DEPLOYMENT GUIDE

Grid and Services Deployment on IPv6-only Networks, and Migration from IPv4 Networks

Table of Contents

IPv6 Planning **3**
- Planning with Abundance 3
- Standard Subnet Size 3
- Point-to-point Links 3
- Standard Site Allocation 3
- PI vs. PA 3
- Making your Address Plan Readable 4
- Location and Function Assignments 4
- Host Address Assignment 4

Deployment Instructions **5**
- Grid Communication 5

IPAM **7**
- Add an IPv6 Network 7

DNS **9**
- IPv6 Specific Records 10
- Create an Alias Record 12
- Create a Host Record 14
- DNS64 16
- Configuring DNS64 18
- Setting DNS64 Group Properties 19
- Modifying DNS64 Group Properties 19
- Enabling DNS64 25

Match Clients for DNS Views 28
- Configuring Match Clients List for a DNS View 29

Enabling IPv6 Grid DNS Properties 32
Enabling IPv6 Grid DNS Member Properties 34

DHCP **36**
Configuring for IPv6 DHCP 36
- Enable IPv6 Grid Member DHCP Properties 38
- Associating Networks with Zones 39
- Keeping Leases in Deleted IPv6 Networks and Ranges 42
- Configuring Fixed Address Leases For Display 44
- Scavenging Leases 46
- DHCPv6 Lease Affinity 48
- Configuring the Lease Logging Member 50
- Adding an IPv6 DHCP Network Range or IPv6 DHCP Scope 53
- Setting the Prefix Length Mode for DHCPv6 56

Dual Stack Grid **58**
Incorporating IPv6 in a High Availability Environment 58
Converting Individual Members to IPv6 62
Anycast Configuration 65
References **69**
IPv4 and IPv6 Dual-Stack) 69
Creating IPv6 Network From Scratch 69
Interesting Links 69

IPv6 Planning

The astronomically larger address space available in IPv6 gives network administrators a new flexibility in defining address plans that are both logical and practical. But in order to create an effective IPv6 addressing plan, network administrators will benefit from new best practices that more efficiently manage the unprecedented abundance of bits available in IPv6 address allocations. Here are eight concepts or fundamentals that should be considered.

Planning with Abundance

Because of the virtually inexhaustible supply of IPv6 address space, subnets are no longer sized according to how many hosts are expected per segment or broadcast domain. Instead, the standard IPv6 address plan uses a one-size-fits-all subnet (the /64, as noted below) and a large enough primary allocation from your ISP or RIR (regional internet registries) to provide sufficient subnets.

Efficiency in IPv6 addressing becomes about readability and consistency rather than address conservation.

Standard Subnet Size

In IPv6 addressing, a /64 (1.8×10^{19} host addresses) is the standard subnet size for addressing interfaces. Allocating and deploying smaller subnets--i.e. more than 64 bits--is not recommended (with the exception of point-to-point links noted below).

Point-to-point Links

The exception to the /64 standard are subnets used for point-to-point links. Current best practice (RFC6164) dictates that these links should use a /127 (though the use of a /126 subnet or a /64 exist in some real-world deployments). For address plan consistency, every point-to-point link can be allocated a /64 configured with a single /127 from that allocation. /128 loopback addresses can all be assigned from the first /64 of the /48 reserved for infrastructure. (Alternatively, all point-to-point subnets could be allocated from one /64 per routing area).

Standard Site Allocation

The standard per-site allocation provided to an organization is typically a /48. If you have more than one site you'll need a larger allocation--e.g., /44 for up to 16 sites, /40 for up to 256 sites, /36 for up to 4,096 sites, and /32 for up to 65,536 sites.

PI vs. PA

IPv6 allocations from IP transit providers or ISPs are referred to as Provider Aggregatable (or PA) allocations. These allocations are usually tied to the duration of the contract for IPv6 connectivity. Alternatively, IPv6 allocations from the Regional Internet Registries (or RIRs) are Provider Independent (or PI) allocations and are considered permanent. Both types are globally registered and globally routable. In general, multi-homed networks connected to multiple ISPs or transit providers require PI allocations.

Making your Address Plan Readable

Groups of IPv6 subnet assignments broken out from the primary allocation are often restricted to multiples of four bits –e.g., /36, /44, /48, /52, /56, /60. While this method reduces the overall granularity available to the address plan, it improves network prefix readability (see inset). With each group of subnets aligning with a hexadecimal digit (or nibble)in the network prefix, the resulting readability can make geographic and functional significance more immediately decipherable. This can improve operational efficiencies.

Subnet bits a multiple of four	**Subnet bits not a multiple of four**
Prefix: 2001:db8:abcd::/48 Range: 2001:db8:abcd:0000:0000:0000:0000:0000 to 2001:db8:abcd:ffff:ffff:ffff:ffff:ffff	Prefix: 2001:db8:abcd::/49 Range: 2001:db8:abcd:0000:0000:0000:0000:0000 to 2001:db8:abcd:7fff:ffff:ffff:ffff:ffff

Location and Function Assignments

The abundance of addresses in an IPv6 allocation provides the opportunity to efficiently assign groups of networks based on geographical and functional requirements (see inset for an example). Such assignments allow for potentially more efficient and effective routing and firewall policies. Further, it is possible to encode existing IPv4 addresses into IPv6 addresses if consistency is desired between address families during the initial stages of IPv6 adoption (though it is generally recommended that this technique be used only temporarily as it may interfere with the ultimate efficiency and scalability of the IPv6 address plan).

Host Address Assignment

Three primary mechanisms exist for addressing hosts with IPv6. They are Stateless Address Auto Configuration (SLAAC), Dynamic Host Control Protocol for IPv6 (DHCPv6), and static addressing. In most production deployments, compliance and security requirements may make the use of SLAAC undesirable and compel the use of DHCPv6 for hosts (network infrastructure and servers will most likely use static assignments).

Deployment Instructions

Grid Communication

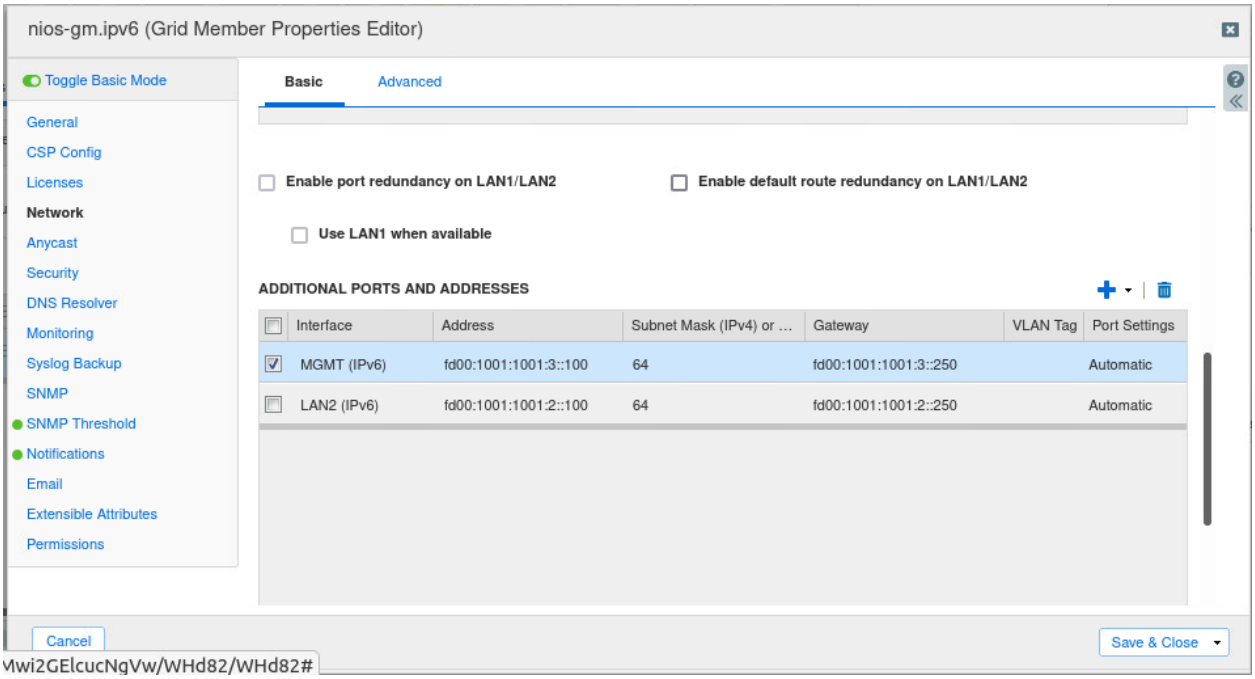
The LAN1 port can be configured with an IPv6 address by using the '`set network`' command and then following the prompts.

```
Infoblox >
Infoblox > set network
NOTICE: All HA configuration is performed from the GUI.  This interface is
        used only to configure a standalone node or to join a Grid.
Enter IP address: fd00:1001:1001:1::50

WARNING: local IPv6 unicast address.

Enter IPv6 Prefix Length [Default: none]: 64
Enter IPv6 gateway [Default: none]: fd00:1001:1001:1::51
Enter VLAN tag [Default: Untagged]:
Configure IPv4 network settings? (y or n): n
Become grid member? (y or n): n

 New Network Settings:
  IPv6 address:         fd00:1001:1001:1::50/64
  IPv6 Gateway address: fd00:1001:1001:1::51
  IPv6 VLAN tag:        Untagged

 Old IPv4 Network Settings:
  IPv4 address:         192.168.1.2
  IPv4 Netmask:         255.255.255.0
  IPv4 Gateway address: 192.168.1.1
  IPv4 VLAN tag:        Untagged
        Is this correct? (y or n): y
```

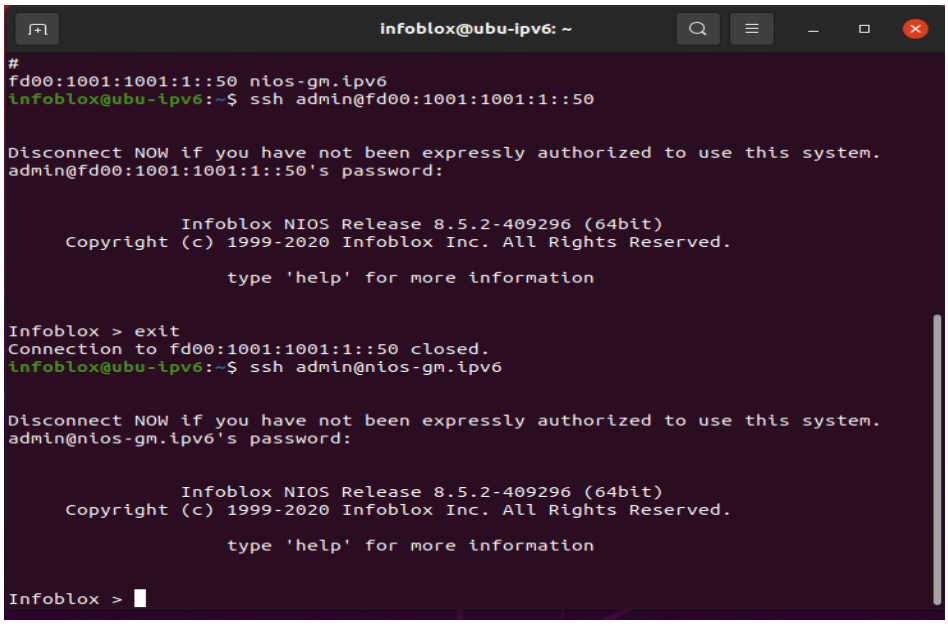
To add a LAN2 port and/or MGMT port, from the GUI, follow these steps:

1. Navigate to **Grid**→ **Grid Manager** → **Members**.
2. Click on the **member** that needs IPv6 interfaces. Click on the **Edit** button.
3. Within the Grid Member Properties Editor, click on the **Network** tab.
4. Scroll down to Additional Ports and Addresses.
5. Click on the **down arrow** next to the '**+**' button and select either LAN2 (IPv6) or MGMT (IPv6).
6. Enter the **Address**, **Subnet Mask**, and **Gateway** information.

7. Optionally, add a **VLAN** tag. Click **Save and Close**.



SSH communication to the Infoblox member can be done using IPv6 address, hostname entry, or DNS FQDN. Below is a screenshot of SSH communication to an Infoblox member using either the IPv6 address or the hostname that is in the host file.

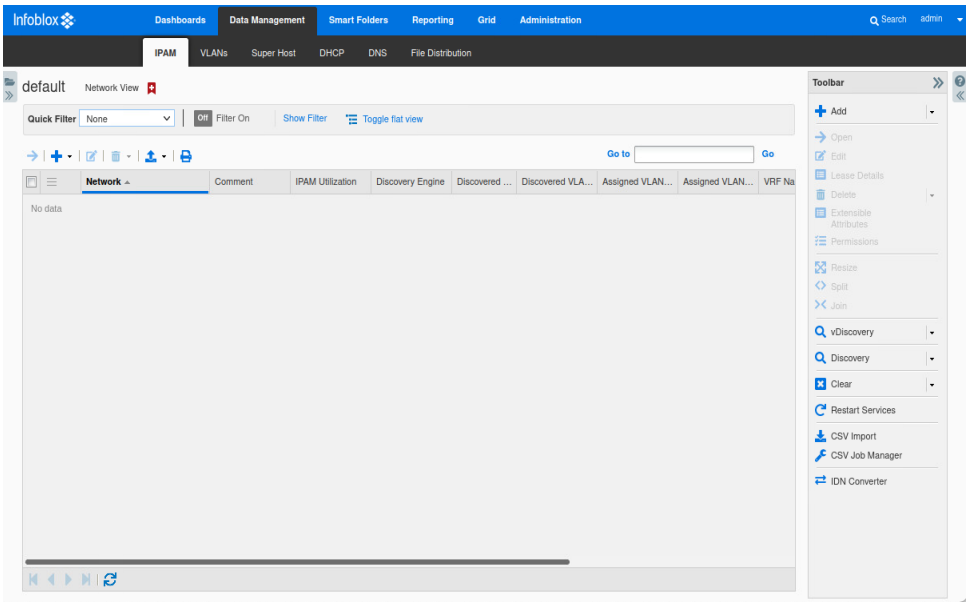


IPAM

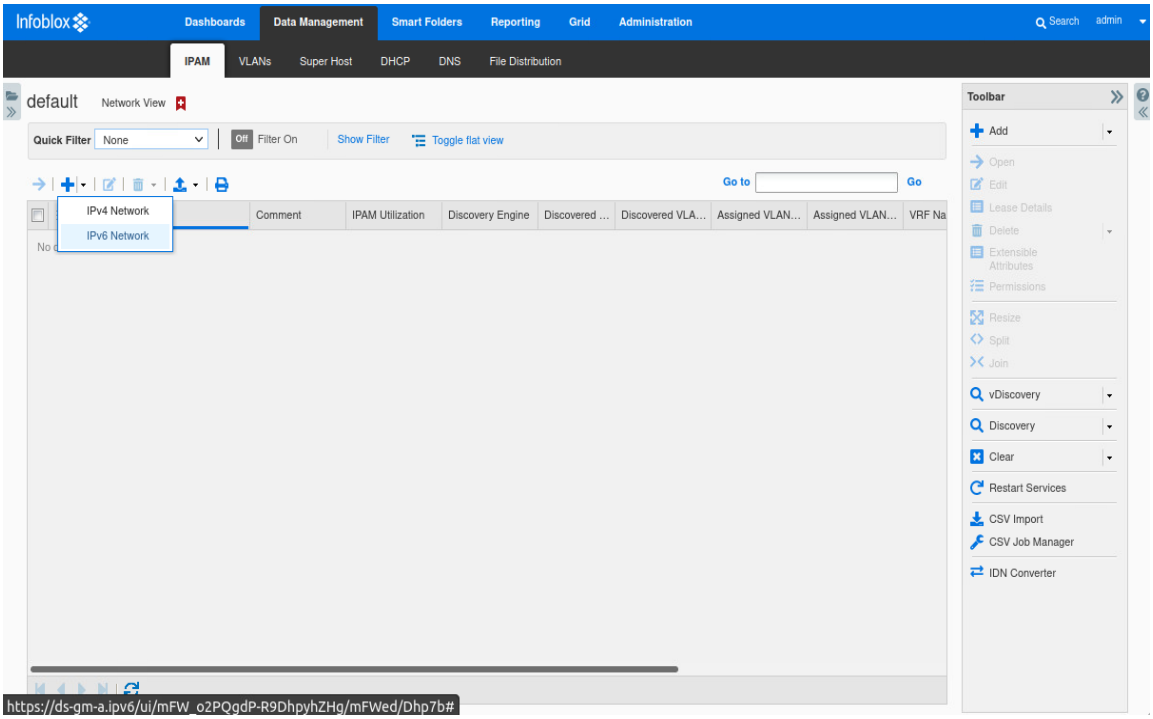
Note: Extensible attributes are supported in IPv4 and IPv6 setups.

Add an IPv6 Network.

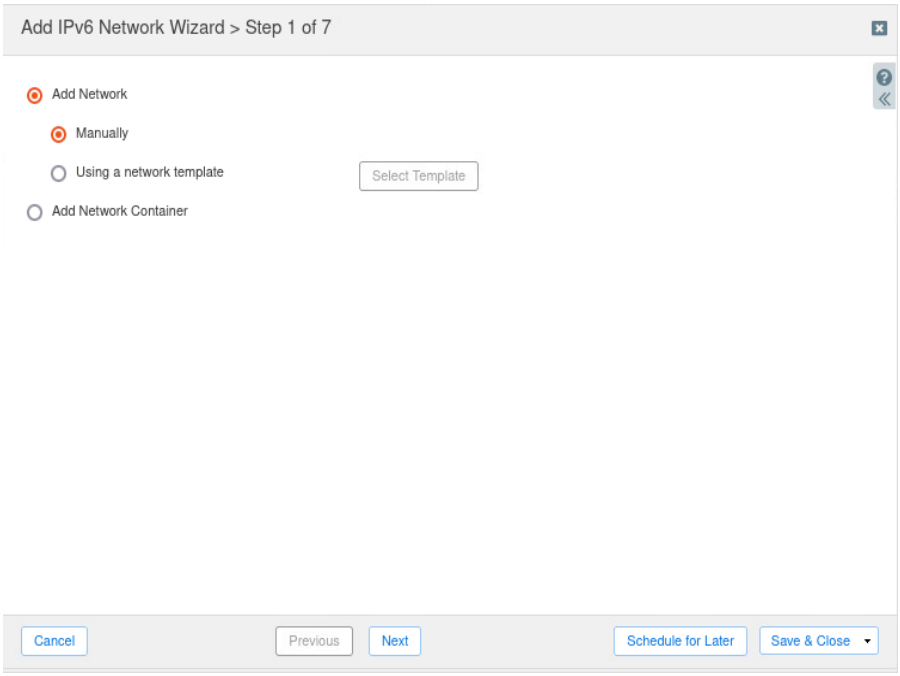
1. Navigate to **Data Management → IPAM**.



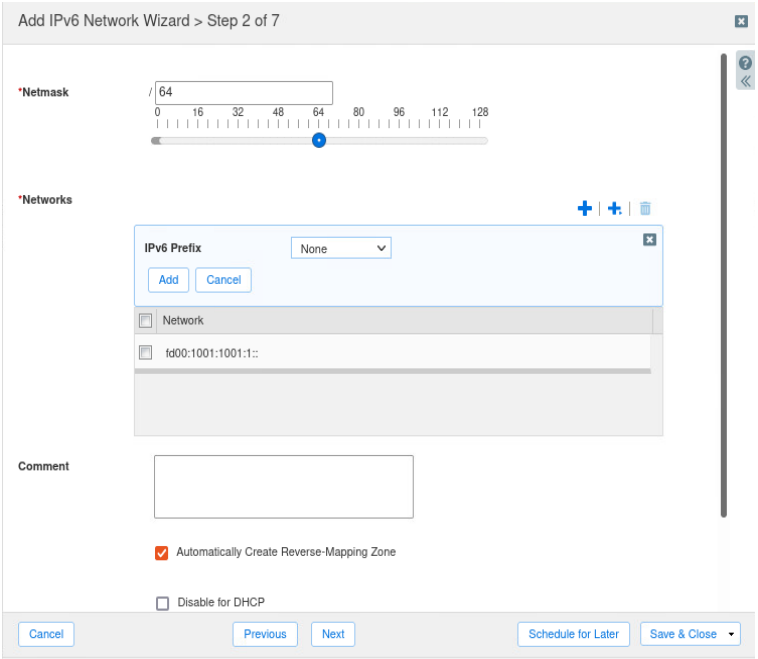
2. Click on the '**+**' button drop-down arrow and select **IPv6 Network**.



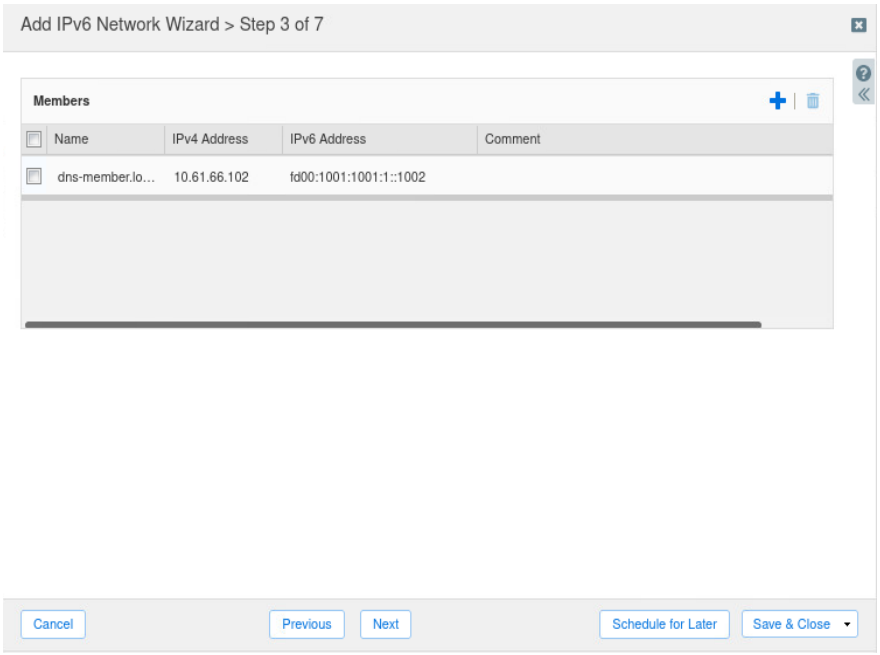
3. Click **Next** if you just want to add a network. Otherwise, you can create a container. For example if you wish to subnet a network like FD00:1001:1001:1::/64, you would create a container with this prefix and then subsequently click into the container and add subnetted networks. Click **Next**.



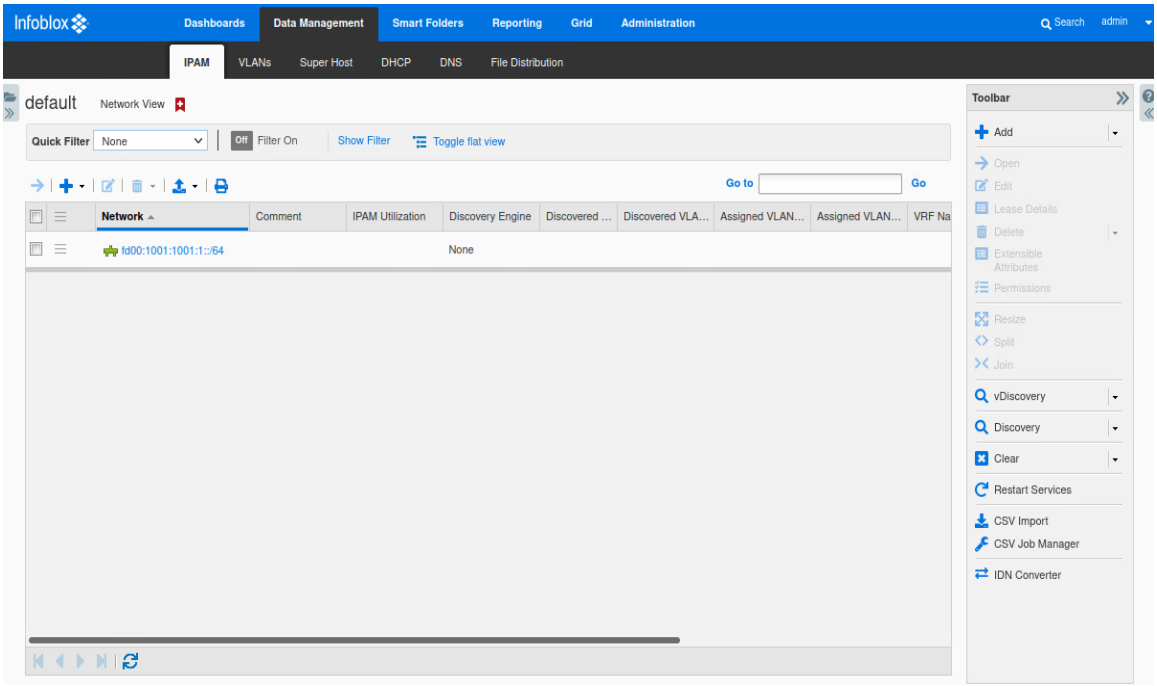
4. For the netmask, slide the circle either way to define the netmask. Click on the left hand '+' button to add a network. Click on the **check box** to automatically create a reverse-mapping zone.



5. Click on the '+' button to add the Grid member that will service this IPv6 address.



6. Click **Save and Close**.



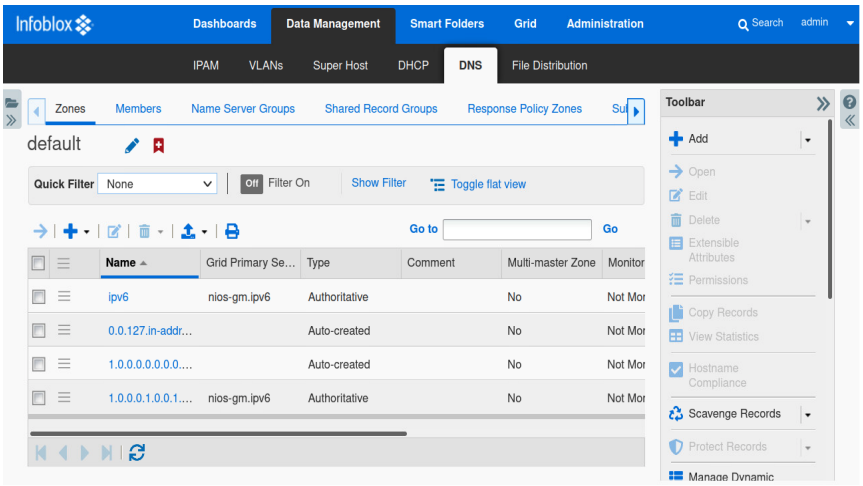
DNS

With the advent of RFC 1886, the DNS protocol is set up to handle IPv6 addresses. A new type of A record was created to handle the 128 bits in an IPv6 address. It is called a **'AAAA'** record and IPv6 reverse mapping domain called **ip6.arpa**

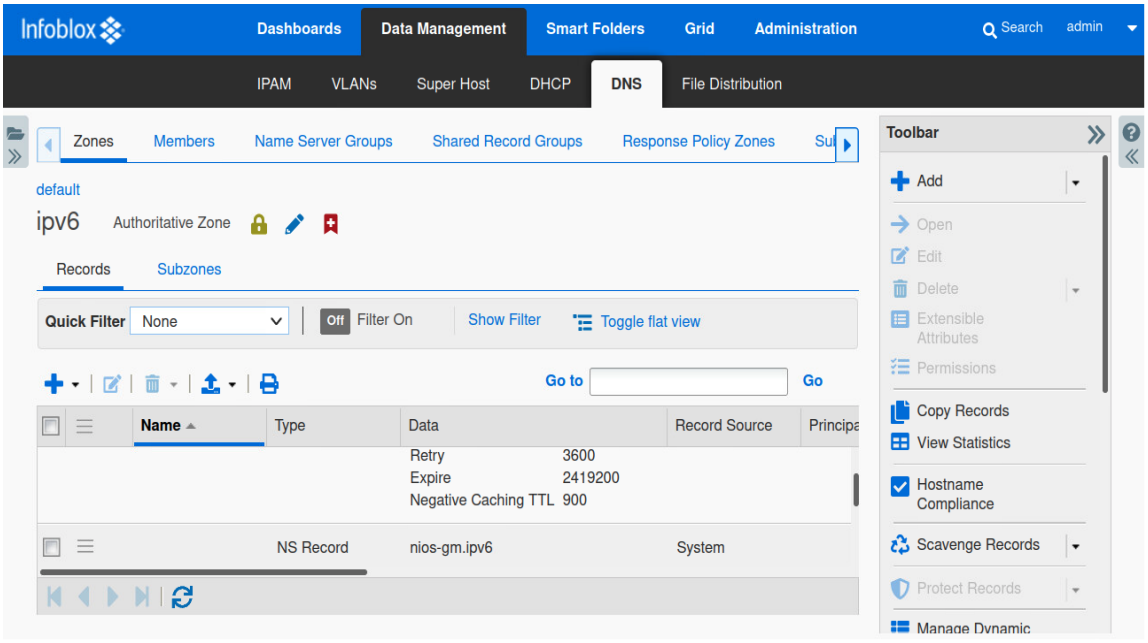
IPv6 Specific Records

Here is how you create an AAAA record:

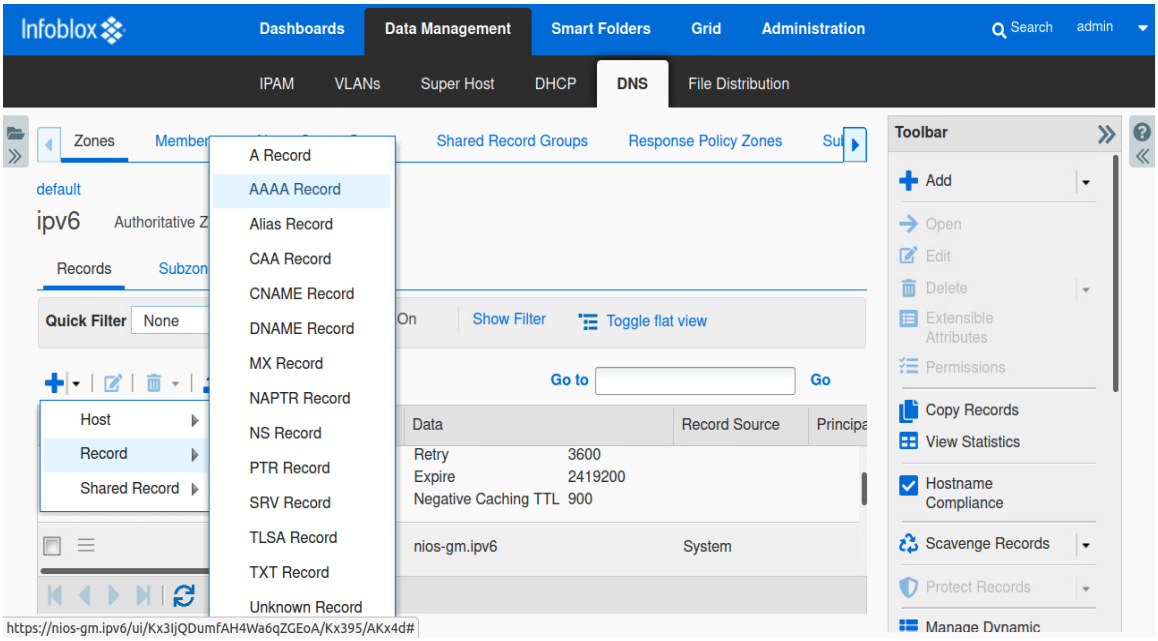
1. Navigate to **Data Management → DNS → Zones**



2. Click on the **zone**. In this case it is ipv6.

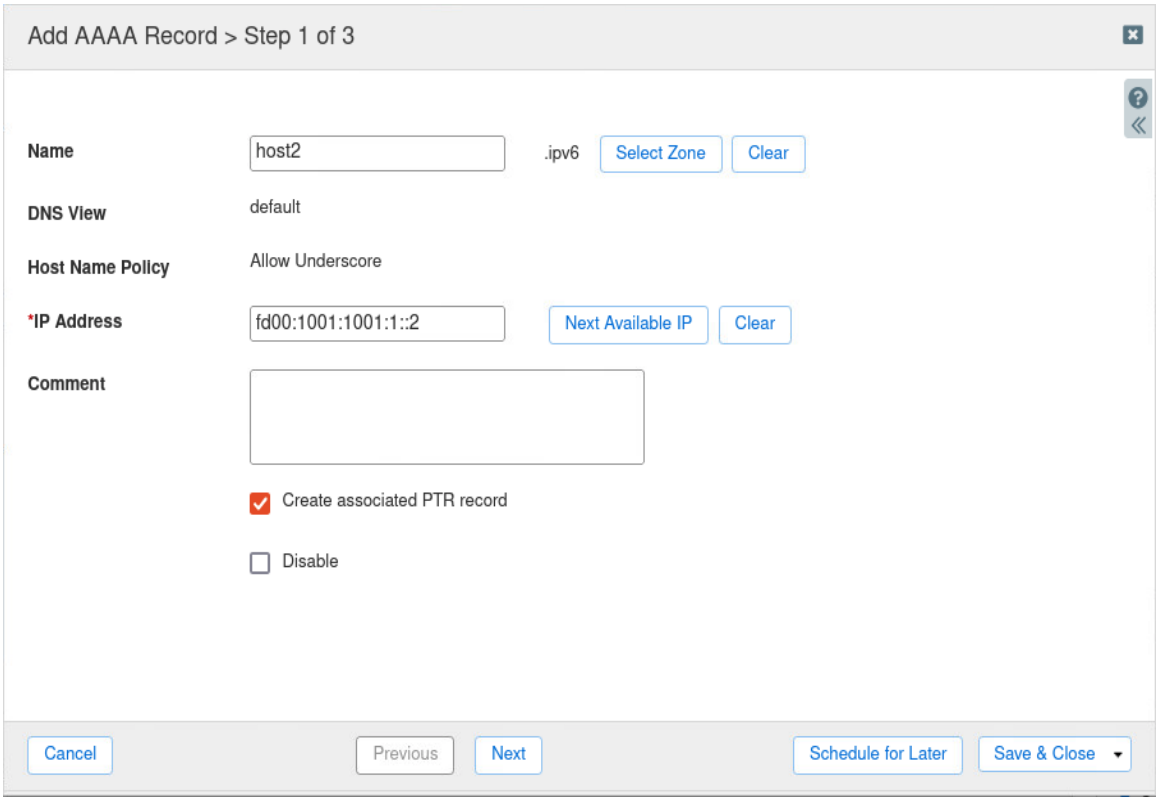


3. Click on the '+' button and navigate to **Record → AAAA Record.**



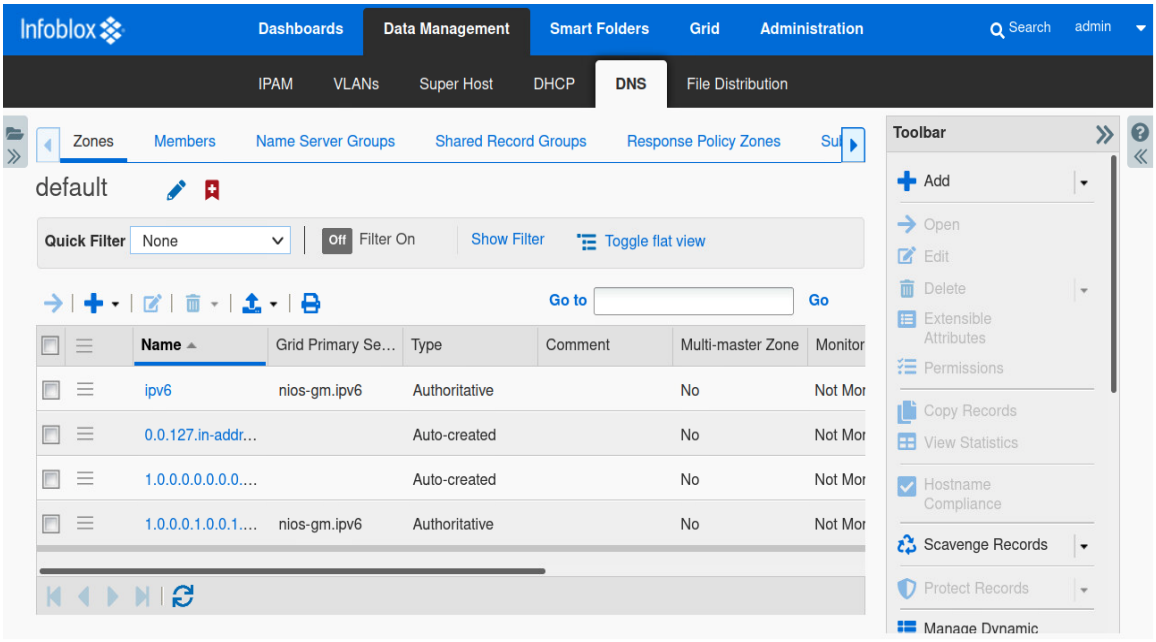
4. Input the **Name**. If you have multiple zones, then click on the **Select Zone** button and select the zone. Input the IP address or click on the **Next Available IP** button and select the next IP.

5. Click **Save and Close**

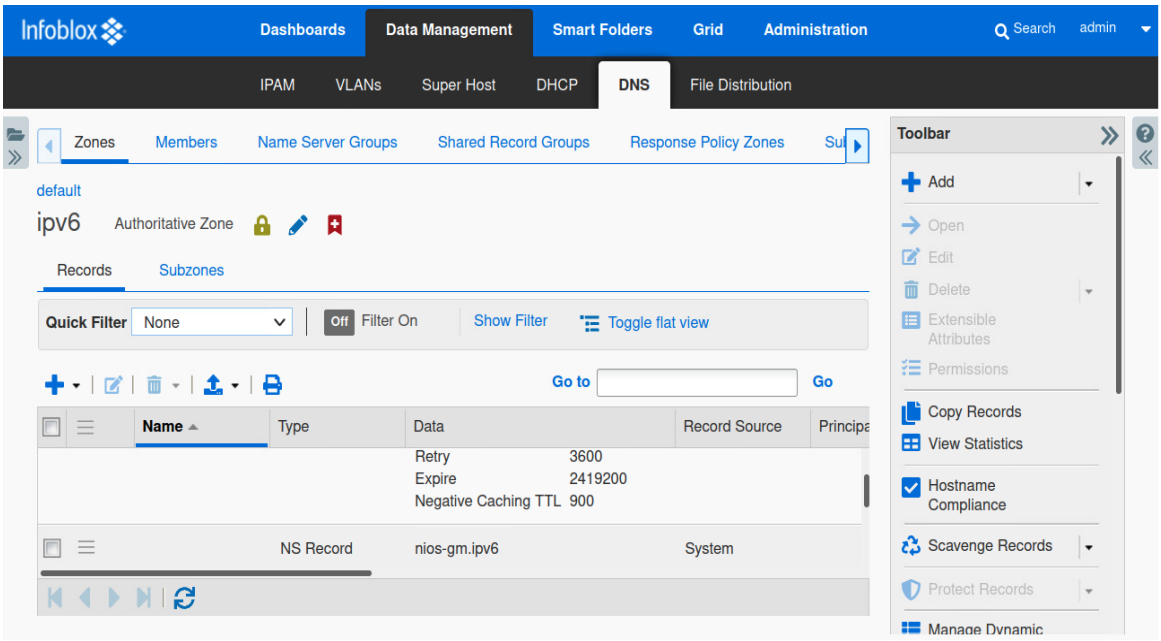


Create an Alias Record

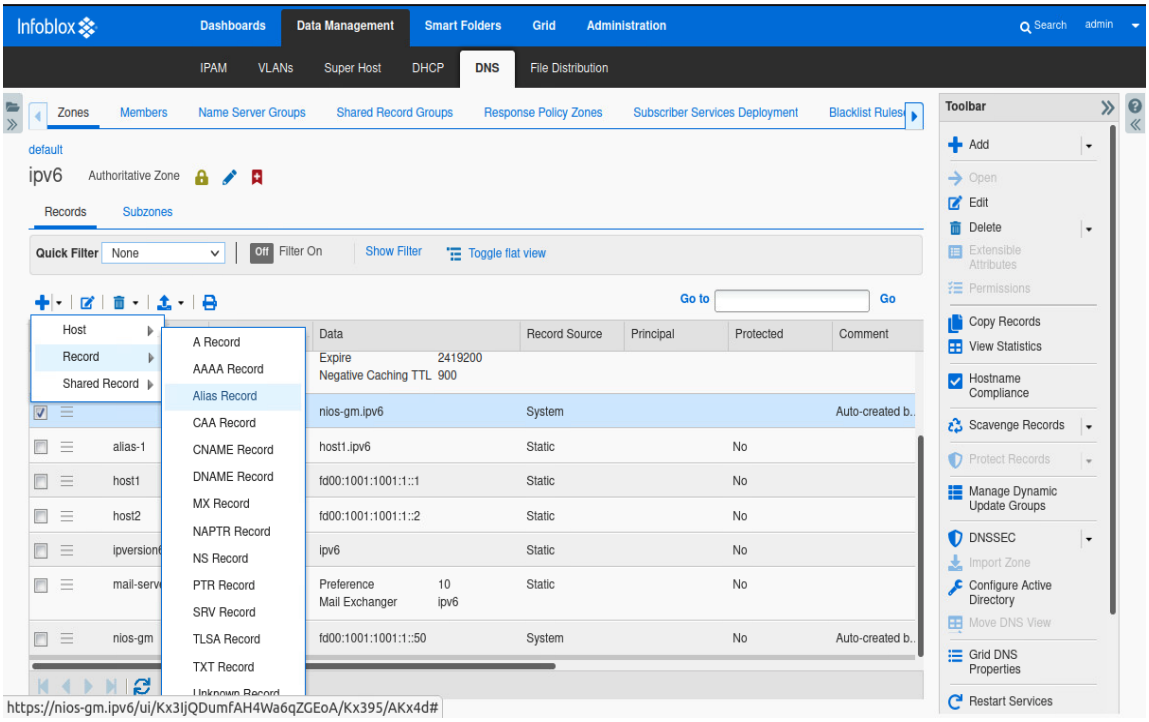
1. Navigate to **Data Management → DNS → Zones**



2. Click on the **zone**. In this case it is IPv6.

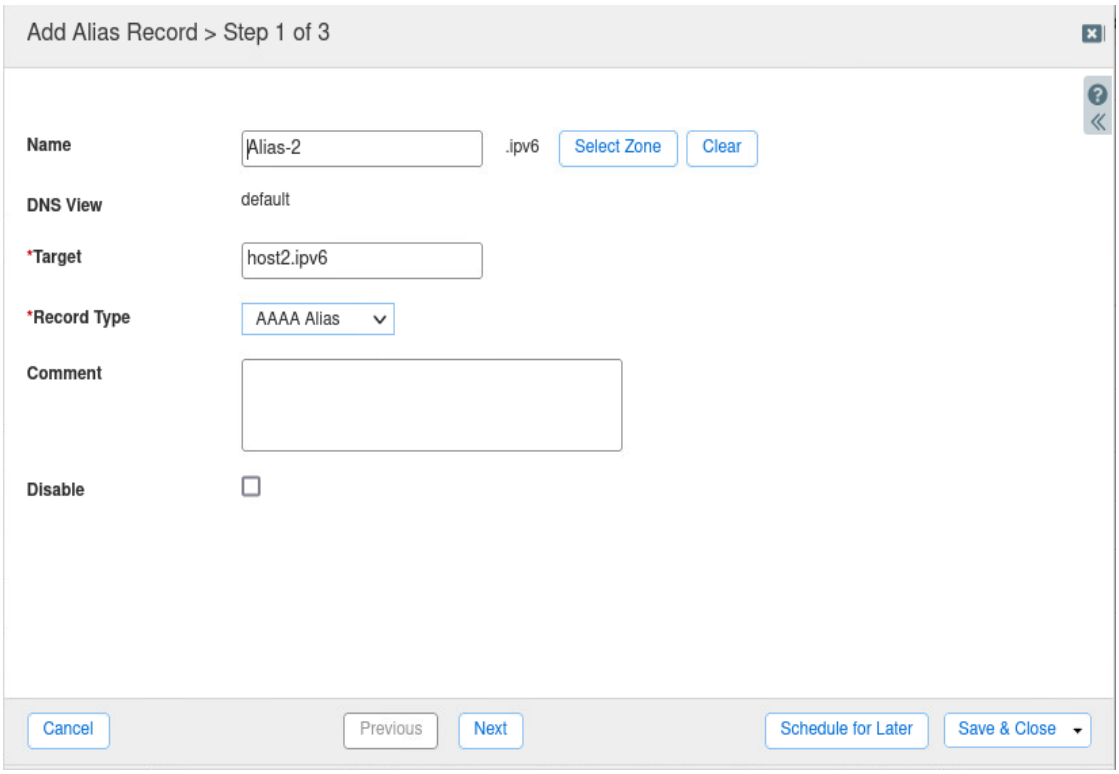


3. Click on the '+' button and navigate to **Record → Alias Record**.



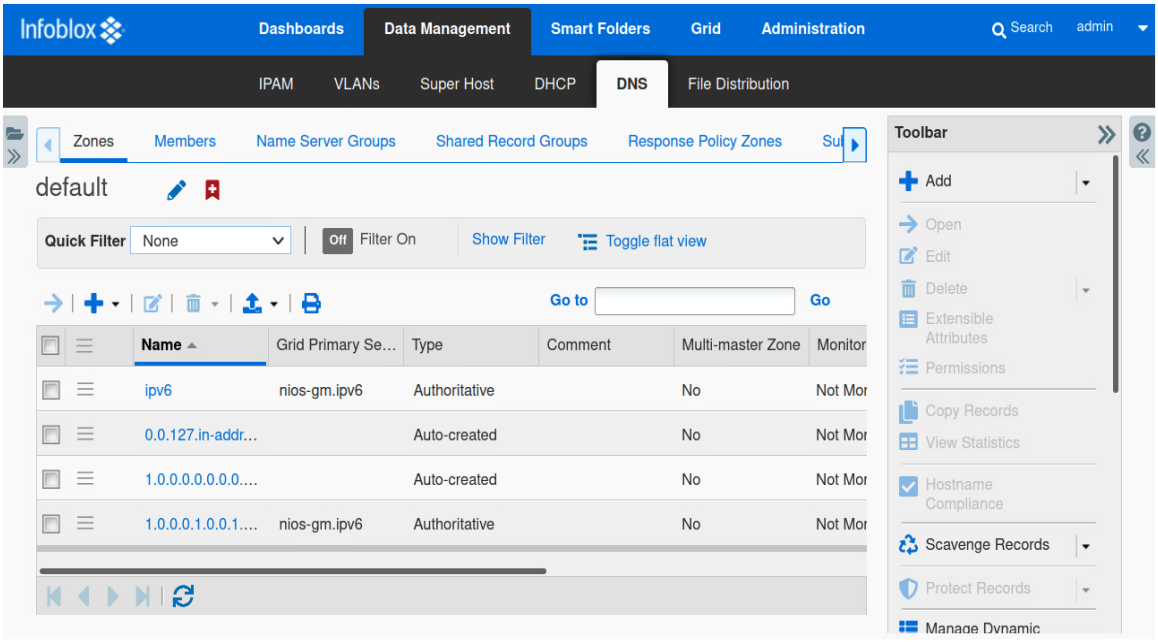
4. Enter the **name** of the alias, target, and the record type of **AAAA** Alias.

5. Click on **Save and Close**.

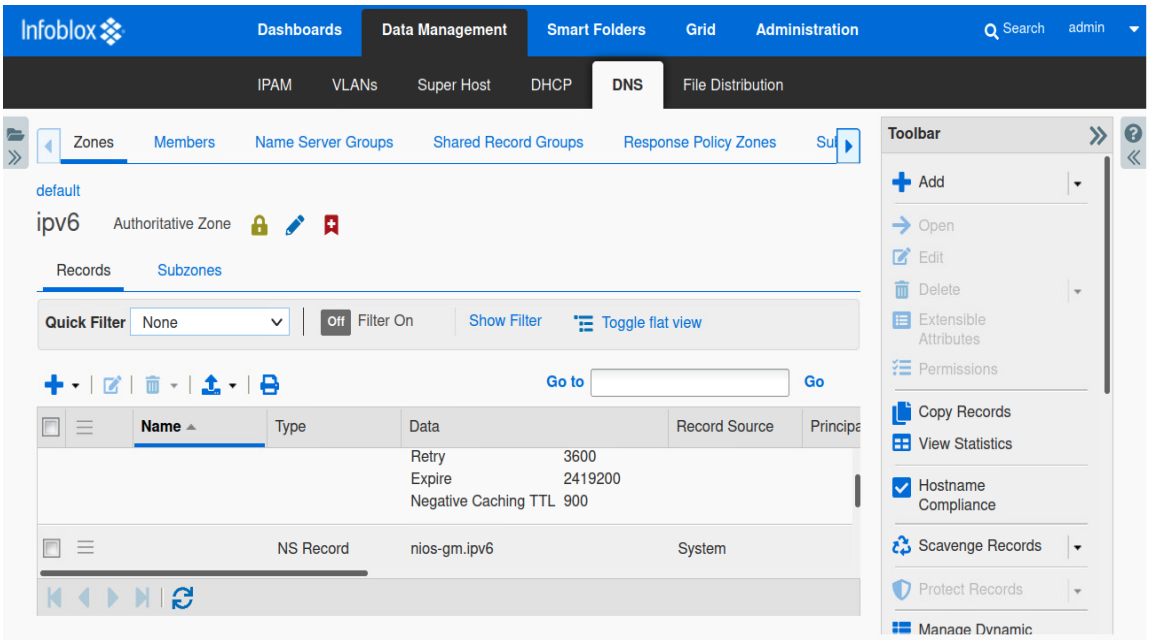


Create a Host Record

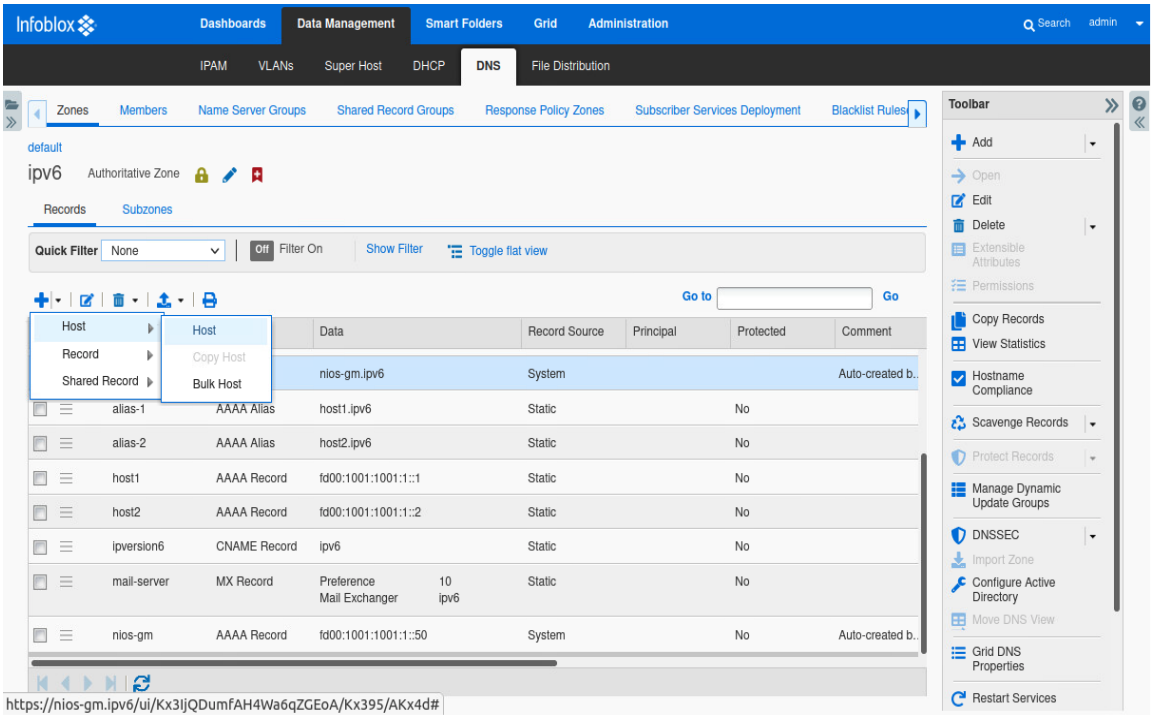
1. Navigate to **Data Management → DNS → Zones**



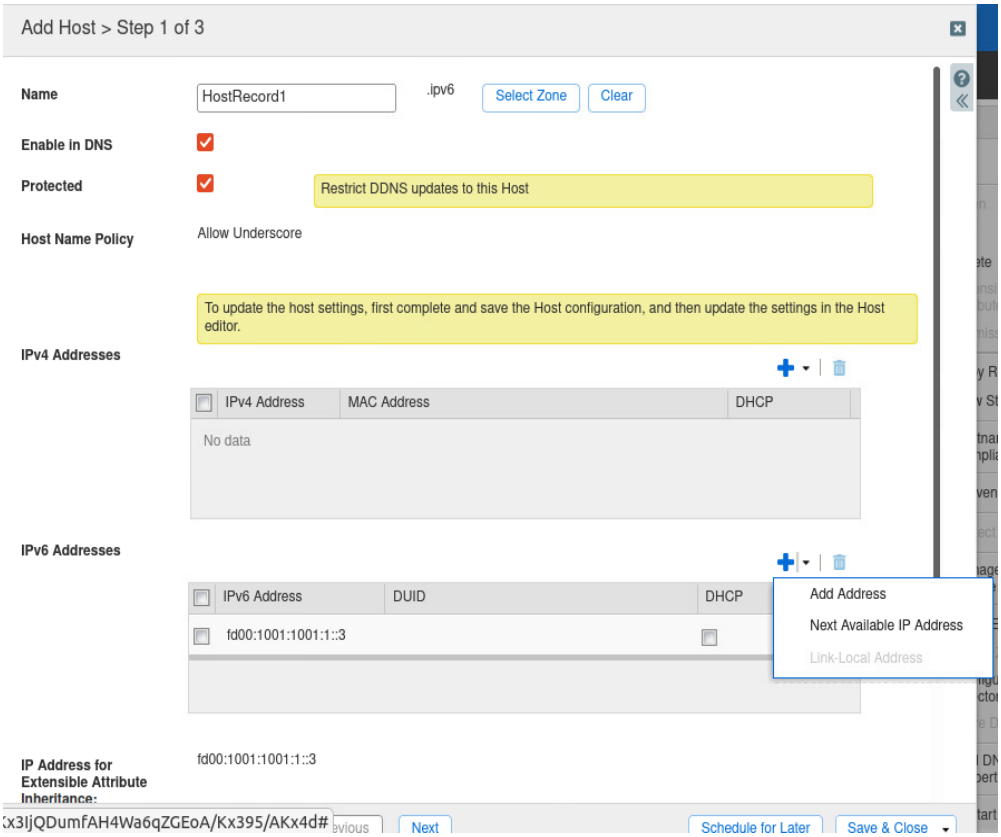
2. Click on the **zone**. In this case it is IPv6.



3. Click on the '+' button and navigate to **Record → Host Record.**



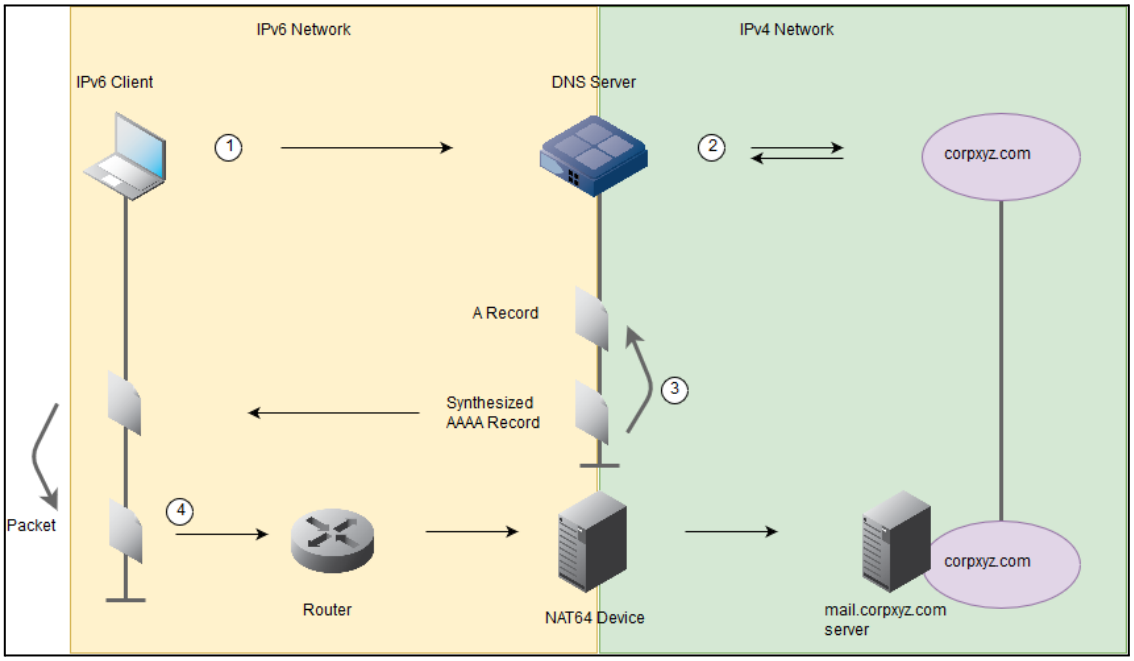
4. Enter the **Name** of the host record, click on **Next Available IP** address or **Add Address** to add the IPv6 address. Click **Save and Close**.



DNS64

To support the increasing number of IPv6 and dual-stack networks, Infoblox DNS servers now support DNS64, a mechanism that synthesizes AAAA records from A records when no AAAA records exist. When you enable DNS64 on anInfoblox DNS server, it can operate with a third-party NAT64 device so IPv6-only nodes can communicate with IPv4-only nodes without any changes to either of the devices.

As illustrated in the following figure, when an IPv6-only host requests the AAAA record of an IPv4-only server and none exists, a DNS64-enabled server can retrieve the A record of the IPv4 server and synthesize an AAAA record. The IPv6-only host can then use the synthesized AAAA record, which contains the IPv6 proxy address for the IPv4 address in the original A record, to initiate communication with the IPv4 host.



Following are the steps illustrated in the above figure:

1. An IPv6-only host sends a recursive query for the AAAA record of the IPv4 server mail1.corpxyz.com.

2. The Infoblox DNS server attempts to resolve the request for the AAAA record, and determines that an AAAA record for mail1.corpxyz.com does not exist. The DNS server then performs a query for the A record of mail1.corpxyz.com.

3. The DNS server creates a synthetic AAAA resource record from the information in the A record, and returns the synthesized AAAA record to the requesting IPv6 host.

4. The host receives the synthetic AAAA record and sends a packet to the destination address specified in the synthetic AAAA record. The packet is routed to the IPv6 interface of the NAT64

device, which translates the packet from IPv6 to IPv4 and forwards it to the server, mail1.corpxyz.com.

Infoblox DNS servers can return synthesized AAAA records to both IPv4 and IPv6 clients when the client explicitly requests an AAAA record and none exists for the requested host. If a host has multiple A records, the DNS server synthesizes an AAAA record for each A record. Infoblox DNS servers can also synthesize records for reverse-mapping zones. When a DNS server receives a query for a PTR record in the IP6.ARPA domain whose address matches a configured DNS64 prefix, the server synthesizes a CNAME record that contains an IPv4 address derived from the IPv6 address in the query. The server then sends a query for the PTR record so it can resolve the IPv4 address to the hostname.

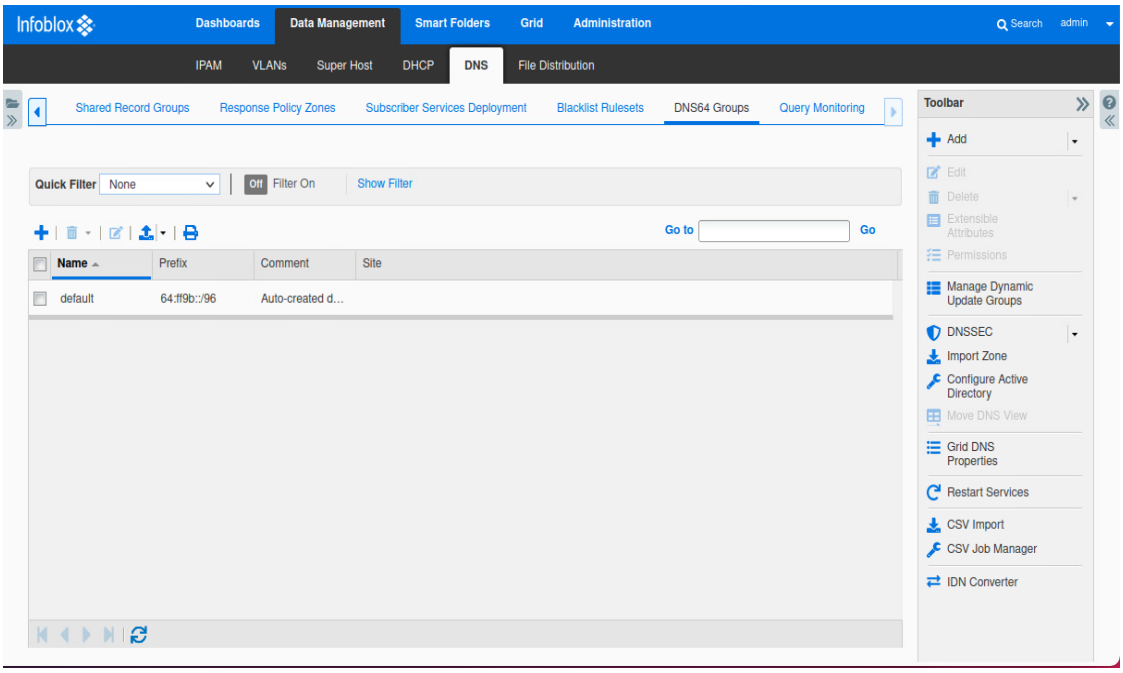
For example, if a DNS server that is configured to synthesize records for the prefix 2001:db8::/96 receives a query for the PTR record of 2001:db8::0102:0304, it synthesizes a CNAME record that contains the IPv4 address 4.3.2.1.in-addr.arpa. The server then resolves the PTR record of the IPv4 address 4.3.2.1.in-addr.arpa.

If the server obtains the PTR record, then it sends the synthesized CNAME record and the PTR record to the client. If the zone exists, but there is no PTR record, then the server sends the synthesized CNAME record only. If the zone does not exist, then the server responds with a SERVFAIL with no answers.

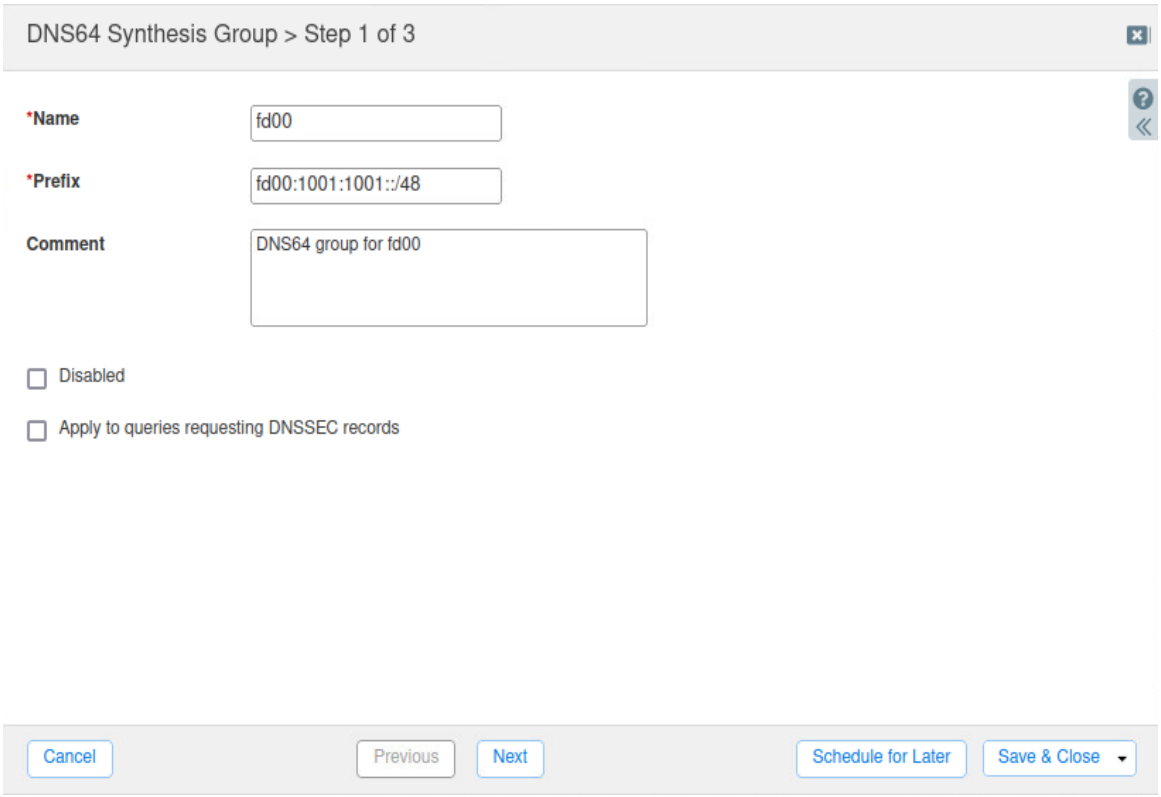
Additionally, Infoblox DNS servers can generate synthesized records for DNSSEC secure zones, but only for non-DNSSEC clients. A DNS client or resolver includes the EDNS OPT pseudo-RR with the DO (DNSSEC OK) bit set to indicate that they are requesting DNSSEC data. DNS servers can generate synthesized AAAA records only when the request does not have the DO bit set. This ensures that DNSSEC clients receive only valid responses.

Configuring DNS64

1. Navigate to **Data Management** → **DNS** → **DNS64 Groups**. Click on the '**+**' sign to add a DNS64 Group.



2. Enter the name of the **group**, **prefix**, and **comment**. Click **Save and Close**.



Setting DNS64 Group Properties

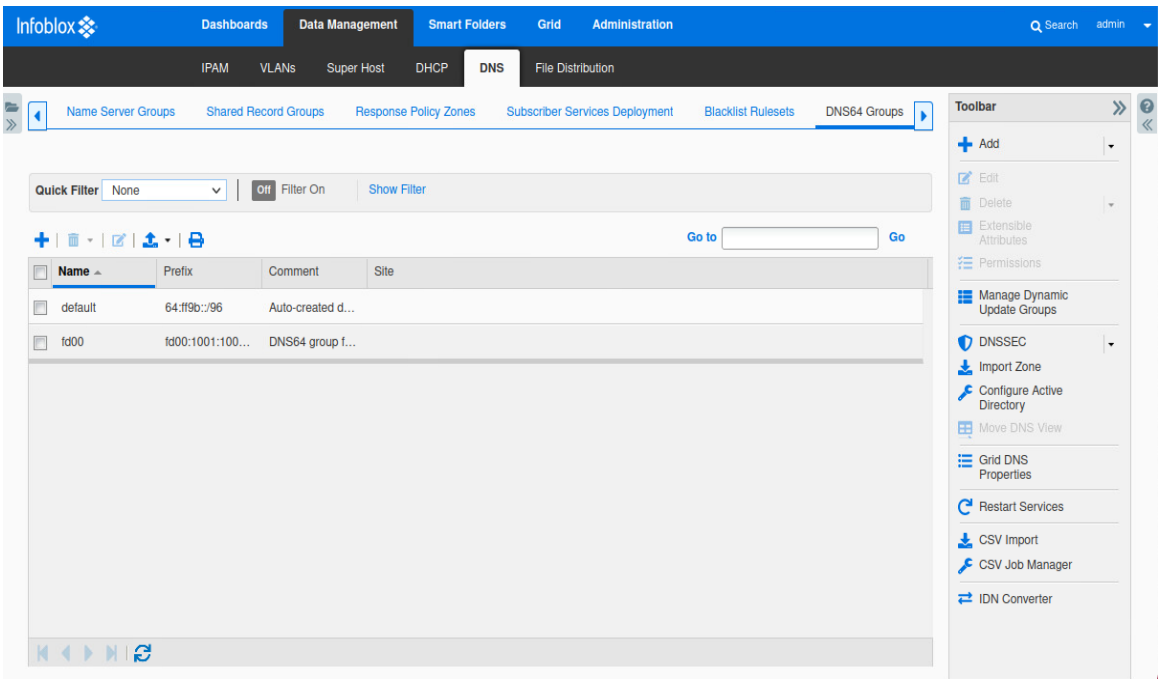
After you create a DNS64 synthesis group, you can specify the following:

- The IPv4 and IPv6 DNS clients and networks to which the DNS server is allowed to send synthesized AAAA records with the specified IPv6 prefix.
- The IPv4 addresses and networks for which the DNS server can synthesize AAAA records with the specified prefix.
- IPv6 addresses or prefix ranges that cannot be used by IPv6 only hosts, such as IP addresses in the ::ffff:0:0/96 network. When the DNS server retrieves an AAAA record that contains an IPv6 address that matches an excluded address, it does not return the AAAA record. Instead, it synthesizes an AAAA record from the A record.

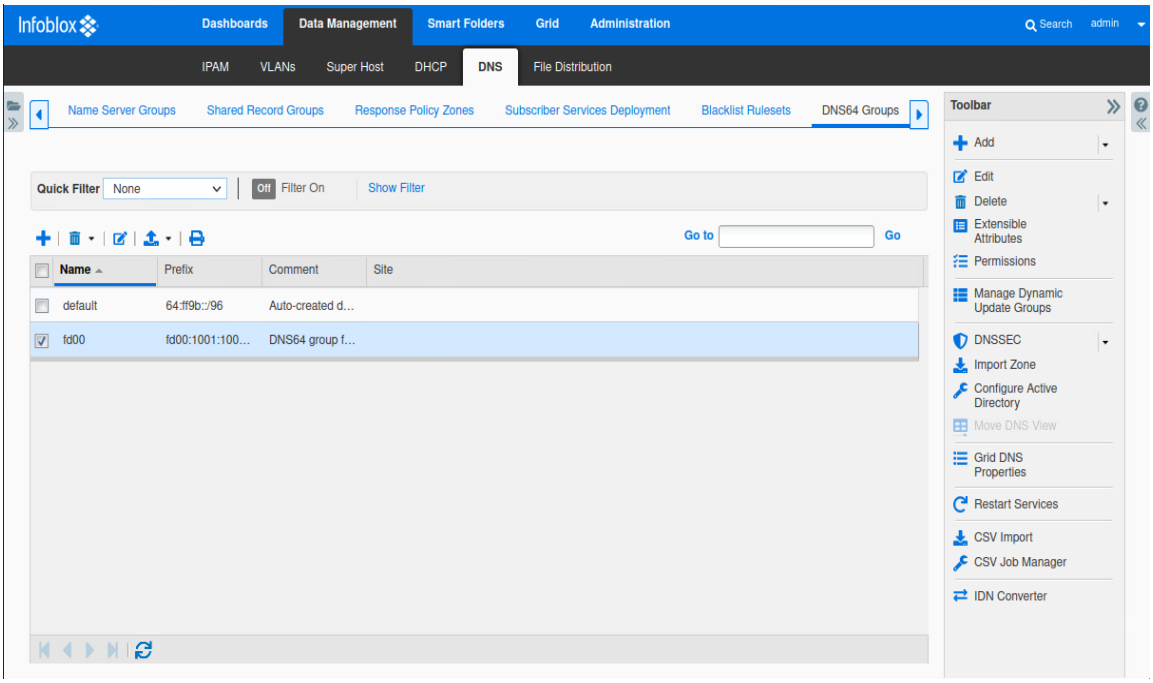
Note that a DNS server synthesizes the AAAA record of a host that has both A and AAAA records when all the IPv6 addresses in the AAAA records match the excluded addresses. If the host has multiple AAAA records and some of them contain excluded IPv6 addresses, then the server returns the remaining AAAA records.

Modifying DNS64 Group Properties

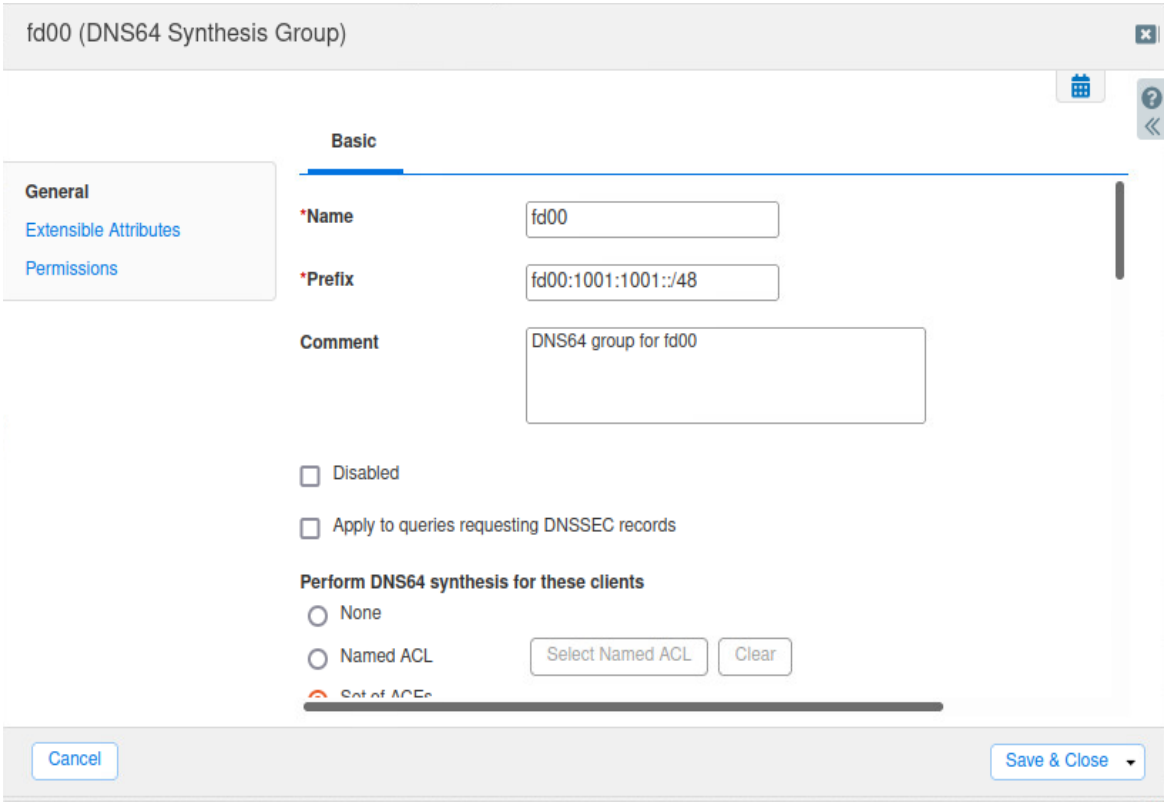
1. Navigate to **Data Management → DNS → DNS64 Groups**.



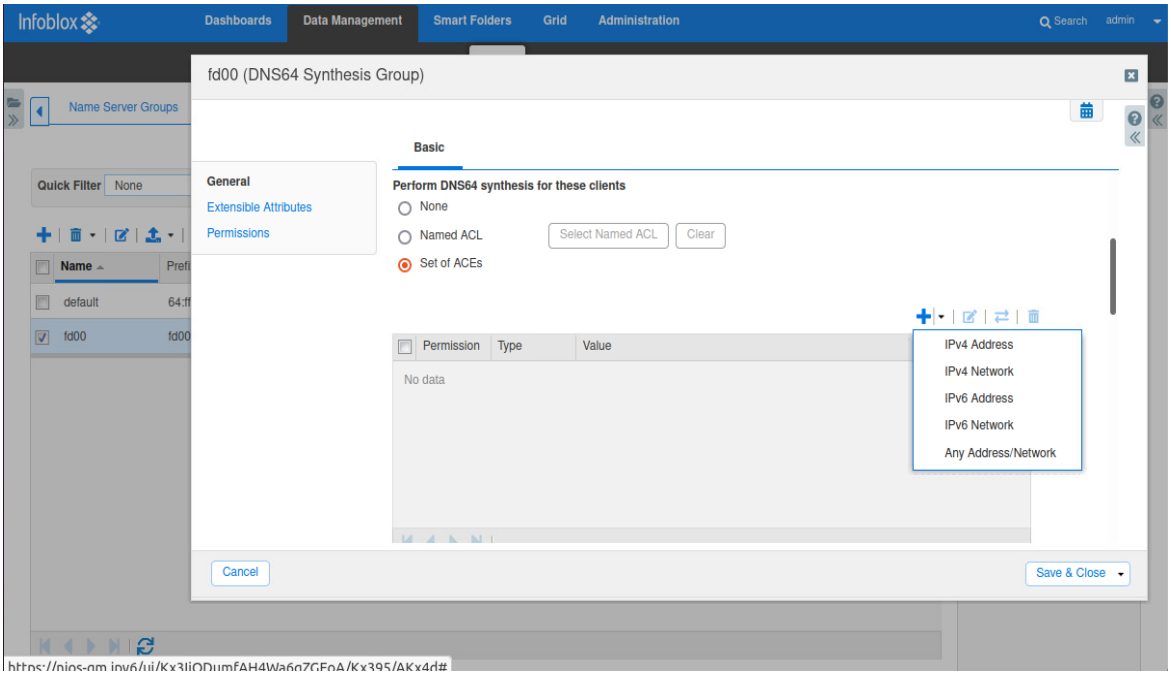
2. Click on the **check box** of the group that you want to modify.



3. Click on the **Edit** icon.



4. Scrolling down the screen, you can perform DNS64 synthesis for specific clients based upon a Named ACL or Set of ACEs.



Perform DNS64 synthesis for these clients: Specify IPv4 and IPv6 hosts and networks to which Infoblox DNS servers can send synthesized AAAA records. The default is to allow any IPv4 and IPv6 address and network.

Select one of the following:

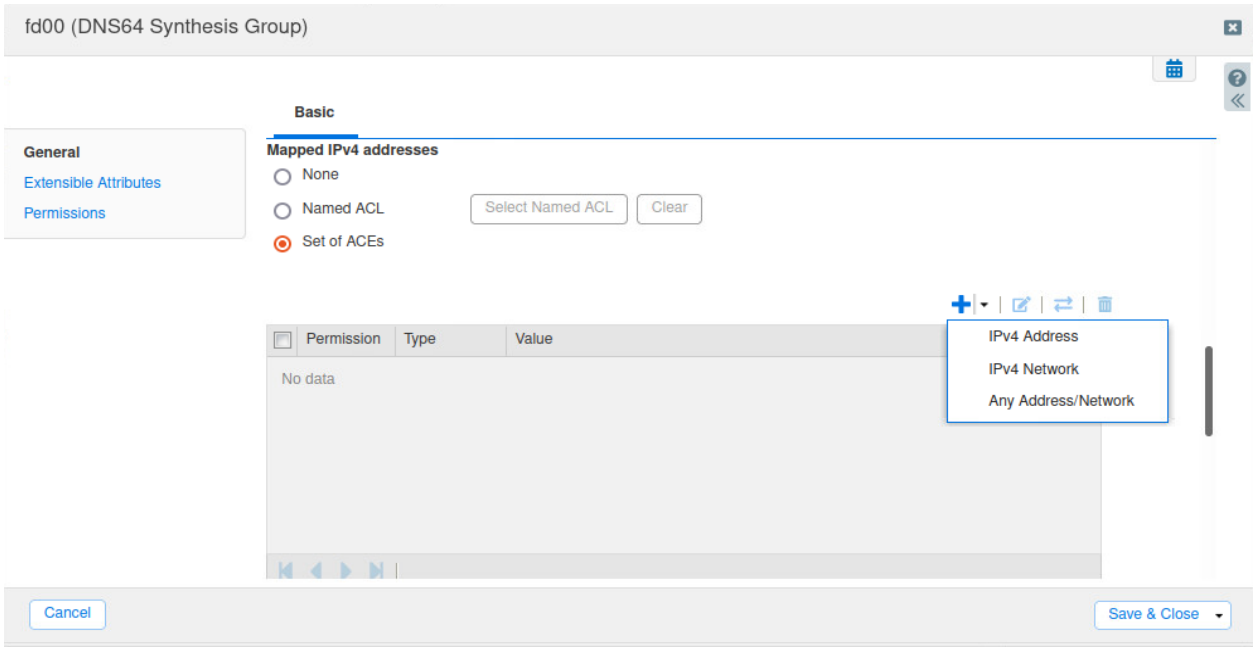
- **None**: Select this if you do not want to define specific addresses or networks to which the appliance sends synthesized AAAA records. When you select this, the appliance sends synthesized AAAA records to all clients. This is selected by default.

- **Named ACL**: Select this and click Select Named ACL to select a named ACL. Grid Manager displays the Named ACLs Selector. Select the named ACL you want to use. If you have only one named ACL, Grid Manager automatically displays the named ACL. When you select this option, the appliance sends synthesized AAAA records to the clients that have the Allow permission in the list. You can click Clear to remove the selected named ACL.

- **Set of ACEs**: Select this to configure individual ACEs. Click the Add icon and select one of the following from the drop-down list. Depending on the item you select, Grid Manager either adds a row for the selected item or expands the panel so you can specify additional information about the item you are adding, as follows.

    - **IPv4 Address and IPv6 Address**: Select this to add an IPv4 address or IPv6 address. Click the Value field and enter the IP address. The Permission column displays Allow by default. You can change it to Deny by clicking the field and selecting Deny from the drop-down list.

- **IPv4 Network**: In the Add IPv4 Network panel, complete the following, and then click Add to add the network to the list:
    - **Address**: Enter an IPv4 network address and either type a netmask or move the slider to the desired netmask.
    - **Permission**: Select Allow or Deny from the drop-down list.
- **IPv6 Network**: In the Add IPv6 Network panel, complete the following, and then click Add to add the network to the list:
    - **Address**: Enter an IPv6 network address and select the netmask from the drop-down list.
    - **Permission**: Select Allow or Deny from the drop-down list.
- **Any Address/Network**: Select this to allow or deny any IP addresses to which the appliance sends synthesized AAAA records



Mapped IPv4 Addresses: Specify IPv4 addresses and networks for which the DNS server synthesizes AAAA records. The default is to allow the DNS server to synthesize AAAA records for any IPv4 address in any network. Select one of the following:

- **None**: Select this if you do not want to define specific IPv4 addresses or networks for which the DNSserver synthesizes AAAA records. The appliance synthesizes AAAA records for all IPv4 clients. This is selected by default.

- **Named ACL**: Select this and click **Select Named ACL** to select a named ACL. Grid Manager displays the Named ACLs Selector. Select the named ACL you want to use. If you have only one named ACL, Grid Manager automatically displays the named ACL. When you select this option, the appliance synthesizes AAAA records for the clients that have the Allow permission in the list. You can click **Clear** to remove the selected named ACL.

- **Set of ACEs**: Select this to configure individual ACEs. Click the **Add** icon and select one of the following from the drop-down list. Depending on the item you select, Grid Manager either adds a row for the selected item or expands the panel so you can specify additional information about the item you are adding, as follows.

- **IPv4 Address**: Select this to add an IPv4 address. Click the **Value** field and enter the IP address. The Permission column displays Allow by default. You can change it to Deny by clicking the field and selecting Deny from the drop-down list.

- **IPv4 Network**: In the Add IPv4 Network panel, complete the following, and then click **Add** to add the network to the list:

    - **Address**: Enter an IPv4 network address and either type a netmask or move the slider to the desired netmask.

    - **Permission**: Select Allow or Deny from the drop-down list.

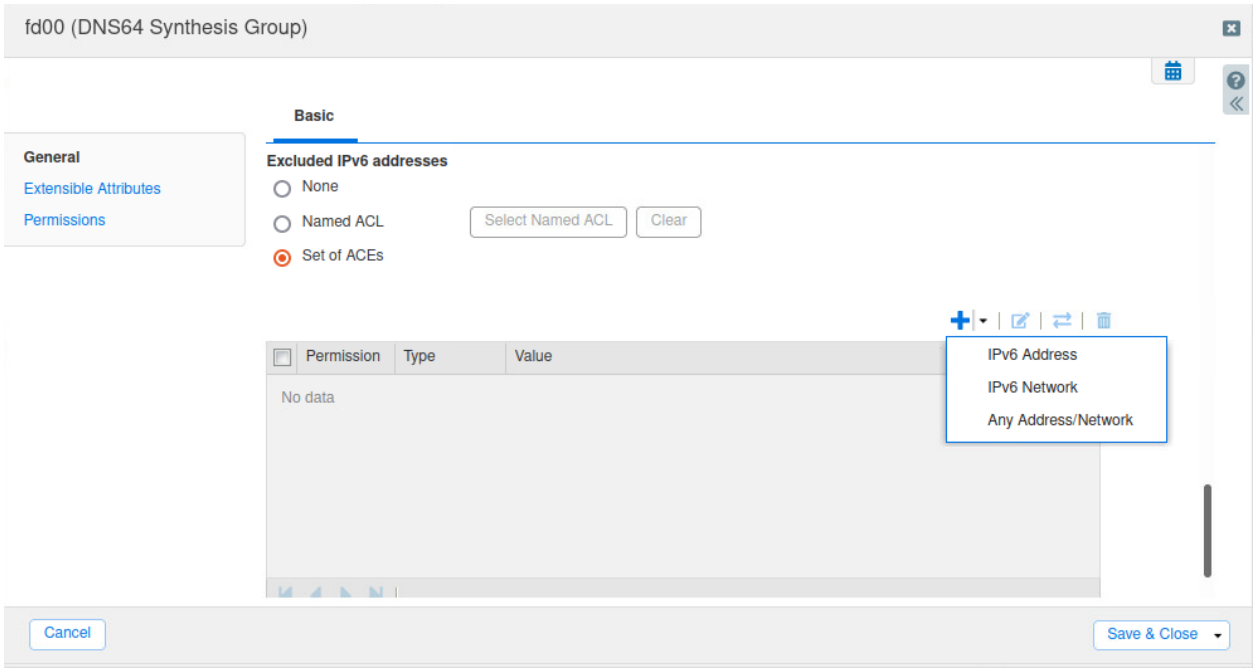
- **Any Address/Network**: Select this to allow or deny any IPv4 addresses for which the appliance synthesizes AAAA records. After you have added access control entries, you can do the following:

    - Select the ACEs that you want to consolidate and put into a new named ACL. Click the **Create** new named ACL icon and enter a name in the Convert to Named ACL dialog box. The appliance creates a new named ACL and adds it to the Named ACL panel. *Note that the ACEs you configured for this operation stay intact.*

    - Reorder the list of ACEs using the up and down arrows next to the table.

    - Select an ACE and click the **Edit** icon to modify the entry.

    - Select an ACE and click the **Delete** icon to delete the entry. You can select multiple ACEs for deletion.



Exclude IPv6 addresses: Specify IPv6 addresses of AAAA records that the appliance treats as nonexistent. The DNS server does not return the AAAA record of an address from this list. Instead, it synthesizes an AAAA record from the A record.

- **None**: Select this if you do not want to define specific IPv6 addresses or networks of AAAA records that the appliance treats as nonexistent. The appliance treats all IPv6 addresses as nonexistent. This is selected by default.

- **Named ACL**: Select this and click **Select Named ACL** to select a named ACL. Grid Manager displays the Named ACLs Selector. Select the named ACL you want to use. If you have only one named ACL, Grid Manager automatically displays the named ACL. When you select this option, the appliance synthesizes AAAA records from A records for the clients that have the Allow permission in the list. You can click **Clear** to remove the selected named ACL.

- **Set of ACEs**: Select this to configure individual ACEs. Click the **Add** icon and select one of the following from the drop-down list. Depending on the item you select, Grid Manager either adds a row for the selected item or expands the panel so you can specify additional information about the item you are adding, as follows.

    - **IPv6 Address**: Select this to add an IPv6 address. Click the **Value** field and enter the IP address. The Permission column displays Allow by default. You can change it to Deny by clicking the field and selecting Deny from the drop-down list.

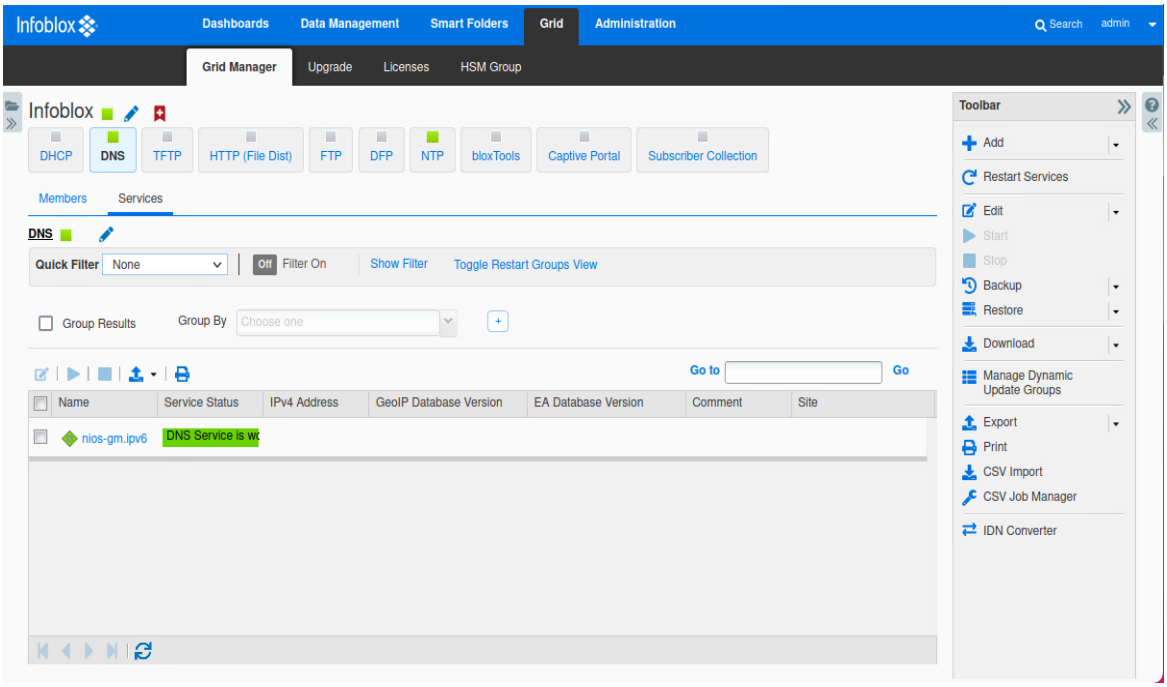
    - **IPv6 Network**: In the Add IPv6 Network panel, complete the following, and then click **Add** to add the network to the list:

        - **Address**: Enter an IPv6 network address and select the netmask from the drop-down list.
        - **Permission**: Select Allow or Deny from the drop-down list.
    - **Any Address/Network**: Select this to allow or deny any IP addresses of AAAA records that the appliance treats as nonexistent.

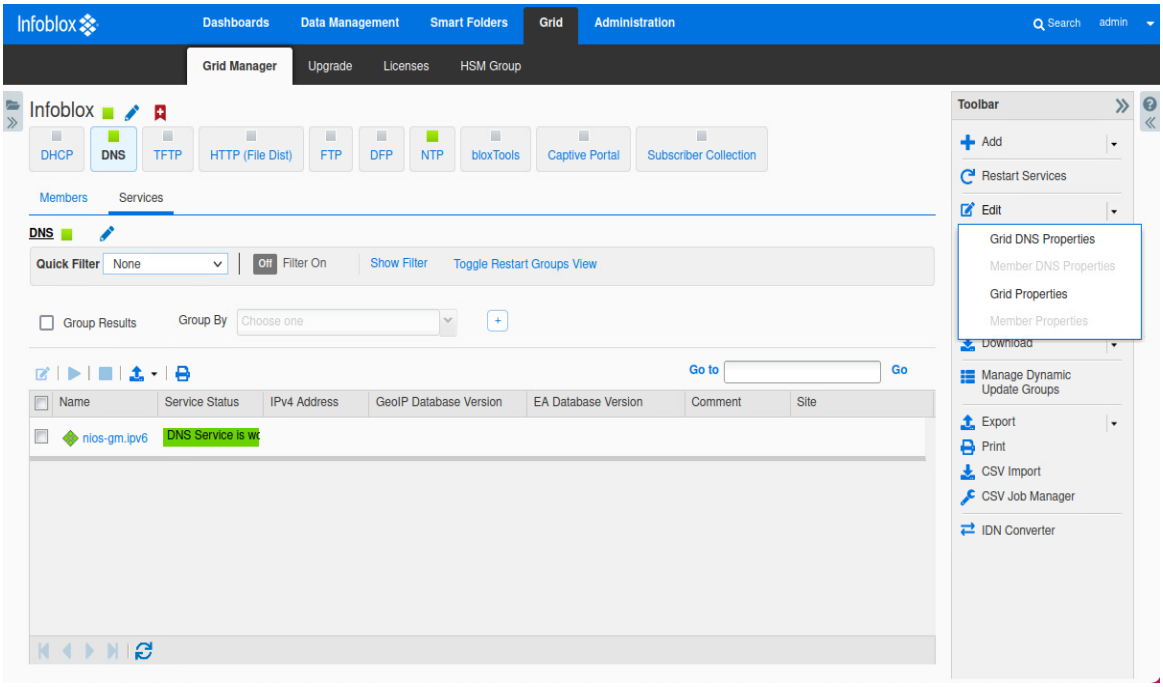
- After you have added access control entries, you can do the following:
    - Select the ACEs that you want to consolidate and put into a new named ACL. Click the **Create** new named ACL icon and enter a name in the Convert to Named ACL dialog box. The appliance creates a new named ACL and adds it to the Named ACL panel. Note that the ACEs you configure for this operation stay intact.
    - Reorder the list of ACEs using the up and down arrows next to the table.
    - Select an ACE and click the **Edit** icon to modify the entry.
    - Select an ACE and click the **Delete** icon to delete the entry. You can select multiple ACEs for deletion.
- Click **Save and Close**.

Enabling DNS64

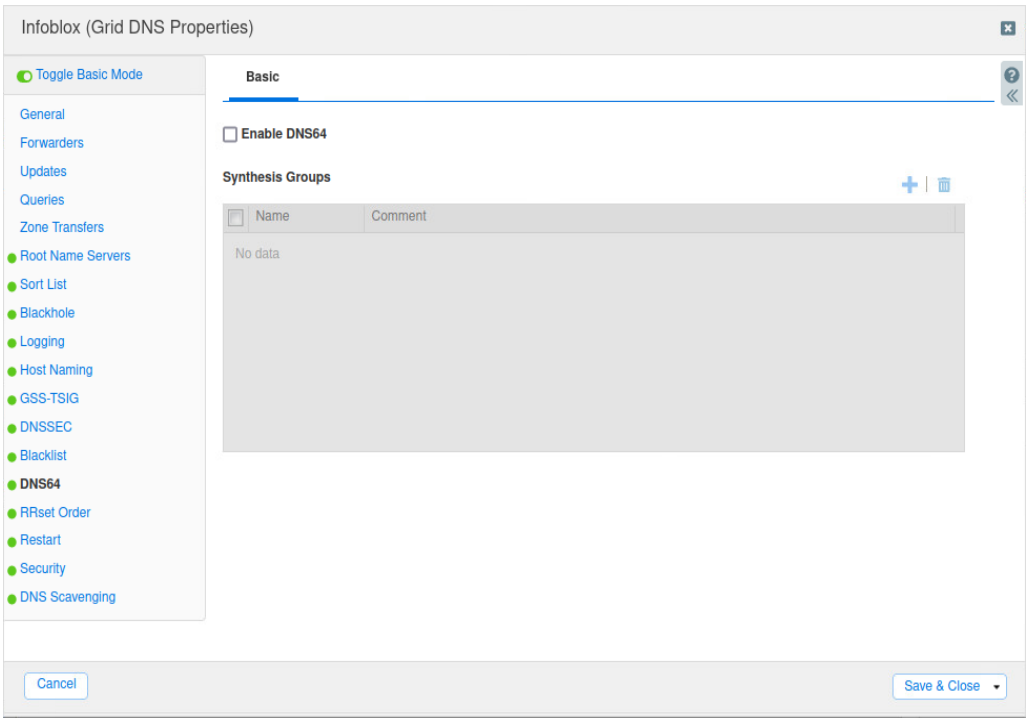
1. Navigate to **Grid → Grid Manager → DNS**.



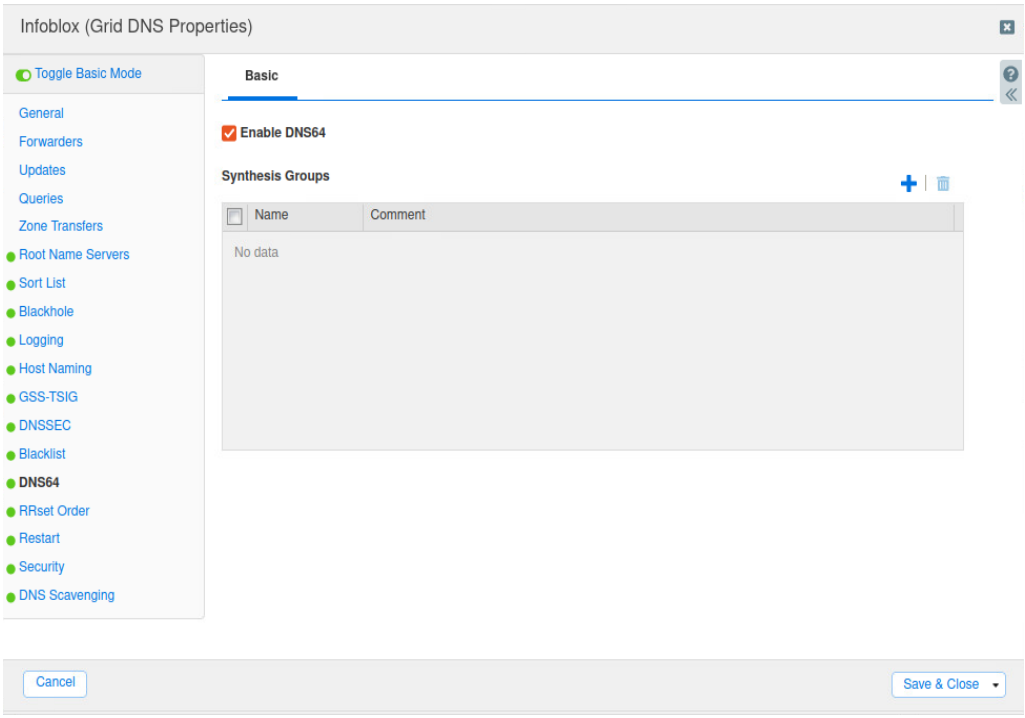
2. On the Toolbar, click on **Edit → Grid DNS Properties**



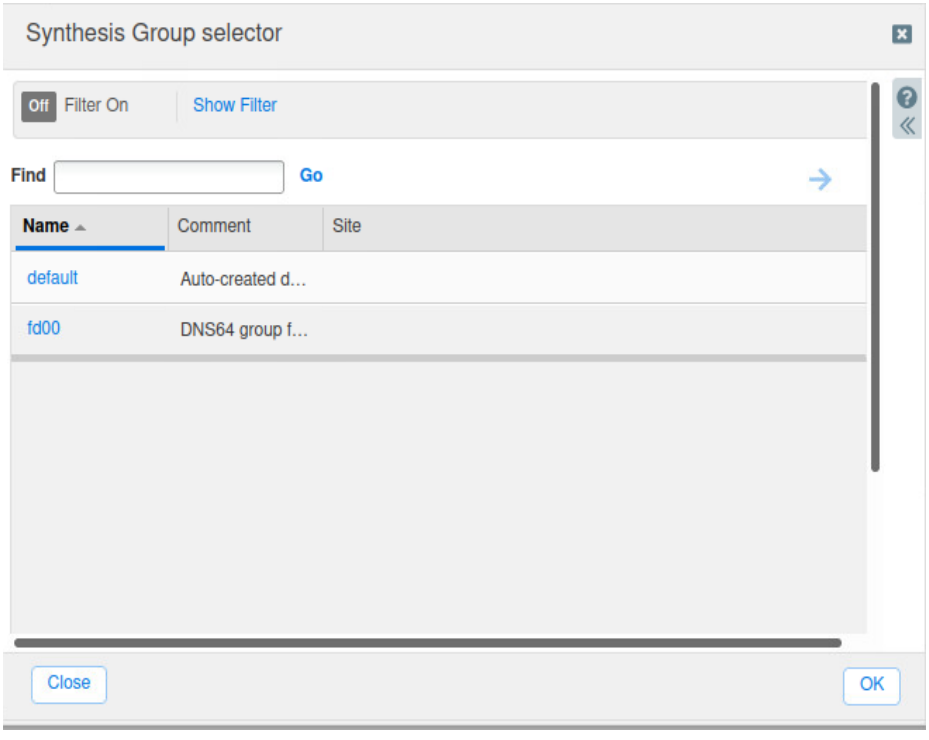
3. Click on **Toggle Advanced Mode** if needed and then click on **DNS64**.



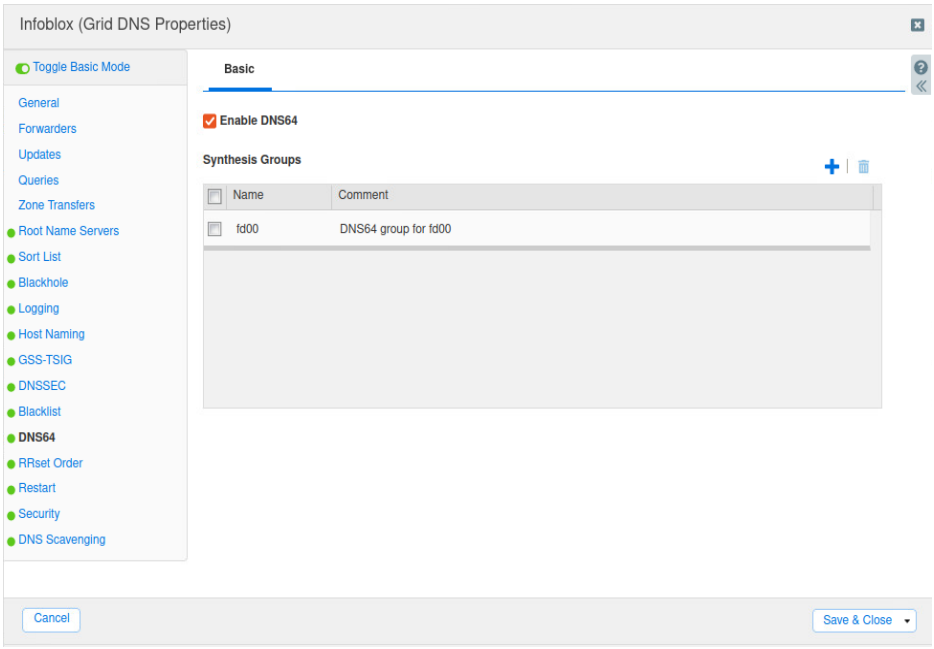
4. Check the **box** to enable DNS64.



5. Click on the '+' sign to add the synthesis group.



6. Click on the **entry** that was created then click **Save and Close**.



7. Click **Restart**.

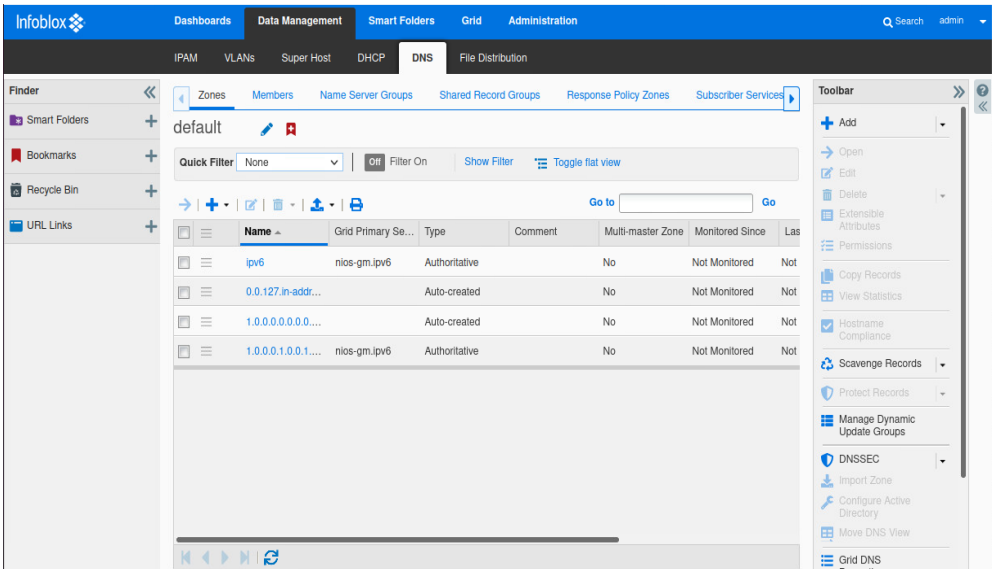
Note: You can add individual access control entries (ACEs) or use a named access control list (ACL) to define these clients.

Match Clients for DNS Views

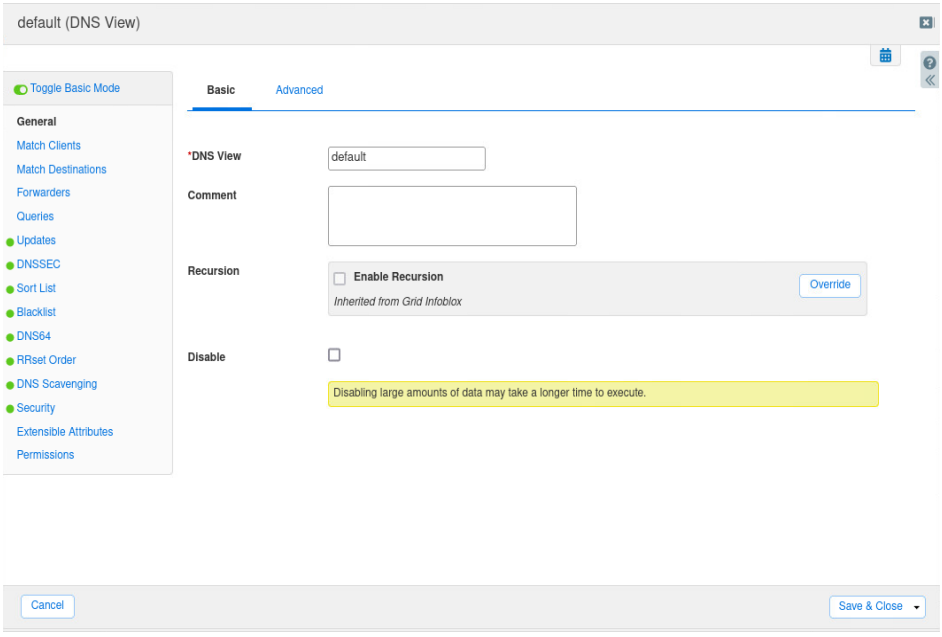
When you configure a DNS view, you can create a Match Clients list to identify source IP addresses and TSIG keys that are allowed or denied access to the DNS view. The NIOS appliance determines which hosts can access a DNS view by matching the source IP address or TSIG key with its Match Clients list. After the appliance determines that a host can access a DNS view, it checks the zone level settings to determine whether it can provide the service that the host is requesting for that zone.

Configuring Match Clients List for a DNS View.

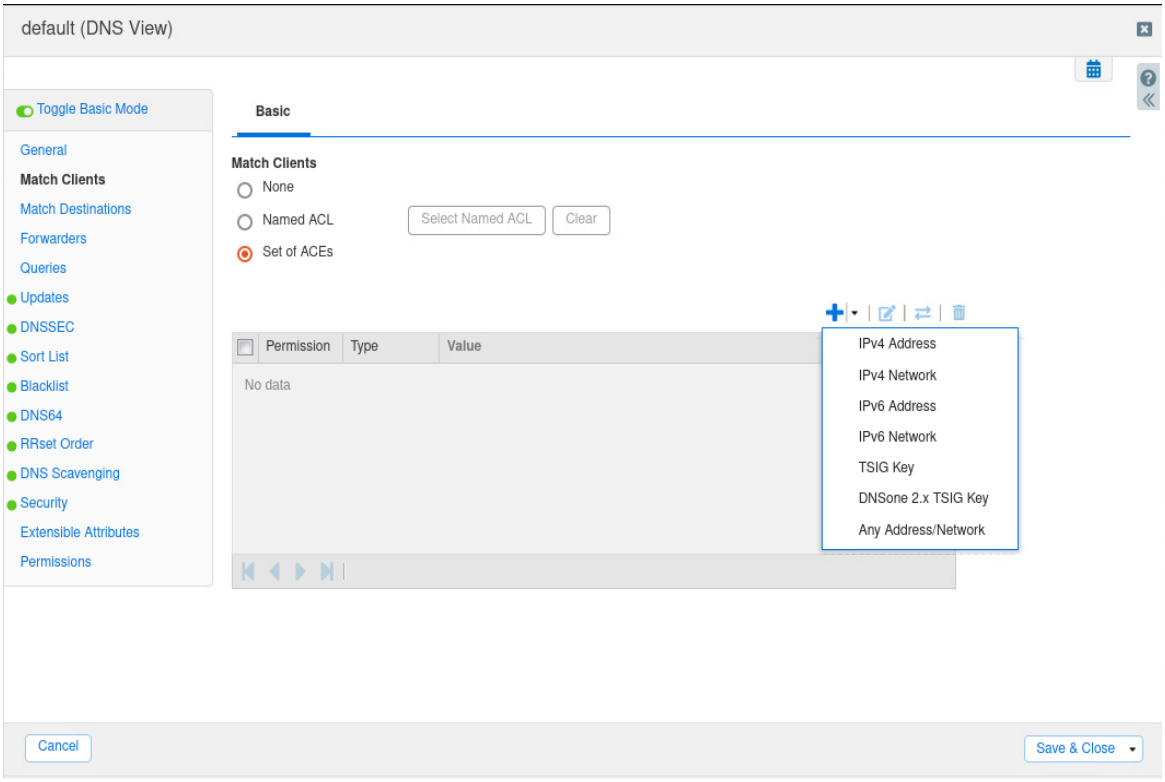
1. Navigate to **Data Management → DNS → Zones**



2. Click on the **Pencil** to the right of the view name which is '**default**' in this example.



3. Click on **Match Clients.**



4. **None**: Select this if you want to configure a Match Clients list. The appliance allows all clients to access the DNS view. This is selected by default.

5. **Named ACL**: Select this and click **Select Named ACL** to select a named ACL. Grid Manager displays the Named ACLs Selector. Select the named ACL you want to use. If you have only one named ACL, Grid Manager automatically displays the named ACL. When you select this option, the appliance allows access to the DNS view from the destination addresses that have the Allow permission in the named ACL. You can click Clear to remove the selected named ACL.

6. **Set of ACEs**: Select this to configure individual ACEs. Click the **Add** icon and select one of the following from the drop-down list. Depending on the item you select, Grid Manager either adds a row for the selected item or expands the panel so you can specify additional information about the item you are adding, as follows.

    - **IPv4 Address and IPv6 Address**: Select this to add an IPv4 address or IPv6 address. Click the **Value** field and enter the IP address. The Permission column displays Allow by default. You can change it to Deny by clicking the field and selecting Deny from the drop-down list.

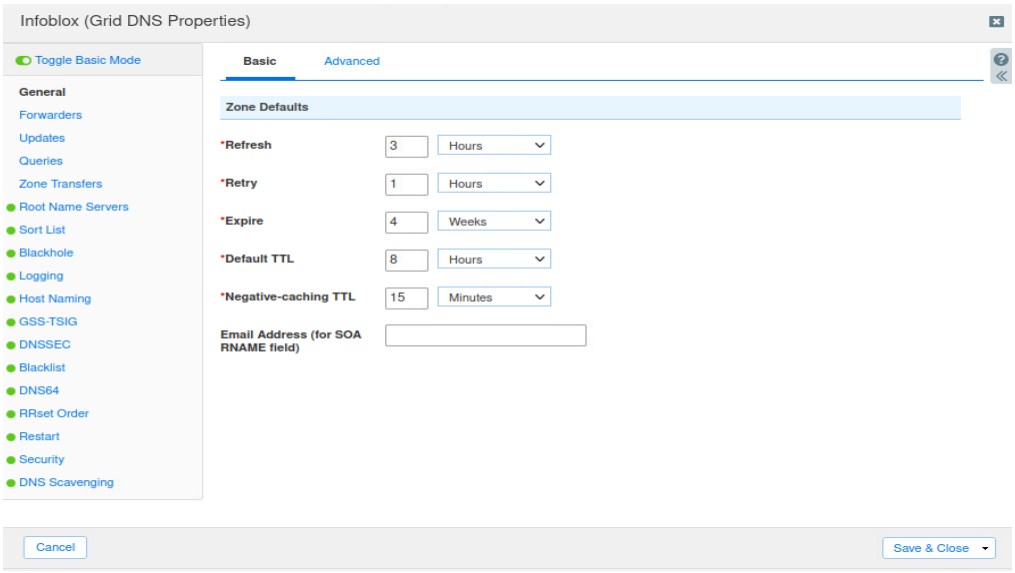
    - **IPv4 Network**: In the Add IPv4 Network panel, complete the following, and then click **Add** to add the network to the list:

        - **Address**: Enter an IPv4 network address and either type a netmask or move the slider to the desired netmask.
        - **Permission**: Select Allow or Deny from the drop-down list.
    - **IPv6 Network**: In the Add IPv6 Network panel, complete the following, and then click Add to add the network to the list:
        - **Address**: Enter an IPv6 network address and select the netmask from the drop-down list.
        - **Permission**: Select Allow or Deny from the drop-down list.
    - **TSIG Key**: In the Add TSIG Key panel, complete the following, and then click Add to add the TSIG key to the list:
        - **Key name**: Enter a meaningful name for the key, such as a zone name or the name of the client or Grid member. This name must match the name of the same TSIG key on other name servers.
        - **Key Algorithm**: Select either HMAC-MD5 or HMAC-SHA256.
        - **Key Data**: To use an existing TSIG key, type or paste the key in the Key Data field. Alternatively, you can select the key algorithm, select the key length from the Generate Key Data drop down list, and then click Generate Key Data to create a new key.
    - **DNSone 2.x TSIG Key**: Select this when the other name server is a NIOS appliance running DNS One 2.x code. The appliance automatically populates the value of the key in the Value field. The Permission column displays Allow by default. You cannot change the default permission.
    - **Any Address/Network**: Select this to allow or deny any IP addresses to access the DNS view. After you have added access control entries, you can do the following:
        - Select the ACEs that you want to consolidate and put into a new named ACL. Click the Create new named ACL icon and enter a name in the Convert to Named ACL dialog box. The appliance creates a new named ACL and adds it to the Named ACL panel. Note that the ACEs you configure for this operation stay intact.
        - Reorder the list of ACEs using the up and down arrows next to the table.
        - Select an ACE and click the **Edit** icon to modify the entry.
        - Select an ACE and click the **Delete** icon to delete the entry. You can select multiple ACEs for deletion.
7. Click **Save and Close**.

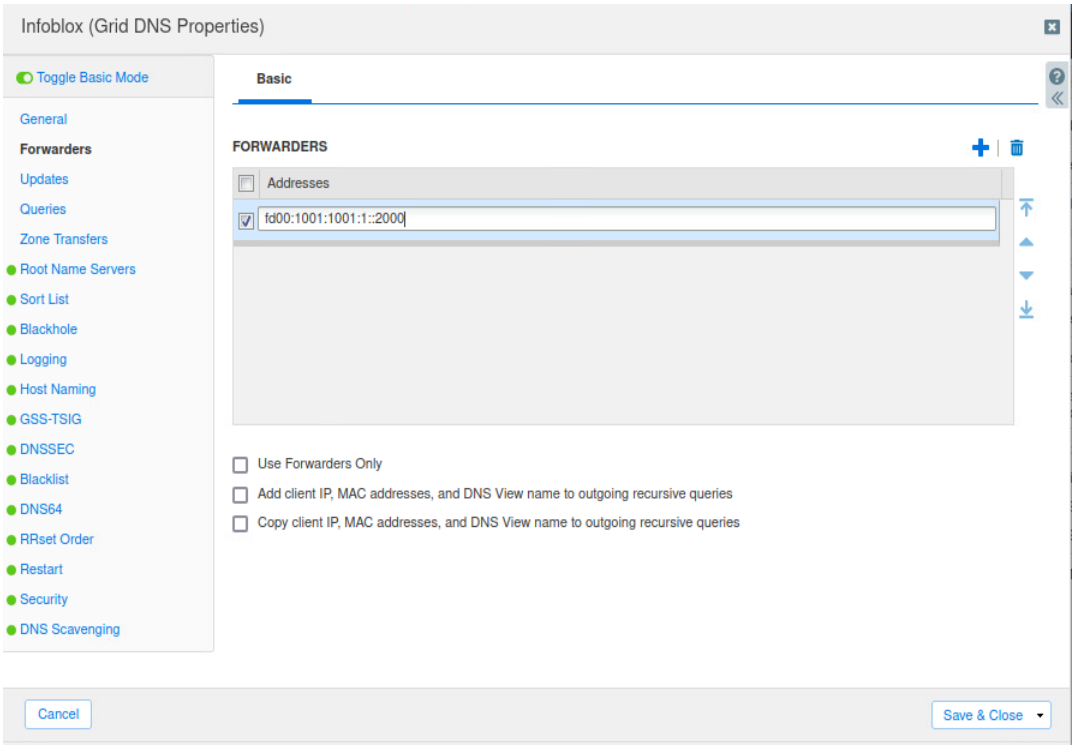
Enabling IPv6 Grid DNS Properties

You can enable the following properties that are relevant to IPv6: forwarders, updates, queries, zone transfer, and blackhole.

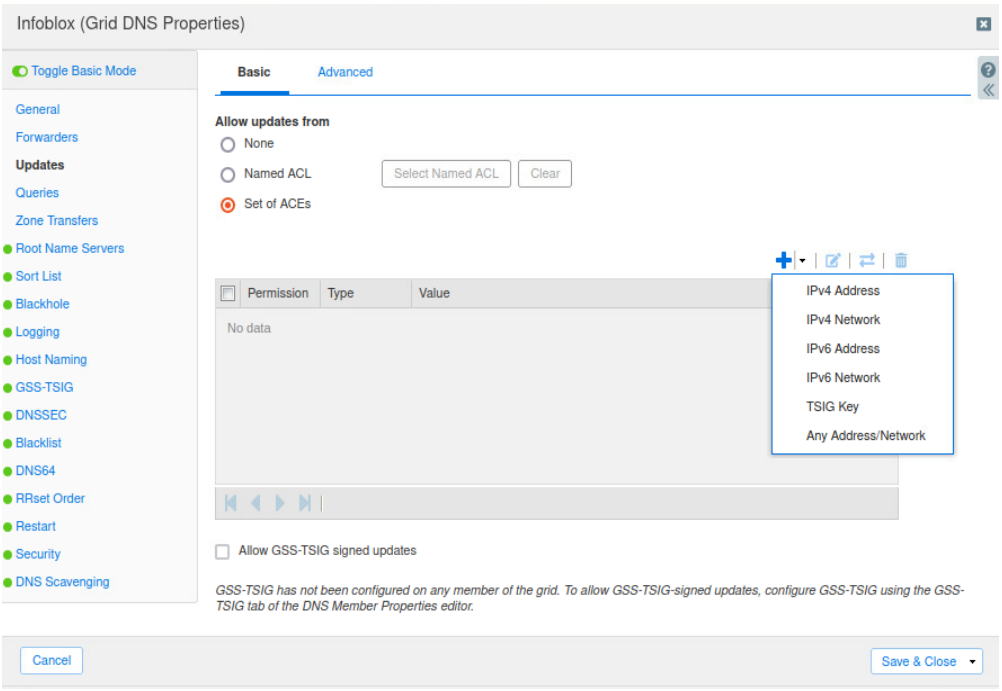
1. Navigate to **Grid** → **Grid Manager** → **DNS** .
2. **In the** toolbar, use the **Edit** dropdown to select **Grid DNS Properties**.



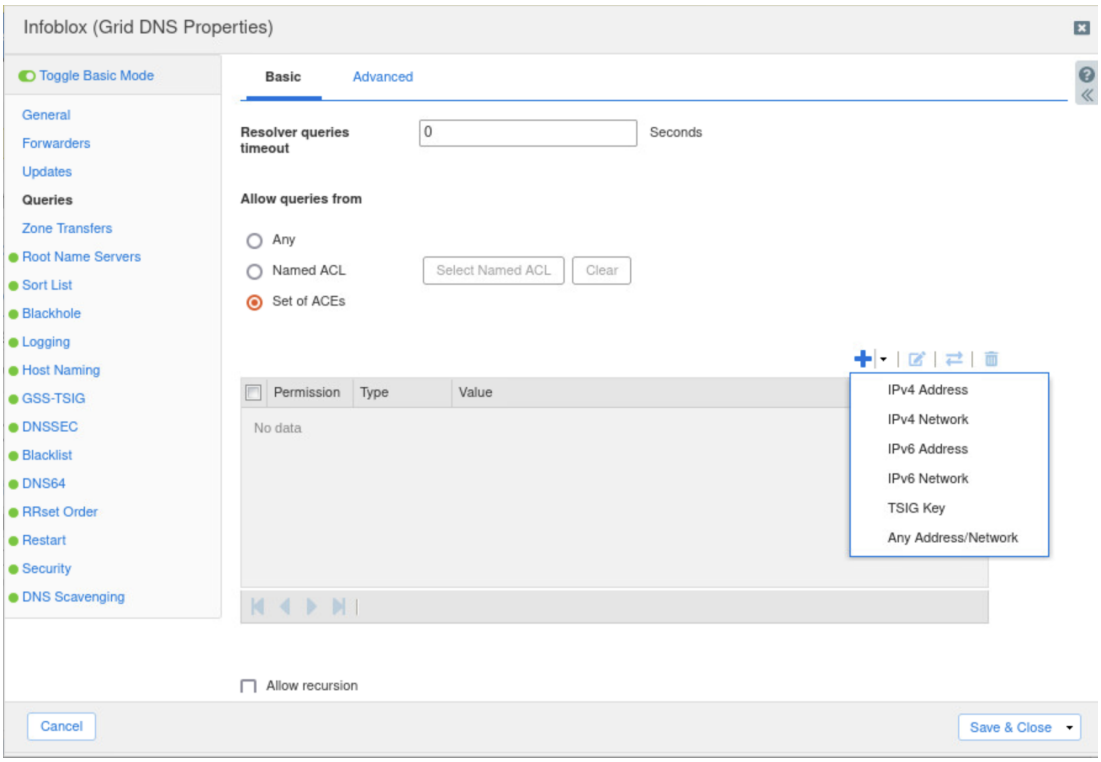
3. Click on the **Forwarders** tab. Click on the '**+**' button to add an IPv6 address for the forwarder.



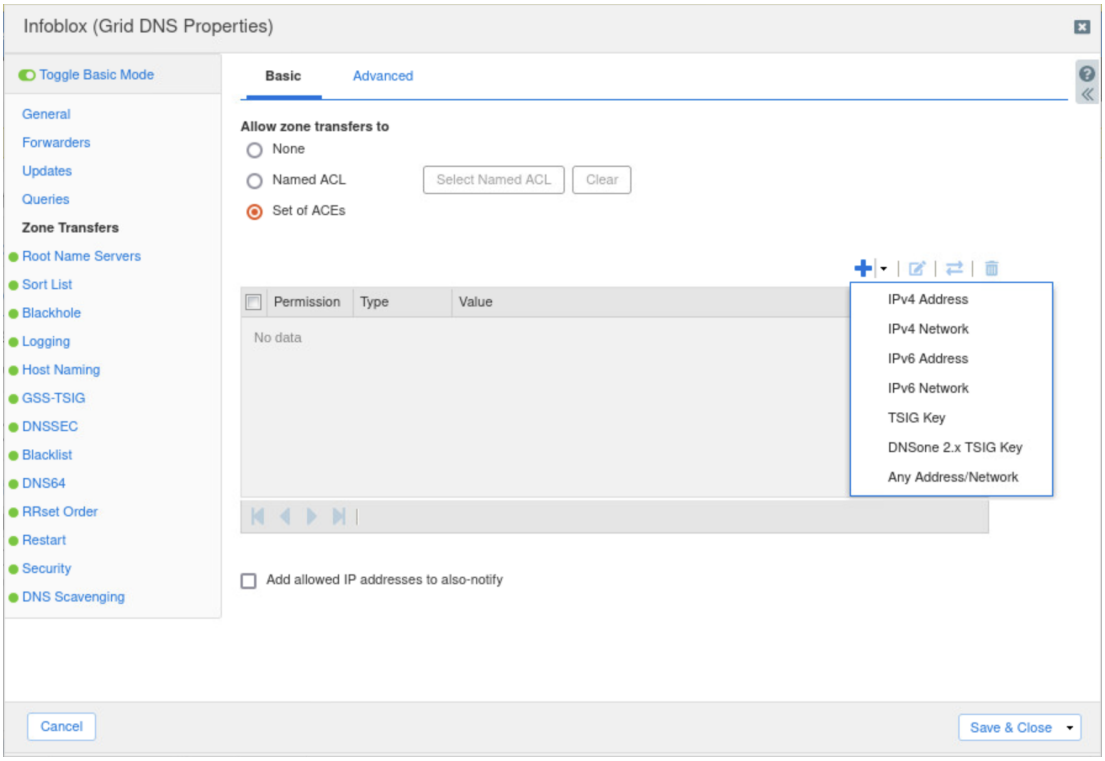
4. Click on the **Updates** tab. Click on **Set of ACEs**. Click on the '**+**' button to add either an IPv6 address or IPv6 network.



5. Click on the **Queries** tab. Enter a **Resolver queries timeout** value and under **Allow Queries from**, click on **Set of ACEs** to add either an IPv6 address or IPv6 network.



6. Click on the **Zone Transfers** tab. Click on **Set of ACEs**. Click on the '**+**' button to add either an IPv6 address or IPv6 network.



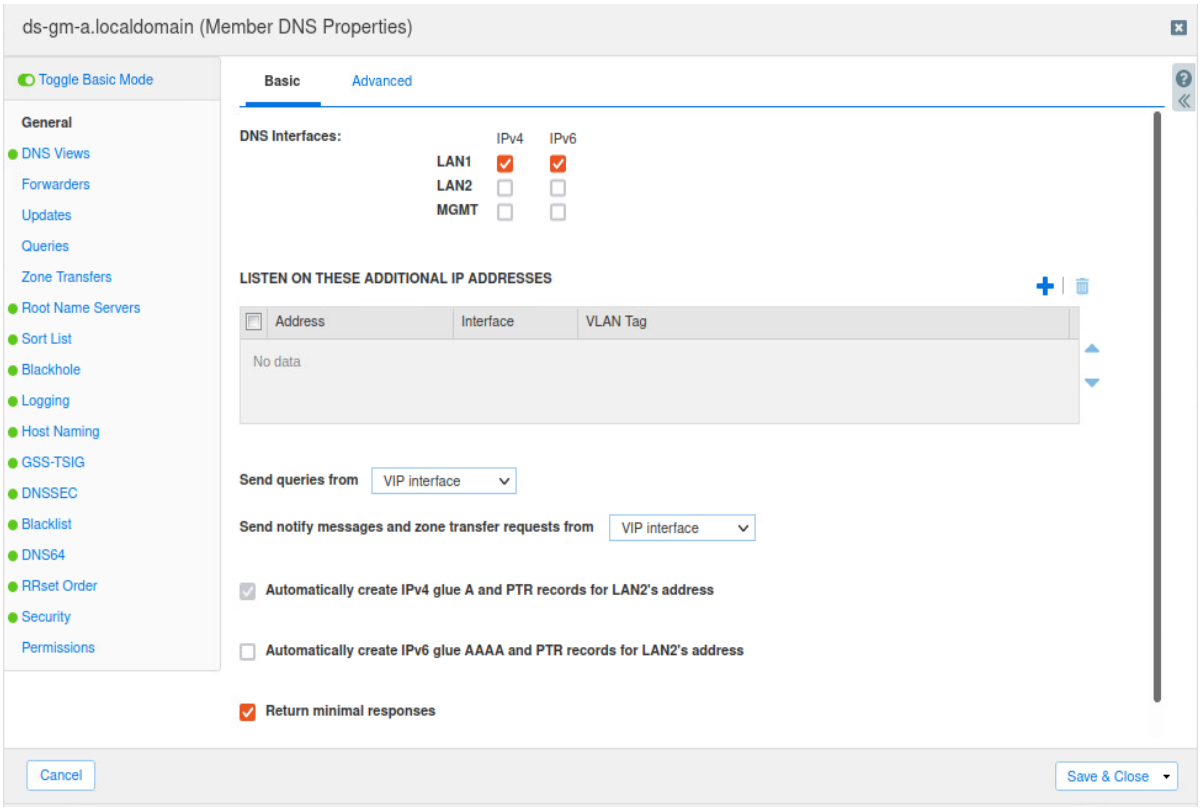
7. Click **Save and Close**.

Enabling IPv6 Grid DNS Member Properties

1. Navigate to **Grid** → **Grid Manager** → **DNS**.

2. Select a **member** to edit. Click on the **Edit** button.

3. Based upon your configuration, enable the **IPv6** box for LAN1, LAN2, and/or MGMT to ensure IPv6 communication.



4. Optionally, you can edit **Forwarder**, **Updates**, **Queries**, **Zone Transfers**, and **Blackhole** in this section if you choose for different settings from the Grid settings.

5. Click **Save and Close**.

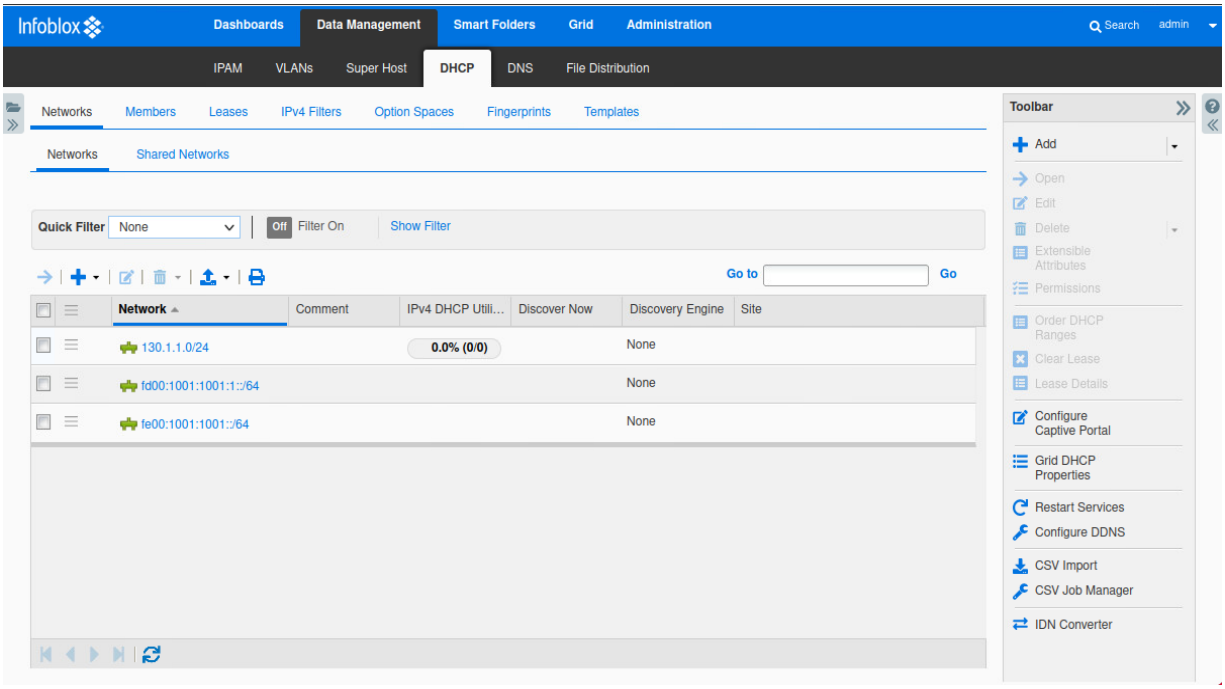
DHCP

NIOS appliances support DHCP for IPv6 (DHCPv6), the protocol for providing DHCP services forIPv6 networks. The DHCPv6 client-server model is similar to that of IPv4. DHCP clients and servers use a reserved, link-scoped multicast address to exchange DHCP messages. When a DHCP client needs to send messages to a DHCP server that is not attached to the same link, a DHCP relay agent can be used to relay messages between the client and server. Each IPv6 DHCP server and client has a unique DHCP unique identifier (DUID). DHCP servers use DUIDs to identify clients when providing configuration parameters, and clients use DUIDs to identify the source of the DHCP messages from servers.

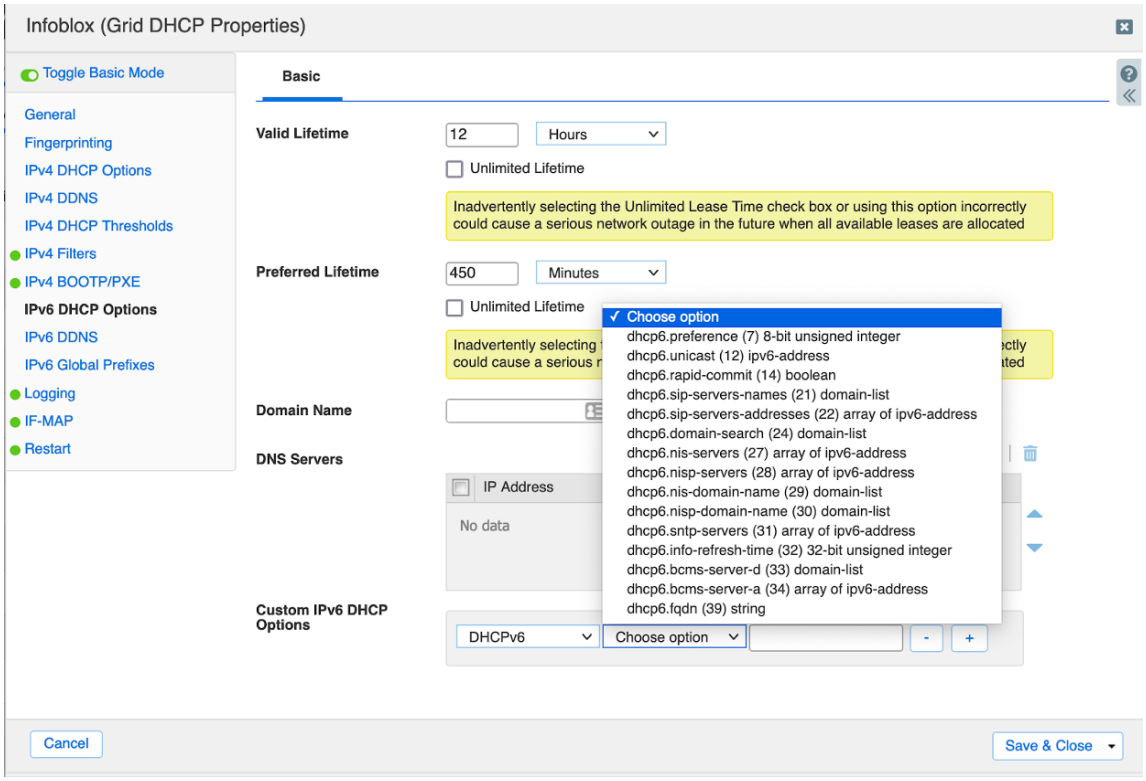
Configuring for IPv6 DHCP

1. Navigate to **Data Management → DHCP**

2. On the Toolbar, click on **Grid DHCP Properties**.



3. Click on the **IPv6 DHCP Options** tab.

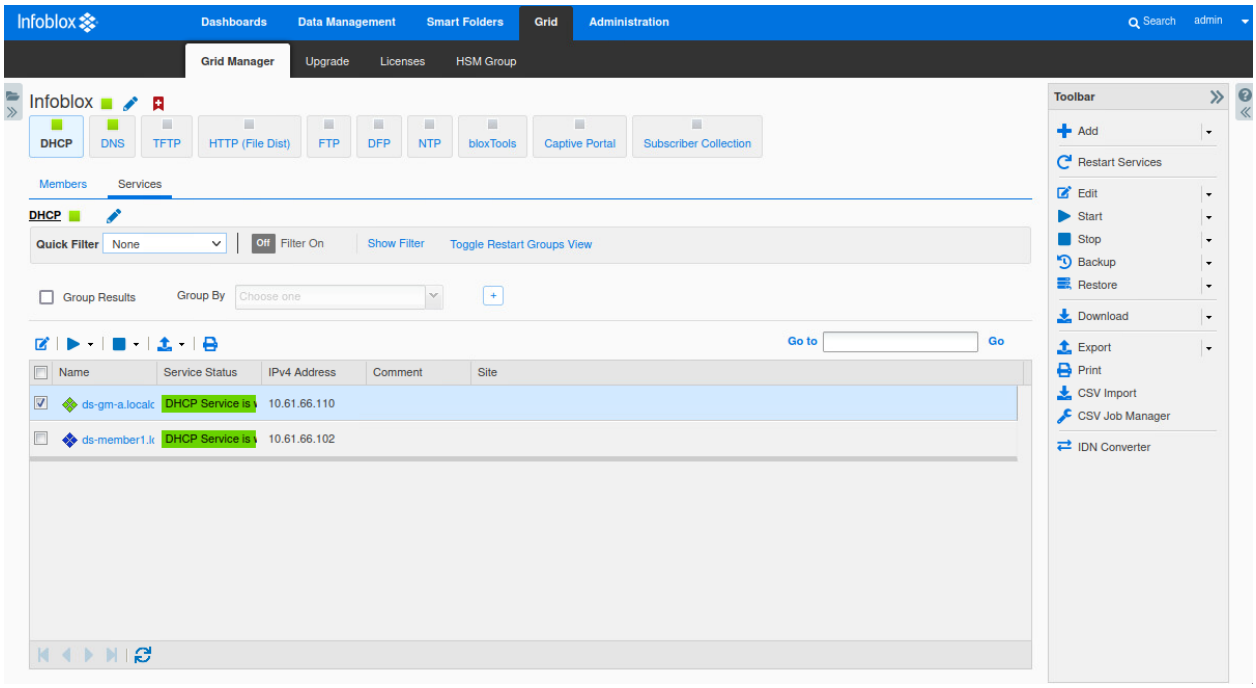


- **Valid Lifetime**: Specify the length of time addresses that are assigned to DHCP clients remain in the valid state. When this time expires, an address becomes invalid and can be assigned to another interface.
- **Preferred Lifetime**: Specify the length of time that a valid address is preferred. A preferred address can be used with no restrictions. When this time expires, the address becomes deprecated.
- **Domain Name**: Enter the name of the domain for which the Grid serves DHCP data.
- **DNS Servers**: Click the **Add** icon. Grid Manager adds a row to the table. In the table, enter the IPv6addresses of DNS recursive name servers to which the DHCP client can send name resolution requests. The DHCP server includes this information in the DNS Recursive Name Server option in Advertise, Rebind, Information-Request, and Reply messages.
- **Custom IPv6 DHCP Options**: In the first field, select one of the following from the drop-down list:
  - **DHCPv6**: Select this to apply DHCPv6 options.
  - **DHCP**: Select this to apply DHCP options (dhcp-renewal-time or dhcp-rebinding-time).

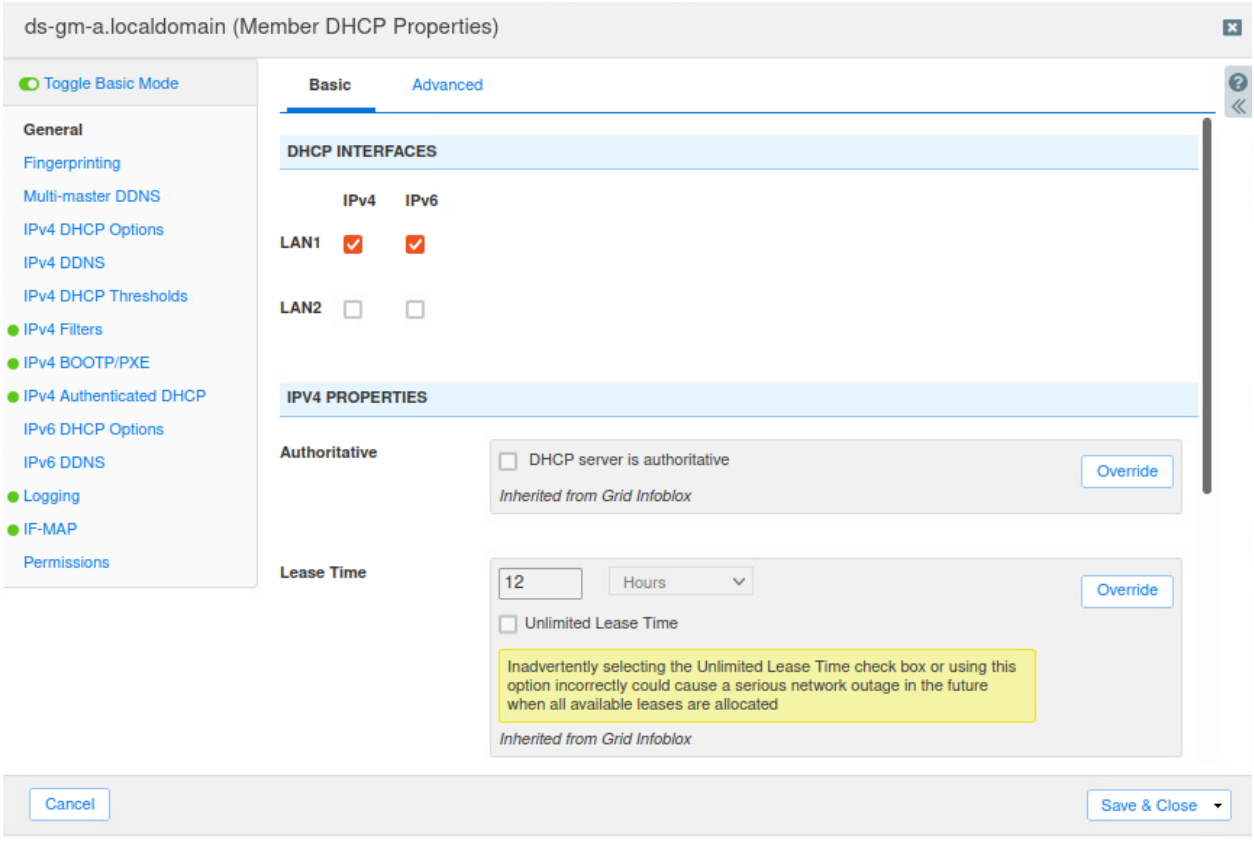
- Click the **Choose** option drop down and then select an option from the list.
- In the third field, enter a value for the selected option. *Note that certain options have predefined data types and their values must be entered in a specific format.* Click **+** to add another option, or click **-** to delete a previously specified option. When overriding an option, enter the new value for the selected option.

Enable IPv6 Grid Member DHCP Properties

1. Navigate to **Grid** → **Grid Manager** → **DHCP**.
2. Click on the member you want to edit. Click on the **Edit** button.



3. Ensure the IPv6 button is enabled for LAN1 and/or LAN2 to ensure IPv6 communication for DHCP.

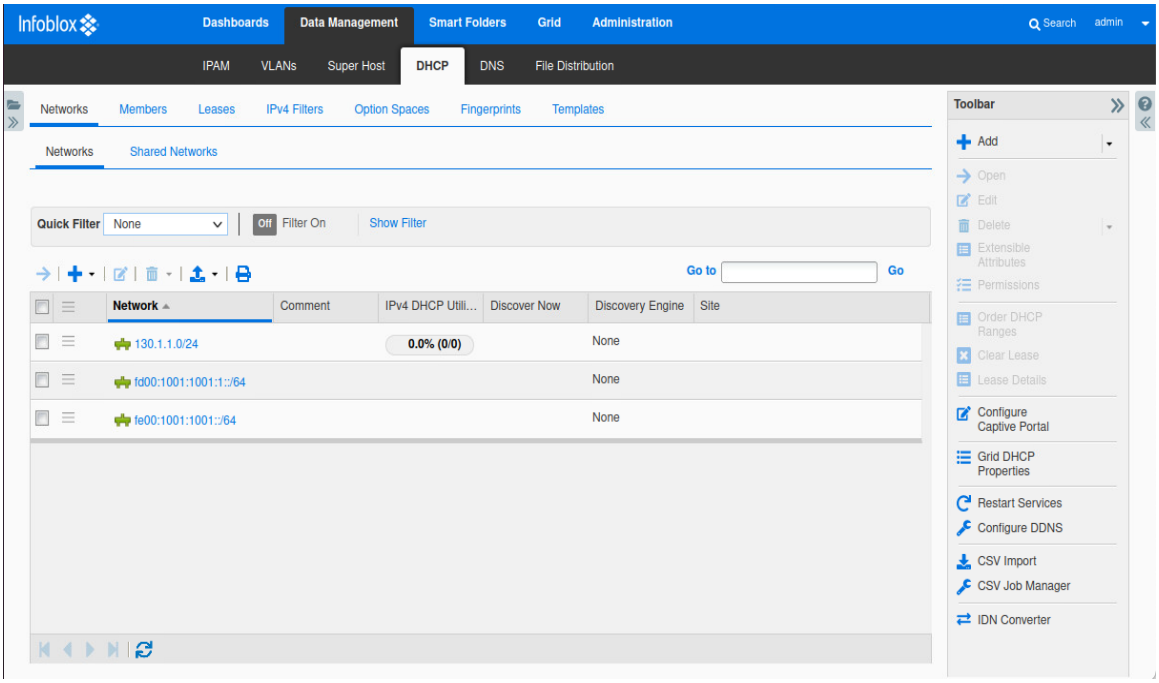


4. Click **Save and Close**.

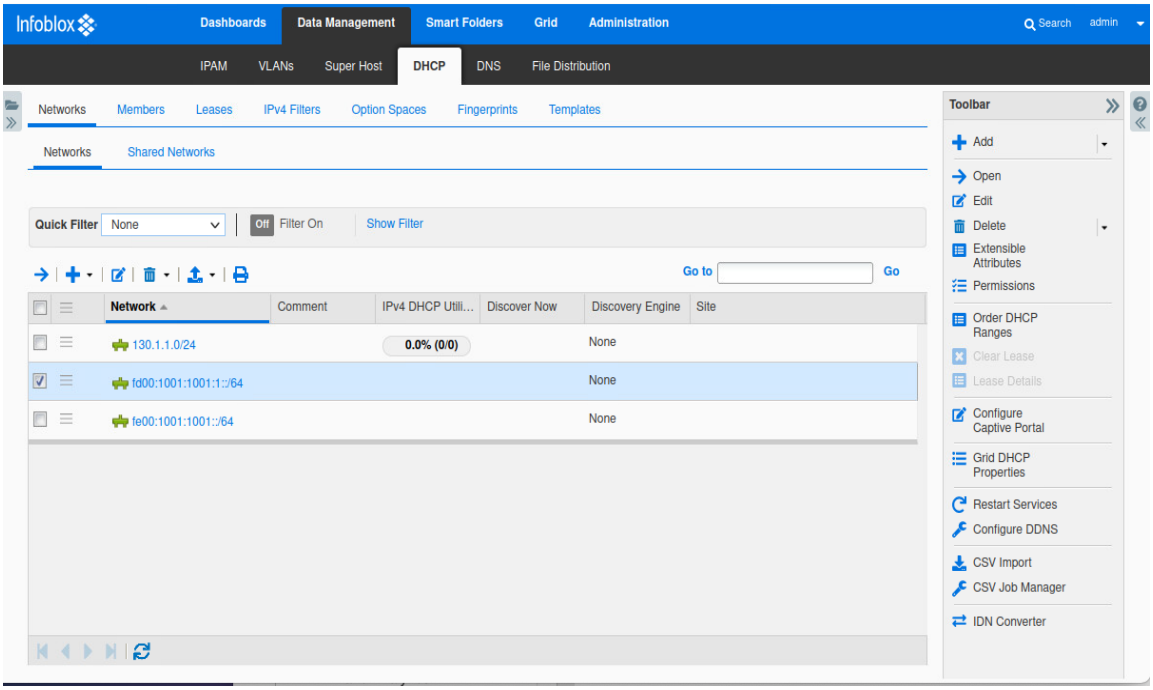
Associating Networks with Zones

You can associate IPv4 and IPv6 networks with DNS zones to limit the zones that admins can use when they create DNS records for IP addresses in the networks. When a network is associated with one or more zones and an admin creates a DNS record for one of its IP addresses, Grid Manager allows the admin to create the DNS record in the associated zones only. For example, if you associate the 10.1.0.0/16 network with the corpxyz.com zone, admins are allowed to create DNS records in the corpxyz.com zone only for IP addresses in the 10.1.0.0/16 network; or if you associate the 2001:db8:1::/48 network with the corp200.com zone, admins are allowed to create DNS records in the corp200.com zone only for IP addresses in the 2001:db8:1::/48 network. This feature applies to A, AAAA and host records only. It does not apply to records in a shared record group. If you are creating a host record with multiple IP addresses in different networks, the networks must be associated with the zone of the host record.

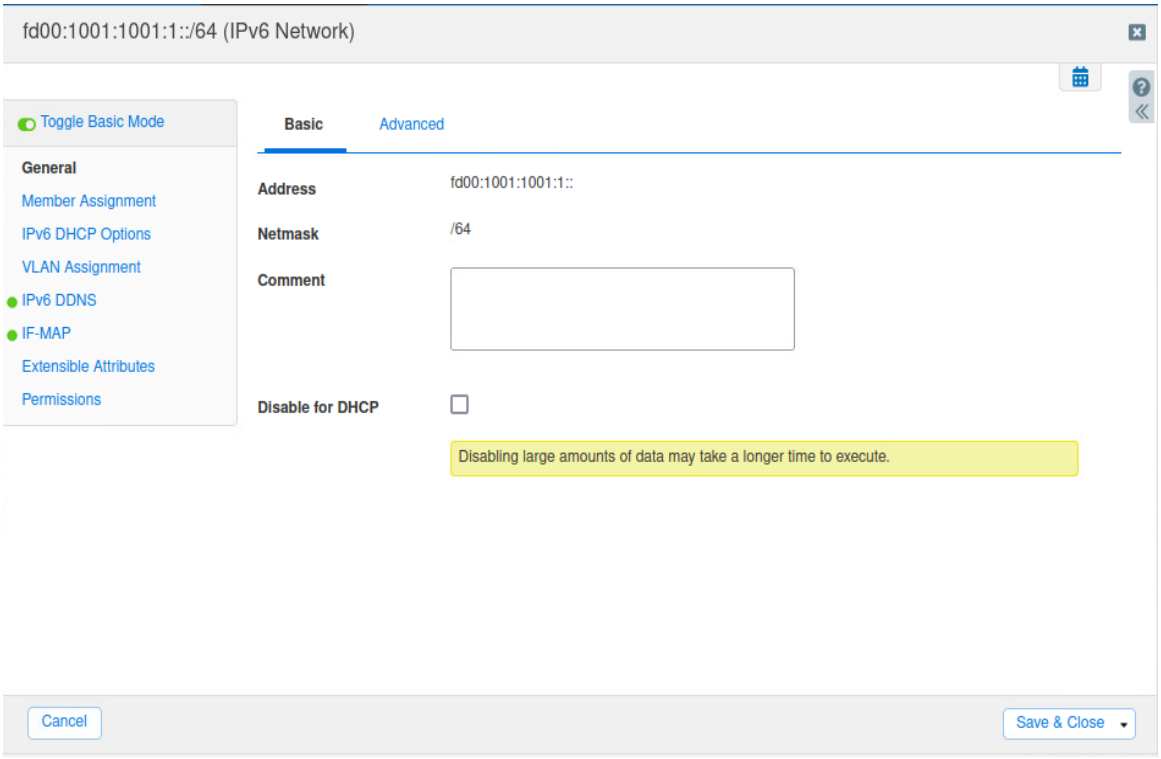
1. Navigate to **Data Management → DHCP → Networks**.



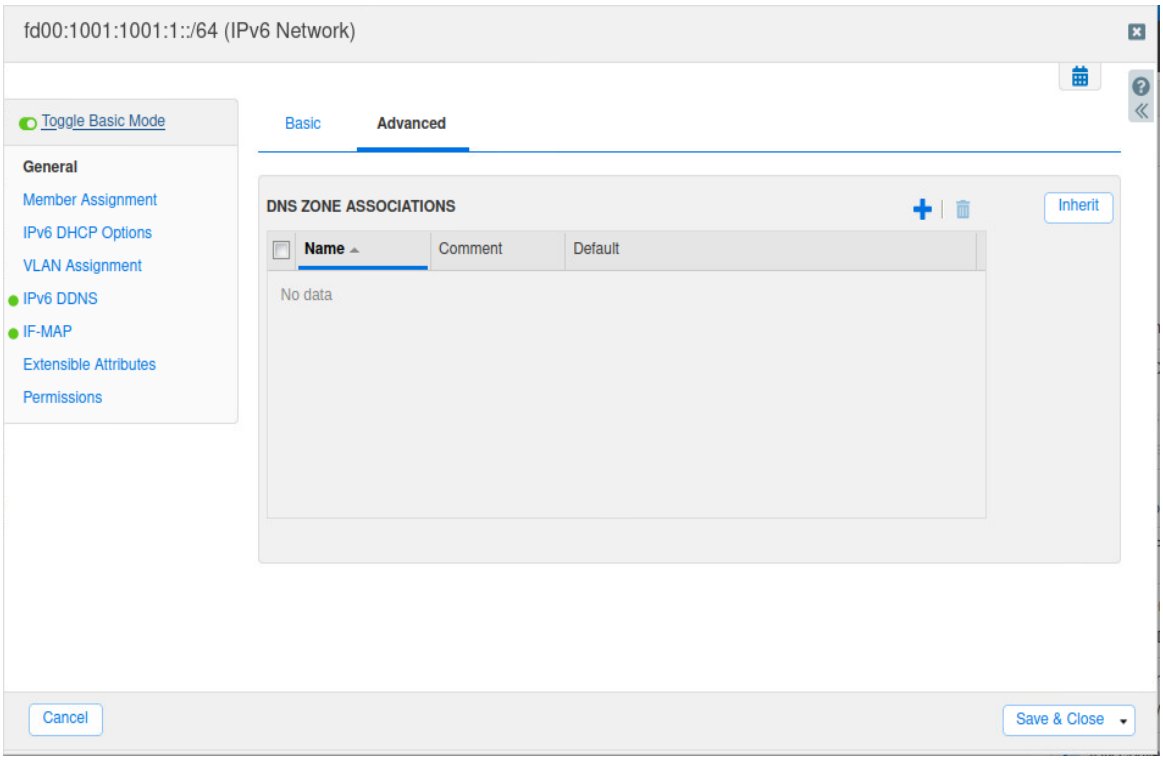
2. Select a **Network**. In this example, network **fd00:1001:1::/64** is chosen.



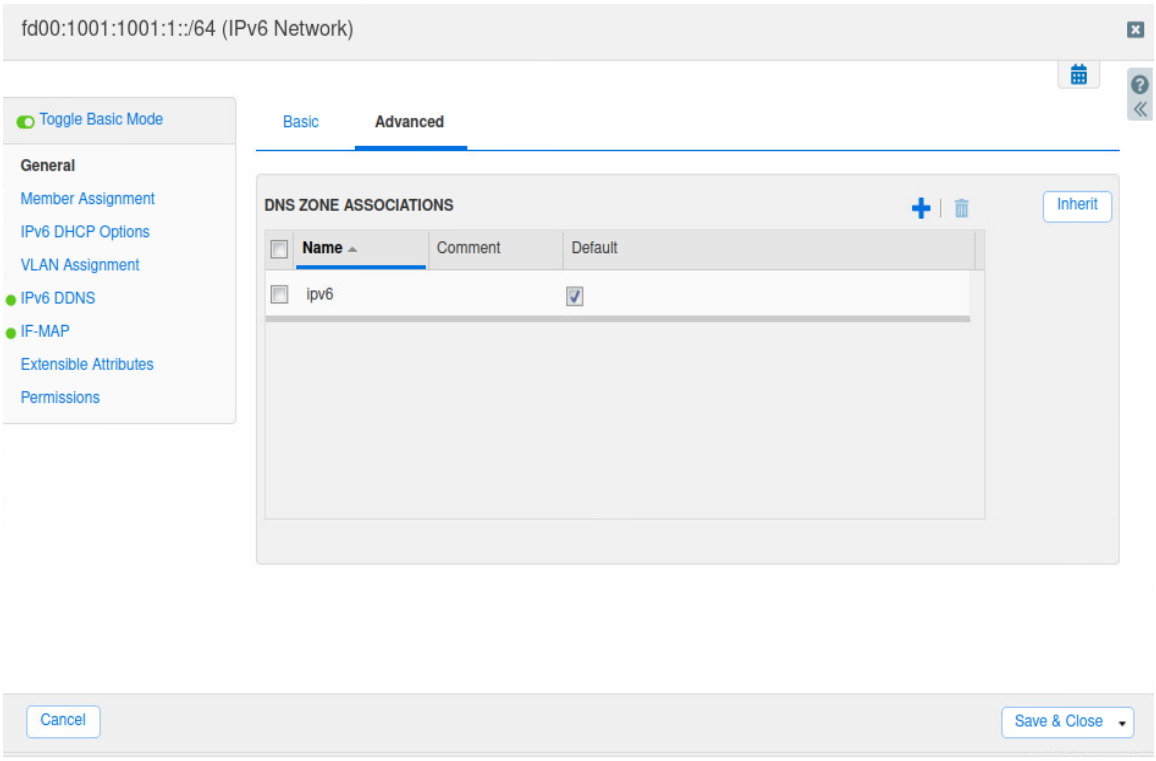
3. Click on the **Edit** button.



4. Click on the **Advanced** Tab.



5. Click on the '+' button to add a DNS zone. In this example, .ipv6 is the DNS zone.

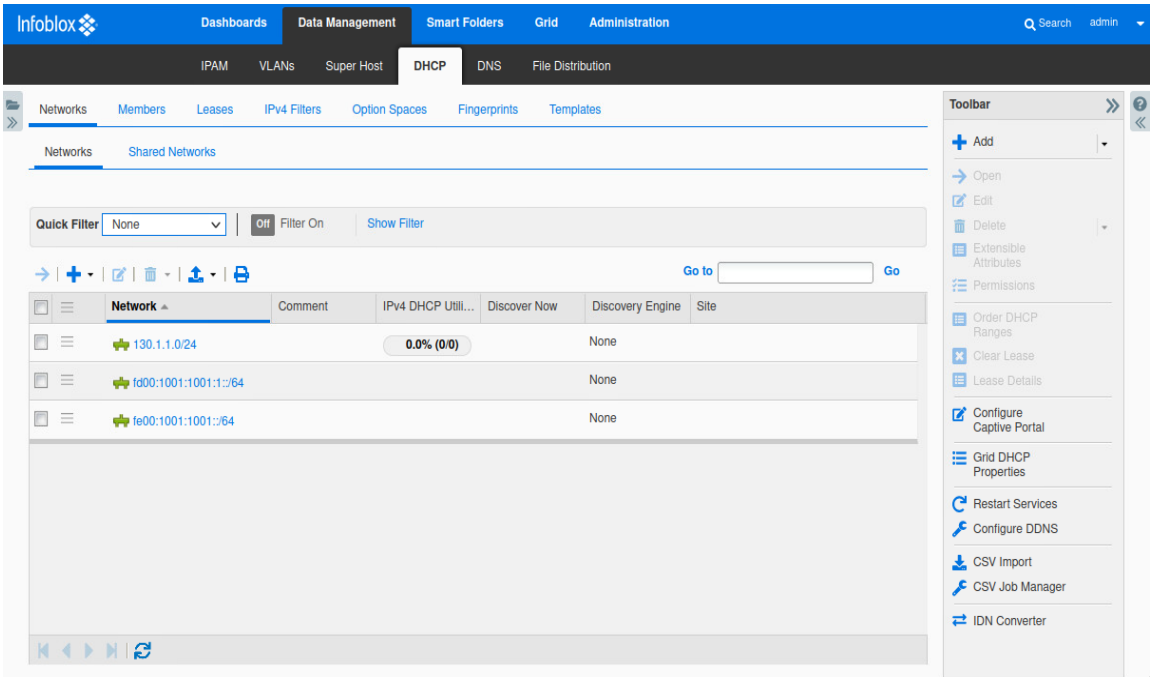


6. Click **Save and Close** and **Restart**

Keeping Leases in Deleted IPv6 Networks and Ranges

You can configure the DHCP server to store leases in a deleted DHCP range for up to one week after the leases expire. When you add a new DHCP range that includes the IP addresses of these leases or assign the DHCP range to another member within the Grid, the appliance automatically restores the active leases. You can configure this feature for the Grid, and override the configuration for members, networks, and DHCP ranges. Below are the instructions.

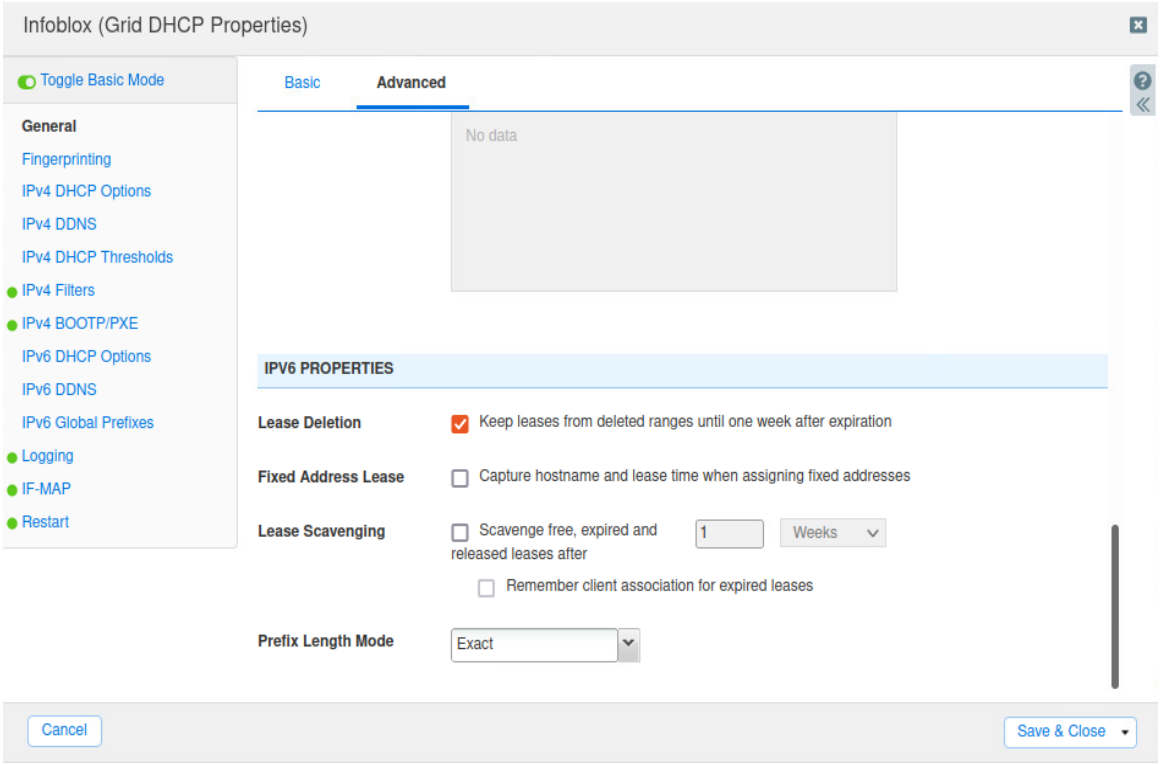
1. Navigate to **Data Management → DHCP**.



2. In the toolbar click on **Grid DHCP Properties**.

3. Click **Advanced** on the General tab.

4. Under IPv6 Properties, select the **checkbox** for Lease Deletion: Keep leases from deleted ranges until one week after expiration

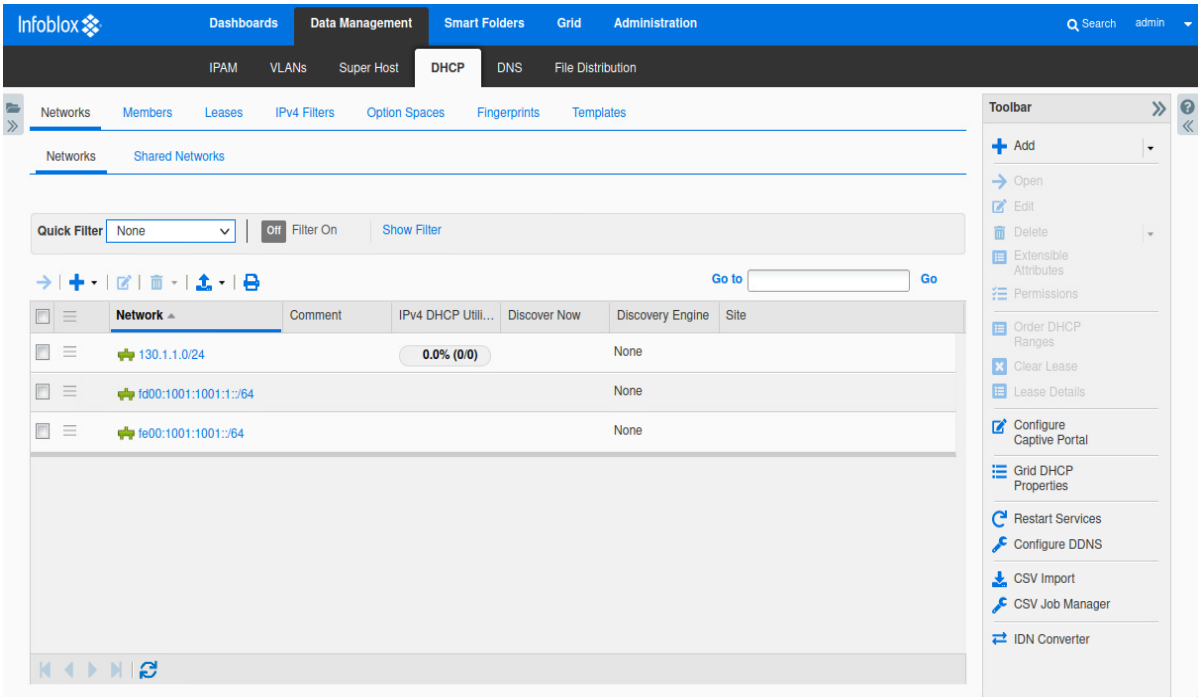


Note: Lease deletion is enabled by default.

Configuring Fixed Address Leases For Display

You can configure the DHCP server to capture the hostname and lease time of a fixed address when you assign an IPv4 or IPv6 fixed address to a client. The appliance displays the hostname, and the start and end time of each fixed address lease in the Current Leases panel in Grid Manager.

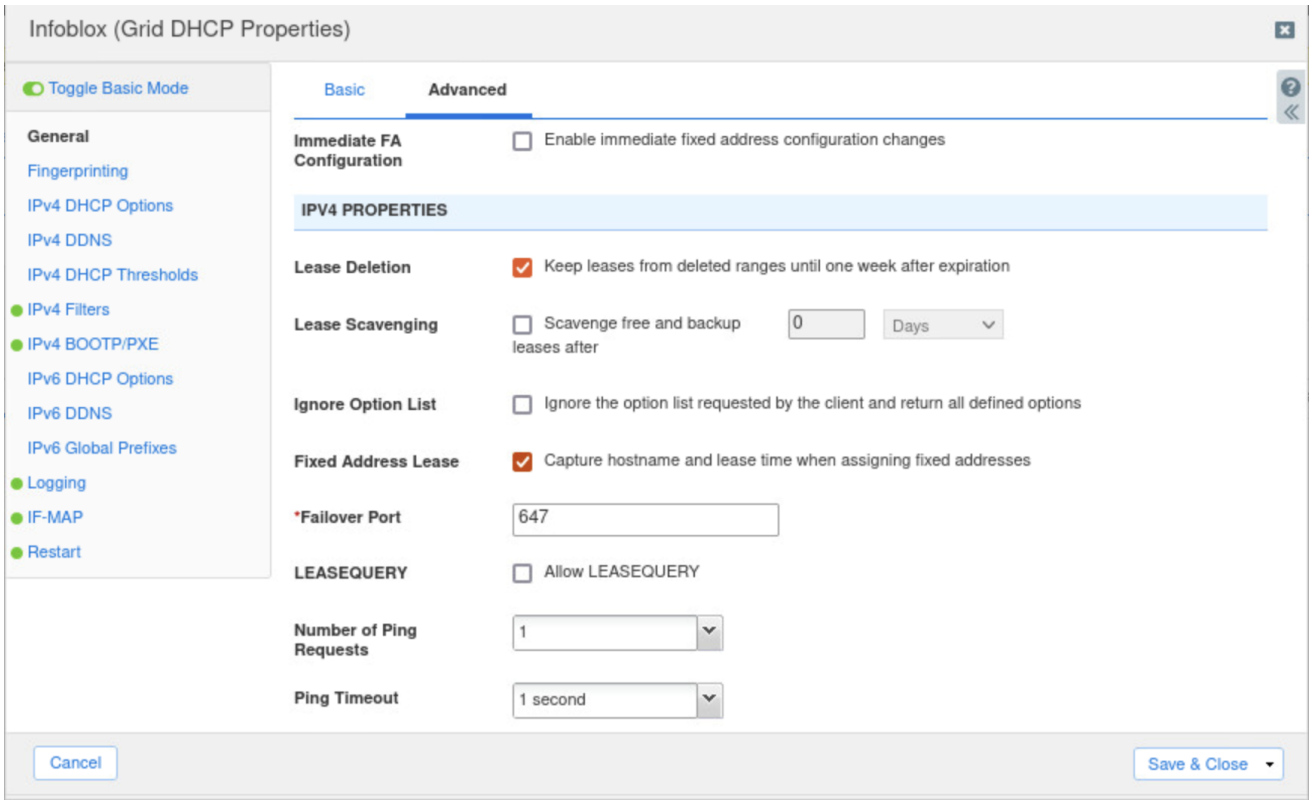
1. Navigate to **Data Management → DHCP**



2. In the toolbar, click **Grid DHCP Properties**.

3. Click **Advanced** on the General tab.

4. Select the checkbox for **Fixed Address Lease: Select Capture hostname and lease time when assigning Fixed Addresses**. *Note: The appliance displays the host name, and the start and end time of each fixed address lease in the Current Leases panel. If there are multiple records (AAAA, host, and lease) for the IP address, it also displays the information for the records. This option is available in the Grid Properties editor only.)*



Scavenging Leases

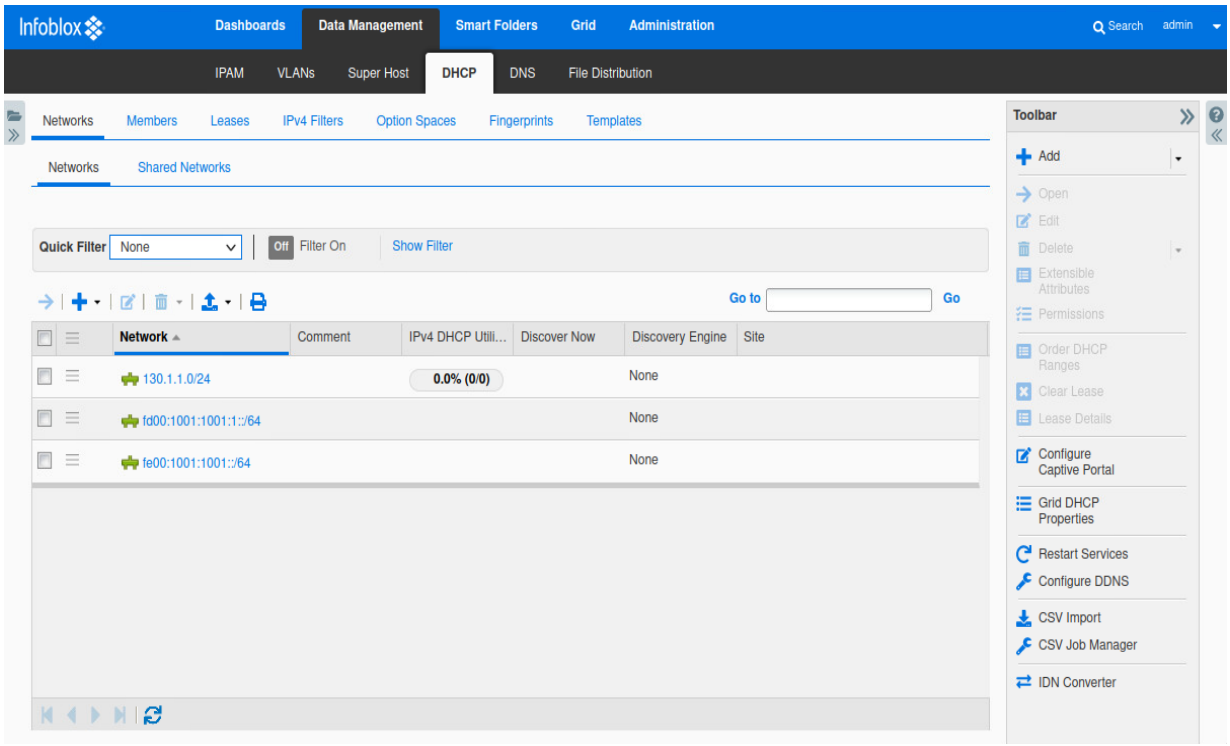
The accumulation of free and backup DHCPv4 leases; and free, expired, and released DHCPv6 leases results in unnecessary growth of database objects. The DHCP lease scavenging feature enables member DHCP servers to automatically delete free and backup IPv4 leases; and free, expired, and released IPv6 leases that remain in the database beyond the specified period of time, thus reducing the number of database objects.

When you enable this feature for DHCPv4 leases, the appliance permanently deletes the free and backup IPv4 leases, and you can no longer view or retrieve the lease information. This option can be enabled globally at the Grid level, and more specifically for a member, shared network, network, network container, DHCP range, network template, DHCP range template.

When you enable this feature for DHCPv6 leases, the appliance permanently deletes the free, expired, and released IPv6 leases, and you can no longer view or retrieve the lease information. This option can be enabled at the Grid level, and overridden at the member level.

The period of time that you specify is the duration after the expiration date of a lease, not its release date. For example,you specify a time period of 5 days when you enable this feature. If the lease time of an IP address is 10 days, but the lease is released after five days, the appliance still deletes the lease from the database after 15 days because the IP address has been leased.

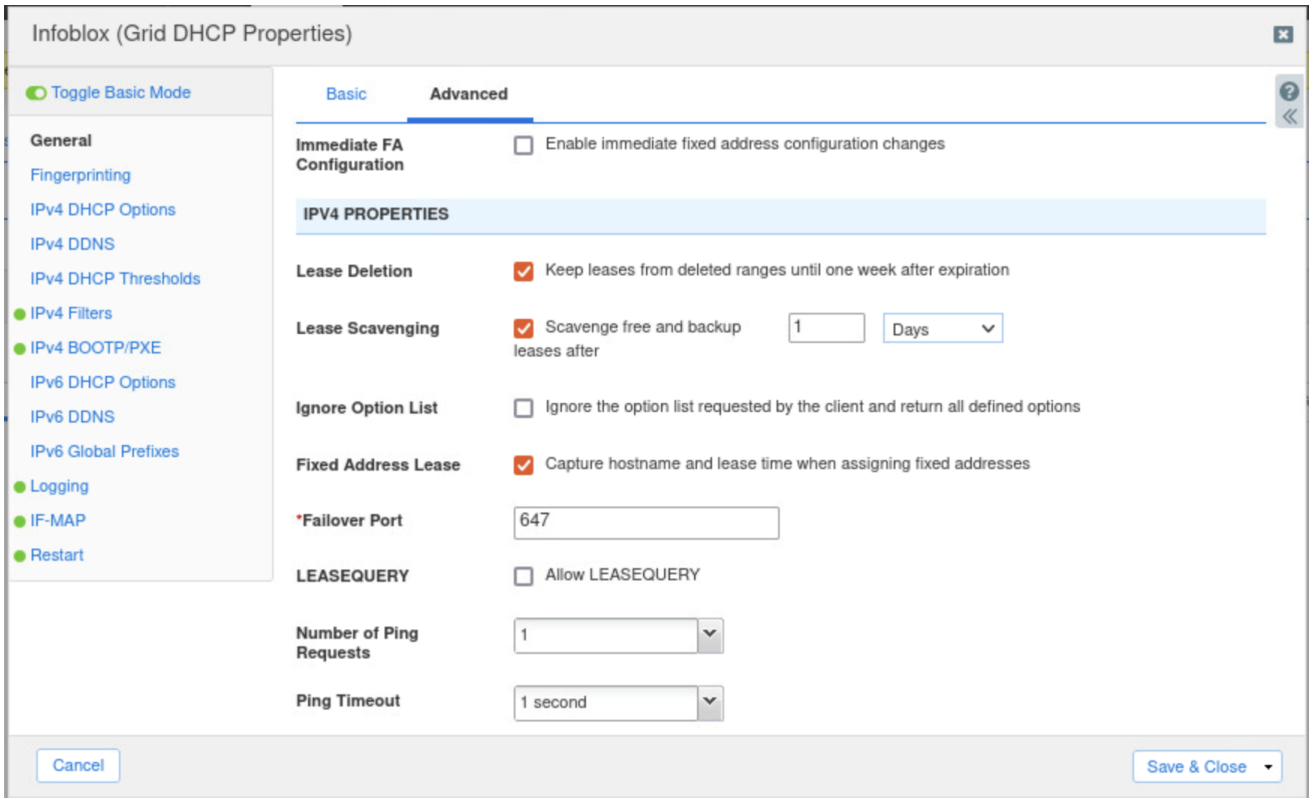
1. Navigate to **Data Management → DHCP**



2. In the toolbar, click **Grid DHCP Properties**.

3. Click **Advanced** on the General tab.

4. Select the checkbox for **Lease Scavenging**: This is disabled by default. Select the **Scavenge free, expired and released leases after check box** and specify the number of days, or weeks that free, expired, and released IPv6 leases remain in the database before they are automatically deleted. The minimum is one day and the maximum is 180 days. The default is one day. This can be set at the Grid and member level.



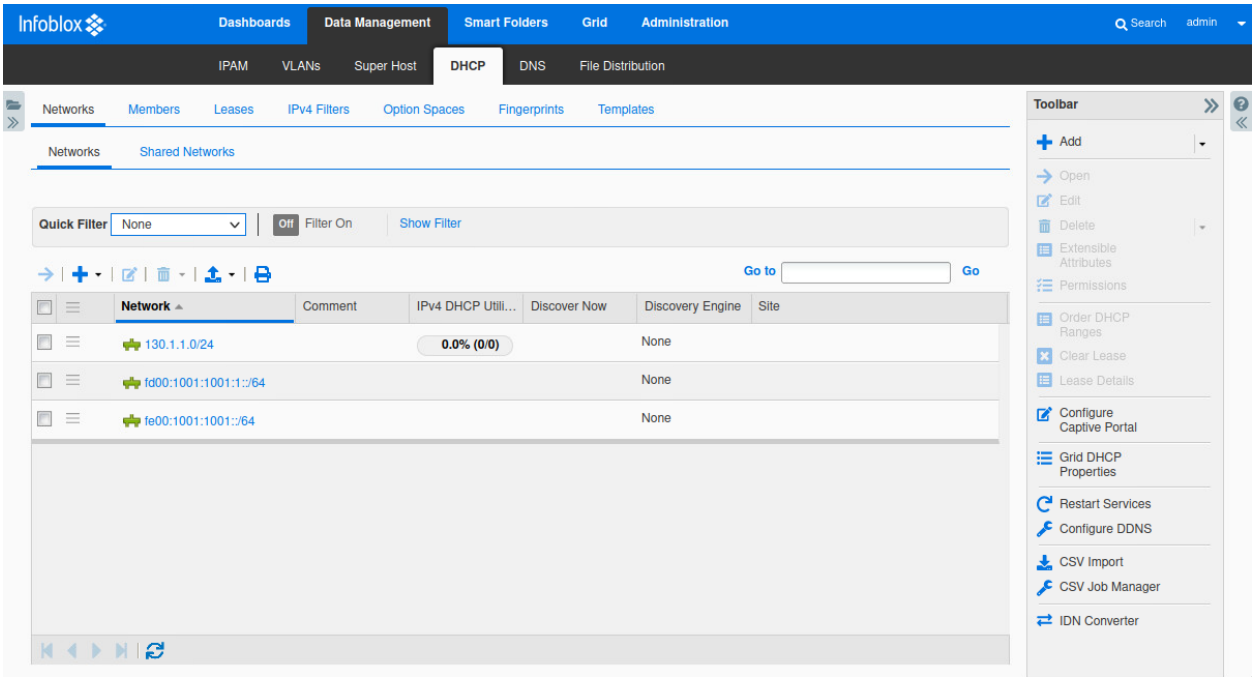
DHCPv6 Lease Affinity

DHCPv6 ranges are usually large and the DHCPv6 server randomly selects a new lease each time a client requests for a lease. The client can use the lease until it expires. After its expiration, the lease stays in the database with an expired state. These expired leases eventually lead to the increase in the number of database objects, because the probability of expired IPv6 leases getting reused is low.

Infoblox provides a DHCPv6 lease affinity feature that allows you to reuse expired IPv6 leases for DHCP clients. When you enable this feature, the DHCPv6 server automatically renews the expired leases. A DHCP client can retrieve the same lease from the DHCPv6 server after it expires and retains the same IP address. This feature helps reduce the amount of IPv6 leases in the database as the DHCP server issues the same lease multiple times for the same client.

The appliance ignores expired leases that are older than the specified period. Such leases are scavenged. Note that the grace period you define for lease scavenging is applicable for DHCPv6 lease affinity also. The minimum time period is six hours, maximum is 180 days and the default is set to seven days.

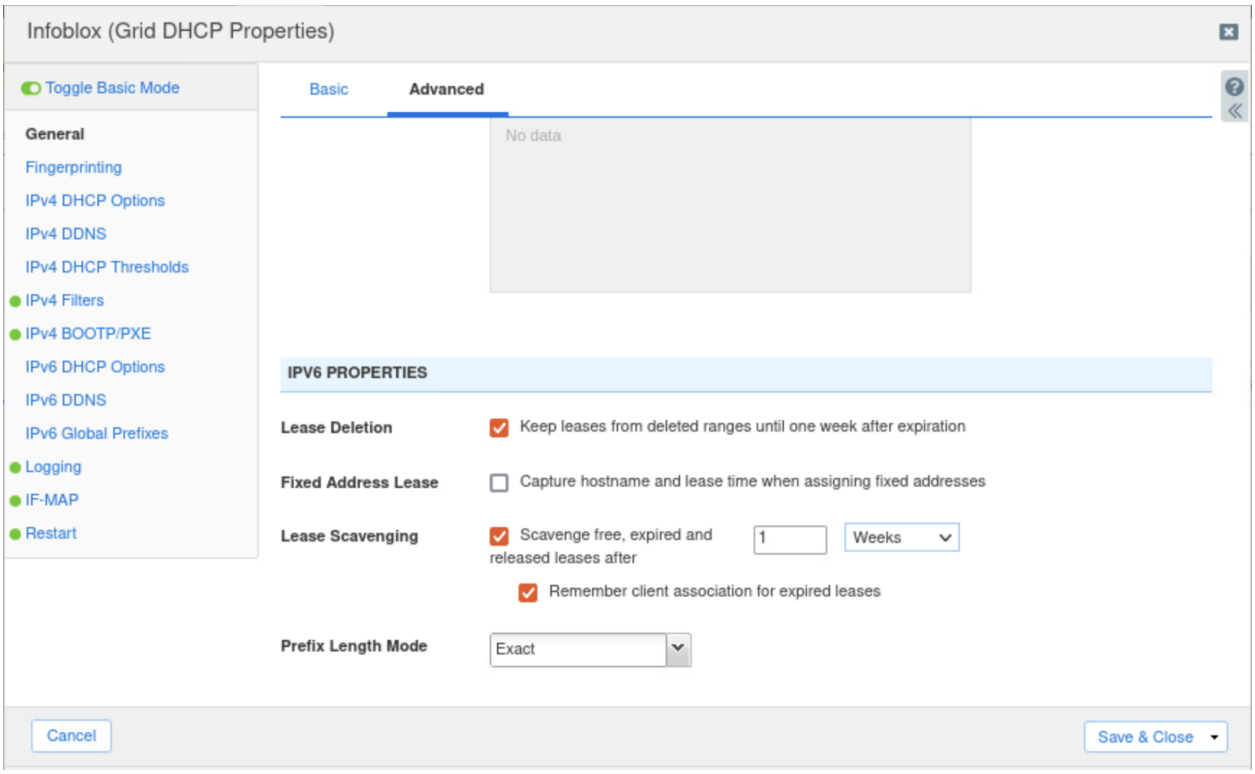
1. Navigate to **Data Management → DHCP**



2. In the toolbar, click **Grid DHCP Properties**.

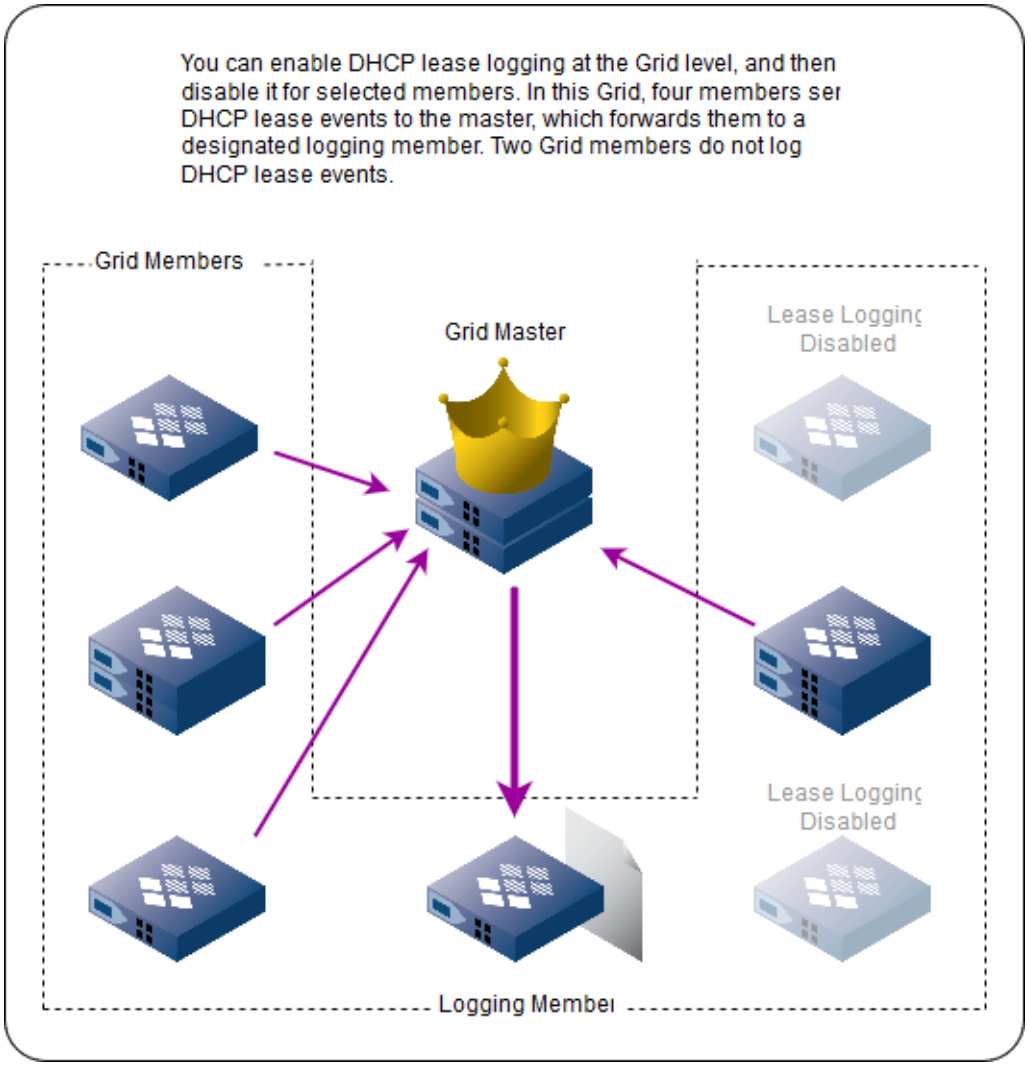
3. Click **Advanced** on the General tab.

4. Select the checkbox for **Remember client association for expired members**: This is disabled by default. Select the check box to remember and reuse expired IPv6 leases that are associated with DHCP clients. You can select this check box only when you select the Scavenge free, expired and released leases after the check box. This can be set at the Grid and member levels.

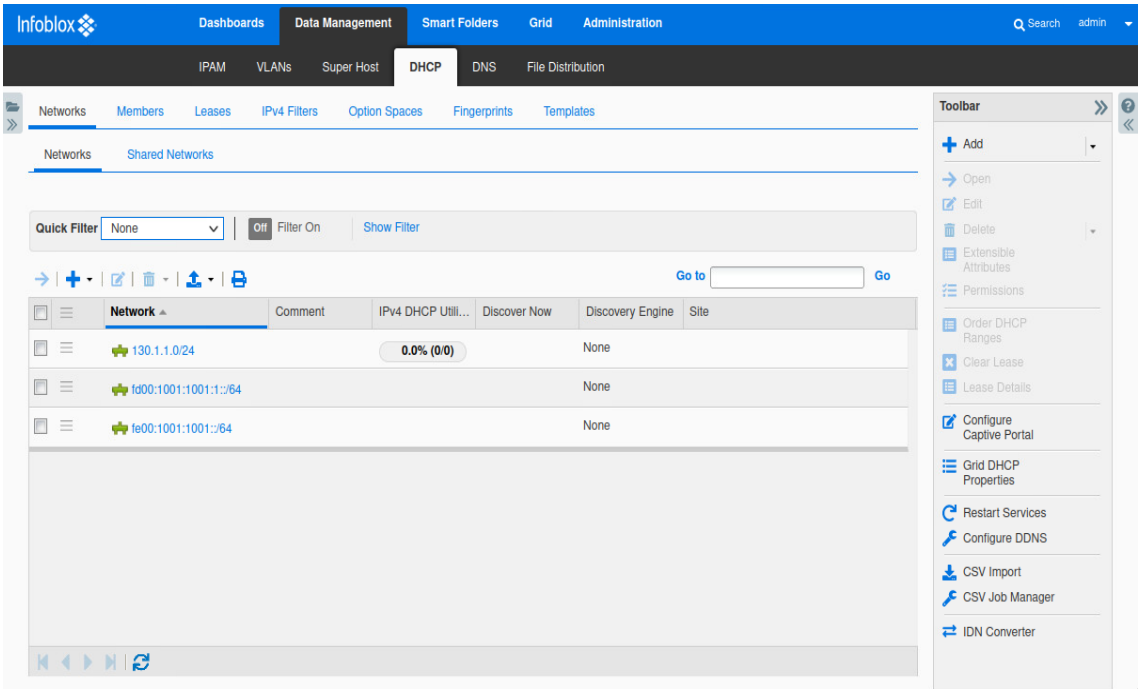


Configuring the Lease Logging Member

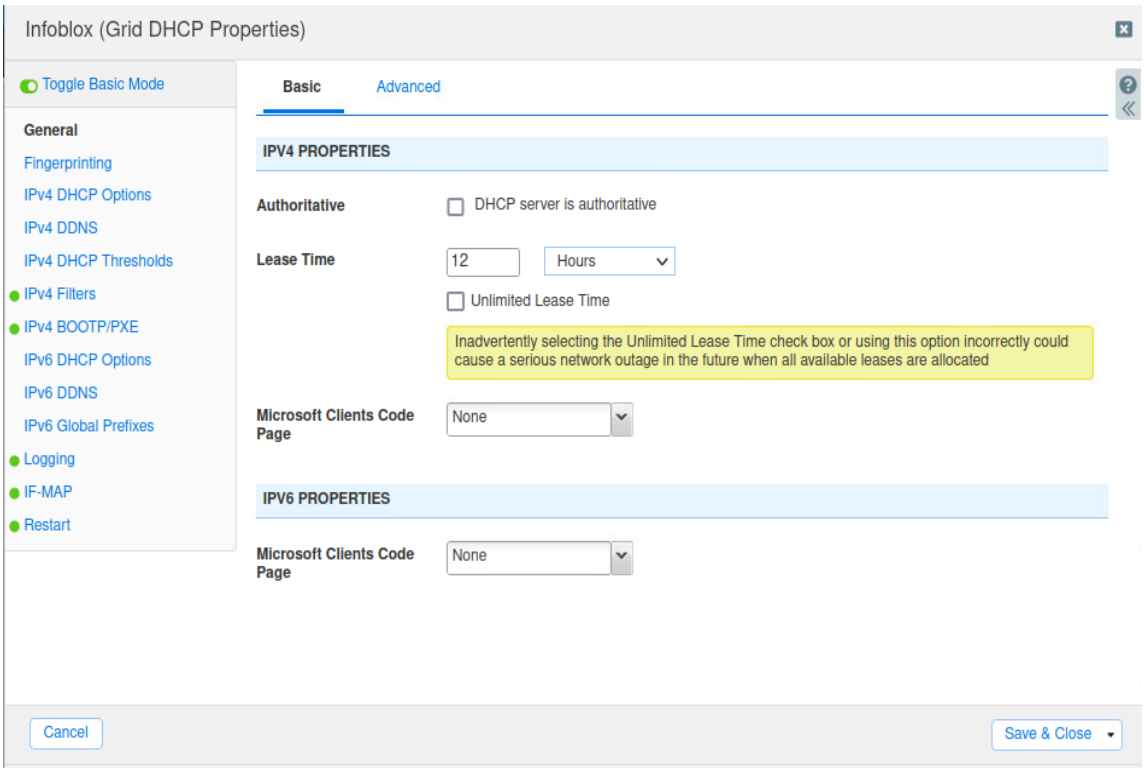
Logging DHCP lease events makes significant CPU demands, especially when there is heavy DHCP activity. Therefore, Infoblox strongly recommends that you designate a Grid member other than the master as a logging member whenever possible. Another way to manage the increased load that logging introduces is to log selectively per Grid member. For example, you might want to log DHCP leases for members serving critical parts of your network and not keep historical logs for members serving other parts.


You can enable DHCP lease logging at the Grid level, and then disable it for selected members. In this Grid, four members ser DHCP lease events to the master, which forwards them to a designated logging member. Two Grid members do not log DHCP lease events.
Grid Members
Grid Master
Lease Logging Disabled
Lease Logging Disabled
Logging Member

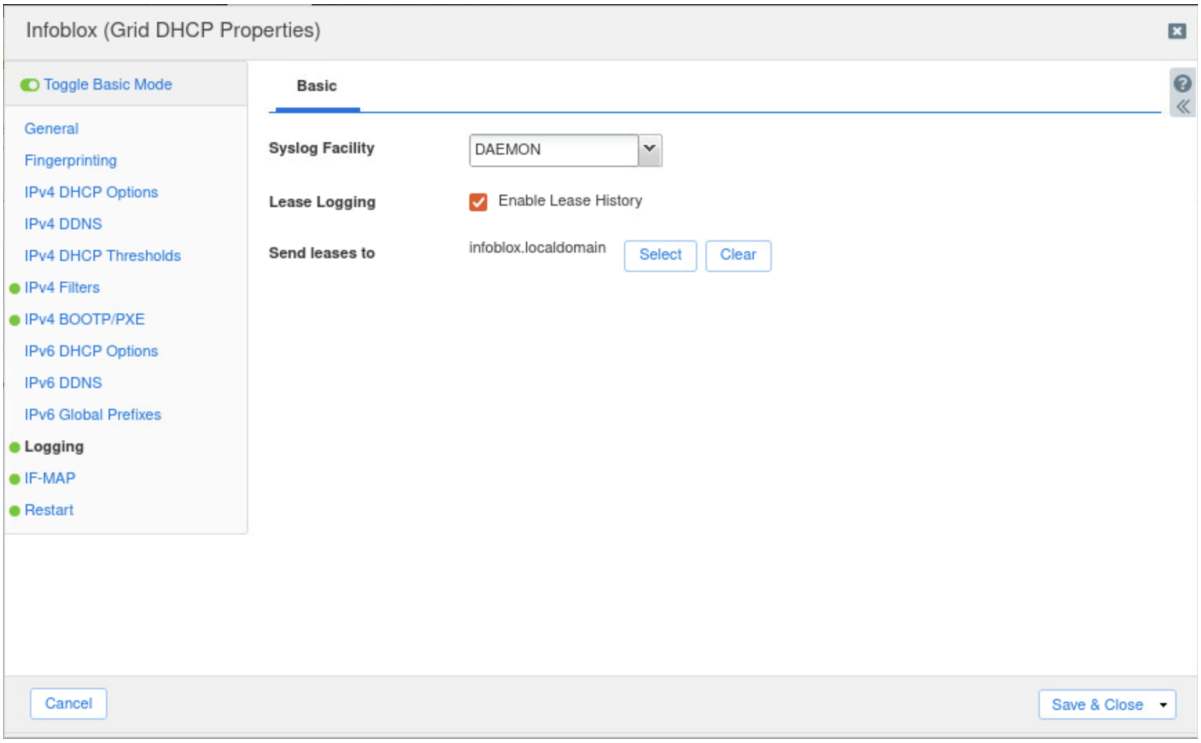
1. Navigate to **Data Management → DHCP**.



2. In the toolbar, click **Grid DHCP Properties**.



3. Click on the **Logging** Tab.



4. **Lease Logging**: Select **Enable Lease History** (for Grid) or Log Lease Events from DHCP Server (for member) to enable DHCP lease logging. To disable DHCP lease logging, clear the check box. You can set member overrides if you want to enable or disable lease logging per member.

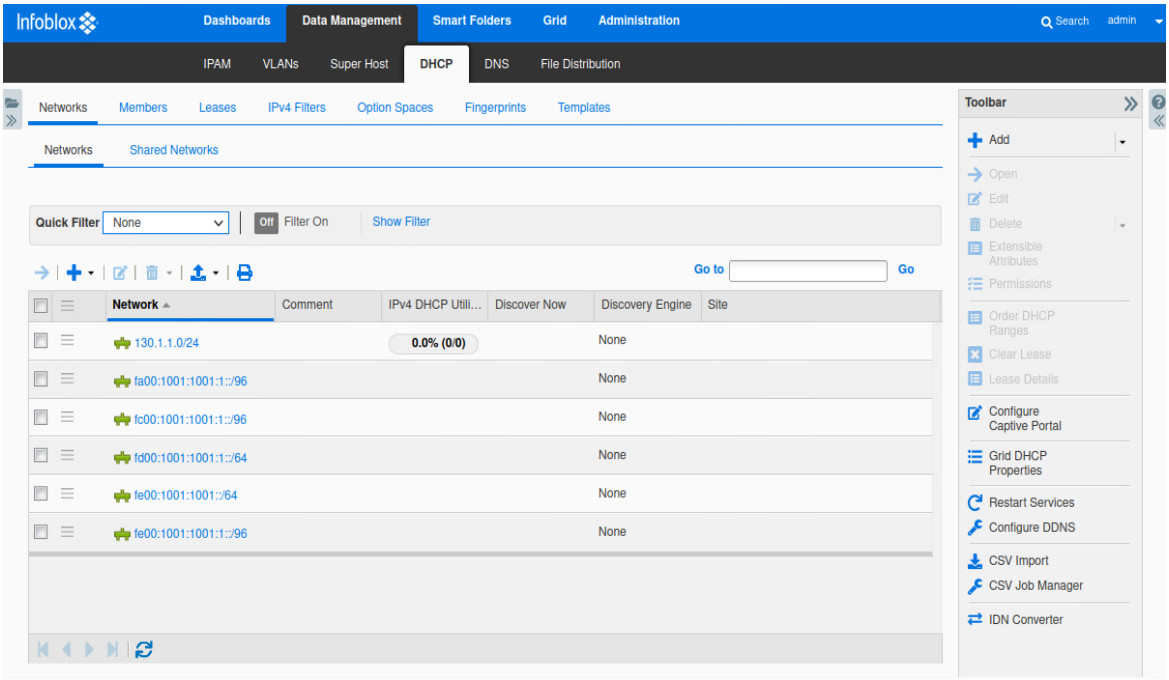
5. **Send leases to:** (For Grid only) Click **Select**. In the Select Member dialog box, select the Grid member on which you want to store the DHCP lease history log. Infoblox recommends that you dedicate a member other than the Grid Master as a logging member. If possible, use this member solely for storing the DHCP lease history log. If you do not select a member, no logging can occur. You can click **Clear** to remove the selected Grid member and select a new one.

Adding an IPv6 DHCP Network Range or IPv6 DHCP Scope

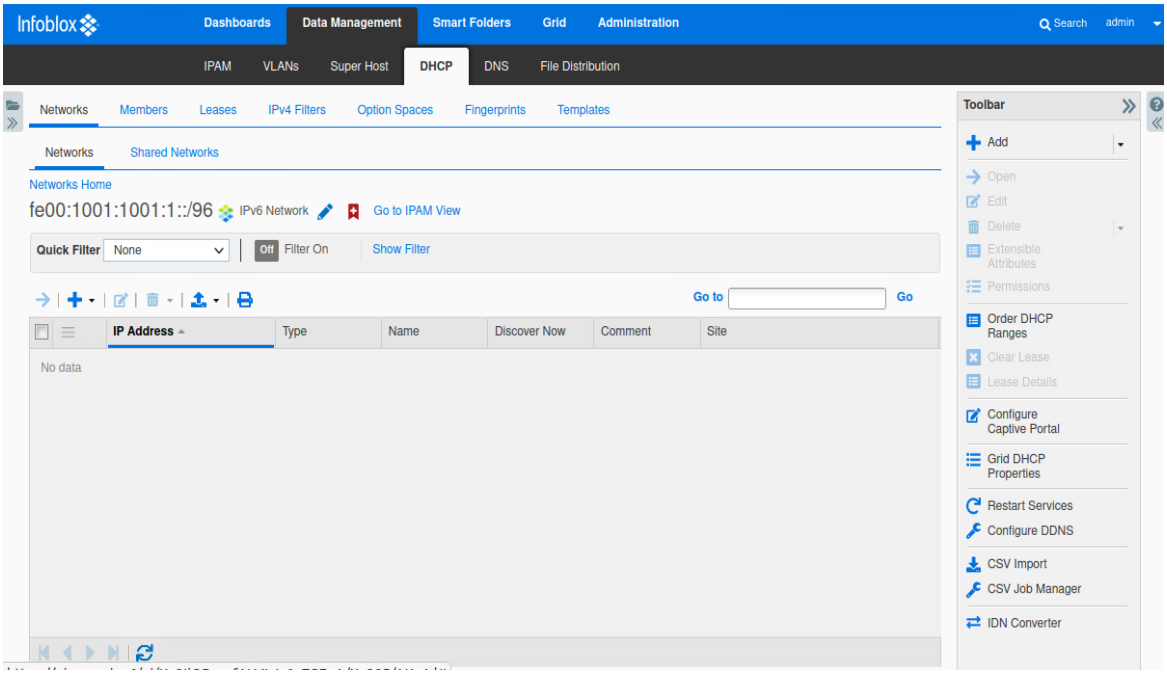
You can configure IPv6 ranges that are used to delegate IPv6 prefixes only, to assign IPv6 addresses only, or to delegate IPv6 prefixes and assign IP v6 addresses. When you define a DHCP range to delegate prefixes, the prefixes can be outside of the network where they are being defined. IPv6 ranges inherit their properties from their network, so each range in a subnet provides the same set of options to their DHCP clients.

When the server grants IPv6 leases, it uses an algorithm based on the DUID of the client.

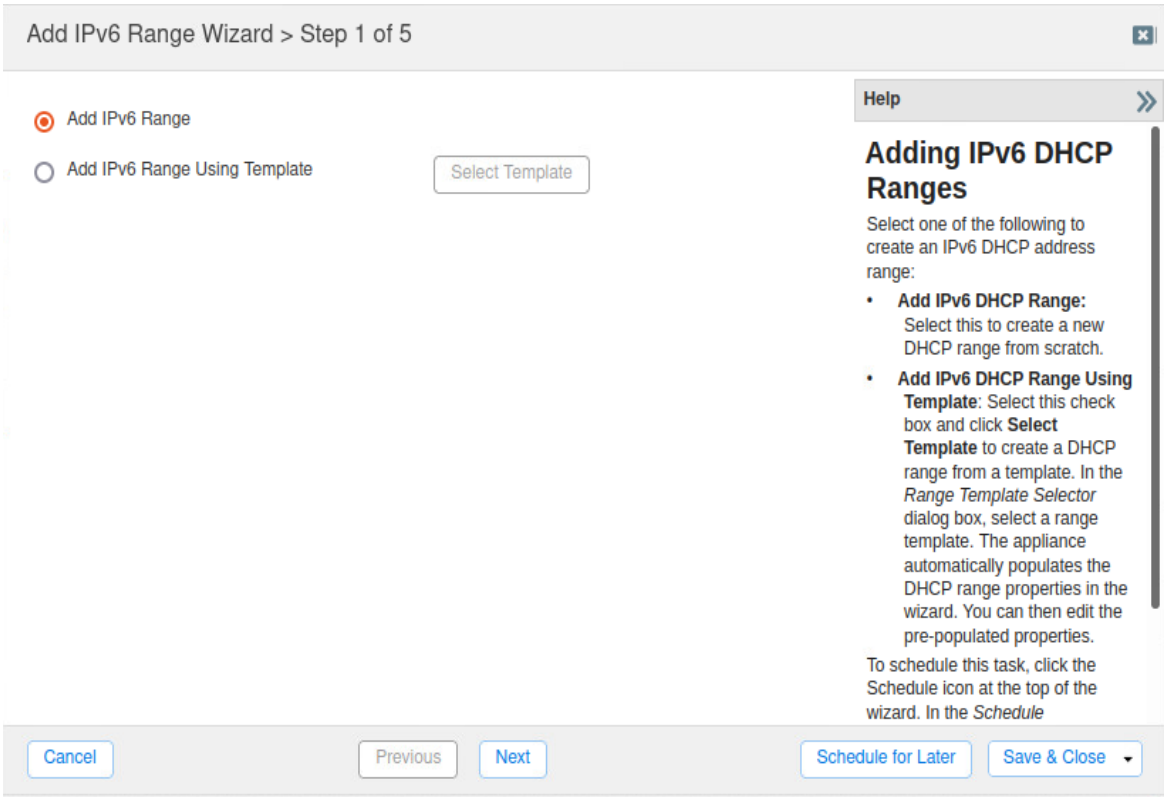
1. Navigate to **Data Management → DHCP→ Networks**



2. Click on the network that you want to add a network range

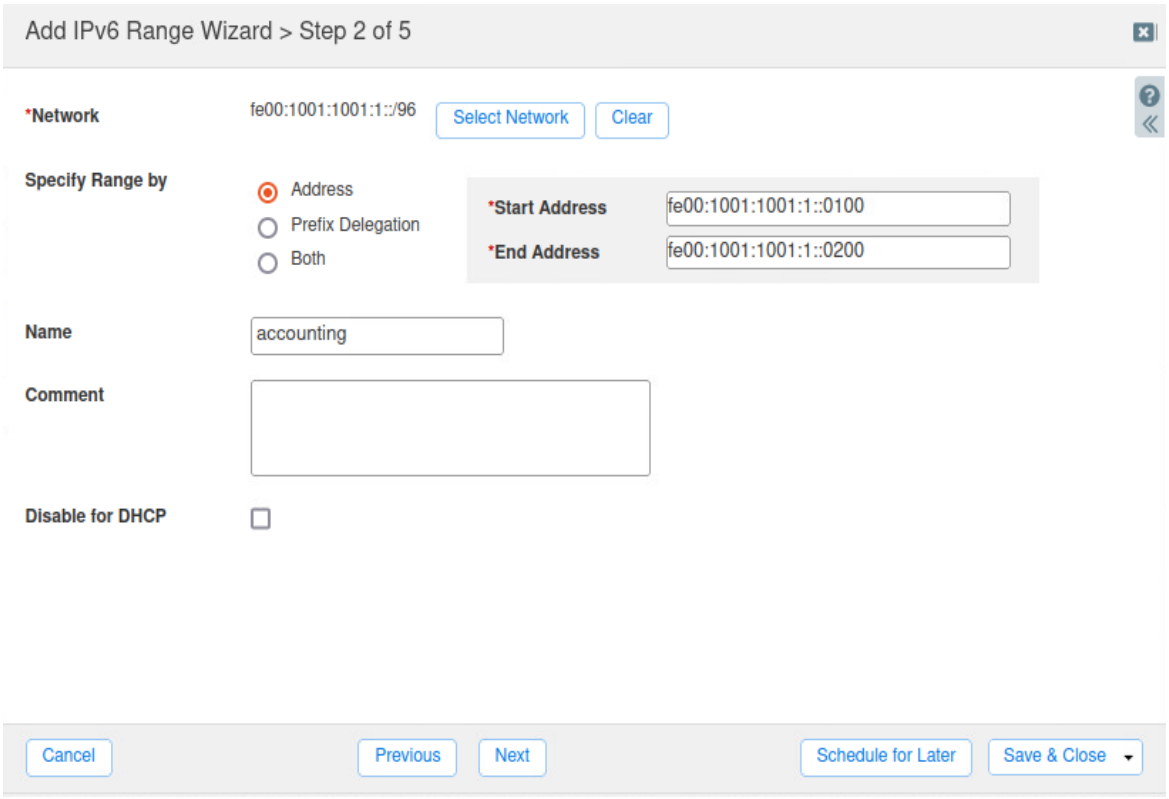


3. Click on the '+' to enter the IPv6 range wizard. Click **Next**.



4. Enter a **Start Address** and **Ending Address**.

5. Click **Next**.



6. Add the member that will be serving IPv6 DHCP.

7. Click **Save and Close**.

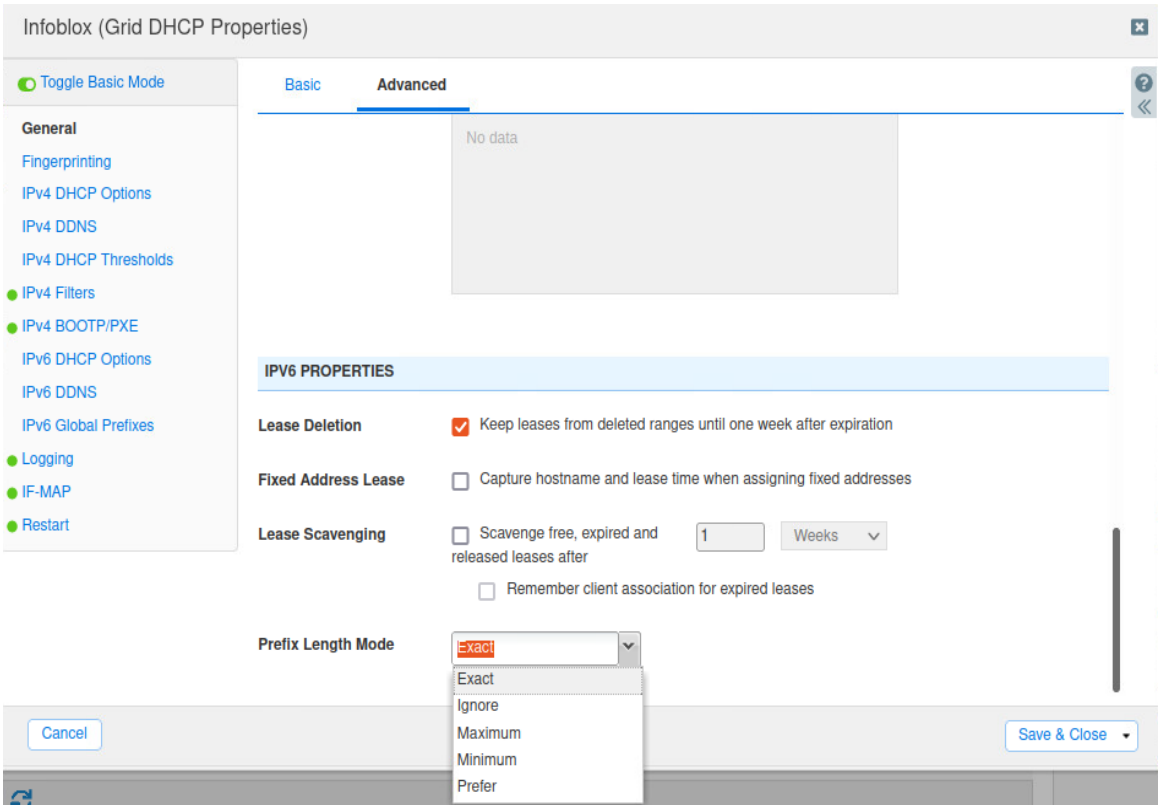
Setting the Prefix Length Mode for DHCPv6

The prefix length mode determines the prefix selection rules employed by the DHCPv6 server when a DHCPv6 client sends an empty prefix with just a prefix length as a hint for the server to specify the required prefix length. This determines the prefix that gets allocated to the DHCPv6 client.

1. Navigate to **Data Management → DHCP.**

2. In the toolbar, click on **Grid DHCP Properties**.

3. Click on **Advanced** in the General tab and scroll to the bottom.



- **Exact**: The DHCP server looks for a prefix with exactly the same length as the length requested by the client. If it cannot find a prefix that has the exact same length as the length requested, the server returns a status indicating that no prefixes are available. If you do not configure the prefix length mode, Exact is the default value.

- **Ignore**: The DHCP server ignores the length requested by the client and offers the first available prefix.

- **Prefer**: The DHCP server looks for prefixes that have the same length as the length requested by the client. If it does not find a prefix of the same length, it offers the first available prefix of any length.

- **Minimum**: The DHCP server looks for a prefix that has the same length as the requested length. If it does not find such a prefix, it returns a prefix whose length is greater than (that is, longer than) the requested value. If it does not even find a prefix of a greater length, it returns a status indicating that no prefixes are available. For example, if the client requests a prefix length of /60, and the DHCP server has prefixes of lengths /56 and /64 available, it offers a prefix of length /64.

- **Maximum**: The DHCP server looks for a prefix that has the same length as the requested length. If it does not find such a prefix, it returns a prefix whose length is less than (that is, shorter than) the requested value. If it does not even find a prefix of a shorter length, it returns a status indicating

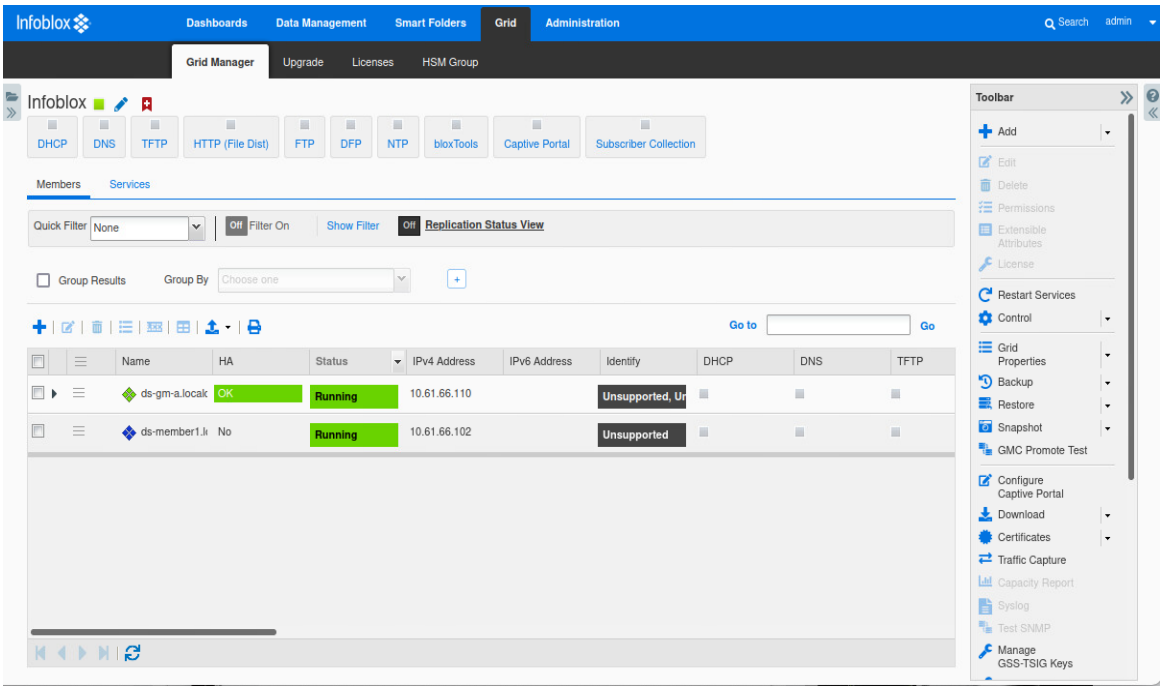
that no prefixes are available. For example, if the client requests a length of /60, and the server has prefixes of lengths /56 and /64 available, it offers a prefix of length /56.

Dual Stack Grid

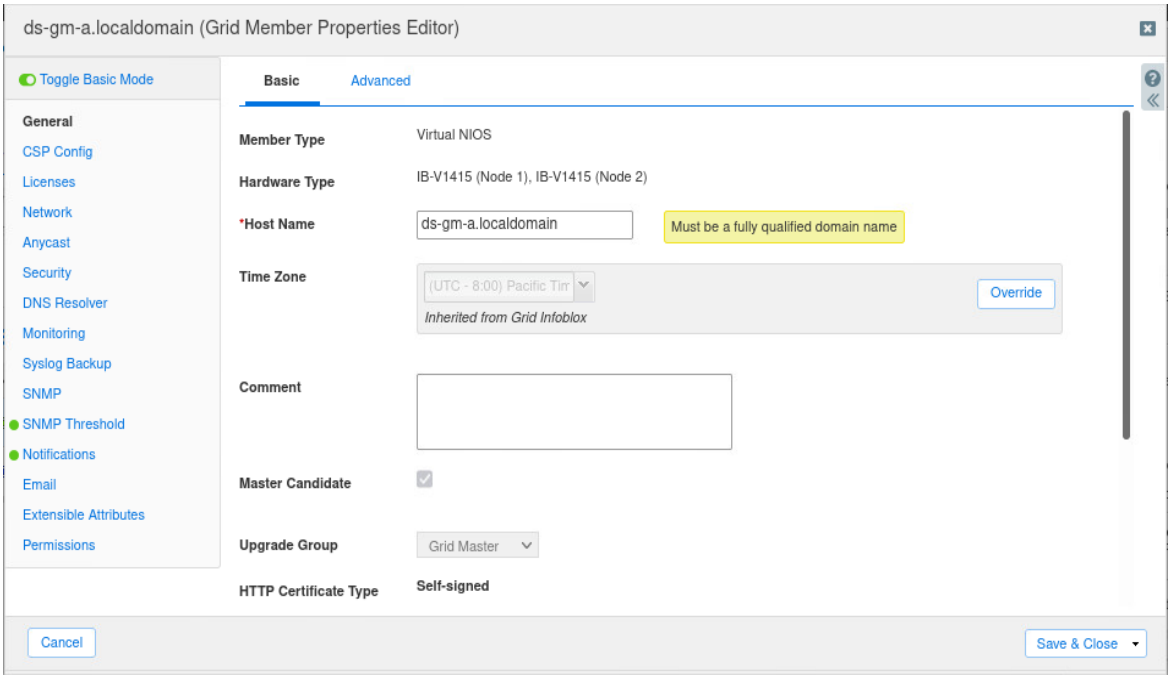
The following instructions show how to add IPv6 addresses and dual stack features to an existing IPv4 grid. In this example, you will see the settings that need to be made to support IPv6.

Incorporating IPv6 in a High Availability Environment

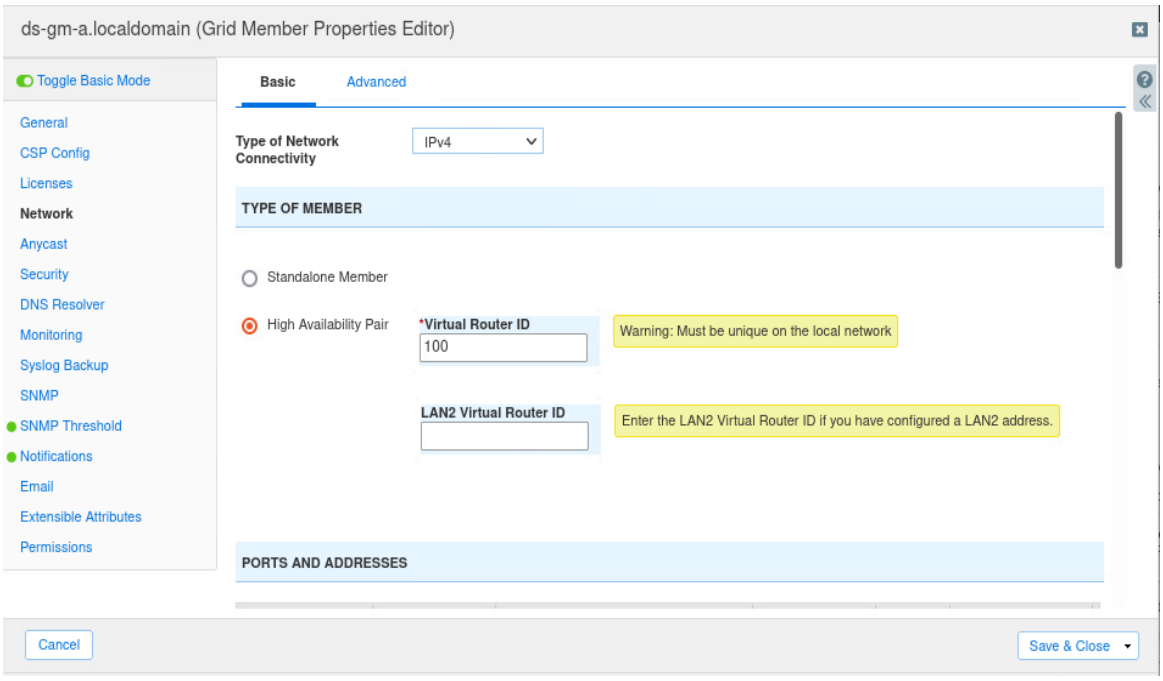
1. Navigate to **Grid → Grid Manager**.



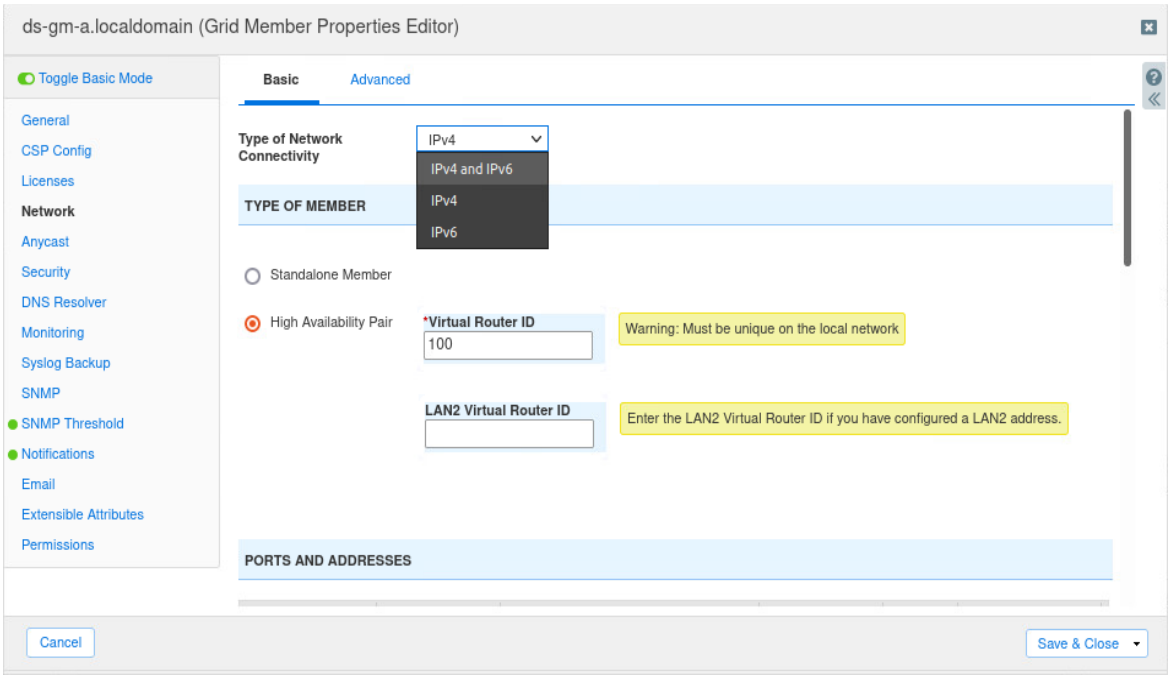
2. Click on the **hamburger** icon for the grid master and select **Edit**.



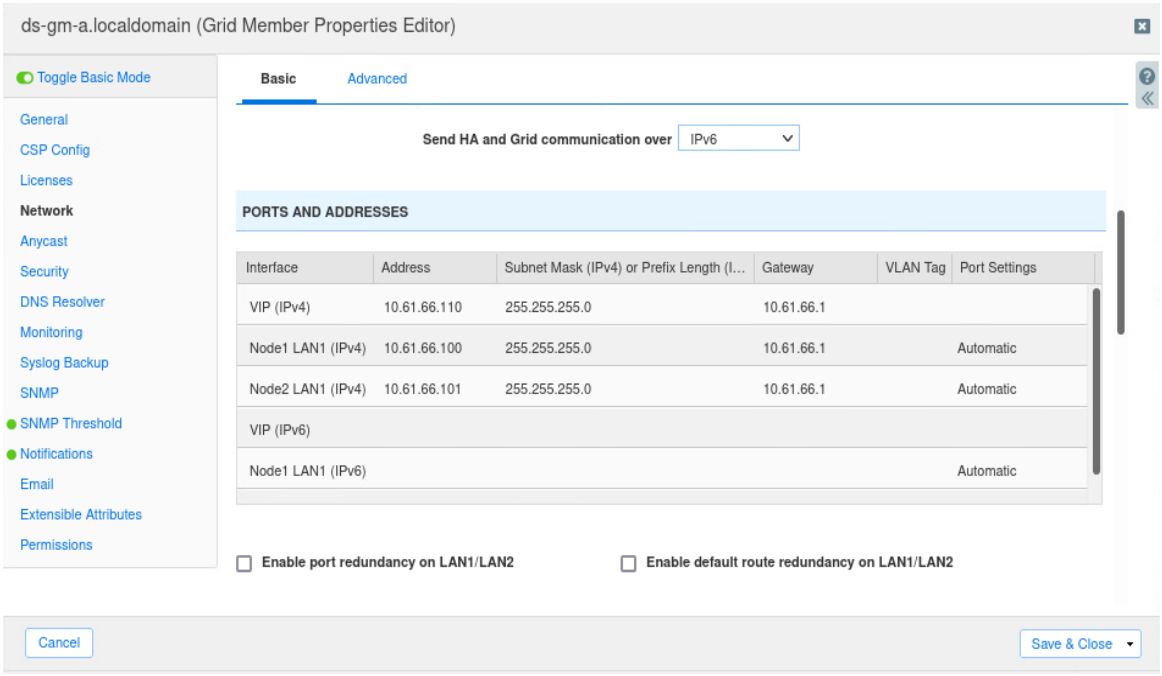
3. Click on the **Network** tab.



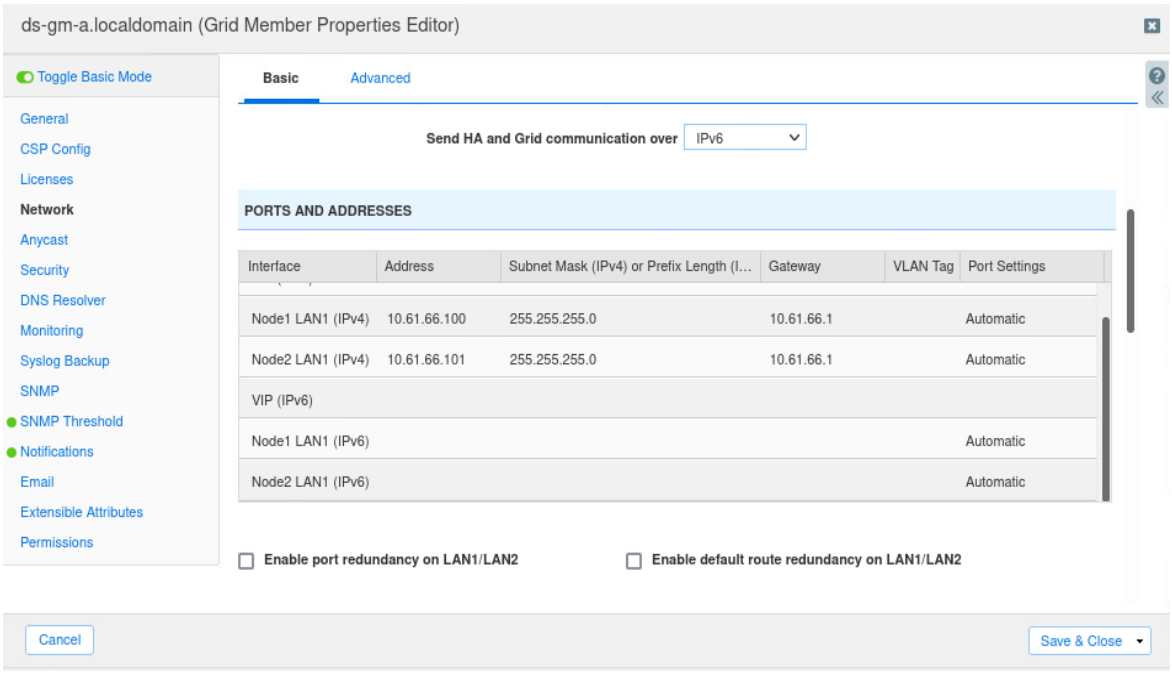
4. Change the **Type of Network Connectivity** to IPv4 and IPv6.



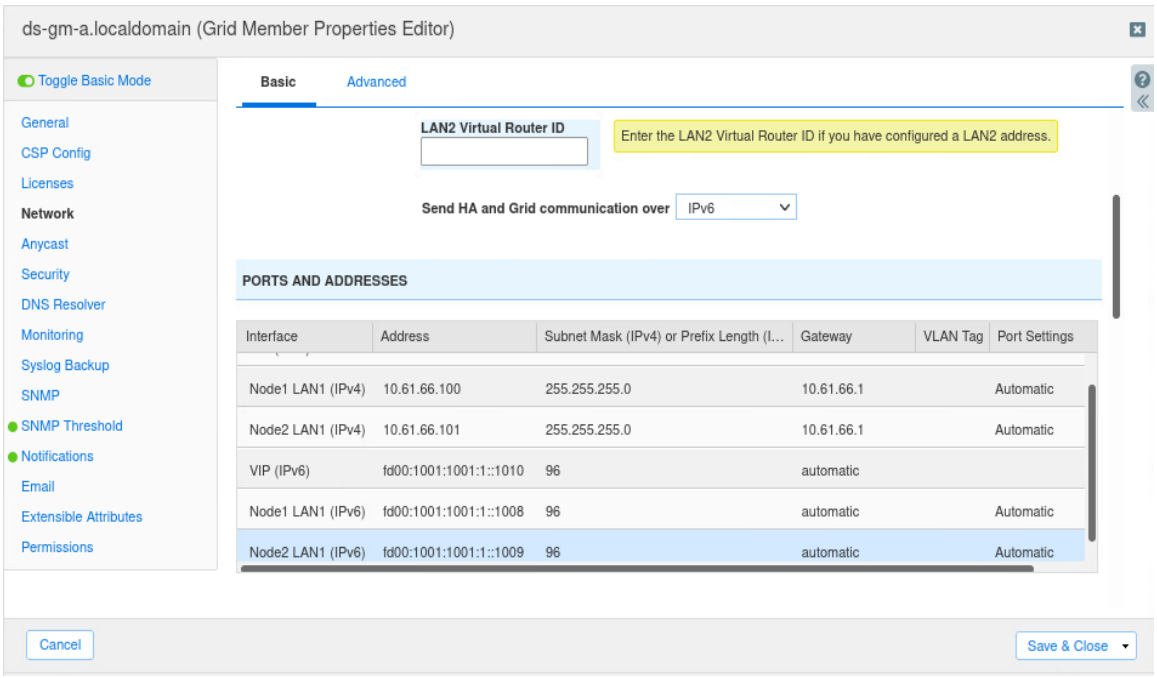
5. Scroll down the screen and select IPv6 for **Send HA and Grid communication over** IPv6.



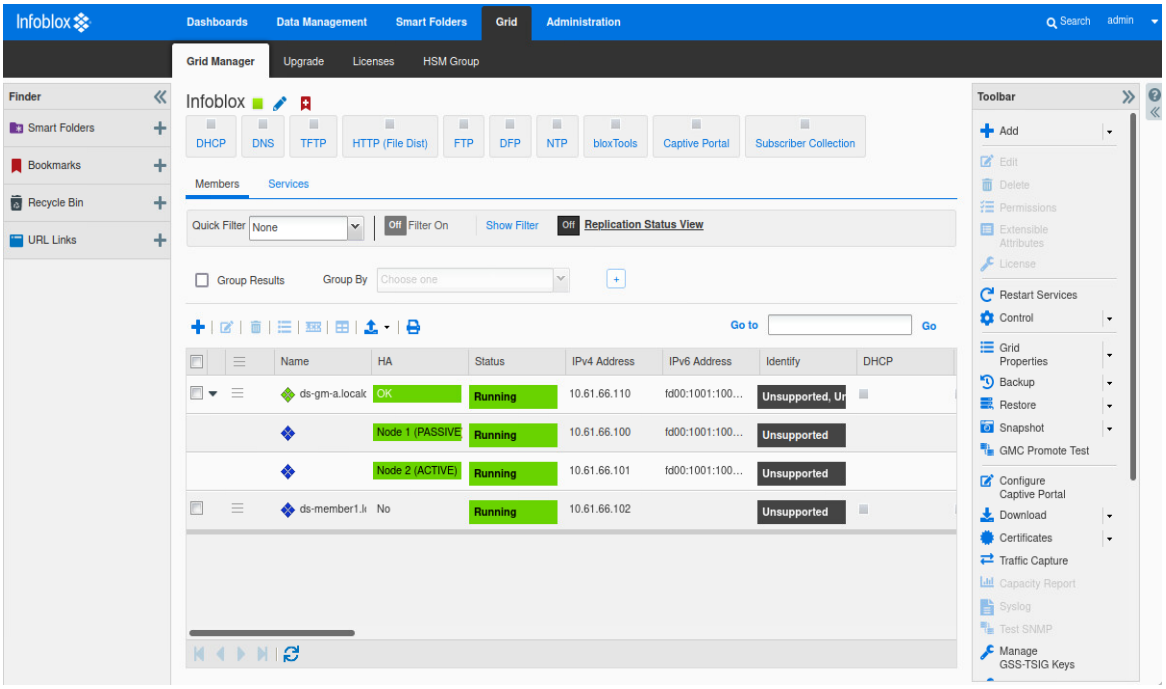
6. Scroll down the Ports and Addresses screen until VIP, Node1 LAN1, and Node2 LAN1 are shown.



7. Input the IPv6 addresses for VIP, Node1 LAN1, and Node2, LAN1. Node1 LAN1 is for the active node and Node2 LAN1 is for the passive node.



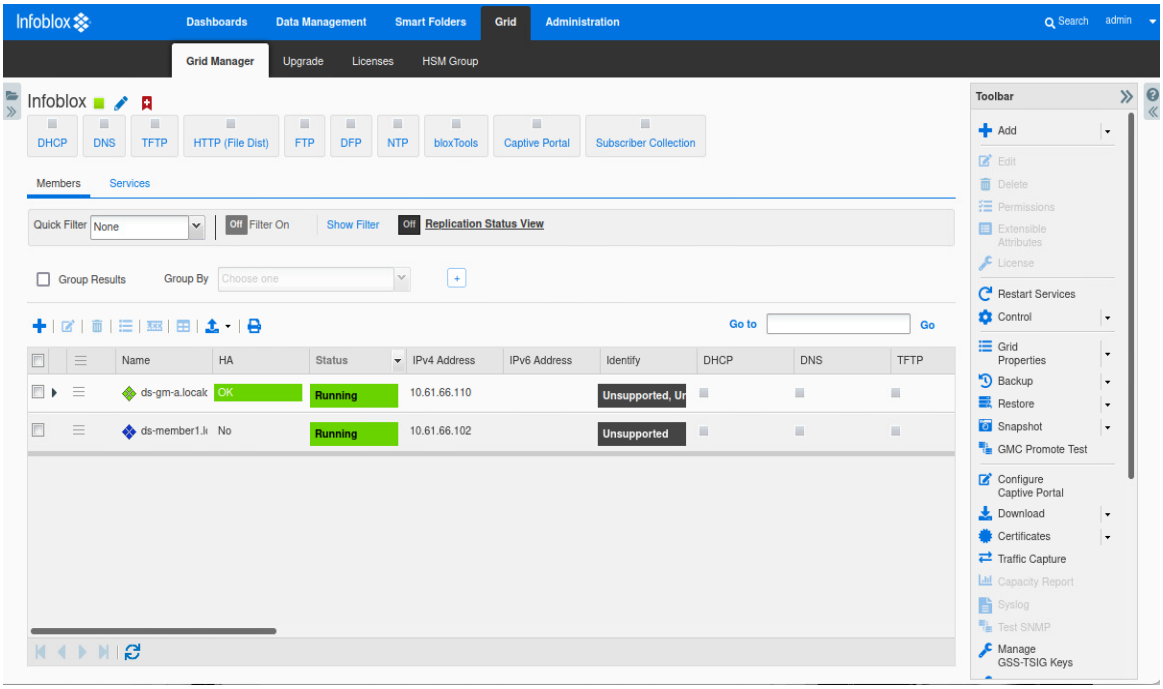
8. Click **Save and Close**. The HA pairs will now reboot to update the IPv6 address settings. This is what you should see on the Grid Manager screen.



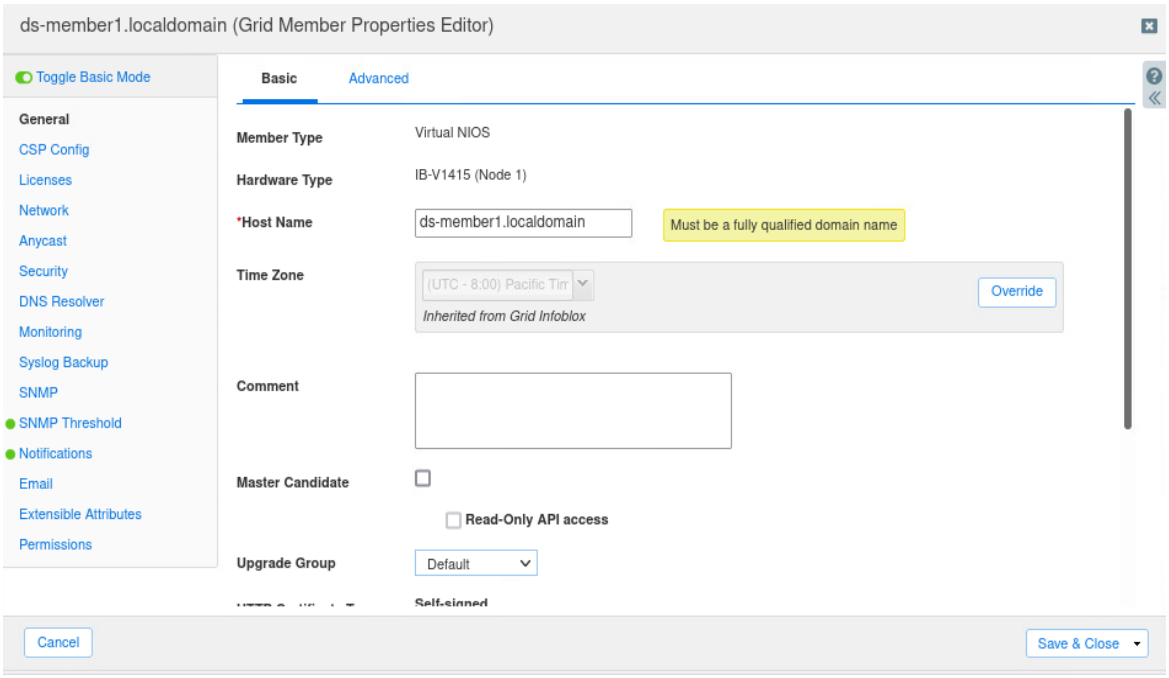
9. Repeat these tasks to convert your HA pairs to IPv6.

Converting Individual Members to IPv6

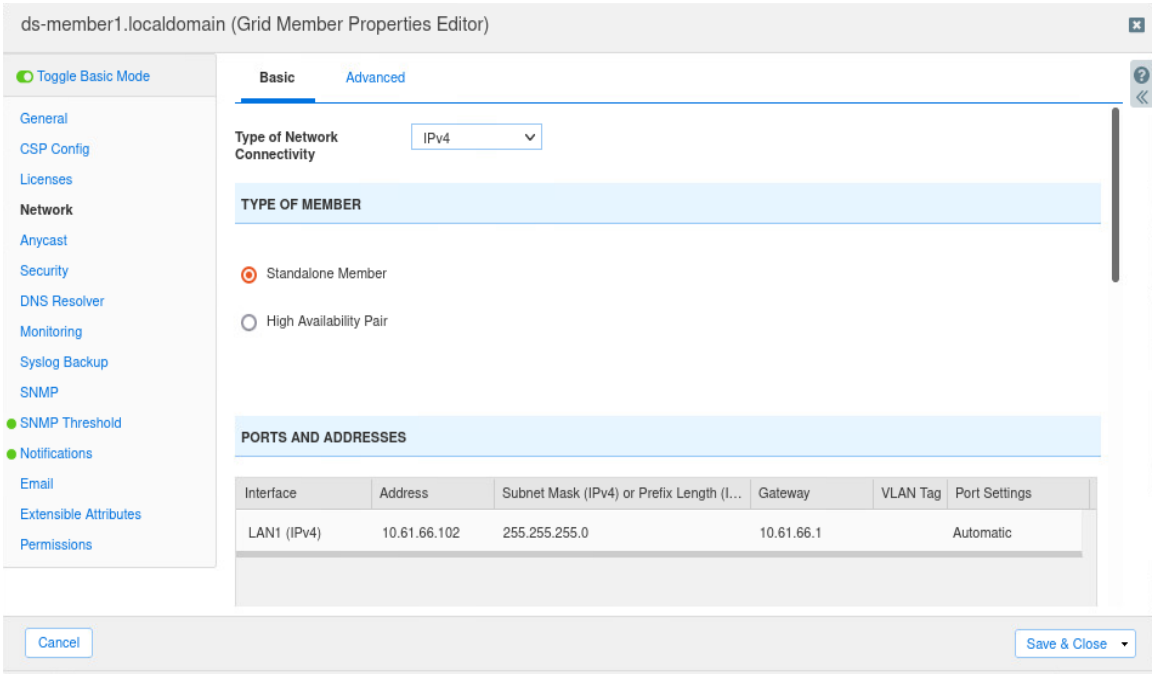
1. Navigate to **Data Management** → **Grid**.



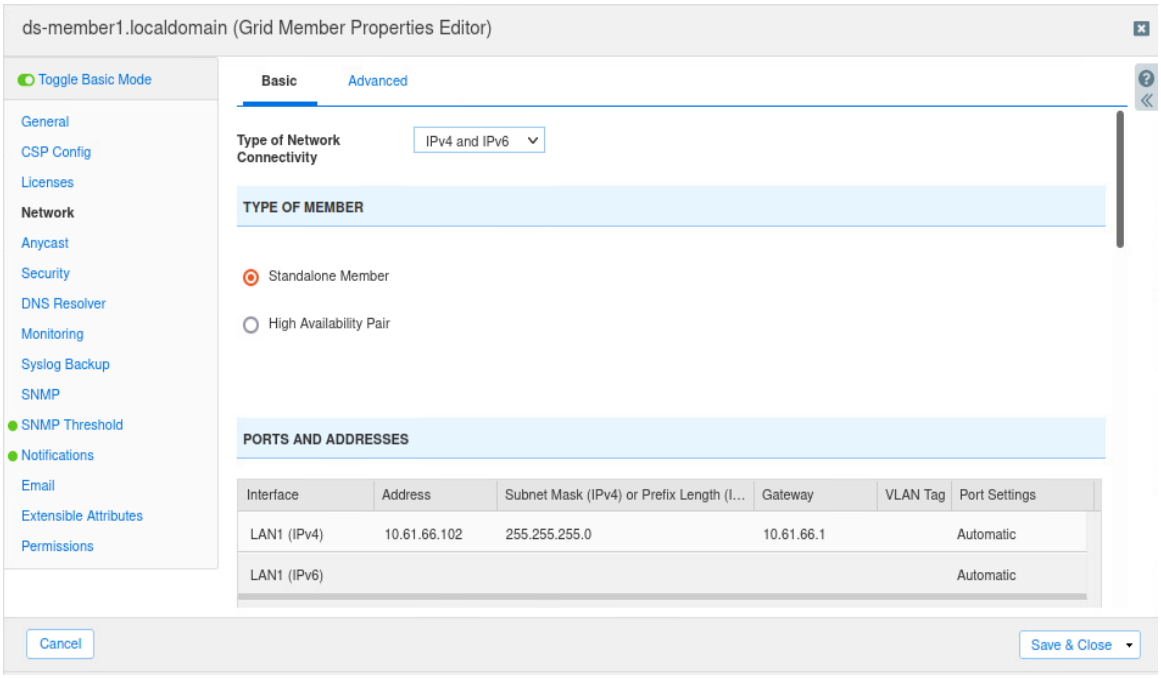
2. **Edit** the second member.



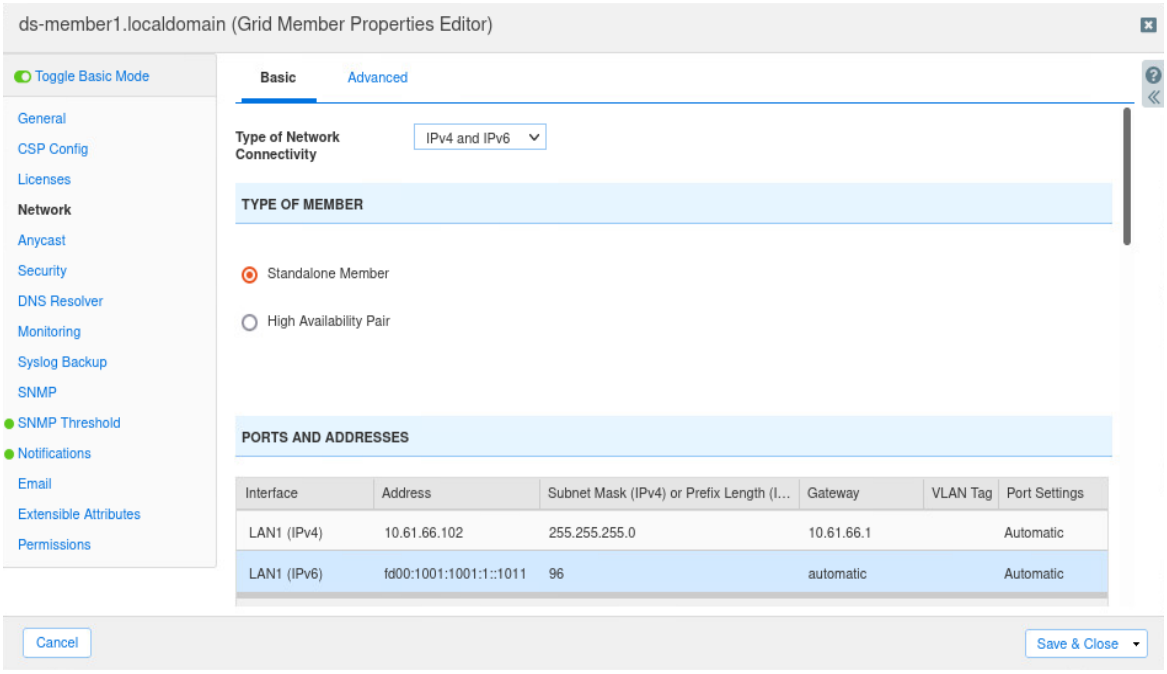
3. Click on the **Network** tab.



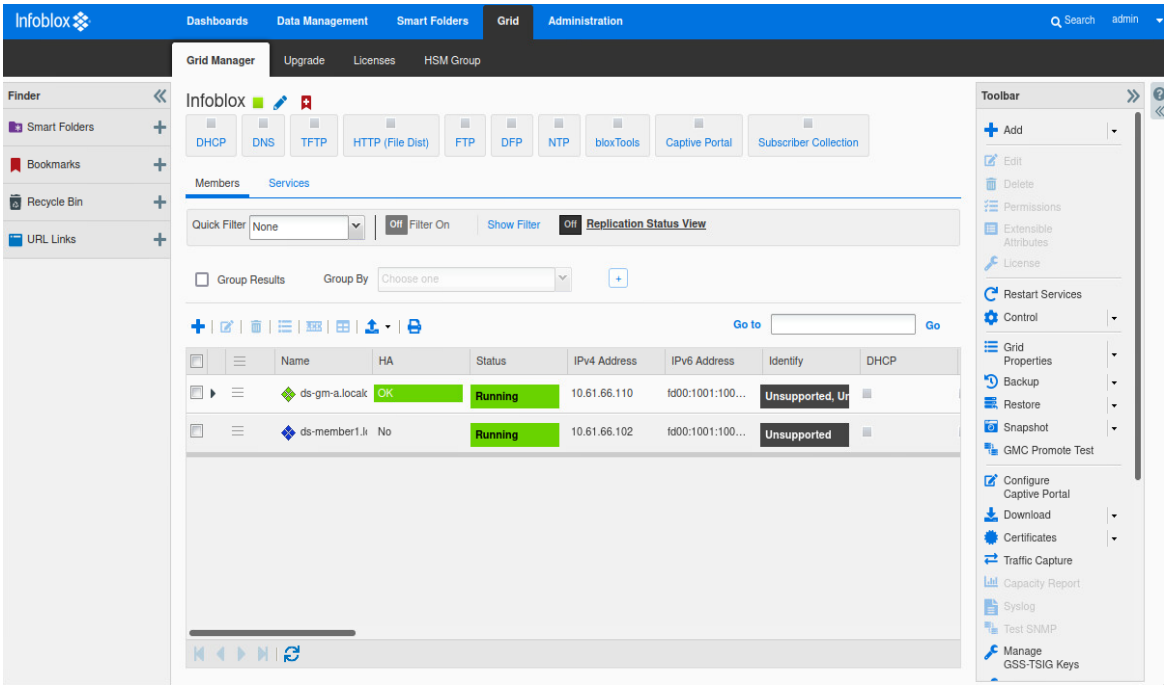
4. Change the **Type of Network Connectivity** to IPv4 and IPv6.



5. Input the IPv6 address in the **Ports** and **Addresses** section.

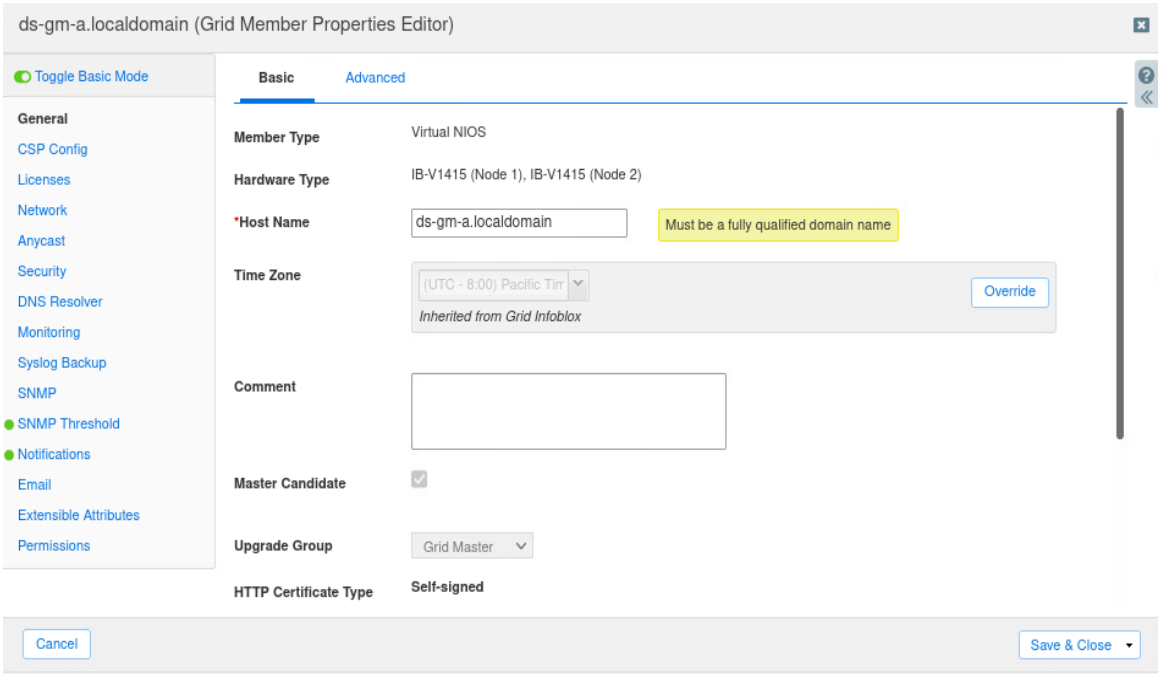


6. Click **Save and Close**. The member will reboot and rejoin the grid.

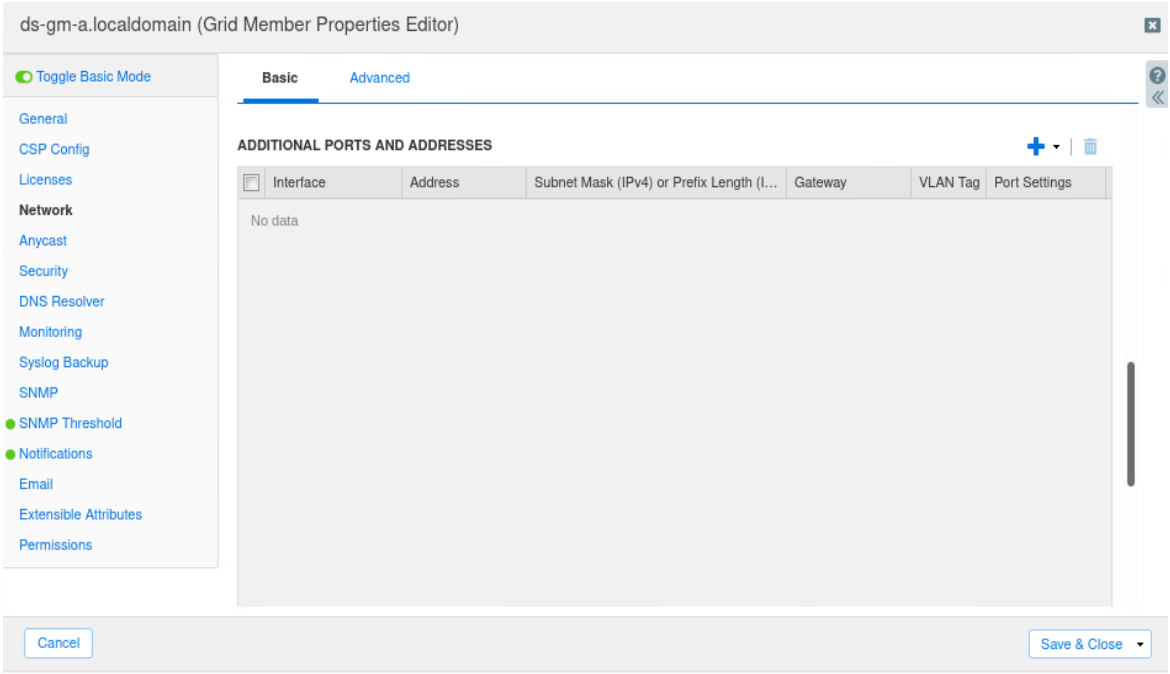


Anycast Configuration

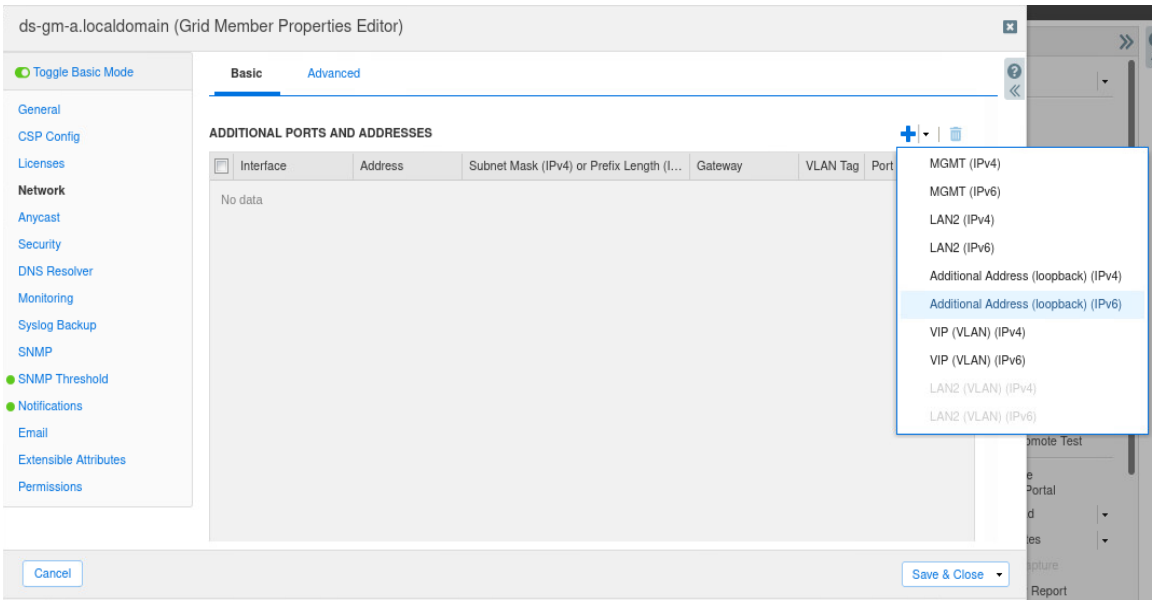
1. Navigate to the **Data Management** → **Grid Manager** → **Members** and edit a member.



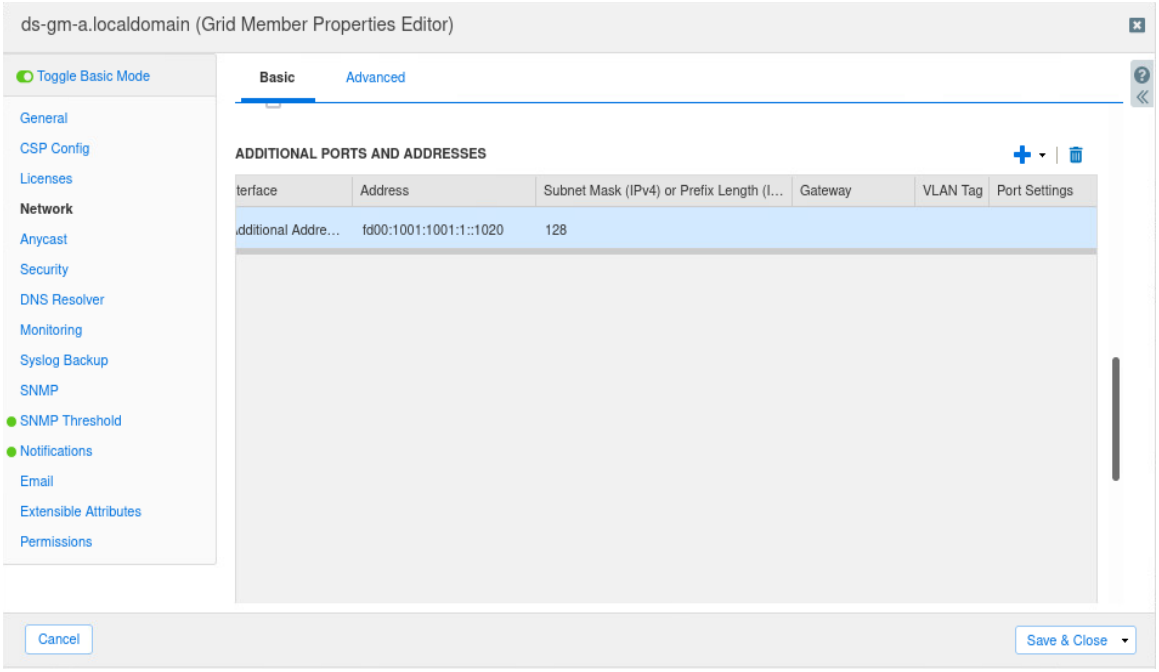
2. Select the **Network** tab and scroll down to **Additional Port and Addresses**.



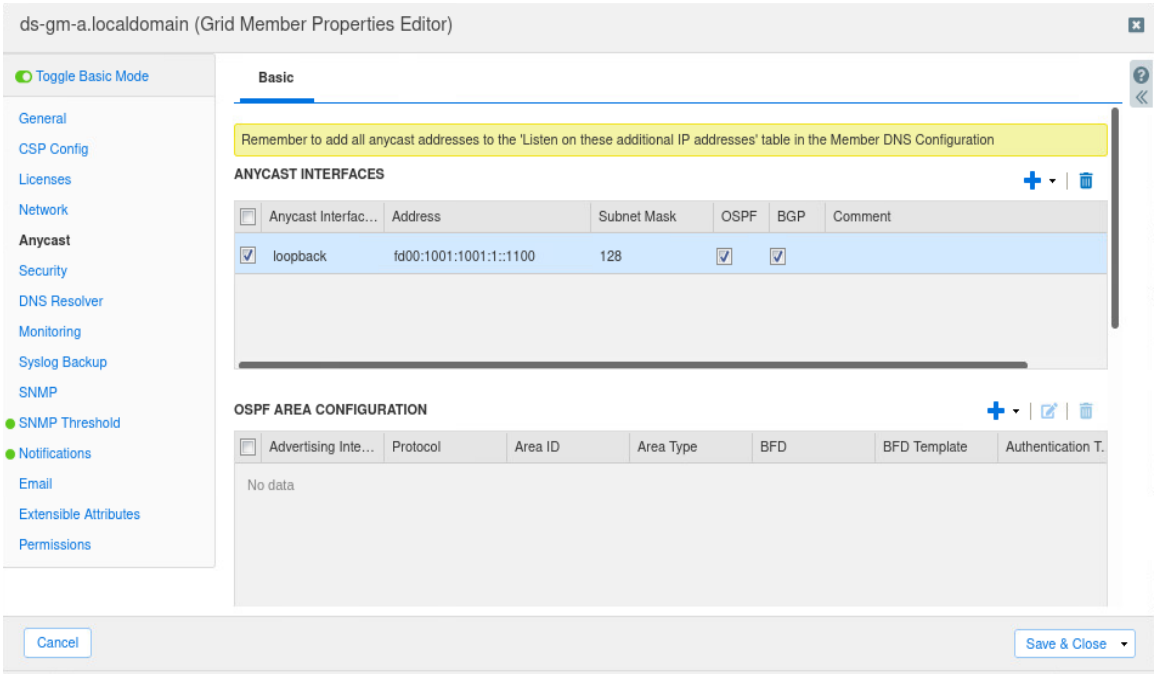
3. Click on the '+' button to add an IPv6 loopback address.



4. Enter an IPv6 address. Click **Save and Close**. The member will reboot to activate the loopback address.

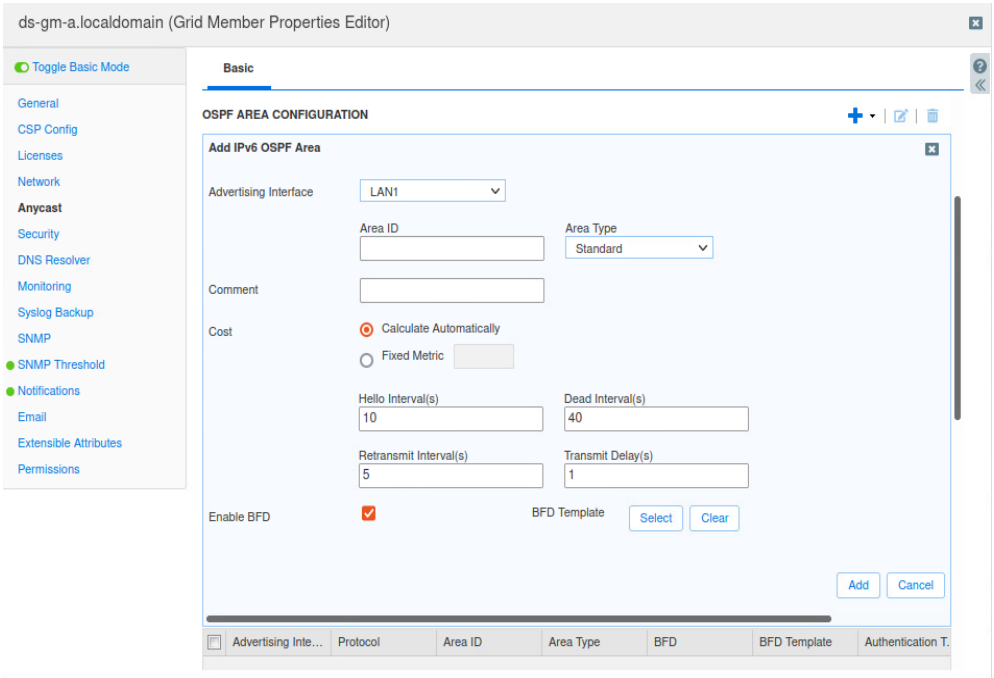


5. Open the Grid Member properties again and click on the **Anycast** tab and click on '+' button to add an IPv6 address. You may add the IPv6 address and select either BGP and/or OSPF.

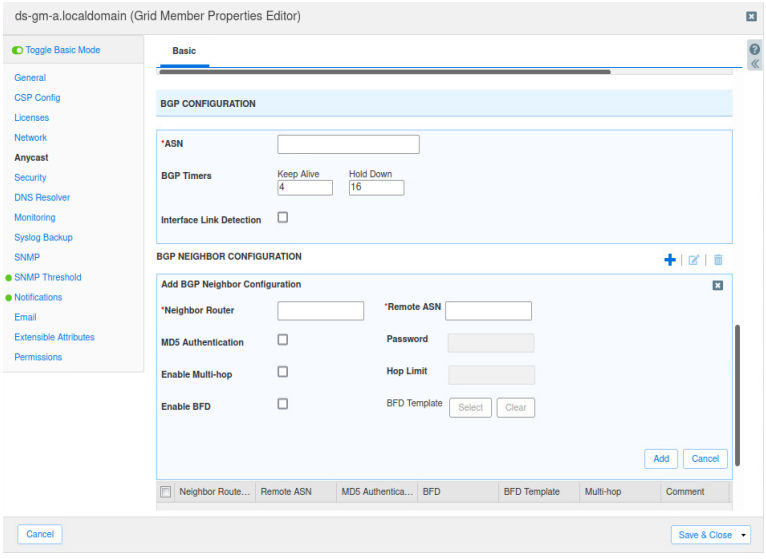


6. Scroll down to the OSPF Area Configuration and click on the '+' button to add an OSPF IPv6 configuration. Select the advertising interface, Area ID, Cost, Hello Intervals, Dead Intervals, Retransmit Interval, and Transmit Delay. You can choose to enable BFD (bidirectional forward

detection). BFD protocol is designed to provide faster failure detection using millisecond timer intervals. BFD templates are used to define the authentication type, key ID, password, and intervals. Refer to the NIOS Administration Guide for steps to create the BFD templates. Click on the **Add** button.



7. Scroll down the page to configure the BGP configuration. Enter the ASN number, BGP timers, Interface Link Detection. For the BGP neighbor configuration, enter the neighbor router, remote ASN, MD5 authentication, multi-hop, and BFD. Click on the **Add** button.



8. Click **Save and Close**.

References

IPv4 and IPv6 Dual-Stack

- IPv6 Chart
- IPV4 to IPV6 Converter - See equivalent of any IPV4 Address

Creating IPv6 Network From Scratch

- Lessons Learned & Recommendations from IPv6-only Deployments – Part One (of Two)
- Lessons Learned & Recommendations from IPv6-only Deployments – Part Two
- IPv6 Prefix Allocation Methods - Part One (of Two)
- IPv6 Prefix Allocation Methods - Part Two
- IPv6 Chart
- How-to: IPv6 address planning | APNIC Blog

Interesting Links

- IPv6 deployment guide | Network World
- USGv6 2014 Client Tester (beta)
- Estimating IPv6 & DNSSEC Deployment Status
- IPv6 Survival Guide

infoblox.

Infoblox unites networking and security to deliver unmatched performance and protection. Trusted by Fortune 100 companies and emerging innovators, we provide real-time visibility and control over who and what connects to your network, so your organization runs faster and stops threats earlier.

Corporate Headquarters
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054
+1.408.986.4000
www.infoblox.com

© 2023 Infoblox, Inc. All rights reserved. Infoblox logo, and other marks appearing herein are property of Infoblox, Inc. All other marks are the property of their respective owner(s).