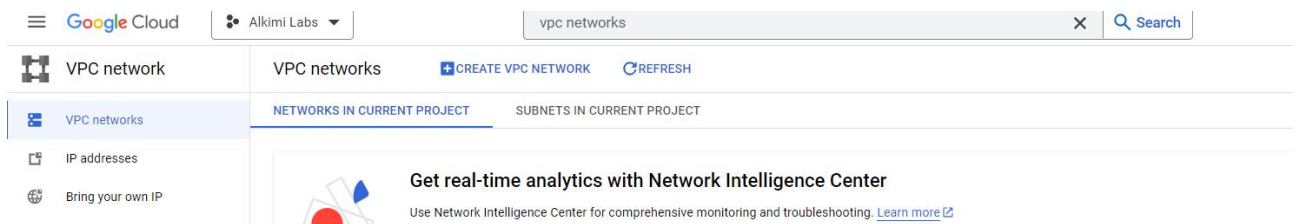


GCP Node Setup procedure

Log on to the GCP console with your credentials.

Setup VPC for the NMS.

Enter “VPC networks” in the search button and click enter.



Click on Create VPC networks and enter details as given below

A screenshot of the 'Create a VPC network' form in the Google Cloud console. The left sidebar shows 'VPC network' and 'VPC networks' (selected). The main content area shows the 'Create a VPC network' form. The form has the following fields: 'Name *' with the value 'nms-vpc' and a help icon; 'Description' with the value 'VPC network for NMS nodes' and a help icon; 'Maximum transmission unit (MTU)' with a dropdown menu showing '1460' and a help icon. Below these fields, there is a section for 'VPC network ULA internal IPv6 range' with a help icon. This section includes a description: 'Enabling this feature will assign a /48 from Google defined ULA prefix fd20::/20.' and two radio buttons: 'Enabled' and 'Disabled' (selected).

Enter subnet details as given below

VPC network

VPC networks

IP addresses

Bring your own IP

Firewall

Routes

VPC network peering

Shared VPC

Serverless VPC access

Packet mirroring

Create a VPC network

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](#)

Subnet creation mode ?

☒ Custom

☐ Automatic

New subnet

Name *

nms-subnet

Lowercase letters, numbers, hyphens allowed

Description

Subnet for NMS nodes

Region *

europa-west2

IP stack type

☒ IPv4 (single-stack)

☐ IPv4 and IPv6 (dual-stack) ?

IPv4 range *

10.0.0.0/24

E.g. 10.0.0.0/24

CREATE SECONDARY IPV4 RANGE

Private Google Access ?

☐ On

☒ Off

Flow logs

Turning on VPC flow logs doesn't affect performance but some systems generate a large number of logs, which can increase costs in Logging. [Learn more](#)

☐ On

☒ Off

DONE

Click on Done .

In the Firewall rules select nms-vpc-allow-ssh as shown below.

Firewall rules ?

Select any of the firewall rules below that you would like to apply to this VPC network.
Once the VPC network is created, you can manage all firewall rules on the Firewall rules page.

IPv4 FIREWALL RULES

	Name	Type	Targets	Filters	Protocols / ports	Action	Priority ↑	
<input type="checkbox"/>	nms-vpc-allow-custom ?	Ingress	Apply to all	IP ranges: 10.0.0.0/24	all	Allow	65,534	EDIT
<input type="checkbox"/>	nms-vpc-allow-icmp ?	Ingress	Apply to all	IP ranges: 0.0.0.0/0	icmp	Allow	65,534	
<input type="checkbox"/>	nms-vpc-allow-rdp ?	Ingress	Apply to all	IP ranges: 0.0.0.0/0	tcp:3389	Allow	65,534	
<input checked="" type="checkbox"/>	nms-vpc-allow-ssh ?	Ingress	Apply to all	IP ranges: 0.0.0.0/0	tcp:22	Allow	65,534	
	nms-vpc-deny-all-ingress ?	Ingress	Apply to all	IP ranges: 0.0.0.0/0	all	Deny	65,535	
	nms-vpc-allow-all-egress ?	Egress	Apply to all	IP ranges: 0.0.0.0/0	all	Allow	65,535	

Dynamic routing mode ?

- ☒ **Regional**
Cloud Routers will learn routes only in the region in which they were created
- ☐ **Global**
Global routing lets you dynamically learn routes to and from all regions with a single VPN or interconnect and Cloud Router

DNS server policy

CREATE

CANCEL

And then click on Create to create a VPC.

Once VPC is created, it is time to set up a Network Firewall Policy.

Search for "Firewall policies" as below and select Firewall Policies

Alkimi Labs

Firewall policies

Search

ALL DOCUMENTATION AND TUTORIALS RESOURCES MARKETPLACE ANI

Filter by

- ☐ Product or page
- ☐ Documentation or tutorial
- ☐ Marketplace and APIs
- ☐ Organisation

Search results

Showing 30 of 49 results for "Firewall policies".

Firewall policies
Network security

and click on Create Firewall Policy

Enter Firewall policy details as below

Network Security

Secure Web Proxy

Cloud Armor

- Cloud Armor policies
- Adaptive Protection
- Managed Protection

Cloud IDS

- IDS Dashboard
- IDS Endpoints
- IDS Threats

Cloud Firewall

Create a network firewall policy

1 Configure policy

Policy name *
nms-node-firewall-policy

Lowercase letters, numbers, hyphens allowed

Description
Firewall Policy for NMS nodes

Deployment scope

- Global
- Regional

Region
europe-west2 (London)

CONTINUE

Click on Continue to Add Rule

Google Cloud

Alkimi Labs

Firewall policies

Network security

Secure web proxy

Cloud Armor

- Cloud Armor policies
- Adaptive protection
- Managed protection

Cloud IDS

- IDS dashboard
- IDS endpoints

Create a network firewall policy

✓ Configure policy

2 Add rules

Firewall rules

Firewall rules control incoming or outgoing traffic to an instance. By default, all traffic is delegated to next level. [Learn more](#)

Google Cloud threat intelligence and geolocation are firewall standard rules, which are paid features

ADD RULEDELETE

Click on ADD RULE to add Firewall Rule

Enter firewall rule details as below

Create a firewall rule

Priority *
1000 ?

Priority can be 0 – 2147483643.

Description
NMS Firewall rules

Direction of traffic ?

☒ Ingress
☐ Egress

Action on match ?

☒ Allow
☐ Deny
☐ Go to next

Logs

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

☐ On
☒ Off

Target

Target type
All instances in the network ?

Source

IP type
IPv4

IP ranges
0.0.0.0/0 ?

Tags

[SELECT SCOPE](#)

Select "Specified protocols and ports" as shown below

Then Enter port details as below for Guardian Nodes (For Master Node check next Step)

Destination

IP type
None ▼

Protocols and ports ?

- ☐ Allow all
- ☒ Specified protocols and ports

☒ TCP

Ports

8000-8001,9000,9065-9066

E.g. 20, 50-60

☐ UDP

Ports

E.g. all

☐ Other

Protocols

Separate multiple protocols by commas, e.g. ah, sctp

CREATE

CANCEL

OR enter port details as below for Master node

Destination

IP type

None



Protocols and ports

☐ Allow all

☒ Specified protocols and ports

☒ TCP

Ports

8000-8001,9000,19001-19004

E.g. 20, 50-60

☐ UDP

Ports

E.g. all

☐ Other

Protocols

Separate multiple protocols by commas, e.g. ah, sctp

CREATE

CANCEL

and Click on Create.

Network Security

Secure Web Proxy

Cloud Armor

Cloud Armor policies

Adaptive Protection

Managed Protection

Cloud IDS

IDS Dashboard

IDS Endpoints

IDS Threats

Cloud Firewall

Firewall policies

Threats

Firewall endpoints

Common components

Security profiles

SSL policies

Client Authentication

Create a network firewall policy

<input type="checkbox"/>	Priority	Description	Direction of traffic	Targets	Source	Destination	Protocols and ports	Action	Security profile group	TLS inspection
<input type="checkbox"/>	2147483545	Deny known malicious IPs egress traffic	Egress	Appl...	—	Google Cloud T	all	Deny	—	—
<input type="checkbox"/>	2147483544	Deny known malicious IPs ingress traffic	Ingress	Appl...	Google Cloud T	—	all	Deny	—	—
<input type="checkbox"/>	2147483546	Deny sanctioned countries ingress traffic	Ingress	Appl...	Geolocations: C	—	all	Deny	—	—
<input type="checkbox"/>	2147483543	Deny TOR exit nodes ingress traffic	Ingress	Appl...	Google Cloud T	—	all	Deny	—	—
<input type="checkbox"/>	2147483541	Exclude communication with private IP ranges, leaving only internet traffic to be inspected	Egress	Appl...	—	IPv4 ranges: 10	all	Go to next	—	—
<input type="checkbox"/>	2147483542	Exclude communication with private IP ranges, leaving only internet traffic to be inspected	Ingress	Appl...	IPv4 ranges: 10	—	all	Go to next	—	—
<input type="checkbox"/>	1000	Nms Firewall rules	Ingress	Appl...	IPv4 ranges: 0.1	—	tcp:8000-8001, 9000, 19000-19004, 19011-19014	Allow	—	—

CONTINUE

Click on Continue

Associate this with the VPC created already

Google Cloud

Alkimi Labs

Firewall policies

Network security

Secure web proxy

Cloud Armor

Cloud Armor policies

Adaptive protection

Managed protection

Cloud IDS

IDS dashboard

IDS endpoints

IDS threats

Cloud firewall

Firewall policies

Create a network firewall policy

Configure policy

Add rules

Associate policy with VPC networks (optional)

You can associate network firewall policy with a network. Associating a policy with a network applies the policy rules to targets in the network.

ASSOCIATE

DELETE

You can associate the policy with VPC networks after it is created.

CONTINUE

CREATE

CANCEL

Click on Associate.

Select the VPC network name created in earlier steps.

Associate policy with VPC networks

Select the VPC networks to associate this policy with


 **Filter** Enter property name or value 


	Network name 	Subnets	Regions
<input type="checkbox"/>	alkimi-exchange-prod	1	1
<input checked="" type="checkbox"/>	alkimi-labs	1	1
<input type="checkbox"/>	default	41	41

ASSOCIATE CANCEL


After Selecting network Click on Continue


And finally click on Create


 Google Cloud


Alkimi Labs 


 Firewall policies


 Network security


 Secure web proxy


Cloud Armor 

 Cloud Armor policies

 Adaptive protection

 Managed protection

Cloud IDS 

 Create a network firewall policy

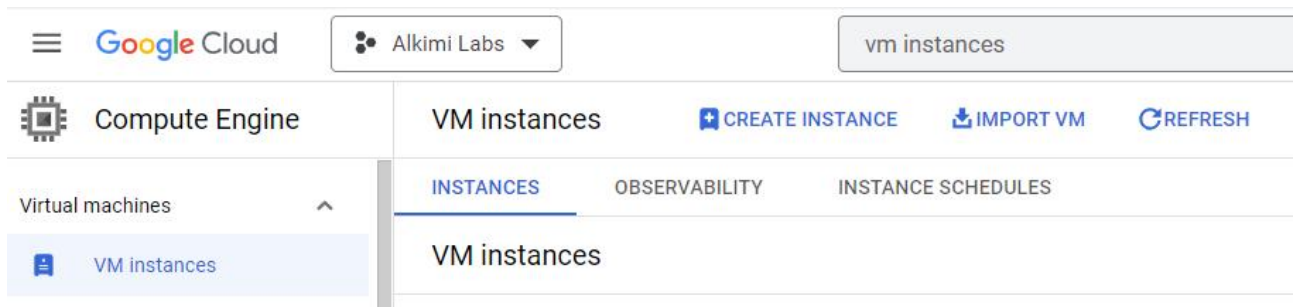
☒ Configure policy

☒ Add rules

☒ Associate policy with VPC networks (optional)

CREATE CANCEL

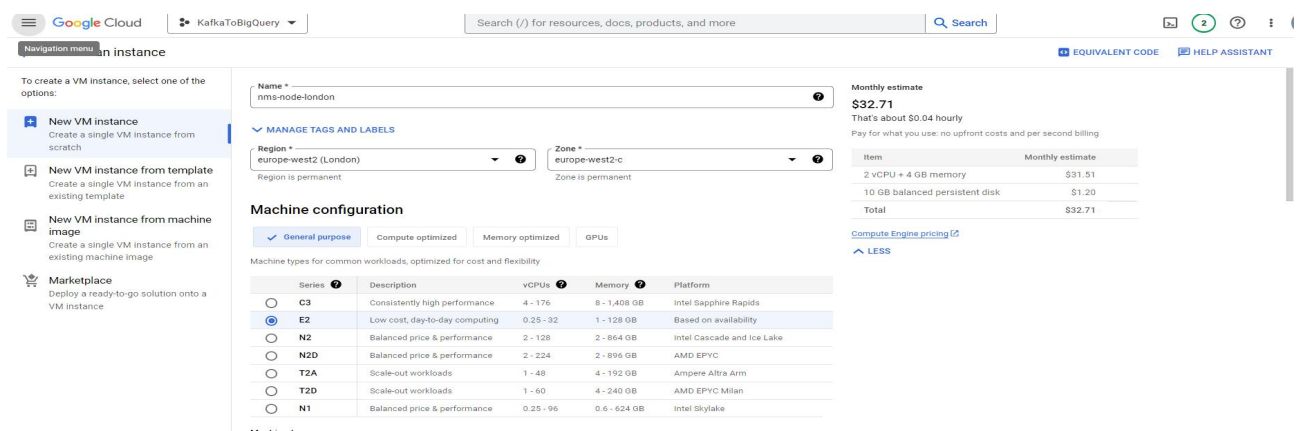
Now a VM instance has to be created. Search for “VM instances”



Now click on Create Instance as shown below

Create Instance shows below screen. Enter the name of the VM instance in the Name field.

Select europe-wes2 (London) region from Region field.



Now in Machine Type please select Custom option and enter suggested number of CPUs and Memory combinations as below

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](#)

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](#)

CUSTOM

Cores

2



32

8

vCPU

(4 core)

Memory

4



64

16

GB

Availability policies

- VM provisioning model
Standard

Choose 'Spot' to get a discounted, pre-emptible VM. Otherwise, stick to 'Standard'. [Learn more](#)

✓ VM PROVISIONING MODEL ADVANCED SETTINGS

Deploy a container image to this VM instance

DEPLOY CONTAINER

Boot disk ?

Name	nms-node
Type	New balanced persistent disk
Size	10 GB
Licence type ?	Free
Image	 Debian GNU/Linux 11 (bullseye)

CHANGE

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

Now click on Change in Boot disk

Enter Operating System - Ubuntu, Version - Ubuntu 20.04 LTS(x86/64) and disk size (320GB) as given below.

Ubuntu 20.04 LTS

x86/64, amd64 focal image built on 2023-10-25

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 20.04 LTS

x86/64, amd64 focal image built on 2023-10-25

Boot disk type *

Balanced persistent disk

COMPARE DISK TYPES

Size (GB) *

320

Provision between 10 and 65536 GB

SHOW ADVANCED CONFIGURATION

SELECT

CANCEL

Please make sure Version is selected as below

Ubuntu 20.04 LTS

x86/64, amd64 focal image built on 2023-09-18

And click on SELECT

Now select/expand Advanced Options

☐ Install Ops Agent for monitoring and logging

Advanced options





Networking, disks, security, management, sole-tenancy



Now select/expand Networking and select the VPC created earlier in "Network Interfaces" as given below.

[← Create an instance](#)

To create a VM instance, select one of the options:

-  **New VM instance**
Create a single VM instance from scratch
-  **New VM instance from template**
Create a single VM instance from an existing template
-  **New VM instance from machine image**
Create a single VM instance from an existing machine image
-  **Marketplace**
Deploy a ready-to-go solution onto a VM instance

Networking

Hostname and network interfaces

Network tags

Hostname

Set a custom hostname for this instance or leave it default. Choice is permanent

IP forwarding ☐ Enable

Network performance configuration

- Network interface card

Network bandwidth ?

☐ Enable per VM Tier_1 networking performance

Maximum outbound network bandwidth: 2Gbps

VM to Public IP: 2Gbps

Network interfaces ?

Network interface is permanent

Edit network interface

Network * ———
nms-vpc-network

Subnetwork * _____
nms-nodes-subnet IPv4 (10.0.0.0/24)

Now click on Done

Network Service Tier

 Premium

☐ Standard (europa-west2) ?


Public DNS PTR Record ?

☐ Enable for IPv4

PTR domain name

DONE

Click on Create now to create the instance. Once VM is created it is shown as below


Compute Engine

VM instances

[CREATE INSTANCE](#)
[IMPORT VM](#)
[REFRESH](#)

Virtual machines

VM instances

Instance templates

Sole-tenant nodes

Machine images

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	Connect
<input type="checkbox"/>		nms-node-london	us-central1-a			10.128.0.21 (nic0)	35.184.140.68 (nic0)	SSH ▾ ⋮

Note down the External IP (highlighted in the image above).

Node Registration Procedure (GCP).

Now the VM instance is created, it is time to connect and install NMS software.

To connect the VM instance click on SSH on the VM Instance dashboard as given below

VM instances

CREATE INSTANCE

IMPORT VM

REFRESH

HELP ASSISTANT

LEARN

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	Connect	
<input type="checkbox"/>		nms-node-london	europe-west2-c			10.154.0.4 (nic0)	35.246.96.47 (nic0)	SSH	⋮

