

DevOps Lab

CLOUD COMPUTE - GCP

NETWORKING

Home tasks



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

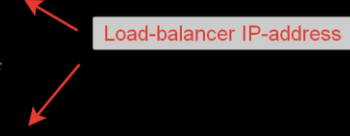
TASK 1

Learn about two types of [load balancers in Google Cloud Platform](#):

- a L3 [Network Load Balancer](#)

```
[root@CentOS LB]# gcloud compute instances list
NAME                                ZONE          MACHINE_TYPE  PREEMPTIBLE  INTERNAL_IP  EXTERNAL_IP  STATUS
nginx-6222                          europe-west1-c  nl-standard-1               10.132.0.2   34.76.196.62  RUNNING
nginx-d34k                          europe-west1-c  nl-standard-1               10.132.0.3   104.155.58.175  RUNNING
[root@CentOS LB]# gcloud compute target-pools list
NAME                                REGION  SESSION_AFFINITY  BACKUP  HEALTH_CHECKS
nginx-pool                          europe-west1  NONE
[root@CentOS LB]# gcloud compute forwarding-rules list
NAME                                REGION  IP_ADDRESS     IP_PROTOCOL  TARGET
nginx-lb                          europe-west1  34.78.244.28  TCP          europe-west1/targetPools/nginx-pool
[root@CentOS LB]# curl http://34.78.244.28 -LI
HTTP/1.1 200 OK
Server: nginx/1.14.2
Date: Tue, 01 Sep 2020 14:05:26 GMT
Content-Type: text/html
Content-Length: 786
Last-Modified: Tue, 01 Sep 2020 13:21:50 GMT
Connection: keep-alive
ETag: "5f4e4aea-312"
Instance: number1
Accept-Ranges: bytes

[root@CentOS LB]# curl http://34.78.244.28 -LI
HTTP/1.1 200 OK
Server: nginx/1.14.2
Date: Tue, 01 Sep 2020 14:05:29 GMT
Content-Type: text/html
Content-Length: 786
Last-Modified: Tue, 01 Sep 2020 13:21:46 GMT
Connection: keep-alive
ETag: "5f4e4aea-312"
Instance: number2
Accept-Ranges: bytes
```



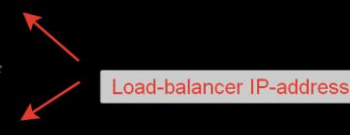
Load-balancer IP-address

- a L7 [HTTP\(s\) Load Balancer](#).

```
[root@CentOS LB]# curl -LI http://34.107.176.62
HTTP/1.1 200 OK
Server: nginx/1.14.2
Date: Tue, 01 Sep 2020 15:06:09 GMT
Content-Type: text/html
Content-Length: 786
Last-Modified: Tue, 01 Sep 2020 13:21:50 GMT
ETag: "5f4e4aea-312"
Instance: number1
Accept-Ranges: bytes
Via: 1.1 google

[root@CentOS LB]# curl -LI http://34.107.176.62
HTTP/1.1 200 OK
Server: nginx/1.14.2
Date: Tue, 01 Sep 2020 15:06:10 GMT
Content-Type: text/html
Content-Length: 786
Last-Modified: Tue, 01 Sep 2020 13:21:46 GMT
ETag: "5f4e4aea-312"
Instance: number2
Accept-Ranges: bytes
Via: 1.1 google

[root@CentOS LB]# gcloud compute forwarding-rules list
NAME                                REGION  IP_ADDRESS     IP_PROTOCOL  TARGET
http-content-rule                  europe-west1  34.107.176.62  TCP          http-lb-proxy
[root@CentOS LB]# gcloud compute target-http-proxies list
NAME                                URL_MAP
http-lb-proxy                      web-map
[root@CentOS LB]# gcloud compute url-maps list
NAME                                DEFAULT_SERVICE
web-map                            backendServices/nginx-backend
[root@CentOS LB]# gcloud compute backend-services list
NAME                                BACKENDS                                PROTOCOL
nginx-backend                      europe-west1-c/instanceGroups/nginx-group  HTTP
[root@CentOS LB]# gcloud compute instance-groups list
NAME                                LOCATION  SCOPE  NETWORK  MANAGED  INSTANCES
nginx-group                        europe-west1-c  zone  default  Yes      2
[root@CentOS LB]# gcloud compute instances list
NAME                                ZONE          MACHINE_TYPE  PREEMPTIBLE  INTERNAL_IP  EXTERNAL_IP  STATUS
nginx-6222                          europe-west1-c  nl-standard-1               10.132.0.2   34.76.196.62  RUNNING
nginx-d34k                          europe-west1-c  nl-standard-1               10.132.0.3   104.155.58.175  RUNNING
[root@CentOS LB]#
```



Load-balancer IP-address

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.

```
[root@CentOS networking101]# gcloud deployment-manager deployments update networking101 --config networking-lab.yaml
The fingerprint of the deployment is xlaig341V3yHCBvAeuhxk==
Waiting for update [operation-1598991460805-Sae4636052c2f-1377fd34-89fdd029]...done.
Update operation operation-1598991460805-Sae4636052c2f-1377fd34-89fdd029 completed successfully.
NAME      TYPE      STATE      ERRORS  INTENT
asia-east1  compute.v1.subnetwork  COMPLETED  []
asia1-vm    compute.v1.instance    COMPLETED  []
e1-vm      compute.v1.instance    COMPLETED  []
eul-vm     compute.v1.instance    COMPLETED  []
europe-west1  compute.v1.subnetwork  COMPLETED  []
networking101  compute.v1.network    COMPLETED  []
networking101-firewall-allow-icmp  compute.v1.firewall    COMPLETED  []
networking101-firewall-allow-internal  compute.v1.firewall    COMPLETED  []
networking101-firewall-allow-ssh    compute.v1.firewall    COMPLETED  []
us-east1    compute.v1.subnetwork  COMPLETED  []
us-west1-s1  compute.v1.subnetwork  COMPLETED  []
us-west1-s2  compute.v1.subnetwork  COMPLETED  []
w1-vm      compute.v1.instance    COMPLETED  []
w2-vm      compute.v1.instance    COMPLETED  []
```

Firewall rules and instances

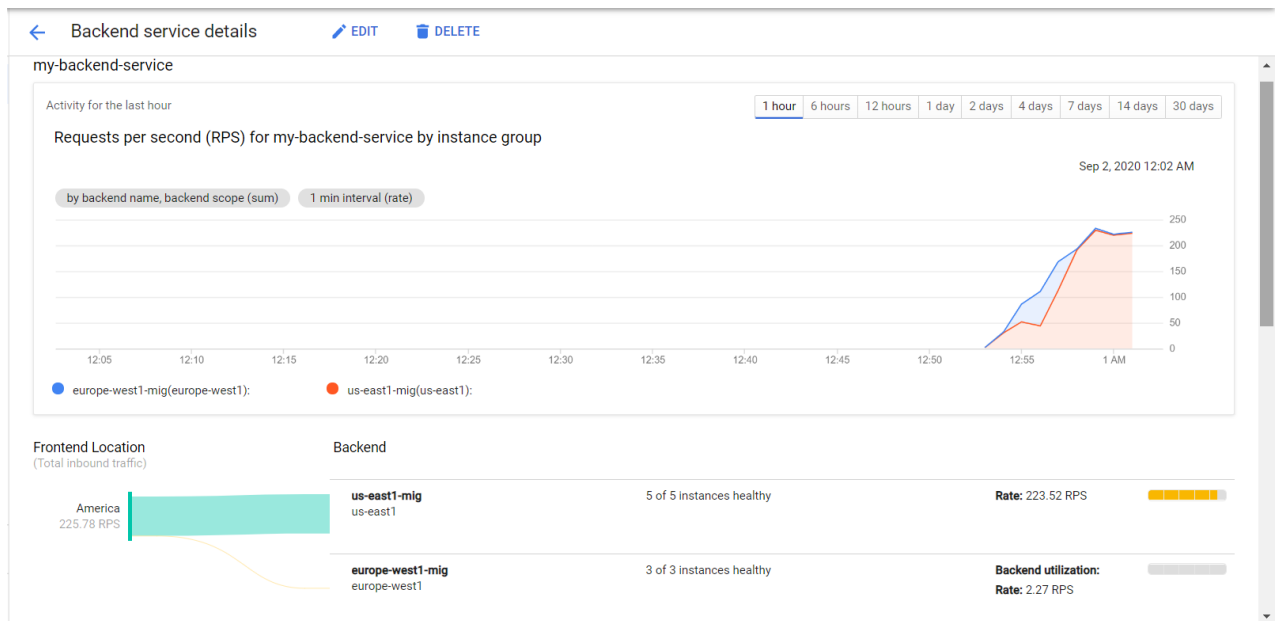
2. Use of common open source tools to explore your network around the world.

```
anastasiya_rob@w1-vm:~$ ping eul-vm.europe-west1-d.c.my-networking-lab-288219.internal
PING eul-vm.europe-west1-d.c.my-networking-lab-288219.internal (10.30.0.2) 56(84) bytes of data.
64 bytes from eul-vm.europe-west1-d.c.my-networking-lab-288219.internal (10.30.0.2): icmp_seq=1 ttl=64 time=139 ms
64 bytes from eul-vm.europe-west1-d.c.my-networking-lab-288219.internal (10.30.0.2): icmp_seq=2 ttl=64 time=138 ms
64 bytes from eul-vm.europe-west1-d.c.my-networking-lab-288219.internal (10.30.0.2): icmp_seq=3 ttl=64 time=138 ms
64 bytes from eul-vm.europe-west1-d.c.my-networking-lab-288219.internal (10.30.0.2): icmp_seq=4 ttl=64 time=139 ms
64 bytes from eul-vm.europe-west1-d.c.my-networking-lab-288219.internal (10.30.0.2): icmp_seq=5 ttl=64 time=138 ms
^C
--- eul-vm.europe-west1-d.c.my-networking-lab-288219.internal ping statistics ---
6 packets transmitted, 5 received, 16% packet loss, time 5007ms
rtt min/avg/max/mdev = 138.310/138.831/139.670/0.562 ms
anastasiya_rob@w1-vm:~$
```

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

Network services	Load balancer details	EDIT	DELETE
Load balancing	my-gclb		
Cloud DNS	Details Monitoring Caching		
Cloud CDN	Frontend		
Cloud NAT	Protocol IP-Port Network Tier		
Traffic Director	HTTP 34.120.182.221:80 Premium		
Service Directory	Host and path rules		
	Hosts Paths Backend		
	All unmatched (default) All unmatched (default) my-backend-service		
	Backend		
	Backend services		
	1. my-backend-service		
	Endpoint protocol: HTTP Named port: http Timeout: 30 seconds Cloud CDN: disabled Traffic policy: disabled Health check: my-http-hc		
	Advanced configurations		
	Name Type Zone Healthy Autoscaling Balancing mode Capacity Selected ports		
	europe-west1-mig Instance group europe-west1 3 / 3 Off: Target CPU utilization 60% Max backend utilization: 80% 100% 80		
	us-east1-mig Instance group us-east1 1 / 1 On: Target CPU utilization 60%, LB capacity fraction 80% Max RPS: 50 (per instance) 100% 80		

4. Testing and monitoring your network and instances.



TASK 3

The Objectives are to learn:

- Setting up NAT gateways

```
[root@CentOS networking101]# gcloud compute instances create nat-gw-us --network nw102 --subnet nw102-us --address nat-gw-us-ip --can-ip-forward --zone us-central1-f --image-project debian-cloud
Created [https://www.googleapis.com/compute/v1/projects/my-networking-lab-288219/zones/us-central1-f/instances/nat-gw-us].
NAME      ZONE      MACHINE_TYPE  PREEMPTIBLE  INTERNAL_IP  EXTERNAL_IP  STATUS
nat-gw-us  us-central1-f  nl-standard-1  192.168.10.2  34.121.144.188  RUNNING
[root@CentOS networking101]# gcloud compute instances create nat-gw-eu --network nw102 --subnet nw102-eu --address nat-gw-eu-ip --can-ip-forward --zone europe-west1-c --image-project centos-cloud
Created [https://www.googleapis.com/compute/v1/projects/my-networking-lab-288219/zones/europe-west1-c/instances/nat-gw-eu].
NAME      ZONE      MACHINE_TYPE  PREEMPTIBLE  INTERNAL_IP  EXTERNAL_IP  STATUS
nat-gw-eu  europe-west1-c  nl-standard-1  192.168.20.2  34.77.185.22  RUNNING
[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  NAT_GATEWAY  nw102  europe-west1  IN USE
nat-gw-us-ip  34.121.144.188  EXTERNAL  NAT_GATEWAY  nw102  us-central1  IN USE
[root@CentOS networking101]# gcloud compute instances create nat-node-us --network nw102 --subnet nw102-us --image-family debian-9 --image-project debian-cloud
Created [https://www.googleapis.com/compute/v1/projects/my-networking-lab-288219/zones/us-central1-f/instances/nat-node-us].
NAME      ZONE      MACHINE_TYPE  PREEMPTIBLE  INTERNAL_IP  EXTERNAL_IP  STATUS
nat-node-us  us-central1-f  nl-standard-1  192.168.10.3  34.68.17.246  RUNNING
[root@CentOS networking101]# gcloud compute instances create nat-node-eu --network nw102 --subnet nw102-eu --zone europe-west1-c --image-family centos-7 --image-project centos-cloud
Created [https://www.googleapis.com/compute/v1/projects/my-networking-lab-288219/zones/europe-west1-c/instances/nat-node-eu].
NAME      ZONE      MACHINE_TYPE  PREEMPTIBLE  INTERNAL_IP  EXTERNAL_IP  STATUS
nat-node-eu  europe-west1-c  nl-standard-1  192.168.20.3  192.168.20.3  RUNNING
```

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

```
[root@CentOS networking101]# gcloud compute firewall-rules list
NAME      NETWORK  DIRECTION  PRIORITY  ALLOW  DENY  DISABLED
default-allow-icmp  default  INGRESS    65534    icmp  False  False
default-allow-internal  default  INGRESS    65534    tcp:0-65535,udp:0-65535,icmp  False  False
default-allow-rdp  default  INGRESS    65534    tcp:3389  False  False
default-allow-ssh  default  INGRESS    65534    tcp:22  False  False
nw102-allow-app  nw102  INGRESS    1000    tcp:22,tcp:80  False  False
nw102-allow-egress  nw102  INGRESS    1000    tcp:80,tcp:443  False  False
nw102-allow-internal  nw102  INGRESS    1000    icmp  False  False
nw102-allow-ssh  nw102  INGRESS    1000    tcp:22  False  False
nw102-allow-traceroute  nw102  INGRESS    1000    udp:33434-33534  False  False
nw102-allow-traceroute  nw102  INGRESS    1000    udp:33434-33534  False  False
nw102-allow-web  nw102  INGRESS    1000    tcp:22,tcp:80  False  False
```

- 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          us-central1  IN_USE
nat-gw-us-ip  34.121.144.188  EXTERNAL          us-central1  IN_USE
web-ext-16    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-5ae50251747e3"
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

NAME	ZONE	INSTANCE	NAT_POLICY
nat-node-w-eu	eu-central1-c	nl-standard-1	192.168.20.4
faux-on-prem-svc	us-central1-f	nl-standard-1	10.128.0.2 34.71.94.202
nat-gw-us	us-central1-f	nl-standard-1	192.168.10.2 34.121.144.188
nat-node-us	us-central1-f	nl-standard-1	192.168.10.3
nat-node-w-us	us-central1-f	nl-standard-1	192.168.10.4

- 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

VPC network
VPC networks
External IP addresses
Firewall
Routes
VPC network peering
Shared VPC
Serverless VPC access
Packet mirroring

VPC network details
EDIT
DELETE VPC NETWORK

custom-net
Subnet creation mode
Custom subnets
Dynamic routing mode
Regional
DNS server policy
None
Subnets Static internal IP addresses Firewall rules Routes VPC Network Peering Private service connection
Add firewall rule Delete
Filter resources
Columns

Name	Type	Targets	Filters	Protocols / ports	Action	Priority	Logs	Hit count	Last hit
private-fw	Ingress	private-tag	Tags: public-tag	icmp	Allow	1000	Off	—	—
public-fw	Ingress	public-tag	IP ranges: 0.0.0.0/0	icmp	Allow	1000	Off	—	—
ssh-all	Ingress	Apply to all	IP ranges: 0.0.0.0/0	tcp:22	Allow	1000	Off	—	—

Equivalent REST

```

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 = "35.202.68.201" -> (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  false        10.8.1.3     35.202.68.156  RUNNING
nginx-gcloud                        us-central1-c  custom-1-4608      false        10.128.0.4   35.193.86.223  RUNNING
nginx-gcp-ul                        us-central1-c  custom-1-4608      false        10.128.0.2   35.193.86.223  TERMINATED
[root@CentOS task2]# curl 35.202.68.156
Hello from nrabeichykava
[root@CentOS task2]#

```