IPAM Driver for VMware vRA 7.3 User's Guide
1. Infoblox IPAM Plugin for VMware vRA 7.3 User's Guide ......................................................... 4
   1.1 Introduction to Infoblox IPAM Plug-In for VMware ....................................................... 5
   1.2 Deployment Requirements ............................................................................................ 6
   1.3 Before Deploying Infoblox IPAM Plug-In for VMware ............................................... 8
       1.3.1 Setting Up the Infoblox NIOS Appliance .............................................................. 9
   1.4 Deploying Infoblox IPAM Plug-In for VMware .......................................................... 10
       1.4.1 Preparing Your Environment for vRealize Automation Management ................... 11
       1.4.2 Importing NIOS SSL Certificate ....................................................................... 14
       1.4.3 Installing Infoblox IPAM Plug-In for VMware ............................................... 15
       1.4.4 Performing Basic Plug-In Setup ....................................................................... 16
       1.4.5 Configuring vRealize Automation Management .............................................. 25
           1.4.5.1 Configuring Tenant Settings ................................................................. 26
           1.4.5.2 Configure vRealize Orchestrator Server .............................................. 28
           1.4.5.3 Creating vSphere and vRealize Orchestrator Endpoints ....................... 29
           1.4.5.4 Creating an Infoblox IPAM Endpoint ................................................... 30
           1.4.5.5 Creating a Fabric Group .................................................................... 32
           1.4.5.6 Viewing Compute Resources .............................................................. 33
           1.4.5.7 Creating a Machine Prefix .................................................................. 35
           1.4.5.8 Creating a Business Group .................................................................. 36
           1.4.5.9 Creating an External Network Profile .................................................... 37
           1.4.5.10 Creating a Routed Network Profile ...................................................... 40
           1.4.5.11 Creating a NAT Network Profile .......................................................... 41
           1.4.5.12 Creating a Reservation .................................................................... 42
           1.4.5.13 Customizing the Property Group .......................................................... 46
           1.4.5.14 Activating the Blueprint Designer .......................................................... 47
           1.4.5.15 Designing a Blueprint .................................................................... 48
           1.4.5.16 Creating a VM Request Service in vRealize Catalog ......................... 53
           1.4.5.17 Specifying DNS domain while requesting VM ...................................... 56
   1.5 Provisioning and De-provisioning VMs with Registration in NIOS ........................ 57
       1.5.1 Provisioning a VM ....................................................................................... 58
       1.5.2 De-provisioning a VM ............................................................................... 59
   1.6 Using Extensible Attributes in Infoblox IPAM Plug-In for NIOS ....................... 60
       1.6.1 Extensible Attributes in IPAM Workflows .................................................... 61
       1.6.2 Reloading Extensible Attributes ................................................................. 62
   1.7 Using Workflows of Infoblox IPAM Plug-In for VMware ............................... 63
       1.7.1 IPAM Workflows ....................................................................................... 64
           1.7.1.1 Reserve IP Address Workflow ............................................................. 65
           1.7.1.2 Reserve IP in Network Workflow ....................................................... 67
           1.7.1.3 Reserve IP in Range Workflow ............................................................ 68
           1.7.1.4 Remove Host Record Workflow .......................................................... 69
           1.7.1.5 Remove DHCP Record Workflow ...................................................... 70
           1.7.1.6 Remove DNS Record Workflow .......................................................... 71
           1.7.1.7 Add Network Workflow ................................................................ 72
           1.7.1.8 Remove Network Workflow ............................................................... 73
           1.7.1.9 Add Range Workflow ...................................................................... 74
           1.7.1.10 Remove Range Workflow ................................................................. 75
           1.7.1.11 Restart IPAM Services Workflow ....................................................... 76
       1.7.2 vRA Workflows .............................................................................................. 77
           1.7.2.1 Create/Update Property Definition Workflow .................................... 78
           1.7.2.2 Create Property Group Workflow .......................................................... 80
           1.7.2.3 Add an IaaS Host Wrapper Workflow .................................................. 83
           1.7.2.4 Add a vRA Host Wrapper Workflow ................................................... 84
           1.7.2.5 Update an IaaS Host Wrapper Workflow ............................................ 85
           1.7.2.6 Update a vRA Host Wrapper Workflow ............................................. 86
           1.7.2.7 Validate an IaaS/vRA Host Wrapper Workflow .................................. 87
           1.7.2.8 Remove IaaS/vRA Host Wrapper Workflow ..................................... 88
       1.7.3 Verifying Workflow Execution ........................................................................ 89
   1.8 Using Actions of Infoblox IPAM Plug-In for VMware ........................................ 90
   1.9 Using API of Infoblox IPAM Plug-In for VMware ........................................... 91
   1.10 Integrating Infoblox IPAM Plug-In for VMware with Microsoft DNS and DHCP Servers ......................... 93
       1.10.1 Use Case: IP Address Allocation from NIOS with DNS Registration in Microsoft DNS Server 94
       1.10.2 Use Case: IP Address Allocation from NIOS with DHCP Registration in Microsoft DHCP Server 95
   1.11 Integrating Infoblox IPAM Plug-In for VMware with NSX .................................... 96
       1.11.1 Provisioning NSX Load Balancers with Registration in NIOS ...................... 97
           1.11.1.1 Setting Up a Network Profile ................................................................ 98
           1.11.1.2 Making a Reservation of the IP Address .......................................... 99
           1.11.1.3 Creating a Blueprint for the NSX Load Balancer ................................ 100
           1.11.1.4 Provisioning NSX Virtual Machines .................................................. 101
           1.11.1.5 Scaling the NSX Deployment .............................................................. 102
       1.11.2 Provisioning VMs in NSX Routed Networks Registered in NIOS ............. 103
           1.11.2.1 Provisioning a VM in NSX Routed Network ...................................... 104
Introduction to Infoblox IPAM Plug-In for VMware

This guide describes how to install and use the Infoblox IPAM Plug-In for VMware with vRealize Orchestrator (further vRO; formerly vCenter Orchestrator) and vRealize Automation (further vRA; formerly vCloud Automation Center). It provides information about the Infoblox Plug-In workflows and actions library.

The Infoblox IPAM Plug-In for VMware supports Infoblox NIOS and its Cloud Network Automation platform, which automates IP address and DNS management for physical and virtual network devices for your VMware management platform. Instead of manually provisioning IP addresses and DNS or DHCP records for network devices and interfaces, you can use Cloud Network Automation to leverage DNS and DHCP features of the Infoblox GridTM to manage your cloud networks, through your current VMware management platform. For more information, see Cloud Network Automation Deployments.

The Infoblox IPAM Plug-In for VMware supports static and fixed IP address allocation and address allocation from DHCP ranges. When you use the Infoblox IPAM Plug-In for VMware to allocate IP addresses to virtual machines (VMs), it creates corresponding DNS records on your Infoblox Grid NIOS or vNIOS appliance. The Plug-In is configurable and can create Infoblox host records or individual DNS resource records along with fixed address records to enable VMs to be located through their FQDNs as soon as the VM is provisioned. This information is also visible through the vRealize Automation console. For information, see Provisioning and De-provisioning VMs with Registration in NIOS.

If you use Microsoft servers for DNS and DHCP, you can integrate them with the Infoblox IPAM Plug-In for VMware to synchronize records. For more information, see Integrating Infoblox IPAM Plug-In for VMware with Microsoft DNS and DHCP Servers.

You can also use Infoblox IPAM Plug-In for VMware with VMware’s NSX platform to provision machines for your load-balanced resources and automatically create routed and NAT networks in NIOS at VM deployment. For information, see Integrating Infoblox IPAM Plug-In for VMware with NSX.

The following figure illustrates the architecture of the Infoblox IPAM Plug-In for VMware.

Intended Audience

Information in this document is intended for anyone who is installing and configuring the Infoblox IPAM Plug-In for VMware, and using its workflows and actions library and API. This information is written for experienced users who are familiar with virtual machine technology, vRealize Orchestrator workflows, vRealize Automation, and VMware vSphere. This guide also assumes that the readers are familiar with NIOS appliances and NIOS software.
Deployment Requirements

The following table lists recommended software combinations that are verified for compatibility with the Infoblox IPAM Plug-In for VMware v.4.4.0:

<table>
<thead>
<tr>
<th>NIOS</th>
<th>ESXi</th>
<th>vCenter</th>
<th>vRO (Embedded)</th>
<th>vRO (External)</th>
<th>vRA</th>
<th>NSX</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.3.0</td>
<td>6.0.0</td>
<td>6.0.0</td>
<td>7.3</td>
<td>7.3</td>
<td>7.3</td>
<td>6.2.4</td>
</tr>
<tr>
<td>8.2.x</td>
<td>5.5.0</td>
<td>5.5.0</td>
<td>7.3</td>
<td>7.3</td>
<td>7.3</td>
<td></td>
</tr>
<tr>
<td>8.1.x</td>
<td>5.5.0</td>
<td>5.5.0</td>
<td>7.3</td>
<td>7.3</td>
<td>7.3</td>
<td></td>
</tr>
<tr>
<td>8.0.x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Not tested</td>
</tr>
</tbody>
</table>

To ensure compatibility of the Infoblox IPAM Plug-In for VMware with other combinations of VMware software components, check that the components are compatible with each other. You can do so using documentation for these products and VMware Product Interoperability Matrixes. See Resources for the links.

For deployment steps, see Deploying Infoblox IPAM Plug-In for VMware. For more information on cloud deployments, see Cloud Network Automation Deployments.

Cloud Network Automation Deployments

Cloud Network Automation includes two components:

- The Cloud Network Automation license provides the ability to view VM-related information from VMware vCenter directly within the Infoblox GUI organized by Tenant. This enables networking teams to have direct visibility on information normally only available through VMware vSphere Web Client enabling the networking and server teams to better manage IP address and DNS record allocations and troubleshoot issues.
- Cloud Platform Appliances that enable API calls to be sent directly to the Infoblox appliances serving DNS and/or DHCP locally within the datacenter hosting the Cloud Management Platform (CMP) rather than sending all API calls to the Grid Master.

The current release of the Infoblox Plug-In allows you to work with both non-Cloud Network Automation and Cloud Network Automation NIOS deployments, using the Infoblox WAPI and Cloud API respectively.

In order to use the Cloud Network Automation solution for visibility and/or federating API calls, the Plug-In must be configured to use the Infoblox Cloud API. The Cloud API unlike standard Infoblox WAPI supports additional objects such as the Tenant object and supports the federated API capability of the Cloud Platform Appliances.

The following figure illustrates the usage of Cloud Network Automation with the VMware Plug-In.

You may use one of three different configurations of your VMware Plug-In with NIOS Cloud Network Automation:

- The Cloud Network Automation license is installed on the Grid Master; the user configures the Infoblox VMware Plug-In to connect directly to the Grid Master. This deployment assumes no Cloud Platform Appliances are in the NIOS Grid.
- One or more Infoblox Cloud Platform members are added to the NIOS Grid; the Cloud Network Automation license is not installed on the Grid Master; the user configures the Infoblox VMware Plug-In to connect directly to the Grid Master.

Note: To ensure that the cloud API service is functioning properly, open port 443 for HTTPS connectivity and configure your firewalls accordingly.

Copyright ©2019, Infoblox, Inc. All right reserved.
Grid Master, and the VMware Plug-In is configured to connect directly to a primary Cloud Platform member instead of to the Grid Master;
• One or more Infoblox Cloud Platform members are added to the NIOS Grid; the Cloud Network Automation license also is installed on the Grid Master; the Infoblox VMware Plug-In is configured to connect directly to a primary Cloud Platform member instead of to the Grid Master just as in the second option.

Note: For a complete overview of NIOS Cloud Network Automation, see the chapter Deploying Cloud Network Automation in the NIOS Documentation.
Before Deploying Infoblox IPAM Plug-In for VMware

To ensure a successful deployment of Infoblox IPAM Plug-In for VMware, Infoblox recommends that you proceed in the following order:

1. Obtain or update all required products, plug-ins, and packages listed in the section Deployment Requirements.
2. Set up your NIOS or vNIOS appliance as described in Setting Up the Infoblox NIOS Appliance.
3. Deploy the Infoblox IPAM Plug-In for VMware following the order described in Deploying Infoblox IPAM Plug-In for VMware.
Setting Up the Infoblox NIOS Appliance

Before you deploy the Infoblox IPAM Plug-In for VMware, complete the following tasks on the NIOS or vNIOS Grid Master or independent appliance. For information about how to perform tasks specific to Infoblox, refer to the Infoblox NIOS Documentation.

Ensure that you have set up a NIOS administrator account with appropriate permissions. For information, see NIOS Permissions Requirements.

- Create a network to use for operations with the Infoblox IPAM Plug-In for VMware. vRealize Automation supports IPv4 networks. For more information, see the section Adding IPv4 Networks in the Infoblox NIOS Documentation.
- After you create a DHCP network, set the IPv4 DHCP options for the network. For information, see the section About IPv4 DHCP Options in the Infoblox NIOS Documentation. Note that IPv4 DHCP options can be used for storing network configuration information in Infoblox (default gateway, netmask, DNS, etc.) both for statically allocated IP addresses and DHCP allocated addresses.
- (Optional) Define DHCP address ranges from which you plan to allocate IP addresses through the Infoblox IPAM Plug-In for VMware. Also define DHCP options on the DHCP ranges. For information, see the section Configuring IPv4 Address Ranges in the Infoblox NIOS Documentation.
- If you use internal DNS servers, create the authoritative DNS zones to be used by the Infoblox IPAM Plug-In for VMware. For the creation of PTR records, you must set up a reverse DNS zone. Ensure that you associate the zones with networks. For information, Configuring DNS Zones in the Infoblox NIOS Documentation.
- (Optional) Set up DHCP network templates that are used by Infoblox IPAM Plug-In for VMware. For information, see About IPv4 Network Templates in the Infoblox NIOS Documentation.
- Create the extensible attribute definitions in NIOS for the IPAM object attributes that are used in the workflows of Infoblox IPAM Plug-In for VMware. For more information, see Using Extensible Attributes in Infoblox IPAM Plug-In for VMware.

Note: Infoblox IPAM Plug-In for VMware is qualified against Infoblox RESTful API (WAPI)2.0+

NIOS Permissions Requirements

On the Infoblox NIOS system, ensure that the admin and user accounts to be used with the Infoblox Plug-In for VMware meet the following requirements:

- To set up extensible attribute definitions, you must have a NIOS administrator account with GUI access.
- To use the Plug-In with the cloud API: Infoblox recommends that the cloud-api-only user account should not be given GUI access in NIOS.
  — For NIOS version earlier than 7.3: users must be members of the cloud-api-only admin group under NIOS.
  — For NIOS 7.3 and later: users must be members of an admin group under NIOS for which the role “Cloud API” is assigned. This can be any admin group, not only “cloud-api-only”. For more information, see Creating Superuser Admin Groups in Infoblox NIOS Documentation.
  — If the Cloud Network Automation license is installed on the Grid Master, you can assign Tenant permissions to admin users to restrict them to view objects related to a given tenant or a set of tenants.
- To use the Plug-In without the cloud API: users require API access.
- When using host records, read/write permissions are required for host objects in the destination forward zone(s) and for host objects in the destination reverse zone(s):
  — The Infoblox IPAM Plug-In for VMware generates an Infoblox host object that automatically creates A and PTR records in the appropriate forward and reverse zones. This implies a requirement for the write permissions to the zone(s).
- When using individual A/PTR records, read/write permissions are required for A and PTR in the forward and reverse zones associated with those records.
- Read/write permissions are required for the appropriate subnetworks:
  — Read/write permissions for NIOS fixed address/host is a minimum requirement. The Infoblox IPAM Plug-In for VMware by default adds the host with the MAC address, creating a fixed address in the appropriate subnet.
- Read/write permissions to the Grid members or associated appliance:
  — The Infoblox IPAM Plug-In for VMware performs a service restart, if enabled, when NIOS adds a fixed address. Without the read/write permissions, the Restart Service call by the Plug-In to the NIOS appliance will not work.
  — Note that this release supports disabling restarts. If you choose to disable restarts, the above permission is not required.
- Read permission to access Grid DHCP Properties:
  — This is required for retrieving DHCP options from NIOS for provisioning VMs.
Deploying Infoblox IPAM Plug-In for VMware

**Note:** Deployment of Infoblox IPAM Plug-in for VMware assumes that your vRealize Orchestrator and vRealize Automation instances are configured and running correctly. To make sure that the versions of vRealize Orchestrator and vRealize Automation are compatible with each other, refer to corresponding product documentation and VMware Product Interoperability Matrixes. See Resources for the links.

To deploy Infoblox IPAM Plug-In and configure it to work with vRealize Automation and NIOS, do the following:

1. Prepare your environment, as described in [Preparing Your Environment for vRealize Automation Management](#).
2. Import an SSL certificate for Infoblox NIOS, as described in [Importing NIOS SSL Certificate](#).
3. Install Infoblox IPAM Plug-In for VMware, as described in [Installing Infoblox IPAM Plug-In for VMware](#).
4. Perform the basic setup of the Plug-In, as described in [Performing Basic Plug-In Setup](#).
5. Configure your vRealize Automation, as described in [Configuring vRealize Automation](#).
Preparation Your Environment for vRealize Automation Management

You need to prepare some elements outside of vRealize Automation to support VM provisioning. To prepare your environment, do the following:

- Configure VMware vCenter Server with a customization specification, as described in Creating a Customization Specification in vCenter Server.
- Ensure that required services are up and running in vRealize Automation, as described in Ensuring Required Services are Up and Running.
- If you use external vRO, configure the vRealize Orchestrator authentication provider, as described in Configuring Authentication Provider.

Creating a Customization Specification in vCenter Server

You need to have a VM template and a customization specification in VMware vCenter Server to be able to create VMs in vSphere using vRealize Automation.

Customization specifications are XML files containing guest operating system settings for virtual machines. Specifications are handy for defining global features in guest operating systems such as the guest OS host’s name, domain name and other settings.

To create a customization specification:

1. In vCenter, choose vCenter -> Inventory -> Management -> Customization Specifications Manager.

2. Click New.
3. Select the Target Virtual Machine OS type.
4. In the Name field, enter the name for the new specification.
5. Click Next.
6. Select Use the virtual machine name and fill in the Domain Name field for the VM specification at the bottom of the pane. The Use the virtual machine name setting allows the VM to use the same name as for the guest operating system, which makes locating VMs easier for administrative purposes.
7. Click Next.
8. Select Area, Location and Hardware Clock Set, and then click Next.
9. Keep the Typical settings selected by default.
10. Click Next.
11. Enter the DNS Search Path (such as testrollout.infobloxIPAMdemo.com), click Add, and then click Next.
12. Click Finish. The vSphere Client appears, showing your new customization specification in the table.

Ensuring Required Services are Up and Running

Note: Before you proceed, make sure NIOS is operational and all necessary licenses are installed on it.

You can use vRealize Orchestrator embedded to your vRealize Automation or a standalone vRealize Orchestrator. The following instructions apply to the embedded vRealize Orchestrator.

Do the following:

1. Log in to the vRealize Automation Appliance console as root.
1. Execute the following command using the command line:
   
   ```
   service vco-configurator start
   ```

2. Enable the vRealize Orchestrator configurator to start on boot up of the vRealize Automation Appliance:
   
   ```
   chkconfig vco-configurator on
   ```

3. In the vRealize Automation Appliance window, click **VMware vRealize Appliance management**.

4. Click the **Services** tab.

5. Make sure that all services are registered. If some services are not registered, wait for some time and click **Refresh** to see if the services are registered.
Configuring Authentication Provider

To work properly and manage user permissions, external vRealize Orchestrator requires a method of authentication. If you log in to Orchestrator Control Center for the first time, you have to specify the authentication provider.

To configure the authentication provider:

1. Log in to Orchestrator Control Center.
2. On the Configure Authentication Provider page, select an authentication mode:
   — vRealize Automation: Orchestrator is authenticated through the vRealize Automation component registry.
   — vSphere: Orchestrator is authenticated through Platform Services Controller.
3. In Host address, enter your vRealize Automation or Platform Services Controller host address and click Connect.
4. Click Accept Certificate.
5. In User name and Password, enter the credentials of the vRealize Automation or vCenter Single Sign-On administrator account.
6. In Default tenant, enter the default domain to authenticate a user who logs in without a domain name. The default value is "vsphere.local".
7. Click Register.
8. In Admin group, enter an administrators group and click Search.
9. Select an administrators group.
10. Click Save Changes.

You can test the defined authentication provider on the Test Login tab. After you finish configuring the authentication provider, you can proceed to the next steps using the vRO Control Center.
Importing NIOS SSL Certificate

To ensure interoperability of vRealize Orchestrator with the Infoblox IPAM Plug-In for VMware, you must import valid SSL certificates from the NIOS appliance into vRealize Orchestrator.

To import an SSL certificate:

1. Log in to Orchestrator Control Center page.
2. Click Certificates.
3. In the Trusted Certificates tab, click Import.
4. Under Import from URL, enter the IP address or, under Import from file, select the certificate file for the NIOS appliance.
5. Click Import, and then click Import again to confirm.

The new SSL certificate appears in the Trusted SSL Certificates list.

Note: You can also generate a self-signed NIOS/vNIOS certificate for testing purposes if your existing NIOS/vNIOS certificate is expired. To do so, in the Grid Manager select -> Grid -> Grid Manager -> Members -> member check box, and then from Toolbar select Certificates -> HTT PS Cert -> Generate Self-Signed Certificate.
Installing Infoblox IPAM Plug-In for VMware

The Infoblox IPAM Plug-In for VMware is delivered as a zip archive file containing all versions of the Plug-in with a separate installation file for each version (o11nplugin-ipam.dar) in the corresponding folder.

To install the Infoblox IPAM Plug-In for VMware:

1. Unzip the Plug-In archive file into a folder on your system.
2. Log in to vRealize Orchestrator Control Center.

3. Click Manage Plug-Ins.
4. In the Manage Plug-Ins page, click Browse.
5. In the file upload dialog, select the .dar file (o11nplugin-ipam.dar) for the Plug-in version 4.4.0, and click Open.
6. Click Install.

   Note: If you see a warning message “Plug-In is incompatible” at this point, disregards the message and follow the steps described below. The message is due to a vRA issue and does not impact normal Plug-In installation.

7. Click Install again to confirm.
   The Infoblox IPAM Plug-In appears in the list of installed plug-ins.
8. If the Infoblox IPAM check box is not selected in the Enable plug-in column, select it and click Save Changes.
9. On the Startup Options page, click Restart and wait until the current status becomes “RUNNING”.

Copyright ©2019, Infoblox, Inc. All right reserved.
Performing Basic Plug-In Setup

Using the Setup Wizard workflow of the Infoblox IPAM Plug-In for VMware, you can perform basic setup of the Plug-In, including:

- Creating vRA and IaaS host instances in the vRealize Orchestrator inventory.
- Registering the “Infoblox IPAM” type of endpoint in vRealize Automation.
- Performing vRO customization in vRealize Automation. This customization consists in creating a vRO subscription to the events of the VM provisioning workflows in vRA.
- Creating the default property group with default Infoblox IPAM settings in the vRealize Automation dictionary. The Infoblox property group is used in the VM request blueprint.

If you use an embedded vRealize Orchestrator in to vRealize Automation, you select a predefined vRO instance as the vRA host. If you use an external vRealize Orchestrator, you must specify the host and connection parameters.

To perform basic Plug-In setup:

1. Log in to vRealize Orchestrator Client.
2. On the Workflows tab, expand Library -> Infoblox -> vRA -> Installation.
3. Right-click Setup Wizard and choose Start workflow.
4. In step 1 vRA Host, do one of the following for Create vRA host:
   - Select Yes if you use a standalone vRO and specify the host properties and connection parameters.
   - Select No if you use a built-in vRO and do not need to create the vRA host. Click Not set and select the predefined host.

**Note:** Infoblox recommends that you always install SSL certificates when creating a vRA host. To do so, select Yes for Automatically install SSL certificates.

---

Copyright ©2019, Infoblox, Inc. All right reserved.
5. Click Next.

6. If you are creating a new vRA host, specify the user credentials information.
7. Click **Next**.
8. In step 2 **IaaS host**, do one of the following for Create IaaS host:
   — Select **Yes** if you create a new IaaS host and specify the host properties and connection parameters. Optionally, you can use a proxy for the IaaS host.
Note: Infoblox recommends that you always install SSL certificates when creating an IaaS host. To do so, select Yes for Automatically install SSL certificates.

— Select No if you use a predefined IaaS host and do not need to create a new one. Click Not set and select the predefined host.

9. Click Next.

10. Specify the user credentials information. You can select either NTLM or SSO authentication type.
11. Click **Next**.
12. Specify the domain and workstation information.
13. Click Next.

14. In step 3 Property group, do the following:
   — Specify the details for the default Infoblox IPAM property group. If necessary, you can edit Infoblox IPAM properties in the default group later in vRA.
14. For Infoblox IPAM properties description, see Appendix B, “Infoblox IPAM Properties”.

15. Click Submit.

You can see the log of the Setup Wizard workflow execution on the Logs tab of the vRealize Orchestrator Client:

To verify that the required items are created in the result of the basic setup, see the next section, Verifying Basic Setup Results in Your Environment.

Note: If there is an error during the Setup Wizard workflow execution, the changes are rolled back.
Verifying Basic Setup Results in Your Environment

Verify that the following are in place:

- The vRA host instance is created: go to the vRealize Orchestrator Client → Inventory tab → refresh the vRealize Automation entry.

- The IaaS host instance is created: go to the vRealize Orchestrator Client → Inventory vRealize Automation Inventory entry.

- The “Infoblox IPAM” type of endpoint is created: go to vRealize Automation → Infrastructure → Endpoints → Endpoints → refresh the page. Then click New and see the “Infoblox IPAM” endpoint type created.
The vRO customization is performed in vRealize Automation. See the Setup Workflow execution log in vRealize Orchestrate to verify it. The default Infoblox IPAM properties groups is created: go to vRealize Automation -> Administration -> Property Dictionary -> Property Groups. The new property definitions are also added in the property dictionary.
Configuring vRealize Automation

To configure vRealize Automation, perform the following steps:

1. Add a tenant and local users, as described in Configuring Tenant Settings.
2. Configure an external or built-in vRealize Orchestrator server, as described in Configure vRealize Orchestrator Server.
3. Create vSphere and vRealize Orchestrator endpoints, as described in Creating vSphere and vRealize Orchestrator Endpoints.
4. Create an Infoblox IPAM endpoint, as described in Creating an Infoblox IPAM Endpoint.
5. Create a fabric group, as described in Creating a Fabric Group.
6. View compute resources, as described in Viewing Compute Resources.
7. Create a machine prefix, as described in Creating a Machine Prefix.
8. Create a business group, as described in Creating a Business Group.
9. Create a network profile of required type, as described in the corresponding sections:
   a. Creating an External Network Profile
   b. Creating a Routed Network Profile
   c. Creating a NAT Network Profile
10. Create a resource reservation and assign the Infoblox network profile to it, as described in Creating a Reservation.
11. Optionally, customize the Infoblox IPAM property group, as described in Customizing the Property Group.
12. Activate the blueprint designer, as described in Activating the Blueprint Designer.
13. Design a VM request blueprint and assign the Infoblox network profile and property group to it, as described in Designing a Blueprint.
14. Create a catalog service, as described in Creating a VM Request Service in vRealize Catalog.
Configuring Tenant Settings

You need to add a new tenant and local users in vRealize Automation. This is the tenant and users that work with Infoblox IPAM Plug-in for VMware to accomplish VM provisioning tasks.

Do the following:

1. Log in to vRealize Automation console as a tenant administrator.
2. On the Tenants tab, click New.
3. Specify general details for the new tenant.

New Tenant

<table>
<thead>
<tr>
<th>General</th>
<th>Local users</th>
<th>Administrators</th>
</tr>
</thead>
<tbody>
<tr>
<td>* Name:</td>
<td>newtenant</td>
<td></td>
</tr>
<tr>
<td>Description:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>* URL name:</td>
<td>nt</td>
<td></td>
</tr>
<tr>
<td>Contact email:</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Note: The URL name is used to append a tenant-specific identifier to the vRealize Automation console URL. For example, enter mytenant to create the URL https://vrealize-appliance-hostname.domain.name/vcac/org/mytenant.

4. Click Submit and Next.
5. On the Local Users tab, click New.
6. Specify user details.
7. Click **OK**, and then click **Next**.
8. On the **Administrators** tab, select the user to grant the Tenant and IaaS administrator roles in the corresponding fields:
   a. In the search field, type the user name or a part of it.
   b. Click the magnifying glass icon.
   c. Select the user from the found users list.
9. Click **Finish**.
### Configure vRealize Orchestrator Server

Indicate for vRealize Automation whether you use an external or the built-in (i.e., the default one) vRealize Orchestrator server.

To configure the vRealize Orchestrator server:

1. In vRA, click **Administration** -> **vRO Configuration** -> **Server Configuration**.
2. Do one of the following:
   - Select **Use the default Orchestrator server that was configured by the system administrator**.
   - Select **Use an external Orchestrator server**. Specify the server details.

   ![Server Configuration](image)

3. Optionally, click **Test Connection**.
4. Click **OK**.
Creating vSphere and vRealize Orchestrator Endpoints

To allow vRealize Automation to communicate with the vSphere environment and discover compute resources, collect data, and provision machines, you need to create a vSphere endpoint. After the vRealize Automation agent discovers the compute resources, create a vRealize Orchestrator endpoint. This allows vRealize Automation to communicate with vRealize Orchestrator and run custom workflows.

To create a vSphere endpoint:

1. In vRA, click Infrastructure -> Endpoints -> Endpoints.
2. Click New -> Virtual -> vSphere (vCenter).
3. Enter the required values for the following:
   - Name: For example, “vCenter”.
   - Description: Optionally, enter a description for the endpoint.
   - Address: Enter the URL in the format: `https://ip_address_or_FQDN/sdk` for vCenter, for example, `https://vcenter.infoblox.demo.com/sdk`.
   - User name: Specify the user name for connecting to vSphere.
   - Password: Specify the password for the above user name.
4. Click OK.
   The vRA agent starts discovering compute resources for the created vSphere endpoint.

To create a vRealize Orchestrator endpoint:

You need to specify a vRealize Orchestrator instance as an endpoint with which vRealize Automation communicates for VM provisioning.

1. Go to vRealize Automation and click Infrastructure -> Endpoints -> Endpoints.
2. Click New -> Orchestration -> vRealize Orchestrator.
3. On the General tab, specify the endpoint details:
   - Name: For example, “vRO”.
   - Description: Optionally, enter a description for the endpoint.
   - Address: For an embedded vRO, the URL should have the following format: `https://<vroip>/<fqdn>/vco`. For an external vRO, the URL should have the following format: `https://<vroip>/<fqdn>:8281/vco`.
   - User name: Specify the user name for connecting to vRO.
   - Password: Specify the password for the above user name.
   - Priority: Specify the endpoint priority. This is used when you have multiple vRO endpoints for connection.
4. If necessary, add custom properties on the Properties tab:
   a. Click New.
   b. Enter the property name and value.
   c. Click OK.
5. Click OK.
Creating an Infoblox IPAM Endpoint

When you create an Infoblox IPAM endpoint, you specify the master connection that vRealize Automation uses for communicating with NIOS. In addition to master connection, you can specify up to four connections for failover and API type in the endpoint properties. All connections use the same API type specified in the properties for interaction with NIOS.

See also Notes on Cloud Network Automation Connectivity.

1. In vRealize Automation, click Infrastructure → Endpoints → Endpoints.
2. Click New → IPAM → Infoblox.
3. Specify the endpoint details. Note that the fields Address, User name, and Password are mandatory despite the fact that they are not marked as such in the vRA interface. You must complete these fields for the endpoint to work correctly.

New Endpoint - Infoblox

Create an endpoint

The address specified here is the master connection.

4. In the Properties tab, click New and specify the API type for the endpoint:
   a. Enter the name-value pair for the API type of the connection: Infoblox.IPAM.APIType = WAPI or Cloud API.
   b. Click OK.

   Note: The Infoblox.IPAM.APIType custom property is optional. If it is not defined, the WAPI API type is used by default.

5. If necessary, add a failover connection in the following way:
   a. Click New and enter the name-value pair for the hostname of the NIOS connection for failover: Infoblox.IPAM.Endpoint1.Hostname = IP address or FQDN. Then click OK.
   b. Click New and enter the name-value pair for the user name: Infoblox.IPAM.Endpoint1.Username = username. Then click OK.
   c. Click New and enter the name-value pair for the password: Infoblox.IPAM.Endpoint1.Password = password. Then click OK.

6. If necessary, add more failover connections as described in the previous step. Use numbering in the failover name (1 to 4) to define the failover priority.
7. If you want to modify the default number of network ranges to retrieve for the network profile, define the custom property Infoblox.IPAM.GetIPRanges.maxResults:
   a. Click **New** and enter the name-value pair for the property: Infoblox.IPAM.GetIPRanges.maxResult= custom value.
   
   **Note:** By default, Infoblox IPAM Plug-In retrieves up to 1000 networks and ranges from NIOS while searching for network ranges to be added to the network profile. You can modify this max number as described above or by using the “max” option when searching for networks and ranges in the network profile. You can also use additional filters for network ranges to narrow down the number of results and finally be able to select the required network ranges. For more information, see Using Network Range Filters.

   b. Click **OK**.

8. Click **OK**.

### Notes on Cloud Network Automation Connectivity

Carefully consider the NIOS appliance to which you connect the Infoblox IPAM Plug-In for VMware. To use the Cloud Network Automation feature, you can connect to the Grid Master (if it is using the Cloud Network Automation license) or to a designated Cloud Platform Appliance (with the correct licensing) as necessary for your deployment. For more information, see the chapter Deploying Cloud Network Automation in the Infoblox NIOS Documentation.

See the table below for information on which API to use (WAPI or Cloud API) to support Cloud Network Automation and what connection options are supported.

<table>
<thead>
<tr>
<th>API Type</th>
<th>Cloud Network Automation UI</th>
<th>Connection Support</th>
<th>Tenant Object</th>
<th>Cloud EA Support*</th>
<th>Admin Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>WAPI</td>
<td>No</td>
<td>GM/GMC (Failover only)</td>
<td>No</td>
<td>No</td>
<td>Any</td>
</tr>
<tr>
<td>Cloud API</td>
<td>Yes</td>
<td>GM/GMC (Failover Only) and/or Cloud Platform Appliance</td>
<td>Yes</td>
<td>Yes</td>
<td>cloud-api-only</td>
</tr>
</tbody>
</table>

* Only some Cloud EAs can be accessed through WAPI. This requires setting Cloud EAs to read-only mode for cloud members.
Creating a Fabric Group

Fabric group is a group of administrators assigned to manage different types of network infrastructure and compute resources for the cloud. Administrators with this assignment can create infrastructure reservations, create and assign business groups and group managers, and configure approvals.

To create a fabric group:

1. In vRealize Automation, click **Infrastructure → Endpoints → Fabric Groups**.
2. Click **New**.
3. In the **Name** field, specify a name for the fabric group.
4. In **Fabric administrators**, specify one or more administrator accounts.
5. In **Compute resources**, select the discovered vSphere resources (ESXi hosts, clusters, etc.) to be managed by the group. For information about resource discovery, see the next section, *Viewing Compute Resources*.
6. Click **OK**.
7. Log out and log back in.
Viewing Compute Resources

To ensure that vRA fully discovered the VM templates and other compute resources needed for creating VMs, make sure that the data collection was successful:

1. In vRealize Automation, click **Infrastructure → Endpoints → Endpoints**.
2. Highlight to select the vCenter endpoint that you created earlier and in the Actions menu, click **View Compute Resources**.

3. Point to the compute resource associated with the vCenter endpoint and select **Data Collection**.

The data collection status is displayed as “Succeeded” as shown below.
3. If certain resources still are not discovered, click **Request now**.
   The status becomes “In queue”.

4. After a few minutes, click the **Refresh** button.
   The discovery process is completed successfully and displays the “Succeeded” status.
Creating a Machine Prefix

Machine prefixes are used for virtual machine naming when VMs are provisioned through vRA. They must contain only ASCII alphanumeric characters and hyphens and should not be longer than 15 characters, to conform to Windows host name 15-character limits. You need machine prefixes for creating business groups and blueprints.

To create a machine prefix:

1. In vRealize Automation, click **Infrastructure → Administration → Machine Prefixes**.
2. Click **New**.
3. In the **Name** field, type a name for the machine prefix.
4. Specify the number of digits (e.g., 2) and the next number (e.g., 1).
5. Click the green check mark to save the settings.

After the machine prefixes are complete, administrators can create business groups to allow users to access vRA to request virtual machines.
Creating a Business Group

A business group associates a set of resources and cloud services to a set of cloud users such as a company department or any other organizational unit. Business groups are created for the tenant by the tenant administrator. Tenant may have different business groups in its organization.

To create a business group:

1. In vRealize Automation, click Administration --> Users & Groups --> Business Groups.
2. Click New and fill in the following required fields:
   - Name
   - Send manager emails to

   New Business Group
   
   * Name: BG
   Description:
   * Send manager emails to: orgadmin@oro.com
   Active Directory Policy: No policy selected

3. Click Next.
4. Select users for the following roles:
   - Group manager role
   - Support role
   - Shared access role
   - User role
5. Click Next.
6. Specify the default machine prefix.

7. Click Finish.
   The new group appears in the business groups list.
Creating an External Network Profile

An external network profile specifies settings for an existing network. This network profile points to one or more networks or ranges in NIOS. These networks and ranges are used for allocating external IP addresses in NIOS while creating VMs.

To create an external network profile:

1. In vRealize Automation, click **Infrastructure** --> **Reservations** --> **Network Profiles** --> **New** --> **External**.
2. On the **General** tab, specify the network profile details, including the name of the IPAM endpoint created earlier.

3. Click the **Network Ranges** tab.
4. In **Address space**, select a network view in NIOS from those made available by the Infoblox IPAM endpoint. If you do not select a specific network view, IPAM Plug-In uses the default network view from NIOS.
5. In the **Select Network Range** dialog, specify the search criteria and click the Search icon. For how to search using filters, see *Using Network Range Filters*.

You can select more than one item from the search results. It means that if the first network range is exhausted while allocating IP addresses for VMs, the next one will be used for IP allocation.

**Note:** By default, the search returns no more than 1000 network ranges. You can modify the default max value of “1000” in the endpoint properties to accommodate your environment. For more information, see *Creating an Infoblox IPAM Endpoint*. If the results count is more than the specified limit, a warning message is displayed in the first row of the result table. However, if the number of results is too big, the operation may fail due to the 30 seconds vRealize Automation timeout. In this case, the Select Network Range dialog displays no or old
results. You can use filters to refine the search results and avoid both these problems. For more information, see Using Network Range Filters.

6. Select the appropriate network ranges.
7. Click Apply, and then OK.

Using Network Range Filters

To refine the network range search results, you can use the following filters in the Search field of the Select Network Range dialog:

- **max**: Specifies the number of the network ranges to retrieve from NIOS. This parameter takes higher priority over the value specified in the properties of the Infoblox IPAM endpoint (see Creating an Infoblox IPAM Endpoint). For example, `max=500` means that first 500 network and ranges will be retrieved from NIOS and displayed in the Select Network Range dialog. If NIOS contains more than 500 networks and ranges in the specified network view, a warning message is displayed in the first row of the results table. Then you can use additional filters described below to narrow down the number of results and finally be able to select the required network ranges.

- **network**: Refines the results by the network mask. You can use one of the two methods for specifying network mask:
  - Simple syntax. You can use the `*` special character only. For example, `network = 172.10.*`
  - Regular expression syntax. You may need this syntax type to retrieve a specific span of network ranges. For example, `network~=^\[1\]{1,2}\`.  
- **type**: Refines the results by specifying the type of object in NIOS. There are two possible values for this option:
  - network, for example, `type = network`
  - range, for example, `type = range`
- **Extensible attributes**: Filters network ranges by EAs that were set for them in NIOS. Enter the extensible attribute name and its value. You can use more than one extensible attribute. For example, `Country = USA and Building = 3111`.
Additionally, you can use the “ea” prefix preceding an extensible attribute name in order to differentiate the EA name from a filter name. For example, network = 172.10.* and ea:network = wireless. If your extensible attribute contains special characters such as a space, use double quotes (“ ”) to paraphrase the name and/or value. For example, ea: “Room Name” = “Spider Man”.

To combine filters, use the “and” operator. For example, type = network and network = 172.10.* and max = 10. To further refine your search, you can filter columns. To do so, click a column header and select Filters from the drop-down menu. In the text field, enter a string you want to use as the filter. For example, if you want to locate network ranges with prefix 20, enter ‘20.’ in the text field. The dialog displays only the network ranges that match your filtering criteria.
Creating a Routed Network Profile

To create a routed network profile:

1. In vRealize Automation, click Infrastructure -> Reservations -> Network Profiles -> New -> Routed.
2. In the General tab, specify a name for the routed network profile.
3. In IPAM endpoint, select the Infoblox NIOS endpoint that you created previously.
4. In External network profile, select the Infoblox network profile that you created previously for allocating external IP addresses.
5. In Range subnet mask, specify the network mask for on-demand networks to create.
6. In the IP Blocks tab, select the desired address space and click Add.
   A list of network containers available in NIOS is displayed. Note that address space in the vRA terminology corresponds to network view in NIOS and IP block corresponds to network container. You can search for specific network containers with the help of filters identical to those used for network ranges. For information, see Using Network Range Filters.
7. Select an IP block and click OK.
8. Click Apply, and then OK.
Creating a NAT Network Profile

To create a NAT network profile:

1. In vRealize Automation, click Infrastructure -> Reservations -> Network Profiles -> New -> NAT.
2. In the General tab, specify a name for the NAT network profile.
3. In IPAM endpoint, select the Infoblox NIOS endpoint that you created previously.
4. In External network profile, select the Infoblox network profile that you created previously for allocating external IP addresses.

   **Note:** If the NAT network is of “One-to-One” type, the corresponding external network profile must contain only one network or network range. Also, it must have at least two available IP addresses.

5. In NAT type, select One-to-One or One-to-Many.
6. In Subnet mask, specify the subnet mask for internal IP addressing.
7. In Gateway, specify the address of the network where internal NAT ranges will be created.
8. In the DNS tab, specify the DHCP options for the network. If no options are specified here, they are inherited from the network indicated in the external network profile.
9. In the Network Ranges tab, specify the details for the range or ranges to be created. The ranges must reside in the same network that the gateway you specified earlier. For a “One-to-Many” NAT network, you can add as many ranges as you need. If the IP address allocation from a range fails, an attempt is made to allocate an address from another range, and so on.
10. Click Apply, and then OK.
Creating a Reservation

A reservation reflects memory and storage allocations of the currently active VMs. To allocate part of available resources to a specific business group, you create a vSphere reservation. Also, you associate the NIOS network profile with the reservation.

To create a reservation:

1. Click Infrastructure -> Reservations -> Reservations.
2. Click New -> vSphere (vCenter).
   The New Reservation page appears.
3. On the General tab, complete the following required fields:
   — Name
   — Tenant: The tenant that you configured earlier.
   — Business group: Only users in this business group can provision machines by using this reservation.
   — Priority: The priority is used when a business group has more than one reservation. A reservation with priority 1 is used for VM provisioning over a reservation with priority 2.
   — Enable this reservation: Select this check box to enable the reservation.

New Reservation - vSphere (vCenter)

Create a reservation to allocate provisioning resources to a business group in a tenant. You also can copy from an existing reservation.

<table>
<thead>
<tr>
<th>General</th>
<th>Resources</th>
<th>Network</th>
<th>Properties</th>
<th>Alerts</th>
</tr>
</thead>
<tbody>
<tr>
<td>* Name: res1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>* Tenant: vsphere.local</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>* Business group: prod-business-group</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reservation policy:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>* Priority: 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

   Enable this reservation

4. On the Resources tab, complete the following fields:
   — Compute resource: Select the previously configured compute resource on which to provision machines.
   — Memory: Specify the amount of memory in GB to be allocated to this reservation.
   — Storage: Select one or more listed storage paths and reserve the capacity.

New Reservation - vSphere (vCenter)

Create a reservation to allocate provisioning resources to a business group in a tenant. You also can copy an existing reservation to use as a starting point.

<table>
<thead>
<tr>
<th>General</th>
<th>Resources</th>
<th>Network</th>
<th>Properties</th>
<th>Alerts</th>
</tr>
</thead>
<tbody>
<tr>
<td>* Compute resource: 10.30.1.59 (vCenter)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

   Machine quota: Unlimited

   * Memory: Physical | Total Reserved | Total Allocated | This Reservation

   128 | 0 | 0 | 50

   * Storage:

<table>
<thead>
<tr>
<th>Storage Path</th>
<th>Physical</th>
<th>Free</th>
<th>Total Reserved</th>
<th>Total Allocated</th>
<th>This Reservation</th>
<th>Priority</th>
<th>Disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>10_30_1_59_datastore1</td>
<td>1674</td>
<td>447</td>
<td>0</td>
<td>50</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10_30_1_59_datastore2</td>
<td>1674</td>
<td>178</td>
<td>0</td>
<td></td>
<td></td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>
For information on forcing the resource discovery, see the next section, *Forcing Resource Discovery.*

5. Click the **Network** tab.
6. Select **VM Network**, and then select the external Infoblox network profile that you created previously.

### New Reservation - vSphere (vCenter)

Create a reservation to allocate provisioning resources to a business group in a tenant. You also can copy an existing reservation to use as a starting point.

- **Copy from existing reservations:**

  - **Network**

    - **VM Network**
      - Infoblox-External
    - **vCenter-External-1**
      - Infoblox-External
    - **vCenter-External-2**
      - Infoblox-External

- **Advanced Settings**

  - **Transport zone:**
    - Global-TransportZone
  - **Security group:**
    - Activity-Healthcheck-DataCollection

- **Distributed logical router:**

  - **Name:**
    - DLB
  - **Network Profile:**
    - Infoblox-External

**Note:** If you use the Infoblox IPAM Plug-In for provisioning VMware NSX load balancers, select a web switch instead of VM network.

7. In **Advanced Settings**, specify the following for an on-demand routed or NAT network profile:
   - Transport zone
   - Distributed logical router

8. Click **OK**.

The new reservation appears in the list.

**Note:** When you request a VM, it can be provisioned on any reservation of the appropriate type that has sufficient capacity for the machine, and cannot guarantee from which reservation it is provisioned. You apply a reservation policy to a blueprint to restrict the machines provisioned from that blueprint to a subset of available reservations. A reservation policy is simply a container with a name, which contains one or more reservations. The VMs created from the request use the resources assigned to them from the policy.

---

**Forcing Resource Discovery**

If certain resources are not visible during the creation of a new reservation, run the resource discovery process again so they become visible.

To force the resource discovery:

1. Click **Infrastructure** -> **Compute Resources** -> **Compute Resources**.
2. Point to the compute resource associated with the vCenter endpoint and select **Data Collection**.
3. Click **Request now**. The status becomes “In queue”.
4. After a few minutes, click **Refresh**. The discovery process is completed successfully and displays the “Succeeded” status.

Now you can go back to the **Reservation** section and verify that the new resources are visible. Note that you must do this every time you add or remove a VM template from ESXi/vCenter so you will see the most up-to-date templates listed when creating a new blueprint.
Customizing the Property Group

A property group contains a list of parameters that are applied to the VM when you initialize a new vRA request. Using the properties, you can specify the type of record to create in NIOS when provisioning a VM, the desired DNS view in NIOS where DNS records should be created, and so on. For properties descriptions, see Appendix B, “Infoblox IPAM Properties”.

The “Infoblox-Default” property group is created automatically after the execution of the Setup Wizard workflow at Plug-In setup. For information, see Performing Basic Plug-In Setup. The default property group contains predefined default values that are applicable to most configurations. You can either use the default Infoblox property group as is or customize it to meet your particular requirements.

To customize the default Infoblox property group:

1. In vRealize Automation, click Administration -> Property Dictionary -> Property Groups.
2. Select the “Infoblox-Default” property group and click Edit.
3. Modify the values of the properties according to your needs.
4. Click OK.

Alternatively, you can create a custom Infoblox property group and use it instead of the default one for designing a blueprint. For information about creating a custom property group, see Create Property Group Workflow.
Activating the Blueprint Designer

You design a blueprint to assemble infrastructure components and define the item that you request from the catalog. To be able to design a blueprint, you need to obtain certain permissions for your account by activating the blueprint designer.

To activate the blueprint designer:

1. In vRA, click Administration -> Users & Groups -> Directory Users & Groups.
2. Find your current tenant admin account using the search field.
3. Click on the account to open it for editing.
4. In Add roles to this User, select all available roles.
5. Click Finish.
6. Log off and log in again using the same account. The Design tab is activated in the vRealize Automation tabs menu.
Designing a Blueprint

In the simplest configuration, you can publish just one machine component as a blueprint. You can design a blueprint for a specific network type, including:

- Existing network
- On-demand routed network
- On-demand NAT network

To design a blueprint:

1. In vRA, click **Design -> Blueprints -> New.**
2. Enter the name (e.g., Linux) and the number of archive days for the new blueprint.

![New Blueprint dialog](image)

3. If you create the blueprint for a routed or NAT network, click the **NSX Settings** tab and specify the transport zone.

![NSX Settings](image)

4. Click **OK.**
5. In the **Categories** pane, select **Machine Types** and drag-and-drop the **vSphere Machine** component onto the design canvas.
6. On the **General** tab, complete the following fields:
   — An ID (e.g., Linux).
   — The machine prefix created earlier.
   — The number of instances.
6. On the Build Information tab, complete the following fields:
   — In the Action field, select Clone.
   — In the Clone from field, select a VM template for creating VMs in vSphere.

   **Note:** If you do not find the required VM template in the Clone from field, run the resource discovery process as described in *Forcing Resource Discovery* so that vRA can locate the required template.

   — In the Customization spec field, always specify the customization specification that you created earlier for configuring VMs on vSphere. For information, see *Creating a Customization Specification in vCenter Server*.

7. Specify the network type for the blueprint: in the Categories pane, select Network & Security and drag-and-drop the required network type onto the design canvas. Select one of the following:
   — Existing Network
   — On-Demand Routed Network
   — On-Demand NAT Network

8. For an existing network, do the following:
   a. On the General tab of the network properties, click the three dots button for *Existing network* and select the external Infoblox IPAM network profile that you created earlier.
For an on-demand routed network, do the following:

a. In the General tab of the network properties, click the three-dots button for Parent network profile and select the routed network profile that you set up previously. Notice in the IP Blocks tab a list of NIOS network containers retrieved by the Get IP Ranges workflow. If you open a network container for viewing, you can see the DHCP options of the network container in NIOS.

b. Click Save.

For an on-demand NAT network, do the following:

a. In the General tab of the network properties, click the three-dots button for Parent network profile and select the NAT network profile that you set up previously.

b. Click Save.

If you use a load balancer, do the following to define it:

a. In the Categories pane –> Network & Security, drag-and-drop the On-Demand Load Balancer component onto the design canvas.

b. Specify the ID for the load balancer.

c. In Member, specify the vSphere machine that you defined earlier.

d. In Member network and VIP network, select the predefined network items.

e. In Virtual servers, click New and add the required protocols to use.

f. Leave the IP address field blank as the IP address is taken from NIOS when the machine is provisioned.

g. Click the vSphere Machine component and in the General tab, specify the minimum and maximum number of instances.

In the vSphere Machine component details, assign the network profile to the machine blueprint as follows:

a. On the Network tab, click New.

b. Select the network that you have defined earlier. This can be either an external, routed, or NAT network.

c. Click OK.

The network profile is assigned to the blueprint.
14. On the **Properties** tab of the vSphere Machine component, click **Add** and specify the property group. You can specify either the Infoblox default property group generated at the Plug-In deployment or a custom Infoblox property group created earlier.

![Property Groups](image)

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Infoblox-Default</td>
<td>test-1</td>
</tr>
</tbody>
</table>

15. Click **Finish**. The created blueprint appears in the list of blueprints.

16. Select the created blueprint and click **Publish**. The new blueprint is published in vRealize Automation.
Creating a VM Request Service in vRealize Catalog

The vRealize Automation service catalog is where you request virtual machines. You can request a VM by creating and using a specific service which contains the machine blueprint that you published in the previous section. The machine blueprint is a catalog item that you associate with the service and entitle to users.

To create a VM request service:

1. Click **Administration** -> **Catalog Management** -> **Services**.
2. Click **New**.
3. Specify the name and set the status to **Active**.
4. Click **OK**.
5. Click the **Catalog Items** tab.
6. Select the name of the published blueprint to open it for configuring.
7. In **Service**, select the newly-created service.
8. Click **OK**.
9. Click **Entitlements** in the left pane.
10. Click **New**.
11. On the **General** tab, complete the following fields:
   — **Name**
   — **Status**: Set the status to Active.
   — **Business group**: Select the business group that you created earlier.
   — **Users & Groups**: Add your current tenant admin account.
12. Click **Next**.
13. On the **Items & Approvals** tab, complete the following fields:
   — Click the plus sign for **Entitled Services**, select the check box for the service that you created above, and then click **OK**.
   — Click the plus sign for **Entitled Items**, select the check box for the service that you created above, and then click **OK**.
   — Click the plus sign for **Entitled Actions**, select the check boxes for any services needed for the new entitlement, and then click **OK**.
14. Click Finish. The added entitlement appears in the list.
15. Refresh the web browser. The newly-added service item appears on the Catalog tab of vRealize Automation.

You are now ready to provision and deprovision VMs and have their host, DNS, and DHCP records simultaneously reflected in NIOS. As an example, see the next section, Provisioning and De-provisioning VMs with Registration in NIOS.
Specifying DNS domain while requesting VM

You can override the domain name under DHCP option of a network by providing the custom dnsSuffix value or domain name as a custom property in vRA during the provisioning of VMs. This will allow you to have a different domain name for a set of IPAddress/IP Range in a network.

Example:
Infoblox.IPAM.Network0.dnsSuffix = "<custom dnsSuffix>"

You can provide the custom dnsSuffix value by using one of the following methods:

- During creation/design of a Blueprint:
  1. In vRA, navigate to Design -> Blueprints  Edit Blueprint screen in vRA. For more information, see Designing a Blueprint.
  2. On the Properties tab, click Custom Properties.
  3. Click New and add the following custom dnsSuffix property:
     Infoblox.IPAM.Network0.dnsSuffix = "<custom dnsSuffix>".
  4. Click Save.

- While requesting a published catalog item:
  1. In vRealize Automation, go to the Catalog tab.
  2. Click Request for the appropriate pre-configured service.
  3. In the Deployment panel, click Properties.
  4. Click New and add the following custom dnsSuffix property:
     Infoblox.IPAM.Network0.dnsSuffix = "<custom dnsSuffix>".
  5. Click Save.
Provisioning and De-provisioning VMs with Registration in NIOS

After you deployed the Infoblox IPAM Plug-In for VMware, you can submit requests for VM provisioning and de-provisioning using vRealize Automation. When you provision a VM, the specified host record, DNS records, or DHCP records are registered in NIOS. When you de-provision the VM previously registered in NIOS using the Infoblox IPAM Plug-In, the records are removed from NIOS. For more information, see the following:

- Provisioning a VM
- De-provisioning a VM
Provisioning a VM

To create a VM with Infoblox IPAM properties:

1. In vRealize Automation, go to the Catalog tab.
2. Click Request for the appropriate pre-configured service.
3. Select the machine defined in the blueprint.
4. Specify the general details for the VM.
5. Specify the storage details for the VM.
6. In the Properties tab, you can either use the displayed Infoblox IPAM properties as is or modify them by selecting a property and clicking Edit.

For properties description, see Appendix B, “Infoblox IPAM Properties”. For which properties to set to TRUE and FALSE when requesting a VM with specific records, see Appendix D, “Record Properties for VM Requests”. For information about customizing the Infoblox IPAM properties, see Customizing the Property Group.

7. Click Submit.
8. Click OK.

To see the execution information for the request, go to the Requests tab in vRealize Automation and select the request. In vRealize Orchestrator, you can go to the Infoblox vRA workflows section and see that the Allocate workflow is triggered and displays its execution information in the Logs tab. See vRA Workflows.

Then you can go to the Infoblox Grid Manager, select Data Management → IPAM Home and see that the IP address is registered.
De-provisioning a VM

To de-provision a VM:

1. In vRealize Automation, go to Items → Deployments.
2. Select the required VM.
3. Click Destroy.

When you destroy a VM, the Release workflow of the Infoblox IPAM Plug-In is called to remove the machine records from NIOS. See vRA Workflows.
Using Extensible Attributes in Infoblox IPAM Plug-In for VMware

The Infoblox IPAM Plug-In for VMware uses extensible attributes to tag objects in NIOS (host records, fixed addresses, networks, etc.) that belong to the VMware platform. They are typically manually created by admins in the NIOS Grid Manager. Each attribute tracks specific information about the object. It allows the Plug-In to locate and track IPAM objects in NIOS and synchronize the data with vRealize Automation.

For the integration of the Infoblox Plug-In and NIOS with vRealize Automation, you must create the following extensible attributes on NIOS:

<table>
<thead>
<tr>
<th>Extensible Attribute</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware resource ID</td>
<td>String</td>
</tr>
<tr>
<td>VMware NIC index</td>
<td>Integer</td>
</tr>
<tr>
<td>VMware On-Demand Network</td>
<td>String</td>
</tr>
<tr>
<td>VMware Request ID</td>
<td>String</td>
</tr>
<tr>
<td>VMware Network Profile ID</td>
<td>String</td>
</tr>
<tr>
<td>VMware External Network Profile ID</td>
<td>String</td>
</tr>
<tr>
<td>VMware Blueprint Request ID</td>
<td>String</td>
</tr>
<tr>
<td>VMware External Range ID</td>
<td>String</td>
</tr>
</tbody>
</table>

(If you use the Cloud API connection type, you need to make sure that the following set of Cloud extensible attributes has been automatically created on NIOS:

<table>
<thead>
<tr>
<th>Extensible Attribute</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tenant ID</td>
<td>String</td>
</tr>
<tr>
<td>VM ID</td>
<td>String</td>
</tr>
<tr>
<td>VM Name</td>
<td>String</td>
</tr>
</tbody>
</table>

These attributes become visible only when the Cloud Network Automation license is applied.

Note that these Cloud extensible attributes are not required for the WAPI connection type that is used by default.

You can use extensible attributes for searching and filtering data or grouping objects in NIOS. For more information, see About Extensible Attributes in the Infoblox NIOS Documentation.

See also Extensible Attributes in IPAM Workflows and Reloading Extensible Attributes.
Extensible Attributes in IPAM Workflows

In the IPAM workflows of the Infoblox Plug-In, you can use extensible attributes to assign attribute values to objects created in the result of workflow executions. Some workflows, including Reserve IP address, Reserve IP in range, Reserve IP in network, and Add network enable you to set EA values for the object when it is created in NIOS through the workflow. Other workflows, such as Remove host record, Remove network, and Remove range allow you to use extensible attributes as criteria to search for host records, networks, or ranges. This is illustrated in the following figure:

![Start Workflow: Remove host record](image)

The Definition of the extensible attribute #... field specifies the extensible attribute pre-existing on NIOS and selected from the vRO inventory. The Type of the comparison... parameter specifies a comparison operator used for searching. The following figure shows the list of six comparison operators available in the Infoblox IPAM Plug-In for VMware:

![Comparer](image)

For information about workflows that use extensible attributes, see IPAM Workflows.

Note: You can add up to ten extensible attributes to the Infoblox IPAM Plug-In through vRO. You can add more attributes with the Infoblox JavaScript API which has no restrictions on EA count.
Reloading Extensible Attributes

The extensible attributes from NIOS are cached in the Infoblox IPAM Plug-in. Therefore, if an extensible attribute is added, changed, or deleted in NIOS, you need to reload your extensible attributes in the Infoblox IPAM Plug-in for the changes to apply.

To reload extensible attributes:

1. In the vCO client, click the **Inventory** tab.
2. Click to expand **Infoblox IPAM** --> IP address of the NIOS appliance --> **Extensible Attributes**.
3. Right-click **Extensible Attributes** and select **Reload** or press the F5 hot key.

You can also reload extensible attributes via the `IpamConnection.reloadExtensibleAttributeDefinitions()` API method.
Using Workflows of Infoblox IPAM Plug-In for VMware

The Infoblox IPAM Plug-In for VMware operates with workflows of the following types:

- **IPAM Workflows**
- **vRA Workflows**

To access the Infoblox IPAM Plug-In for VMware workflows library in vRO:

1. Log in to the VMware vRealize Orchestrator client and choose either **Run** or **Design** mode.
2. Click the **Workflows** tab.
3. Expand the administrator entry in the workflows tree.
4. Expand the **Infoblox** folder. This folder contains the workflows of the Infoblox IPAM Plug-In for VMware:

![Workflows Tree](image)

You can also build custom workflows using actions and API objects and methods of the Infoblox IPAM Plug-In for VMware. See *Using Actions of Infoblox IPAM Plug-In for VMware* and *Using API of Infoblox IPAM Plug-In for VMware*. 
IPAM Workflows

The IPAM workflows of the Infoblox IPAM Plug-In for VMware automate IPAM operations in a virtualized environment. They provide integration of the VMware environment with NIOS, used for running IPAM operations related to NIOS objects. The IPAM workflows are called from the higher-level vRA workflows or can be run manually by the vRO admin.

In the IPAM workflows, you can use extensible attributes. For more information, see Using Extensible Attributes in Infoblox IPAM Plug-In for VMware.

You access the IPAM workflows from <Admin>→ Library → Infoblox. The IPAM workflows include the following:

<table>
<thead>
<tr>
<th>Workflow Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reserve IP address</td>
<td>Reserves the specified static IP address and creates either a host, DNS, or DHCP record in the NIOS database. See Reserve IP Address Workflow.</td>
</tr>
<tr>
<td>Reserve IP in network</td>
<td>Gets next available IP address from the specified network and reserves it. Creates either a host, DNS, or DHCP record in the NIOS database. See Reserve IP in Network Workflow.</td>
</tr>
<tr>
<td>Reserve IP in range</td>
<td>Gets next available IP address from the specified network range and reserves it. Creates either a host, DNS, or DHCP record in the NIOS database. See Reserve IP in Range Workflow.</td>
</tr>
<tr>
<td>Remove host record</td>
<td>Removes the host record of the specified host or of multiple hosts from the NIOS database. See Remove Host Record Workflow.</td>
</tr>
<tr>
<td>Remove DHCP record</td>
<td>Removes one or more fixed IP addresses or reservations from the NIOS database. See Remove DHCP Record Workflow.</td>
</tr>
<tr>
<td>Remove DNS record</td>
<td>Removes DNS records from the NIOS database. See Remove DNS Record Workflow.</td>
</tr>
<tr>
<td>Add network</td>
<td>Creates a new IP network in the NIOS database. See Add Network Workflow.</td>
</tr>
<tr>
<td>Remove network</td>
<td>Removes previously configured IP network or multiple networks from the NIOS database. See Remove Network Workflow.</td>
</tr>
<tr>
<td>Add range</td>
<td>Adds a network range to the NIOS database. See Add Range Workflow.</td>
</tr>
<tr>
<td>Remove range</td>
<td>Removes a network range from the NIOS database. See Remove Range Workflow.</td>
</tr>
<tr>
<td>Restart IPAM services</td>
<td>Restarts IPAM services. See Restart IPAM Services Workflow.</td>
</tr>
</tbody>
</table>

The Infoblox IPAM Plug-In for VMware workflows support the following types of records:

- Host record
- Fixed address
- IPv4 reservation
- A record (for IPv4 addresses)
- AAAA record (for IPv6 addresses)
- PTR record
- CNAME record

You can also use the IPAM workflows to build custom batch workflows in vRealize Orchestrator. For information about building batch workflows, refer to the vRealize Orchestrator documentation.

**Note:** Before you execute IPAM workflows, make sure that the Infoblox IPAM connection is available in the vRO Inventory tab. If it is not there, run the Create IPAM Connection workflow from vRO <admin> → Library → Infoblox → vRA → Helpers. Then go to the vRO inventory, select Infoblox IPAM, and refresh the selected node. Before creating a new IPAM connection, make sure that there is no connection with the same priority in the vRO inventory.
Reserve IP Address Workflow

The Reserve IP address workflow allows you to reserve a specified IPv4 or IPv6 address, create a host record, or create a DNS record for a host in NIOS. The workflow creates the specified IPAM records with the defined static IP address.

You can choose which IPAM object to create in this workflow:

- Host record
- A/AAAA record with or without an associated PTR record
- CNAME records related to the created A/AAAA record
- Fixed address or reservation

Using the Reserve IP address workflow, you can assign extensible attributes to the IPAM objects that you create.

To reserve an IP address:

1. Log in to the vCenter Orchestrator client.
2. Choose Run mode.
3. On the Workflows tab, select the administrator entry -> Library -> IPAM.
4. Right-click the Reserve IP address workflow and choose Start workflow.
5. Complete the Connection step to establish the connection to the NIOS IPAM appliance: click the Connection to the IPAM server field.
   
   Expand Infoblox IPAM, select the IP address of a NIOS Grid member, and click Select.
6. Click Next.
7. In the IP Address step, specify the IP address to be reserved and, optionally, a network view, and then click Next.
8. In the Common parameters step, select one of the following for Create host record?
   
   - Select Yes and specify the FQDN host name, enable or disable DNS and DHCP for the host record and, optionally, specify a MAC address or DUID, aliases, and a comment.
   
   - Select No and specify if you want to create a DNS record and/or fixed address/reservation.

9. To create a DNS record, specify the type of DNS record (A/AAAA or A/AAAA/PTR), the FQDN hostname and, optionally, a DNS view, CNAME aliases, and a comment. You can associate CNAME records with the created A/AAAA record by setting aliases in FQDN format.
   
   For more information, see the section Managing CNAME Records in the NIOS Documentation.
10. To create a fixed address or reservation, specify which of them to create, the name and comment. For the fixed address, specify a MAC address or DUID and, optionally, an IPv4 address of the Microsoft DHCP server.
11. Click Next.
12. (Optional) In the Extensible attributes step, specify the number of, and the values for, any extensible attributes that you want to assign to the records or objects that will be created in the result of the workflow execution. For more information about extensible attributes, see
13. Click Next.
14. Specify if restarting the DHCP service is needed. When you select Yes, the DHCP service will be restarted when it is required by NIOS configuration. For more information, see Appendix E, "Operations Requiring Service Restart".
15. Click Submit.
Reserve IP in Network Workflow

This workflow reserves an IP address in IPAM: it gets the next available IP address from the specified network and creates the specified IPAM object. Note that allocating the next available IP address and creating a host record with it is performed by a single `addHostInNetwork` action within this workflow. You can choose which IPAM object to create in this workflow:

- Host record
- A/AAAA record with or without an associated PTR record
- CNAME records related to the created A/AAAA record
- Fixed address or reservation

Using the `Reserve IP` in network workflow, you can assign extensible attributes to the created objects.

To reserve an IP address in a network:

1. Log in to the vCenter Orchestrator client.
2. Choose Run mode.
3. On the Workflows tab, select the administrator entry —> Library —> IPAM.
4. Right-click the `Reserve IP in network` workflow and choose Start workflow.
5. Complete the Connection step to establish the connection to the NIOS IPAM appliance: click the Connection to the IPAM server field. Expand Infoblox IPAM and select the IP address of the Infoblox NIOS Grid member. Click Select.
6. Click Next.
7. In the Network step, specify the network IP address, the CIDR of the network range and, optionally, a network view.
8. Click Next.
9. In the Common parameters step, specify the records to create as described in Step 8 of the section Reserve IP Address Workflow.
10. Click Next.
11. (Optional) In the Extensible attributes step, specify the number of, and the values for, any extensible attributes that you want to assign to the records or objects that will be created in the result of the workflow execution. For more information about extensible attributes, see Extensible Attributes in IPAM Workflows.

12. Click Next.
13. Specify if restarting the DHCP service is needed. When you select Yes, the DHCP service will be restarted when it is required by NIOS configuration. For more information, see Appendix E, "Operations Requiring Service Restart".
14. Click Submit.
Reserve IP in Range Workflow

Use the Reserve IP in range workflow to allocate an IPv4 or IPv6 address within a specific DHCP address range to a virtual machine on your network. When you use this workflow, the NIOS appliance obtains the next available IP address within the defined address range and creates the specified IPAM records. Note that allocating the next available IP address and creating a host record with it is performed by a single addHostInRange action within this workflow.

You can choose which IPAM object to create in this workflow:
- Host record
- A/AAAA record with or without an associated PTR record
- CNAME records related to the created A/AAAA record
- Fixed address or reservation

Using the Reserve IP in range workflow, you can assign extensible attributes to the created objects.

To reserve an IP address in a network range:

1. Log in to the vCenter Orchestrator client.
2. Choose Run mode.
3. On the Workflows tab, select the administrator entry → Library → IPAM.
4. Right-click the Reserve IP in range workflow and choose Start workflow.
5. Complete the Connection step to establish the connection to the NIOS IPAM appliance; click the Connection to the IPAM server field. Expand Infoblox IPAM and select the IP address of the Infoblox NIOS Grid member. Click Select.
6. Click Next.
7. In the Network range step, specify the start address and end address of the network range and, optionally, a network view.
8. In the Common parameters step, specify the records to create as described in Step 8 of the section Reserve IP Address Workflow.
9. Click Next.
10. (Optional) In the Extensible attributes step, specify the number of, and the values for, any extensible attributes that you want to assign to the records or objects that will be created in the result of the workflow execution. For more information about extensible attributes, see Extensible Attributes in IPAM Workflows.
11. Click Next.
12. Specify if restarting the DHCP service is needed. When you select Yes, the DHCP service will be restarted when it is required by NIOS configuration. For more information, see Appendix E, "Operations Requiring Service Restart".
13. Click Submit.
Remove Host Record Workflow

Use the Remove host record workflow to remove a host that you previously created in the NIOS database. When you use this workflow, the NIOS appliance releases the IP address and removes IPAM records associated with the host.

In this workflow, you can specify either a particular host name or extensible attributes to search for hosts by certain criteria. The matching hosts and their associated records are removed from NIOS.

1. Log in to the vCenter Orchestrator client.
2. Choose Run mode.
3. On the Workflows tab, select the administrator entry –> Library –> IPAM.
4. Right-click the Remove host record workflow and choose Start workflow.
5. Complete the Connection step to establish the connection to the NIOS IPAM appliance: click the Connection to the IPAM server field. Expand Infoblox IPAM and select the IP address of the Infoblox NIOS Grid member. Click Select.
6. Click Next.
7. In the Remove criteria step, define how you want to remove the host record. Select one of the following criteria by which to remove:
   - Host name: Specify the FQDN host name and, optionally, the DNS view of the host record.
   - IP address: Specify the IP address and, optionally, the network view of the host record.
   - Extensible attributes: To find and remove the host or hosts that match some criteria, you can specify extensible attributes.

For more information about extensible attributes, see Extensible Attributes in IPAM Workflows.

8. Click Submit.
Remove DHCP Record Workflow

This workflow removes a fixed address or reservation from the NIOS database. You can specify either a particular IP address or extensible attributes to search for the fixed addresses/reservations to be removed. Note that IP reservation objects in NIOS consist only of IPv4 addresses. Fixed address objects may be either IPv4 or IPv6.

1. Log in to the vCenter Orchestrator client.
2. Choose Run mode.
3. On the Workflows tab, select the administrator entry –> Library –> IPAM.
4. Right-click the Remove DHCP record workflow and choose Start workflow.
5. Complete the Connection step to establish the connection to the NIOS IPAM appliance: click the Connection to the IPAM server field. Expand Infoblox IPAM and select the IP address of the Infoblox NIOS Grid member. Click Select.
6. Click Next.
7. In the Remove criteria step, do one of the following:
   - Specify the IP address assigned to the fixed address or reservation records and, optionally, the network view where they reside.
   - Select Yes to use extensible attributes to search for records and specify the EAs options. For more information about extensible attributes, see Extensible Attributes in IPAM Workflows.
8. Click Submit.
Remove DNS Record Workflow

This workflow removes A/AAAA, PTR and CNAME records from the NIOS database if they exist. You can specify either a particular host name or extensible attributes to search for the DNS records to be removed.

1. Log in to the vCenter Orchestrator client.
2. Choose Run mode.
3. On the Workflows tab, select the administrator entry –> Library –> IPAM.
4. Right-click the Remove DNS record workflow and choose Start workflow.
5. Complete the Connection step to establish the connection to the NIOS IPAM appliance: click the Connection to the IPAM server field. Expand Infoblox IPAM and select the IP address of the Infoblox NIOS Grid member. Click Select.
6. Click Next.
7. In the Remove criteria step, do one of the following:
   — Specify the FQDN host name assigned to the DNS records and, optionally, the DNS view where they reside.
   — Select Yes to use extensible attributes to search for records and specify the EAs options. For more information about extensible attributes, see Extensible Attributes in IPAM Workflows.
8. Click Submit.
Add Network Workflow

This workflow creates a new network on the NIOS appliance that can be later assigned to vApps and other resources through vRealize Automation. You can choose to use a network template in this workflow. If you choose to create the network without a template, you will specify the DHCP options (routers, DNS suffix, DNS servers, search DNS suffixes, and WINS) and assign members for the network.

In the Add network workflow, you can specify the extensible attributes to assign to the newly-created network.

To add a network:

1. Log in to the vCenter Orchestrator client.
2. Choose Run mode.
3. On the Workflows tab, select the administrator entry -> Library -> IPAM.
4. Right-click the Add network workflow and choose Start workflow.
5. Complete the Connection step to establish the connection to the NIOS IPAM appliance: click the Connection to the IPAM server field. Expand Infoblox IPAM and select the IP address of the Infoblox NIOS Grid member. Click Select.
6. Click Next.
7. In the Template step, specify whether to use or not a template for the new network:
   — Select Yes, enter the template name, and click Next.
   — Select No and click Next.
   For information about NIOS network templates, see the chapter Managing DHCP Templates in the NIOS Documentation.
8. In the Network step, specify the network parameters:
   — Enter the IPv4 or IPv6 network address.
   — Enter the CIDR of the network range such as 24 or 80. Enter only the numeric value without a forward slash (/).
   — Optionally, select the network view.
   — Optionally, provide a comment.
9. Click Next.
10. (Optional) In the Extensible attributes step, specify the number of, and the values for, any extensible attributes that you want to assign to the network object that will be created in the result of the workflow execution. For more information about extensible attributes, see Extensible Attributes in IPAM Workflows.
11. Click Next.
12. Specify if restarting the DHCP service is needed. When you select Yes, the DHCP service will be restarted when it is required by NIOS configuration. For more information, see Appendix E, "Operations Requiring Service Restart".
13. Click Submit.
Remove Network Workflow

This workflow removes a NIOS network or multiple networks previously created with the Add network workflow. You can specify either a particular network address with network mask or extensible attributes to search for networks to be removed.

To remove a network:

1. Log in to the vCenter Orchestrator client.
2. Choose Run mode.
3. On the Workflows tab, select the administrator entry -> Library -> IPAM.
4. Right-click the Remove network workflow and choose Start workflow.
5. Complete the Connection step to establish the connection to the NIOS IPAM appliance: click the Connection to the IPAM server field. Expand Infoblox IPAM and select the IP address of the Infoblox NIOS Grid member. Click Select.
6. Click Next.
7. In the Remove Criteria step, do one of the following:
   — Specify the IP address of the network, the CIDR, and, optionally, the network view where the network resides.
   — Select Yes to use extensible attributes to search for networks and specify the EAs options. For more information about extensible attributes, see Extensible Attributes in IPAM Workflows.
8. Click Next.
9. Click Submit.
Add Range Workflow

This workflow creates a new network range on the NIOS appliance that can be later assigned to vApps and other resources through vRealize Automation. In the Add range workflow, you can specify extensible attributes to assign to the newly-created range.

To add a range:

1. Log in to the vCenter Orchestrator client.
2. Choose Run mode.
3. On the Workflows tab, select the administrator entry -> Library -> IPAM.
4. Right-click the Add range workflow and choose Start workflow.
5. Complete the Connection step to establish the connection to the NIOS IPAM appliance: click the Connection to the IPAM server field. Expand Infoblox IPAM and select the IP address of the Infoblox NIOS Grid member. Click Select.
6. Click Next.
7. In the Range step, specify the network range parameters:
   — Start Address
   — End Address
   — Name of the range
   — Comments about the range
   — Disable for DHCP
   — Network address of range’s network
   — Network CIDR of range’s network
   — Network view to which the range belongs
8. Click Next.
9. In the Member step, specify if you want to assign an Infoblox Grid member to the range.
   — If you select Yes, specify the IP address or FQDN of the Infoblox Grid member and the member type.
10. Click Next.
11. (Optional) In the Extensible attributes step, specify the number of, and the values for, any extensible attributes that you want to assign to the network range object that will be created in the result of the workflow execution. For more information about extensible attributes, see Extensible Attributes in IPAM Workflows.
12. Click Next.
13. In the DHCP options step, select if you want to assign DHCP options to the network range.
   — If you select Yes, specify the following:
     • Domain name (DNS suffix)
     • DNS suffixes for search
     • IP addresses of the DNS servers
     • IP addresses of the routers
     • IP addresses of the NetBIOS name servers
14. Click Next.
15. Specify if restarting the DHCP service is needed. When you select Yes, the DHCP service will be restarted when it is required by NIOS configuration. For more information, see Appendix E, "Operations Requiring Service Restart".
16. Click Submit.
Remove Range Workflow

This workflow removes a NIOS network range or multiple ranges previously created with the Add range workflow.
You can specify either the start and end addresses of a particular range or extensible attributes to search for ranges to be removed.

To remove a range:

1. Log in to the vCenter Orchestrator client.
2. Choose Run mode.
3. On the Workflows tab, select the administrator entry -> Library -> IPAM.
4. Right-click the Remove range workflow and choose Start workflow.
5. Complete the Connection step to establish the connection to the NIOS IPAM appliance: click the Connection to the IPAM server field. Expand Infoblox IPAM and select the IP address of the Infoblox NIOS Grid member. Click Select.
6. Click Next.
7. In the Remove Criteria step, do one of the following:
   — Specify the start address and end address of the range, and, optionally, the network view where the range resides.
   — Select Yes to use extensible attributes to search for ranges and specify the EAs options. For more information about extensible attributes, see Extensible Attributes in IPAM Workflows.
8. Click Submit.
Restart IPAM Services Workflow

You can use the *Restart IPAM services* workflow to manually initiate on-demand IPAM services restart or to embed such restart into a custom-built workflow. For example, you may need to restart services after a batch of requests has been served.

In this workflow, you can specify restart options which include:

- The order in which Grid members are restarted (simultaneously or sequentially)
- The type of restart request (forced or if needed)
- Grid services to restart (all, DHCP, or DNS)
- Delayed time, in case of restart in sequential order
vRA Workflows

These workflows are called automatically by vRA while processing a Blueprint request. They are not intended to be run manually. The Infoblox IPAM Plug-In for VMware includes the following vRA workflows:

<table>
<thead>
<tr>
<th>Workflow Type</th>
<th>Description</th>
</tr>
</thead>
</table>
| Administration workflows | The administration workflows are used to create custom property groups and property definitions in vRA. You access the vRA administration workflows from `<admin> -> Library -> Infoblox -> vRA -> Administration`. These workflows include:  
  - Create/Update Property Definitions: Creates or updates property definitions that are used by the Infoblox IPAM Plug-In for the integration with vRA. See [Create/Update Property Definitions Workflow](#).  
  - Create Property Group: Creates an Infoblox-specific property group in vRealize Automation. See [Create/Update Property Definitions Workflow](#). |
| Configuration workflows | The configuration workflows are used to create/update/verify/remove vRA Infrastructure Administration hosts (IaaS) and vRA hosts in the Inventory tab of the vRealize Orchestrator client. You access the vRA configuration workflows from `<admin> -> Library -> Infoblox -> vRA -> Configuration`. These workflows include:  
  - Add an IaaS host wrapper: Adds an IaaS host to the vRO inventory. See [Add an IaaS Host Wrapper Workflow](#).  
  - Add a vRA host wrapper: Adds a vRA host to the vRO inventory. See [Add a vRA Host Wrapper Workflow](#).  
  - Update an IaaS host wrapper: Updates properties of the IaaS host instance. See [Update an IaaS Host Wrapper Workflow](#).  
  - Update a vRA host wrapper: Updates properties of the vRA host instance. See [Update a vRA Host Wrapper Workflow](#).  
  - Validate an IaaS host wrapper: Validates the connection to an IaaS host. See [Validate an IaaS/vRA Host Wrapper Workflow](#).  
  - Validate a vRA host wrapper: Validates the connection to a vRA host. See [Validate an IaaS/vRA Host Wrapper Workflow](#).  
  - Remove an IaaS host wrapper: Removes an IaaS host from the vRO inventory. See [Remove IaaS/vRA Host Wrapper Workflow](#).  
  - Remove a vRA host wrapper: Removes a vRA host from the vRO inventory. See [Remove IaaS/vRA Host Wrapper Workflow](#). |
| Installation workflows | These are workflows used during the deployment of the Infoblox IPAM Plug-In. You access these workflows from `<admin> -> Library -> Infoblox -> vRA -> Installation, Installation -> IP AM registration, and Installation -> vRO customization`. These workflows include:  
  - Setup Wizard: Performs basic Plug-In setup after the Plug-In is installed. See [Performing Basic Plug-In Setup](#).  
  - Register IPAM Endpoint: Calls the endpoint-configuration-service API to register the “Infoblox” endpoint type under the “IPAM” category in vRealize Automation. Once this endpoint type is registered, you can add IPAM endpoint instances in vRA.  
  - Deregister IPAM Endpoint: Removes the previously registered Infoblox IPAM type of endpoint in vRealize Automation.  
  - Install vRO customization wrapper: Installs the vRO customization which includes the customization of workflow stubs and vRO menu operation workflows.  
  - Uninstall vRO customization wrapper: Uninstalls the vRO customization which includes the customization of workflow stubs and vRO menu operation workflows. |
| vRA workflows for VM provisioning/deprovisioning | These workflows are called internally when vRA executes VM provisioning and deprovisioning requests. You access the vRA workflows for VM provisioning from <admin> → Library → Infoblox → vRA. These workflows include:

- **Allocate**: This workflow is called by vRealize Automation to allocate a block of IP addresses in NIOS during VM provisioning. In each allocation, there are multiple sub-allocations. Each sub-allocation is the allocation of IP addresses for a single NIC interface for the Virtual Machine. As part of the Allocate, the workflow returns the DHCP options along with the IP address.
- **Release**: This workflow is called by vRealize Automation when a VM is destroyed. It releases the IP addresses allocated to the resource in NIOS.
- **Create Endpoint Connection**: Creates an Infoblox IPAM connection. It tries to connect with the master endpoint and if it fails, it tries to connect with the failover endpoints.
- **Get Address Spaces**: This workflow is called by vRealize Automation to get the network views from NIOS.
- **Get IP Ranges**: This workflow is called by vRealize Automation to get a list of IP ranges (networks and ranges) from NIOS.
- **Create IP Ranges**: Creates a number of IP ranges within the same address space for on-demand routed network. This may include creating an address space as well.
- **Delete IP Ranges**: Deletes IP ranges for the previously created routed network from NIOS.
- **Update**: Updates MAC addresses and host names of the records in NIOS associated with the VM. It is triggered on the WFStubMachineProvisioned event from vRA.

| Helpers | These include various helper workflows called internally by the Plug-In during the execution of various tasks. |
Create/Update Property Definitions Workflow

Use this workflow to create or update the property definitions that are used by the Infoblox-specific property group. You can use this workflow to update EA definitions when the connection object API type is changed.

**Note:** The Create/Update Property Definitions workflow is a pre-requisite to the Create Property Group workflow. It should be run at least once prior to Create Property Group workflow to create property definitions.

1. Log in to the vRealize Orchestrator client.
2. Choose **Design** mode.
3. On the **Workflows** tab, select **IPAM -> vRA -> Administration -> Property Dictionary**.
4. Right-click **Create/Update Property Definitions** and choose **Start workflow**.
5. Specify the following parameters:
   - **vRA host**
     - **Visibility**: Select **All tenants**.
     - **Update existing property definitions**: Select **Yes**.
6. Click **Submit**.
Create Property Group Workflow

In addition to the “Infoblox-Default” property group created by the Setup Wizard workflow, you can create a custom Infoblox-specific property group by using the Create Property Group workflow. You can use a custom property group for VM provisioning. For the complete list of properties, see Appendix B, “Infoblox IPAM Properties”.

**Note:** Before you create a custom property group, execute the Create/Update Property Definitions workflow above.

1. Log in to the vRealize Orchestrator client.
2. Choose Design mode.
4. Right-click Create Property Group and choose Start workflow.
5. Specify the vRA host.
6. Click Next.
7. Specify the property group name, description, and visibility (select All tenants).
8. Click Next.
9. In the Common parameters step, do the following:
   — Specify the record type that you want this property group to create through a vRA request (host record, DNS record, or DHCP record) and the required details for the selected record types.
   — Specify if restarting the DHCP service is needed. If you select Yes, the DHCP service will be restarted when it is required by NIOS configuration. For more information, see Appendix E, “Operations Requiring Service Restart”.
10. Click Next.
11. In the Network interfaces step, select the desired number of virtual network interfaces and specify details for each of them.
12. In the **Custom hostnaming** step, specify the following:

- **Enable custom hostnaming**: If you select **Yes**, the Infoblox.IPAM.enableHostName property will be set to TRUE in the created property group and Infoblox Plug-In will update VM’s host name in NIOS when a VM is created. Otherwise, the records in NIOS will be created with the vRA default host name.
- **Automatically detect if custom hostname is set**: Specify if you want Infoblox Plug-In to always update VM’s host name in NIOS or only when a custom hostname was set for the VM instead of the vRA default. If you select **Yes**, then specify the next option.
- **Use properties specific for Custom Hostnaming Extension in vRA**: If you use Custom Hostname Extension for vRA, select **Yes**. If you want to use another third-party extension for custom hostnaming, select **No** and specify the properties manually in the next step.

13. If you selected **No** for **Use properties specific to Custom Hostnaming Extension for vRA**, select the number of conditions to detect VM name change and click **Next**. You can select up to three conditions.
14. Specify each condition as a name-value pair specific to the custom hostnaming extension that you use.

15. Click Submit.

For more information about properties specific to Custom Hostname Extension for vRA, see Appendix B, "Infoblox IPAM Properties".
Add an IaaS Host Wrapper Workflow

Use this workflow to add an IaaS host instance to the vRO Inventory. An IaaS host instance is required in the vRO inventory for executing workflows for creating build profiles and for commissioning and decommissioning vRA virtual machines.

1. Log in to the vRealize Orchestrator client.
2. Choose Design mode.
3. On the Workflows tab, select IPAM → vRA → Configuration.
4. Right-click the Add an IaaS host wrapper workflow and choose Start workflow.
5. Specify the following parameters:
   — Host name
   — Host address (in IP or FQDN format)
   — Automatically install SSL certificates (set to YES)
   — Connection timeout and Operation timeout (Infoblox recommends retaining the default values in each field)
   — Session mode (Shared Session)
   — Authentication user name and Authentication password
   — Domain for NTLM authentication (support for NT Lan Manager challenge-response authentication)
6. Click Submit.
Add a vRA Host Wrapper Workflow

Use this workflows to add a vRA host instance to the vRO Inventory. A vRA host instance is required in the vRO inventory for executing workflows for commissioning vRA virtual machines.

1. Log in to the vRealize Orchestrator client.
2. Choose Design mode.
3. On the Workflows tab, select IPAM → vRA → Configuration.
4. Right-click the Add a vRA host wrapper workflow and choose Start workflow.
5. Specify the following parameters:
   — Host name
   — Host address (in IP or FQDN format)
   — Tenant ("vsphere.local")
   — Automatically install SSL certificates (set to YES)
   — Connection timeout and Operation timeout (Infoblox recommends retaining the default values in each field)
   — Session Mode (Shared Session)
   — Authentication user name and Authentication password
6. Click Submit.
Update an IaaS Host Wrapper Workflow

Use this workflow to update an existing IaaS host instance.

1. Log in to the vRealize Orchestrator client.
2. Choose Design mode.
3. On the Workflows tab, select IPAM -> vRA -> Configuration.
4. Right-click the Update IaaS host wrapper workflow and choose Start workflow.
5. Specify the following parameters:
   — IaaS host instance to update
   — Host name
   — Host address (in IP or FQDN format)
   — Automatically install SSL certificates
   — Connection timeout and Operation timeout
   — Session Mode
   — Authentication user name and Authentication password
   — Domain for NTLM authentication (support for NT Lan Manager challenge-response authentication)
6. Click Submit.
Update a vRA Host Wrapper Workflow

Use this workflow to update an existent vRA host instance.

1. Log in to the vRealize Orchestrator client.
2. Choose Design mode.
4. Right-click the Update a vRA host wrapper workflow and choose Start workflow.
5. Specify the following parameters:
   — vCloud Automation Center host instance to update
   — Host name
   — Host address (in IP or FQDN format)
   — Tenant ("vsphere.local")
   — Automatically install SSL certificates
   — Connection timeout and Operation timeout
   — Session Mode
   — Authentication user name and Authentication password
6. Click Submit.
Validate an IaaS/vRA Host Wrapper Workflow

Use these workflows to validate connections to an IaaS or vRA host at any time.

1. Log in to the vRealize Orchestrator client.
2. Choose Design mode.
3. On the Workflows tab, select IPAM → vRA → Configuration.
4. Right-click the Validate a vRA host wrapper or Validate IaaS host wrapper workflow and choose Start workflow.
5. On the Common parameters page, select the required host instance.
6. Click Submit.
Remove IaaS/vRA Host Wrapper Workflow

Use these workflows to remove an IaaS or vRA host instance from the vRO Inventory.

1. Log in to the vRealize Orchestrator client.
2. Choose Design mode.
3. On the Workflows tab, select IPAM -> vRA -> Configuration.
4. Right-click the Remove vRA host wrapper or Remove IaaS host wrapper workflow and choose Start workflow.
5. On the Common parameters page, select the required host instance.
6. Click Submit.
Verifying Workflow Execution

You can verify successful workflow execution by viewing its status in the following locations:

- You can check recent events and history on the Recent Events tab in vRA.
- In vRA, in the Infrastructure -> Managed Machines tab, check to ensure the new virtual machine’s status is ON.
- In the Logs section in the vRealize Orchestrator workflow run;
- In the Logs tab on the vRealize Orchestrator configuration server;
- The audit log on the NIOS appliance. For more information, see Using the Audit Log in the Infoblox NIOS Documentation.
- You can check the new records created in NIOS by using the Data Management tab in the Infoblox Grid Manager Web UI.
Using Actions of Infoblox IPAM Plug-In for VMware

Actions are the building blocks of workflows. Actions of Infoblox IPAM Plug-In for VMware are Javascript segments that use the API exposed by the Infoblox IPAM Plug-In for VMware. You can use the Infoblox IPAM Plug-In for VMware actions to develop custom workflows.

The Infoblox IPAM for VMware Plug-In actions are located in the following modules in the vRO client:

- `com.infoblox.integrated.ipam` contains actions for integrating with vRA.
- `com.infoblox.ipam` contains actions for interacting with NIOS.
- `com.infoblox.ipam.util` contains helper actions that are used in IPAM workflows.
- `com.infoblox.ipam.vcac` contains actions for interacting with vRA.
- `com.infoblox.ipam.vcac.util` contains helper actions that are used in vCAC (vRA) workflows.
- `com.infoblox.ipam.vcaccafe` contains actions for interacting with the VCACCAFE host.

To access the Infoblox IPAM for VMware Plug-In actions:

1. Log in to the vRealize Orchestrator client.
2. Choose Design mode.
3. Click the Actions tab.
4. Click admin –> any of the action modules mentioned above. The list of Infoblox IPAM actions is shown in the tree.
5. Select an action.
6. Click the Scripting tab. This provides the list of input parameters comprising the selected action.

You can also access actions through the vRO API Explorer. For more information, refer to the following section, Using API of Infoblox IPAM Plug-In for VMware. For information about how to build workflows by using actions, refer to the vRealize Orchestrator documentation.
Using API of Infoblox IPAM Plug-In for VMware

The Infoblox IPAM Plug-In for VMware exposes a Javascript API that enables you to build actions and workflows.

To locate the Infoblox IPAM API objects:

1. In the vRealize Orchestrator client, click Tools → API Explorer.

2. Use the term “infoblox” on the API Search tab to locate the Infoblox IPAM Plug-In for VMware API objects.

3. In the API Explorer tree, select Infoblox IPAM.
Note: For information about the NIOS Cloud API, see the chapter *Deploying Cloud Network Automation* in the *Infoblox NIOS Documentation*. 

---

Copyright ©2019, Infoblox, Inc. All right reserved.
Integrating Infoblox IPAM Plug-In for VMware with Microsoft DNS and DHCP Servers

When you use a Microsoft server for DHCP and DNS services, you can synchronize the Microsoft DHCP and DNS server records with Infoblox NIOS. You can do so by setting Infoblox custom properties in the vRealize Automation blueprint used for VM requests.

Infoblox NIOS supports synchronization of fixed addresses (or reservations), A records, and PTR records in Microsoft DHCP and DNS servers. This requires the Microsoft license installed in NIOS. For more information about the integration of Microsoft servers with NIOS, refer to Part 6 Managing Microsoft Windows Servers in the Infoblox NIOS Documentation.

Synchronization with Microsoft servers is performed at the DHCP range level and not at the network level. Therefore, you need to add a NIOS DHCP range in which the records will be created. For more information about the difference in DHCP data representation between NIOS and Microsoft servers, refer to Synchronizing DHCP Data from Microsoft Servers in the Infoblox NIOS Documentation.

The following sections describe typical use cases involving Microsoft Windows servers:

- **Use Case: IP Address Allocation from NIOS with DNS Registration in Microsoft DNS Server.**
- **Use Case: IP Address Allocation from NIOS with DHCP Registration in Microsoft DHCP Server.**
Use Case: IP Address Allocation from NIOS with DNS Registration in Microsoft DNS Server

To provision a VM with address and PTR records in NIOS and synchronize them with a Microsoft DNS server, perform the following sample steps:

1. Configure your NIOS with the Grid and MS Management licenses.
2. In NIOS, add a Microsoft DNS server.
3. Verify that synchronization works correctly: in NIOS, go to Grid -> Microsoft Servers -> Servers tab. The synchronization column should display the Running status.
4. In NIOS, add a network with the Microsoft DNS server as a member.
5. In NIOS, add an appropriate DHCP range with the Microsoft server as a member.
6. Verify that the above network is synchronized in the Microsoft DNS server.
7. In NIOS, add a zone with the Microsoft DNS server as the Primary.
8. In NIOS, add a reverse mapping zone for the network with the Microsoft DNS server as the Primary.
9. Verify that both zones are synchronized in the Microsoft DNS server by using the server management console.
10. If necessary, edit the Infoblox IPAM properties group.
11. In vRA, associate the created property group with the appropriate blueprint. For more information, see Designing a Blueprint.
12. In the network profile used in your blueprint, make sure that the DHCP range of the member Microsoft server is selected as the network range. For more information, see Creating an External Network Profile.
13. In the property group, modify the values of the Infoblox IPAM properties as follows:
   — Infoblox.IPAM.createAddressAndPtrRecords: TRUE
   — Infoblox.IPAM.createAddressRecord: FALSE
   — Infoblox.IPAM.createFixedAddress: FALSE
   — Infoblox.IPAM.createHostRecord: FALSE
   — Infoblox.IPAM.createReservation: FALSE
   — Infoblox.IPAM.Networkx.dnsView: default
   — Infoblox.IPAM.Networkx.enableDHCP: FALSE
   — Infoblox.IPAM.Networkx.enableDns: TRUE
14. In vRA Catalog, request a VM with the above properties.
15. In vRO, verify that the Allocate workflow completes successfully.
16. Check the result of the VM provisioning and DNS registration:
   — In NIOS, the address and PTR records are added.
   — In the Microsoft DNS server, the address and PTR records are synchronized.
   — In vCenter, the VM is deployed and powered on.
Use Case: IP Address Allocation from NIOS with DHCP Registration in Microsoft DHCP Server

To provision a VM with a fixed address in NIOS and synchronize it with a Microsoft DHCP server, you need to specify the following properties in the VM request:

- Infoblox.IPAM.createFixedAddress
- Infoblox.IPAM.Network0.enableDhcp
- Infoblox.IPAM.NetworkX.msDHCPServer

As an example, do the following:

1. Configure your NIOS with the Grid and MS Management licenses.
2. In NIOS, add a network with a Microsoft DHCP server as a member.
3. In NIOS, add an appropriate DHCP range with the Microsoft DHCP server as a member.
4. Verify that the above network is synchronized in the Microsoft DHCP server by using the server management console.
5. If necessary, edit the Infoblox IPAM properties group.
6. In vRA, associate the created property group with the appropriate blueprint. For more information, see Designing a Blueprint.
7. In the network profile used in your blueprint, make sure that the DHCP range of the member Microsoft server is selected as the network range. For more information, see Creating an External Network Profile.
8. In the property group, modify the values of the Infoblox IPAM properties as follows:
    - Infoblox.IPAM.Network0.dnsView: default
    - Infoblox.IPAM.createHostRecord: FALSE
    - Infoblox.IPAM.createAddressRecord: FALSE
    - Infoblox.IPAM.createAddressAndPtrRecords: FALSE
    - Infoblox.IPAM.createFixedAddress: TRUE
    - Infoblox.IPAM.createReservation: FALSE
    - Infoblox.IPAM.NetworkX.enableDhcp: TRUE
    - Infoblox.IPAM.NetworkX.enableDns: FALSE
    - Infoblox.IPAM.NetworkX.msDHCPServer: <address of the Microsoft DHCP server to be associated with the fixed address>
9. In vRA Catalog, request a VM with the above properties.
10. In vRO, verify that the Allocate workflow completes successfully.
11. Check the result of the VM provisioning and DHCP registration:
    - In NIOS, the fixed address is added.
    - In the Microsoft DHCP server, the fixed address is synchronized.
    - In vCenter, the VM is deployed and powered on.
Integrating Infoblox IPAM Plug-In for VMware with NSX

You can integrate the Infoblox IPAM Plug-In for VMware with VMware’s NSX platform and use it in the following tasks:

- Provisioning NSX Load Balancers with Registration in NIOS.
- Provisioning VMs in NSX Routed Networks Registered in NIOS.
- Provisioning VMs in NAT Networks Registered in NIOS.

For help in setting up your NSX environment, see the link to the NSX public documentation in the section Resources.
Provisioning NSX Load Balancers with Registration in NIOS

If you load balance your application traffic by using the VMware NSX platform with vRealize Automation, you can provision NSX load balancers, and the NSX Edge will get IP addresses for external and internal interfaces from NIOS. The internal interface IP is the router DHCP option. The external interface is assigned from NIOS.

This section explains how to perform a sample NSX provisioning use case.

Prerequisites:

- You have deployed the Infoblox IPAM Plug-In for VMware as described in Deploying Infoblox IPAM Plug-In for VMware.
- You have the VMware NSX platform integrated with your VMware environment.
- Everything is configured correctly with respect to NSX. This includes:
  — A pre-configured transport zone for NSX. The transport zone is a logical switch span across which the NSX is extended, for example, a datacenter or a set of clusters.
  — Logical switches.
- You have pre-configured an IPv4 network on NIOS and set up IPv4 DHCP options for the network. The DHCP options should include the router IP address. This is the virtual IP that will be assigned to the load balancer through the network profile in vRA.

To provision NSX load balancers with registration in NIOS, do the following:

- Set up the network profile to use with NSX, as described in Setting Up a Network Profile.
- Make an IP reservation in the DHCP range, as described in Making a Reservation of the IP Address.
- Create a blueprint, as described in Creating a Blueprint for the NSX Load Balancer.
- Create an NSX provisioning service in vRA Catalog, as described in Creating a VM Request Service in vRealize Catalog.
- Provision NSX VMs, as described in Provisioning NSX Virtual Machines.
- Scale the NSX deployment out and in, as described in Scaling the NSX Deployment.
Setting Up a Network Profile

To set up a network profile:

1. In vRealize Automation, go to Infrastructure -- Reservations -- Network Profiles -- New -- External.
2. On the General tab, specify the necessary details. For IPAM endpoint, select the pre-configured NIOS endpoint.
3. On the Network Ranges tab, select the address space (network view on NIOS) and the network range. The router IP address (i.e. load balancer's virtual IP) is obtained from the DHCP options of the range.
4. Click Apply, and then OK.
Making a Reservation of the IP Address

To make a reservation:

1. In vRealize Automation, go to Infrastructure --> Reservations --> New --> vSphere.
2. On the General tab, complete the necessary fields.
3. On the Resources tab, complete the necessary fields.
4. On the Network tab, select the check box for the web switch and select the previously configured NSX network profile. This reserves the IP address of the Load Balancer.
5. In the Advanced Settings for the network, select the pre-configured transport zone.
6. Click OK.
Creating a Blueprint for the NSX Load Balancer

To create a blueprint:

1. In vRealize Automation, click **Design --> Blueprints**.
2. Click **New**.
3. On the **General** tab, specify the necessary information.
4. On the **NSX Settings** tab, specify the transport zone.
5. Click **OK**.
6. In the **Categories** pane, select **Machine Types** and drag-and-drop the **vSphere Machine** component onto the design canvas.
7. On the **General** tab for the machine, complete the necessary information, including the maximum number of instances of the NSX machines.
8. On the **Build Information** tab, select to clone the machines and specify the necessary information.
9. Click **Save**.
10. In the **Categories** pane, select **Network & Security** and drag-and-drop the **Existing Network** component onto the design canvas.
11. On the **General** tab for the network, click the three dots button for **Existing network**, select the NSX network profile, and click **OK**.
12. Click the vSphere Machine component in the design canvas.
13. On the **Network** tab, click **New**.
14. Select the NSX network added earlier and click **OK**.
15. From **Categories --> Network & Security**, select **On-Demand Load Balancer** and drag-and-drop it onto the design canvas.
16. On the **General** tab for the load balancer, specify the necessary information, including the above vSphere machine in the **Member** field, the predefined NSX items in **Member network** and **VIP network**, and the required protocols in **Virtual servers**.

**Note:** Leave the IP address blank as it is taken from NIOS when the machine is provisioned.

17. Click the vSphere Machine component in the design canvas.
18. On the **Properties** tab, click **Add** to add a property group.
19. Select the Infoblox property group, for example, **Infoblox-Default**, and click **OK**.
20. Click **Finish**.
   The created blueprint appears in the list of blueprints.
21. Select the created blueprint and click **Publish**.
   The new blueprint is published in vRealize Automation.

Once the blueprint is published, create an NSX provisioning service in vRA Catalog. See *Creating a VM Request Service in vRealize Catalog*. After that, you can provision NSX machines and scale out the NSX deployment.
Provisioning NSX Virtual Machines

To provision NSX virtual machines:

1. In vRealize Automation, go to the Catalog tab.
2. Click Request for the NSX service.
3. In the NSX deployment details, specify general details. In this sample case, set the number of deployments to 1.
4. Select the vSphere machine.
5. In the General tab, specify the required details. In this sample case, set the number of the web machine instances to 2 in the Instances field.
6. Click Submit, and then click OK.

Now if you go to the Requests tab in vRA, you can see the details of the NSX machines provisioning execution.

In vRealize Orchestrator, you can notice that three instances of the Allocate workflow are executed, which corresponds to the NSX load balancer and the two web machines. The IP addresses allocation took place through NIOS.

In NIOS Grid Manager, go to Data Management -> IPAM -> network used for IP address provisioning and notice that the IP addresses are allocated to the corresponding machines. On the DNS -> Zones tab in the Grid Manager, notice that the corresponding DNS records are created.

In vSphere Client, you can check that the load balancer machine and the two web machines are spun and have the IP addresses allocated.
Scaling the NSX Deployment

When the load on the VMs increases, you can scale out the NSX deployment to provision more VMs that will load balance the traffic.

To scale out the NSX deployment:

1. In vRealize Automation, go to Items -> Deployments.
2. Select the NSX load balancer.
3. In the Actions pane, click Scale Out.
4. In the Properties tab, select Machines.
5. In the New Total column, set the number of machines to 3.
6. Click Save.

Now in vRealize Orchestrator, notice that a third Allocate workflow is executed. In NIOS Grid Manager, an IP address is allocated to the third machine. In vSphere Client, the machine is powered on.

When the machine is no longer needed, you can scale it in.

To scale in the NSX deployment:

1. In vRealize Automation, go to Items -> Deployments.
2. Select the NSX load balancer.
3. In the Actions pane, click Scale In.
4. In the Properties tab, select Machines.
5. In the New Total column, set the number of machines back to 2.
6. Click Save.

Notice in vRealize Orchestrator that the Release workflow is executed. In NIOS Grid Manager, notice that the IP address of the VM was reclaimed. In the NSX deployment in vRA, notice that the VM is destroyed.

When you destroy the entire NSX deployment item as described in De-provisioning a VM, you can notice in vRealize Orchestrator that the Release workflows are executed, which corresponds to the NSX load balancer and the two VMs. In NIOS Grid Manager, the IP addresses are released back to the pool.
Provisioning VMs in NSX Routed Networks Registered in NIOS

This section explains how to perform a sample NSX routed network use case.

Prerequisites:

- You have the VMware NSX platform integrated with your VMware environment, including vSphere Web Client.
- Everything is configured correctly with respect to NSX. This includes:
  - A pre-configured transport zone for NSX. The transport zone is a logical switch span across which the NSX is extended, for example, a datacenter or a set of clusters.
  - Logical switches.
- You have pre-configured an IPv4 network container on NIOS and set up Domain Name in IPv4 DHCP options of the container. You can also set up other DHCP options (DNS servers, netbios-name-servers, domain-search) for the network container. These DHCP options will be inherited by the on-demand network created in the container, except the router IP address. The latter will be set to the first available IP address in the created network and will be used as an internal interface by the distributed logical router.
- You have created the “VMware On-Demand Network” extensible attribute of string type in NIOS. This EA will be automatically assigned to any on-demand created network at the Create IP Ranges workflow execution. This allows filtering out on-demand networks from other available NIOS networks when creating an external network profile. For information on how to create EAs, see About Extensible Attributes in the Infoblox NIOS Documentation.
- You have deployed the Infoblox IPAM Plug-In for VMware as described in Deploying Infoblox IPAM Plug-In for VMware. This must include the following:
  - A configured external network profile that points to the pre-configured IPv4 network in NIOS.
  - A reservation with the above-mentioned external network profile selected for the distributed logical router in Infrastructure > Reservations -> your Infoblox reservation -> Network Advanced Settings -> Distributed logical router.

To provision a VM in an NSX routed network with registration in NIOS, do the following:

1. Set up an on-demand routed network profile for the VM blueprint, as described in Creating a Routed Network Profile.
2. Design and publish a blueprint with the routed network profile, as described in Designing a Blueprint.
3. Associate the blueprint with the appropriate VM request service, as described in Creating a VM Request Service in vRealize Catalog.
   After that, you are ready to provision VMs in the NAT network.
4. Request a VM in the routed network, as described in the next section, Provisioning a VM in NSX Routed Network.
Provisioning a VM in NSX Routed Network

Submit a provisioning request for a VM in the NSX routed network, as described in Provisioning and De-provisioning VMs with Registration in NIOS.

Now if you go to the Requests tab in vRA, you can see the details of the NSX machines provisioning execution.

In vRealize Orchestrator, you can notice that an instance of the Create IP Ranges workflow is executed.

In NIOS, a new on-demand network is created in the specified network container. First available IP address in the network is assigned to the router. The IP address of the corresponding VM is allocated in the on-demand created network.

In vSphere Client, you can check that the new VM is spun.
Destroying a VM in NSX Routed Network

When you destroy a VM in an NSX routed network, as described in *De-provisioning a VM*, it removes the reserved IP address and the network from NIOS. The *Delete IP Ranges* workflow is used to delete the on-demand created network on NIOS.
Provisioning VMs in NAT Networks Registered in NIOS

You can use the Infoblox IPAM Plug-In for VMware to provision VMs in NAT networks. The Plug-In supports One-to-One and One-to-Many NAT networks which can be used with load balancers as well.

When a NAT network profile is configured with the Infoblox IPAM Plug-In for VMware, an internal set of IP addresses defined with one or more ranges are created in NIOS for every instance of the NAT network. These IP ranges are used to allocate IP addresses for machines assigned to the NAT network in the same deployment. Because there cannot be duplicate IP addresses defined within a single network view (i.e. address space in the VMware terminology), a new network view is created in NIOS, if required, for an instance of the NAT network. When a NAT network is destroyed, its ranges are destroyed in NIOS, as well as the corresponding network view, if it contains no other networks.

Note that when the internal IP address allocation occurs in NIOS, the created records are always of the Reservation type. This section explains how to perform a sample NAT network use case.

Prerequisites:

- You have the VMware NSX platform integrated with your VMware environment.
- Everything is configured correctly with respect to NSX. This includes:
  - A pre-configured transport zone. The transport zone is a logical switch span across which the NSX is extended, for example, a datacenter or a set of clusters.
  - Logical switches.
- You have pre-configured an IPv4 network on NIOS and set up the following DHCP options for it, as shown in the figure below:

<table>
<thead>
<tr>
<th>NIOS DHCP Option Name</th>
<th>vRA DNS/WINS Option Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routers</td>
<td>Gateway</td>
</tr>
<tr>
<td>Domain Name</td>
<td>DNX suffix</td>
</tr>
<tr>
<td>DNS Servers</td>
<td>Primary DNS</td>
</tr>
<tr>
<td></td>
<td>Secondary DNS</td>
</tr>
<tr>
<td>netbios-name-servers</td>
<td>Preferred WINS</td>
</tr>
<tr>
<td>(44)</td>
<td>Alternate WINS</td>
</tr>
<tr>
<td>domain-search</td>
<td>DNS search suffixes</td>
</tr>
<tr>
<td>(119)</td>
<td></td>
</tr>
</tbody>
</table>

You have created the following extensible attributes of string type in NIOS:
- VMware On-Demand Network: This EA is automatically assigned to any on-demand created network at the Create IP Ranges
workflow execution. This allows filtering out on-demand networks from other available NIOS networks when creating an external network profile.

— VMware Blueprint Request ID: This EA is automatically assigned to any on-demand created IP range created for the same Blueprint request. This identifies a request for the whole blueprint. This EA is used for error handling.

— VMware External Range ID: This EA is used for retrieving DHCP options from the external IP range if they are not specified in the NAT network profile. The value of this attribute points to the IP range used for the allocation of external IP address for NSX Edge in this deployment.

— VMware Request ID: This EA is used for error handling. It identifies a request to create on-demand ranges.

— VMware Network Profile ID: This EA identifies the NAT or routed network profile that is used to create on-demand ranges.

— VMware External Network Profile ID: This EA identifies NAT ranges created for the specific external network profile.

For information on how to create EAs, see About Extensible Attributes in the Infoblox NIOS Documentation.

You have deployed the Infoblox IPAM Plug-In for VMware as described in Deploying Infoblox IPAM Plug-In for VMware. This must include the following:

— A configured external network profile that points to the pre-configured IPv4 network in NIOS.

— A reservation with the above-mentioned external network profile selected for the distributed logical router in Infrastructure -> Reservations -> your Infoblox reservation -> Network Advanced Settings -> Distributed logical router.

To provision a VM in a NAT network with registration in NIOS, do the following:

1. Set up a NAT network profile for the VM blueprint, as described in Creating a NAT Network Profile.
2. Design and publish a blueprint to be used with the NAT network request, as described in Designing a Blueprint.
3. Associate the blueprint with the appropriate VM request service, as described in Creating a VM Request Service in vRealize Catalog.

   After that, you are ready to provision VMs in the NAT network.

4. Request a VM in the NAT network, as described in the next section, Provisioning a VM in NAT Network.
Provisioning a VM in NAT Network

This section describes generic steps for both One-to-One and One-to-Many NAT network use cases and highlights the differences.

Submit a provisioning request for a VM in the NAT network, as described in Provisioning and De-provisioning VMs with Registration in NIOS.

Now if you go to the Requests tab in vRA and view details of the request, you can see the details of the VMs provisioning execution.

In vRealize Orchestrator, you can notice that an instance of the Create IP Ranges workflow is executed. This created the ranges that you defined in the NAT network profile. In the workflow execution log, under “Create IP range result”, you can notice that a new on-demand NAT network is created on NIOS in an existing or newly-generated on-demand network view. The network view appears as “AddressSpaceId” in the log and has the “vRA-” prefix, followed by an auto-generated ID. You can locate the newly-generated network view in Infoblox Grid Manager by going to Data Management and expanding the network views drop-down list in the top left corner.

Note: Do not use on-demand network views for other tasks. e.g. creating networks etc., as they are created and deleted automatically.

In One-to-Many NAT case, the IP address allocation happens in the following order:

1. An external IP address is allocated to the NSX Edge. In vRO, you can notice the corresponding instance of the Allocate workflow. In the corresponding network on NIOS, you can see that the IP address is allocated with the IPv4 Reservation record type.
2. An internal IP address is allocated to the VM. In vRO, you can notice the second instance of the Allocate workflow.

In One-to-One NAT case, the IP address allocation happens in the following order:

1. An external IP address is allocated to the NSX Edge. In vRO, you can notice the corresponding instance of the Allocate workflow. In the corresponding network on NIOS, you can see that the IP address is allocated with the IPv4 Reservation record type.
2. An external IP address is allocated to the VM. In vRO, you can notice the second instance of the Allocate workflow.
3. An internal IP address is allocated to the VM. In vRO, you can notice the third instance of the Allocate workflow.

In vSphere Client, you can see that the NSX Edge and the new VM are provisioned, with the external and internal IP addresses allocated. In the One-to-One NAT case, an update of the host record is performed for the VM’s external IP address. To this end, the Update workflow of the Infoblox IPAM Plug-In for VMware is used. It updates the MAC address and hostname in the host record or another type of record indicated in the request properties.
Locating Provisioned VM on NIOS

To locate the provisioned VM through Grid Manager:

1. In vRealize Orchestrator, go to the Get IP Ranges workflow log and find the generated network view ID by the "AddressSpaceId" log entry.
2. In Grid Manager, go to Data Management.
3. In the network views drop-down list, select the required view.
4. In IPAM tab -> List tab, locate the VM in the table by the name or IP address.
Destroying a VM in NAT Network

When you destroy a VM in a NAT network, as described in De-provisioning a VM, it removes the reserved IP address and the NAT network from NIOS. Instances of the Release workflow of the Infoblox IPAM Plug-In for VMware deallocate the IP addresses of the VM and NSX Edge in NIOS. After that, the Delete IP Ranges workflow is used to delete the created NAT network and the network view, if not used by other deployments, from NIOS.
Upgrading Infoblox IPAM Plug-In for VMware

This section explains how to upgrade Infoblox IPAM Plug-In for VMware in vRealize Orchestrator 7.1.

To upgrade Infoblox IPAM Plug-In for VMware:

1. Log in to the vRealize Orchestrator Control Center.
2. Click Plug-Ins --> Manage Plug-Ins.
3. Deselect the Infoblox IPAM Plug-in check box and click Save changes.
4. On the Startup Options page, click Restart and wait until the current status becomes “RUNNING”.
5. Click Manage Plug-Ins.
6. In the Manage Plug-Ins page, click Browse.
7. In the file upload dialog, select the .dar file (o11nplugin-ipam.dar) for the plug-in version 4.4.0, and click Open.
8. Click Install, and then click Install again to confirm. The Infoblox IPAM Plug-In 4.4.0 overwrites the existing plug-in version.
9. If the Infoblox IPAM check box is not selected in the Enable plug-in column, select it and click Save Changes.
10. On the Startup Options page, click Restart and wait until the current status becomes “RUNNING”.
Uninstalling Infoblox IPAM Plug-In for VMware from vRealize Orchestrator

You can manually remove the Infoblox IPAM Plug-In for VMware from vRealize Orchestrator. The following sections describe the procedures for Plug-In uninstallation on Windows and Linux.
Uninstalling Infoblox IPAM Plug-In for VMware on Windows

To remove the Infoblox IPAM Plug-In for VMware from vRealize Orchestrator on Windows:

1. Log in to the vRealize Orchestrator Control Center web page.
2. Click Plug-Ins -> Manage Plug-Ins.
3. Deselect the Infoblox IPAM Plug-in check box and click Save changes.
4. Go back to the vRealize Orchestrator Control Center page.
5. Click Certificates.
6. In the certificates list, click Delete for those which common name is "www.infoblox.com".
7. Open the Windows Services list and stop the following services:
   - VMware vRealize Orchestrator Configuration
   - VMware vRealize Orchestrator Server
8. Navigate to the installation directory of the vRealize Orchestrator server. The default path is:
   `C:\Program Files (x86)\VMware\vCAC\Server\`
9. Remove the following files and directories from the vRO installation directory:
   - Infoblox_IPAM_Plugin.xml
   - o11nplugin-ipam.dar
   - o11nplugin-ipam-config.war
   - o11nplugin-ipam-config directory
10. In the installation directory of the vRealize Orchestrator server, open the file _VSOPPluginInstallationVersion.xml for editing.
11. Remove the Infoblox IPAM Plug-In for VMware version data from the file by deleting all the lines that start with <entry key="Infoblox IPAM"> or <entry key="InfobloxIPAM">.
12. Open the Windows Services list and start the following services:
    - VMware vRealize Orchestrator Configuration
    - VMware vRealize Orchestrator Server
13. Log in to the vRealize Orchestrator client.
14. Select either Administer or Design mode.
15. Click the Packages tab.
16. Delete the vRA and IPAM packages of the Plug-in in the following order:
    a. Right-click com.infoblox.integrated.ipam and select Delete element with content.
    b. In the Delete confirmation window, click Keep shared.
    c. Repeat steps a and b for com.infoblox.ipam.
17. Log in to the vRealize Orchestrator Control Center.
18. Click **Startup Options** → **Restart**.
Uninstalling Infoblox IPAM Plug-In for VMware on Linux

To uninstall the Infoblox IPAM Plug-In for VMware from vRealize Orchestrator on Linux:

1. Log in to the vRealize Orchestrator Control Center.
2. Click Plug-ins -> Manage Plug-ins.
3. Deselect the Infoblox IPAM Plug-in check box and click Save changes.
4. Go back to the vRealize Orchestrator Control Center page.
5. Click Certificates.
6. In the certificates list, click Delete for those which common name is “www.infoblox.com”.
7. On the vRealize Orchestrator Linux appliance, shut down the vRO server and the vRO configuration service by using the following commands:
   ```
   sudo /etc/init.d/vco-server stop
   sudo /etc/init.d/vco-configurator stop
   ```
8. Navigate to the vRO server installation directory by using the following commands on the vRO Linux appliance:
   ```
   cd /var/lib/vco
   ```
9. Remove the following files and directories from the vRO installation directory by using the following commands:
   ```
   rm ./app-server/plugins/o11nplugin-ipam.dar
   ```
10. In the installation directory of the vRealize Orchestrator server, open the file by entering the following:
    ```
    vi ./app-server/conf/plugins/_VSOPluginInstallationVersion.xml
    ```
11. Remove the Infoblox IPAM Plug-In for VMware version data from the file by deleting all the lines that start with `<entry key="Infoblox IPAM">` or `<entry key="InfobloxIPAM">`. To do so, press `dd`, then press `Shift+q`, and then enter `wq` to save your changes.

   **Note:** The “Infoblox IPAM” entry may not be available in the file _VSOPluginInstallationVersion.xml_. If you cannot find it, follow the steps described below. In this case, there is no guarantee that the Plug-In will be uninstalled correctly.

12. On the vRealize Orchestrator Linux appliance, start the vRO server and the vRO configuration service by using the following commands:
    ```
    sudo /etc/init.d/vco-server start
    sudo /etc/init.d/vco-configurator start
    ```
13. Log in to the vRealize Orchestrator client.
14. Select either Administer or Design mode.
15. Click the Packages tab.
16. Delete the vRA and basic IPAM packages of the Plug-in in the following order:
    a. Right-click com.infoblox.integrated.ipam and select Delete element with content.
    b. In the Delete confirmation window, click Keep shared.
    c. Repeat steps a and b for com.infoblox.ipam.
17. Log in to the vRealize Orchestrator Control Center web page.
18. Click **Startup Options** → **Restart**.
Best Practices for Infoblox IPAM Plug-In for VMware

Organizations can use VMware's vRealize Automation to provision and de-provision new services based on virtual machines. vRealize Orchestrator is the workflow engine that is used by vRA to automate this process. The organization may execute the provisioning process using an existing vRealize Orchestrator interface, or a third party portal or customized provisioning portal. The interface used for the process is generic to the operation of the Infoblox IPAM Plug-In for VMware.

Best practices for using the Infoblox IPAM Plug-In for VMware include the following:

- Ensure that you can connect to the desired NIOS appliance from vRealize Orchestrator.
- Define an admin account on the NIOS appliance, the name of which corresponds to the vRealize Orchestrator account performing plug-in operations. This helps ensure that related event logs are directed to the right administrator.
- Avoid using the NIOS superuser account.
- Ensure that the desired extensible attributes are defined on the NIOS system with which the Infoblox IPAM Plug-In for VMware is connected. For more information, see Deploying Infoblox IPAM Plug-In for VMware.
- When production requires a new VM in a particular network or range, this DHCP network or range must be already defined in NIOS.
- The DHCP network or range also should be exclusively for use by the vRealize Orchestrator and not be used to define IP configurations for other networks or devices.
- When configuring individual workflows for operation, ensure that all required values are accurate. If any single value is incorrect, the workflow does not execute properly.
- Ensure that each workflow call for creating a VM must have the corresponding workflow call that destroys that VM. Otherwise, the IPAM information could be out of synchronization between the NIOS or vNIOS appliance and vSphere.
- Deploy the Cloud Network Automation license and use the Cloud API to provide improved visibility on VM IP address and DNS record utilization.
- Consider deploying Cloud Platform Appliances to improved API scalability and provide local survivability for large scale single site or multi-site data center deployments.
- Infoblox recommends you to use the Create Property Group workflow to create a custom property group required for your configuration. It can help avoid problems with irrelevant settings in the Infoblox property group. For more information, see Create Property Group Workflow.
- When the number of networks and ranges in NIOS is very big (more than 2000-3000), the “Get IP Ranges” workflow may not fit into 30 seconds vRA timeout (it also depends on the performance of your environment). As a result, when you create a new external network profile in vRA and click Add to select network ranges, it spins for a while and returns nothing in the “Select Network Range” window. Therefore, always specify an address space (network view) while creating a new network profile. This can help you to narrow down the number of networks and ranges to be retrieved from NIOS and fit into 30 seconds vRA timeout.
Resources

Go to the following locations on the Web to obtain the various plug-ins, packages, and executables mentioned in this guide and their related documentation:

- Infoblox IPAM Plug-In for VMware – You download the Infoblox IPAM Plug-In for VMware ZIP file and all relevant documents from the Infoblox Support web site at http://support.infoblox.com. The Infoblox IPAM Plug-In for VMware is delivered as a Zip archive file containing the VMware-compatible .DAR file. Consult the README file in the Zip archive for full information on the files in the download.
Reference

This section provides reference information in the following appendices:

- Appendix A Glossary of Terms
- Appendix B Infoblox IPAM Properties
- Appendix C Infoblox Endpoint Properties
- Appendix D Record Properties for VM Requests
- Appendix E Operations Requiring Service Restart
## Appendix A Glossary of Terms

The following table provides descriptions of some key terminology used in the Infoblox products. Some terms, such as Grids and high availability, are used in different ways by other networking product vendors. The alphabetically arranged table can help you understand the terms and concepts as Infoblox uses them and as they are used in this guide.

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CIDR (Classless Inter-Domain Routing) Notation</strong></td>
<td>A compact specification of an IPv4 or IPv6 address and its associated routing prefix. For example, the CIDR notation of 192.168.100.1/24 represents the IPv4 address of 192.168.100.1 and its routing prefix of 192.168.100.0, or its subnet mask of 255.255.255.0. The CIDR notation of 2001:db8::/48 represents the IPv6 addresses from 2001:db8:0:0:0 to 2001:db8:0:ffff:ffff:ffff:ffff.</td>
</tr>
<tr>
<td><strong>DHCP (Dynamic Host Configuration Protocol)</strong></td>
<td>A configuration protocol that provides address assignments to network devices within a network. It keeps track of network configuration for each network device.</td>
</tr>
<tr>
<td><strong>DHCP Template</strong></td>
<td>A set of predefined properties that you use to create IPv4 and IPv6 DHCP objects, such as networks and DHCP ranges, on the Infoblox appliance.</td>
</tr>
<tr>
<td><strong>DNS (Domain Name System)</strong></td>
<td>A hierarchical naming system that translates domain names of any network devices into IP addresses for the purpose of locating and addressing these devices worldwide.</td>
</tr>
<tr>
<td><strong>DNS View</strong></td>
<td>On Infoblox appliances, a DNS view provides the ability to serve one version of DNS data to one set of clients and another version to another set of clients. With DNS views, the Infoblox appliance can provide a different answer to the same DNS query, depending on the source and match destinations of the query.</td>
</tr>
<tr>
<td><strong>Extensible Attribute</strong></td>
<td>Metadata you define to capture additional information about an object managed by the Infoblox NIOS appliance. You can use predefined attributes or create your own. You can also specify required attributes and restrict the values that users can enter for each attribute.</td>
</tr>
<tr>
<td><strong>Fixed Address</strong></td>
<td>A fixed address is a specific IP address that a DHCP server assigns when a lease request comes from a particular MAC address of the client.</td>
</tr>
<tr>
<td><strong>FQDN (fully qualified domain name)</strong></td>
<td>A complete domain name that specifies its exact location in the hierarchy of the DNS. It specifies all the domain levels, including the top-level domain and the root domain.</td>
</tr>
<tr>
<td><strong>Grid™ Technology</strong></td>
<td>Infoblox’s unique and patented high availability Grid technology ensures network reliability. The Infoblox Grid provides resilient network services, failover, recovery, and seamless maintenance for an Infoblox deployment inside a single building, across a networked campus, or between remote locations. The Infoblox Grid establishes a distributed relationship between individual or paired appliances to remove single points of failure and other operational risks inherent in legacy DNS, DHCP, and IP address management infrastructure.</td>
</tr>
<tr>
<td><strong>Grid Manager</strong></td>
<td>The NIOS web interface that provides access to your Grid for performing IPAM, DNS, and DHCP management and other administration tasks.</td>
</tr>
<tr>
<td><strong>Grid Master</strong></td>
<td>The Grid member in an Infoblox Grid that maintains the NIOS database that is distributed among all members of the Grid. You connect to the Grid Master to configure and monitor the entire Grid.</td>
</tr>
<tr>
<td><strong>Grid Member</strong></td>
<td>Any single Infoblox NIOS appliance or HA (high availability) pair that belongs to a Grid. Each member can use the data and services of the Grid. You can also modify settings so that a Grid member can use unique data and member-specific services.</td>
</tr>
<tr>
<td><strong>Host Record</strong></td>
<td>On Infoblox appliances, host records provide a unique approach that enables you to manage multiple DNS records and DHCP and IPAM data collectively, as one object on the appliance.</td>
</tr>
<tr>
<td><strong>IPAM (IP Address Management)</strong></td>
<td>Infoblox IPAM provides a means of planning, tracking, and managing IP address space in a network. It glues DNS and DHCP services together so that each service is aware of changes in the other. The Infoblox IPAM implementation offers an IP address-centric approach so you can manage your networks and IP addresses through a centralized GUI.</td>
</tr>
<tr>
<td><strong>Network Mask or Netmask</strong></td>
<td>A numeric representation of the bits that are used to split an IP address into the network portion and the host portion. In Infoblox products, this is represented by either quad-dotted decimal representation or CIDR notation for IPv4 network masks, or by CIDR notation for IPv6 network masks.</td>
</tr>
<tr>
<td><strong>Network View</strong></td>
<td>On Infoblox appliances, a single routing domain with its own networks and shared networks. A network view can contain both IPv4 and IPv6 networks. All networks must belong to a network view on the Infoblox appliance.</td>
</tr>
<tr>
<td><strong>NIOS</strong></td>
<td>An Infoblox proprietary system that powers Infoblox solutions with an embedded processor that delivers core network services. It is the operating system that runs on the NIOS appliances—a security-hardened, real-time set of appliances built to ensure the non-stop operation of network infrastructure. NIOS automates the error-prone and time-consuming manual tasks associated with deploying and managing IPAM, DNS, and DHCP required for continuous IP network availability and business uptime.</td>
</tr>
<tr>
<td>----------</td>
<td>-------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>NIOS Virtual Appliance</strong></td>
<td>Any Infoblox supported platform, such as the Riverbed Steelhead appliances or VMware appliances, that runs the vNIOS software. These appliances are also known as the vNIOS appliances.</td>
</tr>
<tr>
<td><strong>Reservation</strong></td>
<td>On Infoblox appliances, a static IP address that you create for future use. A reservation is a pre-provisioned fixed address. You can reserve this static IP address on the NIOS appliance and assign it to a client in the future.</td>
</tr>
<tr>
<td><strong>Subnet (or network)</strong></td>
<td>A logical division of an IP network. A subnet of network may also be called a network. For example, 10.0.0.0/8 is a subnet of 10.0.0.0/16 and fc80:8:8:16::/64 is a subnet of fc80:8:8::/48.</td>
</tr>
<tr>
<td><strong>Superuser</strong></td>
<td>An admin user account that has unrestricted access to Infoblox Multi-Grid Manager, Grid Manager, or System Manager.</td>
</tr>
<tr>
<td><strong>vNIOS</strong></td>
<td>The virtual version of NIOS. You can install Infoblox vNIOS software on any supported virtual platform and configure the system as a vNIOS virtual appliance.</td>
</tr>
</tbody>
</table>
# Appendix B Infoblox IPAM Properties

The following table provides descriptions of the Infoblox IPAM properties used for VMs.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Infoblox.IPAM.createHostRecord</td>
<td>If TRUE, only the host record is created.</td>
</tr>
<tr>
<td>Infoblox.IPAM.createAddressRecord</td>
<td>If TRUE, the A record is created.</td>
</tr>
<tr>
<td>Infoblox.IPAM.createAddressAndPtrRecords</td>
<td>If TRUE, the PTR record which is associated with the A record is created.</td>
</tr>
<tr>
<td>Infoblox.IPAM.createFixedAddress</td>
<td>If TRUE, the fixed address is created.</td>
</tr>
<tr>
<td>Infoblox.IPAM.createReservation</td>
<td>If TRUE, the reservation is created.</td>
</tr>
<tr>
<td>Infoblox.IPAM.restartIfNeeded</td>
<td>If TRUE, the DHCP service in NIOS is automatically restarted if this is required by NIOS configuration. Enabling this property affects DHCP records: fixed addresses, reservations, and host records with the Enable DHCP option turned on. If you create address and PTR records, enabling this property has no effect. For a list of operations requiring a DHCP service restart, see Appendix E, &quot;Operations Requiring Service Restart&quot;.</td>
</tr>
<tr>
<td>Infoblox.IPAM.NetworkX.aliases</td>
<td>List of aliases for the host record of network interface X in the FQDN format.</td>
</tr>
<tr>
<td>Infoblox.IPAM.NetworkX.enableDhcp</td>
<td>Enables the DHCP flag for the host record of network interface X.</td>
</tr>
<tr>
<td>Infoblox.IPAM.NetworkX.enableDns</td>
<td>Enables the DNS flag for the host record of network interface X.</td>
</tr>
<tr>
<td>Infoblox.IPAM.NetworkX.dnsView</td>
<td>DNS view in which the host record or DNS record of network interface X will be created. The DNS view property should contain DNS zones specified in the DHCP options of networks and ranges selected in the appropriate network profile. If the DNS view is not specified in the property group by default, IPAM Plug-In generates the default DNS view value based on the template “default.&lt;network view&gt;”. When the default network view is selected in the network profile or if the network view (the address space in the vRA terminology) is not specified, the default DNS view from NIOS will be used (typically associated with the default network view).</td>
</tr>
<tr>
<td>Infoblox.IPAM.NetworkX.msDhcpServer</td>
<td>Microsoft DHCP server for the fixed address of network interface X.</td>
</tr>
<tr>
<td>Infoblox.IPAM.NetworkX.comment</td>
<td>Comment for the record of network interface X.</td>
</tr>
<tr>
<td>Infoblox.IPAM.enableCustomHostname</td>
<td>Enables updating hostnames of appropriate records in NIOS on the “MachineProvisioned” event. You should set this property to TRUE if you use Custom Hostnaming Extension for vRA or alternative solutions for customizing VM names through a vRA extensibility mechanism. Set to TRUE by default.</td>
</tr>
</tbody>
</table>
| Infoblox.IPAM.CustomHostname.ConditionalMachineCustomPropertyX.Name | These properties take effect only if “Infoblox.IPAM.enableCustomHostname” is set to TRUE. If they are specified, the Plug-In updates the hostname in NIOS only if the property with the same name and value exists in the VM properties list while the VM is spinning up in vRA. It can be useful when you want to skip updating hostname if the initial VM name was not changed by a third-party custom
| Infoblox.IPAM.CustomHostname.ConditionalMachineCustomPropertyX.Value | hostnaming extension. You can specify up to three properties to identify the case when the VM name was changed. |

**Note:** Infoblox recommends you to use the *Create Property Group* workflow to create a custom property group required for your configuration. It can help avoid problems with irrelevant settings in the Infoblox property group. For more information, see *Create Property Group Workflow*. 
## Appendix C Infoblox Endpoint Properties

The following table provides descriptions of the Infoblox properties that you can define in the Infoblox IPAM endpoint.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Infoblox.IPAM.APIType</td>
<td>The API type for the master connection and failover connections. This can be WAPI or Cloud API.</td>
</tr>
<tr>
<td>Infoblox.IPAM.EndpointX.Hostname</td>
<td>The hostname for a failover connection.</td>
</tr>
<tr>
<td>Infoblox.IPAM.EndpointX.Username</td>
<td>The user name for a failover connection.</td>
</tr>
<tr>
<td>Infoblox.IPAM.EndpointX.Password</td>
<td>The password for a failover connection.</td>
</tr>
<tr>
<td>Infoblox.IPAM.GetIPRanges.maxResults</td>
<td>The maximum number of results retrieved from NIOS when searching for network ranges.</td>
</tr>
</tbody>
</table>
Appendix D Record Properties for VM Requests

The following table specifies which properties you should set to TRUE and FALSE when you request a VM with specific DNS records.

<table>
<thead>
<tr>
<th>Use Case</th>
<th>Host Record</th>
<th>Address Record</th>
<th>Address, PTR</th>
<th>Fixed Address</th>
<th>Reservation</th>
<th>CNAME (Alias)</th>
<th>Enable DNS</th>
<th>Enable DHCP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provisioning VM with Host record by enabling DNS and DHCP</td>
<td>TRUE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>TRUE</td>
<td>TRUE</td>
</tr>
<tr>
<td>Provisioning VM with A record</td>
<td>FALSE</td>
<td>TRUE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
</tr>
<tr>
<td>Provisioning VM with A and PTR record</td>
<td>FALSE</td>
<td>FALSE</td>
<td>TRUE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
</tr>
<tr>
<td>Provisioning VM with A record and Fixed Address</td>
<td>FALSE</td>
<td>TRUE</td>
<td>FALSE</td>
<td>TRUE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
</tr>
<tr>
<td>Provisioning VM with A record and Reservation</td>
<td>FALSE</td>
<td>FALSE</td>
<td>TRUE</td>
<td>TRUE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
</tr>
<tr>
<td>Provisioning VM with A, PTR record and Fixed Address</td>
<td>FALSE</td>
<td>FALSE</td>
<td>TRUE</td>
<td>TRUE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
</tr>
<tr>
<td>Provisioning VM with A, PTR record and Reservation</td>
<td>FALSE</td>
<td>FALSE</td>
<td>TRUE</td>
<td>TRUE</td>
<td>TRUE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
</tr>
<tr>
<td>Provisioning VM with Fixed Address</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>TRUE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
</tr>
<tr>
<td>Provisioning VM with Reservation</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>TRUE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
</tr>
<tr>
<td>Provisioning VM with A and CNAME record</td>
<td>FALSE</td>
<td>TRUE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>TRUE</td>
<td>FALSE</td>
<td>FALSE</td>
</tr>
<tr>
<td>Provisioning VM with A, Fixed Address and CNAME record</td>
<td>FALSE</td>
<td>TRUE</td>
<td>FALSE</td>
<td>TRUE</td>
<td>FALSE</td>
<td>TRUE</td>
<td>FALSE</td>
<td>FALSE</td>
</tr>
<tr>
<td>Provisioning VM with A, Reservation and CNAME record</td>
<td>FALSE</td>
<td>TRUE</td>
<td>FALSE</td>
<td>TRUE</td>
<td>TRUE</td>
<td>TRUE</td>
<td>FALSE</td>
<td>FALSE</td>
</tr>
<tr>
<td>Provisioning VM with A, PTR and CNAME record</td>
<td>FALSE</td>
<td>FALSE</td>
<td>TRUE</td>
<td>TRUE</td>
<td>TRUE</td>
<td>TRUE</td>
<td>FALSE</td>
<td>FALSE</td>
</tr>
<tr>
<td>Provisioning VM with A, PTR, Fixed Address and CNAME record</td>
<td>FALSE</td>
<td>TRUE</td>
<td>TRUE</td>
<td>TRUE</td>
<td>TRUE</td>
<td>TRUE</td>
<td>FALSE</td>
<td>FALSE</td>
</tr>
<tr>
<td>Provisioning VM with A, PTR, Reservation and CNAME record</td>
<td>FALSE</td>
<td>FALSE</td>
<td>TRUE</td>
<td>TRUE</td>
<td>TRUE</td>
<td>TRUE</td>
<td>FALSE</td>
<td>FALSE</td>
</tr>
<tr>
<td>Provisioning VM with Host record by enabling DHCP</td>
<td>TRUE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>TRUE</td>
</tr>
<tr>
<td>Provisioning VM with Host record by enabling DNS</td>
<td>TRUE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>TRUE</td>
</tr>
<tr>
<td>Provisioning VM with Host record by not enabling DNS and DHCP</td>
<td>TRUE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
</tr>
</tbody>
</table>
Appendix E Operations Requiring Service Restart

The following table provides a list of objects that require a DHCP service restart in NIOS after you make configuration changes to them. For a complete list of objects requiring a service restart, refer to Appendix H, “Configuration Requiring Service Restart”, in the Infoblox NIOS Documentation.

<table>
<thead>
<tr>
<th>Object</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host record with DHCP enabled</td>
<td>Add, update, delete</td>
</tr>
<tr>
<td>Fixed address</td>
<td>Add, update, delete</td>
</tr>
<tr>
<td>Reservation</td>
<td>Add, update, delete</td>
</tr>
</tbody>
</table>