Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>3</td>
</tr>
<tr>
<td>Current Challenges</td>
<td>3</td>
</tr>
<tr>
<td>General Pain Points</td>
<td>3</td>
</tr>
<tr>
<td>Limitations in the current Infoblox Cloud Solutions</td>
<td>3</td>
</tr>
<tr>
<td>Solution</td>
<td>3</td>
</tr>
<tr>
<td>Cloud Platform Appliance</td>
<td>3</td>
</tr>
<tr>
<td>Cloud Network Automation</td>
<td>3</td>
</tr>
<tr>
<td>Target Audience</td>
<td>4</td>
</tr>
<tr>
<td>Deployment</td>
<td>4</td>
</tr>
<tr>
<td>Architecture</td>
<td>5</td>
</tr>
<tr>
<td>Deployment Instructions</td>
<td>5</td>
</tr>
<tr>
<td>Setup Details</td>
<td>5</td>
</tr>
<tr>
<td>Grid Master</td>
<td>6</td>
</tr>
<tr>
<td>Grid Member</td>
<td>9</td>
</tr>
<tr>
<td>Cloud Platform Members</td>
<td>12</td>
</tr>
<tr>
<td>Cloud-api-only user</td>
<td>15</td>
</tr>
<tr>
<td>Extensible Attributes</td>
<td>16</td>
</tr>
<tr>
<td>Network Views, Networks, DNS, Tenants and Virtual Machines</td>
<td>18</td>
</tr>
<tr>
<td>Use Cases/Benefits</td>
<td>26</td>
</tr>
<tr>
<td>Locally survivable solution within a data center</td>
<td>26</td>
</tr>
<tr>
<td>Scalable Redundant Solution for API Calls</td>
<td>27</td>
</tr>
<tr>
<td>Multi-tenant Solution</td>
<td>27</td>
</tr>
<tr>
<td>Proxy</td>
<td>29</td>
</tr>
<tr>
<td>UI Support for delegated objects</td>
<td>32</td>
</tr>
<tr>
<td>Enhanced User Interface for Cloud Environments</td>
<td>36</td>
</tr>
<tr>
<td>Cloud Dashboard and Report</td>
<td>36</td>
</tr>
<tr>
<td>Known Limitations</td>
<td>40</td>
</tr>
</tbody>
</table>
Introduction

With an increase in number of customers moving their datacenters to the cloud, there is an increase in demand for the IT industry to comply with their requirements. Infoblox offers simplicity of deployment, ease of management, and a rich set of APIs for data center automation.

Current Challenges
While migrating to the cloud, administrators face a wide range of challenges.

General Pain Points
- Lack of IT Agility: Agility cannot be accomplished without full network automation in IT, including DDI. Network provisioning is not agile for application delivery. People need capabilities such as on-demand provisioning and self-service management for DevOps. DevOps needs automated IP/DNS in network blueprints.
- High Operating Costs: Greater complexity and higher costs in implementing network solutions and troubleshooting. It takes too much time and expense to deploy applications. Manual IP address/DNS provisioning is slow and error-prone. Diverse and complex network configurations like routing and NATing are tough to manage. Also, it is expensive to integrate IP/networks/zones for every acquisition or subsidiary.
- Low Employee Productivity: Risk of slow/failed rollouts of big cloud initiatives. Service levels affected by network outages
- Lack of visibility: There is no central reporting on lease history and records for DDI across enterprise networks, leading to no visibility to IP address/DNS records for VM/network resources.
- Lack of reliable DDI for Private Cloud: Stability and simplified upgrades of underlying network inhibits Cloud/Virtualization rollout. DDI functions don’t recover on failures.

Limitations in the current Infoblox Cloud Solutions
- Lack of local survivability for distributed data centers: By default, all API calls go to the Grid Master for any Grid. If there are WAN connectivity issues, spinning up of VMs and assigning them IP addresses/DNS host records may be impacted.
- Lack of scalability for API calls: API calls to the Grid Master add to its load. Unless you have multiple Grid Master Candidates in your environment that can be used to distribute REST API read only operations, there is no capability to distribute API calls across multiple appliances when VMs are spun up in batches.

Solution
Infoblox Actionable Network Intelligence enables you to support a nimble and dynamic next generation data center that can handle anything your business demands. You can increase business speed, agility, and efficiency by taking charge of your core network services and security.

Infoblox offers a rich set of APIs with which you can automate core network actions across your data center, virtualized environments, and the cloud with Infoblox DNS, DHCP, and IPAM (DDI). It allows you to proactively detect, isolate, and stop data exfiltration that exploits DNS vulnerabilities with enhanced DNS security and real-time threat intelligence.

To help overcome the limitations outlined above, Infoblox offers Cloud Platform (CP) Appliances and the Cloud Network Automation (CNA) License.

Cloud Platform Appliance
A Cloud Platform Appliance is a Grid member designed and dedicated to accept and process WAPI (RESTful API) requests related to cloud objects, in addition to serving DNS and DHCP protocols. Cloud Platform appliances support cloud API requests, which is a subset of the WAPI requests. You can deploy multiple Cloud Platform Appliances within your Grid to scale the processing of API requests and/or to provide redundancy.

Cloud Network Automation
The Infoblox Cloud Network Automation solution enables automation of IPAM (IP address management) for physical and virtual network devices on your Cloud Management Platform (CMP) (whether it is private, public, or
hybrid). Instead of manually provisioning IP addresses and DNS name spaces for network devices and interfaces, you can use Cloud Network Automation to leverage DNS and DHCP features of the Grid to manage your cloud networks. When your cloud consists of many servers and VMs (virtual machines) that have multiple associated network interfaces, manually provisioning and de-provisioning IP addresses and managing DNS and DHCP data can become error-prone. Utilizing Cloud Network Automation can minimize human errors by streamlining IPAM, improve visibility of your cloud networks, and maximize the flexibility and efficiency that virtualization offers in your cloud environment. In multi-tenant heterogenous cloud environments, Cloud Network Automation enables a holistic view of the network components, and simplifies their management. It makes it possible to assign Tenant permissions to admin users to restrict these users to only be able to view objects related to a given tenant or a set of tenants. Cloud Network Automation is a software module license that is enabled on the Grid Master.

Target Audience
This solution is applicable to Enterprise IT organizations, Cloud/Service Providers that:

- Need to allocate Networks/Network Ranges to Tenants for self-service provisioning of VMs by functional teams
- Need to ensure tenant hosts are registered automatically in DNS for both public/external and private/internal networks
- Need to maintain visibility into the IP space allocated in the private cloud environment
- Need to maintain accurate DNS records for VMs allocated in private cloud environments
- Need to be able to view historic data on IP Address assignment for VMs for troubleshooting and security/auditing purposes in private cloud environments

Deployment
Cloud Management Platforms (CMPs) such as VMware vRealize Automation (in conjunction with vRealize Orchestrator) and OpenStack orchestrate the provisioning of virtual machines (VMs) within the data center/private cloud. Infoblox Adapters are available for each of these CMPs and automate IP address allocation and DNS record creation for VMs as part of the VM provisioning process. Every time a VM is created through the CMP, this will result in a WAPI call to the Grid Master to create Host Records or separate Fixed Address/A/PTR records using the Next Available IP function for a given network. Similarly, when a VM is destroyed through the CMP, a WAPI call will be made to the Grid Master to de-allocate the IP address and delete the associated DNS records. Creation of other Infoblox objects such as networks, zones, network views, DNS views, can also be done as part of the provisioning process or by invoking workflows through the CMP. The adapters can be configured to support overlapping networks by specifying the use of Network Views/DNS Views when records are created. This is often used for implementing multi-tenancy for cloud environments.

The Cloud Platform Grid Member introduces the capability to respond to WAPI calls locally within the data center by the same member(s) that are serving protocols to that cloud environment. This enables local survivability for record creation/deletion with the ability to centrally manage multiple data center environments through a single Grid. Having the ability to respond to API calls through local members also increases the scale/responsiveness of the system since APIs do not have to go back to the Grid Master to create objects which must be synchronized to the local members. Instead, all API calls for that particular data center can be served locally and objects created immediately.

In addition to the Cloud Platform Grid Members, Infoblox has a Cloud UI on the Grid Master to enable administrators to view Infoblox Cloud objects in a cloud-centric fashion. For example, IP address assignments for VMs can be filtered for particular tenants and this view can be delegated to specific tenant administrators enabling multi-tenancy.
Architecture

As shown in the figure, we will consider two cloud environments, each served by a cloud platform member within its environment. The cloud platform members will provide DNS and DHCP services, reasons being:

- Since most cloud environments require both an internal/private DNS and the ability to access servers (like web servers) in the cloud via the external network. The adapters can be configured to create DNS records for both private and external DNS.
- Cloud environments are primarily used to host servers. Therefore, most IP address allocation must be done as a static assignment either by means of a Fixed Address served through DHCP or by using tooling within the Hypervisor to statically inject the IP address into the VM configuration. Because of this, a DHCP server may be optional.

Due to the dynamic nature of the environment, if you need to be able to have visibility on which IP addresses have been allocated to which VMs over time, a reporting appliance can be added in the corporate headquarters. Having visibility of IP address assignment for auditing/compliance reasons is one of the drivers for including Infoblox in cloud deployments.

Deployment Instructions
This deployment guide leverages the above-mentioned architecture and covers the steps to deploy an environment for Proof of Concept purposes only. When doing a production deployment, please ensure that you follow the Infoblox recommended best practices.

Setup Details
This deployment guide uses vNIOS appliance for VMWare. For more information, refer to the vNIOS for VMWare Installation Guide found on the Infoblox Support Site. Please note that the Cloud Platform Appliance is only available as a virtual appliance.
vNIO for VMware

The below table gives you the configuration details used in this guide.

<table>
<thead>
<tr>
<th>Virtual Machine</th>
<th>Version</th>
<th>IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Grid Master</td>
<td>8.2.1/820</td>
<td>172.26.1.2</td>
</tr>
<tr>
<td>Grid Member 1</td>
<td>8.2.1/810</td>
<td>172.26.1.3</td>
</tr>
<tr>
<td>Cloud Platform Member 1</td>
<td>8.2.1/V800</td>
<td>172.26.1.4</td>
</tr>
<tr>
<td>Cloud Platform Member 2</td>
<td>8.2.1/V800</td>
<td>172.26.1.5</td>
</tr>
<tr>
<td>Windows</td>
<td>7</td>
<td>172.26.1.7</td>
</tr>
</tbody>
</table>

The below image represents the vApp setup that will be used in this guide.

![Figure 2] VMware vAPP Setup for the CP-CNA Virtual Lab Environment

The Windows machine will be used to access the Grid UI, and the UNIX machine will be used to issue cURL commands to make WAPI calls.

Please note that this guide only covers features related to Cloud Network Automation and Cloud Platform. For details on how to install and configure a Grid, please refer to the NIOS Installation Guide and Administration Guide found on the Infoblox Support Site.

Grid Master

1. Once you have the vNIOs downloaded and imported on the ESXi host from the vSphere Client, power it on and install the NIOS, DNS, DHCP, and Grid licenses from the CLI using the "set temp_license" command.
2. Using the Windows 7 virtual machine, login to the grid UI and configure it as required.
3. Once the configuration is complete, navigate to **Grid → Grid Manager**, and click on each of DHCP, DNS and NTP services and start them on the grid master.

![Grid Manager screenshot](image1)

4. Now, login to the grid master CLI, and add the Cloud Network Automation License.

```
Infoblox > set temp_license
1. DNSone (DNS, DHCP)
2. DNSone with Grid (DNS, DHCP, Grid)
3. Network Services for Voice (DHCP, Grid)
4. Add DNS Server license
5. Add DHCP Server license
6. Add Grid license
7. Add Microsoft management license
8. Add vMIDOS license
9. Add Multi-Grid Management license
10. Add Query Redirection license
11. Add Response Policy Zones license
12. Add FireEye license
13. Add DMS Traffic Control license
14. Add Cloud Network Automation license
15. Add Security Ecosystem license
16. Add Flex Grid Activation license

Select license (1-16) or q to quit: 14

This action will generate a temporary 60-day Cloud Network Automation license. Are you sure you want to do this? (y or n): __
```
5. Logout and login to the grid UI from the Windows machine. You can see the Cloud tab as shown below.

Grid Member

1. Add grid member to the grid. From the UI, navigate to **Grid → Grid Manager → Members → +**
2. Once you have the vNIOs downloaded and imported on the ESXi host from the vSphere Client, power it on and install the NIOS, DNS, DHCP, and Grid licenses from the CLI using the "set temp_license" command.

```
Infoblox > show license
Version : 8.2.1-359366
Hardware ID : 42018a8740211c43c534608221619790
License Type : DNS
Expiration Date : 11/20/2017
License String : EwAAAPBiIrf62+FFc2+MsUS3n30hGYig=
License Type : DHCP
Expiration Date : 11/20/2017
License String : FAAAAPBkvlL4+L4S2a9iVyzhlFcsbCZ0
License Type : Grid
Expiration Date : 11/20/2017
License String : GgAAAPFiquf2uv8HmpPiVy+skRrTyZiF3ccFeGxAr
License Type : vNIOs (model IB-VM-810)
Expiration Date : 11/20/2017
License String : GgAAAOJit+33tr9dl68uGS7gkh×YZTV3d5kISxkr
```
3. From the CLI, type `set network` to configure the network and add the member to the grid.

```
Enter IP address: 172.26.1.3
Enter netmask [Default: 255.255.255.0]:
Enter gateway address [Default: 172.26.1.1]:
Configure IPv6 network settings? (y or n): n
Become grid member? (y or n): y
Enter Grid Master VIP: 172.26.1.2
Enter Grid Name: nios.infoblox.com
Enter Grid Shared Secret: test

New Network Settings:
IPv4 address: 172.26.1.3
IPv4 Netmask: 255.255.255.0
IPv4 Gateway address: 172.26.1.1

Old IPv4 Network Settings:
IPv4 address: 192.168.1.2
IPv4 Netmask: 255.255.255.0
IPv4 Gateway address: 192.168.1.1
Join grid as member with attributes:
Grid Master VIP: 172.26.1.2
Grid Name: nios.infoblox.com
Grid Shared Secret: Infoblox

WARNING: Joining a grid will replace all the data on this node!
Is this correct? (y or n): y
```

4. Once the member has successfully joined the grid, navigate to `Grid → Grid Manager`, and click on each of DHCP, DNS and NTP services and start them on the grid member.
Cloud Platform Members

1. Add the first cloud platform member to the grid. From the UI, navigate to Grid → Grid Manager → Members → +

2. Once you have the vNIOS image for cloud platform downloaded and imported on the ESXi host from the vSphere Client, power it on and install the NIOS, DNS, DHCP, Grid, and Cloud Platform Appliance
licenses from the CLI using the "set temp_license" command.

3. From the CLI, type `set network` to configure the network and add the cloud platform member to the grid.

```
Enter IP address: 172.26.1.4
Enter netmask [Default: 255.255.255.0]:
Enter gateway address [Default: 172.26.1.1]:
Configure IPv6 network settings? (y or n): n
Become grid member? (y or n): y
Enter Grid Master VIP: 172.26.1.2
Enter Grid Name: Infoblox
Enter Grid Shared Secret: test

New Network Settings:
  IPv4 address: 172.26.1.4
  IPv4 Netmask: 255.255.255.0
  IPv4 Gateway address: 172.26.1.1

Old IPv4 Network Settings:
  IPv4 address: 192.168.1.2
  IPv4 Netmask: 255.255.255.0
  IPv4 Gateway address: 192.168.1.1

Join grid as member with attributes:
  Grid Master VIP: 172.26.1.2
  Grid Name: Infoblox
  Grid Shared Secret: test

WARNING: Joining a grid will replace all the data on this node!
  Is this correct? (y or n): _
```
4. Once the member has successfully joined the grid, navigate to **Grid → Grid Manager**, and click on each of DHCP, DNS and NTP services and start them on the cloud platform member.

5. Notice that you can now see an entry for *Cloud-API*. This was automatically added when the Cloud Platform member joined the grid. Select the member and start the service. The cloud API service provides the ability to automate management of IP addresses and DNS records so your cloud environment can take full advantage of IPAM, DNS, and DHCP capabilities in NIOS without the need for manual intervention. This cloud API service accepts and processes a subset of the WAPI requests that are currently supported on the Grid Master either directly from an adapter or proxied through another Cloud Platform Appliance or from the Grid Master.

6. Repeat steps 1 to 5 for the second Cloud Platform Member.
7. Navigate to **Cloud → Cloud Platform Members**. You should be able to see both the members you added.

![Cloud Platform Members](image)

cloud-api-only user

You must define admin users and their permissions in the admin group and assign specific roles to it before you can use these admin users to send cloud API requests. By default, the admin-group with super user permissions does not have authorization to make cloud API requests.

When you install valid licenses, and configure your Grid for Cloud Network Automation, NIOS enables the cloud-api-only admin group. You can assign admin users to this group so they are authorized to send cloud API requests to the Cloud Platform Appliances. Note that you cannot delete this admin group or create a new admin group using the same name.

Since Cloud Platform member supports cloud API requests, which is a subset of the WAPI requests, in order to make API calls to it, you need to create a user in the cloud-api-only group.

![Administrators](image)

1. Navigate to **Administration → Administrators → Admins → +**, and specify the details for the new user. While selecting the **Admin Group**, select **cloud-api-only**.
This guide uses ‘cloud-admin’ as the Login (user name), and ‘infoblox’ as Password.

2. Click **Save & Close**.

Extensible Attributes
Before the Cloud Platform Grid members joined the Grid, the Grid Master had the following list of built-in Extensible Attributes.
Navigate to **Administration → Extensible Attributes** to see the list EAs available after adding the Cloud Platform Members to the Grid.
Network Views, Networks, DNS, Tenants and Virtual Machines

When a network is created either the Grid Master or a Cloud Platform Member can be authoritative on that network to avoid conflicts. The network can be created on a Grid Master and then delegated to a Cloud Platform Member or it can be created directly on a Cloud Platform Member through a WAPI call.

Once the network is created and assigned to a Cloud Platform Member, all further updates to related network objects will be processed by the Cloud Platform Member assigned to it.

In this guide, we will first create a network view, followed by network, authoritative zone, DNS entry for a Virtual Machine within a Tenant.

A network view is 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.

1. In a multi-tenant environment, where you may have overlapping IP address spaces, a network view can be delegated to be served by a Cloud Platform member. All the network objects within that network view will then be delegated to the designated Cloud Platform member. To create a network view, navigate to Administration → Network Views → +, and specify the details.

2. To create a network in this view, navigate to Data Management, select the newly created network view from the drop-down box on the left, and click on +.
3. Select **Manually Add Network**, and specify the network details.

![Network Details](image1)

4. While selecting member, select the Cloud Platform Member.

![Member Selection](image2)

5. Click on **Save & Close**.
6. The network is created.

7. Navigate to **DNS → Zones → + → Add an authoritative forward-mapping zone**, to add an authoritative zone.

8. In the next screen, select the Cloud Platform Member 1 as the name server for this zone. You will see that selecting the name server in this step automatically delegates the zone to the Cloud Platform.
9. Click on **Save & Close**, and Restart the services when prompted.

10. Notice that the newly created zone has been delegated to the cloud platform member.

11. To delegate the entire network view to Cloud Platform Member, navigate to **Administration -> Network Views**, click on the gear icon next to the network view and select **Edit**. Select the Cloud Platform Member in the **Delegated To** field. This will automatically delegate all networks and zones in that network view to the cloud platform member.
12. Click Save & Close, and restart the services. You will notice that the network view has been delegated to the cloud platform member.

13. Navigate to **Data Management → cp1view → IPAM**. You will notice that the previously created network has been delegated to the cloud platform member, and the color of the icon has changed from green to blue.
14. Clicking on the gear icon next to the network to edit it, you will see that delegation has been inherited from the network view.

15. Now that you have isolated a network and an authoritative zone to a network view being served by a locally available cloud platform member, all calls pertaining to that data center will now be made to the cloud platform member.

16. This step demonstrates how to create a host record (for virtual machines) using a cloud API request.
<table>
<thead>
<tr>
<th>Operation</th>
<th>REST Method</th>
<th>API Call</th>
<th>Sample cURL Command</th>
<th>Sample Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create a Host Record within a Tenant</td>
<td>POST</td>
<td><a href="https://172.26.1.4/wapi/v2.7/record:host">https://172.26.1.4/wapi/v2.7/record:host</a></td>
<td>curl -k -u cloud-admin:infoblox-H ‘content-type: application/json’ -X POST &quot;<a href="https://172.26.1.4/wapi/v2.7/record:host?_return_fields%2B=name,extattrs">https://172.26.1.4/wapi/v2.7/record:host?_return_fields%2B=name,extattrs</a>&quot; -d &quot;{&quot;name&quot;: &quot;vm1.test.com&quot;, &quot;ipv4addrs&quot;: [{&quot;ipv4addr&quot;: &quot;10.10.10.11&quot;}], &quot;view&quot;: &quot;default.cp1view&quot;, &quot;extattrs&quot;: { &quot;Tenant ID&quot;: {&quot;value&quot;: &quot;DC1&quot;}, &quot;CMP Type&quot;: {&quot;value&quot;: &quot;Openstack&quot;}, &quot;Cloud API Owned&quot;: {&quot;value&quot;: &quot;True&quot;}, &quot;VM ID&quot;: {&quot;value&quot;: &quot;VM-ID-1&quot;}, &quot;VM Name&quot;: {&quot;value&quot;: &quot;LinuxVM1&quot;} }}]&quot;</td>
<td></td>
</tr>
</tbody>
</table>

17. On the Grid UI, navigate to Data Management → cp1view → DNS → test.com, you can see the newly created host entry. Edit the properties for the vm1 Host record to see Extensible Attributes saved for this record.

![Infoblox Cloud Platform and Cloud Network Automation – October 2017](image)
18. Navigate to **Cloud → Tenants**. You will notice that a new tenant called *DC1* has been created.

19. Click on *DC1 → VMs*. You will see the details of the Virtual Machine you specified while creating the host record.
20. Similarly, you can create, manage and delete other network objects, like containers, and other DNS records.

Use Cases/Benefits

The use cases below use WAPI (RESTful API) calls or a set of GUI based tasks or a combination of both to demonstrate each of its benefits. For more information on WAPIs, please refer to the REST API Documentation available on the Infoblox Support Site.

Locally survivable solution within a data center

This solution offers better localized management of objects by delegating object ownership to cloud platform members. Cloud platform members can serve API calls and protocols (DNS, DHCP) locally within each data center while still retaining centralized management.

The Cloud Platform members will continue to serve APIs even when disconnected from the Grid Master. If for some reason, you are facing WAN connectivity issues or the Grid Master is offline, your environment is not brought down since the API calls are rendered locally by the Cloud Platform members. When the Grid Master comes back online, the Cloud Platform Member and Grid Master automatically sync up and all the updates made to the network in the absence of the Grid Master is now available with the Grid Master.

You can use the following steps to verify this.

1. Turn off the Grid Master.
2. Create a host record for a virtual machine on the locally available Cloud Platform Member using WAPI.

<table>
<thead>
<tr>
<th>Operation</th>
<th>REST Method</th>
<th>API Call</th>
<th>Sample Body</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create a Host Record within a Tenant</td>
<td>POST</td>
<td><a href="https://172.26.1.4/wapi/v2.7/record:host">https://172.26.1.4/wapi/v2.7/record:host</a></td>
<td></td>
</tr>
</tbody>
</table>

This clearly shows that you can continue managing your network objects on the Cloud Platform Member, even when the Grid Master is offline, demonstrating local survivability provided by the Cloud Platform.
3. Power on the Grid Master, and login to the UI after a few minutes. Navigate to **Cloud → Tenants → DC1 → VMs**. You will notice that information about the newly created record is synced with the grid.

Scalable Redundant Solution for API Calls
You can scale the API call capacity horizontally and provide API call redundancy by adding Cloud Platform Appliances to the data center.

Multi-tenant Solution
You can leverage a combination of Network Views and Cloud Platform members to get a multi-tenant solution.

When a Network View is created, a corresponding DNS View is created. DNS Views provide 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 appliance can provide a different answer to the same query, depending on the source and/or destination of the query. Also, a DNS view can be in one network view only, but a network view can have multiple DNS views.

Network Views can be used in cloud environments to isolate each of the data center or tenant to their own respective view. This enables support of overlapping networks across different tenants, each in its own Network View, thus enabling multi-tenancy in cloud environments. In a data center location, a locally available Cloud Platform Member can be associated with a Network View. Please note that when DHCP service is provided, a member may only be associated to a single network view/tenant.

In order to demonstrate multi-tenancy, this guide will show you how to create overlapping networks and tenants with same names. To create Network Views, networks and tenants you can either follow the steps in Network Views, Networks, DNS, Tenants and Virtual Machines or the following steps.
1. To create a Network View and delegate it to the second cloud platform member in our environment, navigate to **Administration → Network Views → +**

2. The next set of steps will demonstrate how to create overlapping networks and tenants using WAPI calls.

<table>
<thead>
<tr>
<th>Operation</th>
<th>REST Method</th>
<th>API Call</th>
<th>Sample Body</th>
</tr>
</thead>
</table>
| On Cloud Platform Member 1, create a network 1.1.1.0/24 in cp1view under a tenant Dev | POST | https://172.26.1.4/wapi/v2.7/network | curl -k -u cloud-admin:infoblox -H 'content-type: application/json' -X POST "https://172.26.1.4/wapi/v2.7/network?_return_fields%2B=network,extattrs" -d '{"network": "1.1.1.0/24","network_view": "cp1view","extattrs": { "Tenant ID": {"value": "Dev"}, "CMP Type": {"value": "Openstack"}, "Cloud API Owned": {"value": "True"}}}'}

<table>
<thead>
<tr>
<th>Operation</th>
<th>REST Method</th>
<th>API Call</th>
<th>Sample Body</th>
</tr>
</thead>
</table>
| On Cloud Platform Member 2, create same network 1.1.1.0/24 in cp2view under same tenant Dev | POST | https://172.26.1.5/wapi/v2.7/network | curl -k -u cloud-admin:infoblox -H 'content-type: application/json' -X POST "https://172.26.1.5/wapi/v2.7/network?_return_fields%2B=network,extattrs" -d '{"network": "1.1.1.0/24","network_view": "cp2view","extattrs": { "Tenant ID": {"value": "Dev"}, "CMP Type": {"value": "Openstack"}, "Cloud API Owned": {"value": "True"}}}'}
3. To verify, login to the Grid UI, and navigate to Cloud → Tenants. You can see that the Dev tenant is associated with both the network views.

4. Navigate to Cloud → Networks. You can see that you have 2 networks belonging to the same subnet, each of them isolated to their own network view and being rendered by a separate cloud platform member. This makes it easy to handle network objects locally and in an isolated, yet centralized fashion. In this example where Cloud Platform Member 1 and 2 are in different data centers, cp1view and cp2view are associated with all the network objects in one data center.

Proxy
Cloud Platform Appliances include built-in HTTPS proxy capability that redirects cloud API requests to the appropriate Cloud Platform Appliance or to the Grid Master for processing. In other words, Cloud API requests can be sent to any of the Cloud Platform Appliances within the Grid and the call is either processed locally or transparently forwarded to the appliance that is authoritative for the object referenced in the cloud API request.

User does not have to maintain (cloud network object ←→ owner) relationships.

To demonstrate the proxying capabilities in action, you can follow the steps below:

1. Clear the Syslog records for both the Cloud Platform Members by navigating to Administration → Logs → Syslog. Select the cloud platform member from the drop-down menu and click on the
2. This step demonstrates creation of a host record on a zone rendered by Cloud Platform Member 2 by issuing a WAPI call to Cloud Platform Member 1.

<table>
<thead>
<tr>
<th>Operation</th>
<th>REST Method</th>
<th>API Call</th>
<th>Sample Body</th>
<th>Sample cURL Command</th>
<th>Sample Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Issue the call to Cloud Platform Member 2 to create a zone cp2.com in cp2view</td>
<td>POST</td>
<td><a href="https://172.26.1.4/wapi/v2.7/record:host">https://172.26.1.4/wapi/v2.7/record:host</a></td>
<td><img src="https://example.com/sample_body.json" alt="Sample Body" /></td>
<td><code>curl -k -u cloud-admin:infoblox -H 'content-type: application/json' -X POST 'https://172.26.1.4/wapi/v2.7/record:host?_return_fields%2B=fqdn,grid_primary,extattrs' -d '{&quot;fqdn&quot;: &quot;cp2.com&quot;, &quot;grid_primary&quot;: [{&quot;name&quot;: &quot;cp2.infoblox.com&quot;}], &quot;view&quot;: &quot;default.cp2view&quot;, &quot;extattrs&quot;: { &quot;Tenant ID&quot;: {&quot;value&quot;: &quot;Dev&quot;}, &quot;CMP Type&quot;: {&quot;value&quot;: &quot;Openstack&quot;}, &quot;Cloud API Owned&quot;: {&quot;value&quot;: &quot;True&quot;} }}'</code></td>
<td><img src="https://example.com/sample_output.json" alt="Sample Output" /></td>
</tr>
<tr>
<td>Issue the call to Cloud Platform Member 1 to create a Host Record under the zone cp2.com in cp2view</td>
<td>POST</td>
<td><a href="https://172.26.1.4/wapi/v2.7/record:host">https://172.26.1.4/wapi/v2.7/record:host</a></td>
<td><img src="https://example.com/sample_body.json" alt="Sample Body" /></td>
<td><code>curl -k -u cloud-admin:infoblox -H 'content-type: application/json' -X POST 'https://172.26.1.4/wapi/v2.7/record:host?_return_fields%2B=name,extattrs' -d '{&quot;name&quot;: &quot;vm1.cp2.com&quot;, &quot;ipv4addrs&quot;: [{&quot;ipv4addr&quot;: &quot;1.1.1.11&quot;}], &quot;view&quot;: &quot;default.cp2view&quot;, &quot;extattrs&quot;: { &quot;Tenant ID&quot;: {&quot;value&quot;: &quot;Dev&quot;}, &quot;CMP Type&quot;: {&quot;value&quot;: &quot;Openstack&quot;}, &quot;Cloud API Owned&quot;: {&quot;value&quot;: &quot;True&quot;}, &quot;VM ID&quot;: {&quot;value&quot;: &quot;VM-ID-1&quot;}, &quot;VM Name&quot;: {&quot;value&quot;: &quot;LinuxVM1&quot;}}}'</code></td>
<td><img src="https://example.com/sample_output.json" alt="Sample Output" /></td>
</tr>
</tbody>
</table>
3. From the UI, navigate to **Administration → Logs → Syslog** → Select the cloud platform member from the drop-down box. You will see that the API request was proxied.
UI Support for delegated objects

The NIOS GUI provides the user an ability to create/delete Fixed Addresses, Reservations and Host within the scope of a Cloud Platform Member delegation. In this case, the creation/deletion is forwarded to the delegated member. Please note that updating is not allowed. Also, this is only supported in NIOS versions 7.3 onwards.

You can see this feature in action using the following steps.

1. From the Grid UI, navigate to **Data Management → cp1view → DNS**. Click on the authoritative zone.

2. To add a Host record, click on the **v** symbol next to **Add**, add **Host → Host**.

![Image of the Grid UI showing Data Management, cp1view, DNS.](image1.jpg)

![Image of adding a Host record in the Grid UI.](image2.jpg)
3. Fill in the necessary details, and click on **Next**. By design, the option to **Schedule for Later** is disabled.

Please note that, you cannot use the **Next Available IP Address** function in the **IPv4 Addresses** field. It will give you the following error.

Request the next available IP address, when parent object (network) is not under authority of current member, is forbidden.

4. In the **Extensible Attributes** window, you will notice that a list of mandatory EAs are pre-populated.
5. Fill in the fields, and **Save & Close**

6. A new host record is created.

7. You can delete the records, one at a time. Please note that, when you select multiple records, the option to delete is greyed out.

8. While trying to add any other type of record, you will encounter the following error.

   The operation insert is not allowed from this member as the authority is delegated to another member.
9. To add a fixed address, navigate to Data Management ➔ cp1view ➔ IPAM and select the network.

10. Click on the v symbol next to Add, and Fixed Address ➔ IPv4

11. In the pop-up window, select Add Fixed Address, and click on Next.

12. Type in the necessary details and click on Next. The Next Available IP and Schedule for Later options are greyed out.
13. In the **Extensible Attributes** window, you will notice that a list of mandatory EAs are pre-populated.

![Extensible Attributes Window](image)

14. Fill in the fields, and **Save & Close**.

**Enhanced User Interface for Cloud Environments**

The **Cloud Network Automation** license allows you to manage all the DDI information, organized by tenant, network and virtual machine for cloud objects in NIOS UI in the Cloud tab, as demonstrated throughout the guide.

**Cloud Dashboard and Report**

Cloud Network Automation enables a dashboard with cloud statistics. This includes statistics for IP address utilization by tenant and IP type (fixed/floating). Cloud Networks have been added to **‘Networks over Thresholds’** widget.

The VM Address History Report (IP Addresses and DNS Record Allocations/De-allocations by VM by Tenant) allows you to understand and troubleshoot your environment better. You can also drill down into lease history for VM IPs.
1. To display the Cloud widget, navigate to **Dashboards → Status → Add Content**.

   ![Dashboard Screenshot]

2. Click on **Cloud Statistics** and drag it over to the dashboard.

   ![Dashboard Screenshot]
3. You can see from the Cloud Statistics widget that there are 2 tenants and 3 Cloud Virtual Machines. This widget can automatically refresh to updated as network objects are added or removed.

4. Similarly, add the **Networks Over Threshold** widget. You can see that the **Cloud Networks** are available.

5. To see the various cloud statistics, you can create a separate dashboard for each cloud environment. To create a dashboard, navigate to **Dashboards → Status → Add Dashboard**, and specify a name for the dashboard in the pop-up.
6. Once you **Save and Close**, it opens the new dashboard. Click on the gear icon next to the name of the dashboard and **Add Content**.
7. Repeat Steps 2 and 4.

8. To get Tenant specific statistics, in the Cloud Statistics widget, under Show Statistics From, Select Tenant. Similarly, in the Networks Over Threshold widget, select View Cloud Networks Only and Select Tenant.

Known Limitations

- DHCP fail over association
- Host records
  - Cloud Platform Grid member must be authoritative for both IPAM and DNS
  - Must be on the same member (IPAM and DNS) for host creation to work
- No current support for Microsoft sync
- No current support for DNS Firewall (RPZ)
- No current support for Advanced Data Protection
• No current support for Reporting
• No current support for Network Insight
• No current support for PAPI
• Not every single WAPI call is supported. For more information on what objects are not supported, refer to the REST API documentation available in the Infoblox Support Site.
  o Supports only cloud API requests which is a subset of the WAPI calls.
  o Must use WAPI version 2.0 and above