About Host Records

Host records provide a unique approach to the management of DNS, DHCP, and IPAM data. By using host records, you can manage multiple DNS records and DHCP and IPAM data collectively, as one object on the appliance.

When you create a host record, you are specifying the name-to-address and address-to-name mappings for the IP address that you assign to the host. The Infoblox DNS server then uses this data to respond to DNS queries for the host. When the server receives a name-to-address query, it responds with an A record for an IPv4 host or an AAAA record for an IPv6 host that contains the data from the host record. Likewise, when it receives an address-to-name query for the host, the appliance responds with a PTR record that contains data from the host record.

Additionally, if you specify an alias in the host record, the appliance uses this data as a CNAME record to respond to queries with the alias. It maps the alias to the canonical name and sends back a response with the canonical name and IP address of the host. Thus, a single host record is equivalent to creating A, PTR, and CNAME resource records for an IPv4 address and AAAA and PTR records for an IPv6 address. The appliance supports IDNs for a host record. You can specify alias and domain names in the native character set. For more information about IDN support, see Support for Internationalized Domain Names.

Hosts also support prefix delegation for IPv6. For example, you can specify an IPv6 prefix in the host record of a router. The router then advertises this prefix on one of its interfaces, so hosts that connect to the interface can generate their IP addresses, using the stateless autoconfiguration mechanism defined in RFC 2462, IPv6 Stateless Autoconfiguration. In addition, if the Infoblox DHCP server manages the IP address assigned to the host, the server uses it as a fixed address record as well. The DHCP server assigns the IP address to the host when it receives a DHCP request with the matching MAC address or DUID. Its response includes configuration information, and any DHCP options defined for the host or inherited from the network to which the fixed address belongs. You can also assign multiple IPv4 and IPv6 addresses to a host, as described in Assigning Multiple IP Addresses to a Host.

You can copy an existing host record and turn it into a new one. When you copy a host record, other than the new host name and IP address, all DHCP and IPAM configuration including the MAC address and extensible attributes apply to the new record. You can also modify information, except for the host name and IP address, of an existing host record. For more information about how to copy or modify a host record, see Copying and Modifying Host Records. Note that you can also modify an IPv4 host record and turn it into a IPv4 reservation. For more information, see Configuring IPv4 Reservations.

You can execute immediate discovery on a host record. This simple setting enables you to determine the precise type of device that is associated with the host, along with its IP addresses, its name and other information. You can define extensible attributes for a host record to further describe the device. You can include information such as its location and owner for IP address management purposes. For more information about extensible attributes, see About Extensible Attributes.

Figure 13.2 illustrates how the appliance uses the host record for both DHCP and DNS.

Assigning Multiple IP Addresses to a Host

You can assign multiple IPv4 and IPv6 addresses to a host depending on the function of the device. For example, you can create a host record for a router that supports three network interfaces in two different networks, and assign IP addresses to each interface, as illustrated in Figure 13.3. When the DNS server responds to DNS queries for the host, it includes an A or AAAA record for each IP address.

In addition, if the IP addresses belong to different networks, they can have different DHCP configurations and options. As shown in Figure 13.3, the configuration information and DHCP options of the interface with the IPv6 address 2001:db8:1::2 may be different from the other two interfaces, 10.31.209.5 and 10.31.209.7, because it is in a different network.

Note that if the zone of the host record is associated with networks, the IP addresses must belong to the associated networks. For example, if the host record is in the corpxyz.com zone, which is associated with 10.1.0.0/16 network, then the IP addresses of the host record must belong to the 10.1.0.0/16 network. For more information about associating zones and networks, see Associating Networks with Zones.

Figure 13.2 Using the Host Record for DHCP and DNS

Figure 13.3 Assigning Multiple IP Addresses to one Host Record
Adding Host Records

You can add host records from the Toolbar of the IPAM, DHCP and DNS tabs of the Data Management tab and from the Tasks Dashboard. For more information about the Tasks Dashboard, see Tasks Dashboard.

When you create a host record, you must specify its zone and at least one IP address. If the zone of the host record is associated with one or more networks, the IP addresses must belong to one of the associated networks. If a zone of a host record contains IDNs, the appliance displays the zone name in the native character set.

For Cloud Network Automation, you can create host records within a delegated network view only when you enable DNS for the host record.

To add a host from the Data Management tab:

1. From the IPAM, DHCP or DNS tab of the Data Management tab, expand the Toolbar.
2. Click Add and select the option to add a host from the drop-down menu.
3. In the first page of the Add Host wizard, do the following:
   - **Name:** If Grid Manager displays a zone name, enter the host name here. The displayed zone name can either be the last selected zone or the zone from which you are adding the host. If no zone name appears or if you want to specify a different zone, click Select Zone. When there are multiple zones, Grid Manager displays the Zone Selector dialog box. Click a zone name in the dialog box, and then enter a unique name for the host. The name you enter is prefixed to the DNS zone name that is displayed, and the complete name becomes the FQDN (fully qualified domain name) of the host. For example, if the zone name displayed is corpxyz.com and you enter admin, then the FQDN is admin.corpxyz.com.
   - **Enable in DNS:** This is selected by default. It enables DNS service for the host. If you clear this check box, DNS does not serve this host and you cannot assign it to a zone.
   - **Protected:** This is selected by default. To mark the record as protected in order to restrict DDNS updates to this record, select the Protected check box. This applies to both static and dynamic records.

Alternatively, you can protect records by selecting them, individually or in bulk, in the Resource Records Viewer and clicking Protect Records -> Enable Protection in the Toolbar.

- **DNS View:** Displays the DNS view for the host record. This appears only when you enable the host record in DNS.
- **Host Name Policy:** Displays the host name policy of the selected zone. This appears only when you enable the host record in DNS.
- **RRset Order:** Select one of the following RRset orders that the appliance uses to return A and AAAA records of the host. This check box appears only when you have enabled the configuration of RRset order for the Grid and there are multiple IP addresses in this host record. For more information about how to enable this feature, see Enabling the Configuration of RRset Orders.
  - **Cyclic:** The records are returned in a round robin pattern. This is the default.
  - **Fixed:** The records are returned in the order you specify in this host record. When you select this check box, the appliance displays up and down arrows next to the IPv4 and IPv6 address tables. You can use these arrows to reorder the address list. The appliance returns the A and AAAA records of this host based on the order you define in the address tables.
  - **Random:** The records are returned in a random order.

Note that when you specify Fixed as the RRset order, the appliance places the resource records as follows:
- A and AAAA records of the host in the fixed order you specify in the address tables. Note that the order of the returned A and AAAA records is independent of each other.
- Other A and AAAA records in an undefined order.
- Other record types in the default cyclic order.

For more information about RRset order, see Enabling the Configuration of RRset Orders.

- In the IPv4 Addresses and IPv6 Addresses sections, specify the IP addresses of the host record. Click the Add icon do one of the following:
  - Select Next Available IP Address to retrieve the next available IP address in a network. Infoblox recommends this option to ensure that you assign an IP address from the appropriate network.
  - DHCP: Select this to enable the DHCP services to manage the host IP address. If you do not select this option, the host IP address is not managed by the DHCP server.
  - Comment: Optionally, enter additional information about the host record.
  - Disable: Select this option to temporarily disable the host record. For example, you might want to disable a host when you need to update the network device.

The Cloud section appears when the Cloud Network Automation license is installed on the Grid Master. For information, see Deploying Cloud Network Automation. This section displays the following information:

- Cloud Usage: This field indicates whether this object is associated with any specific cloud extensible attributes or within a scope of delegation. It can be one of the following:
  - Cloud from adapter: Indicates that this object has been created by a cloud adapter and it may or may not be within a scope of delegation at the moment.
  - Cloud from delegation: Indicates that this object is within the scope of delegation or the object itself defines a scope of authority delegation, and it is not created by a cloud adapter.
  - Used by cloud: Indicates that this network or network container is associated with the extensible attribute Is External or Is Shared and the value is set to True, which implies the network is a private or shared network managed by the CMP, and it is not Cloud from adapter or Cloud from delegation.
  - Non-cloud: The object is a regular NIOS object and is not within the scope of any authority delegation nor is it associated with any of these extensible attributes: Cloud API Owned, Is External or Is Shared. NIOS admin users can modify this object based on their permissions.
  - Owned By: A cloud object can be owned by the Grid Master or the cloud adapter. When the object is created by the Grid Master, this shows Grid. If the object is created by the cloud adapter, this shows Adapter. Delegate authority from the Grid Master
  - Delegate To: This field indicates whether the authority for the object you want to have already been delegated. If so, it displays the name of the delegation.

4. (Applies only to Network Insight) In the current wizard step, you can optionally define the following identification values and settings for the new object's port reservation:

- Choose the Device Type: Router, Switch-Router, Switch, MSFT (Microsoft) Server, NetMRI, NIOS, VNIOS, or ESX (VMware) Server. The values on this page are not required for defining the actual port reservation in a later wizard step.
- Choose the Device Vendor: Cisco, Juniper, Aruba, Dell, Infoblox, or HP.
- You can also enter a Location and a Description. These values are advisory and not required for configuration.
- After you define this group of settings, you will still need to define a device port reservation.

5. (Applies only with Network Insight) Click Next to initiate or disable discovery of the new host.

- Choose either Exclude from Network Discovery or Enable Immediate Discovery. If you choose to Exclude, discovery will not execute on the host. If you choose Enable Immediate Discovery, discovery will execute on the host after you save your settings. You may also choose to leave both options disabled.
- By default, the new host inherits its SNMP credentials from those defined at the grid level. Should you wish to override them for a local set of credentials, check the Override Credentials check box and select the SNMPv1/SNMPv2 or SNMPv3 option and enter the locally used credentials. For more information, see Configuring SNMPv1/v2 Credentials for Polling and Configuring SNMPv3 Properties for a complete description of SNMP credentials for discovery. (You can also test SNMP credentials to ensure they work before use.)
- For the new object, you can check the Override CLI Credentials check box to override the inherited set of CLI credentials taken from the Grid level. This set of credentials may be used for the device that is directly associated with the new object (in this case, a Host) in its port reservation.
- You can also click Test CLI Credentials to enter and test a set of CLI login credentials against a device based on its IP address. Port control operations require CLI credentials for the involved devices. (If you are not using port control for the new object, usage of CLI credentials is optional.) Because some IPAM and DHCP objects will use port control features as part of object creation, CLI credentials are automatically leveraged as part of discovery. Ensure you have the correct sets of CLI credentials for devices in your network. For more information, the section Configuring CLI Discovery Properties.
- SSH is the default for CLI operations. Check the Allow Telnet check box if you know the device involved in the object assignment may support Telnet but may not support SSH, or if you want Telnet as an option.

6. (Applies only with Network Insight) Click Next to define switch port connectivity for the device that will be associated with the new host record. This step is optional and not required for creating the new host record. This feature set is also termed port control in Grid Manager. The device to which the new host record will be associated should already be discovered and managed from Grid Manager.
• Begin by checking the Reserve Port check box. Note that reserving a switch port does not guarantee its availability. Optionally, you can skip connecting port configuration by clicking Next.
  
Click the Clear button to remove the selected device from the configuration.
• Click the Select Device button to choose the device for which the port reservation will be associated. You should know the identity of the device to whose interface the new object will be associated before taking this step. For more information, see the section Using the Device Selector.
• After choosing the device, choose the Interface with which the port reservation will be bound. The drop-down list shows only interfaces that are most recently found to be available by Grid Manager during the last discovery cycle. This list will not include any ports that are Administratively Up and Operationally Up or that are otherwise already assigned to other networks or objects.
• The Wizard page also shows a list of any VLANs that are currently configured in the chosen device (The following VLANs are configured). This Wizard page allows only the assignment of an existing VLAN in the chosen device to the new port reservation.
• Check the Configure Port check box to define specific port control settings for the port reservation.
• Choose the Data VLAN and/or the Voice VLAN settings you may need for the port assignment. Depending on the selected device, you may or may not be able to apply VLAN settings.
• Set the Admin Status to Up if you need to activate the port after assignment in the current task.

All port control operations require CLI credentials to be entered into Grid Manager. Because some IPAM and DHCP objects will use port control features as part of object creation, CLI credentials are automatically leveraged as part of discovery and configuration of port constructions such as Admin Up/Down status.

Ensure you have the correct sets of CLI credentials for devices in your network.
• Enter a Description for the port assignment. Infoblox recommends doing so to help other technicians to recognize the port assignment task.

7. Click Next to define extensible attributes. For more information, see Using Extensible Attributes.
8. As the final step in the Add Host wizard, you define when Grid Manager creates the new object by scheduling it. As a separate task, you also schedule when the associated Port Configuration task executes.
   • To create the new Host and its associated port reservation immediately, select Now. The port control event is automatically synchronized to take place at the same time as the activation of the new host.
   • You can choose to have Grid Manager execute the port reservation at the same time as the host object creation. To do so, select At same time as Host.
   • You can have Grid Manager execute the port reservation at a later time by selecting Later. Choose a Selected time by entering or selecting a Start Date (click the calendar icon to choose a calendar date) and a Start Time, and choose a Time Zone.

9. Choose one of the following from the Save & ... drop-down button menu:
   • Click Save & Close to add the Host object and close the wizard (this is the default).
   • Click Save & Edit to add the Host object and launch the editor.
   • Click Save & New to add the Host object and launch the wizard again to add another Host object.

Copying and Modifying Host Records

You can create a new host record by copying an existing one. When you copy a host record, other than the new host name and IP address, all DHCP and IPAM configuration including the MAC address and extensible attributes apply to the new record. You can also modify information, except for the host name and IP address, of an existing host record.

To copy or modify an existing host record:

1. From the Data Management tab, select the IPAM, DHCP, or DNS tab.
2. In the selected tab, search for or navigate to the host record that you want to copy or modify.
3. Perform one of the following:
   • To copy a host record, select the record and expand the Toolbar, and then click Add -> Host -> Copy Host. Grid Manager displays the Host Record editor.
   • To modify a host record, select the record and click the Edit icon. Grid Manager displays the Host Record editor.
4. The Host Record editor provides the following tabs from which you can modify all the fields:
   • General: Enter the new hostname and specify at least one IP address. Optionally, you can modify the information you entered through the wizard as described in Adding Host Records.
   • IPv4 Addresses: Displays the discovered data of the IPv4 addresses, if any, of the host record. For more information, see Viewing Discov ered Data.
   • IPv6 Addresses: Displays the discovered data of the IPv6 addresses, if any, of the host record. For more information, see Viewing Discovered Data.
   • Extensible Attributes: You can add and delete extensible attributes that are associated with a host record. You can also modify the values of extensible attributes. For more information, see Using Extensible Attributes.
   • Permissions: This tab appears only if you belong to a superuser admin group. For more information, see About Administrative Permissions.

5. Save the configuration and click Restart if it appears at the top of the screen.
About Network Containers

Grid Manager uses network containers to group IPv4 and IPv6 networks. A network container is a parent network that contain other network containers and leaf networks. A leaf network is a network that does not contain other networks. For example, Figure 13.4 illustrates the IPv4 20.0.0.0/8 network, which is a network container with two network containers, 20.8.0.0/13 and 20.72.0.0/13. The 20.8.0.0/13 network has two leaf networks, 20.8.0.0/16 and 20.9.0.0/16. The 20.72.0.0/13 network has one leaf network, 20.72.0.0/16.

Figure 13.4 IPv4 Network Container

From Grid Manager, you can click the link of the network container 20.0.0.0/8 in the IP List panel and drill down to the two network containers, 20.8.0.0/13 and 20.7.0.0/13, as shown in Figure 13.5. You can click the network container links to drill down further to the leaf networks.

Figure 13.5 IP List View of Network Containers

In the IPAM tab, when you create an IPv4 or IPv6 network that belongs to a larger network, the appliance automatically creates a network container and puts the leaf network in the container. The appliance also creates network containers when you split IPv4 or IPv6 networks into smaller networks. For more information, see Splitting IPv4 Networks into Subnets and Splitting IPv6 Networks into Subnets.

Adding IPv4 and IPv6 Network Containers and Networks

To add an IPv4 or IPv6 network container or network:

1. From the Data Management tab, select the IPAM tab.
2. Click the Add icon and select either IPv4 Network or IPv6 Network.
3. In the Add Network wizard, create a network as described in Adding IPv4 Networks or Adding IPv6 Networks.

Modifying IPv4 and IPv6 Network Containers and Networks
You can modify existing network settings, with the exception of the network address and subnet mask. To modify an IPv4 or IPv6 network container or network:

1. From the **Data Management** tab, select the **IPAM** tab -> network check box, and then click the **Edit** icon.
2. In the **DHCP** Network editor, modify the network settings as described in **Modifying IPv4 Networks** or **Modifying IPv6 Networks**.

### Deleting Network Containers

Depending on the configuration, you may or may not be able to delete or schedule the deletion of a network container and all its contents. Contents in a network container can include other network containers, leaf networks, and associated objects. For recursive deletions, only network containers and networks are considered. Objects such as hosts are not considered for recursive deletions.

Superusers can determine which group of users are allowed to delete or schedule the deletion of a network container and all its contents. For more information about how to configure the recursive deletion of network containers, see **Configuring Recursive Deletions of Networks and Zones**.

Note that you must have Read/Write permission to all the contents in order to delete a network container. When you delete a network container only, the appliance reparents the other network containers and leaf networks.

The appliance puts all deleted objects in the Recycle Bin, if enabled. You can restore the objects if necessary. When you restore a parent object from the Recycle Bin, all its contents, if any, are re-parented to the restored parent object. For more information about the Recycle Bin, see **Using the Recycle Bin**.

To delete a network container:

1. From the **Data Management** tab, select the **IPAM** tab -> network_container check box. You can select multiple network containers for deletion.
2. Click the **Delete** icon.
3. Do one of the following in the **Delete Confirmation** dialog box:
   - Select one of the following. Note that these options appear only if you are allowed to delete the network container and all its contents.
     - **Delete only the network container and re-parent the subnets**: Select this to delete only the network container and re-parent its subnets.
     - **Delete the network container and all its subnetworks**: Select this to delete both the network and its contents.
   - Click **Yes**.

The appliance puts the deleted network container in the Recycle Bin, if enabled. You can also schedule the deletion for a later time. Click **Schedule Deletion** and in the **Schedule Change** panel, enter a date, time, and time zone. For information, see **Scheduling Deletions**. For information about scheduling recursive deletions of network containers, see **Scheduling Recursive Deletions of Network Containers and Zones**.

### List View of Network Containers