SteelCentral™ NetShark
Quick Start Guide

Virtual Edition on SteelHead® EX, SteelFusion™ Edge

Version 10.9 for VMware ESXi 5.0, Patch 6 and ESXi 5.1

October 2015

This documentation is furnished "AS IS" and is subject to change without notice and should not be construed as a commitment by Riverbed Technology. This documentation may not be copied, modified or distributed without the express authorization of Riverbed Technology and may be used only in connection with Riverbed products and services. Use, duplication, reproduction, release, modification, disclosure or transfer of this documentation is restricted in accordance with the Federal Acquisition Regulations as applied to civilian agencies and the Defense Federal Acquisition Regulation Supplement as applied to military agencies. This documentation qualifies as "commercial computer software documentation" and any use by the government shall be governed solely by these terms. All other use is prohibited. Riverbed Technology assumes no responsibility or liability for any errors or inaccuracies that may appear in this documentation.

This manual is for informational purposes only. Addresses shown in screen captures were generated by simulation software and are for illustrative purposes only. They are not intended to represent any real traffic or any registered IP or MAC addresses.

riverbed

Riverbed Technology
680 Folsom St.
San Francisco, CA 94107

Phone: 415 247 8800
Fax: 415 247 8801
www.riverbed.com

712-00211-06

Contents

About this guide

The Riverbed® SteelCentral™ NetShark virtual edition is a virtualized implementation of the physical SteelCentral NetShark. It provides visibility into virtual environments by monitoring all traffic traversing the hypervisor.

If you are acquainted with the physical NetShark, you will find the NetShark virtual edition similar in operation and function.

The instructions in this guide cover version 10.5 (and later) of the NetShark software. Support for SteelFusion™ Edge requires version 10.8.5 (and later).

This guide details the steps to deploy NetShark on a VMware ESXi host running on Virtual Services Platform (VSP) on a SteelHead EX (formerly Steelhead EX appliance) or a SteelFusion Edge. A SteelHead EX is used in all of the examples. When you have completed the initial installation and configuration, refer to the *SteelCentral NetShark User's Guide* for further instructions on operational configuration and use.

1. Preparing to deploy the NetShark

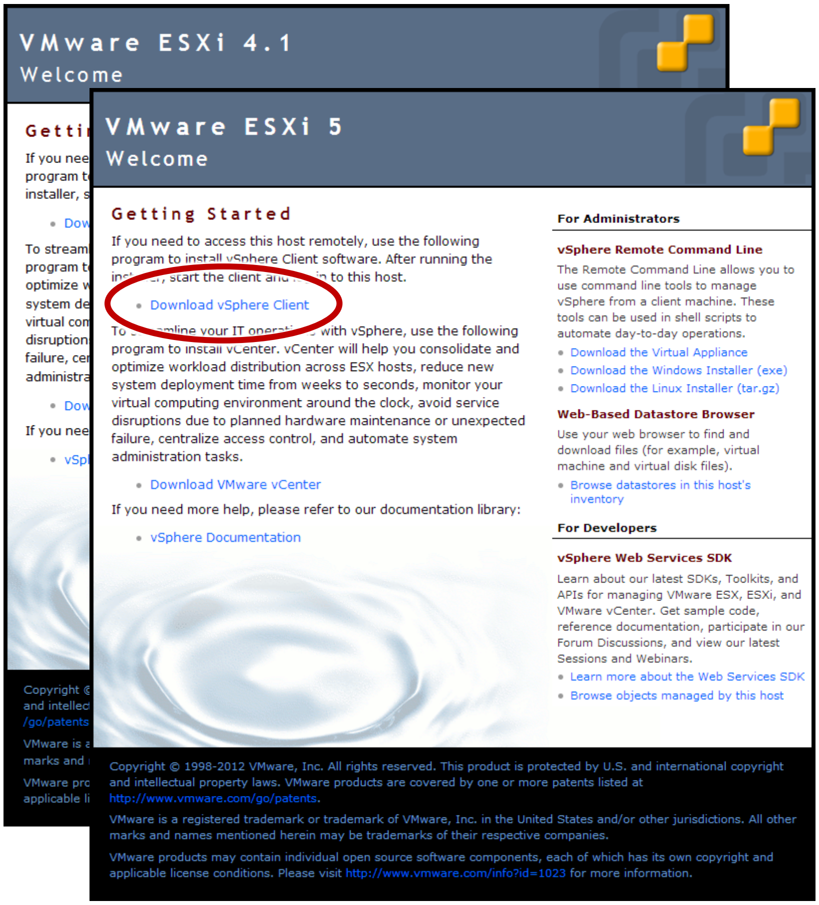
Gathering the software components

Make sure you have these software components available or installed, as appropriate.

- VMware ESXi 5.0, Patch 6, or ESXi 5.1 running on a VSP platform. The host needs to have the capacity for a virtual machine with 2 virtual CPUs, 2 GB of RAM, 30 GB of storage for the system, and up to 2 TB of packet storage.
- VMware vSphere Client, installed on your local system.
- NetShark OVA package, stored on your local system.
- Riverbed® SteelCentral Packet Analyzer (formerly Cascade® Pilot) software 10.5 (or later) software, installed on your local system.

If you do not have the vSphere Client on your local system, you can download it from the ESXi host, as follows:

1. Point your web browser at the ESXi host. You should see this welcome page:



VMware ESXi 4.1
Welcome

VMware ESXi 5
Welcome

Getting Started

If you need to access this host remotely, use the following program to install vSphere Client software. After running the installer, start the client and log in to this host.

- Download vSphere Client

To streamline your IT operations with vSphere, use the following program to install vCenter. vCenter will help you consolidate and optimize workload distribution across ESX hosts, reduce new system deployment time from weeks to seconds, monitor your virtual computing environment around the clock, avoid service disruptions due to planned hardware maintenance or unexpected failure, centralize access control, and automate system administration tasks.

- Download VMware vCenter

If you need more help, please refer to our documentation library:

- vSphere Documentation

For Administrators

vSphere Remote Command Line

The Remote Command Line allows you to use command line tools to manage vSphere from a client machine. These tools can be used in shell scripts to automate day-to-day operations.

- Download the Virtual Appliance
- Download the Windows Installer (exe)
- Download the Linux Installer (tar.gz)

Web-Based Datastore Browser

Use your web browser to find and download files (for example, virtual machine and virtual disk files).

- Browse datastores in this host's inventory

For Developers

vSphere Web Services SDK

Learn about our latest SDKs, Toolkits, and APIs for managing VMware ESX, ESXi, and VMware vCenter. Get sample code, reference documentation, participate in our Forum Discussions, and view our latest Sessions and Webinars.

- Learn more about the Web Services SDK
- Browse objects managed by this host

Copyright © 1998-2012 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents.

VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

VMware products may contain individual open source software components, each of which has its own copyright and applicable license conditions. Please visit http://www.vmware.com/info?id=1023 for more information.

2. Click the ***Download vSphere Client*** link on the welcome page and save the installation file to your local system. Note that the vSphere Client is Windows-only software.
3. Run the vSphere Client installation file and follow the instructions on the screen.

Access to network

If you lock down your network on a port-by-port basis, ensure that the following ports are open between the NetShark and other devices it must communicate with:

- **TCP/22** – (ssh) Command line interface
- **TCP/443** – (https) Web interface and control from Riverbed® SteelCentral Packet Analyzer, also used by concurrent license server for Packet Analyzer
- **TCP or UDP/514** – Default port for external log use, configured in NetShark web UI
- **TCP/41017** – Traffic data to Riverbed® SteelCentral™ NetProfiler
- **UDP/123** – (ntp) Time synchronization
- **UDP/319 and 320** – (ptp) Time synchronization

Preparing the Virtual Services Platform

The Virtual Services Platform (VSP) requires disk space on the SteelHead EX; a management interface for management access to the ESXi virtualization platform; and a port to mirror traffic to virtual machines. If you have not set up VSP on the SteelHead EX, please see "Setting Up the Virtual Services Platform" in the *SteelHead Appliance Management Console User's Guide: SteelhHead EX Appliance (Series xx60) Includes RiOS®, Granite™ Edge, and VSP* for details.

If you are using VSP now, before continuing, please see "Appendix A: Migrating Legacy VSP Data" in the *SteelHead Appliance Management Console User's Guide*, referred to previously, for information on migrating data that you wish to use from legacy VSP and on migrating items you want to continue to use in the new ESXi environment.

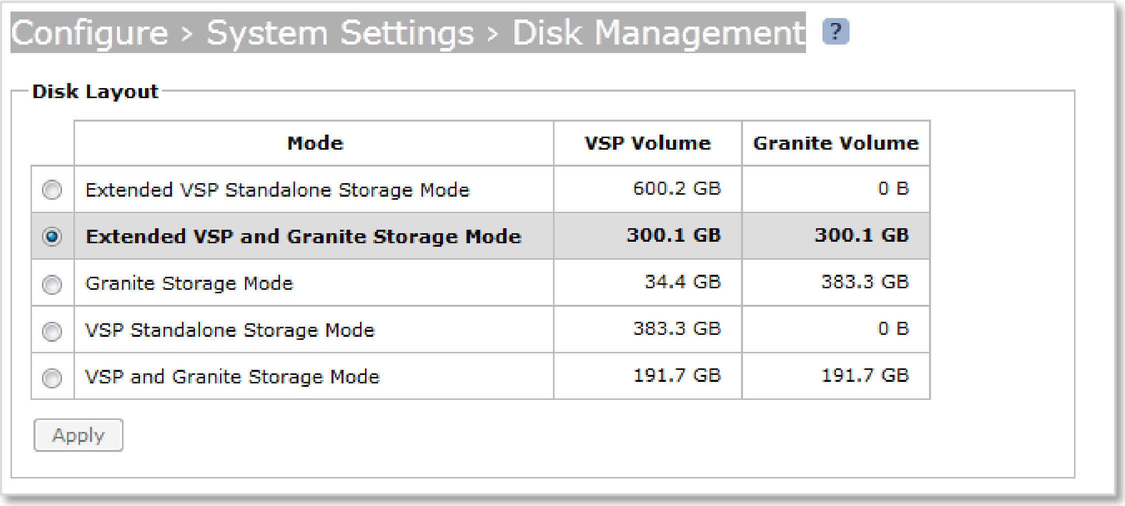
Important: Before continuing, confirm that the Aux port is enabled in RiOS on your SteelHead EX. When installing VSP, be sure to enable ***vmk2 (ESXi aux)*** as shown in Step 3, under "Reinitializing Virtual Services Platform."

Configuring the disk on the SteelHead EX

Log in to the web user interface of the SteelHead EX and use the menu options to navigate to the Disk Management page (Configure › System Settings › Disk Management). Choose the appropriate disk layout mode. For more information on the different disk layout options available, please refer to the *SteelHead Appliance Management Console User's Guide*, referred to previously.

Note: Switching the disk layout is a destructive operation. When you switch the disk layout, you lose your ESXi configuration, local data store, and unconverted VMDKs. For more information, see "Before You Begin" under "Configuring Disk Management" in the *SteelHead Appliance Management Console User's Guide*, referred to previously.

In the example below, the "Extended VSP and Granite Storage Mode" is selected.



Configure > System Settings > Disk Management

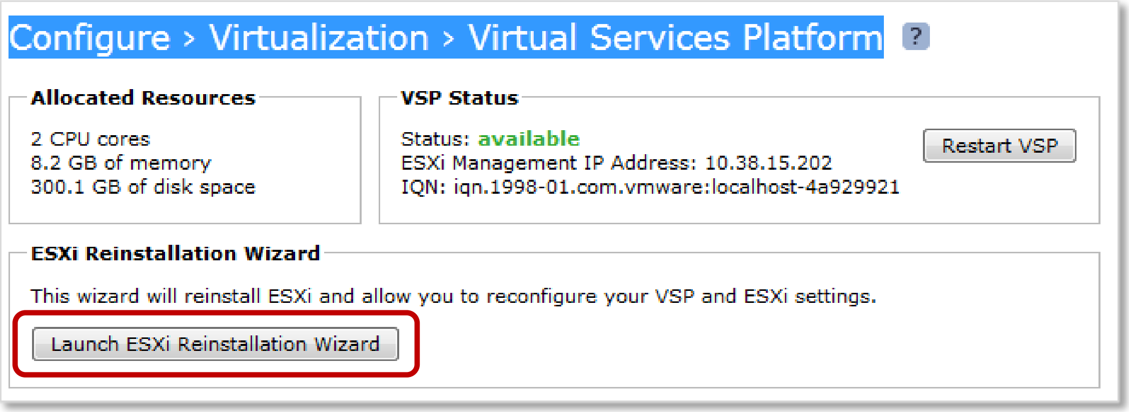
Disk Layout

	Mode	VSP Volume	Granite Volume
○	Extended VSP Standalone Storage Mode	600.2 GB	0 B
●	**Extended VSP and Granite Storage Mode**	**300.1 GB**	**300.1 GB**
○	Granite Storage Mode	34.4 GB	383.3 GB
○	VSP Standalone Storage Mode	383.3 GB	0 B
○	VSP and Granite Storage Mode	191.7 GB	191.7 GB

Reinitializing Virtual Services Platform

You select the settings the ESXi Reinstallation Wizard copies to the ESXi configuration. This overwrites any changes that were made directly in ESXi, for example, using vSphere or vCenter. See "Using the Virtual Machine Migration Wizard" in Appendix A in the *SteelHead Appliance Management Console User's Guide* to convert legacy virtual machines to the new format.

1. Log in to the web user interface of the SteelHead EX and, using the menu options, navigate to the Virtual Services Platforms page (Configure › Virtualization › Virtual Services Platform). If you are installing ESXi for the first time, click ***Launch ESXi Installation Wizard***. Otherwise, click ***Launch ESXi Reinstallation Wizard*** to launch the ESXi wizard.



Configure > Virtualization > Virtual Services Platform

Allocated Resources

2 CPU cores
8.2 GB of memory
300.1 GB of disk space

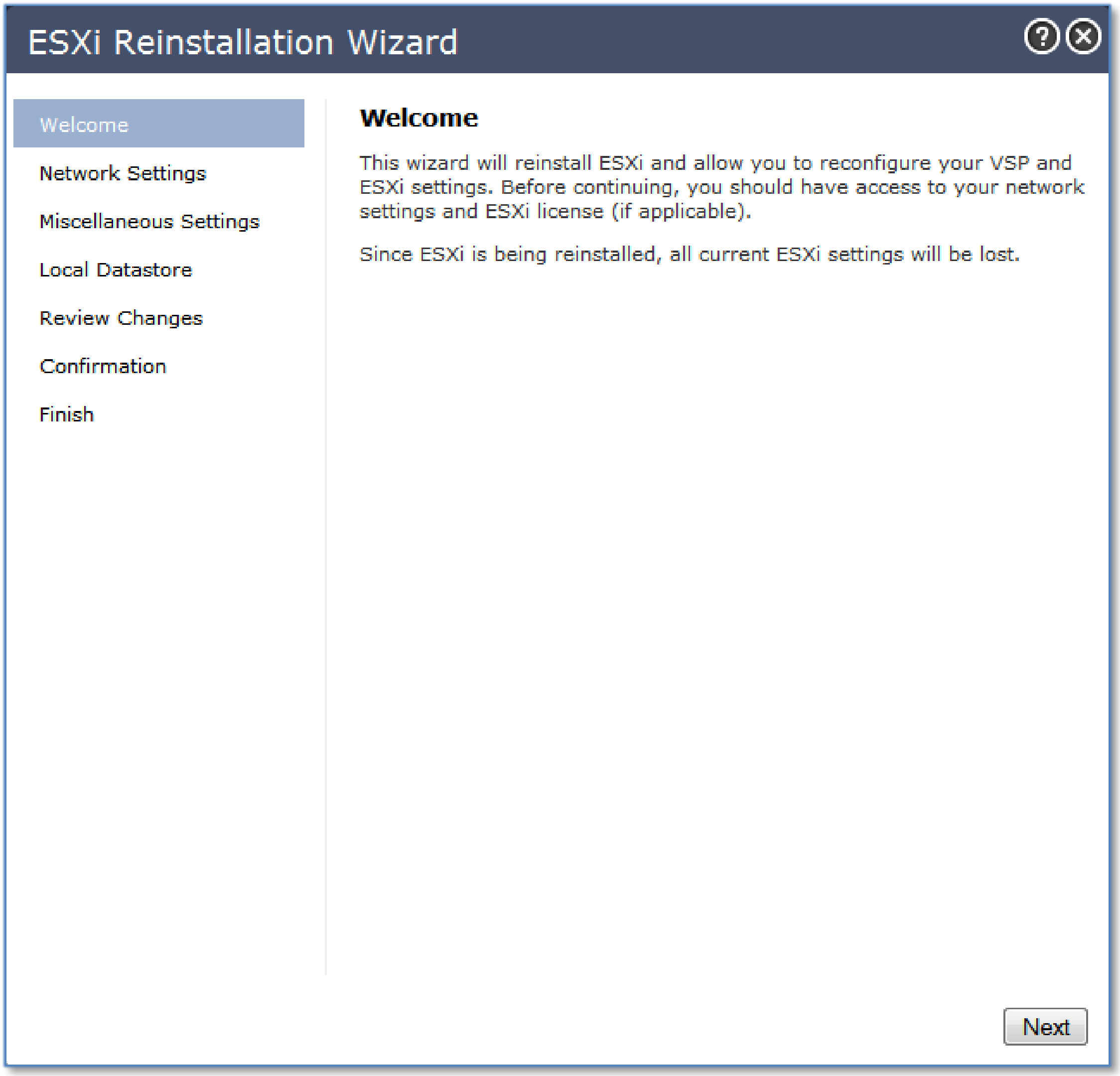
VSP Status

Status: available
ESXi Management IP Address: 10.38.15.202
IQN: iqn.1998-01.com.vmware:localhost-4a929921

ESXi Reinstallation Wizard

This wizard will reinstall ESXi and allow you to reconfigure your VSP and ESXi settings.

2. Click ***Next***.



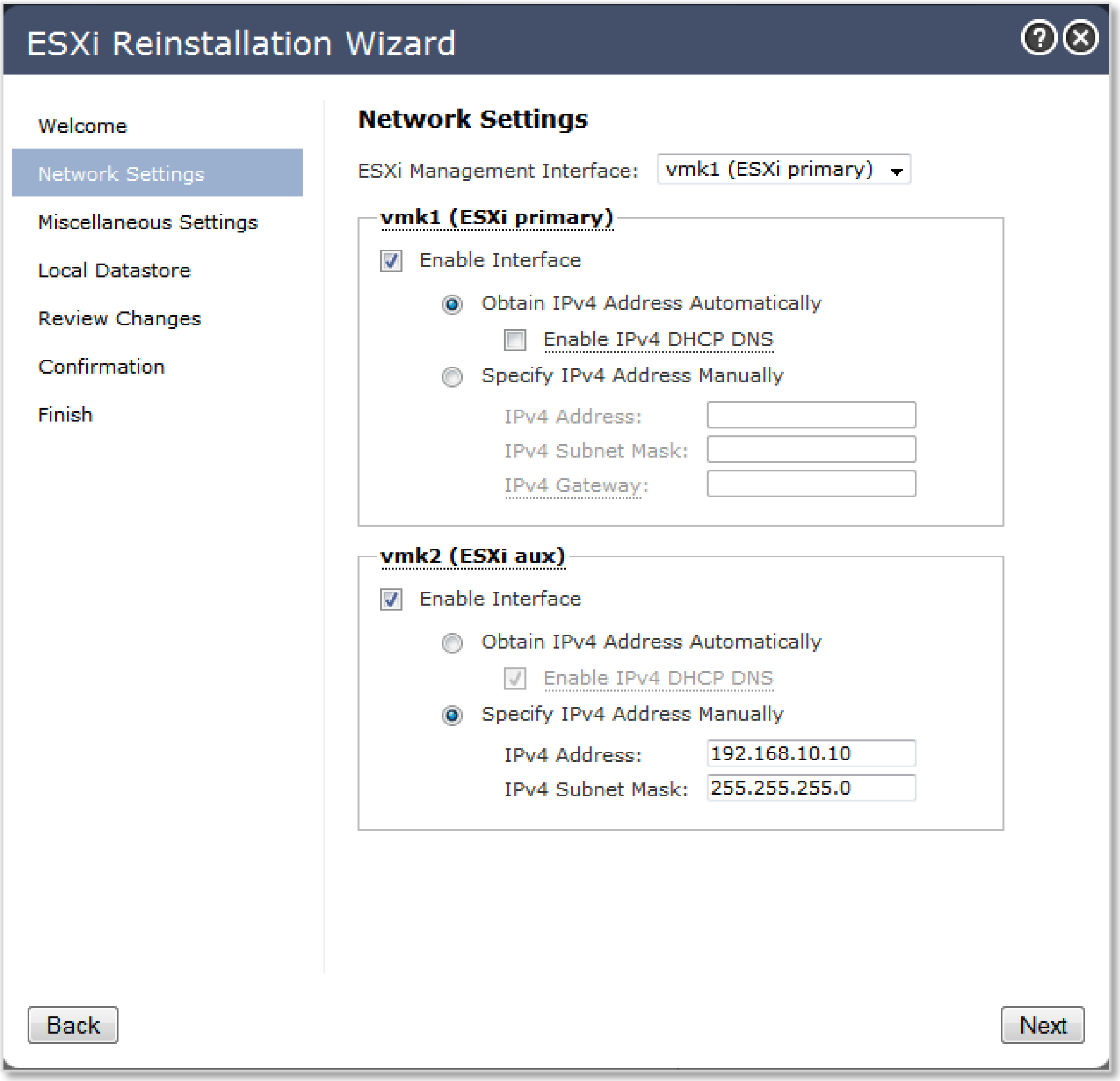
ESXi Reinstallation Wizard

Welcome

This wizard will reinstall ESXi and allow you to reconfigure your VSP and ESXi settings. Before continuing, you should have access to your network settings and ESXi license (if applicable).

Since ESXi is being reinstalled, all current ESXi settings will be lost.

3. On the ***Network Settings*** page you configure the management interface for the ESXi and the port where mirrored traffic from the SteelHead EX is received.



Network Settings

ESXi Management Interface: vmk1 (ESXi primary)

vmk1 (ESXi primary)

☑ Enable Interface

● Obtain IPv4 Address Automatically

☐ Enable IPv4 DHCP DNS

○ Specify IPv4 Address Manually

IPv4 Address:

IPv4 Subnet Mask:

IPv4 Gateway:

vmk2 (ESXi aux)

☑ Enable Interface

○ Obtain IPv4 Address Automatically

☑ Enable IPv4 DHCP DNS

● Specify IPv4 Address Manually

IPv4 Address: 192.168.10.10

IPv4 Subnet Mask: 255.255.255.0

Select which interface will be used as the management interface for the ESXi host from the drop down list for ***ESXi Management Interface***. In this example, the ***vmk1 (ESXi primary)*** interface is selected. This configuration assumes that the management network has a DHCP/DNS server that can provide an IP address.

> **Note:** Either interface can be used as the management interface. The interface to use should be determined based on your network setup.

The interface not selected as the management interface is used to receive mirrored SteelHead EX traffic to capture and analyze. An IP address must be configured for the interface, but the address is not used. In this example the IP address assigned is ***192.168.10.10*** with a subnet mask of ***255.255.255.0***.

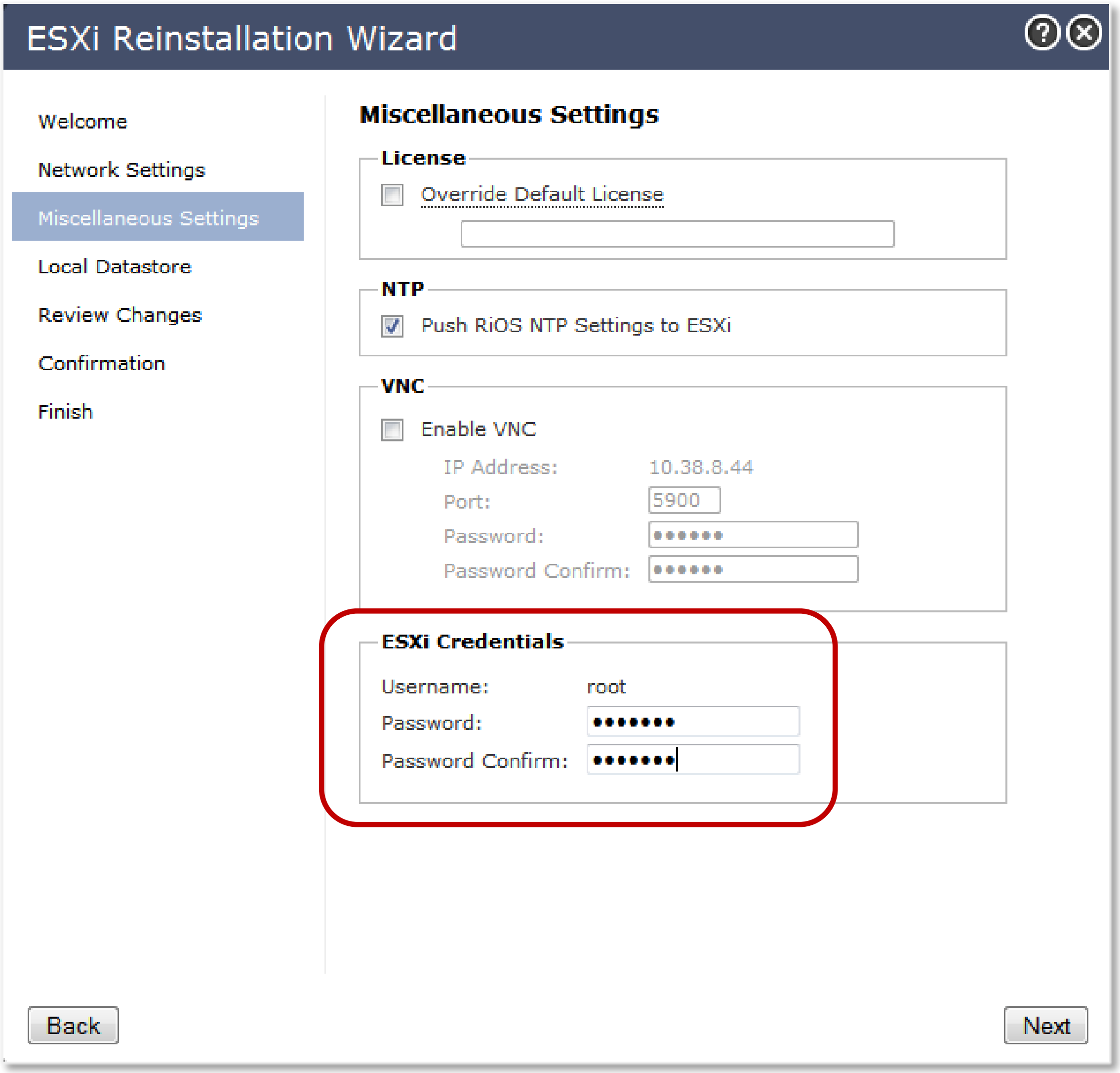
- Under the ***vmk1 (ESXi primary)*** section
  - Select the check box for ***Enable Interface***
  - Select ***Obtain IPv4 Address Automatically***
    - Select ***Enable IPv4 DHCP DNS***
- Under the ***vmk2 (ESXi aux)*** section
  - Select the check box for ***Enable Interface***
  - Select ***Specify IPv4 Address Manually***
  - Configure an IP address with subnet mask

Click ***Next***.

4. Specify a password for the Username ***root*** under the ***ESXi Credentials*** section.

   Important: If you change the ESXi password using a Virtual Network Computing (VNC) connection or using vSphere, you also must change it on this page. Changing the ESXi password using VNC or vSphere triggers the ESXi Communication Failed alarm in RiOS. When the passwords are not synchronized, RiOS cannot communicate with ESXi.

   Click ***Next***.



ESXi Reinstallation Wizard

Miscellaneous Settings

License

□ Override Default License

NTP

☑ Push RiOS NTP Settings to ESXi

VNC

□ Enable VNC

IP Address: 10.38.8.44

Port: 5900

Password: ••••••

Password Confirm: ••••••

ESXi Credentials

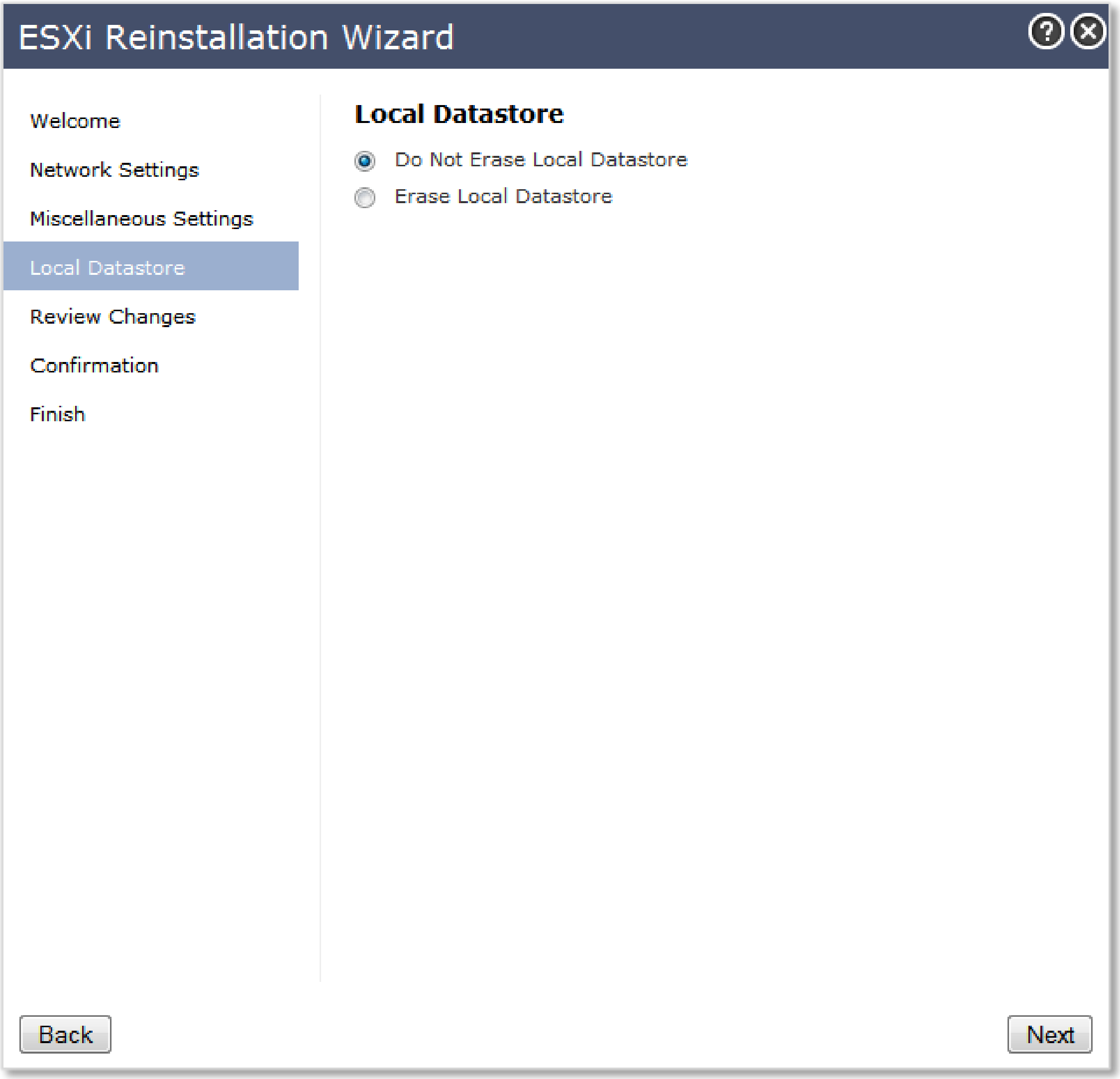
Username: root

Password: •••••••

Password Confirm: •••••••

5. Select the desired option under ***Local Datastore***. Use caution when selecting this option, as it deletes all data from the local datastore, including existing VMs, after you confirm.

   Note: Riverbed recommends that you back up ESXi data before proceeding.



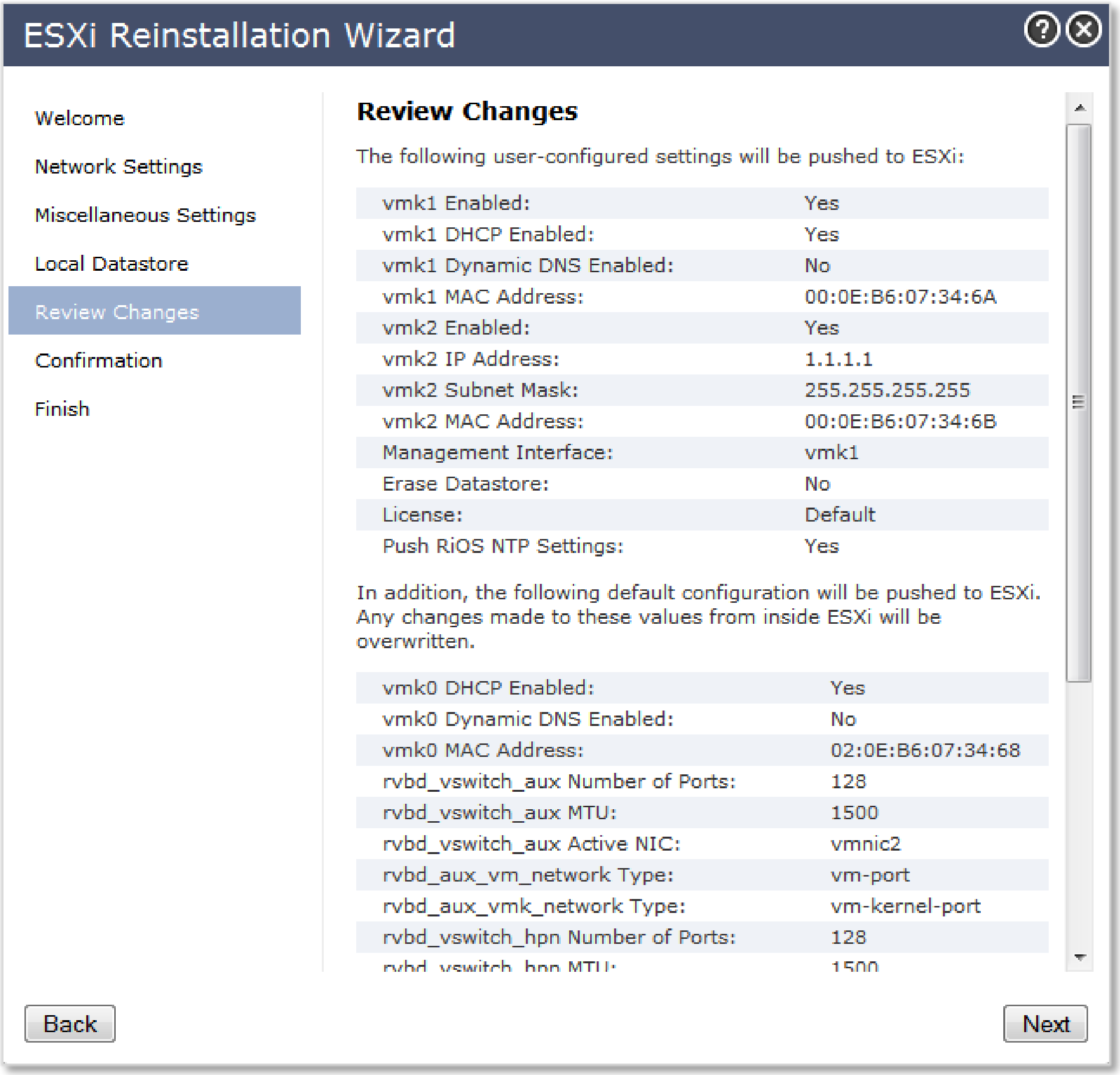
ESXi Reinstallation Wizard

Local Datastore

● Do Not Erase Local Datastore

○ Erase Local Datastore

6. Review the settings and click ***Next***.



Review Changes

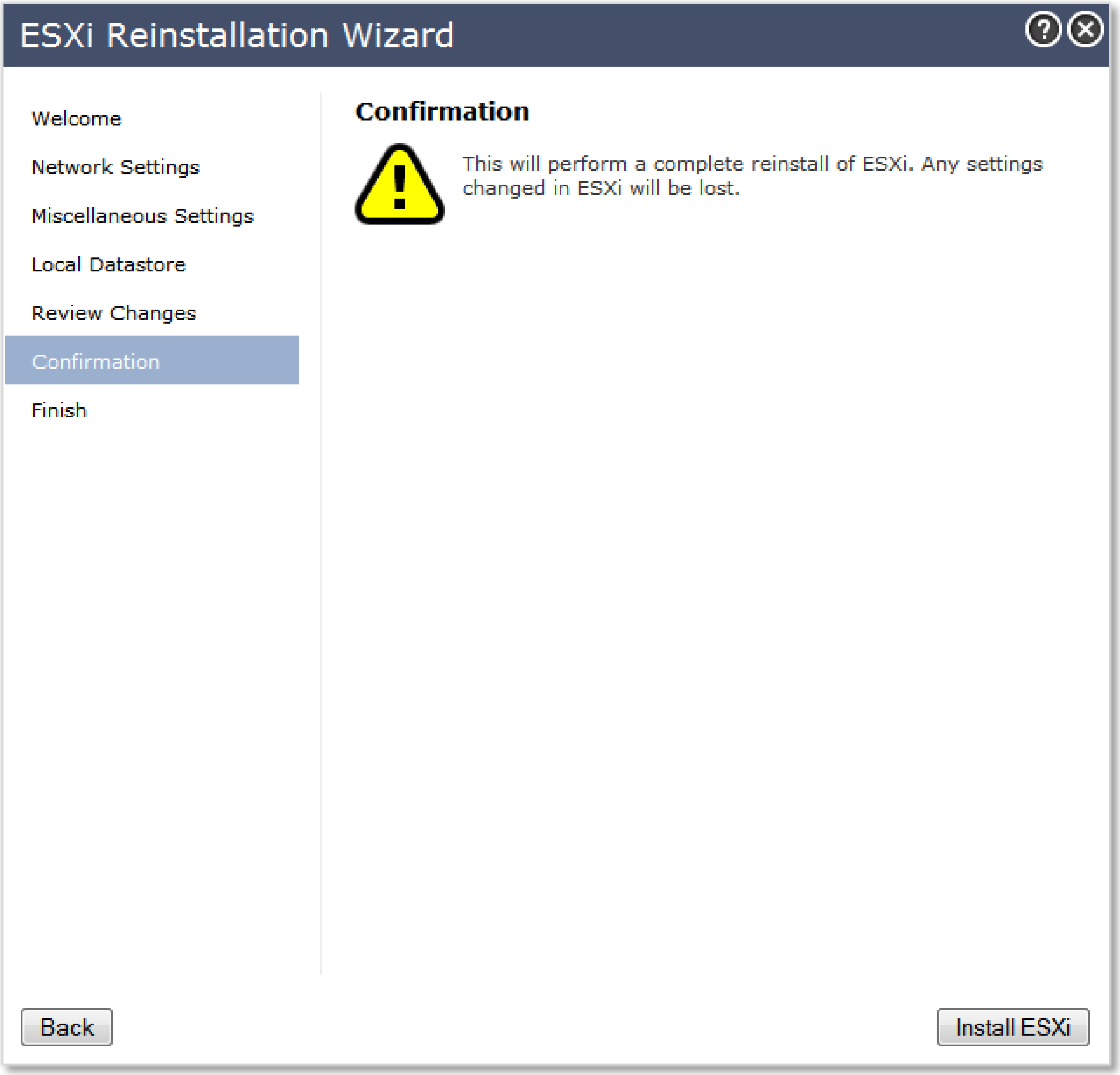
The following user-configured settings will be pushed to ESXi:

vmk1 Enabled:	Yes
vmk1 DHCP Enabled:	Yes
vmk1 Dynamic DNS Enabled:	No
vmk1 MAC Address:	00:0E:B6:07:34:6A
vmk2 Enabled:	Yes
vmk2 IP Address:	1.1.1.1
vmk2 Subnet Mask:	255.255.255.255
vmk2 MAC Address:	00:0E:B6:07:34:6B
Management Interface:	vmk1
Erase Datastore:	No
License:	Default
Push RiOS NTP Settings:	Yes

In addition, the following default configuration will be pushed to ESXi. Any changes made to these values from inside ESXi will be overwritten.

vmk0 DHCP Enabled:	Yes
vmk0 Dynamic DNS Enabled:	No
vmk0 MAC Address:	02:0E:B6:07:34:68
rvbd_vswitch_aux Number of Ports:	128
rvbd_vswitch_aux MTU:	1500
rvbd_vswitch_aux Active NIC:	vmnic2
rvbd_aux_vm_network Type:	vm-port
rvbd_aux_vmk_network Type:	vm-kernel-port
rvbd_vswitch_hpn Number of Ports:	128
rvbd_vswitch_hpn MTU:	1500

7. Please read the warning on the ***Confirmation*** page. You can use the ***Back*** button to modify any settings that have been configured in the previous steps. To continue with the installation, click ***Install ESXi***.

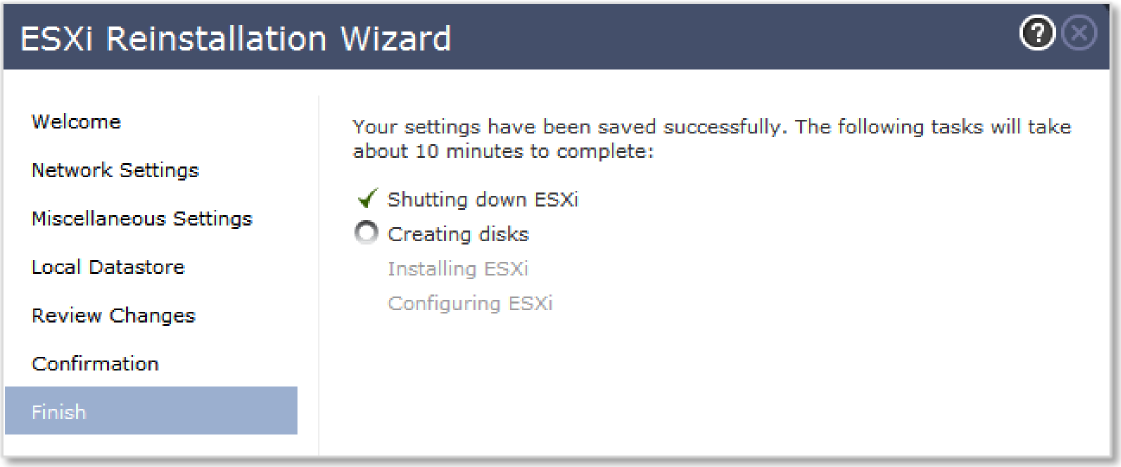


ESXi Reinstallation Wizard

Confirmation

This will perform a complete reinstall of ESXi. Any settings changed in ESXi will be lost.

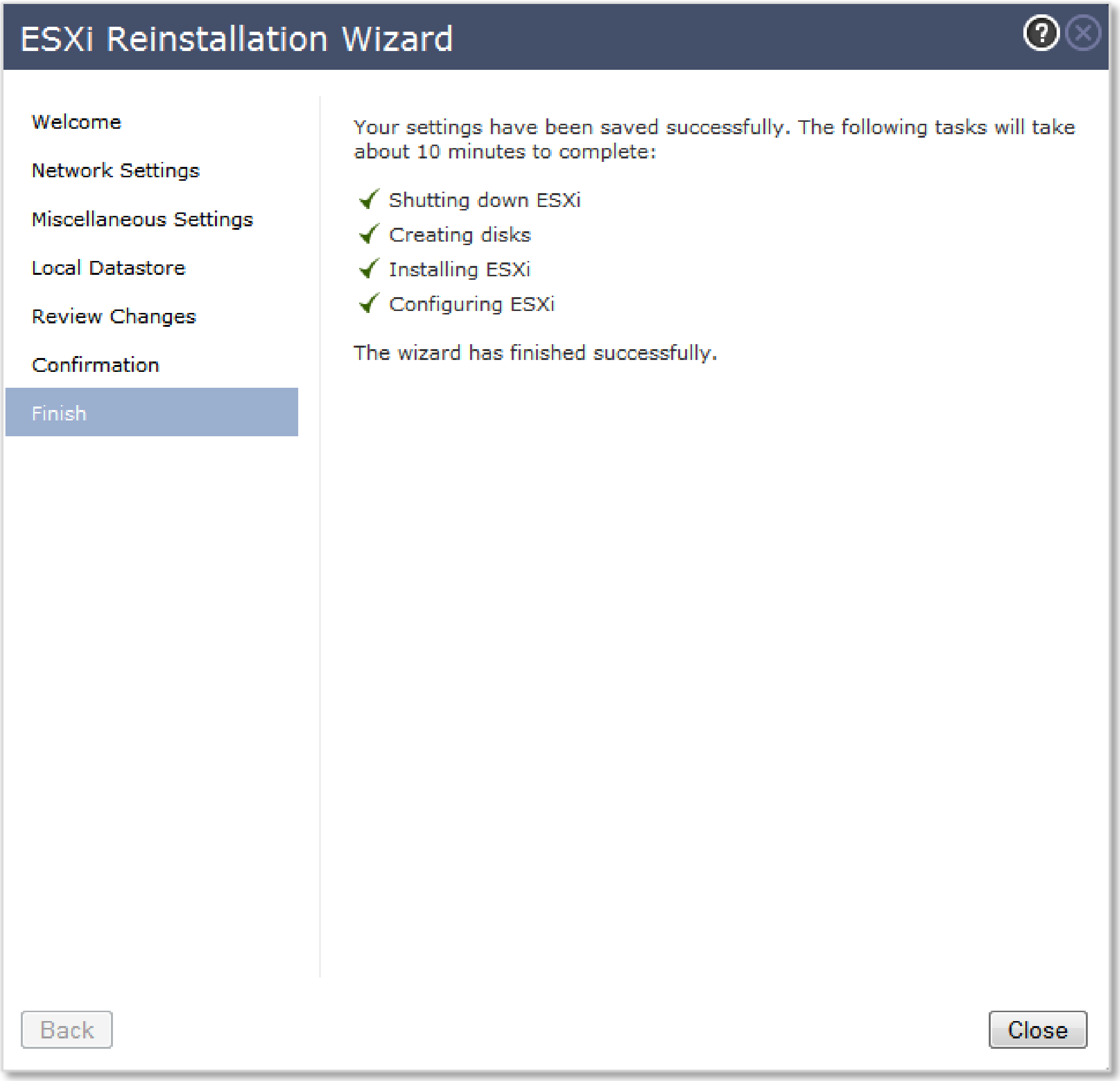
The ESXi reinstallation starts. It may take several minutes to complete.



Your settings have been saved successfully. The following tasks will take about 10 minutes to complete:

- ✓ Shutting down ESXi
- ○ Creating disks
- Installing ESXi
- Configuring ESXi

8. Click ***Close*** when the Wizard has finished successfully



Your settings have been saved successfully. The following tasks will take about 10 minutes to complete:

- ✓ Shutting down ESXi
- ✓ Creating disks
- ✓ Installing ESXi
- ✓ Configuring ESXi

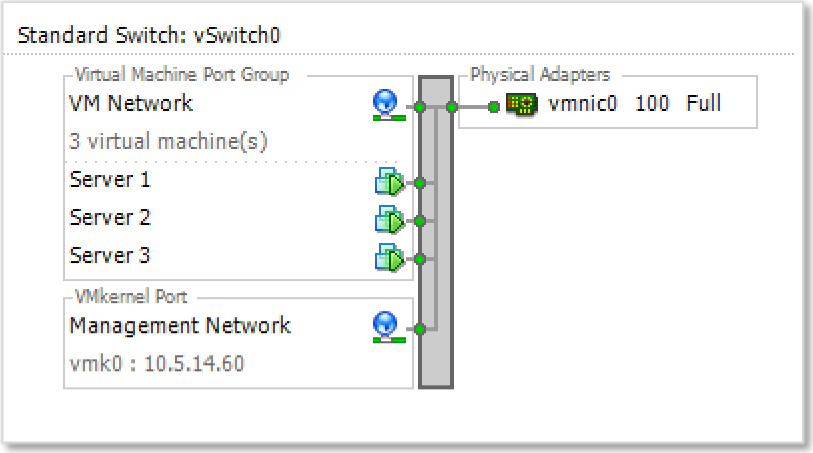
The wizard has finished successfully.

Preparing the ESXi server

Example NetShark configuration on an ESXi server

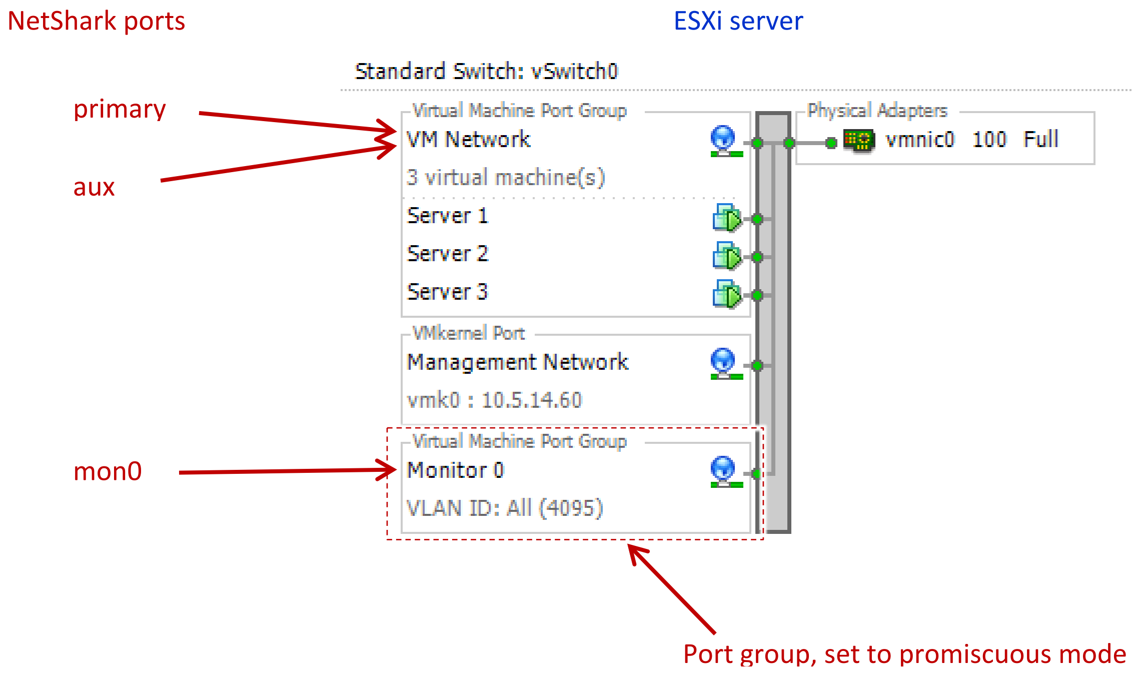
Before deploying the NetShark OVA package, ports on the ESXi server must be prepared for use in NetShark management and traffic monitoring and/or capture. The following example illustrates what is required. You can skip this example if you are already familiar with installing NetShark on an ESXi server.

A typical ESXi server might have a number of application servers running in virtual machines, all located within a single port group (VM Network) on a virtual switch. The diagram below shows these application servers as Server 1, Server 2, and Server 3.



When you add a NetShark to this ESXi server, **the port group that contains the NetShark monitor port must be in promiscuous mode, so that the monitor port sees all the traffic on the virtual switch**. Since the promiscuous mode setting applies to an entire port group, and since the port group containing the application servers should be in non-promiscuous mode (the default mode), you must use a separate port group for the NetShark monitor port, set to promiscuous mode.

During deployment of the OVA package to the ESXi server, you must map the preconfigured ports of the NetShark to port groups on the virtual switch, like this:



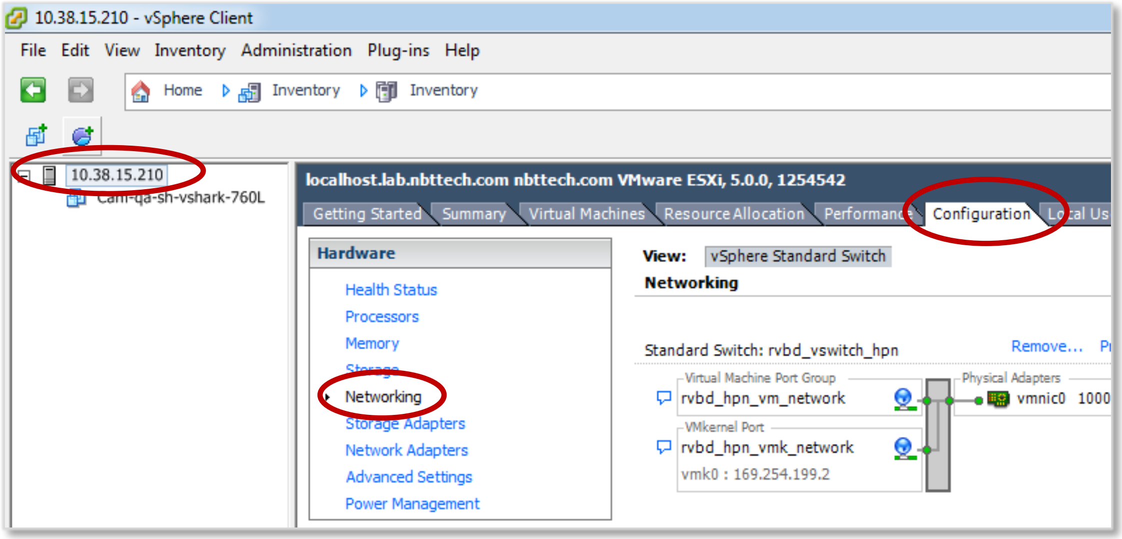
Note that the NetShark management ports, `primary` and `aux`, do not capture data, so they should be in a non-promiscuous-mode port group (VM Network in this example). The monitor port, `mon0`, will be in a promiscuous-mode port group, (Monitor0) in this example.

Setting a port group to promiscuous mode

Note: During the ESXi installation, an HPN virtual switch on vnic0 is created. The switch has a kernel port and a virtual machine port. This switch is used for communication within the appliance. Do not modify or delete this virtual switch.

Set a port group, ***rvbd_aux_vm_network***, to promiscuous mode.

1. In the vSphere Client, select the ESXi host by clicking on the IP address of the ESXi host.
2. Click the ***Configuration*** tab and choose ***Networking*** under ***Hardware***.



10.38.15.210 - vSphere Client

localhost.lab.nbttech.com nbttech.com VMware ESXi, 5.0.0, 1254542

View: vSphere Standard Switch

Standard Switch: rvbd_vswitch_hpn

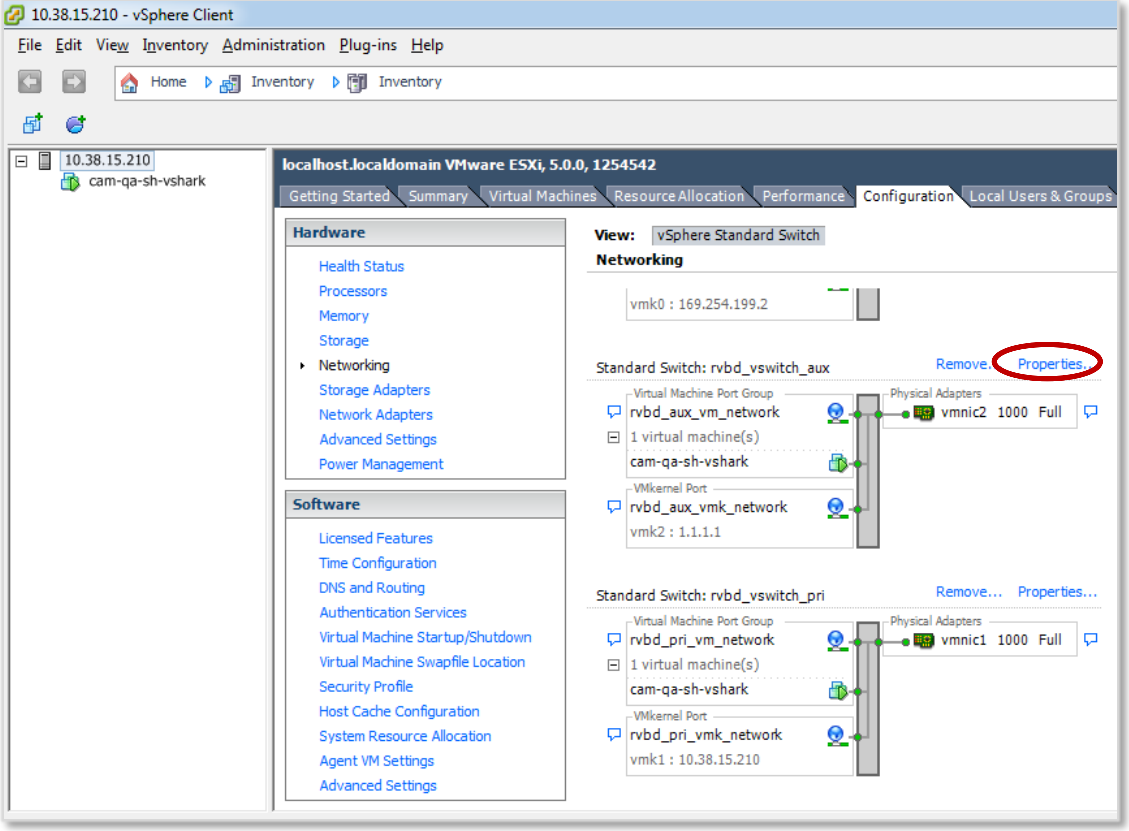
Virtual Machine Port Group: rvbd_hpn_vm_network

VMkernel Port: rvbd_hpn_vmk_network

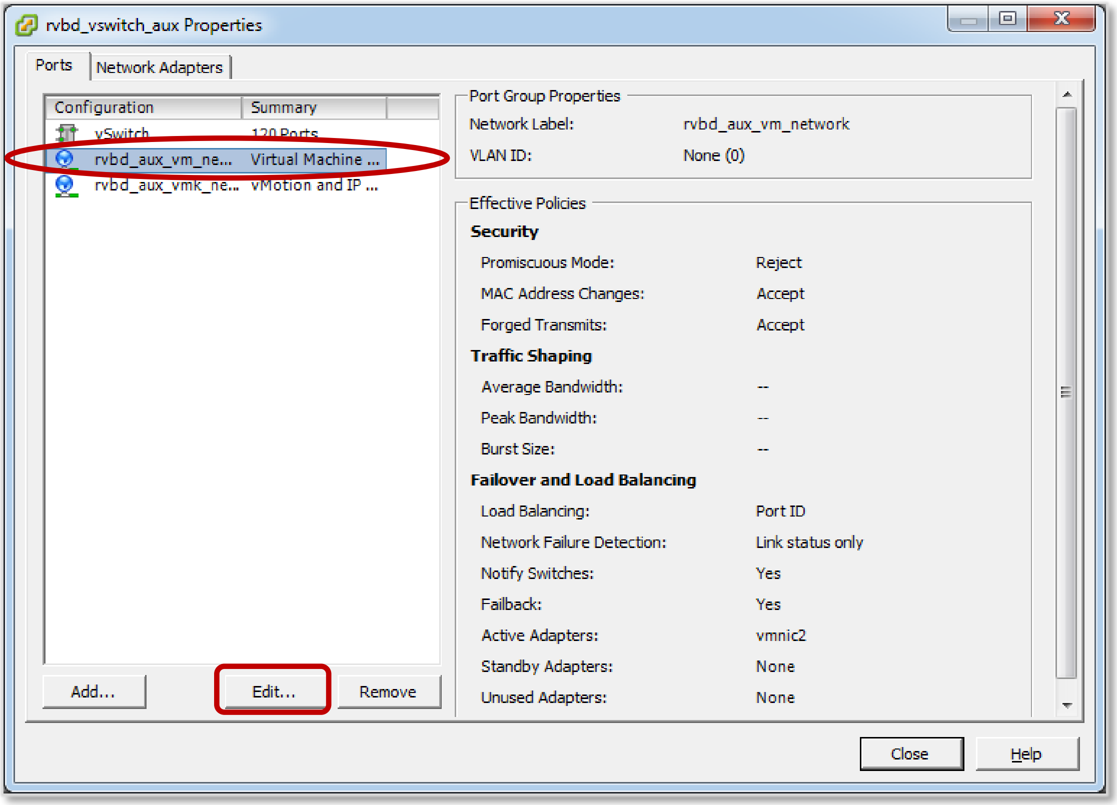
vmk0 : 169.254.199.2

Physical Adapters: vmnic0 1000

3. Click the properties of the ***Standard Switch: rvbd_vswitch_aux***.



4. Select the ***rvbd_aux_vm_network*** port group and click the ***Edit…*** button.



Configuration	Summary
vSwitch	120 Ports
rvbd_aux_vm_ne...	Virtual Machine ...
rvbd_aux_vmk_ne...	vMotion and IP ...

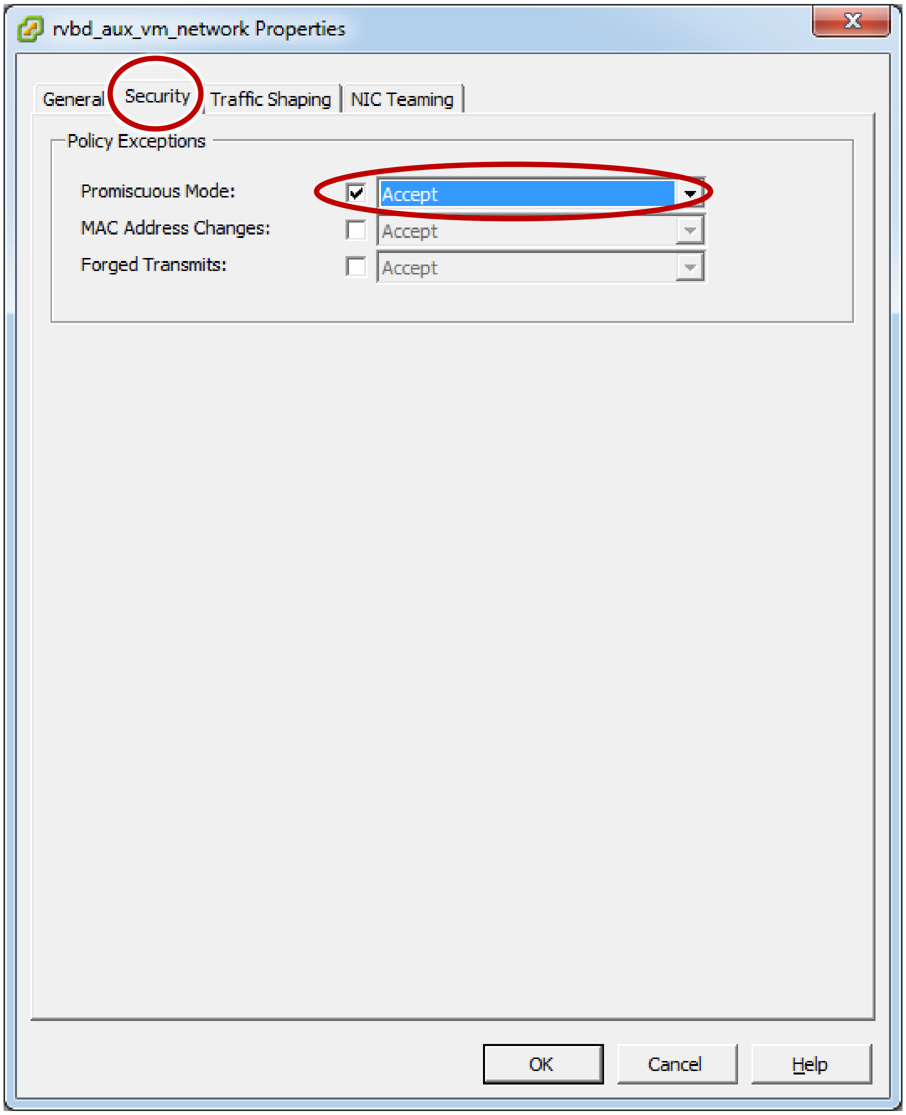
Port Group Properties

Network Label:	rvbd_aux_vm_network
VLAN ID:	None (0)

Effective Policies

Security	
Promiscuous Mode:	Reject
MAC Address Changes:	Accept
Forged Transmits:	Accept
Traffic Shaping	
Average Bandwidth:	--
Peak Bandwidth:	--
Burst Size:	--
Failover and Load Balancing	
Load Balancing:	Port ID
Network Failure Detection:	Link status only
Notify Switches:	Yes
Failback:	Yes
Active Adapters:	vmnic2
Standby Adapters:	None
Unused Adapters:	None

5. Click the ***Security*** tab, check the ***Promiscuous Mode:*** check box, and select a value of ***Accept***. Click ***OK***.



Policy Exceptions

Promiscuous Mode: ☑ Accept

MAC Address Changes: □ Accept

Forged Transmits: □ Accept

Preparing the SteelHead EX environment

The command-line interface (CLI) is used to configure the Riverbed® Optimization System (RiOS®) solution management interface selected to mirror traffic to the ESXi vSwitch (See Step 3 under "Reinitializing Virtual Services Platform.") In this example, the Aux interface is configured to mirror traffic to the ESXi vSwitch.

1. SSH into the SteelHead EX to get to the SteelHead EX CLI.
2. At the console prompt, enter the following commands in the sequence shown.
   Note: A generic console prompt, ***rvbd,*** is included on each command line below. Your console prompt will be different.

   ```
   Riverbed Steelhead
   Last login: Tue Oct 29 19:29:15
   rvbd > enable
   rvbd # config t
   rvbd (config) # interface aux traffic-mode span
   rvbd (config) # end
   rvbd # write mem
   ```

3. Exit from the SteelHead CLI.

   ```
   rvbd # exit
   Connection closed.
   ```

   For information on the above CLI commands, please see the *Riverbed® Command-Line Interface Reference Manual*.

The ESXi server on the SteelHead EX is now prepared for the deployment of the NetShark OVA package.

2. Deploying the NetShark

Deploying the NetShark OVA package to the ESXi server

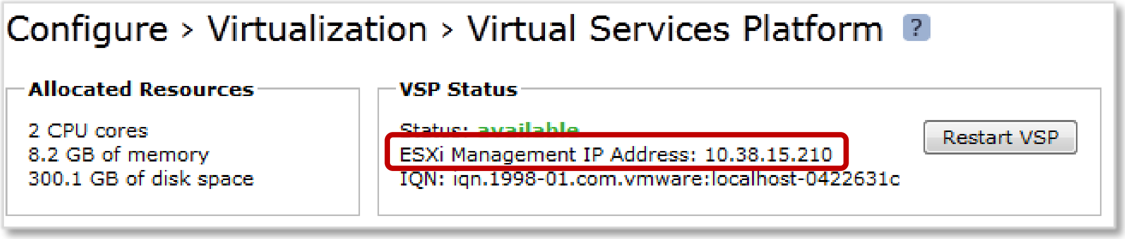
The NetShark software you deploy to the server comes in the form of a NetShark OVA package. This package is preconfigured with these virtual components:

`primary`	primary management port
`aux`	secondary management port
`mon0`	primary monitor (data capture) port
OS disk	operating system disk for the NetShark

After you have deployed the OVA package to the server, you can add more virtual components:

- one additional hard disk for packet storage
- up to three more monitor ports

Log in to the web user interface of the SteelHead EX. Using the menu options, navigate to the Virtual Services Platform page (Configure › Virtualization › Virtual Services Platform). Note the ESXi Management IP Address.



Configure > Virtualization > Virtual Services Platform

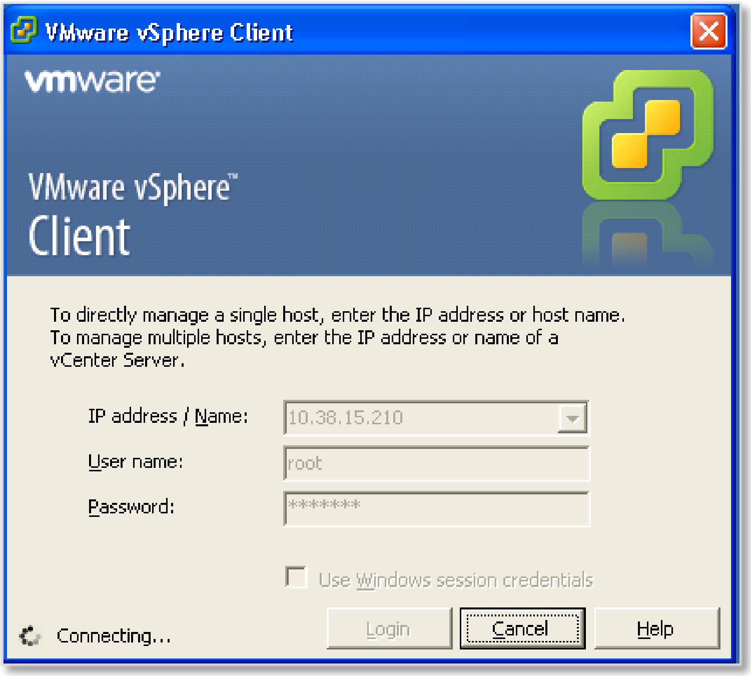
Allocated Resources

2 CPU cores
8.2 GB of memory
300.1 GB of disk space

VSP Status

Status: available
ESXi Management IP Address: 10.38.15.210
IQN: iqn.1998-01.com.vmware:localhost-0422631c

1. Launch the VSphere Client application. Use the IP address noted above to connect to the ESXi host on the SteelHead EX.



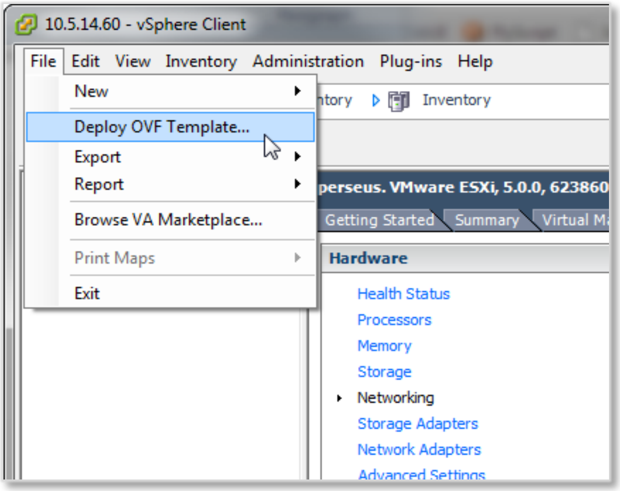
To directly manage a single host, enter the IP address or host name.
To manage multiple hosts, enter the IP address or name of a vCenter Server.

IP address / Name: 10.38.15.210
User name: root
Password: *******

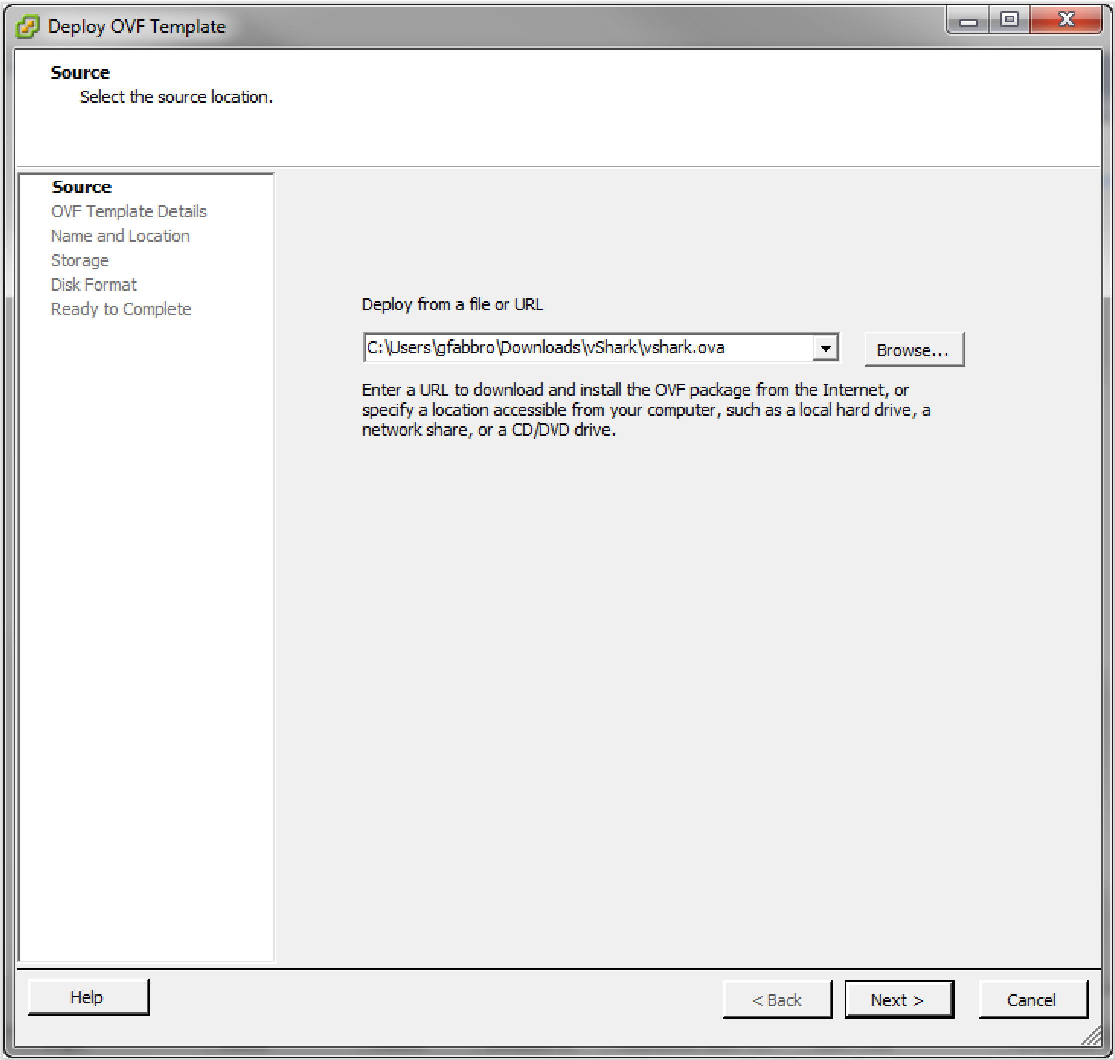
□ Use Windows session credentials

Connecting...

2. Click File->***Deploy OVF Template…***.



3. On the ***Source*** screen enter the path to the NetShark OVA file.



Source

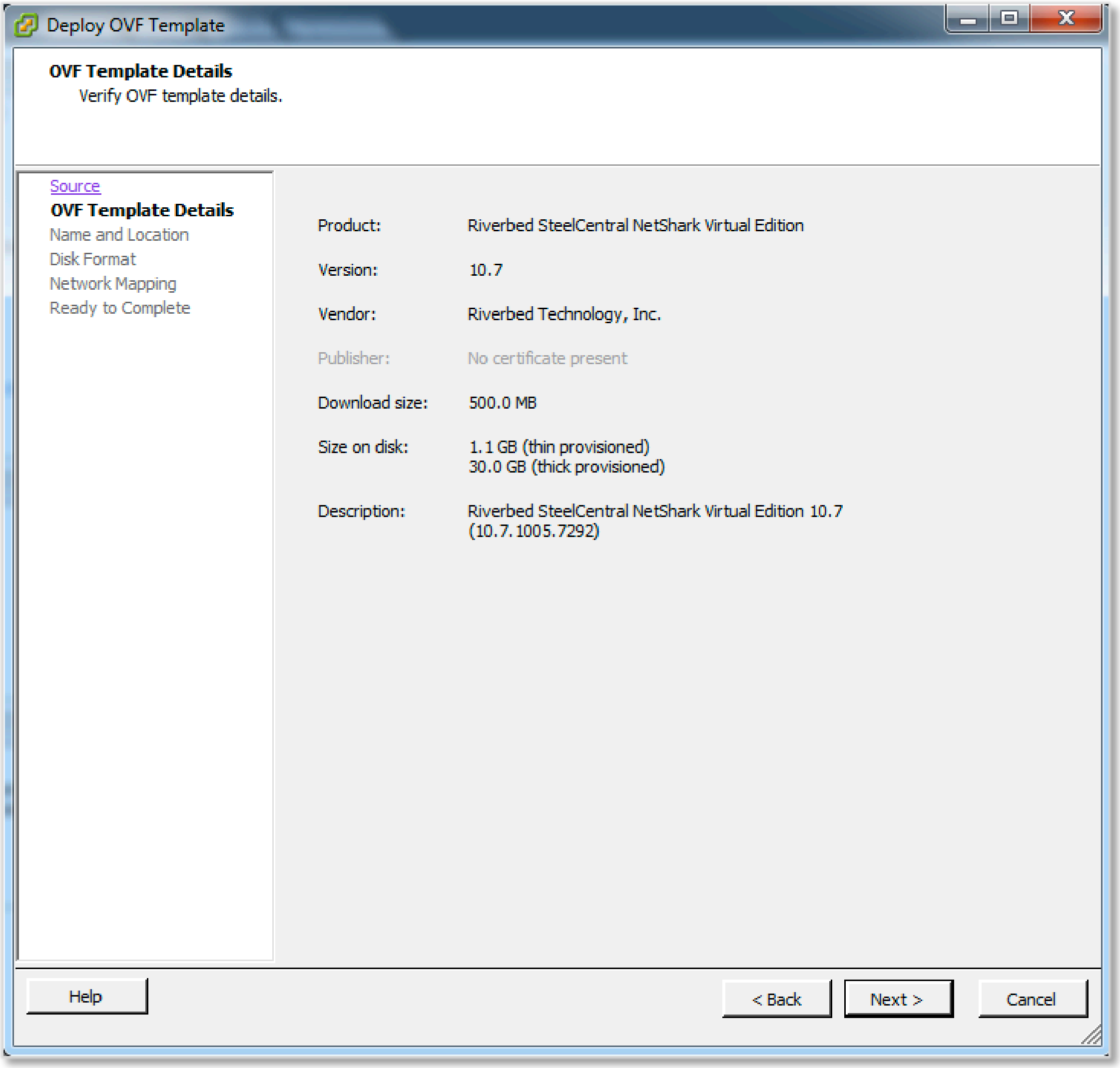
Select the source location.

Deploy from a file or URL

C:\Users\gfabbro\Downloads\vShark\vshark.ova

Enter a URL to download and install the OVF package from the Internet, or specify a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

4. On the ***OVF Template Details*** screen, click ***Next***.

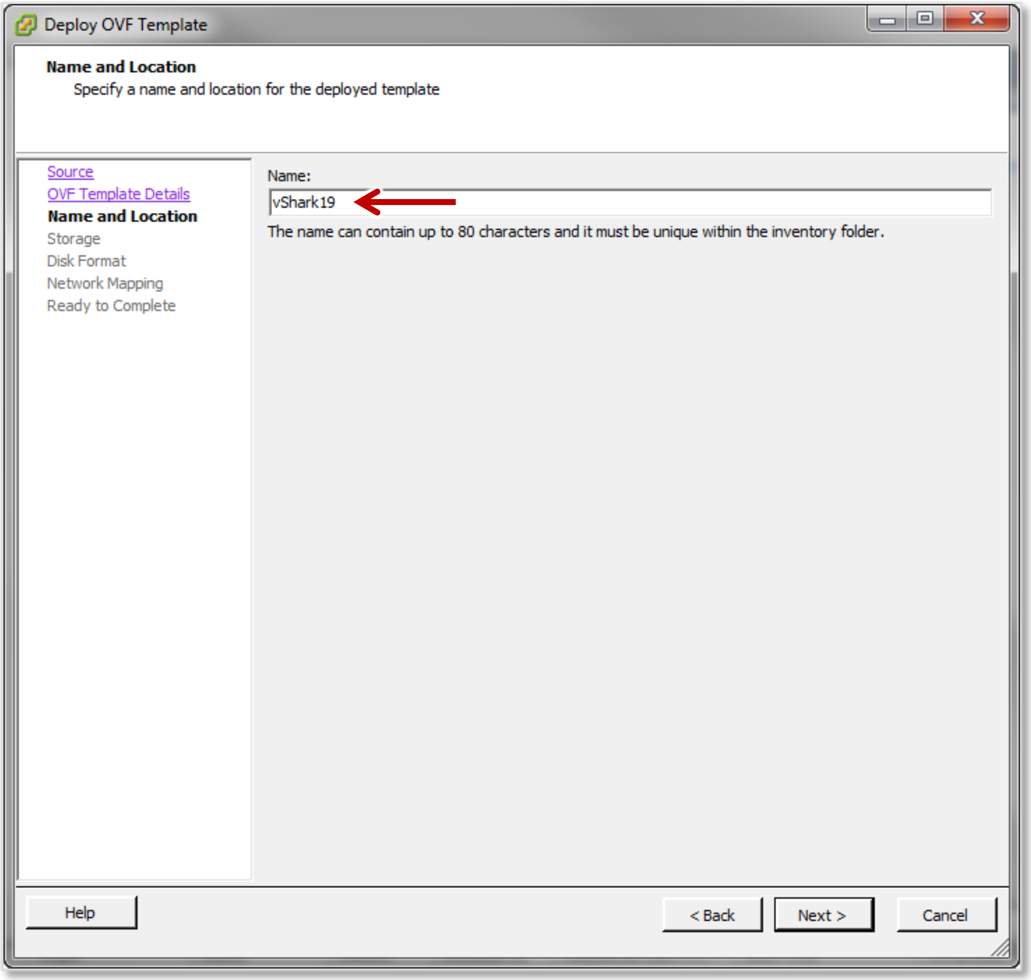


OVF Template Details

Verify OVF template details.

Product:	Riverbed SteelCentral NetShark Virtual Edition
Version:	10.7
Vendor:	Riverbed Technology, Inc.
Publisher:	No certificate present
Download size:	500.0 MB
Size on disk:	1.1 GB (thin provisioned) 30.0 GB (thick provisioned)
Description:	Riverbed SteelCentral NetShark Virtual Edition 10.7 (10.7.1005.7292)

5. On the ***Name and Location*** screen enter a name for the NetShark.



Deploy OVF Template

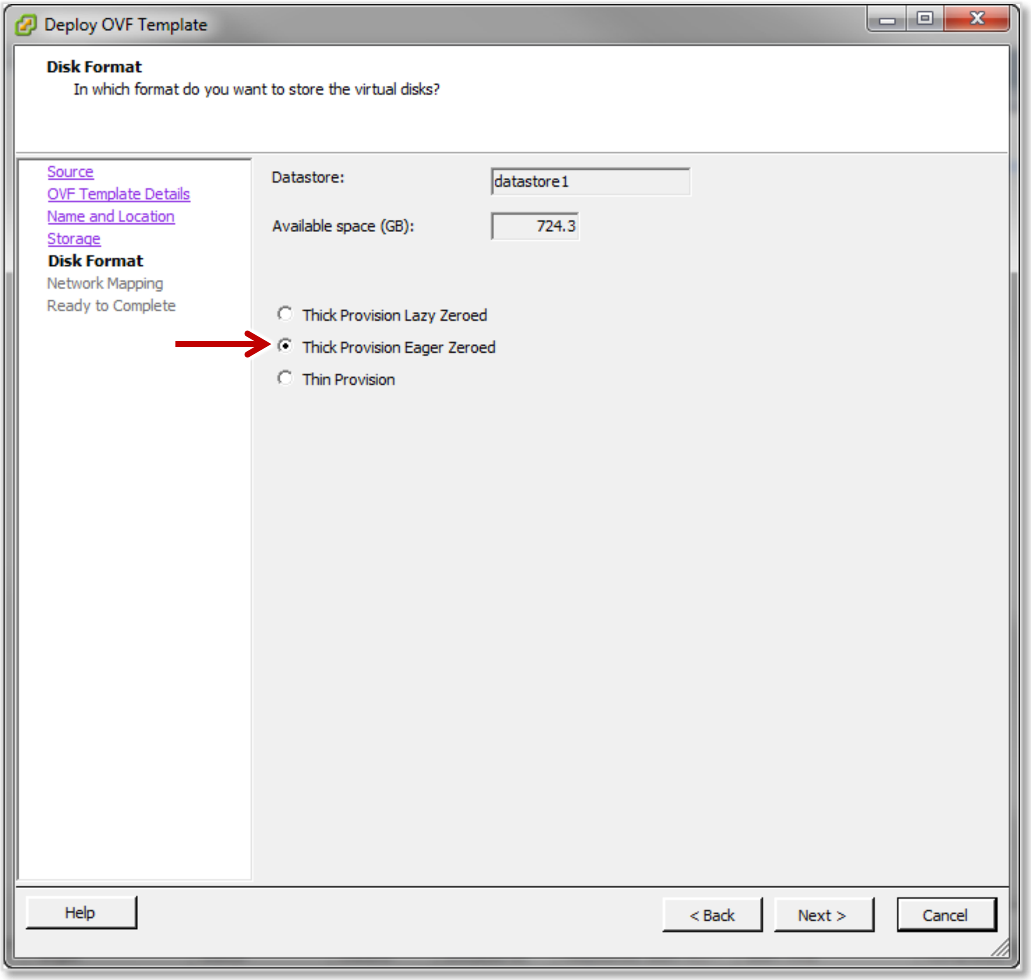
Name and Location

Specify a name and location for the deployed template

Name: vShark19

The name can contain up to 80 characters and it must be unique within the inventory folder.

6. On the ***Disk Format*** screen select the disk provisioning format:
    - Select Thick Provision Eager Zeroed.



Deploy OVF Template

Disk Format

In which format do you want to store the virtual disks?

Datastore: datastore1

Available space (GB): 724.3

○ Thick Provision Lazy Zeroed

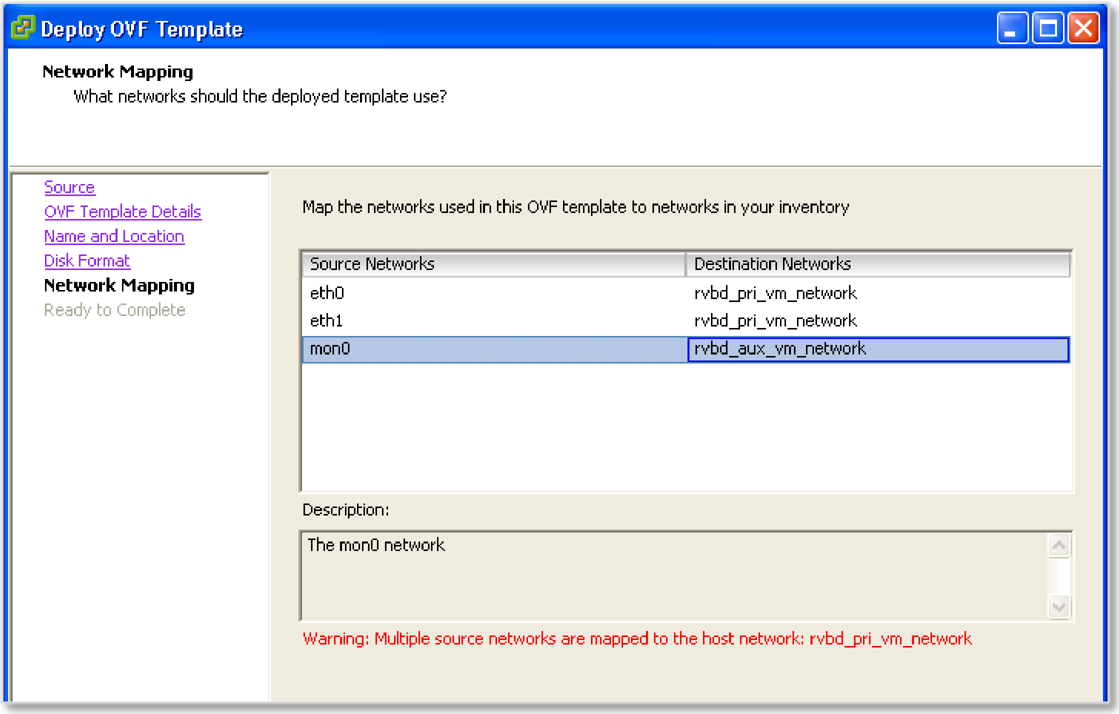
● Thick Provision Eager Zeroed

○ Thin Provision

7. On the ***Network Mapping*** page, map the source networks (ports) of the NetShark to destination networks (port groups) on the server.

   The `primary` and `aux` source networks are for management. Map them to a non-promiscuous mode (the default mode) destination network. In the example below ***rvbd_pri_vm_network*** is a non-promiscuous mode destination network.

   The `mon0` source network is for data capture. **A monitor port must be in promiscuous mode, so that the monitor port sees all the traffic on the virtual switch**. Map it to a promiscuous-mode destination network. In the example below, ***rvbd_aux_vm_network*** is a promiscuous mode destination network.



Network Mapping
What networks should the deployed template use?

Map the networks used in this OVF template to networks in your inventory

Source Networks	Destination Networks
eth0	rvbd_pri_vm_network
eth1	rvbd_pri_vm_network
mon0	rvbd_aux_vm_network

Description:

The mon0 network

Warning: Multiple source networks are mapped to the host network: rvbd_pri_vm_network

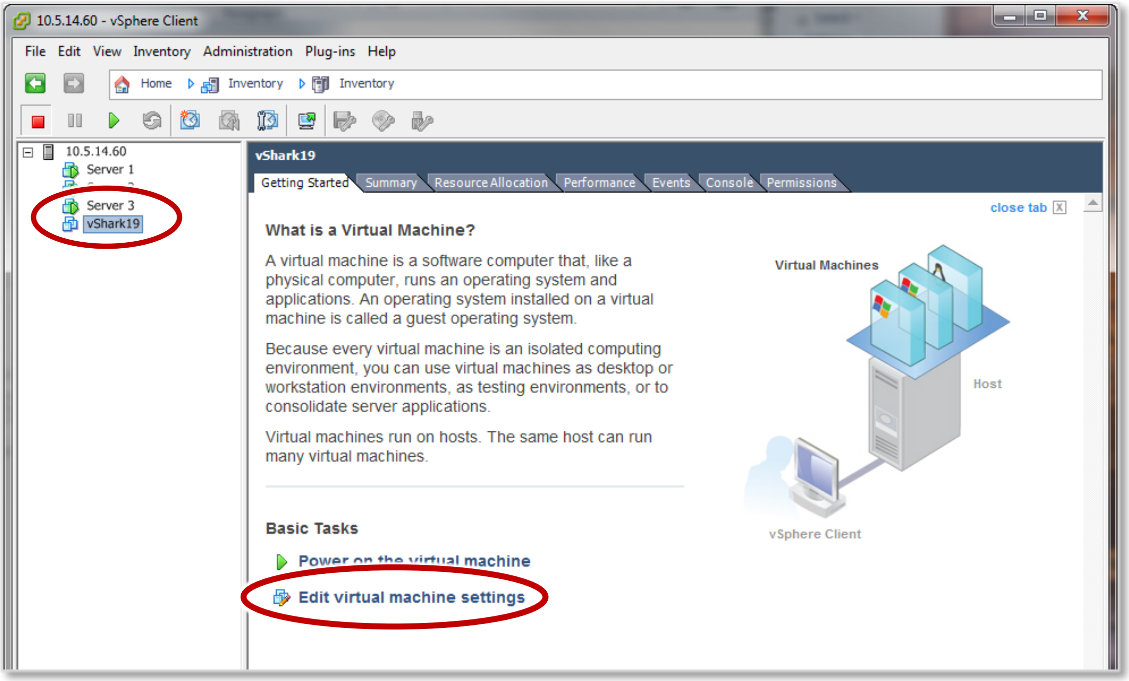
8. On the ***Ready to Complete*** summary page click ***Finish*** to start the deployment.

Adding a hard disk

Important The virtual machine (the NetShark) should be powered off before starting this task. Use the vSphere Client, ***Getting Started*** tab, ***Basic Tasks*** to power off the virtual machine (Refer to Step 1 below).

The preconfigured NetShark has only one hard disk, the operating system disk. It requires a second hard disk for packet storage.

1. Select the NetShark and click ***Edit virtual machine settings***.



What is a Virtual Machine?

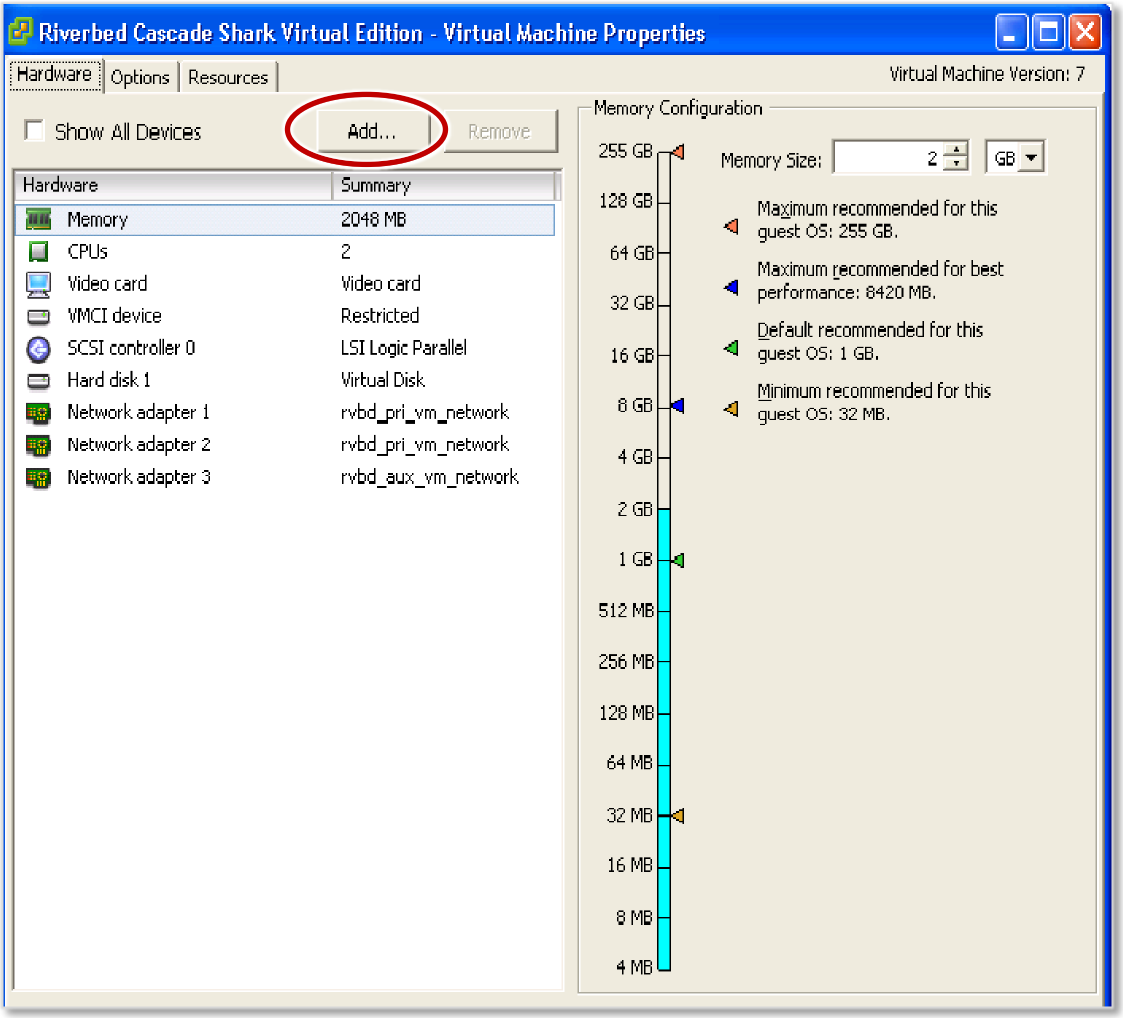
A virtual machine is a software computer that, like a physical computer, runs an operating system and applications. An operating system installed on a virtual machine is called a guest operating system.

Because every virtual machine is an isolated computing environment, you can use virtual machines as desktop or workstation environments, as testing environments, or to consolidate server applications.

Virtual machines run on hosts. The same host can run many virtual machines.

Basic Tasks

2. Click ***Add...*.**



Hardware	Summary
Memory	2048 MB
CPUs	2
Video card	Video card
VMCI device	Restricted
SCSI controller 0	LSI Logic Parallel
Hard disk 1	Virtual Disk
Network adapter 1	rvbd_pri_vm_network
Network adapter 2	rvbd_pri_vm_network
Network adapter 3	rvbd_aux_vm_network

Memory Size: 2 GB

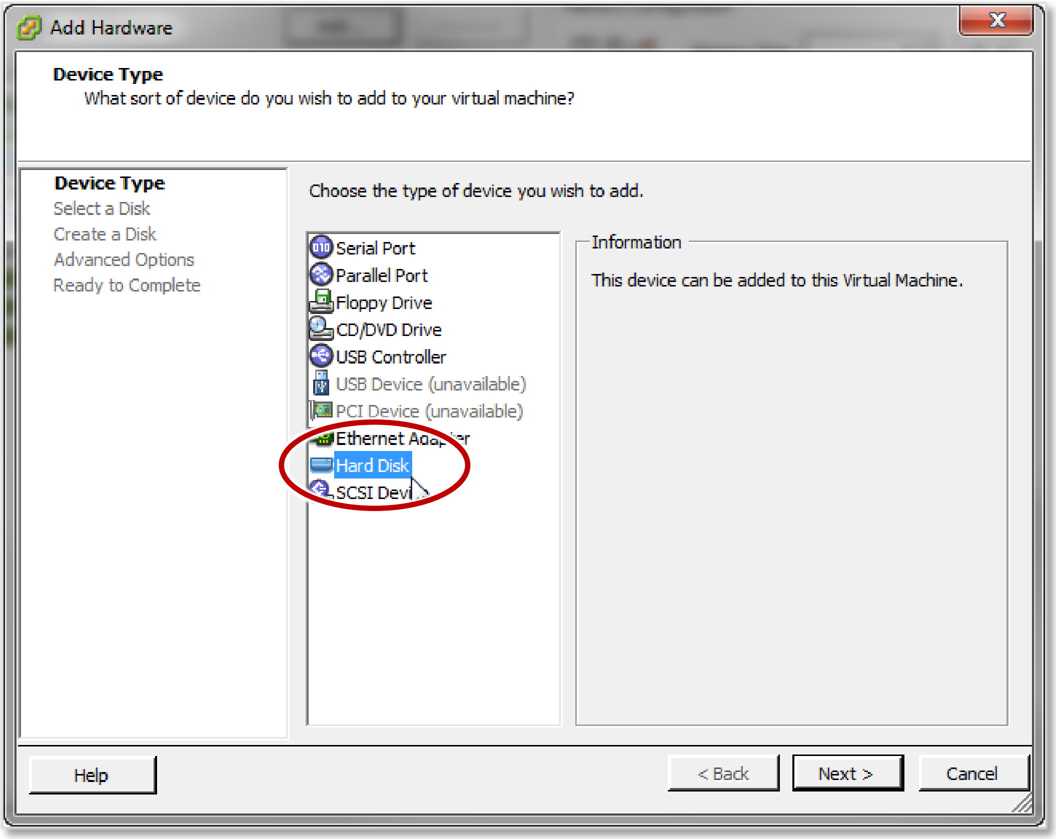
Maximum recommended for this guest OS: 255 GB.

Maximum recommended for best performance: 8420 MB.

Default recommended for this guest OS: 1 GB.

Minimum recommended for this guest OS: 32 MB.

3. On the ***Device Type*** page select ***Hard Disk***.



Add Hardware

Device Type

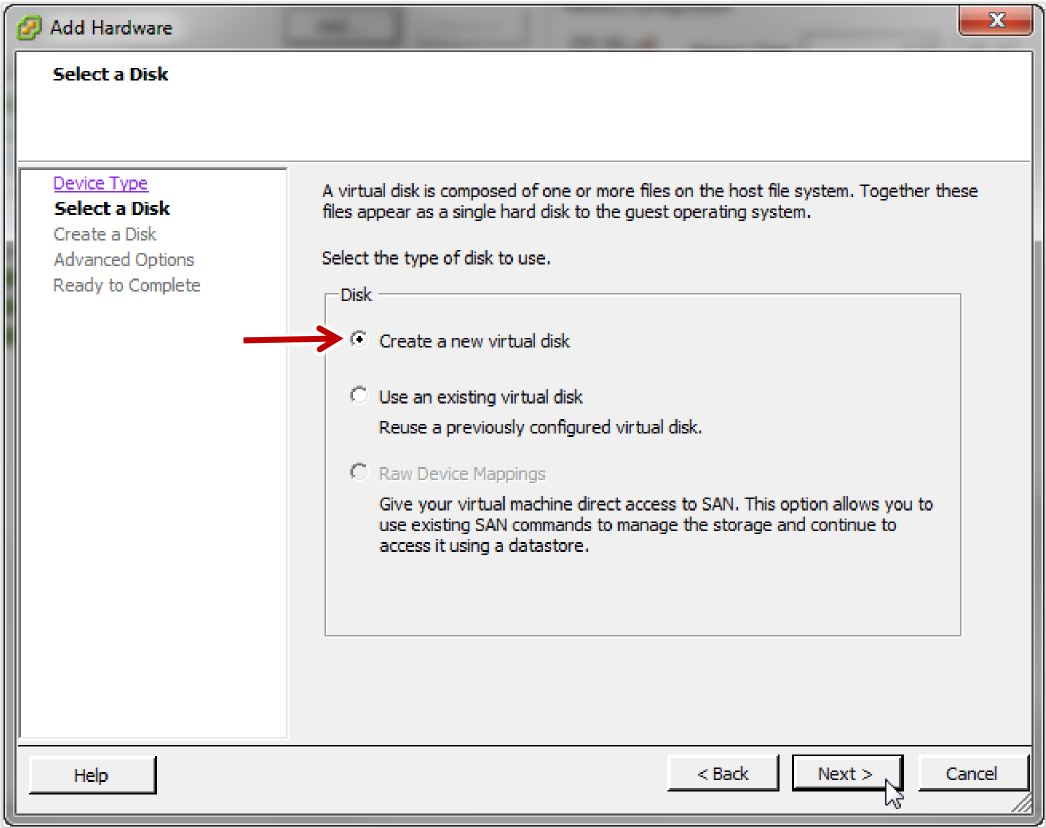
What sort of device do you wish to add to your virtual machine?

Choose the type of device you wish to add.

Information

This device can be added to this Virtual Machine.

4. On the ***Select a Disk*** page select ***Create a new virtual disk***.



Add Hardware

Select a Disk

A virtual disk is composed of one or more files on the host file system. Together these files appear as a single hard disk to the guest operating system.

Select the type of disk to use.

Disk

● Create a new virtual disk

○ Use an existing virtual disk

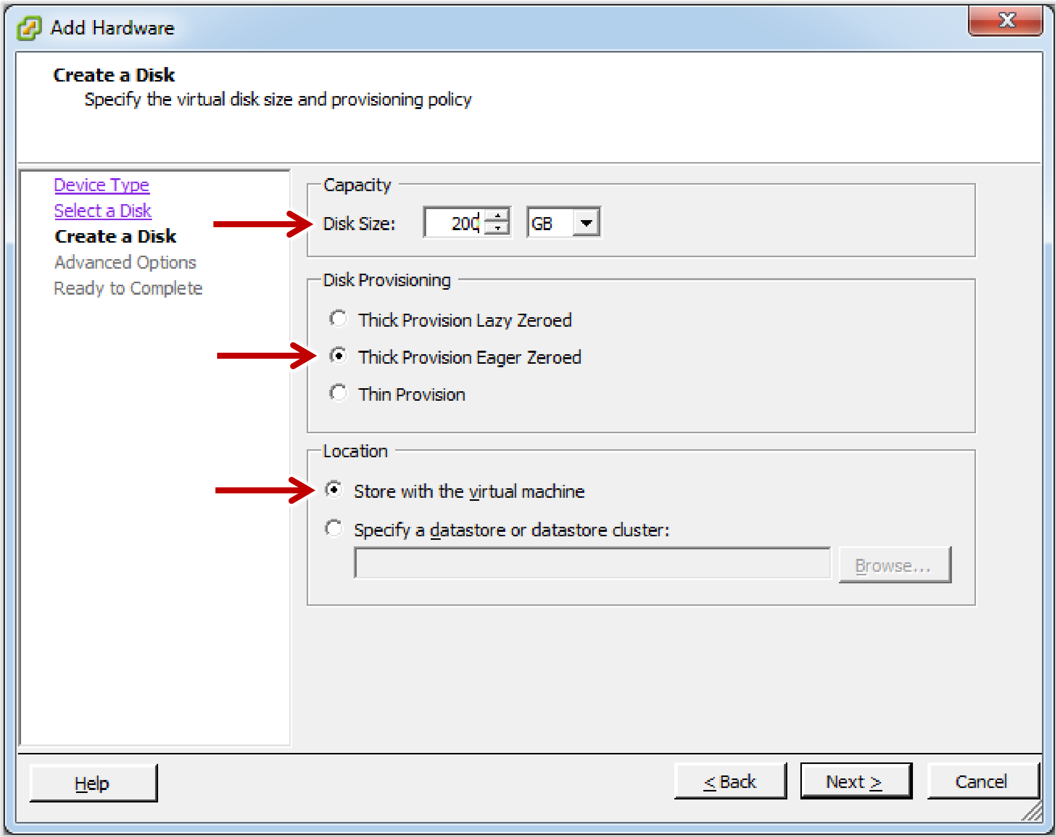
Reuse a previously configured virtual disk.

○ Raw Device Mappings

Give your virtual machine direct access to SAN. This option allows you to use existing SAN commands to manage the storage and continue to access it using a datastore.

5. On the ***Create a Disk*** page

   - Under ***Capacity***, enter a disk size for the packet storage disk.
     Note: The maximum disk size supported by ESXi 5.0 Patch 6 or ESXi 5.1 is 2 TB. Specify the disk size, up to the maximum size disk available (check with vSphere for available space).
   - Under ***Disk Provisioning***, select ***Thick Provision Eager Zeroed***.
   - Under ***Location***, select ***Store with the virtual machine***.



Add Hardware

Create a Disk

Specify the virtual disk size and provisioning policy

Capacity

Disk Size: 200 GB

Disk Provisioning

○ Thick Provision Lazy Zeroed

● Thick Provision Eager Zeroed

○ Thin Provision

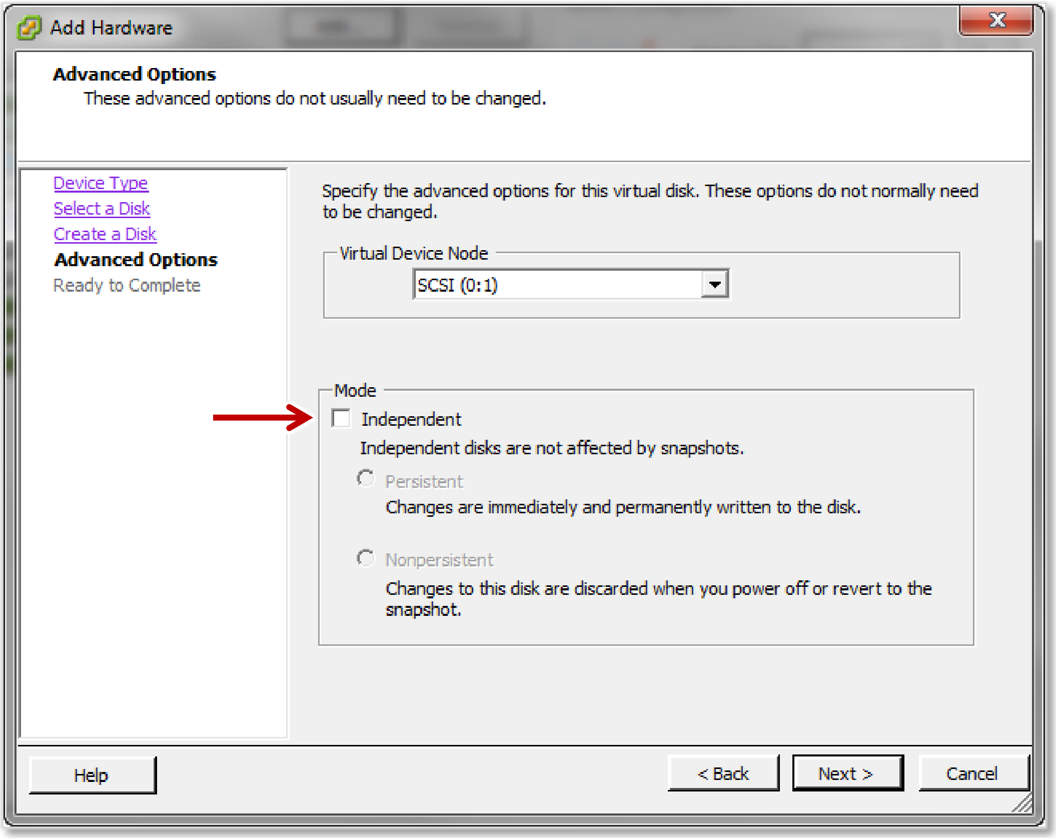
Location

● Store with the virtual machine

○ Specify a datastore or datastore cluster:

6. On the ***Advanced Options*** page, accept the default setting for ***Virtual Device Node***. Make sure that the ***Mode*** settings are the same as for the OS disk. By default, the OS disk is not set to independent mode.

   You can find the OS disk's mode settings as follows: From the vSphere Client main page select the NetShark; click the ***Getting Started*** tab; click ***Edit virtual machine settings***; and click the OS disk in the ***Hardware*** list—usually ***Hard disk 1***. The mode settings appear in the panel on the right.



Advanced Options

These advanced options do not usually need to be changed.

Specify the advanced options for this virtual disk. These options do not normally need to be changed.

Virtual Device Node

SCSI (0:1)

Mode

☐ Independent

Independent disks are not affected by snapshots.

○ Persistent

Changes are immediately and permanently written to the disk.

○ Nonpersistent

Changes to this disk are discarded when you power off or revert to the snapshot.

7. On the ***Ready to Complete*** page, click ***Finish*** to create the hard disk.
8. The ***Virtual Machine Properties*** page shows the new hard disk ready to be added. Click ***OK*** to add it.

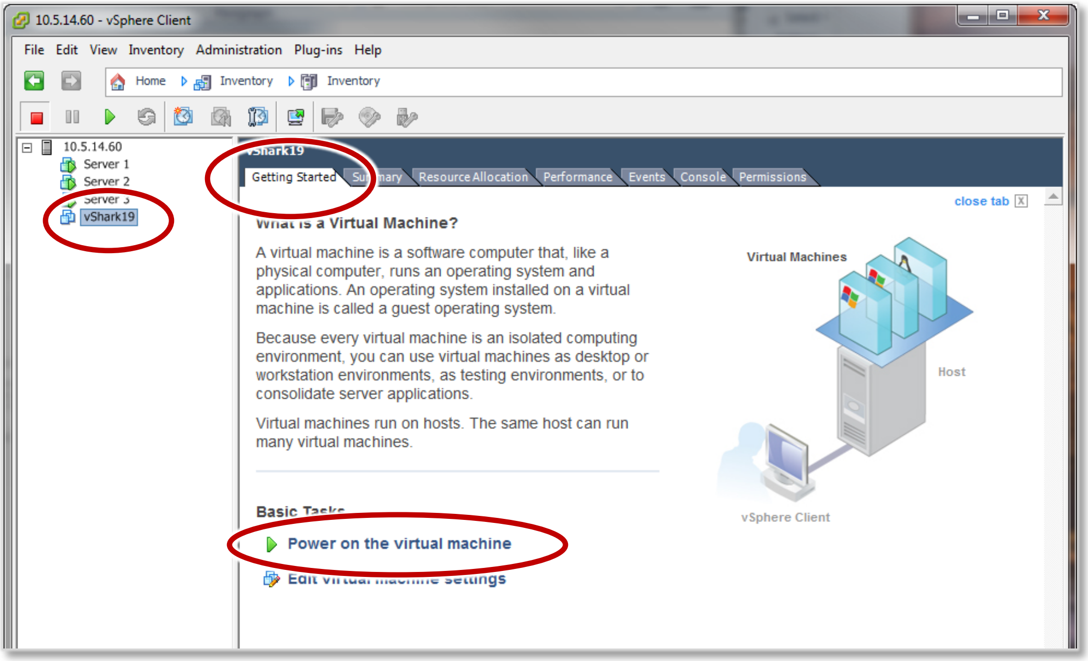
When you have added the hard disk and set up all your monitor ports, you are finished creating the NetShark. Continue with the next chapter to configure the NetShark.

3. Configuring the NetShark

Setting up the initial configuration

The initial configuration of a NetShark sets up its IP address, password, time configuration, and so on. You perform this configuration through the NetShark console port.

1. Power on the NetShark. Select the NetShark icon from the server's list of virtual machines and then click the ***Getting Started*** tab. Click ***Power on the virtual machine***.



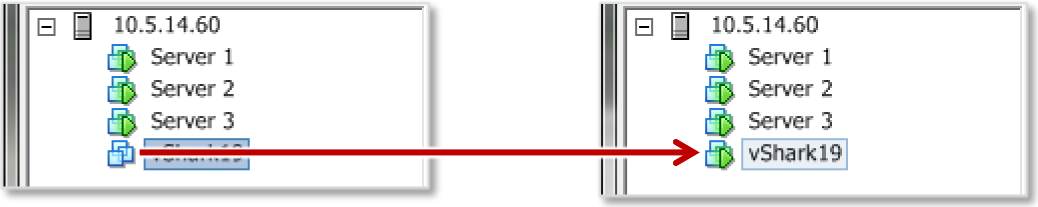
What is a Virtual Machine?

A virtual machine is a software computer that, like a physical computer, runs an operating system and applications. An operating system installed on a virtual machine is called a guest operating system.

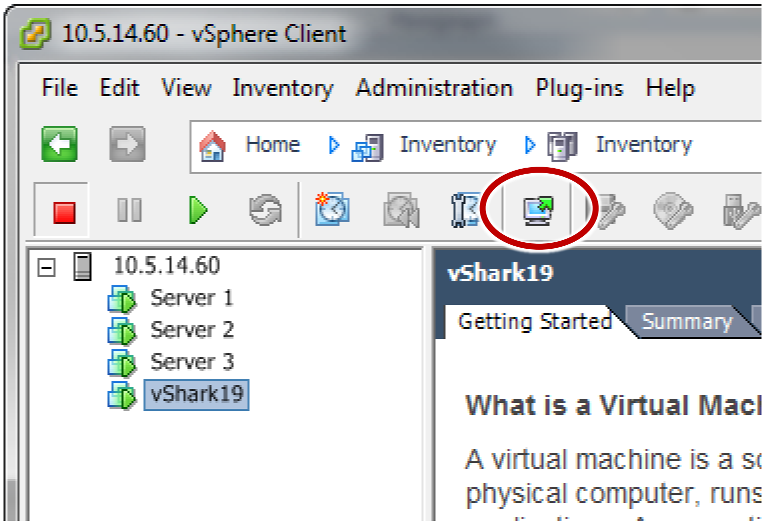
Because every virtual machine is an isolated computing environment, you can use virtual machines as desktop or workstation environments, as testing environments, or to consolidate server applications.

Virtual machines run on hosts. The same host can run many virtual machines.

The NetShark icon in the list of virtual machines adds a green arrowhead to indicate that the NetShark is powered on.



2. Click the console button to launch the NetShark console.



Note: If you lose the mouse cursor while working in the console interface, you can restore it by entering **`Ctrl+Alt`**.

3. At the **`login:`** prompt, enter the NetShark default username and password.

```
login: admin
password: admin
```

Note: You must always keep a record of the login password.

4. At the console prompt, enter **`wizard`** to start the initial configuration wizard, and answer the questions.

```
shark> wizard
```

The setup wizard guides you through the initial configuration of the NetShark. Press **`Enter`** at any step to accept the current setting and move to the next step. A typical configuration dialog might look like this:

```
Step 0: Hostname [shark]? vShark19

Step 1: Use DHCP for primary [yes]?

Step 5: Enable aux [no]?

Step 12: Timezone (type * for list) [America/Los_Angeles]? *

Africa/            America/           Antarctica/        Arctic/

Asia/              Atlantic/          Australia/         Etc/

Europe/            Indian/            Pacific/

Step 12: Timezone (type * for list) [America/Los_Angeles]? Australia/*

Adelaide           Brisbane           Broken_Hill        Currie

Darwin             Eucla              Hobart             Lindeman

Lord_Howe          Melbourne          Perth              Sydney

Step 12: Timezone (type * for list) [America/Los_Angeles]? Australia/Perth

Step 13: Enable SSH [yes]? yes

Step 14: Enable PTP [yes]?
Step 15: PTP Interface [primary]?

Step 16: NTP server names [0.riverbed.pool.ntp.org,1.riverbed.pool.ntp.org,
2.riverbed.pool.ntp.org,3.riverbed.pool.ntp.org]?
```

The purposes of the steps in the setup wizard are as follows:

Step 0 sets the hostname (without the domain). This name will be used as the console prompt, and will identify the appliance in the NetShark Web user interface.

Steps 1 through 4 configure the IP management network. Enter **`yes`** in Step 1 to use DHCP for the **primary** management port or **`no`** to use a static IP configuration, and press Enter. For a static IP configuration, use Step 2 to specify the IP address, Step 3 to specify the IP net mask, and Step 4 to specify the default gateway.

Step 5 selects whether to use the second management port (**aux**). Note that in a standard installation **aux** is not needed. Enter **`yes`** to enable **aux**. If **aux** is enabled, Steps 6 through 9 configure **aux** for either DHCP or a static IP configuration.

Steps 10 and 11 configure the DNS servers (as a comma- or space-separated list) and the domain name of the NetShark. If DHCP is used for the **primary** management network configuration, these steps are skipped (because they are configured by the DHCP server).

Step 12 sets the time zone of the NetShark. Entering an asterisk **`*`** lists the available time zone areas. To list the specific time zones within an area (for example, Europe), enter the area followed by **`/*`**. To specify a particular time zone, enter the full time zone including the area (for example, **`Europe/Rome`**). Use **`Etc/*`** to specify GMT time.

Step 13 enables or disables the remote shell (SSH). It is enabled by default.

Steps 14 and 15 select and configure the use of Precision Time Protocol (PTP) in version 10.6 or later of the software.

Step 16 defines the NTP server(s) used for clock synchronization. Enter one or more NTP server names or IP addresses, separated by commas or spaces.

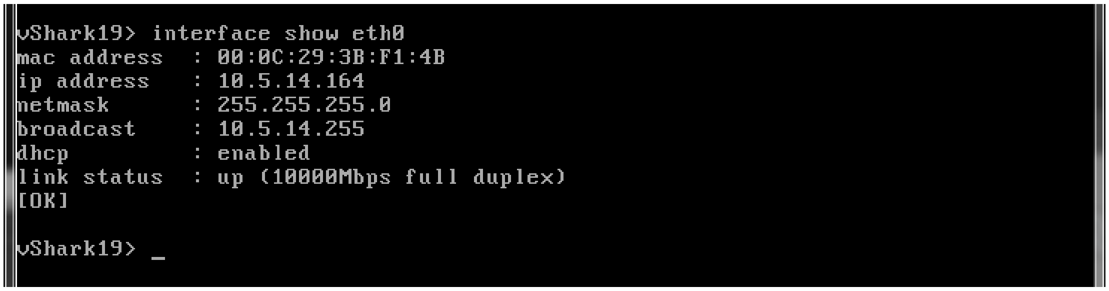
At the end of the configuration, the wizard prints out a summary of the parameters. Each step can be revisited by entering the step number. Entering an “s” saves the configuration, and entering a “c” cancels it.

```
To change an answer, enter the step number to return to.

Type 's' to save changes and exit

Type 'c' to exit without saving changes
```

5. Once the configuration is complete, enter **`s`** to save the configuration and exit.

   Note: A change to the host name, IP address, or time zone requires a reboot in order to take effect. The wizard asks for confirmation before rebooting the NetShark. If you changed the name (the hostname entry in step 0) the new name appears in the console prompt.

6. If you have used DHCP to provision an IP address for your NetShark, at the console prompt enter **`interface show primary`** to find the IP address.



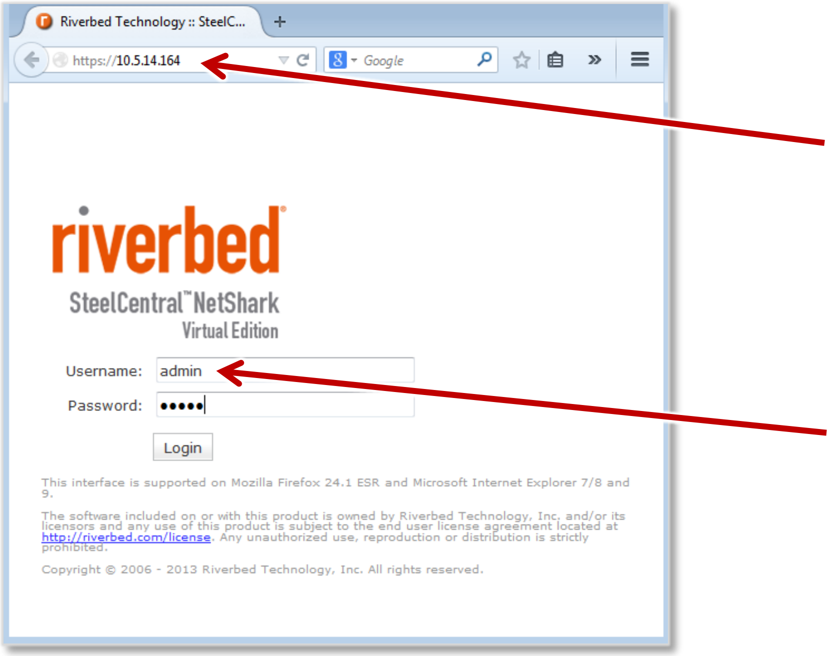
```
vShark19> interface show eth0
mac address   : 00:0C:29:3B:F1:4B
ip address    : 10.5.14.164
netmask       : 255.255.255.0
broadcast     : 10.5.14.255
dhcp          : enabled
link status   : up (10000Mbps full duplex)
[OK]

vShark19> _
```

Record this address (or the DNS name of the NetShark) to use to connect to the web user interface for subsequent configuration and operation of the NetShark.

Logging in to the web user interface

The web user interface (web interface) is a primary means of access to the NetShark. You use it for further configuration of the NetShark, as well as for normal operation.

Connect to the NetShark through its web user interface. You can do this using your web browser. The NetShark web interface is supported on Mozilla Firefox 24.1 ESR and Microsoft Internet Explorer 7/8 and 9. Make sure that SSL, cookies, and JavaScript are enabled in your browser.



Username: admin

Password: •••••

Login

This interface is supported on Mozilla Firefox 24.1 ESR and Microsoft Internet Explorer 7/8 and 9.

The software included on or with this product is owned by Riverbed Technology, Inc. and/or its licensors and any use of this product is subject to the end user license agreement located at http://riverbed.com/license. Any unauthorized use, reproduction or distribution is strictly prohibited.

Copyright © 2006 - 2013 Riverbed Technology, Inc. All rights reserved.

1) Point your browser at

https://<NetShark>

where <NetShark> is the IP address or DNS name of the NetShark.

2) Enter username and password, then click the Login button. (Default value is "admin" for both username and password.)

When you log in, the web user interface displays the ***Status*** page.

Applying licenses

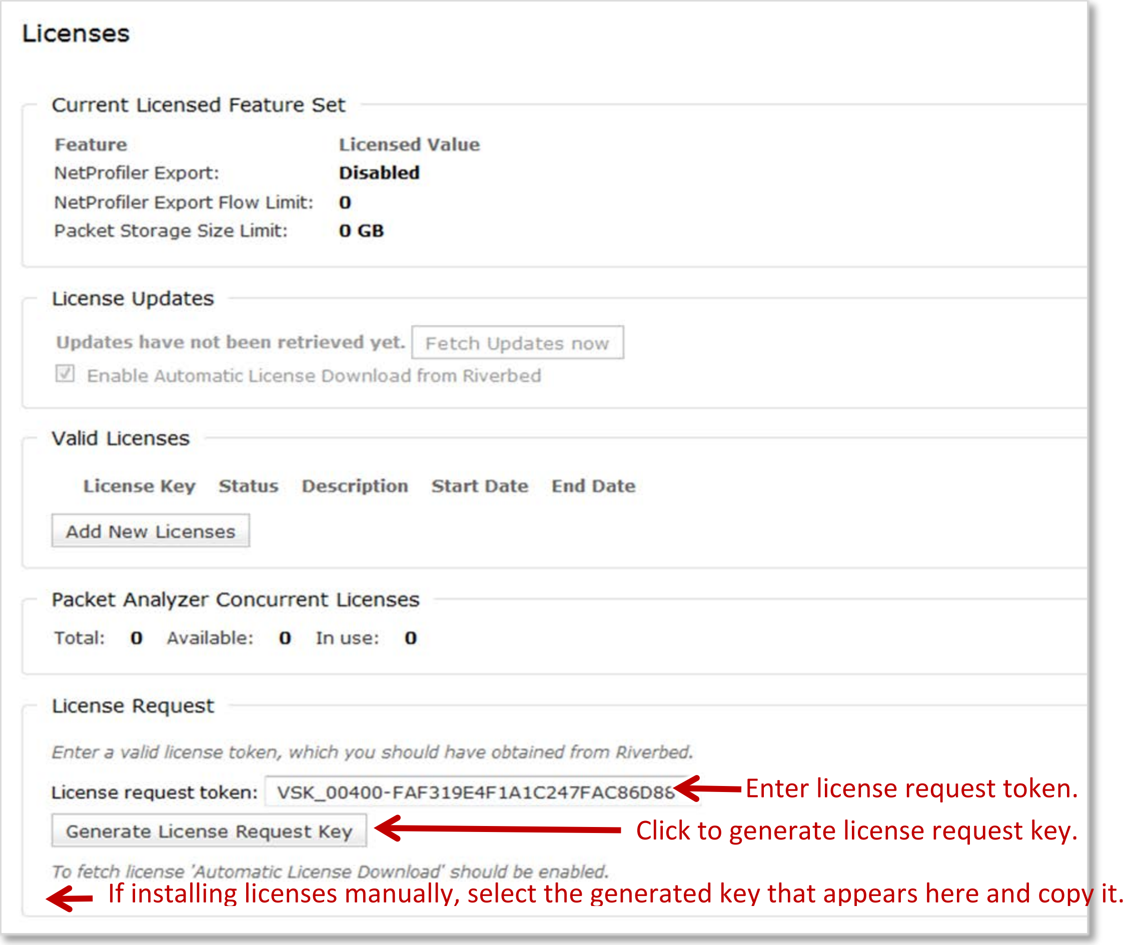
To use packet storage and other NetShark features on a NetShark you must apply licenses. You received a license request token when you purchased your NetShark. NetShark uses this token to obtain license keys from the Riverbed licensing Web site.

If the NetShark has been configured to be accessible on the network and if it has access to the Internet, auto-licensing is used to automatically download and update the license key(s). Otherwise, you can manually license your NetShark using the Riverbed licensing Web site.

1. Log in to the NetShark Web user interface.

2. Navigate to the System->Licenses page.

3. Paste or enter your license request token in the License Request section and click Generate License Request Key. The NetShark generates a license request key and displays it at the bottom of the page.



Licenses

Current Licensed Feature Set

Feature	Licensed Value
NetProfiler Export:	**Disabled**
NetProfiler Export Flow Limit:	**0**
Packet Storage Size Limit:	**0 GB**

License Updates

Updates have not been retrieved yet. Fetch Updates now

☑ Enable Automatic License Download from Riverbed

Valid Licenses

License Key	Status	Description	Start Date	End Date

Add New Licenses

Packet Analyzer Concurrent Licenses

Total: **0** Available: **0** In use: **0**

License Request

Enter a valid license token, which you should have obtained from Riverbed.

License request token: VSK_00400-FAF319E4F1A1C247FAC86D86

Generate License Request Key

To fetch license 'Automatic License Download' should be enabled.

Enter license request token.

Click to generate license request key.

If installing licenses manually, select the generated key that appears here and copy it.

If the NetShark has access to the Internet, licenses are automatically downloaded and installed.

The NetShark must be restarted to activate a license. A message in the upper right corner of the Licenses page allows you to restart or delay the restart of the NetShark to install licenses. Installed licenses are listed in the Valid Licenses section of the Licensing page.

If **Enable Automatic License Download from Riverbed** is enabled (the default after the first license is applied), the NetShark automatically connects to the Riverbed licensing Web site every 12 hours and downloads licenses that you have purchased. Uncheck the box to disable automatic retrieval of license updates.

The **Fetch Updates Now** button causes the NetShark to immediately connect to the Riverbed licensing Web site and download any new licenses that you have purchased.

If the NetExpress does not have Internet connectivity, you can install licenses manually.

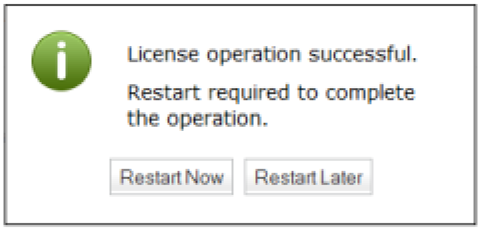
1. Copy the license request key displayed it at the bottom of the page.

2. Point your browser at the Riverbed licensing Web site, https://licensing.riverbed.com, and follow the process found there.

3. The licensing portal returns several license keys. You will copy those keys to the Licenses page.

4. On the **Licenses** page, click **Add Licenses**, then copy and paste the license keys into the window, one line per key. Click **Add** to add the keys to the NetShark**.**

5. When the keys have been added, the NetShark returns a completion message. Click ***Restart Now*** to restart the NetShark probe service.



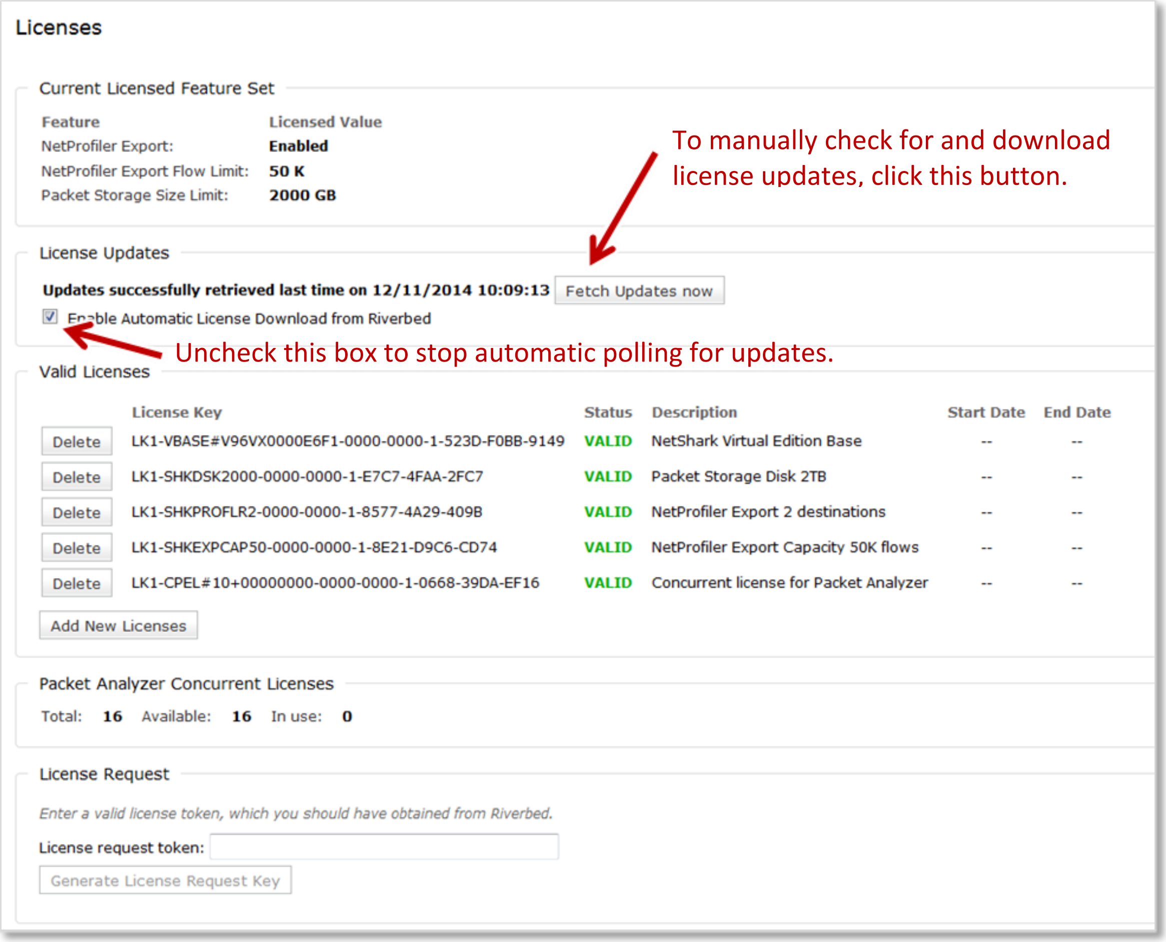
License operation successful.

Restart required to complete the operation.

6. After the NetShark probe service is restarted, the NetShark is fully licensed.

Note: If you purchase and download a license for a higher capacity than a current license, the NetShark uses the license with the higher capacity.

When licensing is completed all installed licenses are listed under Valid Licenses. Remove a license by clicking the **Delete** button next to its licensing key. If a NetShark is connected to the Web it can automatically or manually check for license updates



Licenses

Current Licensed Feature Set

Feature	Licensed Value
NetProfiler Export:	**Enabled**
NetProfiler Export Flow Limit:	**50 K**
Packet Storage Size Limit:	**2000 GB**

To manually check for and download license updates, click this button.

License Updates

Updates successfully retrieved last time on 12/11/2014 10:09:13 Fetch Updates now

☑ Enable Automatic License Download from Riverbed

Uncheck this box to stop automatic polling for updates.

Valid Licenses

	License Key	Status	Description	Start Date	End Date
Delete	LK1-VBASE#V96VX0000E6F1-0000-0000-1-523D-F0BB-9149	**VALID**	NetShark Virtual Edition Base	--	--
Delete	LK1-SHKDSK2000-0000-0000-1-E7C7-4FAA-2FC7	**VALID**	Packet Storage Disk 2TB	--	--
Delete	LK1-SHKPROFLR2-0000-0000-1-8577-4A29-409B	**VALID**	NetProfiler Export 2 destinations	--	--
Delete	LK1-SHKEXPCAP50-0000-0000-1-8E21-D9C6-CD74	**VALID**	NetProfiler Export Capacity 50K flows	--	--
Delete	LK1-CPEL#10+00000000-0000-0000-1-0668-39DA-EF16	**VALID**	Concurrent license for Packet Analyzer	--	--

Add New Licenses

Packet Analyzer Concurrent Licenses

Total: **16** Available: **16** In use: **0**

License Request

Enter a valid license token, which you should have obtained from Riverbed.

License request token:

Generate License Request Key

Additional Configuration

For operational configuration and use, including setting up capture ports and setting up communication with Riverbed® SteelCentral™ NetProfiler, refer to the *SteelCentral NetShark User's Guide* or the *SteelCentral Packet Analyzer Reference Manual*.

4. Beyond the basics

Adding a monitor port

You can have up to four monitor ports in a NetShark. The first monitor port is configured as part of the initial deployment of the NetShark. You can configure additional monitor ports after the initial deployment by following the procedure given below.

In most cases you would not put multiple monitor ports on the same virtual switch; thus, the first step in the procedure is to create a new virtual switch. You might, however, make an exception to this practice if the ports are part of port groups on separate VLANS.

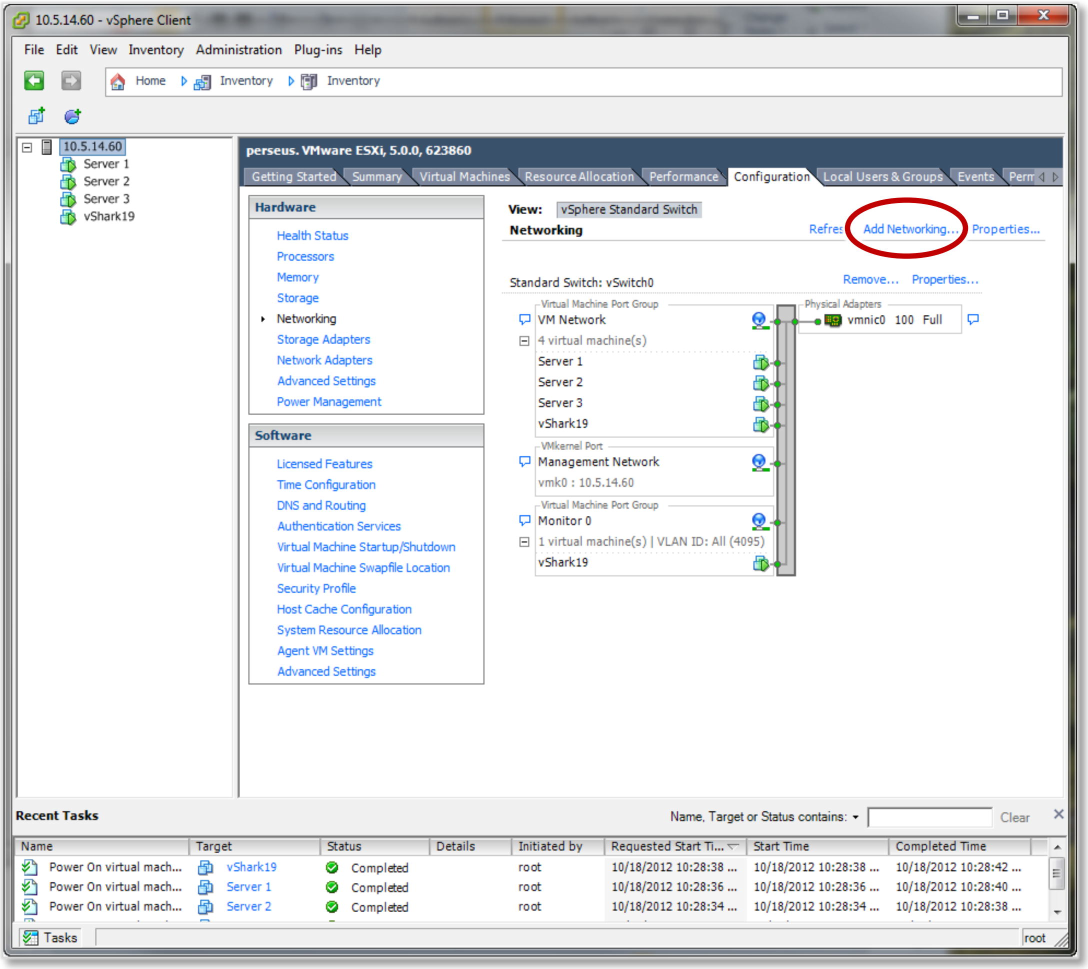
In general, though, the procedure for adding a monitor port contains these steps:

- Create a new virtual switch and port group.
- Set the new port group to promiscuous mode.
- Create a new monitor port in the new port group.

The rest of this section provides the detailed procedure.

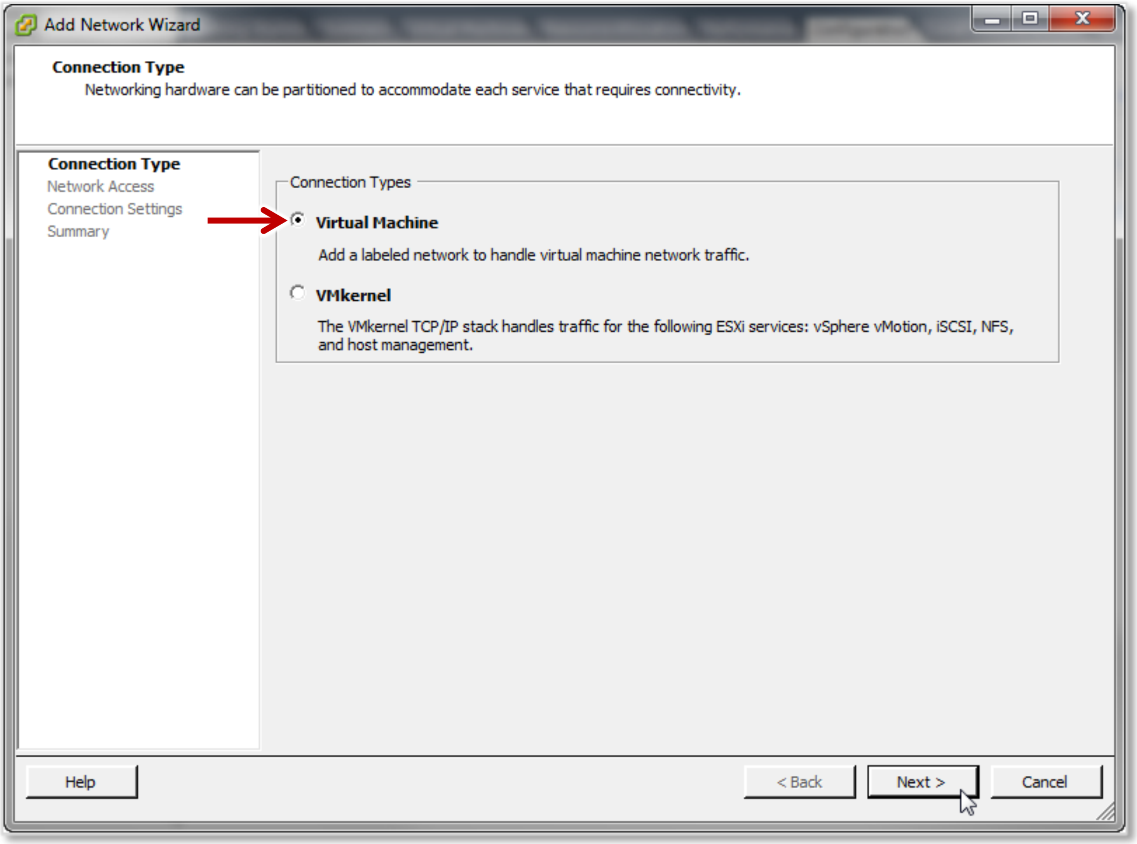
Create a new virtual switch and port group

1. On the ESXi server's networking configuration page, click ***Add Networking…***.



Name	Target	Status	Details	Initiated by	Requested Start Ti...	Start Time	Completed Time
Power On virtual mach...	vShark19	Completed		root	10/18/2012 10:28:38 ...	10/18/2012 10:28:38 ...	10/18/2012 10:28:42 ...
Power On virtual mach...	Server 1	Completed		root	10/18/2012 10:28:36 ...	10/18/2012 10:28:36 ...	10/18/2012 10:28:40 ...
Power On virtual mach...	Server 2	Completed		root	10/18/2012 10:28:34 ...	10/18/2012 10:28:34 ...	10/18/2012 10:28:38 ...

2. Select ***Virtual Machine*** as the connection type.



Add Network Wizard

Connection Type

Networking hardware can be partitioned to accommodate each service that requires connectivity.

Connection Types

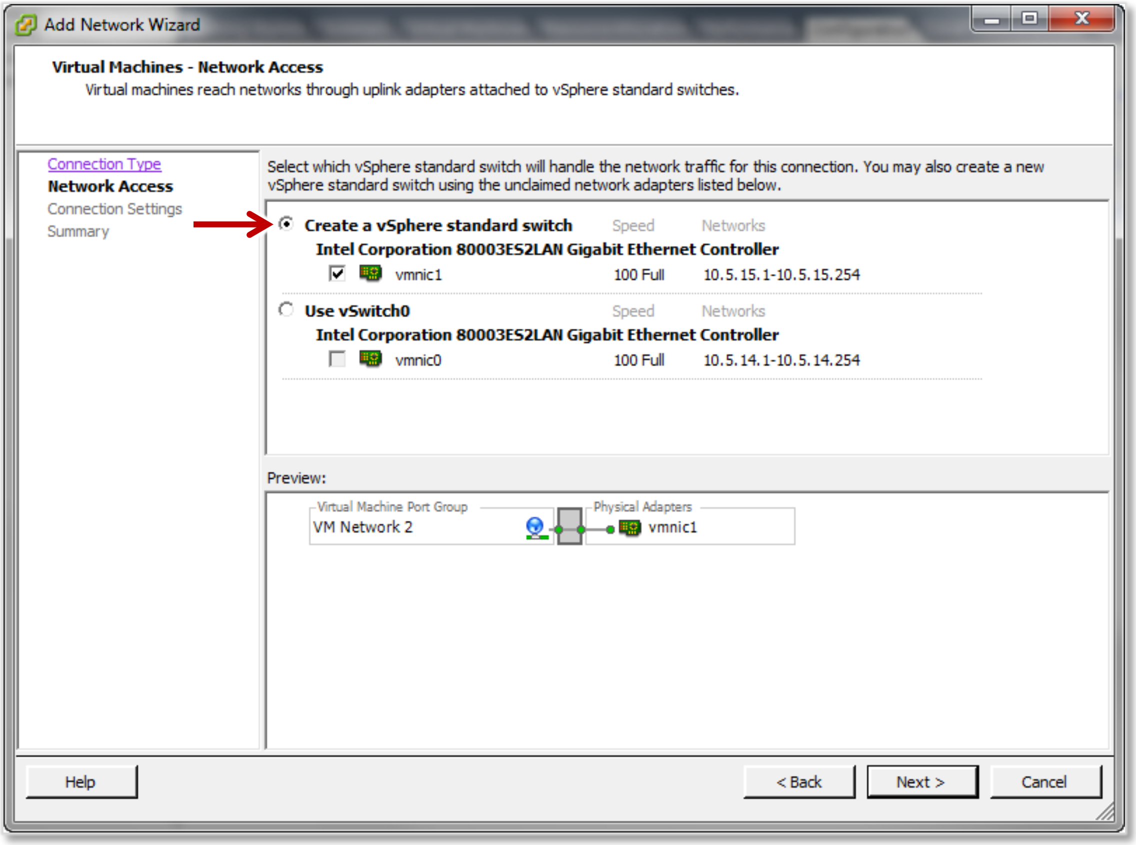
● **Virtual Machine**

Add a labeled network to handle virtual machine network traffic.

○ **VMkernel**

The VMkernel TCP/IP stack handles traffic for the following ESXi services: vSphere vMotion, iSCSI, NFS, and host management.

3. Select ***Create a vSphere standard switch***. The ***Preview*** pane at the bottom of the screen shows what the arrangement of port groups on the switch will be.



Add Network Wizard

Virtual Machines - Network Access

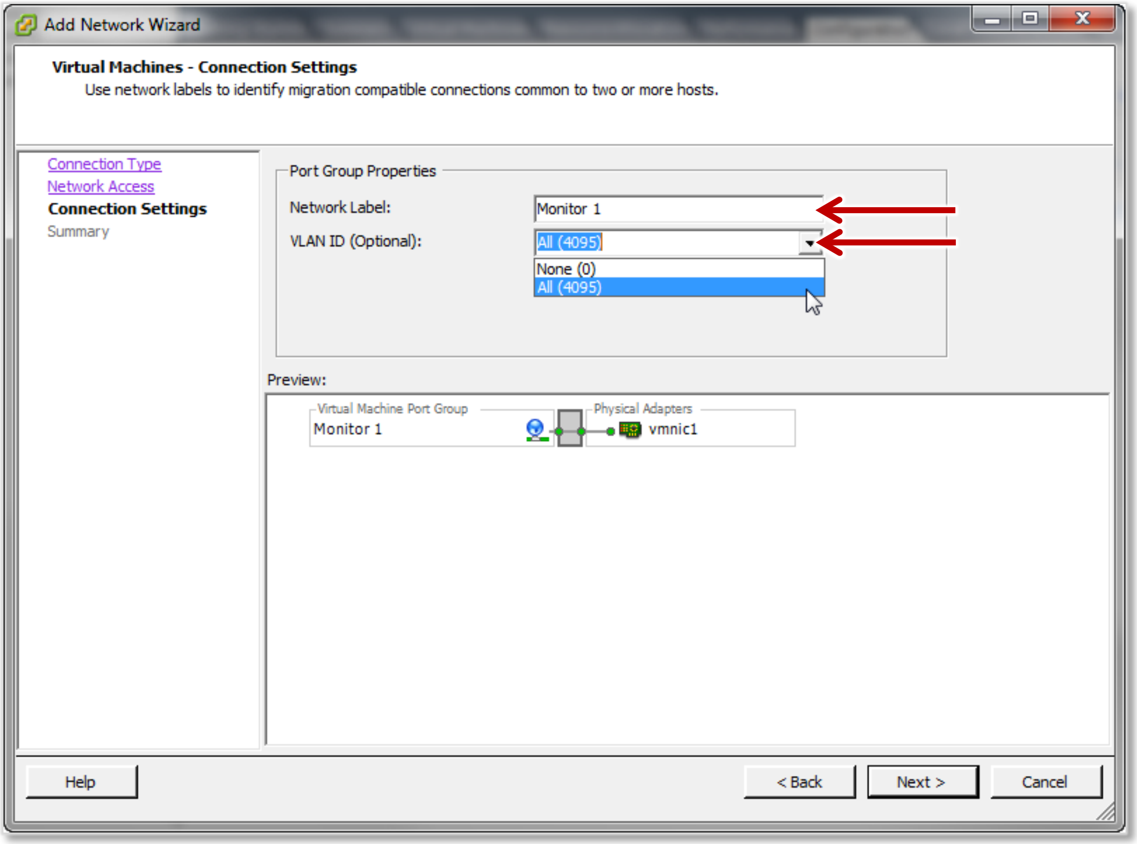
Virtual machines reach networks through uplink adapters attached to vSphere standard switches.

Select which vSphere standard switch will handle the network traffic for this connection. You may also create a new vSphere standard switch using the unclaimed network adapters listed below.

	Speed	Networks
● **Create a vSphere standard switch**		
Intel Corporation 80003ES2LAN Gigabit Ethernet Controller		
☑ vmnic1	100 Full	10.5.15.1-10.5.15.254
○ **Use vSwitch0**		
Intel Corporation 80003ES2LAN Gigabit Ethernet Controller		
□ vmnic0	100 Full	10.5.14.1-10.5.14.254

Preview:

4. Enter a name for the port group in the ***Network Label*** field. Select a ***VLAN ID*** of ***All (4095)***. This allows the port group to see all tagged and untagged traffic on the switch.



Add Network Wizard

Virtual Machines - Connection Settings

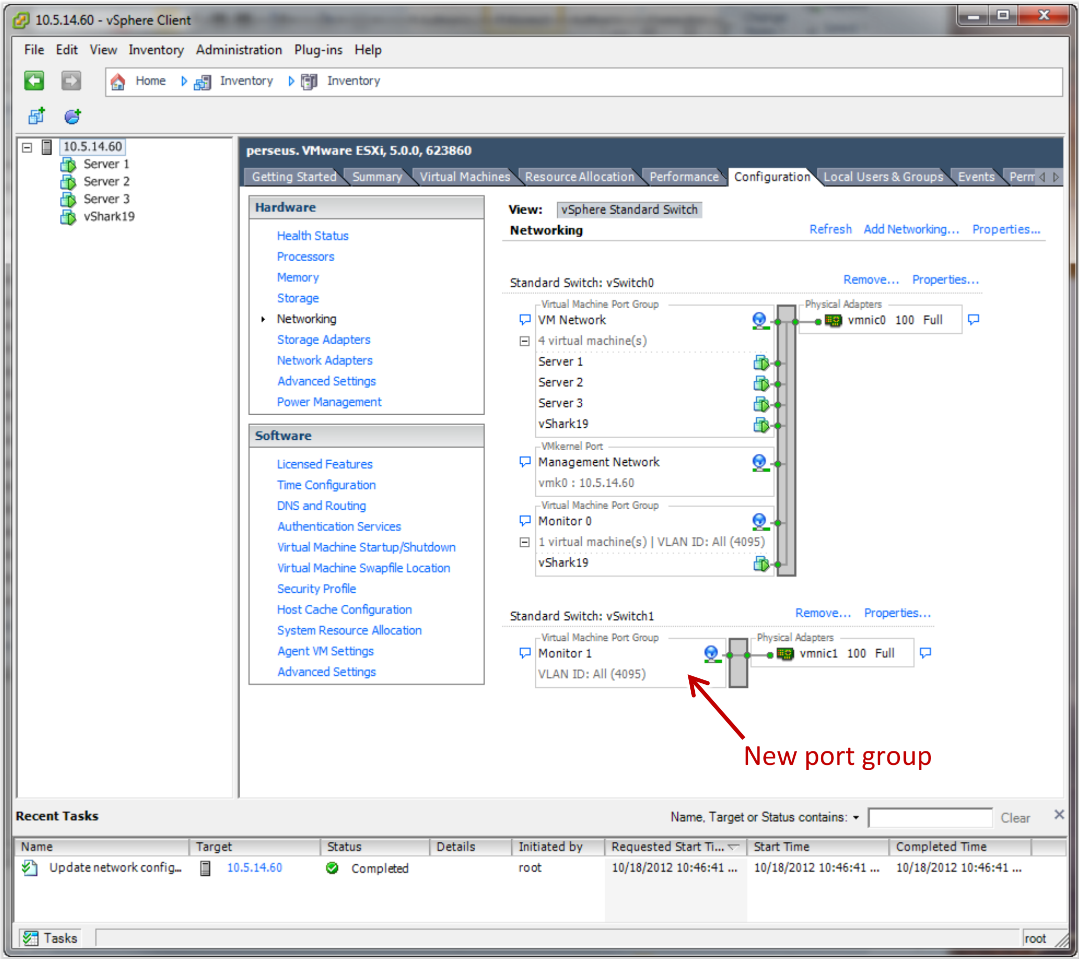
Use network labels to identify migration compatible connections common to two or more hosts.

Port Group Properties

Network Label: Monitor 1

VLAN ID (Optional): All (4095)

5. On the ***Ready to Complete*** page click ***Finish***. The new port group is configured on vSwitch1 and the configuration looks like this:



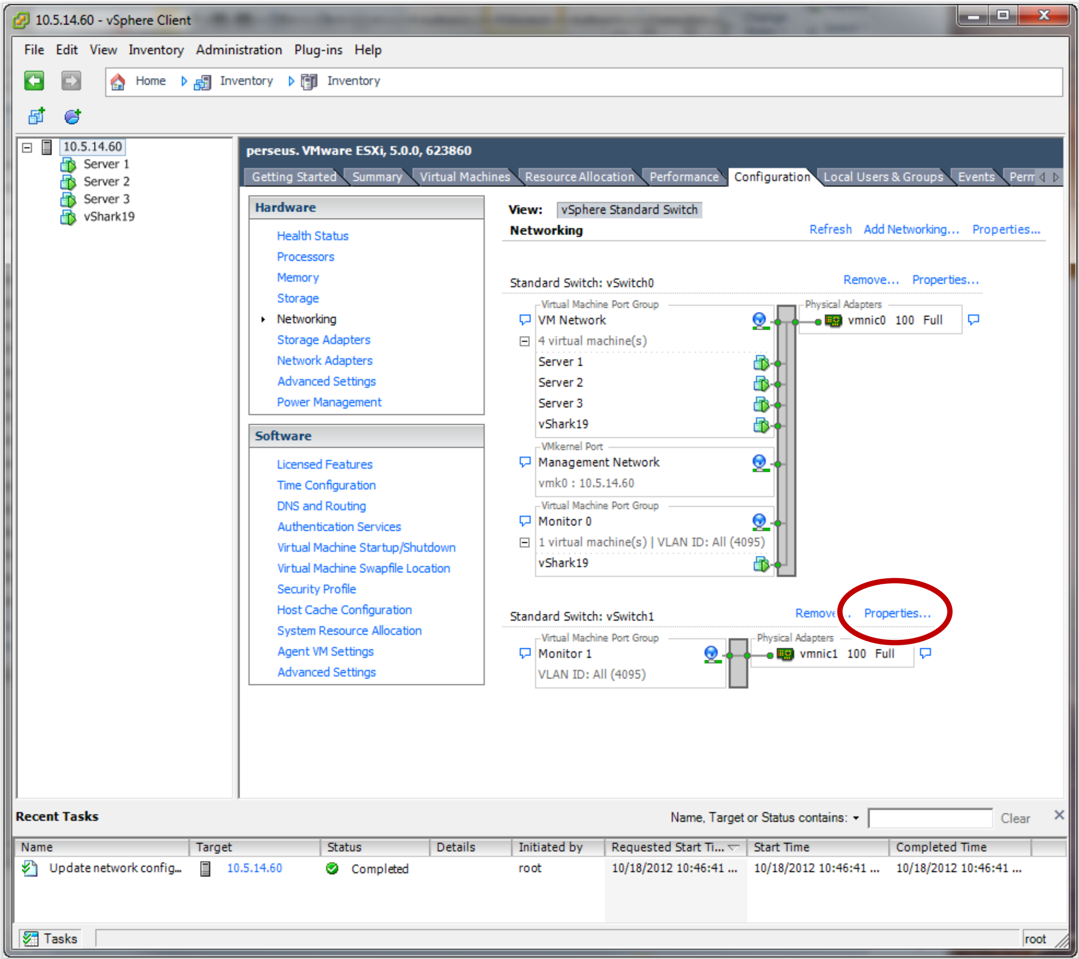
New port group

Name	Target	Status	Details	Initiated by	Requested Start Ti...	Start Time	Completed Time
Update network config...	10.5.14.60	Completed		root	10/18/2012 10:46:41 ...	10/18/2012 10:46:41 ...	10/18/2012 10:46:41 ...

Set the new port group to promiscuous mode

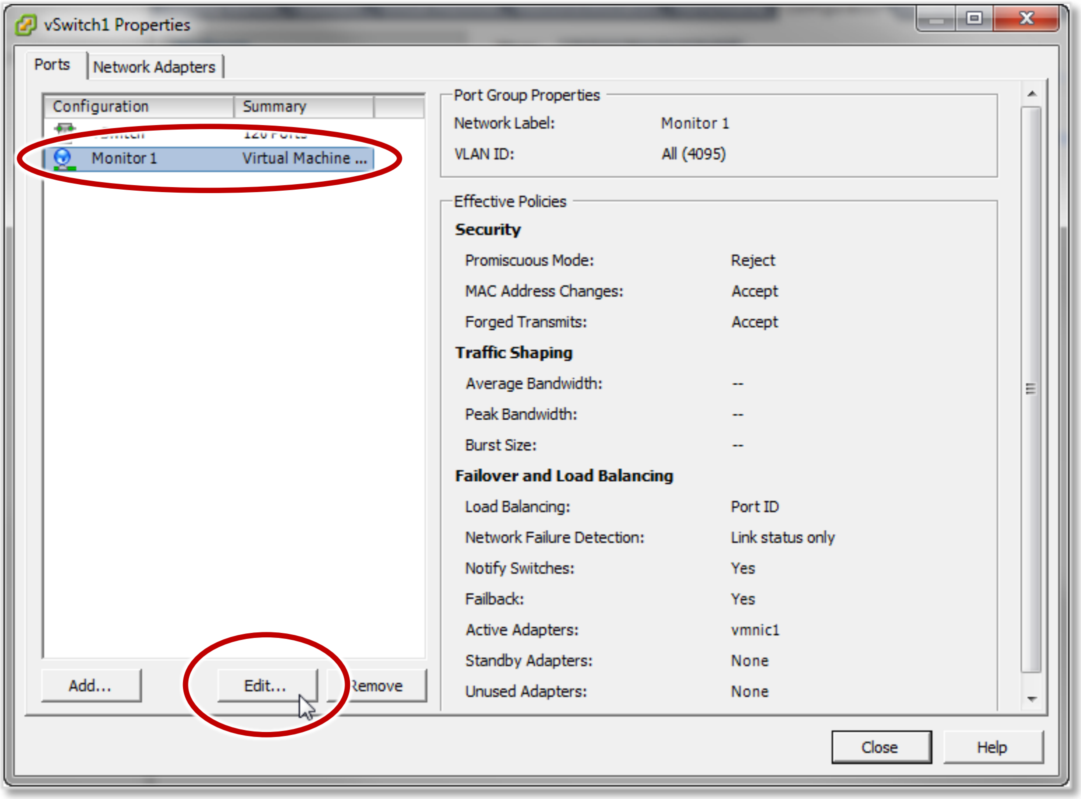
Set the new port group, Monitor1, to promiscuous mode.

1. In the networking configuration page, click the ***Properties…*** link for vSwitch1.



Name	Target	Status	Details	Initiated by	Requested Start Ti...	Start Time	Completed Time
Update network config...	10.5.14.60	Completed		root	10/18/2012 10:46:41 ...	10/18/2012 10:46:41 ...	10/18/2012 10:46:41 ...

2. Select the ***Monitor1*** port group and click the ***Edit…*** button.



Configuration	Summary
vSwitch	120 Ports
Monitor 1	Virtual Machine ...

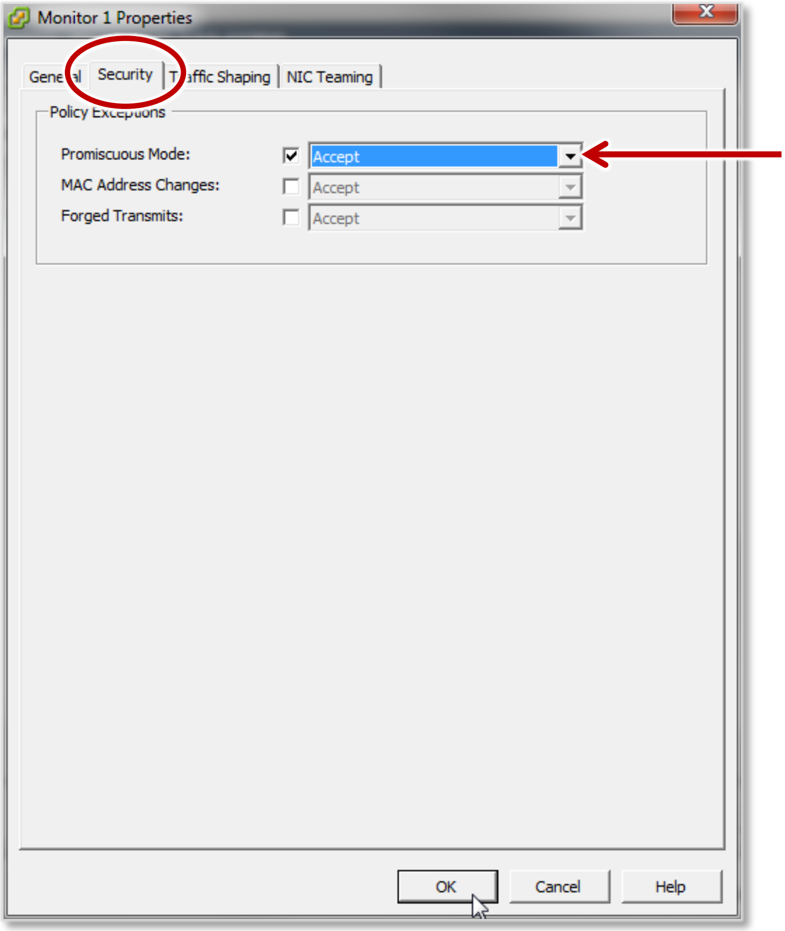
Port Group Properties

Network Label:	Monitor 1
VLAN ID:	All (4095)

Effective Policies

Security	
Promiscuous Mode:	Reject
MAC Address Changes:	Accept
Forged Transmits:	Accept
Traffic Shaping	
Average Bandwidth:	--
Peak Bandwidth:	--
Burst Size:	--
Failover and Load Balancing	
Load Balancing:	Port ID
Network Failure Detection:	Link status only
Notify Switches:	Yes
Failback:	Yes
Active Adapters:	vmnic1
Standby Adapters:	None
Unused Adapters:	None

3. Click the ***Security*** tab, check the ***Promiscuous Mode*** check box, and select a value of ***Accept***. Click ***OK***.

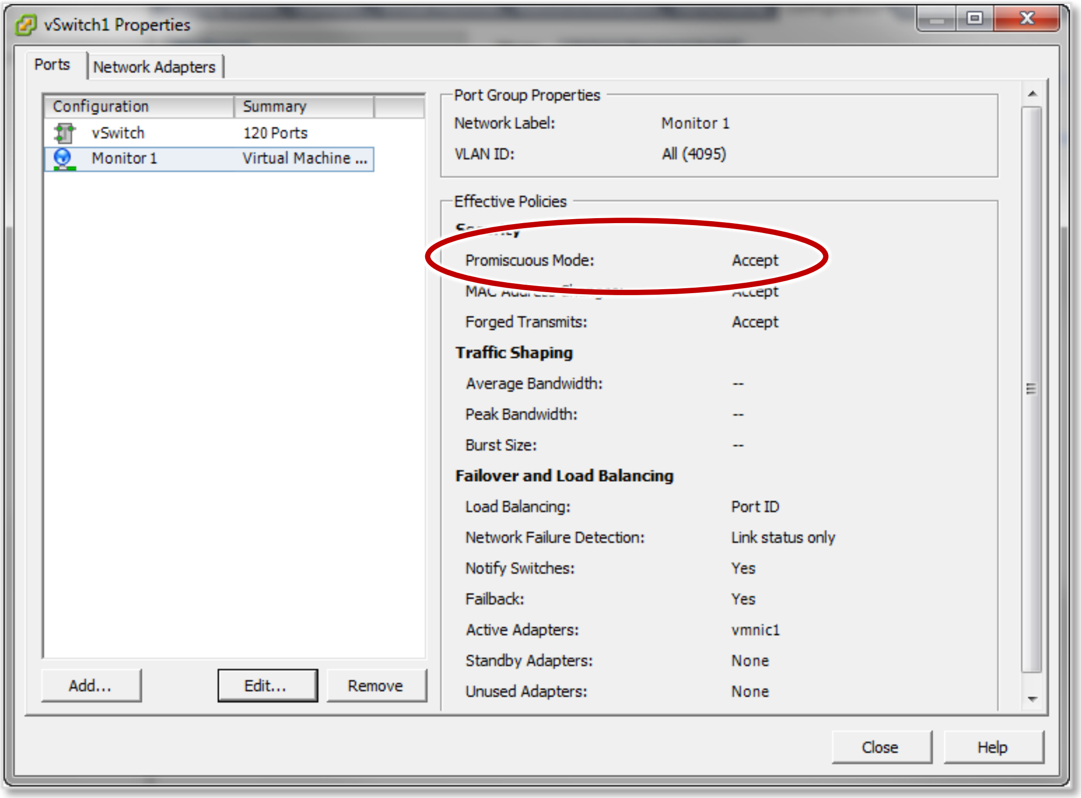


Promiscuous Mode: ☑ Accept

MAC Address Changes: □ Accept

Forged Transmits: □ Accept

4. Verify that ***Promiscuous Mode*** for the Monitor1 port group is set to ***Accept***. Then click ***Close***.



Configuration	Summary
vSwitch	120 Ports
Monitor 1	Virtual Machine ...

Port Group Properties

Network Label:	Monitor 1
VLAN ID:	All (4095)

Effective Policies

Security

Promiscuous Mode:	Accept
MAC Address Changes:	Accept
Forged Transmits:	Accept

Traffic Shaping

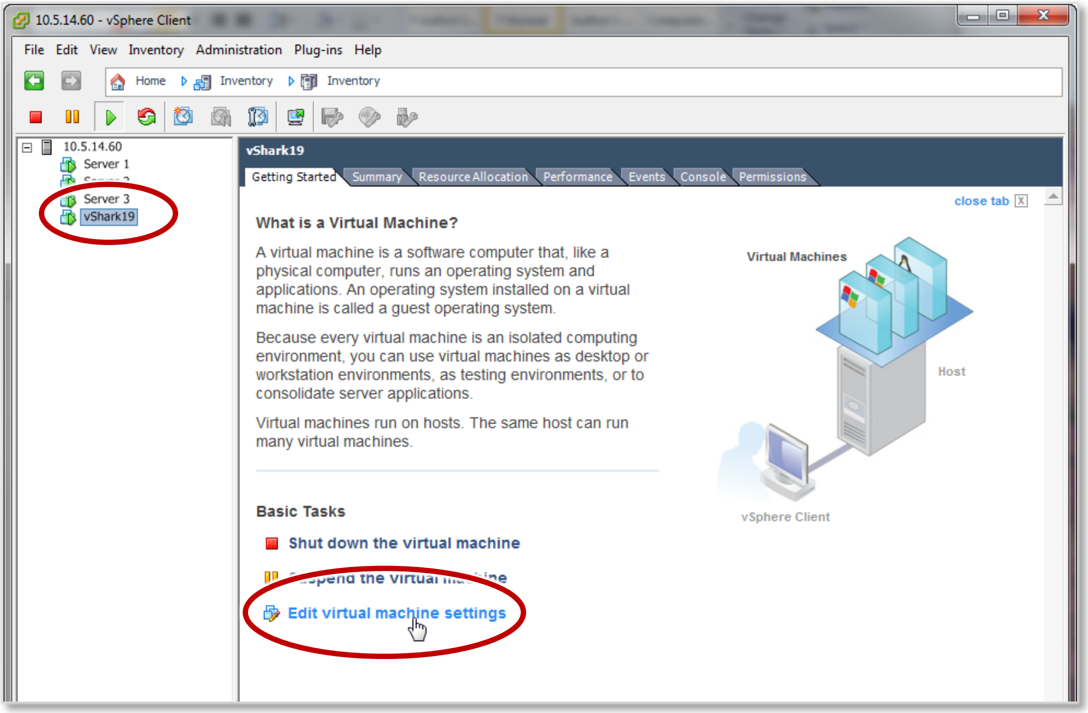
Average Bandwidth:	--
Peak Bandwidth:	--
Burst Size:	--

Failover and Load Balancing

Load Balancing:	Port ID
Network Failure Detection:	Link status only
Notify Switches:	Yes
Failback:	Yes
Active Adapters:	vmnic1
Standby Adapters:	None
Unused Adapters:	None

Create a new monitor port in the new port group

1. Select the NetShark and click ***Edit virtual machine settings***.



What is a Virtual Machine?

A virtual machine is a software computer that, like a physical computer, runs an operating system and applications. An operating system installed on a virtual machine is called a guest operating system.

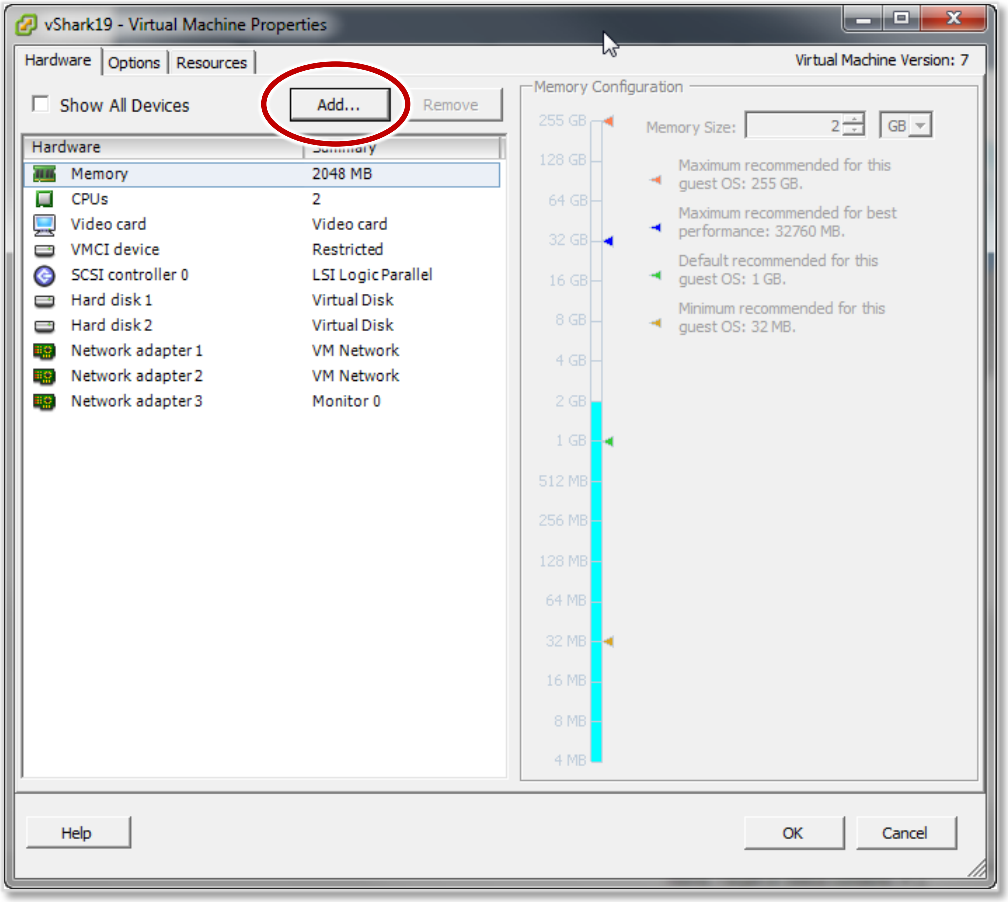
Because every virtual machine is an isolated computing environment, you can use virtual machines as desktop or workstation environments, as testing environments, or to consolidate server applications.

Virtual machines run on hosts. The same host can run many virtual machines.

Basic Tasks

- Shut down the virtual machine
- Suspend the virtual machine
- Edit virtual machine settings

2. On the ***Virtual Machine Properties*** page, click ***Add…***.



Hardware	Summary
Memory	2048 MB
CPUs	2
Video card	Video card
VMCI device	Restricted
SCSI controller 0	LSI Logic Parallel
Hard disk 1	Virtual Disk
Hard disk 2	Virtual Disk
Network adapter 1	VM Network
Network adapter 2	VM Network
Network adapter 3	Monitor 0

Memory Size: 2 GB

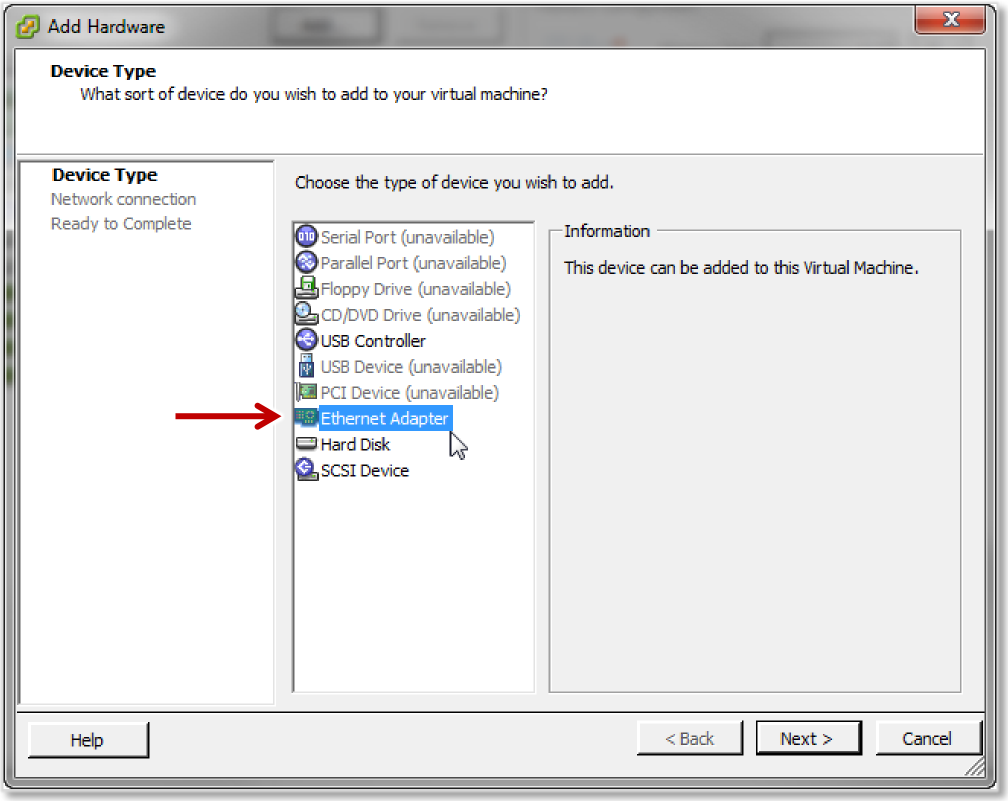
Maximum recommended for this guest OS: 255 GB.

Maximum recommended for best performance: 32760 MB.

Default recommended for this guest OS: 1 GB.

Minimum recommended for this guest OS: 32 MB.

3. On the ***Device Type*** page, select ***Ethernet Adapter***.



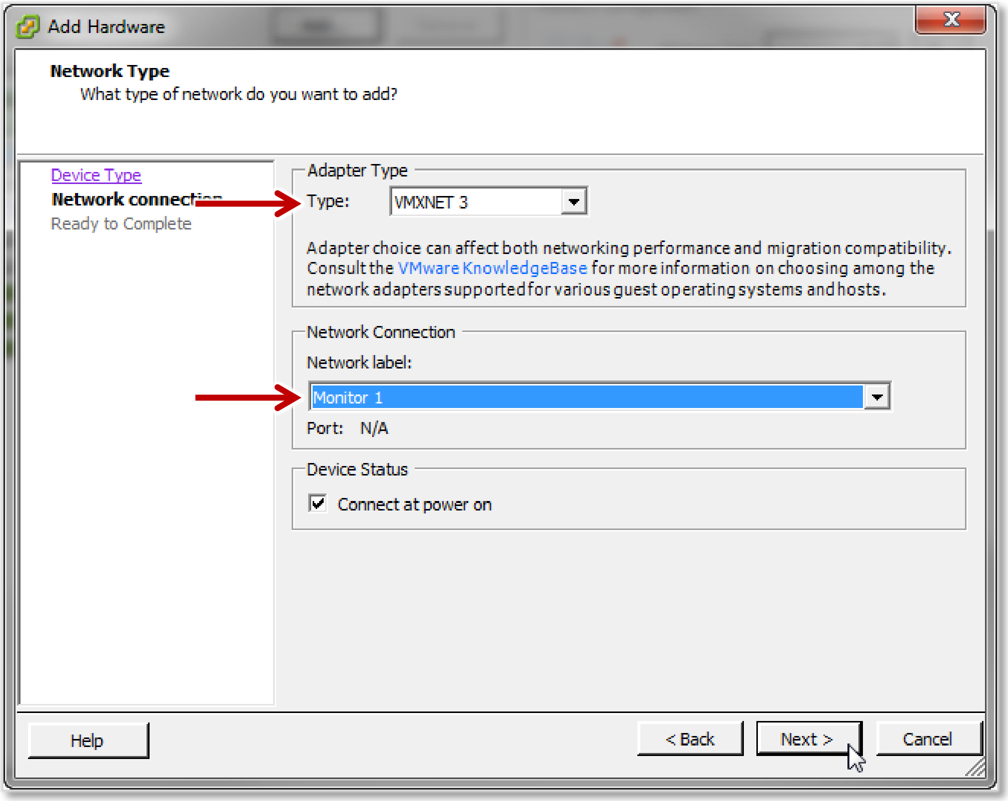
Add Hardware

Device Type
What sort of device do you wish to add to your virtual machine?

Choose the type of device you wish to add.

This device can be added to this Virtual Machine.

4. On the ***Network Type*** page select ***VMXNET3*** for the ***Adapter Type***. For the ***Network Label*** select the name of the port group that you want to map the new monitor port to (***Monitor 1***).



Add Hardware

Network Type

What type of network do you want to add?

Type: VMXNET 3

Adapter choice can affect both networking performance and migration compatibility. Consult the VMware KnowledgeBase for more information on choosing among the network adapters supported for various guest operating systems and hosts.

Network label: Monitor 1

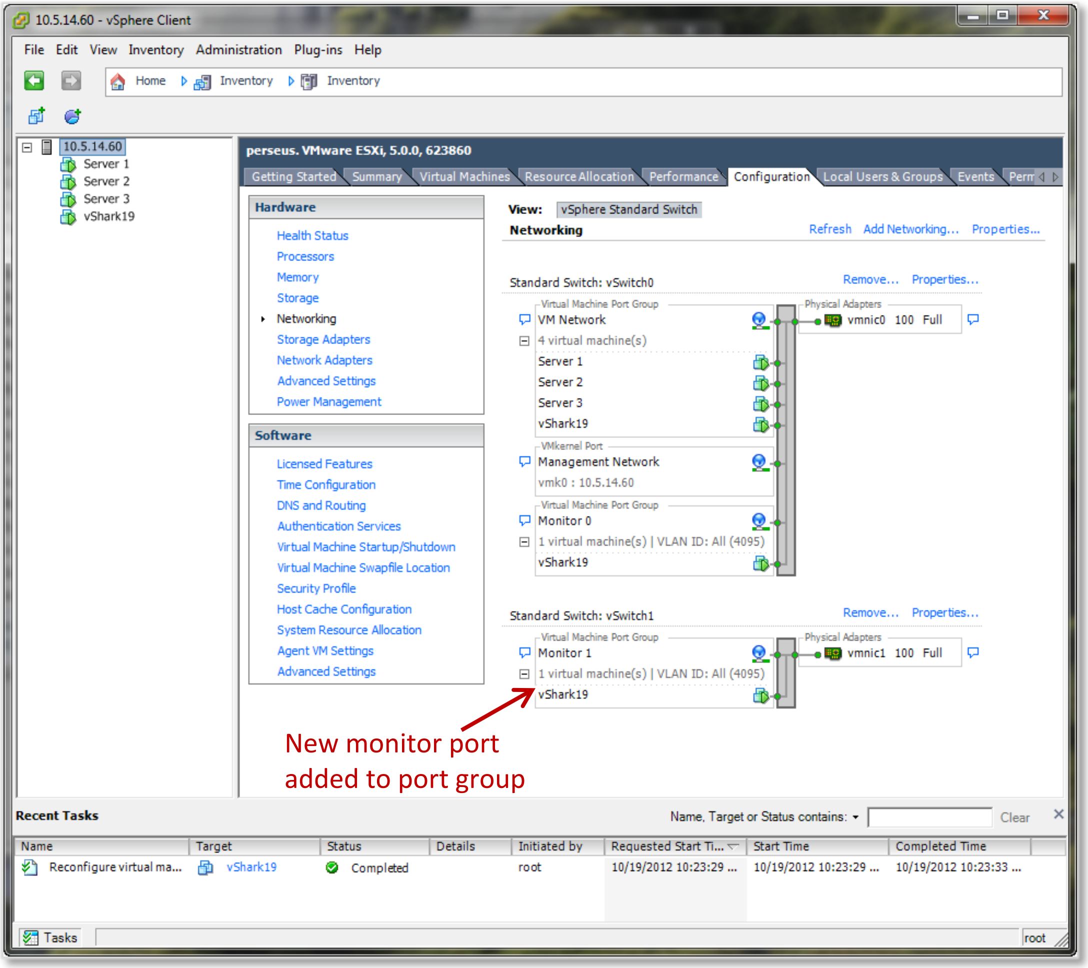
Port: N/A

☑ Connect at power on

5. On the ***Ready to Complete*** page, click ***Finish*** to create the monitor port and add it to the port group.

6. The ***Virtual Machine Properties*** page shows the new monitor port ready to be added. Click ***OK*** to add it.

The ***Networking*** view on the ***Configuration*** tab of the server shows the NetShark added to the Monitor 1 port group, indicating the mapping of the new monitor port (***mon1***).



View: vSphere Standard Switch

Networking

Standard Switch: vSwitch0

Virtual Machine Port Group
VM Network
4 virtual machine(s)
Server 1
Server 2
Server 3
vShark19

VMkernel Port
Management Network
vmk0 : 10.5.14.60

Virtual Machine Port Group
Monitor 0
1 virtual machine(s) | VLAN ID: All (4095)
vShark19

Physical Adapters
vmnic0 100 Full

Standard Switch: vSwitch1

Virtual Machine Port Group
Monitor 1
1 virtual machine(s) | VLAN ID: All (4095)
vShark19

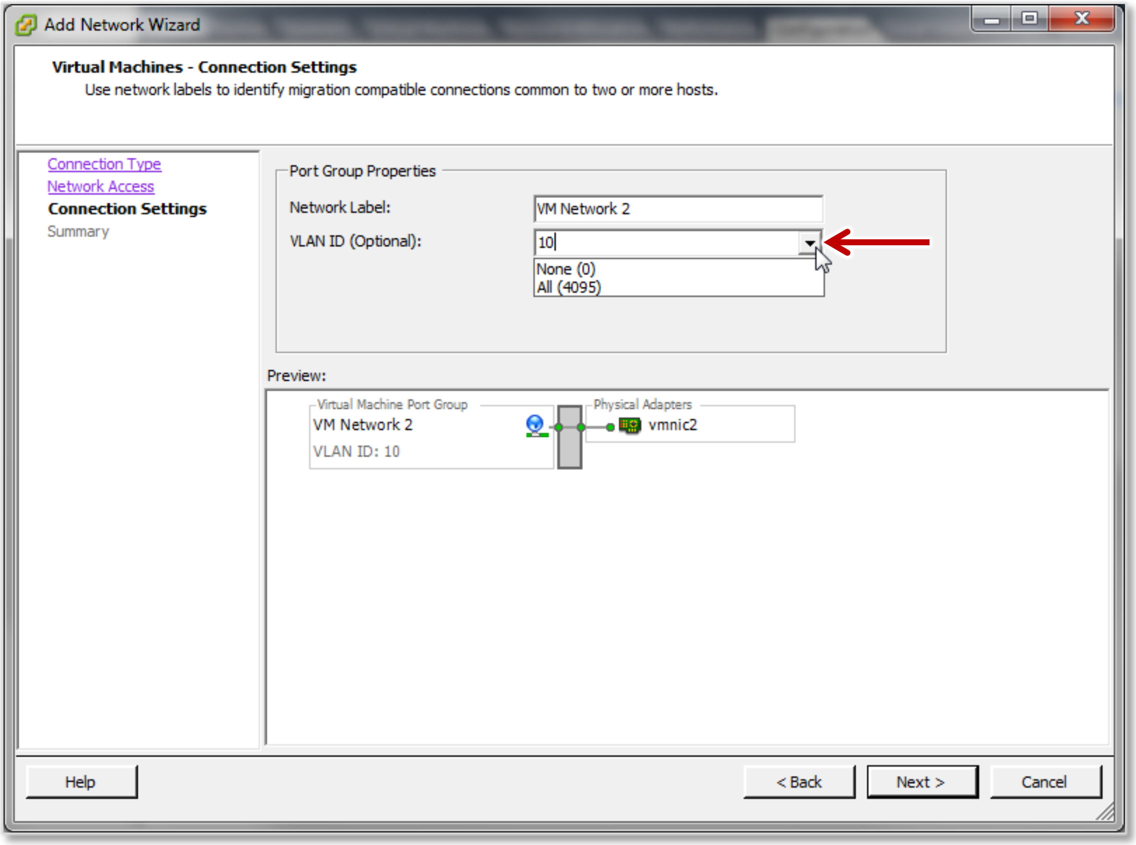
Physical Adapters
vmnic1 100 Full

New monitor port added to port group

Name	Target	Status	Details	Initiated by	Requested Start Ti...	Start Time	Completed Time
Reconfigure virtual ma...	vShark19	Completed		root	10/19/2012 10:23:29 ...	10/19/2012 10:23:29 ...	10/19/2012 10:23:33 ...

VLANs

When you are setting up a port group, the ***Virtual Machines – Connection Settings*** screen allows you to specify a ***VLAN ID***. You can select ***None (0)*** or ***All (4095)*** from the drop-down list, or you can enter a single VLAN ID in the text box.



Add Network Wizard

Virtual Machines - Connection Settings

Use network labels to identify migration compatible connections common to two or more hosts.

Port Group Properties

Network Label: VM Network 2

VLAN ID (Optional): 10

The effect of the ***VLAN ID*** entry is:

If you enter:	**Devices attached to this port group are able to see these packets on the virtual switch:**
None (0)	untagged packets
All (4095)	untagged packets plus packets tagged for all VLANs
a single numeric VLAN ID (for example, 10)	packets tagged for the specified VLAN

Note that if the port group is set to non-promiscuous mode, a device in the port group is able to see only packets that are addressed to it. If the port group is set to promiscuous mode, a device in the port group is able to see packets with any destination address.

NFS datastores and thick provisioning

The ESXi server supports local, NFS, and iSCSI datastores.

By default, NFS datastores use thin provisioning regardless of whether you have specified thin provisioning or thick provisioning when deploying the OVA or adding a hard drive. You can, however, force a hard drive stored on an NFS datastore to use thick provisioning in the following way:

1. If the NetShark is powered on, power it off.
2. Go to the ***Configuration*** tab of your ESXi server.
3. Click ***Storage***.
4. Right-click the datastore where your virtual hard disk is located and choose ***Browse datastore***.
5. Click the ***Folders*** tab, and then select the folder corresponding to the virtual machine of interest.
6. Right-click on the virtual hard disk of interest and select ***Inflate***.

The ESXi server will physically reserve the configured amount of storage. Note that depending on the size of the virtual hard disk and the connection speed, inflation can take a long time, possibly hours.

Contacting Riverbed

Options for contacting Riverbed include:

- Internet - Find out about Riverbed products at http://www.riverbed.com.
- Support - If you have problems installing, using, or replacing Riverbed products, contact Riverbed Technical Support or your channel partner who provides support. To contact Riverbed Technical Support, please open a trouble ticket at https://support.riverbed.com or call 1-888-RVBD-TAC (1-888-782-3822) in the United States and Canada or +1 415 247 7381 outside the United States.
- Professional Services - Riverbed has a staff of engineers who can help you with installation, provisioning, network redesign, project management, custom designs, consolidation project design, and custom-coded solutions. To contact Riverbed Professional Services, go to http://www.riverbed.com or email proserve@riverbed.com.
- Documentation - Riverbed continually strives to improve the quality and usability of its documentation. We appreciate any suggestions you may have about our on line documentation or printed materials. Send documentation comments to techpubs@riverbed.com.

riverbed

Riverbed Technology
680 Folsom St.
San Francisco, CA 94107

Phone: 415 247 8800
Fax: 415 247 8801
www.riverbed.com