



EMC[®] VNXe[®] Series

Configuring Hosts to Access Fibre Channel (FC) or iSCSI Storage

Version 3.1

P/N 302-000-192 REV 03

Copyright © 2014-2015 EMC Corporation. All rights reserved. Published in the USA.

Published June, 2015

EMC believes the information in this publication is accurate of its publication date. The information is subject to change without notice.

The information in this publication is provided as is. EMC Corporation makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose. Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.

EMC², EMC, and the EMC logo are registered trademarks or trademarks of EMC Corporation in the United States and other countries. All other trademarks used herein are the property of their respective owners.

For the most up-to-date regulatory document for your product line, go to the technical documentation and advisories section on the EMC online support website.

CONTENTS

Preface

Chapter 1

Setting Up a Windows or Mac OS Host to Use VNXe LUN storage over iSCSI

Requirements for setting up a host to use VNXe LUN storage over iSCSI.....	10
VNXe system requirements.....	10
Network requirements.....	10
VNXe VSS HW Provider overview.....	12
Windows host — Using multi-path management software.....	14
Setting up a VNXe system for multi-path management software	14
Installing PowerPath	15
Configuring VNXe iSCSI LUNs for the host.....	15
Windows host — Setting up for iSCSI LUNs	16
Windows host — Configuring to connect to a VNXe iSCSI interface.....	20
Configuring a Windows Server 2003 or Windows Server 2008 SP2 or earlier initiator to connect to a VNXe iSCSI interface — multi-path configuration....	21
Configuring a Windows Server 2008 R2 or Windows Server 2012 initiator to connect to a VNXe iSCSI interface — multi-path configuration	25
Configuring a Windows 7 initiator to connect to a VNXe iSCSI interface..	29
Windows host — Setting up to use VNXe iSCSI LUNs.....	30
Mac OS host — Setting up for iSCSI LUNs	32
iSCSI troubleshooting	34
iSCSI session troubleshooting.....	34
Known Microsoft iSCSI Initiator problems.....	35

Chapter 2

Setting Up a Unix Host to Use VNXe iSCSI Storage

Requirements for setting up a host to use VNXe iSCSI storage	38
Network requirements.....	38
VNXe requirements	39
Using multi-path management software on the host.....	40
Setting up a VNXe system for multi-path management software	40
Installing PowerPath	41
Installing native multipath software	41
What next?	42
AIX host — Setting up for iSCSI storage	43
Citrix XenServer host — Setting up for iSCSI storage	45
HP-UX host — Setting up for iSCSI storage.....	46
Linux host — Setting up for iSCSI storage	49
Solaris host — Setting up for iSCSI storage.....	52
iSCSI session troubleshooting.....	54

Chapter 3

Setting Up a Windows or Mac OS Host to Use VNXe LUN storage over FC

Requirements for setting up a host to use VNXe LUN storage over Fibre Channel	58
VNXe system requirements.....	58
SAN requirements	58

	Path management SAN requirements	58
	VNXe VSS HW Provider overview.....	59
	Windows host — Using multi-path management software.....	61
	Setting up a VNXe system for multi-path management software	61
	Installing PowerPath	61
	Configuring VNXe FC LUNs for the host	62
	Windows host — Setting up for FC LUNs	63
	Windows host — Connecting to a VNXe FC LUN	66
	Configuring a Windows Server 2003 or Windows 2008 SP2 host to connect to a VNXe FC LUN.....	66
	Configuring a Windows Server 2008 R2, Windows Server 2012, Windows7, or Windows 8 host to connect to a VNXe FC LUN	67
	Windows host — Setting up to use VNXe FC LUNs	68
	Mac OS host — Setting up for FC LUNs.....	70
Chapter 4	Setting Up a Unix Host to Use VNXe Fibre Channel (FC) Storage	
	Requirements for setting up a host to use VNXe FC storage.....	74
	SAN requirements	74
	VNXe requirements	74
	Using multi-path management software on the host.....	75
	Setting up a VNXe system for multi-path management software	75
	Installing PowerPath	75
	Installing native multipath software	75
	What next?	76
	AIX host — Setting up for FC storage	77
	Citrix XenServer host — Setting up for FC storage.....	78
	HP-UX host — Setting up for FC storage	79
	Linux host — Setting up for FC storage.....	80
	Solaris host — Setting up for FC storage	81
Chapter 5	Migrating FC or iSCSI Data to the VNXe System	
	FC or iSCSI data migration environment and limitations.....	84
	Migrating FC or iSCSI disk data.....	84
Appendix A	Setting Up MPIO for a Windows Cluster Using a VNXe System	
	Configuration	88
	Setting up cluster nodes (hosts).....	90

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 you can configure the following hosts to access Fibre Channel (FC) or iSCSI storage provisioned on a VNXe storage system with VNXe Operating Environment version 3.0 or later:

- ◆ Windows hosts
- ◆ AIX hosts
- ◆ Citrix XenServer hosts
- ◆ HP-UX hosts
- ◆ Linux hosts
- ◆ Solaris hosts

The information included in this document will enable you to achieve a minimum recommended configuration. Use this document along with the relevant host documentation to plan and configure a robust host access solution that your environment requires.

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 FC or iSCSI LUNs and with the operating system running on the hosts that will access VNXe LUNs.

Related documentation

Other VNXe documents include:

- ◆ *Installation Guide*
- ◆ *Hardware Information Guide*
- ◆ *Parts Location Guide*
- ◆ *Configuring Hosts to Access CIFS File Systems*
- ◆ *Configuring Hosts to Access NFS File Systems*

- ◆ *Configuring Hosts to Access VMware NFS or VMware VMFS*
- ◆ *Unisphere Online Help*
- ◆ *Unisphere 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 indicates a hazardous situation which, if not avoided, will result in death or serious injury.



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



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



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: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> Names of interface elements, such as names of windows, dialog boxes, buttons, fields, and menus What the user specifically selects, clicks, presses, or types
<i>Italic</i>	Used in all text (including procedures) for: <ul style="list-style-type: none"> Full titles of publications referenced in text Emphasis, for example, a new term Variables
<code>Courier</code>	Used for: <ul style="list-style-type: none"> 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
<i>Courier italic</i>	Used in procedures for: <ul style="list-style-type: none"> 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 Windows or Mac OS Host to Use VNXe LUN storage over iSCSI

This chapter describes how to set up a Windows or Mac OS host to use EMC VNXe LUN storage over iSCSI.

Topics include:

◆ Requirements for setting up a host to use VNXe LUN storage over iSCSI.....	10
◆ VNXe VSS HW Provider overview.....	12
◆ Windows host — Using multi-path management software.....	14
◆ Configuring VNXe iSCSI LUNs for the host.....	15
◆ Windows host — Setting up for iSCSI LUNs	16
◆ Windows host — Configuring to connect to a VNXe iSCSI interface	20
◆ Windows host — Setting up to use VNXe iSCSI LUNs.....	30
◆ Mac OS host — Setting up for iSCSI LUNs	32
◆ iSCSI troubleshooting	34

Requirements for setting up a host to use VNXe LUN storage over iSCSI

Before you set up a host to use VNXe LUN storage over iSCSI, 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 *Installation Guide* for your storage system.
- ◆ You have used Unisphere or the VNXe CLI to perform basic configuration of one or more iSCSI interfaces on the VNXe system.

Network requirements

For a host to connect to LUNs on a VNXe iSCSI interface, the host must be in a network environment with the VNXe iSCSI interface; to achieve best performance, the host should be on a local subnet with each VNXe iSCSI interface that provides storage for it. For a Windows multi-pathing environment, each physical interface must have two IP addresses assigned. One on each SP. The interfaces should be on separate subnets..

To achieve maximum throughput, connect the VNXe iSCSI interface 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.

For information on data availability in the VNXe system and in your connectivity infrastructure, refer to *EMC VNXe3200 High Availability, A Detailed Review* white paper.

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 LUN is visible to both SPs.
- ◆ You can configure up to 8 IPs per physical interface. If more than one interface is configured on a physical interface, each interface must be configured on a separate VLAN.
- ◆ Network switches may be on separate subnets.

IMPORTANT

Directly attaching a host to a VNXe system is supported if the host connects to both SPs and has the required multipath software.

[Figure 1 on page 11](#) shows a highly-available iSCSI network configuration for hosts accessing a VNXe storage resource (iSCSI LUNs). 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 interfaces 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 interfaces on SP B.

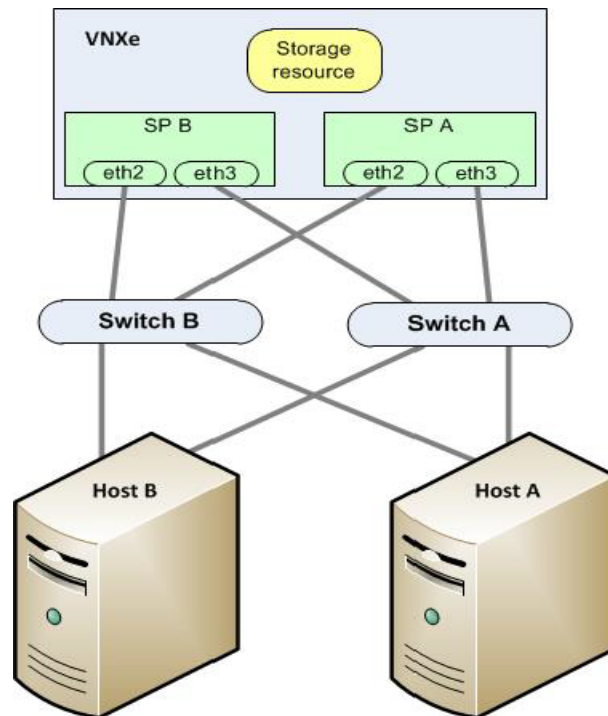


Figure 1 Sample highly-available iSCSI network

VNXe VSS HW Provider overview

The VSS HW Provider runs as a Windows service and provides the interface between the Microsoft Volume Shadow Copy Service (VSS) and VNXe. The VNXe VSS HW Provider enables VSS requestor applications, such as VSS-enabled backup applications, to make snapshots of VNXe iSCSI and FC LUNs.

Microsoft VSS

VSS provides the backup framework for Windows Server 2003 R2, Windows Server 2008, and Windows Server 2012 and enables the creation of snapshots (called shadow copies for Microsoft VSS) — point-in-time copies of data. VSS is integrated with front-end applications so they can create and access shadow copies.

Microsoft VSS shadow copies are:

- ◆ Read-only by default
- ◆ Limited to 512 per volume

The VSS architecture includes VSS providers. A VSS provider creates and maintains shadow copies and acts as the interface to point-in-time imaging capabilities either on a storage platform (hardware-based provider) or in a host operating system (software-based provider).

The VNXe VSS HW Provider is a hardware-based provider that works directly with iSCSI and FC LUNs on the VNXe iSCSI and FC interfaces and with the VSS service on Windows Server 2003 R2, Windows Server 2008, or Windows Server 2012 hosts to provide consistent shadow copy creation and addressing.

Because the VNXe VSS HW Provider is a hardware-based provider, it reduces the load on the CPU and memory of the host. It is also more efficient in an environment where shadow copies of multiple volumes must be taken simultaneously.

The Microsoft website provides more information about VSS and VSS components.

Types of shadow copies

VSS produces three types of shadow copies:

- ◆ Plex copies — Shadow copies initially created by mirroring. A plex copy is a special type of shadow copy data that represents a shadow copy without the need for the original volume data.
- ◆ Differential copies — Shadow copies created by saving only the differences from the original volumes.
- ◆ Redirect-on-write copies — This method does not copy the original volume. It does not make any changes to the original volume after a given time. Instead, it makes a differential copy by redirecting all changes to a different volume.

The VNXe VSS HW Provider supports only differential shadow copies.

Shadow copy backups

You can use VSS shadow copies to back up data on an iSCSI host system. The benefits of shadow copy backups are:

- ◆ You can back up open files.
- ◆ You can copy application data without stopping the application or restricting user access.

Shadow copy backups are available only on Windows Server 2003 R2, Windows Server 2008, and Windows Server 2012 require a VSS provider (such as the VNXe VSS HW Provider) and a backup application that supports VSS (such as EMC NetWorker or Symantec Backup Exec).

Shadow copy transport

Using a VSS hardware provider, such as the VNXe VSS HW Provider, you can create transportable shadow copies for import to other hosts for:

- ◆ Data mining — Make the data in a production database available to other applications by using a shadow copy of the database with those applications.
- ◆ Backup — Instead of overloading a production server with backup traffic, move a shadow copy of a database to another host, and then back up the shadow copy instead of the production database.
- ◆ Data recovery — Keep shadow copies of production data for quick restores. Since creating shadow copies is quick and nondisruptive, shadow copies complement tape-based recovery solutions.

Transportable shadow copies are available with Windows Server 2003, Windows Server 2008, and Windows Server 2012 Enterprise or Datacenter editions.

Limitations

The VNXe VSS HW Provider does *not* support:

- ◆ Microsoft Windows Shadow Copy for Shared Folders.
- ◆ Importing shadow copies to clustered servers. Although you can create shadow copies in a Microsoft Cluster Server (MSCS) environment, you cannot import shadow copies because of a Microsoft restriction. Importing shadow copies to remote hosts is an advanced VSS feature called Shadow Copy Transport, which requires both a VSS hardware provider, such as the VNXe VSS HW Provider, and a third-party VSS requestor that supports Shadow Copy Transport.

[“Shadow copy transport” on page 13](#) provides more information about this VSS feature.

To use Shadow Copy Transport to back up data on a cluster, you must transport and import shadow copies to a nonclustered backup server.

Windows host — 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 if one of the paths fails. The following types of multi-path management software are available for a Windows 2003, Windows Server 2008, or Windows Server 2012 host connected to a VNXe system:

- ◆ EMC PowerPath software on a Windows 2003, Windows Server 2008, or Windows Server 2012 host.

For the supported versions of the PowerPath 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.

Note: PowerPath is not supported for Windows 7.

- ◆ Native MPIO on Windows 2003, Windows Server 2008, or Windows Server 2012 without Multiple Connections per Session (MCS).

Note: The MultiPath IO feature must first be enabled before it can be used.

MCS is not supported by the VNXe.

For information on data availability in the VNXe system and in your connectivity infrastructure, refer to *EMC VNXe3200 High Availability, A Detailed Review* white paper.

Setting up a VNXe system for multi-path management software

For a VNXe system to operate with hosts running multi-path management software, two iSCSI IPs are required. These IPs should be on separate physical interfaces on separate SPs.

Check the configuration on the EMC Unisphere™ **Settings > iSCSI Settings** page. For details on how to configure iSCSI interfaces, refer to the topic on changing iSCSI interface settings in the Unisphere online help.

IMPORTANT

For highest availability, use two network interfaces on the iSCSI interface. The network interfaces should be on separate subnets. If the network interfaces are on the same subnet, a Windows host will let you use only one interface. You can view the network interfaces for an iSCSI interface with Unisphere under **Network Interface** advanced settings (**Settings > iSCSI Settings**).

Installing PowerPath

IMPORTANT

You can set up Native MPIO without using PowerPath. For more information, refer to *Microsoft Multipath I/O Step-by-Step Guide* at: <http://technet.microsoft.com/en-us/library/ee619778>.

1. On the host or virtual machine, download the latest PowerPath version from the PowerPath software downloads section on the EMC Online Support website (<http://support.emc.com>).

2. Install PowerPath as described in the appropriate PowerPath installation and administration guide for the host's or virtual machine'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.

3. When the installation is complete, reboot the host or virtual machine.
4. When the host or virtual machine is back up, verify that the PowerPath service has started.

Configuring VNXe iSCSI LUNs for the host

Use Unisphere or the VNXe CLI to:

1. Create VNXe storage over iSCSI for the host.
2. Add the host to the VNXe system by accessing the **Hosts** tab in Unisphere or using the VNXe CLI and creating a host. If your host is not already logged in, manually create an iSCSI initiator by providing the host IQN.
3. Provide host access to the VNXe storage over iSCSI. Host access options are: **No Access, LUN, Snapshot, LUN and Snapshot**.

IMPORTANT

On a Mac OS host, the Xtend SAN iSCSI initiator will not log into the VNXe iSCSI storage if no vdisk0 is configured on the target (VNXe iSCSI interface). We recommend that you to create a unique VNXe iSCSI interface, create an iSCSI resource on this iSCSI interface, and provide access to the Mac OS host. The first LUN that you create on this iSCSI resource is vdisk0.

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

Windows host — Setting up for iSCSI LUNs

To set up a Windows host for iSCSI LUNs, perform these tasks:

- ◆ [“Task 1: Install the VNXe VSS HW Provider \(Windows Server 2003, Windows Server 2008 SP2\)” on page 16.](#)
- ◆ [“Task 2: Install the Microsoft iSCSI Initiator and iSCSI initiator service on the Windows host \(Windows Server 2003 and Windows Server 2008 SP2\)” on page 17.](#)
- ◆ [“Task 3: Start the iSCSI initiator service \(Windows Server 2008 R2 and Windows Server 2012\)” on page 17.](#)
- ◆ [“Task 4: For a multi-path configuration, install the MPIO feature \(Windows Server 2003 and Windows Server 2008 SP2\)” on page 18.](#)
- ◆ [“Task 5: Set registry values” on page 18.](#)

Task 1: Install the VNXe VSS HW Provider (Windows Server 2003, Windows Server 2008 SP2)

Installing the VNXe VSS HW Provider is optional. However, if you plan to take application consistent snapshots using backup software, you must install the VNXe VSS HW Provider.

EMC recommends that you install the VNXe VSS HW Provider on the host that will use the iSCSI or FC LUNs with backup applications such as EMC NetWorker® and Symantec Backup Exec.

Note: [“VNXe VSS HW Provider overview” on page 12](#) provides information about the VNXe VSS HW Provider.

To install the VNXe VSS HW Provider:

1. Log in to the host using an account with administrator privileges.
2. Download the software package that you want to install as follows:
 - a. Navigate to the Volume Shadow Service (VSS) in the VNXe software downloads section on the **Support** tab of the EMC Online Support website.
 - b. Choose the Volume Shadow Service for your Windows platform, and select the option to save the software to the host.
3. In the directory where you saved the software, double-click the VNXe VSS HW Provider executable file to start the installation wizard.
4. In the **Introduction (Step 1 of 4)** dialog box, click **Next**.
5. In the **Choose Install Folder (Step 2 of 4)** dialog box, select the installation path for the VNXe VSS HW Provider.
6. In the **Pre-Installation Summary (Step 3 of 4)** dialogue box, confirm that you are ready to install by clicking the **Install** button.
7. In the **Installation Complete (Step 4 of 4)** dialog box, click **Finish**.

Starting and stopping the VNXe VSS HW Provider

The VNXe VSS HW Provider runs as a Windows service and is enabled by default. You can stop and start this service from the Windows Services administrative tool.

Task 2: Install the Microsoft iSCSI Initiator and iSCSI initiator service on the Windows host (Windows Server 2003 and Windows Server 2008 SP2)

To connect to the VNXe iSCSI targets (iSCSI interfaces), the host uses an iSCSI initiator, which requires the Microsoft iSCSI Software Initiator and the iSCSI initiator service software. This software is *not* included with the Windows Server operating system software, so you must install it on the host if the host is running Windows Server. When you install the software on the host, the iSCSI initiator software starts.

To install the Microsoft iSCSI Initiator and iSCSI service:

1. Download the latest iSCSI initiator software and related documentation from the Microsoft website to the host.
2. After you download the appropriate software, double-click the executable to open the installation wizard, click **Next** in the **Welcome** page, and follow the steps in the installation wizard.
3. If this is an upgrade of existing iSCSI initiator software, you must restart the host.
4. For shared storage, make the LanManServer service dependent on the iSCSI initiator service by starting the LanManServer before the iSCSI initiator service with the following command:

```
sc config LanManServer depend= MSiSCSI
```

Note: If you use LanManServer on a Windows Server 2003 host to set up shares on a VNXe iSCSI resource, these shares are available only after you reboot the host because the LanManServer service starts before the iSCSI initiator service.

Task 3: Start the iSCSI initiator service (Windows Server 2008 R2 and Windows Server 2012)

To connect to the VNXe targets (iSCSI interfaces), the host uses an iSCSI initiator, which requires the Microsoft iSCSI Software Initiator software and the iSCSI initiator service. This software and service are part of the Windows Server 2008 software; however, the driver for it is not installed until you start the service. You must start the iSCSI initiator service using the administrative tools.

Note: If the host is behind a Windows firewall, Microsoft asks if you want to communicate through the firewall. Before proceeding, we suggest that you consult with your network support administrator.

Task 4: For a multi-path configuration, install the MPIO feature (Windows Server 2003 and Windows Server 2008 SP2)

IMPORTANT

This task is mandatory. Powerpath is an alternative to Native MS MPIO.

If the Windows 2003 or Windows Server 2008 host will use a multi-path configuration to connect to the VNXe iSCSI LUNs, you should install the MPIO feature.

To install MPIO on Windows Server 2008:

1. Open Server Manager.
2. In the **Server Manager** tree, click **Features**.
3. In the **Features** pane, under **Features Summary**, click **Add Features**.
4. In the **Add Features Wizard**, select **Multipath I/O**, and click **Next**.
5. In the **Confirm Installation Selections** dialog box, click **Install**.
6. When the installation is complete, in the Installation **Results** dialog box, click **Close**.
7. When prompted to restart the computer, click **Yes**.

After restarting, the host finalizes the MPIO installation.

8. Click **Close**.

Task 5: Set registry values

NOTICE

Incorrectly modifying the Registry can cause serious system-wide problems that can require you to reinstall the system. Use the Windows Registry Editor at your own risk.

1. On the host, run the Windows Registry Editor (**regedit.exe**).
2. Go to HKEY_LOCAL_MACHINE\SYSTEM\.
3. Right-click **CurrentControlSet**, and search for the **MaxRequestHoldTime** key and modify its value from 60 to 600 (decimal) or from 3c to 258 (hexadecimal).

IMPORTANT

Verify that the path to the parameter is in the CurrentControlSet. If it is not, search for the parameter again. If you make changes to ControlSets other than the top level current set, those changes will not affect the system.

4. If the host is running PowerPath:
 - a. Search for the register keys list in [Table 1](#).

IMPORTANT

Verify that the path to the parameter that you found in the CurrentControlSet. If it is not, search for the parameter again. If you make changes to ControlSets other than the top level current set, those changes will not affect the system.

- b. Record the value of each of these registry keys, so you have them in case you need to uninstall PowerPath.
 - c. Update each of these registry keys [Table 1](#).

Table 1 Registry keys to update

Registry keys	Instructions
LinkDownTime	Set to 600.
AsyncLogoutPauseTimeout (new value)	Add this REG_DWORD key in the same key as LinkDownTime. Set it to 600.
DelayBetweenReconnect PortalRetryCount	Find the DelayBetweenReconnect value. Set the PortalRetryCount value so that $\text{PortalRetryCount} \times \text{DelayBetweenReconnect} = 600$
SrbTimeoutDelta for PowerPath only	Set to 100 for PowerPath only.

5. Quit the Registry Editor.

Windows host — Configuring to connect to a VNXe iSCSI interface

Before an initiator can establish a session with a target, the initiator must discover where the targets are located and the names of the targets available to it. To obtain this information the initiator uses the iSCSI discovery process. The VNXe iSCSI interfaces support discovery with or without an iSNS server. Without iSNS discovery, you must add the target information to the Microsoft iSCSI Initiator. With iSNS discovery, the initiator queries the iSNS server where all iSCSI initiators and targets register themselves, and the server responds with a list of available targets. When the target information is available to the Microsoft iSCSI Initiator, you can connect the host initiator to the target so the host can access the iSCSI LUNs.

NOTICE

Unless you are using VNXe iSCSI targets in a clustered environment, avoid giving more than one initiator access to the same LUN. Conflicts can occur if more than one initiator tries to write to the LUN. If the LUN is formatted with the NTFS file system in Windows, simultaneous writes can corrupt the NTFS file system on the LUN.

Each VNXe iSCSI interface is a target. If a VNXe system has two iSCSI interfaces, it has two targets. Each target has one session.

To connect to an iSCSI target, you must add the target IP address in Microsoft iSCSI Initiator. If you have multiple targets (iSCSI interfaces), you can use the Microsoft iSCSI initiator to discover the targets through an individual IP address.

To configure the Windows host initiators:

Go to the section below for the host's configuration:

For Windows Server 2003 or Windows Server 2008 SP2 or earlier:

- ◆ Multipath configuration with iSCSI or PowerPath:
[“Configuring a Windows Server 2003 or Windows Server 2008 SP2 or earlier initiator to connect to a VNXe iSCSI interface — multi-path configuration” on page 21](#)

For Windows Server 2008 R2 or Windows Server 2012:

- ◆ Multi-path configuration with iSCSI or PowerPath:
[“Configuring a Windows Server 2008 R2 or Windows Server 2012 initiator to connect to a VNXe iSCSI interface — multi-path configuration” on page 25](#)

[Appendix A, “Setting Up MPIO for a Windows Cluster Using a VNXe System,”](#) gives an end-to-end example of setting up a two-node Windows Server 2008 R2 Exchange cluster in an MPIO multi-path configuration with a VNXe system.

For Windows 7:

[“Configuring a Windows 7 initiator to connect to a VNXe iSCSI interface” on page 29](#)

Configuring a Windows Server 2003 or Windows Server 2008 SP2 or earlier initiator to connect to a VNXe iSCSI interface — multi-path configuration

Before you configure a Windows Server 2003 or Windows Server 2008 SP2 or earlier initiator to connect to a VNXe iSCSI interface in a multi-path configuration:

- ◆ You must have configured the VNXe iSCSI interface with two IP interfaces on two separate physical ports. Each IP interface should be on a separate IP subnet.
- ◆ The Windows host must have two network interfaces. One interface must be on the IP subnet with one of the VNXe iSCSI interfaces, and the other interface must be on the IP subnet with the other VNXe iSCSI interface.

To configure a Windows Server 2003 or Windows Server 2008 SP2 or earlier initiator to connect to a VNXe iSCSI interface in a multi-path configuration, perform these tasks:

- ◆ Multi-path configuration with Native MPIO:
 1. [“Setup optional mutual CHAP — Windows Server 2003 or Windows Server 2008 SP2 or earlier in multi-path configuration” on page 22.](#)
 2. [“Discover the VNXe iSCSI interface in an environment — Windows Server 2003 or Windows Server 2008 SP2 or earlier in a multi-path configuration” on page 22.](#)
 3. [“Identify and set active paths to the storage system” on page 24.](#)
- ◆ Multi-path configuration with PowerPath:
 1. [“Setup optional mutual CHAP — Windows Server 2003 or Windows Server 2008 SP2 or earlier in multi-path configuration” on page 22.](#)
 2. [“Discover the VNXe iSCSI interface in an environment — Windows Server 2003 or Windows Server 2008 SP2 or earlier in a multi-path configuration” on page 22.](#)

Note: MCS is not supported.

Setup optional mutual CHAP — Windows Server 2003 or Windows Server 2008 SP2 or earlier in multi-path configuration

To configure optional mutual Challenge Handshake Authentication Protocol (CHAP) you need the mutual CHAP secret specified for the VNXe iSCSI interface.

For the VNXe iSCSI interface to which you want the host iSCSI initiator to access:

1. On the host, start the Microsoft iSCSI Initiator.
2. If mutual CHAP authentication is configured on the VNXe iSCSI interface, then in the Microsoft iSCSI Initiator:
 - a. Click the **General tab** and select **Secret**.
 - b. In the **CHAP Secret Setup** dialog box, enter the mutual CHAP secret for the VNXe iSCSI interface.

If the VNXe system has multiple iSCSI interfaces, this secret is the same for all. You can find this secret in the **CHAP Security** section on the iSCSI Settings page in Unisphere (**Settings > iSCSI Settings**).

- c. Click **OK**.

Discover the VNXe iSCSI interface in an environment — Windows Server 2003 or Windows Server 2008 SP2 or earlier in a multi-path configuration

If the host initiator is configured for optional initiator Challenge Handshake Authentication Protocol (CHAP) on the VNXe iSCSI interface, you need the secret (password) specified for the initiator on the VNXe system.

1. On the host, start the Microsoft iSCSI Initiator.
2. Click the **Discovery** tab.
3. Under **Target Portals**, click **Add**.

The **Add Target Portal** dialog box opens.

4. In the **Add Target Portal** dialog box:
 - a. Enter the IP address of the VNXe iSCSI interface on the *first* subnet with the host interface. You can find this address with Unisphere by selecting **Settings > iSCSI Settings**.
 - b. Click **Advanced**.

The **Advanced Settings** dialog box opens.

5. In the **Advanced Settings** dialog box, set the following:
 - **Local adapter** to **Microsoft iSCSI Initiator**.
 - **Source IP** to the IP address of the host interface on the *first* subnet with the VNXe iSCSI interface.
6. If the host initiator is configured for optional initiator CHAP on the VNXe iSCSI interface:
 - a. Select **CHAP logon information**.
 - b. Leave **User name** as the default value, which is the initiator's IQN.

- c. Set **Target secret** to the *same* secret that is configured for the host initiator on the VNXe iSCSI interface. The VNXe iSCSI interfaces support CHAP secrets of 12 to 16 characters only.
 - d. If the VNXe iSCSI interface is configured for mutual CHAP, select **Perform Mutual Authentication**.
7. Click **OK** to close the **Advanced Settings** dialog box.
8. Click **OK** to close the **Add Target Portal** dialog box.
9. In the **Discovery** tab, verify that the address of the first VNXe iSCSI interface appears in the **Target Portals** list.
10. Click the **Targets** tab. The IQNs representing the ports configured on the storage system appear in the **Targets** list with an **Inactive** status.
11. In the **Targets** tab, select a VNXe iSCSI interface target name, and click **Log On**. The **Log On to Target** dialog box opens.
12. In the **Log On to Target** dialog box:
 - a. Select **Automatically restore this connection when the system reboots**.
 - b. Select **Enable multi-path**.
 - c. Click **Advanced**. The **Advanced Settings** dialog box opens.
13. In the **Advanced Settings** dialog box, set the following:
 - **Local adapter** to **Microsoft iSCSI Initiator**.
 - **Source IP** to the address of the host interface on the *first* subnet with the VNXe iSCSI interface.
 - **Target Portal** to the address of the VNXe iSCSI interface on the *first* subnet with the host interface.

To find the IP address associated with this IQN, note the IQN name, and then go to **Settings > iSCSI Settings** in Unisphere.
14. If the host initiator is configured for optional initiator CHAP on the VNXe iSCSI interface:
 - a. Select **CHAP logon information**.
 - b. Leave **User name** as the default value, which is the initiator's IQN.
 - c. Set **Target secret** to the *same* secret that is configured for the host initiator on the VNXe iSCSI interface. The VNXe iSCSI interfaces support CHAP secrets of 12 to 16 characters only.
 - d. If the VNXe iSCSI interface is configured for mutual CHAP, select **Perform Mutual Authentication**.
15. Click **OK** to close the **Advanced Settings** dialog box.
16. Click **OK** to close the **Log On to Target** dialog box.
17. Repeat steps 11 through 16 for all other targets listed in the **Targets** tab. Ensure that the relevant IP addresses are selected accurately. Once logged on, each listed target must appear with the **Connected** status.

Identify and set active paths to the storage system

Note: This section does not apply to multi-path configuration with PowerPath.

The Microsoft iSCSI Initiator may not accurately identify the active paths to the storage system. Complete the following steps to identify and set the active paths:

Note: To achieve effective load-balancing, ensure that only paths to the SP that owns the LUN are set as Active. Setting paths to the standby SPs as Active can cause issues in your implementation.

1. In the **Targets** tab, select a VNXe iSCSI interface target, and click **Details**.
The **Target Properties** dialog box opens.
2. On the **Devices** tab, click **Advanced**. The **Device Details** dialog box opens.
3. Click the **MPIO** tab. This tab lists all valid paths, with a single path set as Active. This path goes to the SP owner of the storage resource.
4. Ensure that **Load Balance Policy** is set to **Round Robin With Subset**.
5. Click the interface with the path set as **Active**, and click **Details**.
6. In the **MPIO Path Details** dialog box, note the value in the **Target Portal** column. This is the IP address associated with the iSCSI interface created on the relevant port of the SP.
7. Click **OK** to close the **MPIO Path Details** dialog box.
8. For each interface with the path set as **Standby**, click **Details** to launch the associated **MPIO Path Details** dialog box.
9. Review the value in the **Target Portal** column, and identify the interface that has path to the same SP as the interface with the path set as Active.

Note: In Unisphere, go to **Settings > iSCSI Settings** to review the list of interfaces/IP addresses with path to the same SP.

10. For the interface with the path to the same SP, on the **MPIO** tab, click **Edit**.
11. In the **Edit Settings** dialog box, set **Path Type** to **Active**.
12. Click **OK** to close the **Edit Settings** dialog box.
13. On the **MPIO** tab, verify that the interface appears with the path set as **Active**.
14. Click **OK** to close the **Device Details** dialog box.
15. Click **OK** to close the **Target Properties** dialog box.
16. Click **OK** to exit the Microsoft iSCSI Initiator.

What next?

Continue to ["Windows host — Setting up to use VNXe iSCSI LUNs" on page 30](#).

Configuring a Windows Server 2008 R2 or Windows Server 2012 initiator to connect to a VNXe iSCSI interface — multi-path configuration

Before you configure a Windows Server 2008 R2 initiator to connect to a VNXe iSCSI interface in a multi-path configuration:

- ◆ You must have configured the VNXe iSCSI interface with two IP interfaces on two separate physical ports. Each IP interface should be on a separate IP subnet.
- ◆ The Windows host must have two network interfaces. One interface must be on the IP subnet with one of the VNXe iSCSI interfaces, and the other interface must be on the IP subnet with the other VNXe iSCSI interface.

To configure a Windows Server 2008 R2 or later initiator to connect to a VNXe iSCSI interface in a multi-path configuration, perform these tasks:

- ◆ Multi-path configuration with Native MPIO:
 1. [“Setup optional mutual CHAP — Windows Server 2008 R2 in multi-path configuration” on page 26.](#)
 2. [“Configure MPIO to recognize iSCSI devices” on page 26.](#)
 3. [“Discover the VNXe iSCSI interface in an environment — Windows Server 2008 R2 in multi-path configuration” on page 26.](#)
 4. [“Review the paths to the SP” on page 28.](#)
 5. [“Verify the paths MPIO will use for load balancing” on page 28.](#)
- ◆ Multi-path configuration with PowerPath:
 1. [“Setup optional mutual CHAP — Windows Server 2008 R2 in multi-path configuration” on page 26.](#)
 2. [“Discover the VNXe iSCSI interface in an environment — Windows Server 2008 R2 in multi-path configuration” on page 26.](#)

Note: MCS is not supported.

Setup optional mutual CHAP — Windows Server 2008 R2 in multi-path configuration

To configure optional mutual Challenge Handshake Authentication Protocol (CHAP) you need the mutual CHAP secret specified for the VNXe iSCSI interface.

For the VNXe iSCSI interface to which you want the host iSCSI initiator to access:

1. On the host, start the Microsoft iSCSI Initiator.
2. If mutual CHAP authentication is configured on the VNXe iSCSI interface, then in the Microsoft iSCSI Initiator:
 - a. Click the **Configuration** tab.
 - b. On the **Configuration** tab, click **CHAP...**

The **iSCSI Initiator Mutual Chap Secret** dialog box opens.

- c. In the **iSCSI Initiator Mutual Chap Secret** dialog box, enter the mutual CHAP secret for the VNXe iSCSI interface.

If the VNXe system has multiple iSCSI interfaces, this secret is the same for all. You can find this secret in the **CHAP Security** section on the iSCSI Settings page in Unisphere (**Settings > iSCSI Settings**).

- d. Click **OK**.

Configure MPIO to recognize iSCSI devices

Note: This section does not apply to multi-path configuration with PowerPath.

1. Launch the MPIO application.
2. On the **MPIO Properties** dialog box, click the **Discover Multi-Paths** tab.
3. Under **SPC-3 compliant**, select **Add support for iSCSI devices**.
4. Click **Add**. A **Reboot Required** dialog box opens.
5. In the **Reboot Required** dialog box, click **Yes**.
6. Once the server reboots, launch the MPIO application, and verify that the MPIO is configured to claim all iSCSI devices.

Discover the VNXe iSCSI interface in an environment — Windows Server 2008 R2 in multi-path configuration

If the host initiator is configured for optional initiator Challenge Handshake Authentication Protocol (CHAP) on the VNXe iSCSI interface, you need the secret (password) specified for the initiator on the VNXe system.

1. On the host, start the Microsoft iSCSI Initiator.
2. Click the **Discovery** tab.
3. Under **Target Portals**, click **Discover Portal**.

The **Discover Target Portal** dialog box opens.

4. In the **Discover Target Portal** dialog box:
 - a. Enter the IP address of the VNXe iSCSI interface on the *first* subnet with the host interface.
You can find this address with Unisphere by selecting **Settings** > **iSCSI Settings**.
 - b. Click **Advanced**.
The **Advanced Settings** dialog box opens.
5. In the **Advanced Settings** dialog box, set the following:
 - **Local adapter** to **Microsoft iSCSI Initiator**.
 - **Initiator IP** to the IP address of the host interface on the *first* subnet with the VNXe iSCSI interface.
6. If the host initiator is configured for optional initiator CHAP on the VNXe iSCSI interface:
 - a. Select **Enable CHAP logon**.
 - b. Leave **Name** as the default value, which is the initiator's IQN.
 - c. Set **Target secret** to the *same* secret that is configured for the host initiator on the VNXe iSCSI interface.
The VNXe iSCSI interfaces support CHAP secrets of 12 to 16 characters only.
 - d. If the VNXe iSCSI interface is configured for mutual CHAP, select **Perform Mutual Authentication**.
7. Click **OK** to close the **Advanced Settings** dialog box.
8. Click the **Targets** tab.
9. In the **Targets** tab under **Discovered Targets**, select the VNXe iSCSI target and click **Connect**.
The **Connect to Target** dialog box opens.
10. In the **Connect to Target** dialog box:
 - a. Verify that **Add this connection to the list of Favorite Targets** is selected.
 - b. Select **Enable Multi-path**.
 - c. Click **Advanced**.
The **Advanced Settings** dialog box opens.
11. In the **Advanced Settings** dialog box, set the following:
 - **Local adapter** to **Microsoft iSCSI Initiator**.
 - **Initiator IP** to the address of the host interface on the *first* subnet with the VNXe iSCSI interface.
 - **Target portal IP** to the address of the VNXe iSCSI interface on the *first* subnet with the host interface.
You can find this address with Unisphere by selecting **Settings** > **iSCSI Settings**.
12. Click **OK** to close the **Advanced Settings** dialog box.

13. Click **OK** to close the **Connect to Target** dialog box.
14. Repeat steps 8 through 13 for all other targets listed in the **Targets** tab. Ensure that the relevant IP addresses are selected accurately. Once connected, each listed target must appear with the **Connected** status.

Review the paths to the SP

Note: This section does not apply to multi-path configuration with PowerPath.

1. In the **Targets** tab, select a VNXe iSCSI interface target, and click **Devices**.
2. On the **Devices** dialog box, under **Configure Multipath IO (MPIO)**, click **MPIO**. The **Device Details** dialog box opens.
3. This tab lists all valid paths, with a single path set as Active. This path goes to the SP owner of the storage resource.
4. In the **MPIO** tab, ensure that **Load Balance Policy** is set to **Round Robin With Subset**.
5. Review the list of paths to each device, and verify that they are set to **Active**.
6. Although all paths may appear as Active, it does not mean that the IO operations will be active on all connections. The IO will be directed only to the paths on the SP that owns the device or storage resource..
7. Click **OK** to close the **Properties** dialog box.
8. Click **OK** to exit the Microsoft iSCSI Initiator.

Verify the paths MPIO will use for load balancing

Note: This section does not apply to multi-path configuration with PowerPath.

1. Launch the MPIO application.
2. On the **MPIO Properties** dialog box, click the **Configuration Snapshot** tab.
3. Under **Snapshot**, specify a path and file name for the output.
4. Select **Open File upon capture**, and then click **Capture**.

The output will appear in a text editor. It lists available paths to each device or storage resource. Note the following:

- Paths with **Active/Optimized** state are used to balance I/O to a storage resource.
- Paths with **Active/Unoptimized** state are used for failovers only.

What next?

Continue to ["Windows host — Setting up to use VNXe iSCSI LUNs" on page 30.](#)

Configuring a Windows 7 initiator to connect to a VNXe iSCSI interface

If the host initiator is configured for optional initiator Challenge Handshake Authentication Protocol (CHAP) on the VNXe iSCSI interface, you need the secret (password) specified for the initiator on the VNXe system.

To configure a Windows 7 to connect to a VNXe:

1. On the host, start the Microsoft iSCSI Initiator.

One way to start the iSCSI Initiator is by going to the Control Panel and selecting **All Control Panel Items > Administrative Tools > iSCSI Initiator**.

2. If prompted to start the iSCSI service, click **Yes**.
3. In the **Targets** tab, enter the IP address of the VNXe iSCSI interface and click **Quick Connect**.
4. In the Quick Connect window under Discovered targets, select the VNXe iSCSI interface and click **Connect**.

The VNXe iSCSI LUNs on the target (VNXe iSCSI interface) for the host are added to Windows 7.

5. Click **Done**.

The connection to the VNXe iSCSI interface appears on the Targets tab as Connected.

6. Click the **Volumes and Devices** tab and click **Auto Configure**

The LUNs are connected to the host.

Windows host — Setting up to use VNXe iSCSI LUNs

To set up a Windows host to use VNXe iSCSI LUNs, perform the following tasks:

- ◆ “Task 1: Register the LUNs as MPIO devices (Windows Server 2008 SP2 and Windows Server 2012)” on page 30.
- ◆ “Task 2: Set the offset for the LUN to 64 KB” on page 30.
- ◆ “Task 3: Configure a volume on the LUN” on page 31.

Task 1: Register the LUNs as MPIO devices (Windows Server 2008 SP2 and Windows Server 2012)

If you are using Multipath I/O (MPIO) with Windows Server, you must register the VNXe LUNs as MPIO devices and set up MPIO to discover iSCSI devices:

1. On the host, start the MPIO Administrative Tool:

Either **Start > Administrative Tools** and select **MPIO** or **Start > Run** and enter **mpioctrl.exe**.

2. Open the MPIO control panel, and click the **Discover Multi-Paths** tab.
3. Select the **Add support for iSCSI devices** check box, and click **Add**.
4. When prompted to restart the computer, click **Yes**.

When the computer restarts, the MPIO Devices tab lists the additional hardware ID “MSFT2005iSCSIBusType_0x9.” When this hardware ID is listed, all iSCSI bus attached devices will be claimed by the Microsoft DSM.

5. Restart the host when prompted.

Task 2: Set the offset for the LUN to 64 KB

Note: This task is only required for systems running Hyper-V on Windows Server 2003, or systems that were upgraded from Windows Server 2003 to Windows Server 2008 or later.

After the initiator logs in to a target, each of the target’s LUNs that the initiator can access appears as an unknown disk in the Windows Disk Management tool.

To set the offset for the LUN on the host:

1. Select **Run > diskpart**.
2. Select the disk:

select disk *n*

where *n* is the disk number.

If you do not know the disk number, enter:

list disk

3. On the selected disk, create a primary partition with an offset of 64 KB:
create part pri align=64

Task 3: Configure a volume on the LUN

The following configuration process initializes the LUN, creates a partition, formats a volume on the partition, and mounts the partition on a drive letter:

1. On the host, in the Microsoft Disk Management tool, select the LUN.
2. If the system asks you to initialize the disk, click **Yes**, but do not choose to make the disk a dynamic disk because the VNXe iSCSI interfaces do not support dynamic disks.

For a given LUN, its drive letter, disk number, and LUN number are independent.

3. Use a quick format operation (Windows Server 2003 or Windows Server 2008) or the New Simple Volume wizard (Windows 7) to create a volume on the disk with the following properties:
 - NTFS file system
 - 64K location unit size

IMPORTANT

Do not format more than one LUN at a time. Otherwise, some of the volumes can become write-protected and cannot be formatted.

You can change the volume label. Because the disk number of a LUN can change after system restart or after logging in to and out of a target, be sure to change the default volume label ("New Volume") to a descriptive label.

4. Assign an available drive letter to the disk.
5. Close the Disk Management tool.

Mac OS host — Setting up for iSCSI LUNs

To set up a Mac OS for iSCSI LUNs, you must perform these tasks:

- ◆ [“Task 1: Installing and configuring the ATTO Xtend SAN iSCSI Initiator on a Mac OS host” on page 32.](#)
- ◆ [Task 2: Set up a Mac OS host to use the VNXe iSCSI LUN \(page 33\).](#)

Task 1: Installing and configuring the ATTO Xtend SAN iSCSI Initiator on a Mac OS host

To connect a host iSCSI initiator on a Mac OS host to VNXe iSCSI storage, you must install the ATTO Xtend SAN iSCSI Initiator and configure the initiator for the target.

1. On the VNXe system, from the **iSCSI Settings** page in Unisphere (**Settings** > **iSCSI Settings**), determine the IP address of the VNXe iSCSI interface (target) to which you want the host initiator to connect. This iSCSI interface is the one with the iSCSI storage resources for the host.
2. On the Mac OS host, insert the Xtend SAN CD into a CD drive, and following the steps in the installation wizard.

An **iSCSI Xtend SAN** icon appears at the location where you chose to install the initiator.

3. Double-click the **iSCSI Xtend SAN** icon.
4. Click the **Discover Targets** tab.
5. In the **Discover Targets** dialog box:
 - a. Enter the IP address of the target, which is the IP address of the VNXe iSCSI interface with the iSCSI LUNs for the Mac OS.
 - b. To use optional CHAP:
 - Enter the target user name
 - Enter the target secret
 - For optional CHAP mutual authentication, select the **Mutual Authentication** checkbox.
 - c. Click **Finish**.

The **Setup** dialog box appears, displaying the iqn of the discovered VNXe target.

6. In the **Setup** dialog box
 - a. Select **Visible** and **Auto Login**.
 - b. Click **Save**.
7. Click the **Status** tab.
8. In the **Status** dialog box, click **Login**.

When the login operation is complete, the red icon before the iqn name in the left panel turns green.

9. Click **LUNs** to verify the connections.

If the initiator is connected to the VNXe iSCSI interface, the VNXe iSCSI LUN for the host appears in the LUNs list.

Task 2: Set up a Mac OS host to use the VNXe iSCSI LUN

Before the Mac OS host can use the VNXe iSCSI LUN, you must use the Mac OS Disk Utility to:

- ◆ [“Task 1:Format the VNXe iSCSI LUN” on page 33](#)
- ◆ [“Task 2:Partition the VNXe iSCSI LUN” on page 33](#)

Task 1: Format the VNXe iSCSI LUN

1. On the host, go to **Finder > Application > Utilities**.
2. Double-click **Disk Utility**.
3. In the left panel, select the VNXe iSCSI LUN.
VNXe iSCSI LUNs appear in the left panel as **EMC Celerra iSCSI Media**.
4. Click the **Erase** tab.
5. For **Volume Format**, select the format that you want, and confirm your format choice.
6. Click **Erase** and verify the erase procedure, and click **Erase** again to start the erase process.

When the erase process finished, the LUN is ready for you to partition it.

Task 2: Partition the VNXe iSCSI LUN

1. On the host, go to **Finder > Application > Utilities**.
2. Double click **Disk Utility**.
3. In the left panel, select the VNXe iSCSI LUN.
VNXe iSCSI LUNs appear in the left panel as **EMC Celerra iSCSI Media**.
4. Click the **Partition** tab.
5. Under Volume Scheme, select the number of partitions for the LUN.
The utility displays equal-sized partitions to fill the available space on the LUN.
6. For each partition:
 - a. Select the partition.
 - b. In **Name**, enter a name for the partition.
 - c. Under **Format**, select the format for the partition.
The default format - Mac OS Extended (Journaled) - is a good choice for most uses.
 - d. In **Size**, enter the size for the partition.
7. When you have specified, the name, size, and format for each partition, click **Apply**.

The Disk Utility uses the partition information to create volumes that the host can access and use. When the partitioning process is complete, the new volumes are mounted on the desktop and ready to use.

You are now ready to either migrate data to the LUN or have the host start using the LUN. To migrate data to the LUN, go to [Chapter 5, “Migrating FC or iSCSI Data to the VNXe System.”](#)

iSCSI troubleshooting

This section contains information about:

- ◆ [“iSCSI session troubleshooting” on page 34](#)
- ◆ [“Known Microsoft iSCSI Initiator problems” on page 35](#)

iSCSI session troubleshooting

1. Use **ping** with the IP address to verify connectivity from the host to the target’s IP address.

Using the IP address avoids name resolution issues.

Note: You can find the IP address for the target by selecting **Settings > iSCSI 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 interface starts when the VNXe system is powered up.

3. In the Microsoft iSCSI Initiator, verify the following for the VNXe target portal:

- IP address(es) or DNS name of the VNXe iSCSI interface with the host’s LUNs.

Note: For a host running PowerPath or Windows native failover, VNXe target portal has two IP addresses.

- Port is 3260, which is the default communications port for iSCSI traffic.

4. Verify that the iSCSI qualified names (IQN) for the initiators and the iSCSI interface name for the target are legal, globally unique, iSCSI names.

Note: An IQN must be a globally unique identifier of as many as 223 ASCII characters.

For a Windows host initiator — You can find this IQN on the **General** or **Configuration** tab of the Microsoft iSCSI initiator (depending on the version).

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

- The secret for the host initiator in the Microsoft iSCSI Software Initiator or the Linux **open-iscsi** driver.
 - The secret configured for the host initiator on the VNXe iSCSI interface.
6. If you are using optional mutual CHAP authentication, ensure that the following two secrets are *identical* by resetting them to the same value:
- The secret for the host initiator in the Microsoft iSCSI Software Initiator or the Linux **open-iscsi** driver.
 - The secret for the iSCSI interface on the VNXe iSCSI interface.

Known Microsoft iSCSI Initiator problems

[Table 2](#) describes known problems that with the Microsoft iSCSI Initiator and describes workarounds.

Table 2 Microsoft iSCSI Initiator problems

Problem	Symptom	Workaround
Initiator cannot refresh its targets list.	If you use iSNS and an initiator is disconnected from the network, the initiator may not refresh its target list. When attempting to refresh the target list, the initiator logs the iSNS error <code>auth unknown (0x6)</code> to the Windows Event Log.	<ol style="list-style-type: none"> 1. Select Windows Administrative Tools > Services. 2. Stop and restart the Microsoft iSCSI Initiator.
Login problems occur when you use iSNS for target discovery.	When you configure the initiator with iSNS target discovery, it can intermittently fail to log in to a target with the following error message: The target name is not found or is marked as hidden from login.	The Microsoft iSCSI Initiator eventually recovers from this situation. To speed up the process, refresh the target list a few times until the target in question is discovered.
Initiator messages fill up the Windows Event Log.	If the initiator has an active session with a VNXe iSCSI interface and the iSCSI interface becomes unavailable, then the initiator logs multiple messages to the Windows Event Log. If multiple LUNs are configured for each target, the messages that the initiator generates can quickly fill the log.	To avoid this situation, log out all connected initiators before bringing the target down for its scheduled downtime.
Cannot write to a filesystem on a VNXe storage resource connected to the host.	Filesystem is read-only.	<ol style="list-style-type: none"> 1. Verify that the registry values as set as described in “Set registry values” on page 19. 2. Verify that the Microsoft iSCSI Initiator is configured as described in “Windows host — Configuring to connect to a VNXe iSCSI interface” on page 27.

CHAPTER 2

Setting Up a Unix Host to Use VNXe iSCSI Storage

This chapter describes how to set up an AIX, Citrix XenServer, HP-UX, Linux, or Solaris host to use EMC® VNXe® iSCSI storage.

Topics include:

◆ Requirements for setting up a host to use VNXe iSCSI storage	38
◆ Using multi-path management software on the host.....	40
◆ AIX host — Setting up for iSCSI storage	43
◆ Citrix XenServer host — Setting up for iSCSI storage	45
◆ HP-UX host — Setting up for iSCSI storage	46
◆ Linux host — Setting up for iSCSI storage	49
◆ Solaris host — Setting up for iSCSI storage	52
◆ iSCSI session troubleshooting.....	54

Requirements for setting up a host to use VNXe iSCSI storage

Before you set up a host to use VNXe iSCSI storage, the network and VNXe requirements described in this section must be met.

Network requirements

For a host to connect to iSCSI storage on an VNXe iSCSI interface, the host must be in a network environment with the VNXe iSCSI interface; to achieve best performance, the host should be on a local subnet with each VNXe iSCSI interface that provides storage for it. For a multi-pathing environment, each VNXe iSCSI interface providing iSCSI storage for the host, must have two IP addresses associated with it. These two addresses should be on different subnets to ensure high availability.

Note: The Linux iSCSI driver, which is part of the Linux operating system and which you configure so that the host iSCSI initiators can access the VNXe iSCSI storage, does not distinguish between NICs on the same subnet. As a result, to achieve load balancing, a VNXe iSCSI interface connected to a Linux host must have each NIC configured on a different subnet.

To achieve maximum throughput, connect the VNXe iSCSI interface 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

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

- ◆ A VNXe storage resource is visible to both SPs
- ◆ You can configure up to 8 IP iSCSI interfaces per port.
- ◆ Network switches may be on separate subnets.

IMPORTANT

Directly attaching a host to a VNXe system is supported if the host connects to both SPs and has the required multipath software.

[Figure 2 on page 39](#) shows a highly-available iSCSI network configuration for hosts accessing a VNXe storage resource. 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.

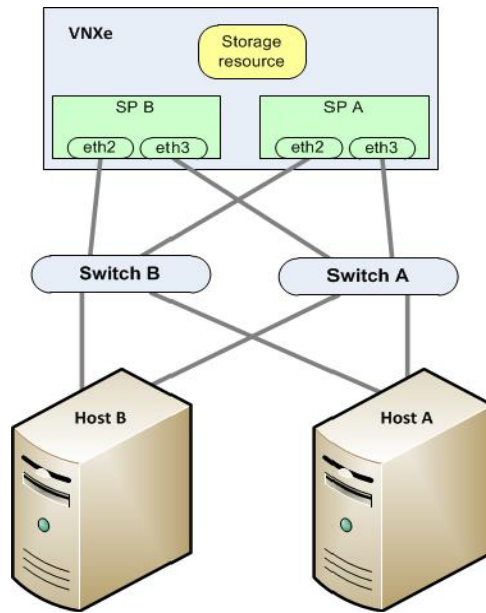


Figure 2 Sample highly-available iSCSI network

VNXe requirements

- ◆ You have installed and configured the VNXe system using the VNXe Configuration Wizard, as described in the *Installation Guide* for your storage system.
- ◆ You have used the Unisphere software or the VNXe CLI to create the VNXe iSCSI LUNs for the host and have added the host to the VNXe system. For information on performing these tasks refer to the Unisphere online help.

IMPORTANT

On a HP-UX host, the iSCSI initiator will not discover the VNXe iSCSI storage if it does not detect a LUN from the VNXe assigned to host LUN ID 0. We recommend that you to create a unique target (iSCSI interface), create a LUN on this iSCSI interface, and give it access to the HP-UX host. The first LUN that you assign to a host is automatically assigned host LUN ID 0.

Using multi-path management software on the host

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

- ◆ EMC PowerPath software on an HP-UX, Linux, or Solaris host
- ◆ Native multipath software on a Citrix XenServer, HP-UX 11i, Linux, or Solaris host

For the supported versions of the PowerPath or native multipath failover 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.

Setting up a VNXe system for multi-path management software

For a VNXe system to operate with hosts running multi-path management software, two iSCSI IPs are required, but they can be on different interfaces.

Check the configuration on the EMC Unisphere™ **Settings > iSCSI Settings** page. For details on how to configure iSCSI interfaces, refer to the topic on changing iSCSI interface settings in the Unisphere online help.

IMPORTANT

For highest availability, use two network interfaces on the iSCSI interface. The network interfaces should be on separate subnets. If the network interfaces are on the same subnet, a host will let you use only one interface. You can view the network interfaces for an iSCSI interface with Unisphere under Network Interface advanced settings (**Settings > iSCSI Settings**).

Installing PowerPath

1. On the host or virtual machine, download the latest PowerPath version from the PowerPath software downloads section on the EMC Online Support website (<http://support.emc.com>).
2. Install PowerPath as described in the appropriate PowerPath installation and administration guide for the host's or virtual machine'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.
3. When the installation is complete, reboot the host or virtual machine.
4. When the host or virtual machine is back up, verify that the PowerPath service has started.

Installing native multipath software

Whether you need to install multipath software, depends on the host's operating system.

Citrix XenServer

By default XenServer uses the Linux native multipathing (DM-MP) as its multipath handler. This handler is packaged with the Citrix XenServer operating system software.

Linux

To use Linux native multipath software, you must install the Linux multipath tools package as described in [“Installing or updating the Linux multipath tools package” on page 41](#).

HP-UX 11i

Native multipath failover is packaged with the HP-UX operating system software.

Solaris

Sun's native path management software is Sun StorEdge™ Traffic Manager (STMS).

For Solaris 10 — STMS is integrated into the Solaris operating system patches you install. For information on install patches, refer to the Sun website.

Installing or updating the Linux multipath tools package

To use Linux native multipath failover software, the Linux multipath tools package must be installed on the host. This package is installed by default on SuSE SLES 10 or higher, but is not installed by default on Red Hat.

If you need to install the multipath tools package, install the package from the appropriate website below.

For SuSE:

<http://www.novell.com/linux/>

The multipath tools package is included with SuSE SLES 9 SP3 and you can install it with YaST or RPM.

For Red Hat:

<http://www.redhat.com>

The multipath tools package is included with Red Hat RHEL4 U3 or RHEL5, and you can install it with YaST or Package Manager. If an update is available, follow the instructions for installing it on the <http://www.novell.com/linux/> or <http://www.redhat.com> website.

What next?

Do one of the following:

- ◆ To set up an AIX host to use iSCSI storage, refer to “[AIX host — Setting up for iSCSI storage](#)” on page 43.
- ◆ To set up a Citrix XenServer host to use iSCSI storage, refer to “[Citrix XenServer host — Setting up for iSCSI storage](#)” on page 45.
- ◆ To set up an HP-UX host to use iSCSI storage, refer to “[HP-UX host — Setting up for iSCSI storage](#)” on page 46.
- ◆ To set up a Linux host to use iSCSI storage, refer to “[Linux host — Setting up for iSCSI storage](#)” on page 49.
- ◆ To set up a Solaris host to use iSCSI storage, refer to “[Solaris host — Setting up for iSCSI storage](#)” on page 52.

AIX host — Setting up for iSCSI storage

To set up an AIX host to use VNXe iSCSI storage, perform these tasks:

- ◆ “Task 1: Install Celerra AIX software” on page 43
- ◆ “Task 2: Configure the AIX iSCSI initiator” on page 44
- ◆ “Task 3: Configure iSCSI LUNs as AIX disk drives” on page 44
- ◆ “Task 4: Prepare the LUNs to receive data” on page 44

Task 1: Install Celerra AIX software

1. Log in to the AIX host using an account with administrator privileges.
2. Download the AIX ODM Definitions software package to the /tmp directory on the AIX host as follows:
 - a. Navigate to AIX ODM Definitions on the software downloads section on the EMC Online Support website (<http://www.emc.com/vnxesupport>).
 - b. Choose the version of the EMC ODM Definitions for the version of AIX software running on the host, and save the software to the /tmp directory on the host.
3. In the /tmp directory, uncompress and untar the EMC AIX fileset for the AIX version running on the host:


```
uncompress EMC.AIX.x.x.x.x.tar.z
tar -xvf EMC.AIX.x.x.x.x.tar
```
4. Start the System Management Interface Tool to install the software:


```
smit installp
```
5. In the Install and Update Software menu, select **Install and Update from ALL Available Software** and enter **/tmp** as the path to the software.
6. Select **SOFTWARE to install**.
7. After making any changes to the displayed values, press **Enter**.
8. Scroll to the bottom of the window to see the Installation Summary, and verify that the message “SUCCESS” appears.
9. Reboot the AIX host to have the changes take effect.

Task 2: Configure the AIX iSCSI initiator

Enable the AIX host to discover iSCSI targets on the VNXe system:

1. On the VNXe system, from the **iSCSI Settings** page in Unisphere (**Settings** > **iSCSI Settings**), determine the IQN and the IP address of the VNXe system iSCSI interface (target) to which you want the host initiator to connect.
2. On the AIX host, start the System Management Interface Tool:
smit
3. Using a text editor, open the file `/etc/iscsi/targets`.
4. For each VNXe iSCSI interface to be accessed by this initiator, add a line in the format:
`<portal> <port> <target_iqn>`
where:
`<portal>` = IP address of the network portal
`<port>` = number of the TCP listening port (default is 3260)
`<target_iqn>` = formal iSCSI name of the Celerral target

Task 3: Configure iSCSI LUNs as AIX disk drives

On the AIX host:

1. Discover the VNXe iSCSI LUNs as disk drives:
cfgmgr
2. To list the iSCSI LUN, enter
lsdev -Cc disk

Task 4: Prepare the LUNs to receive data

If you do not want to use a LUN as a raw disk or raw volume, then before AIX can send data to the LUN, you must either partition the LUN or create a database file systems on it. For information on how to perform these tasks, refer to the AIX operating system documentation.

Citrix XenServer host — Setting up for iSCSI storage

To set up a Citrix XenServer host to use VNXe iSCSI storage, perform these tasks:

- ◆ “Task 1: Configure the iSCSI software initiator” on page 45
- ◆ “Task 2: Configure the iSCSI software initiator for multipathing” on page 45

Task 1: Configure the iSCSI software initiator

The XenServer operating system include iSCSI software that you must configure for each initiator that will connect to the VNXe iSCSI storage.

1. On the VNXe system, from the **iSCSI Settings** page in Unisphere (**Settings** > **iSCSI Settings**), determine the IP address of the VNXe system iSCSI interface (target) to which you want the host initiator to connect.
2. Open the XenCenter console.
3. Click **New Storage** at the top of the console.
4. In the **New Storage** dialog box, under **Virtual disk storage**, select **iSCSI**.
5. Under **Name**, enter a descriptive name of the VNXe virtual disk (Storage Repository).
6. To use optional CHAP
 - a. Check **Use CHAP**.
 - b. Enter the CHAP username and password.
7. Click **Discover IQNs**.
8. Click **Discover LUNs**.
9. Once the **IQN** and **LUN** fields are populated, click **Finish**.

The host scans the target to see if it has any XenServer Storage Repositories (SRs) on it already, and if any exist you are asked if you want to attach to an existing SR or create a new SR.

Task 2: Configure the iSCSI software initiator for multipathing

Citrix recommends either enabling multipathing in XenCenter before you connect the pool to the storage device or if you already created the storage repository, putting the host into Maintenance Mode before you enable multipathing.

If you enable multipathing while connected to a storage repository, XenServer may not configure multipathing successfully. If you already created the storage repository and want to configure multipathing, put all hosts in the pool into Maintenance Mode before configuring multipathing and then configure multipathing on all hosts in the pool. This ensures that any running virtual machines that have LUNs in the affected storage repository are migrated before the changes are made.

1. In XenCenter enable the multipath handler:
 - a. On the host’s **Properties** dialog box, select the **Multipathing** tab.
 - b. On the **Multipathing** tab, select **Enable multipathing on this server**.
2. Verify that multipathing is enabled by clicking the storage resource’s **Storage general properties**.

HP-UX host — Setting up for iSCSI storage

To set up an HP-UX host to use VNXe iSCSI storage, perform these tasks:

- ◆ “Task 1: Download and install the HP-UX iSCSI initiator software” on page 46.
- ◆ “Task 2: Configure HP-UX access to a VNXe iSCSI interface (target)” on page 46.
- ◆ “Task 3: Make the VNXe storage processors available to the host” on page 48.
- ◆ “Task 4: Verify that native multipath failover sees all paths the LUNs” on page 48.
- ◆ “Task 5: Prepare the LUNs to receive data” on page 48.

Task 1: Download and install the HP-UX iSCSI initiator software

1. On the HP-UX host, open a web browser and download the iSCSI initiator software from the HP-UX website.
1. Install the initiator software using the information on the site or that you downloaded from the site.

Task 2: Configure HP-UX access to a VNXe iSCSI interface (target)

Before an HP-UX iSCSI initiator can send data to or received data from VNXe iSCSI LUNs, you must configure the network parameters for the NIC initiators so that they can connect to the VNXe iSCSI interface (target) with the iSCSI LUNs.

To configure access to a VNXe iSCSI interface:

1. Log into the HP-UX host as `superuser` (`root`).
2. Add the path for the `iscsi` util and other iSCSI executables to the root path:

```
PATH=$PATH:/opt/iscsi/bin
```

3. Verify the iSCSI initiator name:

```
iscsiutil -l
```

The iSCSI software initiator configures a default initiator name in an iSCSI Qualified Name (IQN) format.

For example:

```
iqn.1986-03.com.hp:hpfc214.2000853943
```

To change the default iSCSI initiator name or reconfigure the name to an IEEE EUI-64 (EUI) format, continue to the next step; otherwise skip to [step 5](#).

4. Configure the default iSCSI initiator name:

```
iscsiutil [iscsi-device-file] -i -N iscsi-initiator-name
```

Note: For mor information on IQN and EUI formats, refer to the HP-UX `iscsi` software initiator guide.

where:

iscsi-device-file is the iSCSI device path, */dev/iscsi*, and is optional if you include the **-i** or **-N** switches in the command.

-i configures the iSCSI initiator information.

-N is the initiator name. When preceded by the **-i** switch, it requires the iSCSI initiator name. The first 256 characters of the name string are stored in the iSCSI persistent information.

iscsi-initiator-name is the initiator name you have chosen, in IQN or EUI format.

5. Verify the new iSCSI initiator name:

```
iscsiutil -l
```

6. For each iSCSI target device you will statically identify, store the target device information in the kernel registry, adding one or more discovery targets:

```
iscsitutil [/dev/iscsi] -a -I ip-address/hostname [-P tcp-port] [-M portal-grp-tag]
```

where

-a adds a discovery target address into iSCSI persistent information. You can add discovery target addresses only with this option.

-I requires the IP address or hostname of the discovery target address.

ip-address/hostname is the IP address or host name component of the target network portal.

-P *tcp-port* is the listening TCP port component of the discovery target network portal (optional). The default iSCSI TCP port number is 3260.

-M *portal-grp-tag* is the target portal group tag (optional). The default target portal group tag for discovery targets is 1.

For example:

```
iscsiutil -a -I 192.1.1.110
```

or, if you specify the hostname,

```
iscsiutil -a -I target.hp.com
```

If an iSCSI TCP port used by the discovery target is different than the default iSCSI port of 3260, you must specify the default TCP port used by the discovery target, for example,

```
iscsiutil -a -I 192.1.1.110 -P 5001
```

or

```
iscsiutil -a -I target.hp.com -P 5001
```

7. Verify the discovery targets that you have configured:

```
iscsiutil -p -D
```

8. To discover the operational target devices:

```
/usr/sbin/ioscan -H 225
```

```
ioscan -NfC disk (for HP-UX 11i v3 only)
```

9. To create the device files for the targets:

```
/usr/sbin/insf -H 225
```

10. To display operational targets:

```
iscsiutil -p -O
```

Task 3: Make the VNXe storage processors available to the host

Verify that each NIC sees only the storage processors (targets) to which it is connected:

```
ioscan -fnC disk
```

```
insf -e
```

```
ioscan -NfC disk (for HP-UX 11i v3 only)
```

Task 4: Verify that native multipath failover sees all paths the LUNs

If you are using multipath failover:

1. Rescan for the LUNs:

```
ioscan -NfC disk|
```

```
insf -e
```

2. View the LUNs available to the host:

```
ioscan -NfnC disk
```

3. Verify that all paths to the VNXe system are CLAIMED:

```
ioscan -NkfnC lunpath
```

Task 5: Prepare the LUNs to receive data

If you do not want to use a LUN as a raw disk or raw volume, then before HP-UX can send data to the LUN, perform the following tasks as described in the HP-UX operating system documentation:

1. Make the LUN visible to HP-UX.

2. Create a volume group on the LUN.

Linux host — Setting up for iSCSI storage

To set up a Linux host to use VNXe iSCSI storage, perform these tasks:

- ◆ “Task 1: Configure Linux iSCSI initiator software” on page 49
- ◆ “Task 2: Set up the Linux host to use the VNXe iSCSI LUN” on page 51

Task 1: Configure Linux iSCSI initiator software

The Linux operating system includes the iSCSI initiator software — the iSCSI driver **open-iscsi** — that comes with the Linux kernel. You must configure this open-iscsi driver with the network parameters for each initiator that will connect to VNXe iSCSI storage.

NOTICE

The Linux iSCSI driver gives the same name to all network interface cards (NICs) in a host. This name identifies the host, not the individual NICs. This means that if multiple NICs from the same host are connected to a VNXe iSCSI interface on the same subnet, then only one NIC is actually used. The other NICs are in standby mode. The host uses one of the other NICs only if the first NIC fails.

Each host connected to an iSCSI storage system must have a unique iSCSI initiator name for its initiators (NICs). To determine a host's iSCSI initiator name for its NICs use `cat /etc/iscsi/initiatorname.iscsi` for open-iscsi drivers. If multiple hosts connected to the VNXe iSCSI interface have the same iSCSI initiator name, contact your Linux provider for help with making the names unique.

To configure the Linux **open-iscsi** driver:

IMPORTANT

The *EMC Host Connectivity Guide for Linux* on the EMC Online Support website (<http://www.emc.com/vnxesupport>) provide the latest information about configuring the **open-iscsi** driver.

1. From the **iSCSI Settings** page in Unisphere (**Settings** > **iSCSI Settings**), determine the IP address of the VNXe iSCSI interface (target) to which you want the host initiators to connect.
2. For any Linux initiators connected to the VNXe iSCSI interface with CHAP authentication enabled, stop the iSCSI service on the Linux host.
3. Using a text editor, such as vi, open the `/etc/iscsi/iscsi.conf` file.
4. Uncomment (remove the # symbol) before the recommended variable settings in the iSCSI driver configuration file as listed in [Table 3 on page 50](#).

Table 3 Open-iscsi driver recommended settings

Variable name	Default setting	Recommended setting
node.startup	manual	auto
node.session.iscsi.InitialR2T	No	Yes
node.session.iscsi.ImmediateData	Yes	No
node.session.timeo.replacement_timeout	120	120 ¹
node.conn[0].timeo.timeo.noop_out_interval	10	later in congested networks ²
node.conn[0].timeo.timeo.noop_out_timeout	15	later in congested networks ²

1. In congested networks you may increase this value to 600. However, this time must be greater than the combined node.conn[0].timeo.timeo.noop_out_interval and node.conn[0].timeo.timeo.noop_out_time times.

2. This value should *not* exceed the values in node.session.timeo.replacement_timeout.

5. To start the iSCSI service automatically on reboot and powerup, set the run level to 345 for the iSCSI service.

6. Discover and log in to the host to which you want to connect with the **iscsiadm** command for Red Hat 5 or later or YaST for SuSE 10 or later.

You need to perform a discovery on only a single IP address because the VNXe system also returns its other iSCSI target, if it is configured for a second iSCSI interface.

7. Configure optional CHAP authentication on the open-iscsi driver initiator:

For Red Hat 5 or later

Use the **iscsiadm** command to do the following:

For optional initiator CHAP:

- a. Enable CHAP as the authentication method.
- b. Set the username for the initiator to the initiator's IQN, which you can find with the **iscsiadm -m node** command.
- c. Set the secret (password) for the initiator to the *same* secret that you entered for the host initiator on the VNXe system.

For optional mutual CHAP

- a. Set the username (username_in) to the initiator's IQN, which you can find with the **iscsiadm -m node** command.
- b. Set the secret (password_in) for the target to the *same* secret that you entered for the VNXe iSCSI interface.

For SuSE 10 or later

Use the YaST to do the following for the open-iscsi driver initiator:

For optional initiator CHAP:

- a. Enable *incoming* authentication.
- b. Set the initiator CHAP username to the initiator's IQN, which you can find with the **iscsiadm -m node** command.

- c. Set the initiator CHAP password (secret) to the *same* secret that you entered for the host initiator on the VNXe system.

For mutual CHAP:

- a. Enable *outgoing* authentication (mutual CHAP).
 - b. Set the mutual CHAP username to the initiator's IQN, which you can find with the **iscsiadm -m node** command.
 - c. Set the initiator password (secret) for the target to the *same* secret that you entered for the VNXe iSCSI interface.
8. Find the driver parameter models you want to use, and configure them as shown in the examples in the configuration file.
 9. Restart the iSCSI service.

Task 2: Set up the Linux host to use the VNXe iSCSI LUN

Perform the following tasks as described in the Linux operating system documentation:

1. Find the LUN number of the LUN:
 - a. In Unisphere, select **Storage > LUNs**.
 - b. Select the LUN, click **Details**, and click the **LUNs** tab.
2. On the host, partition the LUN.

If the host does not see the LUN, you can have problems with the iSCSI session between the host and an iSCSI target (VNXe iSCSI interface). To troubleshoot this problem, see [“iSCSI session troubleshooting” on page 54](#).

3. Create a file system on the partition.
4. Create a mount directory for the file system.
5. Mount the file system.

The Linux host can now write data to and read data from the file system on the LUN.

Solaris host — Setting up for iSCSI storage

To set up a Solaris host to use VNXe iSCSI storage, perform these tasks:

- ◆ “Task 1: Configure Sun StorEdge Traffic Manager (STMS)” on page 52.
- ◆ “Task 2: Configure Solaris access to a VNXe iSCSI interface (target)” on page 53
- ◆ “Task 3: Prepare the LUN to receive data” on page 53

Task 1: Configure Sun StorEdge Traffic Manager (STMS)

If you want to use STMS on the host to manage the paths to the VNXe LUNs, you must first configure it:

1. Enable STMS by editing the following configuration file:

Solaris 10 — Do one of the following:

- Edit the `/kernel/drv/fp.conf` file by changing the `mpxio-disable` option from `yes` to `no`.
- or
- Execute the following command:
`stmsboot -e`

2. We recommend that you enable the STMS auto-restore feature to restore LUNs to their default SP after a failure has been repaired. In Solaris 10, auto-restore is enabled by default.
3. If you want to install STMS offline over NFS, share the root file system of the target host in a way that allows root access over NFS to the installing host, if you want to install STMS offline over NFS. You can use a command such as the following on `target_host` to share the root file system on `target_host` so that `installer_host` has root access:

```
share -F nfs -d `root on target_host` -o ro,rw=installer  
host,root=installer_host /
```

If the base directory of the package (the default is `/opt`) is not part of the root file system, it also needs to be shared with root access.

4. For the best performance and failover protection, we recommend that you set the load balancing policy to round robin:

```
setting load-balance="round-robin"
```

Task 2: Configure Solaris access to a VNXe iSCSI interface (target)

Before a Solaris iSCSI initiator can send data to or receive data from VNXe iSCSI LUNs, you must configure the network parameters for the NIC initiators so that they can connect to the VNXe iSCSI interface (target) with the iSCSI LUNs.

To configure access to a VNXe iSCSI interface:

1. Log into the Solaris system as superuser (root).
2. Configure the target device to be discovered using SendTargets dynamic discovery.

Example:

```
iscsiadm modify discovery-address 10.14.111.222:3260
```

Note: If you do not want the host to see specific targets, use the static discovery method as described in the Solaris server documentation.

3. Enable the SendTargets discovery method.

Examples:

```
iscsiadm modify discovery --sendtargets enable
```

or

```
iscsiadm modify discovery -t enable
```

4. Create the iSCSI device links for the local system.

For example:

```
devfsadm -l iscsi
```

5. If you want Solaris to login to the target more than once (multiple paths), use:

```
iscsiadm modify target-param -c <logins> <target_iqn>
```

where *logins* is the number of logins and *target_iqn* is the IQN of the VNXe iSCSI interface (target).

Note: You can determine the IQN of the VNXe iSCSI interface from Unisphere on the **iSCSI Settings** page (**Settings** > **iSCSI Settings**).

Task 3: Prepare the LUN to receive data

If you do not want to use the LUN as a raw disk or raw volume, then before Solaris can send data to the LUN, you must perform the following tasks as described in the Solaris operating system documentation:

1. Partition the LUN.
2. Create and mount a file system on the partition.

What next?

You are now ready to either migrate data to the LUN or have the host start using the LUN. To migrate data to the LUN, go to [Chapter 5, “Migrating FC or iSCSI Data to the VNXe System.”](#)

iSCSI session troubleshooting

If you receive a connection error when the host is trying to log in to an iSCSI target (VNXe iSCSI interface), or you cannot see the LUNs on the target, you can be having problems with the iSCSI session between the initiator and the target.

If the session cannot be established or you get unexpected results from the session, follow this procedure:

1. Use **ping** with the IP address to verify connectivity from the host to the target's IP address.

Using the IP address avoids name resolution issues.

Note: You can find the IP address for the target by selecting **Settings > iSCSI 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. Check the host routing configuration using Unisphere under **Settings > More configuration > Routing Configuration**.
3. On the host, verify that the iSCSI initiator service is started.

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

4. In the Microsoft iSCSI Initiator, verify the following for the VNXe target portal:

- IP address(es) or DNS name of the VNXe iSCSI interface with the host's LUNs.

Note: For a host running PowerPath or Windows native failover, VNXe target portal has two IP addresses.

- Port is 3260, which is the default communications port for iSCSI traffic.

5. Verify that the iSCSI qualified names (IQN) for the initiators and the iSCSI interface name for the target are legal, globally unique, iSCSI names.

Note: An iQN must be a globally unique identifier of as many as 223 ASCII characters.

For a Linux host initiator — You can find this IQN with the **iscsiadm -m node** command, which lists the IP address and associated iqn for each iSCSI initiator.

For a Solaris host initiator — You can find this IQN with the **iscsi list initiator-node** command.

6. If you are using optional CHAP authentication, ensure that the following two secrets are *identical* by resetting them to the same value:
 - The secret for the host initiator in the host's iSCSI software.
 - The secret configured for the host initiator on the VNXe iSCSI interface.

7. If you are using optional mutual CHAP authentication, ensure that the following two secrets are *identical* by resetting them to the same value:
 - The secret for the host initiator in the host's iSCSI software.
 - The secret for the iSCSI interface on the VNXe iSCSI interface. You can find this secret in the **CHAP Security** section on the iSCSI Settings page in Unisphere (**Settings** > **iSCSI Settings**).

CHAPTER 3

Setting Up a Windows or Mac OS Host to Use VNXe LUN storage over FC

This chapter describes how to set up a Windows or Mac OS host to use EMC VNXe LUN storage over FC.

Topics include:

- ◆ Requirements for setting up a host to use VNXe LUN storage over Fibre Channel..... 58
- ◆ VNXe VSS HW Provider overview..... 59
- ◆ Windows host — Using multi-path management software..... 61
- ◆ Windows host — Setting up for FC LUNs 63
- ◆ Windows host — Connecting to a VNXe FC LUN 66
- ◆ Windows host — Setting up to use VNXe FC LUNs 68
- ◆ Mac OS host — Setting up for FC LUNs..... 70

Requirements for setting up a host to use VNXe LUN storage over Fibre Channel

Before you set up a host to use VNXe LUN storage over FC, the 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 *Installation Guide* for your storage system.
- ◆ You have used Unisphere or the VNXe CLI to perform basic configuration of one or more FC LUNs on the VNXe system.

SAN requirements

For a host to connect to FC LUNs on VNXe, the host must be in a SAN environment with the VNXe, and zoned so that the host and the VNXe are visible to each other over the SAN. For a Windows multi-pathing environment, each VNXe FC LUN for the host, must have two paths associated with it. These two paths should be on different switches to ensure high availability.

Path management SAN requirements

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

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

- ◆ A VNXe LUN is visible to both SPs
- ◆ You can configure multiple paths for a LUN. These paths should be associated with separate physical ports on the same SP.
- ◆ Each LUN must present the same LUN ID to all hosts.

IMPORTANT

Directly attaching a host to a VNXe system is supported if the host connects to both SPs and has the required multipath software.

VNXe VSS HW Provider overview

The VSS HW Provider runs as a Windows service and provides the interface between the Microsoft Volume Shadow Copy Service (VSS) and VNXe. The VNXe VSS HW Provider enables VSS requestor applications, such as VSS-enabled backup applications, to make snapshots of VNXe iSCSI and FC LUNs.

Microsoft VSS

VSS provides the backup framework for Windows Server 2003 R2, Windows Server 2008, and Windows Server 2012 and enables the creation of snapshots (called shadow copies for Microsoft VSS) — point-in-time copies of data. VSS is integrated with front-end applications so they can create and access shadow copies.

Microsoft VSS shadow copies are:

- ◆ Read-only by default
- ◆ Limited to 512 per volume

The VSS architecture includes VSS providers. A VSS provider creates and maintains shadow copies and acts as the interface to point-in-time imaging capabilities either on a storage platform (hardware-based provider) or in a host operating system (software-based provider).

The VNXe VSS HW Provider is a hardware-based provider that works directly with VNXe iSCSI and FC LUNs and with the VSS service on Windows Server 2003 R2, Windows Server 2008, or Windows Server 2012 hosts to provide consistent shadow copy creation and addressing.

Because the VNXe VSS HW Provider is a hardware-based provider, it reduces the load on the CPU and memory of the host. It is also more efficient in an environment where shadow copies of multiple volumes must be taken simultaneously.

The Microsoft website provides more information about VSS and VSS components.

Types of shadow copies

VSS produces three types of shadow copies:

- ◆ Plex copies — Shadow copies initially created by mirroring. A plex copy is a special type of shadow copy data that represents a shadow copy without the need for the original volume data.
- ◆ Differential copies — Shadow copies created by saving only the differences from the original volumes.
- ◆ Redirect-on-write copies — This method does not copy the original volume. It does not make any changes to the original volume after a given time. Instead, it makes a differential copy by redirecting all changes to a different volume.

The VNXe VSS HW Provider supports only differential shadow copies.

Shadow copy backups

You can use VSS shadow copies to back up data on an FC host system. The benefits of shadow copy backups are:

- ◆ You can back up open files.
- ◆ You can copy application data without stopping the application or restricting user access.

Shadow copy backups are available only on Windows Server 2003R2, Windows Server 2008, and Windows Server 2012 and require a VSS provider (such as the VNXe VSS HW Provider) and a backup application that supports VSS (such as EMC NetWorker or Symantec Backup Exec).

Shadow copy transport

Using a hardware VSS provider, such as the VNXe VSS HW Provider, you can create transportable shadow copies for import to other hosts for:

- ◆ Data mining — Make the data in a production database available to other applications by using a shadow copy of the database with those applications.
- ◆ Backup — Instead of overloading a production server with backup traffic, move a shadow copy of a database to another host, and then back up the shadow copy instead of the production database.
- ◆ Data recovery — Keep shadow copies of production data for quick restores. Since creating shadow copies is quick and nondisruptive, shadow copies complement tape-based recovery solutions.

Transportable shadow copies are available with Windows Server 2003 R2, Windows Server 2008, and Windows Server 2012 Enterprise or Datacenter editions.

Limitations

The VNXe VSS HW Provider does *not* support:

- ◆ Microsoft Windows Shadow Copy for Shared Folders.
- ◆ Importing shadow copies to clustered servers. Although you can create shadow copies in a Microsoft Cluster Server (MSCS) environment, you cannot import shadow copies because of a Microsoft restriction. Importing shadow copies to remote hosts is an advanced VSS feature called Shadow Copy Transport, which requires both a hardware VSS provider, such as the VNXe VSS HW Provider, and a third-party VSS requestor that supports Shadow Copy Transport.

[“Shadow copy transport” on page 60](#) provides more information about this VSS feature.

To use Shadow Copy Transport to back up data on a cluster, you must transport and import shadow copies to a nonclustered backup server.

Windows host — 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 a Windows 2003, Windows Server 2008, or Windows Server 2012 host connected to a VNXe system:

- ◆ EMC PowerPath software on a Windows 2003, Windows Server 2008, or Windows Server 2012 host.

For the supported versions of the PowerPath 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.

Note: PowerPath is not supported for Windows 7.

For information on data availability in the VNXe system and in your connectivity infrastructure, refer to *EMC VNXe High Availability, A Detailed Review*, 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 LUN on the VNXe system should be associated with multiple paths.

IMPORTANT

For highest availability, use multiple paths. The network interfaces can be on separate subnets.

Installing PowerPath

1. You cannot configure your VNXe FC connections to present the VNXe FC LUNs to both a standalone Windows host and its Windows virtual machines. If you will configure your VNXe FC connections to present the VNXe FC LUNs directly to a stand-alone Windows host with HBAs, install PowerPath software on the stand-alone host. If you will configure your VNXe FC connections to present VNXe FC LUNs directly to a Windows virtual machine with HBAs, install PowerPath software on the virtual machine. On the host or virtual machine, download the latest PowerPath version from the PowerPath software downloads section on the EMC Online Support website (<http://support.emc.com>).
2. Install PowerPath using a Custom installation and the Celerra option, as described in the appropriate PowerPath installation and administration guide for the host's or virtual machine'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.

3. When the installation is complete, reboot the host or virtual machine.
4. When the host or virtual machine is back up, verify that the PowerPath service has started.

Configuring VNXe FC LUNs for the host

Use Unisphere or the VNXe CLI to:

1. Create VNXe FC LUNs for the host.
2. Add the host to the VNXe system by accessing the **Hosts** tab in Unisphere or using the VNXe CLI and creating a host.
3. Provide host access to the VNXe FC LUNs. Host access options are: **No Access, LUN, Snapshot, LUN and Snapshot.**

IMPORTANT

On a Mac OS host, Xsan will not log into the VNXe FC storage if no vdisk0 is configured on the VNXe.

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

Windows host — Setting up for FC LUNs

To set up a Windows host for FC LUNs, perform these tasks:

- ◆ [“Task 1: Install the VNXe VSS HW Provider” on page 63.](#)
- ◆ [“Task 2: For a multi-path configuration, install the MPIO feature” on page 64.](#)
- ◆ [“Task 3: Set registry values” on page 64.](#)

Task 1: Install the VNXe VSS HW Provider

EMC recommends that you install the VNXe VSS HW Provider on the host that will use the iSCSI or FC LUNs with backup applications such as EMC NetWorker® and Symantec Backup Exec.

Note: [“VNXe VSS HW Provider overview” on page 59](#) provides information about the VNXe VSS HW Provider.

To install the VNXe VSS HW Provider:

1. Log in to the host using an account with administrator privileges.
2. Download the software package that you want to install as follows:
 - a. Navigate to the Volume Shadow Service (VSS) in the VNXe software downloads section on the **Support** tab of the EMC Online Support website.
 - b. Choose the Volume Shadow Service for your Windows platform, and select the option to save the software to the host.
3. In the directory where you saved the software, double-click the VNXe VSS HW Provider executable file to start the installation wizard.
4. In the **Introduction (Step 1 of 4)** dialog box, click **Next**.
5. In the **Choose Install Folder (Step 2 of 4)** dialog box, select the installation path for the VNXe VSS HW Provider.
6. In the **Pre-Installation Summary (Step 3 of 4)** dialogue box, confirm that you are ready to install by clicking the **Install** button.
7. In the **Installation Complete (Step 4 of 4)** dialog box, click **Finish**.

Starting and stopping the VNXe VSS HW Provider

The VNXe VSS HW Provider runs as a Windows service and is enabled by default. You can stop and start this service from the Windows Services administrative tool.

Task 2: For a multi-path configuration, install the MPIO feature

If the Windows host will use a multi-path configuration to connect to the VNXe FC LUNs, you should install the MPIO feature.

1. Open Server Manager.
2. In the **Server Manager** tree, click **Features**.
3. In the **Features** pane, under **Features Summary**, click **Add Features**.
4. In the **Add Features Wizard**, select **Multipath I/O**, and click **Next**.
5. In the **Confirm Installation Selections** dialog box, click **Install**.
6. When the installation is complete, in the **Installation Results** dialog box, click **Close**.
7. When prompted to restart the computer, click **Yes**.

After restarting, the host finalizes the MPIO installation.

8. Click **Close**.

Task 3: Set registry values

NOTICE

Incorrectly modifying the Registry can cause serious system-wide problems that can require you to reinstall the system. Use the Windows Registry Editor at your own risk.

1. On the host, run the Windows Registry Editor (**regedit.exe**).
2. Go to HKEY_LOCAL_MACHINE\SYSTEM\.
3. Right-click **CurrentControlSet**, and search for the **MaxRequestHoldTime** key and modify its value from 60 to 600 (decimal) or from 3c to 258 (hexadecimal).

IMPORTANT

Verify that the path to the parameter is in the CurrentControlSet. If it is not, search for the parameter again. If you make changes to ControlSets other than the top level current set, those changes will not affect the system.

4. If the host is running PowerPath:
 - a. Search for the register keys list in [Table 4](#).

IMPORTANT

Verify that the path to the parameter that you found in the CurrentControlSet. If it is not, search for the parameter again. If you make changes to ControlSets other than the top level current set, those changes will not affect the system.

- b. Record the value of each of these registry keys, so you have them in case you need to uninstall PowerPath.

- c. Update each of these registry keys [Table 4](#).

Table 4 Registry keys to update

Registry keys	Instructions
LinkDownTime	Set to 600.
AsyncLogoutPauseTimeout (new value)	Add this REG_DWORD key in the same key as LinkDownTime. Set it to 600.
DelayBetweenReconnect PortalRetryCount	Find the DelayBetweenReconnect value. Set the PortalRetryCount value so that $\text{PortalRetryCount} \times \text{DelayBetweenReconnect} = 600$
SrbTimeoutDelta for PowerPath only	Set to 100 for PowerPath only.

5. Quit the Registry Editor.

Windows host — Connecting to a VNXe FC LUN

Windows hosts connect directly to VNXe FC LUNs that they have access to across the SAN. To connect a Windows host to a VNXe FC LUN:

- ◆ [“Configuring a Windows Server 2003 or Windows 2008 SP2 host to connect to a VNXe FC LUN” on page 66](#)
- ◆ [“Configuring a Windows Server 2008 R2, Windows Server 2012, Windows7, or Windows 8 host to connect to a VNXe FC LUN” on page 67](#)

Configuring a Windows Server 2003 or Windows 2008 SP2 host to connect to a VNXe FC LUN

To add VNXe FC storage to a Windows Server host:

1. Select **LUN Management** > **Manage Server Connections**.
2. Click **Add**.
3. In the **Add Server** window, add the VNXe, and optionally specify a description.
4. Click **OK**. The VNXe appears in the **Manage Server Connections** window. All the ports that were discovered appear on the **Fibre Channel Ports** tab.
5. Optionally, add additional FC ports manually:
 - a. Select the **Fibre Channel Ports** tab.
 - b. Click **Add**.
 - c. Specify the WWN of the FC port.
 - d. Click **OK**.
6. Enable the FC ports for LUN access:
 - a. Select the VNXe from the server list.
 - b. Select the **Fibre Channel Ports** tab. Select FC ports to enable.

Note: If the VNXe is not configured for multipathing, enabling more than one FC port may cause data corruption.
 - c. Click **OK**.

What next?

Continue to ["Windows host — Setting up to use VNXe FC LUNs" on page 68](#).

Configuring a Windows Server 2008 R2, Windows Server 2012, Windows7, or Windows 8 host to connect to a VNXe FC LUN

To add VNXe FC storage to a Windows Server 2008 R2, Windows Server 2012, Windows 7, or Windows 8 host:

1. Open Storage Manager for SANs. Click **Manage Server Connections**.
2. Click **Add**.
3. In the **Add Server** window, add the VNXe, and optionally specify a description.
4. Click **OK**. The VNXe appears in the **Manage Server Connections** window. All the ports that were discovered appear on the **Fibre Channel Ports** tab. Optionally, add additional FC ports manually:
 - a. Select the **Fibre Channel Ports** tab.
 - b. Click **Add**.
 - c. Specify the WWN of the FC port.
 - d. Click **OK**.
5. Enable the FC ports for LUN access:
 - a. Select the VNXe from the server list.
6. Select the **Fibre Channel Ports** tab. Select FC ports to enable. If the VNXe is not configured for Multipathing, enabling more than one FC port may cause data corruption. Click **OK**.

What next?

Continue to [“Windows host — Setting up to use VNXe FC LUNs” on page 68](#).

Windows host — Setting up to use VNXe FC LUNs

To set up a Windows host to use VNXe FC LUNs, perform the following tasks:

- ◆ “Task 1: Register the LUNs as MPIO devices (Windows Server 2008 R2 and Windows Server 2012)” on page 68.
- ◆ “Task 2: Set the offset for the LUN to 64 KB” on page 68.
- ◆ “Task 3: Configure a volume on the LUN” on page 69.

Task 1: Register the LUNs as MPIO devices (Windows Server 2008 R2 and Windows Server 2012)

If you are using Multipath I/O (MPIO) with Windows Server, you must register the VNXe LUNs as MPIO devices and set up MPIO to discover FC devices:

1. On the host, start the MPIO Administrative Tool:

Either **Start > Administrative Tools** and select **MPIO** or **Start > Run** and enter **mpioctrl.exe**.

2. Open the MPIO control panel, and click the **Discover Multi-Paths** tab.
3. Select the **Add support for FC devices** check box, and click **Add**.
4. When prompted to restart the computer, click **Yes**.

When the computer restarts, the MPIO Devices tab lists the additional hardware ID “MSFT2005iSCSIBusType_0x9.” When this hardware ID is listed, all iSCSI bus attached devices will be claimed by the Microsoft DSM.

5. Restart the host when prompted.

Task 2: Set the offset for the LUN to 64 KB

Note: This task is only required for systems running Hyper-V on Windows Server 2003, or systems that were upgraded from Windows Server 2003 to Windows Server 2008 or later.

After the initiator logs in to a target, each of the target’s LUNs that the initiator can access appears as an unknown disk in the Windows Disk Management tool.

To set the offset for the LUN on the host:

1. Select **Run > diskpart**.
2. Select the disk:

select disk *n*

where *n* is the disk number.

If you do not know the disk number, enter:

list disk

3. On the selected disk, create a primary partition with an offset of 64 KB:
create part pri align=64

Task 3: Configure a volume on the LUN

The following configuration process initializes the LUN, creates a partition, formats a volume on the partition, and mounts the partition on a drive letter:

1. On the host, in the Microsoft Disk Management tool, select the LUN.
2. If the system asks you to initialize the disk, click **Yes**, but do not choose to make the disk a dynamic disk because the VNXe FC LUNs do not support dynamic disks.

For a given LUN, its drive letter, disk number, and LUN number are independent.

3. Use a quick format operation (Windows Server 2003 or Windows Server 2008) or the New Simple Volume wizard (Windows 7, Windows 8, or Windows Server 2012) to create a volume on the disk with the following properties:
 - NTFS file system
 - 64K location unit size

IMPORTANT

Do not format more than one LUN at a time. Otherwise, some of the volumes can become write-protected and cannot be formatted.

You can change the volume label. Because the disk number of a LUN can change after system restart or after logging in to and out of a target, be sure to change the default volume label ("New Volume") to a descriptive label.

4. Assign an available drive letter to the disk.
5. Close the Disk Management tool.

Mac OS host — Setting up for FC LUNs

To set up a Mac OS for FC LUNs, you must perform these tasks:

- ◆ [“Task 1:Installing and configuring Xsan on a Mac OS host” on page 70.](#)
- ◆ [“Task 2:Set up a Mac OS host to use the VNXe FC LUN” on page 70.](#)

Task 1: Installing and configuring Xsan on a Mac OS host

To connect a Mac OS host to VNXe FC storage, you must add the host to the SAN as a client.

1. On the host, select **System Preferences > Xsan**. Click **Enable Xsan**.
2. Install the Xsan software on the host, and update it to the latest version.
3. Open Xsan Admin and select **Computers**.
4. Add the host to the SAN.

Task 2: Set up a Mac OS host to use the VNXe FC LUN

Before the Mac OS host can use the VNXe FC LUN, you must use the Mac OS Disk Utility to:

- ◆ [“Task 1:Format the VNXe FC LUN” on page 70](#)
- ◆ [“Task 2:Partition the VNXe FC LUN” on page 71](#)

Task 1: Format the VNXe FC LUN

1. On the host, go to **Finder > Application > Utilities**.
2. Double-click **Disk Utility**.
3. In the left panel, select the VNXe FC LUN.
4. Click the **Erase** tab.
5. For **Volume Format**, select the format that you want, and confirm your format choice.
6. Click **Erase** and verify the erase procedure, and click **Erase** again to start the erase process.

When the erase process is finished, the LUN is ready for you to partition it.

Task 2: Partition the VNXe FC LUN

1. On the host, go to **Finder > Application > Utilities**.
2. Double click **Disk Utility**.
3. In the left panel, select the VNXe FC LUN.
4. Click the **Partition** tab.
5. Under Volume Scheme, select the number of partitions for the LUN.

The utility displays equal-sized partitions to fill the available space on the LUN.

6. For each partition:
 - a. Select the partition.
 - b. In **Name**, enter a name for the partition.
 - c. Under **Format**, select the format for the partition.

The default format - Mac OS Extended (Journaled) - is a good choice for most uses.

- d. In **Size**, enter the size for the partition.
7. When you have specified, the name, size, and format for each partition, click **Apply**.

The Disk Utility uses the partition information to create volumes that the host can access and use. When the partitioning process is complete, the new volumes are mounted on the desktop and ready to use.

You are now ready to either migrate data to the LUN or have the host start using the LUN. To migrate data to the LUN, go to [Chapter 5, “Migrating FC or iSCSI Data to the VNXe System.”](#)

CHAPTER 4

Setting Up a Unix Host to Use VNXe Fibre Channel (FC) Storage

This chapter describes how to set up an AIX, Citrix XenServer, HP-UX, Linux, or Solaris host to use EMC® VNXe® FC storage.

Topics include:

- ◆ Requirements for setting up a host to use VNXe FC storage..... 74
- ◆ Using multi-path management software on the host..... 75
- ◆ AIX host — Setting up for FC storage..... 77
- ◆ Citrix XenServer host — Setting up for FC storage..... 78
- ◆ HP-UX host — Setting up for FC storage 79
- ◆ Linux host — Setting up for FC storage..... 80
- ◆ Solaris host — Setting up for FC storage 81

Requirements for setting up a host to use VNXe FC storage

Before you set up a host to use VNXe FC storage, the SAN and VNXe requirements described in this section must be met.

SAN requirements

For a host to connect to FC storage on VNXe, the host must be in a SAN environment with the VNXe, and zoned so that the host and the VNXe are visible to each other over the SAN. For a multi-pathing environment, each VNXe FC LUN must have two paths associated with it. These two paths should be on different switches to ensure high availability.

Path management SAN requirements

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

- ◆ A VNXe storage resource is visible to both SPs.
- ◆ You can configure multiple paths for a LUN. These paths should be associated with separate physical ports on the same SP.

IMPORTANT

Directly attaching a host to a VNXe system is supported if the host connects to both SPs and has the required multipath software.

VNXe requirements

- ◆ You have installed and configured the VNXe system using the VNXe Configuration Wizard, as described in the *Installation Guide* for your storage system.
- ◆ You have used the Unisphere software or the VNXe CLI to create the VNXe FC storage for the host and have added the host to the VNXe system. For information on performing these tasks refer to the Unisphere online help.

IMPORTANT

On a HP-UX host, the iSCSI initiator will not discover the VNXe FC storage if it does not detect a LUN from the VNXe assigned to host LUN ID 0. We recommend that you create a unique target, create a LUN on this interface, and give it access to the HP-UX host. The first LUN that you assign to a host is automatically assigned host LUN ID 0.

Using multi-path management software on the host

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

- ◆ EMC PowerPath software on an HP-UX, Linux, or Solaris host
- ◆ Native multipath software on a Citrix XenServer, HP-UX 11i, Linux, or Solaris host

Note: PowerPath and AIX Native Multipath (MPIO) software are not currently supported for an AIX host connected to VNXe LUNs.

For the supported versions of the PowerPath or native multipath failover 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.

Setting up a VNXe system for multi-path management software

For a VNXe system to operate with hosts running multi-path management software, each LUN on the VNXe system should be associated with two paths.

Installing PowerPath

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

3. When the installation is complete, reboot the host or virtual machine.
4. When the host or virtual machine is back up, verify that the PowerPath service has started.

Installing native multipath software

Whether you need to install multipath software, depends on the host's operating system.

Citrix XenServer

By default XenServer uses the Linux native multipathing (DM-MP) as it multipath handler. This handler is packaged with the Citrix XenServer operating system software.

Linux

To use Linux native multipath software, you must install the Linux multipath tools package as described in [“Installing or updating the Linux multipath tools package” on page 76](#).

HP-UX 11i

Native multipath failover is packaged with the HP-UX operating system software.

Solaris

Sun's native path management software is Sun StorEdge™ Traffic Manager (STMS).

For Solaris 10 — STMS is integrated into the Solaris operating system patches you install. For information on install patches, refer to the Sun website.

Installing or updating the Linux multipath tools package

To use Linux native multipath failover software, the Linux multipath tools package must be installed on the host. This package is installed by default on SuSE SLES 10 or higher, but is not installed by default on Red Hat.

If you need to install the multipath tools package, install the package from the appropriate website below.

For SuSE:

<http://www.novell.com/linux/>

The multipath tools package is included with SuSE SLES 9 SP3 and you can install it with YaST or RPM.

For Red Hat:

<http://www.redhat.com>

The multipath tools package is included with Red Hat RHEL4 U3 or RHEL5, and you can install it with YaST or Package Manager. If an update is available, follow the instructions for installing it on the <http://www.novell.com/linux/> or <http://www.redhat.com> website.

What next?

Do one of the following:

- ◆ To set up an AIX host to use iSCSI storage, refer to “[AIX host — Setting up for FC storage](#)” on page 77.
- ◆ To set up a Citrix XenServer host to use iSCSI storage, refer to “[Citrix XenServer host — Setting up for FC storage](#)” on page 78.
- ◆ To set up an HP-UX host to use iSCSI storage, refer to “[HP-UX host — Setting up for FC storage](#)” on page 79.
- ◆ To set up a Linux host to use iSCSI storage, refer to “[Linux host — Setting up for FC storage](#)” on page 80.
- ◆ To set up a Solaris host to use iSCSI storage, refer to “[Solaris host — Setting up for FC storage](#)” on page 81.

AIX host — Setting up for FC storage

To set up an AIX host to use VNXe LUNs over Fibre Channel, perform these tasks:

- ◆ “Task 1: Install Celerra AIX software” on page 77
- ◆ “Task 2: Configure FC LUNs as AIX disk drives” on page 77
- ◆ “Task 3: Prepare the LUNs to receive data” on page 77

Task 1: Install Celerra AIX software

1. Log in to the AIX host using an account with administrator privileges.
2. Download the AIX ODM Definitions software package to the /tmp directory on the AIX host as follows:
 - a. Navigate to AIX ODM Definitions on the software downloads section on the EMC Online Support website (<http://www.emc.com/vnxesupport>).
 - b. Choose the version of the EMC ODM Definitions for the version of AIX software running on the host, and save the software to the /tmp directory on the host.
3. In the /tmp directory, uncompress and untar the EMC AIX fileset for the AIX version running on the host:


```
uncompress EMC.AIX.x.x.x.x.tar.z
tar -xvf EMC.AIX.x.x.x.x.tar
```
4. Start the System Management Interface Tool to install the software:


```
smit installp
```
5. In the Install and Update Software menu, select **Install and Update from ALL Available Software** and enter **/tmp** as the path to the software.
6. Select **SOFTWARE to install**.
7. After making any changes to the displayed values, press **Enter**.
8. Scroll to the bottom of the window to see the Installation Summary, and verify that the message “SUCCESS” appears.
9. Reboot the AIX host to have the changes take effect.

Task 2: Configure FC LUNs as AIX disk drives

On the AIX host:

1. Discover the VNXe FC LUNs as disk drives using the command: **cfgmgr**
2. To list the iSCSI LUN, enter the command: **lsdev -Cc disk**

Task 3: Prepare the LUNs to receive data

If you do not want to use a LUN as a raw disk or raw volume, then before AIX can send data to the LUN, you must either partition the LUN or create a database file systems on it. For information on how to perform these tasks, refer to the AIX operating system documentation.

Citrix XenServer host — Setting up for FC storage

To set up a Citrix XenServer host to use VNXe LUNs over Fibre Channel, perform these tasks:

- ◆ [“Task 1: Configure the FC target” on page 78](#)
- ◆ [“Task 2: Configure the FC target for multipathing” on page 78](#)

Task 1: Configure the FC target

The XenServer operating system includes FC software that you must configure for each HBA that will connect to the VNXe FC storage.

1. Open the XenCenter console.
2. Click **New Storage** at the top of the console.
3. In the **New Storage** dialog box, under **Virtual disk storage**, select **Hardware HBA**.
4. Under **Name**, enter a descriptive name for the VNXe LUN (Storage Repository).
5. Click **Next**.
6. Select a VNXe LUN, and click **Finish**.

The host scans the target to see if it has any XenServer Storage Repositories (SRs) on it already, and if any exist you are asked if you want to attach to an existing SR or create a new SR.

Task 2: Configure the FC target for multipathing

Citrix recommends either enabling multipathing in XenCenter before you connect the pool to the storage device or if you already created the storage repository, putting the host into Maintenance Mode before you enable multipathing.

If you enable multipathing while connected to a storage repository, XenServer may not configure multipathing successfully. If you already created the storage repository and want to configure multipathing, put all hosts in the pool into Maintenance Mode before configuring multipathing and then configure multipathing on all hosts in the pool. This ensures that any running virtual machines that have LUNs in the affected storage repository are migrated before the changes are made.

1. In XenCenter enable the multipath handler:
 - a. On the host's **Properties** dialog box, select the **Multipathing** tab.
 - b. On the **Multipathing** tab, select **Enable multipathing on this server**.
2. Verify that multipathing is enabled by clicking the storage resource's **Storage general properties**.

HP-UX host — Setting up for FC storage

To set up an HP-UX host to use VNXe LUNs over Fibre Channel, perform these tasks:

- ◆ “Task 1: Download and install the HP-UX FC HBA software” on page 79.
- ◆ “Task 2: Make the VNXe storage processors available to the host” on page 79.
- ◆ “Task 3: Verify that native multipath failover sees all paths the LUNs” on page 79.
- ◆ “Task 4: Prepare the LUNs to receive data” on page 79.

Task 1: Download and install the HP-UX FC HBA software

1. On the HP-UX host, open a web browser and download the initiator software from the HP-UX website.
2. Install the initiator software using the information on the site or that you downloaded from the site.

Task 2: Make the VNXe storage processors available to the host

Verify that each NIC sees only the storage processors (targets) to which it is connected:

```
ioscan -fnC disk
insf -e
ioscan -NfC disk (for HP-UX 11i v3 only)
```

Task 3: Verify that native multipath failover sees all paths the LUNs

If you are using multipath failover:

1. Rescan for the LUNs:


```
ioscan -NfC disk|
insf -e
```
2. View the LUNs available to the host:


```
ioscan -NfnC disk
```
3. Verify that all paths to the VNXe system are CLAIMED:


```
ioscan -NkfnC lunpath
```

Task 4: Prepare the LUNs to receive data

If you do not want to use a LUN as a raw disk or raw volume, then before HP-UX can send data to the LUN, perform the following tasks as described in the HP-UX operating system documentation:

1. Make the LUN visible to HP-UX.
2. Create a volume group on the LUN.

Linux host — Setting up for FC storage

To set up a Linux host to use VNXe LUNs over Fibre Channel, perform these tasks:

- ◆ [“Task 1: Set up the Linux host to use the VNXe FC LUN” on page 80](#)

Task 1: Set up the Linux host to use the VNXe FC LUN

Perform the following tasks as described in the Linux operating system documentation:

1. Find the LUN number of the LUN:
 - a. In Unisphere, select **Storage** > **LUNs**.
 - b. Select the LUN, and click **Details** > **Access Details**.
2. On the host, partition the LUN.

If the host does not see the LUN, you can have problems with the SAN connectivity between the host and SP.

3. Create a file system on the partition.
4. Create a mount directory for the file system.
5. Mount the file system.

The Linux host can now write data to and read data from the file system on the LUN.

Solaris host — Setting up for FC storage

To set up a Solaris host to use VNXe LUNs over Fibre Channel, perform these tasks:

- ◆ [“Task 1: Configure Sun StorEdge Traffic Manager \(STMS\)” on page 81.](#)
- ◆ [“Task 2: Prepare the LUN to receive data” on page 81](#)

Task 1: Configure Sun StorEdge Traffic Manager (STMS)

If you want to use STMS on the host to manage the paths to the VNXe LUNs, you must first configure it:

1. Enable STMS by editing the following configuration file:

Solaris 10 — Do one of the following:

- Edit the `/kernel/drv/fp.conf` file by changing the `mpxio-disable` option from `yes` to `no`.
- or
- Execute the following command:
`stmsboot -e`

2. We recommend that you enable the STMS auto-restore feature to restore LUNs to their default SP after a failure has been repaired. In Solaris 10, auto-restore is enabled by default.
3. If you want to install STMS offline over NFS, share the root file system of the target host in a way that allows root access over NFS to the installing host, if you want to install STMS offline over NFS. You can use a command such as the following on `target_host` to share the root file system on `target_host` so that `installer_host` has root access:

```
share -F nfs -d `root` on target_host -o ro,rw=installer  
host,root=installer_host /
```

If the base directory of the package (the default is `/opt`) is not part of the root file system, it also needs to be shared with root access.

4. For the best performance and failover protection, we recommend that you set the load balancing policy to round robin:

```
setting load-balance="round-robin"
```

Task 2: Prepare the LUN to receive data

If you do not want to use the LUN as a raw disk or raw volume, then before Solaris can send data to the LUN, you must perform the following tasks as described in the Solaris operating system documentation:

1. Partition the LUN.
2. Create and mount a file system on the partition.

What next?

You are now ready to either migrate data to the LUN or have the host start using the LUN. To migrate data to the LUN, go to [Chapter 5, “Migrating FC or iSCSI Data to the VNXe System.”](#)

CHAPTER 5

Migrating FC or iSCSI Data to the VNXe System

You can migrate FC or iSCSI disk data to the VNXe system with either a manual copy or an application-specific tool, if one is available.

This chapter contains the following topics:

- ◆ [FC or iSCSI data migration environment and limitations.....](#) 84
- ◆ [Migrating FC or iSCSI disk data.....](#) 84

FC or iSCSI data migration environment and limitations

[Table 5](#) outlines the environment for a manual copy migration and an application tool migration of FC or iSCSI data.

Table 5 Environment for iSCSI data migration

Component	Requirement
VNXe storage	LUN sized to accommodate the data in the LUN that you want to migrate and to allow for data growth
Host	Single host with access to the LUN with data to be migrated and also to the VNXe LUN for the migrated data
LUN	Single LUN on either a local or attached FC or iSCSI storage device that you migrate in its entirety to the VNXe share

The downtime for a manual copy migration is relative to the time required for copying the data from the LUN to the VNXe LUN. The downtime for an application-specific tool migration should be less than the downtime for a manual copy.

Migrating FC or iSCSI disk data

To migrate iSCSI data to a VNXe LUN, perform these tasks:

- ◆ [“Task 1: Attach the host or virtual machine to the new VNXe LUN” on page 84.](#)
- ◆ [“Task 2: Migrate the data” on page 84.](#)

Task 1: Attach the host or virtual machine to the new VNXe LUN

1. Configure each host or virtual machine initiator that needs access to the LUN to connect to the VNXe iSCSI interface (target) with the new LUN, as described in [“Windows host — Configuring to connect to a VNXe iSCSI interface” on page 20](#) for a Windows host or virtual machine or [“Linux host — Setting up for iSCSI storage” on page 49](#) for a Linux host.
2. Prepare the new LUN to receive data, as described in [“Windows host — Setting up to use VNXe iSCSI LUNs” on page 30](#) for a Windows host or [“Linux host — Setting up for iSCSI storage” on page 49](#) for a Linux host.

Task 2: Migrate the data

1. If any host or virtual machine applications are actively using the device (LUN) with the data being migrated, stop the applications gracefully.
2. Migrate the data with the method best suited for copying data from the device to the new VNXe LUN.

On a Windows host, this method can be a simple cut and paste or drag and drop operation.

3. When the copy operation is complete:

On a Windows host:

- a. Assign a temporary drive letter to the LUN.
- b. Assign the old drive letter to the LUN to which you copied the data.

On a Linux host:

- a. Unmount the original file system on the device.
 - b. Adjust the host's mount tables, which are typically in **/etc/fstab**, to reflect the new location of the data.
 - c. Mount the new LUN using the **mount -a** or a similar command.
4. Restart the applications on the host.

APPENDIX A

Setting Up MPIO for a Windows Cluster Using a VNXe System

This appendix provides an end-to-end example of a two node Windows Server 2008 R2 cluster in an MPIO multi-path configuration with a VNXe system.

This appendix contains the following topics:

- ◆ Configuration 88
- ◆ Setting up cluster nodes (hosts)..... 90

Configuration

The components in this configuration are:

- ◆ Two Server hosts -exhost1, exhost2 - running:
 - Windows Server 2008 R2
 - Microsoft iSCSI Initiator 2.08
 - Failover Clustering
 - Multipath I/O
- ◆ One VNXe system (vnxe1) configured as follows:
 - Two iSCSI interfaces (vnxeiscsia, vnxeiscsib) configured as described in [Table 6](#).

Note: The second iSCSI interface is optional.

- iSCSI storage resources:
 - cluster_disk1 (Quorum disk, which is required for Windows Server 2003 and optional, though recommended for Windows Server 2008)
 - cluster_disk2 (optional)
 - cluster_disk3 (optional)

[Figure 3 on page 89](#) shows how these components are networked together.

Table 6 VNXe iSCSI interface configuration

Name	IP addresses	Target	Storage processor	Ethernet interface
vnxeiscsia	11.222.123.156, 11.222.224.231	IQN.192-05.com.emc:fcnev1005000720000-1-vnxe	SP A	eth3, eth2
vnxeiscsib	11.222.123.157, 11.222.224.232	IQN.192-05.com.emc:fcnev1005000720000-2-vnxe	SP B	eth3, eth2

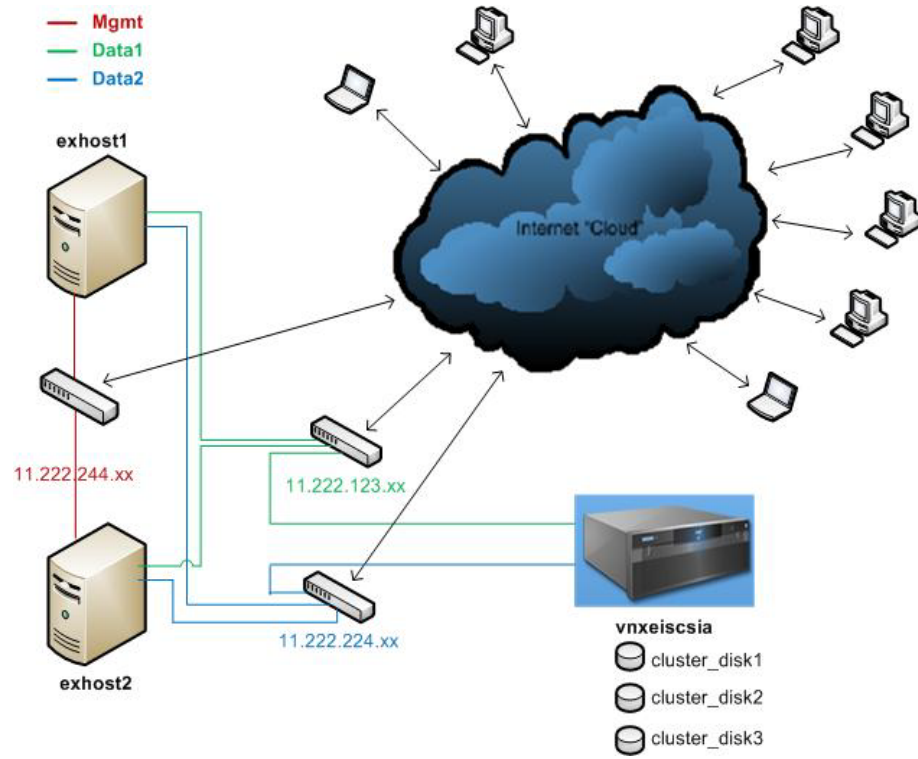


Figure 3 Network configuration

Setting up cluster nodes (hosts)

For simplicity, this section shows only the setup for the single target **vnxeiscsia**.

Task 1: Configure the iSCSI initiator with MPIO on each cluster node.

On each node in the cluster (exhost1 and exhost2):

1. In the Microsoft iSCSI Initiator, select **Discovery > Discover Portal**, add the target portal IP address or the DNS name.
2. Select **Discover Portal > Advanced** and in the **Advanced Settings** dialog box set the following for *both* the primary and secondary local adapters:
 - **Local adapter to Microsoft iSCSI Initiator.**
 - **Initiator IP** to the IP address for the local adapter interface on subnet 11.222.123.xxx for the primary local adapter, and to 11.222.224.xxx for the secondary local adapter.

The host will look for targets on the following portals:

Address	Port	Adapter	IP address
11.222.123.156,	3260	Microsoft iSCSI Initiator	11.222.123.xxx
11.222.224.231	3260	Microsoft iSCSI Initiator	11.222.224.xxx

3. Select **Targets > Log On > Connect**, select the following in the **Connect to Target** dialog box:
 - Add this connection to the list of Favorites
 - Enable multi-path (ensure the Windows MPIO feature is installed first)
4. Select **Connect To Target > Advanced** and in the **Advanced Settings** dialog box, set the following:
 - **Local adapter to Microsoft iSCSI Initiator**
 - **Initiator IP** to the IP address for the local adapter interface on subnet 11.222.123.xxx.
 - **Target portal IP to 11.222.123.156 / 3260.**
5. Add the secondary session to the existing connection for MPIO:
 - a. Select **Targets > Connect to Target > Advanced.**
 - b. In the **Advanced Settings** dialog box, set the following:
 - **Local adapter to Microsoft iSCSI Initiator**
 - **Initiator IP** to the IP address for the local adapter interface on subnet 11.222.124.xxx.
 - **Target portal IP to 11.222.224.231 / 3260.**

Task 2: Enable MPIO on each cluster node.

On each node in the cluster (exhost1 and exhost2):

1. Click **Start** and enter **MPIO** to launch the control panel applet.
2. Click the **Discover Multi-Path** tab, select **Add support for iSCSI devices**, and click **Add**.
3. Reboot the node when prompted to do so.

Task 3: Verify the MPIO settings on each cluster node.

On each node in the cluster (exhost1 and exhost2):

1. After the node finishes rebooting, go to **MPIO Properties > MPIO Devices** and verify that the MPIO hardware IDs (MSInitiator) for the VNXe devices were added.

Note: Device Hardware ID **MSFT2005iSCSIBusType_0x9** adds support for all iSCSI devices.

2. Verify the MPIO settings in the Microsoft iSCSI Initiator:
 - a. In the **Targets** tab, select the VNXe target and click **Properties**.
 - b. In the **Sessions** tab, select the identifier for the session, click **Devices**.
 - c. In the **Devices** tab, for each VNXe storage device (cluster_disk1, cluster_disk2, cluster_disk3), do the following:
 - Select the device and click **MPIO**.
 - In the **MPIO** tab, select the first connection, click **Connections**, and verify the following:

Source Portal	Target Portal
11.222.123.123/xxxx	11.222.123.156/3260

- In the **MPIO** tab, select the second connection, click **Connections**, and verify the following:

Source Portal	Target Portal
11.222.123.224/yyyy	11.222.224.231/3260

Task 4: Present the VNXe storage devices to the Primary Node in the cluster.

On the Primary Node in the cluster (exhost1), format each VNXe storage device (cluster_disk1, cluster_disk2, cluster_disk3) and assign a respective letter to each partition. In this example, E is assigned to cluster_disk1_ quorum; F is assigned to cluster_disk2; and, G is assigned to cluster_disk3.

Task 5: Configure the cluster configuration on the Primary Node.

The steps below follow Microsoft's best practices for clusters.

On the Primary Node (exhost1), in **Failover Cluster Manager**:

1. Select **Create a Cluster... > Add preferred Domain Joined computers (nodes) to the select servers list** and create an Access Point for administering the cluster and choose the static cluster IP.

For example:

Domain: app.com
Node 1: exhost1.app.com
Node 2: exhost2.app.com
Cluster Name: ex_cluster1.app.com
Network: 11.222.224.0/xx with address 11.222.224.yyy

2. Configure the network settings:
 - a. Select the cluster (ex_cluster1).
 - b. Select **Networks > Cluster Network # > Properties > Mgmt Network > 11.222.224.x** (Cluster Network 3) with the following default settings:
 - **Allow cluster network communications on this network**
 - **Allow clients to connect through this network**
 - c. Select **Networks > Cluster Network # > Properties > Data networks (iscsi) > 11.222.123.x** (Cluster Network 1) with the following default setting:
 - **Do not allow cluster network communication on this network**
 - d. Select **Networks > Cluster Network # > Properties > Data networks (iscsi) > 11.222.224.x** (Cluster Network 2) with the following default setting:
 - **Do not allow cluster network communication on this network**
3. Verify dependencies:
 - a. Select the cluster (ex_cluster1).
 - b. Click **Cluster Core Resources** and verify the following:
 - In the cluster's **Name:ex_cluster1 Properties** dialog box, verify that the dependencies are **IP address (11.22.224.x) AND cluster_disk1**.
 - In the cluster's **IP Address: 11.222.224.x Properties** dialog box, verify that the dependencies is **cluster_disk1**.

Note: The Cluster Disk Witness should always be the Quorum disk **cluster_disk1**, which is the default setting, but it can be changed.
