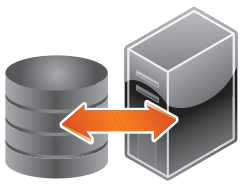
EMC® VNXe™ Series

Using a VNXe System with VMware NFS or VMware VMFS

VNXe Operating Environment Version 2.4

P/N 300-010-553
REV 04



Connect to Storage

EMC²

Published January, 2013

PREFACE

As part of an effort to improve its product lines, EMC periodically releases revisions of its software and hardware. Therefore, some functions described in this document might not be supported by all versions of the software or hardware currently in use. The product release notes provide the most up-to-date information on product features.

Contact your EMC representative if a product does not function properly or does not function as described in this document.

Note: This document was accurate at publication time. New versions of this document might be released on the EMC online support website. Check the EMC online support website to ensure that you are using the latest version of this document.

Purpose

This document is part of the EMC VNXe documentation set. It describes how to set up VMware ESX hosts to access VMware storage on a VNXe system with VNXe Operating Environment version 2.2 or later.

IMPORTANT

The VNXe VMware storage is presented directly to the ESX host and not to the host's virtual machines.

Audience

This document is intended for the person or persons who are responsible for setting up the hosts to access the VNXe storage.

Readers of this document should be familiar with VNXe VMware storage and with the ESX Server operating system running on ESX hosts that will access VNXe VMware storage.

Related documentation

Other VNXe documents include:

- *EMC VNXe3100 Hardware Information Guide*
- *EMC VNXe3100 System Installation Guide*
- *EMC VNXe3150 Hardware Information Guide*
- *EMC VNXe310 Installation Guide*
- *EMC VNXe3300 Hardware Information Guide*
- *EMC VNXe3300 System Installation Guide*
- *Using the VNXe System with CIFS Shared Folders*
- *Using the VNXe System with NFS Shared Folders*
- *Using the VNXe System with Microsoft Exchange 2007 or Microsoft Exchange 2010*
- *Using the VNXe System with Generic iSCSI Storage*

- *Using the Using the VNXe System with Microsoft Windows Hyper-V*
- *VNXe CLI User Guide*

EMC Unisphere help provides specific information about the VNXe storage, features, and functionality. The Unisphere help and a complete set of VNXe customer documentation are located on the EMC Online Support website (http://www.emc.com/vnxesupport).

Conventions used in this document

EMC uses the following conventions for special notices:

⚠DANGER

DANGER indicates a hazardous situation which, if not avoided, will result in death or serious injury.

⚠WARNING

WARNING indicates a hazardous situation which, if not avoided, could result in death or serious injury.

⚠CAUTION

CAUTION, used with the safety alert symbol, indicates a hazardous situation which, if not avoided, could result in minor or moderate injury.

NOTICE

NOTICE is used to address practices not related to personal injury.

Note: A note presents information that is important, but not hazard-related.

IMPORTANT

An important notice contains information essential to software or hardware operation.

Typographical conventions

EMC uses the following type style conventions in this document:

Normal	Used in running (nonprocedural) text for: • Names of interface elements, such as names of windows, dialog boxes, buttons, fields, and menus • Names of resources, attributes, pools, Boolean expressions, buttons, DQL statements, keywords, clauses, environment variables, functions, and utilities • URLs, pathnames, filenames, directory names, computer names, links, groups, service keys, file systems, and notifications
Bold	Used in running (nonprocedural) text for names of commands, daemons, options, programs, processes, services, applications, utilities, kernels, notifications, system calls, and man pages Used in procedures for: • Names of interface elements, such as names of windows, dialog boxes, buttons, fields, and menus • What the user specifically selects, clicks, presses, or types
Italic	Used in all text (including procedures) for: • Full titles of publications referenced in text • Emphasis, for example, a new term • Variables
`Courier`	Used for: • System output, such as an error message or script • URLs, complete paths, filenames, prompts, and syntax when shown outside of running text
`Courier bold`	Used for specific user input, such as commands
`Courier italic`	Used in procedures for: • Variables on the command line • User input variables
< >	Angle brackets enclose parameter or variable values supplied by the user
[ ]	Square brackets enclose optional values
|	Vertical bar indicates alternate selections — the bar means “or”
{ }	Braces enclose content that the user must specify, such as x or y or z
...	Ellipses indicate nonessential information omitted from the example

Where to get help

You can find VNXe support, product, and licensing information as follows:

Product information — For documentation, release notes, software updates, or information about EMC products, licensing, and service, go to the EMC online support website (registration required) at:

http://www.emc.com/vnxesupport

Technical support — For technical support, go to EMC online support. Under Service Center, you will see several options, including one to create a service request. Note that to open a service request, you must have a valid support agreement. Contact your EMC sales representative for details about obtaining a valid support agreement or with questions about your account.

Your comments

Your suggestions will help us continue to improve the accuracy, organization, and overall quality of the user publications. Send your opinions of this document to:

techpubcomments@emc.com

CHAPTER 1
Setting Up a Host to Use VNXe VMware NFS Datastores

This chapter describes how to set up a VMware ESX host or virtual machine to use EMC VNXe VMware NFS datastores.

Topics include:

Requirements for setting up a host to use VNXe VMware NFS datastores

Before you can set up a host to use VNXe NFS datastores, the following VNXe system and network requirements described in this section must be met.

VNXe system requirements

- You have installed and configured the VNXe system using the VNXe Configuration Wizard, as described in the *EMC VNXe3100 System Installation Guide*, the *EMC VNXe3150 Installation Guide*, or the *EMC VNXe3300 System Installation Guide*.
- You have used Unisphere or the VNXe CLI to perform basic configuration of one or more VNXe Shared Folder Servers on the VNXe system.

Network requirements

The host must be in a LAN environment with the VNXe Shared Folder Storage Server.

Users can store files on a VNXe Shared Folder Server in a Network Information Service (NIS) environment, but you cannot configure a VNXe Shared Folder Server as an NIS client.

Using network high availability

The VNXe system provides network high-availability or redundancy with Fail-Safe Networks (FSNs) that extend link failover out into the network by providing switch-level redundancy. On a VNXe system, each port on a storage processor (SP) is configured in an FSN with the corresponding port on the peer SP. When you assign a port to a VNXe Shared Folder Server interface, the VNXe automatically designates that port on the SP where the Shared Folder Server resides as the primary port in the FSN and the port on the peer SP as the secondary port in the FSN. You cannot create, delete, or change the configuration of the VNXe FSNs. For these reasons, to take advantage of FSN in a VNXe3100 system with two SPs, a VNXe3150 with two SPs, or a VNXe3300 system, the Ethernet (eth) ports on each SP must be cabled identically. For example if you cable eth2 and eth4 ports on SP A and create a separate storage server on each port, you must cable eth2 and eth4 ports on SP B the same way.

In addition, the VNXe system supports link aggregations that allows up to four Ethernet ports connected to the same physical or logical switch to be combined into a single logical link. This behavior is called link aggregation. To configure link aggregation on a VNXe system, each storage processor (SP) must have the same type and number of Ethernet ports because configuring link aggregation actually creates two link aggregations — one on each SP. This provides high availability as follows. If one of the ports in the link aggregation fails, the system directs the network traffic to one of the other ports in the aggregation. If all the ports in the aggregation fail, FSN fails over to the corresponding link aggregation on the peer SP so that network traffic continues. If you add an Ethernet I/O module to each SP in a VNXe 3100, 3150, or 3300 system, you can create one additional link aggregation group on the set of ports in the I/O module.

The rest of this section describes:

- “Fail-Safe Networks” on page 11
- “Link aggregations” on page 12

- "Configuring a link aggregation" on page 12

For additional information on data availability in your VNXe system and your connectivity infrastructure, refer to the *EMC VNXe High Availability Overview* in the White Papers section of the VNXe support website (http:\\emc.com\vnxesupport).

Fail-Safe Networks

A Fail-Safe Network (FSN) is a high-availability feature that extends links failover into the network by providing switch-level redundancy. An FSN appears as a single link with a single MAC address and potentially multiple IP addresses. On a VNXe system, an FSN consists of one port on one SP and the corresponding port on the other SP. Each port is considered a single connection. Both connections making up the FSN share a single hardware (MAC) address. If the VNXe system detects that the active connection fails, it automatically switches to the standby connection in the FSN, and that connection assumes the network identity of the failed connection.

To ensure host connectivity to the VNXe system in the event of a hardware failover, connect the VNXe system to different switches that are connected to FSN devices on multiple NICs in the host. As a result, the FSN components are connected to different switches. If the switch for the active connection fails, the FSN fails over to a connection using a different switch, thus extending link failover out into the network.

As shown in Figure 1, when the VNXe SP detects loss of the active communications link to the FSN, the connection automatically fails over to an operational standby connection. This action is independent of any switch features. If a connection in the FSN goes down, the link fails over to the surviving link. If both connections in an FSN fail, the link is down.

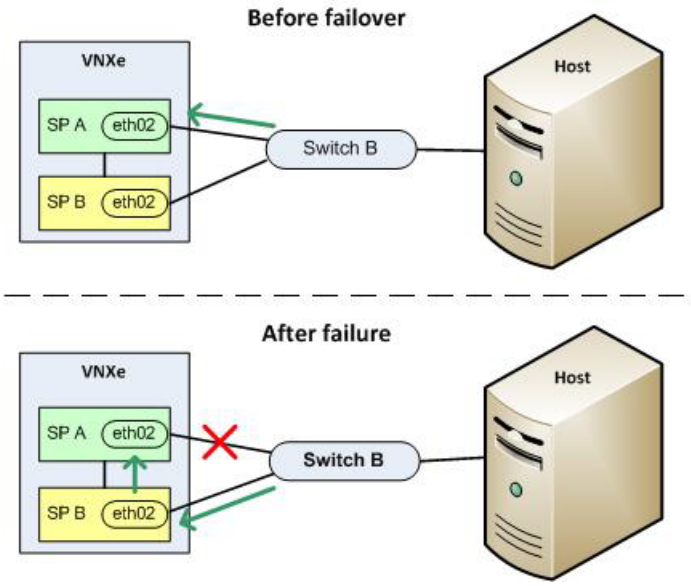


Figure 1 Failover with Fail-Safe Networking

Link aggregations

Link aggregations use the Link Aggregation Control Protocol (LACP) IEEE 802.3ad standard. A link aggregation appears as a single Ethernet link and has the following advantages:

- High availability of network paths to and from the VNXe system — If one physical port in a link aggregation fails, the system does not lose connectivity.
- Possible increased overall throughput — Because multiple physical ports are bonded into one logical port with network traffic distributed between the multiple physical ports.

Although link aggregations can provide more overall bandwidth than a single port, the connection to any single client runs through one physical port and is therefore limited by the port's bandwidth. If the connection to one port fails, the switch automatically switches traffic to the remaining ports in the group. When the connection is restored, the switch automatically resumes using the port as part of the group.

On the VNXe system, you can configure up to four ports in a link aggregation. When you configure a link aggregation, you are actually configuring two link aggregations — one on each SP. If one of the ports in a aggregation fails, the system directs network traffic to one of the other ports in the group. If all the ports in the group fail, FSN fails over to the corresponding link aggregation on the peer SP.

Switch requirements

If the VNXe ports are connected to different network switches, you should configure all switch ports connected to the VNXe ports to immediately switch from blocking mode to forwarding mode and not pass through spanning tree states of listening and learning when an interface comes up. On Cisco switches, this means that you must enable the portfast capability for each switch port connected to a VNXe port to guarantee that the switch forwards the Ethernet frame that the VNXe system generates when a physical link is enabled. You enable the portfast capability on a port-to-port basis, When enabled, the portfast variable causes the port to immediately switch from blocking to forwarding mode. Do *not* use portfast on switch-to-switch connections.

For link aggregation, network switches must have IEEE 802.3ad protocol support and guarantee that packets from a single TCP connection always go through the same link in a single direction.

Configuring a link aggregation

For link aggregation, you have at least one 802.3ad-compliant switch, each with an available port for each switch port you want to connect to a VNXe port in the aggregation.

Note: The term *NIC teaming* refers to all NIC redundancy schemes, including link aggregation with 802.3ad.

For link aggregation, you need to perform two sets of configuration tasks:

- "Configuring link aggregation from the switch to the VNXe system" on page 13
- "Configuring link aggregation from the ESX host to the switch" on page 13

Configuring link aggregation from the switch to the VNXe system

1. Configure the switch ports, which are connected to the VNXe, for LACP in active mode, as described in the documentation provided with your switches.
2. Join the VNXe ports into a link aggregation using the Unisphere Advanced Configuration option (**Settings › More configuration › Advanced Configuration**). For information on using the Advanced Configuration option, refer to the Unisphere online help. Two link aggregations are created with the same ports — one aggregation on each SP.

Configuring link aggregation from the ESX host to the switch

To configure link aggregation from the ESX host to the switch, perform these tasks:

- "Task 1: Configure switch ports for link aggregation" on page 13.
- "Task 2: Set up NIC teaming on the ESX host" on page 13

Task 1: Configure switch ports for link aggregation

Configure the switch ports, which are connected to the ESX host for link aggregation.

NOTICE

Depending on the type of NIC teaming used, you may not need to configure these switch ports for link aggregation. For more information, refer to your VMware documentation.

Task 2: Set up NIC teaming on the ESX host

On an ESX host, you create a NIC team by creating a virtual switch with two or more physical NICs. For information on creating a virtual switch, refer to the VMware documentation for the version of ESX running on the host.

Configuring VNXe NFS datastores for the host

Use Unisphere or the VNXe CLI to:

1. Discover VMware ESX and/or ESXi hosts.
2. Create VNXe NFS datastores.

IMPORTANT

When you create VNXe NFS datastores for discovered VMware ESX and/or ESXi hosts, the VNXe system automatically configures the hosts to use the datastores. If you select multiple discovered hosts for the datastores, all the selected hosts are configured automatically. If an ESX or ESXi host cannot see the NFS datastore after you create the datastore, go to "Manually setting up the connection to a VNXe NFS datastore" on page 14.

For information on performing these tasks refer to the Unisphere online help.

Configuring user and group access to the NFS datastore

Use the steps below to adjust permissions for best security in an environment where the connections from a VNXe system to the ESX hosts are not on a separate physical or virtual network. If you are using an isolated storage network for these connections, the step below may not be required.

1. Log in as root to an ESX host with **Read/Write, allow Root** access to the VNXe NFS datastore.

   If the VNXe datastore is not visible to the host, make sure that you are logged in to the correct domain.

2. Set up the datastore's directory and file structure.

3. Set up user and group permissions to the datastore's directories and files.

   For the best security, use the most restrictive access that is acceptable, such as not allowing root access to the share and mounting the datastore with read-only access wherever feasible.

4. For added security, change the access for the host with Read/Write, allow Root access to Use Default Access, Read-Only, or Read/Write:

   Note: You must be a member of the VNXe local Administrators group to change host access to a share.

   a. Open Unisphere and select **Storage › VMware**.

   b. Select the datastore and click **Details**.

   c. Click the **Host Access** tab and in the **Access** column for the host, select **Use Default Access, Read Only,** or **Read/Write.**

What next?

You are now ready to either migrate (relocate) a virtual disk to the VNXe NFS datastore or have the ESX host start using the NFS datastore. To migrate a virtual disk to the NFS datastore, go to Chapter 3, "Migrating VMware Virtual Machines to the VNXe System."

Manually setting up the connection to a VNXe NFS datastore

If the ESX host cannot see a VNXe NFS datastore, the VNXe system's configuration of the ESX host may not have succeeded. In this situation, you must do the following:

1. Use EMC Unisphere™ software to find the IP address of the VNXe Shared Folder Server for the NFS datastore:

   a. Select **Storage** > **VMware** and select the datastore.

   b. Select **Details › View Access Details**.

   The first part of the Export Path before the colon (:) is the IP address of the Shared Folder Server. For example, in the Export Path 10.222.3.44:/nfsdatastore2, 10.222.3.44 is the IP address of the Shared Folder Server for the datastore nfsdatastore2.

2. Log into VMware vSphere Client VI client as administrator.

3. For each NFS datastore:
   a. In the Inventory panel, select the host and click the **Configuration** tab.
   b. In the Hardware panel, click **Storage**, and then click **Add Storage**.
   c. Select **Network File System** as the file storage type, and then click **Next**.
   d. Enter the following information and click **Next**:
      – For the server — the IP address of the VNXe NFS Shared Folder Server.

        You can find this address using the Unisphere path **Settings** › **Shared Folder Server Settings**.
      – For the folder — the path to the VNXe share.
      – The name of the new VMware datastore.
   e. In the Network File System Summary page, review the configuration options for the new datastore, and click **Finish**.

Perform a rescan to make the VMware NFS datastore visible to ESX Server and verify that the datastore you created is in the datastores list that appears.

CHAPTER 2
Setting Up a Host to Use VNXe VMware VMFS Datastores

This chapter describes the requirements for setting up an ESX host to use EMC VNXe VMFS datastores, how to set up the ESX host for path management software, and how to troubleshoot the connection between the ESX host and a VNXe VMFS datastore.

Note: The procedures in this document use "ESX" to refer to "VMware ESX."

Topics include:

Requirements for setting up a host to use VNXe VMware VMFS datastores

Before you set up a host to use VNXe VMware VMFS datastores, the VNXe system and network requirements in described this section must be met.

VNXe system requirements

- You have installed and configured the VNXe system using the VNXe Configuration Wizard, as described in the *EMC VNXe3100 System Installation Guide*, the *EMC VNXe3150 Installation Guide*, or the *EMC VNXe3300 System Installation Guide*.
- You have used Unisphere or the VNXe CLI to perform basic configuration of one or more iSCSI Servers on the VNXe system.

Network requirements

For a host to connect to VMware VMFS datastores on a VNXe iSCSI Server, the host must be in a network environment with the VNXe iSCSI Server; to achieve best performance, the host should be on a local subnet with each VNXe iSCSI Server that provides storage for it. If possible, you should segment network traffic from the VNXe system through a private LAN using either a virtual LAN or a dedicated network switch.

To achieve maximum throughput, connect the VNXe iSCSI Server and the hosts for which it provides storage to their own private network, that is, a network just for them. When choosing the network, consider network performance.

Path management network requirements

Note: Path management software is not currently supported for a Windows 7 or Mac OS host connected to a VNXe system.

When implementing a highly-available network between a host and the VNXe system, keep in mind that:

- A VNXe VMware VMFS datastore is presented to only one SP at a given time
- You can configure two IP interfaces for an iSCSI Storage Server. These IP interfaces should be associated with two separate physical interfaces on the same SP.
- Network switches may be on separate subnets.

IMPORTANT

Directly attaching an ESX host to a VNXe system is not currently supported.

Figure 2 on page 19 shows a highly-available iSCSI network configuration for hosts accessing a VNXe storage resource (VMware VMFS datastore). Switch A and Switch B are on separate subnets. Host A and Host B can each access the storage resource through separate NICs. If the storage resource is owned by SP A, the hosts can access the storage resource through the paths to the eth2 interface on SP A. Should SP A fail, the VNXe system transfers ownership of the resource to SP B and the hosts can access the storage resource through the paths to the eth2 interface on SP B.

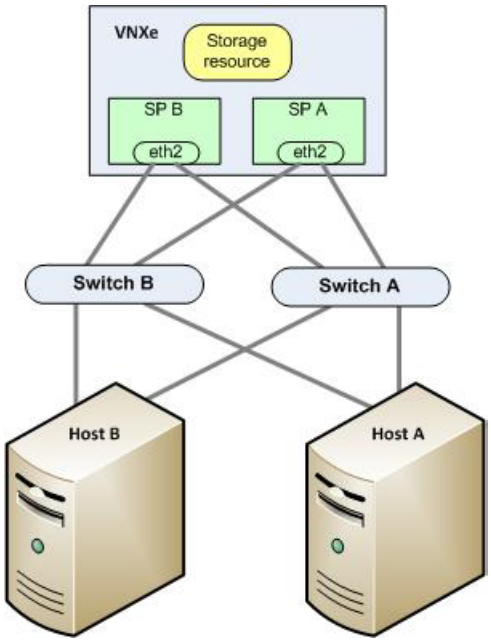


Figure 2 Sample highly-available iSCSI network

Using multi-path management software

Multi-path management software manages the connections (paths) between the host and the VNXe system to provide access to the VNXe storage should one of the paths fail. The following types of multi-path management software are available for an ESX host connected to a VNXe system:

- ESX native failover on any ESX host
- EMC PowerPath/VE software on an ESX 4, ESXi 4.x, ESXi 5, or ESXi 5.1host.

  For the supported versions of the PowerPath/VE software, refer to the VNXe EMC Simple Support Matrix for the VNXe Series on the EMC Online Support website (http://www.emc.com/vnxesupport). To find this matrix on the website, search for "Simple Support Matrix" on the VNXe Support Page.

For information on data availability in the VNXe system and in your connectivity infrastructure, refer to the *EMC VNXe High Availability Overview* in the White Papers section of the VNXe support website (http://emc.com/vnxesupport).

Setting up a VNXe system for multi-path management software

For a VNXe system to operate with hosts running multi-path management software, each iSCSI Server in the VNXe system should be associated with two IP addresses.

Use the EMC Unisphere™ Settings › iSCSI Server Settings page to verify that each iSCSI Server has two network interfaces configured, and if either iSCSI server has only one network interface configured, configure a second network interface for it. For information on configuring more than one network interface for an iSCSI Server, refer to the topic on changing iSCSI Server settings in the Unisphere online help.

IMPORTANT

For highest availability, use two network interfaces on the iSCSI Server. The network interfaces can be on separate subnets. You can view the network interfaces for an iSCSI Server with Unisphere under Network Interface advanced settings (**Settings › iSCSI Server Settings › iSCSI Server Details**).

Installing PowerPath/VE

IMPORTANT

vSphere ESX or VNXe link aggregation is not supported with PowerPath/VE.

1. On the host or virtual machine, download the latest PowerPath/VE version from the PowerPath/VE software downloads section on the EMC Online Support website (http://support.emc.com).
2. Install PowerPath/VE, as described in the appropriate PowerPath/VE installation and administration guide for the host's operating system.

   This guide is available on the EMC Online Support website. If the host or virtual machine is running the most recent version and a patch exists for this version, install it, as described in the readme file that accompanies the patch.

Creating a VMkenel port for the software iSCSI adapter

Connect the VMkernel, which runs services for iSCSI storage, to the physical network adapter:

1. Log in to the vSphere Client as an administrator.
2. From the Inventory panel, select the host.
3. Click the **Configuration** tab, and click **Networking**
4. In the Virtual Switch view, click **Add Networking**.
5. Select **VMkernel** and click **Next**.
6. Select **Create a virtual switch** to create a new vSwitch.
7. Select an adapter that you want to use for iSCSI traffic and click **Next**.

   IMPORTANT

   Do no use iSCSI on 100 Mbps or slower adapters.

   If no adapters appear under **Create a virtual switch**, the existing vSwitches are using all the network adapter in the host. In this situation, you can use an existing vSwitch for iSCSI traffic.

8. Under Port Group Properties, enter the network label, and click **Next**.

   The network label is the name that you want to identify the VMkernel port that you are creating.

9. Specify the IP settings and click **Next**.

10. After you review the summary information, click **Finish**.

What next?

If your host uses only one physical network adapter for iSCSI, your network configuration is complete.

If your host uses more than one physical network adapter for iSCSI, you must connect additional adapters to the vSwitch and associate each port with a VMkernel port using the port binding technique. You can do this in one of following ways:

- Use a single vSwitch for iSCSI multipathing by connecting the additional network adapters and VMkernel ports to the vSwitch that you just created and override the default setup so that each port maps to only one active adapter. To do this, continue to the next section, "Setting up multipathing for Software iSCSI" on page 21.
- Create separate vSwitches for each additional network adapter by repeating the previous steps 1 through 10 for each additional adapter.

Setting up multipathing for Software iSCSI

Use this procedure only if:

- You have two or more NICs that you can designate for iSCSI

  and

- You want to connect all of these iSCSI NICs to a single vSwitch.

The procedure associates VMkernel ports with the iSCSI NICs using a 1-to-1 mapping,

To set up multipathing for Software iSCSI

Before following the procedure below to set up multipathing for software iSCSI, you must have created one VMkernel port for your network adapter.

⚠CAUTION

If the network adapter that you add to the software iSCSI initiator is not in the same subnet as your iSCSI target (VNXe iSCSI Server), the host cannot establish sessions from this network adapter to the target.

1. Log in to the vSphere Client as an administrator.
2. From the Inventory panel, select the host.
3. Click the **Configuration** tab, and click **Networking.**
4. Select the vSwitch that you use for iSCSI and click **Properties**.
5. Bind additional network adapters to the vSwitch:

   a. In the vSwitch Properties dialog box, click the **Network Adapters** tab and click **Add**.

b. From the list of adapters, select the ones that you want to add to the vSwitch and click **Next**.

c. After you review the information on the summary page, click **Finish**.

The list of network adapters reappears, showing the network adapters that the vSwitch claims.

6. Create VMkernel ports for that network adapters that you connected to the vSwitch:

IMPORTANT

Each VMkernel port in a vSwitch with multiple network adapters must have only one network adapter designated as active for each VMkernel port. The other adapters must be designated as unused.

a. In the vSwitch Properties dialog box, click the **Ports** tab and click **Add**.

b. Select **VMkernel** and click **Next**.

c. Under Port Group Properties, enter a network label and click **Next**.

The network label is the name that you want to identify the VMkernel port group that you are creating.

d. Specify the IP settings and click **Next.**

When you enter the subnet mask, be sure that the network adapter are set to the subnet of the VNXe iSCSI Server to which it connects.

e. After you review the information on the summary page, click **Finish**.

7. Map each VMkernel port to just one active adapter.

By default all network adapters appear as active for each VMkernel on the vSwitch. You must override this setup so that each port maps to only one active adapter. For example, VMkernel port vmk1 maps to active adapter vmnic1, port vmk2 maps to vmnic2, and so on.

For *each* VMkernel port on the vSwitch:

a. On the **Ports** tab, select a VMkernel port and click **Edit**.

b. Click the **NIC Teaming** tab and select **Override vSwitch failover order**.

c. Specify only one adapter as active and move all the remaining adapters to the **Unused Adapters** list.

8. Connect the VMkernel ports to the software iSCSI initiator:

For ESX 4 or ESXi 4.x

Use the **esxcli swiscsi nic** command. For example to connect iSCSI ports vmk2 port to the software iSCSI adapter vmba33 and to verify the connection, use:

```
esxcli swiscsi nic add -n vmk2 -d vmhba33
esxcli swiscsi nic list -d vmhba33
```

Port vmk2 should be listed.

For ESXi 5 or ESXi 5.1

a. Log in to the vSphere Client as an administrator.

b. From the Inventory panel, select the host.

c. Click the **Configuration** tab, and click **Storage Adapters**.

d. Select the iSCSI adapter and click **Properties**.

e. Select the **Network Configuration** tab and click select.

f. Select the VMkernel ports on the vSwitch and then click **OK**.

g. Review the summary and click **Finish**.

Configure the ESX iSCSI adapters

IMPORTANT

If you want to use optional initiator CHAP authentication, you should configure CHAP authentication for the initiators (initiator CHAP) on the VNXe iSCSI Server *before* you configure CHAP authentication for the initiators on the ESX host. For information about configuring CHAP on the VNXe iSCSI Server, refer to the Unisphere online help.

1. Log in to the VMware Client or vSphere Client as an administrator.
2. From the Inventory panel, select the host with the initiator you want to configure.
3. Click the **Configuration** tab, and click **Storage Adapters**.
4. For ESXi 5 or ESXI 5.1, if the Software iSCSI adapter is not listed, click **Add** and select **Software iSCSI**.
5. Select the iSCSI adapter that you want to configure, and click **Properties**.
6. Add target addresses for the software iSCSI adapter:

   For the VNXe Operating Environment 2.2 or later

   a. Click the **Static Discovery** tab and click **Add**.

   b. In **iSCSI Server**, enter the IP address for the VNXe iSCSI Server.

   c. In i**SCSI Target Name**, enter the IQN for the VNXe iSCSI Server.

      You can find the IQN with Unisphere on the iSCSI Server Details page (**Settings › iSCSI Server Settings › iSCSI Server Details**).

   d. If you configured initiator CHAP (target authenticates host) and/or Mutual CHAP (host authenticates target, click **CHAP** and:

      For initiator CHAP (target authenticates host) — Select the option to use CHAP and enter the *same* secret that you entered for the host initiator on the iSCSI Server on the VNXe system.

      For Mutual CHAP (host authenticates target) — Select the option to use CHAP and enter the *same* secret that you entered for the iSCSI Server on the VNXe system. This secret must be different from the initiator CHAP secret.

      NOTICE

      If you select not to use CHAP, all sessions that require CHAP authentication terminate immediately.

e. Click **OK** to add target information from the selected VNXe iSCSI Server.

f. Click **Close** to close the iSCSI Initiator Properties page.

g. Review the summary, and if all the settings are correct, click **Finish**.

For the VNXe Operating Environment 2.1 or earlier:

a. Click the **Dynamic Discovery** tab and click **Add**.

b. Enter the send targets server information and click **OK** to add target information from a selected VNXe iSCSI Server.

c. Click **Close** to close the iSCSI Initiator Properties page.

d. Review the summary, and if all the settings are correct, click **Finish**.

e. If you configured optional initiator CHAP for the host initiator on the VNXe iSCSI Server, now configure CHAP for the VMware software initiator:

- Click the **Configuration** tab, and click **Storage Adapters**.
- Select the iSCSI initiator you want to configure, and click **Properties**.
- In the **iSCSI Initiator Properties** page, click the **CHAP Authentication** tab, and click **Configure**.
- Select **Use the following CHAP credentials**.
- Select **Use Initiator name** to use the initiator name as the CHAP name.
- In the **CHAP Secret** box, enter the *same* secret that you entered for the host initiator on the VNXe iSCSI Server.
- Click **OK** to save the changes.

NOTICE

If you disable CHAP, all sessions that require CHAP authentication terminate immediately.

f. Review the summary, and if all the settings are correct, click **Finish**.

Configuring VNXe VMware VMFS datastores for the host

1. For an ESX4 or ESXi 4.x host, enable the software iSCSI adapter, if not already enabled, as described in "ESX 4 or ESXi 4.x — Enable the software iSCSI adapter" on page 27.
2. For an ESXi 5 or ESXi 5.1 host, add the software iSCSI adapter, if not already added, as described in "ESXi 5 or ESXI 5.1— Add the software iSCSI adapter" on page 27.
3. Use Unisphere or the VNXe CLI to:
   a. Discover VMware ESX and/or ESXi hosts
   b. Create VNXe VMFS datastores

   For information on performing the above Unisphere tasks, refer to the Unisphere online help.

IMPORTANT

When you create VNXe VMFS datastores for discovered VMware ESX and/or ESXi hosts, the VNXe system automatically configures the hosts to use the Datastores. If you select multiple discovered hosts for the datastores, all the selected hosts are configured automatically. The VMware VMFS datastores are presented directly to the ESX or ESXI hosts and not to the hosts' virtual machines. If an ESX or ESXi host cannot see the VMFS datastore after you create the datastore, go to "Manually configuring the connection to a VNXe VMFS datastore" on page 27.

4. Rescan for the VMFS datastores:
   a. From the Inventory panel, select the server, and click the **Configuration** tab.
   b. Under **Hardware**, click **Storage Adapters**.
   c. Under **iSCSI Software Adapters** in the list of adapters, right click on the iSCSI Software adapter and then click **Rescan**.
   d. In the **Rescan** dialog box, select the adapter (NIC), and then click **Rescan**.
   e. In the **Rescan** dialog box, select both **Scan for New Storage Devices** and **Scan for New VMFS Volumes,** and click **OK**.

   If the host can see the VMFS datastore, you must set up the host to use the datastore, as described in the next section.

   If the host cannot see the VMFS datastore, you may have problems with one of the following:

   - Connection between the host and iSCSI target iSCSI (VNXe iSCSI Server), in which case you need to manually configure this connection as described in "Manually configuring the connection to a VNXe VMFS datastore" on page 27.

   or

   - Session between the host and an iSCSI target. To troubleshoot this problem, see "iSCSI session troubleshooting" on page 29.

Configuring ESXi or ESX Server native failover

ESXi and ESX Server include native failover for managing the I/O paths between the server and storage system. Native failover provides multiple paths from the server to the storage system. To use the ESXi or ESX Server native failover with your storage system, you must implement one of the failover policies listed below. For more information about these policies, refer to the ESX configuration guide.

- **Fixed with failover mode (default for a VNXe system**) – Uses the designated preferred path. Otherwise, the software uses the first working path discovered when the system reboots. If the preferred path is not available, the software selects the next available path to the storage processor (SP) where the VNXe iSCSI Server with the storage resource resides. If that SP fails, all paths visible to the ESX NMP or PowerPath/VE go down while the iSCSI Server instance fails over to the surviving SP. When failover is complete, all paths recover and the ESX host automatically reverts back to the preferred path.

- **Round Robin** – Determines which host paths are on the SP that owns the datastores, and alternates through these host paths, issuing I/O to each path for a specific period of time before rotating to the next path. If a path to the VNXe system goes down and then comes up again, the host starts using the path again as soon as it comes up.
- **Most Recently Used (MRU)** – Selects the path the ESX host used most recently. If this path becomes unavailable, the host switches to an alternative path and continues to use the new path while it is available. If a path to the VNXe system goes down and then comes up again, the host starts using the path again as soon as it comes up.

Configuring the native failover policy

1. Log into VMware vSphere Client VI client as administrator.
2. From the inventory panel, select the server, and click the **Configuration** tab.
3. Under **Hardware**, click **Storage** and select the datastore (LUN).
4. Click **Properties**.
5. In the properties page, click **Manage Paths**.
6. In the **Manage Paths** page, under **Policy**, verify that the policy is one you want:

   `Fixed (VMware)` for fixed native failover policy
   `Round Robin (VMware)` for Round Robin native failover policy
   `Most Recently Used (VMware)` for MRU native failover policy

   If the policy is not set to the desired policy, in the policy selection dialog, select the correct policy.
7. If you selected the **Fixed (VMware)** policy, under **Paths**, select the preferred path.

   You can statically balance the load using the fixed policy by selecting different paths for each datastore. To designate a different path as preferred, right click on the path and click **preferred**.
8. Click Close.

What next? You are now ready to either migrate a virtual machine to the VMFS datastore or create a virtual machine on the VMFS datastore. To migrate a virtual disk to the VMFS datastore, go to Chapter 3, "Migrating VMware Virtual Machines to the VNXe System." For information about creating a virtual machine on the VMFS datastore, refer to the VMware documentation.

Manually configuring the connection to a VNXe VMFS datastore

If you receive a connection error when the host is trying to log in to an iSCSI target (VNXe iSCSI Server) or you cannot see the datastores on the target, you may be having problems with the iSCSI session between the initiator and the target. This problem may because:

- The VNXe system's configuration of the ESX host for the VMFS datastore either failed to configure Software iSCSI on the host to access the datastore (see "Configuring software iSCSI when host configuration fails" on page 27) or failed to set up the host to use the VMFS datastore (see "Setting up an ESX host to use a VNXe VMFS datastore when host configuration fails" on page 28).

or

- Other issues with the iSCSI session occurred (see "iSCSI session troubleshooting" on page 29).

Configuring software iSCSI when host configuration fails

If the VNXe system successfully configures the ESX host when you add a host to a VMware datastore, the appropriate ESX iSCSI adapters on the host are configured to access the datastore. If this host configuration does not complete successfully or returns an error message, you must:

- For ESX 4 or ESXi 4.x — Enable the software iSCSI adapter as described in "ESX 4 or ESXi 4.x — Enable the software iSCSI adapter" on page 27

or

- For ESXi 5 or ESXI 5.1— Add the software iSCSI adapter as described in "ESXi 5 or ESXI 5.1— Add the software iSCSI adapter" on page 27

ESX 4 or ESXi 4.x — Enable the software iSCSI adapter

If the software iSCSI adapter is not enabled on the host:

1. Log in to the VMware Client or vSphere Client as an administrator.
2. From the Inventory panel, select the host with the initiator you want to configure.
3. Click the **Configuration** tab, and click **Storage Adapters**.
4. Select the iSCSI adapter that you want to configure, and click **Properties**.
5. In the iSCSI Initiator Properties page, click the **General** tab, and click **Configure**.
6. If the adapter is not already enabled, select **Enabled**.
7. If you want a name and alias for the software iSCSI adapter, enter them under iSCSI Properties, and click **OK**.

ESXi 5 or ESXI 5.1— Add the software iSCSI adapter

If the software iSCSI adapter is not added to the host:

1. Log in to the vSphere Client as an administrator.
2. From the Inventory panel, select the host with the initiator you want to configure.
3. Click the **Configuration** tab, and click **Storage Adapters**.

4. If the Software iSCSI adapter is not listed, click **Add** and select **Software iSCSI**.
5. Select the iSCSI adapter that you want to configure, and click **Properties**.
6. In the iSCSI Initiator Properties page, click the **General** tab, and click **Configure**.
7. If the adapter is not already enabled, select **Enabled**.
8. If you want a name and alias for the software iSCSI adapter, enter them under iSCSI Properties, and click **OK**.

Setting up an ESX host to use a VNXe VMFS datastore when host configuration fails

1. Log in to the VMware VI Client as an administrator.
2. Rescan for new storage devices:
   a. From the Inventory panel, select the server, and click the **Configuration** tab.
   b. Under **Hardware**, click **Storage Adapters**.
   c. Under **iSCSI Software Adapters** in the list of adapters, select the adapter (NIC), and then click **Rescan**.
   d. In the **Rescan** dialog box, select the adapter (NIC), and then click **Rescan**.
   e. In the **Rescan** dialog box, select both **Scan for New Storage Devices** and **Scan for New VMFS Volumes,** and click **OK**.
3. Add *each* VNXe VMFS datastore to the ESX host:
   a. From the Inventory panel, select the host and click the **Configuration** tab.
   b. Under **Hardware,** click **Storage**, and click **Add Storage**.
   c. On the **Select Disk/LUN** page, select the VNXe VMFS datastore that you want to use for the datastore, and click **Next**.
   d. On the **Current Disk Layout** page, review the current virtual disk layout, and click **Next**.
   e. On the **Disk/LUN-Properties** page, enter the ***exact same name*** that was used to create the datastore on the VNXe system.

      You can find this name using Unisphere.
   f. On the **Disk/LUN-Formatting** page, if needed, adjust the file system values and the capacity for the datastore, and click **Next**.
   g. On the **Ready to Complete** page, review the datastore information, and click **Finish**.

The datastore (VMFS volume) is created on the VNXe VMFS datastore for the ESX host.

iSCSI session troubleshooting

1. Verify the connectivity between the host and the target either from the VNXe iSCSI Server IP interface or from the ESX host:

   From the VNXe iSCSI Server IP interface

   Use Unisphere under **Settings › More configuration › Routing Configuration**:

   - Select the SP and the interface on the SP and click **Ping Destination**.
   - Enter the network name of the host iSCSI adapter, and click **Ping**.

   From the ESX host

   Use **vmkping** to verify connectivity to the VNXe iSCSI server IP interfaces.

   If jumbo frames are configured, you should use vmkping with the **-s** option at a size larger than 1500 to verify that all network elements are properly configured for jumbo frames. For example:
   vmkping -s 9000 <*IP_address_of_iSCSI _Server***>**

   Using the IP address avoids name resolution issues.

   Note: You can find the IP address for the target by selecting **Settings › iSCSI Server Settings** in Unisphere.

   Some switches intentionally drop ping packets or lower their priority during times of high workload. If the ping testing fails when network traffic is heavy, verify the switch settings to ensure the ping testing is valid.

2. On the host, verify that the iSCSI initiator service is started.

   Note: The iSCSI service on the iSCSI Server starts when the VNXe system is powered up.

3. If you are using optional CHAP authentication, ensure that the following two secrets are *identical* by resetting them to the same value:

   - The ESX Server secret for the host initiator.
   - The secret configured for the host initiator on the VNXe iSCSI Server.

4. If you are using optional mutual CHAP authentication, ensure that the following two secrets are *identical* by resetting them to the same value:

   - The ESX Server secret for the host initiator.
   - The secret for the iSCSI Server on the VNXe iSCSI Server.

CHAPTER 3
Migrating VMware Virtual Machines to the VNXe System

To migrate a VMware virtual machine to the VNXe system, relocate the VMware datastore with the configuration and disk files for the virtual machine from its current storage location to a VNXe VMware datastore. You can migrate the virtual machine with either suspended migration, which relocates a suspended virtual machine, or with vMotion migration, which relocates a powered-on virtual machine using the vMotion software.

This chapter contains the following topics:

VMware virtual machine migration environment and limitations

Table 1 outlines the environments for suspended migration and a vMotion migration. The VMware administrator's guide for your version of ESX Server provides more information about the migration limitations. Table 2 compares the availability of a graphical user interface and access to the virtual machine for a suspended and vMotion migration.

Table 1 Virtual machine migration environment and limitations

Component	Requirement	
	Suspended migration	**vMotion migration**
VNXe3100 VNXe3150 VNXe3300	Datastore sized to accommodate the existing data that you are migrating and to allow for data growth.	Datastore sized to accommodate the existing data that you are migrating and to allow for data growth.
Hosts	One or two ESX or ESXi hosts	One or two ESX or ESXi hosts, each with: • A vMotion license and configured for vMotion. • Access to both the source and target datastores. • Sufficient resources to support two instances of the virtual machine running concurrently for a brief time.
Virtual machine	None	Virtual machine with snapshots cannot be migrated.
Datastore	• Datastore is on either a local or attached iSCSI storage device and does not need to be shared storage. • Entire datastore is migrated to the VNXe3100, VNXe3150, or VNXe3300 datastore.	• Datastore is on either a local or attached iSCSI storage device and must be shared storage. • Entire datastore is migrated to the VNXe3100, VNXe3150, or VNXe3300 datastore. • Datastore is in persistent mode.

Table 2 Comparison of a suspended migration and a vMotion migration of a virtual machine

Parameter	Suspended migration	vMotion migration
Graphic user interface (GUI)	Provided by ESX Server Migrate Virtual Machine wizard.	Provided with vSphere Client for ESX 4, ESXi 4.x, ESXi 5, or ESXi 5.1 with vMotion.
Access to virtual machine	Disrupted relative to time required for the copying of the virtual machine to the VNXe3100, VNXe3150, or VNXe3300 datastore.	No disruption.

Migrating a virtual machine to a VNXe datastore

To migrate a virtual machine to a VNXe datastore, perform these tasks:

- "Task 1: Set up the host for the virtual machine migration" on page 33.
- *Either* "Task 2: Migrating a virtual machine with suspended migration" on page 33.
  or "Task 3: Migrating a virtual machine with vMotion" on page 33.

Note: In Unisphere, the polling period for a VMware ESXi host or vCenter is once every 24 hours.

Task 1: Set up the host for the virtual machine migration

Set up the ESX Server host to access the new datastore, as described in Chapter 1, "Setting Up a Host to Use VNXe VMware NFS Datastores," for an NFS datastore or in Chapter 2, "Setting Up a Host to Use VNXe VMware VMFS Datastores," for a VMFS datastore.

Task 2: Migrating a virtual machine with suspended migration

Use the Migrate Virtual Machine wizard to migrate the datastore, as described in the VMware administrator's guide for your version of ESX Server. After you click **Finish** in the wizard, the migration operation begins. During the migration operation, you have no access to the virtual machine's functions.

Task 3: Migrating a virtual machine with vMotion

Note: You must move the virtual machines .vmx file during a migration with vMotion. If you want to move a virtual machine's disks while keeping the .vmx file in the same place, you must move the .vmx file and the disks to a new location, and then move the .vmx file back to its original location.

Use the vSphere Client:

1. Set up VMkernel for vMotion:
   a. From the Inventory panel, select the server, and click the **Configuration** tab.
   b. Click **Networking**.
   c. In the **Virtual Switch** view, click **Add Networking**.
   d. Select **VMkernel**, and then click **Next**.
   e. Either select the virtual switch or create one.
   f. Select the network adapters for the virtual switch to use and click **Next**.
   g. Specify the name and VLAN ID for the port group you are creating.
   h. Select **Use this port group for vMotion**, and then click **Next**.
   i. Select one of the following:
      – **Obtain IP settings automatically**
      – **Use the following IP settings**, enter the IP settings, click **Edit** to set the VMKernel default gateway for VMkernel services, such a vMotion, and then click **OK** and **Next**.
   j. Proceed through the remaining pages until you reach the summary page.
   k. On the summary page, verify the settings and then click **Finish**.
2. From the Inventory panel, select the server with the virtual machine that you want to migrate and click the **Virtual Machine** tab.
3. Right-click the virtual machine that you want to migrate, select **Migrate** and click **Next**.

4. Select the VNXe3100, VNXe 3150, or VNXe3300 VMware datastore.
5. For Disk format select **Same format as source** and click **Finish**.