DEPLOYMENT GUIDE

Deploy Infoblox vNIOS Instances for AWS

Table of Contents

Introduction

Infoblox vNIOS for AWS is a virtual appliance designed for deployment as a Virtual Machine (VM) instance in Amazon Web Services. Infoblox vNIOS for AWS enables you to deploy robust, manageable, and cost effective Infoblox appliances in the Amazon Cloud.

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

Infoblox vNIOS for AWS Use Cases

Extending your Infoblox grid into AWS 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 AWS VPCs. This allows you to extend your enterprise DNS and RPZ services into the public cloud. Clients running on AWS, attached to your VPCs, 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 or transit virtual networks and used for DNS resolution across other virtual networks via peering relationships. This is powerful especially when combined with the vDiscovery use case for automated creation of DNS records for your AWS resources.

IPAM and vDiscovery for Public Cloud

The Infoblox vDiscovery feature can be used for detecting and obtaining information about Tenants, VPCs, Subnets, and Virtual Machines operating in your AWS environments. Many organizations operate hybrid and multi-cloud environments that may contain many subscriptions and accounts. These environments tend to be very dynamic, with things such as VMs being created and terminated on a frequent basis. This makes it difficult to keep track of everything. With Infoblox vDiscovery, tasks can be configured to run automatically, allowing your Infoblox vNIOS appliance to keep track of all AWS environments, storing this data in IPAM. Infoblox vDiscovery can also be used to automate creation of DNS records for VMs running in your cloud environments. Using vDiscovery in conjunction with the Cloud Network Automation (CNA) feature, you will gain enhanced visibility into your cloud environments, all within a ‘single pane of glass’.

DHCP Service for On-Premises Clients

A vNIOS appliance running on AWS 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 AWS could also be configured for DHCP failover for highly available, fault tolerant DHCP services. Using a vNIOS appliance running on AWS 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 AWS VPC.

Reporting and Analytics

Infoblox Reporting and Analytics automates the collection, analysis, and presentation of core network service data that assists you in planning and mitigating network outage risks so you can manage your networks more efficiently. You can quickly create custom security reports and dashboards to identify security issues, ensuring that your network is secure and available. You can easily meet audit requirements with pre-configured, customizable compliance reports or quickly and easily create your own. To keep your Infoblox Grid running smoothly, you can track and project utilization of the Grid and easily forecast when you will need to scale up. Deploying Reporting members in AWS allows you to migrate workloads from the data center to the cloud and take advantage of the reliability and high availability of AWS deployments.

Fault Tolerance and Disaster Recovery

You can achieve Fault Tolerance and aid in Disaster Recovery of DDI services by deploying vNIOS appliances in AWS. In case of failure in the Primary Datacenter (power outage, network outage, or other critical failure) an Infoblox vNIOS appliance enabled as a Grid Master Candidate (GMC) can be promoted to the Grid Master role so that Grid services can continue to operate. Deploying vNIOS appliances in multiple regions and across availability zones can increase fault tolerance and survivability further. DNS services can also be redirected to vNIOS instances operating in AWS, possibly without even requiring any manual intervention, helping to ensure the business can continue to operate. DHCP fault tolerance can be achieved using Infoblox DHCP Failover configured between on-premises grid members and members running on AWS.

AWS Regions

Infoblox vNIOS for AWS is available in the following regions: us-east-1, us-east-2, us-west-1, us-west-2, ca-central-1, eu-central-1, eu-central-2, eu-west-1, eu-west-2, eu-west-3, eu-north-1, eu-south-1, eu-south-2, ap-east-1, ap-southeast-1, ap-southeast-2, ap-southeast-4, ap-northeast-1, ap-northeast-2, ap-northeast-3, ap-south-1, ap-south-2, sa-east-1, me-central-1, me-south-1, af-south-1.

AWS Services

The following AWS services are used in a typical vNIOS deployment on AWS:

- **VPC**: Virtual Private Clouds are used to deploy virtual networks and associated resources in a logically isolated area of the AWS cloud. https://docs.aws.amazon.com/vpc/index.html
- **EC2**: Elastic Compute Cloud is the underlying service which provides compute resources in the Amazon cloud. https://docs.aws.amazon.com/ec2/index.html
- **EBS**: Elastic Block Store provides storage volumes for use with EC2 instances. https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AmazonEBS.html

Workflow

The following outline lays out the basic steps to deploy and configure Infoblox vNIOS in a new AWS account (steps 7-8 are optional, depending on specific use case):

1. Deploy an AWS VPC and subnets.
2. Deploy and configure Internet access for your VPC.
3. Deploy a vNIOS instance.
4. Add a public IP to your vNIOS instance.
5. Connect to your vNIOS instance.
6. Join your vNIOS instance to a Grid or create a new Grid.
7. Configure vNIOS as DNS server for AWS VPC.
8. Perform vDiscovery for AWS.

Typical time for deployment and configuration of vNIOS for AWS, following this user guide is 30 to 45 minutes, depending on which use cases are configured.

Prerequisites

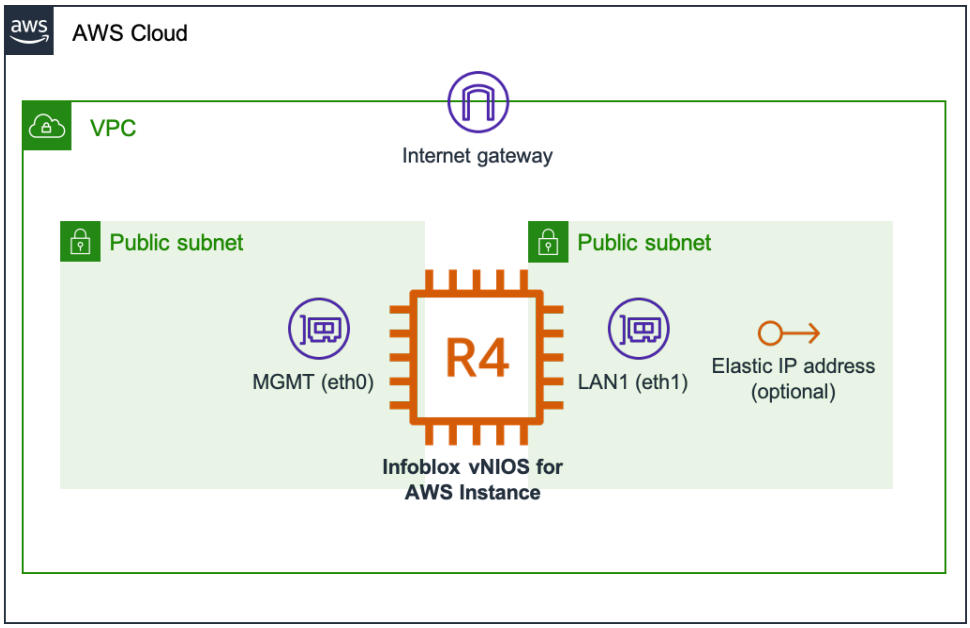
The following are prerequisites to deploying and managing an Infoblox vNIOS for AWS appliance:

- Valid AWS account.
- Permissions on AWS to create VPCs, VMs, and related resources.
- Understanding of basic networking concepts and tools, including public and private IP addressing, DNS, Secure Shell (SSH), and command line/terminal applications.

Architecture

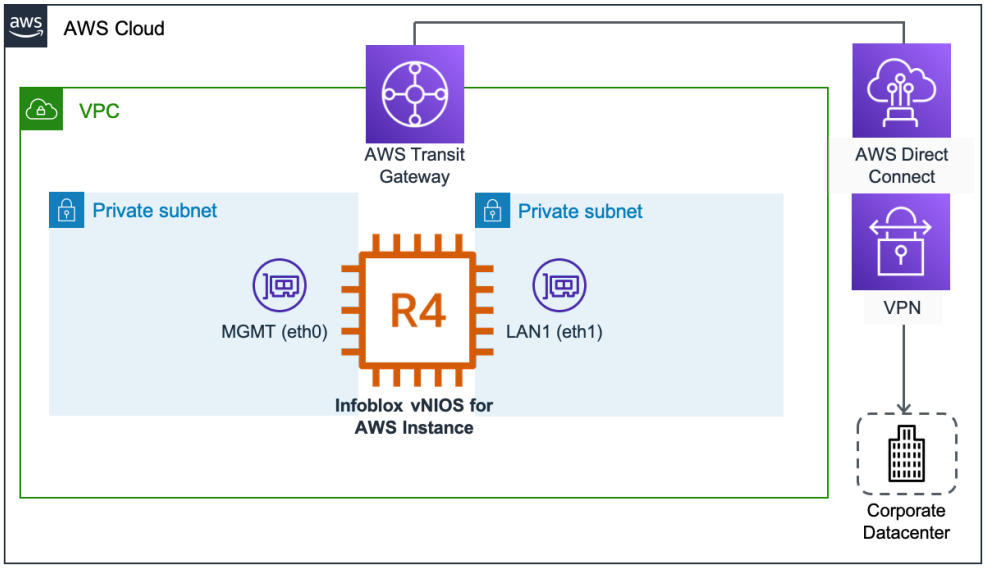
Specific designs for Infoblox vNIOS for AWS deployment architectures can vary based on the use cases and cloud/hybrid environment of an organization. At a minimum, deployments will require a VPC with two subnets and a vNIOS instance with two network interfaces. The diagrams in this section depict basic architecture for a standalone deployment and a hybrid Grid deployment.

Standalone Deployment



This diagram shows a typical stand-alone Infoblox vNIOS for AWS deployment. An Internet gateway allows the instance inbound and outbound connectivity. An Elastic IP can be associated with the vNIOS LAN1 (eth0) interface to allow admin access via the Internet.

Hybrid Grid Deployment



This diagram shows a typical hybrid Grid deployment where the Infoblox vNIOS for AWS instance will communicate with a Grid Master running on-premises. AWS Direct Connect or a site-to-site VPN allows for private communication between Grid members running on-premises and in AWS.

Security Considerations

Infoblox NIOS and Grid technology are purpose-built for security. The NIOS operating system does not allow for root access and services are disabled by default until configured. Infoblox Grid communication takes place through encrypted VPN tunnels established between the Grid Master and member appliances. For information on additional security services and configuration, refer to Infoblox NIOS documentation at https://docs.infoblox.com/display/ILP/NIOS. When deploying and using Infoblox vNIOS on AWS, you should always follow AWS IAM best practices as detailed in AWS IAM documentation: https://docs.aws.amazon.com/iam/index.html. The sections below cover security considerations specific to Infoblox vNIOS for AWS appliance deployment and configuration.

Infoblox vNIOS Admin Accounts

A user must have an admin account to log in to the vNIOS appliance. Each admin account belongs to an admin group, which is assigned roles and permissions that determine the tasks a user can perform. Users connect to the vNIOS appliance with a username and password. Infoblox strongly recommends changing the default administrator password to a complex password containing a mix of uppercase and lowercase letters, numbers, and special characters.

Additionally, Infoblox recommends creating role-based accounts for admins, using the principle of least privilege, granting minimal permissions needed to conduct required tasks.

For additional information on role-based access control in vNIOS and additional authentication methods, refer to the Infoblox NIOS Admin Guide: https://docs.infoblox.com/display/nios85/Managing+Administrators.

IAM Configuration for vDIscovery

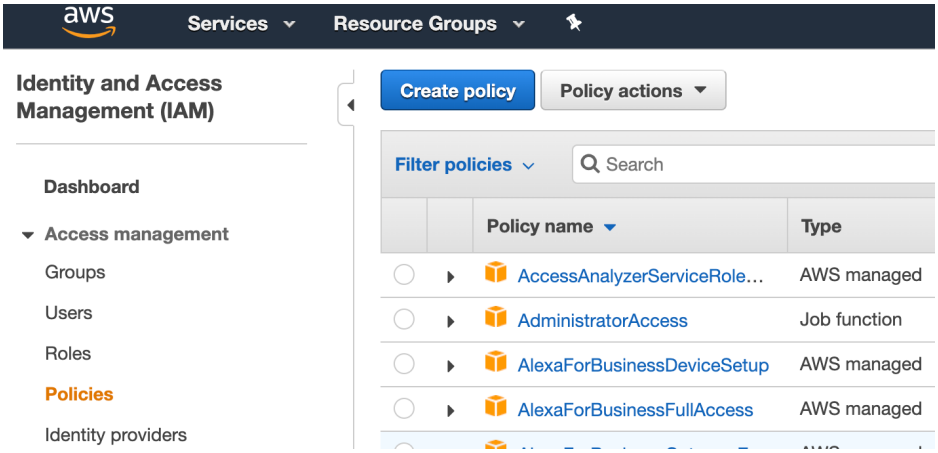
In order to use the Infoblox vDiscovery for AWS feature described in the Configuration section of this guide, you will need an IAM user or role with some minimum permissions to view resources in AWS. Minimum permissions required in AWS to conduct vDiscovery are:

- iam:GetUser
- ec2:DescribeVpcs
- ec2:DescribeSubnets
- ec2:DescribeRouteTables
- ec2:DescribeAddresses
- ec2:DescribeNetworkInterfaces
- ec2:DescribeInstances

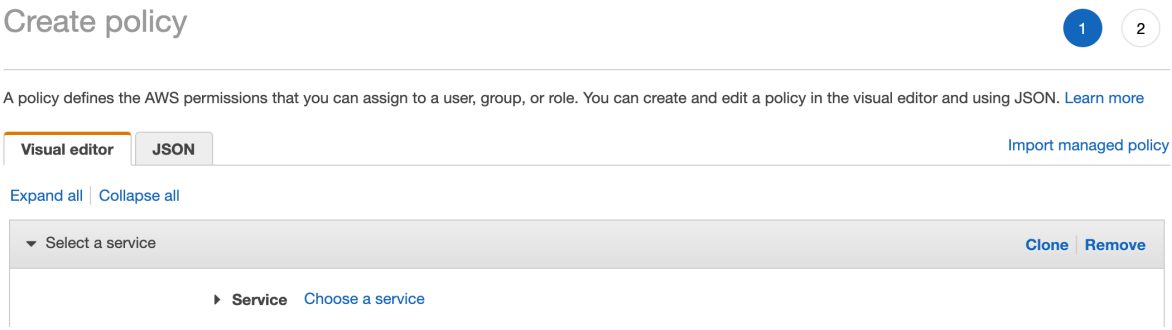
IAM Policy

First, we will create a custom policy with the permissions listed above to assign to users or roles.

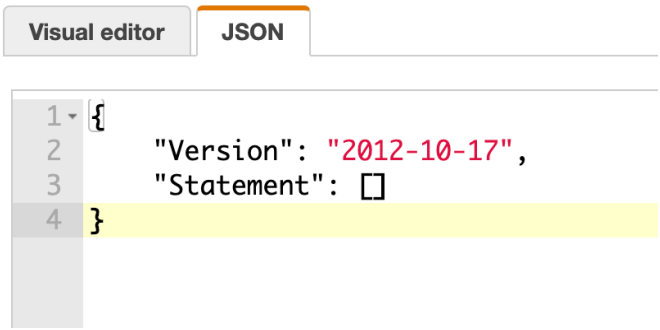
1. In the AWS Management Console, Use the Services menu to navigate to **IAM** under Security, Identity, & Compliance.
2. Select **Policies** from the IAM menu.
3. Click on **Create policy**.



4. Policies can be selected through the visual editor or defined using JSON. For this guide, we will use JSON. Click the **JSON** tab.



5. In the JSON editor view, you will see the base outline for a policy definition:



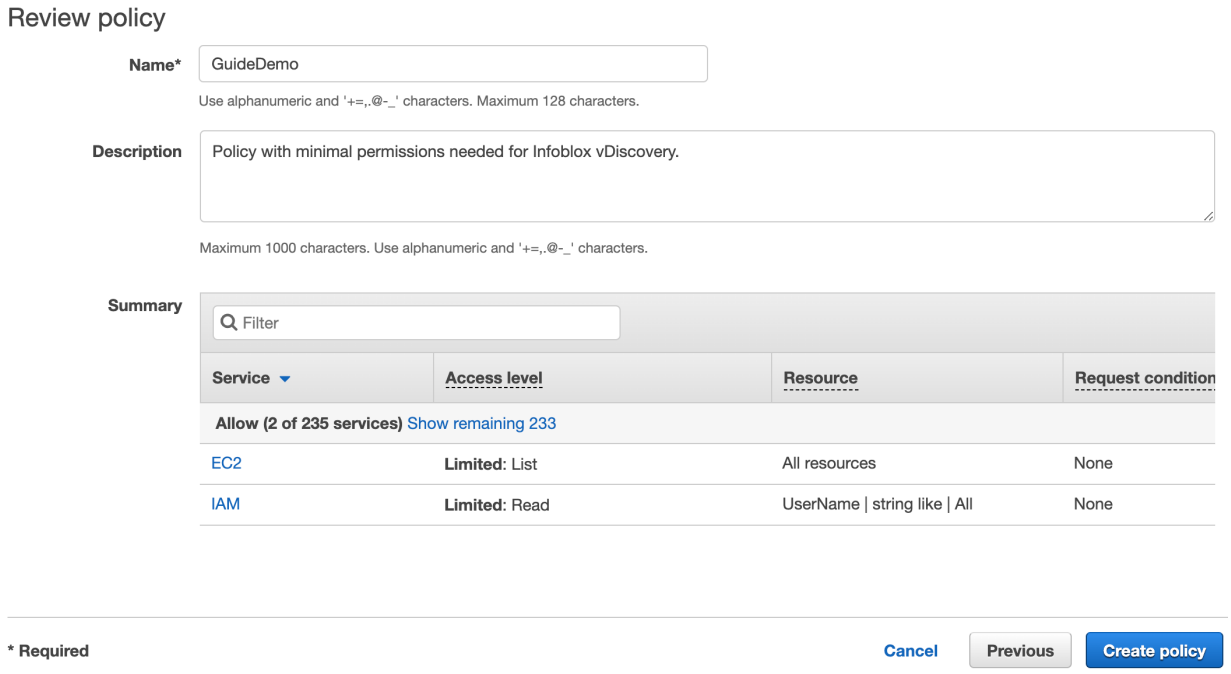
6. Between the square brackets next to Statement, paste the following to define your policy:

```
{
  "Effect": "Allow",
  "Action": [
    "ec2:DescribeAddresses",
    "ec2:DescribeInstances",
    "ec2:DescribeNetworkInterfaces",
    "ec2:DescribeVpcs",
    "ec2:DescribeSubnets",
    "ec2:DescribeRouteTables"
  ],
  "Resource": "*"
},
{
  "Effect": "Allow",
  "Action": "iam:GetUser",
  "Resource": "arn:aws:iam::*:user/*"
}
```

7. Your JSON policy definition should look like this:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeAddresses",
                "ec2:DescribeInstances",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeVpcs",
                "ec2:DescribeSubnets",
                "ec2:DescribeRouteTables"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:GetUser",
            "Resource": "arn:aws:iam::*:user/*"
        }
    ]
}
```

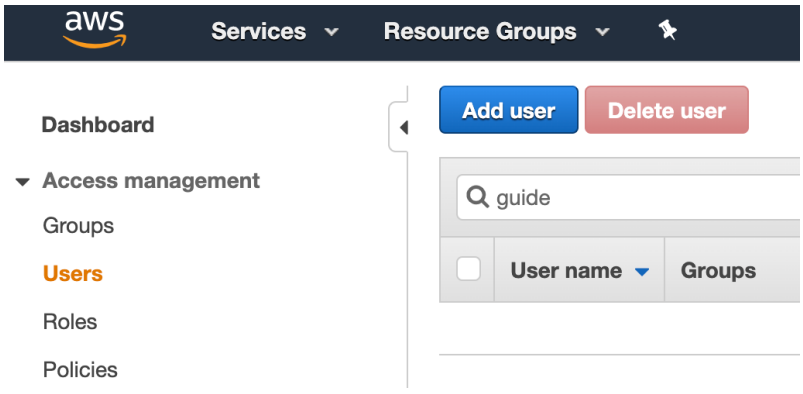
8. Click **Next: Tags**. Add tags if desired.
9. Click **Next: Review**.
10. Name your policy.
11. Optionally, add a description.
12. Review the Summary.
13. Click **Create Policy**.



IAM User

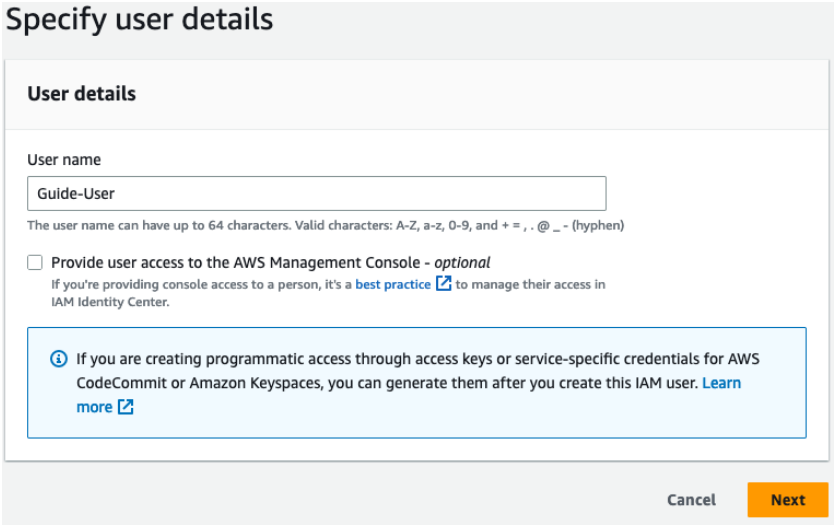
Next, we will create a user with an access key that can be used to authenticate for vDiscovery jobs.

1. Select **Users** from the IAM menu.
2. Click **Add users**.

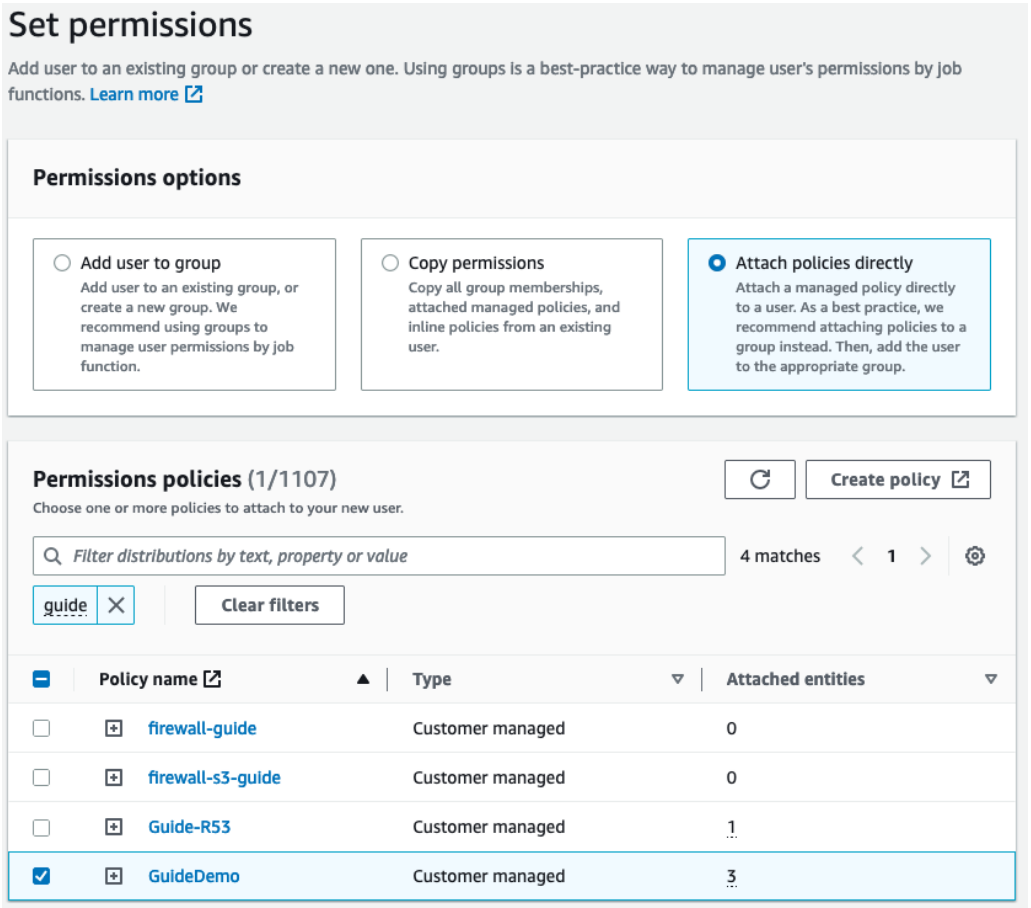


3. Name the user.

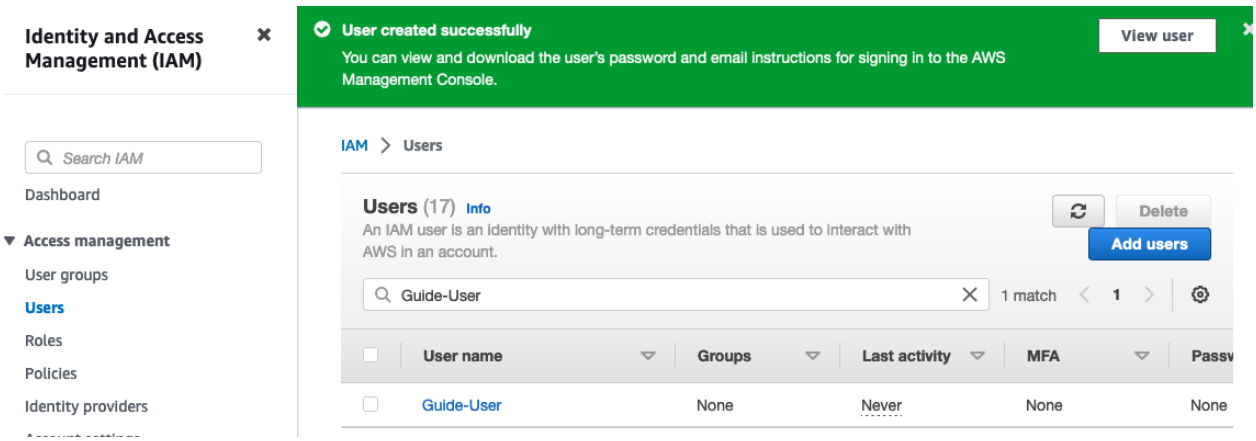
4. Click **Next**.



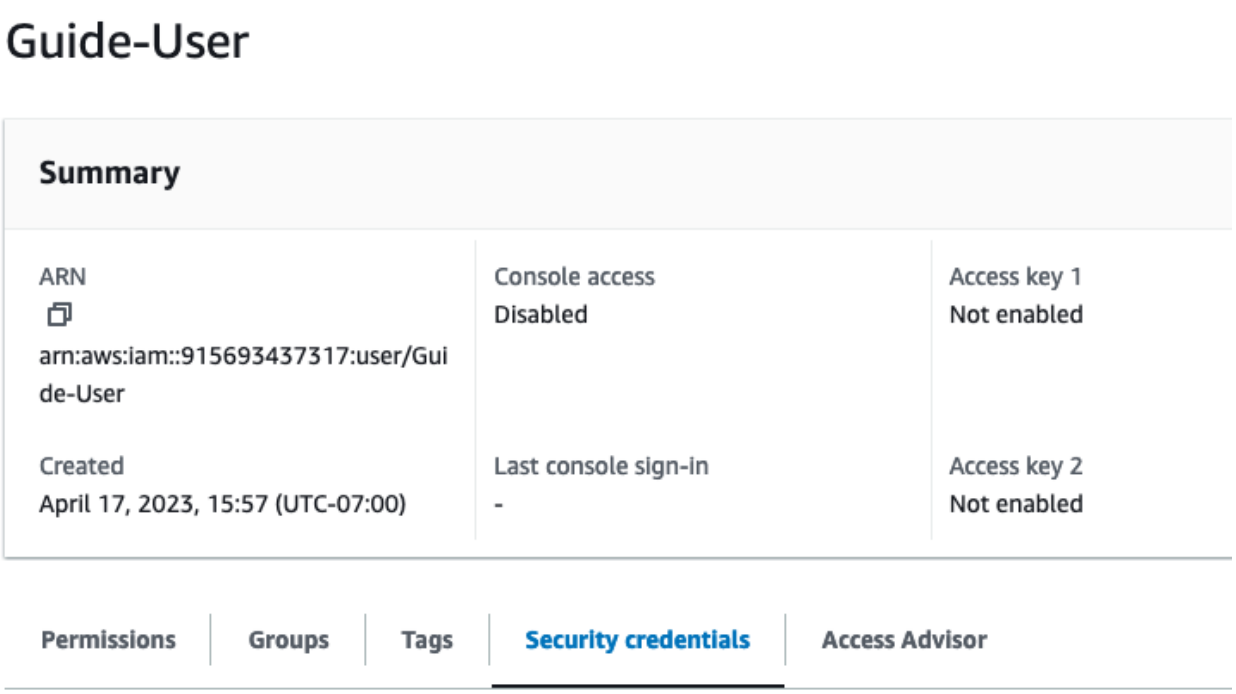
5. Under Permissions options, select **Attach policies directly**.
6. Use the Permissions policies search to locate and select your vDiscovery policy.
7. Click **Next**.



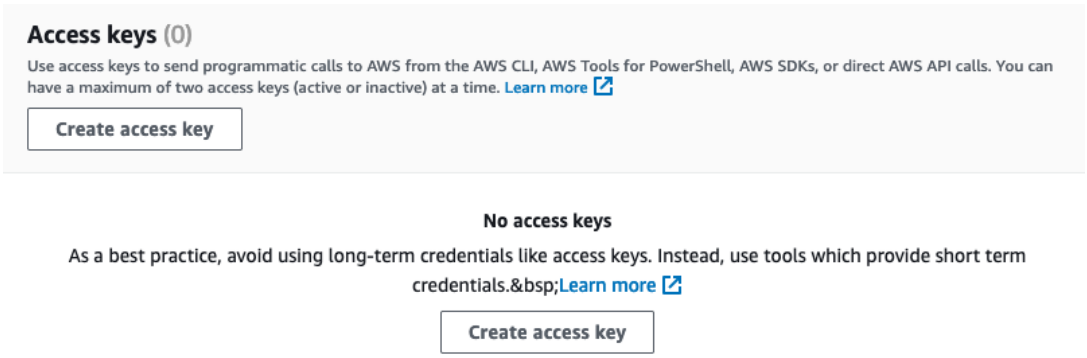
8. On the Review and create step, review details and click **Create user**.
9. After the user is created, search for and click on the new user.



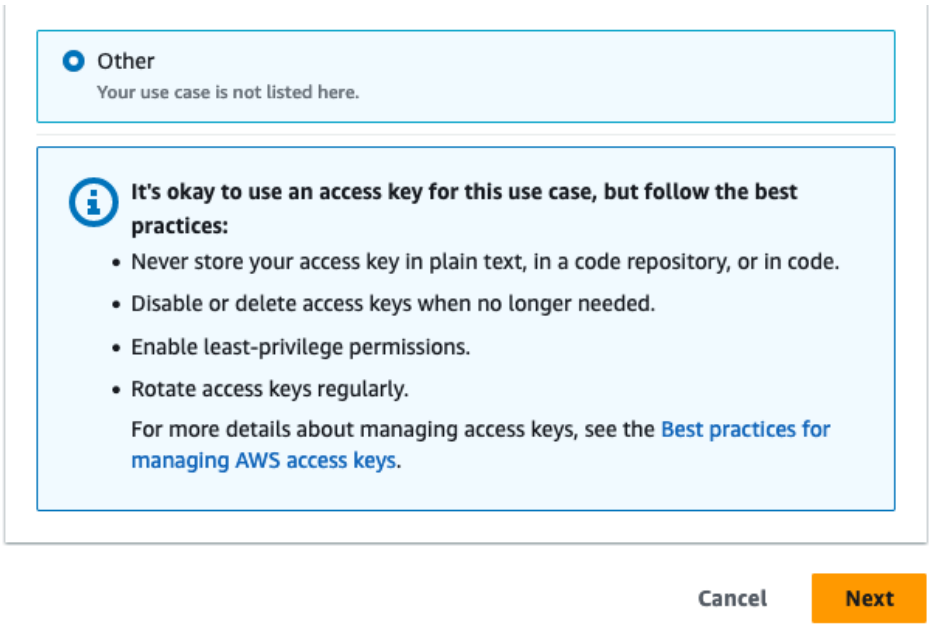
10. Select the **Security credentials** tab.



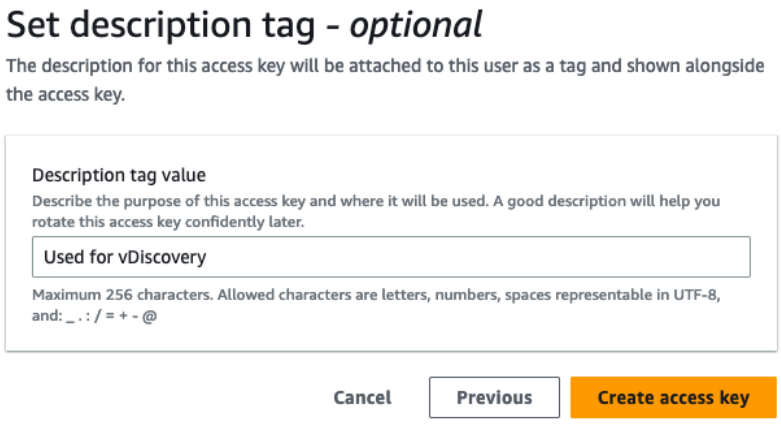
11. Scroll down to the Access Keys section and click **Create access key**.



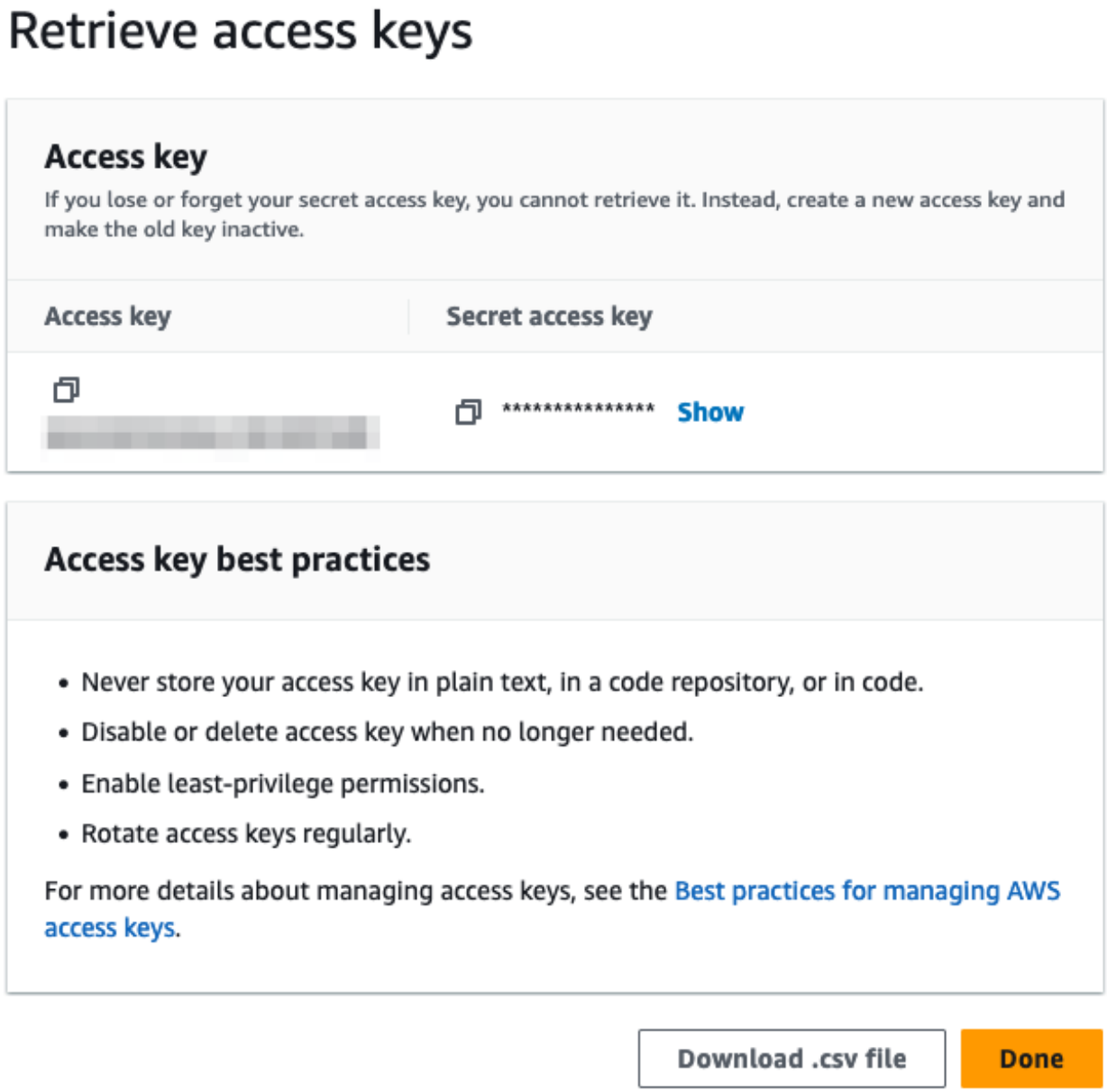
12. Select **Other** and click **Next**.



13. Add a description for the key and click **Create access key**.



14. Click **Download .csv file** to retrieve the new keys.



Warning: This is the only opportunity to download or view these credentials. If you do not save them, or lose them later, you will have to create new access keys for this user.

15. Click **Done**.

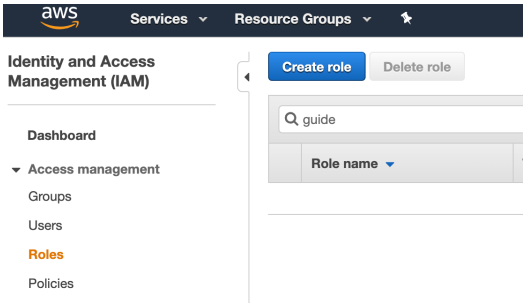
Rotating Credentials

When using user access keys as described in the previous section, keys should be rotated on a regular basis, at a minimum every 90 days. To rotate access keys for an IAM user, follow the guidance in AWS documentation: https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_access-keys.html, specifically the section titled **Rotating access keys**.

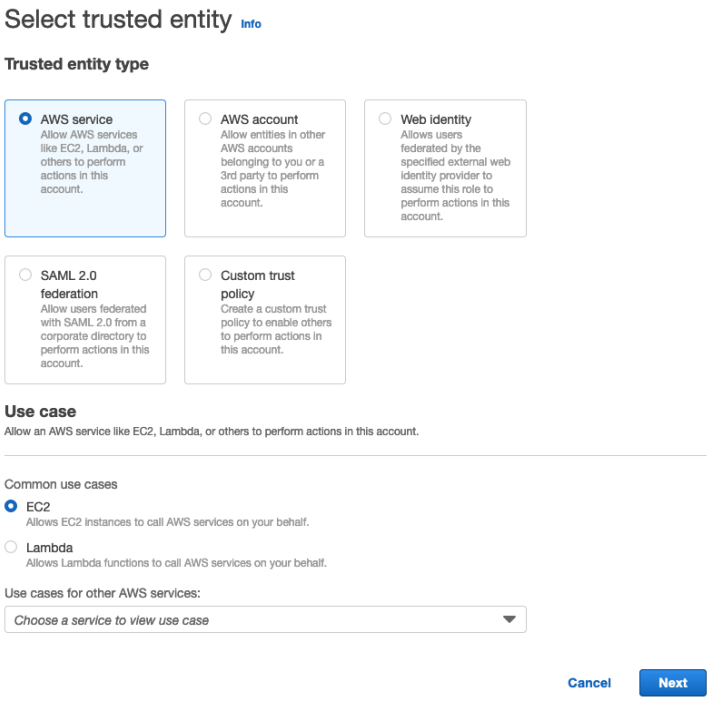
IAM Role

Creating a role to use for vDiscovery is optional and if desired should be completed prior to deploying your vNIOS for AWS instance. The role can be assigned to your instance during deployment, as described in the Deploy vNIOS Instance in AWS → Configure Instance Details section of this guide. It is also possible to add roles to a running instance using the AWS CLI command: **aws ec2 associate-iam-instance-profile**. See AWS CLI documentation for details on working with this and other commands related to IAM roles: https://docs.aws.amazon.com.

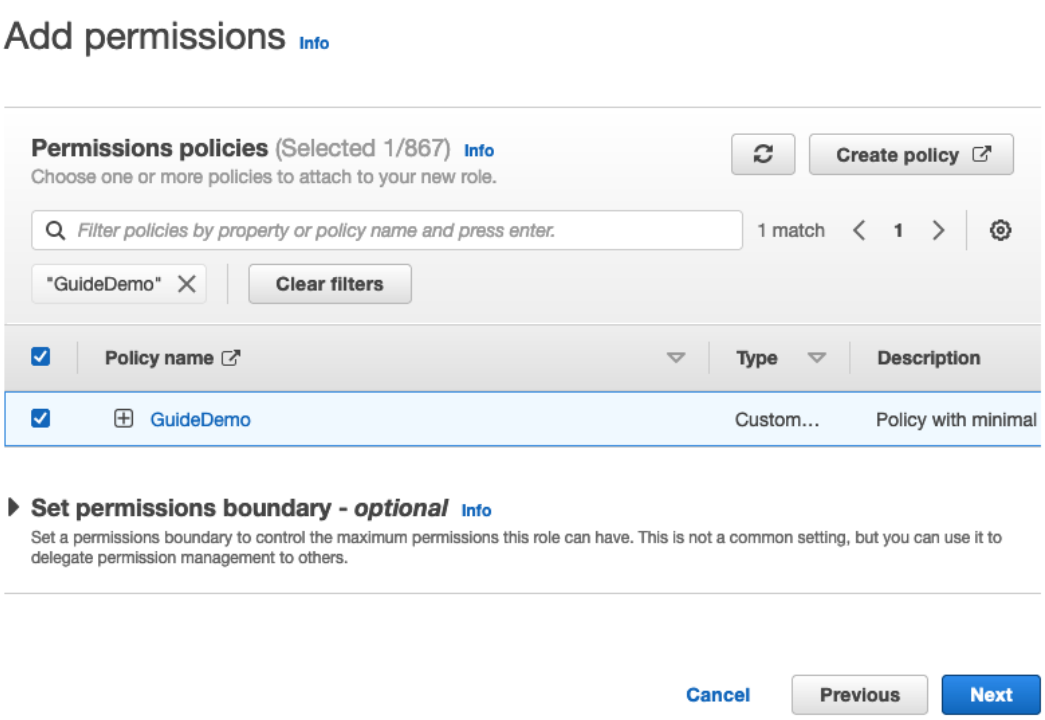
1. In the AWS Management Console, Use the Services menu to navigate to **IAM** under Security, Identity, & Compliance.
2. Select **Roles** from the IAM menu.
3. Click on **Create role**.



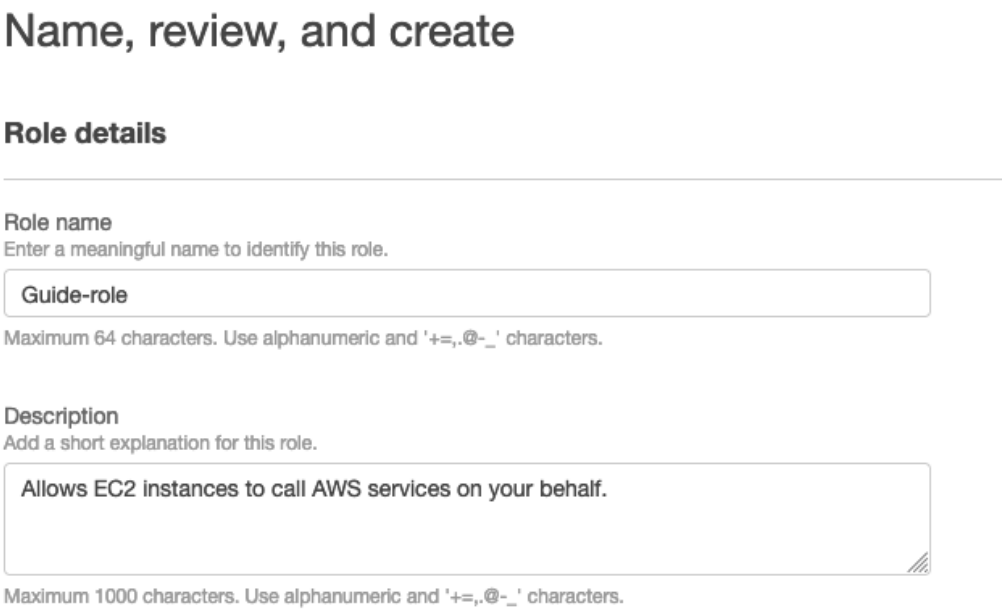
4. For Trusted entity type, select **AWS service**.
5. For Use case, select **EC2**.
6. Click **Next.**



7. Enter the name of your policy in the search bar or scroll down to locate your policy.
8. Check the box next to your vDiscovery policy.
9. Click **Next**.



10. Enter a name under Role name.
11. Optionally, add a description.
12. Review the role properties.
13. Scroll down and click **Create role**.



Network Configuration

Network security and configuration requirements can vary greatly based on use case. You will need a security group in each VPC where vNIOS is deployed to allow for management and service traffic. The following table lists the most common rules needed for Infoblox vNIOS for AWS appliances:

Type	Protocol	Port Range	Purpose
SSH	TCP	22	CLI access for appliance administration
HTTPS	TCP	443	Grid Manager GUI access
Custom UDP Rule	UDP	1194	NIOS Grid Traffic (VPN)
Custom UDP Rule	UDP	2114	NIOS Grid Traffic (key exchange)
DNS (UDP)	UDP	53	UDP DNS
DNS (TCP)	TCP	53	TCP DNS
Custom UDP Rule	UDP	67-68	DHCP
Custom TCP Rule	TCP	8787	Infoblox AWS API Proxy

The following table lists additional rules used when deploying the TR-V5005 reporting appliance:

Type	Protocol	Port Range	Purpose
Custom TCP Rule	TCP	7089	Distributed search
Custom TCP Rule	TCP	7887	Reporting peer replication
Custom TCP Rule	TCP	9997	Reporting forwarders
Custom TCP Rule	TCP	8000	Reporting management
Custom TCP Rule	TCP	8089	Reporting management
Custom TCP Rule	TCP	9185	Splunk REST API
Custom TCP Rule	TCP	7000	WebUI (Master, Indexer)

Infoblox recommends you only allow traffic for necessary management and services. Rules should be as restrictive as possible in regard to where source traffic is allowed from. For further detail on ports and protocols used by Infoblox NIOS, refer to https://docs.infoblox.com/display/nios85/Configuring+Ethernet+Ports.

Planning Considerations

The following sections detail planning considerations specific to Infoblox vNIOS for AWS deployments.

Cost

Billable AWS Resources

The following billable AWS resources may be used as part of an Infoblox vNIOS for AWS deployment:

- **EC2 Instance**: This resource is mandatory and will be used in every Infoblox vNIOS for AWS deployment. Refer to the AWS EC2 Instance Size section of this guide for instance type and size selection. For current AWS EC2 instance prices and options, refer to AWS pricing documentation https://aws.amazon.com/ec2/pricing/.
- **EBS Volume**: This resource is mandatory and will be used in every Infoblox vNIOS for AWS deployment. Refer to the AWS EBS Volume Type and Size section of this guide for specific type and size. For current AWS EBS prices, refer to AWS pricing documentation https://aws.amazon.com/ebs/pricing/.
- **Elastic IP Address (EIP)**: This resource is optional for Infoblox vNIOS for AWS deployments. You can have one EIP associated with a running instance at no charge. For current prices of additional EIPs and EIPs not associated with a running instance, refer to AWS pricing documentation https://aws.amazon.com/ec2/pricing/on-demand/.

Infoblox Licenses

Infoblox vNIOS for AWS appliances use a bring your own license (BYOL) model. Sixty day temporary/trial licenses are available for many virtual appliances and features at no cost. The Deployment section of this guide covers details on installing temporary licenses during deployment. For details on obtaining and installing production licenses, refer to Infoblox documentation https://docs.infoblox.com/display/nios85/Managing+Licenses.

AWS EC2 Instance Size

This section lists the Infoblox vNIOS models available for deployment in AWS and recommends corresponding AWS EC2 instance types and sizes. The following table lists models and sizes available for the most recent NIOS versions (8.4 and 8.5) in most AWS regions.

vNIOS Model	vCPUs	Memory (GiB)	Type
TE-V825	2	15.25	r4.large
TE-V1425	4	30.5	r4.xlarge
TE-V2225	8	61	r4.2xlarge
TE-V4015	16	122	r4.4xlarge

TE-V4025	16	122	r4.4xlarge
CP-V805	2	15.25	r4.large
CP-V1405	4	30.5	r4.xlarge
CP-V2205	8	61	r4.2xlarge
TR-V5005	User Defined	User Defined	r4 Instance

For information on recommended sizes for models available with older NIOS versions and recommendations on alternate instance sizes when the above are not available, refer to vNIOS for AWS appliance documentation https://docs.infoblox.com/display/NAIG/Infoblox+vNIOS+for+AWS+AMI+Shapes+and+Regions.

AWS EBS Volume Type and Size

General Purpose SSD (gp2) EBS volumes should be used for Infoblox vNIOS for AWS instances. Volume size should be set to a default/minimum value of 250 GiB.

For reporting appliances only (NIOS 8.6.2 and later), you must add an additional volume. This volume should have a minimum size of 250 GiB.

Deployment

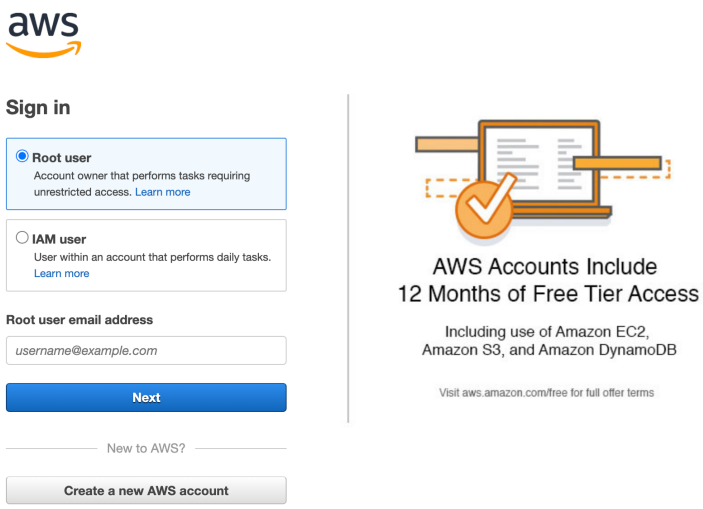
This section provides step-by-step instructions for deploying a new Infoblox vNIOS for AWS instance using the AWS Management Console. Deploying a new VPC is optional and should be skipped if you plan to deploy the vNIOS instance in an existing VPC. *Note: To use the MGMT interface of your vNIOS for AWS instance, you will need a VPC with two subnets in the same availability zone and the LAN1 and MGMT interfaces must be deployed in separate subnets.*

Deploy AWS VPC (Optional)

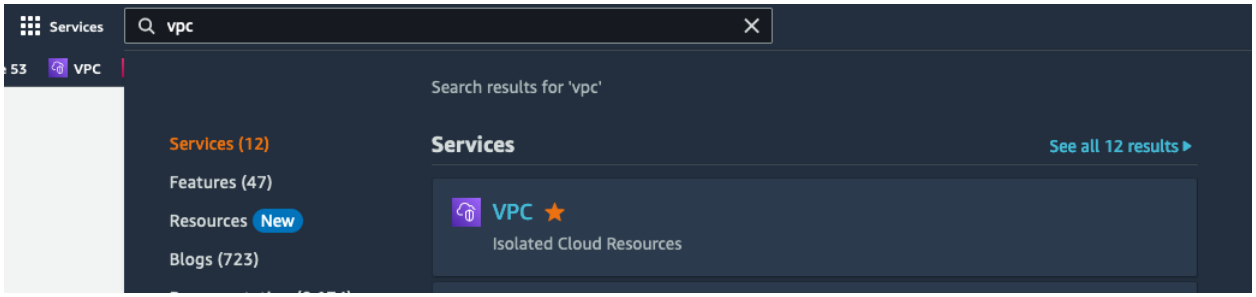
Prior to deploying a vNIOS for AWS instance, you will need a VPC in the desired region. This section details the deployment and configuration of a new VPC. If deploying vNIOS into an existing VPC, skip ahead to the Deploy vNIOS Instance section.

Create VPC

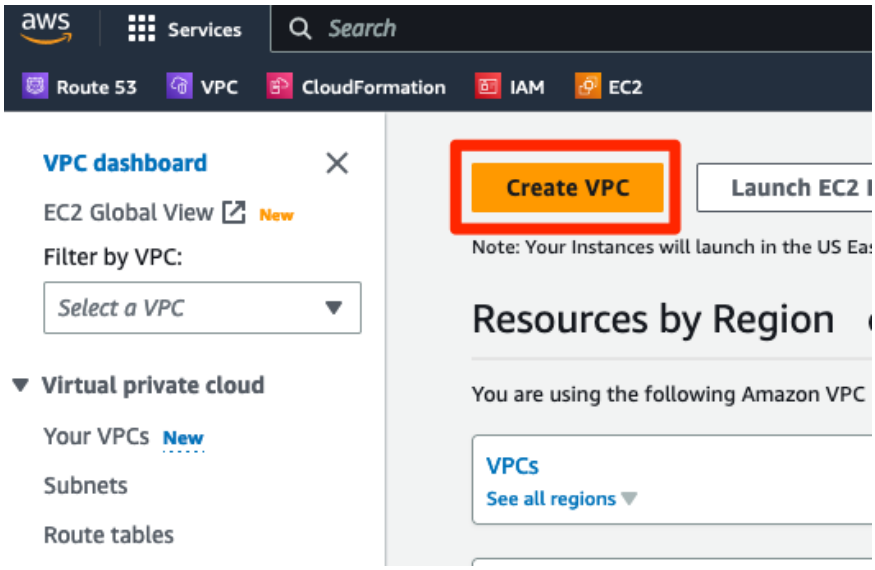
1. Log in to the AWS Management Console.



2. Use the Services search box to find and select **VPC**.

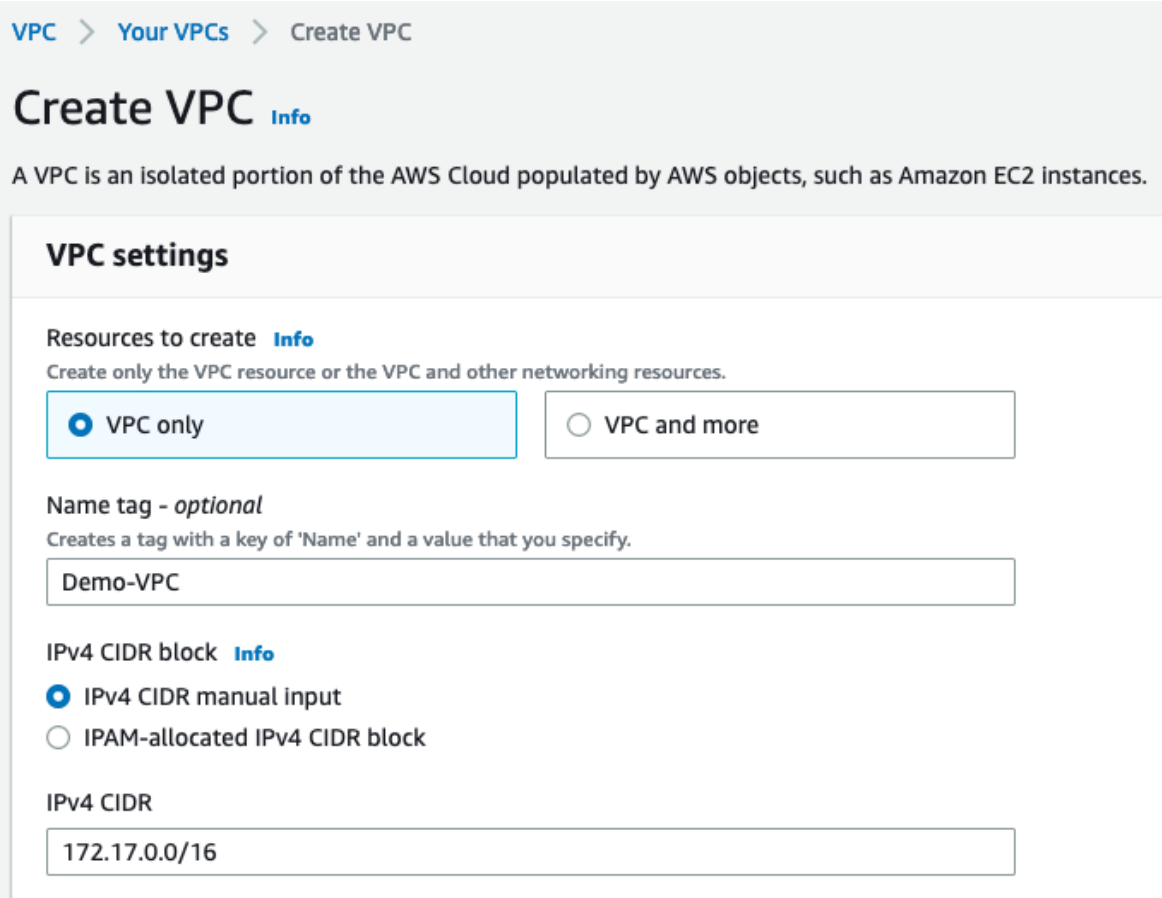


3. On the VPC Dashboard, click on **Create VPC**.



4. Select **VPC only**.

5. Enter a name for your VPC.
6. Enter an IPv4 CIDR block for your VPC.

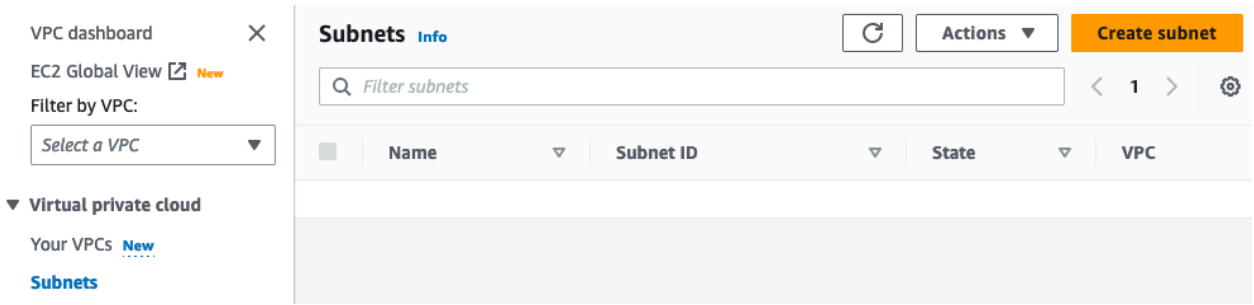


7. Scroll down to click **Create VPC**.

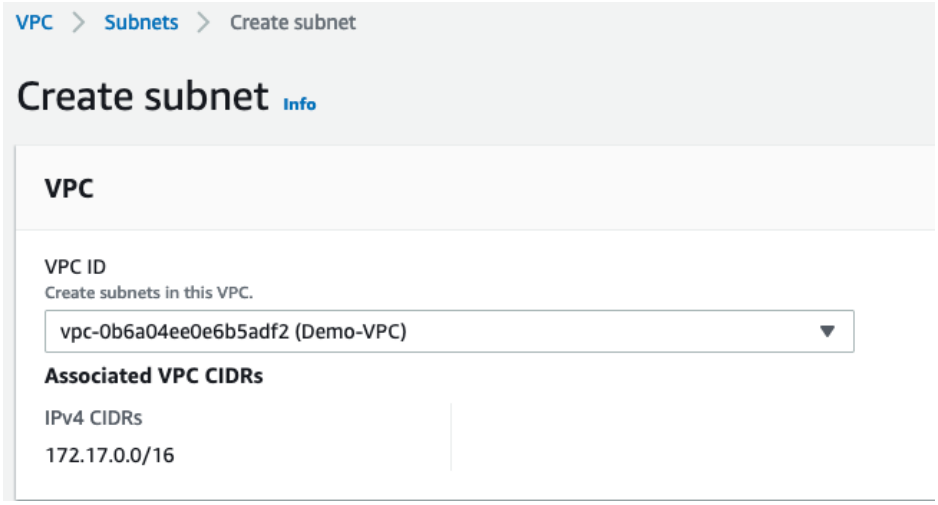
Create Subnets

Before using your new VPC, you will need to create at least one subnet. vNIOS for AWS instances should use two subnets, one for the LAN1 interface and one for the MGMT interface. In this guide, we will create a subnet for each interface.

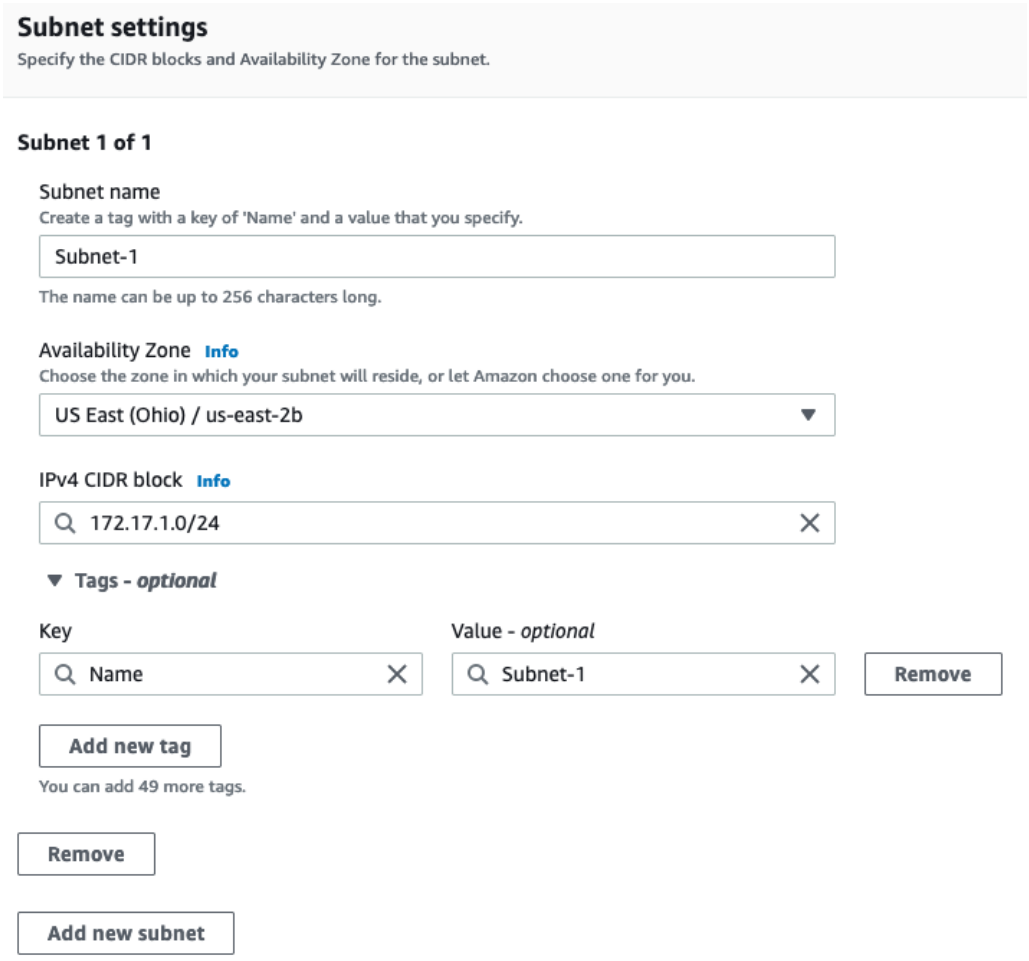
1. Back on the VPC page, click on **Subnets**.
2. Click the **Create subnet** button.



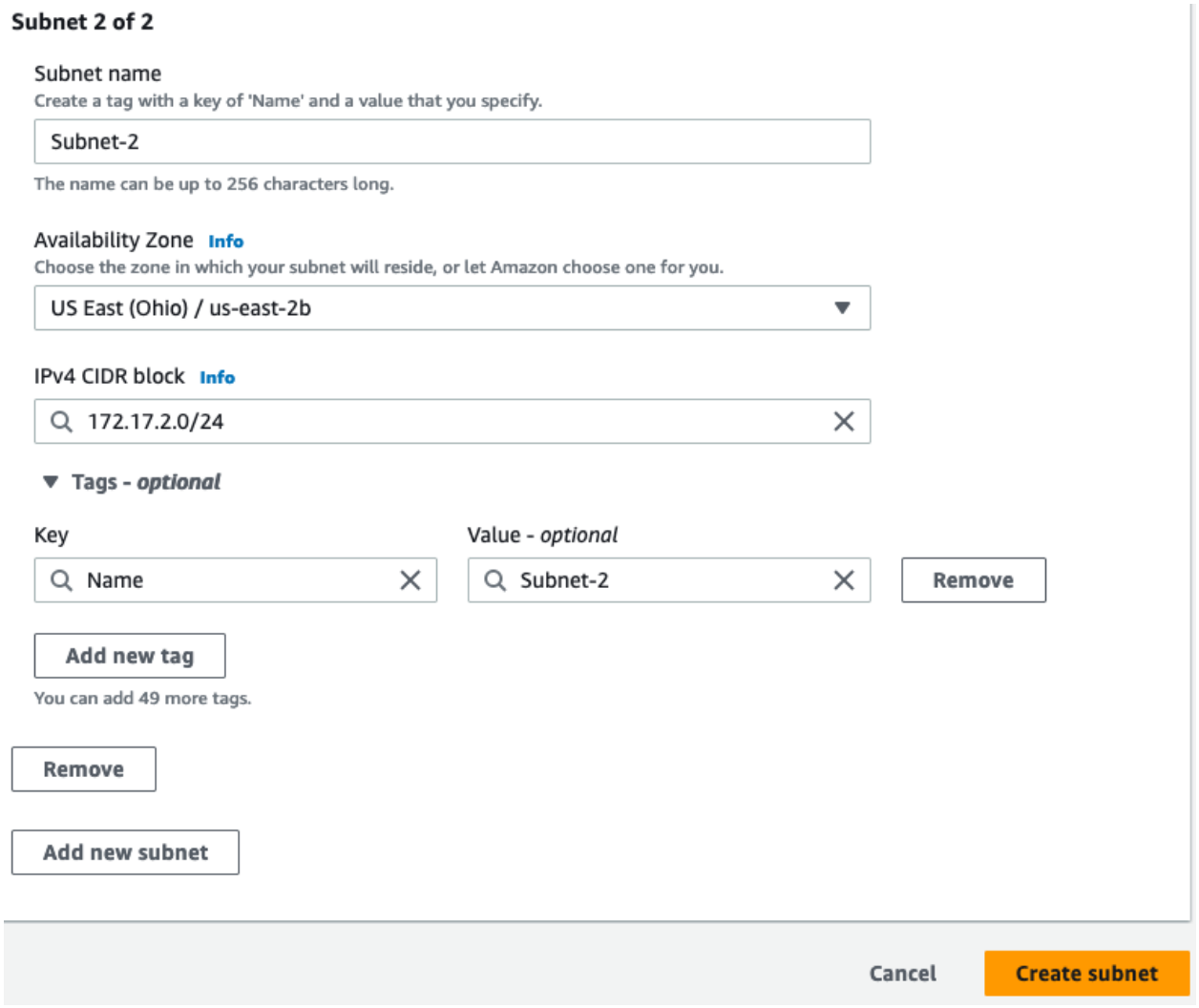
3. Select your new VPC from the dropdown list.



4. Enter a name for the subnet.
5. Select an Availability Zone.
6. Enter a CIDR block for the subnet that fits within the CIDR of your VPC.



7. Click **Add new subnet**.
8. Enter a name for the second subnet.
9. For Availability Zone, use the dropdown to select the same availability zone used by the first subnet.
10. Enter a CIDR for this subnet, which must not overlap with the first subnet.
11. Click **Create subnet**.

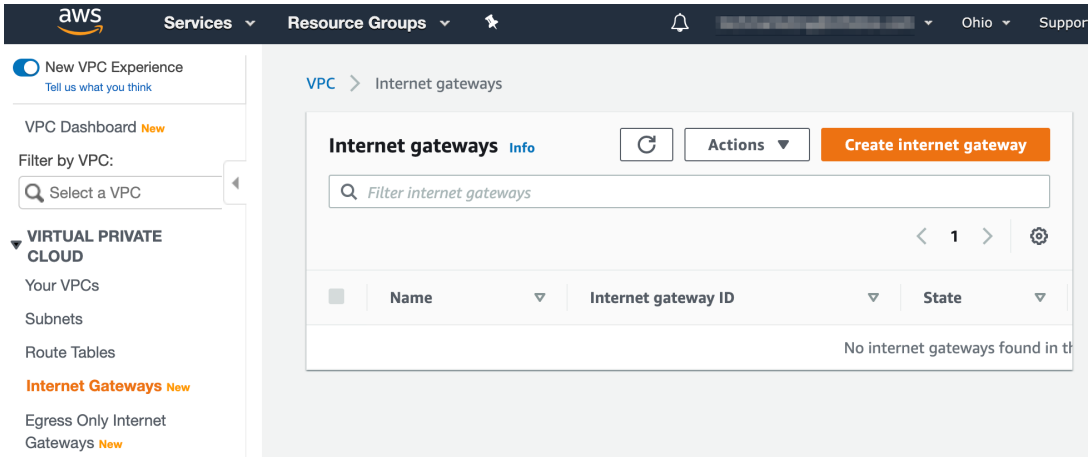


Add Internet Connectivity to the VPC

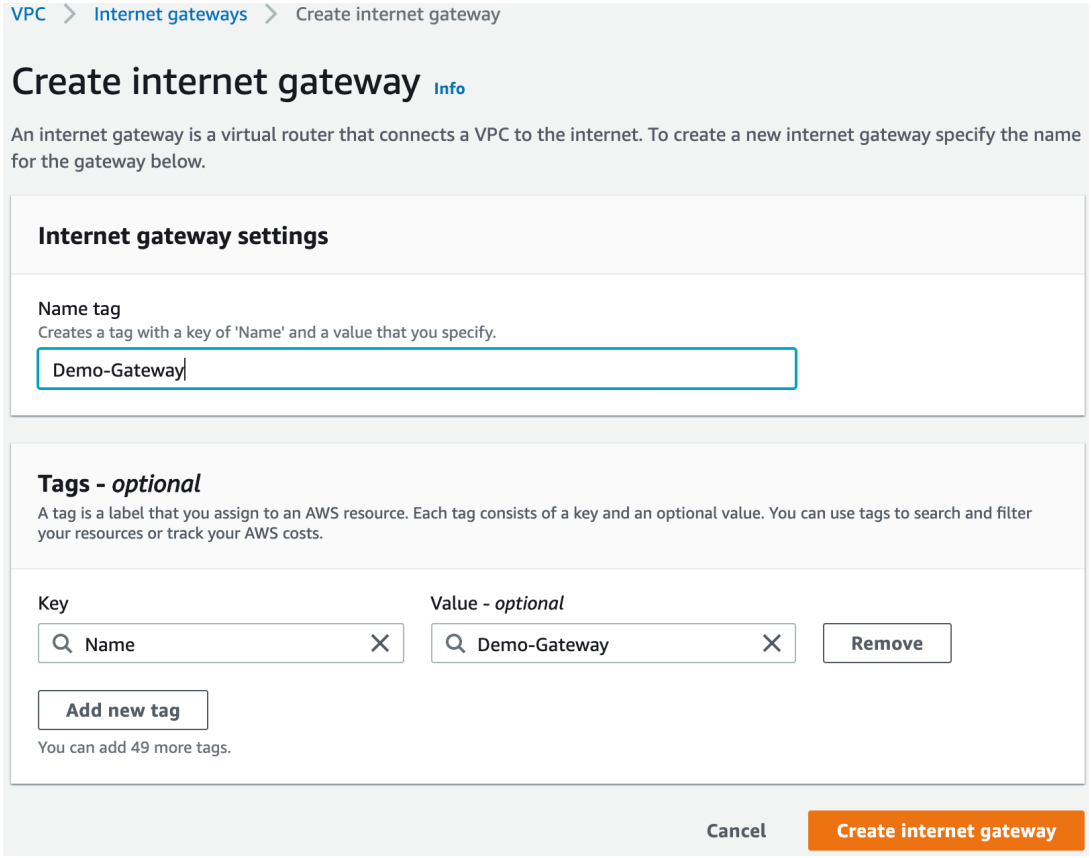
To allow connectivity in and out of your VPC through the Internet, including connectivity for your vNIOS instance, you will need to create an Internet Gateway and associated routes. If you are using site-to-site VPN or other methods of connecting to AWS VPCs, direct Internet connectivity may not be needed. Configuring these other types of connectivity are outside the scope of this guide; please refer to AWS documentation.

Attach Internet Gateway

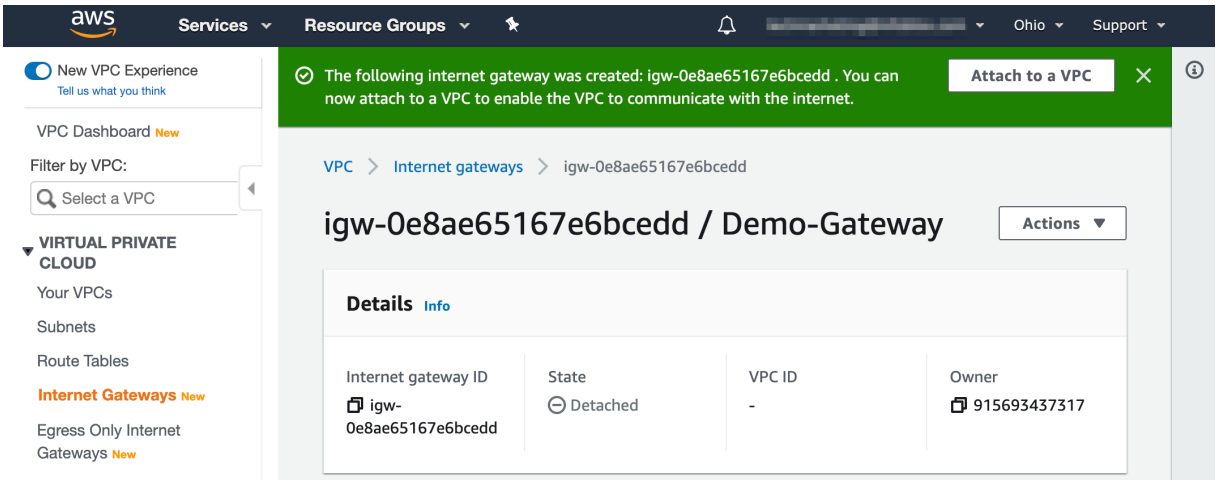
1. Click on **Internet Gateways** in the VPC menu.
2. Click on **Create internet gateway**.



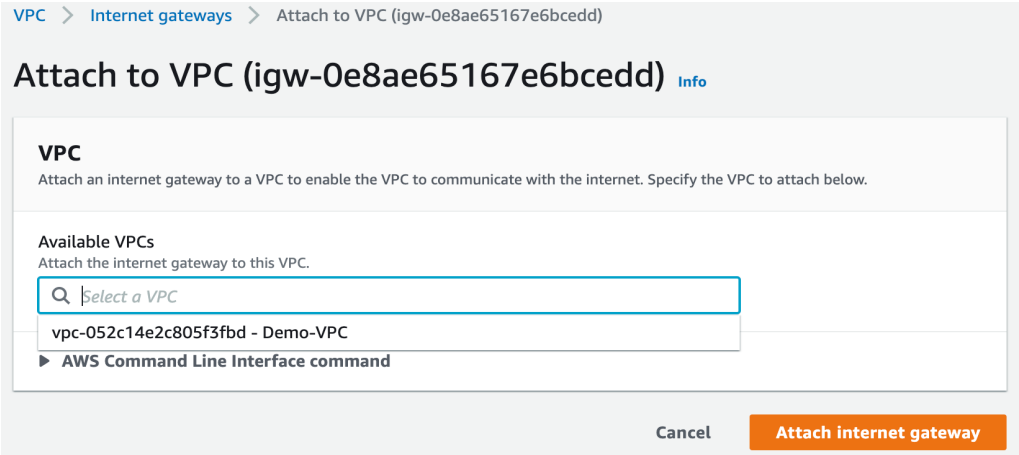
3. Name the gateway and optionally add other Tags.



4. Click **Create internet gateway**.
5. Once the gateway has been successfully created, click on **Attach to a VPC**.



6. Select your VPC from the dropdown.

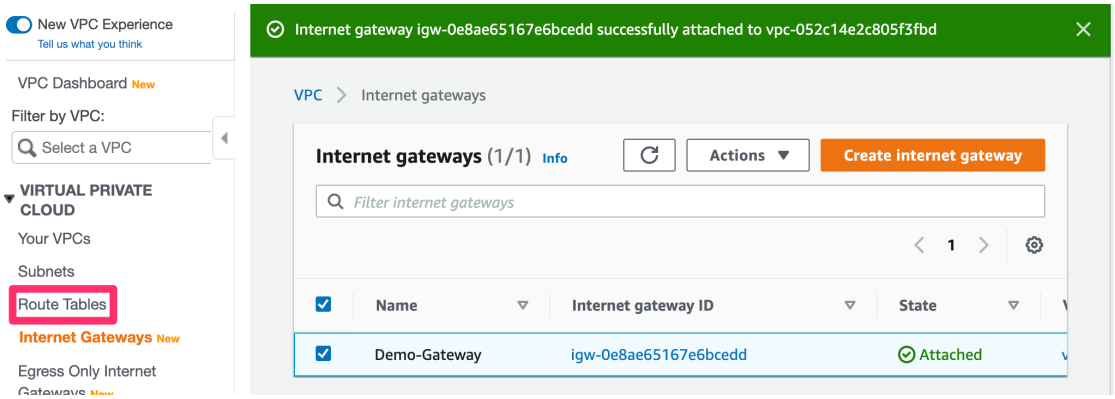


7. Click on **Attach internet gateway**.

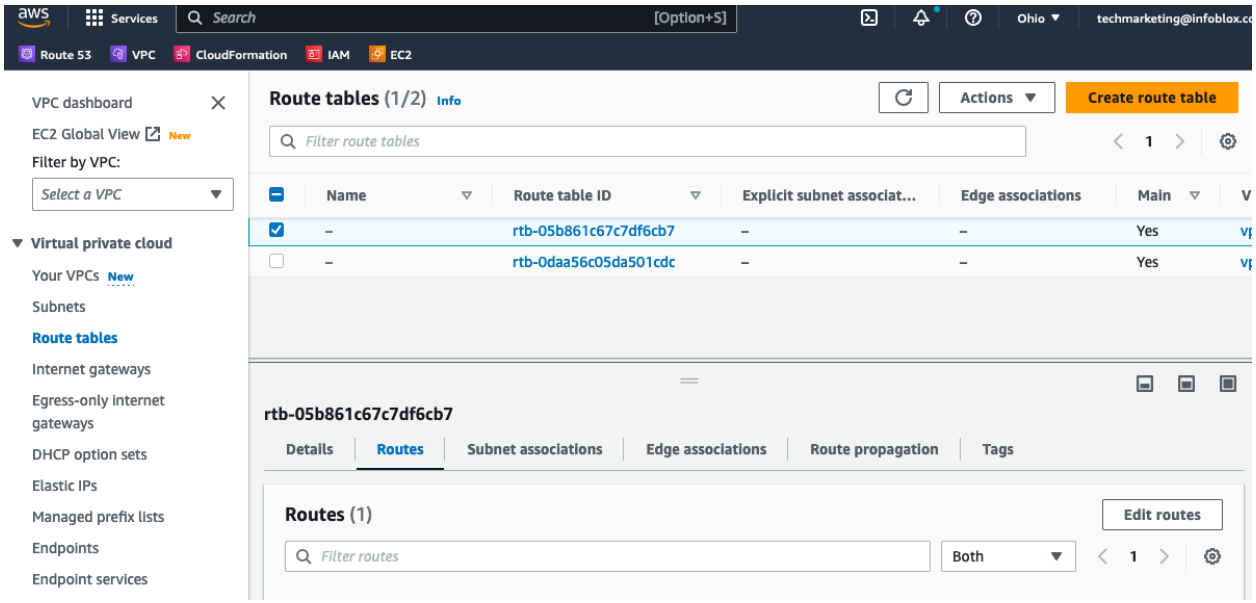
Add Routes

Next, we'll update the VPC route table to send all traffic through the new internet gateway.

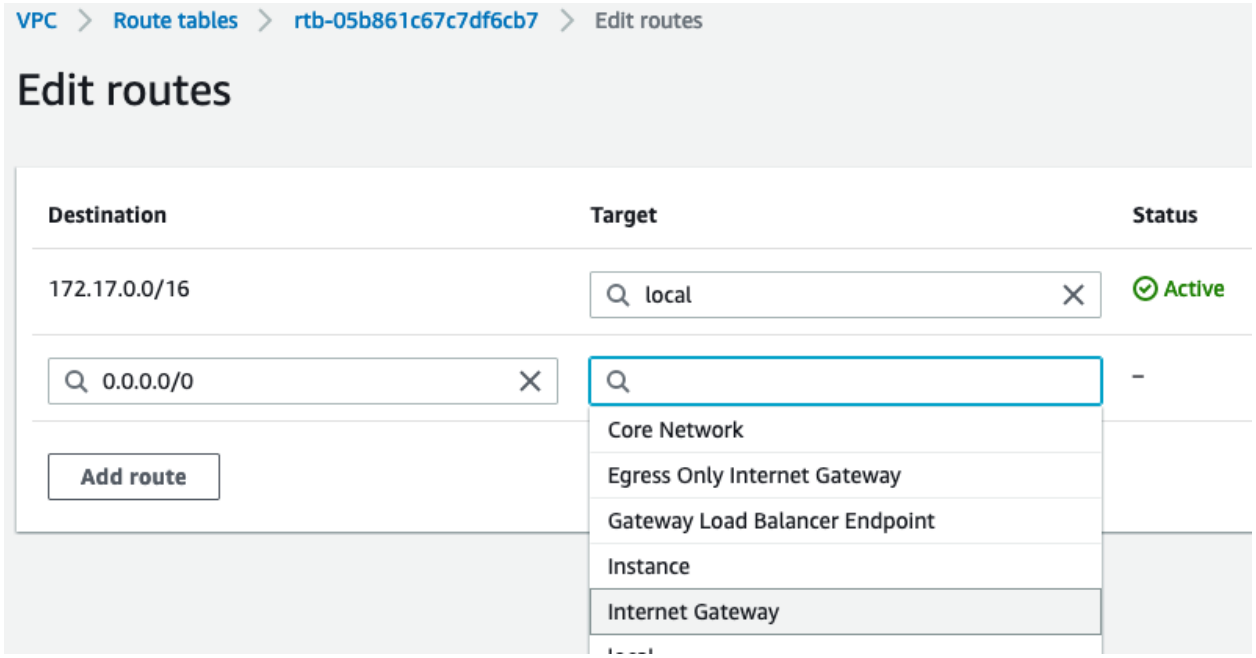
1. Once the attach operation is complete, click **Route tables** in the VPC menu.



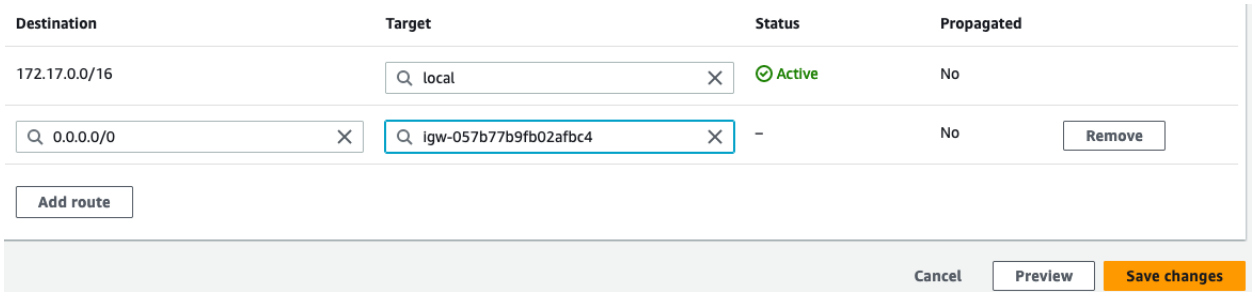
2. Select the route table for the new VPC.
3. Click on the **Routes** tab.
4. Click the **Edit routes** button.



5. On the Edit routes page, click **Add route**.
6. For Destination, enter **0.0.0.0/0**.
7. For Target, select **Internet Gateway** from the dropdown.



8. Select the Internet gateway for this VPC from the dropdown.
9. Click on **Save changes**.

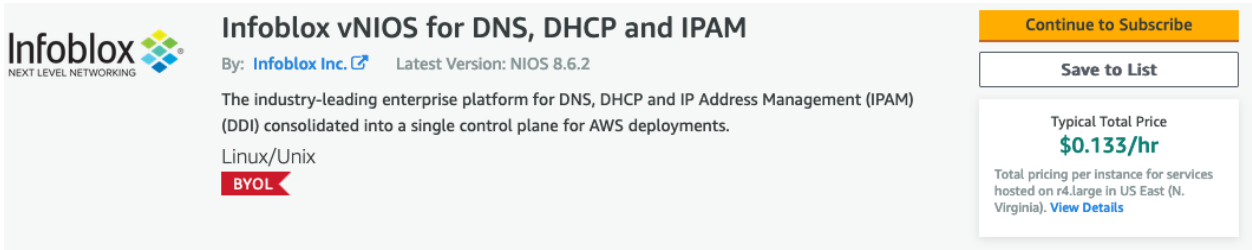


Deploy vNIOS Instance in AWS

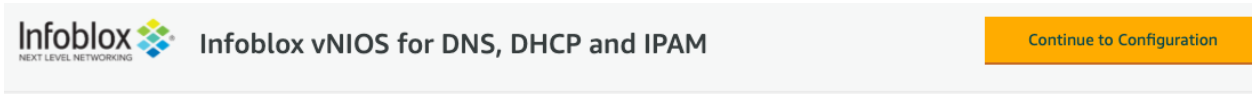
Infoblox vNIOS for AWS instances can be deployed using many different methods, including the AWS CLI, CloudFormation, AWS Management Console, and many other orchestration and automation platforms. Starting with NIOS version 8.5.2, Infoblox vNIOS for AWS can also be found in the AWS Marketplace. This guide will use the AWS Marketplace and AWS Console for deployment. Refer to the Additional Resources section at the end of this guide for links to information on other deployment methods.

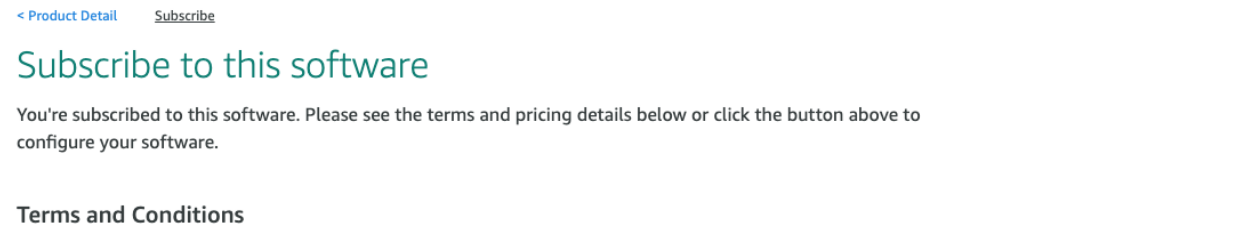
Deploy From Marketplace

1. To begin, in the AWS Marketplace, search for "Infoblox vNIOS for DNS, DHCP and IPAM".
2. Select the listing and click **Continue to Subscribe.**

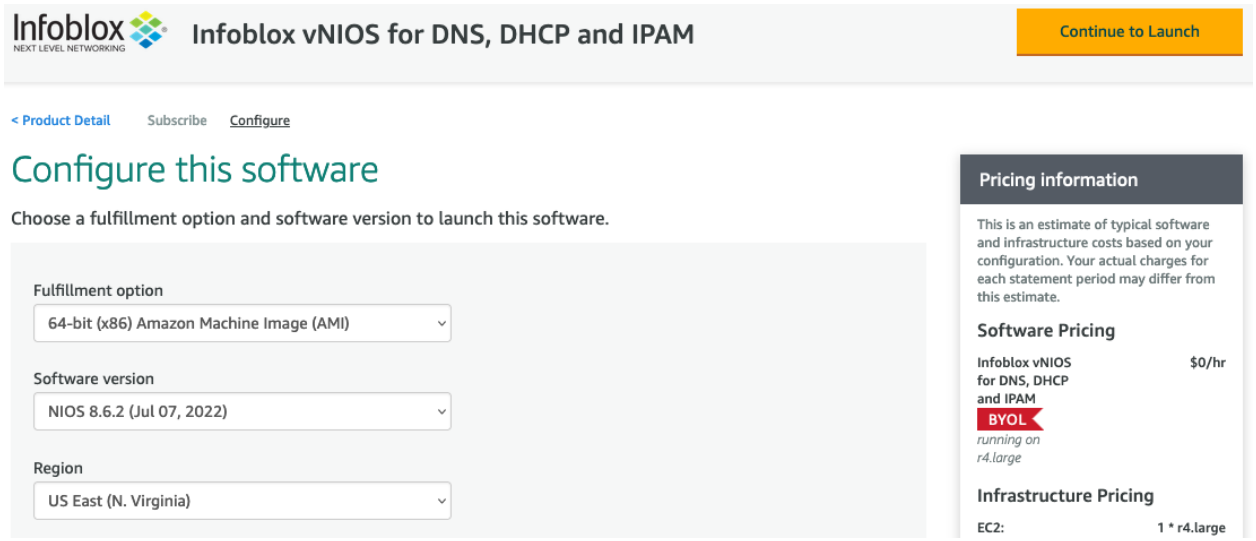


3. Accept terms and click **Continue to Configuration**.



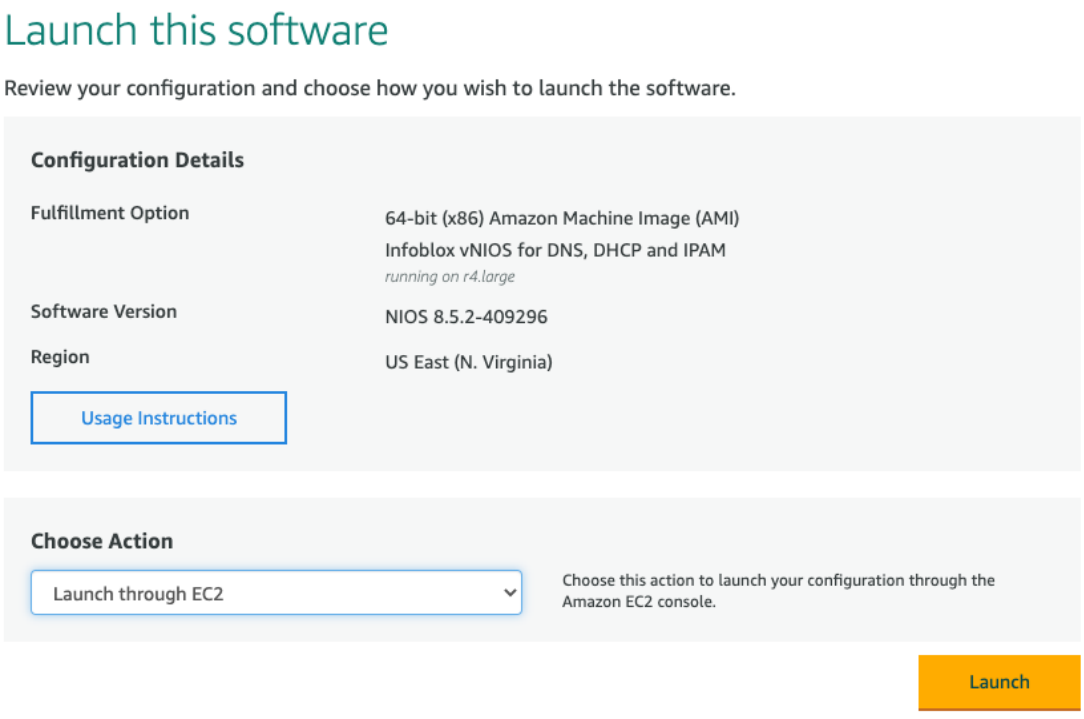


4. Select the **Software Version**.
5. Select your **Region** and click **Continue to Launch**.



6. From the Choose Action dropdown, select **Launch through EC2**.
7. Click **Launch**.

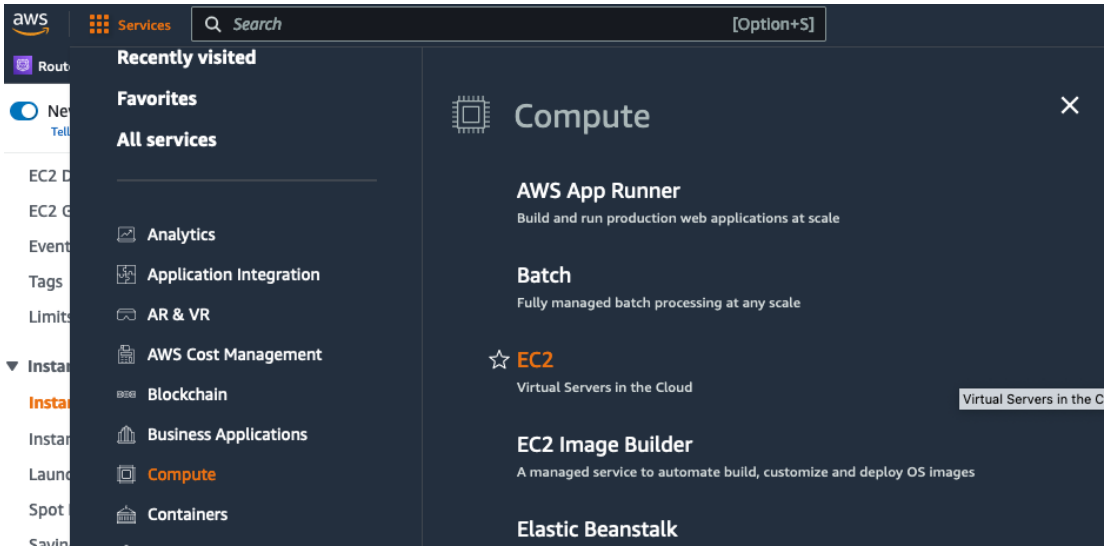
Warning: Do not select the Launch from Website option. This option will launch the instance with a single network interface instead of the required two, and the instance will not function properly.



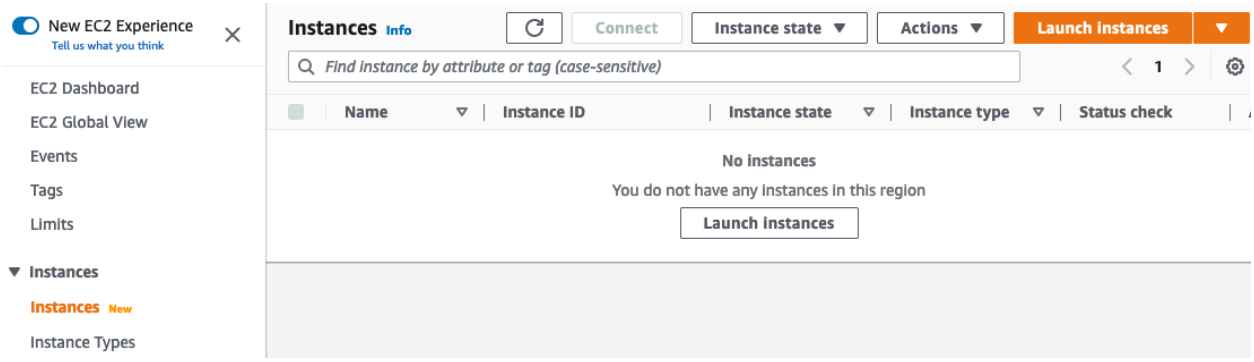
Clicking Launch will bring you to the launch instance wizard in the AWS Console. Continue from the Enter Name and Add Tags section.

Deploy From AWS Console

1. To begin, in the AWS console use the Services dropdown menu to select **EC2** under Compute.



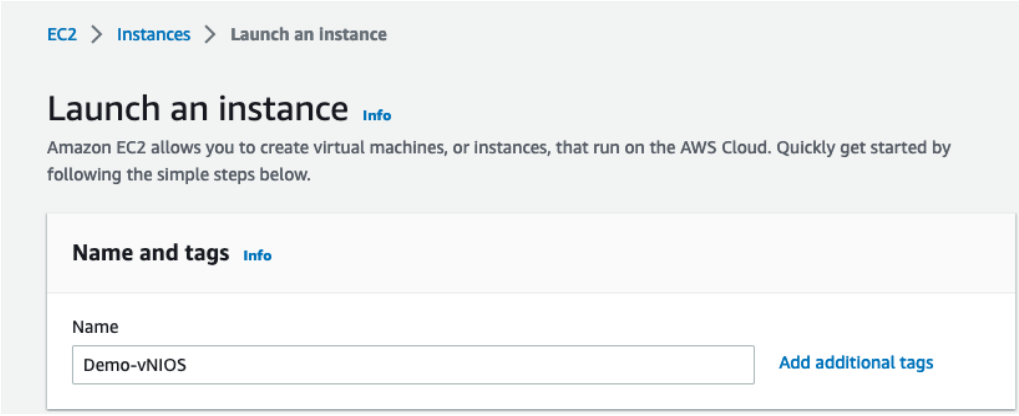
2. Select **Instances** from the EC2 menu.
3. Click the **Launch Instances** button.



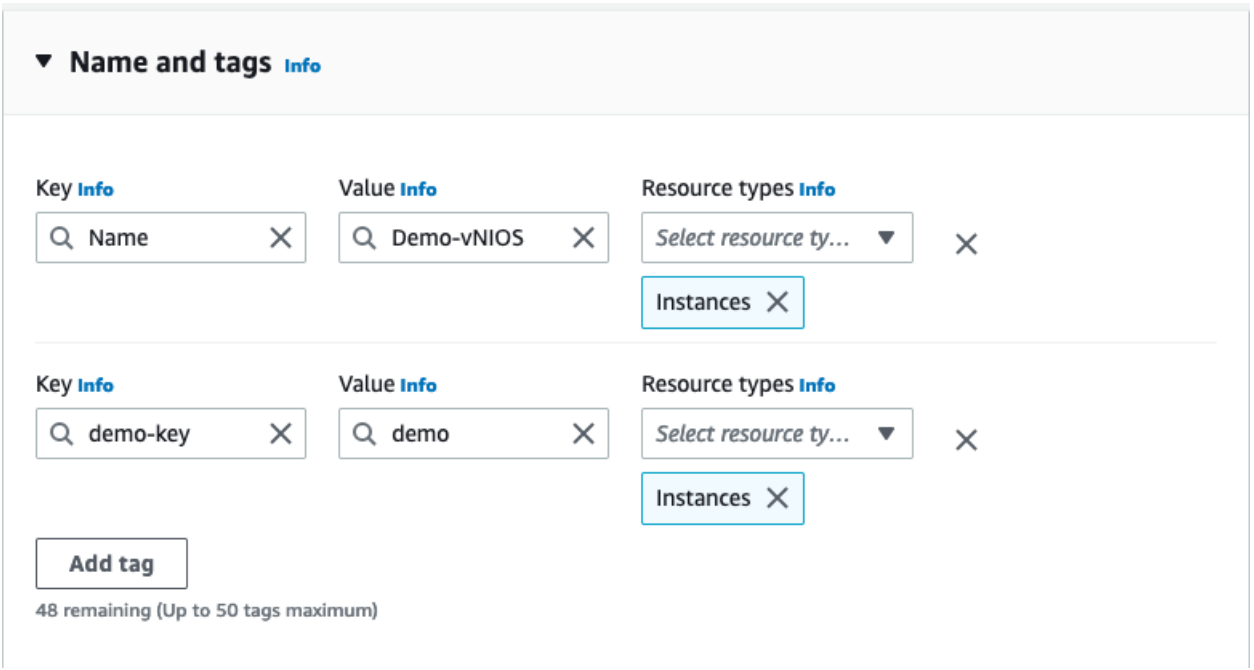
Enter Name and Add Tags

In the first section of the launch instance wizard, provide a name for the instance and optionally add additional tags.

1. Enter a **Name** for the instance.



2. (Optional) Click on **Add additional tags**.
    - Click on **Add tag**.
    - Enter a **Key**.
    - Enter a **Value**.

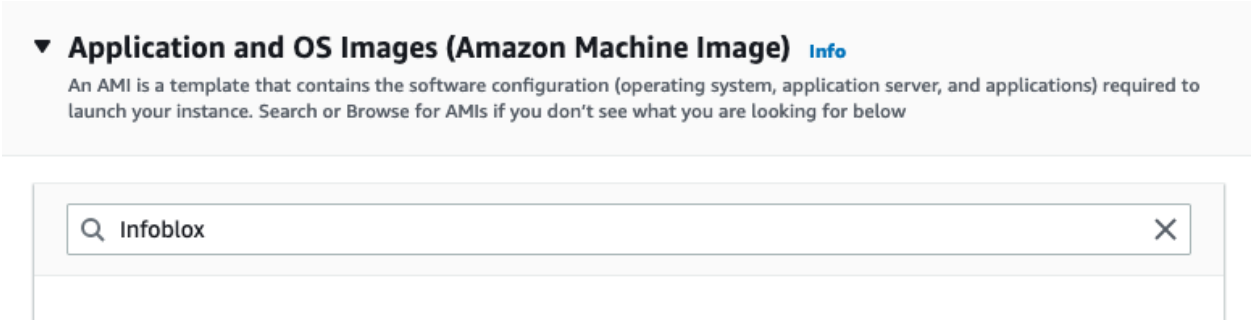


3. Optionally, add additional tags.

Select AMI and Instance Type

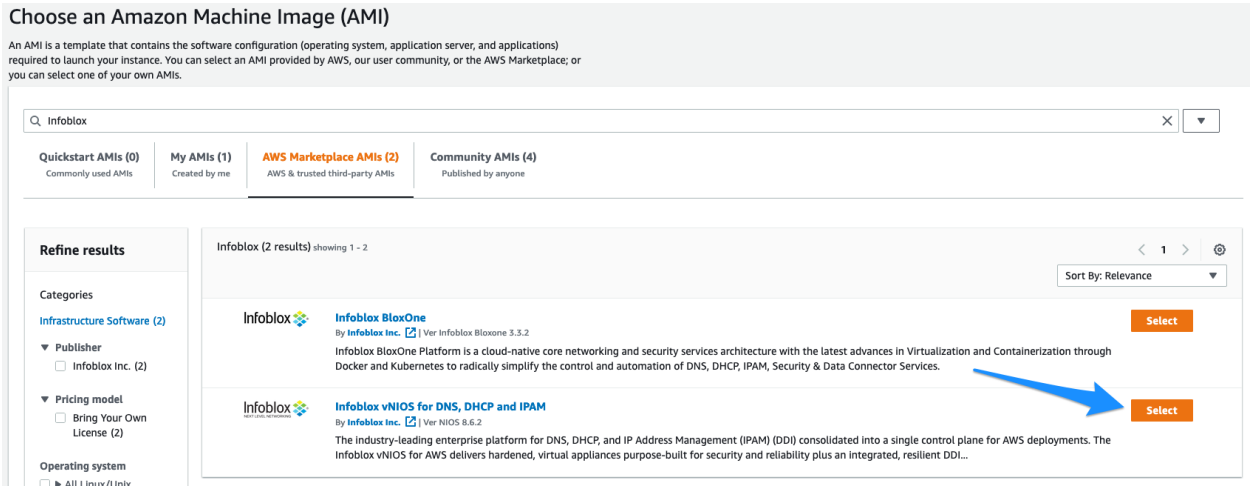
In the next sections of the wizard, select an Amazon Machine Image (AMI) and select an appropriate VM instance size for the appliance. If deploying from the AWS Marketplace, the AMI is already selected; proceed to selecting the instance type.

1. Under Application and OS Images, enter **Infoblox** in the search box and press **Enter.**

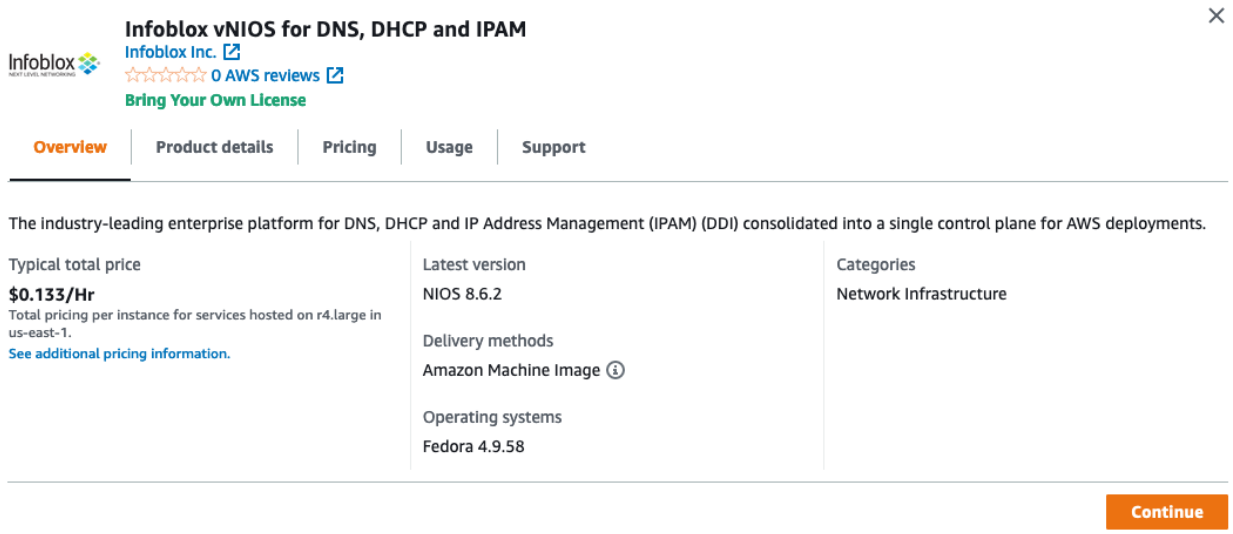


2. Select the **AWS Marketplace AMIs** tab.
3. Click **Select** next to the correct version. This guide uses NIOS version 8.6.2.

Note: Not all versions will be available in all regions. Versions may be added or removed without notice.

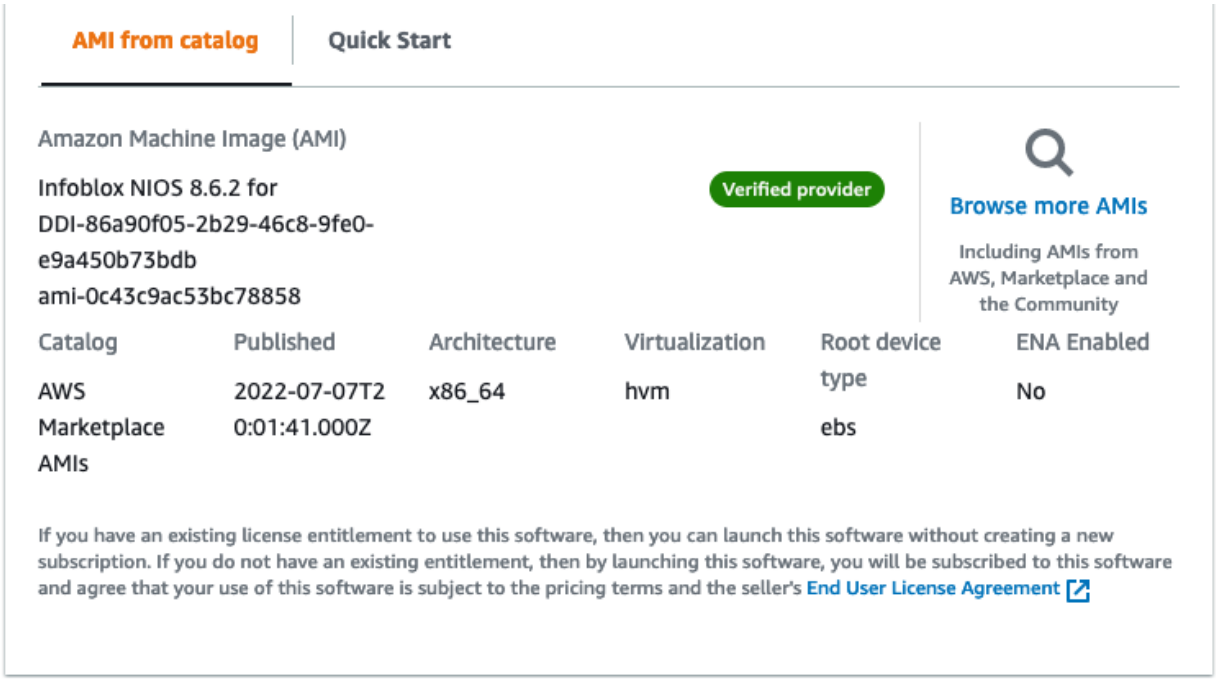


4. Optionally, read through the details.
5. Click **Continue** when ready to proceed.



Instance Type: In this step, we will select a supported instance type for the vNIOS appliance model we are deploying. Not all AWS regions support every instance type. For more information on choosing the right instance type for your vNIOS appliance, refer to Infoblox AWS appliance documentation at: https://docs.infoblox.com/display/NAIG/Infoblox+vNIOS+for+AWS+AMI+Shapes+and+Regions.

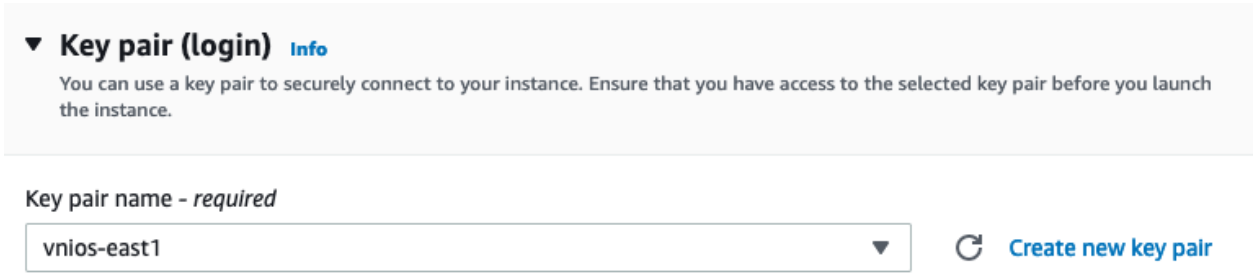
1. Use the Instance type dropdown to select the correct instance type for your vNIOS model. For this guide, we will select **r4.large** for a TE-V825 virtual appliance.



Key Pair

In the next section, we select or create a key pair. Key pair authentication is required for SSH access with vNIOS for AWS version 8.5.2 and newer. If you do not add a key pair on this step, you will need to configure this in Grid Manager.

1. Use the dropdown to select an existing key pair. Or, optionally, create a new key pair.

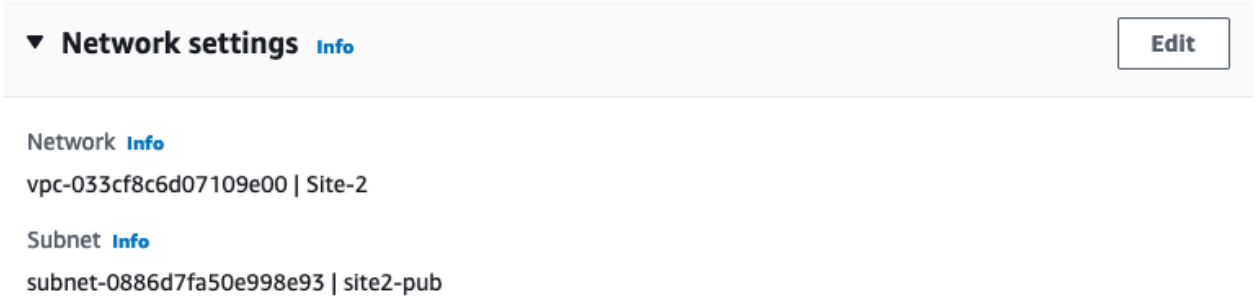


Network Configuration

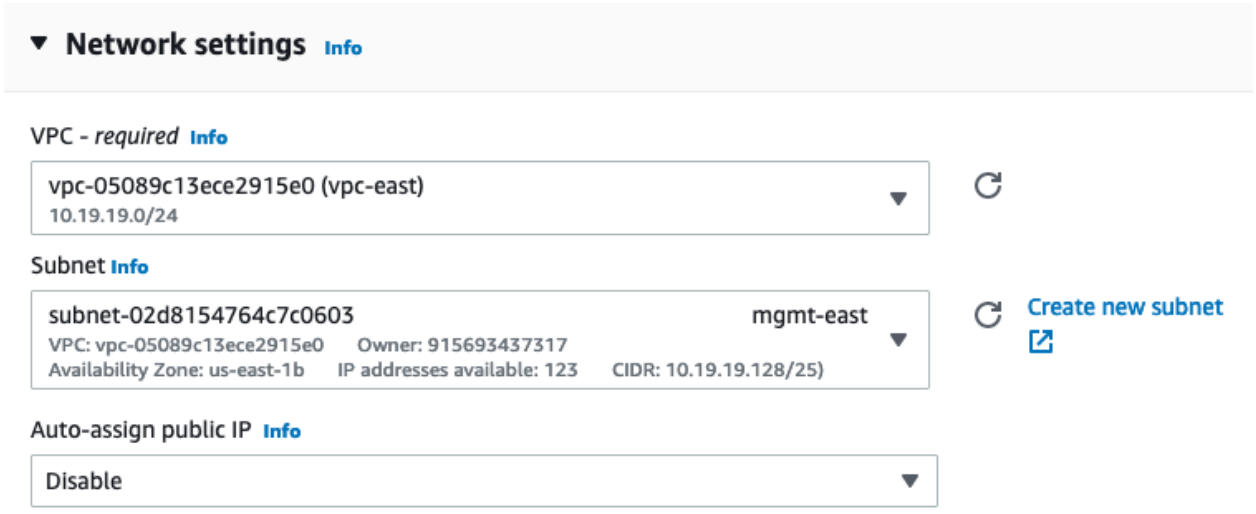
In this section, configure VPC and interface settings as well as a Security Group. Infoblox vNIOS for AWS appliances require two network interfaces. The first AWS network interface, eth0 corresponds to the MGMT interface in NIOS. The second AWS network interface, eth1 corresponds to the LAN1 interface in NIOS.

Warning: Infoblox vNIOS for AWS instances require two virtual network interfaces to deploy successfully, corresponding to the NIOS MGMT(eth0) and LAN1(eth1) interfaces. No additional interfaces are currently supported.

1. In the Network settings section, click on **Edit**.



2. Use the VPC dropdown to select a **VPC**.
3. Use the Subnet dropdown to select a **Subnet** for the eth0 (MGMT) interface.



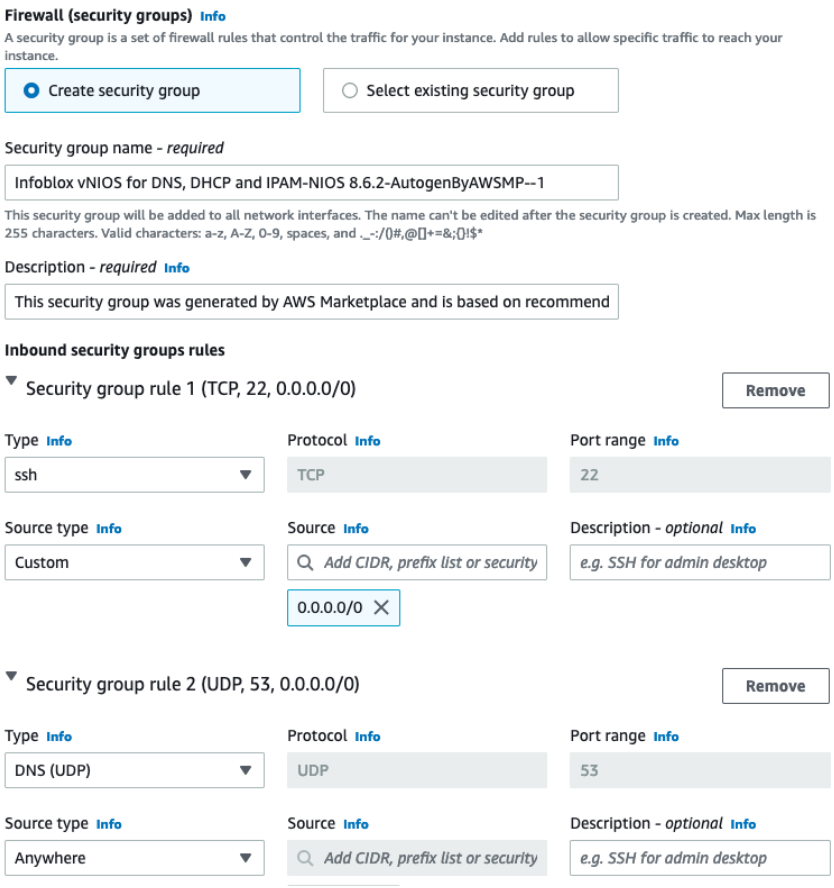
Configure Security Group

Next, we will configure a security group with rules to allow specific traffic to the vNIOS instance. Security groups function as a basic firewall for the instance. By default, the new security group will contain rules to allow common ports and protocols used for NIOS from all IP addresses. While this guide shows allowing traffic from anywhere (0.0.0.0/0) for demonstration purposes, you should restrict

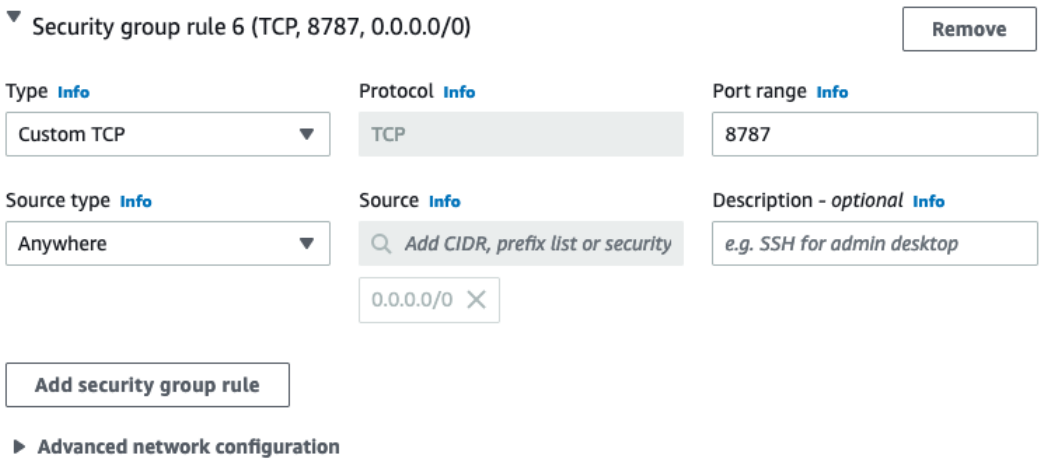
traffic to only necessary source IPs in your environment. The following table lists rules that may be needed for your vNIOS for AWS instance. For further information on ports and protocols used by Infoblox NIOS, refer to https://docs.infoblox.com. Optionally, you can select an existing security group to use instead.

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
Custom TCP Rule	TCP	8787	Infoblox AWS API Proxy

1. (Optional) To change the allowed source for any of the default security group rules, use the Source type dropdown to select **Custom**.
2. (Optional) Under Source, enter the **CIDR block** to allow traffic from, or select a prefix list or security group from the dropdown.
3. (Optional) To remove any of the default security group rules that are not needed, click on **Remove**.



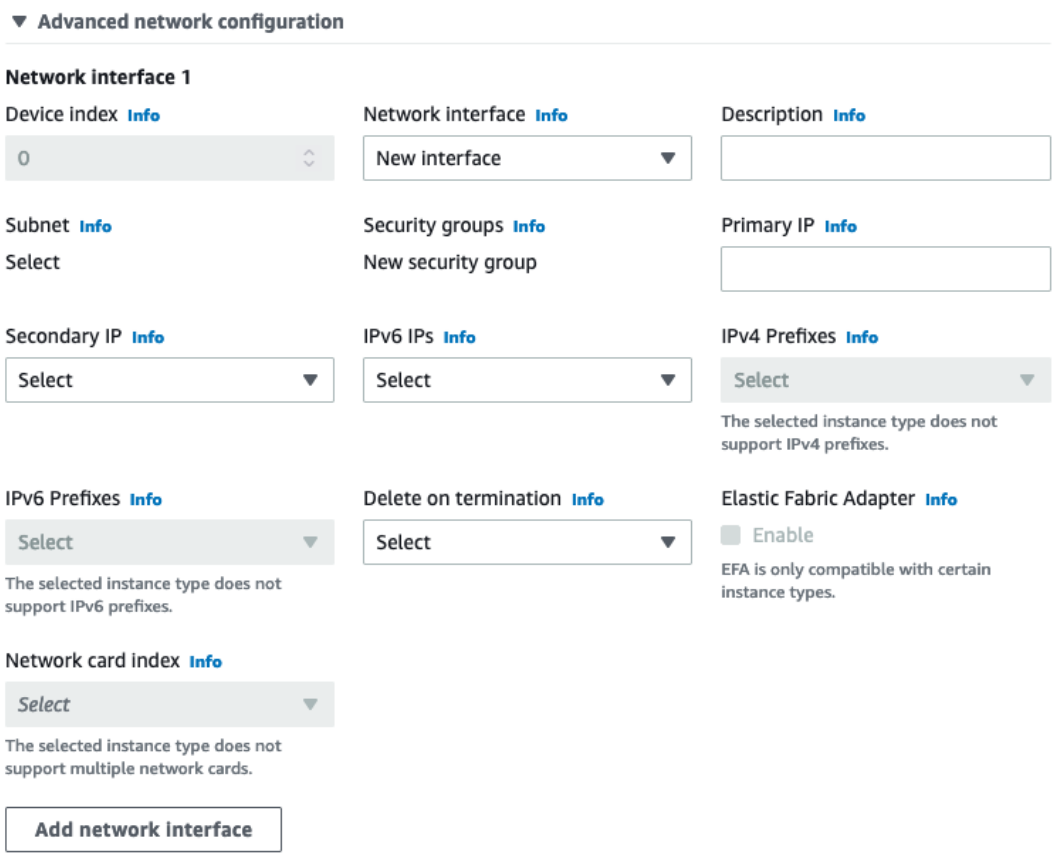
4. (Optional) To add additional security group rules, click on **Add security group rule**.



Add Network Interface

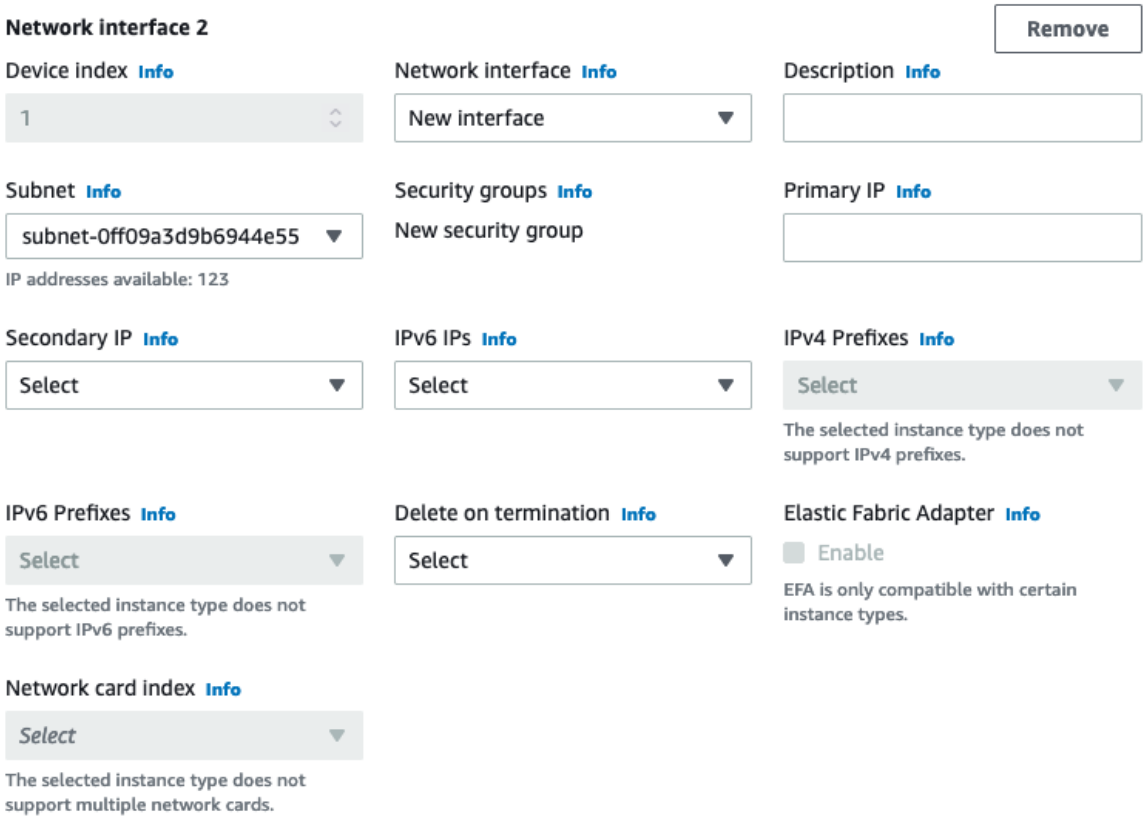
In this section, we add the second network interface (eth1/LAN1). This interface is required for vNIOS deployment in AWS.

1. Expand the **Advanced network configuration** section.
2. Scroll down to click on **Add network interface**.



3. Under Network Interface 2, use the Subnet dropdown to select a **Subnet** for the eth1 (LAN1) interface. This should be a different subnet from eth0 in the same availability zone.

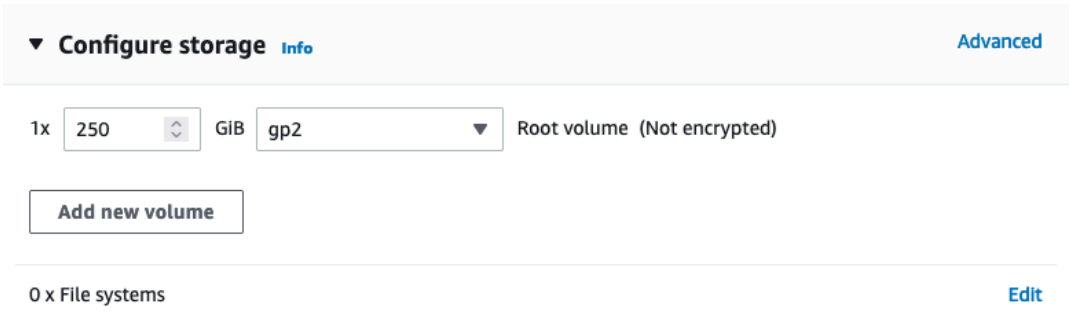
Note: By default, this interface and subnet will be used for all connections to and services provided by your vNIOS for AWS instance.



Configure Storage

AWS instance disks are stored as Elastic Block Store (EBS) volumes. There are multiple EBS types that can be selected for your boot disk. General Purpose SSD is the base level for SSD and will work for most vNIOS deployments. Provisioned IOPS SSD supports high levels of input and output and may be useful for high read/write volume environments. Magnetic (standard) EBS is not recommended for vNIOS deployments except in non-production environments.

1. Verify Size is set to **250** (this should be the default).
2. Select the Root volume type: **gp2**.

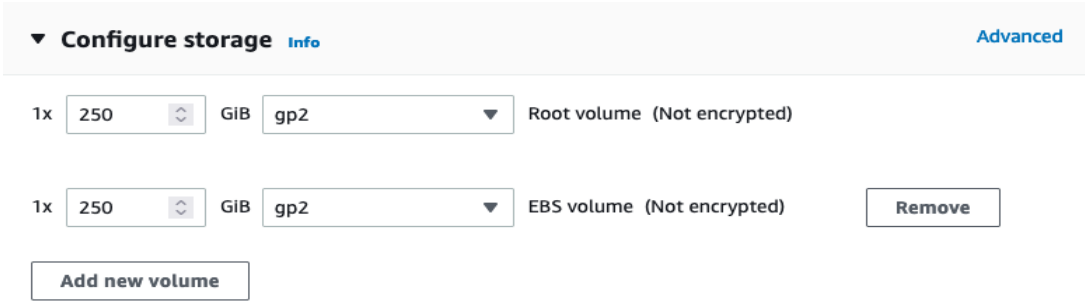


Additional Storage

Infoblox reporting appliances require an additional storage volume. For the TR-V5005 appliance, size of this volume can be selected based on requirements for your Grid. Infoblox recommends a minimum of 250 GiB.

Note: This additional storage is for reporting appliances only. Skip this step for other appliance types.

1. Click **Add new volume**.
2. Set the volume **Size** as needed. Minimum of 250 GiB.
3. Select the EBS volume type: **gp2**.

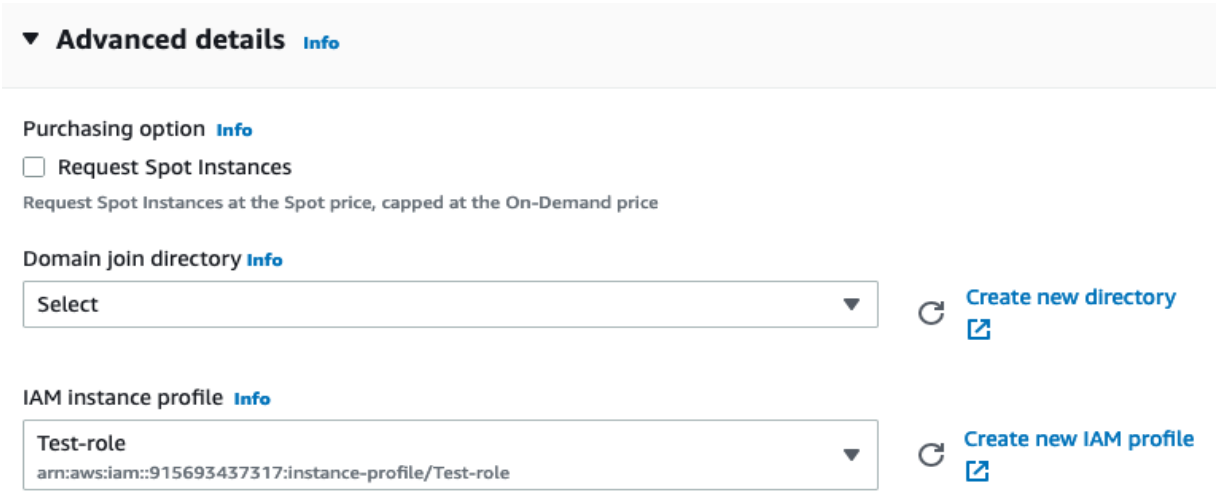


Configure Advanced Details

In the advanced details section, you can add an IAM instance profile to use for Infoblox vDiscovery and Route 53 Sync. Refer to the vDiscovery credentials section of this guide for details. You can also add user data for some initial configuration of NIOS. Configurations in this section are optional in vNIOS for AWS deployment.

IAM Instance Profile (Optional): An instance profile with appropriate permissions can be used for vDiscovery and Route 53 Sync in vNIOS for AWS.

1. Expand the Advanced details section.
2. (Optional) Use the IAM instance profile dropdown to select an **IAM Role** to use.



User Data (Optional): You can use the User Data field in AWS instance deployment for some initial configuration of your Infoblox vNIOS appliance's operating system. For vNIOS, the user data field can pass cloud-init directives, an open-source package used for initial configuration. You can specify settings such as administrator password and allowing SSH access. This section will cover a common configuration for a standalone appliance.

1. Scroll down in the Advanced details section.
2. Use the Metadata version dropdown to select **V1 and V2 (token optional)**.
3. Enter the following in the User data text box:

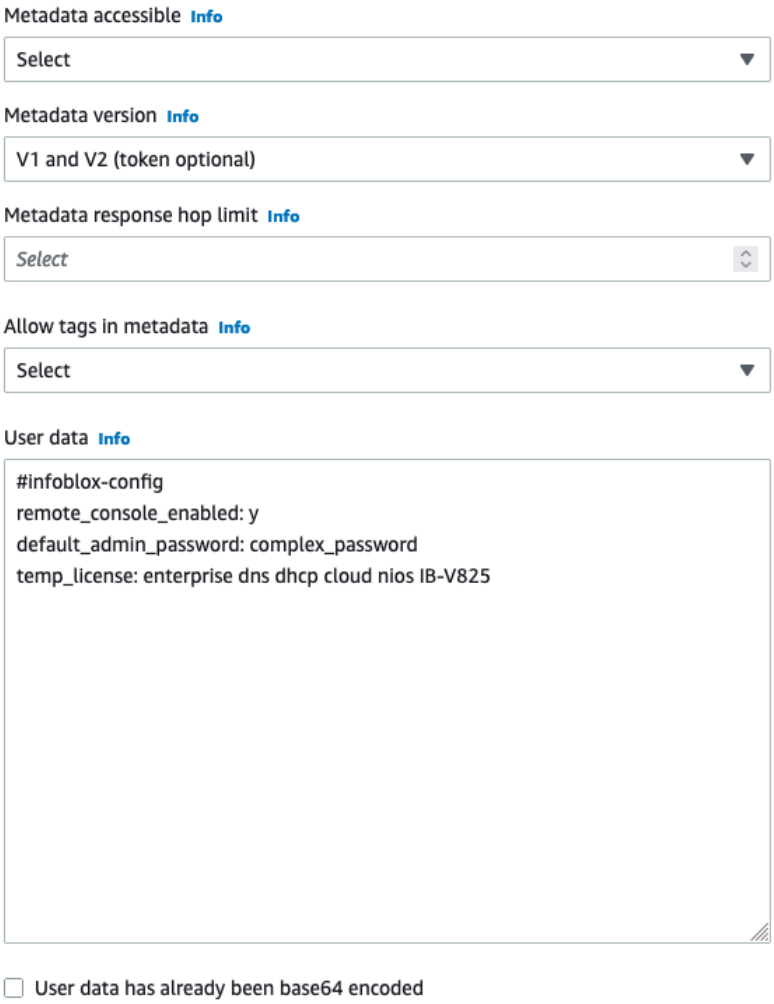
   #infoblox-config

   remote_console_enabled: y

   default_admin_password: *complex_password*

   temp_license: enterprise dns dhcp cloud nios IB-V825

This will enable SSH connection to the instance, set an admin password, and apply temporary licenses for the Grid, DNS, DHCP, CNA, and NIOS model TE-V825 virtual appliance.



Temporary Licenses: To include temporary licenses in user data, use the t**emp_license: <licenses>** entry. All licenses should be listed with a single space between them. For example:

#infoblox-config

temp_license: enterprise dns dhcp cloud nios IB-V825

The following temporary licenses can be used with the latest versions of vNIOS for AWS:

- On any vNIOS for AWS instance: **enterprise dns dhcp rpz cloud vnios**
- **nios** should always be followed by the model. For TE appliances, supported licenses are: **IB-V825 IB-V1425 IB-V2225, IB-V4015, IB-V4025**. For CP appliances, supported licenses are: **CP-V805 CP-V1405 CP-V2205**. For reporting appliances, the **IB-V5005** is supported.
- For a CP appliance, the **cloud_api** license is also required. For example:

  #infoblox-config

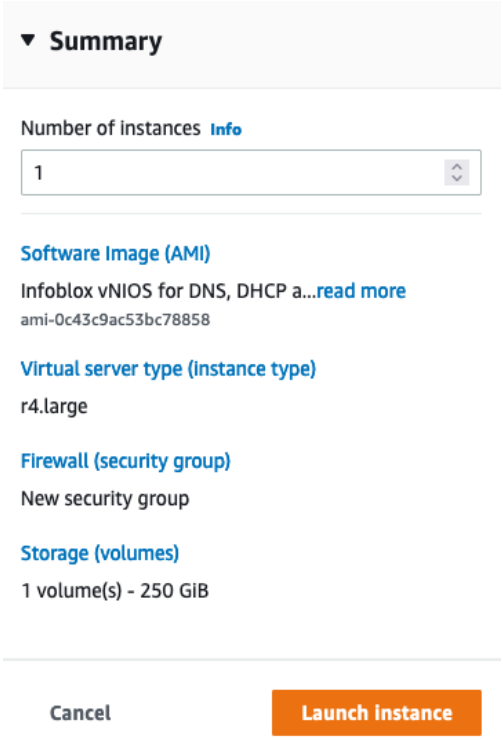
  temp_license: enterprise dns dhcp cloud_api nios CP-V805

For additional information and use cases regarding user data, refer to NIOS documentation at https://docs.infoblox.com.

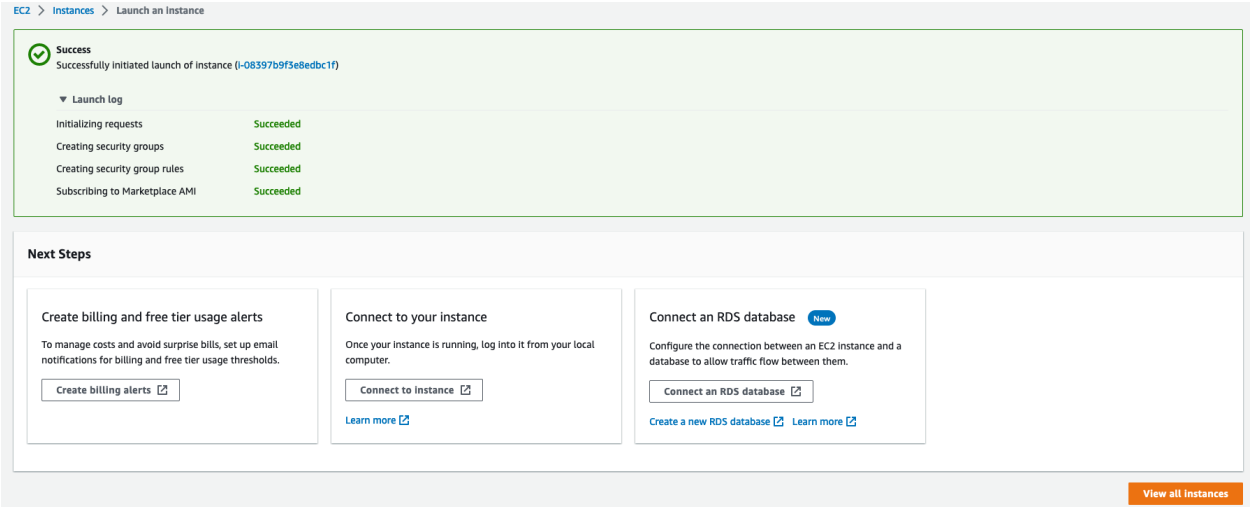
Launch Instance

Once all configuration is complete, review details and launch the instance.

1. Click **Launch instance**.

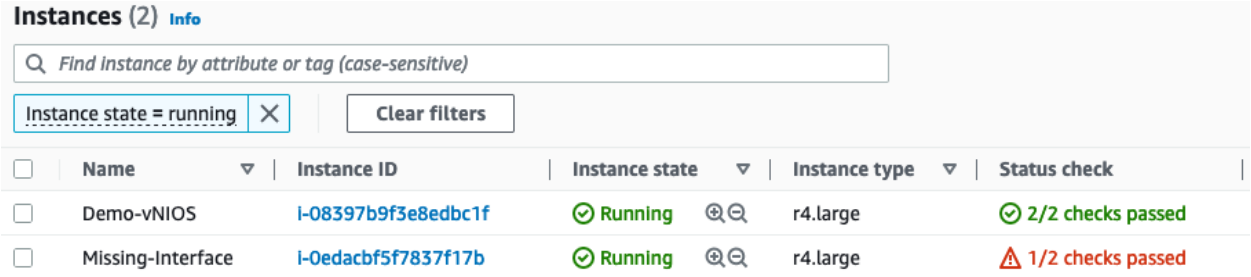


2. On the Launch Status page, you can view status logs and click **View all instances** to return to the Instances page and view your new vNIOS instance.

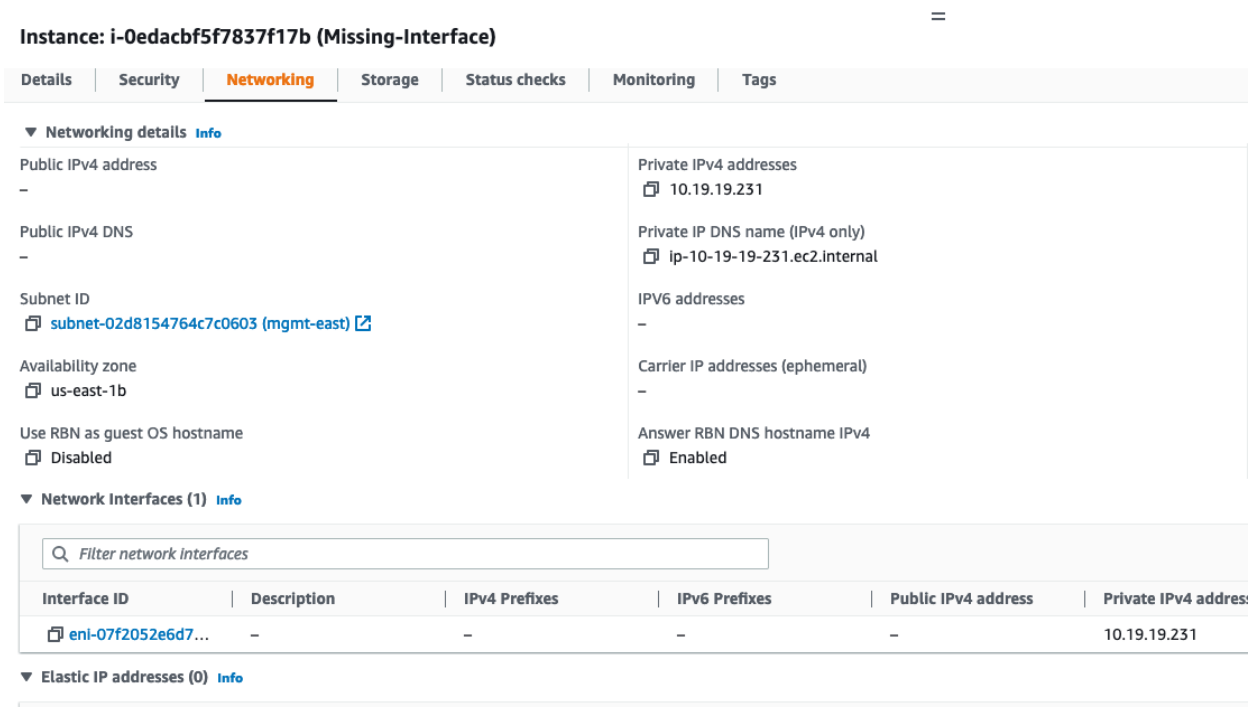


Troubleshooting

Deploying and configuring your Infoblox vNIOS for AWS instances is generally a straightforward process. One of the most common issues encountered while deploying a vNIOS for AWS instance is not adding the required second network interface. This issue can be identified when the instance Status Check is stuck at **1/2 checks passed**.



Verify that a missing interface is the issue by selecting the instance and reviewing the Networking tab.



The Networking tab in the screenshot shows only the single eth0 interface in the Network interfaces section.

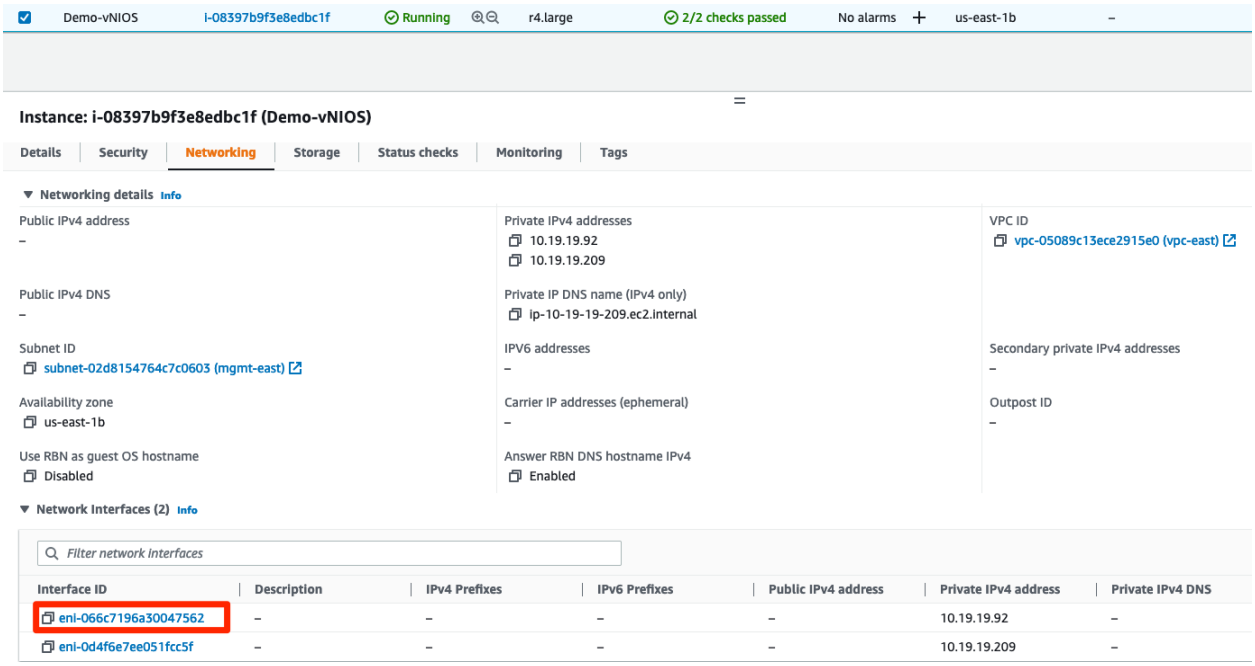
To resolve this issue:

1. Create a new network interface in the same VPC as your instance..
2. Attach the network interface to your instance.
3. Restart your Infoblox vNIOS for AWS instance.

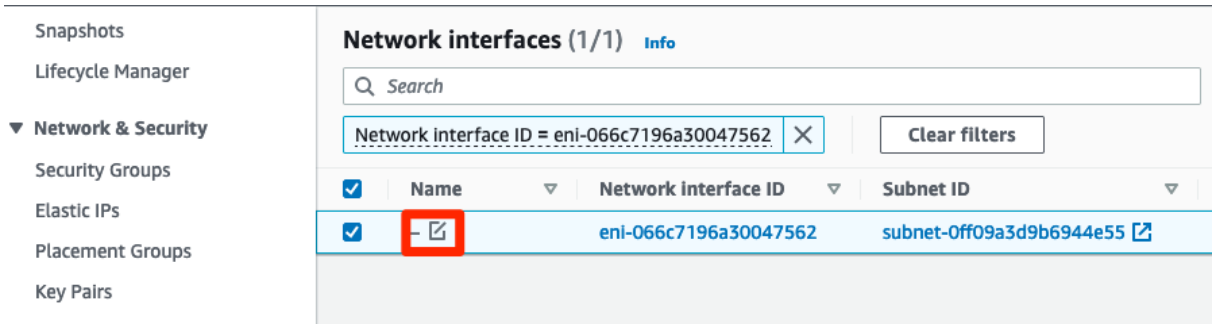
Add a Public IP to vNIOS Instance (Optional)

In this step, we will attach a public IP to the vNIOS for AWS instance in order to connect to it. This is an optional step and not necessary if you are able to connect to your AWS VPC via VPN, Direct Connect, or jumpbox. First, we will give the eth1 (LAN1) interface a custom name to make it easier to recognize.

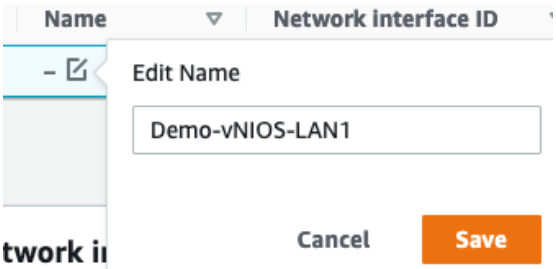
1. On the Instances page, select your instance.
2. On the Networking tab, locate the LAN1 Interface, and click on the **Interface ID**.



3. On the Network Interface page, select the LAN1 interface.
4. Under the Name column, click the Edit icon.

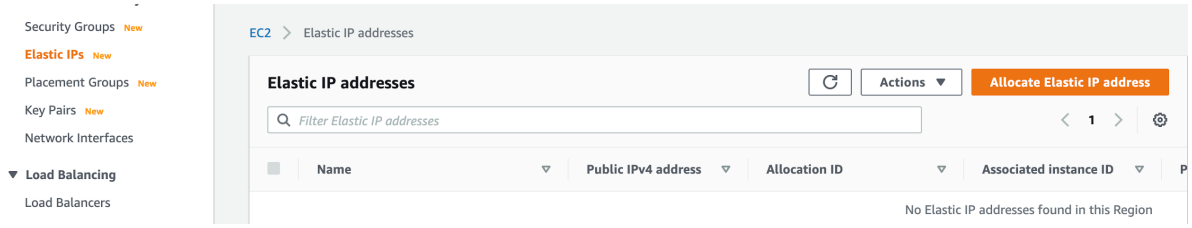


5. Enter a name for the interface and click Save.

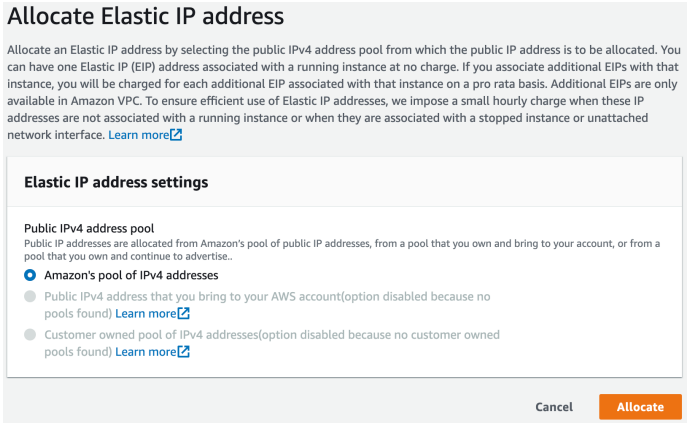


Allocate Elastic IP

1. Select **Elastic IPs** from the EC2 side menu.
2. Click **Allocate Elastic IP address**.

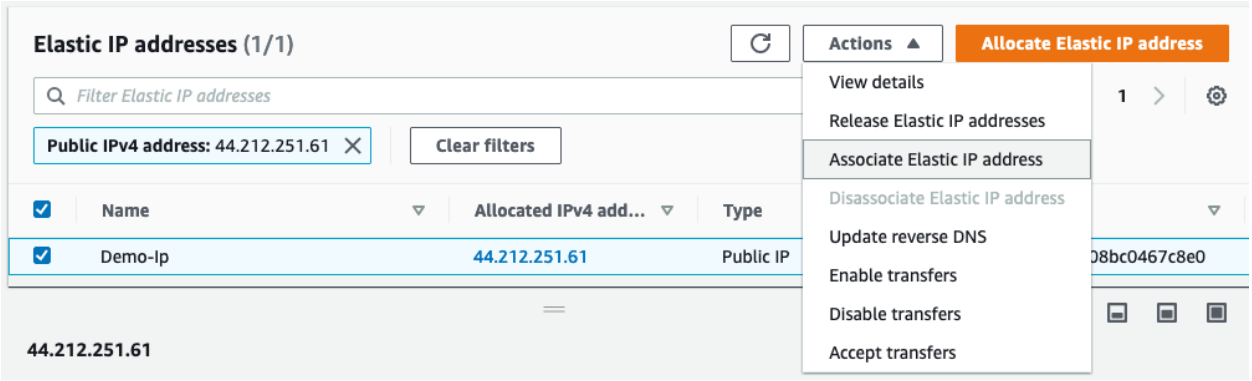


3. Leave Amazon's pool of IPv4 addresses selected.
4. Click Allocate.

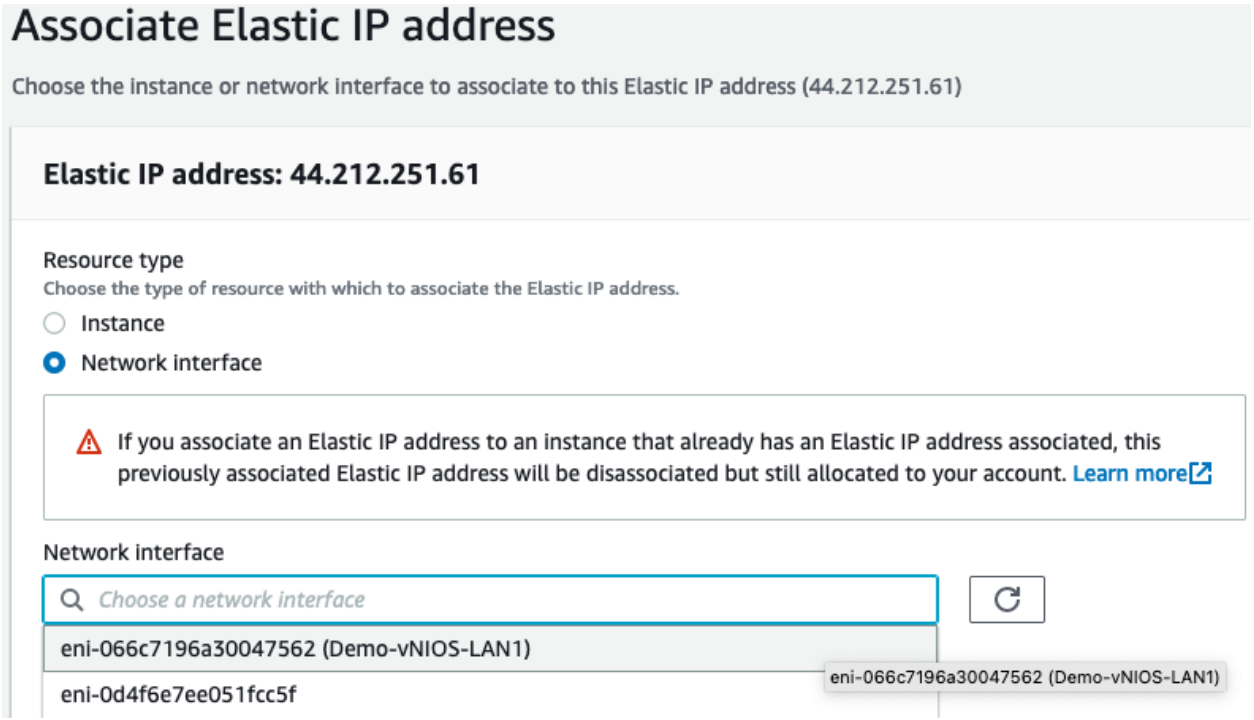


Attach Elastic IP to vNIOS Instance

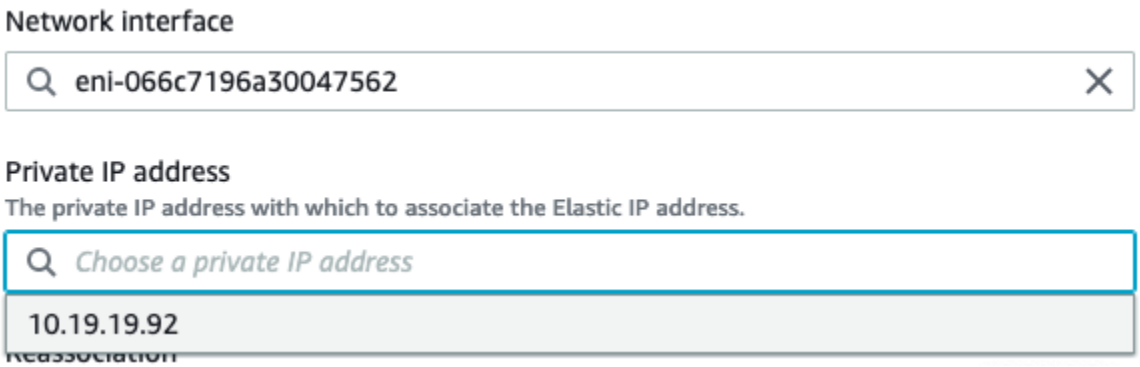
1. To attach the Elastic IP to your vNIOS instance, select the checkbox for the IP.
2. Use the Actions menu to select **Associate Elastic IP address** from the dropdown.



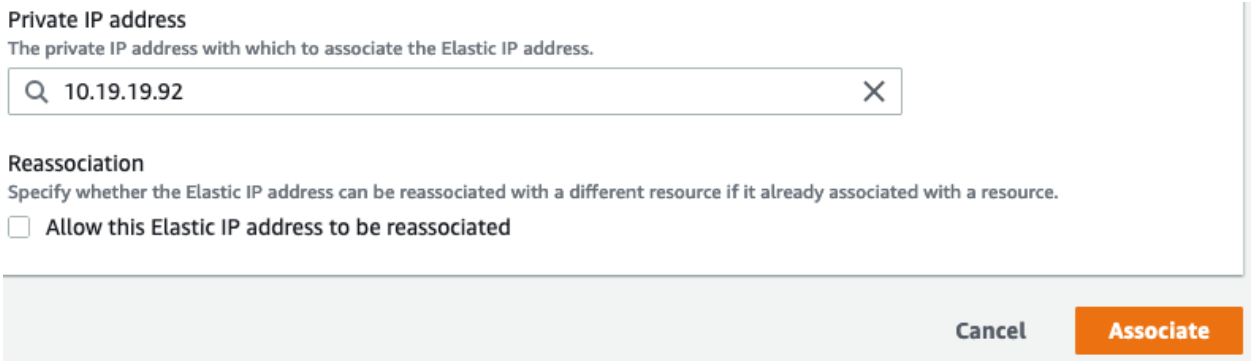
3. Under Resource type, select **Network interface**.
4. Click in the box under Network interface and select the vNIOS instance LAN1 interface from the list.



5. Click in the box under Private IP address and select the interface private IP.



6. Click **Associate**.



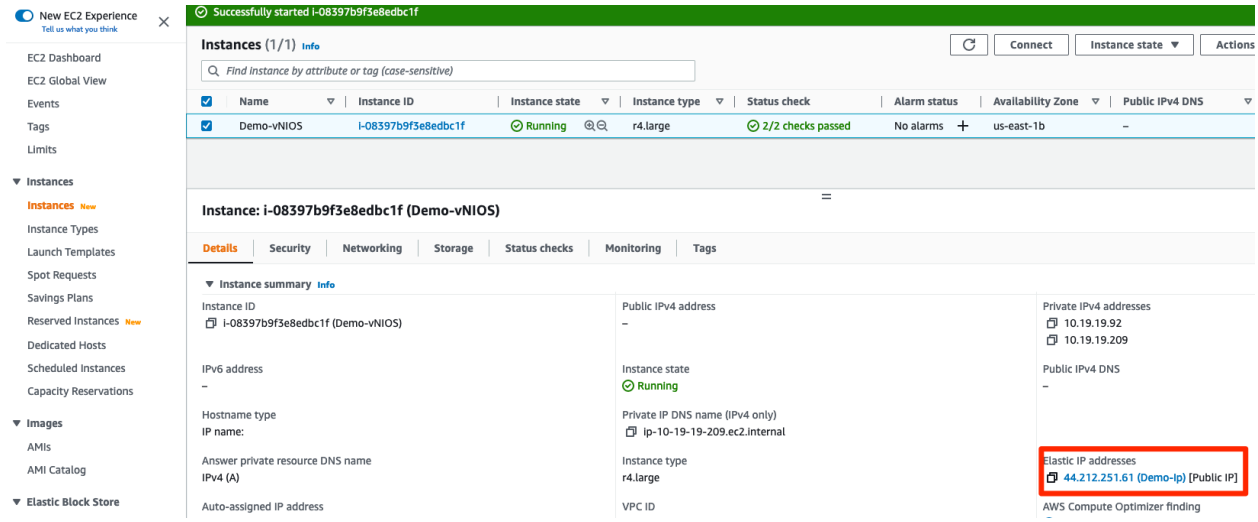
Configuration

Once the Infoblox vNIOS for AWS deployment is complete, the new virtual appliance can be joined to an existing Grid or configured as a Grid Master for a new Grid. This section provides basic guidance for common configuration of vNIOS for AWS appliances.

Connect to vNIOS Instance

There are two methods available by default to connect to your vNIOS for AWS instance, using SSH and the Grid Manager GUI. To connect via either method, 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 Direct Connect, however that is outside the scope of this guide.

1. To find the public IP address of your vNIOS instance, Navigate to the EC2 Instances page.
2. Select your vNIOS instance.
3. On the Details tab, locate the Elastic IP Address.
4. Click the copy symbol to copy this IP address to your clipboard.



SSH

1. Open a PowerShell or Terminal window on your computer.
2. Enter the command ssh admin@<ip_address> to start the SSH connection (use the public IP address of your vNIOS instance).

Note: For vNIOS version 8.5.2 and newer, you will need to add the -i option to your SSH command and specify your private key.

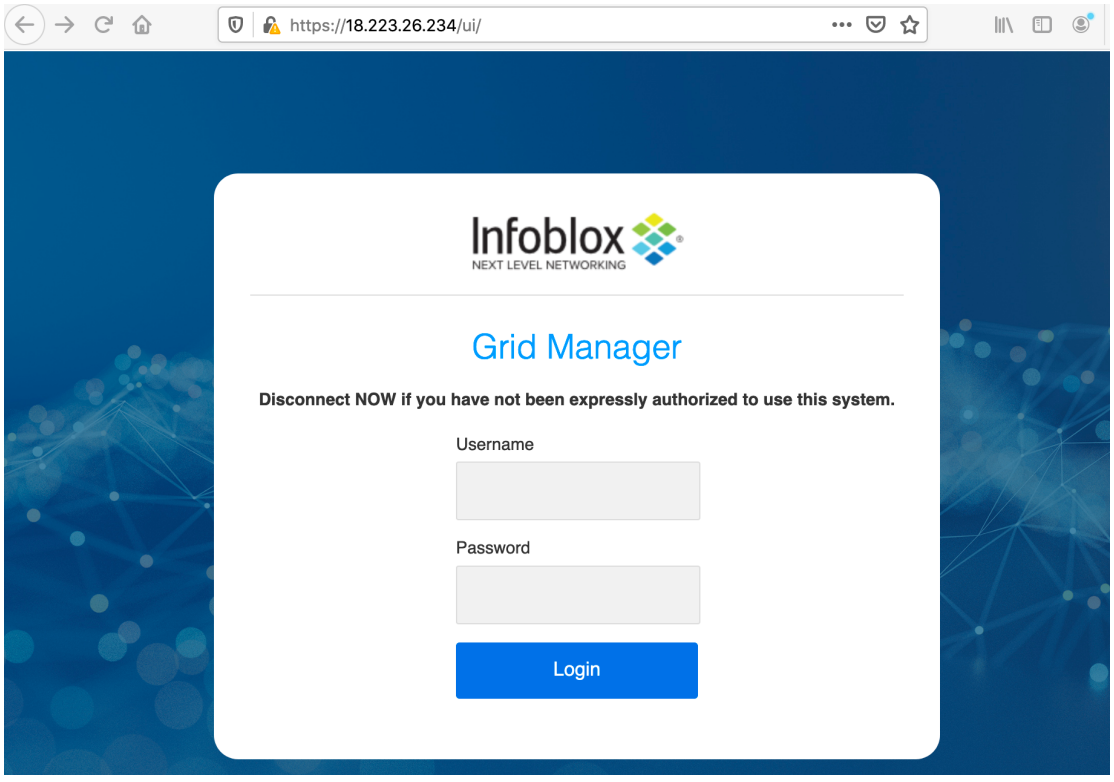
3. When prompted, type yes to add the IP address to your known_hosts file.
4. If you are not using key-pair authentication, enter the password you set in User-Data.

```
[redacted] ~ % ssh -i ~/.ssh/uswest1-aws.pem admin@[redacted]
The authenticity of host '[redacted] ([redacted])' can't be established.
RSA key fingerprint is SHA256:WIqfwUShP/PSLT07h0zBsPEkLrX9BLUGocGAKrXbEmg.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[redacted]' (RSA) to the list of known hosts.


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


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

                  type 'help' for more information


Infoblox >
```

5. Once the SSH session is established, you can interact with the NIOS command line interface (CLI). Refer to NIOS documentation at https://docs.infoblox.com for details on CLI commands and use.

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.

Note: NIOS 8.5.2 and later require you to change the admin password on your first login to the vNIOS for AWS instance.

4. Accept the Infoblox End-User License Agreement.
5. Read and make a selection for the Infoblox Customer Experience Improvement Program.

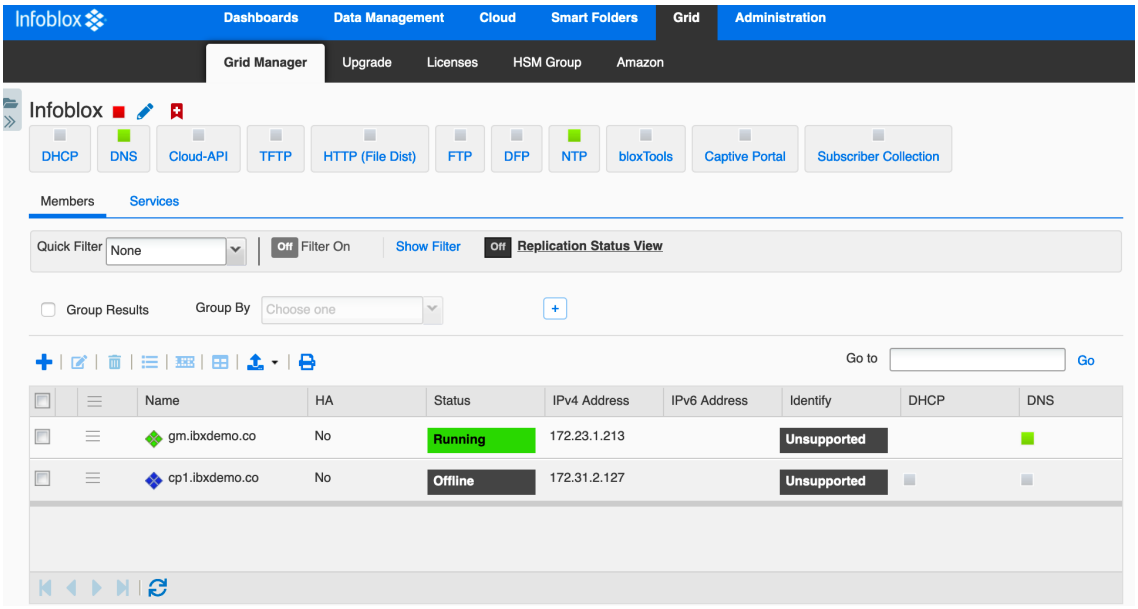
Join vNIOS to Existing Grid

Infoblox vNIOS for AWS instances can be joined to existing Grids running on-premises, in AWS, or across multiple cloud platforms. The vNIOS for AWS instance must be able to communicate with the Grid Master using either private or public IP addressing. At a minimum, communication must be open over UDP ports 1194 and 2114.

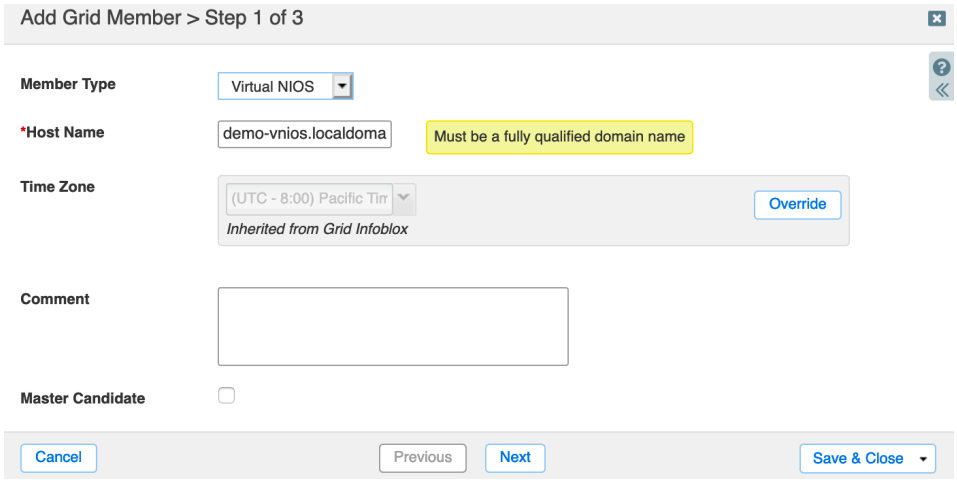
Add New Infoblox Appliance to Grid

Prior to joining a new member to an existing Grid, the member needs to be added (defined) in the Grid. This can be done using the Grid Manager GUI or using the Infoblox API. This guide will demonstrate using the Grid Manager to add a new member.

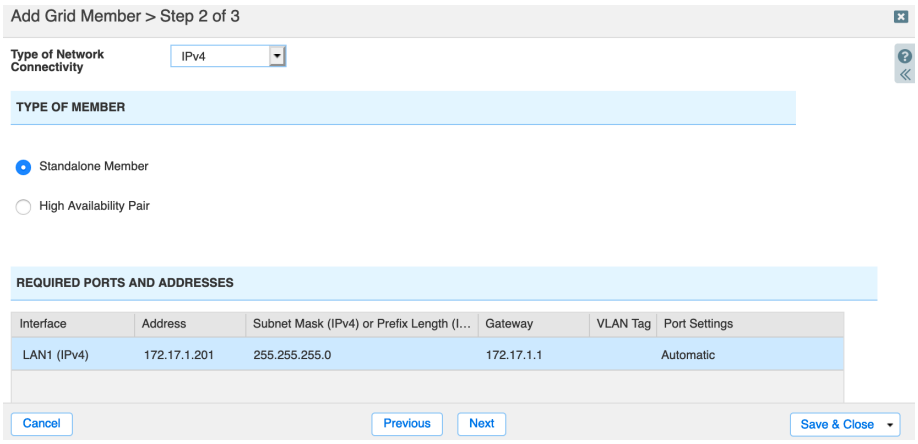
1. Login to the Grid Manager GUI of your existing Grid.
2. Navigate to the **Grid** → **Grid Manager** → **Members** tab.
3. Click the + (add button) to add a new Grid member.



4. In Step 1 of the Add Grid Member wizard, for Member Type, select **Virtual NIOS** from the dropdown.
5. Enter a Host Name for the new member.
6. Click **Next**.

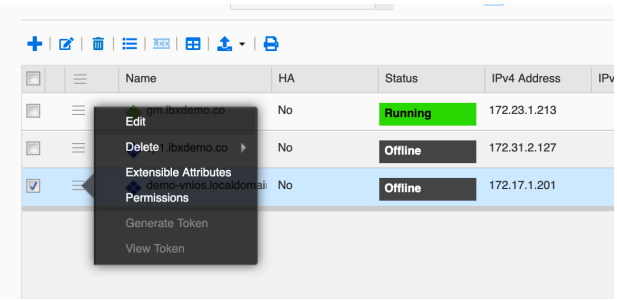


7. On Step 2, Select **Standalone Member**. *Note: vNIOS for AWS instances are not supported for use in High Availability pairs.*
8. For the LAN1 interface, enter the private IP address of your vNIOS for AWS instance eth1 interface.
9. Enter the Subnet Mask.
10. Enter the Gateway address for your VPC subnet. Note: by default, AWS assigns the gateway the .1 IP address in a subnet.
11. Click **Save & Close**.

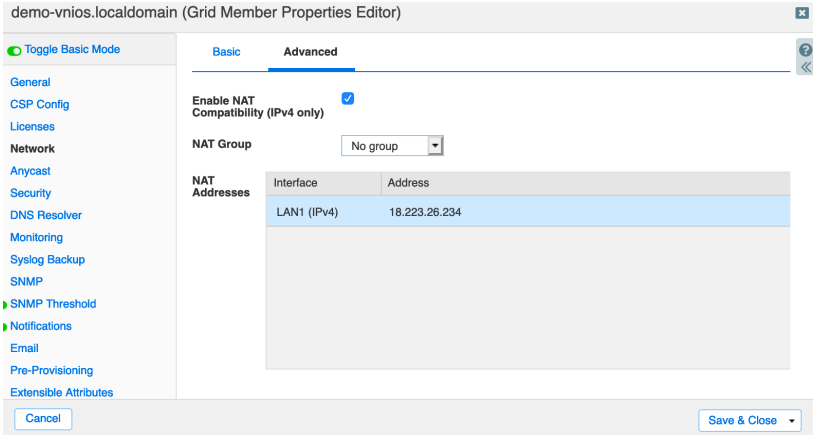


Adding Grid Member Public IP: Complete these steps only if your vNIOS for AWS instance will communicate with the Grid Master using public IP addressing. If you are using VPN or other methods for private IP address communication, skip to the next section.

1. Click the action menu next to your new Grid member. Select Edit.



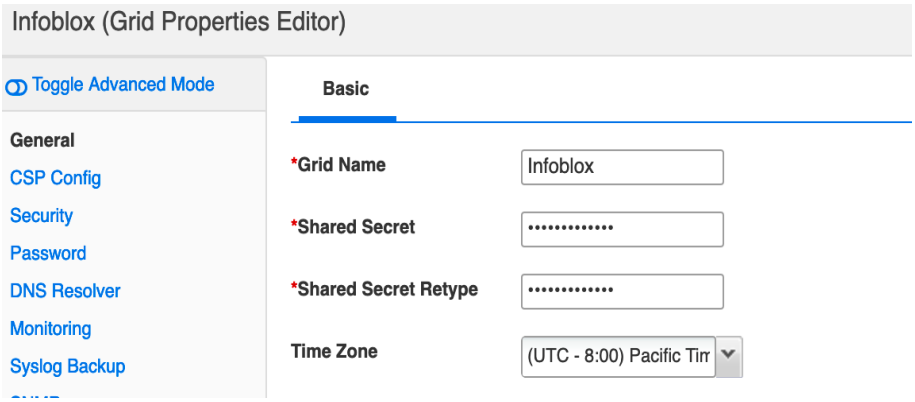
2. In the Grid Member Properties Editor, navigate to the **Network** → **Advanced** tab.
3. Scroll down and select **Enable NAT**.
4. Ensure **No group** is selected for NAT Group.
5. Enter the public IP address of your instance for LAN1 in NAT Addresses.
6. Click Save & Close.



For additional information on configuring network address translation (NAT) and NAT groups in your Grid, refer to NIOS documentation at https://docs.infoblox.com.

Join Appliance to Grid

An Infoblox vNIOS for AWS instance can be joined to the grid using the CLI or the Grid Manager GUI. To join a Grid, you will need to know the Grid Master's IP address, the name of the Grid, and the Shared Secret used to authenticate the connection. In the Grid Manager, navigate to the **Grid** → **Grid Manager** → **Members** tab and click **Grid Properties** in the menu to review or change Grid name and Shared Secret.



Note: The Shared Secret is encrypted once it is saved. There is no recovery mechanism if it is lost. The value can be changed without any impact to any appliances online in your Grid. Any offline Grid members will need to be reset before being joined back to the Grid after any change is made to the Shared Secret. The default Shared Secret is "test".

Join Using CLI

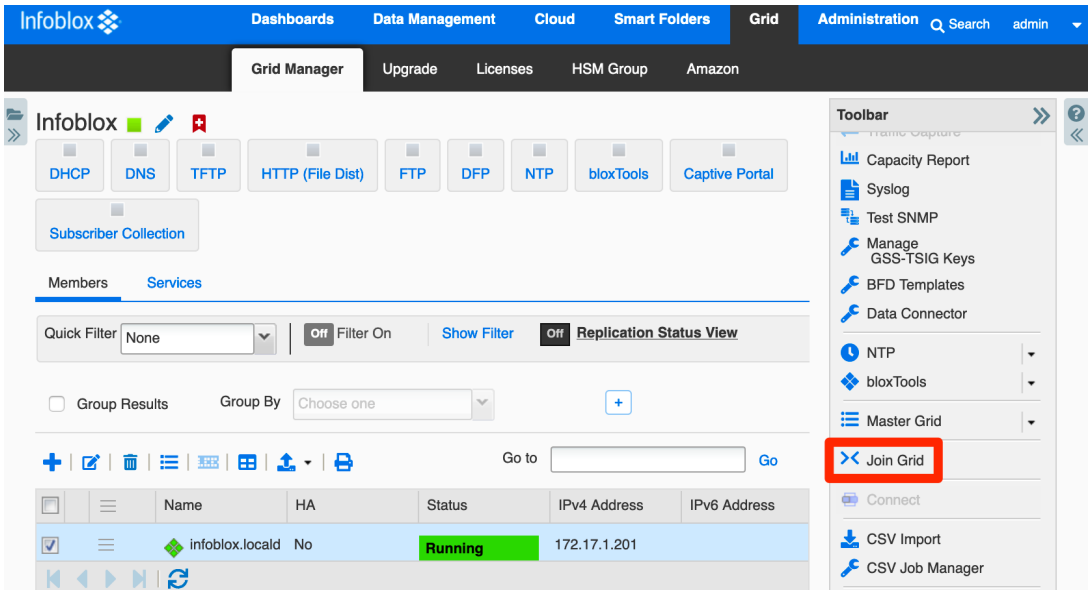
1. Login to your vNIOS for AWS instance using an SSH client.
2. Type the command **set membership** and press **Enter**.
3. Enter the IP address of the Grid Master when prompted. Press **Enter**.
4. Enter the Grid name when prompted if it is different from the default (Infoblox). Press **Enter**.
5. Enter the Shared Secret when prompted. Press **Enter**.
6. Verify that the join details are correct and enter **y** at confirmation prompts to begin the join process.

```
              Infoblox NIOS Release 8.5.0-394706 (64bit)
     Copyright (c) 1999-2020 Infoblox Inc. All Rights Reserved.

                    type 'help' for more information


Infoblox > set membership
Join status: No previous attempt to join a grid.
 Enter New Grid Master VIP: 172.23.1.213
Enter Grid Name [Default Infoblox]: Infoblox
Enter Grid Shared Secret: test
  Join grid as member with attributes:
     Grid Master VIP:     172.23.1.213
     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
        Are you sure? (y or n): y
```

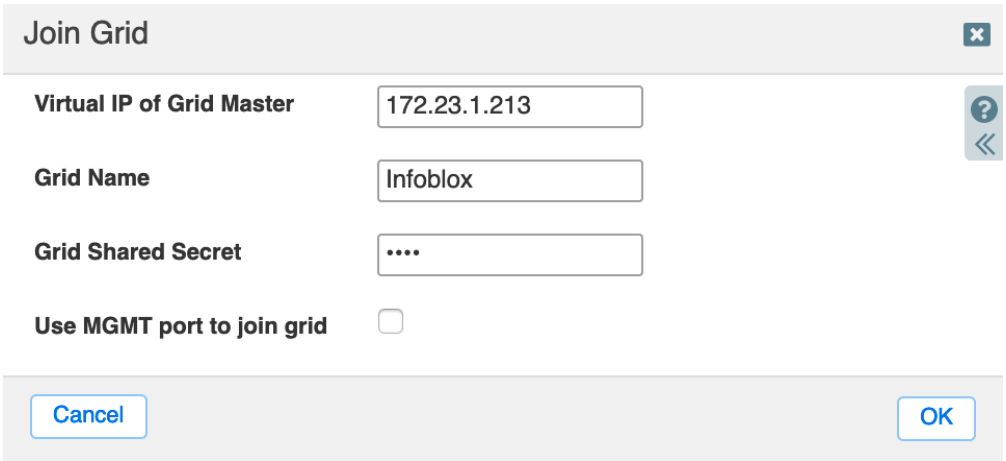
7. Your vNIOS for AWS instance will restart and the SSH session will be closed. Monitor the join process from the Grid Manager on the **Grid → Grid Manager → Members** tab.

Join Using Grid Manager GUI

1. Login to your vNIOS for AWS instance Grid Manager GUI.
2. If the Grid Setup Wizard is displayed, click **Cancel**.
3. Navigate to the **Grid** → **Grid Manager** → **Members** tab.
4. In the vertical toolbar on the right-hand side of the page, click **Join Grid**.



5. Enter the IP address of the Grid Master.
6. Enter the Grid Name and Grid Shared Secret.
7. Click **OK**.

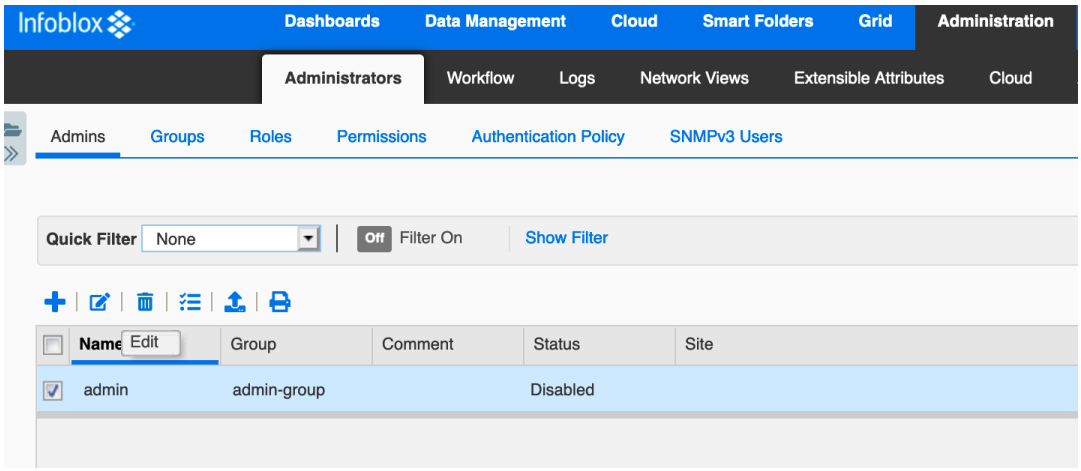


8. Your vNIOS for AWS instance will restart and the GUI session will be closed. Monitor the join process from the Grid Manager of your existing Grid on the **Grid** → **Grid Manager** → **Members** tab.

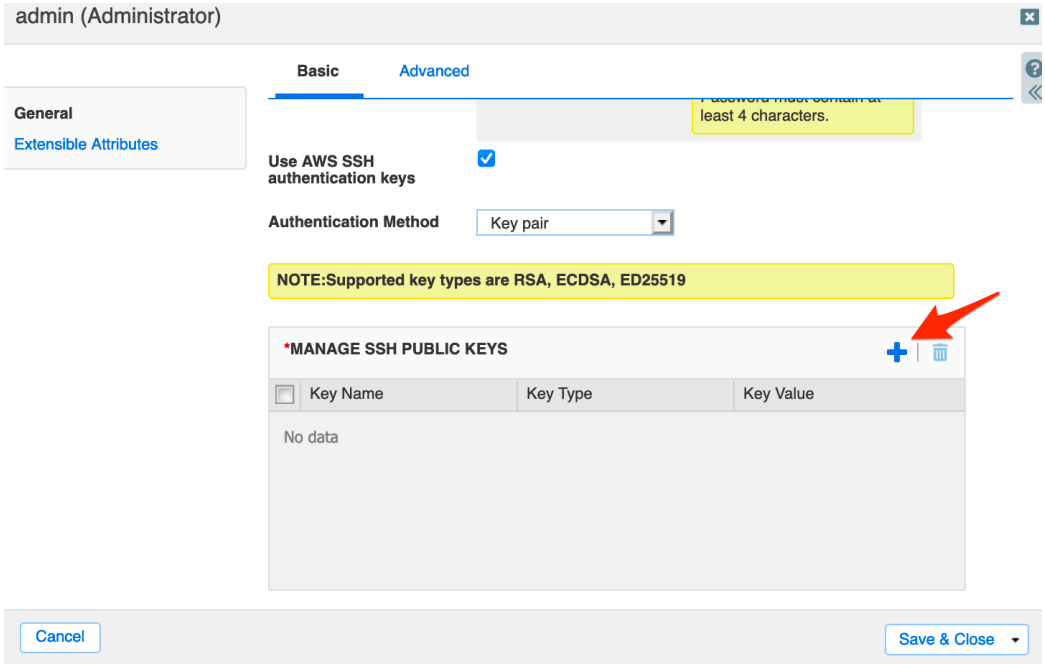
Adding SSH Keys for Administrators

After joining the vNIOS for AWS instance to your existing Grid, the local administrator is replaced by administrators configured in your Grid. With NIOS 8.5.2 and later, you will no longer be able to access your new instance through SSH until you configure a Grid administrator to use key-pair authentication. To enable SSH key authentication for an administrator:

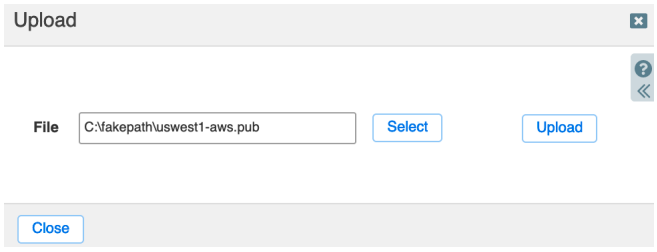
1. Login to your Grid Manager.
2. Navigate to the **Administration** → **Administrators** → **Admins** tab.
3. Select the administrator you will use for SSH to the member and click the **Edit** icon.



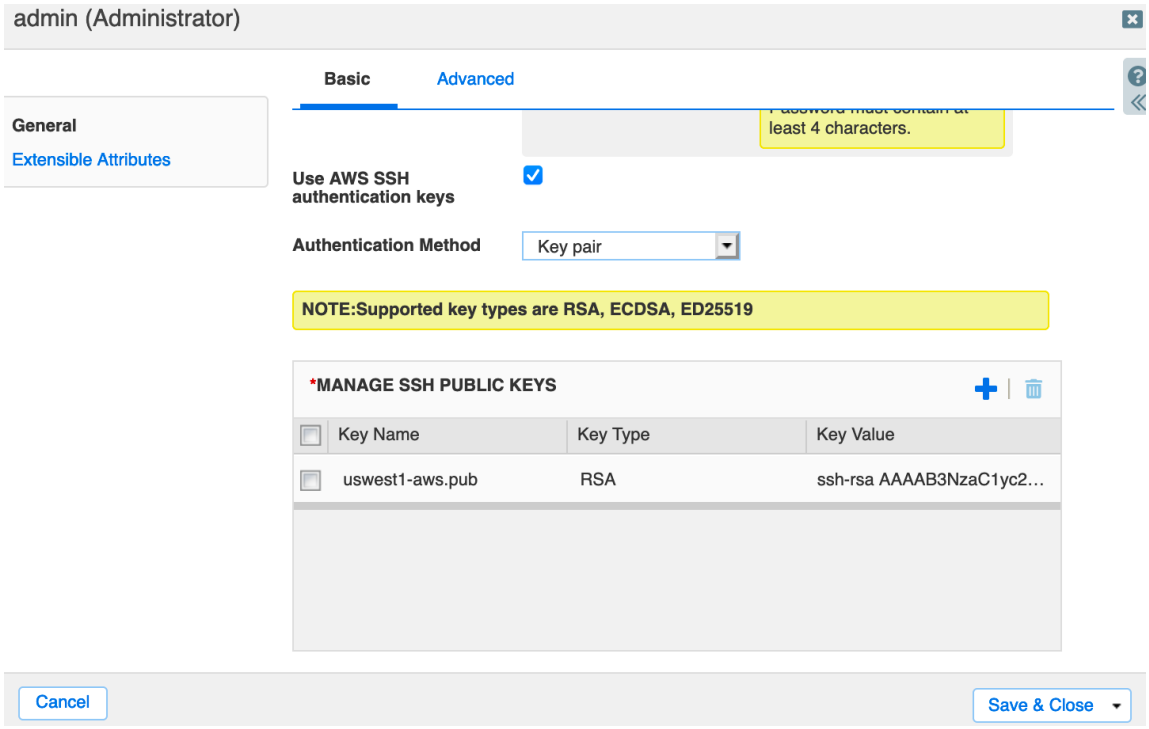
4. In the admin editor, click the check box for **Use AWS SSH authentication keys**.
5. Use the dropdown for Authentication Method to select either **Key pair** or Key pair + Password.
6. Click the (Add) next to Manage SSH Public Keys.



7. Use the Upload dialog to **Select** and **Upload** your public key.



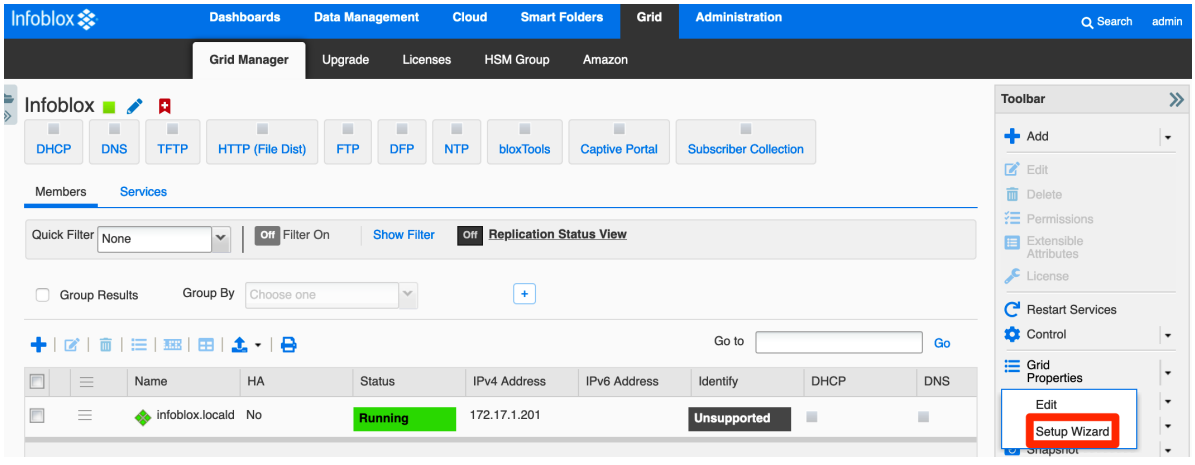
8. Click **Save & Close**. You are now able to SSH to Grid members including your vNIOS for AWS instance using your private key.



Use vNIOS Instance for New Grid

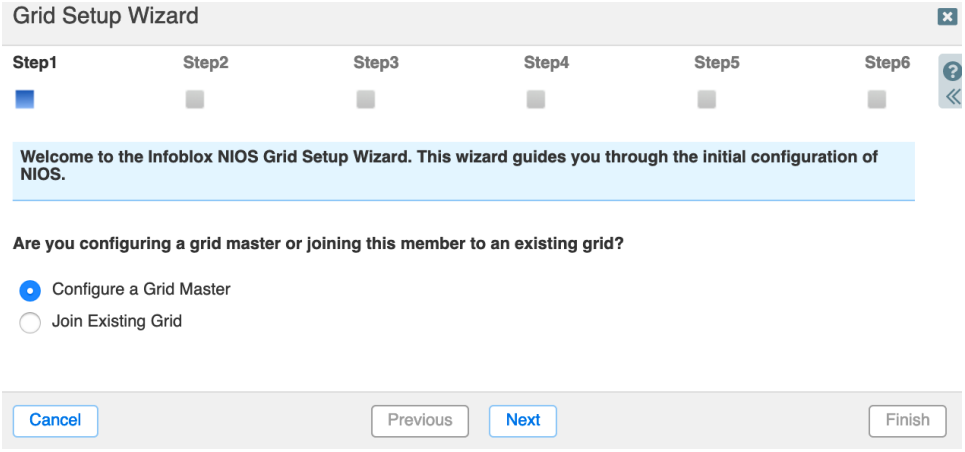
Infoblox vNIOS for AWS instances can be used as a standalone appliance or as a Grid Master for a new Grid. This section covers the basic setup of your new vNIOS instance as a Grid Master.

1. Login to your vNIOS for AWS instance Grid Manager GUI.
2. On your first login to the instance, the Grid Setup Wizard should open. If it is not open, navigate to the **Grid** → **Grid Manager** → **Members** tab. Open the dropdown for **Grid Properties** in the right-hand menu. Select **Setup Wizard**.

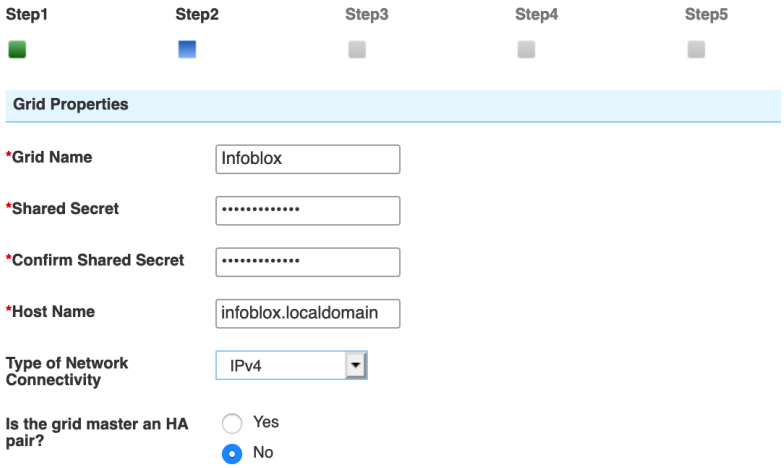


3. In Step 1 of the Grid Setup Wizard, select **Configure a Grid Master**.

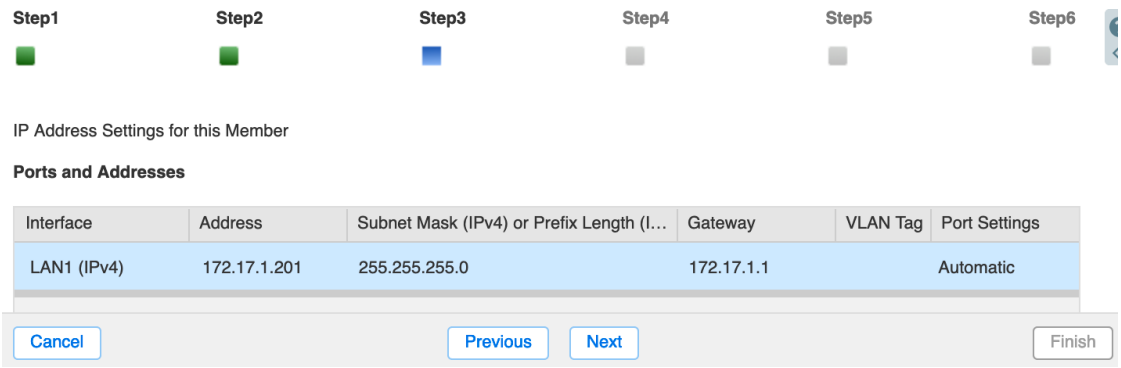
4. Click **Next**.



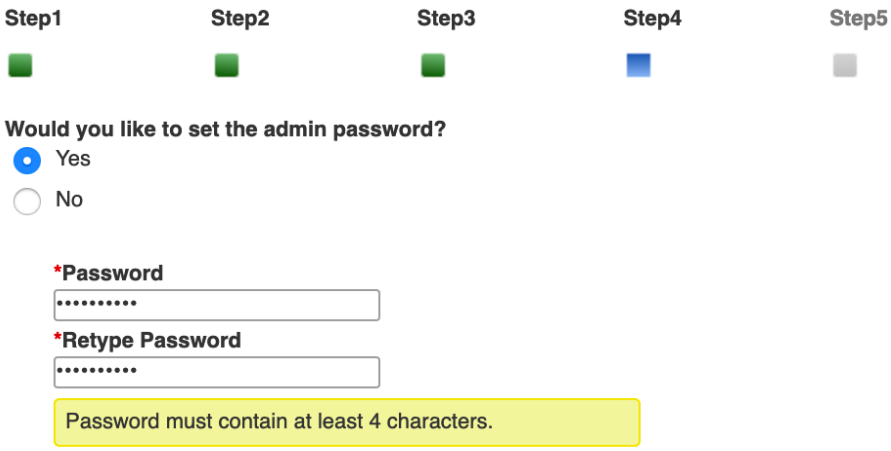
5. In Step 2, optionally change the Grid name and Shared Secret.
6. Leave defaults for Network Connectivity and HA pair.
7. Click **Next**.



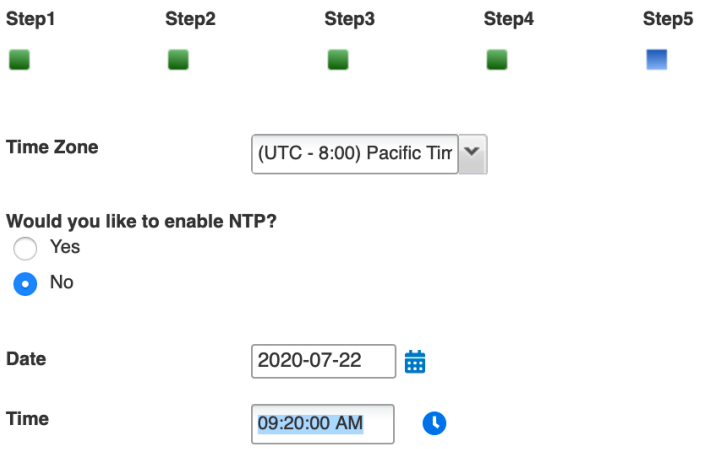
8. On Step 3, verify the IP settings for your instance LAN1 interface. You should not need to make any changes here.
9. Click **Next**.



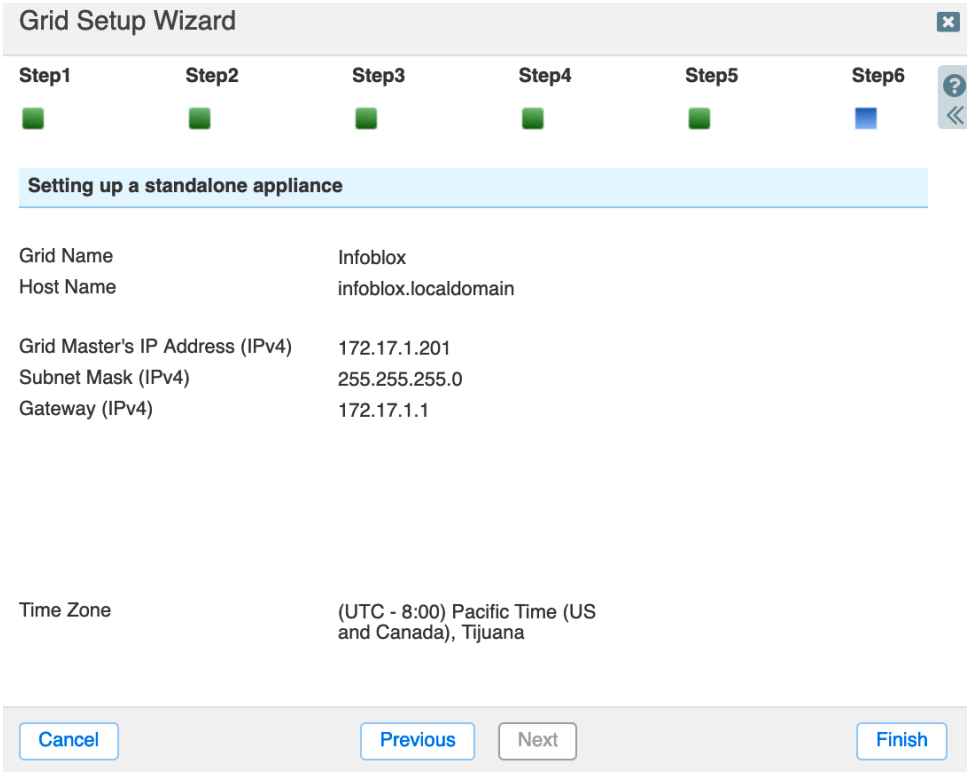
10. On Step 4, optionally select **Yes** to change the admin password (recommended).
11. Enter your new admin password.
12. Click **Next**.



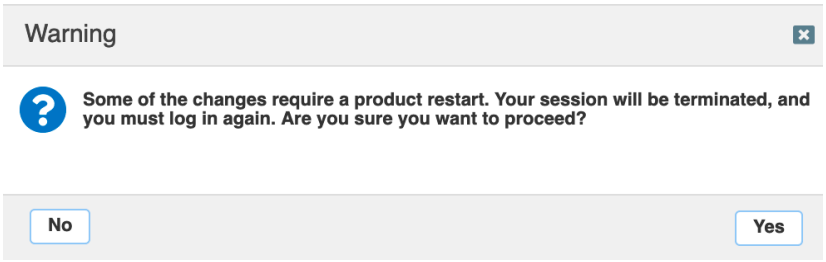
13. On Step 5, set the Time Zone.
14. Optionally, select **Yes** to enable NTP.
15. Set the time and date if they are incorrect.
16. Click Next.



17. On Step 6, review the appliance settings.
18. Click **Finish**.



19. Click **Yes** in the Warning window to restart your vNIOS appliance and apply the settings.



20. Your vNIOS for AWS instance will restart.

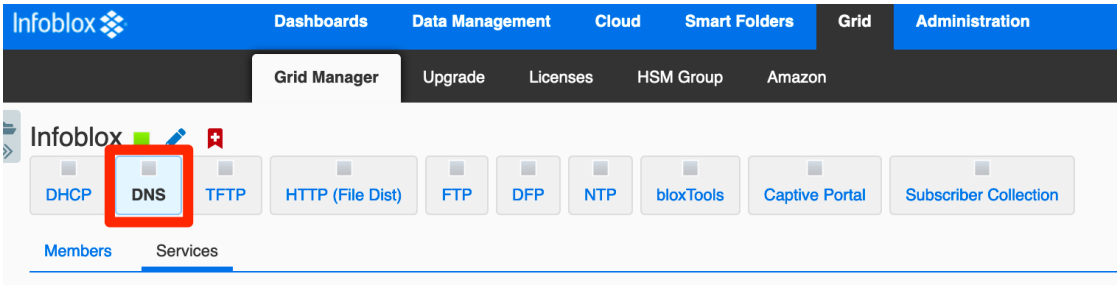
Use vNIOS Instance as Primary DNS for VPC

Infoblox vNIOS for AWS instances can be used as the primary DNS servers for AWS VPC. This allows you to extend your enterprise DNS and RPZ services into your AWS networks.

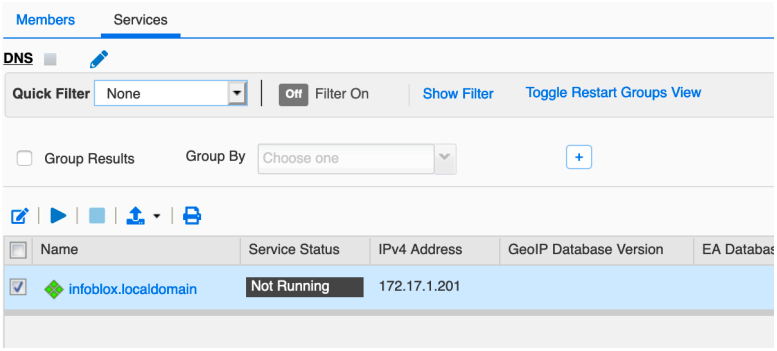
Setup DNS Service

First, we will configure basic DNS service on the Infoblox vNIOS for AWS instance. In this guide we will configure the server for both authoritative and recursive DNS; in production environments you will likely want to separate these roles on multiple appliances.

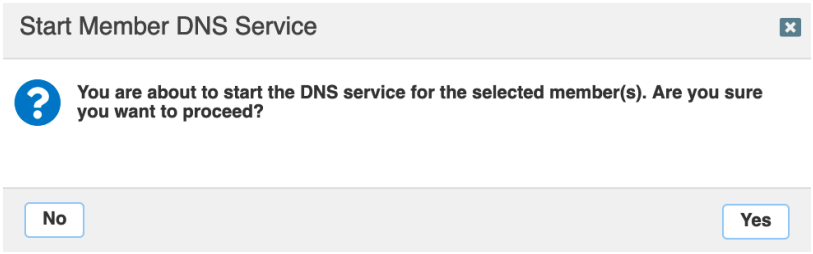
1. Login to your vNIOS for AWS instance Grid Manager GUI.
2. Navigate to the **Grid** → **Grid Manager** → **Services** tab.
3. Click on the **DNS** service.



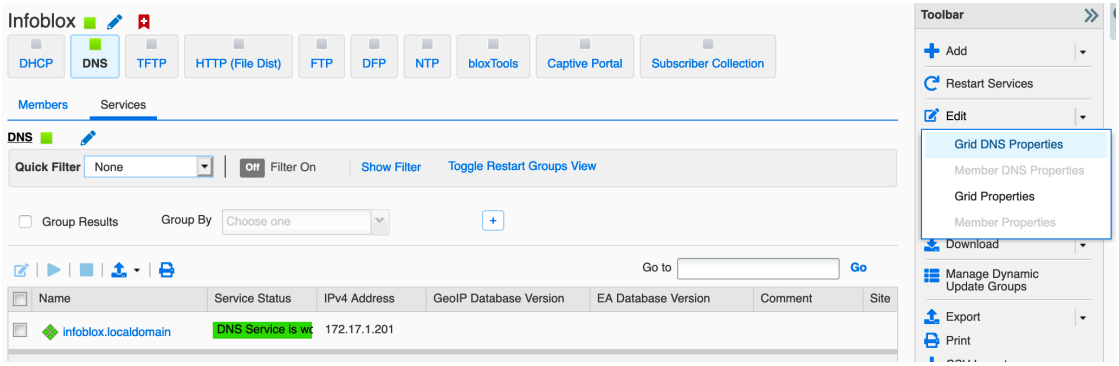
4. Select the checkbox next to your vNIOS member.
5. Click the start button to start the DNS service.



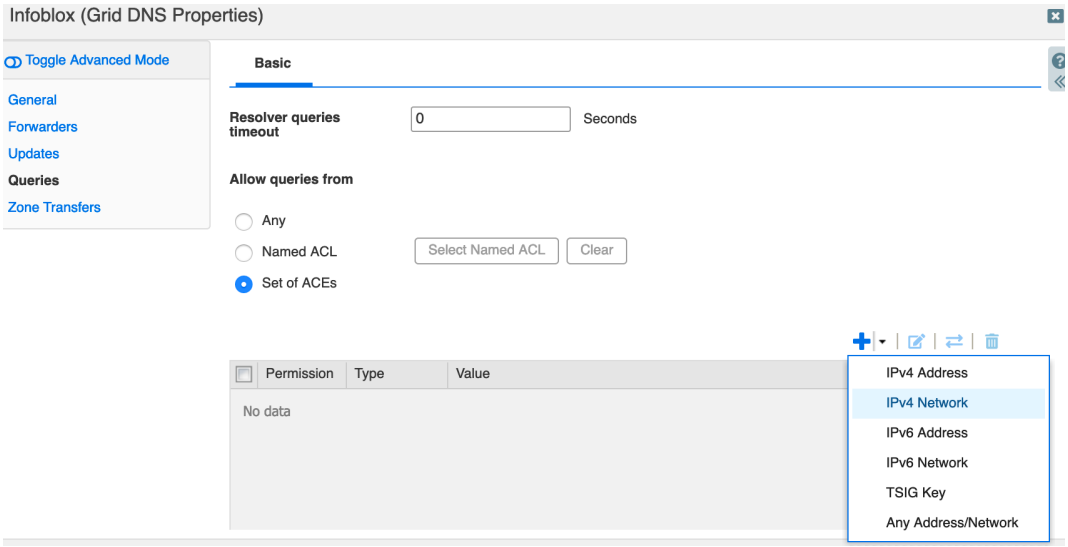
6. Click **Yes** in the popup window to confirm.



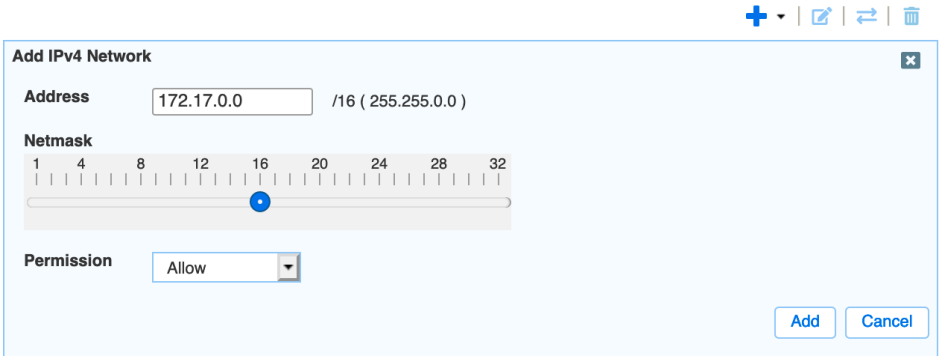
7. Once the service is started, open the dropdown next to Edit in the right-hand menu.
8. Select **Grid DNS Properties**.



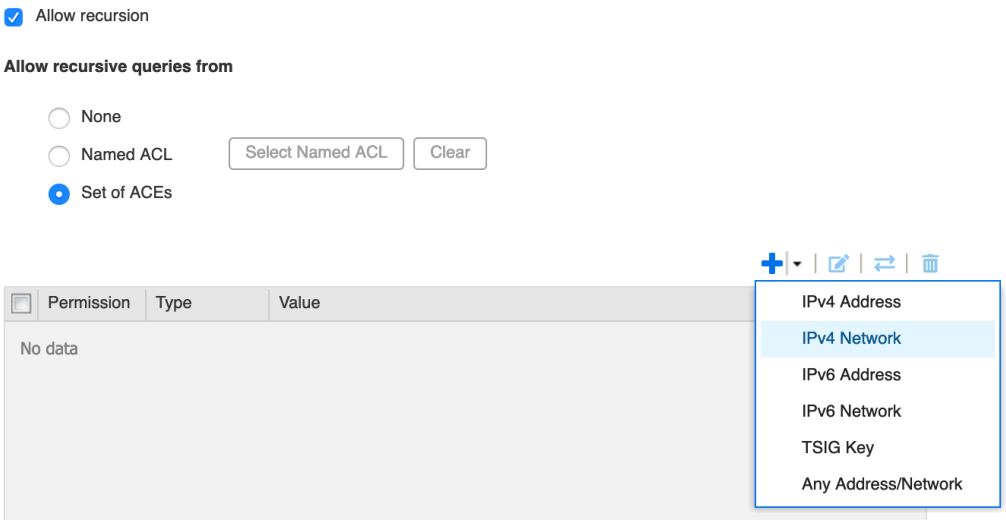
9. In the Grid DNS Properties window, select the **Queries** tab.
10. Optionally, change Allow queries to **Set of ACEs**.
11. Use the + add dropdown to select **IPv4 Network**.



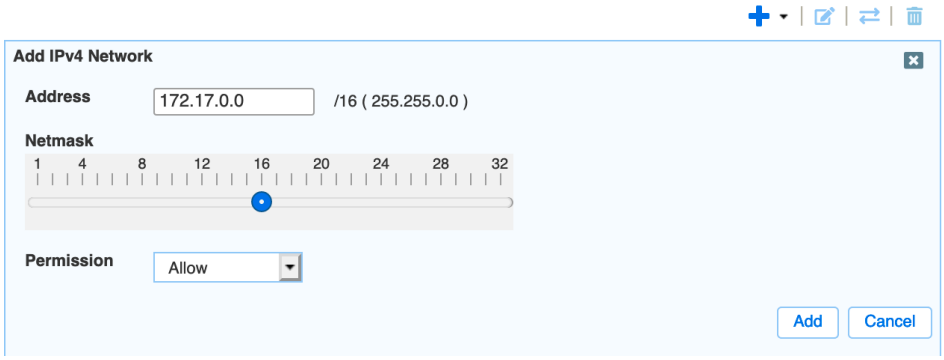
12. For **Address** enter the network prefix for your VPC. For example: **172.17.0.0**.
13. Use the **Netmask** slider to select the correct mask size. For example: **/16**.
14. Click **Add**.



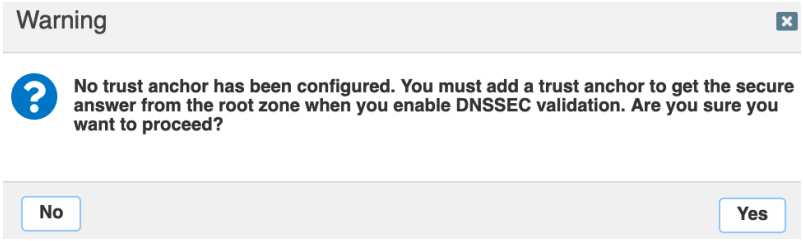
15. Scroll down and select **Allow recursion**.
16. Select **Set of ACEs**.
17. Use the + add dropdown to select **IPv4 Network**.



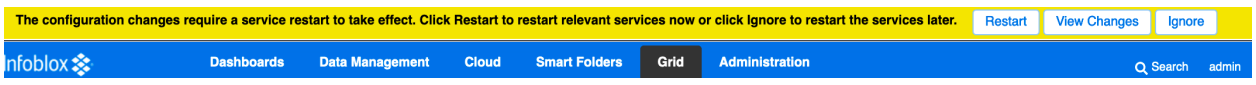
18. For **Address** enter the network prefix for your VPC. For example: **172.17.0.0**.
19. Use the **Netmask** slider to select the correct mask size. For example: **/16**.
20. Click **Add**.



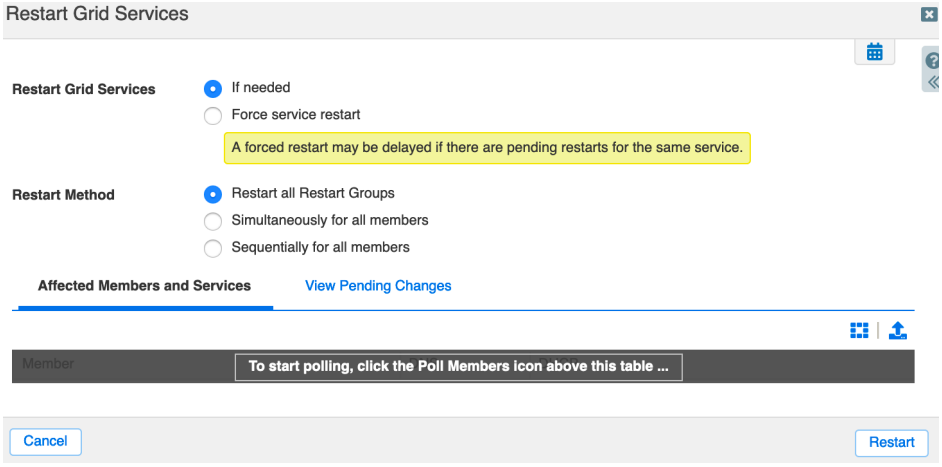
21. Click **Save & Close**.
22. In the Warning window, click **Yes**.



23. Click **Restart** in the banner that opens in the top of the window.

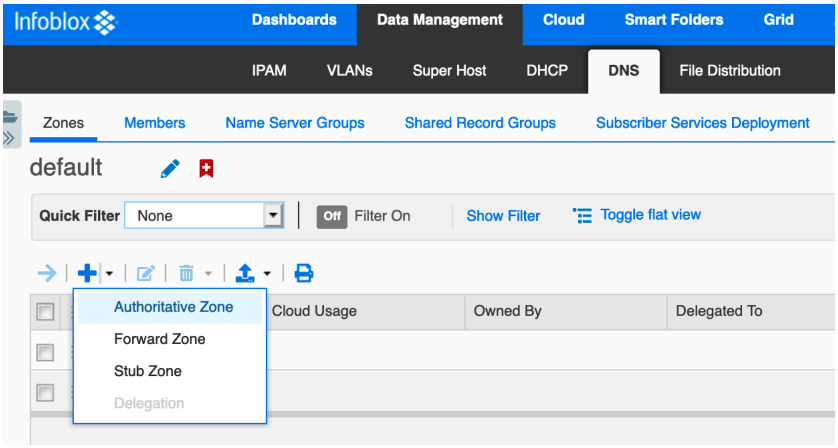


24. Click the **Restart** button in the Restart Grid Services window.

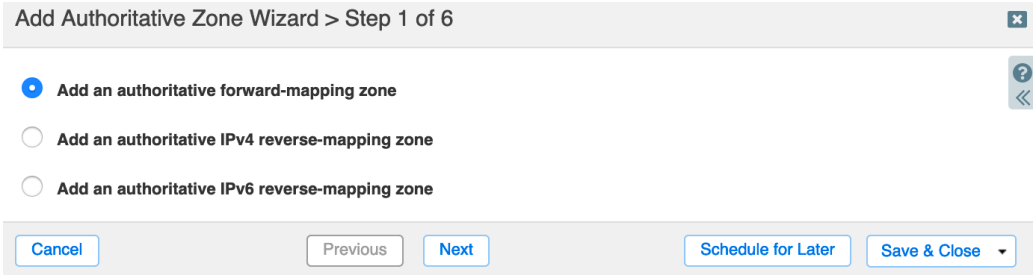


Add DNS Zone

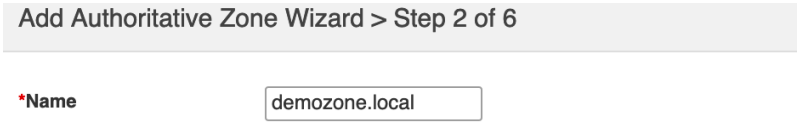
1. To add an authoritative DNS zone, navigate to the **Data Management → DNS → Zones** tab.
2. Use the + add dropdown to select **Authoritative Zone**.



3. On Step 1 of the Add Authoritative Zone Wizard, select **Add an authoritative forward-mapping zone.**
4. Click **Next.**

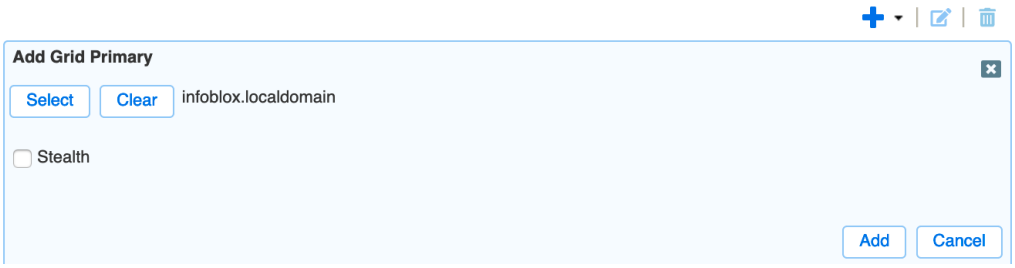


5. On Step 2 enter a name for your DNS zone.
6. Click **Next**.

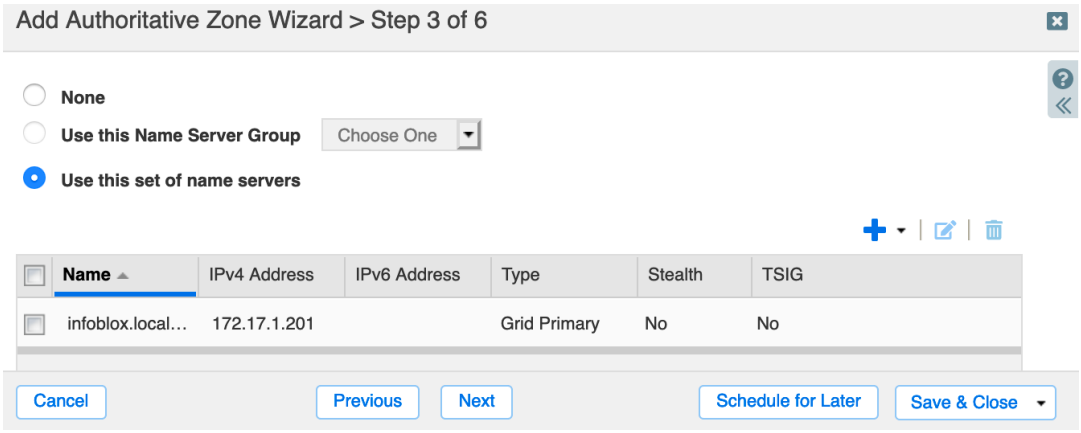


7. On Step 3 select **Use this set of name servers**.
8. Use the + add dropdown to select **Grid Primary**.

9. Click **Select**. The single member of this Grid will automatically be selected.
10. Click **Add**.



11. Click **Save & Close** to create the new zone. Or click **Next** to proceed to optional steps.

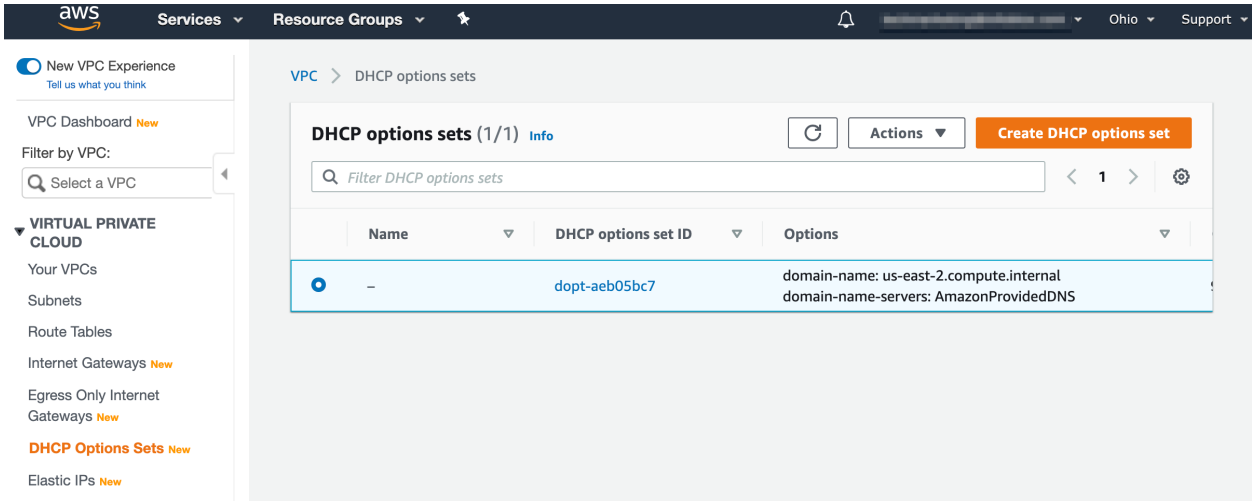


12. Click **Restart** in the banner that opens at the top of the window.
13. Click the **Restart** button in the Restart Grid Services window.

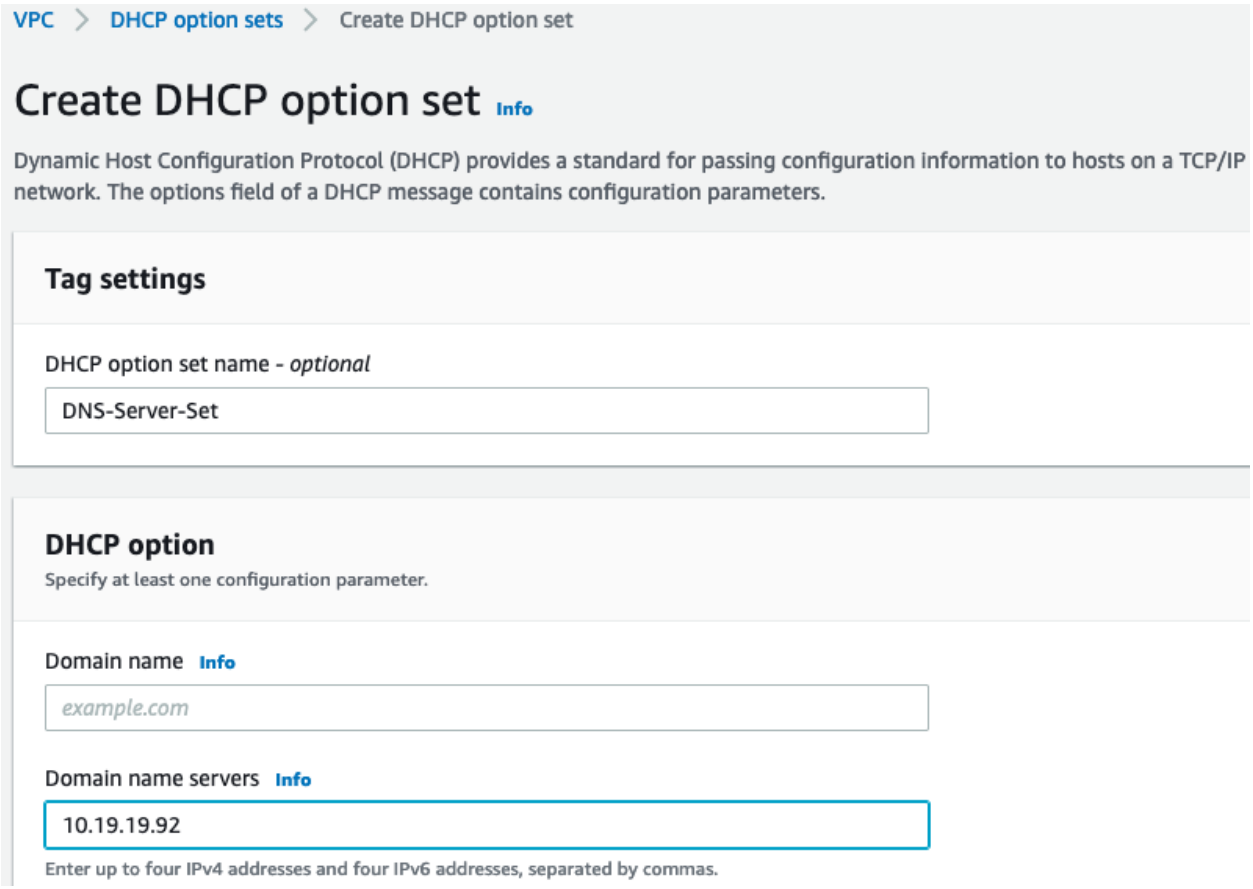
Create AWS DHCP Options Set

AWS VPCs use DHCP options sets to specify optional configurations such as a default domain name or the DNS servers your instances should use. We will use an options set to make the Infoblox vNIOS for AWS instance the primary DNS server for a VPC. DHCP options sets cannot be modified after creation, so we will start by creating a new DHCP options set.

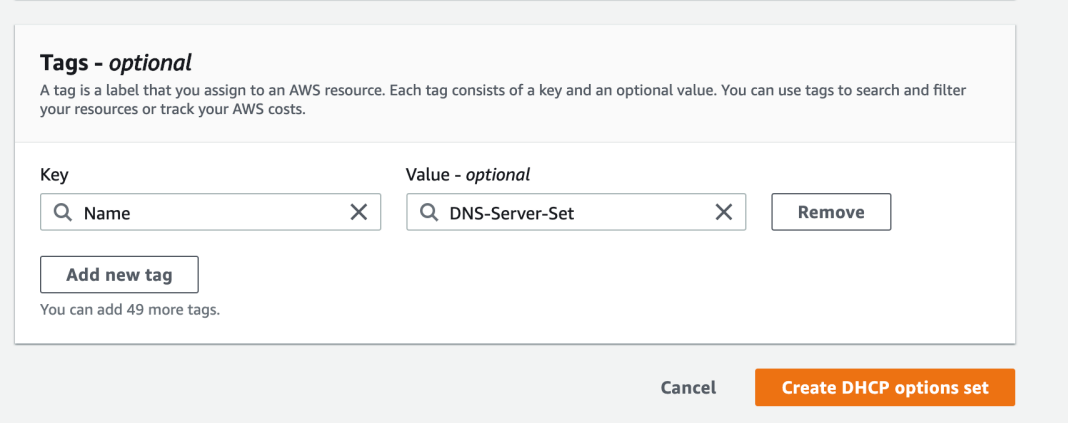
1. In the AWS Management Console, Use the Services menu to navigate to **VPC** under Networking & Content Delivery.
2. From the VPC menu, click on **DHCP Options Sets**.



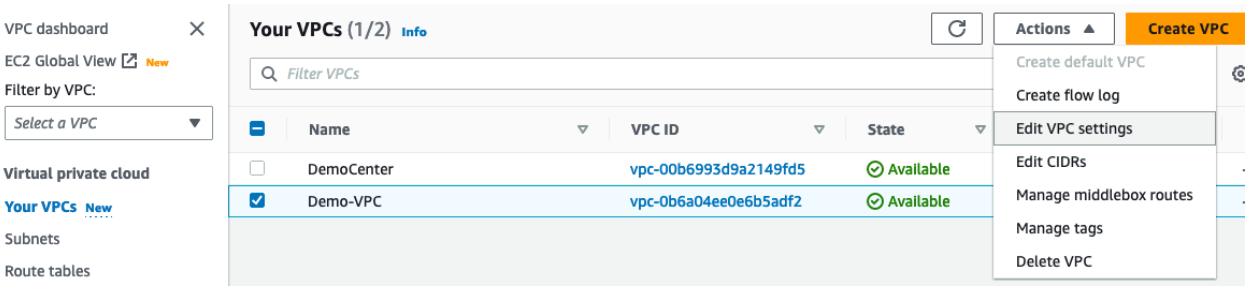
3. Click **Create DHCP options set**.
4. Enter a name for your option set.
5. Under Domain name servers, enter the private IP address of your vNIOS for AWS eth1 (LAN1) interface.



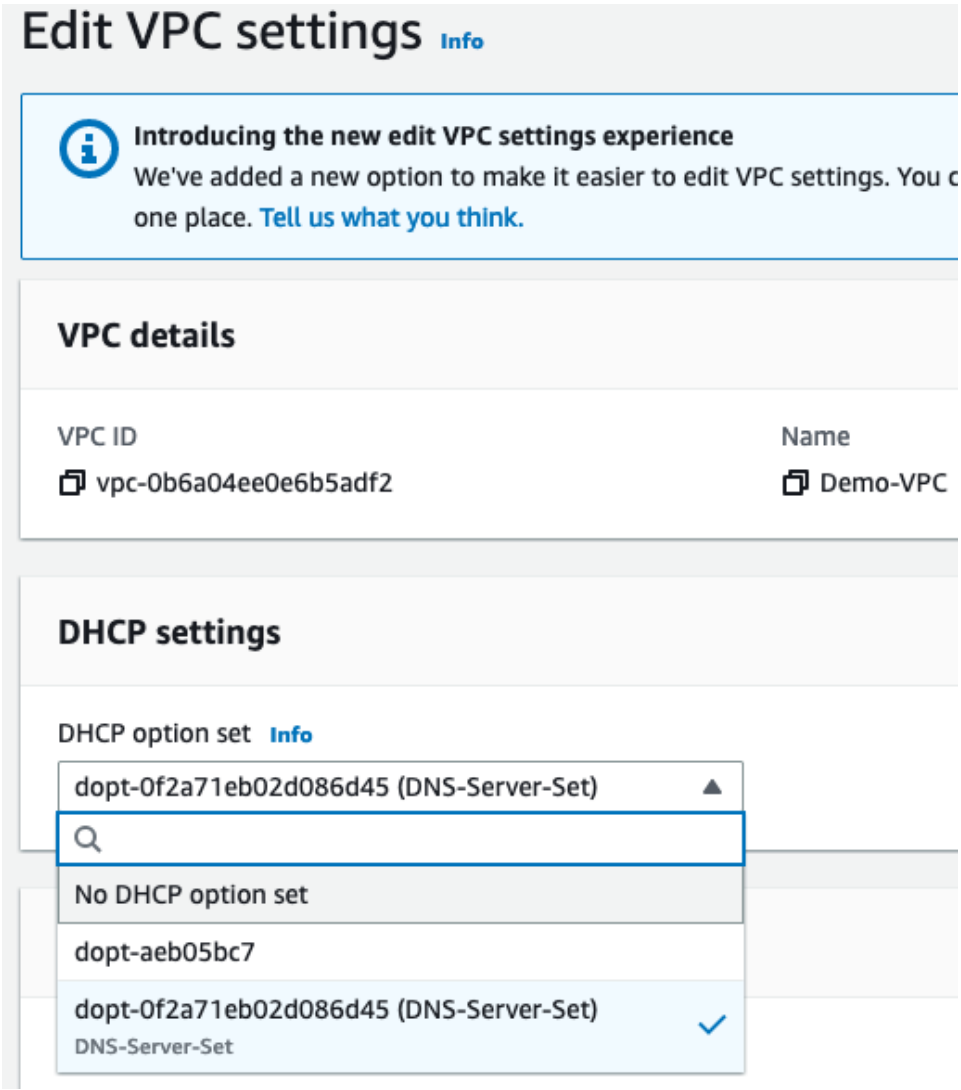
6. Scroll down and click **Create DHCP options set**.



7. To assign this DHCP options set to your VPC, select **Your VPCs** in the menu.
8. Select your VPC.
9. Use the Actions dropdown menu to select **Edit VPC settings**.



10. Use the dropdown menu for DHCP options set to select the new options set you created.



11. Scroll down to click **Save**.

Note: Any new VM instances you create in this VPC will use your Infoblox vNIOS for AWS appliance for DNS resolution. Existing VM instances must be rebooted to apply this change.

vDiscovery for AWS

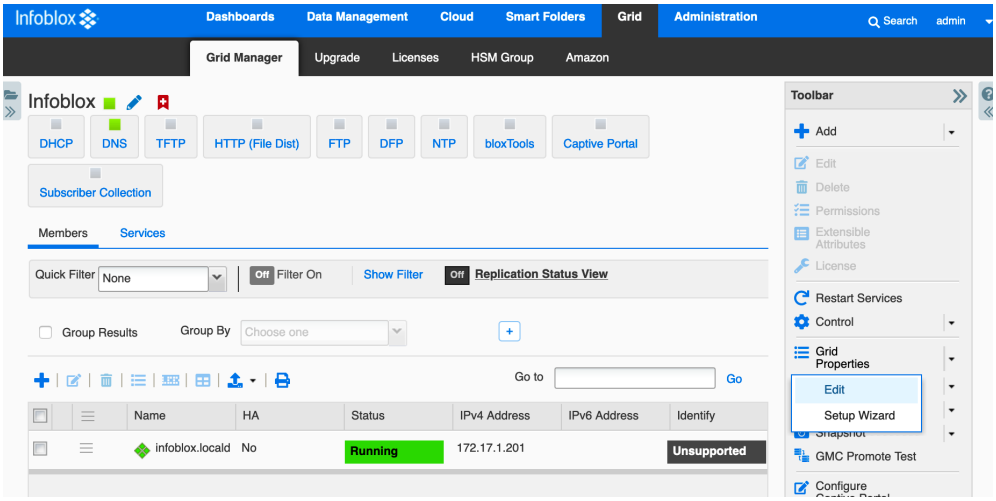
The Infoblox vDiscovery feature is very useful for detecting and obtaining information about Tenants, VPCs, Subnets, and Virtual Machines (VM's) operating in your public cloud environments.

Many organizations operate hybrid and multi-cloud environments that may contain many subscriptions and accounts. These environments tend to be very dynamic, with things such as VMs being created and terminated on a frequent basis. This makes it difficult to keep track of everything. With Infoblox vDiscovery, tasks can be configured to run automatically allowing your Infoblox vNIOS appliance to keep track of all cloud environments, storing this data in IPAM. Infoblox vDiscovery can also be used to automate creation of DNS records for VMs running in your cloud environments. Using vDiscovery in conjunction with the Cloud Network Automation (CNA) feature, you will gain enhanced visibility into your cloud environments, all within a 'single pane of glass'.

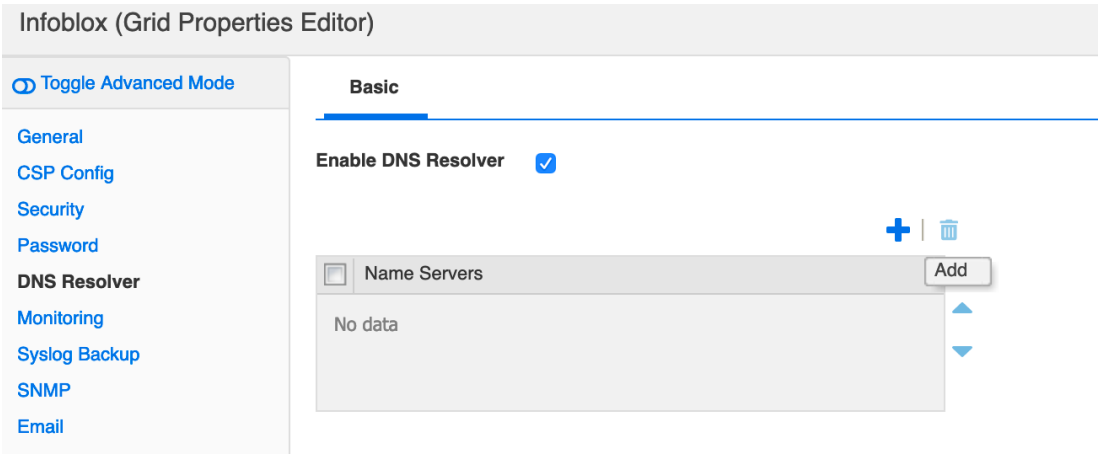
Configure vDiscovery in Grid Manager

DNS Resolver: In order to conduct vDiscovery for AWS, your Infoblox vNIOS for AWS instance must be able to resolve AWS endpoints such as ec2.us-west-1.amazonaws.com. Configuring the DNS Resolver in NIOS will achieve this.

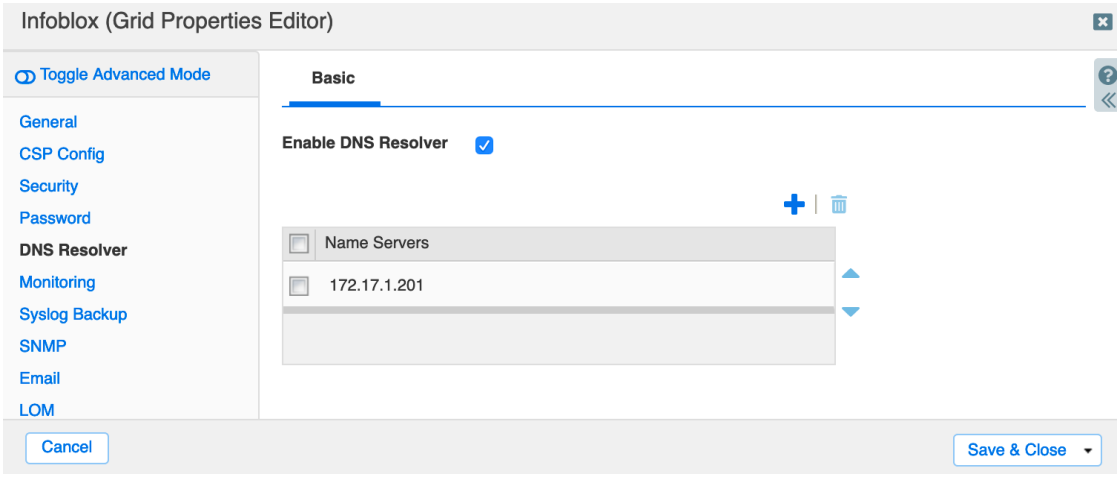
1. Log into the Grid Manager GUI of your vNIOS for AWS instance.
2. Navigate to the **Grid** → **Grid Manager** → **Members** tab.
3. In the **Toolbar**, Open the **Grid Properties** dropdown.
4. Select **Edit**.



5. Navigate to the **DNS Resolver** tab of the Grid Properties Editor.
6. Select the checkbox next to **Enable DNS Resolver**.
7. Click the + (Add) to add an upstream Name Server to use for DNS resolution.



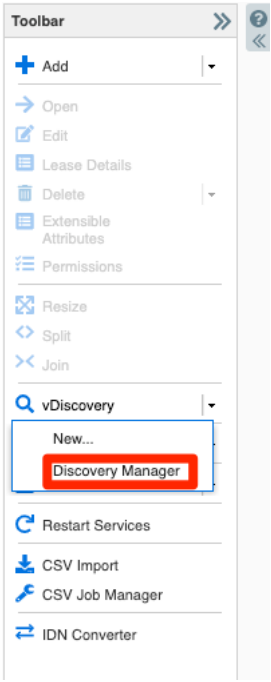
8. Enter the IP address of the name server you wish to use. For example, **172.17.1.201**.
9. Click **Save & Close**.



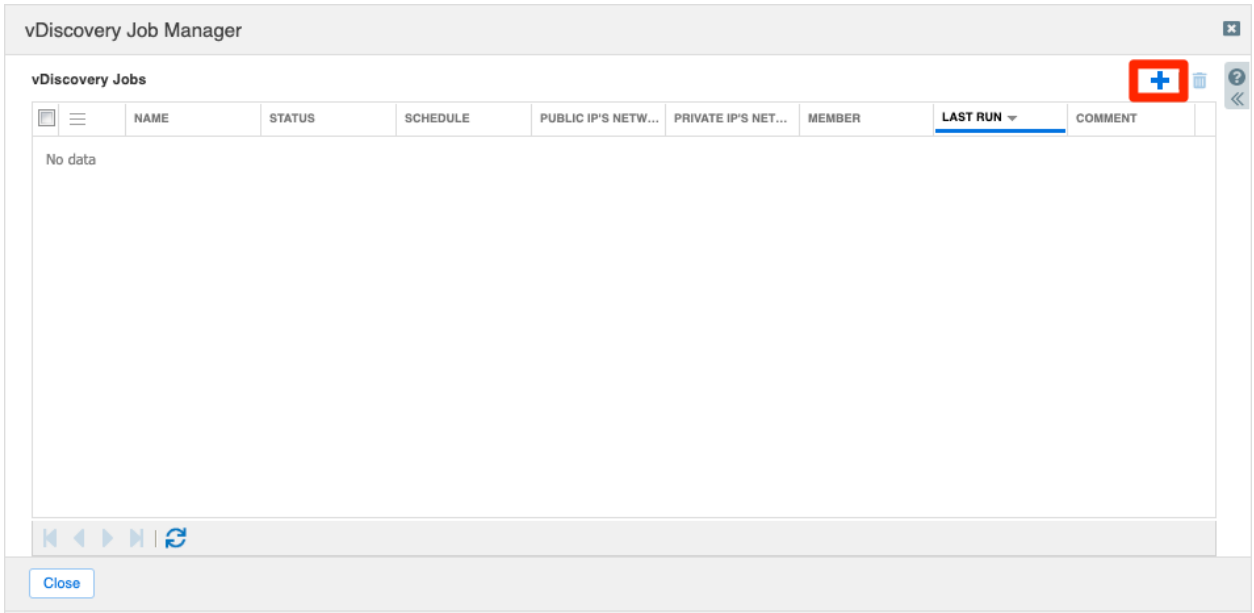
Note: If you have set up your vNIOS for AWS instance as a DNS resolver for the VPC, as specified in the Setup DNS Service section of this guide, you can enter the IP address of the instance's eth1 (LAN1) interface, to use itself for DNS resolution. This method is used in the example system for this guide.

vDiscovery Job: To conduct vDiscovery in AWS, you must configure a discovery job, using the Access Key ID and Secret Access Key created with AWS IAM, as well as the regional EC2 Endpoint identified in AWS.

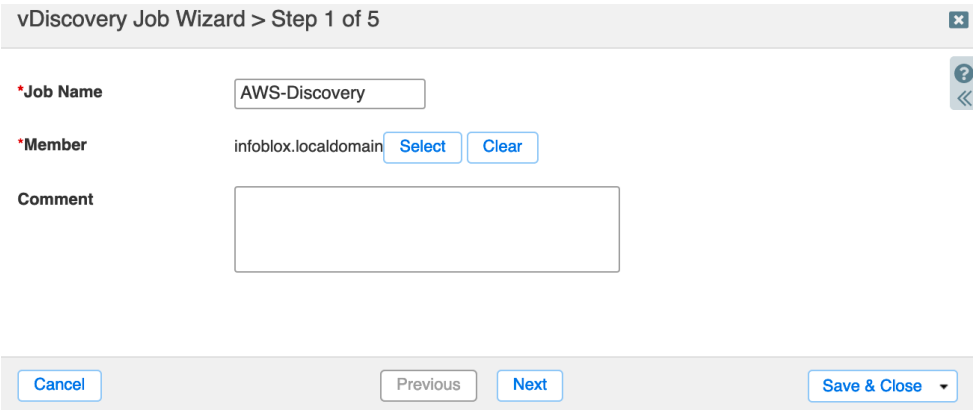
1. Log into the Grid Manager GUI of your vNIOS for AWS instance.
2. Navigate to the **Data Management** → **IPAM** tab.
3. In the **Toolbar**, Open the **vDiscovery** dropdown.
4. Select **Discovery Manager**.



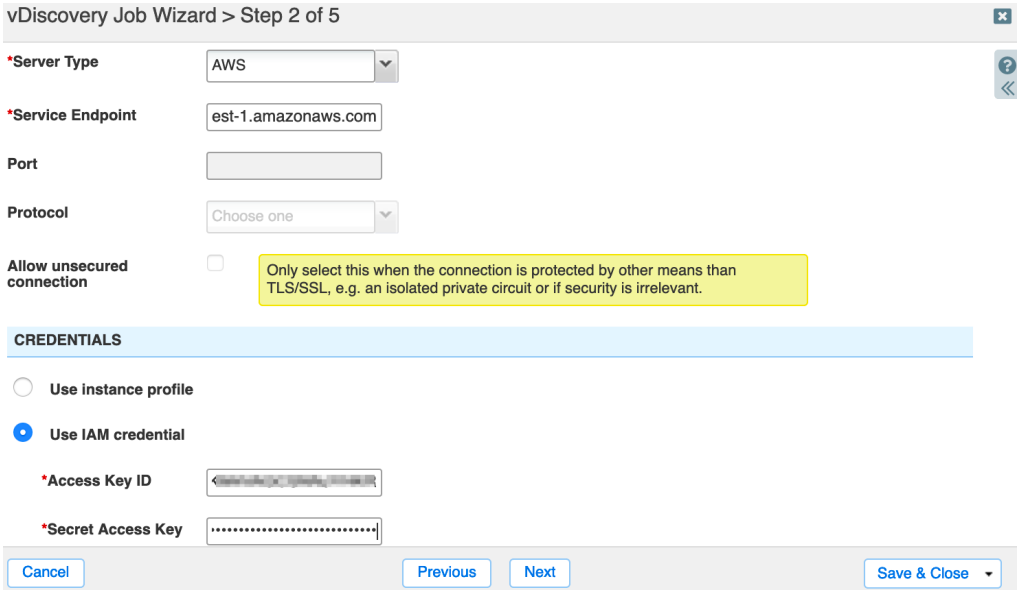
5. In the vDiscovery Job Manager window, click (Add) to add a new job.



6. In the vDiscovery Job Wizard, enter a name for the job.
7. Next to Member, click **Select**.
8. For a Grid with only one member, it will be automatically selected. If your Grid has multiple members, select the one you want to use for vDiscovery.

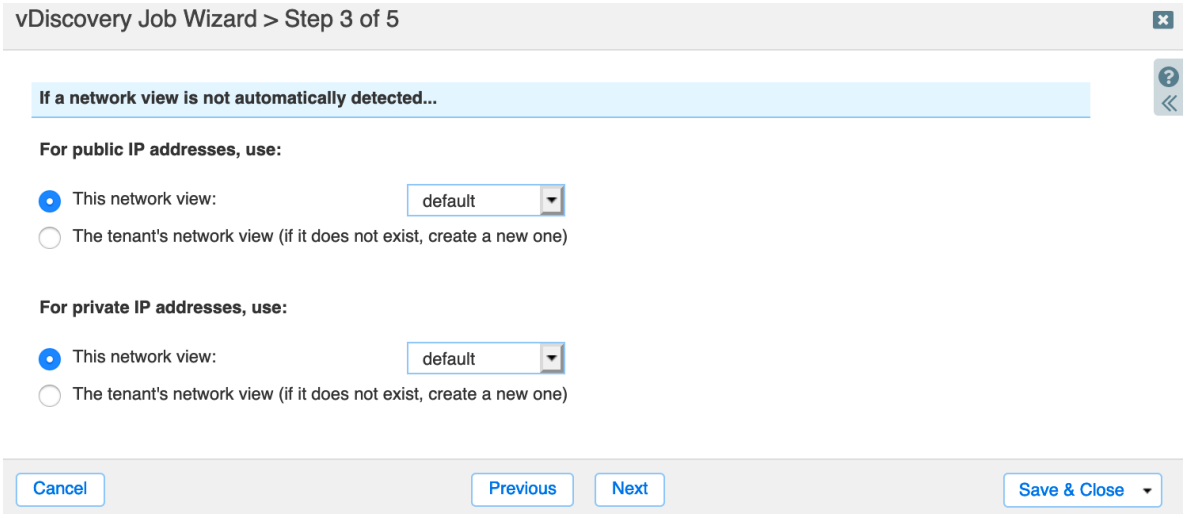


9. Click **Next**.
10. On Step 2, select **AWS** for **Server Type**.
11. For **Service Endpoint**, enter the ec2 endpoint for the AWS region you will conduct vDiscovery in, for example **ec2.us-west-1.amazonaws.com**. A full list of AWS endpoints can be found at https://docs.aws.amazon.com/general/latest/gr/rande.html.
12. Select **Use IAM credential**.
13. Enter the Access Key ID and Secret Access Key for the user you created. You will find these in the CSV file you downloaded earlier.



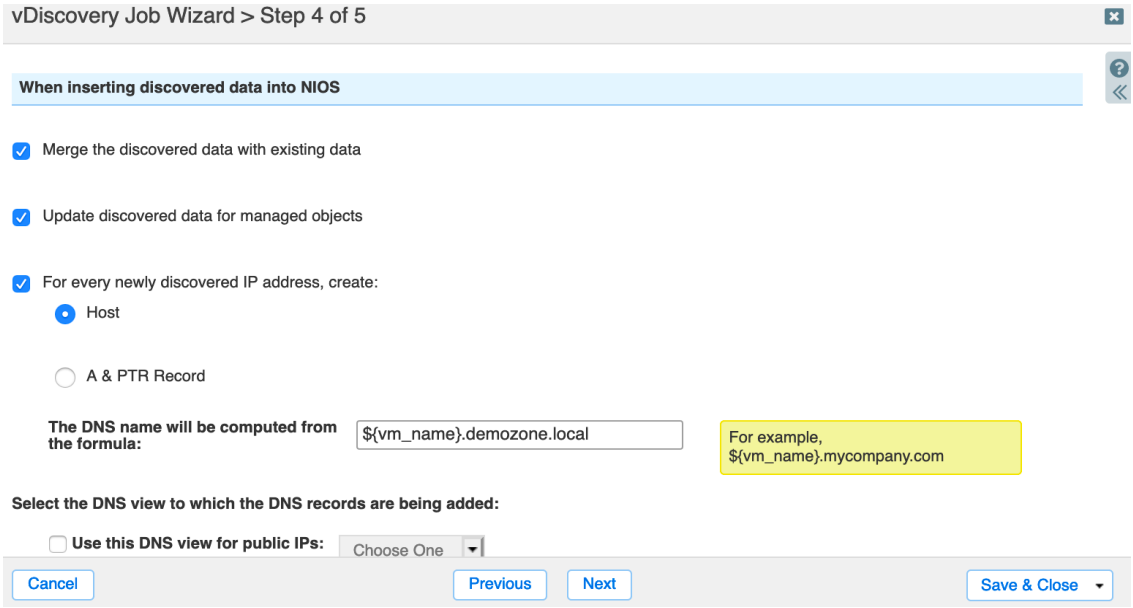
Note: If you have configured the IAM role to use with your vNIOS instance, select Use instance profile here instead.

14. Click **Next**.
15. Review the configuration for Network Views on Step 3.



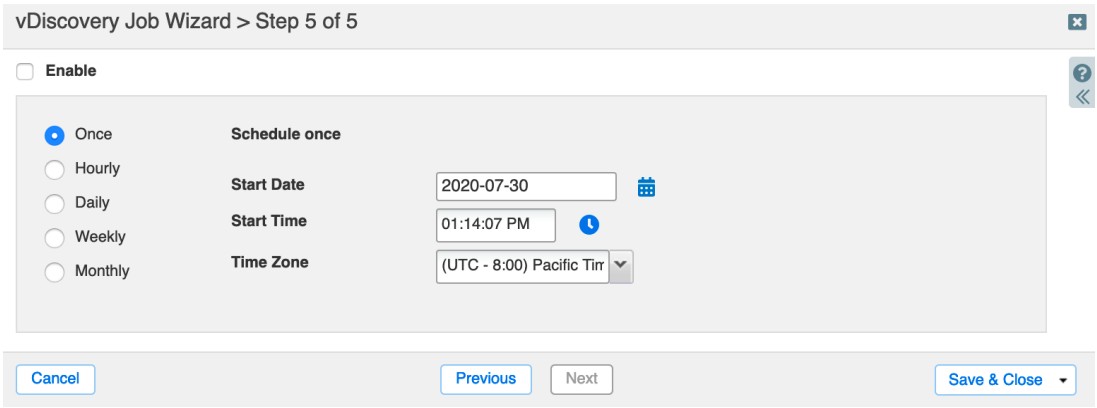
Note: The most common cause for vDiscovery to fail to import any data is a "Sync Error" due to overlapping/conflicting address space. To account for any address space conflicts that are encountered during the vDiscovery process or with your existing IPAM data, you may need to select the option to use ***The tenant's network view (if it does not exist, create a new one)****.*

16. Click **Next**.
17. Optional: For automatic creation of DNS records, on step 4 select the checkbox **For every newly discovered IP address, create:**
18. Select the desired DNS record object type. If in doubt, stick with the default (**Host**) option.
19. The name for DNS records that are created is controlled with a macro, with the most commonly used macro being ${vm_name). In the text box, type the desired macro, followed by the zone that you want to use. Example: **${vm_name}.testzone.com**.



Note: If a different format is desired for the DNS record name, a full list of available macros can be found in the Help panel. To view this, click on  *(Help) at the top-right hand corner of the window and scroll down to the section titled "**The DNS name will be computed from the formula**". Automatic creation of DNS records for discovered VMs is available with the CNA license.*

20. Click **Next**.
21. Optional: Configure a schedule to automatically run the vDiscovery task.

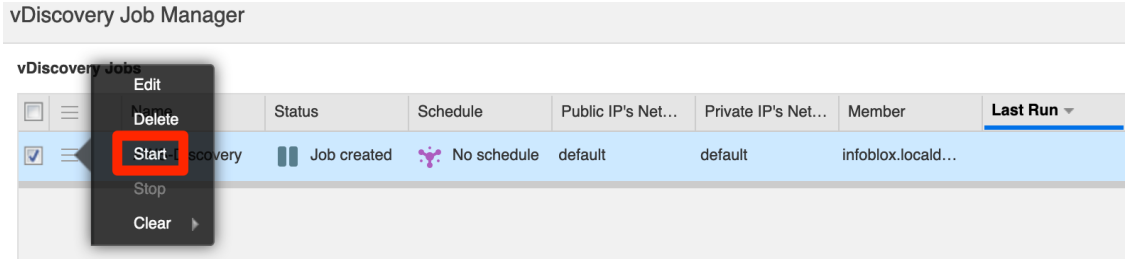


Note: The scheduler enables you to run the vDiscovery task as frequently as once an hour. If this must be run more frequently, you can accomplish this using the API. Refer to the Infoblox REST API guide for examples and guidelines on this process.

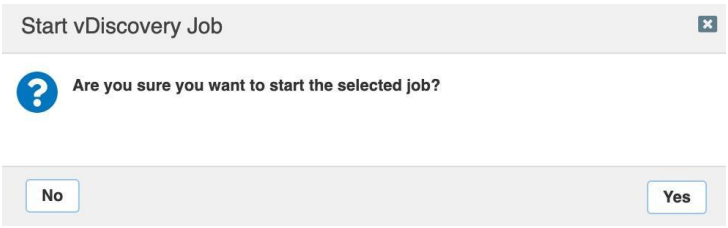
22. Click **Save & Close**.

Run vDiscovery

1. To run your vDiscovery job, from the vDiscovery Job Manager window click the  (Action Menu) for your vDiscovery job.
2. Select **Start**.



3. Click **Yes** in the popup window.

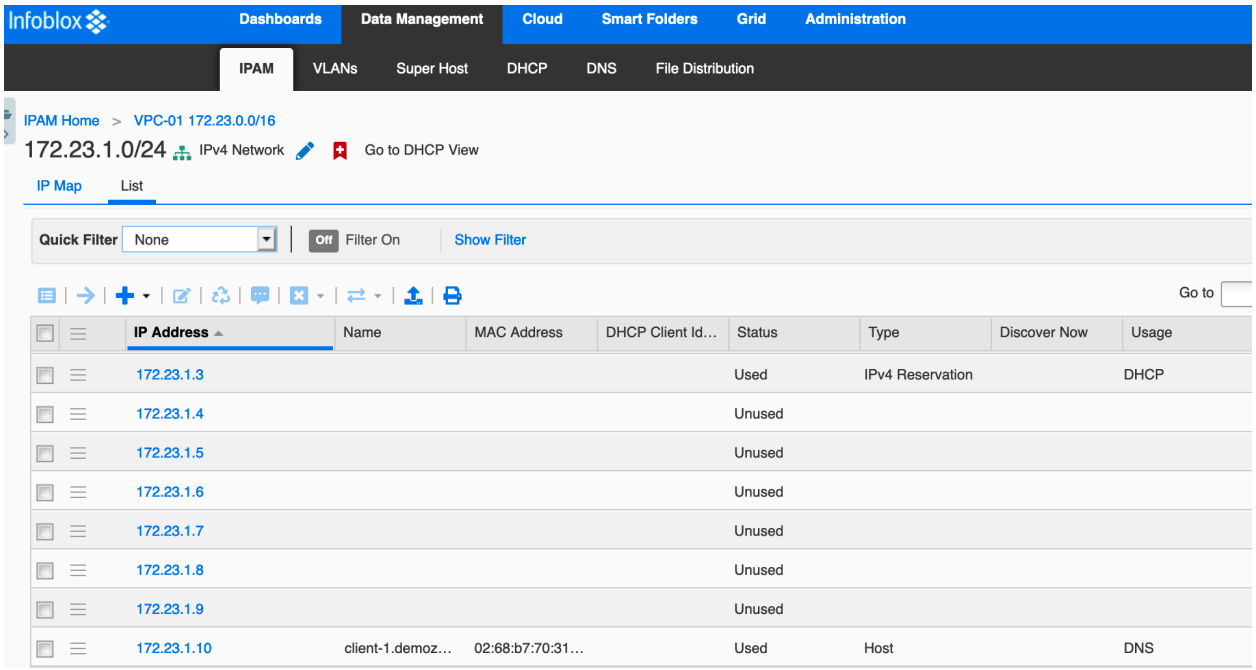


vDiscovery Data

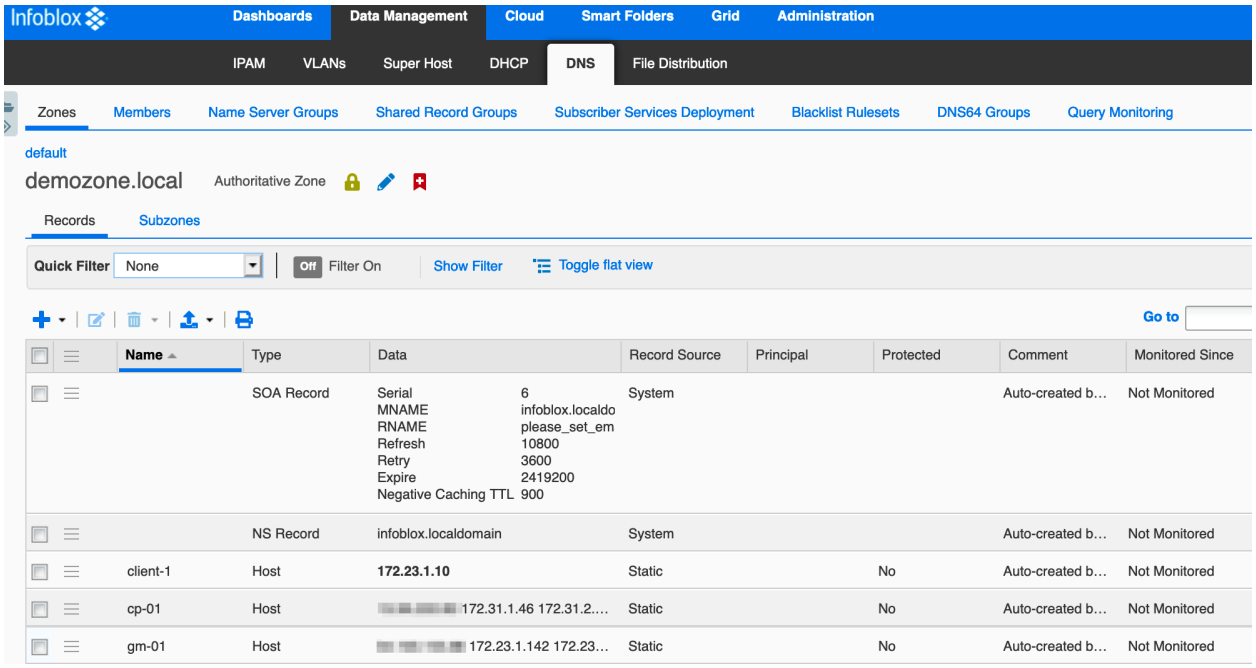
Data collected by vDiscovery can be tracked through Data Management (IPAM, DHCP and DNS) and if the CNA license is installed, additional details will be found under the Cloud tab. Objects created by vDiscovery will automatically include metadata in their properties or extensible attributes (EA's), a useful addition that enables you to easily identify, locate and report on your resources deployed in the cloud.

Data Management: From the Data Management tab, you can access IPAM and DNS data discovered from your AWS environment.

- **IPAM:** IPAM, or IP Address Management, provides an easy view of all data from an IP address perspective. If you are looking for an object based on its IP address, this can be one of the easiest ways to drill down and see everything there is for that IP, including all objects that are associated with it.

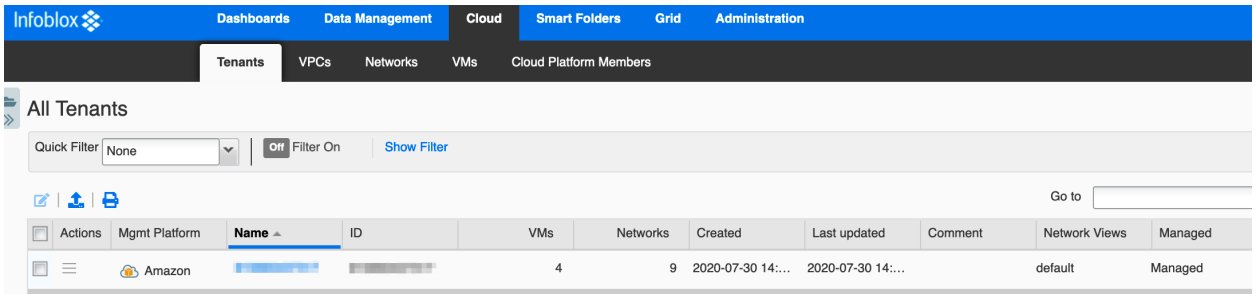


- **DNS:** If you enabled the automatic creation of DNS records, the records can be viewed by drilling down into the DNS zone you specified.

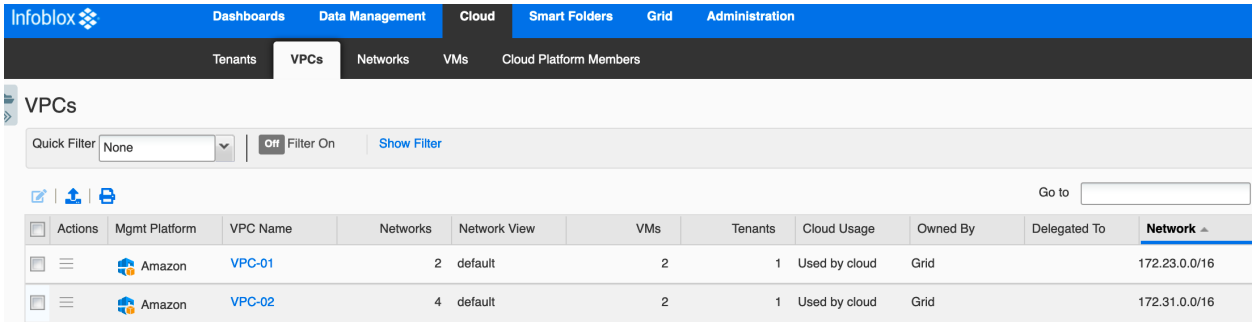


Cloud Network Automation: When the CNA license is installed, you will find the Cloud tab in your Grid Manager GUI. The Cloud tab includes five additional tabs that each provide different perspectives for viewing your cloud data, making it easy to see what is running in your cloud environments.

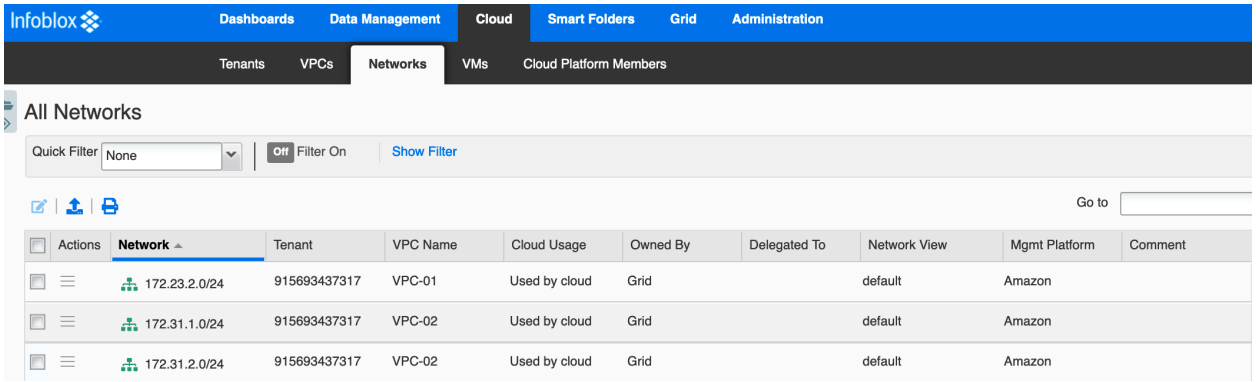
- **Tenants:** For AWS vDiscovery, entries on this tab correspond to AWS accounts. You can drill down to review all subnets and VMs that have been discovered under that account.



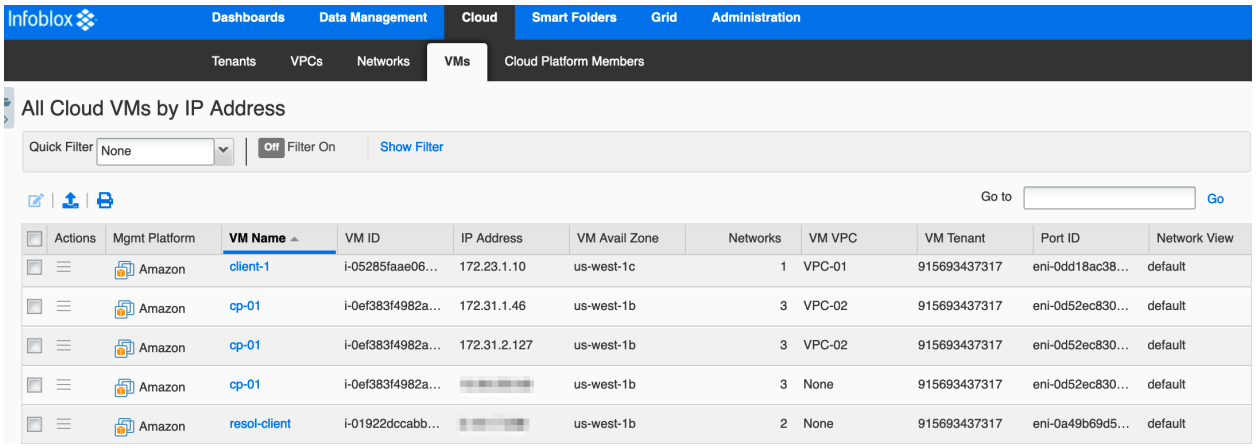
- **VPCs:** This tab displays any discovered AWS VPCs. You can drill down to review all subnets and VMs that have been discovered under an individual VPC.



- **Networks:** This tab displays all subnets that have been discovered in your AWS VPCs. Easily jump to IPAM or other perspectives to view additional details for a subnet. Searches, Smart Folders and reports can also leverage the metadata stored as EAs for each subnet.

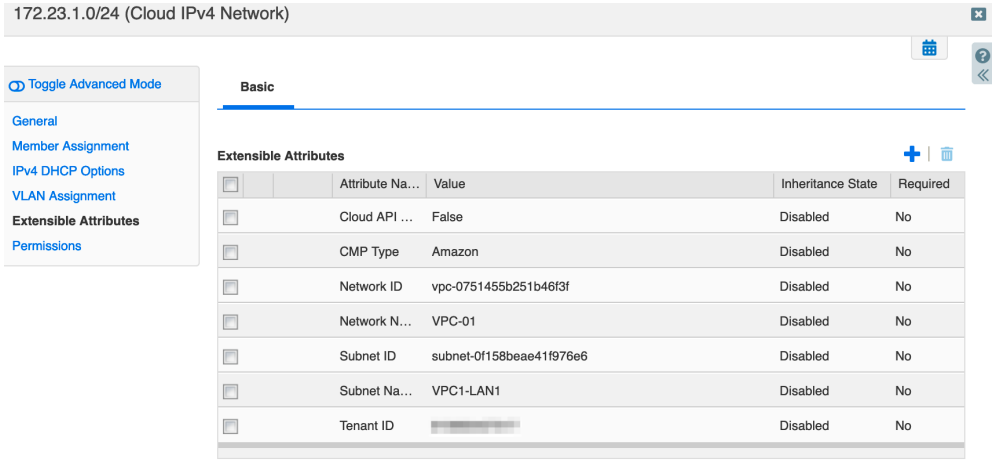


- **VMs:** This tab shows all VMs that have been discovered and are displayed per IP address. Metadata is stored in the properties for each VM, and you can readily jump to other perspectives to view and manage additional resources, including any DNS records that may have been created for the VM.



- **Cloud Platform Members:** This tab shows all Cloud Platform appliances in your Grid. For more information on Cloud Platform appliances, refer to the appropriate deployment guides at https://www.infoblox.com/resources/.

Metadata collected for each type of object discovered varies and is stored as Extensible Attributes in the Infoblox Grid. The following is an example of EAs for a Subnet.

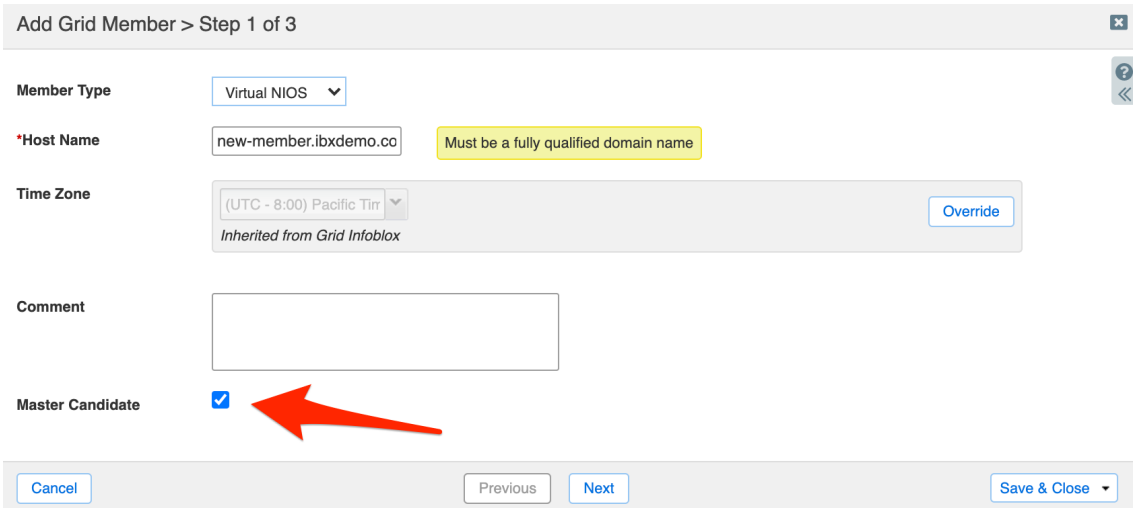


Configuring for Highly Available Services

Infoblox NIOS/vNIOS provides configuration options that can be used to ensure high availability of the Grid and core services such as DNS and DHCP. Additionally, features of AWS global infrastructure such as Regions and Availability Zones can be leveraged to deploy highly available Infoblox Grids.

Grid Master Candidate

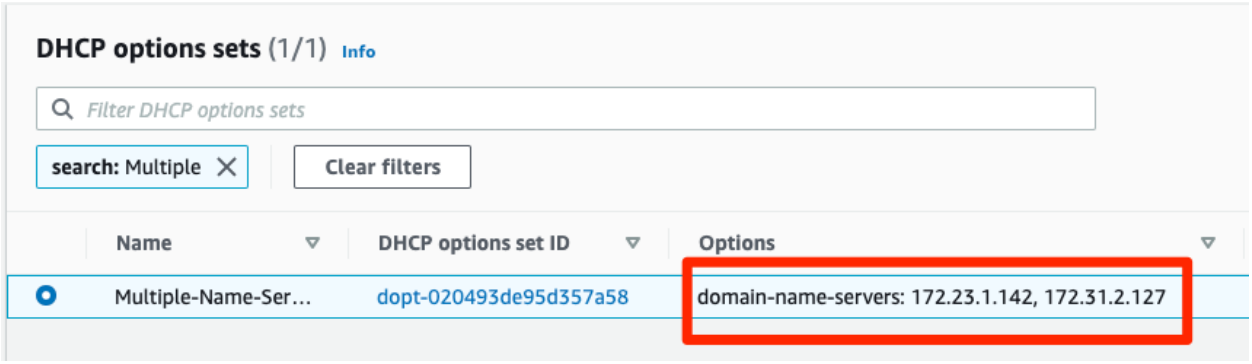
To ensure high availability and recoverability of your Grid, Infoblox recommends your Grid has at least one Grid Master Candidate (GMC), an optional designation when adding a member to the Grid. The GMC holds a complete copy of the Grid database. Ideally, the GMC should be deployed in a different location than the Grid Master so an outage is unlikely to affect both (for example, deploy the GM on-premises and the GMC in AWS or deploy GM and GMC to different regions in AWS). If the Grid Master fails, the GMC can be promoted to GM using the instructions provided in the **Backup and Recovery** section of this document. To designate a member as a Grid Master Candidate, select this option when adding the member to your Grid.



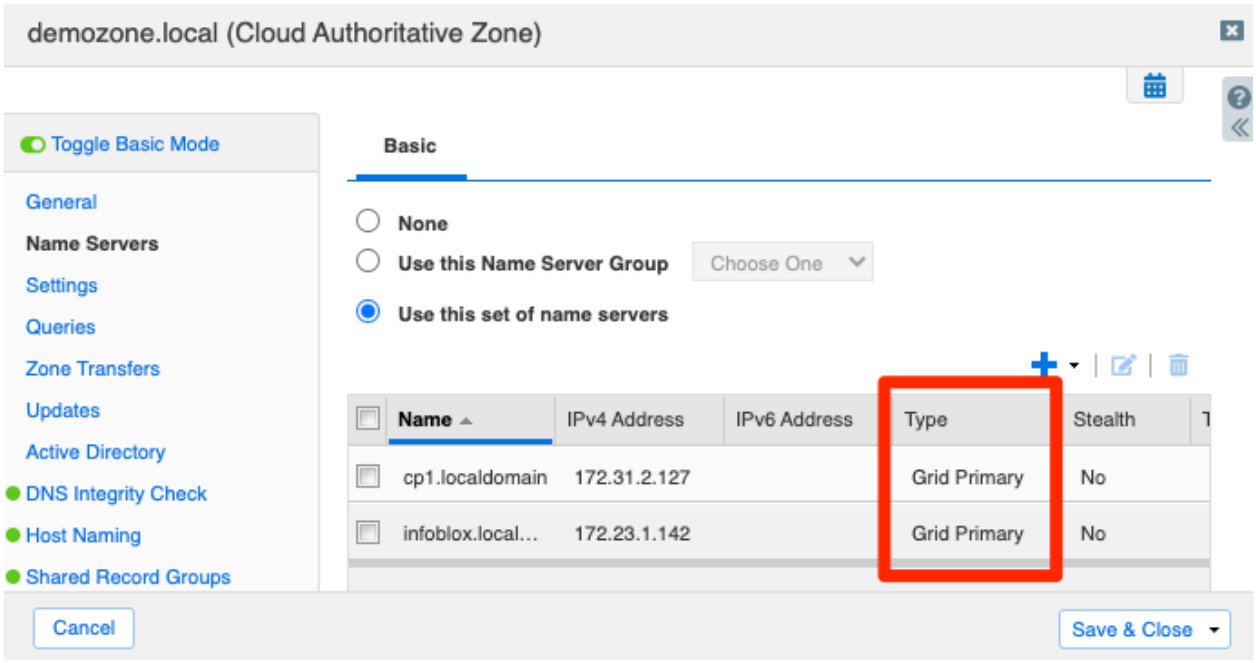
For additional details on adding a Grid Master Candidate, including which virtual appliance models can be used as a GMC, refer to Infoblox documentation: https://docs.infoblox.com/display/nios85/Adding+Grid+Members.

DNS

Highly available DNS services can be provided by ensuring at least two DNS servers, a primary and secondary are specified for each client endpoint. For example, in an AWS VPC, two DNS servers can be specified in a DHCP option set. If the first server is unavailable, the second will be used for DNS resolution. Deploy the primary and secondary DNS servers in different availability zones, regions, or datacenters to increase availability.



Additionally, to increase availability of DNS zones, Infoblox NIOS allows you to configure multiple primary servers for a zone. When you define multiple primary servers for a zone, each server will hold a copy of the zone's authoritative data that can be updated independently.



To resolve any conflicts between zone updates on the multiple primaries, generally the latest update is selected based on the timestamp. Therefore, it is recommended that all DNS primaries have NTP enabled. For additional details and best practices for designating multiple primary DNS servers for a zone, refer to Infoblox NIOS documentation: https://docs.infoblox.com/display/nios85/Assigning+Zone+Authority+to+Name+Servers.

DHCP

Highly available DHCP service can be achieved using DHCP failover. To use DHCP failover, two NIOS/vNIOS appliances are configured with a failover association. The two appliances share a pool of IP addresses to issue to clients. If the Primary DHCP is unavailable, the Secondary is able to continue issuing address leases. To increase availability of appliances in a failover association, they should be deployed in different locations, for example, each in a different region of AWS or one on-premises and one in AWS. For additional details and configuration steps, refer to Infoblox NIOS documentation: https://docs.infoblox.com/display/nios85/DHCP+Failover.

Regions and Availability Zones

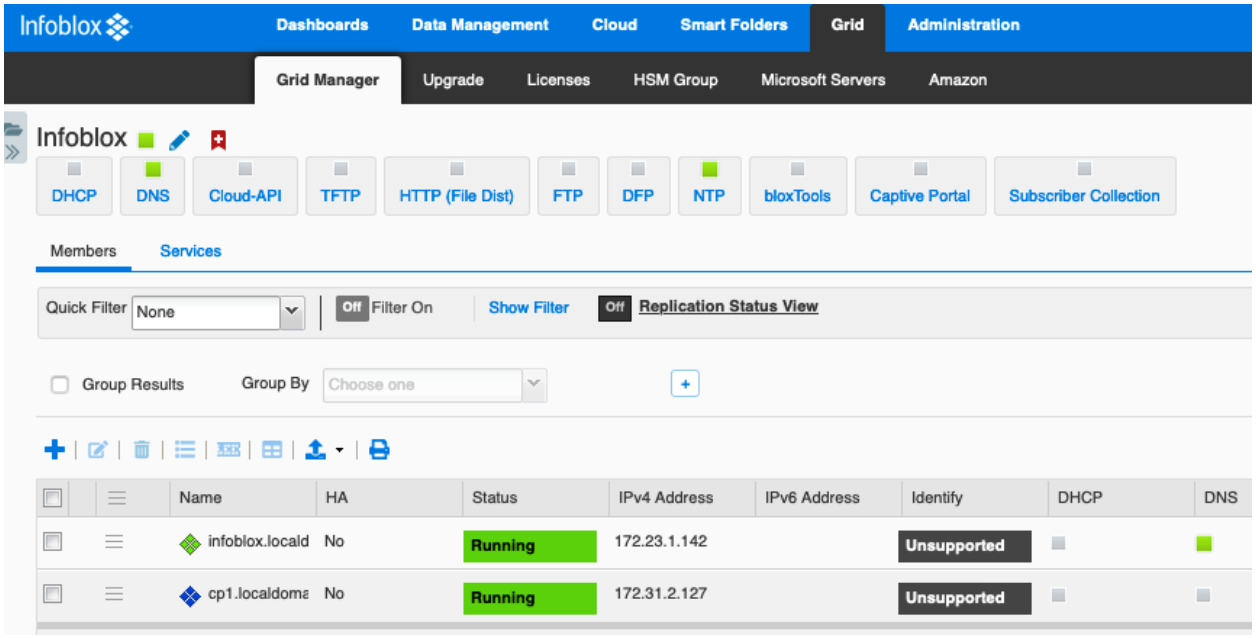
To maximize availability in the configurations described for Grid Master Candidates, DNS, and DHCP, the appliances used for these services should be deployed across multiple Availability Zones and/or Regions. For example, a Grid Master Candidate should be deployed in a different Region than the Grid Master. If the GM fails or connectivity is interrupted due to failures in a specific Region, the GMC in another Region can be promoted to continue Grid services. DNS zones should always use multiple name servers, running in as many different Availability Zones and Regions as feasible. When configuring DHCP failover pairs, the two appliances should be deployed into different Availability Zones.

Operational Guidance

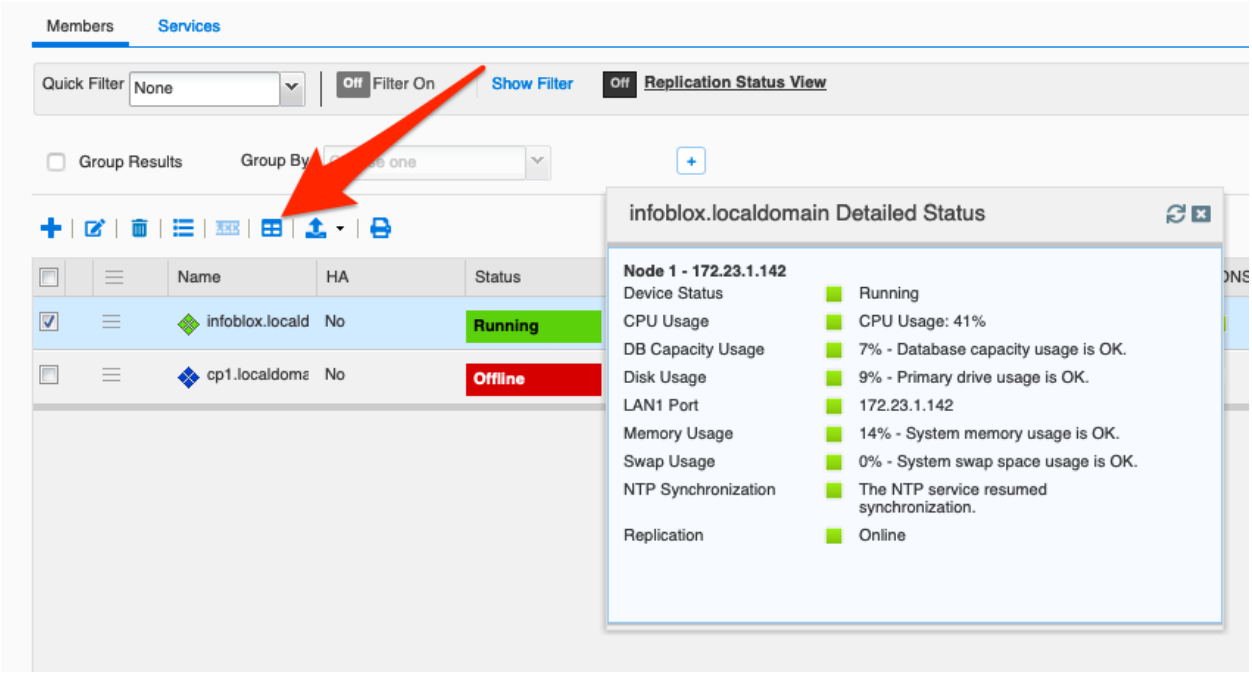
Monitoring

The Infoblox Grid Manager provides monitoring tools for the Grid, Grid members, and services. To view the status, in Grid Manager navigate to the **Grid → Grid Manager → Members** tab.

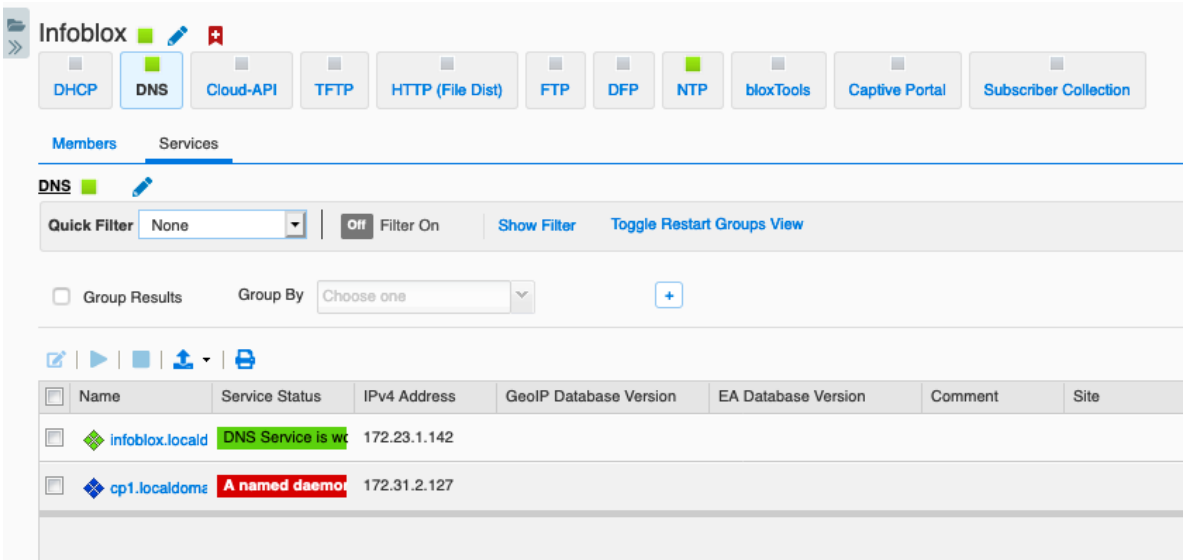
- In the upper left of the tab, next to the Grid name, the small colored square shows the Grid status. **Green** indicates all Grid members are operating normally in a running state. **Yellow** indicates at least one Grid member is connecting or synchronizing. **Red** indicates at least one Grid member is offline or experiencing a different issue.



- Status for individual appliances and virtual appliances is shown in the center pane. Under the status column for each member, the color-coded operational state is shown. To view detailed status on a member, select the member checkbox and click the Detailed Status icon.



- Summary status for services is displayed under the Grid name. Service status on individual members is shown next to the member name. **Green** indicates the service is enabled and running. **Yellow** indicates the service is enabled, but there may be issues requiring attention. **Red** indicates the service is enabled, but it is not running properly. **Grey** indicates that the service is disabled or not configured. To get detailed information on a service's status, navigate to that service's page by clicking on its name. The screenshot below shows the DNS service page.



For additional information on Infoblox Monitoring and Reporting tools and configuration, refer to the Infoblox NIOS documentation: https://docs.infoblox.com/display/NAG8/Part+7+Monitoring+and+Reporting.

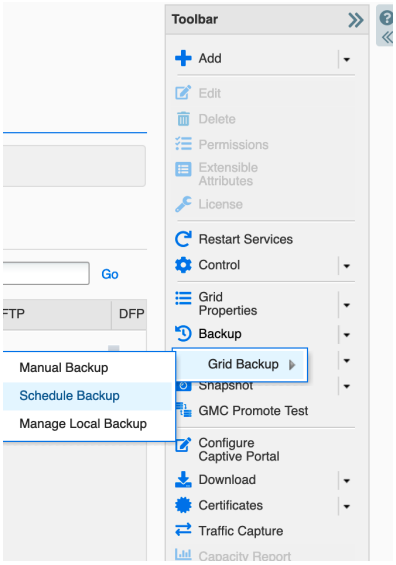
Backup and Recovery

Infoblox recommends that you regularly back up your configuration files and/or discovery database files. You can back up your system files locally on the appliance or to your management system, or use TFTP (Trivial File Transfer Protocol), FTP (File Transfer Protocol), or SCP (Secure Copy) to back them up to a remote server.

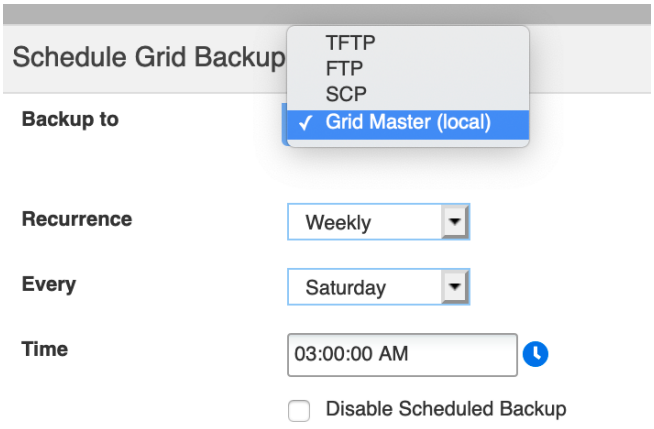
Automated Backup

To configure automatic backup of configuration files and/or discovery database files, use the following procedure:

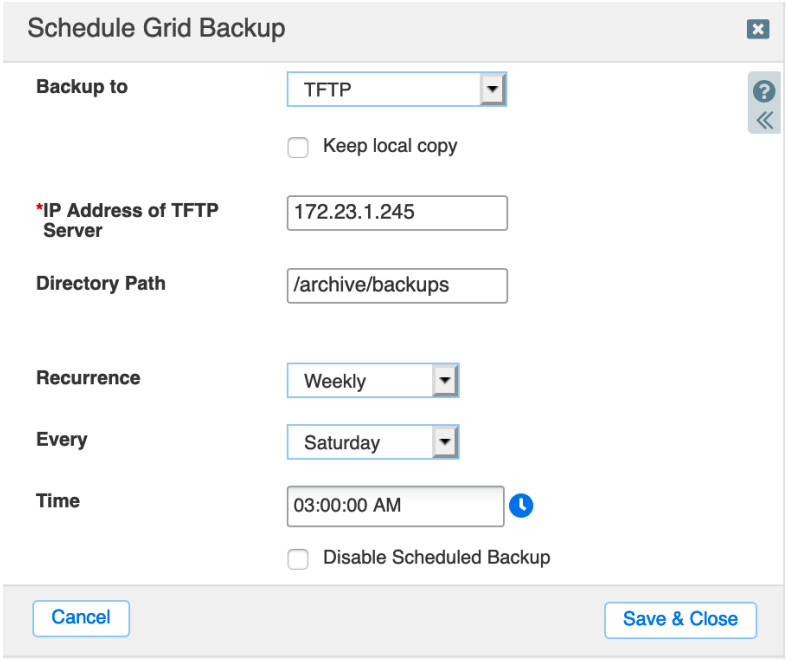
1. In Grid Manager, navigate to the **Grid → Grid Manager** tab.
2. In the **Toolbar**, click the dropdown for **Backup**. Select **Grid Backup** and then **Schedule Backup**.



3. In the Schedule Backup dialog box, select the destination from the **Backup to** dropdown.



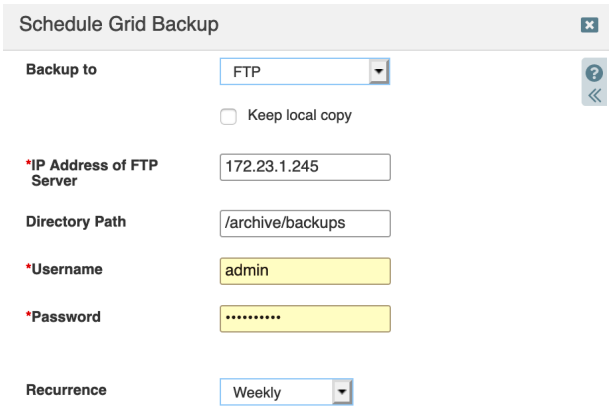
4. Fill in details based on your destination selection:
    a. **TFTP**: Back up system files to a TFTP server.
        - **Keep local copy**: Select this to also save a local copy of the backup file on your appliance. This is disabled by default. The local backup contains only the Grid backup, it does not contain backups for reporting and Network Automation. Note that when you select this, the total backup time will increase.
        - **IP Address of TFTP Server**: Enter the IP address of the TFTP server to which you want to back up the system files.
        - **Directory Path**: Enter the directory path of the file. For example, you can enter **/archive/backups**. The directory path cannot contain spaces. The folder or directory you enter here must already exist on the specified server. Do not include the file name in the directory path.
        - **Recurrence**: Select how often you want to back up the files. You can select **Weekly**, **Daily**, or **Hourly** from the drop-down list. When you select **Weekly**, complete the following:
            - **Every:** Choose a day of the week from the drop-down list.
            - **Time**: Enter a time in the hh:mm:ss AM/PM format. You can also click the clock icon and select a time from the drop-down list. The Grid Master creates a backup file on the selected day and time every week.
        - **Disable Scheduled Backup:** Select this if you want to disable automatic backups from occurring now. You can still save the settings for future use.



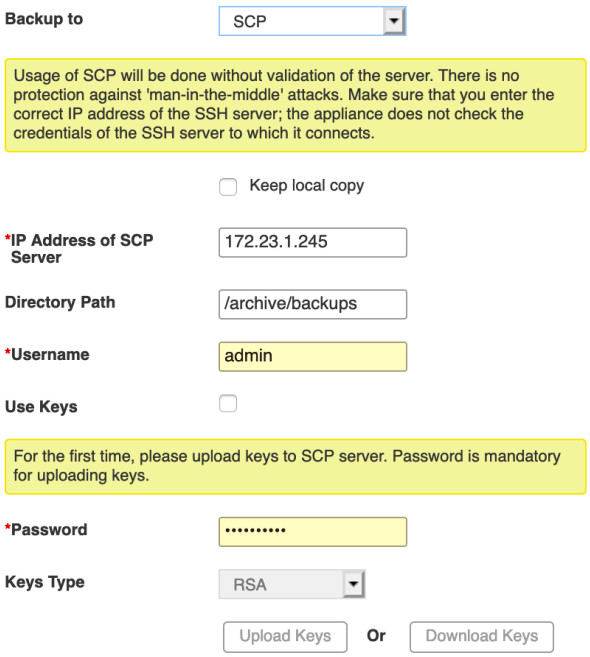
    b. **FTP**: Back up system files to an FTP server.
        - **Keep local copy**: Select this to also save a local copy of the backup file on your appliance. This is disabled by default. The local backup contains only the Grid

backup, it does not contain backups for reporting and Network Automation. Note that when you select this, the total backup time will increase.

- **IP Address of FTP Server**: The IP address of the FTP server.
- **Directory Path**: Enter the directory path of the file. For example, you can enter **/archive/backups**. The directory path cannot contain spaces. The folder or directory you enter here must already exist on the specified server. Do not include the file name in the directory path.
- **Username**: Enter the username of your FTP account.
- **Password**: Enter the password of your FTP account.
- **Recurrence**: Select how often the scheduled backups should occur. You can select **Weekly**, **Daily**, or **Hourly**. For information, see TFTP.
- **Disable Scheduled Backup:** Select this if you want to disable automatic backups from occurring now, but want to save the settings for future use.



c. **SCP**: Back up system files to an SSH server that supports SCP.
   - **Keep local copy**: Select this to also save a local copy of the backup file on your appliance. This is disabled by default. The local backup contains only the Grid backup, it does not contain backups for reporting and Network Automation. Note that when you select this, the total backup time will increase.
   - **IP Address of SCP Server**: The IP address of the SCP server.
   - **Directory Path**: Enter the directory path of the file. For example, you can enter **/archive/backups**. The directory path cannot contain spaces. The folder or directory you enter here must already exist on the specified server. Do not include the file name in the directory path.
   - **Username**: Enter the username of your SCP account.
   - **Password**: Enter the password of your SCP account.
   - Optionally, select **Use Keys** and select keys to Upload.
   - **Recurrence**: Select how often the scheduled backups should occur. You can select **Weekly**, **Daily**, or **Hourly**. For information, see the TFTP section.
   - **Disable Scheduled Backup:**Select this if you want to disable automatic backups from occurring now. You can still save the settings for future use.



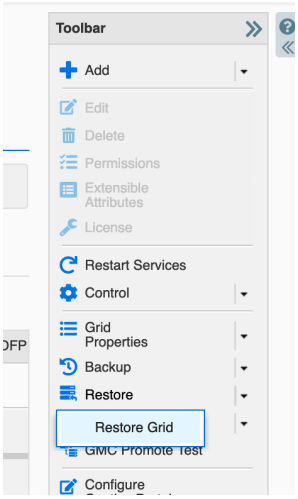
d. **Grid Master (Local)**: Back up to a local directory on the Grid Master. This is the default.
   - **Recurrence**: Select how often the scheduled backups should occur. You can select **Weekly**, **Daily**, or **Hourly**. For information, see the TFTP section.

5. Click **Save & Close**.

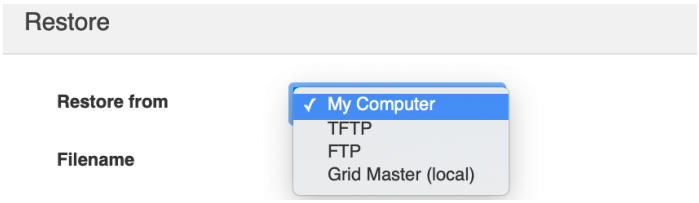
Restoring From Backup

To restore a backup file to a standalone appliance or Grid Master, use the following procedure:

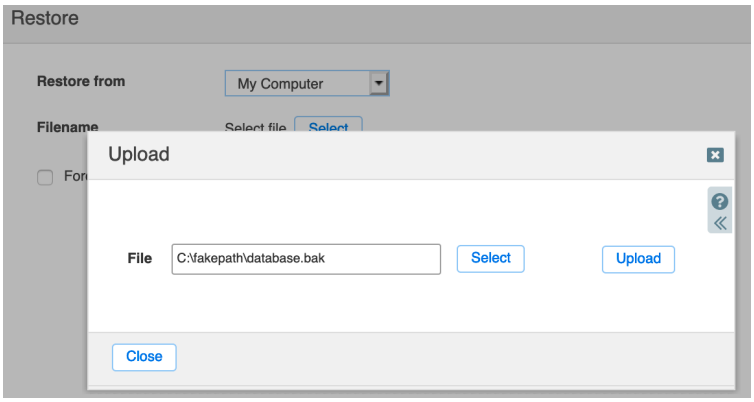
1. In Grid Manager, navigate to the **Grid → Grid Manager** tab.
2. In the **Toolbar**, click the dropdown for **Restore**. Select **Restore Grid**.



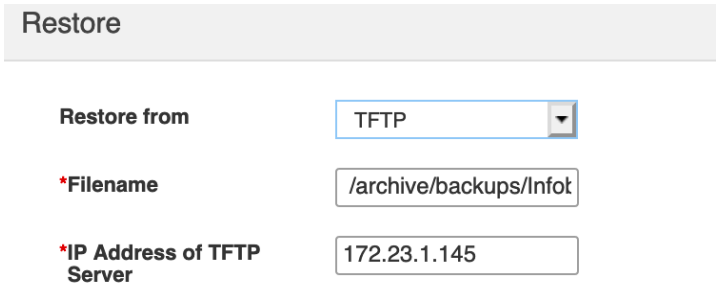
3. In the Restore dialog box, choose a location from the **Restore from** dropdown list.



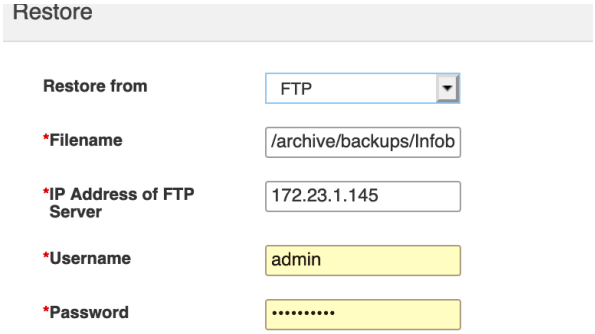
4. Fill in details based on your selection:
    a. **My Computer**: Restore a file from your local computer. This is the default.
        - **Filename**: Click **Select File** to navigate to the configuration file.



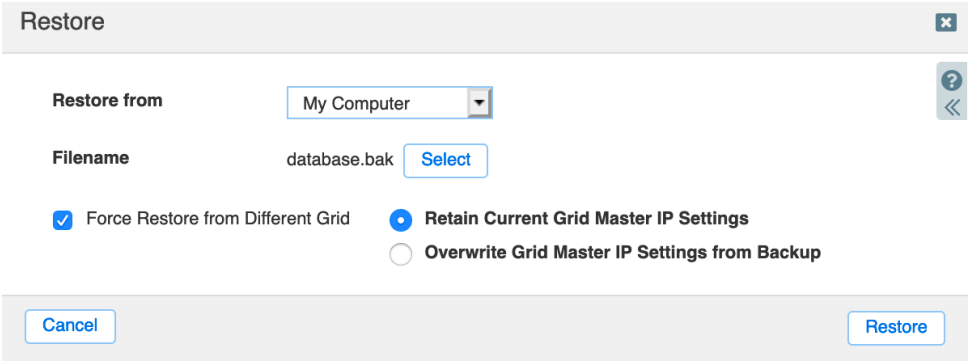
    b. **TFTP**: Restore a file from a TFTP server.
        - **Filename**: Enter the directory path and the file name you want to restore. For example, you can enter **/archive/backups/Infoblox_backup**.
        - **IP Address of TFTP Server**: Enter the IP address of the TFTP server from which you restore the configuration file.



    c. **FTP**: Restore a file from an FTP server.
        - **Filename**: Enter the directory path and the file name you want to restore. For example, you can enter **/archive/backups/Infoblox_backup**.
        - **IP Address of FTP Server**: Enter the IP address of the FTP server.
        - **Username**: Enter the username of your FTP server account.
        - **Password**: Enter the password of your FTP server account.



d. To download a backup file from one appliance to a different appliance, use any of the above sources and select **Force Restore from Different Grid** to enable the feature, and then select one of the following:
    - **Retain Current Grid Master IP Settings** (this is the default)
    - **Overwrite Grid Master IP Settings**



5. Click **Restore**. In the Confirm Restore dialog box, click **Yes**.

Instance Failure

Actions to take if an Infoblox vNIOS for AWS appliance fails differ based on whether the appliance is a Grid Master or Grid Member.

For a Grid Master, Infoblox recommends your Grid has at least one Grid Master Candidate (GMC), an optional designation when adding a member to the Grid. The GMC holds a complete copy of the Grid database. Ideally, the GMC should be deployed in a different location than the Grid Master so an outage is unlikely to affect both (for example, deploy the GM on-premises and the GMC in AWS or deploy GM and GMC to different regions in AWS). If the Grid Master fails, the GMC can be promoted to GM. To promote a GMC, use the following procedure:

1. Establish a serial connection (through a serial console or remote access using SSH) to the Master Candidate.
2. At the CLI prompt, use the command **set promote_master** to promote the Master Candidate and send notifications to all Grid members immediately, or promote the Master Candidate to

the Grid Master immediately and specify the delay time for the Grid members to join the new Grid Master. For more information about the command, refer to the *Infoblox CLI Guide*.

3. To verify the new master is operating properly, log in to the Infoblox Grid Manager on the new master using the IP address of the LAN1 port for a single master.
4. Check the icons in the **Status** column. Also, select the master, and then click the Detailed Status icon in the table toolbar. You can also check the status icons of the Grid members to verify that all Grid members have connected to the new master. If you have configured delay time for Grid member notification, it will take some time for some members to connect to the new master. You can also check your firewall rules and log in to the CLI to investigate those members.

For a Grid with no GMC or a standalone appliance, a new vNIOS appliance can be deployed and restored from a backup as described in the **Restoring From Backup** section of this document.

If a Grid Member fails, actions to take will depend on the services that member was providing. Attempt to restart/restore the member. If this fails, a new member can be deployed and added to the Grid to backfill the role. No restore from backup is necessary as the Grid Master will push configuration to the new virtual appliance.

RTO and RPO

Core network services such as DNS and DHCP provided by the Infoblox Grid should have a recovery time objective (RTO) shorter than that of the most critical application using these services. You can decrease RTO of Infoblox core network services by implementing the highly available, redundant configurations for the Grid, DNS, and DHCP detailed in the **Configuring for Highly Available Services** section of this guide.

The Infoblox Grid is designed to avoid data loss and provide for short recovery point objectives (RPO). Local changes on DNS and DHCP appliances, such as issuing a DHCP lease or updating a DNS record are propagated almost immediately to the Gid Master and vice versa. The Grid database contained on the Grid Master and Master Candidates reflects the real-time state of data across all appliances in the Grid.

The following failure scenarios demonstrate how the Infoblox Grid maximizes availability of services and minimizes RTO/RPO:

1. **Loss of connectivity between a member and the Grid Master**: The member devices will enter a disconnected operation state and continue to provide all services. Any updates bound for the GM are queued until connectivity is restored. When connectivity to the GM is restored, the member will propagate all updates to the GM. Once the GM receives updated data, it will synchronize with all Grid members.
2. **Replacement of a failed appliance or virtual appliance**: Any appliance or virtual appliance of the same type can be used to replace a failed appliance. For example a new vNIOS TE-V1425 instance on AWS can replace a failed TE-V1425. Once the new appliance is configured with the

IP address of the failed one and reaches out to the GM, the following will take place automatically:

a. The new appliance establishes connectivity with the GM.
b. The GM checks the version of software on the replacement member.
c. The GM will download and upgrade the new appliance software to the version running on the Grid.
d. The GM will load all configuration and service data and will start services on the replacement appliance.

3. **Loss of Grid Master**: If the GM fails or becomes unreachable due to network or other failure, all member appliances will enter the disconnected operation state and continue to provide services. At any time, before or after the loss of the GM, an administrator can promote a Grid Master Candidate to the master role as described in the **Instance Failure** section of this guide. The GMC will then assume the role of GM and contact all members informing them of the change.

   If the promotion takes place before a GM is lost, the newly promoted candidate's database will contain an identical copy of the master's database, so time required to re-synchronize between the new GM and members will be minimal.

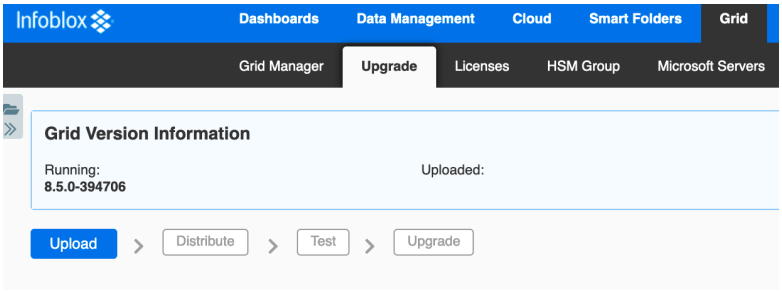
   If the promotion takes place after failure of the GM, and member devices have entered the disconnected operation state, the new GM will automatically re-synchronize the Grid. This can occur in a matter of seconds depending on the total number of objects in the database, bandwidth of network connections, and number of changes that occurred during disconnected operation. At no time is service interrupted on the member devices and synchronization activities are invisible to users.

Routine Maintenance

NIOS Software Patches and Upgrades

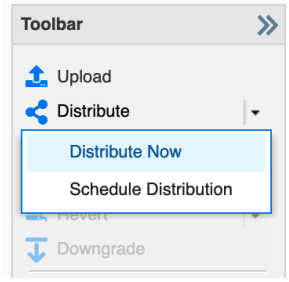
All software patches and updates are controlled and distributed by the Grid Master for members in a Grid. Software updates can be downloaded from https://support.infoblox.com. For detailed information on uploading, distributing, and scheduling/performing software upgrades, refer to NIOS documentation https://docs.infoblox.com. Use the following process to update a standalone appliance or Grid immediately:

1. Download the appropriate upgrade file from the Infoblox support site.
2. Login to your Grid Manager. Navigate to the **Grid** → **Upgrade** tab.
3. Click on **Upload**.

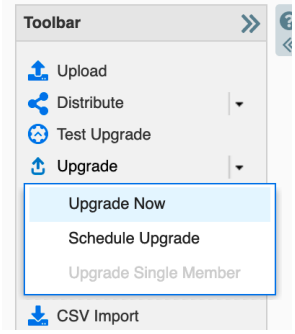


The appliance uploads the file and displays the status of the upload in the status bar. You can click the Stop icon in the status bar to stop the upload. Ensure that you do not navigate away from the **Upgrade** tab until after the upload is complete. Otherwise, the upload process stops.

4. To distribute the software upgrade to each member immediately, including the Grid Master itself, open the dropdown for **Distribute** in the **Toolbar**. Select **Distribute Now**. Click Yes in the Confirm Start Distribution dialog.



5. After distribution is complete, you can optionally test the upgrade on your Grid Master without implementing it. Click on **Test Upgrade** in the **Toolbar** to run this test.
6. To perform the actual software upgrade, open the **Upgrade** dropdown in the **Toolbar** and select **Upgrade Now**.



7. Click **Yes** in the Confirm Start Upgrade dialog box.

Managing Licenses

For full details on managing licenses for Infoblox vNIOS and other services, refer to Infoblox documentation https://docs.infoblox.com/display/nios85/Managing+Licenses. The following important information should be noted regarding subscription licenses.

When a subscription license expires, all features continue to work as is with the following exceptions:

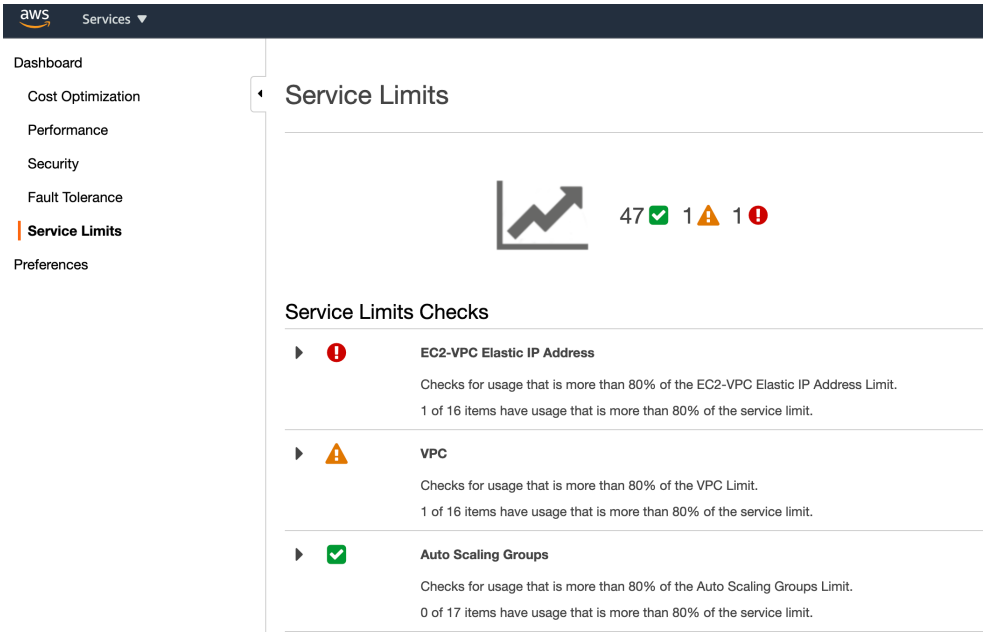
- If the DNS or DHCP license expires, if you add a new authoritative zone or a network, they do not appear in Grid Manager.
- If the Threat Protection or Threat Protection Update license expires, you may experience problems when creating custom rules or publishing data.
- Although NIOS continues to collect data, you will not be able run reports on the data collected during the expired period. After you renew the subscription license, you can run reports on this data.
- Data feeds for features such as RPZ, Threat Analytics, and ADP stop. The services keep running with existing data.

Managing AWS Service Quotas

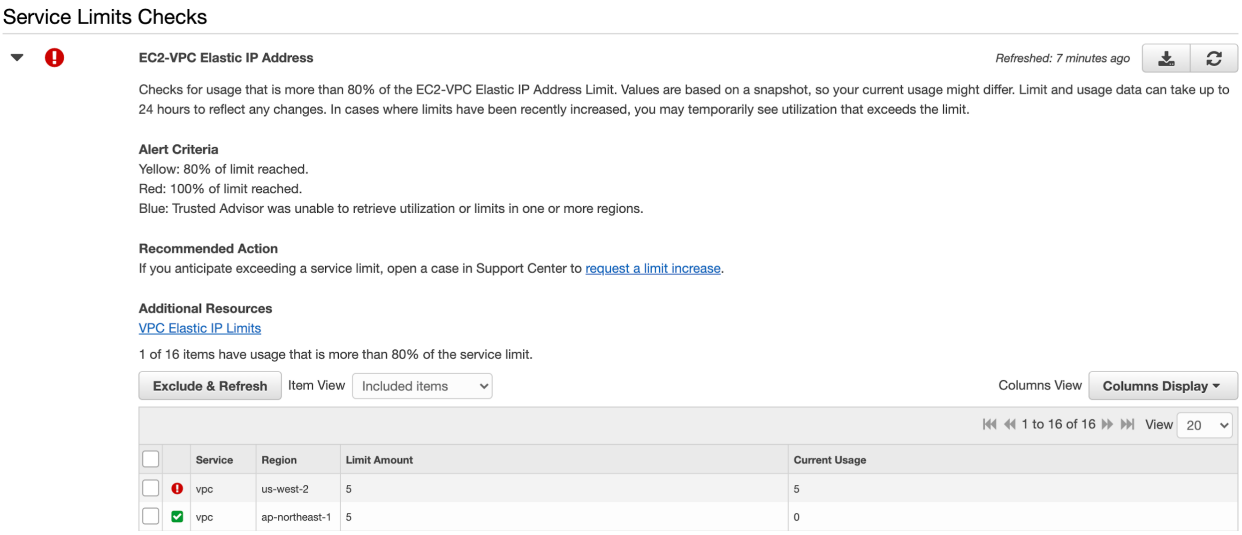
It is important to be aware that each AWS account has default quotas/limits, setting a maximum number of each resource type you can deploy. For example, there is a limit on how many EC2 instances you can deploy in each region. It is especially important to consider these quotas when planning for high availability and disaster recovery. For additional information on Service Quotas, including how to request increases, refer to AWS documentation: https://docs.aws.amazon.com/general/latest/gr/aws_service_limits.html.

The following is one method available to check your limits and usage:

1. In the AWS Management Console, Use the Services menu to navigate to **Trusted Advisor** under Management & Guidance.
2. Select **Service Limits** from the Trusted Advisor menu.



3. Expand any of the categories to view details on the service limit and your usage.



In the above screenshot, you can see this account has reached the limit for Elastic IP Addresses in the US West 2 region.

Emergency Maintenance

Infoblox recommends that you deploy a full Grid with availability and fault tolerance in mind to avoid outages. The most common issue that can affect performance of an Infoblox vNIOS for AWS instance serving as a Grid member, caused by transient failure of services, is loss of network connectivity with the Grid Master. In many cases, no action is necessary; the member will continue to provide services such as DNS. When connectivity with the Grid Master is restored, the member will resynchronize with the Grid. For a more permanent failure, actions depend on the role of your vNIOS for AWS instance in the Grid. For failure of a Grid Master, you should promote a Grid Master Candidate as described in the Backup and Recovery section of this guide. For a Grid member, a new instance should be deployed and added to the Grid, also described in the Backup and Recovery section of this guide.

Support

Receiving Support

Infoblox Support is available for customers with active maintenance contracts via Web, Chat (for certain products), and Phone. Infoblox offers options for maintenance contracts to fit your organization's needs. Details can be found here: https://www.infoblox.com/support/.

Service Level Agreements

Service Level Agreements (SLA) are based on the maintenance contract the customer has and the severity of the case. Details on the SLA matrix can be found here: https://www.infoblox.com/company/legal/terms-premium-maintenance/.

Additional Services

In addition to our world-class support, Infoblox offers the following services to ensure our customer's success:

- **Professional Services**: Infoblox Professional Services help you maximize your investment in your network infrastructure and your Infoblox products by giving you a holistic view of your network. Our experienced and highly skilled consultants work with you in depth to understand your organization's unique challenges and goals, design strategies to help you meet these challenges and achieve your business goals, while reducing the total cost of ownership. For more information see: https://www.infoblox.com/support/professional-services-overview/.
- **Education Services**: Drive the success of your Infoblox implementation with the learning path that works for you! Infoblox Education provides learning options that work for your role – Operator, Administrator, or Architect – and your learning style. Interested in an introduction to Infoblox powerful products or quickly getting up to speed on our most popular product features – then get started with our Free Learning. If hands-on training delivered by an Infoblox expert is more your style, then check out our courses at https://www.infoblox.com/infoblox-education/.

Additional Resources

- AWS EC2 Documentation: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/concepts.html.
- Infoblox NIOS and vNIOS Documentation: https://docs.infoblox.com.
- In addition to the method detailed in this guide, vNIOS for AWS instances may be deployed using automation platforms such as AWS CloudFormation: https://blogs.infoblox.com/community/deploying-vnios-for-aws-with-cloudformation/

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