a note pad and remove the project id so that she can use this script for a create all instances and any project

```
*Untitled - Notepad
File Edit Format View Help
gcloud beta compute --project=python-application-309315 instances create vm-1 --zone=us-centra
```

Step 3:

Add command to add another vm with same settings

```
*Untitled - Notepad
File Edit Format View Help
gcloud beta compute instances create vm-1 vm-2 --zone=us-central1-a --machine-type=f1-micro --
```

Step 4:

She then creates a firewall rule to all http

Google Cloud Platformpython-applicationSearch products and resources

VPC network

VPC networks

External IP addresses

Bring your own IP

Firewall

Routes

VPC network peering

Shared VPC

Serverless VPC access

Packet mirroring

Create a firewall rule

Name *allow-http-test

Description

Logs

Turning on firewall logs can generate a large number of logs which can increase costs in Stackdriver. [Learn more](#)

☐ On

☒ Off

Network *default

Priority *1000

CHECK PRIORITY OF OTHER FIREWALL RULES

Direction of traffic

☒ Ingress

☐ Egress

Action on match

☒ Allow

☐ Deny

Targets

All instances in the network

<https://console.cloud.google.com/networking?project=python-application-309315>

Targets
All instances in the network

Source filter
IP ranges

Source IP ranges *
0.0.0.0/0 ⓘ for example, 0.0.0.0/0, 192.168.2.0/24 ⓘ

Second source filter
None

Protocols and ports ⓘ

☐ Allow all

☒ Specified protocols and ports

☒ tcp : 80,22

☐ udp : all

☐ Other protocols

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

▼ **DISABLE RULE**

CREATE **CANCEL**

Step 5:

Cope the code from commend line (do not create)

Create a firewall rule

Source filter
IP ranges

Source IP ranges
0.0.0.0/0 ⓘ

Second source filter
None

Protocols and ports
☒ Allow all
☒ Specified protocols and ports

☒ tcp :
☐ udp :
☐ Other protocols

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

▼ **DISABLE RULE**

CREATE **CANCEL**

Equivalent: REST **command line**

gcloud command line

This is the gcloud command line with the parameters you have selected. [gcloud reference](#)

```
gcloud compute --project=python-application-309315 firewall-rules create allow-http-test --direction=INGRESS --priority=1000 --network=default --action=ALLOW --rules=tcp:80,tcp:22 --source-ranges=0.0.0.0/0
```

☒ Line wrapping

[RUN IN CLOUD SHELL](#) [CLOSE](#)

Step- 6

Remove the project id from here also

```
gcloud beta compute instances create vm-1 vm-2 --zone=us-central1-a --machine-type=f1-micro --
subnet=default --network-tier=PREMIUM --maintenance-policy=MIGRATE --service-account=442079269779-
compute@developer.gserviceaccount.com --
scopes=https://www.googleapis.com/auth/devstorage.read_only,https://www.googleapis.com/auth/logging.writ
e,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 --
image=debian-10-buster-v20210420 --image-project=debian-cloud --boot-disk-size=10GB --boot-disk-
type=pd-balanced --boot-disk-device-name=vm-1 --no-shielded-secure-boot --shielded-vtpm --shielded-
integrity-monitoring --reservation-affinity=any
```

```
gcloud compute firewall-rules create allow-http-test --direction=INGRESS --priority=1000 --
network=default --action=ALLOW --rules=tcp:80,tcp:22 --source-ranges=0.0.0.0/0
```

Step-7

Create a script file on gcloud shell with the commends that she copied

```
yogibca62@cloudshell:~ (python-application-309315) $ ls
GCP_PYTHON my_app new.sh node-bulletin-board python-docs-samples README-cloudshell.txt
yogibca62@cloudshell:~ (python-application-309315) $ nano test1.sh
yogibca62@cloudshell:~ (python-application-309315) $ ls
GCP_PYTHON my_app new.sh node-bulletin-board python-docs-samples README-cloudshell.txt test1.sh
yogibca62@cloudshell:~ (python-application-309315) $
```

Step – 8

Execute the test1.sh script

```
GCP_PYTHON my_app new.sh node-bulletin-board python-docs-samples README-cloudshell.txt test1.sh
yogibca62@cloudshell:~ (python-application-309315) $ . test1.sh
Created [https://www.googleapis.com/compute/beta/projects/python-application-309315/zones/us-central1-a/instances/vm-1].
Created [https://www.googleapis.com/compute/beta/projects/python-application-309315/zones/us-central1-a/instances/vm-2].
NAME    ZONE    MACHINE TYPE  PREEMPTIBLE  INTERNAL IP  EXTERNAL IP  STATUS
vm-1    us-central1-a  f1-micro      10.128.0.5   34.69.153.134  RUNNING
vm-2    us-central1-a  f1-micro      10.128.0.6   34.72.186.204  RUNNING
Creating firewall...Created [https://www.googleapis.com/compute/v1/projects/python-application-309315/global/firewalls/allow-
http-test].
Creating firewall...done.
NAME    NETWORK  DIRECTION  PRIORITY  ALLOW  DENY  DISABLED
allow-http-test  default  INGRESS    1000      tcp:80,tcp:22  False
yogibca62@cloudshell:~ (python-application-309315) $
```

Script is successfully created and executed, from the commends from the script,

There are 2 vm created

Google Cloud Platform python-application Search products and resources

Compute Engine VM instances CREATE INSTANCE IMPORT VM REFRESH START / RESUME STOP OPERATIONS SHOW INFO PANEL LEARN

Virtual machines

- VM Instances
- Instance templates
- Sole-tenant nodes
- Machine images
- TPUs
- Migrate for Compute Engi...
- Committed use discounts

Storage

- Disks
- Snapshots
- Images

INSTANCES INSTANCE SCHEDULE

Filter Enter property name or value

		Name	Zone	Recommendations	In use by	Internal IP	External IP	Connect
<input type="checkbox"/>	●	vm-1	us-central1-a			10.128.0.5 (nic0)	34.69.153.134	SSH
<input type="checkbox"/>	●	vm-2	us-central1-a			10.128.0.6 (nic0)	34.72.186.204	SSH

Related Actions DISMISS

- View Billing Report**
View and manage your Compute Engine billing
- Monitor VMs**
View outlier VMs across metrics like CPU and Network
- Explore VM Logs**
View, search, analyze, and download VM instance logs
- Setup Firewall Rules**
Control traffic to and from a VM instance
- Patch Management**
Schedule patch updates and view patch compliance on VM instances

And 1 firewall rule also created

Filter Enter property name or value

	Name	Type	Targets	Filters	Protocols / ports	Action	Priority	Network	Logs	Hit count	Last hit
<input type="checkbox"/>	allow-http-test	Ingress	Apply to all	IP ranges: 0.0.0.0/0	tcp:80;tcp:22	Allow	1000	default	Off	—	—