

SteelCentral™ NetExpress Software Installation Guide

Virtual Edition for VMware ESXi 5.5 and 6.0

Version 10.10.x

June 2017

The logo for Riverbed, featuring the word "riverbed" in a bold, orange, lowercase sans-serif font. A small registered trademark symbol (®) is located at the top right of the letter "d".

© 2017 Riverbed Technology. All rights reserved.

Riverbed®, SteelApp™, SteelCentral™, SteelFusion™, SteelHead™, SteelScript™, SteelStore™, Steelhead®, Cloud Steelhead®, Virtual Steelhead®, Granite™, Interceptor®, Stingray™, Whitewater®, WWOS™, RiOS®, Think Fast®, AirPcap®, BlockStream™, FlyScript™, SkipWare®, TrafficScript®, TurboCap®, WinPcap®, Mazu®, OPNET®, and Cascade® are all trademarks or registered trademarks of Riverbed Technology, Inc. (Riverbed) in the United States and other countries. Riverbed and any Riverbed product or service name or logo used herein are trademarks of Riverbed. All other trademarks used herein belong to their respective owners. The trademarks and logos displayed herein cannot be used without the prior written consent of Riverbed or their respective owners.

F5, the F5 logo, iControl, iRules and BIG-IP are registered trademarks or trademarks of F5 Networks, Inc. in the U.S. and certain other countries. Linux is a trademark of Linus Torvalds in the United States and in other countries. VMware, ESX, ESXi are trademarks or registered trademarks of VMware, Incorporated in the United States and in other countries.

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.

Individual license agreements can be viewed at the following location: https://<appliance_name>/license.php

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 Technology
680 Folsom Street
San Francisco, CA 94107

Phone: 415.247.8800
Fax: 415.247.8801
Web: <http://www.riverbed.com>

Part Number
712-00217-06

Contents

Chapter 1 - Introduction	1
Additional Resources	2
Contacting Riverbed	2
Chapter 2 - Requirements	3
License token	3
NetExpress software (OVA package)	3
VMware ESXi host	4
Hardware resources	4
Network access	4
Microsoft Windows system on which to run the VMware vSphere client software	5
VMware vSphere client software	6
VMware ESXi configuration information	6
NetExpress initial configuration information	6
Chapter 3 - Preparing the ESXi host	9
Log in to the vSphere client	9
Create a port group	11
Set the port group to promiscuous mode	15
Chapter 4 - Deploying the NetExpress	17
Uploading the NetExpress OVA package to the ESXi host	17
Configuring the NetExpress ports	21
Adding virtual disks	24
Adding a disk for flow data storage	24
Adding a disk for packet storage	29
Verifying the additional storage	29
Powering on the virtual machine	30

Chapter 5 - Configuring the NetExpress31

 Assigning a network address31

 Initial setup33

 Activating licenses.....36

 Obtaining license keys from the licensing portal36

 Entering license keys in the NetExpress.....37

Chapter 6 - Verifying the installation39

CHAPTER 1 Introduction

The virtual edition of the Riverbed® SteelCentral™ NetExpress is a virtualized implementation of the NetExpress appliance. This document describes how to install the virtual edition on a VMware ESXi host. It describes a basic deployment, although many configurations are possible. Refer to the VMware ESXi documentation for additional configuration information.

The installation procedure includes:

- Requirements
 - Ensuring that you have the required hardware, software and configuration information
 - See [Chapter 2, “Requirements”](#)
- Preparing the ESXi host
 - Logging in and creating a port group for NetExpress monitoring ports
 - Setting the monitoring port group to promiscuous mode
 - See [Chapter 3, “Preparing the ESXi host”](#)
- Deploying the NetExpress
 - Uploading the NetExpress archive (OVA) package to the ESXi host
 - Configuring the NetExpress ports
 - Adding virtual disks for flow data storage and packet storage
 - Powering on the virtual machine
 - See [Chapter 4, “Deploying the NetExpress”](#)
- Configuring the NetExpress
 - Assigning a network address
 - Initial setup
 - Activating licenses
 - See [Chapter 5, “Configuring the NetExpress”](#)
- Verifying the installation
 - Checking system status
 - Confirming that data is being received and processed
 - See [Chapter 6, “Verifying the installation”](#)

Additional Resources

The primary source of product information is the online help system. Additional information is available from the Riverbed Support site at <https://support.riverbed.com>. The Software & Documentation page for your product includes:

- Release Notes - posted with the software for your product.
- Users Guides, Technical Notes and reference documents - posted in the Documentation section of the page for your product.
- Knowledge Base - a database of known issues and how-to documents. You can browse titles or search for key words and strings. Choose “Search Knowledge Base” from the Knowledge Base menu.

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.

CHAPTER 2 Requirements

Before beginning the installation, ensure that you have the required hardware, software and configuration information. This section describes each item on the following checklist of prerequisites.

- License token
- NetExpress software (OVA package)
- VMware ESXi 5.5 or 6.0 host with adequate hardware resources and network access
- Microsoft Windows system on which to run the VMware vSphere client software
- VMware vSphere client software
- VMware ESXi configuration information
- NetExpress initial configuration information

License token

When you purchase a NetExpress virtual appliance, you receive a license request token in email. The general procedure for activating the license is to:

1. Use the token with the NetExpress to generate a license activation code.
2. Paste the generated license activation code into a field on the Riverbed licensing portal to create license keys for all the features you purchased with the NetExpress.
3. Paste the license keys into the NetExpress to activate the licensed features.

This procedure is described in more detail in [Chapter 5, “Configuring the NetExpress.”](#)

NetExpress software (OVA package)

To deploy the NetExpress on the ESXi host, you must provide a path to the OVA package. The package should be downloaded from the Riverbed Support site to a location on your network that is accessible to the computer on which the VMware vSphere client is running. It can be local to that computer or somewhere else on your network.

The OVA package is built using Virtual Machine version 7.

VMware ESXi host

The server hosting the VMware ESXi software must have adequate hardware resources and network access.

Hardware resources

Hardware requirements depend on the licensed flow limits. For an ESXi host that is running only the NetExpress, the recommended computing resources are as follows.

- Virtual CPUs and RAM as listed in the table below
- System disk: 350 GB minimum
- 8 GB swap space on the system disk
- Support for 6 virtual network interfaces (two management and four monitoring)
- Second virtual disk for flow data storage: 250 GB to 4 TB
- Third virtual disk for packet storage: 250 GB to 4 TB

Product Code	License Type	Flow Limit	Minimum	Recommended
SCNE-VE-470-F1	MSPECSCNEV470FLOW1	15k FPM	Four 2.6 GHz CPUs 8 GB RAM	Eight 2.6 GHz CPUs 16 GB RAM
SCNE-VE-470-F2	MSPECSCNEV470FLOW2	30k FPM	Four 2.6 GHz CPUs 8 GB RAM	Eight 2.6 GHz CPUs 16 GB RAM
SCNE-VE-470-F3	MSPECSCNEV470FLOW3	60k FPM	Four 2.6 GHz CPUs 8 GB RAM	Eight 2.6 GHz CPUs 16 GB RAM
SCNE-VE-470-F4	MSPECSCNEV470FLOW4	90k FPM	Four 2.6 GHz CPUs 16 GB RAM	Eight 2.6 GHz CPUs 32 GB RAM
SCNE-VE-470-F5	MSPECSCNEV470FLOW5	120k FPM	Four 2.6 GHz CPUs 16 GB RAM	Eight 2.6 GHz CPUs 32 GB RAM

The system virtual disk should be “thick provisioned” to ensure the disk space will be available to the virtual machine. However, the system virtual disk can be “thin provisioned” if there is enough free space on a datastore to support the size of the disk when it becomes full. If the datastore runs out of disk space when using “thin provisioned” virtual disks, the virtual machine may become unstable and require re-installation.

It is recommended that the second and third virtual disks also be “thick provisioned.”

Network access

The NetExpress must access other SteelCentral products and also network services.

Communication between SteelCentral products

If you lock down your network on a port-by-port basis, ensure that the following ports are open between SteelCentral products:

- TCP/22 – (ssh) This is needed for the NetExpress to transfer upgrade packages to other SteelCentral products that are connected to it.
- TCP/8443 – Exchange of encryption certificates between SteelCentral products.
- TCP/41017 – Encrypted communication between NetExpress and Sensor, Flow Gateway, NetShark or AppResponse appliance.
- UDP/123 – (ntp) Synchronization of time between a Sensor or Flow Gateway and the NetExpress.

Access to and from network access services

- TCP/22 – (ssh) This is needed for secure shell access to SteelCentral software components and for the appliance to obtain information from servers via scripts.
- UDP/161 – (snmp) The NetExpress uses SNMP to obtain interface information from switches. Also, management systems use this port to read the SteelCentral appliance MIB.
- TCP/443 – (https) Secure web-based management interfaces.
- TCP/5432 – (odbc) If you will be allowing other applications to access the NetExpress internal database via ODBC, then you must allow traffic on this port.
- 42999 – If you will be using the NetExpress user identification feature with a Microsoft Active Directory domain controller, then you must allow traffic on port 42999.
- Vulnerability scanner ports – If you will be using the NetExpress vulnerability scan feature, then you must allow traffic on the port that the product is to use for accessing the vulnerability scanner server. Obtain vulnerability scanner server addresses and port numbers from the administrator of those systems. The default ports are as follows:
 - Nessus: 1241
 - nCircle: 443
 - Rapid7: 3780
 - Qualys: Requires external https access to qualysapi.qualys.com (Note: This is separate from qualysguard.qualys.com.)
 - Foundstone: 3800

Microsoft Windows system on which to run the VMware vSphere client software

The computer you use for installing the NetExpress should be running a version of Microsoft Windows that supports the VMware vSphere client.

The NetExpress OVA package deployment will be fastest if the OVA package, the ESXi host, and the computer on which you are running the VMware vSphere client are all on the same subnetwork. Deployment may take considerable time if the machines and OVA package are on different networks.

VMware vSphere client software

If the VMware vSphere client software is not installed on your local system, you can download it from the ESXi host. Use your browser to go to the name or IP address of the ESXi host and click the **Download vSphere Client** link on the ESXi Welcome page and save the installation file to your local Windows system. Run the vSphere client installation file and follow the instructions on the screen.

VMware ESXi configuration information

In addition to the ESXi name or IP address and login credentials, you may want to know about any special configuration requirements. This guide provides instructions for a basic installation requiring minimal configuration of the ESXi host. However, many other configurations are possible. If you require a more complex ESXi configuration, please refer to the VMware ESXi user documentation.

NetExpress initial configuration information

When you configure the NetExpress, you will be asked to provide configuration information. Information that is required to complete the installation is listed in the table that follows with an asterisk (*). Items not marked with an asterisk are optional during installation and can be specified afterwards on the NetExpress Configuration > General Settings page if necessary.

It may be useful to write the configuration values in the blank column of the checklist below so that you can refer to them during the configuration step or afterward.

NetExpress host name:*	
NetExpress IP address:*	
Netmask:*	
Default gateway:*	
DNS name resolution for hosts (enable or disable):	
Primary DNS server IP address:	
Secondary DNS server IP address:	
DNS search domain:	
NTP server IP addresses:*	
Applies only if NetExpress is being synchronized to an external NTP server.	
Time Zone:	
SNMP information: NetExpress is set by default to use SNMP Version 1 and to allow MIB browsing. If you are configuring SNMP at this time, obtain the necessary V1 or V3 information.	

Outgoing mail server name, port number, and “From” address.
Applies only if you will be specifying a server that
NetExpress is to use for sending reports or alert notifications.

Inside addresses:
IP addresses or address ranges of hosts that the NetExpress is
to track individually. The default values are 10/8,172.16/
12,192.168/16

Security Profile settings:*

You can use either three traffic collection profiles (weekdays,
weeknights, and weekends) or four (weekdays, weeknights,
Saturdays, and Sundays). After installation, you can define
others. You can also specify the times when weekdays begin
and end (default times are 9:00 am to 5:00 pm).

Password to use for your initial NetExpress login:*

The default password **admin**.

New password to enter when prompted to change the initial
NetExpress password:*

Applies only to systems not previously configured.

Service Management

Leave this set to **ByLocation** unless you are required to
choose another group type for service locations.

CHAPTER 3 Preparing the ESXi host

The NetExpress is preconfigured for the following virtual network connections:

- Primary Network
- Auxiliary Network
- Monitor Network 1
- Monitor Network 2
- Monitor Network 3
- Monitor Network 4

The Primary and Auxiliary network connections are typically mapped to a management port group in a virtual switch. The Monitor network connections must be mapped to one or more port groups that are set for promiscuous mode so that the NetExpress can monitor all traffic seen on the virtual switch.

This guide describes a simple installation in which the NetExpress monitors traffic in one port group on one virtual switch that is connected to a physical network interface controller (NIC) on the ESXi host hardware. For this configuration, it is necessary to

- log in to the ESXi host,
- create a port group on an ESXi virtual switch, and
- set the port group to promiscuous mode.

before deploying the NetExpress OVA package to the ESXi server. Configuring virtual disks for data storage and connecting virtual ports to the port group are parts of the deployment process, which is described in the next chapter.

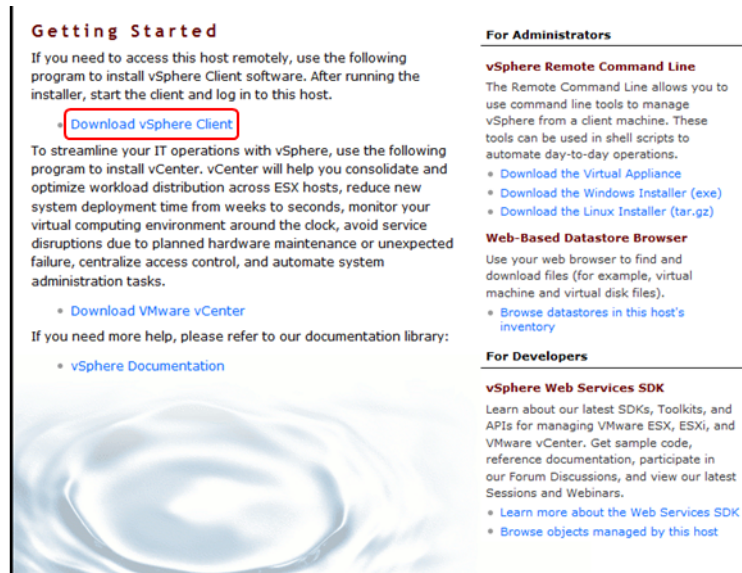
Many more advanced configurations are possible involving multiple port groups, VLANs, virtual switches and physical NICs. Refer to the VMware ESXi documentation for guidance on more advanced deployments.

Log in to the vSphere client

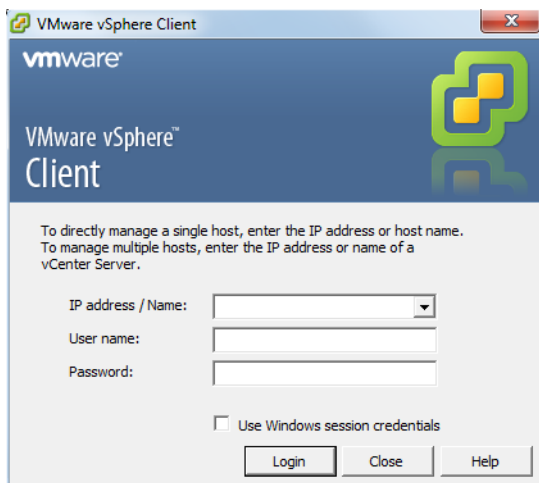
If the VMware vSphere client software is installed on your local system, start it and log in. If it is not installed on your local system, install it as follows:

1. Use your web browser to go to the name or IP address of the ESXi host.

- On the ESXi Welcome page, click **Download vSphere Client** and save the installation file on your local Windows machine.



- Run the vSphere installation file, following the on-screen instructions.
- When the installation completes, open the vSphere client and log in

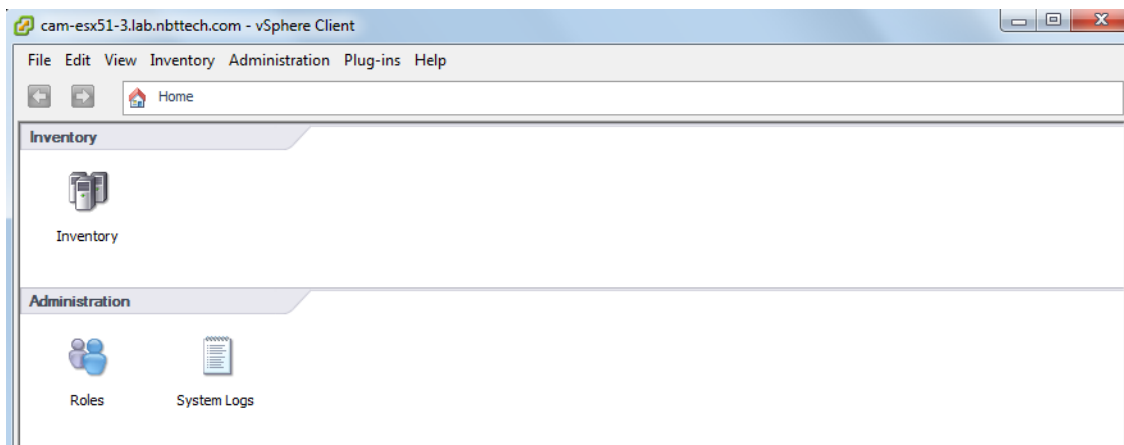


- If you are logging in to a vCenter Server, select the ESXi host on which the NetExpress virtual appliance is to be installed.

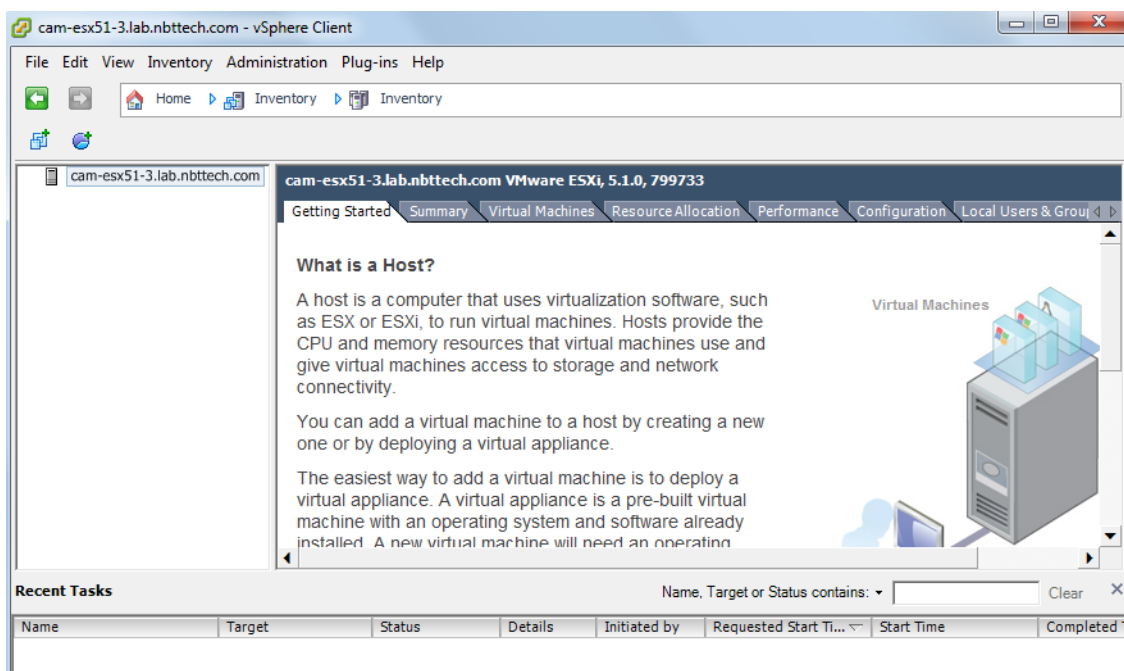
Create a port group

When you log in to the ESXi host, it displays its home page. Starting from the ESXi home page, create a new port group for the NetExpress monitoring ports as follows:

1. Click the Inventory icon.



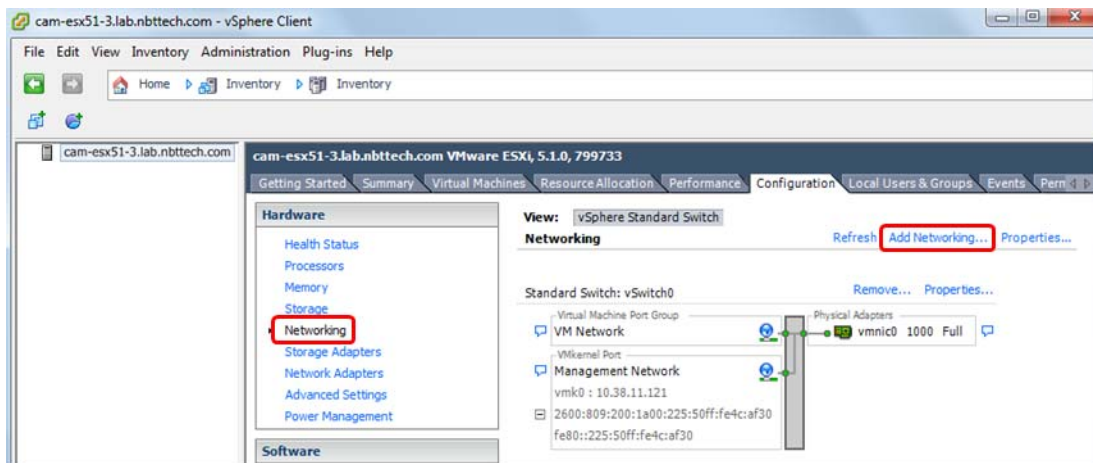
2. If you logged in to a vCenter Server instead of directly in to an ESXi host, select the ESXi host on which to install the NetExpress.



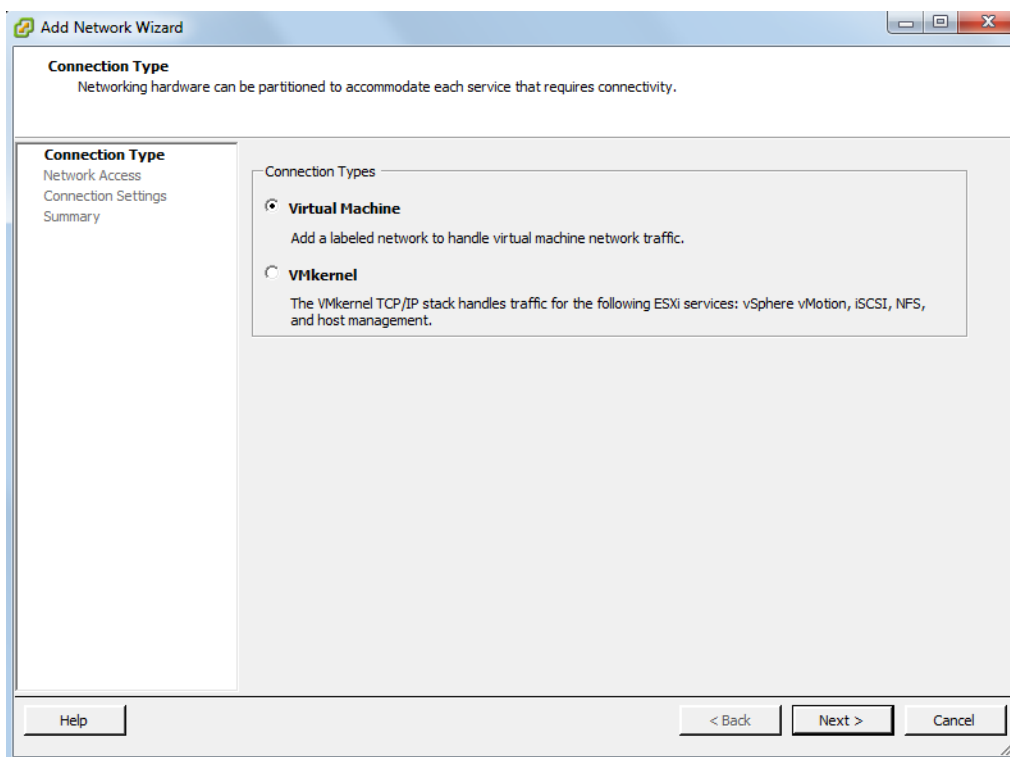
3. Choose the **Configuration** tab.



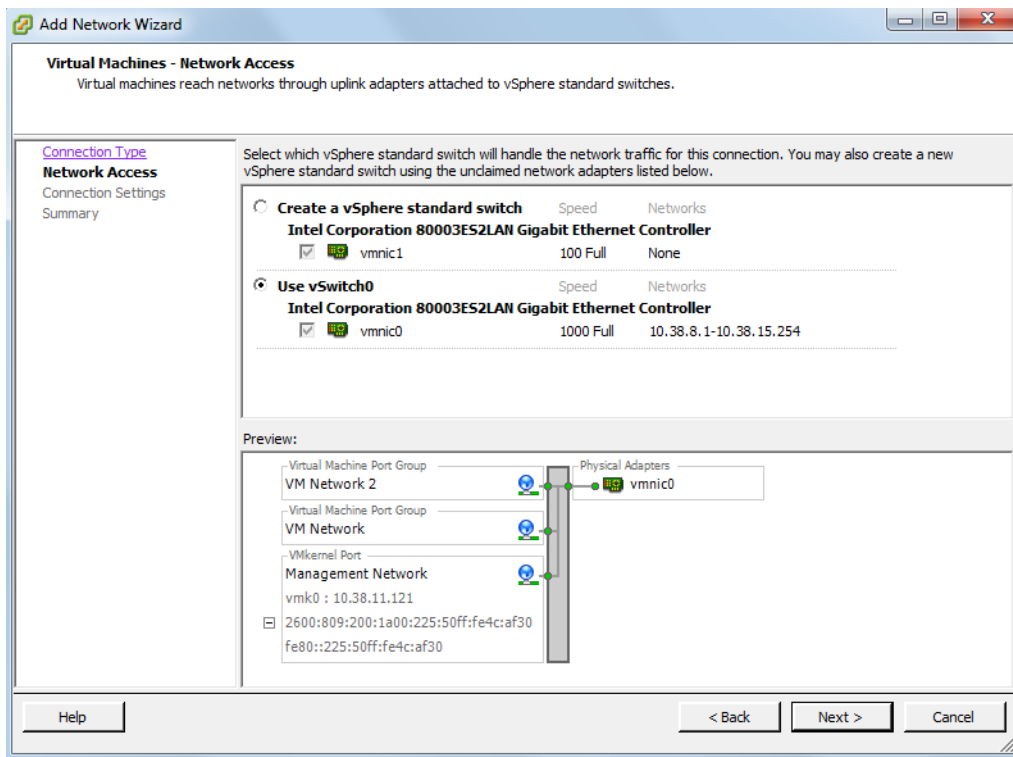
4. In the Hardware section of the Configuration tab, choose **Networking**.



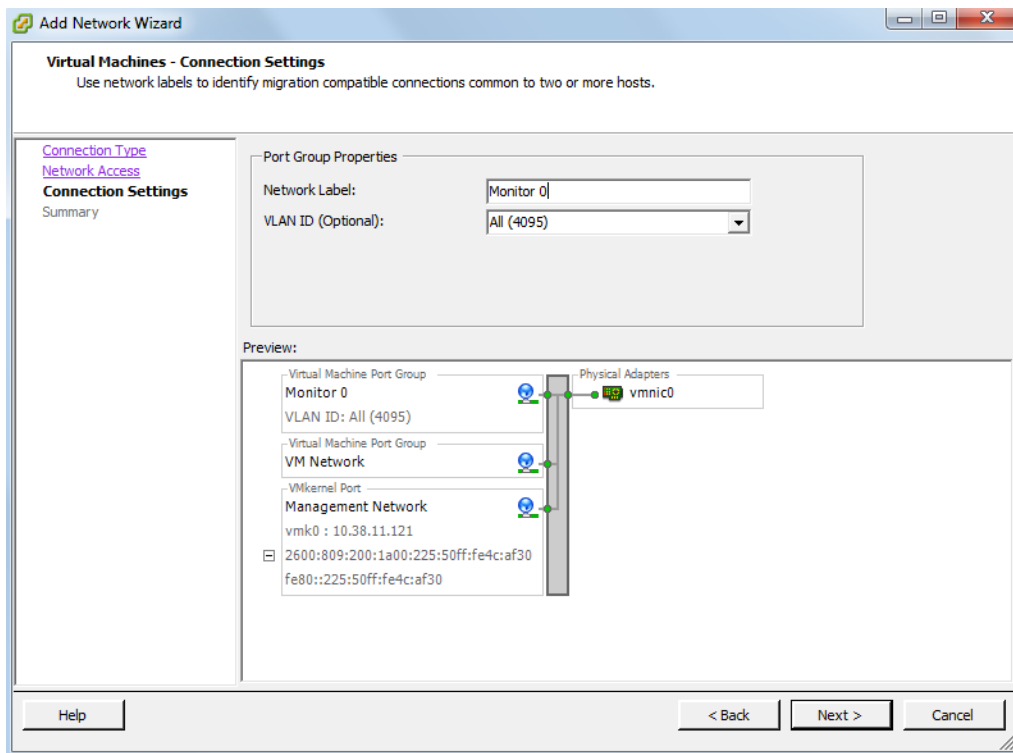
5. If there is more than one virtual switch on the ESXi host, select the one that the NetExpress is to monitor.
6. Choose **Add Networking**. This opens the Add Network wizard.
7. In the Add Network wizard Connection Type section, select **Virtual Machine** and click **Next**.



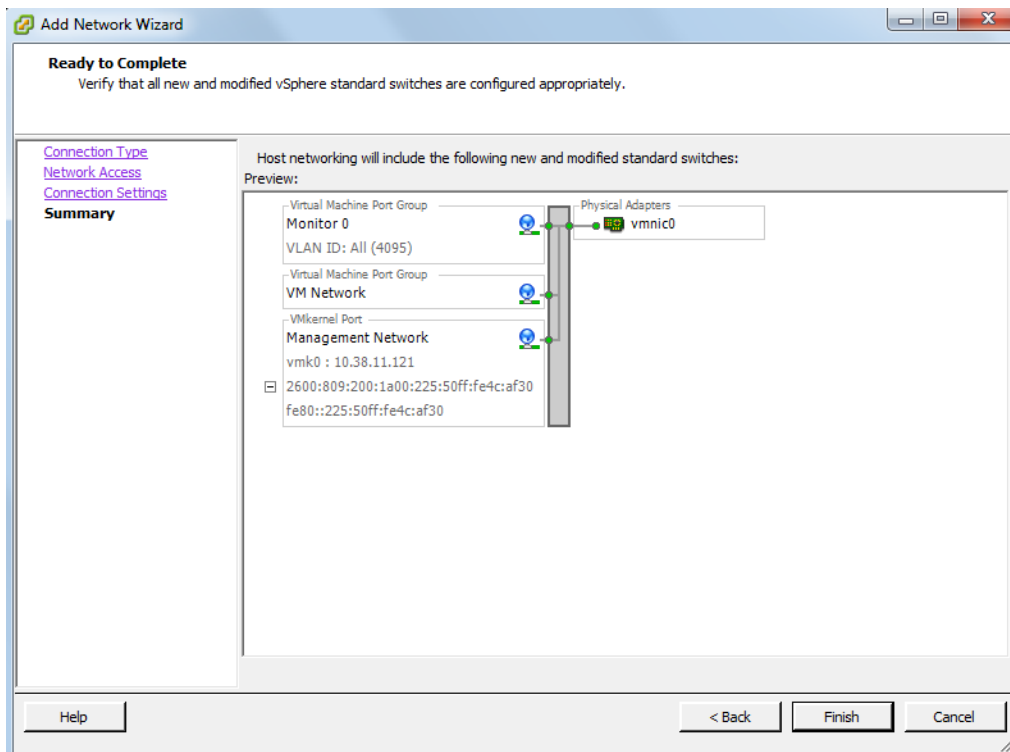
8. In the Add Network wizard Network Access section, select the virtual switch that the NetExpress is to have access to. If no virtual switches have been added to the ESXi host, then select **Use vSwitch0** to use the default virtual switch and click **Next**.



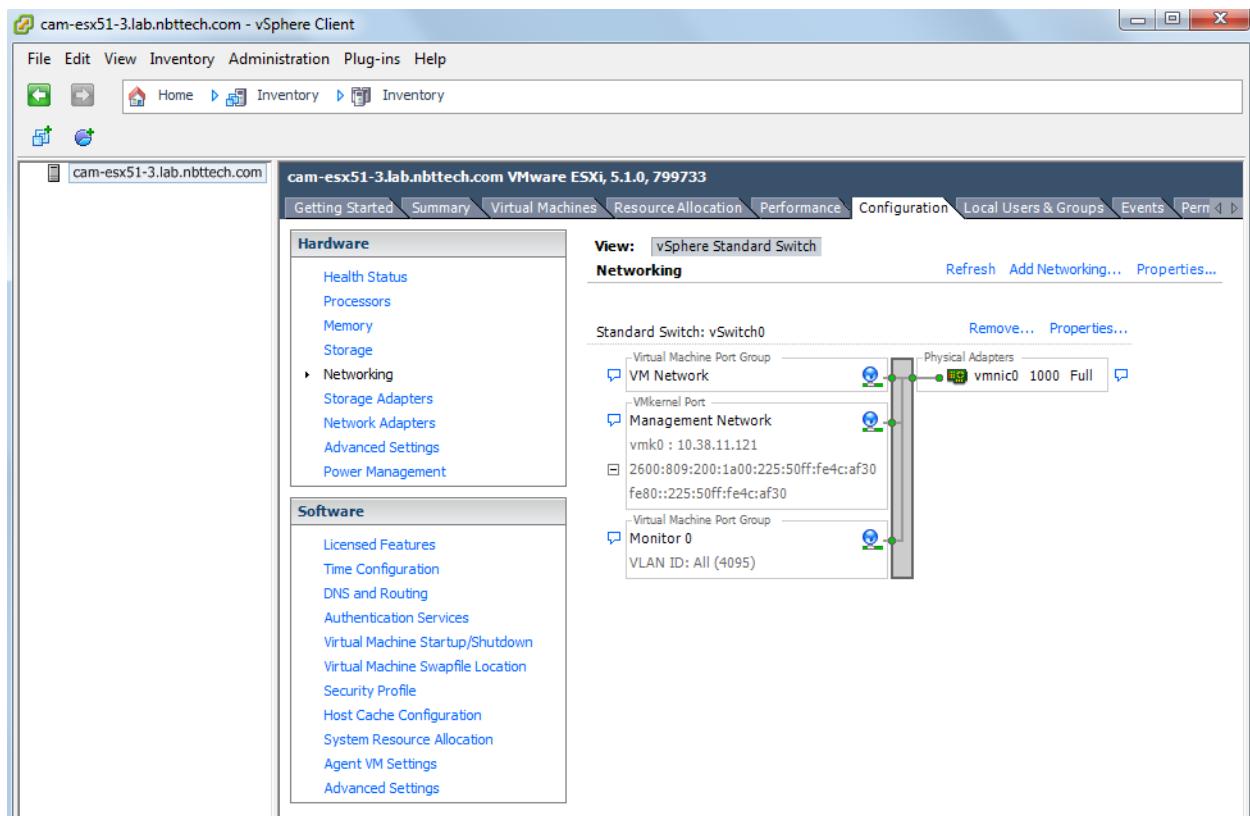
9. In the Add Network wizard Connection Settings section, enter a name for the port group in the **Network Label** field and set the VLAN ID field to **All (4095)**. This allows the port group to see all traffic on the virtual switch. Click **Next** to move on.



10. In the Add Network wizard Summary section (or Ready to Complete section), check to ensure the correct settings and then click **Finish**.



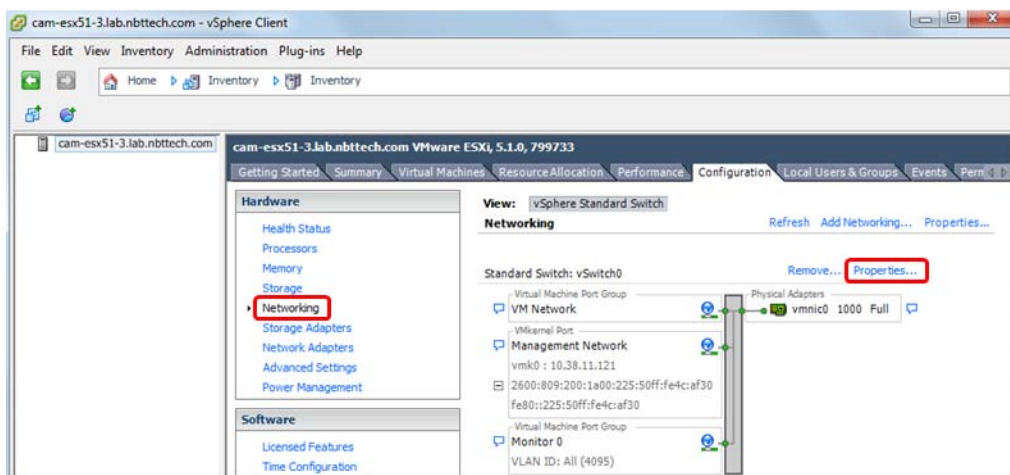
11. On the Configuration tab Networking page, ensure that the new port group is shown in the virtual switch.



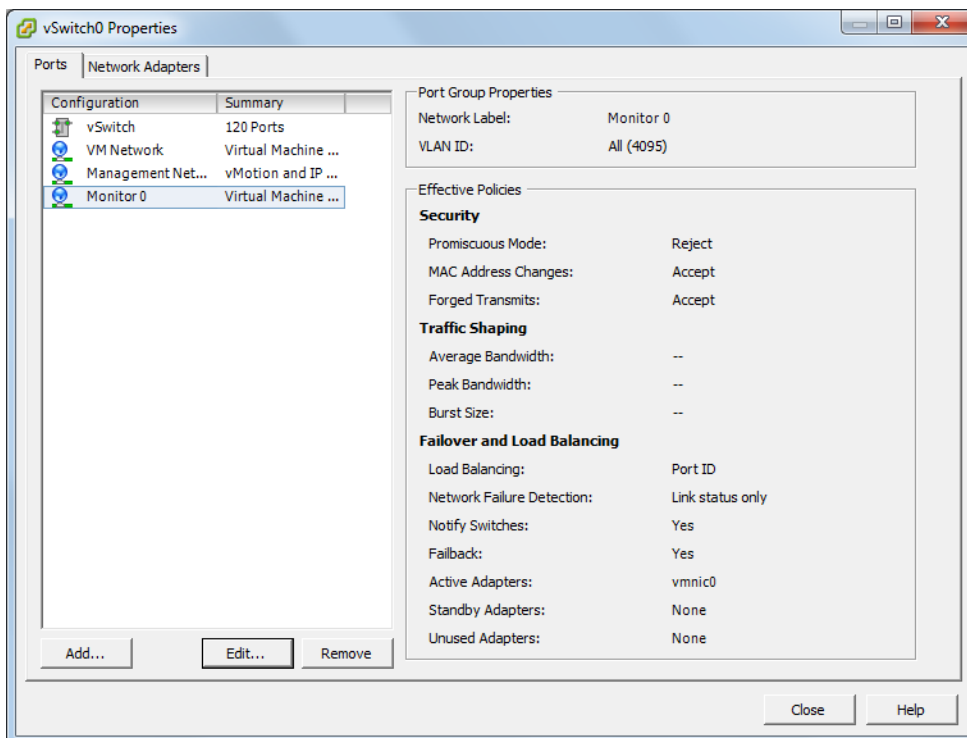
Set the port group to promiscuous mode

Set the new port group (Monitor 0 in this example) to the promiscuous mode as follows:

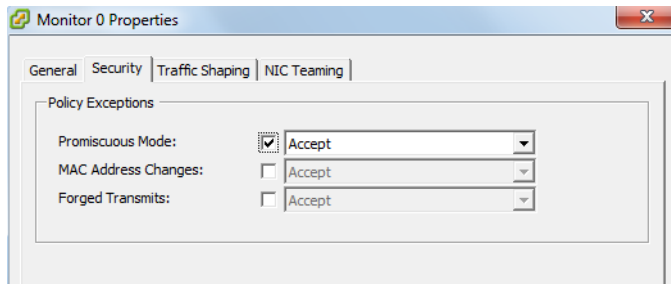
1. In the Configuration tab Networking page, click the **Properties** link for the virtual switch (vSwitch0 in this example).



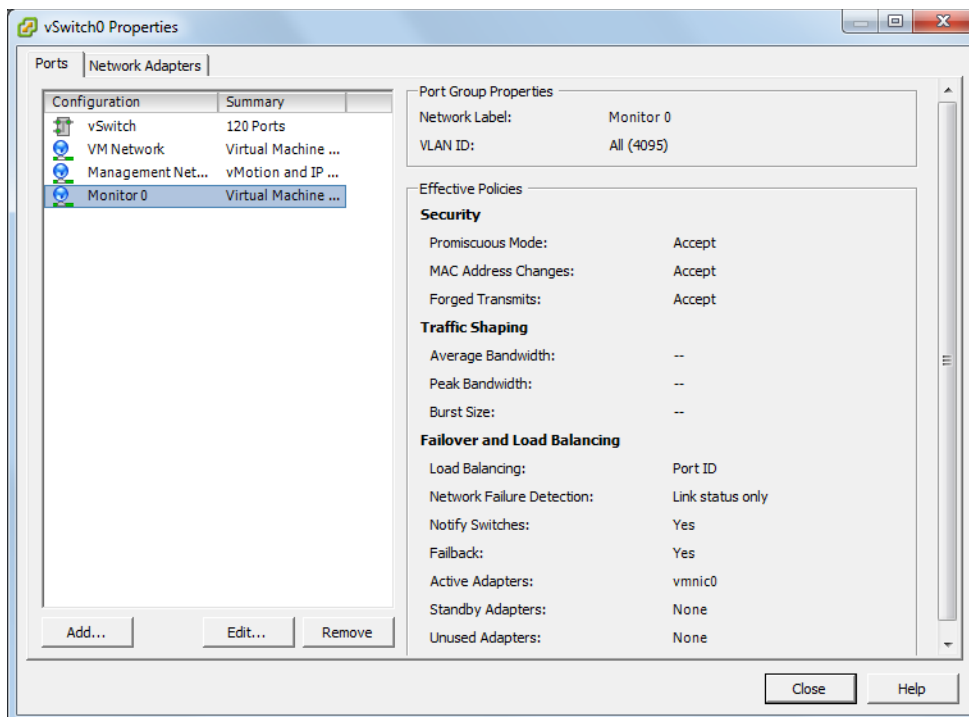
2. On the virtual switch properties page, select **Monitor 0** and click **Edit**.



3. On the port group properties page, go to the Security tab. Select the **Promiscuous Mode** check box and set the field value to **Accept**. Click **OK**.



4. Back on the virtual switch properties page, select the Monitor 0 port group and verify that the Promiscuous Mode is set to **Accept**. Then click **Close**.



This completes preparing the ESXi host for deploying the NetExpress OVA package.

CHAPTER 4 Deploying the NetExpress

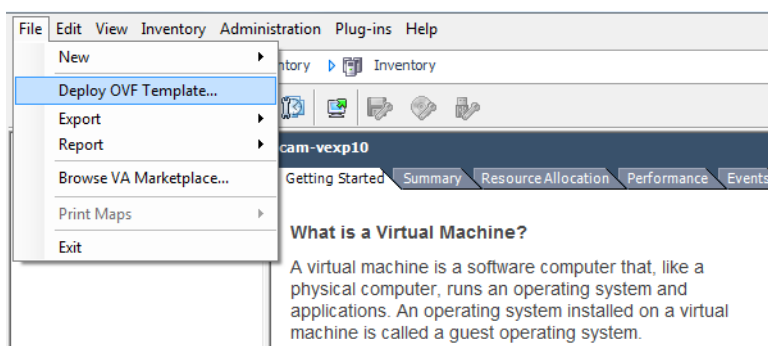
Deploying the NetExpress on an ESXi host involves:

- Uploading the NetExpress archive (OVA) package to the ESXi host.
- Configuring the NetExpress ports.
- Adding virtual disks for flow data storage and packet storage.
- Powering on the virtual machine.

Uploading the NetExpress OVA package to the ESXi host

To deploy the NetExpress virtual appliance on a VMware ESXi host:

1. Log in to the VMware vSphere client or vCenter.
2. If logged into a vCenter, select the ESXi host on which to deploy the NetExpress.
3. On the home page, pull down the File menu and choose **Deploy OVF Template**.

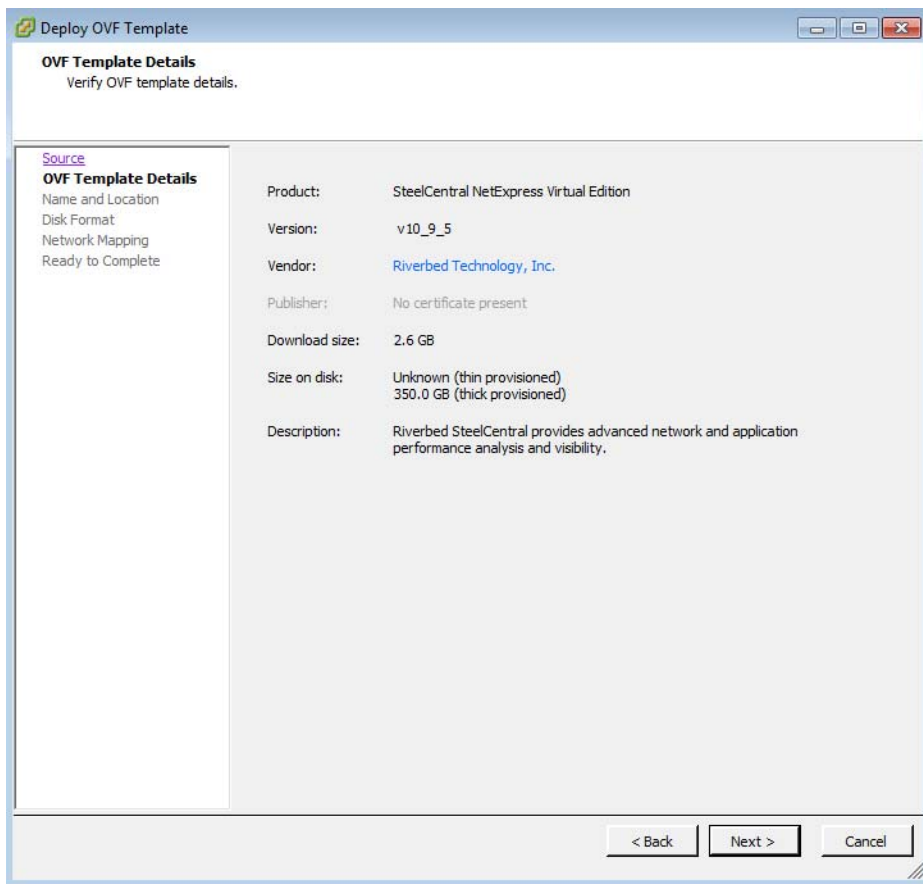


This starts the Deploy OVF Template wizard.

4. On the Source page, enter or browse to the location of the NetExpress OVA file.



5. On the OVF Template Details page, confirm that the correct file is selected and click **Next**.



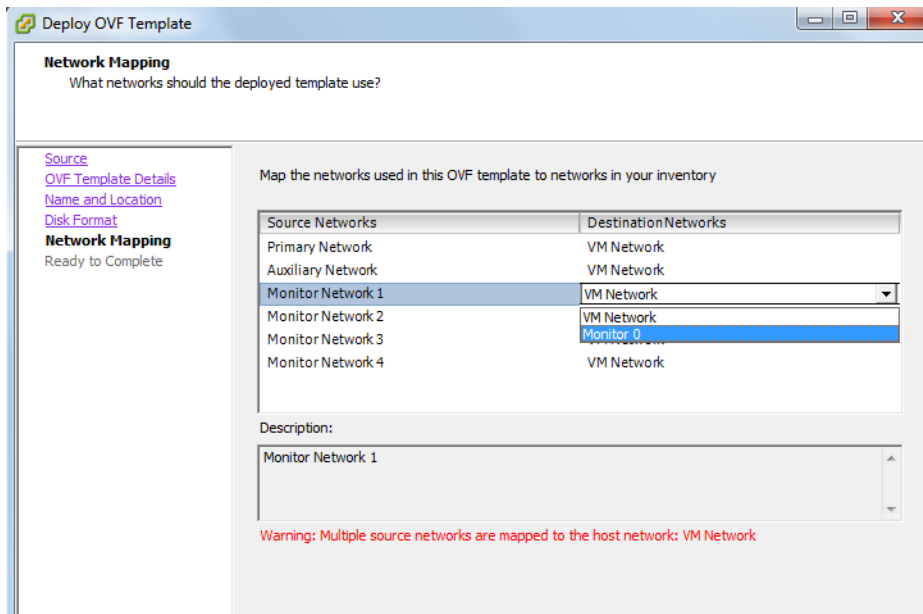
6. On the Name and Location page, enter a name for the NetExpress and click **Next**.

The screenshot shows the 'Deploy OVF Template' wizard window. The title bar says 'Deploy OVF Template'. The main heading is 'Name and Location' with the instruction 'Specify a name and location for the deployed template'. On the left, there is a navigation pane with links: 'Source', 'OVF Template Details', 'Name and Location' (which is highlighted), 'Disk Format', 'Network Mapping', and 'Ready to Complete'. The main area has a 'Name:' text box containing 'SteelCentral NetExpress Virtual Edition'. Below the text box, it says 'The name can contain up to 80 characters and it must be unique within the inventory folder.'

7. Select the ESXi datastore on which the NetExpress will reside (Local, SAN, NAS). If there is more than one location on the ESXi host where you can store the files, the wizard displays a Storage page. Select the datastore where the NetExpress files are to be stored and click **Next**.
8. If the datastore is local, select **Thick Provision Eager Zeroed** on the Disk Format page and click **Next**. (If the datastore is not local, you may not be able to choose a provisioning option.)

The screenshot shows the 'Deploy OVF Template' wizard window at the 'Disk Format' step. The title bar says 'Deploy OVF Template'. The main heading is 'Disk Format' with the instruction 'In which format do you want to store the virtual disks?'. On the left, the navigation pane shows 'Source', 'OVF Template Details', 'Name and Location', 'Disk Format' (highlighted), 'Network Mapping', and 'Ready to Complete'. The main area shows 'Datastore:' with a dropdown menu set to 'datastore1'. Below that, 'Available space (GB):' is shown as '5576.3'. There are three radio button options: 'Thick Provision Lazy Zeroed', 'Thick Provision Eager Zeroed' (which is selected), and 'Thin Provision'. At the bottom, there are buttons for 'Help', '< Back', 'Next >', and 'Cancel'.

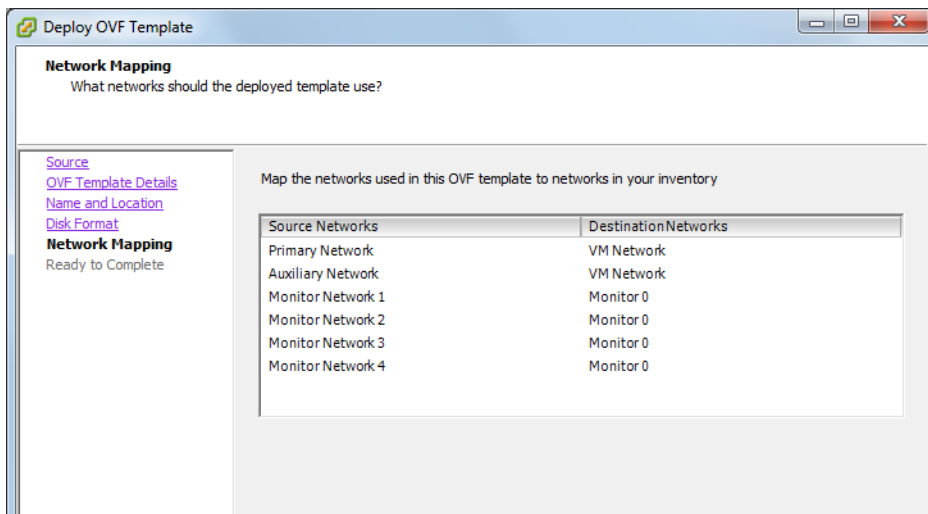
- On the Network Mapping page, map the source networks (ports) of the NetExpress to destination networks (port groups) on the ESXi host. Map the Primary and Auxiliary networks to the default ESXi management port group (VM Network). Map the Monitor networks to the Monitor 0 port group.



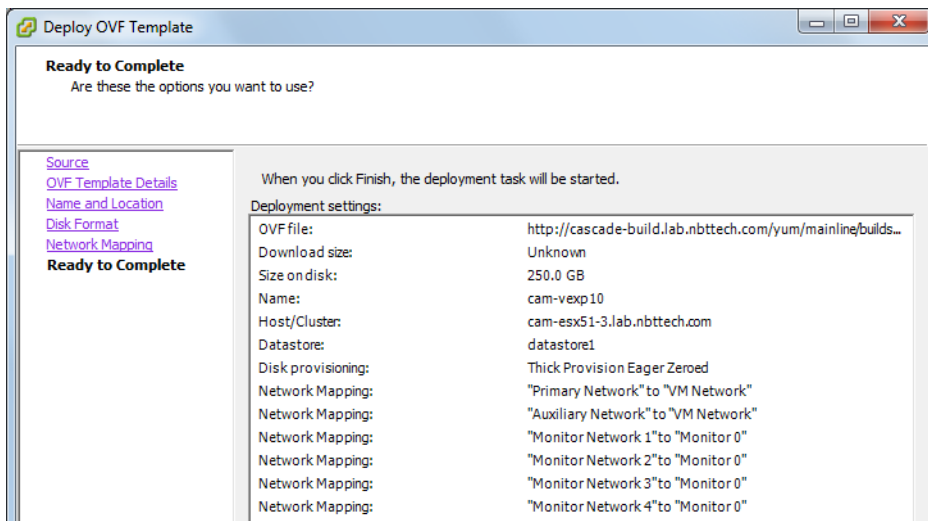
In this installation example, only one monitoring port (Mon 0) is used to monitor traffic on the ESXi virtual switch, so only one monitoring port group is defined on the virtual switch. All ports must be mapped, whether or not they are connected while the virtual appliance is running. Therefore, all ports are mapped to the one monitoring port group. In a later step, Mon 0 is set to be connected to the monitoring port group when the NetExpress virtual appliance is started, and Mon 1, Mon 2 and Mon 3 are set to not be connected.

In more advanced installations, you might create a separate port group for each NetExpress monitoring port. In that case, each port group you created would be listed on the drop-down list and you would map each NetExpress monitoring port to a different port group.

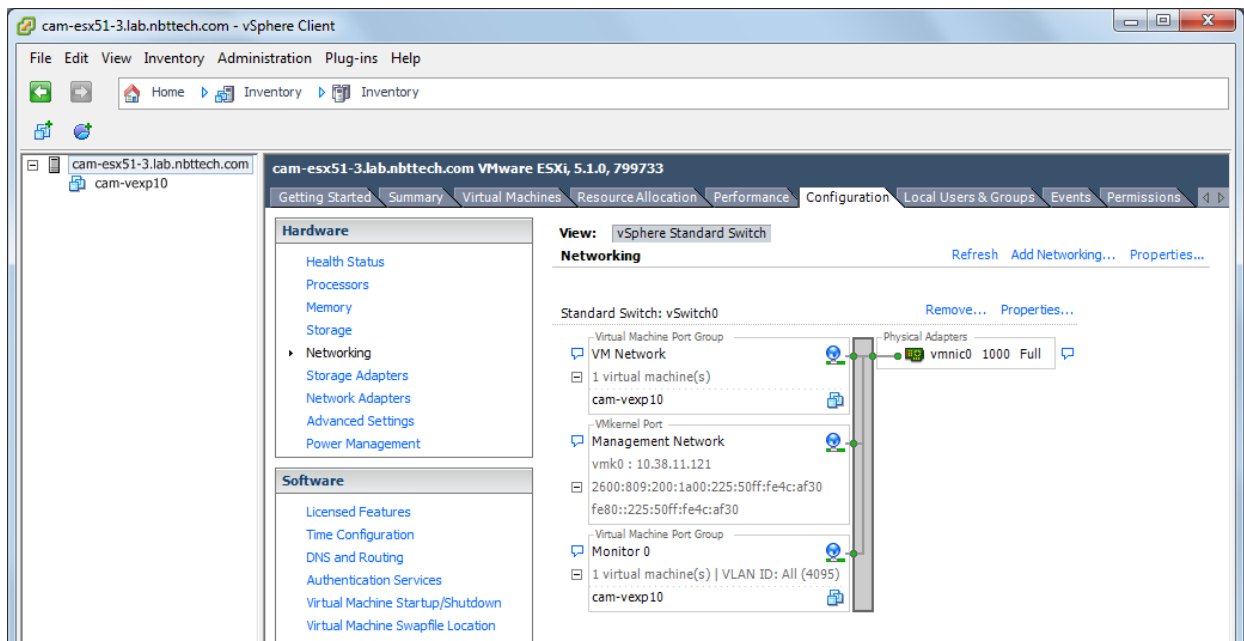
- Ensure that all NetExpress monitor ports are mapped to the monitoring port group. Then click **Next**.



11. On the Ready to Complete summary page, verify the setup information and click **Finish** to start the deployment.



When the deployment has completed, you can see the configuration in the Configuration tab Networking section.



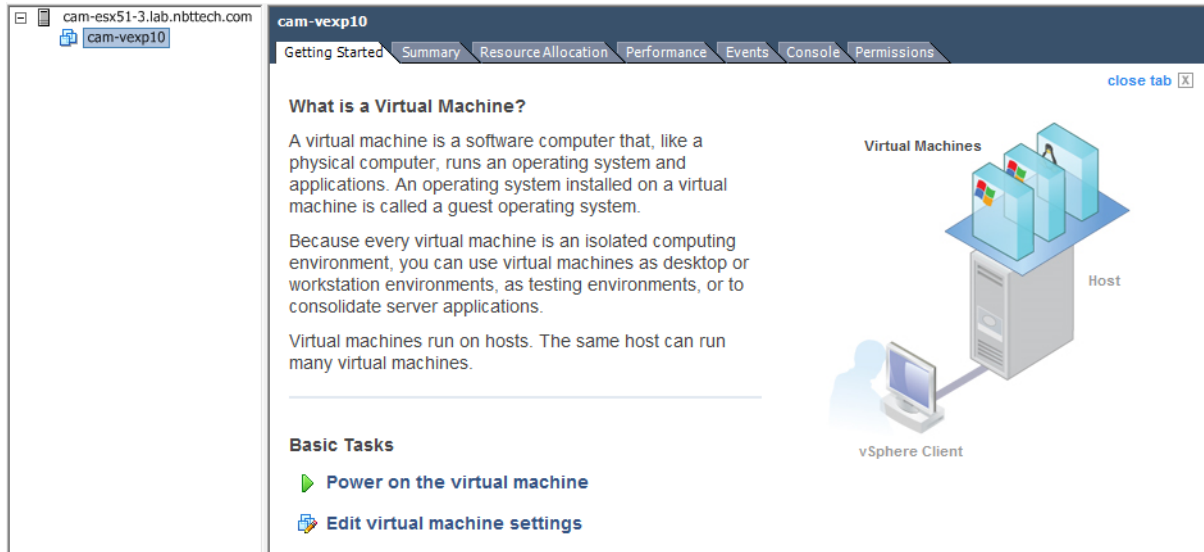
Configuring the NetExpress ports

By default, all virtual hardware is connected when the NetExpress virtual appliance is powered on. This installation example uses only one virtual switch port group for monitoring, and all NetExpress monitoring ports are mapped to that one port group. Therefore, all monitoring ports would be seeing the same traffic. So this example leaves the first NetExpress monitoring port (Mon 0) connected and sets the virtual hardware for monitoring ports Mon1, Mon2 and Mon3 to not be connected.

In more advanced installations, these ports might be set to monitor different VLANs or they might be mapped to different port groups. The different port groups might be on other virtual switches. Refer to the VMware ESXi documentation for information about other configurations.

To set NetExpress monitoring ports Mon1, Mon2 and Mon3 to not be connected when the NetExpress is powered on,

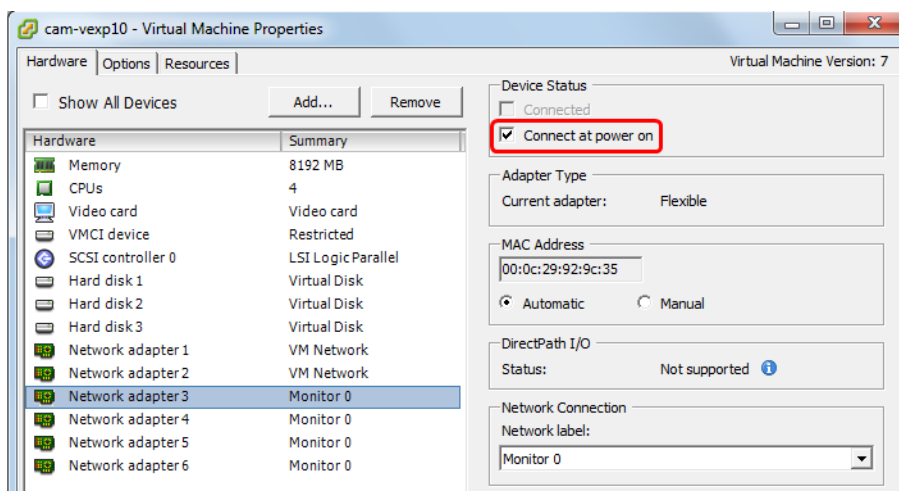
1. Select the NetExpress virtual appliance and click **Edit virtual machine settings**.



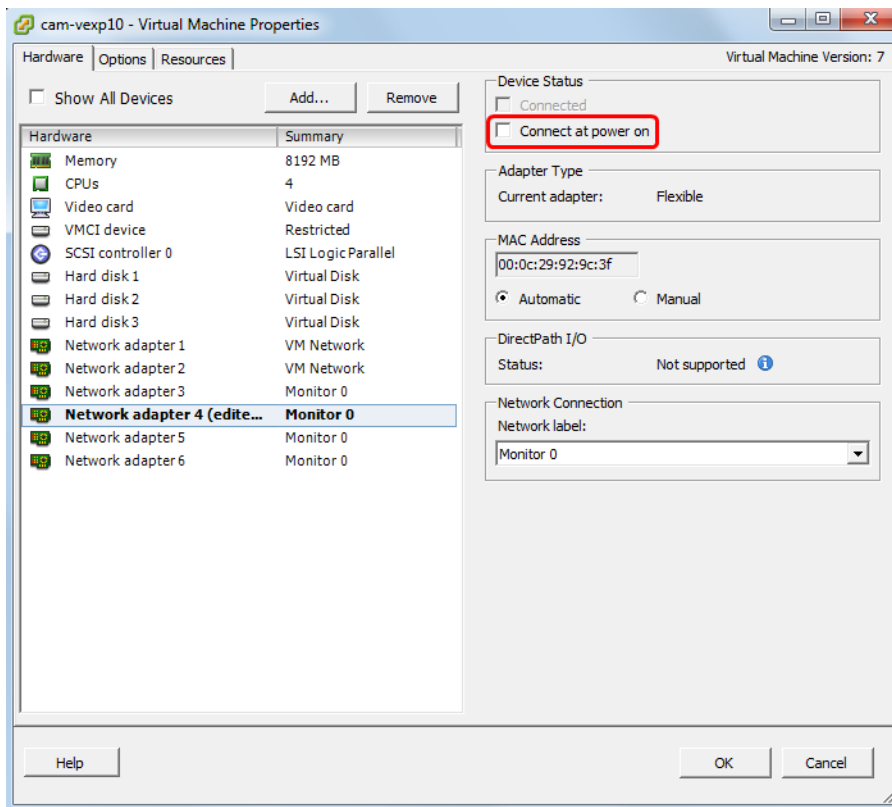
This opens the Virtual Machine Properties page for the NetExpress. The Hardware tab lists the virtual hardware components. The network adapters for the NetExpress ports are identified as follows:

- Network adapter 1 - Primary management port
- Network adapter 2 - Auxiliary management port (AUX)
- Network adapter 3 - Monitoring port 0 (Mon 0)
- Network adapter 4 - Monitoring port 1 (Mon 1)
- Network adapter 5 - Monitoring port 2 (Mon 2)
- Network adapter 6 - Monitoring port 3 (Mon 3)

For this installation example, network adapter 3 is left at its default setting of **Connect at power on**. This results in NetExpress monitoring port 0 (Mon 0) being connected to the monitoring port group.

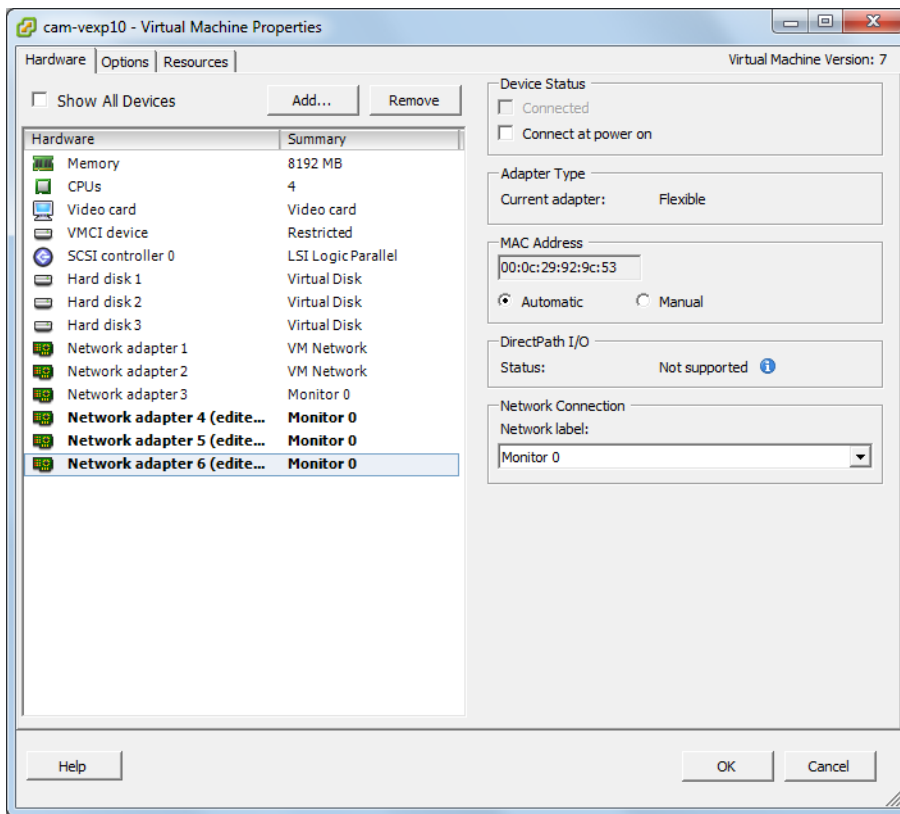


2. Select network adapter 4 and deselect the **Connect at power on** setting.



3. Select network adapters 5 and 6 individually and deselect the **Connect at power on** setting for each.

- With network adapters 4, 5 and 6 set to not connect at power on, click **OK** to make the change take effect.



This completes port configuration.

Adding virtual disks

The NetExpress virtual appliance is preconfigured with one virtual disk, which is the system disk. A second and a third must be added. The second virtual disk is automatically used for flow data storage. The third is automatically used for packet storage.

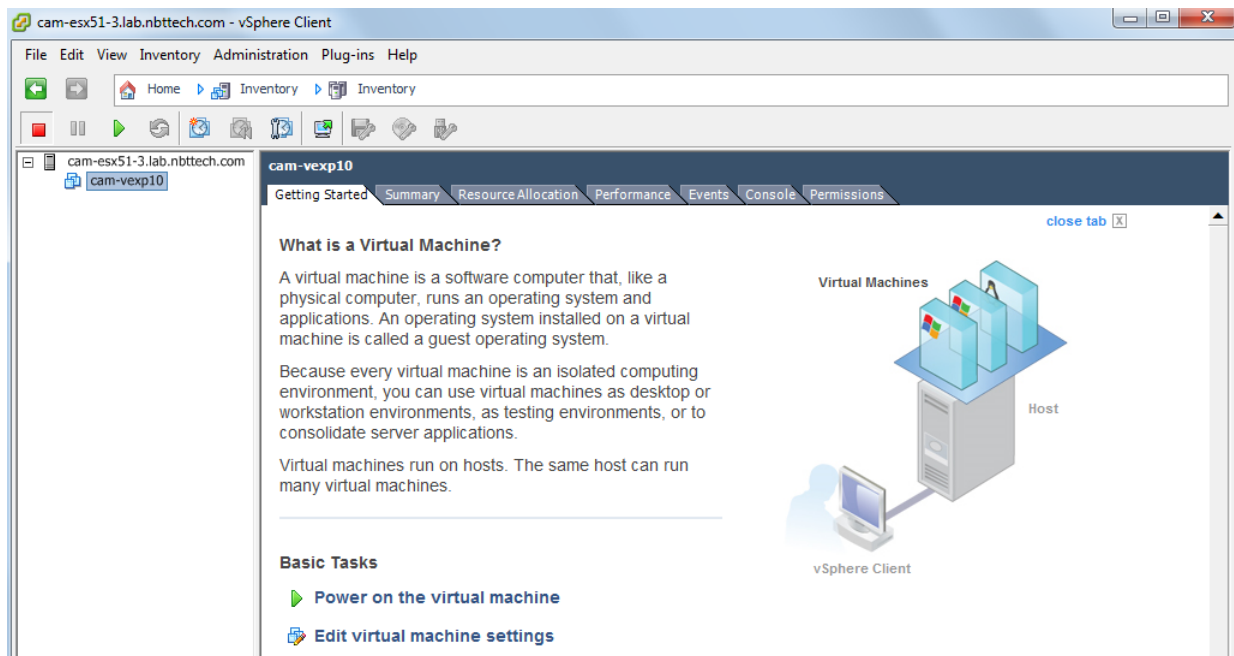
It is recommended that the second and third virtual disks be “thick provisioned.” Both must provide at least 250 GB of storage. For additional storage capacity, the NetExpress can use up to 4 TB on each drive.

The disks can be specified with different storage capacities. Otherwise, the procedure for adding them is the same.

Adding a disk for flow data storage

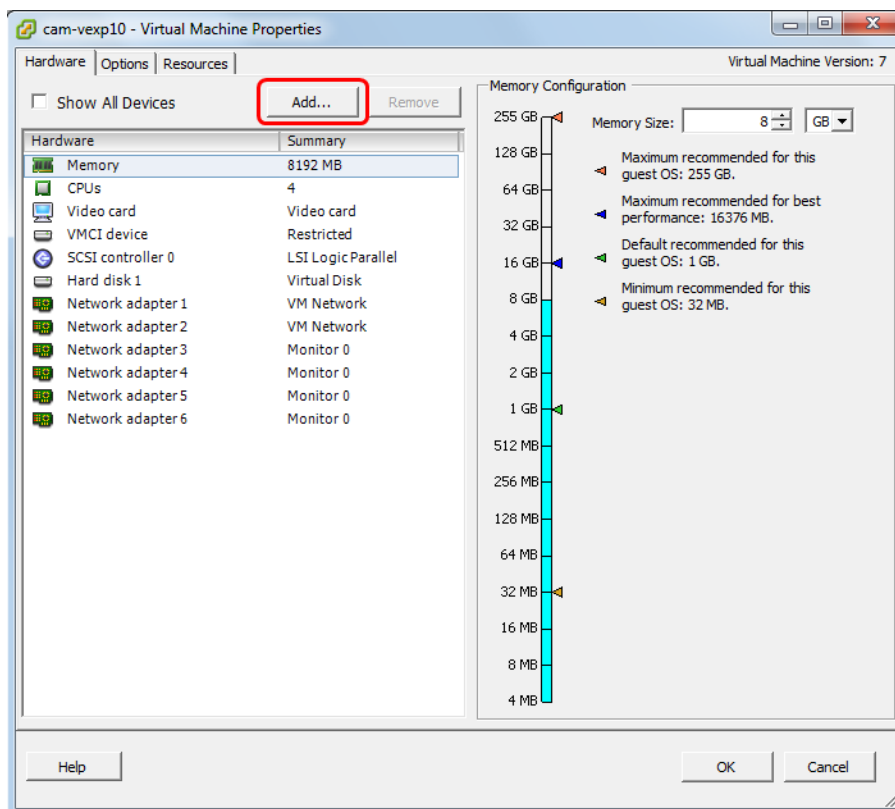
Add a second virtual disk for flow data storage as follows:

- Use the vSphere client to log in to the ESXi host and select the virtual machine (the NetExpress virtual appliance).
- In the Basic Tasks section of the Getting Started tab for the NetExpress, ensure that the NetExpress is powered off and click **Edit virtual machine settings**.

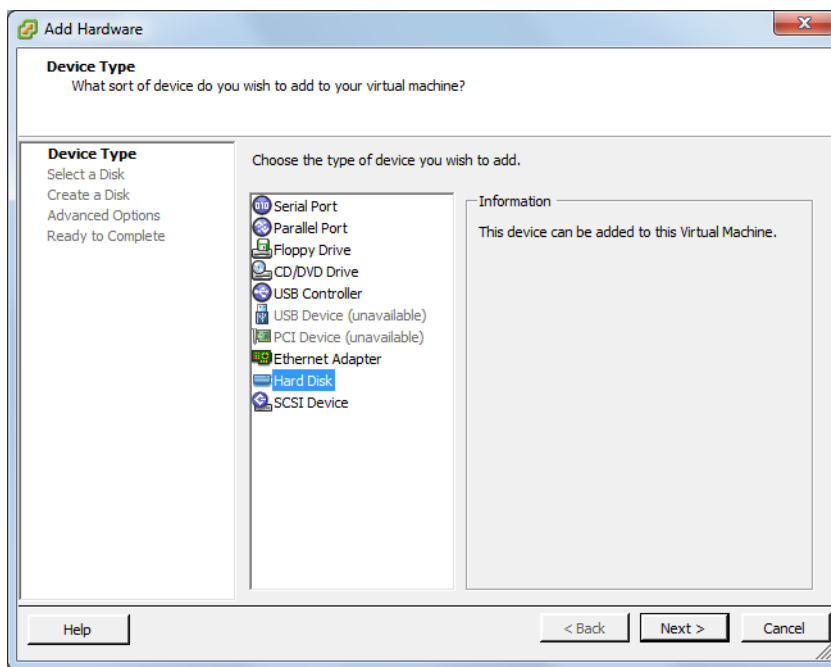


This opens the Virtual Machine Properties page.

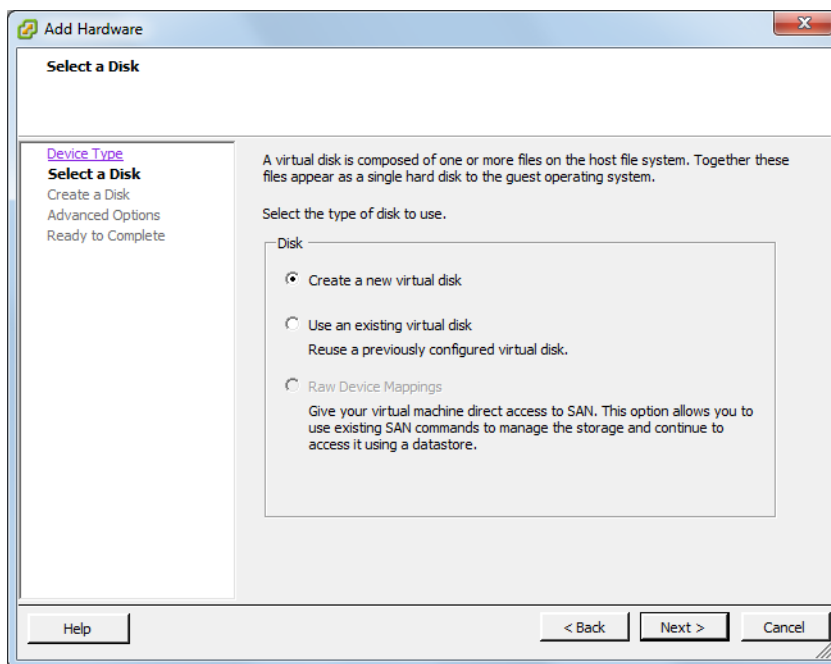
3. On the Hardware tab of the Virtual Machine Properties page, click **Add** to start the Add Hardware wizard.



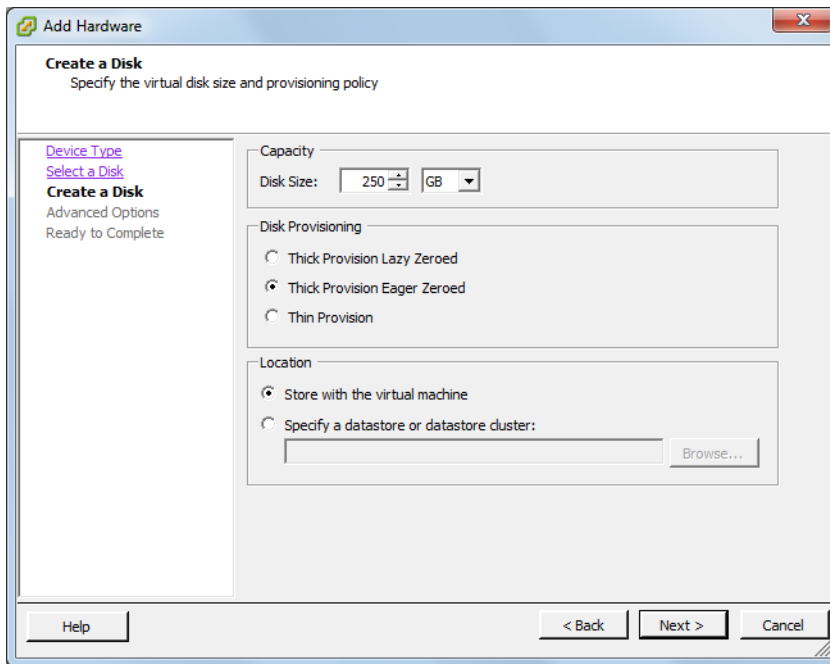
- On the Device Type page, select **Hard Disk** and click **Next**.



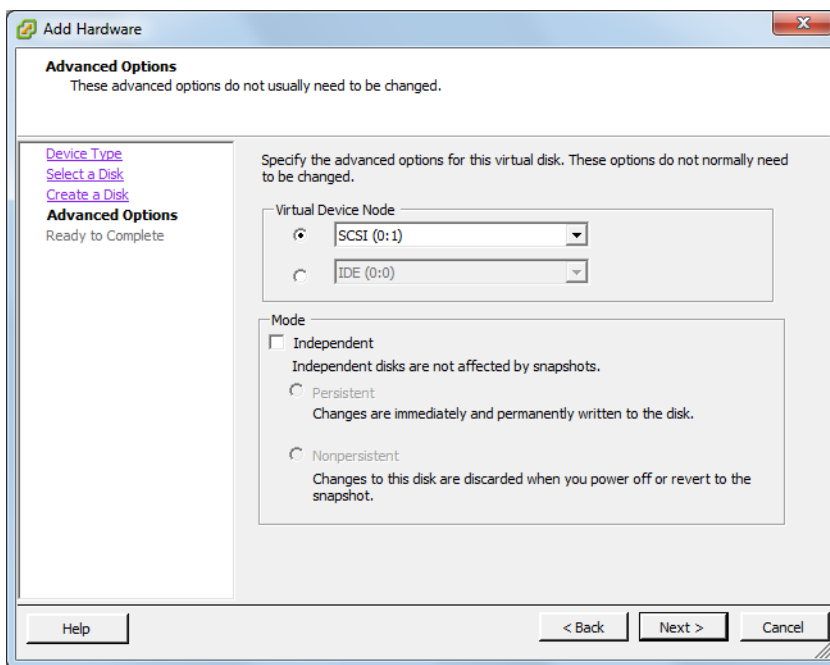
- On the Select a Disk page, select **Create a new virtual disk** and click **Next**.



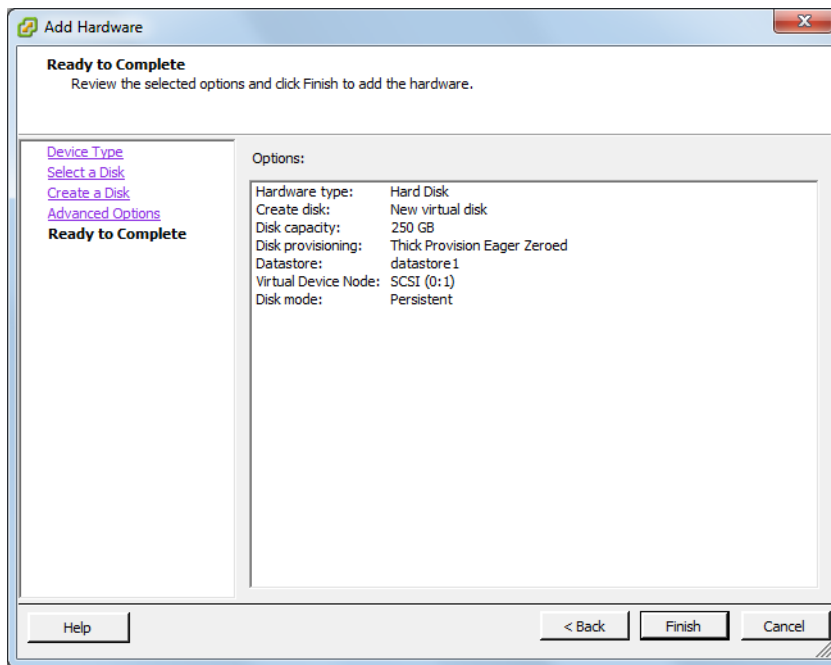
- On the Create a Disk page, enter a size for the flow data storage disk, select **Thick Provisioning Eager Zeroed**, and select the location of the disk. You can store the disk with the virtual machine, or you can specify a different datastore. This example specifies only 250 GB of disk space for flow data storage and chooses to store the flow data with the virtual machine. If you specify a large amount of storage, such as 1 TB or 2 TB, you might want to locate it on a separate datastore that might be faster or have more storage available.



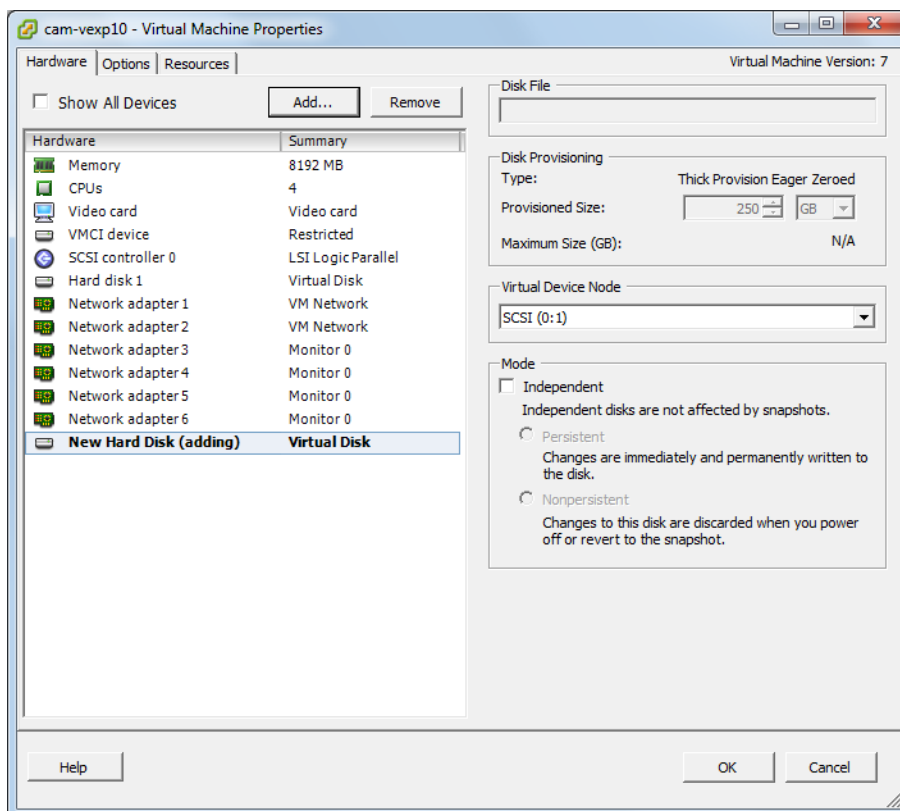
- On the Advanced Options page, use the default setting for the Virtual Device Node. Also, ensure that the Mode settings are the same as those of the system disk. By default, the system disk is **not** set to **Independent** mode.



8. On the Ready to Complete page, click **Finish** to create the virtual hard disk.



9. The Virtual Machine Properties page shows the new virtual disk that is ready to be added. Click **OK** to add it.



The Add Hardware wizard adds the new virtual disk and exits to the main window.

Adding a disk for packet storage

The procedure for adding a disk for packet storage is the same as for adding a disk for flow data storage. Follow the procedure described in the preceding section.

Verifying the additional storage

When you have added the third disk, you can verify that the disks have been added by checking the Summary tab.

The screenshot displays the vSphere Web Client interface for a virtual machine named 'cam-vexp460-101'. The left sidebar shows a tree view of the environment, including the host 'cam-esx50-4.lab.nbttech.com' and several VMs: 'cam-vexp460-101', 'cam-vgw101', 'cam-vpro101', and 'cam-vshark101'. The main panel shows the 'Summary' tab for the selected VM.

General

- Guest OS: Other 2.6.x Linux (64-bit)
- VM Version: 7
- CPU: 4 vCPU
- Memory: 8192 MB
- Memory Overhead: 296.79 MB
- VMware Tools: Running (3rd-party/Independent)
- IP Addresses: 10.38.12.73
- DNS Name: cascade-express-VE
- State: Powered On
- Host: cam-esx50-4.lab.nbttech.com
- Active Tasks:
- vSphere HA Protection: N/A

Resources

- Consumed Host CPU: 294 MHz
- Consumed Host Memory: 2497.00 MB
- Active Guest Memory: 81.00 MB
- Provisioned Storage: 933.05 GB
- Not-shared Storage: 933.05 GB
- Used Storage: 933.05 GB

Storage

Storage	Drive Type	Capacity
cam-esx50-4: vms...	Non-SSD	4.54 TB

Network

Network	Type
Monitor 0	Standard port group
VM Network	Standard port group

Commands

- Shut Down Guest
- Suspend
- Restart Guest
- Edit Settings
- Open Console

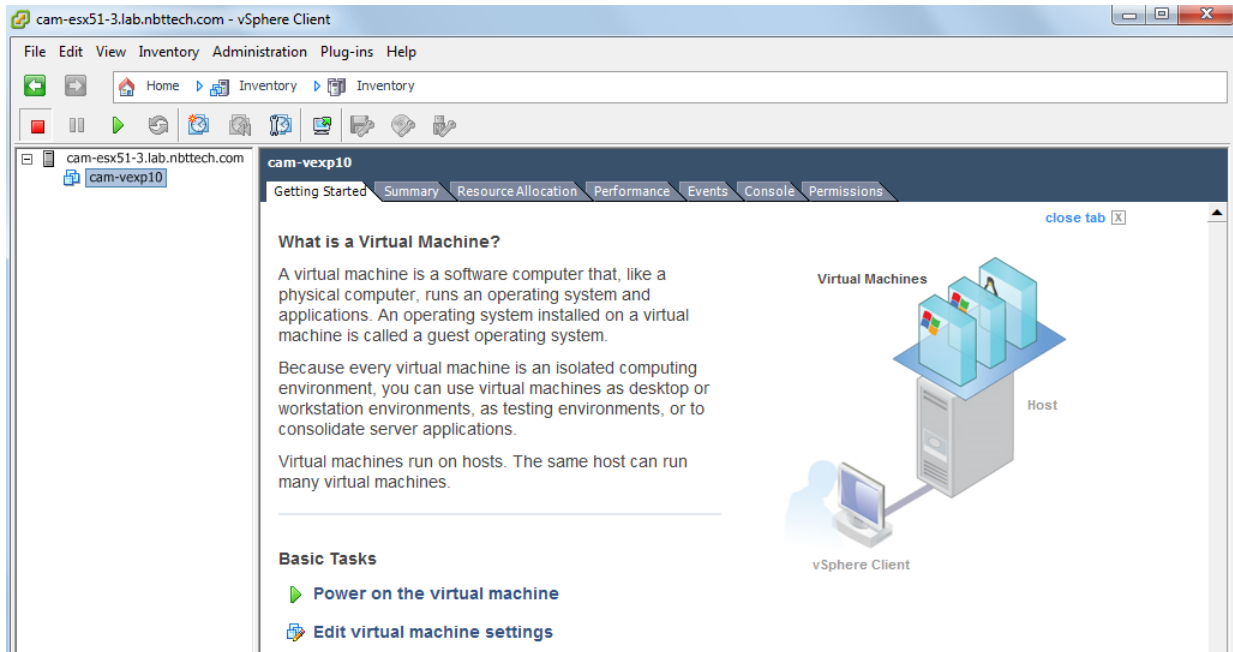
Annotations

Notes: Riverbed Cascade provides advanced network and application performance analysis and visibility.

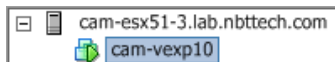
Powering on the virtual machine

To power on the NetExpress virtual appliance,

1. Use the vSphere client to manage the ESXi host and select the virtual machine (the NetExpress virtual appliance).
2. In the Basic Tasks section of the Getting Started tab for the NetExpress, click **Power on the virtual machine**.



3. Verify that the icon for the NetExpress in the navigation pane displays a green arrow. This indicates that the NetExpress is powered on.



CHAPTER 5 **Configuring the NetExpress**

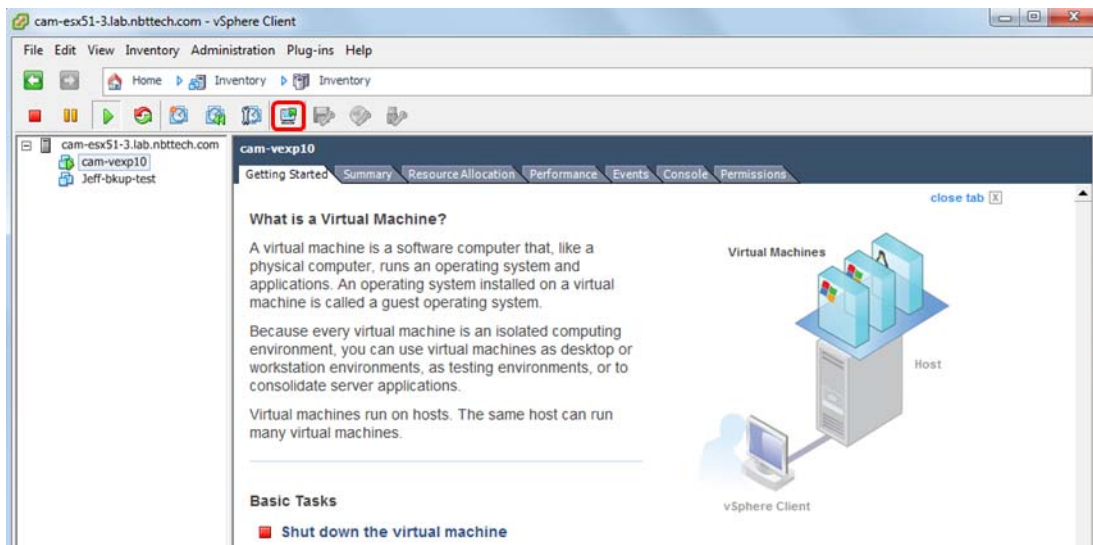
Configuring the NetExpress includes:

- Assigning a network address - Using the vSphere client to access the NetExpress console port and set up the NetExpress to be accessible over the network.
- Initial setup - Using the NetExpress web user interface to complete further configuration tasks if necessary before activating the licenses.
- Activating licenses - Activating your feature and capacity licenses.

Assigning a network address

Assign the NetExpress management IP address and subnet mask as follows:

1. Use the vSphere client to log in to the ESXi host and select the NetExpress virtual appliance.
2. Ensure that the NetExpress is powered on and selected in the navigation tree.
3. Launch a NetExpress console session either from the right-click menu off the virtual machine icon or from the console launch button on the vSphere client.



4. The first time you open a console session with the NetExpress, it starts the initial setup wizard. Log in to the NetExpress console using the default user name and password:

Login: **admin**

Password: **admin**

Note: The console admin account should be used only during initial setup. Once the NetExpress is set up, use the mazu account to log in.

5. Enter the required information at the prompts. Use your keyboard's Up Arrow to choose an IPv4 address or an IPv6 network to pre-populate the Management address field. For IPv6, add the host address before the prefix length. A typical configuration dialog proceeds as follows:

Welcome to SteelCentral Setup!

Configuring SCNE-VE with serial number 00000000000000

Press up arrow to access these addresses or ctrl+c to restart

Discovered IPv4 address 10.38.136.55/18

Discovered IPv6 network 2600:809:200:1a02:/64

Please enter the MGMT IP ADDRESS

ip/prefixlen: **2600:809:200:1a02:100:0:a26:8837/64**

Please enter the GATEWAY IP ADDRESS

ip: **2600:809:200:1a02::1**

Please enter the password for the mazu, dhcp, root, and admin shell users: *****

Please re-enter the password: *****

New Settings:

Product:	SCNE-VE
IP Address:	2600:809:200:1a02:100:0:a26:8837/64
Gateway:	2600:809:200:1a02::1

NOTE: Setup will conclude with a reboot of this SteelCentral device. After all modules have rebooted, setup can be completed by logging into the UI at [https://\[2600:809:200:1a02:100:0:a26:8837\]/](https://[2600:809:200:1a02:100:0:a26:8837]/)
Login as admin/admin.

NOTICE: All existing settings and logs will be lost.

Finish Setup and Reboot? (yes/no): **yes**

Working.....

6. Check to ensure that the settings have been entered correctly and then enter “yes” to reboot the NetExpress.
7. Wait for the reboot to complete. This takes several minutes. If you lose the mouse cursor while working in the console interface, you can restore it by entering Ctrl+Alt.
8. When the NetExpress finishes rebooting, the console window displays the login prompt. This indicates that the NetExpress is installed and ready for you to access using the web user interface. Exit from the console session, exit from the vSphere client, and log into the web user interface using the IP address you just assigned.

Do not use the console admin account except for this setup procedure. After this setup, use the mazu account if you need to log in to the console or command line interface.

Initial setup

The first time you log in to the NetExpress web user interface, the software displays a setup page. Parts of this page are prepopulated with the IP address, subnet mask, and default gateway that you specified using the console session in the previous step. This may be all you need to complete the installation. However, you can specify the rest of the initial configuration information at this time.

1. On the management network, point your web browser to the IP address you assigned in the setup wizard using the console port.

`https://<NetExpress_IP_address>`

2. Log in to the NetExpress web user interface. The default credentials are:

- User name: **admin**
- Password: **admin**

The first time you log in to the NetExpress web user interface, it displays the Setup page.

3. On the Setup page, ensure that all the required fields (marked with an asterisk) are filled in.

Management Interface Configuration

*Hostname: <input type="text" value="qa-profiler"/>		Specify the hostname and other management interface information for the NetProfiler. Use this information to log in to the NetProfiler after it is fully configured.
*IP addresses:	IPv4	
	Address: <input type="text" value="10.38.132.108"/>	
	Netmask: <input type="text" value="255.255.192.0"/>	
	Gateway: <input type="text" value="10.38.128.1"/>	
	IPv6	
	Address: <input type="text" value="2600:809:200:1a02:100:0:a26:846c"/>	
	Prefixlen: <input type="text" value="64"/>	
	Gateway: <input type="text" value="2600:809:200:1a02:1::1"/>	
	Link local: <input type="text" value="fe80::20e:b6ff:fe7a:4e8/64"/>	
	Dynamic: <input type="text"/>	
Management settings: <input type="button" value="Auto Negotiate"/> <input type="button" value="Current status: 1000, Full, On, Link detected, Twisted pair"/>		

4. Fill in the additional information, as necessary:

- Name Resolution - whether to use DNS resolution for hosts reported by the NetExpress and, if so, the addresses and search domains for the DNS servers.

Name Resolution

Search domains:	<input type="text" value="lab.nbtttech.com,nbtttech.com"/>	For resolution of unqualified names, enter the suffix to append for DHCP/DNS searches. You can enter multiple domains as a comma-separated list.
<input checked="" type="checkbox"/> Enable DNS name resolution.	<input type="button" value="Edit /etc/hosts..."/>	
Primary DNS IP address:	<input type="text" value="10.38.130.25"/>	Specify the DNS server that the NetExpress uses to look up hostnames.
Secondary DNS IP address:	<input type="text" value="10.38.131.27"/>	
Hosts name resolution:		
<input checked="" type="checkbox"/> Enable DNS name resolution for hosts.	Resolve host names for only the first <input type="text" value="500"/> hosts in any one table or graph.	
	Send no more than <input type="text" value="500"/> DNS lookup requests at a time.	
<input checked="" type="checkbox"/> Enable DHCP name resolution for hosts managed by DHCP.	Available with DHCP integration.	
<input type="radio"/> IPv4 take precedence over IPv6	<input checked="" type="radio"/> IPv6 take precedence over IPv4	
Network devices name resolution:		
<input checked="" type="checkbox"/> Enable SNMP name resolution for network devices.	Available with SNMP integration. <input type="button" value="Global SNMP Settings..."/>	
<input checked="" type="checkbox"/> Enable DNS name resolution for network devices.		
Refresh data every <input type="text" value="1"/> Week(s)	<input type="button" value="Clear device DNS cache"/>	
<input checked="" type="radio"/> SNMP names take precedence over DNS	<input type="radio"/> DNS names take precedence over SNMP	

- **Auxiliary Interface** - Optionally, the Auxiliary port can be configured. This is useful if you want to keep network data and network control traffic on separate networks.

AUX Interface Configuration

Configure AUX Interface: ☒

AUX Addresses:

IPv4	IPv6
Address: 1.2.3.4	Address:
Netmask: 255.255.255.192	Prefixlen:
	Link local: fe80::20e:b6ff:fe53:58a1/64
	Dynamic:

AUX Settings: Auto Negotiate

- **Static Routes** - If there are multiple subnets on the Auxiliary interface network, or if you need to use a gateway router other than the default gateway, it may be necessary to define static routes. Use the Static Routes section to specify static routes as necessary.

Static Routes

Network	Prefixlen	Gateway
1.2.3.0	26	1.2.3.4

[Edit Static Routes...](#)

- **Monitor Interface Configuration** - The network monitoring ports, which are labeled Mon0 and Mon1, must be configured for the speed of the tap or mirror ports they use on the monitored network. The traffic monitoring ports are preconfigured to auto-negotiate.

Monitor Interface Configuration

mon0_0 settings:	Auto Negotiate	Current status: 100, Half, On, Link detected, Twisted pair
mon0_1 settings:	Auto Negotiate	Current status: speed?, duplex?, On, No link, Twisted pair
mon0_2 settings:	Auto Negotiate	Current status: speed?, duplex?, On, No link, Twisted pair
mon0_3 settings:	Auto Negotiate	Current status: 1000, Full, On, Link detected, Twisted pair

- **Packet Deduplication** - If you believe that your network configuration might cause the NetExpress to see duplicated packets, you should enable packet deduplication.

Packet Deduplication

☒ Enable packet deduplication. Enable packet deduplication if your network configuration might cause the SteelCentral appliance to see duplicated packets.

- **Time Configuration** - The time zone is required. The NTP server IP addresses apply only if the NetExpress is being synchronized to an external NTP server.

Time Configuration

Time Zone: America/New_York

☒ Synchronize to an external NTP server

IP Address	Encryption	Key	Index	Action
10.38.130.25	N/A			Delete
10.38.131.27	N/A			Delete

[Add new NTP server](#)

☐ Use local clock: Jun 13, 2016 12:12:23 PM [Set System Time](#)

You can either configure the NetExpress to synchronize with an external NTP server (recommended) or use the NetExpress's local clock. If you would like to use the local clock, you can set the system time now.

- **Data Sources** - The NetExpress can be configured to receive traffic flow information from devices using NetFlow (versions 1, 5, 7 and 9), SteelFlow Net, CascadeFlow, IPFIX, sFlow (versions 2, 4 and 5), and Packeteer (versions 1 and 2). You can specify one or more ports in a comma-separated list for each type of flow data, up to a combined total of 50 ports.

You can also exclude data sources. NetExpress ignores data sent to it from addresses listed in the Excluded Sources box. For example, it drops NetFlow data sent to it from a router whose address is listed in the Excluded Sources box.

When the NetExpress is configured to use the Aux and Management interfaces on separate networks, use the **Allow on interface** option to control which interface is to receive traffic flow data.

Data Sources

<input checked="" type="checkbox"/> Use NetFlow/IPFIX Port: <input type="text" value="2003, 2055"/>	<p>The NetExpress can be configured to receive traffic flow information from NetFlow (versions 1, 5, 7 and 9), IPFIX, sFlow (versions 2, 4 and 5), and Packeteer (versions 1 and 2). Specify one or more ports in a comma-separated list for each type of flow data, up to a combined total of 50 ports. Do not assign a port to receive more than one type of flow data. That is, each port can be listed only once. The combined capacity of these data sources is 90,000 flows/minute. The common default ports for NetFlow are 2055, 9555, 9995 and 9996.</p>
<input checked="" type="checkbox"/> Use sFlow Port: <input type="text" value="6343"/>	
<input checked="" type="checkbox"/> Use Packeteer Port: <input type="text" value="9800"/>	
Allowed on interface: <input checked="" type="checkbox"/> Management <input type="checkbox"/> AUX	
Excluded Sources: <input type="text"/>	

- **SNMP MIB Configuration** - NetExpress is set by default to use SNMP Version 1 and to allow MIB browsing. If you are configuring SNMP at this time, obtain the necessary V1 or V3 information.

SNMP MIB Configuration

Location:	<input type="text"/>	<p>The NetExpress MIB can be browsed by external applications and devices. The NetExpress supports V1, V2C and V3 clients but can only be configured to support one type of client at a time. To limit support to SNMP V1 and V2C clients, fill out the Community String, Location, Description, and Contact fields. To support SNMP V3 clients also fill out the authentication and optional privacy information.</p>
Description:	<input type="text"/>	
Contact:	<input type="text"/>	
SNMP version:	<input type="radio"/> V1 <input checked="" type="radio"/> V2C <input type="radio"/> V3 <input type="radio"/> Off	
Community:	<input type="text" value="....."/>	
Username:	<input type="text"/>	
Security level:	<input type="text" value="No Authentication/No Privacy"/>	
Authentication passphrase:	<input type="text"/>	
Authentication protocol:	<input type="text"/>	
Privacy passphrase:	<input type="text"/>	
Privacy protocol:	<input type="text"/>	
Maximum length of lists attached to traps:	<input type="text" value="10"/>	

- **Inside Address Configuration** - IP addresses or address ranges of hosts that the NetExpress is to track individually. The default values are 10/8,172.16/12,192.168/16.

Inside Address Configuration

Inside addresses: <input type="text" value="10/8, 172.16/12, 192.168/16"/>	<p>The Inside Address Configuration allows you to specify the "Inside" of your network. Please configure all ranges of addresses (from /32 to /0) that belong inside your network including your public IP Address space and all reserved address space. Addresses that are not included in this definition will not be grouped within Host Groupings and won't be considered by the security module (if enabled) for security policies.</p>
(e.g., "10/8, 172.16/12, 192.168/16")	

- **Service Management** - Leave this set to **ByLocation** unless you are required to choose another group type for service locations.

Service Management

The location-based group type to use for your services: <input type="text" value="ByLocation"/>	<p>The locations in this group type will be used to organize end user systems on dashboards and in reports, allowing you to track performance metrics on a per location basis. This group type will be applied to all service definitions. See the documentation for details on best practices for choosing an appropriate group type and for consequences of switching group types once services are defined.</p>
--	--

5. After you have filled in all necessary fields, click **Configure Now** at the bottom of the page to apply your changes.

6. Enter a new password when prompted. After you enter the new password, your browser session is closed while the configuration changes are made. This requires approximately 5 minutes. Then you can log back in using the new password and activate your licenses.

Activating licenses

When you purchase an NetExpress, your purchase confirmation email includes a license request token. The NetExpress uses this token to generate a license request key, which you use to obtain license keys from the Riverbed licensing portal.

When you enter the license activation code on the Riverbed licensing portal, the portal generates a license key for each license you have purchased. You copy these keys and enter them on the NetExpress licensing page to activate the licenses features.

Obtaining license keys from the licensing portal

To get the license keys for the features you have purchased,

1. Log in to the NetExpress web user interface.
2. Navigate to the Configuration > Licenses page.

Licenses ?

License Updates

Updates have not been retrieved yet. [Fetch Updates now](#)

☐ Enable Automatic License Download from Riverbed

License Request

License request token: [Request key](#)

How to generate license keys ?

Licenses

[Add license\(s\)](#)
[Delete selected](#)

<input type="checkbox"/> License key +	Description	Device serial number	Installed date	Status
<input type="checkbox"/> LK1-MSPECSCNEV470FLOW5-0000-0000	NetExpress 470 Flow Limit (120K flows)	N/A	May 31, 2016	●
<input type="checkbox"/> LK1-CPEL-0000-0000		N/A	May 31, 2016	●
<input type="checkbox"/> LK1-CPEL#2+00000000-0000-0000	Packet Analyzer Concurrent License (2 pack)	N/A	Jun 1, 2016	●

Pilot Concurrent Licenses

Total: 2 | Available: 2 | In use: 0

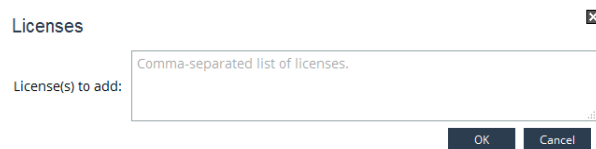
3. Paste or enter your license request token in the **License request token** field and click **Request key**. The NetExpress generates a license request key (activation code) and displays it in a popup window.
4. Copy the activation code.
5. Go to the Riverbed licensing portal at: <https://support.riverbed.com/content/support/licensing.html>
6. Paste or enter your activation code into the **Enter Unique Product Identifier** field and click **Next**.

7. Follow the instructions in the licensing wizard. The licensing portal activates all the licenses that you purchased on the order for which you received the token.
8. When the process is complete, copy the license keys from the list. These must be entered in the NetExpress.

Entering license keys in the NetExpress

Enter your license keys in the NetExpress to activate the licenses you have purchased.

1. Log in to the NetExpress web user interface.
2. Navigate to the Configuration > Licenses page and click **Add license(s)** in the Licenses section. This opens a popup window for entering the license keys.



3. Enter the license keys as a comma-separated list and click **OK**.

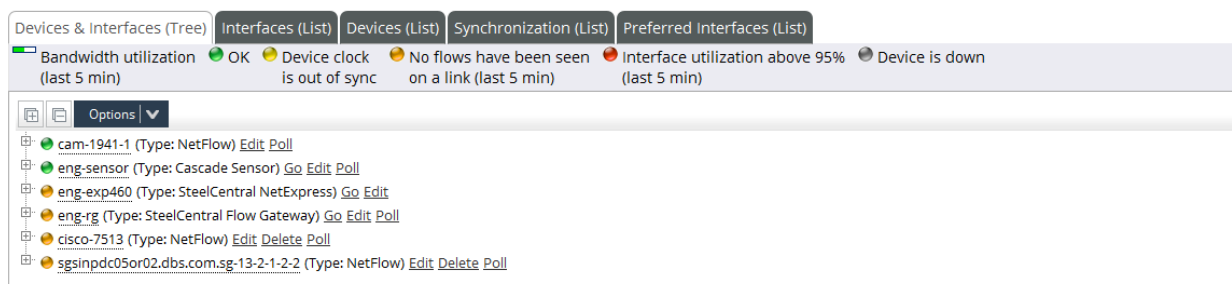
The NetExpress activates the licenses and displays them in a list. If your web user interface session is terminated when the new licenses are activated, log back in and navigate to the Configuration > Licenses page.

4. Review the list of licenses if necessary.

CHAPTER 6 Verifying the installation

Installation verification requires the NetExpress to be receiving traffic data from at least one source. To determine if the NetExpress is receiving data, log in to the web user interface and navigate to the System > Devices/Interfaces page. Check the status of the data source devices on the Devices tab. When a data source comes on line, the NetExpress begins collecting data.

Devices/Interfaces ?



If no data sources are listed on the System > Devices/Interfaces page Devices tab, then NetExpress installation and configuration cannot be verified. Set up at least one data source device (preferably all data source devices) and then perform the installation verification as follows.

1. Go to the Dashboard page and verify that graphs are displaying data.
2. Go to the System > Information page and assure that all status indications (System, Storage, DNS Servers) are displaying **OK**.
3. Also on the System > Information page, check the flow capacity section. The flow capacity graph displays flow capacity usage when the NetExpress is receiving data.
4. Go to the System > Devices/Interfaces page and assure that each data source that is expected to be available is listed and that no status indicators are red.

This completes the installation process. The NetExpress can now be turned over to those who are responsible for setting up user accounts and operational parameters. Refer to the online help system for further configuration procedures.



Riverbed Technology
680 Folsom Street
San Francisco, CA 94107

Phone: 415.247.8800
Fax: 415.247.8801
Web: <http://www.riverbed.com>

Part Number
712-00217-06