vNIOS™ Infoblox Installation Guide for Microsoft Azure®
1. Infoblox vNIOS for Azure ................................................................. 3
2. About Infoblox vNIOS for Azure ................................................... 4
3. Prerequisites .............................................................................. 5
4. Deploying vNIOS for Azure from the Marketplace ....................... 6
   4.1 Configuring Basic Settings ......................................................... 7
   4.2 Configuring VM Settings ........................................................ 8
   4.3 Validating and Accepting Configuration .................................. 10
   4.4 Purchasing and Deploying the Virtual Appliance .................... 11
5. Configuring vNIOS for Azure as the Primary DNS Server ............... 13
6. Performing vDiscovery on VNets ................................................ 14
   6.1 Integrating vDiscovery with Azure Active Directory ............... 15
   6.2 Adding vDiscovery Application as a New User ....................... 23
   6.3 Creating DNS Records for Discovered IP Addresses .......... 24
Infoblox vNIOS for Azure

This chapter provides information about the Infoblox vNIOS for Azure virtual appliance and explains how to deploy it through the Microsoft Azure Marketplace.

Infoblox vNIOS for Azure is a virtual Infoblox appliance designed to operate in the Microsoft Cloud. For information about Microsoft Cloud and Azure, refer to the Microsoft documentation at https://azure.microsoft.com/en-us/overview/what-is-azure. This chapter includes the following topics:

- About Infoblox vNIOS for Azure
- Prerequisites
  - Supported vNIOS for Azure Models
- Deploying vNIOS for Azure from the Marketplace
  - Configuring Basic Settings
  - Configuring VM Settings
  - Validating and Accepting Configuration
  - Purchasing and Deploying the Virtual Appliance
- Configuring vNIOS for Azure as the Primary DNS Server
- Performing vDiscovery on VNets
  - Integrating vDiscovery with Azure Active Directory
  - Adding vDiscovery Application as a New User
  - Creating DNS Records for Discovered IP Addresses
About Infoblox vNIOS for Azure

Infoblox vNIOS for Azure is an Infoblox virtual appliance designed for deployments through Microsoft Azure, a collection of integrated cloud services in the Microsoft Cloud.

The vNIOS for Azure enables you to deploy robust, manageable, and cost effective Infoblox appliances in the Microsoft Cloud. Infoblox NIOS provides core network services and a framework for integrating all the components of the modular Infoblox solution. It provides integrated, secure, and easy-to-manage DNS (Domain Name System) and IPAM (IP address management) services. For more information about the Infoblox Grid, DNS, and IPAM, refer to the Infoblox NIOS Documentation.

You can deploy one or more Infoblox vNIOS for Azure instances through the Microsoft Azure Marketplace and provision them to join the on-prem NIOS Grid. You can then use the vNIOS for Azure instance as the primary DNS server to provide enterprise-grade DNS and IPAM services in the Microsoft Cloud. For information, see Configuring vNIOS for Azure as the Primary DNS Server. You can also utilize Infoblox Cloud Network Automation with your vNIOS for Azure instances to streamline with IPAM, improve visibility of your cloud networks, and increase the flexibility of your cloud environment.

After you spin up your Infoblox vNIOS for Azure instances, you can use vDiscovery to discover and to periodically re-discover all resources in the VNets (Azure virtual networks) within your Microsoft Cloud. For information about how to set up vDiscovery in Azure, see Performing vDiscovery on VNets.
Prerequisites

Before you deploy the vNIOS for Azure, ensure that you have completed the following:

- Set up a Microsoft Azure account and create a resource manager in Azure.
- This is required only if you want to join the vNIOS for Azure instance to the on-prem Grid. Configure an on-prem Infoblox Grid or Grid Master. For more information, refer to the Infoblox NIOS Documentation.

Supported vNIOS for Azure Models

This section lists the supported vNIOS for Azure appliance models for different NIOS releases.

The following table lists the vNIOS for Azure appliance models that are supported for NIOS 8.1.x and earlier releases.

<table>
<thead>
<tr>
<th>vNIOS Appliance</th>
<th>Overall Disk (GB)</th>
<th># of vCPU Cores</th>
<th>Memory Allocation (GB)</th>
<th>Virtual Machine Size</th>
<th>Supported as Grid Master and Grid Master Candidate</th>
</tr>
</thead>
<tbody>
<tr>
<td>TE-V820</td>
<td>160</td>
<td>2</td>
<td>4</td>
<td>DS2 Standard or DS2_V2 Standard</td>
<td>Yes</td>
</tr>
<tr>
<td>TE-V1420</td>
<td>160</td>
<td>4</td>
<td>8</td>
<td>DS3 Standard or DS3_V2 Standard</td>
<td>Yes</td>
</tr>
<tr>
<td>TE-V2200</td>
<td>160</td>
<td>4</td>
<td>12</td>
<td>DS3 Standard or DS3_V2 Standard</td>
<td>Yes</td>
</tr>
<tr>
<td>CP-V800</td>
<td>160</td>
<td>2</td>
<td>2</td>
<td>DS2 Standard or DS2_V2 Standard</td>
<td>No</td>
</tr>
<tr>
<td>CP-V1400</td>
<td>160</td>
<td>4</td>
<td>8</td>
<td>DS3 Standard or DS3_V2 Standard</td>
<td>No</td>
</tr>
<tr>
<td>CP-V2200</td>
<td>160</td>
<td>4</td>
<td>12</td>
<td>DS3 Standard or DS3_V2 Standard</td>
<td>No</td>
</tr>
</tbody>
</table>

The following table lists the vNIOS for Azure appliance models that are supported for NIOS 8.2.0 and later releases.

<table>
<thead>
<tr>
<th>vNIOS Appliance</th>
<th>Overall Disk (GB)</th>
<th># of vCPU Cores</th>
<th>Memory Allocation (GB)</th>
<th>Virtual Machine Size</th>
<th>Supported as Grid Master and Grid Master Candidate</th>
</tr>
</thead>
<tbody>
<tr>
<td>TE-V825</td>
<td>250</td>
<td>2</td>
<td>14</td>
<td>DS11_V2 Standard</td>
<td>Yes</td>
</tr>
<tr>
<td>TE-V1425</td>
<td>250</td>
<td>4</td>
<td>28</td>
<td>DS12_V2 Standard</td>
<td>Yes</td>
</tr>
<tr>
<td>TE-V2225</td>
<td>250</td>
<td>8</td>
<td>56</td>
<td>DS13_V2 Standard</td>
<td>Yes</td>
</tr>
<tr>
<td>CP-V800</td>
<td>160</td>
<td>2</td>
<td>7</td>
<td>DS2 Standard or DS2_V2 Standard</td>
<td>No</td>
</tr>
<tr>
<td>CP-V1400</td>
<td>160</td>
<td>4</td>
<td>14</td>
<td>DS3 Standard or DS3_V2 Standard</td>
<td>No</td>
</tr>
<tr>
<td>CP-V2200</td>
<td>160</td>
<td>4</td>
<td>14</td>
<td>DS3 Standard or DS3_V2 Standard</td>
<td>No</td>
</tr>
</tbody>
</table>

The following table lists the vNIOS for Azure appliance models that are supported for NIOS 8.4.0 and later releases.

<table>
<thead>
<tr>
<th>vNIOS Appliance</th>
<th>Overall Disk (GB)</th>
<th># of vCPU Cores</th>
<th>Memory Allocation (GB)</th>
<th>Virtual Machine Size</th>
<th>Supported as Grid Master and Grid Master Candidate</th>
</tr>
</thead>
<tbody>
<tr>
<td>CP-V805</td>
<td>250</td>
<td>2</td>
<td>16</td>
<td>DS11_V2 Standard</td>
<td>No</td>
</tr>
<tr>
<td>CP-V1405</td>
<td>250</td>
<td>4</td>
<td>32</td>
<td>DS12_V2 Standard</td>
<td>No</td>
</tr>
<tr>
<td>CP-V2205</td>
<td>250</td>
<td>8</td>
<td>64</td>
<td>DS13_V2 Standard</td>
<td>No</td>
</tr>
</tbody>
</table>

Note:

* Trinzic vNIOS appliances (TE-V825, TE-V1425, TE-V2225) for Azure do not support downgrading from NIOS 8.2.x to any earlier NIOS releases. After you successfully install a vNIOS for Azure instance, you may upgrade to a supported NIOS software release on the instance. The vNIOS for Azure is supported starting with NIOS 8.0.0; therefore, downgrading to an earlier NIOS 8.0.0 version will fail. If for any reason your upgrade fails, you can review the Infoblox syslog to find out the reasons for the failure. For information about how to access the syslog, refer to the Infoblox NIOS Documentation.
* CP-V800, CP-V1400, and CP-V2200 are not supported from NIOS 8.4.0 and later releases.
* CP-V805, CP-V1405, and CP-V2205 do not support downgrading from NIOS 8.4.x to any earlier NIOS releases and is only supported in NIOS 8.4 and later releases.
Deploying vNIOS for Azure from the Marketplace

You can easily download and deploy vNIOS for Azure virtual appliances directly from the Azure Marketplace. The vNIOS for Azure virtual appliance is pre-configured for Microsoft Azure so you only need to take a few easy steps to complete the deployment.

To deploy vNIOS for Azure virtual appliance directly from the Azure Marketplace, complete the following (as illustrated in Figure 1.1):

1. For Azure, go to Microsoft Azure web site. For Azure Government Cloud, go to Microsoft Azure Government Cloud web site.
2. Log in to your Microsoft Azure account.
3. On the Microsoft Azure Portal, enter “infoblox” as the search filter, and then select one of the Azure virtual appliances from the search results:
   - Select Infoblox DDI for Microsoft Azure, to deploy vNIOS versions 8.4.0 or below; such as vNIOS 8.2.1, 8.3.0, or 8.4.0.
   - Select Infoblox NIOS 8.4.3 for DDI, to deploy vNIOS version 8.4.3.
4. Use Resource Manager as the deployment model for the new virtual appliance.

   Figure 1.1 Selecting Infoblox DDI for Microsoft Azure for version 8.4.0 and below

   Infoblox DDI for Microsoft Azure

   - Select Infoblox DDI for Microsoft Azure, to deploy vNIOS versions 8.4.0 or below; such as vNIOS 8.2.1, 8.3.0, or 8.4.0.

   Figure 1.2 Selecting Infoblox NIOS 8.4.3 for DDI

   Infoblox NIOS 8.4.3 for DDI

   - Select Infoblox NIOS 8.4.3 for DDI.

5. Click Create and complete the following steps to deploy vNIOS for Azure:
   - Configuring Basic Settings
   - Configuring VM Settings
   - Validating and Accepting Configuration
   - Purchasing and Deploying the Virtual Appliance
Configuring Basic Settings

In the Basics panel, complete the following (as illustrated in Figure 1.2):

- **NIOS model**: From the drop-down list, select the vNIOS model that will be installed on the VM.
- **NIOS VM name**: Enter the VM name that will be used in the Azure portal.
- **Password for 'admin' user**: Enter a password for the admin user. The admin user can make changes to all configuration for this virtual appliance. The password must be between size (6) and 64 characters long and contains from at least three (3) of the following groups: upper case alphabetic character, lower case alphabetic character, numeric number, and special character. Re-enter the password to confirm.
- **Subscription**: You can select the subscription on which you want to create the virtual appliance. This is a pay-as-you-go subscription by default.
- **Resource group**: You must create a new resource group to which this virtual appliance belongs. Enter a unique name for this resource group. You will receive an error message if you use the name of an existing resource group. A resource group is a collection of resources that share the same life cycle, permissions, and policies.
- **Location**: From the drop-down list, select the physical site in which the virtual appliance resides. You must select a site that is compatible with the vNIOS for Azure virtual appliance. The following are the compatible sites: Central US, East US, East US 2, North Central US, South Central US, West US, North Europe, West Europe, East Asia, Southeast Asia, Japan East, Japan West, Australia East, and Australia Southeast.

Figure 1.2 Configuring Basic Settings

<table>
<thead>
<tr>
<th>1</th>
<th>Basics</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Create Infoblox DDI for Microsoft Azure</strong></td>
<td><strong>Configure basic settings</strong></td>
<td></td>
</tr>
<tr>
<td>NIOS model</td>
<td>TE-V1425</td>
<td></td>
</tr>
<tr>
<td><em>NIOS VM name</em></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Password for 'admin' user</td>
<td></td>
<td></td>
</tr>
<tr>
<td><em>'admin' password</em></td>
<td></td>
<td></td>
</tr>
<tr>
<td><em>Confirm 'admin' password</em></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Subscription</td>
<td>TEST2</td>
<td></td>
</tr>
<tr>
<td><em>Resource group</em></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Select existing...</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create new</td>
<td></td>
<td></td>
</tr>
<tr>
<td><em>Location</em></td>
<td>(US) East US</td>
<td></td>
</tr>
</tbody>
</table>

Click OK after you complete the basic configuration. The Portal prompts you to configure VM settings, as described in Configuring VM Settings.
Configuring VM Settings

To ensure that your vNIOS for Azure functions properly, you can set up certain configuration in the Azure Portal. In the NIOS VM settings panel, complete the following (as illustrated in Figure 1.3). Note that some of the fields are automatically populated with values based on previous configuration. Click a field that you want to make changes to. The portal displays relevant information in the right panel. Ensure that you click OK to save changes for each configuration. If certain configuration is missing or invalid, the portal displays a red warning sign next to the field. Click the field to enter valid information.

- **NIOS Version**: Select the NIOS version to run on the selected VM.
- **Virtual Machine Size**: Depending on your selected virtual machine model, you may or may not be able to select a VM size. The portal displays the recommended option by default. You can click View all to see all available options. Click Select to save your selection.

The virtual machine series available under US Gov Iowa region does not support the launching of vNIOS. For more information on the supported virtual machines, see, Azure Products by Region.

- **Storage account**: Click this option to configure the storage account. The Portal opens the Choose storage account panel from which you can select an existing account in the selected location and subscription. This account gives you access to resources in the Azure Storage, which provides a namespace for your DNS data objects. By default, the data in the Azure account is available only to the account owner. You can also click + Create storage account panel to create a new account as follows:
  - **Name**: Enter a name for the storage account you are about to create. The name must have a minimum of 3 characters and a maximum of 24 characters, and it can contain only lower case alphabetic characters and numeric numbers.
  - **Performance**: This field indicates the type of storage account for the data storage. For virtual appliances, you must use Premium storage accounts. You cannot change this to Standard. Premium storage accounts are backed by solid-state drives and offer consistent and low-latency performance. They are used only with Azure virtual machine disks, and are best for I/O-intensive appliances such as databases. Standard storage accounts are backed by magnetic drives and provide the lowest cost per GB of memory. They are the best type of storage account for applications that require bulk storage or where data is accessed infrequently. If you want to create a storage account to save all diagnostics files associated with the VM, click Storage account for BootDiagnostics to create the standard account. You can create a new account or select an existing one from the available list.
  - **Replications**: This field displays the default replication strategy. The data in your Azure storage account is always replicated to ensure durability and high availability. The default replication strategy matches the durability requirements your appliance needs. You might not be able to change this once the storage account is created.

- **Storage account for BootDiagnostics**: Click this option to create a Standard storage account to save all diagnostics files associated with the VM.

- **Virtual network (VNET)**: Select an existing virtual network or create a new one in which the virtual appliance resides. To create a new network, complete the following in the Create virtual network panel:
  - **Name**: Enter the name of the virtual network.
  - **Address space**: Enter the range of the IP address space for the virtual network in the CIDR format. Example: 10.11.0.0/16.
  - **Subnets**: Click this to configure the settings of the network interfaces. Infoblox vNIOS virtual appliances require two network interfaces (LAN1 and MGMT) for proper Grid communications. These interfaces must be assigned to separate subnets within the same Azure virtual network. By default, only the LAN1 communication is activated and all traffic goes through the LAN1 interface (including management and protocol services). If you want to change this configuration, you must activate the MGMT port in the Grid configuration (for information, refer to the Infoblox NIOS Documentation). When you set up the MGMT interface, ensure that you use the same IP address that is currently defined for the NIC card on the Azure portal for the Infoblox GUI. Depending on your configuration, you may have the GUI communication going through the MGMT interface only when you activate the MGMT port.

- **Public IP address**: If you need to communicate with the virtual appliance outside of the virtual network, click here to create a public IP address. In the Choose public IP address panel, you can select an existing public IP address or create a new one by clicking + Create new, and then enter the IP address in the Create public IP address panel. You can select whether this IP is Dynamic or Static. Note that the public IP address can only be associated with the primary interface (LAN1 by default). However, if you change the networking options in NIOS, such as attaching the public IP address to the MGMT interface (because there is no way to change the attachment to another interface), then you must re-map your interfaces so that the current LAN1 is renamed to MGMT and is attached to the MGMT network.

- **Public DNS name**: When you create a public IP address, enter the DNS name for the public address.

- **Install temporary licenses**: Click yes to install the following temporary licenses on your virtual appliance: vNIOS, Grid, DNS, and CNA (Cloud Network Automation). This also installs temporary license of NIOS for these 3 appliances - TE-V825, TE-V1425 and TE-V2225. Installing temporary licenses might prolong the installation time by up to five minutes. Note that the CNA license is active only when the virtual appliance is configured as the Grid Master; the license has no effect on Grid members.

- **Enhanced options**: You may coordinate with Infoblox Technical Support to upload files with custom data. Click OK to save the VM configuration.

Figure 1.3 Configuring VM Settings
Select a VM size

Showing 1 VM sizes.

<table>
<thead>
<tr>
<th>VM SIZE</th>
<th>DATA DISKS</th>
<th>MEMORY</th>
<th>CPU</th>
<th>RAM (GB)</th>
<th>TEMP DISK</th>
<th>TEMP STORAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>DS12_v2</td>
<td>Standard</td>
<td>Memory-optimized</td>
<td>4</td>
<td>28</td>
<td>16</td>
<td>12800</td>
</tr>
</tbody>
</table>

Select by VM size...  ×  Restore default filters

Add filter

NIOS VM settings

NIOS version for TE-V142S
EA3

Virtual machine size for TE-V142S
1x Standard DS12_v2
4 vCPUs, 28 GB memory

Storage account
Configure required settings

Storage account for NIOS Diagnostics
Configure required settings

Virtual network
(none) amit

Subnets
Configure subnets

Public IP address
None

Public DNS name
centralindia.cloudapp.azure.com

Licenses
Install temporary licenses
Yes

Enhanced options
Upload file with custom data if required
Select a file
Validating and Accepting Configuration

After you have entered and saved your VM configuration, you can view the information in the Summary panel. If for any reason you need to make changes to the configuration, you can go back to step 2 (Configure VM settings) to do so. If the configuration is correct, click OK to accept (as illustrated in Figure 1.4).

Figure 1.4 Viewing VM Summary
Purchasing and Deploying the Virtual Appliance

You are now ready to deploy the vNIOS for Azure virtual appliance that you have previously configured. The *Purchase* panel displays the details about your purchase (as illustrated in Figure 1.5). Please peruse the information in this panel so you fully understand the price, the terms of use, and privacy policies of your deployment.

Click **Create** to begin deployment of your Infoblox vNIOS for Azure appliance. This process might take up to 10 minutes to complete. If you have chosen to install temporary licenses, the process might take an additional five minutes. You can monitor the process in your Azure Dashboard.

**Note**

You will be purchasing the VM, storage, and IP address on an hourly basis payable to Microsoft Azure through your Azure account. If you have not installed the Infoblox NIOS temporary licenses, you can purchase them through your Infoblox representatives or contact Infoblox Technical Support.

When the virtual appliance is deployed successfully, you will receive an alert and the Azure Portal displays the *Resource group overview* panel from which you can see an overview of the deployment in the *Essentials* section. You can now complete the following to set up your vNIOS for Azure virtual appliances:

- Setting the virtual appliance as the primary DNS server, as described in *Configuring vNIOS for Azure as the Primary DNS Server*.
- Locating network devices on VNets by performing a vDiscovery, as described *Performing vDiscovery on VNets*.

*Figure 1.5 Purchasing the vNIOS for Azure Virtual Appliance*
Infoblox DDI for Microsoft Azure
by Infoblox Inc.

Terms of use | privacy policy

Deploying this template will result in various actions being performed, which may include the deployment of one or more Azure resources or Marketplace offerings and/or transmission of the information you provided as part of the deployment process to one or more parties, as specified in the template. You are responsible for reviewing the text of the template to determine which actions will be performed and which resources or offerings will be deployed, and for locating and reviewing the pricing and legal terms associated with those resources or offerings.

Current retail prices for Azure resources are set forth here and may not reflect discounts applicable to your Azure subscription.

Prices for Marketplace offerings are set forth here, and the legal terms associated with any Marketplace offering may be found in the Azure portal; both are subject to change at any time prior to deployment.

Neither subscription credits nor monetary commitment funds may be used to purchase non-Microsoft offerings. These purchases are billed separately. If any Microsoft products are included in a Marketplace offering (e.g., Windows Server or SQL Server), such products are licensed by Microsoft and not by any third party.

Template deployment is intended for advanced users only. If you are uncertain which actions will be performed by this template, which resources or offerings will be deployed, or what prices or legal terms pertain to those resources or offerings, do not deploy this template.

Terms of use

By clicking “Create”, I (a) agree to the legal terms and privacy statement(s) provided above as well as the legal terms and privacy statement(s) associated with each Marketplace offering that will be deployed using this template, if any; (b) authorize Microsoft to charge or bill my current payment method for the fees associated with my use of the offering(s), including applicable taxes, with the same billing frequency as my Azure subscription, until I discontinue use of the offering(s); (c) agree that Microsoft may share my contact information and transaction details with any third-party sellers of the offering(s); and (d) give Microsoft permission to share my contact information so that the provider of the template can contact me regarding this product and related products. Microsoft assumes no responsibility for any actions performed by third-party templates and does not provide rights for third-party products or services. See the Azure Marketplace Terms for additional terms.

By clicking Create, you give Microsoft permission to use or share your account information so that the provider or Microsoft can contact you regarding this product and related products.

| Page 12 |
Configuring vNIOS for Azure as the Primary DNS Server

To use vNIOS for Azure as the primary DNS server, complete the following in the Azure Portal (as illustrated in Figure 1.6):

1. Go to the Microsoft Azure web site.
2. Log in to your Microsoft Azure account.
3. On the Microsoft Azure web site, select the VNet for which you want vNIOS for Azure to serve DNS.
4. Click Settings -> DNS servers.
5. In the DNS servers panel, complete the following:
   - DNS servers: Select Custom DNS.
   - Primary DNS server: Enter the IP address of the vNIOS for Azure.

   Note
   For detailed information about setting primary DNS servers in Azure, refer to the Microsoft documentation.

6. Click Save at the top of the panel.

Figure 1.6 Configuring DNS Server in Azure
Performing vDiscovery on VNets

Infoblox provides vDiscovery for detecting and obtaining information about virtual entities and interfaces in the Microsoft Cloud. Infoblox vDiscovery supports the resource manager model in the Azure Portal. However, you must first register the new vDiscovery application with Azure Active Directory through the Azure classic portal.

**Note**

Discovered virtual networks in Microsoft Cloud is mapped to Network Containers in NIOS.

To perform a vDiscovery job for a VNet, complete the following tasks:

1. Configure DNS resolver in NIOS, as described in Configuring DNS Resolver.
2. Register an application with the Azure Active Directory through the Azure classic portal, as described in Integrating vDiscovery with Azure Active Directory.
3. Add the new application as a user through the Azure resource manager portal, as described in Adding vDiscovery Application as New User.
4. Perform vDiscovery for service instances and subnets in selected VNets. For detailed information, refer to Configuring vDiscovery Jobs in the Infoblox NIOS Documentation. When configuring the endpoint for the vDiscovery job, ensure that you select the following:
   - **Server Type**: Select Azure.
   - **Client ID**: Use the CLIENT ID you obtained for the application you created in Azure.
   - **Client Secret**: Enter the key value of the application to authenticate the user account.
   - **Service Endpoint**: Use the token endpoint URL you selected for the new application.
5. After performing a vDiscovery job on your VNets, you can view and manage discovered data in NIOS. For detailed information, refer to Infoblox NIOS Documentation. You can also create DNS records for discovered IP addresses. For information, see Creating DNS Records for Discovered IP Addresses.

Azure Government Cloud vDiscovery job uses different service endpoints than that of Azure. The following table illustrates the use case of different endpoints:

<table>
<thead>
<tr>
<th>Service Endpoint Pattern</th>
<th>API Endpoint</th>
<th>Service Management Endpoint</th>
</tr>
</thead>
</table>

**Note**

Infoblox vNIOS configured in Azure does not currently support DHCP.

Configuring DNS Resolver

To perform vDiscovery for all resources in your Microsoft VNets, you must enable DNS resolvers in NIOS. To configure DNS resolver for the Grid, complete the following in the NIOS GUI, Grid Manager:

1. From the Grid tab -> Grid Manager tab -> Members tab, expand the Toolbar, and then click Grid Properties.
2. In the Grid Properties editor, do the following:
   - Click the DNS Resolver tab and select the Enable DNS Resolver check box if it is not already selected.
   - In the Name Servers list, click Add to add the IP address of the upstream DNS server to the list.
   - Enter the IP address and press Enter.
3. Save the configuration. The changes may take a brief period of time to become active.
Integrating vDiscovery with Azure Active Directory

Before creating a vDiscovery job and performing vDiscovery in Azure, you must integrate the discovery application with Azure Active Directory (Azure AD) to provide secure sign in and authorization. To integrate the application with Azure AD, you must first register the application details with Azure AD through the Azure portal.

You can also register a service principal using the Azure CLI or PowerShell. If you choose to use the CLI or PowerShell, refer to the Microsoft documentation for information about the Azure authentication mechanism and how to create a service principal with Azure Resource Manager, available at https://azure.microsoft.com/en-us/documentation/articles/resource-group-authenticate-service-principal/#authenticate-service-principal-with-password---azure-cli.

If you choose to use the Azure portal to register a service principal, you may still need to use the Azure CLI or PowerShell to customize the access scope for the newly created service principal. The default access scope is the subscription scope that is associated with the user who creates the service principal.

To create and integrate a vDiscovery application through the Azure portal:

1. In the Microsoft Azure portal, click All Services.
2. Search for “Azure Active Directory” and click to open Azure Active Directory.
3. Click App Registrations in the left panel.
4. In the App registrations panel, either select an existing discovery application or click + New registration to add a new application.
5. If you are adding a new application, enter the following to define your application in the **Register an application** wizard, and then click **Register** to add the application.

- **Name**: Enter the name of your new application.
- **Supported account types**: Select the account type.
- **Redirect URI**: Ensure that you use a unique URL for sign-on purposes.

Azure notifies you when the application is successfully created.

To obtain token information for the endpoints, click the **Endpoints** icon next to **New registration** in the **App registration** panel. Azure displays the **Endpoints** page that contains endpoint information for the discovery application. vDiscovery uses the **OAUTH 2.0 TOKEN ENDPOINT** (the second last item on the list). Copy the link from the table. You use this information to define the vDiscovery endpoint in NIOS. The token corresponds to the **Service Endpoint** field in NIOS.
6. Select and click the application from the list. The Azure portal displays details about your application, such as Display name, Application ID, Directory ID, and Object ID. Click API permissions in the left panel, and then click + Add a permission in the API Permissions panel.

Note

Ensure that you copy the Application ID and save this value for future use. This ID is used as the Client ID in your vDiscovery configuration.

API permissions

Applications are authorized to use APIs by granting/deny access.

+ Add a permission

API / PERMISSIONS NAME

Microsoft Graph (1)

User.Read

These are the permissions that this application able permissions dynamically through code.

Grant consent

To consent to permissions that require admin directory.

Grant admin consent for Infoblox Inc
7. In the Request API permissions panel, click APIs my organization uses.
8. Select Windows Azure Service Management API from the list.

<table>
<thead>
<tr>
<th>API / PERMISSIONS NAME</th>
<th>TYPE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Azure Service Management API</td>
<td>Delegated</td>
</tr>
<tr>
<td>Windows Store for Business</td>
<td>Delegated</td>
</tr>
<tr>
<td>Windows Defender ATP</td>
<td>Delegated</td>
</tr>
</tbody>
</table>

9. Select Delegated permissions and Access Azure Service Management as organization users (preview) check box, and then click Add permission.

10. In the left panel, click Certificates & secrets, and then click +New client secret:
    — **Description**: Enter a name or description for the generated key.
    — **Expires**: Select expiry time for the generated key.
    — **Value**: The key will be displayed here after you select the expiry time and save the configuration.

**Note**
Copy the key and save it for your vDiscovery jobs. The key corresponds to the Client Secret in NIOS when you configure vDiscovery jobs.
11. Validate all the configuration and information on this page.

Note

The vDiscovery in Azure is performed on the whole subscription, or resource groups linked to the application.

- **Subscription**: All entities within the subscription will be discovered including the VMs, network interfaces, and VNets.
- **Resource group**: All entities within the specified resource groups will be discovered including the VMs, network interfaces, and VNets. If the discovery of all entities within a subscription is not desired, additional granularity in vDiscovery can be achieved by individually allotting permissions to a resource group.

12. Perform the vDiscovery on **Subscription** or **Resource group** linked to your Azure application.
   a. To perform vDiscovery for resources on **Subscription** you need to perform the following:
      i. Navigate to All services -> Subscriptions.
      ii. Click on the name for your subscription.
iii. Click Access control (IAM).

![Image]

iv. Click Add.

![Image]

b. To perform vDiscovery for resources on **Resource group** you need to perform the following:

i. Navigate to All services -> Resource groups.

![Image]

ii. Click on the name for your Resource groups.

![Image]

iii. Click Access control (IAM).
iv. Click **Add**

13. Expand the **Role** drop-down menu and select **Reader**.

14. In the **Select** box, type the name for your registered app, or locate and select it in the **Selected members** list.

15. Click **Save**. You have completed the vDiscovery configuration in Azure.

**Note**

If Reader role IAM permission is given just to VMs instead of the Subscription or Resource group on Azure, then vDiscovery will not discover any virtual entities.

To configure vDiscovery jobs in NIOS, you must record the following information from the Azure portal:

- **Token Endpoint**: This corresponds to the Service Endpoint field in NIOS. vDiscovery uses the **OAUTH 2.0 TOKEN ENDPOINT (v1)** however, **OAUTH 2.0 TOKEN ENDPOINT (v2)** is not supported. You can copy this from the **Endpoints** panel.
- **Application ID**: This corresponds to the **Client ID** when you configure end point information in NIOS.
• **Key**: Copy the key from the Keys panel and use that for the **Client Secret** field in NIOS.

The following describes the corresponding fields for Azure and NIOS when you configure vDiscovery job properties:

Note
You can specify the same client ID and client secret for a vDiscovery job in which multiple subscriptions are associated with a single application.
Adding vDiscovery Application as a New User

After you have set up the vDiscovery application in Azure Active Directory, you must add this application as a new user to your vNIOS for Azure subscription through the Azure resource manager portal, and then define its administrative role.

To add the application as a new user and define its role:

1. Go to the Access control (IAM) page of your subscription.
2. On the Access control (IAM) page, click + Add at the top of the page to add a new user.
3. In the Add permissions panel, select Reader as the role, and then select a user or a group as the member(s) for the user role. The portal displays all the selected members in this panel.
4. Click Save.

You have added the new vDiscovery application as a user with the Reader role.

You can now configure and perform a vDiscovery job through Grid Manager (Infoblox GUI). Ensure that you have the following information that you previously recorded in order to configure a vDiscovery job:

- **Client ID** = Client ID in NIOS
- **Key value** = Client Secret in NIOS
- **Token endpoint URL** = Service Endpoint in NIOS

When creating a new vDiscovery job, select Azure as the **Server Type**. Infoblox also recommends that you select "The tenant’s network view" as the network views for both public and private IP addresses. For detailed information about vDiscovery jobs and how to configure them, refer to Configuring vDiscovery Jobs in the Infoblox NIOS Documentation.
Creating DNS Records for Discovered IP Addresses

When you configure vDiscovery jobs, you can enable the appliance to automatically create DNS records for discovered virtual entities in your VNets. When you enable this feature, NIOS automatically adds Host records or A and PTR records to the authoritative zones for the discovered IP addresses based on your configuration. You can also enter a formula that NIOS uses to create the DNS names for the discovered IP addresses based on their VM parameters such as vm_name or discovered_name for data discovered through Azure. By doing so, NIOS is able to discover public and private IP addresses by looking up the corresponding DNS names.

Discovered data includes IP addresses for the VMs and associated information such as VM name, VM ID, tenant ID, and others. Note that corresponding zones must already exist in order for NIOS to add DNS records. Otherwise, NIOS does not add any DNS records and it logs a message to the syslog.

NIOS automatically adds DNS records (in the network views specified for vDiscovery) based on the following conditions:

- The corresponding DNS zones must already exist in the NIOS database. NIOS does not automatically create DNS zones for the records.
- To create a PTR records, the corresponding reverse-mapping zone must exist.
- A DNS zone cannot be associated with more than one DNS view. NIOS does not create DNS records for zones that are associated with multiple DNS views.
- NIOS adds new DNS records only if the VM name for the discovered IP address is available and there is no conflict between the discovered data and the associated network view.

The following matrix captures some scenarios about how vDiscovery handles various actions and what the outcome is for the information on the Cloud Platform appliance and in the NIOS database.

Note

vDiscovery modifies records that are created by the vDiscovery process only. It does not create or update DNS records that are originally created by other admin users.

<table>
<thead>
<tr>
<th>Actions and Conditions</th>
<th>Cloud Platform Data before vDiscovery</th>
<th>Cloud Platform Data after vDiscovery</th>
<th>NIOS Data before vDiscovery</th>
<th>NIOS Data after vDiscovery</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add new VM (vma) on Cloud Platform appliance</td>
<td>No data for vma</td>
<td>10.10.10.1, vma.corpxyz.com</td>
<td>Zone: corpxyz.com</td>
<td>Zone: corpxyz.com Host record: vma, corpxyz.com (10.10.10.1)</td>
</tr>
<tr>
<td>Automatic creation of Host records</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>In NIOS: existing zone corpxyz.com; no DNS records</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Add new VM (vma) on Cloud Platform appliance</td>
<td>No data for vma</td>
<td>10.10.10.1, vma.corpxyz.com</td>
<td>Zone: corpxyz.com Host record: vma, corpxyz.com (10.10.10.1)</td>
<td>Zone: corpxyz.com Host record: vma, corpxyz.com (10.10.10.2)</td>
</tr>
<tr>
<td>Automatic creation of Host records</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>In NIOS: existing zone corpxyz.com; existing Host record (originally created by vDiscovery or admin)</td>
<td>10.10.10.1 vma.corpxyz.com</td>
<td>10.10.10.1 vma.corpxyz.com</td>
<td>Zone: corpxyz.com Host record: vma, corpxyz.com (10.10.10.1)</td>
<td>Zone: corpxyz.com Host record: vma, corpxyz.com (10.10.10.1)</td>
</tr>
<tr>
<td>Add new interface to existing VM (vma) with the same discovered name on Cloud Platform appliance</td>
<td>10.10.10.1 vma.corpxyz.com</td>
<td>10.10.10.1 vma.corpxyz.com</td>
<td>Zone: corpxyz.com Host record: vma, corpxyz.com (10.10.10.1)</td>
<td>Zone: corpxyz.com Host record: vma, corpxyz.com (10.10.10.1)</td>
</tr>
<tr>
<td>Automatic creation of Host records</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>In NIOS: existing zone corpxyz.com; existing Host record (originally created by vDiscovery)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Add new interface to existing VM (vma) with different discovered name (vmb) on Cloud Platform appliance</td>
<td>10.10.10.1 vma.corpxyz.com</td>
<td>10.10.10.1 vma.corpxyz.com</td>
<td>Zone: corpxyz.com Host record: vma, corpxyz.com (10.10.10.1)</td>
<td>Zone: corpxyz.com Host record: vma, corpxyz.com (10.10.10.2)</td>
</tr>
<tr>
<td>Automatic creation of Host records</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>In NIOS: existing zone corpxyz.com; existing Host record (originally created by vDiscovery)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Add new interface to existing VM (vma) with different discovered name (vmb) on Cloud Platform appliance</td>
<td>10.10.10.1 vma.corpxyz.com</td>
<td>10.10.10.1 vma.corpxyz.com</td>
<td>Zone: corpxyz.com Host record: vma, corpxyz.com (10.10.10.1)</td>
<td>Zone: corpxyz.com Host record: vma, corpxyz.com (10.10.10.2)</td>
</tr>
<tr>
<td>Automatic creation of Host records</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>In NIOS: existing zone corpxyz.com; existing Host record (originally created by vDiscovery)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remove existing VM (vma) on Cloud Platform appliance</td>
<td>No data for vma</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Automatic creation of Host records</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>In NIOS: existing zone corpxyz.com; existing Host record (originally created by vDiscovery)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remove existing VM (vma) on Cloud Platform appliance</td>
<td>10.10.10.1 vma.corpxyz.com</td>
<td>No data for vma</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Copyright ©2020, Infoblox, Inc. All right reserved.
For a new vDiscovery job:
1. From the Data Management tab, select the IPAM tab, then select vDiscovery -> New from the Toolbar; or from the Cloud tab, select vDiscovery -> New from the Toolbar.
2. or
   a. To modify an existing job: From the Data Management tab, select the IPAM tab and click vDiscovery -> Discovery Manager from the Toolbar, or from the Cloud tab, select vDiscovery -> Discovery Manager from the Toolbar. In the vDiscovery Job Manager editor, click the Action icon next to a selected job and select Edit from the menu.
3. In step four of the vDiscovery Job wizard, or in the Data Consolidation tab of the vDiscovery Job Properties editor, complete the following:
   a. For every newly discovered IP address, create: Select this check box to enable NIOS to automatically create or update DNS records for discovered VM instances if the records were originally created by vDiscovery.
   b. Host: Select this to automatically create Host records for discovered VMs.
   c. A & PTR Record: Select this to automatically create A and PTR records for discovered VMs. Note that the DNS zones and reverse-mapping zones to which the records belong must exist in NIOS. Otherwise, vDiscovery does not create the records.
   d. The DNS name will be computed from the formula: Enter the formula that NIOS uses to create FQDNs for discovered VMs. You can use the auto-generated FQDNs for DNS resolution purposes. You must use the syntax of ${parameter name} for this formula.

To enable the appliance to automatically create DNS records, complete the following in Grid Manager:

1. Automatic creation of Host records
2. In NIOS: existing zone corpxyz.com; existing Host record (originally created by admin)
Azure, this field supports the `vm_name` and `discovered_name` parameters. For example, when you enter `$\{vm\_name\}.corp100.com` and the discovered `vm\_name = XYZ`, the DNS name for this IP becomes `XYZ.corp100.com`. When you enter `$\{discover\_name\}` here and the discovered name for the IP is `ip-172-31-1-64.us-west-1.compute.internal`, the DNS name for this IP is `ip-172-31-1-64.us-west-1.compute.internal`.

Note

If the `$\{vm\_name\}` parameter of an instance contains any special character, the appliance will not be able to identify this instance and will convert it to a managed VM using the `vm\_id` parameter.

Click Add(+).