Dell™ PowerVault™ NX1950 Systems

End-to-End Deployment Guide for iSCSI

Model EMU01

Notes, Notices, and Cautions

NOTE: A NOTE indicates important information that helps you make better use of your computer.

NOTICE: A NOTICE indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

CAUTION: A CAUTION indicates a potential for property damage, personal injury, or death.

Model EMU01

February 2008 Rev. A02

Contents

1

Introduction

This document provides information about configuring the Internet Small Computer System Interface (iSCSI) Software Target on the Dell™ PowerVault™ NX1950 storage system as a block storage device.

iSCSI is a useful and relatively inexpensive way to provide storage for new applications or to provide a network pool of storage for existing applications. Dell and its storage partners provide a variety of storage solutions that can be implemented easily. This document allows administrators and IT managers to explore iSCSI technology and see actual deployment examples.

iSCSI storage solutions and technology have a place in many IT environments. The performance of iSCSI storage solutions is adequate for many applications and iSCSI technology provides the benefits of storage area network technology for a lower cost than Fibre Channel storage solutions.

The following topics are discussed in the document:

- Quick install steps—Provides instructions about creating an iSCSI Target and establishing connection with a Microsoft® iSCSI Initiator
- End-to-End iSCSI configuration:
  - Detailed instructions on installing and configuring the Microsoft iSCSI Initiator Software and the Microsoft iSCSI software Target
  - Configuring the Initiator-Target connections
- Setting up secure iSCSI connections
- Microsoft iSNS Server and other advanced configuration details

NOTE: In this document the iSCSI Initiator is referred to as the *Initiator* and the iSCSI Software Target is referred to as the *Target*.

Terms and Definitions

The following sections describe the terms used in this document.

PowerVault NX1950 Storage Solution Vs. PowerVault NX1950 Cluster Solution

Throughout this document, the term *PowerVault NX1950 storage system* refers to the individual storage unit. The term *PowerVault NX1950 storage solution* refers to the configuration of the storage unit along with the storage arrays. The term *PowerVault NX1950 cluster solution* refers to the configuration of more than one storage units and the storage arrays.

iSCSI

iSCSI is a standard that carries SCSI commands through Transfer Control Protocol/Internet Protocol (TCP/IP)—a protocol that enables transport of block data over IP networks, without the need for a specialized network infrastructure, such as Fibre Channel.

In the context of system storage, iSCSI enables any client/machine (Initiator) on an IP network to contact a remote dedicated server (Target) and perform block I/O on it just as it would perform on a local hard disk.

iSNS

Microsoft iSCSI Internet Storage Name Service (iSNS) is a service that processes iSNS registrations, deregistrations, and queries through TCP/IP from iSNS clients and also maintains a database of these registrations (similar to a DNS server). A common use for Microsoft iSNS Server is to allow iSNS clients (Initiators and Targets) to register themselves and to query for other registered iSNS clients. Registrations and queries are transacted remotely over TCP/IP.

You can download and install the iSNS server from the Microsoft Support website at **support.microsoft.com** on a separate server that does not have Microsoft iSCSI Initiator or Target installed.

NOTE: For details about installing and configuring the iSNS server, see "Appendix" on page 55.

Active/Passive Vs. Active/Active iSCSI

In a PowerVault NX1950 cluster solution that is configured with a 3.0 iSCSI Target, only one node that owns the Cluster Resources can create and own the iSCSI Targets. The iSCSI Target service is operative in only one node at a time (Active/Passive configuration).

In a PowerVault NX1950 cluster solution that is configured with 3.1 iSCSI Target, you can create iSCSI highly-available (HA) instances on all nodes of a cluster and thereby facilitate Active/Active iSCSI Target access. Al nodes of the cluster can use the iSCSI Target service at the same time.

NOTE: The 3.0 iSCSI Target software enables you to configure an Active/Passive cluster solution. The 3.1 iSCSI *Target* software enables you to configure an Active/Active cluster configuration. You can download the 3.1 iSCSI Target software from the Dell Support website at **support.dell.com**.

Before Setting Up the PowerVault NX1950 Storage Solution as an iSCSI Software Target

Before you set up your PowerVault NX1950 storage solution as an iSCSI Target, read this section completely. You must consider features like Ethernet settings, security settings for iSCSI Targets, and specific settings for iSCSI Targets in a PowerVault NX1950 cluster solution.

Best Practices for Setting Up the iSCSI Storage Area Network

Table 1-1 and Table 1-2 provide information about configuring NICs (on Target) in different models of iSCSI networks.

- You can configure redundant paths on Initiator (hosts). Microsoft Multipath I/O (MPIO) is supported with Initiator version of 2.06 or later.
- You require two dedicated iSCSI NICs on the target and initiator for efficient MPIO connection in the PowerVault NX1950 storage solution or PowerVault NX1950 cluster solution.
- It is good practice to have at least four NICs in a cluster configuration and at least three NICs in a stand-alone configuration (two NICs dedicated for iSCSI in different subnets).
- iSCSI NIC teaming is not supported.

- You can configure Initiators with one or two dedicated NICs for iSCSI, based on your requirement.

  NOTE: Table 1-1 and Table 1-2 provide information about the iSCSI Target NIC configuration. The optimal connection information is also provided as options. You can configure the iSCSI NICs according to your network requirements.

Table 1-1. Using a Single PowerVault NX1950 Storage Solution as a Target

Number of NICs	Details	Refer to Figure
4	NIC-1 and NIC-2 - Teamed NICs for public network NIC-3 - iSCSI dedicated traffic (subnet A) NIC-4 - iSCSI dedicated traffic (subnet B)	Figure 1-1
3- Option 1 **NOTE:** Use this configuration if iSCSI traffic has more priority than NFS traffic.	NIC-1 - NIC for public Network NIC-2 - iSCSI dedicated traffic (subnet A) NIC-3 - iSCSI dedicated traffic (subnet B)	Figure 1-2
3- Option 2 **NOTE:** Use this configuration if NFS has more priority than iSCSI traffic.	NIC-1 and NIC-2 - Teamed NICs for public network NIC-3 - iSCSI dedicated traffic	Figure 1-3

Table 1-2. Using a PowerVault NX1950 Cluster Solution as a Target

Number of NICs	Initiator	Refer to Figure
4 (Option 1)	NIC-1 - NIC for public network	Figure 1-4
	NIC-2 - Private network for cluster heartbeat	
	NIC-3 - iSCSI dedicated traffic (subnet A)	
	NIC-4 - iSCSI dedicated traffic (subnet B)	
4 (Option 2)	NIC-1 and NIC-2 - Teamed NICs for public network	Figure 1-5
	NIC-3 - Private network for cluster heartbeat	
	NIC-4 - iSCSI dedicated traffic	

- It is a good practice to have two dual-port Network Interface Cards (NICs), with two ports dedicated for iSCSI. Configure each NIC on a separate subnet. If you have three or less NICs, it is recommended that you do not use the corporate/public network (LAN) link for iSCSI traffic. This helps avoid traffic congestion and to have better performance. Figure 1-1 and Figure 1-2 illustrate redundant NIC configuration for iSCSI path and best practices.
- Secured iSCSI is possible with Challenge-Handshake Authentication Protocol (CHAP). For more information about CHAP settings, see "Configuring Secured iSCSI Connections Using Challenge-Handshake Authentication Protocol" on page 51.

  NOTE: You must configure CHAP only if the iSCSI traffic is configured on the public network.
- You can configure Active/Active iSCSI Target in both nodes of a cluster solution to provide high availability for iSCSI storage.

Figure 1-1. Redundant iSCSI Paths and NIC Teaming for Data Sharing With Four NICs

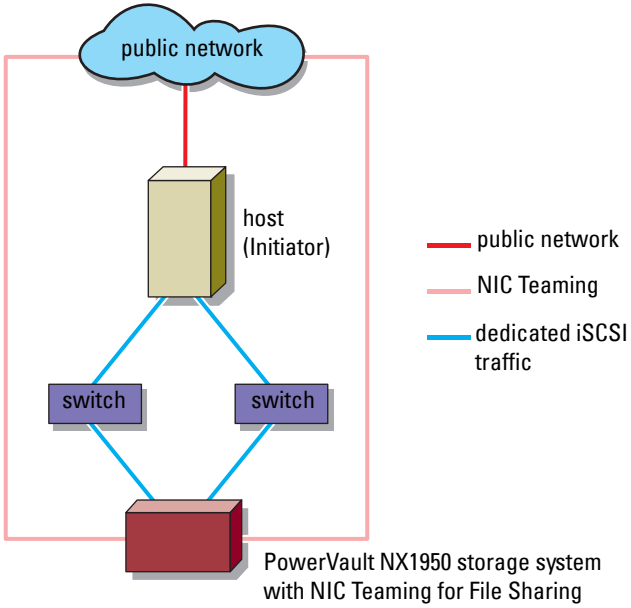


Figure 1-2. Redundant iSCSI Paths With Three NICs

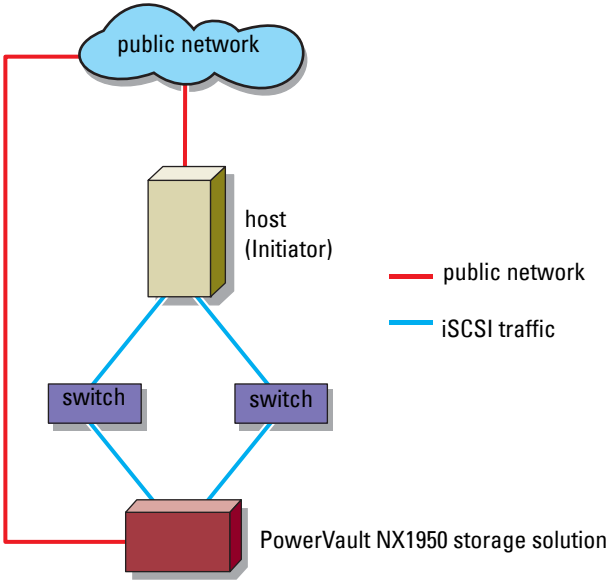
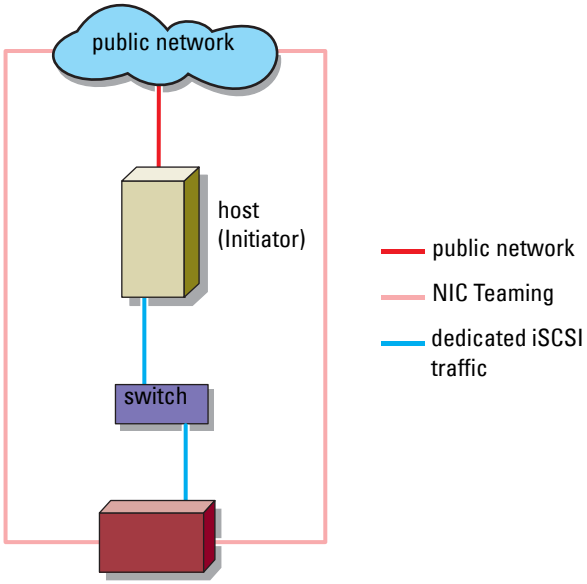


Figure 1-3. Non-Redundant iSCSI Path With Three NICs



PowerVault NX1950 storage solution
with NIC teaming for Data Sharing

NOTE: For 3.0 iSCSI Target—In Figure 1-4 and Figure 1-5, both Initiators can communicate to the Active PowerVault NX1950 storage node through the dedicated iSCSI link (indicated by blue links from Initiators to switch and Active PowerVault NX1950 storage node). The active node owns the cluster group. The passive node and link are active only when the active link from the switch to the active node is lost or the active node dies.

NOTE: For 3.1 iSCSI target—In Figure 1-4 and Figure 1-5 with Active/Active target, both Initiators can communicate to both PowerVault NX1950 storage nodes through the dedicated iSCSI link (indicated by blue links from Initiators to switch and PowerVault NX1950 storage nodes). If one node fails, the surviving node takes ownership of all iSCSI Targets of the failed node and continues the I/O operations.

Figure 1-4. Redundant iSCSI Paths Using Four NICs

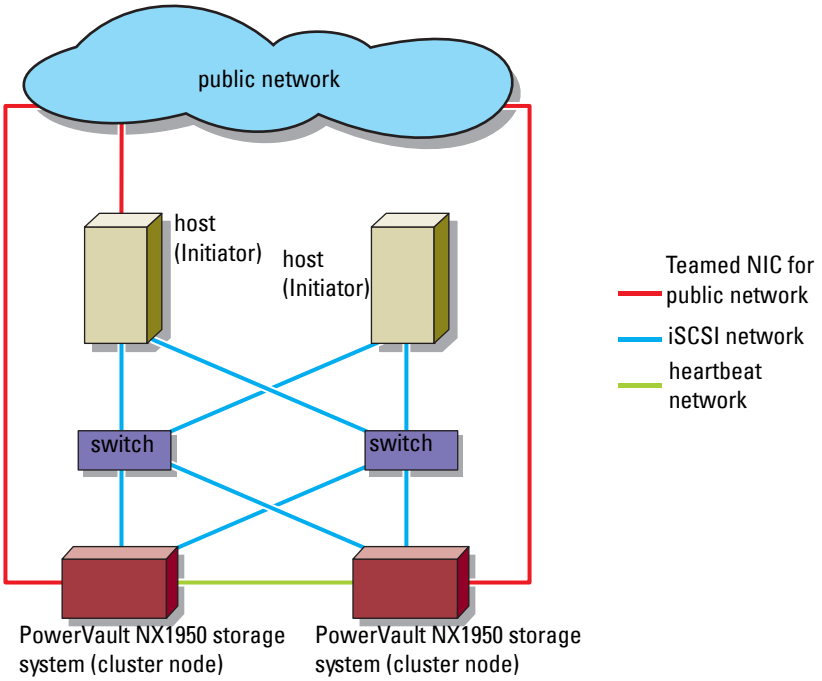
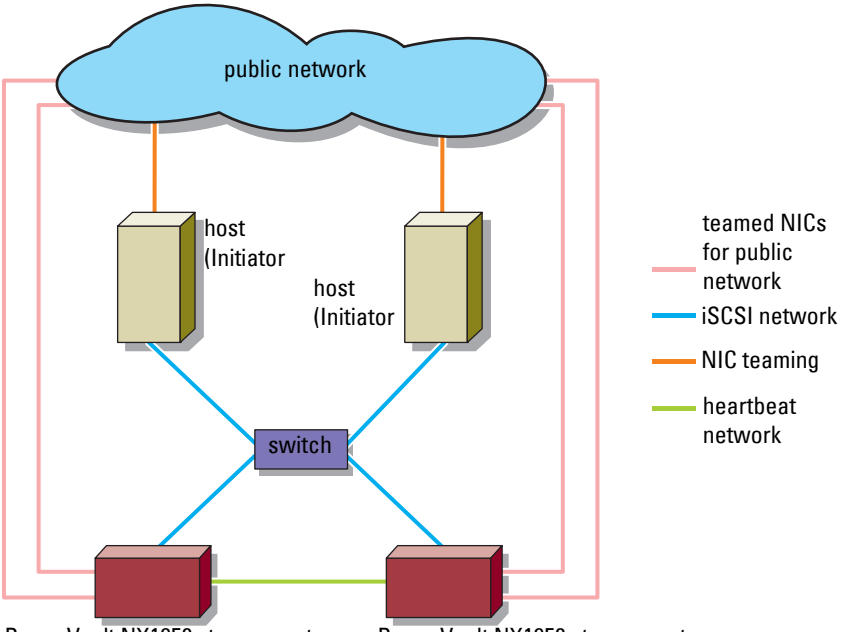


Figure 1-5. Non-Redundant iSCSI Paths Using Four NICs



- For more information about the pre-requisites to configure the PowerVault NX1950 cluster solution as an iSCSI Target, see the section **Creating a Highly Available iSCSI Target** in *Dell PowerVault NX1950 Cluster Systems Installation and Troubleshooting Guide* on the Dell Support website at **support.dell.com**.

  NOTE: Before you configure the PowerVault NX1950 cluster solution as an iSCSI Target, turn off the firewall in all cluster nodes to ensure proper iSCSI Target configuration.

  For more information about PowerVault NX1950 storage solutions, see the *Dell PowerVault NX1950 Systems Support Matrix* located at the Dell Support website at **support.dell.com**.

2

Quick Install Steps for Initiator-Target Connection

This section is targeted towards advanced users that are familiar with the following concepts:

- Operations of iSCSI protocol
- iSCSI Initiator - Target connection information
- Install and setup of Microsoft® iSCSI Initiator and Microsoft iSNS server
- Basic RAID operations of Dell™ PowerVault™ NX1950 storage system

The following sections provide quick step-by-step instructions to set up an iSCSI Target and to establish connection from an Initiator.

Method 1 (Discovery Using Target Portals)

This section describes the procedure for iSCSI Target discovery in Initiator using direct Target portals. To perform the Target discovery, enter the IP address of one of the NICs of PowerVault NX1950 storage solution that is configured for iSCSI traffic in the Initiator and thereby enabling the Initiator to discover all Targets of this Target server.

Pre-Requisites

Before you set up the iSCSI Target, ensure that you perform the following steps:

1. Download the Microsoft iSCSI Initiator software from Microsoft Support website at **support.microsoft.com** and install the Initiator (Host).
2. Install and set up the PowerVault NX1950 storage system and the storage array. Complete the initial setup for storage allocated to the PowerVault NX1950 storage system. Configure and assign the IP addresses for iSCSI traffic.

3 If you are using the PowerVault NX1950 cluster solution with a storage array, perform the following tasks:

   a Turn on all nodes of the cluster.

   b Create one or more volumes on the storage array and assign them to the Cluster Group.

   c Use the volumes that you created to create Virtual Disks for iSCSI Targets.

   d Pre-requisites to configure the PowerVault NX1950 cluster solution as an iSCSI Target can be seen in the section "Creating a Highly Available iSCSI Target" in *Dell PowerVault NX1950 Cluster Systems Installation and Troubleshooting Guide* on the Dell Support website at **support.dell.com**.

NOTE: Before you configure the PowerVault NX1950 cluster solution as an iSCSI Target, turn off the firewall in all cluster nodes to ensure proper iSCSI Target configuration.

Configuring the Initiator (Host)

Configure the Microsoft iSCSI Initiator with the IP address of the Target server's information. Perform the following steps to configure the Initiator:

1 Go to the server that has Microsoft iSCSI Initiator installed. Select **Start**→ **Programs**→**Microsoft iSCSI Initiator**→**iSCSI Initiator Properties**→ **Discovery** tab→Select **Add**.

2 Add the IP address of one of the NICs on the PowerVault NX1950 storage system that is configured for iSCSI traffic.

3 Click **OK**.

NOTE: If you are using the 3.0 iSCSI Target software to configure the PowerVault NX1950 cluster solution as the Target, you must use the IP address configured in the cluster for iSCSI traffic and not the IP address of a specific node or cluster IP address (in public/corporate network). This ensures proper connection between the Initiator and Targets during cluster node failover or Cluster Group move among different nodes of cluster.

NOTE: If you are using the 3.1 iSCSI Target software to configure the PowerVault NX1950 cluster solution as the Target, you must create at least one iSCSI HA instance on each node and use the IP address for iSCSI traffic. This ensures Active/Active Target-Initiator connection (connection with targets created on all nodes of cluster) and high-availability in the event of node failure.

Configuring iSCSI Connection With the PowerVault NX1950 Storage Solution

Creating the Target

1. From the PowerVault NX1950 storage solution, select **Start→Programs→ Administrative Tools→Windows Unified Data Storage Server**. The **PowerVault NX1950 Management Console** appears.
2. Select **Microsoft iSCSI Software Target** option. The options **iSCSI Targets**, **Devices**, and **Snapshots** are displayed.
3. Select **iSCSI Targets** and either right-click or select the **More Actions** option in the **Actions** tab.
4. Select the **Create iSCSI Target** option.
5. The **Welcome to the Create iSCSI Target** wizard screen is displayed. Select **Next**.

   The wizard guides you through the process of Target creation.
6. The **Create iSCSI Target** wizard displays the **iSCSI Target Identification** option. Enter a **Name** and **Description** (optional) for the iSCSI Target. Click **Next**.
7. The **iSCSI Initiators Identifiers** screen appears. Click **Browse** and select the IQN for the host that connects to the Target. The host is listed only if step 1 in "Configuring the Initiator (Host)" on page 18 was completed successfully.

   NOTE: You must fill the IQN identifier field. You can type the Initiator IQN identifier or use the **Browse** and **Advanced** options in the screen to add the IQN identifier. For more information about the **Browse** option, see step 8. For more information about the **Advanced** option, see step 9.
8. If you choose the **Browse** option, you can select the **IQN identifier** by performing the following steps:
   a. Select **Browse** and the **Add iSCSI Initiator** screen appears.
   b. The details for iSCSI Initiator list is displayed. You can type or select iSCSI Initiator from the list, enter the iSCSI Initiator Name, and select **OK**. The **IQN identifier** field in the **iSCSI Initiators Identifiers** screen is populated with the value entered or selected. Select **Next**. Go to step 10.

9 If you choose the **Advanced** option, you can select the **IQN identifier** by performing the following steps:

   a When you choose the **Advanced..** option, the **Advanced Identifiers** screen appears and displays the **Add** option. Select **Add**.

   b The **Add/Edit Identifier** appears and provides four options namely—**IQN**, **DNS Domain Name**, **IP address**, and **MAC Address** to add the **IQN identifier**. Choose any one of the four options.

   c Type in the value or choose the value through the **Browse** option, and then select **OK**.

   The IQN identifier is displayed in the **Advanced Identifiers** screen and the fields **IQN**, **DNS Domain Name**, **IP address**, and **MAC Address** are populated.

   d Select the populated value and select **OK**.

   e In the **iSCSI Initiator Identifiers** screen, the **IQN identifier** field is populated with appropriate information. Click **Advanced** to view alternate identifiers.

   f Select **Next**.

10 The **Completing the Create iSCSI Target** wizard appears. Click **Finish**.

Creating a Virtual Disk

1 Right-click the newly created Target and click **Create Virtual Disk for iSCSI Target**. The **Create Virtual Disk** wizard appears. Select **Next**.

2 To create a file, choose the **Browse** option, select a volume on the storage array and type a file name with an extension **.vhd**.

   For example, create **Z:\vol1.vhd**, where Z is the mounted volume from storage array and *vol1.vhd* is the filename. Select **Next**.

3 In the **Size** screen, choose the appropriate size from **Currently available free space** and click **Next**.

4 The **Description** screen may appear. Enter the Virtual disk description, if required and click **Next**.

5 The **Access** screen appears. In the **Add** option, specify the iSCSI Targets that access the Virtual Disk that you have created. The Target that you chose in step 1 is listed in the **Access** list.

NOTE: Go to **Access→Add→Add Target** to add additional iSCSI Targets. To configure the Targets to access the Virtual disk that you created, select the **iSCSI Targets** available in the list and click **OK**. You are redirected to the **Access** screen and the list of chosen Targets is displayed.

6 In the **Add** screen, select the Target name, and then click **Next**.

7 The **Completing the Create Virtual Disk** wizard appears. Click **Finish**.

NOTICE: If multiple hosts access the same target, data corruption may occur. For more information, see "Enabling Multi-Path on the Initiator" on page 61.

NOTE: You can create multiple VHDs on the same volume.

Configuring iSCSI Connection With the PowerVault NX1950 Cluster Solution

To configure the PowerVault NX1950 cluster solution as an iSCSI Target, perform the actions in "Pre-Requisites" on page 17 and then perform the following steps:

Configuring 3.0 iSCSI Target (Active/Passive)

1 Add the Virtual iSCSI IP address to the **Cluster resources** list. The Virtual IP address is similar to the cluster IP and must be part of the subnet in which the iSCSI NICs of cluster nodes are configured. You must also add the same Virtual iSCSI IP address in the Initiator as **Target portals IP address** for discovery.

NOTE: When you are establishing a connection/session, choose the specific host (source) IP address and exclusive iSCSI virtual IP address of the cluster as Target portal from Initiator. This ensures proper connection during cluster node failover.

2 Configure the Target on the active node of PowerVault NX1950 cluster solution.

3 To create a target, follow the instructions in "Creating the Target" on page 19 and to create a virtual disk, follow the instructions in "Creating a Virtual Disk" on page 20.

The active node is the node on which the cluster resources are running. From any cluster node, click **Start→Administrator Tools→Cluster Administrator→Groups→Cluster Group**. The active node is listed in the middle pane in the **Owner** section.

NOTE: Redundant iSCSI NICs (MPIO) are not supported with PowerVault NX1950 cluster solution configured with 3.0 iSCSI Target.

Configuring 3.1 iSCSI Target (Active/Active)

Create iSCSI highly-available instance on all nodes of PowerVault NX1950 cluster solution. To create a highly-available instance, go to the **PowerVault NX1950 Management Console** of a cluster node and perform the following steps:

1 Right-click the **Microsoft iSCSI Software Target** option and select **Create HA Instance for iSCSI**. If an highly-available instance already exists in the cluster, the following message appears:

```
A highly available instance already exists. Would
you like to configure a new instance?
```

2 Click **Yes**. The **Create Highly Available Instance for iSCSI Storage** screen appears.

3 Click **Add**. The **Add IP Address Resource** screen appears.

4 Enter the resource name, IP address, subnet mask, and choose the network interface according to your iSCSI configuration setup. Configure the iSCSI HA instance IP address on the NIC that is dedicated for iSCSI traffic.

NOTE: If the Resource name exceeds the maximum allowable size of 15 characters, it is truncated to 15 characters.

5 Click **OK**. The highly-available iSCSI instance is created successfully.

6 Repeat the procedure for all nodes of the PowerVault NX1950 cluster solution.

Verify the iSCSI HA Instance Creation (Optional)

1. In any PowerVault NX1950 cluster node, go to **Start→Programs→ Administrative Tools→Cluster Administrator** and verify the newly created iSCSI highly-available instance under **Groups** section. Verify the name, IP address, and other properties of the resource.
2. Create one or more volumes on the storage array and assign them to iSCSI highly-available instances or use the **Cluster Administrator** to move the existing volumes to iSCSI highly-available instances.
3. To create a target, follow the instructions in "Creating the Target" on page 19 and to create a virtual disk, follow the instructions in "Creating a Virtual Disk" on page 20.

   NOTE: Perform step 1 to step 9 of "Creating the Target" on page 19. After you enter the IQN identifier as mentioned, click **Next**. The **Resource Group** screen appears. Choose the corresponding iSCSI highly-available instance resource from the drop-down menu and select **Next**. Perform step 10 of "Creating the Target" on page 19.
4. Create and configure Targets on all nodes of PowerVault NX1950 system.

   NOTE: Redundant iSCSI NICs (MPIO) are supported with your PowerVault NX1950 cluster solution configured with 3.1 iSCSI Target and Microsoft iSCSI Initiator version 2.06 or later.

Configuring the Initiator-Target Connection From Initiator (Host)

1. From the iSCSI Initiator (host), go to **Start→Programs→Microsoft iSCSI Initiator→iSCSI Initiator Properties→Targets** tab. Refresh the screen. The PowerVault NX1950 storage solution Target device that you created in "Creating the Target" on page 19 is displayed in the IQN name format.
2. In the **Log On to Target window**, select **Logon** and check **Automatically restore** and **Enable multi-path** options. Select **Advanced**.
3. In **Advanced Settings** window, select **General** tab, and select the following options from drop-down menu:
   - **Local adapter**—Microsoft iSCSI Initiator
   - **Source IP**—One of the host I/P addresses that is used for iSCSI traffic
   - **Target Portal**—PowerVault NX1950 storage solution's iSCSI IP address
4. In the **Advanced Settings** window, click **OK**.

5 In the **Log On to Target** window, click **OK**.

The **Targets** tab displays the status of the Target as **Connected**.

6 To accomplish Multipathing, you can use Microsoft MPIO to establish multiple sessions from host to the same Target device. To establish multiple sessions:

a Go to the **Targets** tab and select the Target that is **Connected**.

b Repeat step 1 to step 4.

c In the **Advanced Settings→Target Portal** address, choose the redundant host IP address and the IP address of the PowerVault NX1950 storage solution.

NOTE: During the iSCSI Initiator software installation, Microsoft MPIO is already selected. MPIO is supported with Initiator version of 2.06 or later. You require two dedicated iSCSI NICs in the target and initiator for efficient MPIO connection. Multiple connections per session (MC/S) is not supported on the PowerVault NX1950 storage solution.

7 To initialize and configure the iSCSI device as local drive and perform iSCSI I/O operations, select **Computer Management→Disk Management** option.

NOTICE: If you are configuring the host to access multiple targets (VHD files), ensure that the hosts are clustered. If multiple hosts access the same target, data corruption may occur. For more information, see "Enabling Multi-Path on the Initiator" on page 61.

Method 2 (Discovery Using iSNS Server)

This section describes the procedure for iSCSI Target discovery using the iSNS server. For more information about the iSNS server, see "Appendix" on page 55.

Pre-Requisites

Before you perform iSCSI Target discovery, perform the following steps:

1. Download the Microsoft iSCSI Initiator software from Microsoft Support website at **support.microsoft.com** and install the Initiator (Host).
2. Download the Microsoft iSNS Server software from Microsoft Support website at **support.microsoft.com** and install the software on a client/server running Microsoft® Windows® operating system.

   NOTE: Do not install the iSNS Server software on Initiator (host) or Target (PowerVault NX1950 storage solution). Install the software on a separate Client/Server running Windows operating system.
3. Turn on the PowerVault NX1950 storage system and the PowerVault MD3000 storage array or Dell|EMC storage array configured with the storage system. Create one or more volumes on the storage array for creating Virtual Disks for iSCSI Targets.

Configuring Settings From the Initiator Server/Client

1. Configure the Microsoft iSCSI Initiator with iSNS server's information. Go to **Start→Programs→Microsoft iSCSI Initiator→Discovery tab→Add**.
2. Add the IP address of the iSNS server and click **OK**.

Setting Up the Target (PowerVault NX1950 Storage Solution and PowerVault NX1950 Cluster Solution)

1. From the PowerVault NX1950 storage solution, go to **Start→Programs→ Administrative Tools→Windows Unified Data Storage Server**.

   The **PowerVault NX1950 Management Console** appears.
2. Select **Microsoft iSCSI Software Target**, right-click and select **Properties**.
3. In the **Properties** window, select the **iSNS** tab, and add the iSNS server information (DNS Name or IP address).

   NOTE: If you are configuring a PowerVault NX1950 cluster solution, add the iSNS server information in the node that owns the Cluster Group. In all other cluster nodes, go to the **PowerVault NX1950 Management Console** ensure that **iSNS** tab is populated with the iSNS server information.

4 To create a target, follow the instructions in "Creating the Target" on page 19 and to create a virtual disk, follow the instructions in "Creating a Virtual Disk" on page 20. During step 7 of "Creating the Target" on page 19, use the **Browse** option to ensure that the **iSCSI Initiator Identifier** screen displays all Initiators that are registered with iSNS server.

NOTE: The 3.0 iSCSI Software Target does not query the iSNS server for registered iSCSI Initiators during Target creation. You have to enter the IQN name of the Initiator manually. After you create the Target, the Target IQN is listed in iSNS server registered device list and can be accessed by Initiators that were added during Target creation. This issue is resolved in the 3.1 iSCSI Target.

3

Detailed End-to-End iSCSI Setup

This section describes the end-to-end iSCSI setup, including settings for the iSCSI Initiator, Target, and establishing connections.

Setting Up Target IP Addresses in the PowerVault NX1950 Storage Solution

Based on configuration (with one or two dedicated iSCSI NICs) assign IP addresses to the iSCSI NICs. Use the IP address that you assigned to the iSCSI NIC(s) in the **Target Portals** tab of the Initiator for discovery.

Setting up Target IP Addresses in the PowerVault NX1950 Cluster Solution

To set up the Target IP address in a PowerVault NX1950 cluster solution:

Using the 3.0 iSCSI Target

1. Assign IP addresses to the iSCSI NICs in different subnets.
2. Add a virtual IP address as a cluster resource manually by adding virtual IP address for the iSCSI NIC.
3. When you configure the Initiators, add the virtual IP address of the iSCSI NIC in the **Target portals** tab.
4. After you complete the setup, the iSCSI Targets are managed by the active node. During failover, the iSCSI Targets are managed by the surviving node or the node that owns the Cluster Group.

Using the 3.1 iSCSI Target

1. Assign IP address to the iSCSI NICs and create highly available iSCSI instance on each node that is added as cluster resource. Use PowerVault NX1950 Management Console and the iSCSI snap-in to create the highly available iSCSI instances.

2 Add the newly-created highly available iSCSI instances as a resource group. The newly-created highly available iSCSI instances are then listed in **Active Resources** of cluster nodes.

3 When you configure the Initiators, add the highly available iSCSI instance IP address in the **Target Portals** tab.

4 After you complete the setup, the iSCSI Targets created on individual nodes that have highly available iSCSI instances. If the node fails, the iSCSI Targets of the failed node are managed by surviving node or the node that owns the Cluster Group.

Configuring iSCSI Devices

This section provides detailed information about installing and configuring the Initiator and Target in PowerVault NX1950 storage solution.

Installing Microsoft iSCSI Initiator

The Microsoft iSCSI Initiator is a free download on the Microsoft website at **www.microsoft.com**. Different versions of the iSCSI Initiator for x86 (32-bit processors), x64 (AMD64™ and Intel® EM64T processors), and IA64 (for Intel processors) are available. For all procedures in this document, go to the *Dell PowerVault NX1950 Systems Support Matrix* and verify the iSCSI Initiator Version that is used on all hosts. Download and extract the supported iSCSI Initiator software version on the client/server that is used as an *Initiator* device.

NOTE: Other versions of iSCSI Initiator are not supported. If you are running a different version of iSCSI Initiator on the Initiator Clients/Servers, remove the iSCSI Initiator using the **Add/Remove Programs** option and install the supported version.

1 After you download the iSCSI Initiator from the Microsoft website at **www.microsoft.com**, double-click the **Initiator-<version>.exe** (where *version* is the version of the iSCSI Initiator that you downloaded) file to begin installation.

2 The **Software Update Installation Wizard** appears. Click **Next**.

3 The **Microsoft iSCSI Initiator Installation** screen appears. The options **Initiator Service** and **Software Initiator** are selected by default. The **Microsoft MPIO multi-pathing** is unchecked. You must check this options as the installation requires the use of Multipath I/O (MPIO) feature. Click **Next**.

NOTE: You must select the Microsoft MPIO support for iSCSI during installation to accomplish load balancing and failover among multiple NICs and iSCSI host bus adapters (HBAs). MPIO support in a PowerVault NX 1950 cluster system is available only if you install Microsoft iSCSI initiator version 2.06 or later.

4 The **License Agreement** screen appears. Read the agreement and select **I Agree** to continue with the installation. Click **Next**.

5 The **Completing the Microsoft iSCSI Initiator Installation Wizard** appears indicating the installation is complete. Click **Finish**.

6 The Wizard prompts you to reboot the system. Click **OK**.

The system reboots and iSCSI Initiator is installed. A command-line utility called **iSCSICLI** is also installed. You can use the **iSCSICLI** utility to manage the iSCSI Initiator service and HBAs.

The Release Notes and User Guide are saved to the local host when the iSCSI Initiator package is extracted. You can find the following information in the documents that are saved to the hard drive. Some of the restrictions in the list below may change in future releases.

- Dynamic disks on an iSCSI session are not supported.
- The default iSCSI node name is generated from the Windows computer name. If the Windows computer name contains a character that is invalid within an iSCSI node name, such as _ (underscore), then the Microsoft iSCSI Initiator service replaces the invalid character with - (hyphen).
- Both Initiator and Target CHAP secrets should be greater than or equal to 12 bytes, and less than or equal to 16 bytes if IPsec is not being used. The Initiator and Target CHAP secrets should be greater than 1 byte and less than or equal to 16 bytes if IPsec is being used. For more information about CHAP, see "CHAP vs IPSec" on page 52.

Configuring the Microsoft iSCSI Initiator

After the installation is complete, you can use the iSCSI Initiator to manage the iSCSI environment. This section describes the initial configuration steps.

If you use the **Direct Portals** option in the **Discovery** tab of the **iSCSI Initiator Properties** window, add iSCSI NIC IP address of the PowerVault NX1950 storage system.

If you are configuring a PowerVault NX1950 cluster solution:

- **a** Add the highly-available iSCSI instance IP address in the **Target Portals** tab (3.1 Target).
- **b** Add the virtual IP address that was created and added as a cluster resource using the iSCSI NIC (3.0 Target).

All Targets that are created in the PowerVault NX1950 cluster solutions are listed in the **Targets** tab.

If you use the **iSNS servers** option in the **Discovery** tab, the Targets created in all PowerVault NX1950 storage solutions/cluster solutions that are registered with iSNS server are displayed.

Configuring Microsoft iSCSI Software Target

The Microsoft iSCSI Software Target software package is pre-installed on the PowerVault NX1950 storage solution.

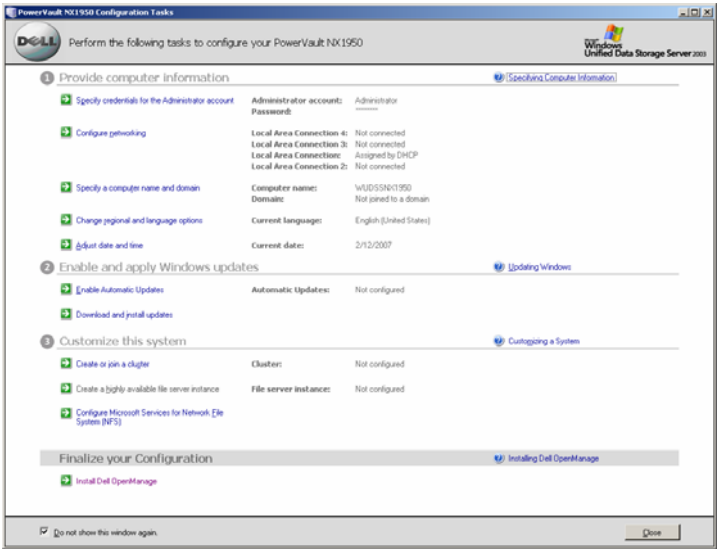
Before configuring iSCSI Targets, you must create a few LUNs and reserve storage space to create Virtual Disks for iSCSI Targets. The following section provides step-by-step instructions to create storage space.

Configuring the Target

1. Configure Network Settings on the iSCSI Target device—The PowerVault NX1950 storage solution is configured to use DHCP for network settings by default. The PowerVault NX1950 storage system is designed for multi-path operations and is equipped with two RJ45 Ethernet connectors. You can add an optional additional NIC. The **PowerVault NX1950 Configuration tasks** window displays the basic settings.

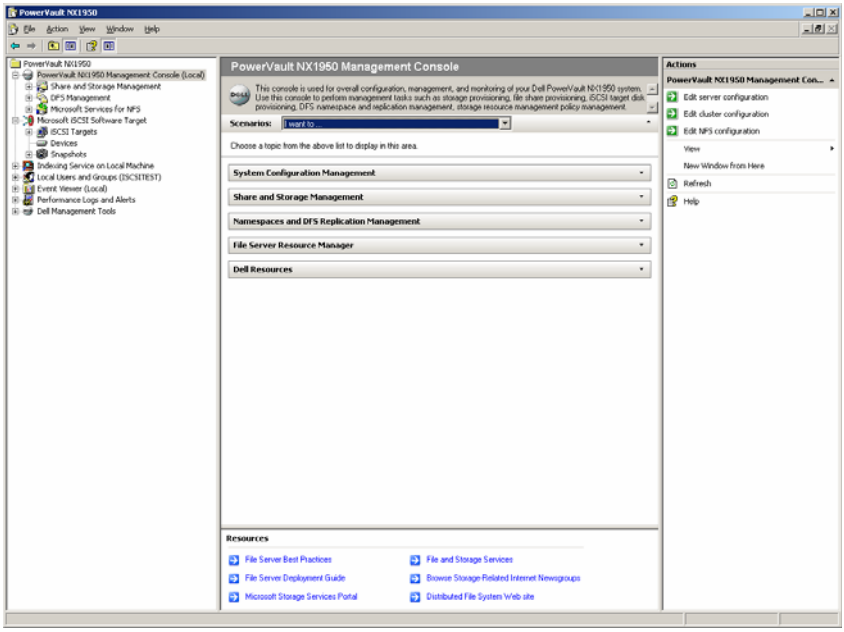
   NOTE: It is recommended that you configure dedicated iSCSI NICs on separate subnets and not on the public network.

Figure 3-1. The PowerVault NX1950 Configuration Tasks Window



2 Launch the **PowerVault NX1950 Management Console**—When you close the **PowerVault NX1950 Configuration Tasks** window, the **PowerVault NX1950 Management Console** is launched. You can use the **PowerVault NX1950 Management Console** to perform all storage management functions for PowerVault NX1950 storage solution.

Figure 3-2. PowerVault NX1950 Management Console



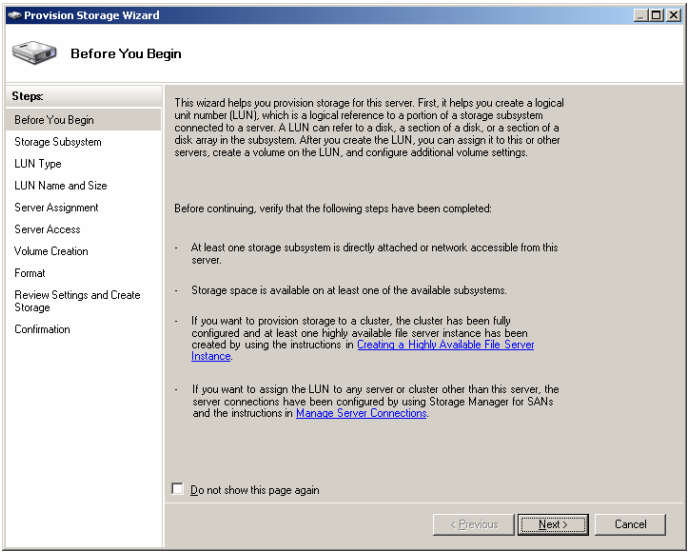
In Figure 3-2, the **Scenarios** section in the middle pane provides several scenarios to help you through each of the storage management processes.

3 Create LUNs on Disk Array—To create the LUNs on the Disk Array, select the **Provision Storage and Create Volume** scenario from the **Scenarios** section. The scenario walks you through the procedure to provision storage and create volumes.

a The right-pane of the **PowerVault NX1950 Management Console** is context-sensitive and changes based on the item you select on the left-pane. When you select **Share and Storage Management** on the left-pane, the **Provision Storage wizard** is displayed on the right-pane.

When you select **Provision Storage** on the right pane, the **Provision Storage** wizard appears. Follow the on-screen instructions provided by the wizard to complete the provisioning process.

Figure 3-3. Provision Storage Wizard



b The **Storage Subsystem** screen appears and prompts you to select at least one storage subsystem. Select at least one subsystem and click **Next**.

c The **LUN Type** screen appears. You can choose the LUN type from the available types of LUNs. Each LUN type has a maximum size that is calculated depending on the LUN type. Choose the appropriate LUN type and click **Next**.

NOTE: It is important at this point to note that the storage solution LUN size should not be confused with the size of the iSCSI Target. The iSCSI Target is configured in a later step and is associated with the storage needed for a particular application on the host server. It is recommended that the LUN size on the storage hardware be as large as reasonably possible to allow the storage subsystem to optimize the use of the physical disks underlying the LUN that is created. In this case, as shown below, we are choosing to create one LUN at the maximum size available for this hardware. This iSCSI LUN cannot accommodate the iSCSI Targets that are created later, based on the needs of the host application.

d The **LUN Name and Size** screen appears. Enter the **LUN name** and **LUN size**. Click **Next**.

e The Server Assignment screen appears. Choose the **This server only** option and click **Next**.

NOTE: The LUN that you have created is assigned to the internal storage server only. The iSCSI Targets that are created are configured to be assigned to external application servers later.

NOTE: If you are configuring a PowerVault NX1950 cluster solution as the Target, select the **All servers in this cluster** option in the **Server Assignment** screen.

f The **Server Access** screen appears. You must provide the name of the internal storage server for assignment.

NOTE: If you are configuring a PowerVault NX1950 cluster solution as the Target, select the cluster name in the **Server Access** screen. The **Server Access** screen displays a generic warning message about the I/O path. This warning does not affect the functionality and no action is required.

NOTE: If you are configuring a PowerVault NX1950 cluster solution with 3.1 iSCSI Target, select the iSCSI HA instance resource name in the **Highly Available Server** screen. If you want use the existing volumes for iSCSI, use **Cluster Administrator** to move the volumes to corresponding iSCSI HA instances.

4 Make LUNs Ready for Use—The PowerVault NX1950 storage solution runs on a Microsoft Windows operating system based platform. Therefore, the steps to prepare LUNs for use—like assigning a drive letter for the internal server, providing a volume name, and so on are familiar to Windows operating system setup. The setup wizard prompts for the required information and then provides a summary screen before performing the necessary tasks to provision the storage.

a In the **Provision Storage** wizard, the **Volume Creation** screen appears. Select **Create a volume on the LUN** and select a drive letter to be assigned to the volume. Click **Next**.

b The **Format** screen appears. Select **Format volume** and specify the label for the volume. Set the **Allocation unit size** to `Default` and select **Quick format**. Click **Next**.

c The **Review Settings and Create Storage** screen appears. Review the storage settings and click **Create**.

The Storage provisioning occurs and the **Confirmation** screen appears indicating a successful provisioning operation.

The LUN is now created and ready for use. The step 5 creates iSCSI Targets and associates the iSCSI Targets with the newly-created LUN. The PowerVault NX1950 storage solution uses Windows Unified Data Storage Server 2003 with Microsoft Virtual Disk Service (VDS) internally. You can also view the LUN in the **PowerVault NX1950 Management Console→Storage Manager for SANs** section.

5 Configuring NICs for iSCSI traffic in the PowerVault NX1950 storage solution in standalone mode— To create iSCSI Targets you must configure dedicated iSCSI NICs for iSCSI traffic and then create iSCSI Targets.

NOTE: Create iSCSI Targets only after configuring the **Discovery** tab in the iSCSI Initiator

To configure dedicated iSCSI NICs:

a Go to **PowerVault NX1950 Management Console→iSCSI Target** section.

b Right-click the iSCSI Software Target and select **Properties**.

c In the **Microsoft iSCSI Software Target Properties** window, go to the **Network** tab. All the NICs on the PowerVault NX1950 storage solution are listed.

d Click **Edit** and uncheck public and private network IP address from the list. Unchecking public and private network IP addresses from the list ensures that only the dedicated iSCSI NICs are configured for iSCSI traffic.

e If you have an iSNS server configured in your network, go to **iSNS** tab and add the iSNS server IP address. Click **OK**.

The following steps describe the procedure to create two iSCSI Targets as shown in the example, Figure 3-4. Each Target is made available to a different application on the host server. The Target in the Microsoft-based iSCSI Target solutions only defines the path that the iSCSI storage traffic uses from the iSCSI Initiator. The storage used by the Target is defined in a later step when the Virtual Disks are created.

6 Configuring NICs for iSCSI traffic in the PowerVault NX1950 storage solution in cluster mode— If you are setting up PowerVault NX1950 cluster solution as an iSCSI Target, perform the following prerequisites:

- Follow the steps listed in the section **Creating a Highly Available iSCSI Target** in the *Dell PowerVault NX1950 Cluster Systems Installation and Troubleshooting Guide* on the Dell Support website at **support.dell.com**.
- Turn off the firewall in all cluster nodes to ensure proper iSCSI Target configuration. You can turn on the firewall after successful Target configuration. You can configure Active/Active clustering to provide high availability for iSCSI storage using 3.1 iSCSI Target. The following steps outline the procedure for 3.1 iSCSI Target configuration.

You can configure the cluster environment for Active/Active iSCSI target access using the **iSCSI Software Target option** in the **PowerVault NX1950 Management Console**. As a part of the initial configuration, you must perform the following tasks:

- Create a highly-available instance (resource group) for Active/Active clustering. Use the iSCSI Software Target MMC interface to create a iSCSI highly-available instance.
- Highly-available instances are used to manage iSCSI Target resources, including iSCSI Targets, iSCSI Virtual Disks, snapshots, and schedules. You have the option of creating new highly-available instances for iSCSI storage or use previously-configured highly-available instances. You can use the same resource group to provide high availability for both file sharing and block sharing.
- Configure the IP addresses for the iSCSI highly-available instances. If you do not configure the cluster environment to support Active/Active clustering, iSCSI Target software creates iSCSI Targets and iSCSI Virtual Disks in a non-clustered environment by default.

To configure the iSCSI HA instance perform the following steps in all nodes of cluster system:

NOTE: To perform this procedure, you must have Administrator rights on the local computer. For best practices, use the **Run** option to perform this procedure.

a Open the **PowerVault NX1950 Management Console**, right-click **Microsoft iSCSI Software Target**, and then click **Create HA Instance for iSCSI**.

b In the **Create Highly Available Instance for iSCSI Storage** dialog box, click **Add**.

c In the **Add IP Address Resource** section, choose the following options:

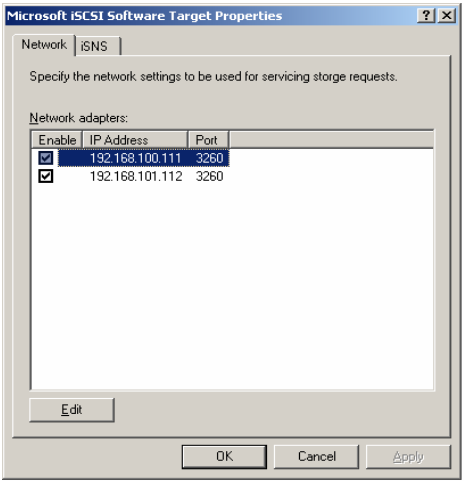
- **Resource name**—Retain the default value or enter a different name
- **IP address**—IP address to be used by iSCSI initiators to connect to the iSCSI Target
- **Subnet mask**—subnet mask to be used by iSCSI initiators to connect to the iSCSI Target
- **Network interface**—select the name of the network interface to be used for the IP address resource of the cluster resource group.

d Click **OK** and add IP address for the second NIC if you have redundant iSCSI NIC. Click **OK** again.

NOTE: Before you create iSCSI Virtual Disks, create few Dell|EMC LUNs or PowerVault MD3000 LUNs and assign them to the Cluster's highly-available Sever (iSCSI HA instance) using PowerVault NX1950 Management console. If you prefer to use the existing volume of Cluster, then move the volume to iSCSI HA instances using **Cluster Administrator**. From any PowerVault NX1950 cluster node, go to **Start→All programs→Administrative Tools→Cluster Administrator**.

7 Perform the following steps to create iSCSI Targets:

Figure 3-4. Creating iSCSI Targets



NOTE: In the **PowerVault NX1950 Management Console**, right-click **Microsoft iSCSI Software Target**, and select **Properties**. In the **Networks** tab, select the corresponding iSCSI NIC IP address and deselect the remaining IP addresses. If you are using the 3.1 iSCSI Target, select the highly available iSCSI instance IP address only.

a In the **PowerVault NX1950 Management Console**, right-click **iSCSI Targets** on the left pane to launch the **Create iSCSI Target Wizard**.

b The **Welcome to the Create iSCSI Target Wizard** screen appears. Click **Next**.

c The **iSCSI Target identification** screen appears. Enter the **Target name** and **Description**. You can use the **Browse** option to view and choose the servers/clients in the network.

d The **iSCSI initiators identifiers** screen appears.

You must associate each iSCSI Target with an iSCSI Initiator. The iSCSI Initiator is the host that requests access to the storage that is represented by the iSCSI Target name.

e In the **iSCSI initiators identifiers** screen, enter the iSCSI Qualified Name (IQN) of the iSCSI Initiator. You can manually enter the IQN or use the **Browse** option and choose the iSCSI Initiator from the list.

- You can also provide alternate ways to identify the iSCSI Initiator by using the **Advanced** option. When you click Advanced, the Advanced Identifiers screen appears. In the **Advanced Identifier** screen, click **Add**, and enter the Identifier type and the specific identifying information.
- Go to **Advanced Identifier→Add→Add/Edit Identifier→ Identifier Type** and choose from the four different options IQN, DNS Domain Name, IP address, and MAC Address to add the Initiator identifier. Figure A-5 uses the IP address to identify the iSCSI Initiator. You can use the **Browse** option to choose the value from the list of available Targets.

NOTE: It is recommended that you use the IQN as the Identifier.

The **PowerVault NX1950 Management Console** now displays the newly-created iSCSI Target. The **PowerVault NX1950 Management Console** also displays the devices available for the iSCSI Targets. The storage that are used by the iSCSI Initiators (application hosts) are defined in a later step when the Virtual Disks are created.

8 Create and assign Virtual Disks to the Target—You must create Virtual Disks on the iSCSI Targets for Microsoft-based iSCSI Target solutions. The Virtual Disks represent the storage volumes that the iSCSI Initiators use. The maximum capacity represented by all the Virtual Disks on a given iSCSI Target on a Microsoft-based iSCSI Target solution is 2 terabytes (2 TB) per Target.

The following procedure describes the procedure to create a Virtual Disk. In this example, a 100 GB Virtual Disk and a 200 GB Virtual Disk are created on the iSCSI Target. The iSCSI Initiators identify these two Virtual Disks as volumes over the TCP/IP network.

a Right-click on the Target name to launch the **Create Virtual Disk Wizard**.

b Click **Next**. The **File** screen appears.

Create the Virtual Disk on the internal disk volume (the RAID volumes available from the attached storage array) that is available to the iSCSI Target.

NOTE: In the **File** screen, use the **Browse** option to choose the internal disk volume using browse and enter a name for Virtual Disk file with a **.vhd** extension.

c Click **Next**. The **Size** screen appears.

The size of the Virtual Disk depends on the needs of the application on the host server. Choose the size for the Virtual Disk and click **Next**. For this example, we choose a size of 100 GB from the available 501 GB on this volume.

d The **Description** screen appears. The **Description** field is optional. However, enter a description for better management. Click **Next**.

e The **Access** screen appears. Click **Add** and enter the iSCSI Target information.

You must associate the Virtual Disk with an iSCSI Target for the application host to use the Virtual Disk as an iSCSI storage volume.

f Click Next. The **Completing the Create Virtual Disk Wizard** appears indicating the successful completion of the Virtual Disk creation.

g Repeat step a through step f to create an additional Virtual Disk.

After configuring the Virtual Disks, the **PowerVault NX1950 Management Console** displays the Virtual Disks associated with the iSCSI Target.

The **iSCSI Target device** view displays the total volume size and the free space on the device (RAID volume) that is available for iSCSI Targets.

The iSCSI Target configuration is now complete.

Configuring Devices

You can perform all operations related to Virtual Disks (Devices) using the following options in **PowerVault NX1950 Management Console**:

- Create/Delete Virtual Disk—Virtual Disks are represented with a **.vhd** extension. You can create or delete Virtual Disks using this option.
- Extend Virtual Disk—You can dynamically increase the size of an iSCSI Virtual Disk without losing data and without restarting the iSCSI Target.
- Import—You can import the old Virtual Disks, existing Virtual Disks previously created on the same server or another server. This feature is useful during software upgrades.
- Disable—You can temporarily take the Virtual Disk offline and can bring the Virtual Disk back online with the Enable option.
- Assign/Remove Target—Associate Virtual Disk with one or more targets, remove the existing association.
- Create Snapshot—You can take a snapshot of the Virtual Disk contents at an given instance.
- Disk Access—Mount Read/Write (Provision of Read/Write access of the Virtual Disk by mounting it as a volume in the PowerVault NX 1950 storage system. Mounted Virtual Disk will appear as a local disk)

NOTICE: Before mounting the Virtual Disk, disconnect all iSCSI Targets using the same Virtual Disk. Failure to do so can cause data corruption.

Establishing Connections

After you install and configure iSCSI Initiators and Targets, you must establish sessions to ensure successful login from Initiator to Target and to perform iSCSI block I/O operations.

Pre-Requisites

- Perform the procedure in "Configuring iSCSI Devices" on page 28.
- Ensure that Target Portals information is added in **Microsoft iSCSI Initiator Properties→Discovery** tab.

Follow these steps to establish sessions:

1. Log on to iSCSI Target device.

2 Go to **iSCSI Initiator Targets** tab.

The IQN of the Targets is listed and status is displayed as **Inactive**. Select one Target device and select **Logon**.

3 The **Log On to Target** screen appears. You can select the **Automatically restore this connection when the system reboots** option for re-establishing connection during probable reset/reboot of the Initiator.

4 You can use the **Enable Multi-path** option for load balancing/failover settings.

a Choose this option to enable MPIO and select **Advanced**.

b Go to **Advanced Settings→General** tab and select the following options from drop-down menu:

– Local Adapter — Microsoft iSCSI Initiator

– Source IP — one of the host I/P addresses

– Target Portal — iSCSI IP address of the PowerVault NX1950 storage solution

c In the **Advanced Settings** window, click **OK**. In the **Log On to Target** window, click **OK**.

The **Targets** tab now displays the Target status as **Connected**.

5 In the **Log On to Target** screen, you can use the **Advanced..** option for other advanced options like CRC/Checksum and IPSec Settings. For more information, see "Appendix" on page 55.

6 In the **Log On to Target** screen, click **OK**.

The connection is established and the status is displayed as **Connected**.

7 To configure multiple paths for iSCSI, repeat step 1 through step 6 and select the following options:

a Selecting the Target that is **Connected** and click **LogOn**.

b In the **Logon to Target** window, select **Advanced..**, and then select the IP address of the second NIC on the Initiator that is not in use.

c In the **Advanced Settings** window, select the redundant iSCSI IP address of the PowerVault NX1950 storage system.

Selecting the redundant iSCSI IP address ensures that the iSCSI network traffic and the public network traffic are on separate subnets. This also allows load balancing/Failover.

The iSCSI connection is now established and the device is ready for block I/O operations.

NOTE: You can also configure Load balancing and failover by using Microsoft MPIO support or Multiple Connections per Session (MC/S). Currently the MPIO option is supported with PowerVault NX1950 storage solution and PowerVault NX1950 cluster solution configured with 3.1 iSCSI Target and Microsoft iSCSI Initiator version 2.06 or later. The MC/S option is not supported with PowerVault NX1950 storage system and PowerVault NX1950 cluster solutions.

Configuring iSCSI LUNs

1 From Disk Management, configure the iSCSI Target device. Go to the iSCSI Initiator host and click **Start →Control Panel →Administrative tools →Computer Management→Disk Management**.

2 In the right pane, the iSCSI disk is displayed as **Unknown Not Initialized** and **Unallocated**.

3 The **Welcome to the Initialize and Convert Disk Wizard** option appears. Run the **Initialize and Convert Disk Wizard**.

a Retain the default settings and select **Next** in all screens.

b The **Completing the Initialize and Convert Disk Wizard** screen appears. Click **Finish**.

NOTE: Dynamic disks are not supported with iSCSI configuration.

4 Go to the **Disk Management**. The **Unallocated** iSCSI disk is now identified as **Basic** and **Unallocated**. Right-click the iSCSI disk and select **New Partition…**.

a The **New Partition Wizard** is launched. Click **Next**.

b In the **Select Partition Type** screen, select the Partition Type as **Primary Partition**. Click **Next**.

c In the **Specify Partition size** screen, specify the partition size. Click **Next**.

d In the **Assign Drive Letter or Path** screen, assign the driver letter from drop-down menu. Click **Next**.

e In the **Format Partition** screen, use the default options to format the partition. Enter a Volume label and click **Next**.

NOTE: Select the **Perform quick format** check box for faster Format.

f In the **Completing the New Partition Wizard** screen, click **Finish**. The new partition is successfully created.

5 Go to the **Disk Management**. The iSCSI disk is identified with the volume label you entered.

NOTE: Dynamic Disks are not supported with iSCSI.

Multiple Sessions

You can create multiple sessions with different Initiator-Target combinations in different devices.

- You can configure one Initiator to access different iSCSI Targets of multiple PowerVault NX1950 storage systems.
- You can configure multiple Initiators to access different iSCSI Targets of same or different PowerVault NX1950 storage systems.
- You cannot configure multiple Initiators to access the same iSCSI Target of a PowerVault NX1950 storage or cluster solution.

NOTICE: Accessing the same Target device using multiple iSCSI Initiators with 3.0 and 3.1 iSCSI Target is not supported, as it requires host clustering which is not supported. An attempt to access the same Target device using multiple iSCSI Initiators with 3.0 and 3.1 iSCSI Target may lead to data corruption.

iSCSI Snapshots

You can use Microsoft iSCSI Software Target to create and manage Snapshots as part of a comprehensive backup and recovery system. Snapshots are shadow copies that are built using the Volume Shadow Copy Service (VSS) technology.

To automate the creation of snapshots and the mounting of iSCSI Virtual Disks for regular backups, you can use the **Schedule Snapshot Wizard**. Snapshots of Virtual Disks that reside on an NTFS file system volume are persistent, which means they remain after a system restart.

Snapshots that are created on the iSCSI Target server are crash consistent. iSCSI Snapshots are created using VSS and a storage array with a hardware provider designed for use with VSS. To enable consistent snapshots in Microsoft iSCSI Software Target, you require the Microsoft iSCSI Software Target VSS Hardware Provider. The Microsoft iSCSI Software Target VSS Hardware Provider is available as an installation option in iSCSI Software Target. The hardware provider coordinates with the local VSS to create a consistent image of the volume that can be transported to a central backup server.

In a PowerVault NX 1950 Storage system, you can create an iSCSI Snapshot in two ways:

- Manually create a Snapshot of a single Virtual Disk in the Microsoft iSCSI Software Target console.
- Use the **Schedule Snapshot Wizard** to set up a schedule for creating a single Snapshot or recurring Snapshots automatically.

Before Creating Snapshots

Before creating snapshots for Virtual Disks perform the following steps. Use the Windows Explorer and go to the volume that contains the Virtual Disks that you are creating snapshots for.

1. Go to **Volume→Properties→Shadow Copies→Settings**. Ensure that the **Located on this volume** option in the **Storage Area** tab displays the same drive letter as that of the volume.
2. Click **Details** to verify the volume usage. The default settings are as follows:
   - **Maximum size**
   - **Use limit**—size in MB or **No Limit**

   Change the size according to Virtual Disk/Snapshot size or change the settings to **No Limit**.

NOTICE: Ensure that you have enough space in the volume to hold Virtual Disk Snapshots. If there is not enough space, the Snapshots are lost.

3 After making necessary changes, click **OK**.

NOTICE: Although you do not change the default settings, go to **Volume→ Properties→Shadow Copies→Settings** and click **OK**. Perform this action especially in a PowerVault NX1950 cluster solution to ensure proper Snapshot recovery in the event of cluster node failure. Active snapshots may be lost on account of a cluster node failure, if you do not have enough space or if you have not configured the Snapshots properly. When the Snapshot size exceeds the maximum size of the storage area, the oldest snapshot is deleted.

NOTE: Each volume can have up to 512 snapshots for iSCSI Virtual Disks, irrespective of the number of Virtual Disks created in the volume. Snapshots are space efficient because they are differential copies.

Scheduling Snapshots

To Schedule Snapshots for iSCSI Virtual Disks, perform the following steps:

1 Go to **PowerVault NX 1950 Management Console→Microsoft iSCSI Software Target**.

2 Go to the **Snapshots** tab, right-click **Schedules** and select **Create Schedule**.

3 The **Welcome to the Schedule Snapshot Wizard** screen is displayed. Click **Next**.

4 The Schedule Actions screen is displayed and the following options are available:

`Take snapshots of the Virtual Disks (default)`

`Take snapshots of the Virtual Disks and mount the snapshots locally`

Select one option and click **Next**.

5 In a PowerVault NX1950 cluster solution, the **Resource Group** screen is displayed. Select the **Resource Group** as **Cluster Group** from the drop-down menu. If your system is configured with 3.1 iSCSI Target, select the **Resource Group** as **iSCSI HA instance** from drop-down menu.

6 In the **Name** screen, enter a Schedule name and click **Next**.

7 The **Virtual Disks** screen appears and displays two options.

```
Include all Virtual Disks (default)

Include only the selected Virtual Disks
```

You can select all or selected Virtual Disks for snapshots.

NOTE: In a PowerVault NX1950 storage solution, all Virtual Disks are listed in the **Virtual Disks** screen. In a PowerVault NX1950 cluster solution, Virtual Disks of the volumes that are available in the selected Resource Group are listed.

8 The **Frequency** screen appears and lists the different options namely—**Daily**, **Weekly**, **Monthly**, and **On-time only**. Choose one option and click **Next**.

9 You must select the Start time, Days, Months, Start Date, and other time parameters based on Frequency selection in step 8. Edit these parameters to the preferred time. Click **Next**.

NOTE: You can modify the Snapshot schedule later.

10 The **Completing the Schedule Snapshot Wizard** screen is displayed. Click **Finish**.

Verifying Scheduling Snapshots (Optional)

After you schedule the creation of Snapshots, go to the **PowerVault NX1950 Management Console→Microsoft iSCSI Software Target→Snapshots→ Schedules** and verify that Schedule name, current run, next run with time-stamping are displayed in the middle-pane.

Active Snapshots

After scheduling the creation of snapshots, go to the **Active Snapshots** tab. All snapshot details including the Source Virtual Disk, Time stamp, and the Export status are listed in the middle-pane.

You can use the **Active Snapshots** tab to export, delete, rollback, and mount Active Snapshots like a local disk.

- Export Snapshot—Use this option to make Snapshot available to a remote system or to take a redundant copy of a Snapshot. Use the **Export Snapshot** wizard to export the Snapshot to one or more iSCSI Targets. The Snapshot can then be accessed by Initiators (read-only access). To export snapshot perform the following steps:
  - **a** Go to the **Active Snapshots** tab, select the snapshot that you want to export from the middle-pane, right-click and select **Export Snapshot**.
  - **b** The **Welcome to the Export Snapshot Wizard** appears. Click **Next**.
  - **c** In the **Snapshot Access** screen, add the Targets that you want to grant read-only access to this Snapshot. Click **Next**.
  - **d** Click **Finish**.
  - **e** Go to the Target and verify that this snapshot has been added as a Virtual Disk.

  NOTE: In a PowerVault NX1950 cluster solution, the snapshot must be exported to the targets belonging to the same resource group.
- Delete snapshot—Select the Snapshot that you want to delete, right-click and click **Delete**.

  NOTE: You cannot delete the Snapshots that are mounted. You must dismount the Snapshot before deleting it.
- Disk Access – You can mount the Snapshot of an iSCSI Virtual Disk in read-only mode from the PowerVault NX1950 storage system and it appears as a local disk.

NOTICE: While dismounting a Snapshot/Virtual Disk, ensure that the disk is not in use. Failure to do so may cause data corruption.

NOTE: You can either mount iSCSI Virtual Disk (read/write or read/only) or its Snapshot (read-only), but not both. If you have mounted Virtual Disk and perform a subsequent mount operation of Snapshot, the previous instance is dismounted before proceeding.

- Rollback—Use this option to rollback an iSCSI Virtual Disk to a previous Snapshot. This operation uses the **temp** directory located at **C:\Windows\Temp**. Ensure that the **temp** directory contains sufficient space to store the differential data. The rollback fails if enough space. is not available.
  - **a** Right-click on the snapshot and select **Rollback to Snapshot**. In the pop-up message, select **Yes**.
  - **b** To check the status of rollback, go to the **Devices** tab. The rollback progress is displayed in % (percentage) in the Virtual Disk section of the middle-pane.
  - **c** You can also abort a rollback operation. Abort a rollback, if you can rollback to a different snapshot. Otherwise it is highly recommended that you allow the rollback to complete.

  NOTE: If you rollback, all data on the current Virtual Disk is lost. Disconnect all iSCSI Targets from initiator that are using this Virtual Disk. If the Virtual Disk mounted as a read/write disk, dismount the Virtual Disk before the rollback.

Disconnecting/Cleaning Up iSCSI Devices

This section describes the procedure for cleanup operations to be performed on iSCSI devices. You must perform the procedure cleanup operations on both iSCSI Target and ISCSI Initiator.

From Initiator

Disconnect an active connection with Target by stopping the iSCSI I/O operations that are running on that Target device by performing the following steps:

1. Go to **Start→All Programs→Microsoft iSCSI Initiator→iSCSI Initiator Properties→Targets** tab.
2. Select the Target that is **Connected** and select **Details**.
3. The **Target Properties** screen appears. In the **Sessions** tab, select the check box beside the Identifier and click **Logoff**. The connection is disconnected.
4. In the **iSCSI Initiator Properties** screen, go to **Persistent Targets** tab and remove entries of persistent Targets.

5 If you want to remove Target IQN name entries, go to the **Discovery** tab and remove the IP address/DNS name of the PowerVault NX1950 storage system in the **Target Portals** section or remove the IP address/DNS name entry of the iSNS server.

6 Go to the **Targets** tab and click the **Refresh**. The Target IQN name is not listed.

From Target

To remove Virtual Disk from iSCSI Target, delete Virtual Disks by performing the following steps:

1 Go to **PowerVault NX1950 Management Console→Microsoft iSCSI Software Target→iSCSI Targets→**and select the Target and the associated Virtual Disks to be deleted.

   a The middle pane lists all Virtual Disks. Right-click the Virtual Disk to be deleted and select the **Remove Virtual Disk From iSCSI Target** option.

   b Repeat step a for all Virtual Disks associated with this Target.

2 To delete a Target, right-click on the Target, and select the **Delete iSCSI Target** option. Manually browse to locate the .vhd file associated with the Target and delete it.

3 To delete a Virtual Disk, choose the **Devices** option, right-click on the Virtual Disk from middle pane, and select **Delete Virtual Disk**.

   NOTE: The step 3 only deletes the association in the iSCSI Target software, but does not clear the disk space in the volume. You must manually browse to the volume and delete the **.vhd** file to clear the disk space.

4 To remove and iSNS server entry, right-click **Microsoft iSCSI Software Target→**select **Properties→iSNS** tab **→Remove the DNS name or IP address entry**.

5 To remove iSCSI HA instance of 3.1 Target, go to **Cluster Administrator** and delete the resource. If you want to retain the volumes, move the volumes to a different resource group.

4

Configuring Secured iSCSI Connections Using Challenge-Handshake Authentication Protocol

Few security features for the iSCSI protocol are included in the iSCSI layer itself, apart from any security layers that may be present in the lower TCP/IP and Ethernet layers. You can enable and disable the iSCSI security features as required.

The Microsoft® iSCSI Initiator uses the Challenge-Handshake Authentication Protocol (CHAP) to verify the identity of iSCSI host systems attempting to access iSCSI Targets. The iSCSI Initiator and iSCSI Target use CHAP and share a predefined secret. The Initiator combines the secret with other information into a value and calculates a one-way hash using the Message Digest 5 (MD5) function. The hash value is transmitted to the Target. The Target computes a one-way hash of its shared secret and other information. If the hash values match, the Initiator is authenticated. The other security information includes an ID value that is increased with each CHAP dialog to protect against replay attacks. The Dell™ PowerVault™ NX1950 storage solution also supports Mutual CHAP.

CHAP is generally regarded as more secure than Password Authentication Protocol (PAP). Fore more information regarding CHAP and PAP, see the RFC 1334 website at **http://rfc.arogo.net/rfc1334.html**.

CHAP vs IPSec

CHAP authenticates the peer of a connection and is based upon the peers sharing a secret (a security key that is similar to a password). IP Security (IPSec) is a protocol that enforces authentication and data encryption at the IP packet layer and provides an additional level of security.

One-Way CHAP Authentication

In One-Way CHAP authentication, only the iSCSI Target authenticates the Initiator. The secret is set only for the Target and all Initiators that are accessing the Target must use the same secret to start a logon session with the Target. To set one-way CHAP authentication, configure the settings described in the following sections on Target and Initiator.

iSCSI Target settings

Before you configure the settings described in this section, ensure that few iSCSI Targets and Virtual Disks are already created and the Virtual Disks are assigned to the Targets.

1. On an iSCSI Target, go to **PowerVault NX1950 Management Console**→ **Microsoft iSCSI Software Target**→**iSCSI Targets** →<Target name> and either right-click and select **Properties** or go to **Actions** pane→**More Actions**→**Properties**.

   The **<Target Name> Properties** window appears, where *Target Name* is the name of the iSCSI Target that you are configuring iSCSI settings for.

2. In the **Authentication** tab, select the check box for **Enable CHAP** and type the User name (IQN name of the Initiator). You can enter the IQN manually or use the **Browse** option to select the IQN from a list.

3. Enter the **Secret**, re-enter the same value in **Confirm Secret**, and click **OK**. The secret must include 12 to 16 characters.

   NOTE: If you are not using IPSec, both Initiator and Target CHAP secrets should be greater than or equal to 12 bytes and less than or equal to 16 bytes. If you are using IPsec, the Initiator and Target secrets must be greater than 1 byte and less than or equal to 16 bytes.

iSCSI Initiator Settings

1. Go to the **Discovery** tab.
2. Log in to the Target on which you have enabled CHAP in "iSCSI Target settings" on page 52 by clicking **iSCSI Initiator Properties→Targets** tab→ **Log On...**.
3. In the **Log On to Target** window, select **Advanced**.
4. In the **Advanced Settings** window, select the check box for **CHAP logon information**.

   The **User name** fields displays the IQN of the Initiator automatically.
5. In the **Target secret** field enter the same value of the target secret that you set in the iSCSI Target and click OK.

   If the Target secret value is correct, you are logged on to the Target. Otherwise the logon fails along with Authentication failure.

Mutual CHAP Authentication

When you use Mutual CHAP authentication, the Target and the Initiator authenticate each other. A separate secret is set for each Target and for each Initiator in the storage area network (SAN).

Initiator Settings

1. On the iSCSI Initiator, go to the **iSCSI Initiator Properties→General** tab→**Secret** button.
2. The **CHAP Secret Setup** screen appears. In the **Enter a secure secret** field, enter a secret code that includes 12 to 16 characters and click **OK**.

   NOTE: This Initiator CHAP secret and the Target CHAP secret must be different.
3. Before you can log on to Target, you must set the Initiator CHAP secret in Target. Therefore, you must complete Target settings and then log on to the iSCSI Initiator.

Target Settings

Configure the Target settings of CHAP as described in "iSCSI Target settings" on page 52 and perform the following steps:

1. In the **<Target Name> Properties** window, select the **Authentication** tab.
2. Select the check box for **Enable reverse CHAP authentication**. In the **User name** field, enter the IQN of the Initiator.
3. In the **Reverse secret** field enter the **Secret** value that you set in the Initiator.

   NOTE: Ensure that the Reverse secret is not the same as the CHAP secret. The Reverse secret must contain 12 to 16 characters.

Initiator Settings Continued

1. Configure the Initiator settings for CHAP as described in "iSCSI Initiator Settings" on page 53.
2. In the **Advanced Settings** window→select **CHAP logon information**→ enter the **User name** and **Target secret**. Select the check box for **Perform mutual authentication** and click **OK**.

   You can log in only if you have credentials that you entered for the Target and Initiator.

A

Appendix

The previous chapters in this document describe the procedures for basic iSCSI session/connection information. This chapter briefly describes procedures for a few advanced configuration settings. The following topics are discussed:

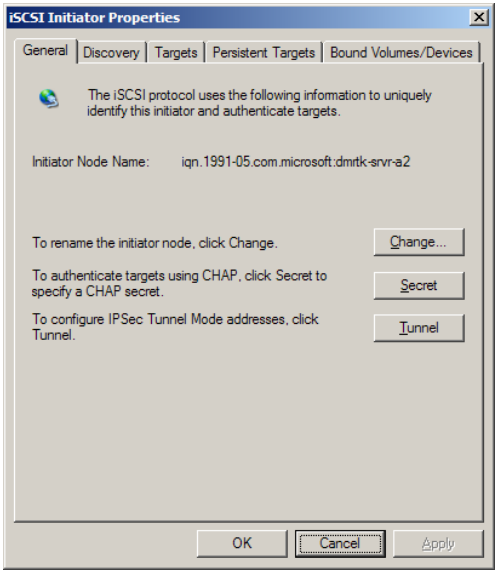
Initiator Details

This section describes the various functionality included in the **iSCSI Initiator Properties** window.

General Tab

The **General** tab displays the Initiator node name which is the Initiator's iSCSI Qualified Name (IQN).

Figure A-1. General Tab in iSCSI Initiator Properties Window



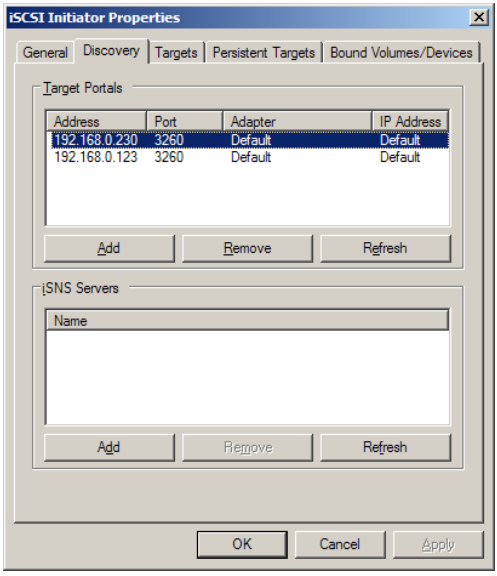
The **General** tab includes three options namely—**Change**, **Secret** and **Tunnel**.

- Change—Allows you to rename the Initiator node name that is displayed.
- Secret—iSCSI security provided CHAP. For more information, see "Configuring Secured iSCSI Connections Using Challenge-Handshake Authentication Protocol" on page 51.
- Tunnel—You can use this option for advanced configuration using IPsec. For more information, see "Appendix" on page 55.

Discovery Tab

Target Portals—The **Discovery** tab provides the list of discovered iSCSI Target portals available to this Initiator. The Target portal is the primary IP address of the iSCSI Target solution. Provide the dedicated iSCSI NIC IP address of the solution for PowerVault NX1950 storage solution. If no Target portals are listed, you can add them using the IP address or DNS name of the Target server. In the following example, two iSCSI Target portals are already added.

Figure A-2. Discovery Tab in iSCSI Initiator Properties Window



NOTE: If you are using the PowerVault NX1950 cluster solution configured with Target 3.0 iSCSI Target software, you must add a virtual iSCSI IP that is part of the Cluster Resource in the **Target Portals** field. This IP address must be a virtual IP address in the same subnet where iSCSI NICs are configured. This ensures proper connection between Initiator and Targets during cluster node failover or during Cluster Group move among different nodes of cluster. This configuration also ensures that iSCSI I/O traffic is not transmitted on the public network.

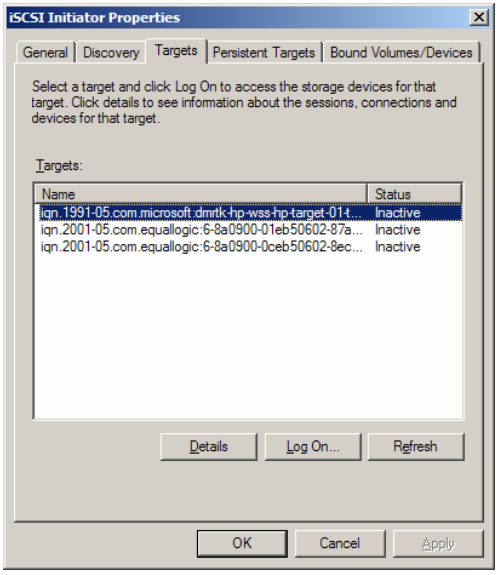
NOTE: If you are using PowerVault NX1950 cluster solution configured with 3.1 iSCSI Target software, you must create at least one iSCSI HA instance on each node and use the IP address of the iSCSI HA instance for iSCSI traffic. This ensures Active/Active Initiator-Target connection (connection with targets created on all nodes of cluster) and high-availability. If one node fails, the surviving node or the node that owns the cluster group takes over and owns all iSCSI Targets (targets of its own and targets of failed node) and the iSCSI I/O operations.

iSNS Servers—You can also perform Target discovery using iSNS servers. Add the iSNS Server IP address or DNS name. If the iSNS service is up and running on a server, all clients (Initiators and Targets) that are registered with the iSNS server are listed in the **Registered Clients** screen. To retrieve this information on the iSNS server, go to **Microsoft iSNS properties→Registered Clients**.

Targets Tab

The **Targets** tab provides the list of individual Targets available to the iSCSI Initiator. In the following example, three Targets are available to the iSCSI Initiator.

Figure A-3. Targets Tab in iSCSI Initiator Properties Window



NOTE: The above illustration is an example of discovery in the **Targets** tab. In practice, the targets are discovered only after you configure the PowerVault NX1950 storage/cluster system as a Target.

Log On—To gain access to the Target, the Initiator must **Log On** to the Target. If only one path is available to the Target, only one step is required for **log on**. Click **Log On..**, specify the **Target name**, and then click **OK**.

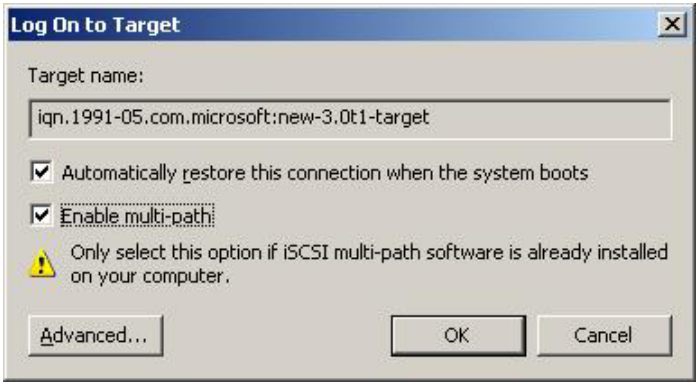
If multiple-paths to the Target are available, then you must describe each path to the iSCSI Initiator. To describe multiple paths to the Initiator:

1. In the **Log On** window, select **Enable multi-path** and select **Advanced**.

   The **Advanced** option provides a drop-down menu with all possible source (Initiator) IP addresses and a separate drop-down menu for all possible Target portal addresses. In this scenario, the Target solution manages the actual paths and IP addresses internally. Other Target solutions display each available IP address that can be used for multi-path operations.

2. Select each desired combination of source IP address and Target IP address and login separately to have multiple sessions for the same Target device.
3. Select **Automatically restore this connection when the system boots** to ensure continuous connection and to avoid establishment of Target-Initiator association during power spike or system reboots.
4. Repeat the **Log on** process for each iSCSI NIC.

Figure A-4. Log On to Target Window



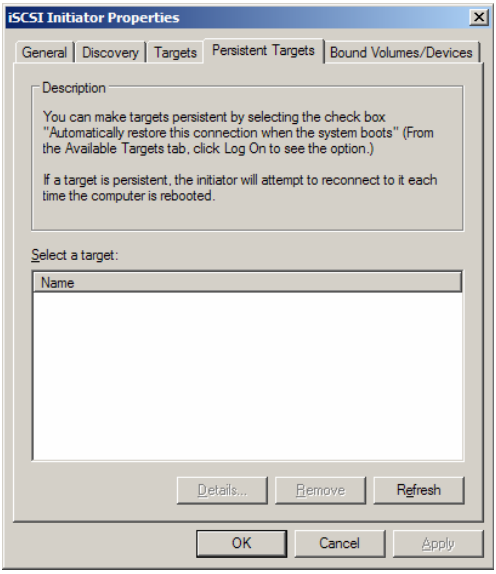
For MPIO connection, you must select the Target that displays status as **Connected** and select **Log On**. In the **Log On to Target** window, select **Advanced** and configure redundant iSCSI Target IP address.

NOTE: MPIO connections are not supported with the PowerVault NX1950 cluster solution configured with 3.0 iSCSI Target. MPIO connections are supported with PowerVault NX1950 cluster solution configured with 3.1 iSCSI Target and Microsoft iSCSI Initiator version 2.06 or later.

Persistent Targets Tab

You can configure Persistent Targets so that the connection to the Target is automatically restored when the system reboots. If the Targets are configured to be persistent, they appear in this **Persistent Targets** tab.

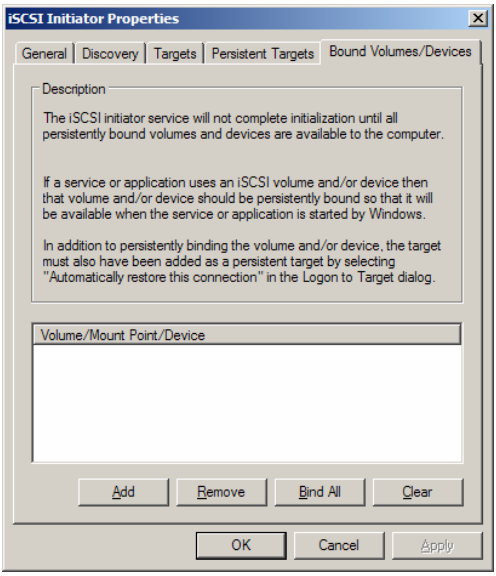
Figure A-5. Persistent Targets Tab in iSCSI Initiator Properties Window



Bound Volumes/Devices Tab

If a host service or application depends on the availability of an iSCSI volume, you must configure it as **bound** so that the iSCSI service includes each **bound** volume as part of its initialization.

Figure A-6. Bound Volumes/Devices Tab in iSCSI Initiator Properties Window



Advanced Configuration Details

Enabling Multi-Path on the Initiator

After you establish the iSCSI Initiator-Target connection, perform the following steps to enable multi-path operation:

1. On the Initiator, go to **iSCSI Initiator Properties→Targets** tab→**Log On...→Log On to Target** window and select the check box for **Enable multi-path** option.
2. You must configure multiple NIC ports for iSCSI operation for efficient block (iSCSI) I/O operations and for provisioning link failover. Multi-path option also enables multiple connections for the same iSCSI Targets using different IP addresses.

Using the Advanced Option

You can use the Advanced option to perform the following functions:

- Go to **iSCSI Initiator Properties**→**Targets** tab→**LogOn...**→**Log On to Target** window→**Advanced** option. The **Advanced Settings** screen appears and consists of two tabs namely—**Advanced** and **IPSec**. The **General** tab allows you to set CRC/Checksum, CHAP and choose source IP address and Target Portal—IP address of iSCSI Target. You can use the Multi-path option to configure load balancing and failover settings.
- In the **Advanced Settings** window, the **Advanced** tab provides a drop-down menu for all the source (Initiator) IP addresses and a drop-down menu for all Target portal addresses. In an iSCSI Initiator-Target connection, the Target solution manages the actual paths and IP addresses internally. If you are using different Target solutions, you can choose the IP address for multi-path operations from the list.
  - **a** Log on and select the combination of source IP address and Target IP address.
  - **b** Log in separately to configure multiple connections for the same Target device.
- In the **Advanced Settings** window, the **IPSec** tab allows you to configure IPSec settings. If you enable IPSec, all IP packets sent during data transfers are encrypted and authenticated. A common key is set on all IP portals, allowing all peers to authenticate each other and negotiate packet encryption.

Verifying the Properties of the Targets That are Connected

Go to **iSCSI Initiator Properties**→**Targets**→highlight the Target that is **Connected** and click **Details**. The **Target properties** screen is displayed and consists of three tabs namely—**Sessions**, **Devices**, and **Properties**. The following sections provide more details about these tabs.

Sessions Tab

The **Sessions** tab provides information about the **Session Identifier**, **Session properties**, and **Sessions Connections**. This tab allows you to Log off sessions. Click **Connections** to launch the **Session Connections** screen and configure the Load Balance Policy. For more information, see "Load Balance Policy" on page 63.

Devices Tab

The **Devices** tab of **Target Properties** screen provides generic device details like the Virtual Disks that are associated with Target.

Click **Advanced** to view information about MPIO and Launch the **Device Details** screen. To modify the MPIO settings, you can use the **MPIO** tab.

Properties Tab

The **Properties** tab of **Target Properties** screen provides information about Target Alias, Authentication, Associated Network portals and other details of the Target.

Load Balance Policy

To set different load balancing policies, perform the following steps after you have established the Initiator-Target Connection:

1. Go to **iSCSI Initiator properties→Targets** tab and select the Target that is Connected→**Details→Target Properties→Sessions** tab→**Connections**.
2. The **Session Connections** screen appears and displays the load balancing policy details. The default option is **Round Robin**. You can select the required option from the **Load Balance Policy** drop-down menu to configure the Load Balance Policy. Click **Apply**.

You can configure Load balancing for each connection from the different Load Balance Policy options that are available. When you select each policy in the **Load Balance Policy** field of the **Connections** tab, the following descriptions are displayed on the screen.

- **Fail Over Policy**—`The fail over policy employs one active path and designates all other paths as standby. The standby paths will be tried on a round-robin approach upon failure of the active path until an available path is found`.
- **Round Robin**—`The round robin policy attempts to evenly distribute incoming requests to all possible paths`.

- Round Robin With Subset—The round robin subset policy executes the round robin policy only on paths designated as active. The stand-by paths will be tried on a round-robin approach upon failure of all active paths.
- Least Queue Depth—The least queue depth policy compensates for uneven loads by distributing propeortiaonately more I/O requests to lightly loaded processing paths.
- Weighted Paths—The weighted paths policy allows the user to specify the relative processing load of each path. A large number means that the path priority is low.

Installing and Configuring iSNS server

The Microsoft iSNS Server is a free download from the Microsoft website at **www.microsoft.com** and is available in two versions namely—x86 and IA64. You can use the iSNS Sever for Target discovery on an iSCSI network.

iSNS Server is supported on the Microsoft Windows 2000 Server Service Pack 4 and Microsoft Windows Server 2003 operating systems. Perform the following steps to install the iSNS server:

NOTE: Do not install iSNS server on the same server that is running Microsoft iSCSI Initiator.

1. Install Microsoft iSNS Server version 3.0. The Installation process is simple and is wizard-based. In the **Welcome to the Microsoft iSNS Server Setup Wizard** screen, click **Next**.
2. The **License Agreement** screen appears. Read the information and click **Next**.
3. The **Select Installation Folder** appears. Enter the folder path or choose a location on your local drive using the **Browse** option and click **Next**.
4. In the **Confirm Installation** screen, click **Next**.
5. The **Installing Microsoft iSNS Server** screen indicates the installation progress. The **Microsoft iSNS Installation Program** prompts you to choose from the **iSNS Installation Options**. Choose **Install iSNS Service** and click **OK**.

6 The **End User License Agreement** screen appears. Read the agreement and click **Agree** to install the program.

7 The **Microsoft iSNS Service Setup Program** windows indicates that the program is installed successfully.

8 The **Microsoft iSNS Server Information** screen appears. Read the information and click **Next**.

9 The **Installation Complete** screen appears indicating the completion of program installation. Click **Close**.

Configuring the iSNS Server

iSNS Server performs the automatic discovery of iSCSI Initiators and Targets; after you register them with iSNS Server.

- The Initiators that are registered with iSNS servers can view all Target devices that are registered with iSNS in the **Targets** tab and logon to the Targets. You do not have to configure Initiators with the IP address or DNS name of individual Target servers in **Target Portals**. iSNS server performs Target Discovery.
- Similarly, PowerVault NX1950 storage system (Target) can query the available Initiators from iSNS server for association.

NOTE: In PowerVault NX1950 storage solution, the 3.0 iSCSI Software Target does not query the iSNS server for registered iSCSI Initiators, during Target creation. You have to enter the IQN name of the Initiator manually. After you create the Target, the Target IQN is listed in iSNS Server registered device list and can be accessed by Initiators that were added during Target creation. This issue is resolved in the 3.1 iSCSI Target.

To configure the iSNS Server, perform the following steps.

1. Log on to the server where you have installed the iSNS Server 3.0 and go to **Start→Programs→Microsoft iSNS Server→Configure iSNS server**.

   The iSNS Server screen consists of three tabs namely—**General**, **Discovery Domains**, and **Discovery Domain Sets**. The **General** tab lists all devices (iSCSI Initiators and Targets) that are registered with the iSNS Server. Perform the following procedure to add Targets and Initiators to the iSNS Server:

   a. Go to the **iSCSI Initiator properties→Discovery→iSNS Servers→Add** and add the IP address or DNS name of the Initiator and register this Initiator to the iSNS server.

   b. Log in to the iSNS server and go to **Start→Programs→Microsoft iSNS Server→Configure iSNS server→General** tab. The Initiator that you registered with iSNS Server in step a is listed. Similarly all iSCSI Initiators that you register with iSNS Server are listed in the **General** tab.

   c. Log in to the PowerVault NX1950 storage solution that you configured as a Target and go to **PowerVault NX1950 Management Console→ Microsoft iSCSI Software Target→**right-click and select **Properties→ iSNS** tab and add iSNS server IP address or DNS name.

   d. To verify, log in to the iSNS Server and check the **General** tab to ensure that all Targets of PowerVault NX1950 storage solution are listed.

   If multiple PowerVault NX1950 storage systems are registered with iSNS server, then all Target Devices that are created in the PowerVault NX1950 storage systems are listed in iSNS server.

2. You can use the **Discovery Domains** feature to group certain Initiators with Targets with specific access:

   a. Go to **iSNS Server Properties→Discovery Domains** tab→click **Create**→enter a name for the Discovery domain→select **Add**.

   b. The **Add registered Initiator or Target to Discovery Domain** screen appears. Select the specific Initiators and Targets that you want to configure and click **OK**.

3. You can configure multiple Discovery Domains in the iSCSI network. The domains are listed in the **Discovery Domain Sets** tab. The **Discovery Domain Sets** tab displays Default DD and Default DDS options. You can create any number of groups as required.

Best Practices for Efficient Storage Management

Storage Manager for SANs

Storage Manager for SANs is a Microsoft Management Console snap-in that system administrators can use to create and manage the logical unit numbers (LUNs) that are used to allocate space on storage arrays in both Fibre Channel and iSCSI environments. Storage Manager for SANs is deployed through a conventional snap-in and can be used on storage area network (SAN) based storage arrays that support Virtual Disk Server (VDS) using a hardware VDS provider. Due to hardware, protocol, transport layer and security differences, configuration and LUN management differ for the two types (iSCSI and Fibre Channel) of supported environments. This feature works with any type of Host Bus Adapter (HBA) or switches on the SAN. For a list of VDS providers that have passed the Hardware Compatibility Tests (HCT), see the Microsoft storage website on **www.microsoft.com/storage**.

LUN Management for iSCSI Subsystems

For iSCSI, a LUN is assigned to a Target—a logical entity that contains one or more LUNs. A server accesses the LUN by logging on to the Target using the server's iSCSI Initiator. To log on to a Target, the Initiator connects to portals on the Target; a subsystem has one or more portals, which are associated with Targets. If a server's Initiator is logged on to a Target, and a new LUN is assigned to the Target, the server can immediately access the LUN.

Securing data on an iSCSI SAN—To help secure data transfers between the server and the subsystem, configure security for the login sessions between Initiators and Targets. Using Storage Manager for SANs, you can configure one-way or mutual Challenge Handshake Authentication Protocol (CHAP) authentication between the Initiator and Targets, and you can also configure Internet Protocol security (IPsec) data encryption.

NOTE: It is recommended that you use CHAP if the iSCSI traffic uses the public network.

Related Links

For more information on storage for Microsoft Windows Storage Server 2003 operating systems and iSCSI in particular, see the following websites:

- Microsoft Storage website at **http://www.microsoft.com/storage/**
- Microsoft iSCSI Storage website at **http://www.microsoft.com/WindowsServer2003/technologies/storage/iscsi/default.mspx**
- Microsoft Windows Storage Server website at **http://www.microsoft.com/windowsserversystem/wss2003/default.mspx**
- Microsoft Windows Unified Data Storage Server 2003 at **http://www.microsoft.com/windowsserversystem/storage/wudss.mspx**
- Microsoft Storage Technical Articles and White Papers at **http://www.microsoft.com/windowsserversystem/storage/indextecharticle.mspx**
- Microsoft Scalable Networking Pack website at **http://www.microsoft.com/technet/network/snp/default.mspx**
- Microsoft Cluster Server website at **http://www.microsoft.com/windowsserver2003/technologies/clustering/default.mspx**

Index

Numerics

C

I

M

V