



3ware[®] SATA+SAS RAID Controller Card Software User Guide

**Supports the 9750 RAID Controller Card Family
Models 9750-4i, 9750-8i, 9750-4i4e, 9750-8e,
9750-16i4e, and 9750-24i4e**

PN: 45414-01, Rev. A
May 2010



45414-01A

User Guide

Document Description

Document 45414-01, Rev. A. May 2010.

This document will remain the official reference source for all revisions and releases of this product until rescinded by an update.

Disclaimer

It is the policy of LSI Corporation to improve products as new technology, components, software, and firmware become available. LSI reserves the right to make changes to any products herein at any time without notice. All features, functions, and operations described herein may not be marketed by LSI in all parts of the world. In some instances, photographs and figures are of equipment prototypes. Therefore, before using this document, consult your LSI representative for information that is applicable and current. LSI DOES NOT ASSUME ANY RESPONSIBILITY OR LIABILITY FOR THE USE OF ANY PRODUCTS DESCRIBED HEREIN EXCEPT AS EXPRESSLY AGREED TO IN WRITING BY LSI.

LSI products are not intended for use in life-support appliances, devices, or systems. Use of any LSI product in such applications without written consent of the appropriate LSI officer is prohibited.

License Restriction

The purchase or use of an LSI Corporation product does not convey a license under any patent, copyright, trademark, or other intellectual property right of LSI or third parties.

Copyright Notice

© 2010 LSI Corporation. All rights reserved.

Trademark Acknowledgments

LSI™, the LSI logo design, 3ware®, 3DM®, 3DM2™, StorSwitch®, and TwinStor®, StorSave™, and StreamFusion™ + are trademarks or registered trademarks of LSI Corporation.

Apple®, the Apple logo, Mac OS®, and Macintosh® are trademarks of Apple Computer Inc., registered in the United States and/or other countries.

Sun, Solaris and OpenSolaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries. All other brand and product names may be trademarks of their respective companies.

Table of Contents

	About this User Guide	viii
	Exceptions to this Document for Mac OS Users	viii
	How this User Guide is Organized	ix
	Conventions	x
	Screenshots	x
	Using the 3ware HTML Bookshelf	xi
Chapter 1.	Introducing the LSI 3ware SATA+SAS RAID Controller Card	1
	What's New for the 10.2 Release	1
	Highlights of the 10.2 Release	2
	System Requirements	3
	Understanding RAID Concepts and Levels	5
	RAID Concepts	5
	Available RAID Configurations	6
	Determining Which RAID Level to Use	12
	Using Drive Capacity Efficiently	13
	3ware Tools for Configuration and Management	14
	Monitoring, Maintenance, and Troubleshooting Features	15
Chapter 2.	First-Time RAID Configuration Using 3BM	18
	Basic Steps for Creating a Unit	18
	Specifying a Hot Spare	26
	Making Drives Visible to the Operating System	27
	Checking the Motherboard Boot Sequence	27
	What Next?	27
Chapter 3.	Getting Started with Your 3ware RAID Controller	28
	Getting Started for PC Users	28
	Getting Started for Mac OS Users	30
	Initial Settings for Policies and Background Tasks	31
Chapter 4.	3ware BIOS Manager (3BM) Introduction	34
	Starting 3BM	34
	Exiting the 3BM Configuration Utility	36
	Working in the 3BM Screens	37
	Adjusting BIOS Option Settings	40
	Displaying Information About the Controller and Related Devices	42
	Getting Help While Using 3BM	43
Chapter 5.	3DM2 (3ware Disk Manager 2) Introduction	44
	Browser Requirements for 3DM2	45
	Installing 3DM2	45
	Starting 3DM2 and Logging In	45
	Logging In to the 3DM2 Web Application	46
	Managing the 3DM2 Daemon under FreeBSD, Linux, Mac OS, OpenSolaris, and VMware	49
	Starting the 3DM2 Process under Microsoft Windows	50
	Viewing 3DM2 Remotely Using a Web Browser	51
	Working with the 3DM2 Screens	51
	3DM2 Menus	52

	Viewing Information About Different Controllers	55
	Refreshing the Screen	55
	Description of 3DM2 Pages	56
	Setting Up 3DM2 Preferences	58
	Setting and Changing 3DM2 Passwords	58
	Managing E-mail Event Notification	59
	Configuring the VMware Firewall to Allow Email Notification	61
	Enabling and Disabling Remote Access	61
	Setting the Listening Port #	62
	Setting the Frequency of Page Refreshes	62
	Controlling Command Logging in 3DM2	62
Chapter 6.	Configuring Your Controller.	65
	Viewing Information About a Controller	65
	About Controller Policies	67
	Viewing Controller Policies	69
	Setting the Auto-Rebuild Policy	71
	Using Auto-Carving for Multi LUN Support	71
	Setting the Size of Volumes Created with Auto-Carving	74
	Enabling and Setting Up Staggered Spin-up	74
	Viewing Information About a Phy	75
	Changing the Phy Link Speed	77
Chapter 7.	Configuring Units	79
	Configuring a New Unit	79
	Configuration Options When Creating a Unit	79
	Creating a Unit through 3DM2	83
	Creating a Unit through 3BM	85
	Ordering Units in 3BM	89
	Partitioning, Formatting, and Mounting Units	90
	Creating a Hot Spare	97
	Specifying a Hot Spare through 3DM2	98
	Specifying a Hot Spare through 3BM	98
	Naming a Unit	99
	Setting Unit Policies	100
	Enabling and Disabling the Unit Write Cache	102
	Working with Read Cache Settings	104
	Enabling or Disabling Auto-Verify for a Unit	107
	Setting Overwrite ECC (Continue on Source Error When Rebuilding)	108
	Enabling and Disabling Queuing for a Unit	110
	Setting the StorSave Profile for a Unit	111
	Rapid RAID Recovery	113
	Changing An Existing Configuration by Migrating	115
	RAID Level Migration (RLM) Overview	116
	Changing RAID Level	117
	Expanding Unit Capacity	118
	Informing the Operating System of Changed Configuration	119
	Deleting a Unit	121
	Deleting a Unit through 3DM2	121
	Deleting a Unit through 3BM	124
	Removing a Unit	125
	Removing a Unit Through 3DM2	125
	Removing a Unit Through 3BM	127
	Moving a Unit from One Controller to Another	127
	Moving Units from an Earlier 9000 Series to a 9750 Controller	128
	Adding a Drive	129

	Removing a Drive	130
	Rescanning the Controller	132
Chapter 8.	Maintaining Units	133
	Checking Unit and Drive Status through 3DM2	133
	Viewing a List of Drives	135
	Enclosure Drive LED Status Indicators	136
	Unit Statuses	137
	Drive Statuses	138
	About Degraded Units	138
	About Inoperable Units	139
	Locating a Drive by Blinking Its LED	139
	Alarms, Errors, and Other Events	141
	Viewing Alarms, Errors, and Other Events	141
	Using the Alert Utility Under Windows	142
	Downloading an Error Log	144
	Viewing SMART Data About a Drive	144
	Background Tasks	145
	About Initialization	146
	About Verification	149
	Using Auto Verification	152
	Starting a Verify Manually	152
	Rebuilding Units	154
	Cancelling a Rebuild and Restarting It with a Different Drive	159
	Working with the Background Task Mode	159
	Setting the Background Task Mode	162
	Setting Background Task Rate	162
	Background Task Prioritization	163
	Scheduling Background Tasks	163
	Viewing Current Task Schedules	165
	Turning On or Off Use of a Rebuild/Migrate Task Schedule	165
	Selecting Advanced or Basic Verify Schedules	166
	Removing a Task Slot from a Schedule	167
	Adding a New Task Schedule Slot	167
	Selecting Self-tests to be Performed	168
Chapter 9.	Maintaining Your Controller	170
	Determining the Current Version of Your 3ware Driver	170
	Updating the Firmware and Driver	171
	Downloading the Driver and Firmware	172
	Updating the Firmware Through 3DM2	174
	Updating the Firmware Through DOS Using the 3ware Bootable CD	174
	Viewing Battery Information	176
	Testing Battery Capacity	176
Chapter 10.	Enclosure Management	179
	Viewing a List of Enclosures	180
	Checking Enclosure Component Status	181
	Fan Status	183
	Temp Sensor Status	183
	Power Supply Status	183
	Slot Summary	184
	Locating a Specific Enclosure Component	184
	Working with Enclosure Alarms	185
	Controlling an Enclosure Alarm In 3DM2	186
	Turning Off an Enclosure Alarm in 3BM	187

Downloading an Enclosure Diagnostic Log	188
Chapter 11. 3DM2 Reference	189
Controller Summary page	190
Controller Details page	191
Unit Information page	192
Unit Details page	193
Drive Information page	195
Drive Details window	197
Controller Phy Summary page	199
Controller Settings page	200
Scheduling page	205
Maintenance page	208
Alarms page	217
Battery Backup page	218
Enclosure Summary page	220
Enclosure Details page	221
3DM2 Settings page	224
Chapter 12. Troubleshooting	227
Web Resources	227
Before Contacting Customer Support	228
Basic Troubleshooting: Check This First	228
Command Logging	229
Drive Performance Monitoring	229
Types of DPM Statistics	229
Available DPM Commands	230
Problems and Solutions	231
Enclosure-Related Problems	231
Hardware Installation Problems	232
Software Installation Problems	232
Problems in 3DM2 and 3BM	234
Error and Notification Messages	235
Error and Notification Message Details	240
Appendices	293
Glossary	294
Driver and Software Installation	301
Installing 3ware Drivers and Software under FreeBSD	301
Driver Installation for FreeBSD	301
Updating Drivers under FreeBSD	304
Installing Management Software (3DM2 and CLI)	308
Installing 3ware Drivers and Software under Linux	309
Driver Installation Under Linux	310
Obtaining 3ware Linux Drivers	311
Driver Installation Under Red Hat or Fedora Core Linux	312
Driver Installation Under SUSE Linux	317
Compiling a 3ware Driver for Linux	321
Updating the 3ware Driver Under Red Hat or Fedora Core	321
Updating the 3ware Driver Under SUSE	323
Installing Management Software (3DM2 and CLI)	324
Installing 3ware Drivers and Software under Mac OS X	325
Driver and Software Installation	325
Uninstalling 3ware Software under Mac OS X	330
Installing 3ware Drivers and Software under OpenSolaris	331

Driver and Software Installation	331
Installing the Driver and Software from the Command Line	336
Uninstalling 3ware Software Under OpenSolaris	337
Installing 3ware Drivers and Software under VMware	338
Driver Installation Under VMware ESX/ESXi 4.x Server	338
Updating the Firmware Under VMware	341
Installing 3ware RAID Controller Management Software for VMware	342
Uninstalling 3ware Software on VMware	342
Installing 3ware Drivers and Software under Windows	343
Driver Installation Under Windows	343
Updating the 3ware Driver Under Windows	348
Installing Software from a Graphical User Interface (GUI)	350
Uninstalling 3ware Software under Microsoft Windows	354
Compliance and Conformity Statements	355
FCC Radio Frequency Interference Statement	355
Canadian Compliance Statement	356
European Community Conformity Statement	356
Warranty, Technical Support, and Service	357
Limited Warranty	357
Warranty Service and RMA Process	358
LSI Technical Support and Services	358
Sales and ordering information	359
Feedback on this manual	359
Index	360

About this User Guide

This document provides instructions for configuring and maintaining RAID units on LSI™ 3ware® 9750 series RAID controller cards, using 3ware software and firmware version 10.2.

This document assumes that you have already installed your 3ware RAID controller and drives in your system and any enclosures, if you have them. If you have not yet done so, refer to the installation guide that came with your controller. If you do not have the printed copy, a PDF of the installation document is available on your 3ware CD, or you can download it from: <http://www.lsi.com/channel/ChannelDownloads>.

There are often multiple ways to accomplish the same configuration and maintenance tasks for your 3ware RAID controller. This manual includes instructions for performing tasks using the following tools:

- 3ware BIOS Manager (3BM), which runs at the BIOS level
- 3ware Disk Manager 2 (3DM2™), which runs in a browser



Mac User Note: The 3ware BIOS Manager (3BM) is not supported for Mac® OS X.

See “Exceptions to this Document for Mac OS Users”.

You also can perform many tasks using 3ware’s command line interface (CLI). The CLI is described in a separate document: *3ware SATA+SAS RAID Controller Card CLI Guide, Version 10.2*. Information from both this Users Guide and the CLI Guide also are available in the *3ware HTML Bookshelf*, available in the 3ware Documentation folder and on your 3ware CD. (For more information, see “Using the 3ware HTML Bookshelf” on page xi.)

Exceptions to this Document for Mac OS Users

Mac OS users should be aware that the 3ware BIOS utility, 3BM, is not supported for Mac OS. Mac users can make use of 3DM2 and CLI to manage their 3ware RAID controllers and RAID units.

Sections throughout this documentation that describe how to accomplish tasks using 3BM are not relevant for Mac users. In addition, the following two chapters in this document are not relevant for Mac OS users: Chapter 2, “First-Time RAID Configuration Using 3BM” and Chapter 4, “3ware BIOS Manager (3BM) Introduction”.

How this User Guide is Organized

Table 1: Chapters and Appendices in this Guide

Chapter/Appendix	Description
1. Introduction	Provides an overview of product features for the 3ware 9750 controller models. Includes system requirements and an introduction to RAID concepts and levels.
2. First-Time RAID Configuration Using 3BM	Provides step-by-step instructions for configuring RAID units in the BIOS (3BM) if you have just installed the controller. <i>Mac users skip this chapter, 3BM instructions only.</i>
3. Getting Started	Provides a summary of the process you should follow to get started using your 3ware RAID controller.
4. 3ware BIOS Manager (3BM)	Describes the basics of using 3BM. <i>Mac users skip this chapter.</i>
5. 3ware Disk Manager (3DM2)	Describes the basics of using 3DM2. Also includes information about installing and uninstalling 3DM2, and how to start the 3DM2 process manually, if required.
6. Configuring Your Controller	Describes how to view details about the controller, check its status, and change configuration settings that affect the controller and all associated drives.
7. Configuring Units	Describes how to configure new units and hot spares, change existing configurations, move units from one controller to another, and set unit policies.
8. Maintaining Units	Describes how to check unit and drive status, review alarms and errors, schedule background maintenance tasks, and manually start them, when necessary or desirable. Includes explanations of initialization, verify, rebuild, and self-tests.
9. Maintaining Your Controller	Describes how to update the driver and firmware. Also includes information about checking battery status on a battery backup unit (BBU).
10. Enclosure Management	Describes how to view details about an enclosure, check the status of enclosure components, and locate specific enclosure components by blinking an associated LED.
11. 3DM2 Reference	Describes the features and functions on each of the pages in 3DM2.
12. Troubleshooting	Provides common problems and solutions, and explains error messages.

Table 1: Chapters and Appendices in this Guide (continued)

Chapter/Appendix	Description
A. Glossary	Includes definitions for terms used throughout this guide.
B. Driver and Software Installation	Provides instructions for installing 3ware drivers and software management tools (3DM2 and CLI).
C. Compliance and Conformity Statements	Provides compliance and conformity statements.
D. Warranty, Technical Support, and Service	Provides warranty information and tells you how to contact technical support.

Conventions

The following conventions are used throughout this guide:

- 3BM refers to the 3ware BIOS Manager.
- 3DM and 3DM2 both refer to the 3ware Disk Manager.
- In the sections that describe using 3DM2, *current controller* is used to refer to the controller that is currently selected in the drop-down list.
- *Unit* refers to one or more disks configured through 3ware to be treated by the operating system as a single drive. Also known as an array. Array and unit are used interchangeably throughout this manual.
- **Boldface** is used for buttons, fields, and settings that appear on the screen.
- `Monospace font` is used for code and to indicate things you type.

Screenshots

The screenshots in this document are examples only, and may not exactly reflect the operating system and browser that you are using. 3ware software works on a number of different operating systems, including Mac[®] OS X, Microsoft Windows[®], FreeBSD[®], OpenSolaris[™], Linux[®], and VMware[®], and runs in a number of different browsers. In addition, the version numbers shown in screenshots for drivers, firmware, and software may not match your version. For the current released and tested version number, refer to the latest release notes.

In addition, the fields and columns in 3DM2 vary for different models of 3ware RAID controllers. If you have multiple controllers of different models, you may notice some differences when switching between them in 3DM2. For example, when displaying information about the 9750 or 9690SA controllers,

3DM2 displays *VPorts* (for virtual port) on some screens while for earlier controllers the label is *port*.

Using the 3ware HTML Bookshelf

The 3ware HTML Bookshelf is an HTML version of this user guide and the CLI Guide, combined as one resource. It is available on your 3ware CD, in the `/doc/3wareHTMLBookshelf` folder.

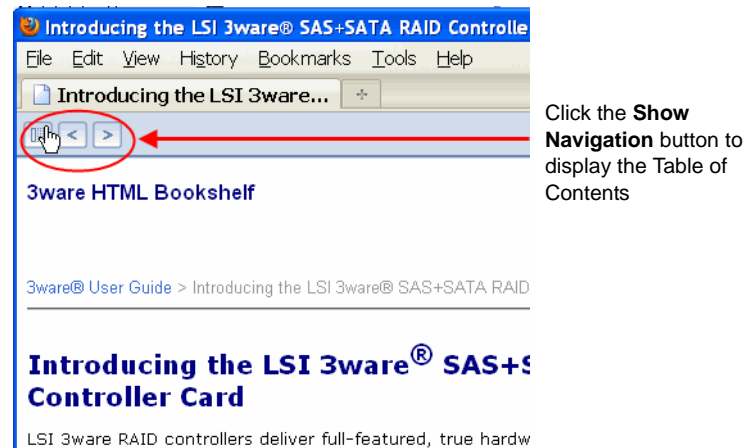
To make use of the 3ware HTML Bookshelf

- To launch the bookshelf at the opening page.
- navigate to the folder `/doc/3wareHTMLBookshelf` on the 3ware CD and double-click the file `index.html`.

When you use this method, a navigation panel at the left automatically opens. It includes a Table of Contents, Index, and Search.

You can also open the bookshelf by double-clicking any HTML file in the 3ware HTMLBookshelf folder. When you open an individual file, the navigation pane does not automatically open. In this case, you can view the navigation pane by clicking the **Show Navigation** button at the left.

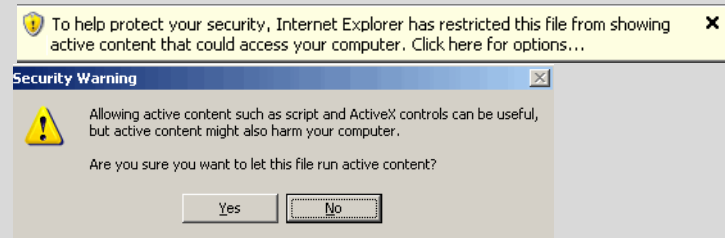
Figure 1. Navigation Button in the 3ware HTML Bookshelf Window





Note: The 3ware HTML Bookshelf is created as a set of HTML documents that are often displayed from a website. When installed on your personal computer, some browsers flag them as “active content,” and require your approval before displaying the content.

If you see messages similar to the following, you must confirm the display of active content in order to see the pages.



Introducing the LSI 3ware SATA+SAS RAID Controller Card

LSI 3ware RAID controllers deliver full-featured, true hardware RAID to servers and workstations. 3ware RAID controllers offer Serial Attached SCSI (SAS) and Serial ATA (SATA) interfaces. Combined with an advanced RAID management feature-set that includes web-based, command-based, and API (application programming interface) software components, LSI RAID controllers provide compelling RAID solutions.

This section introduces the features and concepts of 3ware RAID controllers. It is organized into the following topics:

- What's New for the 10.2 Release
- Highlights of the 10.2 Release
- System Requirements
- Understanding RAID Concepts and Levels
- 3ware Tools for Configuration and Management
- Monitoring, Maintenance, and Troubleshooting Features

What's New for the 10.2 Release

Version 10.2 of the 3ware RAID software and firmware has the following new features and benefits to the 3ware 9750 model RAID controllers.

- Added external enclosure support with the following new 3ware controllers: 9750-4i4e, 9750-8e, 9750-16i4e, 9750-24i4e.
- Added ability to upgrade storage enclosure processor (SEP) firmware. Refer to the *3ware SATA+SAS RAID Controller Card CLI Guide, Version 10.2* for more information.
- Added support for the latest FreeBSD and Linux distributions. For details, refer to the release notes at <http://www.lsi.com/channel/ChannelDownloads>

- Updated 3ware firmware.
- Updated 3DM2 and CLI software.
- Updated Windows drivers.

Highlights of the 10.2 Release

Version 10.2 of the 3ware RAID Software and Firmware provides the following features and benefits to the 3ware 9750 model RAID controllers.

- Support for 6 Gbps SATA+SAS RAID On-a-Chip devices available on the 3ware 9750 RAID controllers, with continued support for the 3ware RAID software feature-set.
- Read cache settings let you enable either Basic Read Caching or Intelligent Read Caching to improve performance.
- Background task mode provides low latency settings to improve performance in video and audio applications.
- Enclosure alarm support allows you to turn off or mute audible alarms in supported enclosures that provide alarms.
- Advanced Content Streaming, a performance feature, provides increased speeds for streamed data, such as video playback and editing, through improved algorithms.
- Rapid RAID Recovery increases the speed with which a degraded unit can be rebuilt. It can also increase the speed of verification or initialization that may occur in the event of an unclean shutdown.
- Improved and simplified auto-verification and scheduling to help ensure that your RAID units are verified on a regular basis.
- Drive performance monitoring provides statistics to help trouble-shoot performance issues.
- Simultaneous RAID 6 parity generation to maximize RAID 6 performance.
- StreamFusion™+ optimizes RAID 5 and RAID 6 disk accesses to maximize application performance under heavy loads.
- StorSave™ BBU with write journaling optimizes data protection and performance.
- Hot-swap and hot-spare for data availability.
- RAID levels 0, 1, 5, 6, 10, 50, and Single Disk.
- With the 9750 models:
 - PCI Express® x8 Gen 2.0
 - Ability to have SAS and/or SATA drives on the same controller (see “Drive Requirements” on page 3)

- Connectivity with up to 127 single-ported drives or 62 dual-ported drives when using cascaded chassis that use expanders of the same type. (see “Enclosure Management Requirements” on page 4)
- Up to 32 drives in a unit
- Up to 32 active units
- Operating system support for Windows, Linux, FreeBSD, Mac OS X, OpenSolaris, and VMware.

System Requirements

This section describes the requirements for the 3ware 9750 model RAID controllers:

Motherboard and Slot Requirements

The 3ware 9750 RAID controller uses workstation-class or server-class motherboards, with an available PCI Express x8 or x16 slot that complies with PCIe Gen 2.0 (recommended for best performance) or PCIe 1.1.

A list of motherboards that have been tested is available at http://www.lsi.com/channel/support/marketing_resources, through the Data & Interoperability tab.

Drive Requirements

The 3ware 9750 RAID controller may be connected to up to 62 SAS and/or SATA dual-ported drives, or 127 SAS and/or SATA single-ported drives, when using one or more enclosures. A maximum of 32 drives are allowed per RAID unit and up to 32 active RAID units per controller.

3ware 9750 RAID controller is designed for use with drive capacities up to 2 TB and over.

You cannot mix SAS and SATA drives in the same unit.

A mix of 3 Gbps and 6 Gbps hard drives are allowed.

Drives and drive enclosures must meet SAS or SATA (3.0 Gbps and 6.0 Gbps) standards.

A list of drives that have been tested is available at http://www.lsi.com/channel/support/marketing_resources, through the Data & Interoperability tab.

Drives may be of any capacity or physical form factor.

The length of internal unshielded interface cables may not exceed 1 meter (39 inches).

The length of external cables for SAS 1.1 at 3 Gbps supports lengths of up to 8 meters and for SAS 2.0 at 6 Gbps supports external cable length to 10 meters.

Enclosure Management Requirements

For 9750 RAID controllers and release 10.2, enclosure management features in 3ware software are available for supported chassis that provide SCSI Enclosure Services 2 (SES-2) through an internal sideband connection, or via an expander.

When chassis enclosures are cascaded, expanders of the same type are recommended. A limit of 4 cascaded expanders is supported.

Chassis and enclosures may be cascaded up to 4 deep, per wide port.

Must support both SAS1 and SAS2, and desirable to allow both within the same domain.

CLI supports in-band firmware downloads to the enclosure processor.

A list of supported enclosures is available at http://www.lsi.com/channel/support/marketing_resources, through the Data & Interoperability tab.

Operating System

3ware 9750 RAID controllers may be used with the following operating systems for Intel and AMD 32-bit and 64-bit x86 based motherboards:

- Microsoft Windows Server 2003 (SP2 or newer) and 2008
- Microsoft Windows Vista and Windows 7
- Red Hat Enterprise Linux®
- openSUSE® Linux
- SUSE® Linux Enterprise Server
- Fedora Core Linux
- Other Linux distributions based on open source Linux 2.6 kernel
- VMware
- OpenSolaris
- FreeBSD
- Mac OS X (Intel only)

For the latest supported operating systems, see the current Release Notes at <http://www.lsi.com/channel/ChannelDownloads> or the file versions.txt, available on the 3ware CD.

Other Requirements

- Adequate air flow and cooling
- Adequate power supply for drives
- 3DM2 (3ware Disk Manager 2) displays information in a browser. It requires one of the following browsers:

- Internet Explorer® (current version)
- Mozilla Firefox® (current version)
- Safari® (current version)

In addition:

- JavaScript must be enabled.
- Cookies must be enabled.
- For best viewing, screen resolution should be 1024 x 768 or greater, with 16-bit color or greater.

For a complete listing of features and system requirements, refer to the 3ware SATA+SAS RAID Controller datasheets, available from the website at <http://www.lsi.com/channel/products/megaraid/sassata/index.html>.

Understanding RAID Concepts and Levels

3ware RAID controllers use RAID (Redundant Array of Independent Disks) to increase your storage system's performance and provide fault tolerance (protection against data loss).

This section includes the following RAID-specific topics:

- "RAID Concepts"
- "Available RAID Configurations" on page 6
- "Determining Which RAID Level to Use" on page 12

RAID Concepts

The following concepts are important to understand when working with a RAID controller:

- **Arrays and Units.** In the storage industry, an *array* refers to two or more disk drives that appear to the operating system as a single unit. When working with a RAID controller, *unit* refers to an array of disks that you can configure and manage through the 3ware software. You can also use the 3ware software to configure Single-disk units.
- **Mirroring.** Mirrored arrays (RAID 1) write data to paired drives simultaneously. If one drive fails, the data is preserved on the paired drive. Mirroring provides data protection through redundancy. In addition, mirroring using a 3ware RAID controller provides improved performance because the 3ware TwinStor® technology reads from both drives simultaneously.
- **Striping.** Striping across disks allows data to be written and accessed on more than one drive simultaneously. Striping combines each drive's

capacity into one large volume. Striped disk arrays (RAID 0) achieve highest transfer rates and performance at the expense of fault tolerance.

- **Distributed Parity.** Parity works in combination with striping on RAID 5, RAID 6, and RAID 50. Parity information is written to each of the striped drives, in rotation. If a failure occurs, you can reconstruct the data on the failed drive from the data on the other drives.
- **Hot Swap.** The process of exchanging a drive without shutting down the system. This process is useful when you need to exchange a defective drive in a redundant unit.
- **Array Roaming.** The process of moving an array from a controller and putting it back either on the same controller, or a different controller, and having the unit recognized as a unit. You can attach the disks to different ports without harm to the data.

Available RAID Configurations

RAID is a method of combining several hard drives into one unit. It can offer fault tolerance and higher throughput levels than a single hard drive or group of independent hard drives. LSI's 3ware controllers support RAID 0, 1, 5, 6, 10, 50, and Single Disk. The following information explains the different RAID levels.

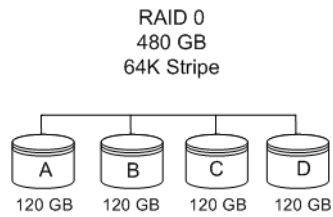
RAID 0

RAID 0 provides improved performance, but no fault tolerance. Because the data is striped across more than one disk, RAID 0 disk arrays achieve high transfer rates because they can read and write data on more than one drive simultaneously. You can configure the stripe size during unit creation. RAID 0 requires a minimum of two drives.

When drives are configured in a striped disk array (see Figure 2), large files are distributed across the multiple disks using RAID 0 techniques.

Striped disk arrays give exceptional performance, particularly for data-intensive applications such as video editing, computer-aided design, and geographical information systems.

RAID 0 arrays are not fault tolerant. The loss of any drive results in the loss of all the data in that array, and can even cause a system hang, depending on your operating system. RAID 0 arrays are not recommended for high-availability systems unless you take additional precautions to prevent system hangs and data loss.

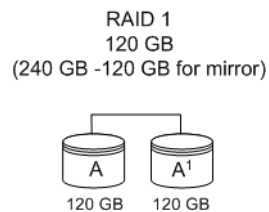
Figure 2. RAID 0 Configuration Example

RAID 1

RAID 1 provides fault tolerance and a speed advantage over non-RAID disks. RAID 1 also is known as a mirrored array. Mirroring is done on pairs of drives. Mirrored disk arrays write the same data to two different drives using RAID 1 algorithms (see Figure 3). This gives your system fault tolerance by preserving the data on one drive if the other drive fails. Fault tolerance is a basic requirement for critical systems should as web and database servers.

3ware firmware uses a patented TwinStor technology, on RAID 1 arrays for improved performance during sequential read operations. With TwinStor technology, read performance during a sequential read operation is twice the speed of a single drive.

The adaptive algorithms in TwinStor technology boost performance by distinguishing between random read request and sequential read requests. For the sequential read requests generated when accessing large files, both drives are used with the drive heads simultaneously reading alternating sections of the file. For the smaller random transactions, the data is read by a single optimal drive head.

Figure 3. RAID 1 Configuration Example

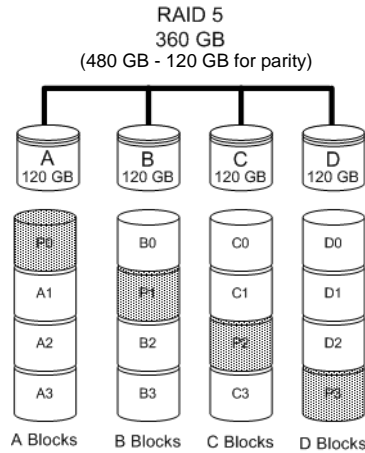
RAID 5

RAID 5 provides performance, fault tolerance, high capacity, and storage efficiency. It requires a minimum of three drives and combines striping data with parity (exclusive OR) to restore data in case of a drive failure. Performance and efficiency increase as the number of drives in a unit increases.

Parity information is distributed across all of the drives in a unit rather than being concentrated on a single disk (see Figure 4). This method avoids throughput loss due to contention for the parity drive.

RAID 5 can tolerate one drive failure in the unit.

Figure 4. RAID 5 Configuration Example

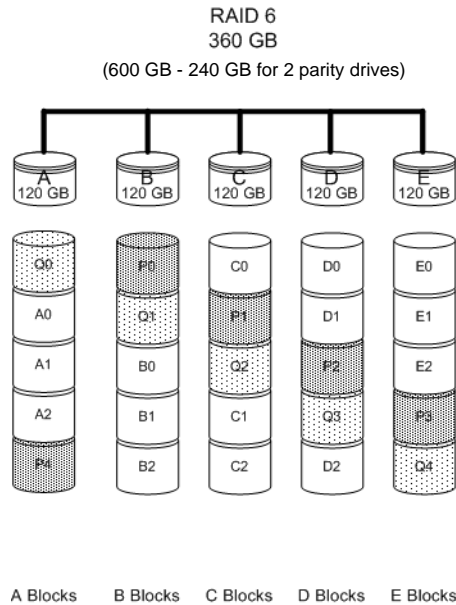


RAID 6

RAID 6 provides greater redundancy and fault tolerance than RAID 5. It is similar to RAID 5 but, instead of a single block, RAID 6 has two blocks of parity information (P+Q) distributed across all the drives of a unit (see Figure 5).

Due to the two parities, a RAID 6 unit can tolerate two hard drives failing simultaneously. This also means that a RAID 6 unit can be in two different states at the same time. For example, one subunit can be degraded while another is rebuilding, or one subunit can be initializing while another is verifying.

The 3ware implementation of RAID 6 requires a minimum of five drives. Performance and storage efficiency also increase as the number of drives increase.

Figure 5. RAID 6 Configuration Example

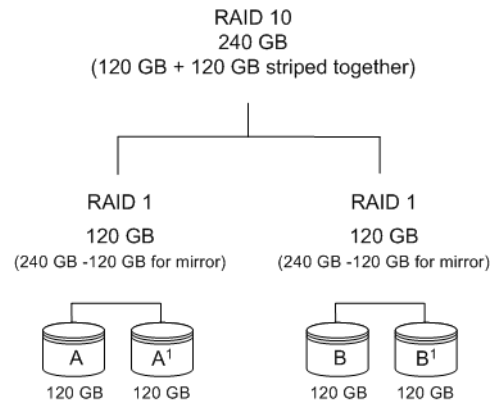
RAID 10

RAID 10 is a combination of striped and mirrored arrays for fault tolerance and high performance.

When drives are configured as a striped mirrored array, the disks are configured using both RAID 0 and RAID 1 techniques (see Figure 6). A minimum of four drives are required to use this technique. The first two drives are mirrored as a fault-tolerant array using RAID 1. The third and fourth drives are mirrored as a second fault-tolerant array using RAID 1. The two mirrored arrays are then grouped as a striped RAID 0 array using a two-tier structure. Higher data transfer rates are achieved by leveraging TwinStor technology and striping the arrays.

In addition, RAID 10 arrays offer a higher degree of fault tolerance than RAID 1 and RAID 5 because the array can sustain multiple drive failures without data loss. For example, in a 12-drive RAID 10 array, up to 6 drives can fail (half of each mirrored pair) and the array continues to function. Note that if both halves of a mirrored pair in the RAID 10 array fail, all of the data is lost.

Figure 6. RAID 10 Configuration Example



RAID 50

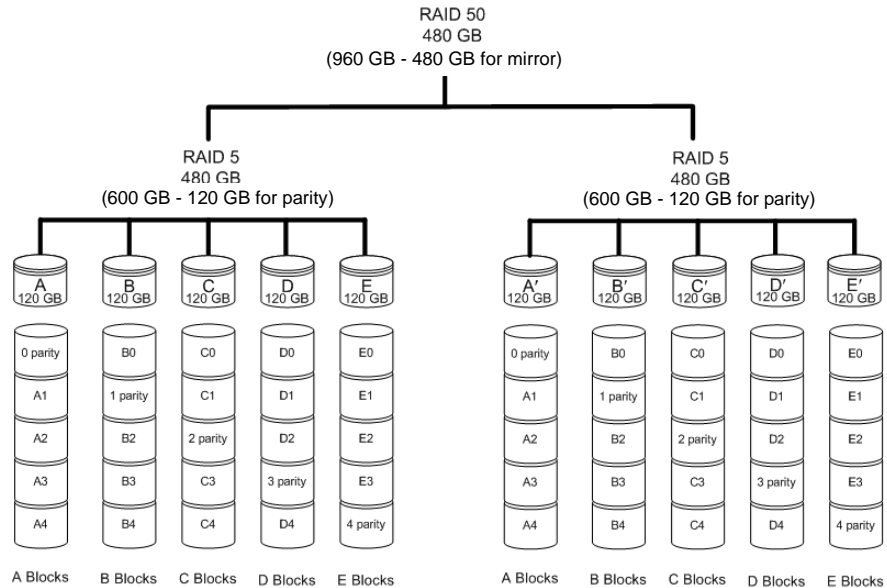
RAID 50 is a combination of RAID 5 and RAID 0. This array type provides fault tolerance and high performance. RAID 50 requires a minimum of six drives.

Several combinations are available with RAID 50. For example, on a 12-port controller, you can have a grouping of three, four, or six drives. A grouping of three means that the RAID 5 arrays used have three disks each; four of these 3-drive RAID 5 arrays are striped together to form the 12-drive RAID 50 array. On a 16-port controller, you can have a grouping of four or eight drives.

No more than four RAID 5 subunits are allowed in a RAID 50 unit. For example, a 24-drive RAID 50 unit may have groups of 12, eight, or six drives, but not groups of four or three (see Figure 7).

In addition, RAID 50 arrays offer a higher degree of fault tolerance than RAID 1 and RAID 5, because the array can sustain multiple drive failures without data loss. For example, in a 12-drive RAID 50 array, one drive in each RAID 5 set can fail and the array continues to function. Note that if two or more drives in a RAID 5 set fail, all of the data is lost.

Figure 7. RAID 50 Configuration Example



Single Disk

You can configure a single drive as a unit through 3ware software. (3BM, 3DM2, or CLI).

Similar to disks in other RAID configurations, single disks contain 3ware Disk Control Block (DCB) information and the OS addresses them as available units.

Single drives are not fault tolerant and, therefore, are not recommended for high availability systems unless you take additional precautions to prevent system hangs and data loss.

Hot Spare

A hot spare is a single drive, available online, so that a redundant unit is automatically rebuilt without human intervention in case of drive failure.

Determining Which RAID Level to Use

The type of RAID unit (array) that you create depends on your needs. You might want to maximize speed of access, total amount of storage, or redundant protection of data. Each type of RAID unit offers a different blend of these characteristics.

The following table summarizes RAID configuration types.

Table 2: RAID Configuration Types

RAID Type	Description
RAID 0	Provides performance, but no fault tolerance.
RAID 1	Provides fault tolerance and a read speed advantage over non-RAID disks.
RAID 5	Provides performance, fault tolerance, and high storage efficiency. RAID 5 units can tolerate one drive failing before losing data.
RAID 6	Provides very high fault tolerance with the ability to protect against two consecutive drive failures. Performance and efficiency increase with higher numbers of drives.
RAID 10	Provides a combination of striped and mirrored units for fault tolerance and high performance.
RAID 50	Provides a combination of RAID 5 and RAID 0. RAID 50 provides high fault tolerance and performance.
Single Disk	Not a RAID type - but supported as a configuration. Provides maximum disk capacity with no redundancy.

You can create one or more units, depending on the number of drives you install. The following table provides possible configurations based on your number of drives.

Table 3: Possible Configurations Based on Number of Drives

Number of Drives	Possible RAID Configurations
1	Single disk
2	RAID 0 or RAID 1
3	RAID 0 RAID 1 with hot spare RAID 5

Table 3: Possible Configurations Based on Number of Drives

Number of Drives	Possible RAID Configurations
4	RAID 5 with hot spare RAID 10 Combination of RAID 0, RAID 1, single disk
5	RAID 6 RAID 5 with hot spare RAID 10 with hot spare Combination of RAID 0, RAID 1, hot spare, single disk
6 or more	RAID 6 RAID 6 with hot spare RAID 50 Combination of RAID 0, 1, 5, 6,10, hot spare, single disk

Using Drive Capacity Efficiently

Because the capacity of each drive is limited to the capacity of the smallest drive in the unit, use drives of the same capacity in a unit.

The total unit capacity is defined as follows:

Table 4: Drive Capacity

RAID Level	Capacity
Single Disk	Capacity of the drive
RAID 0	(number of drives) X (capacity of the smallest drive)
RAID 1	Capacity of the smallest drive
RAID 5	(number of drives – 1) X (capacity of the smallest drive) Storage efficiency increases with the number of disks: storage efficiency = (number of drives – 1)/(number of drives)
RAID 6	(number of drives – 2) x (capacity of the smallest drive)
RAID 10	(number of drives/2) X (capacity of smallest drive)
RAID 50	(number of drives – number of groups of drives) X (capacity of the smallest drive)

Through drive coercion, the capacity used for each drive is rounded down to improve the likelihood that you can use drives from differing manufactures as spares for each other. The capacity used for each drive is rounded down to the

nearest GB for drives under 45 GB (45,000,000,000 bytes), and rounded down to the nearest 5 GB for drives over 45 GB. For example, a 44.3-GB drive is rounded down to 44 GB, and a 123-GB drive is rounded down to 120 GB.



Note: All drives in a unit must be of the same type, either SAS or SATA.

3ware Tools for Configuration and Management

3ware software tools let you easily configure the drives attached to your 3ware RAID controller, specifying which drives you should use together as a RAID unit and the type of RAID configuration that you want, and designating hot spares for use if a drive degrades.

3ware provides the following tools for use in configuring and managing units attached to the 3ware controller:

- **3BM (3ware BIOS Manager)**

3BM is a BIOS-level tool available on PC-based systems that you can use to create, delete, and maintain disk arrays, rebuild arrays, designate hot spares, and set controller policies. 3BM is the tool most frequently used to configure units immediately after installation of the controller, but also can be used after installation to maintain the controller and associated drives. (3BM is not available for Mac OS X.)

For general information about working with 3BM, see Chapter 4, “3ware BIOS Manager (3BM) Introduction.”

- **3DM2 (3ware Disk Manager)**

3DM2 provides browser-based software that you can use to create, delete, and maintain disk arrays, rebuild arrays, designate hot spares, and set controller policies. 3DM2 is a daemon (under FreeBSD, Linux, Mac OS X, OpenSolaris, and VMware) and a service (under Windows) that runs in the background on the controller’s host system. You can access 3DM2 through a web browser to provide ongoing monitoring and administration of the controller and associated drives. You can use 3DM2 locally (on the system that contains the 9750) or remotely (on a system connected via a network to the system containing the 9750).

For details about working with the 3ware Disk Manager 2, see “3DM2 (3ware Disk Manager 2) Introduction” on page 44.

3DM2 is the current version of the 3ware Disk Manager. Throughout this documentation, it is referred to interchangeably as 3DM and 3DM2.

- **3ware Alert Utility (WinAVAlarm)**

The 3ware Alert Utility for Windows runs on the system in which the 3ware RAID controller is installed and provides direct notification by a pop-up message and audio alarm when events occur. You can configure this unit to specify the type of events that should generate these notifications. For details, see “Using the Alert Utility Under Windows” on page 142.

- **3ware CLI (Command Line Interface)**

The 3ware CLI provides the functionality available in 3DM2 through a command line interface. CLI also provides advanced functions not included in 3DM2 such as, drive performance monitoring (DPM). You can view unit status and version information and perform maintenance functions such as adding or removing drives, and reconfiguring RAID units online. You also can use it to remotely administer controllers in a system.

The 3ware CLI is described in *3ware SATA+SAS RAID Controller Card CLI Guide, Version 10.2* and in the *3ware HTML Bookshelf*.

Monitoring, Maintenance, and Troubleshooting Features

Several 3ware RAID controller features aid in monitoring and troubleshooting your drives.

- **Auto-Rebuild.** When you do not have a spare available, setting the Auto Rebuild policy allows rebuilds to occur with an available drive or with a failed drive. (For more information, see “Setting the Auto-Rebuild Policy” on page 71.)
- **Drive Performance Monitoring (DPM).** DPM is an advanced troubleshooting tool used to measure drive performance, and to help identify when a specific drive is causing problems so that you can repair or replace it. Commands are available through the 3ware CLI to enable and disable DPM, and to see a range of different statistics. These statistics can be useful to help troubleshoot problems with your RAID controller and units. For more information, see “Drive Performance Monitoring” on page 229.
- **Enclosure Services.** Drives, fans, temperature sensors, and power supplies in supported chassis and enclosures can be identified by flashing LEDs so that you can quickly identify which component needs to be checked or replaced. For more information, see “Enclosure Management” on page 179.

- **Error Correction.** Bad sectors can be dynamically repaired through error correction (Dynamic Sector Repair). Reallocation of blocks is based intelligently on the location of the block in relation to the stripe.
- **Scheduled Background Tasks.** Initialize, rebuild, verify, and self-test tasks can all be run in the background, at scheduled times. This task lets you choose a time for these tasks to be run when it will be least disruptive to your system. You also can define the rate at which background tasks are performed, specifying whether I/O tasks should be given more processing time, or background rebuild and verify tasks should be given more processing time. (For more information, see “Scheduling Background Tasks” on page 163.)
- **SMART Monitoring.** Self-Monitoring, Analysis and Reporting Technology (SMART) automatically checks the health of SATA and SAS disk drives every 24 hours and reports potential problems. This allows you to take proactive steps to prevent impending disk crashes. SMART data is checked on all disk drives (array members, single disks, and hot spares). Monitoring of SMART thresholds can be turned on and off in 3DM2. For more information, see “Selecting Self-tests to be Performed” on page 168 and “Viewing SMART Data About a Drive” on page 144.
- **Staggered Spinup.** Staggered spinup allows drives that support this feature to be powered-up into the standby power management state to minimize in-rush current at power-up and to allow the controller to sequence the spin-up of drives. Both SATA-2 OOB and ATA spin-up methods are supported. The standby power management state is persistent after power-down and power-up. You can set the number of drives that will spin up at the same time, and the time between staggers in 3BM and CLI. For more details, see Table 5 on page 32. This feature does not apply to drives that are attached to an expander. For details, see “Enabling and Setting Up Staggered Spin-up” on page 74.
- **StorSave™ Profiles** allow you to set the level of protection versus performance that is desired for a unit when write cache is enabled. (For more information, see “Setting the StorSave Profile for a Unit” on page 111.)
- **Verification and Media Scans.** The verify task verifies all redundant units, and checks for media errors on single disks, spares and RAID 0 unit members. If the disk drive is part of a redundant unit, error locations that are found and are deemed repairable are rewritten with the redundant data. This forces the drive firmware to reallocate the error sectors accordingly. (For more information, see “About Verification” on page 149.)
- **Read Cache.** Two read cache settings are available. Basic Read Cache stores data from media locally on the controller to improve read access times for applications. The 3ware Read Cache feature also includes an Intelligent Mode, which enables intelligent read prefetch (IRP). IRP

includes a typical read-ahead caching method which is used to proactively retrieve data from media and store it locally on the controller with the anticipation that it may be requested by the host. By default read cache is set to the Intelligent mode. For more information, see “Working with Read Cache Settings” on page 104.

- **Write Cache.** You can enable or disable write cache using 3BM, 3DM2, and CLI. When write cache is enabled, data will be stored in 3ware controller cache and drive cache before the data is committed to disk. This allows the system to process multiple write commands at the same time, thus improving performance. However when data is stored in cache, it could be lost if a power failure occurs. With a battery backup unit (BBU) installed, the data stored on the 3ware controller can be restored. (For more information, see “Enabling and Disabling the Unit Write Cache” on page 102.

2

First-Time RAID Configuration Using 3BM

If you are installing the operating system on and boot from a unit managed through the new 3ware RAID controller, follow the steps in this chapter to use the 3ware BIOS Manager (3BM) to configure the unit and install the driver.



Mac User Note: The 3ware BIOS Manager (3BM) is not supported for Mac OS X. Mac OS users, skip this chapter.

If the operating system is already installed on another drive in your system, you can use the steps below or you can configure units through 3DM2 or the CLI.

You can create one or more units on a single controller, depending on the number of drives that the specific 3ware RAID controller supports and the number of drives attached. (For more information, see “Determining Which RAID Level to Use” on page 12.)

Basic Steps for Creating a Unit

Configuring your RAID units includes these main steps.

- Launch 3BM (3ware BIOS Manager)
- Select the drives to be included and indicate that you want to create a unit
- Select the desired RAID configuration
- Set other parameters, depending on the type of RAID configuration
- Confirm the unit configuration
- Save your changes and finish up

Launching 3BM

- 1 Power up or reboot your system.

While the system is starting, watch for a screen similar to Figure 8.

Figure 8. 3ware BIOS Screen

```

----Press <Alt-3> to access 3ware BIOS Manager ----
3ware ATA RAID Controller: 9750-4I
BIOS: BE9X X.XX.XX.XXX  Firmware: FE9X X.XX.XX.XXX
BBU Status: Not Present
Number of online units: 1, available drives: 0, hot spare: 0, offline units:0

Available drives:

          SATA - SAMSUNG  HD160JJ                149.04 GB  Phy  0

Exportable Units:Ⓔ

3drive 64K RAID5          298.00 GB (Zygot3)  DEGRADED
          SATA - SAMSUNG  HD160JJ                149.04 GB  (Phy 3)
          SATA - SAMSUNG  HD160JJ                149.04 GB  (Phy 1)

```

- 2 Press **Alt-3** or **3** immediately to bring up the **3ware BIOS Manager (3BM)**.

Normally your 3ware configuration remains on-screen for just a few seconds. However, if a unit has degraded, the screen indicates the problem and remains on your screen longer.

- 3 If you plan to make changes to your configuration and need to backup data before continuing, press **ESC** and do so now. Otherwise, press any key to continue.

Figure 9. Warning Message When you Start 3BM

```

3ware BIOS Manager (Controller 0)

Disks have existing data!

When you configure your disk array(s), existing data on
some drives may be overwritten.
When you hit the Done key, you will be notified which
drives will be overwritten and offered the option of
abandoning the new settings before any data is lost.
If you are concerned about losing data, hit Escape
to stop configuring and back up your drives first.

Press any key to continue.

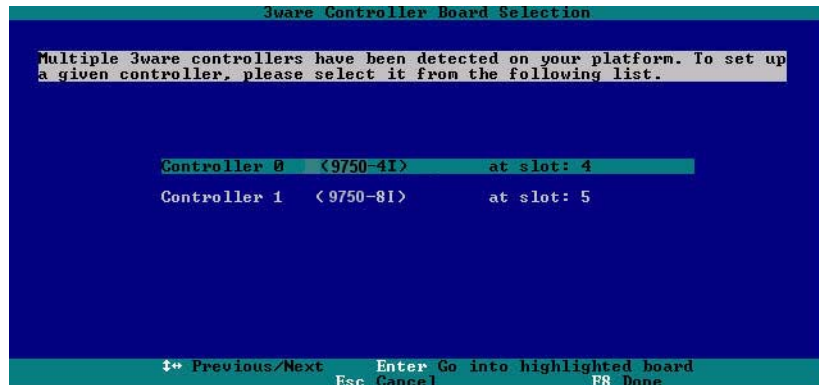
Alt-F1 Help  F2 Prev/Next  Alt-a Select All Drives  Alt-r Rescan  Enter Select/Dese
F6 Restore Initial Values  Esc Cancel  F8 Done  PGUP PGDOWN Reorder

```

- 4 If you have more than one 9750 controller in your system, a screen lists the available boards. (See Figure 10.) In this case, highlight the board with which you want to work and press **Enter**.

If you have more than four boards, you see only four at first (only four can be processed at a time). After you exit from 3BM, you can access the BIOS again, and access the next boards.

Figure 10. 3ware Controller Board Selection Screen



A screen similar to Figure 9 appears, warning you that changing your disk array configuration may overwrite data on the disks.

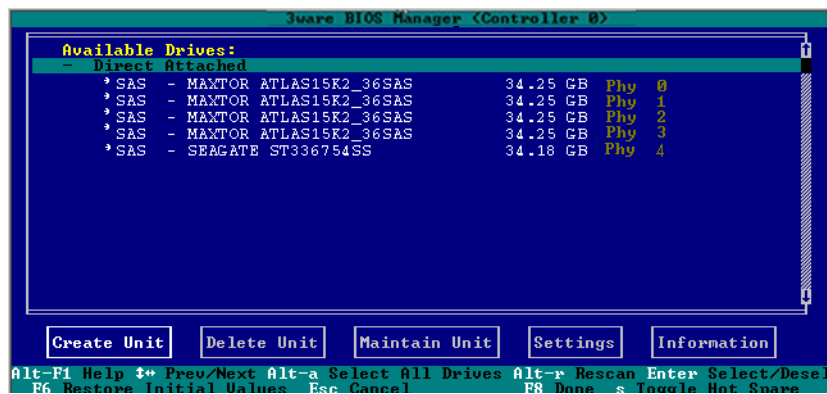
To select the drives and create a unit

- 1 Select the drives to be included by highlighting each one and pressing **Enter** to select it, or select all at once by selecting the heading above them.

When you select a drive, an asterisk appears next to it in the left-most column (see Figure 11).

You may include from 1 to 32 drives in the unit, depending on the number available.

Figure 11. Asterisks Next to Selected Drives

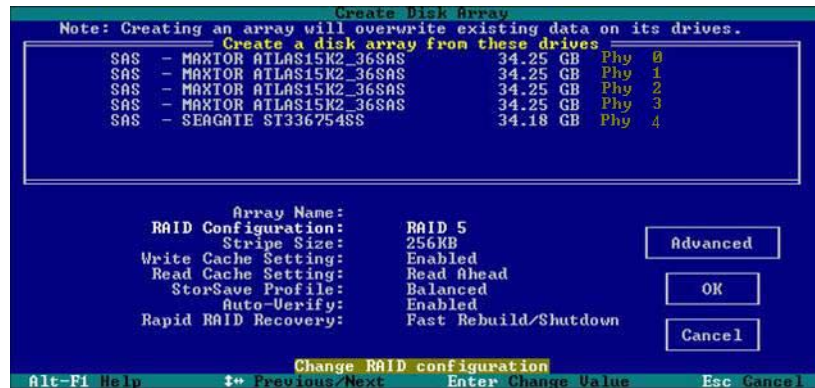


- 2 After all drives for the unit are selected, use the **Tab** to move to the **Create Unit** button and press **Enter**.

The **Create Disk Array** screen appears (see Figure 12).

- 3 Make sure that the proper drives are listed.

Figure 12. Create Disk Array screen



To name the unit and select the desired RAID configuration

- 1 (Optional) Press **Enter** in the **Array Name** field and type a name for the unit. Then press **Enter** again to accept the name.
- 2 Use the **arrow keys** or press **Tab** to move to the **RAID Configuration** field and press **Enter** to view the available RAID levels for the number of drives you selected.

Figure 13. List of Configuration Choices for Four Drives



- 3 Use the **arrow keys** to highlight the desired RAID configuration and press **Enter**.

For information about the different RAID levels and when to use each, see “Understanding RAID Concepts and Levels” on page 5.

- 4 Use the **arrow keys** or press **Tab** to move to the field **Stripe Size** and select the desired stripe size (16KB, 64KB, or 256KB).



Notes:

Striping size is not applicable for RAID 1, because it is a mirrored unit without striping.

For RAID 6, only stripe sizes of 64 KB and 256 KB are supported.

To set other policies for the unit

While creating a unit through 3BM, you can set a number of unit policies. Each of these policies is already set to a default value, so you do not have to change them.

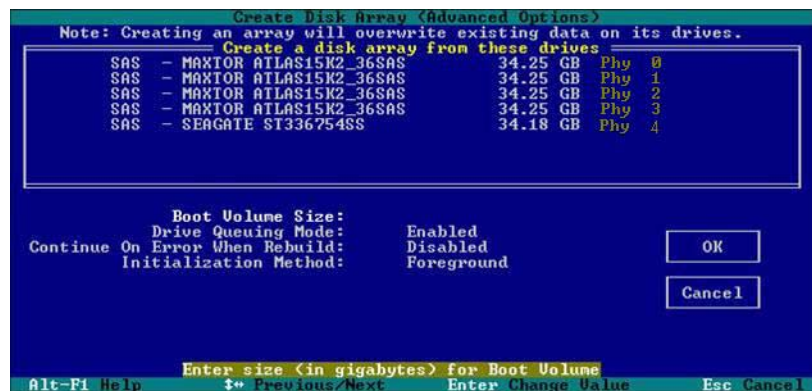
Many of these options are listed on the Create Disk Array screen. A few are available through the Advanced Options screen.

- 1 Use the **arrow keys** to move through the policies shown on the screen, select the option you want and press **Enter** to choose it.
- 2 Press **Tab** to the **Advanced** button and press **Enter** to open the Advanced options screen, where additional policies are available.

For details about the various unit policies, see the following sections:

- “Enabling and Disabling the Unit Write Cache” on page 102
- “Working with Read Cache Settings” on page 104
- “Setting the StorSave Profile for a Unit” on page 111
- “Enabling or Disabling Auto-Verify for a Unit” on page 107
- “Rapid RAID Recovery” on page 113
- “Enabling and Disabling Queuing for a Unit” on page 110
- “Setting Overwrite ECC (Continue on Source Error When Rebuilding)” on page 108
- “Initialization Method” on page 81

Figure 14. Create Disk Array Advanced Options screen



To create a boot volume of a particular size

You can specify a portion of the unit you create to be used as a boot volume. This option is useful if you install your operating system onto the unit and want to have a designated volume for the OS. The remainder of the unit is created as a separate volume (or volumes if auto-carving is also used.).



Note: Setting a Boot Volume Size is optional. In addition, if you specify a boot volume, you do not have to install your operating system onto it. For more information about creating a boot volume, see “Boot volume size” on page 81. If the size of your array is 2 TB or greater, you also may want to review the information about carving the unit into multiple volumes. For details, see “Using Auto-Carving for Multi LUN Support” on page 71.

- 1 Open the Advanced Options screen. (From the Create Disk Array screen, press **Tab** to the **Advanced** button and press **Enter**.)
- 2 In the **Boot Volume Size** field, press **Enter** to display a text box.
- 3 Enter the size in Gigabytes that should be assigned to the boot volume.
- 4 Press **Enter** again to accept the size.

To confirm unit configuration

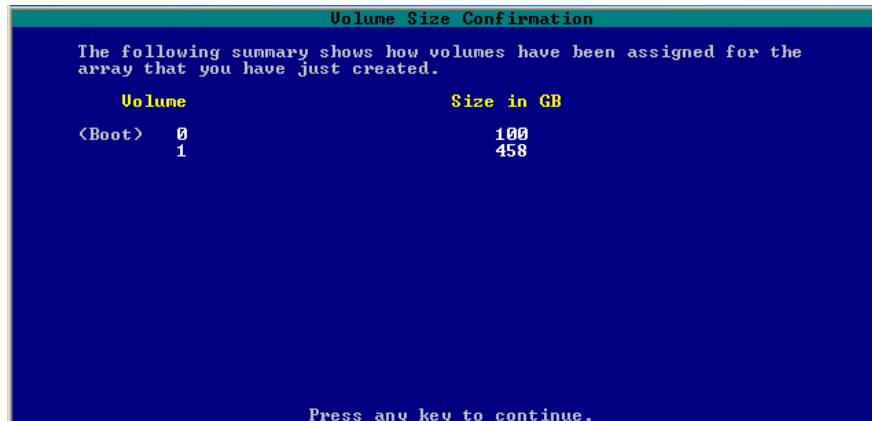
- 1 If you are on the **Advanced Options** screen, press **Tab** to select the **OK** button and press **Enter** to return to the Create Disk Array screen.
- 2 Press **Tab** to select the **OK** button and press **Enter** to confirm creation of the unit.

Or, if you want to cancel the creation of the unit, tab to **Cancel** and press **Enter**.

- 3 If you leave the **Unit Write Cache** field enabled and do not have a BBU installed, 3BM asks you to confirm that you want to enable write cache.
The unit is not actually created and no data is overwritten until you have finished making all of your changes and press **F8**.
- 4 If the volume summary screen appears, review the information and press any key to continue.

Multiple volumes are created if you entered a Boot Volume Size of greater than zero (0), or if auto-carving is enabled and the combined size of the drives in your unit is large enough to divide it into multiple volumes. For more information about auto-carving, see “Using Auto-Carving for Multi LUN Support” on page 71.

Figure 15. Summary of Volumes to be Created



To finish up and save your changes

- 1 If you have additional drives, you can configure an additional RAID unit or designate a hot spare. (For details about hot spares, see page 26.)
- 2 If you configured more than one unit, and you plan to install the operating system on one of them, make that unit be the first unit (Unit 0) in the list of Exportable Units.

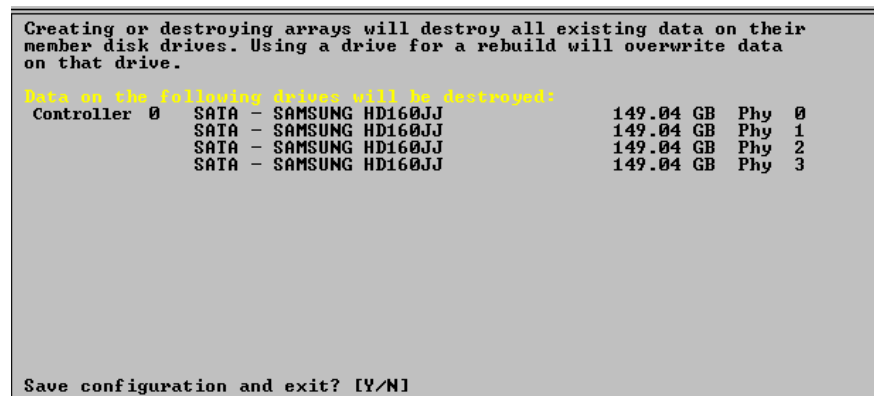
To move a unit up in the list, highlight it and press the **Page Up** key.

Make sure that the controller is the boot device for your computer. After finalizing the configuration below, make sure to follow the steps under “Checking the Motherboard Boot Sequence” on page 27.

- 3 When you are finished configuring units, press **F8** to save the changes and exit 3BM.

A warning message asks you to confirm that all existing data on the drives will be deleted.

Figure 16. Confirmation Message when Saving and Exiting



- 4 Type **Y** to continue, delete any existing data on the drives, and create the unit.

If you chose foreground initialization, then, depending on the RAID configuration you are creating, initialization of the unit may begin immediately and delay your ability to use your unit for several hours. (RAID 6 units and some RAID 5 and RAID 50 units begin immediate initialization.)

- 5 If you want to immediately use a RAID configuration that has started foreground initializing, you can press **Esc** to cancel the progress box. (Before doing this, be sure to read “Trade-offs to cancelling initialization,” below.)

You can then exit 3BM and boot to the operating system before the process of writing zeroes to the drives is complete. After you have booted to the operating system, background initialization of the unit begins after a delay of up to ten minutes.

**Trade-offs to cancelling initialization:****Pros:**

- The unit can be used immediately and is fully fault tolerant.

Cons:

- Performance of these units are lower until initialization is complete.
- Initialization takes longer to complete, because background initialization takes longer than foreground initialization.

For complete information about initialization of RAID units, see “About Initialization” on page 146.

- 6 After you have finished creating RAID units, check the boot sequence for your system, as described under “Checking the Motherboard Boot Sequence” on page 27.

Specifying a Hot Spare

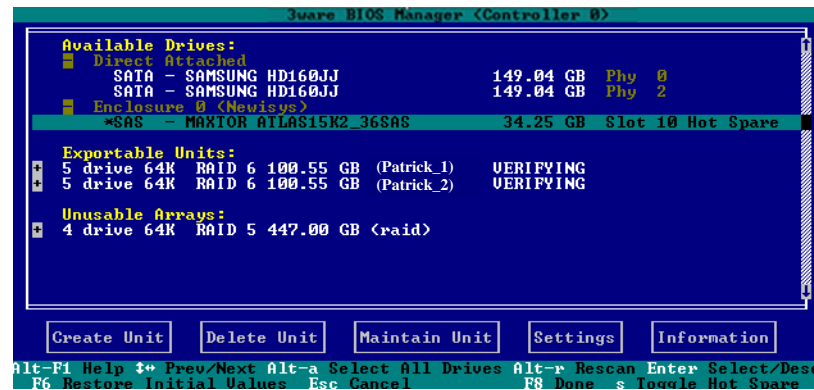
You can designate one of the **Available Drives** as a hot spare in 3BM. If a hot spare is specified and a redundant unit degrades, an event notification is generated. If the hot spare is of the same type (SAS or SATA) and of adequate size, the hot spare automatically replaces the failed drive without user intervention.

To specify a hot spare

- 1 In the list of **Available Drives**, highlight the drive to use.
- 2 Type **s** to specify that the selected drive will be the hot spare.

The words “Hot Spare” appear next to the drive in the Available Drives list.

Figure 17. Hot Spare Indicated



If a hot spare is already enabled, you can disable it by following the same process.



Note: To replace a failed drive in a degraded unit, make sure that a hot spare drive has the same or larger storage capacity than the failed drive.

Making Drives Visible to the Operating System

By default, if you leave individual drives unconfigured, they will not be available to the operating system. If you want to use individual drives, configure them as single-disk units.

Checking the Motherboard Boot Sequence

Using your computer's BIOS setup utility, make sure that it shows the appropriate boot devices.

After installing the 3ware controller in your system, go into the BIOS for your computer system to check and change the boot order. The new controller is usually added as a boot device after previously existing boot devices. You can move it up in the list, if appropriate. Refer to the documentation for your system for information about starting the system BIOS.

- **If the OS is already installed on a unit connected to the system**, make sure that device precedes the 3ware RAID controller in the boot sequence. If you have other disks installed on the motherboard, the 3ware RAID controller should precede them in boot order.
- **If you are installing your OS on a disk or unit attached to the 3ware RAID controller**, specify the controller as the boot device. In 3BM, the unit listed at the top on the 3BM main page will be the boot unit. You can change the order by highlighting a unit and pressing the PgUp or PgDn key. (Note that if you configured more than one unit, the drive(s) specified as Unit 0 is treated as the boot disk.)

What Next?

The final steps in setting up your RAID units is to load the 3ware driver and make the units available to your operating system. For details about loading the 3ware driver, turn to Appendix B, "Driver and Software Installation" on page 301 and for details on making the units available to your system, see Chapter 7, "Configuring Units.", and "Partitioning, Formatting, and Mounting Units" on page 90

After installing the driver, in order to maintain your RAID units, you may also want to install 3ware's browser-based Disk Management tool, 3DM2, or the 3ware command line interface (CLI). For more information, see Appendix B, "Driver and Software Installation" on page 301.

3

Getting Started with Your 3ware RAID Controller

Setting up your 3ware RAID controller involves these main steps:

- Physically Install the RAID Controller and Drives
- Install the Driver and Software
- Configure a RAID Unit
- Set Up Management and Maintenance Features

After you have physically installed the controller and drives, the order in which you perform these steps depends in part on whether one of the units you configure will act as your boot drive.

The start-up process is slightly different for Mac OS users than for users of other operating systems, so this chapter presents these main steps and the initial settings for policies and background tasks in the following three sections:

- Getting Started for PC Users
- Getting Started for Mac OS Users
- Initial Settings for Policies and Background Tasks

Tip: When you are first setting up your system, you may want to review “System Requirements” on page 3.

Getting Started for PC Users

Physically Install the RAID Controller and Drives

To install your controller, follow the instructions in the installation guide that came with your 3ware controller. If you do not have a hardcopy of the installation manual, it is available in the “doc” folder on your 3ware CD, or you can download it from the LSI website at <http://www.lsi.com/channel/ChannelDownloads>.

For drive installation, refer to the instructions that came with your enclosure. If you are installing drives in a computer case, follow the manufacturer's instructions.

Configure a RAID Unit

If you want to install the operating system on and boot from a drive managed through the new 3ware RAID controller, use the 3ware BIOS Manager (3BM) to define the configuration. Follow the instructions for initial installation in Chapter 2, "First-Time RAID Configuration Using 3BM." Additional information about configuration also is included in the later chapters of this user guide.

If the operating system is already installed on another drive in your system, you can configure units through 3BM, through 3ware Disk Manager (3DM2), or through the Command Line Interface (CLI). If you want to use 3DM2 or the CLI for configuration, go ahead and boot to the operating system, install the driver and the 3DM2 software, and then configure your units. You may want to refer to the following information:

- Chapter 5, "3DM2 (3ware Disk Manager 2) Introduction"
- Chapter 7, "Configuring Units"
- *3ware SATA+SAS RAID Controller Card CLI Guide, Version 10.2*, available from the 3ware CD and from the website <http://www.lsi.com/channel/ChannelDownloads>

If you would like more information about what RAID level to choose for your situation, review the information under "Understanding RAID Concepts and Levels" on page 5.

Install the Driver and Software

Instructions for installing drivers are available in "Driver and Software Installation" on page 301.

Set Up Management and Maintenance Features

3ware RAID controllers include a number of features to help you manage and maintain the controller and your configured units. The default settings for these features allow you to begin using your newly configured units right away. You can review and change these features as a final step in your initial setup, or you can make changes to them later, at your convenience. These features include:

- Controller and unit policies, such as Auto-Rebuild, Auto-Verify, use of write cache, use of queuing mode, and selection of a StorSave profile.
- Email notification of alarms and other events
- Schedules for when background tasks will be performed, to minimize the impact on day-to-day performance during peak usage times. (Background tasks include rebuild, verify, initialize, migrate, and self-test.)

Details about these features are described in this documentation. When you first set up your controller, you may want to review these sections in particular:

- “Initial Settings for Policies and Background Tasks” on page 31
- “Configuring Your Controller” on page 65
- “Setting Unit Policies” on page 100
- “Setting Background Task Rate” on page 162

Getting Started for Mac OS Users

Physically Install the RAID Controller and Drives

To install your controller, follow the instructions in the installation guide that came with your 3ware controller. If you do not have a hardcopy of the installation manual, it is available in the “doc” folder on your 3ware CD, or you can download it from the LSI website at <http://www.lsi.com/channel/ChannelDownloads>.

You should also refer to the instructions in the user guide for your Mac Pro for opening your computer and installing a PCI Express card in a PCI Express x8 or x16 slot, and for installing drives in your computer case. If you are installing drives in a separate enclosure, refer to the instructions that came with your enclosure.

Install the Driver and Software

Instructions for installing drivers and software are available under “Installing 3ware Drivers and Software under Mac OS X” on page 325.

Configure a RAID Unit

If you would like more information about what RAID level to choose for your situation, review the information under “Understanding RAID Concepts and Levels” on page 5.

You can configure a RAID unit using either 3DM2 or the CLI. For details on configuring through 3DM2, see “Configuring a New Unit” on page 79. For information about working with the CLI, refer to *3ware SATA+SAS RAID Controller Card CLI Guide, Version 10.2*, available from the 3ware CD and from the website <http://www.lsi.com/channel/ChannelDownloads>

Set Up Management and Maintenance Features

3ware RAID controllers include a number of features to help you manage and maintain the controller and your configured units. The default settings for these features allow you to begin using your newly configured units right away. You can review and change these features as a final step in your initial setup, or you can make changes to them later, at your convenience. These features include:

- Controller and unit policies, such as Auto-Rebuild, Auto-Verify, use of write cache, use of queuing mode, and selection of a StorSave profile.
- Email notification of alarms and other events
- Schedules for when background tasks will be performed, to minimize the impact on day-to-day performance during peak usage times. (Background tasks include rebuild, verify, initialize, migrate, and self-test.)

Details about these features are described in this documentation. When you first set up your controller, you may want to review these sections in particular:

- “Initial Settings for Policies and Background Tasks” on page 31
- “Configuring Your Controller” on page 65
- “Setting Unit Policies” on page 100
- “Setting Background Task Rate” on page 162

Initial Settings for Policies and Background Tasks

The table below lists the default settings for policies and background tasks. These settings are used if you do not explicitly change the policy settings.

Table 5: Default Settings for Policies/Background Tasks

Policy	Default Value	Where to Change
Controller-Level Settings (For details, see “Configuring Your Controller” on page 65)		
Auto-Rebuild	Enabled	3BM, 3DM2, CLI
Auto-Carving	Enabled	3BM, 3DM2, CLI
Auto-Detect	Enabled	CLI
Auto-Verify Preferred Start Day and Time (Basic)	Friday, 12 am	3BM, 3DM2, CLI
Auto-Verify Verify Schedule (Advanced)	Seven days of the week, starting at 12 am and running 24 hours.	3DM2, CLI
Carve Size or Factor	2048 GB	3BM, 3DM2, CLI
Drives Per Spinup	1	3BM, CLI
Delay Between Spinup	6 seconds	3BM, CLI
Export Unconfigured (JBOD) Disks	No	3BM, CLI
Staggered Method	ATA-6	3BM
Staggered Spinup	Enabled	3BM
Unit-Level Settings (For details, see “Setting Unit Policies” on page 100)		
Auto-Verify	Enabled	3BM, 3DM2, CLI
ECC Overwrite (Continue on Error When Rebuilding)	Disabled	3BM, 3DM2, CLI
Boot Volume Size	Unspecified	3BM, CLI
Initialization Method	Foreground	3BM
Queuing (NCQ)	Enabled	3BM, 3DM2, CLI
Rapid RAID Recovery	All (Fast Rebuild/Shutdown)	3BM, 3DM2, CLI
StorSave Profile	Balanced	3BM, 3DM2, CLI

Table 5: Default Settings for Policies/Background Tasks

Policy	Default Value	Where to Change
Write Cache	Enabled	3BM, 3DM2, CLI
Read Cache	Intelligent	3BM, 3DM2, CLI

Background Task Settings

(For details, see “Scheduling Background Tasks” on page 163 and “Setting Background Task Rate” on page 162)

Verify Task Schedules	Basic - Friday 12:00 am Advanced - Daily, starting at 12:00 am and running for 24 hours	3DM2, 3BM, CLI 3DM2, CLI
Follow Verify Task Schedule	Enabled - Basic schedule	3DM2, 3BM, CLI
Rebuild/Migrate Task Schedules	Daily, starting at 12:00 am and running for 24 hours	3DM2, CLI
Follow Rebuild/Migrate Task Schedule	Ignore	3DM2, CLI
Self-test Task Schedules ^a	Daily, starting at 12:00 am and running for 24 hours	3DM2, CLI
Follow Self-test Task Schedule	Yes	3DM2, CLI

- a. Although the default Self-test Task Schedule is for 24 hours, self-test tasks are run only at the beginning of that time period and take just a few minutes. For more information about task schedules, see “Scheduling Background Tasks” on page 163.

4

3ware BIOS Manager (3BM) Introduction

This chapter describes the basics of using 3ware BIOS Manager (3BM), one of the tools that you can use to configure and maintain the units connected to your 3ware RAID controller. It is organized into the following topics:

- Starting 3BM
- Exiting the 3BM Configuration Utility
- Working in the 3BM Screens
- Adjusting BIOS Option Settings
- Displaying Information About the Controller and Related Devices
- Getting Help While Using 3BM

For information about doing particular tasks in 3BM, refer to the later sections in this guide.



Mac User Note: The 3ware BIOS Manager (3BM) is not supported for Mac OS. Mac OS users, skip this chapter.

Starting 3BM

You access 3BM during the start-up process for your computer.

- 1 Power up or reboot your system.
- 2 While the system is starting, watch for a screen similar to the 3ware BIOS screen below.

Figure 18. 3ware BIOS Screen

```

----Press <Alt-3> to access 3ware BIOS Manager ----
3ware ATA RAID Controller: 9750-4I
BIOS: BE9X X.XX.XX.XXX   Firmware: FE9X X.XX.XX.XXX
BBU Status: Not Present
Number of online units: 1, available drives: 0, hot spare: 0, offline units:0

Available drives:

          SATA - SAMSUNG  HD160JJ                149.04 GB  Phy  0

Exportable Units:G

3drive 64K RAID5      298.00 GB (Zygot3)  DEGRADED
          SATA - SAMSUNG  HD160JJ                149.04 GB  (Phy 3)
          SATA - SAMSUNG  HD160JJ                149.04 GB  (Phy 1)

```

- 3 Press **Alt-3** or **3** immediately to bring up the **3ware BIOS Manager (3BM)**.

Normally your 3ware configuration remains on-screen for just a few seconds. However, if a unit has degraded, the screen indicates the problem and remains on your screen longer.

- 4 If you plan to make changes to your configuration and need to backup data before continuing, press **ESC** and do so now. Otherwise, press any key to continue.

If 3BM detects a degraded array, a red message box appears, to alert you to the problem. For information about rebuilding a degraded array, see “About Degraded Units” on page 138.

- 5 If you have more than one 9750 controller in your system, a screen lists the available boards (see Figure 19).

Figure 19. 3ware Controller Board Selection Screen

```

3ware Controller Board Selection

Multiple 3ware controllers have been detected on your platform. To set up
a given controller, please select it from the following list.

Controller 0 <9750-4I> at slot: 4
Controller 1 <9750-81> at slot: 5

⬅ Previous/Next   Enter Go into highlighted board
                   Esc Cancel   F8 Done

```

If you have more than four boards, you see only four at first (only four can be processed at a time). After you exit from 3BM, you can access the BIOS again, to access the remaining boards.



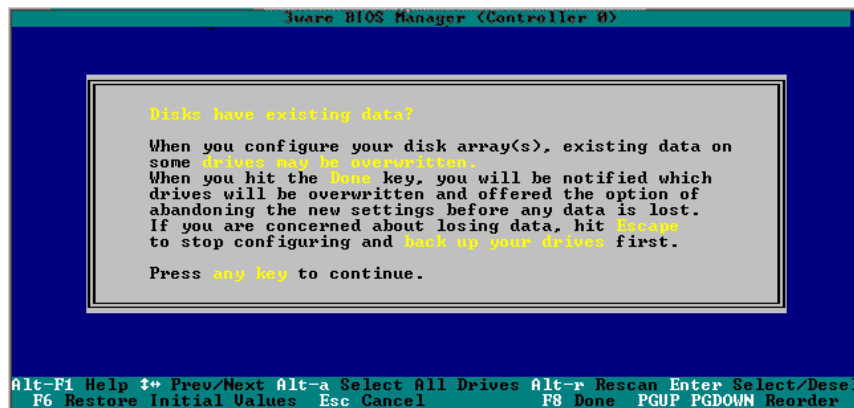
Note: If you have a combination of older 3ware controllers in your system, the older controllers are not listed on the selection screen shown in Figure 19. Instead, an additional BIOS summary appears, similar to Figure 18.

If you have two of the same series controllers that have different versions of the firmware installed, they will also appear in different BIOS summaries, and will launch different versions of 3BM.

Highlight the board with which you want to work and press **Enter**.

You see a screen similar to the following warning message, warning you that changing your disk array configuration might overwrite data on the disks.

Figure 20. Warning Message When you Start 3BM



6 Press any key to continue to the 3BM BIOS Manager screen.

Exiting the 3BM Configuration Utility

When you are ready to exit the 3BM configuration utility, you can save the configuration changes you have made, or to discard the changes.

To save your configuration modifications

1 Press the **F8** or **Esc** key.

A list of affected drives appears, a message asks you to confirm the configuration.

2 Type **y**.

The booting process resumes.

To exit without saving changes

- 1 Press **Esc**.
- 2 If you have unsaved changes, 3BM asks you whether you want to save the changes and exit, or exit without saving the changes.
 - If you want to exit without saving changes, type **N**.
 - If you change your mind and want to save the changes, type **Y**.

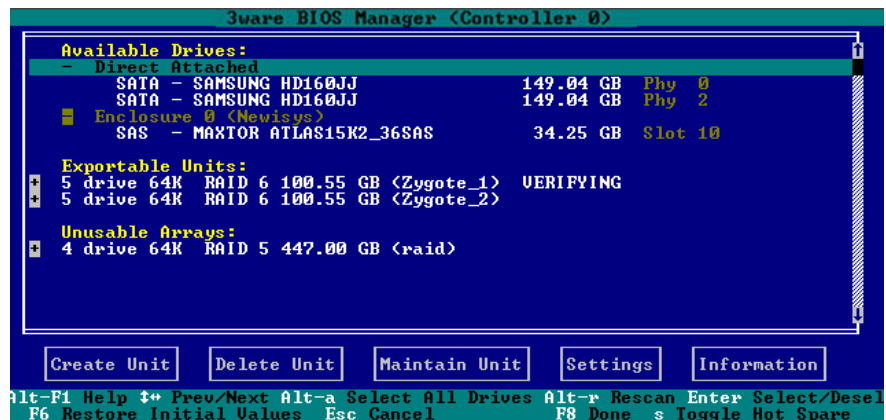


Exception: Changes made to controller policies are saved when you leave the Policy screen. Pressing **F8** is not required to save those changes. For more about changing policies, see “Setting the Auto-Rebuild Policy” on page 71.

Working in the 3BM Screens

The main **3BM** screen (Figure 21) shows the current configuration for the drives attached to your controller, and a list of any available drives. Unusable and incomplete drives are also shown.

Figure 21. 3BM Main Display



The following sections appear in the main 3BM screen:

- **Available Drives** lists any unconfigured drives that are not associated with an array, and hot spares. If this section does not appear, there are no available drives.
 - **Direct Attached** lists the drives directly attached to the controller.
 - **Enclosure** lists the drives attached through an enclosure.
- **Exportable Units** lists the existing units and the drives contained in each unit. These are the units that are available to the operating system when

you boot your computer. If this section does not appear, no units have been configured.

If you have more than one unit, the boot unit is the one at the top of the list. (You can change the order by highlighting a unit and pressing the **PgUp** or **PgDn** key.)

- **Unusable Arrays** lists any RAID configuration missing too many drives to construct the unit. For example, a RAID 5 unit with two or more drives missing appears in this list.
- **Incomplete Drives and Others** lists drives that are remaining from a unit with missing or failed drives and drives that are not usable.

When some of the drives are remaining from a unit, you can power down and add the missing drives to complete the unit. To use drives that are listed here in other units, you must first delete them. For more information, see “Deleting a Unit” on page 121.

If any of the sections are not shown, it means that there are no items of that type connected to the controller.

Table 6 lists how to move around and select information in the 3BM screens. When these commands are available in 3BM, they appear at the bottom of the 3BM screen.

Table 6: Working in 3BM

To do this	Use these keys
Move between units or drives in a list, between fields, and between buttons.	Up and Down Arrow Keys OR Left and Right Arrow Keys OR Tab and Shift+Tab
Select (or unselect) what is currently highlighted. A selection may be a drive in a list of drives, a button at the bottom of the screen, or a field in the middle of the screen. In lists, an asterisk appears to the left of selected drives or units.	Enter or the Spacebar
Show a drop-down list of available choices in a field.	Enter
Move between choices in a field list.	Up and Down Arrow Keys
Select all available drives.	Alt+A

Table 6: Working in 3BM (continued)

To do this	Use these keys
<p>In the list of units, expand a selected unit to see any subunits and drives in the unit, or contract it to see only the heading again.</p> <p>In the list of available drives these keys also work to show or hide the drives in each enclosure.</p>	<p>Shift+</p> <p>-</p>
<p>Highlight one of the primary buttons on the main screen:</p> <ul style="list-style-type: none"> • Create Unit • Delete Unit • Maintain Unit • Settings • Information 	<p>Alt+C</p> <p>Alt+D</p> <p>Alt+M</p> <p>Alt+S</p> <p>Alt+I</p>
<p>Specify (or unspecify) a drive as a hot spare.</p>	<p>S</p>
<p>Blink the LED associated with a drive.</p>	<p>F4, from the Drive Information screen (requires use of a supported enclosure)</p>
<p>Return to starting values for this session in the 3ware BIOS Manager.</p>	<p>F6</p> <p>Note: F6 cannot bring back previous policy settings; they are saved when you exit the Policy screen.</p>
<p>Rescan the controller and update the status of units and drives.</p>	<p>Alt+R</p>
<p>Return to the main 3ware BIOS Manager screen, from the Advanced Details screen.</p>	<p>Any key</p>
<p>Move a highlighted unit up or down in the list of exportable units.</p> <p>(The top-most unit will become the bootable unit, if you install the OS.)</p>	<p>Page Up</p> <p>Page Down</p> <p>(Available only when there are multiple units and a unit is highlighted.)</p>
<p>Show context sensitive help.</p>	<p>F1 or Alt-F1</p>
<p>If you have multiple 3ware controllers in your system, return to the board selection screen.</p>	<p>Esc</p>
<p>Exit the utility and save or abandon all changes.</p>	<p>Esc</p>

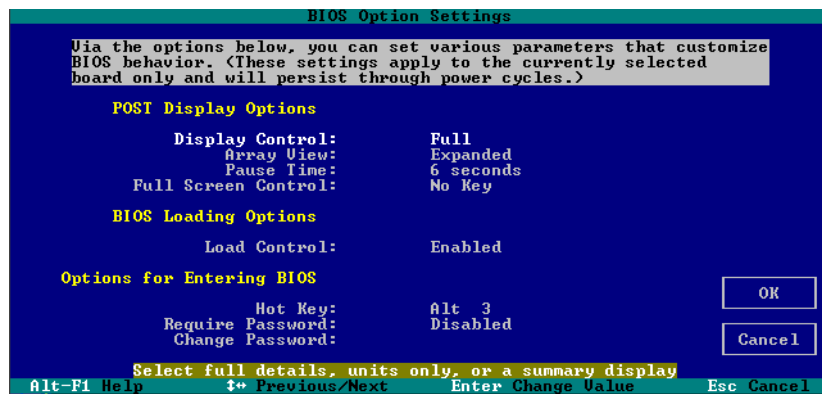
Table 6: Working in 3BM (continued)

To do this	Use these keys
Exit the utility and save all changes.	F8

Adjusting BIOS Option Settings

3BM includes a few settings that let you customize the behavior of the BIOS for the selected controller. You can access these settings by selecting **Settings >> BIOS Settings** from the 3BM BIOS Manager screen.

Figure 22. 3BM BIOS Option Settings



Power-On Self Test (POST) Display Options

Display Control. Specifies what level of detail to display on the start-up screen.

- **Full** displays all available information about the items attached to the controller, including available drives, hot spares, and configured units.
- **Unit Only** displays only configured units.
- **Summary** displays a one-sentence description of the items attached to the controller.

Array View. Specifies what level of information to show about configured units on the start-up screen.

- **Expanded** lists each unit and shows the specific drives that make up the unit.
- **Collapsed** lists only the configured units.

Pause Time. Sets the number of seconds that BIOS loading will pause to displaying the RAID configuration before continuing to boot the operating

system. You can set a pause time of up to 10 seconds. The default is 6 seconds.

Full Screen Control. When you have many drives attached to a controller and choose to display the Full level of detail, the information can extend beyond a screens' worth. The Full Screen Control setting lets you specify whether to wait for a keystroke when the screen is full, before displaying additional information. This option can be either **No Key** or **Wait Key**.

BIOS Loading Options

Load Control. This setting is enabled by default. It allows you to boot from RAID units or drives managed by the controller. If this setting is disabled, you will only be able to boot from hard drives or peripheral devices (such as CD-ROM or floppy) that are not managed by the controller. You might want to disable this setting if you have multiple controllers in a "headless" system with no monitor or keyboard.

Options for Entering BIOS

Hot Key. The default key combination for entering the BIOS is Alt-3 or 3. If you want, you can change this key combination to Ctrl-6 or 6.

Require Password. To control access to the BIOS setup program, you can enable a security password. If you enable the password function, you must then specify a password.

Change Password. This field is where you will enter a password if you have enabled the **Require Password** setting. This password controls access to the BIOS. If you forget your password, use the alternate password: *go3ware*. If that does not work you can reflash your controller to reset the password.



Note: During the boot process, you also can bypass loading of the BIOS for all controllers for one time only by pressing **Alt-B**. Bypass loading the BIOS is useful to temporarily boot from a non-3ware device without having to change the system's boot order.

Changing BIOS Settings

You can change the BIOS settings from the Bios Option Settings screen in 3BM.

To change the BIOS Settings

- 1 On the 3BM BIOS Manager screen, **Tab** to **Settings** and press **Enter**.
- 2 On the pop-up menu, select **BIOS** and press **Enter**.
The BIOS Option Settings screen appears.
- 3 **Tab** through the options and make the desired changes.
- 4 **Tab** to **OK** and press **Enter** to return to the main screen.

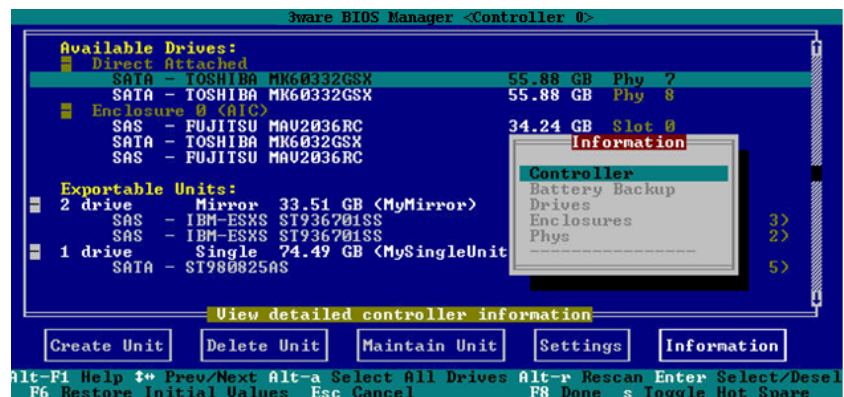
Displaying Information About the Controller and Related Devices

The 3BM Information menu gives you access to detailed information about the controller, BBU, drives, enclosures, and phys.

To see information about the controller or a related device

- 1 On the 3BM BIOS Manager screen, **Tab** to **Information** and press **Enter**.
A pop-up menu appears, listing the available information screens.
- 2 Select the item about which you want to see details and press **Enter**.

Figure 23. Controller Information Screen



A page appears showing details about selected item.

For more about how to use these pages, see the following topics:

- “Viewing Information About a Controller” on page 65
- “Viewing Battery Information” on page 176

- “Viewing a List of Drives” on page 135
- “Viewing a List of Enclosures” on page 180
- “Viewing Information About a Phy” on page 75

To return to the main screen

- Press **Enter**.

Getting Help While Using 3BM

Press **F1** or **Alt-F1** at any time. A description of the basic 3BM tasks appears. When you're finished using help, press **Esc** to close the help window.

5

3DM2 (3ware Disk Manager 2) Introduction



Note: 3DM2 includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>).

3ware Disk Manager 2 (3DM2) allows you to manage and view the status of your 3ware RAID controllers and associated drives.

3DM2 is a service under Windows, or a daemon under FreeBSD, Linux, OpenSolaris, Mac OS, and VMware, that runs in the background on the computer where you have installed your 3ware controller. When 3DM2 is running as a service or daemon, you can use your browser to access 3DM2 application pages, where you can view status information about the controller and RAID units, create RAID units, and perform other administrative and maintenance tasks locally or remotely.

Two levels of access to 3DM2 are provided: user and administrator. Users have view-only access, and can check the status of drives and units. Administrators can view and make changes, using 3DM2 to configure RAID units and designate hot spares, and to perform maintenance tasks on RAID units.

In this section, information is organized into the following topics:

- Browser Requirements for 3DM2
- Installing 3DM2
- Starting 3DM2 and Logging In
- Working with the 3DM2 Screens
- Setting Up 3DM2 Preferences

For details about the settings and fields on each of the 3DM2 screens, see “3DM2 Reference” on page 189.

For additional information about managing and maintaining 3ware controllers using 3DM2, see the remaining chapters in this guide.

Browser Requirements for 3DM2

3DM2 runs in most current web browsers. Tested and supported browsers (latest version available at time of software release) include:

- Internet Explorer
- Mozilla Firefox
- Safari

Additional requirements:

- JavaScript must be enabled.
- Cookies must be enabled.
- For best viewing, use a screen resolution of 1024 X 768 or greater, and set colors to 16 bit color or greater.

Installing 3DM2

You can install 3DM2 from the 3ware CD that came with your 3ware RAID controller. You also can download the current version from the website at <http://www.lsi.com/channel/ChannelDownloads>. Details about the installation are described in Appendix B, “Driver and Software Installation” on page 301.

You must install 3DM2 on the system in which the controller is installed. You do not have to install 3DM2 on a remote system in order to remotely manage the 3ware controller; you simply enter the correct URL into a browser on the remote system. You need to enable remote access first, however.

Starting 3DM2 and Logging In

Normally after installation, the 3DM2 process starts automatically when you start your system.

As a best practice, keep the 3DM2 process running on the system that contains your 3ware RAID controller. That way 3DM2 can send email alerts, and administrators can manage the controller remotely, if remote administration is enabled.

When 3DM2 is running in the background on your computer, you can access the 3DM2 web application through your browser to check status information and manage your 3ware RAID controller.



Note: If the 3DM2 process does not start automatically, you can start it manually, as described under “Managing the 3DM2 Daemon under FreeBSD, Linux, Mac OS, OpenSolaris, and VMware” on page 49, or “Starting the 3DM2 Process under Microsoft Windows” on page 50. You will know if the process is not running, because when you try to use the 3DM2 web application, you will get a page not found error.

If you want to check the status of a controller from a different computer, see “Viewing 3DM2 Remotely Using a Web Browser” on page 51.

Logging In to the 3DM2 Web Application

When the 3DM2 process is running in the background, you can log into the 3DM2 application pages using a browser.

Two levels of access are provided:

- *Users* can check the status of the controller, units, and attached drives.
- *Administrators* can check status, configure, and maintain the units and drives on the 3ware controller.



Note: Administrator and User status in 3DM2 is not related to Administrator/User settings in the operating system.

To log in to the 3DM2 web application, for FreeBSD, Linux, OpenSolaris, and Windows

- 1 Open your browser and enter the URL for your system.

The default URL is `https://localhost:888/`

If you are using Fedora Core 10, use `https://127.0.0.1:888.`

(Fedora Core 10 made changes that affected 3DM2.

`https://localhost:888` can no longer be used in a web browser to access 3DM2. Other Linux distributions may also be affected.)

If remote access is enabled, you also can replace “localhost” with the IP address of the computer that contains the 3ware controller. For example:

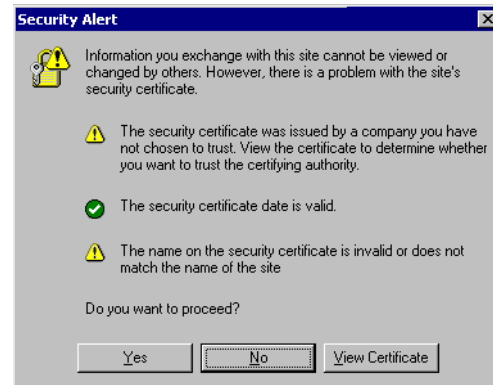
`https://<IP address>:888/.`



Note: If you receive a Page Not Found message, make sure that you entered the URL correctly by specifying `https`, not `http`. If you did, 3DM2 might not be running in the background. You can start it manually. See, “Managing the 3DM2 Daemon under FreeBSD, Linux, Mac OS, OpenSolaris, and VMware” on page 49 or “Starting the 3DM2 Process under Microsoft Windows” on page 50.

- 2 The first time you start 3DM2, your browser might prompt you for a security certificate. If it does, accept the certificate.

For example, when using Windows Internet Explorer, you might see the message shown below. In this example, click **View Certificate** and accept the certificate so that you do not see the security message each time you start 3DM2.

Figure 24. Security Certificate Message from Browser

(You also can click **Yes** or **Continue**, in which case you will see this message the next time you start 3DM2.)

If you are using a different browser, the steps to accept the certificate are different.

- 3 When the 3DM2 logon screen appears, select whether you are a **User** or **Administrator**.
- 4 Enter your password and click **Login**.

If you are logging in for the first time after installing 3DM2, the default password for both User and Administrator is *3ware*.



Note: If you forget the passwords, uninstalling and reinstalling 3DM2 resets the passwords to *3ware*.

To log in to the 3DM2 web application, for Mac OS

- 1 You can start the 3DM2 web application in one of the following ways:
 - In the Finder, choose **Applications >> LSI**, and then double-click **Connect to 3DM2.webarchive**.

Your browser will open and go to the URL for 3DM2.

OR

- Open your browser and enter the URL for your system.

The default URL is `https://localhost:888/`

If remote access is enabled, you can also replace “localhost” with the Hostname or IP address of the computer that contains the 3ware controller. For example: `https://<IP address>:888/`

- 2 The first time you start 3DM2, your browser might prompt you for a security certificate. If it does, accept the certificate.

If you are using Mac OS, you might see the message shown below. In this example, click **Show Certificate** and accept the certificate so that you do not see the security message each time you start 3DM2.

Figure 25. Security Certificate Message from Safari Browser



(You also can click **Yes** or **Continue**, in which case you will see this message the next time you start 3DM2.)

- 3 When the 3DM2 logon screen appears, select whether you are a **User** or **Administrator**.
- 4 Enter your password and click **Login**.

If you are logging in for the first time after installing 3DM2, the default password for both User and Administrator is `3ware`.



Note: If you forget the passwords, uninstalling and reinstalling 3DM2 resets the passwords to `3ware`.

To log in to the 3DM2 web application, for VMware

For VMware you must login remotely, since there is no GUI installed on the host system. Use the IP address of the computer that contains the 3ware controller. For example: `https://<IP address>:888/`

Managing the 3DM2 Daemon under FreeBSD, Linux, Mac OS, OpenSolaris, and VMware

3DM2 should start automatically after installation and upon bootup. If it does not, use the steps below to manage it.

To manage the 3DM2 daemon manually for FreeBSD

1 Login as root on the machine on which 3DM2 is installed.

2 Type:

```
/etc/rc.d/3dm2 start|stop|restart
```

To manage the 3DM2 daemon manually for Linux

1 Login as root on the machine on which 3DM2 is installed.

2 Type:

```
/etc/rc.d/init.d/tdm2 start|stop|restart
```

or (some Linux versions use this directory instead):

```
/etc/rc.d/tdm2 start|stop|restart
```

To manage the 3DM2 daemon manually for Mac OS

You can restart 3DM2 by restarting your Mac. However, you can also manage the 3DM2 Daemon manually by using the steps below.

1 Check to see if the 3DM2 process is already running.

Open a Terminal window and type:

```
ps -ax | grep 3dm2 | grep -v grep
```

If 3DM2 is running, you will see it included on the output line that displays.

2 Stop the 3DM2 process so you can restart the process

In a Terminal window and type:

```
sudo killall 3dm2
```

When prompted, enter your administrator password.

Wait for one minute or so before verifying that the process has been terminated. (It can take a couple of minutes for the process to be stopped)

Verify that the process has been terminated by typing:

```
ps -ax | grep 3dm2 | grep -v grep
```

The output line should not include 3DM2

If the process is still running, contact LSI/3ware Technical Support for assistance.

- 3 Start the 3DM2 process manually

Open terminal window and type:

```
sudo /usr/sbin/3dm2
```

Enter your administrator password, when prompted for it.

The 3DM2 process starts

Open your browser and enter the URL for your system. The default URL is `http://localhost:888/`

You can also replace “localhost” with the IP address of the computer that contains the 3ware controller. For example:

```
http://<IP address>888/
```

To manage the 3DM2 daemon manually for OpenSolaris

Consult OpenSolaris documentation for more information. OpenSolaris System Administrator Collection: <http://docs.sun.com/app/docs/coll/47.24>

To manage the 3DM2 daemon manually for VMware

- 1 Login as root on the machine on which 3DM2 is installed.

- 2 Type:

```
/etc/init.d/tdm2 start|stop|restart
```

Starting the 3DM2 Process under Microsoft Windows

3DM2 should start automatically after installation and upon bootup. If it does not, use the steps below to start it.

To start the 3DM2 process manually

- 1 On the system on which 3DM2 is installed, login as Administrator.
- 2 Open **Control Panel >> Administrative Tools >> Services >> 3DM2** and select the **Start/Play** icon.

Viewing 3DM2 Remotely Using a Web Browser

When remote administration is enabled on the 3DM2 Settings page, you can use 3DM2 to check status and administer your 3ware RAID controller from a browser on any computer, over an internet connection.

You do not need to install the 3DM2 software on the remote computer.

To connect to 3DM2 through your web browser

In the address line of your browser, the IP address of the computer that contains the 3ware RAID controller. For example: `https://<IP address>:888/`

If you do not know the URL or IP address for the system, you can contact your network administrator or:

- From a FreeBSD command prompt, type `ipconfig`.
- From a Linux command prompt, type `ifconfig`.
- From a Mac OS Terminal window, type `ifconfig`.
- From OpenSolaris consult OpenSolaris documentation for more information. OpenSolaris System Administrator Collection: <http://docs.sun.com/app/docs/coll/47.24>
- From a Windows command prompt, type `ipconfig`.
- From VMware consult your VMware user guide for details



Note: When using 3DM2 to access a remote system, and auto logout is enabled, the time on the local system must match the time on the file server. If the time varies by more than 30 minutes, it will not be possible to remotely monitor the system (you will not be able to log in). If you are in a different time zone, you must first change the time of the local system to match the time of the remote system.

Working with the 3DM2 Screens

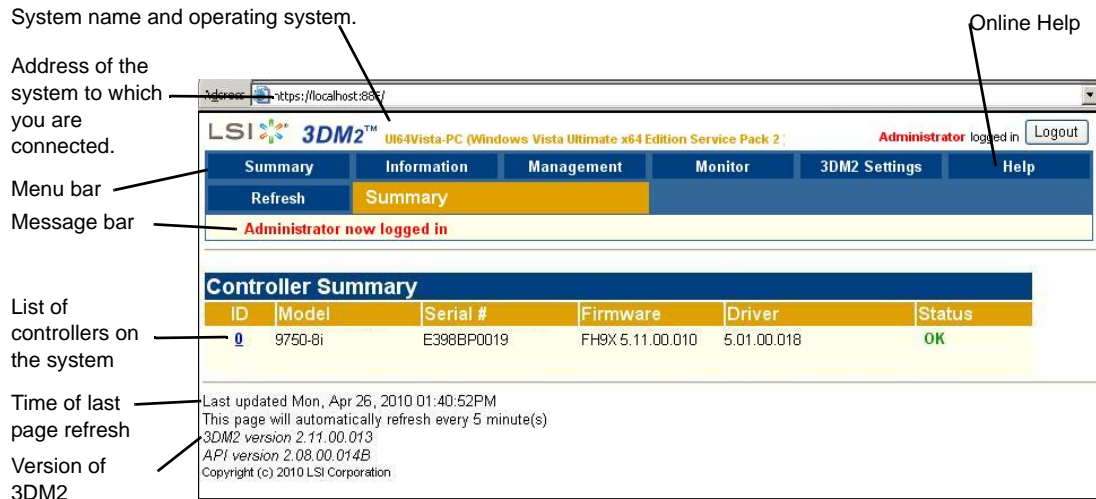
3DM2's features are organized on a series of pages you view in your browser.

After you log in to 3DM2, the Summary page shows a list of controllers installed in the computer at the URL you specified.



Note: If you expect to see a controller that is not listed, it might not be compatible with the driver that is loaded; a firmware flash upgrade might be required.

Figure 26. 3DM2 Main Screen



The menu bar across the top of the screen gives you access to other pages in 3DM2. You can move between pages by using the menu bar, or by clicking a link on the page.

The main area of the page provides summary or detail information about your 3ware RAID controller and the resources connected to it.

As you work in 3DM2, the Messages area just below the menu bar shows information about the results of commands that you have selected.

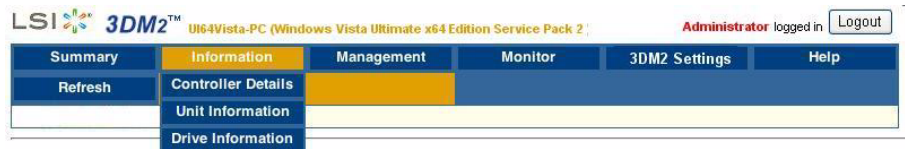


Tip: If you have a question about something that you see on the screen, just click the Help button in the menu bar.

3DM2 Menus

The 3DM2 menu bar groups access to a number of 3DM2 pages on menus, and provides direct link access to others.

Figure 27. 3DM2 Menu Bar



Status information is available from the **Information menu**. You can view:

- Controller Details
- Unit Information

- Drive Information

The **Management menu** gives you access to the following tasks for managing controller-level settings and for maintaining individual units.

- Controller Settings
 - Background Task
 - Unit Policies
 - Unit Names
 - Other Controller Settings
- Scheduling
 - Rebuild Schedule
 - Verify Schedule
 - Self-Test Schedule
- Maintenance
 - Rescan
 - Unit Maintenance
 - Available Drives

The **Monitor menu** gives you access to the following pages: Alarms page, Battery Backup page, and Enclosure Summary page.

- The Alarms page:
 - List of AENs
 - Severity of the event
 - Exact date and time it occurred
- The Battery Backup page:
 - Status of a BBU
 - Battery voltage
 - Battery temperature
 - Battery installation date
 - Test battery capacity
- The Enclosure Summary page:
 - Provides a list of enclosures connected to your controller
 - Provides basic information about any enclosures attached to your system.

The **3DM2 Settings** page lets you set preferences, including email notification for alarms, passwords, page refresh frequency, whether remote access is permitted, the communication port which 3DM2 will use for listening, and whether command logging is enabled.

Help lets you access information about using 3DM2. The Help is context-sensitive, so you first see information about the page you now have in view. A Table of Contents and Index are available to help you find other information.

Viewing Information About Different Controllers

If you have more than one 3ware RAID controller in the system, you select the one that you want to see details about from the drop-down list at the right of the menu bar.

This drop-down is available on all pages that provide controller-specific features.

Figure 28. 3DM2 Controller Selection Drop-down



Note: Throughout these instructions, the term *current controller* is used to refer to the controller that is currently selected in this drop-down list.



Note: The fields and columns in 3DM2 vary for different models of 3ware RAID controllers. If you have multiple controllers of different models, you might notice some differences when switching between them in 3DM2. For example, when showing information about the 9750 or 9690SA controllers, 3DM2 shows “VPort” (for virtual port) on some pages while for earlier controllers the label is “port.”

Refreshing the Screen

You can refresh the data on the screen at any time by clicking **Refresh Page** in the menu bar. Refreshing the data causes 3DM2 to update the information shown with current information from the controller and associated drives.

Automatic refreshes also can be set. For details, see “Setting the Frequency of Page Refreshes” on page 62.



Note: If you click Refresh on the browser window instead of on the 3DM2 menu bar, you are taken back to the Summary page.

Description of 3DM2 Pages

The following table describes 3DM2 pages, including their uses. Details about each page and the fields and features on it are provided in Chapter 11, “3DM2 Reference”. The page names in the table provide links to details about that page.

In addition, the step-by-step instructions provided in the chapters on configuring and maintaining your RAID controller and units explain how to do particular tasks in 3DM2.

Table 7: List of 3DM2 Pages

3DM2 Page	Description
Controller Summary page	Provides basic information about each 3ware RAID controller in your system. To see this page, click Summary in the menu bar.
Controller Details page	Provides detailed information about the current controller. To see this page, select Information >> Controller Details from the menu bar.
Unit Information page	Shows a list of the units on the current controller and provides summary information about each unit. To see this page, select Information >> Unit Information from the menu bar or click an ID number on the Controller Summary.
Unit Details page	Shows details about a particular unit. To see this page, click an ID number on the Unit Information page.
Drive Information page	Shows a list of drives on the current controller and provides summary information about each drive. To see this page, select Information >> Drive Information from the menu bar.
Drive Details window	Shows the SMART data for a specific drive, and shows additional detail information for the drive. To see this page, click the Port # for a drive on the Drive Information page.

Table 7: List of 3DM2 Pages

3DM2 Page	Description
Controller Phy Summary page	<p>Shows the properties of controller phys for 9750 RAID controllers.</p> <p>There are two ways to access this page. If you have a direct-attached drive you can access this page from the Information >> Drive Information page by clicking the phy ID for the drive. If all drives are connected via expanders, select Management >> Controller Settings page. Under Other Controller Settings click the # link for Number of Controller Phys.</p>
Controller Settings page	<p>Lets you view settings that affect the units on the current controller and change some of those settings.</p> <p>Controller-level settings that can be changed include background task rate, Auto-Rebuild, Auto-Carving, and Carve Size. Some additional policies are shown that can only be changed only in the BIOS or the CLI.</p> <p>Unit-level settings include specifying the StorSave Profile and enabling or disabling the Write Cache, Read Cache, Auto-Verify, Overwrite ECC, Queuing, and Rapid RAID Recovery.</p> <p>To see this page, select Management >> Controller Settings from the menu bar.</p>
Scheduling page	<p>Lets you view and change the schedule for tasks that affect all units on the current controller.</p> <p>To see this page, select Management >> Scheduling from the menu bar.</p>
Maintenance page	<p>Lets you configure new units and make changes to existing units.</p> <p>To view this page, select Management >> Maintenance from the menu bar.</p>
Alarms page	<p>Shows a list of alarms, including the specific alarm message, and the exact date and time it occurred.</p> <p>To view this page, choose Monitor >> Alarms on the menu bar.</p>
Battery Backup page	<p>Shows the status of a Battery Backup Unit (BBU), if one is installed, and allows you to test the battery.</p> <p>To view this page, select Monitor >> Battery Backup on the menu bar.</p>
Enclosure Summary page	<p>Lists the installed and supported enclosures attached to your 3ware controller.</p> <p>To view this page, select Monitor >> Enclosure Support on the menu bar.</p>

Table 7: List of 3DM2 Pages

3DM2 Page	Description
Enclosure Details page	Shows details about a particular enclosure, including status information. You also can use this page to blink the LED for a particular drive. To view this page, click the ID number of the Enclosure on the Enclosure Summary page.
3DM2 Settings page	Lets you set preferences, including email notification for alarms, passwords, page refresh frequency, whether remote access is permitted, whether command logging is enabled, and the incoming port which 3DM2 will use for listening. To view this page, click 3DM2 Settings on the menu bar.

Setting Up 3DM2 Preferences

The 3DM2 Settings page lets you define preference settings that affect the overall operation of 3DM2.

On the 3DM2 Settings page you can perform the following tasks:

- Setting and Changing 3DM2 Passwords
- Managing E-mail Event Notification
- Enabling and Disabling Remote Access
- Setting the Listening Port #
- Setting the Frequency of Page Refreshes
- Controlling Command Logging in 3DM2

Setting and Changing 3DM2 Passwords

3DM2 provides different access levels for users and administrators.

The Administrator access level allows the user to fully configure 3DM2. The User access level allows the user to view pages within 3DM2. These passwords work independently of each other.

The default password for both the User and Administrator is “3ware”.

Passwords are case sensitive.

You can only change passwords only if you are logged in as Administrator. If you change the Administrator password, you are automatically logged out, and must log back in with the new password.

To set or change the password

- 1 Click **3DM2 Settings** on the 3DM2 menu bar.
- 2 On the 3DM2 Settings page, in the **Password** section, select the type of password that you want to change: **User** or **Administrator**.
- 3 Type the current password in the **Current Password** field.
If you are changing the password for the first time, the factory-set default password is `3ware`.
- 4 Enter the new password in the **New Password** field and again in the **Confirm New Password** field.
- 5 Click the **Change Password** button to enact the change.



Note: If you forget your password, you can uninstall 3DM2 and then reinstall it. This will reset the password to the default password, `3ware`.

Managing E-mail Event Notification

3DM2 can notify you when the 3ware RAID controller requires attention, such as when a disk unit becomes degraded and is no longer fault tolerant.

E-mail event notification can occur only while 3DM2 is running; therefore, keep the 3DM2 process running in the background on the system that contains the 3ware RAID controller.

When events occur, notification can be e-mailed to one or more recipients. You can specify the type of events for which notifications are sent by selecting the severity:

- **Information** sends e-mails for all events.
- **Warning** sends e-mail for events with severity of Warning and Error.
- **Error** sends e-mail for events with severity of Error only.

Events are listed on the 3DM2 **Alarms** page.

You can set up event notification when you install 3DM2. You also can change the event notification on the 3DM2 Settings page.



Note: If you are using VMware, you will need to configure the VMware firewall to allow outgoing email, as all ports are blocked by default. See “Configuring the VMware Firewall to Allow Email Notification” on page 61

To set up event notification

- 1 Click **3DM2 Settings** on the menu bar.

- 2 In the **E-mail Notification** section of the 3DM2 Settings page, enter or change the settings you want.
 - Enable or Disable all notifications.
 - Set the severity level of events for which e-mail notifications are sent.
 - Specify the email address of the sender. This address appears in the “From” field of the e-mail.
 - Enter the e-mail address(es) to which notifications are sent. (Separate multiple addresses with a comma (,) a semicolon (;), or a space ().
 - Enter the SMTP server name or IP of the mail server for the computer where the 3ware controller is installed.
 - If your email server requires authentication, enter the Mail Server Login and Password.
 - If your email server requires or supports encrypted email, select **Yes** in the field **Mail Server Port Uses SSL**.

Tip: If you are not sure whether any part of the set up applies to you, try enabling it, and then use the **Send Test Message** feature to try out the configuration setting. If the configuration is not correct, an error message appears at the top of the page. If you do receive an error, disable the setting, and try the test again.

You also might want to refer to KnowledgeBase article # 15538, at <http://kb.lsi.com>. This article explains how to use an gmail account as an alternate method to get your email notification working.

- 3 Click **Save E-mail Settings**.

To send a test message

You can send a test message to make sure that you have entered the e-mail notification settings correctly.

- Click **Send Test Message**.

Configuring the VMware Firewall to Allow Email Notification

You can select an option in 3DM2 to allow email notification of alarms and other events reported by the 3ware RAID controller.

However, in order to receive email notification when using VMware, you will need to configure the VMware firewall to allow outgoing email, as all ports are blocked by default.

To configure the VMware firewall to allow email notification

- 1 Login to the server as root.
- 2 Configure the firewall to allow outgoing email.


```
esxcfg-firewall -o 25,tcp,out,smtp
esxcfg-firewall -o 587,tcp,out,smtp
```

Enabling and Disabling Remote Access

When remote access is enabled, you can connect to 3DM2 over the internet or an intranet, to check status or to administer the controller and associated drives. (See “Viewing 3DM2 Remotely Using a Web Browser” on page 51.)

If remote access is disabled and you attempt to connect to 3DM2 remotely, the following error message appears: “Remote Access to 3DM2 has been disabled. Please connect using the local machine by entering “localhost” in the URL bar.”

You can enable or disable remote access on the 3DM2 Settings page.



The VMware version of 3DM2 is installed with remote 3DM2 access enabled by default, since VMware has no GUI to let you run it locally. If you disable remote access, you will need to reinstall 3DM2 in order to be able to connect to it.

To enable or disable remote access

- 1 Click **3DM2 Settings** on the menu bar.
- 2 In the **Remote Access** section of the 3DM2 Settings page, select either **Enabled** or **Disabled** in the **Allow Remote Connections** field.

The page refreshes, and a message at the top of the screen confirms that remote access has been enabled or disabled.

Setting the Listening Port

You can set the port that 3DM2 uses to listen for incoming messages. If you are not sure which port would be the best to use, leave this set to the default port of 888.

To set the listening port

- 1 Click **3DM2 Settings** on the menu bar.
- 2 In the **Listening Port #** section of the 3DM2 Settings page, enter the port number in the **Listening Port** field.
- 3 Click **Change Port**.

The page refreshes, and a message at the top of the screen confirms that the listening port has been changed.

Setting the Frequency of Page Refreshes

Because the status of the drives attached to your 3ware RAID controller can change while you are viewing information about them in 3DM2, make sure that you refresh the page information regularly. That way you know that the information you see in 3DM2 is current.

You can manually refresh the information on a page by clicking **Refresh Page** in the menu bar. But you also can set 3DM2 to refresh the information on a regular basis.

To set the frequency of page refreshes

- 1 Click **3DM2 Settings** on the menu bar.
- 2 In the **Page Refresh** section of the 3DM2 Settings page, select how often you want the page to be refreshed in the **Minutes Between Refresh** field.



Note: If you do not want 3DM2 to refresh the screen automatically, select **Never** in the **Minutes Between Refresh** field. You can then refresh manually by clicking Refresh on your web browser.

Controlling Command Logging in 3DM2

Command logging provides the ability to log each command that makes a change to the controller configuration in a log file (tw_mgmt.log). This can be useful for trouble-shooting.

You can enable and disable command logging from the **3DM2 Settings page**.

Enable or Disable 3DM2 Command Logging

- 1 Click **3DM2 Settings** on the 3DM2 menu bar.
- 2 In the **Server Configuration** section of the 3DM2 Settings page, select either **Enabled** or **Disabled** in the **Command Logging** field.

Figure 29. Command Logging setting on 3DM2 Settings page

The screenshot shows the 3DM2 Settings page with the following sections and fields:

- Navigation:** Summary, Information, Management, Monitor, 3DM2 Settings (selected), Help.
- E-mail notification:**
 - Send E-mail: Enabled Disabled
 - Notify on: INFO (dropdown)
 - Sender: someone@domain.com
 - Recipient(s): someone@domain.com
 - Mail Server (name or IP): mailserver.domain.com
 - Mail Server Login: mailserverusername
 - Mail Server Password: [masked]
 - Mail Server Port uses SSL: Yes No
 - Buttons: Save E-mail Settings, Send Test Message
- Password:**
 - Change Password For: User (dropdown)
 - Current Password: [input]
 - New Password: [input]
 - Confirm New Password: [input]
 - Button: Change Password
- Page Refresh:**
 - Minutes Between Refresh: 5 (dropdown)
- HTTP Settings:**
 - Listening Port: 888 (input)
 - Button: Change Port
- Server Configuration:**
 - Allow Remote Access: Enabled Disabled
 - Command Logging:** Enabled Disabled (highlighted with a red box)



Note: The command logging control in 3DM2 only determines whether or not commands are logged from the 3DM2 interface. Command logging is also available for configuration changes made through the CLI. However, control of whether CLI command logging is enabled or disabled is handled separately. Changing the setting within 3DM2 does not affect command logging from CLI.

For more information, see the *3ware SATA+SAS RAID Controller Card CLI Guide, Version 10.2*.

Locating the Command Log File (tw_mgmt.log)

Under FreeBSD, Linux, Mac OS, OpenSolaris, and VMware tw_mgmt.log is in the /var/log directory. For Windows 7, Windows Vista, and Windows Server 2008, tw_mgmt.log is in \ProgramData\3ware directory. (Note that ProgramData is a hidden folder by default.)

For earlier versions of Windows, tw_mgmt.log is in
\Documents and Settings\All Users\Application Data\3ware
directory

Configuring Your Controller

This chapter describes how to view details about the controller, check its status, and change configuration settings that affect the controller and all of the drives connected to it. This chapter is organized into the following sections:

- Viewing Information About a Controller
- About Controller Policies
- Viewing Controller Policies
- Setting the Auto-Rebuild Policy
- Using Auto-Carving for Multi LUN Support
- Setting the Size of Volumes Created with Auto-Carving
- Enabling and Setting Up Staggered Spin-up
- Viewing Information About a Phy
- Changing the Phy Link Speed



Note: Background task rate is also set for all units on a controller. For information about setting the task rate, see “Setting Background Task Rate” on page 162.



Mac User Note: The 3ware BIOS Manager (3BM) is not supported for Mac OS. Mac users should disregard any 3BM instructions throughout this chapter.

Viewing Information About a Controller

You can check the controller model, serial number, firmware and driver versions, and the status of the 3ware RAID controller in your computer.

If you have more than one controller in your system, you can easily view information about each one using 3DM2. If you are working at the BIOS level in 3BM, you access each controller separately.

To see details about a controller in 3DM2

- 1 Start 3DM2 and log in as an administrator.

The 3DM2 Unit Information page appears, listing all of the 3ware controllers installed in your system.

The right-most column of the list shows the status of each controller.

Figure 30. Controller Summary Page

Controller Summary					
ID	Model	Serial #	Firmware	Driver	Status
1	9750-8i	E398BP0019	FH9X 5.11.00.010	5.01.00.018	OK

Last updated Mon, Apr 26, 2010 01:40:52PM
 This page will automatically refresh every 5 minute(s)
 3DM2 version 2.11.00.013
 API version 2.08.00.014B
 Copyright (c) 2010 LSI Corporation



Tip: If you are managing controllers remotely, the list of controllers is for the machine with the IP or URL you entered in the browser address bar.

- 2 To see more details about a particular controller, click the ID link for that controller to display the Unit Information page.

To see information about a different controller in the 3DM2 pages

If you have more than one controller in the system, you can switch between them by selecting the one you want from the **Select Controller** drop-down list at the right of the menu bar. This drop-down is available on all pages that provide controller-specific features.

When you select a different controller from this list, the page in view changes, to reflect the details for the controller you selected.



Tip: If you are managing controllers remotely, the list of controllers is for the machine with the IP or URL you entered in the browser address bar.



Note: Throughout this documentation, the term *current controller* is used to refer to the controller currently selected in this drop-down list.

To see information about a controller in 3BM (BIOS)

- 1 Power up or reboot your system.
- 2 While the system is starting, watch for a screen showing information about the controller and units you want to work with.

When you have more than one controller installed, information about each one will be shown, sequentially.

- 3 Press **Alt-3** or **3** to bring up the **3ware BIOS Manager (3BM)**.

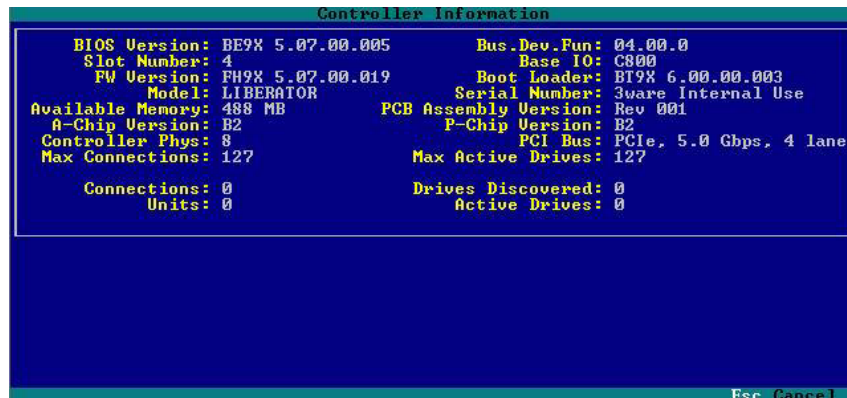


Note: If you accidentally bypass display of the controller you want to work with, press **Ctrl-Alt-Del** to restart your computer and try again

- 4 **Tab** to **Information** and press **Enter**.
- 5 On the pop-up menu, select **Controller** and press **Enter**.

The Controller Information page displays.

Figure 31. Controller Information page



About Controller Policies

The following policies affect all units and drives on a controller and can be adjusted as appropriate for your equipment. Controller policies are shown at the bottom of the Controller Settings page in 3DM2 (Figure 32) and on the Policy Control screen in 3BM (Figure 33).

- **Auto-Rebuild.** Determines whether the Auto-Rebuild policy is enabled or disabled. When disabled, degraded units can only be rebuilt with designated spares. When enabled, the controller firmware will automatically attempt to rebuild a degraded unit if there is no spare, using either an available drive or a failed drive.

- **Auto-Carving.** Determines whether the auto-carving policy is enabled or disabled. When it is enabled, when a new unit is created, any unit larger than a specified size (known as the *carve size*) is broken into multiple volumes that can be addressed by the operating system as separate volumes. The default carve size is 2 TB.

This auto-carving feature is sometimes referred to as multi-LUN, where each volume that is created is referred to as a “LUN.”

- **Carve Size.** (Referred to as *Carving Factor* in 3BM) Sets the size for dividing up units into volumes when Auto-Carving is enabled and a unit is created. This setting can be between 1024 GB and 32768 GB. Changing this setting has no effect on existing units.
- **Staggered spin-up.** Spin-up allows drives to be powered-up into the Standby power management state to minimize in-rush current at power-up and to allow the controller to sequence the spin-up of drives. Compatible drives are sent a spin up command based on the settings specified with the policies **Number of drives per spin-up** and **Delay between spin-up settings**. These policies can only be set using 3BM or the CLI.

Note: This policy does not apply to drives attached to an expander.

- **Number of drives per spin-up.** Number of drives that will spin up at the same time when the controller is powered up, if staggered spin-up is enabled. From 1 to x, depending on the number of ports on the controller.
- **Delay between spin-up.** The delay time (in seconds) between drive groups that spin up at one time on this particular controller, if staggered spin-up is enabled.
- **Delay before spin-up.** (3BM only) The delay time (in seconds) before the first set of drives on this particular controller will start to spin-up.



It is possible to enable or disable automatic detection of drives on the controller's ports for staggered spinup during hot swapping of drives. This feature is only available in the CLI using the **autodetect=on|off** command. For more information, refer to **/cx set autodetect=on|off disk=<p>-p>|all** in the *3ware SATA+SAS RAID Controller Card CLI Guide, Version 10.2*.

- **Export unconfigured disks (JBOD).** This setting is not applicable for 9750 controllers.
- **Staggered method.** Indicates whether the type of staggered spin-up is ATA-6 or SATA OOB (Out Of Band). By default, when Staggered Spin-up is enabled, the OOB scheme is used. If your drives support the SATA ATA-6 method, select that method in 3BM. There is no electronic method for the controller to know if a drive supports this method, so it must be set manually. For staggering to work properly, the drives must support the

selected method. This policy does not apply to drives that are attached to an expander. This policy can only be set and only shows in 3BM.

- **Auto-Verify Preferred Date and Time.** Sets the default date and time for auto-verify to run, when the Verify Schedule follows the weekly "Basic" schedule and Auto-Verify is enabled for specific units. Note that in 3DM2, the Basic and Advanced Auto-Verify schedule is set on the **Schedule** page. Enabling or Disabling Auto-Verify is a Unit Policy and is set on the **Create Disk Array** screen in 3BM and the **Controller Settings** page in 3DM2.

Some additional policies can be set at the unit level. For more information, see "Setting Unit Policies" on page 100.

Viewing Controller Policies

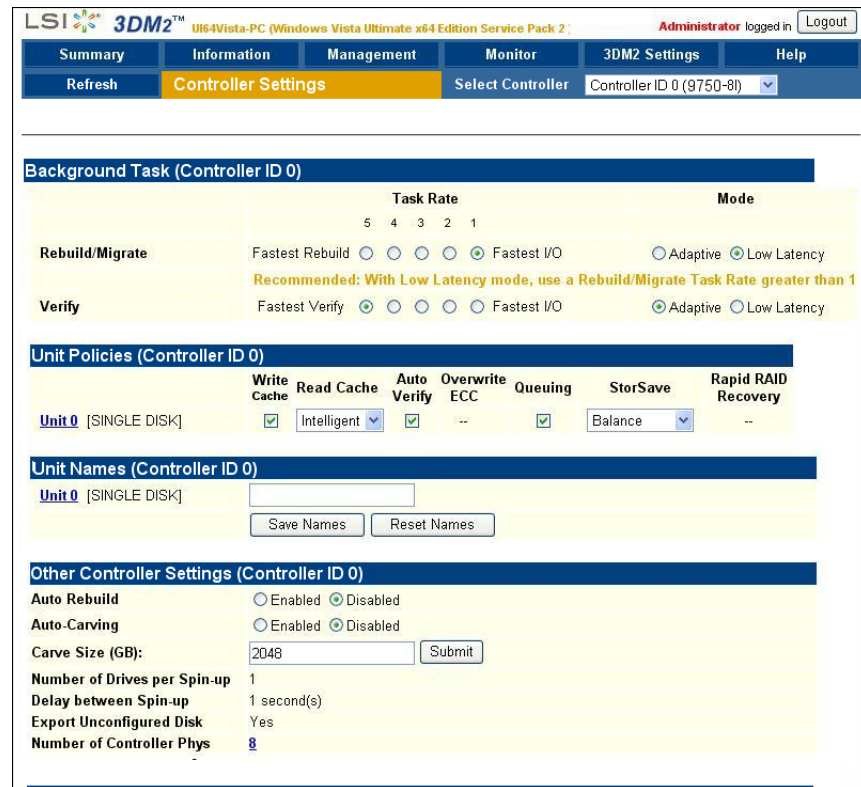
You can view the current state of controller policies in 3DM2, in the **Other Controller Settings** section at the bottom of the Controller Settings page (See Figure 32). Only the Auto-Rebuild, Auto-Carving, and Carve Size policies can be changed on this page. The other policies can be changed in 3BM or through the CLI. For a summary of the initial default settings, see Table 5, "Default Settings for Policies/Background Tasks," on page 32.

To view controller policies in 3DM2

- Choose **Management >> Controller Settings** from the menu bar.

The policies that appear under Other Controller Settings vary, depending on the controller model you are using.

Figure 32. 3DM2 Controller Settings Page

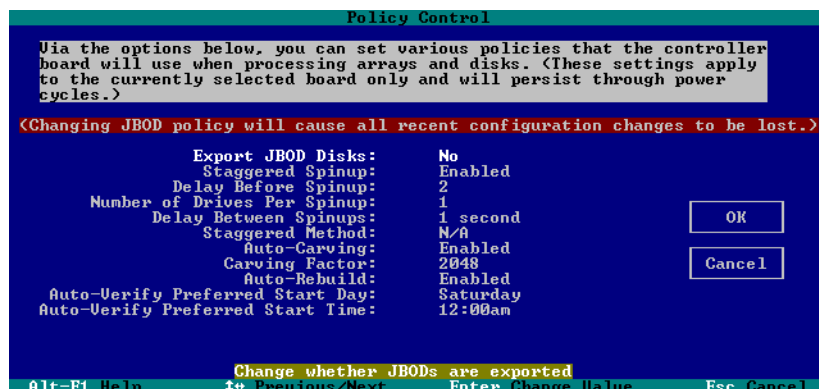


To view controller polices in 3BM

You can also view and change these controller polices in 3BM, as shown in Figure 33.

- 1 On the main 3BM screen, **Tab** to **Settings** and press **Enter**.
- 2 On the pop-up menu, select **Controller Policies** and press **Enter**.
The Policy Control screen displays.

Figure 33. 3BM Policy Control Screen



Setting the Auto-Rebuild Policy

The Auto-Rebuild policy determines how the controller firmware will attempt to rebuild degraded units.

When Auto-Rebuild is disabled, only spares will be automatically used to rebuild degraded units. When Auto-Rebuild is enabled, the firmware will select drives to use for automatically rebuilding a degraded unit using the following priority order.

- Smallest usable spare.
- Smallest usable unconfigured (available) drive.
- Smallest usable failed drive.

Enabling Auto-Rebuild allows you to add a drive to the controller and have it be available for a rebuild, without having to specify it as a spare.

With Auto-Rebuild enabled, if you accidentally disconnect a drive (causing the controller to see it as a failed drive) and then reconnect it, the controller will automatically try to use it again.

You can enable or disable the Auto-Rebuild policy through 3DM2 or 3BM.

To enable Auto-Rebuild through 3DM2

- 1 Choose **Management >> Controller Settings** from the menu bar in 3DM2.
- 2 In the Other Controller Settings section at the bottom of the screen, select the **Enabled** option for **Auto-Rebuild**.

The page refreshes, and a message at the top confirms the change you have made.

To enable Auto-Rebuild through 3BM

- 1 On the main 3BM screen, **Tab** to **Settings** and press **Enter**.
- 2 On the pop-up menu, select **Controller Policies** and press **Enter**.
- 3 On the Policy Settings page, **Tab** to the **Auto-Rebuild** field, press **Enter** to display the options, select **Enable** and press **Enter** again to select it.
- 4 **Tab** to **OK** and press **Enter** to select it.

The policy is enabled immediately.

Using Auto-Carving for Multi LUN Support

Auto-carving is useful for creating multiple volumes out of large arrays at the hardware level. Then, when you boot to the operating system, each volume

appears as a different disk drive, simplifying the partitioning required at the operating system level.

When the Auto-Carving policy is on, any new unit larger than a specified size (known as the *carve size*) will be created as multiple volumes that can be addressed by the operating system as separate volumes. These chunks are sometimes known as multiple LUNs (logical units). However, throughout the 3ware documentation, they are referred to as *volumes*.

For example, using the default carve size of 2 TB, if the unit is 2.5 TB then it will contain two volumes, with the first volume containing 2 TB and the second volume containing 0.5 TB. If the unit is 5.0 TB then it will contain 3 volumes, with the first two volumes containing 2 TB each and the last volume containing 1 TB. (**Note:** If a specific Boot Volume was also specified in 3BM or CLI, the first volume will be the size specified for the Boot Volume, and then the carve size will be applied to the remainder of the unit. For more information, see “Boot volume size” on page 81.)

Each volume can be treated as an individual disk with its own file system. The default carve size is 2 TB; you can change this to a setting in the range of 1 TB to 32 TB (1024 GB to 32768 GB). 3ware firmware supports a maximum of 32 volumes per controller, up to a total of 32 TB.



Note: CLI provides the ability to specify variable sizes for the first 4 volumes of a unit when auto-carving. This is done while creating a unit with the `/cx add type` command attribute `[v0=n|vol=a:b:c:d]`. See the *3ware SATA+SAS RAID Controller Card CLI Guide, Version 10.2*.

If you are migrating a unit to a size that is larger than the carve size and auto-carving is on, multiple volumes will be created.



Note: Carving a unit into multiple volumes can have an impact on performance.



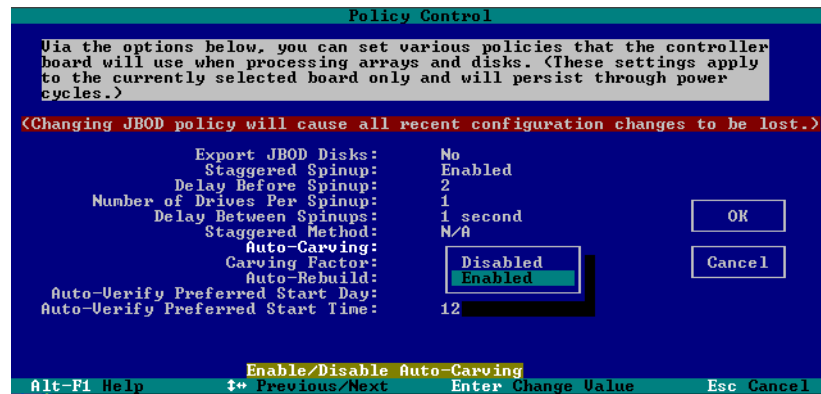
Note: Even though the Linux 2.6 kernel supports partitions larger than 2 TB, the installers for SUSE and Redhat do not. Turn auto-carving on to prevent the installation from failing.

You must turn on the Auto-Carving policy before creating the unit. Units created with this policy turned off will not be affected by a change to the policy. If the policy is turned off later, units that have been carved into volumes will retain their individual volumes; existing data is not affected.

To use auto-carving

- 1 Enable the auto-carving feature. You can do so using 3DM2 or 3BM.
In 3DM2, enable Auto-Carving at the bottom of the **Management >> Controller Settings** page.
In 3BM, you enable Auto-Carving on the **Settings >> Controller Policies** page.

Figure 34. Show Auto-Carve policy in 3BM



- 2 Create a new unit or migrate an existing unit to include the drives you want to use.
If the combined capacity of the drives exceeds the carve size, a number of volumes will be created.
- 3 Verify the creation of the volumes.
In 3DM2, the number of volumes is shown on the Unit Details page.
- 4 Verify that the volumes appear in the operating system. They will appear as additional drives.



Notes:

- If you are configuring a unit for primary storage and it will be greater than 2 TB, be sure to enable the auto-carve policy before creating the unit.
- When volumes have been created through auto-carving, they cannot be deleted except by deleting the unit.
- If you create a bootable unit that has multiple volumes, the first volume can be used as the boot device.
- Changing the auto-carve policy does not affect existing units.

Setting the Size of Volumes Created with Auto-Carving

You can use auto-carving to divide units larger than 1 TB into multiple volumes. You control the size of the volumes to be created by setting the carve size (referred to as *carving factor* in 3BM). The carve size can be between 1 TB (1024 GB) and 32 TB (32768 GB); the default is 2 TB.

When you change this policy, it applies to units you create in the future. Existing units will not be affected.

To set the carve size in 3DM2

- 1 Choose **Management >> Controller Settings** from the menu bar in 3DM2.
- 2 In the Other Controller Settings section at the bottom of the screen, in the **Carve Size** field, enter the size you want (between 1024 GB and 32768 GB) to use and click **Submit**.

The page refreshes, and a message at the top confirms the change you have made.

To set the carve size (carving factor) in 3BM

- 1 On the main 3BM screen, **Tab** to **Settings** and press **Enter**.
- 2 On the pop-up menu, select **Controller Policies** and press **Enter**.
- 3 On the Policy Settings page, **Tab** to the **Carving Factor** field, press **Enter** to display the text entry box, enter the size you want (between 1024 GB and 32768 GB) and press **Enter** again to accept it.
- 4 **Tab** to **OK** and press **Enter** to select it.

The policy is enabled immediately.

Enabling and Setting Up Staggered Spin-up

You can set the number of SAS and SATA drives that will spin up at the same time and the delay time between drive group spinups. This does not apply to SAS or SATA drives that are attached to an expander.

Three policy settings let you set the number of drives that will spin up at the same time and set the delay between drive groups that spin up at one time. Not all SATA drives support staggered spinup. If you enable staggered spinup and have drives that do not support it, the setting will be ignored. You can change these settings in 3BM or using the CLI.



Note: It is possible to enable or disable automatic detection of drives on the controller's ports for staggered spinup during hot swapping of drives. This feature is only available in the CLI using the **autodetect=on|off** command. For more information, refer to **/cx set autodetect=on|off disk=<p:-p>|all** in the *3ware SATA+SAS RAID Controller Card CLI Guide, Version 10.2*.



Note: Some hard drives require that the power management jumper (PM2) be set to enable staggered spinup, in order for the SATA OOB option to be used. For more information, search the LSI KnowledgeBase for keyword 14889 at <http://kb.lsi.com>.

To enable or disable spinup and set the delay between spinups

- 1 At the main 3BM screen, **Tab** to **Policy** and press **Enter**.
- 2 On the Policy **Control** screen, **Tab** through these fields, making the choices you want to use:
 - **Staggered Spinup:** Choose enabled or disabled.
 - **Number of Drives Per Spinup:** Select the number of drives, depending on the number of ports on the controller.
 - **Delay between spinup:** Select the number of seconds—from 1 to 6.
- 3 **Tab** to the **OK** button and press **Enter**.

You will notice a short delay as 3BM makes the policy changes.

Viewing Information About a Phy

The 3ware 9750 RAID controller family has multiple phy transceivers (phys) that receive and transmit the serial data stream between the controller and drives and other devices in the SAS domain.

Phys are associated with the SAS ports on the controller. Multiple phys can be associated with one SAS port, which is then called a “wide port.”

You can check the phy properties on the Controller Phy Summary page.

To see information for a phy in 3DM2

- 1 Select the controller for which you wish to view phy information from the drop-down list on the menu bar.
- 2 If you have a direct-attached drive you can access the Controller Phy Summary page from the **Information >> Drive Information** page by clicking the phy ID for the drive. Otherwise, navigate to the **Management >> Controller Settings** page.
- 3 Under **Other Controller Settings** click the # link for **Number of Controller Phys**.

Figure 35. Phy Summary Page

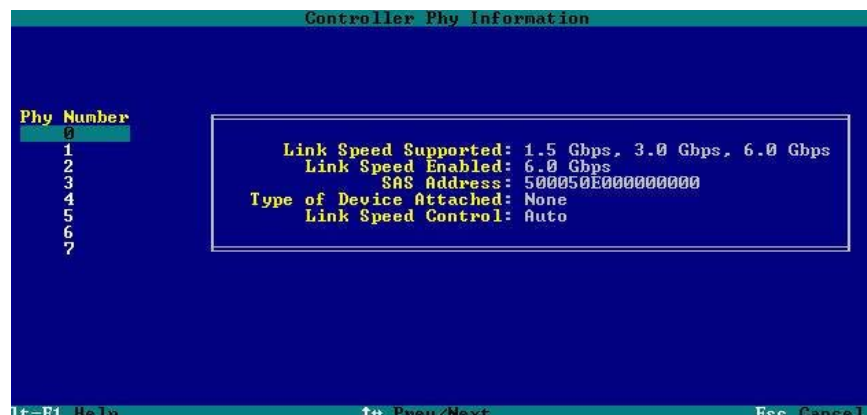
Phy	SAS Address	Link Enabled	Link Control	Type	ID
0	500050E000000127	3.0 Gbps	Auto	Enclosure	--
1	500050E000000126	3.0 Gbps	Auto	Enclosure	--
2	500050E000000125	3.0 Gbps	Auto	Enclosure	--
3	500050E000000124	3.0 Gbps	Auto	Enclosure	--
4	500050E000000123	3.0 Gbps	Auto	Enclosure	--
5	500050E000000122	3.0 Gbps	Auto	Enclosure	--
6	500050E000000121	3.0 Gbps	Auto	Enclosure	--
7	500050E000000120	3.0 Gbps	Auto	Enclosure	--

For details about the columns on this page, see “Controller Phy Summary page” on page 199.

To see information for a phy in 3BM

- 1 On the main 3BM screen, **Tab** to **Information** and press **Enter**.
- 2 On the pop-up menu, select **Phys** and press **Enter**.
- 3 On the Controller Phy Information page, use the arrow keys to select the Phy you want to see details about. The information displays on the right.

Figure 36. Controller Phy Information page



Changing the Phy Link Speed

You can change the link speed between the controller and an expander or between the controller and a drive that is directly connected to the controller. Typically, the phy link speed is set to Auto. If desired for compatibility, troubleshooting or performance analysis, you can specify a specific link speed (1.5 Gbps, 3.0 Gbps, or 6.0 Gbps).

To change the phy link speed in 3DM2

- 1 On the Controller Phy Summary page, identify the phy device for which you wish to change the link speed. Direct-attached drives are identified by their VPort ID.
- 2 In the **Link Control** drop-down menu, select the desired speed: 6 Gbps, 3 Gbps, 1.5 Gbps, or Auto.
- 3 A reboot is required to reset the link speed to the new setting.



Caution: Restricting the link speed to a higher setting will not allow slower devices to be recognized by the firmware.

For details about the information displayed on this screen, see “Controller Phy Summary page” on page 199.

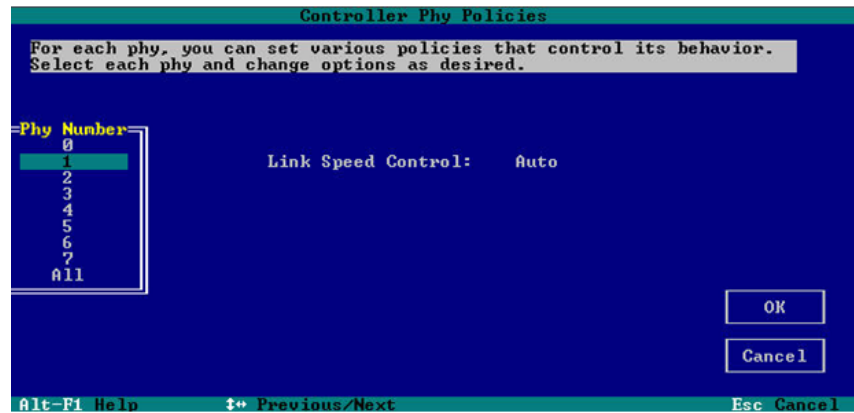
Figure 37. Controller Phy Summary page

Phy	SAS Address	Link Enabled	Link Control	Type	ID
0	500050E000000127	3.0 Gbps	Auto	Enclosure	--
1	500050E000000126	3.0 Gbps	Auto	Enclosure	--
2	500050E000000125	3.0 Gbps	Auto	Enclosure	--
3	500050E000000124	3.0 Gbps	Auto	Enclosure	--
4	500050E000000123	3.0 Gbps	Auto	Enclosure	--
5	500050E000000122	3.0 Gbps	Auto	Enclosure	--
6	500050E000000121	3.0 Gbps	Auto	Enclosure	--
7	500050E000000120	3.0 Gbps	Auto	Enclosure	--

To change the phy link speed in 3BM

- 1 On the main 3BM screen, **Tab** to **Settings** and press **Enter**.
- 2 On the pop-up menu, select **Phy Policies** and press **Enter**.
- 3 On the Controller Phy Policies page, use the arrow keys to select the Phy for which you want to set the link speed.
- 4 Press **Enter** to display a popup of the possible settings, select the one you want, and press **Enter** again.

Figure 38. Controller Phy Policies page



Configuring Units

This section includes information and procedures on configuring units attached to your 3ware RAID controller. It is organized into the following topics:

- Configuring a New Unit
- Creating a Hot Spare
- Naming a Unit
- Setting Unit Policies
- Changing An Existing Configuration by Migrating (RAID Level Migration or Online Capacity Expansion)
- Deleting a Unit
- Removing a Unit
- Moving a Unit from One Controller to Another
- Adding a Drive
- Removing a Drive
- Rescanning the Controller

Configuring a New Unit

When you configure a new unit, you specify some details related to the type of RAID configuration that you want, and others that enable or disable features.

This section first provides an overview of the different settings you can specify during configuration and then provides step-by-step instructions for creating a unit through both 3DM2 and 3BM.

Configuration Options When Creating a Unit

This section provides an overview of the choices you have when configuring a new unit. For step-by-step instructions, see “Creating a Unit through 3DM2” on page 83 and “Creating a Unit through 3BM” on page 85.

When you configure a new unit, you specify the following:

- Drives to be included in the unit
- Name of the unit (optional)

- Type of configuration (RAID Level)
- Stripe size, if appropriate for the RAID level
- Boot volume size (optional; can only be specified in 3BM or CLI)
- Initialization Method (3BM only)
- Unit policies that affect how the unit will be handled

You can make some types of changes to the RAID configuration later, and you can change the unit name and the unit policies. For details, see “Changing An Existing Configuration by Migrating” on page 115 and “Setting Unit Policies” on page 100.



Note: If you will install the operating system on and boot from a unit managed through the new 3ware RAID controller, see Chapter 2, “First-Time RAID Configuration Using 3BM.”

Drives to be included in the unit

You may include from one to thirty-two drives in the unit, depending on the number of drives available and the model of the controller you have. (For information about how many drives to select for a given RAID level, see “Determining Which RAID Level to Use” on page 12.)

When creating units on the 9750 controller, you cannot mix SAS and SATA drives in the same unit.

Available drives are those that are not currently part of a unit. If you want to use drives that are currently part of a different unit, you must first delete that unit to make the drives available. (For details, see “Deleting a Unit” on page 121.) If drives are listed under “Incomplete Drives and Others,” they must be deleted before they can be used.

If you want to add drives to a unit, see “Adding a Drive” on page 129.

Name of the unit (optional)

Units can be given names for easier identification. These names will be visible in 3DM2, CLI, and 3BM.

Type of configuration (RAID Level)

Available configuration types include RAID 0, RAID 1, RAID 5, RAID 6, RAID 10, RAID 50, and Single Disk. For information about the different RAID levels, see “Understanding RAID Concepts and Levels” on page 5



Warning: Creating a unit writes the DCB and makes any earlier data on the drives inaccessible.

Stripe size, if appropriate for the RAID level

Striping is not applicable for RAID 1 units or single drives. It is used only for RAID 0, RAID 10, RAID 5, RAID 50, and RAID 6 units.

Striping is not applicable for RAID 1, because it is a mirrored array without striping.

Using the default stripe size of 256 KB usually gives you the best performance for mixed I/Os. If your application has some specific I/O pattern (purely sequential or purely random), you might want to experiment with a smaller or larger stripe size.

Boot volume size

When you create a unit through 3BM or CLI, you can create a special volume to function as the boot volume. This is useful if you are installing an operating system onto the unit, and want it to be installed in one volume and have a separate volume for data.

This is an optional feature. You do not have to create a boot volume if you plan to install the operating system on the unit.

If you are creating a very large unit and have enabled the Auto-Carving policy, the boot volume will be created in addition to any volumes created through auto-carving. For more information about auto-carving, see “Using Auto-Carving for Multi LUN Support” on page 71.

This feature can only be specified in 3BM and CLI.

Initialization Method

In 3BM, you can choose to do a foreground (default) or background initialization of the unit. 3DM2 and CLI can only use background initialization when creating a unit.

A foreground initialization will take place before the system is booted. It can take up to several hours, depending on the size of the unit.

A background initialization allows you to have immediate use of the unit, but will take longer and slows down performance of the unit until it completes.

If your unit starts a foreground initialization and you want to use it immediately, you can press **Esc** and the unit will switch to using background initialization.

Unit policies

Several unit policies are set when you create a new unit:

- Write Cache (enabled, by default)
- Read Cache (Intelligent, by default)
- Drive Queuing (enabled, by default)
- Ignore ECC (Continue on Source Error When Rebuilding (disabled, by default))
- StorSave Profile (Balanced, by default)
- Auto-Verify (enabled, by default)
- Rapid RAID Recovery (enabled, by default)

The particular policies that you can adjust when you create the unit vary, depending on which program you are using: 3DM2, 3BM, or the CLI.

You can change all of these policies after the unit has been created, with one exception. If Rapid RAID Recovery is disabled, it cannot be enabled later.

For a summary of what these policies do, see the discussion under “Setting Unit Policies” on page 100. For how to adjust each one, see the procedures later in this chapter.

Creating a Unit through 3DM2

In 3DM2, creating a unit starts from the **Management >> Maintenance** page (Figure 39).

Figure 39. 3DM2 Maintenance Page

The screenshot shows the LSI 3DM2 web interface. At the top, there's a navigation bar with tabs for Summary, Information, Management, Monitor, 3DM2 Settings, and Help. The 'Maintenance' tab is active. Below the navigation bar, there's a 'Rescan Controller' button and a note: '(This will scan all ports for newly inserted drives/units)'. The main content area is titled 'Unit Maintenance (Controller ID 0)'. It displays two units, Unit 0 and Unit 1, each with 5 drives. Unit 0 is configured with RAID 6 Zygote 1 and has a total capacity of 100.55 GB. Each drive in the unit is a 34.25 GB MAXTOR ATLAS15K2_36SAS drive, and all are in an 'OK' status. There are 'Remove Drive' links for each drive. Below the unit list, there are buttons for 'Verify Unit', 'Rebuild Unit', 'Migrate Unit', 'Remove Unit', and 'Delete Unit'. A warning message states: '*Before removing or deleting a unit, make sure there is no I/O on the unit and unmount it'. Below this is the 'Available Drives (Controller ID 0)' section, which is a table with columns for VPort, Model, Capacity, Type, Phy, Slot, and Status. Three drives are listed: VPort 0 (MAXTOR ATLAS15K2_36SAS, 34.25 GB, SAS, Enclosure 0 Slot 10, OK), VPort 6 (SAMSUNG HD160JJ, 149.05 GB, SATA, Slot 0, OK), and VPort 13 (SAMSUNG HD160JJ, 149.05 GB, SATA, Slot 2, OK). At the bottom, there are buttons for 'Create Unit', 'Remove Drive', 'Set Spare(s)', and 'Clear Configuration'.

Unit	Drives	RAID	Zygote	Capacity	Status
Unit 0	5 drives	RAID 6	Zygote 1	100.55 GB	OK
	VPort 7	MAXTOR ATLAS15K2_36SAS		34.25 GB	OK
	VPort 8	MAXTOR ATLAS15K2_36SAS		34.25 GB	OK
	VPort 9	MAXTOR ATLAS15K2_36SAS		34.25 GB	OK
	VPort 10	MAXTOR ATLAS15K2_36SAS		34.25 GB	OK
	VPort 11	MAXTOR ATLAS15K2_36SAS		34.25 GB	OK
Unit 1	5 drives	RAID 6	Zygote 2	100.55 GB	OK
	VPort 1	MAXTOR ATLAS15K2_36SAS		34.25 GB	OK
	VPort 2	MAXTOR ATLAS15K2_36SAS		34.25 GB	OK
	VPort 3	MAXTOR ATLAS15K2_36SAS		34.25 GB	OK
	VPort 4	MAXTOR ATLAS15K2_36SAS		34.25 GB	OK
	VPort 5	MAXTOR ATLAS15K2_36SAS		34.25 GB	OK

VPort	Model	Capacity	Type	Phy	Slot	Status
<input type="checkbox"/> 0	MAXTOR ATLAS15K2_36SAS	34.25 GB	SAS	--	Enclosure 0 Slot 10	OK
<input type="checkbox"/> 6	SAMSUNG HD160JJ	149.05 GB	SATA	0	--	OK
<input type="checkbox"/> 13	SAMSUNG HD160JJ	149.05 GB	SATA	2	--	OK

To create a unit

- 1 In 3DM2, choose **Management >> Maintenance**.
- 2 In the Available Drives list, select the drives you want to include in the unit by marking the checkbox in front of the VPort number for each one.

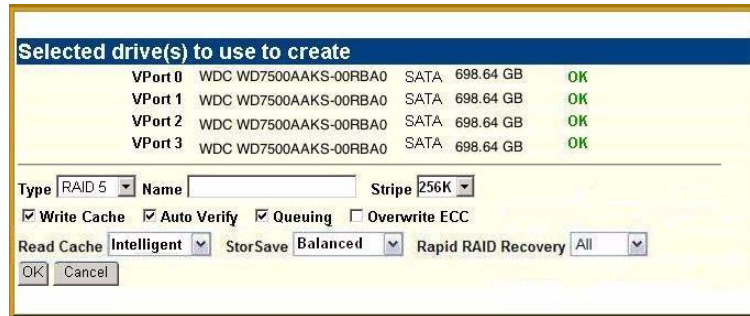
All drives in a unit must be of the same type—either SAS or SATA.

Although the best practice is to create a unit from drives in the same enclosure, you can create a unit with drives from different enclosures.

- 3 Click **Create Unit**.

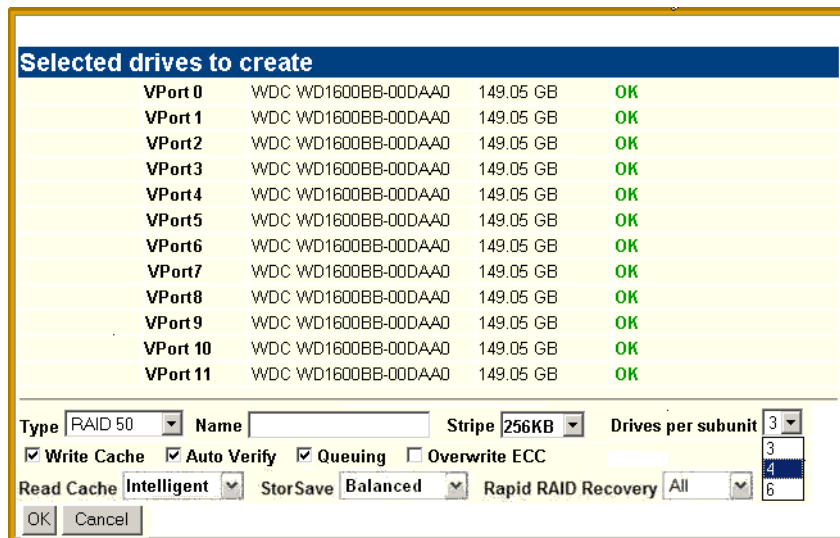
A window similar to the one below shows the drives you selected, and lets you specify configuration settings.

Figure 40. Configuring a Unit in 3DM2



- 4 In the **Type** field, select the RAID configuration you want.
- 5 If stripe size applies to the RAID type you select, select a **Stripe Size**. (Stripe size does not apply to RAID 1.)
- 6 Optional: In the **Name** box, enter a name for the unit (up to 21 characters, including dashes and underscores).
- 7 If you have 12 drives attached to the controller and selected RAID 50 as the configuration in step 3, select whether you want 3, 4, or 6 Drives Per Subunit, as shown here.

Figure 41. Configuring a RAID 50 with 12 Drives



- 8 Make changes to the unit policies, as desired. You can enable or disable the **Write Cache**, **Auto-Verify**, and **Overwrite ECC**. You can also set the **StorSave** policy, the **Rapid RAID Recovery** policy, and the **Read Cache** policy

For details about these settings, see “Setting Unit Policies” on page 100.

9 Click **OK**.

The new unit appears in the Unit Maintenance list at the top of the page and the operating system is notified of the new unit.

If you have auto-carving enabled and the size of your unit exceeds the carve size, you might see multiple unit volumes in your operating system. For details, see “Using Auto-Carving for Multi LUN Support” on page 71.

In FreeBSD, Linux, Mac OS X, OpenSolaris, and VMware a device node will now be associated with each unit created. In Windows, the device manager will reflect the changes under the disk drives icon.

10 Partition, format, and mount the unit. The required steps will vary depending on the operating system. For details, see “Partitioning, Formatting, and Mounting Units” on page 90.



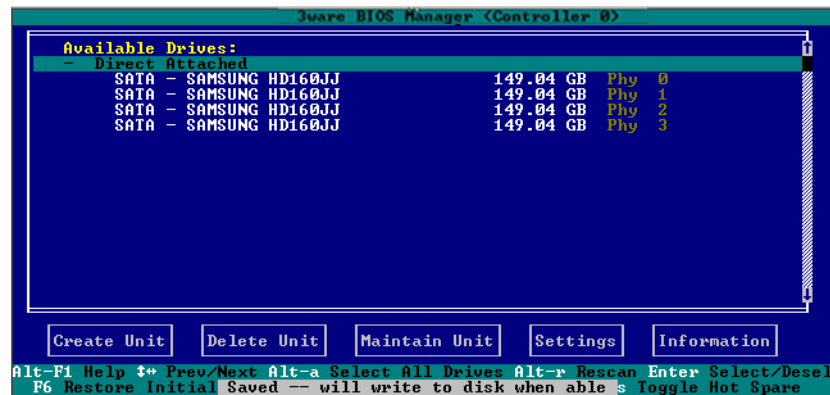
Note: For RAID 5 and RAID 6 units with five or more disks, and RAID 50 units with subunits of five drives or more, initialization (synchronization) of the unit begins immediately.

The unit can be used while it is initializing and is fault-tolerant.

Creating a Unit through 3BM

In 3BM, configuration tasks start from the main 3ware BIOS Manager screen shown in Figure 42.

Figure 42. 3BM Main Display



To create a unit through 3BM

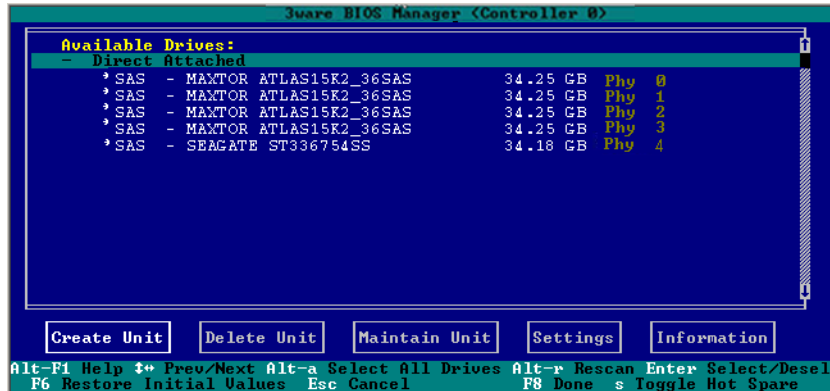
- 1 At the main 3BM screen, select the drives to be included by highlighting each one and pressing **Enter** or **Space** to select it.

When you select a drive, an asterisk appears next to it in the left most column (see Figure 43).



Tip: If you want to use all available drives, press **Alt-A** to select them all.

Figure 43. Asterisks Next to Selected Drives



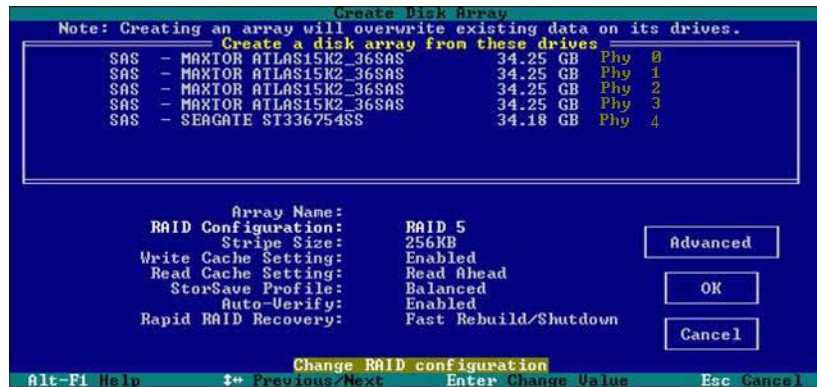
- 2 After all drives for the unit are selected, Tab to the **Create Unit** button and press **Enter**.



Tip: You can also press **Alt-C** to choose Create Unit.

- 3 On the **Create Disk Array** screen, make sure that the proper drives are listed.

Figure 44. Create Disk Array screen



- 4 (Optional) Press **Enter** and type a name for the unit; then press **Enter** again to set the name.

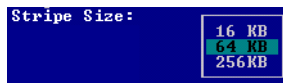
- 5 Tab to the **RAID Configuration** field and press **Enter** to see a list of available configurations for the number of drives you selected.

Figure 45. Configuration Choices for Four Drives



- 6 Use the **arrow keys** to select the configuration you want and press **Enter**.
- 7 **Tab** to the field **Stripe Size** and select the desired striping size (16, 64, or 256 KB).

Figure 46. Stripe Sizes for a RAID 5



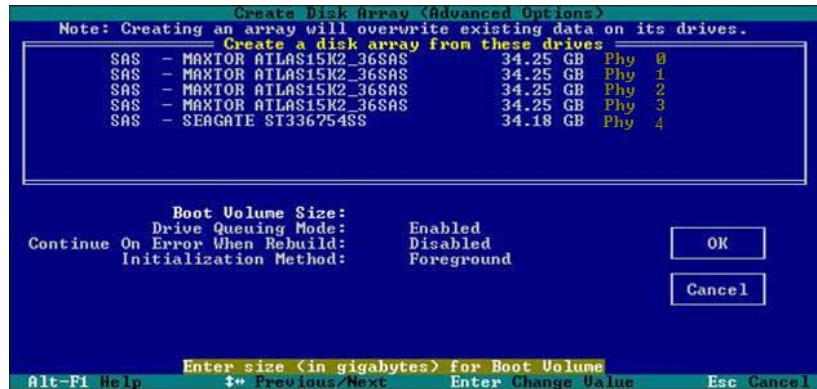
- 8 (Optional) **Tab** through the policy fields and make any appropriate changes to the default settings for:
 - **Write Cache Setting**
 - **Read Cache Setting**
 - **StorSave Profile**
 - **Auto-Verify**
 - Rapid RAID Recovery

For details about these settings, see “Configuration Options When Creating a Unit” on page 79.

- 9 (Optional) **Tab** to the Advanced Options screen and make any appropriate changes to the default settings for:
 - **Boot Volume Size (in gigabytes)**
 - **Drive Queuing Mode**
 - **Continue on Error During Rebuild**
 - **Initialization method**

For details about these settings, see “Configuration Options When Creating a Unit” on page 79.

Figure 47. Create Disk Array Advanced Options screen



- 10 From the Advanced Options screen, **Tab** to the **OK** button and press **Enter** to return to the Create Disk Array screen
- 11 **Tab** to the **OK** button and press **Enter** to confirm creation of the unit.
- 12 If the volume summary screen appears, review the information and press any key to continue.

Multiple volumes will be created if you entered a Boot Volume Size of greater than zero (0), or if auto-carving is enabled and the combined size of the drives in your unit is large enough to divide it into multiple volumes.

If you are not satisfied with how the volumes will be split up in the unit, delete the unit from the main 3BM screen and recreate it using a different Boot Volume Size. If desired, you can change the auto-carving policy or the carve size on the Policies page. For more information, see “Using Auto-Carving for Multi LUN Support” on page 71.

You are returned to the main 3BM screen.

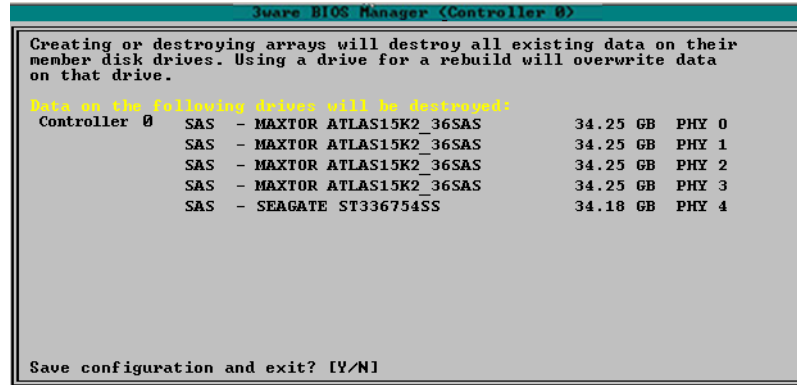


Note: The unit is not actually created and no data is overwritten until you have finished making all your changes and press **F8**.

- 13 When you are finished making configuration changes, press **F8** to save the changes and exit 3BM.

A warning message tells you that all existing data on the drives will be deleted, and asks you to confirm that you want to proceed.

Figure 48. Confirmation Message when Saving and Exiting



If you made changes to units on more than one controller, the details about changes about to be made may extend beyond one screen. In this case, you use the **PgUp** and **PgDn** keys to bring more information into view.

- 14 Type **Y** to continue, delete any existing data on the drives, and create the unit.
- 15 Partition and format the units, as described under "Partitioning, Formatting, and Mounting Units" on page 90.



Note: For RAID 5 and RAID 6 units with 5 or more disks, and RAID 50 units with a subunit of 5 or more disks, initialization of the unit begins immediately. You can postpone initialization if you want to begin using the units right away, however initialization from the BIOS is faster than it is under the operating system, so it will be a longer period of time until the unit has optimal performance. For more information, see "About Initialization" on page 146.

Ordering Units in 3BM

If you configure multiple units in 3BM and you want to install the OS on one of them so that you can boot from that unit, that unit must be the first unit.

You can change the order of the units in 3BM.

To change the order of units in 3BM

- 1 At the main 3BM screen, in the list of exportable units, highlight the unit you want to move.

- 2 Press the **Page Up** key to move the unit up the list; press the **Page Down** key to move the unit down the list.

Position the unit you want to be bootable at the top of the list of exportable units.

- 3 When you are finished working in 3BM, press **F8** to save your changes and exit.

Partitioning, Formatting, and Mounting Units

After you create a unit, whether through 3BM or 3DM2, it needs to be formatted, partitioned, and mounted by the operating system before it can be used.

The steps vary, depending on your operating system. For the appropriate steps, see:

- “To partition, format, and mount under FreeBSD” on page 92
- “To partition, format, and mount under Linux” on page 91
- “To partition, format, and mount under Mac OS” on page 92
- “To partition, format, and mount under OpenSolaris” on page 97
- “To partition, format, and mount under Windows” on page 90

For information about partitioning, formatting, and mounting under VMware, consult VMware’s User Guide or contact VMware’s Technical Support.

To partition, format, and mount under Windows

- 1 Boot the system and log in as a system administrator.
- 2 Partition and format the new arrays or disks using the **Administrative Tools** from the **Start** menu:
 - a Choose **Computer Management** from the **Administrative Tools** menu.
 - b Select **Storage**.
 - c Select **Disk Management**.
- 3 Follow the steps that appear on-screen to write a signature to the drive.
- 4 Right-click on the drive and select **Create Volume**.



Note: If you plan on migrating your unit to a larger array or another RAID type in the future remember to select the dynamic disk option. Only dynamic disks can be resized into larger partitions. Older Windows systems cannot convert basic disks into dynamic disks after the file system has been created.

- 5 Follow the steps that appear on-screen to create a volume and to assign a drive letter.

The volume is automatically mounted after formatting completes.

To partition, format, and mount under Linux

- 1 Boot the system and log in as root.
- 2 Open a terminal window.
- 3 Partition the unit:



Note: Depending on the version of Linux you are using, some of the following parted command outputs will be slightly different.

```
fdisk /dev/sda
```

If the unit is over 2 TB, use:

```
parted /dev/sda
```

```
(parted) mklabel
New disk label type? gpt
(parted) p
```

```
Disk geometry for /dev/sda: 0kB - 1074GB
Disk label type: gpt
Number Start End Size File system Name Flags
parted /dev/sda
```

```
(parted) mkpart
```

```
Partition type? [primary]?
File system type? [ext2]?
Start? 0
End? 1074gb
```

```
(parted) p
Disk geometry for /dev/sda: 0kB - 1074GB
Disk label type: gpt
Number Start End Size File system Name Flags
1 17kB
1074MB 1074MB
```

- 4 Create or make the file system:

```
mkfs /dev/sda1
```

Use of the `-j` option to turn on journaling is recommended for large partitions.

For example:

```
mkfs -j /dev/sda1
```

If the partition is over 2 TB, use `parted` to also make the file system:

```
parted /dev/sda1
```

```
(parted) mkfs
Partition number? 1
File system? [ext2]?
writing per-group metadata (begins)...0% to 100% is
displayed)
```

```
(parted) quit (when completed)
```

5 Mount the volume:

```
mount /dev/sda1 /mnt
```

To partition, format, and mount under FreeBSD

1 Boot the system and log in as root.

2 Open a terminal window.

3 Partition the unit:

```
fdisk -BI /dev/da0;
disklabel /dev/da0 | disklabel -B -R -r da0
```

4 Create or make the file system:

```
newfs /dev/da0c
```

5 Mount the volume:

```
mount /dev/da0c /mnt
```

You can also use `sysinstall` to format and partition the unit.

To partition, format, and mount under Mac OS

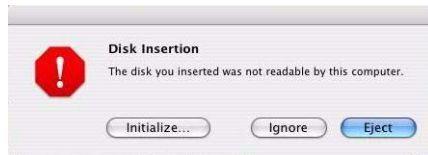


Note: “Initialization” of the unit by your operating system is different from “initialization” of a unit by 3ware. Initialization under your operating system will format your disk, erasing any existing data in the process. Initialization under 3ware does not erase data; it puts redundant data on the drives of redundant units into a known state so that data can be recovered in the event of a disk failure.

When you create a unit through 3DM2, the Mac OS X recognizes that a new disk is available, and displays a message asking what you want to do. (If this message does not appear, you can start the Disk Utility manually from the Finder and skip to step 2.)

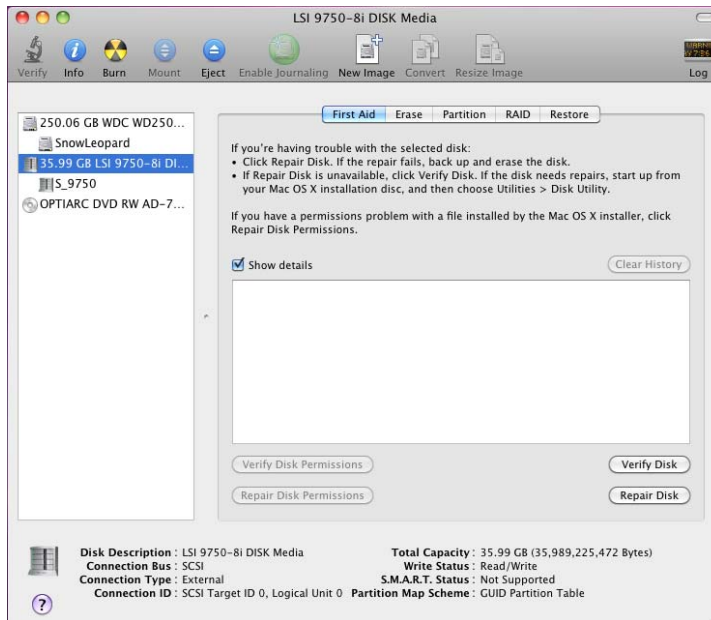
- 1 In the Mac OS message, click **Initialize**.

Figure 49. Disk Insertion Message from the Mac OS



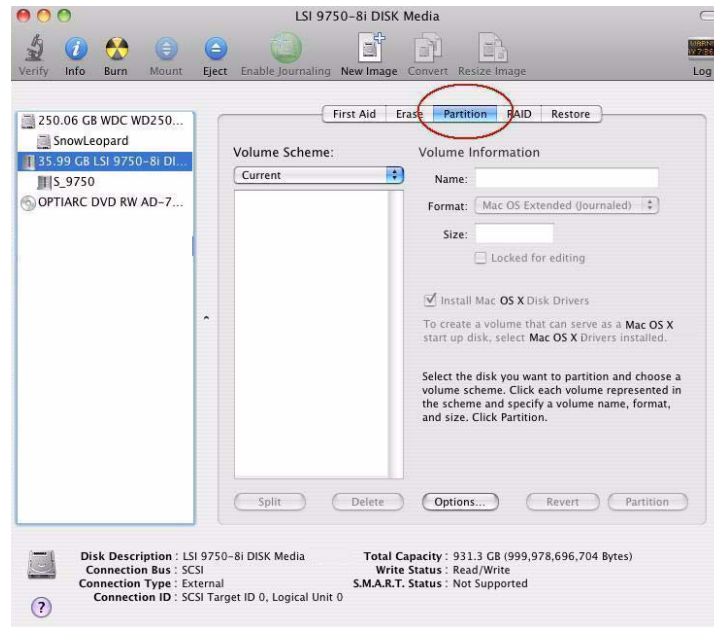
- 2 When the Macintosh[®] Disk Utility window opens, find and select the drive that represents your RAID unit.

Figure 50. Macintosh Disk Utility Window with New RAID Unit



- 3 In the Disk Utility Window, select the **Partition** tab.

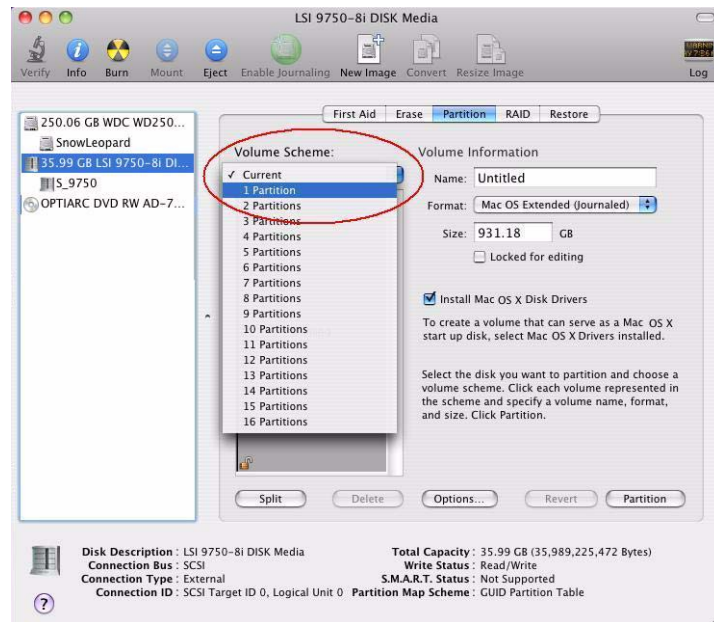
Figure 51. Macintosh Disk Utility Window, Partition Tab



- 4 In the Volume Scheme column, click **Current** to show the drop-down menu and select the number of partitions that you want your RAID unit to have.

Tip: If you only want one storage volume, select **1 Partition**. (Each partition will appear as a separate drive on your computer.)

Figure 52. Selecting the Number of Volumes in Disk Utility

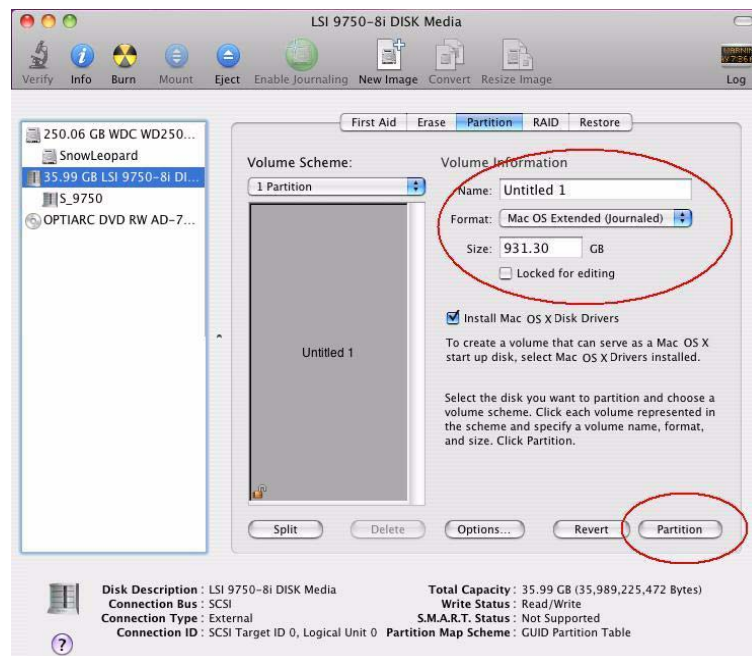


- 5 On the right, specify a volume name and then click **Partition**.

It is recommended to use a unique name, although Mac OS X will allow you to give the same name to more than one partition.

If you have questions about what Format to select, see the Apple documentation.

Figure 53. Defining the Volume in the Macintosh Disk Utility



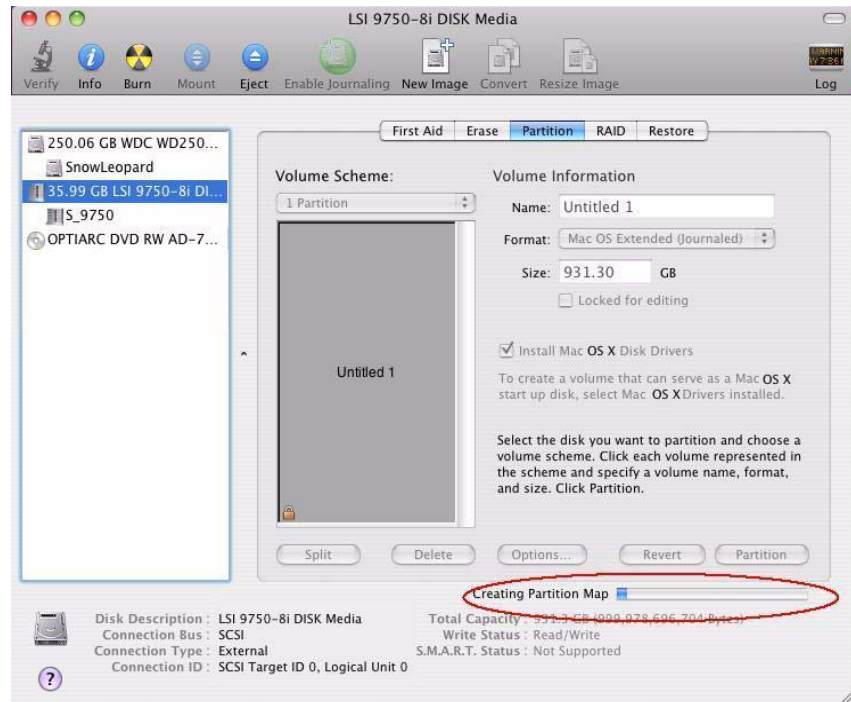
- When a message asks you to confirm you want to partition the disk, click **Partition**.

Figure 54. Confirmation Message to Create the Partition



You will see a series of messages appear toward the bottom of the Disk Utility window as the RAID unit is first partitioned and then formatted. This may take a couple of minutes, depending on the size of the drives in your RAID unit.

Figure 55. Macintosh Disk Utility Showing Partitioning Progress



When the partitioning is complete, icons for each new volume appear on your desktop. They are now ready for use.

You can now close the Macintosh Disk Utility window. Your RAID unit is ready for use.

To partition, format, and mount under OpenSolaris

After you create a RAID unit through 3BM or the 3ware CLI, you will need to format and partition the unit, create a file system, and mount it.

These types of system administration tasks are found in the OpenSolaris documentation.

- OpenSolaris System Administrator Collection:
<http://docs.sun.com/app/docs/coll/47.24>
- OpenSolaris System Administration Guide:
<http://docs.sun.com/app/docs/doc/819-2723>
-Chapter 10 Managing Disks (Overview)
- Solaris ZFS Administration Guide:
<http://docs.sun.com/app/docs/doc/817-2271>
- OpenSolaris Reference Manual Collection:
<http://docs.sun.com/app/docs/coll/40.18>
 - See man pages section 1M: System Administration Commands
 - format (1M)
 - fdisk (1M)
 - newfs (1M)
 - zpool (1M)
 - If you have the documentation installed also try
 - “# man -s 1M format”
 - “# man -s 1M fdisk”
 - “# man -s 1M newfs”
 - “# man -s 1M zpool”

Creating a Hot Spare

You can designate an available drive as a hot spare. If a redundant unit degrades and a hot spare the size of the degraded disk (or larger) is available, the hot spare will automatically replace the failed drive in the unit without user intervention.



Note: When a hot spare replaces a failed drive, an event notification is generated and appears in the list of alarms in 3DM2. You can also have 3DM2 send you an email about this. See “Managing E-mail Event Notification” on page 59.

It is a good idea to create a hot spare after you create a redundant unit.

In order to replace a failed drive, a hot spare must have the same or larger storage capacity than the drive it is replacing, and must be of the same type (SAS or SATA).

The Auto-Rebuild policy allows automatic rebuilding to occur with available drives that are not designated as spares. For more information, see “Setting the Auto-Rebuild Policy” on page 71.



Note: 3ware's 9750 RAID controllers use drive coercion so that drives from differing manufacturers and with slightly different capacities are more likely to be able to be used as spares for each other. Drive coercion slightly decreases the usable capacity of a drive that is used in redundant units.

The capacity used for each drive is rounded down to the nearest GB for drives under 45 GB (45,000,000,000 bytes), and rounded down to the nearest 5 GBytes for drives over 45 GB. For example, a 44.3 GB drive will be rounded down to 44 GBytes, and a 123 GB drive will be rounded down to 120 GBytes.

If you have 120 GB drives from different manufacturers, chances are that the capacity varies slightly. For example, one drive might be 122 GB, and the other 123 GB, even though both are sold and marketed as “120 GB drives.” 3ware drive coercion uses the same capacity for both of these drives so that one could replace the other.

Specifying a Hot Spare through 3DM2

If you need to add a drive to be used as the hot spare, follow the instructions under “Adding a Drive” on page 129.

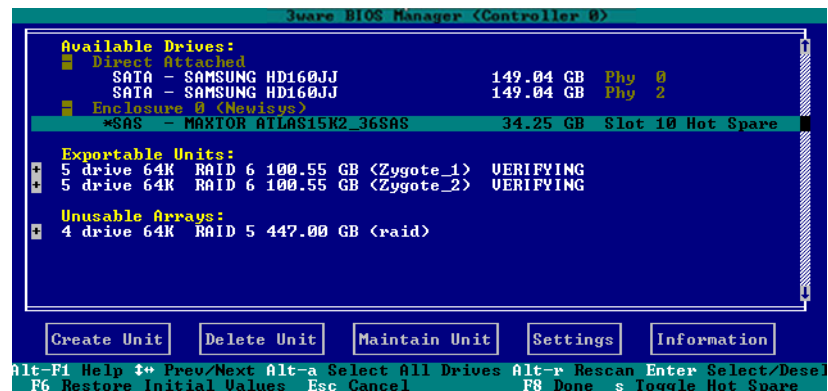
To specify a hot spare

- 1 In 3DM2, choose **Management >> Maintenance**.
- 2 In the Available Drives list, select the drive you want as a hot spare by marking the checkbox in front of its Port number.
- 3 Click **Set Spares**.
You will see the status change to **OK-SPARE**.

Specifying a Hot Spare through 3BM

- 1 On the main 3BM screen, in the list of **Available Drives**, highlight the drive you want to use.
- 2 Type **s** to specify that the selected drive will be the hot spare.
You'll see the words “Hot Spare” appear next to the drive in the Available Drives list.

Figure 56. Hot Spare Indicated



If a hot spare is already enabled, you can disable it by pressing **s** again.

- 3 If you are finished making changes in 3BM, press **F8** to save the changes and exit.



Note: If the drive you designated as a spare is not large enough to replace a failed drive in a fault-tolerant unit, or if there is not a fault-tolerant unit for the spare to support, 3BM will notify you.

Naming a Unit

Units can be given unique names to more easily identify them. A unit can be assigned a name when it is created. It can also be named or renamed at a later time.

To name or rename a unit through 3DM2

- 1 Make sure the appropriate controller is selected in the drop-down list at the right of the menu bar.
- 2 Choose **Management >> Controller Settings** from the menu bar in 3DM2.
- 3 In the **Unit Names** section of the Controller Settings page, locate the unit for which you want to change the name.
- 4 In the text box, enter or type over the name shown. A name can be up to 21 characters, and can include dashes and underscores.
- 5 Click the **Save Names** button.



Note: If you want to cancel your change before saving it, click the **Reset Names** button.

To name or rename a unit through 3BM

- 1 At the main 3BM screen, select the unit by highlighting it and pressing **Enter**.
An asterisk appears in the left-most column to indicate that it is selected.
- 2 **Tab** to the **Maintain Unit** button and press **Enter**.
- 3 On the pop-up menu, select **Configure** and press **Enter**.
On the Configure Disk Array screen, the **Array Name** field is already selected.
- 4 Press **Enter** to open a text box.
- 5 Type a name for the unit and press **Enter**.
- 6 **Tab** to the **OK** button and press **Enter** to select it. You return to the main 3BM screen.
- 7 When you are finished making changes, press **F8** to save them and exit 3BM.

Setting Unit Policies

The following policies are set when you create a unit, and can be adjusted later through settings on the **Management >> Controller Settings** pages of 3DM2 and the Policy Control screen in 3BM. Details about adjusting each policy are described on the following pages.

- **Write Cache.** Determines whether write cache is enabled for the unit. When the write cache is enabled, data is stored locally on the controller before it is written to disk, allowing the computer to continue with its next task. This provides the most efficient access times for your computer system. When disabled, the computer will wait for the controller to write all the data to disk before going on to its next task. For details, see “Enabling and Disabling the Unit Write Cache” on page 102.

This feature interacts with functionality of the BBU, if you have one, and with the unit’s StorSave profile. For details, see “Enabling and Disabling the Unit Write Cache” on page 102.

- **Read Cache.** Determines whether Intelligent or Basic Read Cache is enabled, or whether Read Cache is disabled. Setting the appropriate type of Read Cache can improve performance for different types of applications. For details, see “Working with Read Cache Settings” on page 104.
- **Auto-Verify.** Determines whether the unit will be automatically verified at a time determined by the Verify Schedule. Enabling this feature helps insure that the unit is verified on a regular basis. For details, see “Enabling or Disabling Auto-Verify for a Unit” on page 107.

- Override ECC (Continue on Source Error When Rebuilding).** Determines whether ECC errors are ignored when they are encountered during a rebuild. (ECC errors are an indication of errors that have occurred on a particular drive since it was last read.) When not enabled, a rebuild will abort upon encountering an ECC error and the unit will be set to Degraded. For details, see “Setting Overwrite ECC (Continue on Source Error When Rebuilding)” on page 108.
- Queuing.** Determines whether command queuing is enabled for the unit. When enabled for drives that support it, this policy can improve performance. For details, see “Enabling and Disabling Queuing for a Unit” on page 110.
- StorSave Profile.** Determines what StorSave profile is used for the unit. Three profiles are available: Protection, Balanced, and Performance. For details, see “Setting the StorSave Profile for a Unit” on page 111.
- Rapid RAID Recovery.** Determines which Rapid RAID Recovery option to use, **All**, **Rebuild** or **Disable**. **All** will apply the policy to both rebuilds and unclean shutdowns. **Rebuild** will apply only to rebuilds. You can switch between **All** and **Rebuild** settings, but, once Rapid RAID Recovery is disabled for the unit, it cannot be re-enabled. For details, see “Rapid RAID Recovery” on page 113.

Figure 57. Unit Policies on Controller Settings Page in 3DM2

The screenshot displays the LSI 3DM2 web interface for Controller ID 0. The page is divided into several sections:

- Background Task (Controller ID 0):** A table with columns for Task Rate (5, 4, 3, 2, 1) and Mode. It includes settings for Rebuild/Migrate and Verify tasks, with radio buttons for task rates and checkboxes for Adaptive and Low Latency modes. A note states: "Recommended: With Low Latency mode, use a Rebuild/Migrate Task Rate greater than 1".
- Unit Policies (Controller ID 0):** A table with columns for Write Cache, Read Cache, Auto Verify, Overwrite ECC, Queuing, StorSave, and Rapid RAID Recovery. The Write Cache is checked, Read Cache is set to Intelligent, Auto Verify is checked, Overwrite ECC is set to --, Queuing is checked, StorSave is set to Balance, and Rapid RAID Recovery is set to --.
- Unit Names (Controller ID 0):** A section for Unit 0 [SINGLE DISK] with a text input field and Save Names/Reset Names buttons.
- Other Controller Settings (Controller ID 0):** A section with various settings: Auto Rebuild (Disabled), Auto Carving (Disabled), Carve Size (2048 GB), Number of Drives per Spin-up (1), Delay between Spin-up (1 second(s)), Export Unconfigured Disk (Yes), and Number of Controller Phys (8).
- Update Firmware:** A section with an Image File input field, a Browse... button, and a Begin Update button.

Enabling and Disabling the Unit Write Cache

Write cache is used to store data locally in memory on the controller before it is written to the disk drive media, allowing the computer to continue with its next task. This improves performance. However, there may be instances when you want the computer to wait for the drive to write all the data to disk before going on to its next task. In this case, you must disable the write cache.



Note: If write cache is enabled, in the event of a power failure, the data in the controller cache will be lost if you do not have a Battery Backup Unit (BBU). To avoid a sudden power failure if you do not have a BBU, it is advisable to have an Uninterruptible Power Supply (UPS).

Write cache can be turned on or off for individual units in 3DM2, CLI, and 3BM without changing the configuration or losing data from the drives.

If you have a BBU (Battery Backup Unit) installed on the controller, the battery preserves the contents of the controller cache memory for a limited period of time (up to 72 hours) in the event of a system power loss. When a BBU is installed, if the battery is not “Ready,” write cache is disabled and cannot be enabled.

The unit's StorSave profile can also determine whether the write cache can be enabled or disabled. A warning message will be given if the change is not permitted due to the StorSave setting and the state of the unit.



Note: If the **Write Cache** checkbox is disabled (not selectable), check to see if the unit has degraded or if the BBU is not ready. If a unit has a StorSave policy of “Protect” and the unit degrades, the policy prevents write cache from being re-enabled until the unit has been rebuilt or until the BBU is ready to use.

To enable or disable unit write cache through 3DM2

- 1 Choose **Management >> Controller Settings** from the menu bar in 3DM2.
- 2 In the **Unit Policies** section of the Controller Settings page, check the Write Cache box to enable it for the designated unit.

Figure 58. Write Cache Policy in 3DM2

Unit Policies (Controller ID 0)	
	Write Cache
Unit 0 [RAID 0]	<input checked="" type="checkbox"/>
Unit 1 [RAID 1]	<input checked="" type="checkbox"/>

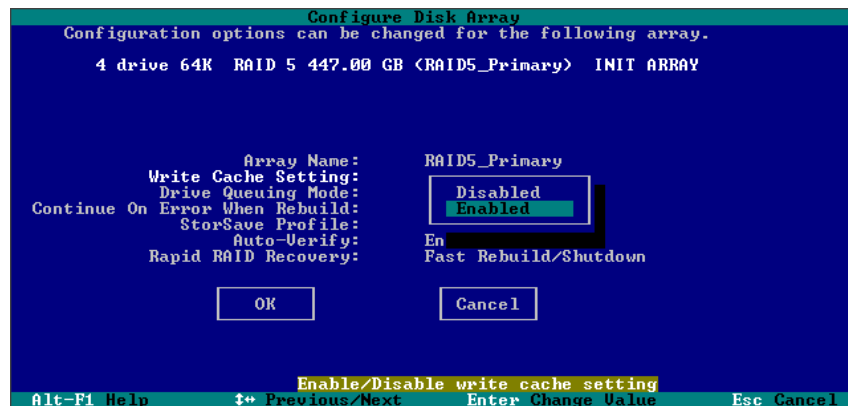
The page refreshes, and a message at the top confirms the change you have made.

If your system has no BBU, a message will caution you about enabling write cache.

To enable or disable unit write cache through 3BM

- 1 At the main 3BM screen, select the unit by highlighting it and pressing **Enter**.
An asterisk appears in the left-most column to indicate that it is selected.
- 2 **Tab** to the **Maintain Unit** button and press **Enter**.
- 3 On the pop-up menu, select **Configure** and press **Enter**.
- 4 In the Configure Disk Array screen, **Tab** to the field **Write Cache Settings**.

Figure 59. Unit Write Cache State in 3BM



The current setting—Enabled or Disabled—is shown. (The initial default setting is for write cache to be enabled.)

- 5 Press **Enter** to display the choices, use the **arrow keys** to select the setting you want, and press **Enter** again to choose it.
- 6 **Tab** to the **OK** button and press **Enter** to select it.
You return to the main 3BM screen.
- 7 When you are finished making changes, press **F8** to save them and exit 3BM.

Working with Read Cache Settings

The Read Cache unit policy lets you enable either Basic Read Caching or Intelligent Read Caching. You can also disable the Read Cache unit policy, if preferred.

By default, Read Cache is set to **Intelligent**. You can change it to **Basic** or to **Disabled**, as appropriate.

About the Read Cache Basic and Intelligent Modes

Basic Mode is used to store read cache data locally on the controller that has recently been written to media and is likely to be frequently accessed. This improves read access times for applications such as a database that can take advantage of storage caching. The read cache may be disabled without reducing performance for applications that are write intensive, or that rarely read back data recently written.

Intelligent Mode enables the Intelligent Read Prefetch (IRP) feature.

The Intelligent Read Prefetch feature includes a typical read-ahead caching method which is used to proactively retrieve data from media and store it locally on the controller with the anticipation that it may be requested by the host. For example, the host may read blocks 1, 2, and 3. With the read-ahead caching included in IRP, the controller will also retrieve and hold in its cache blocks 4, 5, and 6 in anticipation of getting those command requests from the host. By loading a larger set of data into the cache, chances are improved that another request can be filled by data that is already in the cache. This can be helpful with applications that are sequential in nature, such as video on demand, video surveillance playback, and restoring from a disk-to-disk backup. Performance benefits of read-ahead are especially pronounced when the host queue depth is low. In addition, this read-ahead caching also improves sequential read performance when the unit is degraded.

The Intelligent Read Prefetch (IRP) feature also includes an intelligent and adaptive stream management layer to improve performance at higher queue depth in multiple read only or mixed read/write stream environments. The performance improvements should be seen for most RAID types regardless of the unit's operational state (normal, degraded, and so forth).

Note that if Intelligent Mode is enabled, the features in Basic mode are also enabled.

When to Use Each Read Cache Setting

The following table provides some recommendations for when to use each Read Cache setting.

Table 8: Recommendations for Using Each Read Cache Setting

Use this Read Cache Setting	For this reason	Example applications
Intelligent	Sequential applications, with a low host command queue depth	Video on Demand, Video Surveillance Playback Disk-to-Disk Backup Restores, File Server
Basic	Frequent access to recently written data	Database
Disabled	Applications that produce a high queue depth or perform their own read-ahead can generate enough I/O to negate the benefits of controller read caching or read-ahead. This is especially true for applications that produce a lot of random I/O.	Online Transaction Processing (OLTP)

Changing the Read Cache Policy for Existing Units

The Read Cache policy is initially set when you create a unit. You can change it later from either 3DM2 or 3BM.

To change the Read Cache unit policy In 3DM2

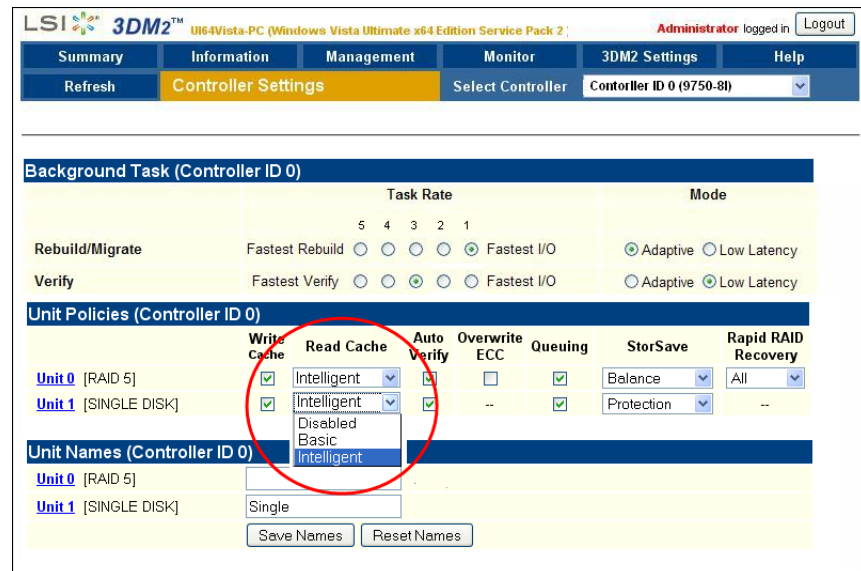
- 1 Choose **Management >> Controller Settings** from the menu bar in 3DM2.
- 2 In the **Unit Policies** section of the Controller Settings page, select the desired Read Cache setting, as shown in Figure 60.

Intelligent: Enables both the Basic and Intelligent Read Prefetch (IRP) caching features.

Basic: Enables the Basic read caching mode for the unit.

Disabled: Disables the Read Cache policy for the unit.

Figure 60. Read Cache policy on the Controller Settings page



After you change the selection, the page refreshes, and a message at the top confirms the change you have made.

To change the Read Cache unit policy In 3BM

- 1 At the main 3BM screen, select the unit by highlighting it and pressing **Enter**.

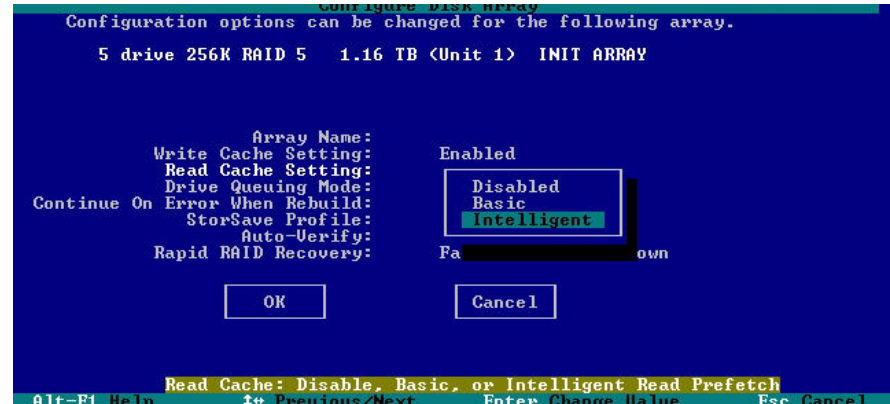
An asterisk appears, indicating that the RAID unit is selected.

- 2 **Tab** to the **Maintain Unit** button and press **Enter**.
- 3 On the pop-up menu, select **Configure** and press **Enter**.
- 4 In the Configure Disk Array screen, **Tab** to the field **Read Cache Setting**.

The current setting—Intelligent, Basic, or Disabled—is shown.

- 5 Press **Enter** to display the choices, use the arrow keys to select the setting you want (Figure 61), and press **Enter** again to choose it.

Figure 61. Read Cache Setting on the Configure screen



- 6 Tab to the **OK** button and press **Enter** to select it.
You return to the main 3BM screen.
- 7 When you are finished making changes, press **F8** to save them and exit 3BM.

Enabling or Disabling Auto-Verify for a Unit

Auto-Verify can help insure that a unit is verified on a regular basis. This is important, as it can provide early warning of unstable units and possible data loss due to a failing drive.

Auto-Verify is set on a per-unit basis, and works in conjunction with the Verify Schedule, which is set on a controller-wide basis. By default, the Verify Schedule is set to “Basic,” which specifies a weekly day and time for verification to occur when Auto-Verify is enabled.

The steps below describe how to enable or disable Auto-Verify for an existing unit. For more detailed information, see “Using Auto Verification” on page 152. For how to view or change the Verify Schedule, see “Selecting Advanced or Basic Verify Schedules” on page 166.



Note: If Auto-Verify is disabled for a unit, then verification will only run if you start it manually or in the event of an unclean shutdown.

You can start a verify manually at any time. See “Starting a Verify Manually” on page 152.

To enable or disable the Auto-Verify policy for an existing unit through 3DM2

- 1 Choose **Management >> Controller Settings** from the menu bar.
- 2 In the **Unit Policies** section of the **Controller Settings** page check the **Auto-Verify** box for the appropriate unit. (To disable this policy, uncheck the box.)

The page refreshes, and a message at the top confirms the change you have made.

To enable or disable the Auto-Verify policy for an existing unit through 3BM

- 1 At the main 3BM screen, select the unit by highlighting it and pressing **Enter**.
An asterisk appears in the left-most column to indicate that it is selected.
- 2 Tab to the **Maintain Unit** button and press **Enter**.
- 3 On the pop-up menu, select **Configure** and press **Enter**.
- 4 In the **Configure Disk Array** screen, **Tab** to the field **Auto-Verify**.
- 5 After completing any other changes you wish to make, tab to **OK** and press **Enter**.

Setting Overwrite ECC (Continue on Source Error When Rebuilding)

The **Overwrite ECC (Continue on Source Error When Rebuilding)** policy is available for units which are redundant. (For units which are not redundant, this option is not shown on the screen.) When this policy is set, ECC (Error Correcting Code) errors are ignored when they are encountered during a rebuild. (ECC errors are typically defects that have been detected in the drive since initialization.) When this policy is not set, if a unit is rebuilding, the rebuild will abort when it encounters an ECC error and the unit will be set back to Degraded.

Since enabling this policy could result in the loss of some source data in the event of source errors, the default is to not enable this policy. Select this option only if you want to ensure that a rebuild will complete successfully without manual intervention. If the rebuild fails and **Overwrite ECC (Continue on Source Error When Rebuilding)** is not selected, then you have the option to start another rebuild manually. After completing a rebuild with this policy enabled, it is recommended that you execute a file system check when the rebuild completes.

- Under **FreeBSD** use the fsck command.
- Under **Linux** use the fsck command.
- Under **Mac OS X**, you can use the First Aid tab in the Disk Utility—select the disk on the left and then click **Verify Disk**. If verification encounters problems, you can then use the **Repair Disk** option on the same screen.
- Under **OpenSolaris** you should follow your operating system's guide to perform a file system check.
- Under **VMware** you should follow your operating system's guide to perform a file system check.
- Under **Windows**, you can do this by right-clicking on the Drive and choosing Properties; then on the Tools tab, click Check Now.

To set the Overwrite ECC policy in 3DM2

- 1 Choose **Management >> Controller Settings** from the menu bar in 3DM2.
- 2 In the **Unit Policies** section of the Controller Settings page, check the boxes to select the policies you want to be in effect for each unit

The page refreshes, and a message at the top confirms the change you have made.

To set the Continue on Source Error When Rebuilding policy in 3BM

- 1 At the main 3BM screen, select the unit by highlighting it and pressing **Enter**.

An asterisk appears in the left-most column to indicate that it is selected.
- 2 Tab to the **Maintain Unit** button and press **Enter**.
- 3 On the pop-up menu, select **Configure** and press **Enter**.
- 4 In the **Configure Disk Array** screen, **Tab** to the field **Continue on Source Error When Rebuilding**.
- 5 Press **Enter** to display the choices, use the **arrow keys** to select the setting you want (Enabled or Disabled), and press **Enter** again to choose it.
- 6 **Tab** to the **OK** button and press **Enter** to select it.

You return to the main 3BM screen.

- 7 When you are finished making changes, press **F8** to save them and exit 3BM.

Enabling and Disabling Queuing for a Unit

Some drives support command queuing, a feature that can result in increased performance for applications that require a lot of random access of data (usually server-type applications). This is accomplished by causing command reordering to be done on the drive.

In order to make use of command queuing, the feature must be enabled at both the drive and the controller. You can enable support for command queuing on a per-unit basis, as described below.

You can see whether command queuing is supported and enabled for a particular drive in the Drive Details window. For details, see “Drive Details window” on page 197.



Note: Not all drives support command queuing. If a drive does not support command queuing, the policy setting for the controller is ignored. Queuing information for SAS is not available.

To enable or disable queuing for a unit through 3DM2

- 1 Choose **Management >> Controller Settings** from the menu bar in 3DM2.
- 2 In the **Unit Policies** section of the Controller Settings page, enable queuing by checking the box under “Queuing” for the designated unit; disable it by unchecking the box.

The page refreshes, and a message at the top confirms the change that you have made.

To enable or disable queuing for a unit through 3BM

- 1 At the main 3BM screen, select the unit by highlighting it and pressing **Enter**. An asterisk appears in the left-most column to indicate that it is selected.
- 2 Tab to the **Maintain Unit** button and press **Enter**.
- 3 On the pop-up menu, select **Configure** and press **Enter**.
- 4 In the **Configure Disk Array** screen, Tab to the field **Drive Queuing Mode**.
- 5 Press **Enter** to display the choices, use the **arrow keys** to select the setting you want (Enabled or Disabled), and press **Enter** again to choose it.

- 6 **Tab** to the **OK** button and press **Enter** to select it.
You return to the main 3BM screen.
- 7 When you are finished making changes, press **F8** to save them and exit 3BM.

Setting the StorSave Profile for a Unit

You can set the desired level of data protection versus performance for a unit by selecting the StorSave Profile. Three profiles are provided: *Protection* (maximum data protection), *Performance* (maximum performance, less data protection), and *Balanced* (a middle ground). The default is *Balanced*.

About StorSave Profile Levels

The three profiles automatically adjust several different factors that affect protection and performance on a per unit basis. These are summarized in the table below and further explained after the table.

Table 9: StorSave Profile Definitions

	Protection	Balanced (Default)	Performance
Definition	Maximum data protection, but slower performance.	More data protection than <i>Performance</i> but less data protection than <i>Protection</i> .	Maximum performance for the unit, but less data protection.
FUA (Force Unit Access)	Honor FUA (If no BBU is present) Ignore FUA (If BBU is present)	Honor FUA (If no BBU is present) Ignore FUA (If BBU is present)	Ignore FUA
Write Journaling	Enabled	Disabled, if no BBU present. (Enabled, if BBU is present.)	Disabled (If BBU is present, this essentially disables the BBU for this unit.)
Disable Cache on Degrade	Enabled	Disabled	Disabled

- **FUA (Force Unit Access).** The FUA bit is a way that the RAID controller or a program (such as a database program) can ensure that data is actually written to the disk drive media, and is not stored in cache. When a write command has the FUA bit set, then the disk drive will only issue “command complete” to the controller once the data is written to media. When performance is considered more important than protection, it may be desirable to ignore the FUA bit.

The Protection and Balanced profiles honor FUA commands if no BBU is present; the Performance profile ignores them regardless of whether a BBU is present.

If you use a battery backup unit (BBU), FUA is ignored, because the BBU preserves the contents of the controller cache memory for a limited period of time (up to 72 hours), in the event of a power failure.

- **Write Journaling.** Write journaling tracks the writing of data to disk and preserves a copy of data that has not yet been written to the disk media. Following a power failure or in the event of accidental drive removal and reinsertion, the firmware can recover the unit without data loss. All pending writes sitting in the controller cache are replayed after power is restored or the drive is reinserted and are flushed from the controller to the drive.

Using write journaling helps protect your data, however it can have an impact on performance.

The Protection profile always enables write journaling and the Performance profile always disables write journaling, regardless of the presence of a BBU. The Balanced Profile disables write journaling if no BBU is present, and enables write journaling if a BBU is present.

If write journaling is disabled and a BBU is present, then it is as if the BBU was disabled for that unit.

- **Write cache disabled on degrade.** In the event that a unit degrades, the use of write cache can be disabled until the unit is rebuilt. Once the unit is rebuilt, the write cache will automatically be re-enabled.

The Protection profile enables this feature, so that write cache is disabled in the event a unit degrades; the Performance and Balanced profiles disable this feature, so that write cache continues to be enabled.

Setting the StorSave Profile through 3DM2

In 3DM2, the StorSave Profile is a unit policy that can be set on the **Controller Settings** page.

To set the StorSave profile through 3DM2

- 1 Choose **Management >> Controller Settings** from the menu bar in 3DM2.
- 2 In the **Unit Policies** section of the Controller Settings page, select the profile you want to use from the drop-down list in the StorSave column.

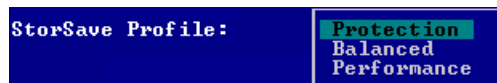
The page refreshes, and a message at the top confirms the change you have made.

Setting the StorSave Profile through 3BM

In 3BM, the StorSave Profile is set on the **Configure Disk Array** screen.

To set the StorSave Profile through 3BM

- 1 At the main 3BM screen, select the unit by highlighting it and pressing **Enter**.
An asterisk appears in the left-most column to indicate that it is selected.
- 2 Tab to the **Maintain Unit** button and press **Enter**.
- 3 On the pop-up menu, select **Configure** and press **Enter**.
- 4 In the **Configure Disk Array** screen, **Tab** to the field **StorSave Profile**.
The current setting—Protection, Balanced, or Performance—is shown.
(The default setting is Balanced.)
- 5 Press **Enter** to display the choices, use the **arrow keys** to select the setting you want, and press **Enter** again to choose it.



- 6 **Tab** to the **OK** button and press **Enter** to select it.
You return to the main 3BM screen.
- 7 When you are finished making changes, press **F8** to save them and exit 3BM.

Rapid RAID Recovery

The Rapid Raid Recovery feature increases the speed with which a redundant unit can be made redundant again when a rebuild is required. It can also increase the speed of verification or initialization that may occur in the event of an unclean shutdown.

Rapid RAID Recovery is possible because the firmware maps the unit, and tracks the areas of the unit where write activity occurs. Then, if a rebuild, initialization, or verify is required, the controller only has to address the active areas. The fewer active areas, the faster the rebuild, initialize or verify.

Since the units are mapped out and tracked from the creation of the unit, this feature can only be enabled during unit creation. Also, once disabled, it cannot be re-enabled.

The more space is available on a unit, the more benefit you will see in the event of a rebuild, if you enable Rapid RAID Recovery. If all of a unit's capacity is being used, you may not see reduction of rebuild speed when using

Rapid RAID Recovery. However, Rapid RAID Recovery still provides benefits to unit verification and to initialization after an unclean shutdown, regardless of the disk usage.

Possible settings are **All** (labeled Fast Rebuild/Shutdown in 3BM), **Rebuild** or **Disable**. **All** will apply the policy to both rebuilds and unclean shutdowns. **Rebuild** will apply only to rebuilds. **Disable** means that rebuilds, initializations and verifies will take place on the entire unit, not just the active sections. The default setting is **All**.

There is some system overhead from setting rapid recovery to **All**. If you have a BBU, you can set rapid recovery to **Rebuild**, as a BBU provides protection against data loss in the event of an unclean shutdown.

Some limitations of Rapid RAID Recovery:

- Units with Rapid RAID Recovery enabled will not be readable if moved to controllers using pre-9.5.1 firmware. If you wish to move the unit to a controller with pre-9.5.1 firmware, you must first disable Rapid RAID Recovery.
- Units created on controllers with pre-9.5.1 firmware will not be able to take advantage of Rapid RAID Recovery when the controller is updated to 9.5.1 or later. These units will show Rapid RAID Recovery as disabled.
- Since the Rapid RAID Recovery feature tracks areas of the unit where write activity occurs, file systems such as FAT, FAT32, NTFS, and XFS are ideally suited to this implementation. For details on other file systems, search the LSI KnowledgeBase for keyword 15462 at [:http://kb.lsi.com](http://kb.lsi.com). Protection against unclean shutdowns to provide a fast verification and initialization is the same regardless of the file system.

Changing or disabling Rapid RAID Recovery

Rapid RAID Recovery can only be enabled (that is - set to All or Rebuild) when the unit is created. You can change between All and Rebuild at any time. However, if you disable Rapid RAID Recovery, you cannot then enable it.

To change or disable Rapid RAID Recovery for an existing unit through 3DM2

- 1 Choose **Management >> Controller Settings** from the menu bar in 3DM2.
- 2 In the **Unit Policies** section of the Controller Settings page, select **All**, **Rebuild**, or **Disable** from the Rapid RAID Recovery dropdown menu.

- 3 Click OK when 3DM2 asks you to confirm your selection.

The page refreshes, and a message at the top confirms the change that you have made.

To change or disable Rapid RAID Recovery for an existing unit through 3BM

- 1 At the main 3BM screen, select the unit by highlighting it and pressing **Enter**.

An asterisk appears in the left-most column to indicate that it is selected.

- 2 Tab to the **Maintain Unit** button and press **Enter**.

- 3 On the pop-up menu, select **Configure** and press **Enter**.

- 4 In the **Configure Disk Array** screen, **Tab** to the field **Rapid RAID Recovery** and select **Fast Rebuild/Shutdown**, **Rebuild**, or **Disable**.

A warning message appears, asking you to confirm your selection.

- 5 Type 'Y'.

- 6 Make any other unit configuration changes you wish to implement and press **Enter**.

Changing An Existing Configuration by Migrating

You can convert one RAID configuration into another while the unit is online. This process is known as RAID Level Migration (RLM).

You can use RAID Level Migration to make two main types of configuration changes:

- RAID Level (for example, a RAID 1 to a RAID 5)
- Unit Capacity Expansion (for example, adding a 4th drive to a 3-drive RAID 5)

You can also use RLM to change the stripe size of a unit.



Note: A unit being migrated can still be used (I/O still continues), however the performance will be affected while the migrating task is active. You can control how much effect this has on performance by setting the background task rate. For more information, see "Setting Background Task Rate" on page 162.

This section includes the following topics about changing existing configurations:

- RAID Level Migration (RLM) Overview
- Changing RAID Level
- Expanding Unit Capacity
- Informing the Operating System of Changed Configuration

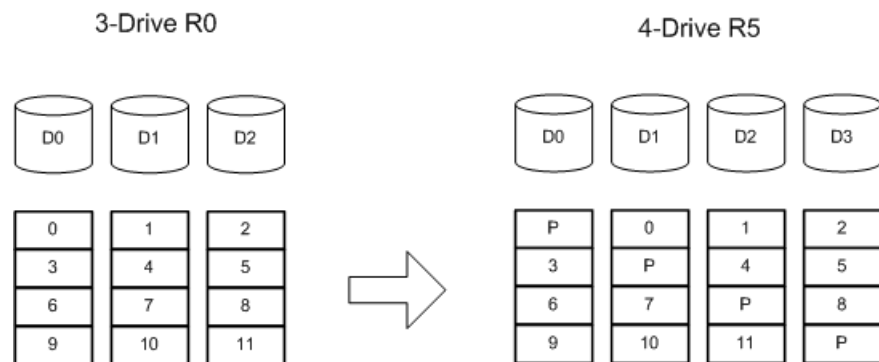
If you want to change the policy settings for an existing unit, there is no need to change the configuration. See “Setting Unit Policies” on page 100.

RAID Level Migration (RLM) Overview

RAID level migration is the process of converting one RAID configuration to another. When you migrate a unit to a different configuration, the user data on it is redistributed to the format of the new configuration. This data redistribution process is a background task, similar to the rebuild or verify processes.

Figure 62 shows an example of how data is reconfigured during a migration. In this example, the migration is from a 3-drive RAID 0 to a 4-drive RAID 5, with both having the same stripe size. As can be seen, every piece of user data is moved from its original physical location.

Figure 62. RAID Level Migration Example



Typically, a unit is reconfigured with the same or more storage capacity. Sometimes additional drives are added. The following table shows valid reconfigurations, some of which will require the addition of more drives.

Table 10: Valid Migration Paths

Source	Destination							
	R0	R1	R5	R6	R10	R50	Single	Spare
R0	Yes	No	Yes	Yes	Yes	Yes	No	No
R1	Yes	No	Yes	Yes	Yes	Yes	Yes	No
R5	Yes	No	Yes	Yes	Yes	Yes	No	No
R6	Yes	No	Yes	Yes	Yes	Yes	No	No
R10	Yes	No	Yes	Yes	Yes	Yes	No	No
R50	Yes	No	Yes	Yes	Yes	Yes	No	No
Single	Yes	Yes	Yes	Yes	Yes	Yes	No	No
Spare	No	No	No	No	No	No	No	No



Note: Rapid RAID Recovery will be disabled on any unit that is migrated.



Warning: If you are booted from a mirror (RAID 1 unit), never split it into 2 single (identical) drives. Once the unit is split, any pending writes cannot be written to the second drive. In addition, the file system on the drive will not be clean. Instead, shut down the system, replace one of the drives, and start the rebuild from 3BM.



Note: You can only migrate a unit to a RAID level that has the same or more capacity as the existing one. A four-drive RAID 5 unit can migrate to a four-drive RAID 0, but a three-drive RAID 0 unit cannot migrate to a three-drive RAID 5, without adding another drive, due to the need for additional storage capacity for parity bits.

Changing RAID Level

You can use migrate to change the RAID level of an existing unit while the unit is online, without experiencing any data loss. When you change a RAID level, you may also add one or more drives to the unit. You can also migrate to change the unit's stripe size. For example, a four-drive RAID 5 with a 64KB

stripe size can be migrated to a four-drive RAID 5 with 256KB stripe size. The steps below describe how to change a RAID level in 3DM2.



Note: Once migration starts, the unit stays in the migrating state until the migration process is complete. The migration process cannot be aborted, and must be allowed to finish before a rebuild or verify to the unit is permitted.



Warning: It is important that you allow migration to complete before removing any drives that are involved in the migration. Removing drives from the unit during migration may cause the migration process to stop, and can jeopardize the safety of your data.

To change the RAID level of a unit

- 1 In 3DM2, choose **Management >> Maintenance**.
- 2 In the Unit Maintenance table on the Maintenance Page, select the unit for which you wish to change the RAID level, by checking the box next to the Unit ID.



Note: The unit to be migrated must be in a normal state (not degraded, initializing, or rebuilding) before starting the migration.

- 3 Click the **Migrate Unit** button.
The Migrate dialog box appears.
- 4 Select any drives to be added to the unit.
- 5 Select the new RAID level.
- 6 Optionally, select a new Stripe size.
- 7 Click **OK**.
The Maintenance page updates to show the new unit and the Migration progress.
- 8 Inform the operating system of the change, as described below under “Informing the Operating System of Changed Configuration”.

Expanding Unit Capacity

You can expand a unit's capacity by adding one or more drives to it without changing the RAID level, except for singles and RAID 1 units. (Since a single

can only have one drive, and a RAID 1 can only have two drives, if you add a drive to either, the RAID level must be changed.)

For example, for a RAID 5 with 3 drives, you can change the capacity by adding a fourth drive.

Expanding unit capacity can be accomplished while the unit is online, without experiencing any data loss. This process is also referred to as Online Capacity Expansion (OCE).

To expand a unit's capacity

- 1 In 3DM2, choose **Management >> Maintenance**.
- 2 In the Unit Maintenance table on the Maintenance Page, select the unit you wish to expand by checking the box next to the Unit ID.
- 3 Click the **Migrate Unit** button.
The Migrate dialog box appears, listing the drives which can be added to the unit.
- 4 Select the drives(s) you wish to add to the unit by checking the Port ID box next to each one.
- 5 If desired or necessary, select the appropriate RAID level.
- 6 Click **OK**.
The Maintenance page updates to show the newly reconfigured unit. The Status column title indicates that Migration is in progress.
- 7 If you booted from the unit that is being migrated, when migration is complete, reboot your system. Then turn to Step 4 under "Informing the Operating System of Changed Configuration" on page 119.
- 8 After the migration is complete, inform the operating system of the change, as described below.

You can check the status of the migration on the Maintenance page.

Informing the Operating System of Changed Configuration

After you change the configuration of a unit, you must inform the operating system of the change, and you may need to re-partition the unit.

The easiest way to see the change in capacity is to reboot the system. If you are not booted from the unit be sure the unit is not mounted and not in use. You should follow the specific operating system guide on how to unmount the

volume. Then use 3DM2 or CLI to remove the unit. Then rescan so the operating system can recognize the new capacity.

In addition, in order to use the new capacity, you need to either resize the existing partition or add a new partition.

To inform the operating system that a unit has been changed

- 1 If the unit you reconfigured is the boot unit, restart the system and skip to Step 3.

If the unit you reconfigured is secondary storage, unmount the file system from the unit.

- Under **FreeBSD**, from a command prompt, type `sync <enter>`, `sync <enter>`, `sync <enter>`.

You can then unmount the unit with this command: `umount <mount location>`

- Under **Linux**, from a command prompt, type `sync <enter>`, `sync <enter>`, `sync <enter>`.

You can then unmount the unit with this command: `umount <mount location>`

- Under **Mac OS**, Unmount the file system from the unit.

Launch the Macintosh Disk Utility, select the unit, and click the Unmount button the toolbar, or select the icon for the unit on the desktop and drag it to the trash.

- Under **OpenSolaris**, Please consult your system documentation and the LSI KnowledgeBase for more information.
- Under **VMware**, Please consult your system documentation and the LSI KnowledgeBase for more information.
- Under **Windows**, go to **Start >> Administrative Tools >> Computer Management**, and select **Disk Management**. Remove the logical drive letter for the unit.

- 2 In the software, remove and rescan the controller, in order to update unit information.
 - a In 3DM2 choose **Management >> Maintenance** and select the appropriate unit.
 - b Click the **Remove Unit** button.
 - c After the unit has been removed, click the **Rescan** button. The new unit capacity displays.
- 4 Resize the partition and file system or create a new partition.

Under **Windows**, use the disk management utility to determine whether the disk is a basic disk or a dynamic disk.

- Go to **Administrative Tools >> Computer Management**, and then select **Disk Management** in the list on the left.

Only dynamic disks can be expanded with Windows Disk Management. If the unit is shown as a basic disk, right-click on the disk icon and change it to a dynamic disk.

Older Windows systems cannot convert basic disks into dynamic disks after the file system has been created.

- If the unit is shown as a dynamic disk, right-click on it and choose **Extend Volume** to launch the Extend Volume wizard.

In other operating systems, the tools to expand the partition and file system can vary, depending on the kernel version and file system that you are using. Please consult your system documentation and the LSI KnowledgeBase for more information.

Deleting a Unit

You delete a unit—either an array of disks, or a Single Disk—when you want to reconfigure the unit or use the drives for other purposes.

After you delete a unit, the drives appear in the list of Available Drives.



Warning: When a unit is deleted, all of the data on that unit will be lost. The drives cannot be reassembled into the same unit because the data on it is erased. If you want to reassemble the drives into the same unit on another controller, use the **Remove Unit** button in 3DM2 instead of the **Delete Unit** button. Or, you can shut down the computer and physically move the drives (or the enclosure containing the drives) to another 3ware RAID controller. When you restart your system, the controller will recognize the unit. For more information see “Moving a Unit from One Controller to Another” on page 127.

If you have incomplete drives, or drives that appear with a message such as “Unsupported DCB,” indicating that they were previously part of a unit on a 3ware 7000/8000 series controller, they must be deleted before you use them. (If you want to move a unit from a 7/8000 controller to a 9750 controller, you must convert the drives first. For more information, see “Moving a Unit from One Controller to Another” on page 127.)

Deleting a Unit through 3DM2

In 3DM2, the command for deleting a unit is on the **Maintenance** page. Be sure to follow steps 1 through 3 in the instructions before using the Delete command.

To delete a unit through 3DM2

- 1 Make sure the operating system is not accessing the unit you want to delete.

For example, make sure you are not copying files to the unit, and make sure that there are no applications with open files on that unit.

If you are not successful at deleting your unit, usually this is because there is currently I/O going to that unit, a message informs you that the unit is busy. In that case, you should stop any I/O first.

- 2 Backup any data you want to keep.
- 3 Unmount the unit.

Make sure the unit is not mounted and not in use. You should follow the specific operating system guide on how to unmount the volume before you delete a unit.

This step is very important. If a unit is not unmounted and you delete it, it is the equivalent of physically yanking a hard drive out from under the operating system. You could lose data, the system could hang, or the controller could reset.

- Under **FreeBSD**, you can unmount the unit with this command:
umount <mount location>
- Under **Linux**, you can unmount the unit with this command:
umount <mount location>
- Under **Mac OS**, launch the Macintosh Disk Utility, select the unit, and click the Unmount button on the toolbar, or select the icon for the unit on the desktop and drag it to the trash.
- Under **OpenSolaris**, please consult your system documentation and the LSI KnowledgeBase for more information.
- Under **VMware**, please consult your system documentation and the LSI KnowledgeBase for more information.
- Under **Windows**, go to **Start >> Administrative Tools >> Computer Management**, and select **Disk Management**. Remove the logical drive letter for the unit. (under Windows it is not necessary to unmount the device before deleting the unit, because the API code correctly does this for you.)

- 4 In 3DM2, choose **Management >> Maintenance**.

- In the Unit Maintenance section of the Maintenance page, select the unit you want to remove and click **Delete Unit** (Figure 63).

Figure 63. Deleting a Unit Through 3DM2

LSI 3DM2™ U64Vista-PC (Windows Vista Ultimate x64 Edition Service Pack 2) Administrator logged in Logout

Summary Information Management Monitor 3DM2 Settings Help

Refresh Maintenance Select Controller Controller ID 0 (9750-4)

Rescan Controller (This will scan all ports for newly inserted drives/units)

Unit Maintenance (Controller ID 0)

Unit	Drives	RAID	Capacity	Status	Actions
Unit 0	3 drives	RAID 6 Zygotte 1	100.55 GB	OK	
VPort 0	SAMSUNG HD160JJ	149.05 GB	OK	[Remove Drive]	
VPort 1	SAMSUNG HD160JJ	149.05 GB	OK	[Remove Drive]	
VPort 2	SAMSUNG HD160JJ	149.05 GB	OK	[Remove Drive]	
Unit 1	1 drive	RAID 6 Zygotte 2	100.55 GB	OK	
VPort 3	SAMSUNG HD160JJ	149.05 GB	OK	[Remove Drive]	

Verify Unit Rebuild Unit Migrate Unit Remove Unit **Delete Unit**

*Before removing or deleting a unit, make sure there is no I/O on the unit and unmount it

Available Drives (Controller ID 0)

NO DRIVES

- When a message asks you to confirm, click **OK**.

Configuration information associating the drives with the unit is deleted, and the individual drives appear in the Available Drives list (Figure 64). You can now use them as part of another unit, or designate them as Spares, for use in a rebuild.

Figure 64. Unit Successfully Deleted through 3DM2

LSI 3DM2™ U64Vista-PC (Windows Vista Ultimate x64 Edition Service Pack 2) Administrator logged in Logout

Summary Information Management Monitor 3DM2 Settings Help

Refresh Maintenance Select Controller Controller ID 0 (9750-4)

Successfully deleted unit(s) 1

Rescan Controller (This will scan all ports for newly inserted drives/units)

Unit Maintenance (Controller ID 0)

Unit	Drives	RAID	Capacity	Status	Actions
Unit 0	3 drives	RAID 6 Zygotte 1	100.55 GB	OK	
VPort 0	SAMSUNG HD160JJ	149.05 GB	OK	[Remove Drive]	
VPort 1	SAMSUNG HD160JJ	149.05 GB	OK	[Remove Drive]	
VPort 2	SAMSUNG HD160JJ	149.05 GB	OK	[Remove Drive]	

Verify Unit Rebuild Unit Migrate Unit Remove Unit Delete Unit

*Before removing or deleting a unit, make sure there is no I/O on the unit and unmount it

Available Drives (Controller ID 0)

VPort	Model	Capacity	Type	Phy	Slot	Status
<input type="checkbox"/>	0	SAMSUNG HD160JJ	149.05 GB	SATA	0	OK

(De)Select All Drives

Create Unit Remove Drive Set Spare(s) Clear Configuration

Deleting a Unit through 3BM

In 3BM, the command for deleting a unit is on the main 3BM screen.

To delete a unit through 3BM

- 1 At the main 3BM screen, select the unit in the list of Exportable Units by highlighting it and pressing **Enter** or **Space**.

An asterisk appears in the left-most column to indicate that it is selected.

- 2 **Tab** to the **Delete Unit** button and press **Enter**.



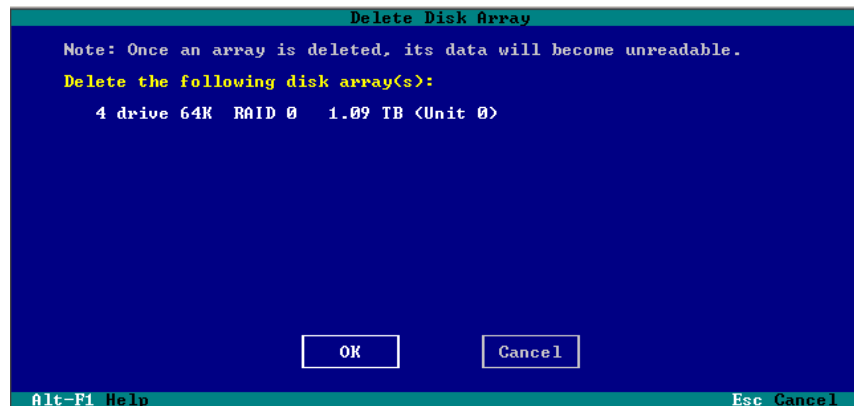
Note: If you want to delete an incomplete drive or unusable unit, or a drive that appears with a message such as “Unsupported DCB,” select it in a similar manner and then select **Delete Unit**, even though it appears in the list **Incomplete Drives and Others**.



Warning: Any data on the unit will be lost once the unit is deleted. Backup any data that you want to keep.

- 3 On the **Delete Disk Array** screen, review the information about the unit to make sure it is the one you want to delete.

Figure 65. Deleting a Unit in 3BM



- 4 **Tab** to the **OK** button and press **Enter**.

You return to the main 3BM screen, and the drives associated with the unit now appear in the list of Available Drives.



Remember: The unit is not actually deleted and no data is overwritten until you press the **F8** key to save your changes, or press **Esc** and select **Yes** when asked if you want to save.

- 5 **Press F8** to save your changes, or press **Esc** and then **Yes**.

Removing a Unit

Removing a unit through software (also known as 'array roaming') keeps the data intact on the unit. It allows you to move the unit to another controller or to store the drives for safekeeping purposes.

Removing a unit is different than deleting a unit. Deleting a unit will destroy the data on the unit.



Warning: It is important to remove the unit through software, before removing it physically. Failure to do so could result in a system crash or hang and may even corrupt the data and the unit configuration from being reassembled later.

Power-down your system before physically removing any drive that is not in a hot swap bay.



Note: You can also remove a drive, if you want to force a degrade on a redundant unit, or if you want to remove a drive from the "Available Drives" list so that you can then remove it from the system. For more information, see "Removing a Drive" on page 130.

Removing a Unit Through 3DM2

In 3DM, the command for deleting a unit is on the **Maintenance** page. Be sure to follow steps 1 and 2 in the instructions before using the Remove command.

To remove a unit through 3DM2



Note: If your drives are not in hot swap bays, you do not need to remove a unit via 3DM2. Simply power down the system and remove the applicable drives. Refer to your system's user guide for details on removing fixed disks. If your drives are in hot swap bays, follow the steps below.

- 1 Make sure the operating system is not accessing the unit you want to remove.

For example, make sure you are not copying files to the unit, and make sure that there are no applications with open files on that unit.

If you are not successful at removing your unit, usually this is because there is currently I/O going to that unit, a message informs you that the unit is busy. In that case, you should stop any I/O first.

- 2 Unmount the unit.

Make sure the unit is not mounted and not in use. You need to follow the specific operating system guide on how to unmount the volume before you remove a unit.

This step is very important. If a unit is not unmounted and you remove it, it is the equivalent of physically yanking a hard drive out from under the operating system. You could lose data, the system could hang, or the controller could reset.

- Under **FreeBSD**, you can unmount the unit with this command:
umount <mount location>
- Under **Linux**, you can unmount the unit with this command:
umount <mount location>
- Under **Mac OS**, launch the Macintosh Disk Utility, select the unit, and click the Unmount button the toolbar, or select the icon for the unit on the desktop and drag it to the trash.
- Under **OpenSolaris**, please consult your system documentation and the LSI KnowledgeBase for more information.
- Under **Windows**, go to **Start >> Administrative Tools >> Computer Management**, and select **Disk Management**. Remove the logical drive letter for the unit. (under Windows it is not necessary to unmount the device before deleting the unit, because the API code correctly does this for you.)
- Under **VMware**, please consult your system documentation and the LSI KnowledgeBase for more information.

- 3 In 3DM2, choose **Management >> Maintenance**.
- 4 In the **Unit Maintenance** table on the Maintenance page, select the unit you want to remove and click **Remove Unit**.
- 5 When a message asks you to confirm, click **OK**.

The unit number and information is removed from the **Maintenance** page in 3DM2.

The operating system is notified that the unit was removed. In Linux the device node associated with this unit is removed. In Windows the Device Manager will reflect the changes under the disk drives icon.

You can now physically remove the drives and move them to another controller. If the drive is in a hot swap bay, you can do this without shutting down the system. If the drive is not in a hot swap bay, power-down the system and ground yourself before making changes to the hardware.

If you change your mind before physically removing the drives and want to reuse the drives and unit on the current controller, just click **Rescan Controller**.

Removing a Unit Through 3BM



Note: Even though removing a unit is supported in 3BM, you can also simply power down to remove the applicable drives since you are not booted yet.

To remove a unit through 3BM

- 1 If your drives are not in hot swap bays, you do not need to remove a unit via 3BM. Simply power down and remove the applicable drives. Refer to your system's user guide for details on removing fixed disks.



Warning: Physically removing drives which are not in hot swap bays can result in a system hang or may even damage the system and the drive.

- 2 At the main 3BM screen, highlight the unit you want to remove and press **Enter** to select it.

An asterisk appears in the left-most column to indicate that the unit is selected.

- 3 Tab to the **Maintain Unit** button and press **Enter**.

- 4 In the pop-up menu, select **Remove** and press **Enter**.

You can now physically remove the drives and move them to another controller. If your drives are in hot swap bays, you can do this without shutting down the system.

Moving a Unit from One Controller to Another

After you have configured a unit on a 3ware 9750 controller, you can move it to a different 3ware 9750 controller, and retain the configuration on the new controller. This is referred to as “array roaming.”

When connecting the unit to the new controller, you do not have to physically connect the drives to the same physical slots to which they were connected on the previous controller. The firmware will still recognize the unit. This feature is referred to as “disk roaming.”

3DM2 includes two features that help you move a unit without powering down the system, allowing you to hot swap the unit. The Remove Unit feature lets you prepare a unit to be disconnected from the controller, and the Rescan feature checks the controller for drives that are now connected, and updates the 3DM2 screens with current information. For details, see “Removing a Unit” on page 125 and “Rescanning the Controller” on page 132.



Note: Moving a unit to another controller while the unit is in the migration state is supported with one restriction. If the unit was in the middle of the migration process and the controller was shutdown uncleanly, the unit cannot be moved to another controller until the unit has recovered from the unclean shutdown. This may require initializing, verifying, or rebuilding the unit.

Moving Units from an Earlier 9000 Series to a 9750 Controller

If you are moving units from a 9550SX or later 9000-series controller to a 9750 controller, the process is a little different from when you are moving units from one 9750 to another. The steps you follow depend on whether you are booting from the drives attached to the older controller, or whether they are being used for secondary storage.



Note: Only SATA-2 drives are supported on the 9750. You cannot move SATA-1 drives.

To move a bootable unit from an earlier 9000 series controller to a 9750 controller

- 1 If you are working with a Linux or OpenSolaris system, skip to step 2.

If you are working with a Windows system:

- a Power down the computer.
- b Install the 9750 controller in the computer, leaving the original controller installed and its drives attached.
- c Boot to the operating system.

- 2 Install the driver for the 9750 RAID controller.

If you are using Linux, you may also need to update the initial RAM disk. For more information, see “Updating the 3ware Driver Under Red Hat or Fedora Core” on page 321 or “Updating the 3ware Driver Under Red Hat or Fedora Core” on page 321.

- 3 Power down the computer.
- 4 Remove the original controller.
- 5 If you are working with a Linux or OpenSolaris system, install the 9750 controller.
- 6 Attach the drives that were on the original controller to the 9750 controller.

- 7 Power up the computer and verify that the upgrade is complete. (The existing units should be available for use.)
- 8 Remove old 3DM2 and CLI files and install new versions.

To move a secondary storage unit from an earlier 9000 series controller to a 9750 controller

- 1 Power down the computer.
- 2 Remove the 9690SA, 9650SE, or 9550SX controller.
- 3 Install the 9750 controller in the computer.
- 4 Attach the drives that were on the original controller to the 9750.
- 5 Boot to the operating system.
- 6 Install the driver for the 9750.

If you are using Linux, you may also need to update the initial RAM disk. For more information, see “Updating the 3ware Driver Under Red Hat or Fedora Core” on page 321 or “Updating the 3ware Driver Under SUSE” on page 323. .

- 7 Reboot if you are prompted to do so by the operating system.
- 8 Remove old 3DM2 and CLI files and install new versions.

Adding a Drive

If you have a hot swap bay or an enclosure with removable trays, you can add a drive to your system and make it available through 3DM2 without powering down the system.

Without hot swap bays, you should not add a drive via 3DM2. Instead, power down the system and add the applicable drives.



Warning: Physically adding a drive without using a hot swap bay and without powering down your system can result in a system hang or may even damage the system and the drive.



Note: When you add a drive to your system and connect it to the controller, it is automatically detected and listed in 3DM2. If it does not immediately display, or if it is part of a unit, you can use the rescan feature, as described below.

To add a drive

- 1 Insert the drive into the hot swap bay or into your enclosure.
For details, refer to the documentation for your enclosure.
- 2 In 3DM2, choose **Management >> Maintenance**.
- 3 On the Maintenance page, click **Rescan Controller**.

The drive will appear in the list of available drives. You can now use it in a new RAID configuration, as part of an existing configuration, or as a replacement drive in the event that another drive degrades.

If you want to use this drive as a spare, see “Creating a Hot Spare” on page 97.

Removing a Drive

If you have hot swappable drives in a carrier or an enclosure and you want to physically remove a drive from your system without powering it down, you should first remove it through the 3ware software.

Follow this procedure if you know that a drive is developing a problem and you want to replace it, or to replace a drive which has already failed.



Warnings:

Physically removing a drive that is not in a hot swap bay or that is part of a non-redundant unit, can result in a system hang or may even damage the system and the drive.

The steps below will destroy any information that identifies this drive as part of a RAID unit. **Existing data on this drive will no longer be available.**



Notes:

If you want to remove a unit from your system and reassemble it in another system, do not follow these steps. Instead, turn to “Removing a Unit” on page 125.

If you physically remove a drive on a controller without first removing it in 3DM2, it will be listed as removed, however it will not be completely removed unless you Rescan the controller.

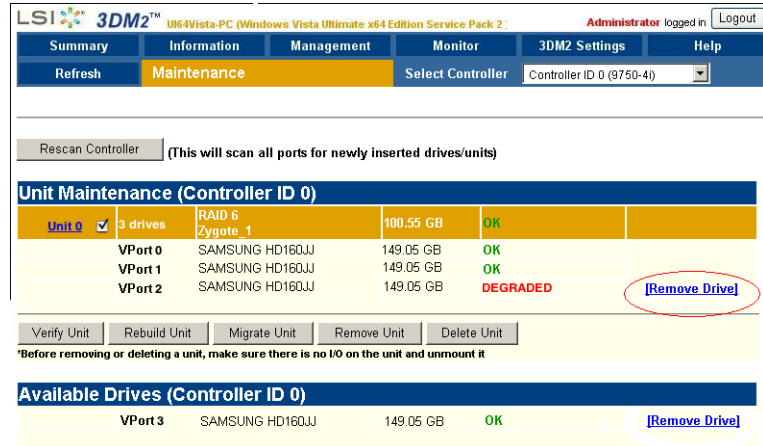
Drives that are part of a non-redundant or degraded unit cannot be removed.

To remove a drive

- 1 In 3DM2, choose **Management >> Maintenance**.
On the Maintenance page, **Remove Drive** links appear next to all drives that can be removed from units, and next to drives in the Available Drives list.

- 2 Locate the drive you want to remove and click the **Remove Drive** link (Figure 66).

Figure 66. Removing a Drive in 3DM2

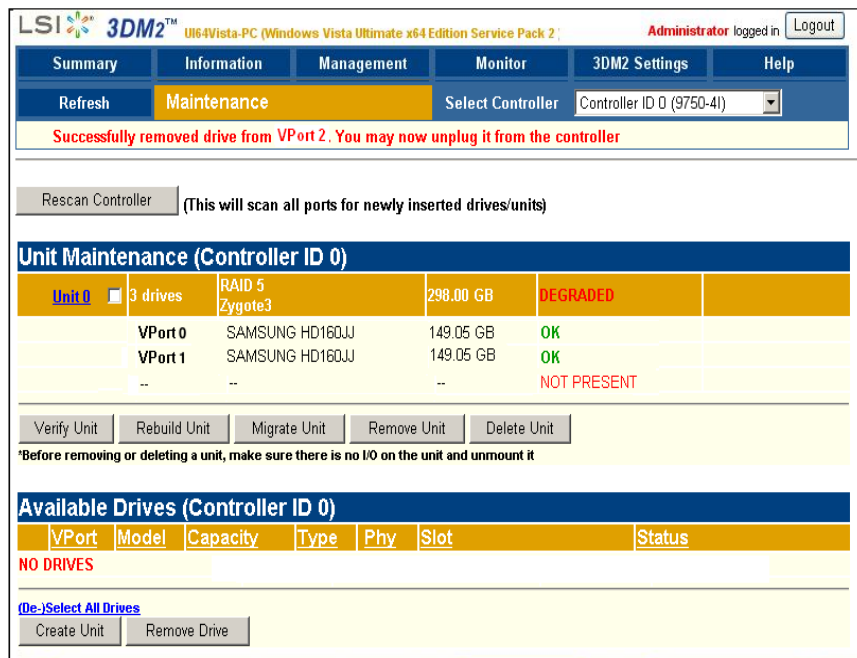


- 3 When 3DM2 asks you to confirm that you want to remove the drive, click **OK**.

You can now remove the drive from your system.

If you removed a drive that was part of a unit, the unit will become degraded, as shown in (Figure 67).

Figure 67. Result of Removing Drive from Unit in 3DM2



Rescanning the Controller

When you make a change by physically adding or removing drives or units, you can have 3DM2 rescan the controller to update the list of units and available drives shown on the **Maintenance** page.

This is useful in a variety of circumstances. For example, if you add new drives to the controller, you can make them available by rescanning the controller. Or if you turn on an enclosure after turning on your computer, you can use rescan to make the controller see the drives.

Rescanning checks all ports on the controller. It then updates the status of all attached disks, so if error conditions have been fixed, the status is updated to reflect that. For more details about how the Rescan feature works, see the information in the 3DM2 Reference section, under “Maintenance page” on page 208.

To rescan the controller through 3DM2

- 1 In 3DM2, choose **Management >> Maintenance**.
- 2 On the Maintenance page, click **Rescan Controller**.

3DM2 scans the controller for information about units and drives, and updates the information shown on the **Maintenance** page.

To rescan the controller through 3BM

- 1 From the main 3BM screen, press Alt-r.
You are warned that any configuration changes you have made in 3BM will be lost.
- 2 Type **Y** for Yes to rescan the controller.

Maintaining Units

3ware RAID controllers include a number of features in the firmware that help maintain the integrity of your drives, check for errors, repair bad sectors, and rebuild units when drives degrade. In addition, 3ware BIOS Manager (3BM) and 3ware Disk Manager 2 (3DM2) provide tools to let you check unit and drive status, and manually start background maintenance tasks.



Mac User Note: The 3ware BIOS Manager (3BM) tool is not available for Mac OS X users. Mac users need to use the 3DM2 tool.

3DM2 also lets you review alarms and errors and schedule background maintenance tasks. On Windows systems, the WinAVAlarm utility monitors the controller and will display a message window and give an audible alarm when events occur at or above the threshold you select for it.

Details about these features are described in this section, which is organized into the following topics:

- Checking Unit and Drive Status through 3DM2
 - Viewing a List of Drives
 - Enclosure Drive LED Status Indicators
 - Unit Statuses
 - Drive Statuses
- About Degraded Units
- About Inoperable Units
- Locating a Drive by Blinking Its LED
- Alarms, Errors, and Other Events
- Background Tasks
- Scheduling Background Tasks

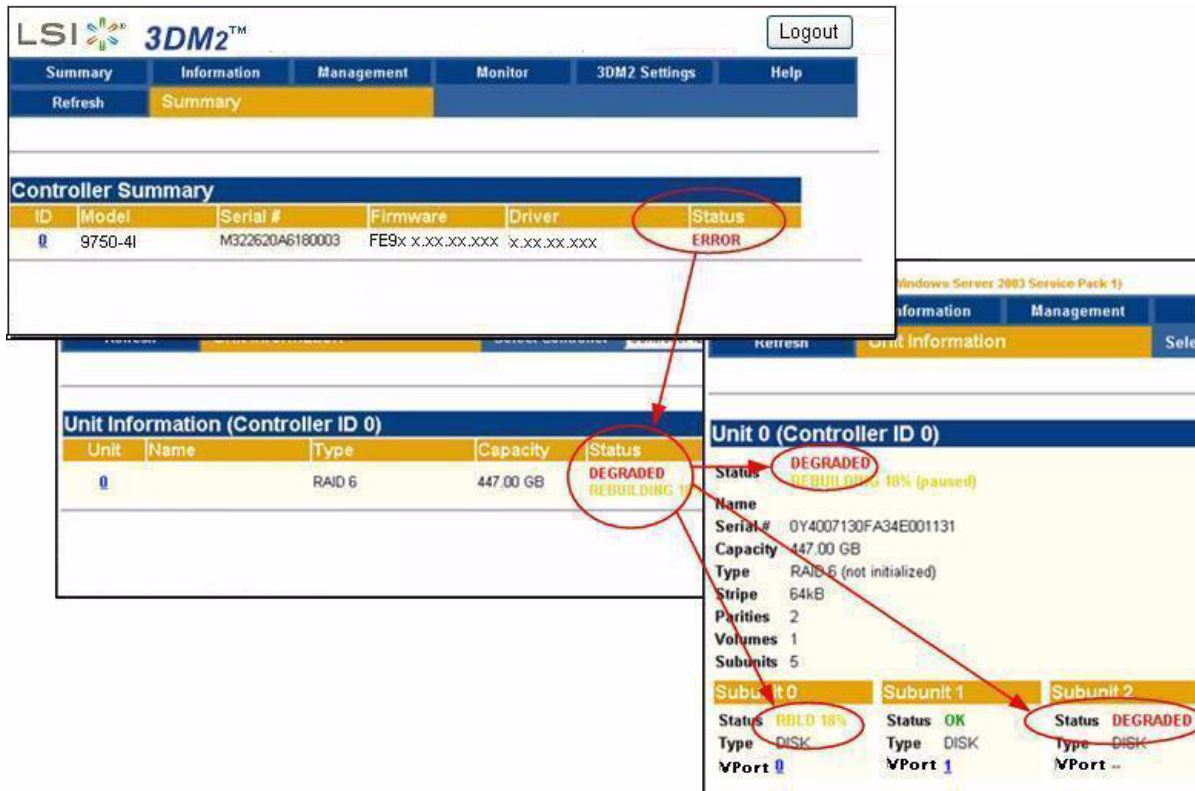
Checking Unit and Drive Status through 3DM2

The information screens in 3DM2 let you see both summary and detailed information about your 3ware RAID controller, configured units, and available drives. You can quickly see the status of your controller and drives, and drill down to find details about any units or drives that have problems.

A status column on the controller, unit, and drive information pages lets you quickly see whether everything is working (OK), performing a task (such as initializing, verifying, or rebuilding), or has a problem (error, degraded, or warning).

The next figure illustrates how you can drill down to get additional detail about units and drives in your system.

Figure 68. Drilling Down to Check Status Information



For some RAID levels (RAID 6, RAID 10, and RAID 50), a single RAID unit may have more than one status. For example, part of the unit could be rebuilding, while another part is degraded or initializing. When this is the case, you will see both statuses listed at the top unit level. When you drill in to see details, you will be able to see which the specific subunits or drives to which the status applies.

For an explanation of unit and drive status, see:

- “Unit Statuses” on page 137
- “Drive Statuses” on page 138

If you use a supported enclosure with enclosure services, the LEDs on your enclosure may also provide some status information. For details, see “Enclosure Drive LED Status Indicators” on page 136.

Viewing a List of Drives

You can see a list of drives connected to your 3ware RAID controller, and see additional detail about each of those drives.

To view a list of drives in 3DM2

- Choose **Information > Drive Information** from the main menu in 3DM2.

On the Drive Information page, you can access details about any of the drives listed by clicking the link for that drive in the **VPort** column.

For more information about the Drive Information page, see page 195.

Figure 69. Drive Information Page

Drive Information (Controller ID 0)								
VPort	Model	Capacity	Type	Phy	Slot	Unit	Status	Identify
0	MAXTOR ATLAS15K2_36SAS	34.25 GB	SAS	--	Enclosure 0 Slot 10	--	OK	<input type="checkbox"/>
1	MAXTOR ATLAS15K2_36SAS	34.25 GB	SAS	--	Enclosure 0 Slot 9	1	OK	<input type="checkbox"/>
2	SAMSUNG HD160JJ	149.05 GB	SATA	0	--	--	OK	<input type="checkbox"/>
3	MAXTOR ATLAS15K2_36SAS	34.25 GB	SAS	--	Enclosure 0 Slot 8	1	OK	<input type="checkbox"/>
4	MAXTOR ATLAS15K2_36SAS	34.25 GB	SAS	--	Enclosure 0 Slot 7	1	OK	<input type="checkbox"/>
5	MAXTOR ATLAS15K2_36SAS	34.25 GB	SAS	--	Enclosure 0 Slot 6	1	OK	<input type="checkbox"/>
6	MAXTOR ATLAS15K2_36SAS	34.25 GB	SAS	--	Enclosure 0 Slot 5	1	OK	<input type="checkbox"/>
7	SAMSUNG HD160JJ	149.05 GB	SATA	1	--	??	OK	<input type="checkbox"/>
8	MAXTOR ATLAS15K2_36SAS	34.25 GB	SAS	--	Enclosure 0 Slot 4	0	OK	<input type="checkbox"/>
9	MAXTOR ATLAS15K2_36SAS	34.25 GB	SAS	--	Enclosure 0 Slot 3	0	OK	<input type="checkbox"/>
10	MAXTOR ATLAS15K2_36SAS	34.25 GB	SAS	--	Enclosure 0 Slot 2	0	OK	<input type="checkbox"/>
11	MAXTOR ATLAS15K2_36SAS	34.25 GB	SAS	--	Enclosure 0 Slot 1	0	OK	<input type="checkbox"/>
12	MAXTOR ATLAS15K2_36SAS	34.25 GB	SAS	--	Enclosure 0 Slot 0	0	OK	<input type="checkbox"/>
13	SAMSUNG HD160JJ	149.05 GB	SATA	2	--	--	OK	<input type="checkbox"/>
14	SAMSUNG HD160JJ	149.05 GB	SATA	3	--	??	OK	<input type="checkbox"/>

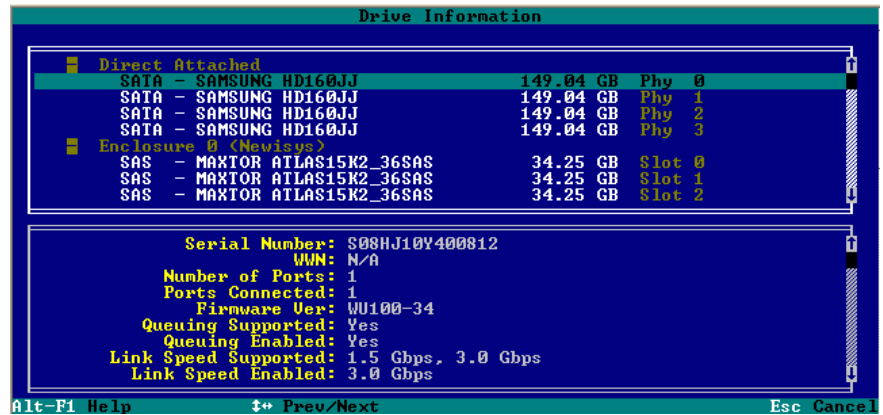
To view a list of drives in 3BM

- On the main 3BM screen, **Tab** to **Information** and press **Enter**.
- On the pop-up menu, select **Drives** and press **Enter**.
- On the Drive Information page, use the arrow keys to move from one drive to another.

Details about the selected drive are displayed in the bottom of the page.

Tip: You can scroll both sections of the Drive Information page to bring additional drive information or drives into view. Press **Tab** to move between the two sections.

Figure 70. Drive Information page (3BM)



Enclosure Drive LED Status Indicators

If you have a supported enclosure or chassis, the LEDs on your enclosure may be able to provide some status information about your drives and units. (You can find a list of supported enclosures from the Data & Interoperability tab, on http://www.lsi.com/channel/support/marketing_resources.)



Note: The following table is an example of how LEDs may be used. Check with your chassis or enclosure documentation for more details. Not all features may be supported or implemented in the same way on all chassis.

Table 11: Meaning of LED Colors and Behavior

Color	Drive Status
Solid green	OK
Blinking green	Identify This occurs when you have used the Identify command in 3DM2 to locate a particular drive or unit. (See "Locating a Drive by Blinking Its LED" on page 139.)
Black	No drive
Solid Amber	Hot spare
Blinking amber	Rebuilding The drive in this slot is part of a RAID unit that is currently rebuilding. You can continue to use the unit. For more information, see "Rebuilding Units" on page 154.

Table 11: Meaning of LED Colors and Behavior (continued)

Color	Drive Status
Solid red	Drive fault This drive has failed. You should replace it and rebuild the unit.
Blinking red	Predicted drive fault 3ware software predicts that this drive will fail soon. You may want to replace it.

Unit Statuses

The following is a list of unit statuses you may see in 3DM2:

- **OK.** The unit is optimal and is functioning normally.
- **Rebuilding.** The unit is in the process of writing data to a newly added disk in a redundant unit, in order to restore the unit to an optimal state. The unit is not fully fault tolerant until the rebuilding is complete. For more information, see “To verify a unit through 3BM” on page 153.
- **Rebuild-Paused.** The unit is set to rebuild, however scheduling is enabled, and the present time is not during a scheduled timeslot. Rebuilding will start at the next scheduled time slot. Rebuilds are also paused for up to ten minutes after a reboot, even during a scheduled timeslot.
- **Initializing.** The unit is in the process of writing to all of the disks in the unit in order to make the array fault tolerant. For more information, see “About Initialization” on page 146.
- **Initializing-Paused.** The unit is set to initialize, however scheduling is enabled and the present time is not during a scheduled timeslot. Initializing will start at the next scheduled time slot. Initializations follow the Rebuild/Migrate task schedule. Initialization is also paused for up to ten minutes after a reboot, even during a scheduled timeslot.
- **Verifying.** The unit is in the process of ensuring that the parity data of a redundant unit is valid. For more information, see “About Verification” on page 149.
- **Verify-Paused.** The unit is set to verify, however, scheduling is enabled, and the present time is not during a scheduled timeslot. Verification will start at the next scheduled time slot.
- **Migrating.** The unit is in the process of being reconfigured while it is online. Migration can be used to change the RAID level, to expand the capacity by adding additional drives, or to change the stripe size. For more information, see “Changing An Existing Configuration by Migrating” on page 115.

- **Migrate-Paused.** The unit is in the process of migrating, however scheduling is enabled, and the present time is not during a scheduled timeslot. Migrating will start at the next scheduled time slot. Migration is also paused for up to ten minutes after a reboot, even during a scheduled timeslot.
- **Degraded.** One or more drives in the redundant unit is no longer being used by the controller. For more information, see “About Degraded Units” on page 138.
- **Inoperable.** This is a condition where one or more drives are missing from a unit, causing the unit to no longer be available to the operating system. Data on an inoperable unit cannot be accessed. For more information, see “About Inoperable Units” on page 139.

Drive Statuses

The following is a list of drive statuses you may see in 3DM2:

- **OK.** The drive is fine and is functioning normally.
- **Not Present.** No drive is present in this slot.
- **Drive Removed.** The drive has been removed.
- **Other.** A number of other drive statuses may appear in the event of a problem. If you have a question about a status shown, contact LSI customer support. Knowing the exact drive status can help trouble-shoot the problem.

About Degraded Units

Fault-tolerant RAID units provide data redundancy by duplicating information on multiple drives. These RAID units make it possible to continue use even if one of the drives in the unit has failed.

- RAID 1 and RAID 10 units each use mirroring to achieve fault tolerance. Identical data is stored on two or more drives to protect against drive failure.
- RAID 5, RAID 6, and RAID 50 units achieve fault tolerance by using a simple (exclusive OR) function to generate the parity data that is distributed on all drives.
- RAID 6 adds an extra level of protection over RAID 5 by generating a second parity when data is written. This allows two drives to fail without compromising data integrity, especially on larger units.

When one of the drives in a fault-tolerant unit fails or is removed or unplugged, the unit is said to be *degraded*.

You can still read and write data from a degraded unit, but the unit will not be fault tolerant until it is rebuilt using the Rebuild feature.

When a RAID unit becomes degraded, it is marked as such, and the drive(s) that failed are marked as **Not In Use** in the 3BM screens and **Degraded** in the 3DM2 pages. If supported by your enclosure, the LED for failed drives may turn red.

You should replace the failed drive and rebuild the unit as soon as it is convenient to do so. The unit will not be fault tolerant until it has been rebuilt. Rebuilding can occur automatically, depending on your settings. For more information, see “Rebuilding Units” on page 154.

About Inoperable Units

Units become inoperable when there are no longer enough drives in the unit for it to function. For example, a RAID 5 unit created from four drives becomes degraded if one drive fails or is removed, but becomes inoperable if two drives fail or are removed. A RAID 6 unit created from five drives becomes degraded if one or two drives is removed, but becomes inoperable if three drives fail or are removed.

Data on an inoperable unit cannot be accessed unless the missing drives are reconnected.

If you have data on a unit that is currently “inoperable,” contact technical support. A form is available on the web at <http://www.lsi.com/channel/ContactUs>.

Locating a Drive by Blinking Its LED

If you use a supported enclosure with enclosure services, you may be able to easily identify the drives in a unit, or locate an individual drive, by causing the LEDs associated with the drives to blink.

You can issue the command to blink the LED through 3DM2 or 3BM.

For details about what the different LED patterns on the enclosure may mean, see “Enclosure Drive LED Status Indicators” on page 136.

To blink the LED for a drive through 3DM2

- 1 Do one of the following:
 - Choose **Information >> Drive Information** from the main menu in 3DM2. On the Drive Information page, identify the drive you want to physically locate.

- Choose **Monitor >> Enclosure** from the main menu in 3DM2. On the list of enclosures, click the ID number of the enclosure. On the Enclosure Detail page, identify the drive you want to physically locate.
- 2 Check the box in the **Identify** column.
The LED on the enclosure begins blinking.
 - 3 When you are finished working with the drive and no longer need to see the LED, return to this page and uncheck the **Identify** box.

To blink the LED for a drive through 3BM

- 1 On the main 3BM screen, **Tab to Information** and press **Enter**.
- 2 On the pop-up menu, select **Drives** and press **Enter**.
- 3 On the Drive Information page, use the arrow keys to select the drive you want to identify.
- 4 Press **F4**.
The LED on the enclosure begins blinking. (Note that this feature is only available for drives in enclosures.)
- 5 When you are finished working with the drive and no longer need to see the LED, return to this page and press **F4** again to halt the blinking.

To blink the LEDs for all drives in a unit

- 1 Choose **Information >> Unit Information** from the main menu in 3DM2.
- 2 On the Unit Information page, identify the unit you are interested in.
- 3 Check the box in the **Identify** column.
The LEDs for the drives in the selected unit begin blinking.
- 4 When you no longer need to see the LEDs, return to this page and uncheck the **Identify** box.

Alarms, Errors, and Other Events

3ware provides several levels of detail about alarms, errors, and other events. This information is available through the 3DM2 web application and the CLI. On Windows systems, the WinAVAlarm alert utility can also be used to notify you of events.

The next few pages describe these capabilities.

- “Viewing Alarms, Errors, and Other Events” on page 141
- “Using the Alert Utility Under Windows” on page 142
- “Downloading an Error Log” on page 144
- “Viewing SMART Data About a Drive” on page 144

CLI capabilities are described in the *3ware SATA+SAS RAID Controller Card CLI Guide, Version 10.2*.



Tip: If you have a supported enclosure, the LEDs on your enclosure may also provide you with status information about drives. For more information, see “Enclosure Drive LED Status Indicators” on page 136.

Viewing Alarms, Errors, and Other Events

The **Alarms** page in 3DM2 shows a log of all events (also called Asynchronous Event Notifications, or AENs) that have occurred on units. These events include alarms that occur when the 3ware RAID controller requires attention, such as when a disk unit becomes degraded and is no longer fault tolerant. They also include SMART notifications and informational notification, such as when sectors have been repaired during verification.

Event messages are categorized into the following levels of severity:

- **Errors** (high severity events), shown next to a red box
- **Warnings**, shown next to a yellow box
- **Information**, shown next to a blue box

Examples of event messages:

- **Error:** Unclean shutdown
- **Warning:** Degraded unit
- **Information:** Start and completion of rebuilding, verifying, initializing, migrating, and so forth.

3DM2 can e-mail notifications of these events to one or more recipients. For more information, see “Managing E-mail Event Notification” on page 59.

If your 3ware RAID controller is installed in a Windows system, the WinAVAlarm alert utility can notify you of events immediately with an audible alarm and a popup message. For details, see “Using the Alert Utility Under Windows” on page 142.

A list of the possible error and other event messages is provided under “Error and Notification Messages” on page 235.

To view alarms, errors and other events in 3DM2

- 1 Choose **Monitor >> Alarms**.

The Alarms page displays, listing all event notifications.

- 2 For details about a particular alarm, click it.

A Help window opens with additional information about the alarm.

To see an explanation of a specific item in 3DM2

- Click on the message you are interested in, on the 3DM2 Alarms page.
A help topic opens with additional information.

Using the Alert Utility Under Windows

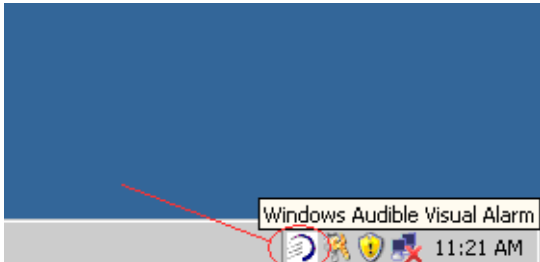
An alert utility, WinAVAlarm, is automatically installed on Windows systems when 3DM2 is installed. It can provide immediate notification of events, through a popup message and an audible alert. By default it is set to notify you whenever an error (high-severity event) occurs, through both a popup message and an audible alert. You can configure the alert settings to specify types of events you want to be notified of: Errors, Warnings, or Information.

WinAVAlarm is a stand-alone utility and does not require 3DM2 to be running, unlike e-mail notification. After it is installed, an icon for it appears in your System tray.

To change the alert utility settings

- 1 Double-click on the 3ware icon in the system tray.

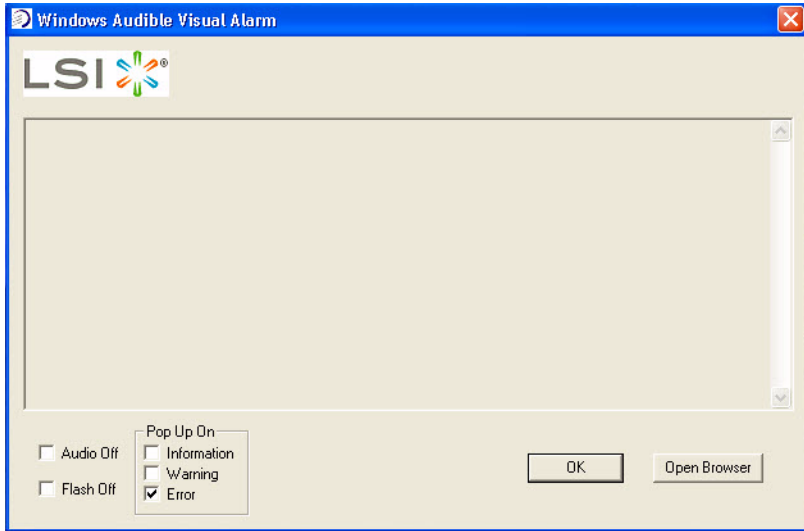
Figure 71. WinAVAlarm in the Windows System Tray



- 2 In the Windows Audible Visual Alarm window, select the types of alerts you want to be notified of.

If you want to turn off the sound alarm and only have a pop-up message appear, check the **Audio Off** button.

Figure 72. WinAVAlarm Popup Window



If you wish, you can open 3DM2 from this window by clicking **Open Browser**. This can be useful when you receive a message, because the 3DM2 Alarms page allows you to easily access online help associated with the events.

- 3 Click **OK** to close the window and accept any changes you have made.

Downloading an Error Log

You can download an error log containing information from the firmware log. This can be useful when troubleshooting certain types of problems. For example, you might want to send the saved file to 3ware Customer Support for assistance when troubleshooting.

To download the error log

- 1 In 3DM2, choose **Information >> Controller Details** from the menu bar.
- 2 Make sure the correct controller is displayed in the **Select Controller** field in the menu bar.
- 3 On the Controller Details page, click the **Download Error Log** link.
- 4 When the Save or Open dialog box appears, navigate to where you want to save the log and click **OK**.

Viewing SMART Data About a Drive

You can view SMART (Self-Monitoring, Analysis, and Reporting Technology) data about a SATA drive to help troubleshoot problems that occur. SMART data is available on all SATA disk drives (unit members, Single Disks, and Hot Spares). Although SAS drives are monitored, the data for them is not displayed.

You can also set self-tests that will check the SMART attributes and post messages to the Alarms page when they are exceeded. For more information, see “Selecting Self-tests to be Performed” on page 168.

To view SMART data

- 1 Choose **Information >> Drive Information** from the menu bar.
- 2 On the Drive Information page, click the port number for the drive you are interested in.

A window showing details of the SMART data opens. The data is shown as hex values.

Only SMART data for SATA drives is displayed.

Background Tasks

Background tasks are maintenance tasks that help maintain the integrity of your drives and data. These tasks include

- Initialization of units
- Verification of units
- Rebuilds when units have become degraded
- Migration of units from one configuration to another
- Self-tests

3ware RAID management software includes some controls to help you balance completion of these tasks with host I/O responsiveness, so as to minimize any conflict between the two. For example, you can schedule when background tasks should be run (to avoid peak work hours) and you can specify the rate at which they run in relationship to foreground I/O tasks. You can also set the background task mode to address the issue of latency.

This section includes the following topics related to background tasks:

- About Initialization
- About Verification
- Starting a Verify Manually
- Rebuilding Units
- Cancelling a Rebuild and Restarting It with a Different Drive
- Working with the Background Task Mode
- Setting the Background Task Mode
- Setting Background Task Rate
- Background Task Prioritization
- Scheduling Background Tasks
- Viewing Current Task Schedules
- Turning On or Off Use of a Rebuild/Migrate Task Schedule
- Removing a Task Slot from a Schedule
- Adding a New Task Schedule Slot
- Selecting Self-tests to be Performed

Although the migration of a unit is handled as a background task, initiating it is similar to creating a new unit. For details, see “Changing An Existing Configuration by Migrating” on page 115.

About Initialization

For 3ware SATA RAID controllers, *initialize* means to put the redundant data on the drives of redundant units into a known state so that data can be recovered in the event of a disk drive failure. This is sometimes referred to as *background initialization* or *resynching*, and does not erase user data.

Some RAID levels must be initialized for best performance. (For specifics, see “Initialization of Different RAID Types” on page 147.) When these units are created in the BIOS (through 3BM), you can choose to do a *foreground initialization*, which will take place before the operating system has loaded, or a *background initialization*, which allows you to put the unit in service immediately, but will slow down the unit performance until it completes. You can elect to cancel foreground initialization, put the units into service, and have initialization run in the background, instead.



Mac User Note: Foreground initializations are only done in 3BM, which is not applicable for Mac users.

Foreground Versus Background Initialization

Initialization makes parity information valid. Foreground initialization does this by simply writing zeroes to all the drives so that they all have the same values, overwriting any existing data in the process. In contrast, background initialization uses an algorithm to resynch the parity information on the drives and does not rewrite existing data.

A foreground initialization can be run from the BIOS using 3BM. It clears all existing data from the drives. Foreground initialization can take up to several hours, depending upon the size of the unit. After foreground initialization completes, you can start the operating system and units will perform at peak efficiency.



Note: Drives that support the Write Same feature (SCT) can write to multiple drive sectors at once, improving initialization time. To take advantage of this feature, all the drives in the unit must support Write Same.

If you are creating a unit through 3BM and if immediate access to the unit is important, select background initialization. Background initialization will then start automatically within about 10 minutes. Background initialization (resynching) does not write zeroes to the drives or harm your data. You can partition, format, and use the unit safely while it is initializing. The unit is fully fault-tolerant while the initialization takes place. That is, if the unit degrades before the initialization is complete, the data will remain intact.

When initializing is done after booting to the operating system, the process of initializing takes longer than it does if initialization is done by writing zeroes to the unit in the BIOS. Consequently, it will be a longer period of time until the performance of the unit is fully optimal.

Although you can use the unit while it is being initialized in the background, initialization does slow I/O performance until completed. You can adjust how much initialization will slow performance by setting the rate at which it occurs. (See “Setting Background Task Rate” on page 162.) You can also postpone initialization until a scheduled time. (See “Scheduling Background Tasks” on page 163).



Note: Units that are not initialized through 3BM are automatically initialized using background initialization when they are verified for the first time. (Verification requires that the units have been previously initialized.) This will not affect the data on the drives, and the units will perform normally, although performance will be slowed until the initialization and verification are completed.

Initialization of Different RAID Types

Information about initialization for each of the different RAID types is described below and summarized in Table 12 on page 148.

Initialization of RAID 0 Units

RAID 0 units do not need to be initialized and cannot be initialized. RAID 0 units are immediately available for use with full performance when created.

Initialization of RAID 5, RAID 6, and RAID 50 Units

RAID 5 units with three or four drives will be automatically initialized the first time they are verified.

Regardless of the size, all 9000-series RAID 5, RAID 6, and RAID 50 units are fully fault tolerant upon creation. These configurations use a specialized scheme for writing to the unit, which does not have to be valid to provide fault tolerance.

Performance of the following types of units will improve after the unit has been initialized: RAID 6, RAID 5 units with 5 or more disks, and RAID 50 units with 2 subunits of 5 or 6 disks. For these configurations, initialization begins automatically after you create them. If you create them in 3BM using the default foreground initialization method, zeroes are written to all unit members before booting to the operating system. If you create them through 3DM2, you will boot to the operating system and the RAID 5 parity is then calculated and written to disk, keeping any data in the unit intact.

RAID 5 units with 3 or 4 disks do not need to be initialized to have full performance upon creation. It is okay that 3 or 4 disk RAID 5 units are not

initialized. These RAID types are fully redundant, regardless of whether or not they are initialized. Similarly, RAID 50 units with a grouping of 3 or 4 disks in a subunit do not need to be initialized. However, RAID 50 with a grouping of 5 or more disks in a subunit do need to be initialized for full performance.



Notes:

For RAID 5 and RAID 6 with more 5 or more drives, it is strongly required that you initialize the unit. Initialization is critical to insuring data integrity on the unit. The initialization can be a background or foreground initialization.

For RAID 5 with 3 or 4 drives, initialization before use is not required. However, initialization is required before a unit can be verified. Consequently, if you attempt to verify a RAID 5 with 3 or 4 drives that has not yet been initialized, you will see a message that the array has not been initialized, and initialization will begin. This is considered part of the normal operation of the unit.

Initialization of RAID 1 and RAID 10 Units

RAID 1 and RAID 10 units do not need to be initialized when they are created. They are fault tolerant and are immediately available for use with full performance when created.

Initialization of RAID 1 or RAID 10 units will take place automatically the first time the unit is verified.

Initialization of a RAID 1 unit results in data from one disk (the disk on the lower port number) being copied to the other disk. In RAID 10 units, data from one half of the unit is copied to the other half.

After the initialization, subsequent verifies to a RAID 1 or RAID 10 unit check for data consistency by comparing the data from one drive (or set of drives) to the other drive (or set of drives).

Table 12: Initialization Requirements for Different RAID Configurations

Initialization Required for Highest Performance?	RAID Configurations
No	Single drive
No	RAID 0
No	RAID 1 RAID 10

Table 12: Initialization Requirements for Different RAID Configurations (continued)

Initialization Required for Highest Performance?	RAID Configurations
No	RAID 5 with 3 or 4 disks RAID 50 with 6, 8, or 9 disks RAID 50 with 12 disks in 3 subunits of 4 RAID 50 with 12 disks in 4 subunits of 3 RAID 50 with 16 disks in 4 subunits of 4
Yes	RAID 5 with 5 or more disks RAID 6 RAID 50 with subunits of 5 or more disks

Background Initialization After Power Failure

The 3ware controller detects and handles power failures, using a mechanism that ensures that redundant units have consistent data and parity. When a redundant unit is unexpectedly shutdown, there is a possibility some data and parity may be inconsistent. If a unit or sub-unit of a redundant unit is detected to have been shutdown uncleanly, the unit or sub-unit will change its mode to either 'Initializing' or 'Verifying.'

When the initialization is complete, the unit is guaranteed to be redundant again. The initialization does not erase user data.

This process will take less time if the unit is created with Rapid RAID Recovery enabled during unit creation. See "Rapid RAID Recovery" on page 113.

About Verification

The verify feature confirms the validity of redundant data on redundant units and performs media scans on non-redundant units.

Regular weekly verification is a good idea, as it can provide early warning of a disk drive problem or failure. This allows you to replace drives before they fail.

You can start a verify manually or regular verification can be done automatically by enabling Auto-Verify. (See "Starting a Verify Manually" on page 152 and "Using Auto Verification" on page 152.)

During verification, I/O continues normally, but with a slight performance loss, depending on your verify rate setting. You can adjust how much verification will slow performance by setting a rate at which it occurs. (See

“Setting Background Task Rate” on page 162.) You can also postpone verification until a scheduled time. (See “Scheduling Background Tasks” on page 163.)



Note: Not verifying the unit periodically can lead to an unstable unit and may cause data loss.

It is strongly recommended that you schedule a verify at least 1 time per week. You can take advantage of the the Auto-Verify and Basic Verify Schedule to accomplish this.

What Verification Does

For a RAID 1 or RAID 10 unit, a verify compares the data of one mirror with the other. For RAID 5, RAID 6, and RAID 50, a verify calculates parity and compares it to what is written on the disk drive. For non-redundant units, it performs a media scan.

Verification checks each sector on a drive. This is important, because day-to-day use of the media may leave many sectors on a drive unused or unchecked for long periods of time. This can result in errors occurring during user operation. Periodic verification of the media allows the disk drive firmware to take corrective actions on problem areas on the disk, minimizing the occurrence of uncorrectable read and write errors.

Verifies can be performed through either 3BM (BIOS) or through 3DM2. In addition, they can be scheduled to run at preferred times, through 3DM2 or through the CLI, or can be run automatically during the Verify schedule window, if scheduling and the Auto-Verify feature are enabled.



Mac User Note: Disregard the paragraph above, and replace with “Verifies can be scheduled to run at preferred times or can be run automatically during the Verify schedule window, if scheduling and the Auto Verify feature are enabled.”

Verification of Non-Redundant Units

Verification of non-redundant units (single disks, spares, and RAID 0 units) read each sector of a drive, sequentially. If a sector can't be read, it is flagged as unreadable, and the next time the controller writes to that location, the drive reallocates the data to a different sector.

Verification of Redundant Units

Verification of redundant units reads each sector, working from lowest block to highest block. If verification cannot read data in a sector, dynamic sector repair is used to recover the lost data from the redundant drive or drives; this

recovered data is written to the problem sector. This forces the drive to reallocate the defective sector with a good spare sector.

If the verify unit process determines that the mirrored drives are not identical or the parity is not correct, the error is corrected. For RAID 1 and 10, this involves copying the miscompared data from the lower port(s) to the higher port(s) of the mirror. For RAID 5, RAID 6, and RAID 50, this involves recalculating and rewriting the parity that was incorrect. AEN 36 (“Verify detected and fixed data/parity mismatch”) is posted to the Alarms page.

For RAID 1 and 10, verification involves copying the data from the lower port(s) to the higher port(s) of the mirror. For RAID 5 and RAID 50, this involves recalculating and rewriting the parity for the entire unit. If the unit is not redundant, a file-system check is recommended to correct the issue. If the errors persist and cannot be overwritten from a backup copy, perform a final incremental backup. You will need to replace the defective drive, recreate the unit, and reinstall the data.

How Errors Are Handled

Verification makes use of the same error checking and error repair techniques used during ordinary use of drives configured through 3ware RAID controllers.

When verification encounters an error, the controller typically retries the command. If there are cable CRC errors, there may be multiple retries including downgrade of the UDMA mode. If the error persists and is unrepairable (e.g., ECC errors), an error notification is issued to indicate the problem. (See AEN “0026 Drive ECC error reported” on page 252.)

If the disk drive is part of a redundant unit that is in a redundant state (not degraded or rebuilding), then Dynamic Sector Repair automatically rewrites the redundant data to the error location to force the drive to reallocate the error location. A notification of repair is posted to the alarms list. The result is a restoration of drive and data integrity; the primary and redundant data are again both valid.

If the unit is not redundant, it is recommended that you perform a file-system check to correct the issue. Under Windows, you can do this by right-clicking on the Drive and choosing Properties; then on the Tools tab, click Check Now. Under Mac OS X, you can do this using the First Aid tab in the Disk Utility—select the disk on the left and then click Verify Disk. If verification encounters problems, you can then use the Repair Disk option on the same screen.

If the errors persist and cannot be overwritten from a backup copy, perform a final backup of files that have changed since your last backup. You will need to replace the defective drive, recreate the array, and reinstall the data.

Using Auto Verification

Auto-Verify is available as a unit policy that can help insure that a unit is verified on a regular basis. This is important, as it can provide early warning of unstable units and possible data loss.

Auto-Verify is enabled on a per-unit basis, and works in conjunction with the Verify Schedule, which is set on a controller-wide basis. Two verify schedules settings are available (Basic and Advanced), and Auto-Verify works differently, depending on which is selected.

The Basic Verify schedule (enabled, by default), provides a weekly day and time for Auto-Verify to occur. When the Basic schedule is used, Auto-Verify will start a verify at the designated time, and run until it has finished.

For users who need more control over when Verify tasks run, an Advanced Verify schedule is also available, which gives you the ability to define seven times during the week when verifications can occur, and allows you to specify the duration of each, effectively creating a series of "schedule windows". This is useful if you want to insure that background tasks such as verification occur during times of low system usage. When you use the Advanced Verify schedule, if a verify does not have time to complete during a scheduled time window, it will pause until the next scheduled time, to resume verifying.

This distinction between Basic and Advanced Verify Scheduling is new in 9.5.1. In previous versions, there was one type of Verify Scheduling, which functioned as the "Advanced" version does in 9.5.1.



Note: Unless you have a specific need for the Advanced Verify schedule, it is recommended that you enable Auto-Verify for units, and that you use Basic Verify scheduling, in order to insure weekly verification of your units.

If Auto-Verify is disabled for a unit, then verification will only run if you start it manually or in the event of an unclean shutdown.

For more details about how to set the Verify Scheduling option, see “Selecting Advanced or Basic Verify Schedules” on page 166.

Starting a Verify Manually

Verification of units can be done automatically, on a schedule, or can be started manually, as described below. You can manually start a verify through either 3DM2 or 3BM. (See “Enabling or Disabling Auto-Verify for a Unit” on page 107 and “Scheduling Background Tasks” on page 163.)



Note: If the unit has not previously been initialized and you manually select **Verify Unit**, the initialization process starts.

To verify a unit through 3DM2

- 1 In 3DM2, choose **Management >> Maintenance**.
- 2 In the **Unit Maintenance** section of the Maintenance page, select the unit you want to verify and click **Verify Unit**.

3DM2 puts the selected unit in verifying mode.

If Basic Verify is selected on the Scheduling page, the verification process begins almost immediately. If Advanced Verify is selected, the unit will not start actively verifying until the next scheduled time.

A **Stop Verify** link appears next to the unit on the Maintenance page. If you need to stop the verify process, use this link. (If initialization starts because the unit had not previously been initialized, it cannot be halted, so no **Stop Verify** link appears.)

To verify a unit through 3BM

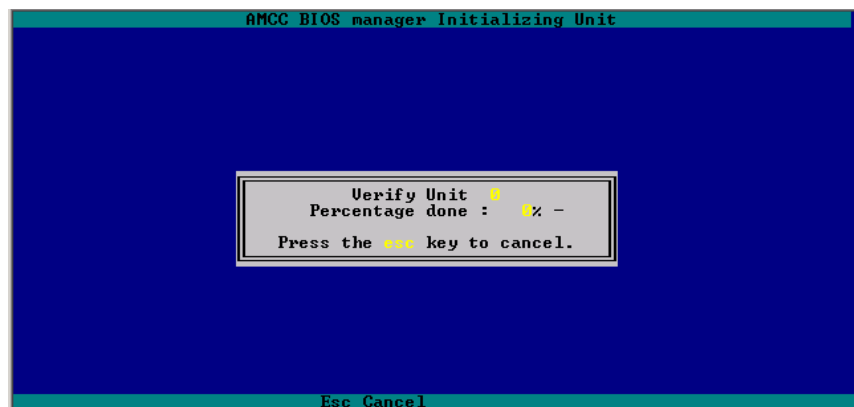
- 1 At the main 3BM screen, select the unit by highlighting it and pressing **Enter**.

An asterisk appears in the left-most column to indicate that it is selected.

- 2 **Tab** to the **Maintain Unit** button and press **Enter**.
- 3 On the pop-up menu, select **Verify** and press **Enter**.

Verification of the selected unit starts immediately.

Figure 73. Verifying a Unit





Notes:

If a unit that requires initialization has not previously been initialized, selecting Verify Unit starts initialization. This is because fault-tolerant units cannot be verified until after they are initialized.

If the unit is already in a state of rebuild, initialization, or verification, the unit cannot be verified in 3BM. You must boot the system and let the task finish in the background.

Rebuilding Units

Rebuilding is the process of generating data on a new drive after it is put into service to replace a failed drive in a fault tolerant unit.

If a hot spare of the appropriate drive type (SAS or SATA) is specified and a redundant unit degrades, it will be used to automatically replace the failed drive in the redundant unit without intervention on your part. The rebuild process will automatically be launched as a background process at the next scheduled time. If scheduling is turned off, the rebuild process will start almost immediately (within a couple of minutes). If 3DM2 is running and E-mail notification is enabled, an event notification will be sent to specified users when the unit degrades and again when the rebuild process is complete.

If the Auto-Rebuild policy is enabled (see “Setting the Auto-Rebuild Policy” on page 71), the firmware will attempt to rebuild a degraded unit with an available drive or a failed drive.

If desired, you can manually replace the drive, rescan the controller, and start the rebuild process. Manual rebuilds can be started from either 3BM, CLI, or 3DM2, although the rebuild itself only happens when the operating system is running.

The rebuild process may take less time if Rapid RAID Recovery has been enabled during unit creation. See “Rapid RAID Recovery” on page 113.

Rebuilds on multiple units can take place simultaneously.

If multiple drives are faulted in a RAID 10 configuration, the drives are rebuilt simultaneously. In a 4-drive RAID 10 configuration, up to two drives can be rebuilt. In a 6-drive configuration, up to three drives can be rebuilt. In an 8-drive configuration, up to four drives can be rebuilt. In a 12-drive configuration, up to six drives can be rebuilt.



Note: If both drives in a RAID 10 mirrored set are faulted, the data is not recoverable. Up to half of the drives in a RAID 10 unit can become defective and still have the user data retained, as long as the failed drives are only half of each mirrored pair.

A RAID 5 unit can have one drive fail before becoming inoperable.

A RAID 50 unit can sustain multiple drive failures, as long there is only one failed drive in each RAID 5 set.

A RAID 6 unit can have two simultaneous drive failures, before becoming inoperable.

When a redundant RAID unit is running in Degraded mode and you rebuild it, the missing data is reconstructed from all functioning drives.



Note: If a rebuild fails, check the Alarms page for the reason. If there was an ECC error on the source disk, you can force the rebuild to continue by checking the Overwrite ECC policy on the Controller Settings page in 3DM2 and then running Rebuild again. This will cause uncorrectable blocks to be rewritten and the data may be incorrect. It is recommended that you execute a file system check when the rebuild completes.

- Under Windows, you can do this by right-clicking on the Drive and choosing **Properties**; then on the **Tools** tab, click **Check Now**.
- Under Linux or FreeBSD use `fsck`
- On Mac OS X, you can do this using the First Aid tab in the Disk Utility—select the disk on the left and then click **Verify Disk**. If verification encounters problems, you can then use the **Repair Disk** option on the same screen.
- For OpenSolaris and VMware you should follow your operating system's guide to perform a file system check.

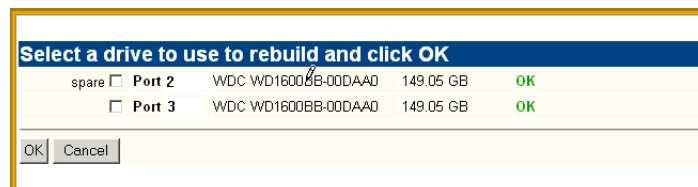
Rebuilding a Unit Through 3DM2

When a drive on a unit becomes defective, you replace it with an available drive and then rebuild the unit. If Auto-Rebuild is enabled and a drive is available, starting the rebuild is optional as it will start automatically.

To rebuild a unit through 3DM2

- 1 If necessary, add a new drive to replace the failed drive. (For details, see “Adding a Drive” on page 129.)
- 2 In 3DM2, choose **Management >> Maintenance**.
- 3 In the **Unit Maintenance** section of the Maintenance page, select the degraded unit and click the **Rebuild Unit** button.
- 4 When a dialog box displays available drives, select the drive you want to replace the failed drive and click **OK**.

Figure 74. Selecting a Drive when Rebuilding



- 5 If the degraded unit has more than one failed drive (for example, a RAID 10 where both mirrored pairs each have a failed drive), repeat step 3 and step 4 to select another drive.

If rebuild scheduling is not enabled on the **Scheduling** page, the rebuild process begins almost immediately in the background. If rebuild scheduling is enabled, the unit will not start actively rebuilding until the next scheduled time.



Note: If you need to cancel a rebuild, you can do so by using the **Remove Drive** link on the Maintenance page to remove the drive from the unit.

Rebuilding Units through 3BM

When a RAID unit becomes degraded, it is marked as such, and the drive(s) that failed are marked as **Not In Use** in the 3BM screens.

Figure 75 shows an example of how a degraded RAID 5 unit appears in 3BM.

Figure 75. Degraded RAID 5 Array to be Rebuilt



You can start the rebuild of a degraded unit manually in 3BM, or you can let the system boot and allow the rebuild to take place automatically.

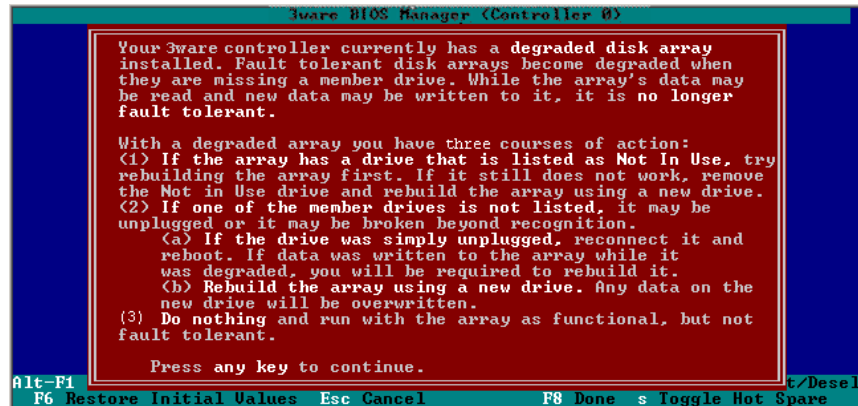
The rebuild process will take less time if Rapid RAID Recovery has been enabled during unit creation. See “Rapid RAID Recovery” on page 113

To start the rebuild of a unit through 3BM

- 1 Reboot the system and start 3BM.

A red message box informs you that the unit is degraded, and suggests some possible approaches. Figure 76 shows an example of a degraded-array message.

Figure 76. Degraded Disk Array Warning Message



- 2 Press a key to continue.
- 3 If your degraded unit has a drive indicated as **Not in Use**, the drive may still be usable. Try rebuilding with the **Not in Use** drive intact. Simply select the unit (highlight it and press **Enter**) and then select the **Rebuild Unit** button.
- 4 When the **Rebuild** confirmation screen appears, confirm that you selected the correct unit by selecting **OK**.
- 5 Press **F8** to save your changes and exit 3BM. The unit will begin rebuilding after the operating system finishes loading.

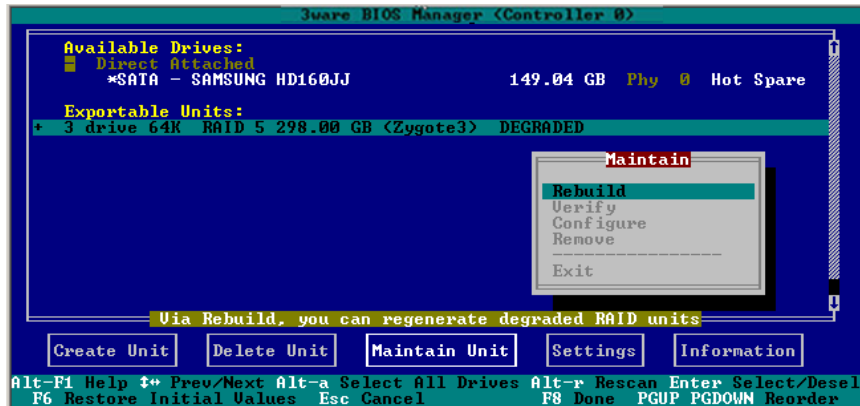
If the rebuild fails and you have no available drives, do one of the following:

- If your system has hot swap bays, you can replace the failed or **Not In Use** drive and rescan (Alt-R) the unit.
- If your system does not have hot swap bays, power down the system and replace the failed or **Not In Use** drive. Then power on the system and restart 3BM.

Then follow these steps:

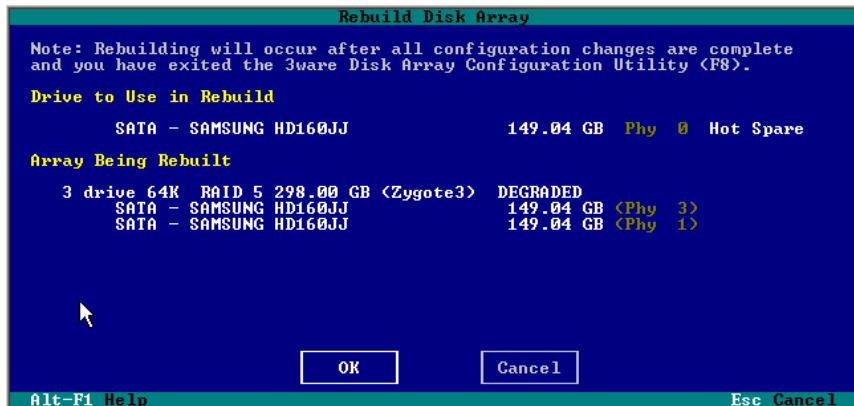
- 1 At the main 3BM screen, highlight an available drive to replace the faulted drive and press **Enter** to select it.
An asterisk appears in the left most column to indicate the drive is selected.
- 2 Press **Tab** to select the degraded unit and press **Enter** to select it.
- 3 **Tab** to the **Maintain Unit** button and press **Enter**.
- 4 Select **Rebuild** from the pop-up menu and press **Enter**.

Figure 77. Rebuild Option on the Maintain Menu



The Rebuild Disk Array screen displays.

Figure 78. Rebuild Disk Array Screen



- 5 Press **Enter** to select the **OK** button to continue.

You are returned to the main screen; “Rebuilding” appears next to the unit you selected.

- 6 Press **F8** to save your changes and exit 3BM.

The unit will begin rebuilding about ten minutes after the operating system finishes loading and the 3ware driver has loaded.

Cancelling a Rebuild and Restarting It with a Different Drive

When you start a rebuild from 3BM, you cannot cancel it in 3BM interface. However, if you have drives in hot swap bays, you can remove and replace the drive, rescan the controller (Alt-R), and then select a new drive to be used in the rebuild. You can also boot the operating system, launch 3DM2, and cancel a rebuild by using the **Remove Drive** link on the Maintenance page.

If your drives are not in hot swap bays and you do not want to boot the operating system and launch 3DM2, you can also cancel a rebuild by powering down the system, physically removing a drive, and installing another one that you want to use. Then when you start 3BM, the unit will appear as degraded and you can rebuild it, using the steps described under “Rebuilding Units through 3BM” on page 156.



Note: If you want to pause the rebuild process through 3DM2, you can do so by setting or changing the rebuild schedule on the Scheduling page. If you set a schedule for rebuilds that does not include the current time, the rebuild process will pause.

Working with the Background Task Mode

Background Task Mode is specifically designed to address the issue of latency, which can cause problems for some applications, by helping you balance the rate of host I/O and efficient completion of background tasks.

About Latency and the Background Task Mode

Latency is the real or perceived delay in response time seen by the host system when accessing some data. For some applications, such as streaming video and audio application, it is important to minimize the latency of read commands, so that users do not perceive a lag when viewing video or listening to audio.

When background tasks are active (for example, rebuild, verify, and initialization), there can be increased latency, and under some circumstances, this can result in a degraded user experience or in an application failure.

You can set the **Background Task Mode** to minimize latency. This mode monitors and paces the relationship between host I/Os and background tasks. You can set the Background Task Mode to either **Adaptive** (the default) or **Low Latency**.

Low Latency mode minimizes the latency (delay) in reading data from the RAID unit by slowing down the background task process. In contrast, **Adaptive** mode allows the firmware to adjust the interaction of background

tasks with host I/Os to maximize the speed of both host I/O and background tasks.

If latency is not an issue in the applications you use, then using the Adaptive Background Task Mode will probably meet your needs and will result in background tasks that complete faster.

Relationship of Task Mode and Task Rate

The Background Task Mode works in conjunction with the Background Task Rate. The settings are shown in Figure 79.

Figure 79. Background Task Settings on Controller Settings page

Background Task (Controller ID 0)								
		Task Rate					Mode	
		5	4	3	2	1		
Rebuild/Migrate	Fastest Rebuild	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	Fastest I/O	<input checked="" type="radio"/> Adaptive <input type="radio"/> Low Latency
Verify	Fastest Verify	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	Fastest I/O	<input type="radio"/> Adaptive <input checked="" type="radio"/> Low Latency

Background Task Rate lets you set the relative performance of background tasks in relation to host I/O activity on a scale of **1 to 5**, with 5 being the fastest background task and slowest I/O, while 1 is the fastest I/O and the slowest background task, as shown in Figure 79. Separate settings are available for Rebuild/Migrate and for Verify. (Initialization occurs at the Rebuild/Migrate rate.)

5 = fastest background task; slowest host I/O

4 = faster background task; slower host I/O

3 = balanced between background tasks and host I/O

2 = faster host I/O; slower background task

1 = fastest host I/O; slowest background task

If you set the **Background Task Mode** to **Low Latency**, it slows down the background task process in the context of the current Task Rate setting, with a graduated pacing of host I/O versus background task I/O, 2 through 5.

Important: It is recommended that if you use the Background Task Mode of Low Latency, you always set the Background Task Rate to at least **2** on the scale of 1 to 5. When used in conjunction with a rate of **1** (fastest host I/O; slowest background task), Low Latency Mode can create a situation in which background tasks never complete, if there is continuous host I/O activity on the unit.

If you do select **Low Latency** when the Rate is set to **1**, 3DM2 will display a warning, and will then continue to display a recommendation to change it until you change either the Rate to **2** or greater, or until you change the Mode to **Adaptive** (Figure 80).

Figure 80. Low Latency Mode with warning when Rate=1

The screenshot shows the LSI 3DM2 web interface. At the top, there are navigation tabs: Summary, Information, Management, Monitor, 3DM 2 Settings, and Help. Below these is a 'Controller Settings' section for Controller ID 0 (9750-8i). The main area is titled 'Background Task (Controller ID 0)' and contains a table with columns for Task Rate (5, 4, 3, 2, 1) and Mode (Adaptive, Low Latency). The 'Rebuild/Migrate' and 'Verify' tasks are both set to 'Fastest I/O' (radio button selected) and 'Low Latency' mode. A red box highlights these settings, and a red text box below it reads: 'Recommended: With Low Latency mode, use a Verify Task Rate greater than 1'. Below this is the 'Unit Policies (Controller ID 0)' section, which shows settings for Unit 0 (RAID 5) and Unit 1 (SINGLE DISK).



Note: The Background Task Rate and Background Task Mode settings are only relevant when there is host I/O activity. When there is no host activity, background tasks (rebuild/migrate, initialization, and verify) always run at the maximum.

Table 13 provides an overview of the impact of selecting different Task Rate and Task Mode settings.

Table 13: Selecting Appropriate Background Task Rate and Mode

Your priority	Rebuild Task Rate	Task Mode	Comments
Fastest rebuild time	5	Adaptive	Potential for higher latency on host I/Os
Balanced host I/O and rebuild tasks	3	Adaptive	Default setting
Minimized host I/O latency	2	Low Latency	Background tasks will complete, but will be slow when there are host I/Os
Minimum host I/O latency	1	Low Latency	Background tasks may never finish when there are continuous host I/Os. For example, a rebuild may never complete.

Setting the Background Task Mode

You set the Background Task Mode on the 3DM2 **Controller Settings** page. Settings are available for both Rebuild/Migrate and for Verify. By default, both Background Mode settings are set to **Adaptive**.

To change the Background Task Mode

- 1 Choose **Management >> Controller Settings** from the menu bar in 3DM2.
- 2 In the Background Task section of the Controller Settings page, select the Background Mode you want for Rebuild/Migrate and for Verify.

Figure 81. Background Task Mode on the 3DM2 Settings page

The screenshot shows the LSI 3DM2 web interface. The top navigation bar includes 'Summary', 'Information', 'Management', 'Monitor', '3DM2 Settings', and 'Help'. The '3DM2 Settings' tab is active, and the 'Controller Settings' sub-tab is selected. The page title is 'Background Task (Controller ID 0)'. Below this, there are two rows of settings for 'Rebuild/Migrate' and 'Verify'. Each row has a 'Task Rate' section with five radio buttons (5, 4, 3, 2, 1) and a 'Mode' section with two radio buttons: 'Adaptive' and 'Low Latency'. In the 'Rebuild/Migrate' row, 'Fastest I/O' (rate 2) and 'Adaptive' mode are selected. In the 'Verify' row, 'Fastest I/O' (rate 2) and 'Adaptive' mode are selected. Below this is the 'Unit Policies (Controller ID 0)' section, which includes a table with columns for 'Write Cache', 'Read Cache', 'Auto Verify', 'Overwrite ECC', 'Queuing', 'StorSave', and 'Rapid RAID Recovery'. The table shows settings for 'Unit 0 [RAID 5]' and 'Unit 1 [SINGLE DISK]'. The 'Mode' section in the Background Task settings is circled in red.

The page refreshes and a message appears at the top to confirm the changes you make.

Setting Background Task Rate

You can set the relative performance of background tasks (initializing, rebuilding/migrating, and verifying) in relation to normal I/O activity (reading and writing to disk).

Controllers can have separate settings for Rebuild/Migrate Rate and Verify Rate. (Initialization occurs at the Rebuild rate.)

To change the background task rate

- 1 Choose **Management >> Controller Settings** from the menu bar.
- 2 In the **Background Task Rate** section of the Controller Settings page, select one of the five radio buttons to indicate the relative task rate for Rebuild and Verify Tasks.

Figure 82. Background Task Rate on Controller Settings page

Background Task (Controller ID 0)		Task Rate					Mode	
		5	4	3	2	1		
Rebuild/Migrate	Fastest Rebuild	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	Fastest I/O	<input checked="" type="radio"/> Adaptive <input type="radio"/> Low Latency
Verify	Fastest Verify	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	Fastest I/O	<input type="radio"/> Adaptive <input checked="" type="radio"/> Low Latency

The furthest left buttons set the firmware to the fastest rebuild and verify settings. This means that maximum processing time will be given to rebuilds or verifies rather than I/O. The furthest right buttons set the firmware to the slowest rebuild and verify settings, giving maximum processing time to I/O.

After you select one of the radio buttons, the page refreshes, and a message at the top confirms the change you have made.

Background Task Prioritization

Although migration tasks follow the same schedule as rebuild and initialization tasks, they are always given the highest priority because of the controller and disk resources required during migration.

Once a unit is put into the migration state, it must be allowed to complete the process. While migrating, rebuilds or verifies to the unit are not permitted.

Rebuilding preempts verify operations. If a unit requires rebuilding, that process will take place before the unit is verified.

Controllers can work on multiple units at the same time. This means that if you have both a redundant unit and a non-redundant unit, the verification of the redundant unit and the media scan of the non-redundant unit will occur at the same time.

Scheduling Background Tasks

You can set up scheduling windows for when background tasks occur so that routine maintenance of storage media occurs when it will be least likely to interfere with day-to-day work on the system (peak I/O times). By creating and using schedules, you can specify when active rebuilding, migrating, verifying, and testing of units should occur. For example, you might wish these tasks to occur at 2 AM each day, or on weekends.



Note: Initialization follows the rebuild/migrate schedule. The default setting for both is to ignore the schedule.

Rebuild/migrate, verify, and self-test tasks are scheduled separately, but in a very similar way. You can perform the following scheduling tasks:

- Viewing Current Task Schedules
- Turning On or Off Use of a Rebuild/Migrate Task Schedule
- Selecting Advanced or Basic Verify Schedules
- Removing a Task Slot from a Schedule
- Adding a New Task Schedule Slot
- Selecting Self-tests to be Performed



Tip: If you want to change a task schedule window, you first remove the schedule item and then add it back with the desired day, time, and duration.



Note: Setting up the scheduling window does not actually request background tasks. It simply specifies when they can run. For more information about the background tasks themselves, see “Background Tasks” on page 145.

You can also set the rate at which background tasks are performed compared to I/O tasks. For more information, see “Setting Background Task Rate” on page 162.

Scheduled Task Duration

If a rebuild does not complete in a scheduled time block, it will pause and continue where it left off at the next scheduled time block.

This is also true for verify, if you use the Advanced Verify schedule. If you use the Basic Verify Schedule, verifies will run to completion, and are not limited to a specific duration.



Note: When using Basic Verify Schedule and Auto-Verify, if the system is off at the scheduled time, a Verify will start when the system is powered on, if it has been longer than a week since a verify last completed.

Viewing Current Task Schedules

You can see the current schedules for background tasks on the **Scheduling** page.

To view the current task schedule

- 1 Choose **Management >> Schedule** from the menu bar.
The Scheduling page appears, showing the schedule for Rebuild Tasks. (Migration and initialization tasks follow the Rebuild Task schedule.)
- 2 To view Verify Tasks or Self-test Tasks, select it from the drop-down list at the top of the page.

Figure 83. Selecting Task Schedules to View

The screenshot shows the LSI 3DM2 management interface. The top navigation bar includes Summary, Information, Management, Monitor, 3DM2 Settings, and Help. The 'Scheduling' tab is selected. Below the navigation bar, there is a dropdown menu for 'Select a type of task you would like to schedule:' with options: Rebuild/Migrate Tasks, Verify Tasks, and Self-test Tasks. The 'Rebuild/Migrate Tasks' option is selected. Below the dropdown, there are radio buttons for 'Follow Schedule' and 'Ignore Schedule'. A table shows the schedule for Rebuild/Migrate Tasks, with columns for Day, Time, and Duration (hours). The table lists days from Sunday to Saturday, all with a time of 12:00am and a duration of 24 hours. At the bottom, there are buttons for 'Remove Checked' and 'Add New Slot', along with dropdown menus for Day, Time, and Duration.

	Day	Time	Duration (hours)
<input type="checkbox"/> 1.	Sunday	12:00am	24
<input type="checkbox"/> 2.	Monday	12:00am	24
<input type="checkbox"/> 3.	Tuesday	12:00am	24
<input type="checkbox"/> 4.	Wednesday	12:00am	24
<input type="checkbox"/> 5.	Thursday	12:00am	24
<input type="checkbox"/> 6.	Friday	12:00am	24
<input type="checkbox"/> 7.	Saturday	12:00am	24

Turning On or Off Use of a Rebuild/Migrate Task Schedule

Turning on the schedule for Rebuild/Migrate tasks forces initializations, rebuilds and migrates to be performed only during the time specified by the schedule. If the schedule is not turned on, rebuilds, migration, and initialization can happen whenever they are required or are manually started.

There may be times when you want to disable scheduled rebuild/migrate tasks, so that you can rebuild or migrate a unit right away, without waiting for the next scheduled time. In this case, you can disable the schedule, as described below.



Note: When you first use 3DM2, daily schedules exist with 24 hour duration—that is, the schedule is for “all the time.” Until you change these 24-hour daily schedule, enabling the schedule will not have any direct effect.

You can easily disable a current Rebuild/Migrate schedule without deleting the schedule itself.

To turn on or off use of the current Migrate/Rebuild task schedule

- 1 Choose **Management >> Schedule** from the menu bar.
The Scheduling page appears, showing the schedule for Rebuild/Migrate Tasks.
- 2 In the Schedule Rebuild Tasks section, select the appropriate setting: **Follow Schedule** or **Ignore Schedule**.

The illustration below shows this setting for the rebuild task schedule.

Schedule Rebuild Tasks (Controller ID 2)		
Scheduled Rebuilds <input type="radio"/> Follow Schedule <input checked="" type="radio"/> Ignore Schedule		
Day	Time	Duration (hours)
<input type="checkbox"/> 1. Sunday	12:00am	24
<input type="checkbox"/> 2. Monday	12:00am	24



Note: Self-test schedules cannot be turned off in this way. To disable self-tests you must either remove all schedule times, or uncheck the tests listed in the **Tasks** column. For more information, see “Selecting Self-tests to be Performed” on page 168.

Selecting Advanced or Basic Verify Schedules

You cannot ignore a verify schedule. You can only select either Basic or Advanced as the verify schedule.

The Basic verify schedule is selected by default and is scheduled to run once a week at Friday 12 am. You can change the time at which it runs on the Schedule page in 3DM2 or on the Policy screen in 3BM.

The Advanced verify schedule is similar to the Rebuild/Migrate schedule and has seven scheduling slots. For details about the functioning of Basic and Advanced verify schedules, see “Using Auto Verification” on page 152.

To select Basic or Advanced verify schedule

- 1 Choose **Management >> Schedule** from the menu bar.
The Scheduling page appears, showing the schedule for Rebuild/Migrate Tasks.

- 2 From the drop-down menu, select **Verify Tasks**.
The Schedule Verify Tasks page appears.
- 3 Select either **Basic** or **Advanced** as the verify schedule.

Removing a Task Slot from a Schedule

By default, seven daily task schedule slots are defined, each starting at 12:00 am and running for 24 hours.

A maximum of seven schedule slots can be defined. When seven schedule slots are shown for any of the tasks, you must remove a schedule slot before you can add another.

To remove a task slot from a schedule

- 1 Choose **Management >> Schedule** from the menu bar.
The Scheduling page appears, showing the schedule for Rebuild/Migrate Tasks.
To view Verify Tasks or Self-test Tasks, select one from the drop-down list at the top of the page. To view the seven verify schedule slots, select **Advanced**.
- 2 Select the checkbox next to the schedule(s) you want to remove.
- 3 Click the **Remove Checked** button.
The page refreshes, and the selected schedule slot(s) are removed. You can now add another schedule slot or slots.

Adding a New Task Schedule Slot

When you add a rebuild/migrate or verify task schedule, you specify the day of the week, time, and duration for the task. For self-test schedules, you specify day and time, but not duration. (Duration is not required for self-tests.)

Depending on the schedule and system workload, background tasks may require more than one scheduled duration to complete.

To add a task schedule slot

- 1 Choose **Management >> Schedule** from the menu bar.
The Scheduling page appears, showing the schedule for Rebuild/Migrate Tasks.
- 2 To view Verify Tasks or Self-test Tasks, select it from the drop-down list at the top of the page.

- 3 Scroll to the section of the Scheduling page that shows the task you want to add.
- 4 In the fields at the bottom of the section, select the Day, Time, and Duration for the task.



- 5 Click the **Add New Slot** button.
The page refreshes and the new schedule is added to the list.



Note: The scheduled tasks can be added in any order. For example a new task scheduled for Tuesday (slot-2) will preempt the task originally scheduled for Wednesday (slot-1).

Selecting Self-tests to be Performed

For 3ware RAID controllers (9550SX and newer), you can check the SMART thresholds for drives. (For more information see the 3DM2 Reference section, “Scheduling page” on page 205.)

Initially, these tests are set to run every 24 hours. You can change the schedule for when they are run, and you can disable the tests, if you prefer not have to have them performed.



Note: These tasks will only be run during scheduled times if they are checked in the **Schedule Self-tests** section of the Scheduling page. If neither of the tasks is checked, self-tests will never run, even if you have scheduled time slots set.

To select self-tests to be performed

- 1 Choose **Management >> Schedule** from the menu bar.
The Scheduling page appears, showing the schedule for Rebuild Tasks.
- 2 Select Self-test Tasks from the drop-down list at the top of the page.
- 3 Check the boxes next to the self-tests you want to be performed.

Schedule Self-tests (Controller ID 2)		
Day	Time	Tasks (applies to all schedule items)
<input type="checkbox"/> 1. Sunday	12:00am	
<input type="checkbox"/> 2. Monday	12:00am	<input checked="" type="checkbox"/> Check S.M.A.R.T. Thresholds

To disable self-tests

Unlike scheduling of rebuilds and verifies, scheduling of self-tests is always enabled.

To disable self-tests you must either remove all schedule times, or uncheck the tests listed in the **Tasks** column.

9

Maintaining Your Controller

This section contains instructions for how to perform tasks that help you maintain your controller, including:

- Determining the Current Version of Your 3ware Driver
- Updating the Firmware and Driver
- Downloading the Driver and Firmware
- Updating the Firmware Through 3DM2
- Updating the Firmware Through DOS Using the 3ware Bootable CD
- Viewing Battery Information
- Testing Battery Capacity

Information about updating the 3ware driver is included in Appendix B, “Driver and Software Installation” on page 301.

Determining the Current Version of Your 3ware Driver

You can view controller and driver information in several different ways:

- Using 3DM2 you can see both the driver and firmware versions (see the “Controller Summary page” on page 190).
- Using 3BM you can see the firmware version (see “Displaying Information About the Controller and Related Devices” on page 42)
- Using the CLI you can see both the driver and firmware versions (see *3ware SATA+SAS RAID Controller Card CLI Guide, Version 10.2*)
- Under Linux, you can type the following command if you have a 2.4 kernel or earlier:

```
cat /proc/modules/scsi/3w-sas/*
```

where the asterisk (*) represents controller number.

If you have a 2.6 kernels with sysfs, type the following command:

```
cat /sys/class/scsi_host/<hostid>/stats
```

where <hostid> is usually host0, unless other SCSI devices are available, in which case it may be host1 or higher.

If you have a 2.6 kernel without sysfs, type the following command:

```
dmesg | grep 3w
(dmesg can also be used with earlier kernel versions.)
```

Updating the Firmware and Driver



Important: Updating the firmware can render the device driver and/or management tools incompatible. Before you update the firmware on your controller, please follow these recommendations:

- 1) Back up your data.
- 2) Make sure you have a copy of the current firmware image so that you can roll back to it, if necessary.
- 3) Close all applications.

This section details several ways to update the firmware and driver for the 3ware RAID controller, depending upon operating system.

Before starting the update of either driver or firmware, you will want to make sure you have the latest files. For details, see “Downloading the Driver and Firmware” on page 172.

To update the firmware

- The 3ware CD contains a bootable DOS firmware update program that will work for most PC-based systems. See “Updating the Firmware Through DOS Using the 3ware Bootable CD” on page 174.

You can download the latest version of the CD from:
<http://www.lsi.com/channel/ChannelDownloads>.

- All supported operating systems can update the firmware through 3DM2. For details, see “Updating the Firmware Through 3DM2” on page 174.
- All supported operating systems can update the firmware through CLI. For details, see *3ware SATA+SAS RAID Controller Card CLI Guide, Version 10.2*.

To update the driver

- **FreeBSD** users can update the driver per “Updating Drivers under FreeBSD” on page 304.
- **Linux** users can update the driver at the command line. For details see:
 - “Updating the 3ware Driver Under Red Hat or Fedora Core” on page 321

- “Updating the 3ware Driver Under SUSE” on page 323
- **Mac OS** users can update the driver for future releases by installing the latest software and driver installation package. For details see “Installing 3ware Drivers and Software under Mac OS X” on page 325.
- **OpenSolaris** users can update the driver for future releases by installing the latest software and driver installation package. For details see “Installing 3ware Drivers and Software under OpenSolaris” on page 331.
- **VMware** users can update the driver for future releases by installing the latest software and driver installation package. For details see “Installing the Driver using vihostupdate” on page 340 or “Installing the Driver using esxupdate” on page 341.
- **Windows** users can update the driver by using the 3ware Device Driver Install Wizard. For more information, see “Updating the 3ware Driver Under Windows” on page 348.

Downloading the Driver and Firmware

You can download the latest drivers and firmware from the LSI website, at <http://www.lsi.com/channel/ChannelDownloads>. You can also download the 3ware CD ISO file and create a CD.



Note: For Linux, do not use the driver from the external Linux distribution if it is older than the currently supported driver. Instead, use the current driver from the 3ware CD or from the LSI 3ware web site.

To download the driver or firmware

- 1 On the LSI website go to <http://www.lsi.com/channel/ChannelDownloads>.
- 2 Select *RAID Controllers* as the *Product Family*.
- 3 Select your *Product* from the drop-down list on the right.
- 4 When the page has refreshed, locate the item you want to download and click the link to the file.



Note: If using Winzip or another Windows utility to extract the Linux file, use the .zip version instead of the .tgz version. Otherwise the files will not be compatible with Linux.

- 5 In the dialog box that appears, click *Save* to save the file to disk.

- 6 Uncompress the file to extract the driver or firmware files to a local directory. (Note that the firmware will not fit on a floppy diskette.)
(Make note of the absolute path to the local directory.)

To download the 3ware CD

- 1 On the LSI website go to
<http://www.lsi.com/channel/ChannelDownloads>.
- 2 Select *RAID Controllers* as the *Product Family*.
- 3 Select your product from the drop-down list on the right.
- 4 When the page has refreshed, locate the ISO for the CD (in the Software section) and click the link to the file.
- 5 In the dialog box that appears, click **Save** to save the file to disk.
- 6 After the download has completed, burn the ISO to a CD.

Updating the Firmware Through 3DM2

You can use 3DM2 to update the 3ware RAID controller firmware for any operating system that has a graphical user interface.

To update the firmware through 3DM2

- 1 Download the firmware update from the LSI website. For details, see “To download the driver or firmware” on page 172.
- 2 In 3DM2, navigate to **Management >> Controller Settings**.
- 3 In the *Update Firmware* section of Controller Settings page, browse to the location where you have saved the downloaded firmware update. The update name will be something like `promxxx.img`.
- 4 Click *Begin Update*.
The Compatibility Information window appears.
- 5 Click *Proceed Update*.
The 3ware RAID controller firmware is updated.
- 6 Restart your system so that the firmware image will take effect.

Updating the Firmware Through DOS Using the 3ware Bootable CD

The 3ware CD can function as a bootable DOS firmware update program that will work for most PC-based systems.

To update the firmware through DOS

- 1 Start your computer with the 3ware CD in your CD-ROM drive and the BIOS set to boot from CD-ROM.
- 2 At the Welcome screen type: `firmware`
- 3 At the next screen select the controller type to upgrade by typing the ID number (1,2...) next to the name of the controller or Q, to quit. For example:
1 - 9750
2 - 9690

(You can only install one controller at a time, you will need to repeat this procedure for each controller.)

The update program is loaded.

- 4 To continue, type:
y
- 5 If multiple controller cards are installed, select the ID number of the card to upgrade, otherwise continue to next step. You must select the same controller type selected in step 3, otherwise the upgrade will fail.
The update program lists the version of your present firmware.
- 6 To continue, type:
y
The program checks that the update program version of the firmware is compatible. If it is, it begins installing the firmware. This will take 1 to 3 minutes. Do not power off your computer until the firmware finishes updating.
- 7 If multiple controllers are being installed, repeat steps 3-5 for the next controller.
- 8 Type q to quit, remove the bootable CD and reboot your system.

Viewing Battery Information

The Battery Backup Unit (BBU) is an add-on card that can be attached to 3ware 9750 RAID controllers to supply power from a battery pack in the event of a system power loss. This allows the controller to use write-caching for optimal performance and to preserve data in the event of a system power failure. When fully charged, the battery preserves the contents of the cache memory for up to 72 hours. When power is restored, the cached write data is written to the disks.

You can see information about a battery backup unit attached to your controller in both 3DM2 and 3BM.



Mac User Note: Disregard the sentence directly above, and use “You can see information about a battery backup unit attached to your controller in 3DM2.”



Note: When the BBU status is not “Ready,” write caching is automatically disabled on all units attached to the controller

To view information about a BBU in 3DM2

- On the menu bar, choose **Monitor >> Battery Backup**.

The Battery Backup page appears, on which you can see details and status about the unit. This page is refreshed every 30 seconds.

For details about the fields on this page, see “Battery Backup page” on page 218.

To view information about a BBU in 3BM

- At the main 3BM screen, tab to the **Information** button and press **Enter**. On the pop-up menu, select **Battery Backup** and press **Enter**.

The Battery Backup Unit screen appears.

The fields on this screen are the same as those available through 3DM2. For details about the fields, see “Battery Backup page” on page 218.

Testing Battery Capacity

Batteries in the BBU need to be replaced periodically. A battery test should be run every four weeks in order to get a reliable estimate of battery capacity, and to determine when it needs to be replaced.

The battery test is used to measure the battery’s capacity to back up write data. In order to make a reliable estimate of battery capacity, the BBU pre-charges

the battery before it proceeds with a full discharge cycle. The battery is automatically charged again after the test completes. The whole process usually takes between 8 and 12 hours.

While running the battery test and until charging is completed, write cache is temporarily disabled.

For how to replace the battery, see the installation guide that came with your battery backup unit.

To test the battery in a BBU in 3DM2

- 1 On the menu bar, choose **Monitor >> Battery Backup**.
- 2 On the Battery Backup page, click the **Test Battery Capacity** link.

Figure 84. Battery Backup Information Screen in 3DM2

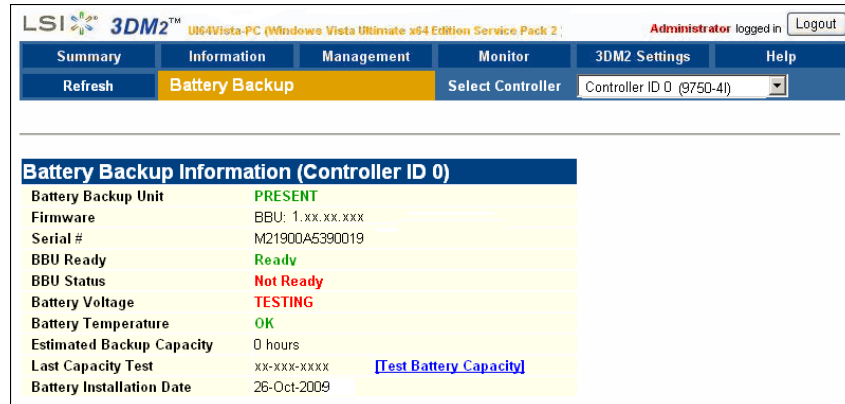
Battery Backup Information (Controller ID 0)	
Battery Backup Unit	PRESENT
Firmware	N/A
Serial #	LSI101000G0804080821
BBU Ready	Ready
BBU Status	OK
Battery Voltage	OK
Battery Temperature	OK (73°F 23°C)
Estimated Backup Capacity	136 hours
Last Capacity Test	xx-xxx-xxxx [Test Battery Capacity]
Battery Installation Date	08-Oct-2009

Last updated Mon, Apr 26, 2010 02:57:52PM
 This page will automatically refresh every 5 minute(s)
 3DM2 version 2.11.00.013
 API version 2.08.00.014B
 Copyright (c) 2010 LSI Corporation

- 3 When a message cautions you that testing the battery will disable the BBU for up to 24 hours, click **OK** to continue.

After the battery test starts, you will see the voltage start dropping; eventually the battery voltage will say "LOW". This is part of the battery test. After the voltage drops to a point, it will start charging again, and the status will change to "Charging." Eventually, the battery voltage will say "OK" again.

Figure 85. BBU Information Screen While Battery is Testing



To test the battery in a BBU in 3BM

- 1 At the main 3BM screen, tab to the **BBU** button and press **Enter**.
- 2 Tab to **Test Battery Capacity** and press **Enter**.

Figure 86. Battery Backup Information Screen in 3BM



Enclosure Management

3ware enclosure management features let you view the status of chassis and enclosure hardware, such as fans, power supplies, and temperature sensors through 3DM2, and locate individual hardware components by blinking LEDs associated with them.

For 3ware 9750 RAID controllers, enclosure management features are available for supported enclosures that provide enclosure services through SCSI Enclosure Services 2 (SES-2). These enclosures may provide services through:

- Enclosures with expanders
- Enclosures employing the AMI 9070 or 9072 backplane controller chip, and with a SAS cable connection supporting the sideband I²C protocol between the 3ware RAID controller and the backplane
- To upgrade storage enclosure processor (SEP) firmware refer to the *3ware SATA+SAS RAID Controller Card CLI Guide, Version 10.2*.

A list of supported enclosures is available at http://www.lsi.com/channel/support/marketing_resources, through the Data & Interoperability tab.

Depending on the manufacturer of your enclosure, you may see variations in the features supported by your enclosure from the ones described in this chapter. For details about what features are supported, refer to the documentation for your enclosure.

This chapter describes how to view and locate enclosure-specific hardware. For information about identifying drives in an enclosure, see “Locating a Drive by Blinking Its LED” on page 139.

Details about enclosure management are organized into the following topics:

- Viewing a List of Enclosures
- Checking Enclosure Component Status
- Locating a Specific Enclosure Component
- Working with Enclosure Alarms
- Downloading an Enclosure Diagnostic Log

Viewing a List of Enclosures

If you have multiple enclosures attached to your 3ware RAID controller, you can see a list of them.

To see a list of enclosures in 3DM2

- Choose **Monitor >> Enclosure Support** from the menu.

The Enclosure Summary screen appears.

Figure 87. Enclosure Summary page

Enclosure Summary								
ID	Status	Vendor	Product ID	Slots	Drives	Fans	Temp Sensor	Power Supply
0	OK	LSI	DE1600-SAS	12	1	4	4	2

Last updated Mon, Apr 26, 2010 02:58:53PM
 This page will automatically refresh every 5 minute(s)
 3DM2 version 2.11.00.013
 API version 2.08.00.014B
 Copyright (c) 2010 LSI Corporation

To see details about a particular enclosure, click the link in the ID column. (For more information, see “Checking Enclosure Component Status” on page 181.)

To see a list of enclosures in 3BM

- 1 On the main 3BM screen, **Tab** to **Information** and press **Enter**.
- 2 On the pop-up menu, select **Enclosures** and press **Enter**.

The Enclosure Information page appears, with information about enclosure components displayed in the top section, and details about the slots in the selected enclosure displayed in the bottom section.

For an explanation of statuses for the different components, see the status topics starting under “Fan Status” on page 183.

- 3 On the Enclosure Information page, use the arrow keys to move from one enclosure to another. You can use the - and Shift+ keys to hide or show details about an enclosure, if desired.

Tip: You can scroll both sections of the Enclosure Information page to bring additional enclosure information or enclosures into view. Press **Tab** to move between the two sections.

Figure 88. Enclosure Information page (3BM)

The screenshot displays the 'Enclosure Information' page. It shows the enclosure ID as 'Enclosure 0 (AIC, SJ24_EM-UC01-R1, 01A1)' with 24 slots, 6 drives, 3 fans, and 1 temperature sensor. The fans are all 'On' and 'Status: OK'. The temperature is 24°C (75°F). Below this, a table lists the drive configurations for each slot:

Slot	Drive Type	Model	Capacity
Slot 0	SAS	FUJITSU MAU2036RC	34.24 GB
Slot 1	SATA	TOSHIBA MK6032GSX	55.88 GB
Slot 2	SAS	IBM-ESXS ST936701SS	33.90 GB
Slot 3	SAS	IBM-ESXS ST936701SS	33.90 GB
Slot 4	SAS	FUJITSU MAU2036RC	34.24 GB
Slot 5	SATA	ST980025AS	74.53 GB
Slot 6	No Drive		
Slot 7	No Drive		
Slot 8	No Drive		

Navigation options at the bottom include 'Alt-F1 Help', 'F10 Previ/Next', and 'Esc Cancel'.

Checking Enclosure Component Status

If your enclosure supports enclosure services, you may be able to check the status of enclosure components such as power supplies, fans, slots, drives, and temperature sensors.

To check the status of components in your enclosure in 3DM2

- 1 Choose **Monitor >> Enclosure Support** from the menu.
- 2 On the Enclosure Summary page, click the blue Enclosure ID link for the enclosure for which you want to see details.

The Enclosure Details page appears.

Explanations of the statuses for the various enclosure components are provided on the next few pages.

Figure 89. Enclosure Details page

The screenshot shows the LSI 3DM2 web interface. At the top, it displays the system information: "LSI 3DM2™ U164Vista-PC (Windows Vista Ultimate x64 Edition Service Pack 2)" and "Administrator logged in" with a "Logout" button. The navigation menu includes "Summary", "Information", "Management", "Monitor", "3DM2 Settings", and "Help". The "Enclosure Details" page is selected, showing a "Refresh" button and a "Select Controller" dropdown menu set to "Controller ID 0 (9750-8i)".

Enclosure ID 0

Status	OK
Vendor	LSI
Product ID	DE1600-SAS
Revision	0314
Diagnostic	Diagnostic Text
Controller ID	1

Audio Alarm Summary

Audio Alarm	Status	State	Audibility
Audio Alarm information is not available			

Fan Summary

Fan	Status	State	Speed	RPM	Identify
0	OK	ON	Lowest	6360	<input type="checkbox"/>
1	OK	ON	Lowest	6480	<input type="checkbox"/>
2	OK	ON	Lowest	6540	<input type="checkbox"/>

Temp Sensor Summary

Temp Sensor	Status	Temperature	Identify
0	OK	31°C (87°F)	<input type="checkbox"/>
1	OK	33°C (91°F)	<input type="checkbox"/>

Power Supply Summary

Power Supply	Status	State	Voltage	Current	Identify
0	OK	ON	NORMAL	NORMAL	<input type="checkbox"/>
1	OK	ON	NORMAL	NORMAL	<input type="checkbox"/>

Slot Summary

Slot	Status	VPort	Identify
0	OK	8	<input type="checkbox"/>
1	OK	9	<input type="checkbox"/>
2	OK	10	<input type="checkbox"/>
3	OK	11	<input type="checkbox"/>
4	OK	14	<input type="checkbox"/>
5	OK	15	<input type="checkbox"/>
6	OK	12	<input type="checkbox"/>
7	OK	13	<input type="checkbox"/>
8	OK	16	<input type="checkbox"/>
9	OK	17	<input type="checkbox"/>
10	OK	18	<input type="checkbox"/>

To check the status of components in your enclosure in 3BM

When you view the list of enclosures in 3BM, the status information is available on the same screen. For details, see “To see a list of enclosures in 3BM” on page 180.

Fan Status

The following is a list of possible fan statuses:

- **OK.** The fan is optimal and is functioning normally.
- **Off.** The fan is off.
- **Failure.** The fan is present, but is malfunctioning.
- **Not Installed.** There is no fan installed.
- **Unknown.** The status of the fan is not reportable.

Temp Sensor Status

Below is a list of possible temperature sensor statuses.

Note that the temp sensor status indicates the temperature of the enclosure or backplane. Drive temperature, if supported, is available on the Drive Details page.

- **OK.** The temperature sensor is functioning normally.
- **Failure.** The temperature sensor is present, but is malfunctioning.
- **Not Installed.** There is no temperature sensor installed.
- **Unknown.** The status of the temperature sensor is not reportable.
- **Over Temp Warning.** Temperature is higher than normal operating temperature.
- **Over Temp Fail.** Temperature is higher than safe operating temperature.
- **Under Temp Warning.** Temperature is colder than normal operating temperature.
- **Under Temp Fail.** Temperature is lower than safe operating temperature.

Power Supply Status

The following is a list of possible power supply statuses.

- **OK.** The power supply is functioning normally.
- **Failure.** The power supply is present, but is malfunctioning.
- **Off.** The power supply is off.
- **Not Installed.** There is no power supply.
- **Unknown.** The status of the power supply is not reportable.

Slot Summary

The following is a list of possible slot statuses:

- **OK.** The slot is functioning normally.
- **Inserted.** A drive has been inserted in the slot.
- **Ready to Insert.** The slot is ready to accept a drive.
- **Ready to Remove.** The drive in the slot can be removed.

Locating a Specific Enclosure Component

If you have a supported enclosure and the identify feature is supported by your enclosure manufacturer, you can locate power supplies, fans, and temperature sensors by blinking the leds associated with them. This can help you quickly identify which component needs to be checked or replaced. The specific components that can be located in this way will depend on your enclosure.

For details about how to locate a drive by blinking an LED, see “Locating a Drive by Blinking Its LED” on page 139.

To locate a fan, power supply, or temperature sensor

- 1 Choose **Monitor >> Enclosure Support** from the 3DM2 menu.
- 2 On the Enclosure Summary page, click the blue Enclosure ID link for the enclosure you are interested in.
- 3 Check the **Identify** box next to the component you want to locate.
- 4 Examine the enclosure for the blinking LED.

Working with Enclosure Alarms



Note: Enclosure alarm support is based on the SES protocol.

9750 controllers support enclosure audio alarm for enclosures with expanders and I²C backplanes that support the SES-2 protocol.

However, enclosure alarm support depends on the capabilities of the specific enclosure or backplane. Not all enclosures provide an audio alarm, and for those that do, not all provide both the On/Off and Mute/Unmute feature.

For details about what specific features are provided with your enclosure, see the documentation that came with the enclosure or backplane.

Tip: Be sure you have the most recent firmware for the enclosure. If the alarm feature does not work as anticipated, contact the manufacturer for updated firmware.

Supported enclosures are listed at http://www.lsi.com/channel/support/marketing_resources, through the Data & Interoperability tab.

Additional support information is available in the LSI KnowledgeBase, at this website: <http://kb.lsi.com>.

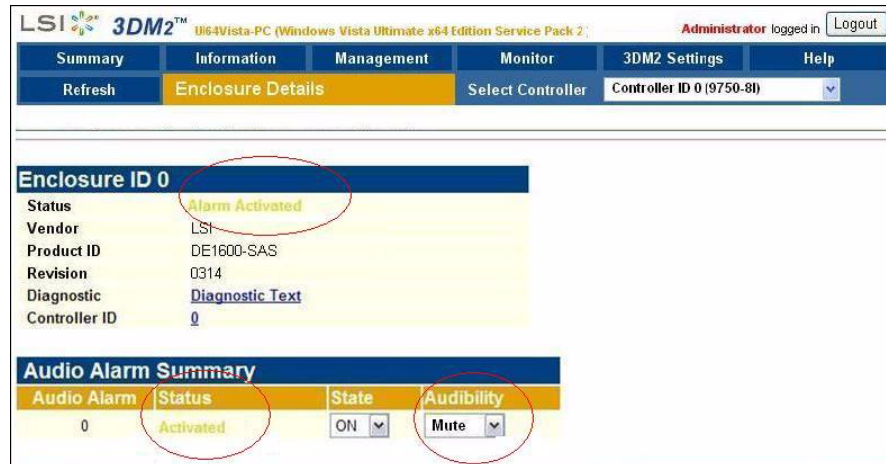
Some enclosures provide an alarm that turns on when a RAID unit becomes degraded or goes offline, or when a drive has failed. (Specific use of the alarm feature may vary somewhat, depending on the enclosure.)

If you have an enclosure with an audio alarm, you can turn the alarm **Off** when it sounds, using 3DM2, 3BM, or the CLI. If the enclosure supports muting, you can also mute and unmute the alarm in 3DM2 or the CLI.

Note that you cannot turn an enclosure alarm *on*. Alarms are only turned on (activated) when an error condition has been detected for a drive or RAID unit. To view any error conditions that may have caused the enclosure alarm to go off, see the **3DM2 Alarms** page. Status information about supported enclosures is also available on the **3DM2 Enclosure Details** page. (You can also use the CLI **/cx show alarms** command, or check the status of the RAID unit in 3BM.)

Muting an alarm provides the ability to silence the alarm, without turning it off completely. You can also set the alarm to Mute in advance, if you do not want the alarm to sound. When the alarm audibility is set to **Mute** and the alarm turns on, the word **Activated** continues to display in the Status column of the Audio Alarm Summary on the 3DM2 Enclosure Details page, as shown in Figure 90.

Figure 90. Alarm displays as “Activated” when muted



Controlling an Enclosure Alarm In 3DM2

In 3DM2, you can turn off an enclosure alarm that has activated, or you can choose to mute or unmute it.

To mute, unmute, or turn off an enclosure alarm

- 1 Choose **Monitor >> Enclosure Support** from the menu bar in 3DM2.

The Status column indicates **Alarm Activated** when the alarm has turned on, as shown in Figure 91.

Figure 91. Enclosure Summary shows Alarm Activated



- 2 On the Enclosure Summary page, click the blue Enclosure ID link for the enclosure to go to the Enclosure Details page.

Figure 92. Enclosure Details page with enclosure alarm On

The screenshot shows the LSI 3DM2 web interface. At the top, there is a navigation bar with tabs: Summary, Information, Management, Monitor, 3DM2 Settings, and Help. Below the navigation bar, there is a sub-menu with 'Refresh', 'Enclosure Details' (highlighted), and 'Select Controller'. The '3DM2 Settings' dropdown menu is open, showing 'Controller ID 0 (9750-8)'.

The main content area displays 'Enclosure ID 0' with the following details:

- Status: Alarm Activated
- Vendor: LSI
- Product ID: DE1600-SAS
- Revision: 0314
- Diagnostic: [Diagnostic Text](#)
- Controller ID: 0

Below this is the 'Audio Alarm Summary' section, which contains a table:

Audio Alarm	Status	State	Audibility
0	Activated	ON	Mute

- 3 In the Audio Alarm Summary section of the Enclosure Details page, do one of the following:

To turn off the alarm, change the **State** to **Off**.

This deactivates and silences the audio alarm.

To mute the alarm, change the **Audibility** to **Mute**.

This silences the alarm without deactivating it. **Activated** remains in the Status field.

To unmute the alarm, change the **Audibility** to **Unmute**

This causes the alarm to sound again, if it is still active.

Turning Off an Enclosure Alarm in 3BM

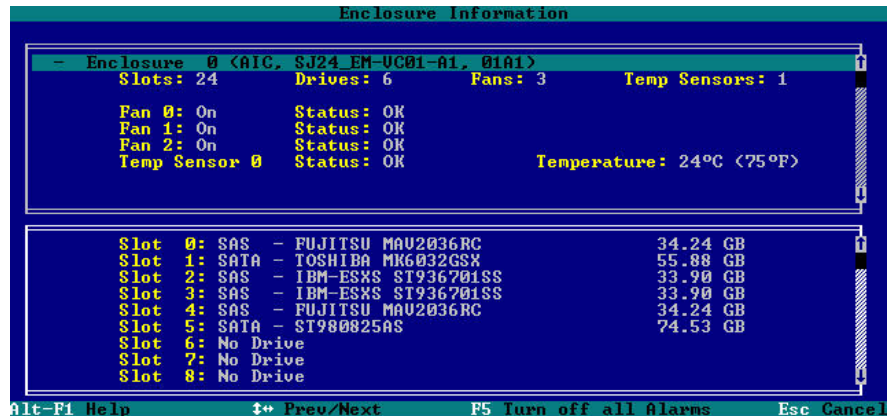
In 3BM, you can turn off enclosure alarms that have activated.

To turn off enclosure alarms in 3BM

- 1 On the main 3BM screen, **Tab** to **Information** and press **Enter**.
- 2 On the pop-up menu, select **Enclosures** and press **Enter**.

The Enclosure Information page appears, with information about enclosure components in the top section, and details about the slots in the selected enclosure in the bottom section.

Figure 93. Enclosure Information page



- To turn off any alarms that are activated to all enclosures attached to the controller, press **F5**.

Downloading an Enclosure Diagnostic Log

The enclosure diagnostic log may be requested by 3ware Customer Support to help troubleshoot problems on your controller. You can download this diagnostic log from the Enclosure Details page.

To download the diagnostic log

- In 3DM2, choose **Monitor >> Enclosure Summary** from the menu bar.
- Make sure the correct controller is displayed in the **Select Controller** field in the menu bar.
- On the Enclosure Summary page, click the **ID** link of the desired enclosure.
The Enclosure Details page for the selected controller appears.
- Click on the **Diagnostic Text** link.
- When the Save or Open dialog box appears, navigate to where you want to save the log and click **OK**.

3DM2 Reference

This section includes details about the fields and features available on the pages you work with throughout 3DM2. It is organized by 3DM2 page, as the pages are organized on the 3DM2 menu bar.

- Controller Summary page
- Controller Details page
- Unit Information page
- Unit Details page
- Drive Information page
- Drive Details window
- Controller Phy Summary page
- Controller Settings page
- Scheduling page
- Maintenance page
- Alarms page
- Battery Backup page
- Enclosure Summary page
- Enclosure Details page
- 3DM2 Settings page

Controller Summary page

Figure 94. Controller Summary Page

Controller Summary					
ID	Model	Serial #	Firmware	Driver	Status
0	9750-8i	E398BP0019	FH9X 5.11.00.010	5.01.00.018	OK

Last updated Mon, Apr 26, 2010 01:40:52PM
 This page will automatically refresh every 5 minute(s)
 3DM2 version 2.11.00.013
 API version 2.08.00.014B
 Copyright (c) 2010 LSI Corporation

The Summary page appears after you first logon to 3DM2, or when you click the Summary link in the menu bar.

This page provides basic information about each 3ware RAID controller in your system. To see details about the units in a controller, click the link in the ID column.

ID. The ID that the operating system assigns to the controller.

Model. The model name of the controller. (The model number is also printed on a sticker on the outside bracket of the controller.)

Serial #. The serial number of the controller. (The serial number is also printed on a sticker on the outside bracket of the controller, or on the backside of the controller.)

Firmware. The firmware version running on the controller.

Driver. The driver version being used to interact with the controller.

Status. The overall status of the controller. Possible statuses include OK, Warning, Error, and No Units. **Warning** indicates that a background task is currently being performed (rebuilding, migrating, or initializing). **Error** indicates that a unit is degraded or inoperable. If both Error and Warning conditions exist, the status will appear as Error. For more information, see “Checking Unit and Drive Status through 3DM2” on page 133.

Controller Details page

Figure 95. Controller Details Page

LSI 3DM2™ U64Vista-PC (Windows Vista Ultimate x64 Edition Service Pack 2) Administrator logged in Logout

Summary Information Management Monitor 3DM2 Settings Help

Refresh Controller Details Select Controller Controller ID 0 (9750-8i)

Controller Details (Controller ID 0)

Model	9750-8i
Serial #	E398BP0019
Firmware	FH9X 5.11.00.010
Driver	5.01.00.018
BIOS	BE9X 5.11.00.003
Boot Loader	BT9X 6.00.00.003
Available Memory	488 MB
Bus Type	PCIe
Bus Width	8 lanes
Bus Speed	2.5 Gbps/lane
Controller Phys	8
Connections	1 of 127
Drives	1 of 127
Units	1 of 127
Active Drives	1 of 127
Active Units	1 of 32
Max Drives per Unit	32
Error Log	Download Error Log

Last updated Wed, Apr 28, 2010 11:41:35AM
 This page will automatically refresh every 5 minute(s)
 3DM2 version 2.11.00.013
 API version 2.08.00.014B
 Copyright (c) 2010 LSI Corporation

The Controller Details page appears when you choose **Information >> Controller Details** from the menu bar.

This page provides detailed information about the controller specified in the drop-down list on the menu bar.

You can also open or download an error log from this screen.

Model. The model name of the controller.

Serial #. The serial number of the controller.

Firmware. The firmware version running on the controller.

Driver. The driver version being used to interact with the controller.

BIOS. The BIOS version on the controller.

Boot Loader. Boot Loader version on the controller.

Available Memory. The amount of available memory on the controller. In the example above, 448MB is available out of the 512MB installed.

Bus Type. The bus type used on the controller. For example: PCIe.

Bus Width. The bus width detected by the controller. This is 8 lanes maximum for the 9750 controller.

Bus Speed. The speed of the bus used on the controller.

Controller Phys. The number of phys on the controller, regardless of whether each currently has a device connected. The 9750 controller has 8 phys.

Connections. The number of connections that are presently being used out of the total number possible on the controller.

Drives. The number of drives that are connected to the controller out of the total number of devices possible on the controller.

Active Drives. The number of drives connected to the controller that are in an active unit out of the total number possible on the controller.

Active Units. The number of units on the controller that are active out of the total number possible on the controller.

Max Drives per Unit. The maximum number of drives that can be in a unit with the present firmware.

Error Log. Provides access to the firmware error log. Click on the **Download Error Log** link to download the firmware error log to your computer. This feature is important when contacting LSI for support with your controller. It will help LSI identify the problem you encountered.

Unit Information page

Figure 96. Unit Information Page

LSI 3DM2™ UI64Vista-PC (Windows Vista Ultimate x64 Edition Service Pack 2) Administrator logged in Logout

Summary Information Management Monitor 3DM2 Settings Help

Refresh Unit Information Select Controller Controller ID 0 (9750-8)

Unit Information (Controller ID 0)

Unit	Name	Type	Capacity	Status	Identify
0		SINGLE DISK	74.50 GB	OK	<input type="checkbox"/>

Last updated Mon, Apr 26, 2010 02:45:08PM
 This page will automatically refresh every 5 minute(s)
 3DM2 version 2.11.00.013
 API version 2.08.00.014B
 Copyright (c) 2010 LSI Corporation

The Unit Information page appears when you choose **Information >> Unit Information** from the menu bar, or when you click an ID number on the Controller Summary page.

This page shows a list of the units on the current controller and provides summary information about each unit.

To see details about a particular unit, click the link in the Unit # column.

Unit #. The unit number assigned to the unit by the firmware.

Name. If a name has been given to this unit, it shows here. If it is empty, no name has been assigned. You can name your unit in the **Unit Names** section of the **Management >> Controller Settings** page.

Type. The type of unit, specified during configuration: RAID 0, RAID 1, RAID 5, RAID 6, RAID 10, RAID 50, or Single Disk. For details about each of the RAID levels, see “Available RAID Configurations” on page 6.

Capacity. The logical capacity (size) of the unit. (1 KB defined as 1024 bytes)

Status. The operational status of the unit: OK, Rebuilding, Initializing, Migrating, Verifying, Degraded, or Inoperable (missing drives). When a unit is Rebuilding, Initializing, Migrating, or Verifying, the percentage (%) complete is also shown. For an explanation of the statuses, see “Unit Statuses” on page 137.



Note: If an asterisk (*) appears next to the status of a unit, there is an error on one of the drives in the unit. This feature provides a diagnostic capability for potential problem drives. The error may not be a repeated error, and may be caused by an ECC error, SMART failure, or a device error. To see if this error condition still exists, rescan the controller; rescanning will clear the drive error status if the condition no longer exists.

Identify. Check this box to cause the LED for the drives associated with this unit to blink in the enclosure. If the box is grayed, identify is not supported.

Unit Details page

Figure 97. Unit Details Page

Unit 0 (Controller ID 0)					
Status	OK				
Name					
Serial #	K20C7XWK9C95C0006115				
Capacity	100.55 GB				
Type	RAID 6				
Stripe	64kB				
Parities	2				
Volumes	1				
Subunits	5				
Subunit 0	Subunit 1	Subunit 2	Subunit 3	Subunit 4	
Status	OK	Status	OK	Status	OK
Type	DISK	Type	DISK	Type	DISK
VPort	7	VPort	8	VPort	9
		VPort	10	VPort	11

The Unit Details page appears when you click an ID number on the Unit Information page. Because it is a sub-page of Unit Information, the page title

in the menu bar continues to display “Unit Information” even when you view details of a unit.

The Unit Details page shows details about a particular unit. The specific information shown depends on what type of unit it is. For example, details about a RAID 5 unit made up of three subunits, each of which contains one drive, will include details about the unit and each subunit, as shown in Figure 97. However, if the unit is a Single Disk, only information about one disk will be shown.

Details on this page may include all or some of the following information described below.

To see details about a particular drive, click the VPort # (virtual port number). You’ll see a list of all drives, with the drive you selected highlighted.

Status. The operational status of the unit or subunit: OK, Rebuilding, Migrating, Initializing, Verifying, Degraded, or Inoperable (missing drives). When a unit is Rebuilding, Initializing, or Verifying, the percentage (%) complete is also shown. For status definitions, see “Unit Statuses” on page 137.

Name. The name assigned to the unit by an administrator.

Serial #. The serial number of the unit. This number is assigned by the firmware when the unit is created.

Capacity. The total capacity of the unit (capacities of subunits are not shown).

Type. The type of unit or subunit. RAID 0, RAID 1, RAID 5, RAID 6, RAID 10, RAID 50, or Single Disk.

Stripe. The stripe size of the unit, if applicable.

Parities. The number of parity drives in the RAID unit.

Volumes. Displays the number of volumes in a unit. This is usually 1. If you created a boot volume on this unit, or if you have a unit on which you have enabled the auto-carving policy, you will see the number of volumes into which the unit has been divided. For more information, see “Using Auto-Carving for Multi LUN Support” on page 71.

Subunits. If the unit has subunits, details of the subunits are shown.



Note: If an asterisk (*) appears next to the status of a subunit, there is an error on one of the drives in the subunit. This feature provides a diagnostic capability for potential problem drives. The error may not be a repeated error, and may be caused by an ECC error, SMART failure, or a device error. Rescanning the controller will clear the drive error status if the condition no longer exists.

VPort #. If the unit Type is Disk, Single Disk, the VPort (Virtual Port) to which the drive is connected is shown. For multiple-drive units, the VPort

numbers are shown in the subunits section. The VPort number is a link to the Drive Information page.

Drive Information page

Figure 98. Drive Information Page

LSI 3DM2™ UI64Vista-PC (Windows Vista Ultimate x64 Edition Service Pack 2) Administrator logged in Logout

Summary Information Management Monitor 3DM2 Settings Help

Refresh Drive Information Select Controller Controller ID 0 (9750-8)

Drive Information (Controller ID 0)

VPort	Model	Capacity	Type	Phy	Slot	Unit	Status	Identify
8	HDS728080PLA380	76.69 GB	SATA	--	Enclosure 0 Slot 4	0	OK	<input type="checkbox"/>

Last updated Mon, Apr 26, 2010 02:47:31PM
 This page will automatically refresh every 5 minute(s)
 3DM2 version 2.11.00.013
 API version 2.08.00.014B
 Copyright (c) 2010 LSI Corporation

The Drive Information page appears when you choose **Information >> Drive Information** from the menu bar, or when you click a VPort # on the Unit Details page. If you arrive at this page from the VPort # hyperlink on the Unit Information page, the line showing the VPort # you clicked on is highlighted.

This page shows a list of drives on the current controller and a summary of each one.

To see additional detail about a particular drive in the Drive Details window, including the SMART data, whether command queuing is supported and enabled, and the SATA Link speed, click the link in the VPort # column.

VPort #. The virtual port to which the drive is assigned.

Model. The model of the drive.

Capacity. The physical capacity of the drive. (Note that the capacity as shown on 3DM2 screen is calculated as 1 KB = 1024. This amount may differ from the capacity that is printed on the disk drive, where it typically has been calculated as 1 KB = 1000. Consequently, the capacity of the drive may appear smaller in the 3DM2 screens. No storage capacity is actually lost; the size has simply been calculated differently for consistency.)

Type. The type of drive: SATA or SAS.

Phy. The number of the controller phy to which the drive is connected. Click the link to go to the Controller Phy Summary page. (For details, see “Controller Phy Summary page” on page 199.)

Slot. The number of the enclosure slot in which the drive is located. Click the link to go to the Enclosure Details page.

Unit. The unit the drive belongs to, if applicable.

Status. The status of the drive: OK, Not Supported, Not Present, and so forth. If you need help regarding a status displayed here, please contact Technical Support. For more information, see “Drive Statuses” on page 138.



Note: In most cases, the status of the drive will not correspond to the status of the unit, shown on the Unit Information page. Different status information is provided for drives and for units.

Identify. Check this box to cause the LED for this drive to blink in the enclosure. If the box is grayed, identify is not supported.

Drive Details window

Figure 99. Drive Details Page

The screenshot shows the LSI 3DM2 web interface. The 'Drive Information (Cont)' table lists 15 VPorts. VPort 7 is selected, and its details are shown in the 'Extra Drive Info' window.

VPort	Model
0	MAXTOR ATLAS15K2_36SAS
1	MAXTOR ATLAS15K2_36SAS
2	MAXTOR ATLAS15K2_36SAS
3	MAXTOR ATLAS15K2_36SAS
4	MAXTOR ATLAS15K2_36SAS
5	MAXTOR ATLAS15K2_36SAS
6	SAMSUNG HD160JJ
7	MAXTOR ATLAS15K2_36SAS
8	MAXTOR ATLAS15K2_36SAS
9	MAXTOR ATLAS15K2_36SAS
10	MAXTOR ATLAS15K2_36SAS
11	MAXTOR ATLAS15K2_36SAS
12	SAMSUNG HD160JJ
13	SAMSUNG HD160JJ
14	SAMSUNG HD160JJ

Extra Drive Info (Controller ID 0 - VPort 7)	
Drive Type	SAS
Serial #	K20C7XWK
Firmware	BK00
Drive Ports	2
Drive Connections	1
Interface Type	Expander Attached
WWN	50010B90001C3FAC
Reallocated Sectors	0
Power On Hour	398
Temperature	41°C (105°F)
Spindle Speed	15000 RPM
Queuing Supported	No
Queuing Enabled	N/A
Link Supported	1.5 Gbps, 3.0 Gbps
Link Enabled	3.0 Gbps

Last updated Mon, Apr 26, 2010 02:47:31PM
 This page will automatically refresh every 5 minute(s)
 3DM2 version 2.11.00.013
 API version 2.08.00.014B
 Copyright (c) 2010 LSI Corporation

The Drive Details window displays when you click a VPort # on the Drive Information page.

This Drive Details window shows some Extra Drive Information, including Queuing and SATA Link Speed support, and the SMART data for SATA drives. SMART data is not displayed for SAS drives.

Extra Drive Information

Drive Type. The type of drive: SAS or SATA.

Serial #. The serial number of the drive.

Firmware. The firmware version of the drive.

Drive Ports. The number of physical ports on the drive.

Drive Connections. The number of connections made to the drive ports.

Interface Type. The drive interface, direct or expander.

SAS WWN. The SAS drive's unique World Wide Number.

Reallocated Sectors. The number of sectors that have been re-allocated due to bad sectors on the drive.

Power On Hour. The total number of hours the drive has been powered-on.

Drive Temperature. The temperature of the drive.

Spindle Speed. The drive speed in RPM.

Queuing Supported and Queuing Enabled.

(Not applicable to SAS drives, only applicable to SATA drives that support NCQ) SATA-2 drives support NCQ (Native Command Queuing), which can result in increased performance for some applications, usually server-type applications. In order to make use of Native Command Queuing, the feature must be enabled at both the drive and the controller. Not all drives support queuing.

The queuing values in this window indicate whether the feature is supported and enabled at the drive. At the controller level, queuing is enabled or disabled for all drives in a unit on the Controller Settings page.

Link Supported and Link Enabled. These fields show the fastest link speed that the disk drive supports and the current link speed.

SMART Data

SMART data is displayed as hex values.

Consult your disk drive manufacturer for information on how to interpret the SMART data. The SMART data meaning varies by disk drive manufacturer and model.

SMART data is not presently displayed for SAS drives.

Controller Phy Summary page

Figure 100. Controller Phy Summary Page

Controller Phy Summary (Controller ID 0)					
Phy	SAS Address	Link Enabled	Link Control	Type	ID
0	500050E000000127	3.0 Gbps	Auto	Enclosure	--
1	500050E000000126	3.0 Gbps	Auto	Enclosure	--
2	500050E000000125	3.0 Gbps	Auto	Enclosure	--
3	500050E000000124	3.0 Gbps	Auto	Enclosure	--
4	500050E000000123	3.0 Gbps	Auto	Enclosure	--
5	500050E000000122	3.0 Gbps	Auto	Enclosure	--
6	500050E000000121	3.0 Gbps	Auto	Enclosure	--
7	500050E000000120	3.0 Gbps	Auto	Enclosure	--

The Controller Phy Summary page shows the properties of controller phys.

The Controller Phy Summary page can be accessed in two ways. If you have a direct-attached drive you can access this page from the **Information >> Drive Information** page by clicking the phy ID for the drive. If all drives are connected via expanders, navigate to the **Management >> Controller Settings** page. Under **Other Controller Settings** click the # link for **Number of Controller Phys**.

Phy. The ID number assigned to the phy connection.

SAS Address. The SAS address of the phy. Phys within each wide port have the same SAS address when they are connected to an enclosure. For directly-connected drives, each phy has a unique SAS address.

Link Enabled. The existing link speed between the controller and the hard drive or enclosure to which it is connected.

Link Control. Selectable field for setting the link speed between the device and the controller. The options are 1.5 Gbps, 3.0 Gbps, 6.0 Gbps, and Auto. The default is Auto. See “Changing the Phy Link Speed” on page 77.

Type. Shows the type of device connected by the phy—either SATA, SAS, or enclosure. A type of SATA or SAS means that the connection is a direct connection to the drive. Enclosure connections are made through an expander.

ID. The VPort address of directly-attached devices. Enclosures do not have VPort numbers, although the drives attached to them do. To find the VPort for a drive in an enclosure, click the ID link to go to the Drive Information page. The drive you selected will be highlighted.

Controller Settings page

Figure 101. Controller Settings Page

The screenshot displays the LSI 3DM2 Controller Settings page. At the top, the user is logged in as Administrator. The navigation bar includes Summary, Information, Management, Monitor, 3DM2 Settings, and Help. The '3DM2 Settings' section is selected, showing 'Controller ID 0 (9750-8)'. The main content area is divided into several sections:

- Background Task (Controller ID 0):** This section contains two tasks: 'Rebuild/Migrate' and 'Verify'. Each task has a 'Task Rate' (5, 4, 3, 2, 1) and a 'Mode' (Adaptive, Low Latency). A recommendation states: 'Recommended: With Low Latency mode, use a Rebuild/Migrate Task Rate greater than 1'.
- Unit Policies (Controller ID 0):** This section shows settings for 'Unit 0 [SINGLE DISK]'. It includes checkboxes for Write Cache, Read Cache, Auto Verify, Overwrite ECC, Queuing, StorSave, and Rapid RAID Recovery. The Read Cache is set to 'Intelligent' and StorSave is set to 'Balance'.
- Unit Names (Controller ID 0):** This section shows settings for 'Unit 0 [SINGLE DISK]'. It includes a text input field for the unit name and buttons for 'Save Names' and 'Reset Names'.
- Other Controller Settings (Controller ID 0):** This section includes:
 - Auto Rebuild: Enabled Disabled
 - Auto-Carving: Enabled Disabled
 - Carve Size (GB): 2048 (with a Submit button)
 - Number of Drives per Spin-up: 1
 - Delay between Spin-up: 1 second(s)
 - Export Unconfigured Disk: Yes
 - Number of Controller Phys: 8
- Update Firmware:** This section includes an 'Image File' field with a 'Browse...' button and a 'Begin Update' button.

The Controller Settings page appears when you choose **Management >> Controller Settings** from the menu bar.

This page lets you view and change settings that affect the units on the controller specified in the drop-down list on the menu bar.

There are four main sections on this page:

- Background Task Rate and Mode
- Unit Policies
- Unit Names
- Other Controller Settings
- Update Firmware

Background Task Rate and Mode

Two Background Task settings allow you to control the balance of background tasks and I/O (reading and writing to disk) performed by the controller.

Background Task Rate lets you set the ratio at which background tasks are performed in comparison to I/O, on a scale from 5 to 1.

There are separate settings for Rebuild/Migrate Rate and Verify Rate. The Rebuild/Migrate Rate also applies to initialization. Although the same rate is used for rebuilding, migrating, and initializing, migrating has the highest priority.

For additional information, see “Setting Background Task Rate” on page 162.

Background Task Mode works with Background Task Rate, to address the issue of latency. Two settings are available: **Adaptive** (the default) and **Low Latency**.

Low Latency mode minimizes the latency (delay) in reading data from the RAID unit by slowing down the background task process. In contrast, **Adaptive** mode allows the firmware to adjust the interaction of background tasks with host I/Os to maximize the speed of both host I/O and background tasks.

For additional information, see See “Working with the Background Task Mode” on page 159.

Unit Policies

On the 3DM2 Controller Settings page you can enable or disable these policies: **Write Cache**, **Auto-verify**, **Overwrite ECC**, and **Queuing**. You can also choose a **StorSave Profile** and change **Rapid RAID Recovery** settings.

Write Cache. When write cache is enabled, data is stored locally in memory on the drive before it is written to the disk drive media, allowing the computer to continue with its next task. This improves performance. However, in the event of a power failure, the data in the controller's write cache will be lost if you do not have a battery backup unit (BBU) or an uninterruptable power supply (UPS).

For additional information, see “Enabling and Disabling the Unit Write Cache” on page 102.

Read Cache. The Read Cache unit policy lets you enable either **Basic** read caching or **Intelligent** read caching. You can also disable the Read Cache unit policy, if preferred. By default, Read Cache is set to **Intelligent**.

Intelligent read caching includes a typical read-ahead caching method which is used to proactively retrieve data from media and store it locally on the controller with the anticipation that it may be requested by the host, and also

includes the Intelligent Read Prefetch (IRP) feature, which can improve performance at higher queue depth in multiple read only or mixed read/write stream environments. For additional information, see “Working with Read Cache Settings” on page 104.

Auto-Verify. Enabling Auto-Verify ensures that a verify takes place following either the Basic Auto-Verify schedule or the Advanced Auto-Verify schedule. For details, see “Enabling or Disabling Auto-Verify for a Unit” on page 107.

When Auto-Verify is not enabled, verify tasks are only run if you manually request one on the 3DM2 **Management** page or in event of an unclean shutdown.

Overwrite ECC (Continue on Source Error When Rebuilding). This policy applies only to units which are redundant. (For units which are not redundant, a check box is not available.) When this policy is set, ECC errors are ignored when they are encountered during a rebuild. When this policy is not set, a rebuild will abort upon encountering an ECC error and the unit will be set back to Degraded.

Since this option could result in the loss of some source data in the event of source errors, select this option only if you want to ensure that a rebuild will complete successfully without manual intervention. If the rebuild fails and **Overwrite ECC** is not selected, then you have the option to start a rebuild manually. It is recommended that you execute a file system check when the rebuild completes.

Under **FreeBSD** use the `fsck` utility command. For example, `fsck /dev/sda1`.

Under **Linux** use the `fsck` utility command. For example, `fsck /dev/sda1`.

On **Mac OS**, you can do this using the First Aid tab in the Disk Utility—select the disk on the left and then click **Verify Disk**. If verification encounters problems, you can then use the **Repair Disk** option on the same screen.

For **OpenSolaris** you should follow your operating system’s guide to perform a file system check.

Under **Windows**, you can do this by right-clicking on the Drive and choosing Properties; then on the Tools tab, click Check Now.

For **VMware** you should follow your operating system’s guide to perform a file system check.



Note: The policy **Overwrite ECC** is equivalent to the “Continue on Source Error” option in 3BM and the “IgnoreECC” option in the CLI.

Queuing. (Not applicable for SAS drives) This policy enables or disables Native Command Queuing (NCQ) for SATA drives in the unit. By default, queuing is disabled. You can enable it, if desired.

NCQ only operates when the feature is enabled at both the drive and the controller. If a drive does not support NCQ, the policy setting for the controller is ignored.

Enabling NCQ can improve performance in many applications; it causes command reordering to be done on the drive itself.

StorSave Profile. The StorSave feature includes an option that lets you change the StorSave Profile used for a unit. Three profiles are available: Protection, Balanced, and Performance. These profiles automatically adjust several different factors that affect protection and performance, including whether FUA (Forced Unit Access) is honored, whether Write Journaling is enabled, and whether Disable Cache on Degrade is enabled. For additional information, see “Setting the StorSave Profile for a Unit” on page 111.



Note: If the write cache setting is disabled for a unit, the StorSave Profile capability does not apply and is automatically disabled.

Rapid RAID Recovery. Determines which Rapid RAID Recovery option to use, **All**, **Rebuild** or **Disable**. **All** will apply the policy to both rebuilds and unclean shutdowns. **Rebuild** will apply only to rebuilds. You can switch between **All** and **Rebuild** settings. However, once Rapid RAID Recovery is disabled for the unit, it cannot be re-enabled. For additional information, see “Rapid RAID Recovery” on page 113.

Unit Names

Units can be assigned names. A name can be assigned when the unit is created and can be changed from this screen. For additional information, see “Naming a Unit” on page 99.

Other Controller Settings

The Other Controller settings displays information about additional settings, some of which can only be changed in the BIOS (3BM) or CLI. 3BM is not available for Mac users.

Auto-Rebuild. The Auto-Rebuild policy determines how the controller firmware will attempt to rebuild degraded units.

When Auto-Rebuild is disabled, only spares will be used to automatically rebuild degraded units. When Auto-Rebuild is enabled, the firmware will

automatically select drives to use for rebuilding a degraded unit using the following priority order.

- Smallest usable spare.
- Smallest usable unconfigured (available) drive.
- Smallest usable failed drive.

For additional information, see “Setting the Auto-Rebuild Policy” on page 71.

Auto-Carving. Auto-carving can be enabled or disabled by selecting the appropriate radio button.

When this feature is enabled, any unit that is over a specified size (known as the *carve size*) will be broken down into multiple volumes of that size, plus a remainder volume. The default carve size is 2048 GB (2 TB). For example, using the default carve size, if the unit is 2.5 TB then it will contain two volumes, with the first volume containing 2 TB and the second volume containing 0.5 TB. If the unit is 5.0 TB then it will contain 3 volumes, with the first two volumes containing 2 TB each and the last volume containing 1 TB.

Carve Size. Sets a size for dividing up units into volumes when Auto-Carving is enabled. This setting can be between 1024 and 2048 GB.

Number of Drives Per Spin-up. Number of drives that will spin up at the same time when the controller is powered up. (This setting only applies when the feature is supported by the disk drives.)

Delay between Spin-ups. The delay time (in seconds) between drive groups that spin up at one time on this particular controller.

Export Unconfigured Disks. This setting is not available for 9750 controllers.

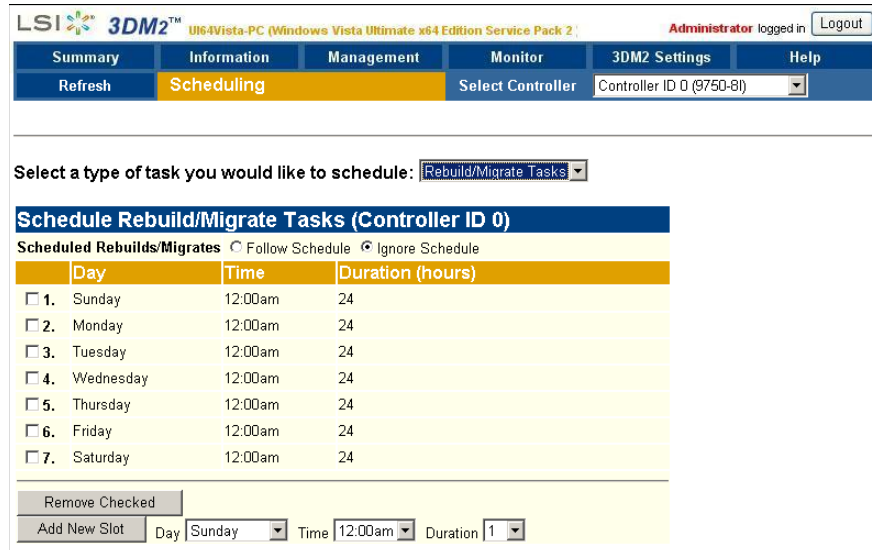
Number of Controller Phys. The number of phy connections possible on the controller. For example the 9750-8i RAID controller has 8 phys and the 9750-24i4e controller has up to 28 phys.

Update Firmware

The Update Firmware function allows you to update the firmware of your 3ware RAID controller to the latest version, which allows you to take advantage of new features and fixes. For additional information, see “Updating the Firmware Through 3DM2” on page 174.

Scheduling page

Figure 102. Scheduling Page



LSI 3DM2™ U16-Vista-PC (Windows Vista Ultimate x64 Edition Service Pack 2) Administrator logged in Logout

Summary Information Management Monitor 3DM2 Settings Help

Refresh Scheduling Select Controller Controller ID 0 (9750-81)

Select a type of task you would like to schedule: Rebuild/Migrate Tasks

Schedule Rebuild/Migrate Tasks (Controller ID 0)

Scheduled Rebuilds/Migrates Follow Schedule Ignore Schedule

	Day	Time	Duration (hours)
<input type="checkbox"/> 1.	Sunday	12:00am	24
<input type="checkbox"/> 2.	Monday	12:00am	24
<input type="checkbox"/> 3.	Tuesday	12:00am	24
<input type="checkbox"/> 4.	Wednesday	12:00am	24
<input type="checkbox"/> 5.	Thursday	12:00am	24
<input type="checkbox"/> 6.	Friday	12:00am	24
<input type="checkbox"/> 7.	Saturday	12:00am	24

Remove Checked

Add New Slot Day Sunday Time 12:00am Duration 1

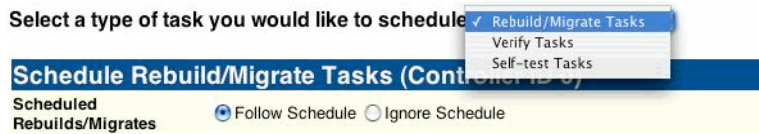
The Scheduling page appears when you choose **Management >> Scheduling** from the menu bar.

The Scheduling page lets you set up a schedule for when background tasks (rebuild, migrate, initialize, verify, and self-test) should occur. Background tasks can have impact on the performance of your system, so you may prefer to schedule them at times when they will be least disruptive, such as in the middle of the night or on a weekend. For details about the different background tasks, see “Background Tasks” on page 145.

Select a type of task you would like to schedule. You start by selecting the type of task for which you want to set the schedule from the drop-down list at the top of the page.

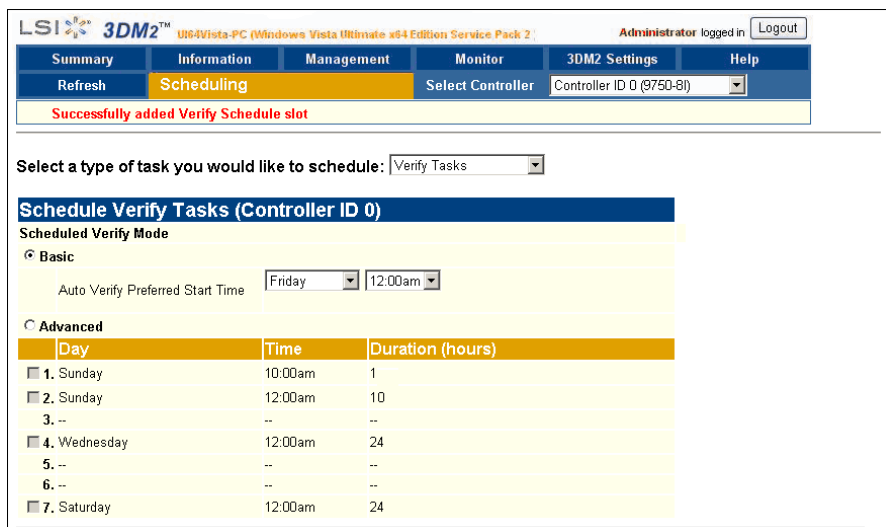
- Rebuild/migrate tasks (also applies to initialization)
- Verify tasks (also applies to media scans)
- Self-tests

3DM2 then updates the page to show you schedule details for that type of task.



Scheduled Rebuild/Migrates. You can enable or disable the schedule for the Rebuild/Migrate tasks by selecting either **Follow Schedule** or **Ignore Schedule**. When schedules are set to be ignored, these tasks can be performed at any time, and are not restricted to the scheduled times.

Scheduled Verify Mode. You can select either **Basic** or **Advanced** verify mode. Basic verify creates a once a week schedule. Advanced verify has seven scheduling slots per week, similar to the Rebuild/Migrate schedule. For more information, see “Selecting Advanced or Basic Verify Schedules” on page 166.



Task Schedules

Initially, 7 schedule slots are defined, for 24 hours each. This means that even if **Follow Schedule** is enabled for Rebuild/Migrate or if **Advanced** is selected for Auto-Verify, this schedule is equivalent to **Ignore Schedule**, because tasks can run at any time, round the clock.

A maximum of 7 slots can be created, so to set a different schedule, start by deleting one or more of the existing scheduled slots, and then add new slots.

For step-by-step instructions for adding and removing schedules, and setting schedules to be followed or ignored, see “Scheduling Background Tasks” on page 163.

Self-test Schedules

Unlike scheduling of rebuilds and verifies, scheduling of self-tests is always followed. To disable self-tests you either remove all schedule times, or uncheck the tests listed in the Tasks column.



Note: Only the checked tasks will be run during the scheduled times. If none of the tasks are checked, self-tests will never run, even if you have scheduled time slots set.

Check SMART Thresholds. This test checks to see whether SMART thresholds have been exceeded.

The SMART thresholds indicate when a SATA or SAS drive is likely to fail, based on the number of errors that have been recorded through SMART (Self-Monitoring, Analysis and Reporting Technology).

If any of the disk drives have detected a “threshold exceeded” condition, then an AEN is logged to the 3DM2 Alarms page. Moreover, if anything unusual is found during any self-test, it will be logged as an Alarm.

Maintenance page

Figure 103. Maintenance Page

LSI 3DM2™ UI64Vista-PC (Windows Vista Ultimate x64 Edition Service Pack 2) Administrator logged in Logout

Summary Information Management Monitor 3DM2 Settings Help

Refresh Maintenance Select Controller Controller ID 0 (9750-8)

Rescan Controller (This will scan all ports for newly inserted drives/units)

Unit Maintenance (Controller ID 0)

Unit	Drives	RAID	Controller	Capacity	Status	Actions
Unit 0	5 drives	RAID 6	Zygoite 1	100.55 GB	OK	
VPort 7			MAXTOR ATLAS15K2_36SAS	34.25 GB	OK	[Remove Drive]
VPort 8			MAXTOR ATLAS15K2_36SAS	34.25 GB	OK	[Remove Drive]
VPort 9			MAXTOR ATLAS15K2_36SAS	34.25 GB	OK	[Remove Drive]
VPort 10			MAXTOR ATLAS15K2_36SAS	34.25 GB	OK	[Remove Drive]
VPort 11			MAXTOR ATLAS15K2_36SAS	34.25 GB	OK	[Remove Drive]
Unit 1	5 drives	RAID 6	Zygoite 2	100.55 GB	OK	
VPort 1			MAXTOR ATLAS15K2_36SAS	34.25 GB	OK	[Remove Drive]
VPort 2			MAXTOR ATLAS15K2_36SAS	34.25 GB	OK	[Remove Drive]
VPort 3			MAXTOR ATLAS15K2_36SAS	34.25 GB	OK	[Remove Drive]
VPort 4			MAXTOR ATLAS15K2_36SAS	34.25 GB	OK	[Remove Drive]
VPort 5			MAXTOR ATLAS15K2_36SAS	34.25 GB	OK	[Remove Drive]

Verify Unit Rebuild Unit Migrate Unit Remove Unit Delete Unit

*Before removing or deleting a unit, make sure there is no I/O on the unit and unmount it

Available Drives (Controller ID 0)

VPort	Model	Capacity	Type	Phy	Slot	Status
<input type="checkbox"/> 0	MAXTOR ATLAS15K2_36SAS	34.25 GB	SAS	--	Enclosure 0 Slot 10	OK
<input type="checkbox"/> 6	SAMSUNG HD160JJ	149.05 GB	SATA	0	--	OK
<input type="checkbox"/> 13	SAMSUNG HD160JJ	149.05 GB	SATA	2	--	OK

(De-)Select All Drives

Create Unit Remove Drive Set Spare(s) Clear Configuration

The Maintenance page appears when you choose **Management >> Maintenance** from the menu bar.

The Maintenance page lets you perform maintenance tasks on existing units on the current controller and lets you create new units by configuring available drives.

Information about the Maintenance page is organized under these headings:

- Rescan Controller
- Unit Maintenance
- Maintenance Task Buttons for Existing Units
- Available Drives (to Create Units)
- Maintenance Task Buttons for Available Drives

Rescan Controller

The **Rescan Controller** button scans the ports on the controller. Rescanning updates the list of available drives shown and updates the status of all attached disks. If error conditions have been fixed, the status is updated to reflect that.

Rescanning is useful in a variety of maintenance tasks. For example, if you physically plug in a drive and want the controller to recognize the newly plugged-in drive, Rescan will find it.



Note: If you unplug a drive without first removing it through 3DM2, Rescan may not recognize it as gone unless the drive was in use or until it is required by the system. Always use the **Remove** link to remove a drive before unplugging it.



Warning: Physically removing or adding drives which are not in hot swap bays can result in a system hang or may even damage the system and the drive.

Rescan checks all ports. It checks empty ports for newly plugged-in drives. If those drives were previously part of a 3ware RAID configuration and they still have valid DCB (Disk Configuration Block) information on them, the controller tries to piece them back together into a working unit. If a working unit can be formed, it will appear in the Unit Maintenance list when the scan is complete, and the operating system will be notified of the unit.

- In Linux, FreeBSD, or OpenSolaris a device node will be associated with each unit created.
- In Windows, you will see additional disk(s) report under Disk Management..
- In Mac OS, the unit shows up under Disk Utility.
- In VMware you need to use vSphere client and go to the Configuration page. Under Storage Adapter, select LSI 3ware 9750 and perform a rescan for the disk to be available for use.

This process is known as importing drives.

If new drives do not have any data indicating they were previously part of a 3ware RAID configuration, they will appear in the Available Drives list.

In addition, if there is a unit with the status Inoperable before a rescan (for example, a RAID 5 unit missing 2 or more drives), and a rescan finds drives that complete the unit, the inoperable unit will become a valid unit.

Unit Maintenance

The Unit Maintenance section of the page lists all existing units on the current controller, and displays summary information about them.

The top row shows information about the unit, while subsequent rows show summary information about each drive in the unit.

Unit Information



Unit	# drives	RAID	Name	Capacity	Status	Action
Unit 0	2	RAID 1 PrimaryMirror		465.65 GB	VERIFYING 80%	[Stop Verify]
	Port 0		ST3500641NS	465.76 GB	OK	[Remove Drive]
	Port 1		ST3500641NS	465.76 GB	OK	[Remove Drive]

[Verify Unit](#)
[Rebuild Unit](#)
[Migrate Unit](#)
[Remove Unit](#)
[Delete Unit](#)

*Before removing or deleting a unit, make sure there is no I/O on the unit and unmount it

Unit Number. The unit number assigned to the unit by the firmware. Use the checkbox next to the unit to select a unit before clicking one of the task buttons.

Drives. Number of drives in the unit.

Type of Unit. Type of unit: RAID 0, RAID 1, RAID 5, RAID 6, RAID 10, RAID 50, or Single Disk. If the unit has been given a unique name, it shows beneath the RAID type.

Name of Unit. User-assigned unique name of the unit. The default setting is blank.

Capacity. The usable capacity (size) of the unit.

Status. Operational status of the unit: Ok, Rebuilding, Initializing, Verifying, Migrating, Degraded, or Inoperable (missing drives). When Rebuilding, Initializing, Migrating, or Verifying, the percentage (%) complete is also shown. The percentage complete can be active or paused. To see whether this task is currently active or paused, click on the unit number to display the Unit Details page, which has that information. For an explanation of the statuses, see “Unit Statuses” on page 137.

Drive Information

VPort. The VPort (virtual port) to which the drive is connected.

Model. The model of the drive.

Capacity. The capacity (size) of the drive.

Status. The status of the drive: OK, Not Supported, Not Present, and so forth. If you need help regarding a status displayed here, please contact Technical Support. For more information, see “Drive Statuses” on page 138.

Remove Drive. The **Remove Drive** link removes a drive from the controller so that you can safely unplug it. In the Unit Maintenance section, this link is only provided for drives that can be safely removed without creating an inoperable unit. (For example, a RAID 5 missing 2 or more drives or a RAID 0 missing 1 or more drives would become inoperable.) If you remove a drive from a redundant unit, the unit will become degraded. Once a unit has become degraded, additional drives cannot be removed without making it inoperable, so no **Remove Drive** link will display.



Warning: Physically removing drives which are not in hot swap bays can result in a system hang, data loss, or may even damage the system and the drive.

Maintenance Task Buttons for Existing Units

Below the list of units, a row of task buttons lets you perform maintenance and configuration tasks related to the unit. Before clicking one of these buttons, select the appropriate unit.



Unit Maintenance (Controller ID 0)					
Unit 0	2 drives	RAID 1 Primary Mirror	465.65 GB	VERIFYING 60%	[Stop Verify]
Port 0		ST3500641NS	465.76 GB	OK	[Remove Drive]
Port 1		ST3500641NS	465.76 GB	OK	[Remove Drive]

Task Buttons: [Verify Unit] [Rebuild Unit] [Migrate Unit] [Remove Unit] [Delete Unit]

*Before removing or deleting a unit, make sure there is no I/O on the unit and unmount it.

Verify Unit. Puts the selected unit in verifying mode. If the Advanced Verify schedule is selected on the Scheduling page, the unit will not start actively verifying until the scheduled time, and the status will indicate “Verify-Paused.” (The Unit Details page will indicate whether a unit is actively verifying.) If the Basic Verify schedule is active, clicking **Verify Unit** begins the verification process, and verify will begin within approximately 10 to 15 minutes.

If the unit you selected to verify is a redundant unit, the redundancy of the unit will be verified. For example, it will check parity for a RAID 5 or check data consistency for a RAID 1. If the unit you checked is not a redundant unit, verify will do a surface scan of the media. During verification, I/O continues normally. For RAID 0 and single disks, there is only a slight performance loss. For redundant units, you can set the background task rate on the Controller Settings page to specify whether more processing time should be given to verifying or to I/O. For more information, see “About Verification” on page 149 and “Setting Background Task Rate” on page 162.

While a unit is verifying, the status changes to Verifying and a **Stop Verify** link appears in the right-most column of the Unit Maintenance table.



Note: If the unit has not previously been initialized and you click **Verify Unit**, the initialization process starts. Initialization cannot be halted, so no Stop Verify link appears. (Initialization can be paused, however, through Scheduling. Initialization follows the Rebuild/Migrate schedule, so turning on scheduling for Rebuild/Migrate will pause initialization, as well.) For more information about initialization, see “About Initialization” on page 146.

Rebuild Unit. Replaces a failed drive in a degraded unit with an available drive and begins rebuilding the RAID. When you select a degraded unit and click **Rebuild Unit**, a dialog box listing available drives appears, so that you

can select the drive you want to use. If the degraded unit has more than one failed drive (for example, a RAID 10 where both mirrored pairs each have a failed drive), you will repeat this process a second time.

If rebuild scheduling is enabled on the Scheduling page, the unit will not start actively rebuilding until the scheduled time, and the status will change to say “Rebuild-Paused.” (The Unit Details page indicates whether a unit is actively rebuilding.) If rebuild scheduling is not enabled, the rebuild process will begin right away.

For more information about rebuilds, see “To verify a unit through 3BM” on page 153.

Migrate Unit. Reconfigures a unit while it is on-line. Migration can be used to change the RAID level, to expand the capacity by adding additional drives, or to change the stripe size.



Warning: Once migration of a unit is started, it can be paused, but it can not be cancelled.

When you select a unit and click **Migrate Unit**, a dialog box appears which lists the drives in the unit and any additional available drives. In the dialog box are two drop-down menus, one for choosing the RAID level and one for choosing stripe size.

Figure 104. Migrating a unit

Unit to Migrate				
Unit 1	5 drives	RAID 6	100.55 GB	OK
Select drive(s) to use to migrate				
<input type="checkbox"/>	Port 0	MAXTOR ATLAS151K2_36SAS	34.25 GB	OK
<input type="checkbox"/>	Port 6	SAMSUNG HD160JJ	149.05 GB	OK
<input type="checkbox"/>	Port 13	SAMSUNG HD160JJ	149.05 GB	OK
Type	RAID 5		Stripe	64k
OK Cancel				

You can only migrate a unit to a RAID level that will be equal to or larger than the original unit. For example, you can migrate from a RAID 5 array with 4 drives to a RAID 0 with four drives but you cannot migrate from a RAID 5 with four drives to a RAID 10 with four drives.

After you have specified changes to the unit, the Unit Maintenance screen reflects your changes and shows the percentage of migration completed.

While the unit is migrating, you can still access the unit as normal but the performance will be lower. You can adjust the I/O rate with the radio buttons on the Controller Settings page. (See “Setting Background Task Rate” on page 162.)

Remove Unit. Removes a selected unit and allows you to unplug the drives and move the unit to another controller. The data on the unit remain intact.



Caution: Before you click **Remove Unit**, make sure the unit you are removing is unmounted from the operating system and that the system is not accessing it.

If a unit is not unmounted and you remove it, it is the equivalent of physically yanking a hard drive out from under the operating system. You could lose data, the system could hang, or the controller could reset.

Under certain operating systems, if you try to remove the unit in either CLI or 3DM2 and the unit is still in use, you get an error message telling you the unit can not be removed. Make sure you do not have any utility accessing the unit then follow your system instructions on the procedure to unmount the unit before removing it.

For how to unmount a unit under various operating systems, see the discussing under “Deleting a Unit through 3DM2” on page 121.



Warning: Physically removing drives which are not in hot swap bays can result in a system hang, data loss, or may even damage the system and the drive.

Delete Unit. Deletes the selected unit and allows you to use the drives to create another unit. The drives appear in the list of Available Drives.



Caution: Before you click **Delete Unit**, make sure the unit you are removing is unmounted from the operating system and that the system is not accessing it.

Devices can be unmounted through the operating system. For details, see the discussion under Remove Unit, above.



Warning: When a unit is deleted, the data will be permanently deleted: the drives cannot be reassembled into the same unit. If you want to reassemble the drives on another controller and access the existing data, use **Remove Unit** instead of **Delete Unit**.

After deletion, the operating system is notified that the unit was deleted.

- In FreeBSD, Linux, and OpenSolaris the device node associated with this unit is removed.
- In Windows the disk is removed from Disk Management.
- In Mac OS the disk is removed from Disk Utility.
- In VMware, the deleted unit won't be updated by the operating system until you perform a rescan on the RAID controller.

Available Drives (to Create Units)

This section lists the drives on the controller which are not currently configured as part of a unit. The VPort number, model, capacity, type, phy, slot, and status are all displayed, as they are for drives in existing units.

The available drives can be sorted by VPort, model, capacity, type, phy, or slot by clicking on the column headings. (For details about these attributes, see “Drive Information page” on page 195.)

Remove Drive. The Remove Drive button removes a drive from the controller so that you can safely unplug it. Select the box for any drive in the Available Drives list you wish to remove.



Warning: Physically removing drives which are not in hot swap bays can result in a system hang or may even damage the system and the drive.

Maintenance Task Buttons for Available Drives

Below the list of available drives, a row of task buttons lets you work with available drives to create new units, remove drives, designate drives as spares, and clear the configuration of a spare so that it can be used for another purpose.

Create Unit

Use the **Create Unit** button to create a unit for use on the current controller. Begin by selecting the drives you want to use in the list of Available Drives, and then click **Create Unit**. You will be prompted to select the unit Type, Name, Stripe size (if applicable), and unit policy settings.

A window like the one below shows the drives you selected, and lets you specify configuration settings.

Figure 105. Configuration Window in 3DM2

Selected drive(s) to use to create					
VPort 0	SAMSUNG HD160JJ	SATA	149.05 GB	OK	
VPort 1	SAMSUNG HD160JJ	SATA	149.05 GB	OK	
VPort 2	SAMSUNG HD160JJ	SATA	149.05 GB	OK	
VPort 3	SAMSUNG HD160JJ	SATA	149.05 GB	OK	

Type: RAID 5 Name: Stripe: 256KB

Write Cache Auto Verify Queuing Overwrite ECC

Read Cache: Intelligent StorSave: Balanced Rapid RAID Recovery: All

OK Cancel

For more detailed instructions, see “Configuring a New Unit” on page 79.

Type. The drop-down list lists the possible RAID configurations for the drives selected in the list of Available Drives. Available configurations may include RAID 0, RAID 1, RAID 5, RAID 6, RAID 10, RAID 50, and Single Disk. For information about these configurations, see “Available RAID Configurations” on page 6.

Depending on the size of the unit, a RAID 50 unit will contain 2 or more subunits. For example, when you are configuring a RAID 50 with twelve drives, an additional field appears, in which you select the number of drives per subunit—3, 4, or 6.

Figure 106. Configuring a RAID 50 with 12 Drives

Selected drives to create				
VPort 0	WDC WD1600BB-00DAA0	149.05 GB	OK	
VPort 1	WDC WD1600BB-00DAA0	149.05 GB	OK	
VPort 2	WDC WD1600BB-00DAA0	149.05 GB	OK	
VPort 3	WDC WD1600BB-00DAA0	149.05 GB	OK	
VPort 4	WDC WD1600BB-00DAA0	149.05 GB	OK	
VPort 5	WDC WD1600BB-00DAA0	149.05 GB	OK	
VPort 6	WDC WD1600BB-00DAA0	149.05 GB	OK	
VPort 7	WDC WD1600BB-00DAA0	149.05 GB	OK	
VPort 8	WDC WD1600BB-00DAA0	149.05 GB	OK	
VPort 9	WDC WD1600BB-00DAA0	149.05 GB	OK	
VPort 10	WDC WD1600BB-00DAA0	149.05 GB	OK	
VPort 11	WDC WD1600BB-00DAA0	149.05 GB	OK	

Type: RAID 50 Name: Stripe: 256KB Drives per subunit: 3

Write Cache Auto Verify Queuing Overwrite ECC

Read Cache: Intelligent StorSave: Balanced Rapid RAID Recovery: All

OK Cancel

Name. You can enter a name for the unit.

Stripe. The drop-down list of stripe sizes lists the possible stripe sizes for the configuration you selected in the RAID level drop-down.

Using the default stripe size of 256 KB usually gives you the best performance for mixed I/Os. If your application has some specific I/O pattern

(purely sequential or purely random), you might want to experiment with a different stripe size.

Write Cache, Auto-Verify, and Overwrite ECC. These check boxes let you set the policies for the unit. These policies can also be set and changed on the Controller Settings page. For details about these policies, see “Unit Policies” on page 201.



Note: If the configuration window disappears while you are selecting drives, 3DM2 may have refreshed. Click **Create Unit** again. If desired, you can reduce the frequency with which information refreshes in 3DM2, or disable refresh temporarily, on the 3DM2 Settings page.

Read Cache. By default, Read Cache is set to Intelligent. You can change it to Basic, or disable it, if desired. Setting the appropriate type of Read Cache can improve performance for different types of applications. For details, see “Working with Read Cache Settings” on page 104.

StorSave. You can specify the StorSave Profile to be used for the unit. Three profiles are available: Protection, Balanced, and Performance. For more information, see “Setting the StorSave Profile for a Unit” on page 111.

Rapid RAID Recovery. Determines which Rapid RAID Recovery option to use, **All**, **Rebuild** or **Disable**. **All** will apply the policy to both rebuilds and unclean shutdowns. **Rebuild** will apply only to rebuilds. You can switch between **All** and **Rebuild** settings, but, once Rapid RAID Recovery is disabled for the unit, it cannot be re-enabled. For details, see “Rapid RAID Recovery” on page 113.

Set Spare

Use the **Set Spare** button to set one or more drives as spares. Select the drives you want to use from the list of Available Drives, then click **Set Spare**.

Clear Configuration

Use the **Clear Configuration** button to reset a Spare to be an Available Drive. Select the drives you no longer want to be Spares, then click **Clear Configuration**.

Alarms page

Figure 107. Alarms Page

LSI 3DM2™ UI64Vista-PC (Windows Vista Ultimate x64 Edition Service Pack 2) Administrator logged in Logout

Summary Information Management Monitor 3DM2 Settings Help

Refresh Alarms Select Controller Controller ID 0 (9750-8i)

Clear Alarms Legend: INFO WARNING ERROR

Sev	Time	Message (Click for Help)
INFO	Apr 26, 2010 02:27:56PM	{0x04:0x002B}: Verify completed: unit=0
INFO	Apr 26, 2010 02:00:06PM	{0x04:0x0029}: Verify started: unit=0
INFO	Apr 22, 2010 11:45:05AM	{0x04:0x001A}: Drive inserted: encl=0, slot=4
INFO	Apr 22, 2010 11:44:58AM	{0x04:0x0063}: Enclosure added: encl=0
WARNING	Apr 22, 2010 11:40:28AM	{0x04:0x0062}: Enclosure removed: encl=0
INFO	Apr 22, 2010 11:40:07AM	{0x04:0x0063}: Enclosure added: encl=0
WARNING	Apr 22, 2010 11:39:43AM	{0x04:0x0062}: Enclosure removed: encl=0
INFO	Apr 22, 2010 11:38:33AM	{0x04:0x0063}: Enclosure added: encl=0
WARNING	Apr 22, 2010 11:27:28AM	{0x04:0x0062}: Enclosure removed: encl=0
INFO	Apr 22, 2010 11:07:56AM	{0x04:0x0063}: Enclosure added: encl=0
INFO	Apr 22, 2010 11:06:02AM	{0x04:0x0053}: Battery capacity test is overdue
INFO	Apr 21, 2010 03:58:38PM	{0x04:0x0063}: Enclosure added: encl=0
WARNING	Apr 21, 2010 03:57:48PM	{0x04:0x0062}: Enclosure removed: encl=0
INFO	Apr 13, 2010 07:54:28PM	{0x04:0x0056}: Battery charging completed

Last updated Mon, Apr 26, 2010 02:56:18PM
 This page will automatically refresh every 5 minute(s)
 3DM2 version 2.11.00.013
 API version 2.08.00.014B
 Copyright (c) 2010 LSI Corporation

The Alarms page appears when you click **Monitor >> Alarms** on the menu bar.

This page displays a list of AENs (asynchronous event notifications) received from the controller displayed in the drop-down list in the menu bar.

Up to 1000 events can be listed. After the 1000-limit is reached, the oldest events are deleted, as new ones occur.

You can sort the events by severity or time. To do so, just click the column header.

For information about a particular event, click it on the Alarms page; the 3DM2 Help will open with information about the event. For a complete listing of the alarms that appear on the Alarms page, see “Error and Notification Messages” on page 235.

Clear Alarms. The **Clear Alarms** button removes all alarms shown in the list.

Sev. Shows the severity of the event. Three levels are provided:

- Errors are shown next to a red box
- Warnings are shown next to a yellow box
- Information is shown next to a blue box

Time. The time shown for alarms is the time the alarm was received by the driver from firmware.

Message. The specific text relating to the alarm condition.

Battery Backup page

Figure 108. Battery Backup Page

Battery Backup Information (Controller ID 0)	
Battery Backup Unit	PRESENT
Firmware	N/A
Serial #	LSI101000G0804080821
BBU Ready	Ready
BBU Status	OK
Battery Voltage	OK
Battery Temperature	OK (73°F 23°C)
Estimated Backup Capacity	136 hours
Last Capacity Test	xx-xxx-xxxx [Test Battery Capacity]
Battery Installation Date	08-Oct-2009

Last updated Mon, Apr 26, 2010 02:57:52PM
 This page will automatically refresh every 5 minute(s)
 3DM2 version 2.11.00.013
 API version 2.08.00.014B
 Copyright (c) 2010 LSI Corporation

The Battery Backup page appears when you choose **Monitor >> Battery Backup** on the menu bar. Use this page to determine whether a backup battery is present, see details about it, and perform a battery test.

Battery Backup Unit. Indicates whether the BBU is present.

Serial Number. Indicates the BBU serial number.

BBU Ready. Indicates if the BBU is able to backup the 3ware RAID controller or not. If the BBU is “Ready”, write cache can be enabled on the 3ware RAID controller. When the status is not “Ready,” write caching is automatically disabled on all units attached to the controller.

BBU Status. Indicates the status of the BBU. Possibly BBU statuses include the following:

- **OK.** The BBU is functioning normally.
- **Not Present.** The BBU was not detected or is disabled. (The BBU can be disabled using CLI.)
- **No Battery.** No battery pack is installed in the BBU.
- **Testing.** A battery capacity test is in process.
- **Charging.** The battery is being charged. Charging of the battery occurs automatically if the battery voltage falls too low. This normally occurs

about once a week to top off the charge level; the process does not change the BBU readiness state.

If the battery is ever discharged through a backup cycle or if the system power is off for more than two weeks, the battery status changes to “Charging” the next time the system is powered on. This indicates the BBU is not able to backup the 3ware RAID controller. When the BBU is in the charging state, write caching is disabled automatically on all units attached to the controller.

- **Fault.** The BBU detected a fault. This occurs if the voltage or temperature is outside the acceptable range.
- **Error.** Other BBU error. Please contact LSI Technical Support.
- **Weak Battery.** The battery should be replaced soon. The results of a battery health test or capacity test indicate that the battery is below the warning threshold (48 hours).
- **Failed Battery.** The battery failed a test and must be replaced. A “Failed Battery” status is displayed if the battery failed the health test or the battery capacity is below the error threshold (24 hours). The battery must be replaced.

Battery Voltage. Indicates the voltage status of the battery. The BBU measures and evaluates the battery voltage continuously. If the voltage falls outside the normal range, warning or error level AENs are generated. In the case of a voltage error the BBU status will change to “Fault” and the battery will be disconnected electronically.

Battery Temperature. Indicates the temperature status of the battery. The BBU measures and evaluates the battery pack temperature continuously. If the temperature falls outside the normal range, warning or error level AENs are generated based on the measured temperature. In the case of a temperature error, the BBU status will change to “Fault” and the battery will be disconnected electronically.

Estimated Backup Capacity. Indicates the estimated backup capacity in hours. This is the amount of time that the battery backup unit can protect the data in the 3ware RAID controller's cache memory. This field is set to zero at the start of a new test and is updated after the test completes. A capacity of zero will also show if the BBU is disconnected and then reconnected.

Under optimal conditions, a battery can protect for up to 72 hours. However, with a fresh battery, you may see a higher number in this field. As the battery ages, the backup capacity diminishes.

Last Capacity Test. Indicates the date when the last battery test was completed. To test the battery click the **Test Battery Capacity** link. For details, see “Testing Battery Capacity” on page 176.

Battery Installation Date. Indicates when the BBU last detected the battery pack was removed and replaced.

Enclosure Summary page

Figure 109. Enclosure Summary Page

LSI 3DM2™ UI64Vista-PC (Windows Vista Ultimate x64 Edition Service Pack 2) Administrator logged in Logout										
Summary		Information		Management		Monitor		3DM2 Settings		Help
Refresh		Enclosure Support		Select Controller		Controller ID 0 (9750-8)				
Enclosure Summary										
ID	Status	Vendor	Product ID	Slots	Drives	Fans	Temp Sensor	Power Supply		
0	OK	LSI	DE1600-SAS	12	1	4	4	2		
Last updated Mon, Apr 26, 2010 02:58:53PM This page will automatically refresh every 5 minute(s) 3DM2 version 2.11.00.013 API version 2.08.00.014B Copyright (c) 2010 LSI Corporation										

The Enclosure Summary page appears when you choose **Monitor >> Enclosure Support** from the menu bar.

The Enclosure Summary page provides basic information about any enclosures attached to your system. The specific details that display depend upon your enclosure. You can find a list of supported enclosures from the Data & Interoperability tab, on http://www.lsi.com/channel/support/marketing_resources.

ID. The ID that the 3ware firmware assigns to the enclosure. This ID is also a link to a page with more detailed information about the enclosure.

Status. The status of the enclosure.

Vendor. The name of the manufacturer of the enclosure.

Product ID. The product ID of the enclosure.

Slots. The number of slots in the enclosure.

Drives. The number of drives in the enclosure.

Fans. The number of fans in the enclosure.

Temp Sensor. The number of temperature sensors in the enclosure.

Power Supply. The number of power supplies in the enclosure.

Enclosure Details page

Figure 110. Enclosure Details Page

LSI 3DM2™ U164Vista-PC (Windows Vista Ultimate x64 Edition Service Pack 2) Administrator logged in Logout

Summary Information Management Monitor 3DM2 Settings Help

Refresh Enclosure Details Select Controller Controller ID 0 (9750-8i)

Enclosure ID 0

Status	OK
Vendor	LSI
Product ID	DE1600-SAS
Revision	0314
Diagnostic	Diagnostic Text
Controller ID	1

Audio Alarm Summary

Audio Alarm	Status	State	Audibility
Audio Alarm information is not available			

Fan Summary

Fan	Status	State	Speed	RPM	Identify
0	OK	ON	Lowest	6360	<input type="checkbox"/>
1	OK	ON	Lowest	6480	<input type="checkbox"/>
2	OK	ON	Lowest	6540	<input type="checkbox"/>

Temp Sensor Summary

Temp Sensor	Status	Temperature	Identify
0	OK	31°C (87°F)	<input type="checkbox"/>
1	OK	33°C (91°F)	<input type="checkbox"/>

Power Supply Summary

Power Supply	Status	State	Voltage	Current	Identify
0	OK	ON	NORMAL	NORMAL	<input type="checkbox"/>
1	OK	ON	NORMAL	NORMAL	<input type="checkbox"/>

Slot Summary

Slot	Status	VPort	Identify
0	OK	8	<input type="checkbox"/>
1	OK	9	<input type="checkbox"/>
2	OK	10	<input type="checkbox"/>
3	OK	11	<input type="checkbox"/>
4	OK	14	<input type="checkbox"/>
5	OK	15	<input type="checkbox"/>
6	OK	12	<input type="checkbox"/>
7	OK	13	<input type="checkbox"/>
8	OK	16	<input type="checkbox"/>
9	OK	17	<input type="checkbox"/>
10	OK	18	<input type="checkbox"/>
11	OK	--	<input type="checkbox"/>

The Enclosure Details page appears when you click the ID of an enclosure on the Enclosure Summary page.

Use this page to view information about the enclosure, fans, temp sensors, power supplies, and drive slots.

Information about the Enclosure Details page is organized under these headings:

- Enclosure ID

- Fan Summary
- Temp Sensor Summary
- Power Supply Summary
- Slot Summary

Enclosure ID

Status. The status of the enclosure.

Vendor. The manufacturer of the enclosure.

Product ID. The product ID of the enclosure.

Revision. The manufacturer's revision number for the enclosure.

Diagnostic. Click the **Diagnostic Text** link to download a log of enclosure diagnostic information to your computer. If you contact LSI for support with your controller, they may ask you to use this feature. It may help identify the problem you encountered.

Controller ID. The ID of the controller connected to the enclosure.

Fan Summary

Fan. Lists the ID number associated with the fan.

Status. Will be one of OK, Failure, Not Installed, Unknown, or Off. For status definitions, see "Fan Status" on page 183.

State. Will be **ON** or **OFF**.

Speed. Fan speed is automatically controlled by the enclosure monitoring software to maintain correct enclosure temperature. Possible settings are Stopped, Lowest, Second Lowest, Third Lowest, Intermediate, Third Highest, Second Highest, Highest, and Unknown.

RPM. The fan speed in revolutions per minute.

Identify. If supported by the enclosure manufacturer, checking this box will cause an LED to blink on the enclosure containing the specified fan. If the box is grayed, identify is not supported.

Temp Sensor Summary

Temp Sensor. The ID number of the specified temperature sensor.

Status. The status of the temperature sensor. Can be OK, Failure, Not Installed, Off, or Unknown. In addition, there are threshold warnings of Over Temp Failure, Over Temp Warning, Under Temp Warning, and Under Temp Failure. For status definitions, see "Temp Sensor Status" on page 183.

Temperature. The temperature of the enclosure in Centigrade and Fahrenheit.

Identify. If supported by the enclosure manufacturer, checking this box will cause an LED to blink on the enclosure containing the specific temperature sensor. If the box is grayed, identify is not supported.

Power Supply Summary

Power Supply. The ID number associated with the specified power supply.

Status. Can be OK, Failure, Not Installed, Off, or Unknown. For status definitions, see “Power Supply Status” on page 183.

State. Indicates if the power supply is ON or OFF.

Voltage. The status of the dc voltage output of the power supply. Can be Normal, Over Voltage, Under Voltage, or Unknown.

Current. The status of the dc amperage output of the power supply. Can be Normal, Over Current, or Unknown.

Identify. If supported by the enclosure manufacturer, checking this box will cause an LED to blink on the enclosure containing the specific power supply. If the box is grayed, identify is not supported.

Slot Summary

Slot Summary. Lists the enclosure slots and indicates which ones contain drives, and the status of each drive.

Slot. The ID of the slot for a drive in the enclosure.

Status. The status of the drive in the slot. Can be **Inserted**, **Ready To Insert**, **Ready To Remove**, or **Activated**.

VPort. The VPort assigned to the drive in the slot. Clicking the link takes you to the Drive Information page. The drive you selected will be highlighted.

Identify. Check the box to cause the LED associated with that slot to blink.

3DM2 Settings page

Figure 111. 3DM2 Settings Page

The screenshot shows the 3DM2 Settings page with the following sections and fields:

- Navigation Bar:** Summary, Information, Management, Monitor, 3DM2 Settings (selected), Help. A "Refresh" button is under Summary. The user "Administrator" is logged in.
- E-mail notification:**
 - Send E-mail: Enabled Disabled
 - Notify on: INFO (dropdown)
 - Sender: someone@domain.com
 - Recipient(s): someone@domain.com
 - Mail Server (name or IP): mailserver.domain.com
 - Mail Server Login: mailserverusername
 - Mail Server Password: [masked]
 - Mail Server Port uses SSL: Yes No
 - Buttons: Save E-mail Settings, Send Test Message
- Password:**
 - Change Password For: User (dropdown)
 - Current Password: [text input]
 - New Password: [text input]
 - Confirm New Password: [text input]
 - Button: Change Password
- Page Refresh:**
 - Minutes Between Refresh: 5 (dropdown)
- HTTP Settings:**
 - Listening Port: 888 (text input)
 - Button: Change Port
- Server Configuration:**
 - Allow Remote Access: Enabled Disabled
 - Command Logging: Enabled Disabled

The 3DM2 Settings page appears when you click **3DM2 Settings** on the menu bar. Use this page to set preferences, including email notification for alarms, passwords, page refresh frequency, whether remote access is permitted, and the incoming port for 3DM2 to listen for requests.

Information about the 3DM2 Settings page is organized under these headings:

- E-mail Notification
- Password
- Page Refresh
- HTTP Settings
- Server Configuration

E-mail Notification

Use the fields in this section to set up and manage notifications of events by e-mail.

Send E-mail. This field determines whether e-mail notification is **Enabled** or **Disabled**. It is a good idea to enable this feature, so that you receive email when your units or drives have problems.

Notify On. Specifies the type of events for which notifications should be sent. A severity of **Information** will send e-mails for all alarms, a severity of **Warning** will send e-mail for alarms with severity of Warning and Error. A severity of **Error** will send e-mail for alarms with severity of Error.

Sender. Enter the email address which will appear in the “From” field.

Recipient. The e-mail address to which notifications should be sent. You can enter multiple addresses, separated by commas (,).

Mail Server (name or IP). If the machine on which you are running 3DM2 has access to a name server, you may enter the machine name of the mail server in the Server field. Otherwise, use the IP address.

Mail Server Login. If your email server requires authentication, enter the login for the server. If you are uncertain of the login, contact the administrator of the email server.

Mail Server Password. If your email server requires authentication, enter the password for the Mail Server login.

Mail Server Port uses SSL. If your mail server requires or supports encrypted email, set this to **Yes**. For more information, See “Managing E-mail Event Notification” on page 59.

Save E-mail Settings button. Saves the e-mail notification settings.

Send Test Message button. Sends a test message using the saved e-mail settings.

Password

Use the fields in this section to set the passwords for the User and Administrator. When 3DM2 is first installed, the default password for both is `3ware`.

Change Password For. Select the access level for which you are setting the password: **User** or **Administrator**. Users can only view status information in 3DM2, while Administrators can make changes and administer the controller and associated drives.

Current Password. Enter the current password.

New Password. Enter the new password.

Confirm New Password. Enter the new password a second time, to be sure you have entered it correctly.

Change Password button. Saves password changes.

Page Refresh

Minutes Between Refresh. Displays how frequently pages in 3DM2 will be refreshed with new data from the controller. To change this setting, select another option from the drop-down. If you prefer 3DM2 to only refresh when you click **Refresh Page**, select **Never**.

The Login, Help and Drive SMART data pages do not automatically refresh. All other 3DM2 pages do.

HTTP Settings

Listening Port. This field specifies the HTTP: port to be used by 3DM2 when listening for communications. The default port setting is 888.

If you change this port, make sure the port you specify is not being used. Failure to do so will cause 3DM2 to stop responding and you will have to restart it by hand.

Change Port button. Saves a new port number.

Server Configuration

Allow Remote Access. This field enables or disables the ability for users and administrators to access 3DM2 from a remote computer.

Command Logging. This field lets you enable or disable command logging. For more information, See “Controlling Command Logging in 3DM2” on page 62.

Troubleshooting

This troubleshooting section includes the following sections:

- Web Resources
- Before Contacting Customer Support
- Basic Troubleshooting: Check This First
- Command Logging
- Drive Performance Monitoring
- Problems and Solutions
- Error and Notification Messages

Web Resources

For the latest information related to 3ware RAID controllers, refer to the following LSI web sites:

- Product information, compatibility lists, software upgrades, and OS driver downloads, refer to:
<http://www.lsi.com/channel/ChannelDownloads>

From the Product Family drop-down, select *RAID Controllers*. Then in the Product list on the right, select your product, for example *3ware SAS 9750-8i*.

- 3ware KnowledgeBase, including frequently asked questions (FAQs), refer to <http://kb.lsi.com>.
- Product compatibility and interoperability lists can also be found at:
http://www.lsi.com/channel/support/marketing_resources.

On the Marketing Resource Center page, select the *Data & Interoperability* tab.

- For specific answers to questions, technical support, or to give feedback about the product, refer to our website at: <http://www.lsi.com/channel/ContactUS>.

Before Contacting Customer Support

Four screens in 3DM2 provide controller version and status information that can be helpful when contacting 3ware Customer Support with questions or for troubleshooting: Controller Summary, Controller Details, Unit Information and Enclosure Summary (The Controller Details and Unit Information screens are available from the Information tab, Enclosure Summary is available from the Monitor tab.)

You can copy and paste the information from these screens into an email using the system clipboard. When each page is displayed on the screen, highlight it using your mouse (or press Ctrl-A to select all text), press Ctrl-C to copy it to the clipboard, and then Ctrl-V to paste it into an e-mail.

You may also want to take a screen capture of these pages so that you can respond to questions about your system configuration to the Customer Support representative.

Additional useful information can be gathered from the error logs. For instructions for collecting error logs, search the LSI KnowledgeBase for keyword 12278 at <http://kb.lsi.com>.

Basic Troubleshooting: Check This First

Many error messages can be traced to improperly connected hardware. Hardware can appear to be connected, yet not be in full contact. This can cause intermittent errors that are hard to identify.

Reseat the following items to make sure they are in full contact and are not loose:

- Cables
- Power cords and power connectors
- BBU connectors
- RAID controller
- Hard drives

If you have insured that all connections are secure and the errors still occur, one strategy to confirm or rule out hardware problems is to swap suspected bad drives, cables or power cords with known good ones. You can also:

- Move the drive to a different drive slot on the controller.
- In the case of a controller, try a different computer.

Command Logging

All changes that are made to RAID configurations using 3DM2 or CLI are automatically stored in a special log file, `tw_mgmt.log`. This log can be helpful for troubleshooting problems with your RAID controller and units.

Under FreeBSD, Linux, Mac OS, OpenSolaris, and VMware Mac OSX, and FreeBSD, the `tw_mgmt.log` is in the `/var/log` directory.

For Windows 7, Windows Vista, and Windows Server 2008, `tw_mgmt.log` is in `\ProgramData\3ware`

For earlier versions of Windows, `tw_mgmt.log` is in `\Documents and Settings\All Users\Application Data\3ware`

You can enable or disable command logging through 3DM2 under Server Configuration on the 3DM2 Settings page. For more information, see “Controlling Command Logging in 3DM2” on page 62.

For more information about command logging, search the LSI KnowledgeBase for keyword 15123 at <http://kb.lsi.com>.

Drive Performance Monitoring

When one drive in a RAID unit is responding much slower than others, it reduces the performance of the entire unit.

Drive Performance Monitoring (DPM) is now available to measure drive performance, and to help identify when a specific drive is causing problems so that you can have the drive manufacturer repair or replace it.

DPM is an advanced trouble-shooting tool. Commands are available through the 3ware CLI to enable and disable DPM, and to see a range of different statistics. These statistics can be useful to LSI technical support to help you troubleshoot problems with your RAID controller and units.

Types of DPM Statistics

The following drive statistical data can be stored and reported:

- **Queue depth**, which indicates the number of read/writes that are currently outstanding.
- **IOP**, which indicates the number of read/writes that have completed
- **Transfer rate**, which indicates the number of sectors that have been read/written
- **Response time**, which indicates the execution time of all commands
- **Command read/writes**, which indicates the drive and drive sectors' accumulated read and write commands.

Available DPM Commands

Drive Performance Monitoring commands are available through the CLI. An overview of the commands is provided below. For more information about the command syntax and for examples of the report output, refer to the CLI Syntax Reference in the *3ware SATA+SAS RAID Controller Card CLI Guide, Version 10.2*.

- **Enable DPM.** This starts the collection of statistics for drives attached to your RAID controller. (`/cx dpmstat=on`).

For efficient collection of data, initiate read/write activity on the specified controller. The numbers will change over time as the new and old data are averaged.

- **Disable DPM.** This stops the collection of statistics. (`/cx dpmstat=off`)

DPM is disabled by default since there is overhead in maintaining the statistics. DPM is also disabled following a reboot or power-on. Turning off DPM does not clear the statistical data that has been recorded. To clear the data, use the command `/cx/px set dpmstat=clear [type=ra|lct|ext]`.

- **Display a DPM Summary.** This shows whether DPM is On or Off, and provides summary statistics for drives attached to a controller. (`/cx show dpmstat`)

Note that if DPM is Off, this summary may still show data, although that data will be static, and not changing over time. Disabling DPM does not clear the existing data. That is done separately, on a per-port basis (see below.)

You can also show a subset of summary data, for individual types of statistics (instantaneous, running average, or extended drive statistics), by specifying a type attribute with the command.

- **Display Specific Drive Statistic.** On a per-port basis, you can display five different statistical reports:
 - **Instantaneous.** This measurement provides a short duration average. (`/cx/px show dpmstat type=inst`)
 - **Running Average.** Running average is a measure of long-term averages that smooth out the data, and results in older results fading from the average over time (`/cx/px show dpmstat type=ra`)
 - **Long Command Times.** This a collection of the commands with the longest read/write response time. (`/cx/px show dpmstat type=lct`)
 - **Histogram Data.** The histogram categorizes the read/write execution times and group them together based on time frames. (`/cx/px show dpmstat type=histdata`)
 - **Extended Drive Statistics.** The extended drive statistics refers to statistics of a drive's read commands, write commands, write

commands with FUA (Force Unit Access), flush commands, and a drive sectors's read, write, and write commands with FUA.

`/cx/px show dpmstat type=ext`)

- **Clear Individual Statistic Counters.** On a per-port basis, you can clear specific statistic counters, using these commands:
 - `/cxpx set dpmstat=clear`
 - `/cxpx set dpmstat=clear type=ra`
 - `/cxpx set dpmstat=clear type=lct`
 - `/cxpx set dpmstat=clear type=ext`

Problems and Solutions

This section covers some common problems and solutions. It is organized into the following sections:

- Enclosure-Related Problems
 - An LED is blinking red on an enclosure.
- Hardware Installation Problems
 - The 3ware BIOS screen never appears
 - Need to boot from a non-3ware device without changing the boot order
- Software Installation Problems
 - The 3ware RAID controller was configured without problems, but the system does not boot
 - A unit shows up as unusable, because of missing drives:
- Problems in 3DM2 and 3BM
 - A 3ware RAID controller does not show in the list of controllers
 - When booting a system, a drive is not showing up in the startup screens, in 3BM, or in 3DM2

Enclosure-Related Problems

An LED is blinking red on an enclosure.

A blinking red LED on an enclosure may indicate that there is a “predicted fault” on the drive in that slot. Actual LED behavior will depend on the enclosure manufacturer. Refer to the user guide for your enclosure.

Such an error can result from a number of different factors, including a SMART error, read error, or cable error. The drive has not failed yet, but may fail soon.

For additional information about the LED indicators on an enclosure, see “Enclosure Drive LED Status Indicators” on page 136.

Hardware Installation Problems

Two common problems during hardware installation are listed below. For details related to other issues, check the LSI KnowledgeBase at <http://kb.lsi.com>.

The 3ware BIOS screen never appears

- The 3ware RAID controller may not be installed properly. Reinstall the hardware and reboot.
- The motherboard may be functional, but may not be compatible. Please check the Motherboard Compatibility List, available on the LSI website at http://www.lsi.com/channel/support/marketing_resources, through the Data & Interoperability tab, to see if your motherboard has been tested by 3ware. If you have a different type of motherboard available, you may want to test the controller in it to see if the 3ware BIOS screen appears.
- The motherboard's BIOS may need to be upgraded. Check the web site of the motherboard manufacturer to download and install their latest BIOS.
- The motherboard may not be functional.
- You may not have the latest 3ware firmware and driver. To see what version you have, see “Determining the Current Version of Your 3ware Driver” on page 170. To download the most recent software, see <http://www.lsi.com/channel/ChannelDownloads>.

Need to boot from a non-3ware device without changing the boot order

If the operating system is installed on a 3ware unit, you can temporarily bypass the 3ware BIOS and prevent the OS from booting from that unit by pressing Alt-b. This saves the step of changing the boot order in the motherboard BIOS and having to change it back again.

Software Installation Problems

The 3ware RAID controller was configured without problems, but the system does not boot

The problem could be one or more of the following:



Note: The 3ware BIOS Manager (3BM) tool is not available for Mac OS X users.

- The BIOS may have changed the order of the boot devices. Check your system BIOS boot sequence.
- The 3ware BIOS will only boot from the first unit listed in 3BM. You can change the unit from which the 3ware controller boots by moving it to the top of the list of units by highlighting the unit and pressing the 'Page Up'/'Page Down' keys.
- The operating system is installed on a device that is not in your system's boot order. Use your system's Setup utility to include the StorSwitch controller in the boot order.
- If your operating system was installed before you configured your RAID units, you may have overwritten your operating system. Remember that creating or deleting a RAID unit overwrites any existing data on the member drives. Reinstall your operating system.
- There may be a compatibility problem between the motherboard system BIOS and the 3ware BIOS. Check the LSI website to see if your motherboard is compatible with the 3ware BIOS, and check with your motherboard manufacturer for potential BIOS updates. Interoperability information is available at http://www.lsi.com/channel/support/marketing_resources/index.html.

A unit shows up as unusable, because of missing drives:

Unusable Arrays:

```
3 drive 64K RAID 5 558.77 GB (Unit 1)
SATA - Maxtor 6B300S0 279.86 GB (Port 6)
```

The unit has some but not all of its members available. The unit will be unusable. If this unit is your boot device, your system will not boot. You must either return the missing disks to complete the unit, or release the member disks by deleting the incomplete unit(s) listed in the display. Remember that deleting a RAID unit overwrites any existing data on the member drives.

CAUTION: Do not delete the inoperable unit and recreate it, as this will overwrite the data and make data recovery very difficult.

If you get this error, contact technical support at <http://www.lsi.com/channel/ContactUs>.

Problems in 3DM2 and 3BM

A 3ware RAID controller does not show in the list of controllers

You may not have the most recent driver for your controller, the driver may not be loaded, or you may not have the most recent version of the CLI or 3DM2.

To find out the driver version currently installed, see “Determining the Current Version of Your 3ware Driver” on page 170

Current drivers and software are available for download on the LSI website at <http://www.lsi.com/channel/ChannelDownloads>.

When booting a system, a drive is not showing up in the startup screens, in 3BM, or in 3DM2

This could be due to one or more of the following:

- Defective cable
- Defective drive
- Defective enclosure or drive slot
- Poorly seated drive
- Poorly connected power cable
- Poorly connected data cable
- Defective connector on the 3ware controller

If a drive that previously showed up in 3DM2 or 3BM does not show up, try the following:

- 1 Power the system down, then reseal the drive in the slot, reseal the data cable, and reseal the power cable.
- 2 Power the system back up.
- 3 If the drive still does not show up in 3DM2 or 3BM, then swap that drive with a drive that is showing up.
- 4 If the drive now shows up, and drive you swapped it with does not, then the drive is OK. The problem could be the controller connector, the cable, the power connector, or the enclosure or drive slot.
- 5 Change each of these things, one at a time
 - Try a different connector on the controller
 - Try a different data cable
 - Power the drive with a different power connector from the power supply
 - Try connecting the drive directly to the motherboard, bypassing the enclosure or drive slot

If the drive shows up, then you will know which hardware component was defective.

If the drive still does not show up, contact 3ware Technical Support.

Error and Notification Messages

Error and notification messages are issued by the 3ware RAID controller when an error is detected or when an action is completed. These messages are sometimes referred to as AENs (asynchronous event notifications).

AEN messages are displayed on the 3DM2 Alarms page and CLI Show Alarms page.

On the 3DM2 Alarms page, you can click on the message to jump to help text about that message. You can also look the message up in the list below. In 3DM2, the message number is the last few digits within the parentheses at the beginning of the message description. For example, in the string (0x04:0x002B), “002B” is the message number. To find additional information about the message 2B, you would look up 002B in the list below.

Note that the messages are listed below in hex order, since the message numbers are in hex.

Error and notification messages are listed in Table 14. Descriptions of each are provided after the table.

Sev	Time	Message
	Mon, Jan 19, 2004 01:12:54AM	(0x04:0x002B): Background verify done: unit=0
	Sun, Jan 18, 2004 11:57:02PM	(0x04:0x0029): Background verify started: unit=0
	Sun, Jan 18, 2004 01:16:35AM	(0x04:0x002B): Background verify done: unit=0
	Sun, Jan 18, 2004 12:00:48AM	(0x04:0x0029): Background verify started: unit=0

Table 14: Error and Notification Message List

Value	Message
0001	Controller reset occurred
0002	Degraded unit
0003	Controller error occurred
0004	Rebuild failed
0005	Rebuild completed
0006	Incomplete unit detected
0007	Initialize completed
0008	Unclean shutdown detected
0009	Drive timeout detected

Table 14: Error and Notification Message List

Value	Message
000A	Drive error detected
000B	Rebuild started
000C	Initialize started
000E	Initialize failed
000F	SMART threshold exceeded
0019	Drive removed
001A	Drive inserted
001E	Unit inoperable
001F	Unit Operational
0021	Downgrade UDMA mode
0022	Upgrade UDMA mode
0023	Sector repair completed
0024	Buffer integrity test failed
0025	Cache flush failed; some data lost
0026	Drive ECC error reported
0027	DCB checksum error detected
0028	DCB version unsupported
0029	Verify started
002A	Verify failed
002B	Verify completed
002C	Source drive ECC error overwritten
002D	Source drive error occurred
002E	Replacement drive capacity too small
002F	Verify not started; unit never initialized
0030	Drive not supported
0032	Spare capacity too small
0033	Migration started
0034	Migration failed
0035	Migration completed
0036	Verify fixed data/parity mismatch

Table 14: Error and Notification Message List

Value	Message
0037	SO-DIMM not compatible
0038	SO-DIMM not detected
0039	Buffer ECC error corrected
003A	Drive power on reset detected
003B	Rebuild paused
003C	Initialize paused
003D	Verify paused
003E	Migration paused
003F	Flash file system error detected
0040	Flash file system repaired
0041	Unit number assignments lost
0042	Primary DCB read error occurred
0043	Backup DCB read error detected
0044	Battery voltage is normal
0045	Battery voltage is low
0046	Battery voltage is high
0047	Battery voltage is too low
0048	Battery voltage is too high
0049	Battery temperature is normal
004A	Battery temperature is low
004B	Battery temperature is high
004C	Battery temperature is too low
004D	Battery temperature is too high
004E	Battery capacity test started
004F	Cache synchronization skipped
0050	Battery capacity test completed
0053	Battery capacity test is overdue
0055	Battery charging started
0056	Battery charging completed
0057	Battery charging fault

Table 14: Error and Notification Message List

Value Message
0058 Battery capacity is below warning level
0059 Battery capacity is below error level
005A Battery is present
005B Battery is not present
005C Battery is weak
005E Cache synchronization completed
005F Cache synchronization failed; some data lost
0062 Enclosure removed
0063 Enclosure added
0064 Local link up
0065 Local link down
0066 Reverted to emergency recovery firmware
0070 Drive write fault; some data lost
0081 RAID key not found
0080 All RAID keys failed validation
8000 Enclosure fan normal
8001 Enclosure fan error
8002 Enclosure fan removed
8003 Enclosure fan added
8004 Enclosure fan unknown
8005 Enclosure fan off
8020 Enclosure temp normal
8021 Enclosure temp low
8022 Enclosure temp high
8023 Enclosure temp below operating
8024 Enclosure temp above operating
8025 Enclosure temp removed
8026 Enclosure temp added
8027 Enclosure temp critical
8028 Enclosure temp unknown

Table 14: Error and Notification Message List

Value	Message
8030	Enclosure power normal
8031	Enclosure power fail
8032	Enclosure power removed
8033	Enclosure power added
8034	Enclosure power unknown
8037	Enclosure power off
8040	Enclosure voltage normal
8041	Enclosure voltage over
8042	Enclosure voltage under
8043	Enclosure voltage unknown
8044	Enclosure current normal
8045	Enclosure current over
8046	Enclosure current unknown
8047	Enclosure audio alarm activated but mute
8048	Enclosure audio alarm failed
8049	Enclosure audio alarm removed
804A	Enclosure audio alarm added
804B	Enclosure audio alarm status unknown

Error and Notification Message Details

0001 Controller reset occurred

Event Type

Information

Cause

The device driver has sent a soft reset to the 3ware RAID controller. The driver does this when the controller has not responded to a command within the allowed time limit (30 sec.). After the soft reset command has been sent, the driver will resend the command.

Action

If this message occurs more than three times a day, collect the system logs and contact Technical Support.

See Also

For how to collect the system logs, search the LSI KnowledgeBase for keyword 12278 at <http://kb.lsi.com>.

0002 Degraded unit

Event Type

Error

Cause

An error was encountered and the unit is now operating in degraded (non-redundant) mode. This is usually due to a drive failure or the physical removal of a drive from a redundant unit.

Action

Check hardware connections and reseal the drive or drives. Rescan the controller from 3DM2 or CLI to see if the unit has been restored. If you are able to restore the unit before any data has been written to the unit, a rebuild will not be necessary. If the unit remains degraded, replace the missing or dead drives and initiate a rebuild.

See Also

“About Degraded Units” on page 138

“Rebuilding Units” on page 154

0003 Controller error occurred**Event Type**

Error

Cause

The 3ware RAID controller has encountered an internal error.

Action

Please collect log files and contact LSI Customer Support, as a replacement board may be required. Technical support is reachable at <http://www.lsi.com/channel/ContactUs>. For information on collecting logs, search the LSI KnowledgeBase for keyword 12278 at <http://kb.lsi.com>.

0004 Rebuild failed**Event Type**

Error

Cause

The 3ware RAID controller was unable to complete a rebuild operation. This error can be caused by drive errors on either the source or the destination of the rebuild. However, because ATA drives can reallocate sectors on write errors, the rebuild failure is most likely caused by the source drive of the rebuild detecting a read error.

Action

The default operation of the 3ware RAID controller is to abort a rebuild if an error is encountered. If you want rebuilds to continue when there is a source error, you can set a unit policy to Continue on Source Error When Rebuilding in 3DM2 or CLI.

The consequence of continuing a rebuild when there is a source error is that there may be corrupt data in your rebuilt unit. In some cases, however, this may be your only alternative for recovering as much data as possible from a unit that has become degraded.

To lower the likelihood of getting this error, schedule regular verifications.

See Also

“Setting Overwrite ECC (Continue on Source Error When Rebuilding)” on page 108.

“Scheduling Background Tasks” on page 163

0005 Rebuild completed

Event Type

Information

Cause

The 3ware RAID controller has successfully completed a rebuild. The data is now redundant.

Action

None required.

0006 Incomplete unit detected

Event Type

Warning

Cause

The 3ware RAID controller has detected an incomplete unit.

An incomplete unit is a unit in which the 3ware RAID controller is unable to detect one or more drives. The drives may be missing, dead, or improperly connected. A unit that is incomplete is also degraded (although a degraded unit can be complete if all drives are still detected, including the failed drive).

Action

Check hardware connections and reseal the drives. Rescan the controller from 3DM2 to see if the unit has been restored. If you are able to restore the unit before any data has been written to the unit, a rebuild will not be necessary. If the unit remains incomplete, replace the missing or dead drives and initiate a rebuild.

0007 Initialize completed

Event Type

Information

Cause

The 3ware RAID controller completed the “synching” background initialization sequence of RAID levels 1, 6, 10, 50, or 5. For RAID 5, RAID 6, and RAID 50, the data on the unit was read and the resultant new parity was written. For RAID 1 and 10, one half of the mirror was copied to the other half (mirrors are synchronized).

This message will not appear for a foreground initialization.

See Also

“Foreground Versus Background Initialization” on page 146

0008 Unclean shutdown detected

Event Type

Warning

Cause

The 3ware RAID controller detected an unclean shutdown of the operating system, either from a power failure or improper shutdown procedure. The controller will force the unit to begin verifying, due to the possibility that data on a redundant unit could be out of synchronization.

Action

Allow the verification to complete. Verifications have little overhead in terms of system performance and keep your units in optimum condition.

To prevent unclean shutdowns, always go through the normal shutdown procedure. It is also recommended to use an uninterruptible power supply (UPS) to prevent unclean shutdowns due to sudden power loss.

See Also

“About Verification” on page 149

0009 Drive timeout detected

Event Type

Error

Cause

A drive has failed to respond to a command from a 3ware RAID controller within the allowed time limit (20 secs.). After sending this error message, the controller will attempt to recover the drive by sending a reset to that drive and retrying the failed command.

Possible causes of drive time-outs (also known as ATA-Port time-outs) include a bad or intermittent disk drive, power cable or interface cable.

Action

If you have checked hardware connections and no cause other than the drive can be found, replace the drive.

You may also want to use the drive manufacturer's diagnostic and repair utilities on the drive.

See Also

For links to drive manufacturer diagnostic utilities and troubleshooting advice, search the LSI KnowledgeBase for keyword 14924 at <http://kb.lsi.com>.

“Basic Troubleshooting: Check This First” on page 228

000A Drive error detected

Event Type

Error

Cause

A drive has returned an error to the 3ware RAID controller that it is unable to complete a command. The error type is not a time-out (000A) or uncorrected ECC (0026).

This message may be seen as part of a recovery operation initiated by the 3ware RAID controller on the drive. One possible cause is multiple write commands to a sector forcing the drive to remap a defective sector. This message may be seen if error recovery operations initiated by the 3ware RAID controller are unsuccessful.

Action

If you see this message, the drive repairs may lie outside of the 3ware RAID controller's abilities. Try running the drive manufacturer's diagnostic and repair utilities on the drive.

If necessary, replace the drive.

See Also

For links to drive manufacturer diagnostic utilities and troubleshooting advice, search the LSI KnowledgeBase for keyword 10894 at <http://kb.lsi.com..>

000B Rebuild started**Event Type**

Information

Cause

The 3ware RAID controller started to rebuild a degraded unit. The rebuild may have been initiated by you, may have started automatically on a hot spare or may have started after drive removal or insertion (due to the Auto-Rebuild policy).

Action

Allow the rebuild to complete. This will return the unit to its normal redundant state.

See Also

“Scheduling Background Tasks” on page 163

“Rebuilding Units” on page 154

“Background Task Prioritization” on page 163

000C Initialize started**Event Type**

Information

Cause

The 3ware RAID controller started an initialization. This is always a “synching” background initialization and does not erase user data. Initialization either occurs at unit creation time for larger RAID 5, 6, or 50 units or later during the initial verification of redundant units.

Action

Allow the initialization to complete. This will return the unit to its normal redundant state.

See Also

For more information, see “About Initialization” on page 146

000E Initialize failed

Event Type

Error

Cause

The 3ware RAID controller was unable to complete the initialization. This error can be caused by unrecoverable drive errors.

If this unit was a redundant unit, and the initialization failed because of a problem on a particular disk drive, then the unit will be degraded.

Action

If the unit was degraded, then rebuild the unit. This may necessitate replacing the drive.

Check physical cable and power connections. You can also run the drive manufacturer’s diagnostic and repair utilities on the drive.

See Also

For links to drive manufacturer diagnostic utilities and troubleshooting advice, search the LSI KnowledgeBase for keyword 10894 at <http://kb.lsi.com>.

“Basic Troubleshooting: Check This First” on page 228

000F SMART threshold exceeded

Event Type

Warning

Cause

SMART monitoring is predicting a potential drive failure.

The 3ware RAID controller supports SMART monitoring for SATA and SAS drives, whereby the individual drives automatically monitor certain parametric information such as error rates and retry counts. This type of monitoring may be able to predict a drive failure before it happens, allowing you to schedule service of the unit before it becomes degraded. The SMART status of each drive attached to the 3ware RAID controller is monitored daily.

Action

LSI recommends that you replace any drive that has exceeded the SMART threshold.

If the drive is part of a redundant unit, remove the drive through 3DM2 or CLI. Replace the drive and start a rebuild.

If the drive is not part of a redundant unit, then you will need to backup your data before replacing the drive.

See Also

“Viewing SMART Data About a Drive” on page 144

“Rebuilding Units” on page 154

0019 Drive removed**Event Type**

Warning

Cause

A drive was physically removed from the controller while the controller was powered on.

Action

If the drive is not part of a redundant unit, return the drive as soon as possible. You may need to rescan the controller to have the drive recognized. If at all possible, do not remove a drive from a non-redundant unit as this may cause data loss or a system hang.

001A Drive inserted**Event Type**

Information

Cause

A drive was connected to the controller while the controller was powered on.

Action

The drive is now available for use. If the drive is part of a unit add the remaining drives and rescan the controller, in 3DM2 or CLI, to bring the unit online.

001E Unit inoperable

Event Type

Error

Cause

The 3ware RAID controller is unable to detect sufficient drives for the unit to be operable. Some drives have failed or are missing.

Examples of inoperable units are as follows:

- RAID 0 missing any drives.
- A RAID 5 or 50 unit with two or more drives missing from the same RAID 5 unit or subunits.
- A RAID 10 unit with both drives missing from one of the RAID 1 subunits.
- A RAID 6 unit with three or more drives missing.

Note: The controller only generates this message if the unit is missing drives for more than 20 seconds. This allows a hot swap of a drive to be completed without generating this error.

Action

The unit is no longer available for use. Return all missing drives to the unit. If the drives are physically present, check all data and power connections.

CAUTION: Do not delete the inoperable unit and recreate it as this will overwrite the data and make data recovery very difficult.

You may wish to contact technical support at <http://www.lsi.com/channel/ContactUs>.

See Also

“About Inoperable Units” on page 139

001F Unit Operational

Event Type

Information

Cause

Drive insertion caused a unit that was inoperable to become operational again. Any data that was on that unit will still be there. This message is only sent if the unit was inoperable for more than 20 seconds. That means that if the hot swap of a drive occurred within 20 seconds, messages are not generated.

Action

None Required. The unit is available for use.

0021 Downgrade UDMA mode

Event Type

Warning

Cause

The 3ware RAID controller has downgraded the UDMA transfer rate between the controller and the ATA disk drives. This message only applies to parallel ATA and certain legacy serial ATA drives.

Background Information

The 3ware RAID controller communicates to the ATA disk drives through the Ultra DMA (UDMA) protocol. This protocol ensures data integrity across the ATA cable by appending a Cyclical Redundancy Check (CRC) for all ATA data that is transferred. If the data becomes corrupted between the drive and the 3ware RAID controller (because of an intermittent or poor quality cable connection) the 3ware RAID controller detects this as a UDMA CRC or cable error. The 3ware RAID controller then retries the failed command three times at the current UDMA transfer rate. If the error persists, it lowers the UDMA transfer rate (for example, from UDMA 100 to UDMA 66) and retries another three times.

Action

Check for possible causes of UDMA CRC errors such as defective or poor quality interface cables or cable routing problems through electrically noisy environments (for instance, cables are too close to the power supply). Also check for cables which are not standard or exceed the ATA specification. A

list of cables for use with 3ware controllers is available at http://www.lsi.com/channel/products/raid_controllers/accessories/cables.

0022 Upgrade UDMA mode

Event Type

Warning

Cause

During a self-test, the controller found that a drive was not in the optimal UDMA mode and upgraded its UDMA transfer rate.

Action

None required. The drive and cable are working in optimal mode.

0023 Sector repair completed

Event Type

Warning

Cause

The 3ware RAID controller moved data from a bad sector on the drive to a new location.

Background Information

The 3ware RAID controller supports a feature called dynamic sector repair that allows the unit to recover from certain drive errors that would normally result in a degraded unit situation. For redundant units such as RAID 1, 5, 6, 10, and 50, the 3ware RAID controller essentially has two copies of your data available. If a read command to a sector on a disk drive results in an error, it reverts to the redundant copy in order to satisfy the host's request. At this point, the 3ware RAID controller has a good copy of the requested data in its cache memory. It will then use this data to force the failing drive to reallocate the bad sector, which essentially repairs the sector.

Action

Sector repairs are an indication of the presence of grown defects on a particular drive. While typical modern disk drives are designed to allow several hundred grown defects, special attention should be paid to any drive in a unit that begins to indicate sector repair messages. This may be an indication

of a drive that is beginning to fail. You may wish to replace the drive, especially if the number of sector repair errors exceeds 3 per month.

0024 Buffer integrity test failed

Event Type

Error.

Cause

The 3ware RAID controller performs diagnostics on its internal RAM devices as part of its data integrity features. Once a day, a non-destructive test is performed on the cache memory. Failure of the test indicates a failure of a hardware component on the 3ware RAID controller. This message is sent to notify you of the problem.

Action

You should replace the 3ware RAID controller.

If the controller is still under warranty, contact 3ware Technical Support for a replacement controller.

0025 Cache flush failed; some data lost

Event Type

Error

Cause

The 3ware RAID controller was not able to commit data to the drive(s) during a caching operation. This is due to a serious drive failure, possibly from a power outage.

Background Information

The 3ware RAID controller uses caching layer firmware to improve performance. For write commands this means that the controller acknowledges it has completed a write operation before the data is committed to disk. If the 3ware RAID controller cannot commit the data to the drive after it has acknowledged to the host, this message is posted.

Action

To troubleshoot the reasons for the failure, collect the logs for your system and contact 3ware technical support at <http://www.lsi.com/channel/ContactUs>. For information on collecting logs, search the LSI KnowledgeBase for keyword 12278 at <http://kb.lsi.com>.

0026 Drive ECC error reported

Event Type

Error

Cause

Drive ECC errors are an indication of grown defects on a particular drive. For redundant units, this typically means that dynamic sector repair has been invoked (see message “0023 Sector repair completed” on page 250). For non-redundant units (Single Disk, RAID 0 and degraded units), which do not have another copy of the data, drive ECC errors result in the 3ware RAID controller returning failed status to the associated host command.

Action

Schedule periodic verifications of all units so that drive ECC errors can be found and corrected. If the unit is non-redundant a unit file system check is recommended.

Under Windows, right-click on your drive icon and choose **Properties >> Tools >> Check Now**.

For Mac OS X, you can use the First Aid tab in the Disk Utility—select the disk on the left and then click Verify Disk. If verification encounters problems, you can then use the Repair Disk option on the same screen.

Under Linux and FreeBSD use the fsck command.

For OpenSolaris and VMware you should follow your operating system’s guide to perform a file system check.

See Also

“Enabling or Disabling Auto-Verify for a Unit” on page 107

“Scheduling Background Tasks” on page 163

0027 DCB checksum error detected

Event Type

Error

Cause

The drive's Drive Configuration Block (DCB) has been corrupted.

The 3ware RAID controller stores certain configuration parameters on a reserved area of each disk drive called the Drive Configuration Block. As part of power-on initialization, the 3ware RAID controller performs a checksum of the DCB area to ensure consistency.

Action

If this error occurs, please contact 3ware technical support at <http://www.lsi.com/channel/ContactUs> for assistance.

0028 DCB version unsupported

Event Type

Error

Cause

The unit that is connected to your 3ware RAID controller was created on a legacy 3ware product that is incompatible with your new controller.

During the evolution of the 3ware product line, the format of the Drive Configuration Block (DCB) has been changed to accommodate new features. The DCB format expected by the 3ware RAID controller and the DCB that is written on the drive must be compatible. If they are not, this message is sent.

Action

Return the drives back to their original controller and contact 3ware technical support at <http://www.lsi.com/channel/ContactUs> for further assistance.

0029 Verify started

Event Type

Information

Cause

The 3ware RAID controller has started verifying the data integrity of a unit. The verification functions for different RAID levels are as follows:

- **Single.** Verify = Media scan
- **RAID 0.** Verify = Media scan
- **RAID 1 and 10.** Verify = Comparison of mirror sides
- **RAID 5, 6, and 50.** Verify = Comparison of parity data with user data

Action

Allow verify to complete to identify any possible data integrity issues.

See Also

For information on scheduling a verify process, see “Scheduling Background Tasks” on page 163. For information on verification of a unit, see “About Verification” on page 149.

002A Verify failed

Event Type

Error

Cause

Verification of a unit has terminated with an error. For each RAID level being verified, this may mean:

- **Single.** A single drive returned an error, possibly because of a media defect.
- **RAID 0.** A single drive returned an error, possibly because of a media defect.
- **RAID 1 and 10.** One side of the mirror does not equal the other side.
- **RAID 5, 6, and 50.** The parity data does not equal the user data.

For any RAID type, the most likely cause of the error is a grown defect in the drive. For out-of-synchronization mirrors or parity, the error could be caused by improper shutdown of the unit. This possibility applies to RAID 1, 5, 6, 10, and 50.

Action

When a verify fails, redundant units will automatically resynchronize user data through a background initialization. The initialize will not erase user data, but will recalculate and rewrite user parity data.

If the unit was non-redundant, any data in the error location is lost. (However, the error could be in a part of the drive that did not contain data.) A unit file system check is recommended.

Under Windows, right-click on your drive icon and choose **Properties >> Tools >> Check Now**.

For Mac OS X, you can use the First Aid tab in the Disk Utility—select the disk on the left and then click Verify Disk. If verification encounters problems, you can then use the Repair Disk option on the same screen.

Under Linux and FreeBSD use the fsck command.

For OpenSolaris and VMware you should follow your operating system's guide to perform a file system check.

The resynchronization of data that takes place during a background initialization can slow down access to the unit. Once initialization has begun, it cannot be canceled. You can pause it, however, by scheduling it to take place during off-hours. For more information, see “Scheduling Background Tasks” on page 163. You can also set the initialization process to go slower and use fewer system resources. For more information, see “Setting Background Task Rate” on page 162. (Initialization occurs at the Rebuild rate.)

See Also

“About Initialization” on page 146

002B Verify completed**Event Type**

Information

Cause

Verification of the data integrity of a unit was completed successfully.

See Also

“About Verification” on page 149

002C Source drive ECC error overwritten

Event Type

Error

Cause

A read error was encountered during a rebuild and the controller is configured to 'ignore ECC' or to 'Force continue on source errors'. The sector in error was reallocated. This will cause uncorrectable blocks to be rewritten, but the data may be incorrect.

Action

It is recommended that you execute a file system check when the rebuild completes.

Under Windows, right-click on your drive icon and choose **Properties >> Tools >> Check Now**.

For Mac OS X, you can use the First Aid tab in the Disk Utility—select the disk on the left and then click Verify Disk. If verification encounters problems, you can then use the Repair Disk option on the same screen.

Under Linux and FreeBSD use the fsck command.

For OpenSolaris and VMware you should follow your operating system's guide to perform a file system check.

002D Source drive error occurred

Event Type

Error

Cause

An error on the source drive was detected during a rebuild operation. The rebuild has stopped as a result.

Action

The controller will report an error, even if the area of the source drive that had the error did not contain data. Scheduling regular verifies will lessen the chance of getting this error.

You can force the rebuild to continue by setting the Overwrite ECC Error policy through 3DM2, 3BM, or CLI, and then rebuilding the unit again. This will cause uncorrectable blocks to be rewritten, but the data may be incorrect.

It is recommended that you execute a file system check when the rebuild completes.

Under Windows, right-click on your drive icon and choose **Properties >> Tools >> Check Now**.

For Mac OS X, you can use the First Aid tab in the Disk Utility—select the disk on the left and then click Verify Disk. If verification encounters problems, you can then use the Repair Disk option on the same screen.

Under Linux and FreeBSD use the fsck command.

For OpenSolaris and VMware you should follow your operating system's guide to perform a file system check.

See Also

“Starting a Verify Manually” on page 152

“Enabling or Disabling Auto-Verify for a Unit” on page 107

“Setting Overwrite ECC (Continue on Source Error When Rebuilding)” on page 108

002E Replacement drive capacity too small

Event Type

Error

Cause

The storage capacity of the drive you are using as a replacement drive is too small and cannot be used.

Action

Use a replacement drive equal to or larger than the drives already in use

002F Verify not started; unit never initialized

Event Type

Warning

Cause

A verify operation has been attempted by the 3ware RAID controller, but the unit has never been initialized before. The unit will automatically transition to initializing mode and then start a verify.

Action

None required.

This is considered a normal part of operation. Not all types of RAID units need to be initialized in order to have full performance. The initialize will not erase user data, but will calculate and write parity data or mirror data to the drives in the unit.

See Also

“About Initialization” on page 146

0030 Drive not supported

Event Type

Error

Cause

3ware 8000 and 9500S Serial ATA controllers only support UltraDMA-100/133 drives when using the parallel-to-serial ATA converter. This message indicates that an unsupported drive was detected during rollcall or a hot swap. This message could also indicate that the parallel-to-serial converter was jumpered incorrectly.

Action

Use a parallel ATA drive which supports UDMA 100 or 133 and check that the parallel-to-serial converter was correctly jumpered to correspond to UDMA 100 or 133 drives.

See Also

For a list of compatible drives, see the Interoperability list on http://www.lsi.com/channel/support/marketing_resources, -Select *Data & Interoperability* tab.

0032 Spare capacity too small

Event Type

Warning

Cause

There is a valid hot spare but the capacity is not sufficient to use it for a drive replacement in existing units.

Action

Replace the spare with a drive of equal or larger capacity than the existing drives.

0033 Migration started

Event Type

Information

Cause

The 3ware RAID controller has started the migration of a unit.

Migration changes can include:

- Expanding capacity of a unit by adding drives
- Changing RAID levels, for example, from RAID 1 to RAID 5

See Also

“RAID Level Migration (RLM) Overview” on page 116

0034 Migration failed

Event Type

Error

Cause

The migration of a unit has failed.

Migration changes can include:

- Expanding capacity of a unit by adding drives.
- Changing RAID levels, for example, from RAID 1 to RAID 5

Action

Review the list of events on the Alarms page for other entries that may give you an idea of why the migration failed (for example, a drive error on a specific port).

You may also wish to get the logs and contact technical support at <http://www.lsi.com/channel/ContactUs>. For information on collecting logs, search the LSI KnowledgeBase for keyword 12278 at <http://kb.lsi.com>.

See Also

“RAID Level Migration (RLM) Overview” on page 116

0035 Migration completed

Event Type

Information

Cause

The migrated unit is now ready to be used.

Migration changes can include:

- Expanding capacity of a unit by adding drives
- Changing RAID levels, for example, from RAID 1 to RAID 5.

Action

If the capacity of the unit did not change, then you do not need to do anything else. If the capacity of the migrated unit is larger, you will need to inform the operating system of the change. See “Informing the Operating System of Changed Configuration” on page 119.

0036 Verify fixed data/parity mismatch

Event Type

Warning

Cause

A verify error was found and fixed by the 3ware RAID controller.

Some examples of errors that can be fixed include:

- A parity inconsistency for a RAID 5 or RAID 50 unit.
- A data mismatch for a RAID 1 or RAID 10 unit.

Action

None required.

0037 SO-DIMM not compatible**Event Type**

Error

Cause

There is incompatible SO-DIMM memory connected to the 9500S controller.

Note: This message only applies to the 3ware 9500S controller, which has removable memory. Other 3ware controller models do not have memory that can be removed.

Action

Replace the incompatible SO-DIMM with a compatible one.

See Also

For a list of SODIMMs compatible with the 9500S, search the LSI KnowledgeBase for keyword 11748 at <http://kb.lsi.com>.

0038 SO-DIMM not detected**Event Type**

Error

Cause

The 3ware 9500S RAID controller is inoperable due to missing SO-DIMM memory.

Note: This message only applies to the 3ware 9500S controller, which has removable memory. Other 3ware controller models do not have memory that can be removed.

Action

Install a compatible SO-DIMM on the controller.

See Also

For a list of SODIMMs compatible with the 9500S, search the LSI KnowledgeBase for keyword 11748 at <http://kb.lsi.com>.

0039 Buffer ECC error corrected

Event Type

Warning

Cause

The controller has detected and corrected a memory ECC error.

Action

None required.

If errors persist, contact technical support at <http://www.lsi.com/channel/ContactUs>.

003A Drive power on reset detected

Event Type

Error

Cause

The controller has detected that a drive has lost power and then restarted. The controller may degrade the unit if it is a redundant unit (non-redundant units cannot be degraded).

Action

If this drive was the only one to lose power, check the cable connections. Also, check that your power supply is adequate for the type and number of devices attached to it.

See Also

For troubleshooting information and a link to drive manufacturer diagnostic utilities, search the LSI KnowledgeBase for keyword 14927 at <http://kb.lsi.com>.

003B Rebuild paused

Event Type

Information

Cause

The rebuild operation is paused.

Rebuilds are normally paused for two (formerly ten) minutes after a system first boots up and during non-scheduled times when scheduling is enabled.

Disabling or modifying the schedule with 3DM2 or CLI will allow the rebuild to resume.

See Also

“Scheduling Background Tasks” on page 163

003C Initialize paused

Event Type

Information

Cause

The initialization is paused.

Initializations are normally paused for two (formerly ten) minutes after a system first boots up. Initialization is also paused during non-scheduled times when scheduling is enabled. Initializations follow the rebuild schedule.

Action

If you want the initialize to resume, you can disable or modify the schedule through 3DM2 or CLI.

See Also

“Viewing Current Task Schedules” on page 165

“About Initialization” on page 146

003D Verify paused

Event Type

Information

Cause

The verify operation is paused.

Verifies are normally paused for 2 (formerly 10) minutes after a system first boots up. Verifies are also paused during non-scheduled times when scheduling is enabled.

Action

If you want the verification to resume, you can disable or modify the schedule through 3DM2 or CLI

See Also

“About Verification” on page 149

“Scheduling Background Tasks” on page 163

003E Migration paused

Event Type

Information

Cause

Migration is paused. Migration follows the rebuild schedule.

Action

If you want the migration to resume, you can disable or modify the schedule through 3DM2 or CLI

See Also

“RAID Level Migration (RLM) Overview” on page 116

“Scheduling Background Tasks” on page 163

003F Flash file system error detected

Event Type

Warning

Cause

A corrupted flash file system was found on the 3ware RAID controller during boot-up.

The 3ware RAID controller stores configuration parameters as files in its flash memory. These files can be corrupted when a flash operation is interrupted by events such as a power failure. The controller will attempt to restore the flash files from a backup copy.

Action

Update to the latest firmware, as earlier firmware resets corrupted files to default settings.

We recommend using 3DM2, 3BM, or CLI to check your settings, in case they were not able to be restored.

0040 Flash file system repaired

Event Type

Information

Cause

A corrupted flash file system has been successfully repaired.

Some of the flash files with insufficient data may have been lost in the operation. The configuration parameters which are lost will then return to their default values.

Action

We recommend using 3DM2, 3BM, or CLI to check your settings, in case they were not able to be restored.

0041 Unit number assignments lost

Event Type

Warning

Cause

The unit number assignments have been lost.
This may have occurred as a result of a soft reset.

Action

Please contact LSI 3ware technical support at
<http://www.lsi.com/channel/ContactUs>

0042 Primary DCB read error occurred

Event Type

Warning

Cause

The controller found an error while reading the primary copy of the Disk Configuration Block (DCB).

The controller will attempt to correct the error by reading the back-up copy of the DCB. If a valid DCB is found, the primary DCB is re-written to rectify the errors.

Action

LSI recommends verifying the unit. See “Starting a Verify Manually” on page 152.

0043 Backup DCB read error detected

Event Type

Warning

Cause

The controller has detected a latent error in the backup Disk Configuration Block (DCB).

The 3ware RAID controller checks the backup DCB, even when the primary DCB is OK. If an error is found, the controller will attempt to correct the error by reading the primary copy. If the primary copy is valid, the backup DCB will be rewritten to rectify the errors.

Action

LSI recommends verifying the unit. See “Starting a Verify Manually” on page 152.

0044 Battery voltage is normal**Event Type**

Information

Cause

The battery pack voltage being monitored by the Battery Backup Unit fell outside of the acceptable range and then came back within the acceptable range.

Action

None required

0045 Battery voltage is low**Event Type**

Warning

Cause

The battery pack voltage being monitored by the Battery Backup Unit has fallen below the warning threshold.

Action

The Battery Backup Unit is presently still able to backup the 3ware RAID controller, but you should replace the battery pack if the warning continues.

0046 Battery voltage is high

Event Type

Warning

Cause

The battery pack voltage being monitored by the Battery Backup Unit has risen above the warning threshold.

Action

The Battery Backup Unit is presently still able to backup the 3ware RAID controller, but you should replace the battery pack if the warning continues.

0047 Battery voltage is too low

Event Type

Error

Cause

The battery pack voltage being monitored by the Battery Backup Unit is too low to backup the 3ware RAID controller.

You may see this message during a battery capacity test. In this case, it is not a sign of battery failure.

You may also see this message if the battery pack is plugged in while the computer is on. This is not advised.

Action

Replace the battery pack if none of the above causes apply and the warning continues.

0048 Battery voltage is too high

Event Type

Error

Cause

The battery pack voltage being monitored by the Battery Backup Unit is too high to backup the 3ware RAID controller.

Action

The battery pack must be replaced.

This may be a fault in the BBU control module. If you get this error, do the following:

- 1 Turn off the computer and remove the 3ware RAID controller.
- 2 Remove the BBU control module from the 3ware RAID controller and the battery module from the remote card.
- 3 Unplug the battery from the control module.
- 4 Return the BBU control module and battery module to 3ware.

For more details on removing the BBU, see the installation guide that came with your 3ware RAID controller.

0049 Battery temperature is normal**Event Type**

Information

Cause

The battery pack temperature being monitored by the Battery Backup Unit fell outside of the acceptable range and then came back within the acceptable range.

Action

None required

004A Battery temperature is low**Event Type**

Warning

Cause

The battery pack temperature being monitored by the Battery Backup Unit has fallen below the acceptable range. The most likely cause is ambient temperature.

Action

The Battery backup Unit is presently still able to backup the 3ware RAID controller, but you should replace the battery pack if the temperature warning persists and is not due to environmental reasons.

004B Battery temperature is high

Event Type

Error

Cause

The battery pack temperature being monitored by the Battery Backup Unit has risen above the acceptable range. However, the BBU is still able to backup the 3ware RAID controller.

Action

Check for sufficient airflow around the card. To increase airflow you can:

- Leave the PCI slots next to the controller empty
- Add fans to your computer case
- Move and bundle wiring that is blocking air circulation

The Battery Backup Unit is presently still able to backup the 3ware RAID controller, but you should replace the battery pack if the temperature warning persists.

Contact 3ware technical support at <http://www.lsi.com/channel/ContactUs> if this problem is not due to environmental reasons or improper case cooling.

004C Battery temperature is too low

Event Type

Error

Cause

The battery pack temperature being monitored by the Battery Backup Unit is too low.

The BBU is unable to backup the 3ware RAID controller.

Action

Contact 3ware technical support at <http://www.lsi.com/channel/ContactUs>.

The battery pack must be replaced if the problem persists and is not due to environmental reasons.

004D Battery temperature is too high

Event Type

Error

Cause

The battery pack temperature being monitored by the Battery Backup Unit is too high.

The BBU is unable to backup the 3ware RAID controller.

Action

Check for sufficient airflow around the card. To increase airflow you can:

- Leave the PCI slots next to the controller empty
- Add fans to your computer case
- Move and bundle wiring that is blocking air circulation

Contact 3ware technical support at <http://www.lsi.com/channel/ContactUs> if this problem is not due to environmental reasons or improper case cooling.

004E Battery capacity test started

Event Type

Information

Cause

A battery test was started through CLI or 3DM2.

Background Information

The test estimates how many hours the Battery Backup Unit will be able to back up the 3ware RAID controller in case of a power failure.

This test performs a full battery charge/discharge/re-charge cycle and may take up to 20 hours to complete. During this test the Battery Backup Unit cannot backup the 3ware RAID controller. In addition, all units have their write cache disabled until the test completes.

Action

None required.

See Also

See the Install Guide for your controller.

004F Cache synchronization skipped

Event Type

Warning

Cause

The cache synchronization that is normally performed when power is restored after a power failure was skipped and write data is still being backed up in the controller cache. This can occur if a unit was physically removed or became inoperable during the power outage.

Action

Return missing drive(s) to the controller so that the missing write data can be saved.

0050 Battery capacity test completed

Event Type

Information

Cause

The Battery Backup Unit has completed a battery capacity test.

The BBU is again able to backup the 3ware RAID controller and write cache has been re-enabled for all units. (During the test, backup and write cache were disabled).

0053 Battery capacity test is overdue

Event Type

Information

Cause

There has not been a battery capacity test run in the last 6 months, which is the maximum recommended interval. This message will be sent once every week until the test is run.

Action

LSI recommends running the test at least once every 6 months, if the measured battery capacity is longer than 120 hours. If the measured battery capacity is less than 120 hours the recommended test interval is 4 weeks.

0055 Battery charging started

Event Type

Information

Cause

The Battery Backup Unit has started a battery charge cycle.

Action

None required

0056 Battery charging completed

Event Type

Information

Cause

The Battery Backup Unit has completed a battery charge cycle.

0057 Battery charging fault

Event Type

Error

Cause

The Battery Backup Unit has detected a battery fault during a charge cycle. The Battery Backup Unit is not ready and is unable to backup the 3ware RAID controller.

Action

Replace the battery pack.

See Also

See the Install Guide for your controller

0058 Battery capacity is below warning level

Event Type

Information

Cause

The measured capacity of the battery is below the warning level. The Battery Backup Unit is presently still able to backup the 3ware RAID controller, but it is weakening.

Action

Replace the battery pack if the warnings persist.

See Also

See the Install Guide for your controller.

0059 Battery capacity is below error level

Event Type

Error

Cause

The measured capacity of the battery is below the error level. The Battery Backup Unit is not ready and is unable to backup the 3ware RAID controller.

Action

Replace the battery pack.

See Also

See the Install Guide for your controller.

005A Battery is present

Event Type

Information

Cause

A battery pack is connected to the 3ware RAID controller.

005B Battery is not present

Event Type

Error

Cause

The battery pack has been removed from the 3ware RAID controller.

Action

Reinstall the battery pack.

005C Battery is weak

Event Type

Warning

Cause

The Battery Backup Unit periodically evaluates the health of the battery and its ability to backup the 3ware RAID controller in case of a power failure. This message is posted when the result of the health test is below the warning threshold.

Action

Replace the battery pack if warnings persist.

005E Cache synchronization completed

Event Type

Information

Cause

The 3ware RAID controller performs cache synchronization when system power is restored following a power failure. This message is posted for each unit when the cache synchronization completes successfully.

You will also see this message if drive insertion causes a unit to become operational and retained write cache data was flushed.

005F Cache synchronization failed; some data lost

Event Type

Error

Cause

The 3ware RAID controller performs cache synchronization when system power is restored following a power failure. The cache synchronization was not successful for some reason.

0062 Enclosure removed

Event Type

Warning.

Cause

Applies to 9750 and 9690SA controllers.

An enclosure is no longer accessible to the RAID controller. The likely cause is that the enclosure has been powered down or that a cable has been unplugged.

0063 Enclosure added

Event Type

Information.

Cause

Applies to 9750 and 9690SA controllers.

An enclosure is now accessible to the RAID controller. The likely cause is that an enclosure connected to the controller has been powered up or that a cable has been plugged in.

0064 Local link up

Event Type

Information.

Cause

Applies to 9750 and 9690SA controllers.

A cable has been plugged in, restoring a link to a controller phy.

0065 Local link down

Event Type

Warning.

Cause

Applies to 9750 and 9690SA controllers.

A cable has been unplugged, removing a link to a controller phy.

0066 Reverted to emergency recovery firmware

Event Type

Information.

Cause

The main firmware image is corrupted because the firmware upgrade was interrupted by a power failure, or the firmware update was not able to successfully complete.

Action

Retry the firmware update; if not successful, call technical support.

0070 Drive write fault; some data lost

Event Type

Error.

Cause

A SAS or SATA drive reported this error asynchronously. Some data loss might have occurred if you are using StorSave Performance mode.

Action

Recommend replacing the drive that reported this error.

0080 All RAID keys failed validation

Event Type

Error.

Cause

A RAID key was detected but validation failed or the OEM code is not correct. Drive detection has been disabled.

Action

Call technical support.

0081 RAID key not found

Event Type

Error.

Cause

The RAID key could not be read from the controller. Drive detection has been disabled.

Action

Call technical support; the board will likely need to be replaced.

8000 Enclosure fan normal

Event Type

Information.

Cause

Applies to 9750 and 9690SA controllers.

The fan's performance or operation is now back within the acceptable range.

Action

None required.

8001 Enclosure fan error

Event Type

Error.

Cause

Applies to 9750 and 9690SA controllers.

The enclosure fan is not functioning normally and may be blocked or defective.

Action

Check that the fan or fans are not blocked. If a fan appears defective, replace it as soon as possible.

For information on replacing a fan, see your enclosure documentation or contact your enclosure manufacturer.

8002 Enclosure fan removed

Event Type

Warning.

Cause

Applies to 9750 and 9690SA controllers.

A fan has either been removed or has become unplugged.

Action

Replace or reseal fan and make sure it is operational. An insufficient number of operating fans may lead to overheating of the components in the enclosure.

8003 Enclosure fan added

Event Type

Information.

Cause

Applies to 9750 and 9690SA controllers.

A fan has been added to the enclosure or an existing fan has been plugged in.

Action

None required.

8004 Enclosure fan unknown

Event Type

Warning.

Cause

Applies to 9750 and 9690SA controllers.

The enclosure is unable to recognize the fan. The fan may not be seated correctly or may be malfunctioning.

Action

Reseat the fan.

If it is necessary to replace the fan, see your enclosure documentation or contact your enclosure manufacturer.

8005 Enclosure fan off

Event Type

Warning.

Cause

Applies to 9750 and 9690SA controllers.

An enclosure fan has been turned off. It is no longer cooling the enclosure.

Action

The enclosure normally controls the on/off function of the fan. If there is no over-heating problem, no action is necessary.

8020 Enclosure temp normal

Event Type

Information.

Cause

Applies to 9750 and 9690SA controllers.

The enclosure temperature is now back within the acceptable range.

Action

None required.

8021 Enclosure temp low

Event Type

Information.

Cause

Applies to 9750 and 9690SA controllers.

The enclosure temperature is lower than normal.

Action

In general, cooler operating temperatures are good for enclosure components.

However, if the temperature is very cold, condensation can occur and cause media errors and damage. Take steps to bring the operating environment back within the enclosure manufacturer's specifications.

Allow cold equipment to warm up gradually before powering on.

8022 Enclosure temp high

Event Type

Warning.

Cause

Applies to 9750 and 9690SA controllers.

The enclosure temperature is higher than normal.

Action

Take steps to lower the enclosure temperature, such as adding fans, clearing enclosure openings of blockages, and increased ventilation.

Make sure that the enclosure environment does not get any hotter. See your enclosure documentation or contact your enclosure manufacturer to ensure that you are adhering to proper operating conditions and environments.

8023 Enclosure temp below operating

Event Type

Information.

Cause

Applies to 9750 and 9690SA controllers.

The enclosure temperature is below the enclosure manufacturer's specified operating temperature.

Action

In general, cooler operating temperatures are good for enclosure components.

However, if the temperature is very cold, condensation can occur and cause media errors and damage. Take steps to bring the operating environment back within the enclosure manufacturer's specifications.

Allow cold equipment to warm up gradually before powering on.

8024 Enclosure temp above operating

Event Type

Error.

Cause

Applies to 9750 and 9690SA controllers.

The enclosure temperature is above the enclosure manufacturer's specified operating temperature.

Action

Make sure that the fans are operational. Check for blocked ventilation in the enclosure and the operating environment.

Continued operation of the enclosure at high temperatures may lead to data loss and operational failure.

8025 Enclosure temp removed

Event Type

Warning.

Cause

Applies to 9750 and 9690SA controllers.

The temperature sensor in the enclosure has been removed or has failed and the enclosure temperature is no longer being monitored.

Action

The temperature sensor should be replaced or repaired. This may require specialized skills. Contact your enclosure manufacturer for more information.

8026 Enclosure temp added

Event Type

Information.

Cause

Applies to 9750 and 9690SA controllers.

A temperature sensor has been added to the enclosure or an existing sensor has been plugged in. This error message can occur due to a poor connection.

Action

If due to a poor connection, the repair will require specialized skills. Contact your enclosure manufacturer for more information.

8027 Enclosure temp critical

Event Type

Error.

Cause

Applies to 9750 and 9690SA controllers.

The temperature in the enclosure is dangerously out of the recommended operating range.

Action

Take immediate steps to correct the temperature problem.

Take steps to lower the enclosure temperature, such as adding fans, clearing enclosure openings of blockages, and increased ventilation of the operating environment

Continued operation of the enclosure at high temperatures may lead to data loss and operational failure.

See your enclosure documentation or contact your enclosure manufacturer to make sure you are following proper operating procedures.

8028 Enclosure temp unknown

Event Type

Warning.

Cause

Applies to 9750 and 9690SA controllers.

The enclosure is reporting that it is unable to determine the temperature of the unit. This may be due to a failed or missing sensor.

Action

Check the operational status of the temperature sensor. If it has failed, replace it.

See your enclosure documentation or contact your enclosure manufacturer for more information.

8030 Enclosure power normal

Event Type

Information.

Cause

Applies to 9750 and 9690SA controllers.

The enclosure power supply is now back within the acceptable range.

Action

None required.

8031 Enclosure power fail

Event Type

Error.

Cause

Applies to 9750 and 9690SA controllers.

One of the enclosure power supplies is not working. Either a power supply has failed or a cord is unplugged.

Action

Reseat the power supply cord. Replace any failed power supply as soon as possible.

It is recommended to use an uninterruptible power supply (UPS) to protect against power failures.

8032 Enclosure power removed

Event Type

Warning.

Cause

Applies to 9750 and 9690SA controllers.

One of the enclosure power supplies has been removed from the enclosure or a power supply is unplugged.

Action

Return or reconnect the power supply as soon as possible.

It is recommended to use an uninterruptible power supply (UPS) to protect against power failures.

8033 Enclosure power added

Event Type

Information.

Cause

Applies to 9750 and 9690SA controllers.

A power supply has been added to the enclosure or an existing power supply has been plugged in.

Action

None required.

8034 Enclosure power unknown

Event Type

Warning.

Cause

Applies to 9750 and 9690SA controllers.

There is a power supply in the enclosure, but it is not of a known type.

Action

Check to be sure the power supply is operational by re-seating or replacing the failed power supply. See your enclosure documentation or contact your enclosure manufacturer for more information.

It is recommended to use an uninterruptible power supply (UPS) to protect against power failures.

8037 Enclosure power off

Event Type

Warning.

Cause

Applies to 9750 and 9690SA controllers.

An enclosure power supply has been turned off.

Action

If needed for power supply redundancy or to meet power requirements, turn the power supply back on.

It is recommended to use an uninterruptible power supply (UPS) to protect against power failures.

8040 Enclosure voltage normal

Event Type

Information.

Cause

Applies to 9750 and 9690SA controllers.

The enclosure power supply voltage is now back within the acceptable range.

Action

None required.

8041 Enclosure voltage over

Event Type

Error.

Cause

Applies to 9750 and 9690SA controllers.

The enclosure power supply voltage is higher than the normal range.

Action

This error is rare. If you see it you may need a UPS or voltage regulator to stay within the recommended voltage range.

8042 Enclosure voltage under

Event Type

Error.

Cause

Applies to 9750 and 9690SA controllers.

The enclosure power supply voltage is lower than the normal range. This can be due to a failing power supply or an unreliable power source.

Action

If due to a failing power supply, replace it as soon as possible.

It is recommended to use an uninterruptible power supply (UPS) to protect against power failures.

8043 Enclosure voltage unknown

Event Type

Warning.

Cause

Applies to 9750 and 9690SA controllers.

The enclosure is not reporting voltage data. This can be due to a failing power supply.

Action

If applicable, replace the failed power supply.

Contact your enclosure manufacturer for more information.

8044 Enclosure current normal

Event Type

Information.

Cause

Applies to 9750 and 9690SA controllers.

The enclosure power supply current is now back within the acceptable range.

Action

None required.

8045 Enclosure current over

Event Type

Error.

Cause

Applies to 9750 and 9690SA controllers.

The enclosure power supply amperage is higher than normal.

Action

Replace the failing power supply or remove any extra devices. This may be caused by too many hard drives, which have exceeded the enclosure power specifications. See your enclosure documentation or contact your enclosure manufacturer for more details.

Too much current cannot be corrected by a UPS, although it can provide some protection against a power surge.

8046 Enclosure current unknown

Event Type

Warning.

Cause

Applies to 9750 and 9690SA controllers.

The enclosure's amperage is unknown. A power supply may have failed.

Action

If applicable, replace the failed power supply.

See your enclosure documentation or contact your enclosure manufacturer for more details.

8047 Enclosure audio alarm activated but mute

Event Type

Error.

Cause

Applies to 9750, 9690SA, and 9650SE controllers.

The enclosure's audio alarm has been activated, but the audibility is mute.

Action

Check the events listing for other error conditions that may have triggered the alarm.

8048 Enclosure audio alarm failed

Event Type

Error.

Cause

Applies to 9750, 9690SA, and 9650SE controllers.

The enclosure's audio alarm has malfunctioned and is not operational.

Action

Refer to the documentation for your enclosure.

8049 Enclosure audio alarm removed

Event Type

Warning.

Cause

Applies to 9750, 9690SA, and 9650SE controllers.

The enclosure's audio alarm is no longer installed.

Action

None required.

804A Enclosure audio alarm added

Event Type

Information.

Cause

Applies to 9750, 9690SA, and 9650SE controllers.

An audio alarm is now available for the enclosure.

Action

None required.

804B Enclosure audio alarm status unknown

Event Type

Warning.

Cause

Applies to 9750, 9690SA, and 9650SE controllers.

The status of the enclosure's audio alarm is not known.

Action

Refer to the documentation for the enclosure.

Appendices

The following information is available in the appendices:

- Appendix A, “Glossary” on page 294
- Appendix B, “Driver and Software Installation” on page 301
- Appendix C, “Compliance and Conformity Statements” on page 355
- Appendix D, “Warranty, Technical Support, and Service” on page 357

A

Glossary

- **3BM.** 3ware BIOS Manager, used on PC machines. The 3ware BIOS (Basic Input Output System) manager is a basic interface used to view, maintain, and manage 3ware controllers, disks, and units, without having to boot the operating system. 3BM is included with the controller and is updated when the controller firmware is upgraded. The latest firmware and code set is available for download from the 3ware web site: <http://www.lsi.com/channel/ChannelDownloads>
- **3DM2.** 3ware Disk Manager. The 3ware disk manager is a web-based graphical user interface that can be used to view, maintain, and manage 3ware controllers, disks, and units. It is available on the 3ware CD that came with your controller and can be downloaded from <http://www.lsi.com/channel/ChannelDownloads>.
- **3ware.** Named after the 3 computer wares: hardware, software and firmware. A leading brand of high-performance, high-capacity Serial ATA (SATA) and SAS (Serial Attached SCSI) RAID storage solutions.
- **A-Chip.** AccelerATA chip. Automated data ports to handle asynchronous SATA or SAS disk drive interface.
- **Array.** One or more disk drives that appear to the operating system as a single unit. Within 3ware software (3BM and 3DM2), arrays are typically referred to as units.
- **Array Roaming.** The process of swapping out or adding in a configured unit without having to shut down the system. This is useful if you need to move the unit to another controller.
- **Auto-Verify.** A unit policy that automates the verify process. When enabled, it performs verifies based on the Verify Schedule. It has two modes, Advanced, which has up to seven scheduling slots per week, or Basic, which has one.
- **Background rebuild rate.** The rate at which a particular controller initializes, rebuilds, and verifies redundant units (RAID 1, RAID 5, RAID 6, RAID 10, RAID 50).
- **Boot volume size.** The size to be assigned to volume 0 when creating a unit through 3BM or CLI on a PC machine. Note that the resulting volume does not have to be used as a boot volume. However, if the operating system is installed on the unit, it is installed in volume 0.

-
- **Cache.** See Read Cache and Write Cache.
 - **Carve size.** The size over which a unit will be divided into volumes, if auto-carving is enabled.
 - **CLI.** Command Line Interface. The 3ware CLI is a text program, rather than a GUI (graphical user interface). It has the same functionality as 3DM2, and can be used to view, maintain, and manage 3ware controllers, disks, and units.
 - **Configuration.** The RAID level set for a unit.
 - **Controller.** The physical card from 3ware that you insert into a computer system and connect to your disk drives or enclosure. The controller contains firmware that provides RAID functionality. 3ware makes a number of different models of SATA RAID controllers.
 - **Controller ID number.** Unique number assigned to every 3ware controller in a system, starting with zero.
 - **Create an array.** The process of selecting individual disk drives and selecting a RAID level. The array will appear to the operating system as a single unit. Overwrites any existing unit configuration data on the drives. Note that in 3ware software tools, arrays are referred to as units.
 - **DCB.** Disk configuration block. This is 3ware proprietary RAID table information that is written to disk drives that are in a RAID unit or single disk. The DCB includes information on the unit type, unit members, RAID level, and other important RAID information.
 - **Delete an array.** Deleting an array (or unit) is the process of returning the drives in a unit to individual drives. This erases the DCB information from the drives and deletes any data that was on them. When a unit is deleted from a controller, it is sometimes referred to as being “destroyed.” If you want to remove a unit without deleting the data on it, do not delete it; instead use the Remove feature in 3DM2, and then physically remove the drives.
 - **Destroying.** Same as deleting a unit.
 - **Degraded unit.** A redundant unit that contains a drive that has failed.
 - **Disk roaming.** When moving a unit from one controller to another, refers to putting disks back in a different order than they initially occupied, without harm to the data.
 - **Distributed parity.** Parity (error correction code) data is distributed across several drives in RAID 5, RAID 6, and RAID 50 configurations. Distributing parity data across drives provides both protection of data and good performance.
 - **Drive ID.** A unique identifier for a specific drive in a system. Also called a port ID.

- **Drive Number.** The SCSI number, or channel number, of a particular drive.
- **ECC.** Error correction code. ECC Errors are grown defects that have occurred on a drive since it was last read.
- **ECC Error policy.** Determines whether an error detected during a rebuild stops the rebuild or whether the rebuild can continue in spite of the error. Specified by the **Ignore ECC (Continue on Source Error When Rebuilding)** unit policy.
- **Enclosure.** An enclosure houses drives and a backplane. The backplane may have an expander.
- **Expander.** Expanders are simple switches in enclosures that provide connectivity between the 3ware 9750 RAID controller and the other devices in the SAS domain. Expanders allow one phy to connect to multiple drives.
- **Export a unit.** To remove the association of a unit with a controller. Does not affect the data on the drives. Used for array roaming, when you want to swap out a unit without powering down the system, and move the unit to another controller. Compare to Delete, which erases all unit configuration information from the drive.
- **Exportable unit or drive.** In 3BM (BIOS), exportable units and drives are those that will be available to the operating system when you boot your computer.
- **Fault tolerant.** A RAID unit which provides the ability to recover from a failed drive, either because the data is duplicated (as when drives are mirrored) or because of error checking (as in a RAID 5 unit).
- **Firmware.** Computer programming instructions that are stored in a read-only memory on the controller rather than being implemented through software.
- **Grown defect.** Defects that arise on a disk from daily use.
- **Hot spare.** A drive that is available, online, and designated as a spare. When a drive fails in a redundant unit, causing the unit to become degraded, a hot spare can replace the failed drive automatically and the unit will be rebuilt.
- **Hot swapping.** The process of removing a disk drive from the system while the power is on. Hot swapping can be used to remove units with data on them, when they are installed in hot swap bays. Hot swapping can also be used to remove and replaced failed drives when a hot swap bay is used.
- **Import a unit.** Attach a set of disk drives with an existing configuration to a controller and make the controller aware of the unit. Does not affect the data on the drives.

-
- **Initialize.** For 3ware SATA RAID controllers, initialize means to put the redundant data on the drives of redundant units into a known state so that data can be recovered in the event of a disk drive failure. For RAID 1 and 10, initialization copies the data from the lower port to the higher port. For RAID 5, 6, and 50, initialization calculates the RAID 5 parity and writes it to disk (background initialization). This is sometimes referred to as *resynching*, and does not erase user data. **Note:** If foreground initialization is done before the operating system has loaded, zeroes are written to all of the drives in the unit. This process, done through the 3ware BIOS, does erase existing data.
 - **Logical Units.** This term is used in the 3ware CLI. It is usually shortened to “units.” These are block devices presented to the operating system. A logical unit can be a one-tier, two-tier, or three-tier arrangement. Single logical units are examples of one-tier units. RAID 1, RAID 5, and RAID 6 are examples of two-tier units and as such will have sub-units. RAID 10 and RAID 50 are examples of three-tier units and as such will have sub-sub-units.
 - **JBOD.** An unconfigured single drive. The acronym is derived from “just a bunch of disks.” Note that earlier versions of the 3ware RAID controller exported JBODs to the OS. This is no longer supported. Individual drives should be configured as Single Disks in order to be made available to the OS.
 - **Migration.** The process of changing the characteristics of a unit. The change can be to expand the capacity of the unit (OCE), change the stripe size of the unit, change the unit from redundant to non-redundant, change the unit from non-redundant to redundant, and to change the unit from one type of redundant unit to another type of redundant unit (for example RAID 1 to RAID 5).
 - **Mirrored disk array (unit).** A pair of drives on which the same data is written, so that each provides a backup for the other. If one drive fails, the data is preserved on the paired drive. Mirrored disk units include RAID 1 and RAID 10.
 - **NCQ (Native Command Queuing).** See “Queuing”
 - **Non-redundant units.** A disk array (unit) without fault tolerance (RAID 0 or single disk.).
 - **OCE (Online Capacity Expansion).** The process of increasing the size of an existing RAID unit without having to create a new unit. See also *migration*.
 - **Parity.** Information that the controller calculates using an exclusive OR (XOR) algorithm and writes to the disk drives in RAID 5, RAID 6, and RAID 50 units. This data can be used with the remaining user data to recover the lost data if a disk drive fails.
 - **PCB.** Printed circuit board.

- **P-Chip.** PCI interface chip that connects the PCI bus to the high-speed internal bus and routes all data between the two using a packet switched fabric. There is one P-chip per controller card.
- **Phy.** Phys are transceivers that transmit and receive the serial data stream that flows between the controller and the drives. 3ware 9750 controllers have multiple phys. These phys are associated with virtual ports (vports) by 3ware software to establish up to 127 potential connections with the SAS or SATA hard drives.
- **Phy Identifier.** The ID number (0-7) assigned to each of the 8 phys on the 9750 controller.
- **Port.** 3ware controller models have one or many ports (typically 4, 8, 12, 16, 24, or 28). Each port can be attached to a single disk drive. On a controller with a Multi-lane™ serial port connector, one connector supports four ports. On 9750 series controllers, connections are made with phys and vports (virtual ports). See “phy” and “VPort”.
- **Port ID.** A unique identifier for a specific port in a system. Also called a drive ID.
- **Queuing.** SATA drives can use Native Command Queuing (NCQ) to improve performance in applications that require a lot of random access to data, such as server-type applications. When NCQ is enabled, the commands are reordered on the drive itself.

NCQ must be supported by the drive. NCQ must be turned on in both the drive and the RAID controller. By default, the RAID unit’s queue policy is disabled when creating a unit.

- **RAID.** Redundant array of inexpensive disks, combined into a unit (array), to increase your storage system’s performance and provide fault tolerance (protection against data loss).
- **Rapid RAID Recovery.** The Rapid Raid Recovery feature increases the speed with which a redundant unit can be made redundant again when a rebuild is required. It can also increase the speed of verification or initialization that may occur in the event of an unclean shutdown.
- **Read Cache.** Read Cache stores data from media locally on the controller to improve read access times for applications. The 3ware Read Cache feature also includes an Intelligent Mode, which enables Intelligent Read Prefetch (IRP). IRP includes a typical read-ahead caching method which is used to proactively retrieve data from media and store it locally on the controller with the anticipation that it may be requested by the host.
- **Rebuild task schedule.** The specification for when rebuilding, may occur, including start time and duration.
- **Rebuild a unit.** To generate data on a new drive after it is put into service to replace a failed drive in a fault tolerant unit (for example, RAID 1, 10, 5, 6, or 50).

-
- **Redundancy.** Duplication of data on another drive or drives, so that it is protected in the event of a drive failure.
 - **Remove a drive.** The process of making a drive unavailable to the controller.
 - **Remove a unit.** The process of making a unit unavailable to the controller and the operating system. After a unit is removed it can be hot swapped out of the system. This is sometimes referred to as exporting a unit.
 - **RLM (RAID Level Migration).** The process of using an existing unit of one or more drives and converting it to a new RAID type without having to delete the original unit. For example, converting a single disk to a mirrored disk or converting a RAID 0 unit to a RAID 5 unit.
 - **Self-test.** A test that can be performed on a scheduled basis. Available self-tests include Check SMART Thresholds.
 - **Stagger time.** The delay between drive groups that will spin up, at one time, on a particular controller.
 - **SAS.** SAS (Serial Attached SCSI) is a serial communication protocol for storage devices. The SAS protocol includes support for SAS and SATA devices.
 - **SAS address.** Each SAS device (SAS drives, controllers, and expanders) has a worldwide unique 64-bit SAS address. Also known as World Wide Number (WWN). SATA drives do not have a WWN and are identified by a VPort ID.
 - **SAS device.** SAS devices include SAS drives, controllers, and any expanders present in the SAS domain. Each SAS device has a unique 64-bit World Wide Number (WWN). SATA drives do not have a WWN and are identified by their VPort IDs
 - **SAS domain.** The SAS domain includes all SAS and SATA devices that are connected to the 9750 controller, either directly or through expanders.
 - **SES (SCSI Enclosure Services).** The SES protocol allows the 9750 RAID controller to manage and report the state of the power supplies, cooling devices, displays, indicators, individual drives, and other non-SCSI elements installed in an enclosure.
 - **Stripe size.** The size of the data written to each disk drive in RAID unit levels that support striping. The size of stripes can be set for a given unit during configuration. The stripe size is user-configurable at 64 KB, 128 KB, or 256 KB.

This stripe size is sometimes referred as a “minor” stripe size. A major stripe size is equal to the minor stripe size times the number of disks in the unit.

- **Striping.** The process of breaking up files into smaller sizes and distributing the data amongst two or more drives. Since smaller amounts of data are written to multiple disk drives simultaneously, this results in an increase in performance. Striping occurs in RAID 0, 5, 6, 10 and 50.
- **Subunit.** A logical unit of storage that is part of another unit. For example, the mirrored pairs (RAID 1) in a RAID 10 unit are subunits of the RAID 10 unit.
- **Unit ID.** A unique identifier for a specific unit in a system.
- **Unit Number.** The SCSI number, or channel number, of a particular unit.
- **Unit.** A logical unit of storage, which the operating system treats as a single drive. A unit may consist of a single drive or several drives. Also known as an array.
- **Verify.** A process that confirms the validity of the redundant data in a redundant unit. For a RAID 1 and RAID 10 unit, a verify will compare the data of one mirror with the other. For RAID 5, RAID 6, and RAID 50, a verify will calculate RAID 5 parity and compare it to what is written on the disk drive.
- **VPort.** The 3ware 9750 RAID controller has 127 addresses available to assign to hard drives. These addresses are known as virtual port (vport) IDs. By using vport IDs and expanders, one controller phy can connect to multiple drives. This is in contrast to standard port connections which are one-to-one physical connections.
- **Wide Port.** A SAS port can consist of one or more phys. When a SAS port consists of one phy it is known as a narrow port, when it contains multiple phys it is known as a wide port. The 3ware 9750 controllers has multiple wide port connectors that contain 4 phys each. These phys can function individually, in which case each phy has its own SAS address, or the 4 phys can be banded together, in which case they share the same SAS address. A 9750 wideport can have a bandwidth of up to 12.0 Gbps for SAS 1.1 and 24 Gbps for SAS 2.0..
- **WWN (World Wide Number).** The unique worldwide 64-bit SAS address assigned by the manufacturer to each SAS port and expander device in the SAS domain. Many SAS drives have 2 ports and thus 2 WWNs.
- **Write Cache.** When write cache is enabled, data will be stored in controller cache and drive cache before the data is committed to disk. This allows the system to process multiple write commands at the same time, thus improving performance

Driver and Software Installation

This appendix provides detailed instructions for installing 3ware drivers and software to your 9750 series controller. Driver and software information is organized by operating system:

- Installing 3ware Drivers and Software under FreeBSD
- Installing 3ware Drivers and Software under Linux
- Installing 3ware Drivers and Software under Mac OS X
- Installing 3ware Drivers and Software under OpenSolaris
- Installing 3ware Drivers and Software under VMware
- Installing 3ware Drivers and Software under Windows

Installing 3ware Drivers and Software under FreeBSD

This section provides detailed instructions for installing the 3ware driver and the RAID management software running under an FreeBSD operating system.

The following topics are included in this section:

- Driver Installation for FreeBSD
- Updating Drivers under FreeBSD
- Installing Management Software (3DM2 and CLI)

Driver Installation for FreeBSD



Note: Before installing the 3ware driver, you must have already installed your 3ware RAID controller in the system. Consult the installation guide that came with your controller for how to do this. You can download the installation guide from: <http://www.lsi.com/channel/ChannelDownloads>.

This section provides details about how to install the driver for your 3ware RAID controller under FreeBSD.

- If the units you have created are your boot device, you install the driver for the controller as you install FreeBSD.
- If the operating system is already installed on a unit connected to another controller or to the motherboard, you start FreeBSD and then install the driver.

This section includes these topics:

- Obtaining 3ware FreeBSD Drivers
- Creating a FreeBSD Driver Diskette
- Installing the Kernel Driver Module while you Install the FreeBSD on a Unit Managed by a 3ware RAID Controller
- Installing the 3ware Kernel Driver on a FreeBSD System that Boots from a Different Device

After installing the driver, you can install the 3ware management tools 3DM2 and CLI. For details, see “Installing Management Software (3DM2 and CLI)” on page 308.

Obtaining 3ware FreeBSD Drivers

3ware drivers can be compiled from source files into the kernel as built-in drivers or can be modules that are loaded by the operating system. Both source files and modules are available from LSI 3ware, but modules with current controller drivers are only available for FreeBSD 7.2.

You can obtain the 3ware RAID controller driver for FreeBSD from one of these two sources:

- **3ware software CD-ROM**
This CD includes: Compiled and tested kernel driver modules for FreeBSD, located at:
 - **32-bit:** `packages/drivers/freebsd/<version>/x86`
 - **64-bit:** `packages/drivers/freebsd/<version>/x86_64`**Driver source files** for FreeBSD located at:
 - **FreeBSD:** `packages/drivers/freebsd/src/<version>`
- **LSI web site.** You can download the latest compiled and tested driver modules and driver source files for FreeBSD from the LSI web site at <http://www.lsi.com/channel/ChannelDownloads>.

Creating a FreeBSD Driver Diskette

You need a diskette drive if you are going to be installing FreeBSD on a unit or drive managed by a 3ware RAID controller card which becomes the boot unit for which your version of FreeBSD does not have a built-in driver.

To create a driver diskette

- 1 Insert a blank diskette and the 3ware software CD into a FreeBSD installed system.
- 2 Navigate to: `packages\drivers\freebsd\<version>`
- 3 Copy the appropriate driver to the diskette, i.e., driver from `x86` folder if you are installing a 32-bit FreeBSD, `x86_64` folder if you are installing 64-bit FreeBSD. You need the driver source from `packages\drivers\freebsd\src\<version>` if you are going to update the kernel with a new driver.

Installing the Kernel Driver Module while you Install the FreeBSD on a Unit Managed by a 3ware RAID Controller



Prerequisite:

You need a copy of:
FreeBSD 7.2 (x86 or amd64) OS Installation CD

Use this procedure if your boot unit is going to be managed by the 3ware RAID controller.

It describes how to load the FreeBSD 7.2 kernel driver module to enable boot device support and how to then compile the current drivers into the kernel from source files.



Note: This procedure is specific to FreeBSD 7.2 as it requires a compiled module. For versions of FreeBSD for which a compiled module is not supplied by 3ware it is necessary to compile your own module from source files. See "Compiling and Loading the Driver as a Module using `kldload`" on page 307.

- 1 Disconnect all SCSI, ATA, and SAS devices in the system, except the CD or DVD and hard drives connected to the 3ware RAID controller.
- 2 Create the RAID units on the 3ware RAID controller using 3BM. For details on how to create and order units, refer to "Creating a Unit through 3BM" and "Ordering Units in 3BM" on pages 97 and 101.
- 3 Insert the diskette containing `twsw.ko` module into the diskette drive.
- 4 At the FreeBSD boot menu, select 6 "Escape to loader prompt."

- 5 At the loader prompt.
- 6 Load `tws.ko` from the diskette drive using.
`load disk0:tws.ko` or `disk1:tws.ko` depending on how many drives you have connected to your system.
- 7 Continue with the installation by typing.
`boot`
- 8 Install the FreeBSD OS, remove the FreeBSD installation CD, and reboot again.

Installing the 3ware Kernel Driver on a FreeBSD System that Boots from a Different Device

Use the steps in this section if FreeBSD boots from a different device and you are using the unit on your 3ware RAID controller for secondary storage.

When you use the unit managed by the 3ware RAID controller for secondary storage, you do not need to use a driver diskette for driver installation.



Tip: Install FreeBSD on the drive attached to the motherboard before installing the 3ware RAID controller. This avoids the possibility of installing to the wrong drive or unit.

- 1 Get the latest driver source files for your version of FreeBSD. See “Obtaining 3ware FreeBSD Drivers” on page 302.
- 2 Make sure the 3ware RAID controller is not yet installed in the system.
- 3 Install FreeBSD on a disk attached to the motherboard.
Be sure to install the full FreeBSD source.
- 4 Once FreeBSD is installed, power down the system and install the 3ware RAID controller. For assistance, see the installation guide that came with the controller.
- 5 Boot to FreeBSD.
- 6 Follow the instructions in “Updating the Kernel with the New Driver Source” on page 305 to update the kernel.

Updating Drivers under FreeBSD

Drivers can be updated either from source files or with driver modules.

Using source files, you can compile drivers into the kernel or you can create modules for versions of FreeBSD for which LSI does not supply modules.

This section includes these topics:

- Updating the Kernel with the New Driver Source
- Updating the 3ware Kernel Driver Module Under FreeBSD
- Compiling and Loading the Driver as a Module using kldload

Updating the Kernel with the New Driver Source

Use this procedure if you wish to update your kernel from driver source files. To obtain source files, see “Obtaining 3ware FreeBSD Drivers” on page 302.

- 1 Unpack `twsw.tgz` then copy the `*.c` and `*.h` files to `/sys/dev/tws` and the Makefile to `/sys/modules/tws`.
- 2 Go to `/usr/src/sys/i386/conf` or `/usr/src/sys/amd64/conf` depending on whether you have a 32-bit or 64-bit version of FreeBSD.
 - a Open your current configuration file: (GENERIC, SMP, or PAE or custom config), with `vi` or other editor.

Make sure “Device `twsw` # 3ware 9750 series” is not commented out.

- b Save changes.
- c In `/usr/src/sys/conf/files` add the following entries between the entries for `twa` and `twe`:

```
dev/tws/tws.c          optional tws \
compile-with "${NORMAL_C} -I${S}/dev/tws"

dev/tws/tws_cam.c     optional tws \
compile-with "${NORMAL_C} -I${S}/dev/tws"

dev/tws/tws_hdm.c     optional tws \
compile-with "${NORMAL_C} -I${S}/dev/tws"

dev/tws/tws_services.c optional tws \
compile-with "${NORMAL_C} -I${S}/dev/tws"

dev/tws/tws_user.c    optional tws \
compile-with "${NORMAL_C} -I${S}/dev/tws"
```

- d In `/usr/src/sys/conf/kern.pre.mk`

Add the following after the entry for `tws`
`# . . .` and the same for `tws`
`INCLUDES+= -I${S}/dev/tws`
- e Run command `config <config_name>` specifying your configuration file: (GENERIC, SMP, PAE, or your custom config), followed by:

```
cd ../compile/<config_name>
make clean
make cleandepend
make depend
make
make install
```

3 Reboot your system.

When the system reboots, the new kernel driver module will load automatically.

Updating the 3ware Kernel Driver Module Under FreeBSD

The following steps describe how to update the 3ware driver with a kernel driver module under FreeBSD.



Make a backup of your original driver before updating in case you need to revert back to it. However, you will not be able to revert back to the original driver if you are booting from that unit.

- 1 Download and extract the driver, as described under “Downloading the Driver and Firmware” on page 178.
- 2 Make a backup of any critical data prior to updating the 3ware driver.
- 3 Change the directory to the location with the extracted driver.
Copy the driver into `/boot/kernel`.
Make sure the module version matches the FreeBSD version. If the versions don't match there could be a kernel panic.
- 4 Load the driver.

```
kldload tws.ko
```


If units are present, you should see unit information in the system log (usually, `/var/log/messages`).
- 5 If you wish to load the driver automatically every time the system is rebooted, add the line `' tws_load="YES"'` to the file `/boot/loader.conf`

Compiling and Loading the Driver as a Module using kldload

If you want to use a driver module and 3ware does not supply one for your version of FreeBSD, use the following procedure. If you just want to install a 3ware-supplied module, see Updating the 3ware Kernel Driver Module Under FreeBSD.



Note: You can only use kldload to load the driver as a module if your boot drive is attached to the mother board and is not managed by the 3ware RAID controller.

To compile the driver as a module

- 1 Boot to FreeBSD.
- 2 Download and extract the driver, as described under “Downloading the Driver and Firmware” on page 178.
- 3 Unpack `tws.tgz`.
Then copy the `*.c` and `*.h` files to
`/sys/dev/tws` and the `Makefile` to `/sys/modules/tws`
- 4 Build the `tws.ko` module
`cd /sys/modules/tws`
`make`

The `tws.ko` module is created in `/sys/modules/tws`.

To load the driver as a module

- 1 In the current configuration file under `/usr/src/sys/i386/conf` or `/usr/src/sys/amd64/conf` comment out the entry: "Device `tws # 3ware 9750 series`". This will unlink the old driver once you rebuild the kernel.
- 2 Rebuild the kernel.
Run command `config <config_name>` specifying your configuration file: (GENERIC, SMP, PAE, or your custom config), followed by:

```
cd ../compile/<config_name>
make clean
make cleandepend
make depend
make
make install
```

- 3 Reboot to FreeBSD.
- 4 Load the kernel driver module

```
cd /sys/modules/tws
kldload ./tws.ko
```
- 5 If you wish to load the driver automatically every time the system boots:
 - a copy `tws.ko` into the boot folder

```
cp /sys/modules/tws/tws.ko /boot/kernel/tws.ko
```

(backup the old module if you wish to revert back)
 - b add the line `'tws_load="YES"'` to the file `/boot/loader.conf`

Installing Management Software (3DM2 and CLI)

This section provides detailed instructions for installing and uninstalling 3ware's RAID management software using the command line installer.

- Installing 3ware Management Software
- Uninstalling 3ware Management Software

Installing 3ware Management Software

The following steps describe how to install software on FreeBSD at a command line, using a text-only interface. You must be root to run the installer.

- 1 Download the LSI 3ware FreeBSD installation image from LSI channel website at <http://www.lsi.com/channel/ChannelDownloads>.
- 2 Mount the image or burn the image to a CD.
- 3 Navigate to the folder on the mounted image or CD that contains the installer.

```
packages/installers/tools/freebsd
```
- 4 Type: `./install.sh -i`
- 5 Respond to each screen as the script walks you through the installation process.
- 6 After the installation is complete, check that the software was installed correctly.

Uninstalling 3ware Management Software

The following steps describe how to uninstall software on FreeBSD at a command line, using a text-only interface. You must be root to run the installer.

- 1 Navigate to the folder on your computer where 3DM2/CLI are installed.

`/opt/3ware/`

Backup files, if needed. All files will be removed during uninstall from:

`/opt/3ware`

This directory is only for use by the 3ware management software. No user data should be stored here.

- 2 Type: `./install.sh -u`
- 3 Respond to each screen as the script walks you through the uninstall process.
- 4 After the uninstall is complete, check that the software is uninstalled.

Installing 3ware Drivers and Software under Linux

This section provides detailed instructions for installing the 3ware driver and the RAID management software running under an Linux operating system.

The following topics are included in this section:

- Driver Installation Under Linux
- Obtaining 3ware Linux Drivers
- Driver Installation Under Red Hat or Fedora Core Linux
- Driver Installation Under SUSE Linux
- Compiling a 3ware Driver for Linux
- Updating the 3ware Driver Under Red Hat or Fedora Core
- Updating the 3ware Driver Under SUSE
- Installing Management Software (3DM2 and CLI)

Driver Installation Under Linux



Note: Before installing the 3ware driver, you may have already installed your 3ware RAID controller in the system. Consult the installation guide that came with your controller for how to do this. If you do not have a hardcopy of the installation manual, it is available in the “doc” folder on your 3ware CD, or you can download it from the LSI website at <http://www.lsi.com/channel/ChannelDownloads>.

A drive or unit managed by the 3ware RAID controller may be configured to be your system's boot device. Or, you can use units managed by the 3ware controller for secondary storage and boot from another device, such as a disk attached to the motherboard, or other bootable media.

The steps you follow to install the driver and make your RAID unit available depend on which version of Linux you are using, and whether it will be your boot device. This chapter provides step-by-step instructions for the following:

- Red Hat / Fedora Core Linux Installation
 - Installing the 3ware Kernel Driver Module while Installing Red Hat Linux on a New Unit
 - Installing the 3ware Kernel Driver Module on a Red Hat or Fedora Core Linux System that Boots From a Different Device
- SUSE Linux Installation
 - Installing the 3ware Kernel Driver Module while Installing SUSE Linux on a New Unit
 - Installing the 3ware Kernel Driver Module on a SUSE Linux System that Boots from a Different Device

The LSI website provides drivers for the latest Linux releases at <http://www.lsi.com/channel/ChannelDownloads>.

Refer to the release notes for more details.

If you are using an unsupported Linux distribution or kernel for which there is not a driver available from the LSI download page, search the LSI KnowledgeBase for keyword 14546 at <http://kb.lsi.com>. You can also contact LSI Technical Support, or email your driver request to support@lsi.com.

For information about how to compile a driver from the 3ware driver source, see the links appended to the KnowledgeBase article mentioned above.

Obtaining 3ware Linux Drivers

Obtain the 3ware driver for Linux from one of these two sources:

- **3ware CD.** Compiled and tested drivers for Red Hat, openSUSE, SUSE Linux Enterprise Server (SLES), and Fedora Core Linux are included on this CD. Also included are the 3ware driver sources to compile kernel-specific drivers for many other Linux distributions.
- **LSI web site.** You can download the latest compiled and tested driver for supported Linux distributions from the LSI web site at <http://www.lsi.com/channel/ChannelDownloads>. Also included are the 3ware driver sources to compile kernel specific drivers for many other Linux distributions.



Warning: Be sure to use the correct driver for your processor. It is possible to load the wrong driver onto a system, however when you boot such systems, they will not work.

LSI offers the following drivers for various Linux distributions:

- 32-bit for Intel x86 and AMD Athlon
- 64-bit for AMD Opteron and Intel Xeon (EM64T)

Determining the Current Version of your 3ware Driver

If you already have a 3ware controller installed, you can check the current driver version, using either 3DM2 or the CLI. (For details, see “Viewing Information About a Controller” on page 65.)

You can also check it using the following method:

If you have a 2.6 kernel with sysfs, type the following command:

```
cat /sys/class/scsi_host/<hostid>/3ware_stats
```

where <hostid> is usually host 0, unless other SCSI devices are available, in which case it may be host1 or higher.

If you have a 2.6 kernel without sysfs, type the following command:

```
dmesg | grep 3w
```

Driver Installation Under Red Hat or Fedora Core Linux

Materials required

- LSI 3ware CD
- Floppy diskette or USB drive, if you need to create a driver install disk.
- Fedora or Red Hat installation disk (Not required if Linux is already installed on another drive.)

Creating a Red Hat Linux Driver Disk

If you are installing Linux on the new drive or unit managed by the 3ware RAID controller, you must create a 3ware driver install disk on a diskette or a USB drive. If Linux is already installed on another device, you may install the 3ware kernel driver module from the 3ware CD.

To create a Red Hat Linux driver install floppy diskette

- 1 Insert the 3ware CD into your Linux system. A GUI such as X windows is required to load the 3ware menu.

To manually mount the CD, type:

```
mount -t iso9660 /dev/cdrom /mnt
```

To start autorun, type:

```
/mnt/autorun
```

When it starts, you will be asked to agree to the LSI software license. To continue, click **Agree**.

- 2 When the 3ware Menu appears, click the **Driver Disk Images** button.
- 3 In the 3ware Driver Disk Images menu, click the button for the driver disk you want to create.

A confirmation window opens.

- 4 Insert a blank diskette into a drive and click the **Yes** button to begin creating the driver floppy diskette.



Note: If you need to create a Linux driver diskette for a Linux distribution other than what is available on the menu, search the LSI KnowledgeBase for keyword 14546 at <http://kb.lsi.com>.

To copy the driver to a USB drive

- 1 Insert the 3ware CD into your system.
To manually mount the CD, type:

```
mount -t iso9660 /dev/cdrom /mnt
```
- 2 On the CD, navigate to packages/images and locate the appropriate driver.
- 3 Insert a USB drive into your computer.
- 4 Unzip (if .zip) or untar (if .tgz) the driver file to the USB drive.

Installing the 3ware Kernel Driver Module while Installing Red Hat Linux on a New Unit



Note: If Red Hat Linux is already installed and bootable on another drive, turn to “Installing the 3ware Kernel Driver Module on a Red Hat or Fedora Core Linux System that Boots From a Different Device” on page 314.



Note: We have tested some older systems where a drive connected to the motherboard interfered with using a drive or unit managed by the 3ware RAID controller as a boot device. Disconnecting the drive while installing Linux will eliminate this problem. After Linux is installed, the drive can be reconnected.

To install the 3ware kernel driver module while installing Red Hat or Fedora Core Linux on a new unit

- 1 Boot with the Red Hat or Fedora Core install disk:
 - a Insert the Linux installation disk into your computer.
 - b Make sure the boot order in your motherboard’s BIOS is correct; then start or reboot your computer.
 - c When the Welcome to Red Hat or Fedora Core display appears, type:

```
linux dd
```


A number of files will load and then a message will prompt you to insert your driver install disk.
- 2 Install the 3ware kernel driver module, using the driver install diskette:
Insert the driver install diskette containing the 3ware driver and press **Enter**.
The system automatically reports: `Loading 3w-sas`

- 3 When prompted, select the proper language and keyboard types for your locality.
- 4 After installation completes, remove media (CD and floppy disks).
- 5 Click reboot button to finish installation.

Installing the 3ware Kernel Driver Module on a Red Hat or Fedora Core Linux System that Boots From a Different Device

The steps for installing the 3ware kernel driver module vary slightly, depending on your specific installation requirements. Select the appropriate set of steps below, based on whether:

- You want to update the RAM disk
- You prefer to load the driver manually or from a script, instead of updating the RAM disk

About Variables In the Kernel Driver Module Installation Instructions

These conventions are used for variable text for kernel strings and module names in the instructions on the following pages.

Kernel String Conventions

<kernel string> refers to the kernel version.

The kernel string will have different endings, depending on the kernel you are using.

- For a default kernel, the kernel string will end in `default`. For example:
`2.6.16-default`
- For an SMP kernel (multi-processor), the kernel string will end in `smp`.
For example: `2.6.16-smp`
- For a Bigmem kernel, the kernel string will end in `big`. For example:
`2.6.16-big`
- For a i586 kernel, the kernel string will end in `586`. For example:
`2.6.16-586`
- For a PAE kernel (Physical Address Extension), the kernel string will end in `pae`. For example: `2.6.16-pae`
- For a Xen kernel, the kernel string will end in `xen`. For example:
`2.6.16-xen`

Module Naming Conventions

3w-sas.* refers to the specific kernel driver module you will copy in the examples shown in steps 3 and 4. The name of the kernel driver module you will copy (3w-sas.*) varies, depending on the kernel; however you will always copy it to a file named 3w-sas.ko for 2.6 kernels. Depending on the supported release, not all modules may be required or available.

The available kernel driver module files are:

- For default kernels: 3w-sas.ko
- For SMP kernels: 3w-sas.smp
- For Bigmem kernels: 3w-sas.big
- For i586 kernels: 3w-sas.586
- For PAE kernels: 3w-sas.pae
- For Xen kernels: 3w-sas.xen

To install the 3ware driver and update the RAM disk

- 1 Log in as root and open a console window.
- 2 Mount the CD which contains the 3ware kernel driver module.

To mount the CD, type:

```
mount /dev/cdrom /mnt and press Enter.
```

- 3 Copy the kernel driver module:

For Redhat Linux Intel x86 and AMD, type:

```
cp /mnt/packages/drivers/linux/redhat/<version>/x86/
3w-sas.<ko or pae> /lib/modules/<kernel string>/kernel/
drivers/scsi/3w-sas.ko
```

For Fedora Core on Intel x86 and AMD, type:

```
cp /mnt/packages/drivers/linux/fedora/<version>/x86/
3w-sas.<ko, 586, or pae> /lib/modules/<kernel string>/
kernel/drivers/scsi/3w-sas.ko
```

If prompted to overwrite, type y.

For Redhat Linux on AMD Opteron and Intel EM64T, type:

```
cp /mnt/cdrom/packages/drivers/linux/redhat/<version>/
x86_64/3w-sas.ko /lib/modules/<kernel string>/kernel/
drivers/scsi/3w-sas.ko
```

For Fedora Core on AMD Opteron and Intel EM64T, type:

```
cp /mnt/packages/drivers/linux/fedora/<version>/x86_64/
3w-sas.ko /lib/modules/<kernel string>/kernel/drivers/
scsi/3w-sas.ko
```

If prompted to overwrite, type y.

4 **For 2.6 Kernels**, add the following line to `/etc/modprobe.conf`
`alias scsi_hostadapter 3w-sas`

5 Update the `modules.dep` file, by issuing the following command:
`/sbin/depmod -a`

6 Run `mkinitrd` by entering the following:

```
/sbin/mkinitrd -v -f /boot/initrd-<kernel string>.img  
<kernel string>
```

where `<kernel string>` is the `/lib/modules` directory from which to copy the `3w-sas` driver.

Example:

```
/sbin/mkinitrd -v -f /boot/initrd-2.6.18-14.img 2.6.18-14
```

7 If you are using the GRUB boot loader, skip to Step 8.

If you are using the LILO boot loader, run LILO to update the boot record on disk by typing the following:

```
/sbin/lilo
```

The output should be similar to:

```
Added linux *
```

8 Reboot.

The 3ware kernel driver module will be loaded from the ram disk automatically at boot time.

To install the 3ware kernel driver module and load the module manually instead of using a RAM disk

1 Log in as root and open a console window.

2 Mount the CD which contains the 3ware kernel driver module.

To mount the CD, type:

```
mount /dev/cdrom /mnt and press Enter.
```

3 Copy the kernel driver module.

For Redhat Linux on Intel x86 and AMD x86, type:

```
cp /mnt/packages/drivers/linux/redhat/<version>/x86/  
3w-sas.<ko or pae> /lib/modules/<kernel string>/kernel/  
drivers/scsi/3w-sas.ko
```

For Fedora Core on Intel x86 and AMD x86, type:

```
cp /mnt/packages/drivers/linux/fedora/<version>/x86/  
3w-sas.<ko, 586, or pae> /lib/modules/<kernel string>/  
kernel/drivers/scsi/3w-sas.ko
```

If prompted to overwrite, type `y`.

For Redhat Linux on AMD Opteron and Intel EM64T, type:

```
cp /mnt/packages/drivers/linux/redhat/<version>/x86_64/  
3w-sas.ko /lib/modules/<kernel string>/kernel/drivers/  
scsi/3w-sas.ko
```

For Fedora Core on AMD Opteron and Intel EM64T, type:

```
cp /mnt/packages/drivers/linux/fedora/<version>/x86_64/  
3w-sas.ko /lib/modules/<kernel string>/kernel/drivers/  
scsi/3w-sas.ko
```

If prompted to overwrite, type *y*.

- 4 Add the following line to `/etc/modprobe.conf`:

```
alias scsi_hostadapter 3w-sas
```

- 5 Update the `modules.dep` file, by issuing the following command:

```
/sbin/depmod -a
```

- 6 Load the kernel driver module manually. Type:

```
modprobe sd_mod  
insmod /lib/modules/<kernel string>/kernel/drivers/scsi/  
3w-sas.ko
```

You can also incorporate the `insmod` command into a startup script.

Driver Installation Under SUSE Linux

Materials required

- LSI 3ware CD
- Floppy diskette or USB drive, if you need to make a driver install disk
- SUSE Linux Installation disk (Not required if SUSE Linux is already installed on another drive.)

Creating a SUSE Linux Driver Disk

If you are installing SUSE Linux on a new drive or unit managed by the 3ware RAID controller, you will need to install the 3ware RAID controller driver at the same time as the operating system.

You can load the driver directly from the 3ware CD, or from a floppy diskette or USB drive on which you have installed the driver.

To create a driver install floppy diskette

- 1 Insert the 3ware CD into your Linux system. A GUI such as X windows is required to load the 3ware menu.

To manually mount the CD, type:

```
mount -t iso9660 /dev/cdrom /mnt
```

To start autorun, type:

```
/mnt/autorun
```

- 2 When the 3ware Menu appears, click **Driver Disk Images**.
- 3 In the 3ware Driver Disk Images menu, click the button for the driver disk you want to create.

A confirmation window opens.

- 4 Insert a blank diskette into a drive and click the **Yes** button to begin copying the driver to the floppy diskette.



Note: If you need to create a Linux driver diskette for a Linux distribution other than what is available on the menu, search the LSI KnowledgeBase for keyword 14546 at <http://kb.lsi.com>.

To copy the driver to a USB drive

- 1 Insert the 3ware CD into your system.

To manually mount the CD, type:

```
mount -t iso9660 /dev/cdrom /mnt
```

- 2 On the CD, navigate to packages/images and locate the appropriate driver.
- 3 Insert a USB drive into your computer.
- 4 Unzip (if .zip) or untar (if .tgz) the driver file to the USB drive.

Note: If using Winzip or another Windows utility to extract the Linux file, use the .zip version instead of the .tgz version. Otherwise the files will not be compatible with Linux.

Installing the 3ware Kernel Driver Module while Installing SUSE Linux on a New Unit



Note: If SUSE Linux is already installed on another drive, turn to "Installing the 3ware Kernel Driver Module on a SUSE Linux System that Boots from a Different Device" on page 319.

- 1 Boot directly from the SUSE installation CD #1 or DVD.
- 2 When installing SUSE, press either the F6 key or the F3 key, depending on the version.
You will then be prompted to insert the driver install disk and to select the media type.
- 3 Insert the 3ware Linux SUSE driver installation disk or 3ware CD.
- 4 Click OK and continue with the installation.

Installing the 3ware Kernel Driver Module on a SUSE Linux System that Boots from a Different Device

In the instruction below, replace <kernel string> with the kernel version you are using (i.e. 2.6, etc.).

In addition, replace 3w-sas.* with the appropriate module file for your kernel. Depending on the supported release, not all modules may be required or available.

The available kernel driver module files are:

- For default kernels: 3w-sas.ko
- For SMP kernels: 3w-sas.smp
- For high memory kernels: 3w-sas.big
- For i586 kernels: 3w-sas.586
- For Xen kernels: 3w-sas.xen

- 1 Log in as root.
- 2 Edit /etc/sysconfig/kernel and make sure the file contains the following line:

```
INITRD_MODULES="reiserfs 3w-sas"
```



Note: Other modules may be listed before or after `3w-sas`, depending on the installation. You may see entries like `reiserfs`, `ext3` or `scsi_mod`. If present, leave them (ensuring there is a space between each module name), since the system needs them to boot properly.

- 3 If you are using SUSE 11.2 or earlier, after the existing `3w-9xxx` entry, add
`3w-sas` to the file `/lib/modules/<kernel string>/modules.dep`
- 4 Mount the CD-ROM and copy and install the appropriate kernel driver module for your system.



Note: The 64-bit driver is also used for 64-bit Intel Xeon and AMD Opteron based motherboards.

```
mount -t iso9660 /dev/cdrom /mnt
```

Copy the kernel driver module:

For openSUSE and SUSE Linux Enterprise Server 32-bit (x86), type:

```
cp /mnt/packages/drivers/linux/suse/<version>/x86/
3w-sas.<kernel extension>
/lib/modules/<kernel string>/kernel/drivers/scsi/
3w-sas.ko
```

For openSUSE and SUSE Linux Enterprise Server 64-bit (x86_64), type:

```
cp /mnt/packages/drivers/linux/suse/<version>/x86_64/
3w-sas.ko
/lib/modules/<kernel string>/kernel/drivers/scsi/
3w-sas.ko
```

If prompted to overwrite, type `y`.

- 5 To load the kernel driver module, type:

```
modprobe sd_mod
```

```
insmod /lib/modules/<kernel string>/kernel/drivers/scsi/
3w-sas.ko
```



Note: If the kernel driver module installation fails, confirm that the correct driver was installed. If a driver is not available for your system, you will need to compile your own driver. For more information, search the LSI KnowledgeBase for keyword 14546 at <http://kb.lsi.com>.

- 6 Type:

```
/sbin/depmod -a
```

- 7 Type:

```
/sbin/mkinitrd
```
- 8 If you are using the GRUB boot loader, you are finished.
 If you are using the LILO boot loader, run LILO to update the boot record on disk by typing the following:

```
/sbin/lilo
```

 The output should be similar to:

```
Added linux *
```

Compiling a 3ware Driver for Linux

If you are using a Linux distribution for which there is not a compiled driver available from 3ware, you can copy the source from the 3ware CD or download the source from the LSI website and compile a new driver. For more information, search the LSI KnowledgeBase for keyword 14546 at <http://kb.lsi.com>.

Updating the 3ware Driver Under Red Hat or Fedora Core

The following steps describe how to update the 3ware driver under Red Hat.



Note: Backup your original driver before updating in case you need to revert back to it. However, you will not be able to revert back to the original driver if you are booting from that unit.

To update the 3ware driver under Red Hat

- 1 Download and extract the driver, as described under “Downloading the Driver and Firmware” on page 172.
- 2 Backup any critical data prior to updating the 3ware driver.
- 3 Change the directory to the location with the extracted driver.
- 4 Copy the files to the appropriate directory.

(In the commands below, replace <version> with the applicable Red Hat or Fedora Core version, such as ws5 or fc11, and replace <kernel string> with the applicable kernel, for example 2.6)

Note: The name of the module you will copy (`3w-sas.*`) varies, depending on the kernel; however you will always copy it to a file named `3w-sas.ko` for 2.6 kernels

For Red Hat or Fedora Core Uniprocessor

```
cp <version>/3w-sas.ko /lib/modules/  
<kernel string>/kernel/drivers/scsi/3w-sas.ko
```

For Red Hat SMP

```
cp <version>/3w-sas.smp /lib/modules/  
<kernel string>/kernel/drivers/scsi/3w-sas.ko
```

For Red Hat Bigmem

```
cp <version>/3w-sas.big /lib/modules/  
<kernel string>/kernel/drivers/scsi/3w-sas.ko
```

For Red Hat Xen

```
cp <version>/3w-sas.xen /lib/modules/  
<kernel string>/kernel/drivers/scsi/3w-sas.ko
```

- 5 **For 2.6 Kernels**, add the following line to

```
/etc/modprobe.conf.  
alias scsi_hostadapter 3w-sas
```

- 6 Complete the upgrade by upgrading the initial ramdisk.

Change the directory to the boot directory:

```
cd /boot
```

Run mkinitrd by entering the following:

(In the commands below, replace <kernel string> with the applicable kernel, for example 2.4.20-8)

For Red Hat or Fedora Core Uniprocessor

```
mkinitrd -v -f initrd-<kernel string>.img <kernel string>
```

For Red Hat SMP

```
mkinitrd -v -f initrd-<kernel string>smp.img <kernel  
string>smp
```

For Red Hat Bigmem

```
mkinitrd -v -f initrd-<kernel string>bigmem.img <kernel  
string>bigmem
```

For Red Hat Xen

```
mkinitrd -v -f initrd-<kernel string>xen.img <kernel  
string>xen
```

- 7 If you are using lilo, run lilo to update to the boot loader.

You should see a printout of kernels that are able to boot on this system after running lilo.

Updating the 3ware Driver Under SUSE

The following steps describe how to update the 3ware driver under SUSE.



Note: Backup your original driver before updating in case you need to revert back to it. However, you will not be able to revert back to the original driver if you are booted from that unit.

To update the 3ware driver under SUSE

- 1 Download and extract the driver, as described under “Downloading the Driver and Firmware” on page 172.
- 2 Backup any critical data prior to updating the 3ware driver.
- 3 Change the directory to the location with the extracted driver.
- 4 Copy the files to the appropriate directory.

(In the commands below, replace <version> with applicable SUSE version, such as su10)

Replace <kernel string> with applicable kernel (i.e.: 2.6.16.x)

For SUSE Uniprocessor (2.6 kernels)

```
cp <version>/3w-sas.ko /lib/modules/<kernel string>/kernel/
drivers/scsi/3w-sas.ko
```

For SUSE SMP (2.6 kernels)

```
cp <version>/3w-sas.smp /lib/modules/<kernel string>/
kernel/drivers/scsi/3w-sas.ko
```

For SUSE high memory systems (2.6 kernels)

```
cp <version>/3w-sas.big /lib/modules/<kernel string>/
kernel/drivers/scsi/3w-sas.ko
```

- 5 Run `/sbin/depmod -a`
- 6 Make sure the file `/lib/modules/<kernel string>/modules.dep` contains an entry for `3w-sas`. If not, add it after the `3w-xxxx` entry.
- 7 Complete the upgrade by upgrading the initial ramdisk. (Skip to step 10 if you prefer to use `insmod 3w-sas.ko`, instead.)

Make sure the file `/etc/sysconfig/kernel` contains the following line:

```
INITRD_MODULES="3w-sas"
```



Note: Other modules may be listed before or after 3w-sas depending on the installation. You may see entries like reiserfs, ext3 or scsi_mod. Leave these entries alone, if present, as the system may need them to boot properly.

- 8 Run mkinitrd.
- 9 If you are using lilo, use lilo to update to the boot loader.
You should see a printout of kernels that are able to boot on this system after running lilo.
- 10 Reboot, if booted from the 3ware controller. Otherwise, continue with step 11.

The driver is now updated.

- 11 Stop the current driver module, if loaded:

```
rmmod 3w-sas
```

- 12 Load the new driver module:

```
modprobe 3w-sas
```

If the new driver fails to load properly, confirm that you used correct driver. If your kernel or SUSE version is not supported, you will need to compile your own driver. For more information, search the LSI KnowledgeBase for keyword 14546 at <http://kb.lsi.com>.

Installing Management Software (3DM2 and CLI)

This section provides detailed instructions for installing and uninstalling 3ware's RAID management software using the command line installer.

- Installing 3ware Management Software
- Uninstalling 3ware Management Software

Installing 3ware Management Software

The following steps describe how to install software on Linux at a command line, using a text-only interface. You must be root to run the installer.

- 1 Download the LSI 3ware FreeBSD installation image from LSI channel website at <http://www.lsi.com/channel/ChannelDownloads>.
- 2 Mount the image or burn the image to a CD.
- 3 Navigate to the folder on the mounted image or CD that contains the installer.

```
packages/installers/tools/linux
```


- 4 Type: `./install.sh -i`
- 5 Respond to each screen as the script walks you through the installation process.
- 6 After the installation is complete, check that the software was installed correctly.

Uninstalling 3ware Management Software

The following steps describe how to uninstall software on Linux at a command line, using a text-only interface. You must be root to run the installer.

- 1 Navigate to the folder on your computer where 3DM2/CLI are installed.
`/opt/3ware/`

Backup files, if needed. All files will be removed during uninstall from:
`/opt/3ware`

This directory is only for use by the 3ware management software. No user data should be stored here.

- 2 Type: `./install.sh -u`
- 3 Respond to each screen as the script walks you through the uninstall process.
- 4 After the uninstall is complete, check that the software is uninstalled.

Installing 3ware Drivers and Software under Mac OS X

This section provides detailed instructions for installing the 3ware driver and the RAID management software running under an Mac operating system.

The following topics are included in this section:

- Driver and Software Installation
- Uninstalling 3ware Software under Mac OS X

Driver and Software Installation

You can install all software at once, or you can use the installer to install specific components.

If you later want to uninstall the 3DM2 software, see “Uninstalling 3ware Management Software” on page 325.

To install the driver and disk management tools

- 1 Download the Mac 3ware installation CD from <http://www.lsi.com/channel/ChannelDownloads>.
- 2 LSI provides two different image type files (3wareCD.cdr or 3wareCD.dmg). Once downloaded to your Mac double-click on either image to mount the image and open the image for browsing.
- 3 Double-click the icon StartInstall to begin the software and driver installation process.

When prompted, enter your Macintosh Admin user name and password and click **OK**.

Figure 112. Authenticate dialog requests user name and password



The installer starts and the welcome screen appears.

- 4 From the Welcome screen, click **Next** to start the installation process.

Figure 113. Welcome Installation Screen



- 5 On the License Agreement page, accept the agreement and click **Next**.

Figure 114. License Agreement Screen



- 6 If you want to change where the 3ware Disk Management tools 3DM2 and CLI will be installed, you can change the path and directory.

Default install location for Mac OS X 10.6.0 is:
`/opt/3ware`

Default install location for Mac OS X 10.5.0 is:
`/Applications/3ware`

When you are ready, click **Next**.

Figure 115. Specify Directory Path Screen



- 7 Select what components you want to install.

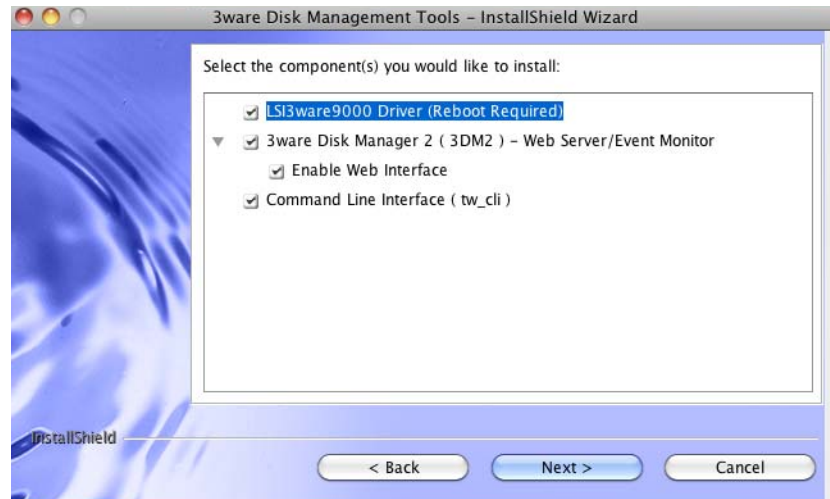
3DM2 and CLI are applications that let you set up and manage RAID units.

If you unselect **Enable Web Interface**, the 3DM2 web interface will not be enabled. In this case, an additional screen will display, that allows you to enable email notification. (If you do enable the web interface, you can enable this feature later, after 3DM2 has been installed.)

Refer to the “3DM2 Reference” on page 189, for details about 3DM2 and setting preferences, including email notification.

When you are ready, click **Next** to continue.

Figure 116. Select Components to Install Screen



- 8 This screen summarizes what you selected in the previous two screens and includes the total size of the installation.

When you are ready, click **Install** to start the installation.

Figure 117. Preinstall Summary Screen



- 9 When the final installation screen lets you know that installation is complete, click **Finish**.

Figure 118. Final Installation Screen



You will be prompted to restart your computer in order for the driver to be used with your 3ware RAID controller.

- 10 Restart your Mac.

If you have other tasks you wish to complete before restarting, you may do so. For example, if you need to update the firmware, through 3DM2 or CLI, you may do before restarting. (For details about updating the firmware, through 3DM2 see “Updating the Firmware Through 3DM2” on page 174, for details about updating the firmware , through CLI, refer to *3ware SATA+SAS RAID Controller Card CLI Guide, Version 10.2*.

Uninstalling 3ware Software under Mac OS X

To uninstall 3DM2, CLI, and driver, go to the following directory:

Default location for Mac OS X 10.5.0:

Macintosh HD/Applications/3ware

Default location for Mac OS X 10.6.0:

/opt/3ware

Then double-click on the StartUninstall icon, enter password when prompted, then you can select to uninstall everything or only certain component like 3DM2, CLI, or the driver.

Installing 3ware Drivers and Software under OpenSolaris

This section provides detailed instructions for installing the 3ware driver and the RAID management software running under an OpenSolaris operating system.

The following topics are included in this section:

- Driver and Software Installation
- Uninstalling 3ware Software Under OpenSolaris

Driver and Software Installation

This section provides detailed instructions for installing the 3ware driver and the RAID management software.

- Installing the Driver and Software when LSI 3ware RAID Controller is used as Primary Storage
- Installing the Driver and Software when LSI 3ware RAID Controller is used as Secondary Storage
- Installing the Driver and Software from the Command Line.

Installing the Driver and Software when LSI 3ware RAID Controller is used as Primary Storage

The steps below describe how to install the 3ware driver and RAID management software as the primary storage.

**Note:**

Installing the driver and software when the RAID controller is used as the primary storage only works on systems that support legacy BIOS.

- 1 Install your 3ware RAID controller. For details, see the installing guide for the controller.
- 2 Create the RAID units on the 3ware RAID controller using 3BM. For details on how to create and order units, refer to "Creating a Unit through 3BM " and "Ordering Units in 3BM" on pages 97 and 101.
- 3 Download the LSI 3ware complete ISO image from <http://www.lsi.com/channel/ChannelDownloads> and burn it to a CD.
- 4 Copy the two driver folders from the CD that you just burned:

```
packages/drivers/opensolaris/amd64
packages/drivers/opensolaris/i386
```

to a USB flash drive or other storage media.

- 5 Insert the OpenSolaris CD into your CD or DVD drive and boot from the CD.
- 6 When booting completes, you will be in the OpenSolaris desktop, open a terminal.
- 7 Insert the USB flash drive into your system. The drive should be mount automatically otherwise you can manually mount the drive.
- 8 From the terminal do the following:
 - a Login as root


```
# su
Passwd: opensolaris
```
 - b Run this command:


```
# pfexec touch /ADD_DRV_IGNORE_ROOT_BASEDIR
```
 - c Copy 3ware drivers from the USB flash drive or other storage media


```
# cp /<mount_point>/amd64/tw /kernel/drv/amd64
# cp /<mount_point>/i386/tw /kernel/drv/
```
 - d Load 3ware driver


```
# add_drv -m "*" 0666 root sys" -i
'"pci13c1,1003"' "'pci13c1,1004"'
"'pci13c1,1005"' "'pci13c1,1010"' -c scsi tw
```
 - e Double-click *Install OpenSolaris* icon on the OpenSolaris desktop to start the installation process. You should be able to select the array on the 3ware controller to install OpenSolaris on it. Follow through to complete the installation and reboot the system
- 9 To install the management software insert the 3ware CD you burned in step 3, after OpenSolaris is rebooted, navigate to the directory on the CD that contains the installer.


```
packages/installers/tools/opensolaris
```
- 10 Type:


```
./setupSolaris_x86.bin
```

 and press *Enter*.

Installing the Driver and Software when LSI 3ware RAID Controller is used as Secondary Storage

- 1 The steps below describe how to install the 3ware driver and RAID management software from a graphical window. You must be root to run

the installer. Download the LSI 3ware complete ISO image from <http://www.lsi.com/channel/ChannelDownloads> and burn it to a CD or mount the ISO image directly under OpenSolaris.

- 2 With your computer on, boot to OpenSolaris from another boot device. Then insert the CD you burned in step 1 and navigate to the folder on the CD that contains the installer.

`packages/installers/tools/opensolaris`

- 3 Type:

`./setupSolaris_x86.bin`

and press **Enter**.

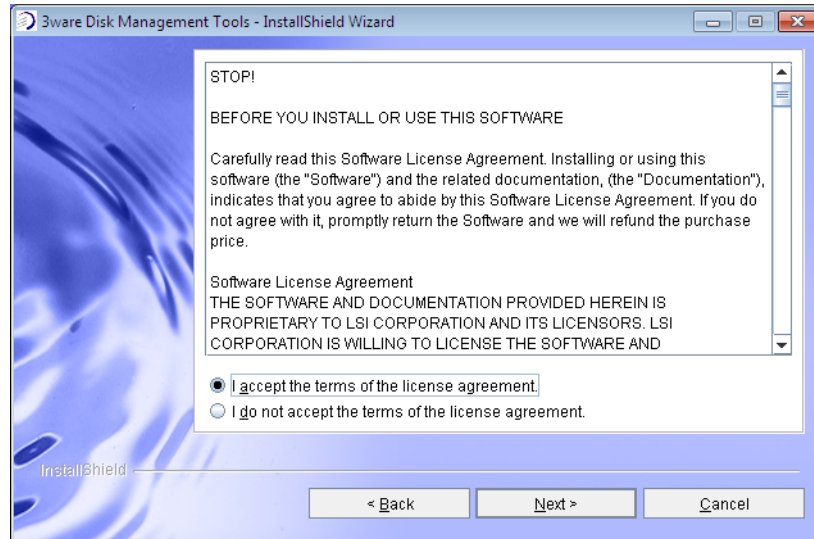
- 4 After you press **Enter**, the application starts in graphical mode. On the Welcome screen, click **Next**.

Figure 119. Welcome Installation Screen



- 5 On the License Agreement page, accept the agreement and click **Next**.

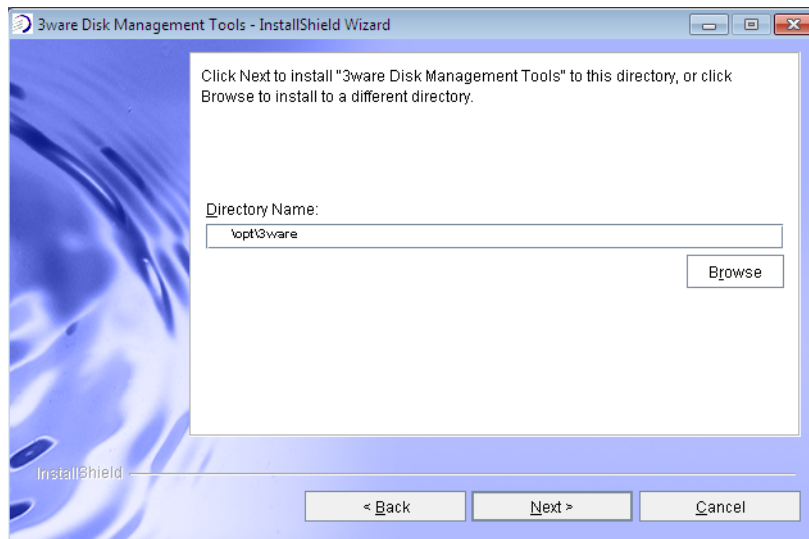
Figure 120. License Agreement Screen



- 6 If you want to change where the components will be installed, you can change the path and directory.

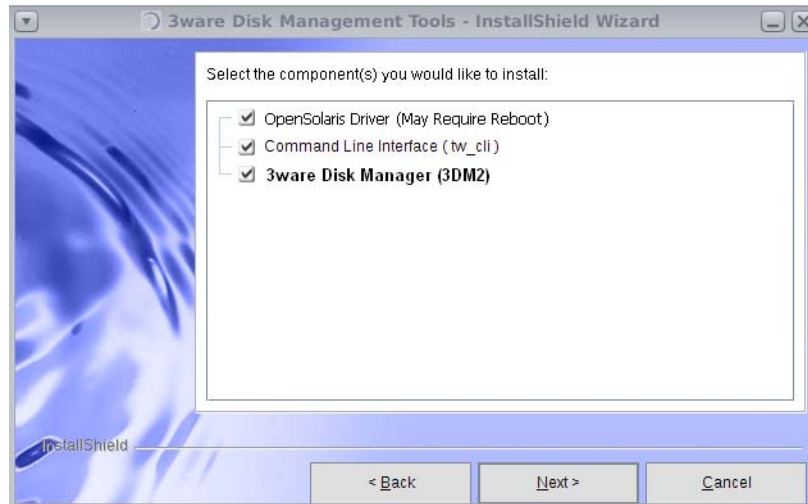
When you are ready, click **Next**.

Figure 121. Specify Directory Path Screen



- 7 Select the components you want to install and click **Next**.

Figure 122. Select Components to Install Screen

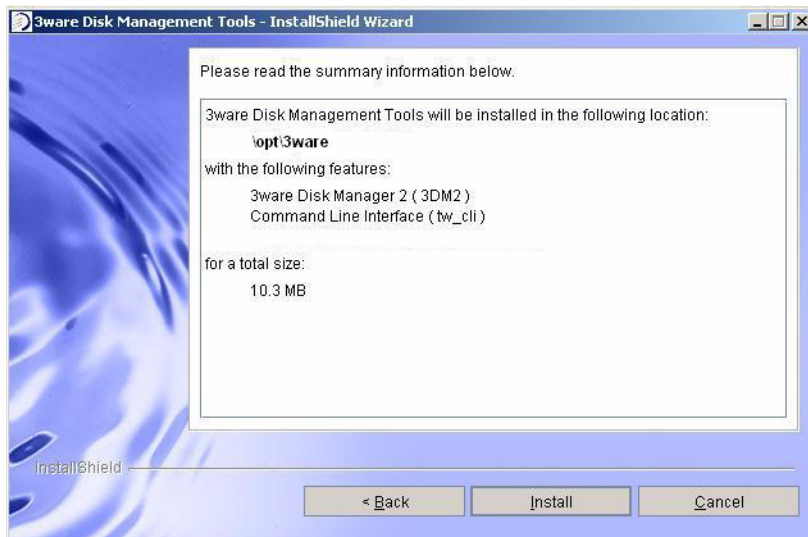


- The **LSI 3ware OpenSolaris driver** is required for the operating system to be able to interact with the 3ware RAID controller. (Installing the driver may require that you restart your computer.)
- **CLI** lets you set up and manage RAID units through a command line interface.

- 8 On the summary screen, review the installation that is about to occur.

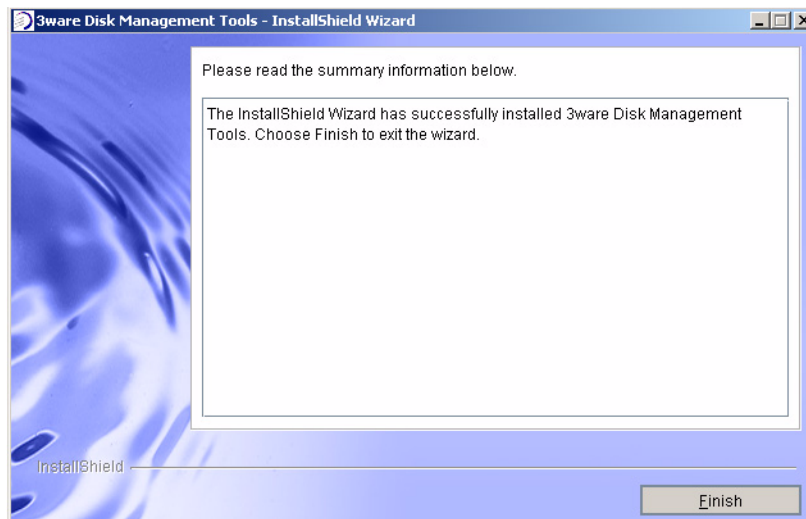
If you want to make changes, use the **Back** button to move back through the screens. When you are ready, click **Install** to continue.

Figure 123. Installation Summary Screen



- 9 When the final installation screen lets you know that installation is complete, click **Finish**.

Figure 124. Final Installation Screen



- 10 If you are prompted, restart your computer to load the driver.
 You can now use the 3ware BIOS Manager (3BM), the 3ware Disk Manager (3DM2), or the 3ware command line interface (CLI) to create and manage RAID units.
 Instructions for using the CLI are available in *3ware SATA+SAS RAID Controller Card CLI Guide, Version 10.2*

Installing the Driver and Software from the Command Line

The following steps describe how to install software on OpenSolaris at a command line, using a console application. You must be root to run the installer.

To install the driver and software on OpenSolaris from the command line

- 1 Download the LSI 3ware OpenSolaris installation image from <http://www.lsi.com/channel/ChannelDownloads> and mount the image or burn it to a CD-ROM disc.
- 2 Navigate to the folder on the mounted image or CD that contains the installer.
`packages/installers/tools/solaris/opensolaris`

3 Type:

```
./setupSolaris_x86.bin -console
```

and press **Enter**.

The application starts in text mode.

4 Respond to each screen as it walks you through the installation process.

The Console installation screens mirror those that display using the GUI installer. For specific information about the screens, see the previous section in this document.

To navigate in text mode, type:

1 for Next

2 for Previous

3 to Cancel

5 to Redisplay

0 to Continue Installing

5 After the installation is complete, check that the driver has loaded correctly.

```
# modinfo | grep tw
```

Uninstalling 3ware Software Under OpenSolaris

The following steps describe how to uninstall software on OpenSolaris from the command line. If you do not use the `-console` option, the installer will assume you want GUI mode. You must be root to run the uninstaller.

1 Navigate to the directory where you installed the software. The default directory is `/opt/3ware`.2 Change to the subdirectory “`_uninst`”.

3 To uninstall in text mode, type:

```
./uninstall.bin -console and press Enter.
```

To uninstall in graphical mode, type:

```
./uninstall.bin and press Enter.
```

Follow the prompts to remove the installed components.

Installing 3ware Drivers and Software under VMware

This section provides detailed instructions for installing the 3ware driver and the RAID management software running under an VMware operating system.

The following topics are included in this section:

- Driver Installation Under VMware ESX/ESXi 4.x Server
- Updating the Firmware Under VMware
- Installing 3ware RAID Controller Management Software for VMware
- Uninstalling 3ware Software on VMware

Driver Installation Under VMware ESX/ESXi 4.x Server

This section provides details about how to install the driver for your LSI 3ware RAID controller under VMware ESX/ESXi Server 4.x. It is organized into these sections:

- Installing the Driver when LSI 3ware RAID Controller is used as Primary Storage
- Installing the Driver when LSI 3ware RAID Controller is used as Secondary Storage
 - Installing the Driver using vihostupdate
 - Installing the Driver using esxupdate

Installing the Driver when LSI 3ware RAID Controller is used as Primary Storage



Prerequisite to Driver Installation: (Primary Storage)

You need a copy of:

VMware ESX/ESXi Server 4.0, Update 1 (U1) installation CD or
VMware ESX/ESXi Server 4.x/4.x GA (see patch below).

Due to a bug in the VMkernel you must run the following patch:

VMware patch ESX400-200907001 for ESX 4.0 or
VMware patch ESXi400-VEM-200907001 for ESXi 4.0

This issue is fixed in the ESX/ESXi 4.0, Update 1 (U1).

You need a copy of:

LSI 3ware VMware 4.0 driver image (3w-sas.iso) on CD.

You need to download the VMware 4.0 driver from the LSI website at:

<http://www.lsi.com/channel/ChannelDownloads>.

Save the compressed file and extract the 3w-sas.iso file. Then burn the image to a iso CD.

- 1 Install your 3ware RAID controller and drives. For details, see the installation guide for the controller.
- 2 Create the RAID units on the 3ware RAID controller using 3BM. You can access 3BM by pressing Alt-3 or 3 during system startup. For details on how to create and order units, refer to "Creating a Unit through 3BM " and "Ordering Units in 3BM" on pages 97 and 101.
- 3 Insert the applicable VMware ESX Installation CD into your CD-ROM or DVD drive and restart your system.

Your system should boot from the CD. (If it does not, change the BIOS settings to boot from the CD and then restart.)
- 4 At the VMware ESX Server 4.0 splash screen, press **Enter** to start the graphical installation method.
- 5 When prompted, choose your language and press **Enter**.
- 6 When prompted, choose your keyboard type and press **Enter**.
- 7 When prompted for additional driver support, provide the 3ware VMware driver CD. After the driver is loaded, you should follow on-screen instructions to complete VMware installation.
- 8 After you have finished your VMware ESX Server 4.x installation, reboot the server.

Installing the Driver when LSI 3ware RAID Controller is used as Secondary Storage



Prerequisite to Driver Installation: (Secondary Storage)

You need a copy of:

VMware vSphere 4.x Client on a windows machine.

You need to download the client from the VMware vSphere website at:

<http://www.vmware.com/support/product-support/vsphere>

You need a copy of:

The VMware VShere Command-Line Interface (CLI)

You need to download the CLI from the VMware communities website at:

http://communities.vmware.com/community/developer/vsphere_cli

vihostupdate.pl is part of VMware vSphere CLI download.

Depending upon your selection of ESX installation or ESXi installation, there are several options available for you to install and update the LSI 3ware VMware 4.x driver.

- If you are using ESX installation you need either:
 - *vihostupdate* to install the driver or
 - *esxupdate* to install the driver
- If you use ESXi installation you need to use:
 - *vihostupdate* to install the driver

Installing the Driver using vihostupdate

To update or add LSI 3ware drivers on existing ESX and ESXi installations using *vihostupdate*.

- 1 insert LSI 3ware VMware driver CDROM or medium that contains the driver file. Copy the file, *offline-bundle.zip* to the root of C: \e.g., C:\offline-bundle.zip.
- 2 Launch the vSphere Client providing the credentials for root.
- 3 Put the ESX/ESXi server into maintenance mode from vSphere Client.
(Double-click on *Inventory* >> click *Summary* tab >> click *Enter Maintenance Mode*)
- 4 Go to *Programs* >> *VMware* >> and launch the vSphere CLI.
- 5 You should have a command prompt showing the following path,
C:\Program Files\VMware\VMware vSphere CLI
- 6 Change directory to bin e.g., `cd bin`

- 7 Now enter the following command via the VMware CLI perl
`vihostupdate.pl -server <x.x.x.x ip address> -username
<root> -password "<>" -b c:\<offline-bundle.zip> -i`
- 8 Once the driver load using vihostupdate is finished, close the VMware CLI.
- 9 Go back into the vSphere Client and take the ESX/ESXi server out of maintenance mode (click *Summary tab* >> click *Exit Maintenance Mode*.)
- 10 Reboot it. (click *Summary tab* >> click *Reboot*, then *Yes* to confirm)
- 11 As the ESX/ESXi server comes back up, you should see the 3ware-sas driver loading.
- 12 On vSphere you see the connection to the ESXi Server automatically reestablished through the vSphere Client, after the system has rebooted and all services have loaded.
- 13 Now you are ready to create VMs; storage pools, etc.

Installing the Driver using esxupdate

To update or add LSI 3ware drivers on existing ESX installations using *esxupdate*.

- 1 Place the driver CD in the CD-ROM drive of the ESX host.
- 2 Mount the driver CD.
`mount -t iso9660 /dev/cdrom /mnt/cdrom`
- 3 Navigate to the directory on the CD that contains the driver.
Navigate to `<cd mount point>/offline-bundle/` and locate the `offline-bundle.zip` file.
- 4 Run the esxupdate command to install drivers using the offline bundle.
`esxupdate --bundle= LSI_3.26.08.001vm40-offline_bundle
xxxxxx.zip update`

Updating the Firmware Under VMware

Firmware updates to the 3ware RAID controller can be done from 3DM2 or CLI. For details, see “Updating the Firmware and Driver” on page 171.

Installing 3ware RAID Controller Management Software for VMware



Prerequisite to Software Installation:

You need a copy of:

Software utilities 3DM2 and CLI are available on the management software CD. You need to download the LSI 3ware management software CD from the LSI website at: <http://www.lsi.com/channel/ChannelDownloads> and burn the image to a CD.

3ware RAID controller management software includes 3DM2 and CLI. CLI can run locally on the VMware server in a console window.

By default, VMware ESX Server 4.0 does not have a GUI and therefore you cannot access 3DM2 locally. You must use another system that has a GUI and a web browser to access 3DM2.

After initial installation and setup, administration will typically be done remotely through CLI or 3DM2.

If you have not yet installed 3DM2 and CLI, use the steps below to do so.

- 1 Mount the 3ware software image CD.

```
mount -t iso9660 /dev/cdrom /mnt/cdrom
```

- 2 Navigate to the appropriate directory where the 3DM2 and CLI rpm files are located.

```
cd /mnt/cdrom/packages/installers/tools/vmware/esx40/
```

- 3 Run the install commands for CLI and 3DM2.

```
rpm -ivh <LSI-3ware-CommandLine-Management-Utility-xxx.rpm>
rpm -ivh <LSI-3ware-3dm2-Management-Utility-xxx.rpm>
```

- 4 Note the URL supplied by 3DM2 at the end of installation, (for example, <https://10.0.0.2:888>), as it will be required in order to connect to 3DM2 through a web browser.

Uninstalling 3ware Software on VMware

You can uninstall CLI, 3DM2, and the 3ware RAID controller driver.

- 1 Login as root.
- 2 Check for installed packages.

```
esxupdate query
```

You will see a list of the packages that have been installed on VMware.

- 3 Run the command

```
rpm -e <package_name>
```

on the package you wish to uninstall.

The software is removed.

Installing 3ware Drivers and Software under Windows

This section provides detailed instructions for installing the 3ware driver and the RAID management software running under an Windows operating system. (Windows 2003, Windows 2008, Windows Vista, and Windows 7.)

The following topics are included in this section:

- Driver Installation Under Windows
- Updating the 3ware Driver Under Windows
- Installing Software from a Graphical User Interface (GUI)

Driver Installation Under Windows



Note: Before installing the 3ware driver, you may want to physically install your 3ware RAID controller in the system.

Consult the installation guide that came with your controller for how to do this. If you do not have a hardcopy of the installation manual, it is available in the “doc” folder on your 3ware CD, or you can download it from the LSI website at <http://www.lsi.com/channel/ChannelDownloads>.

The 3ware RAID controller can be used with Windows Server 2003 (SP2 or newer), Windows 2008, Windows 2008 R2, Vista, and Windows 7, with both the 32-bit and 64-bit versions. It is recommended that you upgrade to the latest service pack available.

A drive or unit managed by the 3ware RAID controller may be configured to be your system’s boot device. Or, you can use units managed by the 3ware controller for secondary storage and boot from another device, such as a disk attached to the motherboard, or other bootable media.

This section contains instructions for how to:

- Create a driver disk for the 3ware RAID controller.
- Install the 3ware driver and Windows on a new drive or unit.

- Install the 3ware driver when Windows is already installed on a different device.



Note: You must have administrator privileges for your system to install the Windows operating system and the 3ware driver.

Materials Required

- LSI 3ware CD
- Microsoft Windows installation media (Not required if Windows is already installed on another drive.).

Floppy diskette or USB drive, to create a driver disk, if required **Creating a 3ware Driver Disk**

If you are installing Windows on a new unit or drive managed by the 3ware RAID controller, you can create a driver disk, or install the driver from the 3ware CD.

To create a driver floppy diskette

- 1 Insert the 3ware CD into your Windows system.
Autorun should start the 3ware menu program. If it does not, open **My Computer** from within the Windows Explorer, select the CD, right-click and choose **AutoPlay**.
- 2 When the License screen appears, review and agree to the license in order to continue.
- 3 When the 3ware Menu appears, click **Driver Disk Images**.
- 4 In the 3ware Driver Disk Images menu, click the appropriate button to create the driver diskette that you need.

Note that there are both 32-bit and 64-bit drivers available for Windows. Be sure to select the correct one.
- 5 When the confirm message appears, insert a blank diskette into a floppy drive and click the **Yes** button to begin the process.

To copy the driver to a USB drive

- 1 Insert the 3ware CD into your Windows system.
- 2 On the CD, navigate to packages/images and locate the appropriate driver.

- 3 Insert a USB drive into your computer.
- 4 Unzip the driver file to the USB drive.

Installing the 3ware Driver and Windows on a New RAID Unit

If you want to install Windows on a new drive configuration managed by the 3ware RAID controller, follow the instructions in this section.

If Windows is already installed on another drive, turn to “Installing the 3ware Driver and Windows on a New RAID Unit” on page 345.

To install Windows 2003 and the 3ware driver

- 1 Boot from the Windows Server 2003 installation CD and press **F6** when you see the message: “Press F6 if you need to install a 3rd party SCSI or RAID driver” at the bottom of the display.
- 2 When you see the message: “Setup could not determine the type of one or more mass storage devices or you have chosen to manually specify an adapter...”
Type **S** to specify that you have an additional 3ware RAID controller.
- 3 Insert the 3ware driver disk and press **Enter**.
- 4 When a box with **LSI 3ware 9750 RAID Controller** appears, press **Enter** to select it.
- 5 Type **S** if you have additional devices to add. Otherwise, press **Enter**.
- 6 If the “Digital Signature Not Found” message appears, click **Yes** to continue the installation.
(If there are multiple controllers in the system, you will see this message once for each controller.)
- 7 Continue with the normal Windows installation at this point. There are no instructions after installing the driver that are specific to 3ware. If you need additional instructions, refer to the Windows documentation supplied by Microsoft.
- 8 Follow the instructions under “Partitioning, Formatting, and Mounting Units” on page 90.

To install Windows Server 2008, Vista, or Windows 7 and the 3ware driver

- 1 Boot from the Windows Server 2008, Vista, or Windows 7 installation CD and specify the following: Language to Install, Time and currency

format, and Keyboard or input method. Click **Next** and then click **Install Now**.

- 2 Accept the Microsoft License Terms and click **Next**.
- 3 When the message “Which type of installation do you want:?” appears, click **Custom (advanced)**.
- 4 When the message “Where do you want to install Windows?” appears, click **Load Driver**.
- 5 Insert the media with the 3ware driver. It can be a floppy, USB flash drive, CD, or DVD. Once inserted, select **Browse** or **OK** and navigate to the location of the driver.
- 6 When the message “Select the driver to be installed” appears, choose **LSI 3ware 9750 RAID Controller** and click **Next**.
- 7 Continue with the normal Windows installation at this point. There are no instructions after installing the driver that are specific to 3ware. If you need additional instructions, refer to the Windows documentation supplied by Microsoft.
- 8 Follow the instructions under “Partitioning, Formatting, and Mounting Units” on page 90.

Installing the 3ware Driver on a Windows System that Boots from a Different Device

If you are installing the 3ware RAID controller on a system that already has a Windows operating system boot device, follow the instructions in this section. If you will be using a unit managed by the 3ware RAID controller as your boot device, see “Installing the 3ware Driver and Windows on a New RAID Unit” on page 345.



Note: It is easiest and simplest to install the driver before you install the 3ware RAID controller card. If you install the controller card first, when Windows displays the Found New Hardware wizard, cancel the prompts. Then continue with the procedure below.

To install the 3ware driver with the Device Driver Install Wizard

- 1 Insert the 3ware CD into your CD-ROM drive. Click **Agree** at the LSI license agreement.
The 3ware menu appears.
- 2 Click **Install Windows Drivers**.

The installer will select the correct driver for your Windows operating system and open the Device Driver Installation Wizard.

Figure 125. 3ware Device Driver Installation Wizard



- 3 Click **Next**.

You will see the following screen. The green checkmarks indicate successful installation of the driver. If unsuccessful, there will be a red checkmark.

Figure 126. Final Installation Screen



- 4 Click **Finish** to exit the installer.
- 5 If your 3ware RAID controller card is not yet installed, power down the system and physically install the controller card.
When you turn your computer on again, Windows will automatically detect that the controller has been installed.
- 6 When prompted, click the default **Next** to have Windows automatically select the driver.
The driver will automatically be detected, and the controller will be ready to use. Windows may or may not require that you reboot your computer.

Updating the 3ware Driver Under Windows

The easiest way to update the driver for Windows is to use the 3ware Device Driver Install Wizard. You can run it from the 3ware CD, or you can download the installer from the website, as described under “Downloading the Driver and Firmware” on page 172.

To update the 3ware driver with the 3ware Device Driver Install Wizard

- 1 Backup any critical data prior to updating the 3ware driver.
- 2 Log in to your system as system administrator.
- 3 If you have the 3ware CD, insert the 3ware CD into your CD-ROM drive. Click **Agree** at the LSI license agreement.
When the 3ware menu appears, click **Install Windows Drivers**.
The installer will select the correct driver for your Windows operating system and open the 3ware Device Driver Installation Wizard.
- 4 If you downloaded the Device Driver Install Wizard from the LSI website, unzip the **file** to a directory, and then double-click that file to open the 3ware Device Driver Installation Wizard.
- 5 When the 3ware Device Driver Installation Wizard opens, click **Next**.

Figure 127. 3ware Device Driver Installation Wizard

After you click **Next**, the following screen appears. The green checkmarks indicate successful installation of the driver. If unsuccessful, there will be a red checkmark.

Figure 128. Final Installation Screen

- 6 Click **Finish** to exit the installer.

Installing Software from a Graphical User Interface (GUI)

The steps below describe how to install the 3ware RAID management software from a windowing graphical user interface such as Microsoft Windows.

To install the 3ware management software

- 1 With your computer on, insert the 3ware CD that came with your 3ware RAID controller.

The CD should automatically launch and display the LSI License window. If it does not, you can start it manually.

- Under Windows, open **My Computer**, select the CD, right-click and choose **AutoPlay**.
- Under Linux, manually mount the CD by typing

```
mount /dev/cdrom /mnt
```

Start autorun by typing:

```
/mnt/autorun
```

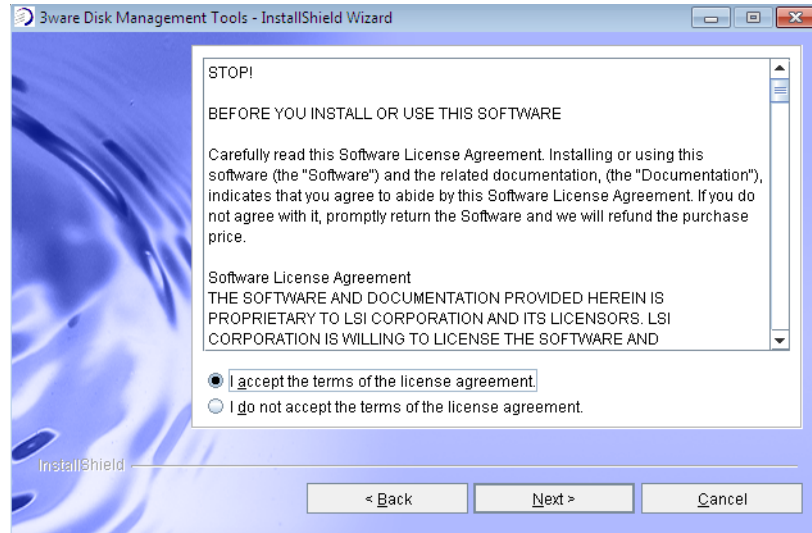
- 2 When the License screen appears, review and agree to the license in order to continue.
- 3 When the 3ware menu appears, click **Install Tools** to launch the installer. The installer will start and the welcome screen appears.
- 4 From the Welcome screen, click **Next** to start the installation process.

Figure 129. Welcome Installation Screen



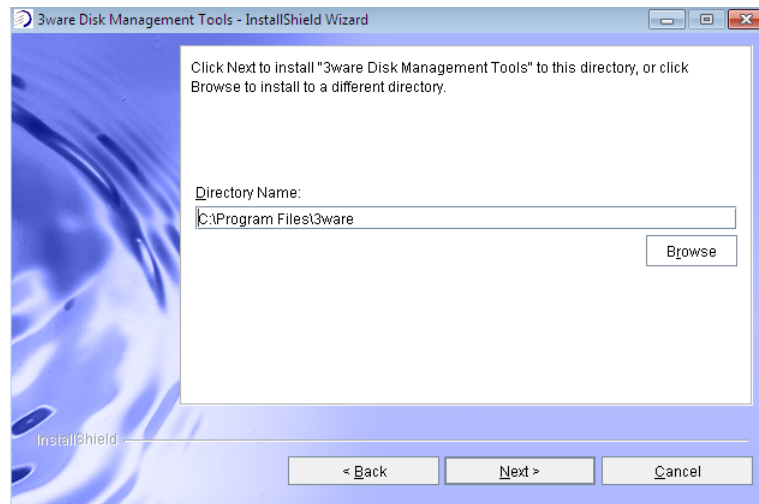
- 5 On the License Agreement page, accept the agreement and click **Next**.

Figure 130. License Agreement Screen

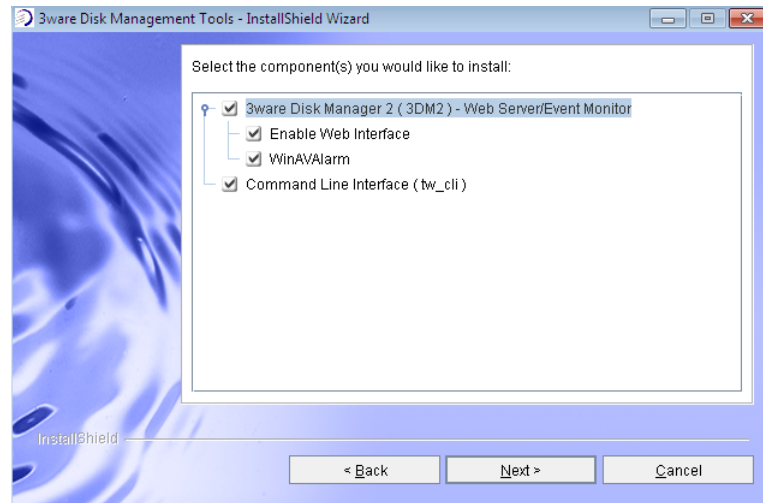


- 6 If you want to change where the 3ware Disk Management tools 3DM2 and CLI will be installed, you can change the path and directory. When you are ready, click **Next**.

Figure 131. Specify Directory Path Screen



- 7 Select what components you want to install and click **Next**. 3DM2 and CLI are applications that let you set up and manage RAID units.

Figure 132. Select Components to Install Screen

If you unselect **Enable Web Interface**, the 3DM2 web interface will not be enabled. In this case, an additional screen will display, that allows you to enable email notification. (If you do enable the web interface, you can enable this feature later, after 3DM2 has been installed.)

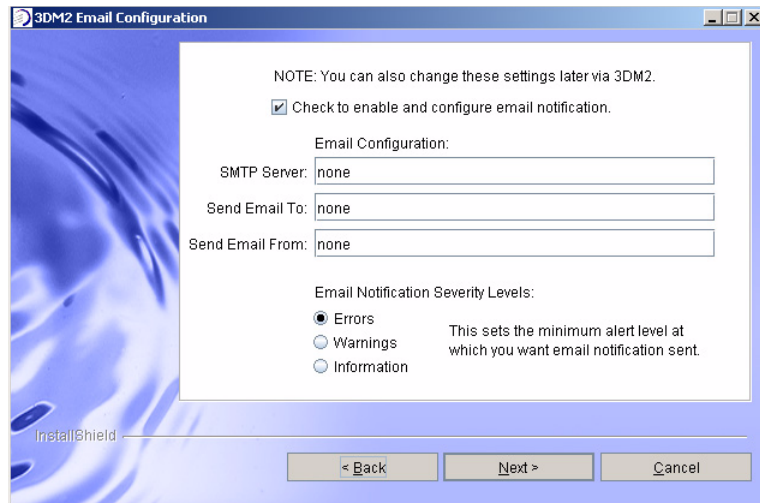
- 8 If you are prompted to configure email notification, check the box and complete the 3DM2 Email Configuration screen.

This features allows you to receive notification of problems with your 3ware RAID controller and units. For details about completing these fields, see “Managing E-mail Event Notification” on page 59.

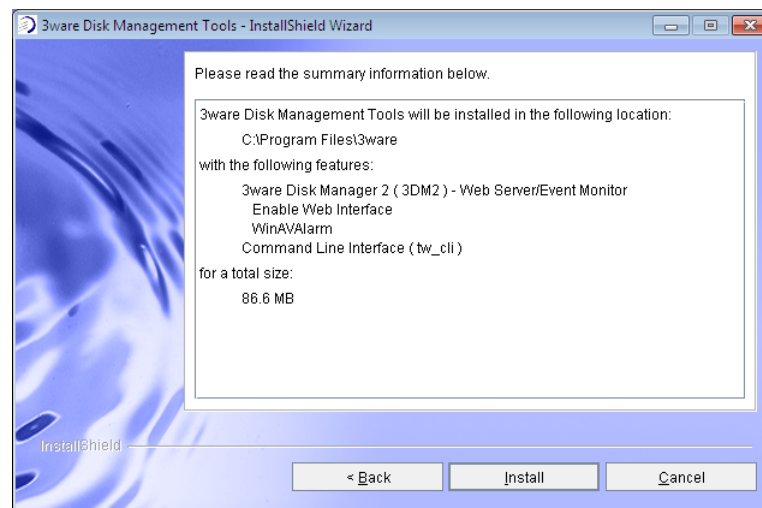
You can select what level of notifications you want to be emailed about.

- **Errors.** You will be notified of Errors only.
- **Warnings.** You will be notified of Warnings and Errors.
- **Information.** You will be notified of Information, Warnings, and Errors.

When you are ready, click **Next** to continue.

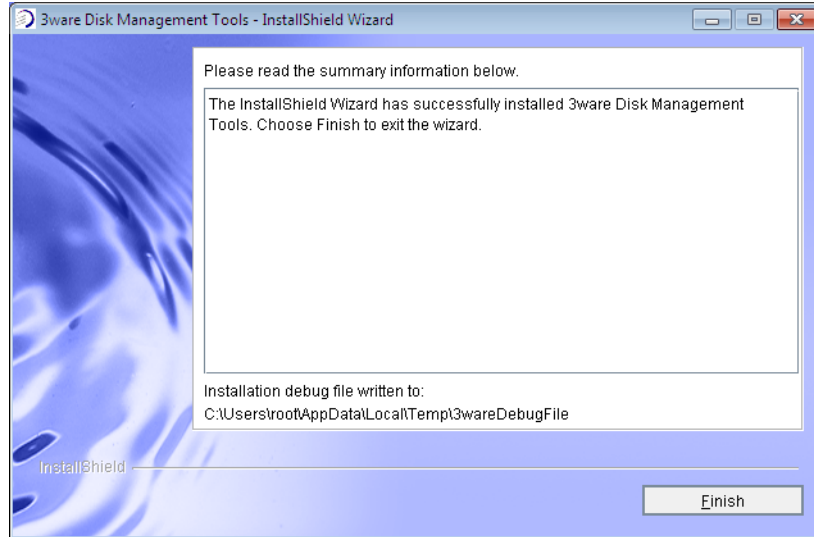
Figure 133. 3DM2 Email Configuration Screen

- 9 On the summary screen, review the installation that is about to occur. If you want to make changes, use **Back** to move back through the screens. When you are ready, click **Install** to continue.

Figure 134. Installation Summary Screen

- 10 When the final installation screen lets you know that installation is complete, click **Finish**.

Figure 135. Final Installation Screen



Uninstalling 3ware Software under Microsoft Windows

Use the **Add or Remove Programs** control panel to uninstall 3DM2.

- From the **Startup** menu, choose **Control Panels >> Add or Remove Programs**.
- In the Add or Remove Programs control panel, select **3ware Disk Management Tools** and click **Change/Remove**.

Compliance and Conformity Statements

This section is organized into the following topics:

- FCC Radio Frequency Interference Statement
- Canadian Compliance Statement
- European Community Conformity Statement

FCC Radio Frequency Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC (Federal Communications Commission) Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

To maintain compliance with FCC radio frequency emission limits, use shielded cables and connectors between all parts of the computer system. Changes or modification to the product may void the user's authority to operate this equipment.



Canadian Compliance Statement

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

European Community Conformity Statement

The Controller Models 9750-4i, 9750-8i, 9750-8e, 9750-4i4e, 9750-16i4e, and 9750-24i4e are in conformity with the following Common Technical Regulations and/or normative documents:

EN 55022 Limits and methods of measurements of radio interference characteristics of information technology equipment

EN 61000-4-2 Electromagnetic compatibility (EMC) Part 4: Testing and measurement techniques Section 2: Electrostatic discharge immunity test

EN 61000-4-3 Electromagnetic compatibility (EMC) Part 4: Testing and measurement techniques Section 3: Radiated, Radio-Frequency, Electromagnetic Field Immunity Test

EN 61000-4-4 Electromagnetic compatibility (EMC) Part 4: Testing and measurement techniques Section 4: Electrical fast transient/burst immunity test

EN 60950 Safety of information technology equipment, including electrical business equipment following the provisions of the Electromagnetic Compatibility Directive 89/23/EEC Low Voltage Directive



Warranty, Technical Support, and Service

This section is organized into the following topics:

- Limited Warranty
- Warranty Service and RMA Process
- LSI Technical Support and Services
- Sales and ordering information
- Feedback on this manual

Limited Warranty

RAID Controller Hardware. LSI warrants the 9750 product against defects in material and workmanship for a period of thirty-six (36) months from the date of original purchase. LSI, at no charge and at its option, will repair or replace any part of this product which proves defective by reason of improper workmanship or materials. Repair parts or replacement products will be provided by LSI on an exchange basis and will be either new or refurbished to be functionally equivalent to new. Products or parts replaced under this provision shall become the property of LSI.

Optional Battery Backup Unit (BBU) Hardware. 1-Year Hardware Warranty: LSI warrants this product against defects in material and workmanship for a period of twelve (12) months from the date of original purchase. LSI, at no charge and at its option, will repair or replace any part of this product which proves defective by reason of improper workmanship or materials. Repair parts or replacement products will be provided by LSI on an exchange basis and will be either new or refurbished to be functionally equivalent to new. Products or parts replaced under this provision shall become the property of LSI.

LSI warranty service is provided by returning the defective product to LSI.

Exclusions

This warranty does not cover any damage to this product which results from accident, abuse, misuse, natural or personal disaster, or any unauthorized disassembly, repair or modification. LSI shall not be liable for any incidental or consequential damages, including but not limited to loss of profits, other loss, damage or expense directly or indirectly arising from the customer's misuse of or inability to use the product, either separately or in combination with other equipment, regardless of whether LSI has been advised of the possibility of such damages. LSI is not liable for and does not cover under warranty, any costs associated with servicing and/or the installation of LSI products. This warranty sets for the entire liability and obligations of LSI with respect to breach of warranty and the warranties set forth or limited herein are the sole warranties and are in lieu of all other warranties, expressed or implied, including warranties or fitness for particular purpose and merchantability.

State Law Provisions

This warranty gives you specific legal rights and you may have other rights which vary from state to state. Some states do not allow the exclusion of incidental or consequential damages or allow limitation of implied warranties or their duration, so that the above exclusions or limitations may not apply.

Warranty Service and RMA Process

To obtain warranty service during the warranty period, contact Technical Support at <http://www.lsi.com/channel/ContactUs> and request a return authorization number.

You will be issued a return material authorization (RMA) number and other instructions for returning the controller. You can also explore options for expedited handling, status for "in process" RMAs and other policy information related to returns in general.

Please use the original packing material contents of the box when exchanging or returning a product.

For information about the status of a replacement, please contact LSI Technical Support.

LSI Technical Support and Services

For the latest information related to 3ware RAID controllers, refer to the following LSI web sites:

- Product information, compatibility lists, software upgrades, and OS driver downloads, refer to:

<http://www.lsi.com/channel/ChannelDownloads>.

From the Product Family drop-down, select *RAID Controllers*. Then in the Product list on the right, select your product, for example *3ware SAS 9750-8i*.

- 3ware KnowledgeBase, including frequently asked questions (FAQs) at <http://kb.lsi.com>.
- Product compatibility and interoperability lists can also be found at: http://www.lsi.com/channel/support/marketing_resources.

On the Marketing Resource Center page, select the *Data & Interoperability* tab.

- For specific answers to questions, technical support, or to give feedback about the product, refer to our website at: <http://www.lsi.com/channel/ContactUS>.

LSI also offers support 24 hours a day, 7 days a week at: 888-646-4566 or 408-433-4567 in North America. For international customers call 00-800-5745-6442.

For the latest LSI news and support updates or tweets sign up on our Twitter account at: <http://www.twitter.com/LSISupport>.

Sales and ordering information

For sales inquiries, visit <http://www.lsi.com/channel/ContactUs>

Feedback on this manual

Your feedback is welcome. If anything in the guide seems unclear please let us know. Please send an email to support1@lsi.com.

Index

Numerics

2TB support 71

3BM

- help 43
- main screen 37
- navigation 38
- screens 37
- working in 38

3BM2

- starting 34

3DM2

- 3DM2 menus 52
- Alarms page 217
- Battery Backup Information page 218
- browser requirements 45
- Controller Details page 191
- Controller Settings page 200
- Controller Summary page 190
- Disk Management Utility Overview 44
- Drive Details page 197
- Drive Information page 195
- enabling remote access 61
- Enclosure Details page (3DM2) 221
- Enclosure Summary page (3DM2) 220
- installation 301
- main 3DM2 screen 52
- Maintenance page 208
- managing email event notification 59
- page refresh frequency 62
- passwords 58
- preferences 58
- problems 234
- remote access, enabling 61
- Scheduling page 205
- setting listening port number 62
- Settings page 224
- starting 45
- starting in Linux 49
- uninstalling 3DM2 on
 - Windows 354
- Unit Details page 193
- Unit Information page 192

3ware HTML Bookshelf xi

A

A-Chip

definition 294

active content in the 3ware HTML Bookshelf,
security message about xii

Advanced Content Streaming 2

AEN

- All RAID keys failed validation (0080) 279
- Backup DCB read error detected (0043) 266
- Battery capacity is below error level (0059) 275
- Battery capacity is below warning level (0058) 274
- Battery capacity test completed (0050) 272
- Battery capacity test is overdue (0053) 273
- Battery capacity test started (004E) 271
- Battery charging completed (0056) 273
- Battery charging fault (0057) 274
- Battery charging started (0055) 273
- Battery is not present (005B) 275
- Battery is present (005A) 275
- Battery is weak (005C) 276
- Battery temperature is high (004B) 270
- Battery temperature is low (004A) 269
- Battery temperature is normal (0049) 269
- Battery temperature is too high (004D) 271
- Battery temperature is too low (004C) 270
- Battery voltage is high (0046) 268
- Battery voltage is low (0045) 267
- Battery voltage is normal (0044) 267
- Battery voltage is too high (0048) 268
- Battery voltage is too low (0047) 268
- Buffer ECC error corrected (0039) 262
- Buffer integrity test failed (0024) 251
- Cache flush failed, some data lost (0025) 251
- Cache synchronization completed (005E) 276
- Cache synchronization failed 276
- Cache synchronization skipped (004F) 272
- Controller error occurred (0003) 241
- Controller reset occurred (1001) 240
- DCB checksum error detected(0027) 253
- DCB version unsupported (0028) 253
- Degraded unit (0002) 240
- Downgrade UDMA (0021) 249
- Drive ECC error reported (0026) 252
- Drive error detected (000A) 244
- Drive inserted (001A) 247
- Drive not supported (0030) 258
- Drive power on reset detected (003A) 262
- Drive removed (0019) 247
- Drive timeout detected (0009) 244
- Drive write fault 278
- Enclosure added (0063) 277

Enclosure audio alarm activated but mute (8047) 291

Enclosure audio alarm added (804A) 292

Enclosure audio alarm failed (8048) 291

Enclosure audio alarm removed (8049) 292

Enclosure audio alarm status unknown (804B) 292

Enclosure current normal (8044) 290

Enclosure current over (8045) 290

Enclosure current unknown (8046) 291

Enclosure fan added (8003) 281

Enclosure fan error (8001) 280

Enclosure fan normal (8000) 279

Enclosure fan off (8005) 281

Enclosure fan removed (8002) 280

Enclosure fan unknown (8004) 281

Enclosure power added (8033) 287

Enclosure power fail (8031) 286

Enclosure power normal (8030) 286

Enclosure power off (8037) 288

Enclosure power removed (8032) 287

Enclosure power unknown (8034) 287

Enclosure removed (0062) 277

Enclosure temp above operating (8024) 284

Enclosure temp added (8026) 284

Enclosure temp below operating (8023) 283

Enclosure temp critical (8027) 285

Enclosure temp high (8022) 283

Enclosure temp low (8021) 282

Enclosure temp normal (8020) 282

Enclosure temp removed (8025) 284

Enclosure temp unknown (8028) 285

Enclosure voltage normal (8040) 288

Enclosure voltage over (8041) 289

Enclosure voltage under (8042) 289

Enclosure voltage unknown (8043) 289

Flash file system error detected (003F) 265

Flash file system repaired (0040) 265

Incomplete unit detected (0006) 242

Initialize completed (0007) 243

Initialize failed (000E) 246

Initialize paused (003C) 263

Initialize started (000C) 245

Local link down (0065) 278

Local link up (0064) 277

Migration completed (0035) 260

Migration failed (0034) 259

Migration paused (003E) 264

Migration started (0033) 259

Primary DCB read error occurred (0042) 266

RAID key not found (0081) 279

Rebuild completed (0005) 242

Rebuild failed (0004) 241

Rebuild paused (003B) 263

Rebuild started (000B) 245

Replacement drive capacity too small (002E) 257

Reverted to emergency recovery firmware (0066) 278

Sector repair completed (0023) 250

SO-DIMM not compatible (0037) 261

SO-DIMM not detected (0038) 261

Source drive ECC error overwritten(002C) 256

Source drive error occurred(002D) 256

Spare capacity too small for some units (0032) 259

Unclean shutdown detected (0008) 243

Unit inoperable (001E) 248

Unit number assignments lost (0041) 266

Unit Operational (001F) 249

Upgrade UDMA mode (0022) 250

Verify completed(002B) 255

Verify failed (002A) 254

Verify fixed data/parity mismatch (0036) 260

Verify not started, unit never initialized (002F) 257

Verify paused (003D) 264

Verify started (0029) 254

AEN messages 141, 217, 235

alarms 141

- alert utility (WinAVAlarm) 142
- viewing 141

Alarms page, 3DM2 217

alert utility (WinAVAlarm) 142

All RAID keys failed validation (0080) 279

arrays 5

- array roaming 6, 125, 127
- definition 294
- definition 294
- moving from one controller to another 127
- removing in 3DM2 125

asterisk next to unit 193, 194

Auto Rebuild policy 15, 67

- setting 71, 203

Auto Verify policy for units 202

- setting (3DM2) 107

auto-carving 71

- auto-carving policy 68

auto-carving policy

- setting 204

available drives, 3DM2 214

B

background initialization after power failure 149

background tasks

- background rebuild rate (definition) 294
- background task mode 159, 201
- background task mode, setting 162
- background task rate 201
- background task rate, setting 162
- definition 16
- initialization 146
- overview 145
- prioritizing 163

- rebuilding a unit 154
- relationship of task mode and task rate 160
- scheduling 163
- verification 149
- Backup DCB read error detected (0043) 266
- Basic read cache mode 104
- Battery capacity is below error level (0059) 275
- Battery capacity is below warning level (0058) 274
- Battery capacity test completed (0050) 272
- Battery capacity test is overdue (0053) 273
- Battery capacity test started (004E) 271
- Battery charging completed (0056) 273
- Battery charging fault (0057) 274
- Battery charging started (0055) 273
- Battery is not present (005B) 275
- Battery is present (005A) 275
- Battery is weak (005C) 276
- Battery temperature is high (004B) 270
- Battery temperature is low (004A) 269
- Battery temperature is normal (0049) 269
- Battery temperature is too high (004D) 271
- Battery temperature is too low (004C) 270
- Battery voltage is high (0046) 268
- Battery voltage is low (0045) 267
- Battery voltage is normal (0044) 267
- Battery voltage is too high (0048) 268
- Battery voltage is too low (0047) 268
- BBU
 - Battery Backup Information page 218
 - testing battery capacity 176
 - viewing battery information 176
- BIOS
 - showing version 191
- BIOS Manager, using 34
- blinking LEDs
 - to locate drives 139
 - to locate enclosure components 184
- blinking LEDs (drive locate) 193, 196, 223
- Boot volume size
 - definition 294
- boot volume size, specifying 81
- bootable unit, specifying 38
- browser requirements, 3DM2 45
- Buffer ECC error corrected (0039) 262
- Buffer integrity test failed (0024) 251

C

- Cache flush failed, some data lost (0025) 251
- Cache synchronization completed (005E) 276
- Cache synchronization failed 276
- Cache synchronization skipped (004F) 272
- cancel rebuild 159
- carve size 68
 - setting 74, 204
- certificate message when starting 3DM2 46
- CLI
 - definition 295
 - installation 301
- Command Logging
 - enabling or disabling 226
- Compliance and Conformity 355
- configuration
 - changing 115
 - controller 65
 - definition 295
 - exit and save modifications 36
 - exit without saving 37
 - unit 79
- configuring
 - a controller 65
 - units 79
- configuring units
 - first time, in BIOS 18
- Continue on Source Error During Rebuild
 - setting as a unit policy 108
- controller
 - controller ID number (definition) 295
 - controller information, viewing 65
 - controller policies
 - overview 67
 - viewing 69
 - definition 295
 - moving unit to another 127
 - rescanning 132
 - status 190
 - updating driver
 - Red Hat 321
 - SuSE 323
 - Windows 348
 - updating firmware 174
- Controller Board Selection screen (3BM2) 20
- Controller Details page, 3DM2 191
- controller details, 3BM 67
- Controller error occurred (0003) 241
- Controller Information screen (3BM) 67
- Controller Phy Information page (3BM) 76
- Controller Phy Policies page 78
- Controller Phy Policies page (3BM) 78
- Controller Phy Summary page (3DM2) 77, 199
- Controller reset occurred (0001) 240
- Controller Settings page, 3DM2 200
- Controller Summary page, 3DM2 190
- conventions
 - in the user guide x
- creating a unit
 - 3BM 85
 - basic steps 18
 - configuration options 79
 - definition 295
 - first time, in BIOS 18

- in 3DM2 83
- introduction 79
- current controller (definition) 55
- customer support
 - contacting 228, 358
- D**
- DCB checksum error detected (0027) 253
- DCB version unsupported (0028) 253
- DCB, definition 295
- default settings
 - policies and background tasks 32
- Degraded (unit status) 138
- degraded unit
 - about 138
 - definition 295
- Degraded unit (0002) 240
- delay between spin-up policy (viewing in 3DM2) 204
- deleting a unit 121, 122
 - 3DM2 213
 - definition 295
- deleting a unit in 3BM 124
- destroy unit (definition) 295
- diagnostic log
 - downloading 188
 - for enclosures 188
- disk arrays 37
- Disk Manager, using 44
- distributed parity 6
- Downgrade UDMA mode (0021) 249
- downloading
 - driver and firmware 172
- drive
 - adding in 3DM2 129
 - capacity considerations 13
 - checking status in 3DM2 133
 - coercion 13
 - drive ID (definition) 295
 - drive number (definition) 296
 - locate by blinking 139
 - removing in 3DM2 130
 - status, viewing (3DM2) 133
 - statuses 138
 - types 3
 - viewing SMART data 144
- Drive Details page, 3DM2 197
- Drive ECC error reported (0026) 252
- Drive error detected (000A) 244
- Drive Information page (3BM) 136
- Drive Information page (3DM2) 135
- Drive Information page, 3DM2 195
- Drive inserted (001A) 247
- drive locate 193, 196, 223
- Drive not supported (0030) 258
- drive performance monitoring

- definition 15
- using 229
- Drive power on reset detected (003A) 262
- Drive removed (0019) 247
- drive requirements 3
- Drive timeout detected (0009) 244
- Drive write fault 278
- driver
 - compiling for Linux 321
 - current version, determining 170
 - downloading 172
 - installation under FreeBSD 301
 - installation under Linux 310
 - installation under Mac OS 325
 - installation under OpenSolaris 331
 - installation under VMware 338
 - installation under VMware ESX 3.x 338
 - installation under Windows 343
 - installation utility for Windows 346, 348
 - updating
 - Red Hat 321
 - SuSE 323
 - Windows 348
- driver diskette
 - creating (Linux) 312
 - creating (Windows) 344
- drives
 - viewing a list of 135
- drives per spin-up policy 204
- dynamic sector repair 151, 250

- E**
- ECC
 - definition 296
 - ECC error policy (definition) 296
- e-mail event notification, managing in 3DM2 59, 225
- Enclosure added (0063) 277
- Enclosure audio alarm activated but mute (8047) 291
- Enclosure audio alarm added (804A) 292
- Enclosure audio alarm failed (8048) 291
- Enclosure audio alarm removed (8049) 292
- Enclosure audio alarm status unknown (804B) 292
- Enclosure current normal (8044) 290
- Enclosure current over (8045) 290
- Enclosure current unknown (8046) 291
- Enclosure Details page (3DM2) 221
- Enclosure fan added (8003) 281
- Enclosure fan error (8001) 280
- Enclosure fan normal (8000) 279
- Enclosure fan off (8005) 281
- Enclosure fan removed (8002) 280
- Enclosure fan unknown (8004) 281
- Enclosure Information page (3BM) 181
- Enclosure power added (8033) 287
- Enclosure power fail (8031) 286

-
- Enclosure power normal (8030) 286
 - Enclosure power off (8037) 288
 - Enclosure power removed (8032) 287
 - Enclosure power unknown (8034) 287
 - Enclosure removed (0062) 277
 - enclosure status indicators 136
 - Enclosure Summary page (3DM2) 220
 - Enclosure temp above operating (8024) 284
 - Enclosure temp added (8026) 284
 - Enclosure temp below operating (8023) 283
 - Enclosure temp critical (8027) 285
 - Enclosure temp high (8022) 283
 - Enclosure temp low (8021) 282
 - Enclosure temp normal (8020) 282
 - Enclosure temp removed (8025) 284
 - Enclosure temp unknown (8028) 285
 - Enclosure voltage normal (8040) 288
 - Enclosure voltage over (8041) 289
 - Enclosure voltage under (8042) 289
 - Enclosure voltage unknown (8043) 289
 - enclosures
 - blinking LEDs for components 184
 - blinking LEDs for drives 139
 - checking status of components (fans, temperature sensors, power supplies) 181
 - detail information 221
 - downloading a diagnostic log 188
 - enclosure (definition) 296
 - enclosure management features 179
 - enclosure requirements 4
 - Enclosure Services, defined 15
 - LED status indicators 136
 - locating a component (fan, temperature sensor, power supply) 184
 - summary information 220
 - viewing a list of 180
 - errors 141
 - error log, downloading 144
 - error messages 235
 - how handled by verification process 151
 - viewing 144
 - European Community Conformity statement 356
 - events (see also errors and alarms) 141
 - expander (definition) 296
 - export a unit
 - definition 296
 - export unconfigured disks (policy) 68
 - F**
 - fan
 - checking status 181
 - possible statuses 183
 - summary 222
 - fault tolerant
 - definition 296
 - FCC Radio Frequency Interference Statement 355
 - firmware
 - definition 296
 - downloading 172
 - showing version 190, 191
 - updating 174
 - Flash file system error detected (003F) 265
 - Flash file system repaired (0040) 265
 - FreeBSD driver
 - installation 301
 - FUA (Force Unit Access) commands, part of StorSave profile 111
 - G**
 - grown defect, definition 296
 - H**
 - hardware installation, troubleshooting 232
 - help, getting for 3BM 43
 - hot spare 11
 - creating 97, 98
 - hot spare (definition) 296
 - specifying 26
 - hot swap 6
 - hot swap (definition) 296
 - HTTP port number for 3DM2 226
 - I**
 - identify
 - drive by blinking LED 193, 196
 - enclosure components by blinking 184
 - identify checkbox in 3DM2 193, 196
 - slot by blinking LED 223
 - identify checkbox in 3DM2 223
 - import a unit
 - definition 296
 - incomplete drives 121
 - incomplete drives, deleting through 3BM 124
 - Incomplete unit detected (0006) 242
 - initialization
 - about 146
 - background initialization after power failure 149
 - background versus foreground 146
 - definition 297
 - RAID 0 units 147
 - RAID 1 units 148
 - RAID 10 units 148
 - RAID 5 units 147
 - RAID 50 units 147
 - selecting method (foreground or background) to use for new unit (3BM) 81
 - Initialize completed (0007) 243
 - Initialize failed (000E) 246
 - Initialize paused (003C) 263
 - Initialize started (000C) 245

Initializing (unit status) 137
Inoperable (unit status) 138
inoperable units (about) 139
installation
 disk management tools (3DM2 and CLI)
 installation 301
 driver utility for Windows 346, 348
 of controller 28, 30
 overview 18
 troubleshooting
 hardware 232
 software 232
Intelligent Mode (read cache) 104
Intelligent Read Prefetch (IRP), a read cache mode
 setting 104

J

JBOD policy 68

L

latency, and how to minimize 159
LEDs
 colors and behavior 136
 indicators 136
Link Control (Phy) 199
link speed
 changing for a phy 77
Linux driver
 compiling 321
 installation 310
 updating 321, 323
listening port for 3DM2 226
listening port number, 3DM2 62
Load Control 41
Local link down (0065) 278
Local link up (0064) 277
locating
 drives 139
 enclosure components 184
logging in to 3DM2 46
logical unit
 definition 297

M

Mac OS driver
 installation 325
main screen, 3BM 37
main screen, 3DM2 52
maintaining units 133
Maintenance page, 3DM2 208
media scans 16
 (verification of non-redundant units) 150
menus, 3DM2 52
message url http://opensolaris.org/os/community/documentation/doc_index/sysadmin/ 97

messages, error 235
Migrate-Paused (unit status) 138
Migrating (unit status) 137
migrating a unit 116, 212
 definition 297
Migration completed (0035) 260
Migration failed (0034) 259
Migration paused (003E) 264
Migration started (0033) 259
mirrored disk array
 definition 5, 297
 RAID 1 7
motherboard boot sequence 27
motherboard requirements 3
Multi LUN support (auto-carving) 68, 71
multiple volumes in one unit 71

N

name of unit 80, 193
 assigning 99, 203
navigation, 3BM 38
NCQ (native command queuing)
 definition 297
 NCQ policy 203
non-redundant units
 definition 297

O

Online Capacity Expansion (OCE), definition 297
OpenSolaris driver
 installation 331
operating systems
 informing of changed configuration 119
operating systems supported 4
Other Controller Settings, 3DM2 203

P

page refresh
 3DM2 226
 frequency, 3DM2 62
parity
 definition 297
 distributed 6
partitioning and formatting units 90
passwords, 3DM2 58, 225
PCB (definition) 297
P-Chip (definition) 298
phy
 changing the link speed 77
 Controller Phy Information page (3BM) 76
 Controller Phy Policies page (3BM) 78
 Controller Phy Summary page (3DM2) 75, 77, 199
 link speed, changing 77

- phy (definition) 298
- phy identifier (definition) 298
- seeing a list of 75
- viewing information about 75
- policies
 - controller 67
 - initial settings 31
 - unit 100
 - units 201
- port
 - definition 298
- port ID (definition) 298
- power supply
 - checking status 181
 - possible statuses 183
- preferences, 3DM2 58
- Primary DCB read error occurred (0042) 266

Q

- queuing
 - enabling and disabling for a unit 110
 - Queuing policy (setting in 3DM2) 203
- queuing (definition) 298

R

- RAID
 - concepts and levels 5
 - configurations 6
 - determining level to use 12
 - RAID 0 6
 - RAID 1 7
 - RAID 10 9
 - RAID 5 7
 - RAID 50 10
 - RAID 6 8
- RAID key not found (0081) 279
- RAID Level Migration (RLM)
 - changing level 117
 - definition 299
 - overview 116
- Rapid RAID Recovery 113
 - enabling or disabling 114
 - enabling or disabling (3BM) 115
 - enabling or disabling (3DM2) 114
- read cache policy 201
 - Basic Mode versus Intelligent Mode 104
 - changing 105
 - setting in 3DM2 104
- Rebuild completed (0005) 242
- Rebuild failed (0004) 241
- Rebuild paused (003B) 263
- Rebuild started (000B) 245
- rebuild task schedule
 - adding a time slot (3DM) 167
 - removing a time slot (3DM2) 167

- viewing (3DM2) 165
- rebuild task schedule (definition) 298
- Rebuilding (unit status) 137
- rebuilding a unit
 - 3BM 156
 - 3DM 155
 - 3DM2 155, 211
 - about 154
 - cancelling and restarting 159
 - definition 298
 - introduction 154
- Rebuild-Paused (unit status) 137, 212
- redundancy
 - definition 299
- redundant units, about 150
- remote access
 - 3DM2 226
 - enabling in 3DM2 61
 - remote viewing of controllers through 3DM2 51
- removing a drive 130
 - 3DM2 210
 - definition 299
- removing a unit 213
 - definition 299
- Replacement drive capacity too small (002E) 257
- rescan controller 132, 208
- Reverted to emergency recovery firmware (0066) 278
- roaming, array 125, 127

S

- S.M.A.R.T data 197
- SAS
 - definition 299
 - SAS address (definition) 299
 - SAS device (definition) 299
 - SAS domain (definition) 299
- SAS Address 199
- scheduled background tasks 16
- scheduling
 - background tasks 163
 - prioritizing background tasks 163
 - selecting basic or advanced verify schedule (3DM2) 166
 - task duration 164
- Scheduling page, 3DM2 205
- Sector repair completed (0023) 250
- security certificate when starting 3DM2 46
- security message related to active content in the 3ware HTML Bookshelf xii
- self-tests
 - about 168, 207
 - definition 299
 - schedule, adding (3DM) 167
 - schedule, removing (3DM2) 167
 - selecting 168

- self-tests schedule
 - viewing (3DM2) 165
- serial number
 - showing 190, 191
- SES (definition) 299
- Settings page, 3DM2 224
- single disk 11
- slot requirements 3
- slot summary (on enclosure) 184
- SMART 141
 - data, viewing 144
 - monitoring 16
- SO-DIMM not compatible (0037) 261
- SO-DIMM not detected (0038) 261
- software installation 301
- software installation, troubleshooting 232
- some data lost (005F) 276
- some data lost (0070) 278
- Source drive ECC error overwritten (002C) 256
- Source drive error occurred (002D) 256
- Spare capacity is too small for some units (0032) 259
- spin-up policy
 - delay between spin-ups (viewing in 3DM2) 204
 - number of drives 204
- stagger time (definition) 299
- staggered method 68
- staggered spin-up 16, 68, 74
- starting 3BM2 34
- starting 3DM2 45
 - under Linux 49
- status
 - controller, viewing (3DM2) 190
 - definitions
 - controller 190
 - drive 138
 - unit 137
 - drive, viewing (3DM2) 133
 - status LEDs 136
 - unit, viewing (3DM2) 133
- StorSave profile 16
 - setting 111, 203
- stripe size
 - changing 115
 - definition 299
- striping 5
 - definition 300
- subunit
 - definition 300
- system requirements 3
 - drive requirements 3
 - enclosure requirements 4
 - motherboard and slot 3
 - operating systems 4
 - other requirements 4

T

- task schedules
 - about, 3DM2 206
 - adding a time slot 167
 - rebuild/migrate 167
 - removing a time slot 167
 - self-test 167
 - task duration 164
 - turning on and off 165
 - verify 167
 - viewing 165
- technical support 357
 - contacting 228, 358
- temperature sensor
 - checking status 181
 - possible statuses 183
- troubleshooting 227
 - 3DM2 234
 - hardware installation 232
 - software installation 232
- TwinStor 9

U

- ultra DMA protocol 249
- Unclean shutdown detected (0008) 243
- unconfigured drives
 - making visible to operating system 27
- uninstalling 3DM2 330
- uninstalling 3DM2 on
 - Windows 354
- unit
 - checking status in 3DM2 133
 - configuring 79
 - creating a unit
 - in 3DM2 83
 - introduction 79
 - creating a unit for the first time, in BIOS 18
 - creating in 3BM 85
 - definition 5, 300
 - deleting a unit 121
 - in 3BM 124
 - in 3DM2 121, 122
 - expanding capacity 118
 - maintaining 133
 - moving from one controller to another 127
 - name 193, 203
 - naming 80, 99
 - ordering in 3BM 89
 - partitioning and formatting 90
 - policies, setting 100, 201
 - read cache policy, 3DM2 201
 - read cache policy, working with 104
 - rebuilding a unit 154
 - in 3BM 156
 - in 3DM 155

- in 3DM2 155
- removing in 3DM2 125
- statuses 137
- Unit Maintenance in 3DM2 209
- unit number (definition) 300
- unit statuses 137
- verifying a unit 152
 - in 3BM 153
 - in 3DM 153
- volumes 194
- write cache, 3DM2 201
- write cache, enabling and disabling 102
- Unit Details page, 3DM2 193
- unit ID
 - definition 300
- Unit Information page, 3DM2 192
- Unit inoperable (001E) 248
- Unit number assignments lost (0041) 266
- Unit Operational (001F) 249
- unit policies
 - enabling and disabling queuing for a unit 110
 - enabling and disabling write cache 102
 - overview 100
 - setting Auto Verify 107
 - setting Continue on Source Error During Rebuild 108
 - setting read cache 104
 - setting the StorSave policy 111
- Unsupported DCB, indication on drive 121, 124
- updating firmware 174
- Upgrade UDMA mode (0022) 250

V

- verification
 - about 149
 - error handling 151
 - media scans 150
 - non-redundant units 150
 - redundant units 150
- Verify completed(002B) 255
- Verify failed (002A) 254
- Verify fixed data/parity mismatch (0036) 260
- Verify not started, unit never initialized (002F) 257
- Verify paused (003D) 264
- verify schedule
 - adding a time slot (3DM) 167
 - removing a time slot (3DM) 167
 - selecting basic or advanced (3DM2) 166
 - viewing (3DM2) 165
- Verify started (0029) 254
- verifying
 - definition 300
- Verifying (unit status) 137
- verifying a unit 152, 153, 211
 - Auto Verify policy 107

- manually 152
 - stopping (3DM2) 153
- Verify-Paused (unit status) 137, 211
- viewing 3DM2 remotely 51
- VMware driver
 - installation 338
- volume
 - specifying a boot volume size 81
- volumes
 - in a unit 194
 - multiple from one unit 71
 - resulting from auto-carvings 194
- vport (definition) 300

W

- Warranty 357
- wide port (definition) 300
- WinAVAlarm 142
- Windows alert utility (WinAVAlarm) 142
- working in 3BM 38
- write cache 17, 201
 - disable on degrade, part of Storsave profile 112
 - enabling in 3BM 103
 - enabling in 3DM2 102
- write journaling, part of StorSave profile 112
- WWN (World Wide Number) (definition) 300