

DEPLOYMENT GUIDE

Infoblox vNIOS for Google Cloud Platform

Table of Contents

Introduction	2
Prerequisites.....	2
Limitations.....	2
Basic Workflow.....	2
Best Practices.....	3
GCP Objects and Terms.....	3
Infoblox vNIOS for GCP Use Cases	4
The DNS and RPZ Services Use Case.....	4
The Fault Tolerance and Disaster Recovery Use Case.....	4
DHCP Service for On-Premises Clients.....	5
The Maximum Availability Use Case.....	5
Install GCP Command Line Tools	5
GCloud CLI.....	5
Prepare your GCP Environment	5
Create VPCs.....	6
Create Firewall Policy and Rules.....	8
Create Outbound Rule.....	9
Create Inbound Rule.....	11
Infoblox vNIOS for GCP Image	15
Download vNIOS for GCP Image.....	15
Upload Infoblox vNIOS for GCP Image File.....	16
Create Bucket.....	17
Upload Image File to Bucket.....	19
Create Infoblox vNIOS for GCP Custom Image.....	20
Deploy Infoblox vNIOS for GCP Instance	22
Configure Instance Size and Image.....	23
Configure Network Interface(s).....	26
Single Network Interface.....	26
Two Network Interfaces.....	29
Configure User Data.....	34
Connecting to Infoblox vNIOS for GCP Instance	35
Virtual Serial Port.....	35
SSH.....	39
Grid Manager.....	40
Troubleshooting	41
Additional Resources	42

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 Google Cloud CLI.

- Navigate to GCP: <https://console.cloud.google.com/>.
- Create one or two new VPCs and Subnets (NIO 8.5 requires two network interfaces, each in a separate VPC. Starting with NIO 8.6, you can deploy one or two network interfaces).
- Upload image file and Create custom image.
- Launch your Infoblox vNIO for GCP appliance using the custom image.
- Once the Infoblox vNIO for GCP appliance has successfully deployed, verify its IP configuration.
- Connect to the Infoblox vNIO 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 NIO.
- Use Name Server Groups to simplify name server assignments for DNS configurations.

GCP Objects and Terms

Before implementing Infoblox vNIO for GCP, an administrator should understand common terms or objects available in GCP related to the implementation of vNIO. 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.
- **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.

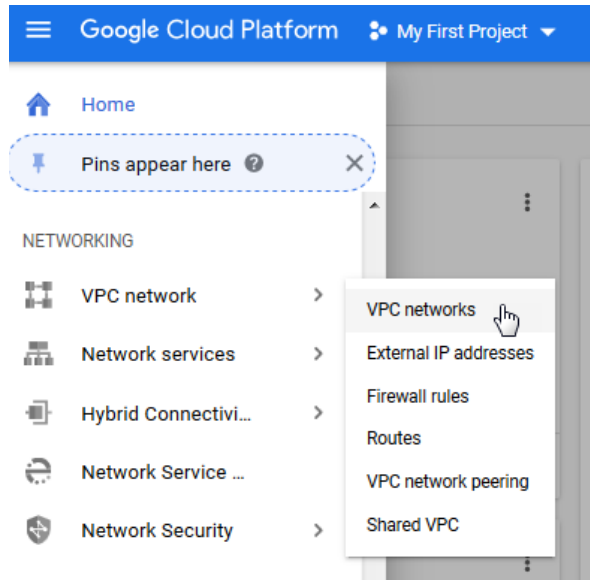
Prepare your GCP Environment

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.

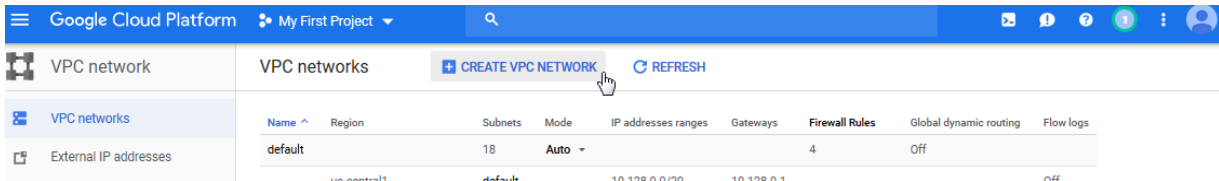
Create VPCs

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

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



2. Click **CREATE VPC NETWORK**.



3. 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

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


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 *
guide-lan1 

Lowercase letters, numbers, hyphens allowed

Description

Region *
us-west1  

IP stack type

IPv4 (single-stack)

IPv4 and IPv6 (dual-stack) 

IPv4 range *
10.0.1.0/24 

E.g. 10.0.0.0/24

8. Scroll down and click **CREATE**.

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.

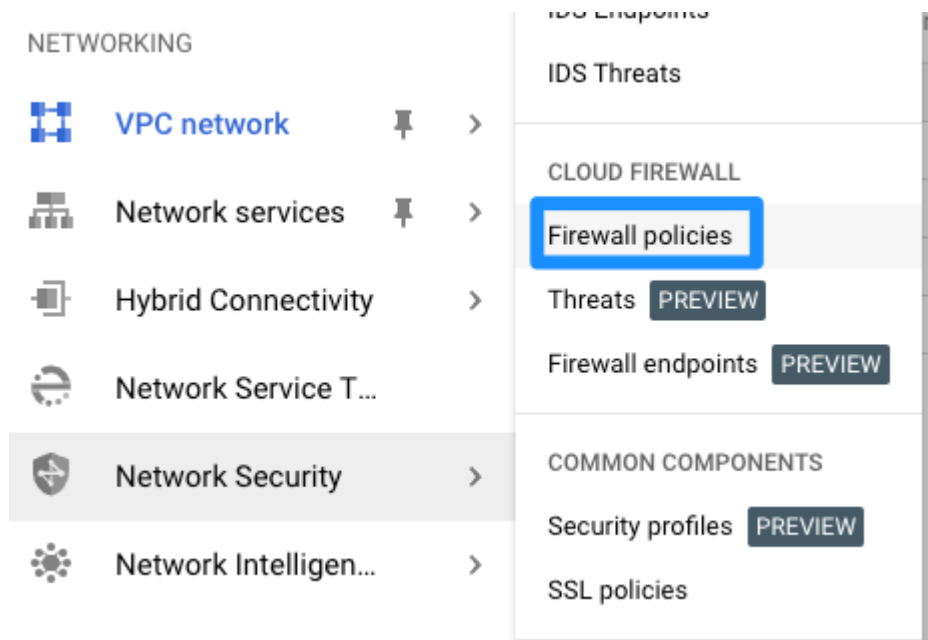
9. Wait and verify that your VPC network(s) are created successfully.

Create Firewall Policy and Rules

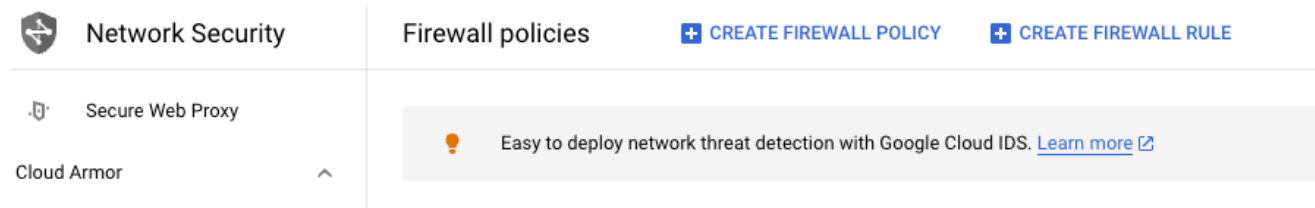
The firewall rules are used to control network access into and out of your VPC networks. In this example, we walk through the steps to create a policy with rules to allow all egress (outbound) traffic from your Infoblox vNIOS for GCP instance and to allow ingress (inbound) traffic on specific ports.

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 **Network Security** and select **Firewall Policies**.



2. Click **CREATE FIREWALL POLICY**.



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

4. Click **CONTINUE**.

1 Configure policy

Policy name * ?

Lowercase letters, numbers, hyphens allowed

Description

Deployment scope

- Global
- Regional

Create Outbound Rule

- 5. Click **ADD RULE**.

✓ 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](#)

i [Google Cloud Threat Intelligence](#) and [Geolocation](#) are Firewall Standard rules, which are paid features. [Learn more about pricing](#)

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

Create a firewall rule

Priority * 

Priority can be 0 - 2147483643.

Direction of traffic 

Ingress

Egress

Action on match 

Allow

Deny

Go to next

Proceed to L7 inspection PREVIEW

8. Expand the **Target Type** menu and select **All instances in the network**.
9. For the **DestinationIP type** select **IPv4**.
10. For the Destination IP ranges, enter **0.0.0.0/0** to allow outbound traffic to any destination.
11. Toggle the **Protocols and ports** option to **Allow all**.
12. Click **CREATE**.

Target

Target type
All instances in the network

Destination

IP type
IPv4

IP ranges
0.0.0.0/0

FQDNs

Geolocations

Address group

Google Cloud Threat Intelligence

Source

IP type
None

Protocols and ports

- Allow all
- Specified protocols and ports

CREATE CANCEL

Create Inbound Rule

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 **ADD RULE**.

2. Set the Priority.
3. Set the Direction of traffic to **Ingress** and Action on match to **Allow**.

Create a firewall rule

Priority * ?

Priority can be 0 - 2147483643.

Direction of traffic ?

Ingress

Egress

Action on match ?

Allow

Deny

Go to next

Proceed to L7 inspection **PREVIEW**

4. Expand the **Target Type** menu and select **All instances in the network**.
5. Expand the **IP type** menu and select **IPv4**.
6. 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.

Target

Target type ?

Source

IP type

IP ranges ?

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

Protocols and ports

- Allow all
- Specified protocols and ports

TCP

Ports

22,53,443

E.g. 20, 50-60

UDP

Ports

53,1194,2114

E.g. all

Other

Protocols

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

CREATE

CANCEL

11. Review the rules you created as well as those automatically created for you.
12. Click **CONTINUE**.

You can also add rules after the policy is created.

<input type="checkbox"/>	↑ Priority	Description	Direction of traffic	Targets	Source
<input type="checkbox"/>	0		Egress	Apply...	—
<input type="checkbox"/>	1		Ingress	Apply...	IPv4 ranges: 0.0.0.0/0
<input type="checkbox"/>	2147483541	Exclude communication with private IP ranges, leaving only Internet traffic to be inspected	Egress	Apply...	—
<input type="checkbox"/>	2147483542	Exclude communication with private IP ranges, leaving only Internet traffic to be inspected	Ingress	Apply...	IPv4 ranges: 10.0.0.0/8, 172.16
<input type="checkbox"/>	2147483543	Deny TOR exit nodes ingress traffic	Ingress	Apply...	Google Cloud Threat Intelligenc
<input type="checkbox"/>	2147483544	Deny known malicious IPs ingress traffic	Ingress	Apply...	Google Cloud Threat Intelligenc
<input type="checkbox"/>	2147483545	Deny known malicious IPs egress traffic	Egress	Apply...	—
<input type="checkbox"/>	2147483546	Deny sanctioned countries ingress traffic	Ingress	Apply...	Geolocations: Cuba (CU), Iran (I

CONTINUE

13. Click ASSOCIATE.

✓ **Configure policy**

✓ **Add rules**

3 **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

14. Select the VPC(s) to associate this policy with.
15. Click **ASSOCIATE**.

Associate policy with VPC networks

Select the VPC networks to associate this policy with

Filter vpc Enter property name or value

<input checked="" type="checkbox"/>	Network name ↑	Subnets	Regions
<input checked="" type="checkbox"/>	vpc1	1	1
<input checked="" type="checkbox"/>	vpc2	1	1

ASSOCIATE CANCEL

16. Click **CREATE**.

Infoblox vNIOs for GCP Image

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

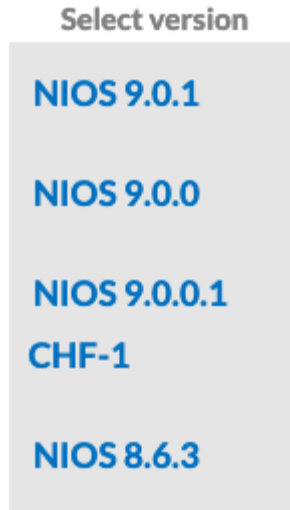
Download vNIOs for GCP Image

To download the virtual machine image file:

1. In your browser, navigate to <https://support.infoblox.com/> and sign in.
2. Click on **Download Center**.



3. Select the desired version of NIOS.



4. Scroll down to and expand the **vNIOS for GCP** option.
5. Click the link to download.



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 resizable 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	

6. 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.

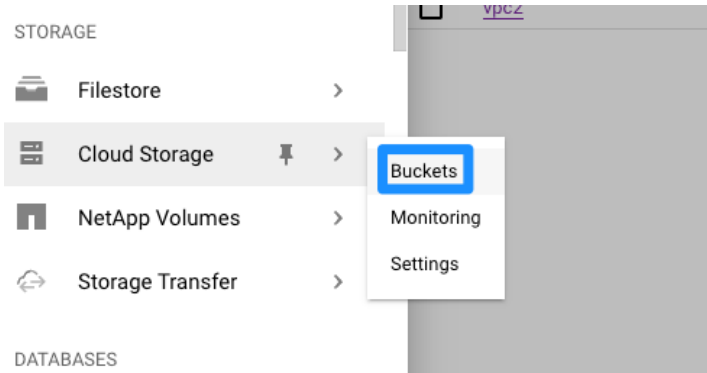
Upload Infoblox vNIOS for GCP Image File

Before you can deploy your Infoblox vNIOS for GCP appliance, you will need to create a storage bucket and upload the appliance image.

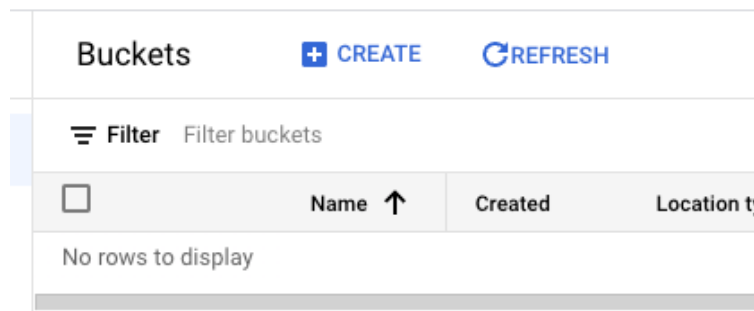
Create Bucket

To create a bucket using the GCP Console:

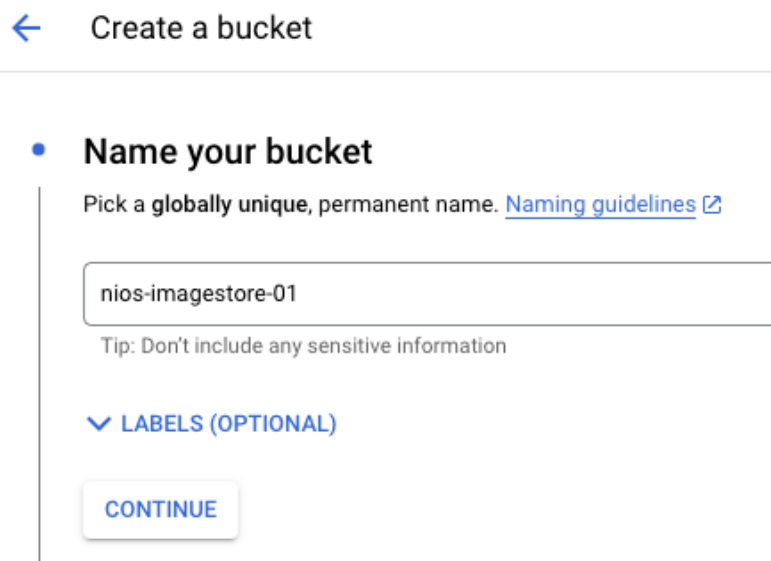
1. In the GCP Console Navigation menu, expand **Cloud Storage**; select **Buckets**.



2. Click **CREATE**.



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



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) ▼

CONTINUE

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

- **Choose a storage class for your data**

A storage class sets costs for storage, retrieval, and operations, with minimal differences in uptime. Choose if you want objects to be managed automatically or specify a default storage class based on how long you plan to store your data and your workload or use case. [Learn more](#)

 - Autoclass** 
Automatically transitions each object to hotter or colder storage based on object-level activity, to optimize for cost and latency. Recommended if usage frequency may be unpredictable. Can be changed to a default class at any time. [Pricing details](#)
 - Set a default class**
Applies to all objects in your bucket unless you manually modify the class per object or set object lifecycle rules. Best when your usage is highly predictable. Can't be changed to Autoclass once the bucket is created.
 - 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

CONTINUE

- Choose your desired access control options.
- 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](#)

CONTINUE

- Choose how to protect object data**

Protection tools: None

Data encryption: Google-managed

CREATE

CANCEL

Upload Image File to Bucket

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

- Click **UPLOAD FILES**.

← Bucket details

nios-imagestore-01

Location	Storage class	Public access	Protection
us-west1 (Oregon)	Standard	Not public	None

OBJECTS CONFIGURATION PERMISSIONS PROTECTION

Buckets > nios-imagestore-01

UPLOAD FILES **UPLOAD FOLDER** **CREATE FOLDER** **TRANSFER DA**


Filter by name prefix only ▾ **Filter** Filter objects and folders

<input type="checkbox"/>	Name	Size	Type	Created	Storage c
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.
3. Verify that the file upload completed successfully.


[UPLOAD FILES](#) [UPLOAD FOLDER](#) [CREATE FOLDER](#) [TRANSFER DATA](#) ▾ [MANAGE HOLDS](#) [DOWNLOAD](#)

Filter by name prefix only ▾ | **Filter** Filter objects and folders

<input type="checkbox"/>	Name	Size	Type	Created [?]	Storage class
<input type="checkbox"/>	 nios-8.6.3-51135-1241097029df-2...	2.4 GB	application/x-gzip	Sep 5, 2023, 1:14:00 PM	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.




← Object details

Buckets > nios-imagestore-01 > nios-8.6.3-51135-1241097029df-2023-06-23-04-17-51-ddi-resizable-43G.tar.gz 

[LIVE OBJECT](#) [VERSION HISTORY](#)

[↓ DOWNLOAD](#) [✎ EDIT METADATA](#) [👥 EDIT ACCESS](#) [🗑 DELETE](#)

Overview

Type	application/x-gzip
Size	2.4 GB
Created	Sep 5, 2023, 1:14:00 PM
Last modified	Sep 5, 2023, 1:14:00 PM
Storage class	Standard
Custom time	—
Public URL [?]	Not applicable
Authenticated URL [?]	https://storage.cloud.google.com/nios-imagestore-01/nios-8.6.3-51135-1241097029df-2023-06-23-04-17-51-ddi-resizable-43G.tar.gz 
gsutil URI [?]	gs://nios-imagestore-01/nios-8.6.3-51135-1241097029df-2023-06-23-04-17-51-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
```

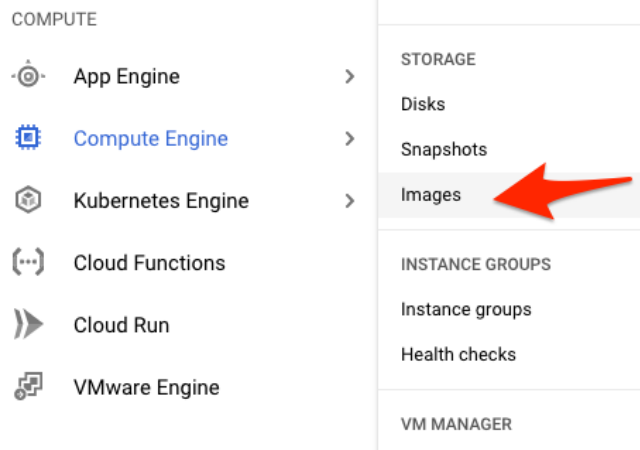
3. Follow prompts in your browser to login.
4. Run the following command to create your custom image:

```
gcloud compute images create <image_name> --guest-os-features MULTI_IP_SUBNET --source-uri <Source_URI>
```

- a. In the above example, replace **<image_name>** 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 **<Source_URI>** with the URI for the Infoblox vNIOS for GCP appliance image file you uploaded in the last section.

```
jradebaugh@IB-C02F61PQMD6N ~ % gcloud compute images create nios-863 --guest-os-features MULTI_IP_SUBNET --source-uri gs://nios-imagestore-01/nios-8.6.3-51135-1241097029df-2023-06-23-04-17-51-ddi-resizable-43G.tar.gz
Created [https://www.googleapis.com/compute/v1/projects/my-first-project-277818/global/images/nios-863].
NAME          PROJECT          FAMILY  DEPRECATED  STATUS
nios-863      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.

IMAGES IMAGE IMPORT HISTORY IMAGE EXPORT HISTORY

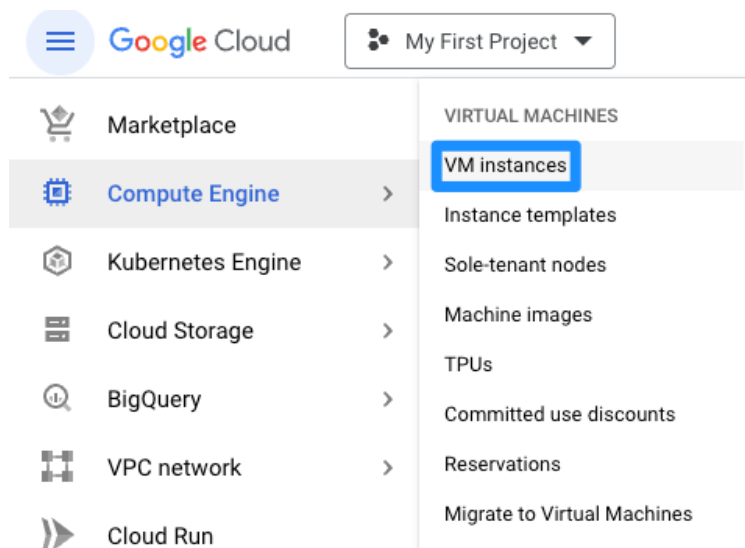
Filter Enter property name or value

<input type="checkbox"/>	Status	Name	Location	Archive size [?]	Disk size	Created by
<input type="checkbox"/>	✓	nios-863	us	2.53 GB	43 GB	my-first-project-277818

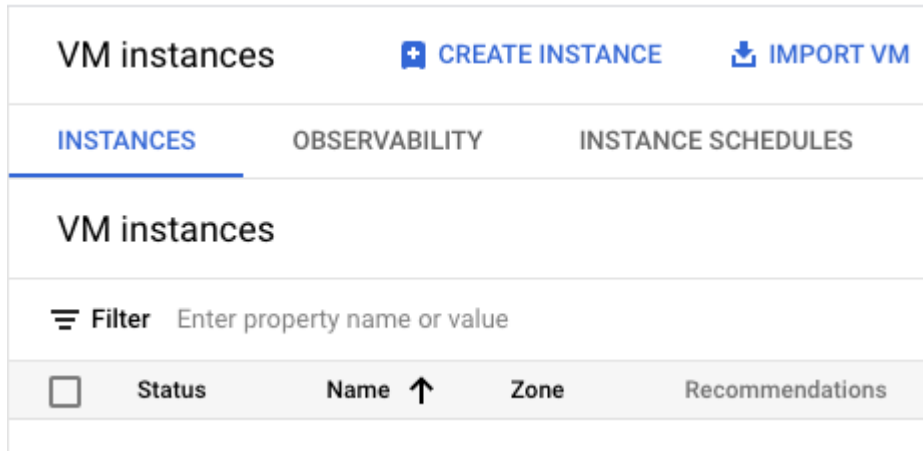
Deploy Infoblox vNIOS for GCP Instance

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 INSTANCE**.



Configure Instance Size and Image

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

Name *
instance-1

MANAGE TAGS AND LABELS

Region *
us-west1 (Oregon)

Region is permanent

Zone *
us-west1-b

Zone is permanent

3. In the Machine configuration section, select **General purpose**.
4. For Series, select **N1**.
5. Use the Machine type dropdown to select the instance size corresponding to desired NIOS model. Supported models and instance types are found in [vNIOS for GCP documentation](#) (the example used in this guide is an IB-V825).

Machine configuration

✓ General purpose

Compute optimized

Memory optimized

GPUs

Machine types for common workloads, optimized for cost and flexibility

	Series [?]	Description	vCPUs [?]	Memory [?]	Platform
<input type="radio"/>	C3	Consistently high performance	4 - 176	8 - 1,408 GB	Intel Sapp
<input type="radio"/>	E2	Low cost, day-to-day computing	0.25 - 32	1 - 128 GB	Based on
<input type="radio"/>	N2	Balanced price & performance	2 - 128	2 - 864 GB	Intel Casc
<input type="radio"/>	N2D	Balanced price & performance	2 - 224	2 - 896 GB	AMD EPYC
<input type="radio"/>	T2A	Scale-out workloads	1 - 48	4 - 192 GB	Ampere A
<input type="radio"/>	T2D	Scale-out workloads	1 - 60	4 - 240 GB	AMD EPYC
<input checked="" type="radio"/>	N1	Balanced price & performance	0.25 - 96	0.6 - 624 GB	Intel Skylake

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

n1-highmem-2 (2 vCPU, 1 core, 13 GB memory)



vCPU

2 (1 core)

Memory

13 GB

6. For Boot disk, click Change.

Boot disk [?]

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

CHANGE

7. Switch to the Custom images tab.

8. Select the custom image for your vNIOS for GCP appliance image from the dropdown.
9. For Boot disk type, select **Standard persistent disk**.
10. Set the **Size (GB)** field to match the size required for the appliance model type being deployed. Refer to [vNIOS for GCP documentation](#) for the supported disk sizes.
11. 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](#)

PUBLIC IMAGES

CUSTOM IMAGES

SNAPSHOTS

ARCHIVE SNAPSHOTS

Source project for images *

my-first-project-277818



CHANGE

Show deprecated images

Image *

nios-863



Created on Sep 5, 2023, 1:23:39 PM

Boot disk type *

Standard persistent disk



COMPARE DISK TYPES

Size (GB) *

250

✓ SHOW ADVANCED CONFIGURATION

SELECT

CANCEL

Configure Network Interface(s)

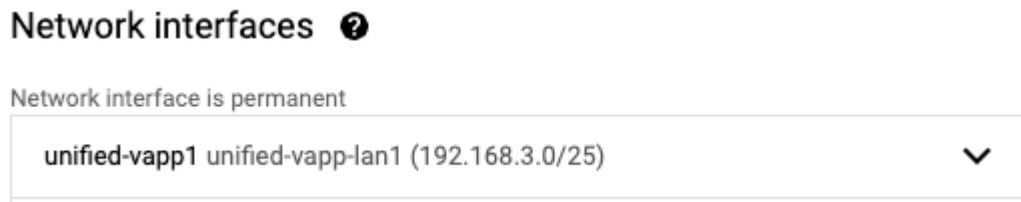
Infoblox vNIOS for GCP instances using NIOS version 8.6 and later can be deployed with one or two network interfaces. Instances deployed with a single network interface can be deployed into a standard VPC or a shared VPC. Older versions of NIOS require two network interfaces. Follow instructions in the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

Single Network Interface

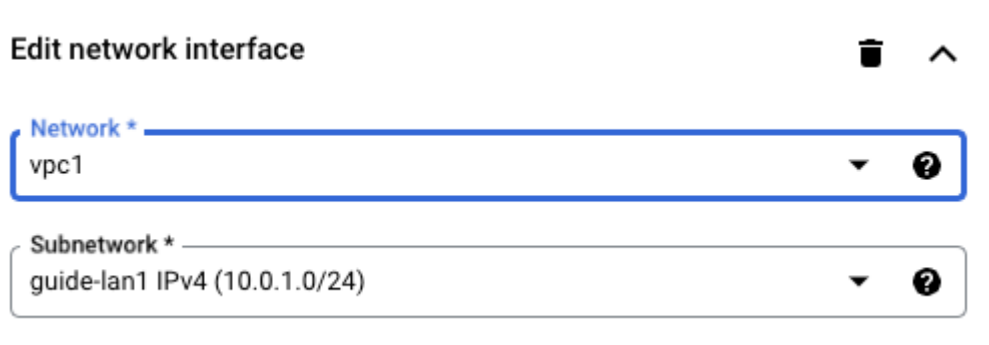
1. Expand the **Advanced Options** section.
2. Expand the **Networking** section.



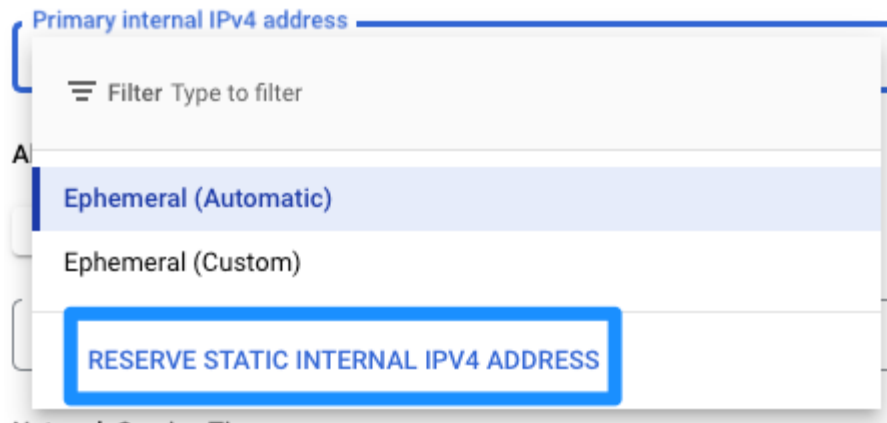
3. Under **Network Interfaces**, expand the default network interface.



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



6. 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 IPv4 dropdown.



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

Reserve a static internal IP address

Name *
nios-lan1 ?

Lowercase letters, numbers, hyphens allowed

Description

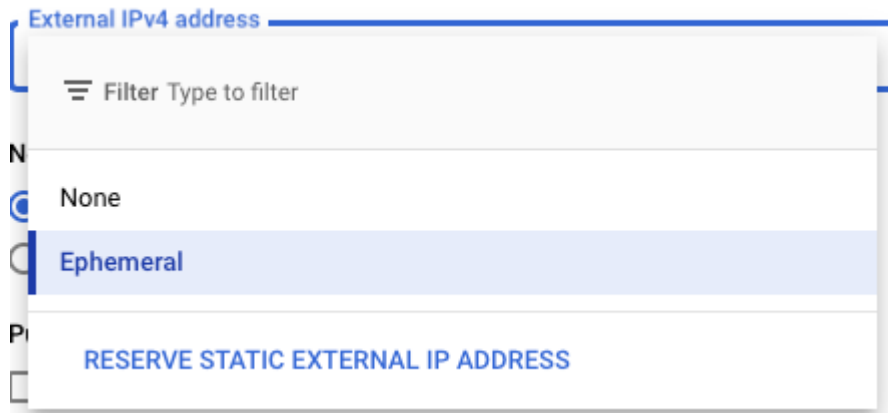
Static IP address
Assign automatically ▼

Purpose
Non-shared ▼ ?

CANCEL **RESERVE**

10. Select **RESERVE STATIC EXTERNAL IP ADDRESS** from the External IPv4 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.



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

Reserve a new static IP address

Name * ?
Lowercase letters, numbers, hyphens allowed

CANCEL **RESERVE**

14. Click **Done**.

Edit network interface 🗑️ ^

Network *

vpc1 ▼ ?

Subnetwork *

guide-lan1 IPv4 (10.0.1.0/24) ▼ ?

i To use IPv6, you need an IPv6 subnet range. [LEARN MORE](#) ↗

IP stack type

IPv4 (single-stack)

IPv4 and IPv6 (dual-stack)

Primary internal IPv4 address

nios-lan1 (10.0.1.2) ▼ ?

Alias IP ranges

[+ ADD IP RANGE](#)

External IPv4 address

nios-ip (34.168.224.0) ▼ ?

Network Service Tier

Premium

Public DNS PTR Record ?

Enable for IPv4

PTR domain name

[DONE](#)

Two Network Interfaces

1. Expand the **Advanced Options** section.
2. Expand the **Networking** section.
3. 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.

4. Expand the **Network** dropdown and select the VPC to use for the interface.
5. Select the subnet that you want to use for your interface.
6. For External IPv4 address, select **None**.

Note: You can add an external IP for the MGMT interface if desired, but this is not commonly needed.

7. Click **Done**.

Edit network interface


Network *

vpc2  

Subnetwork *

guide-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 IPv4 address

Ephemeral (Automatic)  

Alias IP ranges

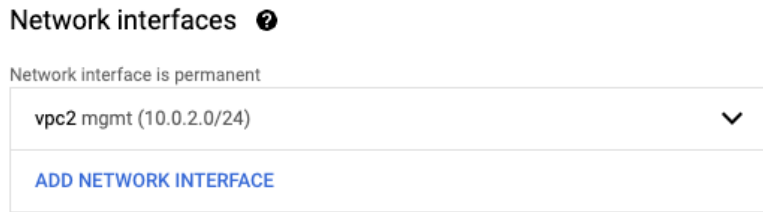
[+ ADD IP RANGE](#)

External IPv4 address

None  

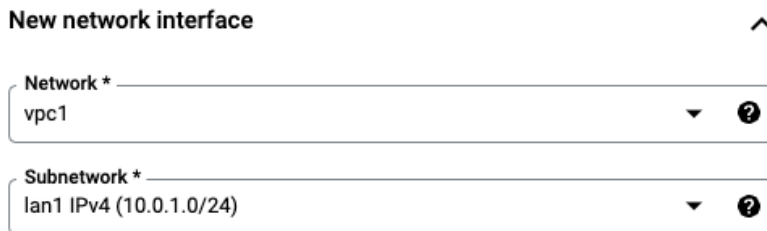
DONE

8. Click **Add network interface**.

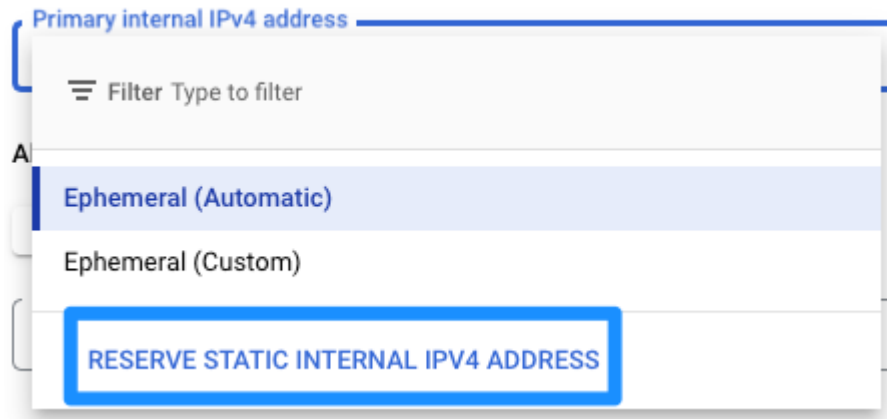


Note: This new network interface will be labeled as nic1 for the GCP VM instance. This will be the LAN1 interface in vNIOS.

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



10. 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.



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

Reserve a static internal IP address

Name *
nios-lan1 ?

Lowercase letters, numbers, hyphens allowed

Description

Static IP address
Assign automatically ▼

Purpose
Non-shared ▼ ?

CANCEL RESERVE

14. Select **RESERVE STATIC EXTERNAL IP ADDRESS** from the External IPv4 address 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.

External IPv4 address

☰ Filter Type to filter

N

None

Ephemeral


P

RESERVE STATIC EXTERNAL IP ADDRESS

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

16. Click **RESERVE**.

Reserve a new static IP address

Name *
nios-ip 



Lowercase letters, numbers, hyphens allowed



Description



CANCEL RESERVE

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

New network interface

Network *
vpc1  



Subnetwork *
guide-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 IPv4 address
nios-lan1 (10.0.1.2)  

Alias IP ranges

[+ ADD IP RANGE](#)

External IPv4 address
nios-ip (34.168.224.0)  




Network Service Tier
Premium

DONE

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

Network interfaces

Network interface is permanent

vpc2 guide-mgmt (10.0.2.0/24)	
vpc1 guide-lan1 (10.0.1.0/24)	 
ADD A NETWORK INTERFACE	

Configure User Data

1. Expand the **Management** panel.
2. Under Metadata, click **Add Item**.

Management

Description, deletion protection, reservations, and automation

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](#) 

[+ ADD ITEM](#)

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
-----------------------------	---

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

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.

Filter VM instances Columns

<input type="checkbox"/> Name ^	Zone	Recommendation	In use by	Internal IP	External IP	Connect
<input type="checkbox"/> instance-1	us-west1-b			10.0.2.2 (nic0)	None	SSH ⌵ ⋮

- Click **EDIT**.

← **instance-1** EDIT RESET + (

DETAILS OBSERVABILITY OS INFO SC

SSH ⌵ CONNECT TO SERIAL CONSOLE ⌵

Connecting to serial ports is disabled ?

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

← Edit instance-1 instance

Basic information

Instance ID	6363143126170344012
Status	✓ Running
Creation time	Sep 5, 2023, 2:59:00 PM UTC-07:00
Zone	us-west1-a
Reservation	Automatically choose
Confidential VM service ?	Disabled

Rename

VM instance name

instance-1

Tip: Reference the VM by its URI in API calls and gcloud CLI commands to make sure your project isn't affected by any name changes. [Learn more](#) ↗

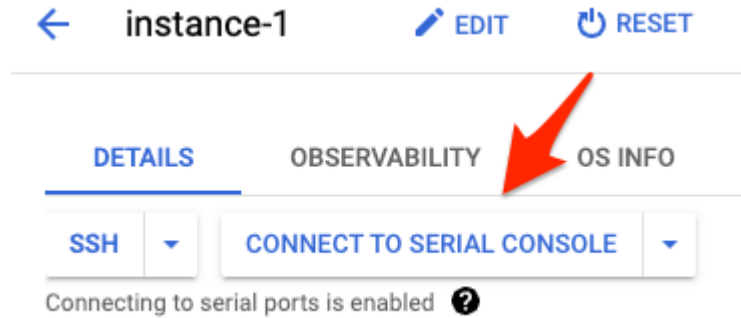
Remote access ?

Enable connecting to serial ports

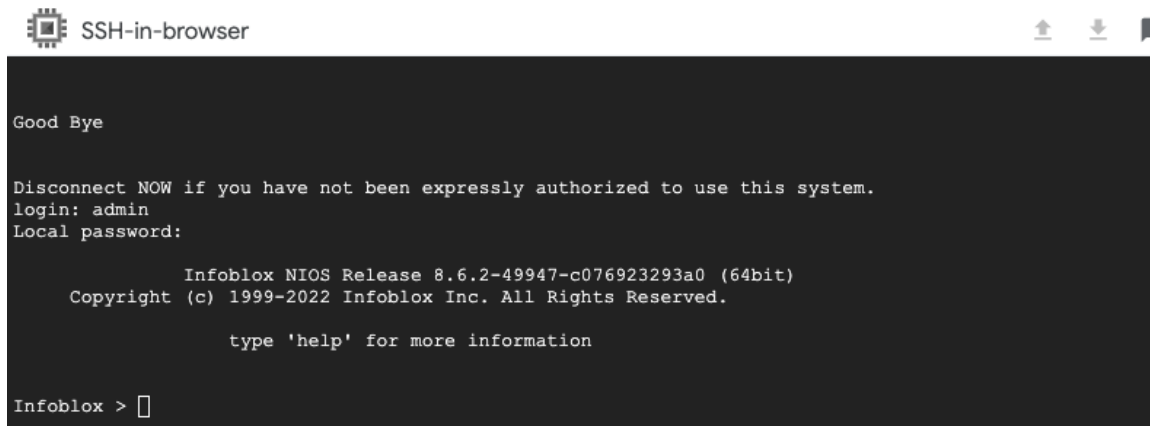
5. Scroll to the bottom of the page and click **Save**.



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



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.



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 : GgAAAPXmWozootkFfdN1ZkZd+L7gKF8IdIsb02H1

License Type : DNS
Expiration Date : 08/13/2022
License String : EwAAAP/hRoOmoJVIf5wrZERdtqbl01I=

License Type : Grid
Expiration Date : 08/13/2022
License String : GgAAAP7hQZrm4JsQP4V1ZkYT+/GtPlcIc9NMhzPy

License Type : Cloud Network Automation
Expiration Date : 08/13/2022
License String : FQAAAPjjWorw7NtJMNEqKERf+Pct01YKdw==
```

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: █

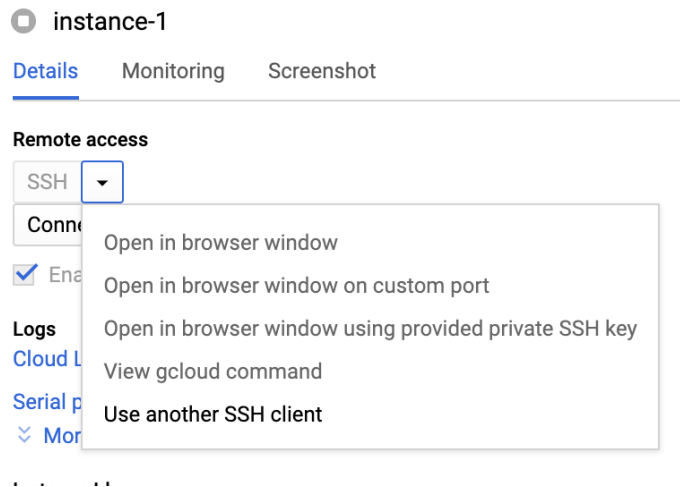
```

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.

VM instances are highly configurable virtual machines for running workloads on Google infrastructure. [Learn more](#)

Filter Enter property name or value

<input type="checkbox"/>	Status	Name ↑	Zone	Recommendations	In use by	Internal IP	External IP
<input type="checkbox"/>	✓	instance-1	us-west1-b			10.0.2.7 (nic0)	instance-1-primary (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`)

```
~ % 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+4Fn4dutp09/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:

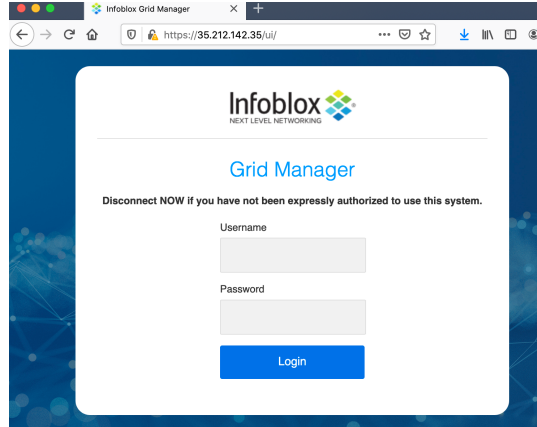
Infoblox NIOS Release 8.6.2-49947-c076923293a0 (64bit)
Copyright (c) 1999-2022 Infoblox Inc. All Rights Reserved.

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).



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.

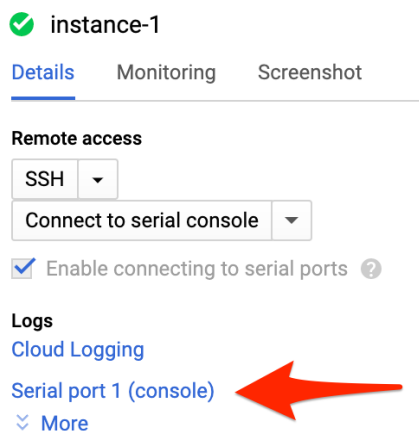
3. Login with the username admin and the password specified during deployment.
4. Accept the Infoblox End-User License Agreement.
5. Read and make a selection for the Infoblox Customer Experience Improvement Program.

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-v-discovery-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 unites networking and security to deliver unmatched performance and protection. Trusted by Fortune 100 companies and emerging innovators, we provide real-time visibility and control over who and what connects to your network, so your organization runs faster and stops threats earlier.

Corporate Headquarters
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054
+1.408.986.4000
www.infoblox.com