DEPLOYMENT GUIDE

Infoblox vNIOS for Microsoft Azure

Table of Contents

Introduction

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

Infoblox NIOS is the underlying software running on Infoblox appliances and provides core network services and a framework for integrating all the components of the modular Infoblox solution. It provides integrated, secure, and easy-to-manage DNS (Domain Name System), IPAM (IP address management) and other services.

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

Prerequisites

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

- Valid subscription for Microsoft Azure.
- Permissions to create Resource Groups, Virtual Networks, Virtual Machines, and App Registrations in your Azure subscription.
- Understanding of basic networking concepts and tools, including public and private IP addressing, DNS, Secure Shell (SSH), and command line/terminal applications.

Workflow

The following outline lays out the basic steps to deploy and configure Infoblox vNIOS in a new Azure subscription:

1. Deploy vNIOS VM using the Azure Portal.
2. Connect to Azure vNIOS Appliance.
3. Configure the vNIOS Appliance.
4. Configure Azure VNet DNS server.
5. Perform vDiscovery for Azure.

Azure Objects

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

- **Azure Subscription**: An account which is used to access Azure services and through which billing is managed.
- **Azure Marketplace**: An online storefront where applications and other services (including virtual machines) can be hosted or purchased.
- **VNet**: A virtual network where individual subnets and other network settings (such as security groups) are applied.
- **VNet Peering**: Connects one or more (non-overlapping) VNets together.
- **Network Security Group**: The configuration where port access can be allowed or blocked (firewall).
- **Availability Zone**: Physically and logically separated datacenters within an Azure region, connected by an extremely low-latency network.
- **Storage Account**: Holds the image files for the OS or boot diagnostics for a VM.
- **Resource Group**: A container which holds objects such as VM's and their related resources and can be used to simplify management of all objects within that resource group.
- **Express Route**: A direct connection between an ISP and the Azure Cloud which is used to provide faster and more secure connections.
- **Virtual Network Gateway**: The connection point that is used as part of a VPN gateway and enables connectivity between different vNets or VPN tunnels.

Infoblox vNIOS for Azure Use Cases

The following are some of the common use cases for the Infoblox vNIOS for Azure appliance:

- Providing DNS and RPZ/DNS Firewall services from within the Azure cloud for Azure, on-prem, and public clients.
- Expanding services to the Azure cloud for additional fault tolerance and disaster recovery (DR) purposes.
- Providing services with maximum availability and across multiple VNets.
- Add Reporting and Analytics to the Infoblox Grid.

- Network Insight for IPAM discovery.

DNS and RPZ Services

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

Fault Tolerance and Disaster Recovery

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

Maximum Availability

In many cases, it can be a challenge to implement services in a way that maximizes availability across a distributed environment in a secure manner and without deploying more resources than are required. One method for accomplishing this may be by leveraging 'management' or 'transit' VNets where critical services, including your Infoblox servers, operate from. VNet peering can be used to connect other VNets to the management VNet. This allows for seamless communications between those VNets and the management VNet, without allowing connectivity between the other subnets. Traditional routing and/or VPN's can also be used to allow connectivity into the management VNet for VNets which cannot leverage VNet peering or even for networks from outside of Azure.

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 Azure allows you to migrate workloads from data center to the cloud and take advantage of the reliability and high availability of Azure deployments.

Network Insight

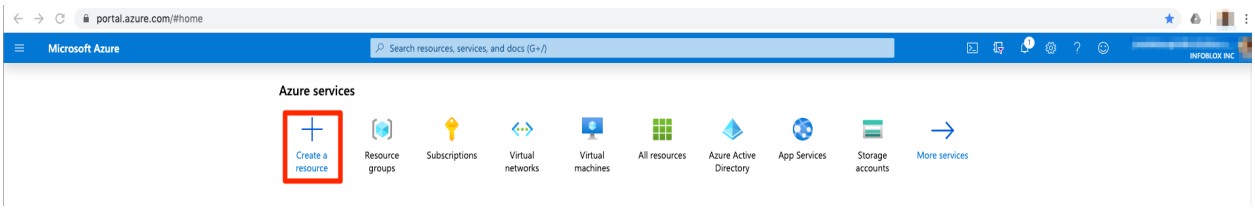
Infoblox Network Insight automates network discovery and provides a unified network view of layer 2 to layer 3 devices connected to the network such as routers, switches, load balancers, SDN and SD-WAN devices, virtual devices etc. Built on Infoblox's flagship solution NIOS DDI, Network Insight enables

authoritative IP address management with enhanced visibility. It enables network administrators to easily gather, correlate, and view network data to increase agility, reduce risk and lower cost. Thus, it provides unprecedented on-prem network visibility for network management, eliminates conflicts and outages, improves operational efficiency and silos with streamlined workflows, and simplifies audit and compliance.

Deploy vNIOS From Azure Marketplace

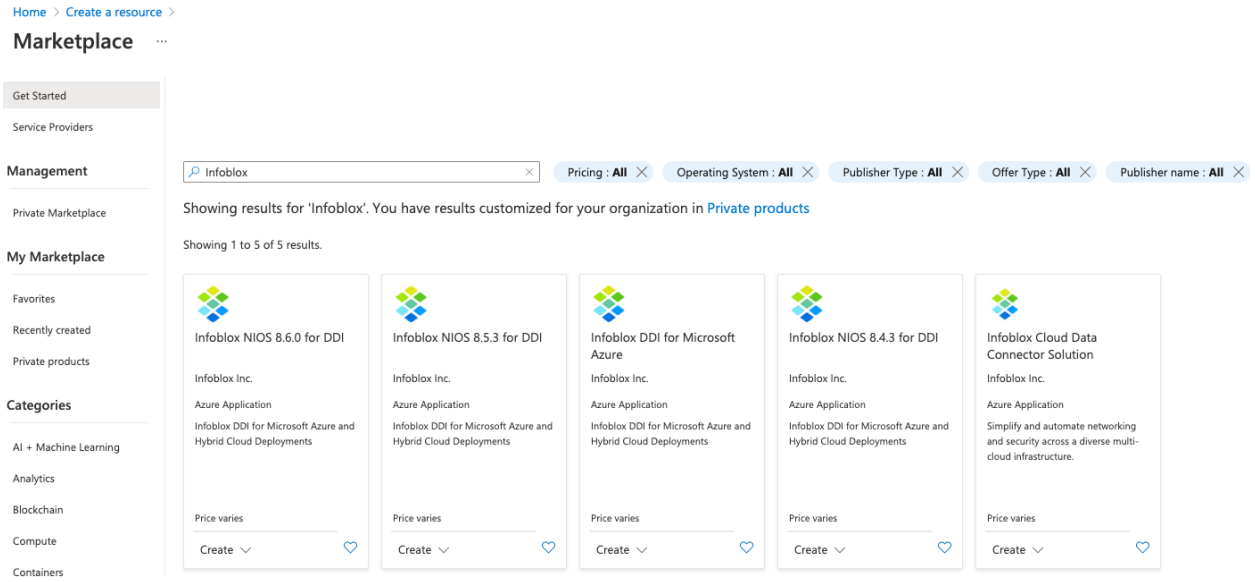
1. Login to the Azure Portal at https://portal.azure.com.

2. Click on **Create a resource**.



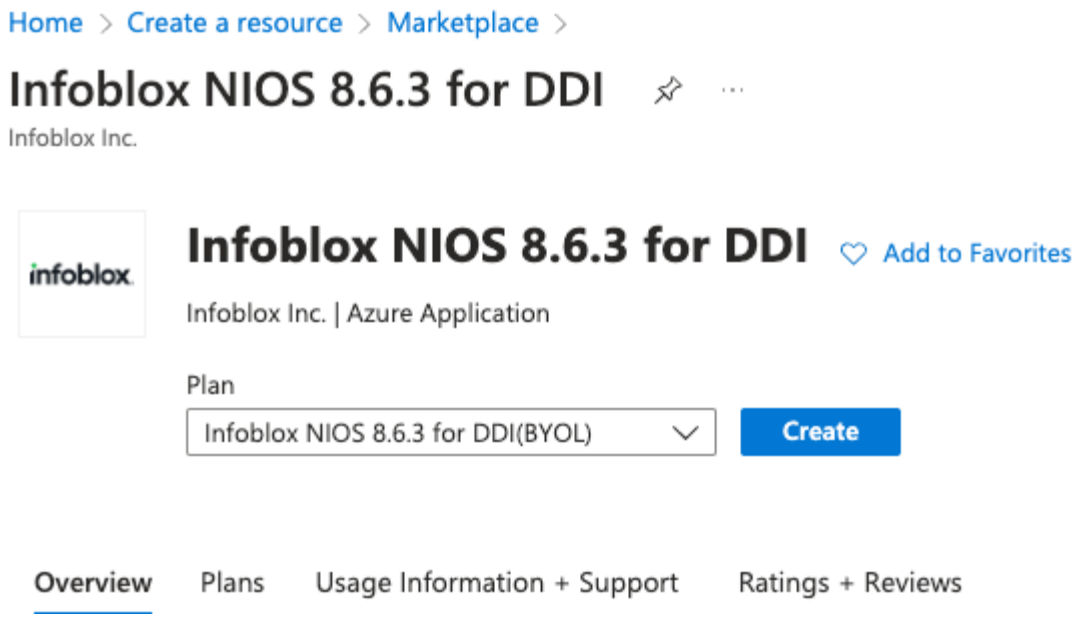
3. In the Azure Marketplace search box, type **Infoblox** and press **Enter**.

4. Click the latest Infoblox vNIOS for Azure offering.



Note: Offerings can change often as new vNIOS versions are released. Versions currently available may vary from those displayed here.

5. Review the Overview page and click **Create**.



Basic Configuration

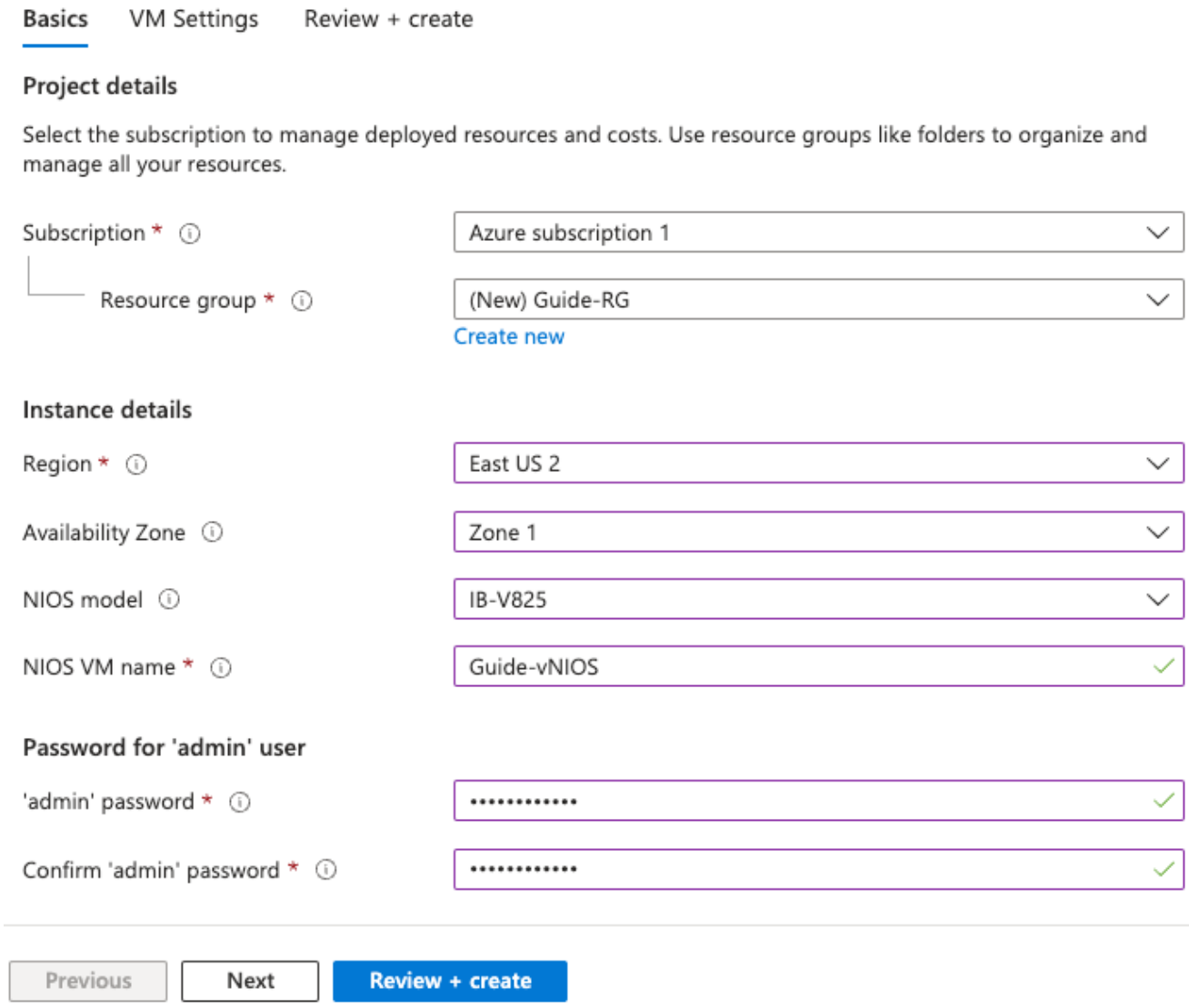
6. On the Basics tab, select the desired **Subscription** from the dropdown if you have more than one.
7. Under Resource group, click **Create new**. Name the resource group and click OK.

Warning: When setting up vNIOS deployment through the Azure Portal, a new or empty resource group is required.

8. Select a R**egion** from the dropdown.
9. Select an **Availability Zone** from the dropdown if the region supports this. *Note: This selection is available for NIOS 8.6.3 and later versions.*
10. Select a **NIOS model** from the dropdown.
11. Enter a **Name** for the vNIOS VM.
12. Enter and confirm a **Password** for the admin user.

Note: The password must be between 12 and 72 characters long, and contain characters from all of the following groups: uppercase letters, lowercase letters, numbers, and special characters. Additionally, Azure does not allow some specific passwords. The list can be found here: https://docs.microsoft.com/en-us/azure/virtual-machines/windows/faq#what-are-the-password-requirements-when-creating-a-vm-.

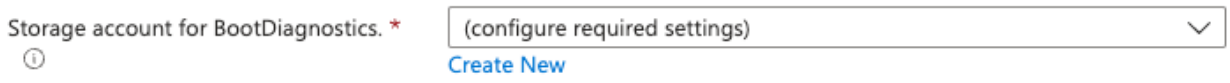
13. Click **Next** for **VM Settings**.



Disks and Storage

14. On the VM Settings tab, under Storage account for BootDiagnostics, click **Create New**.

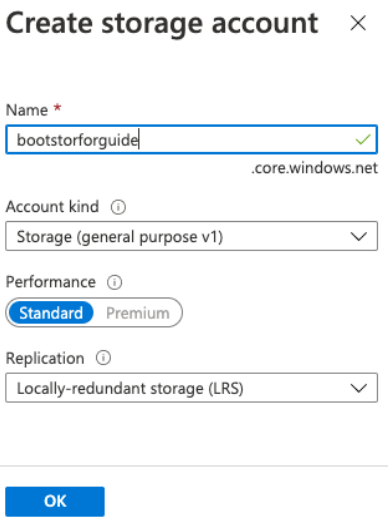
Note: You can alternatively select an existing storage account from the dropdown.



15. On the Create storage account blade, enter a **Name** for the storage account.

Note: Azure requires that the storage account name must be globally unique.

16. Click **OK**.

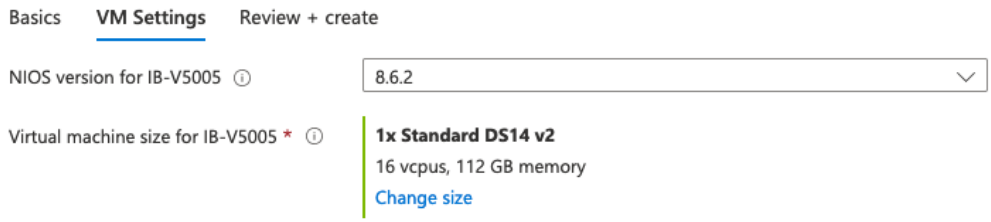


Reporting Appliance

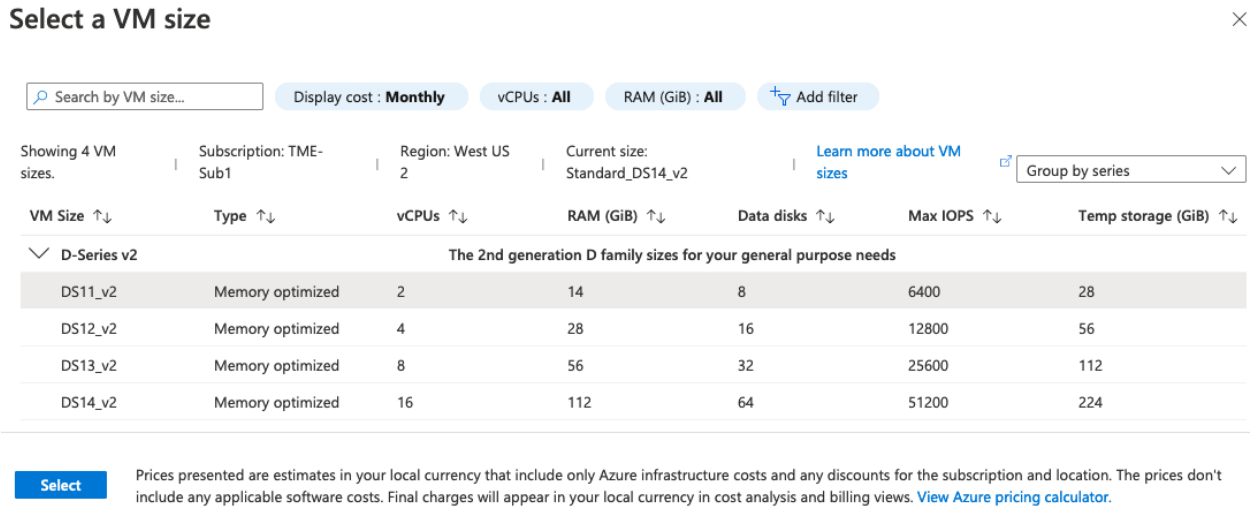
17. When deploying the IB-V5005 reporting appliance, you can select a desired VM size and an additional data disk is required. If not deploying an IB-V5005, skip to step 20.

Note: Infoblox has validated the IB-V5005 with DSv2 VM series and recommends you choose a VM from this series.

a. Click on **Change size** to select a VM size.

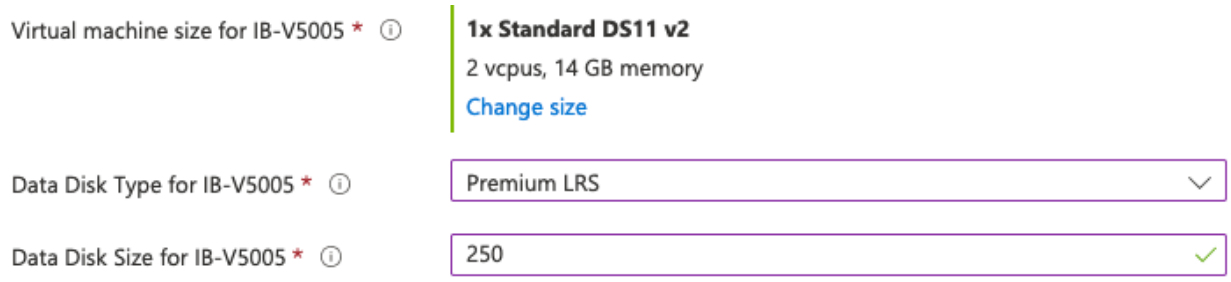


b. Select your desired VM size and click **Select**.



c. Use the dropdown to select a **Data Disk Type**.

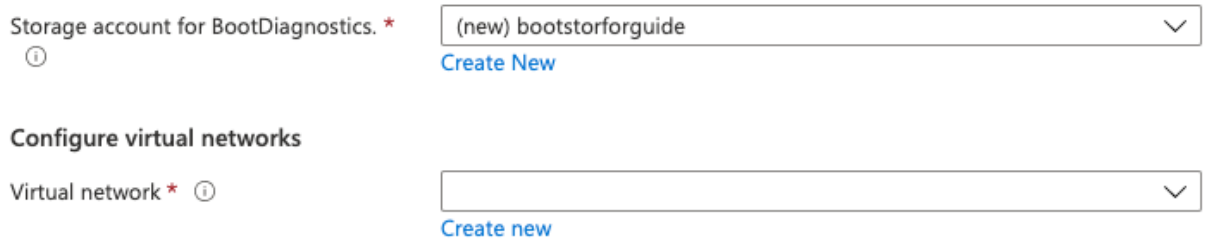
d. Enter a **Data Disk Size**, minimum is 250GB.



Networking

18. On the VM Settings tab, under Virtual network, click **Create New**.

Note: You can alternatively select an existing Virtual network from the dropdown. The VNet used to deploy vNIOS must have at least 2 subnets. You should also ensure the VNet has sufficient IP space for all interfaces you will eventually deploy.



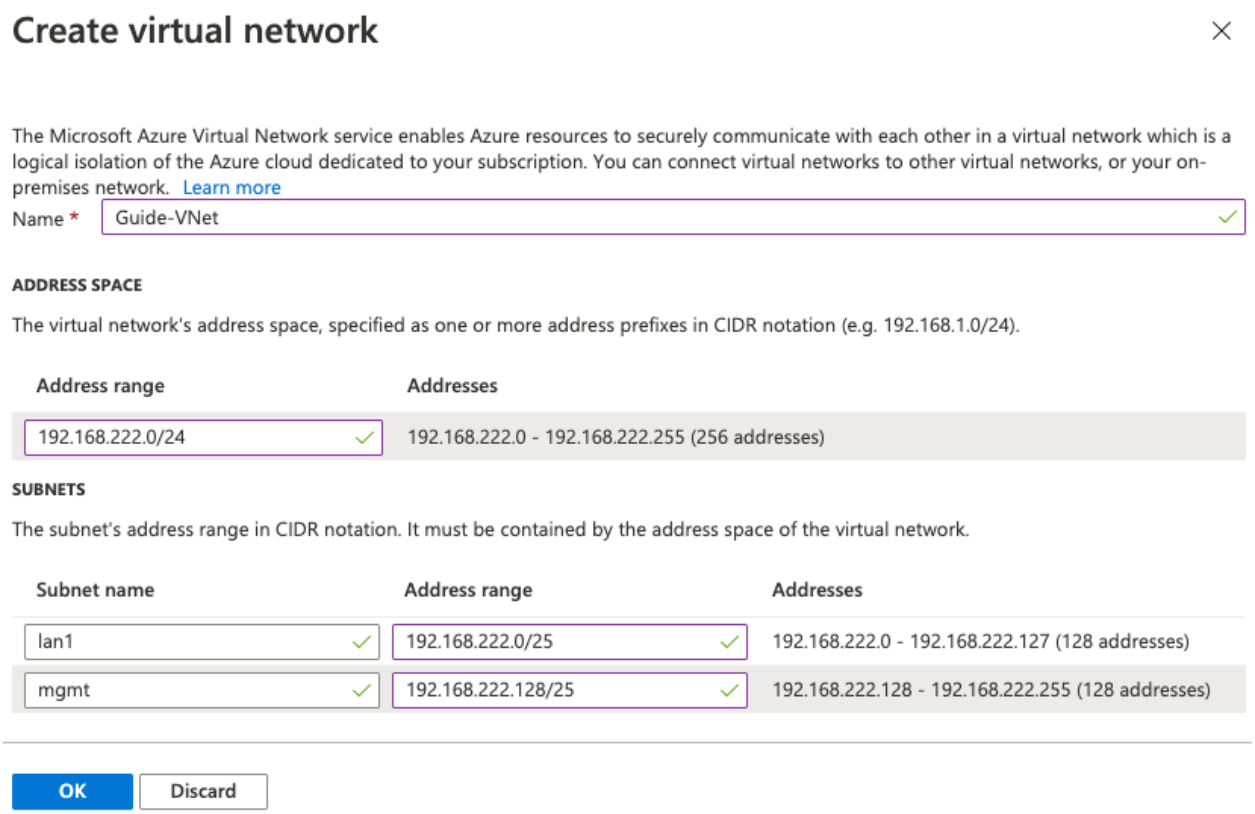
19. On the Create virtual network blade, enter a **Name** for your VNet.

20. Under **Address range**, leave the default or specify an address space in CIDR notation, for example **192.168.222.0/24**.

21. Under **Subnets**, leave the default names or enter **Names** for your subnets.

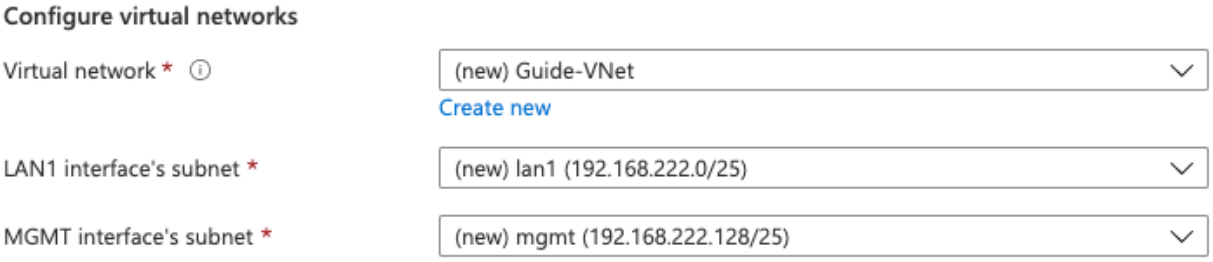
22. For the subnet address ranges, leave the defaults or specify address spaces for each subnet in CIDR notation, for example **192.168.222.0/25** and **192.168.222.128/25**.

23. Click **OK**.

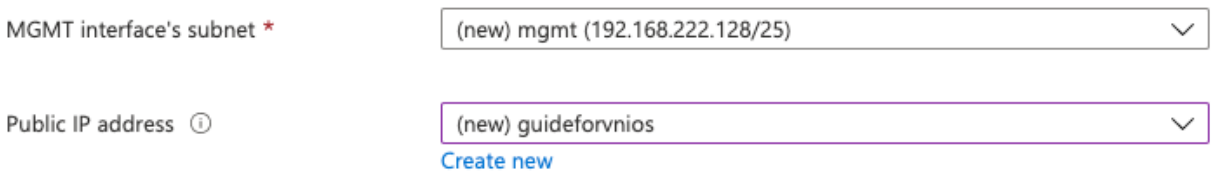


24. On the VM Settings tab, use the dropdowns to select the desired subnets for the vNIOS LAN1 and MGMT interfaces.

Note: LAN1 is the default primary interface. Using the MGMT interface requires configuration via the NIOS CLI or Grid Manager GUI after deployment.



25. For Public IP address, select **New** or **None** from the dropdown. If you need a Public IP, click **Create new**.



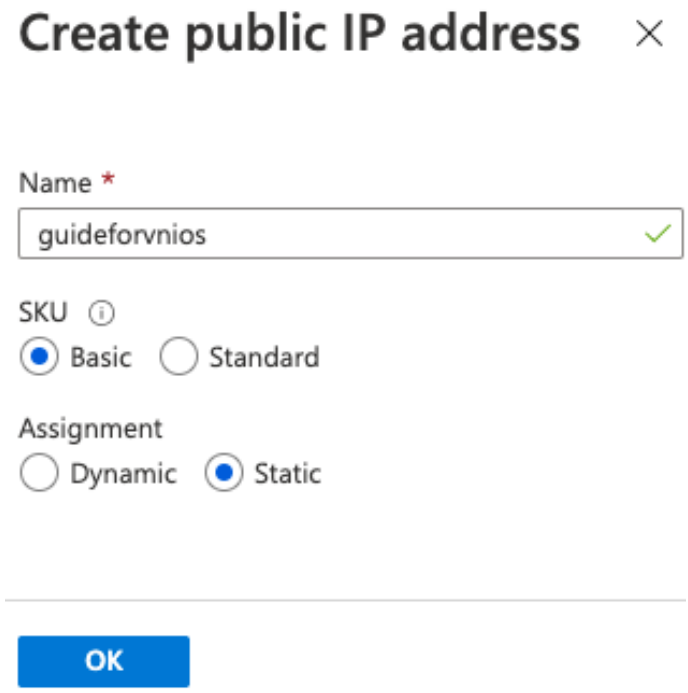
26. If you are creating a Public IP, on the Create public IP address blade, enter a **Name** for the address resource.

27. Select **Basic** or **Standard** for SKU.

Note: If you plan to use a load balancer with your vNIOS for Azure VM, the Public IP SKU must match the SKU of the load balancer.

28. For Assignment, select **Dynamic** or **Static** (Static is recommended for production use).

29. Click **OK**.

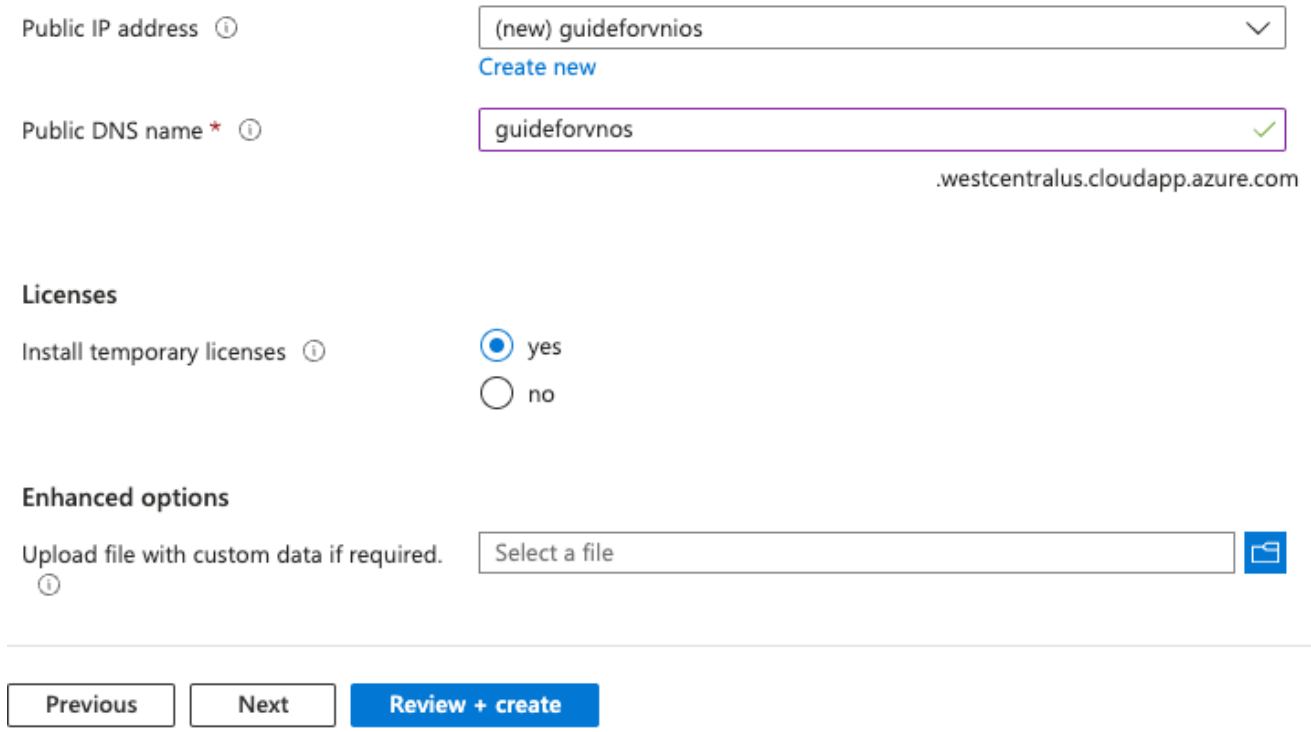


30. On the VM Settings tab, if you are using a Public IP address, enter a **Public DNS name**.

31. Under Licenses, select **yes** to install temporary licenses for NIOS, Grid, DNS, RPZ, and Cloud.

32. Enhanced options can be used in coordination with Infoblox Support for specific use cases. This is outside the scope of this guide.

33. Click **Next: Review + create**.

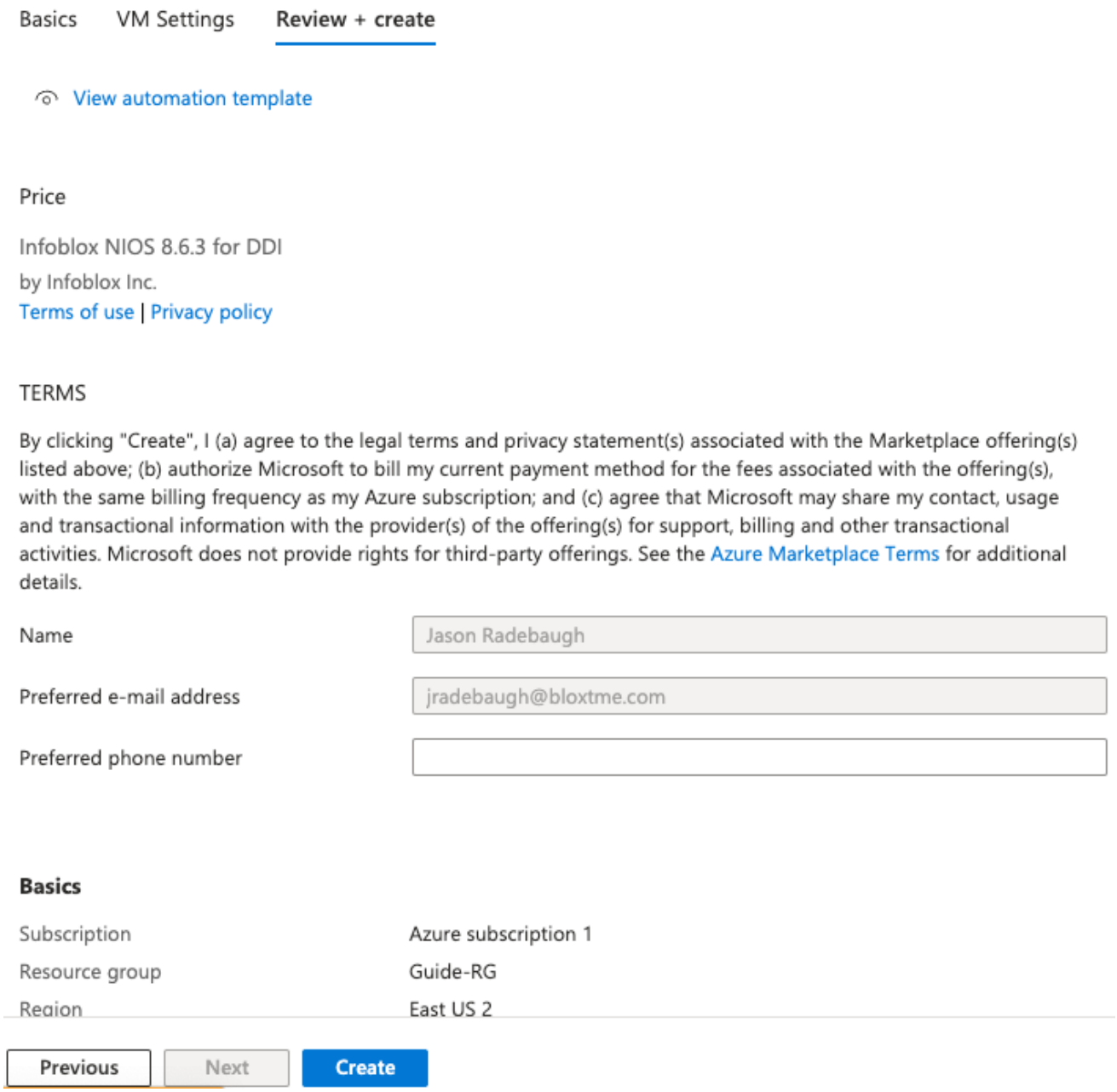


34. On the Review + create tab, Azure will validate your configuration.

Review and Create

35. Once the validation is passed, you can review details. If the validation does not pass, fix any identified errors.

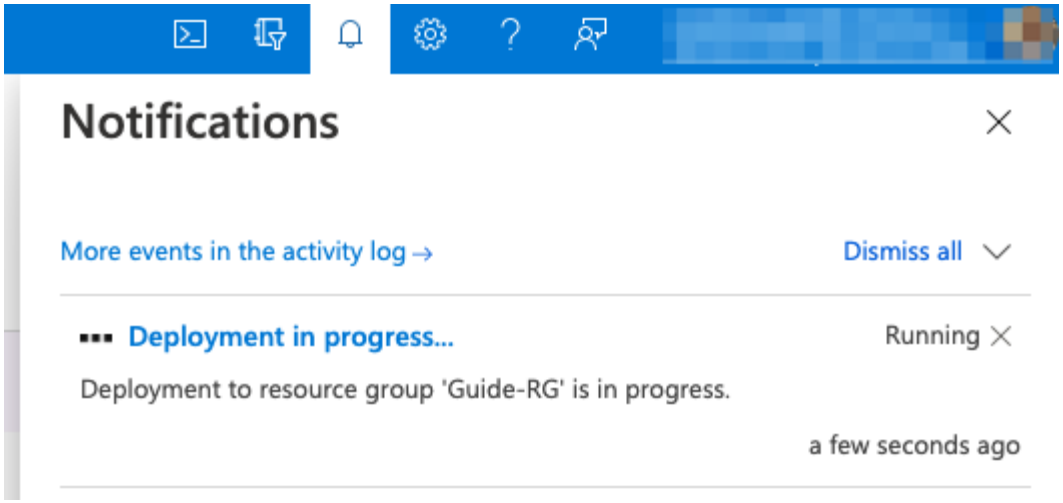
36. Click **Create**.



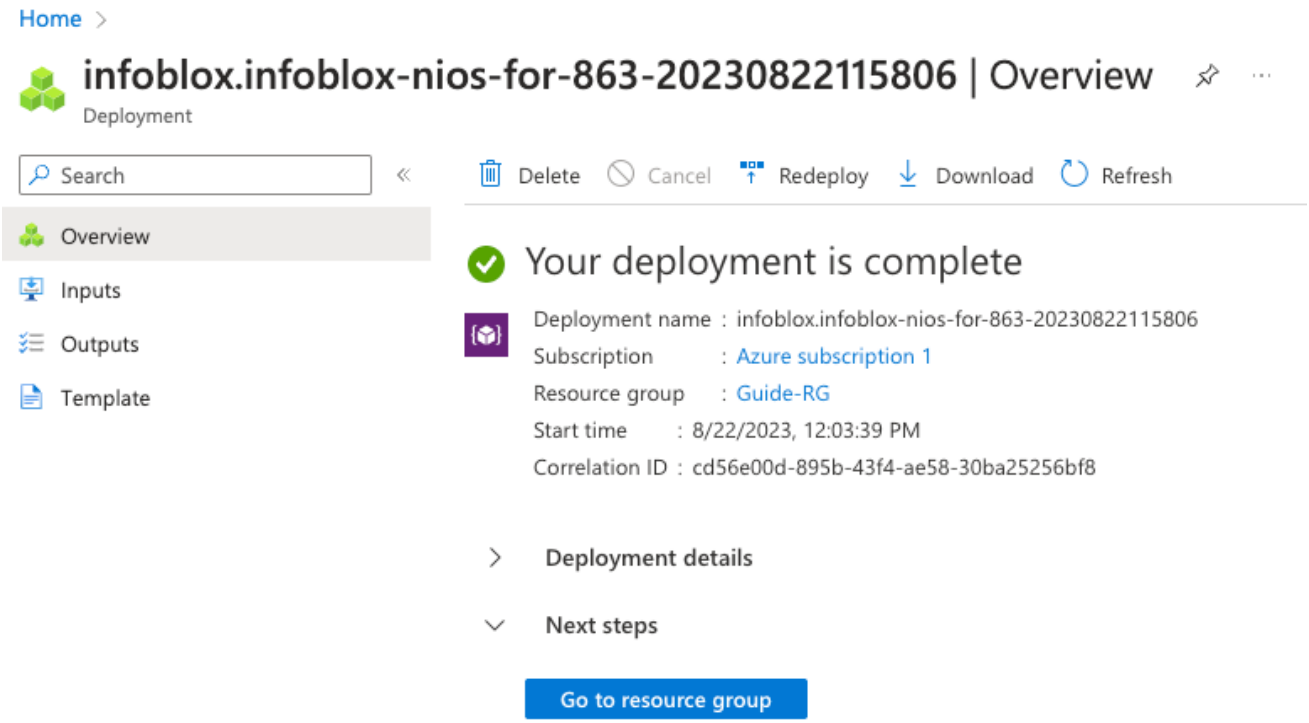
Monitoring Deployment

To monitor the progress of your deployment:

1. Near the top right corner of the Azure Portal, Click on the Notifications button.
2. Click on **Deployment in progress**.



3. Watch for the status of the deployment to show complete.



4. Click on **Go to resource group** to find the resources you deployed.

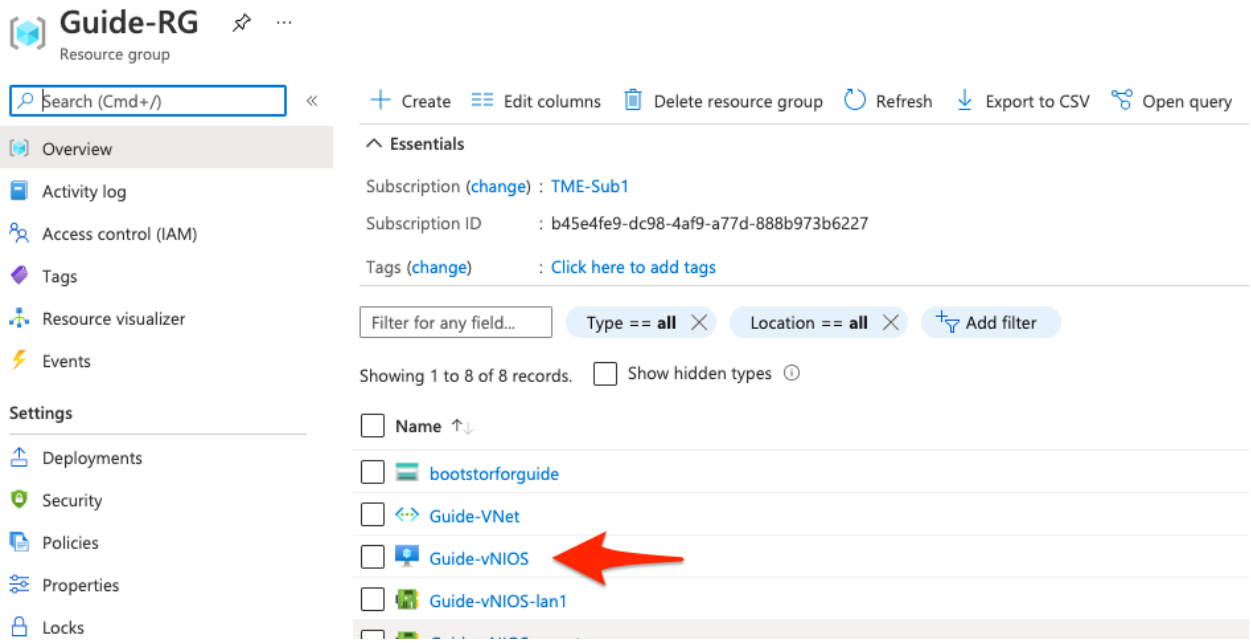
Connect to and Configure Infoblox vNIOS in Azure

The vNIOS for Azure appliance can be added as a member to an existing on-premise or multi-cloud grid, or configured as a new grid running entirely in Azure. To add your vNIOS appliance to an existing grid or for other use cases not covered by this guide, refer to the NIOS Administrator guide or other documents available at https://docs.infoblox.com.

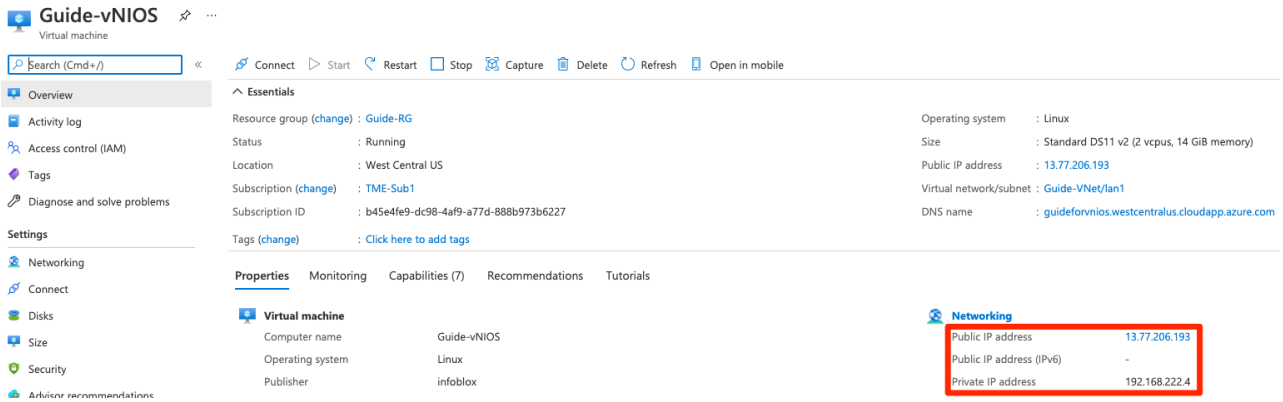
Find Private and Public IP Addresses of vNIOS

Before configuring your vNIOS for Azure appliance, you need to find the private and public (if used) IP addresses for this VM. The private and public (if used) IP addresses will be used to connect to the VM and in the configuration process.

1. In your Resource Group, click on the new VM.



2. On the overview page of the VM blade, locate the Public and Private IP addresses.



Connect to vNIOS for Azure Appliance

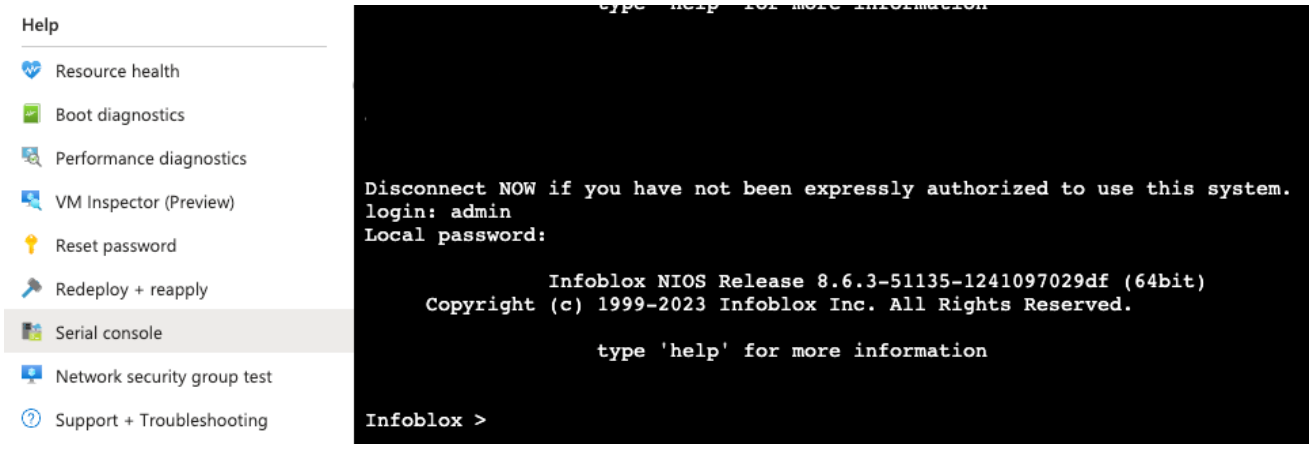
There are three methods available by default to connect to your vNIOS appliance in Azure: Virtual Serial Console, SSH, and the Grid Manager GUI.

Virtual Serial Console

1. From the Overview page of your VM, scroll to the bottom of the VM menu.

2. Click on **Serial console**, under the Help section.

3. This will open a virtual serial console in your browser. Login with the default username: **admin**, and the password you created during deployment.



4. Once you are logged in to the console, 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.

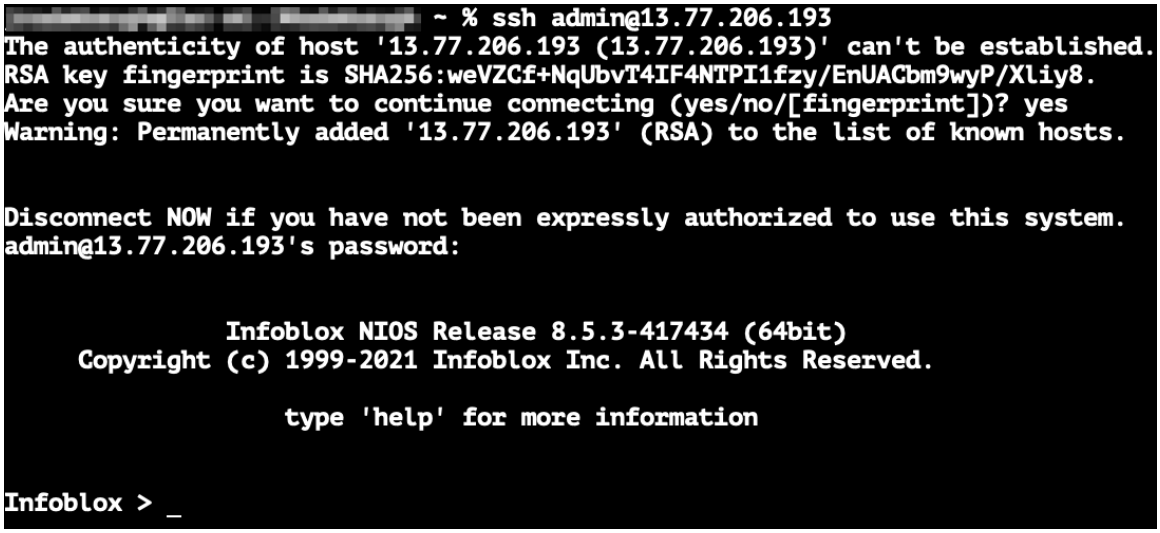
Secure Shell

1. Open a PowerShell or Terminal window on your computer.

2. Use the command **ssh admin@<ip_address>** to start the SSH connection (use the public or private IP of your VM, based on your connection to Azure).

3. When prompted, type **yes** to add the IP to your known hosts.

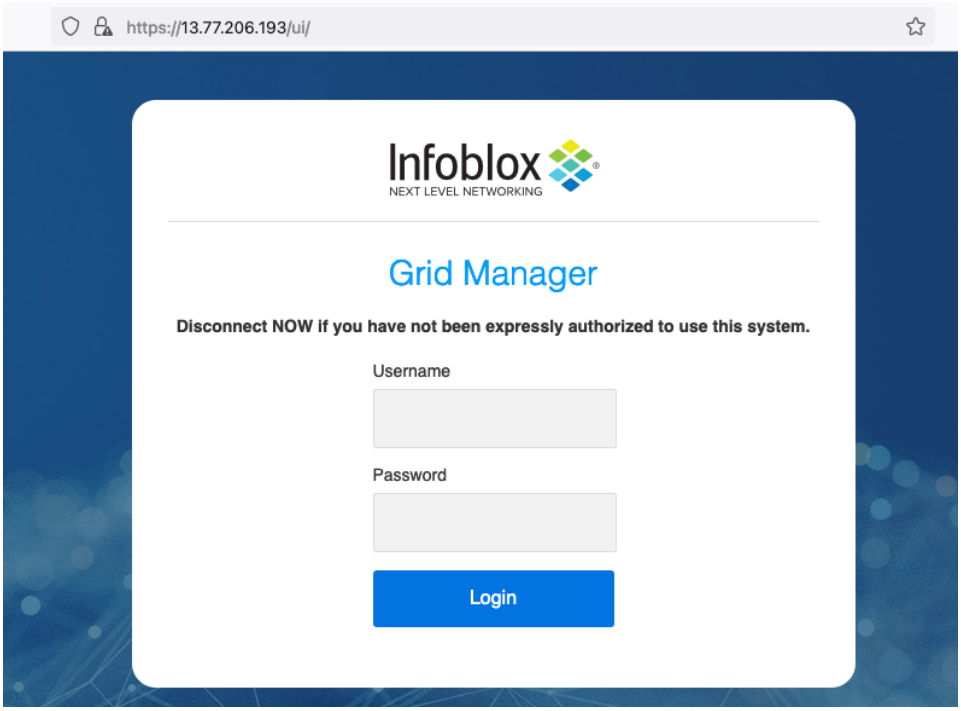
4. Enter the **password** you created during deployment.



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

Grid Manager GUI

1. Open a web browser.
2. Enter **https://<ip_address>** (use the public or private IP of your VM, based on your connection to Azure).



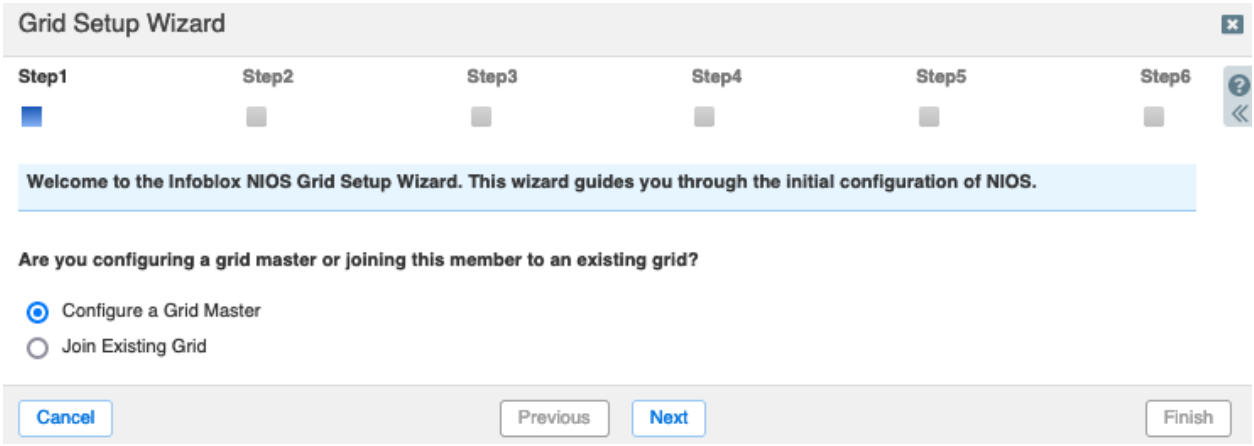
Note: Newly deployed NIOS uses a self-signed certificate. Warnings about the connection being insecure are to be expected and might require that you add an exception before being able to connect.

3. Login with the username **admin** and the password you created during deployment.
4. Read and accept the Infoblox End-User License Agreement.
5. Read the Data Collection and Opt-Out Notice and click **OK**.

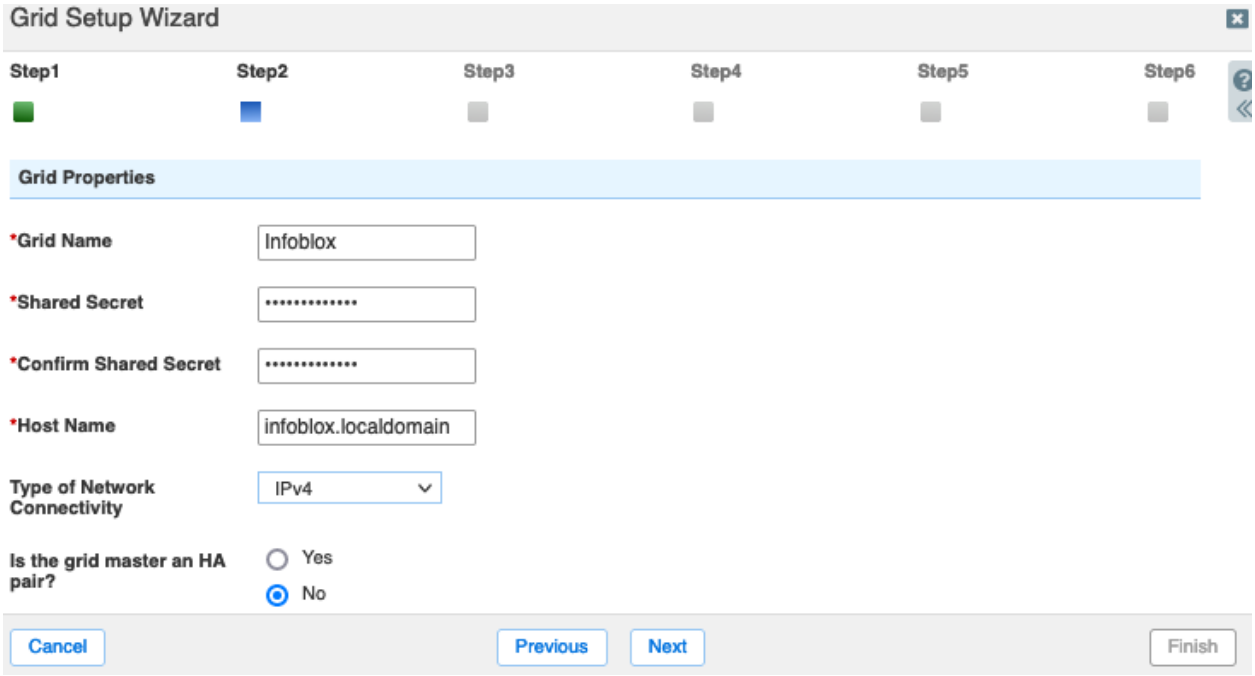
Configure Grid Master

This section details steps to configure your new vNIOS for Azure appliance as an Infoblox Grid Master. If you are joining this device to an existing Grid, refer to NIOS documentation at https://docs.infoblox.com.

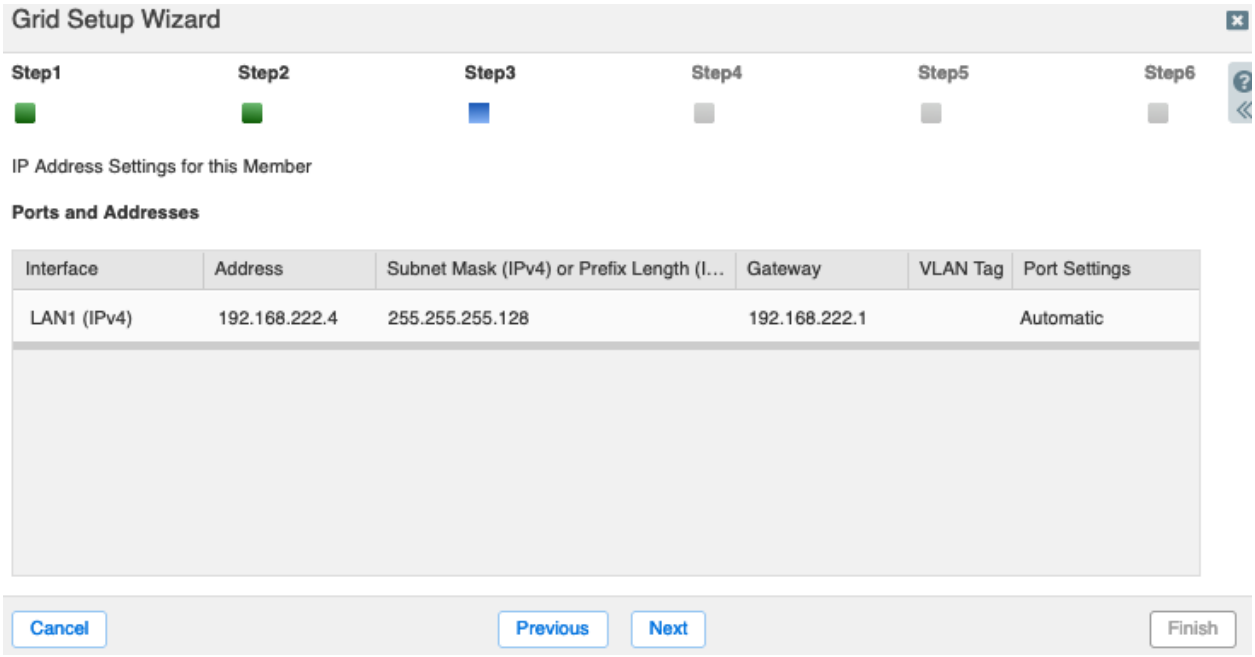
1. When you login to the Grid Manager for the first time, the Grid Setup Wizard will open.
2. Select **Configure a Grid Master** and click **Next**.



3. On Step 2, enter a name for your Grid, a Shared Secret used to join new members to the Grid, and a Host Name for your Grid Master. Or, leave the default values and click **Next**.



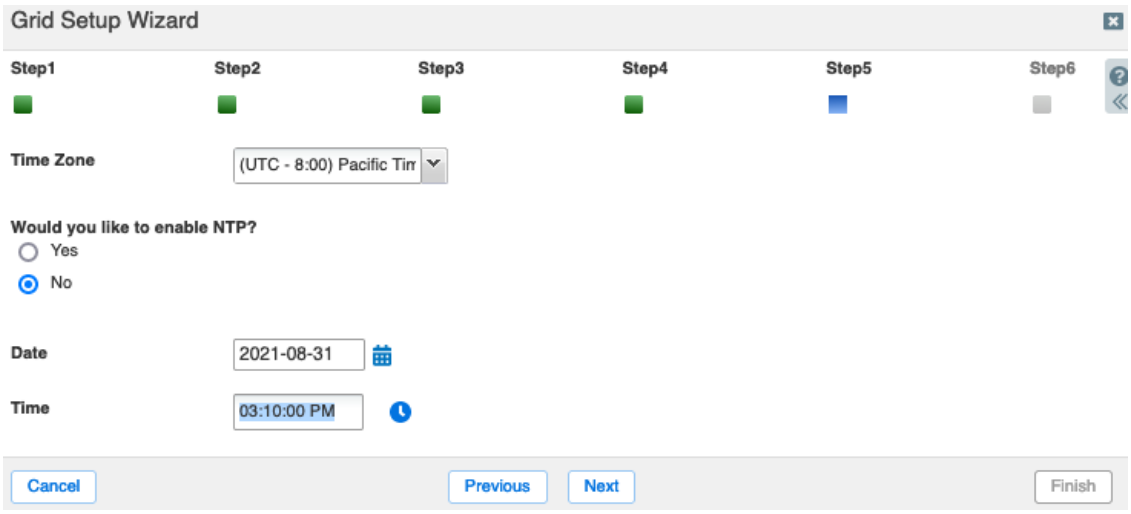
4. On Step 3, verify the IP address information for your Grid Master. This should be the private IP address of the vNIOS appliance. You will not usually need to make any changes on this step. Click **Next** to continue to Step 4.



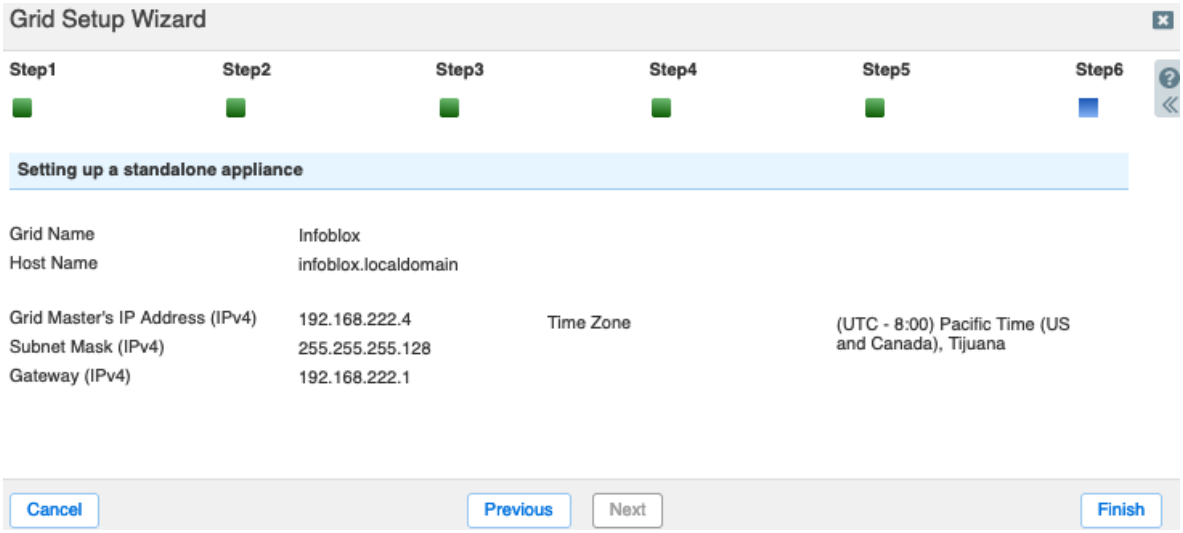
5. On Step 4, you can optionally change the administrator password. Click **Next** to continue.

6. On Step 5, select your **Time Zone** from the dropdown.

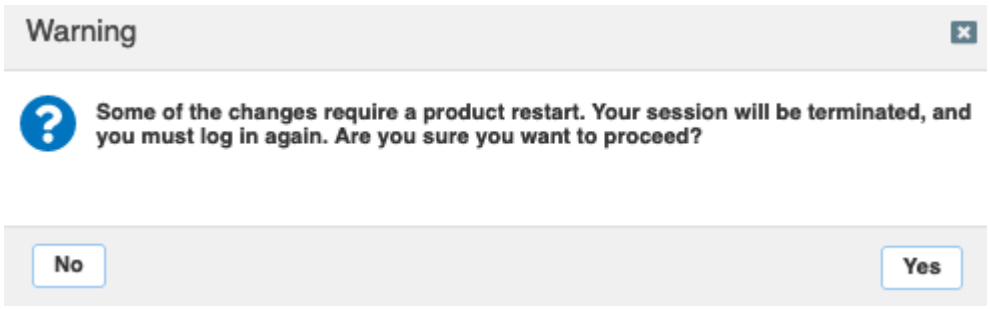
7. Enter the current **time** and click **Next**.



8. Review the details on Step 6 and click **Finish**.



9. Click **Yes** in the warning window to restart your vNIOS appliance.

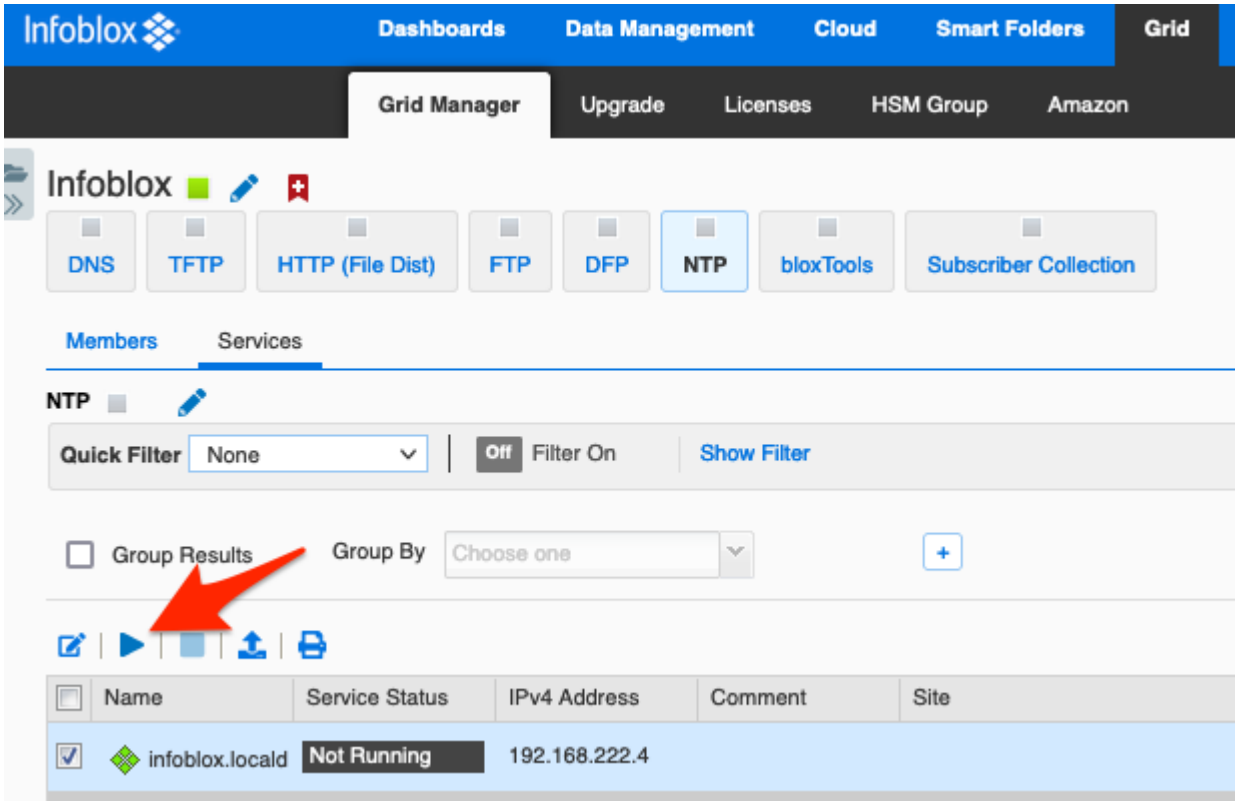


Configure NTP and DNS

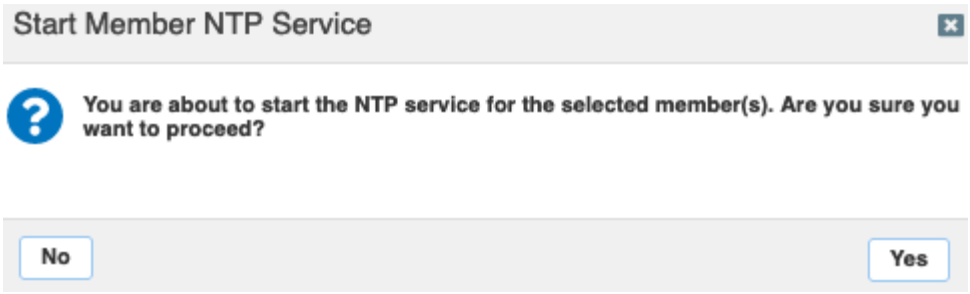
In order to use your new vNIOS appliance for DNS and discovery of resources in Azure, you will need to enable some basic services, Network Time Protocol (NTP), and Domain Name System (DNS).

Start the NTP Service

1. Log back in to Grid Manager.
2. Navigate to the **Grid** → **Grid Manager** tab.
3. Click on **NTP** in the Services bar.
4. Select the checkbox next to your Grid Master.
5. Click the start button to start the NTP service.

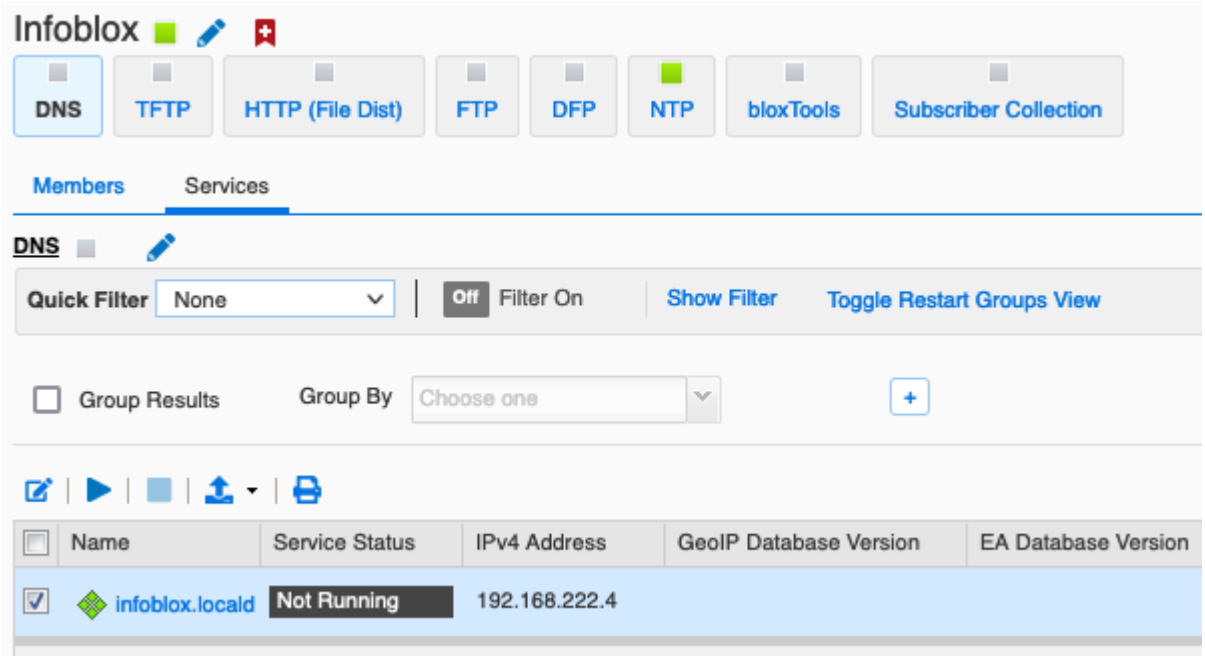


6. Click **Yes** in the warning window.

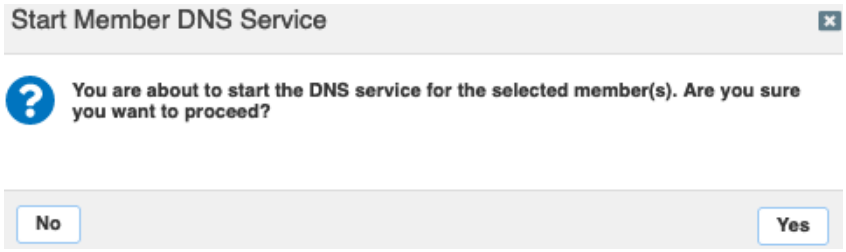


Start and Configure DNS Service

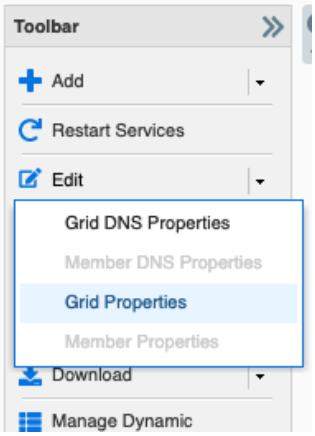
1. Click on **DNS** in the Services bar.
2. Select the checkbox next to your Grid Master.
3. Click the start button to start the DNS service.



4. Click **Yes** in the warning window.



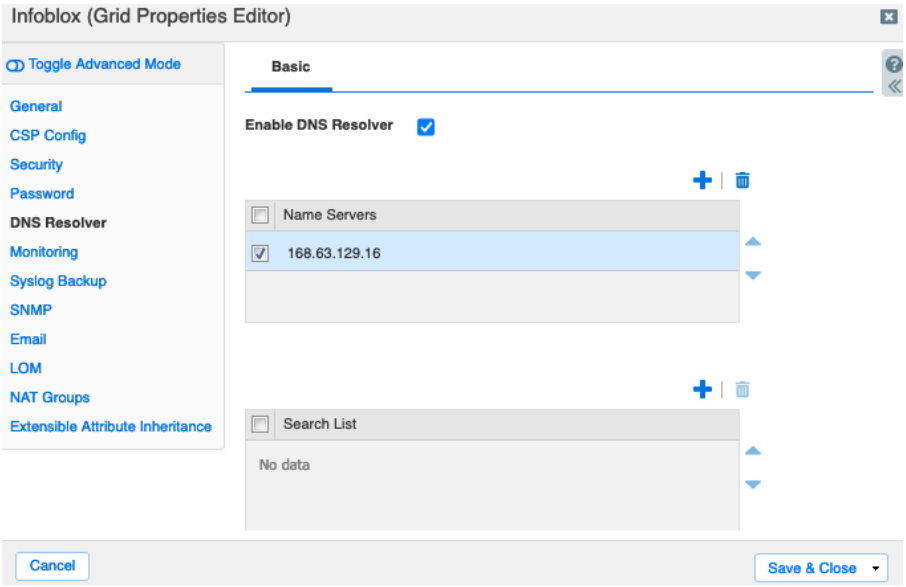
5. From the Toolbar on the right, use the Edit dropdown to select Grid **Properties**.



6. In the Grid Properties Editor, select the **DNS Resolver** page.

7. Click the check box for **Enable DNS Resolver**.

8. Click the + add button and enter the IP of an upstream name server. This can be the default Azure resolver, 168.63.129.16, or a name server of your choosing. This resolver is used by NIOS to resolve names used by services in the Grid. For example, this will be used to resolve the Azure API endpoint used for vDiscovery.

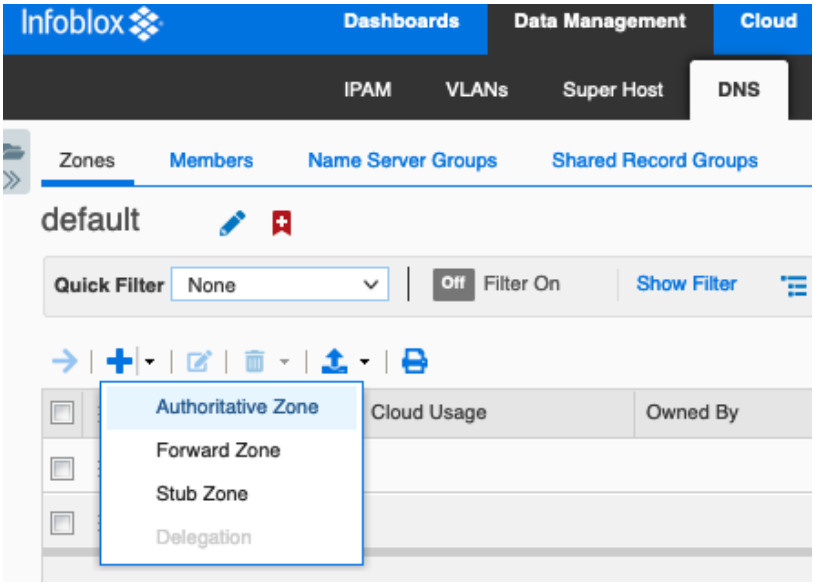


Create a DNS Zone

To enable automatic creation of DNS records when using vDiscovery for Azure, the Infoblox grid must be authoritative for at least one DNS Zone. To create a DNS zone in Grid Manager:

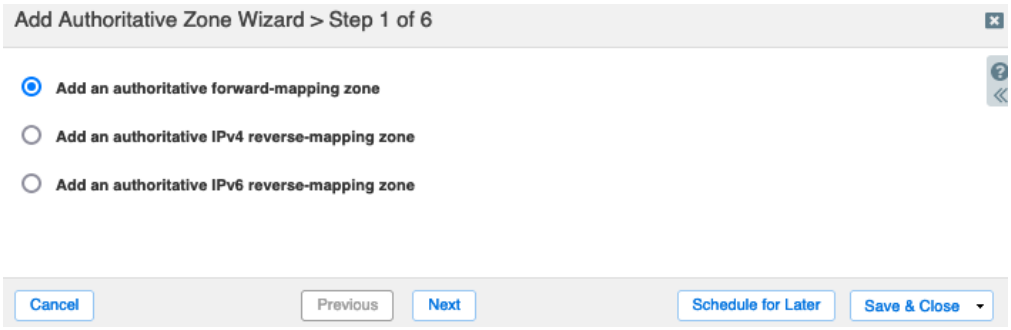
1. In the Grid Manager, navigate to **Data Management → DNS → Zones**.

2. Use the + add zone dropdown to select **Authoritative Zone**.

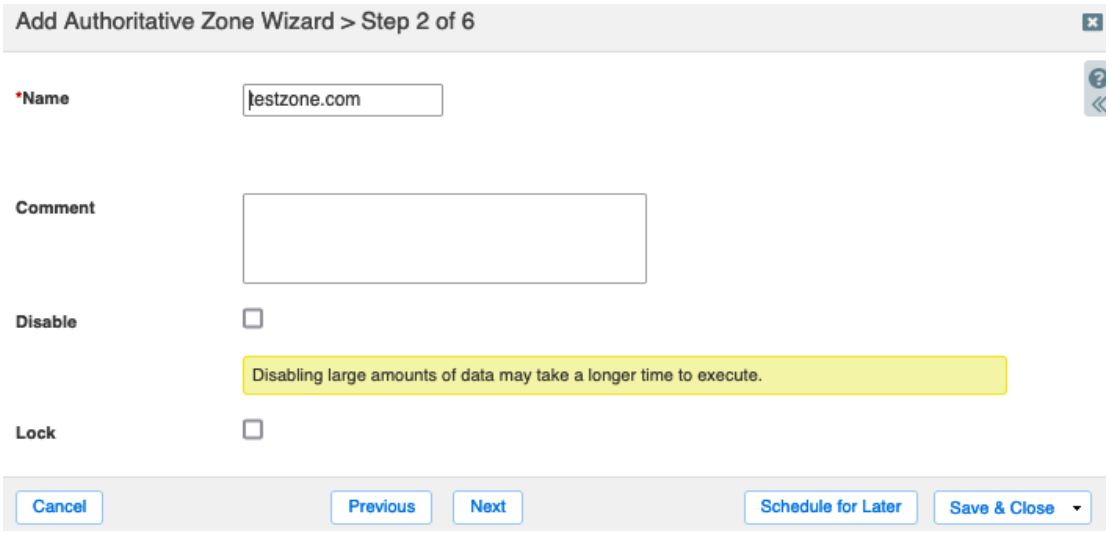


3. In the Add Authoritative Zone Wizard, select **Add an authoritative forward-mapping zone**.

4. Click **Next**.

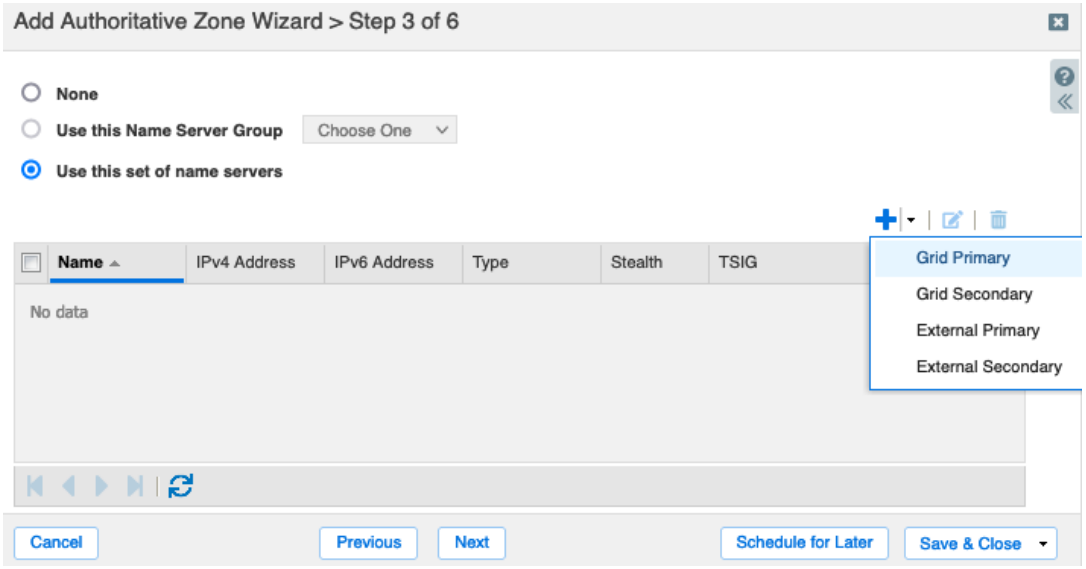


5. Enter the **name** of your zone and click **Next**.

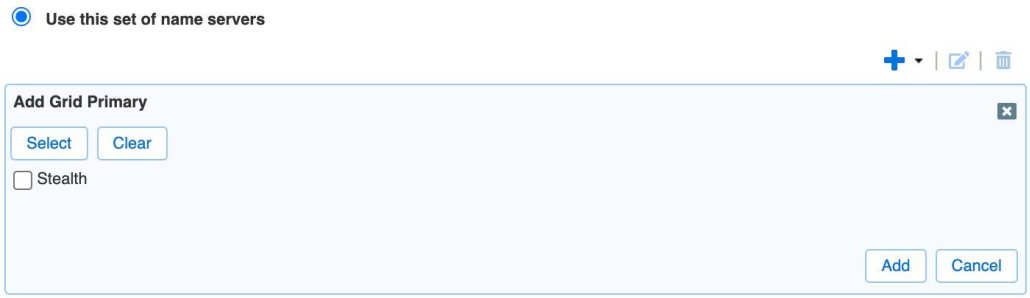


6. On Step 3, select **Use this set of name servers**.

7. Click the + icon and select **Grid Primary** from the dropdown.

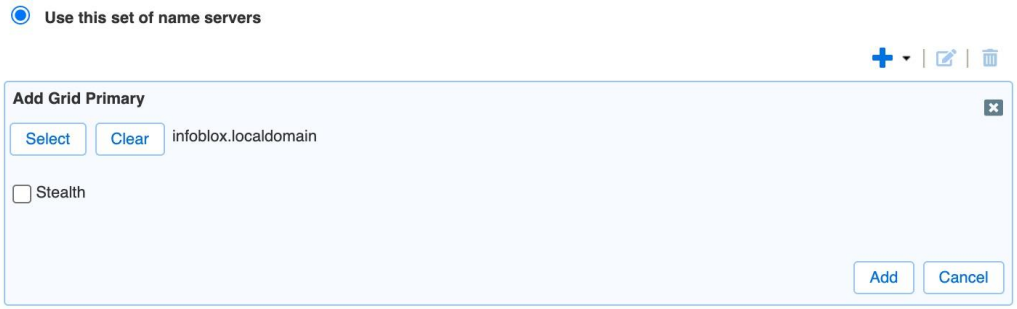


8. Click **Select** in the Add Grid Primary panel.

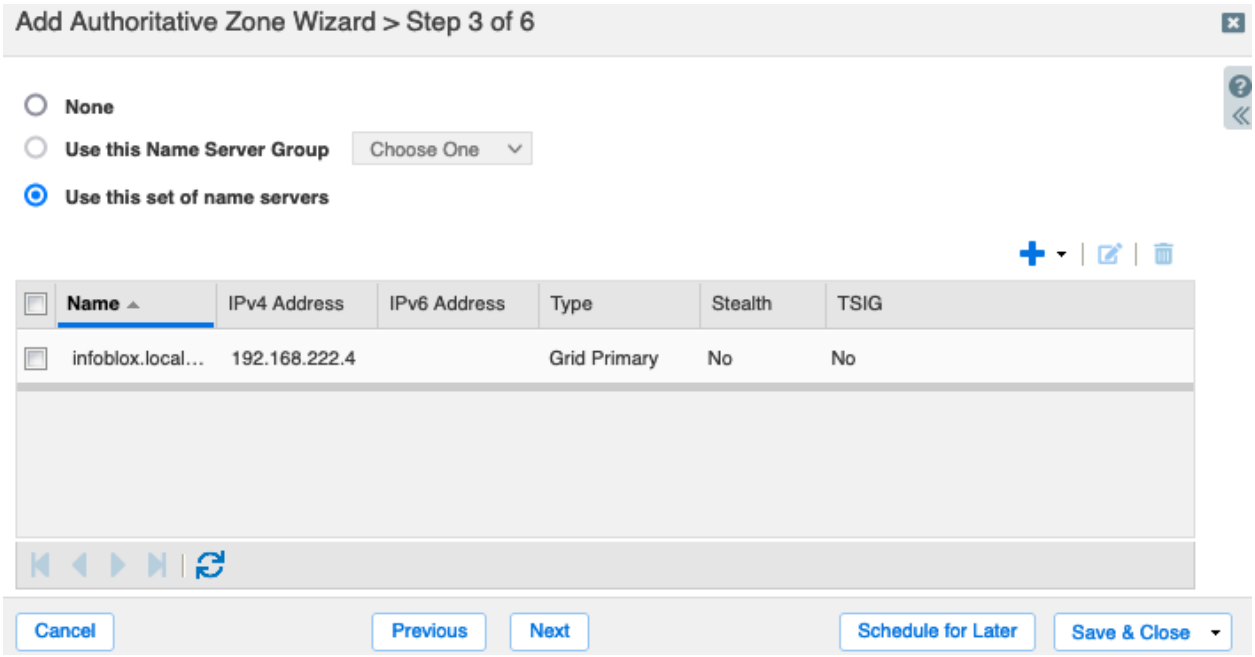


9. For a Grid with only one member, it will be automatically selected. If your Grid has multiple members, select the one you want to use as the primary for this zone.

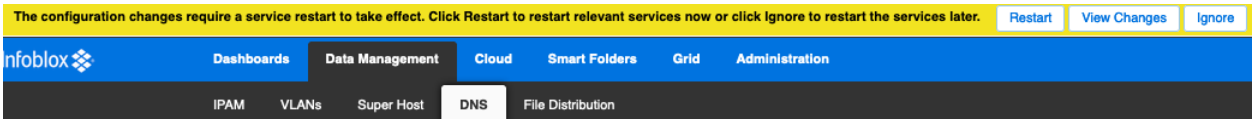
10. Click **Add**.



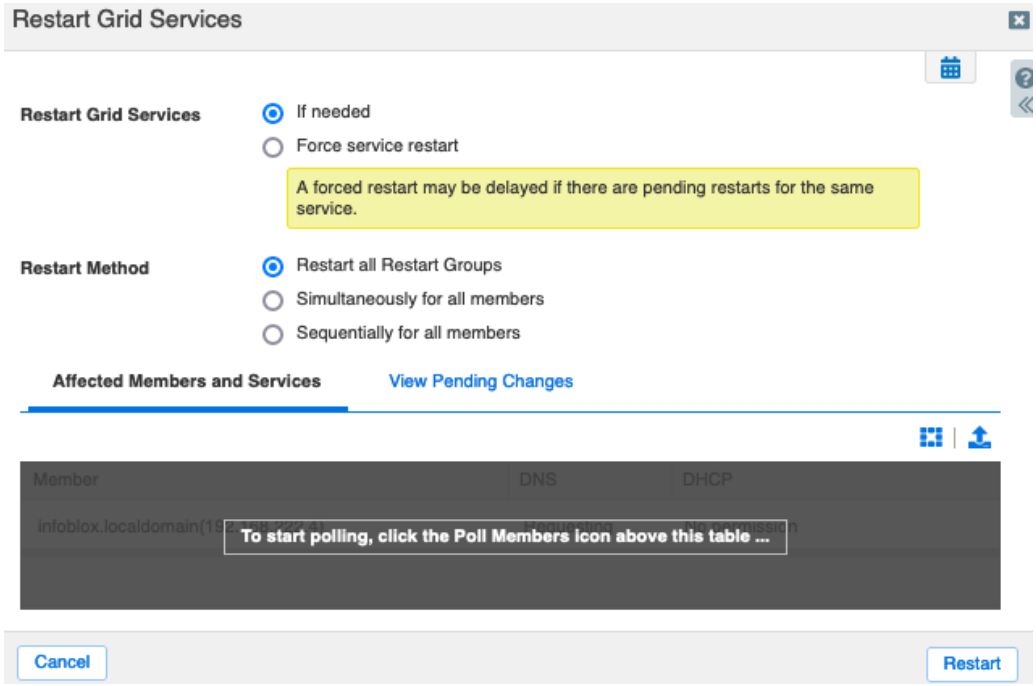
11. Click **Save & Close**.



12. Click **Restart** in the warning bar when prompted.



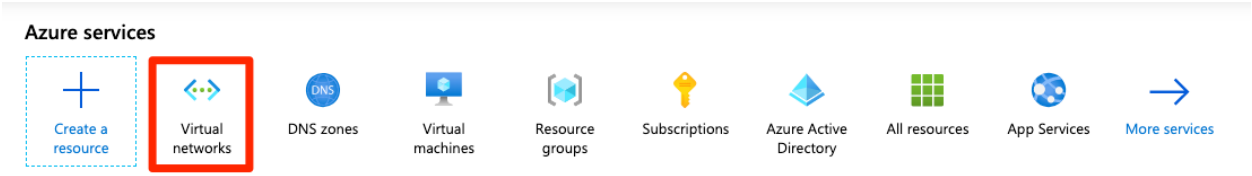
13. Click **Restart** in the Restart Grid Services window.



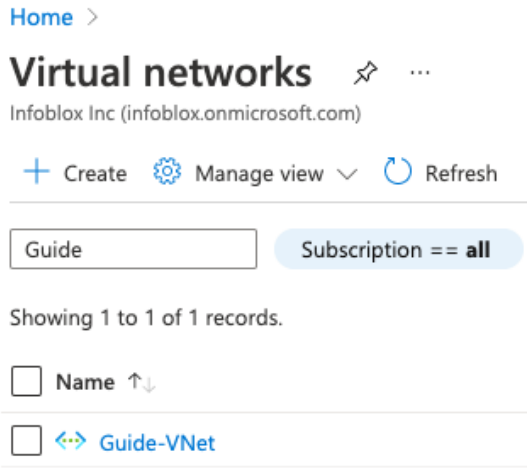
Configure vNIOS as Primary DNS for Azure VNets

Once your vNIOS for Azure appliance has been deployed, you can update Azure VNet settings to allow VMs to use the Infoblox device for DNS resolution.

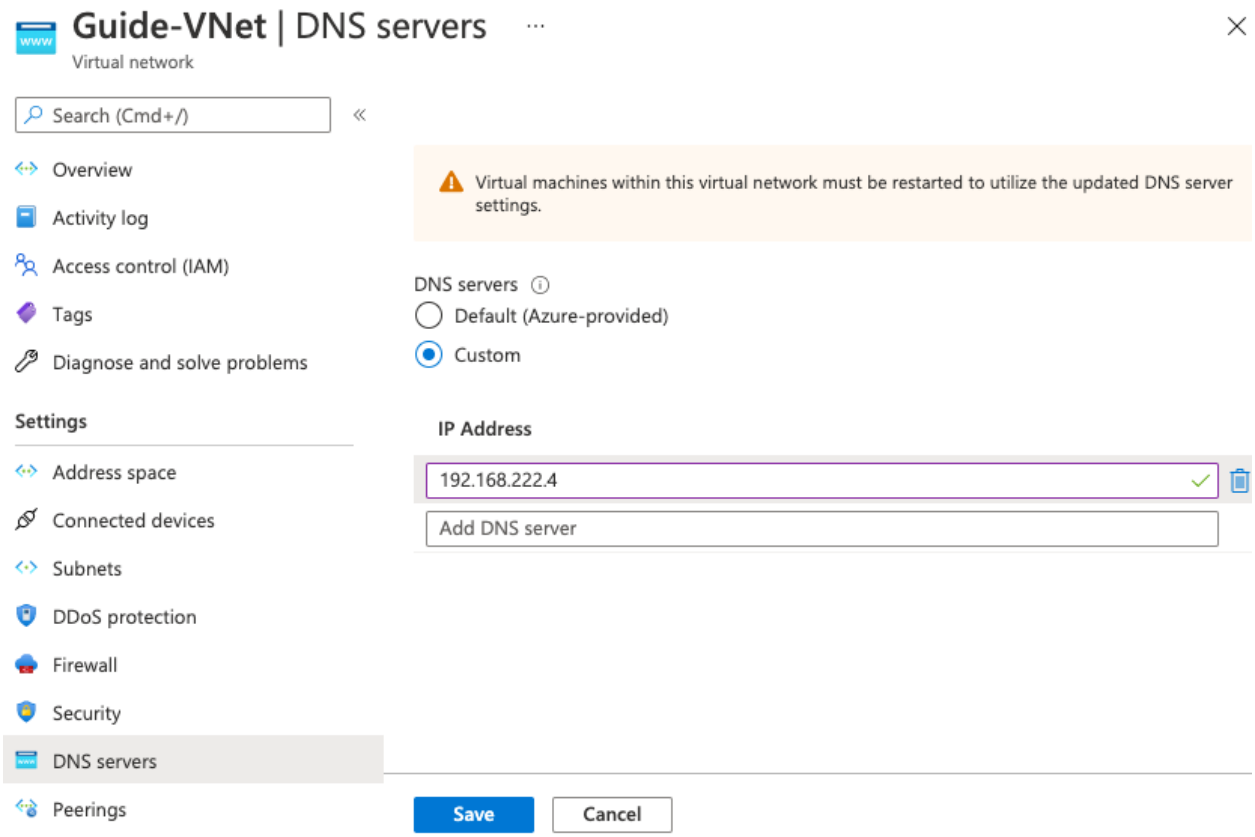
1. In the Azure Portal, click on **Virtual networks**.



2. Select your VNet from the list.



3. In the VNet blade, click on **DNS servers** under Settings.
4. Select **Custom**.
5. Enter the private IP of the LAN1 interface of your vNIOS for Azure VM.
6. Click **Save**.



VMs currently running in this VNet will now use your vNIOS appliance for DNS after they are restarted. Any new VMs deployed into this VNet will use your vNIOS appliance for DNS immediately.

Infoblox vDiscovery for Azure

The Infoblox vDiscovery feature is very useful for detecting and obtaining information about Tenants, VNETs, Subnets, and Virtual Machines (VM's) operating in your public cloud environments. This can include Microsoft Azure, Amazon Web Services (AWS), and Google Cloud Platform (GCP).

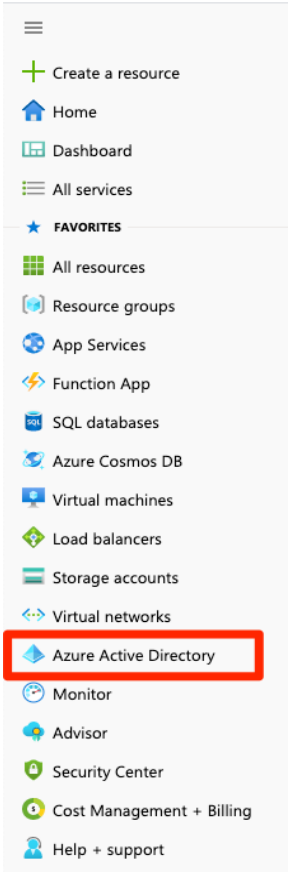
Many organizations operate hybrid and multi-cloud environments that may contain many subscriptions and accounts. These environments tend to be very dynamic, with things such as VMs being created and terminated on a frequent basis. This makes it difficult to keep track of everything. With Infoblox vDiscovery, tasks can be configured to run automatically allowing your Infoblox Grid to keep track of all cloud environments, storing this data in IPAM. 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'.

Enable vDiscovery in Azure

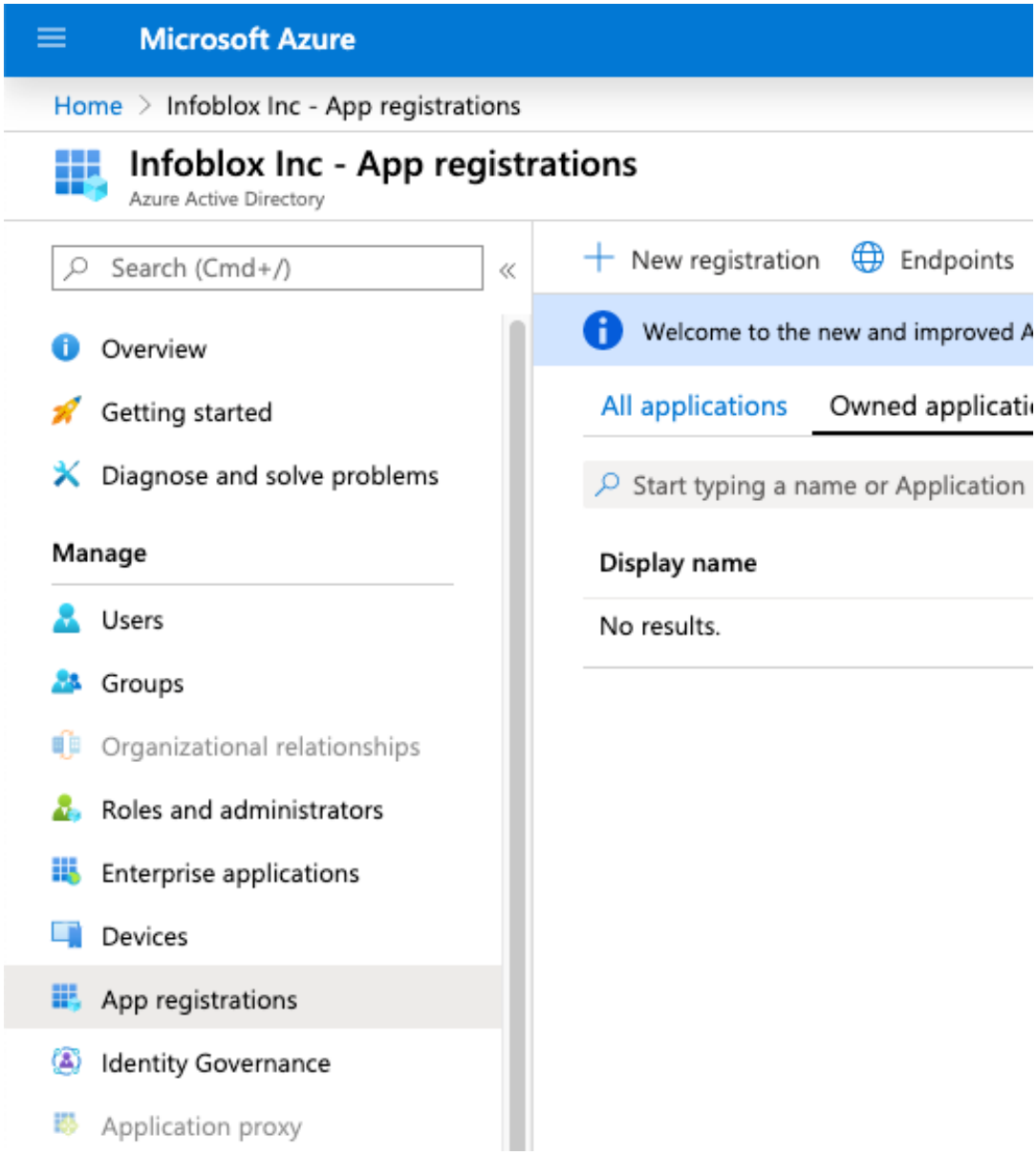
In order to use vDiscovery in Azure, you must integrate the discovery application with Azure Active Directory (AAD) for secure authentication and authorization.

Create an App Registration in Azure AD

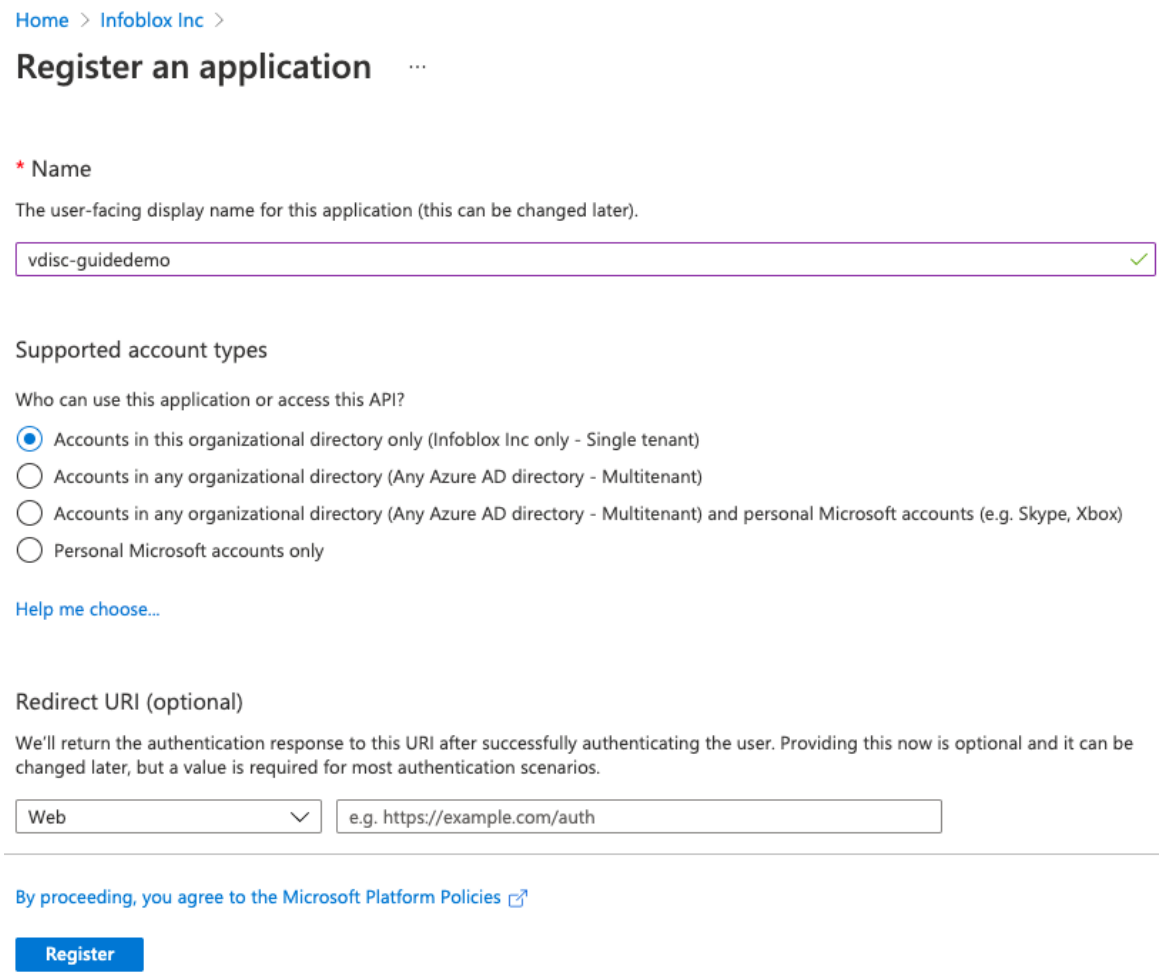
1. In the Azure Portal, click the menu.
2. Select **Azure Active Directory**.



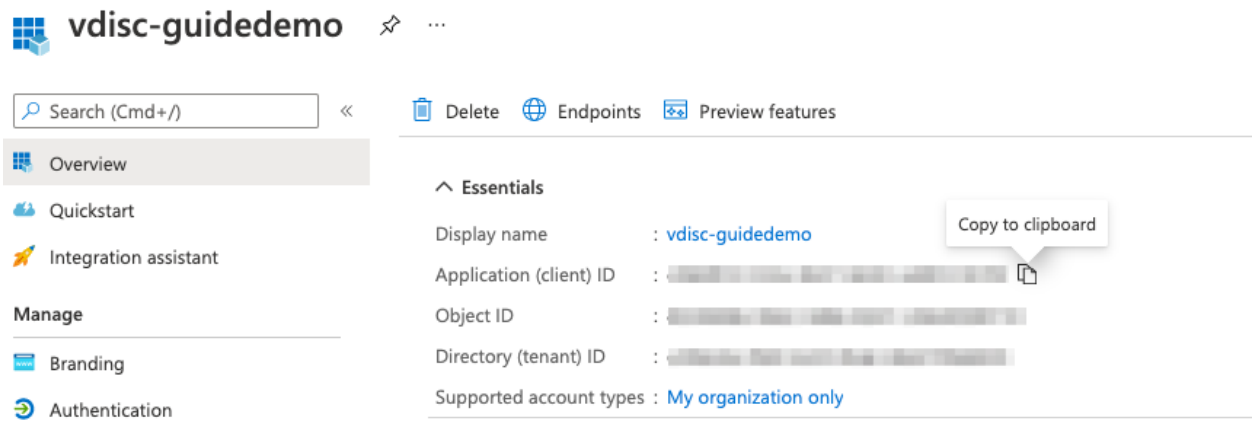
3. Click on **App registrations**.
4. Click **New registration**.


Microsoft Azure
Home > Infoblox Inc - App registrations
Infoblox Inc - App registrations
Azure Active Directory
Search (Cmd+/)
Overview
Getting started
Diagnose and solve problems
Manage
Users
Groups
Organizational relationships
Roles and administrators
Enterprise applications
Devices
App registrations
Identity Governance
Application proxy
New registration
Endpoints
Welcome to the new and improved A
All applications
Owned applicati
Start typing a name or Application
Display name
No results.

5. Type a **Name** for your App.
6. Ensure **Accounts in this organizational directory only** is selected under **Supported account types**.
7. Click **Register**.

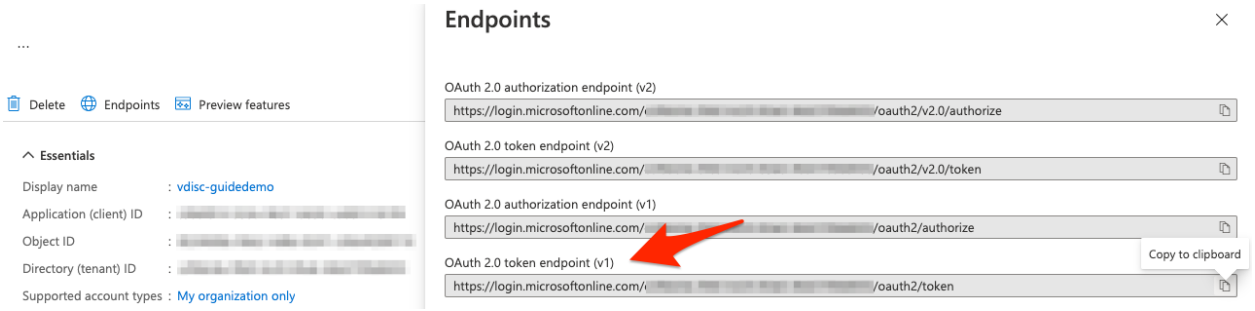


8. On the App's Overview page, hover over **Application (client) ID**.
9. Click to copy the value to the clipboard. Save this ID.



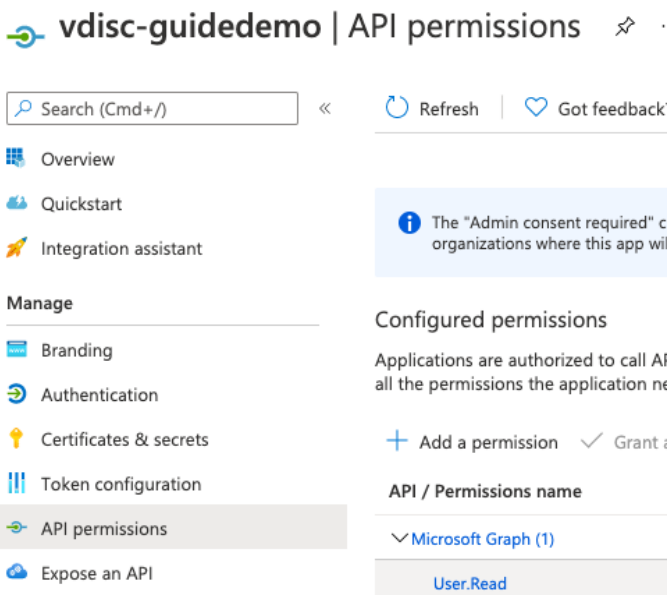
10. Click on **Endpoints**.

11. Hover over the **OAuth 2.0 token endpoint (v1)** and click to copy the value to the clipboard. Save this Endpoint.

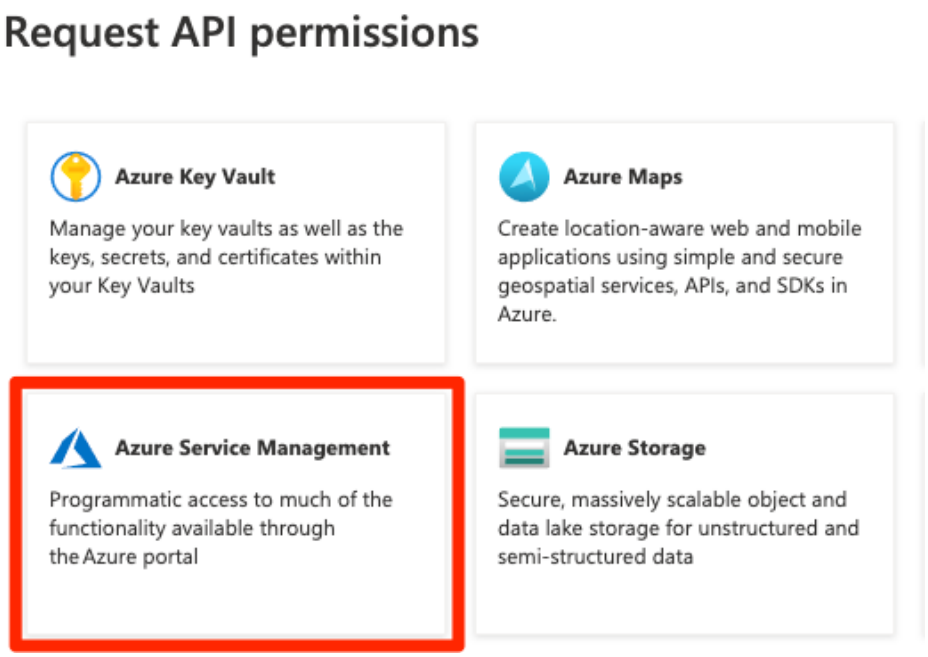


12. Click on **API permissions**.

13. Click **Add a permission**.

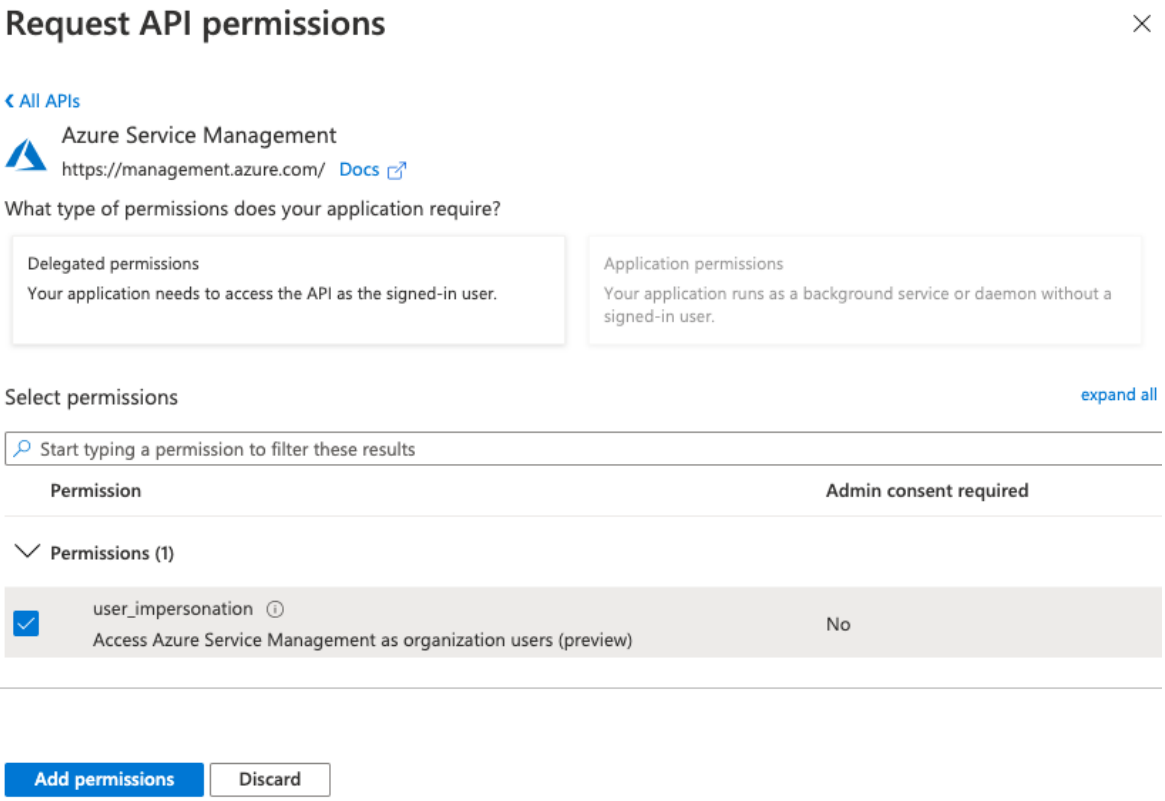


14. Select the **Azure Service Management** API.



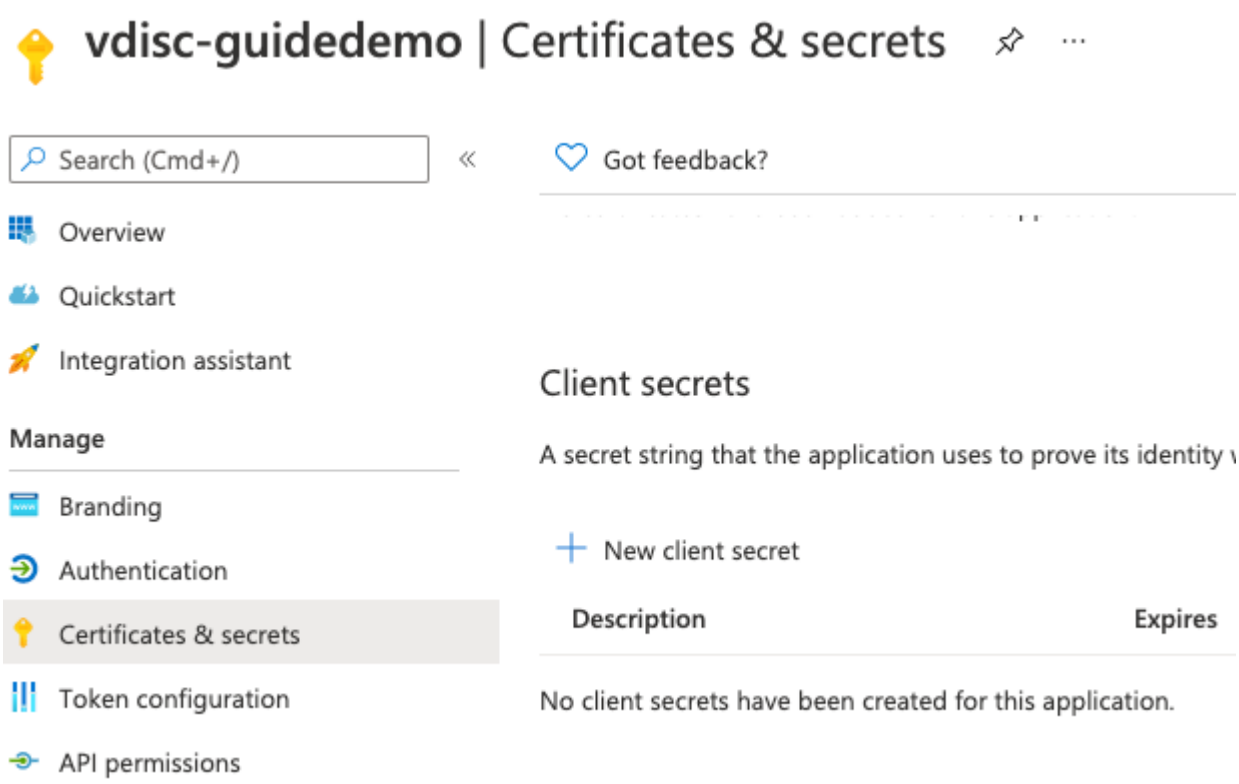
15. Select the checkbox for **user_impersonation**.

16. Click **Add permissions**.



17. Click on **Certificates & secrets**.

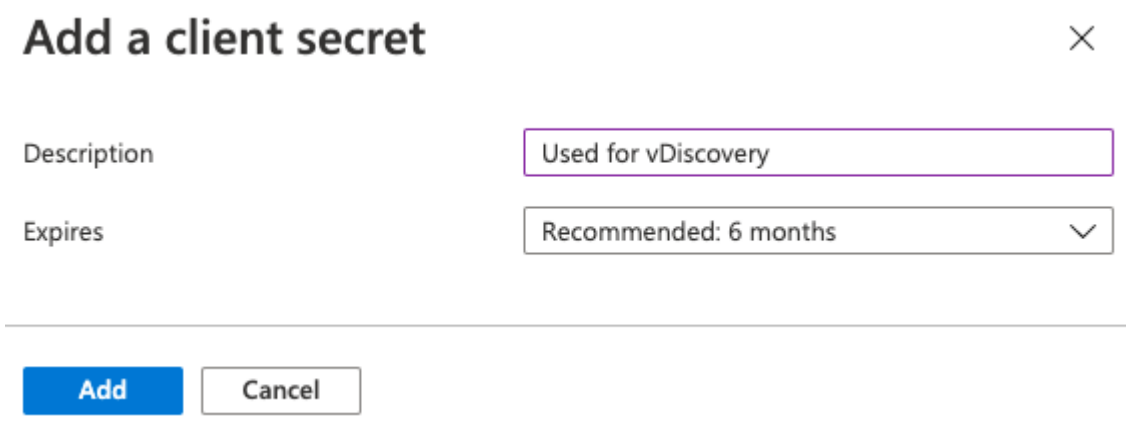
18. Click **New client secret**.



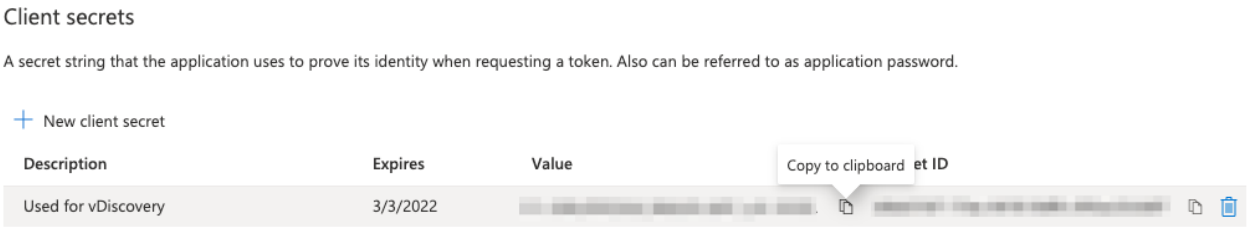
19. Enter a **Description**.

20. Select when the secret **Expires**.

21. Click **Add**.



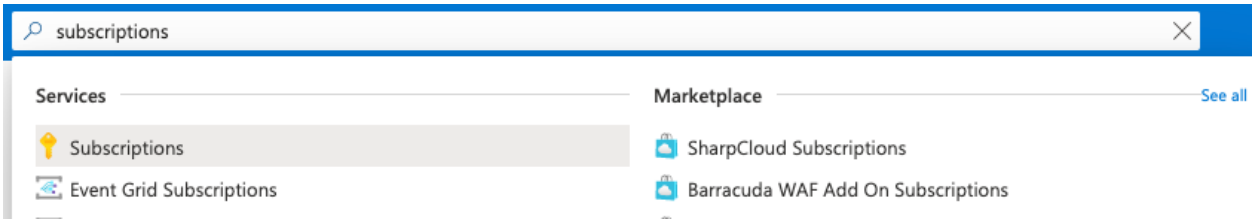
22. Hover over the key **Value** of your new secret and click to copy the value to the clipboard. Save this Client Secret.



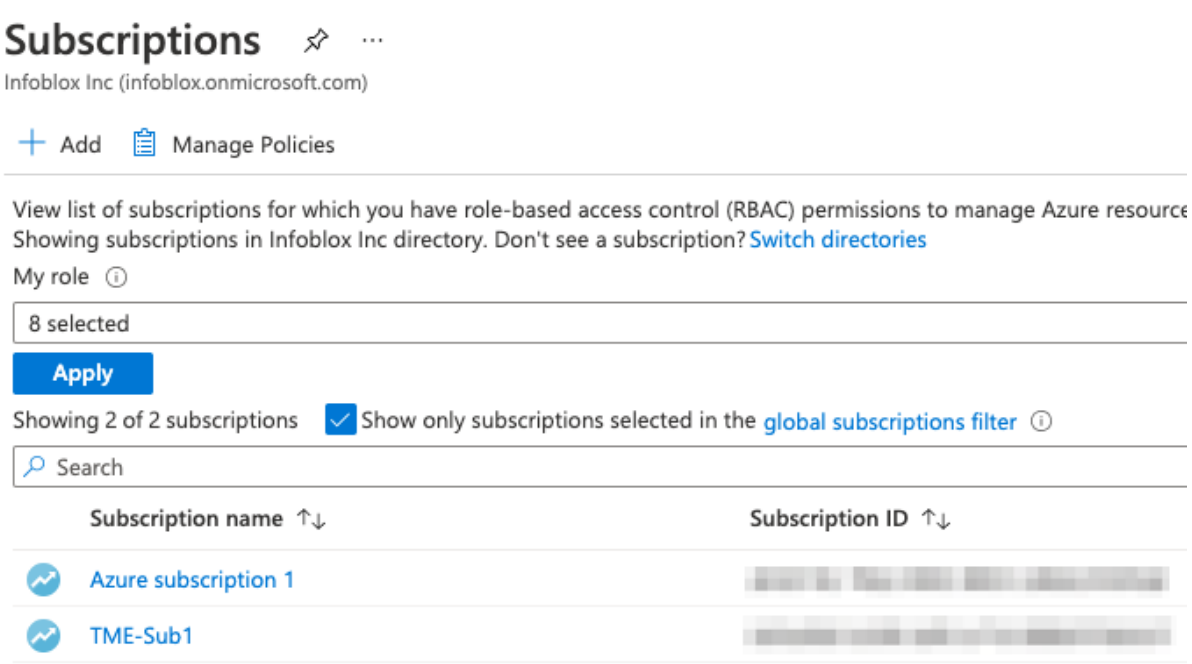
Add Role Assignment to Subscription

For each Azure subscription where vDiscovery will be conducted, the new App needs to be added as a Reader. Alternatively, Reader permissions can be assigned at the Resource Group level for more granular control of what is included for vDiscovery.

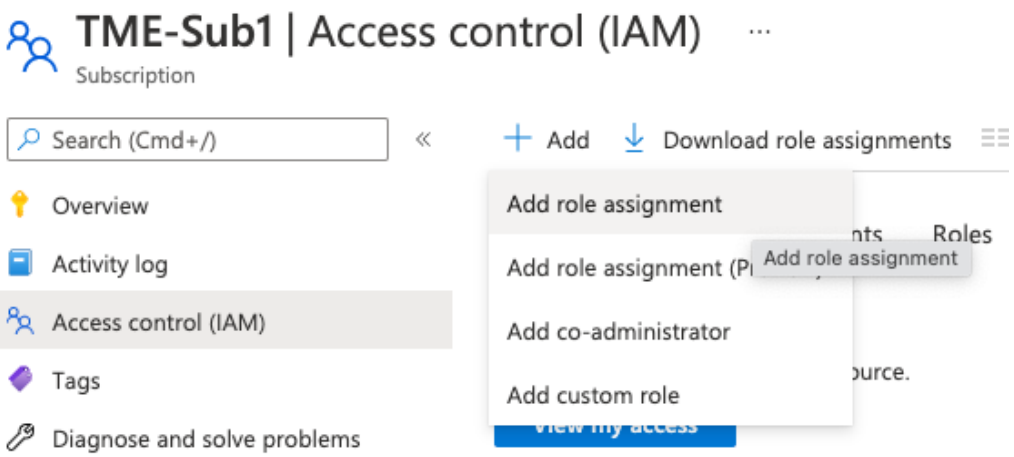
1. In the Azure Portal, type **subscription** into the search box.
2. Click on **Subscriptions**.



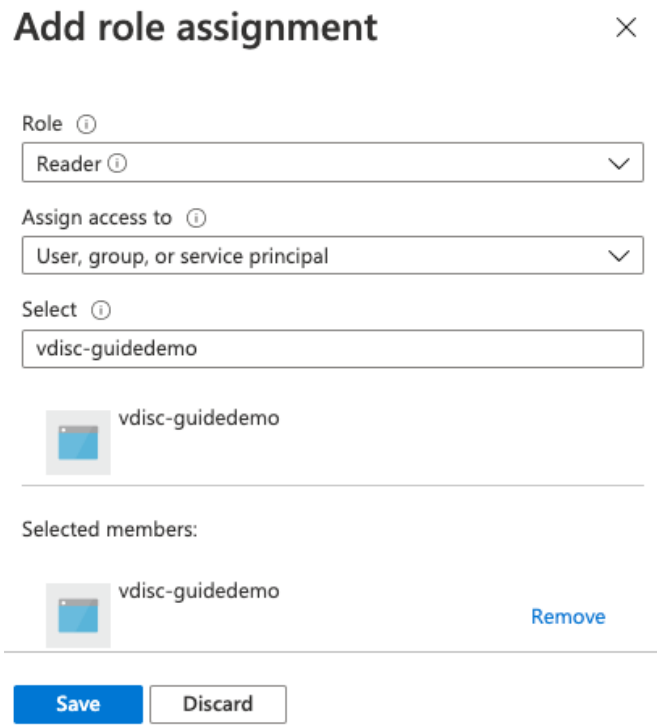
3. Select your desired subscription from the list.



4. On the Subscription blade, select **Access control (IAM)**.
5. Click on **Add**.
6. Select **Add role assignment** from the dropdown.



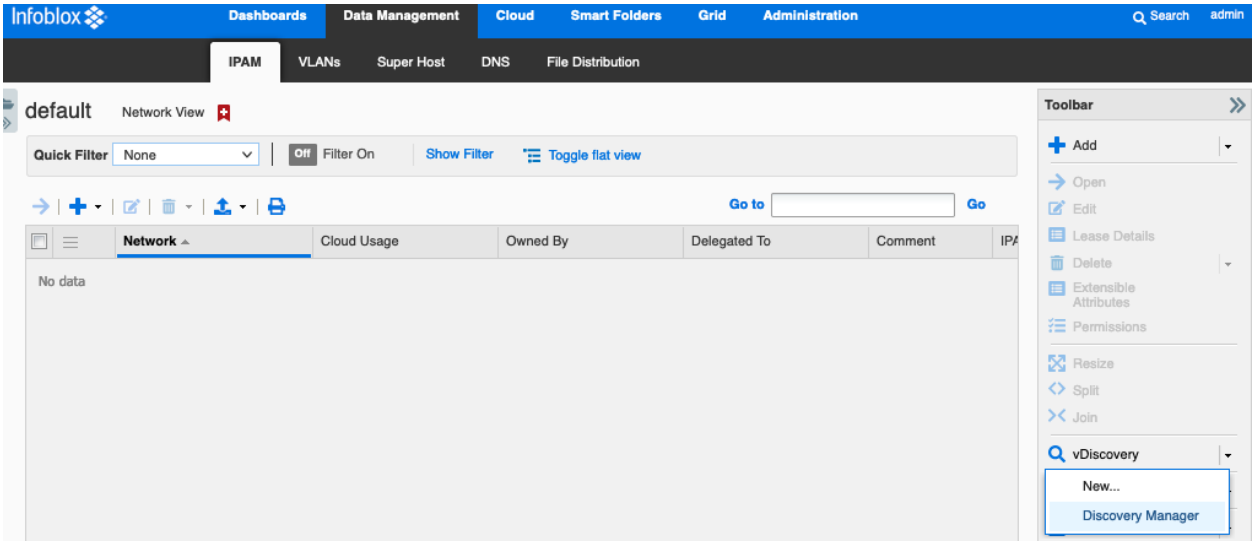
7. Select **Reader** from the Role dropdown.
8. Type the name of your App in the Select box.
9. Select your new App registration.
10. Click **Save**.



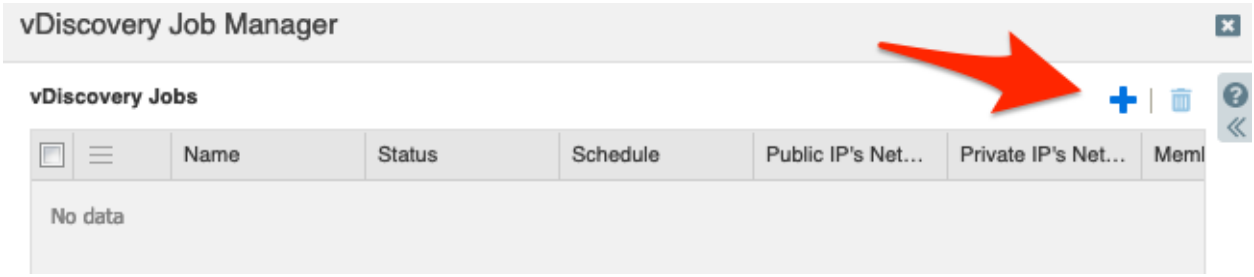
Configure vDiscovery in Grid Manager

To run vDiscovery in Azure, you will configure a vDiscovery job, using the Client ID, Client Secret, and Endpoint identified in Azure.

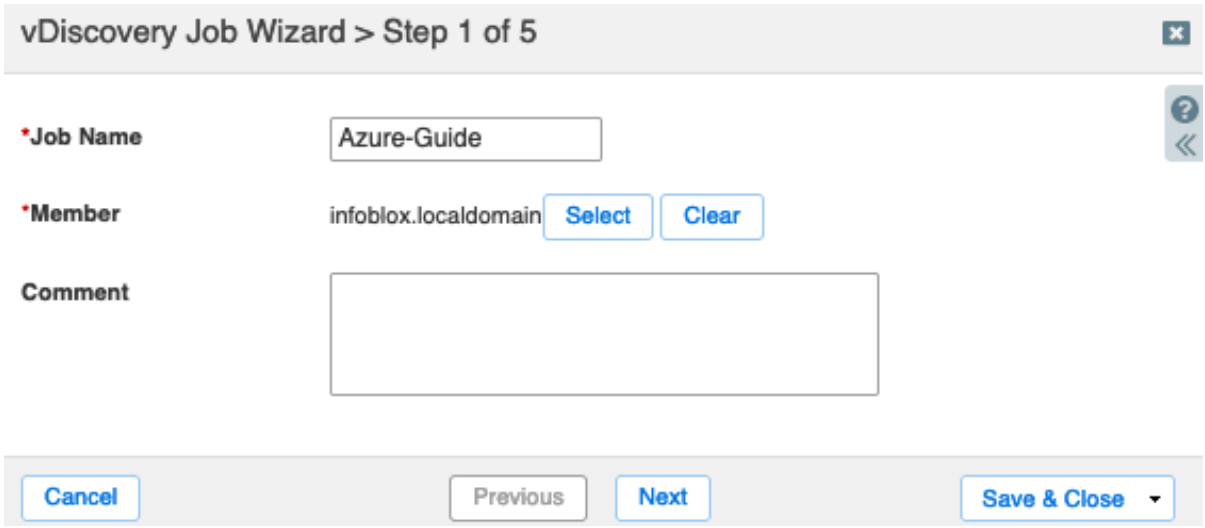
1. Log back in to the Grid Manager.
2. Navigate to the **Data Management** → **IPAM** tab.
3. In the Toolbar, open the **vDiscovery** dropdown.
4. Select **Discovery Manager**.



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



6. On Step 1 of 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**.

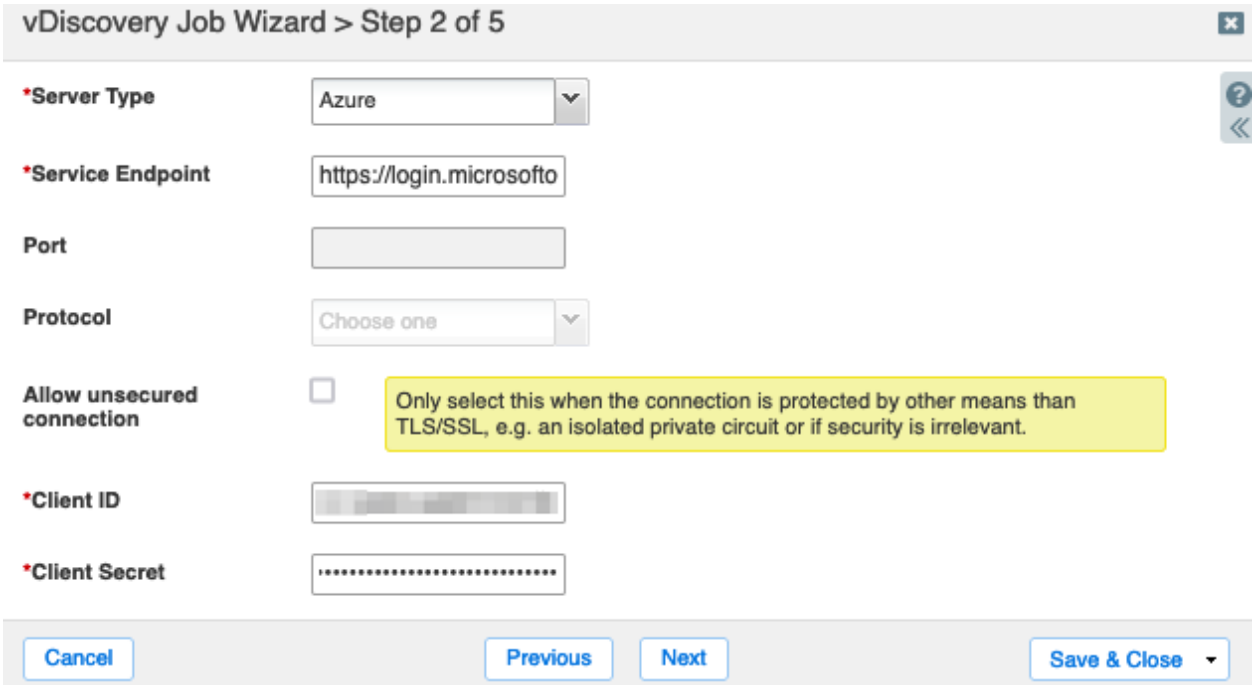


10. On Step 2 of the wizard, select **Azure** from the Server Type dropdown.

11. For Service Endpoint, enter the **OAuth token endpoint (v1)** that you saved earlier.

12. Enter the **Client ID** and **Client Secret** from your App registration.

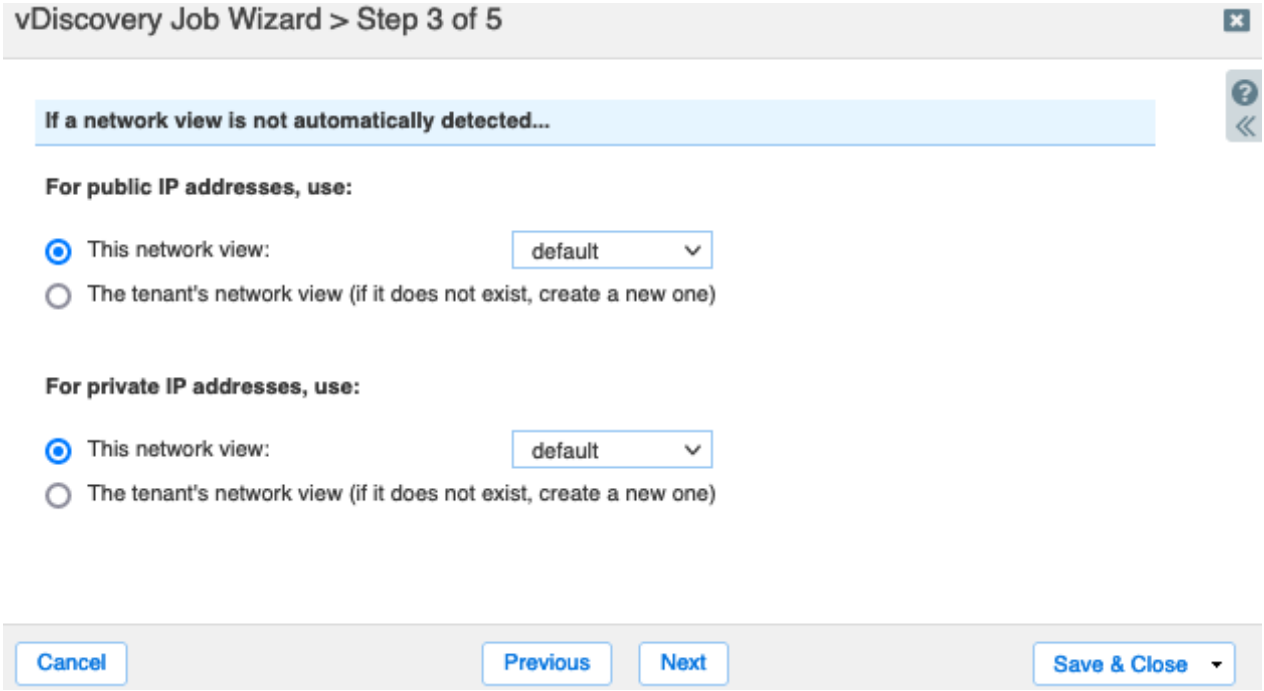
13. Click **Next**.



14. Optionally, on Step 3, change the Network Views where vDiscovery data will be added.

15. Click **Next**.

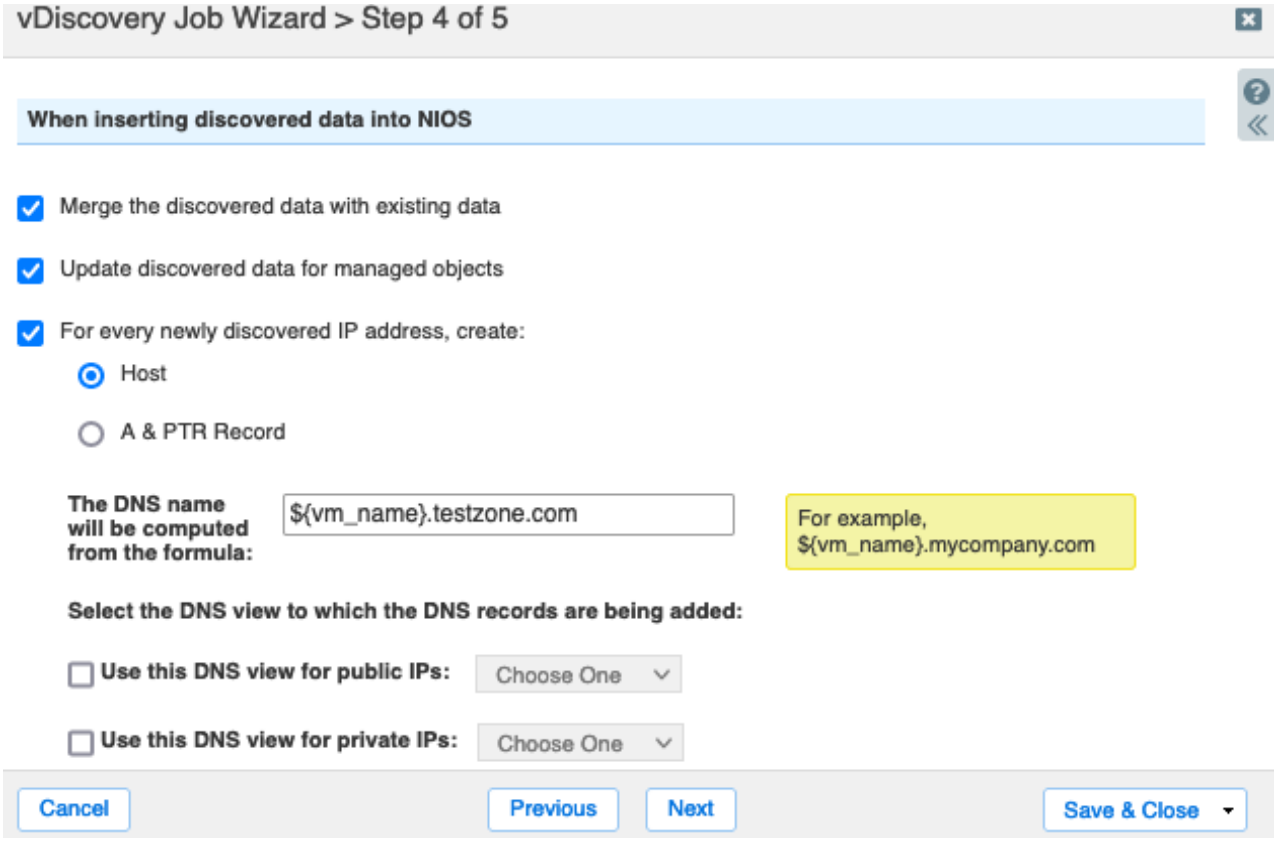
Note: The most common cause for vDiscovery to fail to import any data is a "Sync Error" due to overlapping/conflicting address space. To account for any address space conflicts that are encountered during the vDiscovery process or with your existing IPAM data, you may need to select the option to use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



16. Optional: For automatic creation of DNS records for discovered VMS, on Step 4 select the checkbox **For every newly discovered address, create:**.
17. Select the desired DNS record type. If in doubt, stick with the default (**Host**) option.
18. 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**.
19. Click **Next**.

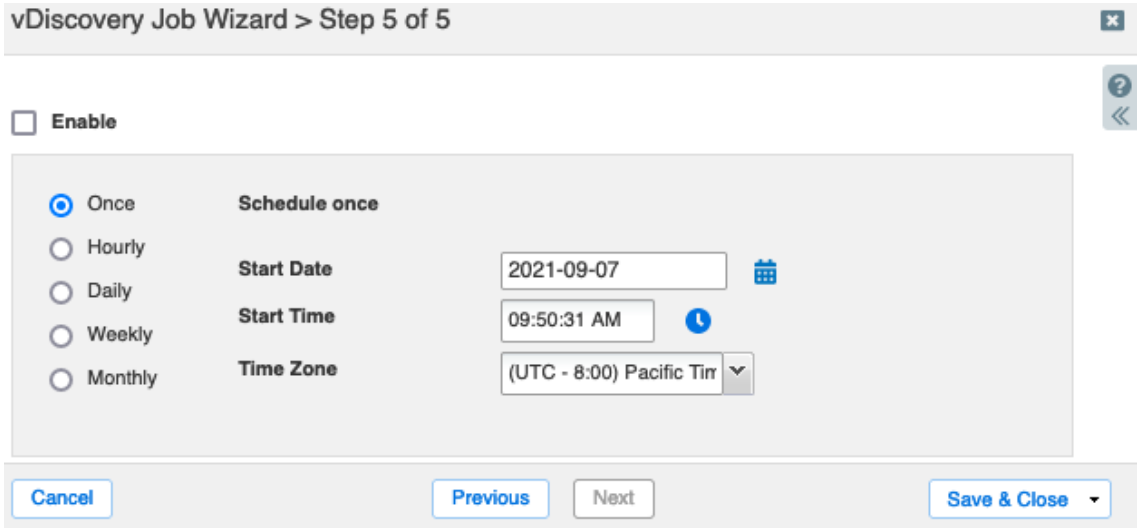
Note: Automatic creation of DNS records is only available if you have the Cloud Network Automation license.

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".*



20. On Step 5, select Enable and set the schedule you want this job to run. Or, leave the schedule disabled to run manually.

21. Click **Save & Close**.

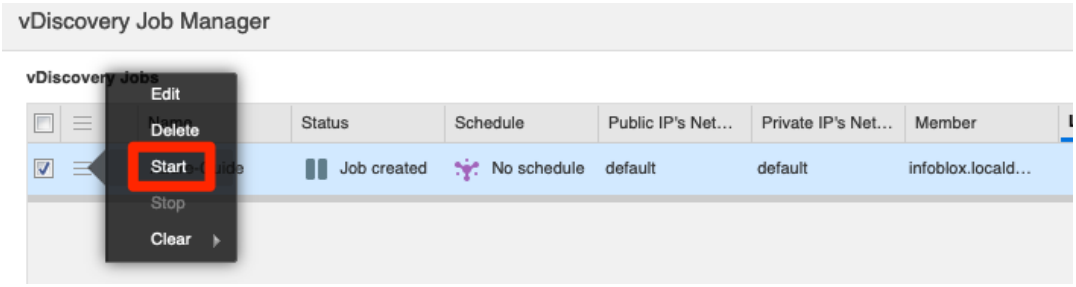


Note: The scheduler enables you to run the vDiscovery task as frequently as once an hour. If this must be run more frequently, this can be accomplished using the API. Refer to the Infoblox REST API guide for examples and guidelines on this process.

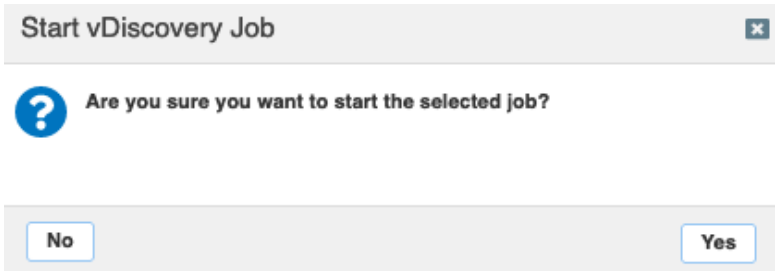
Run vDiscovery

To manually run your vDiscovery job, from the vDiscovery Job Manager window click the (Action Menu) for your vDiscovery job.

Select **Start**.



Click **Yes** in the popup window.



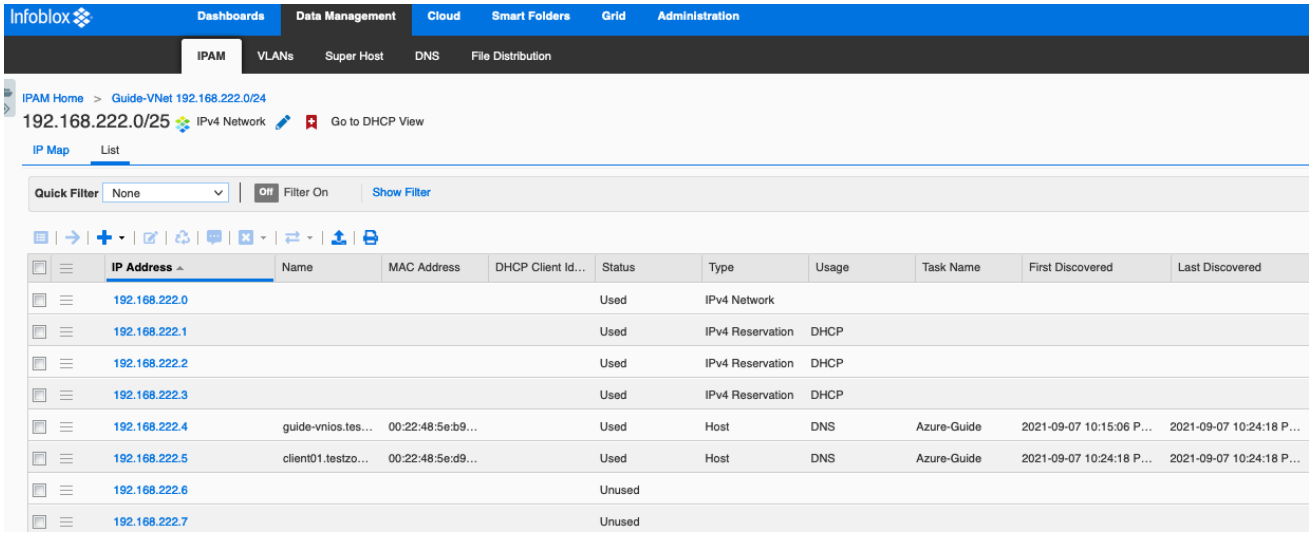
vDiscovery Data

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.

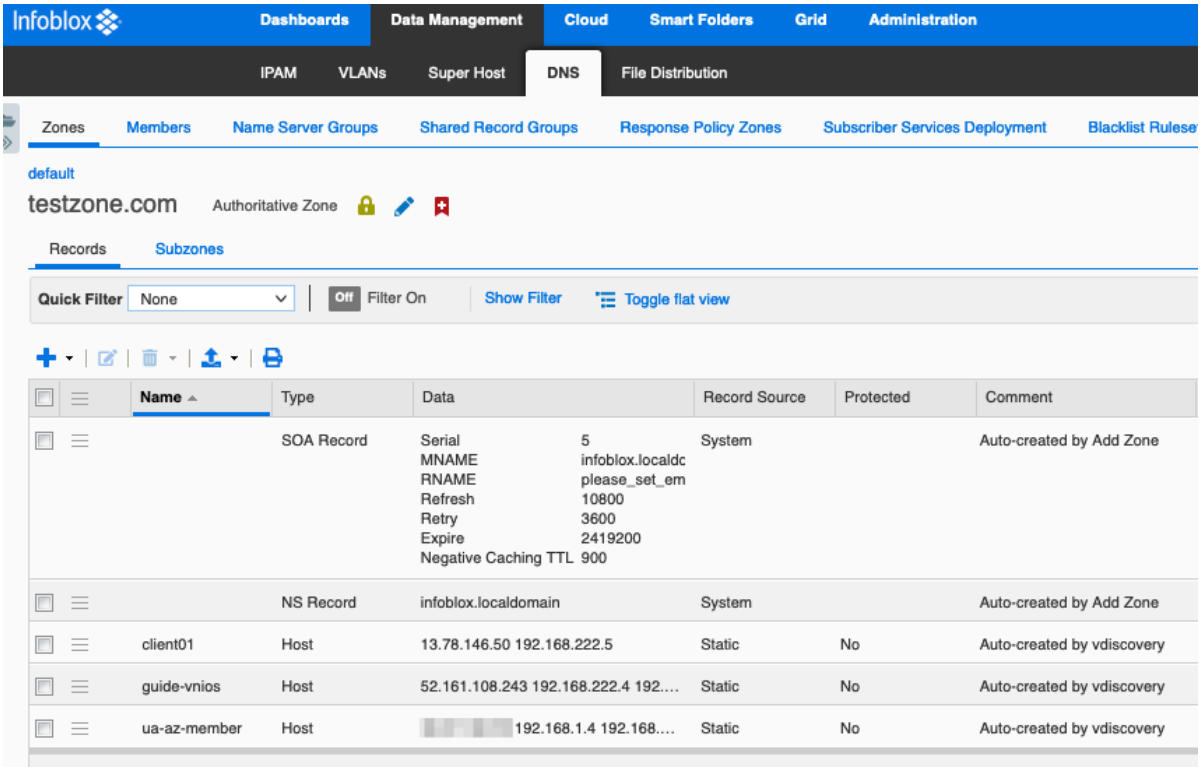
Data Management

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



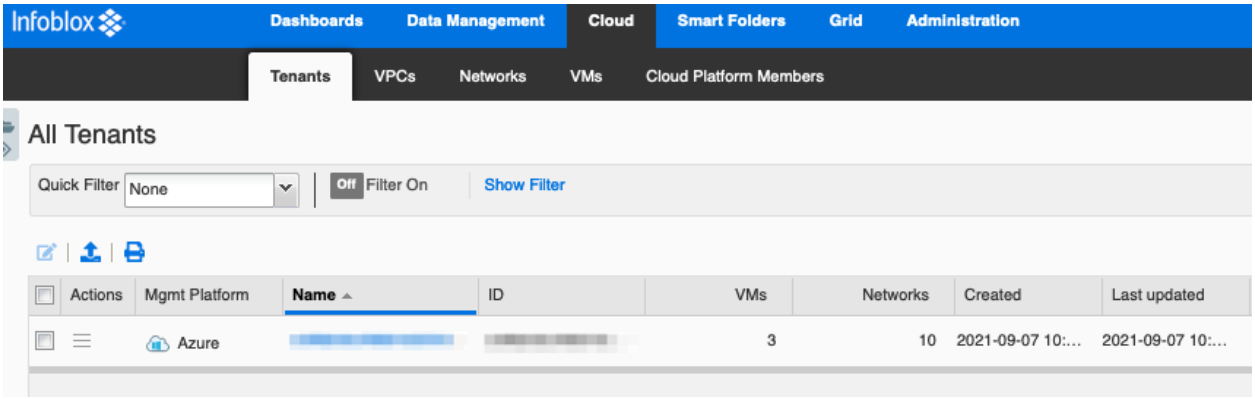
- **DNS**: If you enabled the automatic creation of DNS records, the records can be viewed by drilling down into the DNS zone you specified.



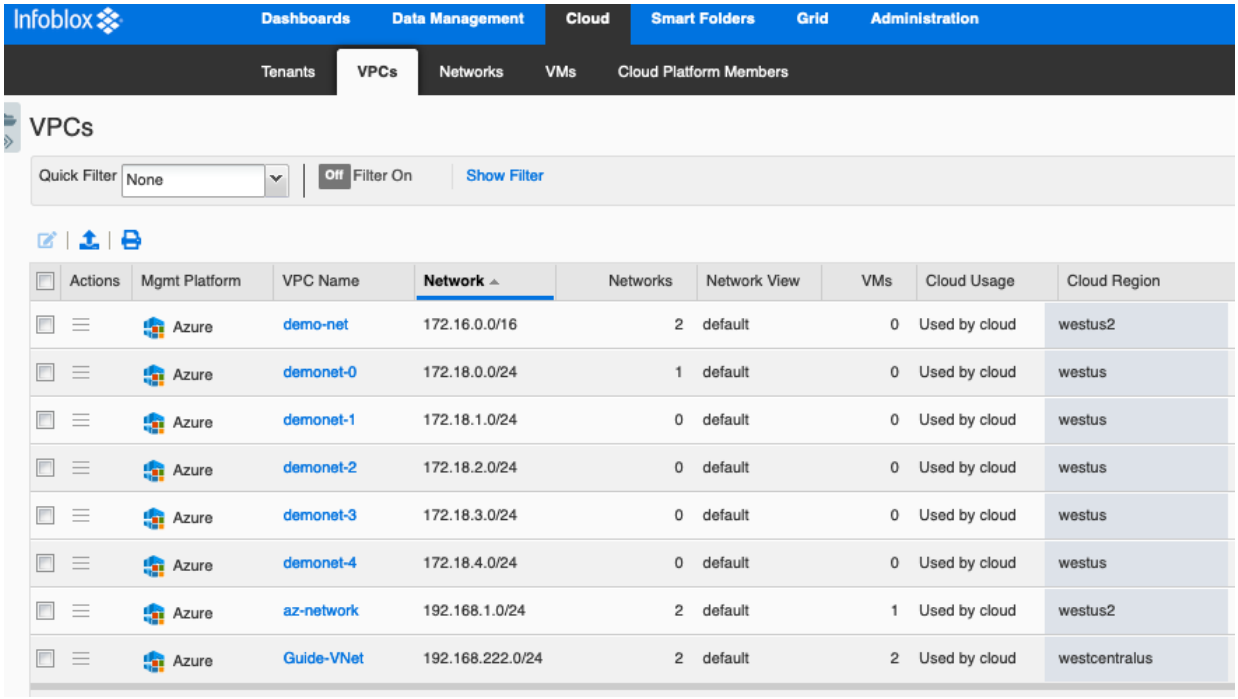
Cloud Network Automation

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.

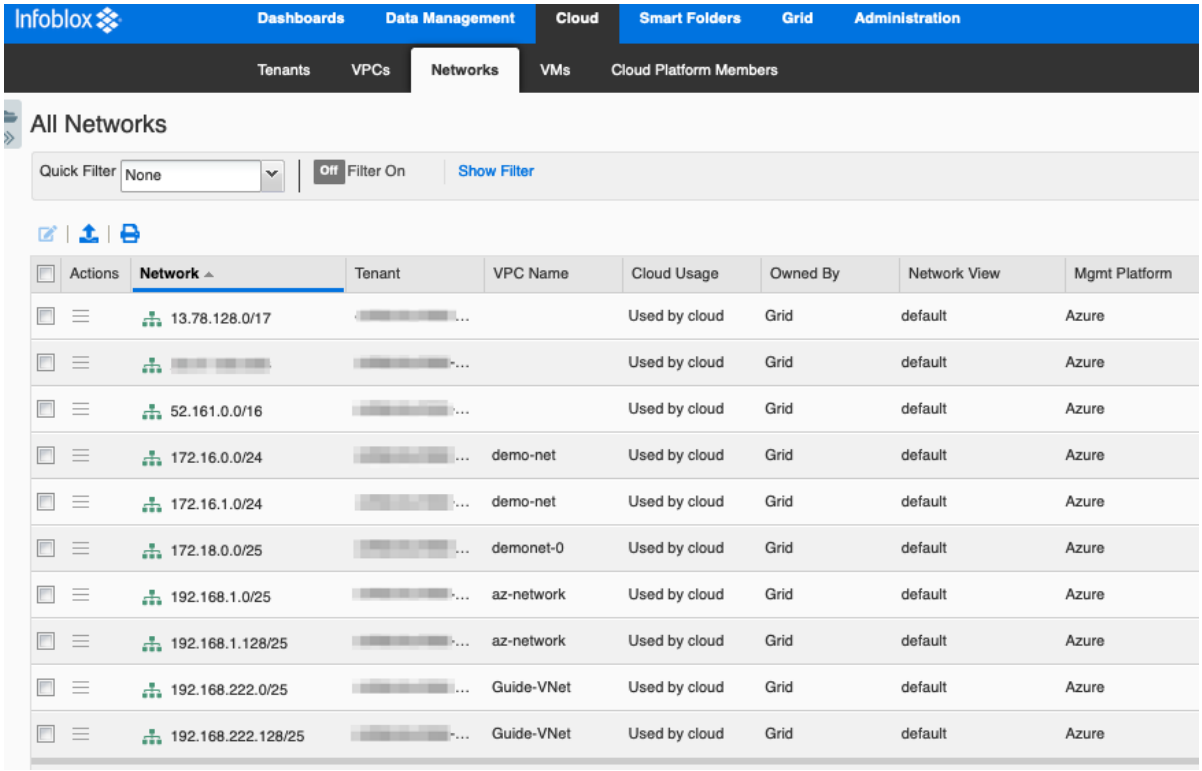
- **Tenants**: For Azure vDiscovery, entries on this tab correspond to Azure AD tenants. You can drill down to review all VNets and VMs that have been discovered under that tenant.



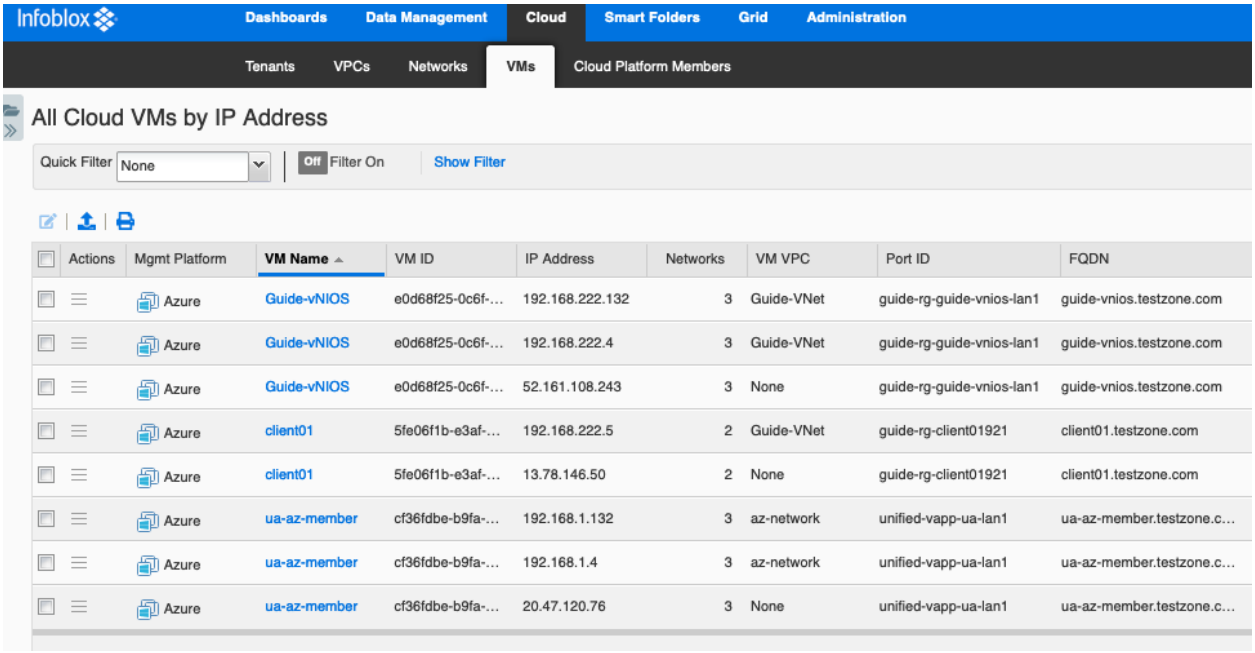
- **VPCs**: This tab displays any discovered Azure VNets. You can drill down to review all subnets and VMs that have been discovered under an individual VNet.



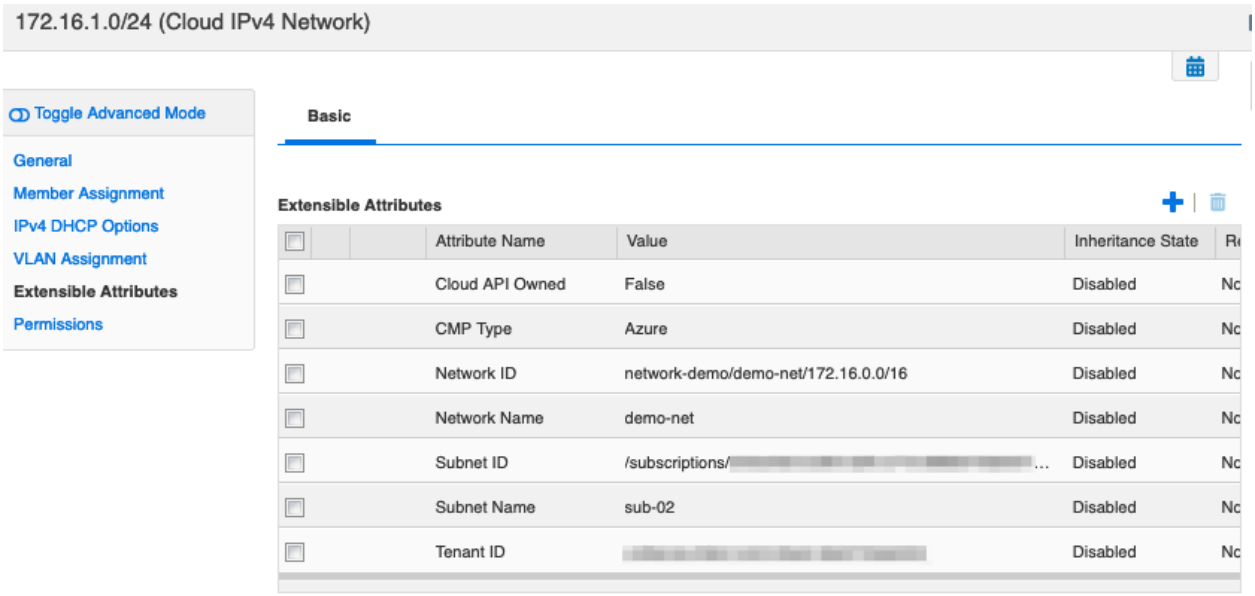
- **Networks**: This tab displays all subnets that have been discovered in your Azure VNets. Easily jump to IPAM or other perspectives to view additional details for a subnet. Searches, Smart Folders and reports can also leverage the metadata stored as EAs for each subnet.



- **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.



- **Extensible Attributes**: 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.



- **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/.

Alternative Deployment Method

You can also deploy vNIOS instances to Azure using the Azure Command Line Interface (CLI). You can use this method to achieve configurations that may not be readily available in marketplace deployments, for example deploying multiple vNIOS VMs into a single resource group. For details on using the Azure CLI to deploy vNIOS, refer to Infoblox documentation: https://docs.infoblox.com/display/vniosazure/Deploying+vNIOS+for+Azure+from+the+CLI.

Additional Resources

- Infoblox Documentation: https://docs.infoblox.com/
- Infoblox Community: https://community.infoblox.com/
- Infoblox Support (account required): https://support.infoblox.com/

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