

Dell™ PowerVault™ NF500/NF600  
Systems

# End-to-End Deployment Guide for iSCSI

# Notes and Notices



**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.

---

**Information in this document is subject to change without notice.**

**© 2007 Dell Inc. All rights reserved.**

Reproduction in any manner whatsoever without the written permission of Dell Inc. is strictly forbidden.

Trademarks used in this text: *Dell*, the *DELL* logo, *PowerEdge*, *PowerVault*, and *OpenManage* are trademarks of Dell Inc.; *AMD64* is a trademark of Advanced Micro Devices; *Intel* is a registered trademark of Intel Corporation; *Microsoft* and *Windows*, and *Windows Server* are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries.

Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Dell Inc. disclaims any proprietary interest in trademarks and trade names other than its own.

# Contents

1	Introduction . . . . .	5
	<b>Terminology . . . . .</b>	<b>6</b>
	iSCSI . . . . .	6
	iSNS. . . . .	6
	Naming Convention. . . . .	7
	<b>Features of iSCSI Software Target . . . . .</b>	<b>7</b>
	Virtual Disk Storage . . . . .	7
	Snapshots. . . . .	7
	Wizards . . . . .	8
	<b>Quick Install Steps for Initiator-Target Connection. . . . .</b>	<b>8</b>
	Method 1 (Discovery Using Target Portals) . . . . .	8
	Setting Up the PowerVault 500/PowerVault 600 Storage System as Target . . . . .	9
	Method 2 (Discovery Using iSNS Server) . . . . .	13
2	Detailed End-to-End iSCSI Setup . . . . .	15
	<b>Configuring iSCSI Devices . . . . .</b>	<b>15</b>
	Installing Microsoft iSCSI Initiator . . . . .	15
	Configuring the Microsoft iSCSI Initiator. . . . .	16
	<b>Configuring Microsoft iSCSI Software Target . . . . .</b>	<b>22</b>
	Configuring the Target . . . . .	23
	<b>Establishing Connections . . . . .</b>	<b>27</b>
	Pre-Requisites . . . . .	27

3	Configuring Secured iSCSI Connections Using Challenge-Handshake Authentication Protocol . . . . .	31
	<b>CHAP vs IPsec</b> . . . . .	31
	<b>One-Way CHAP Authentication</b> . . . . .	32
	iSCSI Target Settings . . . . .	32
	iSCSI Initiator Settings . . . . .	33
	<b>Mutual CHAP Authentication</b> . . . . .	33
	Initiator Settings . . . . .	33
	Target Settings . . . . .	34
	Initiator Settings Continued. . . . .	34
A	Appendix . . . . .	35
	<b>Advanced Configuration Details</b> . . . . .	35
	Enabling Multi-Path on the Initiator . . . . .	35
	Using the Advanced Option. . . . .	36
	Verifying the Properties of the Targets That are Connected. . . . .	36
	Load Balance Policy . . . . .	37
	<b>Installing and Configuring iSNS server</b> . . . . .	38
	Configuring the iSNS Server . . . . .	39
	<b>Best Practices for Efficient Storage Management</b> . . . . .	41
	Storage Manager for SANs. . . . .	41
	LUN Management for iSCSI Subsystems. . . . .	41
	<b>Related Links</b> . . . . .	42
	Index . . . . .	43

# Introduction

This document provides information about configuring the Dell™ PowerVault™ 500 or PowerVault 600 storage system as an Internet Small Computer System Interface (iSCSI) Software Target. This document also provides information on setting up the PowerVault 500 or PowerVault 600 storage system that has been configured as iSCSI Target as a block storage device.



**NOTE:** The term Dell PowerVault 500 refers to the hardware platform. PowerVault NF500 refers to the configuration of PowerVault 500 storage system and Microsoft® Windows® Storage Server 2003 R2 with SP2 operating system. The term Dell PowerVault 600 refers to the hardware platform. PowerVault NF600 refers to the configuration of PowerVault 600 storage system and Microsoft Windows Storage Server 2003 R2 with SP2 operating system.

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 further sections:

- Quick install steps—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:** Throughout this document the iSCSI Initiator is referred to as the *Initiator* and the iSCSI Software Target is referred to as the *Target*. The iSCSI Target feature is supported only on systems running the Microsoft Windows Storage Server R2 with SP2 Standard and Enterprise Editions.

## Terminology

### 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 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 Microsoft Windows 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 website at [www.microsoft.com](http://www.microsoft.com) on a separate server that does not have Microsoft iSCSI Initiator or Target installed.

## **Naming Convention**

The term Dell PowerVault 500 refers to the hardware platform. PowerVault NF500 refers to the configuration of PowerVault 500 storage system and Microsoft Windows Storage Server 2003 R2 with SP2 operating system.

The term Dell PowerVault 600 refers to the hardware platform. PowerVault NF600 refers to the configuration of PowerVault 600 storage system and Microsoft Windows Storage Server 2003 R2 with SP2 operating system.

## **Features of iSCSI Software Target**

### **Virtual Disk Storage**

The disks you create using iSCSI Software Target are iSCSI Virtual Disks, which are files in the virtual hard disk (VHD) format. These Virtual Disks offer flexible and effective storage. They are dynamically extendable to provide extra capacity on demand, enable efficient storage utilization, and minimize the time required to create new disks and the down time typically required to install new disks.

### **Snapshots**

To facilitate backup and recovery operations, you can schedule and create snapshots of iSCSI Virtual Disks. A snapshot is a point-in-time, read-only copy of an iSCSI Virtual Disk. Snapshots are typically used as interim copies of data that has been modified since the most recent backup. Snapshots offer the following advantages:

- Snapshots can be scheduled to be created automatically.
- Snapshots are space-efficient because they are differential copies.
- It is not necessary to close files or stop programs when creating snapshots, so application servers can continue servicing clients without disruption.
- Each snapshot is typically created in less than one minute, regardless of the amount of data.

- Snapshots are useful for fast system recovery of files and volumes, in case of accidental data deletion by a user, overwritten data, or data corruption resulting from a malicious program.
- Snapshots can be mounted locally or exported to facilitate backup and recovery operations.



**NOTE:** Snapshots are not an alternative to system/data backup.

## Wizards

To support creation and management of iSCSI Targets, Virtual Disks, and snapshots, the iSCSI Software Target console provides the following wizards:

- **Create iSCSI Target Wizard**—For more information, see "Creating the Target" on page 9.
- **Create Virtual Disk Wizard**—For more information, see "Creating a Virtual Disk" on page 11.

## Quick Install Steps for Initiator-Target Connection

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

- Operating iSCSI protocol
- Setting up iSCSI Initiator-Target connection
- Installing and setting up Microsoft iSCSI Initiator and Microsoft iSNS server

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. You can perform Target discovery by entering the IP address of one of the NICs of PowerVault 500/PowerVault 600 storage system 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 the Microsoft Support website at [support.microsoft.com](http://support.microsoft.com) and install the Initiator (Host).
- 2 Turn on the PowerVault 500/PowerVault 600 storage system. Create one or more volumes on the internal hard drives and use them for creating Virtual Disks for iSCSI Targets.
- 3 On the iSCSI Target, right-click **Microsoft iSCSI Software Target** and click **Properties**. If the system is configured with multiple NICs, select the NICs that are being used for iSCSI traffic in the **Network** tab and click **OK**.

## Configuring the Initiator (Host)

Configure the Microsoft iSCSI Initiator with the IP address of the Target server. 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 500/PowerVault 600 storage system that is configured for iSCSI traffic.
- 3 Click **Advanced** and select the following options:
  - **Local Adapter**—**Microsoft iSCSI Initiator**
  - **Source IP**—IP address of the host that is being used for iSCSI
- 4 Click **OK** and click **OK** again.



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

## Setting Up the PowerVault 500/PowerVault 600 Storage System as Target

### Creating the Target

- 1 Click **Programs**→**Administrative Tools**→**Microsoft iSCSI Software Target** to open the Microsoft iSCSI Software Target console.

- 2 In the **Microsoft iSCSI Software Target** console, right-click **iSCSI Target**, and then click **Create iSCSI Target**. The **Welcome to the Create iSCSI Target wizard** screen appears. Click **Next**.

The wizard guides you through the process of Target creation.

- 3 The **Create iSCSI Target wizard** displays the **iSCSI Target Identification** option. Enter a **Name and Description** (optional) for the **iSCSI Target**. Click **Next**.
- 4 The **iSCSI Initiators Identifiers** screen appears. Click **Browse** and select the **IQN** of the host that you are configuring the Initiator to connect to. The host **IQN** is listed only if Initiator configuration 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 5. For more information about the **Advanced** option, see step 6.

- 5 If you choose the **Browse** option, select the **IQN** identifier by performing the following steps:
  - a The **Add iSCSI Initiator** screen appears and the details for **iSCSI Initiator** list are displayed. You can type or select **iSCSI Initiator** from the list, enter the **iSCSI Initiator Name**, and click **OK**.
  - b The **IQN** identifier field in the **iSCSI Initiators Identifiers** screen is populated with the value you had entered or selected. Click **Next**.
- 6 If you choose the **Advanced** option, select the **IQN** identifier by performing the following steps:
  - a The **Advanced Identifiers** screen appears. Click **Add**.
  - b The **Add/Edit Identifier** appears and you are provided with four options, namely—**IQN**, **DNS Domain Name**, **IP address**, and **MAC Address** to add the **IQN** identifier. Choose any one of the four options.



**NOTE:** If you choose **MAC** address as the **IQN** identifier, ensure that you enter the **MAC** address in the same format that it is displayed. Each octet should be separated by a hyphen. For example, **00-08-74-4C-7F-1D**.

- c Enter the value or choose the value through the **Browse** option, and then click **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 click **OK**.
- e In the **iSCSI Initiator Identifiers** screen, the **IQN identifier** field is populated with appropriate information. Click **Advanced** to view alternate identifiers.
- f Click **Next**.

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

### **Verifying the Target Creation (Optional)**

- 1 Go to the **Microsoft iSCSI Software Target** console. The Target name that you entered in step 3 during the Target creation is displayed.
- 2 Right-click the Target name. The options **Create/Delete iSCSI Target**, **Create Virtual Disk**, **Add Existing Virtual Disk**, **Properties**, and **Help** appear.

### **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. Click **Next**.
- 2 To create a file, choose the **Browse** option, select a volume on the local hard disks and type a file name with an extension **.vhd**.  
For example, create **Z:\voll.vhd**, where **Z** is the created volume on the local drive and **voll.vhd** is the filename. Click **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 can 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 add additional Targets and 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**.

### **Verify Virtual Disk Creation (Optional)**

- 1 Go to the **Microsoft iSCSI Software Target console**→**Devices** option. The attributes of the newly created Virtual Disk like Index, Description, Size, Status and the Name of the iSCSI Target that accesses this device for iSCSI I/O operations are displayed.
- 2 Select the Virtual Disk to view the volume associated with it. All available volumes where additional Virtual Disks can be created are also listed.

### **Verify Target-Virtual Disk Association (Optional)**


Select the iSCSI Target you created. The Virtual Disk that is assigned to the Target is displayed in the middle pane. The attributes Virtual Disk Index ID, Name, Size, and LUN ID are also displayed.

### **Configuring the Initiator-Target Connection From Initiator Host**

To establish an iSCSI Initiator-Target connection, perform the following steps:

- 1 From the iSCSI Initiator host, go to **Start**→**Programs**→**Microsoft iSCSI Initiator**→**iSCSI Initiator Properties**→**Targets** tab. Refresh the screen. The PowerVault 500/PowerVault 600 storage system Target device that you created in "Creating the Target" on page 9 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. Click **Advanced**.

- 3 In **Advanced Settings** window, select **General** tab, and select the following options from drop-down menu and click **OK**.
    - Local adapter—Microsoft iSCSI Initiator
    - Source IP—One of the host IP addresses
    - Target Portal—iSCSI IP address of the PowerVault 500/PowerVault 600 storage system
  - 4 In the **Log On to Target** window, click **OK**.

The **Targets** tab displays the status of Target as **Connected**.
  - 5 To accomplish Multipathing, you can establish multiple sessions from the host to the same Target device using Microsoft MPIO. To enable multiple sessions:
    - a Go to the **Targets** tab and select the Target that is **Connected**.
    - b Perform step 1 to step 3 listed in "Targets Tab" on page 18.
    - c In the **Advanced Settings** window, configure the redundant host IP address and Target Portal as the iSCSI IP address of the PowerVault 500/PowerVault 600 storage system.
-  **NOTE:** You must select the option **Microsoft MPIO** during iSCSI Initiator software installation. Multiple connections per session (MC/S) is not supported on the PowerVault 500/PowerVault 600 storage system.
- 6 To initialize and configure the iSCSI device as local drive and perform iSCSI I/O operations, go to **Computer Management** → **Disk Management** option.

## Method 2 (Discovery Using iSNS Server)

This section describes the procedure for iSCSI Target discovery using the iSNS server.

### Pre-Requisites

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

- 1 Download the Microsoft iSCSI Initiator software from the Microsoft Support website at [support.microsoft.com](http://support.microsoft.com) and install the Initiator (Host).
- 2 Download the Microsoft iSNS Server software from the Microsoft Support website at [support.microsoft.com](http://support.microsoft.com) and install a Client/Server running Windows operating system.



**NOTE:** Do not install the iSNS Server software on Initiator (host) or Target (PowerVault500/PowerVault 600 storage system). Install the software on a separate Client/Server running Windows operating system.

- 3 Turn on the PowerVault 500/PowerVault 600 storage system.
- 4 Create one or more volumes on the local drives for creating Virtual Disks for iSCSI Targets.

### **From 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**.

### **Verifying the iSNS Server Settings (Optional)**

- 1 In the iSNS Server, go to **iSNS Server Properties**→ **General** tab. The Registered iSCSI Initiators and Targets list is displayed.
- 2 The iSCSI Initiator that you added is listed.

### **Setting Up the Target (PowerVault 500/PowerVault 600 Storage System)**

- 1 Go to the PowerVault 500/PowerVault 600 storage system. Select **Start**→ **Programs**→ **Administrative Tools**→ **Microsoft iSCSI Software Target** to open **Microsoft iSCSI Software Target** console. Select the iSCSI Target, right-click and select **Properties**.
- 2 In the **iSCSI Target Properties** window, go to the **iSNS** tab and add the iSNS server information (DNS Name or IP address).
- 3 Repeat step 2 to step 5 in the "Creating the Target" on page 9. When you use the **Browse** option, the iSCSI Initiator Identifier of all Initiators that are registered with iSNS server are listed.



**NOTE:** The iSCSI Target may cause errors when you query the iSNS server for Initiator discovery. This is a known issue and will be addressed in a future release.

# 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.

## Configuring iSCSI Devices

The following sections provide detailed information about installing and configuring the Initiator and Target in Dell™ PowerVault™ 500/PowerVault 600 storage system.

### Installing Microsoft iSCSI Initiator

You can download the Microsoft® iSCSI Initiator for free from the Microsoft website at [www.microsoft.com](http://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. iSCSI Initiator Version 2.05 and above is used on all hosts for this document. 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 a different version of iSCSI Initiator is used in 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](http://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 multipathing** is unchecked. You must select this option as all installations in this document use the 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).

- 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 completely. A command-line utility called iSCSICLI is also installed. You can use the iSCSICLI feature to control the iSCSI Initiator service and HBAs.

The release notes and user guide are saved onto the local host when the iSCSI Initiator package is extracted. Some of the restrictions listed here may change in future releases.

- Dynamic disks on an iSCSI session are not supported.
- The default iSCSI node name is generated from the Microsoft Windows<sup>®</sup> computer name. If the Windows computer name contains a character that would be invalid within an iSCSI node name, such as an \_ (underscore), then the Microsoft iSCSI Initiator service converts the invalid character to a - (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. It should be greater than 1 byte and less than or equal to 16 bytes if IPsec is being used.

## Configuring the Microsoft iSCSI Initiator

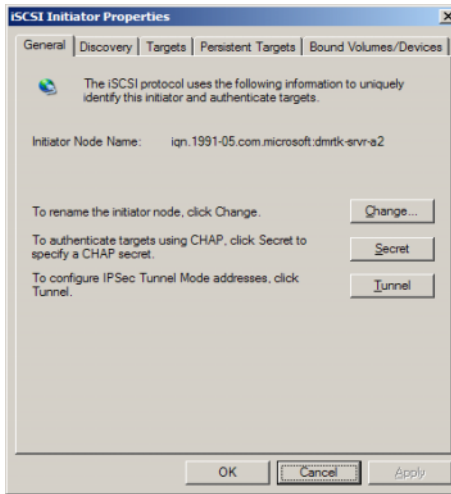
After the installation is complete, you can use the **iSCSI Initiator Properties** to manage the iSCSI environment. This section describes the various configuration options that are available.



## General Tab

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

**Figure 2-1. General Tab**



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.
- Tunnel—Allows you to perform advanced configuration using IPsec.

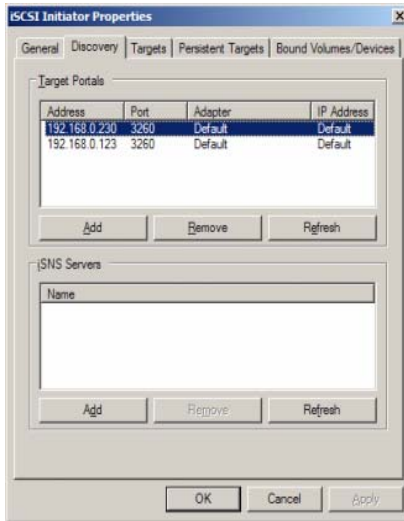
## Discovery Tab

The **Discovery** tab provides information about Target Portals and iSNS Servers.

- 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 500/PowerVault 600 storage

system. If no Target portals are listed, you can add them using the IP address or DNS name of Target server. In the following example, two iSCSI Target portals are already added.

**Figure 2-2. Discovery Tab**

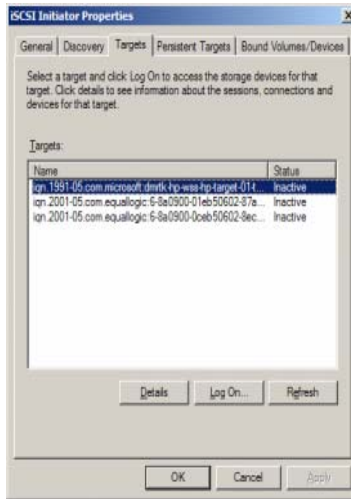


- iSNS Servers—You can also perform Target discovery using iSNS servers. Add the iSNS Server IP address or DNS name. If the iSNS service is up and running on a server, all clients (Initiators and Targets) that are registered with the iSNS server are listed in the **Registered Clients** screen. To retrieve 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 2-3. Targets Tab**



If you use the Direct Portals option the **Discovery** tab, the Targets of the IP address that you provided are listed. If you use the iSNS servers option in the **Discovery** tab, the Targets created in all PowerVault 500/PowerVault 600 storage systems that are registered with iSNS server are displayed.

**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:

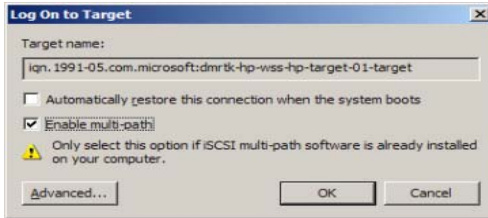
- 1 In the **Log On** window, select **Enable multi-path** and click **Advanced**.

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 2-4. Log On to Target Window**

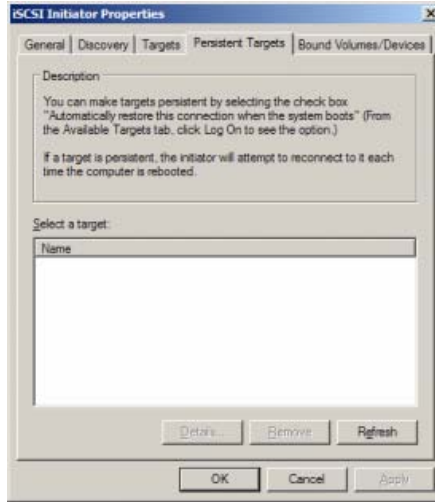


For MPIO connection, you must select the Target that displays status as Connected and select Log On. In the **Log On to Target** window, select **Advanced** and configure redundant iSCSI Target IP address.

### **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 2-5. Persistent Targets Tab**



### **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 2-6. Bound Volumes/Devices Tab**



## Configuring Microsoft iSCSI Software Target

The Microsoft iSCSI Software Target software package is available in the iSCSI software target application CD. Before configuring iSCSI Targets, you must create a few LUNs and reserve storage space to create Virtual Disks for iSCSI Targets. The following sections provide step-by-step instructions to create storage space.

## Configuring the Target

- 1 Configure Network Settings on the iSCSI Target device—The PowerVault 500/600 storage system is configured to use DHCP for network settings by default. The PowerVault 500/600 storage system is designed for multipath operations and is equipped with two RJ45 Ethernet connectors. You can add an optional additional NIC.

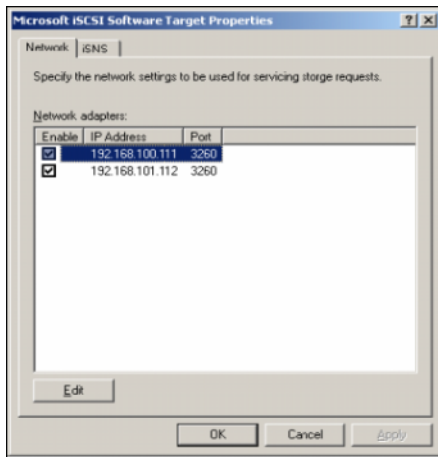


**NOTE:** It is recommended that you configure dedicated iSCSI NICs on separate subnets and not on the public network.

- 2 Create Volumes on the Internal Drives by performing the following:
  - a Use Dell OpenManage Server Administrator to create a Virtual Disk on the PowerVault 500/PowerVault 600 storage system local hard drive.
  - b Perform a quick format and assign a drive letter to the volume. This volume is now available and is listed in the **Disk Management** interface.
  - c You can then use the volume that you created to create a Virtual Disk for the iSCSI Target. For more information, see the *Dell OpenManage System Administrator User's Guide* located on the Dell Support website at [support.dell.com](http://support.dell.com).
- 3 Create iSCSI Targets—To Create iSCSI Targets you must configure dedicated iSCSI NICs for iSCSI traffic and then create iSCSI Targets. Follow the steps below to configure dedicated iSCSI NICs:
  - a Go to Microsoft iSCSI Software target Console→ iSCSI Target
  - 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 500/600 storage system are listed.
  - d Deselect the public and private network IP address from the list. Deselecting 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 that use two dedicated NICs for iSCSI traffic as shown in Figure 2-7. Each Target is made available to a different application on the host server. The Target in the Microsoft-based iSCSI Target solution only defines the path that the iSCSI storage traffic uses from the iSCSI Initiator.


**Figure 2-7. Microsoft iSCSI Software Target Properties**



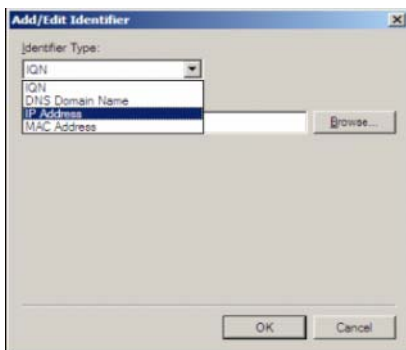
Follow the steps below to create iSCSI Targets:

- a** In the Microsoft iSCSI Software target Console, right-click iSCSI Target 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.  
The **iSCSI initiators identifiers** screen appears.



- d 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.
- 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 2-8 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:** iSCSI Initiators are identified by their IQN. You can enter the IQN, use Browse option, or the **Advanced** option and use the MAC Address, IP address, or DNS Domain name of the Initiator. The example in Figure 2-8 uses the IP address as the Identifier. You can use the **Advanced** option and repeat similar steps to add more identifiers.

**Figure 2-8. Add/Edit Identifier**



- e In the iSCSI Initiator identifiers screen, choose the identifier and click **Next**.
- f The **Completing the Create iSCSI Target Wizard** screen appears indicating that the iSCSI Target has been created.


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

- 4 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 Microsoft iSCSI Software Target 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.

## Establishing Connections

After you install and configure iSCSI Initiators and Targets, you must establish connections/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 15.
- Ensure that Target Portals information is added in **Microsoft iSCSI Initiator Properties**→ **Targets** tab.

Follow these steps to establish connections/sessions:

- 1 Log on to iSCSI Target device.
- 2 Go to **iSCSI Initiator Properties Wizard**→ **Targets** tab.

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

- 3 The **Log On to Target** screen appears. You can select the **Automatically restore this connection when the system reboots** option for continuous 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 the drop-down menu:
  - Local Adapter — Microsoft iSCSI Initiator
  - Source IP — one of the host IP addresses
  - Target Portal — iSCSI IP address of the PowerVault NF500/NF600 storage system.
- 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 35.
- 6 In the **Log On to Target** screen, click **OK**.  
The connection is established and the status is displayed as **Connected**.
- 7 To configure MPIO, 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 a different host.
- c In the **Advanced Settings** window, select the redundant iSCSI IP address of the PowerVault NF500/NF600 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.



**NOTE:** You can also configure load balancing and failover by using Microsoft MPIO support or Multiple Connections per Session (MC/S). Currently the PowerVault NF500/NF600 storage systems only supports the MPIO option. The MC/S option is not supported with PowerVault NF500/NF600 storage solution and PowerVault NF500/NF600 cluster systems.

- 8 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**.

- 9 In the right pane, the iSCSI disk that is **Connected** is displayed as **Unknown Not Initialized** and **Unallocated**.
- 10 The **Welcome to the Initialize and Convert Disk Wizard** option is displayed. 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**.
- 11 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 the 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.
- 12 Go to the **Disk Management**. The iSCSI disk is identified with the volume label you entered.

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



# 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™ NF500 and NF600 storage solutions also support Mutual CHAP.

CHAP is generally regarded as more secure than Password Authentication Protocol (PAP). For more information regarding CHAP and PAP, see the RFC 1334 website at <http://rfc.arogonet/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 **Microsoft iSCSI Software Target Console**→ **iSCSI Targets** → <Target name> and either right-click and select **Properties** or go to **Actions** pane→ **More Actions**→ **Properties**.  
The <**Target Name**> **Properties** window is displayed, 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 Log in to the Target on which you have enabled CHAP in "iSCSI Target Settings" on page 32 by clicking **iSCSI Initiator Properties**→ **Targets** tab→ **Log On**....
- 2 In the **Log On to Target** window, select **Advanced**.
- 3 In the **Advanced Settings** window, select the check box for **CHAP logon information**.

The **User name** field displays the **IQN** of the Initiator automatically.

- 4 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

- 1 Configure the Target settings of CHAP as described in "iSCSI Target Settings" on page 32 and perform the following steps:
    - a In the **<Target Name> Properties** window, select the **Authentication** tab.
    - b Select the check box for **Enable reverse CHAP authentication**. In the **User name** field, enter the IQN of the Initiator.
    - c 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 33.
- 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:

- "Advanced Configuration Details" on page 35
- "Installing and Configuring iSNS server" on page 38
- "Best Practices for Efficient Storage Management" on page 41
- "Related Links" on page 42

### 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 appears 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 37.

## Devices Tab

The **Devices** tab of **Target Properties** screen provides generic device details like the Virtual Disks that are associated with the 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 is populated with 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 proportionately 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](http://www.microsoft.com) and is available in two versions namely—x86 and IA64. You can use the iSNS Server 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** is displayed. 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, Dell™ PowerVault™ NF500/NF600 storage system (Target) can query the available Initiators from iSNS server for association.



**NOTE:** In PowerVault NF500/NF600 storage solution, the current version of 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.

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 NF500/NF600 storage system that you configured as a Target and go to **Microsoft iSCSI Software Target Console**→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 NF500/NF600 storage system are listed.

If multiple PowerVault NF500/NF600 storage systems are registered with iSNS server, then all Target Devices that are created in the PowerVault NF500/NF600 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](http://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.

## 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.aspx>
- Microsoft Windows Storage Server website at <http://www.microsoft.com/windowsserversystem/wss2003/default.aspx>
- Microsoft Storage Technical Articles and White Papers at <http://www.microsoft.com/windowsserversystem/storage/indextecharticle.aspx>
- Microsoft Scalable Networking Pack website at <http://www.microsoft.com/technet/network/snp/default.aspx>
- For information on CHAP and PAP, see the RFC1334 website at <http://rfc.arigo.net/rfc1334.html>.

# Index

## C

- CHAP, 31
  - Mutual CHAP, 33
  - One-Way CHAP, 32

## I

- iSCSI, 5
  - Configuring, 15
  - Configuring Target, 22

## L

- Load Balance Policy, 37

## M

- Multi-Path, 35

## P

- PowerVault 500, 7
- PowerVault 600, 7
- PowerVault NF500, 7
- PowerVault NF600, 7

## S

- Snapshots, 7
- Storage Manager for SANs, 41

## V

- Virtual Disk, 7, 11

## W

- Wizards, 8
  - Create iSCSI Target Wizard, 8
  - Create Virtual Disk Wizard, 8

