DevOps Lab

CLOUD COMPUTE - GCP

NETWORKING

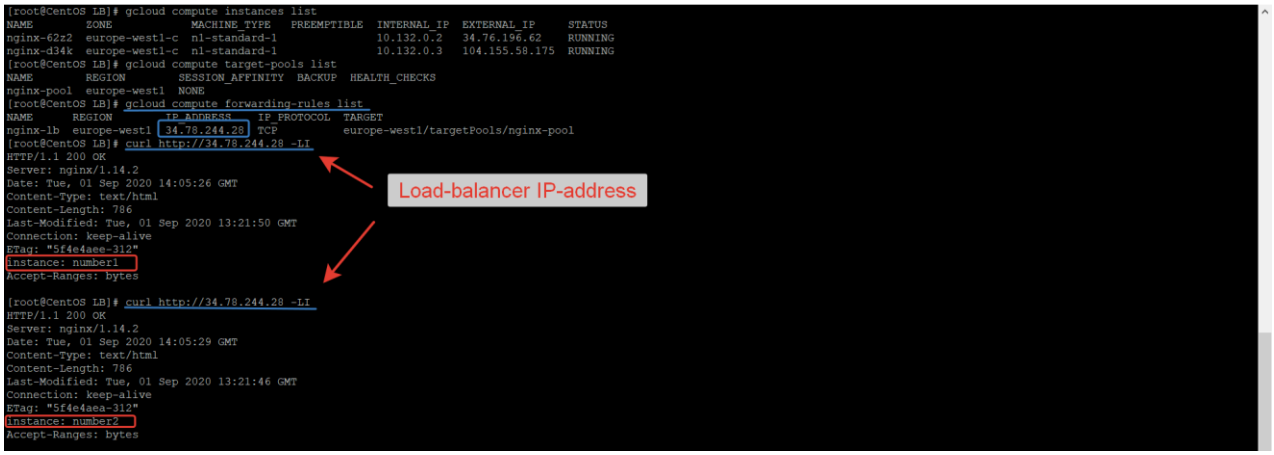
Home tasks

It’s aiming to gain knowledge about Networking in Google Cloud.

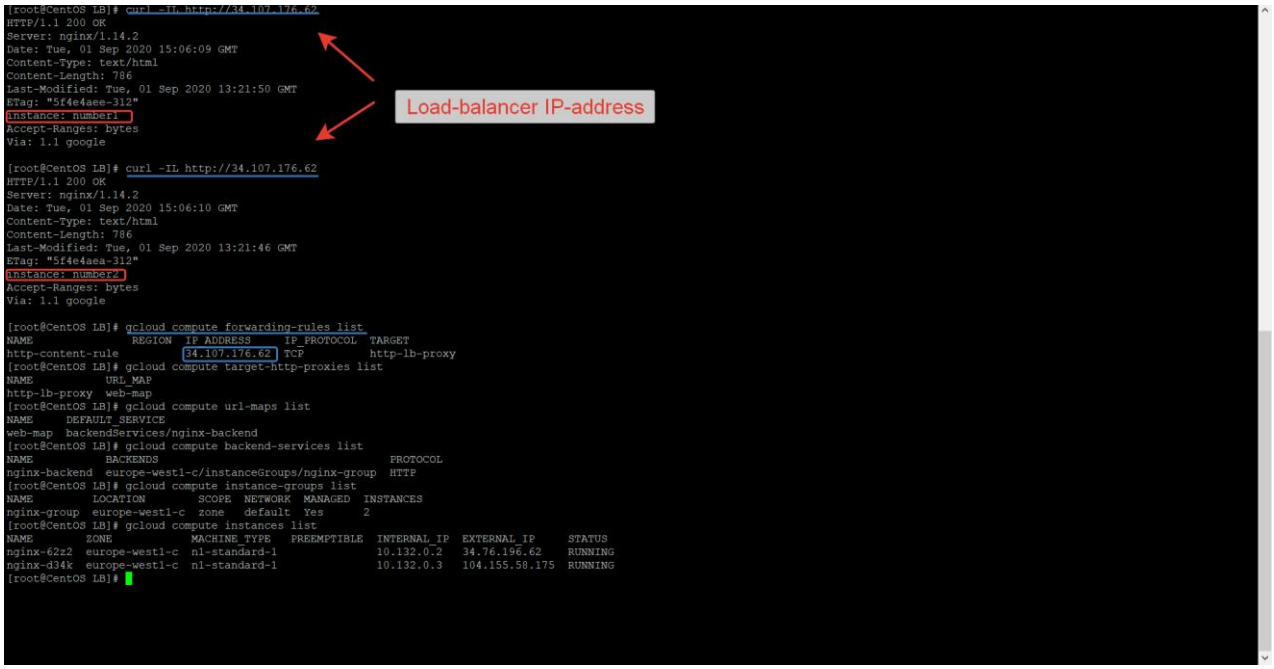
TASK 1

Learn about two types of load balancers in Google Cloud Platform:

- a L3 Network Load Balancer



- a L7 HTTP(s) Load Balancer.

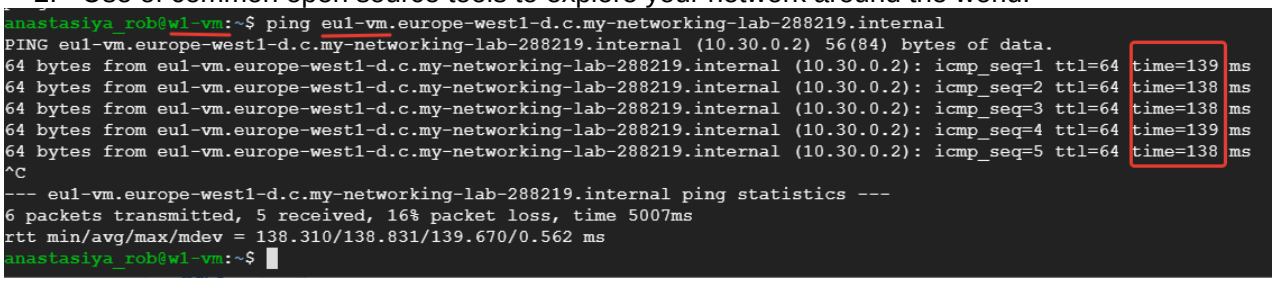


TASK 2

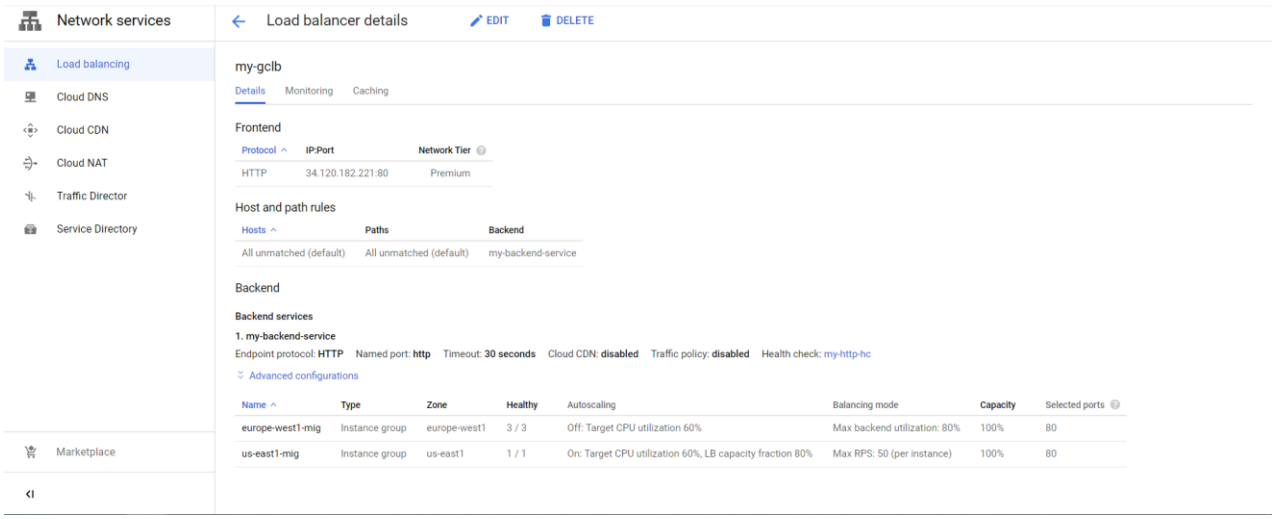
These exercises are ordered to reflect a common cloud developer experience as follows:

1. Set up your lab environment and learn how to work with your GCP environment.

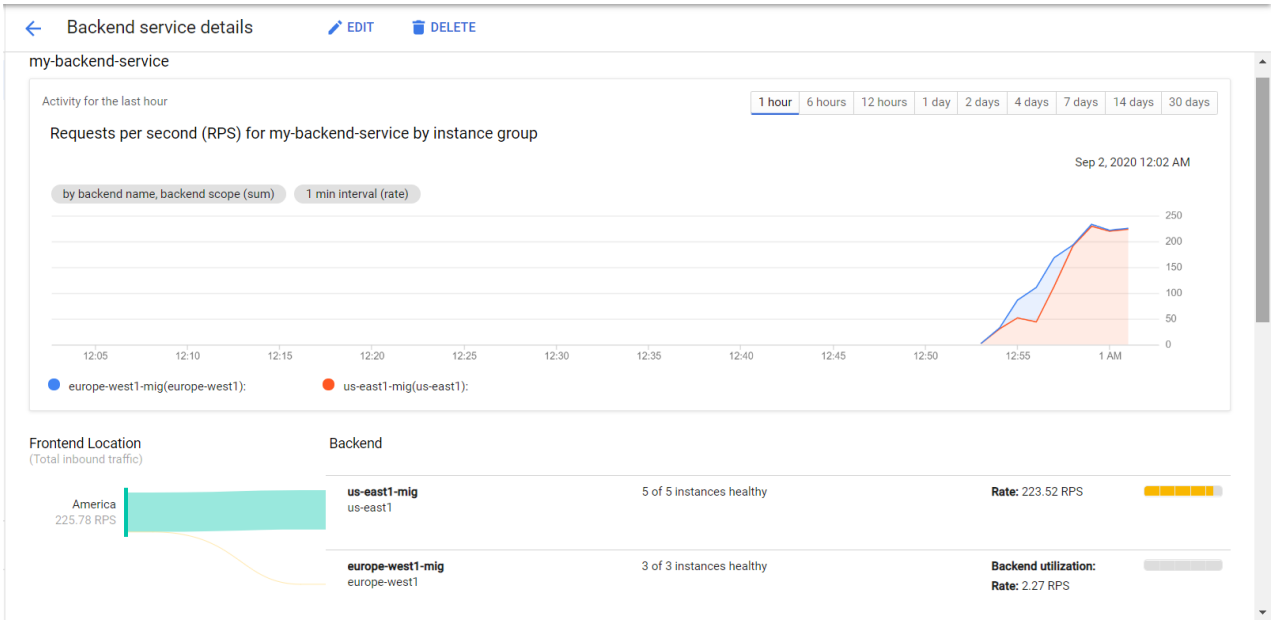
2. Use of common open source tools to explore your network around the world.



3. Deploy a common use case: use of HTTP Load Balancing and Managed Instance Groups to host a scalable, multi-region web server.



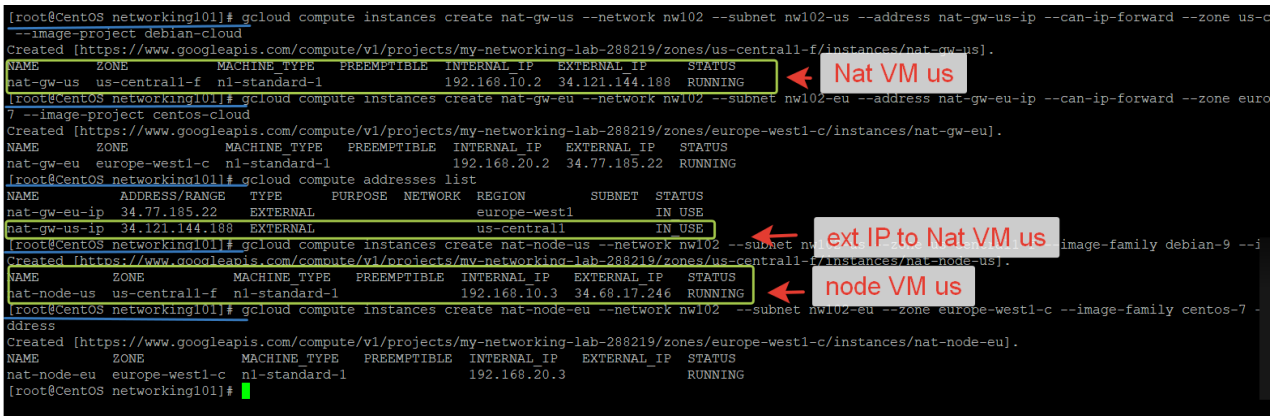
4. Testing and monitoring your network and instances.



TASK 3

The Objectives are to learn:

- Setting up NAT gateways



- How to restrict network traffic that certain tiers of an app cannot talk to each other

- Setting up alternate connectivity options to instances

```
[root@CentOS networking101]# gcloud compute addresses list
NAME           ADDRESS/RANGE    TYPE      PURPOSE  NETWORK  REGION        SUBNET  STATUS
nat-gw-eu-ip   34.77.185.22     EXTERNAL                    europe-west1          IN_USE
nat-gw-us-ip   34.121.144.188   EXTERNAL                    us-central1           IN_USE
web-ext-ip     34.68.17.246     EXTERNAL                    us-central1           IN_USE
[root@CentOS networking101]# curl -IL  34.68.17.246
HTTP/1.1 200 OK
Date: Wed, 02 Sep 2020 09:13:46 GMT
Server: Apache/2.4.25 (Debian)
Last-Modified: Wed, 02 Sep 2020 08:08:48 GMT
ETag: "29cd-5ae50253747e3"
Accept-Ranges: bytes
Content-Length: 10701
Vary: Accept-Encoding
Content-Type: text/html

[root@CentOS networking101]# gcloud compute forwarding-rules list
NAME     REGION       IP_ADDRESS     IP_PROTOCOL  TARGET
web-ext  us-central1  34.68.17.246   TCP          us-central1-f/targetInstances/web-target
[root@CentOS networking101]# gcloud compute firewall-rules list
NAME                    NETWORK  DIRECTION  PRIORITY  ALLOW                         DENY  DISABLED
default-allow-icmp      default  INGRESS    65534     icmp                                False
default-allow-internal  default  INGRESS    65534     tcp:0-65535,udp:0-65535,icmp        False
default-allow-rdp       default  INGRESS    65534     tcp:3389                            False
default-allow-ssh       default  INGRESS    65534     tcp:22                              False
nw102-allow-app         nw102    INGRESS    1000      tcp:22,tcp:80                       False
nw102-allow-egress      nw102    INGRESS    1000      tcp:80,tcp:443                      False
nw102-allow-ext         nw102    INGRESS    1000      tcp:80                              False
nw102-allow-internal    nw102    INGRESS    1000      icmp                                False
nw102-allow-ssh         nw102    INGRESS    1000      tcp:22                              False
nw102-allow-traceroute  nw102    INGRESS    1000      udp:33434-33534                     False
nw102-allow-traceroute1 nw102    INGRESS    1000      udp:33434-33534                     False
nw102-allow-web         nw102    INGRESS    1000      tcp:22,tcp:80                       False

To show all fields of the firewall, please show in JSON format: --format=json
To show all fields in table format, please see the examples in --help.

[root@CentOS networking101]# gcloud compute target-instances list
NAME        ZONE        INSTANCE      NAT_POLICY
web-target  us-central1-f  nat-node-w-us  NO_NAT
[root@CentOS networking101]#
```

- Map an external service to look like an internal service

```
nat-node-w-eu     europe-west1-c  n1-standard-1  192.168.20.4                  RUNNING
faux-on-prem-svc  us-central1-f   n1-standard-1  10.128.0.2    34.71.94.202    RUNNING
nat-gw-us         us-central1-f   n1-standard-1  192.168.10.2  34.121.144.188  RUNNING
nat-node-us       us-central1-f   n1-standard-1  192.168.10.3                  RUNNING
nat-node-w-us     us-central1-f   n1-standard-1  192.168.10.4                  RUNNING
```

- How to setup an Egress proxy limiting access to specific resources

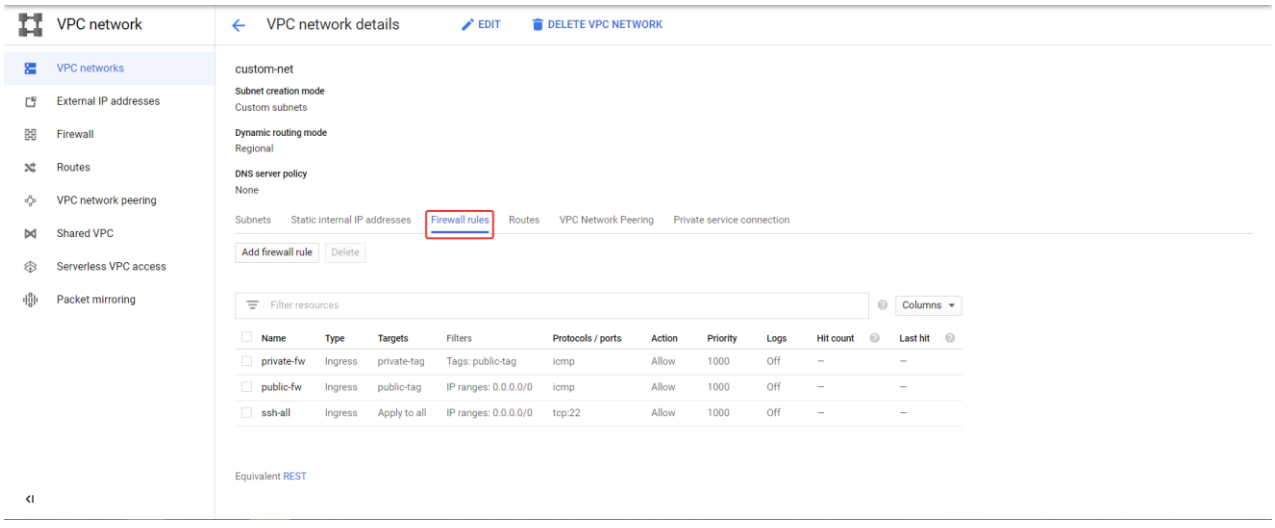
```
anastasiya_rob@nat-node-us:~$ curl nat-gw-us -IL
HTTP/1.1 200 OK
Date: Wed, 02 Sep 2020 09:41:50 GMT
Server: Apache/2.4.25 (Debian)
Last-Modified: Wed, 02 Sep 2020 09:31:20 GMT
ETag: "29cd-5ae514c6406a3"
Accept-Ranges: bytes
Content-Length: 10701
Vary: Accept-Encoding
Content-Type: text/html
```

← response from VM faux-on-prem-svc

TASK 4

The Objectives are to learn:

- Secure app in custom network



```
anastasiya_rob@public-vm:~$ ping private-vm.us-central1-b.c.my-networking-lab-288219.internal
PING private-vm.us-central1-b.c.my-networking-lab-288219.internal (192.168.1.2) 56(84) bytes of data.
64 bytes from private-vm.us-central1-b.c.my-networking-lab-288219.internal (192.168.1.2): icmp_seq=1 ttl=64 time=1.
70 ms
64 bytes from private-vm.us-central1-b.c.my-networking-lab-288219.internal (192.168.1.2): icmp_seq=2 ttl=64 time=0.
269 ms
64 bytes from private-vm.us-central1-b.c.my-networking-lab-288219.internal (192.168.1.2): icmp_seq=3 ttl=64 time=0.
361 ms
64 bytes from private-vm.us-central1-b.c.my-networking-lab-288219.internal (192.168.1.2): icmp_seq=4 ttl=64 time=0.
339 ms
64 bytes from private-vm.us-central1-b.c.my-networking-lab-288219.internal (192.168.1.2): icmp_seq=5 ttl=64 time=0.
297 ms
^C
--- private-vm.us-central1-b.c.my-networking-lab-288219.internal ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4073ms
rtt min/avg/max/mdev = 0.269/0.594/1.705/0.556 ms
```

TASK 5

Create network configuration via terraform.

```
            ~ nat_ip       = "35.222.200.201" -> (known after apply)
            ~ network_tier = "PREMIUM" -> (known after apply)
          }
      }

    ~ scheduling {
        ~ automatic_restart   = true -> (known after apply)
        ~ on_host_maintenance = "MIGRATE" -> (known after apply)
        ~ preemptible         = false -> (known after apply)

        + node_affinities {
            + key      = (known after apply)
            + operator = (known after apply)
            + values   = (known after apply)
          }
      }

    ~ shielded_instance_config {
        ~ enable_integrity_monitoring = true -> null
        ~ enable_secure_boot          = false -> null
        ~ enable_vtpm                 = true -> null
      }
  }

Plan: 1 to add, 0 to change, 1 to destroy.

Do you want to perform these actions?
  Terraform will perform the actions described above.
  Only 'yes' will be accepted to approve.

  Enter a value: yes

google_compute_instance.vm_instance: Destroying... [id=projects/devops-lab-2020/zones/us-central1-a/instances/nginx-networking]
google_compute_instance.vm_instance: Still destroying... [id=projects/devops-lab-2020/zones/us-central1-a/instances/nginx-networking, 10s elapsed]
google_compute_instance.vm_instance: Still destroying... [id=projects/devops-lab-2020/zones/us-central1-a/instances/nginx-networking, 20s elapsed]
google_compute_instance.vm_instance: Destruction complete after 22s
google_compute_instance.vm_instance: Creating...
google_compute_instance.vm_instance: Still creating... [10s elapsed]
google_compute_instance.vm_instance: Creation complete after 15s [id=projects/devops-lab-2020/zones/us-central1-a/instances/nginx-networking]

Apply complete! Resources: 1 added, 0 changed, 1 destroyed.
[root@CentOS task2]# gcloud compute instances list
NAME              ZONE           MACHINE_TYPE      PREEMPTIBLE  INTERNAL_IP  EXTERNAL_IP     STATUS
nginx-networking  us-central1-a  custom-1-4608-ext              10.8.1.3     35.202.68.156   RUNNING
nginx-gcloud      us-central1-c  custom-1-4608                  10.128.0.4   35.193.86.223   RUNNING
nginx-gcp-ui      us-central1-c  custom-1-4608                  10.128.0.2                   TERMINATED
[root@CentOS task2]# curl 35.202.68.156
Hello from nrabeichykava
[root@CentOS task2]#
```