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

June 2015

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:

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

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.	• 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	• 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 2-4.

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

For Prime vNAM you must have the following;

- Any X86_64 hardware with 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 Requirement Per Prime vNAM[1]

NAM Version	Supported Hypervisors	RAM	CPU	Network	Hard Disk
6.0, 6.1	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))
6.2	VMware vSphere 5.1 (ESXi 5.1 and later)			Two virtual NICs (VMXNET3)	100 GB for a vNAM[2] (PVSCSI storage driver)
	Red Hat Enterprise Linux 6.1 Openstack Juno			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 Requirement

The following table lists the client requirement:

Hardware	IBM-compatible or Macintosh computer with 2-GHz or faster processor
RAM	1 GB

Operating System	• Windows 7 • Windows Vista with Service Pack 1 • Windows XP Professional with Service Pack 2 • Red Hat Enterprise Linux 6.1 (base server)
Browser	• 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 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.

Host Configuration Requirement for UCS E vNAM

For Cisco UCS E vNAM, you must have the following;

- UCS E platform that has adequate resources to deploy a virtual environment for Cisco UCS E vNAM. See Table 2-2 for hardware requirements.
- VMware with ESXi or RHEL with KVM installed on the hardware of choice. See Table 2-2 for supported hypervisor details.

The hypervisor must have access to the Cisco UCS E vNAM software image on an FTP or HTTP server for deployment. The Cisco UCS E vNAM supports the platforms/hypervisors in Table 2-2.

Table 2-2 Requirements Per Cisco UCS E vNAM[1]

Supported Hypervisors	RAM	CPU	Network	Hard Disk
VMware vSphere 5.1 (ESXi 5.1 and later)	4GB Per vNAM	Two CPU Cores	Two/Three 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/Three 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.

vNAM's disk performance depends on the actual configuration of the hard disks in the server that runs the hypervisor. In order to improve the disk performance, you should configure a suitable RAID, if you have the necessary RAID controller and disks that support the RAID controller. This applies to all the vNAMs on all the hypervisors.

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 Cisco UCS E vNAM license, see section SMART Licensing in *Cisco Prime Network Analysis Module User Guide*.

For details about installing a license, see Installing the License, page 2-4. For CLI licensing commands, see the *Cisco Prime Network Analysis Module Command Reference Guide*.

Installing the License

See section SMART Licensing in *Cisco Prime Network Analysis Module User Guide.*

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 6-1
5. (Optional) Request permanent license to replace 90-day evaluation license.	Installing the License, page 2-4

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

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. The vSphere client is a windows application. But the same functionality is also provided by the vSphere web client which runs on any operating system with a standard web browser.

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 Deployment Configuration page appears.

Step 8 Select one of the following configuration:

- Small NAM Deployment
- Large NAM Deployment
- NAM on UCS E

Step 9 Click **Next.**

The Properties page appears.

Step 10 Enter the CLI root credentials, hostname, domain, IPv4 address and IPv4 network mask details.

Step 11 Click **Next**.

The Ready to Complete window appears.

Step 12 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 13 Click **Close** to dismiss the dialog box.

Step 14 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 15 Continue with your post-installation tasks using a console to the Cisco Prime vNAM to perform the steps in the Establishing Network Connectivity, page 6-1.

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 file and <target locator> is an appropriate URL to the target ESXi host or vCenter server. For example:

ovftool nam-app-x86_64.x-y-z.ova vi://esxi-host.cisco.com/

For further details on ovftool syntax and usage, refer to the *VMware OVF Tool User's Guide*. This document, and additional OVF resources, can be found at https://www.vmware.com/support/developer/ovf/.

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 2-4

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

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

Installation Method	See...
Command Line	Deploying Prime vNAM on KVM using CLI, page 4-3
Virtual Machine Manager	Deploying Prime vNAM on KVM using Virtual Machine Manager, page 4-3
Openstack running on RHEL or Ubuntu VM	Deploying Prime vNAM on KVM using Openstack, page 4-4
Command Line on RHEL Openstack host	Deploying Prime vNAM on RHEL Openstack KVM using CLI, page 4-5

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

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 writable 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.

Deploying Prime vNAM on KVM using Openstack

To deploy a vNAM on KVM using Openstack:

Step 1 Install Openstack on RHEL or Ubuntu VM and make sure that the Openstack dashboard is up and running. It should be reachable using an IP address in the URL.

Step 2 Download the qcow2 image of the vNAM on the RHEL/Ubuntu VM from the below location:

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

Step 3 Add the downloaded image to the glance storage.

For details on the glance image CLI, see http://docs.openstack.org/user-guide/content/cli_manage_images.html.

Step 4 Modify the properties of the image by adding the hw-diskbus property as IDE.

For details, see http://docs.openstack.org/user-guide/content/cli_manage_images.html.

Step 5 Create a vNAM flavor (2 VCPUs, 4GB RAM and 100GB hard disk) by running the following command on the RHEL/Ubuntu VM:

```
$ nova flavor-create FLAVOR_NAME FLAVOR_ID RAM_IN_MB ROOT_DISK_IN_GB NUMBER_OF_VCPUS
```

Step 6 Open the openstack dashboard from RHEL/Ubuntu VM and launch the vNAM instance from the image added to glance storage and choose the flavor you created.

Step 7 Add two NICs in the Networking section by dragging the required two networks.

Step 8 Choose a config drive and also upload the configuration file, if you wish to configure the vNAM. The configuration file is in the XML file format.

Step 9 Click the **Launch** button to launch the vNAM instance. You can view the logs in the console as the vNAM is booting up.

Step 10 Associate a floating IP address to the vNAM.

Deploying Prime vNAM on RHEL Openstack KVM using CLI

To boot the vNAM instance on RHEL Openstack KVM using CLI:

Step 1 Run the following command on the RHEL Openstack KVM:

```
$ nova boot --image vNAM --flavor <#> --nic port-id=<PORT ID> --nic port-id=<Port ID>
vNAM_NAME --config-      drive=true --file <FileName>=<Config_File>
```

Where:

- *image* is the vNAM's image name in your glance storage.
- *flavor* is the vNAM's flavor ID.

  Run `$ nova flavor-list` command on the host to check the flavor id of the vNAM.
- *port-id* is either the management or data port ids for vNAM.

  You can create two ports (Management and Data) from the Openstack GUI or using CLI:

  ```
  $ neutron port-create --fixed-ip subnet_id=<SUBNET_ID> ip_address=<IP_ADDRESS>
  <NET_ID>
  ```

  To view the list of subnet IDs in order to choose the right subnet, run the following command:

  ```
  $ neutron subnet-list
  ```

  To view the list of network IDs in order to choose the right network, run the following command:

  ```
  $neutron net-list
  ```

  To view the port IDs, run the following command:

  ```
  $ neutron port-list
  ```
- *config-drive* is a virtual drive that will contain the configuration file.

  Set this option as TRUE to provide the vNAM with virtual drive.
- *file* is the vNAM configuration file in XML format.

When you run the above command with all the parameters in place, you will see the instance booting up on the Openstack dashboard.

Step 2 Once the instance comes up, vNAM is configured with the properties specified in the configuration file.

Deploying Prime vNAM in Nexus 1000V Environment

Table 4-2 summarizes how to quickly get up and running on Nexus 1000V environment:

Table 4-2 Installation Overview in Nexus 1000V Environment

Task	See...
1. Review the requirements and preparations for Prime vNAM	Installation Requirements, page 2-1
2. Setting up Virtual Supervisor module (VSM) and Virtual Ethernet Module (VEM)	Setting up Virtual Supervisor Module (VSM) and Virtual Ethernet Module (VEM), page 4-6
3. Setting up a vNAM on the RHEL Host Containing VEM	Setting up a vNAM on the RHEL Host Containing VEM, page 4-6

Setting up Virtual Supervisor Module (VSM) and Virtual Ethernet Module (VEM)

To setup the VSM and VEM follow the below steps and run the below commands as root user:

Step 1 Deploy the VSM OVA on an ESXi host. Assign an IP address and set up the routing.

Step 2 Install the VEM RPM on RHEL 7 host by running the below commands:

- `yum install libn`
- `yum install openvswitch`
- `rpm -ivh  nexus_1000v_vem-7.0-5.2.1.SK3.2.0.196.S0-0.x86_64.rpm`

Step 3 Restart the host by running the below command:

```
systemctl restart nexus1000v
```

Step 4 Edit /etc/n1kv/n1kv.conf to have the correct details of VSM (IP/DomainID) and Management Interface.

Step 5 Restart the service.

Step 6 Execute the command `show mod` on the VSM command prompt. You will see the details of the VEM you deployed on the RHEL host.

Setting up a vNAM on the RHEL Host Containing VEM

To setup a vNAM on the RHEL host containing VEM:

Step 1 Start deploying a vNAM on RHEL host using ISO image.

Step 2 Create interfaces of type bridge (vNAM_mgmt and vNAM_dataport), and then connect them to the OVS bridge.

Step 3 Run the command `ifconfig` on the RHEL host. You will see the vNAM's interfaces in the output.

Step 4 Run the below commands on the RHEL host to add the vNAM ports to the VEM:

```
ovs-vsctl add-port n1kvdvs vNam_mgmt
```

```
ovs-vsctl add-port n1kvdvs
```

Step 5 Log into the VSM and run the command `attach vem <vem#>`.

Step 6 Create a port profile for the vNAM_mgmt using the Nexus commands so that you have the management in a private vLAN.

Step 7 Create a port profile for the vNAM_dataport (without any vlan configs).

Step 8 Run the following command on the RHEL host to attach the ports of the vNAM to the port-profiles:

```
vemcmd attach port vNam_mgmt profile <port-profile name>    vemcmd attach port
vNam_dataport profile <port-profile name>
```

You can now connect data traffic to an available physical interface on the server.

Step 9 Add the port to the OVS bridge and set up a local span using NX-OS commands to span traffic to the vNAM_dataport.

To make the vNAM accessible from outside you need to deploy a virtual or connect a physical router.

Installing Cisco UCS E Virtual Network Analysis Module

This chapter provides details about installing Cisco UCS E Virtual Network Analysis Module (vNAM) software. The Cisco UCS E vNAM is only supported with Cisco NAM 6.2 and later versions.

Prerequisites

Table 5-1 contains information about the prerequisites that should be met before installing Cisco UCS E Virtual Network Analysis Module (vNAM) software.

Table 5-1 Prerequisites for Cisco UCS E vNAM Installation

Task	See...
1. Update the UCS E CIMC firmware to version 2.3.3 or later.	Updating UCS E CIMC Firmware Version, page 5-1
2. Verify the router, E-Series server, and Cisco IOS software version compatibility.	Verifying the Router, E-Series Server, and Cisco IOS Software Version Compatibility, page 5-2
3. Install the UCS E on ISR with CIMC IP configured and hypervisor installed.	Installing UCS E on ISR with CIMC IP Configured and Hypervisor Installed, page 5-2
4. Enable NAM feature on UCS E CIMC.	Enabling NAM Feature on Cisco UCS E CIMC, page 5-2
5. Enable CEF traffic on ISR.	Enabling CEF Traffic on ISR, page 5-3

Updating UCS E CIMC Firmware Version

You must update the CIMC firmware release version to 2.3.3 or later. You can download the latest CIMC firmware from:

https://software.cisco.com/download/release.html?mdfid=286231776&flowid=50082&softwareid=284480160&release=2.3.3&relind=AVAILABLE&rellifecycle=&reltype=latest

Verifying the Router, E-Series Server, and Cisco IOS Software Version Compatibility

Table 5-2 provides the router, E-Series Server, and Cisco IOS software version compatibility information.

Table 5-2 Router, E-Series Server, and Cisco IOS Version Compatibility

Router	Cisco IOS Software Version for Single-Wide E-Series Servers	Cisco IOS Software Version for Double-Wide E-Series Servers
2911	15.2(4)M and later versions	—
2921	15.2(4)M and later versions	15.2(4)M and later versions **Note**: Supports 4-core only.
2951	15.2(4)M and later versions	15.2(4)M and later versions **Note:** Supports 4-core only.
3925	15.2(4)M and later versions	15.2(4)M and later versions
3925e	15.2(4)M and later versions	15.2(4)M and later versions
3945	15.2(4)M and later versions	15.2(4)M and later versions
3945e	15.2(4)M and later versions	15.2(4)M and later versions

Installing UCS E on ISR with CIMC IP Configured and Hypervisor Installed

See *Getting Started Guide for Cisco UCS E-Series Servers and the Cisco UCS E-Series Network Compute Engine, Release 2.x* to understand how to configure CIMC IP on UCS E.

Enabling NAM Feature on Cisco UCS E CIMC

To enable the NAM feature on Cisco UCS E CIMC CLI:

Step 1 Connect Cisco UCS E CIMC with NAM installed through SSH.

Step 2 Enter the following commands to enable the NAM monitoring feature:

```
E160DP-FOC16270UC0# scope cimc
E160DP-FOC16270UC0 /cimc # scope network
E160DP-FOC16270UC0 /cimc/network # scope nam
E160DP-FOC16270UC0 /cimc/network/nam # set enabled yes
E160DP-FOC16270UC0 /cimc/network/nam *# commit
```

Step 3 Enter the command to verify the NAM feature status.

```
E160DP-FOC16270UC0 /cimc/network/nam # show detail
Network Analysis Module:
Enabled: yes
E160DP-FOC16270UC0 /cimc/network/nam #
```

Enabling CEF Traffic on ISR

Cisco UCS E vNAM allows you to monitor the CEF traffic that passes through the ISR.

To enable CEF monitoring on a ISR interface, enter the below commands in ISR terminal:

```
enable
configure terminal
ip cef
interface type slot/port
or
interface type slot/wic-slot/port
analysis-module monitoring
```

See section "Forwarding CEF Traffic" and "Understanding How the Prime NAM uses CEF" in *Cisco Prime Network Analysis Module User Guide for details, Release 6.2*.

Installation Requirements

See section Host Configuration Requirement for UCS E vNAM, page 2-3 and Client Requirements, page 5-3 for details.

Configuring Cisco UCS E vNAM to Receive Data Traffic

In order for the Cisco UCS E 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.

As Cisco UCS E vNAM supports three different deployment models on hypervisor, each one has different network configuration and has its own advantage/disadvantage. For more details see section Deploying Cisco UCS E NAM on Hypervisor, page 5-9.

Installing Cisco UCS E vNAM on VMware vSphere ESXi

This section provides instructions on how to install the Cisco UCS E vNAM on VMware vSphere ESXi.

Table 5-3 summarizes how to quickly get up and running on ESXi:

Table 5-3 Installation Overview for ESXi

Task	See...
1. Review the prerequisites for Cisco UCS E vNAM.	Prerequisites, page 5-1
2. Review the requirements and preparations for Cisco Prime vNAM.	Installation Requirements, page 5-3

Table 5-3 Installation Overview for ESXi

Task	See...
3. Download the Cisco UCS E vNAM OVA file from Cisco.com.	Downloading Cisco UCS E vNAM Virtual Appliance OVA File, page 5-4
4. Install Cisco UCS E vNAM software.	Deploying Cisco UCS E vNAM on ESXi Server Using vSphere Client, page 5-4
5. (Optional) Request permanent license to replace 90-day evaluation license.	Configuring Cisco UCS E vNAM to Receive Data Traffic, page 5-3

Downloading Cisco UCS E vNAM Virtual Appliance OVA File

The Cisco UCS E 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 Cisco UCS E vNAM in an ESX virtualization environment. The OVA defines the network interface requirements for Cisco UCS E vNAM.

Cisco UCS E vNAM on ESXi platform is distributed as an OVA file, named nam-yyy-x.x.x.ova.

Note You can deploy the Cisco UCS E vNAM software file directly from any of the supported hypervisors (for example, the vSphere Client); and do not need to extract the archive before performing the deployment.

Step 1 Access the Cisco UCS E 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 Cisco UCS E vNAM on ESXi Server Using vSphere Client

You can use a vSphere client to install an instance of Cisco UCS E vNAM. We recommend you to use the two Dataports two vSwitches deployment model. For more details see section 2 Dataports, 2 vSwitches Model, page 5-12 for more details.

To set up the Cisco UCS E vNAM on VMware ESXi using the OVA file:

Step 1 Download a vSphere client and connect it to the VMware ESXi server. You must 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. For details on how to download the OVA file, see Downloading Cisco UCS E vNAM Virtual Appliance OVA File, page 5-4.

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 (Cisco UCS E 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 Deployment Configuration page appears.

Step 8 Choose the UCSe model, verify the hardware profile detail, and click **Next**.

Step 9 Choose the Storage location for the virtual machine files and click **Next** to choose the Disk Format type.

Step 10 Click **Next**. The Network Mapping page appear.

- Set the MgmtNetwork's destination network to the management network in your environment.
- Set the DataNetwork1 to the management network to monitor the management traffic as well as the CEF traffic that pass through your ISR.
- Set the DataNetwork2 to the front panel port for monitoring the external traffic.

Step 11 Click **Next**, if you are using the vCenter to configure the virtual machine. The Properties page appears. The vNAM's network credentials, root password, snmp community string can be set from the vsphere client, so you do not have to configure it when the vNAM installation is completed.

Step 12 Click **Next**. The Ready to Complete window appears.

Step 13 Click **Finish** to Review the setting details of your deployment.

Deploying Cisco UCS E vNAM on 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 Cisco UCS E 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 UCS E vNAM on Red Hat Enterprise Linux KVM

This section provides instructions on how to install Cisco UCS E vNAM on Red Hat Enterprise Linux (RHEL) KVM using an ISO file.

Table 5-4 summarizes how to quickly get up and running on RHEL KV.

Table 5-4 Installation Overview for KVM

Task	See...
1. Review the prerequisites for Cisco UCS E vNAM.	Prerequisites, page 5-1
2. Review the requirements and preparations for Cisco Prime vNAM	Installation Requirements, page 5-3
3. Download the Cisco UCS E vNAM ISO file from Cisco.com	Downloading Cisco UCS E vNAM Virtual Appliance ISO File, page 5-7
4. Configure Virtual Network Bridges.	Configuring Virtual Network Bridges, page 5-6
5. Install Cisco UCS E vNAM software on the virtual machine	Deploying Cisco UCS E vNAM on KVM using Virtual Machine Manager, page 5-7
6. (Optional) Request permanent license to replace 90-day evaluation license.	Configuring Cisco UCS E vNAM to Receive Data Traffic, page 5-3

Configuring Virtual Network Bridges

In order to make the Cisco UCS E 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.

Note You must perform this task before Cisco UCS E vNAM installation.

This section provides details on how to configure your virtual network bridges for the two or three required Cisco UCS E 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 Cisco UCS E vNAM management port.
- Data port—Bridge to include the physical port receiving the SPAN traffic.

To configure the virtual network bridges to the Prime Cisco UCS E vNAM ports:

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, and you want to set a Cisco UCS E vNAM to monitor both management port and dataport's traffic:

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

Step 3 Step 3 : Enter the commands to let the bridges work all the time:

```
brctl setageing bridge0 0
brctl setageing bridge1 0
```

To download the Prime vNAM image onto your KVM host continue to Downloading Cisco UCS E vNAM Virtual Appliance ISO File, page 5-7.

Downloading Cisco UCS E 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 Cisco UCS E vNAM installation.

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

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

Step 2 Download the Cisco UCS E 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 is:

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

Deploying Cisco UCS E vNAM on KVM using CLI

You can deploy Cisco UCS E vNAM using command line interface. See KVM documentation for details. See also the Configuring Cisco UCS E vNAM to Receive Data Traffic, page 5-3.

To deploy the Cisco UCS E vNAM and start a console connection, use something similar to the following command.

Note 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.

Deploying Cisco UCS E vNAM on KVM using Virtual Machine Manager

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

To create a new Cisco UCS E 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 Cisco UCS E 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. 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**.

Step 12 Before you install, make sure the following are configured correctly.

Step 13 Select **Disk 1** in the installation menu panel, change the advanced option Disk Bus to *IDE*, then click **Apply**.

Step 14 Select **Boot Options** in the installation menu panel. Check the select hard disk, then click **Apply**.

Step 15 Select **NIC** in the installation menu panel. The NIC that displays is that of the management port for the vNAM. In the Device Model drop-down, choose **virtio**.

Step 16 Click **Add Hardware**.

Step 17 In the Add new virtual hardware window, select **Network**. We recommend you to select the 2 Dataports 2 vSwitches deployment model (see 2 Dataports, 2 vSwitches Model, page 5-12 for more details), so you should add two network hardwares. Select **NIC** in the installation menu panel. Select the NIC that displays the bridge including the management port for newly added Network Hardware 1, to monitor the management traffic as well as the CEF traffic pass through the ISR, Select the NIC that displays the bridge including the front panel port for newly added Hardware 2, to monitor the external traffic.

Step 18 In the Device Model drop-down, choose **virtio**.

Step 19 From the Host device details drop-down, select the interface on which your Cisco UCS E vNAM will connect to the network. This will be the bridge you created for data.

Step 20 In the Device Model drop-down, choose **virtio**.

Step 21 Click **Finish**. Do a quick review of the NIC and other details.

Step 22 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.

Deploying Cisco UCS E NAM on Hypervisor

As the network on hypervisor is configurable, there are many deployment models and each has its own advantage and disadvantage. This section explains VMware ESXi host based configuration instance. For the KVM hypervisor, you must follow the same rule to map the related port with created bridges. 2 Dataports, 2 vSwitches model is recommended.

Note When you install vNAM with OVA image and select "UCS E model", it will automatically create two dataports on NAM and you need to use 2 Dataports, 2 vSwitches Model.

This section describes the following UCS E NAM deployment models on hypervisor:

- 1 Dataport, 1 vSwitch Model
- 1 Dataport, 2 vSwitches Model
- 2 Dataports, 2 vSwitches Model

1 Dataport, 1 vSwitch Model

- vSwitch connects to Cisco UCS E port0 and front panel port.
- NAM management port connects to vSwitch.
- NAM dataport connects to vSwitch.
- Traffic from all physical ports, port0 and front panel port will flood into the switch.

Advantage

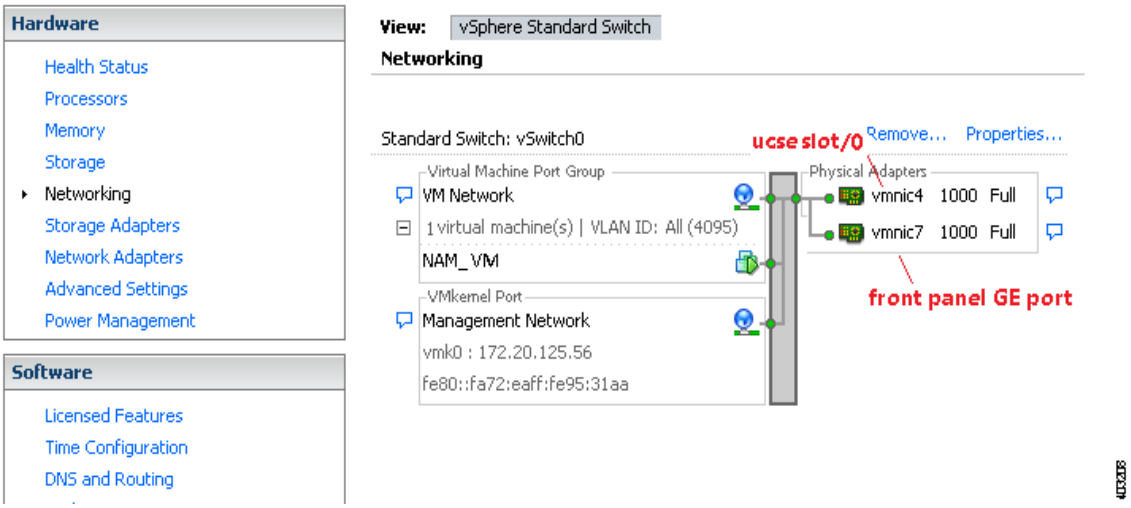
- Management traffic from ISR and traffic from front panel ports will be monitored on NAM data port.
- CEF dataport will be created when it receives CEF traffic from ISR.

Disadvantage

- System performance will be impacted as each port will be flooded with various traffic including management, CEF traffic and SPAN traffic.
- Miscellaneous packets from router interface will be received on dataport.
- Internal management traffic from router and traffic from front panel are integrated into one dataport in GUI.

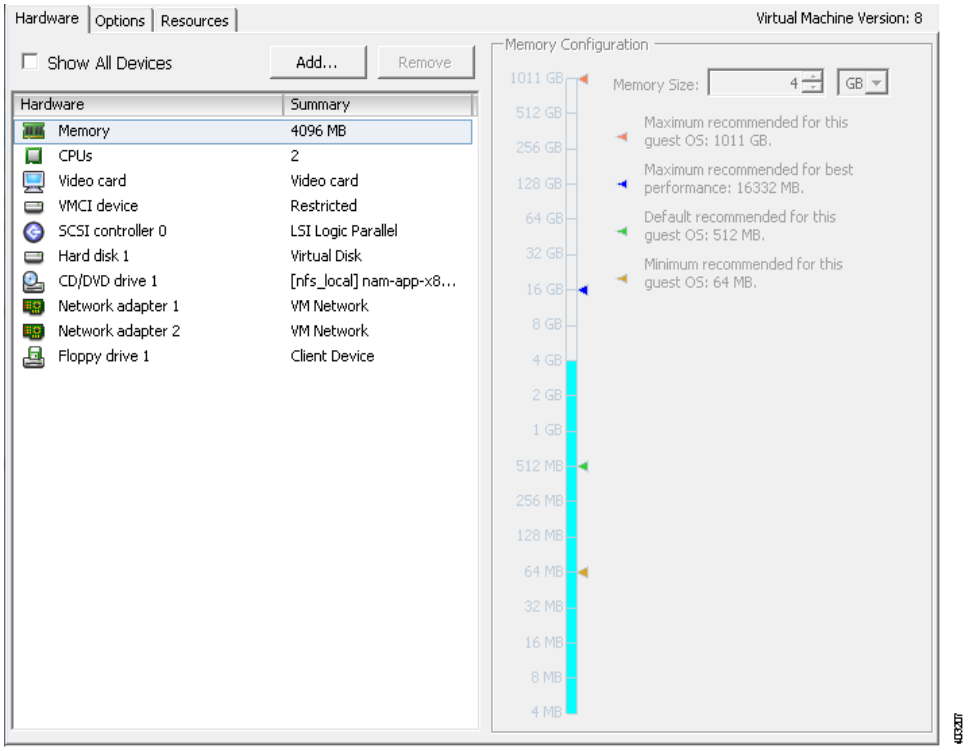
Configuring Network on Hypervisor using 1 Dataport, 1 vSwtich Model

Figure 5-1 Network Configuration on Hypervisor for 1 Data Port, 1 vSwitch Model



Configuring Virtual Machine using 1 Dataport, 1 vSwtich Model

Figure 5-2 Virtual Machine Configuration for One Dataport One vSwtich Model



1 Dataport, 2 vSwitches Model

- First vSwitch connects to Cisco UCS E port0.
- Second vSwitch connects to front panel port.
- NAM management port (Network Adapter 1 on virtual machine) connects to the first vSwitch.
- NAM dataport (Network Adapter 2 on virtual machine) connects to either first vSwitch (when monitoring internal management traffic) or the second vSwitch (when monitoring external traffic) depending on the traffic that the NAM needs to monitor.

Disadvantage

- It cannot monitor CEF traffic or external traffic at a same time.
- ISR miscellaneous packets are not filtered when dataport connects to the first vSwitch.

Configuring Virtual Machine using 1 Dataport, 2 vSwitches Model

Figure 5-3 Virtual Machine Configuration for 1 Dataport 2 vSwitches model_1

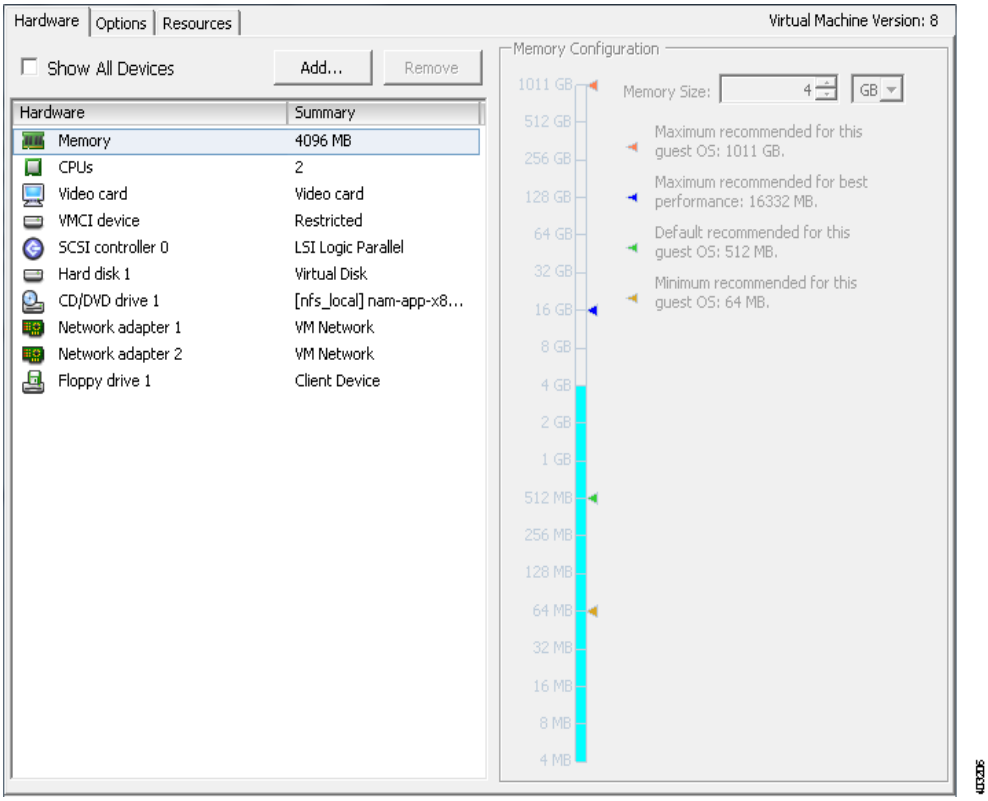
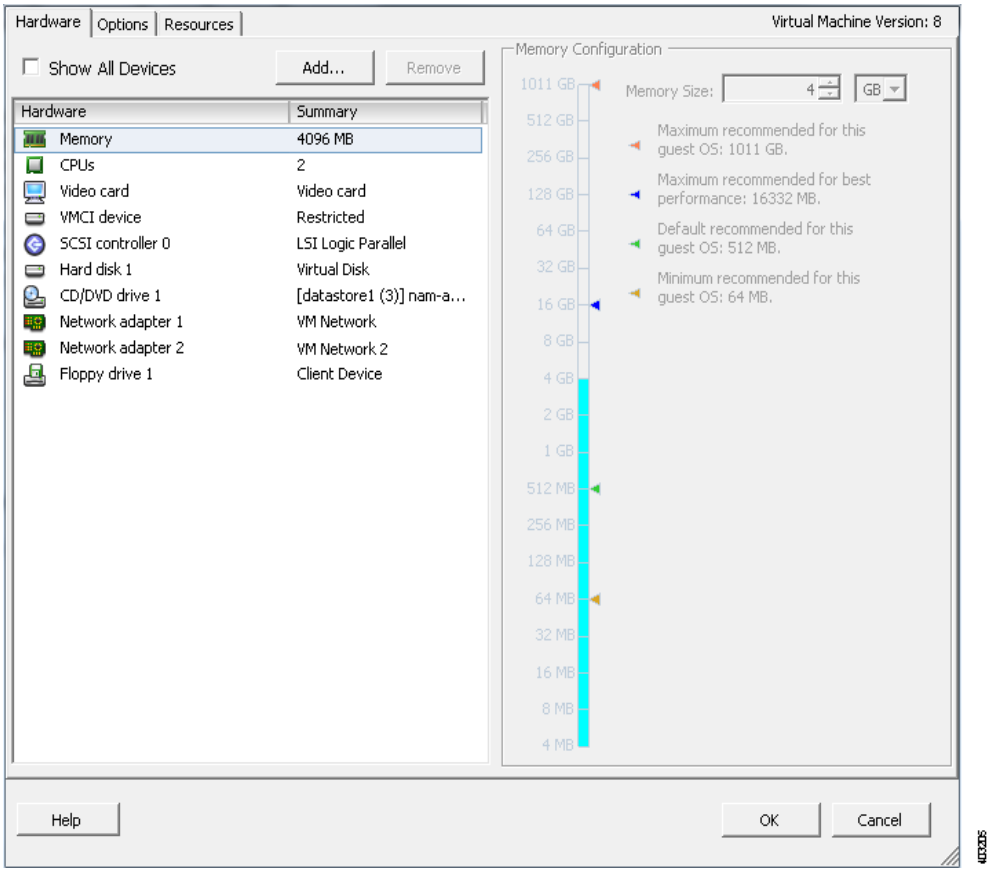


Figure 5-4 Virtual Machine Configuration for 1 Dataport 2 vSwitches Model_2



2 Dataports, 2 vSwitches Model

We recommend you to use this deployment model as it has the ability to support two dataports.

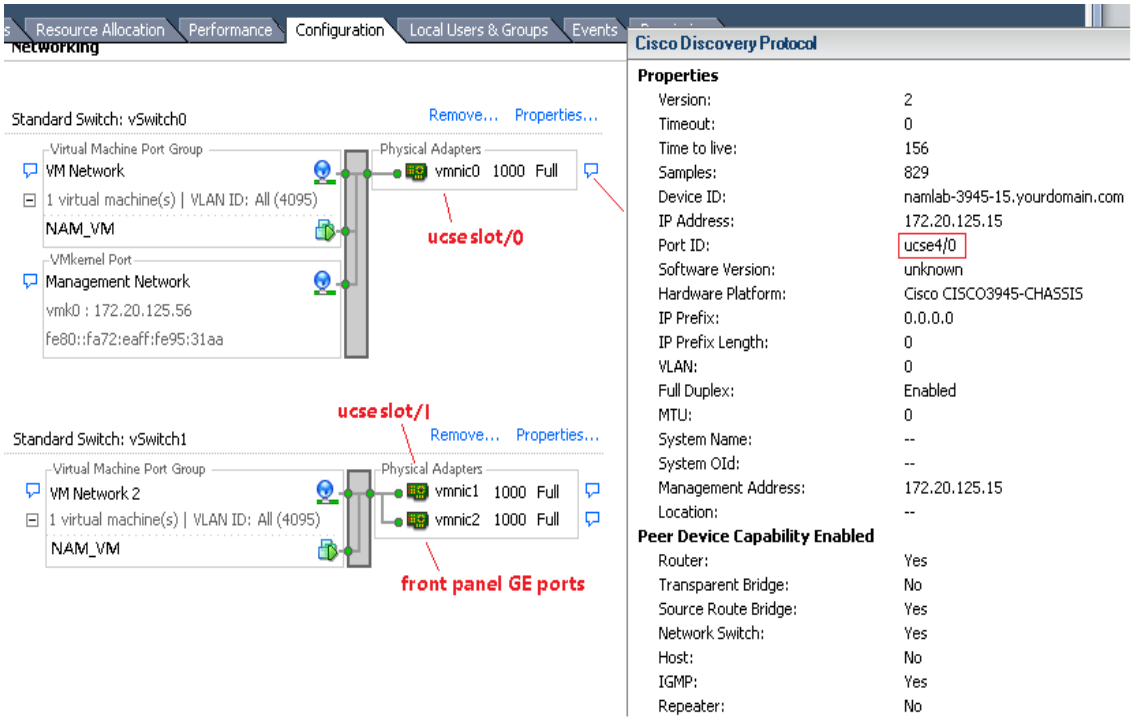
- First vSwitch connects to Cisco UCS E port0 for CEF traffic monitoring and ISR to UCS E management traffic.
- Second vSwitch connects to front panel port for external traffic monitoring.
- NAM management port (Network Adapter 1 on virtual machine) connects to the first vSwitch.
- NAM dataport 1 (Network Adapter 2 on virtual machine) connects to the first vSwitch for CEF traffic and internal management traffic monitoring.
- NAM dataport 2 (Network Adapter 3 on virtual machine) connects to the second vSwitch for external traffic monitoring.

Advantage

- ISR to Cisco UCS E management traffic is monitored on dataport 1.
- ISR to Cisco UCS E CEF traffic is monitored on CEF port.
- Internal and external traffic will not flood together.

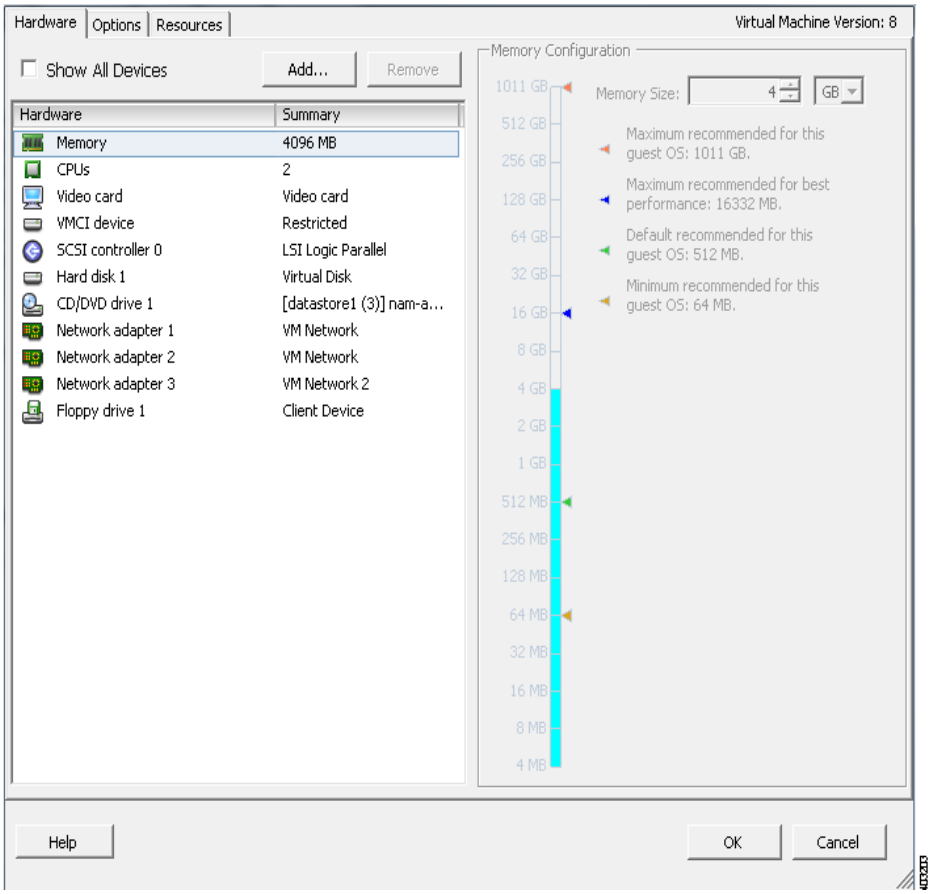
Configuring Network on Hypervisor using 2 Dataports, 2 vSwtiches Model

Figure 5-5 Network Configuration on Hypervisor for 2 Dataports 2 vSwitches Model



Configuring Virtual Machine using 2 Dataports, 2 vSwitches Model

Figure 5-6 Virtual Machine Configuration for 2 Dataports 2 vSwitches Model



- Network adapter 1: NAM management port
- Network adapter 2: NAM dataport 1
- Network adapter 3: NAM dataport 2

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:

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 6-2 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 and HTTPS secure server. 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

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 7-1.

Table 7-1 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 7-1), 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-namxxxx-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 [12345678fsnrh]: 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 Telent 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.

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

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 C-3.

Step 4 Set the IP path to the Prime vNAM management port. For details, see Connecting the Storage Array, page C-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.