Copyright Statements
© 2015, Infoblox Inc.—All rights reserved.
The contents of this document may not be copied or duplicated in any form, in whole or in part, without the prior written permission of Infoblox, Inc.
The information in this document is subject to change without notice. Infoblox, Inc. shall not be liable for any damages resulting from technical errors or omissions which may be present in this document, or from use of this document.
This document is an unpublished work protected by the United States copyright laws and is proprietary to Infoblox, Inc. Disclosure, copying, reproduction, merger, translation, modification, enhancement, or use of this document by anyone other than authorized employees, authorized users, or licensees of Infoblox, Inc. without the prior written consent of Infoblox, Inc. is prohibited.
For Open Source Copyright information, refer to the *Infoblox NIOS Administrator Guide*.

Trademark Statements
Infoblox, the Infoblox logo, Grid, NIOS, bloxTools, Network Automation and PortIQ are trademarks or registered trademarks of Infoblox Inc.
All other trademarked names used herein are the properties of their respective owners and are used for identification purposes only.

Company Information
http://www.infoblox.com/contact/

Product Information
Hardware Models
- Trinzic product line: 100, 810, 820, 1410, 1420, 2210, 2220, and Infoblox-4010
- Network Insight: ND-800, ND-1400, ND-2200, and ND-4000
- Trinzic Reporting: TR-1400, TR-2000, TR-2200, and TR-4000
- Advanced DNS Protection: PT-1400, PT-2200, and PT-4000
- Infoblox-4030 and Infoblox-4040 DNS Caching Accelerator Appliances
- Network Automation: NetMRI-1102-A, NT-1400, NT-2200, and NT-4000

Document Number: 400-0568-006 Rev. A
Document Updated: April 20, 2015

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

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction to the Infoblox IPAM Plug-In for VMware</td>
<td>1</td>
</tr>
<tr>
<td>Intended Audience</td>
<td>2</td>
</tr>
<tr>
<td>Deployment Requirements</td>
<td>2</td>
</tr>
<tr>
<td>Before Deploying Infoblox IPAM Plug-In for VMware</td>
<td>4</td>
</tr>
<tr>
<td>Setting Up the Infoblox NIOS Appliance</td>
<td>4</td>
</tr>
<tr>
<td>Deploying the Infoblox IPAM Plug-In for VMware</td>
<td>5</td>
</tr>
<tr>
<td>vCloud Director Deployment</td>
<td>5</td>
</tr>
<tr>
<td>vCloud Director Deployment with AMQP</td>
<td>8</td>
</tr>
<tr>
<td>vRealize Automation Deployment</td>
<td>11</td>
</tr>
<tr>
<td>vRA/vCAC Configuration Steps</td>
<td>14</td>
</tr>
<tr>
<td>Performing a vRealize Automation Request</td>
<td>21</td>
</tr>
<tr>
<td>Using Extensible Attributes in Infoblox IPAM Plug-In for VMware</td>
<td>26</td>
</tr>
<tr>
<td>Reloading Extensible Attributes</td>
<td>26</td>
</tr>
<tr>
<td>Using Infoblox IPAM Plug-In for VMware Workflows</td>
<td>28</td>
</tr>
<tr>
<td>Basic IPAM Workflows</td>
<td>28</td>
</tr>
<tr>
<td>vCloud Director Workflows</td>
<td>37</td>
</tr>
<tr>
<td>AMQP Workflows</td>
<td>44</td>
</tr>
<tr>
<td>Overview of vCAC Workflows</td>
<td>50</td>
</tr>
<tr>
<td>vCAC Configuration Workflows</td>
<td>50</td>
</tr>
<tr>
<td>Workflows for Commissioning and Decommissioning of Virtual Machines</td>
<td>53</td>
</tr>
<tr>
<td>Verifying Workflow Execution</td>
<td>55</td>
</tr>
<tr>
<td>Using Infoblox IPAM Plug-In for VMware Actions</td>
<td>56</td>
</tr>
<tr>
<td>Utility Actions Table</td>
<td>66</td>
</tr>
<tr>
<td>AMQP Utility Actions Table</td>
<td>68</td>
</tr>
<tr>
<td>Infoblox IPAM Plug-In for VMware API</td>
<td>69</td>
</tr>
<tr>
<td>Removing Infoblox IPAM Plug-In for VMware</td>
<td>83</td>
</tr>
<tr>
<td>Removing Infoblox IPAM Plug-In for VMware on Windows</td>
<td>83</td>
</tr>
<tr>
<td>Removing Infoblox IPAM Plug-In for VMware on Linux</td>
<td>85</td>
</tr>
<tr>
<td>Infoblox IPAM Plug-In for VMware Best Practices</td>
<td>88</td>
</tr>
<tr>
<td>Infoblox IPAM Plug-In for VMware CPU and Memory Utilization for Workflow Execution</td>
<td>88</td>
</tr>
<tr>
<td>Resources</td>
<td>89</td>
</tr>
</tbody>
</table>
INTRODUCTION TO THE INFIBLOX IPAM PLUG-IN FOR VMWARE

This guide describes how to install and use the Infoblox IPAM Plug-In for VMware™ with vRealize® Orchestrator (vRO) (formerly vCenter® Orchestrator), vRealize Automation (formerly vCloud Automation Center) or vCloud Director (vCD). It provides information about the Infoblox plug-in workflows and actions library, and the Infoblox IPAM Plug-In for VMware API.

The Infoblox IPAM Plug-In for VMware v.2.4.2 provides support for VMware virtualization platforms with VMware vRealize Automation (vRA) 6.0, 6.1 and 6.2. You can evaluate IPAM Plug-In compatibility with various releases of this virtualization platforms in the section Deployment Requirements on page 2.

The Infoblox IPAM Plug-In for VMware allows 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 automatically forwards a DNS request to your Infoblox IPAM server, i.e. NIOS or vNIOS appliance. NIOS creates a complete host record in its database to enable the VMs to be located through their FQDNs. This information is also replicated in VMware platforms such as vRealize Automation or vCloud Director.

The Infoblox IPAM Plug-In for VMware allows you to control vCD workflows execution on blocking tasks by using the Advanced Message Queuing Protocol (AMQP). This deployment type does not use vRealize Automation. For example, you can configure vCD to trigger specific workflows that synchronize IPAM data when a VM is modified or a vApp is recomposed. For more information, see AMQP Workflows on page 48.

You can integrate the Infoblox IPAM Plug-In for VMware with VMware’s vRealize Automation (vRA). vRA (vCAC) invokes the Infoblox IPAM Plug-In for vCO workflows that allocate an IP address and a DNS record to a new VM, or delete them for a removed VM. For more information, see Overview of vCAC Workflows on page 54.

The figure to the right illustrates the Infoblox IPAM Plug-In for VMware architecture.

Additional benefits in Infoblox IPAM Plug-In for VMware v.2.4.2 include:
- Support for vCAC 6.1 in conjunction with vCO 5.5.2 (for details, see Deployment Requirements on page 2);

Improvements in the Infoblox IPAM Plug-In for VMware v.2.4.1 include:
- Improved integration with vRA (vCAC), eliminating manual import of Build Profiles and use of vCAC Designer;
- vSphere Port Group Support in vCAC Workflows;
- Simplified methods for using extensible attributes;
- CNAME records support for simple workflows and vCAC workflows.

You can build custom workflows using Infoblox IPAM Plug-In for VMware actions, API objects and methods. See Using Infoblox IPAM Plug-In for VMware Actions on page 60 and Infoblox IPAM Plug-In for VMware API on page 73.
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, vCloud Director, vCenter Orchestrator workflow development, vRealize Automation (formerly vCloud Automation Center), and VMware vSphere. This guide also assumes that the readers are familiar with NIOS appliances and NIOS software. For locations where to obtain more information about these, see Resources on page 93.

DEPLOYMENT REQUIREMENTS

You can choose from three Infoblox IPAM Plug-In for VMware deployment options according to your business needs:

1. vRealize Automation Deployment

The following table lists recommended software combinations that are verified for compatibility with the Infoblox IPAM Plug-In for VMware v.2.4.2 in this deployment type:

<table>
<thead>
<tr>
<th>NIOS</th>
<th>ESXi</th>
<th>vCenter</th>
<th>vRO (vCO)</th>
<th>vRA (vCAC)</th>
<th>vRA (vCAC) Plug-In</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.11.7</td>
<td>5.5.0</td>
<td>5.5.0</td>
<td>vRO 6.0.1 embedded</td>
<td>vRA 6.2.0</td>
<td>6.2.0</td>
</tr>
<tr>
<td>6.11.7</td>
<td>5.5.0</td>
<td>5.5.0</td>
<td>vRO 6.0.1 standalone</td>
<td>vRA 6.2.0</td>
<td>6.2.0</td>
</tr>
<tr>
<td>6.11.7</td>
<td>5.5.0</td>
<td>5.5.0</td>
<td>vCO 5.5.2</td>
<td>vCAC 6.1</td>
<td>6.1</td>
</tr>
<tr>
<td>6.11.7</td>
<td>5.1.0</td>
<td>5.1.0</td>
<td>vCO 5.5.1</td>
<td>vCAC 6.0.1</td>
<td>6.0.1</td>
</tr>
<tr>
<td>6.11.7</td>
<td>5.1.0</td>
<td>5.1.0</td>
<td>vCO 5.5.1</td>
<td>vCAC 5.1.1</td>
<td>5.2.0</td>
</tr>
</tbody>
</table>

This deployment option also requires the following:

— A VMware community package, com.vmware.pso.vcac.proptoolkit.package (included in the Infoblox IPAM plugin distribution package).

The following figure illustrates components of the vRealize Automation deployment:

![vRealize Automation Diagram](image)

The section vRealize Automation Deployment on page 11 describes how to perform the vRealize Automation-enabled setup of the Infoblox IPAM Plug-In for VMware.

2. vCloud Director deployment

The following table lists recommended software combinations that are verified for compatibility with the Infoblox IPAM Plug-In for VMware v.2.4.2 in this deployment type:

<table>
<thead>
<tr>
<th>NIOS</th>
<th>ESXi</th>
<th>vCenter</th>
<th>vCO</th>
<th>vShield</th>
<th>vCD</th>
<th>vCD Plug-In</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.11.7</td>
<td>5.5.0</td>
<td>5.5.0</td>
<td>5.5.0</td>
<td>5.5.0</td>
<td>5.5.0</td>
<td>5.5.0</td>
</tr>
<tr>
<td>6.11.7</td>
<td>5.1.0</td>
<td>5.1.0</td>
<td>5.1.0</td>
<td>5.1.0</td>
<td>5.1.0</td>
<td>5.1.0</td>
</tr>
</tbody>
</table>
This deployment option does not use AMQP messaging and requires only the Infoblox IPAM Plug-In for VMware and the VMware vCO Plug-In for vCloud Director. The section vCloud Director Deployment on page 5 describes how to perform this deployment. The following figure illustrates components of the deployment.

3. vCloud Director with AMQP deployment

The following table lists recommended software combinations that are verified for compatibility with the Infoblox IPAM Plug-In for VMware v.2.4.2 in this deployment type:

<table>
<thead>
<tr>
<th>NIOS</th>
<th>ESXi</th>
<th>vCenter</th>
<th>vCO</th>
<th>vShield</th>
<th>vCD</th>
<th>vCD Plug-In</th>
<th>RabbitMQ</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.11.7</td>
<td>5.5.0</td>
<td>5.5.0</td>
<td>5.5</td>
<td>5.5</td>
<td>5.5</td>
<td>5.5</td>
<td>2.8.2</td>
</tr>
<tr>
<td>6.11.7</td>
<td>5.1.0</td>
<td>5.1.0</td>
<td>5.1</td>
<td>5.1</td>
<td>5.1</td>
<td>5.1</td>
<td>2.8.2</td>
</tr>
</tbody>
</table>

The vCloud Director with AMQP deployment option with AMQP requires the following in addition to the vCloud Director deployment components:
- An AMQP messaging server;
- The VMware vCO AMQP Plug-In;
- The VMware vCO vCenter Server Plug-In;
- The Infoblox IPAM AMQP Package;
- The VMware vCD Notifications Package for vCO.

The following figure illustrates components of the deployment.

The section vCloud Director Deployment with AMQP on page 8 describes how to perform the AMQP deployment of the Infoblox IPAM Plug-In for VMware.

**Note:** For all deployment types, to check compatibility of the Infoblox IPAM Plug-In for VMware with other combinations of software components, ensure that the components are compatible with each other. You can do so using documentation for these products and VMware Product Interoperability Matrixes accessible by the following link: [http://www.vmware.com/resources/compatibility/sim/interop_matrix.php](http://www.vmware.com/resources/compatibility/sim/interop_matrix.php).

The Infoblox IPAM Plug-In for VMware v.2.4.2 supports vRO/vCO versions 5.1, 5.5/5.5.1/5.5.2, and 6.0.0/6.0.1.
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 on page 2.
2. Set up your NIOS or vNIOS appliance as described in Setting Up the Infoblox NIOS Appliance on page 6.
3. Deploy the Infoblox IPAM Plug-In for VMware following the order described in Deploying the Infoblox IPAM Plug-In for VMware on page 7.

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 Administrator Guide.

- Ensure that you have set up a NIOS account with appropriate user permissions. For information, see NIOS Permissions Requirements on page 6.
- Create a network to use for operations with the Infoblox IPAM Plug-In for VMware. For more information, see the section Configuring DHCP Overview in the NIOS Administrator Guide.
- 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 NIOS Administrator Guide.
- Define DHCP address ranges from which you plan to allocate IP addresses through the Infoblox IPAM Plug-In for VMware. For information, see the section Configuring IPv4 Address Ranges in the NIOS Administrator Guide.
- Define 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, see Chapter 18, Configuring DNS Zones in the NIOS Administrator Guide.
- Set up DHCP network templates that are used by Infoblox IPAM Plug-In for VMware. For information, see About IPv4 Network Templates in the NIOS Administrator Guide.
- Create the extensible attribute definitions in NIOS for the IPAM objects attributes that are used in the Infoblox IPAM Plug-In for VMware workflows. For more information, see About Extensible Attributes in the NIOS Administrator Guide.

Note: For more information about using extensible attributes that are required for vCloud Director workflows, see Required Extensible Attributes for Basic Workflows on page 33 and Required Extensible Attributes for vCloud Director Workflows on page 41.

Note: v.2.4.2 of the Infoblox IPAM Plug-In for VMware is qualified against Infoblox RESTful API 1.6.

NIOS Permissions Requirements

On the Infoblox NIOS system, ensure that the admin accounts meet the following requirements:

- The NIOS user account requires both GUI and API permissions.
- 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 at least Read Only permissions to the zone(s).
- Read/Write permissions are required for the appropriate subnetworks:
Read/Write permissions for NIOS fixed address/hosts is a minimum requirement. The Infoblox IPAM Plug-In for VMware automatically adds the host with the MAC address and DHCP enabled, 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 automatically performs a service restart 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.

### DEPLOYING THE INFOLBOX IPAM PLUG-IN FOR VMWARE

This section provides details on each of the Infoblox IPAM Plug-In for VMware deployment options:

- **vCloud Director Deployment** (below);
- **vCloud Director Deployment with AMQP** on page 11;
- **vRealize Automation Deployment** on page 14.

### vCloud Director Deployment

Before you deploy the Infoblox IPAM Plug-In for VMware, verify the configured and running instances of vCenter Orchestrator and vCloud Director in their correct versions. Proceed in the following order:

1. Import SSL certificates from NIOS and vCloud Director as described in **Importing SSL Certificates** on page 7.
2. Install the Infoblox IPAM Plug-In for VMware as described in **Installing the Infoblox IPAM Plug-In for VMware** on page 7.
3. Set up an Infoblox IPAM connection as described in **Configuring an Infoblox IPAM Connection** on page 8.
4. Install the VMware vCO plug-in for vCloud Director as described in **Installing VMware vCenter Orchestrator Plug-In for vCloud Director** on page 9.
5. Set up a connection to vCloud Director as described in **Setting Up the vCloud Director Connection** on page 10.

### Importing SSL Certificates

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

To import an SSL certificate:

1. On the VMware vCenter Orchestrator Configuration page, click the Network tab.
2. In the right panel, click the SSL Trust Manager tab.
3. Under Import from URL, enter the IP address or, under Import from file, select the certificate file for the NIOS appliance or vCloud Director.
4. Click Import, and then click Import again to confirm.

The new SSL certificate appears in the SSL Trust Manager page.

### Installing the 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 v.2.4.2:

1. Unzip the plug-in archive file into a folder on your management system.
2. Log in to the VMware vCenter Orchestrator Configuration page using a Web browser.
3. Click the Plug-ins tab.
4. In the right panel, under **Install new plug-in**, click the **Plug-in file** field.

5. In the file upload dialog, select **All Files**, select the .dar file (o11nplugin-ipam-dar) for the plug-in version v.2.4.2, and click **Open**.

6. Click **Upload and install**.
   The Infoblox IPAM Plug-In for VMware tab appears in the Orchestrator Configuration page.

7. If the Infoblox IPAM Plug-In for VMware check box is not selected under **Enabled plug-ins installation status**, select it and click **Apply Changes**.

8. On the **Startup Options** tab, click **Restart service** and, if necessary, click **Restart the vCO configuration server**.

9. Click the **Plug-ins** tab and make sure that the text “Installation OK” is visible to the right of the IPAM plug-in. If not, restart vCO till the “Installation OK” message is visible before you continue with the IPAM plug-in configuration.

   **Note:** If you experience difficulty having the installed Infoblox IPAM Plug-In show the status “Installation OK,” restart the vCO appliance. This forces a load on the IPAM Plug-In. Do attempt to proceed with further deployment until you see the status “Installation OK” for the installed Infoblox IPAM Plug-In.

---

**Configuring an Infoblox IPAM Connection**

After you have installed the Infoblox IPAM Plug-In for VMware and imported the SSL certificate from NIOS, you configure a connection to your Infoblox appliance. You can add a number of connections to different NIOS servers, or Grids, and indicate the default one. You can then edit or delete the added Infoblox IPAM connections. For details, see **Managing Infoblox IPAM Connections** on page 9.

To configure an Infoblox IPAM connection:

1. On the VMware vCenter Orchestrator Configuration page, click the **Infoblox IPAM 2.4.2** tab.

2. Click **New Connection**.

3. Complete the following:
   - **Infoblox IPAM Host Name**: Enter the IP address or host name of the NIOS, vNIOS appliance or Cloud Platform appliance.
   - **Infoblox IPAM User Name**: Enter the Cloud API user name for the NIOS, vNIOS appliance or Cloud Platform appliance.
   - **Infoblox IPAM Password**: Enter the Cloud API password for the NIOS, vNIOS appliance or Cloud Platform appliance.
   - **Default Network View**: Optionally, enter the network view that will be used as the default in the workflows.
   - **Default DNS View**: Optionally, enter the DNS view that will be used as the default in the workflows.

   **Note:** In workflows related to operations on NIOS objects, you can specify a custom network view and a DNS view, if they exist in the NIOS Grid. If no custom view is indicated for a workflow, the default view is used. If no default network or DNS view is specified in the connection configuration, then the default NIOS views are used for plug-in operation. Check your NIOS configuration to verify the view configurations.

4. Click **Apply changes**. The new connection to your Infoblox IPAM appliance is added on the **Connections** tab and is automatically set as the default.
On the Startup Options tab, click Restart service and, if necessary, click Restart the vCO configuration server.

To verify the vCO connection to the Infoblox IPAM server:
1. Open your vCenter Orchestrator Java client.
2. Click the Inventory tab. You should see an Infoblox IPAM item in the vCO inventory list. Clicking the arrow next to Infoblox IPAM shows the IP address for the NIOS system.

Managing Infoblox IPAM Connections
You can manage connections to your Infoblox IPAM servers from the Connections tab for the Infoblox IPAM Plug-In from the vCO configuration page.

• To set a connection as default, select By default for the desired connection.
• To edit a connection, click Edit and modify the connection information described in Configuring an Infoblox IPAM Connection on page 8.
• To delete a connection, click Delete.

Note: From the Connections tab, you can also import an SSL certificate for the Infoblox IPAM Plug-In for VMware by clicking SSL Certificates.

Installing VMware vCenter Orchestrator Plug-In for vCloud Director
Your current VMware deployment may already have the vCloud Director plug-in installed. If so, you can skip the following procedure and go to Setting Up the vCloud Director Connection on page 10.

To install the vCloud Director plug-in:
1. Download the vCloud Director plug-in installation file in the .vmoapp or .dar format.
2. Log in to the VMware vCenter Orchestrator Configuration web page.
3. Click the Plug-ins tab.
4. In the right panel, under Install new plug-in, click the Plug-in file field.
5. In the file upload dialog, select All Files, select the vCloud Director plug-in installation file, and click Open.
6. Click Upload and install, and then click I Accept the Terms of the License Agreement. The vCloud Director plug-in tab appears in the Orchestrator Configuration page.
7. If the vCloud Director plug-in check box is not selected under Enabled plug-ins installation status, select it and click Apply Changes.
8. On the Startup Options tab, click Restart service and, if necessary, click Restart the vCO configuration server.

Setting Up the vCloud Director Connection
After installing the vCO plug-in for vCloud Director and imported the vCD SSL certificate, you set up a connection to an admin account in vCloud Director.
To set up a vCloud Director connection:

1. Click the **vCloud Director** tab.
2. In the right panel, click **New vCloud Director Connection**.
3. Define the connectivity settings:
   - **Available**: Select **Enabled**.
   - **Host** (IP address or host name)
   - **Port** (443 is the default value)
   - **Maximum connections**
   - **Connection timeout**
   - **Organization**: Enter **system**.

   **Note**: You specify **system** for the organization to ensure that the Infoblox IPAM Plug-In for VMware has access to all required entities, such as port groups.

4. Under **Authentication Strategy**, choose **Basic Authentication**, and then select **Shared Session**.
5. In the **User Name** and **Password** fields, enter the credentials of the system administrator in vCloud Director.
6. Click **Apply Changes**.
7. On the **Startup Options** tab, click **Restart service** and, if necessary, click **Restart the vCO configuration server**.

To verify connection of vCenter Orchestrator to vCloud Director, do any of the following:

- On the vCO Configuration page, click the **vCloud Director** plug-in tab, and then click **Connections**. The new connection is displayed.
- In the vCO client, click the **Inventory** tab while in the Administer or Run mode. The new connection is displayed under **vCloud Director** in the inventory list.

You have completed the basic deployment of the Infoblox IPAM Plug-In for VMware. You can now use the plug-in with vCloud Director workflows. For more information, see **vCloud Director Workflows** on page 40.

### vCloud Director Deployment with AMQP

**Note**: This section assumes that you have performed all the installations and configurations from the preceding section, **vCloud Director Deployment** on page 7.

For the AMQP deployment option, proceed in the following order:

1. Set up the AMQP server as described in **Setting Up AMQP Messaging Server** on page 11.
2. Configure vCloud Director for AMQP operations as described in **Configuring vCloud Director for AMQP Operations** on page 12.
3. Install the VMware vCO AMQP Plug-In as described in **Installing VMware vCenter Orchestrator AMQP Plug-In** on page 13.
4. Enable the VMware vCO vCenter Server Plug-In as described in **Enabling the VMware vCO vCenter Server Plug-In** on page 13.
5. Install the vCloud Director Notifications Package for vCO as described in *Installing the vCloud Director Notifications Package for vCO* on page 13.

6. Install the Infoblox IPAM AMQP Package as described in *Installing the Infoblox IPAM AMQP Package* on page 13.

### Setting Up AMQP Messaging Server

An AMQP server is required for operation of workflows for the *vCD Notification Support on Blocking Tasks* Package. This section describes an example of the RabbitMQ server running on a Windows 7 client. Linux-based AMQP server deployments are also supported.

The following elements are needed for a successful installation:
- A static IP address for the AMQP server;
- Microsoft Internet Information Services (MS IIS) 7.0 and above;
- An Erlang/OTP programming language interpreter, version 15b and above;
- The RabbitMQ distributable for Windows, version 2.8.2 and above.

To set up the RabbitMQ server:

1. If necessary, install MS IIS:
   a. Under Windows 7, click Control Panel → Programs and Features → Turn Windows Features on or off.
   b. Select the Internet Information Services check box and click OK.
2. Download and install the Erlang command interpreter.
3. Download and install the RabbitMQ server.
4. Restart the system.
5. Start a Windows command-line session as Administrator.
6. `cd` to the following location:
   ```
   C:\Program Files\erl5.9\bin
   ```
7. Execute the following command to start the Erlang interpreter:
   ```
   C:\Program Files\erl5.9\bin> erl.exe
   ```
8. Then, `cd` to the following location:
   ```
   C:\Program Files\RabbitMQ Server\rabbitmq_server-2.8.2\sbin
   ```
9. Run the following three commands in the sequence shown below:
   ```
   C:\Program Files\RabbitMQ Server\rabbitmq_server-2.8.2\sbin> rabbitmq-server stop
   C:\Program Files\RabbitMQ Server\rabbitmq_server-2.8.2\sbin> rabbitmq-plugins enable rabbitmq_management
   C:\Program Files\RabbitMQ Server\rabbitmq_server-2.8.2\sbin> rabbitmq-server restart
   ```
10. To check the server operation, open a browser and connect to `http://localhost:55672` with the server default login guest/guest. If you are unable to connect, restart Windows and retry connection.

### Configuring vCloud Director for AMQP Operations

To configure vCloud Director for AMQP operations, you perform the following tasks:
- Enable the notifications to be handled by the AMQP server.
- Enable the vCD blocking tasks on which the Infoblox plug-in AMQP workflows will be triggered.

To enable vCD notifications:
1. Log in to your vCloud Director instance.
2. Go to *System → Administration → Extensibility → Settings*.
3. Under *Notifications*, select *Enable Notifications*. 

4. Under AMQP Broker Settings, do the following:
   a. In the AMQP Host field, enter the IP address of the AMQP server.
   b. In the AMQP Port field, enter 5672. This is the required TCP port that vCloud Director uses to communicate to the AMQP server.
   c. In the Exchange field, enter: systemExchange.
   d. In the vHost field, enter /.
   e. In the Prefix field, enter vcloud in lower case.
   f. In the User Name and Password fields, enter guest. This is the default value used for vCD connectivity to the RabbitMQ server.

5. Click Test AMQP Connection. You should see an AMQP Connection Succeeded message.

6. Click Apply.

To enable the vCD blocking tasks:
1. In vCloud Director, click the Blocking Tasks tab.
2. Expand the All Tasks folder.
3. Select the following blocking tasks located in the folders as described in Table 3.1.

Table 3.1 vCloud Director Blocking Tasks for Plug-In Usage

<table>
<thead>
<tr>
<th>Blocking Task</th>
<th>Used for Workflow</th>
</tr>
</thead>
<tbody>
<tr>
<td>All tasks/vApp Lifecycle/Instantiate vApp from Template</td>
<td>IPAM Provision All VMs in New vApp on Blocking Task</td>
</tr>
<tr>
<td>All tasks/vApp Lifecycle/Delete vApp</td>
<td>IPAM Delete vApp</td>
</tr>
<tr>
<td>All tasks/Virtual Machine/Add, Move or Delete Virtual Machines from vApp</td>
<td>IPAM Sync on vApp Recomp Workflow</td>
</tr>
<tr>
<td>All tasks/Virtual Machine/Modify Virtual Machine Configuration</td>
<td>IPAM Sync on VM Modification</td>
</tr>
<tr>
<td>All tasks/Network/Delete Network</td>
<td>IPAM Delete Network</td>
</tr>
</tbody>
</table>

Installing VMware vCenter Orchestrator AMQP Plug-In

The vCO AMQP plug-in contains workflows that allow vCenter Orchestrator to interact with the AMQP server and run custom AMQP operations. (See Resources on page 93 for the package download location.)

1. Download the vCO AMQP plug-in installation file from the VMware site.
2. Log in to the VMware vCenter Orchestrator Configuration page.
3. Click the Plug-ins tab.
4. In the right panel, under Install new plug-in, click the Plug-in file field.
5. In the file upload dialog, select All Files, select the file o11nplugin-amqp-1.0.2-228.vmoapp, and click Open.
6. Click Upload and install, and then click I Accept the Terms of the License Agreement.
7. If the AMQP plug-in check box is not selected under Enabled plug-ins installation status, select it and click Apply Changes.
8. On the **Startup Options** tab, click **Restart service** and, if necessary, click **Restart the vCO configuration server**.

### Enabling the VMware vCO vCenter Server Plug-In

By default, the VMware vCO vCenter Server Plug-In is not enabled in many deployments. To enable it, do the following:

1. Log in to the VMware vCenter Orchestrator Configuration page.
2. Click the **Plug-ins** tab.
3. In the right panel, under **Enabled plug-ins installation status**, select the vCenter Server plug-in check box.
4. Click **Apply changes**.
5. On the **Startup Options** tab, click **Restart service**.

### Installing the vCloud Director Notifications Package for vCO

The vCloud Director Notifications package provides an AMQP-based mechanism for triggering workflows in response to blocking tasks and notifications detected by vCloud Director. See **Resources** on page 93 for the location from which to download the package.

1. Log in to the VMware vCenter Orchestrator client.
2. Choose **Administer** mode.
3. Click the **Packages** tab.
4. Click **Import Package**.
5. Select the package file `com.vmware.coe.vcd55.notifications.package` and click **Open**.
6. In the **Import Package** window that appears, click **Import**, and then click **Import Selected Elements**.
   
   The package name appears in the packages list in the **Administer** mode. In the **Run** or **Design** mode, the workflows library of the vCD Notifications package is located in **Admin** → **PSO** → **vCloud Director Notifications**.
7. If an error indicator appears for the package, restart the vCenter Orchestrator client.

### Installing the Infoblox IPAM AMQP Package

To install the Infoblox IPAM AMQP Package:

1. Ensure that you have unzipped the archive file containing the Infoblox IPAM Plug-In for VMware v.2.4.2.
2. Log in to the VMware vCenter Orchestrator client.
3. Choose **Administer** mode.
4. Click the **Packages** tab.
5. Click **Import Package**.
6. Select the Infoblox IPAM AMQP package file `com.infoblox.ipam.amqp.package` and click **Open**.
7. In the **Import Package** window that appears, click **Import**, and then click **Import Selected Elements**.
   
   After a moment, the package file name appears in the packages list in the **Administer** mode. In the **Run** or **Design** mode, the workflows library of the Infoblox IPAM AMQP package is located in **Admin** → **IPAM** → **IPAM vCD Notification Support on Blocking Tasks**.
8. If an error indicator appears for the package, restart the vCenter Orchestrator client.

You have completed the AMQP deployment of the Infoblox IPAM Plug-In for VMware. You can now use the plug-in AMQP workflows. For more information, see **AMQP Workflows** on page 48.

### vRealize Automation Deployment

Before you deploy the Infoblox IPAM Plug-In for VMware, verify that you have configured and running instances of vRealize Orchestrator (formerly vCenter Orchestrator) and vRealize Automation (formerly vCloud Automation Center). For this deployment type, you perform the following procedures in the listed order below:

1. Import SSL certificates from NIOS and IaaS host as described in **Importing SSL Certificates** on page 14 (below).
2. Install the Infoblox IPAM Plug-In for VMware as described in *Installing the Infoblox IPAM Plug-In for VMware* on page 7.

3. Set up an Infoblox IPAM connection as described in *Configuring an Infoblox IPAM Connection* on page 8.

4. Install the vCO plug-in for vRA/vCAC as described in *Installing VMware vCenter Orchestrator Plug-In for vRA/vCAC* on page 15.

5. Install the external VMware package as described in *Importing the VMware vCO proptoolkit Package* on page 15.

6. Add an IaaS host as described in *Add an IaaS Host Wrapper Workflow* on page 54.

7. Install a vCO Customization as described in *Install vCO Customization Wrapper* on page 56.

8. Create a customization specification in vCenter as described in *Creating a Customization Specification in vCenter* on page 16.

9. Create vCenter and vCenter Orchestrator endpoint credentials as described in *Creating vCenter and vCenter Orchestrator Endpoint Credentials* on page 17.

10. Create vCenter and vCenter Orchestrator endpoints as described in *Creating vCenter and vCenter Orchestrator Endpoints* on page 17.

11. Create a Fabric Group in vRA/vCAC as described in *Creating a Fabric Group* on page 18.

12. Create a virtual machine prefix in vRA/vCAC as described in *Creating a Machine Prefix* on page 19.

13. Create a business group in vRA/vCAC as described in *Creating a Business Group* on page 19.

14. Verify compute resources in vRA/vCAC as described in *Viewing Assign Compute Resources* on page 19.

15. Create a resource reservation in vRA/vCAC as described in *Creating a Reservation* on page 20.

16. If necessary, force vRA/vCAC data collection as described in *Forcing Data Collection* on page 20.

17. Create a vRA/vCAC blueprint as described in *Creating a Blueprint* on page 21.

18. Create a vRA/vCAC build profile as described in *Creating Build Profiles* on page 21.

19. Associate the necessary build profile to your blueprints as described in *Setting a Build Profile to a Blueprint* on page 22.

20. Create services in vRA/vCAC as described in *Creating Services and Adding them to the Catalog* on page 22.

**Importing SSL Certificates**

To ensure interoperability of vCenter Orchestrator with the Infoblox IPAM Plug-In for VMware, you must import valid SSL certificates from the NIOS appliance and the vCAC Infrastructure Administration host (a Windows computer with the IaaS Service installed) into vCenter Orchestrator.

To import an SSL certificate:

1. On the VMware vCenter Orchestrator Configuration page, click the **Network** tab.

2. In the right panel, click the **SSL Trust Manager** tab.

3. Under **Import from URL**, enter the IP address or, under **Import from file**, select the certificate file for the NIOS appliance or IaaS host.

4. Click **Import**, and then click **Import** again to confirm.

   The new SSL certificate appears in the **SSL Trust Manager** page.

**Installing VMware vCenter Orchestrator Plug-In for vRA/vCAC**

The vCO plug-in for vRA/vCAC contains the workflows that allow vCenter Orchestrator to interact with the vCAC Infrastructure Administration host and run custom vRA/vCAC operations. (See *Resources* on page 93 for the package download location.)

1. Download the vCO plug-in for vRA/vCAC installation file from the VMware site.

2. Log in to the VMware vCenter Orchestrator Configuration page.

3. Click the **Plug-Ins** tab.
4. In the right panel, under Install new plug-in, click the Plug-in file field.
5. In the file upload dialog, select All Files, select the file o11nplugin-vcac-<version>.vmoapp, (the <version> number depends on the version of your vRA/vCAC setup), and click Open.
6. Click Upload and install, and then click I Accept the Terms of the License Agreement.
   The vCAC plug-in appears in the vCenter Orchestrator plug-ins list in the right pane.
7. If the vCAC plug-in check box is not selected under Enabled plug-ins installation status, select it and click Apply Changes.
8. On the Startup Options tab, click Restart service and, if necessary, click Restart the vCO configuration server. It may take more than one attempt for the new Plug-In to show the “Installation OK” status.

Importing the VMware vCO proptoolkit Package

You must install the vCO proptoolkit package before running any workflows from the vCAC package:
- com.vmware.pso.vcac.proptoolkit.package

These packages are located in the \2.4.2\vcac folder of the provided .zip archive. To install packages, do the following:
1. Open the vCO Java client.
2. Choose Administer or Design mode.
3. Click the Packages tab.
4. Click Import Package.
5. Select the package file com.vmware.pso.vcac.proptoolkit.package and click Open.
6. In the Import Package window that appears, all associated workflows are enabled. Click Import and Trust Provider, and then click Import Selected Elements. After a moment, the vCO client updates to show the new package and its description in the General tab.

Validating the Infoblox IPAM vCAC Workflows

Installation of the Plug-In also installs the Infoblox vCO package com.infoblox.ipam.vcac, which is the key package used to support the Infoblox workflows for the vRA/vCAC integration. To ensure operation, you should verify that this package is both present in your vCenter Orchestrator environment and validate the workflows associated with this package before continuing setup. This helps determine that all dependencies are addressed for IPAM vCO Plug-In support before continuing with deployment in the following sections. Do the following:
1. Open the vCO Java client.
2. Choose Administer or Design mode.
3. Click the Packages tab.
4. Right-click the com.infoblox.ipam.vcac package and choose Validate Workflows. A Workflows Validation window appears listing all events including any warnings.
5. Click Close when finished.
You can select the com.infoblox.ipam.vcac package and click the Workflows tab in the right pane to view a list of workflows.

Creating a Customization Specification in vCenter

You use a customization specification in vCenter as part of making a vCAC Blueprint. 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. Customization specifications are used to help deploy VMs.
To create a customization specification, do the following.
1. In vCenter, choose vCenter → Inventory → Management → Customization Specifications Manager:
2. Click **New**.

3. Select the **Target Virtual Machine OS type**.
   The New Customization Specification wizard opens.

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. *(Note: this Domain Name value is also used in other parts of vCAC configuration, including creating the Infoblox IPAM Build Profile in vCAC.)*
   
   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. Click **Next**.

10. Enter the **DNS Search Path** (such as testrollout.infobloxiPAMdemo.com), click **Add**, and then click **Next**.

11. Click **Finish**. The vSphere Client appears, showing your new customization specification in the table.

### vRA/vCAC Configuration Steps

A number of elements must be configured in your vRA/vCAC instance before use with the Infoblox IPAM Plug-In for VMware, including the following:

- vCO Endpoint Credentials;
- vCO Endpoints;
- A Fabric Group;
- A Machine Prefix;
- A Business Group;
- A new vSphere (vCenter) Reservation, including resources to provision VMs;
- Build Profiles;
- A Blueprint matching your VM template in vCenter;
- vRA/vCAC Service.

Your vRA/vCAC must be licensed before you can perform these configurations in vRA/vCAC.

### Creating vCenter and vCenter Orchestrator Endpoint Credentials

To enable communication with vRO/vCO by creating a vCO entry in vRA/vCAC, vCenter administrator endpoint credentials are necessary. Do the following:

1. In vRA/vCAC, choose **Infrastructure → Endpoints → Credentials**.
2. Click **New Credentials**.
3. In the **Name** field, type “vCenter”.
4. Enter the username and password.
5. Click the green check mark to save the settings.
6. Click **New Credentials** and fill in the fields as shown below. In the **Name** field, type “vCO”. Enter “vcoadmin” for the **Username** and “vcoadmin” for the **Password**.

![Credentials](image)

7. Click the green check mark to save the settings.

### Creating vCenter and vCenter Orchestrator Endpoints

When you use vRA/vCAC workflows from the Infoblox IPAM Plug-In, you must configure the vCenter Orchestrator, and vCenter, as endpoints in vRA/vCAC.

1. In vRA/vCAC, choose **Infrastructure → Endpoints → Endpoints**.
2. Choose **New Endpoint → Virtual → vSphere (vCenter)**.
3. Enter the required values for the following:
   - **Name**;
   - **Address**. Enter the url in the format `https://<ip_address>/sdk` for vCenter;
   - The **Credentials** field is automatically defined and cannot be selected;
4. Click **OK**.
5. After the vCAC Agent discovers the vCenter/ESXi resources, choose **New Endpoint → Orchestration → vCenter Orchestrator**.

![New Endpoint - vCenter Orchestrator](image)

6. Enter the required values for:
   - **Name**;
   - **Address**. Enter the url in the format `https://<ip_address>/vco` for vCO;
   - The **Credentials** field is automatically defined and cannot be selected;
7. Click **OK**.
8. Click **New Property**.
9. Type “VMware.VCenterOrchestrator.Priority” and set the value to “1”.
10. Click on the green check mark to save the settings.
11. Click OK. The new endpoint appears in the vCO Endpoints list.

Creating a Fabric Group

**Note:** Previous versions of vRA/vCAC termed the current feature an Enterprise Group.

Fabric groups are groups 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.

1. Click Infrastructure → Groups → Fabric Group.
2. Click New Fabric Group.
3. Enter the required value in the Name: field.
4. Enter one or more vCloud administrator accounts in the Fabric administrators: field. Press Enter for each account entry. This value is not immediately required but is advisable for group administration.
5. Select the resources (clusters, VMs...) to be managed by the group from the Compute resources: field.
6. Click OK.

Creating a Machine Prefix

The machine prefix is used for virtual machine naming, to help create names for VMs provisioned through vCAC. The prefixes are used in blueprints and business group settings. 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.

To create a prefix:
1. Click Infrastructure → Blueprints → Machine Prefixes.
2. Click New Machine Prefix and enter the values as shown below:
3. 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/vCAC 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 a tenant by the tenant administrator. Tenants may have different business groups in their organization.
1. Click **Infrastructure → Groups → Business Groups**.

2. Click **New Business Group** and fill in or select the following:
   - **Name** (required);
   - **Default machine prefix** (required);
   - **Active directory container** and **Group manager role** (if necessary);
   - **Send manager emails to** (required);
   - **Support role** and **User role** (if necessary);
   - **Custom properties** (if necessary).

3. Click **OK**. The new group appears in the Business Groups list.

### Viewing Assign Compute Resources

You can view the currently configured list of computer resources for vRA/vCAC by doing the following:

1. Click **Infrastructure → Compute Resources → Compute Resources**.

You can edit the resource, create new resource reservations (for information, see *Creating a Reservation*), view existing reservations, and view the virtual machines using the compute resources.

### Creating a Reservation

Each reservation consists of service resources, such as storage, memory allocations, and assignments to specific networks. When a user requests 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 a 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. You can copy settings from an existing resource reservation to create new ones. A reservation consists of four settings tabs: **Reservation information**, **Resources**, **Network** and **Alerts**.

1. Click **Infrastructure → Reservations → Reservations**. Each listed reservation will also reflect any currently active VMs’ memory and storage allocations.

2. Click **New Reservation → Virtual → vSphere (vCenter)**. The New Reservation page appears.

3. Click the **Reservation Information** tab.

4. Enter or select for the following required values:
• Compute resource;
• Name (of the new reservation);
• Tenant;
• Business group;
• Priority (sets the priority of the reservation—the lower the number, the higher the priority);

Other non-required but possibly helpful settings include the following:

• Copy from existing reservation (applies only to reservations of the same type; an existing vSphere reservation cannot be used for a new vCloud vApp reservation, for example);
• Reservation policy (if applicable, choose a reservation policy from the list);  
• Custom properties. (Can be Enabled or disabled by selecting the check box.)

5. Click the Resources tab and enter the values in the Memory and Storage fields. Under Memory, choose the desired amount from the This reservation selector.

6. Click on the green check mark to save the Storage parameters.

7. Click OK. The new reservation appears in the list.

Forcing Data Collection

Perform this procedure to ensure that vRA/vCAC fully discovers the VM templates and other resources needed to create blueprints and successfully create VMs.

To run data collection, do the following.

1. Click Infrastructure → Compute Resources → Compute Resources.

2. Right click on the compute resource and select Data Collection.

3. Click Request Now buttons in the Inventory and State sections. The “In queue” statuses display.

4. After a few minutes, click Refresh. Data collection settings appear.

5. If any data category shows a data collection setting of Off, select On.

6. Click OK to commit settings.
Creating a Blueprint

Ensure that a VM template exists in vCenter that matches the name for your Blueprint. (Using vSphere, you can clone or convert an existing VM to define a template, or clone a template to edit and create a new one.) This template will be selected during the creation of the blueprint to ensure that a new VM is created from it. You also use the machine prefix you created in Creating a Machine Prefix on page 19, and the customization specification created in the procedure Creating a Customization Specification in vCenter on page 16.

Perform the following steps to create a new blueprint for your vCAC workflow:

1. Click Infrastructure → Blueprints.
2. On the Blueprints tab, click New Blueprint.
3. Select Virtual → vSphere (vCenter) as the new blueprint type.
4. On the Blueprint Information tab, enter the blueprint (for example “Linux”).
5. Select the Shared Blueprint (can be shared across groups) check box.
6. Select the Machine prefix from the dropdown list (for information, see Creating a Machine Prefix on page 19);
7. Click the Build Information tab.
8. Select the aforementioned vCenter VM template to be used for your new blueprint. (If you know the template exists in vCenter, and it does not appear here, you may need to perform a Force Resource Discovery as described in Forcing Data Collection on page 20.)
9. Click OK. The new blueprint is completed.
10. Navigate to the newly created blueprint for your workflow, right-click on it and select Publish.

Creating Build Profiles

You create a separate build profile for each of the three methods of allocating an IP address to a VM:
- Static IP allocation (using the Create build profile for reserve an IP for vCAC VM workflow);
- Allocating from a network (using the Create build profile for reserve an IP for vCAC VM in network workflow);
- Allocating from an IP range (using the Create build profile for reserve an IP for vCAC VM in range workflow).

The current example describes how to execute any Build Profile workflow on an example of the Create build profile for Reserve an IP for vCAC VM workflow. You execute all other Infoblox Create Build Profile workflows the same way. The build profiles are required for operation of the Infoblox IPAM Plug-In with vCAC workflows, to ensure that VMs will receive the necessary IP addresses.

1. Log in to the vCenter Orchestrator client.
2. Choose Design mode.
3. On the Workflows tab, select <admin> → Library → IPAM → vCAC → Build Profiles → vCAC 6.x.
4. Right-click the Create Build Profile for Reserve an IP for vCAC VM workflow and choose Start workflow.
5. Enter the common parameters and click Submit.
6. The build profile for Reserve an IP for vCAC VM workflow is created in the Build Profiles tab in vRA/vCAC.

After you create the build profile, you need to edit its properties. Do the following:

7. Open vRA/vCAC and select Infrastructure → Blueprints → Build Profiles.
8. Select the created build profile and click Edit.
9. Set the Prompt user to “yes” for all custom properties starting with “Infoblox,” which you are going to specify in a vRA/vCAC request. You can also specify the value for each of the properties that should be constant in each vRA/vCAC request. The ‘stub’ properties define the workflows that are called during the creation of the VM, after which a new request is submitted to vRA/vCAC.

Note: Avoid changing the stub properties for any Build Profile workflows.

10. Click Ok.
Setting a Build Profile to a Blueprint

Perform the following steps to associate your new build profile to your blueprint:
In vRA/vCAC, select Infrastructure → Blueprints → Blueprints.
2. Open the Blueprint that you created in the previous procedure, Creating a Blueprint.
2. Click the Properties tab.
3. Select the build profile that uses the appropriate Infoblox IPAM plug-in workflow for your application.
4. Click OK.

Note: Plug-In users should always use one Infoblox Plug-In-created build profile per blueprint.

Creating Services and Adding them to the Catalog

vRA/vCAC provides a service catalog that more easily enables blueprints to be assigned to users and groups. The blueprint simply appears in the vRA/vCAC Service Catalog as a service that can be selected. To enable this, you create a new service, which is simply a container in the Service Catalog page that holds a blueprint.

1. Click Administration → Catalog Management → Services. The Services page appears, showing a list of all currently configured vRA/vCAC services.
2. Click the Add icon (+) to the right of Services, enter the name for the new service (such as, for example, “Linux-Service”) in the Name field, and select the Active status.
3. Click Add.
4. Click Administration → Catalog Management → Catalog Items.
   The Catalog Items pane appears, showing the list of completed blueprints. You select these blueprints to add to the catalog as the new service.
5. Under Actions (to the far right of the page), choose Configure in the row for the desired blueprint.

   The Configure Catalog Item pane appears, showing two tabs: Details and Entitlements. (The Entitlements tab in this context shows only the entitlements directly associated with the currently opened catalog item.)

6. In the Details page, for the Status dropdown, choose Active.
7. In the Service dropdown, choose the service you’ve created to associate the blueprint with, or to an existing vCAC service.

   Note: If desired, you can associate an icon graphic with the new vRA/vCAC service.

8. Click Update.
9. Click Administration → Catalog Management → Entitlements in the left pane.
10. Click the Add icon (+) to the right of Entitlements. The Add Entitlement page appears.
   a. Enter the Name;
   b. Select the Status;
   c. Select the Business Group;
   d. Select the cloud admin users or admin groups that will use the entitlement;
   e. Click Next.
11. Define the entitlement settings.
   a. Click the Add icon (+) to the right of **Entitled Services**. The Add Services to Entitlement dialog box appears. Enable the checkbox for any services needed for the new Entitlement and click **OK**.
   b. Click the Add icon (+) to the right of **Entitled Catalog Items**. The Add Catalog Items to Entitlement dialog box appears. (Note that if you are entitling an entire service then individual catalog items do not need to be added to the entitlement.)
      1. Select the **Service**, the **Type** (All, Cloud Machine, Physical Machine, Virtual Machine, Multi-Machine Service or vCD vApp) and choose from the **Apply this Policy to selected items** list if necessary, then click **OK**.
   c. Click the Add icon (+) to the right of **Entitled Actions**. The Add Actions to Entitlement dialog box appears. Enable the checkbox for any services needed for the new Entitlement and click **OK**.

   **Note:** Consult the VMware vRA/vCAC documentation for deeper explanations about Entitlement configuration.

12. Click **Add**. The new entitlement is added to the list.

---

**PERFORMING A vREALIZE AUTOMATION REQUEST**

To perform a Create a new VM request in vRA/vCAC, go to the Catalog tab in vRA/vCAC and click the **Request** button on the appropriate catalog item. The New Request page opens, showing all of the workflow settings for executing the request under the **Request Information** tab:

You choose between two methods of providing Network Properties for VM creation:

- Specify DHCP Options in NIOS from a Network object or Range object to apply to the new VM;
- Specify default values for Network Properties directly in the vCAC request, using a vRA/vCAC Build Profile.

To specify DHCP Options in NIOS, locate the desired Network object or Range object in NIOS, and open it for editing:
In NIOS, when you create a network, setting the Basic tab’s IPv4 DHCP Options values for that network or network range, including the DNS domain name and network prefix, ensures that the network data will be passed to the VM when the network gets used by the Infoblox IPAM Plug-In for VMware.

In a Create a New VM request, you may use the following properties to define default network properties:

- `Infoblox.IPAM.defaultGateway`
- `Infoblox.IPAM.defaultDnsSuffix`
- `Infoblox.IPAM.defaultDnsSearchSuffixes`
- `Infoblox.IPAM.defaultPrimaryDns`
- `Infoblox.IPAM.defaultSecondaryDns`
- `Infoblox.IPAM.defaultPrimaryWins`
- `Infoblox.IPAM.defaultSecondaryWins`

The precedence for whether NIOS DHCP options or default values are used depends on the vRA request type.

1. Requests for reserve an IP for vCAC VM in network:
   During the execution of this vRA/vCAC request, if DHCP options are not found in the specified network, the default values from the vRA request will be used;

2. Requests for reserve an IP for vCAC VM in range:
   During the execution of this vRA/vCAC request, if NIOS DHCP options are not found in the specified range, the request uses the DHCP options that are inherited from the parent network in NIOS. If DHCP options in the parent network also are not defined, the default values from the vRA/vCAC request will be used;

3. Requests for reserve an IP for vCAC VM:
   The user must specify default Network Properties in the vRA/vCAC request.

For reserve an IP for vCAC VM in network requests, you can specify the network from which an IP address will be allocated, by choosing from one out of two methods:

- By IP address and CIDR;
  To specify the network by IP address and CIDR, you use the following properties presented in the build profile:
  - `Infoblox.IPAM.netaddr`
  - `Infoblox.IPAM.cidr`

- Using the set of extensible attributes to search the network in NIOS.
  To find the network in NIOS by searching extensible attributes, set the Custom Property `Infoblox.IPAM.searchByEa` to True and provide a set of extensible attributes for search using the following properties:
  - `Infoblox.IPAM.searchEa1Name`
  - `Infoblox.IPAM.searchEa1Value`
  - `Infoblox.IPAM.searchEa1Comparison`
Performing a vRealize Automation Request

Infoblox User’s Guide For the Infoblox IPAM Plugin for VMware Version 2.4.2 (Rev. A)  23

— Infoblox.IPAM.searchEa10Name
— Infoblox.IPAM.searchEa10Value
— Infoblox.IPAM.searchEa10Comparison

You can use up to 10 extensible attributes for searching from within a vRA/vCAC request:

For the network in NIOS to be matched in EA searches, NIOS must contain the correct values in the network object’s Extensible Attributes configuration, as shown in the following figure.

Note: For more information about using Extensible Attributes in the Infoblox IPAM Plug-In for VMware, see Using Extensible Attributes in Infoblox IPAM Plug-In for VMware on page 29.

Attribute Search Example - Port Groups

You can use a vSphere port group name to allocate an IP address in the desired network and/or assign a port group to the vNIC of a created VM.

If you know only the name of the port group in vSphere, and don’t know the real network to which it is mapped in NIOS, set the Infoblox.IPAM.searchByEa custom property to True, and specify the name of the vSphere port group in extensible attributes for search. (Also see Customizing vRA/vCAC to Search by Extensible Attributes on page 27.) As an example:
In this case, an extensible attribute Port Group must exist in NIOS, and one or more network objects in NIOS also require the Port Group extensible attribute to contain the value equaling the specified port group name, and one or more network objects in NIOS also require the Port Group extensible attribute to contain the value equaling the specified port group name. The IP address of the created VM will be allocated from the matching network in NIOS. The specified port group name will be assigned to the vNIC of the created VM.

- If you specify the network by IP address and CIDR, the port group name from the Port Group extensible attribute of this network in NIOS will be assigned to the vNIC.
- If the Port Group extensible attribute is not specified for this network in NIOS, the default value of the port group name from the vRA/vCAC request will be used.
- If you use a DHCP range to allocate an IP address, the port group attribute from the parent network in NIOS will be used.
- If the Port Group extensible attribute is not specified for the parent network in NIOS, the default value of the port group name from the vRA/vCAC request will be used.
- If you don’t specify the default port group value and there is no Port Group extensible attribute in a network in NIOS, the port group name defined in the vRA/vCAC reservation will be used (the Network path).

If you want to assign the particular port group to the vNIC of the newly created VM, ensure that the appropriate Network Path exists in the vRA/vCAC Reservation used for creating VMs. Each reservation contains a reference to one or network paths, and allocates resources to VMs created under a specific vRA/vCAC request.

To manage which vCAC reservation will be used for new requests of a specific Blueprint, you use a Reservation Policy; otherwise, you cannot guarantee which reservation will be used for each successive request. Do the following:

- Create a Reservation Policy in vRA/vCAC (see Creating a Reservation on page 20).
- Assign the Reservation Policy to a Reservation.
- Assign the Reservation Policy to a Blueprint.

When you submit a new vCAC request for this Blueprint, the request uses the correct Reservation.

To use the Port Group extensible attribute through vRA/vCAC, create a new Build Profile and locate the Infoblox.IPAM.defaultPortGroup attribute in the Custom Properties dropdown menu; or open the Build Profile that you need to edit in vCAC (Infrastructure -> Blueprints -> Build Profiles and select the profile) and edit the infoblox.IPAM.defaultPortGroup attribute, which appears in the Custom Properties list:

This specifies a default Port Group in a created Build Profile.

Set the Prompt User flag to True to enable changes to the value of the Infoblox.IPAM.defaultPortGroup property at the time of a vRA/vCAC request.

**Customizing vRA/vCAC to Search by Extensible Attributes**

You can customize vRA/vCAC to provide a pull-down menu for users to choose a specific value before submitting a request to provision a VM. For example, you may want to provide a user with a pull down menu for the Country Extensible Attribute in which the user can select the Country value to be set to USA, Britain or France before submitting the VM provisioning request. To do so, you edit the Infoblox IPAM build profile and its associated Property Dictionary and Blueprint. To perform this task, do the following:

1. In vRA/vCAC, click Infrastructure -> Blueprints -> Build Profiles.
2. Open the Infoblox IPAM Build Profile for editing. (If you have not created this profile, go to Creating Build Profiles on page 21.)
3. Scroll down the Custom Properties list and locate the section of properties listed with the prefix Infoblox.IPAM.searchByEa as shown below:
4. Define the following properties.
   — Set the Infoblox.IPAM.searchByEa property to True;
   — Set the Infoblox.IPAM.searchEa1Name to Country;
   — Set the Infoblox.IPAM.searchEa1Comparison to EQUAL;
   — Set the Infoblox.IPAM.searchEa1Value to be empty.

5. Scroll down to the bottom of the page and click OK to save changes.

   Note: Extensible attributes support up to ten possible values at a time for searching, from ...Ea1 to ...Ea10.

6. Click Infrastructure → Blueprints → Property Dictionary.

7. Find the Infoblox.IPAM.searchEa1Value property and enter the following:
   — Display Name: Country
   — Control Type: Drop Down List

8. Click the green check mark to save the configuration.

9. In the new Property Dictionary's Property Attributes column, click Edit and enter the following values:
   — Type: Value List
   — Name: Country
   — Value: USA, Britain, France

10. Click the green check mark to save the configuration.

11. Click OK.

    Now, you edit the Blueprint.

12. Click Infrastructure → Blueprints → Blueprints.

13. Select your blueprint and click the Properties tab.

14. Click the New Property link and enter the following:
    
    Infoblox.IPAM.searchEa1Value

    a. Set this value to USA. This defines the default value that will appear in the dropdown menu.
    b. Check the check box for Prompt User. this enables the dropdown menu.

15. Click the green check mark to save the configuration.

16. Click OK to save the Blueprint.

The next time you request a VM through vCAC's Catalog, you will see the dropdown Country menu as part of the vCAC UI. You can use as many customizations as needed to use Infoblox extensible attributes for VM provisioning.
Using Extensible Attributes in Infoblox IPAM Plug-In for VMware

Extensible attributes (EA) are identifiers that you use to locate and track an IPAM object, e.g. a host, network, or range. They are typically manually created by admins in the NIOS Grid Manager. Each attribute tracks specific information about the object. These details provide searchable metadata for network, asset, and service management. For example, you can use attributes when searching for data in NIOS, filtering data, or grouping objects.

Another advantage of using the extensible attribute search capability in conjunction with the VMware platform is that users can change network properties, including but not limited to values such as the port group, in NIOS without having to make those changes in the IPAM VMware Plug-In or through vRA/vCAC. Network changes are then recognized by VMware through the Plug-In.

Prior to using an extensible attribute in a workflow, you must first create extensible attribute definitions in NIOS or customize one of the predefined NIOS extensible attributes. For more information, refer to “About Extensible Attributes” in the Infoblox NIOS Administrator Guide.

After you add or edit the extensible attribute definitions in NIOS, you reload the extensible attributes in the Infoblox IPAM plug-in. For details, see Reloading Extensible Attributes on page 29. After that, you can use the new attributes in the plug-in workflows. The Infoblox IPAM Plug-In for VMware extensible attributes accept two types of data: string and integer. The following table shows the typical mappings between NIOS EA types and plug-in values for extensible attributes.

<table>
<thead>
<tr>
<th>EA Type in NIOS</th>
<th>EA Type in Infoblox IPAM Plug-In for VMware</th>
</tr>
</thead>
<tbody>
<tr>
<td>String</td>
<td>String</td>
</tr>
<tr>
<td>List</td>
<td>String</td>
</tr>
<tr>
<td>Integer</td>
<td>Integer</td>
</tr>
<tr>
<td>Email</td>
<td>String</td>
</tr>
<tr>
<td>URL</td>
<td>String</td>
</tr>
<tr>
<td>Date</td>
<td>String (in ISO 8601-compliant format, e.g. &quot;2012-03-19T07:22:00Z&quot;)</td>
</tr>
</tbody>
</table>

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

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

- Basic Workflows (described in Basic IPAM Workflows on page 31);
- vCloud Director workflows (described in vCloud Director Workflows on page 40);
- AMQP workflows (described in AMQP Workflows on page 48);
- vCAC workflows (described in Overview of vCAC Workflows on page 54).

Each of these workflow types is available in the corresponding deployment option of the plug-in.

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

1. Log in to the VMware vCenter Orchestrator client and choose either Run or Design mode.
2. Click the Workflows tab.
3. Click Admin. The Infoblox IPAM Plug-In for VMware workflows are located in the respective folders.

Basic IPAM Workflows

Note: This information applies to all deployment types; the Basic workflows are called from the higher-level vCloud Director, AMQP and vCAC workflows.

The basic workflows set of the Infoblox IPAM Plug-In for VMware automates IPAM operations in a virtualized environment. They provide basic integration of the VMware environment with NIOS, used for running IPAM operations related to NIOS objects. In the basic IPAM workflows, you can use extensible attributes. For more information, see Extensive Attributes for Basic Workflows on page 32.

You access the Basic IPAM workflows in vCO from <Admin> –> Library –> IPAM. (The <Admin> entry reflects the actual administrator entry, such as vcoadmin@172.16.1.2. Your values will differ.) The basic workflows are as follows:

<table>
<thead>
<tr>
<th>Workflow Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reserve an IP</td>
<td>Reserves an IP address and creates either a host record, DNS records or a fixed address/reservation in the NIOS database with the specified static IP address. See Reserve an IP Workflow on page 33.</td>
</tr>
<tr>
<td>Reserve an IP in Network</td>
<td>Gets next available IP address from the specified network and reserves it. Creates either a host record, DNS records or a fixed address/reservation in the NIOS database. See Reserve an IP in Network Workflow on page 34.</td>
</tr>
<tr>
<td>Reserve an IP in Range</td>
<td>Gets next available IP address from the specified network range and reserves it. Creates either a host record, DNS records or a fixed address/reservation in the NIOS database. See Reserve an IP in Range Workflow on page 35.</td>
</tr>
<tr>
<td>Remove Host Record or A/AAAA/PTR/CNAME</td>
<td>Removes the host record or A/AAAA/PTR/CNAME record of the specified host or of multiple hosts from the NIOS database. See Remove Host Record or A/AAAA/PTR/CNAME Workflow on page 37.</td>
</tr>
<tr>
<td>Add Network</td>
<td>Creates a new IP network in the NIOS database. See Add Network Workflow on page 37.</td>
</tr>
<tr>
<td>Remove Network</td>
<td>Removes previously configured IP network or multiple networks from the NIOS database. See Remove Network Workflow on page 38.</td>
</tr>
<tr>
<td>Remove Fixed Address or Reservation</td>
<td>Removes a fixed IP address or reservation. See Remove Fixed Address or Reservation Workflow on page 39.</td>
</tr>
<tr>
<td>Restart Services</td>
<td>Restarts IPAM services. See Remove Fixed Address or Reservation Workflow on page 39.</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

### Extensive Attributes for Basic Workflows

In the Basic workflows, you can use extensible attributes (EA) for two purposes:

- Assign attribute values to objects created in the result of workflow executions. Some workflows, including `Add Network`, `Reserve an IP`, `Reserve an IP in Range`, and `Reserve an IP in Network`, enable you to set EA values for the object when it is created in NIOS through the workflow.
- Specify search criteria for IPAM objects, e.g. hosts, networks, or fixed addresses, typically for deletion. These attributes are called searchable extensible attributes.

A searchable extensible attribute consists of the following parameters:

- **Definition of the extensible attribute**...
- **Value of the extensible attribute**...
- **Type of the comparison for extensible attribute**...

In the workflow wizard, this corresponds to the following figure.

The **Definition of the extensible attribute**... field specifies the extensible attribute selected from the vCO inventory. You can specify up to ten extensible attributes for your search criteria. 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:

---

**Note:** By default, you can add up to 10 extensible attributes to the Infoblox IPAM Plug-In through vCO. You can add more attributes with the Infoblox Java Script API which has no restrictions on EA count.
You can also use the Basic workflows to build custom batch workflows in vCenter Orchestrator (vCO). For information about building batch workflows, refer to the vCO documentation.

**Required Extensible Attributes for Basic Workflows**

Before executing Basic workflows, the following extensible attributes must exist in NIOS, being manually created where necessary:

- CMP Type (String);
- Cloud API Owned (Enum [True, False]);
- Tenant ID (String);
- VM ID (String).

To manually run Reserve an IP, Reserve an IP in Network, and Reserve an IP in Range workflows, the user must specify values for the following EAs:

- Tenant ID;
- VM ID.

To manually run the Add Network workflow, the user must specify a value for the following EA:

- Tenant ID.

**Reserve an IP Workflow**

The Reserve an IP 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
- DNS records (A/AAAA/PTR/CNAME records)
- Fixed address/reservation

Using the Reserve an IP workflow, you can assign extensible attributes to the IPAM objects that you select for creation.

1. Log in to the vCenter Orchestrator client.
2. Choose Run mode.
3. On the Workflows tab, select the administrator listing (example: vCO Administrator@10.1.1.1) → Library → IPAM.
4. Right-click the Reserve an IP workflow and choose Start workflow.
5. Complete Step 1, Connection, to establish the connection to the NIOS IPAM appliance: click the Connection to the IPAM server field. In the left pane of the dialog box, click Infoblox IPAM and select the IP address of the Infoblox NIOS Grid member (there may be more than one). Click Select when finished.
6. Click Next.
7. In Step 2, Network, specify the IP address to be reserved. Then, click Next.
8. In Step 3 (Common parameters), do one of the following:
   - Create host record?
   - Create DNS record?
   - Create fixed address or reservation?

   a. If you want to create a host record, select Yes and enter the following:
      1. Select the DNS view (not required, but may be necessary);
      2. The Host name (FQDN) (this value is required),
      3. Whether to enable DHCP;
      4. The MAC Address or DUID if necessary;
      5. List of aliases for the host record in FQDN format;
   b. If you choose to create a DNS record, provide the necessary information:
Using Infoblox IPAM Plug-In for VMware Workflows

Select DNS Record to create:
For the new DNS record, select the type of records to create:

- A/AAAA
- A/AAAA/PTR

Choose the DNS view (if necessary); enter the Host name (FQDN) (this is a required value);

Select for a List of aliases for CNAME records (if necessary). You can also 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 Administrator Guide.)

If you choose to create a fixed address or reservation, provide the following:

1. A Name for the fixed address or reservation;
2. Select the Network view (if there is only the default, select the default network view);
3. Enter the MAC Address or DUID value (the only required value in this configuration step).

Click Next.

(Optional) In Step 4, Extensible attributes, 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 from workflow execution. You may specify
zero or more attributes to a limit of ten. For more information, see Reloading Extensible Attributes on page 29.

Specify if restarting services is needed (Yes or No). When you select Yes, services will be restarted when
necessary.

Click Submit.

Reserve an 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.

Instead of indicating a particular network in this workflow, you can specify extensible attributes to find networks that
match these attributes. The found networks are then used to obtain the next available IP address.

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

- Host record
- DNS records (A/AAAA/PTR/CNAME records)
- Fixed address/reservation

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

1. Log in to the vCenter Orchestrator client.
2. Choose Run mode.
3. On the Workflows tab, select the administrator listing (example: vCO Administrator@10.1.1.1) → Library → IPAM.
4. Right-click the Reserve an IP in Network workflow and choose Start workflow.
5. Complete Step 1, Connection, to establish the connection to the NIOS IPAM appliance: click the Connection to
the IPAM server field. In the left pane of the dialog box, click Infoblox IPAM and select the IP address of the
Infoblox NIOS Grid member (there may be more than one). Click Select when finished.
6. Click Next.
7. In Step 2, specify the network in one of the following ways:
   - Select Yes for the option Search networks by extensible attributes?, select the Network view, and click Next.
     (Go to Step 8 in this procedure for more information.)
   - or-
   - Select No for the option Search networks by extensible attributes?, and define the following:
     1. The IPv4 or IPv6 address of the network;
     2. The CIDR of the network range;
     3. Select the Network view (if there is only the default, select the default network view) and click Next.
8. If you choose to search networks by extensible attributes, complete Step 3, Search Networks.
a. Select the expected **Number of attributes** to search by, by numbers in quantity 1 through 10. If you select to search by more than one attribute, the wizard list updates to show multiple entries (**Extensible attribute #1...**) that you select for each in the configuration.

b. For more information, see *Reloading Extensible Attributes* on page 29.

9. When finished with attribute configuration, click **Next**.

10. In Step 4, **Common parameters**, do one of the following:
   - Create host record?
   - Create DNS record?
   - Create fixed address or reservation?

   a. If you want to create a host record, select **Yes** and enter the following:
      1. Select the **DNS view** (not required, but may be necessary);
      2. The **Host name (FQDN)** (this value is required),
      3. Whether to enable DHCP;
      4. The **MAC Address or DUID** if necessary;
      5. **List of aliases for the host record in FQDN format**;

   b. If you want to create a DNS record, provide the necessary information:
      1. Select **DNS Record to create**;
         For the new DNS record, select the type of records to create:
         - A/AAAA –or–
         - A/AAAA/PTR
      2. Choose the **DNS view** (if necessary); enter the **Host name (FQDN)** (this is a required value);
      3. Select for a **List of aliases for CNAME records** (if necessary). You can also 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 Administrator Guide*.)

   c. If you want to create a fixed address or reservation, provide the following:
      1. A **Name** for the fixed address or reservation;
      2. Select the **Network view** (if there is only the default, select the **default** network view);
      3. Enter the **MAC Address or DUID** value (the only required value in this configuration step).

11. Click **Next**.

12. (Optional) In Step 5, **Extensible attributes**, 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 from workflow execution. You may specify zero or more attributes to a limit of ten. For more information, see *Reloading Extensible Attributes* on page 29.

13. When finished with attribute configuration, click **Next**.

14. Specify if restarting services is needed (**Yes** or **No**). When you select **Yes**, services will be restarted when necessary.

15. Click **Submit**.

**Reserve an IP in Range Workflow**

Use the *Reserve an 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 also choose which IPAM object to create in this workflow:

- Host record
- DNS records (A/AAAA/PTR/CNAME records)
- Fixed address/reservation

Using the *Reserve an IP in Range* workflow, you can assign extensible attributes to the created objects.
1. Log in to the vCenter Orchestrator client.
2. Choose Run mode.
3. On the Workflows tab, select the administrator listing (example: vCO Administrator@10.1.1.1) → Library → IPAM.
4. Right-click the Reserve an IP in Range workflow and choose Start workflow.
5. Complete Step 1, Connection, to establish the connection to the NIOS IPAM appliance: click the Connection to the IPAM server field. In the left pane of the dialog box, click Infoblox IPAM and select the IP address of the Infoblox NIOS Grid member (there may be more than one). Click Select when finished.
6. Click Next.
7. In Step 2, Network range do the following:
   a. Specify the Starting address of the network range and the Ending address of the network range.
   b. Select the Network view (if there is only the default, select the default network view);
   c. Click Next.
8. In Step 3, Common parameters, do one of the following:
   • Create host record?
   • Create DNS record?
   • Create fixed address or reservation?
   a. If you want to create a host record, select Yes and enter the following:
      1. Select the DNS view (not required, but may be necessary);
      2. The Host name (FQDN) (this value is required),
      3. Whether to enable DHCP;
      4. The MAC Address or DUID if necessary;
      5. List of aliases for the host record in FQDN format;
   b. If you choose to create a DNS record, provide the necessary information:
      1. Select DNS Record to create;
         For the new DNS record, select the type of records to create:
         • A/AAAA –or–
         • A/AAAA/PTR
      2. Choose the DNS view (if necessary); enter the Host name (FQDN) (this is a required value);
      3. Select for a List of aliases for CNAME records (if necessary). You can also 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 Administrator Guide.)
   c. If you choose to create a fixed address or reservation, provide the following:
      1. A Name for the fixed address or reservation;
      2. Select the Network view (if there is only the default, select the default network view);
      3. Enter the MAC Address or DUID value (the only required value in this configuration step).
9. Click Next.
10. (Optional) In Step 4, Extensible attributes, 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 from workflow execution. You may specify zero or more attributes to a limit of ten. For more information, see Reloading Extensible Attributes on page 29.
   a. When finished with attribute configuration, click Next.
11. Specify if restarting services is needed (Yes or No). When you select Yes, services will be restarted when necessary.
12. Click Submit.

Remove Host Record or A/AAAA/PTR/CNAME Workflow

Use the Remove Host Record or A/AAAA/PTR/CNAME workflow to remove a host that you previously created in NIOS database. When you use this workflow, the NIOS appliance releases the IP address and removes IPAM records associated with the host:
Host record
A/AAAA/PTR/CNAME record

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 listing (example: vCO Administrator@10.1.1.1) → Library → IPAM.
4. Right-click the Remove Host Record or A/AAAA/PTR/CNAME workflow and choose Start workflow.
5. Complete Step 1, Connection, to establish the connection to the NIOS IPAM appliance: click the Connection to the IPAM server field. In the left pane of the dialog box, click Infoblox IPAM and select the IP address of the Infoblox NIOS Grid member (there may be more than one). Click Select when finished.
6. Click Next.
7. In Step 2, Remove criteria, define the record removal:
   a. Enter the parameters of a specific host name.
   b. If you choose to use extensible attributes, go to Step 8 below.
8. (Optional) If you wish to use Step 3, Extensible Attributes: as search criteria for removal of Host records or A/AAAA/PTR/CNAME records matching particular values, you may select zero or more attributes to a limit of ten. Each must be defined based on attributes that are already defined in NIOS. For more information, see Reloading Extensible Attributes on page 29.
   a. When finished with attribute configuration, click Next.
9. Specify if restarting services is needed (Yes or No). When you select Yes, services will be restarted when necessary.
10. 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 vCloud Director. 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. You can then use these extensible attributes in other workflows when searching for networks. For example, you can create a number of networks with identical extensible attributes and then run a Reserve an IP in Network workflow with the option to search for networks by the predefined extensible attributes. As the workflow automatically reserves available addresses in the found networks one by one, you do not have to manually check your NIOS appliance for free networks.

1. Log in to the vCenter Orchestrator client.
2. Choose Run mode.
3. On the Workflows tab, select the administrator listing (example: vCO Administrator@10.1.1.1) → Library → IPAM.
4. Right-click the Add Network workflow and choose Start workflow.
5. Complete Step 1, Connection, to establish the connection to the NIOS IPAM appliance: click the Connection to the IPAM server field. In the left pane of the dialog box, click Infoblox IPAM and select the IP address of the Infoblox NIOS Grid member (there may be more than one). Click Select when finished.
6. Click Next.
7. In Step 2, specify whether to use or not a template for the new network:
   For information about NIOS network templates, see the chapter Managing DHCP Templates in the NIOS Administrator Guide.
a. If you want to use a network template, select Yes, enter the template name, and click Next.
b. If you do not want to use a template, select No and click Next.

8. In Step 3, Network, specify the network parameters:
   a. Enter the IPv4 or IPv6 network address;
   b. Enter the CIDR of the network range such as 24 or 80. Enter only the numeric value without a forward slash (/);
   c. Select the Network view (if there is only the default, select the default network view);

9. Click Next.

10. In Step 4, Members, specify the NIOS Grid member(s) or Microsoft server(s) that will service the new network through DHCP. You will need to know the names of the NIOS Grid members or Microsoft servers.
   a. Under Assign a list of members:
      — if no DHCP service will be specified for the new network, select No and click Next;
      — If a DHCP server or servers will serve the network; select Yes;
   b. Click the List of members... field that contains the
   c. Select the Type of members setting: Infoblox or Microsoft;
   d. Click Next.

11. (Optional) In Step 5, Extensible attributes, 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 from workflow execution. You may specify zero or more attributes to a limit of ten. For more information, see Reloading Extensible Attributes on page 29.
   a. When finished with attribute configuration, click Next.

12. If necessary, specify DHCP options:
   a. If DHCP configuration options are needed, click Yes. Otherwise, retain the No default and click Next;
   b. If necessary, enter the expected Domain name (DNS suffix) for the new network (clicking in this field opens a dialog box. Enter the domain name information in the New value field, click Insert value and then click Accept. You may enter multiple values for domain names if needed);
   c. If necessary, enter the IP address of the DNS servers for the new network (clicking in this field opens a dialog box. Enter the IP address in the New value field, click Insert value and click Accept when finished. You may enter multiple values for DNS servers if needed);
   d. Enter the IP addresses for the routers... serving the new network. (Clicking in this field opens a dialog box. Enter the IP address in the New value field, click Insert value and click Accept when finished. You may enter multiple IP values if needed);
   e. If a NetBIOS name server is necessary for host configurations using DHCP, enter those values in the IP Addresses of the NetBIOS name servers... field.
   f. When finished with DHCP option configuration, click Next.

13. Specify if restarting services is needed (Yes or No). When you select Yes, services will be restarted when necessary.

14. 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.

1. Log in to the vCenter Orchestrator client.
2. Choose Run mode.
3. On the Workflows tab, select the administrator listing (example: vCO Administrator@10.1.1.1) → Library → IPAM.
4. Right-click the Remove Network workflow and choose Start workflow.
5. Complete Step 1, **Connection**, to establish the connection to the NIOS IPAM appliance: click the **Connection to the IPAM server** field. In the left pane of the dialog box, click **Infoblox IPAM** and select the IP address of the Infoblox NIOS Grid member (there may be more than one). Click **Select** when finished.

6. Click **Next**.

7. In Step 2, **Remove Criteria**, specify the network parameters:
   a. Enter the IPv4 or IPv6 network address;
   b. Enter the CIDR of the network range such as 24 or 80. Enter the numeric value without a forward slash (/);
   c. Select the Network view (if there is only the default, select the default network view);

8. Click **Next**.

9. (Optional) If using them for matching criteria for removal of a network, complete Step 5, **Extensible Attributes**. For more information, see **Reloading Extensible Attributes** on page 29.
   a. When finished with attribute configuration, click **Next**.

10. Specify if restarting services is needed (**Yes or No**). When you select **Yes**, services will be restarted when necessary.

11. Click **Submit**.

**Remove Fixed Address or Reservation 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 listing (example: vCO Administrator@10.1.1.1) → **Library** → **IPAM**.

4. Right-click the **Remove Fixed Address or Reservation** workflow and choose **Start workflow**.

5. Complete Step 1, **Connection**, to establish the connection to the NIOS IPAM appliance: click the **Connection to the IPAM server** field. In the left pane of the dialog box, click **Infoblox IPAM** and select the IP address of the Infoblox NIOS Grid member (there may be more than one). Click **Select** when finished.

6. Click **Next**.

7. In Step 2, **Remove criteria**, define the object removal.
   a. If you choose not to use extensible attributes to locate the fixed address or IP reservation object for deletion, do the following:
      1. Retain the **No** default setting;
      2. Enter the IPv4/IPv6 address assigned... value;
      3. Select the Network view if not using the default view.
      4. Click **Next** to go to Step 9 of this procedure.
   b. If you want to use extensible attributes to perform matching for the Fixed Address(es) or IP reservation object, do the following:
      1. Click **Yes**;
      2. Select the number to define one or more attributes to a limit of ten. The Start Workflow window will refresh to show a list of new attribute settings.
      3. Select the Network view if not using the default view.
      4. Click **Next** to go to Step 8 of this procedure.

8. (Optional) In Step 3, **Extensible Attributes**: define the attributes that will form the search criteria for removal of a fixed address or IP reservation. For more information, see **Reloading Extensible Attributes** on page 29.
   a. When finished with attribute configuration, click **Next**.

9. Specify if restarting services is needed (**Yes or No**). When you select **Yes**, services will be restarted when necessary.

10. Click **Submit**.
vCloud Director Workflows

Note: The vCloud Director workflows support only the host record type.

You can access the vCloud Director workflows in vCO from Admin → Library → IPAM → vCD. VCloud Director (vCD) workflows are used for running IPAM operations on VMs and vApps managed through vCD. These workflows combine the vCD and basic workflows to manage vCD objects and associated objects in NIOS.

Note: Due to possible IPAM conflicts, Infoblox does not recommend using the vCloud Director workflows together with the AMQP workflows. If you want to use the vCD workflows, make sure that you disable all blocking tasks on your vCloud Director. For more information, see Configuring vCloud Director for AMQP Operations on page 12. Also, remove any vCD notification subscriptions and stop the subscription listener workflows. For more information, see Create a vCloud Director Notification Subscription Workflow on page 50 and Start a Subscription Listener Workflow on page 52.

<table>
<thead>
<tr>
<th>Workflow Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create vApp with VM Networks configured via IPAM</td>
<td>Instantiates a vApp template as a new vApp. Defines IP addresses and host records for all network interfaces on the VMs in the new vApp. Updates vApp with the new network configurations obtained via IPAM. See Create a vApp with VM Networks Configured via IPAM Workflow on page 41.</td>
</tr>
<tr>
<td>Destroy vApp from IPAM</td>
<td>Deletes a vApp from the system and removes the IPAM host records associated with it. See Destroy vApp from IPAM Workflow on page 42.</td>
</tr>
<tr>
<td>Add an IP address to a new vNIC of an existing VM</td>
<td>Adds a new vNIC to the VM and allocates an IP address for it. See Add an IP Address to a New vNIC of an Existing VM Workflow on page 42.</td>
</tr>
<tr>
<td>Add a secondary IP address to an existing vNIC of a VM</td>
<td>Adds a secondary IP address to an existing vNIC of a VM. See Add a Secondary IP Address to an Existing vNIC of a VM Workflow on page 43.</td>
</tr>
<tr>
<td>Reserve an IP for VM</td>
<td>Adds a VM to the existing vApp and reserves a specified static IP address for the new VM. See Reserve an IP for VM Workflow on page 44.</td>
</tr>
<tr>
<td>Reserve an IP for VM in Network</td>
<td>Adds a VM to the existing vApp and reserves an IP address allocated from the specified network or port group. See Reserve an IP for VM Workflow on page 44.</td>
</tr>
<tr>
<td>Reserve an IP for VM in a Network Range</td>
<td>Adds a VM to the existing vApp and reserves an IP address allocated from the specified network range. See Reserve an IP for VM in a Network Range Workflow on page 45.</td>
</tr>
<tr>
<td>Remove VM and related Host records</td>
<td>Removes the VM and the related host and DNS CNAME records. See Remove VM and Related Host Records Workflow on page 46.</td>
</tr>
<tr>
<td>Change DNS names</td>
<td>Renames host records associated with VMs in the specified vApp. Optionally changes VMs computer names. See Change DNS Names Workflow on page 46.</td>
</tr>
<tr>
<td>Promote a new vNIC as primary</td>
<td>Changes the primary host record associated with the vNIC of a VM. See Promote a New vNIC as Primary Workflow on page 47.</td>
</tr>
</tbody>
</table>

Required Extensible Attributes for vCloud Director Workflows

Before executing vCloud Director workflows, the following extensible attributes must exist in NIOS, being manually created where necessary:

- **CMP Type (String)**
- **Tenant ID (String)**
- **VM ID (String)**
• VM Name (String)
• vCD Org (String)
• vCD App (String)
• vDC (String)

These attributes are implicitly used in the vCD workflows, and you do not specify values for them during workflow configuration.

Create vApp with VM Networks Configured via IPAM Workflow

This vCD workflow uses IPAM to instantiate a vApp from a template. It assigns an IP address and creates a host record for all network connections of a VM in this vApp. It also updates the vApp with the new network configurations obtained via IPAM. Note that obtaining the next available IP address and creating a host record with it is performed by a single addHost action within this workflow. For more information, see Infoblox IPAM Plug-In for VMware Best Practices on page 92.

In this workflow, you can choose between the old (i.e. inherited from the previous plug-in version) and new host name generation algorithms. The algorithms are as follows:

• Old algorithm (independent of the primary/non-primary status of vNIC):
  — For non-AMQP workflows: prefix + VM computer name + vNIC number + DNS suffix
  — For AMQP workflows: prefix + VM computer name+ vNIC number + VM number + DNS suffix

• New algorithm:
  — For primary vNIC: prefix (optional) + VM name + DNS suffix
  — For non-primary vNIC: prefix (optional) + VM name + vNIC number + DNS suffix

Note: If you want to apply the new algorithm, select Yes for the option Use actual virtual server name as DNS Hostname for primary vNIC in the common parameters.

In this workflow, you can choose one of the following options for assigning IP addresses:

• From networks predefined in the selected vApp template.
• From a specific network in the vApp.
• From a vApp network associated with a specific port group. In this case, you specify a port group to retrieve the list of networks associated to it, and then select a particular network from which to obtain the next available IP address. This is useful, for example, when multiple servers are spun up as part of a vApp and those servers will not all reside on the same subnet.

1. Log in to the vCenter Orchestrator client.
2. Choose Run mode.
3. On the Workflows tab, select the administrator listing (example: vCO Administrator@10.1.1.1) –> Library –> IPAM –> vCD.
4. Right-click the Create vApp with VM networks configured via IPAM workflow and choose Start workflow.
5. Complete Step 1:
   a. Select the Connection, to establish the connection to the NIOS IPAM appliance: click the Connection to the IPAM server field. In the left pane of the dialog box, click Infoblox IPAM and select the IP address of the Infoblox NIOS Grid member (there may be more than one).
   b. Select the Network view... that contains the IPAM network you want to use for the vApp provisioning;
   c. Select the DNS view... . Select the default view if no other is used in the network;
   d. Select Yes or No in the Use actual virtual server name as DNS Hostname for primary vNIC field.
   e. Enter the Prefix to the hostname;
   f. Enter the VM computer name.
6. Click Next.
7. Complete Step 2, Configure vApp:
Using Infoblox IPAM Plug-In for VMware Workflows

**Destroy vApp from IPAM Workflow**

Use the *Destroy vApp from IPAM* workflow to remove a previously created vApp. When you use this workflow, the vApp and its associated VMs are deleted from the vCloud Director. The workflow also removes the NIOS-side host records that are identified by the implicitly used extensible attributes of vApp, vOrg, and vDC.

1. Log in to the vCenter Orchestrator client.
2. Choose Run mode.
3. On the Workflows tab, select the administrator listing (example: vCO Administrator@10.1.1.1) → Library → IPAM → vCD.
4. Right-click the *Destroy vApp from IPAM* workflow and choose Start workflow.
5. In Step 1, Common parameters, Select the Connection, to establish the connection to the NIOS IPAM appliance: click the Connection to the IPAM server field. In the left pane of the dialog box, click Infoblox IPAM and select the IP address of the Infoblox NIOS Grid member (there may be more than one).
6. Select the vApp that you wish to destroy, and click Next.
7. Click Submit.

**Add an IP Address to a New vNIC of an Existing VM Workflow**

This workflow adds a new vNIC (virtual Network Interface Controller) to the VM and allocates an IP address for it in the NIOS database.

In this workflow, you can select how you want the IP address to be allocated:

- From the network associated with the vNIC.
- From a specific network in the vApp.
- From a network that is associated to a specific port group in the vApp.

1. Log in to the vCenter Orchestrator client.
2. Choose Run mode.
3. On the Workflows tab, select the administrator listing (example: vCO Administrator@10.1.1.1) → Library → IPAM → vCD.
4. Right-click the *Add an IP address to a new vNIC of an existing VM* workflow and choose Start workflow.
5. In Step 1, Common parameters, do the following:
   a. Click the Connection to the IPAM server field. In the left pane of the dialog box, click Infoblox IPAM and select the IP address of the Infoblox NIOS Grid member (there may be more than one). Click Select when finished.
   b. Select the Network view... (if there is only the default, select the default network view);
   c. Select the DNS view... (if there is only the default, select the default network view);
   d. Select Yes or No in the Use actual virtual machine name as DNS hostname field.
   e. Enter the Prefix to the Hostname.
   f. Click Next to continue.
6. In Step 2, Select VM, select the VM to create the new IP address by clicking the Not Set value in the Virtual machine field. The Select VM dialog box appears. Click vCloud Director in the left pane and select the VM from the hierarchical list, then click Select.

7. Configure how an IP address will be allocated to the vNIC for the VM. Do one of the following:
   a. If you want the IP to be assigned from a specific network in the vApp, select No for the option Use vApp network associated with the port group?, select the network, and click Next.
   – or –
   b. If you want the IP to be assigned from a network associated to a specific port group in the vApp, select Yes for the option Use vApp network associated with the port group?, select the port group, select one of the associated networks, and click Next.

8. Specify if restarting services is needed (Yes or No). When you select Yes, services will be restarted when necessary.

9. Click Submit.

Add a Secondary IP Address to an Existing vNIC of a VM Workflow

This workflow adds a secondary IP address to an existing vNIC of a VM. In this workflow, you can select how you want the IP address to be allocated:

- From the network associated with the vNIC.
- From a specific network in the vApp.
- From a network that is associated to a specific port group in the vApp.

1. Log in to the vCenter Orchestrator client.
2. Choose Run mode.
3. On the Workflows tab, select the administrator listing (example: vCO Administrator@10.1.1.1) –> Library –> IPAM –> vCD.
4. Right-click the Add a secondary IP address to an existing vNIC of a VM workflow and choose Start workflow.
5. In Step 1, Common parameters, do the following:
   a. Click the Connection to the IPAM server field. In the left pane of the dialog box, click Infoblox IPAM and select the IP address of the Infoblox NIOS Grid member (there may be more than one). Click Select when finished.
   b. If there is only the default, select the default network view;
   c. Select the DNS view... (if there is only the default, select the default network view);
6. In Step 2, Select VM’s vNIC, choose the VM by clicking the Not Set value in the Virtual machine field. The Select VM dialog box appears. Click vCloud Director in the left pane and select the VM from the hierarchical list, then click Select.
7. The vNIC field appears in the wizard page. Select the desired vNIC from the dropdown list.
   a. Configure the vNIC in one of the following ways:
      1. If you want the IP address to be allocated from the network assigned to the vNIC, select Yes for the option Use the networks assigned to the vNIC? and click Next.
      2. If you want the IP to be allocated from a specific network in the vApp, select No for the option Use vApp network associated with the port group?, select the network, and click Next.
      3. If you want the IP to be allocated from a network associated to a specific port group in the vApp, select Yes for the option Use vApp network associated with the port group?, select the port group, select the network from the vApp network name field, and click Next.
8. Specify if restarting services is needed (Yes or No). When you select Yes, services will be restarted when necessary.
9. Click Submit.

**Reserve an IP for VM Workflow**

This workflow adds a VM to the existing vApp and reserves an IP address for the new VM using the specified static IP. You can reserve an IP address for each vNIC of the VM.

1. Log in to the vCenter Orchestrator client.
2. Choose Run mode.
3. On the Workflows tab, select the administrator listing (example: vCO Administrator@10.1.1.1) → Library → IPAM → vCD.
4. Right-click the Reserve an IP for VM workflow and choose Start workflow.
5. Complete Step 1, Common parameters:
   a. Enter the NIOS appliance’s IP address in the Connection to the IPAM Server field;
   b. Enter the DNS View…;
   c. Choose Yes or No for the Use actual virtual machine name as DNS Hostname? setting;
   d. Enter the Prefix to the Hostname;
   e. Enter a comment if necessary.

**Note:** For the DNS hostname generation algorithm, see Create vApp with VM Networks Configured via IPAM Workflow on page 41.

6. Click Next.
7. In Step 2, select an existing vApp.
8. Click Next.
9. In Step 3, configure the VM:
   a. Enter the Virtual machine template (this can be found in the vCenter VM templates list);
   b. Enter the Virtual machine name;
   c. If necessary, enter the VM computer name;
10. Click Next.
11. In Step 4, configure the vNIC for the VM:
    a. Enter the VApp network to connect NIC 0 to (this value is a string);
    b. Enter the IPv4/IPv6 address assigned to the NIC 0 value;
12. Click Next.
13. If there are several vNICs for the VM, repeat the above steps for each of them.
14. Specify if restarting services is needed (Yes or No). When you select Yes, services will be restarted when necessary.
15. Click Submit.

**Reserve an IP for VM in Network Workflow**

This workflow adds a VM to the existing vApp and reserves an IP address for the new VM from the specified network or a network associated to a specific port group. You can reserve an IP address for each vNIC of the VM.

Log in to the vCenter Orchestrator client.
1. Choose Run mode.
2. On the **Workflows** tab, select the administrator listing (example: vCO Administrator@10.1.1.1) → **Library** → **IPAM** → **vCD**.

3. Right-click the **Reserve an IP for VM in Network** workflow and choose **Start workflow**.

4. Complete Step 1, **Common parameters**:
   a. Set the **Connection to the IPAM server** field. In the left pane of the dialog box, click **Infoblox IPAM** and select the IP address of the Infoblox NIOS Grid member (there may be more than one). Click **Select** when finished.
   b. Select the **Network view**... (if there is only the default, select the **default** network view);
   c. Select the **DNS view**... (if there is only the default, select the **default** network view);

   **Note:** For the DNS hostname generation algorithm, see *Create vApp with VM Networks Configured via IPAM Workflow* on page 41.

5. Click **Next**.

6. In Step 2, select an existing vApp.

7. Click **Next**.

8. In Step 3, configure the VM:
   a. Enter the **Virtual machine template** (this can be found in the vCenter VM templates list);
   b. Enter the **Virtual machine name**;
   c. If necessary, enter the **VM computer name**;

9. Click **Next**.

10. In Step 4, configure how an IP address will be allocated to the vNIC for the VM. Do one of the following:
    a. If you want to specify a particular network from which to obtain the IP address, select **No** for the option **Use vApp network associated with the port group**, select the network, and click **Next**.
    b. If you want to specify the network based on the port group, select **Yes** for the option **Use vApp network associated with the port group**, select the port group, select one of the associated networks, and click **Next**.

11. If the VM uses two or more NICs, repeat the above steps for each.

12. Specify whether restarting of DHCP services is needed (**Yes** or **No**). For most record and object creation operations, select **No**. If you select **Yes**, the DHCP service will be restarted when necessary.

13. Click **Submit**.

**Reserve an IP for VM in a Network Range Workflow**

This workflow adds a VM to the existing vApp and reserves an IP address for the new VM from the specified network range. You can reserve an IP address for each vNIC of the VM.

1. Log in to the vCenter Orchestrator client.

2. Choose **Run** mode.

3. On the **Workflows** tab, select the administrator listing (example: vCO Administrator@10.1.1.1) → **Library** → **IPAM** → **vCD**.

4. Right-click the **Reserve an IP for VM in Network range** workflow and choose **Start workflow**.

5. Complete Step 1, **Common parameters**:
   a. Set the **Connection to the IPAM server** field. In the left pane of the dialog box, click **Infoblox IPAM** and select the IP address of the Infoblox NIOS Grid member (there may be more than one). Click **Select** when finished.
   b. Select the **Network view**... (if there is only the default, select the **default** network view);
   c. Select the **DNS view**... (if there is only the default, select the **default** network view);
   d. If necessary, click **Yes** to enable the **Use actual virtual machine name as DNS hostname** setting, and enter the value in the **Prefix to the hostname** field.
Using Infoblox IPAM Plug-In for VMware Workflows

Note: For the DNS hostname generation algorithm, see Create vApp with VM Networks Configured via IPAM Workflow on page 41.

6. Click Next.
7. In Step 2, select the vApp for which the VM is a member.
8. Click Next.
9. In Step 3, Configure VM, configure the VM's Virtual machine name and the VM computer name.
10. Click Next.
11. In Step 4, VM vNICs, configure the vNIC for the VM;
   a. In the vApp network to connect the NIC, field, select the vApp network from the drop-down list.
   b. In the IP range for the NIC... field, select the network range from which the IP address will be allocated.
12. Click Next.
13. If there are several vNICs for the VM, repeat Step 4 for each of them.
14. Specify if restarting services is needed (Yes or No). When you select Yes, services will be restarted when necessary.
15. Click Submit.

Remove VM and Related Host Records Workflow

This workflow removes the specified VM and the related host records from the NIOS database. The host records to remove are identified implicitly by the predefined extensible attributes VM, vApp, vDC, and vOrg.

1. Log in to the vCenter Orchestrator client.
2. Choose Run mode.
3. On the Workflows tab, select the administrator listing (example: vCO Admin@10.1.1.1) → Library → IPAM → vCD.
4. Right-click the Remove VM and related Host records workflow and choose Start workflow.
5. Complete Step 1, Common Parameters:
   a. Connection to the IPAM server (click the Not Set link to select the Infoblox IPAM server);
   b. Enter the Virtual machine (click the Not Set link to select the managed VM);
   c. Select the DNS view (if necessary);
   d. Click Next.
6. Click Submit.

Change DNS Names Workflow

This workflow renames the host records associated with VMs in the specified vApp. Optionally, you can change the hostname prefix and the VMs computer names.

1. Log in to the vCenter Orchestrator client.
2. Choose Run mode.
3. On the Workflows tab, select the administrator listing (example: vCO Administrator@10.1.1.1) → Library → IPAM → vCD.
4. Right-click the Change DNS Names workflow and choose Start workflow.
5. Complete Step 1, Common Parameters:
   a. Connection to the IPAM server (click the Not Set link to select the Infoblox IPAM server);
   b. Select the DNS view... (if there is only the default, select the default network view);
   c. Select Yes or No in the Use actual virtual machine name as DNS hostname field;
   d. Enter the Prefix to the Hostname (not required);
1. Log in to the vCenter Orchestrator client.
2. Choose Run mode.
3. On the Workflows tab, select the administrator listing (example: vCO Administrator@10.1.1.1) → Library → IPAM → vCD.
4. Right-click the Promote a new vNIC as primary workflow and choose Start workflow.
5. Complete Step 1., Common Parameters:
   a. Connection to the IPAM server (click the Not Set link to select the Infoblox IPAM server);
   b. Select the DNS view... (if there is only the default, select the default network view);
   c. Select Yes or No in the Use actual virtual machine name as DNS hostname field;
   d. Enter the Prefix to the Hostname (not required);
   e. Click Next to continue.
6. You must specify the same hostname generation algorithm as at VM creation to ensure the same hostname scheme for the associated host records. For hostname generation algorithm, see Create vApp with VM Networks Configured via IPAM Workflow on page 41.
7. Click Next.
8. In Step 2, select the virtual machine.
9. Select the vNIC that you want to promote as primary.
10. Click Next.
11. Specify if restarting services is needed (Yes or No). When you select Yes, services will be restarted when necessary.
12. Click Submit.

AMQP Workflows

The AMQP workflows are used to handle blocking tasks on vCloud Director (shown in the figure below), including:
- Instantiating a vApp from a template
• Deleting a vApp
• Recomposing a vApp, i.e adding or removing VMs to/from the vApp
• Deleting a network
• Modifying a VM, which includes:
  — Changing the primary vNIC
  — Adding or removing a vNIC
  — Changing the IP address
  — Changing the MAC address

The following figure shows the list of blocking task workflows.

![Blocking Tasks](image)

The Infoblox IPAM AMQP package contains the following types of workflows:

• Common workflows – Use these workflows to set up subscriptions to vCD blocking tasks which trigger specific Infoblox IPAM workflows.
• Workflows triggered by policies – These workflows are automatically triggered by the vCO policies according to the subscriptions that you have set up with the help of the aforementioned common workflows.
• Helper workflows – Utility workflows.

You can access the common workflows from Library → IPAM vCD Notification Support on Blocking Tasks.

<table>
<thead>
<tr>
<th>Workflow Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create a vCloud Director notification subscription</td>
<td>Creates a vCD notification subscription by using the AMQP configuration from vCD. See Create a vCloud Director Notification Subscription Workflow on page 50.</td>
</tr>
<tr>
<td>Remove a vCloud Director notification subscription</td>
<td>Removes a previously created vCD subscription and its queues. Cancels dependent workflows. See Remove a vCloud Director Notification Subscription Workflow on page 52.</td>
</tr>
<tr>
<td>Start a subscription listener</td>
<td>Starts a looping workflow waiting for messages from the specified subscription created with the workflow Create a vCloud Director notification subscription and then runs the workflow runner which converts a message to vCD inputs and passes these to the specified workflow. See Start a Subscription Listener Workflow on page 52.</td>
</tr>
<tr>
<td>Stop a subscription listener</td>
<td>Cancels the workflow listening for vCD messages. See Stop a Subscription Listener Workflow on page 52.</td>
</tr>
<tr>
<td>Workflow runner</td>
<td>A utility workflow started by an AMQP policy or by a looping workflow waiting for a message. Gets all relevant objects from an AMQP message and passes them to the specified workflow.</td>
</tr>
</tbody>
</table>
You can access the workflows to be triggered by the policies from Library → IPAM vCD Notification Support on Blocking Tasks → Workflows to be triggered by the policies.

<table>
<thead>
<tr>
<th>Workflow Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPAM Provision All VMs in new vApp on blocking Task</td>
<td>A workflow to be triggered from vCloud Director on vApp instantiation from template. See IPAM Provision All VMs in New vApp on Blocking Task Workflow on page 53.</td>
</tr>
<tr>
<td>IPAM Sync on vApp Recomp</td>
<td>A workflow to be triggered from vCloud Director on vApp changes. See IPAM Sync on vApp Recomp Workflow on page 53.</td>
</tr>
<tr>
<td>IPAM Sync on VM Modification</td>
<td>A workflow to be triggered from vCloud Director on VM modifications. See IPAM Sync on VM Modification Workflow on page 53.</td>
</tr>
<tr>
<td>IPAM Delete vApp</td>
<td>Destroys a vApp from the system and removes the IPAM host associated with it. See IPAM Delete vApp Workflow on page 53.</td>
</tr>
<tr>
<td>IPAM Delete Network</td>
<td>A workflow that is triggered by vCloud Director and removes a network from the IPAM. See IPAM Delete Network Workflow on page 53.</td>
</tr>
</tbody>
</table>

You can access the Helper workflows from Library → IPAM vCD Notification Support on Blocking Tasks → Helper.

<table>
<thead>
<tr>
<th>Workflow Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change VM Names</td>
<td>Renames the VM name and then changes the VM computer name.</td>
</tr>
<tr>
<td>Configure vCloud Director AMQP subscription</td>
<td>Creates an AMQP broker host, declares an exchange, creates a queue, binds it, and creates a subscription.</td>
</tr>
<tr>
<td>Provision new VM via IPAM</td>
<td>Assigns a unique name to the VM and creates host records for each vNIC of the VM in IPAM.</td>
</tr>
</tbody>
</table>

### Configuring an AMQP Workflow

To configure an Infoblox AMQP workflow to run on specific vCD blocking task, perform the following steps:

1. Enable the vCD blocking task on which the AMQP workflow will be triggered. For details, see Configuring vCloud Director for AMQP Operations on page 12.

2. Create and run a vCO subscription for notifications received upon the occurrence of the configured blocking task. For this purpose, use the dedicated Infoblox AMQP workflow Create a vCloud Director Notification Subscription. In the notification subscription, you specify the following items that will be bound to the configured vCD blocking task:
   - Blocking task operation type;
   - Event type;
   - Infoblox plug-in AMQP workflow to be triggered.
   For details, see Create a vCloud Director Notification Subscription Workflow on page 50.

3. Create and run a vCO subscription listener by using the dedicated Infoblox AMQP workflow. For details, see Start a Subscription Listener Workflow on page 52.

The following sections provide detailed descriptions for AMQP workflows of the Infoblox IPAM Plug-In for VMware. Only the common workflows and those triggered by policies are described.

### Create a vCloud Director Notification Subscription Workflow

To bind AMQP messaging with an IPAM workflow, first create a notification for blocking tasks by using the Infoblox plug-in workflow Create a vCloud Director Notification Subscription.

1. In the VMware vCenter Orchestrator client, choose Run mode.
2. Choose the **Workflows** tab.

3. Under **IPAM vCD Notification Support on Blocking Tasks**, right-click **Create a vCloud Director Notification Subscription** and select **Start Workflow**.

4. In Step 1a, do the following:
   - Specify the queue and subscription name.
   - Specify the vCloud Director host.
   - Enter the password for the AMQP server: for example, *guest*.
   - Under **Create a Broker?** select **Yes**.
   - Click **Next**.

5. In Step 2, do the following:
   - In Step 2a, **Operation Success**, click **No** and click **Next**.
   - In Step 2b, **Organization**, click **No** and click **Next**.
   - In Step 2c, **User**, click **No** and click **Next**.

6. In Step 2d, **Blocking Task Operation Type**, do the following:
   - Click **Yes**.
   - Click in the **Blocking Task Operation Type** field.
   - In the Chooser, select the blocking task operation type depending on the workflow to trigger and the pre-enabled vCD blocking task.

<table>
<thead>
<tr>
<th>Blocking Task Operation Type</th>
<th>Used for Workflow</th>
</tr>
</thead>
<tbody>
<tr>
<td>vdcInstantiateVapp</td>
<td>IPAM Provision All VMs in New vApp on Blocking Task</td>
</tr>
<tr>
<td>vdcDeleteVapp</td>
<td>IPAM Delete vApp</td>
</tr>
<tr>
<td>vdcRecomposeVapp</td>
<td>IPAM Sync on vApp Recomp Workflow</td>
</tr>
<tr>
<td>vappUpdateVm</td>
<td>IPAM Sync on VM Modification</td>
</tr>
<tr>
<td>networkDelete</td>
<td>IPAM Delete Network</td>
</tr>
</tbody>
</table>

   - Click **Select** and click **Next**.

7. In Step 2e, **Event Type**, do the following:
   - Click **Yes**.
   - Click in the **Event Type** field.
   - In the Chooser, select *com/vmware/vcloud/event/blockingtask/create*. 
— Click **Select** and click **Next**.

2. In Step 2f, Entity Type, click **No** and click **Next**.

3. In Step 3a, Workflow, do the following:
   — Click in the **Workflow** field.
   — In the Chooser, type **ipam** in the **Filter** field. A list of the Infoblox AMQP workflows that can be triggered appears in the Chooser. (Pressing spacebar here displays the library of vCD workflows.)
   
   — Choose the workflow to be triggered.
   — Click **Select**.

4. Click **Submit**.

**Remove a vCloud Director Notification Subscription Workflow**

When you no longer need a notification subscription, remove it by using the Infoblox workflow **Remove a vCloud Director notification subscription**.

**Start a Subscription Listener Workflow**

1. In the VMware vCenter Orchestrator client, choose **Run** mode.

2. Click the **Workflows** tab.
3. Under **IPAM vCD Notification Support on Blocking Tasks**, right-click **Start a subscription listener workflow** and choose **Start Workflow**.

4. Click in the **Subscription** field.
   A list of previously created subscriptions appears.

5. Choose the required subscription and click **Select**.

6. Click **Submit**. After a moment, the new listener appears in the workflows list with a Pause icon, indicating that the listener is waiting for an event to trigger a notification.

The vApps are instantiated in vCloud Director. Once a workflow is started in vCloud Director, the listener for a particular workflow activates in the vCenter Orchestrator client display and you can watch its execution.

**Stop a Subscription Listener Workflow**

When you no longer need a subscription listener, stop it by using the Infoblox workflow **Stop a Subscription Listener**.

---

**IPAM Provision All VMs in New vApp on Blocking Task Workflow**

This workflow is triggered when a vApp is instantiated on vCD. Prerequisites:

- Blocking task **Instantiate vApp from Template** is enabled on vCD. For details, see Configuring vCloud Director for AMQP Operations on page 12.
- Notification subscription is created on vCO and the blocking task operation type **vdcInstantiateVapp** is selected in the subscription. See Create a vCloud Director Notification Subscription Workflow on page 50.

**IPAM Sync on vApp Recomp Workflow**

This workflow is triggered from vCloud Director on the following vApp changes:

- New VMs are added to a vApp
- VMs are removed from a vApp

Prerequisites:

- Blocking task **Add, Move or Delete Virtual Machines** from vApp is enabled on vCD. For details, see Configuring vCloud Director for AMQP Operations on page 12.
- Notification subscription is created on vCO and the blocking task operation type **vdcRecomposeVapp** is selected in the subscription. See Create a vCloud Director Notification Subscription Workflow on page 50.
IPAM Sync on VM Modification Workflow

This workflow is triggered from vCloud Director on the following VM modifications:

- Add vNIC
- Remove vNIC
- Change primary vNIC
- Change MAC address of the vNIC
- Change IP address of the vNIC

Prerequisites:

- Blocking task Modify Virtual Machine Configuration is enabled on vCD. For details, see Configuring vCloud Director for AMQP Operations on page 12.
- Notification subscription is created on vCO and the blocking task operation type vappUpdateVm is selected in the subscription. For details, see Create a vCloud Director Notification Subscription Workflow on page 50.

IPAM Delete vApp Workflow

This workflow destroys a vApp from the system and removes the associated IPAM host.

Prerequisites:

- Blocking task Delete vApp is enabled on vCD. For details, see Configuring vCloud Director for AMQP Operations on page 12.
- Notification subscription is created on vCO and the blocking task operation type vdcDeleteVapp is selected in the subscription. For details, see Create a vCloud Director Notification Subscription Workflow on page 50.

IPAM Delete Network Workflow

This workflow is triggered by vCloud Director and removes the network from the IPAM server.

Prerequisites:

- Blocking task Delete Network is enabled on vCD. For details, see Configuring vCloud Director for AMQP Operations on page 12.
- Notification subscription is created on vCO and the blocking task operation type networkDelete is selected in the subscription. For details, see Create a vCloud Director Notification Subscription Workflow on page 50.

Overview of vCAC Workflows

The vCAC package of the Infoblox IPAM Plug-In for VMware includes the following types of workflows:

- Configuration Workflows (see vCAC Configuration Workflows below);
- Workflows for creating Build Profiles (see Creating Build Profiles on page 21);
- Workflows for commissioning and decommissioning of vCAC virtual machines (see Workflows for Commissioning and Decommissioning of Virtual Machines on page 57).

The configuration workflows are used to create/update/verify/remove vCAC Infrastructure Administration hosts in the Inventory tab of the vCloud Orchestrator client. You must create an vCAC Infrastructure Administration host instance before executing vCAC workflows for creating build profiles and for commissioning and decommissioning of vCAC virtual machines.

vCAC Configuration Workflows

You access the vCAC configuration workflows in vCO from <admin> → Library → IPAM → vCAC → Configuration. (The <Admin> entry reflects the actual administrator entry, such as vcoadmin@172.16.1.2. Your values will differ.)

vCAC configuration workflows include the following:
Add a vCAC Host Wrapper Workflow

This workflow is used to add a vCAC Infrastructure Administration host to the vCO inventory. This workflow is mandatory because in order to run the reservation workflows, this host must be in inventory.

1. Log in to the vCenter Orchestrator client.
2. Choose Design mode.
3. On the Workflows tab, select Library → IPAM → vCAC → Configuration.
4. Right-click the Add a vCAC host wrapper workflow and choose Start workflow.
5. Enter the Common parameters: (required values listed below)
   a. Host's name (for example, “IaaS”);
   b. The Host address (in IP or FQDN form, for example “vm.test.com”);
   c. Automatically install SSL certificate (recommended setting: Yes)
   d. Connection timeout and Operation timeout (Infoblox recommends retaining the default values in each field);
   e. Session mode;
   f. Authentication user name (for example, “Administrator”) and Authentication password;
   g. Domain for NTLM authentication (support for NT Lan Manager challenge-response authentication).
6. Click Submit.

Update a vCAC Host Wrapper Workflow

This workflow is used to update the vCAC Infrastructure Administration host connection.

1. Log in to the vCenter Orchestrator client.
2. Choose Design mode.
3. On the Workflows tab, select Library → IPAM → vCAC → Configuration.
4. Right-click the Update a vCAC host wrapper workflow and choose Start workflow.
5. Enter the Common parameters: (required values listed below)
   a. Select the vCloud Automation Center host instance;
   b. Host's name (for example, “IaaS”);
   c. The Host address (in IP or FQDN form, for example “vm.test.com”);
d. **Session mode:**
e. **Authentication user name** (for example, “Administrator”) and **Authentication password:**
f. **Domain for NTLM authentication** (support for NT Manager challenge-response authentication).

6. Click **Submit.**

**Validate a vCAC Host Wrapper Workflow**

This workflow is used to validate connections to the vCAC Infrastructure Administration at any time.

1. Log in to the vCenter Orchestrator client.
2. Choose **Design** mode.
3. On the **Workflows** tab, select **Library → IPAM → vCAC → Configuration.**
4. Right-click the **Validate a vCAC host wrapper workflow** and choose **Start workflow.**
5. In the **Common parameters** page, click the **vCloud Automation Center host instance value** to select the host from the Inventory, then click **Submit.**
6. Enter common parameters and click **Submit.**

**Install vCO Customization Wrapper**

This workflow is an Infoblox-created wrapper workflow. It includes customized state change workflow stubs and vCO menu operation workflows. This wrapper installs an Orchestrator customization including customized state change workflow stubs and Orchestrator menu operation workflows.

1. Log in to the vCenter Orchestrator client.
2. Choose **Design** mode.
3. On the **Workflows** tab, select **Library → IPAM → vCAC → Configuration → Install vCO customization Wrapper.**
4. Right-click the **IPAM → vCAC → Configuration → Install vCO customization Wrapper workflow** and choose **Start workflow.**
5. In the **Common Parameters** page, click the **The vCloud Automation Center host instance field.**
6. In the Select Host window, click the top vCAC Infrastructure Administration entry in the left pane’s hierarchical list. The list of current vCAC VM hosts appears.
7. Select the desired host to configure and click **Select.**
8. Select the **Yes** or **No** settings for the remaining stub parameters and click **Submit.**

**Remove vCO Customization Wrapper**

You use this workflow to remove vCO customization wrappers that may have been previously created by other admins.

1. Log in to the vCenter Orchestrator client.
2. Choose **Design** mode.
3. On the **Workflows** tab, select **Library → IPAM → vCAC → Configuration → Remove vCO customization Wrapper.**
4. In the Common Parameters page, click the **The vCloud Automation Center host instance field.**
5. In the Select Host window, click the top vCAC Infrastructure Administration entry in the left pane’s hierarchical list. The list of current vCAC VM hosts appears.
6. Select the desired host from which to remove vCO Customizations and click **Select.**
7. Click **Submit.**

**Remove a vCAC Host Wrapper**

Remove a vCAC Infrastructure Administration host from the vCO inventory.

1. Log in to the vCenter Orchestrator client.
2. Choose Design mode.
3. On the Workflows tab, select Library → IPAM → vCAC → Configuration → Remove a vCAC Host Wrapper.
4. In the Common Parameters page, click the The vCloud Automation Center host instance field.
5. In the Select Host window, click the top vCAC Infrastructure Administration entry in the left pane's hierarchical list. The list of current vCAC VM hosts appears.
6. Select the desired host to remove and click Select.
7. Click Submit.

**Workflows for Commissioning and Decommissioning of Virtual Machines**

Wrapper workflows, for commissioning and decommissioning of vRA/vCAC virtual machines, are not designed for use in running directly as Configuration workflows or workflows for creating Build Profiles. They are automatically called from vCAC on certain events during the process of creating VMs.

The workflows for Commissioning and Decommissioning include the following:

<table>
<thead>
<tr>
<th>Workflow Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reserve an IP for vCAC VM Wrapper</td>
<td>Reserves a fixed IP address from NIOS by making the respective entry and assigns it to the provisioned VM. For details, see Reserve an IP for vCAC VM Wrapper Workflow on page 57.</td>
</tr>
<tr>
<td>Reserve an IP for vCAC VM in Network Wrapper</td>
<td>Reserves an IP in network for virtual machines when provisioned. For details, see Reserve an IP for vCAC VM in Network Wrapper Workflow on page 57.</td>
</tr>
<tr>
<td>Reserve an IP for vCAC VM in Range Wrapper</td>
<td>Reserves an IP in range for virtual machines when provisioned. For details, see Reserve an IP for vCAC VM in Range Wrapper Workflow on page 58.</td>
</tr>
<tr>
<td>Update MAC Address for vCAC VM Wrapper</td>
<td>Updates the MAC address for a vCAC VM. See Update MAC Address for vCAC VM Wrapper Workflow on page 58.</td>
</tr>
<tr>
<td>Remove Host Record or A/PTR/CNAME/Fixed address/Reservation of vCAC VM Wrapper</td>
<td>Removes the host record, A record, PTR record, CNAME record, fixed address, or IPv4 reservation associated with a vCAC VM. The workflow is triggered from vCAC at the moment of removing a vCAC VM. For details, see Remove Host Record or A/PTR/CNAME/Fixed Address/Reservation of vCAC VM Wrapper Workflow on page 58.</td>
</tr>
</tbody>
</table>

**Reserve an IP for vCAC VM Wrapper Workflow**

You use this workflow (on the Workflows tab, select Administrator → Library → vCAC → Main) to reserve a fixed IP address from NIOS, make the respective entry in NIOS and assign this IP to the provisioned Virtual Machine.

This workflow triggers from vRA/vCAC on the following event:

- Building Machine

Prerequisites:

- A vCO customization is installed on the vCAC Infrastructure Administration host;
- A Build Profile is created by running the Create Build Profile for Reserve an IP for vCAC VM workflow (for information, see Creating Build Profiles on page 21) and is assigned to the requested Blueprint.

For detailed instructions on how to create a blueprint, refer to the section Creating a Blueprint on page 21.

**Reserve an IP for vCAC VM in Network Wrapper Workflow**

This workflow (on the Workflows tab, select Administrator → Library → vCAC → Main) is used to reserve an IP address in the specified network from NIOS, make the respective entry in NIOS and assign this IP to the Virtual Machine.
This workflow triggers from vRA/vCAC on the following event:

- Building Machine

Prerequisites:

- A vCO customization is installed on the vCAC Infrastructure Administration host;
- A Build Profile is created by running the **Create Build Profile for Reserve an IP for vCAC VM in Network** workflow (for information, see **Creating Build Profiles** on page 21) and is assigned to the requested Blueprint.

For detailed instructions on how to create a blueprint, refer to the section **Creating a Blueprint** on page 21.

**Reserve an IP for vCAC VM in Range Wrapper Workflow**

You use this workflow (on the Workflows tab, select Administrator → Library → vCAC → Main), to reserve an IP address in the specified network range from NIOS, make the respective entry in NIOS and assign this IP to the Virtual Machine.

This workflow triggers from vRA/vCAC on the following event:

- Building Machine

Prerequisites:

- A vCO customization is installed on the vCAC Infrastructure Administration host;
- A Build Profile is created by running the **Create Build Profile for Reserve an IP for vCAC VM in Range** workflow and is assigned to the requested Blueprint. For instructions on how to create a blueprint, refer to the section **Creating a Blueprint** on page 21.

**Update MAC Address for vCAC VM Wrapper Workflow**

You use this workflow (on the Workflows tab, select Administrator → Library → vCAC → Main) to retrieve the current MAC address from a created VM in vRA/vCAC and update appropriate records in NIOS.

This workflow triggers from vRA/vCAC on the following event:

- Machine Provisioned

Prerequisites:

- A vCO customization is installed on the vCAC Infrastructure Administration host;
- A Build Profile is created by running one of the following workflows and is assigned to the requested Blueprint (see **Creating Build Profiles** on page 21 and **Setting a Build Profile to a Blueprint** on page 22):
  - **Create Build Profile for Reserve an IP for vCAC VM** workflow;
  - **Create Build Profile for Reserve an IP for vCAC VM in Network** workflow;
  - **Create Build Profile for Reserve an IP for vCAC VM in Range** workflow.

**Remove Host Record or A/ PTR/CNAME/Fixed Address/Reservation of vCAC VM Wrapper Workflow**

You use this workflow to remove IPAM objects created in NIOS that are associated with a vRA/vCAC-managed virtual machine.

This workflow triggers from vRA/vCAC on the following event:

- Machine Disposing

Prerequisites:

- A vCO customization is installed on the vCAC Infrastructure Administration host;
- The VM was created through using one of three vCAC workflows of the Infoblox IPAM Plug-In for VMware:
  - **Reserve an IP for vCAC VM Wrapper Workflow**
  - **Reserve an IP for vCAC VM in Network Wrapper Workflow**
  - **Reserve an IP for vCAC VM in Range Wrapper Workflow**

For detailed instructions on how to create a blueprint, refer to the section **Creating a Blueprint** on page 21.
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/vCAC.
- In vRA/vCAC, in the Infrastructure → Managed Machines tab, check to ensure the new virtual machine's status is ON.
- In the Logs section in the vCenter Orchestrator workflow run;
- In the Logs tab on the vCenter Orchestrator configuration server;
- The audit log on the NIOS appliance. For more information, see Using the Audit Log in the Infoblox NIOS Administrator Guide.
- Under the Data Management → DNS → Zones page in the NIOS appliance, check for the new record.
Using Infoblox IPAM Plug-In for VMware Actions

Actions are the building blocks of workflows. An Infoblox IPAM Plug-In for VMware action is a Javascript segment that uses 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 actions are located in two folders in the vCO client:

- `com.infoblox.ipam` contains all base workflows working with plug-in API to get/create/remove/update objects in NIOS.
- `com.infoblox.ipam.util` contains utility actions to support validations in workflows and prepare data for workflows presentations.

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

1. Log in to the vCenter Orchestrator client.
2. Choose Design mode.
3. Click the Actions tab.
4. Click admin -> com.infoblox.ipam. The list of Infoblox IPAM actions is shown in the tree.
5. Click the Scripting tab. This provides the list of input parameters comprising the selected action.
The Infoblox IPAM Plug-In for VMware includes the following actions in three categories:

- *Infoblox IPAM Plug-In for VMware Actions* on page 61;
- *Utility Actions* on page 70;
- *AMQP-Related Utility Actions* on page 72;

<table>
<thead>
<tr>
<th>Table 3.2  Infoblox IPAM Plug-In for VMware Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Action</strong></td>
</tr>
</tbody>
</table>
| addAddressRecord | Adds an A or AAAA DNS record to IPAM with specified static IP address. Optionally, the action creates a PTR record (withPtrRecord=true). | ipamConnection name  
dnsView  
ipAddress  
comment  
withPtrRecord  
ea1Definition  
ea1Value  
...  
ea10Definition  
ea10Value | – |
| addAddressRecordInRange | Adds an A or AAAA DNS record to IPAM by getting next available IP address in the specified network range. Optionally, the action creates a PTR record (withPtrRecord=true). | ipamConnection name  
dnsView  
netaddr  
cidr  
networkView  
comment  
withPtrRecord  
ea1Definition  
ea1Value  
...  
ea10Definition  
ea10Value | String – allocated IP address for the created record. |
| addAddressRecordInRangeNetwork | Adds an A or AAAA DNS record to IPAM by getting next available IP address in the specified network. Optionally, the action creates a PTR record (withPtrRecord=true). | ipamConnection name  
dnsView  
netaddr  
cidr  
networkView  
comment  
withPtrRecord  
ea1Definition  
ea1Value  
...  
ea10Definition  
ea10Value | String – allocated IP address for the created record. |
<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
<th>Input Parameters</th>
<th>Output Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>addCnameRecord</td>
<td>Adds a CNAME record to IPAM objects.</td>
<td>ipamConnection canonical alias dnsView comment ea1Definition ea1Value ... ea10Definition ea10Value</td>
<td>–</td>
</tr>
<tr>
<td>addCnameRecords</td>
<td>Adds CNAME records to IPAM objects.</td>
<td>ipamConnection aliases canonical dnsView comment ea1Definition ea1Value ... ea10Definition ea10Value</td>
<td>–</td>
</tr>
<tr>
<td>addFixedAddress</td>
<td>Adds a fixed address to the IPAM.</td>
<td>ipamConnection ipAddress macAddress name networkView comment ea1Definition ea1Value ... ea10Definition ea10Value</td>
<td>–</td>
</tr>
<tr>
<td>addFixedAddressInNetwork</td>
<td>Adds a fixed address by getting next available IP address in the specified network.</td>
<td>ipamConnection netaddr cidr networkView macAddress name comment ea1Definition ea1Value ... ea10Definition ea10Value</td>
<td>String – allocated IP address for the created fixed address.</td>
</tr>
<tr>
<td>Action</td>
<td>Description</td>
<td>Input Parameters</td>
<td>Output Parameters</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>addFixedAddressInRange</td>
<td>Adds a fixed address by getting next available IP address in the specified network range.</td>
<td>ipamConnection startAddress endAddress name networkView macAddress comment ea1Definition ea1Value ... ea10Definition ea10Value</td>
<td>String – allocated IP address for the created fixed address.</td>
</tr>
<tr>
<td>addHost</td>
<td>Adds a host record with specified IP. Creates host or adds host address to the existing host record.</td>
<td>ipamConnection hostName dnsView ipAddress macAddress enableDhcp aliases comment ea1Definition ea1Value ... ea10Definition ea10Value</td>
<td>–</td>
</tr>
<tr>
<td>addHostInNetwork</td>
<td>Adds a host record by getting next available IP address in the specified network. Creates host or adds host address to the existing host record.</td>
<td>ipamConnection hostName dnsView netaddr cidr networkView macAddress enableDhcp aliases comment ea1Definition ea1Value ... ea10Definition ea10Value</td>
<td>String – allocated IP address for the created host.</td>
</tr>
<tr>
<td>Action</td>
<td>Description</td>
<td>Input Parameters</td>
<td>Output Parameters</td>
</tr>
<tr>
<td>---------------</td>
<td>------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
<td>----------------------------------------</td>
</tr>
<tr>
<td>addHostInRange</td>
<td>Adds a host record by getting next available IP address in the specified network range. Creates host or adds host address to the existing host record.</td>
<td>ipamConnection hostName dnsView dnsView startAddress endAddress networkView networkView macAddress enableDhcp aliases comment ea1Definition ea1Value ... ea10Definition ea10Value</td>
<td>String – allocated IP address for the created host.</td>
</tr>
<tr>
<td>addNetwork</td>
<td>Adds a new IP network to the Infoblox NIOS database.</td>
<td>ipamConnection networkView netaddr cidr template comment members membersType ea1Definition ea1Value ... ea10Definition ea10Value dhcpOptionDomainName dhcpOptionDomainSearch dhcpOptionDomainNameSearch dhcpOptionDomainNameS绫 eServers dhcpOptionRouters dhcpOptionNetbiosName eServers</td>
<td>–</td>
</tr>
<tr>
<td>addReservation</td>
<td>Adds an IPv4 reservation to the IPAM.</td>
<td>name ipamConnection ipAddress networkView comment ea1Definition ea1Value ... ea10Definition ea10Value</td>
<td>–</td>
</tr>
<tr>
<td>Action</td>
<td>Description</td>
<td>Input Parameters</td>
<td>Output Parameters</td>
</tr>
<tr>
<td>---------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>addReservationInNetwork</td>
<td>Adds an IPv4 reservation by getting next available IP address from specified network.</td>
<td>name, ipamConnection, netaddr, cidr, networkView, comment, ea1Definition, ea1Value, ... ea10Definition, ea10Value</td>
<td>String – allocated IP address for the created IPv4 reservation.</td>
</tr>
<tr>
<td>addReservationInRange</td>
<td>Adds an IPv4 reservation by getting next available IP address from specified network range.</td>
<td>name, ipamConnection, startAddress, endAddress, networkView, comment, ea1Definition, ea1Value, ... ea10Definition, ea10Value</td>
<td>String – allocated IP address for the created IPv4 reservation.</td>
</tr>
<tr>
<td>changeDNSName</td>
<td>Changes the name of A/AAAA/PTR/CNAME DNS records.</td>
<td>ipamConnection, oldName,dnsView, newName</td>
<td>–</td>
</tr>
<tr>
<td>changeHostName</td>
<td>Changes the name of the host record.</td>
<td>ipamConnection, oldHostName, newName, dnsView</td>
<td>–</td>
</tr>
<tr>
<td>findAddressRecordsByEA</td>
<td>Searches for A/AAAA records in IPAM by specified extensible attributes.</td>
<td>ipamConnection, dnsView, searchEa1Definition, searchEa1Value, searchEa1Comparison, ... searchEa10Definition, searchEa10Value, searchEa10Comparison</td>
<td>Array of Any(IpamAddressRecord)</td>
</tr>
<tr>
<td>findCnameRecordsByCanonicalName</td>
<td>Searches for CNAME records in IPAM by the specified canonical name.</td>
<td>ipamConnection, canonical, dnsView</td>
<td>Array of Any(IpamCnameRecord)</td>
</tr>
<tr>
<td>Action</td>
<td>Description</td>
<td>Input Parameters</td>
<td>Output Parameters</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>------------------------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>findCnameRecordsByEA</td>
<td>Searches for CNAME records in IPAM by the specified extensible attributes.</td>
<td>ipamConnection, dnsView, searchEa1Definition, searchEa1Value, searchEa1Comparison, ...</td>
<td>Array of Any(IpamCnameRecord)</td>
</tr>
<tr>
<td>findFixedAddressesByEA</td>
<td>Searches for fixed addresses in IPAM by specified extensible attributes.</td>
<td>ipamConnection, networkView, searchEa1Definition, searchEa1Value, searchEa1Comparison, ...</td>
<td>Array of Any(IpamFixedAddress)</td>
</tr>
<tr>
<td>findHostsByEA</td>
<td>Searches for hosts in IPAM by specified extensible attributes.</td>
<td>ipamConnection, dnsView, searchEa1Definition, searchEa1Value, searchEa1Comparison, ...</td>
<td>Array of Any(IpamHost)</td>
</tr>
<tr>
<td>findNetworksByEA</td>
<td>Searches for IPv4 and IPv6 networks in IPAM by specified extensible attributes.</td>
<td>ipamConnection, networkView, searchEa1Definition, searchEa1Value, searchEa1Comparison, ...</td>
<td>Array of Any(IpamNetwork)</td>
</tr>
<tr>
<td>findPTRRecordsByEA</td>
<td>Searches for PTR records in IPAM by specified extensible attributes.</td>
<td>ipamConnection, dnsView, searchEa1Definition, searchEa1Value, searchEa1Comparison, ...</td>
<td>Array of Any(IpamPtrRecord)</td>
</tr>
<tr>
<td>getDefaultIpamConnection</td>
<td>Returns the default connection to the IPAM server (NIOS appliance).</td>
<td>ipamConnection</td>
<td>ipamConnection</td>
</tr>
<tr>
<td>Action</td>
<td>Description</td>
<td>Input Parameters</td>
<td>Output Parameters</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>getEAAttributeDefinitionNames</td>
<td>Retrieves the Array of EA Attribute Definitions by Name</td>
<td>ipamConnection</td>
<td>Array of string</td>
</tr>
<tr>
<td>getIPAMConnection</td>
<td>Returns IPAM connection if the IPAM server specified found otherwise returns the default IPAM Connection</td>
<td>ServerName</td>
<td>ipamConnection</td>
</tr>
<tr>
<td>getNetwork</td>
<td>Gets IPv4 or IPv6 network with specified parameters from IPAM.</td>
<td>ipamConnection networkView netaddr</td>
<td>Any (IpamNetwork)</td>
</tr>
<tr>
<td>getNextAvailableIP</td>
<td>Finds the next available IPv4 or IPv6 address within the specified network.</td>
<td>ipamConnection netaddr</td>
<td>string</td>
</tr>
<tr>
<td>getNextAvailableIPFromRange</td>
<td>Finds the next available IP Address (IPv4 or IPv6) within the specified network range.</td>
<td>ipamConnection startAddress endAddress networkView</td>
<td>string</td>
</tr>
<tr>
<td>getPortGroupFromNetwork</td>
<td>Retrieves Port Group extensible attribute value from the Network.</td>
<td>network</td>
<td>string</td>
</tr>
<tr>
<td>getRange</td>
<td>Gets IPv4 or IPv6 DHCP range with specified parameters from IPAM.</td>
<td>ipamConnection startAddress endAddress networkView</td>
<td>Any (IpamDhcpRange)</td>
</tr>
<tr>
<td>getVCACEntityFromUniqueID</td>
<td>Action to get vCAC entity from Unique ID</td>
<td>vm</td>
<td>vCAC:Entity</td>
</tr>
<tr>
<td>getVCACHostFromEntity</td>
<td>Action to get vCAC host from entity</td>
<td>vCACEntity</td>
<td>vCAC:VCACHost</td>
</tr>
<tr>
<td>isAddressRecordExists</td>
<td>Checks if an A/AAAA record exists in IPAM.</td>
<td>ipamConnection name</td>
<td>Boolean</td>
</tr>
<tr>
<td>isHostExists</td>
<td>Checks if a host exists in IPAM.</td>
<td>ipamConnection hostName</td>
<td>Boolean</td>
</tr>
<tr>
<td>isPTRRecordExists</td>
<td>Checks if a PTR record exists in IPAM.</td>
<td>ipamConnection domainName</td>
<td>Boolean</td>
</tr>
<tr>
<td>removeAddressRecord</td>
<td>Removes an A/AAAA record from the IPAM.</td>
<td>ipAddress ipamConnection</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>name dnsView</td>
<td></td>
</tr>
<tr>
<td>Action</td>
<td>Description</td>
<td>Input Parameters</td>
<td>Output Parameters</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>removeAddressRecordsByEA</td>
<td>Removes A/AAAA records in IPAM that match the specified extensible attributes.</td>
<td>ipamConnection dnsView searchEa1Definition searchEa1Value searchEa1Comparison ... searchEa10Definition searchEa10Value searchEa10Comparison</td>
<td>–</td>
</tr>
<tr>
<td>removeCnameRecord</td>
<td>Removes a CNAME record from the IPAM.</td>
<td>ipamConnection alias dnsView</td>
<td>–</td>
</tr>
<tr>
<td>removeCnameRecordsByCanonicalName</td>
<td>Removes CNAME records in IPAM by the specified canonical name.</td>
<td>ipamConnection canonical dnsView</td>
<td>–</td>
</tr>
<tr>
<td>removeCnameRecordsByEA</td>
<td>Removes CNAME records in IPAM by the specified extensible attributes.</td>
<td>ipamConnection dnsView searchEa1Definition searchEa1Value searchEa1Comparison ... searchEa10Definition searchEa10Value searchEa10Comparison</td>
<td>–</td>
</tr>
<tr>
<td>removeFixedAddressesAndReservationsByEA</td>
<td>Removes fixed addresses and IPv4 reservations that match the specified extensible attributes.</td>
<td>ipamConnection networkView searchEa1Definition searchEa1Value searchEa1Comparison ... searchEa10Definition searchEa10Value searchEa10Comparison</td>
<td>–</td>
</tr>
<tr>
<td>removeFixedAddressOrReservation</td>
<td>Removes a fixed address or IPv4 reservation from NIOS.</td>
<td>ipamConnection ipAddress networkView</td>
<td>–</td>
</tr>
<tr>
<td>removeHost</td>
<td>Removes a host record from IPAM.</td>
<td>ipamConnection hostName dnsView</td>
<td>–</td>
</tr>
<tr>
<td>Action</td>
<td>Description</td>
<td>Input Parameters</td>
<td>Output Parameters</td>
</tr>
<tr>
<td>------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>removeHostsByEA</td>
<td>Removes IPAM hosts that match the specified extensible attributes.</td>
<td>ipamConnection, dnsView, searchEa1Definition, searchEa1Value, searchEa1Comparison ...</td>
<td>–</td>
</tr>
<tr>
<td>removeNetwork</td>
<td>Removes an IP network and all associated data from the Infoblox NIOS database.</td>
<td>ipamConnection, networkView, netaddr, cidr</td>
<td>–</td>
</tr>
<tr>
<td>removeNetworksByEA</td>
<td>Removes IPv4 and IPv6 networks that match the specified extensible attributes.</td>
<td>ipamConnection, networkView, searchEa1Definition, searchEa1Value, searchEa1Comparison ...</td>
<td>–</td>
</tr>
<tr>
<td>removePTRRecord</td>
<td>Removes a PTR record from the IPAM.</td>
<td>ipAddress, ipamConnection, domainName, dnsView</td>
<td>–</td>
</tr>
<tr>
<td>removePTRRecordsByEA</td>
<td>Removes PTR records in IPAM that match the specified extensible attributes.</td>
<td>ipamConnection, dnsView, searchEa1Definition, searchEa1Value, searchEa1Comparison ...</td>
<td>–</td>
</tr>
<tr>
<td>restartIpamServices</td>
<td>Restarts services on the NIOS appliance to ensure that IPAM changes are applied.</td>
<td>ipamConnection, memberOrder, requestType, serviceOption, sequentialDelay</td>
<td>–</td>
</tr>
<tr>
<td>updateFixedAddressMac</td>
<td>Updates the MAC address of the fixed address in IPAM.</td>
<td>ipamConnection, ipAddress, networkView, newMac</td>
<td>–</td>
</tr>
<tr>
<td>Action</td>
<td>Description</td>
<td>Input Parameters</td>
<td>Output Parameters</td>
</tr>
<tr>
<td>-------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>updateHostIP</td>
<td>Updates the IP address of the host in IPAM.</td>
<td>ipamConnection hostName dnsView mac newIpAddress</td>
<td>–</td>
</tr>
<tr>
<td>updateHostMac</td>
<td>Updates the MAC address of the host in IPAM.</td>
<td>ipamConnection hostName dnsView ipAddress newMac enableDHCP</td>
<td>–</td>
</tr>
</tbody>
</table>

**Utility Actions Table**

*Table 3.3 Utility Actions*

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
<th>Input Parameters</th>
<th>Output Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>calculateNetaddr</td>
<td>Gets the network address from given gateway address and network mask. E.g. for given gateway 10.0.0.1 and mask 255.255.255.0, the network address 10.0.0.0 will be received.</td>
<td>gatewayIP netMask</td>
<td>String – network address.</td>
</tr>
<tr>
<td>checkConsistencyOfViews</td>
<td>Checks if the DNS view is owned by the network view.</td>
<td>ipamConnection dnsView networkView</td>
<td>–</td>
</tr>
<tr>
<td>cidr2netmask</td>
<td>Converts CIDR of IPv4 network to network mask.</td>
<td>cidr</td>
<td>String – network mask in format 255.255.255.0.</td>
</tr>
<tr>
<td>connectionContainsDefinition</td>
<td>Checks if an extensible attribute definition is contained in the specified IPAM connection.</td>
<td>ipamConnection eaDefinition</td>
<td>Boolean – returns true, if the definition is contained in the specified IPAM connection, otherwise false.</td>
</tr>
<tr>
<td>findVcIVMByVAppVmName</td>
<td>Finds the vCloud VM by its name in the given vCloud vApp.</td>
<td>vclIVApp vmName</td>
<td>vCloud:VM – found VM.</td>
</tr>
<tr>
<td>generateComputerName</td>
<td>Returns a generated computer name of the VM.</td>
<td>vm vmIndex computerName</td>
<td>String</td>
</tr>
<tr>
<td>generateHostName</td>
<td>Returns a generated host name.</td>
<td>vm useVmNameAsHostName prefix networkConnectionIndex dnsSuffix vmComputerName</td>
<td>String</td>
</tr>
<tr>
<td>Action</td>
<td>Description</td>
<td>Input Parameters</td>
<td>Output Parameters</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------------------</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td>getDnsViews</td>
<td>Gets a list of DNS views for specified IPAM connection and network view. If no connection is specified, the default connection to the IPAM server is used. If no network view is specified, gets all DNS views for specific connection.</td>
<td>ipamConnection networkView</td>
<td>Array of string – list of DNS views.</td>
</tr>
<tr>
<td>getNetworkViews</td>
<td>Gets a list of network views for specified IPAM connection. If no connection is specified, the default connection to the IPAM server is used.</td>
<td>ipamConnection</td>
<td>Array of string – list of network views.</td>
</tr>
<tr>
<td>getOrgVdcNetworksByPortGroup</td>
<td>Gets names of the Org vDC networks that are associated with the specified port group.</td>
<td>vDC portGroupName</td>
<td>Array of string</td>
</tr>
<tr>
<td>getPortGroupFromNetwork</td>
<td>Retrieves Port Group extensible attribute value from the Network</td>
<td>Network</td>
<td>String</td>
</tr>
<tr>
<td>getPortGroupsOfVdc</td>
<td>Gets names of the port groups that are associated with networks of the specified vDC.</td>
<td>vDC</td>
<td>Array of string</td>
</tr>
<tr>
<td>getPortGroupsOfVAppNetworks</td>
<td>Gets names of the port groups that are associated with networks of the specified vApp.</td>
<td>vApp</td>
<td>Array of string</td>
</tr>
<tr>
<td>getVAppNetworks</td>
<td>Gets names of the vApp networks.</td>
<td>vApp</td>
<td>Array of string</td>
</tr>
<tr>
<td>getVAppNetworksByPortGroup</td>
<td>Gets names of the vApp networks that are associated with the specified port group.</td>
<td>vApp portGroupName</td>
<td>Array of string</td>
</tr>
<tr>
<td>isIPv4Address</td>
<td>Checks if the IP address is a valid IPv4 address.</td>
<td>ipAddress</td>
<td>Boolean – returns true if the IP address is a valid IPv4 address, otherwise false.</td>
</tr>
<tr>
<td>isIPv6Address</td>
<td>Checks if the IP address is a valid IPv6 address.</td>
<td>ipAddress</td>
<td>Boolean – returns true if the IP address is a valid IPv6 address, otherwise false.</td>
</tr>
<tr>
<td>netmask2cidr</td>
<td>Converts network mask to CIDR.</td>
<td>netMask</td>
<td>Number – CIDR</td>
</tr>
<tr>
<td>validateHostName</td>
<td>Checks whether the host name is in the right format. Returns true if host name is in the right format, otherwise false.</td>
<td>hostName</td>
<td>Boolean – true if host name is in the right format, otherwise false.</td>
</tr>
<tr>
<td>validateIPAddress</td>
<td>Checks whether the IP address is in the IPv4 or IPv6 format.</td>
<td>ipAddress</td>
<td>String – error message or null if validation successful.</td>
</tr>
<tr>
<td>validateMacAddress</td>
<td>Checks if the MAC address or DUID is in the right format. Returns a message (string) if validation fails, otherwise returns null.</td>
<td>macAddress</td>
<td>String – error message or null if validation successful.</td>
</tr>
</tbody>
</table>
## AMQP Utility Actions Table

Table 3.4 AMQP-Related Utility Actions

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
<th>Input Parameters</th>
<th>Output Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>getSubscriptionsWith Listener</td>
<td>Gets the subscriptions for which the listener workflow is running.</td>
<td>wf</td>
<td>Array of AMQP: subscription – list of subscriptions for which the listener workflow is running.</td>
</tr>
<tr>
<td>isSystemConnection</td>
<td>Checks if the vCloud host is connected to vCO under System Administrator.</td>
<td>vCloudHost</td>
<td>Boolean – returns true if the vCloud host connected to vCO under System Administrator, otherwise false.</td>
</tr>
<tr>
<td>isVmModificationLocked</td>
<td>Checks the lock of the VM modification. Is used to prevent recalls of an AMQP workflow from another.</td>
<td>vm</td>
<td>Boolean – returns true if VM modification is locked, otherwise false.</td>
</tr>
<tr>
<td>lockVmModification</td>
<td>Locks the virtual machine modification. Is used to prevent recalls of an AMQP workflow from another.</td>
<td>vm</td>
<td>void</td>
</tr>
<tr>
<td>unlockVmModification</td>
<td>Unlocks the virtual machine modification. Is used to prevent recalls of an AMQP workflow from another.</td>
<td>vm</td>
<td>void</td>
</tr>
<tr>
<td>getVAppNetworkRanges</td>
<td>Gets a list of the vApp network ranges from the specified vApp network.</td>
<td>vApp networkName</td>
<td>Array of string</td>
</tr>
<tr>
<td>getVMNetworkPropertiesForIPAM</td>
<td>Returns a Properties object with the following IPAM-related network properties key/value. Top level keys are: &quot;vmId&quot;, &quot;vmName&quot;, &quot;vmComputerName&quot;, &quot;arrayVMNetConnProperties&quot;. The &quot;arrayVMNetConnProperties&quot; is an array of Properties objects, each representing a network connection of a virtual machine by keys: &quot;networkConnIdx&quot;, &quot;netmask&quot;, &quot;ipAddress&quot;, &quot;ipAddressAllocationMode&quot;, &quot;macAddress&quot;, &quot;netaddr&quot;, &quot;networkName&quot;, &quot;fqdn&quot;, &quot;dnsSuffix&quot;, &quot;isPrimary&quot;.</td>
<td>vm</td>
<td>Properties – VM Properties.</td>
</tr>
</tbody>
</table>

For information about how to build workflows by using actions, refer to the vCenter Orchestrator documentation.
INFOBLOX IPAM PLUG-IN FOR VMWARE API

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 vCenter 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**.

The Infoblox IPAM objects API consist of the following:
For the Infoblox IPAM Plug-In for VMware Version 2.4.2 (Rev. A) Infoblox User's Guide

- `IpamConnection`
- `IpamViewManager`
- `IpamHostManager`
- `IpamNetworkManager`
- `IpamDnsRecordManager`
- `IpamFixedAddressManager`
- `IpamHost`
- `IpamHostInfo`
- `IpamExtensibleAttributeDefinition`
- `IpamExtensibleAttributeDefinitionType`
- `IpamExtensibleAttribute`
- `IpamExtensibleAttributeType`
- `IpamSearchableExtensibleAttribute`
- `IpamSearchComparisonType`
- `IpamHostAddress`
- `IpamNetwork`
- `IpamMemberType`
- `IpamMembers`
- `IpamDhcpOptions`
- `IpamDhcpRange`
- `IpamAddressRecord`
- `IpamPtrRecord`
- `IpamCnameRecord`
- `IpamFixedAddress`
- `IpamRestartMemberOrder`
- `IpamRestartRequestType`
- `IpamRestartServiceOption`
- `IpamRestartOptions`

### IpamConnection

**Attributes:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hostName</td>
<td>String</td>
<td>Host address of the NIOS/IPAM server.</td>
</tr>
<tr>
<td>configDefaultDnsView</td>
<td>String</td>
<td>Default DNS view from connection configuration.</td>
</tr>
<tr>
<td>id</td>
<td>String</td>
<td>ID of the IPAM Connection.</td>
</tr>
<tr>
<td>configDefaultNetworkView</td>
<td>String</td>
<td>Default network view from connection configuration.</td>
</tr>
<tr>
<td>defaultConnection</td>
<td>Boolean</td>
<td>Default connection.</td>
</tr>
</tbody>
</table>

**Methods:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Parameters</th>
<th>Returned Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>restartServices(restartOptions)</td>
<td>restartOptions(Ipam RestartOptions)</td>
<td>–</td>
<td>Restarts Grid services.</td>
</tr>
<tr>
<td>getNetworkManager()</td>
<td>–</td>
<td>IpamNetworkManager</td>
<td>Gets the network manager object.</td>
</tr>
<tr>
<td>getHostManager()</td>
<td>–</td>
<td>IpamHostManager</td>
<td>Gets the host manager object.</td>
</tr>
<tr>
<td>getFixedAddressManager()</td>
<td>–</td>
<td>IpamFixedAddressManager</td>
<td>Gets the fixed address manager object.</td>
</tr>
<tr>
<td>getDnsRecordManager()</td>
<td>–</td>
<td>IpamDnsRecordManager</td>
<td>Gets the DNS record manager object.</td>
</tr>
<tr>
<td>getViewManager()</td>
<td>–</td>
<td>IpamViewManager</td>
<td>Gets the view manager object.</td>
</tr>
</tbody>
</table>
IpamViewManager

Methods:

<table>
<thead>
<tr>
<th>Name</th>
<th>Parameters</th>
<th>Returned Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>getAllNetworkViews()</td>
<td>–</td>
<td>Array of string</td>
<td>Gets all network views.</td>
</tr>
<tr>
<td>getAllDnsViews()</td>
<td>–</td>
<td>Array of string</td>
<td>Gets all DNS views.</td>
</tr>
<tr>
<td>getDefaultNetworkView()</td>
<td>–</td>
<td>String</td>
<td>Gets default network view.</td>
</tr>
<tr>
<td>getDefaultDnsView()</td>
<td>–</td>
<td>String</td>
<td>Gets default DNS view.</td>
</tr>
<tr>
<td>getDnsViewsForNetworkView(networkView)</td>
<td>networkView(string)</td>
<td>Array of string</td>
<td>Gets the list of DNS views for the specified network view.</td>
</tr>
<tr>
<td>isDnsViewOwnedByNetworkView(dnsView, networkView)</td>
<td>dnsView(string), networkView(string)</td>
<td>Boolean – true if the DNS view is owned by the network view.</td>
<td>Checks if the DNS view is owned by the network view.</td>
</tr>
</tbody>
</table>

IpamHostManager

Methods:

<table>
<thead>
<tr>
<th>Name</th>
<th>Parameters</th>
<th>Returned Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>addHost(host, hostAddress)</td>
<td>host (string) – specified new FQDN host name. hostAddress(IpamHostAddress) – host address to add.</td>
<td>–</td>
<td>Adds a host record with specified IP address to IPAM.</td>
</tr>
<tr>
<td>addHostAddress(hostName, dnsView, hostAddress)</td>
<td>hostName(string) – name of the existing host record; dnsView(string) – name of the DNS view in which host record resides; hostAddress(IpamHostAddress) – host address to add.</td>
<td>–</td>
<td>Adds a host address with specified IP address to the existing host record in IPAM.</td>
</tr>
<tr>
<td>Name</td>
<td>Parameters</td>
<td>Returned Value</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>---------------------------------------------------------------------------</td>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>addHostAddressInNetwork (hostName, dnsView, hostAddress, network)</td>
<td>hostName(string) – name of the existing host record; dnsView(string) – name of the DNS view in which host record resides; hostAddress – host address to add; network (string) – network name.</td>
<td>ipAddress(string) – allocated IP address for the host address</td>
<td>Adds a host address to the existing host record in IPAM using specified network to get next available IP address.</td>
</tr>
<tr>
<td>addHostAddressInRange (hostName, dnsView, hostAddress, dhcpRange)</td>
<td>hostName(string) – name of the existing host record; dnsView(string) – name of the DNS view in which host record resides; hostAddress – host address to add; dhcpRange(IpamDhcpRange) – DHCP range for getting next available IP address for the new host address.</td>
<td>ipAddress(string) – allocated IP address for the host address</td>
<td>Adds a host address to the existing host record in IPAM using specified DHCP network range to get next available IP address.</td>
</tr>
<tr>
<td>addHostInNetwork(host, hostAddress, network)</td>
<td>host (string) – specified new FQDN host name; hostAddress(IpamHostAddress) – host address to add, network (string) – network name.</td>
<td>ipAddress(string) – allocated IP address for the host</td>
<td>Adds a host record to the IPAM using specified network to get next available IP address.</td>
</tr>
<tr>
<td>addHostInRange(host, hostAddress, dhcpRange)</td>
<td>host (string) – specified new FQDN host name; hostAddress – host address to add; dhcpRange(IpamDhcpRange) – DHCP range for getting next available IP address for the new host address.</td>
<td>ipAddress(string) – allocated IP address for the host</td>
<td>Adds a host record to the IPAM using specified DHCP network range to get next available IP address.</td>
</tr>
<tr>
<td>changeHostName(old Name, dnsView, newName)</td>
<td>dnsView(string) – name of the DNS view in which host record resides; dnsView(string) – name of the DNS view in which host record resides. newName – specified new name</td>
<td>–</td>
<td>Changes the name of the host record.</td>
</tr>
<tr>
<td>findHostsByEA(extensible Attributes, dnsView)</td>
<td>extensibleAttributes (Array of IpamSearchableExtensibleAttribute) – list of extensible attributes; dnsView(string) – name of the DNS view in which host record resides.</td>
<td>Array of IpamHost</td>
<td>Gets the list of host records which match the query by extensible attributes.</td>
</tr>
</tbody>
</table>
IpamNetworkManager

Methods:

<table>
<thead>
<tr>
<th>Name</th>
<th>Parameters</th>
<th>Returned Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>addExclusionRange(startAddress, endAddress, network)</td>
<td>startAddress(string) – start IPv4/IPv6 address of the exclusion range. endAddress(string) – end IPv4/IPv6 address of the exclusion range. network(IpamNetwork) – IPv4/IPv6 network to which the specified exclusion range will be added.</td>
<td>–</td>
<td>Adds exclusion range in the specified IPAM network.</td>
</tr>
</tbody>
</table>
IpamDnsRecordManager

Methods:

<table>
<thead>
<tr>
<th>Name</th>
<th>Parameters</th>
<th>Returned Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>addAddressRecord(ipamAddressRecord)</td>
<td>ipamAddressRecord(ipamAddressRecord) – address record to add.</td>
<td>–</td>
<td>Adds A/AAAA record to IPAM.</td>
</tr>
<tr>
<td>Name</td>
<td>Parameters</td>
<td>Returned Value</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>----------------------------------------------------------------------------</td>
<td>---------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td><code>addAddressRecordInNet</code> work(ipamAddressRecord, ipamNetwork)</td>
<td>ipamAddressRecord(Ipa mAddressRecord) – address record to add. ipamNetwork(Ipa mNetwo rk) – network for getting next available IP address for the record.</td>
<td>ipAddress(string) – allocated IP address for the record</td>
<td>Adds A/AAAA record to the IPAM using specified network to get next available IP address.</td>
</tr>
<tr>
<td><code>addAddressRecordInRange (ipamAddressRecord, ipamDhcpRange)</code></td>
<td>ipamAddressRecord(Ipa mAddressRecord) – address record to add. ipamDhcpRange(Ipa mDhcpRange) – DHCP range for getting next available IP address for the record.</td>
<td>ipAddress(string) – allocated IP address for the record</td>
<td>Adds A/AAAA record to the IPAM using specified network range to get next available IP address.</td>
</tr>
<tr>
<td><code>addCnameRecord(ipamCnameRecord)</code></td>
<td>ipamCnameRecord(Ipa mCnameRecord) – CNAME record to add.</td>
<td>–</td>
<td>Adds CNAME record to IPAM.</td>
</tr>
<tr>
<td><code>addPtrRecord(ipamPtrRecord)</code></td>
<td>ipamPtrRecord(Ipa mPtrRecord) – PTR record to add.</td>
<td>–</td>
<td>Adds PTR record to IPAM.</td>
</tr>
<tr>
<td><code>changeDnsName(oldName, dnsView, newName)</code></td>
<td>oldName(string) – name of the existing DNS records. dnsView(string) – name of the DNS view in which DNS records reside. newName(string) – new name for DNS records.</td>
<td>–</td>
<td>Changes the name of A/AAAA/PTR/CNAME DNS records with specified old name.</td>
</tr>
<tr>
<td><code>changeIpAddress(name, dnsView, newIpAddress)</code></td>
<td>name(string) – name of the existing DNS records. dnsView(string) – name of the DNS view in which DNS records reside. newIpAddress(string) – new IP address.</td>
<td>–</td>
<td>Changes the IP address of A/AAAA/PTR DNS records with specified name.</td>
</tr>
<tr>
<td><code>findAddressRecordsByEA (extensibleAttributes, dnsView)</code></td>
<td>extensibleAttributes(Arra y of IpamSearchable ExtensibleAttribute) – list of extensible attributes. dnsView(string) – name of the DNS view in which A/AAAA records reside.</td>
<td>Array of IpamAddressRecord</td>
<td>Gets the list of A/AAAA records that match the query by extensible attributes.</td>
</tr>
<tr>
<td><code>findCnameRecordsByCanonicalName(canonicalName, dnsView)</code></td>
<td>canonicalName(string) – canonical name of the CNAME records. dnsView(string) – name of the DNS View in which CNAME records reside.</td>
<td>Array of IpamCnameRecord</td>
<td>Gets the list of CNAME records that match the query by canonical name.</td>
</tr>
<tr>
<td>Name</td>
<td>Parameters</td>
<td>Returned Value</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>------------</td>
<td>----------------</td>
<td>-------------</td>
</tr>
<tr>
<td>findCnameRecordsByEA(extensibleAttributes, dnsView)</td>
<td>extensibleAttributes(Array of IpamSearchable ExtensibleAttribute?) – list of extensible attributes. dnsView(string) – name of the DNS View in which CNAME records reside.</td>
<td>Array of IpamCnameRecord</td>
<td>Gets the list of CNAME records that match the query by extensible attributes.</td>
</tr>
<tr>
<td>findPtrRecordsByEA(extensibleAttributes, dnsView)</td>
<td>extensibleAttributes(Array of IpamSearchable ExtensibleAttribute?) – list of extensible attributes. dnsView(string) – name of the DNS View in which PTR records reside.</td>
<td>Array of IpamPtrRecord</td>
<td>Gets the list of PTR records that match the query by extensible attributes.</td>
</tr>
<tr>
<td>isAddressRecordExists(name, dnsView)</td>
<td>name(string) – name of the A/AAAA record. dnsView(string) – name of the DNS View in which A/AAAA record resides.</td>
<td>Boolean</td>
<td>Checks if A/AAAA record exists in IPAM.</td>
</tr>
<tr>
<td>isPtrRecordExists(domainName, dnsView)</td>
<td>domainName(string) – domain name of the PTR record. dnsView(string) – name of the DNS View in which PTR record resides.</td>
<td>Boolean</td>
<td>Checks if PTR record exists in IPAM.</td>
</tr>
<tr>
<td>removeAddressRecord(name, ipAddress, dnsView)</td>
<td>name(string) – name of the address record. ipAddress(string) – IP address of the A/AAAA record. If null, all A/AAAA records with the specified name will be removed. dnsView(string) – name of the DNS view in which address record resides.</td>
<td>–</td>
<td>Removes A/AAAA record from IPAM.</td>
</tr>
<tr>
<td>removeCnameRecord(alias, dnsView)</td>
<td>alias(string) – alias of the CNAME record. dnsView(string) – name of the DNS view in which CNAME record resides.</td>
<td>–</td>
<td>Removes CNAME record from IPAM.</td>
</tr>
<tr>
<td>removePtrRecord(domainName, ipAddress, dnsView)</td>
<td>domainName(string) – domain name of the PTR record. ipAddress(string) – IP address of the PTR record. If null, all PTR records with the specified name will be removed. dnsView(string) – name of the DNS view in which PTR record resides.</td>
<td>–</td>
<td>Removes PTR record from IPAM.</td>
</tr>
</tbody>
</table>
IpamFixedAddressManager

Methods:

<table>
<thead>
<tr>
<th>Name</th>
<th>Parameters</th>
<th>Returned Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>addFixedAddress(fixedAddress)</td>
<td>fixedAddress(IpamFixedAddress) – fixed address to add.</td>
<td>–</td>
<td>Adds fixed address to the IPAM.</td>
</tr>
<tr>
<td>addFixedAddressInNetwork(fixedAddress, network)</td>
<td>fixedAddress(IpamFixedAddress) – fixed address to add.</td>
<td>ipAddress(string) – allocated IP address for the fixed address.</td>
<td>Adds fixed address to the IPAM using specified network to get next available IP address.</td>
</tr>
<tr>
<td>addFixedAddressInRange(fixedAddress, dhcpRange)</td>
<td>fixedAddress(IpamFixedAddress) – fixed address to add.</td>
<td>ipAddress(string) – allocated IP address for the fixed address.</td>
<td>Adds fixed address to the IPAM using specified network range to get next available IP address.</td>
</tr>
<tr>
<td>findFixedAddressesByEA(extenensibleAttributes, networkView)</td>
<td>extensibleAttributes(Array of IpamSearchableExtensibleAttribute) – list of extensible attributes.</td>
<td>Array of IpamFixedAddress</td>
<td>Gets the list of fixed addresses which match the query by extensible attributes.</td>
</tr>
<tr>
<td>removeFixedAddress(ipAddress, networkView)</td>
<td>ipAddress(string) – IP address of the fixed address.</td>
<td>–</td>
<td>Removes fixed address from the IPAM.</td>
</tr>
<tr>
<td>updateFixedAddressMac(ipAddress, networkView, newMac)</td>
<td>ipAddress(string) – IP address of fixed address.</td>
<td>–</td>
<td>Updates the MAC address of the fixed address in IPAM.</td>
</tr>
</tbody>
</table>
IpamHost
Attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>addresses</td>
<td>Array of IpamHostAddress</td>
<td>List of host addresses.</td>
</tr>
<tr>
<td>aliases</td>
<td>Array of string</td>
<td>List of host aliases.</td>
</tr>
<tr>
<td>comment</td>
<td>String</td>
<td>Comment.</td>
</tr>
<tr>
<td>dnsView</td>
<td>String</td>
<td>DNS view.</td>
</tr>
<tr>
<td>extensibleAttributes</td>
<td>Array of IpamExtensibleAttribute</td>
<td>List of extensible attributes.</td>
</tr>
<tr>
<td>fqdn</td>
<td>String</td>
<td>The Fully Qualified Domain Name of the host.</td>
</tr>
</tbody>
</table>

IpamHostInfo
Attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fqdn</td>
<td>String</td>
<td>The Fully Qualified Domain Name of the host.</td>
</tr>
<tr>
<td>comment</td>
<td>String</td>
<td>Comment.</td>
</tr>
<tr>
<td>extensibleAttributes</td>
<td>Array of IpamExtensibleAttribute</td>
<td>List of extensible attributes.</td>
</tr>
<tr>
<td>dnsView</td>
<td>String</td>
<td>DNS view.</td>
</tr>
<tr>
<td>aliases</td>
<td>Array of string</td>
<td>List of host aliases.</td>
</tr>
</tbody>
</table>

IpamExtensibleAttributeDefinition
Attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>String</td>
<td>Name of the extensible attribute definition.</td>
</tr>
<tr>
<td>type</td>
<td>IpamExtensibleAttributeDefinitionType</td>
<td>Type of the extensible attribute definition.</td>
</tr>
<tr>
<td>defaultValue</td>
<td>String</td>
<td>Default value of the extensible attribute.</td>
</tr>
<tr>
<td>comment</td>
<td>String</td>
<td>Comment for the extensible attribute.</td>
</tr>
</tbody>
</table>

Methods:

<table>
<thead>
<tr>
<th>Name</th>
<th>Parameters</th>
<th>Returned Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>getConnection()</td>
<td>–</td>
<td>IpamConnection</td>
<td>Gets the IPAM connection the object belongs to.</td>
</tr>
</tbody>
</table>
IpamExtensibleAttributeDefinitionType

Attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>STRING</td>
<td>IpamExtensibleAttributeDefinitionType</td>
<td>String extensible attribute type of Infoblox IPAM.</td>
</tr>
<tr>
<td>INTEGER</td>
<td>IpamExtensibleAttributeDefinitionType</td>
<td>Integer extensible attribute type of Infoblox IPAM.</td>
</tr>
<tr>
<td>DATE</td>
<td>IpamExtensibleAttributeDefinitionType</td>
<td>Date extensible attribute type of Infoblox IPAM.</td>
</tr>
<tr>
<td>EMAIL</td>
<td>IpamExtensibleAttributeDefinitionType</td>
<td>Email extensible attribute type of Infoblox IPAM.</td>
</tr>
<tr>
<td>LIST</td>
<td>IpamExtensibleAttributeDefinitionType</td>
<td>List extensible attribute type of Infoblox IPAM.</td>
</tr>
<tr>
<td>URL</td>
<td>IpamExtensibleAttributeDefinitionType</td>
<td>URL extensible attribute type of Infoblox IPAM.</td>
</tr>
</tbody>
</table>

IpamExtensibleAttribute

Attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>String</td>
<td>Name of the extensible attribute definition.</td>
</tr>
<tr>
<td>type</td>
<td>IpamExtensibleAttributeType</td>
<td>Type of the extensible attribute definition.</td>
</tr>
<tr>
<td>value</td>
<td>String</td>
<td>Value of the extensible attribute.</td>
</tr>
</tbody>
</table>

IpamExtensibleAttributeType

Attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>STRING</td>
<td>IpamExtensibleAttributeType</td>
<td>String, List, Email, URL, Date extensible attribute types of Infoblox IPAM.</td>
</tr>
<tr>
<td>INTEGER</td>
<td>IpamExtensibleAttributeType</td>
<td>Integer extensible attribute type of Infoblox IPAM.</td>
</tr>
</tbody>
</table>

IpamSearchableExtensibleAttribute

Attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>extensibleAttribute</td>
<td>IpamExtensibleAttribute</td>
<td>Extensible attribute.</td>
</tr>
<tr>
<td>comparison</td>
<td>IpamSearchComparisonType</td>
<td>Equals (EQUAL), Does not equal (NOT_EQUAL), etc.</td>
</tr>
</tbody>
</table>
**IpamSearchComparisonType**

Attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EQUAL</td>
<td>IpamSearchComparisonType</td>
<td>Exact match.</td>
</tr>
<tr>
<td>EQUAL_CASE_INSENSITIVE</td>
<td>IpamSearchComparisonType</td>
<td>Makes string matching case insensitive.</td>
</tr>
<tr>
<td>NOT_EQUAL</td>
<td>IpamSearchComparisonType</td>
<td>Negates the condition.</td>
</tr>
<tr>
<td>REGULAR_EXPRESSION</td>
<td>IpamSearchComparisonType</td>
<td>Regular expression search. Expressions are unanchored.</td>
</tr>
<tr>
<td>LESS_OR_EQUAL</td>
<td>IpamSearchComparisonType</td>
<td>Less than or equal.</td>
</tr>
<tr>
<td>GREATER_OR_EQUAL</td>
<td>IpamSearchComparisonType</td>
<td>Greater than or equal.</td>
</tr>
</tbody>
</table>

**IpamHostAddress**

Attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip</td>
<td>String</td>
<td>IPv4/IPv6 address.</td>
</tr>
<tr>
<td>mac</td>
<td>String</td>
<td>Mac address/DUID.</td>
</tr>
<tr>
<td>enableDhcp</td>
<td>Boolean</td>
<td>Enable DHCP flag.</td>
</tr>
</tbody>
</table>

**IpamNetwork**

Attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>address</td>
<td>String</td>
<td>Network address(IPv4/IPv6).</td>
</tr>
<tr>
<td>cidr</td>
<td>Number</td>
<td>Network CIDR.</td>
</tr>
<tr>
<td>comment</td>
<td>String</td>
<td>Comment.</td>
</tr>
<tr>
<td>networkView</td>
<td>String</td>
<td>Network view.</td>
</tr>
<tr>
<td>extensibleAttributes</td>
<td>Array of IpamExtensibleAttribute</td>
<td>List of extensible attributes.</td>
</tr>
<tr>
<td>dhcpOptions</td>
<td>IpamDhcpOptions</td>
<td>DHCP options.</td>
</tr>
</tbody>
</table>

**IpamMemberType**

Attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>INFOBLOX</td>
<td>IpamMemberType</td>
<td>Infoblox Grid member.</td>
</tr>
<tr>
<td>MICROSOFT</td>
<td>IpamMemberType</td>
<td>Microsoft member.</td>
</tr>
</tbody>
</table>
**IpamMembers**

Attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>addresses</td>
<td>Array of string</td>
<td>IP addresses of members.</td>
</tr>
<tr>
<td>type</td>
<td>IpamMemberType</td>
<td>Members type.</td>
</tr>
</tbody>
</table>

**IpamDhcpOptions**

Attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>routers</td>
<td>Array of string</td>
<td>IP addresses of routers. Applicable only for IPv4 networks.</td>
</tr>
<tr>
<td>domainName</td>
<td>String</td>
<td>Domain name (DNS suffix).</td>
</tr>
<tr>
<td>domainNameServers</td>
<td>Array of string</td>
<td>IP addresses of DNS servers.</td>
</tr>
<tr>
<td>domainSearch</td>
<td>Array of string</td>
<td>DNS suffixes for search.</td>
</tr>
<tr>
<td>netbiosNameServers</td>
<td>Array of string</td>
<td>IP addresses of NetBIOS name servers. Applicable only for IPv4 networks.</td>
</tr>
</tbody>
</table>

**IpamDhcpRange**

Attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>startAddress</td>
<td>String</td>
<td>Start of IPv4/IPv6 address range.</td>
</tr>
<tr>
<td>endAddress</td>
<td>String</td>
<td>End of IPv4/IPv6 address range.</td>
</tr>
<tr>
<td>networkView</td>
<td>String</td>
<td>Network view.</td>
</tr>
<tr>
<td>networkAddress</td>
<td>String</td>
<td>The address of network to which this range belongs.</td>
</tr>
<tr>
<td>networkCidr</td>
<td>String</td>
<td>The CIDR of network to which this range belongs.</td>
</tr>
<tr>
<td>dhcpOptions</td>
<td>IpamDhcpOptions</td>
<td>DHCP options.</td>
</tr>
</tbody>
</table>

**IpamAddressRecord**

The IpamAddressRecord object can represent either an A or AAAA record.

Attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>address</td>
<td>String</td>
<td>IPv4/IPv6 address of the A/AAAA record.</td>
</tr>
<tr>
<td>name</td>
<td>String</td>
<td>Name of the A/AAAA record.</td>
</tr>
<tr>
<td>view</td>
<td>String</td>
<td>DNS view.</td>
</tr>
<tr>
<td>comment</td>
<td>String</td>
<td>Comment.</td>
</tr>
<tr>
<td>extensibleAttributes</td>
<td>Array of IpamExtensibleAttribute</td>
<td>List of extensible attributes.</td>
</tr>
</tbody>
</table>
### IpamPtrRecord
Attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>address</td>
<td>String</td>
<td>IPv4/IPv6 address of the PTR record.</td>
</tr>
<tr>
<td>domainName</td>
<td>String</td>
<td>Name of the PTR record.</td>
</tr>
<tr>
<td>dnsView</td>
<td>String</td>
<td>DNS view.</td>
</tr>
<tr>
<td>comment</td>
<td>String</td>
<td>Comment.</td>
</tr>
<tr>
<td>extensibleAttributes</td>
<td>Array of IpamExtensibleAttribute</td>
<td>List of extensible attributes.</td>
</tr>
</tbody>
</table>

### IpamCnameRecord
Attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>alias</td>
<td>String</td>
<td>Alias of the CNAME record.</td>
</tr>
<tr>
<td>canonical</td>
<td>String</td>
<td>Name of the CNAME record.</td>
</tr>
<tr>
<td>view</td>
<td>String</td>
<td>DNS view.</td>
</tr>
<tr>
<td>comment</td>
<td>String</td>
<td>Comment.</td>
</tr>
<tr>
<td>extensibleAttributes</td>
<td>Array of IpamExtensibleAttribute</td>
<td>List of extensible attributes.</td>
</tr>
</tbody>
</table>

### IpamFixedAddress
Attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>address</td>
<td>String</td>
<td>IPv4/IPv6 address of the fixed address.</td>
</tr>
<tr>
<td>mac</td>
<td>String</td>
<td>Mac address/DUID.</td>
</tr>
<tr>
<td>name</td>
<td>String</td>
<td>Name of the fixed address.</td>
</tr>
<tr>
<td>networkView</td>
<td>String</td>
<td>Network view.</td>
</tr>
<tr>
<td>comment</td>
<td>String</td>
<td>Comment.</td>
</tr>
<tr>
<td>extensibleAttributes</td>
<td>Array of IpamExtensibleAttribute</td>
<td>List of extensible attributes.</td>
</tr>
</tbody>
</table>

### IpamRestartMemberOrder
Attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIMULTANEOUSLY</td>
<td>IpamRestartMemberOrder</td>
<td>Simultaneous order.</td>
</tr>
<tr>
<td>SEQUENTIALLY</td>
<td>IpamRestartMemberOrder</td>
<td>Sequential order.</td>
</tr>
</tbody>
</table>
IpamRestartRequestType
Attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FORCE_RESTART</td>
<td>IpamRestartRequestType</td>
<td>Forced restart.</td>
</tr>
<tr>
<td>RESTART_IF_NEEDED</td>
<td>IpamRestartRequestType</td>
<td>Restart if needed.</td>
</tr>
</tbody>
</table>

IpamRestartServiceOption
Attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALL</td>
<td>IpamRestartServiceOption</td>
<td>Restarts all services.</td>
</tr>
<tr>
<td>DHCP</td>
<td>IpamRestartServiceOption</td>
<td>Restarts DHCP service.</td>
</tr>
<tr>
<td>DNS</td>
<td>IpamRestartServiceOption</td>
<td>Restarts DNS service.</td>
</tr>
</tbody>
</table>

IpamRestartOptions
Attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>memberOrder</td>
<td>IpamRestartMemberOrder</td>
<td>Restart member order.</td>
</tr>
<tr>
<td>requestType</td>
<td>IpamRestartRequestType</td>
<td>Restart request type.</td>
</tr>
<tr>
<td>serviceOption</td>
<td>IpamRestartServiceOption</td>
<td>Restart service option.</td>
</tr>
<tr>
<td>sequentialDelay</td>
<td>number</td>
<td>Delayed time, in seconds, between Grid member restarts.</td>
</tr>
</tbody>
</table>

**Removing Infoblox IPAM Plug-In for VMware**

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

**Removing Infoblox IPAM Plug-In for VMware on Windows**

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

1. Log in to the Orchestrator configuration interface.
2. Click **Plug-ins**.
3. In the right panel, under **Enabled plug-ins installation status**, clear the Infoblox IPAM plug-in check box and click **Apply changes**.
4. In the left panel, click **Network**.
5. Click **SSL Trust Manager**.
6. In the certificates table, click **Delete** for those records which common name is “www.infoblox.com”.
7. Open the Windows Services list and stop the following services:
   - VMware vCenter Orchestrator Configuration
8. Navigate to the installation directory of the vCenter Orchestrator server:
   - If you installed vCO with the vCenter Server installer, the path is C:\Program Files\VMware\Infrastructure\Orchestrator\vCO version
   - If you installed the standalone version of vCO, the path is C:\Program Files\VMware\Orchestrator\
9. Remove the following files and directories from the vCO installation directory:

<table>
<thead>
<tr>
<th>vCO version</th>
<th>Remove files and directories</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCO 5.1</td>
<td>./app-server/server/vmo/conf/plugins/Infoblox_IPAM_Plugin.xml</td>
</tr>
<tr>
<td></td>
<td>./app-server/server/vmo/plugins/o11nplugin-ipam.dar</td>
</tr>
<tr>
<td></td>
<td>./configuration/jetty/contexts/o11nplugin-ipam-config.xml</td>
</tr>
<tr>
<td></td>
<td>./configuration/jetty/webapps/o11nplugin-ipam-config.war</td>
</tr>
<tr>
<td>vCO 5.5</td>
<td>./app-server/conf/plugins/Infoblox_IPAM_Plugin.xml</td>
</tr>
<tr>
<td></td>
<td>./app-server/plugins/o11nplugin-ipam.dar</td>
</tr>
<tr>
<td></td>
<td>./configuration/webapps/o11nplugin-ipam-config/</td>
</tr>
<tr>
<td></td>
<td>./configuration/webapps/o11nplugin-ipam-config.war</td>
</tr>
</tbody>
</table>

10. In the installation directory of the vCenter Orchestrator server, open the file:
   - For vCO 5.1: /app-server/server/vmo/conf/plugins/_VSOPluginInstallationVersion.xml
   - For vCO 5.5: /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">`.
12. If you did the IPAM plug-in integration with vCAC, perform the following steps to remove the installed blueprints, build profiles, and workflows. If not, go to Step 13 in this procedure.
   a. Open vRealize Automation.
   b. In the **Enterprise Administrator** section, click **Global Blueprints**.
   c. Right-click the installed blueprint and select **Edit** from the context menu.
   d. Click the **Properties** tab, clear the check box for the Infoblox IPAM build profile, and then click **OK**.
   e. Repeat the above step to disable the Infoblox IPAM build profile in all your blueprints.
   f. Click **Build Profiles**. For the Infoblox IPAM build profile, navigate to the action item list and click **Delete**. Click **OK** to confirm.
   g. In vRA/vCAC, go to **Infrastructure -> Blueprints -> Build Profiles**.
   h. Click **Manage Property Sets**, navigate to the action item list and remove the **InfobloxIpamProperties** property set.
   i. Go to your machine with the installed vCAC workflows (XAML files).
   j. Create a cmd.exe shortcut on the desktop, right click on it, and select **Run as administrator**.
   k. Change directory to where the CloudUtil command-line tool is located. By default, it is located in C:\Program Files (x86)\VMware\vCAC\Design Center\.
   l. Revert your three XAML files back to revision 0 by entering the following CMD commands:
      
      C:\Program Files (x86)\VMware\vCAC\Design Center\CloudUtil.exe workflow-rollback -n WFStubBuildingMachine -r 0
      C:\Program Files (x86)\VMware\vCAC\Design Center\CloudUtil.exe workflow-rollback -n WFStubMachineDisposing -r 0
      C:\Program Files (x86)\VMware\vCAC\Design Center\CloudUtil.exe workflow-rollback -n WFStubMachineProvisioned -r 0
13. Open the Windows Services list and start the following services:
   - VMware vCenter Orchestrator Configuration
• VMware vCenter Orchestrator Server

14. Log in to the vCO client.
15. Select either **Administer** or **Design** mode.
16. Click the **Packages** tab.
17. Delete the vCAC, AMQP, and basic packages of the plug-in the following order:
   a. Right-click `com.infoblox.ipam.vcac` and select **Delete element with content**.
   b. In the **Delete confirmation** window, click **DELETE ALL!**
   c. Repeat steps **a** and **b** for `com.infoblox.ipam.amqp`.
   d. Repeat steps **a** and **b** for `com.infoblox.ipam`.

18. Log in to the vCO configuration interface.
19. On the **Startup Options** tab, click **Restart service**, and then click **Restart the vCO configuration server**.

**Removing Infoblox IPAM Plug-In for VMware on Linux**

To remove the Infoblox IPAM Plug-In for VMware from vCenter Orchestrator on Windows:
1. Log in to the Orchestrator configuration interface.
2. Click **Plug-ins**.
3. In the right panel, under **Enabled plug-ins installation status**, clear the Infoblox IPAM plug-in check box and click **Apply changes**.
4. In the left panel, click **Network**.
5. Click **SSL Trust Manager**.
6. In the certificates table, click **Delete** for those records which common name is “www.infoblox.com”.
7. On the vCenter Orchestrator Linux appliance, shut down the vCO server and the vCO configuration service by using the following commands:

<table>
<thead>
<tr>
<th>vCO version</th>
<th>Enter commands</th>
</tr>
</thead>
</table>
| vCO 5.1     | `sudo /etc/init.d/vcod stop`  
|             | `sudo /etc/init.d/jettyd stop` |
8. Navigate to the vCO server installation directory by using the following commands on the vCO Linux appliance:

<table>
<thead>
<tr>
<th>vCO version</th>
<th>Enter commands</th>
</tr>
</thead>
</table>
| vCO 5.5     | sudo /etc/init.d/vco-server stop  
sudo /etc/init.d/vco-configurator stop |

9. Remove the following files and directories from the vCO installation directory by using the following commands:

<table>
<thead>
<tr>
<th>vCO version</th>
<th>Enter commands to remove files and directories</th>
</tr>
</thead>
</table>
| vCO 5.1     | rm ./app-server/server/vmo/conf/plugins/Infoblox_IPAM_Plugin.xml  
rm ./app-server/server/vmo/plugins/o11nplugin-ipam.dar  
rm ./configuration/jetty/context/o11nplugin-ipam-config.xml  
rm ./configuration/jetty/webapps/o11nplugin-ipam-config.war |
| vCO 5.5     | rm ./app-server/conf/plugins/Infoblox_IPAM_Plugin.xml  
rm ./app-server/plugins/o11nplugin-ipam.dar  
rm -R ./configuration/webapps/o11nplugin-ipam-config/  
rm ./configuration/webapps/o11nplugin-ipam-config.war |

10. In the installation directory of the vCenter Orchestrator server, open the file by entering the following:

<table>
<thead>
<tr>
<th>vCO version</th>
<th>Enter commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCO 5.1</td>
<td>vi /app-server/server/vmo/conf/plugins/_VSOPluginInstallationVersion.xml</td>
</tr>
<tr>
<td>vCO 5.5</td>
<td>vi /app-server/conf/plugins/_VSOPluginInstallationVersion.xml</td>
</tr>
</tbody>
</table>

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="Infoblox IPAM">`. To do so, press **dd**, then press **Shift+q**, and then enter **wq** to save your changes.

12. On the vCenter Orchestrator Linux appliance, start the vCO server and the vCO configuration service by using the following commands:

<table>
<thead>
<tr>
<th>vCO version</th>
<th>Enter commands</th>
</tr>
</thead>
</table>
| vCO 5.1     | sudo /etc/init.d/vcod start  
sudo /etc/init.d/jettyd start |
| vCO 5.5     | sudo /etc/init.d/vco-server start  
sudo /etc/init.d/vco-configurator start |

13. If you did the IPAM plug-in integration with vCAC, perform the following steps to remove the installed blueprints, build profile and workflows. If not, go to Step 14 in this procedure.
   a. Open the vRealize Automation.
   b. In the **Enterprise Administrator** section, click **Global Blueprints**.
c. Right-click the installed blueprint and select **Edit** from the context menu.
d. Click the **Properties** tab, clear the check box for the Infoblox IPAM build profile, and then click **OK**.
e. Repeat the above step to disable the Infoblox IPAM build profile in all your blueprints.
f. Click **Build Profiles**. For the Infoblox IPAM build profile, navigate to the action item list and click **Delete**. Click **OK** to confirm.
g. In vCAC, go to **Infrastructure → Blueprints → Build Profiles**.
h. Click **Manage Property Sets**, navigate to the action item list and remove the **InfobloxIpamProperties** property set.
i. Go to your machine with the installed vCAC workflows (XAML files).
j. Create a **cmd.exe** shortcut on the desktop, right click on it, and select **Run as administrator**.
k. Change directory to where the CloudUtil command-line tool is located. By default, it is located in `C:\Program Files (x86)\VMware\vCAC\Design Center\`.
l. Revert your three XAML files back to revision 0 by entering the following CMD commands:

```
C:\Program Files (x86)\VMware\vCAC\Design Center\CloudUtil.exe workflow-rollback -n WFStubBuildingMachine -r 0
C:\Program Files (x86)\VMware\vCAC\Design Center\CloudUtil.exe workflow-rollback -n WFStubMachineDisposing -r 0
C:\Program Files (x86)\VMware\vCAC\Design Center\CloudUtil.exe workflow-rollback -n WFStubMachineProvisioned -r 0
```

14. Log in to the vCO client.
15. Select either **Administer** or **Design** mode.
16. Click the **Packages** tab.
17. Delete the vCAC, AMQP, and basic packages of the plug-in the following order:
   a. Right-click **com.infoblox.ipam.vcac** and select **Delete element with content**.
   b. In the **Delete confirmation** window, click **DELETE ALL!**
   c. Repeat steps **a** and **b** for **com.infoblox.ipam.amqp**.
   d. Repeat steps **a** and **b** for **com.infoblox.ipam**.

18. Log in to the vCO configuration interface.
19. On the **Startup Options** tab, click **Restart service**, and then click **Restart the vCO configuration server**.
INFOBLOX IPAM PLUG-IN FOR VMWARE BEST PRACTICES

Organizations can use VMware’s vCloud Director to provision and de-provision new services based on virtual machines. vCenter Orchestrator (part of vCenter) is the workflow engine used to automate this process. The organization may execute the provisioning process using an existing vCenter 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 vCenter Orchestrator.
- Define an admin account on the NIOS appliance, the name of which corresponds to the vCenter 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 the Infoblox IPAM Plug-In for VMware on page 7.
- When production requires a new VM or vApp, the workflow or action must know which DHCP network or range from which to assign an IP address to a new VM. This DHCP network or range must already be defined in NIOS.
- Ensure you have the vApp templates envisioned for use with the Infoblox IPAM Plug-In for VMware.
- The DHCP network or range also should be exclusively for use by the vCenter 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.
- Each workflow creating a vApp must have a corresponding workflow that destroys that vApp. Otherwise, the IPAM information could be out of synchronization between the NIOS or vNIOS appliance and the vSphere or vCloud Director systems.

INFOBLOX IPAM PLUG-IN FOR VMWARE CPU AND MEMORY UTILIZATION FOR WORKFLOW EXECUTION

<table>
<thead>
<tr>
<th>Workflow</th>
<th>CPU Utilization</th>
<th>RAM Utilization</th>
<th>RAM Utilization in %</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add Network</td>
<td>2.6%</td>
<td>0.023 GB</td>
<td>1.5%</td>
</tr>
<tr>
<td>Create vApp with VM networks configured via IPAM</td>
<td>3.6%</td>
<td>0.060 GB</td>
<td>3.0%</td>
</tr>
<tr>
<td>Destroy vApp from IPAM</td>
<td>6.0%</td>
<td>0.060 GB</td>
<td>3.0%</td>
</tr>
<tr>
<td>Remove Host Record or A/AAAA/PTR/CNAME</td>
<td>5.2%</td>
<td>0.061 GB</td>
<td>3.0%</td>
</tr>
<tr>
<td>Remove Network</td>
<td>3.1%</td>
<td>0.058 GB</td>
<td>2.9%</td>
</tr>
<tr>
<td>Reserve an IP</td>
<td>4.5%</td>
<td>0.046 GB</td>
<td>2.3%</td>
</tr>
<tr>
<td>Reserve an IP in Range</td>
<td>4.1%</td>
<td>0.058 GB</td>
<td>2.9%</td>
</tr>
</tbody>
</table>
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.


- **Erlang/OTP** programming language interpreter, version 15b or above (for example, otp_win32_R15B) – Download from http://www.erlang.org/.

- **RabbitMQ** distributable for Windows, version 2.8.2 or above (for example, rabbitmq-server-2.8.2.exe), from http://www.rabbitmq.com/install-windows.html.

- **VMware vCenter Orchestrator AMQP Plug-In** version 1.0.2 – Download from https://my.vmware.com/web/vmware/details?downloadGroup=VCO_AMQP_PLUGIN_102&product=268

- **vCloud Director Notifications** package – Download the package from the VMware web site http://communities.vmware.com/docs/DOC-20446. The file is named com.vmware.coe.vcd55.notifications.package. The latest 5.5 version of the package is compatible with vCloud Director 5.1 and 5.5.


### 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>CIDR (Classless Inter-Domain Routing) Notation</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:DB8:0:0:0:0:0:0 to 2001:DB8::FFFF:FFFF:FFFF:FFFF.</td>
</tr>
<tr>
<td>DHCP (Dynamic Host Configuration Protocol)</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>DHCP Template</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>DNS (Domain Name System)</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>DNS View</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>Extensible Attribute</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>Fixed Address</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>FQDN (fully qualified domain name)</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>Grid™ Technology</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>Grid Manager</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>Grid Master</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>Grid Member</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>
</tbody>
</table>
## Term | Description
--- | ---
Host Record | 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.

IPAM (IP Address Management) | 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.

Network Mask or Netmask | 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.

Network View | 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.

NIOS | 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.

NIOS Virtual Appliance | 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.

Reservation | 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.

Subnet (or network) | A logical division of an IP network. A subnet of network may also be called a network. For example, 10.1.0.0/16 is a subnet of 10.0.0.0/8, and fc80:8:8:16::/64 is a subnet of fc80:8:8::/48.

Superuser | An admin user account that has unrestricted access to Infoblox Multi-Grid Manager, Grid Manager, or System Manager.

vNIOS | 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.