Infoblox
CONTROL YOUR NETWORK

Infoblox Installation Guide

vNIOS™ for Microsoft Azure®

Copyright Statements

For Open Source Copyright information, see *Appendix C, Open Source Copyright and License Statements* in the *Infoblox NIOS Administrator Guide*.

Trademark Statements

Company Information

http://www.infoblox.com/contact

Product Information

Document Number: 400-0503-000 Rev. E

Document Updated: August 16, 2017

Warranty Information

Your purchase includes a 90-day software warranty and a one year limited warranty on the Infoblox appliance, plus an Infoblox Warranty Support Plan and Technical Support. For more information about Infoblox Warranty information, refer to Infoblox Web site, or contact Infoblox Technical Support.

Contents

Preface 1

Document Overview 1
- Documentation Organization 1
- Conventions 2

Related Documentation 2

Customer Care 3
- User Accounts 3
- Software Upgrades 3
- Technical Support 3

Infoblox vNIOS for Azure 5

About Infoblox vNIOS for Azure 6

Prerequisites 6
- Supported vNIOS for Azure Models 6

Deploying vNIOS for Azure from the Marketplace 7
- Configuring Basic Settings 8
- Configuring VM Settings 9

Validating and Accepting Configuration 12
- Purchasing and Deploying the Virtual Appliance 12

Configuring vNIOS for Azure as the Primary DNS Server 13

Performing vDiscovery on VNets 14
- Configuring DNS Resolver 15
- Integrating vDiscovery with Azure Active Directory 15
- Adding vDiscovery Application as a New User 19
- Creating DNS Records for Discovered IP Addresses 20

Preface

The preface describes the content and organization of this guide, how to find additional product information, and how to contact Infoblox Technical Support. It includes the following topics:

- *Document Overview* on page 1
  - *Documentation Organization* on page 1
  - *Conventions* on page 2
- *Related Documentation* on page 2
- *Customer Care* on page 3
  - *User Accounts* on page 3
  - *Software Upgrades* on page 3
  - *Technical Support* on page 3

Document Overview

This guide introduces the Infoblox vNIOS virtual appliance for Microsoft Azure (vNIOS for Azure). It describes how to install the Infoblox vNIOS virtual appliance in Microsoft Azure. This manual describes the following:

For complete information about administering Infoblox appliances, refer to the *Infoblox NIOS Administrator Guide*.

For the latest Infoblox documentation, visit the Infoblox Support web site at https://support.infoblox.com.

Documentation Organization

This guide covers the following topics:

Chapter	Content
Chapter , Infoblox vNIOS for Azure, on page 5	Describes the vNIOS for Azure virtual appliance and how to deploy it in Microsoft Azure.

Conventions

This guide follows the Infoblox documentation style conventions, as listed in the following table.

Style	Usage
bold	Indicates anything that you input by clicking, choosing, selecting, typing or by pressing on the keyboard.
`input`	Signifies command line entries that you type.
variable	Signifies variables typed into the GUI that you need to modify specifically for your configuration, such as command line variables, file names, and keyboard characters.

Navigation

Infoblox technical documentation uses an arrow "->" to represent navigation through the GUI. For example, to access member information, the description is as follows:

From the **Grid** tab, select the **Grid Manager** tab -> **Members** tab.

Related Documentation

Other Infoblox documentation:

- *Infoblox CLI Guide*
- *Infoblox API Documentation*
- *Infoblox WAPI Documentation*
- *Infoblox CSV Import Reference*
- *Infoblox Installation Guide for the Trinzic 100 Appliance*
- *Infoblox Installation Guide for the 800 Series Platforms*
- *Infoblox Installation Guide for the 805 Series Platforms*
- *Infoblox Installation Guide for the 1400 Series Platforms*
- *Infoblox Installation Guide for the 1405 Series Platforms*
- *Infoblox Installation Guide for the 2200 Series Platforms*
- *Infoblox Installation Guide for the 2205Series Platforms*
- *Infoblox Installation Guide for the 4000 Series Platforms*
- *Infoblox Installation Guide for the Infoblox-4010 Appliance*
- *Infoblox Installation Guide for the IB-4030 and IB-4030-10GE Appliances*
- *Infoblox DNS Cache Acceleration Administrator Guide*
- *Infoblox Installation Guide for vNIOS for Microsoft Azure*
- *Infoblox Installation Guide for vNIOS for AWS*
- *Infoblox Installation Guide for vNIOS for VMware*
- *Infoblox Installation Guide for vNIOS on Microsoft 2008 R2 for Hyper-V*
- *Infoblox Installation Guide for vNIOS for KVM Hypervisor and KVM-based OpenStack*
- *Infoblox Safety Guide*

To provide feedback on any of the Infoblox technical documents, please e-mail *techpubs@infoblox.com*.

Customer Care

This section addresses user accounts, software upgrades, licenses and warranties, and technical support.

User Accounts

The Infoblox appliance ships with a default user name and password. Change the default `admin` account password immediately after the system is installed to safeguard its use. Make sure that the NIOS appliance has at least one administrator account with superuser privileges at all times, and keep a record of your account information in a safe place. If you lose the `admin` account password, and did not already create another superuser account, the system will need to be reset to factory defaults, causing you to lose all existing data on the NIOS appliance. You can create new administrator accounts, with or without superuser privileges.

Software Upgrades

Software upgrades are available according to the Terms of Sale for your system. Infoblox notifies you when an upgrade is available. Register immediately with Infoblox Technical Support at http://www.infoblox.com/support/customer/evaluation-and-registration to maximize your Technical Support.

Technical Support

Infoblox Technical Support provides assistance via the Web, e-mail, and telephone. The Infoblox Support web site at https://support.infoblox.com provides access to product documentation and release notes, but requires the user ID and password you receive when you register your product online at: http://www.infoblox.com/support/customer/evaluation-and-registration.

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* on page 6
- *Prerequisites* on page 6
  - *Supported vNIOS for Azure Models* on page 6
- *Deploying vNIOS for Azure from the Marketplace* on page 7
  - *Configuring Basic Settings* on page 8
  - *Configuring VM Settings* on page 9
  - *Validating and Accepting Configuration* on page 12
  - *Purchasing and Deploying the Virtual Appliance* on page 12
- *Configuring vNIOS for Azure as the Primary DNS Server* on page 13
- *Performing vDiscovery on VNets* on page 14
  - *Integrating vDiscovery with Azure Active Directory* on page 15
  - *Adding vDiscovery Application as a New User* on page 19
  - *Creating DNS Records for Discovered IP Addresses* on page 20

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 Administrator Guide*.

You can deploy one or more Infoblox vNIOS for Azure instances through the Microsoft Azure Marketplace and provision them to join an existing NIOS Grid or create a new one. You can then use the vNIOS for Azure instance as the primary or additional DNS servers to provide enterprise-grade DNS and IPAM services in the Microsoft Cloud. For information, see *Configuring vNIOS for Azure as the Primary DNS Server* on page 13. 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* on page 14.

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 Administrator Guide*.

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.

vNIOS Appliance	Overall Disk (GB)	# of vCPU Cores	Memory Allocation (GB)	Virtual Machine Size	Supported as Grid Master and Grid Master Candidate
TE-V820 *	160	2	7	DS2 Standard or DS2_V2 Standard	Yes
TE-V1420 *	160	4	14	DS3 Standard or DS3_V2 Standard	Yes
TE-V2200 *	160	4	14	DS3 Standard or DS3_V2 Standard	Yes
CP-V800	160	2	7	DS2 Standard or DS2_V2 Standard	No
CP-V1400	160	4	14	DS3 Standard or DS3_V2 Standard	No
CP-V2200	160	4	14	DS3 Standard or DS3_V2 Standard	N0

The following table lists the vNIOS for Azure appliance models that are supported for 8.2.x and later NIOS releases.

vNIOS Appliance	Overall Disk (GB)	# of vCPU Cores	Memory Allocation (GB)	Virtual Machine Size	Supported as Grid Master and Grid Master Candidate
TE-V825 *	250	2	14	DS11_V2 Standard	Yes
TE-V1425 *	250	4	28	DS12_V2 Standard	Yes
TE-V2225 *	250	8	56	DS13_V2 Standard	Yes
CP-V800	160	2	7	DS2 Standard or DS2_V2 Standard	No
CP-V1400	160	4	14	DS3 Standard or DS3_V2 Standard	No
CP-V2200	160	4	14	DS3 Standard or DS3_V2 Standard	N0

Note: * All TE vNIOS appliances 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 Administrator Guide*.

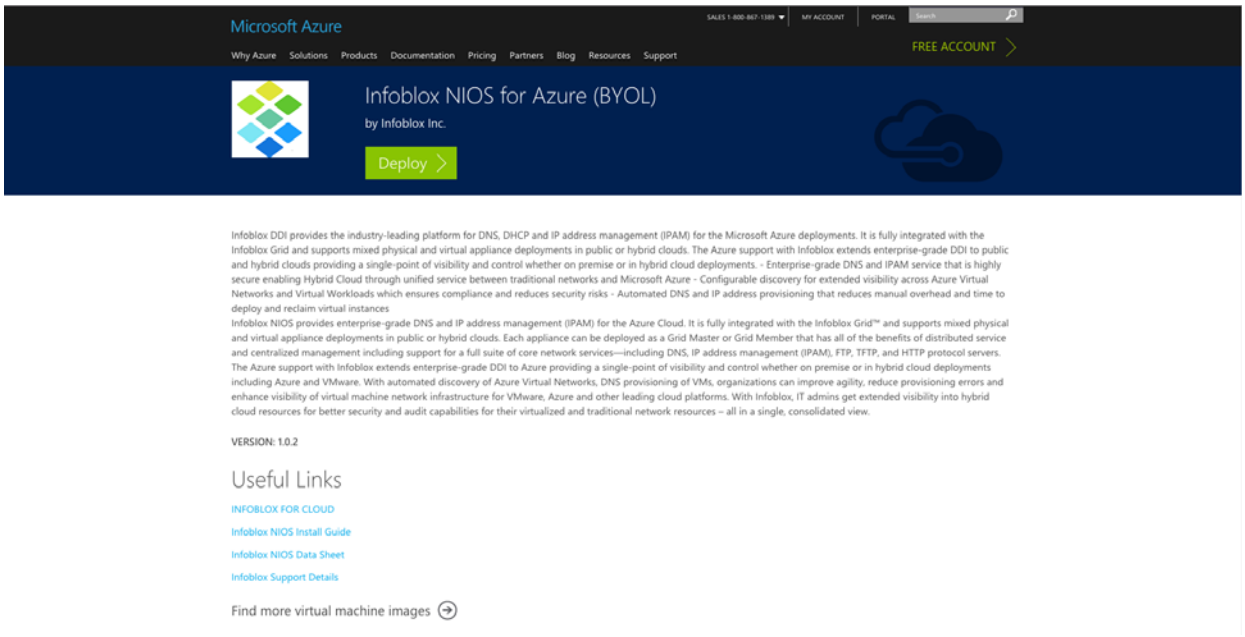
Deploying vNIOS for Azure from the Marketplace

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. Go to the Microsoft Azure web site.
2. Log in to your Microsoft Azure account.
3. On the Microsoft Azure Portal, click **New** -> **Marketplace** from the left panel.
4. Enter “infoblox” as the search filter, and then select an Infoblox for Azure virtual appliance from the search results.
5. Use **Resource Manager** as the deployment model for the new virtual appliance.

Figure 1.1 Selecting vNIOS for Azure Model



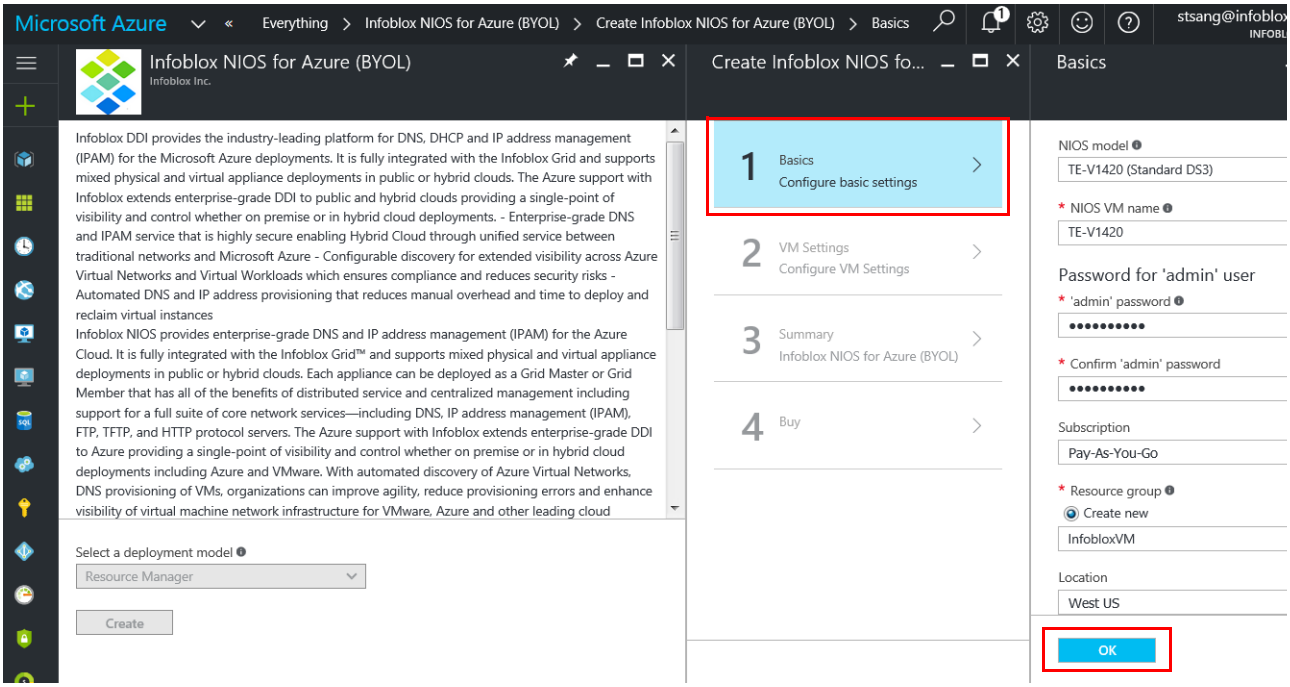
6. Click **Deploy** and complete the following steps to deploy vNIOS for Azure:
   - *Configuring Basic Settings* on page 8
   - *Configuring VM Settings* on page 9
   - *Validating and Accepting Configuration* on page 12
   - *Purchasing and Deploying the Virtual Appliance* on page 12

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



Click **OK** after you complete the basic configuration. The Portal prompts you to configure VM settings, as described in *Configuring VM Settings* on page 9.

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.
- **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 new** in the *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

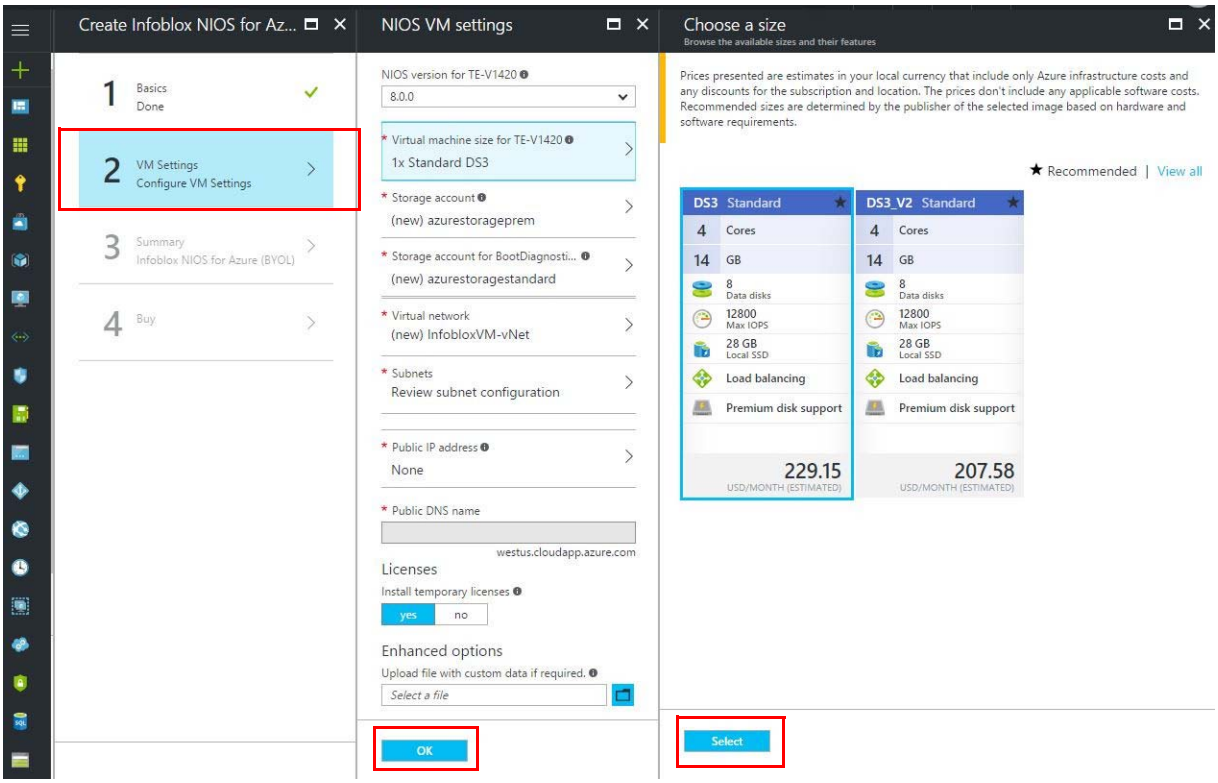
GB of memory. They are the best type of storage account for applications that require bulk storage or where data is accessed infrequently. If you want to create a storage account to save all diagnostics files associated with the VM, click **Storage account for BootDiagnostics** to create the standard 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**: 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 Administrator Guide*). 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.
- **Licenses**: Click **yes** to install the following temporary licenses on your virtual appliance: vNIOS, Grid, DNS, DNS RPZ, and CNA (Cloud Network Automation). 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.

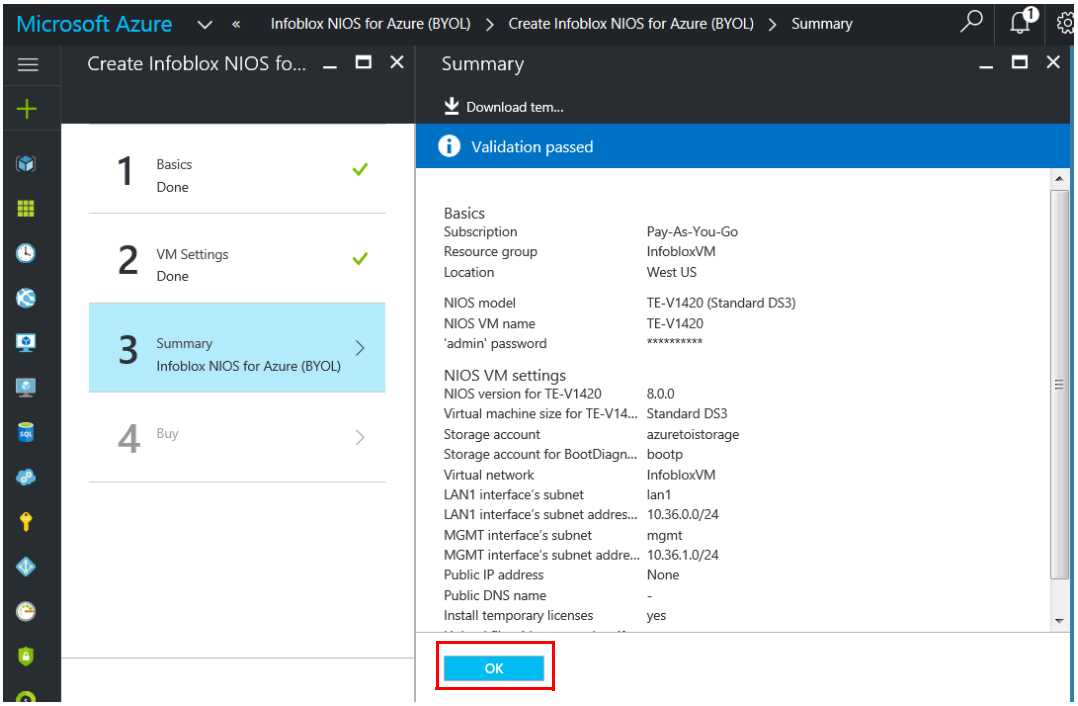
Figure 1.3 Configuring VM Settings



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.

Now click **Purchase** to start the deployment of your vNIOS for Azure virtual 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.

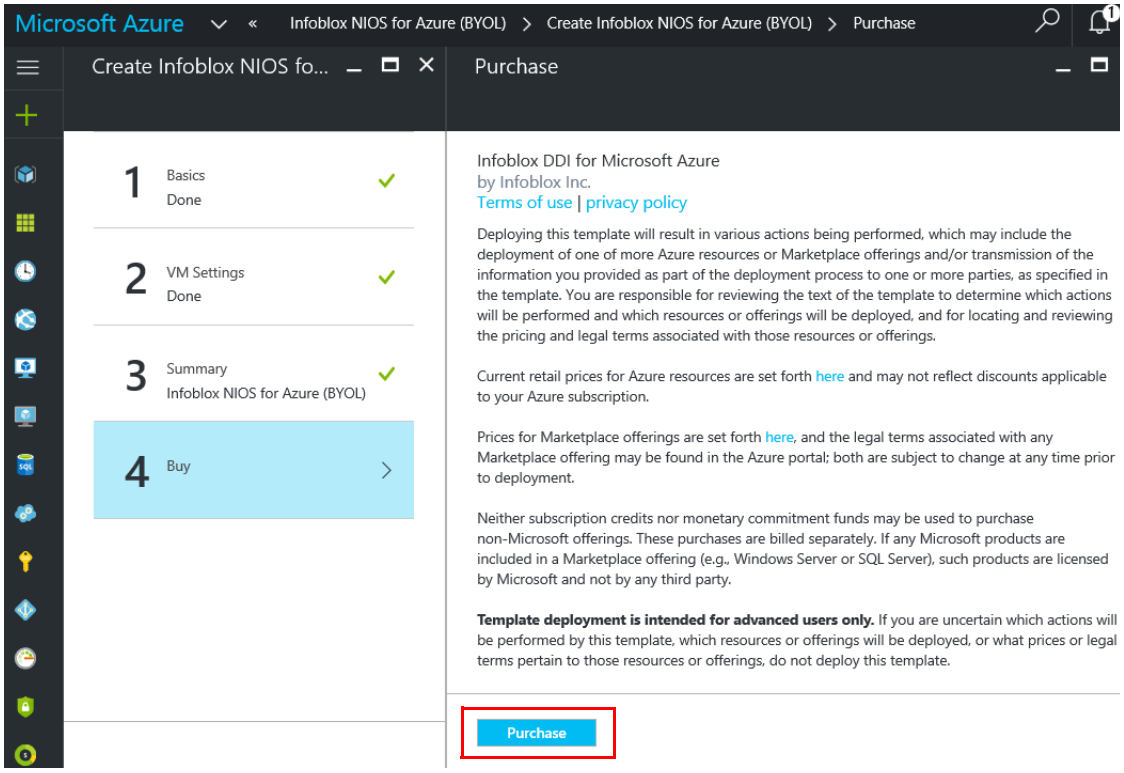
Note: You will be purchasing the VM, storage, and IP address on an hourly basis payable to Microsoft Azure through your Azure account. If you have not installed the Infoblox NIOS temporary licenses, you can purchase them through your Infoblox representatives or contact Infoblox Technical Support.

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* on page 13
- Locating network devices on VNets by performing a vDiscovery, as described *Performing vDiscovery on VNets* on page 14.

Figure 1.5 Purchasing the vNIOS for Azure Virtual Appliance



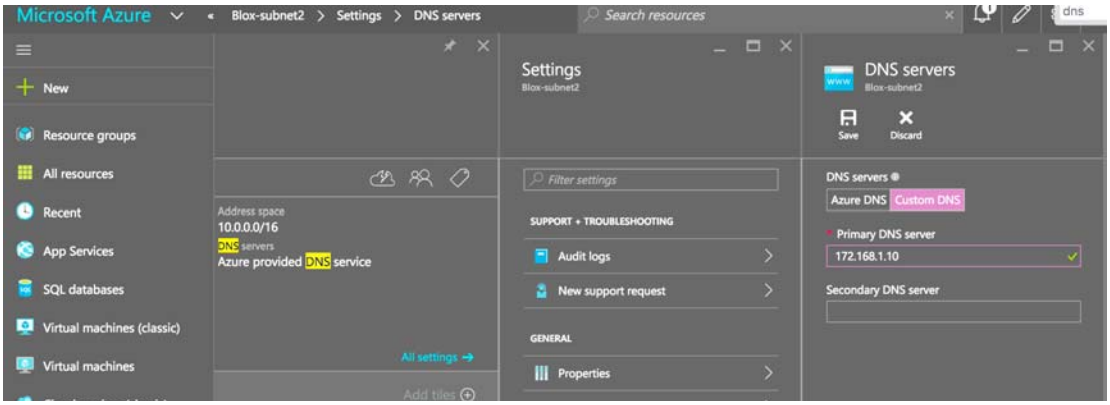
Configuring vNIOS for Azure as the Primary DNS Server

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 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* on page 15.
2. Register an application with the Azure Active Directory through the Azure portal, as described in *Integrating vDiscovery with Azure Active Directory* on page 15.
3. Add the new application as a user through the Azure resource manager portal, as described in *Adding vDiscovery Application as a New User* on page 19.
4. Perform vDiscovery for service instances and subnets in selected VNets. For detailed information, refer to *Configuring vDiscovery Jobs* in the *Infoblox NIOS Administrator Guide*. 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 the *Infoblox NIOS Administrator Guide*. You can also create DNS records for discovered IP addresses. For information, see *Creating DNS Records for Discovered IP Addresses* on page 20.

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

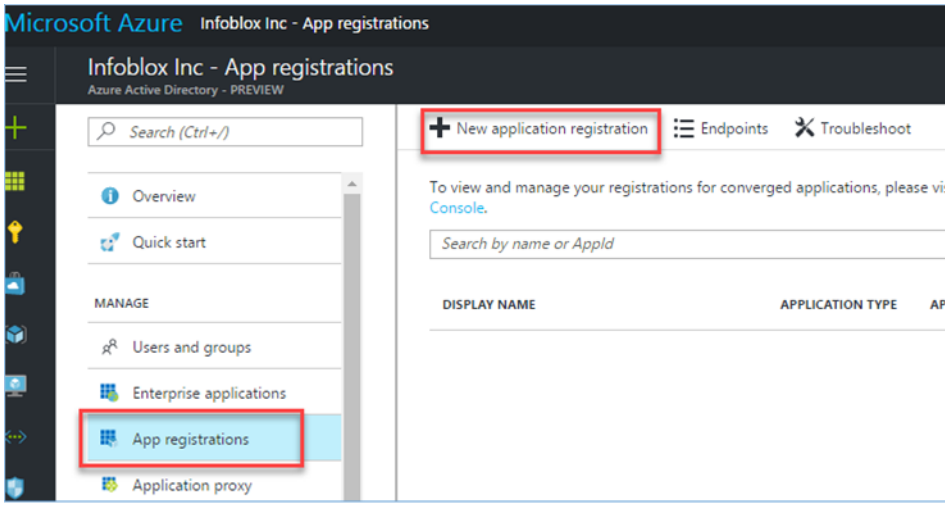
Before creating a vDiscovery job and performing vDiscovery in Azure, you must integrate the discovery application with Azure Active Directory (Azure AD) to provide secure sign in and authorization. To integrate the application with Azure AD, you must first register the application details with Azure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

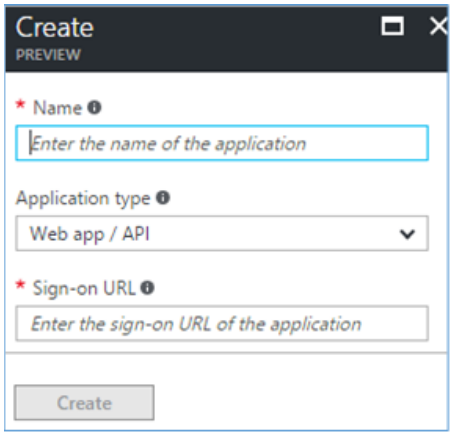
To create and integrate a vDiscovery application through the Azure portal:

1. In the Microsoft Azure portal, open **More 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 application registration** to add a new application.

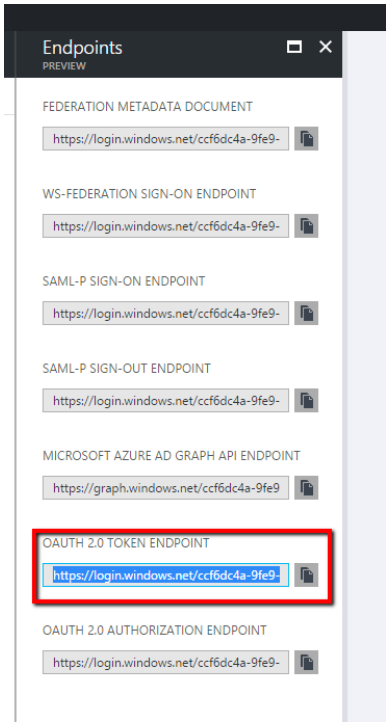


5. If you are adding a new application, enter the following to define your application in the *Create* wizard, and then click **Create** to add the application.
   - **Name**: Enter the name of your new application.
   - **Application Type**: Select **Web app/API**.
   - **Sign on URL**: Ensure that you use a unique URL for sign-on purposes.

   Azure notifies you when the application is successfully created.

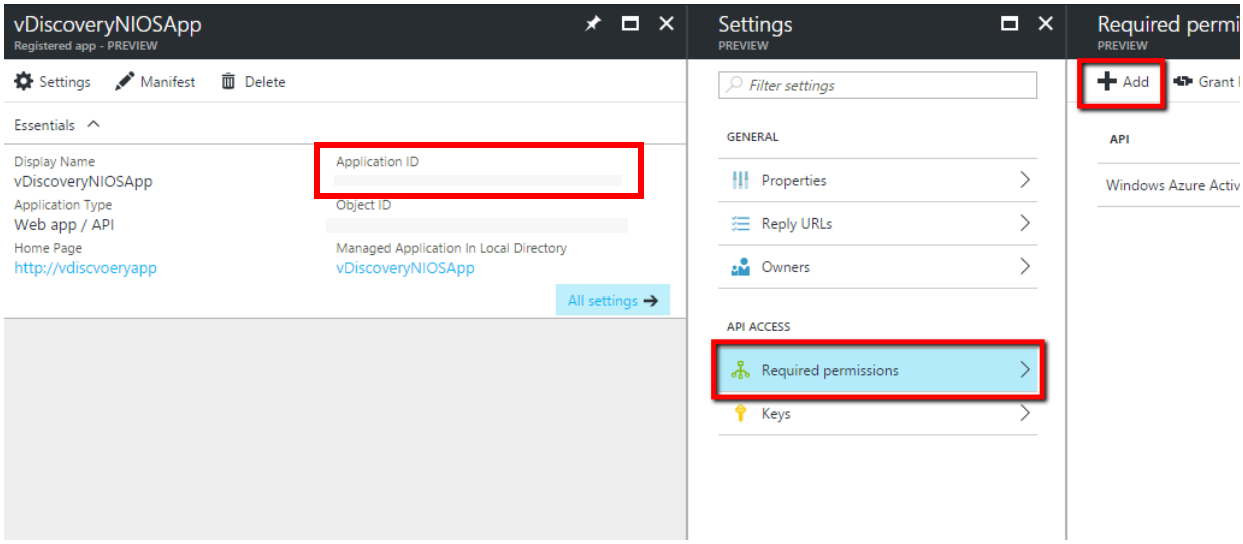


Note: To obtain token information for the endpoints, click the **Endpoints** icon next to **+ New application registration** in the *App registration* panel. Azure displays the *Endpoints* page that contains endpoint information for the discovery application. vDiscovery uses the **OAUTH 2.0 TOKEN ENDPOINT** (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.

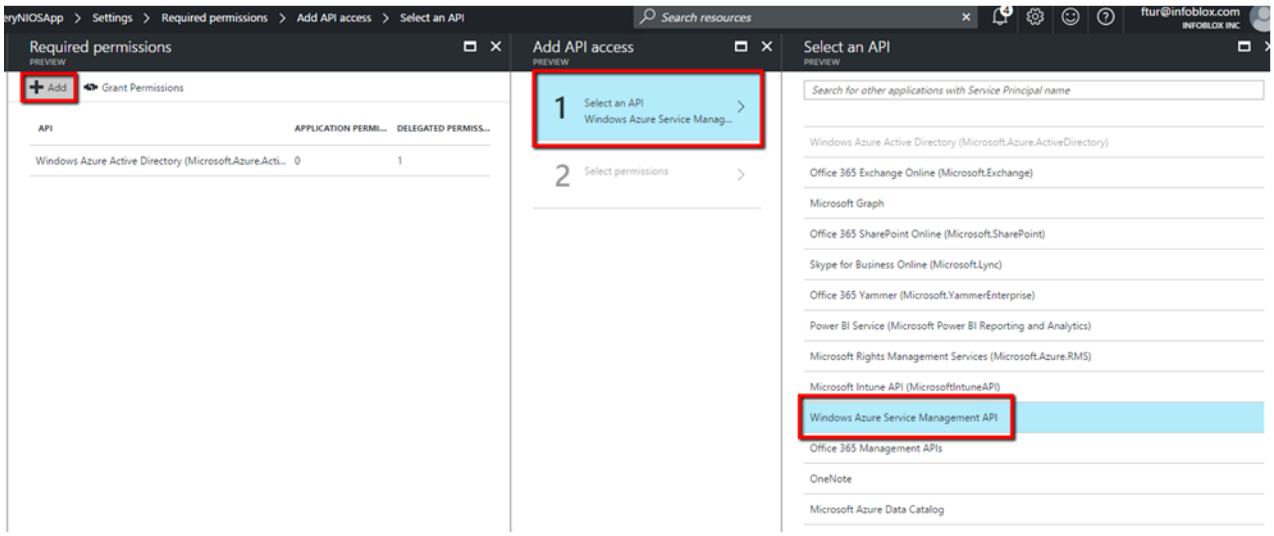


6. Select and click the application from the list. The Azure portal displays details about your application, such as **Display name**, **Application type**, **Home page**, **Application ID**, and **Object ID**. In the *Settings* panel, click **Required permissions**, and then click **+ Add** in the *Required Permissions* panel.

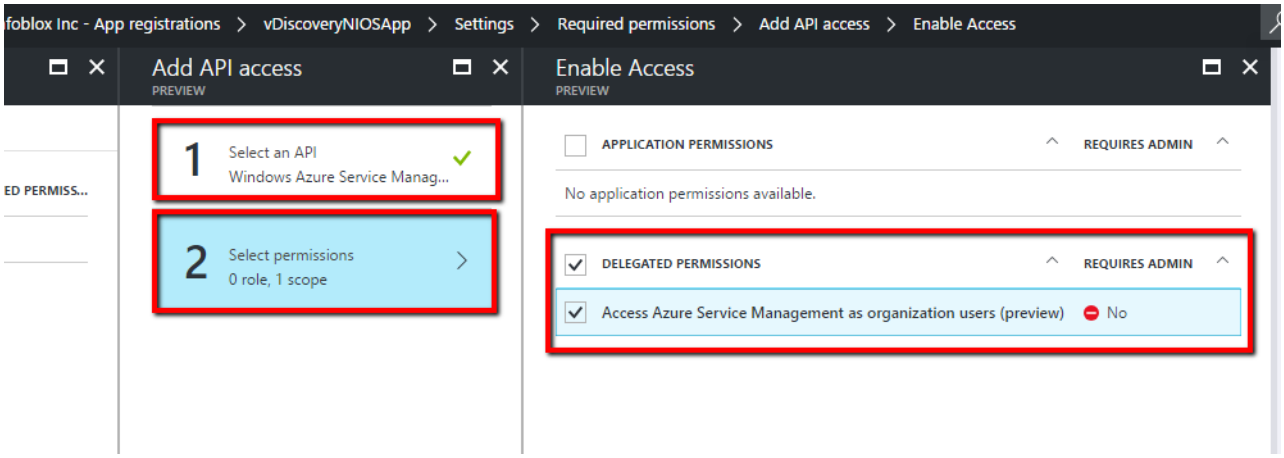
Note: Ensure that you copy the **Application ID** and save this value for future use. This ID is used as the **Client ID** in your vDiscovery configuration.



7. In the *Add API access* panel, click **Select an API**.
8. Select **Windows Azure Service Management API** from the list in the *Select an API* panel, and then click **Select**.

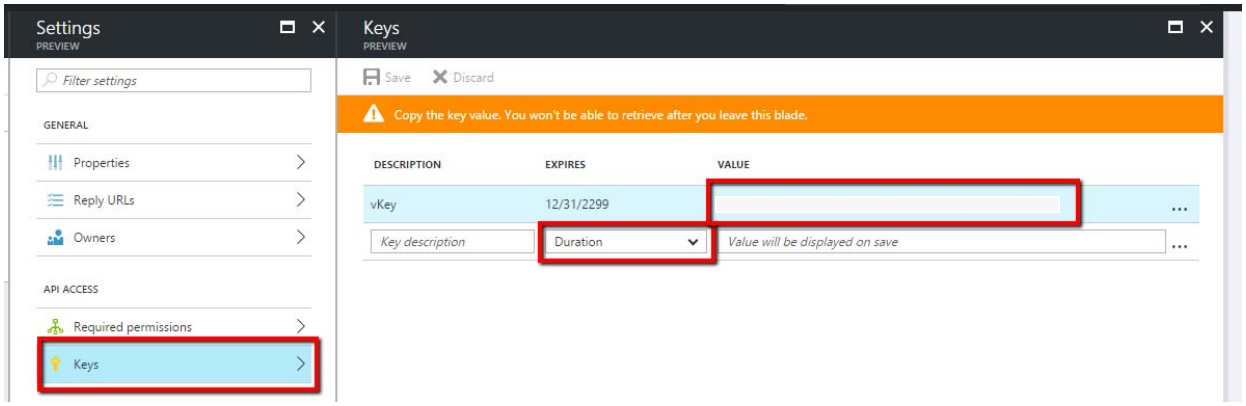


9. In the *Add API access* panel, click **Select permissions**. In the *Enable Access* panel, select the **DELEGATED PERMISSIONS** and **Access Azure Service Management as organization users (Preview)** check boxes, and then click **Select**.
10. Click **Done** in the *Add API access* panel.



11. In the *Settings* panel, click **Keys**, and then complete the following in the *Keys* panel:
    - **Description**: Enter a name or description for the generated key.
    - **Duration**: Select duration time for the generated key.
    - **Value**: The key will be displayed here after you select the duration 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.

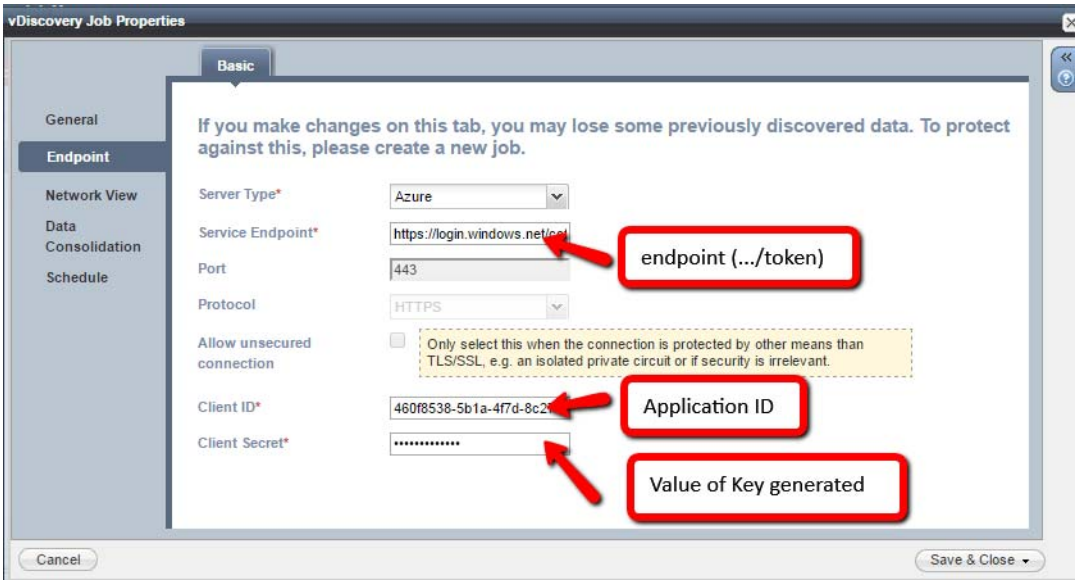


12. Validate all the configuration and information on this page. Click the **Save** icon to save your configuration. You have completed the vDiscovery configuration in Azure.

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**. 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:

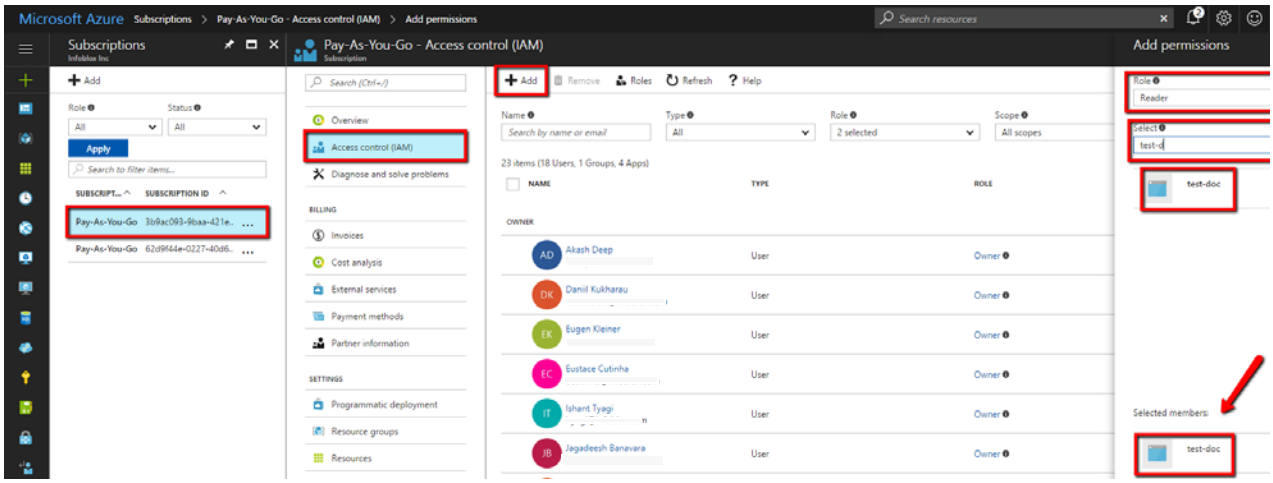


Adding vDiscovery Application as a New User

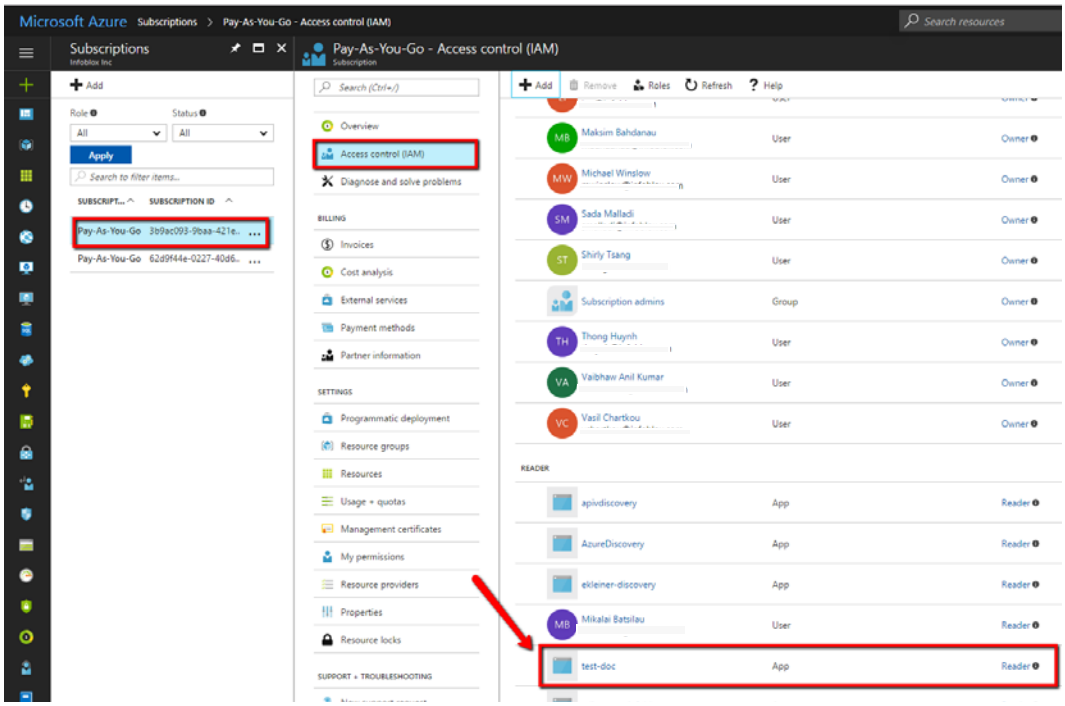
After you have set up the vDiscovery application in Azure Active Directory, you must add this application as a new user to your vNIOS for Azure subscription through the Azure resource manager portal, and then define its administrative role.

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**.



5. 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 Administrator Guide*.

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.

Actions and Conditions	Cloud Platform Data before vDiscovery	Cloud Platform Data after vDiscovery	NIOS Data before vDiscovery	NIOS Data after vDiscovery
• Add new VM (vma) on Cloud Platform appliance • Automatic creation of Host records • **In NIOS:** existing zone corp1.com; no DNS records	No data for vma	10.10.10.1 vma.corp1.com	**Zone:** corp1.com	**Zone:** corp1.com **Host record:** vma.corp1.com (10.10.10.1)
• Add new VM (vma) on Cloud Platform appliance • Automatic creation of Host records • **In NIOS:** existing zone corp1.com; existing Host record (*originally created by vDiscovery or admin*)	No data for vma	10.10.10.1 vma.corp1.com	**Zone:** corp1.com **Host record:** vma.corp1.com (10.10.10.1)	**Zone:** corp1.com **Host record:** vma.corp1.com (10.10.10.1)
• Add new interface to existing VM (vma) with the same discovered name on Cloud Platform appliance • Automatic creation of Host records • **In NIOS:** existing zone corp1.com; existing Host record (*originally created by vDiscovery*)	10.10.10.1 vma.corp1.com	10.10.10.1 vma.corp1.com	**Zone:** corp1.com **Host record:** vma.corp1.com (10.10.10.1)	**Zone:** corp1.com **Host record:** vma.corp1.com (10.10.10.1, 10.10.10.2)
• Add new interface to existing VM (vma) with the same discovered name on Cloud Platform appliance • Automatic creation of Host records • **In NIOS:** existing zone corp1.com; existing Host record (*originally created by admin*)	10.10.10.1 vma.corp1.com	10.10.10.1 vma.corp1.com	**Zone:** corp1.com **Host record:** vma.corp1.com (10.10.10.1)	**Zone:** corp1.com **Host record:** vma.corp1.com (10.10.10.1)

Actions and Conditions	Cloud Platform Data before vDiscovery	Cloud Platform Data after vDiscovery	NIOS Data before vDiscovery	NIOS Data after vDiscovery
• Add new interface to existing VM (vma) with different discovered name (vmb) on Cloud Platform appliance • Automatic creation of Host records • **In NIOS:** existing zone corp1.com; existing Host record (*originally created by vDiscovery*)	10.10.10.1 vma.corp1.com	10.10.10.1 vma.corp1.com 10.10.10.2 vmb.corp1.com	**Zone:** corp1.com **Host record:** vma.corp1.com (10.10.10.1)	**Zone:** corp1.com **Host record:** vma.corp1.com (10.10.10.1) **Host record:** vmb.corp1.com (10.10.10.2)
• Add new interface to existing VM (vma) with different discovered name (vmb) on Cloud Platform appliance • Automatic creation of Host records • **In NIOS:** existing zone corp1.com; existing Host record (*originally created by admin*)	10.10.10.1 vma.corp1.com	10.10.10.1 vma.corp1.com 10.10.10.2 vmb.corp1.com	**Zone:** corp1.com **Host record:** vma.corp1.com (10.10.10.1)	**Zone:** corp1.com **Host record:** vma.corp1.com (10.10.10.1) **Host record:** vmb.corp1.com (10.10.10.2)
• Remove existing VM (vma) on Cloud Platform appliance • Automatic creation of Host records • **In NIOS:** existing zone corp1.com; existing Host record (*originally created by vDiscovery*)	10.10.10.1 vma.corp1.com	No data for vma	**Zone:** corp1.com **Host record:** vma.corp1.com (10.10.10.1)	**Zone:** corp1.com
• Remove existing VM (vma) on Cloud Platform appliance • Automatic creation of Host records • **In NIOS:** existing zone corp1.com; existing Host record (*originally created by admin*)	10.10.10.1 vma.corp1.com	No data for vma	**Zone:** corp1.com **Host record:** vma.corp1.com (10.10.10.1)	**Zone:** corp1.com **Host record:** vma.corp1.com (10.10.10.1)

Actions and Conditions	Cloud Platform Data before vDiscovery	Cloud Platform Data after vDiscovery	NIOS Data before vDiscovery	NIOS Data after vDiscovery
• Remove existing interface (10.10.10.2) from VM (vma) with different discovered name (vmb) on Cloud Platform appliance • Automatic creation of Host records • **In NIOS:** existing zone corp1.com; existing Host record (*originally created by vDiscovery*)	10.10.10.1 vma.corp1.com 10.10.10.2 vmb.corp1.com	10.10.10.1 vma.corp1.com	**Zone:** corp1.com **Host record:** vma.corp1.com (10.10.10.1) **Host record:** vmb.corp1.com (10.10.10.2)	**Zone:** corp1.com **Host record:** vma.corp1.com (10.10.10.1)
• Remove existing interface (10.10.10.2) from VM (vma) with different discovered name (vmb) on Cloud Platform appliance • Automatic creation of Host records • **In NIOS:** existing zone corp1.com; existing Host record (*originally created by admin*)	10.10.10.1 vma.corp1.com 10.10.10.2 vmb.corp1.com	10.10.10.1 vma.corp1.com	**Zone:** corp1.com **Host record:** vma.corp1.com (10.10.10.1) **Host record:** vmb.corp1.com (10.10.10.2)	**Zone:** corp1.com **Host record:** vma.corp1.com (10.10.10.1) **Host record:** vmb.corp1.com (10.10.10.2)
• Update record name (from vma to vm1) for the existing interface (10.10.10.1) on Cloud Platform appliance • Automatic creation of Host records • **In NIOS:** existing zone corp1.com; existing Host record (*originally created by vDiscovery*)	10.10.10.1 vma.corp1.com	10.10.10.1 vm1.corp1.com	**Zone:** corp1.com **Host record:** vma.corp1.com (10.10.10.1)	**Zone:** corp1.com **Host record:** vm1.corp1.com (10.10.10.1)
• Update record name (from vma to vm1) for the existing interface (10.10.10.1) on Cloud Platform appliance • Automatic creation of Host records • **In NIOS:** existing zone corp1.com; existing Host record (*originally created by admin*)	10.10.10.1 vma.corp1.com	10.10.10.1 vm1.corp1.com	**Zone:** corp1.com **Host record:** vma.corp1.com (10.10.10.1)	**Zone:** corp1.com **Host record:** vma.corp1.com (10.10.10.1) **Host record:** vm1.corp1.com (10.10.10.1)

Actions and Conditions	Cloud Platform Data before vDiscovery	Cloud Platform Data after vDiscovery	NIOS Data before vDiscovery	NIOS Data after vDiscovery
• Automatic creation of Host records • Change FQDN template from ${discover_name) to ${vm_name} • **In NIOS**: existing zone corp1.com; existing Host record (*originally created by vDiscovery*)	10.10.10.1 vma.corp1.com vm_name: ABC	10.10.10.1 vm1.corp1.com vm_name: ABC	**Zone**: corp1.com **Host record**: vma.corp1.com (10.10.10.1)	**Zone**: corp1.com **Host record**: ABC.corp1.com (10.10.10.1)
• Automatic creation of Host records • Change FQDN template from ${discover_name) to ${vm_name} • **In NIOS**: existing zone corp1.com; existing Host record (*originally created by admin*)	10.10.10.1 vma.corp1.com vm_name: ABC	10.10.10.1 vm1.corp1.com vm_name: ABC	**Zone**: corp1.com **Host record**: vma.corp1.com (10.10.10.1)	**Zone**: corp1.com **Host record**: vma.corp1.com (10.10.10.1) **Host record**: ABC.corp1.com (10.10.10.1)
• Change vDiscovery task configuration from creation of Host record to A and PTR records • **In NIOS**: existing zone corp1.com; existing Host record (*originally created by vDiscovery*)	10.10.10.1 vma.corp1.com	10.10.10.1 vma.corp1.com	**Zone**: corp1.com **Host record**: vma.corp1.com (10.10.10.1)	**Zone**: corp1.com **A record**: vma.corp1.com (10.10.10.1)
• Change vDiscovery task configuration from creation of Host record to A and PTR records • **In NIOS**: existing zone corp1.com; existing Host record (*originally created by admin*)	10.10.10.1 vma.corp1.com	10.10.10.1 vma.corp1.com	**Zone**: corp1.com **Host record**: vma.corp1.com (10.10.10.1)	**Zone**: corp1.com **Host record**: vma.corp1.com (10.10.10.1) **A record**: vma.corp1.com (10.10.10.1)

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

1. For a new vDiscovery job: 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.

   or

   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.
2. In step four of the v*Discovery Job* wizard, or in the **Data Consolidation** tab of the *vDiscovery Job Properties* editor, complete the following:
   — **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.

- **Host**: Select this to automatically create Host records for discovered VMs.
- **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.
- **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.