

Author: Piotr Artman

Student No: C00220223

Course: Cloud Data Centres

Content: Lab 2 – notes and screenshots from creating a Nebula network

## Nebula zero-trust network

### A Certificate Authority

Certificate Authority can be set in any device with Nebula software installed. This software is necessary to create digital signatures used in an authentication process within Nebula mesh network.

### Step by step guide

Follow quick start tutorial available [here](#) [1].

## Instance in Google Cloud Platform

### Creating an instance.

In order to avail a Free Tier in Google Cloud Platform it is necessary to select machine with following parameters[2]:

Machine type: **e2-micro VM instance**

Geographic regions: **Oregon: us-west1, Iowa: us-central1, South Carolina: us-east1**

Disk size: **30 GB-months standard persistent disk.**

Network traffic: **1 GB of outbound data transfer from North America to all region destinations (excluding China and Australia) per month.**

**Note: A free usage of e2-micro instances is based on total hours used across all instances.**


Machine type

Choose a machine type with preset amounts of vCPUs and memory that suit most workloads.  
Or, you can create a custom machine for your workload's particular needs. [Learn more](#)

PRESET

CUSTOM

e2-micro (2 vCPU, 1 core, 1 GB memory)



vCPU

0.25-2 vCPU (1 shared core)

Memory


1 GB

CPU platform

Automatic

Fig. 1. Step 1 - select machine type.

Boot disk

Name	instance-20240401-161717
Type	New balanced persistent disk
Size	10 GB
License type	Free
Image	 Debian GNU/Linux 12 (bookworm)

CHANGE

Fig. 2. Step 2 - select boot disk.

# Boot disk

Select an image or snapshot to create a boot disk; or attach an existing disk. Can't find what you're looking for? Explore hundreds of VM solutions in [Marketplace](#)

PUBLIC IMAGES

CUSTOM IMAGES

SNAPSHOTS

ARCHIVE SNAPSHOTS

EXISTING DISKS

Operating system

Ubuntu

Version \*

Ubuntu 22.04 LTS

x86/64, amd64 jammy image built on 2024-03-19

Boot disk type \*

Balanced persistent disk

COMPARE DISK TYPES

Size (GB) \*

10

Provision between 10 and 3072 GB

Deletion rule

When deleting instance

☐ Keep boot disk

☒ Delete boot disk

Fig. 3. Step 3 - select boot disk type.

## Encryption

Data is encrypted automatically. Select an encryption key management solution.

- ☒ Google-managed encryption key  
No configuration required
- ☐ Customer-managed encryption key (CMEK)  
Manage via [Google Cloud Key Management Service](#)
- ☐ Customer-supplied encryption key (CSEK)  
Manage outside of Google Cloud

## Snapshot schedule

Use snapshot schedules to automate disk backups. [Learn more](#) 

Select a snapshot schedule 

## Device name

Used to reference the device for mounting or resizing.

- ☒ Use a custom device name

Device name \*

Nebula\_lighthouse\_instance

Custom

 [HIDE ADVANCED CONFIGURATION](#)

SELECT

CANCEL

Fig. 4. Step 4 - change of device (instance) name.

## Identity and API access ?

### Service accounts ?

Service account  
Compute Engine default service account

Requires the Service Account User role (roles/iam.serviceAccountUser) to be set for users who want to access VMs with this service account. [Learn more](#)

### 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
- ☒ Allow Load Balancer Health Checks

## Observability - Ops Agent ?

Monitor your system through collection of logs and key metrics.

- ☐ Install Ops Agent for Monitoring and Logging

Fig. 5. Step 5 - select firewall and API related options.

VM instances									
<div>CREATE INSTANCE</div> <div>IMPORT VM</div> <div>REFRESH</div>									
INSTANCES									
OBSERVABILITY									
INSTANCE SCHEDULES									
VM instances									
Filter Enter property name or value									
<input type="checkbox"/>	Status	Name ↑	Zone	Recommendations	In use by	Internal IP	External IP	Labels	Connect
<input type="checkbox"/>	✓	<a href="#">instance-20240401-161717</a>	us-central1-a			10.128.0.2 (nic0)	<a href="#">34.28.64.175</a> (nic0)		SSH

Fig. 6. New instance displayed on Google Cloud Compute Engine control panel.

## Nebula lighthouse on Google Cloud Platform instance.

### Step 1: Download Nebula

```
wget https://github.com/slackhq/nebula/releases/download/v1.8.2/nebula-linux-amd64.tar.gz
```

### Step 2: Extract the Archive

```
tar -xzf nebula-linux-amd64.tar.gz
```

### Step 3: Move Nebula Binaries to '/usr/local/bin'

```
sudo mv nebula /usr/local/bin/
```

```
sudo mv nebula-cert /usr/local/bin/
```

### Step 4: Configuration

```
! lighthouse_config.yaml X
D: > IT Carlow > Y4_2023_2024 > OneDrive - South East Technological University > Y4 2023_2024 > Cloud Data Centers > labs > Lab2 > ! lighthouse_config.yaml
1 # This is the nebula example configuration file. You must edit, at a minimum, the static_host_map, lighthouse, and firewall sections
2 # Some options in this file are HUPable, including the pki section. (A HUP will reload credentials from disk without affecting existing tunnels)
3
4 # PKI defines the location of credentials for this node. Each of these can also be inlined by using the yaml ":" syntax.
5 pki:
6   # The CAs that are accepted by this node. Must contain one or more certificates created by 'nebula-cert ca'
7   ca: /home/peter_artman/ca.crt
8   cert: /home/peter_artman/lighthouse.crt
9   key: /home/peter_artman/lighthouse.key
10 # blocklist is a list of certificate fingerprints that we will refuse to talk to
11 #blocklist:
12 # - c99d4e650533b92061b09918e838a5a0a6a0ee21eed1d12fd937682865936c72
13 # disconnect_invalid is a toggle to force a client to be disconnected if the certificate is expired or invalid.
14 #disconnect_invalid: false
15
16 # The static host map defines a set of hosts with fixed IP addresses on the internet (or any network).
17 # A host can have multiple fixed IP addresses defined here, and nebula will try each when establishing a tunnel.
18 # The syntax is:
19 # "{nebula ip}": [{"routable ip/dns name}:{routable port}"]
20 # Example, if your lighthouse has the nebula IP of 192.168.100.1 and has the real ip address of 100.64.22.11 and runs on port 4242:
21 static_host_map:
22   "192.168.100.1": [{"34.28.64.175:4242"}]
23 lighthouse:
24   # am_lighthouse is used to enable lighthouse functionality for a node. This should ONLY be true on nodes
25   # you have configured to be lighthouses in your network
26   am_lighthouse: true
```

# Certificates used inside Nebula network.

```
nebula nebula-cert nebula-linux-amd64.tar.gz
```

```
(peter@LAPTOP-I062M5BI)-[/mnt/c/Users/peter/Desktop/nebula]  
$ ./nebula-cert ca -name "Piotr Artman, Y4, Cloud Data Centres"
```

```
(peter@LAPTOP-I062M5BI)-[/mnt/c/Users/peter/Desktop/nebula]  
$ ls  
ca.crt ca.key nebula nebula-cert nebula-linux-amd64.tar.gz
```

```
(peter@LAPTOP-I062M5BI)-[/mnt/c/Users/peter/Desktop/nebula]  
$ ./nebula-cert sign -name "lighthouse" -ip "192.168.100.1/24"
```

```
(peter@LAPTOP-I062M5BI)-[/mnt/c/Users/peter/Desktop/nebula]  
$ ./nebula-cert sign -name "laptop_P50" -ip "192.168.100.3/24" -groups "laptop,ssh"
```

```
(peter@LAPTOP-I062M5BI)-[/mnt/c/Users/peter/Desktop/nebula]  
$ ./nebula-cert sign -name "laptop_SurfacePro6" -ip "192.168.100.5/24" -groups "laptop,ssh"
```

```
(peter@LAPTOP-I062M5BI)-[/mnt/c/Users/peter/Desktop/nebula]  
$ ls  
ca.crt          laptop_P50.key      lighthouse.crt      nebula-cert  
ca.key          laptop_SurfacePro6.crt lighthouse.key      nebula-linux-amd64.tar.gz  
laptop_P50.crt  laptop_SurfacePro6.key nebula
```

```
(peter@LAPTOP-I062M5BI)-[/mnt/c/Users/peter/Desktop/nebula]  
$ rm laptop_P50.key lighthouse.crt laptop_SurfacePro6.crt lighthouse.key laptop_P50.crt laptop_SurfacePro6.key
```

```
(peter@LAPTOP-I062M5BI)-[/mnt/c/Users/peter/Desktop/nebula]  
$ ls  
ca.crt ca.key nebula nebula-cert nebula-linux-amd64.tar.gz
```

```
(peter@LAPTOP-I062M5BI)-[/mnt/c/Users/peter/Desktop/nebula]  
$ ./nebula-cert sign -name "lighthouse" -ip "192.168.100.1/24"
```

```
(peter@LAPTOP-I062M5BI)-[/mnt/c/Users/peter/Desktop/nebula]  
$ ./nebula-cert sign -name "laptop_SurfacePro6" -ip "192.168.100.5/24"
```

```
(peter@LAPTOP-I062M5BI)-[/mnt/c/Users/peter/Desktop/nebula]  
$ ./nebula-cert sign -name "laptop_P50" -ip "192.168.100.3/24"
```

```
(peter@LAPTOP-I062M5BI)-[/mnt/c/Users/peter/Desktop/nebula]  
$ ./nebula-cert sign -name "mobile_SamsungS21" -ip "192.168.100.7/24"
```

```
(peter@LAPTOP-I062M5BI)-[/mnt/c/Users/peter/Desktop/nebula]  
$ ls  
ca.crt          laptop_SurfacePro6.crt mobile_SamsungS21.crt nebula-linux-amd64.tar.gz  
ca.key          laptop_SurfacePro6.key mobile_SamsungS21.key  
laptop_P50.crt  lighthouse.crt        nebula  
laptop_P50.key  lighthouse.key        nebula-cert
```

```
(peter@LAPTOP-I062M5BI)-[/mnt/c/Users/peter/Desktop/nebula]  
$
```

# Settings on client machine

```
! laptop_P50_config.yaml X
D: > IT Carlow > Y4_2023_2024 > OneDrive - South East Technological University > Y4 2023_2024 > Cloud Data Centers > labs > Lab2 > ! laptop_P50_config.yaml
1 # This is the nebula example configuration file. You must edit, at a minimum, the static_host_map, lighthouse, and firewall sections
2 # Some options in this file are HUPable, including the pki section. (A HUP will reload credentials from disk without affecting existing tunnels)
3
4 # PKI defines the location of credentials for this node. Each of these can also be inlined by using the yaml ":" |" syntax.
5 pki:
6   # The CAs that are accepted by this node. Must contain one or more certificates created by 'nebula-cert ca'
7   ca: /home/peter/ca.crt
8   cert: /home/peter/laptop_P50.crt
9   key: /home/peter/laptop_P50.key
10  # blocklist is a list of certificate fingerprints that we will refuse to talk to
11  #blocklist:
12  # - c99d4e650533b92061b09918e838a5a0a6aaee21eed1d12fd937682865936c72
13  # disconnect_invalid is a toggle to force a client to be disconnected if the certificate is expired or invalid.
14  #disconnect_invalid: false
15
16 # The static host map defines a set of hosts with fixed IP addresses on the internet (or any network).
17 # A host can have multiple fixed IP addresses defined here, and nebula will try each when establishing a tunnel.
18 # The syntax is:
19 #   "{(nebula ip)}": [{"(routable ip/dns name):(routable port)"}]
20 # Example, if your lighthouse has the nebula IP of 192.168.100.1 and has the real ip address of 100.64.22.11 and runs on port 4242:
21 static_host_map:
22   "192.168.100.1": [{"34.28.64.175:4242"}]
23 lighthouse:
24   # am_lighthouse is used to enable lighthouse functionality for a node. This should ONLY be true on nodes
25   # you have configured to be lighthouses in your network
26   am_lighthouse: false
27 # nebula does not natively support a dns lighthouse that responds to various queries and can even be
```

## REFERENCES:

- [1] "Quick Start - Nebula Docs." Accessed: Apr. 02, 2024. [Online]. Available: <https://nebula.defined.net/docs/guides/quick-start/>
- [2] "Free cloud features and trial offer - Google Cloud Free Program." Accessed: Apr. 01, 2024. [Online]. Available: <https://cloud.google.com/free/docs/free-cloud-features#compute>