



Cisco Prime Virtual Network Analysis Module (vNAM) Installation and Configuration Guide

August, 2014

Cisco Systems, Inc.

www.cisco.com

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

Text Part Number:

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco Prime Virtual Network Analysis Module (vNAM) Installation and Configuration Guide
© 2014 Cisco Systems, Inc. All rights reserved.



Preface

This document contains information about installing and configuring Cisco Prime Virtual NAM (Prime vNAM). There are specific sections that provide information based on your hypervisors. There are installation differences between hypervisors, so be sure to refer to the appropriate sections for your setup.

Audience

This guide is designed for personnel who install, configure, and maintain Prime vNAM

Prime vNAM is deployed on a virtual server. These engineer must be conversant with VMware or Red Hat KVM virtualization systems, and be familiar with virtualization concepts and virtualized environments.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to *What's New in Cisco Product Documentation* as an RSS feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service. Cisco currently supports RSS Version 2.0.



Introduction

This guide explains how to install and configure the Cisco Prime Virtual NAM (Prime vNAM) on virtualized servers.

Prime vNAM is a network management software that can be downloaded and installed on any x86 server with the supported virtualization environment.

Installation Overview

The following table describes a summary of the main tasks involved in the Prime vNAM installation.

Task	See...
1. Review the Prime vNAM requirements for your virtual environment (ESXi or KVM).	Installation Requirements, page 2-1.
2. Download the Prime vNAM OVA file for ESXi or ISO file for KVM from Cisco.com.	<ul style="list-style-type: none">• Downloading Your Prime vNAM Virtual Appliance OVA File, page 3-1• Downloading Your Prime vNAM Virtual Appliance ISO File, page 4-2
3. Install Prime vNAM software on the virtual machine	<ul style="list-style-type: none">• Installing Cisco Prime vNAM on VMware vSphere ESXi, page 3-1• Installing Cisco Prime vNAM on Red Hat Enterprise Linux KVM, page 4-1
4. (Optional) Request permanent license to replace 60-day evaluation license	Installing the License, page 2-3.



Installation Requirements

This chapter provides details about the host and client requirements that should be met before you deploy and configure Cisco Prime Virtual Network Analysis Module (Prime vNAM). The following sections contain information about the requirements and restrictions:

- [Host Configuration Requirements, page 2-1](#)
- [Client Requirements, page 2-2](#)

Host Configuration Requirements

For Prime vNAM you must have the following;

- Any X86_64 hardware has adequate resources to deploy a virtual environment for Prime vNAM. See [Table 2-1](#) for hardware requirements.
- VMware with ESXi or RHEL with KVM installed on the hardware of choice. See [Table 2-1](#) for supported hypervisor details.

The hypervisor must have access to the Prime vNAM software image on an FTP or HTTP server for deployment.

The Cisco Prime vNAM virtual appliance supports the platforms/hypervisors in [Table 2-1](#).

Table 2-1 Requirements Per Prime vNAM¹

Supported Hypervisors	RAM	CPU	Network	Hard Disk
VMware vSphere 5.1 (ESXi 5.1 and later)	4 GB per vNAM	Two CPU core	Two virtual NICs (VMXNET3)	100 GB for a vNAM ² (PVSCSI storage driver)
Red Hat Enterprise Linux and included KVM that comes with RHEL 6.1			Two virtual NICs (virtio)	100 GB per vNAM ² (IDE/SCSI))

1. Any deviation from the system requirements may cause unexpected results and is not supported.
2. VMware configuration is automatic when you use the OVA; manual configuration of KVM is required.

**Note**

Before you deploy the virtual appliance, verify that your host server is running on supported hardware. If you are not sure whether your environment can support a 64-bit VM, you should verify using your server tools. For ESXi, you can verify by downloading and running the VMware CPU Identification Utility which indicates 64-bit VMware support. This utility can be found on the VMware site at: http://www.vmware.com/download/shared_utilities.html. For RHEL, you can run **uname -a** from the command line shell.

Client Requirements

The following table lists the client requirements:

Hardware	IBM-compatible or Macintosh computer with 2-GHz or faster processor
RAM	1 GB
Operating System	<ul style="list-style-type: none"> • Windows 7 • Windows Vista with Service Pack 1 • Windows XP Professional with Service Pack 2 • Red Hat Enterprise Linux 6.1 (base server)
Browser	<ul style="list-style-type: none"> • Microsoft Internet Explorer 9.0 on Windows XP Professional with Service Pack 2, Windows Vista with Service Pack 1, or Windows 7 • Mozilla Firefox 17.0.5 (ESR) or later on Windows XP Professional with Service Pack 2, Windows Vista with Service Pack 1, Windows 7, FireFox on OSX, or Red Hat Enterprise Linux <p>All browsers require that you enable cookies, JavaScript/scripting 1.7 or later, and popup windows. If you reinstall Prime vNAM or upgrade to a newer release, before you access the appliance, make sure that you delete the cookies and clear the browser cache of each client.</p>

Licensing

The Prime vNAM software requires a product license to run. An evaluation license is included with the product. It allows you to use the software for up to 60 days. When using an evaluation license, open the About window to view licensing information such as how many days remain before the evaluation license expires or details about your permanent license.

The evaluation license has a traffic limitation of 100 Mbps. After 60 days, you will no longer be able to access the user interface and must install a permanent license. After you purchase your license, you have permanent access to the software.

You have two license options for Prime vNAM—NAM-VX10 and NAM-VX20. The difference between the options is in the performance in terms of traffic monitoring throughput. See the [Cisco Prime Virtual Network Analysis Module Data Sheet](#) for details.

You can use the 60-day evaluation license to run Prime vNAM out-of-the-box and obtain your permanent license from Cisco to complete the license installation before the license expires. Your login window indicates how many days remain before the evaluation license expires. You will be unable to log in to the user interface after the evaluation license expires.

For details about installing a license, see [Installing the License, page 2-3](#). For CLI licensing commands, see the [Cisco Prime Network Analysis Module Command Reference Guide](#).

Installing the License

This section describes how to obtain and install the Prime vNAM license on the virtual appliance.

SUMMARY STEPS

1. Install Prime vNAM.
 2. Obtain your product ID (PID) and serial number (SN) details from the Prime vNAM.
 3. Log into Cisco Product Registration website for your license information.
 4. Copy the emailed license file to your FTP server.
 5. Install the Prime vNAM software license.
-

DETAILED STEPS

Step 1 Install and log into the virtual NAM. See [Installation Overview, page 1-1](#).

Step 2 Use the **show inventory** CLI command from the Prime vNAM console to obtain the PID and SN. For example:

```
vnam1# show inventory
PID: ESX VID: SN: <serial number>
vnam1#
```

Here:

- PID—Product identification (ID) number of the device
- VID—Version ID of the device. Displays as 0 if the version number is not available

- SN—Serial number of the device.

Step 3 Access your license product activation kit via Cisco.com. Use the PID and SN from the show inventory command to access your unique license.

Step 4 You will receive an e-mail with the PAK information.

Step 5 Copy the PAK file to an FTP server to which you have access from the vNAM server.

Step 6 Install the Prime vNAM license using the **license install** CLI command.

The following is an example of the install license command:

```
license install ftp://joseph@computer.com/bin/licenses/NAM_VA_License.lic
```

In this example, the **install license** command fetches the license file, *NAM_VA_License.lic*, from the directory */bin/licenses* of the *host computer.com*

Step 7 Run **show license** command to see the installed license status.

Configuring Prime vNAM to Receive Data Traffic

In order for the Prime vNAM to receive traffic, you must configure its data port to receive data traffic from your virtual machine. Any traffic that arrives on the data port will be processed and analyzed.

Connectivity using vswitch in VMware ESXi requires promiscuous mode to be configured. See VMware documentation for details.

Connectivity using network bridge on RHEL KVM requires promiscuous mode to be configured. See RHEL documentation for details. See the [Configuring Virtual Network Bridges](#) section for details about creating network bridging.



Installing Cisco Prime vNAM on VMware vSphere ESXi

This section provides instructions on how to install the Cisco Prime vNAM virtual appliance on VMware vSphere ESXi using an Open Virtual Application (OVA) file.

[Table 3-1](#) summarizes how to quickly get up and running on ESXi:

Table 3-1 Installation Overview for ESXi

Task	See...
1. Review the requirements and preparations for Cisco Prime vNAM	Installation Requirements, page 2-1
2. Download the Cisco Prime vNAM OVA file from Cisco.com.	Downloading Your Prime vNAM Virtual Appliance OVA File, page 3-1
3. Install Cisco Prime vNAM software on the virtual machine	Deploying Prime vNAM on VMware ESXi, page 3-2
4. Setting up your connection between Prime vNAM and your virtual machine	Establishing Network Connectivity, page 5-1
5. (Optional) Request permanent license to replace 90-day evaluation license.	Installing the License, page 2-3

Downloading Your Prime vNAM Virtual Appliance OVA File

The Prime vNAM software is distributed as an Open Virtualization Archive (OVA) file. The file contains everything in the Open Virtualization Format (OVF) folder and is all you need to install Prime NAM in an ESX virtualization environment. The OVA defines the network interface requirements for Prime vNAM.

Prime vNAM on ESXi platform is distributed as an OVA file, named `nam-yyy-x.x.x.ova`.



Note

You deploy the Prime vNAM software file directly from any of the supported hypervisors (for example, the vSphere Client); you do not need to extract the archive before performing the deployment.

Step 1

Access the Cisco Prime vNAM application image at the following location:

<https://software.cisco.com/download/navigator.html>

Step 2 Download the file to your desktop and ensure it is accessible.

Deploying Prime vNAM on VMware ESXi

Cisco Prime vNAM virtual appliance is supported for production use on the VMware operating systems (OS).



Note

Virtual management software applications that support the OS (for example, vSphere client installation) are not documented in this guide and are not shipped as part of the Prime vNAM product.

You can install Prime vNAM by deploying the OVA file using the following methods:

Installation Method	See...
vSphere client running on your local desktop	Deploying the Prime vNAM on an ESXi Server Using vSphere Client, page 3-2
VMware OVF tool command-line client	Deploying the Prime vNAM on an ESXi Server Using VMware Command Line, page 3-3

While the following procedures provide a general guideline for how to deploy Cisco Prime vNAM, the exact steps that you need to perform may vary depending on the characteristics of your VMware environment and setup. See VMware documentation for details specific to VMware.

Deploying the Prime vNAM on an ESXi Server Using vSphere Client

You can use a vSphere client to install an instance of Prime vNAM.

To set up the Prime vNAM virtual appliance on VMware ESXi using the OVA file:

Step 1 Download a vSphere client and connect it to the VMware ESXi server. You will need to ensure you use the same IP address as that of the management port.

Step 2 Once connected to the VMware ESXi server, choose **File > Deploy OVF Template** from vSphere menu bar. For details on how to download the OVA file, see [Downloading Your Prime vNAM Virtual Appliance OVA File, page 3-1](#).

Press **Ctrl + Alt** to exit the console at any time.



Note

Do not use **Ctrl + Alt + Del**. This results in a VMware reboot.

Step 3 To select the OVA file from hard disk, click **Browse** and choose the OVA file (.ova) available in the local machine where the vSphere is running, in the directory in which you unzipped the file earlier. You can also enter a URL to download and install the OVA package from the internet.

Step 4 In the Deploy OVF Template Source window, click **Next**.

The OVF Template Details window appears. It displays the product name, the size of the OVA file, and the amount of disk space that needs to be available for the virtual appliance.

Step 5 Verify the OVF template details and click **Next**

The Name and Location window appears.

Step 6 Enter the name of the new virtual appliance (Prime vNAM). If you are using the vCenter to manage the virtual machine, then you also have the option of selecting the location of the inventory.

For example, *nam-vs-x.x-yyy*. Select a location from the Datastore defaults that display. You can also customize a location, if desired.

Step 7 Click **Next**.

The Ready to Complete window appears.

Step 8 Review the setting details of your deployment and click **Finish** to complete the deployment.

A progress bar keeps pace with your Prime vNAM deployment, which can take from 10 to 30 minutes to finish. When the deployment is finished, the Deployment Completed Successfully dialog box opens.

Step 9 Click **Close** to dismiss the dialog box.

Step 10 Edit the Prime vNAM template to map the management and data interfaces network interfaces to the desired configuration before powering up the Prime vNAM.

Step 11 Continue with your post-installation tasks using a console to the Cisco Prime vNAM to perform the steps in the [Establishing Network Connectivity, page 5-1](#).

Deploying the Prime vNAM on an ESXi Server Using VMware Command Line

This section describes how to deploy Prime vNAM from the command line.

As an alternative to using the vSphere Client to deploy the Prime vNAM OVA distribution, you can use the VMware OVF Tool, which is a command-line client.

To deploy an OVA with the VMware OVF Tool, use the following command syntax:

```
ovftool <source locator> <target locator>
```

where <source locator> is the path to the OVA package and <target locator> is the path target for the virtual machine, OVA package or VI. A VI location refers to any location on a VMware product, such as vSphere, VMware Server or ESXi.

For complete documentation on the VMware OVF Tool, see the VMware vSphere or OVF Tool user documentation.



Installing Cisco Prime vNAM on Red Hat Enterprise Linux KVM

This chapter provides instructions on how to install Cisco Prime vNAM virtual appliance on Red Hat Enterprise Linux KVM using an ISO file.

[Table 4-1](#) summarizes how to quickly get up and running on Red Hat Enterprise Linux KVM:

Table 4-1 Installation Overview on KVM

Task	See...
1. Review the requirements and preparations for Prime vNAM	Installation Requirements, page 2-1
2. Set up the network bridges to the Prime vNAM management and data ports. You may also use passthrough mode for data traffic.	Configuring Virtual Network Bridges, page 4-1
3. Download the Prime vNAM ISO file from Cisco.com	Downloading Your Prime vNAM Virtual Appliance ISO File, page 4-2
4. Install Prime vNAM software on the virtual machine	Deploying Prime vNAM on KVM using Virtual Machine Manager, page 4-3.
5. (Optional) Request permanent license to replace 60-day evaluation license	Installing the License, page 2-3

Configuring Virtual Network Bridges

In order to make the Prime vNAM accessible to the public network and to provide an interface that will accept SPAN data, you must create network bridging which reflects the local configuration and matches the bridges appropriately to the interfaces on the VM. This cannot be standardized and delivered as an automatic and simple installation due to the generic KVM environment and requires customer input. You must perform this task before Prime vNAM installation.

This section provides details on how to configure your virtual network bridges for the two required Prime vNAM ports:

- Management port—Bridge to include the external physical management port

You can skip this step if you already have a network bridge configured, which can be used for the Prime vNAM management port.

- Data port—Bridge to include the physical port receiving the SPAN traffic

To configure the virtual network bridges to the Prime vNAM ports:



Note

There are many options, so we recommend you see your Red Hat KVM user documentation.

Step 1 Log into RHEL KVM as root.

Step 2 Enter the commands to add the two bridges.

For example, the commands below assume eth0 is the physical management port and eth1 is the data port.

```
brctl addbr bridge1
brctl addbr bridge2
brctl addif bridge1 eth0
brctl addif bridge2 eth1
```

Continue to [Downloading Your Prime vNAM Virtual Appliance ISO File, page 4-2](#) to download the Prime vNAM image onto your KVM host.

Downloading Your Prime vNAM Virtual Appliance ISO File

The ISO file contains configuration requirements. The file will be named similar to *nam-yyy-x.x.x.bin.gz*. One ISO file contains the pieces necessary for Prime vNAM installation.

Step 1 Access the Cisco Prime vNAM application image at the following location:

<http://software.cisco.com/download/navigator.html>

Step 2 Download the Prime vNAM image onto the RH KVM host where there is enough disk space. Usually /home is the largest partition. An example of the internal download command follows:

```
wget ftp://172.20.98.174/pub/nam1/mydir/kvm/filename.iso -O /home/admin/filename.iso
```

Deploying Prime vNAM on KVM using CLI

You can deploy Prime vNAM using command line interface. See KVM documentation for details. See also the [Host Configuration Requirements](#)

Step 3 To deploy the Prime vNAM and start a console connection, use something similar to the following command. Change the iso path (-disk), and network bridge names as appropriate.

```
virt-install -n <name>_ -c /<path to .iso file> -r 4096 --vcpus=2 --arch=x86_64
--os-type=linux --os-variant=generic26 --disk
path=</path/to/file/that/contains/disk,size=100,bus=ide --network
bridge=<management_bridge>,model=virtio --network bridge=<data_bridge>,model=virtio
```

This command starts a console session on the terminal. You should see the installation process and eventually the Prime vNAM login appears. See [Configuring the Cisco Prime vNAM](#) for details on configuring the Prime vNAM.

Deploying Prime vNAM on KVM using Virtual Machine Manager

This section provides steps to perform Prime vNAM installation on the RHEL KVM operating system. While the following procedure provides a general guideline for how to deploy Cisco Prime vNAM, the exact steps that you need to perform may vary depending on the characteristics of your KVM environment and setup.

These steps assume you have already configured the virtual network bridges before starting the installation. The network bridges enable Prime vNAM to share the KVM host system's physical network connections.

To create a new Prime vNAM virtual machine:

-
- Step 1** Log in to the server, and launch the KVM console.
 - Step 2** Launch the Virtual Machine Manager ,and click the Create a New Virtual Machine icon.
 - Step 3** Enter the unique name for this instance of Prime vNAM and select the installation option, then click **Forward**. In the example below, the name is *vNAM_Sample*.
 - Step 4** Under Choose how you would like to install the operating system, select Local install media (ISO image or CDROM), then click **Forward**.
 - Step 5** Select Use ISO Image, click **Browse** to select the location of the Prime vNAM iso file, then click **Forward**.
 - Step 6** Enter the RAM memory size of 4096 MB and select two CPUs.
 - Step 7** Select **Enable storage for this virtual machine** and ensure the **Allocate entire disk now** check box is checked.



Tip

Ensure the LUN is readable and writeable by everyone if your Prime vNAM is using external storage.

Create a new volume, and choose raw format. You must also enter the maximum size for the storage unit (100GB).

- Step 8** Select the new volume and click **Choose Volume**.
- Step 9** Verify your VM settings, check the **Customize configuration before install** check box.
- Step 10** Click Advanced Options drop-down. Make sure that the bridge you have created for management is selected.
- Step 11** Click **Finish**.
Before you install, make sure the following are configured correctly.
- Step 12** Select **Disk 1** in the installation menu panel, change the advanced option Disk Bus to *IDE*, then click **Apply**.
- Step 13** Select **Boot Options** in the installation menu panel. Check the select hard disk, then click **Apply**.
- Step 14** Select **NIC** in the installation menu panel. The NIC that displays is that of the management port for the Prime vNAM. In the Device Model drop-down, choose **virtio**.
- Step 15** Click **Add Hardware**.
- Step 16** In the Add new virtual hardware window, select **Network**.
- Step 17** From the Host device details drop-down, select the interface on which your Prime vNAM will connect to the network. This will be the bridge you created for data.

- Step 18** In the Device Model drop-down, choose **virtio**.
- Step 19** Click **Finish**. Do a quick review of the NIC and other details.
- Step 20** Close the window.

The installation begins.

We recommend that you monitor the messages that appear in the console window to ensure that you are informed about the progress of the installation process.



Note

You may want to set your hypervisor to automatically power up the Cisco Prime vNAM virtual appliance when power is restored to the hypervisor layer. This will avoid having to manually restart your Prime vNAM software. See your hypervisor software documentation for detailed instructions.



Configuring the Cisco Prime vNAM

This section describes how to establish network connectivity, configure IP parameters, and perform other required administrative tasks using the Prime vNAM command line interface (CLI). It also provides information about how to get started with the Prime vNAM graphical user interface (GUI) and how to perform various system management tasks. You must complete all tasks in this section unless they are marked optional.

This chapter contains the following sections:

- [Establishing Network Connectivity, page 5-1](#)
- [Enabling the Prime vNAM Web Server, page 5-2](#)
- [Checking Your Configuration, page 5-4](#)

For more advanced Prime vNAM configuration information, use the Prime vNAM web server interface or see the *Network Analysis Module Command Reference*. For details on how to use the software, see the *Cisco Prime vNAM User Guide*.

Establishing Network Connectivity

This section describes how to configure Prime vNAM IP parameters and establish network connectivity.

-
- Step 1** Log in to Prime vNAM from the management console as the root user.
- On first log in you will be asked to change the root password. Because this document is available to the public by way of Cisco.com, it is a good idea to change this and all default passwords as soon as possible.
- Step 2** Enter the following CLI commands with the appropriate information for your site:
- Step 3** Use the **ip address** command to configure the Prime vNAM IP address. The syntax for this command is as follows:

```
ip address ip-address subnet-mask
```

Example

```
root@localhost# ip address 172.20.104.126 255.255.255.248
```

- Step 4** Use the **ip gateway** command to configure the NAM default gateway address. The syntax for this command is as follows:

```
ip gateway ip-address
```

Example

```
root@localhost# ip gateway 172.20.104.123
```

- Step 5** You can use the **exsession** command to enable remote login to the NAM using either Telnet or SSH. The syntax for this (optional) command is as follows:

```
exsession on (for Telnet)
```

or

```
exsession on ssh (for SSH)
```

Examples

To configure the NAM to enable Telnet access:

```
root@localhost# exsession on
```

To configure the NAM to enable SSH access:

```
root@localhost# exsession on ssh
```

Once you have established connectivity, continue to the [Enabling the Prime vNAM Web Server, page 5-2](#) section.

Enabling the Prime vNAM Web Server

This section describes how to enable the Prime vNAM web server and browser-based access to the Prime vNAM graphical user interface (GUI).

**Note**

You can enable Prime vNAM to function as an HTTP server or an HTTPS secure server, but not as both simultaneously. HTTPS is optional.

Before you enable the NAM web server and provide browser-based access, confirm that your web browser supports your Prime vNAM software release.

**Note**

For a list of supported browsers, see the [Prime NAM Release Notes](#).

To enable the NAM web server:

- Step 1** Open a Telnet or SSH session to the NAM appliance and at the password prompt, enter your password.

```
telnet {ip-address | hostname}
```

or

```
ssh {ip-address | hostname}
```

- Step 2** Enter one of the following commands to enable either an HTTP server or an HTTPS secure server:

To enable the NAM HTTP web server:

```
ip http server enable
```

(Optional) To enable the NAM HTTPS secure web server:

ip http secure server enable

The NAM requests a web administrator username.

```
Enabling HTTP server...
```

```
No web users are configured.
```

```
Please enter a web administrator user name [admin]: <CR>
```

The NAM web server requires at least one properly-configured web administrator. If the NAM does not prompt you for a web username and password, then at least one web administrator was previously configured.

- Step 3** Enter the username of the web administrator. Otherwise, press **Enter** to use the default web administrator username *admin*.

The NAM requests a password for the web administrator, then requests the password to be entered again to ensure accuracy.

```
New password: <adminpswd>
```

```
Confirm password: <adminpswd>
```

- Step 4** Enter the password for the web administrator and confirm it. Otherwise, press **Enter** to use the default web administrator password *adminpswd*.

- Step 5** To check the NAM web server functionality, launch an approved internet browser and enter the IP address or host and domain name in the browser address field. Then, log in to the NAM web server as the administrative user you configured when you enabled the web server.

- Step 6** (Optional) To configure the NAM appliance system domain name you can use the **ip domain** command. This allows users to enter the domain name instead of the IP address.

ip domain name

Example

```
root@localhost# ip domain your_company.com
```

- Step 7** (Optional) To configure the NAM appliance system hostname, use the **ip host** command.

ip host name

Example

```
root@localhost# ip host nam_machine
```

- Step 8** To configure one or more name servers for the NAM appliance, use the **ip nameserver** command.

ip nameserver ip-address [ip-address] [ip-address]

Examples

```
root@localhost# ip nameserver 172.20.104.10
```

```
root@localhost# ip nameserver 172.20.104.10 172.20.104.20 172.20.104.30
```

Checking Your Configuration

After you finish configuring the NAM appliance for network connectivity, it is a good idea to check your connectivity and verify the IP parameters you have just configured for the NAM appliance.

If you have difficulty with your NAM network connectivity, check your configuration.

-
- Step 1** Use the **ping** command to check connectivity between the NAM appliance and a network device.

```
ping {hostname | ip-address}
```

Examples

```
root@localhost# ping nam_machine.your_company.com
root@localhost# ping 172.20.104.10
```

The following is an example of the **ping** command showing successful connectivity:

```
root@nam_machine.your_company.com# ping 172.20.104.10
PING 172.20.104.10 (172.20.104.10) 56(84) bytes of data.
64 bytes from 172.20.104.10: icmp_seq=1 ttl=254 time=1.27 ms
64 bytes from 172.20.104.10: icmp_seq=2 ttl=254 time=1.13 ms
64 bytes from 172.20.104.10: icmp_seq=3 ttl=254 time=1.04 ms
64 bytes from 172.20.104.10: icmp_seq=4 ttl=254 time=1.08 ms
64 bytes from 172.20.104.10: icmp_seq=5 ttl=254 time=1.11 ms

--- 172.20.104.10 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4003ms
rtt min/avg/max/mdev = 1.043/1.129/1.278/0.090 ms
root@nam_machine.your_company.com#
```

- Step 2** To verify that you have configured the NAM appliance IP parameters successfully, use the **show ip** command.

show ip

```
root@localhost# show ip root@nam1.company.com# show ip
```

The following is an example of the **show ip** command output that shows a configured NAM appliance:

```
root@namesx# sho ip
IP address: 172.20.103.209
Subnet mask: 255.255.255.128
IP Broadcast: 172.20.103.255
DNS Name: nam2_es
Default Gateway: 172.20.103.129
Nameserver(s): 171.68.226.120
HTTP server: Enabled
HTTP secure server: Disabled
HTTP port: 80
HTTP secure port: 443
TACACS+ configured: No
Telnet: Enabled
SSH: Disabled
```



Note

To verify the status of an installation, upgrade, or downgrade or to troubleshoot problems, use commands documented in the [Cisco NAM Command Reference Guide](#), on Cisco.com.



Upgrade Procedures

Cisco occasionally provides upgrades to the software which you can download and install on your Prime vNAM. You might also use the downloadable software to restore your software in the case of a catastrophic failure.

Before you begin the upgrade process, we recommend that you perform a complete backup of your current configuration.

After you upgrade or restore your appliance software, if you have backed up your Prime vNAM configuration, you can restore that configuration and resume network monitoring without undue delay.

This section contains the following topics:

- [Backing Up Your Configuration, page 6-1](#)
After you complete any changes to your appliance configuration, use the command line interface to upload your configuration to an archive server.
- [Upgrading Your Software, page 6-2](#)
Download a version of the current software and use a single CLI command (upgrade) to perform the software upgrade.
- [Restoring Your Configuration, page 6-3](#)
Use the command line interface to restore your previous configuration.

Backing Up Your Configuration

We recommend that you perform a complete backup of your current Prime vNAM configuration.



Note

Having a backup configuration file can save you time and frustration if your server should suffer a hard disk failure that requires you to reformat or repartition your hard disk drives.

To back up your current configuration, use the Prime vNAM CLI **config upload** command like the following:

```
config upload ftp://user:password@server/path
```

For example:

```
config upload ftp://
```

```
admin:secret@172.20.104.11/archive/nam_config
```

The **config upload** command sends a copy of the Prime vNAM running configuration to the destination you specify. The copy of your configuration is stored in a back-up configuration file with an ending suffix of **.config** as in **NAM_host-namxxxx-y.y.y.config**. The destination address should be a valid server name and directory path where you have read and write permissions.

Upgrading Cisco Prime vNAM Virtual Appliance

This section describes the procedures for upgrading Prime NAM to Cisco Prime vNAM virtual appliance and upgrading the operating system for Cisco Prime vNAM virtual appliance. There are two options that are dependent on the circumstances for the upgrade. You can use the upgrade command as long as your Prime vNAM can reboot successfully. If your Prime vNAM has experience a catastrophic event and you can no longer boot the Prime vNAM application, you will need to perform a recovery.

Upgrading Your Software

If your Prime vNAM requires an update to the application image and it is a generic upgrade that does not involve any reboot issues with the Prime vNAM, you should use this procedure.

To download and install a new application image on the Prime vNAM using the preferred method:

- Step 1** Download the Prime vNAM application software for the Prime vNAM from the Cisco.com at the following URL:

<http://www.cisco.com/cgi-bin/tablebuild.pl/nam-appl>


Look for a file that begins with nam-vxyy, as in **nam-vx.x-x-x.bin.gz** (where **x-x-x** is the Prime vNAM software release number). The file will be described as the Virtual NAM Application Image.

- Step 2** Store the Prime vNAM application software on the same server where you archived your Prime vNAM configuration.

If you did not archive your vNAM configuration as recommended previously, you will still need an FTP or HTTP server to serve the application image file.

- Step 3** Use the commands as needed from the list of upgrade commands shown in [Table 6-1](#).

Table 6-1 Upgrade Commands

Command ¹	Purpose
upgrade ftp://user:password@server/path/ filename	Enter the command with the path to the location of the upgrade application image.
upgrade ftp://user:password@server/path/ filename reformat	Reformats the existing installation.
	 Caution All configuration and data will be lost.

1. You may also use HTTP instead of FTP.

For example, use the Prime vNAM CLI command **upgrade** to perform the software upgrade:

```
upgrade
ftp://admin:secret@10.10.10.1/archive/nam_software/nam-app-vnam-x86_64.0-0-0.bin.gz
reformat
```

**Note**

By default, the CDB will be converted to the latest schema.

Step 4

Enter **Yes** to complete the installation.

After the installation is complete, you can log into the user interface.

Restoring Your Configuration

If you have stored your Prime vNAM configuration file at a remote server location that you can access using FTP or HTTP (see [Backing Up Your Configuration, page 6-1](#)), you can restore your Prime vNAM configuration file after a system recovery.

Use the **config network** command to restore your previous Prime vNAM configuration, as in the following:

```
config network ftp://user:password@server/path
```

For example:

```
config network  
ftp://admin:secret@10.10.10.1/archive/nam_config/NAM_host-namxxx-y.y.y.config
```

The config upload command sends a copy of the Prime vNAM running configuration to the destination you specify. The copy of your configuration is stored in a back-up configuration file with an ending suffix of .config as in *NAM_host-namvx-0.0.config*. The destination address should be a valid server name and directory path where you have read and write permissions.





Helper Utility

The following sections describe the [Helper Utility Menu Summary, page A-1](#), what each option does, and any requirements for using a particular option.

Helper Utility Menu Summary



Note

Before you can use menu items 1 and 2, you must first use menu item n to configure network parameters for the module.

Table A-1 *Helper Utility Menu Options Summary*

Menu Option	Description	See...
1	Download the application image and write it to the hard disk drive.	Downloading an Application Image and Writing to HDD, page A-3
2	Download the application image and reformat the hard disk drive.	Downloading an Application Image and Reformatting the HDD, page A-3
3	Display the current Prime vNAM application image version stored on your hard disk.	Displaying Software Versions, page A-4
4	Reset the password for users root and admin to their default values.	Resetting Application Image CLI Passwords to Default, page A-4
6	Change the file transfer method. Only FTP and HTTP are supported.	Changing the System File Transfer Method, page A-4
7	Send a ping to determine if network connectivity exists.	Confirming Network Connectivity Using Ping, page A-4
n	Configure the network parameters for the appliance	Configuring Network Parameters, page A-2
r	Exit the helper utility and power cycle (reboot) into the Prime vNAM application image.	Rebooting a New Application Image, page A-5
f	Check and fix local disk errors	
s	Show upgrade log	

Table A-1 Helper Utility Menu Options Summary (continued)

Menu Option	Description	See...
r	Exit and reset Services Engine	
h	Exit the helper utility and shut down the Prime vNAM appliance.	Shutting Down the Prime vNAM, page A-5

Configuring Network Parameters

Use **Option n** to configure the network parameters for the software.

- Step 1** When the Configure Network Interface menu displays, enter **1** to configure the network manually.

```
-----
Configure Network interface:
1 - Configure network manually
2 - Show config
3 - Write config to application image
r - return to main menu
Selection [123r]: 1
```

- Step 2** The utility prompts you for the IP address, netmask, and default gateway for the module.

```
Enter IP configuration:
IP address []: 172.20.122.93
netmask []: 255.255.255.128
default gateway []: 172.20.122.1
```

```
-----
Configure Network interface:
1 - Configure network manually
2 - Show config
3 - Write config to application image
r - return to main menu
Selection [123r]:
```

- Step 3** To check your network configuration, enter **2**.

```
Selection [123r]: 2

eth0      Link encap:Ethernet HWaddr 00:0E:0C:EE:50:3E
          inet addr:172.20.122.93 Bcast:172.20.122.127 Mask:255.255.255.128
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:210 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:13632 (13.3 KiB) TX bytes:0 (0.0 b)

Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
172.20.122.0 0.0.0.0 255.255.255.128 U 0 0 eth0
0.0.0.0 172.20.122.1 0.0.0.0 UG 0 0 eth0
-----
Configure Network interface:
1 - Configure network manually
2 - Show config
3 - Write config to application image
r - return to main menu
```

Selection [123r]:

Downloading an Application Image and Writing to HDD

Use **Option 1** to download a version of the current application image from an FTP server location and write the image to the hard disk.



Note

If the Prime vNAM application has already been installed and the network settings were configured, they will be automatically be detected by the helper. Otherwise, you must use **Option n** to configure the network *before* using this option.

This option downloads a version of the current application from an FTP server location or from a location you can access using HTTP. You can also [download the latest Prime vNAM software version](#) from Cisco.com.

This URL requires you to have a Cisco service agreement and access to the internet to download the zipped software.

Downloading an Application Image and Reformatting the HDD

Use **Option 2** to download the current application image and write the image to the hard disk.



Caution

Using this option reformats the hard disk before writing the application image and will destroy all data such as reports, packet captures, and configuration. Network connectivity configuration, however, will be retained.



Note

If the Prime vNAM application has already been installed and the network settings were configured, they will be automatically be detected by the helper. Otherwise, you must use **Option n** to configure the network *before* using this option.

This option downloads a version of the current application image from an FTP server location or from a location you can access using HTTP. You can also [download the latest Prime vNAM software version](#) from Cisco.com.

This URL requires you to have a Cisco service agreement and access to the internet to download the zipped software.

Installing an Application Image from CD

Most Prime NAM platforms have the option to map the virtualization system to a virtual CD. If your Prime NAM platform does not have this capability you will need to burn a CD to use if you want to use this option.

Use **Option 3** to install the current application image from the recovery CD. This option might be necessary if you are unable to connect to your network and download a version of Prime vNAM software you archived earlier.


Caution

This option reformats the hard disk before writing the application image and will destroy all data such as reports, packet captures, and configuration. Network connectivity configuration, however, will be retained.

Displaying Software Versions

Use **Option 4** to display the current software application image version stored on your hard disk.

```
Selection [123456789dnfrh]:4
-----
NAM application version: 78-xxxxx-xx(1)
Selection [123456789dnfrh]:
```

Resetting Application Image CLI Passwords to Default

Use **Option 5** to reset the password for users root and admin to their default values.

Changing the System File Transfer Method

Use **Option 6** to change the file transfer method. This option is only necessary if you change the file transfer method by mistake. Only **FTP** and **HTTP** are supported.

```
Selection [123456789dnfrh]: 6
-----
Change file transfer method menu
The current file transfer method is ftp/http.
1 - Change to FTP/HTTP
r - return to main menu
```

Confirming Network Connectivity Using Ping

Use **Option 7** to send a ping to determine if network connectivity exists. When prompted, enter the IP address or full domain name of the location to send the ping.

```
IP address to ping []: 172.20.122.91

Sending 5 ICPM ECHO_REQUEST packets to 172.20.122.91.
PING 172.20.122.91 (172.20.122.91) 56(84) bytes of data.
64 bytes from 172.20.122.91: icmp_seq=1 ttl=64 time=0.151 ms
64 bytes from 172.20.122.91: icmp_seq=2 ttl=64 time=0.153 ms
64 bytes from 172.20.122.91: icmp_seq=3 ttl=64 time=0.125 ms
64 bytes from 172.20.122.91: icmp_seq=4 ttl=64 time=0.102 ms
64 bytes from 172.20.122.91: icmp_seq=5 ttl=64 time=0.166 ms

--- 172.20.122.91 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4000ms
rtt min/avg/max/mdev = 0.102/0.139/0.166/0.025 ms
```


If there is no network connectivity, ensure that the management cable is connected to the LAN1 port.

Rebooting a New Application Image

Use **Option r** to exit the helper utility and power cycle (reboot) into the newly installed application image.

Shutting Down the Prime vNAM

Use **Option h** to exit the helper utility and shut down the Prime vNAM.

```
-----  
Selection [12345678fnsnrh]: h  
About to exit and shutdown NAM.  
Are you sure? [y/N] y  
Stopping internet superserver: inetd.  
Stopping OpenBSD Secure Shell server: sshd.  
Stopping internet superserver: xinetd.  
Stopping internet superserver: xinetd-ipv4.  
: done.  
Shutting down NAM (NAM2304-RJ45-K9), part 1:  
Stopping klogd . . .  
Stopping syslogd . . .  
Sending all processes the TERM signal... done.  
Sending all processes the KILL signal... done.  
Unmounting remote filesystems... done.  
Deactivating swap...done.  
Unmounting local filesystems...done.  
Starting halt command: halt  
Power down.  
-----
```




Troubleshooting

The Cisco Prime vNAM software undergoes extensive testing before software release. If you encounter problems, use the information in this section to help isolate problems or to eliminate the virtual appliance as the source of the problem.

This topic does not cover every possible trouble event that might occur on an virtual appliance, but instead focuses on those events that are frequently seen by the customer.

Frequently Asked Questions

- Q.** The monitored traffic rate does not match the expected value. How do I troubleshoot?
- A.** If the monitored traffic rate does not match the expected value, check the license type using the `show license` command.

- Q.** I'm unable to connect to the Prime vNAM webserver. What do I do?
- A.** Run `ping`. Run `show ip`. Ensure that the webserver is enabled.

- Q.** I do not see any data traffic reaching the Prime vNAM. What do I do?
- A.** Ensure that the bridge connected to the data port is configured in promiscuous mode.

- Q.** Telnet do not work. What do I do?
- A.** Run `show ip` command to see whether Telnet is enabled. If not, enable Telnet.

- Q.** How do I recover the installation if the Prime vNAM image gets corrupted?
- A.** Try rebooting the Prime vNAM. If it is persistently not responding, you might need to deploy a new Prime vNAM.

- Q.** It appears like the data is corrupted. What do I need to do?

Use the `clear monitoring data` command to clear the monitoring data.

Additional References

All product documentation is available on Cisco.com under **Cloud and System Management > Network Analysis Module (NAM) Products > Cisco Prime Network Analysis Module Software**.

For an detailed list of all documentation, see the Cisco Prime Network Analysis Module [Documentation Overview](#).



Additional Tasks

This section covers Prime vNAM specific tasks that you can perform after installation is complete.



Note

Some of these tasks are required while others are optional.

- [Changing the Root Password, page 1-1](#)
- [Resetting the Prime vNAM Root Password to the Default Value, page 1-2](#)
- [Rebooting and Shutting Down the Prime vNAM, page 1-2](#)
- [Installing and Configuring Local and External Storage, page 1-2](#)

For more detailed information about the product and tasks, see the Cisco Prime Network Analysis Module *User Guide*.

Changing the Root Password

This section describes how to change the root user password after you have done so during the initial login session.

To clear the password and return it to default factory setup state, use: **clear system-passwords**.

If you have forgotten the root password and cannot get into the system, boot the system to the helper utility using **reboot -helper** and reset using the menu selections.'

To change the root password:

Step 1 Open a console session or serial session with the NAM appliance.

Step 2 When prompted for a username, enter **root**.

Step 3 When prompted, enter the password for user root you created at initial logon.

After you log in as the root user, you have read and write access to the root level of the NAM appliance, and you can enter and perform CLI commands.

```
root@hostname#
```

Step 4 Enter the following command to change the root user password.

```
password root
```

```
New password:
```

```
Confirm password:
```

- Step 5** Enter the new password for user root and confirm it.
- We recommend that you make a record of the password and store this information in a secure location. You should change this password regularly in accordance with your site's password security policies.
- Step 6** Type **exit** to end the session and log out.
-

Resetting the Prime vNAM Root Password to the Default Value

For information about how to reset the NAM root password to the default value, see the [Cisco Prime Network Analysis Module Software User Guide](#).

Rebooting and Shutting Down the Prime vNAM

To perform a shutdown or reboot you can perform one of the following actions from the Prime vNAM CLI.

- From the Prime vNAM CLI, enter **shutdown** to power off the Prime vNAM.
- From the Prime vNAM CLI, enter **reboot** to reboot the Prime vNAM.
- From the Prime vNAM CLI, enter **reboot -helper** to enter the Helper Utility menu for installation or recovery.



Note

Reboot and shutdown, as well as power up, can also be performed using the hypervisor interface.

Installing and Configuring Local and External Storage

Depending on your virtualization system, you may need to configure local storage or install and configure external storage for your capture data.

You can use local or external storage as a repository for long term data for performance comparisons.



Note

Ensure that when you install Prime vNAM that the designated disk is readable and writeable by everyone so that all users can store capture data successfully.

Here is a brief summary describing which Prime vNAMs require you to configure external storage:

- ESXi vNAM—No configuration necessary. Local hard disk preallocates external storage.
- KVM vNAM—Configuration required.

This section describes how to manually prepare your external iSCSI storage information to work with KVM vNAM. It contains the following sections:

- [Configuring the iSCSI Array](#)
- [Locating the Prime vNAM IQN](#)
- [Connecting the Storage Array](#)

Configuring the iSCSI Array

You may decide that in addition to or instead of local storage that you want to set up an external storage drive using iSCSI. This section contains the required settings for Prime vNAM.

Use your vendor's user documentation to ensure you have properly configured the iSCSI array. The Prime vNAM is independent of most array settings, but some are important for accessibility and performance.

-
- Step 1** To configure the Logical Unit Numbers (LUNs) on the array, there is often a Segment Size setting. Larger segment sizes can improve write speeds. Configure the Segment Size setting to use the largest possible segment size (up to 512 KB).
Multiple LUNs can be configured on a single array.
 - Step 2** Map the LUNs to iSCSI Qualified Names (IQNs) on the array. Each IQN represents a different list of LUNs for hosts (such as the Prime vNAM) to access.
Prime vNAM supports up to 32 LUNs between all protocols and multiple LUNs mapped to one IQN.
 - Step 3** Prime vNAM also has an IQN, which represents the host side of an iSCSI session. Ensure you map each Prime vNAM IQN to the LUNs for host read-write access. Most storage arrays require this for security reasons, to ensure that only certain hosts can access the LUNs. Each Prime vNAM has a unique IQN, so perform this step for each Prime vNAM that requires access and for each target LUN that is to be accessed. For more details about which CLI command to use, see [Locating the Prime vNAM IQN](#), page 1-3.
 - Step 4** Set the IP path to the Prime vNAM management port. For details, see [Connecting the Storage Array](#), page 1-3.
-

Locating the Prime vNAM IQN

To find the Prime vNAM IQN, use the **remote-storage iscsi local-iqn** CLI command:

```
root@nam.domain# remote-storage iscsi local-iqn
```

```
Local iSCSI Qualified Name: iqn.1987-05.com.cisco:WS-SVC-NAM3-6G-K9.00:19:55:07:15:9A
```

Connecting the Storage Array

After you configure the iSCSI storage arrays, be sure that it has an IP path to the Prime vNAM management port. The array can be connected while the Prime vNAM is running.

Some arrays come with multiple storage controller modules. As a security feature, module ownership must often be mapped to each LUN.

The Prime vNAM logs into the storage to start an iSCSI session using the IP address and IQN(s) of the storage array. To connect the storage array using the user interface, follow these steps:

-
- Step 1** Log into the Prime vNAM web interface. To access the Data Storage page, choose **Capture > Packet Capture/Decode > Data Storage**.
 - Step 2** Click the **iSCSI Login** button and enter the target IP and IQN.
The storage table refreshes with the newly discovered LUNs.

If the LUNs do not appear:

- a. Check **remote-storage iscsi list** to verify the iSCSI session was properly started.

The follow example shows how to verify the iSCSI session.

```
root@nam.domain# remote-storage iscsi list
Storage ID: 16
___ Label:
___ Status: Ready
   Protocol: ISCSI
   Target IP: 172.20.122.81
   Target IQN: iqn.2011-09:celeros.target11
___ Type: LUN
___ Model: IET VIRTUAL-DISK
___ LUN: 4
   Capacity: 24.98GB
   Available: 24.98GB
Active iSCSI Sessions:
tcp: [8] 172.20.122.81:3260,1 iqn.2011-09:celeros.target11
```

The LUN number (in the above example, LUN 4) can help you identify one LUN from others of the same IQN. This number is unique to each IQN, meaning two LUNs from different IQNs can have the same number.

- b. If the iSCSI session was properly started, check the storage array configuration to verify that:
 - The LUNs are mapped to the target IQN, and
 - The Prime vNAM IQN has been given Read/Write access to the LUNs.
- c. If you make any configuration changes, logout of the iSCSI session and login again. To logout, use the CLI **remote-storage iscsi logout**. If the LUNs appear on the user interface, you can select one of them and click **iSCSI Logout**. All LUNs mapped to that target IQN will be disconnected.

You can now use the iSCSI external storage from within Prime vNAM. For more information, see the [Cisco Prime Network Analysis Module Software User Guide](#).

Migrating Prime vNAM to a new Host

To migrate the Prime vNAM to a new host:

-
- Step 1** Ensure that the new host meets the system requirements. See the [Host Configuration Requirements](#) section for details.
 - Step 2** Create a backup of your data. See [Backing Up Your Configuration](#).
 - Step 3** Shut down the vNAM.
 - Step 4** Perform migration.
-



B

backing up appliance configuration [6-1](#)

C

clear system -passwords [1-1](#)

CLI commands

exsession [5-2](#)

ip domain [5-3](#)

ip gateway [5-1](#)

ip host [5-3](#)

ip interface [5-1](#)

ip nameserver [5-3](#)

ping [5-4](#)

show ip [5-4](#)

Configuration

restoring [6-3](#)

configuration

backing up [6-1](#)

checking [5-4](#)

Configuring

ip address [5-1](#)

NAM interface for management traffic [5-1](#)

connectivity

establishing [5-1](#)

E

eoot user password

changing [1-1](#)

F

forgotten password [1-1](#)

P

password, recovering [1-1](#)

S

Software

upgrading [6-2](#)

Software download URL [6-2](#)

U

upgrading software [6-2](#)

V

virtual appliance

managing [6-2](#)

upgrading [6-2](#)

W

web server

enabling [5-2](#)

