Welcome

]

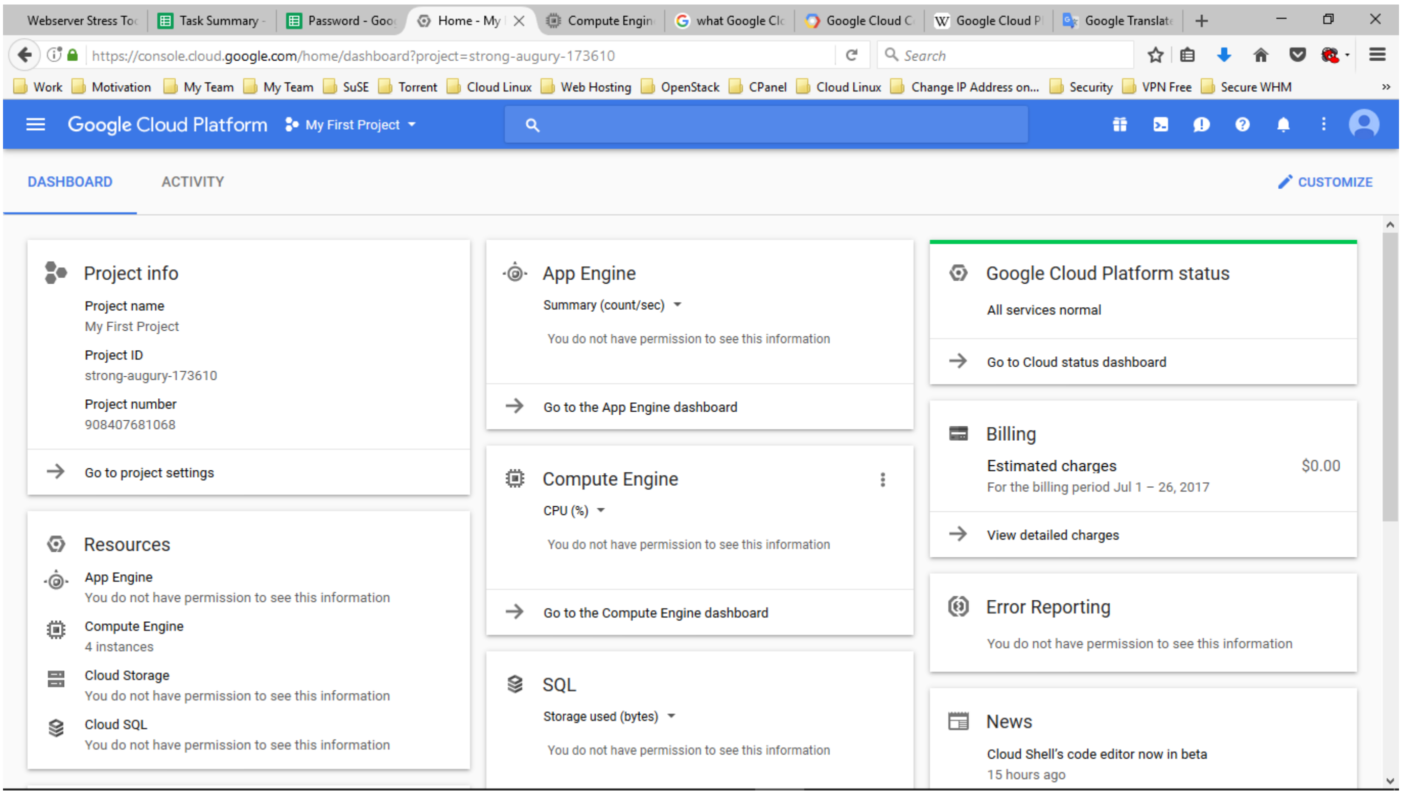
Table of Content

1/What is Google Cloud Platform

Google Cloud Platform, offered by Google, is a suite of cloud computing services that runs on the same infrastructure that Google uses internally for its end-user products, such as Google Search and YouTube. Alongside a set of management tools, it provides, a series of modular cloud services including computing, data storage, data analytics and machine learning.

You can access to Google Cloud Platform from this link https://cloud.google.com/

Here is the first view of Google Cloud Platform when you logged in



Project info
Project name
My First Project
Project ID
strong-augury-173610
Project number
908407681068
Go to project settings

Resources
App Engine
You do not have permission to see this information
Compute Engine
4 instances
Cloud Storage
You do not have permission to see this information
Cloud SQL
You do not have permission to see this information

App Engine
Summary (count/sec)
You do not have permission to see this information
Go to the App Engine dashboard

Compute Engine
CPU (%)
You do not have permission to see this information
Go to the Compute Engine dashboard

SQL
Storage used (bytes)
You do not have permission to see this information

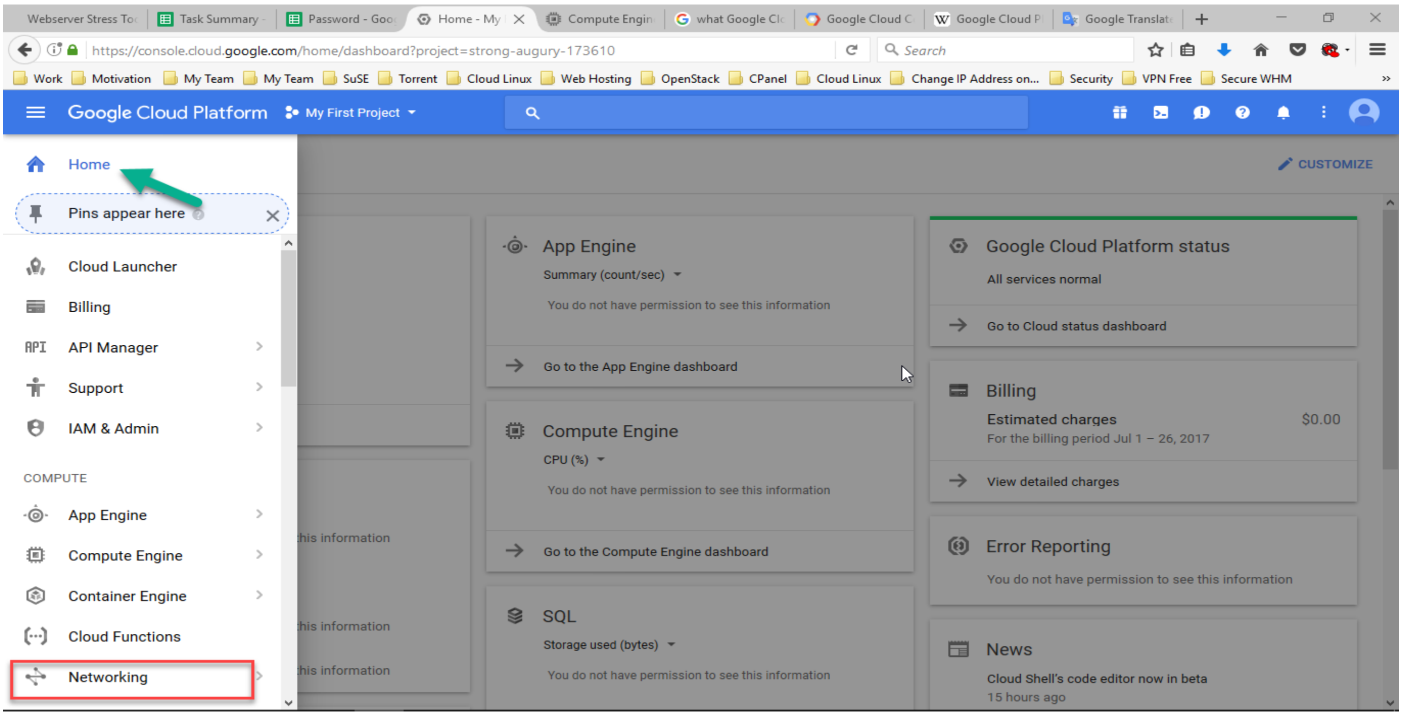
Google Cloud Platform status
All services normal
Go to Cloud status dashboard

Billing
Estimated charges $0.00
For the billing period Jul 1 – 26, 2017
View detailed charges

Error Reporting
You do not have permission to see this information

News
Cloud Shell's code editor now in beta
15 hours ago

2/ Networking



App Engine
Summary (count/sec)
You do not have permission to see this information
Go to the App Engine dashboard

Compute Engine
CPU (%)
You do not have permission to see this information
Go to the Compute Engine dashboard

SQL
Storage used (bytes)
You do not have permission to see this information

Google Cloud Platform status
All services normal
Go to Cloud status dashboard

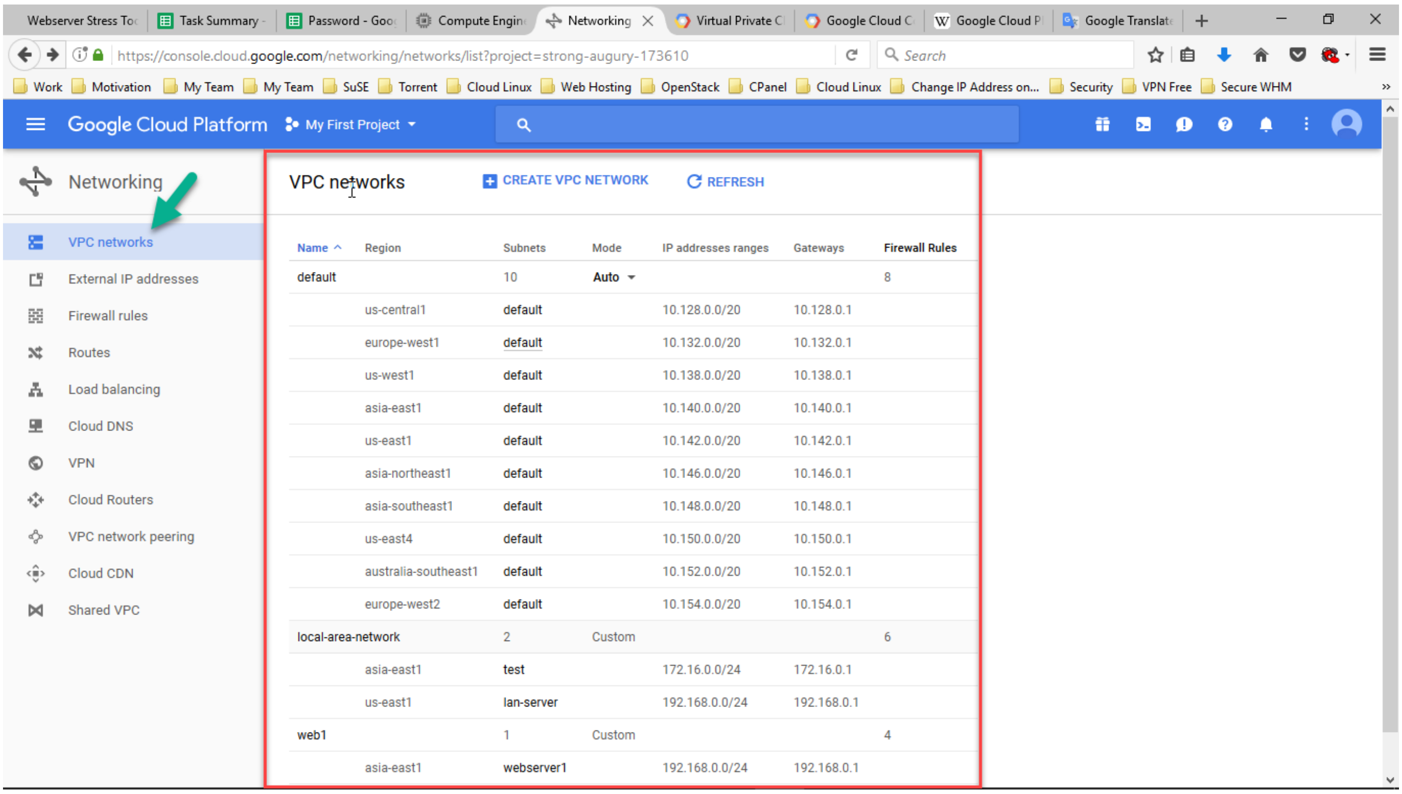
Billing
Estimated charges $0.00
For the billing period Jul 1 – 26, 2017
View detailed charges

Error Reporting
You do not have permission to see this information

News
Cloud Shell's code editor now in beta
15 hours ago

A/Virtual Private Cloud (VPC) Network

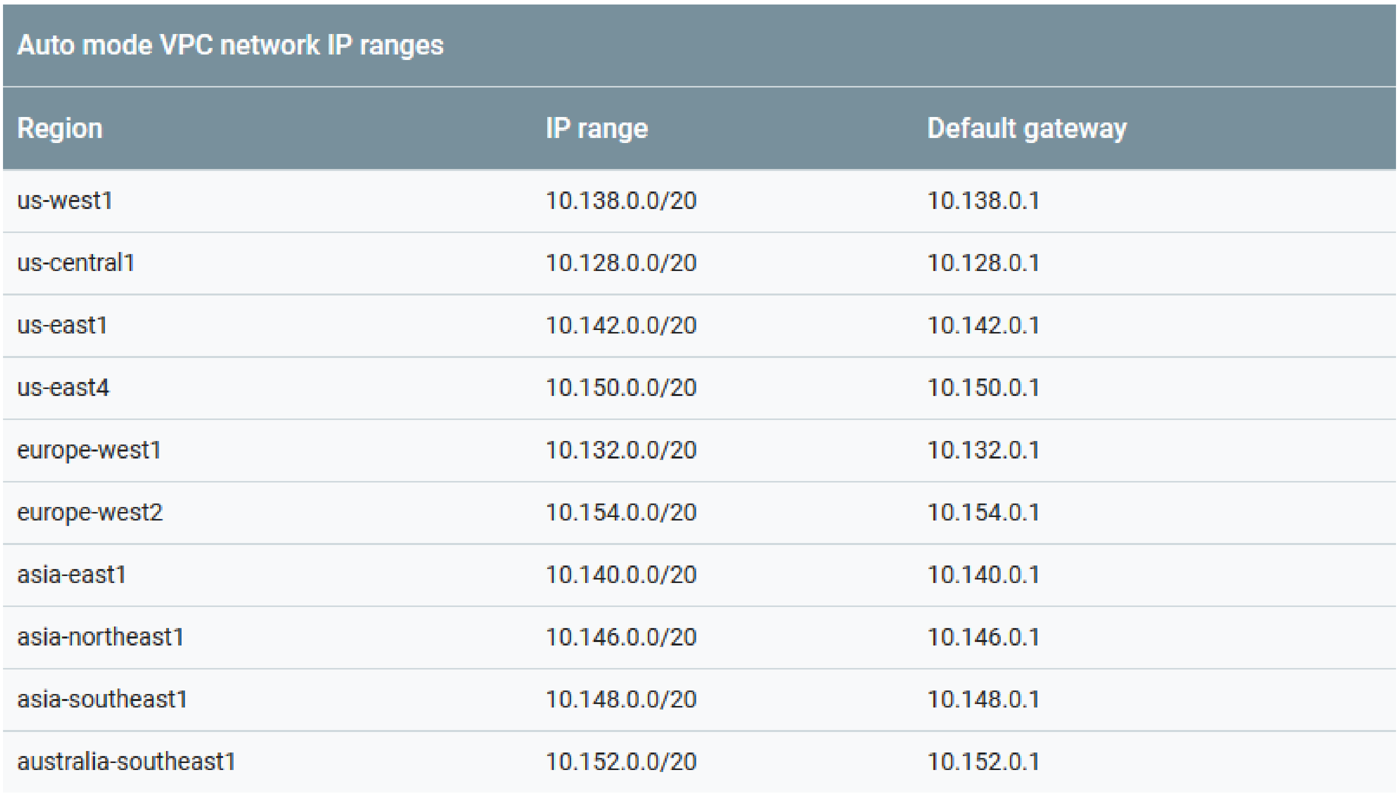
A Virtual Private Cloud (VPC) is a global private isolated virtual network partition that provides managed networking functionality for your Google Cloud Platform (GCP) resources.



Name	Region	Subnets	Mode	IP addresses ranges	Gateways	Firewall Rules
default		10	Auto			8
	us-central1	default		10.128.0.0/20	10.128.0.1	
	europe-west1	default		10.132.0.0/20	10.132.0.1	
	us-west1	default		10.138.0.0/20	10.138.0.1	
	asia-east1	default		10.140.0.0/20	10.140.0.1	
	us-east1	default		10.142.0.0/20	10.142.0.1	
	asia-northeast1	default		10.146.0.0/20	10.146.0.1	
	asia-southeast1	default		10.148.0.0/20	10.148.0.1	
	us-east4	default		10.150.0.0/20	10.150.0.1	
	australia-southeast1	default		10.152.0.0/20	10.152.0.1	
	europe-west2	default		10.154.0.0/20	10.154.0.1	
local-area-network		2	Custom			6
	asia-east1	test		172.16.0.0/24	172.16.0.1	
	us-east1	lan-server		192.168.0.0/24	192.168.0.1	
web1		1	Custom			4
	asia-east1	webserver1		192.168.0.0/24	192.168.0.1	

There are two types of VPC such as **Auto Mode VPC Network** and **Custom Mode VPC network.**

+Auto Mode VPC Network is a default network that start with a single subnet in each region with the ranges listed in the table



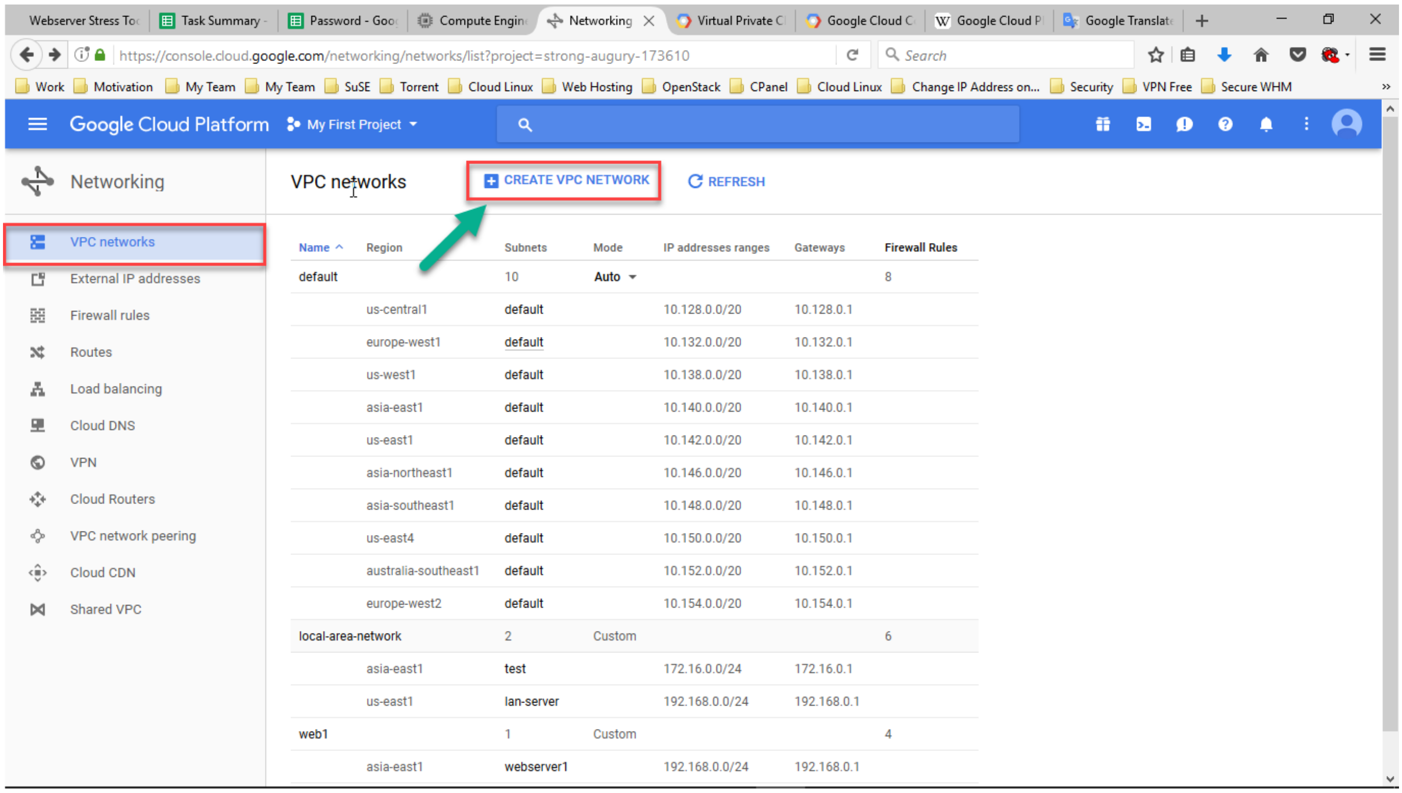
Auto mode VPC network IP ranges

Region	IP range	Default gateway
us-west1	10.138.0.0/20	10.138.0.1
us-central1	10.128.0.0/20	10.128.0.1
us-east1	10.142.0.0/20	10.142.0.1
us-east4	10.150.0.0/20	10.150.0.1
europe-west1	10.132.0.0/20	10.132.0.1
europe-west2	10.154.0.0/20	10.154.0.1
asia-east1	10.140.0.0/20	10.140.0.1
asia-northeast1	10.146.0.0/20	10.146.0.1
asia-southeast1	10.148.0.0/20	10.148.0.1
australia-southeast1	10.152.0.0/20	10.152.0.1

+**Custom Mode VPC network** do not start with any subnets. You must create the subnets manually. If you need different IP ranges or more than one subnet in a region, create a custom mode VPC network.

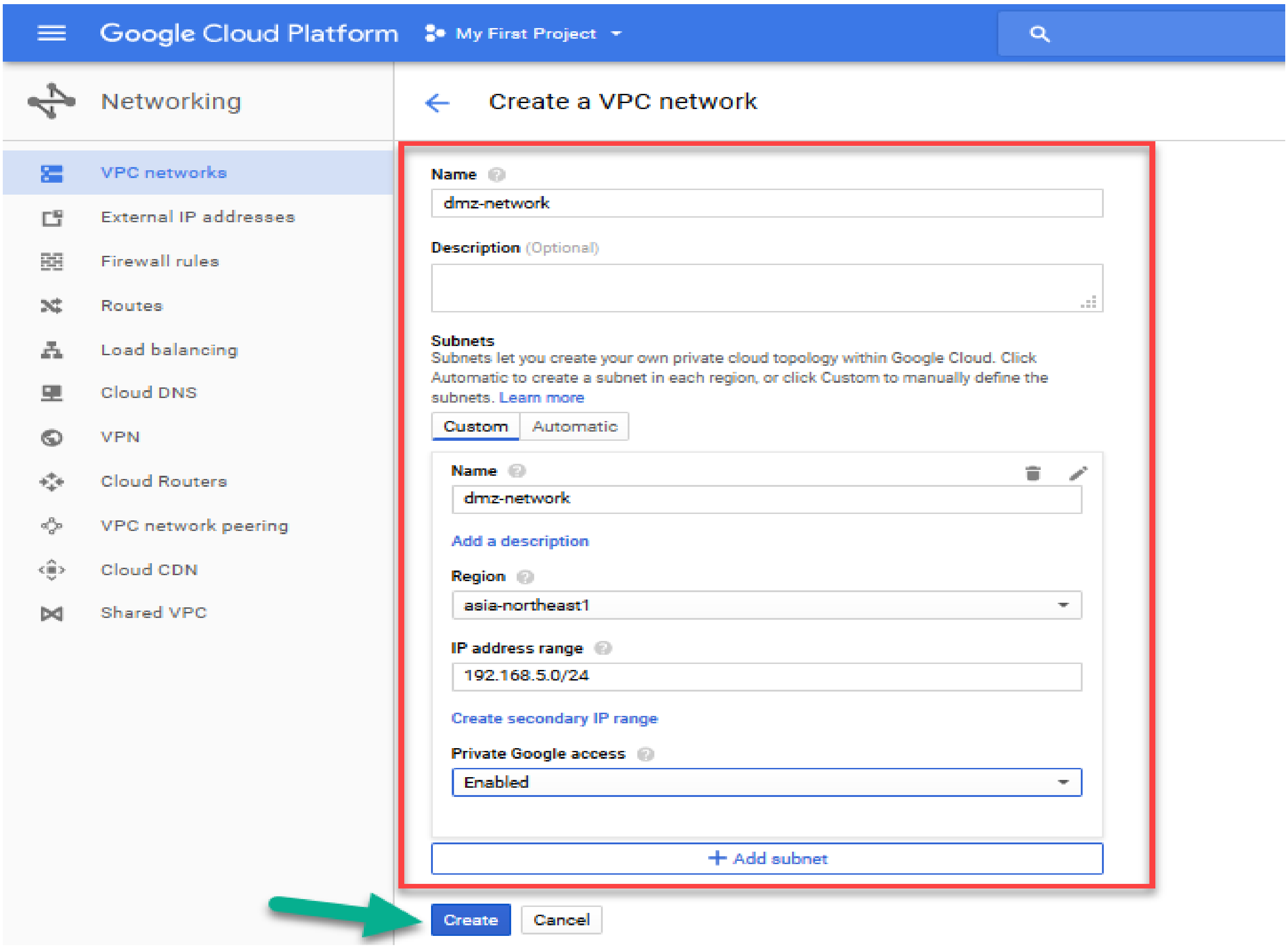
Here is the Demonstration how to create custom VPC Network

+Go to **Home**> **Networking**> VPC **Network** then click **CREATE VPC NETWORK**



VPC networks

Name	Region	Subnets	Mode	IP addresses ranges	Gateways	Firewall Rules
default		10	Auto			8
	us-central1	default		10.128.0.0/20	10.128.0.1	
	europe-west1	default		10.132.0.0/20	10.132.0.1	
	us-west1	default		10.138.0.0/20	10.138.0.1	
	asia-east1	default		10.140.0.0/20	10.140.0.1	
	us-east1	default		10.142.0.0/20	10.142.0.1	
	asia-northeast1	default		10.146.0.0/20	10.146.0.1	
	asia-southeast1	default		10.148.0.0/20	10.148.0.1	
	us-east4	default		10.150.0.0/20	10.150.0.1	
	australia-southeast1	default		10.152.0.0/20	10.152.0.1	
	europe-west2	default		10.154.0.0/20	10.154.0.1	
local-area-network		2	Custom			6
	asia-east1	test		172.16.0.0/24	172.16.0.1	
	us-east1	lan-server		192.168.0.0/24	192.168.0.1	
web1		1	Custom			4
	asia-east1	webserver1		192.168.0.0/24	192.168.0.1	



Create a VPC network

Name: dmz-network

Description (Optional)

Subnets

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. Learn more

Custom | Automatic

Name: dmz-network

Add a description

Region: asia-northeast1

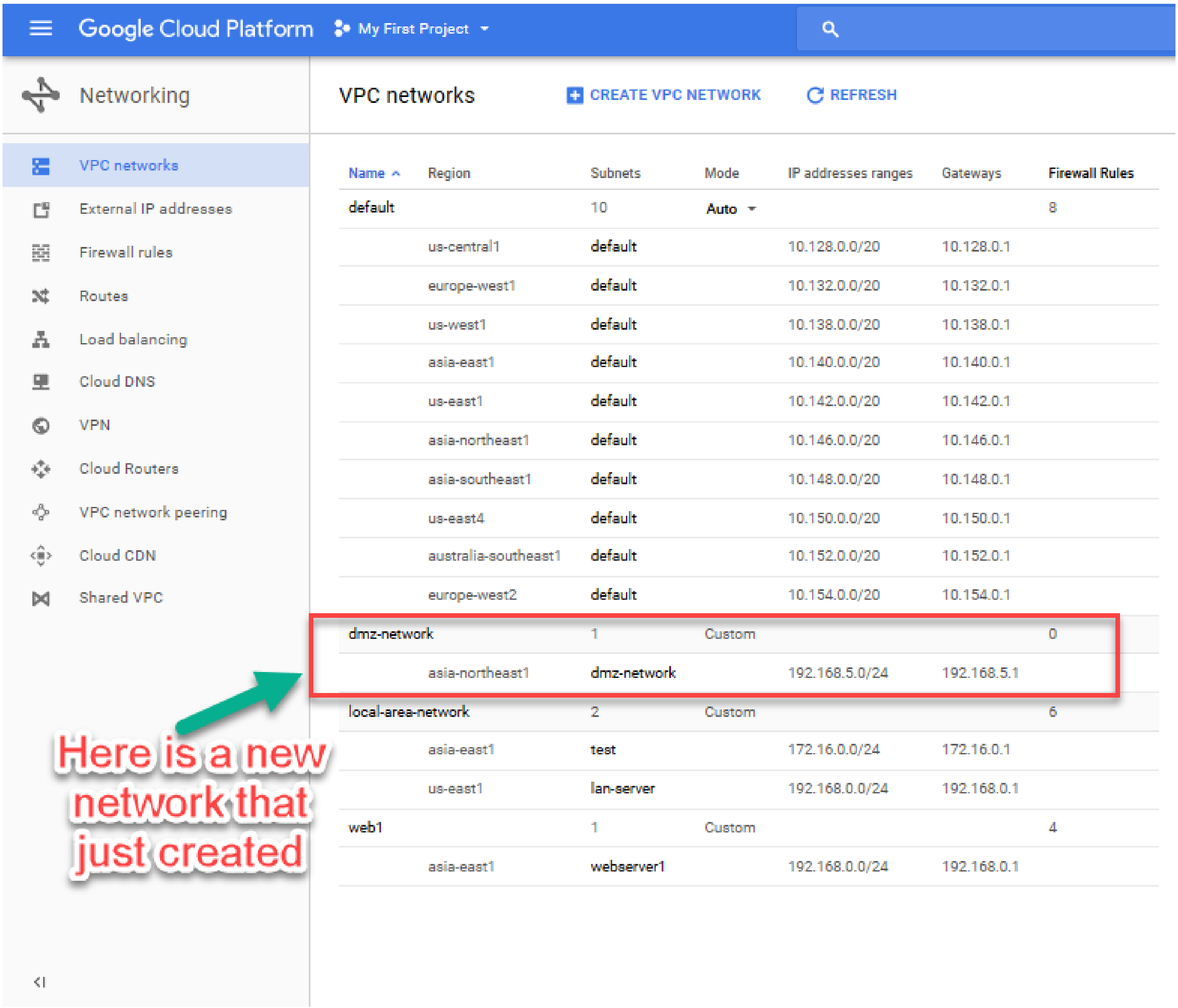
IP address range: 192.168.5.0/24

Create secondary IP range

Private Google access: Enabled

+ Add subnet

Create | Cancel



Name	Region	Subnets	Mode	IP addresses ranges	Gateways	Firewall Rules
default		10	Auto			8
	us-central1	default		10.128.0.0/20	10.128.0.1	
	europe-west1	default		10.132.0.0/20	10.132.0.1	
	us-west1	default		10.138.0.0/20	10.138.0.1	
	asia-east1	default		10.140.0.0/20	10.140.0.1	
	us-east1	default		10.142.0.0/20	10.142.0.1	
	asia-northeast1	default		10.146.0.0/20	10.146.0.1	
	asia-southeast1	default		10.148.0.0/20	10.148.0.1	
	us-east4	default		10.150.0.0/20	10.150.0.1	
	australia-southeast1	default		10.152.0.0/20	10.152.0.1	
	europe-west2	default		10.154.0.0/20	10.154.0.1	
dmz-network		1	Custom			0
	asia-northeast1	dmz-network		192.168.5.0/24	192.168.5.1	
local-area-network		2	Custom			6
	asia-east1	test		172.16.0.0/24	172.16.0.1	
	us-east1	lan-server		192.168.0.0/24	192.168.0.1	
web1		1	Custom			4
	asia-east1	webserver1		192.168.0.0/24	192.168.0.1	

Here is a new network that just created

For more detail please visit https://cloud.google.com/compute/docs/vpc/

B/Firewall Rule

Google Cloud Platform (GCP) Firewall Rules protects your virtual machine (VM) instances from unapproved connections, both inbound (`ingress`) and outbound (`egress`). You can create firewall rules to allow or deny specific connections based on a combination of IP addresses, ports, and protocol.

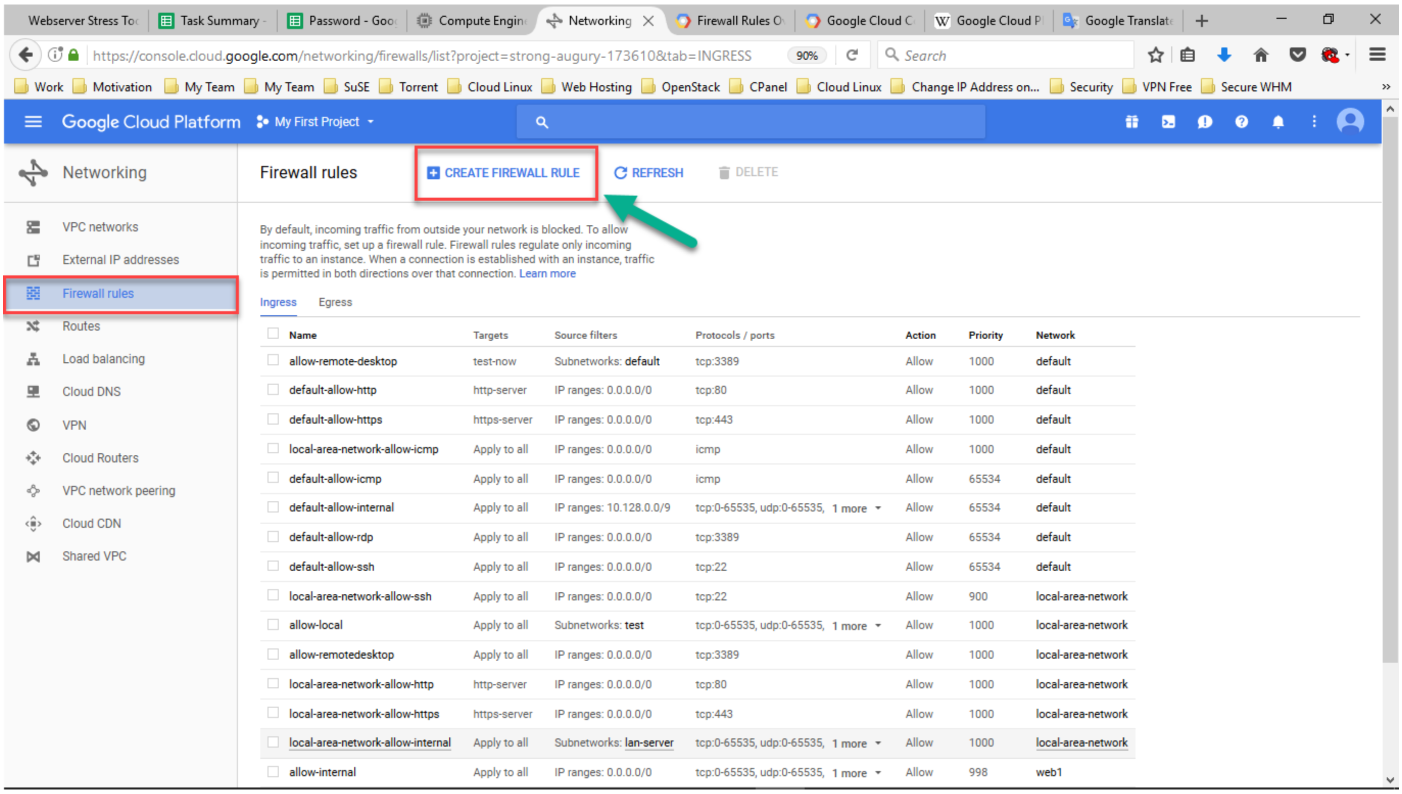
Note: If there are no firewall rules in a network or all rules were deleted, there is still an implied "Deny all" ingress rule and an implied "Allow all" egress rule for the network.

Note: You cannot specify both `allow` and `deny` in the same firewall rule. However, you can specify multiple overlapping or conflicting `allow` and `deny` firewall rules. If two rules conflict, then the rule with the highest `priority` is used. If both rules have the same `priority`, then the `deny` rule is used.

Note: By default, every rule governs every instance in the network. So, if a rule allows inbound traffic on a particular port, every instance in the network will be able to receive traffic on that port. However, you can assign `targetTags` to certain instances and assign the same tag to a firewall rule. In this way, you can apply that rule only to the instances with that tag. If no tag is specified, then the rule applies to all instances in the network.

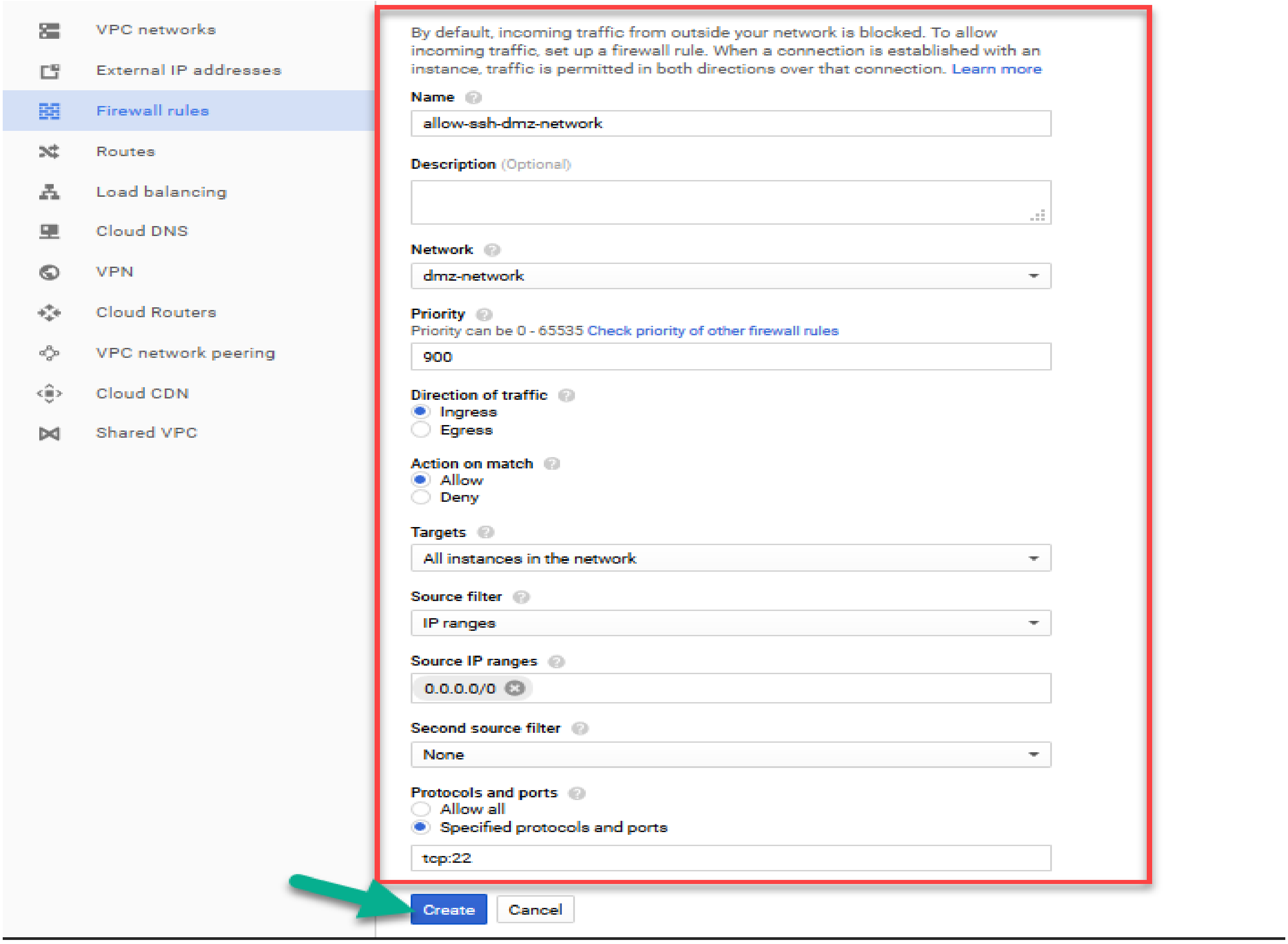
Note: Priority may be any integer value from `0` through `65535`, both inclusive. When unspecified, a priority value of `1000` is given. A lower priority "number" indicates higher priority, so a rule with a priority of `1` has a higher priority than, and is evaluated before, a rule with a priority of 2. If a connection matches conflicting rules with same priority, the deny policy takes precedence.

Example: I will create one firewall rule that allow all other networks can use ssh client remote into all instances in my network(dmz-network) with rule priority 900.



By default, incoming traffic from outside your network is blocked. To allow incoming traffic, set up a firewall rule. Firewall rules regulate only incoming traffic to an instance. When a connection is established with an instance, traffic is permitted in both directions over that connection. Learn more

Name	Targets	Source filters	Protocols / ports	Action	Priority	Network
allow-remote-desktop	test-now	Subnetworks: default	tcp:3389	Allow	1000	default
default-allow-http	http-server	IP ranges: 0.0.0.0/0	tcp:80	Allow	1000	default
default-allow-https	https-server	IP ranges: 0.0.0.0/0	tcp:443	Allow	1000	default
local-area-network-allow-icmp	Apply to all	IP ranges: 0.0.0.0/0	icmp	Allow	1000	default
default-allow-icmp	Apply to all	IP ranges: 0.0.0.0/0	icmp	Allow	65534	default
default-allow-internal	Apply to all	IP ranges: 10.128.0.0/9	tcp:0-65535, udp:0-65535, 1 more	Allow	65534	default
default-allow-rdp	Apply to all	IP ranges: 0.0.0.0/0	tcp:3389	Allow	65534	default
default-allow-ssh	Apply to all	IP ranges: 0.0.0.0/0	tcp:22	Allow	65534	default
local-area-network-allow-ssh	Apply to all	IP ranges: 0.0.0.0/0	tcp:22	Allow	900	local-area-network
allow-local	Apply to all	Subnetworks: test	tcp:0-65535, udp:0-65535, 1 more	Allow	1000	local-area-network
allow-remotedesktop	Apply to all	IP ranges: 0.0.0.0/0	tcp:3389	Allow	1000	local-area-network
local-area-network-allow-http	http-server	IP ranges: 0.0.0.0/0	tcp:80	Allow	1000	local-area-network
local-area-network-allow-https	https-server	IP ranges: 0.0.0.0/0	tcp:443	Allow	1000	local-area-network
local-area-network-allow-internal	Apply to all	Subnetworks: lan-server	tcp:0-65535, udp:0-65535, 1 more	Allow	1000	local-area-network
allow-internal	Apply to all	IP ranges: 0.0.0.0/0	tcp:0-65535, udp:0-65535, 1 more	Allow	998	web1



By default, incoming traffic from outside your network is blocked. To allow incoming traffic, set up a firewall rule. When a connection is established with an instance, traffic is permitted in both directions over that connection. Learn more

Name: allow-ssh-dmz-network

Description (Optional):

Network: dmz-network

Priority: Priority can be 0 - 65535 Check priority of other firewall rules: 900

Direction of traffic: ● Ingress ○ Egress

Action on match: ● Allow ○ Deny

Targets: All instances in the network

Source filter: IP ranges

Source IP ranges: 0.0.0.0/0

Second source filter: None

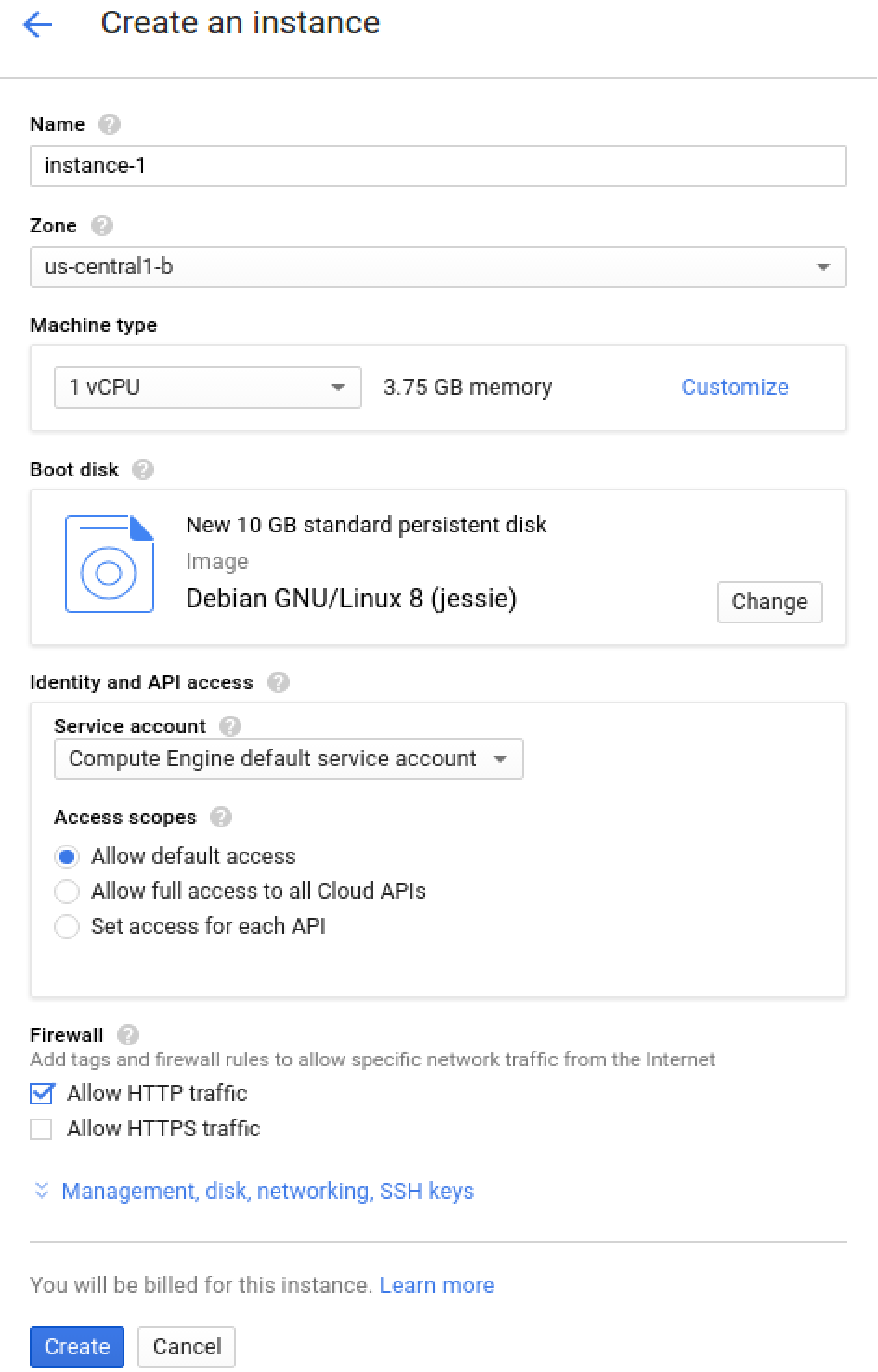
Protocols and ports: ○ Allow all ● Specified protocols and ports: tcp:22

For more detail about Firewall Rule please visit https://cloud.google.com/compute/docs/vpc/firewalls

3/ Compute Engine

A/VM Instance

1. In the **Cloud Platform Console**, go to the **VM Instances** page.
2. Click the **Create instance** button.
3. In the **Boot disk** section, click **Change** to begin configuring your boot disk.
4. In the **OS images** tab, choose **the Debian 8 image**.
5. Click **Select**.
6. In the **Firewall** section, select **Allow HTTP traffic**.
7. Click the **Create** button to create the instance.



Create an instance

Name: instance-1

Zone: us-central1-b

Machine type: 1 vCPU — 3.75 GB memory

Boot disk: New 10 GB standard persistent disk
Image: Debian GNU/Linux 8 (jessie)

Identity and API access

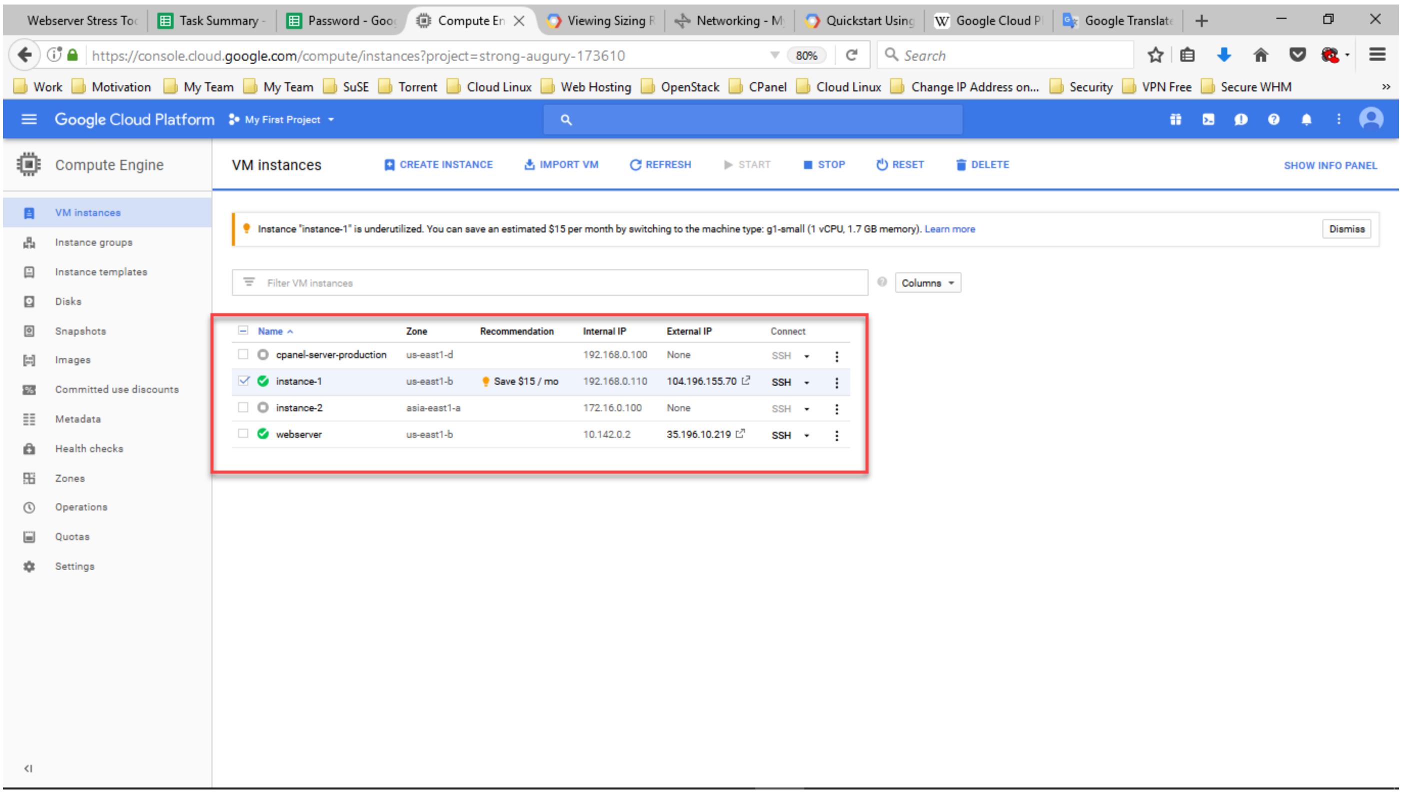
Service account: Compute Engine default service account

Access scopes
● Allow default access
○ Allow full access to all Cloud APIs
○ Set access for each API

Firewall
Add tags and firewall rules to allow specific network traffic from the Internet
☑ Allow HTTP traffic
□ Allow HTTPS traffic

You will be billed for this instance. Learn more

After you created VM instance, you can view them here:



Instance "instance-1" is underutilized. You can save an estimated $15 per month by switching to the machine type: g1-small (1 vCPU, 1.7 GB memory). Learn more

	Name	Zone	Recommendation	Internal IP	External IP	Connect
□	cpanel-server-production	us-east1-d		192.168.0.100	None	SSH
☑	instance-1	us-east1-b	Save $15 / mo	192.168.0.110	104.196.155.70	SSH
□	instance-2	asia-east1-a		172.16.0.100	None	SSH
□	webserver	us-east1-b		10.142.0.2	35.196.10.219	SSH

For more detail about Firewall Rule please visit https://cloud.google.com/compute/docs/instances/

B/Instance Group

You can create and manage groups of virtual machines (VM) instances so that you don't have to individually control each instance in your project. Compute Engine offers two different types of instance groups: **managed** and **unmanaged** instance groups.

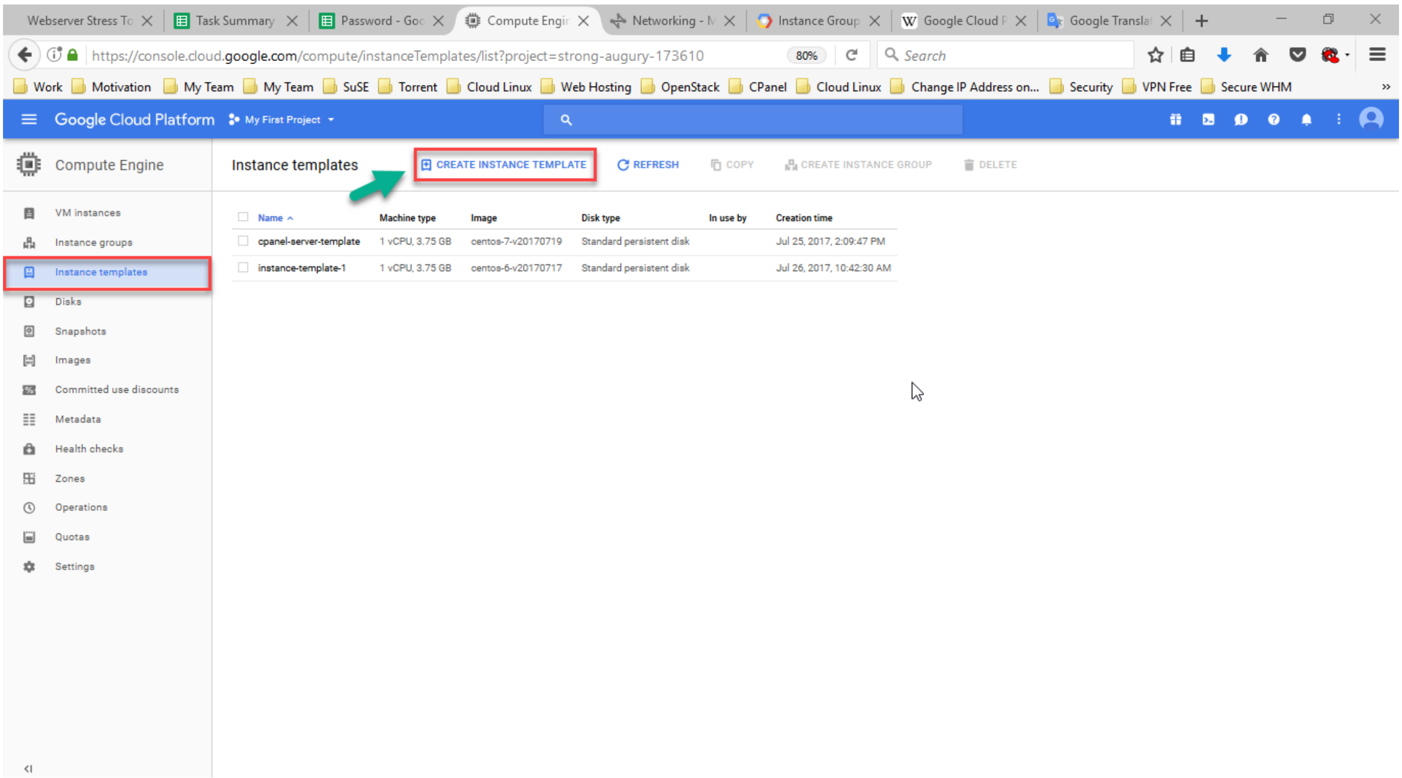
+**Manged Instance Group**: A managed instance group uses an instance template to create a group of identical instances. You control a managed instance group as a single entity.If you wanted to make changes to instances that are part of a managed instance group, you would make the change to the whole instance group.

+**Unmanaged Instance Group**: Unmanaged instance groups are groups of dissimilar instances that you can arbitrarily add and remove from the group. Unmanaged instance groups do not offer auto scaling, rolling update support, or the use of instance templates so Google recommends creating managed instance groups whenever possible. Use unmanaged instance groups only if you need to apply load balancing to your pre-existing configurations or to groups of dissimilar instances.

Note: Before you can create Instance Group, you must create instance template first.

Example: I will create Managed Instance Group name “multiple-server” that have 2 VM instances:

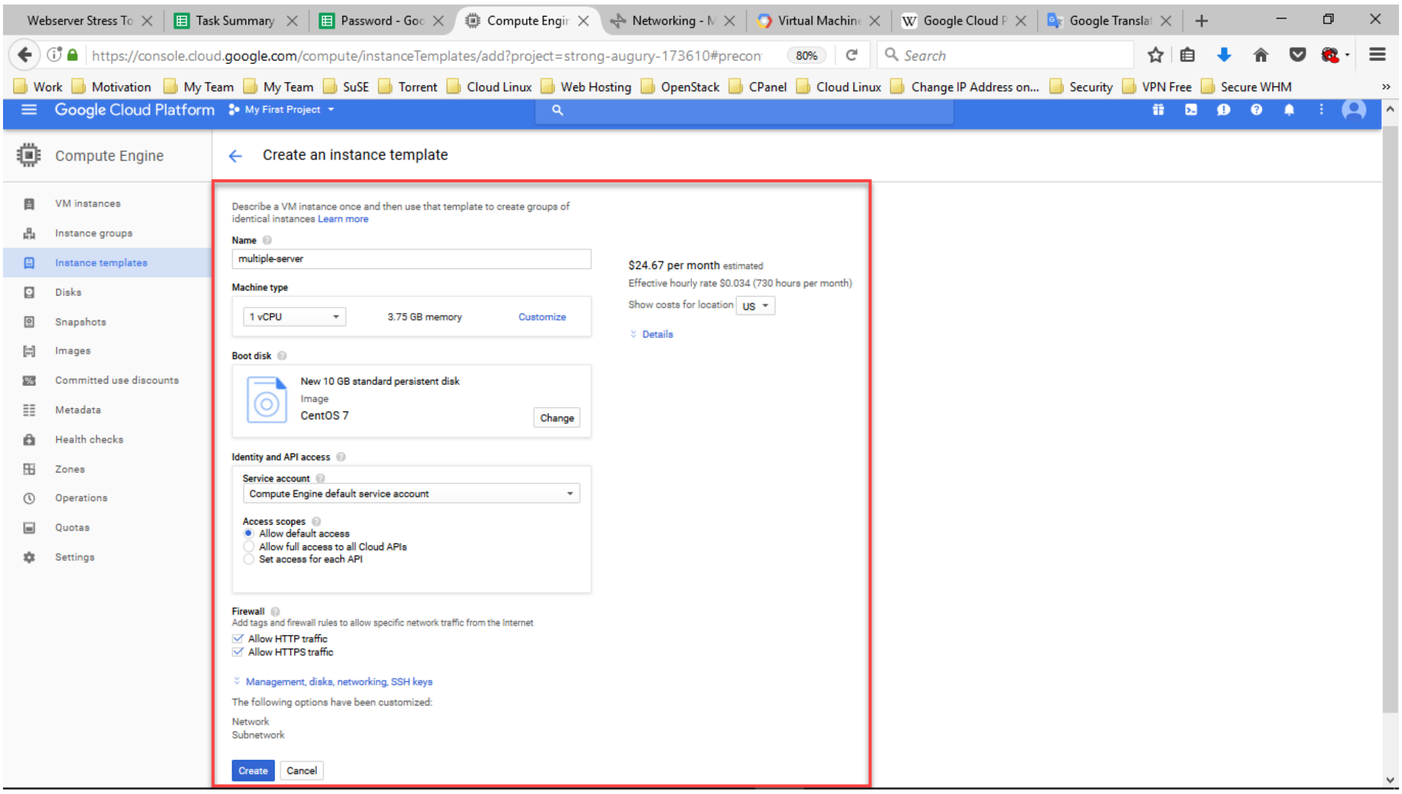
+Create Instance template(Name=multiple-server)



https://console.cloud.google.com/compute/instanceTemplates/list?project=strong-augury-173610

Instance templates

Name	Machine type	Image	Disk type	In use by	Creation time
cpanel-server-template	1 vCPU, 3.75 GB	centos-7-v20170719	Standard persistent disk		Jul 25, 2017, 2:09:47 PM
instance-template-1	1 vCPU, 3.75 GB	centos-6-v20170717	Standard persistent disk		Jul 26, 2017, 10:42:30 AM



https://console.cloud.google.com/compute/instanceTemplates/add?project=strong-augury-173610#precon

Create an instance template

Describe a VM instance once and then use that template to create groups of identical instances Learn more

Name: multiple-server

Machine type: 1 vCPU, 3.75 GB memory, Customize

Boot disk: New 10 GB standard persistent disk, Image CentOS 7, Change

Identity and API access

Service account: Compute Engine default service account

Access scopes

● Allow default access

○ Allow full access to all Cloud APIs

○ Set access for each API

Firewall

Add tags and firewall rules to allow specific network traffic from the Internet

☑ Allow HTTP traffic

☑ Allow HTTPS traffic

Management, disks, networking, SSH keys

The following options have been customized:

Network

Subnetwork

$24.67 per month estimated

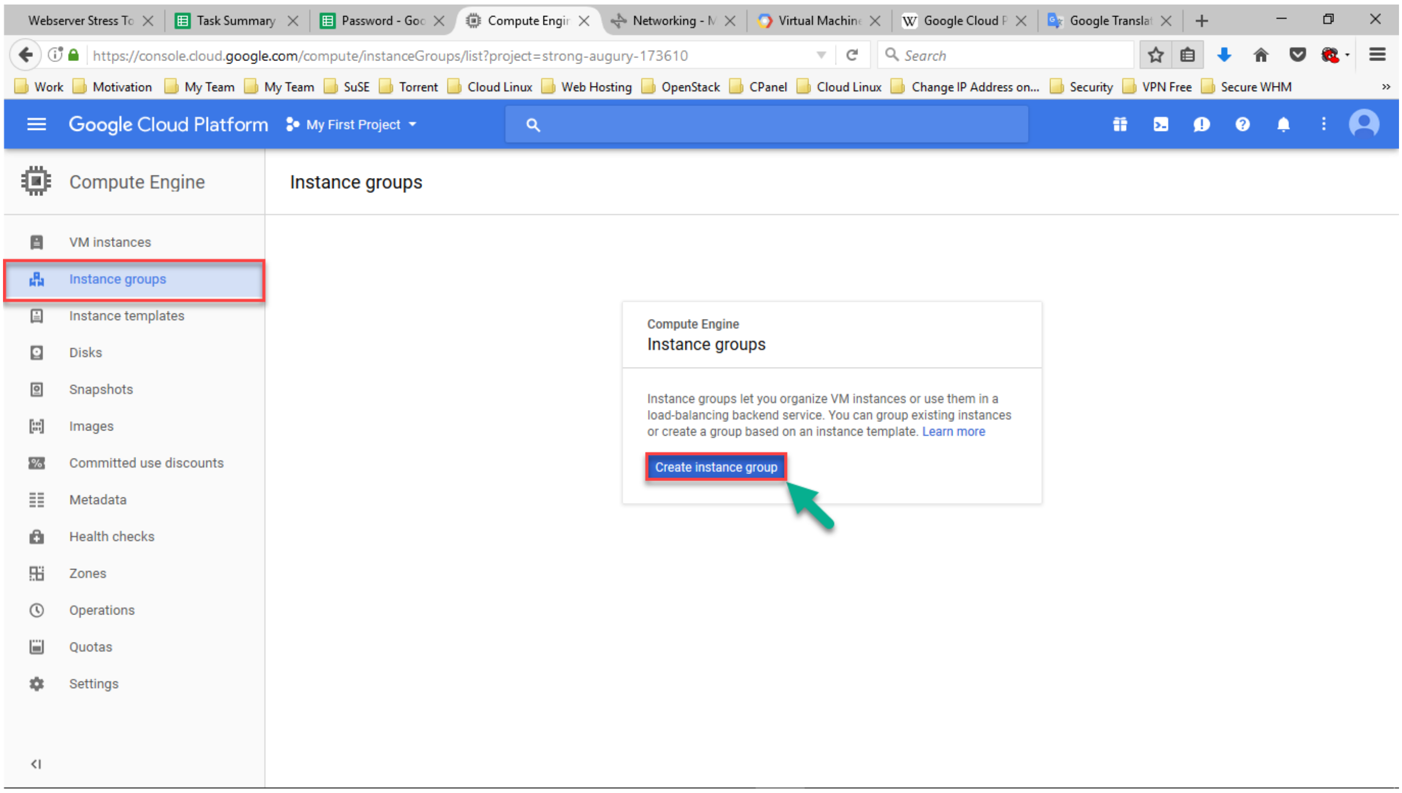
Effective hourly rate $0.034 (730 hours per month)

Show costs for location: US

Details

Create Cancel

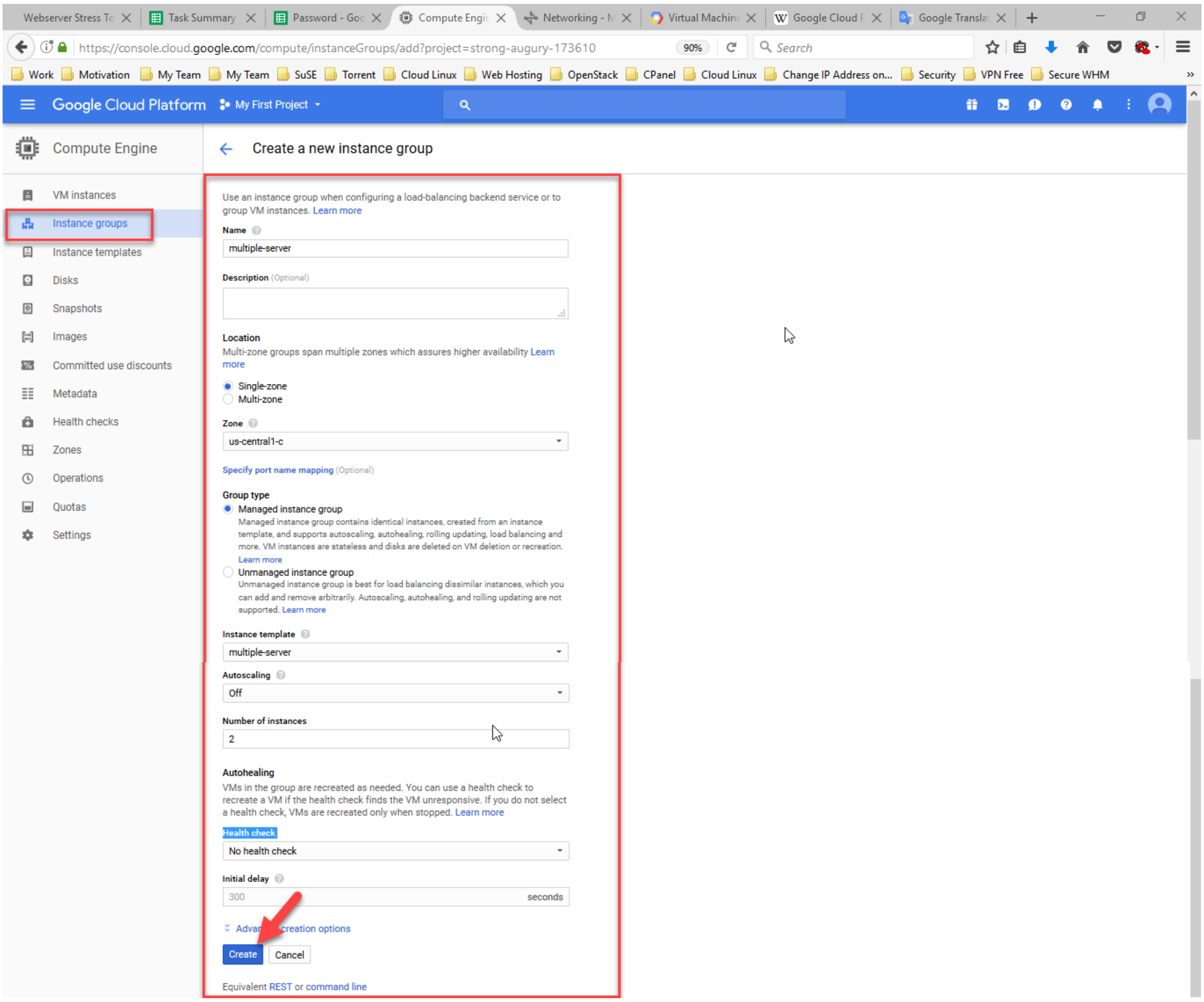
+Create Instance Group



Instance groups

Compute Engine
Instance groups

Instance groups let you organize VM instances or use them in a load-balancing backend service. You can group existing instances or create a group based on an instance template. Learn more



Create a new instance group

Use an instance group when configuring a load-balancing backend service or to group VM instances. Learn more

Name: multiple-server

Description (Optional)

Location
Multi-zone groups span multiple zones which assures higher availability Learn more

● Single-zone
○ Multi-zone

Zone: us-central1-c

Specify port name mapping (Optional)

Group type
● Managed instance group
Managed instance group contains identical instances, created from an instance template, and supports autoscaling, autohealing, rolling updating, load balancing and more. VM instances are stateless and disks are deleted on VM deletion or recreation. Learn more
○ Unmanaged instance group
Unmanaged instance group is best for load balancing dissimilar instances, which you can add and remove arbitrarily. Autoscaling, autohealing, and rolling updating are not supported. Learn more

Instance template: multiple-server

Autoscaling: Off

Number of instances: 2

Autohealing
VMs in the group are recreated as needed. You can use a health check to recreate a VM if the health check finds the VM unresponsive. If you do not select a health check, VMs are recreated only when stopped. Learn more

Health check: No health check

Initial delay: 300 seconds

Equivalent REST or command line

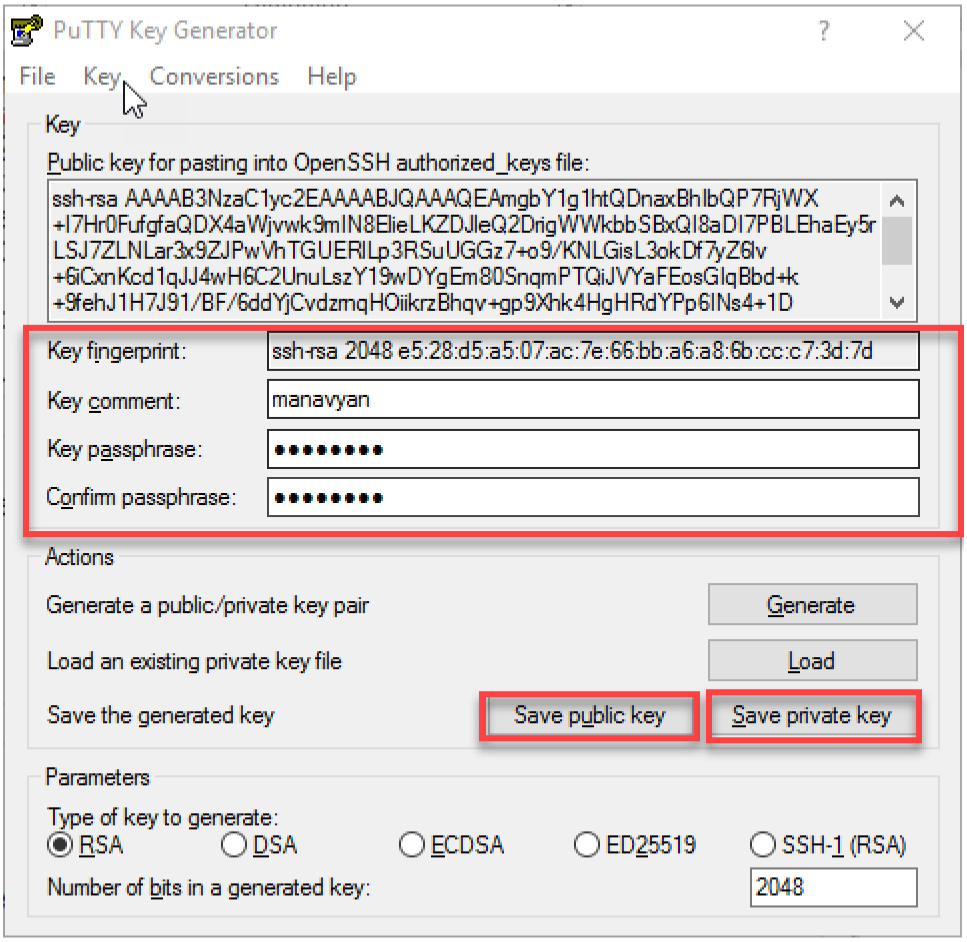
For more detail about Instance Group please visit https://cloud.google.com/compute/docs/instance-groups/

C/Access VM Instance via SSH client for Windows OS

1/Generate Key for SSH via puttygen

You can download putty.exe here https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html

+After generated the key, let fill username of VM instance in “Key comment”, put password in “Key passphrase” , then save Public & Private key in the safe place



Public key for pasting into OpenSSH authorized_keys file:

```
ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAAQEAmgbY1g1htQDnaxBhlbQP7RjWX
+I7Hr0FufgfaQDX4aWjvwk9mIN8ElieLKZDJleQ2DrigWWkbbSBxQI8aDI7PBLEhaEy5r
LSJ7ZLNLar3x9ZJPwVhTGUERILp3RSuUGGz7+o9/KNLGisL3okDf7yZ6lv
+6iCxnKcd1qJJ4wH6C2UnuLszY19wDYgEm80SnqmPTQiJVYaFEosGlqBbd+k
+9fehJ1H7J91/BF/6ddYjCvdzmqHOiikrzBhqv+gp9Xhk4HgHRdYPp6INs4+1D
```

Key fingerprint: ssh-rsa 2048 e5:28:d5:a5:07:ac:7e:66:bb:a6:a8:6b:cc:c7:3d:7d

Key comment: manavyan

Key passphrase: ●●●●●●●●●

Confirm passphrase: ●●●●●●●●●

Generate a public/private key pair

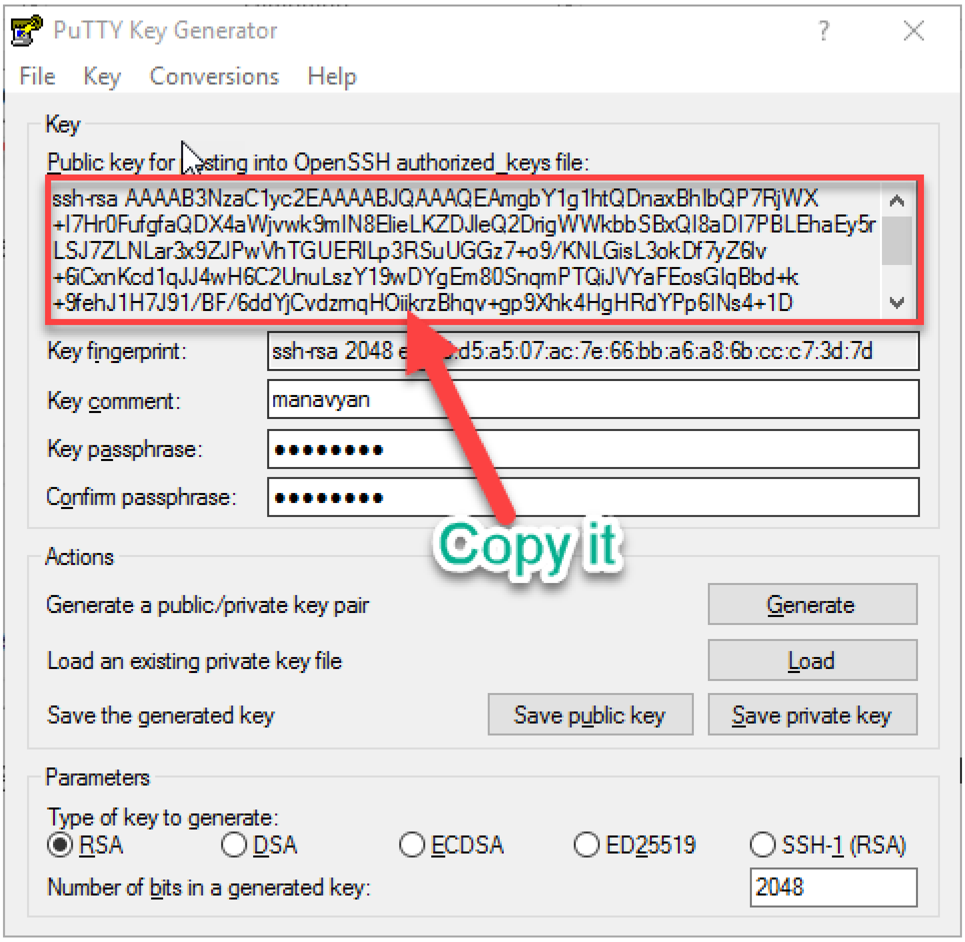
Load an existing private key file

Save the generated key

Type of key to generate:
● RSA ○ DSA ○ ECDSA ○ ED25519 ○ SSH-1 (RSA)

Number of bits in a generated key: 2048

After save the key, let copy generated key and pass it to “Metadata” in Google Cloud Platform



Key

Public key for pasting into OpenSSH authorized_keys file:

```
ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAAQEAmgbY1g1htQDnaxBhIbQP7RjWX
+I7Hr0FufgfaQDX4aWjvwk9mIN8ElieLKZDJleQ2DrigWWkbbSBxQI8aDI7PBLEhaEy5r
LSJ7ZLNLar3x9ZJPwVhTGUERILp3RSuUGGz7+o9/KNLGisL3okDf7yZ6lv
+6iCxnKcd1qJJ4wH6C2UnuLszY19wDYgEm80SnqmPTQiJVYaFEosGIqBbd+k
+9fehJ1H7J91/BF/6ddYjCvdzmqHOiikrzBhqv+gp9Xhk4HgHRdYPp6INs4+1D
```

Key fingerprint: ssh-rsa 2048 e d5:a5:07:ac:7e:66:bb:a6:a8:6b:cc:c7:3d:7d

Key comment: manavyan

Key passphrase: ●●●●●●●●●

Confirm passphrase: ●●●●●●●●●

Actions

Generate a public/private key pair

Load an existing private key file

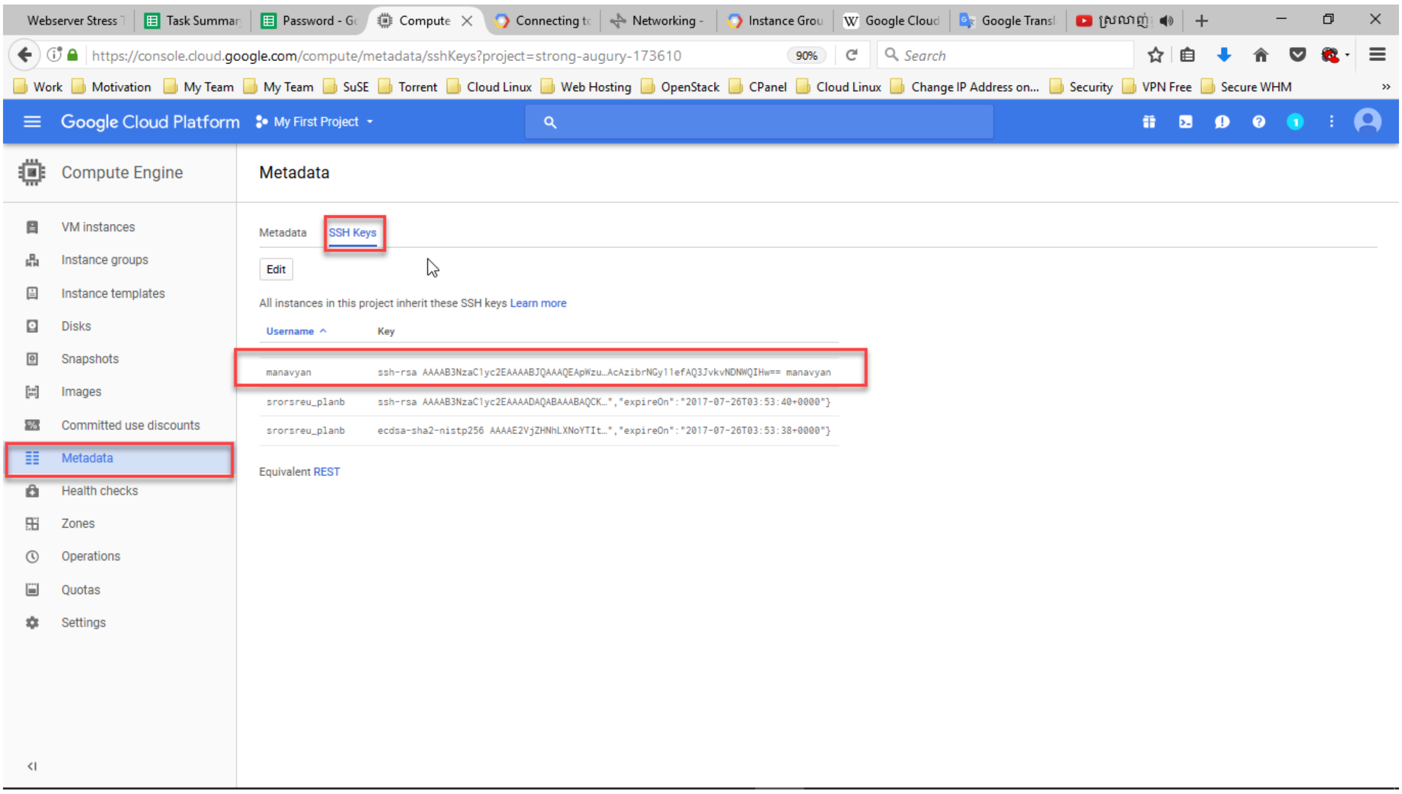
Save the generated key

Parameters

Type of key to generate:
● RSA ○ DSA ○ ECDSA ○ ED25519 ○ SSH-1 (RSA)

Number of bits in a generated key: 2048

Pass the key to Metadata, then save



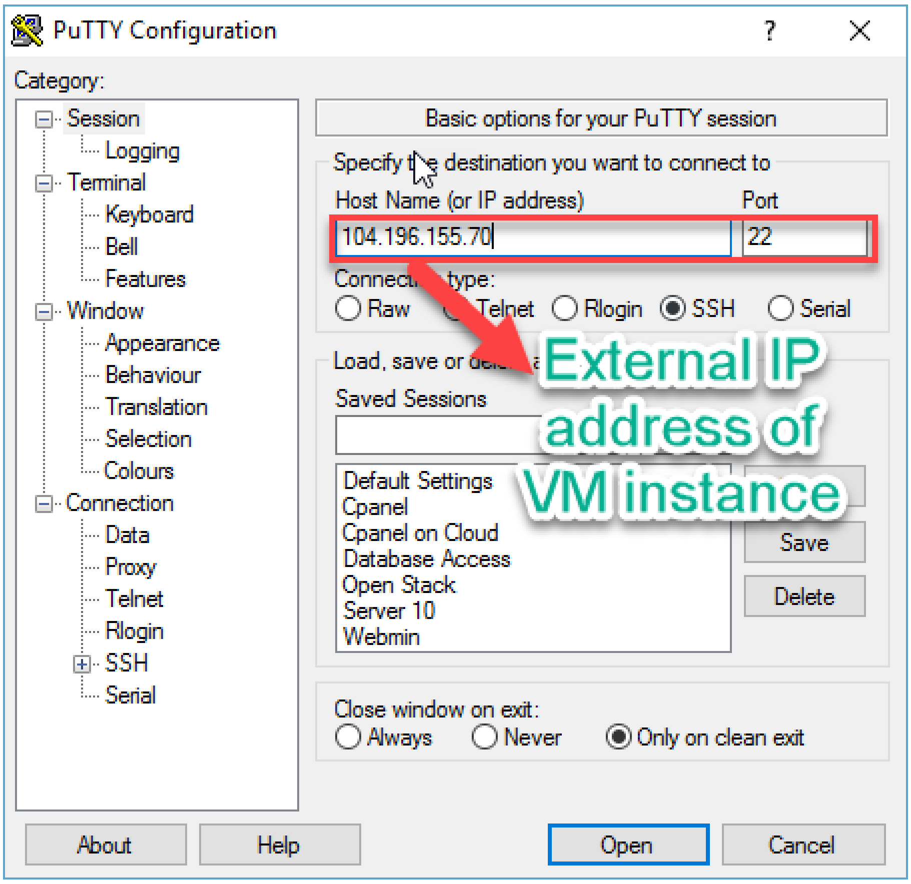
Metadata

Metadata | SSH Keys

All instances in this project inherit these SSH keys

Username ^	Key
manavyan	ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAAQEApWzu…AcAzibrNGy1lefAQ3JvkvNDNWQIHw== manavyan
srorsreu_planb	ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCK…","expireOn":"2017-07-26T03:53:40+0000"}
srorsreu_planb	ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTIt…","expireOn":"2017-07-26T03:53:38+0000"}

Configure Putty to use the key



PuTTY Configuration

Category:

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address): 104.196.155.70

Port: 22

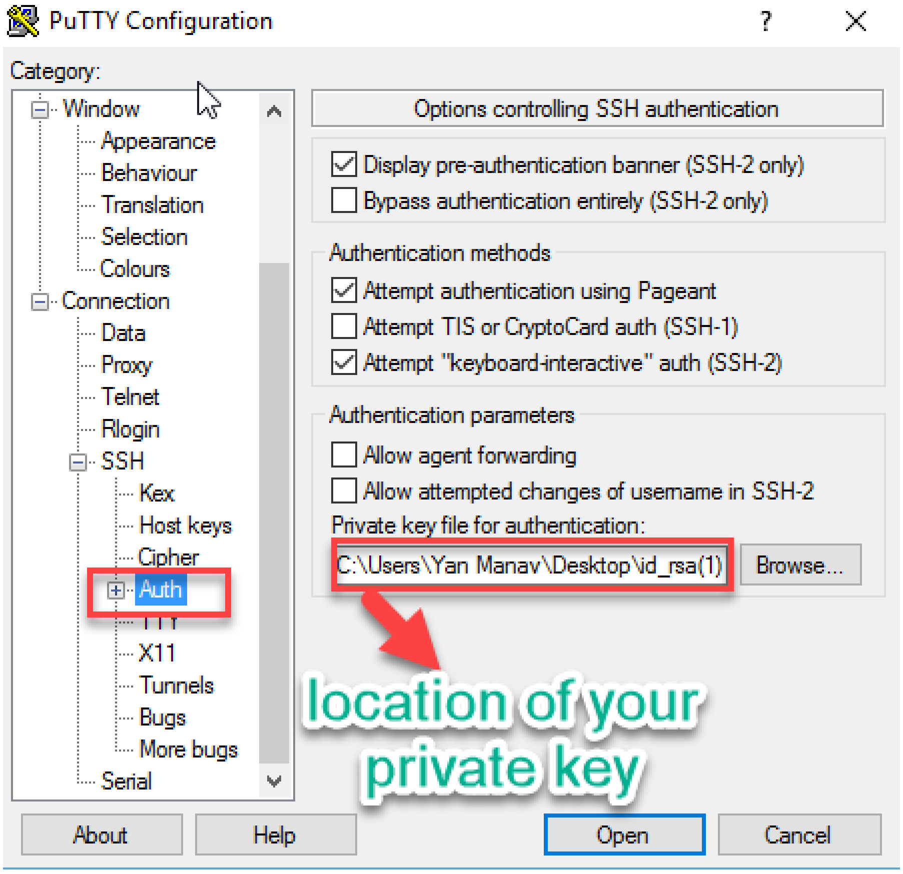
Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Load, save or delete a stored session

Saved Sessions

Default Settings
Cpanel
Cpanel on Cloud
Database Access
Open Stack
Server 10
Webmin

Close window on exit: ○ Always ○ Never ● Only on clean exit



PuTTY Configuration

Category:

Options controlling SSH authentication

☑ Display pre-authentication banner (SSH-2 only)
□ Bypass authentication entirely (SSH-2 only)

Authentication methods

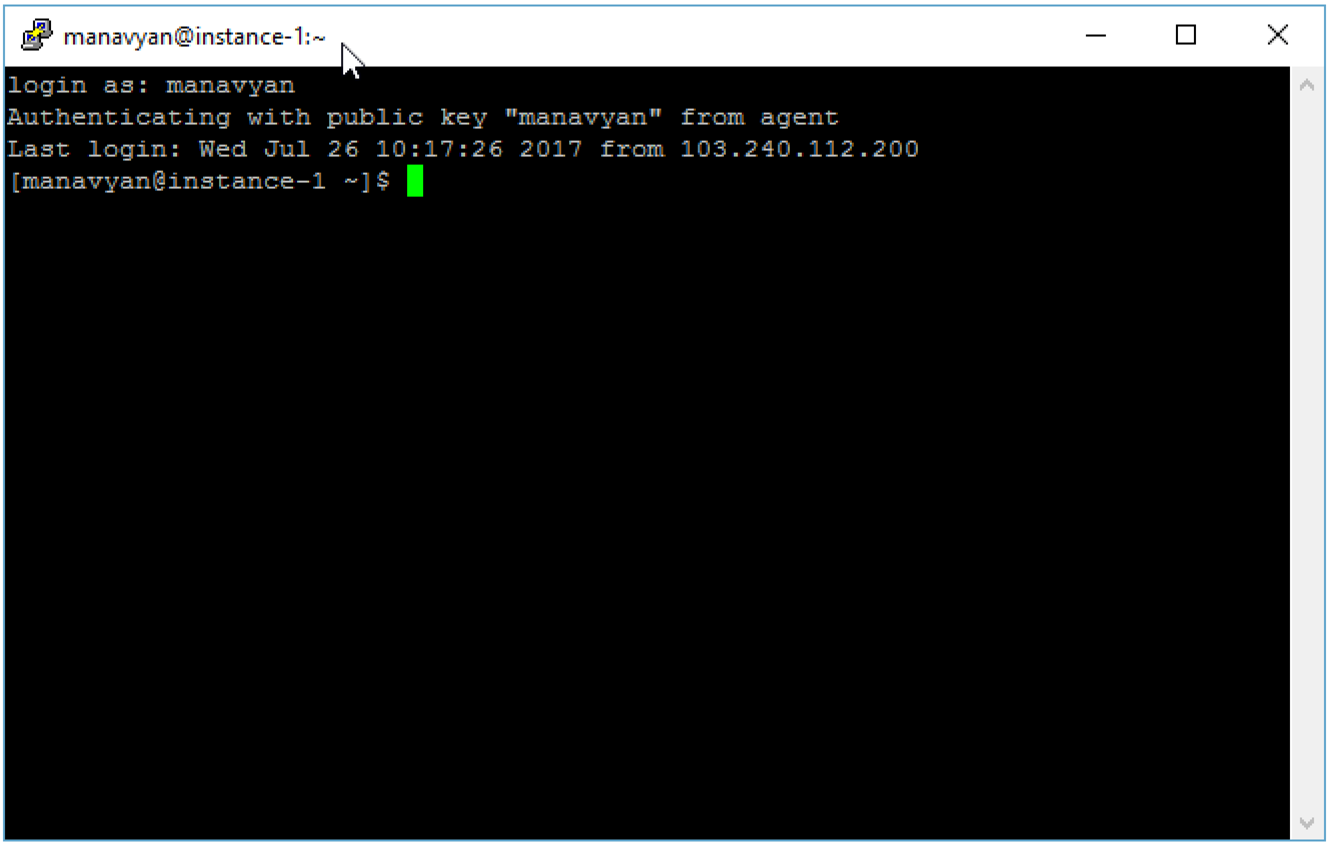
☑ Attempt authentication using Pageant
□ Attempt TIS or CryptoCard auth (SSH-1)
☑ Attempt "keyboard-interactive" auth (SSH-2)

Authentication parameters

□ Allow agent forwarding
□ Allow attempted changes of username in SSH-2

Private key file for authentication: C:\Users\Yan Manav\Desktop\id_rsa(1)

Finally, go to “Session” and click on “Open”. The windows will appear, type your username correctly.



```
login as: manavyan
Authenticating with public key "manavyan" from agent
Last login: Wed Jul 26 10:17:26 2017 from 103.240.112.200
[manavyan@instance-1 ~]$
```

For more detail about using putty remote to Instance, please visit https://cloud.google.com/compute/docs/instances/connecting-to-instance#standardssh