Infoblox

DEPLOYMENT GUIDE

Infoblox vNIOS for Google Cloud Platform (GCP)

Table of Contents

Introduction

Infoblox vNIOS for Google Cloud Platform (GCP) is a virtualized Infoblox appliance designed for deployment as a virtual machine (VM) instance in Google Cloud Platform.

Infoblox vNIOS for GCP enables you to deploy robust, manageable, and cost effective Infoblox appliances in the Google Cloud. Infoblox NIOS is the underlying software running on Infoblox appliances and provides core network services and a framework for integrating all the components of the modular Infoblox solution. It provides integrated, secure, and easy-to-manage DNS (Domain Name System), IPAM (IP address management), DHCP (Dynamic Host Configuration Protocol) and other services.

Infoblox vNIOS for GCP appliances can either be joined to an existing on-premises or hybrid/multi cloud grid, or the entire grid can run in GCP. The vNIOS appliance can be configured as a primary DNS server for your GCP VPCs. You can also use Infoblox Cloud Network Automation with vNIOS for GCP to improve visibility of cloud resources and increase the flexibility of your cloud environment.

Prerequisites

The following are prerequisites for deploying an Infoblox vNIOS for GCP appliance:

- Valid subscription in GCP.
- Appropriate permissions in GCP to create a VM instance and other required resources.
- Infoblox Support account at https://support.infoblox.com.
- Understanding of basic networking concepts and tools, including public and private IP addressing, DNS, Secure Shell (SSH), and command line/terminal applications.

Limitations

The following general limitations apply for Infoblox vNIOS for GCP appliances:

- Only provides the LAN1 and MGMT (not enabled by default) interfaces.
- No High Availability (HA) support.
- No native GCP support for Anycast with NIOS.
- DHCP can be served for on-prem clients only, not for clients running in GCP.

Basic Workflow

The following bullet points provide a basic outline of steps that an administrator new to GCP may follow when creating an Infoblox vNIOS VM:

- Install GCloud CLI and gsutil.
- Navigate to GCP: https://console.cloud.google.com/.
- Create one or two new VPCs and Subnets (NIOS 8.5 and 8.4 require two network interfaces, each in a separate VPC. Starting with NIOS 8.6, you can deploy one or two network interfaces).
- Upload image file and Create custom image.
- Launch your Infoblox vNIOS for GCP appliance using the custom image.
- Once the Infoblox vNIOS for GCP appliance has successfully deployed, verify its IP configuration.
- Connect to the Infoblox vNIOS for GCP appliance and begin using it.

Best Practices

- For maximum availability, Infoblox appliances should be deployed across as many different Availability Zones and Regions as needed.
- Promptly change the default admin password in NIOS.
- Use Name Server Groups to simplify name server assignments for DNS configurations.

GCP Objects and Terms

Before implementing Infoblox vNIOS for GCP, an administrator should understand common terms or objects available in GCP related to the implementation of vNIOS. The following are common objects and terms:

- **VPC**: Virtual Private Clouds provide network functionality for Compute Engine and other resources. Networks and subnets are found within VPCs.
- **Shared VPC**: Shared VPCs allow resources from multiple projects to connect to a central VPC network, providing connectivity between all resources using private IP addresses.
- **Persistent Disk**: Block storage used for virtual machine instance disks.
- **Cloud Storage**: Object storage with options suitable for many use-cases.
- **Instance Availability Policies**: Used to control a VM's maintenance or restart behavior.
- **GCloud CLI**: A CLI tool installed locally that enables you to script operations and to create and manage services and resources in GCP.
- **GSUTIL**: A CLI tool for managing Google Storage resources.
- **Instance:** A virtual machine (VM) deployed in GCP.
- **Compute Engine:** Infrastructure as a Service (IaaS) offering on Google Cloud that provides VMs and other compute workloads.
- **Bucket:** Basic organizational containers that hold data and objects in Google Cloud storage.
- **Region:** A collection of datacenters in a specific geographic area where you can choose to host resources.
- **Zone:** Often referred to as an Availability Zone. An isolated location within a Region. Some resources, such as VM instances are zonal, meaning they are contained in a single zone. Other resources, including subnets span multiple zones in a region.
- **Cloud Interconnect:** A highly available, low latency connection between your on-premises network and Google Cloud. Can also connect through a partner service provider.

Source: https://cloud.google.com/docs/

Infoblox vNIOS for GCP Use Cases

The following are common use cases for the Infoblox vNIOS for GCP appliance:

- Providing DNS and RPZ/DNS Firewall services from within the Google Cloud for GCP, on-prem, and other cloud-based clients.
- Expanding services to the GCP cloud for additional fault tolerance and disaster recovery (DR) purposes.
- Providing services with maximum availability across multiple zones and regions.

The DNS and RPZ Services Use Case

In this use case, DNS and RPZ services are hosted in GCP. This enables you to distribute enterprise DNS services for clients operating in GCP, on-prem, and across the Internet. One or more Infoblox vNIOS for GCP appliances are deployed in GCP across as many different zones and regions as feasible. These appliances can also be integrated with an existing Grid, either on-prem or in the cloud. Clients are then updated to use your Infoblox vNIOS for GCP appliance(s) for DNS resolution, providing them with your enterprise DNS and RPZ services.

The Fault Tolerance and Disaster Recovery Use Case

This use case is for Fault Tolerance and Disaster Recovery. In case of failure in the Primary Datacenter (power outage, network outage, or other critical failure) an Infoblox vNIOS for GCP appliance enabled as a Grid Master Candidate (GMC) can be promoted to the Grid Master role so that Grid services can continue to operate. DNS services can also be redirected to servers operating in GCP, possibly without even requiring any manual intervention and helping ensure that business continues to function.

DHCP Service for On-Premises Clients

A vNIOS appliance running on GCP can provide DHCP service for your on-premises clients. This DHCP appliance can serve as your primary DHCP server or be configured as part of a failover pair with a NIOS DHCP server running on-premises for a hybrid, survivable solution. Two vNIOS appliances, each running in GCP could also be configured for DHCP failover for highly available, fault tolerant DHCP services. Using a vNIOS appliance running on GCP for DHCP requires using DHCP Relay or IP Helper on your router or layer 3 switch to send DHCP traffic from your on-premises network to your GCP VPC.

The Maximum Availability Use Case

In many cases, it can be a challenge to implement services in a way that maximizes availability across a distributed environment in a secure manner and without deploying more resources than are required. One method for accomplishing this may be by leveraging a ‘shared services VPC Network’ where critical services, including your Infoblox servers, operate from. VPC Network Peering can be used to connect other VPC Networks to the management VPC Network.

This allows for seamless communications between those VPC Networks and the shared services VPC Network, without allowing connectivity between the other subnets. Traditional routing and/or VPN’s can also be used to allow connectivity into the shared services VPC Network for VPC Networks which cannot leverage VPC Network Peering, or even from networks outside of GCP.

Install GCP Command Line Tools

Uploading and creating the custom image used to deploy vNIOS in GCP requires the use of GCP command line tools. This section describes how to install these tools prior to starting deployment.

GCloud CLI

One tool that is required is the GCloud CLI. The steps to install the GCloud CLI will vary depending on your operating system. Visit https://cloud.google.com/sdk/gcloud/ for installation instructions and to download the installer for your operating system.

Make sure to install the GCloud CLI before proceeding through this guide. Once installed, run the command **gcloud auth login** to login and start your session. This will open a browser window. Follow the prompts to complete the login process.

GSUTIL

Another tool that is optional here is the GSUTIL (Google Storage Utilities), an open-source project available on GitHub. This command line tool is used to interact with GCP storage objects and buckets. The project page can be found at https://github.com/GoogleCloudPlatform/gsutil/.

Installation instructions will vary depending on your operating system version and can be found at https://cloud.google.com/storage/docs/gsutil_install.

For additional references and usage information, visit https://cloud.google.com/storage/docs/gsutil.

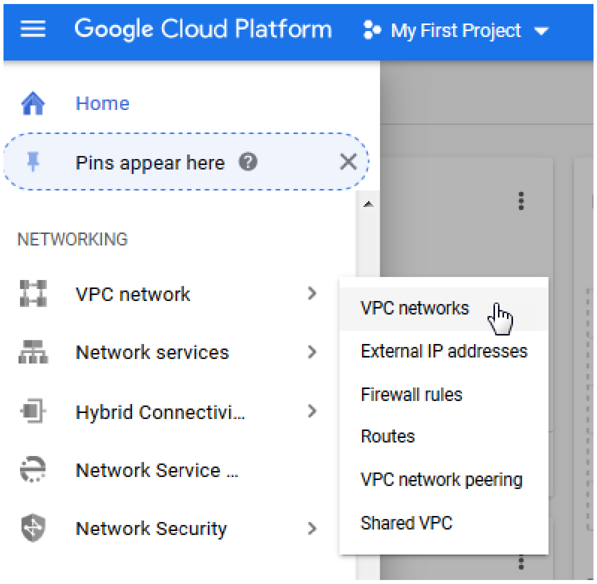
Prepare your GCP Environment

Once you install the necessary tools and login to your GCP account, you are ready to begin setup of resources such as the VPC networks and Firewall rules. These will be required before you can deploy and use any virtual machines.

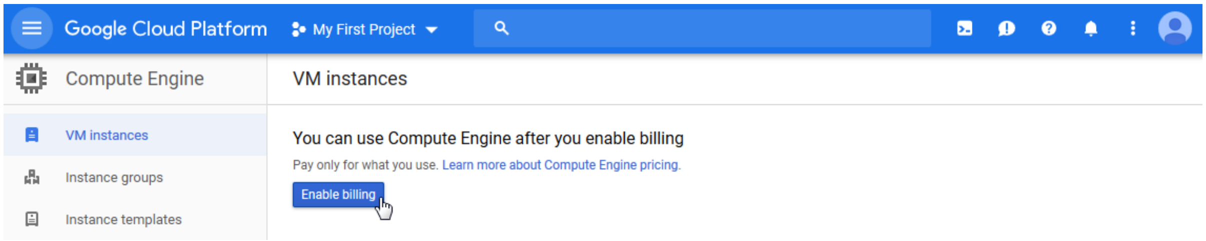
Create VPCs

To create your VPCs and subnets, login to the GCP Console.

1. In the **Navigation menu**, expand **VPC network** and select **VPC networks**.



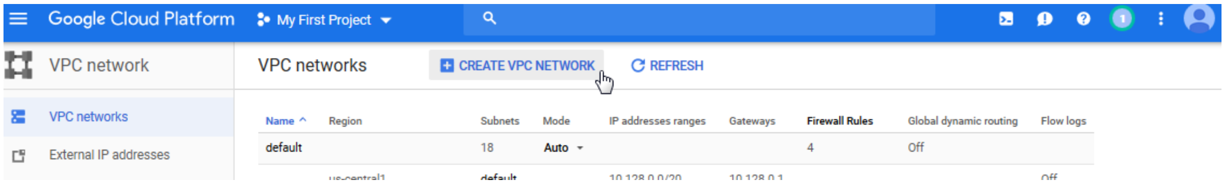
2. If prompted, click **Enable billing** (This is required for first time use on a new account).



You can use Compute Engine after you enable billing

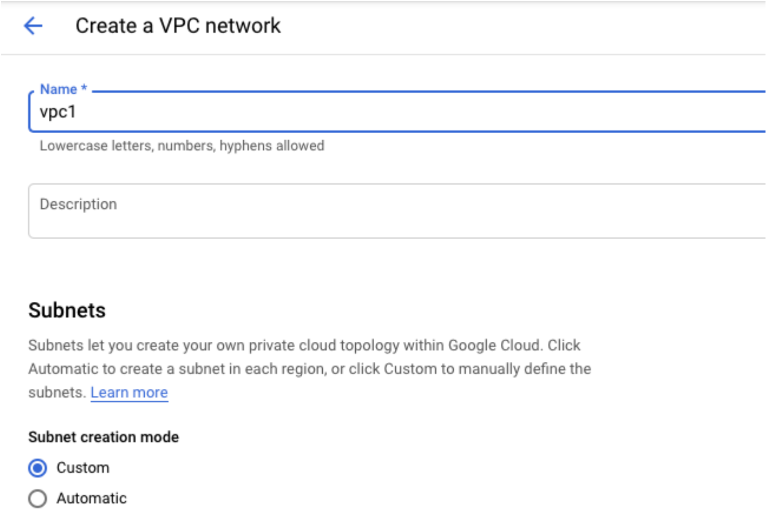
Pay only for what you use. Learn more about Compute Engine pricing.

3. Click **CREATE VPC NETWORK**.



Name	Region	Subnets	Mode	IP addresses ranges	Gateways	Firewall Rules	Global dynamic routing	Flow logs
default		18	Auto			4	Off	
	us-central1	default		10.128.0.0/20	10.128.0.1			Off

4. Type a name, description (optional) and set the **Subnet creation mode** to **Custom**.


Create a VPC network

Name *: vpc1

Lowercase letters, numbers, hyphens allowed

Description

Subnets

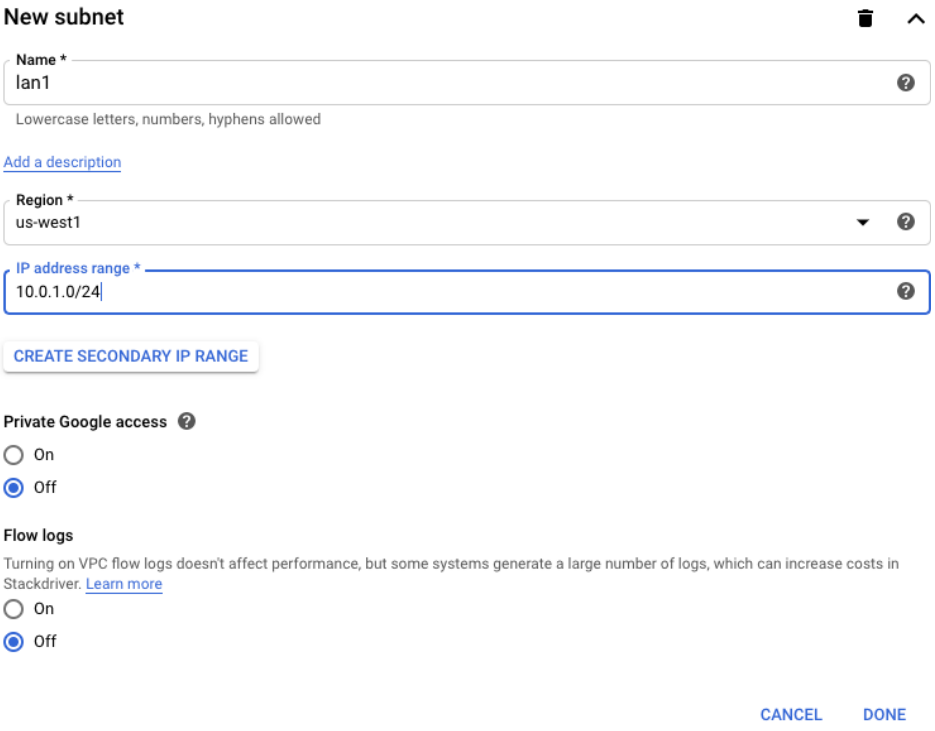
Subnets let you create your own private cloud topology within Google Cloud. Click Automatic to create a subnet in each region, or click Custom to manually define the subnets. Learn more

Subnet creation mode

● Custom

○ Automatic

5. Type a name for your subnet.
6. Expand the **Region** menu and select the region for your subnet.
7. Type the IP address range for your subnet. Example: **10.0.1.0/24**.
8. Click **Done** for the subnet.


New subnet

Name *: lan1

Lowercase letters, numbers, hyphens allowed

Add a description

Region *: us-west1

IP address range *: 10.0.1.0/24

Private Google access

○ On

● Off

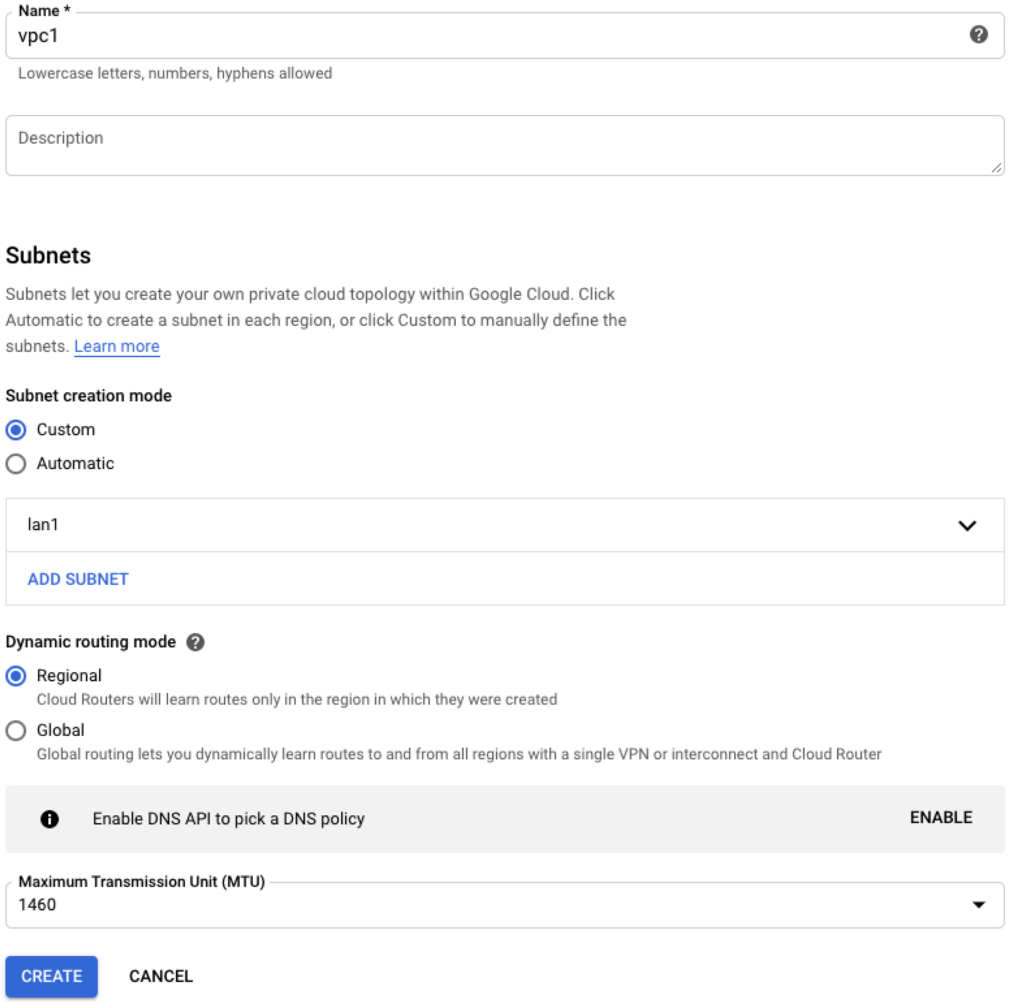
Flow logs

Turning on VPC flow logs doesn't affect performance, but some systems generate a large number of logs, which can increase costs in Stackdriver. Learn more

○ On

● Off

9. Click **CREATE**.



Name *
vpc1
Lowercase letters, numbers, hyphens allowed

Description

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

lan1

ADD SUBNET

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

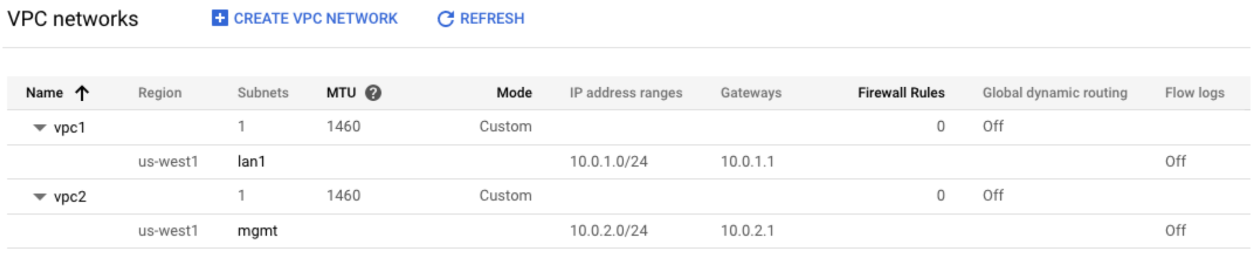
Enable DNS API to pick a DNS policy ENABLE

Maximum Transmission Unit (MTU)
1460

CREATE CANCEL

Note: Starting with NIOS version 8.6, instances can be deployed with either one or two NICs. For older NIOS versions, two NICs and two VPC networks are required when deploying vNIOS for GCP appliances. If required or desired, repeat the above steps to create a second VPC network with a subnet in the same region, using a different address range.

10. Wait and verify that your VPC network(s) are created successfully.



VPC networks CREATE VPC NETWORK REFRESH

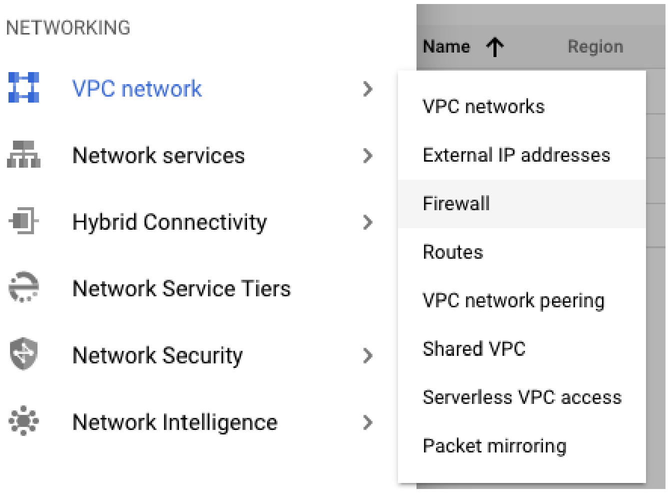
Name ↑	Region	Subnets	MTU	Mode	IP address ranges	Gateways	Firewall Rules	Global dynamic routing	Flow logs
▾ vpc1		1	1460	Custom			0	Off	
	us-west1	lan1			10.0.1.0/24	10.0.1.1			Off
▾ vpc2		1	1460	Custom			0	Off	
	us-west1	mgmt			10.0.2.0/24	10.0.2.1			Off

Create Firewall Rules

The firewall rules are used to control network access into and out of your VPC networks. In this example, we walk through the steps to create a rule to allow all egress (outbound) traffic from your Infoblox vNIOS for GCP instance and a rule to allow ingress (inbound) traffic on specific ports.

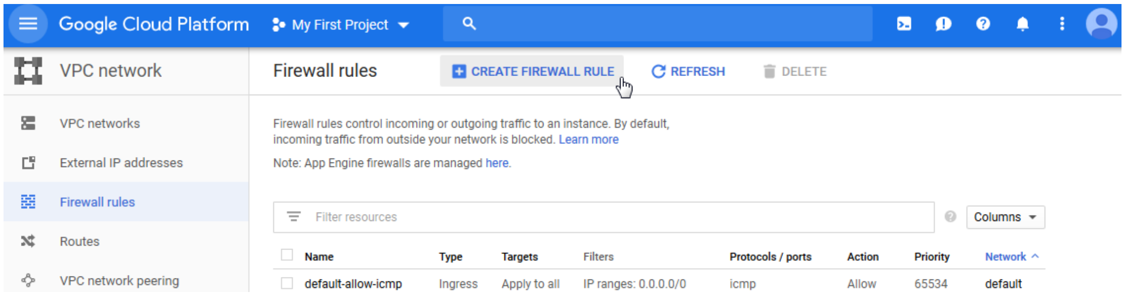
Note: Examples shown here are overly permissive, allowing traffic from any IP, and are for example purpose only. Use best practices in your environment, allowing only the minimal traffic necessary.

1. In the **Navigation menu**, expand the **VPC network** and select **Firewall**.



Create Outbound Rules

2. Click **CREATE FIREWALL RULE**.



Firewall rules control incoming or outgoing traffic to an instance. By default, incoming traffic from outside your network is blocked. Learn more

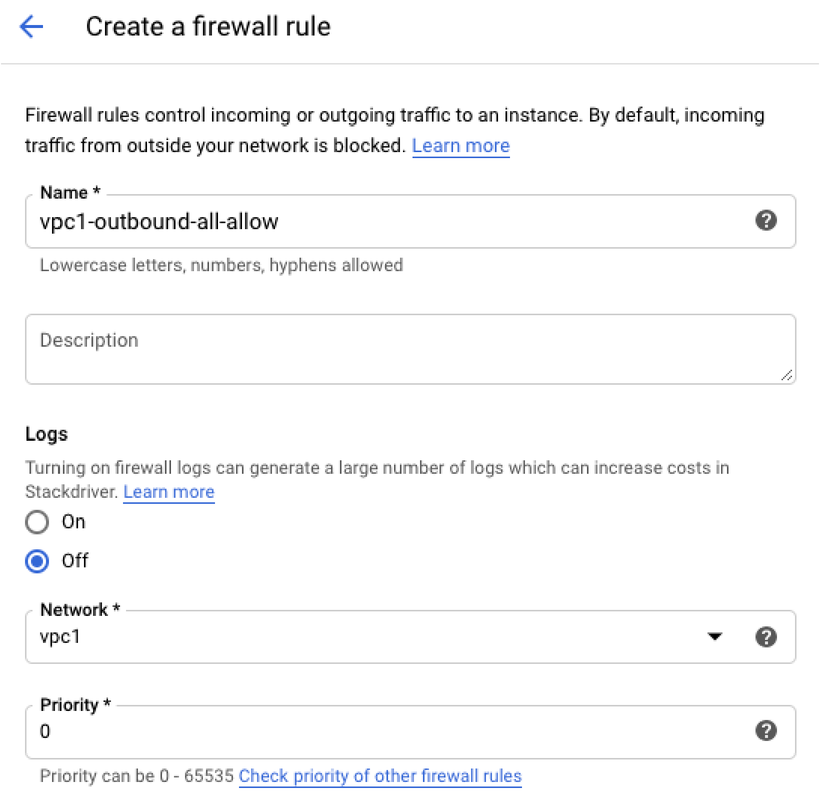
Note: App Engine firewalls are managed here.

	Name	Type	Targets	Filters	Protocols / ports	Action	Priority	Network
□	default-allow-icmp	Ingress	Apply to all	IP ranges: 0.0.0.0/0	icmp	Allow	65534	default

3. Type a name and (optional) a description.

Note: To make it easy to identify the rules you are creating for your VPC, prefix the rule name with your VPC name. Example: **vpc1-outbound-all-allow**.

4. Expand the **Network** menu and select your VPC network.
5. The priority is used to control the order in which the firewall rules are processed, starting from 0. GCP uses a default of 1000. In this example, we will first set the Egress rule to allow all outbound traffic, so we will change this to **0**.



Create a firewall rule

Firewall rules control incoming or outgoing traffic to an instance. By default, incoming traffic from outside your network is blocked. Learn more

Name *
vpc1-outbound-all-allow
Lowercase letters, numbers, hyphens allowed

Description

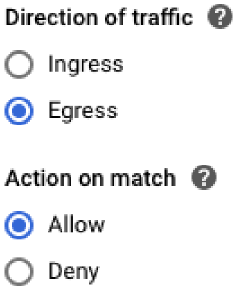
Logs
Turning on firewall logs can generate a large number of logs which can increase costs in Stackdriver. Learn more

○ On
● Off

Network *
vpc1

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

6. Set the **Direction of traffic** to **Egress** and **Action on match** to **Allow**.



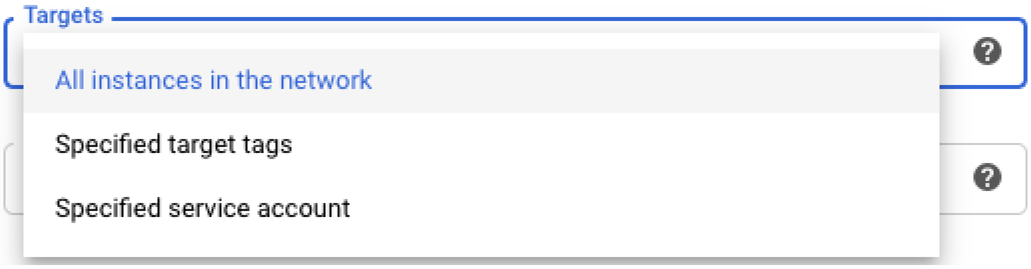
Direction of traffic

○ Ingress
● Egress

Action on match

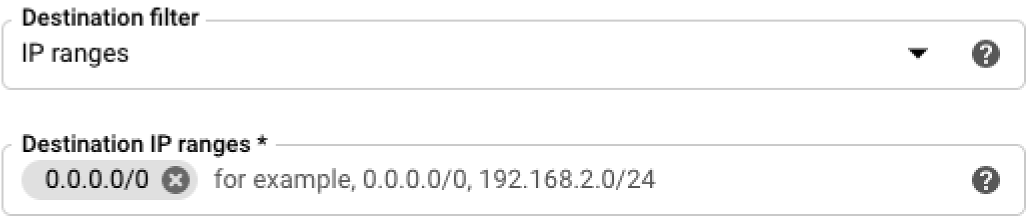
● Allow
○ Deny

7. Expand the **Targets** menu and select **All instances in the network**.



Targets

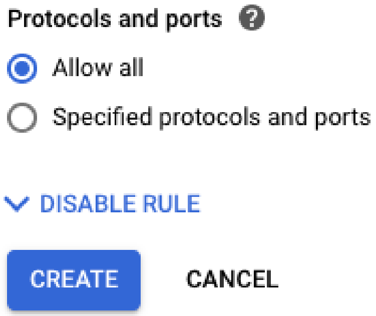
8. For the **Destination filter** select **IP ranges**.
9. For the **Destination IP ranges**, enter **0.0.0.0/0** to allow outbound traffic to any destination.



Destination filter: IP ranges

Destination IP ranges *: 0.0.0.0/0

10. Toggle the **Protocols and ports** option to **Allow all**.
11. Click **CREATE**.



Protocols and ports

● Allow all

○ Specified protocols and ports

12. If you are deploying an instance with two NICs, repeat the above process to create an outbound rule for your second VPC.

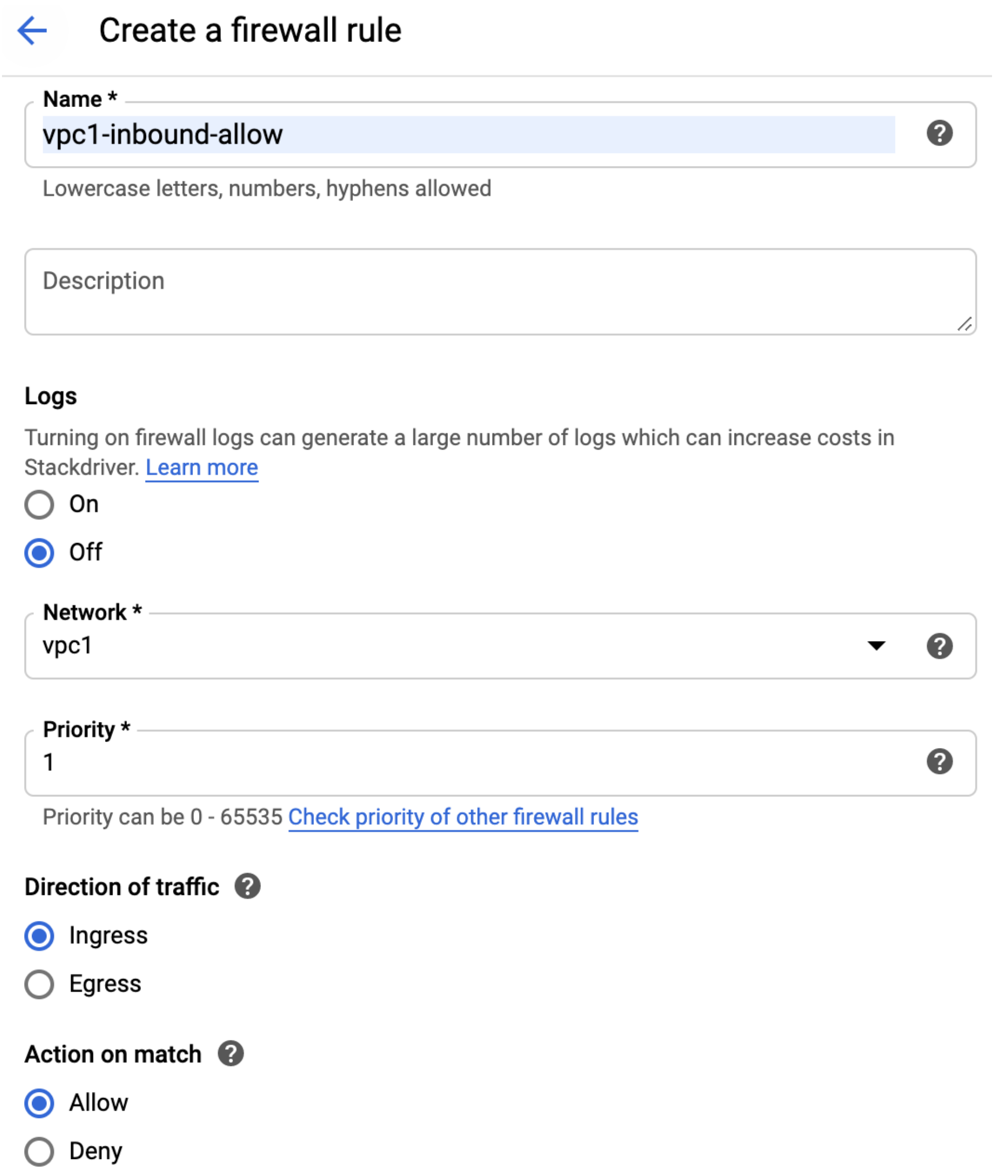
Create Inbound Rules

Next, we'll create a firewall rule to allow appropriate traffic inbound to the VPC for the vNIOS instances. For full details on ports and protocols used by Infoblox NIOS, refer to NIOS documentation at https://docs.infoblox.com.

1. Click **CREATE FIREWALL RULE**.
2. Type a name and (optional) a description.

Note: To make it easy to identify the rules you are creating for your VPC, prefix the rule name with your VPC name. Example: **vpc1-inbound-allow**.

3. Select your VPC network and set the Priority.
4. Set the **Direction of traffic** to **Ingress** and **Action on match** to **Allow**.



Create a firewall rule

Name *
vpc1-inbound-allow
Lowercase letters, numbers, hyphens allowed

Description

Logs
Turning on firewall logs can generate a large number of logs which can increase costs in Stackdriver. Learn more
○ On
● Off

Network *
vpc1

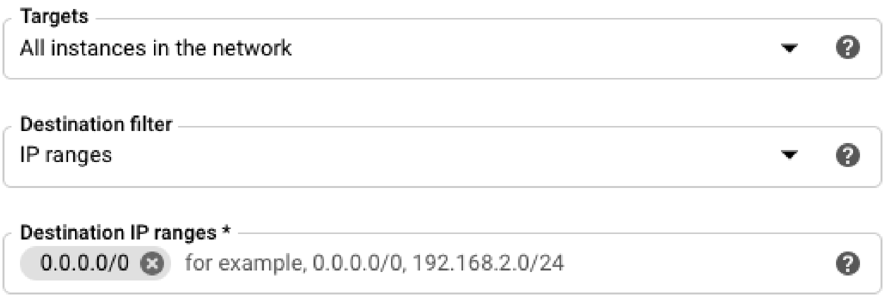
Priority *
1
Priority can be 0 - 65535 Check priority of other firewall rules

Direction of traffic
● Ingress
○ Egress

Action on match
● Allow
○ Deny

5. Expand the **Targets** menu and select **All instances in the network**.
6. Expand the **Source filter** menu and select **IP ranges**.
7. For the Source IP ranges, enter 0.0.0.0/0 to allow traffic from anywhere.

Note: For security of production environments, limit the source IP ranges.

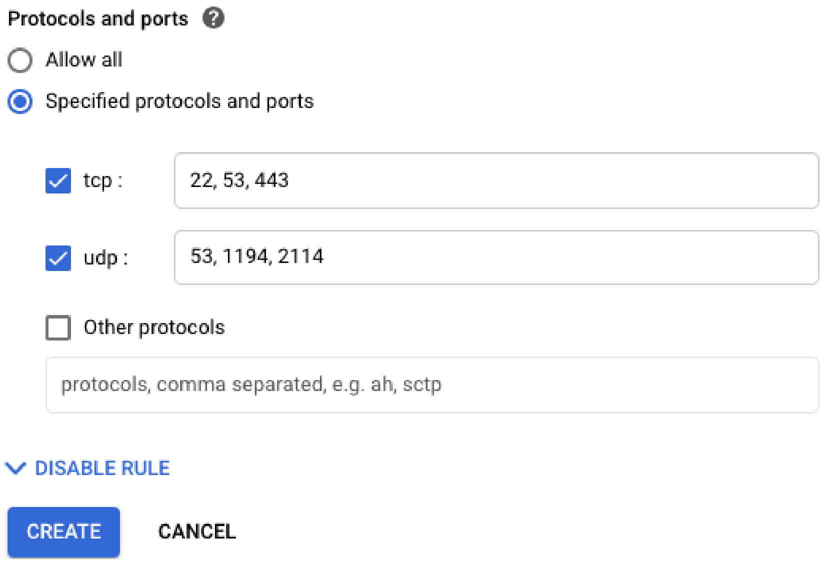


Targets
All instances in the network

Destination filter
IP ranges

Destination IP ranges *
0.0.0.0/0 for example, 0.0.0.0/0, 192.168.2.0/24

8. Toggle the **Protocols and ports** option to **Specified protocols and ports**.
9. Check the boxes for **tcp** and **udp**.
10. Enter the following ports:
    - TCP: 22, 53, 443
    - UDP: 53, 1194, 2114



Protocols and ports

○ Allow all

● Specified protocols and ports

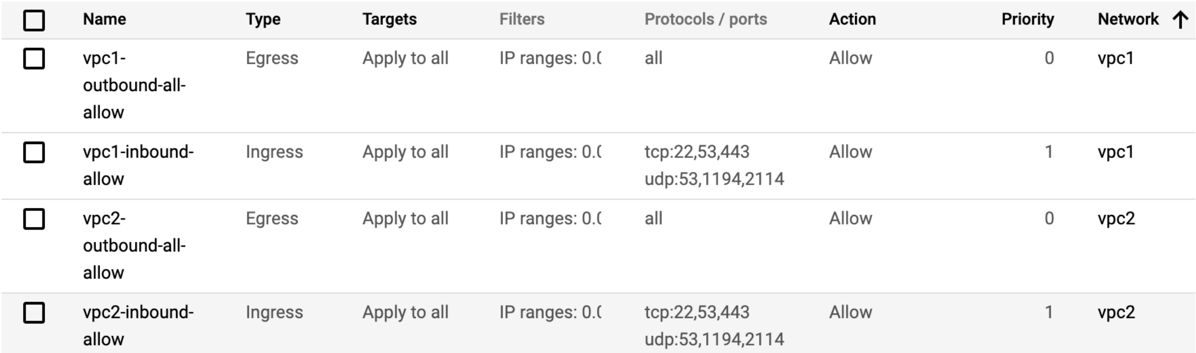
☑ tcp : 22, 53, 443

☑ udp : 53, 1194, 2114

□ Other protocols

protocols, comma separated, e.g. ah, sctp

11. Click **CREATE**.
12. If you are deploying an instance with two NICs, repeat the above process to create an inbound rule for your second VPC.
13. Verify all rules were created successfully.



□	Name	Type	Targets	Filters	Protocols / ports	Action	Priority	Network ↑
□	vpc1-outbound-all-allow	Egress	Apply to all	IP ranges: 0.(	all	Allow	0	vpc1
□	vpc1-inbound-allow	Ingress	Apply to all	IP ranges: 0.(	tcp:22,53,443 udp:53,1194,2114	Allow	1	vpc1
□	vpc2-outbound-all-allow	Egress	Apply to all	IP ranges: 0.(	all	Allow	0	vpc2
□	vpc2-inbound-allow	Ingress	Apply to all	IP ranges: 0.(	tcp:22,53,443 udp:53,1194,2114	Allow	1	vpc2

Infoblox vNIOS for GCP Image

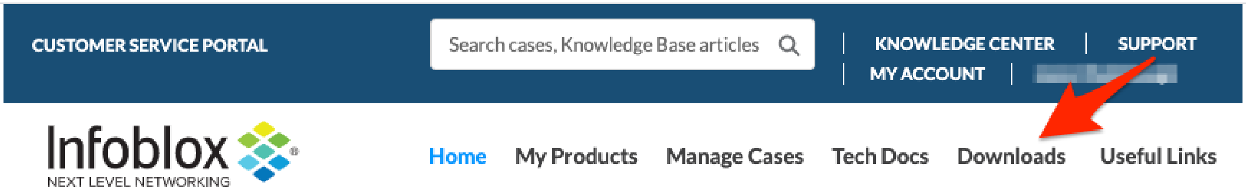
The Infoblox vNIOS for GCP appliance can be deployed using an image file downloaded from the Infoblox Support portal.

Download vNIOS for GCP Image

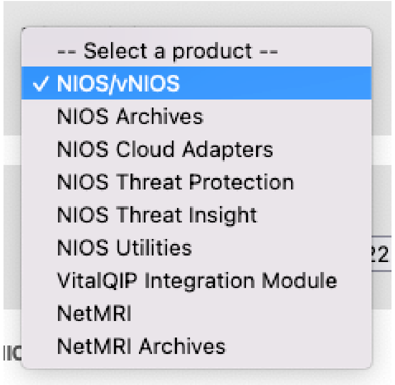
To download the virtual machine image file:

1. In your browser, navigate to https://support.infoblox.com/ and sign in.

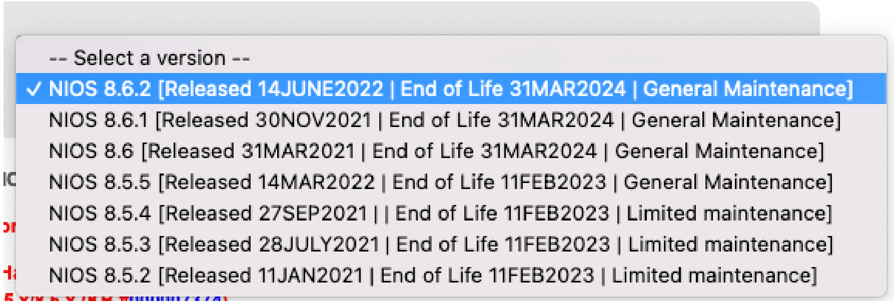
2. Click on **Downloads**.



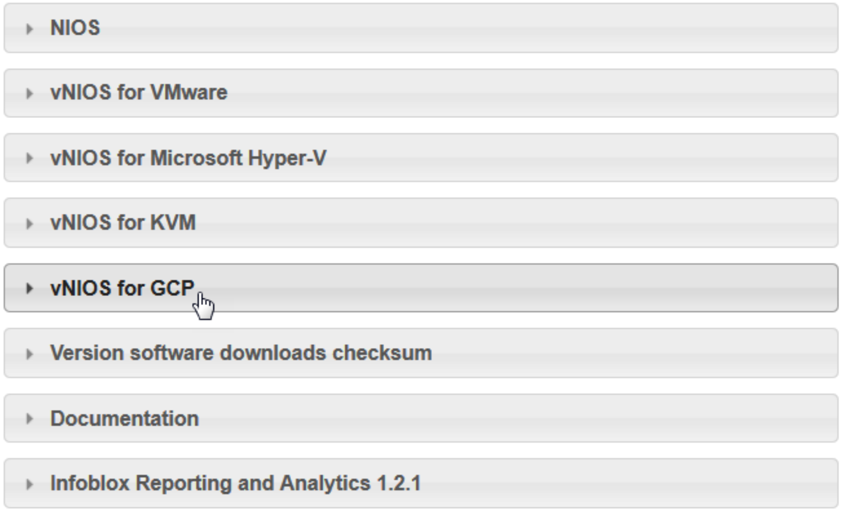
3. Expand the **Infoblox Software** menu and select **NIOS/vNIOS**.



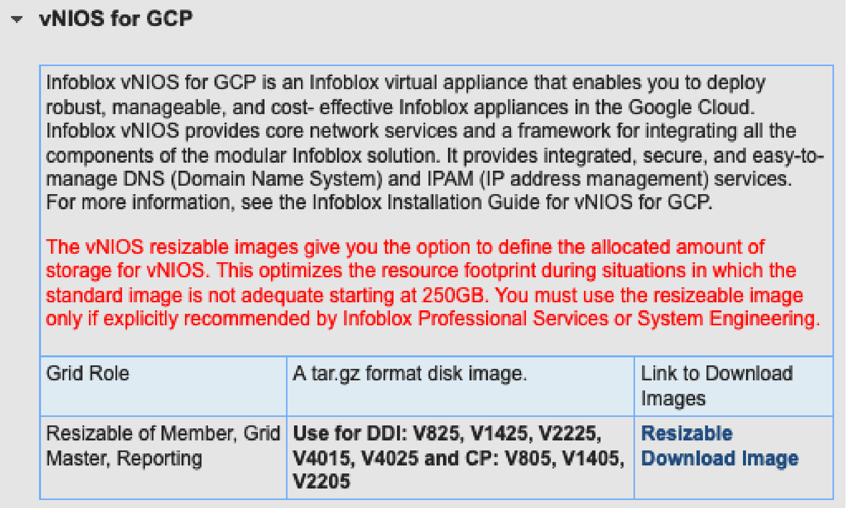
4. Expand the **Select Version** menu and select the desired version.


-- Select a version --
✓ NIOS 8.6.2 [Released 14JUNE2022 | End of Life 31MAR2024 | General Maintenance]
NIOS 8.6.1 [Released 30NOV2021 | End of Life 31MAR2024 | General Maintenance]
NIOS 8.6 [Released 31MAR2021 | End of Life 31MAR2024 | General Maintenance]
NIOS 8.5.5 [Released 14MAR2022 | End of Life 11FEB2023 | General Maintenance]
NIOS 8.5.4 [Released 27SEP2021 | | End of Life 11FEB2023 | Limited maintenance]
NIOS 8.5.3 [Released 28JULY2021 | End of Life 11FEB2023 | Limited maintenance]
NIOS 8.5.2 [Released 11JAN2021 | End of Life 11FEB2023 | Limited maintenance]

5. Scroll down to and expand the **vNIOS for GCP** option.


NIOS
vNIOS for VMware
vNIOS for Microsoft Hyper-V
vNIOS for KVM
vNIOS for GCP
Version software downloads checksum
Documentation
Infoblox Reporting and Analytics 1.2.1

6. Click on the **Resizable Download Image** link.



vNIOS for GCP

Infoblox vNIOS for GCP is an Infoblox virtual appliance that enables you to deploy robust, manageable, and cost- effective Infoblox appliances in the Google Cloud. Infoblox vNIOS provides core network services and a framework for integrating all the components of the modular Infoblox solution. It provides integrated, secure, and easy-to-manage DNS (Domain Name System) and IPAM (IP address management) services. For more information, see the Infoblox Installation Guide for vNIOS for GCP.

The vNIOS resizable images give you the option to define the allocated amount of storage for vNIOS. This optimizes the resource footprint during situations in which the standard image is not adequate starting at 250GB. You must use the resizeable image only if explicitly recommended by Infoblox Professional Services or System Engineering.

Grid Role	A tar.gz format disk image.	Link to Download Images
Resizable of Member, Grid Master, Reporting	**Use for DDI: V825, V1425, V2225, V4015, V4025 and CP: V805, V1405, V2205**	**Resizable Download Image**

7. Accept any terms (if prompted). Depending on your browser settings, you may be prompted to save the file, or it may download automatically. Proceed through the prompts (if any) to complete the download.

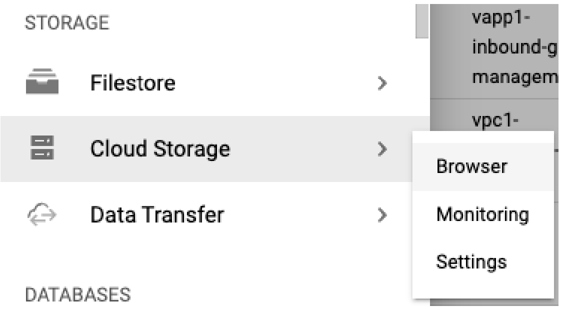
Upload Infoblox vNIOS for GCP Image File

Before you can deploy your Infoblox vNIOS for GCP appliance, you will need to create a storage bucket and upload the appliance image. This can be done using the GCP Console or GSUTIL.

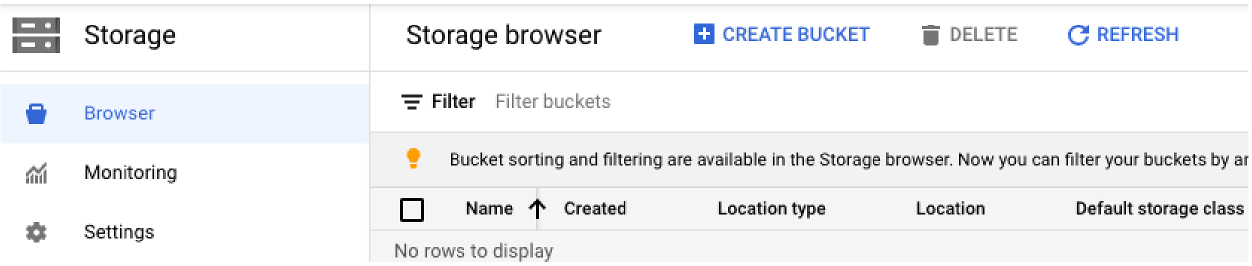
Create Bucket

To create a bucket using the GCP Console:

1. In the GCP Console Navigation menu, expand **Cloud Storage**; select **Browser.**



2. Click **CREATE BUCKET**.

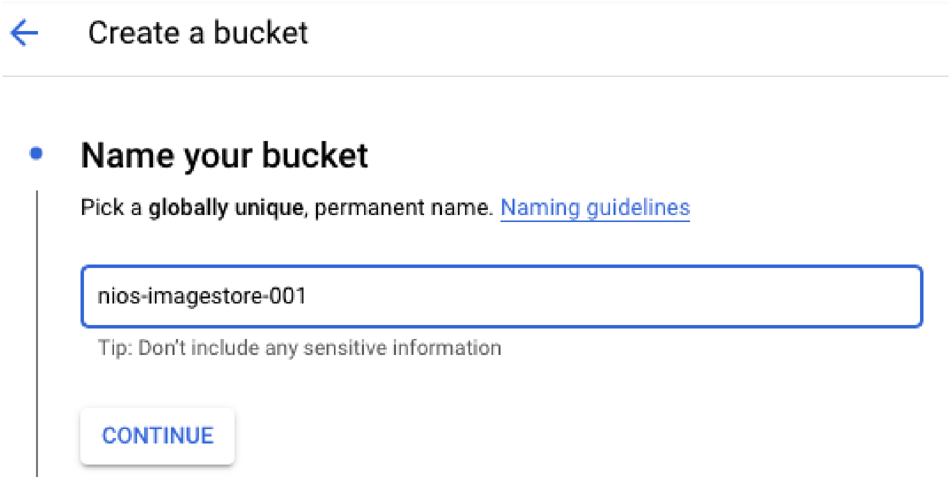


Bucket sorting and filtering are available in the Storage browser. Now you can filter your buckets by ar

□	Name ↑	Created	Location type	Location	Default storage class

No rows to display

3. Type a **name**, click **CONTINUE**.



Create a bucket

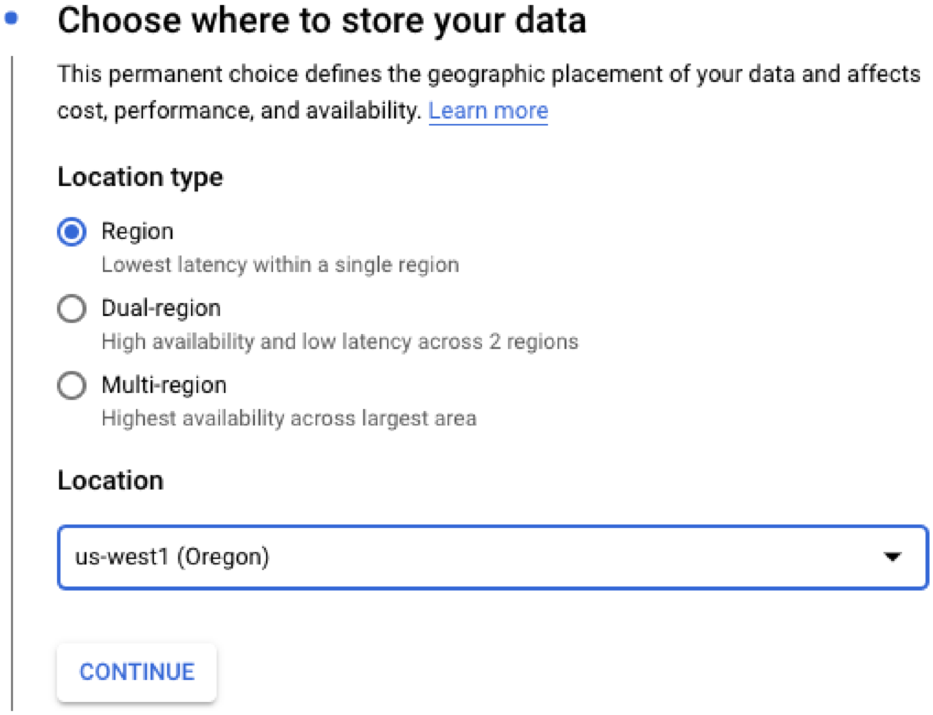
Name your bucket

Pick a **globally unique**, permanent name. Naming guidelines

nios-imagestore-001

Tip: Don't include any sensitive information

4. Select **Region** for Location type and choose a Location from the dropdown.
5. Click **CONTINUE**.



Choose where to store your data

This permanent choice defines the geographic placement of your data and affects cost, performance, and availability. Learn more

Location type

● Region
Lowest latency within a single region

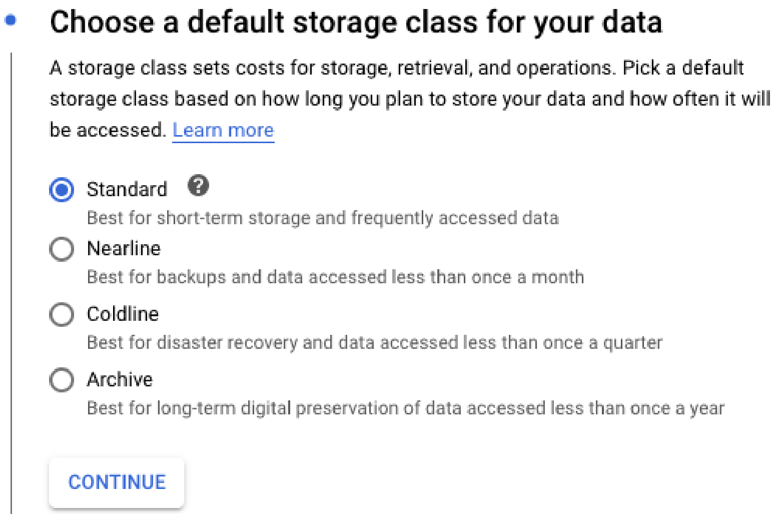
○ Dual-region
High availability and low latency across 2 regions

○ Multi-region
Highest availability across largest area

Location

us-west1 (Oregon)

6. Use the default **Standard** storage class. Click **CONTINUE**.



Choose a default storage class for your data

A storage class sets costs for storage, retrieval, and operations. Pick a default storage class based on how long you plan to store your data and how often it will be accessed. Learn more

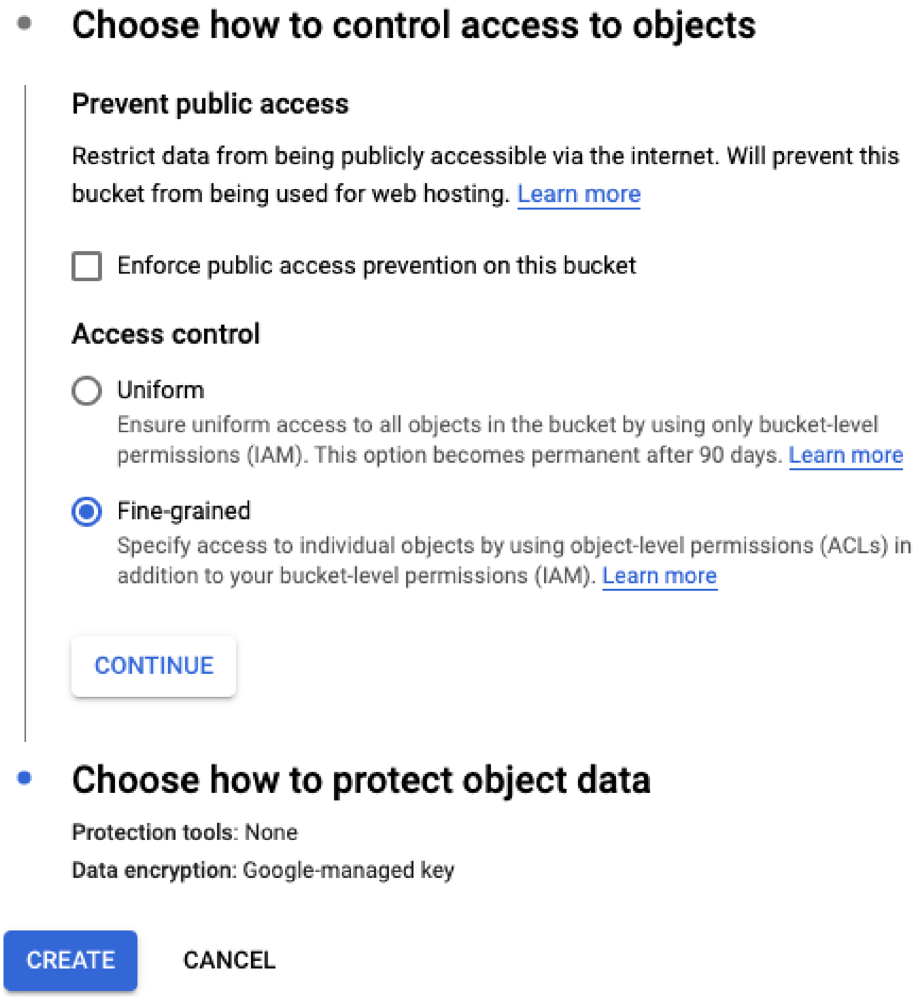
● Standard
Best for short-term storage and frequently accessed data

○ Nearline
Best for backups and data accessed less than once a month

○ Coldline
Best for disaster recovery and data accessed less than once a quarter

○ Archive
Best for long-term digital preservation of data accessed less than once a year

7. Set Access control to **Fine-grained.**
8. Click **CREATE**.



Choose how to control access to objects

Prevent public access

Restrict data from being publicly accessible via the internet. Will prevent this bucket from being used for web hosting. Learn more

□ Enforce public access prevention on this bucket

Access control

○ Uniform
Ensure uniform access to all objects in the bucket by using only bucket-level permissions (IAM). This option becomes permanent after 90 days. Learn more

● Fine-grained
Specify access to individual objects by using object-level permissions (ACLs) in addition to your bucket-level permissions (IAM). Learn more

Choose how to protect object data

Protection tools: None

Data encryption: Google-managed key

To create a bucket using the GSUTIL, use the following command examples:

Note: This is optional and not required if you used the console method.

1. If not already logged in, first authenticate using the GCloud CLI:

   gcloud auth login

2. Use the following example to create a bucket:

   gsutil mb -c <class> -l <location> gs://<unique_bucket_name>

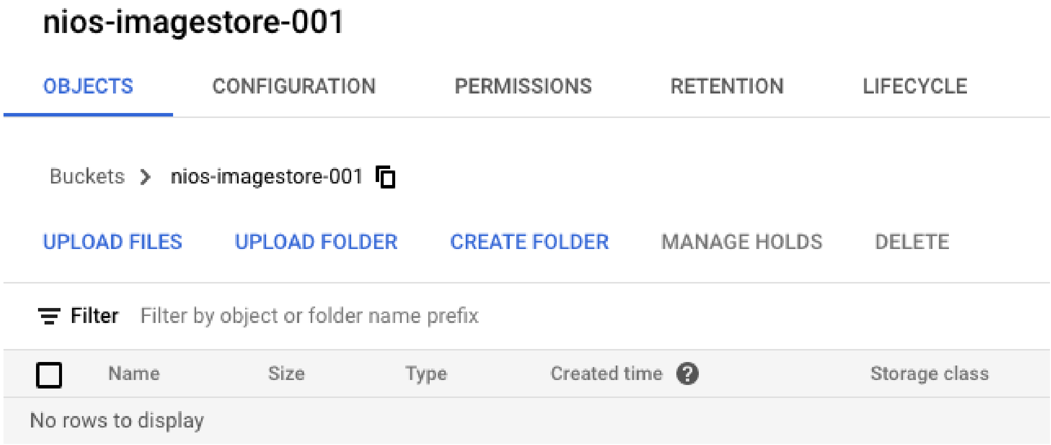
3. In the above example:
   a. <class>: Replace this string with the class you want to use for your bucket. Available classes include multi-regional, regional, nearline and coldline. If in doubt, you can omit this option and it will default to Standard Storage, which is equivalent to either multi-regional or regional (depending on the location where your bucket is created).
   b. <location>: Specify the location where you want your bucket to be created in. If this option is omitted, the default location (US) is used.
   c. <unique_bucket_name>: Replace this value with the name that you want to use for your bucket. This must be a unique name not only within your account but throughout GCP.

Additional information regarding buckets and GSUTIL can be found at
https://cloud.google.com/storage/docs/gsutil/commands/mb

Upload Image File to Bucket

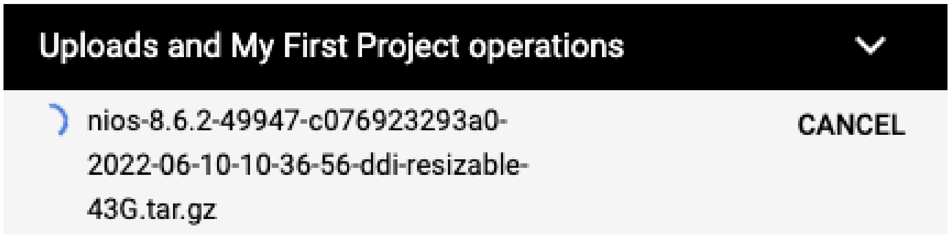
Once the bucket creation completes, your new bucket will be open in the browser.

1. Click **UPLOAD FILES**.



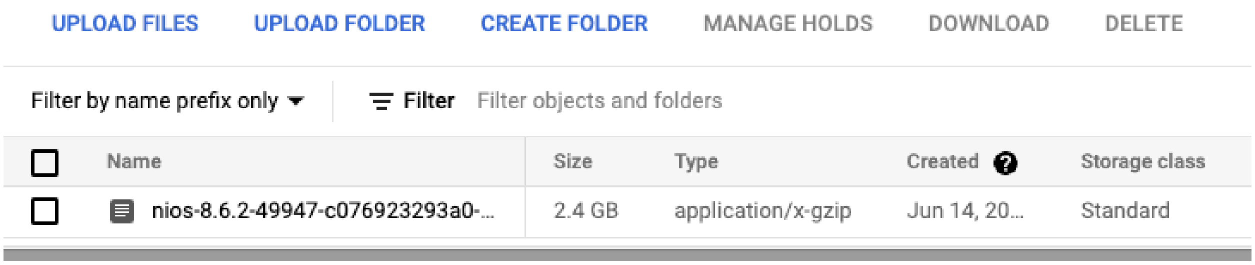
No rows to display

2. Follow the prompts to browse to and upload your Infoblox vNIOS for GCP appliance image file. This file can be over 2 GB in size and the upload may take a while to complete.



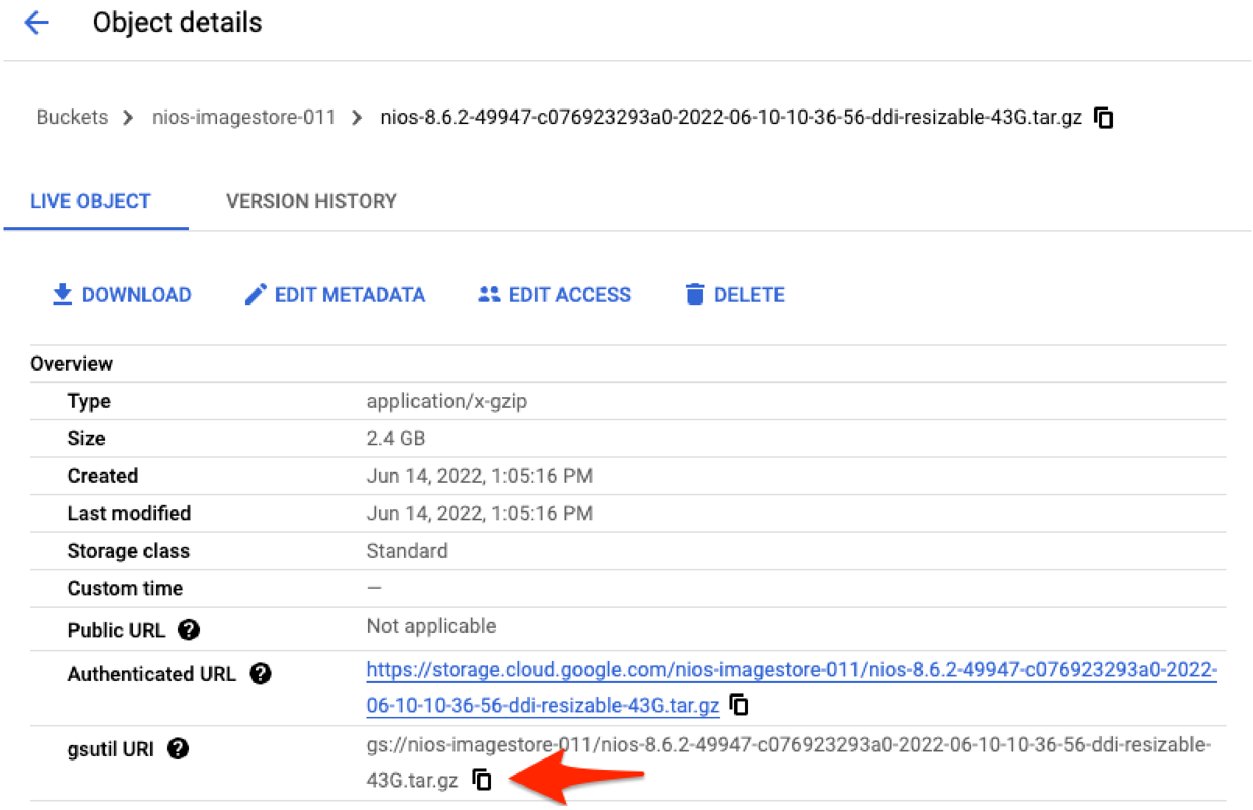
nios-8.6.2-49947-c076923293a0-2022-06-10-10-36-56-ddi-resizable-43G.tar.gz

3. Verify that the file upload completed successfully.



□	Name	Size	Type	Created	Storage class
□	nios-8.6.2-49947-c076923293a0-...	2.4 GB	application/x-gzip	Jun 14, 20...	Standard

4. To get the URI of your uploaded image, which you will need to create a custom image, click on the file name in your bucket.
5. On the Object details page, click the copy button next to gsutil URI to copy this to your clipboard.



Overview

Type	application/x-gzip
Size	2.4 GB
Created	Jun 14, 2022, 1:05:16 PM
Last modified	Jun 14, 2022, 1:05:16 PM
Storage class	Standard
Custom time	—
Public URL	Not applicable
Authenticated URL	https://storage.cloud.google.com/nios-imagestore-011/nios-8.6.2-49947-c076923293a0-2022-06-10-10-36-56-ddi-resizable-43G.tar.gz
gsutil URI	gs://nios-imagestore-011/nios-8.6.2-49947-c076923293a0-2022-06-10-10-36-56-ddi-resizable-43G.tar.gz

Create Infoblox vNIOS for GCP Custom Image

VM instances are deployed using a predefined image. This guide provides the steps to create a custom image using an Infoblox vNIOS for GCP image file previously uploaded into your project's storage bucket.

Important: Infoblox vNIOS version 8.4 and 8.5 appliances are deployed with two network interfaces that will correspond to the LAN1 and MGMT (not enabled by default in NIOS). Because of this, the MULTI_IP_SUBNET feature must be enabled in the image or else the deployed vNIOS appliance will be unable to communicate on the network. While the second network interface is optional beginning with NIOS 8.6, this method should still be used for creating custom images. As of this writing, the MULTI_IP_SUBNET feature is only available using the GCloud CLI.

For more information regarding the deployment of virtual machines with multiple network interfaces in GCP, refer to https://cloud.google.com/vpc/docs/create-use-multiple-interfaces.

To create a custom image using the GCloud CLI:

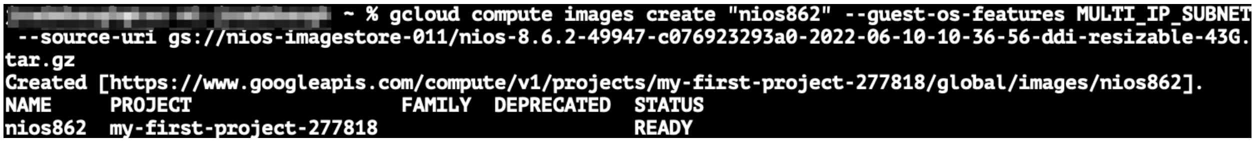
1. Open a terminal or command line application on the computer where you installed the GCloud CLI.
2. If not already logged in, first authenticate using the GCloud CLI:

   gcloud auth login
3. Follow prompts in your browser to login.
4. Run the following command to create your custom image:

   gcloud compute images create "imagename" --guest-os-features MULTI_IP_SUBNET --source-uri gs://<bucket_name>/nios-8.6.2-49947-c076923293a0-2022-06-10-10-36-56-ddi-resizable-43G.tar.gz

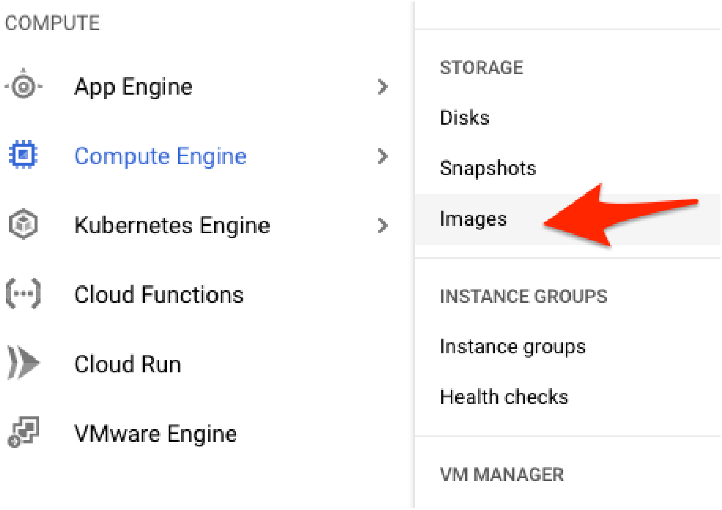
   a. In the above example, replace **imagename** with the name you want for your image. Note: Names can be up to 62 characters, must start with a lowercase letter, may contain lowercase letters, numbers, or hyphens, and cannot end with a hyphen.

   b. In the above example, replace the URI with the URI for the Infoblox vNIOS for GCP appliance image file you uploaded in the last section.

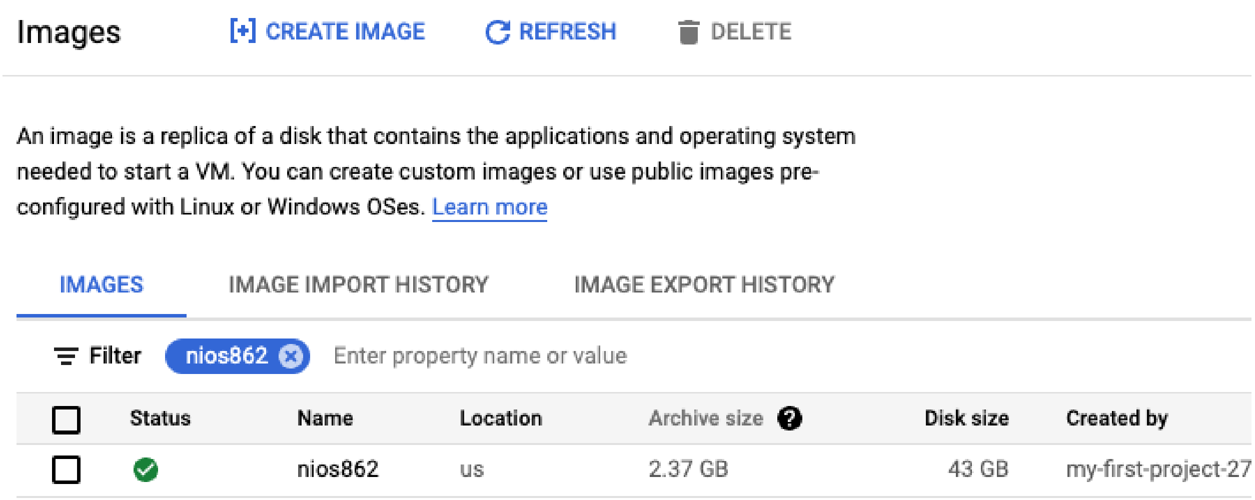


```
[redacted] ~ % gcloud compute images create "nios862" --guest-os-features MULTI_IP_SUBNET
 --source-uri gs://nios-imagestore-011/nios-8.6.2-49947-c076923293a0-2022-06-10-10-36-56-ddi-resizable-43G.
tar.gz
Created [https://www.googleapis.com/compute/v1/projects/my-first-project-277818/global/images/nios862].
NAME     PROJECT                  FAMILY  DEPRECATED  STATUS
nios862  my-first-project-277818                      READY
```

5. Wait for the image creation to complete.
6. To view your new custom image in the GCP Console, in the navigation menu expand **Compute Engine**. Select **Images**.



7. Enter the name of your image in the filter.



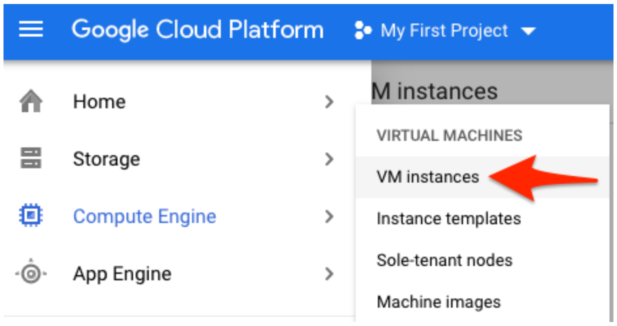
An image is a replica of a disk that contains the applications and operating system needed to start a VM. You can create custom images or use public images pre-configured with Linux or Windows OSes. Learn more

□	Status	Name	Location	Archive size	Disk size	Created by
□	✓	nios862	us	2.37 GB	43 GB	my-first-project-27

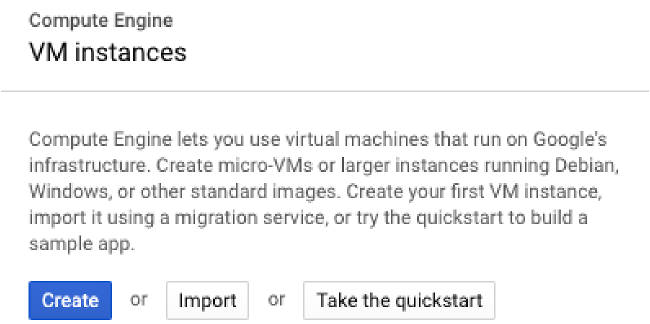
Deploy Infoblox vNIOS for GCP Instance

To deploy an Infoblox vNIOS for GCP virtual machine instance using the custom image you created:

1. In the GCP Console Navigation menu, expand **Compute Engine**. Select **VM Instances**.



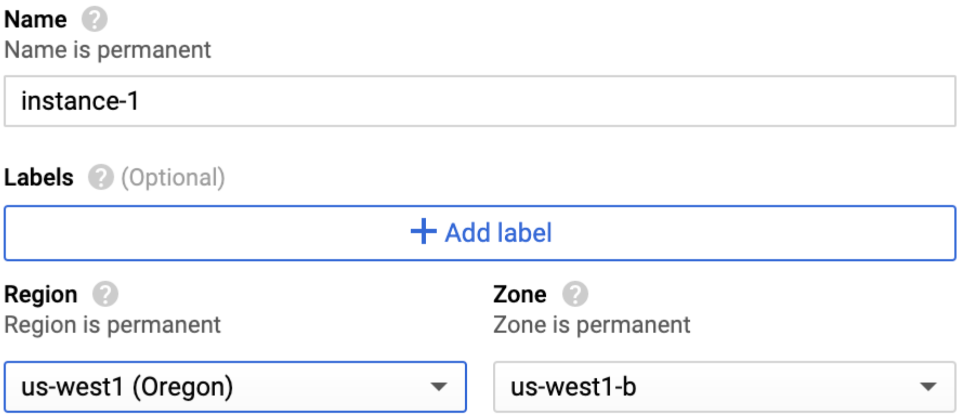
2. Click **Create**.



Compute Engine lets you use virtual machines that run on Google's infrastructure. Create micro-VMs or larger instances running Debian, Windows, or other standard images. Create your first VM instance, import it using a migration service, or try the quickstart to build a sample app.

Configure Instance Size and Image

1. Type a name for your instance and select the desired Region and Zone. Note: This should be the same region your VPC subnets are in.



Name

Name is permanent

instance-1

Labels (Optional)

Region

Region is permanent

us-west1 (Oregon)

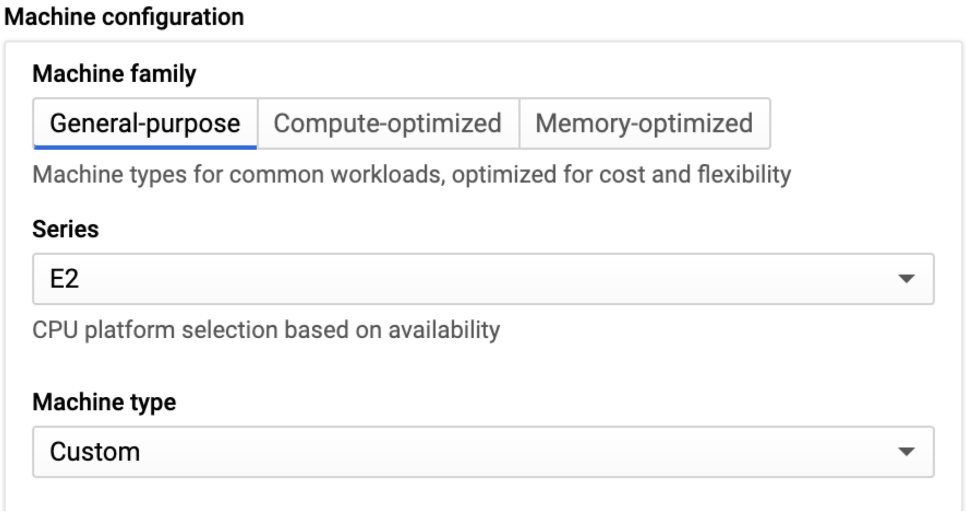
Zone

Zone is permanent

us-west1-b

2. In the **Machine configuration** section, select the E2 or N2 series.
3. For **Machine type**, select **Custom**.

Note: For some vNIOS models, standard or high memory sizes can be used instead of custom. Virtual hardware should meet the requirements shown for vNIOS models in the table below.



Machine configuration

Machine family

Machine types for common workloads, optimized for cost and flexibility

Series

E2

CPU platform selection based on availability

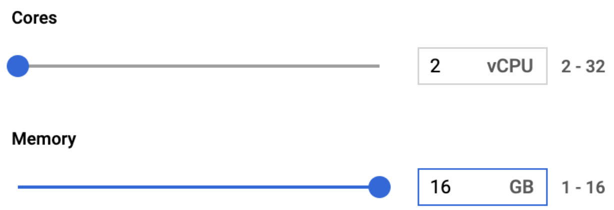
Machine type

Custom

The following table outlines the hardware specifications for the vNIOS appliance models supported on GCP:

vNIOS Appliance	Disk Size (GB)	# of vCPU Cores	Memory Allocation (GB)	Supported as GM and GMC
TE-V825	250	2	16	Yes
TE-V1425	250	4	32	Yes
TE-V2225	250	8	64	Yes
TE-V4015 (8.6.2 and later)	250	14	28	Yes
TE-V4025 (8.6.2 and later)	250	14	28	Yes
CP-V805	250	2	16	No
CP-V1405	250	4	32	No
CP-V2205	250	8	64	No

4. Set the **Cores** (CPU) and **Memory** to match the intended vNIOS Appliance model (the example used in this guide is an IB-V825).



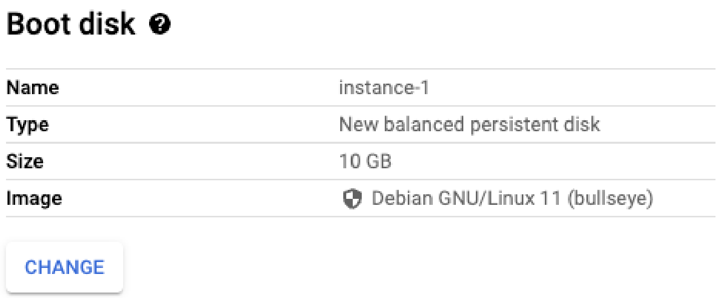
Cores

2 vCPU 2 - 32

Memory

16 GB 1 - 16

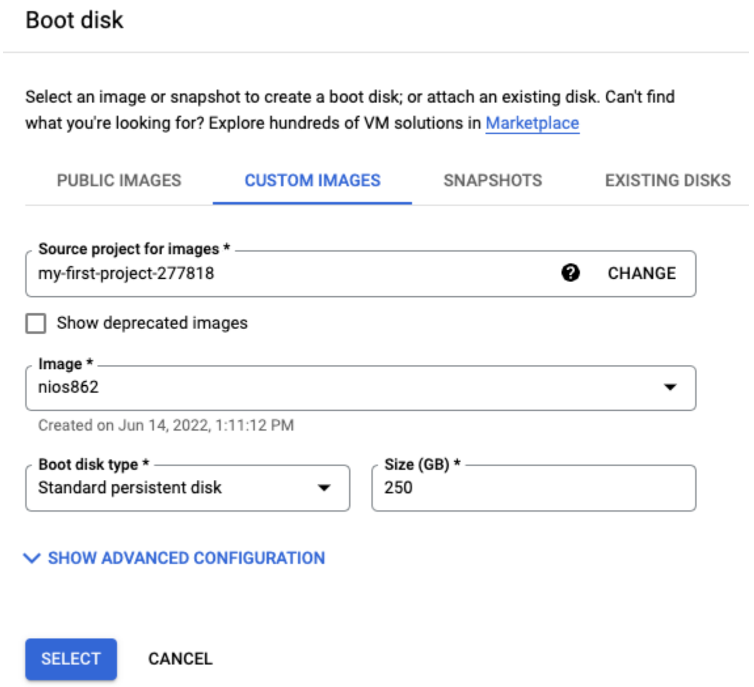
5. For **Boot disk**, click **Change**.



Boot disk

Name	instance-1
Type	New balanced persistent disk
Size	10 GB
Image	Debian GNU/Linux 11 (bullseye)

6. Switch to the **Custom images** tab.
7. Select the custom image for your vNIOS for GCP appliance image from the dropdown.
8. For Boot disk type, select **Standard persistent disk**.
9. Set the **Size (GB)** field to match the size required for the appliance model type being deployed. Refer to the table above for the supported disk sizes.
10. Click **Select**.



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

Source project for images *: my-first-project-277818

□ Show deprecated images

Image *: nios862

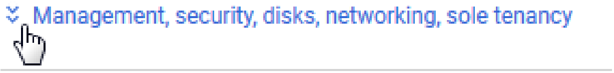
Created on Jun 14, 2022, 1:11:12 PM

Boot disk type *: Standard persistent disk

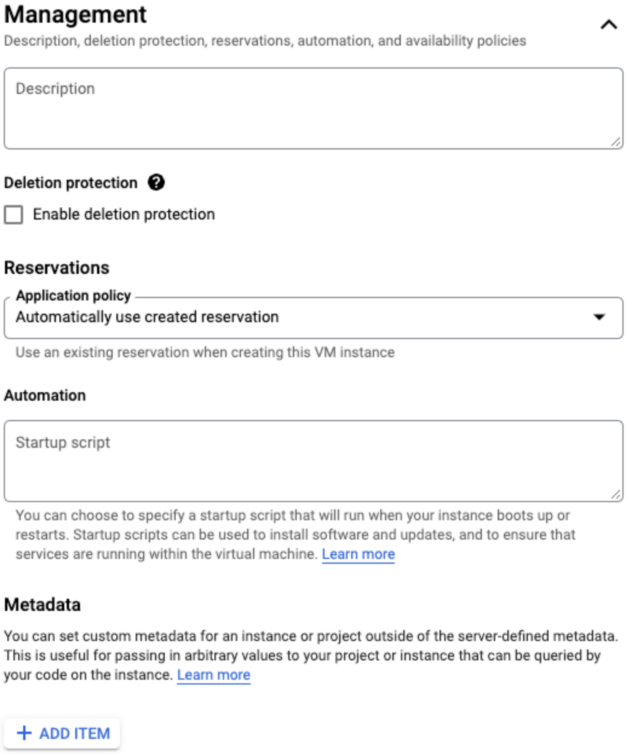
Size (GB) *: 250

Configure User Data

1. Expand the **Management, security, disks, networking, sole tenancy** panel.



2. Expand the **Management** section, under Metadata, click **Add Item**.



Management

Description, deletion protection, reservations, automation, and availability policies

Description

Deletion protection

□ Enable deletion protection

Reservations

Application policy: Automatically use created reservation

Use an existing reservation when creating this VM instance

Automation

Startup script

You can choose to specify a startup script that will run when your instance boots up or restarts. Startup scripts can be used to install software and updates, and to ensure that services are running within the virtual machine. Learn more

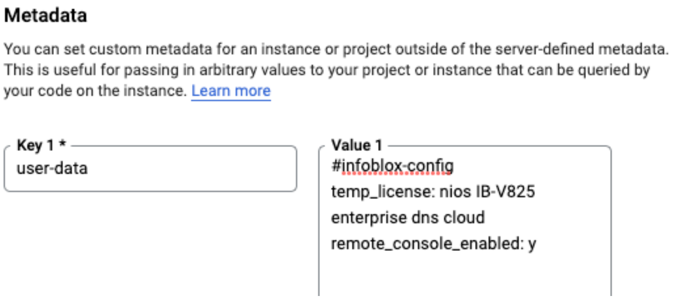
Metadata

You can set custom metadata for an instance or project outside of the server-defined metadata. This is useful for passing in arbitrary values to your project or instance that can be queried by your code on the instance. Learn more

3. Enter **user-data** for Key.
4. For Value 1, enter:

#infoblox-config
temp_license: nios IB-V825 enterprise dns dhcp cloud
remote_console_enabled: y

This will enable the SSH console and set temporary licenses for your vNIOS appliance. You should change the temporary license strings to reflect the vNIOS model you are deploying as well as appropriate service licenses. Refer to Infoblox Documentation for additional details. This is optional, as temporary and other licensing can be added later using the NIOS CLI.



Metadata

You can set custom metadata for an instance or project outside of the server-defined metadata. This is useful for passing in arbitrary values to your project or instance that can be queried by your code on the instance. Learn more

Key 1 *: user-data

Value 1:

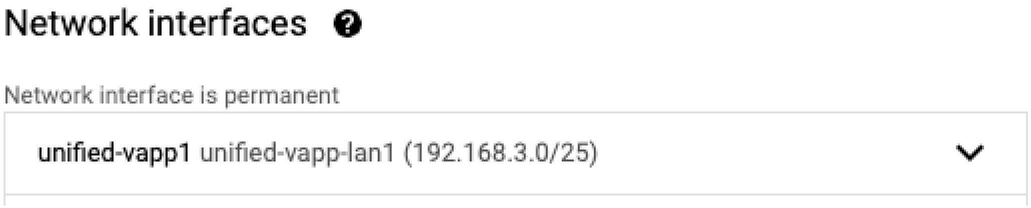
```
#infoblox-config
temp_license: nios IB-V825
enterprise dns cloud
remote_console_enabled: y
```

Configure Network Interface(s)

Infoblox vNIOS for GCP instances using NIOS version 8.6 and later can be deployed with one or two network interfaces. Instances deployed with a single network interface can be deployed into a standard VPC or a shared VPC. Older versions of NIOS require two network interfaces. Follow instructions in the appropriate subsection depending on the number of network interfaces and VPC type you will deploy.

Single Network Interface (NIOS 8.6)

1. Expand the **Networking** section.
2. Under **Network Interfaces**, expand the default network interface.

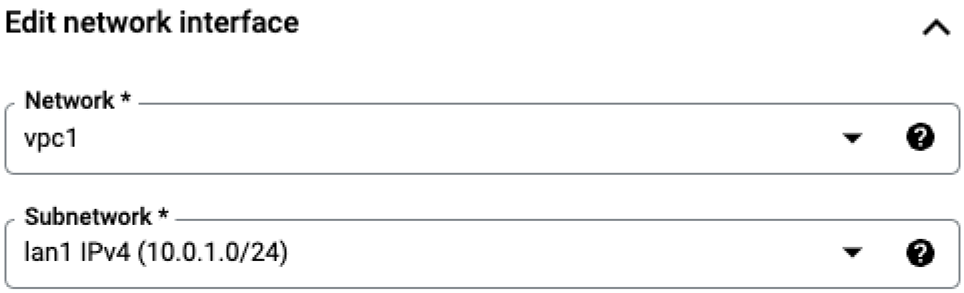


Network interfaces

Network interface is permanent

unified-vapp1 unified-vapp-lan1 (192.168.3.0/25)

3. Expand the **Network** dropdown and select the VPC to use for the interface.
4. Select the subnet that you want to use for your interface.

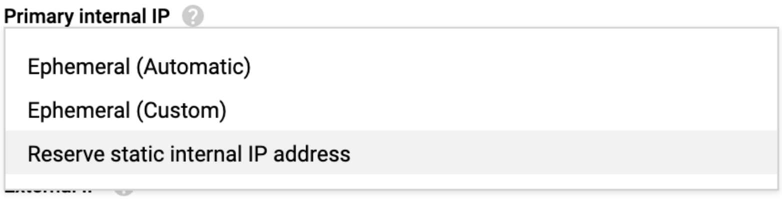


Edit network interface

Network *
vpc1

Subnetwork *
lan1 IPv4 (10.0.1.0/24)

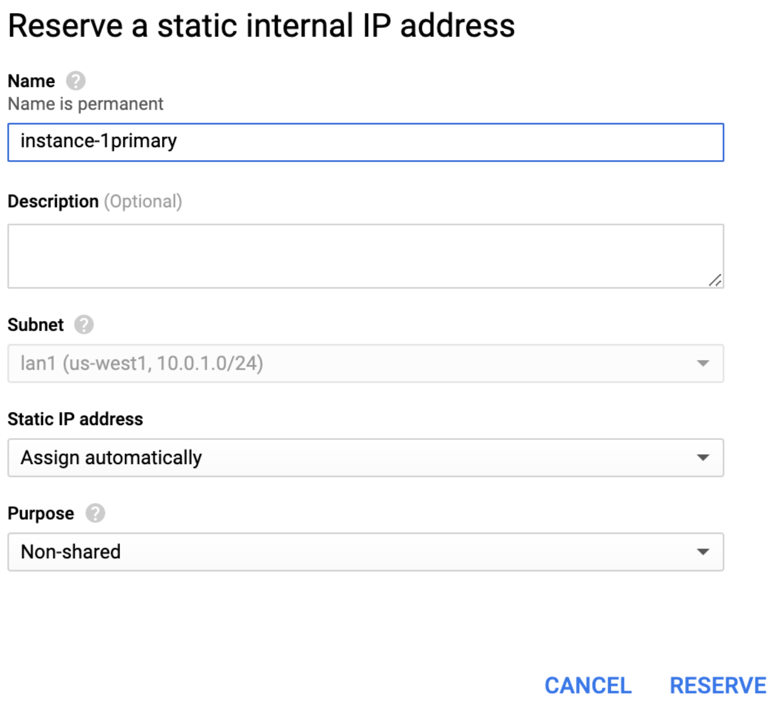
5. It is recommended that you have a static IP address for the LAN1 interface. To reserve a static address, select **Reserve static internal IP address** from the **Primary internal IP** dropdown.



Primary internal IP

Ephemeral (Automatic)
Ephemeral (Custom)
Reserve static internal IP address

6. In the dialog window, enter a Name for the IP reservation.
7. Under **Static IP address**, you can leave it set to **Assign automatically** or choose an IP address if desired.
8. Click **RESERVE**.



Reserve a static internal IP address

Name
Name is permanent
instance-1primary

Description (Optional)

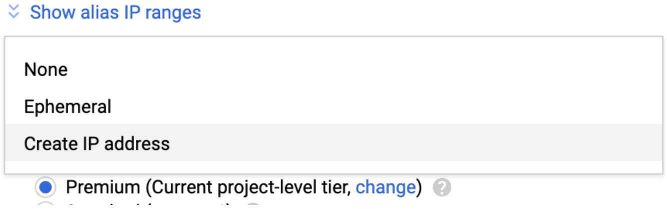
Subnet
lan1 (us-west1, 10.0.1.0/24)

Static IP address
Assign automatically

Purpose
Non-shared

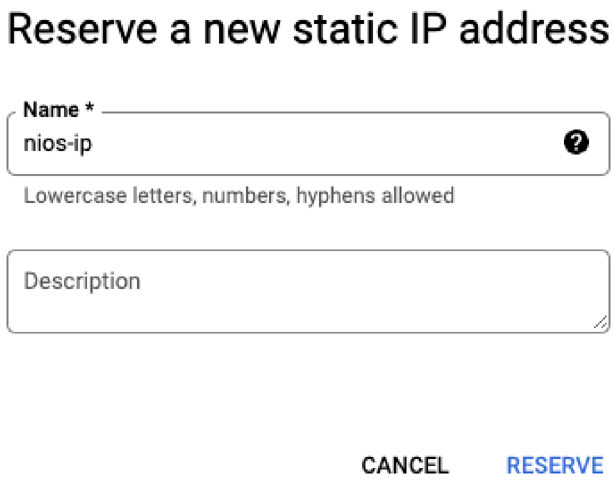
9. Select **Create IP address** from the **External IP** dropdown.

Note: If you plan to connect to your vNIOS instance using VPN, Cloud Interconnect, or another private method, you may not need an External IP address.



● Premium (Current project-level tier, change)

10. In the Reserve IP dialog, enter a name for the reservation.
11. Select a Network Service Tier.
12. Click **RESERVE**.

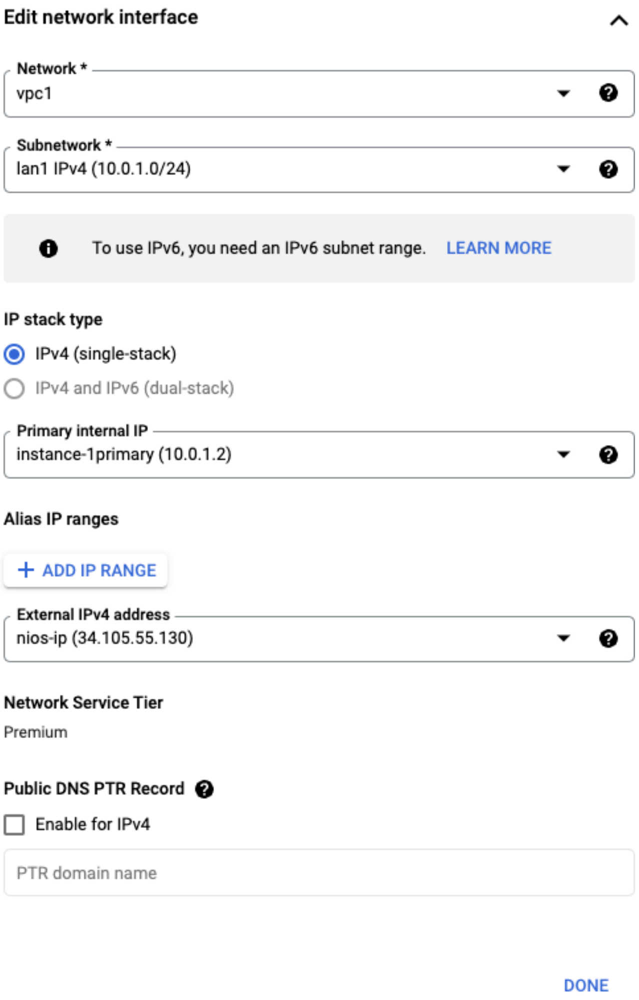


Reserve a new static IP address

Name *
nios-ip
Lowercase letters, numbers, hyphens allowed

Description

13. Click **Done**.



Edit network interface

Network *
vpc1

Subnetwork *
lan1 IPv4 (10.0.1.0/24)

To use IPv6, you need an IPv6 subnet range. LEARN MORE

IP stack type

● IPv4 (single-stack)

○ IPv4 and IPv6 (dual-stack)

Primary internal IP
instance-1primary (10.0.1.2)

Alias IP ranges

External IPv4 address
nios-ip (34.105.55.130)

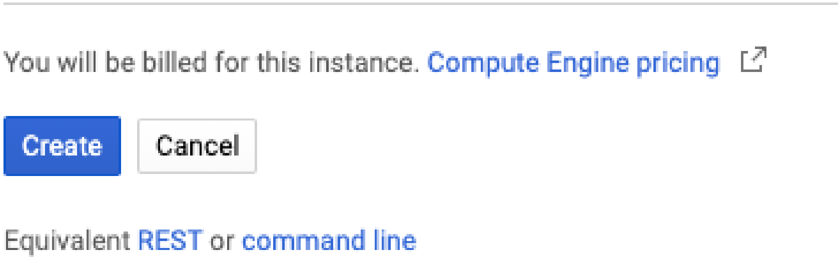
Network Service Tier
Premium

Public DNS PTR Record

□ Enable for IPv4

PTR domain name

14. Click on **Create** to begin deployment.

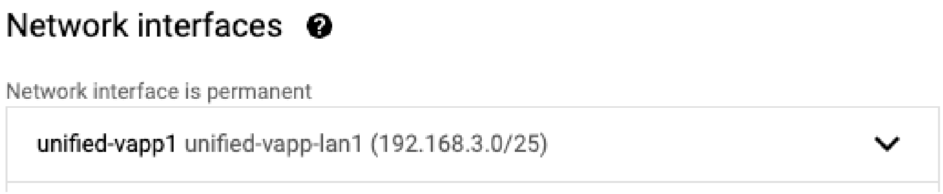


You will be billed for this instance. Compute Engine pricing

Equivalent REST or command line

Two Network Interfaces

1. Expand the **Networking** section.
2. Under **Network Interfaces**, expand the default network interface.



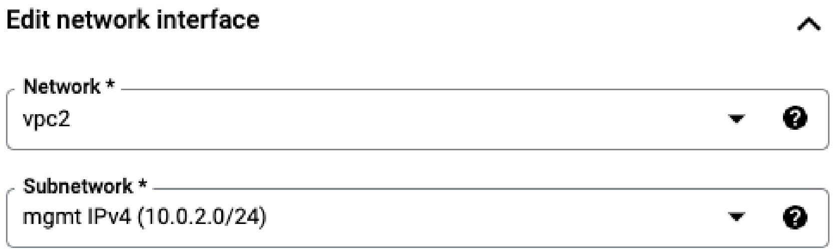
Network interfaces

Network interface is permanent

unified-vapp1 unified-vapp-lan1 (192.168.3.0/25)

Note: This first network interface will be labeled as **nic0** for the GCP VM instance. When deploying instances with two interfaces, this will be the **MGMT** interface in vNIOS.

3. Expand the **Network** dropdown and select the VPC to use for the interface.
4. Select the subnet that you want to use for your interface.

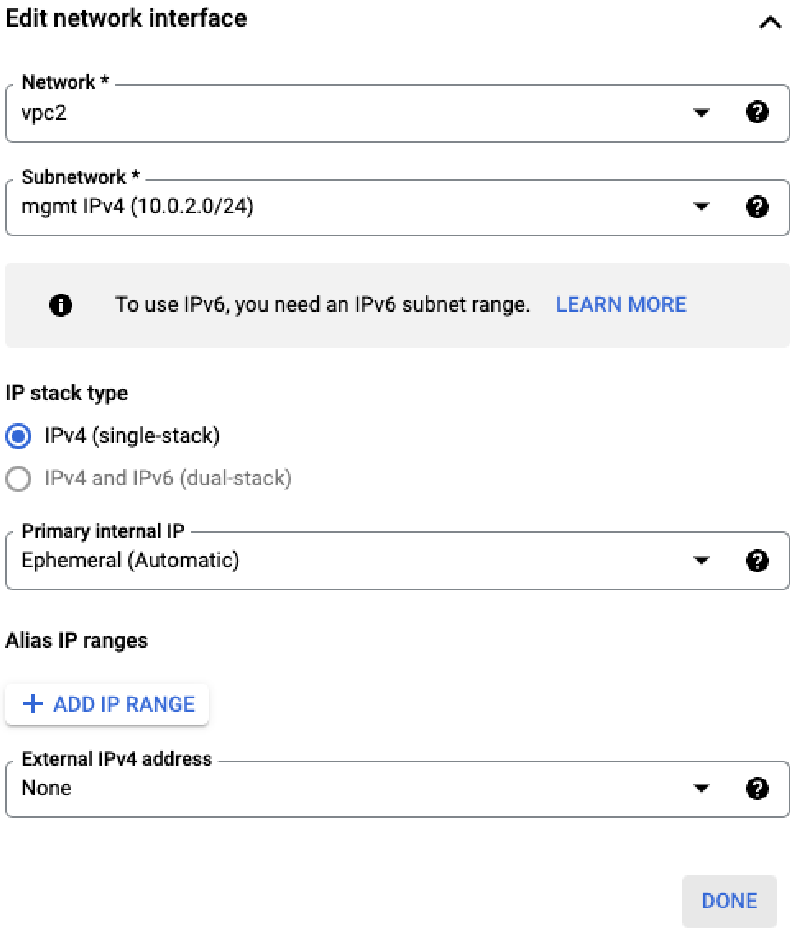


Edit network interface

Network *
vpc2

Subnetwork *
mgmt IPv4 (10.0.2.0/24)

5. Update any other settings as required.
6. Click **Done**.



Edit network interface

Network *
vpc2

Subnetwork *
mgmt IPv4 (10.0.2.0/24)

To use IPv6, you need an IPv6 subnet range. LEARN MORE

IP stack type

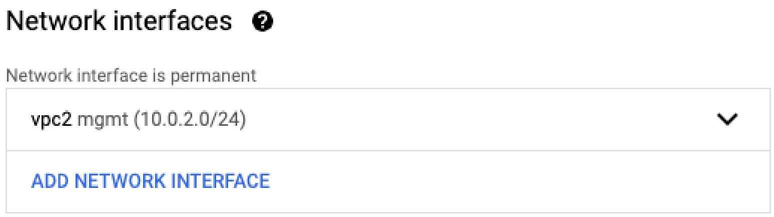
● IPv4 (single-stack)
○ IPv4 and IPv6 (dual-stack)

Primary internal IP
Ephemeral (Automatic)

Alias IP ranges

External IPv4 address
None

7. Click **Add network interface**.



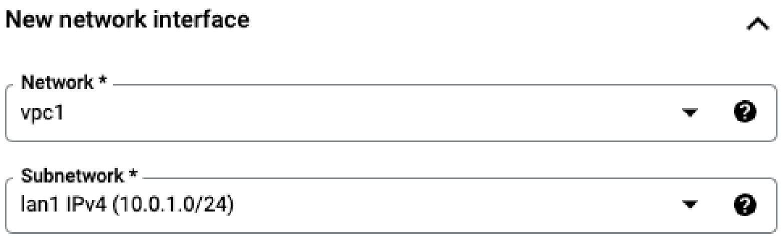
Network interfaces

Network interface is permanent

vpc2 mgmt (10.0.2.0/24)

Note: This new network interface will be labeled as **nic1** for the GCP VM instance. This will be the **LAN1** interface in vNIOS.

8. Select the VPC and subnet to use with this interface (this must be a different VPC than the one used with the MGMT interface).

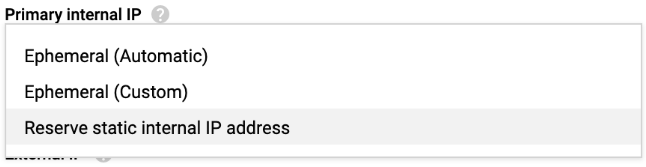


New network interface

Network * vpc1

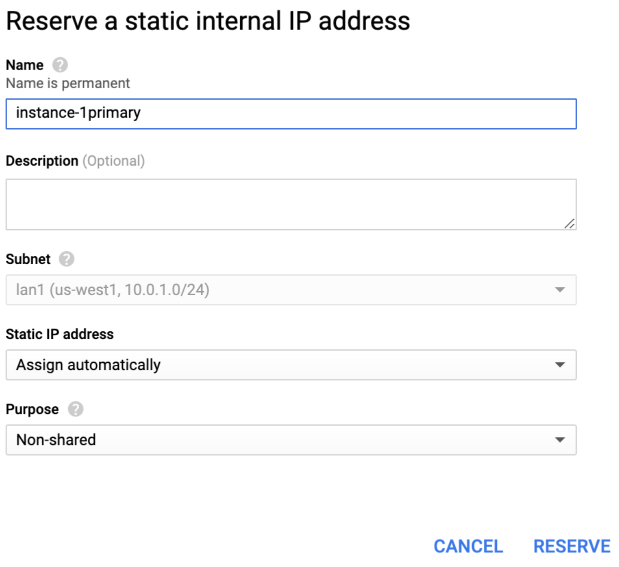
Subnetwork * lan1 IPv4 (10.0.1.0/24)

9. It is recommended that you have a static IP address for the LAN1 interface. To reserve a static address, select **Reserve static internal IP address** from the **Primary internal IP** dropdown.



Primary internal IP

10. In the dialog window, enter a Name for the IP reservation.
11. Under **Static IP address**, you can leave it set to **Assign automatically** or choose an IP address if desired.
12. Click **RESERVE**.



Reserve a static internal IP address

Name

Name is permanent

instance-1primary

Description (Optional)

Subnet

lan1 (us-west1, 10.0.1.0/24)

Static IP address

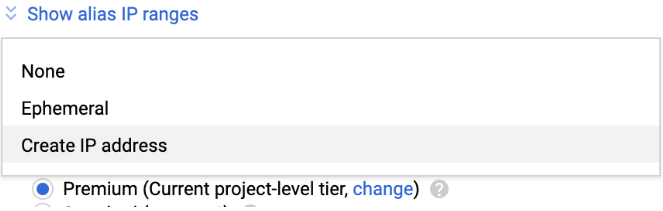
Assign automatically

Purpose

Non-shared

13. Select **Create IP address** from the **External IP** dropdown.

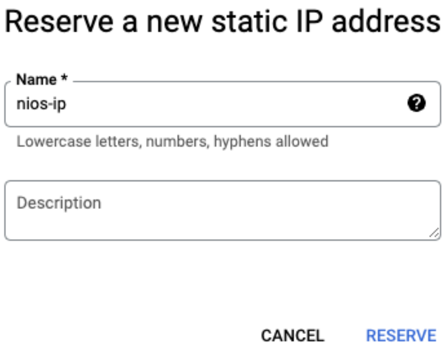
Note: If you plan to connect to your vNIOS instance using VPN, Cloud Interconnect, or another private method, you may not need an External IP address.



● Premium (Current project-level tier, change)

14. In the Reserve IP dialog, enter a name for the reservation.

15. Click **RESERVE**.

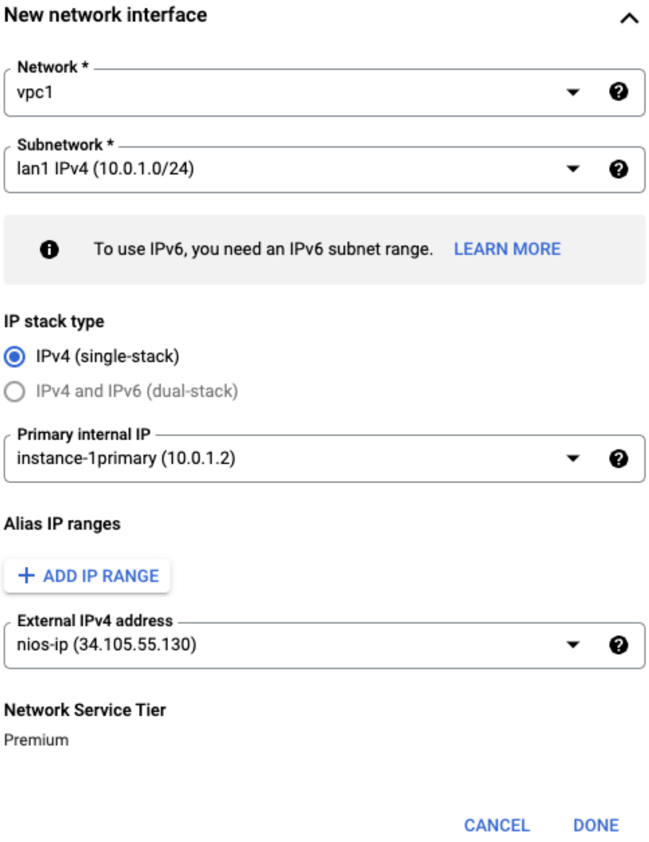

Reserve a new static IP address

Name *: nios-ip

Lowercase letters, numbers, hyphens allowed

Description

16. Click **Done** for the new (LAN1) Network Interface.


New network interface

Network *: vpc1

Subnetwork *: lan1 IPv4 (10.0.1.0/24)

To use IPv6, you need an IPv6 subnet range. LEARN MORE

IP stack type

● IPv4 (single-stack)

○ IPv4 and IPv6 (dual-stack)

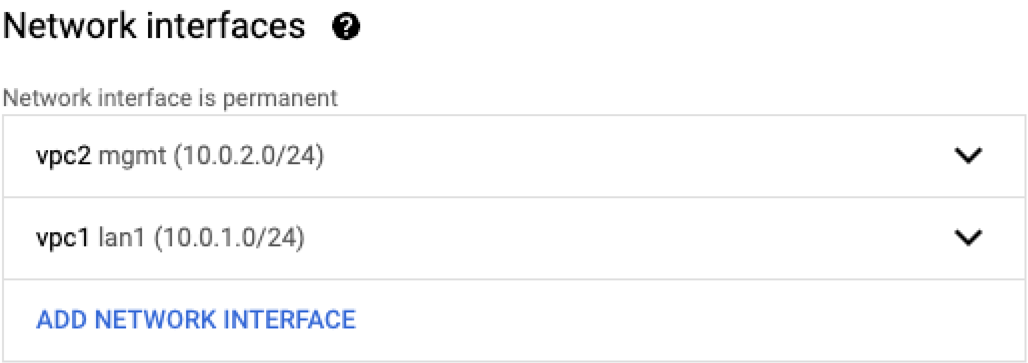
Primary internal IP: instance-1primary (10.0.1.2)

Alias IP ranges

External IPv4 address: nios-ip (34.105.55.130)

Network Service Tier: Premium

You should now have two network interfaces for the VM, as shown below.



Network interfaces

Network interface is permanent

vpc2 mgmt (10.0.2.0/24)

vpc1 lan1 (10.0.1.0/24)

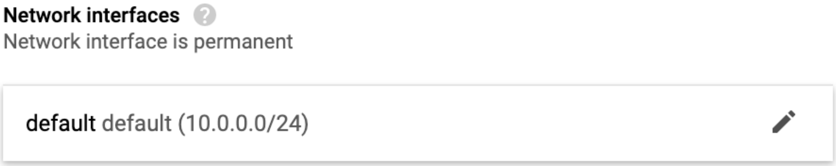
ADD NETWORK INTERFACE

17. Click **Create** to create the VM.

Shared VPC (NIOS 8.6)

When deploying a vNIOS for GCP instance with a single network interface, you can connect your instance to a Shared VPC network, provided from a host project. For additional information on GCP shared VPC, refer to https://cloud.google.com/vpc/docs/shared-vpc.

1. Expand the **Networking** section.
2. Under **Network Interfaces**, expand the default network interface.

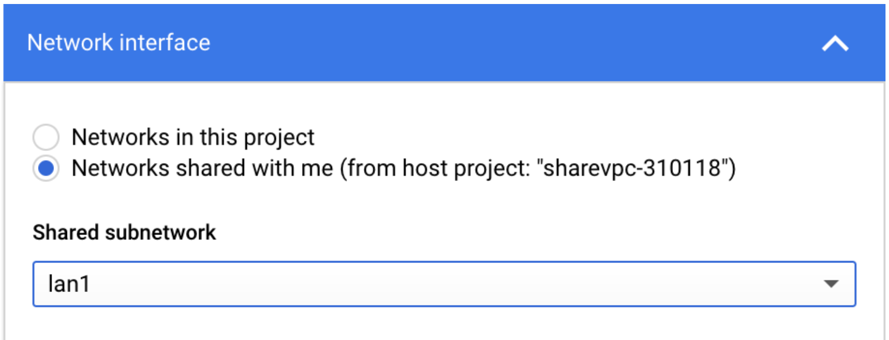


Network interfaces

Network interface is permanent

default default (10.0.0.0/24)

3. Select **Networks shared with me**.
4. Select the Shared subnetwork that you want to use for your interface.



Network interface

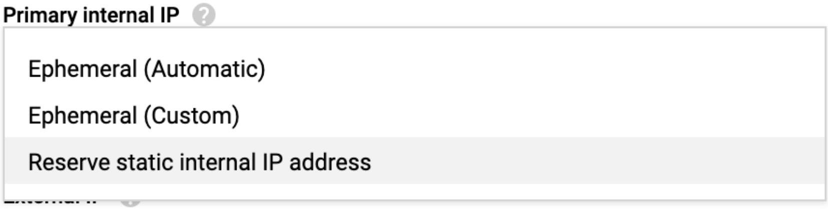
○ Networks in this project

● Networks shared with me (from host project: "sharevpc-310118")

Shared subnetwork

lan1

5. It is recommended that you have a static IP address for the LAN1 interface. To reserve a static address, select **Reserve static internal IP address** from the **Primary internal IP** dropdown.



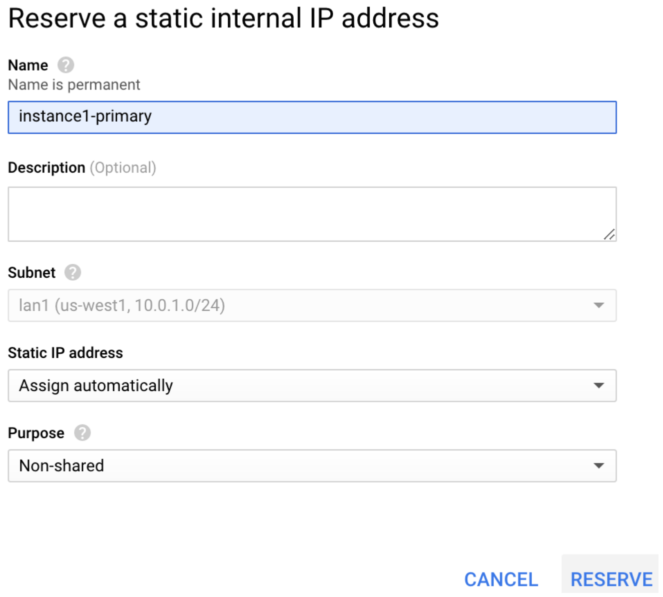
Primary internal IP

Ephemeral (Automatic)

Ephemeral (Custom)

Reserve static internal IP address

6. In the dialog window, enter a Name for the IP reservation.
7. Under **Static IP address**, you can leave it set to **Assign automatically** or choose an IP address if desired.
8. Click **RESERVE**.



Reserve a static internal IP address

Name
Name is permanent
instance1-primary

Description (Optional)

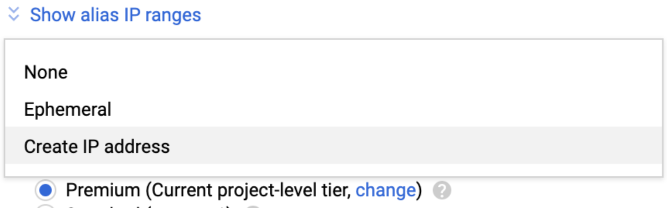
Subnet
lan1 (us-west1, 10.0.1.0/24)

Static IP address
Assign automatically

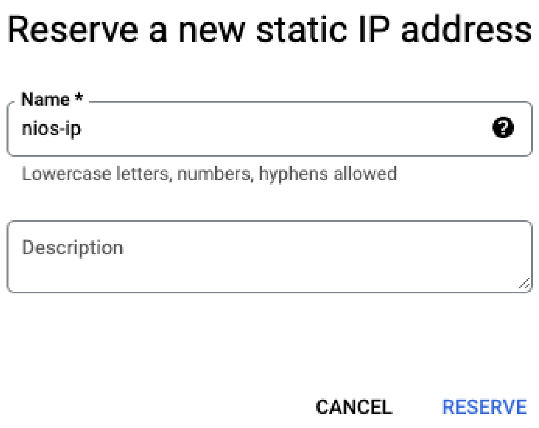
Purpose
Non-shared

9. Select **Create IP address** from the **External IP** dropdown.

Note: If you plan to connect to your vNIOS instance using VPN, Cloud Interconnect, or another private method, you may not need an External IP address.



10. In the Reserve IP dialog, enter a name for the reservation.
11. Select a Network Service Tier.
12. Click **RESERVE**.

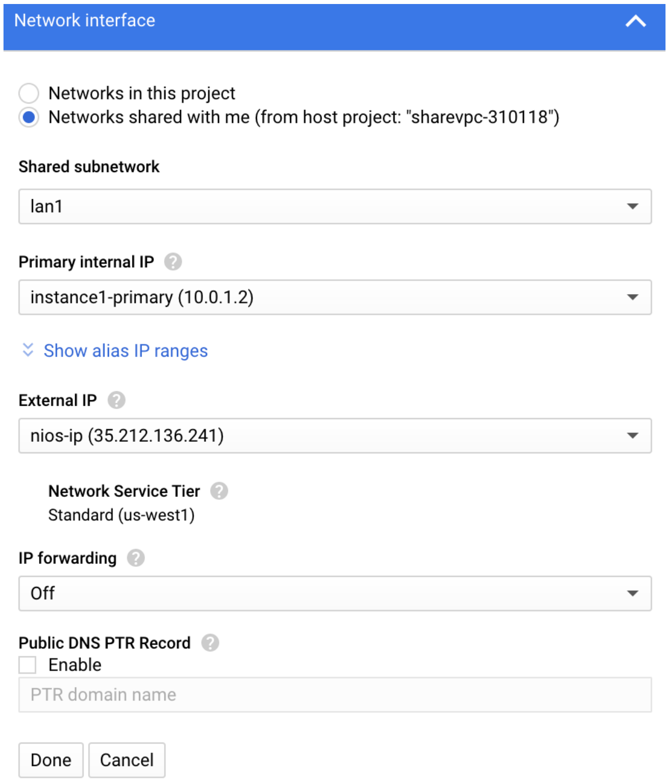


Reserve a new static IP address

Name *
nios-ip
Lowercase letters, numbers, hyphens allowed

Description

13. Click **Done**.



Network interface

○ Networks in this project
● Networks shared with me (from host project: "sharevpc-310118")

Shared subnetwork
lan1

Primary internal IP
instance1-primary (10.0.1.2)

Show alias IP ranges

External IP
nios-ip (35.212.136.241)

Network Service Tier
Standard (us-west1)

IP forwarding
Off

Public DNS PTR Record
□ Enable
PTR domain name

14. Click on **Create** to begin deployment.

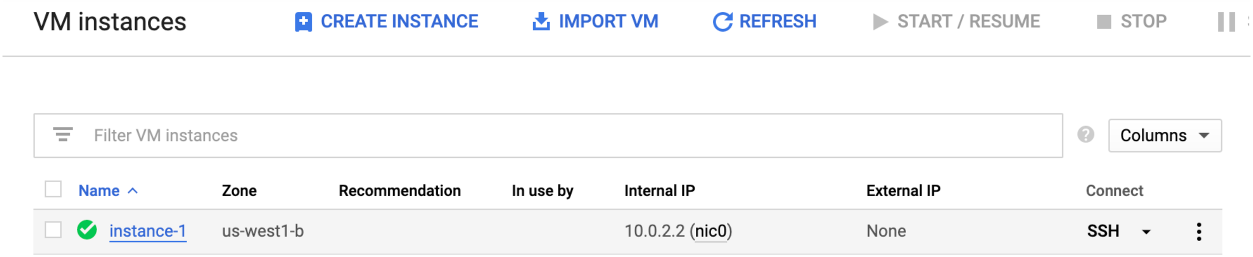
Connecting to Infoblox vNIOS for GCP Instance

Once your vNIOS for GCP appliance has been successfully deployed, you are ready to begin testing and using it. There are three methods available to connect to your vNIOS for GCP instance: virtual serial port, using SSH, and the Grid Manager GUI. To use the serial port, you will first need to enable it. To connect via SSH or Grid Manager GUI, you will need to know the public IP address of your instance. It is also possible to connect to your instance using the private IP address over VPN or Cloud Interconnect/Direct Peering, however that is outside the scope of this guide.

Virtual Serial Port

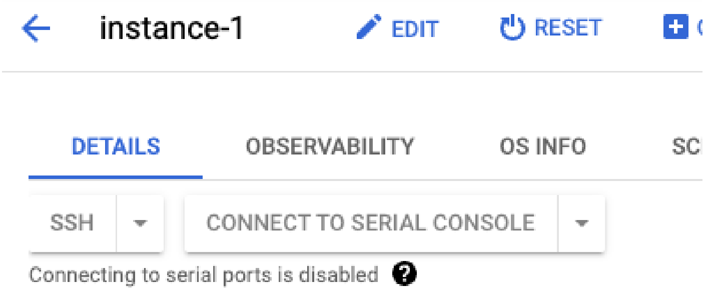
Follow the steps in this section to use the virtual serial port for your vNIOS for GCP instance.

1. In the GCP Console Navigation menu, expand **Compute Engine**. Select **VM Instances**.
2. Click on your new vNIOS instance.



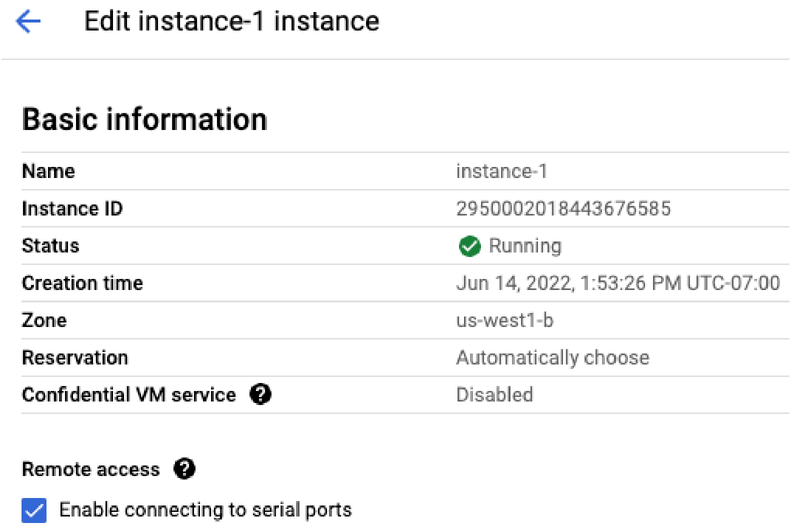
Name	Zone	Recommendation	In use by	Internal IP	External IP	Connect
instance-1	us-west1-b			10.0.2.2 (nic0)	None	SSH

3. Click **EDIT**.



Connecting to serial ports is disabled

4. Click the checkbox to **Enable connecting to serial ports** under Remote access.



Basic information

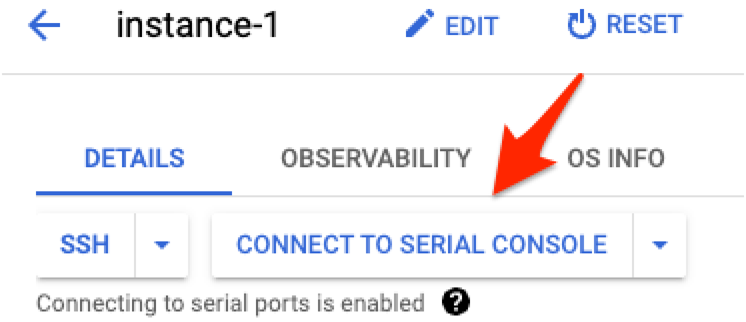
Name	instance-1
Instance ID	2950002018443676585
Status	Running
Creation time	Jun 14, 2022, 1:53:26 PM UTC-07:00
Zone	us-west1-b
Reservation	Automatically choose
Confidential VM service	Disabled

Remote access

☑ Enable connecting to serial ports

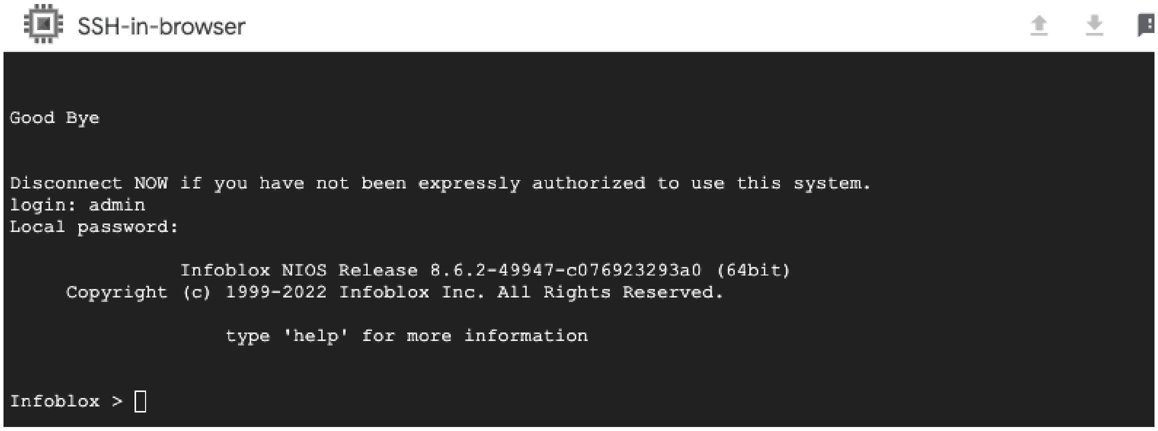
5. Scroll to the bottom of the page and click **Save.**

6. Back at the top of the **VM instance details** page, click **Connect to serial console**.



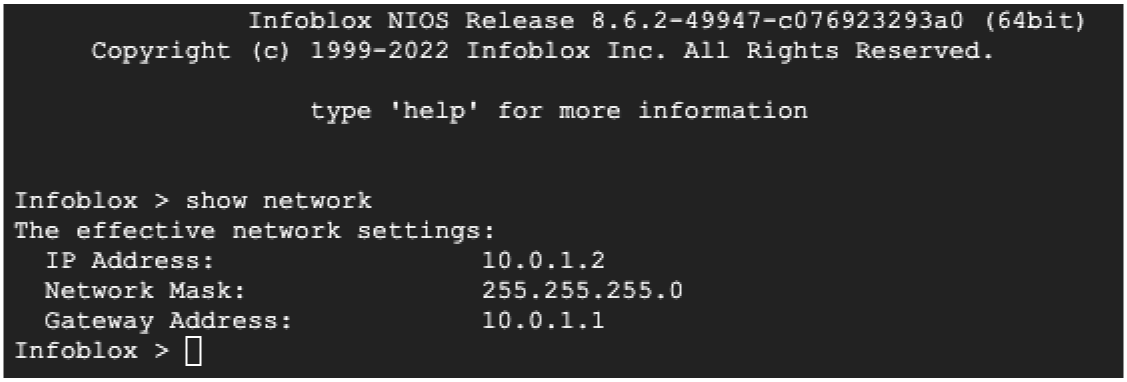
Connecting to serial ports is enabled

7. A new browser tab should open. This may take a few moments to connect as the console session is established with your Infoblox vNIOS for GCP appliance.



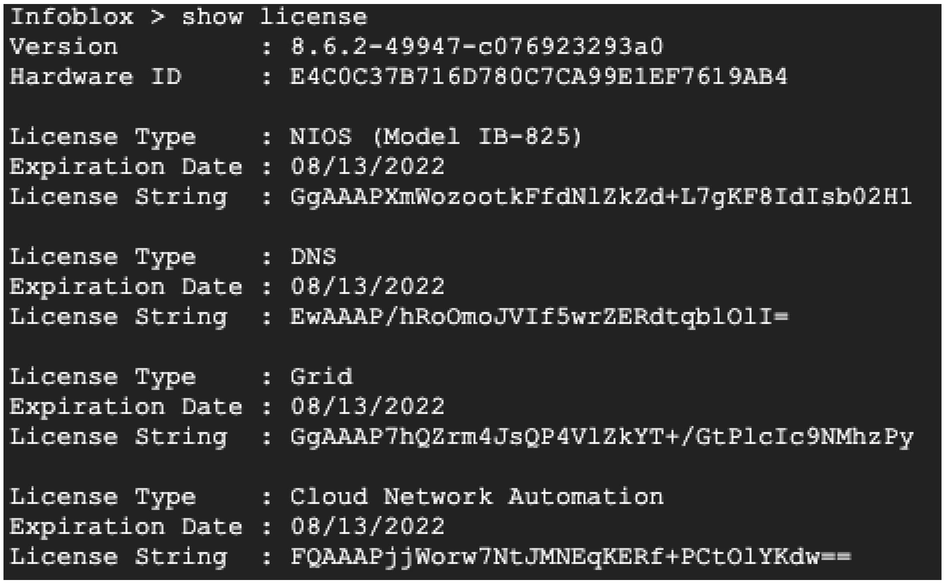
```
Good Bye


Disconnect NOW if you have not been expressly authorized to use this system.
login: admin
Local password:

               Infoblox NIOS Release 8.6.2-49947-c076923293a0 (64bit)
     Copyright (c) 1999-2022 Infoblox Inc. All Rights Reserved.

                   type 'help' for more information


Infoblox > 
```

8. Login using the default credentials (admin/infoblox).
9. Run the command **show network** to view the local network configuration.



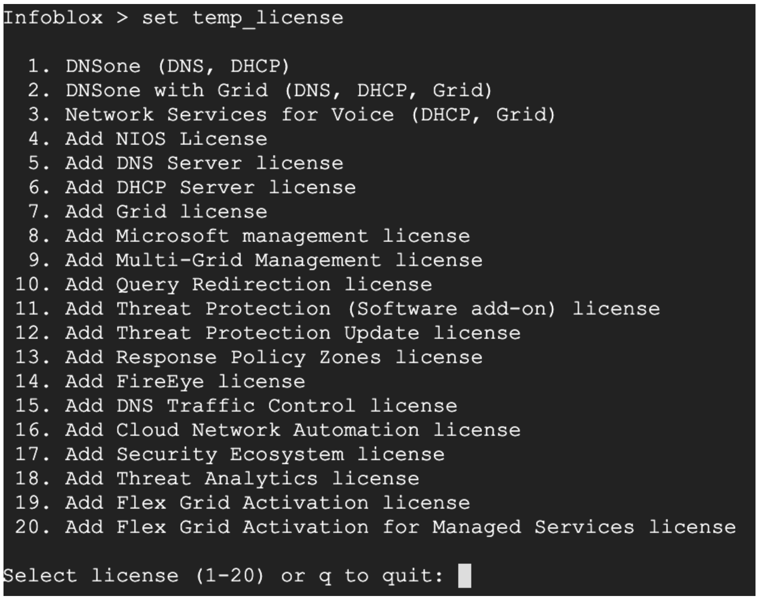
```
               Infoblox NIOS Release 8.6.2-49947-c076923293a0 (64bit)
     Copyright (c) 1999-2022 Infoblox Inc. All Rights Reserved.

                   type 'help' for more information


Infoblox > show network
The effective network settings:
  IP Address:                  10.0.1.2
  Network Mask:                255.255.255.0
  Gateway Address:             10.0.1.1
Infoblox > 
```

10. Run the command **show license** to review any installed licenses.



```
Infoblox > show license
Version         : 8.6.2-49947-c076923293a0
Hardware ID     : E4C0C37B716D780C7CA99E1EF7619AB4

License Type    : NIOS (Model IB-825)
Expiration Date : 08/13/2022
License String  : GgAAAPXmWozootkFfdNlZkZd+L7gKF8IdIsb02H1

License Type    : DNS
Expiration Date : 08/13/2022
License String  : EwAAAP/hRoOmoJVIf5wrZERdtqblOlI=

License Type    : Grid
Expiration Date : 08/13/2022
License String  : GgAAAP7hQZrm4JsQP4VlZkYT+/GtPlcIc9NMhzPy

License Type    : Cloud Network Automation
Expiration Date : 08/13/2022
License String  : FQAAAPjjWorw7NtJMNEqKERf+PCtOlYKdw==
```

11. You can use the **set temp_license** command to install additional temporary licenses if needed. Note: This is not needed if you set the temporary licenses in user-data during VM creation.



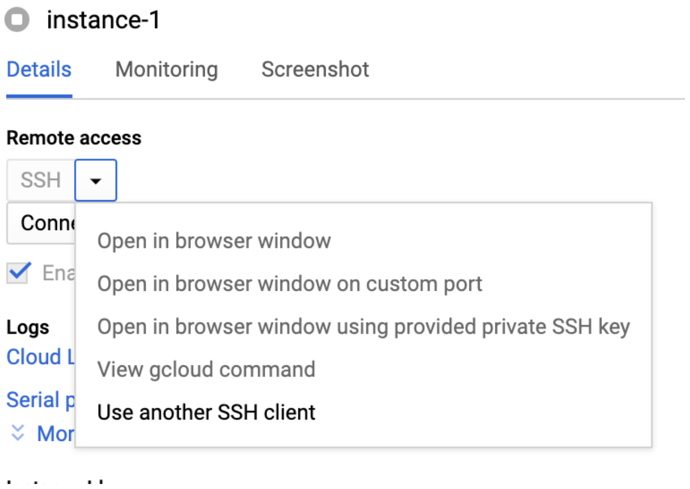
```
Infoblox > set temp_license

  1. DNSone (DNS, DHCP)
  2. DNSone with Grid (DNS, DHCP, Grid)
  3. Network Services for Voice (DHCP, Grid)
  4. Add NIOS License
  5. Add DNS Server license
  6. Add DHCP Server license
  7. Add Grid license
  8. Add Microsoft management license
  9. Add Multi-Grid Management license
 10. Add Query Redirection license
 11. Add Threat Protection (Software add-on) license
 12. Add Threat Protection Update license
 13. Add Response Policy Zones license
 14. Add FireEye license
 15. Add DNS Traffic Control license
 16. Add Cloud Network Automation license
 17. Add Security Ecosystem license
 18. Add Threat Analytics license
 19. Add Flex Grid Activation license
 20. Add Flex Grid Activation for Managed Services license

Select license (1-20) or q to quit:
```

12. For additional information on using the NIOS CLI, refer to https://docs.infoblox.com.

13. When you are done using the serial console, use the command **exit**, and then close the browser tab.

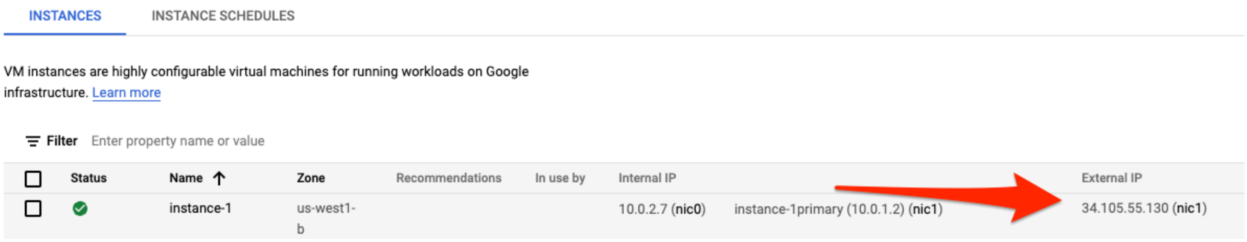
SSH

GCP provides multiple methods for establishing SSH connection to virtual machine instances as shown below. For additional information on using these connection methods, refer to https://cloud.google.com/compute/docs/instances/connecting-to-instance.



We will use a standard SSH client to connect for this guide. In order to connect via SSH, you will need to know the public IP address of your vNIOS for GCP VM instance. To find the public IP address:

1. On the **VM Instances** page in the GCP Console, locate your instance and the External IP.



INSTANCES   INSTANCE SCHEDULES

VM instances are highly configurable virtual machines for running workloads on Google infrastructure. Learn more

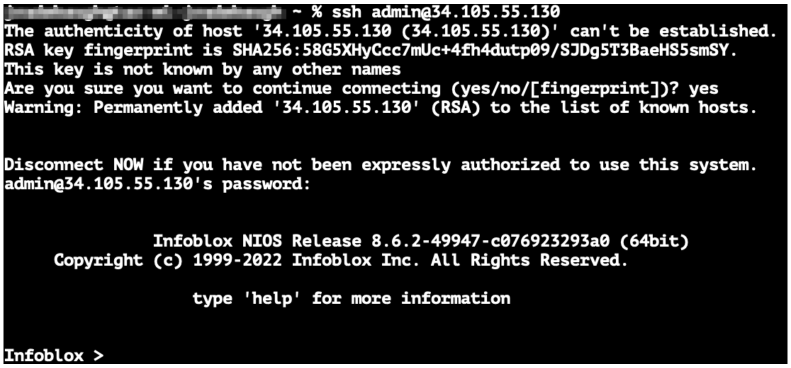
Filter Enter property name or value

□	Status	Name ↑	Zone	Recommendations	In use by	Internal IP		External IP
□	✓	instance-1	us-west1-b			10.0.2.7 (nic0)	instance-1primary (10.0.1.2) (nic1)	34.105.55.130 (nic1)

2. Click the copy icon to copy the external IP address.

Once you have the public IP address, you are ready to connect via SSH.

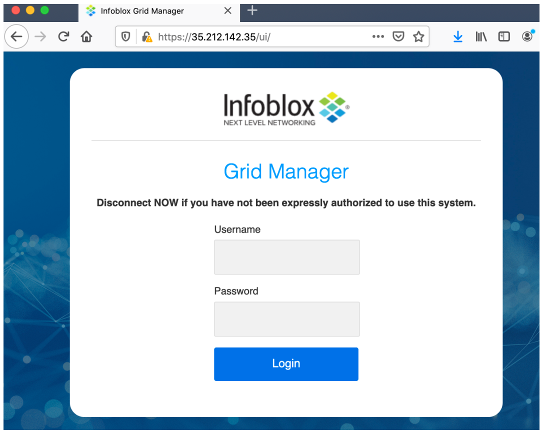
3. Open a PowerShell or Terminal window on your computer (Putty or other SSH clients can also be used).
4. Enter the command ssh admin@<ip_address> to start the SSH connection (use the public IP address of your vNIOS instance).
5. When prompted, type yes to add the IP address to your known_hosts file.
6. Enter the password (default is infoblox)



```
[redacted] ~ % ssh admin@34.105.55.130
The authenticity of host '34.105.55.130 (34.105.55.130)' can't be established.
RSA key fingerprint is SHA256:58G5XHyCcc7mUc+4fh4dutp09/SJDg5T3BaeHS5smSY.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '34.105.55.130' (RSA) to the list of known hosts.


Disconnect NOW if you have not been expressly authorized to use this system.
admin@34.105.55.130's password:


               Infoblox NIOS Release 8.6.2-49947-c076923293a0 (64bit)
     Copyright (c) 1999-2022 Infoblox Inc. All Rights Reserved.

                        type 'help' for more information


Infoblox >
```

Grid Manager

1. Open a web browser on your computer.
2. Navigate to https://<ip_address> (use the public IP address of your vNIOS instance).



Grid Manager

Disconnect NOW if you have not been expressly authorized to use this system.

Username

Password

Login

Note: By default, NIOS uses a self-signed certificate. Warnings about the connection being insecure are to be expected and might require that you add an exception before being able to connect.

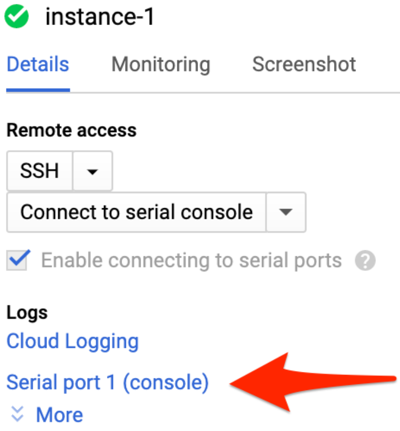
3. Login with the username **admin** and the password specified during deployment.
4. Accept the Infoblox End-User License Agreement.
5. Read and make a selection for the Infoblox Customer Experience Improvement Program.

Troubleshooting

If you are unable to connect to your vNIOS for GCP appliance, the first thing to check is that it started up successfully. The easiest way to do this is through the logs from the **Serial port 1 (console)**.

To check the Serial port logs:

1. On the VM instance details page, click on the **Serial port 1 (console)** link.



2. The Serial port viewer will be displayed and show a history of input/output.
3. Review for any errors.
    a. If you see a **Fatal error during Infoblox startup** message, the system is unable to load all required resources. The most common cause for this is not attaching the required second network interface when using a version that requires it. To recover from this error, delete the VM and create a new one, making sure to use two network interfaces for the VM.
    b. If you see the system successfully started up and is sitting at the login prompt, then the issue is external from the appliance. You will need to verify all network settings and firewall rules in your GCP environment.

Additional Resources

- Deployment Guide: Infoblox vDiscovery for Google Cloud Platform: https://insights.infoblox.com/resources-deployment-guides/infoblox-deployment-guide-infoblox-vdiscovery-for-gcp-google-cloud-platform.
- Infoblox NIOS and vNIOS Documentation: https://docs.infoblox.com.
- GCP Compute Engine Documentation: https://cloud.google.com/compute/docs.
- GCP Virtual Private Cloud Documentation: https://cloud.google.com/vpc/docs.

Infoblox
NEXT LEVEL NETWORKING

Infoblox enables next level network experiences with its Secure Cloud-Managed Network Services. As the pioneer in providing the world's most reliable, secure and automated networks, we are relentless in our pursuit of network simplicity. A recognized industry leader, Infoblox has 50 percent market share comprised of 8,000 customers, including 350 of the Fortune 500.

Corporate Headquarters | 3111 Coronado Dr. | Santa Clara, CA | 95054
+1.408.986.4000 | 1.866.463.6256 (toll-free, U.S. and Canada) | info@infoblox.com | www.infoblox.com