Infoblox

DEPLOYMENT GUIDE

Infoblox vNIOS for Oracle Cloud Infrastructure (OCI)

Table of Contents

Introduction

Infoblox vNIOS for Oracle Cloud Infrastructure (OCI) is a virtual appliance designed for deployment as a Virtual Machine (VM) instance on OCI. Infoblox vNIOS for OCI enables you to deploy robust, manageable and cost effective Infoblox appliances in the Oracle Cloud.

Infoblox NIOS is the underlying software running on Infoblox appliances and virtual appliances which provide 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), DHCP (Dynamic Host Configuration Protocol, IPAM (IP address management) and other services.

Infoblox vNIOS for OCI supports deployment of a Cloud Platform (CP) appliance which can be joined to your existing on-premises Infoblox Grid. The CP appliance allows you to extend DNS and IPAM services into your OCI Virtual Cloud Networks (VCN). The vNIOS appliance can be configured as a primary DNS server for your OCI VCNs to gain advantages of centralized management, security, and other features of Infoblox DNS. You can also use Infoblox Cloud Network Automation with vNIOS for OCI to enable automated provisioning of apps and services in OCI.

Prerequisites

The following are prerequisites to deploying and managing an Infoblox vNIOS for OCI appliance:

- Valid OCI account.
- Permissions on OCI to create VCNs, VMs, and related resources.
- On-premises Infoblox Grid which the vNIOS for OCI appliance will connect to.
- Understanding of basic networking concepts and tools, including public and private IP addressing, DNS, Secure Shell (SSH), and command line/terminal applications.

Workflow

The following are the basic steps to deploy and configure an Infoblox vNIOS for OCI instance (steps 1 and 2 may be skipped if deploying into an existing VCN):

1. Deploy OCI VCN and subnets.
2. Configure VCN security, gateway, and routes.
3. Create Infoblox vNIOS for OCI instance.
4. Join vNIOS instance to Grid.

OCI Objects and Terms

Before deploying Infoblox vNIOS for OCI, an administrator should understand some common terms and resources available in OCI which relate to the deployment of vNIOS. The following are some of these common terms and resources:

- **Compartment**: A container used for grouping related resources. Compartments can be used to organize and manage access to resources.
- **Console Connection**: OCI Console Connections provide virtual serial or VNC consoles for connecting to and troubleshooting your compute instances.
- **FastConnect**: OCI FastConnect is used to establish private connections between OCI VCNs and on-premises networks.

- **Object Storage**: OCI Object storage provides storage for unstructured data of any type. Objects are organized into logical storage containers, called Buckets.
- **Security List**: Security Lists serve as a virtual firewall in OCI VCNs. Ingress and Egress rules are added to security lists to allow communication outside of VCNs.
- **VCN**: Virtual Cloud Networks are private virtual networks deployed in an OCI region. Within VCNs, you can configure subnets, firewall rules, and gateways for external communication.
- **VNIC**: Virtual Network Interface Cards are used to connect instances to VCNs, providing all network communication.

Infoblox vNIOS for OCI Use Cases

Extending your Infoblox Grid into OCI with vNIOS appliances can provide solutions for many hybrid cloud infrastructure requirements and issues. The following are some of the common use cases:

DNS and RPZ for Public Cloud

A vNIOS appliance can be used as the primary DNS server in OCI VCNs. This allows you to extend your enterprise DNS and RPZ services into the public cloud. Clients running on OCI, attached to your VCNs, are able to use the same consolidated and secure DNS service as clients on-premises and in your private cloud environments. vNIOS appliances running the DNS service can be deployed in shared services virtual cloud networks and used for DNS resolution across other virtual cloud networks via peering relationships.

IPAM and DNS Automation for Public Cloud

Infoblox Cloud Platform appliances, such as the CP-V2205 available for OCI, process API requests for automated provisioning of apps and services in your cloud environments. Since API requests are processed locally on the CP appliance, these features are sustained even if there is a network outage between your on-premises Grid Master and the vNIOS for OCI appliance. Additionally, supported Infoblox plugins for tools such as Ansible and Terraform can be used to integrate the CP appliances running on OCI into your DevOps automation workflows.

DHCP Service for On-Premises Clients

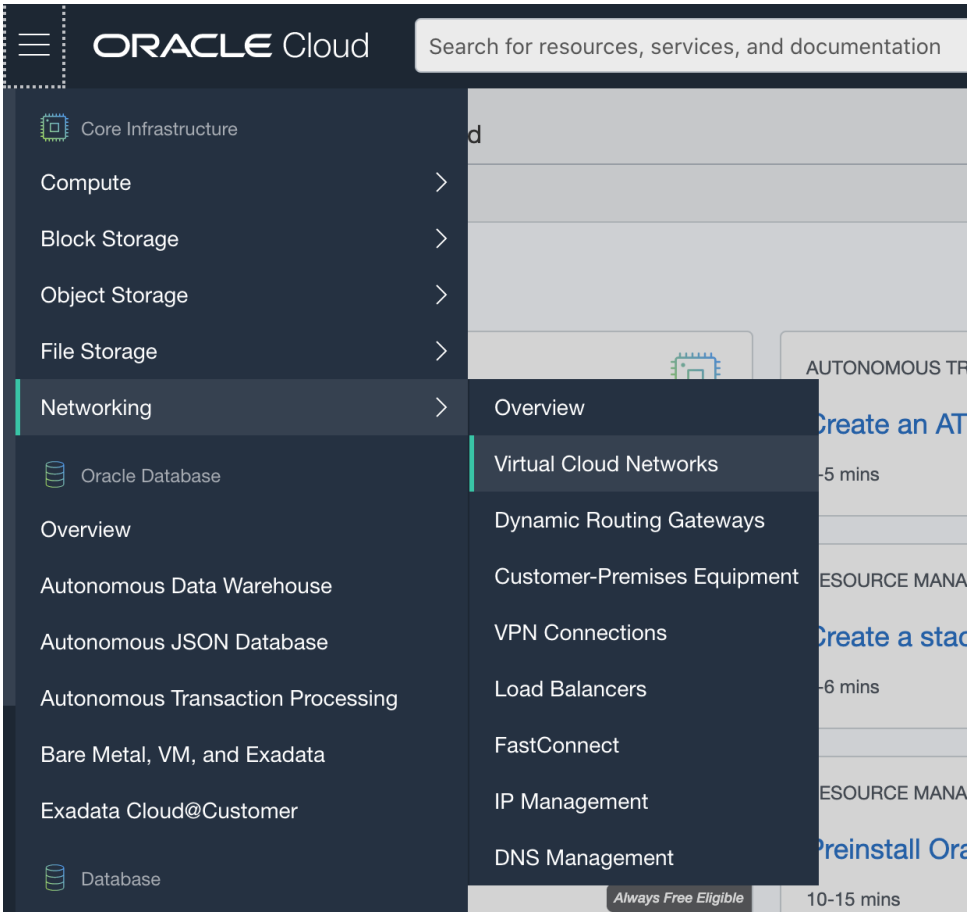
A vNIOS appliance running on OCI can provide DHCP service for your on-premises clients. This DHCP appliance can serve as a primary DHCP server for your on-premises networks. Using a vNIOS appliance running on OCI for DHCP requires using DHCP Relay or IP Helper on your router or layer 3 switch to send DHCP traffic from your on-premises network to your OCI VCN.

Deploy OCI VCN

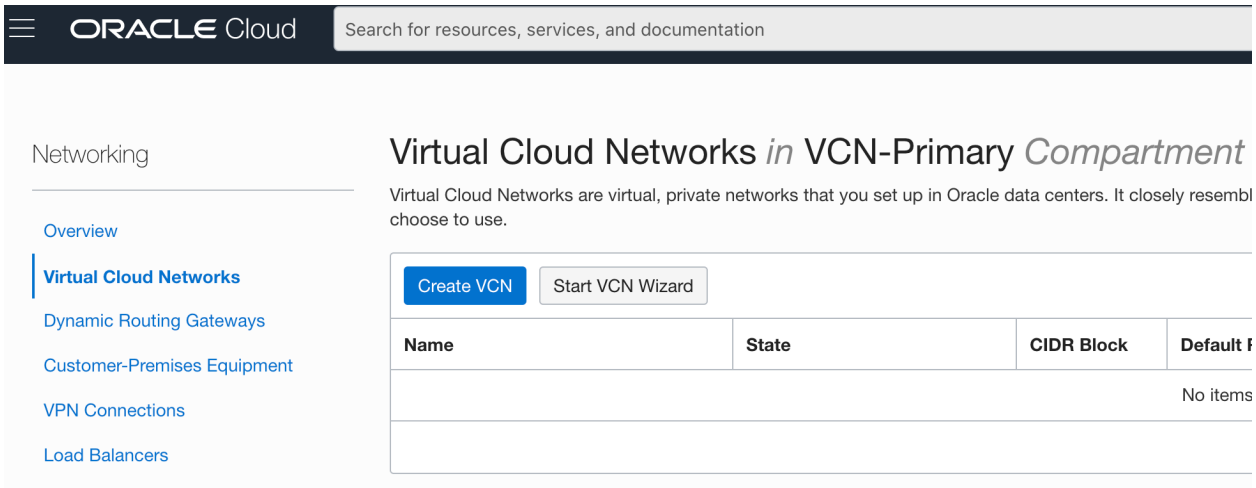
Prior to deploying a vNIOS for OCI instance, you will need a VCN in the desired region. If you are deploying vNIOS into an existing VCN, ensure you have two available subnets and security list rules will allow the minimum necessary for Infoblox Grid communication, then skip ahead to the Deploy vNIOS Instance in OCI section.

Create VCN

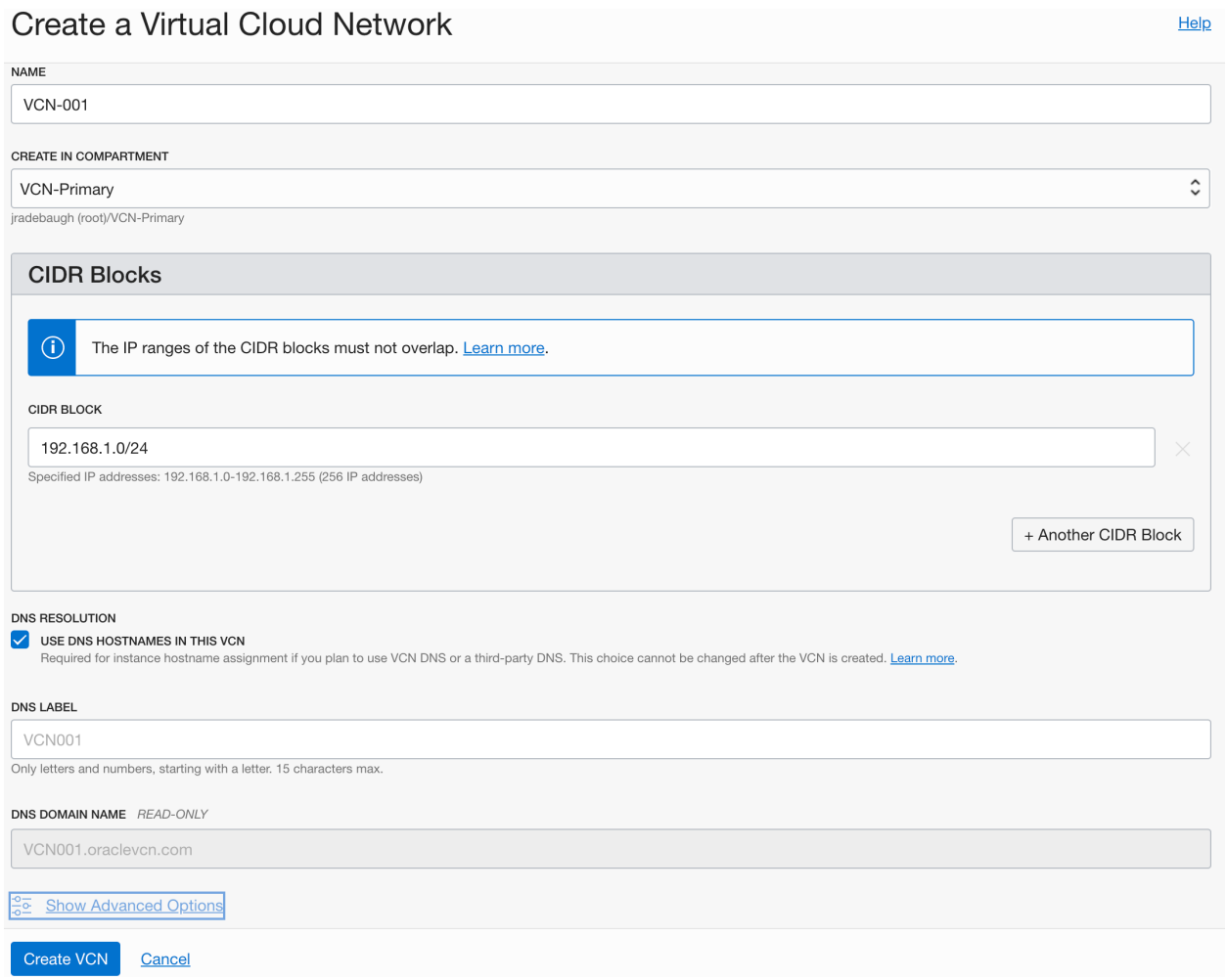
1. Login to the Oracle Cloud Infrastructure Console.
2. In the Service menu in the upper left corner, hover on **Networking** to expand.
3. Select **Virtual Cloud Networks**.



4. Use the Compartment dropdown to select the desired compartment.
5. Click on **Create VCN**.



6. In the Create a Virtual Cloud Network pane, enter a name for your VCN.
7. If needed, use the dropdown to select the compartment where you will create the VCN.
8. Enter a CIDR Block for your VCN, for example **192.168.1.0/24**.
9. Click on **Create VCN**.



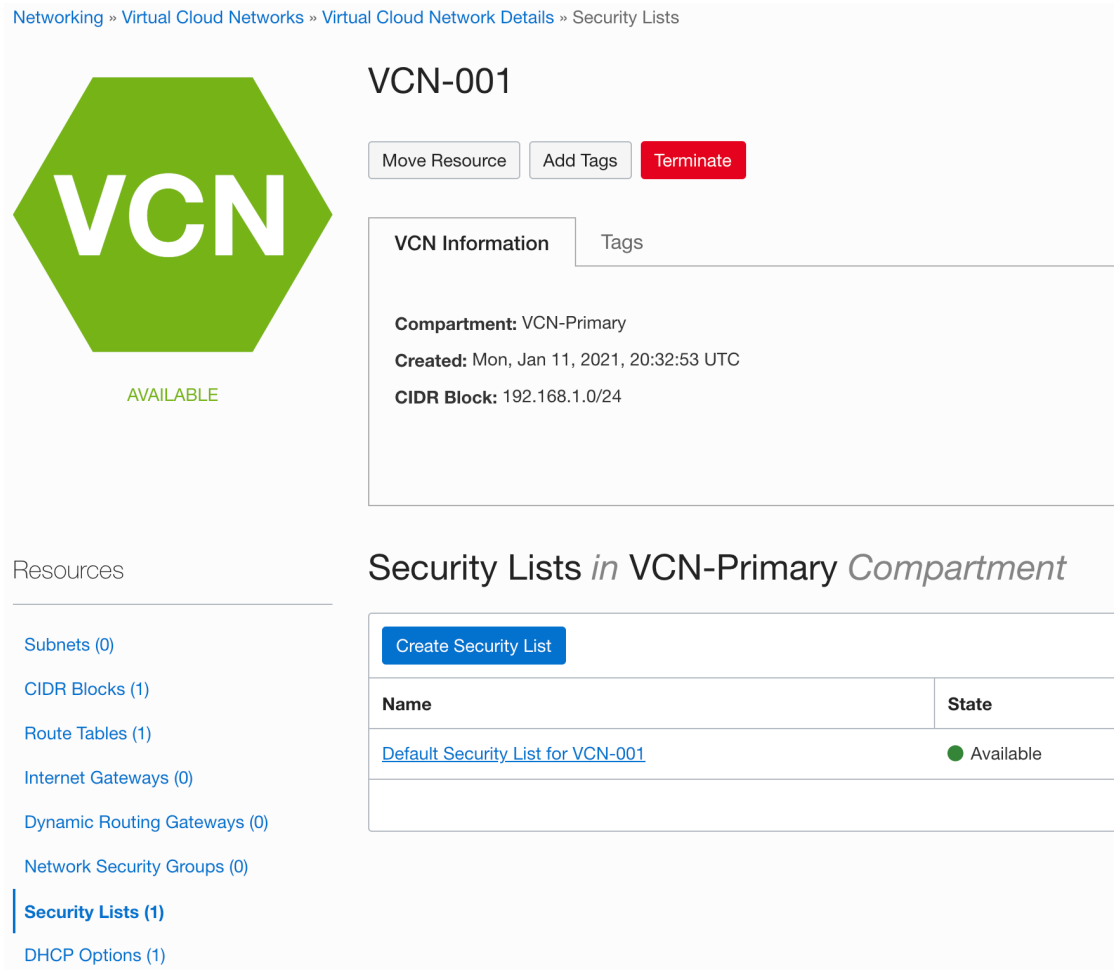
10. When the VCN has been successfully created, you will be taken to the Virtual Cloud Network Details page.

Configure Security List

Next, we'll create a Security List to control ingress and egress of Grid and services traffic for the vNIOS instance.

1. From the VCN Details page, select **Security Lists** under resources.
2. Click on **Create Security List**.

Note: You could instead add rules to the Default Security List for the VCN. Creating a new list allows you to be more selective about which subnets it is applied to.

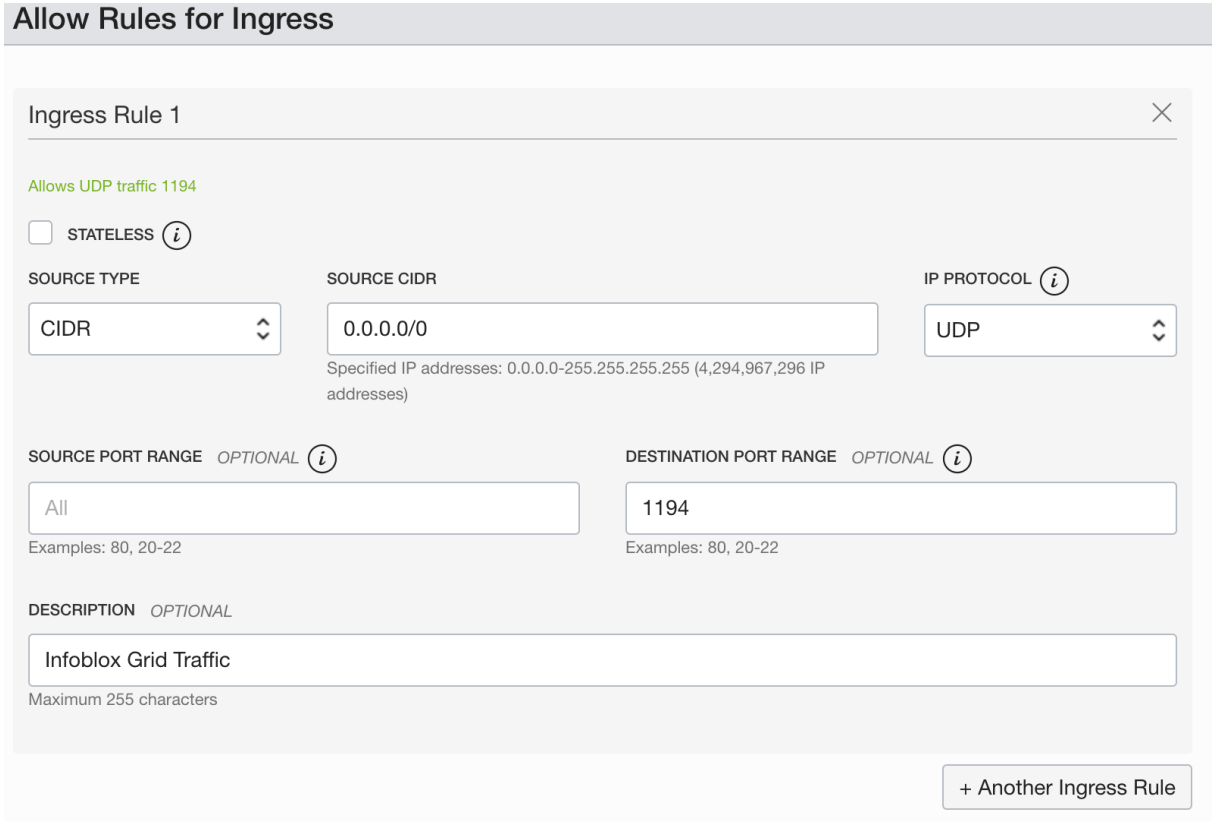


3. In the Create Security List window, enter a name for your Security List.
4. If needed, use the dropdown to select the compartment.
5. Click on **+ Another Ingress Rule**.

6. Under Ingress Rule 1, leave Source Type as **CIDR**.
7. Enter a Source CIDR range.

Warning: For this guide, we use 0.0.0.0/0 to allow traffic from any source IP. For production environments, it is recommended that you limit the range of source IPs to only those necessary.

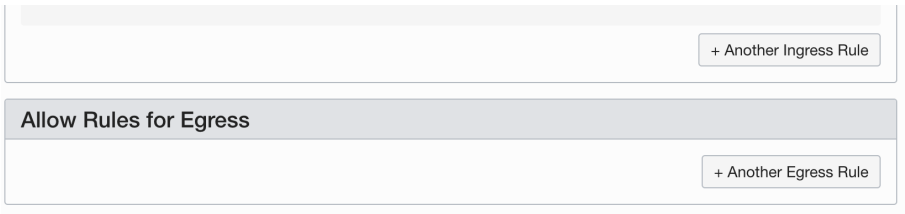
8. Select **UDP** from the IP Protocol dropdown.
9. For Destination Port Range, enter **1194**.
10. Optionally, enter a Description.



11. Repeat Steps 5-10 for the protocols and ports you plan to use from the table below. At a minimum, you will need rules for UDP 1194 and 2114 to allow for Infoblox Grid traffic.

Type	Protocol	Port Range	Description
SSH	TCP	22	SSH for Administration
DNS (UDP)	UDP	53	UDP DNS
DNS (TCP)	TCP	53	TCP DNS
HTTPS	TCP	443	HTTPS for Grid Manager
Custom UDP Rule	UDP	1194	NIOS Grid Traffic
Custom UDP Rule	UDP	2114	NIOS Grid Traffic
Custom UDP Rule	UDP	67-68	DHCP

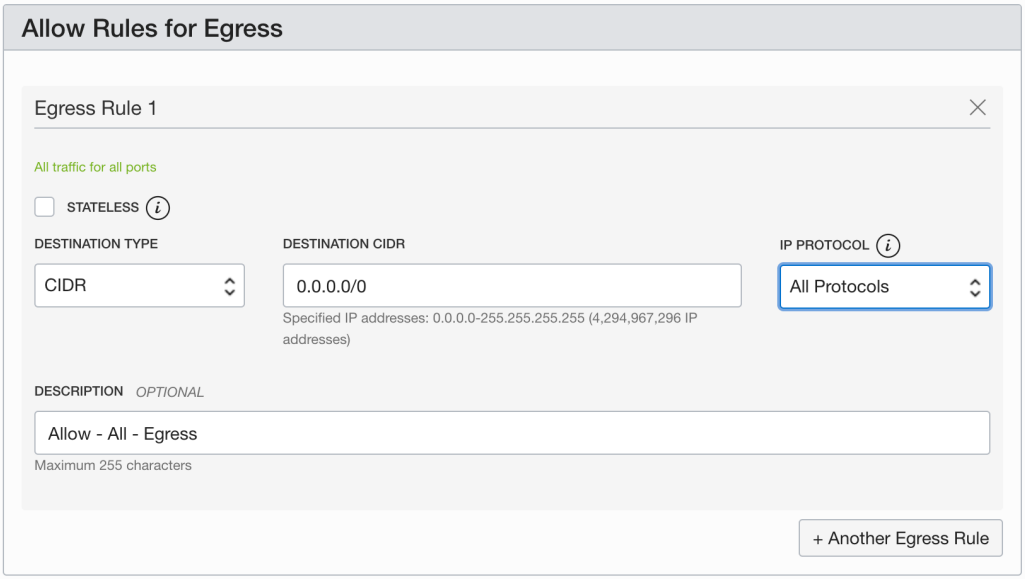
12. Once you have entered all necessary Ingress rules, click on **+ Another Egress Rule**.



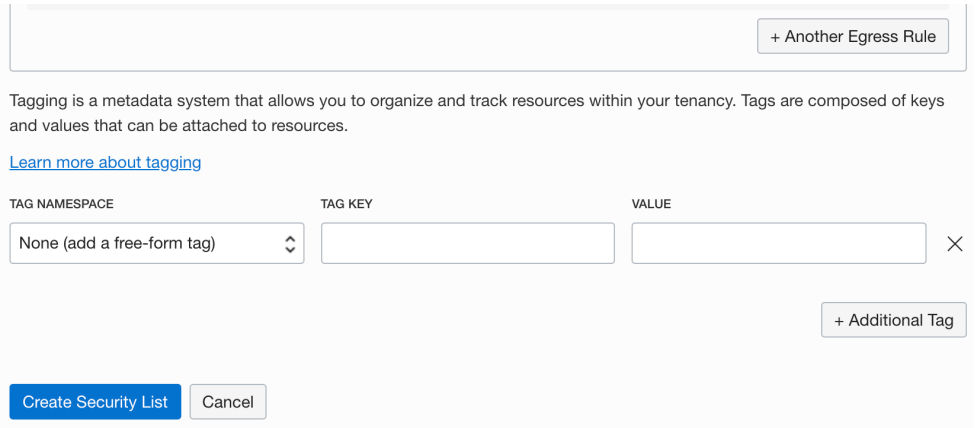
13. Under Egress Rule 1, leave Source Type as **CIDR**.
14. Enter a Destination CIDR. Example, **0.0.0.0/0**.
15. Use the IP Protocols dropdown to select **All Protocols**.

Note: For this guide, we use 0.0.0.0/0 and All Protocols to allow all egress traffic. You can optionally add more restrictive rules to limit egress traffic.

16. Optionally, enter a Description.



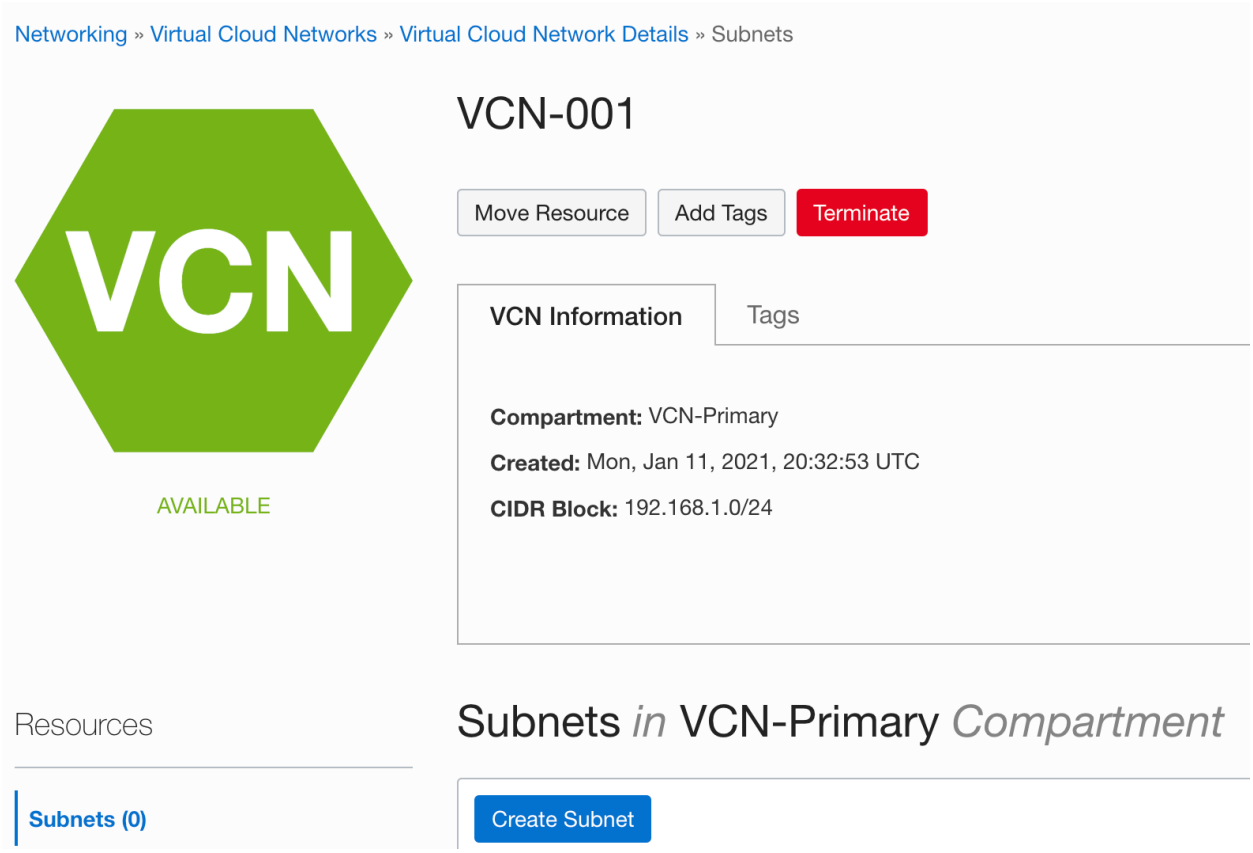
17. Once you have finished adding all Ingress and Egress rules, Click on **Create Security List**.



Create Subnets

Infoblox vNIOS for OCI instances require two subnets, one for the LAN1 interface and one for the MGMT interface.

1. From the VCN Details page, select **Subnets** under resources.
2. Click on **Create Subnet**.

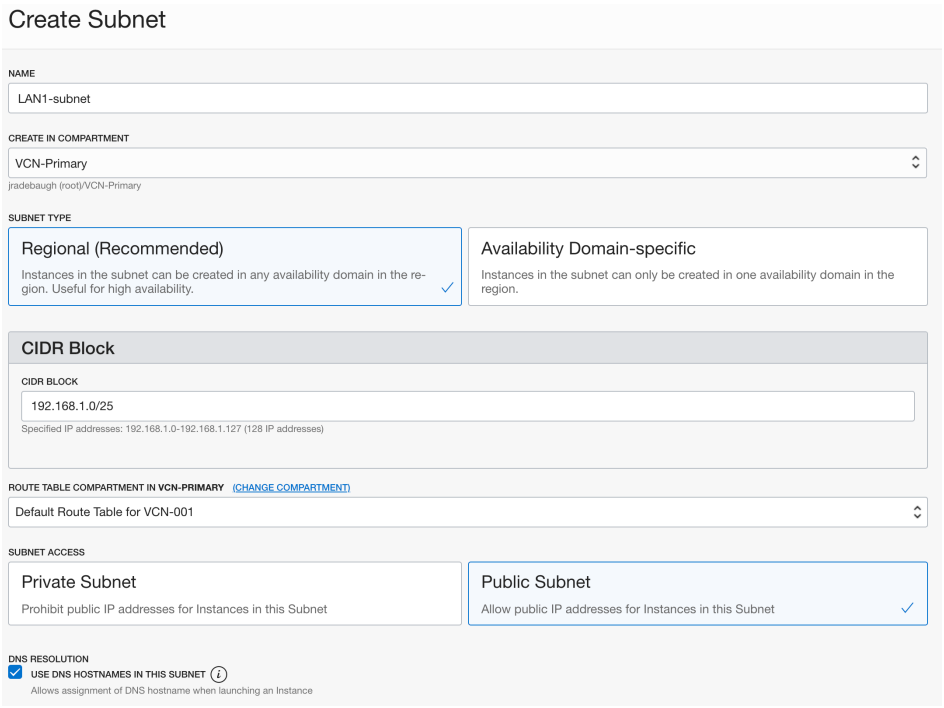


3. In the Create Subnet pane, enter a name for your subnet.
4. If needed, use the dropdown to select the compartment where you will create the subnet.
5. For Subnet Type, select **Regional**, unless you have a specific use case requiring otherwise.
6. Enter a CIDR Block for the subnet. For example, **192.168.1.0/25**.

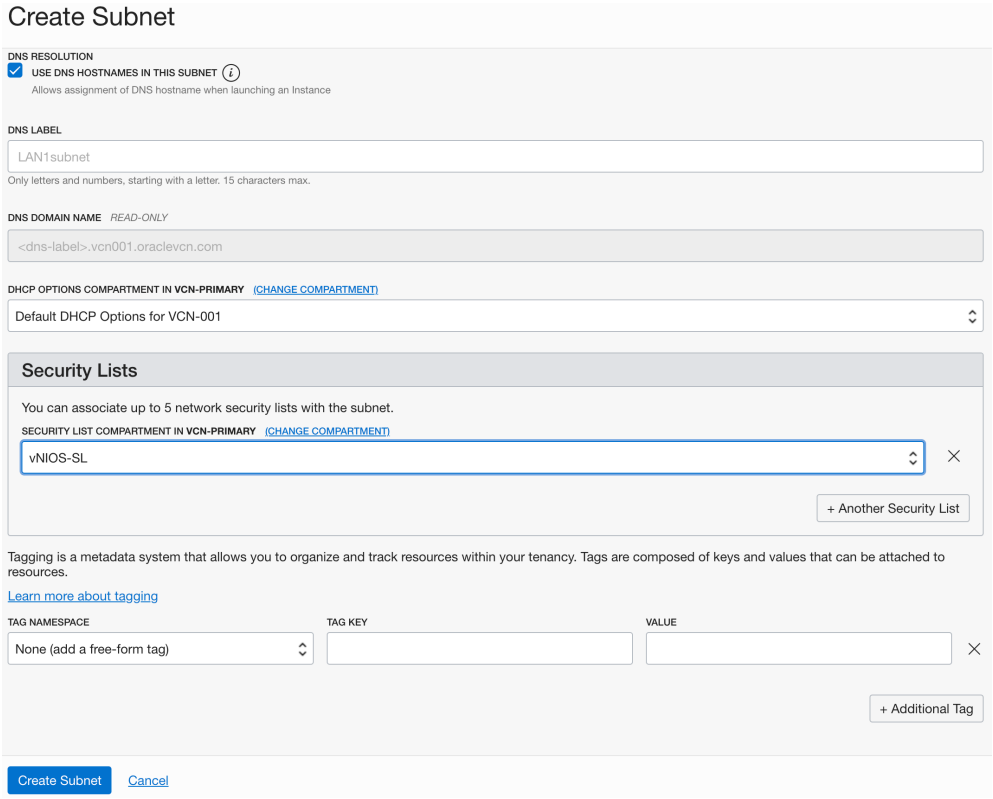
Note: This CIDR must fit inside a CIDR specified for the VCN.

7. Use the Route Table dropdown to select a route table. If this is a new VCN, only the **Default Route Table** will be listed.
8. Under Subnet Access, select **Public Subnet**.

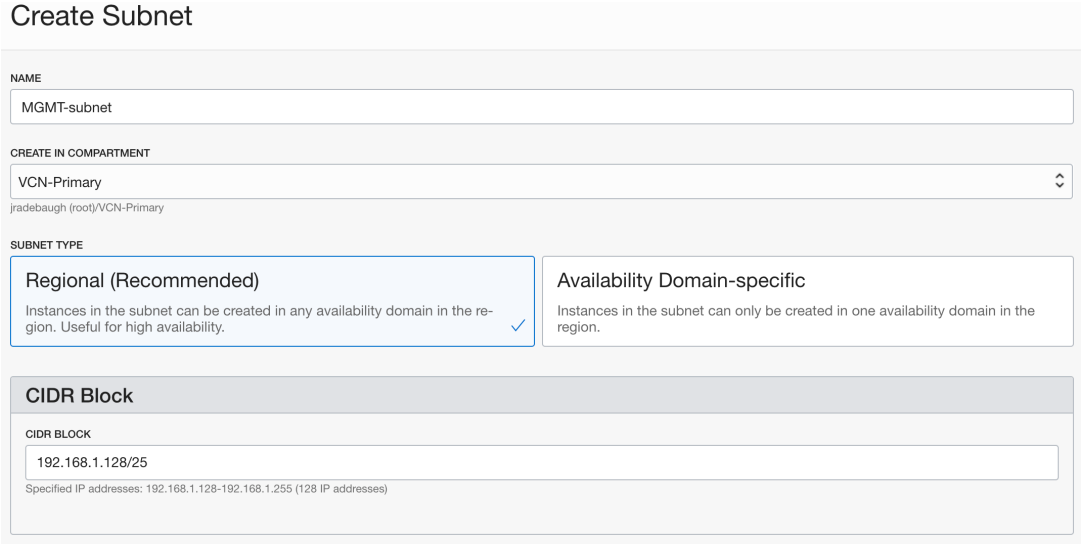
Note: If you will be connecting your instance to the Grid over VPN or FastConnect, you may wish to select Private Subnet.



9. Scroll down in the pane. Use the DHCP Options dropdown to select a DHCP options set. If this is a new VCN, only the **Default DHCP Options** will be listed.
10. Use the Security List dropdown to select the Security List you configured for vNIOS.
11. Click on **Create Subnet**.



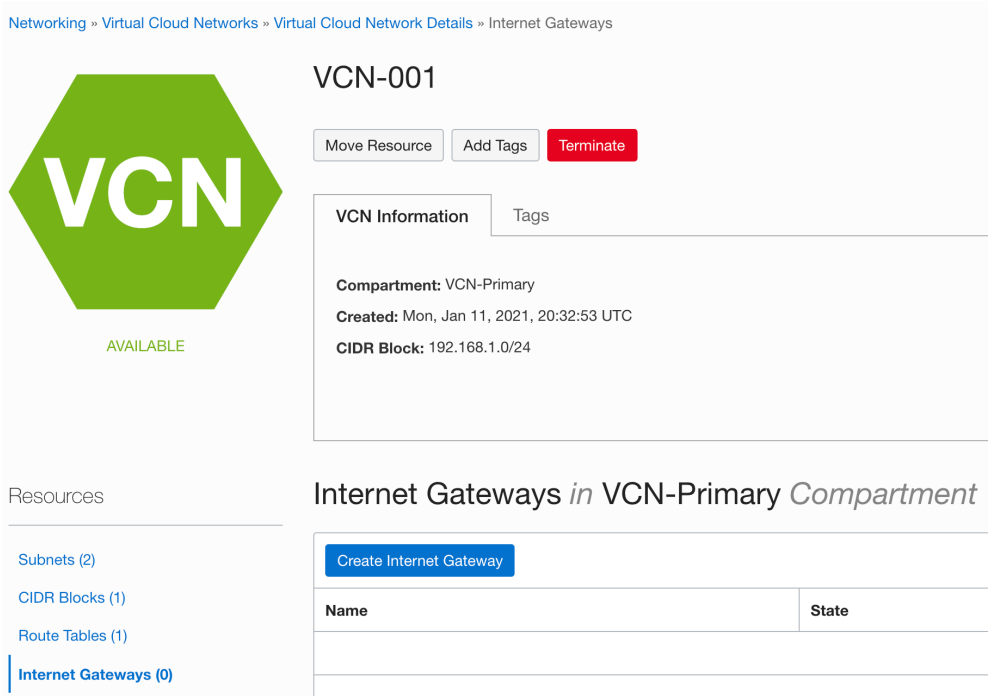
12. Repeat steps 2-11 for a second subnet, giving it a unique name and non-overlapping CIDR.



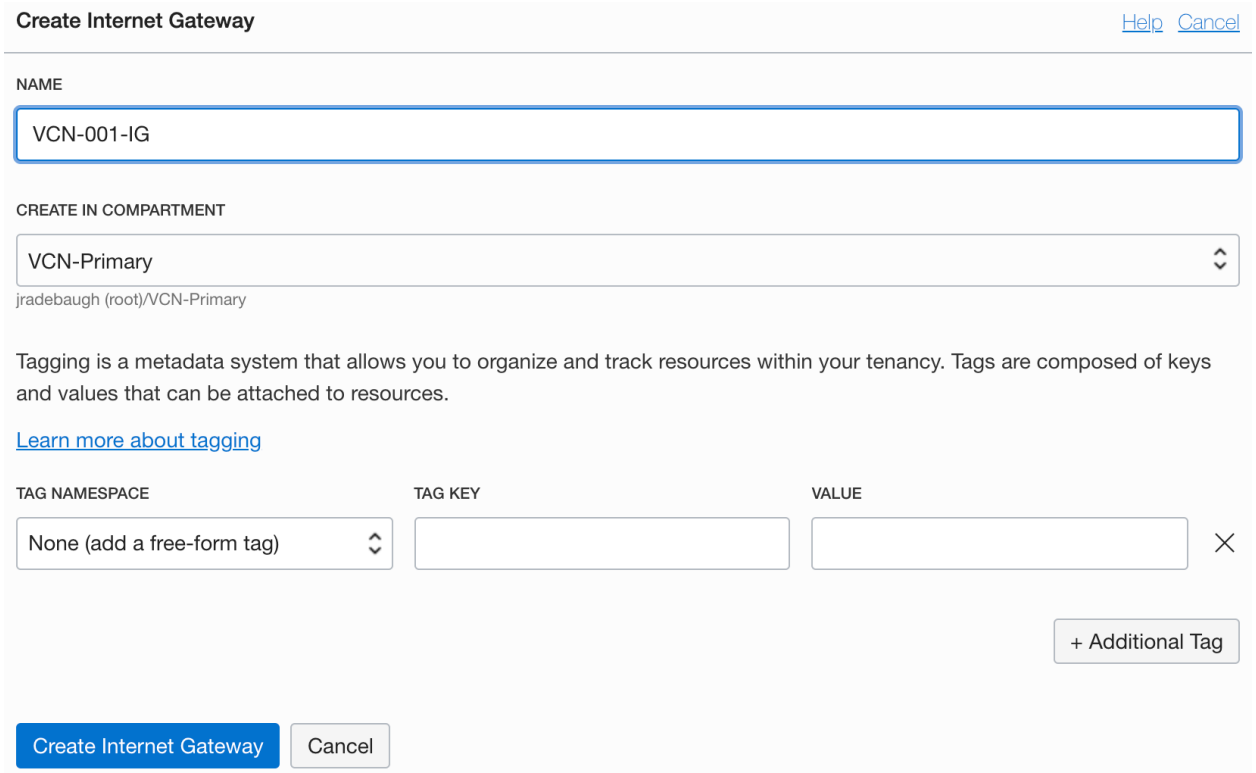
Create Gateway

Next, we will create a gateway and configure route tables to allow communication outside of the VCN. For this guide, we create an Internet Gateway to allow communication over the public Internet. If you are using a VPN or FastConnect between your on-premises and OCI networks, you will need to create a Dynamic Routing Gateway instead.

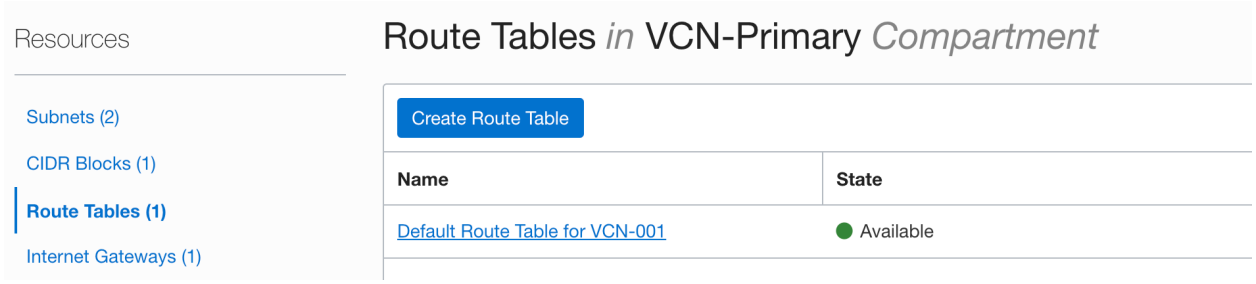
1. From the VCN Details page, select **Internet Gateways** under resources.
2. Click on **Create Internet Gateway**.



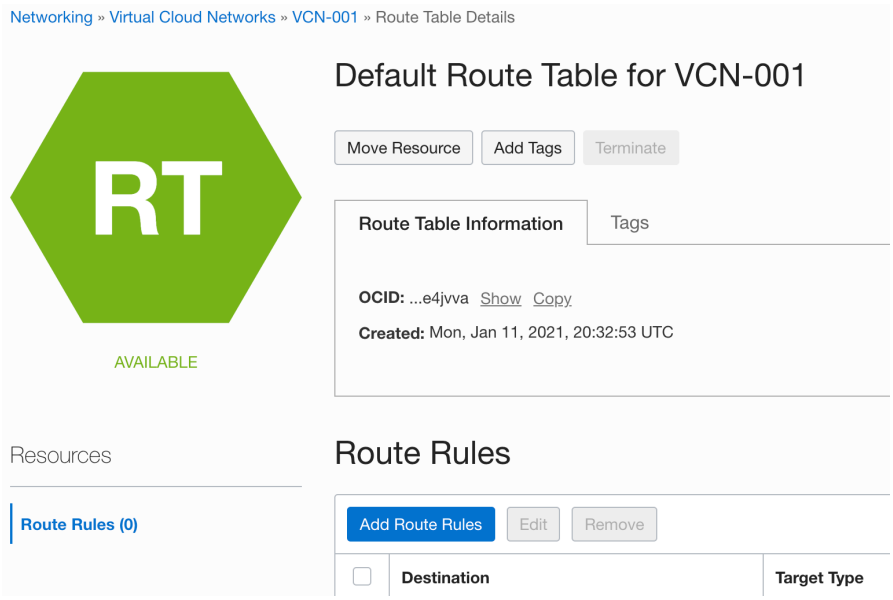
3. In the Create Internet Gateway window, enter a name for your gateway.
4. If needed, use the dropdown to select the compartment where you will create the gateway.
5. Click on **Create Internet Gateway**.



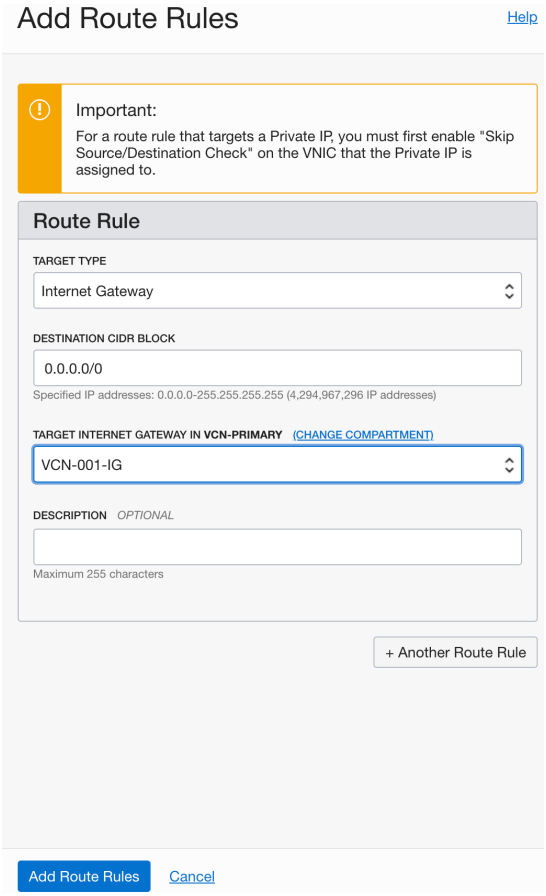
6. From the VCN Details page, select **Route Tables** under resources.
7. Select the route table which you assigned to your subnets. For this guide, we are using the **Default Route Table**.



8. On the Route Table Details page, click on **Add Route Rules**.



9. Use the Target Type dropdown to select **Internet Gateway**.
10. Enter a Destination CIDR Block. For example, **0.0.0.0/0**.
11. Use the Target Internet Gateway dropdown to select the gateway you created for this VCN.
12. Click **Add Route Rules**.



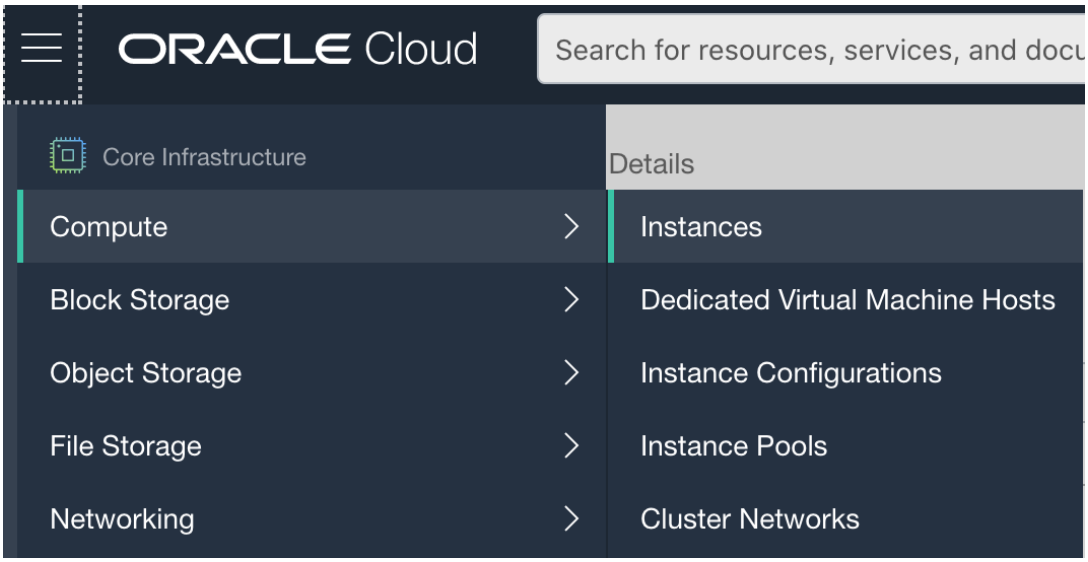
Deploy vNIOS Instance in OCI

Now that you have a VCN, subnets, security list, and routes configured, you can deploy a vNIOS instance in OCI. Infoblox vNIOS for OCI can be found in the Oracle Cloud Marketplace at https://cloudmarketplace.oracle.com/marketplace/app/Infoblox_NIOS or selected from partner images during instance deployment. To deploy from the Oracle Cloud Marketplace, use the Get App button to begin deploying into your OCI tenancy.

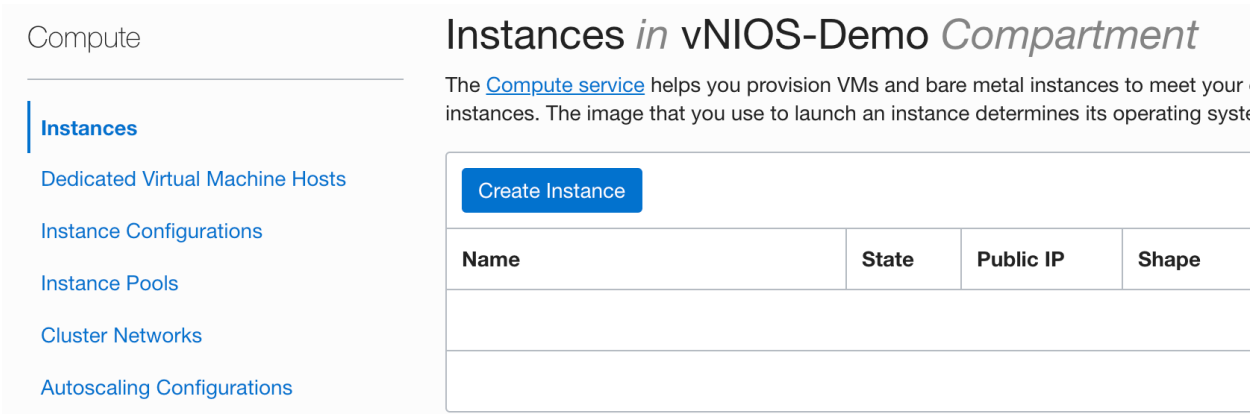
Create Instance

With the VCN configured, you are ready to deploy your Infoblox vNIOS for OCI instance. If you are deploying this image from the Oracle Cloud Marketplace, skip to Step 6 of the Select Image and Shape section to continue deployment.

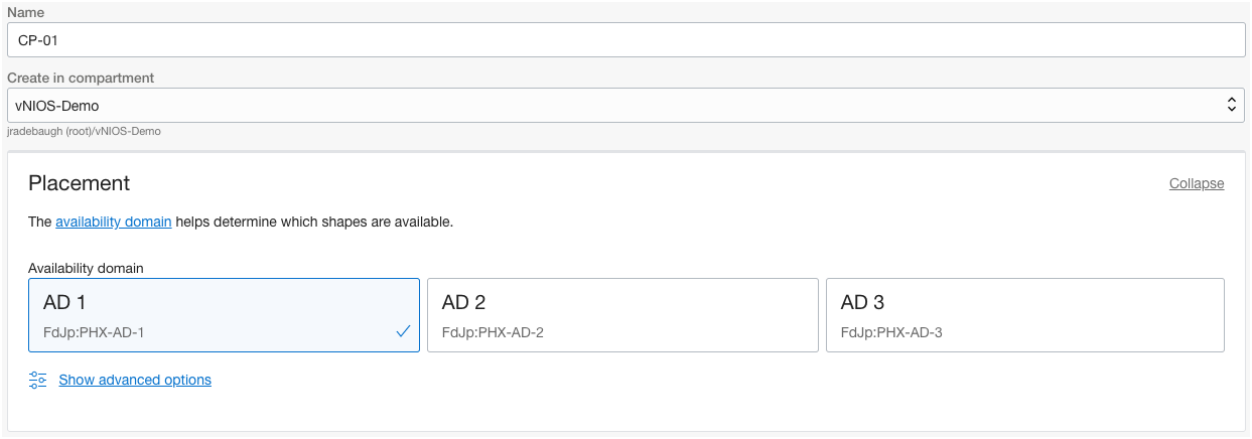
1. In the OCI Console, open the Services menu.
2. Hover on **Compute** to expand.
3. Select **Instances**.



4. Click on **Create Instance**.

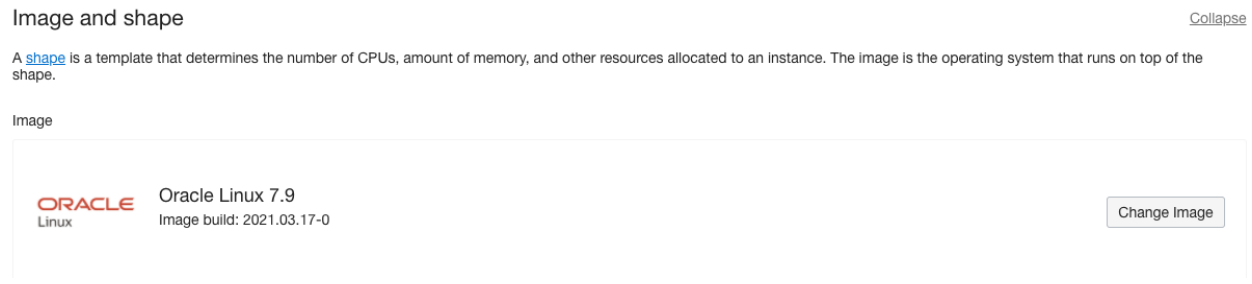


5. Enter a name for your instance.
6. Use the Create in compartment dropdown to select your desired compartment.
7. Under Placement, select your desired Availability domain.

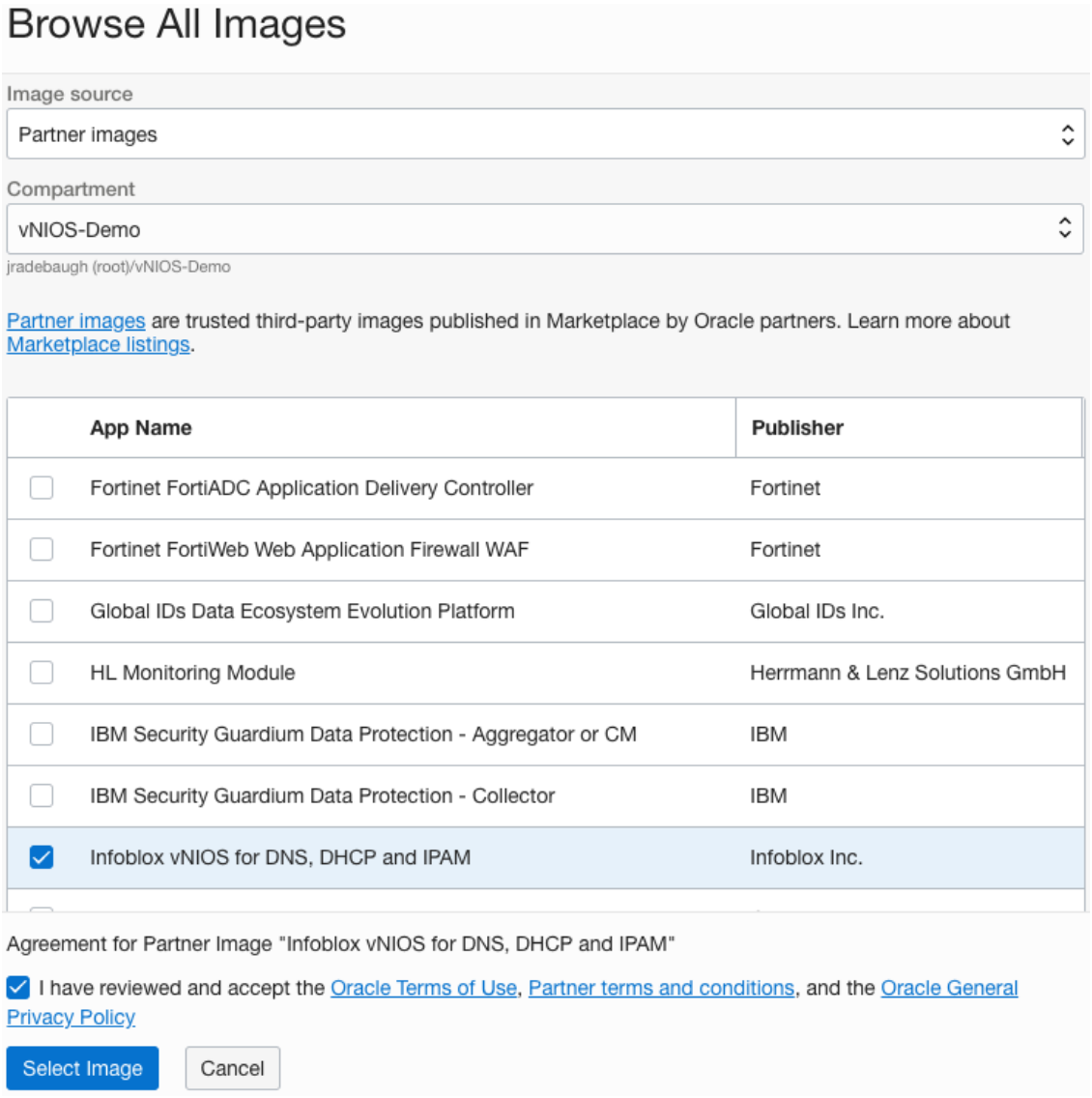


Select Image and Shape

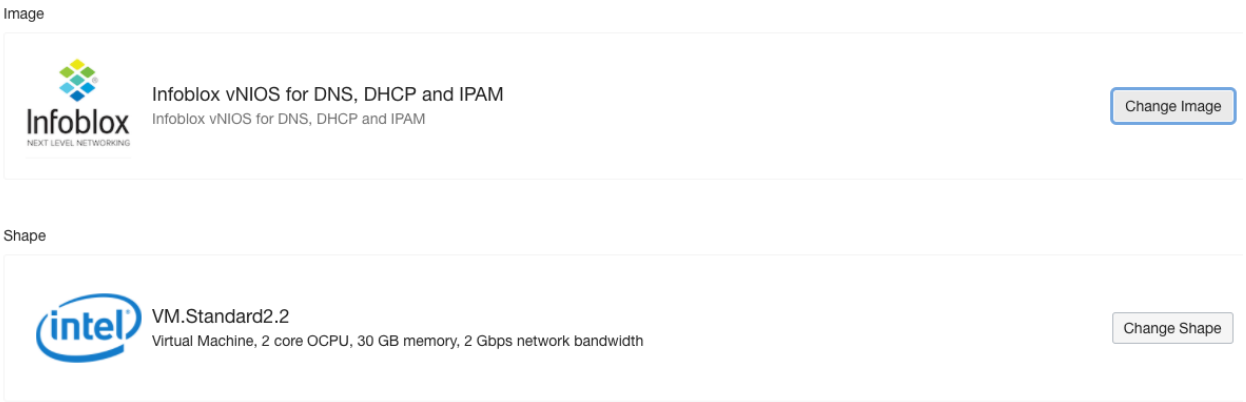
1. Under Image, click **Change Image**.



2. On the Browse All Images pane, select **Partner Images** from Image source.
3. Browse for and select the **Infoblox vNIOS for DNS, DHCP, and IPAM** image.
4. Check the box to review and accept the agreements.
5. Click on **Select Image**.



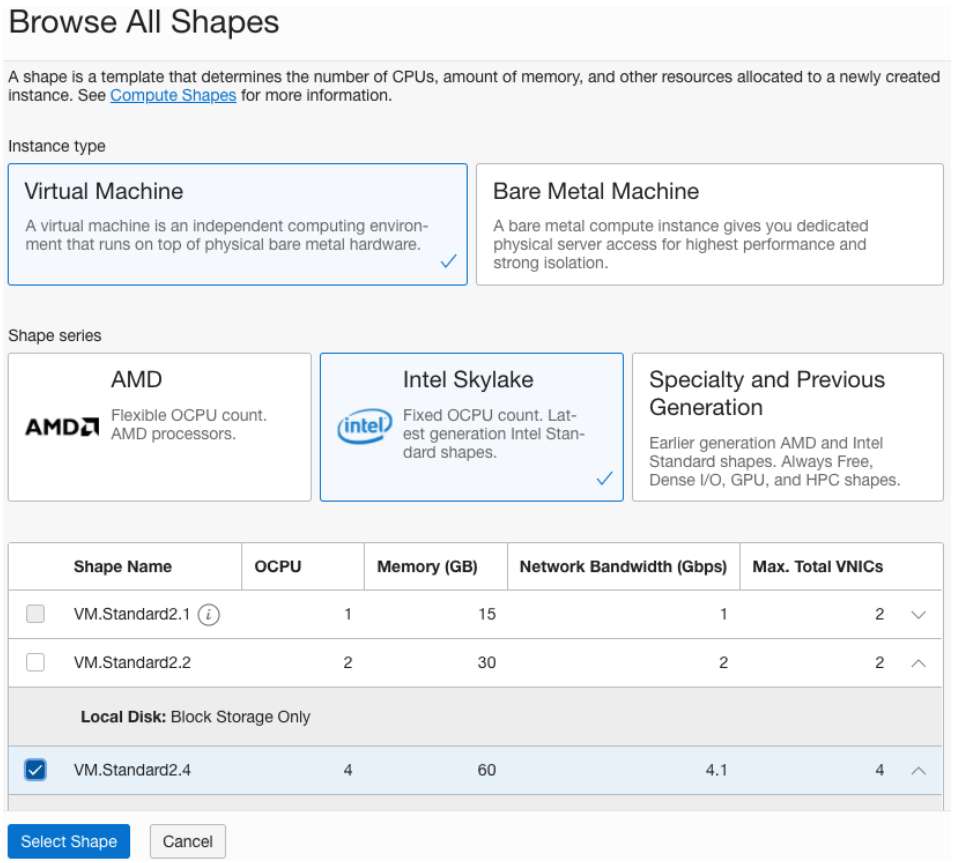
6. Back on the Create Compute Instance page, under Shape click **Change Shape**.



7. On the Browse All Shapes pane, select **Virtual Machine** for Instance type.
8. Select **Intel Skylake** for Shape series.

9. Select the checkbox for **VM.Standard2.4**.
10. Click **Select Shape**.

Note: If you are using a free trial tenancy on OCI, you may need to select a smaller image size due to quotas on VCPU use. This may degrade performance of the vNIOS instance and should only be used in testing. This should NOT be used for production systems.

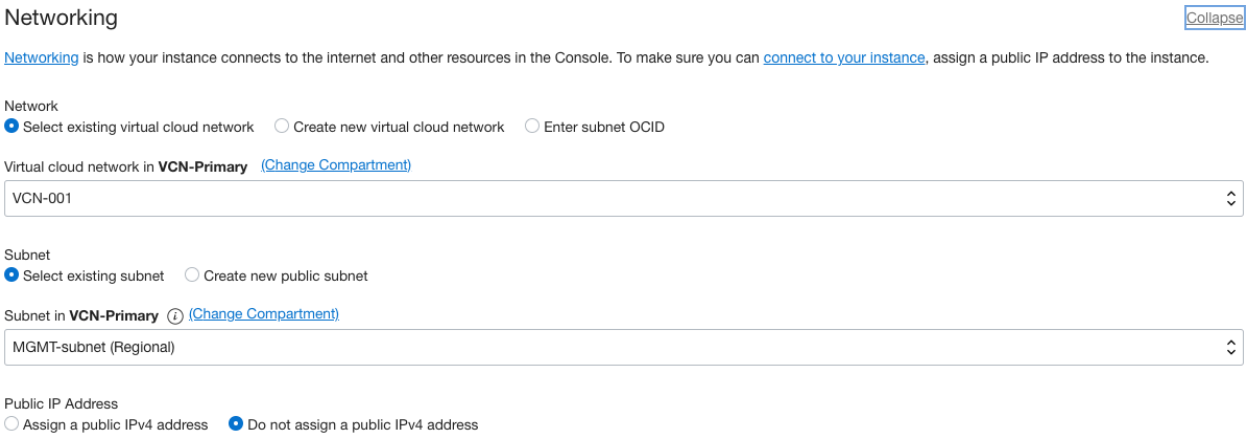


Configure Networking

1. On the Create Compute Instance page, scroll down to the Networking section.
2. Under Network, choose **Select existing virtual cloud network**.
3. If needed, click **Change Compartment** to select the compartment holding your VCN.
4. Use the Virtual cloud network dropdown to select your VCN.
5. Under Subnet, choose **Select existing subnet**.
6. If needed, click **Change Compartment** to select the compartment holding your subnet.
7. Use the Subnet dropdown to select the subnet for your MGMT interface.

Note: The VNIC created during initial deployment of the instance will be the MGMT interface in NIOS. In the next section, we will add a second interface, which is required for the vNIOS instance to boot successfully.

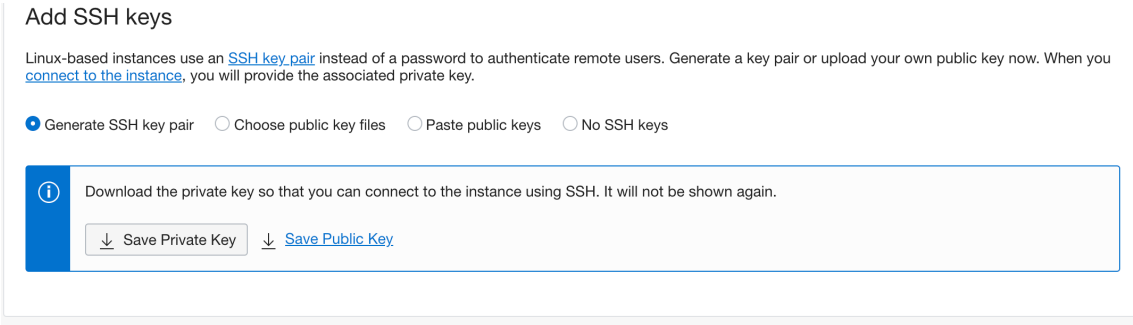
8. Under Public IP Address, choose whether to assign a public IP address or not. A public IP address will not normally be needed for the MGMT interface. It is recommended that you select **Do not assign a public IPv4 address**.



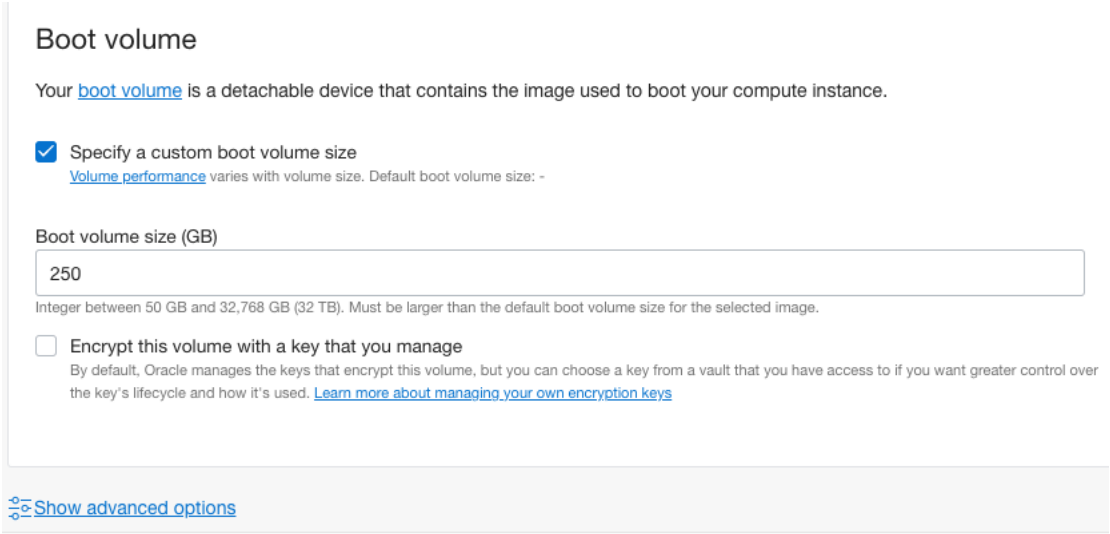
9. Scroll down to the Add SSH keys section.
10. Choose from the available options.

*Note: While SSH keys are not required here, you will need keys later to connect to the instance virtual console. To generate keys now, select **Generate SSH key pair**. Click on **Save Private Key** and **Save Public Key** to download these keys.*

11. Leave Configure boot volume settings at their default.



12. Under Boot volume, check the box to **Specify a custom boot volume size**.
13. For the Boot volume size in GB, enter **250**.



Cloud-Init

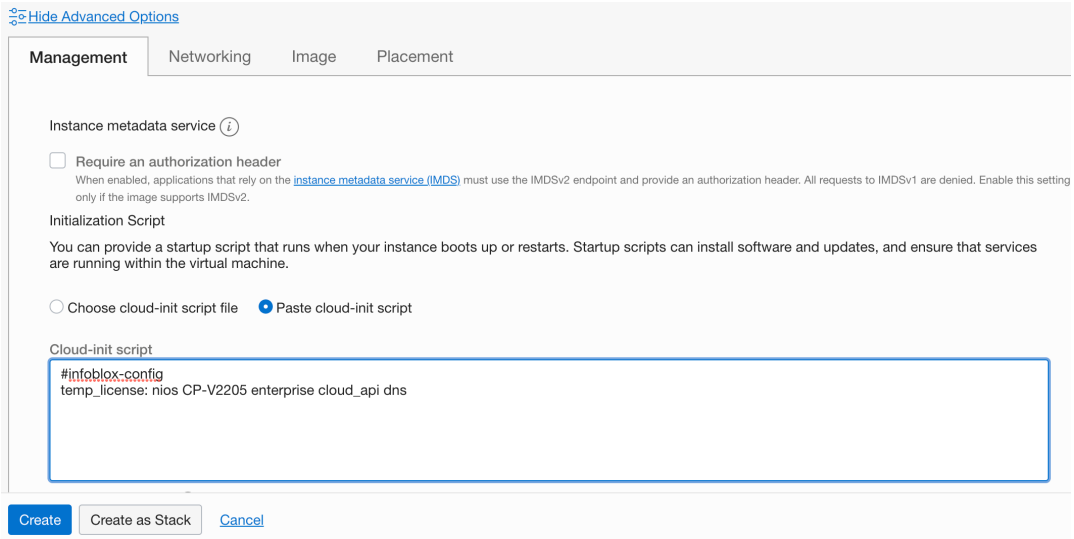
You can use cloud-init, an open-source package used for initial configuration to specify some settings for your new vNIOS for OCI instance. In this guide, we will use cloud-init to set necessary temporary licences for the vNIOS instance.

1. Click on **Show Advanced Options**.
2. On the Management tab of Advanced Options, under Initialization Script you will see options for cloud-init.
3. Select **Paste cloud-init script**.
4. In the Cloud-init script text box, paste the following:

#infoblox-config

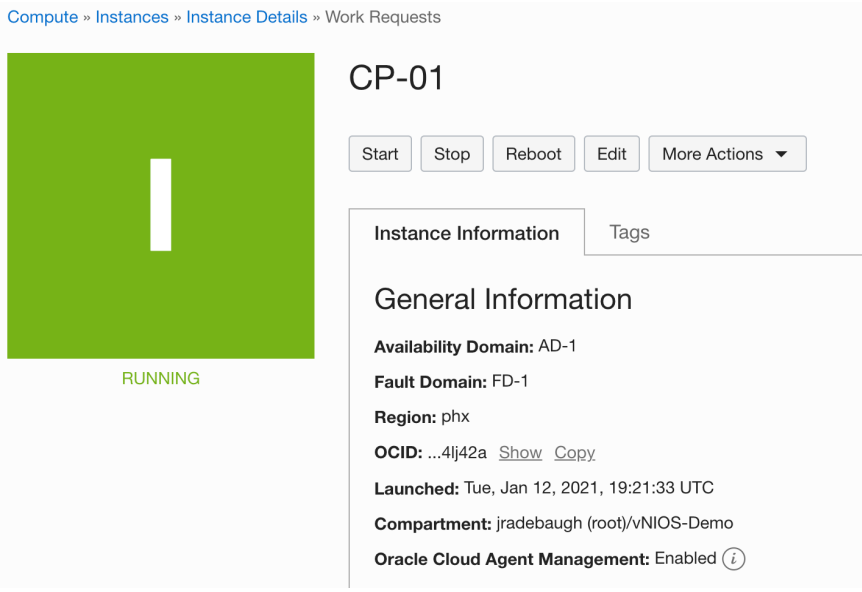
temp_license: nios CP-V2205 enterprise cloud_api dns

Note: This will apply temporary licenses for the Grid, NIOS model CP-V2205 virtual appliance, cloud platform, and DNS. For additional information on cloud-init configuration available for vNIOS instances, refer to NIOS documentation at https://docs.infoblox.com.



5. To finish deploying the instance, click on **Create**.
6. You may see a popup warning that you will not have SSH access. Click **Yes, Create Instance Anyway** to dismiss.

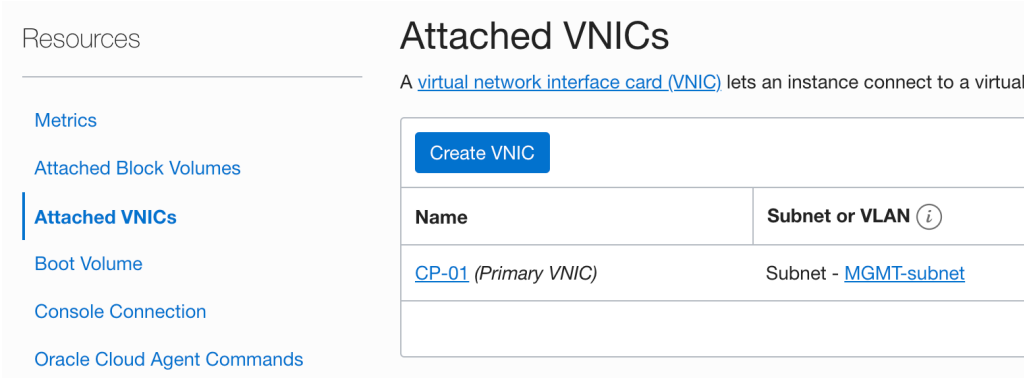
7. You can monitor the deployment of your instance on the Instance Details page. Wait for the status to show Running.



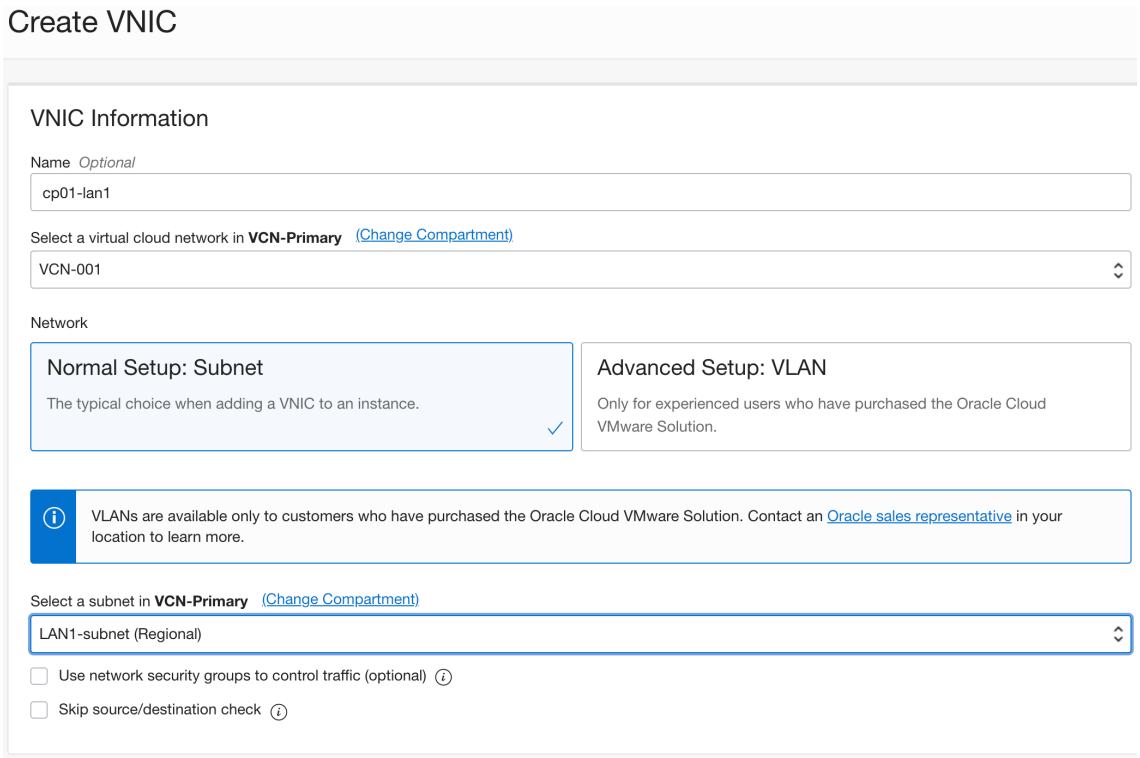
Add Secondary VNIC

Oracle Cloud does not provide an option to add additional VNICs while deploying an instance. The vNIOS instance requires two network interfaces to boot. To complete the deployment, we will attach a second VNIC to serve as the vNIOS LAN1 interface.

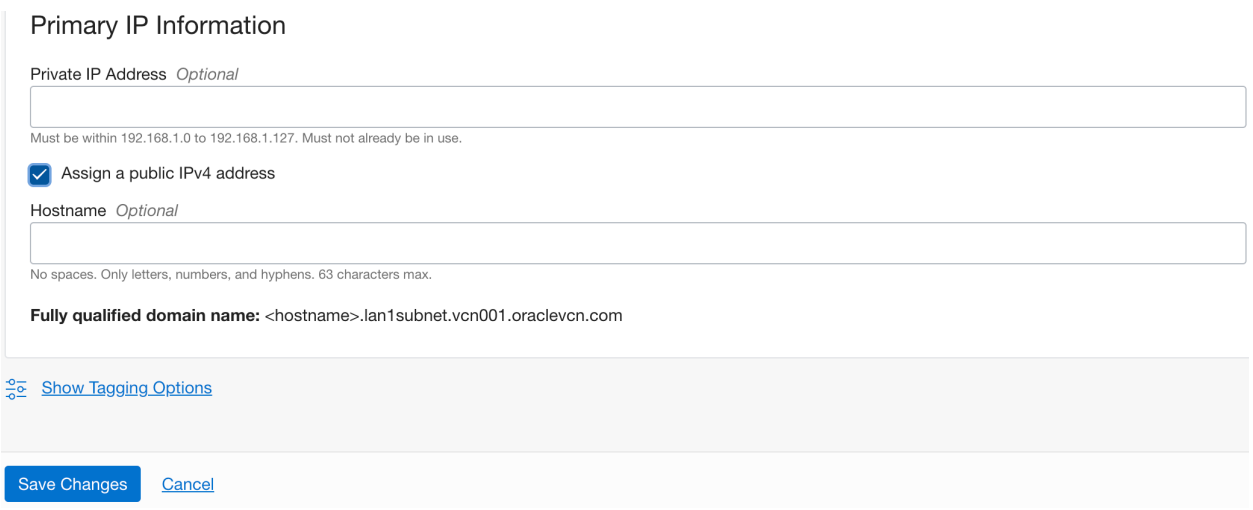
1. On the Instance Details page, scroll down and select **Attached VNICs** under resources.
2. Click **Create VNIC**.



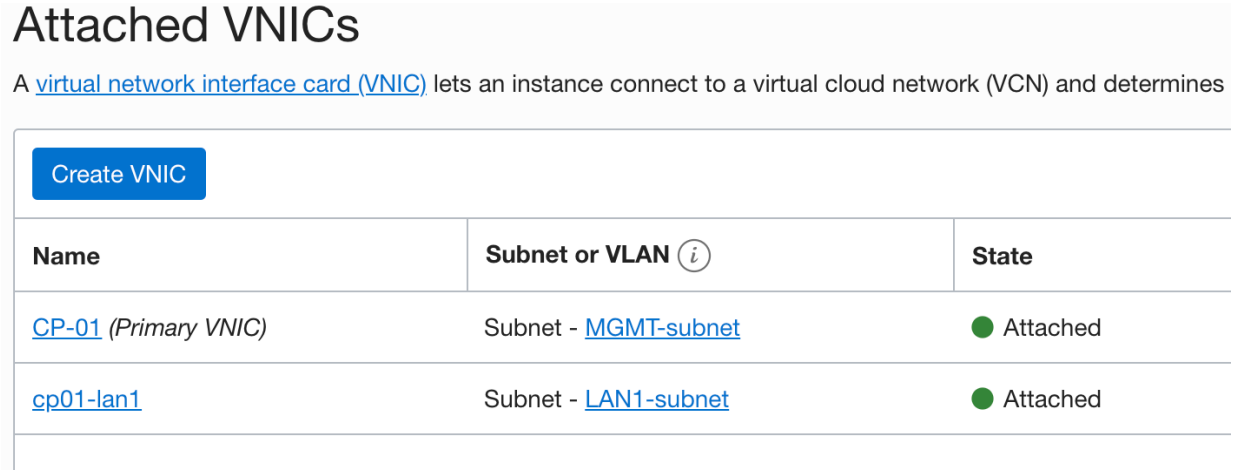
3. On the Create VNIC pane, enter a name for the VNIC.
4. If needed, click **Change Compartment** to select the compartment holding your VCN.
5. Use the Virtual cloud network dropdown to select your VCN.
6. Under Network, select **Normal Setup: Subnet**.
7. If needed, click **Change Compartment** to select the compartment holding your subnet.
8. Use the Subnet dropdown to select the subnet for your LAN1 interface.



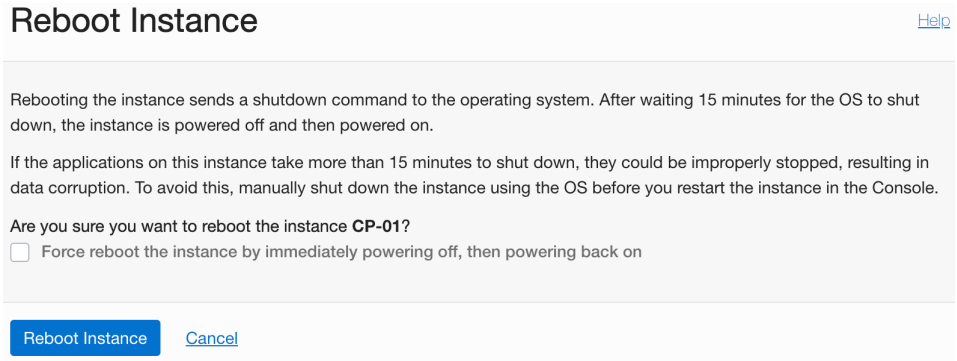
9. Scroll down to the Primary IP Information section.
10. If your instance will communicate with the Grid using public IPs or you need a public IP for other services, select **Assign a public IPv4 address**.
11. Click **Save Changes**.



12. Wait for the new VNIC to show a state of **Attached**.



13. Scroll to the top of the Instance Details page.
14. Click on **Reboot**.
15. In the Reboot Instance warning dialog, click **Reboot Instance**.

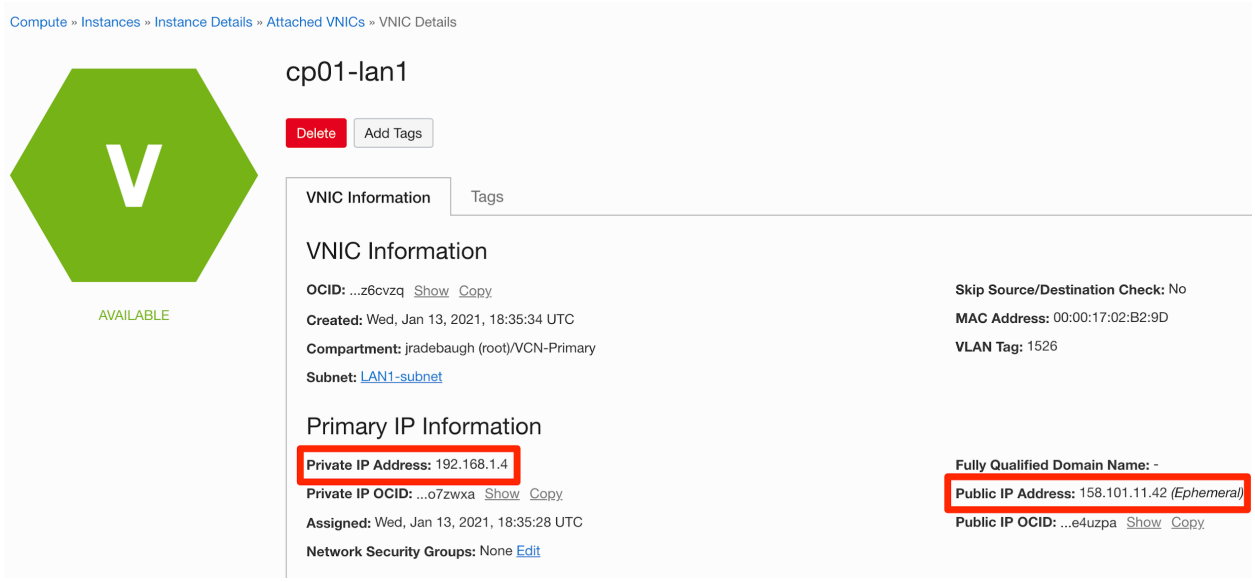


16. Wait for the instance to reboot and show a status of Running.

Find VNIC IP Address

In order to join your vNIOS for OCI instance to an Infoblox Grid later, you will need to know the IP address of the LAN1 interface, which is the new VNIC just created. If you will connect to the Grid using VPN or FastConnect, you will only need the private IP. If you will be connecting via public IP, you will need to know that as well.

1. From the Instance Details page, click on **Attached VNICs** under Resources.
2. Click on the new VNIC you created.
3. The VNIC Details page shows private and public IP addresses for this interface.

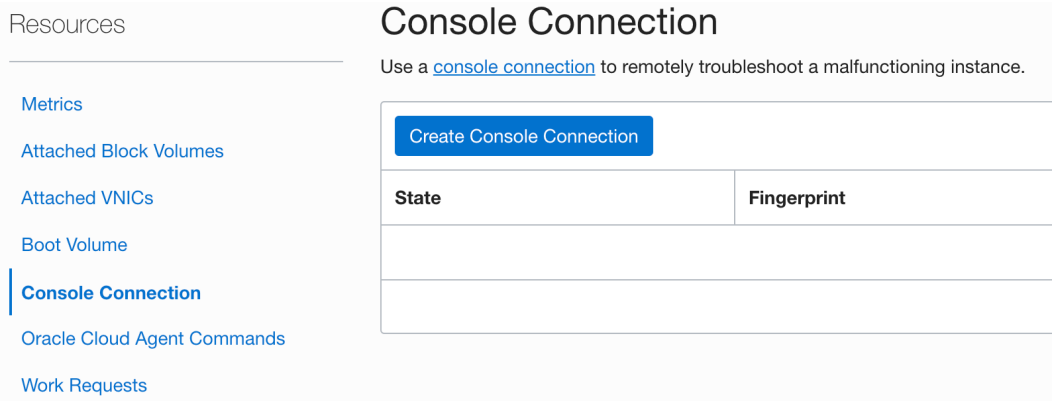


Connect to vNIOS Instance

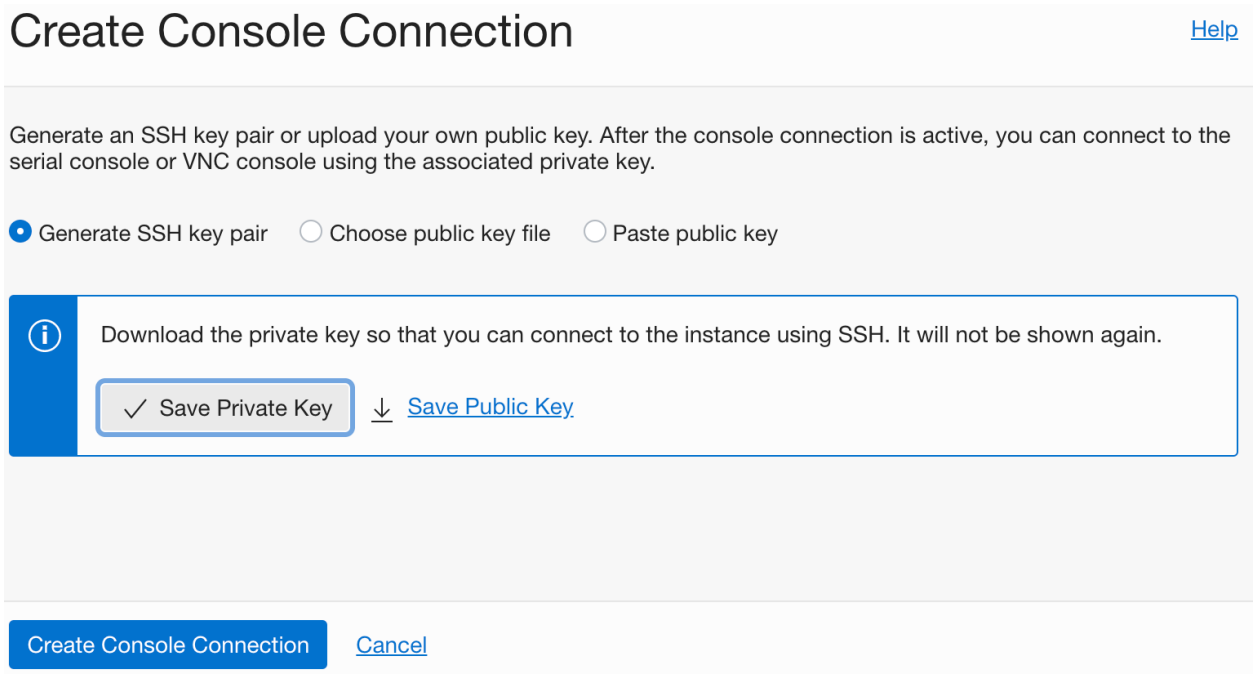
For the initial connection to your vNIOS instance, you will need to use a virtual console connection. From here you will be able to configure licensing and other basic settings as well as join the instance to your Infoblox Grid.

Create Console Connection

1. To create the Console Connection, scroll down on the Instance Details page.
2. Under Resources, select **Console Connection**.
3. Click on **Create Console Connection**.



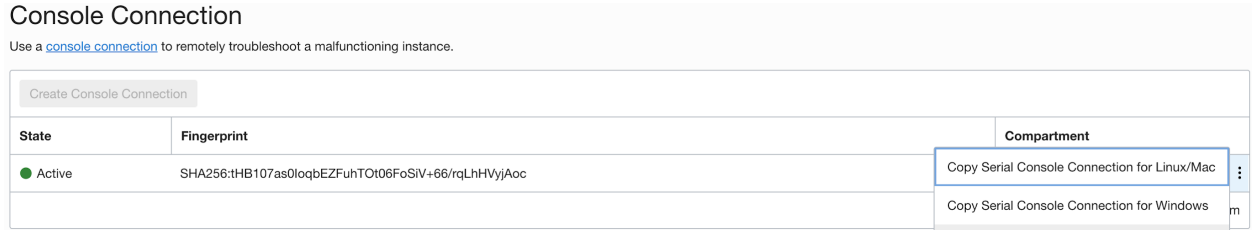
4. On the Create Console Connection pane, select an SSH key option.
5. Either download the newly generated keys or select your public key file to use.
6. Click on **Create Console Connection**.



7. Wait for the connection state to show Active.

Connect to Virtual Serial Console

1. Click on the 3 dots next to your Console Connection.
2. Select **Copy Serial Console** for your operating system.



3. Paste the connection string into a text editor.

```
ssh -o ProxyCommand='ssh -W %h:%p -p 443 ocid1.instanceconsoleconnection.oc1.phx.
anyhqljtgl535cqceoa7t7xb5qsn4igbnmllweydym4mqwszsbt5sxg4hvda@instance-console.us-phoenix-1.oraclecloud.com' ocid1.instance.oc1.phx.
anyhqljtgl535cqc4c2yzrq7jj2pjgbevxbfakszgjbyxh26yzxuyx4lj42a
```

4. After the initial ssh, add **-i <your-private-key>**.
5. Inside the proxy command, after ssh, enter **-i <your-private-key>**.

```
ssh -i ssh-key-2021-01-12.key -o ProxyCommand='ssh -i ssh-key-2021-01-12.key -W %h:%p -p 443 ocid1.instanceconsoleconnection.oc1.phx.
anyhqljtgl535cqceoa7t7xb5qsn4igbnmllweydym4mqwszsbt5sxg4hvda@instance-console.us-phoenix-1.oraclecloud.com' ocid1.instance.oc1.phx.
anyhqljtgl535cqc4c2yzrq7jj2pjgbevxbfakszgjbyxh26yzxuyx4lj42a
```

6. Open a terminal and navigate to the directory where you stored your private key.
7. Copy and paste your edited connection string into the terminal.

```
[redacted] oci-ssh % ssh -i ssh-key-2021-01-12.key -o ProxyCommand='ssh -i ssh-key-2021-01-12.key -W %h:%p -p 443
ocid1.instanceconsoleconnection.oc1.phx.anyhqljtgl535cqceoa7t7xb5qsn4igbnmllweydym4mqwszsbt5sxg4hvda@instance-console.us-phoenix-1.o
raclecloud.com' ocid1.instance.oc1.phx.anyhqljtgl535cqc4c2yzrq7jj2pjgbevxbfakszgjbyxh26yzxuyx4lj42a
```

8. If prompted, enter **yes** to continue connecting.
9. If prompted, enter **yes** again to add the instance to your known hosts.

```
The authenticity of host '[instance-console.us-phoenix-1.oraclecloud.com]:443 ([129.146.13.191]:443)' can't be established.
RSA key fingerprint is SHA256:Ghg/XkZv4W42u0xaqNhN7LMQcxrYuRTE+IYBD+kBxEc.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[instance-console.us-phoenix-1.oraclecloud.com]:443,[129.146.13.191]:443' (RSA) to the list of known hos
ts.

=================================================
IMPORTANT: Use a console connection to troubleshoot a malfunctioning instance. For normal operations, you should connect to the inst
ance using a Secure Shell (SSH) or Remote Desktop connection. For steps, see https://docs.cloud.oracle.com/iaas/Content/Compute/Task
s/accessinginstance.htm

For more information about troubleshooting your instance using a console connection, see the documentation: https://docs.cloud.oracl
e.com/en-us/iaas/Content/Compute/References/serialconsole.htm#four
=================================================
The authenticity of host 'ocid1.instance.oc1.phx.anyhqljtgl535cqc4c2yzrq7jj2pjgbevxbfakszgjbyxh26yzxuyx4lj42a (<no hostip for proxy
command>)' can't be established.
RSA key fingerprint is SHA256:kO21CWCl+u2glmu55SHCLSV3vPPh+2hlZTuAmr4eJqA.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'ocid1.instance.oc1.phx.anyhqljtgl535cqc4c2yzrq7jj2pjgbevxbfakszgjbyxh26yzxuyx4lj42a' (RSA) to the list o
f known hosts.
```

10. At the login prompt, use the NIOS default username and password to login: **admin/infoblox**.

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

               Infoblox NIOS Release 8.5.2-409296 (64bit)
     Copyright (c) 1999-2020 Infoblox Inc. All Rights Reserved.

                    type 'help' for more information


Infoblox >
```

11. Once logged into the console, you can use NIOS CLI commands to view and configure settings.
12. To verify necessary licenses are installed, use the **show license** command.

```
Infoblox > show license
Version          : 8.5.2-409296
Hardware ID      : F6A074D50EC6495BA9C766432CFCBE20

License Type     : NIOS (Model CP-V2205)
Expiration Date  : 03/20/2021
License String   : GwAAAKCmkJzLe2CimbpuQs1Fdzbz1n4BJwp4hb5prw==

License Type     : DNS
Expiration Date  : 03/20/2021
License String   : EwAAAKqhjJOGfynsm/YgQM9GOimkxHU=

License Type     : Grid
Expiration Date  : 03/20/2021
License String   : GgAAAKuhi4rFOie32O9uQcgLdHq+wHwBJk5uhLtr

License Type     : Cloud Platform
Expiration Date  : 03/20/2021
License String   : GQAAAK2jkJrTFTSuwvYjRYFFdjbwwn4Cawo/0u0=
```

Join vNIOS Instance to Grid

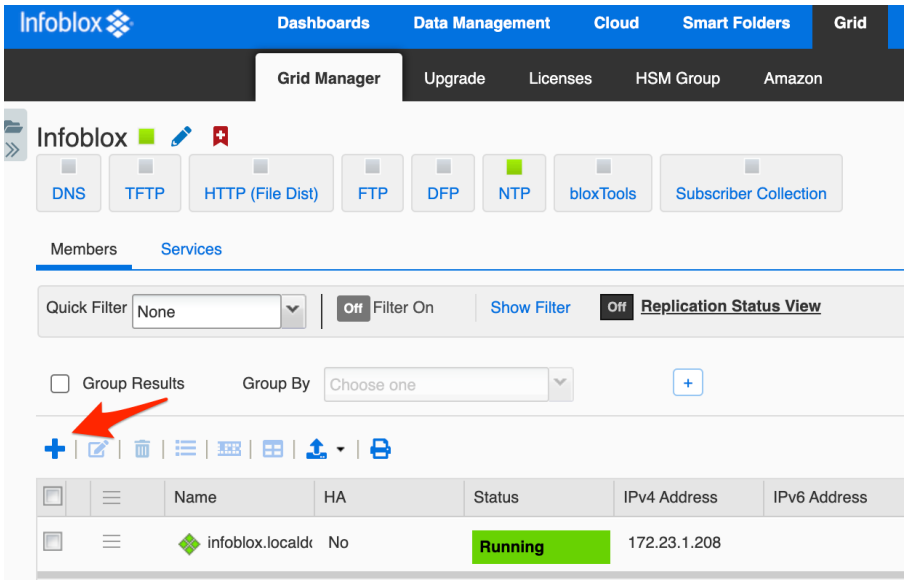
Cloud Platform members such as the CP-V2205 available on OCI cannot serve as Grid Masters and must be joined to an existing on-premises Grid. Grid communication can take place over VPN and OCI FastConnect or

if needed using public IP addresses via the public Internet. In this guide we will use Infoblox NIOS NAT settings to join a Grid using public IP addresses.

Provision vNIOS Member in Grid

Before joining the new member to your Infoblox Grid, you will need to add the member in your Grid Manger. This can be done through the Grid Manager GUI or APIs. This guide demonstrates how to add a Grid member using the GUI.

1. In the Grid Manager of your existing Grid, navigate to the **Grid** → **Grid Manager** → **Members** tab.
2. Click the (Add) button.

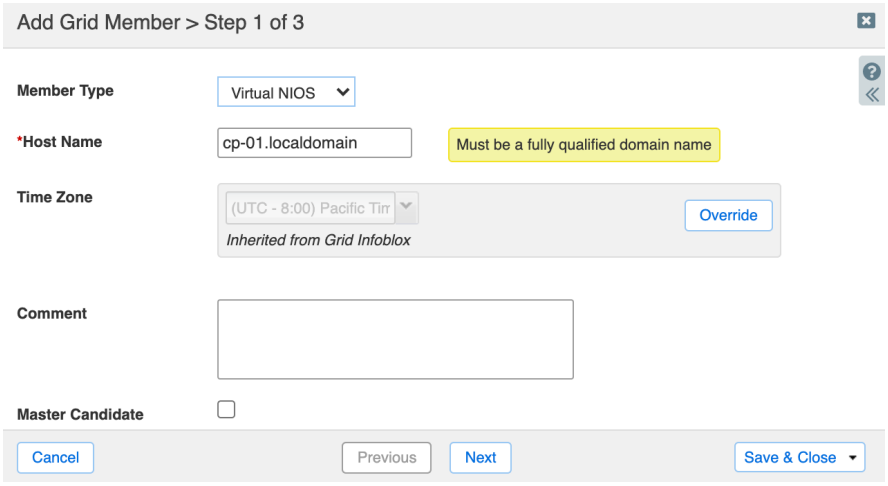


3. On step 1 of the Add Grid Member wizard, use the dropdown to select **Virtual NIOS** for Member Type.
4. Enter a Host Name.

Note: This must be a fully qualified domain name, for example cp-01.localdomain.

Warning: Do NOT select Master Candidate for this member as CP appliances cannot serve as GM or GMC.

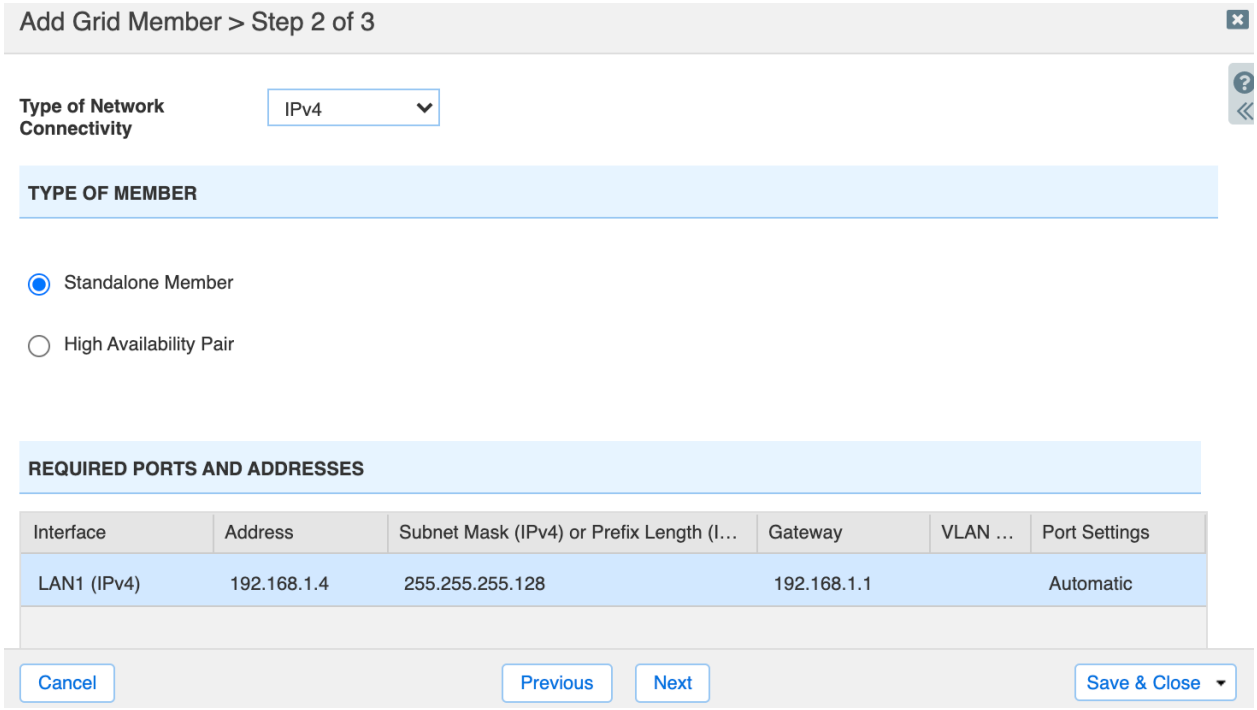
5. Click **Next**.



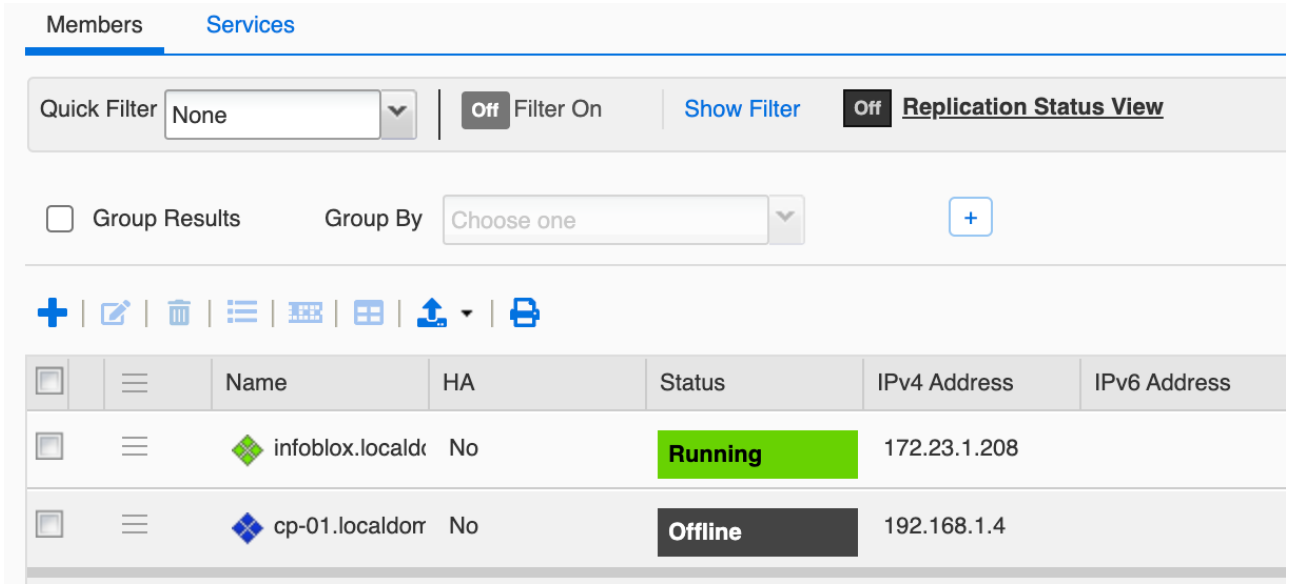
6. On step 2, use the dropdown to select **IPv4** for Type of Network Connectivity.
7. Select **Standalone Member** for Type of Member.
8. Enter the private IP address for the LAN1 interface.
9. Enter the Subnet Mask for LAN1.
10. Enter the default gateway for LAN1.

Note: The default gateway for a subnet in OCI will be the first available IP address in the subnet by default.

11. Click **Save & Close**.



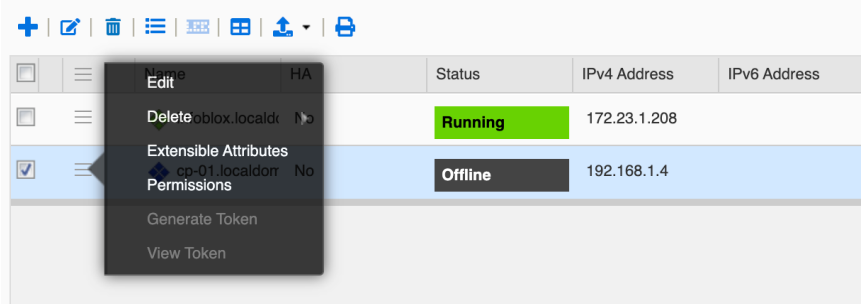
12. The new member will be visible in Grid Manager with an Offline Status.



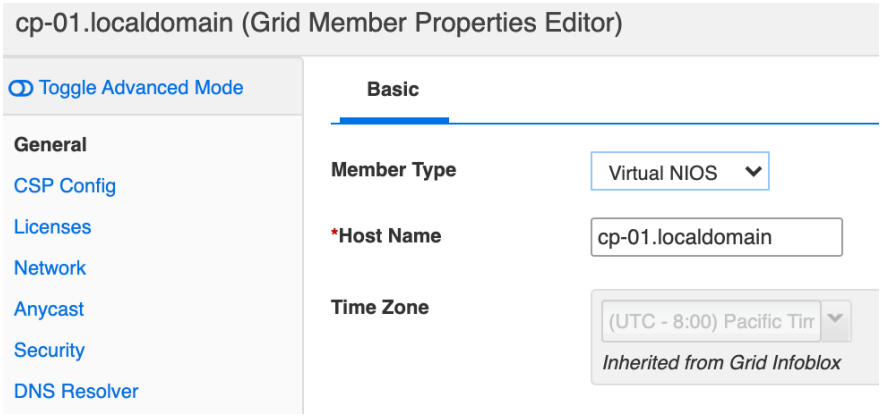
Configure NAT

If you will be using public IP addressing to join this member to the Grid, the following steps describe how to enable NAT for the member. You will also need to configure NAT and potentially NAT groups for the Grid Master if you have not set this up before. Refer to NIOS documentation at https://docs.infoblox.com for further information on configuring NAT and NAT Groups.

1. If you will be using public IP addressing to join this member to the Grid, select the member.
2. Open the action menu for the member and select **Edit**.



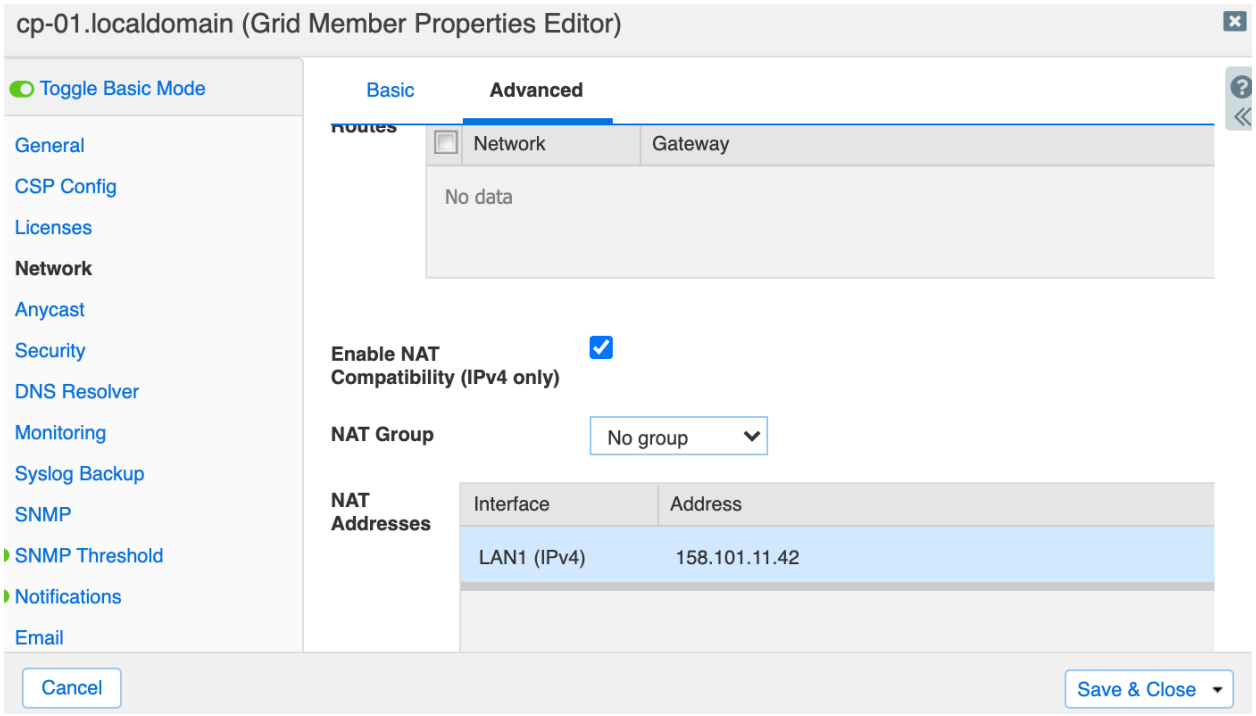
3. In the Grid Member Properties Editor, click **Toggle Advanced Mode**.
4. Click **Network**.



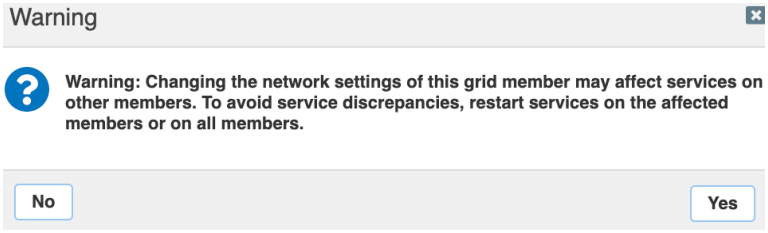
5. On the Network page, click on **Advanced**.
6. Scroll down and select the checkbox for **Enable NAT Compatibility**.
7. Enter the public IP address for LAN1 of your vNIOS for OCI instance.

Note: NAT Groups are not covered in this guide. For information on configuring NAT groups, refer to NIOS documentation at https://docs.infoblox.com.

8. Click **Save & Close**.



9. Click **Yes** in the Warning dialog.



Configure and Join Member to Grid

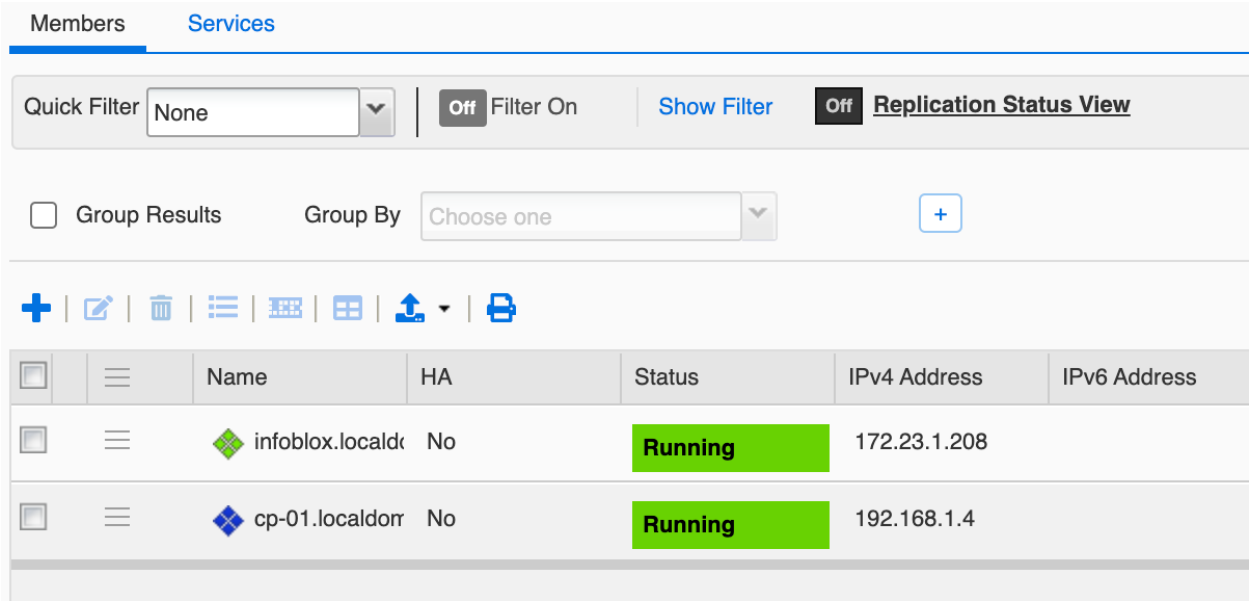
Once you have completed provisioning the new member in the Grid, you can use the CLI to join the member.

1. Log back into your vNIOS for OCI instance using the console connection as previously described.
2. Enter the command **set membership**.
3. Enter the private or public IP address of your Grid Master, depending on the type of networking used for Grid communication.
4. Enter the Grid name (default is **Infoblox**).
5. Enter the Grid shared secret (default is **test**).
6. Enter **Y** to confirm (you will be prompted twice).

```
Infoblox > set membership
Join status: No previous attempt to join a grid.
 Enter New Grid Master VIP: 184.169.254.86
Enter Grid Name [Default Infoblox]: Infoblox
Enter Grid Shared Secret: test
  Join grid as member with attributes:
     Grid Master VIP:     184.169.254.86
     Grid Name:           Infoblox
     Grid Shared Secret:  test

WARNING: Joining a grid will replace all the data on this node!
        Is this correct? (y or n): y
```

7. The instance will restart and attempt to contact the Grid Master. You can watch progress in the console or in Grid Manager.
8. Once the member successfully joins the Grid, It will show as Running in Grid Manager.



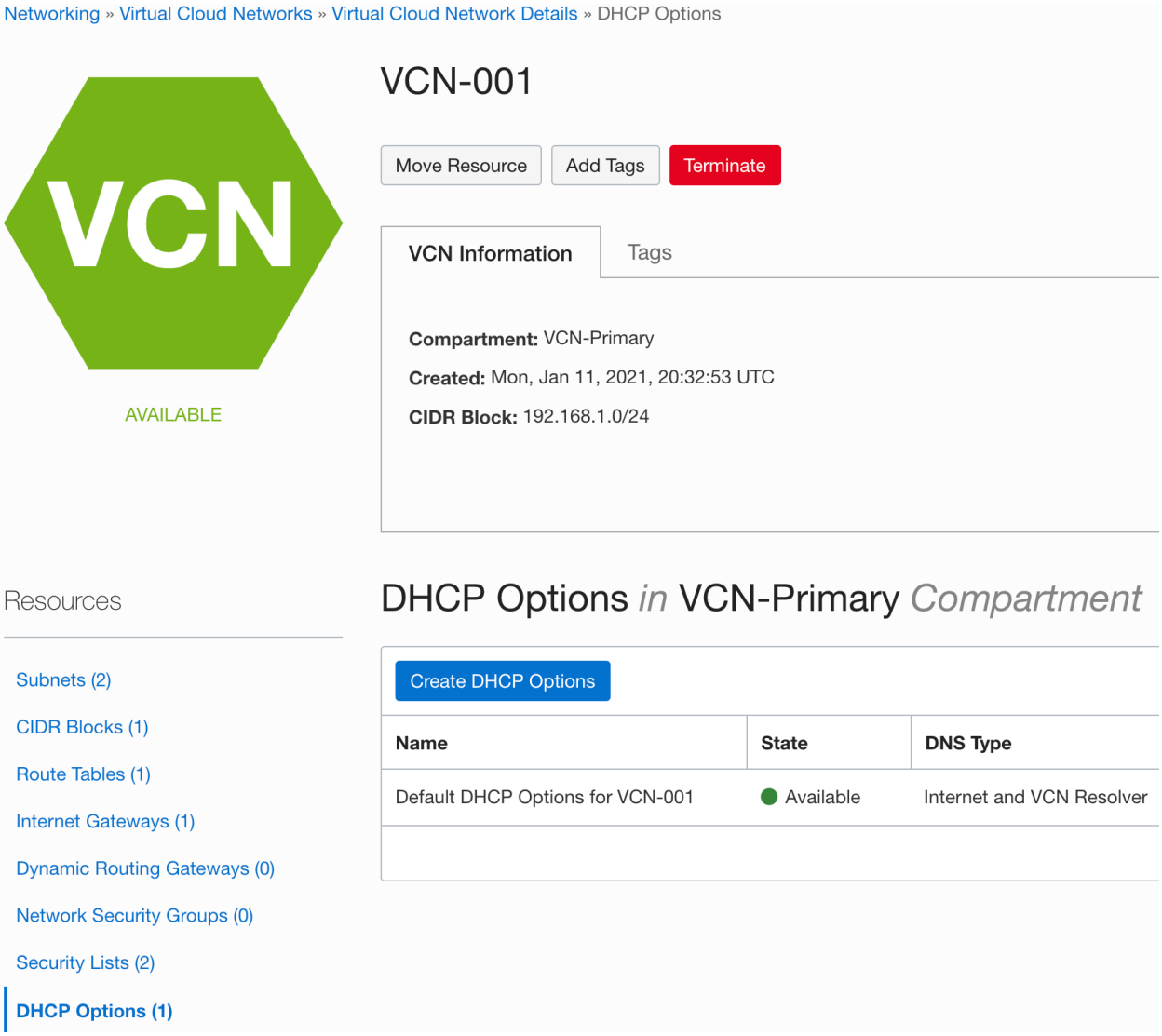
9. Once the member shows as Running, you can configure services as desired. Refer to https://docs.infoblox.com for information on configuring members and services. Additionally, you can refer to the Deployment Guide: Infoblox Cloud Platform and Cloud Network Automation for details specific to CP members.

Set vNIOS Instance as Primary DNS for Subnet

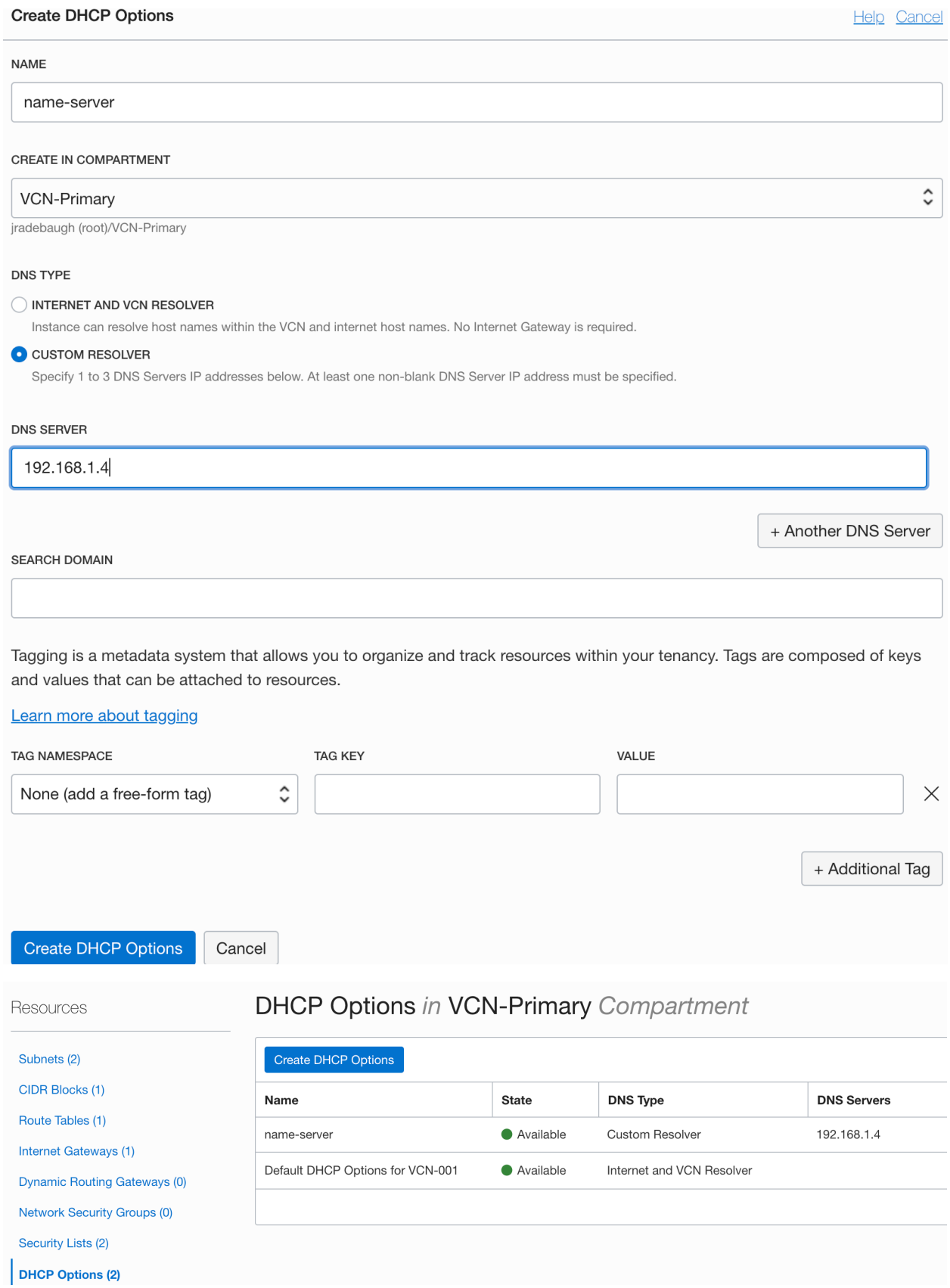
OCI allows you to specify custom DNS name servers for your VCN using DHCP options. These can be name servers on the Internet, in a VCN, or in your on-premises network via VPN or FastConnect. Prior to setting your vNIOS for OCI instance as a name server for your VCN, ensure you have configured the DNS service. Refer to https://docs.infoblox.com for details on configuring the DNS service.

1. In the OCI console, use the services menu to navigate to **Networking → Virtual Cloud Networks**.
2. Click on your VCN.

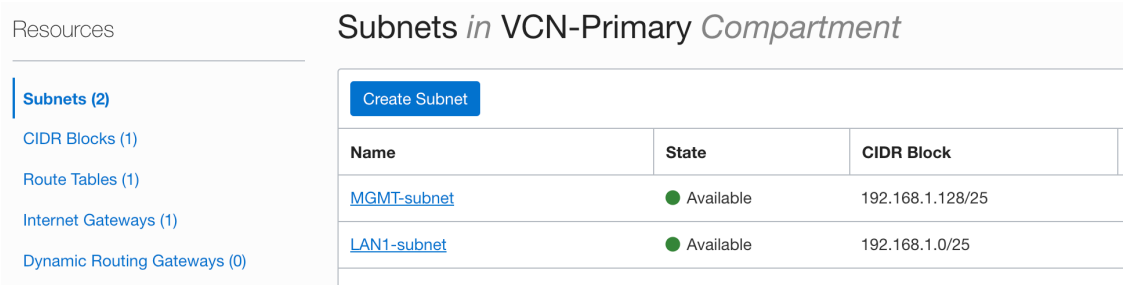
3. On the VCN Details page, click on **DHCP Options** under Resources.
4. Click on **Create DHCP Options**.



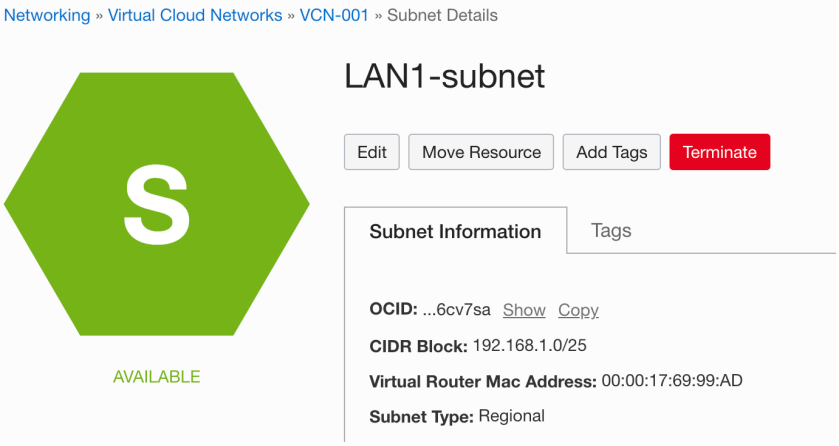
5. In the Create DHCP Options window, enter a name.
6. For DNS Type, select **Custom Resolver**.
7. For DNS Server, enter the private IP address of your vNIOS for OCI instance LAN1 VNIC.
8. Click on **Create DHCP Options**.


Create DHCP Options
Help
Cancel
NAME
name-server
CREATE IN COMPARTMENT
VCN-Primary
jradebaugh (root)/VCN-Primary
DNS TYPE
INTERNET AND VCN RESOLVER
Instance can resolve host names within the VCN and internet host names. No Internet Gateway is required.
CUSTOM RESOLVER
Specify 1 to 3 DNS Servers IP addresses below. At least one non-blank DNS Server IP address must be specified.
DNS SERVER
192.168.1.4
+ Another DNS Server
SEARCH DOMAIN
Tagging is a metadata system that allows you to organize and track resources within your tenancy. Tags are composed of keys and values that can be attached to resources.
Learn more about tagging
TAG NAMESPACE
TAG KEY
VALUE
None (add a free-form tag)
+ Additional Tag
Create DHCP Options
Cancel
Resources
Subnets (2)
CIDR Blocks (1)
Route Tables (1)
Internet Gateways (1)
Dynamic Routing Gateways (0)
Network Security Groups (0)
Security Lists (2)
DHCP Options (2)
DHCP Options in VCN-Primary Compartment
Create DHCP Options
Name
State
DNS Type
DNS Servers
name-server
Available
Custom Resolver
192.168.1.4
Default DHCP Options for VCN-001
Available
Internet and VCN Resolver

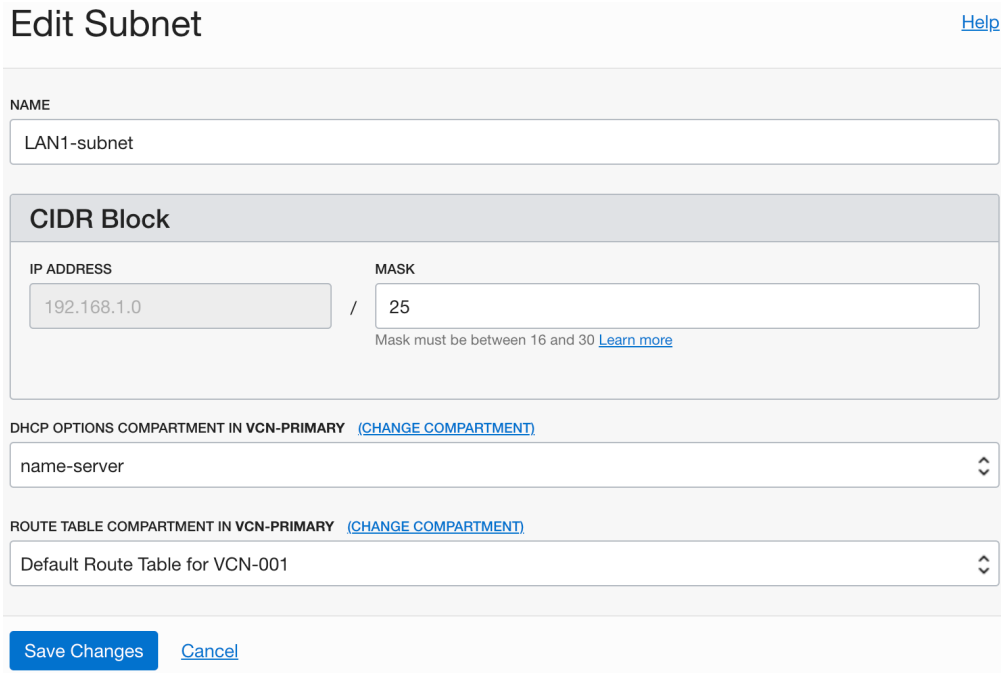
9. To set your newly created DHCP Options for a subnet, click on **Subnets** under Resources.
10. Click on the Subnet you want to edit.



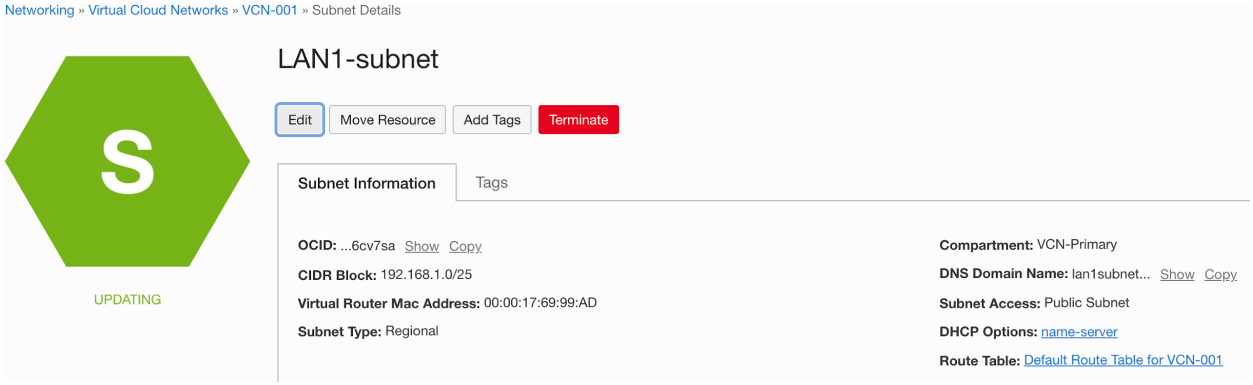
11. On the Subnet Details page, click **Edit**.



12. On the Edit Subnet pane, use the DHCP Options dropdown to select your new DHCP Option.
13. Click on **Save Changes**.



14. You can now see the new DHCP Options set on the Subnet Details page.



15. You will need to reboot or restart the DHCP client of any existing instances on the subnet for the change to take effect.

Limitations

The following are current limitations of using Infoblox NIOS with OCI:

- DHCP from Infoblox vNIOS instances can only be used to serve on-premises clients. The DHCP service will not work for OCI VCNs and VMs.
- vDiscovery of OCI resources is not available.
- Only the CP-V2205 model appliance is supported on OCI. CP appliances cannot act as GM or GMC, thus the virtual appliance must be connected to an existing Grid.
- HA and LAN2 interfaces are not supported for vNIOS appliances running on OCI.

Additional Resources

- Infoblox NIOS and vNIOS Documentation: https://docs.infoblox.com.
- Infoblox Support: https://support.infoblox.com.
- OCI Documentation: https://docs.oracle.com.
- Deployment Guide for Cloud Platform Appliances: https://insights.infoblox.com/resources-deployment-guides/infoblox-deployment-guide-infoblox-cloud-platform-and-cloud-network-automation.

Infoblox is the leader in modern, cloud-first networking and security services. Through extensive integrations, its solutions empower organizations to realize the full advantages of cloud networking today, while maximizing their existing infrastructure investments. Infoblox has over 12,000 customers, including 70 percent of the Fortune 500.

Corporate Headquarters | 2390 Mission College Boulevard, Ste. 501 | Santa Clara, CA | 95054
+1.408.986.4000 | info@infoblox.com | www.infoblox.com