Infoblox User Guide

For the Infoblox-550 Appliance

Version 4.0

P/N 400-0106-100 Rev. A

Infoblox User Guide

For the Infoblox-550 Appliance

Contents

Copyright Statements

For Open Source Copyright information, see *Open Source Copyright and License Statements* in the Online Help.

Trademark Statements

Warranty Information

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

Company Information

Infoblox is located at:
4750 Patrick Henry Drive
Santa Clara, CA 95054-1851, USA

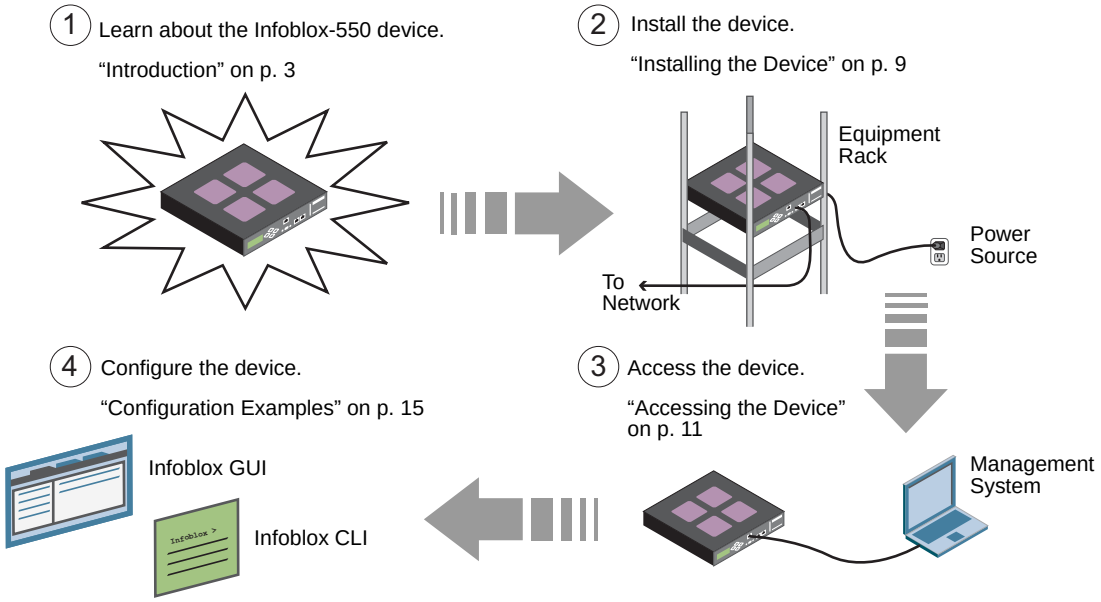
Web: www.infoblox.com
www.infoblox.com/support

Phone: 408.625.4200
Toll Free: 888.463.6259
Outside North America: +1.408.716.4300
Fax: 408.625.4201

Introduction

This guide provides an overview of the Infoblox-550 network identity appliance with Infoblox NIOS (Network Identity Operating System) version 4.0 or later, and it explains how to install and configure it. Two configuration examples are presented. The first example describes how to deploy a single device as an independent external DNS server. The second describes how to deploy two devices as an HA (high availability) pair for internal DNS and DHCP services.

Figure 1 *Tasks in This Guide*



Product Overview

The Infoblox-550 appliance provides a powerful, cost-effective solution for small and medium-sized businesses that need integrated DNS (Domain Name System) and DHCP (Dynamic Host Configuration Protocol) services. In addition to DNS and DHCP services, it also includes RADIUS (Remote Authentication Dial-In User Service) proxy and TFTP (Trivial File Transfer Protocol) network services.

You can configure and manage the Infoblox-55o appliance through an easy-to-use GUI (graphical user interface) that works seamlessly in both Windows and Linux environments using standard web browsers. This appliance provides DNS and DHCP services for up to 500 users, 1000 host devices, and 5000 records while serving 10,000 DNS queries per second.

The Infoblox-550 appliance is RoHS and WEEE compliant, and its hardware meets the mechanical requirements for FIPS 140-2 compliance.

Infoblox-550 Network Identity Appliance

The Infoblox-550 appliance is a 1-U platform that you can easily mount in a standard equipment rack using the mounting brackets and bolts shipped with the device. The front panel components include the LCD (liquid crystal display) panel and navigation buttons, communication ports, and indicator lights. The back panel components include the power connector and switch, fan and air vent, and the model and serial number label.

Figure 2 shows the components on the front and back of the Infoblox-550, and *Table 1* provides descriptions.

Figure 2 *Infoblox-550 Appliance, Front and Back Views*

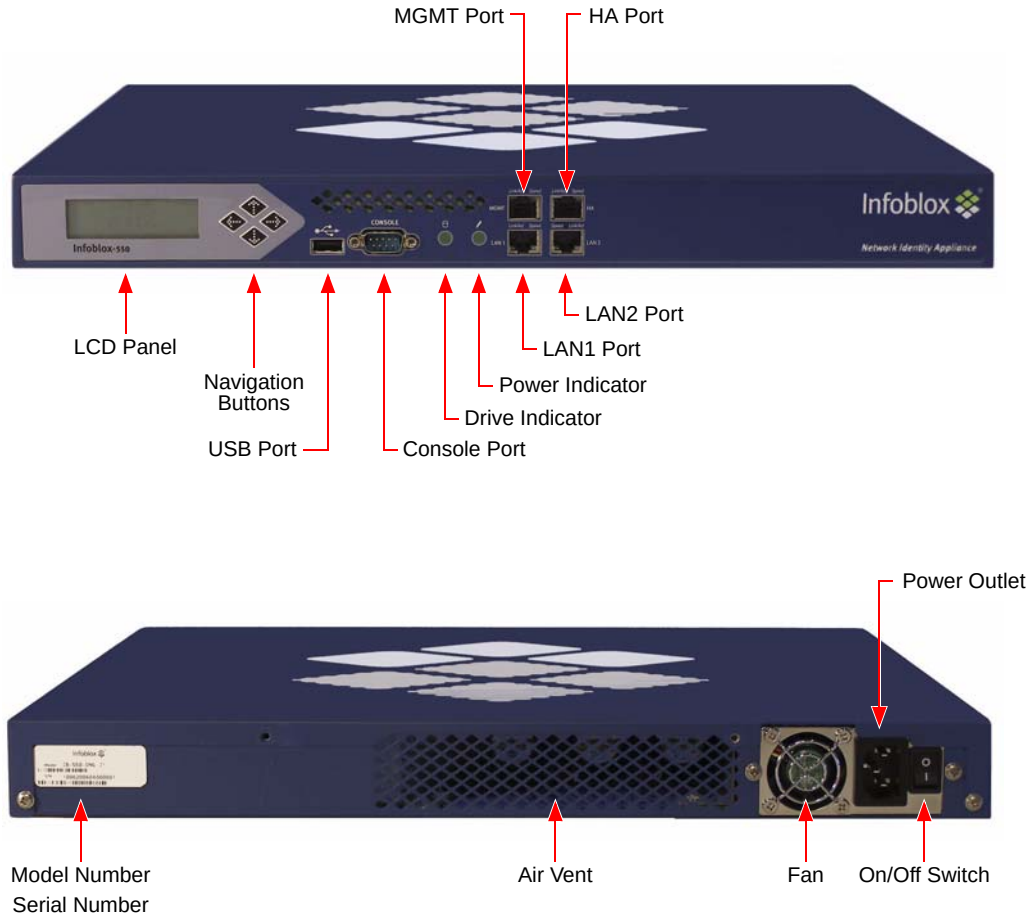


Table 1 *Infoblox-550 Component Descriptions*

Component	Description
LCD Panel	An LCD screen that displays HA (high availability) status, network settings, software version number, hardware serial number, and software licenses. Additionally, you can view and configure the IP address, netmask, and gateway for the LAN1 port.
Navigation Buttons	Buttons that allow you to enter the IP address, subnet mask, and gateway of the LAN1 port through the LCD. Use the Up and Down arrow buttons to specify numbers and the Left and Right buttons to navigate across digits. You must specify whether to save input (OK) or discard it (CNCL). Selecting **CNCL** at any time returns you to the previous entry. Entering **OK** on the third screen returns you to the system status screen.
USB Port	Reserved for future use.
Console Port	A male DB-9 serial port for a console connection to change basic configuration settings and view basic system functions through the CLI (command line interface). Use the serial cable and connection adapters that ship with the device to make a console connection to this port.
Drive Indicator	An LED that flashes green to indicate when the hard drive processes data.
Power Indicator	An LED that glows green to indicate when there is power to the device.
MGMT Port	A 10/100/1000-Mbps fast ethernet port that you can use for device management or DNS service. You can enable the MGMT port and define its use through the GUI.
HA Port	A 10/100/1000-Mbps fast ethernet port through which the active node in an HA (high availability) pair connects to the network using a VIP (virtual IP) address. HA pair nodes also use their HA ports for VRRP (Virtual Router Redundancy Protocol) advertisements.
LAN1 Port	A 10/100/1000-Mbps fast ethernet port that connects a single device to the network. If the MGMT port is not in use, a single device uses the LAN1 port for management traffic. The passive node in an HA pair uses this port to synchronize the database with the active node.
LAN2 Port	Reserved for future use.
Model Number	An identifier of the hardware model type, software type, and power cord type.
Serial Number	The serial number of the device. Use it to register the device to obtain software upgrades and technical support services.
Air Vent	An air vent that allows warm air to flow out of the device. Do not obstruct.
Fan	A fan to help maintain optimum operating temperature. Do not obstruct.
Power Outlet	A three-prong power outlet for connecting the device to a standard AC power source.
On/Off Switch	A power switch to turn the device on and off.

Connector Pin Assignments

The Infoblox-550 appliance has three types of ports on its front panel:

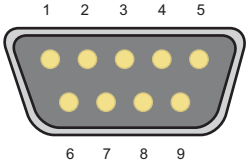
- USB port (reserved for future use)
- Male DB-9 console port
- RJ-45 10Base-T/100Base-T/1000Base-T ethernet ports

Figure 3 shows the DB-9 and RJ-45 connector pin assignments. The DB-9 pin assignments follow the EIA232 standard. To make a serial connection from your management system to the console port, you can use the RJ-45 rollover cable and two female RJ-45-to-female DB-9 adapters that ship with the device, or a female DB-9-to-female DB-9 null modem cable. The RJ-45 pin assignments follow IEEE 802.3 specifications. All Infoblox ethernet ports are auto-sensing and automatically adjust to standard straight-through and cross-over ethernet cables.

10Base-T ethernet and 100Base-T fast ethernet use the same two pairs of wires. The twisted pair of wires connecting to pins 1 and 2 transmit data, and the twisted pair connecting to pins 3 and 6 receive data. For 1000Base-T connections, all four twisted-pair wires are used for bidirectional traffic.

Figure 3 *Connector Pin Assignments*

Male DB-9 Console Port

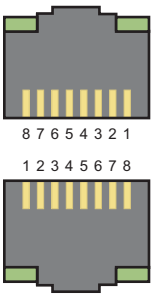


(Looking into the console port on an Infoblox device)

DB-9 Connector Pin Assignments

Pin	Signal	Direction
1	(not used)	
2	Receive	Input
3	Transmit	Output
4	DTE Ready	Output
5	Ground	—
6	DCE Ready	Input
7	RTS (Request to Send)	Output
8	CTS (Clear to Send)	Input
9	(not used)	

RJ-45 Ethernet Ports



(Looking into RJ-45 ethernet ports on an Infoblox device)

RJ-45 Connector Pin Assignments

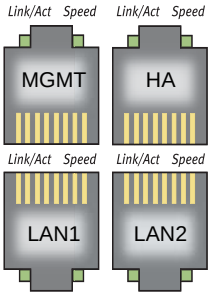
Pin	10Base-T 100Base-T Signal	1000Base-T Signal	T568A Straight-Through Wire Color	T568B Straight-Through Wire Color
1	Transmit +	BI_DA+	White/Green	White/Orange
2	Transmit -	BI_DA-	Green	Orange
3	Receive +	BI_DB+	White/Orange	White/Green
4	(not used)	BI_DC+	Blue	Blue
5	(not used)	BI_DC-	White/Blue	White/Blue
6	Receive -	BI_DB-	Orange	Green
7	(not used)	BI_DD+	White/Brown	White/Brown
8	(not used)	BI_DD-	Brown	Brown

Legend: BI_D = bidirectional; A, B, C, D = wire pairings

Ethernet Port LEDs

To see the link activity and connection speed of an ethernet port, you can look at its Link/Act and Speed LEDs. The status the LEDs convey through their color and illumination (steady glow or blinking) are presented in *Figure 4*.

Figure 4 *LEDs*



Label	Color	Port Status
Link/Act	Steady Green	Link is up but inactive
	Blinking Green	Link is up and active
	Dark	Link is down
Speed	Steady Amber	1000 Mbps
	Steady Green	100 Mbps
	Dark	10 Mbps

System, Environmental, and Power Specifications

Understanding the full range of specifications for the Infoblox-550 appliance is critical for maintaining and protecting the hardware from misuse. There are three types of specifications. System specifications describe the physical characteristics of the device. Environmental specifications describe the temperature and moisture limits the device can withstand. Power specifications describe the electrical range within which the device circuitry can operate.

System Specifications

- **Form Factor:** 1-U rack-mountable device
- **Dimensions**: 1.75” H x 17.25” W x 15” D (4.45 cm H x 43.82 cm W x 38.1 cm)
- **Weight**: Approximately 13 pounds
- **Ethernet Ports**: MGMT, HA, LAN1, LAN2 – auto-sensing 10Base-T/100Base-T/1000Base-T
- **Serial Port**: DB-9 (9600/8n1, Xon/Xoff)
- **LCD Panel**: LCD (liquid crystal display) with input buttons

Environmental Specifications

- Operating Temperature: 41 to 95 degrees F (5 to 35 degrees C)
- Storage Temperature: -40 to 122 degrees F (-40 to 50 degrees C)
- Relative Humidity: 5% to 95%, relative humidity (non-condensing)

Electrical Power Specifications

- Input Voltage: 100 – 240 VAC switchable, 47 – 63 HZ, 3A
- Output Power: 250 watts
- Power plug and cable specifications by region:

Region	Plug Type	Cable Type	Maximum Power Rating	Maximum Temperature Rating
North America	NEMA5-15P 3-prong male plug	VCTF 3C 18 AWG	7A, 125 V	75° C
Japan	NEMA5-15P 3-prong male plug	VCFI 3G	12A, 125 V	60° C
Europe	CEE7 standard VII 2-prong male plug	H05VV-F	6A, 250 V	70° C
United Kingdom	LP-60L 3-prong male plug with fuse	H05VV-F	10A, 250 V	70° C

Installing the Device

Follow these instructions to rack mount the device, connect it to a power source, and cable it to a network. However, before proceeding review the Safety Guide and follow the necessary precautions.

Rack Mounting

The device mounts into a standard 19" (48 cm) equipment rack. In addition to the screws and brackets that ship with the product, you also need a screwdriver with a cross-headed tip.

Attach the brackets to the device, and mount it to an equipment rack.

1. Remove the four screws that ship attached to the left and right sides of the device—two screws per side.
2. Remove the pair of brackets from the accessory kit that ships with the device.
3. Position one bracket so that the two holes in the bracket align with two of the holes on one side of the device.

   Note: There are five evenly spaced holes on each side of the device. You can secure the brackets to any two adjacent holes so that you can mount the device more or less deeply in the rack.

4. Secure the bracket to the device with two of the screws that you removed previously.
5. Secure the second bracket in the same position on the other side of the device.
6. Using the screws from the accessory kit, attach the brackets to the equipment rack.

Powering the Device

Use the power cable that ships with the Infoblox-550 appliance to connect it to a power source.

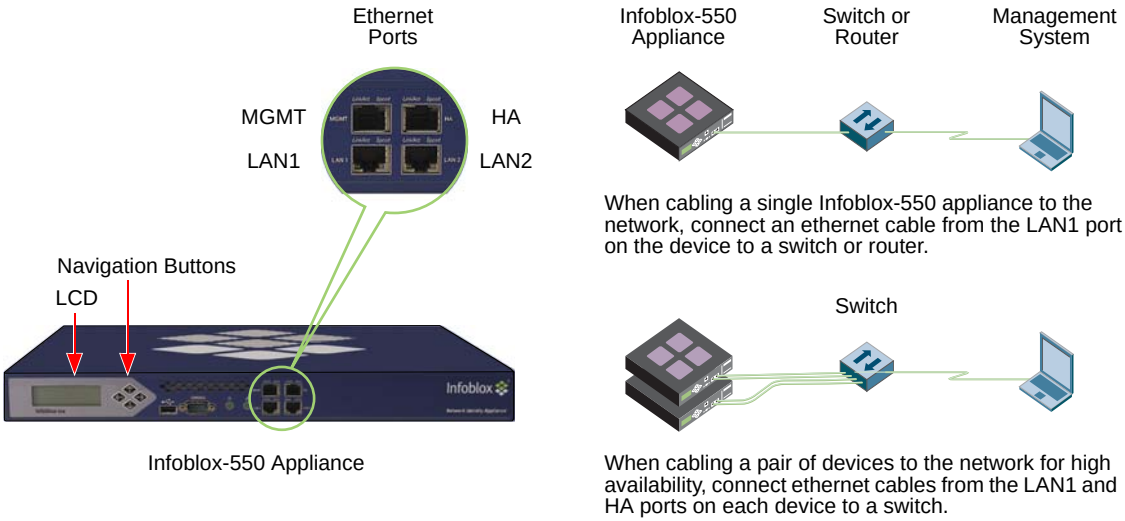
1. Make sure the power switch on the device is turned off.
2. Connect a power cable between the power connector on the back of the appliance and a properly grounded and rated power circuit that meets the provisions of the current edition of the National Electrical Code, or other wiring rules that apply to your location. Make sure the outlet is near the appliance and is easily accessible.
3. Turn on the power switch.

Cabling the Device to a Network

Use the ethernet cables shipped with the product to connect the device to the network.

1. Connect an ethernet cable from the LAN1 port on the device to your network switch or router.
2. If you want to connect your device for HA (high availability), connect the HA ports on both devices to a switch on your network. The VIP (Virtual IP), LAN1, and HA port addresses must be on the same subnet and must be unique for that subnet.

Figure 5 *Cabling a Single Device and an HA Pair to a Network*



Note: By default, an Infoblox device automatically negotiates the optimal connection speed and transmission type (full or half duplex) on the physical links between its LAN1, HA, and MGMT ports and the ethernet ports on a connecting switch. If the two devices fail to auto-negotiate the optimal settings, see the *Infoblox Administrator Guide* for steps you can take to resolve the problem.

3. HA pair: To ensure that VRRP (Virtual Router Redundancy Protocol) works properly, configure the following settings on the connecting switch:
   - Portfast: enable
   - Trunking: disable
   - Port list: disable
   - Port channeling: disable
4. Use the Infoblox GUI to access the Infoblox device from a management system. Through the GUI, you can set up and administer the device. For management system requirements and access instructions, see *Accessing the Device* on page 11.

Accessing the Device

The management system is the computer from which you configure and monitor the Infoblox device. You can access the device from the management system remotely across an ethernet network or directly through a serial cable.

After completing the steps in *Cabling the Device to a Network* on page 10, you can make an HTTPS connection to the device and access the Infoblox GUI through JWS (Java Web Start) or make an SSHv2 connection and access the CLI through an SSHv2 client. You can also access the CLI by connecting a serial cable directly from the console port of a management system to the console port on the device, and then using a terminal emulation program.

The management system must meet the following requirements to operate an Infoblox device.

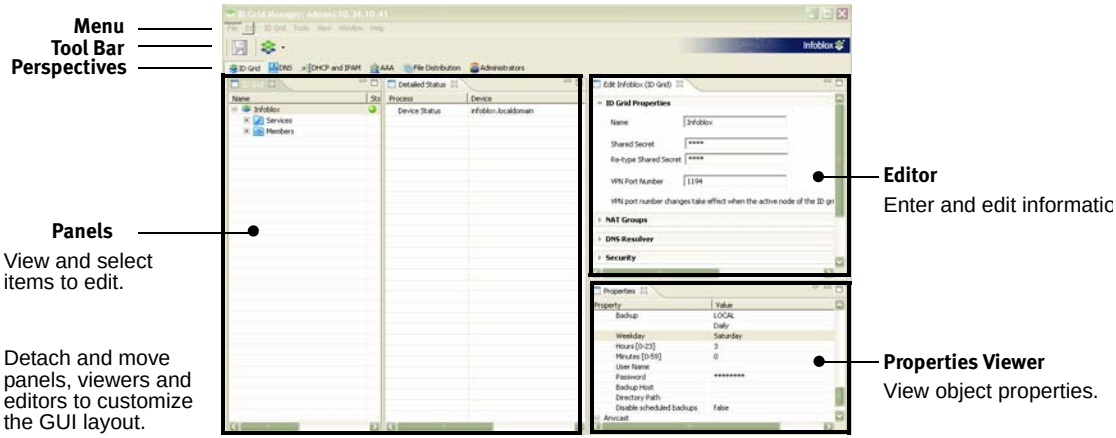
Table 2 *Software and Hardware Requirements for the Management System*

Management System Software Requirements	Management System Hardware Requirements
GUI ACCESS • Microsoft Internet Explorer® 6.0 or higher on Microsoft Windows NT® 4.0, Microsoft Windows® 2000, Microsoft Windows XP® or • Mozilla 1.7 or higher on Linux or variants of UNIX (Irix, Solaris, HP-UX, AIX) and • Sun® Java Runtime Environment (JRE) versions 1.5.0_06 or later • JWS application, which is automatically installed with JRE 1.5.0_06 or later CLI ACCESS • Secure Socket Shell (SSH) client that supports SSHv2 • Terminal emulation program, such as minicom or Hilgraeve Hyperterminal®.	• Minimum System: 500 MHz CPU with 256 MB RAM available to the product GUI, and 56 Kbps connectivity to an Infoblox device • Recommended System: 1 GHz (or higher) CPU with 512 MB RAM available for the product GUI, and network connectivity to an Infoblox device • Monitor Resolution: 1024 x 768 (minimum) to 1600 x 1200 (maximum)

Infoblox GUI

You can view data and configuration settings and make configuration changes through the Infoblox GUI. When an Infoblox device functions as an independent device, you launch the ID Device Manager to access the GUI. When the device is in an ID grid, you log in to the grid master and launch the ID Grid Manager.

Figure 6 *Infoblox GUI Overview*



When you make an HTTPS connection to the device and access the Infoblox GUI through JWS, the Java installation typically associates JNLP file types with the JWS application automatically, although not in all UNIX environments. If the browser does not automatically associate a JNLP file with the JWS application, when you click **Launch ID Grid Manager** or **Launch ID Device Manager**, you receive a prompt. Internet Explorer running on a Windows system and Mozilla running on a Linux system provide different prompts:

Internet Explorer prompts you to save the JNLP file. Click **Cancel**, and make the file association as follows:

1. Click **Start -> Control Panel -> Folder Options -> File Types -> New**.
2. In the File Extension field, type **JNLP**, and then click **Advanced**.
3. From the Associated File Type drop-down list, choose **JNLP File**, and then click **OK**.
4. To close the *Folder Options* dialog box, click **Close**.
5. You can now continue logging in to the device.

Mozilla prompts you to save the JNLP file or choose an application to open it.

1. Select the **Open with** button, and then choose **Other** from the drop-down list.
2. Navigate to the Java directory—typically in a standard system directory like /usr/java/ on Linux systems.
3. Open the jre1.5.0_06 (or later) subdirectory, and select the JWS application, which is usually named *javaws*. Although the exact path and directory names can differ, it might be in a directory named *javaws* or *bin*.

Infoblox CLI

The Infoblox CLI allows you to configure and monitor the device using a small set of Infoblox commands. There are some tasks, such as resetting the device, that you can only do through the CLI. You can access the Infoblox CLI through a direct console connection from your management system to the Infoblox device. You can also enable remote console access—that is, SSHv2 (Secure Shell version 2) access—through the GUI or CLI, and then access the CLI from a remote location using an SSHv2 client.

Using the Console Port

The Infoblox device has a male DB-9 console port on its front panel. You can log in to the device through this port to access the Infoblox CLI.

1. Connect a console cable from the console port on your management system to the console port on the Infoblox device.
2. Using a serial terminal emulation program such as Hilgraeve Hyperterminal® (provided with Windows® operating systems), launch a session. The connection settings are:
   - Bits per second: 9600
   - Data bits: 8
   - Parity: None
   - Stop bits: 1
   - Flow control: Xon/Xoff
3. Log in using the default user name and password *admin* and *infoblox*. User names and passwords are case-sensitive.

Using an SSHv2 Client

In addition to making a direct serial connection to the Infoblox device through its console port, you can also access the Infoblox CLI remotely across a network connection by using an SSHv2 (Secure Shell version 2) client. By default, remote console access (SSHv2 access) is disabled. To access the Infoblox CLI using SSHv2, perform the following steps:

1. Make either an HTTPS or console connection to the Infoblox device, and then log in.
2. To enable remote console access through the GUI:

   From the ID Grid perspective, click *id_grid* -› **Edit** -› **Grid Properties** -› **Security**, select **Enable remote console access**, and then click the **Save** icon.

   From the ID Device perspective, click *hostname* -› **Edit** -› **ID Device Properties** -› **Security**, select **Enable remote console access**, and then click the **Save** icon.

   To enable remote console access through the CLI:

   ```
   Infoblox > set remote_console
   Enable remote console access (grid-level)? (y or n): y
   ```

   Confirm the setting.
3. On the management system, open a remote console connection using an SSHv2 client.
4. In a shell window (or terminal window), log in through SSHv2 using an account with superuser privileges. Enter the user name and host name or IP address of the device. For example: `ssh admin@192.168.1.2`
5. Optionally, you can launch a graphical SSHv2 client and enter the information into the appropriate fields.

Using CLI Help

You can display a list of available CLI commands by typing **help** at the command prompt. For example:

```
> help
    exit            exit command interpreter
    help            display help
    ping            send ICMP ECHO
    reboot          reboot device
    reset           reset system settings
    set             set current system settings
    show            show current system settings
    shutdown        shut down the device
    traceroute      route path diagnostics
    dig             perform a DNS lookup and print the results
```

To view an in-depth explanation of a CLI command and its syntax, type **help *command*** after the command prompt. For example:

```
> help ping
    Synopsis:
    ping [ hostname | IP address ] <numerical>
    Description:
        Send 5 sequential ICMP ECHO requests to a remote host and display the
        results. Use optional <numerical> to avoid DNS lookups.
```

The two main groups of Infoblox CLI commands are `set` and `show`. To see the complete list of the `set` commands, enter **help set** after the command prompt. Likewise, to see a complete list of the `show` commands, enter **help show**.

The following are some CLI commands that you might find particularly useful:

reset all

Resets the system to factory defaults.

set network

Sets the system network settings.

show interface

Displays network interface details.

show network

Displays current network settings.

Configuration Examples

This chapter explains two possible deployment scenarios as examples that you can refer to when setting up your Infoblox-550 appliance:

- *Example 1 – Single Infoblox-550 Appliance for External DNS* on page 15
- *Example 2 – HA Pair for Internal DNS and DHCP* on page 23

To perform the configuration examples in this chapter, you need to use the Infoblox device LCD or console, and the Infoblox GUI and CLI. For management system requirements and an introduction to the Infoblox GUI and CLI, see *Accessing the Device* on page 11.

Example 1 – Single Infoblox-550 Appliance for External DNS

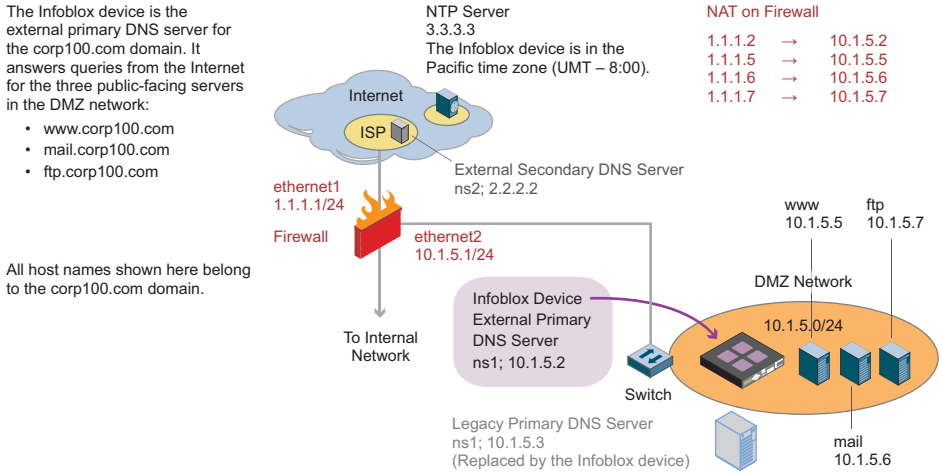
In this example, you configure the Infoblox-550 appliance as the external primary DNS server for corp100.com. Its FQDN (fully-qualified domain name) is ns1.corp100.com. The interface IP address of the LAN1 port is 10.1.5.2/24. Because this is a private IP address, you must also configure the firewall to perform NAT (network address translation), mapping the public IP address 1.1.1.2 to 10.1.5.2. Using its public IP address, ns1 can communicate with devices on the public network.

The FQDN and IP address of the external secondary DNS server are ns2.corp100.com and 2.2.2.2. The ISP hosts this server. The primary and secondary servers answer queries for the following public-facing servers in the DMZ:

- www.corp100.com
- mail.corp100.com
- ftp.corp100.com

When you create the corp100.com zone on the Infoblox-550 appliance, you import zone data from the legacy DNS server at 10.1.5.3.

Figure 7 *Example 1 Network Diagram*



Task 1.1 Cable the Device to the Network and Turn On Power

Connect an ethernet cable from the LAN1 port of the Infoblox-550 appliance to a switch in the DMZ network and turn on the power. See *Installing the Device* on page 9.

Task 1.2 Specify Initial Network Settings

Before you can configure the Infoblox-550 appliance through the GUI, you must be able to make a network connection to it. The default network settings of the LAN1 port are 192.168.1.2/24 with a gateway at 192.168.1.1 (the HA and MGMT ports do not have default network settings). To change these settings to suit your network, use either the LCD or the console port. In this example, you change the IP address/netmask of the LAN1 port to 10.1.5.2/24, and the gateway to 10.1.5.1.

LCD

The Infoblox-550 appliance has an LCD and navigation buttons on its front panel. At startup, the Infoblox logo appears in the LCD on the front panel of the device. Then the LCD scrolls repeatedly through a series of display screens.

1. To change the network settings from the default, press one of the navigation buttons.
   The LCD immediately goes into input mode, in which you can enter the IP address, netmask, and gateway for the LAN1 port.
2. Use the navigation buttons to enter the following information:
   - IP Address: 10.1.5.2
   - Netmask: 255.255.255.0
   - Gateway: 10.1.5.1

Note: To learn how to disable LCD input functionality, see the *Infoblox Administrator Guide*.

Console Port

The Infoblox-550 appliance has a male DB-9 console port on the front panel. You can log in to the device through this port and specify initial network settings using the Infoblox CLI.

1. Connect a console cable from the console port of the management system to the console port of the Infoblox-550 appliance. For more information, see *Using the Console Port* on page 13.
2. Access the Infoblox CLI. For more information, see *Infoblox CLI* on page 13.
3. To change the network settings from the default, enter the **`set network`** command. Then enter information as prompted to change the IP address, netmask, and gateway for the LAN1 port.

```
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 an ID grid.
Enter IP address: 10.1.5.2
Enter netmask: [Default: 255.255.255.0]:
Enter gateway address [Default: 10.1.5.1]:
Become grid member? (y or n): n
```

After you confirm your network settings, the device automatically restarts.

Task 1.3 Specify Device Settings

When you make the initial HTTPS connection to the Infoblox-550 appliance, you see the Appliance Startup Wizard, which guides you through the basic deployment of the device on your network. Use the wizard to enter the following information:

- Deployment: single independent device (standalone node)
- Host name: ns1.corp100.com
- Password: SnD34n534
- NTP (Network Time Protocol) server: 3.3.3.3; time zone: (UMT – 8:00 Pacific Time (US and Canada), Tijuana

Note: For more information about using an NTP server, refer to the *Infoblox Administrator Guide*, or use the integrated online Help and perform a search for "NTP".

1. Open a browser window and enter **https://10.1.5.2**.
2. Accept the certificate when prompted.

   Several certificate warnings appear during the login process. This is normal because the preloaded certificate is self-signed (and, therefore, is not in the trusted certificate stores in your browser, Java application, and Java Web Start application) and has the hostname www.infoblox.com, which does not match the destination IP address you entered in step 1. To stop the warning messages from occurring each time you log in to the GUI, you can generate a new self-signed certificate or import a third-party certificate with a common name that matches the FQDN (fully-qualified domain name) of the device. This is a very simple process. For information about certificates, see the *Infoblox Administrator Guide*.
3. Click **LAUNCH ID DEVICE MANAGER**.
4. If the browser prompts you for an application to use, see *Infoblox GUI* on page 12.
5. Log in using the default user name and password *admin* and *infoblox*.

Note: User names and passwords are case-sensitive.

6. The Infoblox Appliance Startup Wizard opens with a splash screen that provides basic information about the wizard, and then displays license agreement information. Beginning on the third screen, enter the following:

Wizard Screen	Enter or Select
Deployment type	**Standalone**
Node type	**Standalone appliance**
Node information	Host name: **ns1.corp100.com**
Default password	Change admin's password: (select), **SnD34n534**
Time settings	Enable NTP: (select) NTP Server: **3.3.3.3** (click **Add**) Time zone: **(UMT – 8:00 Pacific Time (US and Canada), Tijuana**

The last screen of the wizard states that the changed settings require the application to restart. When you click **Finish**, the Infoblox GUI application restarts.

7. Log back in to the device. When you log in the second time, you access the Infoblox GUI application. For system requirements to use the GUI, see *Table 2* on page 11.

Task 1.4 Define a NAT Address

Because the firewall translates the public IP address 1.1.1.2 to the interface IP address 10.1.5.2, all DNS queries originating outside the firewall use 1.1.1.2 (not 10.1.5.2) to reach the Infoblox device. Accordingly, you must configure the device to indicate to other external DNS servers that its address is 1.1.1.2.

1. From the ID Device perspective, click **ns1.corp100.com -> Edit -> ID Device Properties.**
2. In the *ID Device* editor, click **NAT** and enter the following:
   - Enable NAT compatibility: Select check box.
   - Group: None
   - NAT (V)IP Address: 1.1.1.2
3. Click the **Save** icon.

The glue record is an A record for a name server. The device automatically generates the A record for ns1.corp100.com using either the interface address or NAT address (if configured). To verify that the A record uses the NAT address (1.1.1.2) instead of the interface address (10.1.5.2):

1. Click **DNS** to open the DNS perspective, and then click **DNS Members -> +** (for Infoblox) **-> ns1.corp100.com -> Edit -> Member DNS Properties.**
2. In the Member DNS Properties editor, click **General**.
3. In the table labelled *Member address for glue record inside view*, select the default view and click **Modify**.
4. In the *Select Member Address* dialog box, select **NAT IP address**.
5. Click the **Save** and **Restart Services** icons.

Task 1.5 Enable Zone Transfers on the Legacy Name Server

To allow the device to import zone data from the legacy server at 10.1.5.3, you must configure the legacy server to allow zone transfers to the device at 10.1.5.2.

Legacy BIND Server

1. Open the named.conf file using a text editor and change the allow-transfer statement as shown below:
   For All Zones — To set the allow-transfer statement as a global statement in the named.conf file for all zones:

```
options {
zone-statistics yes;
directory "/var/named/named_conf";
version "";
recursion yes;
listen-on { 127.0.0.1; 10.1.5.3; };
…
allow-transfer { 10.1.5.2; };
transfer-format many-answers;
};
```

For a Single Zone — To set the allow-transfer statement in the named.conf file for the corp100.com zone:

```
zone "corp100.com" in {
type master;
allow-transfer { 10.1.5.2; };
notify yes;
};
```

2. After editing the named.conf file, restart DNS service for the change to take effect.

Legacy Windows 2000/2003 Server

1. Click **Start** -› **All Programs** -› **Administrative Tools** -› **DNS**.
2. Click **+** (for ns1) -› **+** (for Forward Lookup Zones) -› **corp100.com**.
3. Right-click **corp100.com**, and then select **Properties** -› **Zone Transfers**.
4. On the *Zone Transfers* page in the *corp100.com Properties* dialog box, enter the following:
   - Allow zone transfers: Select check box.
   - Only to the following servers: Select.
   - IP address: Enter **10.1.5.2**, and then click **Add**.
5. To save the configuration change and close the *corp100.com Properties* dialog box, click **OK**.

Task 1.6 Import Zone Data

You can import zone data from a legacy server or manually enter it. When you import both forward- and reverse-mapping zone data, the Infoblox device automatically creates Infoblox host records if corresponding A and PTR records are present. You can then modify the host records to add MAC addresses. However, if you only import forward-mapping zone data, the Infoblox device cannot create host records from just the A records. In that case, because you cannot later convert A records to host records, it is more efficient to create the corp100.com zone, and define host records manually.

Infoblox host records are data models that represent IP devices within the Infoblox semantic database. The Infoblox device uses a host object to define A, PTR, and CNAME resource records in a single object as well as a DHCP fixed address if you include a MAC address in the host object definition. The host object prevents costly errors because you only maintain a single object for multiple DNS records and a DHCP fixed address. Therefore, it is advantageous to use host records instead of separate A, PTR, and CNAME records.

Note: If you only have forward-mapping zones on your legacy servers and you want to add reverse-mapping zones and automatically convert A records to host records in the imported forward-mapping zones and create reverse host records in corresponding reverse-mapping zones, create the reverse-mapping zones on the Infoblox device and then import the forward-mapping zones data. The Infoblox device automatically converts the imported A records to host records in the forward-mapping zones and creates reverse host records in the reverse-mapping zones.

You also have the option of using the Data Import Wizard for loading DNS and DHCP configurations and data. For large data sets, this option is an efficient approach. To download the Data Import Wizard, visit www.infoblox.com/support, log in with your support account, and then click the **Data Import Wizard** hyperlink.

In this example, when you create the corp100.com forward-mapping zone, you import zone data for the existing corp100.com zone from the legacy server at 10.1.5.3. When you create the 1.1.1.0/24 reverse-mapping zone, you also import the reverse-mapping zone records from the legacy server. After the device has both the forward- and reverse-mapping zone data, it converts the A and PTR records to Infoblox host records.

1. Open a browser window, and log in to the device at https://10.1.5.2, using the user name *admin* and the password *SnD34n534*.
2. From the DNS perspective, click **Infoblox Views** -› **+** (for Infoblox Views) -› **+** (for default) -› **Forward Mapping Zones** -› **Edit** -› **Add Forward Mapping Zone** -› **Authoritative**.
3. In the *Authoritative Zone Properties* section of the *Add Forward Authoritative Zone* editor, enter the following:
   - Name: corp100.com
   - Comment: External DNS zone
4. In the *Primary* Server *Assignment* section, click **Select Member** to open the *Select ID Grid Member* dialog box.
5. Select **ns1.corp100.com**, and then click **OK** to close the dialog box.
6. In the *Secondary Server Assignment* section, click **Add** in the External Secondaries table to open the *Zone External Secondary Server* dialog box.
7. Enter the following information, and then click **OK** to close the dialog box:
   - Name: ns2.corp100.com
   - IP Address: 2.2.2.2
   - Stealth: Clear check box.
8. Click the **Save** icon.
9. In the *Infoblox Views* panel of the DNS perspective, click **+** (for Forward Mapping Zones) -› **corp100.com** -› **Edit** -› **Authoritative Zone Properties**.
10. In the *Forward Authoritative Zone* editor, click **Settings** and enter the following:
    - E-mail address: admin@corp100.com
    - Import zone from: Select check box, and enter **10.1.5.3** in the adjacent text field.
11. Click the **Save** icon.
12. After successfully importing the zone data, click **corp100.com** in the *Infoblox Views* panel.

    You can see all the imported forward-mapping zone data in the *Records* panel. Because you have not yet imported the reverse-mapping zone data, most of the records appear as A records.
13. From the DNS perspective, click **Infoblox Views** -› **+** (for Infoblox Views) -› **+** (for default) -› **Reverse Mapping Zones** -› **Edit** -› **Add Reverse Mapping Zone** -› **Authoritative**.
14. In the *Authoritative Zone Properties* section of the *Add Reverse Authoritative Zone* editor, enter the following:
    - Network Address: 1.1.1.0
    - Subnet Mask: /24 (255.255.255.0)
    - Comment: External DNS zone
15. In the *Primary* Server *Assignment* section, click **Select Member** to open the *Select ID Grid Member* dialog box.
16. Select **ns1.corp100.com**, and then click **OK** to close the dialog box.
17. In the *Secondary Server Assignment* section, click **Add** in the External Secondaries table to open the *Zone External Secondary Server* dialog box.

18. Enter the following information, and then click **OK** to close the dialog box:
    - Name: ns2.corp100.com
    - IP Address: 2.2.2.2
    - Stealth: Clear check box.
19. Click the **Save** icon.
20. In the Infoblox Views panel of the DNS perspective, click **+** (for Reverse Mapping Zones) -> **1.1.1.in-addr.arpa** -> **Edit** -> **Authoritative Zone Properties**.
21. In the *Authoritative Reverse Zone* editor, click **Settings** and enter the following:
    - E-mail address: admin@corp100.com
    - Import zone from: Select check box, and enter **10.1.5.3** in the adjacent text field.
22. Click the **Save** and **Restart Services** icons.
23. Click **1.1.1.in-addr.arpa** -> **View** -> **Records**.
    You can see all the imported reverse-mapping zone data in the *Records* panel.
24. Click **corp100.com** in the Forward Mapping Zones list.
    Because you have now imported both the forward- and reverse-mapping zone data, most of the records appear as host records.
25. Finally, you must remove the ns1 host record for the legacy server (value 1.1.1.3). To remove it, select **ns1** (the host record for 1.1.1.3), and then click **Edit** -> **Remove**.

Task 1.7 Designate the New Primary on the Secondary Name Server (at the ISP Site)

In this example, the external secondary name server is maintained by an ISP, so you must contact your ISP administrator to change the IP address of the primary (or *master*) name server. (If you have administrative access to the secondary name server, you can make this change yourself.)

Because a firewall performing NAT exists between the secondary and primary name servers, specify the NAT address 1.1.1.2 for the primary name server instead of 10.1.5.2.

Secondary BIND Server

1. Open the named.conf file using a text editor and set ns1 (with NAT address 1.1.1.2) as the primary (or *master*) from which ns2 receives zone transfers in the named.conf file for the corp100.com zone:

```
zone "corp100.com" in {
type slave;
masters { 1.1.1.2; };
notify yes;
file “/var/named/db.corp100.com”;
};
```

2. After editing the named.conf file, restart DNS service for the change to take effect.

Secondary Windows 2000/2003 Server

1. Click **Start** -> **All Programs** -> **Administrative Tools** -> **DNS**.
2. Click **+** (for ns2) -> **+** (for Forward Lookup Zones) -> **corp100.com**.
3. Right-click **corp100.com**, and then select **Properties** -> **General**.

4. On the *General* page in the *corp100.com Properties* dialog box, enter the following:
   - Zone file name: corp100.com.dns
   - IP address: Enter **1.1.1.2**, and then click **Add**.
   - In the IP Address field, select **1.1.1.3** (the NAT IP address of the legacy DNS server), and then click **Remove**.
5. To save the configuration change and close the *corp100.com Properties* dialog box, click **OK**.

Task 1.8 Configure NAT and Policies on the Firewall

Change the NAT and policy settings on the firewall to allow bidirectional DNS traffic to and from ns1.corp100.com and NTP traffic from ns1.corp100.com to the NTP server at 3.3.3.3.

For example, enter the following commands on a Juniper firewall running ScreenOS 4.x or later:

```
set address dmz ns1 10.1.5.2/32
set address untrust ntp_server 3.3.3.3/32
set interface ethernet1 mip 1.1.1.2 host 10.1.5.2
set policy from dmz to untrust ns1 any dns permit
set policy from untrust to dmz any mip(1.1.1.2) dns permit
set policy from dmz to untrust ns1 ntp_server ntp permit
```

At this point, the new DNS server can take over DNS service from the legacy server. You can remove the legacy server and unset any firewall policies permitting traffic to and from 10.1.5.3.

Example 2 – HA Pair for Internal DNS and DHCP

In this example, you set up an HA pair of Infoblox-550 appliances to provide internal DNS and DHCP services. The HA pair answers internal queries for all hosts in its domain (corp100.com). It forwards internal queries for external sites to ns1.corp100.com at 10.1.5.2 and ns2.corp100.com at 2.2.2.2. It also uses DHCP to provide dynamic and fixed addresses.

The HA pair consists of two devices (nodes). The IP addresses of the VIP (virtual IP) address of the HA pair and the HA and LAN1 ports on each node, are as follows:

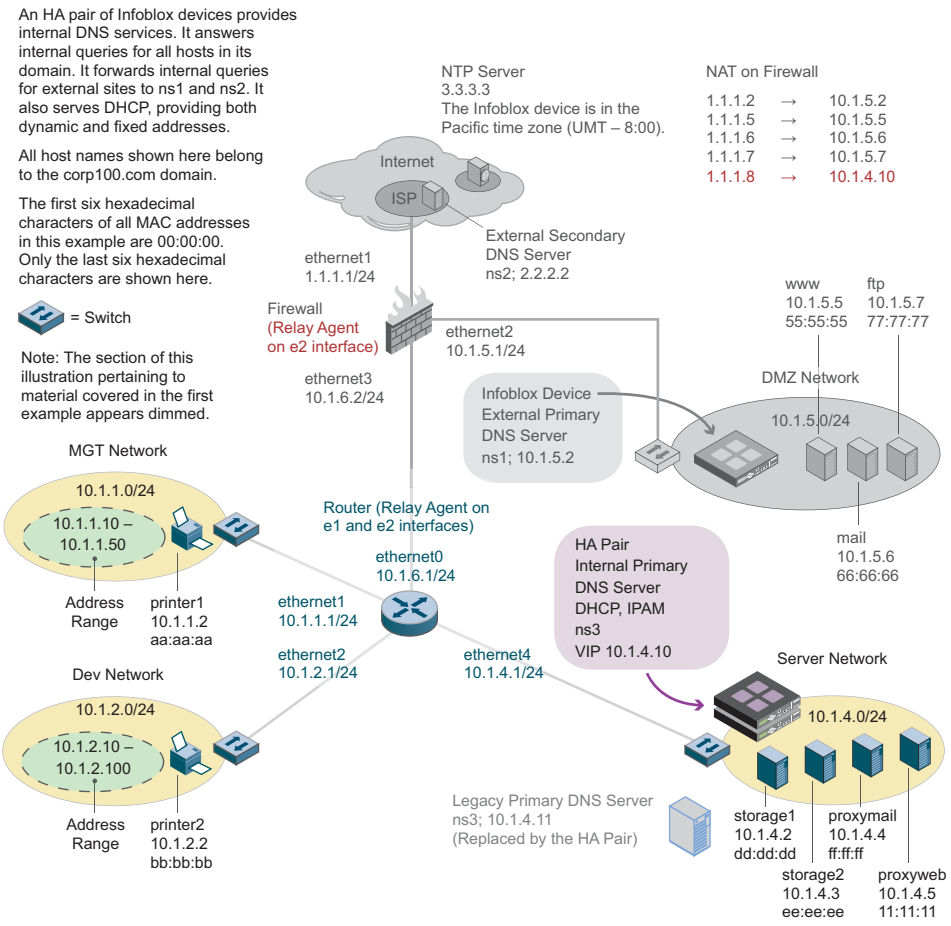
HA Pair IP Addresses

VIP: 10.1.4.10 (the address that the active node of the HA pair uses)	
Node 1	Node 2
• LAN1: 10.1.4.6 • HA: 10.1.4.7	• LAN1: 10.1.4.8 • HA: 10.1.4.9

The virtual router ID number for the HA pair is 150. (The ID number must be unique for this network segment.)

When you create the corp100.com zone on the HA pair, you import DNS data from the legacy server at 10.1.4.11.

Figure 8 *Example 2 Network Diagram*



Task 2.1 Cable Devices to the Network and Turn On Power

Connect ethernet cables from the LAN1 and HA ports on both Infoblox-550 appliances to a switch in the Server network and turn on the power for both devices. See *Installing the Device* on page 9.

Task 2.2 Specify Initial Network Settings

Before you can configure the devices through the GUI, you must be able to make a network connection to them. The default network settings of the LAN1 port are 192.168.1.2/24 with a gateway at 192.168.1.1 (the HA and MGMT ports do not have default network settings). To change these settings, you can use the LCD or make a console connection to each device.

Note: For details about using the LCD, see *Task 1.2 Specify Initial Network Settings* on page 16. For details on using the console, see *Accessing the Device* on page 11 first, and then *Console Port* on page 16.

Node 1

Using the LCD or console port on one of the devices, enter the following information:

- IP Address: 10.1.4.6 (for the LAN1 port)
- Netmask: 255.255.255.0
- Gateway: 10.1.4.1

Node 2

Using the LCD or console port on the other device, enter the following information:

- IP Address: 10.1.4.8 (for the LAN1 port)
- Netmask: 255.255.255.0
- Gateway: 10.1.4.1

After you confirm your network settings, the Infoblox GUI application automatically restarts.

Task 2.3 Specify Device Settings

When you make the initial HTTPS connection to an Infoblox device, you see the Infoblox Appliance Startup Wizard, which guides you through the basic deployment of the device on your network. To set up an HA pair, you must connect to and configure each device individually.

Node 1

1. Open a browser window and connect to https://10.1.4.6.

   Note: For details about making an HTTPS connection to an Infoblox device, see *Task 1.3 Specify Device Settings* on page 17.

2. Log in using the default user name and password *admin* and *infoblox*.

   Note: User names and passwords are case-sensitive.

3. The Infoblox Appliance Startup Wizard opens with a splash screen that provides basic information about the wizard, and then displays license agreement information. Beginning on the third wizard screen, enter or select the following to set up node 1 of the HA pair:

Wizard Screen	Enter
Deployment type	**Stand alone**
Node type	**First HA node**
ID Grid information	ID Grid Name: **Infoblox** Shared Secret: **37eeT1d** (Note: The nodes use the shared secret to form an encrypted VPN tunnel between themselves. They synchronize the shared database through this tunnel.)

Wizard Screen	Enter
Node information	Virtual IP: **10.1.4.10** Subnet Mask: **255.255.255.0** Gateway: **10.1.4.1** Host Name: **ns3.corp100.com** Node 1: • LAN1 Address: **10.1.4.6** • HA Address: **10.1.4.7** Node 2: • LAN1 Address: **10.1.4.8** • HA Address: **10.1.4.9** Virtual Router ID: **150**
Default password	New admin password: **SnD34n534**
Time settings	Enable NTP: Select check box. IP address: **3.3.3.3** Time zone: **(UMT – 8:00 Pacific Time (US and Canada), Tijuana**

The last screen of the wizard states that the changed settings require the application to restart. When you click **Finish**, the Infoblox GUI application restarts.

Node 2

1. In the JWS (Java Web Start) login window, type **10.1.4.8** in the Hostname field.

   When you enter the IP address, JWS queries the device at that address, checking for a login banner. The following default Infoblox banner appears above the Hostname field: “Restricted Access – Login Required”.
2. Log in using the default user name and password *admin* and *infoblox*.

Note: User names and passwords are case-sensitive.

3. The Infoblox Appliance Startup Wizard opens with a splash screen that provides basic information about the wizard, and then displays license agreement information. Beginning on the third wizard screen, enter or select the following to set up node 2 of the HA pair:

Wizard Screen	Enter or Select
Deployment type	**Stand alone**
Node type	**Second HA node**
Node information	IP Address: **10.1.4.8** Subnet Mask: **255.255.255.0** Gateway: **10.1.4.1**

Wizard Screen	Enter or Select
Node provisioning	Master's Virtual IP: **10.1.4.10** ID Grid Name: **Infoblox** Shared Secret: **37eeT1d**

On the last screen of the wizard, click **Finish**. The Infoblox GUI application terminates.

The setup of the HA pair is complete. From now on, when you make an HTTPS connection to the HA pair, use the VIP address 10.1.4.10.

Task 2.4 Enable Zone Transfers on the Legacy Name Server

To allow the Infoblox device to import zone data from the legacy server at 10.1.4.11, you must configure the legacy server to allow zone transfers to the device at 10.1.4.10.

Legacy BIND Server

1. Open the named.conf file using a text editor and change the allow-transfer statement to allow zone transfers to the device at 10.1.4.10. (For a sample of the required changes to the named.conf file, see *Legacy BIND Server* on page 18.)
2. After editing the named.conf file, restart DNS service for the change to take effect.

Legacy Windows 2000/2003 Server

Navigate to the *corp100.com Properties* dialog box, and add 10.1.4.10 to the list of IP addresses to which you want to allow zone transfers. (For more detailed navigation and configuration instructions, see *Legacy Windows 2000/2003 Server* on page 19.)

Task 2.5 Import Zone Data

You can import zone data from a legacy server or manually enter it. When you import both forward- and reverse-mapping zone data, the Infoblox device automatically creates Infoblox host records if corresponding A and PTR records are present. You can then modify the host records to add MAC addresses. However, if you only import forward-mapping zone data, the Infoblox device cannot create host records from just the A records. In that case, because you cannot later convert A records to host records, it is more efficient to create the corp100.com zone, and define host records manually.

Infoblox host records are data models that represent IP devices within the Infoblox semantic database. The Infoblox device uses a host object to define A, PTR, and CNAME resource records in a single object as well as a DHCP fixed address if you include a MAC address in the host object definition. The host object prevents costly errors because you only maintain a single object for multiple DNS records and a DHCP fixed address. Therefore, it is advantageous to use host records instead of separate A, PTR, and CNAME records.

Note: If you only have forward-mapping zones defined on your legacy servers and you want to add reverse-mapping zones and automatically create host records in the imported forward-mapping zones and reverse host records in corresponding reverse-mapping zones, create the reverse-mapping zones and then import the forward-mapping zones data. The Infoblox device automatically converts the imported A records to host records in the forward-mapping zones and creates the necessary reverse host records in the reverse-mapping zones.

You also have the option of using the Data Import Wizard for loading DNS and DHCP configurations and data. For large data sets, this option is an efficient approach. To download the Data Import Wizard, visit www.infoblox.com/support, log in with your support account, and then click the **Data Import Wizard** hyperlink.

In this example, when you create the corp100.com forward-mapping zone, you import zone data for the existing corp100.com zone from the legacy server at 10.1.4.11. When you create the 1.10.in-addr.arpa reverse-mapping zone, you also import the zone records for the existing 1.10.in-addr.arpa zone from the legacy server. After the device has both the forward- and reverse-mapping zone data, it converts the A and PTR records to Infoblox host records.

1. Open a browser window, and log in to the HA pair at https://10.1.4.10, using the user name *admin* and the password *SnD34n534*.
2. To check that the HA pair is set up and functioning properly, from the ID Device perspective, click **ns3.corp100.com** and check that the status indicators are all green.
3. Click **DNS** to open the DNS perspective, and then click **Infoblox Views** -> **+** (for Infoblox Views) -> **+** (for default) -> **Forward Mapping Zones** -> **Edit** -> **Add Forward Mapping Zone** -> **Authoritative**.
4. In the *Authoritative Zone Properties* section of the *Add Forward Authoritative Zone* editor, enter the following:
   - Name: corp100.com
   - Comment: Internal DNS zone
5. In the *Primary* Server *Assignment* section, click **Select Member** to open the *Select ID Grid Member* dialog box.
6. Select **ns3.corp100.com**, and then click **OK** to close the dialog box.
7. Click the **Save** icon.
8. In the *Infoblox Views* panel of the DNS perspective, click **+** (for Forward Mapping Zones) -> **corp100.com** -> **Edit** -> **Authoritative Zone Properties**.
9. In the *Forward Authoritative Zone* editor, click **Settings** and enter the following:
   - E-mail address: admin@corp100.com
   - Import zone from: Select check box, and enter **10.1.4.11** in the adjacent text field.
10. Click the **Save** icon.
11. After successfully importing the zone data, click **corp100.com** in the *Infoblox Views* panel.

    You can see all the imported forward-mapping zone data in the *Records* panel. Because you have not yet imported the reverse-mapping zone data, most of the records appear as A records.
12. From the DNS perspective, click **Infoblox Views** -> **+** (for Infoblox Views) -> **+** (for default) -> **Reverse Mapping Zones** -> **Edit** -> **Add Reverse Mapping Zone** -> **Authoritative**.
13. In the *Authoritative Zone Properties* section of the *Add Reverse Authoritative Zone* editor, enter the following:
    - Network Address: 10.1.0.0
    - Subnet Mask: 255.255.0.0
    - Comment: Internal DNS zone
14. In the *Primary* Server *Assignment* section, click **Select Member** to open the *Select ID Grid Member* dialog box.
15. Select **ns3.corp100.com**, and then click **OK** to close the dialog box.
16. Click the **Save** icon.
17. In the *Infoblox Views* panel of the DNS perspective, click **+** (for Reverse Mapping Zones) -> **1.1.1.in-addr.arpa** -> **Edit** -> **Authoritative Zone Properties**.

18. In the *Authoritative Reverse Zone* editor, click **Settings** and enter the following:
    - E-mail address: admin@corp100.com
    - Import zone from: Select check box, and enter **10.1.4.11** in the adjacent text field.
19. Click the **Save** and **Restart Services** icons.
20. Click **1.1.1.in-addr.arpa -› View -› Records**.

    You can see all the imported reverse-mapping zone data in the *Records* panel.
21. Click **corp100.com** in the *Infoblox Views* panel.

    Because you have now imported both the forward- and reverse-mapping zone data, most of the records appear as host records.
22. Finally, you must remove the ns1 host record for the legacy server (value 10.1.4.11). To remove it, select **ns3**, and then click **Edit -› Remove**.

Task 2.6 Define Networks, Reverse-Mapping Zones, DHCP Ranges, and Infoblox Hosts

In this task, you enter data manually because the configuration is fairly simple. For large data sets, you have the option of using the Data Import Wizard for loading DNS and DHCP configurations and data to make the process more efficient. To download the Data Import Wizard, visit www.infoblox.com/support, log in with your support account, and then click the **Data Import Wizard** hyperlink.

Networks

You can create all the subnetworks individually (which in this example are 10.1.1.0/24, 10.1.2.0/24, 10.1.4.0/24, and 10.1.5.0/24), or you can create a parent network (10.1.0.0/16) that encompasses all the subnetworks and then use the Infoblox split network feature to create the individual subnetworks automatically. The split network feature accomplishes this by using the IP addresses that exist in the forward-mapping zones to determine which subnets it needs to create. This example uses the split network feature. For information about creating networks, see the *Infoblox Administrator Guide*.

1. From the DHCP and IPAM perspective, click **Networks -› Edit -› Add Network -› Network**.
2. In the *Network Properties* section of the *Add Configure Network* editor, enter the following:
    - Network Address: 10.1.0.0
    - Netmask: /16 (255.255.0.0)
3. Click **Member Assignment -› Add** to open the the *Select ID Grid Members* dialog box.
4. Select **ns3.corp100.com**, and then click **OK** to close the dialog box.
5. Click the **Save** icon.
6. Click **+** (for Networks) **-› 10.1.0.0/16 -› Edit -› Split Network**.
    - Subnetworks: Move the slider to 24.
    - Immediately add only networks with ranges and fixed addresses: Select check box.

    The device immediately creates the following 24-bit subnets for the imported Infoblox hosts:
    - 10.1.1.0/24
    - 10.1.2.0/24
    - 10.1.4.0/24
    - 10.1.5.0/24
7. Click **-› +** (for Networks) **-› +** (for 10.1.0.0/16) **-› 10.1.1.0/24 -› Edit -› Network Properties**.

8. In the *Configure Network* editor, enter information in the following sections:
   Network Properties
   - Comment: MGT

   Member Assignment
   - Members: ns3.corp100.com
9. Click the **Save** icon.
10. To modify the other networks, repeat steps #8 – 10 for each network and use the following information:
    10.1.2.0/24 Network:
    - Comment: Dev
    - Members: ns3.corp100.com

    10.1.4.0/24 Network:
    - Comment: Server
    - Members: ns3.corp100.com

    10.1.5.0/24 Network:
    - Comment: DMZ
    - Members: ns3.corp100.com

Reverse-Mapping Zones

When you create a network, the device automatically creates a corresponding reverse-mapping zone and "reparents" the relevant resource records from the parent zone (10.1.0.0/16) to that zone. To enable DNS service for the new zone, you need to assign ns3.corp100.com as the primary DNS server for each zone. In this example, the device creates four reverse-mapping zones. You must modify each zone by assigning ns3.corp100.com as its primary DNS server.

1. From the DNS perspective, click **Infoblox Views** -> **+** (for Infoblox Views) -> **+** (for default) -> **+** (for Reverse Mapping Zones) -> **+** (for 1.10.in-addr.arpa) -> **1.1.10.in-addr.arpa** -> **Edit** -> **Authoritative Zone Properties**.
2. In the *Primary Server Assignment* section, click **Select Member** to open the *Select ID Grid Member* dialog box.
3. Select **ns3.corp100.com**, and then click **OK** to close the dialog box.
4. Click the **Save** icon.
5. Repeat steps #1–4 for the 2.1.10.in-addr.arpa, 4.1.10.in-addr.arpa, and 5.1.10.in-addr.arpa reverse-mapping zones.

DHCP Ranges

1. From the DHCP and IPAM Perspective, select **Networks** -> **+** (for Networks) -> **+** (for 10.1.0.0/16) -> **10.1.1.0/24** -> **Edit** -> **Add DHCP Range**.
2. In the *DHCP Range* section, enter the following:
   - Start Address: 10.1.1.10
   - End Address: 10.1.1.50
3. In the *Member Assignment* section, select **ns3.corp100.com** from the ID Grid Member drop-down list.
4. Click the **Save** icon.

5. From the DHCP and IPAM Perspective, select **Networks -> +** (for Networks) **-> +** (for 10.1.0.0/16) **-> 10.1.2.0/24 -> Edit -> Add DHCP Range**.
6. In the *DHCP Range* section, enter the following:
   - Start Address: 10.1.2.10
   - End Address: 10.1.2.100
7. In the *Member Assignment* section, select **ns3.corp100.com** from the ID Grid Member drop-down list.
8. Click the **Save** icon.

Infoblox Hosts

Defining both a MAC and IP address for an Infoblox host definition creates a DHCP host entry—like a fixed address—that you can manage through the host object. To add a MAC address to each host record that the device created when you imported forward- and reverse-mapping zone records, you must first delete the IP address for that host, and then add the same IP address with the MAC address.

1. From the DNS perspective, click **Infoblox Views -> +** (for Infoblox Views) **-> +** (for default) **-> +** (for Forward Mapping Zones) **-> +** (for corp100.com**).**
2. Double-click **10.1.1.2** to open the *Host* editor.
3. In the *Host Record Properties* section, select **10.1.1.2**, and then click **Remove**.
4. Click **Add** next to the IP Address field to open the *Host Address* dialog box.
5. Enter the following, and then click **OK** to close the dialog box:
   - IP Address: 10.1.1.2
   - MAC Address: 00:00:00:aa:aa:aa
6. Click the **Save** icon.
7. Follow steps 1 – 6 to modify hosts with the following information:

   printer2
   - IP Address: 10.1.2.2
   - MAC Address: 00:00:00:bb:bb:bb

   storage1
   - IP Address: 10.1.4.2
   - MAC Address: 00:00:00:dd:dd:dd

   storage2
   - IP Address: 10.1.4.3
   - MAC Address: 00:00:00:ee:ee:ee

   proxymail
   - IP Address: 10.1.4.4
   - MAC Address: 00:00:00:ff:ff:ff

   proxyweb
   - IP Address: 10.1.4.5
   - MAC Address: 00:00:00:11:11:11

www
- IP Address: 10.1.5.5
- MAC Address: 00:00:00:55:55:55

mail
- IP Address: 10.1.5.6
- MAC Address: 00:00:00:66:66:66

ftp
- IP Address: 10.1.5.7
- MAC Address: 00:00:00:77:77:77

Task 2.7 Define Multiple Forwarders

Because ns3.corp100.com is an internal DNS server, you configure it to forward DNS queries for external DNS name resolution to the primary and secondary DNS servers—ns1.corp100.com at 10.1.5.2 and ns2.corp100.com at 2.2.2.2.

Note: You must also configure ns1 and ns2 DNS servers to allow recursion when resolving DNS queries on behalf of ns3. For information, see *Task 2.8 Enable Recursion on External DNS Servers*.

---

1. From the DNS perspective, click **DNS Members -> Infoblox -> Edit -> Grid DNS Properties**.
2. In the *ID Grid DNS Properties* editor, click **Forwarders**, and then enter the following:
   - IP Address: Type **2.2.2.2**, and then click **Add**.
   - IP Address: Type **10.1.5.2**, and then click **Add**.
   - Use Forwarders Only: Clear check box.
3. Click the **Save** icon.

The Infoblox device initially sends outbound queries to forwarders in the order that they appear in the Forwarders list, starting from the top of the list. If the first forwarder does not reply, the device tries the second one. The device keeps track of the response time of both forwarders and uses the quicker one for future queries. If the quicker forwarder does not respond, the device then uses the other one.

Task 2.8 Enable Recursion on External DNS Servers

Because the HA pair forwards outbound queries to the two external DNS servers ns1.corp100.com (10.1.5.2) and ns2.corp100.com (2.2.2.2) for resolution, you must enable recursion on those servers. When a DNS server employs recursion, it queries other DNS servers for a domain name until it either receives the requested data or an error that the requested data cannot be found. It then reports the result back to the querist—in this case, the internal DNS server ns3.corp100.com (10.1.4.10), which in turn reports back to the DNS client.

Infoblox Server in the DMZ Network (ns1.corp100.com, 10.1.5.2)

1. Log in to ns1.corp100.com at 10.1.5.2.
2. From the DNS perspective, click **DNS Members -> Infoblox -> Edit -> Grid DNS Properties**.
3. In the **ID Grid DNS Properties** editor, click **Queries**, and then select the **Allow Recursion** check box.
4. Click the **Save** icon.

BIND Server at ISP Site (ns2.corp100.com, 2.2.2.2)

1. Open the named.conf file using a text editor and change the recursion and allow-recursion statements to allow recursive queries from 1.1.1.8 (the NAT address of ns3).

```
options {
zone-statistics yes;
directory "/var/named/named_conf";
version  "";
recursion yes;
listen-on { 127.0.0.1; 2.2.2.2; };
…
allow-recursion { 1.1.1.8; };
transfer-format many-answers;
};
```

2. After editing the named.conf file, restart DNS service for the change to take effect.

Windows 2000/2003 Server at ISP Site (ns2.corp100.com, 2.2.2.2)

1. Click **Start -› All Programs -› Administrative Tools -› DNS**.
2. Right-click **ns3**, and then select **Properties -› Advanced**.
3. On the *Advanced* page in the *ns3 Properties* dialog box, clear the **Disable recursion** check box.
4. To save the configuration change and close the *ns3 Properties* dialog box, click **OK**.

Task 2.9 Modify the Firewall and Router Configurations

Configure the firewall and router in your internal network to allow the following DHCP, DNS, and NTP traffic:

- To allow messages to pass from the DHCP clients in the DMZ—the web, mail, and FTP servers—to ns3 in the Server network, configure policies and DHCP relay agent settings on the firewall.
- To forward DHCP messages from DHCP clients in the MGT and Dev networks to ns3 in the Server network, configure relay agent settings on the router.
- To translate the private IP address of ns3 (10.1.4.10) to the public IP address (1.1.1.8) when forwarding DNS queries from ns3 to ns2, set a MIP (mapped IP) address on the firewall.
- To allow DNS queries from ns3 to ns1 and ns2 and NTP traffic from ns3 to the NTP server, configure firewall policies.

Firewall

For example, enter the following commands on a Juniper firewall running ScreenOS 4.x or later:

DHCP Relay Configuration

```
set address trust ns3 10.1.4.10/32
set interface ethernet2 dhcp relay server-name 10.1.4.10
set policy from dmz to trust ns1 ns3 DHCP-Relay permit
```

DNS Forwarding

```
set interface ethernet1 mip 1.1.1.8 host 10.1.4.10
set policy from trust to untrust ns3 ns2 dns permit
set policy from trust to dmz ns3 ns1 dns permit
```

NTP

```
set policy from dmz to untrust ns1 ntp_server ntp permit
```

Router

For example, enter the following commands on a Cisco router running IOS for release 12.x or later:

DHCP Relay Configuration

```
interface ethernet1
    ip helper-address 10.1.4.10
interface ethernet2
    ip helper-address 10.1.4.10
```

Task 2.10 Enable DHCP and Switch Service to the Infoblox Device

With the Infoblox in place and the firewall and router configured for relaying DHCP messages, you can switch DHCP service from the legacy DHCP server at 10.1.4.11 to the HA pair at 10.1.4.10 (VIP address).

Tip: To minimize the chance of duplicate IP address assignments during the transition from the legacy DHCP server to the device, shorten all lease times to a one-hour length in advance of the DHCP server switch. Then, when you take the legacy DHCP server offline, the DHCP clients quickly move to the new server when their lease renewal efforts fail and they broadcast DHCPDISCOVER messages. To determine how far in advance you need to shorten the lease length, find the longest lease time (for example, it might be two days). Then change the lease length to one hour at a slightly greater interval of time before you plan to switch DNS service to the device (for example, three days before the switch over). By changing the lease length this far in advance, you can be sure that all DHCP leases will be one-hour leases at the time of the switchover. If the longest lease length is longer—such as five days—and you want to avoid the increased amount of traffic caused by more frequent lease renewals over a six-day period, you can also employ a stepped approach: Six days before the switchover, change the lease lengths to one-day leases. Then two days before the switchover, change them to one-hour leases.

---

1. Open a browser window, and log in to the HA pair at https://10.1.4.10, using the user name *admin* and the password *SnD34n534*.
2. From the DHCP and IPAM Perspective, select **DHCP Members** -› **+** (for Infoblox) -› **ns3.corp100.com** -› **Edit** -› **Member DHCP Properties**.
3. In the *Member DHCP Properties* editor, click **General Properties** and select **Enable DHCP Server**.
4. Click the **Save** and **Restart Services** icons.

   The HA pair is ready to provide DHCP service to the network.
5. Take the legacy DHCP server at 10.1.4.11 offline.

   When the DHCP clients are unable to renew their leases from the legacy DHCP server, they broadcast DHCPDISCOVER messages to which the new DHCP server responds.

Task 2.11 Manage and Monitor

Infoblox provides tools for managing IP address usage and several types of logs to view events of interest and DHCP and DNS data. After configuring the device, you can use the following resources to manage and monitor IP address usage, DNS and DHCP data, and administrator and device activity.

IPAM (IP Address Management)

IPAM offers the following services:

- Simple IP address modification – Within a single IP address-centric data set, you can modify the Infoblox host, DHCP, and DNS settings associated with that IP address.
- Address type conversion — Through IPAM functionality, you can make the following conversions:
  - Currently active dynamic addresses -› fixed addresses, reserved addresses, or Infoblox hosts
  - Fixed addresses -› reserved addresses or hosts
  - Reserved addresses -› hosts
- Device classification – You can make detailed descriptions of devices in DHCP ranges and devices defined as Infoblox hosts and as fixed addresses.
- Three distinct views of IP address usage – To monitor the usage of IP addresses on your network, you can see the following different views:
  - High-level overall network view: From the DHCP and IPAM perspective, click **DHCP Members -› +** (for Infoblox) **-› 10.1.4.10 -› View -› IPAM Statistics**.
  - Run-time view that allows you to zoom in and out to varying levels of detail: From the DHCP and IPAM perspective, click **Networks** -› *network* **-› View -› IP Address Management** -› *ip_addr* **-› View -› Properties.**
  - DHCP lease history records: From the DHCP and IPAM perspective, click **View -› DHCP Lease History**.

Note: For more information about IPAM functionality, see the *Infoblox Administrator Guide*.

Logs

The following are some useful logs:

- Logs
  - Audit Log – Contains administrator-initiated events
  - System Log – Contains events related to hardware and software operations
- IPAM
  - IPAM Statistics – Contains the number of currently assigned static and dynamic addresses, and the high and low watermarks per network
- DNS
  - DNS Cache – Contains cached DNS-to-IP address mappings
  - DNS Configuration – Contains DNS server settings for the Infoblox DNS server
  - Zone Statistics – Contains a record of the results of all DNS queries per zone

- DHCP
  - DHCP Configuration – Contains DHCP server settings and network, DHCP range, and host settings for the Infoblox DHCP server
  - DHCP Leases – Contains a real-time record of DHCP leases
  - DHCP Lease History – Contains an historical record of DHCP leases
  - DHCP Statistics – Contains the number of static hosts, dynamic hosts, and available hosts per network

Joining an ID Grid

An Infoblox-550 appliance running NIOS 4.0 with the DNSone package and the Keystone upgrade can be a member of an ID grid. You can join a single Infoblox-550 appliance to a grid or you can join two Infoblox-550 appliances in an HA pair. In the former case, the device becomes a single grid member. In the latter case, the pair becomes an HA member. For information about setting up an ID grid, refer to the *Infoblox Administrator Guide*. For information about adding the Infoblox-550 appliance to a grid, see the following instructions.

Adding a single device or an HA pair to an ID grid involves two basic steps:

1. On the ID grid master, add the device or HA pair as a new grid member.
2. On the single device or HA pair, join it to the grid.

You can use the above procedure to add a device or HA pair to a grid, but it erases all existing data and configurations from the device or HA pair. This procedure is suitable for an initial deployment or if you do not need to retain any existing data. If you want to retain some or all of an existing data and configuration on the device or HA pair, you must do two additional steps:

1. Save a backup file of the device or HA pair to your local management system.
2. On the ID grid master, add the device or HA pair as a new grid member.
3. On the ID grid master, merge the backup file data with the grid database.
4. On the single device or HA pair, join it to the grid.

The complete procedure is presented below. If you do not need to retain any data or configuration settings, perform only *Task 2 Add a New Grid Member* and *Task 4 Join the ID Grid*.

Task 1 Create a Backup File

On the device or HA pair whose data you want to merge with an ID grid database:

1. Create a backup file by opening the ID Grid perspective and then clicking **ID Grid -> Backup -> to Local File**.
2. Save the backup file as *filename*.tar.gz on your local management system.

Task 2 Add a New Grid Member

On the ID grid master:

1. From the ID Grid perspective, click *id_grid* -> **Edit** -> **Add Grid Member**.
2. In the *Add ID Grid Member* dialog box, enter the host name and network settings for the device or HA pair that you want to add to the grid, and then click the **Save** icon.

Task 3 Merge the Backup File

On the ID grid master:

1. Merge the backup file from the single device or HA pair with that of the ID grid by clicking **ID Grid -> Merge Database**.

   The *Merge Database* dialog box appears.

Note: In the *Merge Database* dialog box, you can click the **Backup** button to back up the current database for the ID grid. Infoblox strongly recommends that you create a backup file before proceeding.

2. In the *Merge Database* dialog box, enter the following:
   - **New data overwrites current data:** Select the check box if you want the DNS, DHCP, and global and member properties from the device or HA pair to overwrite matching data on the ID grid. Exceptions to this are user profiles (with matching user names but mismatching passwords) and ID grid-level settings for DHCP failover. In these cases, the new data does not overwrite existing data. Clear the check box to merge only that data that does not conflict with existing data.
   - **Merge in DNS data:** Select the check box to merge the DNS information, such as DNS properties and all the zone information.
   - **Merge in DHCP data:** Select the check box to merge the DHCP information.
   - **Merge in ID grid and member properties:** Select the check box to merge global and member properties, and system administration information.
   - **Detailed Logging:** Select the check box to log errors and all transactions during the merge. Clear this option to log errors only. (To view the system log: From the ID Grid perspective, click *grid_master* -› **File** -› **System Log** -› *active_node*.)
3. Click **OK**.
4. Type the location of the backup file or navigate to the file and select it, and then click **OK**.
   After the merge process completes, the Infoblox application restarts and the JWS (Java Web Start) application terminates.
5. Wait a few minutes, and then log back in to the ID grid master from the JWS login prompt.

Task 4 Join the ID Grid

On the device or HA pair you want to join to an ID grid:

1. From the ID Grid perspective, click **+** (for *id_grid*) -› **+** (for Members) -› *member* -› **Edit** -› **Join ID Grid**.
2. Enter the following in the *Join ID Grid* dialog box:
   - **Virtual IP of Grid Master:** Type the VIP address of the grid master for the ID grid to which you want to add the single device or HA pair.
   - **Grid Name:** Type the name of the ID grid.
   - **Grid Shared Secret:** Type the shared secret of the ID grid.
   - **Re-type Grid Shared Secret:** To ensure accuracy, retype the shared secret.
   - **Use MGMT port to join grid:** If you have already enabled the MGMT port, this option becomes available. Select it to connect to the ID grid through the MGMT port.

Note: For information about using the MGMT port, refer to the *Infoblox Administrator Guide*.

3. Click **OK** to close the dialog box and initiate the join grid operation.

You can monitor the status of the join grid operation by looking at the *Detailed Status*, *Upgrade Status*, and *Replication Status* viewers in the ID Grid perspective on the grid master.