HITACHI
Inspire the Next

Hitachi AMS 2000 Family Host Installation Guide for iSCSI

FASTFIND LINKS

Hitachi Data Systems

MK-08DF8188-07

Table of Contents

Preface

This document provides guidelines on how to connect an Hitachi AMS 2000 Family iSCSI array to the following host operating systems:

- Microsoft Windows 2000 (Service Pack 4), Windows XP Windows 2003 (Service Pack 1), and Windows 2008
- Solaris
- VMware
- Red Hat Enterprise Linux
- SuSE Linux Enterprise Server
- Asianux
- IBM AIX
- HP-UX

This guide also provides information on where to find resources to ensure proper functioning between the array and the host. Please read this document carefully to understand how to implement your operating system with the Hitachi array using iSCSI. It is recommended that you maintain a copy for reference purposes.

NOTE: This guide assumes that the array is installed and functioning correctly. If it is not, install the system before reading this guide. Refer to your array user's guide and quick installation guide for more information.

Notice: The use of the Hitachi array and all Hitachi Data Systems products is governed by the terms of your agreement(s) with Hitachi Data Systems.

Document Revision Level

This section provides a history of the revision changes to this document.

Revision	Date	Description
MK-08DF8188-00	December 2008	Initial Release
MK-08DF8188-01	December 2008	Supersedes and replaces MK-08DF8188-00
MK-08DF8188-02	February 2009	Supersedes and replaces MK-08DF8188-01
MK-08DF8188-03	April 2009	Supersedes and replaces MK-08DF8188-02
MK-08DF8188-04	August 2009	Supersedes and replaces MK-08DF8188-03
MK-08DF8188-05	November 2009	Supersedes and replaces MK-08DF8188-04
MK-08DF8188-06	January 2010	Supersedes and replaces MK-08DF8188-05
MK-08DF8188-07	April 2010	Supersedes and replaces MK-08DF8188-06

Changes in this Revision

- Changed Related Documents section in Preface.
- In Setting Microsoft iSCSI MPIO on Windows 2000 and 2003 on page 2-10, removed statement that said the Hitachi array only supports the Failover Only load balancing policy. Do not select other policies.

Intended Audience

This document is intended for system administrators, Hitachi Data Systems representatives, Authorized Service Providers, and modular storage customers who are involved in verifying that the LUNs connected to the host server are discovered by the array and can be used by the operating system and other applications. It also assumes the user is familiar with the following:

- Your Hitachi array and the LUN configurations described in supporting Hitachi documents.
- Your server hardware and operating system.
- UNIX® file system, system commands, and utilities (if applicable).
- Direct-access storage device (DASD) systems and their basic functions (if applicable).

In addition, you should be familiar with your server's iSCSI HBAs, network-interface cards (NICs), and iSCSI initiator.

For the latest information about operating systems supported by your array, refer to Hitachi's interoperability information at:

http://www.hds.com/products/interoperability/

Document Organization

The following table provides an overview of the contents and organization of this document. Click the chapter title in the first column to go to that chapter. The first page of every chapter or appendix contains a brief list of the contents of that section of the manual, with links to the pages where the information is located.

Chapter/Appendix Title	Description
Chapter 1, System Configuration Prerequisites	Describes the prerequisites for setting up an array to work with supported hosts.
Chapter 2, Microsoft Windows	Describes how to connect a Windows host to the array.
Chapter 3, Solaris	Describes how to connect a Solaris host to the array.
Chapter 4, VMware	Describes how to connect a VMware host to the array.
Chapter 5, Red Hat Enterprise Linux	Describes how to connect a Red Hat Enterprise Linux host to the array.
Chapter 6, SuSE Linux Enterprise Server	Describes how to connect an SUSE Linux Enterprise Server host to the array.
Chapter 7, Asianux	Describes how to connect an Asianux host to the array.
Chapter 8, IBM AIX	Describes how to connect an IBM AIX host to the array.
Chapter 9, HP-UX	Describes how to connect an HP-UX host to the array.
Chapter 10, Troubleshooting	Contains troubleshooting information you can use in the unlikely event you encounter a problem with your array.
Glossary	Defines special terms and acronyms used in this document.
Index	Provides links to specific information in this manual.

Related Documents

Hitachi Data Systems offers a complete library of user and online documentation to ensure you get the most out of the Hitachi AMS 2000 Family storage systems.

The entire documentation set for the Hitachi AMS 2000 Family storage systems can be accessed on the documentation CD supplied with your storage system and through downloads from the Hitachi Web Portal at:

support.hds.com

This documentation set consists of the following documents.

Release Notes

- Hitachi Adaptable Modular Storage System Release Notes (RN-AMS100)
- Hitachi Storage Navigator Modular 2 Release Notes (RN-SNM2)

Please read the Release Notes before installing and/or using this product. They may contain requirements and/or restrictions not fully described in this document, along with updates and/or corrections to this document.

Installation and Getting Started

Hitachi Data Systems offers a complete library of user and online documentation to ensure you get the most out of the Hitachi AMS 2000 Family storage systems.

The entire documentation set for the Hitachi AMS 2000 Family storage systems can be accessed on the documentation CD supplied with your storage system and through downloads from the Hitachi Web Portal at:

support.hds.com

This documentation set consists of the following documents.

Release Notes

- Hitachi Adaptable Modular Storage System Release Notes (RN-AMS100)
- Hitachi Storage Navigator Modular 2 Release Notes (RN-SNM2)

Please read the Release Notes before installing and/or using this product. They may contain requirements and/or restrictions not fully described in this document, along with updates and/or corrections to this document.

Installation and Getting Started

The following documents provide instructions for installing an AMS 2000 Family storage system. They include rack information, safety information, site-preparation instructions, getting-started guides for experienced users, and host connectivity information. The symbol ☞ identifies documents that contain initial configuration information about Hitachi AMS 2000 Family storage systems.

☞ **Hitachi AMS2100/2300 Getting Started Guide** (MK-98DF8152)

Provides quick-start instructions for getting an AMS 2100 or AMS 2300 storage system up and running as quickly as possible.

☞ **Hitachi AMS2500 Getting Started Guide** (MK-97DF8032)

Provides quick-start instructions for getting an AMS 2500 storage system up and running as quickly as possible.

Hitachi AMS 2000 Family Site Preparation Guide (MK-98DF8149)

Contains initial site planning and pre-installation information for AMS 2000 Family storage systems, expansion units, and high-density expansion units. This document also covers safety precautions, rack information, and product specifications.

Hitachi AMS 2000 Family Fibre Channel Host Installation Guide (MK-08DF8189)

Describes how to prepare Hitachi AMS 2000 Family Fibre Channel storage systems for use with host servers running supported operating systems.

Hitachi AMS 2000 Family iSCSI Host Installation Guide (MK-08DF8188) — this document

Describes how to prepare Hitachi AMS 2000 Family iSCSI storage systems for use with host servers running supported operating systems.

Storage and replication features

The following documents describe how to use Storage Navigator Modular 2 (Navigator 2) to perform storage and replication activities.

Hitachi Storage Navigator 2 Advanced Settings User's Guide (MK-97DF8039)

Contains advanced information about launching and using Navigator 2 in various operating systems, IP addresses and port numbers, server certificates and private keys, boot and restore options, outputting configuration information to a file, and collecting diagnostic information.

Hitachi Storage Navigator Modular 2 User's Guide (MK-99DF8208)

Describes how to use Navigator 2 to configure and manage storage on an AMS 2000 Family storage system.

Hitachi AMS 2000 Family Dynamic Provisioning Configuration Guide (MK-09DF8201)

Describes how to use virtual storage capabilities to simplify storage additions and administration.

Hitachi Storage Navigator 2 Storage Features Reference Guide for AMS (MK-97DF8148)

Contains concepts, preparation, and specifications for Account Authentication, Audit Logging, Cache Partition Manager, Cache Residency Manager, Data Retention Utility, LUN Manager, Performance Monitor, SNMP Agent, and Modular Volume Migration.

Hitachi AMS 2000 Family Copy-on-write SnapShot User Guide (MK-97DF8124)

Describes how to create point-in-time copies of data volumes in AMS 2100, AMS 2300, and AMS 2500 storage systems, without impacting host service and performance levels. Snapshot copies are fully read/write compatible with other hosts and can be used for rapid data restores, application testing and development, data mining and warehousing, and nondisruptive backup and maintenance procedures.

Hitachi AMS 2000 Family ShadowImage In-system Replication User Guide (MK-97DF8129)

Describes how to perform high-speed nondisruptive local mirroring to create a copy of mission-critical data in AMS 2100, AMS 2300, and AMS 2500 storage systems. ShadowImage keeps data RAID-protected and fully recoverable, without affecting service or performance levels. Replicated data volumes can be split from host applications and used for system backups, application testing, and data mining applications while business continues to operate at full capacity.

Hitachi AMS 2000 Family TrueCopy Remote Replication User Guide (MK-97DF8052)

Describes how to create and maintain multiple duplicate copies of user data across multiple AMS 2000 Family storage systems to enhance your disaster recovery strategy.

Hitachi AMS 2000 Family TrueCopy Extended Distance User Guide (MK-97DF8054)

Describes how to perform bi-directional remote data protection that copies data over any distance without interrupting applications, and provides failover and recovery capabilities.

Hitachi AMS 2000 Data Retention Utility User's Guide (MK-97DF8019)

Describes how to lock disk volumes as read-only for a certain period of time to ensure authorized-only access and facilitate immutable, tamper-proof record retention for storage-compliant environments. After data is written, it can be retrieved and read only by authorized applications or users, and cannot be changed or deleted during the specified retention period.

Hitachi Storage Navigator Modular 2 online help

Provides topic and context-sensitive help information accessed through the Navigator 2 software.

Hardware maintenance and operation

The following documents describe how to operate, maintain, and administer an AMS 2000 Family storage system. They also provide a wide range of technical information and specifications for the AMS 2000 Family storage systems. The symbol ☞ identifies documents that contain initial configuration information about Hitachi AMS 2000 Family storage systems.

☞ **Hitachi AMS 2100/2300 Storage System Hardware Guide** (MK-97DF8010)

Provides detailed information about installing, configuring, and maintaining AMS 2100 and 2300 storage systems.

☞ **Hitachi AMS 2500 Storage System Hardware Guide** (MK-97DF8007)

Provides detailed information about installing, configuring, and maintaining an AMS 2500 storage system.

☞ **Hitachi AMS 2000 Family Storage System Reference Guide** (MK-97DF8008)

Contains specifications and technical information about power cables, system parameters, interfaces, logical blocks, RAID levels and configurations, and regulatory information about AMS 2100, AMS 2300, and AMS 2500 storage systems. This document also contains remote adapter specifications and regulatory information.

Hitachi AMS 2000 Family Storage System Service and Upgrade Guide (MK-97DF8009)

Provides information about servicing and upgrading AMS 2100, AMS 2300, and AMS 2500 storage systems.

Hitachi AMS 2000 Family Power Savings User Guide (MK-97DF8045)

Describes how to spin down volumes in selected RAID groups when they are not being accessed by business applications to decrease energy consumption and significantly reduce the cost of storing and delivering information.

Command and Control (CCI)

The following documents describe how to install the Hitachi AMS 2000 Family Command Control Interface (CCI) and use it to perform TrueCopy and ShadowImage operations.

Hitachi AMS 2000 Family Command Control Interface (CCI) Installation Guide (MK-97DF8122)

Describes how to install CCI software on open-system hosts.

Hitachi AMS 2000 Family Command Control Interface (CCI) Reference Guide (MK-97DF8121)

Contains reference, troubleshooting, and maintenance information related to CCI operations on AMS 2100, AMS 2300, and AMS 2500 storage systems.

Hitachi AMS 2000 Family Command Control Interface (CCI) User's Guide (MK-97DF8123)

Describes how to use CCI to perform TrueCopy and ShadowImage operations on AMS 2100, AMS 2300, and AMS 2500 storage systems.

Command Line Interface (CLI)

The following documents describe how to use Hitachi Storage Navigator Modular 2 to perform management and replication activities from a command line.

Hitachi Storage Navigator Modular 2 Command Line Interface (CLI) Unified Reference Guide (MK-97DF8089)

Describes how to interact with all Navigator 2 bundled and optional software modules by typing commands at a command line.

Hitachi Storage Navigator 2 Command Line Interface Replication Reference Guide for AMS (MK-97DF8153)

Describes how to interact with Navigator 2 to perform replication activities by typing commands at a command line.

Hitachi Dynamic Replicator documentation

The following documents describe how to install, configure, and use Hitachi Dynamic Replicator to provide AMS Family storage systems with continuous data protection, remote replication, and application failover in a single, easy-to-deploy and manage platform.

Hitachi Dynamic Replicator - Scout Release Notes (RN-99DF8211)

Hitachi Dynamic Replicator - Scout Host Administration Guide (MK-98DF8212)

Hitachi Dynamic Replicator - Scout Installation and Configuration Guide (MK-98DF8213)

Hitachi Dynamic Replicator - Scout Quick Start Guide (MK-98DF8214)

Hitachi Dynamic Replicator - Scout Host Troubleshooting Guide (MK-98DF8215)

Hitachi Dynamic Replicator DR-Scout ICAT Utility Guide (MK-98DF8216)

Hitachi Dynamic Replicator - Scout RX Server Deployment Guide (MK-98DF8217)

Hitachi Dynamic Replicator VX Solution for Oracle (Solaris) (MK-98DF8218)

Hitachi Dynamic Replicator - Scout Solution for SharePoint 2007 (MK-98DF8219)

Hitachi Dynamic Replicator - Scout Solution for MySQL (Windows) (MK-98DF8220)

Protecting Citrix XenServer Using Hitachi Dynamic Replicator - Scout (MK-98DF8221)

Hitachi Dynamic Replicator Quick Install/Upgrade Guide (MK-98DF8222)

Hitachi Dynamic Replicator - Scout Protecting MS SQL Server (MK-98DF8223)

Hitachi Dynamic Replicator - Scout - Protecting Microsoft Exchange Server (MK-98DF8224)

Hitachi Dynamic Replicator - Scout File Server Solution (MK-98DF8225)

Hitachi Dynamic Replicator - Scout ESX - Protecting ESX Server (RCLI) (MK-99DF8226)

Related Web Sites

Before you install iSCSI initiators, NICs, iSCSI HBAs and drivers, verify they are supported by your array and operating system by referring to the following Web sites:

- For devices supported by your array, check the interoperability information at http://www.hds.com/products/interoperability/.
- For information about iSCSI initiators, iSCSI HBAs, and NICs (including latest HBA/NIC drivers and BIOSes), check the vendor Web sites.
- Operating systems-related issues, check the Web site for your operating system.
  - For Microsoft Windows: http://www.microsoft.com/en/us/default.aspx
  - For Solaris: http://www.sun.com/
  - For VMware: http://www.vmware.com/

    In addition, a best practices document entitled *Hitachi Adaptable Modular Storage 2000 Family Best Practices for VMware Virtual Infrastructure*, is available to download from the following site:

    http://www.hds.com/solutions/applications/vmware.htmls
  - For Red Hat Enterprise Linux: http://www.redhat.com
  - For SuSE Linux Enterprise Server: http://www.novell.com/
  - For Asianux: http://www.asianux.com/asianux.do
  - For IBM AIX: http://www.ibm.com/us/
  - For HP-UX: http://www.hp.com

NOTE: Hitachi Data Systems is not responsible for the availability of third-party Web sites mentioned in this document. Hitachi Data Systems does not endorse and is not responsible or liable for any content advertising, products, or other materials that are available on or through such sites or resources. Hitachi Data Systems will not be responsible or liable for any actual or alleged damage or loss caused by or in connection with the use of or reliance on any such content goods, or services that are available on or through such sites or resources.

Document Conventions

This document uses the following conventions to draw your attention to certain information.

Safety and Warnings

This document also uses the following symbols to draw your attention to certain information.

Symbol	Meaning	Description
	Tip	Tips provide helpful information, guidelines, or suggestions for performing tasks more effectively.
	Note	Notes emphasize or supplement important points of the main text.
	Caution	Cautions indicate that failure to take a specified action could result in damage to the software or hardware.
	WARNING	Warnings indicate that failure to take a specified action could result in loss of data or serious damage to the hardware.
	DANGER	The Danger symbol warns users of possible injury or death if instructions are not followed.
	ELECTRIC SHOCK HAZARD!	This symbol warns users of electric shock hazard. Failure to take appropriate precautions such as not opening or touching hazardous areas of the equipment could result in injury or death.
	Electrostatic Sensitive	The ESD symbol warns users that the equipment is sensitive to electrostatic discharge (ESD) and could be damaged if users do not take appropriate precautions such as using a grounded wrist strap when touching or handling the equipment.
	Burn Hazard	HOT SURFACE! Turn off power and allow to cool before touching.
	Sharp Edges or Corners	WARNING! Sharp edges or corners.Avoid touching or wear gloves

Typographic Conventions

The following typographic conventions are used in this document.

Convention	Description
Bold	Indicates text on a window, other than the window title, including menus, menu options, buttons, fields, and labels. Example: Click OK.
Italic	Indicates a variable, which is a placeholder for actual text provided by the user or system. Example: copy source-file target-file.
< > angled brackets	Indicates a variable, which is a placeholder for actual text provided by the user or system. Example: # pairdisplay -g <group>
screen/code	Indicates text that is displayed on screen or entered by the user. Example: # pairdisplay -g oradb
[ ] square brackets	Indicates optional values. Example: [a | b] indicates that you can choose a, b, or nothing.
{ } braces	Indicates required or expected values. Example: { a | b } indicates that you must choose either a or b.
| vertical bar	Indicates that you have a choice between two or more options or arguments. Examples: [a | b] indicates that you can choose a, b, or nothing. { a | b } indicates that you must choose either a or b.
underline	Indicates the default value. Example: [a | b]

Convention for Storage Capacity Values

Storage capacity values for hard disk drives (HDDs) in Hitachi Data Systems' storage products are calculated based on the following values:

- 1 KB = 1,000 bytes
- 1 MB = $1,000^2$ bytes
- 1 GB = $1,000^3$ bytes
- 1 TB = $1,000^4$ bytes

For further information on Hitachi Data Systems products and services, please contact your Hitachi Data Systems account team, or visit Hitachi Data Systems online at http://www.hds.com.

Getting Help

Support Contact Information

If you purchased this product from an authorized Hitachi Data Systems reseller, contact that reseller for support. For the name of your nearest Hitachi Data Systems authorized reseller, refer to the Hitachi Data Systems support website for locations and contact information.

To contact the Hitachi Data Systems Support Center, please visit the Hitachi Data Systems website for current telephone numbers and other contact information. https://extranet.hds.com/http://aim.hds.com/portal/dt

Please provide at least the following information about the problem:

- Product name, model number, part number (if applicable) and serial number
- System configuration, including names of optional features installed, host connections, and storage configuration such as RAID groups and LUNs
- Operating system name and revision or service pack number
- Exact content of any error message(s) displayed on the host system(s)
- The circumstances surrounding the error or failure
- A detailed description of the problem and what has been done to try to solve it

Hitachi Data Systems Support Web site

The following pages on the Hitachi Data Systems support Web site contain other further help and contact information:

Home Page: https://extranet.hds.com/http://aim.hds.com/portal/dt

Comments

Please send us your comments on this document: doc.comments@hds.com. Include the document title, number, and revision, and refer to specific section(s) and paragraph(s) whenever possible.

Thank you! (All comments become the property of Hitachi Data Systems Corporation.)

1

System Configuration Prerequisites

This chapter provides an overview of the tasks that need to be completed before you connect your host to a Hitachi storage array.

This chapter covers the following key topics:

- Planning Your Configuration
- Installation and Configuration Prerequisites
- Booting from a SAN-Attached Disk
- Vendor High Availability (HA) Cluster Configurations
- Upgrading the Firmware

Planning Your Configuration

There are several ways to configure your storage array. Therefore, before you connect the host server to the array, we recommend you plan your configuration. For more configuration information, refer to the user's guide for your array.

NOTE: Hitachi Data Systems recommends that the array not be directly connected to the network. Internet Small Computer System Interface (iSCSI) consumes nearly all Ethernet bandwidth, and iSCSI traffic disturbs network traffic.

Before implementing any configuration, decide whether the guidelines below are useful and appropriate for your needs:

- **CHAP authentication and LUN Manager.** Using CHAP authentication, LUN Manager, or both can prevent illegal access and isolate the IP-SAN completely from the external network.
- **iSNS.** Your array supports the iSNS client. If more than one array is running iSCSI with many targets, iSNS allows the host to discover the iSCSI target automatically. For this function to work, iSNS must be connected to the IP-SAN and be accessible from the array and the host.
- **iSCSI digest.** iSCSI digest is a feature found with software-based targets and iSCSI initiators that ensures high data integrity. If you enable this feature, system performance is reduced significantly. This occurs because software initiators depend on the host CPU for processing data digest, and data digest is a processor-intensive function. If the host processor is busy processing storage communication transactions, it has less CPU power available for its primary server operations.
- **Redundancy.** Redundancy on the I/O path between the host and array LUNs is created using multi-path software. Multipathing eliminates host system outages due to single-path I/O failures, thereby increasing system reliability.

Installation and Configuration Prerequisites

Table 1-1 on page 1-3 summarizes required installation and configuration tasks necessary for the host and system to work properly. It also includes references where you can find detailed information on each task. Verify the tasks outlined below have been completed before attempting to connect the Microsoft host to the array.

Table 1-1: Installation Tasks

Task	Reference
Install all array hardware and cabling. To avoid damage to the array or array components due to electrostatic discharge, wear an anti-static wrist strap when handling the array. Connect the clip to an unpainted part of the array chassis frame to safely channel any static electricity generated by your body to ground. If no wrist strap is available, ground yourself by touching an unpainted part of the array chassis frame.	Your array comes with all the hardware and cabling required for installation. Refer to the user's guide for your array.
Upgrade to the latest array firmware if necessary.	Refer to the following: • Latest Release Notes for your array • The user's guide for your array. • Storage Navigator Modular 2 (Navigator 2) online help.
Identify and configure the topology in which the array will be used.	Refer to the user's guide for your array.
Set the iSCSI port parameter on the array, if appropriate for your operating system.	Use Navigator 2 and refer to the online help.
Set the IP address, subnet mask, and default gateway for each iSCSI port.	Use Navigator 2 and refer to the online help.
If you use iSNS server, set the IP address and port number for iSNS server to each iSCSI port of the array.	Use Navigator 2 and refer to the 2 online help.
Create a target and assign the appropriate hosts to that target. If two or more hosts will be accessing one iSCSI data port, use LUN Manager to create a host group for each host.	Refer to the chapter on LUN Manager in the *Hitachi Storage Navigator Modular 2 Storage Features Reference Guide for Adaptable Modular Storage,* and Navigator 2 online help.
Set the host group operation parameters and targets using Storage Navigator Modular 2. If you choose the platform and middleware parameter, the required option is set automatically. If there is no corresponding parameter for the connected host environment, select **not specified**.	Use Navigator 2. Refer to the user's guide for your array and the Navigator 2 online help.
Set CHAP security if required.	See the following: • The section on CHAP authentication in the chapter appropriate to your OS. • Navigator 2 online help. • Your vendor's Web site.
Create and set LU mapping parameters if appropriate for your operating system.	Use Navigator 2. Refer to the online help.
Set any appropriate settings for your network switch (for example, VLAN settings).	Refer to the documentation for your switch.

Table 1-1: Installation Tasks (Continued)

Task	Reference
Host Bus Adapters (HBAs)	One or more supported HBAs with the latest supported BIOS and driver are required. Verify that the HBAs, drivers, and BIOSes are the latest versions supported by the array, and are functioning properly. • To check the latest supported versions, refer to the Hitachi interoperability matrix: http://www.hds.com/products/interoperability/. • For information about HBAs supported by your operating system, refer to the HBA vendor and operating system Web sites.
Install the network-interface card (NIC) or iSCSI HBA hardware.	Refer to the NIC or iSCSI HBA vendor's documentation and Web site.
Install the iSCSI initiator software or iSCSI HBA.	Refer to the iSCSI initiator's or iSCSI HBA vendor's documentation and Web site.
Set operating system parameters.	Refer to the operating system documentation or Web site for parameter settings.

NOTE: If you plan to connect different types of servers to the array through the same fabric switch, use the switch's zoning feature, the Hitachi Volume Security (LUN Manager) feature on the array, or a combination of both.

Booting from a SAN-Attached Disk

If your operating system permits booting from a SAN-attached disk, verify that the configurations on your array and your HBA hardware support boot from SAN.

To verify boot from SAN support on your system:

- Contact your Hitachi Data Systems account representative to determine the supported configurations when booting from a LUN.
- Contact your HBA vendor or check the vendor's Web site to verify your HBA card will support a boot-from-SAN configuration (for example, OS maintenance level, HBA model, HBA BIOS level, etc.).
- Check your operating system's Web site listed in Related Web Sites on page xvii for available documentation on Booting from SAN and how to install on external LUNs (direct or in a fabric).

Vendor High Availability (HA) Cluster Configurations

For vendor cluster software supported by Hitachi Data Systems:

- Consult the vendor documentation for installation and configuration details.
- Your array requires no unique operating system cluster-related settings.
- For required array parameter/mode settings related to supported vendor clusters, refer to the user's guide for your array and the Storage Navigator Modular 2 online help.

For additional information about setting up a cluster for your operating system, refer to your operating system vendor's Web site.

HA Multipath Configurations

The Hitachi modular array currently supports various HA multipath software products for operating systems that support such software. Contact your Hitachi Data Systems account representative for the latest information on supported software products, or refer to the Hitachi Data Systems interoperability support matrix:

http://www.hds.com/products/interoperability/

Multipathing software should be installed and configured before connecting to the array.

If your array configuration utilizes a switch, a redundant path to the host path is required when upgrading firmware. Since I/O cannot be stopped during the upgrade procedure, use path switching prior to upgrading the firmware.

Upgrading the Firmware

I/O execution may pause for up to 30 seconds when the firmware operation starts and finishes. If your topology uses a network switch, perform the firmware update using a redundant path configuration to the host, with path switching enabled.

2

Microsoft Windows

This chapter discusses guidelines on how to prepare the following host servers for connection to the array and verify that the host server can connect to the target:

- Microsoft Windows 2000 (Service Packs 3/4)
- Microsoft Windows 2003 and 2003 Server (Service Pack 1)
- Microsoft Windows 2008
- Microsoft Windows XP (Service Pack 2)

This chapter covers the following key topics:

Preparing the Host Server

Table 2-1 lists guidelines and tasks you need to follow to prepare the host server.

One or more supported network-interface cardS (NIC) or Internet Small Computer System Interface (iSCSI) host bus adapters (HBA) with the latest supported drivers and BIOS, along with the latest supported iSCSI initiator, are required. Verify that these items are the latest supported versions by Hitachi Data Systems, and are functioning properly. To check the latest supported versions, refer to the Hitachi Data systems Web sites listed below:

- Hitachi Customer Support Portal: http://support.hds.com
- Hitachi Interoperability Web Site: http://www.hds.com/products/interoperability/

Table 2-1: Host Server Preparation Guidelines

Item	Task
NICs	Use NICs supported by your array (refer to the Hitachi interoperability matrix) and operating system.
iSCSI HBAs (Optional)	Use the most current iSCSI HBA and drivers/BIOSes supported by your array (refer to the Hitachi interoperability matrix) and operating system. Install all utilities and tools that come with the HBA.
Install the HBA or iSCSI software initiator in the host server.	For installation information, check the Web sites for your HBA, NIC, and iSCSI initiator. Be sure the HBA, NIC, and iSCSI initiator are supported by your array (refer to the Hitachi interoperability matrix).
Windows operating system	Verify the planned OS version, architecture, relevant patches, and maintenance levels are supported by Hitachi Data Systems. Refer to the Hitachi interoperability matrix for information about supported versions.

The following list describes general requirements for using the array with iSCSI. For more information about supported Microsoft iSCSI software initiators, check the interoperability information at http://www.hds.com/products/interoperability/. For current requirements, please contact your Hitachi Data Systems representative.

- Hitachi Storage Navigator Modular 2 v1.0.0-00 or higher.
- For the array's microcode version, use the latest product release.
- The NIC, iSCSI HBA, and Ethernet switch that are directly connected to the array must support the Institute of Electrical and Electronics Engineers (IEEE) 802.3ab 1000Base-T, full-duplex operations.
- Category 5e (enhanced Category 5) or Category 6 network cabling.
- If using the array as an iSNS client, Microsoft iSNS Server 3.0 or higher must be installed on the same IP-SAN.
- Set OS parameters if needed.
- Do not change the Challenge Handshake Authentication Protocol (CHAP) authentication settings that correspond to hosts that are

logging in to the array. If you disable CHAP authentication for the array while it is communicating with the software initiator that uses CHAP authentication, the host will not be able to access the target device without rebooting.

- Stop all unused applications and services to reduce server loads.

Connecting to the Array

This section provides guidelines on how to connect the array to the host.

Before you connect to the system:

1. Verify the items in Table 1-1 on page 1-3 were completed.
2. Verify the iSCSI port address configuration and the status of the SMS iSCSI adapters and LUNs are normal.
3. Set the queue depth if necessary on the Windows host (see Setting Queue Depth on page 2-3).
4. Install the Ethernet cables between the array and the Windows system. Refer to your array's user's guide for details on hardware installation tasks.
5. From the Windows prompt, execute the `ping` command to confirm that the cabling and IP address settings are correct.
6. Log in to the array from Windows.
7. If using Microsoft MPIO, set the IP address of two or more host ports to divide the segment.

Dynamic Disk is supported with no restrictions for the array connected to the Windows 2003 or 2008 operating system. Using the Dynamic Disk on a Windows Server 2008 operating system may require you to reduce the logical unit capacity. For more information, refer to the Microsoft Windows online help.

Setting Queue Depth

You may need to change the queue depth value on the server. If the number is small, I/O performance can deteriorate. The array reports a queue full status when the queue depth exceeds an allowable limit. The system may not operate correctly when the queue is full and a large value is set. Set an appropriate number according to your configuration. If necessary, set a queue depth number for each server. Refer to the documentation for your HBA before setting a value.

Guidelines for settings:

- 32 commands per LUN
- 512 commands per port
- 30 or more for device timeout value on the Hitachi array LU.

NOTE: For Windows, neither the iSCSI software initiator nor the HBA has a Queue Depth parameter. Please adjust job execution on the server.

Installing Microsoft iSCSI Initiator

Microsoft iSCSI software initiator is the iSCSI software initiator driver for your Windows operating system as provided by Microsoft.

For Windows Server 2008 and Windows Vista, Microsoft iSCSI Initiator is installed natively. On these two platforms, no installation steps are required.

For Windows Server 2003 and Windows 2000, you install the Microsoft iSCSI Initiator package and run the appropriate installer package for your computer from a command line or by double-clicking a file icon from an Explorer window. Administrator privileges are required to install the Microsoft iSCSI software initiator package. The installer package uses the Software Update Installation Wizard to install or upgrade the Microsoft iSCSI initiator. The installer can be run in interactive, passive, or quiet mode.

- Interactive mode lets you select the installation options from the wizard.
- Passive and quiet modes let you select installation options using environment variable settings.

For more information about which installer package to run for your Windows version, refer to the Microsoft iSCSI Software Initiator Version 2.X Users Guide. This guide can be downloaded from http://download.microsoft.com/download/a/e/9/ae91dea1-66d9-417c-ade4-92d824b871af/uguide.doc#_Toc197174270.

Installing and Configuring Microsoft iSCSI Software Initiator

Installing and configuring Microsoft iSCSI software Initiator for Windows 2000, 2003, and 2008 operating systems involves three steps:

1. **Install the Microsoft initiator**
   Select the MPIO function as an installation option to install Microsoft iSCSI software initiator (version 2.0 or higher) if appropriate for your operating system.
2. **Connect to the Target using the Microsoft initiator**
   Set the MPIO function to enabled when connecting to the Target. Refer to the Microsoft iSCSI User's Guide and latest release notes.
3. **Set Microsoft iSCSI MPIO**
   Change the settings of each connection path for all the targeted LUs using the load balance policy "Failover only."

The following sections summarize the steps associated with installing and configuring the version of Microsoft iSCSI software Initiator for Windows 2000 and 2003 downloaded from the Microsoft Web site. For detailed information, refer to the release notes for Microsoft iSCSI software Initiator, which are available on the Microsoft Web site http://www.microsoft.com/windowsserver2003/technologies/storage/iscsi/default.mspx

Installation Instructions

NOTE: For Windows 2008 and Windows Vista, no installation is required, the iSCSI Initiator is embedded in the software.

To install Microsoft iSCSI software Initiator on Windows 2000 and 2003 operating systems:

1. When you install Microsoft iSCSI software Initiator, the confirmation window in Figure 2-1 appears.
2. Verify that the two check boxes, **Initiator Service** and **Software Initiator**, are checked. If they are not checked, check them.
3. Check the checkbox **Microsoft MPIO Multipathing Support for iSCSI** if your system will use Microsoft MPIO (if it is not checked by default).
4. Click **Next**.

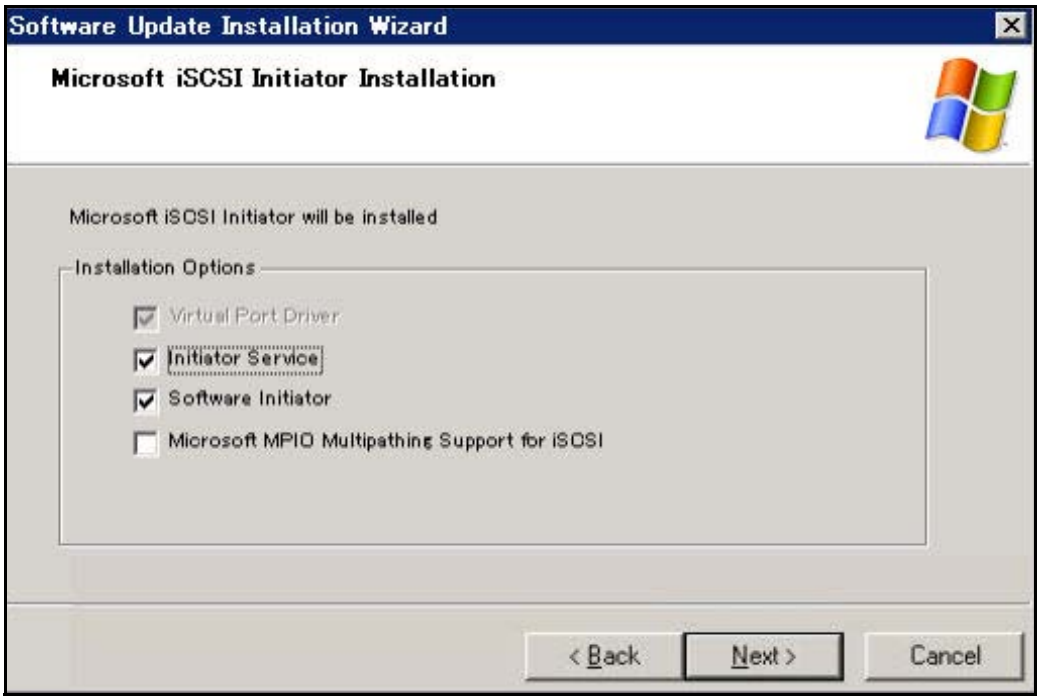

Figure 2-1: Installation Options

Configuration Instructions

To configure Microsoft iSCSI software initiator for Windows 2000, 2003, and 2008 operating systems:

1. On your Windows Server, open the Windows **Control Panel**.
2. Open the **iSCSI Initiator Properties** dialog box (see Figure 2-2 on page 2-6).

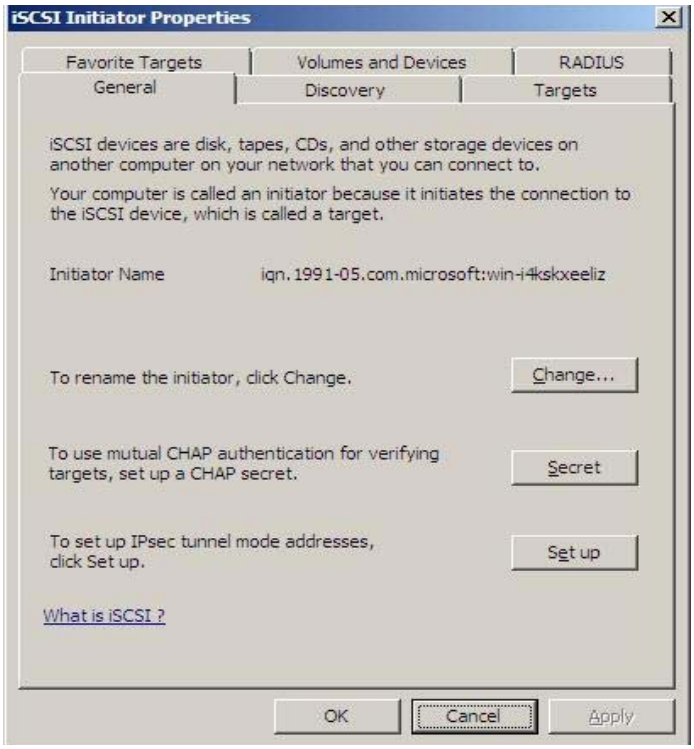

Figure 2-2: iSCSI Initiator Properties Dialog Box

3. Click the **Discovery** tab (see Figure 2-3).

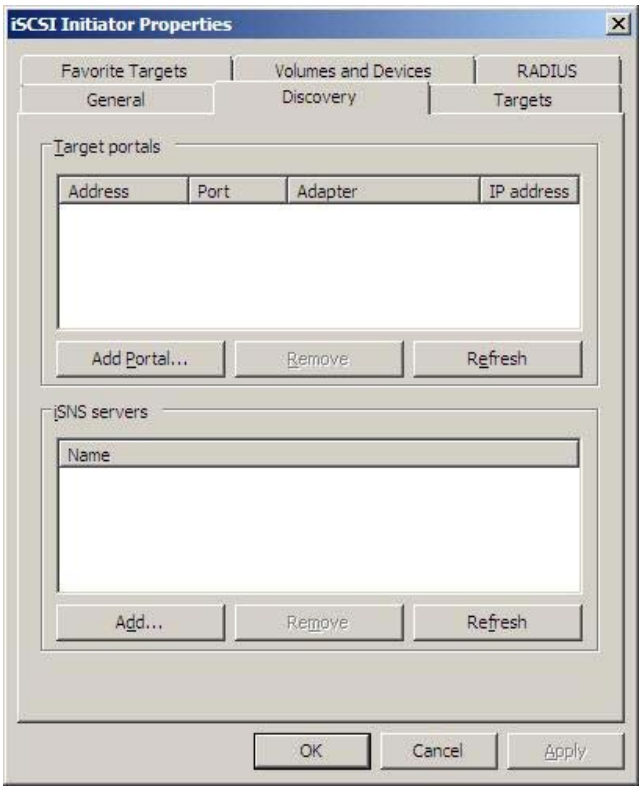

Figure 2-3: iSCSI Initiator Properties, Discovery Tab

4. Under **Target Portals**, click **Add** and add the target you want to connect.
5. In the **Add Target Portal** dialog box, specify the target's Internet Protocol (IP) address and, if appropriate, change the default port number from 3260 (see Figure 2-4).

NOTE: Verify there is no firewall blocking the TCP port specified under **Port**.

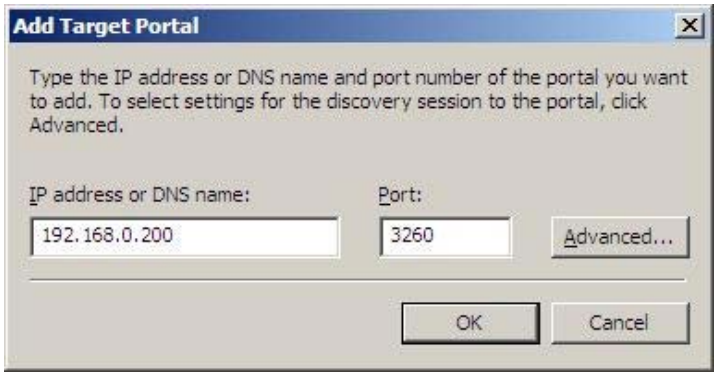

Figure 2-4: Add Target Portal Dialog Box

6. Click **OK**.

NOTE: iSCSI does not support CHAP authentication in the discovery session.

7. Click **OK**. The iSCSI Initiator Properties dialog box appears (see Figure 2-5).

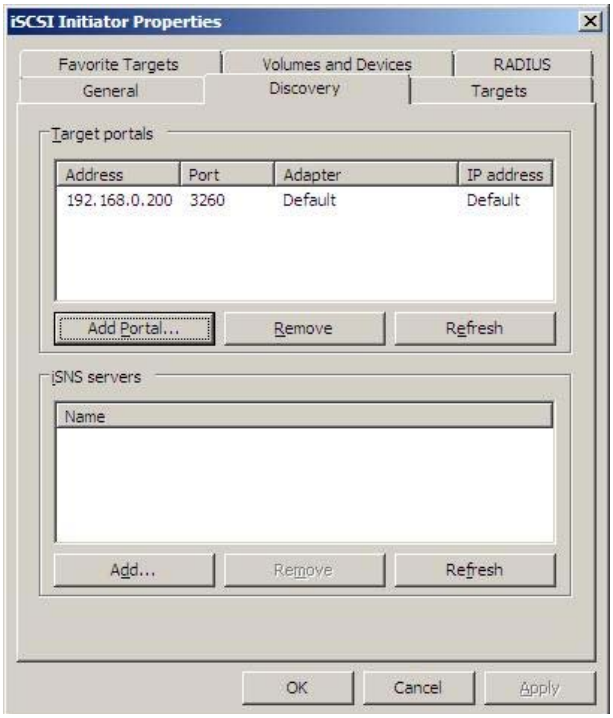

Figure 2-5: iSCSI Initiator Properties Dialog Box

8. In the iSCSI Initiator Properties dialog box, click the **Targets** tab (see Figure 2-6).

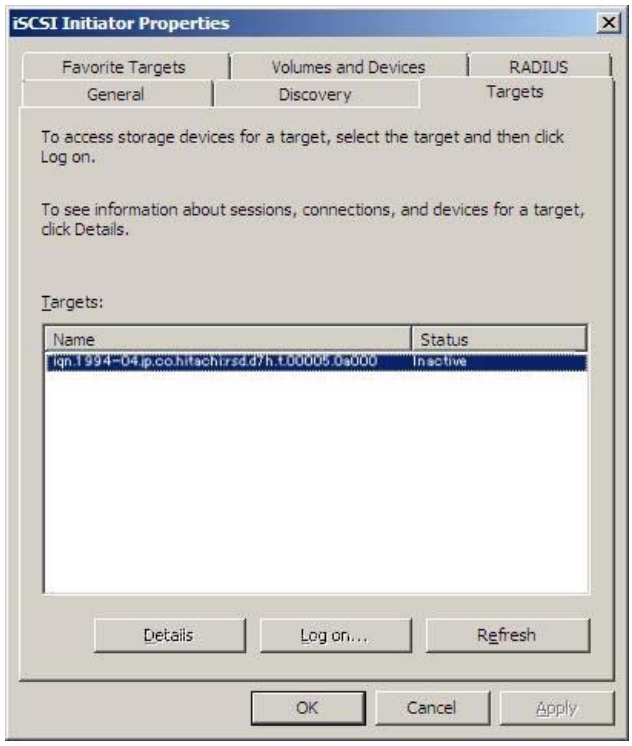

Figure 2-6: iSCSI Initiator Properties Dialog Box, Targets Tab

9. Select the target to login from the displayed target and then click **Log On**. The **Log On to Target** dialog box displays (see Figure 2-7).

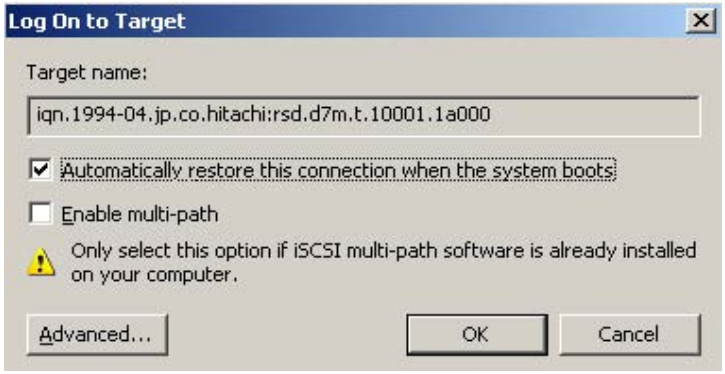

Figure 2-7: Log On to Target Dialog Box

10. To reboot the host every time a reconnection is performed automatically, click **Automatically restore this connection when the system boots**. If using Microsoft MPIO, check **Enable multi-path**.
11. Click **OK**.
12. Under **Targets**, verify that the status of the selected target is **Connected** (see Figure 2-8 on page 2-9).

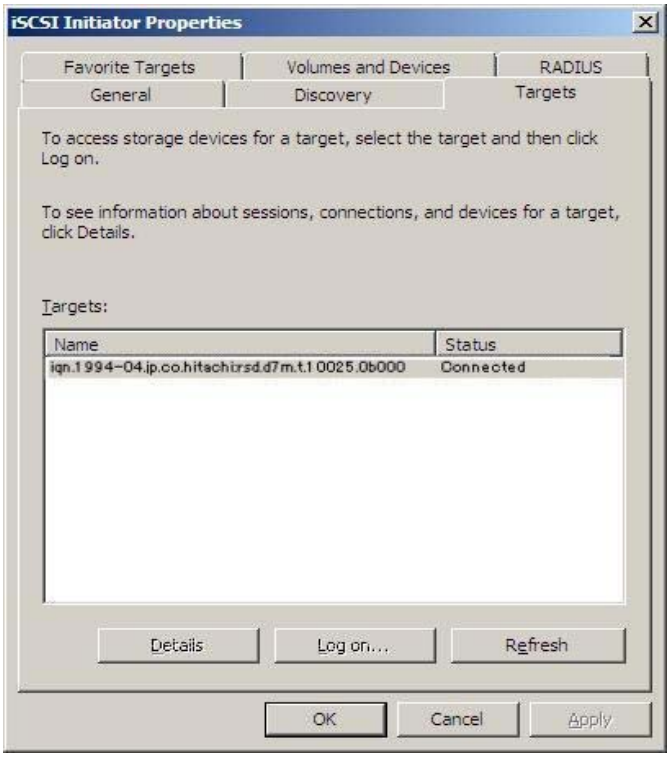

Figure 2-8: iSCSI Initiator Properties Dialog Box

13. Click **OK**.

Disk drive authentication and formatting for iSCSI are the same as drives connected through Fibre Channel. Perform the appropriate processing for the added disk drive from **Control Panel->Management Tool->Computer Management ->Disk Management.**

Installing Multi-path I/O (MPIO)

This section provides information about installing and using Multipath I/O (MPIO). MPIO is a feature that provides support for using multiple data paths to a storage device. Multipathing increases the availability of storage resources by providing path failover from a server or cluster to a storage subsystem.

You must install MPIO on a server if it will access a logical unit number (LUN) through multiple iSCSI initiator adapters.

What is Multipathing?

Multipathing gives systems the ability to use more than one read/write path to a storage device using redundant physical path components — adapters, cables, and switches — between the server and storage device. Multipathing is key in keeping mission-critical data continuously available in the enterprise environment, where the goal for many organizations is continuous availability.

Because multipathing allows two or more data paths to be used simultaneously for read/write operations, a failure with one or more components still allows applications to access their data. In addition to providing fault tolerance, multipathing also serves to redistribute the read/write load among multiple paths between the server and storage, helping to remove bottlenecks and balance workloads.

Installation Prerequisites

Observe the following prerequisite before installing MPIO.

Environmental Prerequisites

- The host computer(s) must be connected to the Hitachi storage system using dual-redundant data paths, either end-to-end or via routing devices such as network switches. The driver-level MPIO then manages the redundant connections.
- All NICs and iSCSI HBAs and their associated drivers should be installed to the host computer(s) before you install MPIO.

Hardware Prerequisites

- To create path redundancy in a storage network or applications using other host-side links, apply at least two single-ported HBAs or two dual-ported NICs or iSCSI HBAs on the host computer(s). To optimize performance, place the NICs or iSCSI HBAs on different buses in the server to distribute the workload over the server's PCI bus architecture.
- Before installing and using MPIO, RAID volumes must be created and properly associated with host ID/LUNs to use the MPIO functions.

Setting Microsoft iSCSI MPIO on Windows 2000 and 2003

This section explains how to set Microsoft iSCSI MPIO on Windows 2000 and 2003 operating systems.

To set MPIO on Windows 2000 and 2003 operating systems:

1. If the Target Properties dialog box is not displayed:
   a. Launch the iSCSI Initiator Properties Control Panel applet. The iSCSI Initiator Properties Dialog Box appears (see Figure 2-9 on page 2-11).

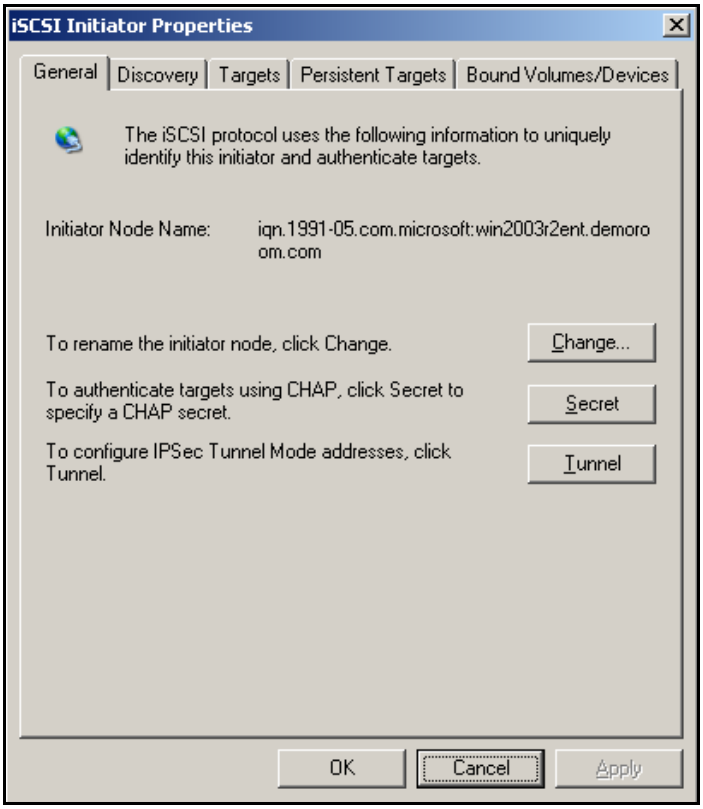

Figure 2-9: iSCSI Initiator Properties Dialog Box

b. Click the **Targets** tab to display a list of available targets that you can log on to.

NOTE: If your target is not listed on the **Targets** tab, verify that the target has Logical Unit Numbers (LUNs) assigned to this server (refer to the Microsoft iSCSI Software Initiator Version 2.X Users Guide).

c. Select a target and click **Details**. The Target Properties dialog box appears.

d. Click the **Devices** tab

e. Select a LUN and click **Advanced** to display the Device Details dialog as shown in Figure 2-10 on page 2-12.

Figure 2-10: Device Details Dialog Box - General Tab

2. To configure the MPIO settings for the LUN, click the **MPIO** tab (see Figure 2-11).
3. Set the load balance policy to **Round Robin**. It is not necessary to switch the path type of the active and standby paths. Do not click **Edit** and use the default setting.

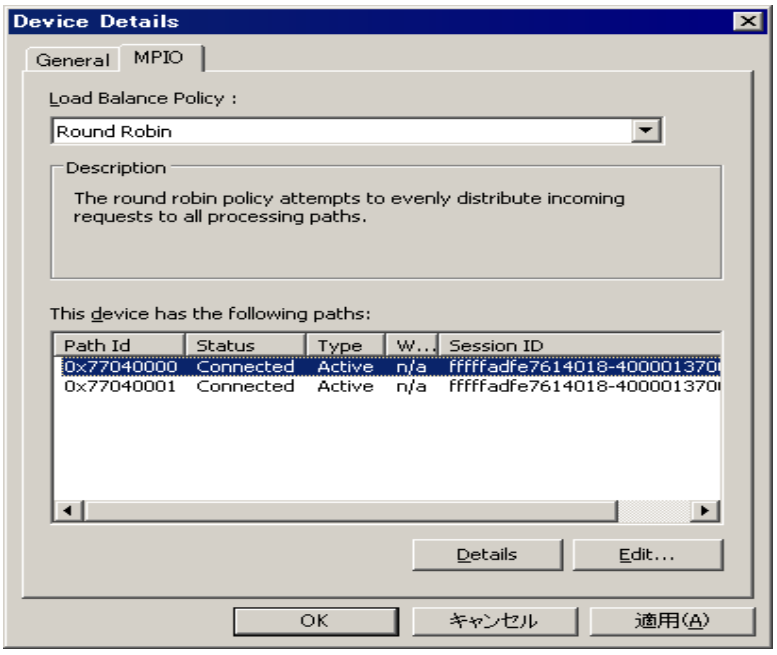

Figure 2-11: Device Details Dialog Box - MPIO Tab

4. Return to the **Device Details** window, and click **Apply** and **OK**.

Checking Session and Device Information

Use the following procedure to check the session and device information when Microsoft iSCSI MPIO is used on Windows 2000 and 2003 operating systems.

1. Select the Target from **iSCSI Initiator Properties** ->**Targets**, and click **Details**. The property of the Target is displayed.
2. Select the **Sessions** tab.

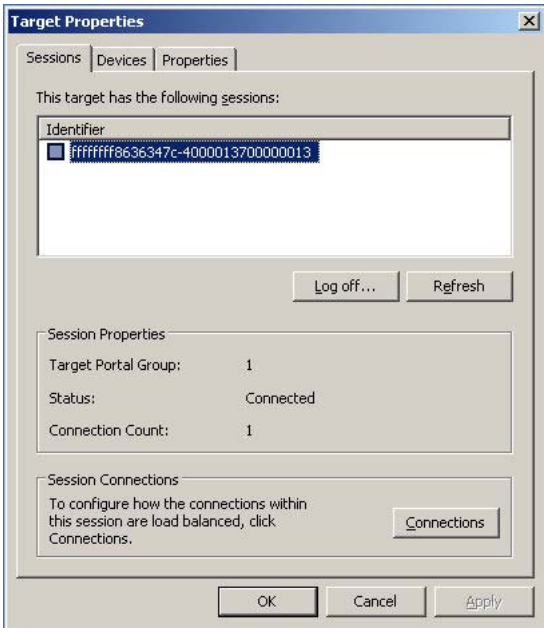

Figure 2-12: Target Properties Dialog Box - Sessions Tab

3. With the session identifier still highlighted, click on the **Devices** tab. The devices are displayed in a list (see Figure 2-13).

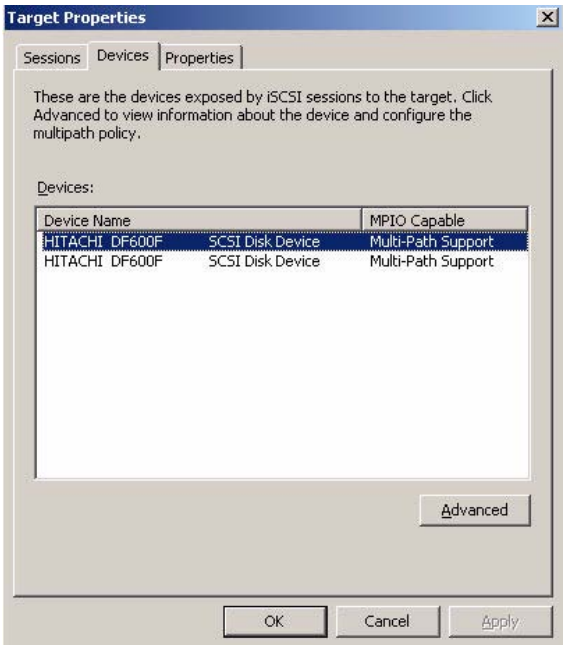

Figure 2-13: Target Properties Dialog Box - Devices Tab

4. Select the chosen target from **iSCSI Initiator Properties ->Targets**, and click **Details**. The target property is displayed.
5. Select the chosen devices and click **Advanced**. Device Details is displayed.
6. Click the **MPIO** tab (see Figure 2-14).

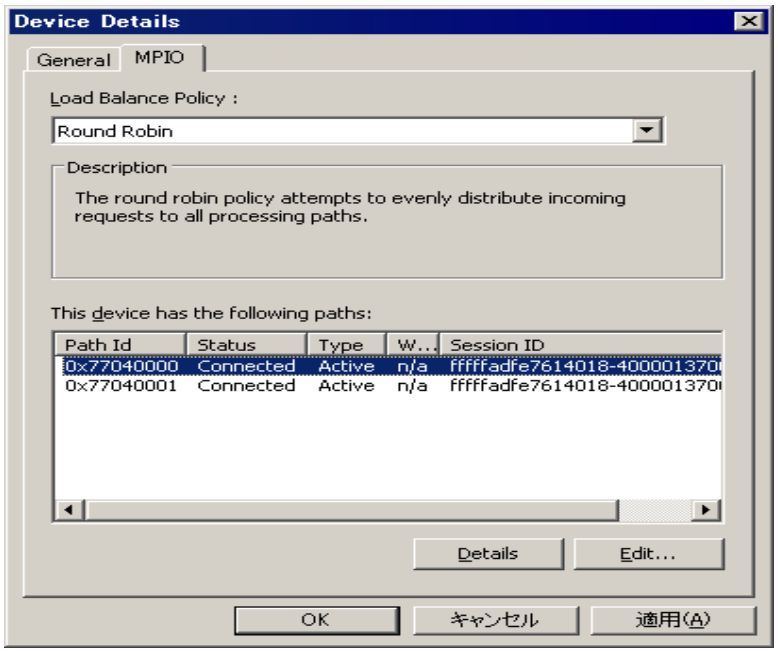

Figure 2-14: Device Details Dialog Box - MPIO Tab

7. Each active path that has separate session I/Os is set in the path information of the devices.

Setting iSCSI Authentication

The Microsoft Challenge Handshake Authentication Protocol (CHAP) is an encrypted password authentication protocol that cannot be reversed. It sends a challenge to the remote access client, and the client returns the username, string encryption, session identifier, and password. If the information returned is valid, the credentials are authenticated.

The length of the secret security key must be from 12-characters (96 bits) to 16-characters. The CHAP secret is case sensitive. For security, each typed letter appears as a dot.

To apply two-way authentication, please refer to the Microsoft iSCSI user guide and the Hitachi array user's guide.

Figure 2-15: CHAP Setup

Enabling Header digest may decrease performance by nearly 90%, depending on network configuration, host performance, and host applications. iSCSI Data digest and Header digest should be used with an L3 switch or router that is in the path of the hosts and the array's iSCSI port.

8. The array does not support CHAP authentication in the discovery session. Disk drive authentication and formatting for iSCSI are the same as drives connected through Fibre Channel. Perform the appropriate processing for the added disk drive from **Control Panel --> Management Tool --> Computer Management --> Disk Management**.

Installing and Configuring MPIO on Windows 2008

On Windows 2008, MPIO is available as a standard installable feature. The following procedure provides general guidelines for installing MPIO on a Windows 2008 operating system. For more information, refer to http://go.microsoft.com/fwlink/?LinkId=81020.

Installation Instructions for Windows 2008

Before proceeding with the installation, observe the following guidelines:

- If you will be using MPIO, refer to http://technet.microsoft.com/en-us/library/cc725907.aspx and your host server documentation for information about implementing MPIO.
- If you will enable access to a LUN from a cluster, be sure that Failover Clustering is installed on each server in the cluster; otherwise, data loss can occur. For more information, refer to http://go.microsoft.com/fwlink/?LinkId=86168.
- You must have Administrator privileges on the computer to install MPIO.

To install MPIO on a Windows 2008 operating system:

1. In the Server Manager console tree, click the **Features** node.
2. In the Features pane, under **Features Summary**, click **Add Features**.
3. In the Add Features Wizard, select the **Multipath I/O** check box and click **Next**.
4. Follow the steps in the Add Features Wizard to complete the installation.

5. After the wizard is completed, click the **Close** button and verify that MPIO is installed:
   a. Click the Windows **Start** button, point to **Administrative Tools**, and click **Server Manager**. The Server Manager window opens.
   b. In the left pane, click the **Features** category if it is not selected.
   c. Confirm that **Multipath I/O** appears under the Features group (see Figure 2-16). You may need to expand the group to see all installed features.
   d. Close or minimize the Server Manager window.

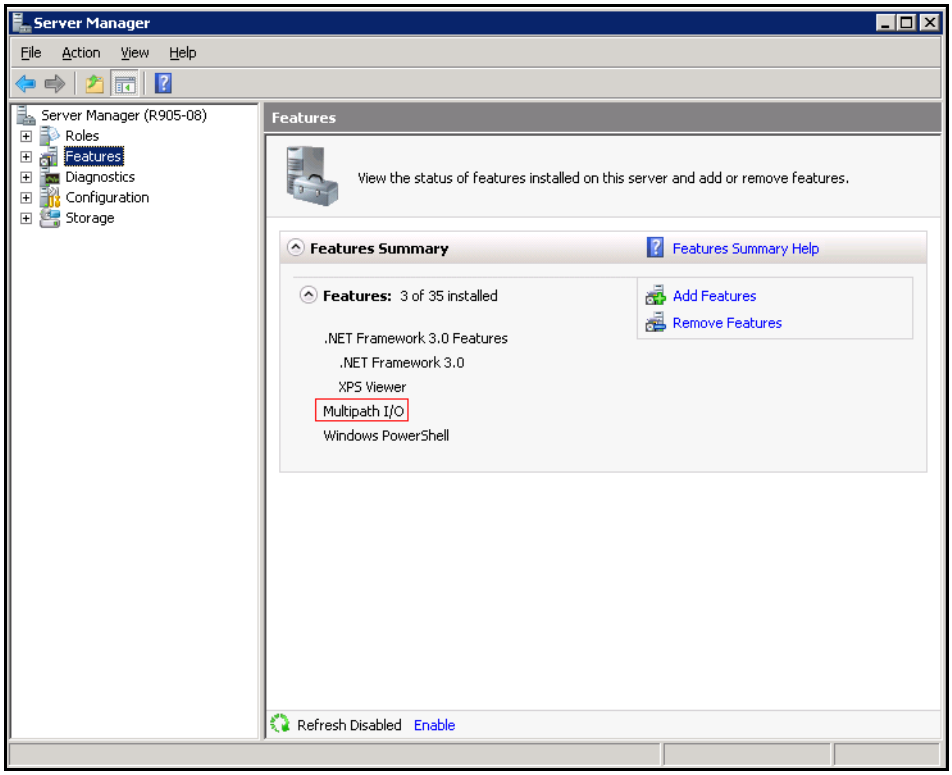

Figure 2-16: Server Manager Window with Multipath I/O Displayed

Configuring Native MPIO for Your Hitachi Storage System

After MPIO is installed, use the following procedure to add the device hardware ID for your Hitachi storage system. This procedure requires you to reboot your system. Optionally, you can also remove the default MPIO hardware ID, but this requires a second system reboot.

1. Click the Windows **Start** button.
2. Point to **Administrative Tools** and click **MPIO**. The **MPIO-ed Devices tab** of the MPIO Properties dialog box appears. In this panel, the **Device Hardware Id** field shows the IDs of the MPIO hardware devices installed. The first time this dialog box appears, the default string in Figure 2-17 on page 2-17 is displayed to indicate that the vendor ID is limited to 8 characters and the product ID is limited to 16 characters.

3. Optional: To remove the default MPIO hardware ID, perform the following steps; otherwise, proceed to step 4 on the next page.
   a. Select the default string in the **Device Hardware Id** field and click the **Remove** button to delete the string. The Reboot Required message in Figure 2-18 appears.

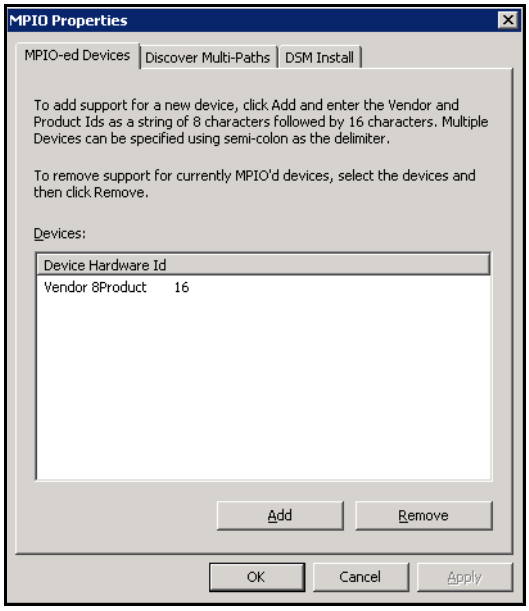

Figure 2-17: MPIO Properties Dialog Box

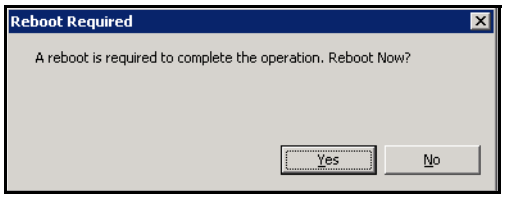

Figure 2-18: Reboot Required Message

   b. Click **Yes** to reboot your host.
   c. After your host reboots, click the Windows **Start** button, point to **Administrative Tools**, and click **MPIO** to display the **MPIO-ed Devices tab** of the MPIO Properties dialog box again.
   d. Continue with step 4.
4. Click the **Add** button. The Add MPIO Support dialog box appears (see Figure 2-19 on page 2-18).

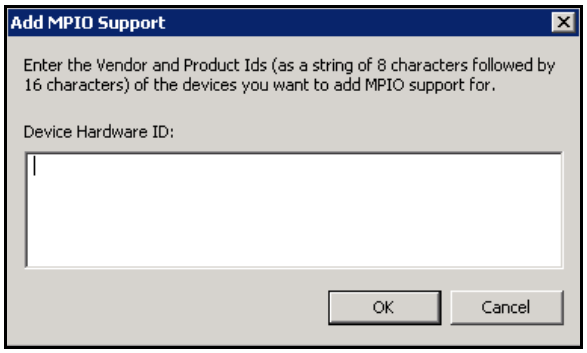

Figure 2-19: Add MPIO Support Dialog Box

5. In the **Device Hardware ID** field, type: **HITACHI DF600F**
6. Click the **OK** button. The Reboot Required message in Figure 2-20 appears.

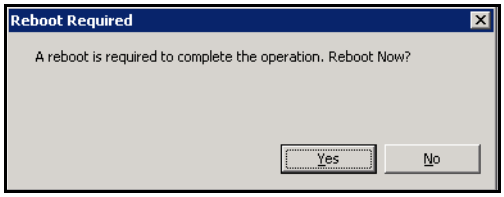

Figure 2-20: Reboot Required Message

7. Click **Yes** to reboot your host.
8. After the host reboots, confirm that the device hardware ID was added to the MPIO configuration:
   a. Click the Windows **Start** button.
   b. Point to **Administrative Tools**.
   c. Click **MPIO**. The **MPIO-ed Devices** tab of the MPIO Properties dialog box appears. In this panel, verify that the **Device Hardware Id** field shows the vendor and product IDs of your Hitachi MPIO hardware (as well as any other MPIO hardware devices that may be installed). See Figure 2-21 on page 2-19.

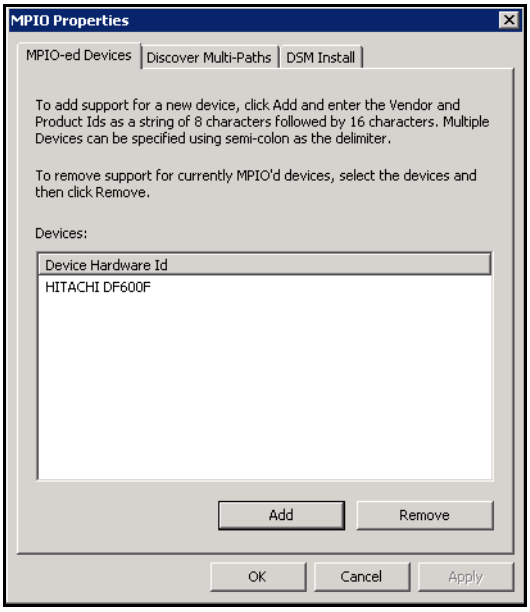

Figure 2-21: MPIO Properties Dialog Box with Hitachi Vendor and Product IDs

This completes the procedure for configuring MPIO on Windows 2008 operating systems for use with your Hitachi storage system.

Verifying and Discovering LUNs

When the Hitachi array, Windows operating system, and HBA drivers and software are installed correctly and working properly, LUN discovery occurs automatically.

Windows assigns the disk numbers sequentially, starting with the local disks, and then assigns them by adapter and by TID/LUN. If the system is attached to the first adapter (displayed first during system start-up), the disk numbers for the new devices start at 1 (the local disk is 0). If the system is not attached to the first adapter, the disk numbers for the new devices start at the next available disk number. For example, if 40 disks are attached to the first adapter (disks 1-40) and the system is attached to the second adapter, the disk numbers for the system start at 41.

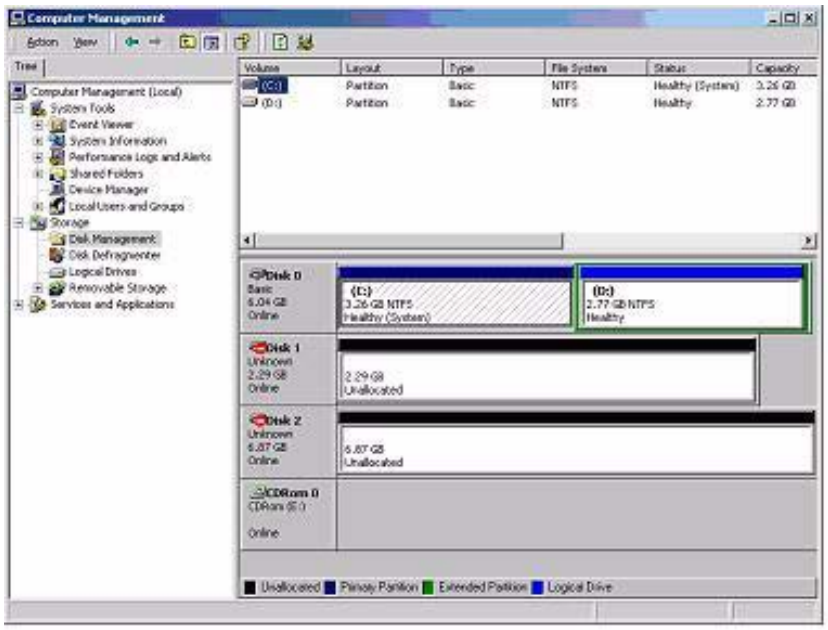

Figure 2-22: Example of Disk Management Panel Showing New Devices

Microsoft Windows 2003 and Microsoft Windows XP

To verify and discover LUNs on a Microsoft Windows 2003 or Microsoft Windows XP operating system:

1. Start Microsoft iSCSI Software Initiator.
2. Select the **Bound Volumes/Devices** tab, and click **Bind All** (see Figure 2-23 on page 2-21). Be sure to perform this step if the LU configuration was changed.

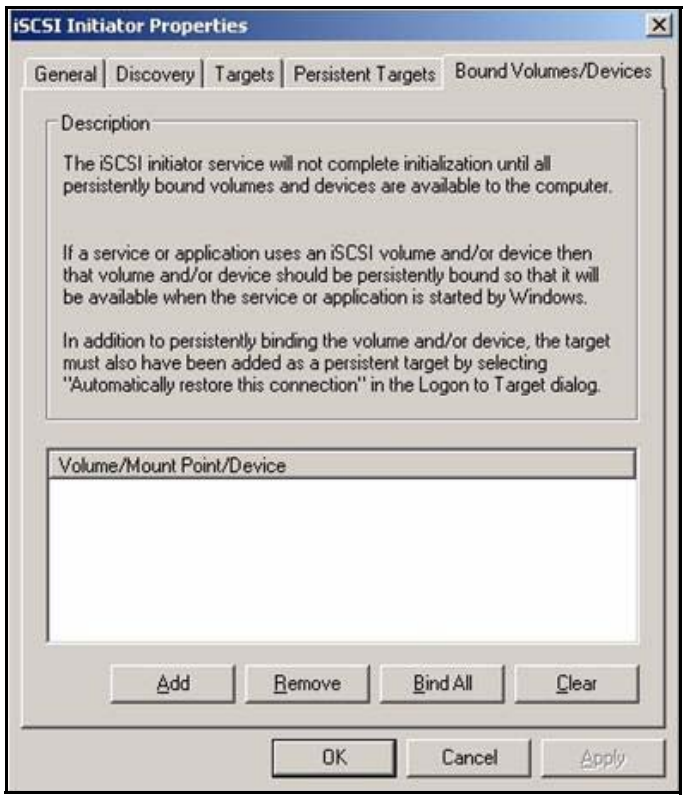

Figure 2-23: Bound Volumes/Devices Tab with No Devices Added

3. Click **OK**.
4. You may want to reboot your system after adding new devices.

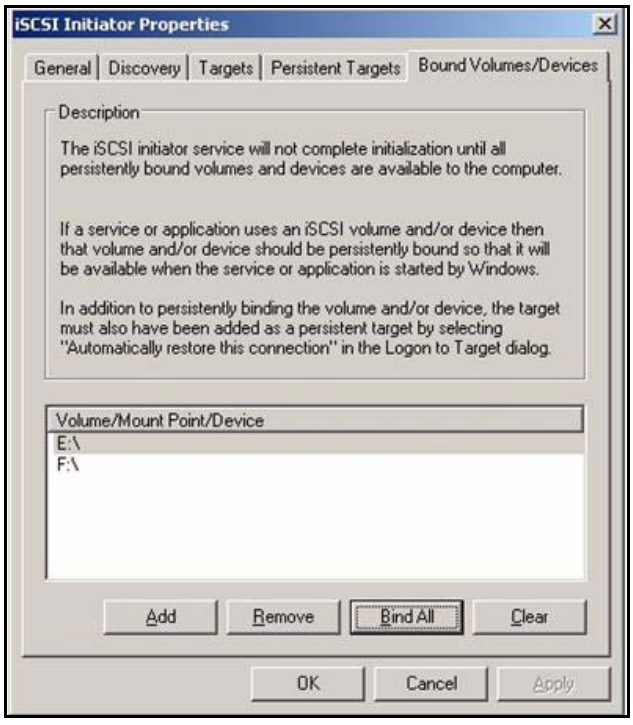

Figure 2-24: Bound Volumes/Devices Tab with New Devices Added

Microsoft Windows Vista

To verify and discover LUNs on a Microsoft Windows Vista operating system:

1. Start Microsoft iSCSI Software Initiator.
2. Select the **Volumes and Devices** tab and click **Autoconfigure**. Be sure to perform this step if the LU configuration was changed.

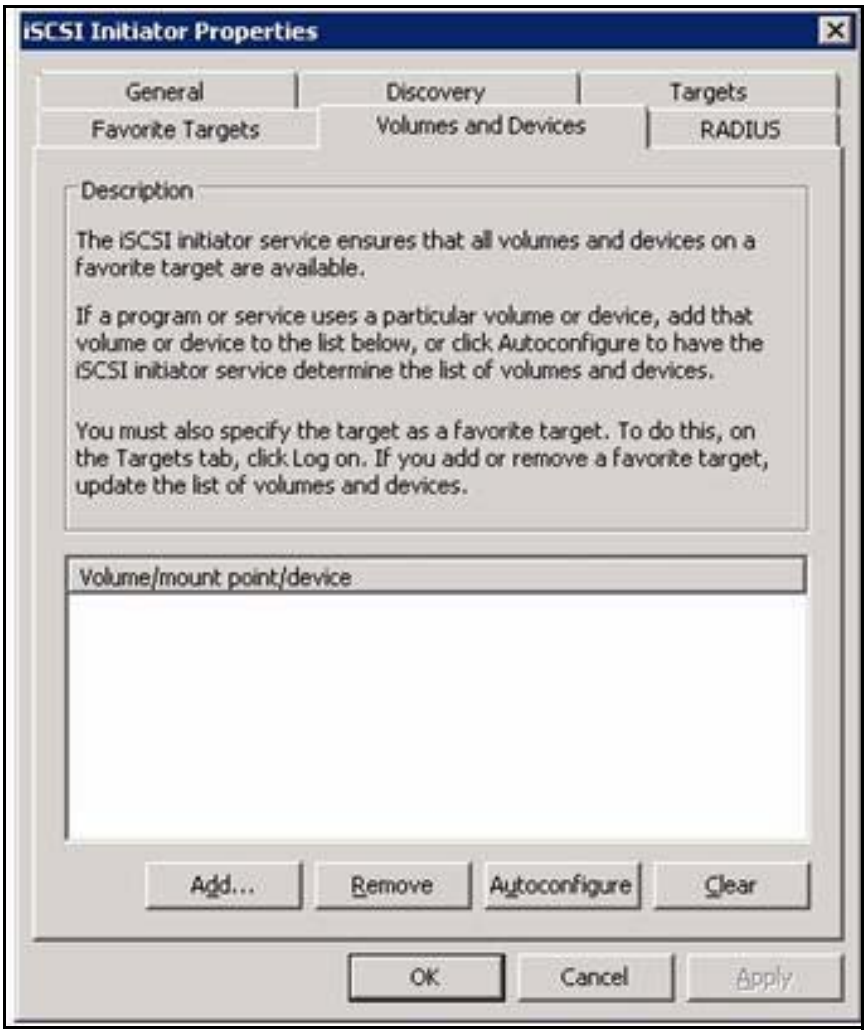

Figure 2-25: Volumes and Devices Tab with No Devices Added

3. Click **OK**.
4. You may want to reboot your system after adding new devices.

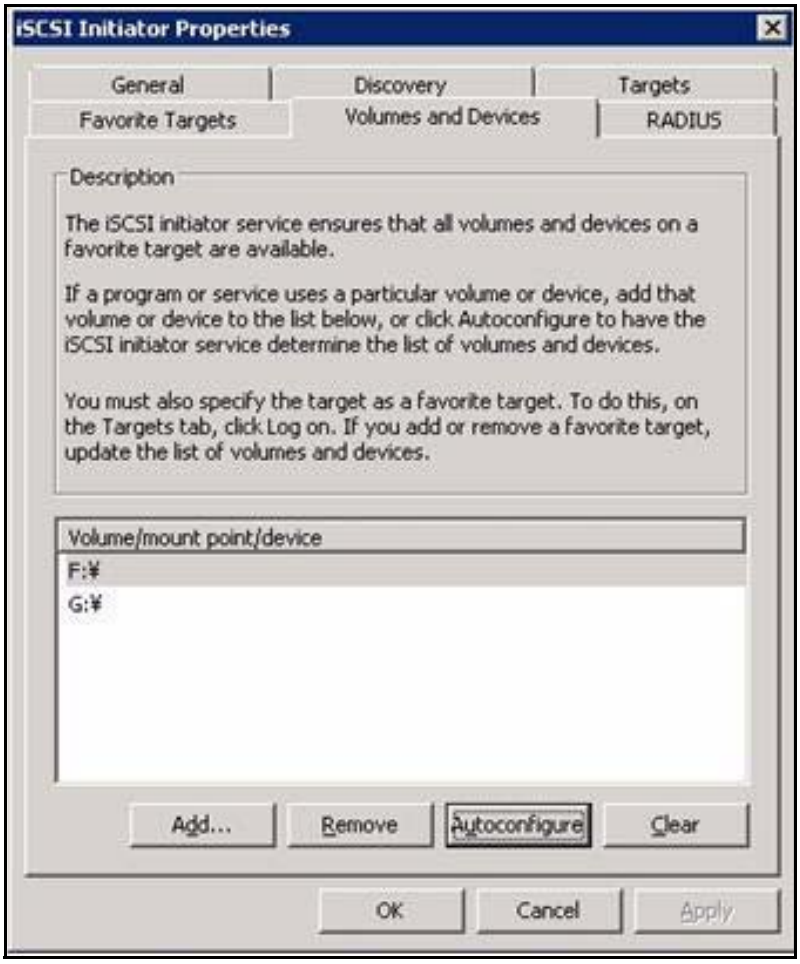

Figure 2-26: Volumes and Devices Tab with New Devices Added

3

Solaris

This chapter discusses guidelines on how to prepare a Solaris host server for connection to the array and verify that the host server can connect to the target.

This chapter covers the following key topics:

- Preparing the Host Server
- Connecting to the Array
- Setting the Disk and Device Parameters
- Configuring iSCSI on the Host
- Using Sun StorageTek Traffic Manager
- Using Sun StorageTek Traffic Manager
- iSCSI LUN Discovery

Preparing the Host Server

Table 3-1 lists guidelines and settings you need to follow to prepare the host server.

One or more supported network-interface cards (NIC) with the latest supported Internet Small Computer System Interface (iSCSI) initiator or host bus adapters (HBA) with the latest supported BIOS and driver are required. Verify the NICs, HBAs, drivers, and BIOSes are the latest supported versions by Hitachi Data Systems, and are functioning properly. To check the latest supported versions, refer to the Hitachi interoperability matrix at http://www.hds.com/products/interoperability/.

For information about iSCSI initiators supported by your operating system, refer to the Solaris Web site: http://www.sun.com/

Table 3-1: Host Server Preparation Guidelines

Item	Task
NICs	Use NICs supported by your array (refer to the Hitachi interoperability matrix) and operating system.
iSCSI HBAs (Optional)	Use the most current iSCSI HBA and drivers/BIOSes supported by your array (refer to the Hitachi interoperability matrix) and operating system. Install all utilities and tools that come with the HBA.
Install the HBA/NIC and iSCSI software initiator in the host server.	For installation information, check the Web sites for your HBA, NIC, and iSCSI initiator Web sites. Be sure the HBA, NIC, and iSCSI initiator are supported by your array (refer to the Hitachi interoperability matrix).
Solaris operating system	Verify the planned OS version, architecture, relevant patches, and maintenance levels are supported by Hitachi Data Systems. Refer to the Hitachi interoperability matrix for information about supported versions.

Multipath HA Configurations with MPxIO

If you use Multiplexed I/O (MPxIO) for Sun Solaris on a SPARC station running Solaris v10 OS U5 or higher, you can download a patch from the following URL that will enable the use of both array controllers in a multipath HA configuration:

http://sunsolve.sun.com/search/document.do?assetkey=1-21-138308-02-1

To use this patch, your server and array system must meet the requirements in Table 3-2 and Table 3-3.

Table 3-2: MPxIO Settings for Hitachi AMS 2000 Family Storage Systems

Parameters		Settings
Storage Navigator Modular 2 Settings	Simple Settings	Platform = Solaris Middleware = none
	Host Connection Mode 1	Standard Mode
	Host Connection Mode 2	None

Table 3-3: MPxIO Host Settings

Activity	Description
Solaris 8, Solaris 9, and Solaris 10 U4 or earlier	Patch = not necessary
	scsi_vhci.conf = edit as below: • load-balance = round-robin • auto-failback = enable • device-type-scsi-options-list = HITACHI DF600F • symmetric-option • symmetric-option = 0x1000000
Solaris 10 U5	Patch = one of the following patches is required, based on the Solaris version installed on the host: • SPARC = patch 138308-02 • x64/x86 = patch 138309-02
	• scsi_vhci.conf = use default settings
Solaris 10 U6	Patch = not necessary
	scsi_vhci.conf = use default settings

Connecting to the Array

This section provides guidelines on how to connect the array to the host.

Before you connect to the system:

1. Verify the items in Table 1-1 on page 1-3 were completed.
2. Log in to the host system as `root`, and make sure that all existing devices are powered on and are properly connected to the host system.
3. Display the host configuration:

   ```
   /usr/platform/ [platform: sun4u]/sbin/prtdiag
   ```

4. Verify the host recognizes the following four classes: iSCSI adapter, SCSI bus characteristics, world wide name, and iSCSI driver. If this information does not display or error messages display, the host environment may not be configured properly.
5. Connect the array to the Solaris host.

NOTE: For information on the HBA-specific text displayed on screen, refer to the MAN pages and/or user documentation for the HBA.

Completing the System and Host Connections

After connecting the array to the host system, perform the following tasks before rebooting the host:

1. Modify `/etc/system` with appropriate time-out and max throttle values. Check the interoperability information at http://www.hds.com/products/interoperability/ for the correct values.
2. Modify `/kernel/drv.sd.conf` so LUNs can be discovered.
3. Configure the host iSCSI adapters.
4. Power on all peripheral devices. The array should already be on and the iSCSI ports should already be configured. If the array's iSCSI ports are configured after the host system is powered on, the system must be restarted to recognize the new devices.
5. Confirm the ready status of all devices.
6. Power on the host system.
7. Log in to the array from Solaris.

Setting the Disk and Device Parameters

Once the array is installed and connected, you must set the queue depth parameter (sd_max_throttle) and I/O time-out value (sd_io_time) for the array devices. Smaller queue depth settings (for instance, 1) lowers I/O performance because only one I/O is issued at a time. The array reports a queue full status when the queue depth exceeds an allowable limit. The array may not operate correctly when the queue depth is full, and a large value is set. Set appropriate queue depth according to your configuration when installing for the first time and when adding LUNs. the information below is a guideline only. Check your HBA vendor and Solaris documentation for information on how to set these parameters.

The required I/O time-out value (TOV) for array devices is 60 seconds (0x3C), which is also the default value. If the I/O TOV has been changed from the default, you must change it back to 60 seconds by editing the sd_io_time parameter in the /etc/system file.

To set the I/O TOV and queue depth for your array devices:

1. Make a backup of /etc/system:

   ```
   cp /etc/system /etc/system.bak
   ```

2. Edit /etc/system.
3. Add the following lines to /etc/system:

   ```
   set sd:sd_io_time=0x3c
   sd_max_throttle = x
   ```

The sd _max_throttle setting is determined by dividing 512 by the total number of LUNs configured to a port. For example, if the user has configured a total of 67 LUNs to port -0A- on a 9570, the sd_max_throttle setting will be:

512 /67 = 7.6 (always round down to the next EVEN integer).

In the example above, the sd_max_throttle would be set to (6). This number should not exceed 32, or, if using Veritas Volume Manager DMP, this number should not exceed 8.

4. Save your changes and exit the text editor. You will reboot the system later to apply the above I/O TOV setting.

Configuring iSCSI on the Host

When you install the iSCSI adapter, the array can communicate to hosts through iSCSI. There are two ways to configure iSCSI on the host:

- Configuring the NIC and iSCSI Software Initiator, below
- Configuring iSCSI HBAs on page 3-8

Configuring the NIC and iSCSI Software Initiator

1. Check that the following software is installed:
   - A Solaris release that supports the iSCSI protocol.Refer to the Sun Microsystems Web site for the correct version.
   - Software packages:

     ```
     SUNWiscsir-Sun iSCSI device driver (root)
     SUNWiscsiu-Sun iSCSI management utility (usr)
     ```
2. Use the following command to check the Solaris version:

   ```
   % cat/etc/release
   ```

Setting CHAP

iSCSI can be configured for one-way or two-way CHAP authentication. This section discusses both procedures.

Setting One-way CHAP Authentication

1. Log in as super user.
2. Set the CHAP Secret you want to use for authentication. The character length should be 12-16 characters.

   ```
   # iscsiadm modify initiator-node --CHAP-secret
   Enter secretxxxxxxxxxxxxxxx
   Re-enter secretxxxxxxxxxxxxxxx
   ```
3. (Optional) Set the CHAP name to be used for the authentication. If you choose not to enter a name, the CHAP name becomes the initiator name.

   # iscsiadm modify initiator-node --CHAP-name *iqn.1986-03.com.sun:bd100-a1-000*
4. Enable the CHAP authentication after setting the secret and the CHAP name.

   ```
   # iscsiadm modify initiator-node -authentication CHAP
   ```

Setting Two-way CHAP Authentication

Perform the following procedure after setting one-way CHAP authentication.

1. Enable the two-way CHAP authentication parameters.

   ```
   # iscsiadm modify target-param -B enable
   iqn.1994-04.jp.co.hitachi:rsd.d8a.t.10025.0a000
   ```

2. Set the authentication method to CHAP in two-way.

```
# iscsiadm modify target-param —authentication CHAP
iqn.1994-04.jp.co.hitachi:rsd.d8a.t.10025.0a000
```

3. Set the Target device secret:

```
# iscsiadm modify target-param --CHAP-secret
iqn.1994-04.jp.co.hitachi:rsd.d8a.t.10025.0a000

  Enter secretxxxxxxxxxxxxxxxx

  Re-enter secretxxxxxxxxxxxxxxx
```

Changing iSCSI Initiator Parameters

You can change the following parameters on the iSCSI initiator:

- Header Digest
- Data Digest
- CHAP authentication setting

To change the parameters:

- When the Header Digest is changed to CRC32:

```
# iscsiadm modify initiator-node -h CRC32
```

- When the Data Digest is changed to CRC32:

```
# iscsiadm modify initiator-node -d CRC32
```

Connecting to the Target

You can connect to the target by using either the SendTarget function or discovering the device statically.

Using the SendTarget function

1. Discover the target on the network by specifying the IP address. (When the default value (3260) is used, the Port number can be omitted.)

```
# iscsiadm add discovery-address 192.168.0.200:3260
```

2. Enable the discovered target:

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

3. Connect it to the enabled Target.

```
# devfsadm -i iscsi
```

Discovering the Device Statically

1. Specify the Target Name and the IP address, and discover the Target on the network. (When the default value (3260) is used, the Port number can be omitted.)

```
#iscsiadm add static-config
iqn.1994-
04.jp.co.hitachi:rsd.d8a.t.10025.0a000,192.168.0.200
```

2. Enable the discovered target:

```
#iscsiadm modify discovery-static enable
```

3. Connect it to the enabled Target:

```
# devfsadm -i iscsi
```

If the host can't connect to the target in either method described above, perform the following procedure:

1. Check the configuration of the iSCSI initiator:

```
# iscsiadm list initiator-node
```

2. Confirm that the LAN cable is connected.
3. Use the `ping` command from the host to the target and confirm the response.
4. Use the `ping` command from the target to the host and confirm the response.
5. Confirm that the target configuration is correct.

Configuring iSCSI HBAs

Use the following procedure to configure an iSCSI HBA. Before you begin, verify the HBA is supported by HDS by checking the interoperability information at http://www.hds.com/assets/pdf/simple-modular-storage-100-sms100.pdf.

1. Install the QLogic iSCSI HBA driver according to the manual that comes with the HBA.
2. Install the SANsurfer iSCSI HBA Manager corresponding to the HBA and the Solaris OS according to the vendor's documentation.There are two methods to configure the target setting: remote host and local host.
   - To set the target by remote host (for larger scale networks), install the SANsurfer iSCSI BA Manager GUI on the remote host, and install the agent on the local host. The target information is set by the remote host.
   - To set the target information by the local host (for smaller scale networks), install the SANsurfer iSCSI HBA Manager GUI and Agent on the local host. The target information is set by each local host.

Setting Target Connections

Set the following items for SANsurfer, and describe the necessary items for target connection. Refer to the SANsurfer manual for details.

1. Set the following items in Port Option:
   a. IP Address Subnet Mask–Select the **HBA option** tab and set the IP address and the subnet mask of the HBA port in **Port option – network**.

b. Target Setting–Select the **HBA option** tab.Set the IP address and the subnet mask of the target in the IP address dialog box of **Target settings**. Set the iSCSI name of the target in **iSCSI Name**.

When the Send Target function is used, select **Auto-bind Discovered Targets** other than the settings for IP address and Subnet Mask.

2. Check the target connection status. The **Target Setting** status should be **Session Active**, and the LUN is recognized in the Target Information.

Setting the Header/Data Digest Parameter

1. Select the **HBA Option** tab.
2. Click **Config Authentication** of **Target Setting**.
3. The Security Check dialog box is displayed. Enter the password, and click **OK**.
4. Set enable/disable of the Header Digest/Data Digest.

Setting Authentication Targets

1. Select the **HBA** option tab.
2. Click **Config Authentication** of **Target Setting**.
3. The Security Check dialog box is displayed. Enter the password, and click **OK**.
4. Set the initiator name and the initiator Secret in **CHAP Entries**.
5. Set the CHAP name and the Secret in **Targets**.

Using Sun StorageTek Traffic Manager

If you use Solaris 10 u4 or earlier, you can duplicate the path between Solaris and your array using Sun StorageTek Traffic Manager (commonly called MPxIO) by:

- Editing the file `/kernel/drv/scsi_vhci.conf`.
- Executing the `stmshoot` command.

The following steps provide an example of setting MPxIO in your array. For more information, refer to the Sun Microsystems Web site.

NOTE: If Sun patch for Solaris 10 u5 is installed, ignore this section and use patch 138308-02 (for SPARC) or 138309-02 (for x64/x86). The file `kernel/drv/scsi_vhci.conf` should be the default setting.

1. Edit the file `/kernel/drv/scsi_vhci.conf` as shown below.

   ```
   load-balance="round-robin";
   auto-failback="enable";
   device-type-scsi-options-list = "<vendorID> <productID>",
   symmetric-option = 0x1000000;
   ```

   Specify the VendorID (eight characters) and ProductID (16 characters or less) for device-type-scsi-options-list.

2. Execute the stmshoot command:

```
# stmsboot -e

WARNING: This operation will require a reboot. Do you want to
continue? [y/n] (default: y) y

The changes will come into effect after rebooting the system.
Reboot the system now? [y/n] (default: y) y
```

3. Check the path status after rebooting the host.

```
# mpathadm show lu /dev/rdsk/
c4t60060E80108003A004D3F67A00000000d0s2

Logical Unit:/dev/rdsk/
c4t60060E80108003A004D3F67A00000000d0s2
  mpath-support:libmpscsi_vhci.so
  Vendor:HITACHI
  Product:DF600F
  Revision:0000
  Name Type:unknown type
  Name: 60060e801080004004d3f64400000000
  Asymmetric:no
  Current Load Balance:round-robin
  Logical Unit Group ID:NA
  Auto Failback:on
  Auto Probing:NA
  Paths:
  Initiator Port Name:
  iqn.1986-03.com.sun:01:0003ba0b102d.46fb4a9a,4000002a00ff
  Target Port Name:
  4000002a0000,iqn.1994-
04.jp.co.hitachi:rsd.d8a.t.00058.1a000,1
  Override Path: NA
  Path State: OK
  Disabled: no
  Initiator Port Name:
  iqn.1986-03.com.sun:01:0003ba0b102d.46fb4a9a,4000002a00ff
  Target Port Name:
  4000002a0000,iqn.1994-
04.jp.co.hitachi:rsd.d8a.t.00058.0a000,1
  Override Path:  NA
  Path State: OK
  Disabled: no
```

iSCSI LUN Discovery

The array supports up to 512 logical units per iSCSI port (256 per host group), but the Linux system only supports a maximum of 64 LUNs in one system. If other devices already exist on different host adapters, the number of available LUNs will be reduced.

To set the number of LUNs:

1. Edit the `/etc/modules.conf` file to add a line similar to the following:

   ```
   options scsi_mod max_scsi_luns=16
   ```

2. To set the Emulex driver, add the following line to the `/etc/modules.conf` file:

   ```
   Alias scsi_hostadapter lpfcdd
   ```

3. To activate the above modification, make an image file for booting. For example:

   ```
   # mkinitrd /boot/initrd-2.4.x.scsiluns.img `uname -r`
   ```

Changing the Bootloader Settings

There are two options you can use as Bootloader:

- Linux Loader (LILO)
- Grand Unified Boot Loader (GRUB)

For more information about modifying LILO and GRUB settings, see the Linux Web site

4

VMware

This chapter discusses guidelines on how to prepare a VMware host server for connection to the array and verify that the host server can connect to the target.

This chapter covers the following key topics:

- Preparing the Host Server
- Connecting to the Array
- Configuring iSCSI on the Host
- Setting the Queue Depth Parameter
- Upgrading the Firmware Online
- Creating a Virtual Machine File System
- Attaching a Raw Device
- Using CHAP

Preparing the Host Server

Table 4-1 lists guidelines and tasks you need to follow to prepare the host server.

One or more supported network-interface cards (NIC) with the latest supported Internet Small Computer System Interface (iSCSI) initiator or iSCSI host bus adapters (HBAs) with the latest supported BIOS and driver are required. Verify the NICs, HBAs, and drivers are the latest supported versions by Hitachi Data Systems, and are functioning properly. To check the latest supported versions, refer to the Hitachi interoperability matrix at http://www.hds.com/products/interoperability/.

For information about iSCSI initiators supported by your operating system, refer to the VMware Web site: http://www.vmware.com/.

In addition, a best practices document entitled *Hitachi Adaptable Modular Storage 2000 Family Best Practices for VMware Virtual Infrastructure*, is available to download from the following site: http://www.hds.com/solutions/applications/vmware.html

Table 4-1: Host Server Preparation Guidelines

Item	Task
NICs	Use NICs supported by your array (refer to the Hitachi interoperability matrix) and operating system.
iSCSI HBAs (Optional)	Use the most current iSCSI HBA and drivers supported by your array (refer to the Hitachi interoperability matrix) and operating system. Install all utilities and tools that come with the HBA.
Install the HBA/NIC and iSCSI software initiator in the host server.	For installation information, check the Web sites for your HBA, NIC, and iSCSI initiator. Be sure the HBA, NIC, and iSCSI initiator are supported by your array (refer to the Hitachi interoperability matrix).
VMware ESX Server Operating System	Verify the planned OS version, architecture, relevant patches, and maintenance levels are supported by HDS. Refer to the Hitachi Data Systems interoperability matrix for information on supported versions.

Connecting to the Array

This section provides guidelines on how to connect the array to the host.

Before you connect to the system:

1. Verify the items in Installation Tasks on page 1-3 were completed.
2. Shut down the VMware ESX system.
3. Power off all external devices except for the array.
4. Power off the VMware system.

To connect the array to the VMware system:

1. Install the iSCSI cables between the array and the VMware system. Refer to your array user's guide for details on hardware installation tasks.
2. Power on all peripheral devices. The array should already be turned on, and the iSCSI ports should already be configured. If the array's iSCSI ports are configured after the VMware system is powered on, the system must be restarted to recognize the new devices.
3. Confirm the ready status of all array devices.
4. Power on the VMware system.
5. Log in to the array from VMware.

Configuring iSCSI on the Host

After connecting the array and rebooting the VMware server, configure the iSCSI adapter connected to the array. For information about configuring your iSCSI adapter(s), refer to the documentation that came with your adapter, the Hitachi interoperability matrix and the Server Configuration Guide on the VMware Web site:

http://www.vmware.com/pdf/vi3_301_201_server_config.pdf

The user documentation for your iSCSI adapter should also describe whether other options are required to meet your operational requirements.

After configuring the iSCSI adapter, you may have to reset the VMware server to have the change take effect before restarting the VMware server.

Setting the Queue Depth Parameter

You may need to change the queue depth value on the server. If the number is small, I/O performance can deteriorate.The array reports a queue full status when the queue depth exceeds an allowable limit. The system may not operate correctly when the queue is full and a large value is set. Set an appropriate number according to your configuration. If necessary, set a queue depth number for each server. Refer to the documentation for your HBA before setting a value.

Guidelines for settings:

- 32 commands per LUN
- 512 commands per port
- 30 or more for device timeout value on the Hitachi array LU.

Upgrading the Firmware Online

I/O execution may pause for up to 30 seconds when the online firmware operation starts and finishes.

Creating a Virtual Machine File System

The following procedure describes how to create a VMFS.

1. Log on to your VMware ESX host or to your virtual center using VMware Infrastructure Client. The VMware Infrastructure page appears.
2. With the VMware Infrastructure page displayed:
   a. In the left pane, select a VMware host.
   b. Click the **Configuration** tab in the VMware Infrastructure page.
   c. Under **Hardware** on the left side of the page, click **Storage Adapters**. A page similar to the one in Figure 4-1 on page 4-5 appears.

NOTE: If your **Configuration** tab is not completely populated, do not be concerned. Performing the next step will populate the tab with the LUNs in your system.

3. Click **Rescan** in the top-right area above **Storage Adapters** to scan the NICs or iSCSI HBAs in your system for LUNs.

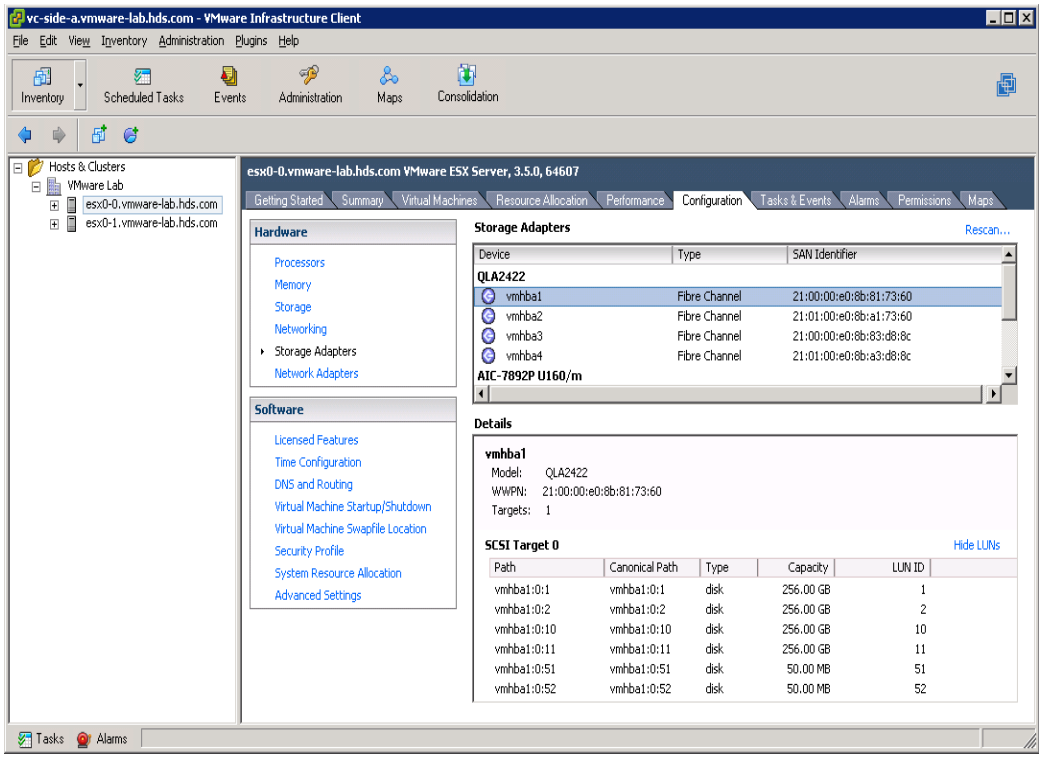

Figure 4-1: Example of Initial VMware Infrastructure Client Page

4. Select a NIC or iSCSI HBA under **Storage Adapters**. Then right-click a LUN in the lower part of the screen (under **SCSI Target 0** in the figure above) and click **Properties**. A LUN Properties dialog box similar to the one in Figure 4-2 appears.

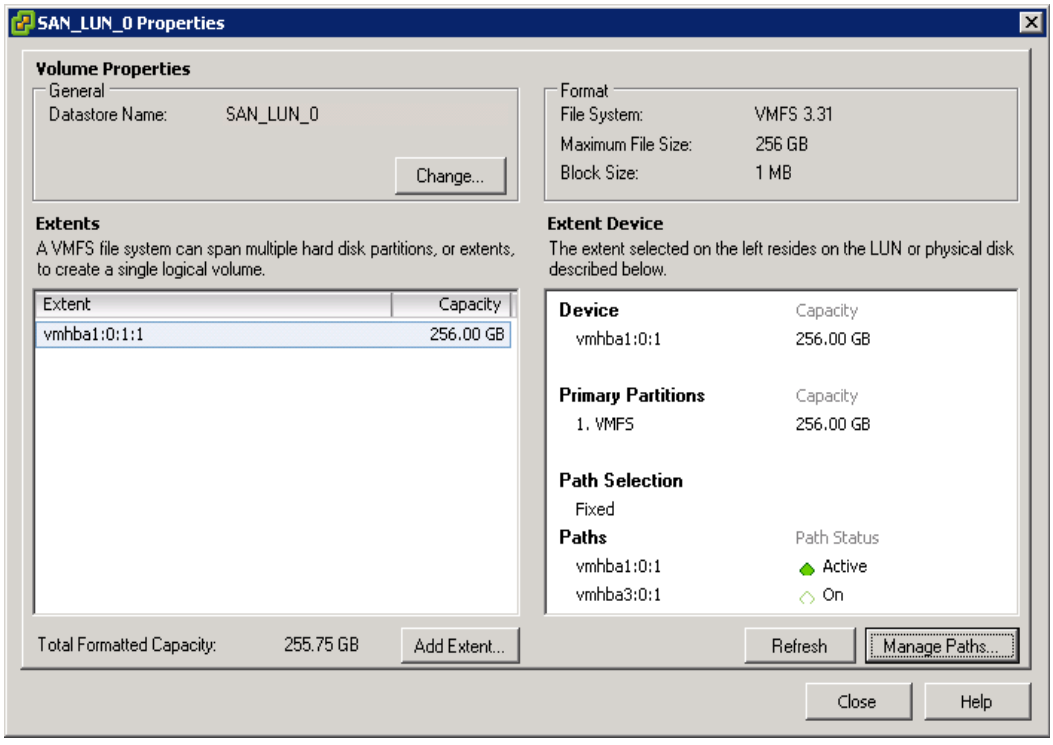

Figure 4-2: Example of LUN Properties Dialog Box

5. In the LUN Properties dialog box, click **Manage Paths**. A Manage Paths dialog box similar to the one in Figure 4-3 appears. This dialog box shows the paths defined for the selected LUN. In the example, below, one path is active while the other path is on.

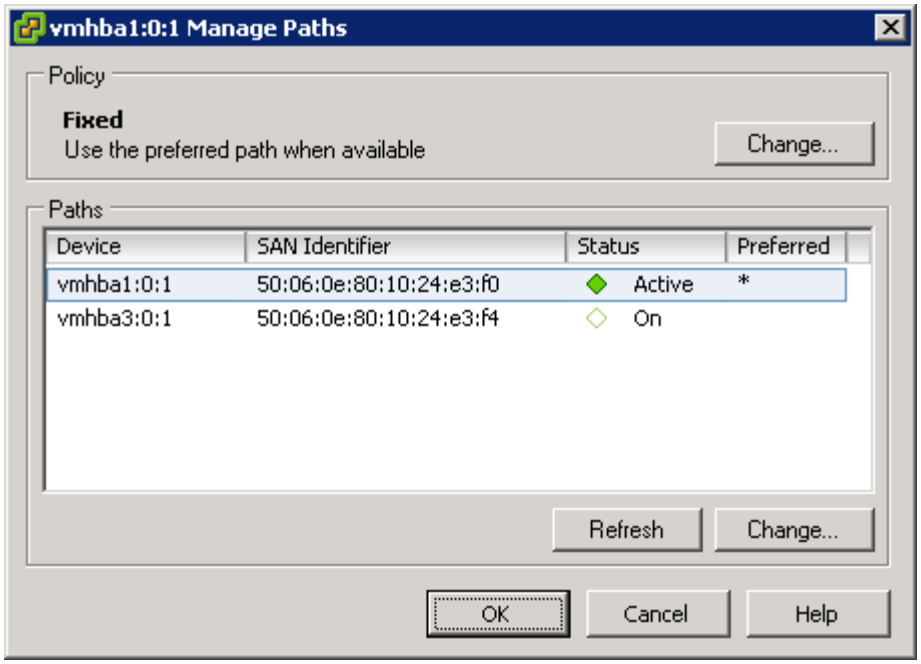

Figure 4-3: Example of Manage Paths Dialog Box

6. In the **Policy** area, click the **Change** button. The Manage Paths - Selection Policy dialog box appears.
7. The default policy is **Most Recently Used**. The recommended path policy is **Fixed** as shown in Figure 4-4.

NOTE: Please apply VMware ESX 3.5 Patch ESX350-200804401-BG, which also sets the default path policy to **Fixed** for HDS systems.

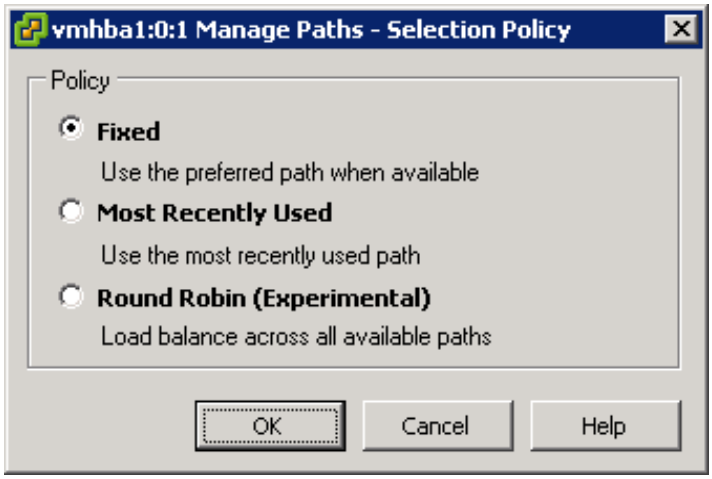

Figure 4-4: Manage Paths - Selection Policy Dialog Box

8. Click **OK** to exit the Manage Paths - Selection Policy dialog box.

9. In the Manage Paths dialog box, click the **Change** button in the lower right side of the dialog box. The Change Path State dialog box appears (see Figure 4-5).

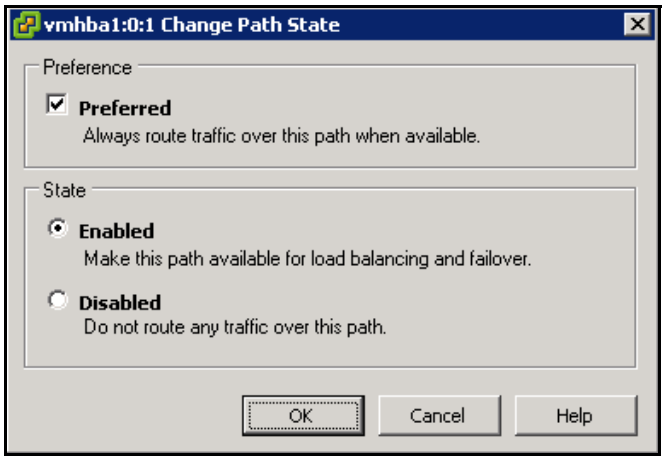

Figure 4-5: Change Path State Dialog Box

10. Under **Preference**, confirm that **Preferred** is checked. Under **State**, confirm that **Enabled** is selected. If these are not configured this way, do so now.
11. Click **OK** to exit the Change Path State dialog box.
12. Click **OK** to exit the Managed Paths dialog box.
13. Click **Close** to exit the LUN Properties dialog box.
14. From the VMware Infrastructure page (see Figure 4-6), select a VMware host in the left pane and click **Storage** under **Hardware**.

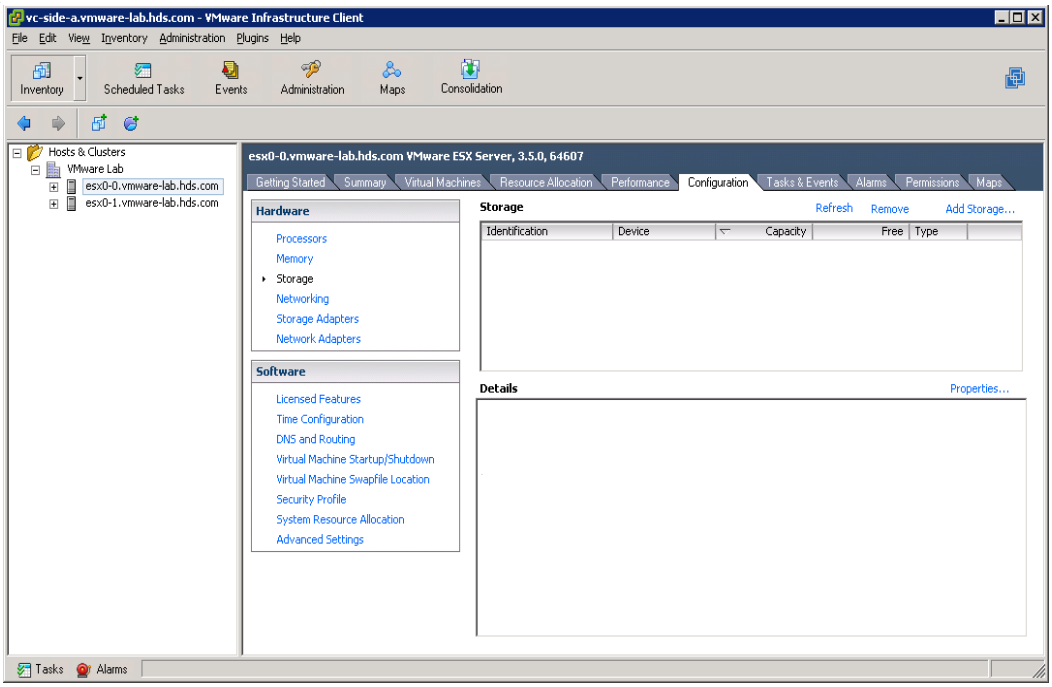

Figure 4-6: Initial VMware Infrastructure Client Page with Storage Selected

15. Click **Add Storage** in the top right the top-right area above **Storage**. The Add Storage Wizard starts, with the Select Storage Type screen displayed (see Figure 4-7).

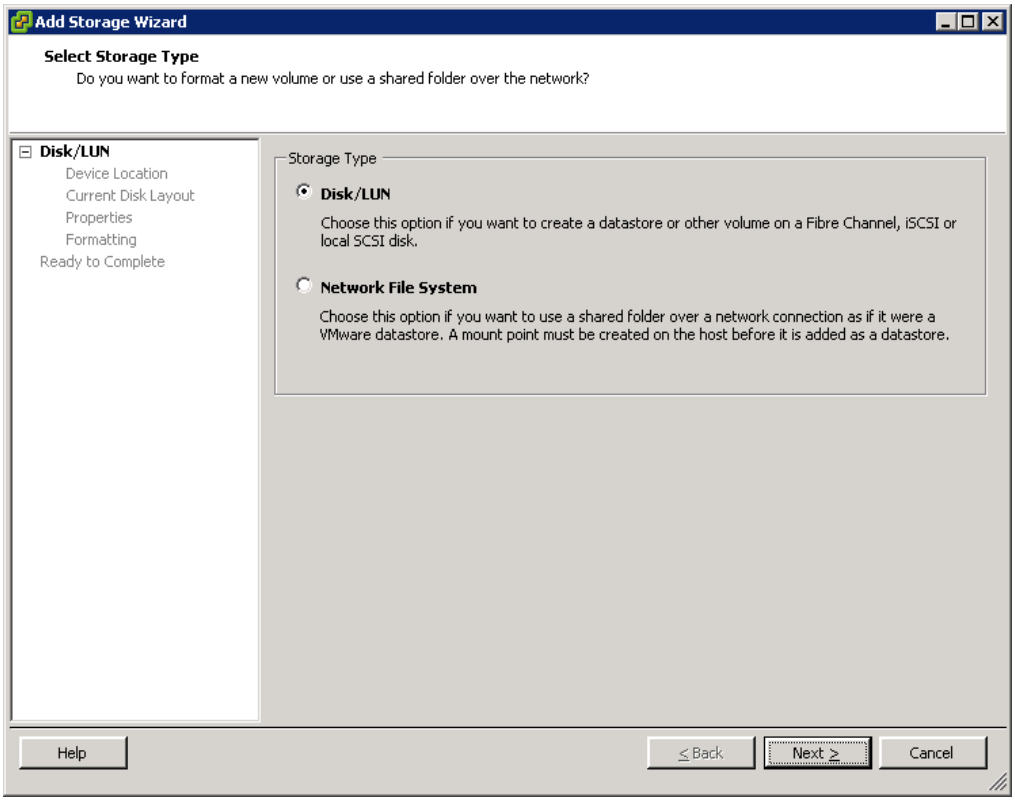

Figure 4-7: Select Storage Type Screen (Add Storage Wizard)

16. Under **Storage Type**, select **Disk/LUN** (if it is not already selected, then click **Next**. The Select Disk /LUN screen appears (see Figure 4-8).

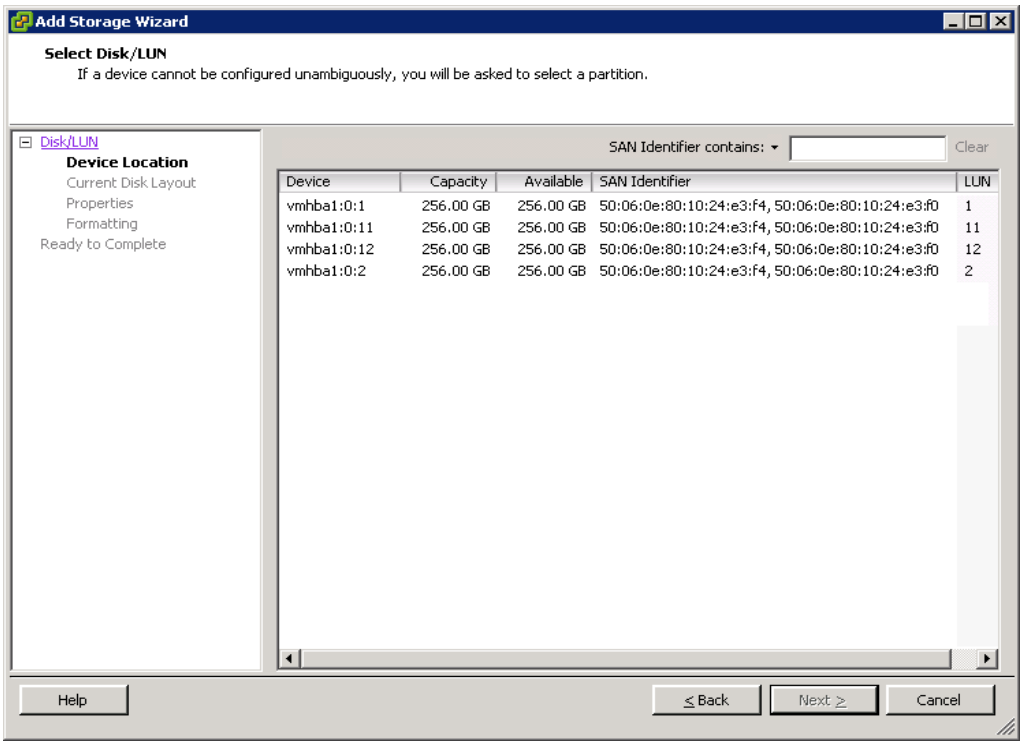

Figure 4-8: Select Disk/LUN Screen (Add Storage Wizard)

17. Select the LUN on which you want to create the VMFS and click **Next**. The Current Disk Layout screen appears (see Figure 4-9).

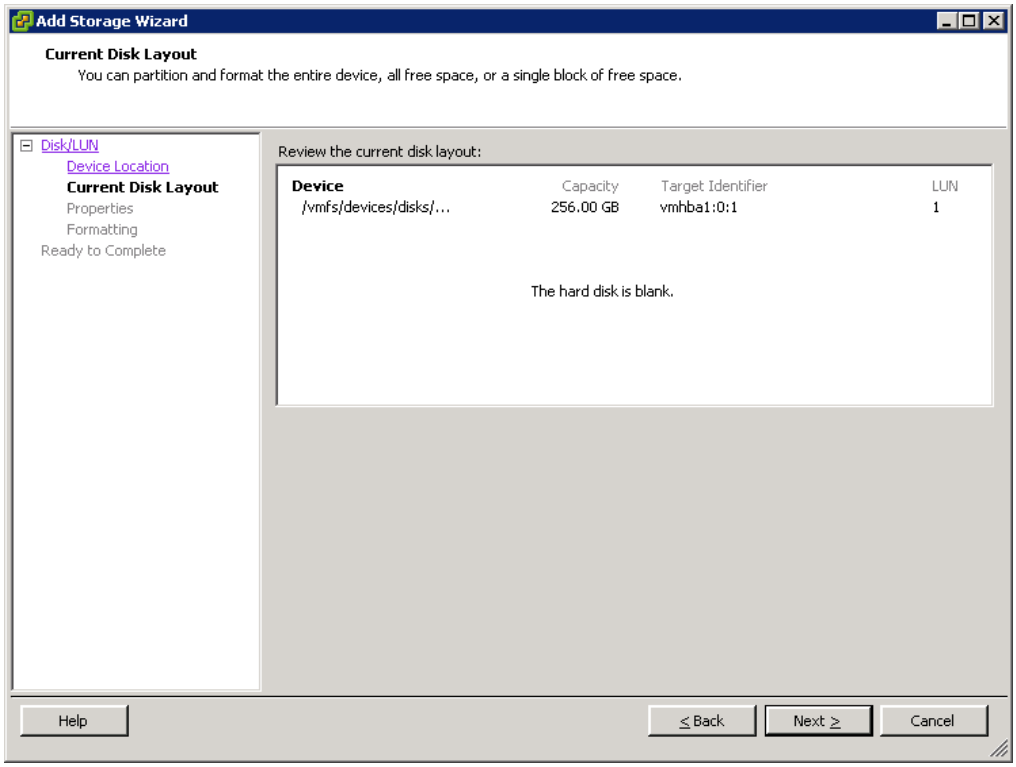

Figure 4-9: Current Disk Layout Screen (Add Storage Wizard)

18. Click **Next**. The Disk/LUN Properties screen appears (see Figure 4-10).

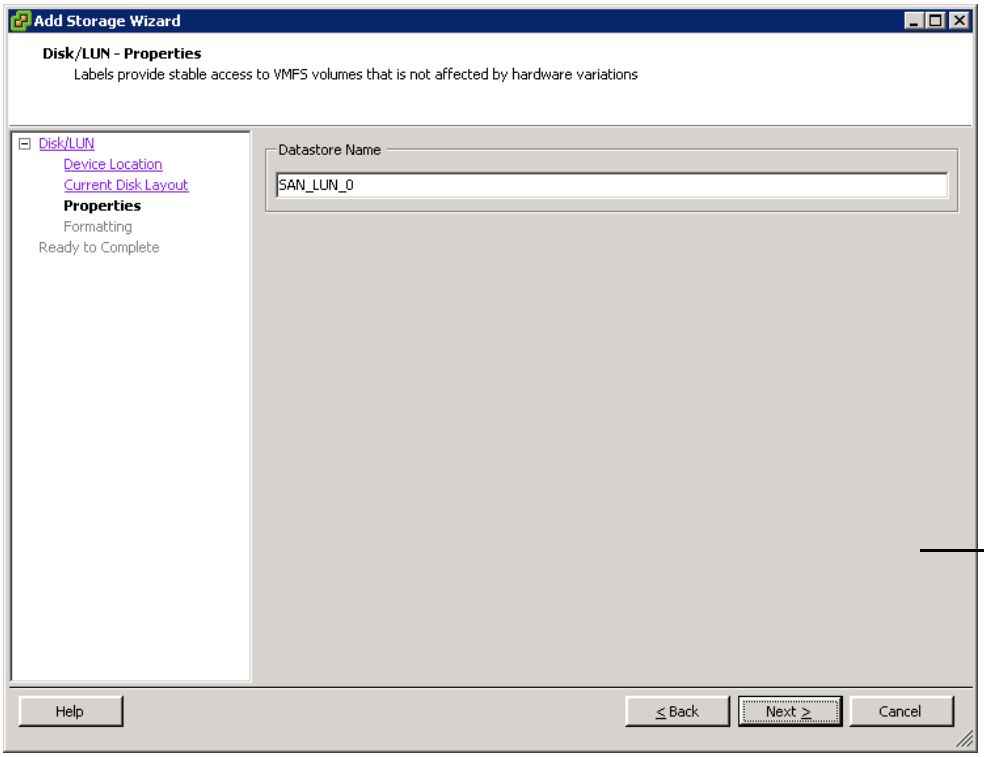

Figure 4-10: Disk/LUN Properties Screen (Add Storage Wizard)

19. Under **Datastore Name**, enter a name for the VMFS volume and click **Next**. The Disk LUN Formatting screen in Figure 4-11 appears.

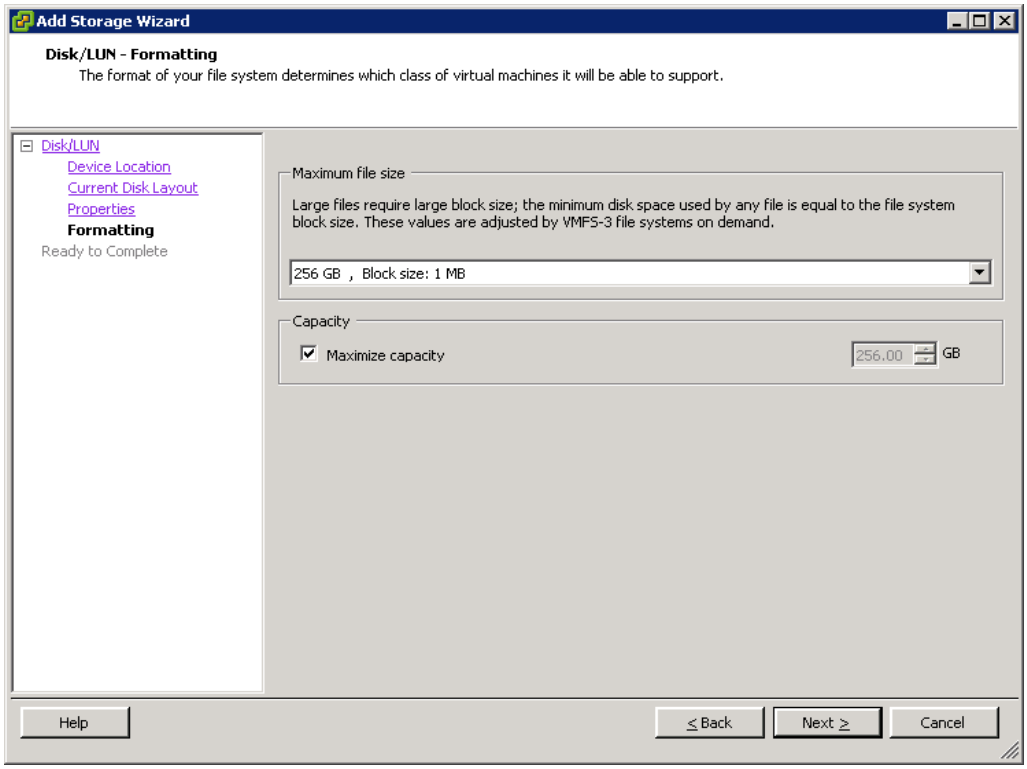

Figure 4-11: Disk/LUN Formatting Screen (Add Storage Wizard)

20. Accept the default selection in the Disk LUN Formatting screen and confirm that **Maximize capacity** under **Capacity** is checked.
21. Click **Next**. The Ready to Complete screen appears (see Figure 4-12).

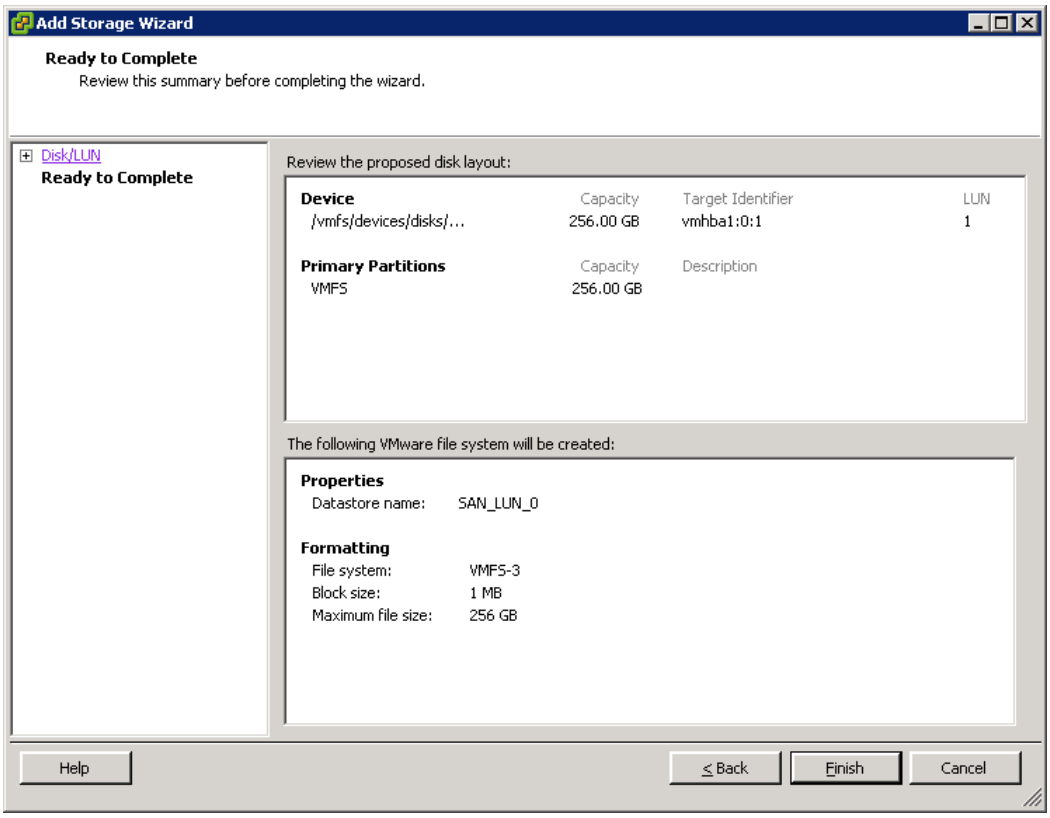

Figure 4-12: Ready to Complete Screen (Add Storage Wizard)

22. Review the summary information displayed. If you need to change a setting, click the **Back** button to return to the appropriate screen, change the setting, and click **Next** until you return to the Ready to Complete screen.
23. After confirming that the settings are correct, click **Finish**. The VMware Infrastructure page appears, with your LUN/VMFS settings displayed (see Figure 4-13 on page 4-12).

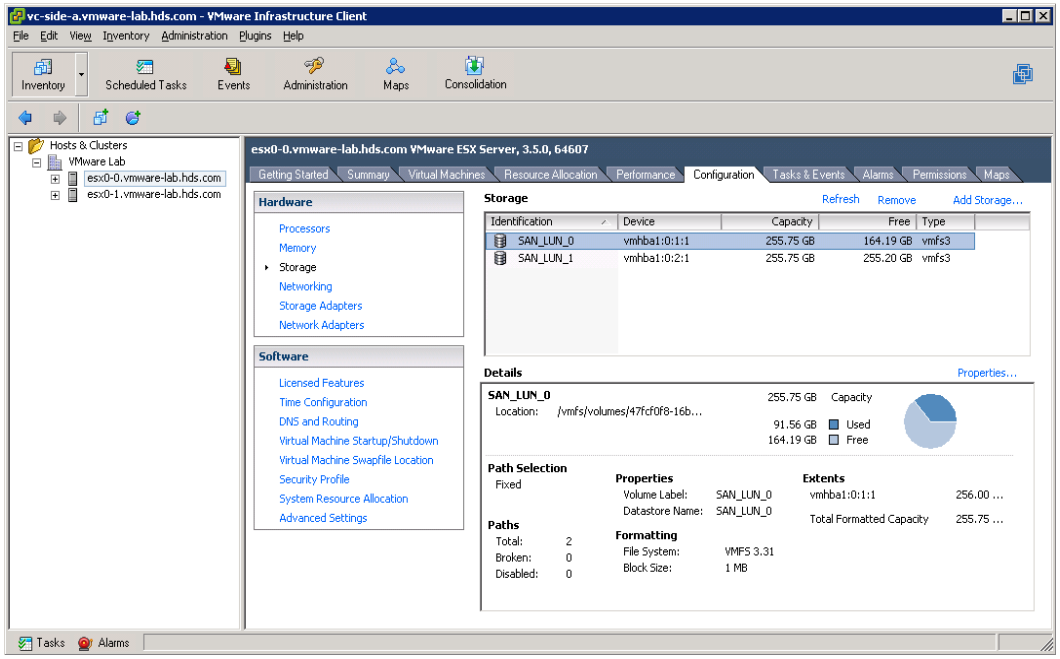

Figure 4-13: Example of VMware Infrastructure Page

24. If needed, repeat steps 15 through 23 to create additional VMFS's.

TIP: On any additional hosts that will have access to the LUNs, you do not have to create the VMFS's again. Instead, on the other host, click **Refresh** above **Storage** on the VMware Infrastructure page (see Figure 4-13).

This completes the procedure for creating a VMFS. Proceed to the section below for instructions on attaching a raw device.

Attaching a Raw Device

The following procedure describes how to attach a raw device, such as a command device, to a virtual machine.

1. From the VirtualCenter client, right-click a virtual machine and select **Edit Settings**. The Virtual Machine Properties dialog box appears (see Figure 4-14 on page 4-13).

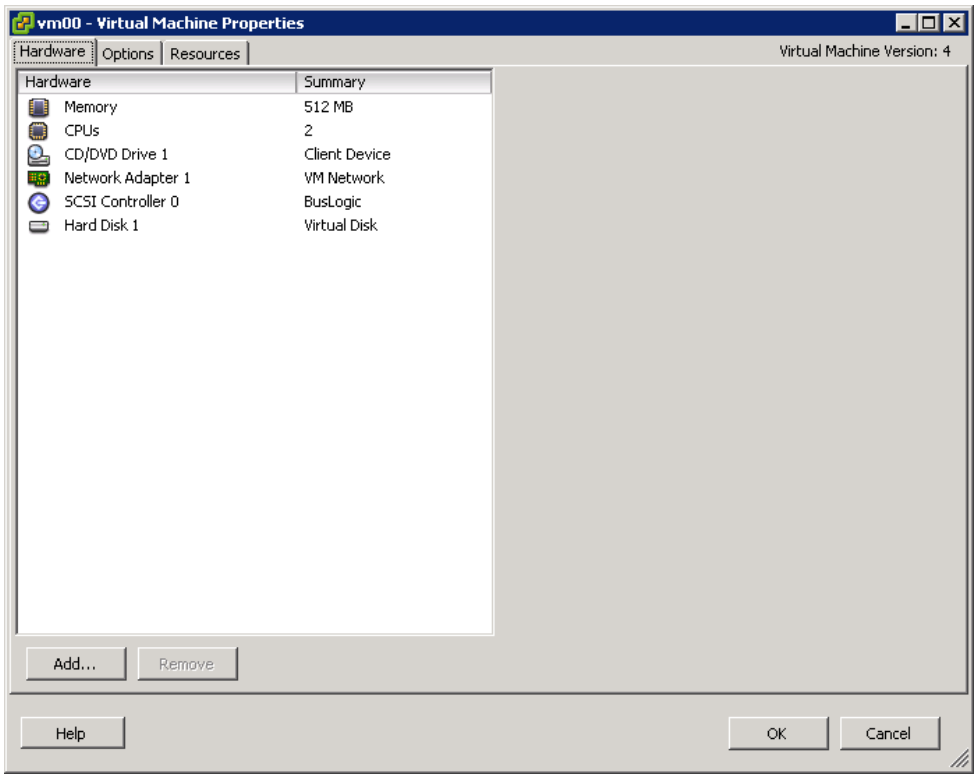

Figure 4-14: Virtual Machine Properties Dialog Box

2. Select **Add**. The Add Hardware Device wizard starts, with the Select Device Type screen displayed (see Figure 4-15).

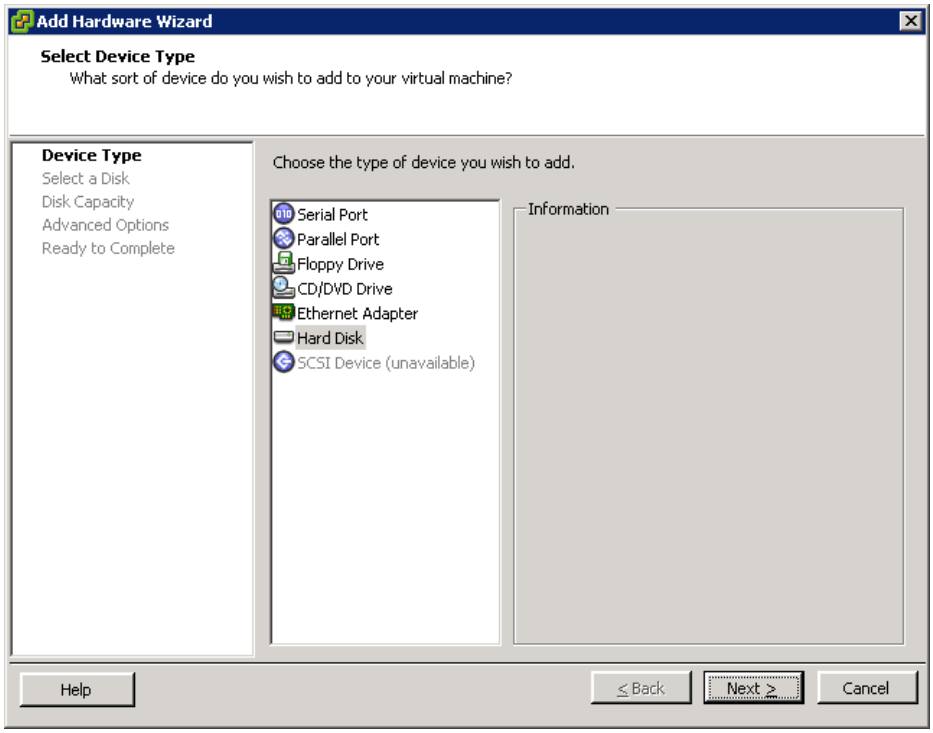

Figure 4-15: Select Device Type Screen (Add Hardware Wizard)

3. Select **Hard Disk** and click **Next**. The Select a Disk Screen appears.

4. Select **Raw Device Mappings**, as shown in Figure 4-16.

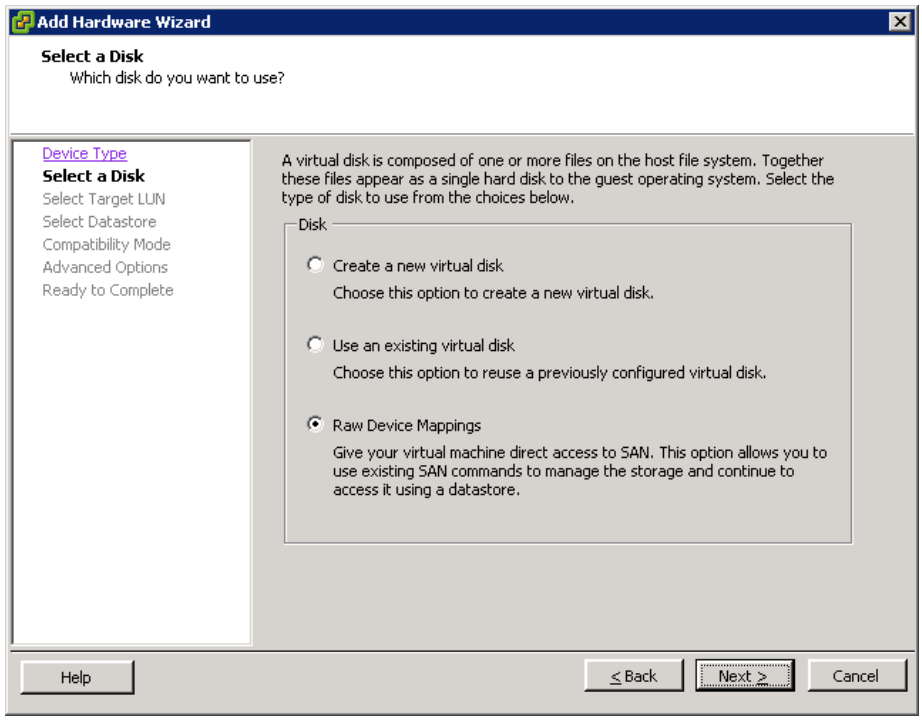

Figure 4-16: Select a Disk Screen (Add Hardware Wizard)

5. Click **Next**. The Select and Configure a Raw LUN screen appears (see Figure 4-17).

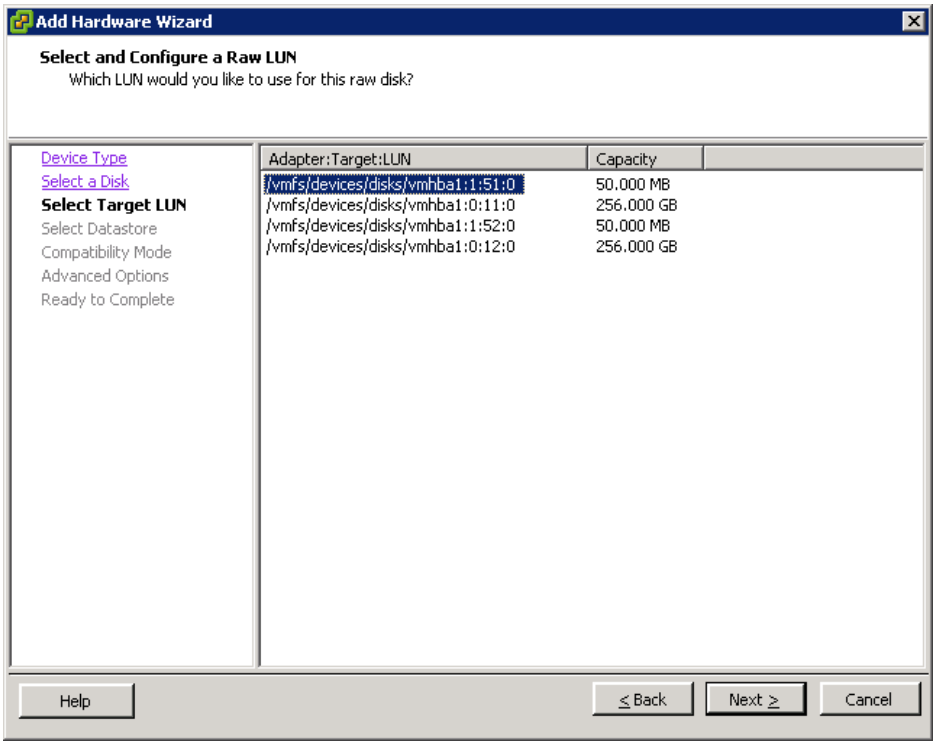

Figure 4-17: Select and Configure a Raw LUN Screen (Add Hardware Wizard)

6. Select the LUN you want to use for the raw device (Command Device) and click **Next**. The Select a Datastore screen appears (see Figure 4-18).

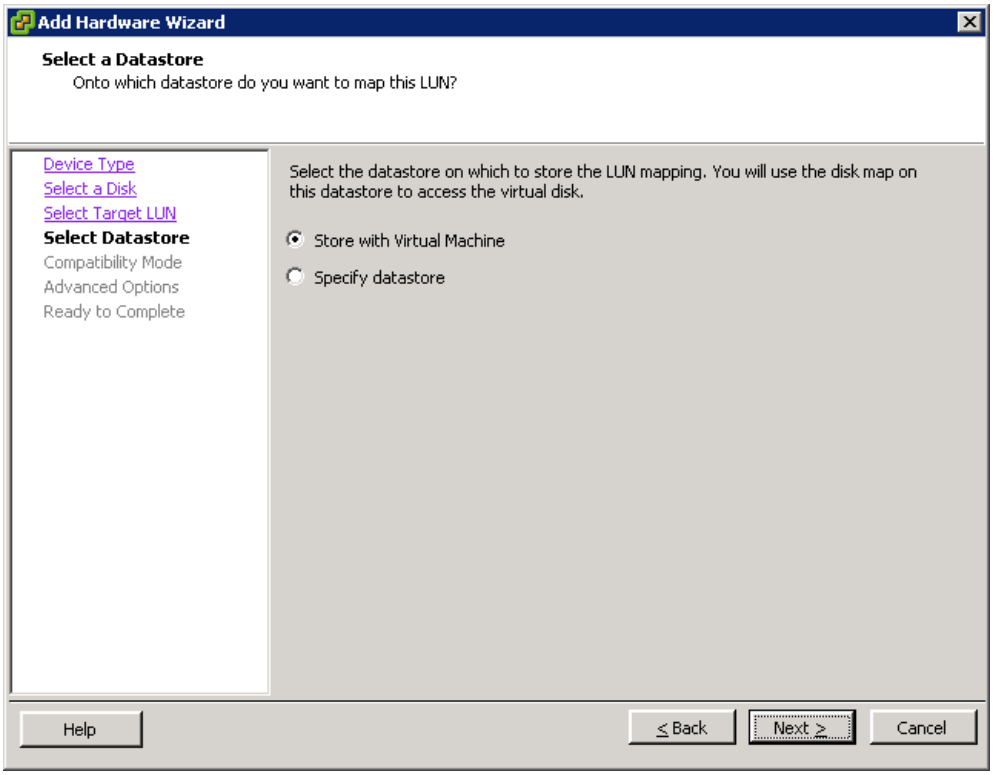

Figure 4-18: Select a Datastore Screen (Add Hardware Wizard)

7. Confirm that **Store with Virtual Machine** is selected. If it is not, select it.
8. Click **Next**. The Select Compatibility Mode screen appears (see Figure 4-19 on page 4-16).

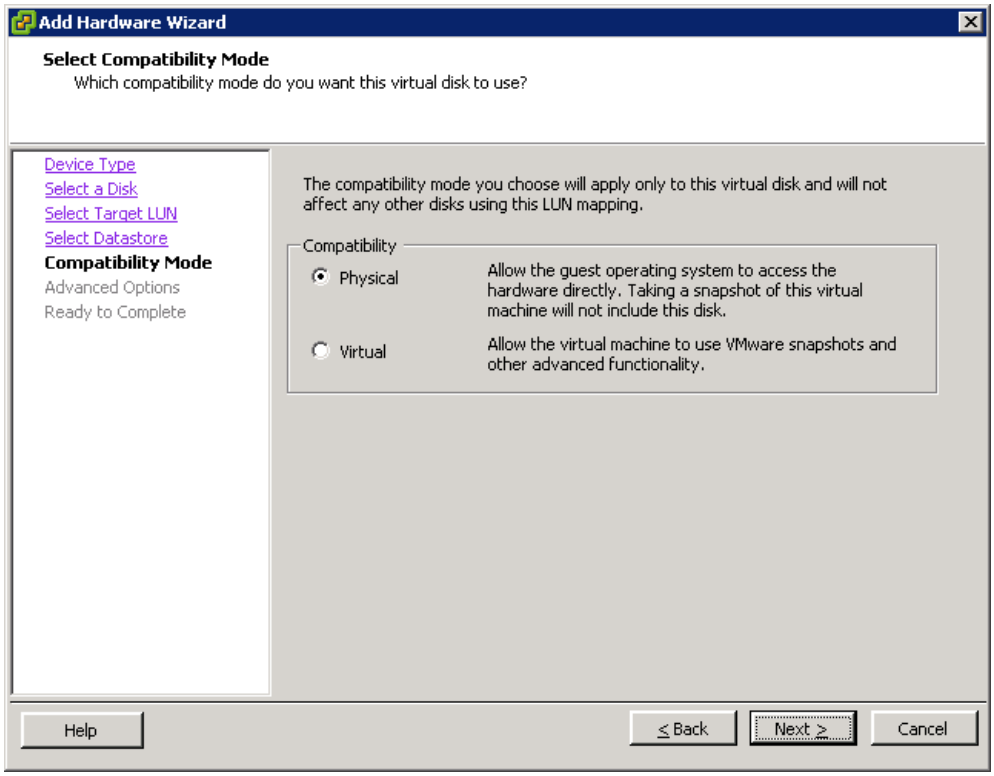

Figure 4-19: Select Compatibility Mode (Add Hardware Wizard)

9. Under **Compatibility**, confirm that **Physical** is selected. If it is not selected, select it.
10. Click **Next**. The Specify Advanced Options screen appears (see Figure 4-20).

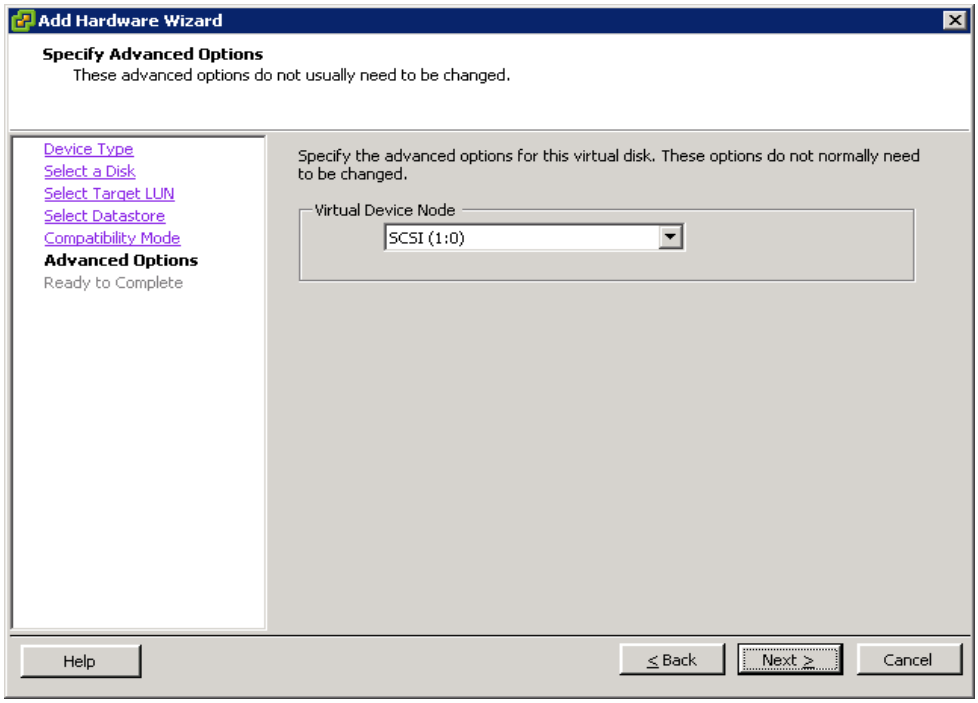

Figure 4-20: Specify Advanced Options Screen (Add Hardware Wizard)

11. Under **Virtual Device Node**, select a virtual device node local to the Virtual Machine.
12. Click **Next**. The Ready to Complete Screen appears (see Figure 4-21).

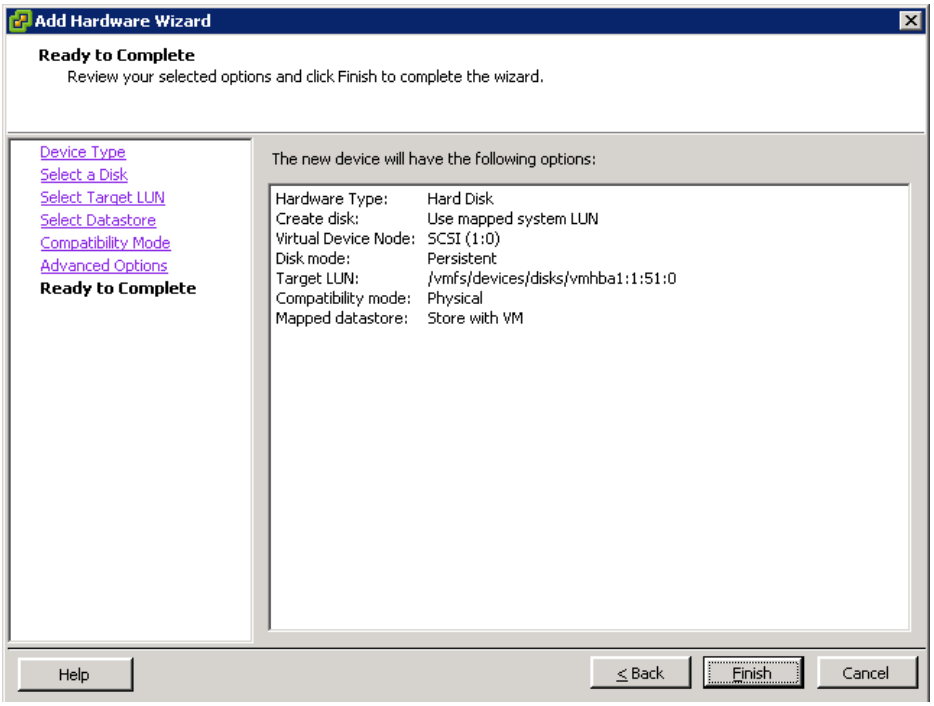

Figure 4-21: Ready to Complete Screen (Add Hardware Wizard)

13. Review the summary information displayed. If you need to change a setting, click the **Back** button to return to the appropriate screen and change the setting. To confirm that the settings are correct, click **Finish**. The Virtual Machine Properties dialog box appears (see Figure 4-22).

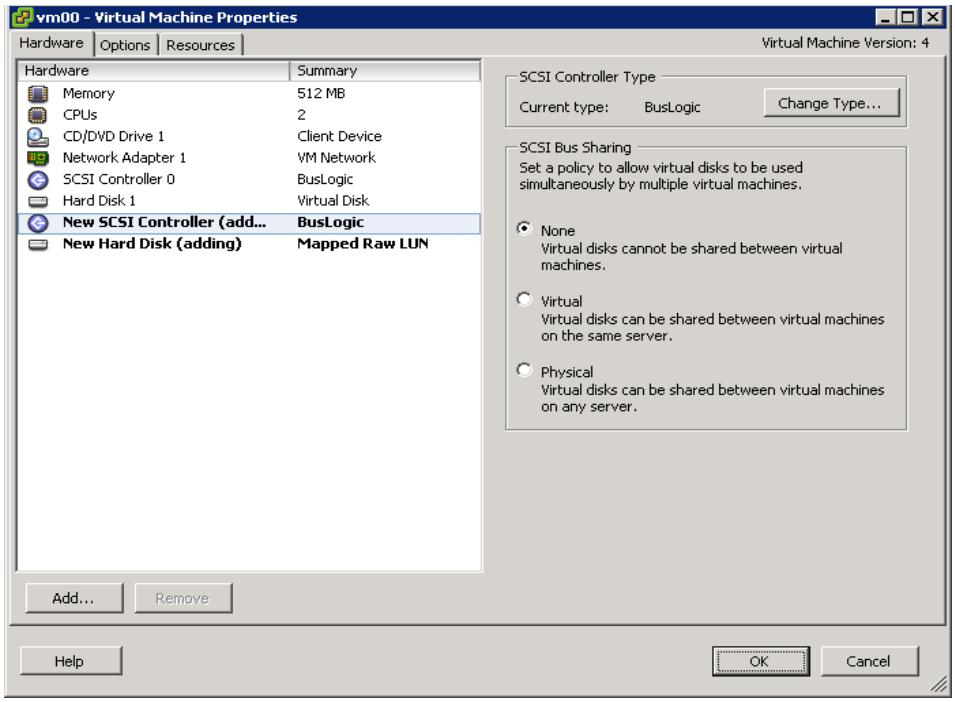

Figure 4-22: Virtual Machine Properties Dialog Box

14. Click **OK** to exit the Virtual Machine Properties dialog box.
15. Right-click the same virtual machine and select **Edit Settings**. The Virtual Machine Properties dialog box appears, with the new SCSI controller and hard disk you added (see Figure 4-23).

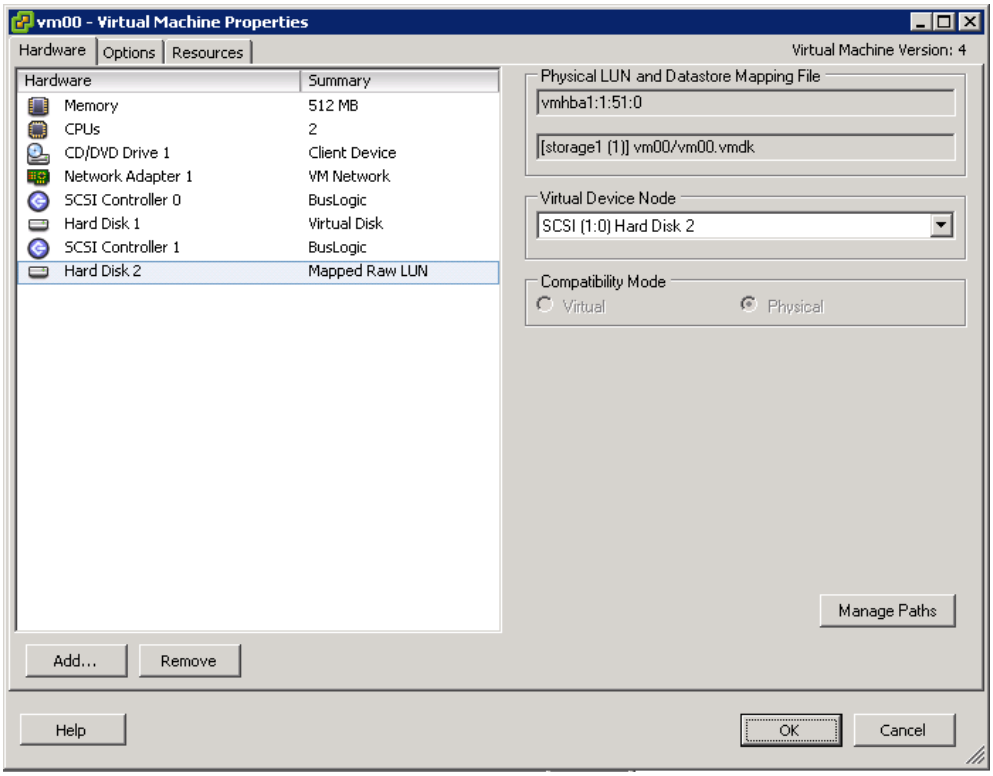

Figure 4-23: Example of Virtual Properties Dialog Box with New SCSI Controller and Hard Disk Added

16. Click **Cancel** to exit the Virtual Properties dialog box.

This completes the procedure for adding a raw device.

Using CHAP

To use CHAP on an iSCSI connection, use Navigator 2 to enable the option **Discovery CHAP Mode** on the array. For additional information about using Navigator 2, refer to the Navigator 2 online help.

1. Launch a browser on the management console and log in to Navigator 2:

   http://<*IP address*>:23015/StorageNavigatorModular/Login

   OR

   https://<*IP address*>:23016/StorageNavigatorModular/Login

   where <*IP address*> is the IP address of the management console.

NOTE: If entering an IPv6 address in your Web browser, enter the URL in brackets. Example: http://[xxxx]:23015/StorageNavigatorModular/Login

2. In the Arrays page, click the array you want to configure.

3. In the Arrays pane, click **Groups > iSCSI Targets**. The iSCSI Targets page appears, with the **iSCSI Targets** tab displayed (see Figure 4-24).

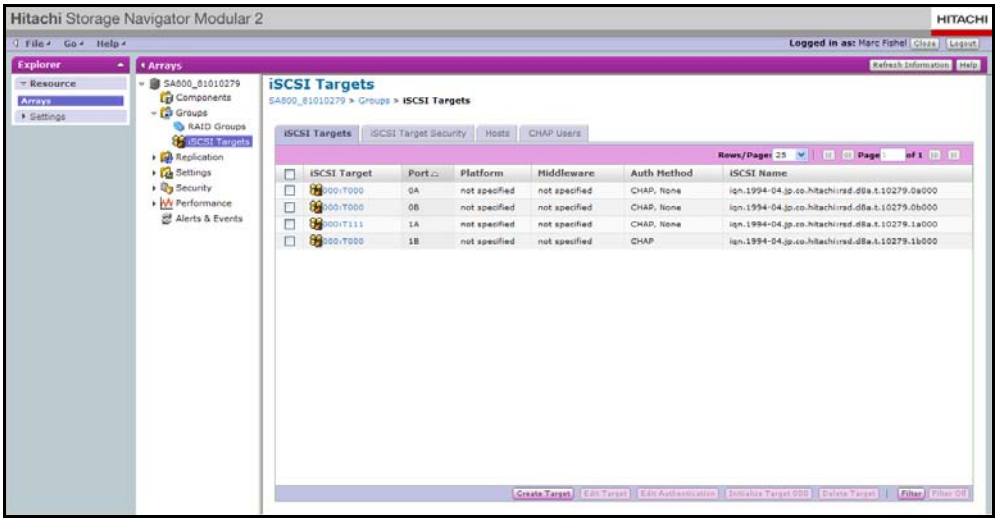

Figure 4-24: iSCSI Targets Page

4. In the **iSCSI Targets** tab, check an iSCSI target and then click **Edit Target**. The Edit iSCSI Target window appears, with the **Logical Units** tab displayed.
5. Click the **Options** tab (see Figure 4-25 on page 4-20).

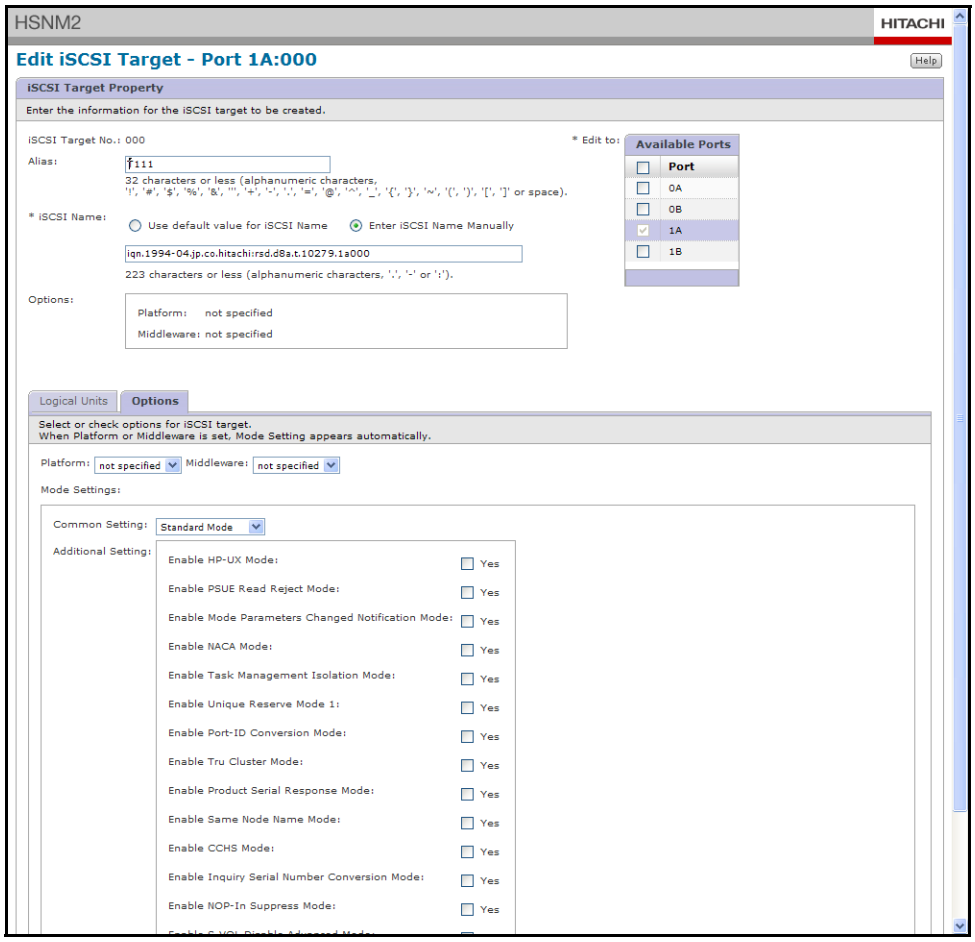

Figure 4-25: Edit ISCSI Target Window with Options Tab Displayed

6. For **Platform**, select **VMware**. Discovery CHAP Mode is selected automatically when **VMware** is selected as the **Platform**.
7. Click **OK**.

5

Red Hat Enterprise Linux

This chapter discusses guidelines on how to prepare a Red Hat Enterprise Linux host server for connection to the array and verify that the host server can connect to the target.

This chapter covers the following key topics:

- Preparing the Host Server
- ISCSI Initiator Considerations
- Guidelines for Using iSCSI
- Setting Queue Depth
- High Availability (HA) Cluster Configurations
- HA Multipath Configurations

Preparing the Host Server

Table 5-1 lists guidelines and tasks you need to follow to prepare the host server.

One or more supported network-interface cards (NIC) with the latest supported Internet Small Computer System Interface (iSCSI) initiator or host bus adapters (HBA) with the latest supported BIOS and driver are required. Verify the NICs, HBAs, drivers, and BIOSes are the latest supported versions by Hitachi Data Systems, and are functioning properly. To check the latest supported versions, refer to the Hitachi interoperability matrix at http://www.hds.com/products/interoperability/.

For information about iSCSI initiators supported by your operating system, refer to the Red Hat Linux Web site at http://www.redhat.com.

Table 5-1: Host Server Preparation Guidelines

Item	Task
iSCSI NICs	Use NICs supported by your array (refer to the Hitachi interoperability matrix) and operating system.
iSCSI HBAs (Optional)	Use the most current iSCSI HBA and drivers/BIOSes supported by your array (refer to the Hitachi interoperability matrix) and operating system. Install all utilities and tools that come with the HBA.
Install the HBA/NIC and iSCSI software initiator in the host server.	For installation information, check the Web sites for your HBA, NIC, and iSCSI initiator. Be sure the HBA, NIC, and iSCSI initiator are supported by your array (refer to the Hitachi interoperability matrix).
Linux operating system	Verify the planned OS version, architecture, relevant patches, and maintenance levels are supported by Hitachi Data Systems. Refer to the Hitachi interoperability matrix for information about supported versions.

ISCSI Initiator Considerations

The following list describes the requirements for using the array with iSCSI. For current requirements, please contact your Hitachi Data Systems representative.

- Hitachi Storage Navigator Modular 2 v1.0.0-00 or higher.
- Use the latest supported firmware for your array.
- The NIC, iSCSI HBA, and Ethernet switch connected to the array must support the Institute of Electrical and Electronics Engineers (IEEE) 802.3ab 1000Base-T, full-duplex operations.
- Category 5e (enhanced Category 5) or Category 6 network cabling.
- Set operating system parameters if needed.

Guidelines for Using iSCSI

Observe the following guidelines when using iSCSI:

- Do not change the Challenge Handshake Authentication Protocol (CHAP) authentication settings that correspond to hosts that are logging in to the array. If you disable CHAP authentication for the array while it is communicating with software initiator using CHAP authentication, the host will not be able to access the target device without rebooting.
- Stop all unused applications and services to eliminate extraneous operations and reduce server loads.

Downloading and Configuring the iSCSI Initiator

The array can communicate with hosts through iSCSI connections. This section gives guidelines on downloading and configuring the iSCSI Initiator for Linux.

Downloading the iSCSI Initiator

Some versions of the Linux OS may provide the iSCSI initiator for download. If your Linux OS does not provide the initiator, download it from one of the following Web sites:

- For Red Hat Enterprise Linux 4

  http://linux-iscsi.sourceforge.net/
- For Red Hat Enterprise Linux 5

  http://www.open-iscsi.org/

Download all the necessary files to install iSCSI initiator from the Web site. Install the iSCSI software initiator according to the documentation provided with it.

Configuring the iSCSI Initiator

This section discusses how to configure the `iscsi.conf` file, a file that controls and configures the iSCSI initiator.

iSCSI.conf Configuration for Red Hat Enterprise Linux 4

1. Start the iSCSI driver software service.
2. Change the host login to the specified target in `iscsi.conf`. You do not need to reboot the host.
3. Stop the iSCSI service:

   ```
   service open-iscsi stop
   ```

4. Modify the file and set up the configuration.
5. Type the following command for the iSCSI initiator to automatically login to the specified targets:

   ```
   service open-iscsi start
   ```

iSCSI.conf Configuration for Red Hat Enterprise Linux 5

1. Start the iSCSI service:

   ```
   service open-iscsi start
   ```

2. Find the target LUN:

   ```
   iscsiadm -m discovery
   ```

3. Display the target list:

   ```
   iscsiadm -m node
   ```

4. Log in to the target:

   ```
   iscsiadm -m node -L
   ```

5. Stop the iSCSI service:

   ```
   service open-iscsi stop
   ```

6. Customize the system by modifying the `iSCSI.conf` file.
7. Allow the initiator to automatically log in to the specified targets:

   ```
   service open-iscsi start
   ```

Connecting to the Array

This section provides guidelines on how to connect the array to the host.

Before you connect to the system:

1. Verify the items in Table 1-1 on page 1-3 were completed.
2. Connect the array to the Red Flag Linux Asianux Red Hat Linux server.
3. Install the Ethernet cables between the array and the Linux server. Refer to the user's guide for your array for details on hardware installation tasks.

4. Execute the ping command to confirm whether the cabling and IP addresses are correct.
5. For Red Hat Enterprise Linux 4 and 5, edit the \etc\iscsi.conf\ file and start the iSCSI service to see the devices.
6. Log in to the array from Linux.

iscsi.conf Notes

- The array does not support mutual CHAP authentication on Linux hosts.
- The minimum setting to iscsi.conf allows Linux iSCSI software initiator to start at the minimum level support. See the example below.

```
TargetName=iqn.1994-
04.jp.co.hitachi:rsd.d8h.t.00005.0a000

DiscoveryAddress=192.168.0.200

PingTimeout=60
```

Setting the iSCSI Data and Header Digests

Use the iSCSI Header and Data digest with an L3 switch (including a router) in the hosts and array iSCSI port.

Table 5-2: Data Digest and Header Digest Parameter Settings

Parameter	Definition	Negotiation Value on iSCSI Login
Always	Always enable digest	CRC32C
Never	Always disable digest	none
Prefer-on	Prioritize enabling over disabling	CRC32C, none
Prefer-off	Prioritize disabling over enabling	None, CRC32C

In the Data and Header digest, select **Enabling / Disabling CRC / Checksum**. Enabling Header digest may decrease performance by nearly 90%, depending on network configuration, host performance, and host applications. iSCSI Data digest and Header digest should be used with an L3 switch or router that is in the path of the hosts and the array iSCSI port. Set the parameters to:

- HeaderDigest=always
- DataDigest=always

CHAP Authentication

The array does not support mutual CHAP authentication with Linux software initiators.

Setting CHAP

CHAP provides authentication of iSCSI users. If you use CHAP security, Username and secret are set to both the host and array iSCSI port. Table 5-3 shows the CHAP parameters and their definitions and values.

Table 5-3: Setting Value of CHAP Authentication

Parameter	Meaning	Negotiation Value on iSCSI Login
OutgoingUsername	Username for authentication of initiator	Username of CHAP User
OutgoingPasword	Password for authentication of initiator	Secret of CHAP User
IncomingUsername	Username for authentication of target	Username of Target
IncomingPassword	Password for authentication of target	Secret of Target

Setting Keep Alive Timer Parameter

The parameters `IdleTimeout`, `ActiveTimeout` and `PingTimeout` control the Keep Alive Timer. To change the time setting in the `PingTimeout` parameter, do the following:

1. Find the line `#PingTimeout=<number>` in the `iscsi.conf` file.
2. Delete the comment out symbol (#).
3. Change `<number>` to 60.

See the example below:

```
Change: #PingTimeout=<number>

To: PingTimeout=60
```

Configuring an iSCSI HBA

Follow the procedures below to configure an iSCSI HBA. Before you begin, verify the HBA is supported by HDS by check the interoperability information at http://www.hds.com/products/interoperability/.

1. Install the QLogic iSCSI HBA driver according to the documentation for the HBA.

2. Install the SANsurfer iSCSI HBA Manager corresponding to the HBA and the Linux OS according to the vendor's documentation.There are two methods to configure the target setting: remote host and local host.
   a. To set the target by remote host (for larger scale networks), install the SANsurfer iSCSI HBA Manager GUI on the remote host, and install the agent on the local host. The target information is set by the remote host.
   b. To set the target information by the local host (for smaller scale networks), install the SANsurfer iSCSI HBA Manager GUI and Agent on the local host. The target information is set by each local host.

Setting Target Connections

Set the following items for SANsurfer, and describe the necessary items for target connection. Refer to the SANsurfer manual for details.

1. Set the following items in Port Option:
   a. IP Address Subnet Mask — Select the **HBA option** tab and set the IP address and the subnet mask of the HBA port in **Port option – network**.
   b. Target Setting — Select the **HBA option** tab.Set the IP address and the subnet mask of the Target in the IP address dialog box of **Target settings**. Set the iSCSI Name of the Target in **iSCSI Name**.

      When the Send Target function is used, select **Auto-bind Discovered Targets** other than the settings for IP address and Subnet Mask.
2. Check the Target connection status. The **Target Setting** status should be **Session Active**, and the LUN is recognized in the Target Information.

Setting the Header/Data Digest Parameter

1. Select the **HBA Option** tab.
2. Click **Config Authentication** of **Target Setting**.
3. The Security Check dialog box is displayed. Enter the password, and click **OK**.
4. Set enable/disable of the Header Digest/Data Digest.

Setting Authentication Targets

1. Select the **HBA** option tab.
2. Click **Config Authentication** of **Target Setting**.
3. When the Security Check dialog box appears, enter the password and click **OK**.
4. Set the initiator name and the initiator secret in **CHAP Entries**.
5. Set the CHAP name and the Secret in **Targets**.

Setting Queue Depth

You may need to change the queue depth value on the server. If the number is small, I/O performance can deteriorate.The array reports a queue full status when the queue depth exceeds an allowable limit. The system may not operate correctly when the queue is full and a large value is set. Set an appropriate number according to your configuration. If necessary, set a queue depth number for each server. Refer to the documentation for your HBA before setting a value.

Guidelines for settings:

- 32 commands per LUN
- 512 commands per port
- 30 or more for device timeout value on the array LU.

High Availability (HA) Cluster Configurations

The Hitachi AMS 2000 Family storage system is compatible with various cluster software applications. For more information about:

- Compatible cluster software applications, refer to the Hitachi Data Systems interoperability matrix at http://www.hds.com/products/interoperability/.
- Installing and configuring the cluster software, refer to the documentation provided by the cluster software vendor.

HA Multipath Configurations

The Hitachi AMS 2000 Family storage system supports various HA multipathing software products for the Red Hat Enterprise Linux operating system. Refer to the Hitachi Data Systems interoperability matrix at http://www.hds.com/products/interoperability/ for currently supported HA software applications. Then consult the documentation provided by the HA multipathing vendor for information about installing, configuring, operating, and best practices when using the software with Active/Active storage systems like the Hitachi AMS 2000 Family storage systems.

If the Hitachi Data Systems interoperability matrix show that Red Hat Enterprise Linux's bundled multipathing software, referred to as “Device Mapper,” is supported for the intended Red Hat operating system version / update level and you want to use this bundled Multipath solution, refer to the appropriate Red Hat Device Mapper documentation for proper installation, configuration, and operation. Some Device Mapper release level documentation can be obtained at the following link:

http://www.redhat.com/docs/en-US/Red_Hat_Enterprise_Linux/5.4/html/DM_Multipath/queueifnopath_issues.html

To ensure Active/Active I/O activity by the host Linux I/O to the Hitachi AMS 2000 Family storage system, confirm that the following minimum parameters are set in the file `/etc/multipath.conf`:

- Vendor: Hitachi

- Product: DF600F
- Path_grouping _policy: Multibus

Install and configure the multipathing software on the server before connecting the server to the Hitachi AMS 2000 Family storage system.

6

SuSE Linux Enterprise Server

This chapter discusses guidelines on how to prepare a SuSE Linux Enterprise server for connection to the array and verify that the host server can connect to the target.

This chapter covers the following key topics:

- Preparing the Host Server
- ISCSI Initiator Considerations
- Guidelines for Using iSCSI
- Setting Queue Depth
- iSCSI LUN Discovery
- High Availability (HA) Cluster Configurations
- HA Multipath Configurations

Preparing the Host Server

Table 6-1 lists guidelines and tasks you need to follow to prepare the host server.

One or more supported network-interface cards (NIC) with the latest supported Internet Small Computer System Interface (iSCSI) initiator or host bus adapters (HBA) with the latest supported BIOS and driver are required. Verify the NICs, HBAs, drivers, and BIOSes are the latest supported versions by Hitachi Data Systems, and are functioning properly. To check the latest supported versions, refer to the Hitachi interoperability matrix at http://www.hds.com/products/interoperability/.

For information about iSCSI initiators supported by your operating system, refer to the SLES Web site: http://www.novell.com/linux/.

Table 6-1: Host Server Preparation Guidelines

Item	Task
NICs	Use NICs supported by your array (refer to the Hitachi interoperability matrix) and operating system.
iSCSI HBAs (Optional)	Use the most current iSCSI HBA and drivers/BIOSes supported by your array (refer to the Hitachi interoperability matrix) and operating system. install all utilities and tools that come with the HBA.
Install the HBA or iSCSI software initiator in the host server.	For installation information, check the Web sites for your HBA, NIC, and iSCSI initiator. Be sure the HBA, NIC, and iSCSI initiator are supported by your array (refer to the Hitachi interoperability matrix).
Linux operating system	Verify the planned OS version, architecture, relevant patches, and maintenance levels are supported by Hitachi Data Systems. Refer to the Hitachi interoperability matrix for information about supported versions.

ISCSI Initiator Considerations

The following list describes the requirements for using the array with iSCSI. For current requirements, please contact your Hitachi Data Systems representative.

- Hitachi Storage Navigator Modular 2 v1.0.0-00 or higher.
- Use the latest supported firmware for your array.
- The NIC, iSCSI HBA, and Ethernet switch connected to the array must support the Institute of Electrical and Electronics Engineers (IEEE) 802.3ab 1000Base-T, full-duplex operations.
- Category 5e (enhanced Category 5) or Category 6 network cabling.
- Set operating system parameters if needed.

Guidelines for Using iSCSI

Observe the following guidelines when using iSCSI:

- Do not change the Challenge Handshake Authentication Protocol (CHAP) authentication settings that correspond to hosts that are logging in to the array. If you disable CHAP authentication for the array while it is communicating with software initiator using CHAP authentication, the host will not be able to access the target device without rebooting.
- Stop all unused applications and services to eliminate extraneous operations and reduce server loads.

Downloading and Configuring the iSCSI Initiator

The array can communicate with hosts through iSCSI connections. This section gives guidelines on downloading and configuring the iSCSI Initiator for Linux.

Downloading the Initiator

Some versions of the Linux OS may provide the iSCSI initiator for download. If your Linux OS does not provide the initiator, download it from one of the following Web sites:

- For SLES 9: http://linux-iscsi.sourceforge.net/
- For SLES 10: http://www.open-iscsi.org/

Download all the necessary files to install iSCSI initiator from the Web site. Install the iSCSI software initiator according to the documentation provided with it.

Configuring the iSCSI Initiator

This section discusses how to configure the `iscsi.conf` file, a file that controls and configures the iSCSI initiator.

iSCSI.conf Configuration for SLES 9

1. Start the iSCSI driver software service.
2. Change the host login to the specified target in `iscsi.conf`. You do not need to reboot the host.
3. Stop the iSCSI service:

   ```
   service open-iscsi stop
   ```

4. Modify the file and set up the configuration.
5. Type the following command for the iSCSI initiator to automatically login to the specified targets:

   ```
   service open-iscsi start
   ```

iSCSI.conf Configuration for SLES 10

1. Start the iSCSI service:

   ```
   service open-iscsi start
   ```

2. Find the target LUN:

   ```
   iscsiadm -m discovery
   ```

3. Display the target list:

   ```
   iscsiadm -m node
   ```

4. Log in to the target:

   ```
   iscsiadm -m node -L
   ```

5. Stop the iSCSI service:

   ```
   service open-iscsi stop
   ```

6. Customize the system by modifying the `iSCSI.conf` file.
7. Allow the initiator to automatically log in to the specified targets:

   ```
   service open-iscsi start
   ```

Target Log In Failure

Sometimes, SLES may fail to log in to the specified targets. If this occurs, Hitachi recommends you modify the `/etc/init.d.open-iscsi` file to reflect the following changes:

```
iscsi_login_all_nodes ()
{
sleep 50 #Add
```

Connecting to the Array

This section provides guidelines on how to connect the array to the host.

Before you connect to the system:

1. Verify the items in Table 1-1 on page 1-3 were completed.
2. Connect the array to the server.
3. Install the Ethernet cables between the array and the Linux server. Refer to the user's guide for your array for details on hardware installation tasks.
4. Execute the `ping` command to confirm whether the cabling and IP addresses are correct.
5. Log in to the array from Linux.

iscsi.conf Notes

- The array does not support mutual CHAP authentication on Linux hosts.
- The minimum setting to `iscsi.conf` allows Linux iSCSI software initiator to start at the minimum level support. See the example below.

```
TargetName=iqn.1994-
04.jp.co.hitachi:rsd.d8h.t.00005.0a000

DiscoveryAddress=192.168.0.200

PingTimeout=60
```

Setting the iSCSI Data and Header Digests

Use the iSCSI Header and Data digest with an L3 switch (including a router) in the hosts and array iSCSI port.

Table 6-2: Data Digest and Header Digest Parameter Settings

Parameter	Definition	Negotiation Value on iSCSI Login
Always	Always enable digest	CRC32C
Never	Always disable digest	none
Prefer-on	Prioritize enabling over disabling	CRC32C, none
Prefer-off	Prioritize disabling over enabling	None, CRC32C

In the Data and Header digest, select **Enabling / Disabling CRC / Checksum**. Enabling Header digest may decrease performance by nearly 90%, depending on network configuration, host performance, and host applications. iSCSI Data digest and Header digest should be used with an L3 switch or router that is in the path of the hosts and the iSCSI port. Set the parameters to:

- HeaderDigest=always
- DataDigest=always

CHAP Authentication

The array does not support CHAP authentication in the mutual CHAP authentication against Linux software initiator. Please set it if necessary.

Setting CHAP

CHAP provides authentication of iSCSI users. If you use CHAP security, Username and secret are set to both the host and array iSCSI port. Table 6-3 on page 6-6 shows the CHAP parameters and their definitions and values.

Table 6-3: Setting Value of CHAP Authentication

Parameter	Meaning	Negotiation Value on iSCSI Login
OutgoingUsername	Username for authentication of initiator	Username of CHAP User
OutgoingPasword	Password for authentication of initiator	Secret of CHAP User
IncomingUsername	Username for authentication of target	Username of Target
IncomingPassword	Password for authentication of target	Secret of Target

Setting Keep Alive Timer Parameter

The parameters `IdleTimeout`, `ActiveTimeout` and `PingTimeout` control the Keep Alive Timer. To change the time setting in the `PingTimeout` parameter, do the following:

1. Find the line `#PingTimeout=<number>` in the `iscsi.conf` file.
2. Delete the comment out symbol (#).
3. Change `<number>` to 60.

See the example below:

Change: #PingTimeout=<number>

To:

PingTimeout=60

Configuring an iSCSI HBA

Follow the procedures below to configure an iSCSI HBA. Before you begin, verify the HBA is supported by HDS by check the interoperability information at http://www.hds.com/products/interoperability/.

1. Install the QLogic iSCSI HBA driver according to the documentation for the HBA.
2. Install the SANsurfer iSCSI HBA Manager corresponding to the HBA and the Linux OS according to the vendor's documentation.There are two methods to configure the target setting: remote host and local host.
   a. To set the target by remote host (for larger scale networks), install the SANsurfer iSCSI HBA Manager GUI on the remote host, and install the agent on the local host. The target information is set by the remote host.
   b. To set the target information by the local host (for smaller scale networks), install the SANsurfer iSCSI HBA Manager GUI and Agent on the local host. The target information is set by each local host.

Setting Target Connections

Set the following items for SANsurfer, and describe the necessary items for target connection. Refer to the SANsurfer manual for details.

1. Set the following items in Port Option:
   a. IP Address Subnet Mask — Select the **HBA option** tab and set the IP address and the subnet mask of the HBA port in **Port option – network**.
   b. Target Setting — Select the **HBA option** tab.Set the IP address and the subnet mask of the Target in the IP address dialog box of **Target settings**. Set the iSCSI Name of the Target in **iSCSI Name**.

      When the Send Target function is used, select **Auto-bind Discovered Targets** other than the settings for IP address and Subnet Mask.
2. Check the Target connection status. The **Target Setting** status should be **Session Active**, and the LUN is recognized in the Target Information.

Setting the Header/Data Digest Parameter

1. Select the **HBA Option** tab.
2. Click **Config Authentication** of **Target Setting**.
3. The Security Check dialog box is displayed. Enter the password, and click **OK**.
4. Set enable/disable of the Header Digest/Data Digest.

Setting Authentication Targets

1. Select the **HBA** option tab.
2. Click **Config Authentication** of **Target Setting**.
3. When the Security Check dialog box appears, enter the password and click **OK**.
4. Set the initiator name and the initiator secret in **CHAP Entries**.
5. Set the CHAP name and the Secret in **Targets**.

Setting Queue Depth

You may need to change the queue depth value on the server. If the number is small, I/O performance can deteriorate.The array reports a queue full status when the queue depth exceeds an allowable limit. The system may not operate correctly when the queue is full and a large value is set. Set an appropriate number according to your configuration. If necessary, set a queue depth number for each server. Refer to the documentation for your HBA before setting a value.

Guidelines for settings:

- 32 commands per LUN
- 512 commands per port
- 30 or more for device timeout value on the Hitachi array LU.

NOTE: For SUSE Linux, neither the iSCSI software initiator nor the HBA has a Queue Depth parameter. Please adjust job execution on the server.

iSCSI LUN Discovery

The array supports up to 512 logical units per iSCSI port (256 per host group), but the Linux system only supports a maximum of 64 LUNs in one system. If other devices already exist on different host adapters, the number of available LUNs will be reduced.

To activate the above modification, make an image file for booting.

Changing the Bootloader Settings

There are two options you can use as Bootloader:

- Linux Loader (LILO)
- Grand Unified Boot Loader (GRUB)

For more information about modifying LILO and GRUB settings, see the Linux Web site.

High Availability (HA) Cluster Configurations

The Hitachi AMS 2000 Family storage system is compatible with various cluster software applications. For more information about:

- Compatible cluster software applications, refer to the Hitachi Data Systems interoperability matrix at http://www.hds.com/products/interoperability/.
- Installing and configuring the cluster software, refer to the documentation provided by the cluster software vendor.

HA Multipath Configurations

The Hitachi AMS 2000 Family storage system supports various HA multipathing software products for the SuSE Linux operating system. Refer to the Hitachi Data Systems interoperability matrix at http://www.hds.com/products/interoperability/ for currently supported HA software applications. Then consult the documentation provided by the HA multipathing vendor for information about installing, configuring, operating, and best practices when using the software with Active/Active storage systems like the Hitachi AMS 2000 Family storage systems.

If the Hitachi Data Systems interoperability matrix show that SuSE Linux's bundled multipathing software, referred to as “Device Mapper,” is supported for the intended SuSE operating system version /update level and you want to use this bundled Multipath solution, refer to the appropriate SuSE Device Mapper documentation for proper installation, configuration, and operation. Some Device Mapper release level documentation can be obtained at the following link:

http://www.novell.com/

To ensure Active/Active I/O activity by the host Linux I/O to the Hitachi AMS 2000 Family storage system, confirm that the following minimum parameters are set in the file `/etc/multipath.conf`:

- Vendor: Hitachi
- Product: DF600F
- Path_grouping _policy: Multibus

Install and configure the multipathing software on the server before connecting the server to the Hitachi AMS 2000 Family storage system.

7

Asianux

This chapter discusses guidelines on how to prepare an Asianux host server for connection to the array and verify that the host server can connect to the target.

This chapter covers the following key topics:

- Preparing the Host Server
- ISCSI Initiator Considerations
- Guidelines for Using iSCSI
- Setting Queue Depth and Timeout Value
- iSCSI LUN Discovery
- Changing the Bootloader Settings
- High Availability (HA) Cluster Configurations
- HA Multipath Configurations

Preparing the Host Server

Table 7-1 lists guidelines and tasks you need to follow to prepare the host server.

One or more supported network-interface cards (NIC) with the latest supported Internet Small Computer System Interface (iSCSI) initiator or host bus adapters (HBA) with the latest supported BIOS and driver are required. Verify the NICs, HBAs, drivers, and BIOSes are the latest supported versions by Hitachi Data Systems, and are functioning properly. To check the latest supported versions, refer to the Hitachi interoperability matrix at http://www.hds.com/products/interoperability/.

For information about iSCSI initiators supported by your operating system, refer to the AsianuxWeb site at http://www.asianux.com/asianux.do

Table 7-1: Host Server Preparation Guidelines

Item	Task
NICs	Use NICs supported by your array (refer to the Hitachi interoperability matrix) and operating system.
iSCSI HBAs (Optional)	Use the most current iSCSI HBA and drivers/BIOSes supported by your array (refer to the Hitachi interoperability matrix) and operating system. Install all utilities and tools that come with the HBA.
Install the HBA or iSCSI software initiator in the host server.	For installation information, check the Web sites for your HBA, NIC, and iSCSI initiator. Be sure the HBA, NIC, and iSCSI initiator are supported by your array (refer to the Hitachi interoperability matrix).
Asianux operating system	Verify the planned OS version, architecture, relevant patches, and maintenance levels are supported by Hitachi Data Systems. Refer to the Hitachi interoperability matrix for information about supported versions.

ISCSI Initiator Considerations

The following list describes the requirements for using the array with iSCSI. For current requirements, please contact your Hitachi Data Systems representative.

- Hitachi Storage Navigator Modular 2 v1.0.0-00 or higher.
- For the array's microcode version, use the latest product release.
- The NIC, iSCSI HBA, and Ethernet switch that are directly connected to the array must support the Institute of Electrical and Electronics Engineers (IEEE) 802.3ab 1000Base-T, full-duplex operations.
- Category 5e (enhanced Category 5) or Category 6 network cabling.
- If using the array as an iSNS client, Microsoft iSNS Server 3.0 or higher must be installed on the same IP-SAN.
- Set OS Parameters if needed.

Guidelines for Using iSCSI

Observe the following guidelines when using iSCSI:

- Do not change the Challenge Handshake Authentication Protocol (CHAP) authentication settings that correspond to hosts that are logging in to the array. If you disable CHAP authentication for the array while it is communicating with software initiator using CHAP authentication, the host will not be able to access the target device without rebooting.
- Stop all unused applications and services to eliminate extraneous operations and reduce server loads.

Downloading and Configuring the iSCSI Initiator

The array can communicate with hosts through iSCSI connections. This section gives guidelines on downloading and configuring the iSCSI Initiator for Linux.

Downloading the iSCSI Initiator

Some versions of the Linux OS may provide the iSCSI initiator for download. If your Linux OS does not provide the initiator, download it from one of the following Web sites:

http://www.asianux.com/asianux.do

Download all the necessary files to install iSCSI initiator from the Web site. Install the iSCSI initiator according to the provided documentation.

Configuring the iSCSI Initiator

This section discusses how to configure the `iscsi.conf file`, which controls and configures the iSCSI initiator.

iSCSI.conf Configuration for Asianux 2.0

1. Start the iSCSI driver software service.
2. Change the host login to the specified target in the `iscsi.conf` file. You do not need to reboot the host.
3. Stop the iSCSI service:

   ```
   service open-iscsi stop
   ```

4. Modify the file and set up the configuration.
5. Type the following command for the iSCSI initiator to automatically login to the specified targets:

   ```
   service open-iscsi start
   ```

iSCSI.conf Configuration for Asianux 3.0

1. Start the iSCSI service:

   ```
   service open-iscsi start
   ```

2. Find the target LUN:

   ```
   iscsiadm -m discovery
   ```

3. Display the target list:

   ```
   iscsiadm -m node
   ```

4. Log in to the target:

   ```
   iscsiadm -m node -L
   ```

5. Stop the iSCSI service:

   ```
   service open-iscsi stop
   ```

6. Customize the system by modifying the `iSCSI.conf` file.
7. Allow the initiator to automatically log in to the specified targets:

   ```
   service open-iscsi start
   ```

Target Log In Failure

Sometimes, Asianux may fail to log in to the specified targets. If this occurs, Hitachi recommends you modify the `/etc/init.d.open-iscsi` file to reflect the following changes:

```
iscsi_login_all_nodes ()
{
sleep 50 #Add
```

Connecting to the Array

This section provides guidelines on how to connect the array to the host.

Before you connect to the system:

1. Verify the items in Table 1-1 on page 1-3 were completed.
2. Connect the array to the Asianuxserver.
3. Install the Ethernet cables between the array and the Linux server. Refer to the user's guide for your array for details on hardware installation tasks.
4. Execute the `ping` command to confirm whether the cabling and IP addresses are correct.
5. Log in to the array from Linux.

iscsi.conf Notes

- The array does not support mutual CHAP authentication on Linux hosts.
- The minimum setting of `iscsi.conf` allows Linux iSCSI software initiator to start at the minimum level support. See the example below.

```
TargetName=iqn.1994-
04.jp.co.hitachi:rsd.d7h.t.00005.0a000

TargetName=iqn.1994-
04.jp.co.hitachi:rsd.d7h.t.00005.0a000

DiscoveryAddress=192.168.0.200

PingTimeout=60
```

Setting the iSCSI Data and Header Digests

Use the iSCSI Header and Data digest with an L3 switch (including a router) in the hosts and array iSCSI port.

Table 7-2: Data Digest and Header Digest Parameter Settings

Parameter	Definition	Negotiation Value on iSCSI Login
Always	Always enable digest	CRC32C
Never	Always disable digest	none
Prefer-on	Prioritize enabling over disabling	CRC32C, none
Prefer-off	Prioritize disabling over enabling	None, CRC32C

In the Data and Header digest, select **Enabling/Disabling CRC/Checksum**. Enabling Header digest may decrease performance by nearly 90%, depending on network configuration, host performance, and host applications. iSCSI Data digest and Header digest should be used with an L3 switch or router that is in the path of the hosts and the array iSCSI port. Set the parameters to:

- HeaderDigest=always
- DataDigest=always

CHAP Authentication

The array does not support CHAP authentication in the mutual CHAP authentication against Linux software initiator. Please set it if necessary.

Setting CHAP

CHAP provides authentication of iSCSI users. If you use CHAP security, Username and secret are set to both the host and array iSCSI port. Table 7-3 shows the CHAP parameters and their definitions and values.

Table 7-3: Setting Value of CHAP Authentication

Parameter	Meaning	Negotiation Value on iSCSI Login
OutgoingUsername	Username for authentication of initiator	Username of CHAP User
OutgoingPasword	Password for authentication of initiator	Secret of CHAP User
IncomingUsername	Username for authentication of target	Username of Target
IncomingPassword	Password for authentication of target	Secret of Target

Setting Keep Alive Timer Parameter

The parameters `IdleTimeout`, `ActiveTimeout` and `PingTimeout` control the Keep Alive Timer. To change the time setting in the `PingTimeout` parameter, do the following:

1. Find the line `#PingTimeout=<number>` in the `iscsi.conf` file.
2. Delete the comment out symbol (#).
3. Change `<number>` to 60.

See the example below:

```
Change: #PingTimeout=<number>

To: PingTimeout=60
```

Configuring an iSCSI HBA

Follow the procedures below to configure an iSCSI HBA. Before you begin, verify the HBA is supported by HDS by check the interoperability information at http://www.hds.com/products/interoperability/.

1. Install the QLogic iSCSI HBA driver according to the documentation for the HBA.
2. Install the SANsurfer iSCSI HBA Manager corresponding to the HBA and the Linux OS according to the vendor's documentation.There are two methods to configure the target setting: remote host and local host.
   a. To set the target by remote host (for larger scale networks), install the SANsurfer iSCSI HBA Manager GUI on the remote host, and install the agent on the local host. The target information is set by the remote host.
   b. To set the target information by the local host (for smaller scale networks), install the SANsurfer iSCSI HBA Manager GUI and Agent on the local host. The target information is set by each local host.

Setting Target Connections

Set the following items for SANsurfer, and describe the necessary items for target connection. Refer to the SANsurfer manual for details.

1. Set the following items in Port Option:
   a. IP Address Subnet Mask — Select the **HBA option** tab and set the IP address and the subnet mask of the HBA port in **Port option – network**.
   b. Target Setting — Select the **HBA option** tab.Set the IP address and the subnet mask of the Target in the IP address dialog box of **Target settings**. Set the iSCSI Name of the Target in **iSCSI Name**.

      When the Send Target function is used, select **Auto-bind Discovered Targets** other than the settings for IP address and Subnet Mask.
2. Check the Target connection status. The **Target Setting** status should be **Session Active**, and the LUN is recognized in the Target Information.

Setting the Header/Data Digest Parameter

1. Select the **HBA Option** tab.
2. Click **Config Authentication** of **Target Setting**.
3. The Security Check dialog box is displayed. Enter the password, and click **OK**.
4. Set enable/disable of the Header Digest/Data Digest.

Setting Authentication Targets

1. Select the **HBA** option tab.
2. Click **Config Authentication** of **Target Setting**.

3. When the Security Check dialog box appears, enter the password and click **OK**.
4. Set the initiator name and the initiator secret in **CHAP Entries**.
5. Set the CHAP name and the Secret in **Targets**.

Setting Queue Depth and Timeout Value

You may need to change the queue depth value on the server. If the number is small, I/O performance can deteriorate.The array reports a queue full status when the queue depth exceeds an allowable limit. The system may not operate correctly when the queue is full and a large value is set. Set an appropriate number according to your configuration. If necessary, set a queue depth number for each server. Refer to the documentation for your HBA before setting a value.

Guidelines for settings:

- 32 commands per LUN
- 512 commands per port
- 30 or more for device timeout value on the Hitachi array LU.

NOTE: For Asianux, neither the iSCSI software initiator nor the HBA has a Queue Depth parameter. Please adjust job execution on the server.

iSCSI LUN Discovery

The array supports up to 512 logical units per iSCSI port (256 per host group), but the Linux system only supports a maximum of 64 LUNs in one system. If other devices already exist on different host adapters, the number of available LUNs will be reduced.

To set the number of LUNs:

1. Edit the `/etc/modules.conf` file to add a line similar to the following:

   ```
   options scsi_mod max_scsi_luns=16
   ```

2. To set the Emulex driver, add the following line to the `/etc/modules.conf` file:

   ```
   Alias scsi_hostadapter lpfcdd
   ```

3. To activate the above modification, make an image file for booting. For example:

   ```
   # mkinitrd /boot/initrd-2.4.x.scsiluns.img `uname -r`
   ```

Changing the Bootloader Settings

There are two options you can use as Bootloader:

- Linux Loader (LILO)
- Grand Unified Boot Loader (GRUB)

See the Linux Web site for more information on modifying LILO and GRUB settings.

High Availability (HA) Cluster Configurations

The Hitachi AMS 2000 Family storage system is compatible with various cluster software applications. For more information about:

- Compatible cluster software applications, refer to the Hitachi Data Systems interoperability matrix at http://www.hds.com/products/interoperability/.
- Installing and configuring the cluster software, refer to the documentation provided by the cluster software vendor.

HA Multipath Configurations

The Hitachi AMS 2000 Family storage system supports various HA multipathing software products for the Asianux Linux operating system. Refer to the Hitachi Data Systems interoperability matrix at http://www.hds.com/products/interoperability/ for currently supported HA software applications. Then consult the documentation provided by the HA

multipathing vendor for information about installing, configuring, operating, and best practices when using the software with Active/Active storage systems like the Hitachi AMS 2000 Family storage systems.

If the Hitachi Data Systems interoperability matrix show that Asianux's bundled multipathing software, referred to as "Device Mapper," is supported for the intended Asianux operating system version /update level and you want to use this bundled Multipath solution, refer to the appropriate Asianux Device Mapper documentation for proper installation, configuration, and operation. Some Device Mapper release level documentation can be obtained at the following link:

http://www.asianux.com/asianux.do

To ensure Active/Active I/O activity by the host Linux I/O to the Hitachi AMS 2000 Family storage system, confirm that the following minimum parameters are set in the file `/etc/multipath.conf`:

- Vendor: Hitachi
- Product: DF600F
- Path_grouping _policy: Multibus

Install and configure the multipathing software on the server before connecting the server to the Hitachi AMS 2000 Family storage system.

8

IBM AIX

This chapter discusses guidelines on how to prepare an IBM AIX host server for connection to the array and verify that the host server can connect to the target.

This chapter covers the following key topics:

- Preparing the Host Server
- Connecting to the Host Server
- Setting the iSCSI Configuration
- Setting iSCSI Targets
- Setting Disk and Device Parameters
- Using SMIT to Change Device Parameters
- Changing Device Parameters from the AIX Command Line
- Verifying New Device Recognition

Preparing the Host Server

Table 8-1 lists guidelines and tasks you need to follow to prepare the host server.

One or more supported network-interface cards (NIC) with the latest supported Internet Small Computer System Interface (iSCSI) initiator or host bus adapters (HBA) with the latest supported BIOS and driver are required. Verify the NICs, HBAs, drivers, and BIOSes are the latest supported versions by Hitachi Data Systems, and are functioning properly. To check the latest supported versions, refer to the Hitachi interoperability matrix at http://www.hds.com/products/interoperability/.

For information about iSCSI initiators supported by your operating system, refer to the IBM Web site: http://www.ibm.com/us/.

Table 8-1: Host Server Preparation Guidelines

Item	Task
NICs	Use NICs supported by your array (refer to the Hitachi interoperability matrix) and operating system.
iSCSI HBAs (Optional)	Use the most current iSCSI HBA and drivers/BIOSes supported by your array (refer to the Hitachi interoperability matrix) and operating system. Install all utilities and tools that come with the HBA.
Install the HBA or iSCSI software initiator in the host server.	For installation information, check the Web sites for your HBA, NIC, and iSCSI initiator. Be sure the HBA, NIC, and iSCSI initiator are supported by your array (refer to the Hitachi interoperability matrix).
IBM AIX operating system	Verify the planned OS version, architecture, relevant patches, and maintenance levels are supported by Hitachi Data Systems. Refer to the Hitachi Data Systems interoperability matrix for information about supported versions.

Connecting to the Host Server

After preparing the host server, follow the steps in Table 8-2 to connect the array to the server.

Table 8-2: Connecting the Array to the Host Server

Step	Task	Description
1.	Verify the system installation.	Confirm that the status of the NICs or iSCSI HBAs and LDEVs is NORMAL.
2.	Shut down the IBM AIX system.	• Power off the AIX system before connecting the array. • Shut down the IBM system. • When shutdown is complete, power off the IBM AIX display. • Power off all peripheral devices, except the array. • Power off the host system. • You are now ready to connect the array.
3.	Connect the array.	• Install LAN cables between the array and the IBM system via an Ethernet switch. • Follow all precautions and procedures in the user's guide for your array. • Check all specifications to ensure proper installation and configuration.
4.	Power on the IBM system.	Power on the IBM system after connecting the array: • Power on the IBM AIX system display. • Power on all peripheral devices. The array should be on, the iSCSI ports should be configured, and the driver configuration file and system configuration file should be edited. If the iSCSI ports are configured or configuration files edited after the IBM system is powered on, restart the system to have the new devices recognized. • Confirm the ready status of all peripheral devices, including the array. • Power on the IBM system.

Setting the iSCSI Configuration

The following procedure describes how to set the iSCSI configuration using the IBM AIX System Management Interface Tool (SMIT).

1. At the AIX command line prompt, type the following command on the command line to start SMIT to open the System Management panel:

   ```
   smit
   ```

2. When the SMIT System Management panel appears, select **Devices** to display the Devices panel (Figure 8-1).

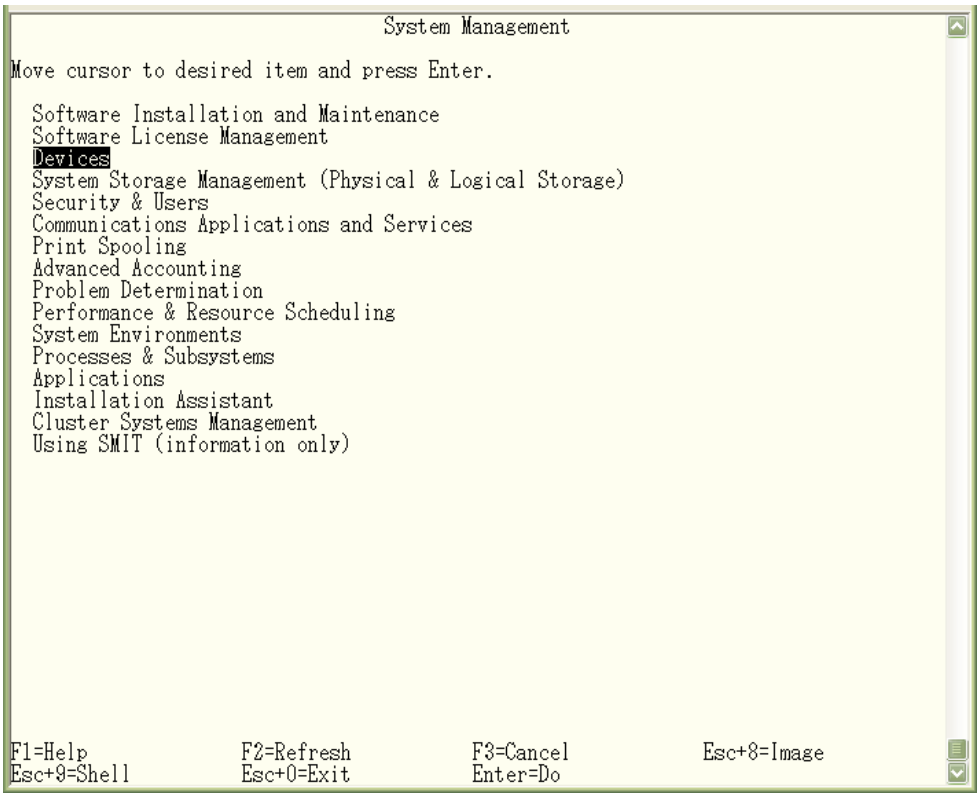

Figure 8-1: System Management Pool

3. From the Devices panel, select **iSCSI** and press the Enter key (Figure 8-2 on page 8-5).

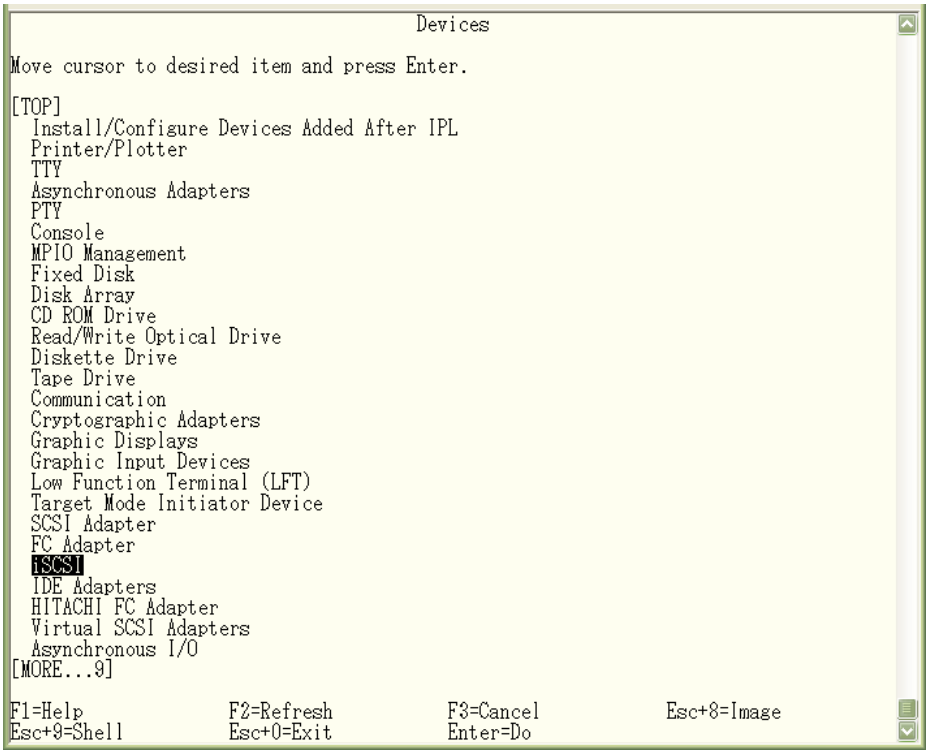

Figure 8-2: Device Window

4. Select **iSCSI Protocol Device** and press the Enter key (Figure 8-3).

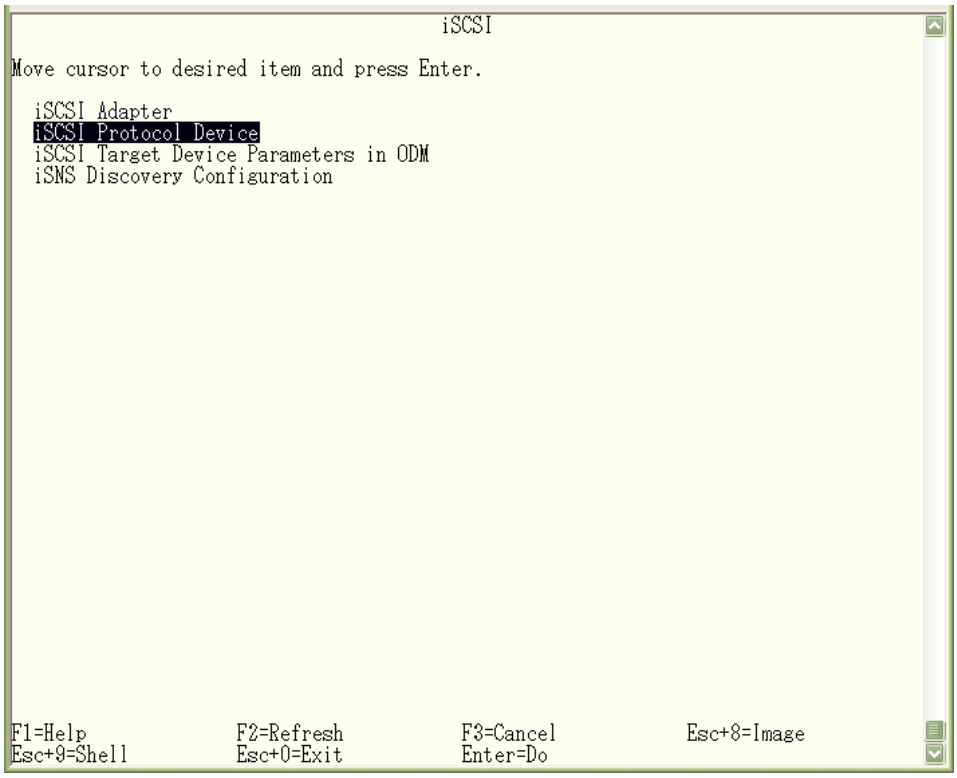

Figure 8-3: iSCSI Window

5. Select **Change / Show Characteristics of iSCSI Protocol Device** and press the Enter key (Figure 8-4).

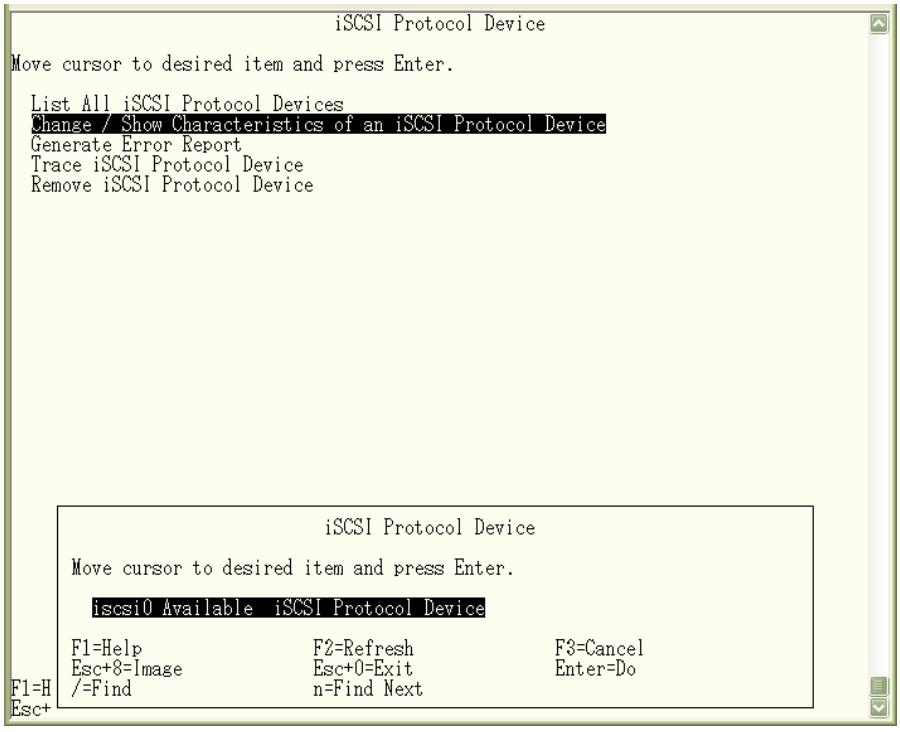

Figure 8-4: iSCSI Protocol Device Window

6. Enter the **iSCSI Initiator Name** and the value of **Maximum Targets Allowed** (Figure 8-5).

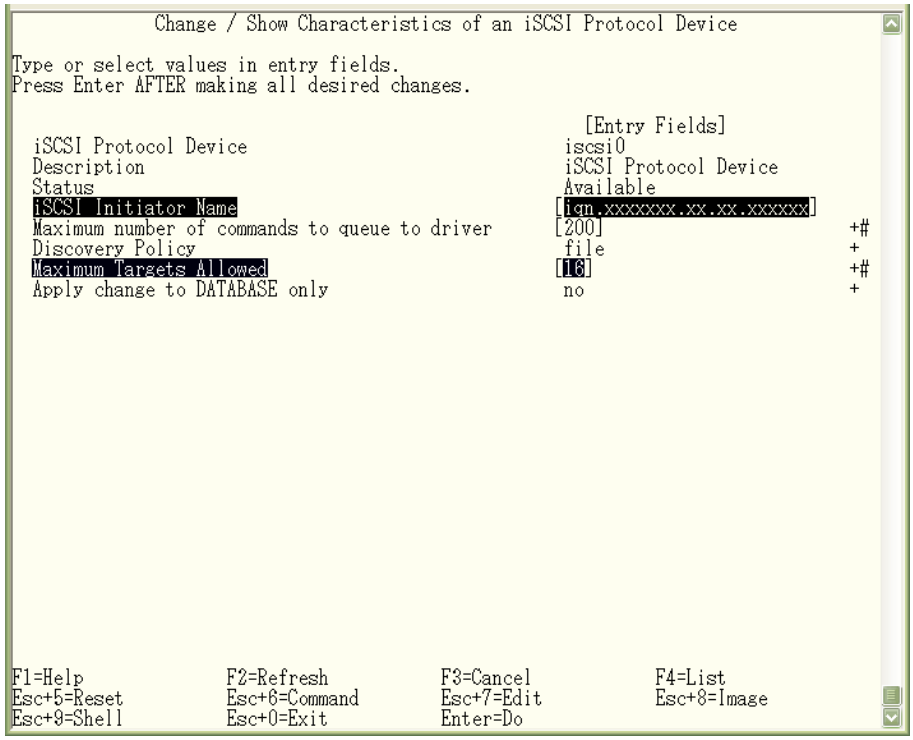

Figure 8-5: Change / Show Characteristics of an iSCSI Protocol Device

Setting iSCSI Targets

After installing the iSCSI initiator software, add the following to the `/etc/iscsi/targets` file.

If CHAP authentication is not used:

192.168.0.200	3260	iqn.1994-04.jp.co.hitachi:rsd.d8s.t.10007.0a000
Target IP address	Port number to be used (default =3260)	Name of iSCSI initiator

If CHAP authentication is used:

192.168.0.200	3260	iqn.1994-04.jp.co.hitachi:rsd.d8s.t.10007.0a000	“test00000000”
Target IP address	Port number to be used (default =3260)	Name of iSCSI initiator	CHAP authentication password (2-way authentication is not installed)

After editing the file and connecting to the target, issue the following command:

```
# cfgmgr -l iscsi0
```

If the host cannot connect to the target, check the contents of the `/etc/iscsi/targets` file. If the problem remains after checking the file:

1. Confirm that the LAN cable is connected securely.
2. Send a ping from the host to the target and confirm the response of the ping.
3. Send a ping from the target to the host and confirm the response of the ping.
4. Confirm that the target is configured properly.

Setting Disk and Device Parameters

After the array is installed and connected, and device files are created, the IBM system sets device parameters to system default values. Using SMIT or the AIX command line, you can change the read/write time-out, queue type, and queue depth parameters for each new array. Both methods are described in the following sections

NOTE: If you set parameters for iSCSI disk devices, use the same settings and device parameters for all Hitachi arrays.

Table 8-3 lists the read/write time-out and queue type requirements for the array. Table 8-4 lists the queue depth requirements for the array.

Table 8-3: Read/Write Time-Out and Queue Type Requirements

Parameter	Default Value	Required Value for Array
Read/write time-out	30	30
Queue type	none	simple

Table 8-4: Array Queue Depth Requirements

Parameter	Requirement
Option 1	32 commands per LUN
Option 2	512 commands per port

NOTE: To optimize the I/O performance, you can adjust the queue depth for the array within the specified range as needed.

Using SMIT to Change Device Parameters

To change the device paramseters using SMIT:

1. At the AIX command line prompt, type the following command on the command line to start SMIT and display the System Management panel:

   `smit`

2. On the SMIT System Management panel, select **Devices**. The Devices panel appears.
3. Select **Fixed Disk**. The Fixed Disk panel appears.
4. Select **Change/Show Characteristics of a Disk**. The Disk panel appears (see Figure 8-6 on page 8-9).
5. On the **Disk** menu, select the desired device. The Change/Show Characteristics of a Disk panel.
6. Enter the desired queue depth (see Table 8-4) and queue type (simple). Press Enter to complete the parameter changes.
7. Repeat steps 5 and 6 for each new device on the array.

8. To verify that the parameters for all devices were changed, type the following command:

   ```
   lsattr -E -1 hdiskx
   ```

```
                  Change/Show Characteristics of a Disk
Type or select values in entry fields.
Press Enter AFTER making all desired changes.
[MORE...11]                                                [Entry Fields]
  FC Node Name
  Physical volume IDENTIFIER                none
  ASSIGN physical volume identifier         no
  Queue DEPTH                               [1]       <- See Table 8-4.
  Queuing TYPE                              [simple] <- Enter simple here.
  Use QERR bit                              [yes]
  Device CLEARS its Queue on error          [no]
  READ/WRITE time out value                 [30]
  Maximum LUN inquiried on device           []
  START UNIT time out value                 [60]
  REASSIGN time out value                   [120]
  Maximum TRANSFER Size                     [0x40000]
  Apply change to DATABASE only             no
[BOTTOM]

F1=Help             F2=Refresh          F3=Cancel           F4=List
Esc+5=Reset         Esc+6=Command       Esc+7=Edit          Esc+8=Image
Esc+9=Shell         Esc+0=Exit          Enter=Do
```

Figure 8-6: Using SMIT to Change Device Parameters

Changing Device Parameters from the AIX Command Line

To change the device parameters from the AIX command line:

1. Type the following command at the AIX command line prompt to display the parameters for the specified device:

   ```
   lsattr -E -l hdiskx
   ```

NOTE: 'hdiskx is the device file name (for example, hdisk2.) You can also use the `lscfg -vl hdiskx` command (see Figure 8-9 on page 8-10).

2. Type the following command to change the device parameters:

   ```
   chdev -l hdiskx -a rw_timeout='30' -a q_type='simple' -a
   queue_depth='x'
   ```

```
# chdev -l hdisk4 -a rw_timeout=30
hdisk4 changed
EP8000-521# lsattr -El hdisk4
PR_key_value   none                      Reserve Key                        True
clr_q          no                        Device CLEARS its Queue on error   True
location                                 Location Label                     True
lun_id         0x1000000000000           Logical Unit Number ID             False
max_transfer   0x40000                   Maximum TRANSFER Size              True
node_name                                FC Node Name                       False
pvid           00c1e29aec8fa056000000000000000000 Physical Volume ID       False
q_err          yes                       Use QERR bit                       False
q_type         simple                    Queue TYPE                         True
queue_depth    16                        Queue DEPTH                        True
reassign_to    120                       REASSIGN time out                  True
reserve_policy single_path               Reserve Policy                     True
rw_timeout     30                        READ/WRITE time out                True
scsi_id        0xef                      SCSI ID                            False
start_timeout  60                        START UNIT time out                True
www_name        0x50060e8010400780       FC World Wide Name                 False
```

Figure 8-7: Changing Device Parameters Using SMIT (Timeout)

```
# chdev -l hdisk4 -a queue_depth=16
hdisk4 changed
```

Figure 8-8: Changing Device Parameters Using SMIT (Queue_depth)

NOTE: *x* is used to indicate the desired queue depth within the limits specified in Table 8-3 on page 8-8.

3. Repeat steps 1 and 2 for each new array device.
4. Type the following command to verify that the parameters for all devices were changed (see Figure 8-9):

   `lsattr -E -1 hdiskx`

```
#lsattr -E -l hdisk4
clr_q         no                                  Device CLEARS its Queue on error True
location                                          Location Label                   True
lun_id        0x1000000000000                     Logical Unit Number ID           False
max_transfer  0x40000                             Maximum TRANSFER Size            True
node_name                                         FC Node Name                     False
pvid          00c1e29aec8fa056000000000000000000  Physical volume identifier       False
q_err         yes                                 Use QERR bit                     True
q_type        simple                              Queuing TYPE                     True
queue_depth   1                                   Queue DEPTH                      True
reassign_to   120                                 REASSIGN time out value          True
rw_timeout    30                                  READ/WRITE time out value        True
scsi_id       0xef                                SCSI ID                          False
start_timeout 60                                  START unit time out value        True
ww_name       0x50060e8010400780                  FC World Wide Name               False
```

Figure 8-9: Verifying the Device Parameters Using the lsattr -E -1 hdiskx Command

```
lscfg -vl hdisk4
  hdisk4  U787A.001.DPM0GZG-P1-C1-T1-W50060E8010400780-L1000000000000  Other FC SCSI Disk Drive
        Manufacturer................HITACHI
        Machine Type and Model......DF600F
        Part Number.................p
        ROS Level and ID............30303030
        Serial Number...............83000120
        EC Level....................
        FRU Number..................0120
        Device Specific.(Z0)........00000432B3001102
        Device Specific.(Z1)........0001
```

Figure 8-10: Verifying the Device Parameters Using the lscfg -vl hdisk1 Command

Verifying New Device Recognition

This section provides guidelines on how to connect the array to the host.

Before you connect to the system:

1. Verify the items in Table 8-1 on page 8-2 were completed.
2. Hitachi Data Systems recommends that the devices should be installed and formatted with the fibre ports configured before the host system is powered on. Enter the `cfgmgr` command to force the system to check the buses for new devices.

To verify new device recognition:

1. Log in to the host system as root.
2. Display the system device data by entering the following command (see Figure 8-11):

   `lsdev -C -c disk`

```
# lsdev -C -c disk                                        <- Display device data.
hdisk0  Available 08-08-00-4,0 16 Bit LVD SCSI Disk Drive
hdisk1  Available 08-08-00-5,0 16 Bit LVD SCSI Disk Drive
hdisk2  Available 08-08-00-8,0 16 Bit LVD SCSI Disk Drive
hdisk3  Available 04-08       Other iSCSI Disk Drive   <- New device (or NA shown)
hdisk4  Available 04-08       Other iSCSI Disk Drive   <- New device (or NA shown)
hdisk5  Available 04-08       Other iSCSI Disk Drive   <- New device (or NA shown)
hdisk6  Available 04-08       Other iSCSI Disk Drive   <- New device (or NA shown)

          Device file name = hdiskx.
 :
#
```

Figure 8-11: Verifying New Device Recognition

9

HP-UX

This chapter discusses guidelines on how to prepare an HP-UX host server for connection to the array and verify that the host server can connect to the target.

This chapter covers the following key topics:

- Preparing the Host Server
- ISCSI Initiator Considerations
- Setting Queue Depth
- Recommended Timeout Value
- Connecting to the Target

Preparing the Host Server

Table 9-1 lists guidelines and tasks you need to follow to prepare the host server.

One or more supported network-interface cards (NIC) with the latest supported Internet Small Computer System Interface (iSCSI) initiator or host bus adapters (HBA) with the latest supported BIOS and driver are required. Verify the NICs, HBAs, drivers, and BIOSes are the latest supported versions by Hitachi Data Systems, and are functioning properly. To check the latest supported versions, refer to the Hitachi interoperability matrix at http://www.hds.com/products/interoperability/.

For information about iSCSI initiators supported by your operating system, refer to the HP Web site: http://www.hp.com/.

Table 9-1: Host Server Preparation Guidelines

Item	Task
iSCSI NICs	Use NICs supported by your array (refer to the Hitachi interoperability matrix) and operating system.
iSCSI HBAs (Optional)	Use the most current iSCSI HBA and drivers/BIOSes supported by your array (refer to the Hitachi interoperability matrix) and operating system. Install all utilities and tools that come with the HBA.
Install the HBA/NIC and iSCSI software initiator in the host server.	For installation information, check the Web sites for your HBA, NIC, and iSCSI initiator. Be sure the HBA, NIC, and iSCSI initiator are supported by your array (refer to the Hitachi interoperability matrix).
HP-UX operating system	Verify the planned OS version, architecture, relevant patches, and maintenance levels are supported by Hitachi Data Systems. Consult the Hitachi Data Systems interoperability matrix for supported versions.

Connecting to the Array

This section provides guidelines on how to connect the array to the host. Before you connect to the array:

1. Verify the items in Table 1-1 on page 1-3 were completed.
2. Verify the iSCSI port address configuration and the status of the SMS iSCSI adapters and LUNs are normal.
3. Set the queue depth if necessary on the HP-UX host.
4. Install the Ethernet cables between the array and the HP-UX system. Refer to the user's guide for your array for information about hardware installation tasks.
5. From the HP-UX prompt, execute a `ping` command to confirm that the cabling and IP address settings are correct.
6. Log in to the array from HP-UX.

7. Use Storage Navigator Modular 2 to configure the array as follows (for more information, refer to the Storage Navigator Modular 2 online help):
   - Platform = **HP-UX**
   - Mode Settings:

     Common Setting = **Standard Mode**

     Additional Setting = **HP-UX Mode** and **PSUE Read Reject Mode**

NOTE: HP-UX supports PVLink (HP-UX 11.i V1.0/V2.0) multi-pathing software.

iSCSI Initiator Considerations

The following list describes the requirements for using the array with iSCSI. For current requirements, please contact your Hitachi Data Systems representative.

- Hitachi Storage Navigator Modular 2 v1.0.0-00 or higher.
- Use the latest supported firmware for your array.
- The NIC, iSCSI HBA, and Ethernet switch connected to the array must support the Institute of Electrical and Electronics Engineers (IEEE) 802.3ab 1000Base-T, full-duplex operations.
- Category 5e (enhanced Category 5) or Category 6 network cabling.
- Set operating system parameters if needed.

Guidelines for Using iSCSI

Observe the following guidelines when using iSCSI:

- Do not change the Challenge Handshake Authentication Protocol (CHAP) authentication settings that correspond to hosts that are logging in to the array. If you disable CHAP authentication for the array while it is communicating with the software initiator that uses CHAP authentication, the host will not be able to access the target device without rebooting.
- Stop all unused applications and services to reduce server loads.

Installing iSCSI Initiator

HP-UX iSCSI software initiator is the iSCSI initiator software for HP-UX. Perform the following procedure to confirm that the iSCSI initiator is installed.

1. Type the following command line:

   ```
   swlist iscsi-00
   ```

   If the iSCSI software initiator is installed, the generated output will resemble the following.

   For HP-UX11iv2 systems:

```
# swlist iSCSI-00                                          ← command
    |
    |
    |
# iSCSI-00            B.11.11.03.e   HP-UX iSCSI Software Initiator }  message
  iSCSI-00.ISCSI-SWD  B.11.11.03.e   HP-UX iSCSI Software Initiator }
```

For HP-UX11iv3 systems:

```
# swlist iSCSI-00                                          ← command
    |
    |
    |
# iSCSI-00            B.11.31.01     HP-UX iSCSI Software Initiator }  message
  iSCSI-00.ISCSI-SWD  B.11.31.01     HP-UX iSCSI Software Initiator }
```

2. Type the following command line:

   `ioscan-kfnC iscsi`

   If the iSCSI software initiator is installed, the generated output will resemble the following:

For HP-UX11iv2 systems:

```
# ioscan -kfnC iscsi                                       ← command
     |
     |
     |
Class   I   H/W Path   Driver   S/W State   H/W Type   Description          }
=================================================================          } (a)
ISCSI   0   255/0      iscsi    CLAIMED     VIRTBUS    iSCSI Virtual Node   }
```

For HP-UX11iv3 systems:

```
# ioscan -kfnC iscsi                                       ← command
     |
     |
     |
Class   I   H/W Path   Driver   S/W State   H/W Type   Description          }
=================================================================          } (a)
ISCSI   0   64000/0x0  iscsi    CLAIMED     VIRTBUS    iSCSI Virtual Node   }
```

Setting iSCSI Authentication

The Challenge Handshake Authentication Protocol (CHAP) is an encrypted password authentication protocol that cannot be reversed. It sends a challenge to the remote access client, and the client returns the username, string encryption, session identifier, and password. If the information returned is valid, the credentials are authenticated.

The length of the secret security key must be from 12-characters (96 bits) to 16-characters. The CHAP secret is case sensitive. For security, each typed letter appears as a dot.

By default, CHAP is disabled. To enable 1-way CHAP, use the following procedure.

1. Type the following command line to enable 1-way CHAP:

```
# iscsiutil -u -H CHAP_UNI -T
iqn.1994-04.jp.co.hitachi:rsd.d8a.t.10025.0a000 -I 192.168.0.200 -P 5000
          iSCSI name of Target                  IP address of Target   Port number
```

2. Set the CHAP name of the initiator. If the CHAP name is omitted, the iSCSI initiator name is used as the CHAP name.

```
# iscsiutil -u -N DF800User000 -T
            Name of initiator
iqn.1994-04.jp.co.hitachi:rsd.d8a.t.10025.0a000 -I 192.168.0.200 -P 5000
```

3. Set the initiator CHAP secret:

```
# iscsiutil -u -W test00000000 -T
               secret
iqn.1994-04.jp.co.hitachi:rsd.d8a.t.10025.0a000 -I 192.168.0.200 -P 5000
```

Specifying the Initiator to be Connected to the Target

To specify the initiator that will connect to the target, use the following procedure.

1. Save the Target device information in the kernel registry.

```
# iscsiutil -a -I 192.168.0.200                    ← When 3260 is used as the Port number.
          IP address of Target
```

or

```
# iscsiutil -a -I 192.168.0.200 -P 5000            ← When 5000 is used as the Port number.
```

Setting the Header or Data Digest

Enabling header digest may decrease performance by nearly 90%, depending on network configuration, host performance, and host applications. iSCSI Data digest and header digest should be used with an L3 switch or router that is in the path of the hosts and the array's iSCSI data port.

The following shows an example of changing the header digest to CRC32.

```
# iscsiutil -t headerdigest CRC32C -I 192.168.0.200 -T
iqn.1994-04.jp.co.hitachi:rsd.d8a.t.10025.a0
```

The following shows an example of changing the data digest to CRC32.

```
# iscsiutil -t datadigest CRC32C -I 192.168.0.200 -T
iqn.1994-04.jp.co.hitachi:rsd.d8a.t.10025.a0
```

Confirming Parameter Settings

Use the Display Target Discovery information screen to confirm that your parameter settings are correct.

```
# iscsiutil -p -D
Discovery Target Information
----------------------------

Target # 1
----------
        IP Address                  : 192.168.0.200
        iSCSI TCP Port              : 3260
        iSCSI Portal Group Tag      : 1

  User Configured:
  ----------------

        Authenticaton Method        : None
        CHAP Method                 : CHAP_UNI
        Initiator CHAP Name         : SA800User000
        CHAP Secret                 : test00000000
        Header Digest               : None,CRC32C (default)
        Data Digest                 : None,CRC32C (default)
```

Setting Queue Depth

You may need to change the command multiplex value on the host server. If the number is small, I/O performance can deteriorate. The array reports a queue full status when the queue depth exceeds an allowable limit. The system may not operate correctly when the queue is full and a large value is set. Set an appropriate number according to your configuration. If necessary, set a queue depth number for each server. You may also have to change the queue depth number when adding disk drives. Refer to the documentation for your HBA before setting a value.

Guidelines for settings:

- 32 commands per LUN
- 512 commands per port

To set the queue depth for array on the server, enter the following command lines.

For HP-UX11iv2:

```
# scsictl -a /dev/rdsk/c2t0d1                          ← Command to verify setting
immediate_report = 0; queue_depth = 8
#
# scsictl -a -m queue  _depth=32 /dev/rdsk/c2t0d1      ← Command to change setting
immediate_report = 0; queue_depth = 8
# scsictl -a /dev/rdsk/c2t0d1
immediate_report = 0; queue_depth = 32
#
```

If you use HP-UX11iv2, create a start-up script that includes the **scsictl** command for setting the queue depth automatically on subsequent server boots.

For HP-UX11iv3:

```
# scsimgr get_attr -D /dev/rdisk/disk591 -a max_q_depth      ← Command to verify setting

        SCSI ATTRIBUTES FOR LUN : /dev/rdisk/disk591

name = max_q_depth
current = 32
default = 8
saved = 32
#
# scsimgr save_attr -D /dev/rdisk/disk591 -a max_q_depth=32  ← Command to change setting
# scsimgr get_attr -D /dev/rdisk/disk591 -a max_q_depth

        SCSI ATTRIBUTES FOR LUN : /dev/rdisk/disk591

name = max_q_depth
current = 32
default = 8
saved = 32
#
```

Recommended Timeout Value

Set the device timeout value of the array LU to 30 or more.

Connecting to the Target

Enter the appropriate command to connect to the Target.

For HP-UX11iv2:

1. Type the following command line to discover the target:

```
# /usr/sbin/ioscan -H 255
                   (a)
```

NOTE: In this example, **(a)** denotes the default node number allocated by HP-UX.

2. Type the following command line to create a device file:

```
# /usr/sbin/insf -H 255
```

3. Type the following command line to display the connected device:

```
# iscsiutil -p -O
```

For HP-UX11iv2:

1. Type the following command line to discover the target and create a device file:

```
# /usr/sbin/ioscan -H H 64000
                   (a)
```

NOTE: In this example, **(a)** denotes the default node number allocated by HP-UX.

2. Type the following command line to display the connected device:

```
# iscsiutil -p -0
```

If the host cannot connect to the array's data port, see Table 10-1 on page 10-2.

10

Troubleshooting

This chapter provides troubleshooting information for your array and instructions for calling technical support. This chapter covers the following key topics:

- Potential Error Conditions
- Calling the Hitachi Data Systems Support Center

Potential Error Conditions

Table 10-1 lists potential error conditions that can occur when configuring the array with a host, and provides instructions for resolving each condition. If you are unable to resolve an error condition, please contact your Hitachi Data Systems representative or VAR for help, or log on to the Hitachi Customer Support Center:

https://extranet.hds.com/http://aim.hds.com/portal/dt

Table 10-1: Error Conditions and Recommended Actions

Error Condition	Recommended Action
General Troubleshooting	
The host cannot connect to the target.	• Check that the iSCSI interface cables are correctly installed and firmly connected. • Issue a ping from the host to the target and confirm the response of ping. • Issue a ping from the target to the host and confirm the response of ping. • Confirm that configuration of the target is correct.
The iSCSI host bus adapter (HBA) LEDs do not indicate that you are logged in.	• If using an iSCSI switch, verify that the iSCSI cable is connected securely to an operational iSCSI switch. • If two different iSCSI HBAs are installed, they may be causing a system conflict.
The array's red Alarm LED is ON.	Contact the Hitachi Data Systems Support Center.
The LUN devices are not recognized by the system.	• Verify that the READY LEDs on the are working properly. • Check that the iSCSI interface cables are correctly installed and firmly connected. • For Solaris operating systems: - Recheck the iSCSI buses for new devices using `diag` command. - Verify the contents of `/kernel/drv/sd.conf` file.
Solaris Troubleshooting	
The system hangs, or devices are declared and then the system hangs.	Verify that the target IDs are set 0 through 6 and 8 through 15, and target ID 7 has been reserved for the SCSI controller card.
A "wrong magic number" message appears.	• If you receive a wrong magic number" message, label your disk. • At the command line, type **format** to list all the disks on your array. • Choose the disk by entering its number. • When asked whether you want to label the disk. type **Y** for yes. (If you are not asked, type **I** for label.) • Label all disk attached to your system. • Reboot the system.

Calling the Hitachi Data Systems Support Center

If you need to call the Hitachi Data Systems Support Center, make sure to provide as much information about the problem as possible, including:

- The circumstances surrounding the error or failure.
- The exact content of any error messages displayed on the host system(s).
- The exact content of any error messages displayed by Storage Navigator Modular 2.
- The Storage Navigator Modular 2 configuration information.

The Hitachi Data Systems customer support staff is available 24 hours/day, seven days a week. If you need technical support, please call:

- United States: (800) 446-0744
- Outside the United States: (858) 547-4526

Glossary

This glossary provides definitions of general storage networking terms as well as specific terms related to the technology that supports your array. Click the letter of the glossary section to display that page.

A	B	C	D	E	F	G	H	I	M	N	Q	S	T	W

A

array

A set of hard disks mounted in a single enclosure and grouped logically together to function as one contiguous storage space.

B

BIOS

Basic Input Output System, built-in software code that determines the functions that a computing device can perform without accessing programs from a disk.

Bps

Bits per second, the standard measure of data transmission speeds.

C

capacity

The amount of information (usually expressed in megabytes) that can be stored on a disk drive. It is the measure of the potential contents of a device; the volume it can contain or hold. In communications, capacity refers to the maximum possible data transfer rate of a communications channel under ideal conditions.

Challenge Handshake Authentication Protocol (CHAP)

Challenge Handshake Authentication Protocol, a security protocol that requires users to enter a secret for access.

channel

The link between the central processor and the peripherals. A channel can be the physical cabling that connects the nodes on a network, an electronic signal traveling over a pathway, or a sub-channel in a carrier frequency.

CLI

See command line interface.

cluster

A group of disk sectors. The operating system assigns a unique number to each cluster and then keeps track of files according to which clusters they use.

cluster capacity

The total amount of disk space in a cluster, excluding the space required for system overhead and the operating system. Cluster capacity is the amount of space available for all archive data, including original file data, metadata, and redundant data.

command line interface (CLI)

A method of interacting with an operating system or software using a command line interpreter. With Hitachi's Storage Navigator Modular Command Line Interface, CLI is used to interact with and manage Hitachi storage and replication systems.

D

data volume

A volume that stores database information. Other files, such as index files and data dictionaries, store administrative information (metadata).

direct access storage device (DASD) fast write (DFW)

An attribute of record caching (while DASD Fast Write Access is a function of record caching) in which a specified record ID is placed in the cache and nonvolatile storage when a file-type macro is issued. If the cache is not available or the nonvolatile storage is not available, the record is written directly to the DASD surface.

disk array

An enterprise storage system containing multiple disk drives. Also referred to as "disk array device" or "disk storage system."

E

Ethernet

Local area networking technology, based on transmission packets that go between physical ports over different types of electrical and optical media.

F

fabric

The hardware that connects workstations and servers to storage devices in a SAN. The SAN fabric enables any-server-to-any-storage device connectivity through the use of Fibre Channel switching technology.

failover

The automatic substitution of a functionally equivalent system component for a failed one. The term failover is most often applied to intelligent controllers connected to the same storage devices and host computers. If one of the controllers fails, failover occurs, and the survivor takes over its I/O load.

FC

See Fibre Channel.

FCP

Fibre-Channel Protocol.

Fibre Channel

A gigabit-speed network technology primarily used for storage networking.

firmware

Software embedded into a storage device. It may also be referred to as Microcode.

G

Gbps

Gigabit per second.

GUI

Graphical user interface.

H

HBA

See Host Bus Adapter

High Availability (HA) software

An application designed for use during a primary host or disk failure. The software switches the failed host to a standby host (fail-over). High Availability software must be installed on the primary and secondary hosts.

Host Bus Adapter

An I/O adapter that connects a host I/O bus to the memory system of a computer.

I

I/O

Input/output.

Initiator

A system component that originates an I/O command over an I/O bus or network, such as an I/O adapters or network interface cards.

IP-SAN

Block-level Storage Area Networks over TCP/IP using the iSCSI protocol.

iSNS

Internet-Small Computer Systems Interface, a TCP/IP protocol for carrying SCSI commands over IP networks.

iSCSI

Internet SCSI, an IP-based standard for connecting data storage devices over a network and transferring data using SCSI commands over IP networks. iSCSI enables a Storage Area Network to be deployed in a Local Area Network.

L

LAN

Local Area Network, a computer network that spans a relatively small area, such as a single building or group of buildings.

logical

Describes a user's view of the way data or systems are organized. The opposite of logical is physical, which refers to the real organization of a system. A logical description of a file is that it is a quantity of data collected together in one place. The file appears this way to users. Physically, the elements of the file could live in segments across a disk.

logical unit

See logical unit number.

logical unit number (LUN)

An address for an individual disk drive, and by extension, the disk device itself. Used in the SCSI protocol as a way to differentiate individual disk drives within a common SCSI target device, like a disk

array. LUNs are normally not entire disk drives but virtual partitions (or volumes) of a RAID set.

logical volume

An area on a disk consisting of device files that are logically integrated using a volume manager.

LU

Logical unit.

LUN

See logical unit number.

LUN Manager

This storage feature is operated through Storage Navigator Modular 2 software and manages access paths among host and logical units for each port in your array.

M

microcode

The lowest-level instructions directly controlling a microprocessor. Microcode is generally hardwired and cannot be modified. It is also referred to as firmware embedded in a storage subsystem.

Middleware

Software that connects two otherwise separate applications. For example, a middleware product can be used to link a database system to a Web server. Using forms, users request data from the database; then, based on the user's requests and profile, the Web server returns dynamic Web pages to the user.

N

NIC

Network Interface Card, an expansion board in a computer that allows the computer to connect to a network.

node

In networks, a node is a processing location. A node can be a computer or other device, such as a printer. Every node has a unique network address.

Q

queue depth

When a host queues successive commands to the array before execution of a previous command can complete, the number of times successive commands are issued is called queue depth. When two or more hosts are connected to a port of an array, the number of queue commands for the port is increased because the host issues commands to each array separately.

S

SAN

Storage Area Network, a network of shared storage devices that contain disks for storing data.

SCSI

Small Computer System Interface, a parallel interface standard that provides faster data transmission rates than standard serial and parallel ports.

Software initiator

A software application initiator communicates with a target device. A software initiator does not require specialized hardware because all processing is done in software, using standard network adapters.

SNM2

See Storage Navigator Modular 2.

SNMP

Simple Network Management Protocol, a protocol used to facilitate monitoring and management of clusters through an external interface. SNMP sends notifications to IP addresses whenever certain types of events occur.

software initiator

A software application initiator communicates with a target device. A software initiator does not require specialized hardware because all processing is done in software, using standard network adapters.

Storage Navigator Modular 2

A multi-featured scalable storage management application that is used to configure and manage the storage functions of Hitachi arrays. Also referred to as “Navigator 2”.

T

Target

Devices that receive iSCSI requests that originate from an iSCSI initiator.

target port

A port-type which differs from an “Initiator Port” or “Remote Control Unit Target Port”. The target is used without configuration of Fibre Remote Copy. It allows LOGIN of host computers, but does not allow LOGIN of MCUs.

V

volume

A disk array object that most closely resembles a physical disk from the operating environment's viewpoint. The basic unit of storage as seen from the host.

W

World Wide Name (WWN)

A unique identifier for an open systems host. It consists of a 64-bit physical address (the IEEE 48-bit format with a 12-bit extension and a 4-bit prefix). The WWN is essential for defining the SANtinel™ parameters because it determines whether the open systems host is to be allowed or denied access to a specified logical unit or a group of logical units.

Index

I

K

L

M

N

O

P

Q

R

S

T

U

V

W

Hitachi Data Systems

Corporate Headquarters
750 Central Expressway
Santa Clara, California 95050-2627
U.S.A.
Phone: 1 408 970 1000
www.hds.com
info@hds.com

Asia Pacific and Americas
750 Central Expressway
Santa Clara, California 95050-2627
U.S.A.
Phone: 1 408 970 1000
info@hds.com

Europe Headquarters
Sefton Park
Stoke Poges
Buckinghamshire SL2 4HD
United Kingdom
Phone: + 44 (0)1753 618000
info.eu@hds.com

Hitachi Data Systems

MK-08DF8188-07