Dell PowerVault MD3200i and MD3220i Storage Arrays

Deployment Guide

Notes, Cautions, and Warnings

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

CAUTION: A CAUTION indicates potential damage to hardware or loss of data if instructions are not followed.

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

2011 - 09 **Rev. A01**

Contents

1

Introduction

This guide provides information about deploying Dell PowerVault MD MD3200i and Dell PowerVault MD3220i storage arrays. The deployment process includes:

- Hardware installation
- Modular Disk Storage Manager (MDSM) software installation
- Initial system configuration

Other information provided include system requirements, storage array organization, and utilities.

NOTE: For more information on product documentation see, support.dell.com/manuals.

MDSM enables an administrator to configure and monitor storage arrays for optimum usability. The version of MDSM included on the PowerVault MD series resource media can be used to manage both the PowerVault MD3200i series and the earlier PowerVault MD series storage arrays. MDSM is compatible with both Microsoft Windows and Linux operating systems.

System Requirements

Before installing and configuring the PowerVault MD3200i series hardware and software, ensure that the operating system is supported and minimum system requirements are met. For more information, see the *Dell PowerVault Support Matrix* available on support.dell.com/manuals.

Management Station Requirements

A management station uses MDSM to configure and manage storage arrays across the network. A management station must meet the following minimum system requirements:

- Intel Pentium or an equivalent processor (1333 MHz or faster) with 512 MB RAM (1024 MB recommended)
- 1 GB disk space

- Display resolution of 1024x768 with 16 million colors (1280x1024 32-bit recommended)
- Microsoft Windows, Red Hat Enterprise Linux, and SUSE Linux Enterprise Server.

  NOTE: Operating system installations can be either native or hypervisor guest configurations.

  NOTE: Supported hypervisors include Microsoft Hyper-V, Citrix XenServer, and VMware. For information about the supported versions, see the *Support Matrix* at **support.dell.com**.
- Administrator or equivalent permissions

Introduction to Storage Arrays

A storage array includes various hardware components, such as physical disks, RAID controller modules, fans, and power supplies, gathered into enclosures. An enclosure containing physical disks accessed through RAID controller modules is called a storage array.

One or more host servers attached to the storage array can access the data on the storage array. You can also establish multiple physical paths between the host(s) and the storage array so that loss of any single path (for example, through failure of a host server port) does not result in loss of access to data on the storage array.

The storage array is managed by MDSM running on a:

- Host server—On a host server, MDSM and the storage array communicate management requests and event information using iSCSI ports.
- Management station—On a management station, MDSM communicates with the storage array either through an Ethernet connection to the storage array management port or though an Ethernet connection to a host server. The Ethernet connection passes management information between the management station and the storage array using iSCSI ports.

Using MDSM, you can configure the physical disks in the storage array into logical components called disk groups and then divide the disk groups into virtual disks. Disk groups are created in the unconfigured capacity of a storage array. Virtual disks are created in the free capacity of a disk group.

Unconfigured capacity comprises of physical disks not already assigned to a disk group. When a virtual disk is created using unconfigured capacity, a disk group is automatically created. If the only virtual disk in a disk group is deleted, the disk group is also deleted. Free capacity is space in a disk group that is not assigned to any virtual disk.

Data is written to the physical disks in the storage array using RAID technology. RAID levels define the way in which data is written to physical disks. Different RAID levels offer different levels of accessibility, redundancy, and capacity. You can set a specified RAID level for each disk group and virtual disk on your storage array.

For more information about using RAID and managing data in your storage solution, see the *Owner's Manual* at support.dell.com/manuals.

2

Hardware Installation

Before using this guide, ensure that you review the instructions in the:

- *Getting Started Guide*—The *Getting Started Guide* that shipped with the storage array provides information to configure the initial setup of the system.
- Planning section of the *Owner's Manual*—The planing section provides information about important concepts you must know before setting up your storage solution. See the *Owner's Manual* at support.dell.com.

Planning the Storage Configuration

Consider the following before installing your storage array:

- Evaluate data storage needs and administrative requirements.
- Calculate availability requirements.
- Decide the frequency and level of backups, such as weekly full backups with daily partial backups.
- Consider storage array options, such as password protection and e-mail alert notifications for error conditions.
- Design the configuration of virtual disks and disk groups according to a data organization plan. For example, use one virtual disk for inventory, a second for financial and tax information, and a third for customer information.
- Decide whether to allow space for hot spares, which automatically replace failed physical disks.

Connecting the Storage Array

The storage array is connected to a host using two hot-swappable RAID controller modules. The RAID controller modules are identified as RAID controller module 0 and RAID controller module 1.

Each RAID controller module has four iSCSI In port connectors that provide Ethernet connections to the host server or switches. Each RAID controller module also contains an Ethernet management port and a SAS Out port. The Ethernet management port allows you to install a dedicated management station (server or stand-alone system). The SAS Out port allows you to connect the storage array to optional PowerVault MD1200 series expansion enclosures for additional storage capacity.

Each PowerVault MD3200i series storage array can be expanded to a maximum of 120 (or 192, if enabled using Premium Feature activation) physical disks through a maximum of seven PowerVault MD1200 series expansion enclosures.

Cabling the Storage Array

The iSCSI interface enables different host-to-controller configurations. The figures in this chapter are grouped according to the following categories:

- Direct-attached configurations (no Ethernet switches are used)
- Network-attached (SAN) configurations (Ethernet switches are used)

Redundant and Non-Redundant Configurations

Non-redundant configurations are configurations that provide only a single data path from a host to the storage array. This type of configuration is only recommended for non-critical data storage. Path failure from a failed or removed cable, a failed NIC, or a failed or removed RAID controller module results in loss of host access to storage on the storage array.

Redundancy is established by installing separate data paths between the host and the storage array, in which each path is to one of the two RAID controller modules installed in the storage array. Redundancy protects the host from losing access to data in the event of path failure, because both RAID controller modules can access all the disks in the storage array.

Direct-Attached Configurations

You can connect the Ethernet ports of the host servers directly to the storage array RAID controller module iSCSI ports.

Single Path Data Configurations

With a single path configuration, a group of heterogeneous hosts can be connected to the storage array through a single physical Ethernet port. Since there is only one port, there is no redundancy, although each iSCSI portal supports multiple connections. This configuration is supported for both single controller and dual controller modes.

Figure 2-1 shows a non-redundant cabling configuration to the RAID controller modules using a single path data configuration.

Figure 2-1. Four Hosts Connected to a Single Controller

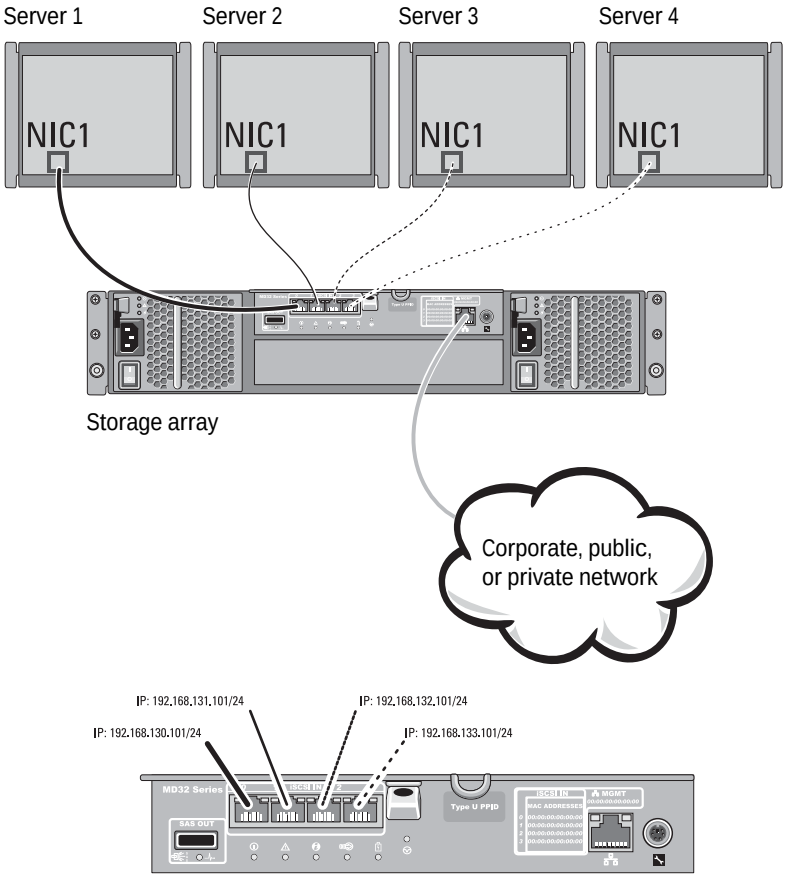


Figure 2-2 shows two hosts connected to a single controller array.

Figure 2-2. Two Hosts Connected to a Single Controller

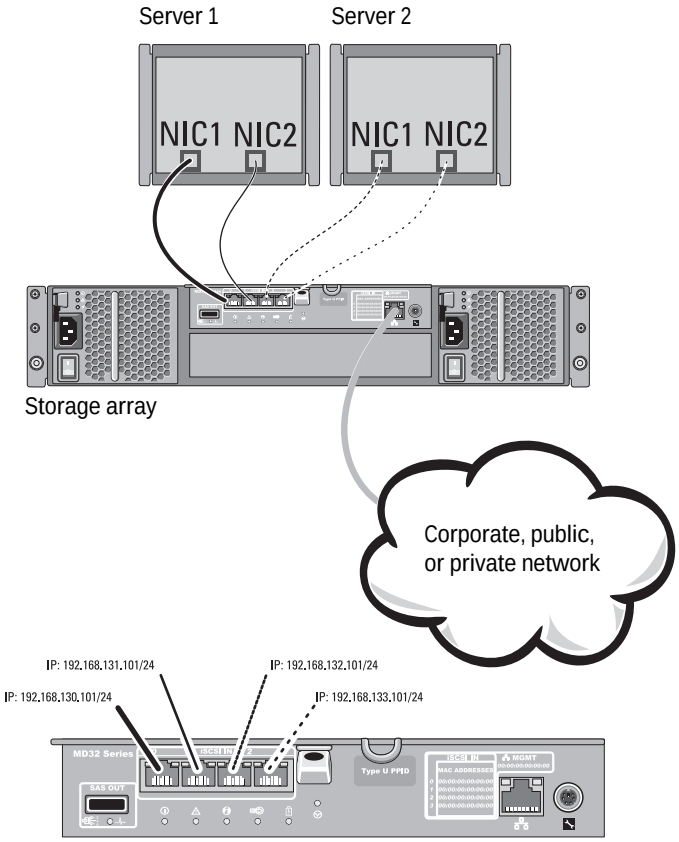
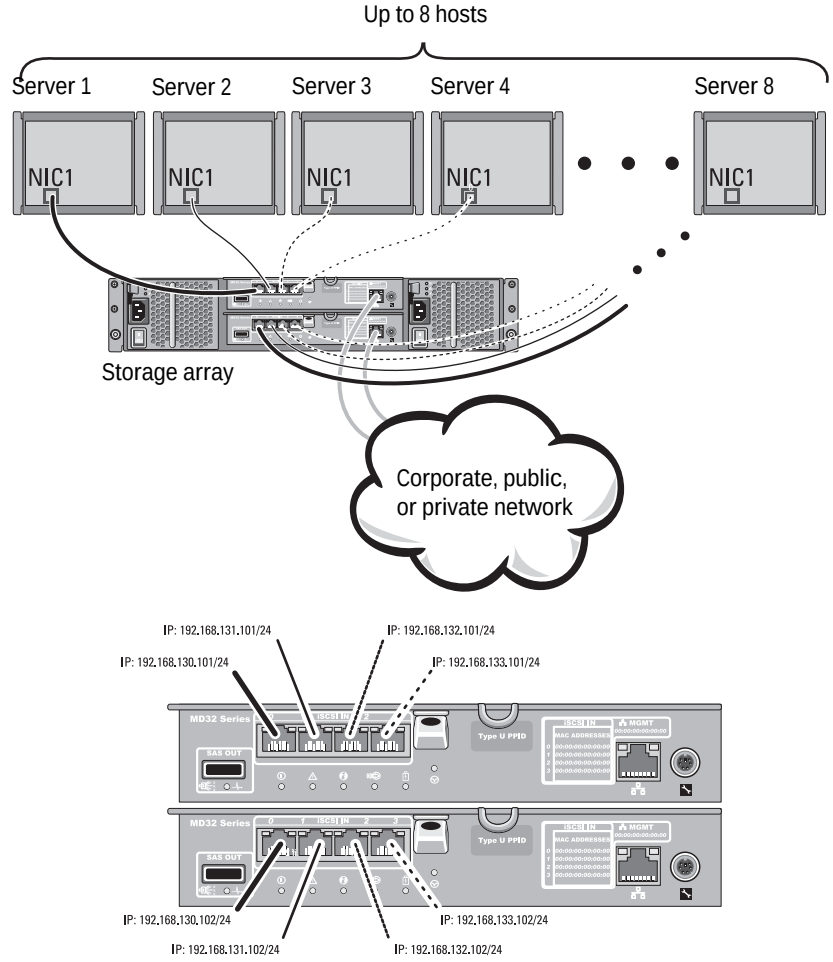


Figure 2-3 shows eight stand-alone hosts supported in a dual controller array configuration with a single data path.

Figure 2-3. Eight Hosts in a Dual-Controller Configuration

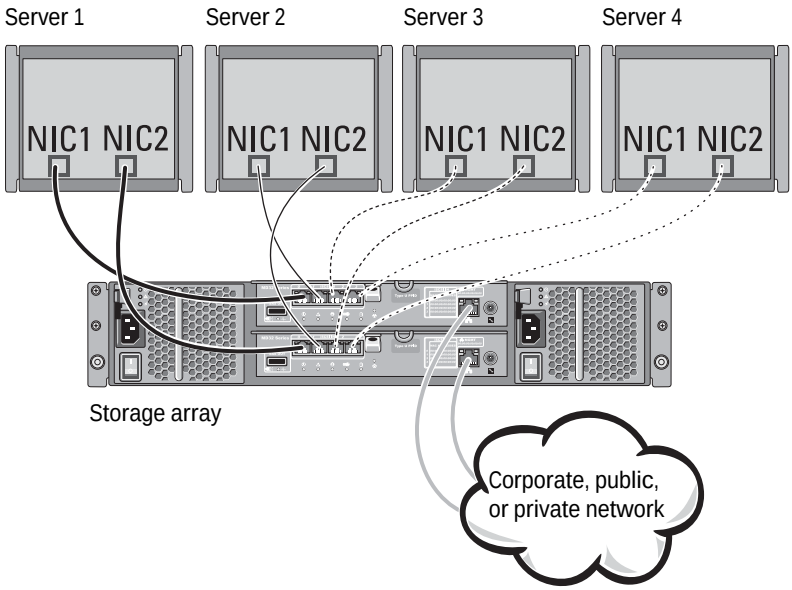


Dual-Path Data Configuration

In Figure 2-4, up to four servers are directly attached to the RAID controller modules. If the host server has a second Ethernet connection to the array, it can be attached to the iSCSI ports on the array's second controller. This configuration provides improved availability by allowing two separate physical paths for each host, which ensures full redundancy if one of the paths fail.

In Figure 2-5, up to four cluster nodes are directly attached to two RAID controller modules. Since each cluster node has redundant paths, loss of a single path would still allow access to the to the storage array through the alternate path.

Figure 2-4. Four Hosts Connected to Two Controllers



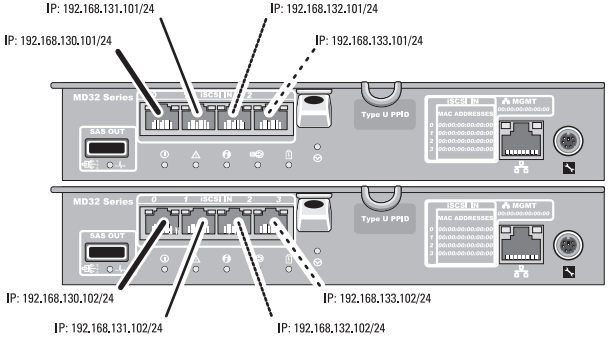
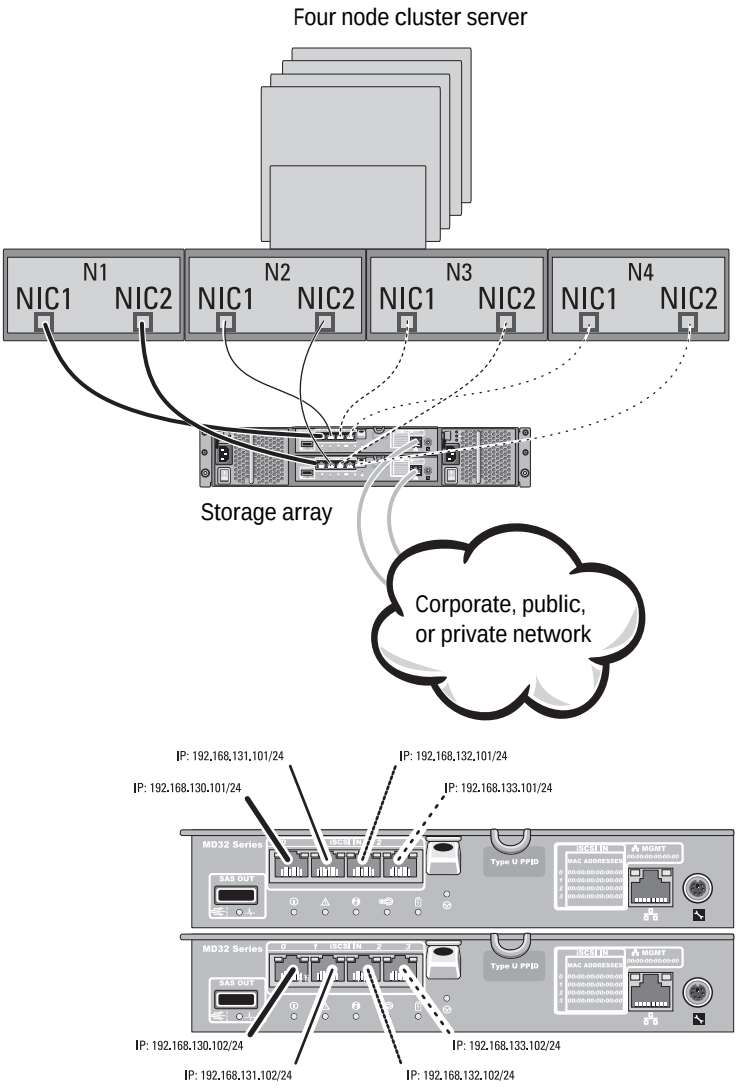


Figure 2-5. Four Hosts Connected in a Dual-Controller Configuration



Network-Attached Configurations

You can also cable the host servers to the RAID controller module iSCSI ports through industry-standard 1GB Ethernet switches. An iSCSI configuration that uses Ethernet switches is frequently referred to as an IP SAN. By using an IP SAN, the PowerVault MD3200i series storage array can support up to 64 hosts simultaneously. This configuration supports either single- or dual-path data configurations and either single or dual controller modules.

Figure 2-6 shows up to 64 stand-alone servers attached (using multiple sessions) to a single RAID controller module through a network. Hosts that have a second Ethernet connection to the network allow two separate physical paths for each host, which ensures full redundancy if one of the paths fail. Figure 2-7 shows how the same number of hosts can be similarly attached to a dual RAID controller module configuration.

Figure 2-6. 64 Servers Connected to a Single Controller

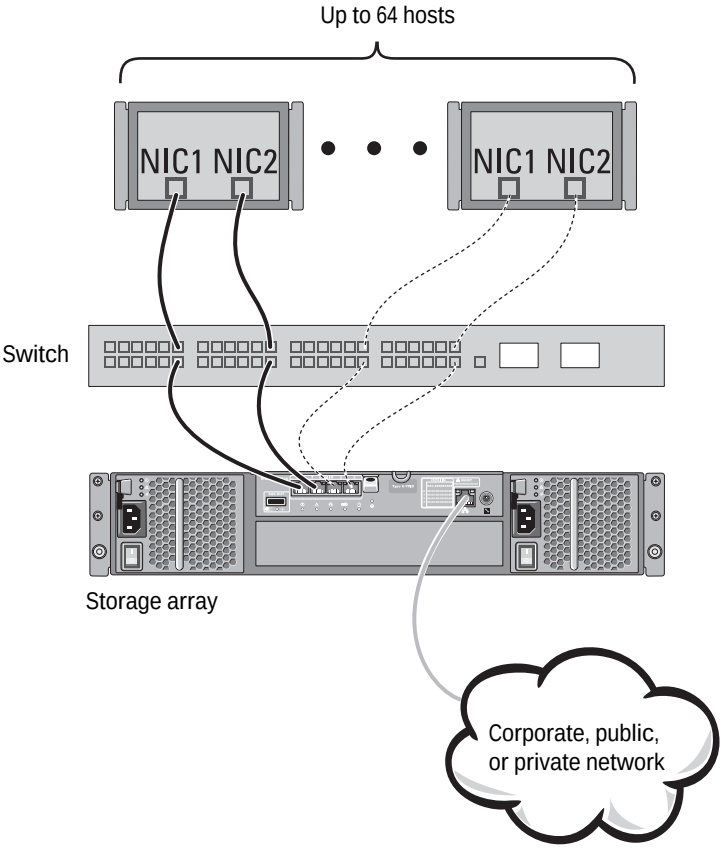
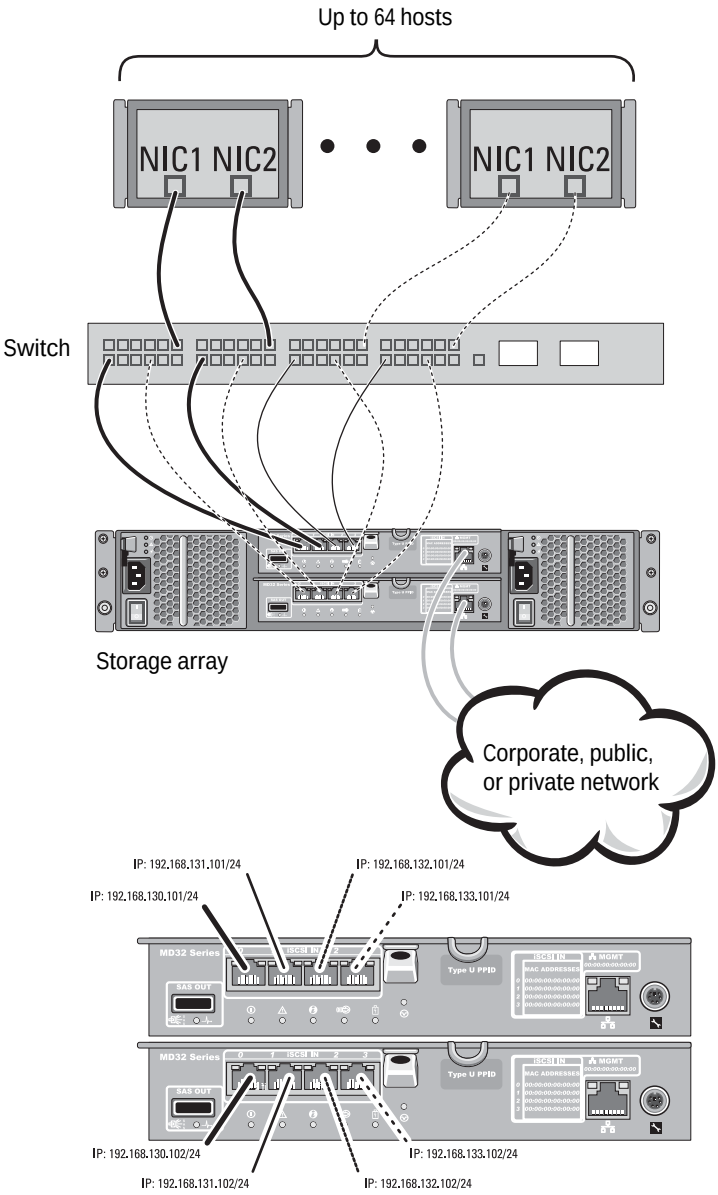


Figure 2-7. 64 Servers Connected to Two Controllers



Cabling PowerVault MD1200 Series Expansion Enclosures

You can expand the capacity of your PowerVault MD3200i series storage array by adding PowerVault MD1200 series expansion enclosures. You can expand the physical disk pool to a maximum of 120 (or 192, if enabled using Premium Feature activation) physical disks using a maximum of seven expansion enclosures.

Expanding With Previously Configured PowerVault MD1200 Series Expansion Enclosures

Use this procedure if your expansion enclosure is directly attached to and configured on a Dell PowerEdge RAID Controller (PERC)H800 adapter. Data from virtual disks created on a PERC H800 adapter cannot be directly migrated to a PowerVault MD3200i series storage array or to a PowerVault MD1200 series expansion enclosure connected to a PowerVault MD3200i series storage array.

CAUTION: If a PowerVault MD1200 series expansion enclosure that was previously attached to PERC H800 adapter is used as an expansion enclosure to a PowerVault MD3200i series storage array, the physical disks of the expansion enclosure are reinitialized and data is lost. You must backup all data on the expansion enclosure before attempting the expansion.

To attach previously configured PowerVault MD1200 series expansion enclosures to the PowerVault MD3200i series storage array:

1. Back up all data on the expansion enclosure(s).
2. While the enclosure is still attached to the PERC H800 controller, upgrade the expansion enclosure firmware to the latest version available at support.dell.com.

   Windows systems users can reference the DUP.exe package and Linux kernel users can reference the DUP.bin package.
3. Ensure that the storage array software is installed and up to date before adding the expansion enclosure(s).

   For more information, see the *Support Matrix* at support.dell.com/manuals.

a Install the software and driver package included on the PowerVault MD series resource media.

   For information about installing the software, see "Installing PowerVault MD Storage Software" on page 25.

b Update the storage array RAID controller module firmware and NVSRAM to the latest versions available at support.dell.com, using PowerVault MDSM.

c Click Tools→ Upgrade RAID Controller Module Firmware in the Enterprise Management Window (EMW).

4 Stop all I/O and turn off the system and attached units.

a Stop all I/O to the storage array and turn off the host systems attached to the storage array.

b Turn off the storage array.

c Turn off the expansion enclosure(s) in the affected system.

5 Cable the expansion enclosure(s) to the storage array.

6 Turn on attached units:

a Turn on the expansion enclosure(s). Wait for the enclosure status LED to turn blue.

b Turn on the storage array and wait for the status LED to indicate that the unit is ready:

- If the status LEDs are solid amber, the storage array is still coming online.
- If the status LEDs are blinking amber, there is an error that can be viewed using the PowerVault MDSM.
- If the status LEDs are solid blue, the storage array is ready.

c When the storage array is online and ready, turn on any attached host systems.

7 After the PowerVault MD1200 series expansion enclosure is configured as an expansion enclosure of the storage array, restore the data that was backed up in step 1.

After the expansion enclosures are online, they can be accessed as a part of the storage array.

Expanding With New PowerVault MD1200 Series Expansion Enclosures

Perform the following steps to attach new PowerVault MD1200 series expansion enclosures to a PowerVault MD3200i series storage array:

1. Before adding the expansion enclosure(s), ensure that the storage array software is installed and up to date. For more information, see the *Support Matrix* at support.dell.com/manuals.

   a. Install the software and driver package included on the PowerVault MD series resource media.

      For information about installing the software, see "The PowerVault MD series storage software installer provides features that include the core software, providers, and optional utilities. The core software feature includes the host-based storage agent, multipath driver, and MD Storage Manager (MDSM) application used to configure, manage, and monitor the storage array solution. The providers feature includes providers for the Microsoft Virtual Disk Service (VDS) and Microsoft Volume Shadow-Copy Service (VSS) framework. The PowerVault Modular Disk Configuration Utility (MDCU) is an optional utility that provides a consolidated approach for configuring the management ports, iSCSI host ports, and creating sessions for the iSCSI Modular Disk storage arrays. It is recommended that you install and use PowerVault MDCU to configure iSCSI on each host connected to the storage array." on page 27.

   b. Set up the PowerVault MD1200 series expansion enclosure(s).

      For information about setting up the PowerVault MD1200 series expansion enclosure(s), see the *Hardware Owner's Manual* at support.dell.com/manuals.

   c. Using PowerVault MDSM, update the RAID controller module firmware and NVSRAM to the latest versions available on support.dell.com. From the Enterprise Management Window (EMW).

   d. Click Tools→ Upgrade RAID Controller Module Firmware.

2. Stop I/O and turn off all systems:

   a. Stop all I/O to the storage array and turn off affected host systems attached to the storage array.

   b. Turn off the storage array.

c Turn off any expansion enclosure(s) in the affected system.

3 Cable the expansion enclosure(s) to the storage array.

4 Turn on attached units:

a Turn on the expansion enclosure(s). Wait for the enclosure status LED to turn blue.

b Turn on the storage array and wait for the status LED to indicate that the unit is ready:

- If the status LEDs are solid amber, the storage array is still coming online.
- If the status LEDs are blinking amber, there is an error that can be viewed using PowerVault MDSM.
- If the status LEDs are solid blue, the storage array is ready.

c After the storage array is online and ready, turn on any attached host systems.

5 Using PowerVault MDSM, update all attached expansion enclosure firmware if it is out of date:

a From the EMW, select the enclosure that you want to update and enter the Array Management Window (AMW).

b Click Advanced→ Maintenance→ Download→ EMM Firmware.

c Select Select All to update all the attached expansion enclosures simultaneously.

3

Installing PowerVault MD Storage Software

The Dell PowerVault MD series resource media contains software and drivers for both Linux and Microsoft Windows operating systems.

The root of the media contains a readme.txt file covering changes to the software, updates, fixes, patches, and other important data applicable to both Linux and Windows operating systems. The readme.txt file also specifies requirements for accessing documentation, information regarding versions of the software on the media, and system requirements for running the software.

For more information on supported hardware and software for PowerVault systems, see the *Support Matrix* located at support.dell.com/manuals.

NOTE: It is recommended that you install all the latest updates available at support.dell.com.

The PowerVault MD series storage software installer provides features that include the core software, providers, and optional utilities. The core software feature includes the host-based storage agent, multipath driver, and MD Storage Manager (MDSM) application used to configure, manage, and monitor the storage array solution. The providers feature includes providers for the Microsoft Virtual Disk Service (VDS) and Microsoft Volume Shadow-Copy Service (VSS) framework. The PowerVault Modular Disk Configuration Utility (MDCU) is an optional utility that provides a consolidated approach for configuring the management ports, iSCSI host ports, and creating sessions for the iSCSI Modular Disk storage arrays. It is recommended that you install and use PowerVault MDCU to configure iSCSI on each host connected to the storage array.

NOTE: For more information about the Microsoft VDS and Microsoft VSS providers, see the *Owner's Manual*. To install the software on a Windows or Linux system, you must have administrative or root privileges.

NOTE: If Dynamic Host Configuration Protocol (DHCP) is not used, initial configuration of the management station must be performed on the same physical subnet as the storage array. Additionally, during initial configuration, at least one network adapter must be configured on the same IP subnet as the storage array's default management port (192.168.128.101 or 192.168.128.102). After initial configuration, the management ports are configured using MDSM and the management station's IP address can be changed back to the previous settings.

The PowerVault MD series resource media offers the following three installation methods:

- Graphical Installation (Recommended)—This is the recommended installation procedure for most users. The installer presents a graphical wizard-driven interface that allows customization of which components are installed.
- Console Installation—This installation procedure is useful for Linux users that do not desire to install an X-Window environment on their supported Linux platform.
- Silent Installation—This installation procedure is useful for users that prefer to create scripted installations.

Graphical Installation (Recommended)

The PowerVault MD Storage Manager software configures, manages and monitors the storage array. The PowerVault MD Configuration Utility (MDCU) is an optional utility that provides a consolidated approach for configuring the management and iSCSI host ports, and creating sessions for the iSCSI modular disk storage arrays. It is recommended that you use PowerVault MDCU to configure iSCSI on each host server connected to the storage array. To install the PowerVault MD storage software:

1. Insert the PowerVault MD series resource media.

   Depending on your operating system, the installer may launch automatically. If the installer does not launch automatically, navigate to the root directory of the installation media (or downloaded installer image) and run the md_launcher.exe file. For Linux-based systems, navigate to the root of the resource media and run the autorun file.

NOTE: By default, Red Hat Enterprise Linux mounts the resource media with the **–noexec mount** option which does not allow you to run executable files. To change this setting, see the **Readme** file in the root directory of the installation media.

2. Select Install MD Storage Software.
3. Read and accept the license agreement.
4. Select one of the following installation options from the Install Set dropdown menu:
   - Full (recommended)—Installs the PowerVault MD Storage Manager (client)software, host-based storage agent, multipath driver, and hardware providers.
   - Host Only—Installs the host-based storage agent and multipath drivers.
   - Management—Installs the management software and hardware providers.
   - Custom—Allows you to select specific components.
5. Select the PowerVault MD storage array model(s) you are setting up to serve as data storage for this host server.
6. Choose whether to start the event monitor service automatically when the host server reboots or manually.

NOTE: This option is applicable only to Windows client software installation.

7. Confirm the installation location and choose Install.
8. If prompted, reboot the host server once the installation completes.
9. When the reboot is complete, the PowerVault MDCU may launch automatically. If the PowerVault MDCU does not launch automatically, launch it manually.
   - In a Windows-based operating system, click Start→ Dell→ Modular Disk Configuration Utility.
   - In a Linux-based operating system, double-click the Modular Disk Configuration Utility icon on the desktop.
10. Start MD Storage Manager and discover the array(s).
11. If applicable, activate any premium features purchased with your storage array. If you purchased premium features, see the printed activation card shipped with your storage array.

NOTE: The **MD Storage Manager** installer automatically installs the required drivers, firmware, and operating system patches/hotfixes to operate your storage array. These drivers and firmware are also available at **support.dell.com**. In addition, see the *Support Matrix* at **support.dell.com/manuals** for any additional settings and/or software required for your specific storage array.

Console Installation

NOTE: Console installation only applies to Linux systems that are not running a graphical environment.

The autorun script in the root of the resource media detects when there is no graphical environment running and automatically starts the installer in a text-based mode. This mode provides the same options as graphical installation with the exception of the PowerVault MDCU specific options. The PowerVault MDCU requires a graphical environment to operate.

NOTE: The console mode installer provides the option to install the PowerVault MDCU.However a graphical environment is required to utilize the PowerVault MDCU.

Silent Installation

To run silent installation on a Windows system:

1. Copy the custom_silent.properties file in the /windows folder of the installation media or image to a writable location on the host server.
2. Modify the custom_silent.properties file to reflect the features, models and installation options to be used. Then, save the file.
3. Once the custom_silent.properties file is revised to reflect your specific installation, run the following command to begin the silent installation:

```
mdss_install.exe –f <host_server_path>\
custom_silent.properties
```

To run silent installation on a Linux system:

NOTE: On Red Hat Enterprise Linux 6 operating systems, run the following script from the root directory to install prerequisite packages:

```
# md_prereq_install.sh
```

1. Copy the custom_silent.properties file in the /windows folder of the installation media or image to a writable location on the host server.

2 Modify the custom_silent.properties file to reflect the features, models and installation options to be used. Then, save the file.

3 Once the custom_silent.properties file is revised, run the following command to begin the installation:

```
./mdss_install.bin –f
<host_server_path>/custom_silent.properties
```

Upgrading PowerVault MD Storage Software

To upgrade from a previous version of the MD Storage Manager application, uninstall the previous version (see "Uninstalling PowerVault MD Storage Software" on page 53), and then follow the instructions in this chapter to install the new version.

4

Post Installation Tasks

Before using the storage array for the first time, complete a number of initial configuration tasks in the order shown. These tasks are performed using the MD Storage Manager (MDSM) software.

NOTE: If Dynamic Host Configuration Protocol (DHCP) is not used, initial configuration using the management station must be performed on the same physical subnet as the storage array. Additionally, during initial configuration, at least one network adapter must be configured on the same IP subnet as the storage array's default management port (192.168.128.101 or 192.168.128.102). After initial configuration, the management ports are configured using MDSM and the management station's IP address can be changed back to the previous settings.

Before You Begin

Before you begin configuring iSCSI, you must fill out the iSCSI configuration worksheet. Gathering this type of information about your network prior to starting the configuration steps helps you to complete the process in less time.

iSCSI Configuration Terminology

Table 4-1. Standard Terminology Used in iSCSI Configuration

Term	Definition
CHAP (Challenge Handshake Authentication Protocol)	An optional security protocol used to control access to an iSCSI storage system by restricting use of the iSCSI data ports on both the host server and storage array. For more information on the types of CHAP authentication supported, see "Understanding CHAP Authentication" on page 63.
Host or host server	A server connected to the storage array using iSCSI ports.
Host server port	SCSI port on the host server used to connect it to the storage array.

Table 4-1. Standard Terminology Used in iSCSI Configuration

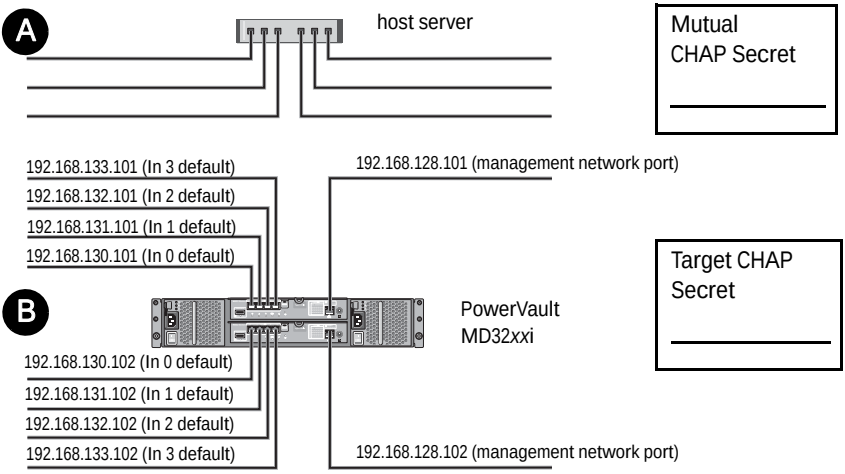
Term	Definition
iSCSI initiator	The iSCSI-specific software installed on the host server that controls communications between the host server and the storage array.
iSCSI host port	The iSCSI port (two per controller) on the storage array.
iSNS (Microsoft Internet Storage Naming Service)	An automated discovery, management and configuration Storage Naming Service) tool used by some iSCSI devices.
Management station	The system from which you manage your host server/storage array configuration.
Storage array	The enclosure containing the storage data accessed by the host server.
Target	An iSCSI port on the storage array that accepts and responds to requests from the iSCSI initiator installed on the host server.

iSCSI Configuration Worksheet

The iSCSI configuration worksheet helps you plan your configuration. Recording host server and storage array IP addresses at a single location enables you to configure your setup faster and more efficiently.

"Guidelines for Configuring Your Network for iSCSI" on page 49 provides general network setup guidelines for both Windows and Linux environments. It is recommended that you review these guidelines before completing the worksheet.

IPv4 Settings

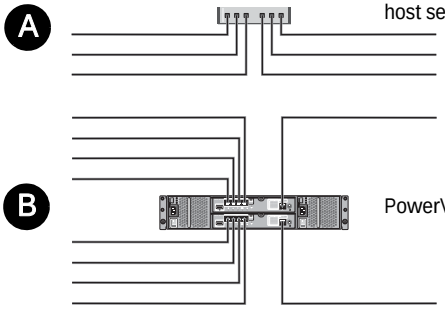


If you need additional space for more than one host server, use an additional sheet.

A	Static IP address (host server)	Subnet *(should be different for each NIC)*	Default gateway
iSCSI port 1	___ . ___ . ___ . ___	___ . ___ . ___ . ___	___ . ___ . ___ . ___
iSCSI port 2	___ . ___ . ___ . ___	___ . ___ . ___ . ___	___ . ___ . ___ . ___
iSCSI port 3	___ . ___ . ___ . ___	___ . ___ . ___ . ___	___ . ___ . ___ . ___
iSCSI port 4	___ . ___ . ___ . ___	___ . ___ . ___ . ___	___ . ___ . ___ . ___
Management port	___ . ___ . ___ . ___	___ . ___ . ___ . ___	___ . ___ . ___ . ___
Management port	___ . ___ . ___ . ___	___ . ___ . ___ . ___	___ . ___ . ___ . ___

B	Static IP address (host server)	Subnet	Default gateway
iSCSI controller 0, In 0	___ . ___ . ___ . ___	___ . ___ . ___ . ___	___ . ___ . ___ . ___
iSCSI controller 0, In 1	___ . ___ . ___ . ___	___ . ___ . ___ . ___	___ . ___ . ___ . ___
iSCSI controller 0, In 2	___ . ___ . ___ . ___	___ . ___ . ___ . ___	___ . ___ . ___ . ___
iSCSI controller 0, In 3	___ . ___ . ___ . ___	___ . ___ . ___ . ___	___ . ___ . ___ . ___
Management port cntrl 0	___ . ___ . ___ . ___	___ . ___ . ___ . ___	___ . ___ . ___ . ___
iSCSI controller 1, In 0	___ . ___ . ___ . ___	___ . ___ . ___ . ___	___ . ___ . ___ . ___
iSCSI controller 1, In 1	___ . ___ . ___ . ___	___ . ___ . ___ . ___	___ . ___ . ___ . ___
iSCSI controller 1, In 2	___ . ___ . ___ . ___	___ . ___ . ___ . ___	___ . ___ . ___ . ___
iSCSI controller 1, In 3	___ . ___ . ___ . ___	___ . ___ . ___ . ___	___ . ___ . ___ . ___
Management port cntrl 1	___ . ___ . ___ . ___	___ . ___ . ___ . ___	___ . ___ . ___ . ___

IPv6 Settings



Mutual CHAP

Target CHAP

If you need additional space for more than one host server, use an additional sheet.

A

Host iSCSI port 1		Host iSCSI port 2	
Link local IP address	___ . ___ . ___ . ___	Link local IP address	___ . ___ . ___ . ___
Routable IP address	___ . ___ . ___ . ___	Routable IP address	___ . ___ . ___ . ___
Subnet prefix	___ . ___ . ___ . ___	Subnet prefix	___ . ___ . ___ . ___
Gateway	___ . ___ . ___ . ___	Gateway	___ . ___ . ___ . ___

B

iSCSI controller 0, In 0	
IP address	FE80 : 0000 : 0000 : 0000 : ____ : ____ : ____ : ____
Routable IP address 1	____ : ____ : ____ : ____ : ____ : ____ : ____ : ____
Routable IP address 2	____ : ____ : ____ : ____ : ____ : ____ : ____ : ____
Router IP address	____ : ____ : ____ : ____ : ____ : ____ : ____ : ____
iSCSI controller 0, In 1	
IP address	FE80 : 0000 : 0000 : 0000 : ____ : ____ : ____ : ____
Routable IP address 1	____ : ____ : ____ : ____ : ____ : ____ : ____ : ____
Routable IP address 2	____ : ____ : ____ : ____ : ____ : ____ : ____ : ____
Router IP address	____ : ____ : ____ : ____ : ____ : ____ : ____ : ____
iSCSI controller 0, In 2	
IP address	FE80 : 0000 : 0000 : 0000 : ____ : ____ : ____ : ____
Routable IP address 1	____ : ____ : ____ : ____ : ____ : ____ : ____ : ____
Routable IP address 2	____ : ____ : ____ : ____ : ____ : ____ : ____ : ____
Router IP address	____ : ____ : ____ : ____ : ____ : ____ : ____ : ____

iSCSI controller 0, In 3

IP address FE80 : 0000 : 0000 : 0000 : ____ : ____ : ____ : ____

Routable IP address 1 ____ : ____ : ____ : ____ : ____ : ____ : ____ : ____

Routable IP address 2 ____ : ____ : ____ : ____ : ____ : ____ : ____ : ____

Router IP address ____ : ____ : ____ : ____ : ____ : ____ : ____ : ____

iSCSI controller 1, In 0

IP address FE80 : 0000 : 0000 : 0000 : ____ : ____ : ____ : ____

Routable IP address 1 ____ : ____ : ____ : ____ : ____ : ____ : ____ : ____

Routable IP address 2 ____ : ____ : ____ : ____ : ____ : ____ : ____ : ____

Router IP address ____ : ____ : ____ : ____ : ____ : ____ : ____ : ____

iSCSI controller 1, In 1

IP address FE80 : 0000 : 0000 : 0000 : ____ : ____ : ____ : ____

Routable IP address 1 ____ : ____ : ____ : ____ : ____ : ____ : ____ : ____

Routable IP address 2 ____ : ____ : ____ : ____ : ____ : ____ : ____ : ____

Router IP address ____ : ____ : ____ : ____ : ____ : ____ : ____ : ____

iSCSI controller 1, In 2

IP address FE80 : 0000 : 0000 : 0000 : ____ : ____ : ____ : ____

Routable IP address 1 ____ : ____ : ____ : ____ : ____ : ____ : ____ : ____

Routable IP address 2 ____ : ____ : ____ : ____ : ____ : ____ : ____ : ____

Router IP address ____ : ____ : ____ : ____ : ____ : ____ : ____ : ____

iSCSI controller 1, In 3

IP address FE80 : 0000 : 0000 : 0000 : ____ : ____ : ____ : ____

Routable IP address 1 ____ : ____ : ____ : ____ : ____ : ____ : ____ : ____

Routable IP address 2 ____ : ____ : ____ : ____ : ____ : ____ : ____ : ____

Router IP address ____ : ____ : ____ : ____ : ____ : ____ : ____ : ____

Configuring iSCSI on Your Storage Array

The following sections contain step-by-step instructions for configuring iSCSI on your storage array. However, before beginning, it is important to understand where each of these steps occur in relation to your host server/storage array environment.

Table 4-2 below shows each specific iSCSI configuration step and where it occurs.

Table 4-2. Host Server Vs. Storage Array

This Step is Performed on the Host Server Using the Microsoft or Linux iSCSI Initiator	This Step is Performed on the Storage Array Using PowerVault MD Storage Manager
	1 Discover the storage array
	2 Configure the iSCSI ports on the storage array
3 Perform target discovery from the iSCSI initiator	
	4 Configure host access
	5 (Optional) Configure CHAP authentication on the storage array
6 (Optional) Configure CHAP authentication on the host server	
7 Connect to the storage array from the host server	
	8 (Optional) Set up in-band management

NOTE: It is recommended that you use the PowerVault Modular Disk Configuration Utility (MDCU) for iSCSI configuration. The PowerVault MDCU wizards guides you through the configuration steps described above. If you want to perform a manual configuration, see "Appendix—Manual Configuration of iSCSI" on page 55.

Automatic Configuration Using the Modular Disk Configuration Utility

NOTE: If PowerVault MDCU is not installed, it can be installed from the PowerVault MD series resource media.

PowerVault MDCU provides a consolidated approach for configuring the iSCSI network of host servers and iSCSI-based storage arrays using a wizard-driven interface. This utility also enables the user to configure the iSCSI sessions of the host server according to the best practices and to achieve load-balanced paths with the storage array iSCSI host ports.

NOTE: PowerVault MDCU is only applicable to iSCSI-based PowerVault MD3200i series storage arrays. It does apply to SAS-based PowerVault MD3200 series storage arrays.

If you select Launch the MDCU after reboot during the installation of the host software, the utility automatically launches after the next host server reboot. This utility can also be launched manually.

The utility has a context sensitive online help to guide you through each step of the wizard.

The PowerVault MDCU performs:

- Storage array configuration
- Host configuration

Storage Array Configuration

Before a host iSCSI initiator and an iSCSI-based storage array can communicate, they must be configured with information such as which IP addresses and authentication method to use. Since iSCSI initiators establish connections with an already configured storage array, the first task is to configure your storage arrays to make them available for iSCSI initiators.

This utility requires network access to the management ports of the storage arrays you wish to configure. You must have a properly functioning network infrastructure before attempting to configure your storage arrays. If your storage arrays are already configured, you can skip directly to the host configuration.

This configuration task generally involves the following steps:

1. Discover available storage array(s) for configuration.
2. Select a storage array to configure.
3. Set a storage array name and password.

4 Configure the IP protocols and addresses for the management ports.

5 Configure the IP protocols and addresses for the iSCSI ports.

6 Specify the CHAP authentication method.

7 Apply the settings after reviewing a summary.

8 Repeat the process starting from step 2 to configure additional arrays.

Host Configuration (Host Connectivity Configuration)

After you have completed configuring your iSCSI-based storage arrays, the next task is to run this utility on all hosts that need to access the storage arrays. Depending on your network configuration, your host may be the same machine you use to manage your storage arrays, or it may be on a completely separate network.

The option to configure a host is disabled if the machine the utility is running on does not have an iSCSI initiator or the required driver components installed. When the option is disabled, the utility also displays an informational message. If you are running the utility on a host which is not connected to the iSCSI–based storage array (or which you do not wish to connect to the array), the informational message can be ignored.

The task generally involves the following steps:

1 Discover available storage array(s) for connection.

2 Select a storage array to connect to.

3 Specify the CHAP secret.

4 Select the iSCSI ports the host's initiator uses to log on.

5 Repeat the process starting from step 2 to connect to additional arrays.

6 Repeat these steps on each host that needs access to the storage array(s).

Before Starting the Configuration Process

Before you start configuring the storage array or host connectivity, it is recommended that you fill out the iSCSI configuration worksheet to help you plan your configuration. You may need to use several worksheets depending on your configuration.

Keep the following guidelines in mind for the storage array and host configuration:

- For optimal performance, ensure your network configuration is valid by consulting the storage array's support matrix.
- If your host has multiple network interfaces, it is recommended that each network interface uses a separate subnet.
- For redundancy in a dual controller (duplex) configuration, ensure each host network interface is configured to connect to both storage array controllers.
- For optimal load balancing, ensure each host network interface that is used for iSCSI traffic is configured to connect to each storage array controller.
- It is recommended that each host network interface only establishes one iSCSI session per storage array controller.

NOTE: The utility tries to follow the guidelines for the host connectivity whenever possible based on the available host network interfaces and their connectivity with the iSCSI host ports of the storage array.

Configure the Storage Array Using PowerVault MDCU

To configure the iSCSI-based storage array(s) using PowerVault MDCU:

1. Launch the utility (if it is not launched automatically) from the server with access to the management ports of the storage array(s) to be configured.

   For Windows, click Start→ All Programs→ Dell→ MD Storage Software→ Modular Disk Configuration Utility.

   For Linux, click the MDCU icon on the desktop or navigate to the /opt/dell/mdstoragesoftwaare/mdconfigurationutility directory in a terminal window and run PowerVault MDCU.

2. Click Next to continue.
3. Select the configuration task Configure Modular Disk Storage Array and click Next to continue.
4. Select the method by which the utility should discover the storage arrays for configuration and click Next.

- Automatic Discovery—Automatic discovery queries the local sub-network for all iSCSI-based storage arrays and may take several minutes to complete.
- Manual Discovery—Manual discovery allows you to locate iSCSI-based storage arrays that are outside of the local sub-network. Manual discovery requires selecting whether your storage array has a single controller (simplex) or dual controllers (duplex) and whether to use IPv4 or IPv6 protocol for communicating with the management port of the storage array.

5 The next screen presents a list of the iSCSI-based storage arrays that were discovered based on the discovery process selected in step 3.

If you select Automatic Discovery, the screen displays a list of all the iSCSI-based storage arrays that were discovered in the subnet.

If you select Manual Discovery, then the list contains only the arrays whose IP addresses were entered. You can add additional arrays to the list by clicking the Add button on this screen.

You can also remove the arrays from this list by using the Remove button.

You can click Blink Array to start the blinking of the array's front panel LED in order to locate the array physically and ensure it is the array you intend to configure. Click Stop Blinking to stop the blinking of the array before you proceed.

Select the array by clicking the radio button of the corresponding storage array and then click Next.

6 Enter the name of the storage array and the password.

If you want to set a new password for the array, select Set Password and then enter the new password in the New Password and Confirm New Password fields. Click Next to continue.

7 Select the IP protocol (IPv4/IPv6) to be used by the management port. Also, for each protocol, select whether the configuration of the management port IP addresses is to be done manually or automatically. For more information, see the *online help*.

Click Next to continue after you has finished selecting the protocols and the configuration method.

If you have not selected Specify Configuration Manually for any of the two protocols, then you can skip step 8.

8 If you have selected Specify Configuration Manually for any of the two protocols in the last step, a series of screens showing the backend view image of the storage array controllers is displayed. Each image contains IP addresses of management ports of the controllers. Also each image has one management port highlighted in red.

For IPv4 address of the highlighted port, enter the IP address, subnet mask and gateway address in the fields shown below the image in order to modify it.

For IPv6 address of the highlighted port, enter the local IP address, routable IP, and router IP address in the fields shown below the image in order to modify it.

Click Next to continue through these images to complete the configuration of all the management ports for the selected protocols.

9 In the CHAP Configuration screen, select the CHAP method and click Next. For more information on CHAP see "Understanding CHAP Authentication" on page 63.

10 In the Summary screen, review the information that you entered for the storage array.

Click Apply to save the changes to the storage array.

NOTE: To abort the configuration for the storage array and to go back to select a storage array for configuration, click **Cancel Array**.

11 On the Configure Additional Arrays screen, select whether you want to configure additional array. Click Next to continue.

12 If you selected Yes in the above step, then start again from step 4.

13 If you selected No in step 12, then on the Configure Host Connectivity screen, select whether you want to configure the connectivity for current host's iSCSI initiator. Click Next to continue.

If you selected No above, then you are done with the configuration task.

14 Click Finish on the final screen to exit the utility.

15 If you selected Yes in the last step, then the Select Storage Array screen is displayed. Select the storage array that you want to configure for connectivity to the local host.

NOTE: The storage arrays configured by the utility are marked as **Configuration Complete** against their names in the list. This helps you to identify the arrays that are ready to be configured for host access.

16 In the Storage Array Login screen, in the Controller# column, select the iSCSI host port of the storage array that needs to be configured and it's IP address(es). In the Host Address column, from drop-down menu list, select the host IP address that will login to the iSCSI host port of the storage array.

See "Source Port Selection for iSCSI Host Ports" on page 46' for more information about how these host IP addresses are listed in the drop-down menu and the recommended guidelines for selecting the host IP addresses.

Click Next to continue to enter the log in information for another controller or Click Apply to save the log in information.

17 In the Connect to Additional Arrays screen, select whether you want to connect to another storage array or not.

If you want to connect to another storage array, repeat the above steps starting from step 15.

If you do not want to connect to additional arrays, then click Finish on the final screen to exit the utility.

Configure the Host Connectivity Using PowerVault MDCU

To configure the host connectivity for an iSCSI-based storage array(s) using PowerVault MDCU:

1. Launch the utility (if it is not launched automatically) from the server which needs to be configured for access to the iSCSI-based storage array(s). This server must have access to the array either using the array's management ports or using the array's iSCSI host ports.

   See step 1 in "Configure the Storage Array Using PowerVault MDCU" on page 41 for the instructions on how to launch the utility.

   Click Next to continue.

2. In the Configuration Task screen, select Configure Host and click Next.

   NOTE: This task is not supported or is disabled if the MDSM agent is not installed on the host where you are running the utility. The agent is typically not installed on the Windows client systems such as Windows XP.

3. In the Discovery Method screen, select one of the discovery methods.

   If the host has access to the management ports of the PowerVault MD storage array(s), then select Discover via Management Port method and click Next.

   If the host does not have the access to the management ports of the array, then select the Discover via iSCSI Port method (assuming that the host has access to the iSCSI host ports of the storage array) and click Next. Continue to step 5.

4. Follow the instructions in step 3 and step 4 of "Configure the Storage Array Using PowerVault MDCU" on page 41 to select the storage array that needs to be configured for connectivity with the host. Go to step 6.

5. In the iSCSI Port IP Address screen, enter the IPv4 IP address of any one of the iSCSI host port of the array that the host can connect to or enter the IPv6 local address of the any of the iSCSI host port. Click Next to continue.

6. In the CHAP Configuration screen, enter the CHAP secret if you have configured a CHAP secret for the storage array.

7 In the Storage Array Login screen, in the Controller# column, select the iSCSI host port of the storage array that needs to be configured and its IP address(es). In the Host Address column, from drop-down menu list, select the host IP address that logs into the iSCSI host port of the storage array.

See "Source Port Selection for iSCSI Host Ports" on page 46 for more details about how these host IP addresses are listed in the drop-down menu and the recommended guidelines for selecting the host IP addresses.

Click Next to continue to enter the login information for another controller or Click Apply to commit the array login information.

8 In the Connect to Additional Arrays screen, select whether you want to connect to another storage array or not.

If you want to connect to another storage array, repeat the above steps starting from step 4 or step 5 depending on your last selection.

If you do not want to connect to additional arrays, then click Finish on the final screen to exit the utility.

Source Port Selection for iSCSI Host Ports

In order to establish data communication between a host and an iSCSI-based storage array, the iSCSI initiator on the host must be configured to establish iSCSI sessions to the iSCSI host ports of the storage array. The iSCSI port login screen allows you to specify the host and storage array IP addresses the iSCSI initiator uses to establish these iSCSI sessions.

Port Login Selection

Each iSCSI port for each controller in the storage array is presented with a list of host IP addresses through which the iSCSI initiator is able to login. The host IP addresses are the source IP addresses and the iSCSI port is the target.

Each list contains only the host IP addresses that are able to communicate with the associated iSCSI port. If none of the host IP addresses are able to communicate with an iSCSI port, Not Available is the only option shown for that iSCSI port. If none of the host IP addresses are able to communicate with any iSCSI ports of either storage array controller, the host configuration option is aborted for that storage array.

NOTE: The behavior described in the preceding paragraph does not apply to Microsoft Windows Server 2003.

For Microsoft Windows Server 2003, each list contains all available host IP addresses regardless of whether or not the address is able to communicate with the associated iSCSI port. You must select the appropriate host IP addresses for each iSCSI port.

Automatic Selection

NOTE: The contents in this section do not apply to Microsoft Windows Server 2003.

The utility attempts to automatically find and select the best possible configuration of host IP address(es) and storage array iSCSI ports for optimal performance and redundancy.

This automatic selection attempts to ensure that a host IP address (up to two IP addresses for PowerVault MD3000i storage arrays and up to four IP addresses for PowerVault MD3200i and MD3220i storage arrays) establishes an iSCSI session with each storage array controller and that the host IP address is logged into a maximum of one iSCSI port per controller. Configuration in this manner ensures redundancy and load balancing among the multiple host IP addresses (NICs).

The Do Not Connect option may be selected as the default option if the utility recommends not to connect to the iSCSI port. Also, even if the best recommended configuration is presented (whenever possible), you can still override this configuration by selecting the other host IP addresses from the drop-down list.

Suboptimal Configuration Warnings

In the following cases, a warning is displayed, that you must confirm, to continue:

- The host IP addresses are selected in such a way that any host IP address establishes an iSCSI session with only one storage array controller in a dual controller (duplex) configuration.
- The host IP addresses are selected in such a way that a host IP address establishes two or more iSCSI sessions with the same storage array controller.

Post Connection Establishment Steps

After iSCSI connectivity is established between the host server(s) and the storage array, you can create virtual disks on the storage array using MDSM and these virtual disks can be utilized by the host server(s). For more information about storage planning and using MDSM, see the *Owner's Manual* at support.dell.com/manuals.

5

Guidelines for Configuring Your Network for iSCSI

This section provides general guidelines for setting up your network environment and IP addresses for use with the iSCSI ports on your host server and storage array. Your specific network environment may require different or additional steps than shown here, so make sure you consult with your system administrator before performing this setup.

Microsoft Windows Host Setup

To set up a Windows host network, you must configure the IP address and netmask of each iSCSI port connected to the storage array. The specific steps depend on whether you are using a Dynamic Host Configuration Protocol (DHCP) server, static IP addressing, Domain Name System (DNS) server, or Windows Internet Name Service (WINS) server.

NOTE: The server IP addresses must be configured for network communication to the same IP subnet as the storage array management and iSCSI ports.

If you are using a DHCP server:

1. In the Control Panel, select Network connections or Network and Sharing Center and then click Manage network connections.
2. Right-click the network connection you want to configure and select Properties.
3. On the General tab (for a local area connection) or the Networking tab (for all other connections), select Internet Protocol (TCP/IP), and then click Properties.
4. Select Obtain an IP address automatically, then click OK.

If you are using static IP addressing:

1. In the Control Panel, select Network connections or Network and Sharing Center and then click Manage network connections.
2. Right-click the network connection you want to configure and select Properties.

3 On the General tab (for a local area connection) or the Networking tab (for all other connections), select Internet Protocol (TCP/IP), and then click Properties.

4 Select Use the following IP address and enter the IP address, subnet mask, and default gateway addresses.

If you are using a DNS server:

1 In the Control Panel, select Network connections or Network and Sharing Center and then click Manage network connections.

2 Right-click the network connection you want to configure and select Properties.

3 On the General tab (for a local area connection) or the Networking tab (for all other connections), select Internet Protocol (TCP/IP), and then click Properties.

4 Select Obtain DNS server address automatically or enter the preferred and alternate DNS server IP addresses and click OK.

If you are using a WINS server:

NOTE: If you are using a DHCP server to allocate WINS server IP addresses, you do not need to add WINS server addresses.

1 In the Control Panel, select Network connections.

2 Right-click the network connection you want to configure and select Properties.

3 On the General tab (for a local area connection) or the Networking tab (for all other connections), select Internet Protocol (TCP/IP), and then click Properties.

4 Select Advanced→ WINS tab and click Add.

5 In the TCP/IP WINS server window, type the IP address of the WINS server and click Add.

6 To enable use of the Lmhosts file to resolve remote NetBIOS names, select Enable LMHOSTS lookup.

7 To specify the location of the file that you want to import into the Lmhosts file, select Import LMHOSTS and then select the file in the Open dialog box.

8 Enable or disable NetBIOS over TCP/IP.

If using Microsoft Windows Server 2008 Core Version, use the `netsh` interface command to configure the iSCSI ports on the host server.

Linux Host Setup

To set up a Linux host network, you must configure the IP address and netmask of each iSCSI port connected to the storage array. The specific steps depend on whether you are configuring TCP/IP using DHCP or configuring TCP/IP using a static IP address.

NOTE: The server IP addresses must be configured for network communication to the same IP subnet as the storage array management and iSCSI ports.

If you are using DHCP (root users only):

1 Edit the /etc/sysconfig/network file:

```
NETWORKING=yes HOSTNAME=mymachine.mycompany.com
```

2 Edit the configuration file for the connection you want to configure, either

/etc/sysconfig/network-scripts/ifcfg-ethX (for Red Hat Enterprise Linux) or /etc/sysconfig/network/ifcfg-eth-id-XX:XX:XX:XX:XX (for SUSE Enterprise Linux).

```
BOOTPROTO=dhcp
```

Also, verify that an IP address and netmask are not defined.

3 Restart network services using the following command:

```
/etc/init.d/network  restart
```

If you are using a static IP address (root users only):

1. Edit the /etc/sysconfig/network file as follows:

   ```
   NETWORKING=yes HOSTNAME=mymachine.mycompany.com
   GATEWAY=255.255.255.0
   ```

2. Edit the configuration file for the connection you want to configure, either

   /etc/sysconfig/network-scripts/ifcfg-ethX (for Red Hat Enterprise Linux) or /etc/sysconfig/network/ifcfg-eth-id-XX:XX:XX:XX:XX (for SUSE Enterprise Linux).

   ```
   BOOTPROTO=static BROADCAST=192.168.1.255 IPADDR=
   192.168.1.100 NETMASK=255.255.255.0 NETWORK=
   192.168.1.0 ONBOOT=yes TYPE=Ethernet
   ```

   ```
   HWADDR=XX:XX:XX:XX:XX:XX GATEWAY=192.168.1.1
   ```

3. Restart network services using the following command:

   ```
   /etc/init.d/network  restart
   ```

6

Uninstalling PowerVault MD Storage Software

Uninstalling Dell PowerVault MD Storage Software From Windows

Use the Change/Remove Program feature to uninstall Dell PowerVault Modular Disk Storage Software from Microsoft Windows operating systems other than Microsoft Windows Server 2008:

1. From the Control Panel, double-click Add or Remove Programs.
2. Select Dell MD32*xxi* Storage Software from the list of programs.
3. Click Change/Remove.

   The Uninstall Complete window appears.
4. Follow the instructions on screen.
5. Select Yes to restart the system, and then click Done.

Use the following procedure to uninstall Modular Disk Storage software from Windows Server 2008 GUI versions:

1. From the Control Panel, double-click Programs and Features.
2. Select MD Storage Software from the list of programs.
3. Click Uninstall/Change.

   The Uninstall Complete window appears.
4. Select Yes to restart the system, then click Done.

Use the following procedure to uninstall Modular Disk Storage Software on Windows Server 2008 Core versions:

1. Navigate to the Dell\MD Storage Software\Uninstall Dell 32xxi Storage Software directory.

NOTE: By default, Dell PowerVault MD Storage Manager is installed in the **\Program Files\Dell\MD Storage Software** directory. If another directory was used during installation, navigate to that directory before beginning the uninstallation procedure.

2 From the installation directory, type the following command and press <Enter>:

```
Uninstall Dell MD Storage Software
```

3 From the Uninstall window, click Next and follow the instructions on the screen.

4 Select Yes to restart the system, then click Done.

Uninstalling PowerVault MD Storage Software From Linux

1 By default, PowerVault MD Storage Manager is installed in the /opt/dell/mdstoragemanager/Uninstall Dell MD32xxi Storage Software directory. If another directory was used during installation, navigate to that directory before beginning the uninstallation procedure.

2 From the installation directory, open the Uninstall Dell MD Storage Software directory.

3 Run the file Uninstall Dell MD Storage.

4 From the Uninstall window, click Next, and follow the instructions on the screen.

While the software is uninstalling, the Uninstall window is displayed. When the uninstall procedure is complete, the Uninstall Complete window is displayed.

5 Click Done.

A

Appendix—Manual Configuration of iSCSI

The following sections contain step-by-step instructions for configuring iSCSI on your storage array. However, before beginning, it is important to understand where each of these steps occur in relation to your host server or storage array environment.

Table A-1 below shows each iSCSI configuration step and where it occurs.

Table A-1. Host Server Vs. Storage Array

This Step is Performed on the Host Server Using the Microsoft or Linux iSCSI Initiator	This Step is Performed on the Storage Array Using PowerVault MD Storage Manager
	1 Discover the storage array
	2 Configure the iSCSI ports on the storage array
3 Perform target discovery from the iSCSI initiator	
	4 Configure host access
	5 (Optional) Configure CHAP authentication on the storage array
6 (Optional) Configure CHAP authentication on the host server	
7 Connect to the storage array from the host server	
	8 (Optional) Set up in-band management

Step 1: Discover the Storage Array (Out-of-band Management Only)

Default Management Port Settings

By default, the storage array management ports are set to Dynamic Host Configuration Protocol (DHCP). If the controllers on your storage array are unable to get IP configuration from a DHCP server, it times out after 10 seconds and falls back to a default static IP address. The default IP configuration is:

```
Controller 0: IP: 192.168.128.101 Subnet Mask:
255.255.255.0

Controller 1: IP: 192.168.128.102 Subnet Mask:
255.255.255.0
```

NOTE: No default gateway is set.

NOTE: If DHCP is not used, initial configuration using the management station must be performed on the same physical subnet as the storage array. Additionally, during initial configuration, at least one network adapter must be configured on the same IP subnet as the storage array's default management port (192.168.128.101 or 192.168.128.102). After initial configuration (management ports are configured using PowerVault MD Storage Manager), the management station's IP address can be changed back to its previous settings.

NOTE: This procedure applies to out-of-band management only. If you choose to set up in-band management, you must complete this step and then see "Step 8: (Optional) Set Up In-Band Management" on page 74.

You can discover the storage array either automatically or manually. Select one and complete the steps below.

Automatic Storage Array Discovery

1. Launch MD Storage Manager (MDSM).

   If this is the first storage array to be set up, the Add New Storage Array window is displayed.

2. Select Automatic and click OK.

   It may take several minutes for the discovery process to complete. Closing the discovery status window before the discovery process completes cancels the discovery process.

   After discovery is complete, a confirmation screen is displayed. Click Close to close the screen.

Manual Storage Array Discovery

1. Launch MDSM.

   If this is the first storage array to be set up, the Add New Storage Array window is displayed.

2. Select Manual and click OK.
3. Select Out-of-band management and enter the host server name(s) or IP address(es) of the iSCSI storage array controller.
4. Click Add.

   Out-of-band management should now be successfully configured.

   After discovery is complete, a confirmation screen is displayed. Click Close to close the screen.

Setting Up the Array

1. When discovery is complete, the name of the first storage array found is displayed under the Summary tab in MDSM.
2. The default name for the newly discovered storage array is Unnamed. If another name is displayed, click the down arrow next to that name and select Unnamed in the drop-down list.
3. Click the Initial Setup Tasks option to see links to the remaining post-installation tasks. For more information about each task, see the *Owner's Manual*. Perform these tasks in the order shown in Table 4-3.

NOTE: Before configuring the storage array, check the status icons on the **Summary** tab to ensure that the enclosures in the storage array are in an Optimal status. For more information on the status icons, see the *Owner's Manual* at **support.dell.com/manuals**.

Table A-2. Initial Setup Tasks Dialog Box

Task	Purpose
Rename the storage array	To provide a more meaningful name than the software-assigned label, *Unnamed*.
Set a storage array password	To restrict unauthorized access. MDSM may ask for a password before changing the configuration or performing a destructive operation.
Set up alert notifications Set up e-mail alerts Set up SNMP alerts	To notify individuals (by e-mail) and/or storage enterprise management consoles, such as Dell Management Console, (by SNMP) when a storage array component degrades or fails, or an adverse environmental condition occurs.
Configure a storage array	To create virtual disks and map them to hosts.

Step 2: Configure the iSCSI Ports on the Storage Array

By default, the iSCSI ports on the storage array are set to the following IPv4 settings:

```
Controller 0, Port 0: IP: 192.168.130.101 Subnet Mask:
255.255.255.0 Port: 3260

Controller 0, Port 1: IP: 192.168.131.101 Subnet Mask:
255.255.255.0 Port: 3260

Controller 0, Port 2: IP: 192.168.132.101 Subnet Mask:
255.255.255.0 Port: 3260

Controller 0, Port 3: IP: 192.168.133.101 Subnet Mask:
255.255.255.0 Port: 3260

Controller 1, Port 0: IP: 192.168.130.102 Subnet Mask:
255.255.255.0 Port: 3260
```

```
Controller 1, Port 1: IP: 192.168.131.102 Subnet Mask:
255.255.255.0 Port: 3260

Controller 1, Port 2: IP: 192.168.132.102 Subnet Mask:
255.255.255.0 Port: 3260

Controller 1, Port 3: IP: 192.168.133.102 Subnet Mask:
255.255.255.0 Port: 3260
```

NOTE: No default gateway is set.

To configure the iSCSI ports on the storage array:

1. From MDSM navigate to the Setup tab on the AMW. Click configure Ethernet management ports and then select Configure iSCSI Host Ports.
2. Configure the iSCSI ports on the storage array.

NOTE: Using static IPv4 addressing is recommended, although DHCP is supported.

The following settings are available (depending on your specific configuration) by clicking the Advanced button:

- Virtual LAN (VLAN) support—A VLAN is a network of different systems that behave as if they are connected to the same segments of a local area network (LAN) and are supported by the same switches and routers. When configured as a VLAN, a device can be moved to another location without being reconfigured. To use VLAN on your storage array, obtain the VLAN ID from your network administrator and enter it here.
- Ethernet priority—This parameter is set to determine a network access priority.
- TCP listening port—The port number on the storage array listens for iSCSI logins from host server iSCSI initiators.

  NOTE: The TCP listening port for the iSNS server is the port number the storage array controller uses to connect to an iSNS server. This allows the iSNS server to register the iSCSI target and portals of the storage array so that the host server initiators can identify them.
- Jumbo frames—Jumbo Ethernet frames are created when the maximum transmission units (MTUs) are larger than 1500 bytes per frame. This setting is adjustable port-by-port.

3 To enable ICMP PING responses for all ports, select Enable ICMP PING responses.

4 Click OK when all iSCSI storage array port configurations are complete.

5 Test the connection by performing a ping command on each iSCSI storage array port.

Step 3: Perform Target Discovery From the iSCSI Initiator

This step identifies the iSCSI ports on the storage array to the host server. Select the set of steps in one of the following sections (Microsoft Windows or Linux) that corresponds to your operating system.

If you are using *Microsoft Windows Server 2003* or *Windows Server 2008 GUI version*:

1 Click Start→ Programs→ Microsoft iSCSI Initiator or click Start→ All Programs→ Administrative Tools→ iSCSI Initiator.

2 Click the Discovery tab.

3 Under Target Portals, click Add and enter the IP address or DNS name of the iSCSI port on the storage array.

4 If the iSCSI storage array uses a custom TCP port, change the Port number. The default is 3260.

5 Click Advanced and set the following values on the General tab:

- Local Adapter—Must be set to Microsoft iSCSI Initiator.
- Source IP—The source IP address of the host you want to connect with.
- Data Digest and Header Digest—Optionally, you can specify that a digest of data or header information be compiled during transmission to assist in troubleshooting.
- CHAP logon information—Leave this option unselected and do not enter CHAP information at this point, unless you are adding the storage array to a SAN that has target CHAP already configured.

NOTE: IPSec is not supported.

6. Click OK to exit the Advanced menu and click OK again to exit the Add Target Portals screen.
7. To exit the Discovery tab, click OK.

If you plan to configure CHAP authentication, do not perform discovery on more than one iSCSI port at this point. Go to "Step 4: Configure Host Access" on page 62.

If you do not plan to configure CHAP authentication, repeat step 1 thorough step 6 for all iSCSI ports on the storage array.

If you are using *Windows Server 2008 Core Versio*n:

1. Set the iSCSI initiator service to start automatically:

   ```
   sc \\<server_name> config msiscsi start= auto
   ```

2. Start the iSCSI service: `sc start msiscsi`
3. Add a target portal:

   ```
   iscsicli QAddTargetPortal
   <IP_address_of_iSCSI_port_on_storage array>
   ```

If you are using *Red Hat Enterprise Linux 5, Red Hat Enterprise Linux 6, SUSE Linux Enterprise Server 10*, or *SUSE Linux Enterprise Server 11*:

Configuration of the iSCSI initiator for Red Hat Enterprise Linux 5 and SUSE Linux Enterprise Server 10 SP1 distributions is done by modifying the /etc/iscsi/iscsid.conf file, which is installed by default when you install MDSM. You can edit the file directly, or replace the default file with a sample file included on the PowerVault MD series resource media.

To use the sample file included on the media:

1. Save the default /etc/iscsi/iscsid.conf file by naming it to another name of your choice.
2. Copy the appropriate sample file from /linux/etc on the media to /etc/iscsi/iscsid.conf.
3. Rename the sample file to iscsid.conf.
4. Edit the following entries in the /etc/iscsi/iscsid.conf file:
   a. Edit or verify that the `node.startup = manual` line is disabled.
   b. Edit or verify that the `node.startup = automatic` line is enabled. This enables automatic startup of the service at boot time.

c Verify that the following time-out value is set to 30:
`node.session.timeo.replacement_timeout = 30`

d Save and close the /etc/iscsi/iscsid.conf file.

5 From the console, restart the iSCSI service with the following command:
`service iscsi start`

6 Verify that the iSCSI service is running during boot using the following command from the console:

```
chkconfig  iscsi  on
```

7 To display the available iSCSI targets at the specified IP address, use the following command:

```
iscsiadm –m discovery –t st -p
<IP_address_of_iSCSI_port>
```

8 After target discovery, use the following command to manually log in:
`iscsiadm -m node –l`

This log in is performed automatically at startup if automatic startup is enabled.

9 Manually log out of the session using the following command:

```
iscsiadm -m node -T <initiator_username> -p
<target_ip> -u
```

Step 4: Configure Host Access

This step specifies which host servers access virtual disks on the storage array. You should perform this step:

- Before mapping virtual disks to host servers
- Any time you connect new host servers to the storage array

1 Launch MDSM.

2 Navigate to the AMW and click Manually define hosts.

3 At Enter host name, enter the host server for virtual disk mapping.

This can be an informal name, not necessarily a name used to identify the host server to the network.

4 Select a method for adding the host port identifier.

5 Select the host type.

6 Select whether or not the host server will be part of a host server group that shares access to the same virtual disks as other host servers. Select Yes only if the host is part of a Microsoft cluster.

7 Click Next.

8 Specify if this host will be part of a host group.

9 Click Finish.

Understanding CHAP Authentication

What is CHAP?

Challenge Handshake Authentication Protocol (CHAP) is an optional iSCSI authentication method where the storage array (target) authenticates iSCSI initiators on the host server. Two types of CHAP are supported

- Target CHAP
- Mutual CHAP

Target CHAP

In target CHAP, the storage array authenticates all requests for access issued by the iSCSI initiator(s) on the host server using a CHAP secret. To set up target CHAP authentication, you must enter a CHAP secret on the storage array, then configure each iSCSI initiator on the host server to send that secret each time it attempts to access the storage array.

Mutual CHAP

In addition to setting up target CHAP, you can set up mutual CHAP in which both the storage array and the iSCSI initiator authenticate each other. To set up mutual CHAP, configure the iSCSI initiator with a CHAP secret that the storage array must send to the host sever in order to establish a connection. In this two-way authentication process, both the host server and the storage array send information that the other must validate before a connection is allowed.

CHAP is an optional feature and is not required to use iSCSI. However, if you do not configure CHAP authentication, any host server connected to the same IP network as the storage array can read from and write to the storage array.

NOTE: When using CHAP authentication, you should configure it on both the storage array (using MDSM) and the host server (using the iSCSI initiator) before preparing virtual disks to receive data. If you prepare disks to receive data before you configure CHAP authentication, you lose visibility to the disks once CHAP is configured.

CHAP Definitions

To summarize the differences between target CHAP and mutual CHAP authentication, see Table A-3.

Table A-3. CHAP Types Defined

CHAP Type	Description
Target CHAP	Sets up accounts that iSCSI initiators use to connect to the target storage array. The target storage array then authenticates the iSCSI initiator.
Mutual CHAP	Applied in addition to target CHAP, mutual CHAP sets up an account that a target storage array uses to connect to an iSCSI initiator. The iSCSI initiator then authenticates the target.

Step 5: Configure CHAP Authentication on the Storage Array (Optional)

If you are configuring CHAP authentication of any kind (either target-only or target and mutual), you must complete this step and "Step 5: Configure CHAP Authentication on the Storage Array (Optional)" on page 64.

If you are not configuring any type of CHAP, skip these steps and go to "Step 7: Connect to the Target Storage Array From the Host Server" on page 70.

NOTE: If you choose to configure mutual CHAP authentication, you must first configure target CHAP.

In terms of iSCSI configuration, the term target always refers to the storage array.

Configuring Target CHAP Authentication on the Storage Array

1 From MDSM, click the iSCSI tab and then click Change Target Authentication.

Select one of the CHAP settings described in Table A-4.

Table A-4. CHAP Setting

Option	Description
None	This is the default selection. If None is the only selection, the storage array allows an iSCSI initiator to log on without supplying any type of CHAP authentication.
None and CHAP	The storage array allows an iSCSI initiator to log on with or without CHAP authentication.
CHAP	If CHAP is selected and None is deselected, the storage array requires CHAP authentication before allowing access.

2 To configure a CHAP secret, select CHAP and select CHAP Secret.

3 Enter the Target CHAP Secret (or Generate Random Secret). Confirm it in Confirm Target CHAP Secret and click OK.

Although the storage array allows sizes from 12 to 57 characters, many initiators only support CHAP secret sizes up to 16 characters (128-bit).

NOTE: A CHAP secret is not retrievable after it is entered. Ensure that you record the secret in an accessible place. If Generate Random Secret is used, copy and paste the secret into a text file for future reference since the same CHAP secret is used to authenticate any new host servers you may add to the storage array. If you forget this CHAP secret, you must disconnect all existing hosts attached to the storage array and repeat the steps in this chapter to re-add them.

4 Click OK.

Configuring Mutual CHAP Authentication on the Storage Array

The initiator secret must be unique for each host server that connects to the storage array and must not be the same as the target CHAP secret.

Change the initiator authentication settings in the Change Target Authentication window. Use these options to change the settings:

- None—Select None if you permit no initiator authentication. If you select None, any initiator can access this target. Use this option only if you do not require secure data. However, you can select both None and CHAP at the same time.
- CHAP—Select CHAP if you want to enable an initiator that tries to access the target to authenticate using CHAP. Define the CHAP secret only if you want to use mutual CHAP authentication. If you select CHAP, and if no CHAP target secret is defined, an error message is displayed. Click CHAP Secret to view the Enter CHAP Secret windows. Use this window to define the CHAP secrets.

NOTE: To remove a CHAP secret, you must delete the host initiator and re-add it.

Step 6: Configure CHAP Authentication on the Host Server (Optional)

If you configured CHAP authentication in "Step 5: Configure CHAP Authentication on the Storage Array (Optional)" on page 64, complete the following steps. If not, skip to "Step 7: Connect to the Target Storage Array From the Host Server" on page 70.

Select the set of steps in one of the following sections (Windows or Linux) that corresponds to your operating system.

If you are using *Windows Server 2008 GUI version*:

1. Click Start→ Programs→ Microsoft iSCSI Initiator or click Start→ All Programs→ Administrative Tools→ iSCSI Initiator.
2. If you are not using mutual CHAP authentication, go to the step 4.
3. If you are using mutual CHAP authentication, click the General tab and select Secret. At Enter a secure secret, enter the mutual CHAP secret you entered for the storage array
4. Click the Discovery tab.

5 Under Target Portals, select the IP address of the iSCSI port on the storage array and click Remove.

The iSCSI port you configured on the storage array during target discovery disappears.

6 Under Target Portals, click Add and re-enter the IP address or DNS name of the iSCSI port on the storage array (removed above).

7 Click Advanced and set the following values on the General tab:

- Local Adapter—Should always be set to Microsoft iSCSI Initiator.
- Source IP—The source IP address of the host you want to connect with.
- Data Digest and Header Digest—Optionally, you can specify that a digest of data or header information be compiled during transmission to assist in troubleshooting.
- CHAP logon information—Enter the target CHAP authentication user name and secret you entered (for the host server) on the storage array.
- Perform mutual authentication—If mutual CHAP authentication is configured, select this option.

NOTE: IPSec is not supported.

8 Click OK.

If you require a discovery session failover, repeat step 5 and step 6 (in this step) for all iSCSI ports on the storage array. Otherwise, single-host port configuration is sufficient.

NOTE: If the connection fails, ensure that all IP addresses are entered correctly. Mistyped IP addresses result in connection problems.

If you are using *Windows Server 2008 Core version*:

1 Set the iSCSI initiator services to start automatically (if not already set):
`sc \\<server_name> config msiscsi start= auto`

2 Start the iSCSI service (if necessary): `sc start msiscsi`

3 If you are not using mutual CHAP authentication, go to step 5.

4 Enter the mutual CHAP secret you entered for the storage array:
`iscsicli CHAPSecret <secret>`

5 Remove the target portal that you configured on the storage array during target discovery:

```
iscsicli RemoveTargetPortal <IP_address>
<TCP_listening_port>
```

6 Add the target portal with CHAP defined:

```
iscsicli QAddTargetPortal
<IP_address_of_iSCSI_port_on_storage_array>
[CHAP_username]

[CHAP_password]
```

where, [CHAP_username] is the initiator name and [CHAP_password] is the target CHAP secret.

If you require a discovery session failover, repeat step 5 for all iSCSI ports on the storage array. Otherwise, single-host port configuration is sufficient.

If you are using *Red Hat Enterprise Linux 5*, *Red Hat Enterprise Linux 6*, *SUSE Linux Enterprise Server 10*, or *SUSE Linux Enterprise Server 11*:

1 To enable CHAP (optional), the following line needs to be enabled in your /etc/iscsi/iscsid.conf file:

```
node.session.auth.authmethod = CHAP
```

2 To set a user name and password for CHAP authentication of the initiator by the target(s), edit the following lines:

```
node.session.auth.username =
<iscsi_initiator_username>

node.session.auth.password =
<CHAP_initiator_password>
```

3 If you are using Mutual CHAP authentication, you can set the user name and password for CHAP authentication of the target(s) by the initiator by editing the following lines:

```
node.session.auth.username_in=
<iscsi_target_username>

node.session.auth.password_in =
<CHAP_target_password>
```

4 To set up discovery session CHAP authentication, first uncomment the following line:

```
discovery.sendtargets.auth.authmethod  =  CHAP
```

5 Set a user name and password for a discovery session CHAP authentication of the initiator by the target(s) by editing the following lines:

```
discovery.sendtargets.auth.username =
<iscsi_initiator_username>
```

```
discovery.sendtargets.auth.password =
<CHAP_initiator_password>
```

6 To set the user name and password for discovery session CHAP authentication of the target(s) by the initiator for Mutual CHAP, edit the following lines:

```
discovery.sendtargets.auth.username =
<iscsi_target_username>
```

```
discovery.sendtargets.auth.password_in =
<CHAP_target_password>
```

7 The final configuration contained in the /etc/iscsi/iscsid.conf file might look like this:

```
node.session.auth.authmethod = CHAP
```

```
node.session.auth.username = iqn.2005-
03.com.redhat01.78b1b8cad821
```

```
node.session.auth.password  =  password_1
```

```
node.session.auth.username_in= iqn.1984-
05.com.dell:powervault.123456
```

```
node.session.auth.password_in  =  test1234567890
```

```
discovery.sendtargets.auth.authmethod  =  CHAP
```

```
discovery.sendtargets.auth.username = iqn.2005-
03.com.redhat01.78b1b8cad821
```

```
discovery.sendtargets.auth.password  =  password_1
```

```
discovery.sendtargets.auth.username = iqn.1984-
05.com.dell:powervault.123456

discovery.sendtargets.auth.password_in =
test1234567890
```

If you are using *SUSE Linux Enterprise Server SP3 using the GUI*:

1. Click Desktop→ YaST→ iSCSI Initiator.
2. Click Service Start, then select When Booting.
3. Select Discovered Targets, then select Discovery.
4. Enter the IP address of the port.
5. Click Next.
6. Select any target that is not logged in and click Log in.
7. Select one:
   - If you are not using CHAP authentication, select No Authentication. Go to step 8.

     or

   - If you are using CHAP authentication, enter the CHAP user name and password. To enable Mutual CHAP, select and enter the Mutual CHAP user name and password.
8. Repeat step 7 for each target until at least one connection is logged in for each controller.
9. Go to Connected Targets.
10. Verify that the targets are connected and displays a status of true.

Step 7: Connect to the Target Storage Array From the Host Server

If you are using *Windows Server 2008 GUI*:

1. Click Start→ Programs→ Microsoft iSCSI Initiator or click Start→ All Programs→ Administrative Tools→ iSCSI Initiator.
2. Click the Targets tab.

   If previous target discovery was successful, the iqn of the storage array should be displayed under Targets.

3 Click Log On.

4 Select Automatically restore this connection when the system boots.

5 Select Enable multi-path.

6 Click Advanced and configure the following settings under the General tab:

- Local Adapter—Must be set to Microsoft iSCSI Initiator.
- Source IP—The source IP address of the host server you want to connect from.
- Target Portal—Select the iSCSI port on the storage array controller that you want to connect to.
- Data Digest and Header Digest—Optionally, you can specify that a digest of data or header information be compiled during transmission to assist in troubleshooting.
- CHAP logon information—If CHAP authentication is required, select this option and enter the Target secret.
- Perform mutual authentication—If mutual CHAP authentication is configured, select this option.

NOTE: IPSec is not supported.

7 Click OK.

To support storage array controller failover, the host server must be connected to at least one iSCSI port on each controller. Repeat step 3 through step 8 for each iSCSI port on the storage array that you want to establish as failover targets. The Target Portal address is different for each port you connected to.

NOTE: To enable the higher throughput of multipathing I/O, the host server must connect to both iSCSI ports on each controller, ideally from separate host-side NICs. Repeat step 3 through step 7 for each iSCSI port on each controller. If using a duplex PowerVault MD32*xx*i configuration, then LUNs should also be balanced between the controllers.

The Status field on the Targets tab should now display as Connected.

8 Click OK to close the Microsoft iSCSI initiator.

NOTE: PowerVault MD32*xx*i supports only round robin load-balancing policies.

If you are using *Windows Server 2008 Core Version*:

1. Set the iSCSI initiator services to start automatically (if not already set):
   `sc \\<server_name> config msiscsi start= auto`
2. Start the iSCSI service (if necessary): `sc start msiscsi`
3. Log on to the target:

   ```
   iscsicli PersistentLoginTarget <Target_Name>
   <Report_To_PNP> <Target_Portal_Address>
   <TCP_Port_Number_Of_Target_Portal> * * *

   <Login_Flags> * * * * * <Username> <Password>
   <Authtype> * <Mapping_Count>
   ```

   where

   - < *Target_Name* > is the target name as displayed in the target list. Use the iscsicli ListTargets command to display the target list.
   - < *Report_To_PNP* > is T, which exposes the LUN to the operating system as a storage device.
   - < *Target_Portal_Address* > is the IP address of the iSCSI port on the controller being logged in to.
   - < *TCP_Port_Number_Of_Target_Portal* > is 3260.
   - < *Login_Flags* > is 0x2 to enable multipathing for the target on the initiator. This value allows more than one session to be logged in to a target at one time.
   - < *Username* > is the initiator name.
   - < *Password* > is the target CHAP secret.
   - < *Authtype* > is either 0 for no authentication, 1 for Target CHAP, or 2 for Mutual CHAP.

   : **NOTE:** <*Username*>, <*Password*> and <*Authtype*> are optional parameters. They can be replaced with an asterisk (*) if CHAP is not used.

   - < *Mapping_Count* > is 0, indicating that no mappings are specified and no further parameters are required.

* * * An asterisk (*) represents the default value of a parameter.

For example, your log on command might look like this:

```
iscsicli PersistentLoginTarget iqn.1984-
05.com.dell:powervault.6001372000ffe3332xx0000046
72edf2 3260 T 192.168.130.101 * * * 0x2 * * * * *
*  *  *  *  0
```

To view active sessions to the target, run the following command:

```
iscsicli SessionList
```

To support storage array controller failover, the host server must be connected to at least one iSCSI port on each controller. Repeatstep 3 for each iSCSI port on the storage array that you want to establish as a failover target. The *Target_ Portal_Address* is different for each port you connect to.

PersistentLoginTarget does not initiate a login to the target until after the system is rebooted. To establish immediate login to the target, substitute LoginTarget for PersistentLoginTarget.

: **NOTE:** See the *Microsoft iSCSI Software Initiator 2.x User's Guide* for more information about the commands used in the previous steps. For more information about Windows Server 2008 Server Core, see the Microsoft Developers Network (MSDN) at microsoft.com.

If you are using a *Linux Server*:

In MDSM, the Configure iSCSI Host Ports displays the status of each iSCSI port you attempt to connect and the configuration state of all IP addresses. If either displays Disconnected or Unconfigured, respectively, check the following and repeat the iSCSI configuration steps:

- Are all cables securely attached to each port on the host server and storage array?
- Is TCP/IP correctly configured on all target host ports?
- Is CHAP set up correctly on both the host server and the storage array?

To review optimal network setup and configuration settings, see "Guidelines for Configuring Your Network for iSCSI" on page 49.

Step 8: (Optional) Set Up In-Band Management

Out-of-band management (see "Step 1: Discover the Storage Array (Out-of-band Management Only)" on page 56) is the recommended method for managing the storage array. However, to optionally set up in-band management, use the steps shown below.

The default iSCSI host port IPv4 addresses are shown below for reference:

Controller 0, Port 0: IP: 192.168.130.101 Controller 0, Port 1: IP: 192.168.131.101

Controller 0, Port 0: IP: 192.168.132.101 Controller 0, Port 1: IP: 192.168.133.101

Controller 1, Port 0: IP: 192.168.130.102 Controller 1, Port 1: IP: 192.168.131.102

Controller 1, Port 0: IP: 192.168.132.102 Controller 1, Port 1: IP: 192.168.133.102

NOTE: The management station you are using must be configured for network communication to the same IP subnet as the PowerVault MD32*xxi* host ports.

1. Establish an iSCSI session to the PowerVault MD3200i RAID storage array.
2. Restart the SMagent service.
3. Launch MDSM.

   If this is the first storage array to be set up for management, the Add New Storage Array window is displayed. Otherwise, click New.
4. Select Manual and click OK.
5. Select In-band management and enter the host server name(s) or IP address(es) of the host server that is running the PowerVault MD Storage Manager software.
6. Click Add.

   In-band management should now be successfully configured.

B

Appendix—Using Internet Storage Naming Service

Internet Storage Naming Service (iSNS) server, supported only on Microsoft Windows iSCSI environments, eliminates the need to manually configure each individual storage array with a specific list of initiators and target IP addresses. Instead, iSNS automatically discovers, manages, and configures all iSCSI devices in your environment.

For more information on iSNS, including installation and configuration, see microsoft.com.

C

Appendix—Load Balancing

Load Balance Policy

Multi-path drivers select the I/O path to a virtual disk through a specific RAID controller module. When the multi-path driver receives a new I/O to process, the driver tries to find a path to the current RAID controller module that owns the virtual disk. If the path to the current RAID controller module that owns the virtual disk cannot be found, the multi-path driver migrates the virtual disk ownership to the secondary RAID controller module. When multiple paths to the RAID controller module that owns the virtual disk exist, you can choose a load balance policy to determine which path is used to process I/O. Multiple options for setting the load balance policies let you optimize I/O performance when mixed host interfaces are configured.

You can choose one of the following load balance policies to optimize I/O performance:

- Round robin with subset
- Least queue depth with subset
- Least path weight with subset (Windows operating systems only)

Round Robin With Subset

The round robin with subset I/O load balance policy routes I/O requests, in rotation, to each available data path to the RAID controller module that owns the virtual disks. This policy treats all paths to the RAID controller module that owns the virtual disk equally for I/O activity. Paths to the secondary RAID controller module are ignored until ownership changes. The basic assumption for the round-robin policy is that the data paths are equal. With mixed host support, the data paths might have different bandwidths or different data transfer speeds.

Least Queue Depth With Subset

The least queue depth with subset policy is also known as the least I/Os or least requests policy. This policy routes the next I/O request to a data path that has the least outstanding I/O requests queued. For this policy, an I/O request is simply a command in the queue. The type of command or the number of blocks that are associated with the command are not considered.

The least queue depth with subset policy treats large block requests and small block requests equally. The data path selected is one of the paths in the path group of the RAID controller module that owns the virtual disk.

Least Path Weight With Subset

The least path weight with subset policy assigns a weight factor to each data path to a virtual disk. An I/O request is routed to the path with the lowest weight value to the RAID controller module that owns the virtual disk. If more than one data path to the virtual disk has the same weight value, the round-robin with subset path selection policy is used to route I/O requests between the paths with the same weight value. The least path weight with subset load balance policy is not supported on Linux operating systems.

Changing Load Balance Policies on the Windows Server 2008 Operating System

Load balancing with the MD3200i series storage array is only available for Windows Server 2008 and later versions of the operating system. You can change the load balance policies from the default round robin with subset by using either the:

- Device manager
- Disk management

To change the load balance policy using Windows Server 2008 device manager:

1. From the desktop of the host, right-click My Computer and select Manage to open the Computer Management dialog.
2. Click Device Manager to show the list of devices attached to the host.
3. Right-click on the multi-path disk device for which you want to set the load balance policies, then select Properties.
4. From the MPIO tab, select the load balance policy that you want to set for this disk device.

To change the load balance policy using Windows Server 2008 disk management:

1. From the desktop of the host, right-click My Computer and click Manage to open the Computer Management dialog.
2. Click Disk Management to show the list of virtual disks attached to the host.
3. Right-click on the virtual disk for which you want to set the load balance policy, then click Properties.

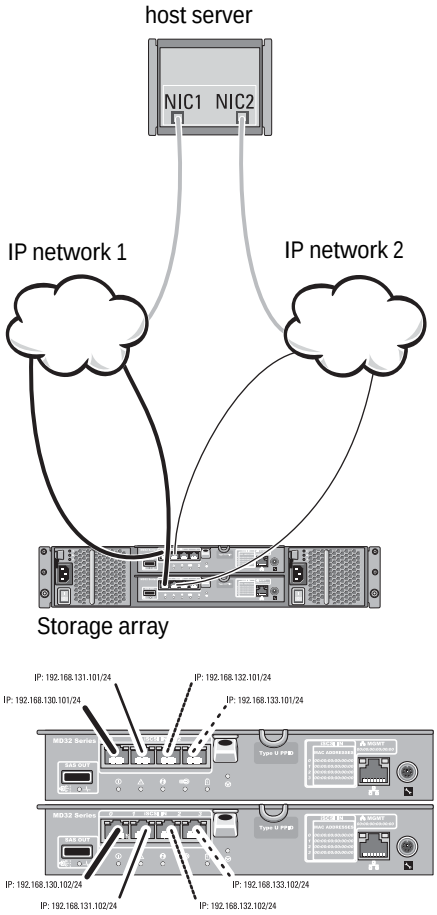
From the MPIO tab, select the load balance policy that you want to set for this virtual disk.

Increasing Bandwidth With Multiple iSCSI Sessions

The PowerVault MD3200i series storage array in a duplex configuration supports two active/active asymmetric redundant controllers. Each controller has four 1 Gbps Ethernet ports that support iSCSI. The bandwidth of the four ports on the same controller can be aggregated to provide optimal performance. A host can be configured to simultaneously use the bandwidth of both the ports on a controller to access virtual disks owned by the controller. The multi-path failover driver that Dell provides for the MD3200i series storage array can be used to configure the storage array so that all ports are used for simultaneous I/O access. If the multi-path driver detects multiple paths to the same virtual disk through the ports on the same controller, it load-balances I/O access from the host across all ports on the controller.

Figure C-1 illustrates how the initiator can be configured to take advantage of the load balancing capabilities of the multi-path failover driver.

Figure C-1. Initiator Configuration



IP Addresses
Host
If1: IP_Addr_If1
If2: IP_Addr_If2

MD32*xx*i Controller 0
P0: IP_Addr_C0_P0
P1: IP_Addr_C0_P1
P2: IP_Addr_C0_P2
P3: IP_Addr_C0_P3
MD32*xx*i Controller 1
P0: IP_Addr_C1_P0
P1: IP_Addr_C1_P1
P2: IP_Addr_C1_P2
P3: IP_Addr_C1_P3

TCP Connections
To MD32*xx*i Controller 0
T01: IP_Addr_If1 / IP_Addr_C0_P0
T02: IP_Addr_If2 / IP_Addr_C1_P1
T03: IP_Addr_If3 / IP_Addr_C1_P2
T04: IP_Addr_If4 / IP_Addr_C1_P3
To MD32*xx*i Controller 1
T11: IP_Addr_If1 / IP_Addr_C1_P0
T12: IP_Addr_If2 / IP_Addr_C1_P1
T13: IP_Addr_If3 / IP_Addr_C1_P2
T14: IP_Addr_If4 / IP_Addr_C1_P3

iSCSI Sessions
To MD32*xx*i Controller 0
Session 00: T01
Session 01: T02
Session 02: T03
Session 03: T04
To MD32*xx*i Controller 1
Session 10: T11
Session 11: T12
Session 12: T13
Session 14: T14

Two sessions with one TCP connection are configured from the host to each controller (one session per port), for a total of four sessions. The multi-path failover driver balances I/O access across the sessions to the ports on the same controller. In a duplex configuration, with virtual disks on each controller, creating sessions using each of the iSCSI data ports of both controllers increases bandwidth and provides load balancing.

D

Appendix—Stopping and Starting iSCSI Services in Linux

To manually stop the iSCSI services in Linux, certain steps must be followed to maintain parallel processing between the storage array and the host server.

1. Stop all I/O.
2. Unmount all correlated file systems. Stop iSCSI service by running the following command:

   ```
   /etc/init.d/open-iscsi stop
   ```