DEPLOYMENT GUIDE

Configuring BloxOne™ DDI Post Deployment

Table of Contents

Summary

This guide covers the steps to configure a very basic BloxOne DDI DNS and DHCP implementation, after deploying a Host. Your particular needs will most certainly call for additional configuration. The intention of this guide is to walk through the configuration workflow to configure basic DNS and DHCP services, and serve as a hands-on introduction to the configuration process.

Prerequisites

- A BloxOne Host meeting minimum system requirements and necessary ports opened for inbound and outbound access depending on services used as shown in BloxOne documentation.
- Access to Infoblox Cloud Service Portal (CSP) located at csp.infoblox.com.

Configure the Zero Touch Provisioning (ZTP) instance

Once a Host is deployed, it is possible to manage the configuration of the Host and various application services via the Cloud Service Portal (CSP).

Configure the Host in the BloxOne Portal

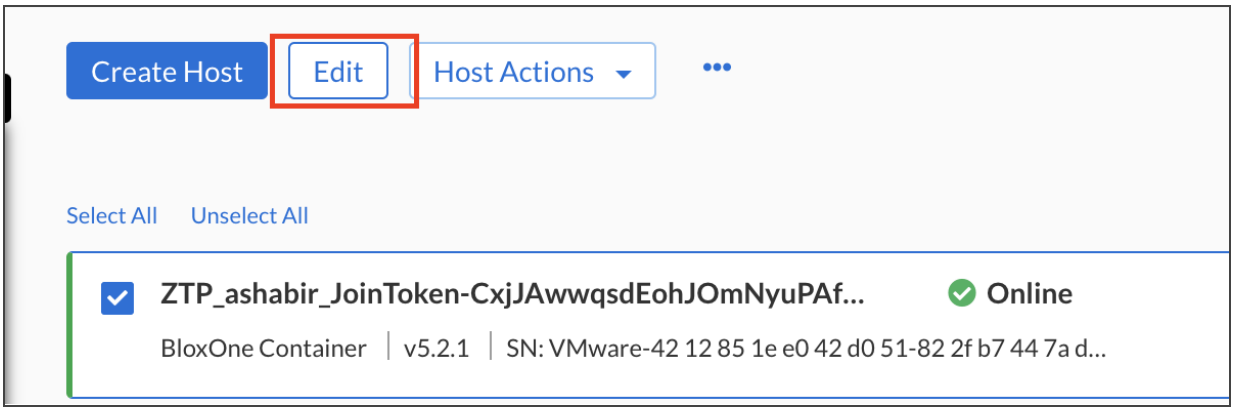
1. Log in to the CSP at: https://csp.infoblox.com .
2. Navigate to **Manage > Infrastructure > Hosts** . You should now see your host in the list with a status of online.

Note: the Host name will begin with "ZTP_" for Zero Touch Provisioning, followed by the join token's name. For example: ZTP_ashabir_JoinToken-CxjJAwwqsdEohJOmNyuPAfKM24MUXvPzBQzeZ9qnJISn

Note: If desired, filter by the Owner tag or Host's IP address to find the new Host instance, by using the Search bar located near the top right of the Host page.

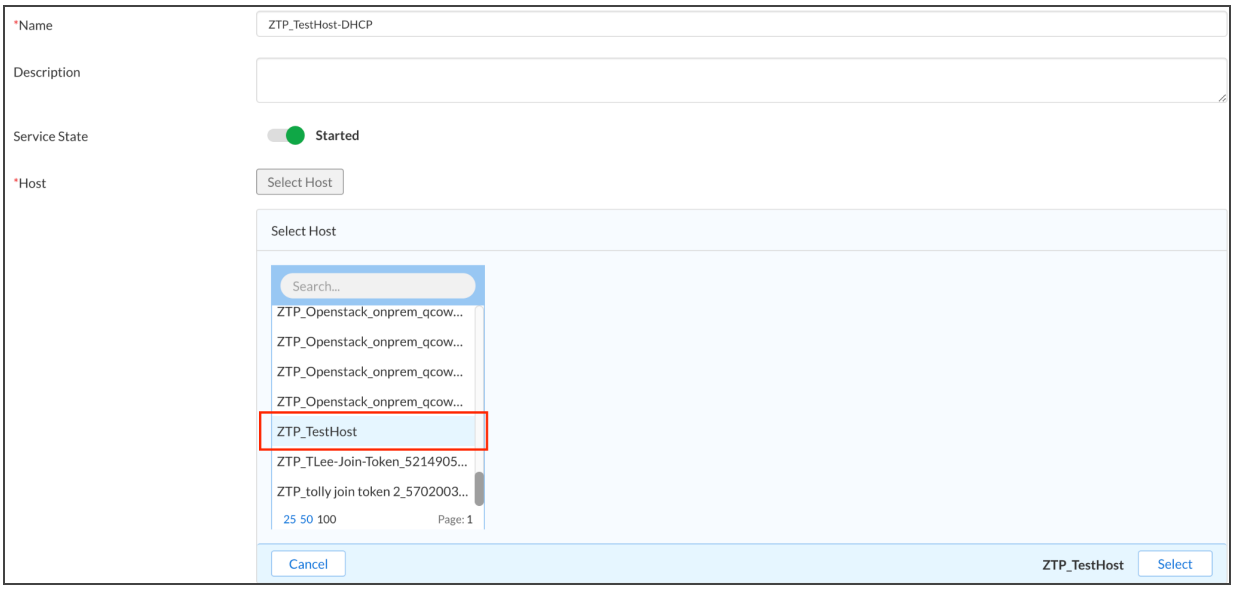
Rename the Host

1. Check the box to the left of the ZTP entry and click Edit. Here you should set the name and a description for the Host. This will be very helpful to locate it for future configuration.



Enable DNS and DHCP Services for the Host

1. Under **Manage > Infrastructure**, click on **Services > Create Service** and select DHCP.



2. Name the service and select the Host you want to associate it with.

3. Click on **Finish** and then **Save and Close**. Repeat steps 1 & 2, this time creating a DNS service.

Configure DHCP

Basic Configuration

This section covers a basic single instance DHCP configuration. There are many additional configuration options available to meet your needs, including high availability options. For more information, refer to BloxOne DDI documentation. About the configuration model for DHCP

DHCP options and lease configuration can be set at many levels through an inheritance model. Going from the most general to the most specific configuration:

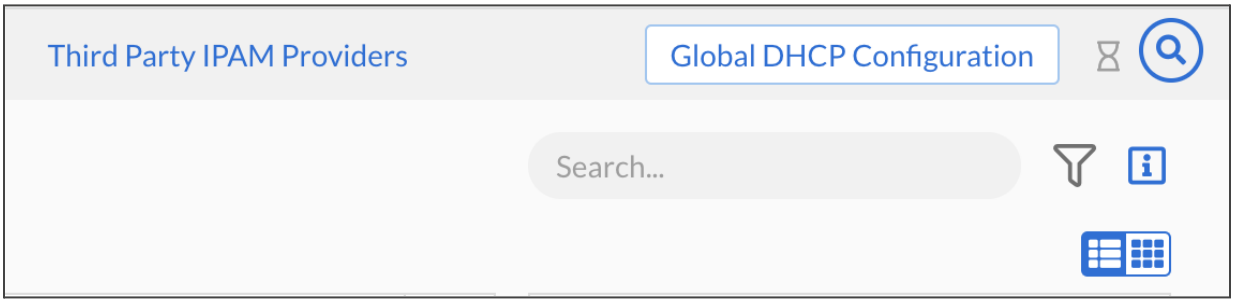
1. Global
2. DHCP Config Profile
3. Host
4. IP Space
5. Subnet
6. DHCP Range

Each level can override DHCP configuration from the level above it. This allows you to set broad parameters at the global, host or profile levels and override for specific needs as you define hosts, IP spaces, subnets and ranges. For example, you might keep a global lease time of 1 hour for a largely dynamic and transient device population, like offices, but override this to 24 hours for a more static environment, such as fixed point of sale equipment. For a more detailed explanation of the inheritance model and options, view this section of the documentation, About DHCP Inheritance.

Set Global DHCP Configuration

Some DHCP settings you may want to apply to most or all of your BloxOne DDI instances. These can be set in the global configuration, and overridden at more specific levels of configuration as needed. Some items that are common for customers to set at the global level include default lease time and DHCP options. To set the default lease time at the global level:

1. In the CSP, navigate to **Manage** → **IPAM/DHCP** and click **Global DHCP Configuration** in the upper right.



2. Expand the **Leases** section and set the Lease Time to your desired default, for example, 1 hour.

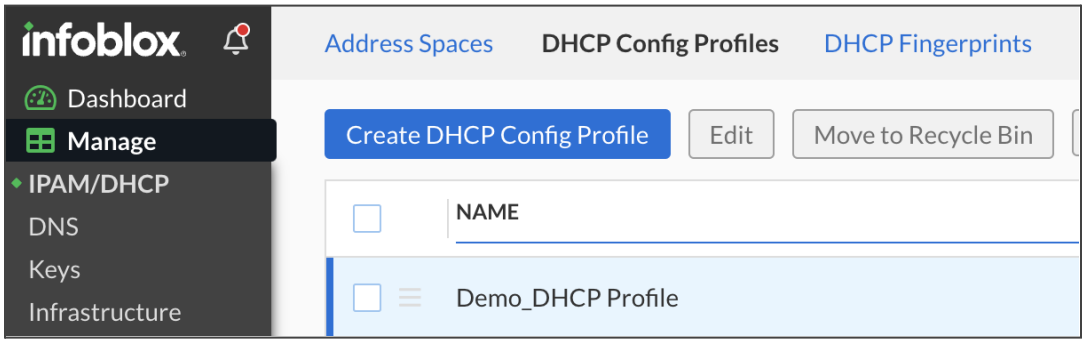
Note: Depending on your needs, a longer lease time, such as 8 hours or more, might be more appropriate. In many environments with a large number of transient mobile devices, a lease time of one hour can make more efficient use of your IP space.

3. Click **Save & Close**.

Create a DHCP Config Profile and Set Some Options

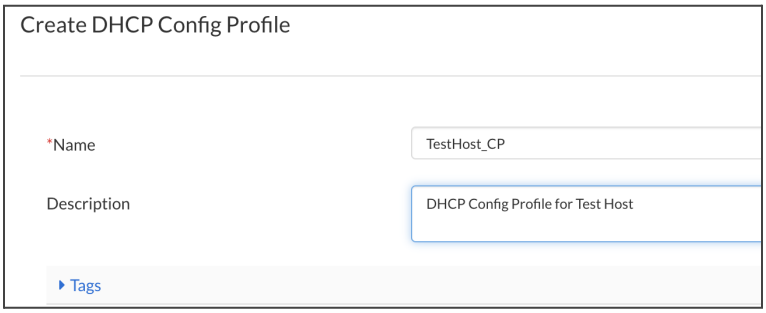
Config profiles are settings templates that can be applied to multiple hosts. DHCP Config profiles are often the preferred way to configure DHCP settings, and are considered best practice, because they can be applied to many hosts. This allows you the ability to modify and keep the configuration consistent across multiple sites and locations. This can save significant time and effort in the management of your deployment.

1. In the CSP, navigate to **Manage** → **IPAM/DHCP** → **DHCP Config Profiles** and click **Create DHCP Config Profile**.



2. On the *Create DHCP Config Profile* page, specify the following:

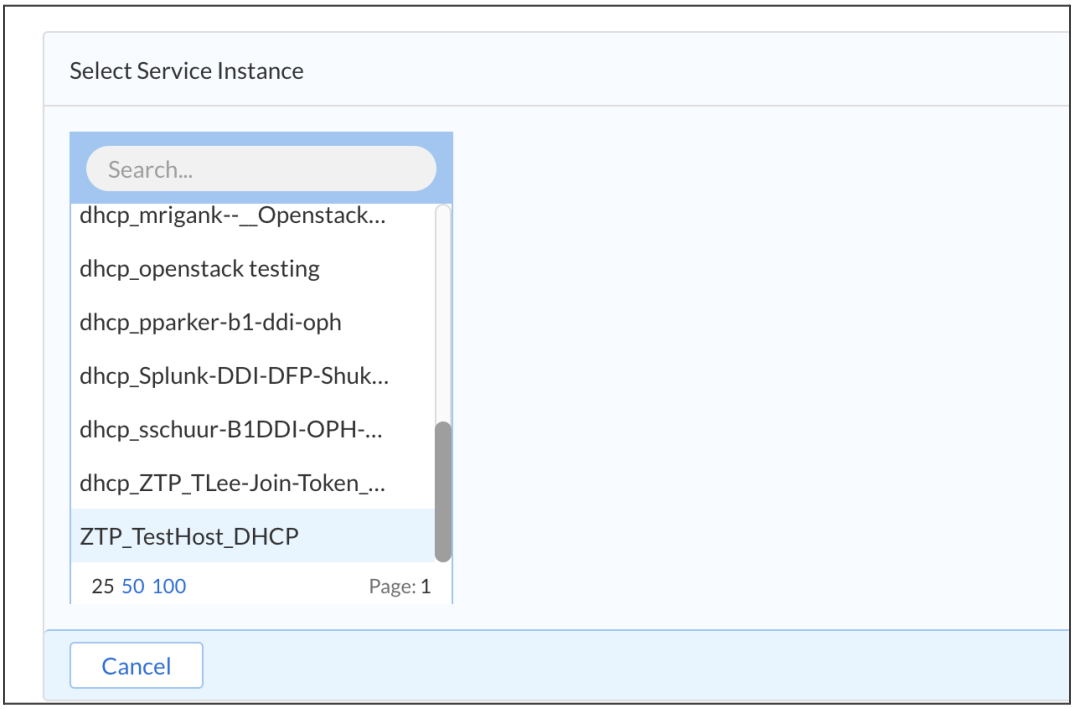
   a. **Name**: Enter a **Name** for the DHCP Config Profile.



b. **Description**: Enter a **Description** in the DHCP Config Profile to help identify it in a list.

3. Click **Save**, this will save the profile, and enable the host selection fields. *Note: If you clicked Save & Close already, simply find the config profile in the list again, and click on the hamburger icon next to it to edit.*

4. Under Service Instance, click **Add**. Scroll or search for your host or hosts, click on them to select them, and then click the **Select** button to associate the profile to them.



*Note: If the Host does not appear in the drop-down, ensure the service is enabled, and attached to the host. You can check this by selecting the Host under **Manage** → **Infrastructure**, and viewing the status for the host .*

If the services don't have a green checkmark, make sure they are enabled, and make sure the hosts are running and connected. A simple initial troubleshooting step can be to restart the VMs/containers.

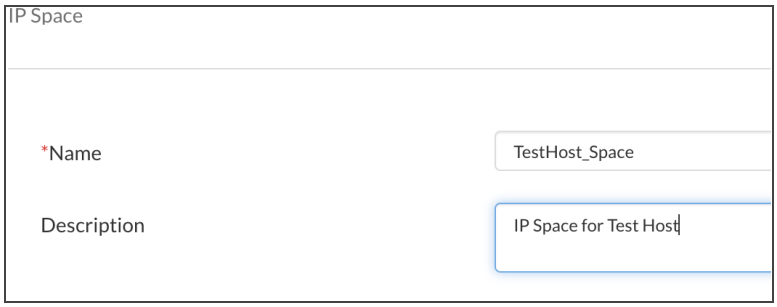
5. Click **Save & Close**.

Add an IP Space

1. Navigate to **Manage** → **IPAM/DHCP**

2. Create an **Address Space** for your network by clicking Address Spaces at the top, then click Create, and select **IP Space** in the dropdown.

3. Fill in a **Name** and **Description**.



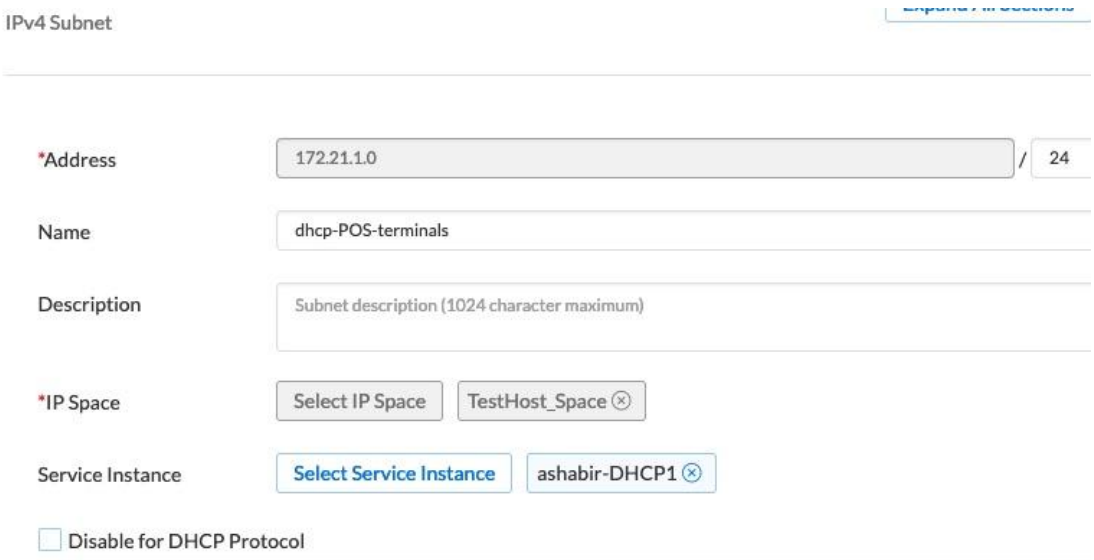
4. Click **Save & Close**.

Add Local Subnet

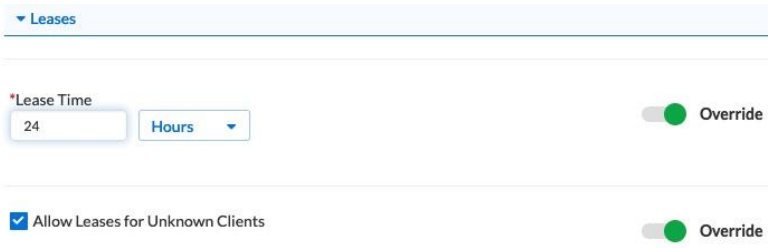
All subnets are created in an IP Space. In this example, we utilize the built-in IP Space named "default." You can also create your own named IP Spaces, which are particularly useful if you have overlapping subnets in different locations.

1. Navigate to **Manage → IPAM/DHCP → Address Spaces**.
2. Select your newly created **IP space**, click Create, and then select **Subnet**.
3. In the address field enter the IP and subnet mask length in the number of bits for your network, for example: 172.21.1.0/24 .
4. Give your subnet a **Name**.
5. Select the **Service Instance** that will be used for DHCP in this subnet.

*Note: You can also disable the DHCP protocol for the subnet which stops the server from offering addresses. This can be useful when pre-provisioning resources or for troubleshooting purposes. Leave this box **unchecked** to follow along with this guide.*



6. In this example, this is a subnet of mobile POS terminals that stay within the location, and do not change hour-to-hour. We will set a lease time of 24 hours. Open Leases, enable Override and Set the lease time to 24 hours. Also, enable Override, and check Allow Leases for Unknown Clients.

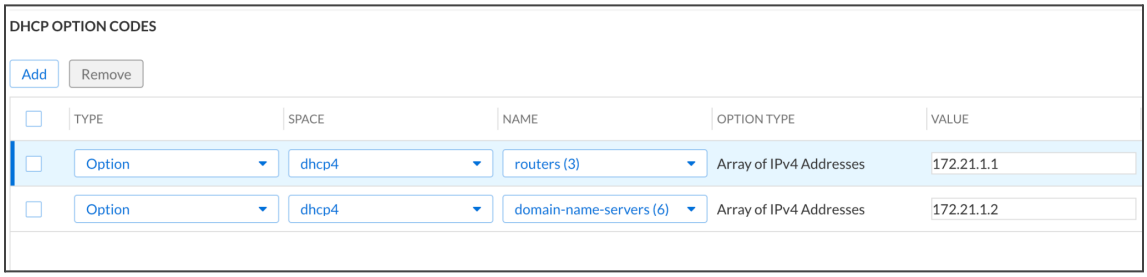


Note: It may make more sense for you to enable Allow Leases for Unknown Clients at the Global configuration level, since without it being checked, no new clients will get leases, unless they have a specific reservation. This might be easier than setting it at lower level configurations.

7. As an example of how to add DHCP options, expand the **DHCP Options** section and click **Override**.

8. Add an **Option 3 (routers)**, in space dhcp4, and enter the default gateway for your network section, for example: 172.21.1.1 .

9. Add an **Option 6 (domain-name-servers)** pointing to your Host serving DNS. You can add multiple addresses here, separated by a comma. Options can also be bundled in groups and applied, at this level, or at a higher config level, such as Host, Config Profile or Global.



Note: These options and settings have all been made specific to this subnet. For more scalability, some or all of these could be set at a higher IP Space configuration level or at the Global Configuration level.

10. Click **Save & Close**.

Add DHCP Range

1. Open your IP range by navigating to **Manage** → **IPAM/DHCP**, scroll or search to find your chosen IP Space (which is "default" in this example), click it, and then click on your subnet.

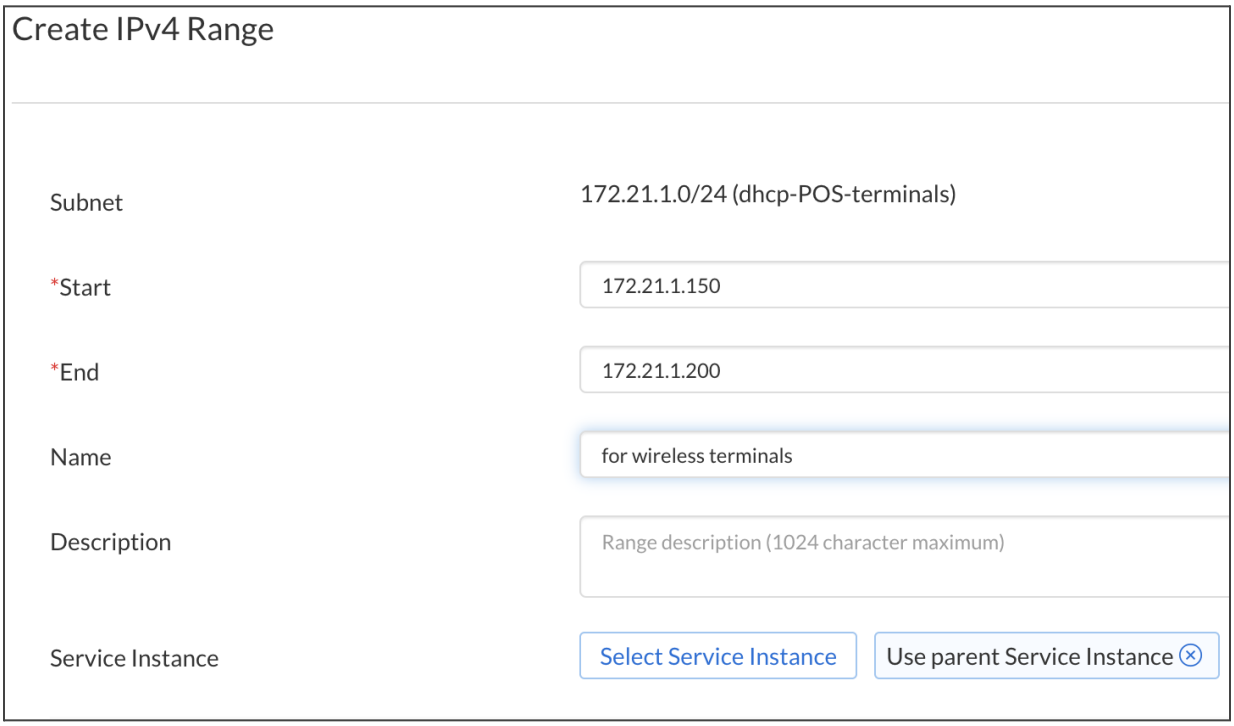
2. You should see the network and broadcast addresses for the subnet.

3. Click **Create**, and then click **Range**.

4. Enter a Start IP and End IP for the DHCP range, and give it a name.

Note: You can look under DHCP options and see that it has inherited the options from the IP range you created the subnet in. You can of course override these and add more options if needed.

5. Click **Save & Close**.



Connect a Client

You can now boot up a client and see if it gets a lease. If you click into your DHCP range in the CSP portal, you should see a host, which you can click on for more info.

On the client command line, you can check that the client has been issued an IP and can ping a public domain, such as infoblox.com on a Linux machine:

```
> ifconfig | grep 172.21.1 -B 2
vmnet2: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
                ether 00:50:5D:c0:01:02
                inet 172.21.1.150 netmask 0xffffff00 broadcast 172.21.1.255
```

On a Windows machine, use the command ipconfig /all:

```
C:\> ipconfig /all

Windows IP Configuration
```

```
        Host Name . . . . . . . . . . . . : vm-w10-7781
        Primary Dns Suffix . . . . . . . :
        Node Type . . . . . . . . . . . . : Hybrid IP Routing
        Enabled. . . . . . . . : No
        WINS Proxy Enabled. . . . . . . . : No
        DNS Suffix Search List. . . . . . : localdomain Ethernet adapter

Ethernet0:

        Connection-specific DNS Suffix . : localdomain
        Description . . . . . . . . . . . : Intel(R) 82574L Gigabit Network Connection
        Physical Address. . . . . . . . . : 00-xx-xx-xx-xx-xx
        DHCP  Enabled. . . . . . . . . . . :  Yes
        Autoconfiguration  Enabled . . . . :  Yes
        Link-local IPv6 Address . . . . . :
fe80::xxxx:xxxx:xxxx:xxxx%11(Preferred)
        IPv4 Address. . . . . . . . . . . : 172.21.1.150(Preferred)
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Lease Obtained. . . . . . . . . . : Tuesday, February 9, 2021 12:37:04 PM
        Lease Expires . . . . . . . . . . : Wednesday, February 10, 2021 12:37:03 PM
        Default Gateway . . . . . . . . . : 172.21.1.1
        DHCP Server . . . . . . . . . . . : 172.21.1.2
        DHCPv6 IAID . . . . . . . . . . . : 5033xxxx
        DHCPv6 Client DUID. . . . . . . . :
00-01-00-01-26-95-3                 A-xx-xx-xx-xx-xx-xx-xx
        DNS Servers . . . . . . . . . . . : 172.21.1.2
        Primary WINS Server . . . . . . . : 172.21.1.2 NetBIOS over Tcpip. . .
        . . . . . : Enabled
```

If a lease is not being provisioned, double check that the Hosts are running. Additionally, check that they are communicating with the CSP portal in the local console screen. Finally, check that they are active in the CSP and that the DNS and DHCP services are running as shown earlier in this section.

Going Further With DHCP

There are many ways to configure DHCP in BloxOne DDI, depending on your needs. You can configure settings using the inheritance model within option spaces, option groups and other config items. Additionally, with multiple Hosts, you can configure high availability with HA groups.

To dig deeper on configuration, refer to DHCP documentation.

Configure DNS

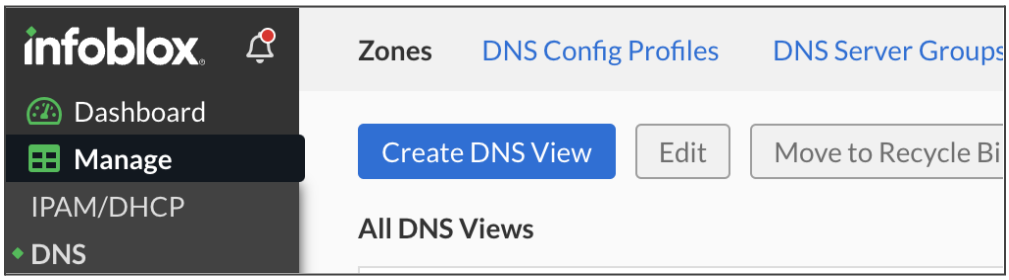
Primary Authoritative Zone

Zones are created in a DNS View. Similar to IP Spaces with DHCP, you can use a default view, or you can create a new one. Again, these can be useful for structuring configuration options for groups of Hosts, or to address overlap. In this example, we will keep it simple by using the default view.

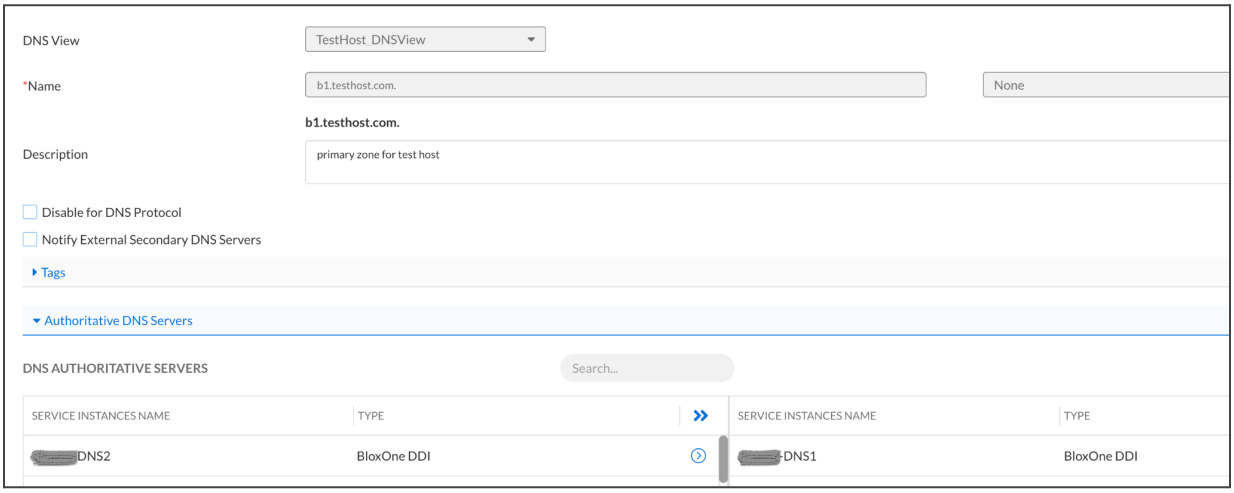
Note: By creating a new DNS View and associating an IP Space with it, you will see a symbol in the usage column next to a DHCP address in the IPAM as an indicator, if there is a DNS record associated with it.

Next, we'll create an authoritative zone for your domain.

1. Go to **Manage** → **DNS** → **Zones**.



2. Find the **default** DNS view and click on it to enter it.
3. Click **Create**, then pick the **Primary Zone**.
4. Name the domain. In the example screenshot, the domain is b1.testhost.com, leave the drop-down set to None, and provide a description that will help you find it later.
5. Expand **Authoritative DNS Servers** and find your DNS server in the left hand column. Once you find your Host, click the arrow next to it to add it to the selected column.
6. Click **Save & Close.**

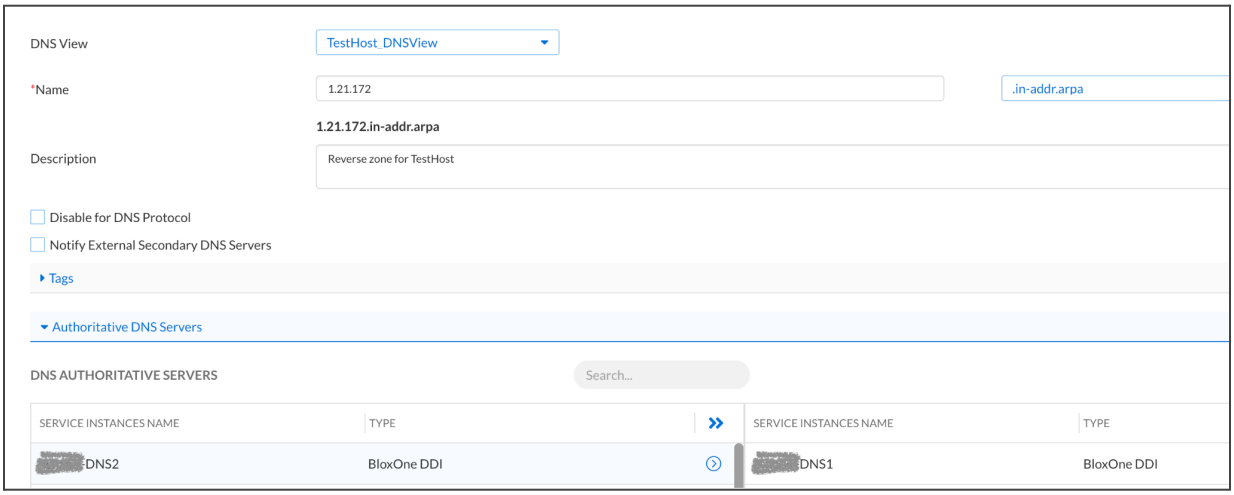


Primary Authoritative Reverse Lookup Zone

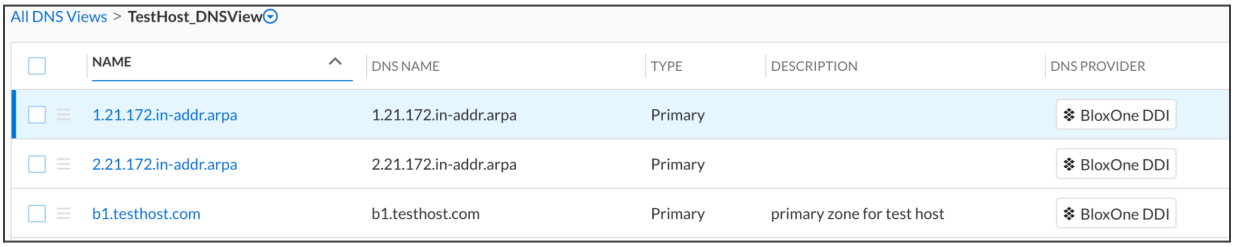
To align with the primary authoritative zone, we'll create a primary authoritative reverse lookup zone.

1. Go to **Manage** → **DNS** → **Zones**.
2. Find your new **DNS view** and click on it to enter it.

3. Click **Create** then pick **Primary Zone**.
4. Ensure your intended DNS View is in the DNS View field.
5. In the Name field, enter your subnet address in reverse order, omitting the first octet, e.g. if your subnet is 172.21.1.0/24 enter 1.21.172 .
6. Select "**.in-addr.arpa**" from the drop down.
7. Expand **Authoritative DNS Servers** and find your DNS server in the left hand column by scrolling or searching. Once you find your instance, click the down arrow next to it to add it to the selected column.
8. Click **Save & Close**.



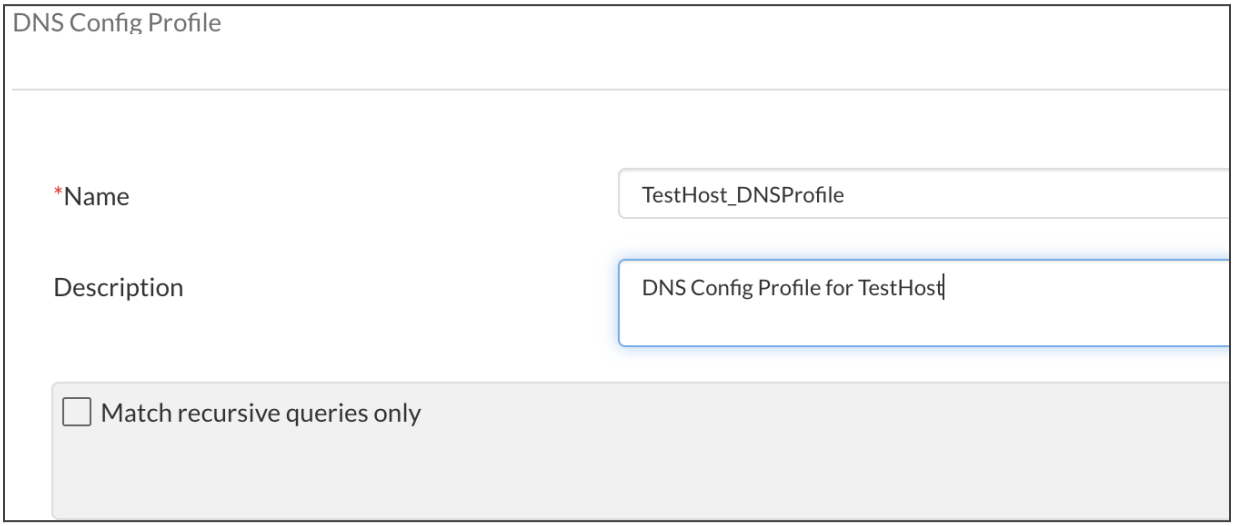
9. You should now see a forward and reverse zone in your DNS View:



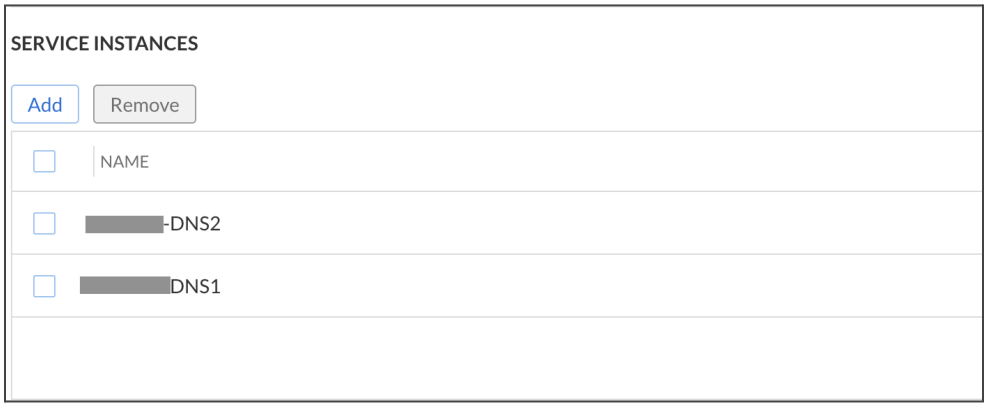
DNS Config Profile

DNS Config Profiles are very powerful tools in BloxOne DDI. They allow you to set a number of configuration parameters in one place, and apply it to multiple Hosts. A change made in the Config Profile will propagate to all associated Hosts. It can save a lot of time to configure the broadly used settings in a Profile, and handle any exceptions or special cases by overriding the Profile settings on individual host configurations.

1. Go to **Manage → DNS → DNS Config Profiles**.
2. Click **Create DNS Config Profile**.
3. Enter a **Name** and **Description** for the profile.

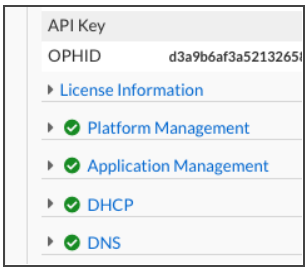


4. Click **Save**. This will save the profile, and enable the host selection fields. *Note: If you clicked Save & Close already, simply find the config profile in the list again, and click on the hamburger icon next to it to edit.*
5. Under **Service Instances** add your Host, by searching by name and clicking on it, then clicking Select.



Note: If the Host does not appear in the drop-down, ensure the service is started on the host. You can check this by selecting the Host under Manage → Hosts, and viewing the status for the host on the right side of the page:

If the services don't have a green checkmark, make sure they are enabled, and make sure the hosts are running and connected. A simple initial troubleshooting step can be to restart the VMs/containers.



6. Let's allow queries from our subnet. Expand **Queries** and toggle **Override** on **ALLOW QUERIES FROM.**

7. Add your **IPv4 Network** in CIDR format, with an **Allow** permission.

8. Now, let's allow recursion from our internal networks. Expand **Recursion** and then switch on the override for **ALLOW RECURSIVE QUERIES FROM**.

9. Add a **Named ACL** and input an IPv4 Network.

Note: If your network doesn't conform to RFC1918 (192.168.x.x, 10.x.x.x or 172.16.0.0/12) you will need to use IPv4 network instead and enter your IP subnet.

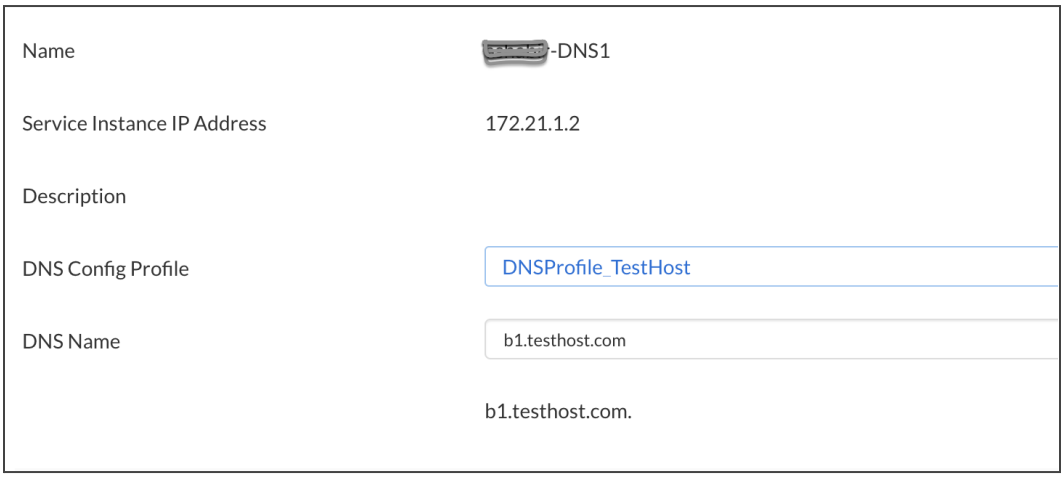
Note: If you are utilizing a BloxOne Threat Defense DNS Forwarding Proxy, keep in mind that the DNS settings that you make here can affect how that proxy operates.

10. Click **Save & Close**.

Check the Application of Config Profile on the DNS Server

1. On the DNS page, click **DNS Servers** (at the top of the page).
2. Find your DNS server in the list, check it, then click **Edit**.
3. Check that the **DNS profile** is set to the one you just created.

Note: This step is not necessary, it is only illustrative to see the connection.



Test DNS Configuration

To test your DNS Configuration use the following commands:

1. You can test that resolution is working in your client with dig. The IP of the DNS instance in this example is 172.21.1.2, as configured during deployment:

```
dig @172.21.1.2 www.infoblox.com +noall +answer
```

2. It should reply with a valid lookup to the A query, similar to this:

```
; <<>> DiG 9.10.6 <<>> www.infoblox.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 63270
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.infoblox.com.                      IN      A
;; ANSWER SECTION:
www.infoblox.com.               1720    IN      CNAMEagcdn.pantheon.map.fastly.net.
agcdn.pantheon.map.fastly.net. 30 IN    A       151.101.122.253
```

3. If you are on Windows, you can test with nslookup as well:

```
C:\> nslookup www.infoblox.com 172.21.1.2
```

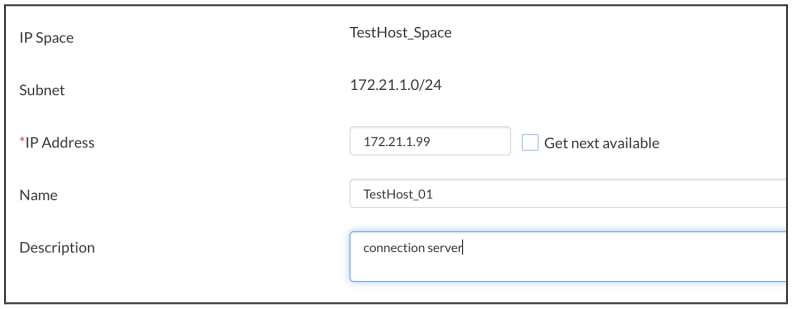
4. It should reply with a valid lookup to the A query, similar to this:

```
Server:         172.21.1.2
Address:        172.21.1.2#53
Non-authoritative answer:

www.infoblox.com        canonical name = live-infoblox-network.pantheonsite.io.
live-infoblox-network.pantheonsite.io   canonical name = fe3.edge.pantheon.io.
Name: fe3.edge.pantheon.io      Address: 23.185.0.3
```

Make an IP Reservation

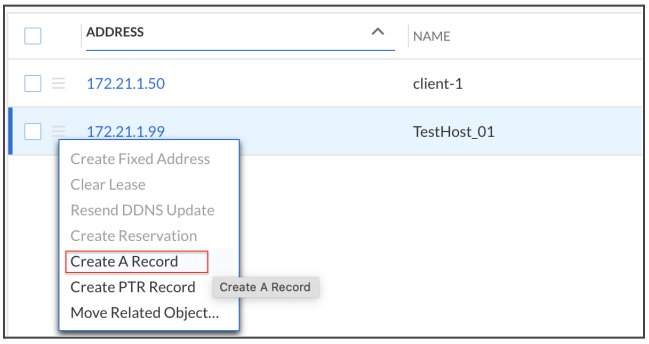
1. Go to **Manage** → **IPAM/DHCP** → **Address Spaces**.
2. Find and click on your **IP Space**.
3. Click on your **Subnet**.
4. Click **Create**, and then click IPv4 Reservation.
5. Enter the **IP address** of a host contained in that network and give it a **Name**.



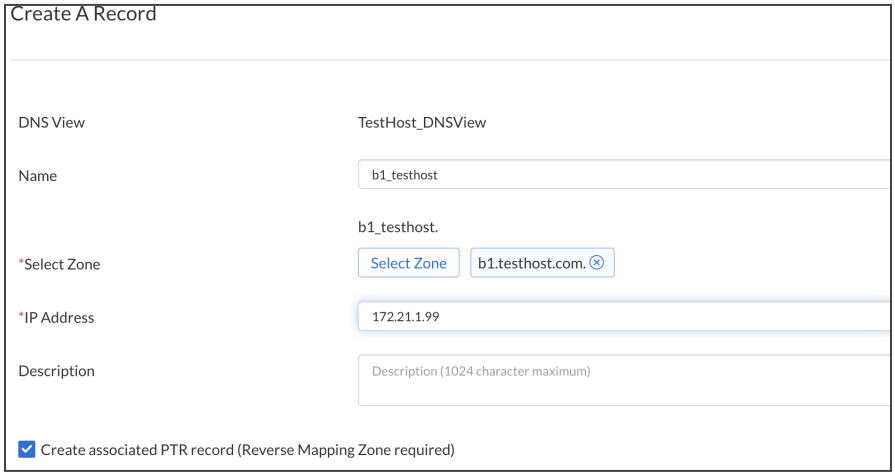
6. Click **Save & Close**.

Create A and PTR Records For Reserved Host

1. Click the **properties button (Hamburger button)** next to your reservation and select **Create A Record**.



2. Designate a Name for the host.
3. Select your **DNS zone** in the Select Zone portion of the window.

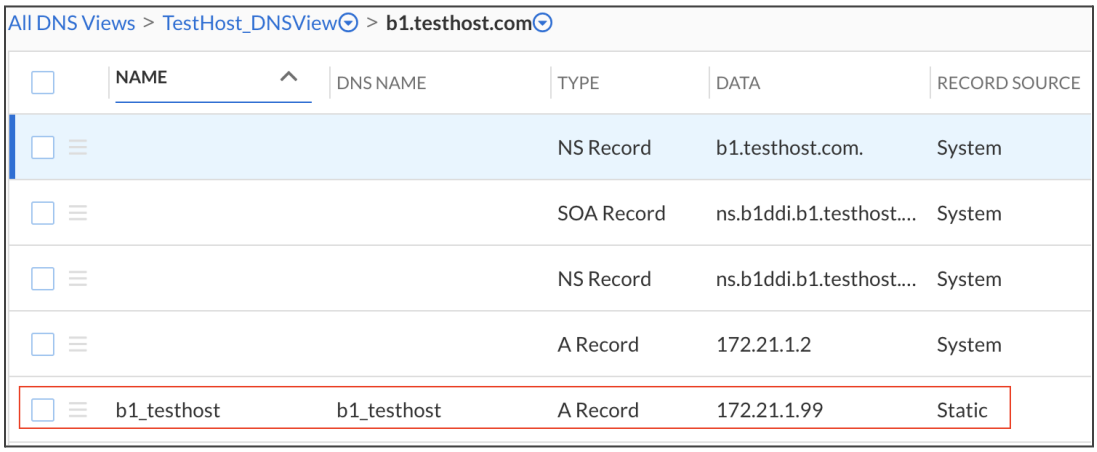


4. Check the **Create associated PTR** record box.
5. Click **Save & Close**.

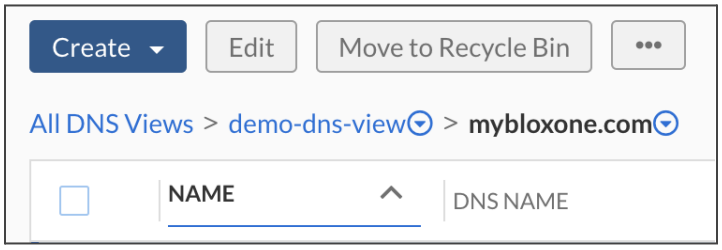
Check A and PTR Records

Verify that the A and PTR Records were created by performing the following steps:

1. Go to **Manage** → **DNS** → **Zones**.
2. Find and click on your **DNS view**.
3. Click on the **forward zone**, for example b1.testhost.com.
4. You should see the A record you created:

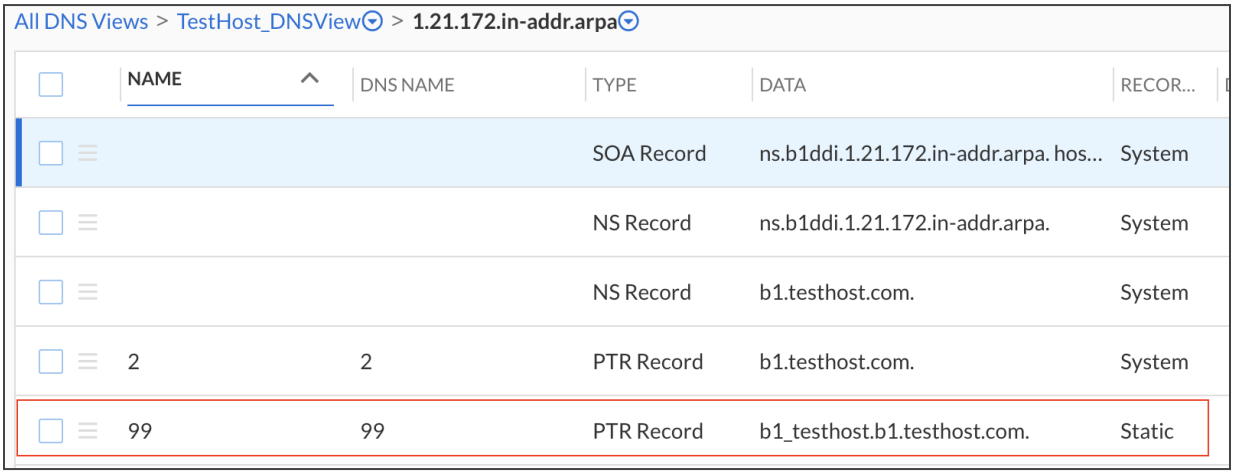


5. Return to the DNS view by clicking on the DNS View name.



6. Click on the **reverse zone**, for example **1.21.172.in-addr.arpa** .

7. You should see the PTR record you created along with the A record:



Test Queries From the Client

Test your DNS setup and see how the resource records look like:

1. You can now test this in your client, querying the DNS server on the Host directly for your A record, directly to the Host (for example, 172.21.1.2):

   dig @172.21.1.2 b1_testhost.b1.testhost.com.

2. Look for a matching answer section, with your DNS server and BloxOne DDI in the authority section, similar to this:

```
;; QUESTION SECTION:
;b1_testhost.b1.testhost.com.    IN      A

;; ANSWER SECTION:
b1_testhost.b1.testhost.com. 28800 IN   A       172.21.1.99

;; AUTHORITY SECTION:
b1.testhost.com.        28800   IN      NS      b1.testhost.com.
b1.testhost.com.        28800   IN      NS      ns.b1ddi.b1.testhost.com.

;; ADDITIONAL SECTION:
b1.testhost.com.        28800   IN      A       172.21.1.2
ns.b1ddi.b1.testhost.com. 28800 IN      A       172.21.1.2
```

Note: The ns.biddilocal.infoblox.com entry is the default MNAME field in the SOA record signifying that the zone is cloud managed. The associated A record for this nameserver will point to the IP of the BloxOne DDI server that was queried. Currently, this record cannot be changed, removed or hidden.

3. Now, check the inverse host on the Host directly for the corresponding PTR record:

   dig @172.21.1.2 -x 172.21.1.99

   - Look for a matching answer section, with your DNS server and BloxOne DDI in the authority section, similar to this:

```
;; QUESTION SECTION:
;99.1.21.172.in-addr.arpa.      IN      PTR

;; ANSWER SECTION:
99.1.21.172.in-addr.arpa. 28800 IN      PTR     b1_testhost.b1.testhost.com.

;; AUTHORITY SECTION:
1.21.172.in-addr.arpa.  28800   IN      NS      b1.testhost.com.
1.21.172.in-addr.arpa.  28800   IN      NS      ns.b1ddi.1.21.172.in-addr.arpa.

;; ADDITIONAL SECTION:
b1.testhost.com.        28800   IN      A       172.21.1.2
ns.b1ddi.1.21.172.in-addr.arpa. 28800 IN A      172.21.1.2
```

4. You can also test with these nslookup commands:

   C:\> nslookup b1_testhost.b1.testhost.com. 172.21.1.2

   C:\> nslookup 172.21.1.99 172.21.1.2

Going Further With DNS Configuration

Like DHCP, there are many ways to configure DNS in BloxOne DDI, depending on your needs. Additional common DNS configurations include adding an additional instance, setting up DDNS, creating server groups and assigning a secondary zone.

To dig deeper on configuration, refer to DNS documentation. To configure DDNS, refer to DDNS documentation.

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