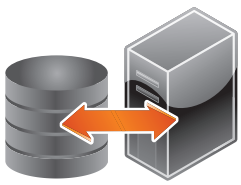
EMC® VNXe™ Series

Using a VNXe System with Microsoft Exchange 2007 or Microsoft Exchange 2010

VNXe Operating Environment Version 2.4

P/N 300-010-551
REV 04



Connect to Storage

EMC²

Published January, 2013

PREFACE

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

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

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

Purpose

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

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 Exchange storage and with the versions of the Windows operating system and Microsoft Exchange Server running on hosts that will access VNXe Microsoft Exchange storage.

Related documentation

Other VNXe documents include:

- *EMC VNXe3100 Hardware Information Guide*
- *EMC VNXe3100 System Installation Guide*
- *EMC VNXe3150 Hardware Information Guide*
- *EMC VNXe310 Installation Guide*
- *EMC VNXe3300 Hardware Information Guide*
- *EMC VNXe3300 System Installation Guide*
- *Using the VNXe System with CIFS Shared Folders*
- *Using the VNXe System with NFS Shared Folders*
- *Using the VNXe System with Generic iSCSI Storage*
- *Using the Using the VNXe System with Microsoft Windows Hyper-V*
- *Using the VNXe System with VMware NFS or VMware VMFS*
- *VNXe CLI User Guide*

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

Conventions used in this document

EMC uses the following conventions for special notices:

DANGER

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

WARNING

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

CAUTION

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

NOTICE

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

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

IMPORTANT

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

Typographical conventions

EMC uses the following type style conventions in this document:

Normal	Used in running (nonprocedural) text for: • Names of interface elements, such as names of windows, dialog boxes, buttons, fields, and menus • Names of resources, attributes, pools, Boolean expressions, buttons, DQL statements, keywords, clauses, environment variables, functions, and utilities • URLs, pathnames, filenames, directory names, computer names, links, groups, service keys, file systems, and notifications
Bold	Used in running (nonprocedural) text for names of commands, daemons, options, programs, processes, services, applications, utilities, kernels, notifications, system calls, and man pages Used in procedures for: • Names of interface elements, such as names of windows, dialog boxes, buttons, fields, and menus • What the user specifically selects, clicks, presses, or types

Italic	Used in all text (including procedures) for: • Full titles of publications referenced in text • Emphasis, for example, a new term • Variables
`Courier`	Used for: • System output, such as an error message or script • URLs, complete paths, filenames, prompts, and syntax when shown outside of running text
`Courier bold`	Used for specific user input, such as commands
`Courier italic`	Used in procedures for: • Variables on the command line • User input variables
< >	Angle brackets enclose parameter or variable values supplied by the user
[ ]	Square brackets enclose optional values
|	Vertical bar indicates alternate selections — the bar means "or"
{ }	Braces enclose content that the user must specify, such as x or y or z
...	Ellipses indicate nonessential information omitted from the example

Where to get help

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

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

`http://www.emc.com/vnxesupport`

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

Your comments

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

`techpubcomments@emc.com`

CHAPTER 1

Setting Up a Windows Exchange Server to Use VNXe Microsoft Exchange Storage

This chapter describes how to set up a Windows Exchange Server host to use EMC VNXe Microsoft Exchange storage. It also describes how to setup up a Windows Exchange Server to use VNXe Generic iSCSI storage for a quorum disk in an Exchange cluster.

Topics include:

Requirements for setting up a host to use VNXe Microsoft Exchange storage

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

VNXe system requirements

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

Host requirements

You have installed and configured Microsoft Exchange Server 2003, or Exchange Server 2007, or Exchange Server 2010 on the host.

Network requirements

For a host to connect to Microsoft Exchange and Generic iSCSI storage on a VNXe iSCSI Server, the host must be in a network environment with the VNXe iSCSI Server; to achieve best performance, the host should be on a local subnet with each VNXe iSCSI Server that provides storage for it. For a Windows multi-pathing environment, each VNXe iSCSI Server providing Microsoft Exchange and Generic 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.

To achieve maximum throughput, connect the VNXe iSCSI Server and the hosts for which it provides storage to their own private network, that is, a network just for them. When choosing the network, consider network performance. The Microsoft website (http://www.microsoft.com) has information about the requirements for Microsoft Exchange with iSCSI.

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

IMPORTANT

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

Figure 1 shows a highly-available iSCSI network configuration for hosts accessing a VNXe storage resource (Microsoft Exchange storage). 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.

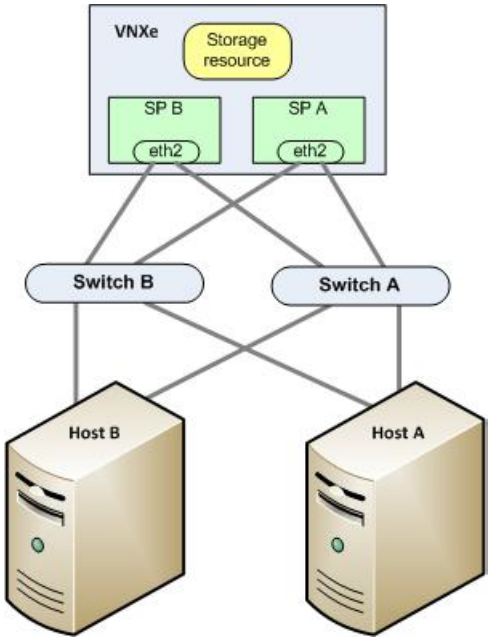


Figure 1 Sample highly-available iSCSI network

What next?

Do one of the following:

- To learn about the EMC Celerra® VSS Provider for iSCSI for Windows hosts, refer to "EMC VSS Provider overview" on page 12.
- To use EMC PowerPath® software on any Windows host or Multiple Connections per Session (MCS) on a Windows Server 2008 host, refer to "Using multi-path management software" on page 13.
- To configure the VNXe system, refer to "Configuring VNXe Microsoft Exchange storage and/or Generic iSCSI storage (quorum disk) for the host" on page 15.

EMC VSS Provider overview

The EMC VSS Provider runs as a Windows service and provides the interface between the Microsoft Volume Shadow Copy Service (VSS) and certain VNXe and other EMC storage functionality. The EMC VSS Provider enables VSS requestor applications, such as VSS-enabled backup applications, to make snapshots of VNXe iSCSI virtual disks.

Microsoft VSS

VSS provides the backup framework for Windows Server 2003 and Windows Server 2008 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 EMC VSS Provider is a hardware-based provider that works directly with iSCSI virtual disks on the VNXe iSCSI Servers and with the VSS service on Windows Server 2003 or Windows Server 2008 hosts to provide consistent shadow copy creation and addressing.

Because the EMC VSS Provider is a hardware-based provider that works on the VNXe iSCSI Servers, it reduces the load on the CPU and memory of the iSCSI host. It is also more efficient in an environment where shadow copies of multiple volumes must be taken simultaneously. This provider supports a maximum of 2000 snapshots.EMC Replication Manager has a built-in VSS hardware provider that replaces the EMC VSS Provider in configurations that use Replication Manager to create consistent shadow copies.

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

Types of shadow copies

VSS produces two 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.

The EMC VSS 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 and Windows Server 2008 and require a VSS provider (such as the EMC VSS Provider) and a backup application that supports VSS (such as EMC NetWorker 7.1 or VERITAS Backup Exec 9.1).

Shadow copy transport

Using a hardware VSS provider, such as the EMC VSS 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 and Windows Server 2008 Enterprise or Datacenter editions.

Remote VSS

The EMC VSS Provider supports remote application backup at the server, share, or single volume level.

Limitations

The EMC VSS 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 EMC VSS 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.

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 or Windows Server 2008 host connected to a VNXe system:

- EMC PowerPath software on a Windows 2003 or Windows Server 2008 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.

- Multiple Connections per Session (MCS), which is part of the Microsoft iSCSI Software Initiator on a Windows 2003 or Windows Server 2008 host.

  Note: MCS is not supported for Windows 7.

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

Setting up a VNXe system for multi-path management software

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

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

IMPORTANT

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

Installing PowerPath

IMPORTANT

You cannot configure your VNXe iSCSI connections to present the VNXe Exchange storage to both a standalone Windows host and its Windows virtual machines. If you will configure your VNXe iSCSI connections to present the VNXe Exchange storage directly to a stand-alone Windows host with network interface cards (NICs), install PowerPath software on the stand-alone host. If you will configure your VNXe iSCSI connections to present VNXe Exchange storage directly to a Windows virtual machine with NICs, install PowerPath software on the virtual machine.

VNXe link aggregation is not supported with 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.

Configuring VNXe Microsoft Exchange storage and/or Generic iSCSI storage (quorum disk) for the host

Use Unisphere or the VNXe CLI to:

- Create VNXe Microsoft Exchange storage and/or Generic iSCSI storage (quorum disk) for the host.
- Add the host to the VNXe system and specify its access to the Microsoft Exchange storage and/or Generic iSCSI storage (quorum disk). When you specify access, be sure to select only the IQNs for the host iSCSI initiators that you want to access the Microsoft Exchange storage and/or Generic iSCSI storage (quorum disk).

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

Setting up the host for Microsoft Exchange and Generic iSCSI storage

To set up a Windows host for Microsoft Exchange and Generic iSCSI storage, perform these tasks:

- "Task 1:Install the EMC VSS Provider (Windows Server 2003, Windows Server 2008)" on page 16.
- "Task 2:Install the Microsoft iSCSI Initiator and iSCSI initiator service on the Windows host (Windows Server 2003 only)" on page 16.
- "Task 3:Start the iSCSI initiator service (Windows Server 2008 only)" on page 17.
- "Task 4:For a multi-path configuration with MCS, install the MPIO feature (Windows 2003 and Windows Server 2008)" on page 17.
- "Task 5:Set registry values" on page 17.

Task 1: Install the EMC VSS Provider (Windows Server 2003, Windows Server 2008)

EMC recommends that you install the EMC VSS Provider on the host that will use the Microsoft Exchange and/or Generic iSCSI storage with backup applications other than EMC Replication Manager, such as EMC NetWorker® and VERITAS Backup Exec.

Note: "EMC VSS Provider overview" on page 12 provides information about the EMC VSS Provider.

To install the EMC VSS 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 **VSS-***windowsversionplatform***.exe** to start the installation wizard.
4. In the **Welcome to the InstallShield Wizard** dialog box, click **Next**.
5. In the **License Agreement** dialog box, if you agree to the license terms, select **I accept the terms in the license agreement**, and click **Next**.
6. In the **Customer Information** dialog box, enter your information, and to permit anyone logging in to the host to use the EMC VSS Provider, click **Next** to accept the default setting.
7. In the **Setup Type** dialog box, verify that **Complete** is selected and click **Next**.
8. In the **Ready to Install the Program** dialog box, click **Install**.
9. In the **InstallShield Wizard Completed** dialog box, click **Finish**.

Starting and stopping the EMC VSS Provider

The EMC VSS 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 only)

To connect to the VNXe iSCSI targets (iSCSI Servers), 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 2003 operating system software, so you must install it on the host if the host is running Windows Server 2003. 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.

Task 3: Start the iSCSI initiator service (Windows Server 2008 only)

To connect to the VNXe targets (iSCSI Servers), 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 with MCS, install the MPIO feature (Windows 2003 and Windows Server 2008)

If the Windows 2003 or Windows Server 2008 host will use a multi-path configuration with MCS to connect to the VNXe Exchange storage, 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 is it 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 is it 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 PortalRetryCount*DelayBetweenReconnect=600
SrbTimeoutDelta for PowerPath only	Set to 100 for PowerPath only.

5. Quit the Registry Editor.

Configuring the host to connect to a VNXe iSCSI Server

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 Servers 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 virtual disks in its Exchange and Generic iSCSI storage resources.

NOTICE

Unless you are using VNXe iSCSI targets in a clustered environment, do not give more than one initiator access to the same virtual disk. Conflicts can occur if more than one initiator tries to write to the virtual disk. If the virtual disk is formatted with the NTFS file system in Windows, simultaneous writes can corrupt the NTFS file system on the virtual disk.

As a best practice, do not give an initiator access to a virtual disk that does not exist.

For VNXe iSCSI servers configured with multiple IP addresses, you need to add target portals for each of the IPs configured for each server.

Each VNXe iSCSI Server is a target. If a VNXe system has two iSCSI Servers, it has two targets. Each target has one session. Each IP address associated with a VNXe iSCSI Server is a target portal. If a VNXe iSCSI Server has two IP addresses associated with it, it has two target portals. For multiple paths to the host, a VNXe iSCSI Server must have two IP addresses (two target portals) associated with it. You must add each target portal, which you want to connect to the host, to the Microsoft iSCSI Initiator on the host when you configure an initiator to connect to an iSCSI Server. For a single-path configuration with the host, you add one target portal. For a multi-path configuration, you add the two target portals.

For a single-path configuration, each session has one connection. For a multi-path configuration, each session has two connections — one connection for each IP address (target portal).

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:

- Single-path configuration
  "Configuring a Windows Server 2003 or Windows Server 2008 SP2 or earlier initiator to connect to a VNXe iSCSI Server — single-path configuration" on page 20
- Multipath configuration with iSCSI Multiple Connections per Session (MCS):
  "Configuring a Windows Server 2003 or Windows Server 2008 SP2 or earlier initiator to connect to a VNXe iSCSI Server — multi-path configuration with MCS" on page 22
- Multi-path configuration with PowerPath
  "Configuring a Windows Server 2003 or Windows Server 2008 SP2 or earlier initiator to connect to a VNXe iSCSI Server — multi-path configuration with PowerPath" on page 25

For Windows Server 2008 R2:

- Single-path configuration
  "Configuring a Windows Server 2008 R2 initiator to connect to a VNXe iSCSI Server — single-path configuration" on page 29
- Multi-path configuration with iSCSI Multiple Connections per Session (MCS):
  "Configuring a Windows Server 2008 R2 initiator to connect to a VNXe iSCSI Server — multi-path configuration with MCS" on page 31

- Multi-path configuration with PowerPath
  "Configuring a Windows Server 2008 R2 initiator to connect to a VNXe iSCSI Server — multi-path configuration with PowerPath" on page 35

Appendix A, "Setting Up MPIO for a Windows Exchange 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 Server" on page 38

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

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

- "Task 1:Setup optional mutual CHAP — Windows Server 2003 or Windows Server 2008 SP2 or earlier in a single-path configuration" on page 20.
- "Task 2:Discover the VNXe iSCSI Server in an environment — Windows Server 2003 or Windows Server 2008 SP2 or earlier in a single-path configuration" on page 20.

Task 1: Setup optional mutual CHAP — Windows Server 2003 or Windows Server 2008 SP2 or earlier in a single-path configuration

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

For the VNXe iSCSI Server 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 Server, 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 Server.

      If the VNXe system has multiple iSCSI Servers, this secret is the same for all. You can find this secret in the **CHAP Security** section on the iSCSI Server Settings page in Unisphere (**Settings › iSCSI Server Settings**).
   c. Click **OK**.

Task 2: Discover the VNXe iSCSI Server in an environment — Windows Server 2003 or Windows Server 2008 SP2 or earlier in a single-path configuration

If the host initiator is configured for optional initiator Challenge Handshake Authentication Protocol (CHAP) on the VNXe iSCSI Server, 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 Server interface on the subnet with the host interface.
   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 subnet with the VNXe iSCSI Server interface.
6. If the host initiator is configured for optional initiator CHAP on the VNXe iSCSI Server, in the **Advanced Settings** dialog box:
   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 Server.

      The VNXe iSCSI Servers support CHAP secrets of 12 to 16 characters only.
   d. If the VNXe iSCSI Server is configured for mutual CHAP, select **Perform Mutual Authentication**.
7. Click **OK** to close the **Advanced Settings** dialog box.
8. In the **Add Target Portal** dialog box, enter the IP address of the VNXe iSCSI interface on the subnet with the host interface.

   You can find this address with Unisphere by selecting **Settings** › **iSCSI Server Settings**.
9. Click **OK** to close the **Add Target Portal** dialog box.
10. In the **Discovery** tab, verify that the address of the VNXe iSCSI Server target appears in the **Target Portals** list.
11. Click the **Targets** tab.
12. In the **Targets** tab, select the VNXe iSCSI Server target and click **Log On**.

    The **Log On to Target** dialog box opens.
13. In the **Log On to Target** dialog box:
    a. Select **Automatically restore this connection when the system boots**.
    b. Click **Advanced**.

       The **Advanced Settings** dialog box opens.
14. 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 subnet with the VNXe iSCSI Server interface.

- **Target Portal** to the address of the VNXe iSCSI Server interface on the subnet with the host interface.

  You can find this address with Unisphere by selecting **Settings** › **iSCSI Server Settings**.

15. Click **OK** to close the **Advanced Settings** dialog box.
16. Click **OK** to close the **Log On to Target** dialog box.
17. In the **Targets** tab, select the VNXe iSCSI target and click **Details**.

    The **Target Properties** dialog box opens.
18. In the **Target Properties** dialog box, verify that one session appears on the **Sessions** tab.
19. Click **OK** to close the **Target Properties** dialog box.
20. Click **OK** to exit the Microsoft iSCSI Initiator.

What next?

Continue to "Setting up the host to use VNXe virtual disks" on page 39.

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

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

- You must have configured the VNXe iSCSI Server 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 Server interfaces, and the other interface must be on the IP subnet with the other VNXe iSCSI Server interface.

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

- “Task 1:Setup optional mutual CHAP — Windows Server 2003 or Windows Server 2008 SP2 or earlier in multi-path configuration with MCS” on page 22.
- “Task 2:Discover the VNXe iSCSI Server in an environment — Windows Server 2003 or Windows Server 2008 SP2 or earlier in a multi-path configuration with MCS” on page 23.

Task 1: Setup optional mutual CHAP — Windows Server 2003 or Windows Server 2008 SP2 or earlier in multi-path configuration with MCS

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

For the VNXe iSCSI Server 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 Server, 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 Server.

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

c. Click **OK**.

Task 2: Discover the VNXe iSCSI Server in an environment — Windows Server 2003 or Windows Server 2008 SP2 or earlier in a multi-path configuration with MCS

If the host initiator is configured for optional initiator Challenge Handshake Authentication Protocol (CHAP) on the VNXe iSCSI Server, 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 Server interface on the *first* subnet with the host interface.

      You can find this address with Unisphere by selecting **Settings › iSCSI Server 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 Server interface.
6. If the host initiator is configured for optional initiator CHAP on the VNXe iSCSI Server:

   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 Server.

      The VNXe iSCSI Servers support CHAP secrets of 12 to 16 characters only.

   d. If the VNXe iSCSI Server is configured for mutual CHAP, select **Perform Mutual Authentication**.
7. Click **OK** to close the **Advanced Settings** dialog box.
8. In the **Add Target Portal** dialog box, enter the IP address of the VNXe iSCSI Server interface on the *first* subnet with the host interface.

9. Click **OK** to close the **Add Target Portal** dialog box.
10. In the **Discovery** tab, verify that the address of the first VNXe iSCSI Server interface appears in the **Target Portals** list.
11. Under **Target Portals**, click **Add** again to add the second VNXe iSCSI Server interface.
12. In the **Add Target Portal** dialog box:
    a. Enter the IP address of the VNXe iSCSI Server interface on the *second* subnet with the host interface.

       You can find this address with Unisphere by selecting **Settings** › **iSCSI Server Settings**.

    b. Click **Advanced**.
13. 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 *second* subnet with the VNXe iSCSI Server interface.
14. If the host initiator is configured for optional initiator CHAP on the VNXe iSCSI Server:
    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 Server.

       The VNXe iSCSI Servers support CHAP secrets of 12 to 16 characters only.

    d. If the VNXe iSCSI Server is configured for mutual CHAP, select **Perform Mutual Authentication**.
15. Click **OK** to close the **Advanced Settings** dialog box.
16. In the **Add Target Portal** dialog box, enter the IP address of the VNXe iSCSI Server interface on the *second* subnet with the host interface.
17. Click **OK** to close the **Add Target Portal** dialog box.
18. In the **Discovery** tab, verify that the address of both VNXe iSCSI Server interfaces appear in the **Target Portals** list.
19. Click the **Targets** tab.
20. In the **Targets** tab, select the VNXe iSCSI Server target name and click **Log On**.

    The Log **On to Target** dialog box opens.
21. In the **Log On to Target** dialog box:
    a. Select **Automatically restore this connection when the system reboots**.
    b. Click **Advanced**.

       The **Advanced Settings** dialog box opens.
22. 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 Server interface.
- **Target Portal** to the address of the VNXe iSCSI Server interface on the *first* subnet with the host interface.

  You can find this address with Unisphere by selecting **Settings** › **iSCSI Server Settings**.

23. Click **OK** to close the **Advanced Settings** dialog box.
24. Click **OK** to close the **Log On to Target** dialog box.
25. In the **Targets** tab, select the VNXe iSCSI Server target, and click **Details**.

    The **Target Properties** dialog box opens.
26. In the **Target Properties** dialog box, click the check box next to the identifier, and click **Connections**.

    The **Session Connections** dialog box opens.
27. In the **Session Connections** dialog box, click **Add**.

    The **Add Connection** dialog box opens.
28. In the **Add Connection** dialog box, click **Advanced**.

    The **Advanced Settings** dialog box opens.
29. In the **Advanced Settings** dialog box, set the following:
    a. **Source IP** to the IP address of the host interface on the *second* subnet with the VNXe iSCSI Server interface.
    b. **Target Portal** to the IP address of the VNXe iSCSI Server interface on the *second* subnet with the host interface.
30. Click **OK** to close the **Advanced Settings** dialog box.
31. Click **OK** to close the **Add Connection** dialog box.
32. In the **Session Connections** dialog box, verify that two connections are listed.
33. Click **OK** to close the **Session Connections** dialog box.
34. Click **OK** to close the **Target Properties** dialog box.
35. Click **OK** to exit the Microsoft iSCSI Initiator.

What next?

Continue to "Setting up the host to use VNXe virtual disks" on page 39.

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

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

- You must have configured the VNXe iSCSI Server 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 Server interfaces, and the other interface must be on the IP subnet with the other VNXe iSCSI Server interface.

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

- "Task 1:Setup optional mutual CHAP — Windows Server 2003 or Windows Server 2008 SP2 or earlier in multi-path configuration with PowerPath" on page 26.
- "Task 2:Discover the VNXe iSCSI Server in an environment — Windows Server 2003 or Windows Server 2008 SP2 or earlier in a multi-path configuration with PowerPath" on page 26.

Task 1: Setup optional mutual CHAP — Windows Server 2003 or Windows Server 2008 SP2 or earlier in multi-path configuration with PowerPath

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

For the VNXe iSCSI Server 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 Server, 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 Server.

      If the VNXe system has multiple iSCSI Servers, this secret is the same for all. You can find this secret in the **CHAP Security** section on the iSCSI Server Settings page in Unisphere (**Settings › iSCSI Server Settings**).
   c. Click **OK**.

Task 2: Discover the VNXe iSCSI Server in an environment — Windows Server 2003 or Windows Server 2008 SP2 or earlier in a multi-path configuration with PowerPath

If the host initiator is configured for optional initiator Challenge Handshake Authentication Protocol (CHAP) on the VNXe iSCSI Server, 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 Server interface on the *first* subnet with the host interface.

You can find this address with Unisphere by selecting **Settings › iSCSI Server 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 Server interface.
6. If the host initiator is configured for optional initiator CHAP on the VNXe iSCSI Server:
   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 Server.

      The VNXe iSCSI Servers support CHAP secrets of 12 to 16 characters only.

   d. If the VNXe iSCSI Server is configured for mutual CHAP, select **Perform Mutual Authentication**.
7. Click **OK** to close the **Advanced Settings** dialog box.
8. In the **Add Target Portal** dialog box, enter the IP address of the VNXe iSCSI Server interface on the *first* subnet with the host interface.

   You can find this address with Unisphere by selecting **Settings › iSCSI Server Settings**.
9. Click **OK** to close the **Add Target Portal** dialog box.

   The IP address of the first VNXe iSCSI Server should appear on the **Discovery** tab under **Target Portals**.
10. In the **Discovery** tab, under **Target Portals,** click **Add** again to add the second VNXe iSCSI Server interface.
11. In the **Add Target Portal** dialog box:
    a. Enter the IP address of the VNXe iSCSI Server interface on the *second* subnet with the host interface.

       You can find this address with Unisphere by selecting **Settings › iSCSI Server Settings**.

    b. Click **Advanced**.
12. 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 *second* subnet with the VNXe iSCSI Server interface.
13. If the host initiator is configured for optional initiator CHAP on the VNXe iSCSI Server:
    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 Server.

The VNXe iSCSI Servers support CHAP secrets of 12 to 16 characters only.

d. If the VNXe iSCSI Server is configured for mutual CHAP, select **Perform Mutual Authentication**.

14. Click **OK** to close the **Advanced Settings** dialog box.
15. In the **Add Target Portal** dialog box, enter the IP address of the VNXe iSCSI Server interface on the *second* subnet with the host interface.

You can find this address with Unisphere by selecting **Settings › iSCSI Server Settings**.

16. Click **OK** to close the **Add Target Portal** dialog box.
17. In the **Discovery** tab, verify that the addresses of both VNXe iSCSI Server targets appear in the **Target Portals** list.
18. Click the **Targets** tab.
19. In the **Targets** tab, select the VNXe iSCSI Server target name and click **Log On**.

The **Log On to Targets** dialog box opens.

20. In the **Log On to Targets** dialog box, click **Advanced**.
21. 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 Server interface.
    - **Target Portal** to the address of the VNXe iSCSI Server interface on the *first* subnet with the host interface.

      You can find this address with Unisphere by selecting **Settings › iSCSI Server Settings**.
22. Click **OK** to close the **Advanced Settings** dialog box.
23. In the **Log On to Target** dialog box:

a. Select **Automatically restore this connection when the system boots**.

b. Select **Enable multi-path**.

24. Click **OK** to close the **Log On to Target** dialog box.
25. In the **Targets** tab, select the VNXe iSCSI target and click **Log On** again to log on to the second VNXe iSCSI Server interface.
26. In the **Log On to Targets** dialog box, click **Advanced**.
27. 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 *second* subnet with the VNXe iSCSI Server interface.

- **Target Portal** to the address of the VNXe iSCSI Server interface on the *second* subnet with the host interface.

  You can find this address with Unisphere by selecting **Settings** › **iSCSI Server Settings**.

28. Click **OK** to close the **Advanced Settings** dialog box.
29. In the **Log On to Target** dialog box:
    a. Select **Automatically restore this connection when the system boots**.
    b. Select **Enable multi-path**.
30. Click **OK** to close the **Log On to Target** dialog box.
31. In the **Targets** tab, select the VNXe iSCSI Server target and click **Details**.

    The **Target Properties** dialog box opens.
32. In the **Sessions** tab, verify that two sessions are listed.
33. Click **OK** to close the **Target Properties** dialog box.
34. Click **OK** to exit the Microsoft iSCSI Initiator.

What next?

Continue to "Setting up the host to use VNXe virtual disks" on page 39.

Configuring a Windows Server 2008 R2 initiator to connect to a VNXe iSCSI Server — single-path configuration

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

- "Task 1:Setup optional mutual CHAP — Windows Server 2008 R2 in single-path configuration" on page 29.
- "Task 2:Discover the VNXe iSCSI Server in an environment — Windows Server 2008 R2 in single-path configuration" on page 30.

Task 1: Setup optional mutual CHAP — Windows Server 2008 R2 in single-path configuration

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

For the VNXe iSCSI Server 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 Server, 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 Server.

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

d. Click **OK**.

Task 2: Discover the VNXe iSCSI Server in an environment — Windows Server 2008 R2 in single-path configuration

If the host initiator is configured for optional initiator Challenge Handshake Authentication Protocol (CHAP) on the VNXe iSCSI Server, 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 Server interface on the subnet with the host interface.

      You can find this address with Unisphere by selecting **Settings › iSCSI Server 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 subnet with the VNXe iSCSI Server.
6. If the host initiator is configured for optional initiator CHAP on the VNXe iSCSI Server:
   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 Server.

      The VNXe iSCSI Servers support CHAP secrets of 12 to 16 characters only.

   d. If the VNXe iSCSI Server is configured for mutual CHAP, select **Perform Mutual Authentication**.
7. Click **OK** to close the **Advanced Settings** dialog box.
8. In the **Discover Target Portal** dialog box, enter the IP address of the VNXe iSCSI Server interface on the subnet with the host interface.

   You can find this address with Unisphere by selecting **Settings › iSCSI Server Settings**.
9. Click **OK** to close the **Discover Target Portal** dialog box.
10. In the **Discovery** tab, verify that the address of the VNXe iSCSI Server target appears in the **Target Portals** list.

11. Click the **Targets** tab.
12. In the **Targets** tab, select the VNXe iSCSI Server target under **Discovered targets** and click **Connect**.

    The **Connect to Target** dialog box opens.
13. In the **Connect to Target** dialog box:
    a. Select **Add this connection to the list of Favorite Targets**.
    b. Verify that **Enable multi-path** is *not* selected.
    c. Click **Advanced**.

       The **Advanced Settings** dialog box opens.
14. 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 subnet with the VNXe iSCSI Server interface.
    - **Target Portal** to the address of the VNXe iSCSI Server interface on the subnet with the host interface.

      You can find this address with Unisphere by selecting **Settings › iSCSI Server Settings**.
15. Click **OK** to close the **Advanced Settings** dialog box.
16. Click **OK** to close the **Connect to Target** dialog box.
17. In the **Targets** tab, select the VNXe iSCSI target, and click **Properties**.

    The **Properties** dialog box opens.
18. In the **Target Properties** dialog box, verify that one session appears on the **Sessions** tab.
19. Click **OK** to close the **Properties** dialog box.
20. Click **OK** to exit the Microsoft iSCSI Initiator.

What next?

Continue to "Setting up the host to use VNXe virtual disks" on page 39.

Configuring a Windows Server 2008 R2 initiator to connect to a VNXe iSCSI Server — multi-path configuration with MCS

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

- You must have configured the VNXe iSCSI Server 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 Server interfaces, and the other interface must be on the IP subnet with the other VNXe iSCSI Server interface.

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

- "Task 1:Setup optional mutual CHAP — Windows Server 2008 R2 in multi-path configuration with MCS" on page 32.
- "Task 2:Discover the VNXe iSCSI Server in an environment — Windows Server 2008 R2 in multi-path configuration with MCS" on page 32.

Task 1: Setup optional mutual CHAP — Windows Server 2008 R2 in multi-path configuration with MCS

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

For the VNXe iSCSI Server 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 Server, 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 Server.

      If the VNXe system has multiple iSCSI Servers, this secret is the same for all. You can find this secret in the **CHAP Security** section on the iSCSI Server Settings page in Unisphere (**Settings › iSCSI Server Settings**).
   d. Click **OK**.

Task 2: Discover the VNXe iSCSI Server in an environment — Windows Server 2008 R2 in multi-path configuration with MCS

If the host initiator is configured for optional initiator Challenge Handshake Authentication Protocol (CHAP) on the VNXe iSCSI Server, 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 Server interface on the *first* subnet with the host interface.

      You can find this address with Unisphere by selecting **Settings › iSCSI Server 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 Server interface.

6. If the host initiator is configured for optional initiator CHAP on the VNXe iSCSI Server:
   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 Server.

      The VNXe iSCSI Servers support CHAP secrets of 12 to 16 characters only.
   d. If the VNXe iSCSI Server is configured for mutual CHAP, select **Perform Mutual Authentication**.
7. Click **OK** to close the **Advanced Settings** dialog box.
8. In the **Discover Target Portal** dialog box, enter the IP address of the VNXe iSCSI Server interface on the *first* subnet with the host interface.

   You can find this address with Unisphere by selecting **Settings** › **iSCSI Server Settings**.
9. Click **OK** to close the **Discover Target Portal** dialog box.
10. In the **Discovery** tab, verify the address of the first VNXe iSCSI Server interface appears in the **Target Portals** list.
11. Click **Discover Portal** again to configure the second VNXe iSCSI Server interface.
12. In the **Discover Target Portal** dialog box:
    a. Enter the IP address of the VNXe iSCSI Server interface on the *second* subnet with the host interface.

       You can find this address with Unisphere by selecting **Settings** › **iSCSI Server Settings**.
    b. Click **Advanced.**

       The **Advanced Settings** dialog box opens.
13. 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 *second* subnet with the VNXe iSCSI Server interface.
14. If the host initiator is configured for optional initiator CHAP on the VNXe iSCSI Server:
    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 Server.

       The VNXe iSCSI Servers support CHAP secrets of 12 to 16 characters only.
    d. If the VNXe iSCSI Server is configured for mutual CHAP, select **Perform Mutual Authentication**.

15. Click **OK** to close the **Advanced Settings** dialog box.
16. In the **Discover Target Portal** dialog box, enter the IP address of the VNXe iSCSI Server interface on the *second* subnet with the host interface.
17. Click **OK** to close the **Discover Target Portal** dialog box.
18. In the **Discovery** tab, verify that the addresses of both the VNXe iSCSI Server interfaces appear in the **Target Portals** list.
19. Click the **Targets** tab.
20. In the **Targets** tab under **Discovered Targets**, select the VNXe iSCSI Server and click **Connect**.

    The **Connect to Target** dialog box opens.
21. In the **Connect to Target** dialog box:
    a. Verify that **Add this connection to the list of Favorite Targets** is selected.
    b. Verify that **Enable Multi-path** is *not* selected.
    c. Click **Advanced**.

       The **Advanced Settings** dialog box opens.
22. 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 Server interface.
    - **Target Portal** to the address of the VNXe iSCSI Server interface on the *first* subnet with the host interface.

      You can find this address with Unisphere by selecting **Settings** › **iSCSI Server Settings**.
23. Click **OK** to close the **Advanced Settings** dialog box.
24. Click **OK** to close the **Connect to Target** dialog box.
25. In the **Targets** tab, select the VNXe iSCSI target, and click **Properties**.

    The **Properties** dialog box opens.
26. In the **Sessions** tab of the **Properties** dialog box, click the check box for the session identifier and click **MCS**.

    The **Multiple Connected Session (MCS)** dialog box opens.
27. In the **Multiple Connected Session (MCS)** dialog box, set the **MCS policy** to **Round Robin**, and click **Add**.

    The **Add Connection** dialog box opens.
28. In the **Add Connection** dialog box, click **Advanced**.
29. In the **Advanced Settings** dialog box, set the following:
    - **Source IP** to the address of the host interface on the *second* subnet with the VNXe iSCSI Server interface.

- **Target Portal** to the address of the VNXe iSCSI Server interface on the *second* subnet with the host interface.

30. Click **OK** to close the **Advanced Settings** dialog box.
31. Click **Connect** to close the **Add Connection** dialog box.
32. In the **Multiple Connected Session (MCS**) dialog box, verify that two connections are listed for the session.
33. Click **OK** to close **Multiple Connected Session (MCS)** dialog box.
34. In the **Properties** dialog box, verify that the **Connection count** is 2.
35. Click **OK** to close the **Properties** dialog box.
36. Click **OK** to exit the Microsoft iSCSI Initiator.

What next?

Continue to "Setting up the host to use VNXe virtual disks" on page 39.

Configuring a Windows Server 2008 R2 initiator to connect to a VNXe iSCSI Server — multi-path configuration with PowerPath

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

- You must have configured the VNXe iSCSI Server 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 Server interfaces, and the other interface must be on the IP subnet with the other VNXe iSCSI Server interface.

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

- “Task 1:Setup optional mutual CHAP — Windows Server 2008 R2 in multi-path configuration with PowerPath” on page 35.
- “Task 2:Discover the VNXe iSCSI Server in an environment — Windows Server 2008 R2 in multi-path configuration with PowerPath” on page 36.

Task 1: Setup optional mutual CHAP — Windows Server 2008 R2 in multi-path configuration with PowerPath

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

For the VNXe iSCSI Server 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 Server, 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 Server.

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

d. Click **OK**.

Task 2: Discover the VNXe iSCSI Server in an environment — Windows Server 2008 R2 in multi-path configuration with PowerPath

If the host initiator is configured for optional initiator Challenge Handshake Authentication Protocol (CHAP) on the VNXe iSCSI Server, 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 Server interface on the *first* subnet with the host interface.

      You can find this address with Unisphere by selecting **Settings › iSCSI Server 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 Server interface.
6. If the host initiator is configured for optional initiator CHAP on the VNXe iSCSI Server:
   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 Server.

      The VNXe iSCSI Servers support CHAP secrets of 12 to 16 characters only.

   d. If the VNXe iSCSI Server is configured for mutual CHAP, select **Perform Mutual Authentication**.
7. Click **OK** to close the **Advanced Settings** dialog box.
8. In the **Discover Target Portal** dialog box, enter the IP address of the VNXe iSCSI Server interface on the *first* subnet with the host interface.

   You can find this address with Unisphere by selecting **Settings › iSCSI Server Settings**.

9. Click **OK** to close the **Discover Target Portal** dialog box.
10. In the **Discovery** tab, verify that the address of the iSCSI Server interface is listed under **Target Portals**.
11. Click **Discover Portal** again to configure the second VNXe iSCSI Server interface.
12. In the **Discover Target Portal** dialog box:
    a. Enter the IP address of the VNXe iSCSI Server interface on the *second* subnet with the host interface.

       You can find this address with Unisphere by selecting **Settings** › **iSCSI Server Settings**.

    b. Click **Advanced**.
13. 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 *second* subnet with the VNXe iSCSI Server interface.
14. If the host initiator is configured for optional initiator CHAP on the VNXe iSCSI Server:
    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 Server.

       The VNXe iSCSI Servers support CHAP secrets of 12 to 16 characters only.

    d. If the VNXe iSCSI Server is configured for mutual CHAP, select **Perform Mutual Authentication**.
15. Click **OK** to close the **Advanced Settings** dialog box.
16. In the **Discover Target Portal** dialog box, enter the IP address of the VNXe iSCSI Server interface on the *second* subnet with the host interface.
17. Click **OK** to close the **Discover Target Portal** dialog box.
18. In the **Discovery** tab, verify that the addresses for both VNXe iSCSI Server interfaces appear in the **Target Portals** list.
19. Click the **Targets** tab.
20. In the **Targets** tab, select the VNXe iSCSI Server target under **Discovered targets** and click **Connect**.

    The **Connect to Target** dialog box opens.
21. In the **Connect to Target** dialog box, click **Advanced**.

    The **Advanced Settings** dialog box opens.
22. 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 Server interface.
- **Target Portal** to the address of the VNXe iSCSI Server interface on the *first* subnet with the host interface.

  You can find this address with Unisphere by selecting **Settings** › **iSCSI Server Settings**.

23. Click **OK** to close the **Advanced Settings** dialog box.
24. In the **Connect to Target** dialog box, select the following:
    - **Add this connection to the list of Favorite Targets**.
    - **Enable multi-path**.
25. Click **OK** to close the **Connect to Target** dialog box.
26. In the **Targets** tab, click **Connect** to connect to the second VNXe iSCSI Server interface.
27. In the **Connect to Target** dialog box, click **Advanced**.
28. 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 *second* subnet with the VNXe iSCSI Serve interface.
    - **Target Portal** to the address of the VNXe iSCSI Server interface on the *second* subnet with the host interface.

      You can find this address with Unisphere by selecting **Settings** › **iSCSI Server Settings**.
29. Click **OK** to close the **Advanced Settings** dialog box.
30. In the **Connect to Target** dialog box, select the following:
    - **Add this connection to the list of Favorite Targets**.
    - **Enable multi-path**.
31. Click **OK** to close the **Connect to Target** dialog box.
32. On the **Targets** tab, select the VNXe iSCSI Server interface and click **Properties**.
33. In the **Properties** dialog box, verify that two sessions are listed in the **Sessions** tab.
34. Click **OK** to close the **Properties** dialog box.
35. Click **OK** to exit the Microsoft iSCSI Initiator.

What next?

Continue to "Setting up the host to use VNXe virtual disks" on page 39.

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

If the host initiator is configured for optional initiator Challenge Handshake Authentication Protocol (CHAP) on the VNXe iSCSI Server, 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.

   On 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 Server and click **Quick Connect**.
4. In the Quick Connect window under Discovered targets, select the VNXe iSCSI Server and click **Connect**.

   The VNXe iSCSI virtual disks on the target (VNXeiSCSI Server) for the host are added to Windows 7.

5. Click **Done**.

   The connection to the VNXeiSCSI Server appears on the Targets tab as Connected.

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

   The virtual disks are connected to the host.

Setting up the host to use VNXe virtual disks

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

- "Task 1:Register the virtual disks as MPIO devices (Windows Server 2008 only)" on page 39.
- "Task 2:Set the offset for the virtual disk to 64 KB" on page 40.
- "Task 3:Configure a volume on the virtual disk" on page 40.

Task 1: Register the virtual disks as MPIO devices (Windows Server 2008 only)

If you are using Multipath I/O (MPIO) with Windows Server 2008, you must register the VNXe virtual disks 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 **mpiocpl.exe**.

2. Add the following entry to the MPIO device list:

   EMC Celerra

   IMPORTANT

   The above entry must have 5 spaces between `EMC` and `Celerra` and 9 spaces after `Celerra`.

3. Restart the host when prompted.

Task 2: Set the offset for the virtual disk to 64 KB

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

To set the offset for the virtual disk 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 virtual disk

The following configuration process initializes the virtual disk, 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 virtual disk.
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 Servers do not support dynamic disks.

   For a given virtual disk, 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 virtual disk 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 virtual disk 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. A change in disk number should not affect Microsoft Exchange because Exchange uses logical drive mappings (drive letters), not physical disk numbers. EMC recommends that you use consecutive drive letters for the virtual disks in a Exchange storage resource.
4. Assign an available drive letter to the disk.
5. Close the Disk Management tool.

Adding VNXe Mailbox Database Copies to a Mailbox server in a Data Availability Group

To use VNXe Mailbox Databases in a Data Availability Group (DAG):

1. Open the Exchange Management Console and navigate to **Organization Configuration**.

   Note: Under the Mailbox node, select the **Database Management** tab.

2. For each VNXe Mailbox Database that you want to add to a DAG:
   a. Right-click the database and select **Add Mailbox Database Copy**.
   b. In the Add Mailbox Database Copy Wizard, browse to the Mailbox server to which you want to add the database copy and click **OK.**
   c. In the Add Mailbox Database Copy Wizard, click **Add**.
3. Click **Finish** to exit.

Adding a VNXe Public Folder Database to a Mailbox server in a Data Availability Group

In Exchange 2010, you cannot use continuous replication to replicate VNXe Public Folder Databases because continuous replication is for mailbox databases only. You can host a VNXe Public Folder Database on a mailbox server in a Data Availability Group. For data redundancy, however, you must configure multiple VNXe Public Folder Databases across the DAG servers and configure public folder replication, which replicates public folder content and hierarchy across multiple servers. Each public folder database keeps a copy of the hierarchy. Content replicas, however, exist only on the public folder databases that you configure.

Note: For information on creating a VNXe Public Folder Database, refer to the VNXe Unisphere online help.

After you have set up the host to use all the virtual disks in the storage groups or databases in an Exchange storage resources, you are ready to:

- Migrate Exchange databases and logs to the storage groups, as described in Chapter 2, “Migrating Exchange Storage Groups or Databases and Quorum Disks to the VNXe System.”

  or

- Deploy the Exchange storage resource as a new Exchange Server, as described in Microsoft’s Exchange Server documentation.

iSCSI troubleshooting

This section contains information about:

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 Server Settings** in Unisphere.

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

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

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

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

   - IP address(es) or DNS name of the VNXe iSCSI Server with the host's virtual disks.

     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 Server 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** tab of the Microsoft iSCSI initiator.

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

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.

- The secret for the iSCSI Server on the VNXe iSCSI Server.

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 `auth unknown (0x6)` to the Windows Event Log.	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 Server and the iSCSI Server becomes unavailable, then the initiator logs multiple messages to the Windows Event Log. If multiple virtual disks 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.	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 "Configuring the host to connect to a VNXe iSCSI Server" on page 20.

CHAPTER 2
Migrating Exchange Storage Groups or Databases and Quorum Disks to the VNXe System

You can migrate Exchange storage groups (Exchange 2003 or 2007) or databases (Exchange 2010) to the VNXe system with the Exchange management software. You can migrate a quorum disk to the VNXe system with either a manual copy or an application-specific tool, if one is available.

This chapter contains the following topics:

Exchange migration environment and limitations

Table 3 outlines the environment for storage group migrations with Exchange management software.

Table 3 Environment for Exchange storage group migration

Component	Exchange management software migration
VNXe storage	Exchange storage resource with virtual disks sized to accommodate the disks in the storage group or database that you want to migrate and to allow for data growth.
Microsoft Exchange Server	Single server.
Software	No special software.

Using the Exchange management software for the migration disrupts access to the data. The downtime is relative to the time required for the Exchange Migration Wizard to copy the Exchange storage group to the virtual disks in the VNXe storage group or database.If the data you are migrating will occupy 25% or more of the space available in the new storage resource, an option to revert to thin provisioning is not available. When migrating a Microsoft Exchange based storage resource with large number of folders of same relative capacity, create the new storage resource with thin provisioning disabled, and leave the system with thin provisioning disabled once the migration is complete.

Migrating an Exchange storage group or database

IMPORTANT

By default, the VNXe system provisions Exchange storage according to Microsoft best practices for mailbox count and average mailbox size. If the Exchange storage that you are migrating does not meet these best practices, you may have to provision additional mailboxes or additional storage groups to the standard VNXe Exchange storage resource that you created. To determine the number of storage groups in an Exchange storage resource, use Unisphere.

To migrate an Exchange storage group or database to a VNXe Exchange storage resource, perform these tasks:

- "Task 1: Set up the Exchange Server host to use the virtual disks in the new VNXe Exchange storage group or database" on page 46.
- "Task 2: Migrate the storage group or database with the Exchange System Manager or Exchange Management Console" on page 47.

Task 1: Set up the Exchange Server host to use the virtual disks in the new VNXe Exchange storage group or database

If the Exchange Server host is not already set up to use the virtual disks in the new VNXe Exchange storage group or database, connect them as described in Chapter 1, "Setting Up a Windows Exchange Server to Use VNXe Microsoft Exchange Storage."

Task 2: Migrate the storage group or database with the Exchange System Manager or Exchange Management Console

To migrate Exchange 2003 storage group, use the Exchange System Manager and to migrate Exchange 2007 storage groups or Exchange 2010 databases, use the Exchange Management Console.

Migration using the Exchange System Manager (Exchange 2003)

To minimize downtime, EMC recommends that you move the database and transaction logs in the storage group when their usage is low and right after you have backed them up, so that the number of transaction logs is low.

To migrate a storage group with the Exchange System Manager:

1. On the Exchange Server, open the Exchange System Manager.
2. Locate the Administrative Group with the Exchange Server, and browse to the storage group that you want to migrate.
3. Right-click the storage group and click **Properties**.
4. On the **General** tab change both the transaction log location and the system path location to the path for the virtual disk in the VNXe system that you want to use for the storage group's logs, and click **OK**.

   A warning appears saying that if you choose to continue, all databases the storage group will be dismounted and any users of the databases will be disconnected. Depending on the number of logs being moved, this dismounting can take a long time.
5. Under the storage group that you want to migrate, right-click the mailbox of public folder that you want to migrate, and click **Properties.**
6. In the **Properties** dialog box, click the **Database** tab and browse to the new locations for the native content database (edb file) and the streaming database (stm file) on the virtual disk in the VNXe system that you want to use for the storage group's databases.

   The content database is *virtual_disk_path*.edb and the streaming database is *virtual_visk_path*.stm.

   A warning appears saying that if you choose to continue, the storage will be temporarily dismounted, making it inaccessible to any user.
7. In the warning message box, click **Yes** to continue.

   Depending on the number and size of the databases being moved, this dismounting can take a long time.
8. Use Outlook web access to verify that the migrated mailboxes are available on the migrated Exchange storage group.

Migration using the Exchange Management Console (Exchange 2007)

To minimize downtime, EMC recommends that you move the database and transaction logs in the storage group when their usage is low and right after you have backed them up, so the number of transaction logs is low.

If you are using local continuous replication, suspend it before migrating Exchange databases or transaction logs.

To migrate an Exchange 2007 storage group with the Exchange Management Console:

1. On the Exchange Server, open the Exchange Management Console.
2. Expand the Server Configuration, and click **Mailbox**.
3. Click the Exchange Server, and right-click the storage group that you want to migrate and click **Move Storage Group Path**.
4. In the Storage Group Path Wizard, for both the log files path and the system files path, browse to the path to the virtual disk in the VNXe system that you want to use for the storage group's logs, and click **Move**.
5. Locate and select the database that you want to move, and select **Move Database Path** from the Action pane.
6. In the Move Database Path Wizard, for the database file path, browse to the path for the virtual disk in the VNXe system that you want to use for the storage group's database, and click **Move**.

   Any users connected to the database are disconnected. Depending on the number and size of the databases being moved, this dismounting can take a long time.
7. When the migration is complete, use Outlook web access to verify that the migrated mailboxes are available on the migrated Exchange storage group.

Migration using the Exchange Management Console (Exchange 2010)

To minimize downtime, EMC recommends that you move the mailbox databases or public folder databases when their usage is low and right after you have backed them up, so the number of transaction logs is low.

Before you begin - Dismount the database that you want to migrate. If you are using local continuous replication, suspend it before migrating Exchange databases.

To migrate an Exchange 2010 storage group with the Exchange Management Console:

1. On the Exchange Server, open the Exchange Management Console.
2. Expand the Organization Configuration, and click **Mailbox**.
3. Click the **Database Management** tab, and select the database that you want to migrate.
4. In the work pane, click **Move Database Path**.
5. In the Move Database Path Wizard:
   a. For the **Database file path**, browse to the path for the virtual disk in the VNXe system that you want to use for the mailbox database in the database that you are migrating.
   b. For the **Log folder path**, browse to the path for the virtual disk in the VNXe system that you want to use for the log folder for the database that you are migrating.
   c. Click **Move**.
6. View the status of the move operation.

7. On the **Completion** page, confirm that the move operation completed successfully, and click **Finish**.
8. When the migration is complete, remount the migrated database.
9. Use Outlook web access to verify that the migrated mailboxes are available on the migrated Exchange database.

Quorum disk data migration environment and limitations

Table 4 outlines the environment for a manual copy migration and an application tool migration of Generic iSCSI data.

Table 4 Environment for quorum disk data migration

Component	Requirement
VNXe storage	Generic iSCSI storage resource for quorum disk 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 Generic iSCSI storage resource for the migrated data
LUN	Single LUN on either a local or attached 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 Generic iSCSI storage resource. The downtime for an application-specific tool migration should be less than the downtime for a manual copy.If the data you are migrating will occupy 25% or more of the space available in the new storage resource, an option to revert to thin provisioning is not available. When migrating a Microsoft Exchange based storage resource with large number of folders of same relative capacity, create the new storage resource with thin provisioning disabled, and leave the system with thin provisioning disabled once the migration is complete.

Migrating quorum disk data

To migrate quorum disk data to a VNXe Generic iSCSI storage resource, perform these tasks:

- "Task 1: Attach the host or virtual machine to the new VNXe Generic iSCSI storage resource for the quorum disk" on page 49.
- "Task 2: Migrate the quorum disk data" on page 50.

Task 1: Attach the host or virtual machine to the new VNXe Generic iSCSI storage resource for the quorum disk

1. Configure each host or virtual machine initiator that needs access to the iSCSI data to connect to the VNXe iSCSI Server (target) with the new Generic iSCSI storage resource, as described in "Configuring the host to connect to a VNXe iSCSI Server" on page 18.
2. Prepare the new Generic iSCSI storage resource to receive data, as described in "Setting up the host to use VNXe virtual disks" on page 39.

Task 2: Migrate the quorum disk data

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

   This method can be a simple cut and paste or drag and drop operation.
3. When the copy operation is complete:
   a. Assign a temporary drive letter to the Generic iSCSI storage resource.
   b. Assign the old drive letter to the Generic iSCSI storage resource to which you copied the data.
4. Restart the applications on the host.

APPENDIX A

Setting Up MPIO for a Windows Exchange Cluster Using a VNXe System

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

This appendix contains the following topics:

Configuration

The components in this configuration are:

- Two Exchange 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 Servers (vnxeiscsia, vnxeiscsib) configured as described in Table 5.

    Note: The second iSCSI server is optional.

  - Exchange 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 2 on page 53 shows how these components are networked together.

Table 5 VNXe iSCSI Server 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

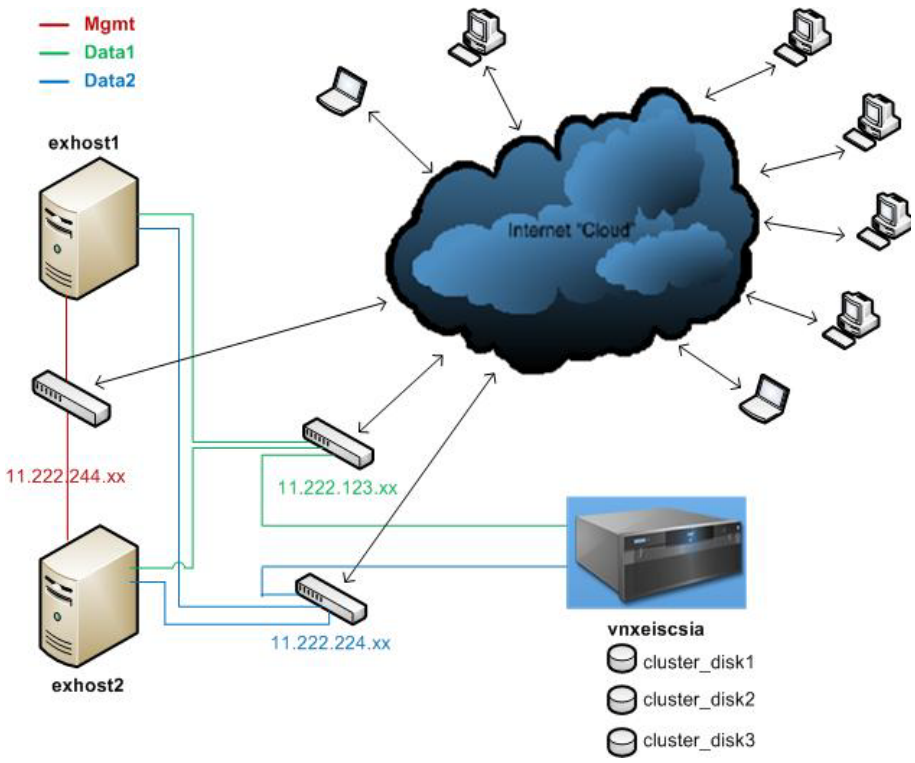


Figure 2 Network configuration

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, 11.222.224.231	3260 3260	Microsoft iSCSI Initiator Microsoft iSCSI Initiator	11.222.123.xxx 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
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 Exchange 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 Exchange storage devices to the Primary Node in the cluster.

On the Primary Node in the cluster (exhost1), format each VNXe Exchange 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.
