Infoblox
NEXT LEVEL NETWORKING

DEPLOYMENT GUIDE

NetMRI and Operations Center

Copyright Statements

The information in this document is subject to change without notice. Infoblox, Inc. shall not be liable for any damages resulting from technical errors or omissions which may be present in this document, or from use of this document.

Trademark Statements

Infoblox, the Infoblox logo, Grid, NIOS, bloxTools, NetMRI and PortIQ are trademarks or registered trademarks of Infoblox Inc.

All other trademarked names used herein are the properties of their respective owners and are used for identification purposes only.

Company Information

http://www.infoblox.com/contact/

Product Information

Hardware Models

NetMRI: NetMRI-1102-A, NT-1400, NT-2200, and NT-4000

Infoblox Advanced Appliances: PT-1400, PT-2200, PT-4000, and PT-4000-10GE

Network Insight Appliances: ND-800, ND-1400, ND-2200, and ND-4000

Trinzic Appliances: TE-100, TE-810, TE-820, TE-1410, TE-1420, TE-2210, TE-2220, Infoblox-4010, and Infoblox-4020

All Trinzic Rev-1 and Rev-2 appliances

Cloud NetMRI: CP-V800, CP-V1400, and CP-V2200

Trinzic Reporting: TR-800, TR-1400, TR-2200, and TR-4000

DNS Cache Acceleration Appliances: IB-4030 and IB-4030-10GE

Document Number: 400-0275-000 Rev. D

Document Updated: January 11, 2018

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 the Infoblox Web site, or contact Infoblox Technical Support.

Table of Contents

Preface. 5

Document Overview 5

Documentation Conventions. 5

Navigation 6

Related Documentation. 6

Customer Care 6

User Accounts 6

Software Upgrades 6

Technical Support 6

Before You Start. 7

Obtaining Valid Licenses. 7

Security Registration 7

Chapter 1 Deploying a Standalone NetMRI Appliance 9

Ethernet Connections 9

Connecting NetMRI to the Network 10

Configuring the Workstation. 10

Chapter 2 Deploying a NetMRI Virtual Appliance 11

Benefits of Deploying NetMRI as a Virtual Appliance 11

NetMRI Virtual Appliance Installation Worksheet 12

Best Practices for configuring NetMRI Virtual Appliances. 13

Benchmarking the VMware Infrastructure 13

Overview of the Benchmarking Suite 14

System Requirements for the Benchmarking Suite. 14

Installing the Benchmarking Suite 14

Interpreting the Benchmarking Suite Results 15

Installing a Standalone NetMRI Virtual Appliance. 15

Downloading and Unpacking the Virtual Appliance ZIP Archive. 15

Importing the Virtual Appliance Files 16

Installing on vSphere/vCenter5.x/6.x and ESXi 5.x/6.x 16

Installing on VMware Workstation 10.x and Later. 16

Installing on VMware Player 16
Installing All Other Versions 17
Configuring the NetMRI Virtual Appliance 17
Adding Processors, Memory and Storage 17
Adding vCPUs 17
Adding Memory 18
Adding Storage 18

Chapter 3 Configuring NetMRI 19

Configuring Network Interfaces 19
Configuring NetMRI Using the Setup Wizard 20
Setup Wizard: Admin Password 21
Setup Wizard: License 21
Setup Wizard: Welcome 21
Setup Wizard: Discovery Ranges 21
Setup Wizard: Static IPs 22
Setup Wizard: CLI Credentials 22
Setup Wizard: SNMP v1/2 Credentials. 23
Setup Wizard: SNMP v3 Credentials. 23
Setup Wizard: Seed Routers 23
Setup Wizard: Device Type Hints 24
Setup Wizard: Device Interrogation Techniques 24
Setup Wizard: Configuration Collection 24
Setup Wizard: Summary 24
Monitoring the Initial Discovery Process 25
Troubleshooting Discovery 25
Additional Considerations 25
Domain Name Assignment 25
Accessing Using HTTPS 25
Using NetMRI 26
Shutdown Procedure 26
Resetting to Factory Defaults 26

Chapter 4 Deploying the Operations Center 27

Operations Center Requirements 28
Recommended Best Practices. 28
Connecting NetMRI to the Network (Hardware Appliances Only) 29
Configuring the UI Client 30
Configuring the NetMRI Appliance for IPv6 30
Deploying Automatic Failover for New Appliances 32
Migrating Existing Systems as Failover Pairs. 33
Installing NetMRI Operations Center 34
Installing the Operations Center Software. 34
Configuring the Operations Center Controller for Factory Defaults 34
Configuring An Operations Center Controller From an Existing NetMRI Instance 35
Operations Center Command-Line Setup. 36
Running the Setup Wizard 37
Setup Wizard: Admin Setup 37
Setup Wizard: License Install (Operations Center Only) 37
Setup Wizard: Welcome 37
Setup Wizard: Discovery Ranges 38
Setup Wizard: Static IPs 38

Setup Wizard: CLI Credentials 39
Setup Wizard: SNMPv1/2 Credentials 39
Setup Wizard: SNMPv3 Credentials (Rare). 40
Setup Wizard: Seed Routers 40
Setup Wizard: Device Type Hints 41
Setup Wizard: Device Interrogation Techniques 41
Setup Wizard: Configuration Collection 41
Setup Wizard: Summary 42
Additional Considerations 42
Domain Name Assignment 42
HTTPS Accessibility 42
Shutdown Procedure 42
Resetting to Factory Defaults 42
Discovery Import Formats 43
Range Examples 43
Static IP Examples 44
Seed Router Examples 44
Credential Import Formats 44
Configuring NetMRI Collectors 45
NetMRI Virtual Appliance Installation Worksheet 46
Installing NetMRI Virtual Appliances (for Collectors). 47
Downloading and Unpacking the Virtual Appliance ZIP Archive 48
Installing on vSphere/vCenter 5.x/6.x and ESXi 5.x/6.x 48
Configuring and Registering NetMRI Collectors. 49
Monitoring the Initial Discovery Process 50
Troubleshooting 50
Reviewing Operations Center Configuration Details 51
Adding More Resources 51

Chapter 5 Deploying Automatic Failover 53

Deploying Automatic Failover for New Appliances 53
Migrating Existing Systems as Failover Pairs. 54

Preface

This preface describes the document conventions of this guide, and describes how to find additional product information, including accessing Infoblox Technical Support. It includes the following sections:

- *Document Overview* on page 5
- *Related Documentation* on page 6
- *Customer Care* on page 6
- *Before You Start* on page 7

Document Overview

This guide describes how to deploy and configure NetMRI appliances. It was last updated on January 11, 2018. For updated documentation, visit our Support site at the following location:

https://support.infoblox.com

Documentation Conventions

The text in this guide follows the following style conventions.

Style	Usage
bold	• Indicates anything that you input in the user interface, by clicking, choosing, selecting, typing, or by pressing on the keyboard. • Indicates field names in the user interface. • Indicates variable and argument names in SNMP, Perl and other languages.
`input`	Signifies command line entries that you type, contents of text files, and operating system screen text.
variable	Signifies variables typed into the user interface that you need to modify specifically for your configuration. These can be command line variables, file names, and keyboard characters. Indicates the names of the wizards, editors, and dialog boxes in Grid Manager, such as the *Add Network* wizard or the *DHCP Network* editor.

Navigation

Infoblox technical documentation uses an arrow " –> " to represent navigation through the user interface. For example, to edit a fixed address, the description is as follows:

> From the **Data Management** tab, select the **DHCP** tab –> **Networks** tab –> **Networks** –> *network* –> *fixed_address* check box, and then click the Edit icon.

Related Documentation

Other Infoblox appliance documentation includes the following:

- *Infoblox NetMRI Administrator Guide*
- *Infoblox NetMRI CCS Scripting Guide*
- *Infoblox NetMRI API Guide*
- *Infoblox Installation Guide for the NetMRI 1102-A Appliance*
- *Infoblox Installation Guide for the NetMRI NT-4000 Appliance*
- *Infoblox Installation Guide for the NetMRI NT-2200 Appliances*
- *Infoblox Installation Guide for the NetMRI NT-1400 Appliances*

To provide feedback on any Infoblox technical documents, please e-mail *techpubs@infoblox.com*.

Customer Care

This section addresses user accounts, software upgrades, licenses and warranties, and technical support.

User Accounts

The Infoblox appliance ships with a default user name and password. Change the default `admin` account password immediately after the system is installed to safeguard its use. Make sure that the NetMRI appliance has at least one administrator account with superuser privileges at all times, and keep a record of your account information in a safe place. If you lose the `admin` account password, and did not already create another superuser account, the system will need to be reset to factory defaults, causing you to lose all existing data on the NIOS appliance. You can create new administrator accounts, with or without superuser privileges. For more information, see the *Creating Admin and User Accounts* section in the *Infoblox NetMRI Administrator Guide*.

Software Upgrades

Software upgrades are available according to the Terms of Sale for your system. Infoblox notifies you when an upgrade is available. Register immediately with Infoblox Technical Support at http://www.infoblox.com/en/support/product-registration.html to fully utilize your Technical Support.

Technical Support

Infoblox Technical Support provides assistance via the Web, e-mail, and telephone. The Infoblox Support web site at http://www.infoblox.com/en/support/support-center-login.html provides access to product documentation and release notes, but requires the user ID and password you receive when you register your product online at: http://www.infoblox.com/en/support/product-registration.html.

Before You Start

Obtaining Valid Licenses

Contact Infoblox Technical Support or your Infoblox representatives to obtain valid licenses for NetMRI and other related features.

Security Registration

NetMRI is designed to continuously gather data from critical devices throughout your network. Such behavior, however, will often be detected by the various security devices and monitoring processes already scattered throughout your network. Therefore, it is important to register your NetMRI IP address appropriately with each of the security services across your network. Furthermore, in order to access SNMP ports on some devices, you may need to add the NetMRI IP address to the Access Control List (ACL) on those devices.

Chapter 1 Deploying a Standalone NetMRI Appliance

This chapter provides information about how to deploy NetMRI on a traditional hardware-based appliance. The appliance on which NetMRI runs should be supported by an uninterruptible power supply (UPS) to avoid data corruption problems should there be a power outage. Contact your Infoblox representatives about the different NetMRI hardware appliance models.

Complete the following to install NetMRI on your physical appliance:

1. Consider your Ethernet connections, as described in *Ethernet Connections* on page 9.
2. Connect the NetMRI appliance to the network, as described in *Connecting NetMRI to the Network* on page 10.
3. Configure your workstation to connect to the NetMRI appliance, as described in *Configuring the Workstation* on page 10.
4. Configure NetMRI on your appliance, as described in *Configuring NetMRI* on page 19.

Ethernet Connections

Each NetMRI Network Analysis Appliance is equipped with two Ethernet ports, labeled MGMT and SCAN. By default, the NetMRI appliance is configured to use the MGMT port for both system administration and network analysis functions (the latter involves accessing network devices).

In some environments, system administration and network analysis must take place through different appliance ports for one or both of the following reasons:

- Security.
- To enable management service providers to access NetMRI from remote locations

Before installing your NetMRI appliance, decide whether it should be set up to use one Ethernet port or two. Separate instructions for these cases are provided at the appropriate points in the next chapter.

Connecting NetMRI to the Network

The NetMRI appliance does not need a monitor, keyboard, or mouse for normal operation—it only needs an Ethernet connection.

Follow these steps to connect NetMRI to your network:

1. **If you are configuring the appliance to use one port** (same port for both system administration and network analysis): Use a straight-through RJ45 Ethernet cable to connect the MGMT Ethernet connector to an available Ethernet connection on your network.

   or

   If you are configuring the appliance to use two ports (one for system administration and one for network analysis), use a straight-through RJ45 Ethernet cables and complete the following:

   a. Connect the MGMT Ethernet connector to the network supporting your management systems.

   b. Connect the SCAN Ethernet connector to an available Ethernet port on the network NetMRI will be analyzing.

   Note: The NetMRI appliance models support 10/100/1000Mbps network connections.

2. After completing your Ethernet connection, simply plug the NetMRI appliance into an AC power source.
3. Verify that the green Link LED on the RJ45 port is lit, indicating a good connection to your network. If possible, verify that the link indicator is lit on the network hub or switch port to which NetMRI is connected.

   Note: NetMRI and the workstation that is used for this configuration process must be connected to the same subnet or VLAN for the process to be successful.

Configuring the Workstation

NetMRI always listens on the private IP address **169.254.1.1** and subnet mask **255.255.255.0**, which can be used at any time to configure NetMRI using the following procedure. The easiest way to access NetMRI on that address is to temporarily configure your workstation to use address **169.254.1.5**, subnet mask **255.255.255.0**.The process for Windows XP is described here, but it may be slightly different for different versions of Windows or other operating systems:

1. From the **Start** menu button, select **Control Panel**.
2. In the **Control Panel** dialog, click **Network Connections**.
3. In the **Network Connections** dialog, click **Local Area Connection**.
4. In the **Local Area Connections Status** dialog, click **Properties**.
5. In the **Local Area Connection Properties** dialog, click **Internet Protocol (TCP/IP)** in the **Network Components** list, and then click the **Properties** button.
6. In the **Internet Protocol (TCP/IP) Properties** dialog, fill in the **IP address** and **Subnet mask** fields with an IP address of **169.254.1.5** and subnet mask of **255.255.255.0**. Click the **OK** buttons in the **Internet Protocol (TCP/IP) Properties** and **Local Area Connection Properties** dialog boxes. (For some versions of Windows, you might need to reboot your computer.)

   Note: This IP address change is only necessary for initial setup. Once the setup is complete, you should return your workstation to its prior configuration.

7. Access NetMRI at 169.254.1.1 using SSH.
8. Log in with user name **`admin`** and password **`admin`**.
9. Configure NetMRI on your appliance, as described in *Configuring NetMRI* on page 19.

Chapter 2 Deploying a NetMRI Virtual Appliance

This chapter provides information about how to install and deploy the NetMRI virtual appliance on a VMware Infrastructure virtual machine. Since VMware installation parameters and hardware configurations vary, this chapter is meant as a guide to configurations that have worked well for NetMRI installations. It addresses the following deployment scenarios:

- Running NetMRI in a VMware Infrastructure.
- Moving NetMRI from a physical NetMRI appliance to a VMware Infrastructure.

This chapter provides prerequisites and procedures to successfully complete the following:

- Prepare the VMware Infrastructure for a NetMRI installation.
- Install and configure the NetMRI virtual appliance.

While Infoblox has made the deployment of NetMRI as a virtual appliance as simple as possible by including the OS, patches and all required tools, you still need to configure the VM server based on your business requirements. For information about VMware, refer to the official VMware documentation at *http://www.vmware.com/*.

Benefits of Deploying NetMRI as a Virtual Appliance

You can download and run NetMRI as a virtual appliance within a VMware virtual machine. The virtual appliance comes bundled with all required system components, simplifying installation. There is no need to install and maintain an operating system or database.

NetMRI as a virtual appliance dynamically scales with the VM (Virtual Machine) resources provisioned to meet the needs of different customer requirements, allowing greater flexibility than the traditional appliance. In short, the NetMRI virtual appliance provides all the benefits of a virtual machine, combined with all of the convenience of a physical appliance.

The NetMRI virtual appliance provides the following benefits:

- Reduce data center footprints and provide scalability to NetMRI.
- House multiple NetMRI Collectors on one VM server.
- Deploy an Operations Center to collect data from multiple remote NetMRI Collectors.

Note: The hardware on which NetMRI runs should be supported by an uninterruptible power supply (UPS) to avoid data corruption problems should there be a power outage.

NetMRI Virtual Appliance Installation Worksheet

Installing a NetMRI virtual appliance involves various procedures, and you might need to skip instructions that do not apply. The following worksheet helps you navigate through the instructions. Infoblox strongly recommend that you use the worksheet while deploying a NetMRI virtual appliance.

	Step	Procedure	Reference
□	1.	Review best practices and verify that the VMware platform on which NetMRI will be deployed adheres to the recommendations.	*Best Practices for configuring NetMRI Virtual Appliances*
□	2.	Review the recommended VMware server requirements and record the following information: Number of devices to be monitored: ________ Number of interfaces to be monitored: ________ VMware hypervisor: ________ Number of vCPUs: ________ Memory available: ________ Size of local disk storage: ________	*System Requirements for the Benchmarking Suite*
□	3.	Install and run the VM Benchmarking Suite on the VMware server.	*Overview of the Benchmarking Suite*
□	4.	Confirm that the platform meets NetMRI virtual appliance requirements: MySQL Bench Alter Table Result: _____ seconds (should be less than 15 seconds) MySQL Bench Create Result: ________ seconds (should be less than 30 seconds) MySQL Bench Wisconsin Result: _____seconds (should be less than 7 seconds)	*System Requirements for the Benchmarking Suite*
□	5.	Download and unpack the NetMRI virtual appliance zip archive.	*Downloading and Unpacking the Virtual Appliance ZIP Archive*
□	6.	Import the NetMRI virtual appliance files. Follow the instructions in the sub section for the Appliance Distributable downloaded in zip file.	*Importing the Virtual Appliance Files*
□	7.	Configure the NetMRI virtual appliance.	*Configuring NetMRI*
□	8.	Configure NetMRI network interface. NetMRI IP address is now: __________________________	*Configuring Network Interfaces*
□	9.	Configure NetMRI using the Setup Wizard.	*Configuring NetMRI Using the Setup Wizard*
□	10.	Monitor the initial discovery process.	*Monitoring the Initial Discovery Process*
□	11.	Review additional considerations to determine whether additional security should be placed around the NetMRI installation.	*Additional Considerations*

Best Practices for configuring NetMRI Virtual Appliances

This section outlines the best practices that have been found specific to NetMRI virtual appliance installation on a VMware server:

- AMD Processors

  Issue: Hardware platforms using AMD processors may present performance bottlenecks to VMware running NetMRI, in certain cases.

  Recommendation: Avoid AMD processor hardware if at all possible. If this is not feasible, pay attention to the results of the platform benchmark and resolve any issues before installing NetMRI.

- Disk Performance

  Issue: In high-performance applications, such as high license count deployments, NetMRI can be I/O intensive. If multiple applications are configured to access the same physical disk, NetMRI can experience significant read/write delays that might degrade its performance.

  Recommendation: Provision NetMRI to use dedicated disks/spindles.

- Processors with Hardware Virtualization Support

  Issue: NetMRI benefits greatly from the hardware virtualization support included in the latest generation processors. Performance of older generations of processors may not be suitable for high-performance applications, such as high license count deployments.

  Recommendation: Run NetMRI on the latest generation of processors having hardware virtualization support. Intel i7 based servers have been shown to be particularly effective.

- Server Performance Monitoring

  Issue: NetMRI is a high-performance network analysis system that can be different than the enterprise applications you regularly monitor. It may use CPUs intensely for extended periods of time and may exceed the CPU thresholds currently set on server performance monitoring applications.

  Recommendation: If monitoring is set up for your VMware server, you may need to raise or eliminate the alert threshold values for NetMRI to eliminate unnecessary alarms.

- vCPU Allocation

  Issue: Due to context-switching overhead, allocating more vCPUs to NetMRI may hurt performance.

  Recommendation: Adhere to the recommended vCPU allocation parameters listed in *Adding vCPUs* on page 17. If system performance is suffering, check the CPU Ready State times. If times are high, try reducing the number of vCPUs and see if that helps. If times are low, try increasing vCPUs. For additional information relative to vCPU allocation, refer to the documentation on Performance Best Practices for VMware vSphere.

- Memory Allocation

  Issue: Additional memory helps almost any application. If memory can be increased for the NetMRI virtual appliance without over-subscribing, that will help performance.

  Recommendation: It is recommended you adhere to at least the recommended memory allocation parameters set forth in *Adding Memory* on page 18.

Benchmarking the VMware Infrastructure

VMware servers and their performance can vary widely. The NetMRI virtual appliance is a very I/O-intensive program and requires high I/O performance. Infoblox has compiled a suite of industry standard tests for benchmarking the platform on which NetMRI will be installed.

The Benchmarking Suite runs on your VM server and performs a platform benchmark of your VMware server. The platform benchmark is specifically designed for gathering information that will be useful in predicting the performance of a NetMRI installation, but is also useful in predicting the performance of other I/O-intensive applications on your VM server.

Overview of the Benchmarking Suite

The Infoblox VM Platform Benchmarking Suite is a fully configured instance of the Infoblox Benchmarking Suite that runs on your hardware under VMware. The Suite contains the files necessary for you to import the Infoblox VM Platform Benchmarking Suite into any of the following VMware products:

- VMware ESXi 5.x or 6.x managed hosts (vCenter or Virtual Center)
- VMware ESXi 5.x or 6.x (standalone)

System Requirements for the Benchmarking Suite

The minimum requirements for the Infoblox VM Platform Benchmarking Suite are:

- 2.4 GHz CPU
- 512MB Memory
- 10GB Storage.

Installing the Benchmarking Suite

The following sections outline how to install the Benching Suite:

Unpacking the Benchmarking Suite

If you downloaded an .ova package, you will need to unzip the contents of the Infoblox VM Platform Benchmarking Suite ZIP archive file into an appropriate directory.

Importing the Benchmarking Suite

1. Start your VMware Virtual Infrastructure Client and connect to your ESXi or vSphere/vCenter server.
2. In the **Inventory** tab, click the ESXi host on which you want to place the virtual appliance.
3. Go to **File** -> **Virtual Appliance** -> **Import...** . The *Import Virtual Appliance Wizard* is displayed.
4. Choose **Import** from file and click the **Browse** button.
5. Select the .ova file that was unpacked and click **Open**.
6. Click **Next** and then click **Next** again.
7. Enter the name for the VM and click **Next.**
8. Choose a data store for the VM and click **Next.**
9. Choose the network that you would like to use and click **Next**. This will be the management network for the VM and may also serve as the network to be scanned. If you want to use a second network for scanning, you may add an additional adapter at a later time.
10. Verify that your settings are correct and click **Finish**.

Running the Benchmarking Suite

Note: An IP address is automatically assigned to the Benchmark Suite VM created above by DHCP by default. You can assign a static IP address by using the process outlined at www.infoblox.com/en/products/netmri/virtualapplianceFAQ.html.

1. Log in to the IP address assigned to your virtual machine via DHCP or manually. The username is benchmarked against the password benchmark.
2. Decide which benchmark tests you want to run:
    a. The **full** option will run a comprehensive benchmark on the system, which takes about one-and-a-half to two hours to complete.

   b. The **quick** option will only run database tests and takes about 20 to 30 minutes to complete.

3. After logging into the command line, type **full** or **quick**.
4. After the benchmark completes, you can view and download results by pointing your web browser to the VM IP address. For example, if your VM is on IP address 192.168.1.1, enter http://192.168.1.1 to view and download results.
5. Save your results in a spreadsheet after each run.

Note: You may want to run the benchmark more than once to ensure that you are getting consistent results.

Interpreting the Benchmarking Suite Results

The Benchmarking Suite returns measurements in 19 separate categories: 11 categories from the Phoronix Test Suite (http://www.phoronix-test-suite.com) and eight categories from the MySQL Bench benchmarking suite (http://dev.mysql.com/downloads). Three measurements in particular are important for establishing that the platform will provide a suitable environment for NetMRI. They are:

- **MySQL-Bench Alter Table:** Acceptable values will be approximately 10 seconds or less. Poor system performance may result if results returned are 25 seconds or more. If the result on your system is greater than 15 seconds, please confirm you are following all of the best practices outlined in *Best Practices for configuring NetMRI Virtual Appliances* on page 13.
- **MySQL-Bench Create:** Results for this test can vary greatly between approximately 20 seconds to more than 10 minutes. NetMRI uses many temporary tables in its processing. The lower the number here, the better the performance of NetMRI will be in allocating temporary tables. If the result on your system is greater than 30 seconds, please confirm you are following all of the best practices outlined in *Best Practices for configuring NetMRI Virtual Appliances* on page 13.
- **MySQL-Bench Wisconsin:** Results for the Wisconsin test—which tests relatively complex queries—can also vary greatly. Results can vary from approximately 4 seconds to more than 3 minutes. NetMRI uses hundreds of complex queries in its operation. The lower the number, the better the performance of NetMRI queries is likely to be. If the result on your system is greater than 7 seconds, please confirm you are following all of the best practices outlined in *Best Practices for configuring NetMRI Virtual Appliances* on page 13.

If you have confirmed you are following the best practices outlined in *Best Practices for configuring NetMRI Virtual Appliances* on page 13, and you are still experiencing results greater than the results outlined above, please contact Infoblox for further analysis. If there is an issue, Infoblox will want to review the complete set of measurements, as the other 16 measurements are useful in troubleshooting.

Installing a Standalone NetMRI Virtual Appliance

Complete the following to install a NetMRI virtual appliance:

1. Download and unpack the virtual appliance zip archive, as described in *Downloading and Unpacking the Virtual Appliance ZIP Archive* on page 15.
2. Import the virtual appliance files, as described in *Importing the Virtual Appliance Files* on page 16.
3. Configure the NetMRI virtual appliance, as described in *Configuring the NetMRI Virtual Appliance* on page 17.

Downloading and Unpacking the Virtual Appliance ZIP Archive

You can add additional vCPUs to the NetMRI VM in accordance with the VMware administration guide. No additional configuration of NetMRI is required when adding additional processors.

Complete the following to download and unpack the NetMRI VM:

1. Download the appropriate Appliance distributable according to the following table:

VMware version	Zip (VMX)	OVF 1.0	OVA
vSphere/vCenter 5.x/6.x (ESXi 5.x/6.x managed hosts)		✓	✓
ESXi 5.x/6.x Standalone		✓	✓
VMware Workstation, Player 10.x and later	✓		
VMware Fusion 8.x and later	✓		

2. If you download an OVF version, unzip the file into a directory on your computer.
3. Install the distributable according to the corresponding instructions in the next section.

Importing the Virtual Appliance Files

Follow the instructions corresponding to the appliance distributable you obtained in the previous section.

Installing on vSphere/vCenter5.x/6.x and ESXi 5.x/6.x

Do the following:

1. Download the .zip archive containing the appropriate OVA/OVF NetMRI virtual appliance template and unzip it into a directory on your computer.
2. Import the unzipped OVA/OVF template using either VMware vSphere Client or VMware vSphere/ESXi Web Client. For more information on the OVA/OVF import into VMware vSphere/vCenter/ESXi environments, refer to VMware documentation.

   The NetMRI virtual appliance is installed on your ESXi host. Installation may take 10-20 minutes, depending on your hardware and network speed.

Complete the installation process by configuring NetMRI on the appliance, as described in *Configuring NetMRI* on page 19.

Installing on VMware Workstation 10.x and Later

1. Download the.zip archive containing the appropriate VMX/VMDK NetMRI virtual appliance and unzip it into a directory on your computer.
2. Open the unzipped VMX/VMDK NetMRI virtual appliance in VMware Workstation. For more information on running VMX/VMDK virtual appliances on VMware Workstation, refer to VMware documentation.

   The new VM is displayed in a tab in the VMware Workstation’s main window.

Complete the installation process by configuring NetMRI on the appliance, as described in *Configuring NetMRI* on page 19.

Installing on VMware Player

Note: Use of VMware Player is not recommended on a production instance of the NetMRI virtual appliance. VMware Player should only be used for testing purposes.

1. Download the .zip archive containing the appropriate VMX/VMDK NetMRI virtual appliance and unzip it into a directory on your computer.
2. Start VMware Player.
3. Click **Open**.
4. Select the .VMX file, then click **Open**.

5. The Player will import and run your virtual appliance.
6. Complete the installation as described in *Configuring the NetMRI Virtual Appliance* on page 17.

Installing All Other Versions

1. In your VMware application, click **File › Open**.
2. Browse to the directory where you unzipped your virtual appliance.
3. Open the*.VMX* file.
4. Work through the Setup Wizard.
5. Complete the installation as described in *Configuring the NetMRI Virtual Appliance* on page 17.

Configuring the NetMRI Virtual Appliance

After installing the NetMRI appliance, follow the instructions below to configure it to run on your network.

1. Log in to VMware Virtual Center, ESX, Workstation, etc.
2. Power on the NetMRI virtual appliance you imported earlier.
3. Open the console view of your NetMRI virtual appliance.
4. After the initial boot, you will see a license agreement. Read the agreement (press SPACE to page down). At the prompt, enter **`yes`**, and then press ENTER.
5. The boot will continue for about five minutes as the NetMRI application configures itself.
6. When the blue screen is displayed, select **Log in** using the arrow keys, then press ENTER.
7. Enter the default user name **`admin`** and the default password **`admin`**. This puts you in the admin shell of NetMRI, a command line interface.

   Note: You can change the password later when running through NetMRI browser-based interface.

8. Complete the installation process by configuration NetMRI on your virtual appliance, as described in *Configuring NetMRI* on page 19.

Adding Processors, Memory and Storage

One benefit of installing NetMRI as a virtual appliance is the ability to dynamically allocate additional resources to NetMRI. Additional resources can be in the form of additional vCPUs, additional memory, and/or additional storage for NetMRI. The following section describes each resource:

Adding vCPUs

Adding additional vCPUs to the NetMRI virtual appliance should be done in accordance with the VMware administration guide. No additional configuration of NetMRI is needed when adding additional processors.

Keep in mind that more is not always better. Due to context-switching, adding additional vCPUs to NetMRI may actually hurt overall performance.

Adding Memory

Allocating additional memory to the NetMRI virtual appliance should be done in accordance with the VMware administration guide. If the amount of memory being added to NetMRI exceeds 3.6 GB, then NetMRI will need to have the PAE kernel enabled. Download the latest version of NetMRI, and then update in the admin shell using procedures provided in the “Manually updating NetMRI software” section of the NetMRI online help or Administrator Guide.

Adding Storage

Allocating additional storage to the NetMRI virtual appliance should be done by adding storage as RDM or VMDK-based disks. Configure the disks as additional storage in NetMRI by following the steps outlined in the “Settings” -> “NetMRI Database section” -> “Storage Management” topic in the NetMRI online help or Administrator Guide.

Chapter 3 Configuring NetMRI

This chapter provides configuration information for completing the NetMRI installation process, whether you have installed NetMRI on a hardware appliance or as a virtual appliance.

It includes the following sections:

- *Configuring Network Interfaces* on page 19
- *Configuring NetMRI Using the Setup Wizard* on page 20
- *Monitoring the Initial Discovery Process* on page 25
- *Additional Considerations* on page 25

Configuring Network Interfaces

If you are using DHCP with NetMRI, record the IP address that is assigned to NetMRI, and then continue the configuration as described in *Configuring NetMRI Using the Setup Wizard* on page 20.

If you are configuring a static IP for NetMRI, complete the following:

1. At the CLI (command line interface) command prompt, enter **`configure ip`**, and then complete the following:
   — Enter the Management IP Address: The IPv4 address of the management interface of the NetMRI, e.g., **`192.168.10.10`**.
   — Enter the Management Subnet Mask: The subnet mask of the management interface of the NetMRI, e.g., **`255.255.255.0`**.
   — Enter the Management Gateway Address: The IPv4 default gateway of the management interface of the NetMRI, e.g, **`192.168.10.1`**.
   — Enter the Primary DNS Server: The primary DNS server for the NetMRI to query, e.g., **`172.23.16.20`**.
   — Enter the Primary DNS Domain: The DNS domain name for the NetMRI, e.g., **`infoblox.local`**.
2. In the **`Current Settings`** section, review your entries.
3. At the **`Edit these settings? <y/n> [n]`** prompt, enter **n** and then press ENTER.
4. At the **`Configure these IP settings? <y/n> [y]`** prompt, enter **y** to configure the IP settings. Wait while NetMRI configures the network and sets the web interface to use the new IP address.
5. When prompted, enter **y** to complete the configuration.
6. At the command prompt, enter **`configure server`**, and then complete the following (values you entered in the configure ip command will be the default values here):
   — Type **y** to continue.
   — Enter your network name: e.g., **`MyNetwork`**.

- Enter your server name: e.g., **MyNetMRI**.
- Enter your domain name(s).
- Enter a time server if applicable.
- Enter the time zone region to be used for timestamps within NetMRI.
- Enter the location within your time zone region.
- Enter NetMRI IP address.
- Enter the Subnet Mask for NetMRI.
- Enter the IPv6 address if applicable.
- Enter the IPv6 prefix if applicable.
- Enter your default gateway for NetMRI.
- Enter the IPv6 default gateway if applicable.
- Enter **n** for the scan port.
- Enter the DNS server(s) for NetMRI.
- Review your settings. If you accept the settings, enter **n**.
- Enter **y** to configure the server with the settings you just entered. Wait while NetMRI configures the network and sets the web interface to use the new IP address.
- When prompted, enter **y**.
- Restart the server and reboot.
- At the shell prompt, type **exit** to log out.

Configuring NetMRI Using the Setup Wizard

The Setup Wizard provides a multi-step process for configuring NetMRI. As shown in the table below, steps in the Wizard depend on whether you choose to use auto discovery in the **Welcome** step.

Step	Auto Discovery	No Auto Discovery
Setup Wizard: Admin Password on page 21	✓	✓
Setup Wizard: License on page 21	✓	✓
Setup Wizard: Welcome on page 21	✓	✓
Setup Wizard: Discovery Ranges on page 21	✓	
Setup Wizard: Static IPs on page 22	✓	✓
Setup Wizard: CLI Credentials on page 22	✓	✓
Setup Wizard: SNMP v1/2 Credentials on page 23	✓	✓
Setup Wizard: SNMP v3 Credentials on page 23	✓	✓
Setup Wizard: Seed Routers on page 23	✓	
Setup Wizard: Device Type Hints on page 24	✓	
Setup Wizard: Device Interrogation Techniques on page 24	✓	✓
Setup Wizard: Configuration Collection on page 24	✓	✓
Setup Wizard: Summary on page 24	✓	✓

Open a browser window and navigate to the IP address assigned to NetMRI by DHCP or as configured by you. The NetMRI Setup Wizard should appear in your browser.

Setup Wizard: Admin Password

1. Enter and confirm the password for the NetMRI administrative account. Requirements for the password are listed at the bottom of the screen.
2. Click the **Next>** button.

The administrative account is used by the NetMRI administrator to create user accounts and configure NetMRI. This account user name and password are also required to access the administrative shell (a command line interface). Other NetMRI users do not have the special privileges available to the administrator.

The administrative account user name is “admin” and cannot be changed. Since this user name is easy to guess, it is essential to assign a strong password to prevent unauthorized users from impersonating the administrator.

Setup Wizard: License

1. Browse to the location of the NetMRI license file, and then select the license file. The license file ends with the extension *.gpg*.
2. Click the **Next>** button.

A license is required to use NetMRI for production or evaluation purposes. Each license is keyed to a specific NetMRI serial number and specifies the maximum number of devices and interfaces that NetMRI can monitor, as well as which modules are enabled.

If you have not received a license file or you have misplaced it, you can obtain a license file at http://netmri-license.infoblox.com. When you receive the file, save it in a location you can access from the Setup Wizard.

Setup Wizard: Welcome

1. Enable or disable auto discovery.
2. Click the **Next>** button.

Enabling automatic discovery means NetMRI will attempt to discover devices on the network using its own discovery methods. There is less configuration required when implementing automatic discovery, but it may take longer to completely discover all the devices you are expecting to be managed.

Disabling automatic discovery means NetMRI will only manage the devices manually input during configuration. Devices known to exist, but not explicitly configured, are not included in any reports or topology data. Configuring NetMRI with discovery disabled may take longer depending on the number of devices on the network.

Setup Wizard: Discovery Ranges

Note: IPv6 network discovery supports the use of CIDR ranges.

1. Specify devices to include or exclude during discovery.
   - *To add an item:* Click **New**, fill in the fields above the table, and then click **Add**.
   - *To edit an item:* Select the item, click **Edit**, change the fields above the table, and then click **Save**.
   - *To delete an item:* Select the item, click **Delete**, and then confirm the deletion.
   - *To import discovery setting data:* Click **Import**. In the dialog, click **Browse...** to select the CSV file, and then click the **Import** button.
2. Click the **Next>** button.

   Discovery ranges define the scope of the network NetMRI explores by defining CIDR address blocks, IP address ranges and IP address wildcards. NetMRI limits its network exploration to the set of ranges defined in this tab.

   - A CIDR address block is defined by a network address and bit mask (for example 192.168.1.0/24).
   - An IP address range defines a start and ending IP address. For instance, you could define 192.168.1.0 as the start of the IP range and 192.168.1.255 as the end of the IP range.

- An IP address wildcard pattern defines a single IP address range using a wildcard character or range for a specific set of octets. For example, you could define either 192.168.1.* or 192.168.1.0-255 as the IP address wildcard pattern. An IP address wildcard pattern can substitute an asterisk or range for any single octet in the definition.

Ranges included for discovery indicate that any device found matching that range will be discovered and managed by NetMRI. Ranges excluded for discovery indicate that any device found matching that range will be excluded from discovery by NetMRI. Ranges marked “Exclude from management” indicate that any device found matching that range will be discovered by NetMRI, however NetMRI will not manage the device (i.e., collect data from the device)

Setup Wizard: Static IPs

1. Enter IP addresses you want NetMRI to manage.
   - *To add an item:* Click **New**, fill in the fields above the table, then click **Add**.
   - *To edit an item:* Select the item, click **Edit**, change the fields above the table, then click **Save**.
   - *To delete an item:* Select the item, click **Delete**, then confirm the deletion.
   - *To import discovery setting data:* Click **Import**. In the dialog, click **Browse...** to select the CSV file, then click the **Import** button.
2. Click the **Next›** button.

   Devices matching IP addresses listed here are given priority over other devices discovered in determining which devices are counted toward NetMRI license limits.

Setup Wizard: CLI Credentials

Note: Skip this step when installing the NetMRI Discovery and Inventory Module.

1. Enter the CLI credentials used by the devices specified in the **Discovery Ranges** and **Static IPs** steps. NetMRI will automatically determine which credentials are associated with each device.
   - *To add an item:* Click **New**, fill in the fields above the table, then click **Add**.
   - *To edit an item:* Select the item, click **Edit**, change the fields above the table, then click **Save**.
   - *To test an item:* Select the item, then click **Test**. In the test dialog, select the **Hostname or IP**, then click **Start**.
   - *To delete an item:* Select the item, click **Delete**, then confirm the deletion.
   - *To import credential data:* Click **Import**. In the dialog, click **Browse...** to select the CSV file, then click the **Import** button.
2. Click the **Next›** button.

   NetMRI will try site-specific username/passwords, in priority order, when first logging in to a device via a CLI connection (SSH or telnet). Once a password is determined, NetMRI will save it as device-specific information. If there is no site-specific password, NetMRI will try the vendor default credentials in priority order. NetMRI will always use site-specific username/password combinations when trying to determine the new login credentials for a device, and they will not be used for vendor default credential checks.

   Note: NetMRI needs the ENABLE password in order to access configuration files on some devices and to run the Configuration Command Scripts. We strongly recommend that you create a username and password on your network equipment specifically for NetMRI so that it is easier to identify NetMRI actions.

Setup Wizard: SNMP v1/2 Credentials

1. Enter the SNMP v1/2 credentials used by the devices specified in the **Discovery Ranges** and **Static IPs** steps. NetMRI will automatically determine which credentials are associated with each device.
   — *To add an item:* Click **New**, fill in the fields above the table, then click **Add**.
   — *To edit an item:* Select the item, click **Edit**, change the fields above the table, then click **Save**.
   — *To test an item:* Select the item, then click **Test**. In the test dialog, select the **Hostname or IP**, then click **Start**.
   — *To delete an item:* Select the item, click **Delete**, then confirm the deletion.
   — *To import credential data:* Click **Import**. In the dialog, click **Browse...** to select the CSV file, then click the **Import** button.
2. Click the **Next›** button.

NetMRI uses SNMP read-only community strings to collect data for its analysis. NetMRI is pre-configured with several commonly used community strings taken from the list of default community strings configured by the device vendor at delivery time. If the community strings provided during NetMRI installation do not work for a given device, NetMRI tries well-known vendor defaults. If a default community string works for the device, NetMRI begins normal SNMP processing and the “Weak Community String” issue is fired to alert you to this condition. If you are using the optional Compliance Module, you will see all vendor default community strings that were able to return SNMP data for a device in the Default Credentials Report.

Manually entered community strings will be used first, in priority order, then the default community strings will be tried in priority order if the **Use Vendor Default Community Strings** option is enabled in the **Settings › Setup** section › **Collectors and Groups › Global** tab › **Network Polling** panel. That option allows you to disable use of the vendor default community strings for determination of which strings NetMRI can use. This is typically done in installations having tight security setups that have removed all vendor defaults from their installation. Note that this option does not prevent the vendor default from running.

Setup Wizard: SNMP v3 Credentials

1. Enter the SNMP v3 credentials used by the devices specified in the **Discovery Ranges** and **Static IPs** steps. NetMRI will automatically determine which credentials are associated with each device.
   — *To add an item:* Click **New**, fill in the fields above the table, then click **Add**.
   — *To edit an item:* Select the item, click **Edit**, change the fields above the table, then click **Save**.
   — *To test an item:* Select the item, then click **Test**. In the test dialog, select the **Hostname or IP**, then click **Start**.
   — *To delete an item:* Select the item, click **Delete**, then confirm the deletion.
   — *To import credential data:* Click Import. In the dialog, click **Browse...** to select the CSV file, then click the **Import** button.
2. Click the **Next›** button.

NetMRI uses SNMPv3 credentials to collect data for its analysis. When determining SNMP credentials to be used, NetMRI attempts any configured SNMPv3 credentials before using SNMPv1/v2c credentials.

Setup Wizard: Seed Routers

Seed router values are recommended for IPv4 network discovery and are required for IPv6 network discovery.

1. Enter IP addresses for seed routers.
   — *To add an item:* Click **New**, fill in the fields above the table, then click **Add**.
   — *To edit an item:* Select the item, click **Edit**, change the fields above the table, then click **Save**.
   — *To force immediate discovery:* Click **Discover Now**.
   — *To delete an item:* Select the item, click **Delete**, then confirm the deletion.
   — *To import discovery setting data:* Click **Import**. In the dialog, click **Browse...** to select the CSV file, then click the **Import** button.

2. Click the **Next›** button.

NetMRI uses seed routers to quickly perform network discovery. Definition of seed routers is highly recommended for IPv4 networks and is required for IPv6 networks. Seed routers are also given priority (like static IP definitions) for determining which devices are counted toward NetMRI license limits.

The table lists each defined seed router with its discovery status (as defined in the **Network Explorer** tab › **Discovery** tab). By reviewing the discovery status for each seed router you can determine whether NetMRI should be able to discover the network successfully, or if there are possible configuration errors preventing network discovery, without having to wait to see what NetMRI finds.

Setup Wizard: Device Type Hints

1. Enter device type hints.
   - *To add an item:* Click **New**, fill in the fields above the table, then click **Add**.
   - *To edit an item:* Select the item, click **Edit**, change the fields above the table, then click **Save**.
   - *To delete an item:* Select the item, click **Delete**, then confirm the deletion.
2. Click the **Next›** button.

Device hints help the NetMRI discovery engine locate specific types of network devices using IP address patterns and DNS name patterns. For instance, if most routers are found at an IP address ending with ".10", specifying "*.*.*.10" and associating the Router device type for an IP address hint will allow NetMRI to prioritize any discovered devices matching that hint higher in its credential collection queue to help speed discovery. Additionally, this hint is taken into account when NetMRI attempts to determine a device's type.

Valid IP address patterns are either the numeric values of the octet, or an asterisk for any number of octets in the IP address. For device name matches, valid DNS characters and the asterisk character are valid definitions. For instance *rtr* will match any device name with "rtr" in it's definition.

Device hints are optional and are only used in helping to speed network discovery and to assist with determination of device types absent other discovery data.

Setup Wizard: Device Interrogation Techniques

1. Select the desired options. Descriptions are provided in the wizard.
2. Click the **Next›** button.

Setup Wizard: Configuration Collection

Note: Skip this step when installing the NetMRI Discovery and Inventory Module.

1. Select the desired options. Descriptions are provided in the wizard.
2. Click the **Next›** button.

Setup Wizard: Summary

1. Review the summary.
2. For any item flagged as a possible configuration problem, click the **Edit** link to go directly to the corresponding step in the wizard to make changes. After making changes, return to the **Summary** step.
3. Click the **Finish** button.

NetMRI is now configured.

Monitoring the Initial Discovery Process

After the NetMRI setup process has been completed, check discovery progress in the **Tools › Network** section › **Discovery Status** page. If the Default Gateway, CIDR blocks, SNMP credentials and Telnet/SSH credentials were entered correctly, you should start to see devices listed in this table within a few minutes. Periodically click the **Refresh** button ↻ to see how discovery is progressing.

At this point, you may return your workstation to its previous network configuration. Further access to NetMRI may be done by accessing the IP address that was assigned in the Setup Wizard Step 4 or using the DNS name that has been associated with that address.

Troubleshooting Discovery

If you don't see any devices within a few minutes, you should verify the accuracy of the network information added during the configuration process as follows:

1. In the NetMRI header panel, click the **Settings** button. In the menu along the right side of the **Settings** window, click the **Setup** section, then click **Discovery Settings**. Ensure that the given CIDR blocks cover the desired parts of your network. Also, ensure that the Default Gateway is covered by one of the Included CIDR blocks, but not by one of the Excluded CIDR blocks.
2. In the menu along the right side of the **Settings** window, click **Collectors and Groups** (just above **Discovery Settings**). Ensure that **SNMP collection** is Enabled. In the **Settings** window, click **SNMP Credentials** and verify that the community strings for your network devices are entered properly (e.g., check spelling and case-sensitivity).
3. If NetMRI was configured using a crossover Ethernet cable and NetMRI was not on the network following completion of the configuration process, then NetMRI may not have been successful in its initial probes of the network. Navigate to **Settings › Settings** section › **Discovery Settings** page and click the **Reset Discovery Counters** button (below the table) to kick off the initial network probes again, then continue to monitor the discovery process as before.

Any changes made using the forms described above will be automatically used by the discovery process. If the new information is correct, you should start to see devices appearing in the table at **Network Explorer** tab › **Inventory** tab › **Devices / Interfaces** section › **Devices**.

Additional Considerations

This section contains a few recommendations for integrating NetMRI into your operational environment.

Domain Name Assignment

For long-term use, we recommend that you add NetMRI to your DNS server configuration so that references to NetMRI can be made by name instead of IP address. You are free to assign any name to the NetMRI server, but Infoblox recommends that you use the same Server Name that was assigned to NetMRI in the first step of the NetMRI setup process. That way, the DNS name, SNMP system name and HTTPS server certificate name will all be consistent.

Accessing Using HTTPS

NetMRI is configured to accept browser requests on the standard HTTP port (80) for convenience and the HTTPS port (443) for additional security. During the initial setup process, the **Server Name** assigned to NetMRI is used as the HTTPS server certificate name.

When connecting to NetMRI via HTTPS for the first time from a given browser, the browser will display a dialog box indicating that a) the NetMRI server certificate has not been seen before and b) it is not currently trusted. At that point, you should examine the NetMRI server certificate to confirm that it contains the specified **Server Name** and that it was signed by “Infoblox, Inc.” If the certificate appears authentic, you should accept/install the certificate using the standard process supported by your browser. After the certificate is installed, the dialog will no longer be displayed when you connect to NetMRI using HTTPS.

Note: **Note:**Some browsers, such as Internet Explorer, automatically display the certificate dialog if the host name used in the URL is not the same as the name provided in the server’s certificate. Therefore, it is recommended that the DNS name used to access the NetMRI server and the Server Name entered when configuring NetMRI be the same.

Using NetMRI

At this point, you should review the NetMRI online help, which describes all the capabilities provided by NetMRI, including all reports, issues and displays. Access the online help by clicking the **Help** button ? at the right end of the navigation area. A few useful topics for new users are “About NetMRI,” “Strategies” and “Getting started” › “Quick start.”

Tip: You can access page-specific help from any location that displays the help button ? at the right end of the green header bar.

Shutdown Procedure

NetMRI includes embedded database and file systems to manage the vast amount of information gathered from the network. Although the database and file systems are designed to be resilient to failures, it is always best to shut the system down gracefully whenever possible to avoid data corruption.

NetMRI can be properly shutdown at the **Settings** › **NetMRI Settings** section › **Shutdown Server** page or by using the **`halt`** command in the NetMRI Administrative Shell accessible via SSH (see “Other information” › “Administrative Shell” in the online help for details).

Resetting to Factory Defaults

If you are evaluating NetMRI on a production network and want to erase all data collected before returning the unit, this is most easily accomplished using the **`reset`** command in the NetMRI Administrative Shell (accessible via SSH; see reference above). When that command is executed, the network database will be erased, all files stored in the *Administrator* directory will be deleted and NetMRI will be returned to its factory default settings.

Chapter 4 Deploying the Operations Center

This chapter provides requirements for administrators and engineers planning to install the NetMRI Operations Center distributed network analysis environment. It outlines the prerequisites to successfully prepare a NetMRI Operations Center hardware appliance to act as the central node in the OC environment; specify and plan the VMware infrastructure for a NetMRI installation, and to install and configure NetMRI virtual appliance VMs (virtual machines) as data collectors in the OC environment.

Because VMware installation parameters and hardware configurations vary by organization, this document provides guidance for configurations that have worked well for NetMRI installations, and outlines some general best practices for VMware installations.

This documentation is intended for:

- Customers who want to run NetMRI in a VMware Infrastructure, whether as a standalone or as part of an Operations Center deployment.
- Administrators and engineers responsible for the installation and administration of the NetMRI virtual appliance in a VMware Infrastructure.

Note: In the event of a power outage, the hardware on which NetMRI runs should be supported by an uninterruptible power supply (UPS) to avoid data corruption problems.

The Operations Center deployment includes the following:

- *Operations Center Requirements* on page 28
- *Recommended Best Practices* on page 28
- *Configuring the NetMRI Appliance for IPv6* on page 30
- *Deploying Automatic Failover for New Appliances* on page 32
- *Migrating Existing Systems as Failover Pairs* on page 33
- *Benchmarking the VMware Infrastructure* on page 13
- *Installing NetMRI Operations Center* on page 34
- *Installing the Operations Center Software* on page 34
- *Running the Setup Wizard* on page 37
- *Running the Setup Wizard* on page 37
- *Additional Considerations* on page 42
- *Discovery Import Formats* on page 43
- *Credential Import Formats* on page 44
- *Configuring NetMRI Collectors* on page 45

- *NetMRI Virtual Appliance Installation Worksheet* on page 46
- *Installing NetMRI Virtual Appliances (for Collectors)* on page 47
- *Configuring and Registering NetMRI Collectors* on page 49
- *Monitoring the Initial Discovery Process* on page 50

Operations Center Requirements

NetMRI appliances are offered in several models:

— NetMRI-1102-A (Discontinued–appliances in the field may operate as Collectors only)

NetMRI-1102-A appliances are equipped with two Ethernet ports, labeled MGMT and SCAN. The MGMT port may be used singly as a dedicated management port for the appliance or may operate as the only active port, carrying both management and network monitoring traffic. By default, the appliance is configured to use the MGMT port for both system administration and network analysis functions.

— NetMRI NT-4000

NT-4000 appliances are a next-generation 2U appliance that supports a larger CPU, memory and storage configuration, along with field-replaceable power supplies and disk drives in a RAID-10 array. The NT-4000 appliance may operate as an Operations Center and as a Collector appliance. It is equipped with two Ethernet ports, labeled LAN1 and LAN2. LAN1 connects the NT-4000 appliance to the management network and is used for managing the appliance. LAN1 may operate as the only active port, carrying both management and network monitoring traffic. If activated, LAN2 connects the appliance to the network. LAN2 is used for network analysis, connecting to the networks that the appliance will scan and analyze.

— NetMRI NT-1400

The NetMRI NT-1400 is designed for smaller enterprise deployments and for use as a Collector for Operations Center deployments.

— NetMRI NT-2200

The NetMRI NT-2200 appliances may operate as both Operations Center appliances and as Collectors.

— NetMRI VM

A virtual machine version installed on a VMware ESXi server to provide greater flexibility for network monitoring and analysis. VMs are often used as collectors for an Operations Center deployment. A NetMRI VM also can operate as an Operations Center.

Note: In the Operations Center context, when an appliance acts as the Operations Center it uses only a single port, which is the LAN1 port for the NT-1400, NT-2200 or NT-4000.

In this Guide, both hardware models are treated generically and referred to as a “NetMRI appliance.” Either model can operate as a NetMRI Operations Center central node.

Infoblox NetMRI appliances should always be supported by an uninterruptible power supply (UPS) to avoid data corruption problems in cases of power outage.

Recommended Best Practices

In ideal cases, the appliance that is designated as the Operations Center should be installed first, as described in described in *Installing the Operations Center Software* on page 34.

Then, install the NetMRI virtual machines to act as collectors using the standard installation procedures described in *Configuring and Registering NetMRI Collectors*.

Configuring a VMware server and the virtual appliances that run on it is beyond the scope of this document. The following items outline best practices that have been found specific to NetMRI Virtual appliance installations.

Table 4.1 Best Practice Guidelines

AMD and Intel Processors	*Issue:* Hardware platforms using AMD processors may present performance bottlenecks to VMware running NetMRI, in certain cases. *Recommendation:* Avoid AMD processor hardware if possible. If this is not feasible, pay close attention to the results of the platform benchmark and resolve any issues before installing NetMRI. *Issue:* NetMRI benefits from hardware virtualization support included in the latest generation Intel processors. Performance of older generations of processors may not be suitable for high-performance applications, such as high license count deployments. *Recommendation:* Infoblox recommends running NetMRI on the latest generation of processors having hardware virtualization support. Intel i7 based servers are shown to be particularly effective.
Disk Performance	*Issue:* In high-performance applications, such as high license count deployments, NetMRI is I/O-intensive. If multiple applications are configured to be accessing the same physical disk, NetMRI can experience significant read/write delays that degrade its performance. *Recommendation:* Infoblox recommends that NetMRI be provisioned to use dedicated disks/spindles.
Server Performance Monitoring	*Issue:* NetMRI is a high-performance network analysis system. It may use CPUs intensely for extended periods and may exceed CPU thresholds currently set on server performance monitoring applications. *Recommendation:* If monitoring is set up for your VMware server, you need to raise or eliminate the alert threshold values for NetMRI to eliminate unnecessary alarms.
CPU Allocation	*Issue:* Due to context-switching overhead, allocating more vCPUs to NetMRI may, in fact, impair performance. *Recommendation:* Infoblox recommends adherence to the recommended vCPU allocation parameters listed in *Recommended Best Practices* on page 28. If system performance is suffering, check the CPU Ready State times. If times are high, try reducing the number of vCPUs and see if that helps. If times are low, try increasing vCPUs. Additional information relative to vCPU allocation can be found at: http://www.vmware.com/pdf/vi_performance_tuning.pdf.

Connecting NetMRI to the Network (Hardware Appliances Only)

Note: This section applies only to Infoblox NetMRI hardware appliances.

NetMRI appliance communications require only an Ethernet connection. Follow these steps to connect NetMRI to your network:

1. **(NetMRI-1102-A) Configure the appliance to use one port** (same port for both system administration and network analysis): Using a straight-through RJ45 Ethernet cable, connect from the MGMT Ethernet connector on the back panel of the NetMRI appliance to an available Ethernet connection on your network.
   or
   Configure the appliance to use two ports (one for system administration and one for network analysis), using straight-through RJ45 Ethernet cables:
   a. Connect from the MGMT Ethernet connector on the back panel, to the management network;
   b. Connect from the SCAN Ethernet connector on the back panel to an Ethernet connection on the network to be analyzed by NetMRI.

   Note: All NetMRI appliance models support 10/100/1000Mbps network connections.

2. **(NT-4000) Configure the appliance to use one port:** Using a straight-through RJ45 Ethernet cable, connect from the LAN1 Ethernet connector on the back panel of the NetMRI appliance to an Ethernet connection on the network. The LAN1 port is enabled by default to carry both management and analysis traffic;
   or
   Configure the appliance to use two ports (one for system administration and one for network analysis), using straight-through RJ45 Ethernet cables,

a. Connect from the LAN1 Ethernet connector on the back panel, to the management network;

b. Connect from the LAN2 Ethernet connector on the back panel to an Ethernet connection on the network to be analyzed by NetMRI. The LAN2 port is disabled by default and must be enabled through the NetMRI UI after initial setup of the appliance. Once enabled, LAN2 is designated as the analysis port.

3. After connecting any necessary network cables, simply plug NetMRI into an AC power source.
4. Verify that the green Link LED on NetMRI's RJ45 port is lit, indicating a good connection to your network. If possible, verify that the link indicator is lit on the network hub or switch port to which NetMRI is connected.

Note: For a successful configuration process, NetMRI and the workstation used during setup must be connected to the same subnet or VLAN.

Configuring the UI Client

NetMRI always listens on the private IP address **169.254.1.1**, subnet mask **255.255.255.0**, which can be used at any time to configure NetMRI using the following procedure. The easiest way to access NetMRI on that address is to temporarily configure the workstation to use address **169.254.1.5**, subnet mask **255.255.255.0**.

The process for Windows XP is described here, but it may be slightly different for other versions of Windows or other operating systems:

1. From the **Start** menu button, select **Control Panel**.
2. In the *Control Panel* dialog, click **Network Connections**.
3. In the *Network Connections* dialog, click **Local Area Connection**.
4. In the *Local Area Connection Status* dialog, click **Properties**.
5. In the *Local Area Connection Properties* dialog, click **Internet Protocol (TCP/IP)** in the **Network Components** list. Then click the **Properties** button.
6. In the *Internet Protocol (TCP/IP) Properties* dialog, fill in the **IP address** and **Subnet mask** fields with an IP address of **169.254.1.5** and subnet mask of **255.255.255.0**.
7. Click the **OK** buttons in the *Internet Protocol (TCP/IP) Properties* and *Local Area Connection Properties* dialog boxes. (For some versions of Windows, you are required to reboot your computer.)

   Note: This address change is only necessary for NetMRI's initial setup. Once setup is complete, return your workstation to its prior configuration.

8. Click **Close** in the *Local Area Connections Status* dialog box.
9. Temporarily disconnect the NetMRI appliance from the network by unplugging the Ethernet cable from the MGMT port of the appliance. Use a cross-over Ethernet cable and connect your computer to the MGMT port.
10. Access NetMRI at 169.254.1.1 using SSH.
11. Log in with user name `admin` and password `admin`.
12. Continue the installation by following instructions in *Configuring NetMRI* on page 19.

Configuring the NetMRI Appliance for IPv6

Users can manage NetMRI on an IPv6 network. The NetMRI Management port has its own factory default link-local IPv6 address, which is unique on its connected subnet. The default IPv6 address derives from the Ethernet MAC address of the NetMRI interface.

You must use a Windows 7 system to configure NetMRI to run on the IPv6 network because Windows 7 natively supports IPv6.

To configure a new NetMRI appliance to be managed through IPv6, do the following:

1. Reboot Windows 7, ensure that it is enabled for IPv6 networking, and connect it to the management (MGMT) port of the NetMRI appliance, using a standard Ethernet cable.
2. On the Windows 7 system, open a command line window and run **ipconfig**.

   Check the listing in the Local Area Connection section of the **ipconfig** display and take note of the interface number associated with the PC's IPv6 Link Local address. The value will have an **fe80:** prefix and end with a %* designator, such as **fe80::505:ac3b:49b7:dc38%15**. The value **15** in this example is the interface number.
3. In a Windows command line, run the following command:

   netsh interface ipv6 show neighbor
4. Find the **Interface *: Local Area Connection** section (the * corresponds to the interface number for your PC system's IPv6 address). No entry should be present in this category for any address starting with the **fe80:** prefix.

   In the Windows PC's command line, you must now run a multicast IPv6 ping to all nodes on the subnet on which the Management port is running. Effectively, this means you are running a multicast IPv6 ping to the single NetMRI management port connected to the PC.
5. In the Windows command prompt, run the following command:

   ping -6 -n 5 ff02::1

   Allow the command to complete whether or not responses occur.
6. In the Windows PC's command line, run the following command a second time:

   netsh interface ipv6 show neighbor

   The NetMRI Management port IPv6 link-local address should now appear in the neighbor table under the **Interface xx: Local Area Connection** section, similar to the following:

   ```
   fe80::230:48ff:febc:97da         00-30-48-bc-97-da   Reachable
   ```

   This is the link-local address of the NetMRI appliance's management port.
7. Open an SSH client session to the NetMRI CLI at the IPv6 address shown in Step 6 along with the interface number. Log in with the factory default username/password *admin/admin*.

   Next, you assign a globally routable static IPv6 address on the management port.
8. In the NetMRI CLI, enter the command:

   configure ip
9. Enter a new IPv6 address for the management interface in the IPv6 Address (optional) field. The address should begin with the **2001:** prefix and conform to the IPv6 prefix for the network. Also enter the Primary DNS Server Address, the default gateway and the Primary DNS Domain. An example appears below:

   ```
   IPv4 Address (optional) [172.23.27.40]:
   IPv4 Subnet Mask (optional) [255.255.255.0]:
   IPv6 Address (optional): 2001:db8:a2:2c0:ee22::40
   IPv6 Prefix (optional): 64
   IPv4 Default Gateway (optional) []:
   IPv6 Default Gateway (optional) []:2001:db8:a2:2c0:ee22::1
   IPv4 Default Gateway (optional) []:
   IPv6 Default Gateway (optional) []:
   Primary DNS Server [172.23.27.236]: 2001:db8:a2:2c0::236
   Primary DNS Domain [qanet.com]: customer.com
   ```
10. Save the new settings.
11. Shut down the NetMRI unit and physically install it in the global network. The unit is now reachable on its global static IPv6 address for further CLI configuration and UI access.

Deploying Automatic Failover for New Appliances

Following are the pre-requisites for deploying automatic failover for new appliances:

- Configure two supported NetMRI appliances with licenses installed.
- Both the appliances must be of the same appliance model and same software version number.
- Provision three IP addresses on the same subnet: a VIP address and two management IP addresses for the appliances.
- If you are using direct replication method to connect both appliances, you need an Ethernet cable to connect the systems directly through their HA Ports.
- If you are using the network replication method to connect the appliances, you must connect the systems over a local network and two replication IP addresses must be acquired on the same subnet. You must also select a TCP port for the replication traffic.

Note: Infoblox recommends you to use the direct replication method for best reliability and performance. The network replication method will have higher latency and a greater chance of connection breakage, and thus lower reliability and performance.

You can deploy two new Operation Center (OC) or standalone appliances to form a failover pair, as follows:

1. Set up and configure two new NetMRI appliances as separate systems. Ensure that the appliances are running NetMRI 7.1.1 or later.
2. Connect both the systems using one of the following methods:
   - Direct replication: Connect the systems directly through their HA ports.
   - Network replication: Connect the HA port of both systems to a network using an Ethernet cable.

   Infoblox recommends that you connect the systems using the direct replication method.
3. Run the Setup Wizard on both appliances and set the admin password and install the license. The admin password must be the same on both systems. For information about the Setup Wizard, see the *Running the Setup Wizard* topic and its subsections in the NetMRI online Help.

   At this point of time, it is not necessary to complete the entire configuration wizard on both systems. You can complete the configuration only on the primary system.
4. If the systems were not shipped with version 7.1.1 or greater, you must upgrade the systems to the latest release.
5. After upgrading both systems to NetMRI 7.1.1 or later, repartition the systems by logging in to the Admin Shell of both the systems and enter the **repartition** command.

   For new systems with no network device data collected, you can proceed without resetting and without generating a backup. For systems that are already deployed, and have collected data, follow the steps mentioned in *Migrating Existing Systems as Failover Pairs* on page 33.
6. Choose one system to take the primary role. You can choose the system for which you have completed the entire configuration, otherwise the configuration might be lost.
7. Log in to the primary system, go to **Settings** -> **Setup** -> **Failover Configuration**, and then specify the configuration settings in the **Failover Configuration** page. For information about specifying the configuration settings, see the *Specifying Automatic Failover Settings* topic in the NetMRI online Help.

Note: After specifying the failover configuration settings and completing the enable operation, the systems start synchronizing data. This process might take up to one hour, depending on the appliance model.

Migrating Existing Systems as Failover Pairs

You can migrate two existing Operation Center (OC) or standalone appliances to form a failover pair. Ensure that both appliances are running versions NetMRI 7.1.1 or later.

Following are the pre-requisites for migrating existing systems as a failover pair:

- Two supported NetMRI appliances with licenses installed. You can choose an existing appliance and a second appliance of the same model.
- Provision two additional IP addresses on the same subnet: a management IP address assigned to each system and a VIP address shared between the failover pair.
- If you are using direct replication method to connect both appliances, you need an Ethernet cable to connect the appliances directly through their HA ports.
- If you are using network replication method to connect the appliances, you must connect the systems over a local network and two replication IPs must be acquired on the same subnet. You must also select a TCP port for the replication traffic.

To migrate two existing systems to form a failover pair:

Note: In the below steps, the system that is referred to as the second system takes the primary role and the system that is referred to as the existing system takes the secondary role in the failover pair.

1. Choose an existing NetMRI system and configure a second NetMRI system of the same model.
2. If you are using scan ports, connect the scan ports of the second system to the network in the same way as the existing system. For information, see the *Failover and Scan Interfaces* topic in the NetMRI online Help.
3. Connect both systems using one of the following methods:
   - Direct replication: Connect the systems directly through their HA ports.
   - Network replication: Connect the HA port of both systems to a network using an Ethernet cable.
4. Run the Setup Wizard on the second system and set the admin password and install the license. For information about the Setup Wizard, see the *Running the Setup Wizard* topic and its subsections in the NetMRI online Help.
5. Exit the Setup Wizard after setting the password and installing the license on the second system.
6. Upgrade the systems to NetMRI 7.1.1, if necessary.
7. After upgrading both systems to NetMRI 7.1.1 or later, repartition the systems to prepare them for automatic failover, as follows:
   - Log in to the Admin Shell on the second system, and enter the **repartition** command. Note that if the system is already partitioned for failover, an error message appears when you run the **repartition** command.
   - Generate a database archive of your existing system, and restore this to the second system. Re-enable SNMP collection after restoring the archive on the second system. To enable SNMP collection, go to **Settings** -> **Setup** -> **Collection and Groups** -> **Global** tab -> **Network Polling side** tab, and then select the **SNMP Collection** check box.
   - If the data restore is not successful, do not proceed to the next step. If the restore failed due to disk space exhaustion, you may try reducing data retention settings on your existing NetMRI system to reduce the archive size. For more information, see *Data Retention* on page 353 or contact Infoblox Support for further assistance. Note that it might take up to 24 hours for reduced data retention settings to take effect.
   - If the data restore is successful, log in to the Admin Shell on the existing system, enter the **reset system** command, and then enter the **repartition** command. Note that if the system is already partitioned for failover, an error message appears when you run the **repartition** command. After repartitioning is complete, run the **configure server** command, install the license, and then reset the admin password in GUI to match the other system.
8. If you want to use the management IP address of your existing system as the VIP of the failover pair, then you must change the management IP address of the existing system.

9. Configure the second system to take the role of the primary system, as follows:
   - Log into the second system.
   - Go to **Settings -> Setup -> Failover Configuration**.
   - Specify the configuration settings in the **Failover Configuration** page. For information about specifying the failover configuration settings, see the *Specifying Automatic Failover Settings* topic in the NetMRI online Help.
10. For an Operation Center, complete the following:
    - Log in to the Admin Shell on the Operation Center and run the **reset tunserver** and **configure tunserver** commands. Enter the VIP address of the Operation Center when prompted for the IP address of the Operation Center server.
    - Log in to the Admin Shell on each Collector and run the **reset tunclient** and **register tunclient** commands. Enter the VIP address of the Operation Center when prompted for the IP address of the Operation Center.

Note: After specifying the failover configuration settings and completing the enable operation, the systems start synchronizing data. This process might take up to one hour, depending on the appliance model.

Installing NetMRI Operations Center

A NetMRI Operations Center system consists of a Controller and multiple Collectors. The system aggregates data and analyzes results from the Collectors to provide a consolidated view of the entire enterprise within one user interface, which is hosted by the Controller. Communication between the Controller and its associated Collectors takes place over a Secure Sockets Layer Virtual Private Network (SSL VPN).

The starting point for installing an Operations Center is a fully functioning NetMRI appliance, whether physical or virtual. The following sections describe how to install and configure the Operations Center Controller and Collectors.

Note: In the event of a power outage, the hardware on which NetMRI runs should be supported by an uninterruptible power supply (UPS) to avoid possible data corruption problems.

Installing the Operations Center Software

1. Convert the NetMRI Virtual appliance to an Operations Center Controller:
   a. Obtain an Operations Center license from Infoblox.
   b. Upload the license into the admin account's /Backup directory using WinSCP or a similar program.
   c. Log into the admin shell and enter the **license <NameOfLicenseFile>** command.
2. Log in to the admin shell and enter **configure tunserver**. Answer the prompts to set up the basic server and network.

Depending on how you want to proceed, continue in one of the following sections:

- *Configuring the Operations Center Controller for Factory Defaults*
- *Configuring An Operations Center Controller From an Existing NetMRI Instance*

Configuring the Operations Center Controller for Factory Defaults

Note: If you want to use scripts, policies, settings and user accounts already present in a NetMRI instance, follow the instructions in *Configuring An Operations Center Controller From an Existing NetMRI Instance*.

1. Log in to the admin shell.
2. Enter **configure tunserver**.
3. When prompted to `Enter the reference system serial number or RETURN to skip`, press ENTER.
4. Proceed to build out the system.

Configuring An Operations Center Controller From an Existing NetMRI Instance

The OC can import a library of scripts, custom reports, custom jobs, policies and user data from an existing NetMRI appliance. The instance from which you are importing does not become the OC itself.

1. Choose the NetMRI instance as a reference system from which data will be copied.

   All scripts, policies, settings and user accounts from this instance will be transferred to the Operations Center Controller.

   When adding multiple NetMRI instances to an Operations Center environment, the scripts, policies and settings may differ between NetMRI instances. Only information from the reference NetMRI is imported into the Operations Center. Therefore, any of the deltas you want imported into the Operations Center must either be manually added to the reference NetMRI or imported into the Operations Center after the reference NetMRI is restored on the Operations Center.
2. Configure the Controller:
   a. Log in to the admin shell on the Operations Center Controller.
   b. At the command prompt, enter **configure tunserver**.
   c. When prompted to `Enter the reference system serial number or RETURN to skip`, type the serial number of the NetMRI reference system, then press ENTER.

   Tip: In each prompt, defaults are shown in square brackets [ ]. To accept the default, simply press ENTER.

   d. When prompted: `Use these settings?`, enter **y**.
   e. When prompted to restart the Controller, enter **y**.

      The complete package of scripts, policies and user data is downloaded by the Operations Center. You install the data in a following step.
3. Register the reference system with the Controller:
   a. Log in to the admin shell on the reference system.
   b. At the command prompt, enter **register**.
   c. When prompted to `Register this system?`, enter **y**.
   d. You are prompted to run `restore-settings` on the master server. Continue in step 4.
4. Define restore settings on the Controller: (This installs the uploaded reference data.)
   a. If needed, log in to the admin shell on the Controller.
   b. At the command prompt, enter **restore-settings**.
   c. At the `Continue with import?` prompt, enter **y**. (This installs the reference data on the Controller.)
   d. When prompted to restart the Controller, enter **y**.
5. Re-register the reference unit with the Controller.
   a. If needed, log in to the admin shell on the reference system.
   b. At the command prompt, enter **register**.
   c. When prompted to `Register this system?`, enter **y**.
   d. The Collector restarts. After restarting, the instance will be a Collector in the Operations Center system.

Note: As part of the registration process, the admin password on each Collector synchronizes with the password on the Operations Center Controller. After registration completes, the admin password for the Collector may be different than the password you initially used to log in to the admin shell on that instance.

Note: After registration, the NetMRI GUI is not available on the reference NetMRI unit. All access to the unit must be through the Controller.

6. Continue to the following section, *Operations Center Command-Line Setup*.

Operations Center Command-Line Setup

After the NetMRI Operation Center appliance and its surrounding Collectors have been installed, do the following for the Operations Center:

If the NetMRI Operations Center appliance uses DHCP, note the IP address assigned to the appliance.

If you are configuring a static IP for NetMRI, do the following:

1. In the administrative shell, enter **configure ip**, then complete the following:
   a. Enter the Management IP Address: the IPv4 address of the management interface of NetMRI.
   b. Enter the Management Subnet Mask: the subnet mask of the management interface of NetMRI.
   c. Enter the Management Gateway Address: the IPv4 default gateway of the management interface of NetMRI.
   d. Enter the Primary DNS Server: the primary DNS server for the NetMRI appliance.
   e. Enter the Primary DNS Domain: the DNS domain name for NetMRI.
2. In the **Current Settings** section, review your entries.
   a. At the **Edit these settings? <y/n> [n]** prompt, enter **n** and press ENTER.
   b. At the **Configure these IP settings? <y/n> [y]** prompt, enter **y** to configure the IP settings. Wait while NetMRI configures the network and sets the web interface to use the new IP address.
   c. When prompted, enter **y** to complete the configuration.
3. At the command prompt, enter **configure server,** then complete the following (values you entered in the **configure ip** command are the default values here).
   a. Enter your network name, server name and domain name(s).
   b. Enter the NTP time server if applicable.
   c. Enter the time zone region to be used for timestamps within NetMRI.
   d. Enter the location within your time zone region.
   e. Enter IP address and the Subnet Mask for the NetMRI system.
      1. Enter the IPv6 address if applicable.
      2. Enter the IPv6 prefix if applicable.
   f. Enter the default gateway.
      1. Enter the IPv6 default gateway if applicable.
   g. Enter **n** for the scan port.
   h. Enter the DNS server(s) for NetMRI.
   i. Review your settings. If you accept the settings, enter **n**.
   j. Enter **y** to configure the server with the settings you just entered.
   k. Wait while NetMRI configures the network and sets the web interface to use the new IP address.
   l. When prompted, enter **y**.
   m. Restart the server and reboot.
   n. At the shell prompt, type **exit** to log out.
4. Continue to the following section, *Running the Setup Wizard*.

Running the Setup Wizard

Note: The Setup Wizard is run only on the Operations Center central node. The Collectors should be registered to the central OC node before running the Setup Wizard. Consult the topics in XXX for more information.

The Setup Wizard (**Settings** icon –> **Setup** –> **Setup Wizard**) provides a multistep process for installing and configuring NetMRI. In the Operations Center context.

The Setup Wizard should only be run after the Operations Center appliance and all of the associated Collectors have been installed, and all Collectors have been registered with the Operations Center appliance.

Setup Wizard: Admin Setup

Note: This step is present only during initial NetMRI setup. It does not appear after NetMRI is successfully configured and the wizard subsequently accessed via **Settings** icon –> **Setup** –> **Setup Wizard**.

The primary administrative account is used by the NetMRI administrator to create user accounts and configure NetMRI. This account's user name and password are also required to access the administrative shell (a command line interface). Other NetMRI users do not have the special privileges available to the administrator. This administrator account is the “superuser” account in the NetMRI appliance.

The primary administrative account's user name is “admin” and cannot be changed. Since this user name is easy to guess, it is essential to assign a strong password to prevent unauthorized users from impersonating the administrator.

Do the following:

1. Enter and confirm the password for the NetMRI administrative account. Requirements for the password are listed at the bottom of the screen.
2. Click **Next**.

Setup Wizard: License Install (Operations Center Only)

Note: This step is present only during initial NetMRI setup. It does not appear after NetMRI is successfully configured and the wizard subsequently accessed via **Settings** icon –> **Setup** –> **Setup Wizard**. Subsequent license installations can be carried out by going to **Settings** icon –> **Setup** –> **Settings Summary** and clicking the **Install** link above **License Configuration**.

A license is required to use NetMRI for production or evaluation purposes. Each license is keyed to a specific NetMRI OC serial number and specifies the maximum number of devices and interfaces that NetMRI can monitor, as well as which software modules are enabled.

If you have not received a license file, or you have misplaced it, you can obtain a license file at *http://support.infoblox.com*. When you receive the file, save it in a location you can access from the Setup Wizard.

Do the following:

1. Browse to the location of the NetMRI license file, then select the license file. The license file ends with the extension **.gpg**.
2. Click **Next**.

Setup Wizard: Welcome

Note: Infoblox recommends enabling automatic discovery during the Setup Wizard.

Automatic discovery directs NetMRI to discover devices on the network using SNMP and terminal command-line discovery methods. Automatic discovery requires less configuration, but it may take longer to completely discover all devices to be detected and managed.

Disabling automatic discovery directs NetMRI to manage devices that are manually input during configuration. Devices known to exist, but not explicitly configured, are not included in any reports or topology data. Configuring NetMRI with discovery disabled may take longer depending on the number of devices on the network.

Do the following:

1. Enable or disable auto discovery.
2. Click **Next**.

Setup Wizard: Discovery Ranges

Note: You can add new IP address ranges and seed routers at any time after initial NetMRI setup. IPv4 and IPv6 are supported. For more in-depth information, see the *Defining Ranges* topic and its subsections in the NetMRI online Help.

Discovery ranges define the scope of the network that NetMRI explores by defining CIDR address blocks, IP address ranges and IP address wildcards. NetMRI limits its network exploration to the set of ranges defined in this tab. You can also exclude values and ranges from the Discovery process and hence from monitoring by NetMRI.

- A CIDR address block is defined by a network address and bit mask (for example 192.168.1.0/24).
- An IP address range defines a start and ending IP address. For instance, you could define 192.168.1.0 as the start of the IP range and 192.168.1.255 as the end of the IP range.
- An IP address wildcard pattern defines a single IP address range using a wildcard character or range for a specific set of octets. For example, you could define either 192.168.1.* or 192.168.1.0-255 as the IP address wildcard pattern. An IP address wildcard pattern can substitute an asterisk or range for any single octet in the definition.
- A desired set of values can also be imported from a *.CSV file.

Ranges included in discovery indicate that any device found matching that range will be discovered and managed by NetMRI. Ranges excluded for discovery indicate that any device found matching that range will be excluded from discovery.

Ranges marked **Exclude from Management** indicate that any device found matching that range will be discovered, but NetMRI will not manage/collect data from the device.

Do the following:

1. Specify devices to include or exclude during discovery.

   To add an item: Click **New**, enter the new values in the s above the table, elect the **Discovery Mode**, then click **Add**.

   To edit an item: Select an entry and click **Edit**. Change the value in the **Network** field above the table, including the subnet mask if necessary (the mask value is a drop-down menu), then click **Save**.

   To delete an item: Select an entry, click **Delete**, then confirm the deletion.

   To import discovery setting data: Click **Import**. In the dialog, click **Browse...** to select the CSV file, then click **Import**.
2. Click **Next**.

Setup Wizard: Static IPs

You can specify individual IPs that you explicitly want NetMRI to manage. Adding values to this Wizard step prioritizes the specified addresses over other IPs or subnets specified for Discovery. IPv6 and IPv4 values are supported.

Do the following:

1. Specify IP addresses that you want NetMRI to manage.

   To add an item: Click **New**, enter the new IP address in the **IP Address** field (subnet is not necessary), select the **Discovery Mode**, then click **Add**.

   To edit an item: Select an entry and click **Edit**. Change the value in the **IP Address** field above the table or change the **Discovery Mode**, then click **Save**.

   To delete an item: Select an entry, click **Delete**, then confirm the deletion.

   To import discovery setting data: Click **Import**. In the dialog, click **Browse...** to select the CSV file, then click **Import**. (See *Discovery Import Formats* on page 43 for information on import file syntax.)
2. Click **Next**.

Setup Wizard: CLI Credentials

Note: For more information about credential definitions and NetMRI, see the topic *Adding and Editing Credentials* and its subsections in the NetMRI online Help.

Note: NetMRI needs the ENABLE password in order to access configuration files on some devices and to run the Configuration Command Scripts. Infoblox recommends creation of a username and password on the network equipment specifically for NetMRI so that it is easier to identify NetMRI actions.

NetMRI attempts site-specific username/passwords, in priority order, when first logging in to a device via an SSH or telnet CLI connection. When NetMRI determines a password, it saves it as device-specific information. If there is no site-specific password, the system tries the vendor default credentials in priority order, and uses site-specific username/password combinations when trying to determine the new login credentials for a device. They are not used for vendor default credential checks.

Do the following:

1. Enter the CLI credentials used by the devices specified in the Discovery Ranges and Static IPs steps. NetMRI automatically determines which credentials are associated with each device.

   To add an item: Click **New**, enter the values for the **Priority**, **Password Type** (**User** or **Enable**), **Username** and **Password** fields, then click Add.

   To edit an item: Select the item, click **Edit**, change the values for the **Priority**, **Password Type**, **Username** and **Password** fields, then click **Save**.

   To test an item: Select the item, then click **Test**. In the test dialog, select the Hostname or IP, then click **Start**.

   To delete an item: Select the item, click **Delete**, then confirm the deletion.

   To import credential data: Click **Import**. In the dialog, click **Browse...** to select the CSV file, then click **Import**. (See the *Discovery Import Formats* topic for import file syntax.)
2. Click **Next**.

Setup Wizard: SNMPv1/2 Credentials

Note: For more information about credential definitions and NetMRI, see the topic *Adding and Editing Credentials* and its subsections in NetMRI online Help.

NetMRI uses SNMP read-only community strings to collect data for analysis. The system is pre-configured with several commonly used community strings taken from the list of default community strings configured by the device vendor at delivery time. If the community strings provided during NetMRI installation do not work for a given device, the system tries well-known vendor defaults. If a default community string works for the device, NetMRI begins normal SNMP processing and the “Weak Community String” issue is fired to alert to this condition.

NetMRI first uses the manually entered community strings, in priority order, then the default community strings are tried in priority order if the Use Vendor Default Community Strings option is enabled in **Settings** icon –> **Setup** –> **Collectors and Groups** –> **Global** tab –> **Network Polling** panel. Here, you disable use of the vendor default community strings for determination of which strings NetMRI can use. Do this for installations having tight security setups with all vendor defaults removed from the network. This option does not prevent the vendor default from running.

Do the following:

1. Enter the SNMP v1/2 credentials used by any devices specified in the **Discovery Ranges** and **Static IPs** steps. NetMRI automatically determines which credentials are associated with each device.

   To add an item: Click **New**, fill in the **Priority** and **Community** fields above the table, then click **Add**.

   To edit an item: Select the item, click **Edit**, change the fields above the table, then click **Save**.

   To test an item: Select the item, then click **Test**. In the test dialog, select the Hostname or IP, then click **Start**.

   To delete an item: Select the item, click **Delete**, then confirm the deletion.

   To import credential data: Click **Import**. In the dialog, click **Browse...** to select the CSV file, then click **Import**. (See the *Discovery Import Formats* topic for import file syntax.)
2. Click **Next**.

Setup Wizard: SNMPv3 Credentials (Rare)

NetMRI also uses SNMPv3 encrypted community strings to collect data for analysis, if any exist for any devices in the network. If SNMPv3 strings are provided for devices in the network, the v3 credentials are used before any SNMPv2 credentials.

Do the following:

1. Enter the SNMP v3 credentials used by any devices specified in the **Discovery Ranges** and **Static IPs** steps. NetMRI automatically determines which credentials are associated with each device.

   To add an item: Click **New**, fill in the **Priority** and **Community** fields above the table along with the required Authentication and Privacy protocols and passwords, then click **Add**.

   To edit an item: Select the item, click **Edit**, change the fields above the table, then click **Save**.

   To test an item: Select the item, then click **Test**. In the test dialog, select the Hostname or IP, then click **Start**.

   To delete an item: Select the item, click **Delete**, then confirm the deletion.

   To import credential data: Click **Import**. In the dialog, click **Browse...** to select the CSV file, then click **Import**. (See the *Discovery Import Formats* topic for import file syntax.)
2. Click **Next**.

Setup Wizard: Seed Routers

Note: Definition of seed routers is highly recommended for IPv4 networks and is required for IPv6 networks.

NetMRI uses seed routers to quickly perform network discovery. Seed routers are also given priority for determining which devices are counted toward NetMRI's license limits.

The table lists each defined seed router with its discovery status (as defined in the **Network Insight** tab –> **Discovery** tab). By reviewing the discovery status for each seed router you can determine whether NetMRI should be able to discover the network successfully, or if there are possible configuration errors preventing network discovery, without having to wait to see what NetMRI finds.

Do the following:

1. Enter IP addresses for seed routers.

   To add an item: Click **New**, enter the value in the **Seed Router IP Address** field, then click **Add**.

   To edit an item: Select the item, click **Edit**, change the fields above the table, then click **Save**.

   To force immediate discovery: click **Discover Now**.

   To delete an item: select the item, click **Delete**, then confirm the deletion.

   To import discovery setting data: click **Import**. In the dialog, click **Browse...** to select the CSV file, then click **Import**. (See the *Discovery Import Formats* topic for information on import file syntax.) The imported file data is applied as a set of one or more Seed Routers. Ensure correct values before importing.
2. Click **Next**.

Setup Wizard: Device Type Hints

Device hints are optional and are used to speed network discovery and assist with determination of device types without other discovery data.

Device hints help NetMRI locate specific types of network devices using IP address patterns and DNS name patterns. For instance, if many routers are found at an IP address ending with ".65", specifying "*.*.*.65" and associating the Router device type for an IP address hint, allows NetMRI to prioritize discovered devices matching that hint higher in its credential collection queue to help speed discovery. The hint is taken into account when NetMRI attempts to determine a device's type. Also, you can specify the device type itself in the hint—**router**, **switch**, **switch-router**, **firewall**, and numerous other choices.

Valid IP address patterns are the numeric values of the octet, or an asterisk for any number of octets in the IP address. For device name matches, valid DNS characters and the * character are valid definitions. For example, *rtr* matches any device name with "rtr" in it's definition.

Do the following:

1. Enter information for device type hints, if necessary.

   To add an item: Click **New**, select the type in the **Device Type** drop-down list, enter the required value in the **IP Address** field, then click **Add**.

   To edit an item: Select the item, click **Edit**, change the fields above the table, then click **Save**.

   To delete an item: select the item, click **Delete**, then confirm the deletion.
2. Click **Next**.

Setup Wizard: Device Interrogation Techniques

This Wizard step defines the methods by which NetMRI polls network devices for information. Those protocols are based upon three methods: CLI, SNMP and ARP.

Do the following:

1. Select desired interrogation options (descriptions are provided in the Wizard step, and in the topic). Enable any options you consider applicable for your network.
2. Click **Next**.

Setup Wizard: Configuration Collection

This Wizard step defines the methods by which NetMRI obtains information such as routing tables, ARP tables and configuration files.

Do the following:

1. Select desired configuration collection options (descriptions are provided in the Wizard step). Under most circumstances, it should not be necessary to modify settings in this step.
2. Click **Next**.

Setup Wizard: Summary

Do the following:

1. Study the summary information in this final Wizard page before finishing setup. For any item flagged as a possible configuration problem, click the **Edit** link to go directly to the corresponding step in the wizard to make changes. After making changes, return to the Summary step.
2. Click **Finish**.

Additional Considerations

Additional considerations for integrating NetMRI into the operational network environment include the following:

Domain Name Assignment

For long-term use, Infoblox recommends adding NetMRI to the network's DNS server configuration to allow references by name to NetMRI instead of IP address. You are free to assign any name to the NetMRI server, but Infoblox recommends using the same Server Name that is assigned to NetMRI in the first step of the NetMRI setup process. When doing so, the DNS name, SNMP system name and HTTPS server certificate name will all be consistent.

HTTPS Accessibility

Note: Some browsers, such as Internet Explorer, automatically display the certificate dialog if the host name used in the URL is not the same as the name provided in the server's certificate. Infoblox recommends the DNS name used to access the NetMRI server, and the Server Name entered when configuring NetMRI, be the same value.

NetMRI accepts browser requests on the standard HTTP port (80), and the HTTPS port (443) for additional security. During the initial setup process, the **Server Name** assigned to NetMRI is used as the HTTPS server certificate name.

When connecting to NetMRI via HTTPS for the first time from a given browser, the browser will display a dialog box indicating that the NetMRI server certificate has not been seen before and that the server is not currently trusted. Check the NetMRI server certificate to confirm that it contains the specified **Server Name** and is signed by "Infoblox, Inc." If the certificate appears authentic, accept and install the certificate using the process supported by the Internet browser. After the certificate is installed, the dialog will no longer appear when you connect to NetMRI using HTTPS.

Shutdown Procedure

NetMRI includes embedded database and file systems to manage the information gathered from the network. Although the database and file systems are designed to be resilient to failures, Infoblox recommends shutting the system down properly to avoid data corruption.

NetMRI can be properly shutdown at the **Settings –> General Settings** section **–> Shutdown Server** page or by using the **halt** command in the Administrative Shell accessible via SSH (see **Other information –> Administrative Shell** in the online help for details).

Resetting to Factory Defaults

Note: Use caution with the Administrative Shell **reset** command. It erases all existing data in the NetMRI system and restores the unit to factory defaults.

If you are evaluating NetMRI on a production network and want to erase all data collected before returning the unit, this is accomplished using the **reset** command in the NetMRI Administrative Shell (accessible via SSH; see reference above). Executing **reset** erases the network database, deletes all files stored in the *Administrator* directory and returns NetMRI to its factory default settings.

Discovery Import Formats

The following sections detail the syntax for CIDR address block data files imported through corresponding tabs in the Discovery Settings page and in the Setup Wizard's Discovery Ranges, Static IPs and Seed Routers steps.

Range Examples

```
<ipv4 or ipv6 CIDR <tab or space CIDR <tab or space INCLUDE | IGNORE | EXCLUDE
```

Keyword CIDR is optional.

INCLUDE, IGNORE and EXCLUDE are optional. If not specified, INCLUDE is assumed.

Examples:

```
1.1.1.1/32 CIDR EXCLUDE
1.1.1.1/32 EXCLUDE
```

```
fe80:0:0:0:0:0:ac10:100/113 INCLUDE
```

```
fe80::ac10:1ff/128 EXCLUDE
```

```
<ipv4 or ipv6 CIDR,CIDR,INCLUDE | IGNORE | EXCLUDE
```

Keyword CIDR is optional.

INCLUDE, IGNORE and EXCLUDE are optional. If not specified, INCLUDE is assumed.

Examples:

```
1.1.1.1/32,CIDR,INCLUDE
1.1.1.1/32,INCLUDE
```

```
A.B.C.D-A.B.C.D <tab or space RANGE <tab or space INCLUDE | IGNORE | EXCLUDE
```

Keyword RANGE is optional.

INCLUDE, IGNORE and EXCLUDE are optional. If not specified, INCLUDE is assumed.

Examples:

```
10.1.1.1-10.1.1.255 RANGE EXCLUDE
172.16.1.1-172.16.1.255 EXCLUDE
```

```
fe80:0:0:0:0:0:ac10:100/113-fe80:0:0:0:0:0:ac10:1ff/128 RANGE EXCLUDE
```

```
fe80::ac10:100/113-fe80::ac10:1ff/128 RANGE EXCLUDE
```

```
A.B.C.D-A.B.C.D,RANGE,INCLUDE | IGNORE | EXCLUDE
```

Keyword RANGE is optional.

INCLUDE, IGNORE and EXCLUDE are optional. If not specified, INCLUDE is assumed.

Examples:

```
1.1.1.1-1.1.1.255,RANGE,EXCLUDE
1.1.1.1-1.1.1.255,EXCLUDE
```

```
<ipv4 or ipv6 pattern <tab or space WILDCARD <tab or space INCLUDE | IGNORE | EXCLUDE
```

Keyword WILDCARD is optional.

INCLUDE, IGNORE and EXCLUDE are optional. If not specified, INCLUDE is assumed.

Examples:

```
10.1.1.* WILDCARD EXCLUDE
10.1.1.* EXCLUDE
```

```
<ipv4 or ipv6 pattern,WILDCARD,INCLUDE | IGNORE | EXCLUDE
```

Keyword WILDCARD is optional.

INCLUDE, IGNORE, and EXCLUDE are optional. If not specified, INCLUDE is assumed.

Examples:

```
10.1.1.*,WILDCARD,EXCLUDE
10.1.1.*,EXCLUDE
```

NetMRI will import files previously exported from a discovery settings grid. The export file must have a header line, and each column is comma-separated.

Static IP Examples

```
<ipv4 or ipv6 address <tab or space INCLUDE | IGNORE | EXCLUDE
or
<ipv4 or ipv6 address,INCLUDE | IGNORE | EXCLUDE

INCLUDE, IGNORE and EXCLUDE are optional. If not specified, INCLUDE is assumed.

208.13.222.237 IGNORE

2002::d00d:deed INCLUDE
```

NetMRI will import a file previously exported from a discovery settings grid. Export files must have a header line, and each column is comma-separated.

Seed Router Examples

```
<ipv4 or ipv6 address

2002::d00d:feed
```

NetMRI will import a file previously exported from a discovery settings grid. The Export file must have a header line, and each column is comma-separated.

Credential Import Formats

The syntax for credential data files imported through corresponding tabs in the **Settings** icon –> **Setup** –> **Credentials** page, and in the Setup Wizard's *Setup Wizard: CLI Credentials*, *Setup Wizard: SNMPv1/2 Credentials* and *Setup Wizard: SNMPv3 Credentials (Rare)* steps, is described in this section.

For credential import, NetMRI also accepts files previously exported from a credential settings table, ignoring any priority values in imported files. To specify a different collector in the import file, remove the UnitID column and update the Collector field. *Table 4.2* provides the list of supported credential types and their associated data types.

Note: When importing credentials on an Operations Center, if no collector is specified in the import file, the credentials will be applied to all collectors.

Table 4.2 CLI Credentials

SNMPv1/2 and SNMPv3 Credentials	
SNMP Credentials	‹community string›
SNMP Vendor Defaults	‹community string› ‹tab› ‹vendor name›
SNMPv3 noAuthNoPriv credentials	‹snmpv3 user›
SNMPv3 authNoPriv credentials	‹snmpv3 user› ‹tab› ‹auth protocol› ‹tab› ‹auth password›. The authentication protocol is `md5` or `sha`.
SNMPv3 AuthPriv Credentials	
`<snmpv3 user> <tab> <auth protocol> <tab> <auth password> <tab> <priv protocol> <tab> <privacy password>`	`<priv protocol>` is 3des, aes or des.
CLI Credentials	
`<username> <tab> <password>`	`<username>` can be empty for a line password credential.
`ENABLE <tab> <password>`	Used for privileged mode passwords.
`<username>`	For username -only scenarios.
`<tab> <password>`	For password-only scenarios.
CLI Vendor Default Credentials	
`<username> <tab> <password> <tab> <vendor>`	‹Username› can be empty for a line password credential. ‹Password› can be empty.
`ENABLE <tab> <password> <tab> <vendor>`	Used for privileged mode passwords.

Configuring NetMRI Collectors

Recommended NetMRI Operations Center deployments use the following:

- A physical NetMRI appliance as the central node (termed the Operations Center), and one or more virtual machine-based NetMRI nodes that operate as data collectors across the managed network;
- A NetMRI virtual appliance as the central node (termed the Operations Center), and one or more virtual machine-based NetMRI nodes that operate as data collectors across the managed network

This chapter describes how to install and set up NetMRI virtual appliances to operate as Collectors as port of a larger Operations Center environment.

Note: When you deploy NetMRI Collectors, the Collectors themselves do not run Discovery. Discovery is done through the Operations Center after the collectors are registered to the Operations center.

Infoblox partners and customers download and run at least one instance of NetMRI as a virtual appliance within a VMware server. The virtual appliance comes bundled with all required system components, simplifying installation. The NetMRI instance is called a *Collector*.

Each Collector is separately licensed and configured to operate as part of the NetMRI Operations Center environment.

As a virtual appliance, NetMRI dynamically scales with Virtual Machine resources for CPU, memory and disk allocations, allowing greater flexibility than a traditional hardware appliance. VMs also may be easier to deploy and manage as data collectors than hardware appliances.

Note: Any NetMRI appliance, whether virtual or physical, can operate as a Collector. The working assumption in this guide is that NetMRI VMs are being deployed as Collectors.

A NetMRI virtual appliance is ideal for customers seeking to do the following:

- Deploy an Operations Center to collect data from multiple remote NetMRI Collectors. This is the optimal application for NetMRI Operations Center.
- Take advantage of the benefits of running a virtual appliance to reduce data center footprints and provide scalability to NetMRI.
- House multiple NetMRI Collectors on one VM server, or distribute NetMRI Collectors to VMware servers reflecting the existing topology of their environment.

Because VMware installation parameters and hardware configurations vary, this section presents configurations that have worked well for NetMRI installations, outlines general best practices for VMware installations and provides full instructions for setting up NetMRI virtual machines to act as Collectors in the NetMRI Operations Center.

Note: The hardware on which NetMRI runs should be supported by an uninterruptible power supply (UPS) to avoid data corruption problems should there be a power outage.

NetMRI Virtual Appliance Installation Worksheet

Table 4.3. provides a quick-reference list of the tasks to perform when installing and deploying a VM-based version of NetMRI.

Table 4.3 NetMRI Virtual Appliance Worksheet

		Procedure	See Section
□	1.	Review recommended best practices and verify that the VMware and platform on which NetMRI will be deployed adheres to Infoblox's recommendations.	*Best Practices for configuring NetMRI Virtual Appliances*
□	2.	Review the recommended VMware server requirements and record the following information: Number of devices to be monitored:________________________________ Number of interfaces to be monitored:______________________________ VMware hypervisor:____ Number of vCPUs:____ Memory available:____ Size of local disk storage:_______________________________________	*Benchmarking the VMware Infrastructure*
□	3.	Install and run the Benchmarking Suite on the VMware server.	*Benchmarking the VMware Infrastructure*
□	4.	Confirm that the platform meets NetMRI Virtual appliance requirements: MySQL Bench Alter Table Result: _____seconds (should be less than 15 seconds) MySQL Bench Create Result: ________seconds (should be less than 30 seconds) MySQL Bench Wisconsin Result: _____seconds (should be less than 7 seconds)	*Benchmarking the VMware Infrastructure*
□	5.	Download and unpack the NetMRI Virtual appliance ZIP archive.	*Downloading and Unpacking the Virtual Appliance ZIP Archive*
□	6.	Import the Virtual appliance files. (Follow instructions in the subsection for the appliance Distributable downloaded in step 5.)	*Importing the Virtual Appliance Files*
□	7.	Configure the NetMRI Virtual appliance.	*Installing NetMRI Virtual Appliances (for Collectors)*
□	8.	Configure NetMRI network interface. Network configuration is done in the virtual appliance Installation Wizard under your VMware version. NetMRI's IP address is now: ___________________________	*Configuring Network Interfaces*
□	9.	Configure NetMRI using the Setup Wizard. (Performed on the Operations Center node only.)	*Configuring NetMRI Using the Setup Wizard*
□	10.	Register the NetMRI VM with the Operations Center controller.	*Configuring and Registering NetMRI Collectors*
□	11.	Monitor the initial discovery process.	*Monitoring the Initial Discovery Process*

Installing NetMRI Virtual Appliances (for Collectors)

Getting started with the NetMRI Virtual appliance is a three-step process, summarized as follows:

1. Downloading and unpacking the Virtual appliance ZIP archive.
2. Importing the Virtual appliance files as a new VM.
3. Configuring the NetMRI Virtual appliance.

Details are provided in the next sections.

Downloading and Unpacking the Virtual Appliance ZIP Archive

Adding additional vCPUs to the NetMRI Virtual appliance should be done in accordance with the VMware administration guide. No additional configuration of NetMRI is needed when adding additional processors.

1. Download the appropriate appliance distributable according to *Table 4.4*.
2. If you download an OVF version, unzip the file into a directory on your computer.
3. Install the distributable according to the corresponding instructions in the next section.

Table 4.4 VMware Software Support

VMware Version	Zip (VMX)	OVF 1.0	OVA
vSphere/vCenter 5.x/6.x (ESXi 5.x/6.x managed hosts)		Yes	Yes
ESXi 5.x/6.x Standalone		Yes	Yes
VMware Workstation, Player 10.x and later	Yes		
VMware Fusion 8.x and later	Yes		

Instructions provided below are for a limited selection of VMware versions. Consult the administrator documentation for the VMware product involved in the deployment for more information on OVA or OVF image file installation.

Installing on vSphere/vCenter 5.x/6.x and ESXi 5.x/6.x

Do the following:

1. Download the .zip archive containing the appropriate OVA/OVF NetMRI virtual appliance template and unzip it into a directory on your computer.
2. Import the unzipped OVA/OVF template using either VMware vSphere Client or VMware vSphere/ESXi Web Client. For more information on the OVA/OVF import into VMware vSphere/vCenter/ESXi environments, refer to VMware documentation.

   The NetMRI virtual appliance is installed on your ESXi host. Installation may take 10-20 minutes, depending on your hardware and network speed.
3. Continue to *Configuring and Registering NetMRI Collectors* on page 49.

Installing on VMware Workstation 10.x and Later

Do the following:

1. Download the.zip archive containing the appropriate VMX/VMDK NetMRI virtual appliance and unzip it into a directory on your computer.
2. Open the unzipped VMX/VMDK NetMRI virtual appliance in VMware Workstation. For more information on running VMX/VMDK virtual appliances on VMware Workstation, refer to VMware documentation.

   The new VM is displayed in a tab in the VMware Workstation's main window.

Continue to *Configuring and Registering NetMRI Collectors* on page 49.

Configuring and Registering NetMRI Collectors

One of three different methods are used to set up NetMRI Collector nodes in an Operations Center deployment:

- You can install a new NetMRI instance on a VM (or a NetMRI physical appliance, for that matter), allow it to fully discover the network, and then run the **register** command to register the NetMRI instance with a newly configured Operations Center;
- You can install the Operations Center and run the Setup Wizard to perform initial configuration. Then, install the NetMRI virtual appliances, that will act as Collectors, into their VMware server(s). On each NetMRI VM, run the NetMRI admin shell **configure server** command to set up basic IP information and immediately run the NetMRI admin shell **register** command to register the NetMRI VMs to the Operations Center. Global settings will be synchronized with the OC node and you configure the discovery ranges and other Discovery settings in the OC for the network-wide process. This procedure is described in this section;
- Migrate from a standalone NetMRI appliance to an Operations Center environment, as described in *Configuring An Operations Center Controller From an Existing NetMRI Instance* on page 35.

After installing the Virtual appliance in your VMware server, follow the instructions below to configure it to run on your network.

1. Log in to VMware Virtual Center, ESX, Workstation, etc.
2. Power on the NetMRI Virtual appliance you imported earlier.
3. Open the console view of the NetMRI virtual appliance.
4. After the initial boot, you will see a license agreement. Read the agreement (press SPACE to page down). At the prompt, enter **yes**, then press ENTER.
5. The boot will continue for about five minutes as the NetMRI application configures itself.
6. When the blue screen is displayed, select **Log in** using the arrow keys, then press ENTER.
7. Enter the default user name **admin** and the default password **admin**. This puts you in the admin shell of NetMRI, a command line interface.
8. Run the **configure server** command and define the IP configuration for the NetMRI virtual machine.

Note: You can change the password later when running through NetMRI's browser-based interface.

Repeat the instructions in this section for each NetMRI instance you want to add to the Operations Center system.

1. Log in to the admin shell on the NetMRI instance being added to the Operations Center system.
2. At the command prompt, run the **register** command.
3. At the `Register this system?` prompt, respond with **y**.
4. The instance will automatically restart. After restarting, the instance will be a Collector in the Operations Center system.

Note: As part of the registration process, the admin password on the Collector is synchronized with the password on the Operations Center Controller. Therefore, after registration is complete, the admin password for the Collector may be different than the password you initially used to log in to the admin shell on that instance.

After registration, the NetMRI GUI will not be visible on this instance. All access to the instance must be through the Controller. You access the NetMRI GUI from the Operations Center Controller.

When you execute Discovery on the Operations Center, it automatically uses the outlying Collectors as its means for performing Discovery on the network.

Monitoring the Initial Discovery Process

Discovery does not run on the Operations Center node. The discovery process takes place on the collectors after they are registered to the Operations Center.

Note: The NetMRI online Help and its associated NetMRI Administrator's Guide provide substantial details on setup and discovery topics that is beyond the scope of this document. Consult the topic *Configuring and Executing Network Discovery* and its subtopics in NetMRI's online Help for greater detail on all associated elements of network discovery.

After the NetMRI setup process has been completed, check discovery progress in the **Tools –> Network** section –> **Discovery Status** page. If the Default Gateway, CIDR blocks, SNMP credentials and Telnet/SSH credentials were entered correctly, you should start to see devices listed in this table within a few minutes.

Periodically click the **Refresh** button to see how discovery is progressing.

At this point, you can return your workstation to its previous network configuration. Further access to NetMRI is done by accessing the IP address assigned in the Setup Wizard Step 4 or using the DNS name that has been associated with that address.

For IPv6 networks, NetMRI discovers and stores the following information about IPv6 interfaces on network devices:

- The IPv6 networks and subnet masks
- Link-local interface IP addresses
- Globally routable interface IP addresses
- VRRP/HSRP virtual IP address (if applicable)
- Associated VLANs
- GLBP virtual IP (if applicable)
- BGP AS and neighbor adjacencies (if applicable)
- Cisco VoIP endpoint devices

When NetMRI discovers devices, IPv4 and IPv6 addresses are reported equally by the appliance.

Troubleshooting

If no devices appear within a few minutes, verify the accuracy of the network information added during the configuration process as follows:

1. In the NetMRI header panel, click the **Settings** button. In the menu along the right side of the **Settings** window, click the **Setup** section, then click **Discovery Settings**. Ensure that the given CIDR blocks cover the desired parts of your network. Also, ensure that the Default Gateway is covered by one of the Included CIDR blocks, but not by one of the Excluded CIDR blocks.
2. In the menu along the right side of the **Settings** window, click **Collectors and Groups** (just above **Discovery Settings**). Ensure that **SNMP collection** is Enabled. In the **Settings** window, click **SNMP Credentials** and verify that the community strings for your network devices are entered properly (e.g., check spelling and case-sensitivity).
3. If NetMRI was configured using a crossover Ethernet cable and NetMRI was not on the network following completion of the configuration process, initial probes of the network may not be successful. Navigate to **Settings –> Settings** section –> **Discovery Settings** and click the **Reset Discovery Counters** button (below the table) to kick off the initial network probes again, then monitor the discovery process.

Any changes made using the forms described above will be automatically used by the discovery process. If the new information is correct, you should start to see devices appearing in the table at **Network Explorer –> Inventory** tab –> **Devices / Interfaces** section –> **Devices**.

Reviewing Operations Center Configuration Details

To review Controller configuration details and list connected Collectors:

1. Log in to the administrative shell on the Controller.
2. Run the **show tunserver** command.

To review Collector configuration details:

1. Log in to the admin shell on the Collector.
2. Run the **show tunclient** command.

Adding More Resources

As a virtual appliance, NetMRI allows allocation of additional VMware server resources to the VM. Additional resources can be in the form of additional vCPUs, additional memory, and/or additional storage.

Adding vCPUs	Adding additional vCPUs to the NetMRI virtual appliance should be done in accordance with the VMware administration guide. No additional configuration of NetMRI is needed when adding additional processors. Keep in mind that more is not always better. Due to context-switching, adding additional vCPUs to NetMRI may impair performance.
Adding Memory	Allocating additional memory to any NetMRI virtual appliance should be done in accordance with the VMware administration guide.
Adding Storage	Allocating additional storage to the NetMRI virtual appliance should be done by adding storage as RDM or VMDK-based disks in accordance with the VMware administration guide.

Chapter 5 Deploying Automatic Failover

You can create a NetMRI failover pair using two NetMRI appliances, in which one acts as the primary appliance and the other as the secondary appliance. A failover pair provides a backup or redundant operational mode between the primary and secondary appliances so you can greatly reduce service downtime when one of them is out of service. You can configure two Operation Center (OC) appliances or standalone appliances to form a failover pair.

In a failover pair, the primary appliance actively discovers and manages network devices and serves the Web UI and the CLI over the shared VIP address while the secondary appliance constantly keeps its database synchronized with the primary. Although you can access a failover pair using either the VIP address of the failover pair or the management IP address of the primary appliance, using the management IP is not recommended because during a failover, the roles of the primary and secondary appliances reverse and the management IP becomes unreachable. Accessing the failover pair using the VIP address ensures that you are contacting the active primary appliance. Note that during a failover, all active connections between the NetMRI appliances and the network devices are disrupted and all ongoing processes fail. Also, all active Web UI and CLI sessions are disrupted during a failover and all users with active sessions must reconnect and log in again after the secondary appliance assumes the role of the primary appliance.

Note the following about the automatic failover feature:

- Failover pair is supported only on NetMRI NT-1400, NT-2200, and NT-4000 (G8 only) appliances. It is not supported on NetMRI virtual appliances.
- Failover is supported in NetMRI 7.1.1 and later releases.
- Both the primary and secondary must be of the same appliance model and same software version number.
- The management IP address of both the primary and secondary must be on the same subnet.
- The VIP address, shared by the primary and secondary must be on the same subnet as the management IP address.

Deploying Automatic Failover for New Appliances

Following are the pre-requisites for deploying automatic failover for new appliances:

- Configure two supported NetMRI appliances with licenses installed.
- Both the appliances must be of the same appliance model and same software version number.
- Provision three IP addresses on the same subnet: a VIP address and two management IP addresses for the appliances.
- If you are using direct replication method to connect both appliances, you need an Ethernet cable to connect the systems directly through their HA Ports.

- If you are using the network replication method to connect the appliances, you must connect the systems over a local network and two replication IP addresses must be acquired on the same subnet. You must also select a TCP port for the replication traffic.

Note: Infoblox recommends you to use the direct replication method for best reliability and performance. The network replication method will have higher latency and a greater chance of connection breakage, and thus lower reliability and performance.

You can deploy two new Operation Center (OC) or standalone appliances to form a failover pair, as follows:

1. Set up and configure two new NetMRI appliances as separate systems. Ensure that the appliances are running NetMRI 7.1.1 or later.
2. Connect both the systems using one of the following methods:
   - Direct replication: Connect the systems directly through their HA ports.
   - Network replication: Connect the HA port of both systems to a network using an Ethernet cable.

   Infoblox recommends that you connect the systems using the direct replication method.
3. Run the Setup Wizard on both appliances and set the admin password and install the license. The admin password must be the same on both systems.

   At this point of time, it is not necessary to complete the entire configuration wizard on both systems. You can complete the configuration only on the primary system.
4. If the systems were not shipped with version 7.1.1 or greater, you must upgrade the systems to the latest release.
5. After upgrading both systems to NetMRI 7.1.1 or later, repartition the systems by logging in to the Admin Shell of both the systems and enter the **repartition** command.

   For new systems with no network device data collected, you can proceed without resetting and without generating a backup. For systems that are already deployed, and have collected data, follow the steps mentioned in *Migrating Existing Systems as Failover Pairs* on page 54.
6. Choose one system to take the primary role. You can choose the system for which you have completed the entire configuration, otherwise the configuration might be lost.
7. Log in to the primary system, go to **Settings** -> **Setup** -> **Failover Configuration**, and then specify the configuration settings in the **Failover Configuration** page.

Note: After specifying the failover configuration settings and completing the enable operation, the systems start synchronizing data. This process might take up to one hour, depending on the appliance model.

Migrating Existing Systems as Failover Pairs

You can migrate two existing Operation Center (OC) or standalone appliances to form a failover pair. Ensure that both appliances are running versions NetMRI 7.1.1 or later.

Following are the pre-requisites for migrating existing systems as a failover pair:

- Two supported NetMRI appliances with licenses installed. You can choose an existing appliance and a second appliance of the same model.
- Provision two additional IP addresses on the same subnet: a management IP address assigned to each system and a VIP address shared between the failover pair.
- If you are using direct replication method to connect both appliances, you need an Ethernet cable to connect the appliances directly through their HA ports.
- If you are using network replication method to connect the appliances, you must connect the systems over a local network and two replication IPs must be acquired on the same subnet. You must also select a TCP port for the replication traffic.

To migrate two existing systems to form a failover pair:

Note: In the below steps, the system that is referred to as the second system takes the primary role and the system that is referred to as the existing system takes the secondary role in the failover pair.

1. Choose an existing NetMRI system and configure a second NetMRI system of the same model.
2. If you are using scan ports, connect the scan ports of the second system to the network in the same way as the existing system.
3. Connect both systems using one of the following methods:
   - Direct replication: Connect the systems directly through their HA ports.
   - Network replication: Connect the HA port of both systems to a network using an Ethernet cable.
4. Run the Setup Wizard on the second system and set the admin password and install the license.
5. Exit the Setup Wizard after setting the password and installing the license on the second system.
6. Upgrade the systems to NetMRI 7.1.1, if necessary.
7. After upgrading both systems to NetMRI 7.1.1 or later, repartition the systems to prepare them for automatic failover, as follows:
   - Log in to the Admin Shell on the second system, and enter the **repartition** command. Note that if the system is already partitioned for failover, an error message appears when you run the **repartition** command.
   - Generate a database archive of your existing system, and restore this to the second system. Re-enable SNMP collection after restoring the archive on the second system. To enable SNMP collection, go to **Settings -> Setup -> Collection and Groups -> Global** tab -> **Network Polling side** tab, and then select the **SNMP Collection** check box.
   - If the data restore is not successful, do not proceed to the next step. If the restore failed due to disk space exhaustion, you may try reducing data retention settings on your existing NetMRI system to reduce the archive size. For more information, refer to the *Infoblox NetMRI Administrator Guide* or contact Infoblox Support for further assistance. Note that it might take up to 24 hours for reduced data retention settings to take effect.
   - If the data restore is successful, log in to the Admin Shell on the existing system, enter the **reset system** command, and then enter the **repartition** command. Note that if the system is already partitioned for failover, an error message appears when you run the **repartition** command. After repartitioning is complete, run the **configure server** command, install the license, and then reset the admin password in GUI to match the other system.
8. If you want to use the management IP address of your existing system as the VIP of the failover pair, then you must change the management IP address of the existing system.
9. Configure the second system to take the role of the primary system, as follows:
   - Log into the second system.
   - Go to **Settings -> Setup -> Failover Configuration**.
   - Specify the configuration settings in the **Failover Configuration** page.
10. For an Operation Center, complete the following:
    - Log in to the Admin Shell on the Operation Center and run the **reset tunserver** and **configure tunserver** commands. Enter the VIP address of the Operation Center when prompted for the IP address of the Operation Center server.
    - Log in to the Admin Shell on each Collector and run the **reset tunclient** and **register tunclient** commands. Enter the VIP address of the Operation Center when prompted for the IP address of the Operation Center.

Note: After specifying the failover configuration settings and completing the enable operation, the systems start synchronizing data. This process might take up to one hour, depending on the appliance model. For details about how to configure these settings, refer to the *Infoblox NetMRI Administrator Guide*.

NEXT LEVEL NETWORKING

Corporate Headquarters | 3111 Coronado Dr. | Santa Clara, CA | 95054
+1.408.986.4000 | 1.866.463.6256 (toll-free, U.S. and Canada) | info@infoblox.com | www.infoblox.com