**Introduction**

The MegaRAID® Storage Manager™ software enables you to configure, monitor, and maintain storage configurations on the LSISAS controllers and all the storage-related devices connected to them. The MegaRAID Storage Manager graphical user interface makes it easy for you to create and manage storage configurations. Select the following topics to learn more about the MegaRAID Storage Manager software:

- Configuration
- Monitoring
- Maintenance
- Hardware Requirements

**Configuration**

The MegaRAID Storage Manager software enables you to configure the controllers, drives, battery backup units, and other storage-related devices installed on a server or on a workstation. The configuration utility simplifies the process of creating drive groups and virtual drives and allows you to easily create new storage configurations and modify the configurations. For more information, see the Configuration topic.

You can create configurations using the following modes:

- **Simple configuration** specifies a limited number of settings and has the system select drives for you. This option is the easiest way to create a virtual drive.

- **Advanced configuration** lets you choose additional settings and customize the creation of virtual drives. This option provides greater flexibility when creating virtual drives for your specific requirements because you can select the drives and the virtual drive settings when you create a virtual drive. In addition, you can use the advanced configuration procedure to create spanned drive groups.

The Modify Drive Group Wizard enables you to increase the capacity of a virtual drive and to change the RAID level of a drive group.

**Note:** The Modify Drive Group Wizard was previously known as the Reconstruction Wizard.

**Monitoring**

The MegaRAID Storage Manager software displays the status of virtual drives, physical drives, and other storage devices on the workstation or on the servers that you are monitoring. The system errors and the events are recorded in an event log file and are displayed on the screen. Special device icons appear on the screen to notify you of drive failures and other situations that require immediate attention. For more information, see the Monitoring Controllers and Its Attached Devices topic.
Maintenance

You can use the MegaRAID Storage Manager software to easily perform system maintenance tasks, such as running patrol read operations, upgrading firmware, and running consistency checks on drive groups that support redundancy. For more information, see the Maintaining and Managing Storage Configurations topic.

Hardware Requirements

The hardware requirements for the MegaRAID Storage Manager software are as follows:

- PC-compatible computer with an IA-32 (32-bit) Intel Architecture processor or an EM64T (64-bit) processor; also compatible with SPARC V9 architecture-based systems
- Minimum 256 MB of system memory (512 MB recommended)
- Drive with at least 400 MB of free space available; Solaris 10 SPARC requires a minimum of 640 MB

The supported operating systems for the MegaRAID Storage Manager software are as follows:

- Red Hat Linux 3.0, 4.0, 5.0, and 6.0
- Solaris 10 x86, SPARC
- SuSE Linux/SLES 9, 10, and 11, with the latest updates and service packs
- VMware ESX 3.5 and above

Refer to your server documentation and to the operating system (OS) documentation for more information on hardware and operating system requirements.
Installation

You can install the MegaRAID® Storage Manager™ software on systems running the following operating systems:

- Red Hat Linux 3.0, 4.0, 5.0, and 6.0
- Solaris™ 10 x86, Solaris SPARC
- SuSE Linux/SLES 9, 10, and 11, with latest updates and service packs
- VMware ESX 3.5 and above

Refer to your server documentation and to the operating system documentation for more information on hardware and operating system requirements.

You can use the MegaRAID Storage Manager software to remotely monitor the systems running the VMware ESXi (3.5 and above) operating system.

**Note:** Storelib libraries need the capability to be installed with more than one version. All the storelib libraries have been moved to a private location. Please do a clean un-installation and only then install the MegaRAID Software Manager to avoid any conflicts.

Select the following topics for additional information on installation:

- Installing MegaRAID Storage Manager Software on Microsoft Windows
- Installing MegaRAID Storage Manager Software on RHEL or SLES/SuSE Linux
- Installing and Supporting MegaRAID Storage Manager Software on Solaris 10U5, U6, U7, and U8 (Both x86 and x64)
- MegaRAID Storage Manager Software Customization
- Uninstalling MegaRAID Storage Manager Software on Linux
- Installing and Supporting MegaRAID Storage Manager Software on VMware
- Uninstalling MegaRAID Storage Manager Software

In addition, you can install and configure a Simple Network Management Protocol (SNMP) Agent. For more details, refer to **Installing and Configuring an SNMP Agent.**

**Installing MegaRAID Storage Manager Software on Microsoft Windows**

To install the MegaRAID Storage Manager software on a Microsoft® Windows® Server 2003, Microsoft Windows Server 2008, Microsoft Server 2008R2, Microsoft Windows XP, Microsoft Windows Vista, or Microsoft Windows 7 operating system, follow these steps:

1. Insert the MegaRAID Storage Manager software installation CD in the CD-ROM drive.
   
   If necessary, find and double-click the `setup.exe` file to start the installation program.

2. In the Welcome screen that appears, click **Next.**
   
   If the MegaRAID Storage Manager software is already installed on this system, an upgraded installation occurs.
3. Read and accept the user license and click Next.
   The Customer Information screen appears.

4. Enter your user name and the organization name. In the bottom part of the screen, select an installation option:
   – If you select All users, any user with administrative privileges can use this installation of the MegaRAID Storage Manager software to view or change storage configurations.
   – If you select Only for current user, the MegaRAID Storage Manager short-cuts and associated icons will be available only to the user with this username.

5. Click Next to continue.

6. On the next screen, accept the default Destination Folder, or click Change to select a different destination folder.

7. Click Next to continue.
   The Setup Type screen appears.

8. Select one of the setup options. The options are fully explained in the screen text.
   – Typically, you would select Complete if you are installing the MegaRAID Storage Manager software on a server.
   – Select Custom Installation if you want to select individual program components.

9. Click Next to continue.
   If you select Custom Installation as your setup option, the second Setup Type screen appears.

10. Select one of the custom setup options. The options are fully explained in the screen text.
    – Select the Client radio button if you are installing the MegaRAID Storage Manager software on a computer that will be used to view and configure servers over a network. To begin installation, click Install on the next screen that appears.
      In the Client mode of installation, the MegaRAID Storage Manager software installs only the client-related components, such as the MegaRAID Storage Manager GUI and the monitor configurator. Use the Client mode if you want to manage and monitor servers remotely. When you install the MegaRAID Storage Manager software in a Client mode on a laptop or on a desktop, you can log in to a specific server by providing the IP address.
    – Select the Server radio button to install only those components required for remote server management. To begin installation, click Install on the next screen that appears.
    – Select the StandAlone radio button if you will use the MegaRAID Storage Manager software to create and manage storage configurations on a stand-alone workstation. To begin installation, click Install on the next screen that appears.
    – Select the Local radio button if you want to view only the workstation that has the MegaRAID Storage Manager software installed. You will not be able to discover other remote servers and other remote servers will also not be able to connect to your workstation. In a local mode installation, you will be using the loopback address instead of the IP address.
    – Select the Custom radio button if you want to specify individual program features to install.
If you select **Custom**, a window listing the installation features appears. Select the features you want on this screen.

11. Click **Next** to proceed.

12. Click **Install** to install the program.

13. In the final Configuration Wizard screen, click **Finish** to complete the installation process.

If you select the **Client** installation for a computer used to monitor servers and if there are no available servers with a registered framework on the local subnet (that is, servers with a complete installation of MegaRAID Storage Manager software), the server screen appears. The server screen does not list any servers. You can use this screen to manage systems remotely.

**Prerequisites for Installing MegaRAID Storage Manager Software on RHEL6.0 RC1 x64 Operating System**

Before installing the MegaRAID Storage Manager software on the RHEL6.0 x64 system, install the following RPMs. Without these files/RPMs, the MegaRAID Storage Manager software may not be installed properly or may not work as expected.

- `libstdc++-4.4.4-13.el6.i686.rpm`
- `compat-libstdc++-33-3.2.3-69.i686.rpm`
- `libXau-1.0.5-1.el6.i686.rpm`
- `libxcb-1.5-1.el6.i686.rpm`
- `libX11-1.3-2.el6.i686.rpm`
- `libXext-1.1-3.el6.i686.rpm`
- `libXi-1.3-3.el6.i686.rpm`
- `libXtst-1.0.99.2-3.el6.i686.rpm`

The RHEL6.0 RC1 complete operating system installation is required for the MegaRAID Storage Manager software to work. The above mentioned rpm's come as part of RHEL6 RC1 Operating System DVD. These RPM's may need additional dependent RPM's as well. All the dependent RPM's also must be installed on the target system.

**Installing MegaRAID Storage Manager Software on RHEL or SLES/SuSE Linux**

To install MegaRAID Storage Manager software on a system running Red Hat Linux 3.0/4.0/5.0/6.0 or SuSE Linux/SLES 9, 10, and 11, follow these steps:

1. Copy the file `MSM_linux_installer-11.02.00-00.tar.gz` to a temporary folder.
2. Extract the `MSM_linux_installer-11.02.00-00.tar.gz` file using the following command:
   ```bash
tar -zxvf MSM_linux_installer-11.02.00-00-...tar.gz
   ```
   This action creates a new disk directory.
3. Go to the new **disk** directory.
4. In the **disk** directory, find and read the **readme.txt** file.
   To start the installation, enter the following command:
   ```bash
csh install.sh -a
   ```
If you select the **Client** installation for a computer used to monitor servers, and if there are no available servers with a registered framework on the local subnet (that is, servers with a complete installation of MegaRAID Storage Manager software), the server screen appears. The server screen does not list any servers. You can use this screen to manage systems remotely.

To install the software using interactive mode, run the command `./install.sh` from the installation disk.

To install the product in a non-interactive or silent mode, use the command `./install.sh [-options] [ -ru popup]` from the installation disk. The installation options are:

- Complete installation
- Client Component Only
- Stand Alone
- Local mode

The `-ru popup` command removes the pop-up from the installation list.

You also can run a non-interactive installation using the `RunRPM.sh` command.

The installer offers the following setup options:

- **Complete** – This option installs all the features of the product.
- **Client Components Only** – The storelib feature of the product is not installed in this type of installation. As a result, the resident system can only administer and configure all of the servers in the subnet but it cannot serve as a server.
- **Stand Alone** – Only the networking feature is not installed in this case, so the resident system is not a part of the network. This implies that the system cannot browse any other MegaRAID Storage Manager servers in the subnet, and the MegaRAID Storage Manager servers cannot recognize it as a server.
- **Local** mode - This option enables you to view only the workstation that has the MegaRAID Storage Manager software installed. You will not be able to discover other remote servers and other remote servers will also not be able to connect to your workstation. In a local mode installation, you will be using the loopback address instead of the IP address.

This installation helps you select any of the setup types, but if you run `RunRPM.sh`, it installs the complete feature.

---

**Uninstalling MegaRAID Storage Manager Software on Linux**

To uninstall the MegaRAID Storage Manager software on a system running Linux, follow these steps:

1. Go to `/usr/local/MegaRAID Storage Manager`.
2. Run `./uninstaller.sh`.

   This procedure uninstalls the MegaRAID Storage Manager software.

**Executing a CIM Plug-in on Red Hat Enterprise Linux 5**

To execute a Common Information Model (CIM) plug-in on Red Hat Enterprise Linux 5, you must create the following symbolic links:
1. cd /usr/lib on RHEL 5
2. Search for libcrypto, libssl, and libsysfs libraries as follows:
   
   \[ \text{ls -lrt } \text{libcrypto*}, \text{ls -lrt } \text{libssl*}, \text{ls -lrt } \text{libsysfs*} \]
3. If the files libcrypto.so.4, libssl.so.4, and libsysfs.so.1 are missing, manually create sym links as follows:
   
   \[ \text{ln -s libcrypto.so libcrypto.so.4} \]
   \[ \text{ln -s libssl.so libssl.so.4} \]
   \[ \text{ln -s libsysfs.so libsysfs.so.1} \]

   See Installing and Supporting MegaRAID Storage Manager Software on VMware for more information about CIM.

   \textbf{Note:} If the `.so` files are not present in the /usr/lib directory, create a link with the existing version of the library.

   For example, if libcrypto.so.6 is present and libcrypto.so is not, create the link as follows:
   
   \[ \text{ln -s libcrypto.so.6 libcrypto.so.4} \]

   On a 64-bit operating system, the system libraries are present in the /usr/lib64 directory by default. However, for supporting CIM Plug-in, make sure that the libraries are also present in /usr/lib by installing the appropriate RPMs.

---

**Installing and Supporting MegaRAID Storage Manager Software on Solaris 10U5, U6, U7, and U8 (Both x86 and x64)**

This section documents the installation of MegaRAID Storage Manager software on the Solaris U5, U6, U7, and U8 x86 and x64 operating systems, and Solaris SPARC. This section also includes the following topics:

- Installing MegaRAID Storage Manager Software for Solaris 10 x86
- Uninstalling MegaRAID Storage Manager Software for Solaris 10 x86
- Installing MegaRAID Storage Manager Software for Solaris 10 SPARC
- Uninstalling MegaRAID Storage Manager Software for Solaris 10 SPARC

**Installing MegaRAID Storage Manager Software for Solaris 10 x86**

Follow these steps to install the MegaRAID Storage Manager software on a system running Solaris 10 x86:

1. Copy the MegaRaidStorageManager-SOLX86-...tar.gz file to a temporary folder.
2. Untar the MegaRaidStorageManager-SOLX86-...tar.gz file using the following command:
   
   \[ \text{tar -zxvf MegaRaidStorageManager-SOLX86-...tar.gz} \]
   
   This step creates a new disk directory.
3. Go to the new disk directory and find and read the readme.txt file.
4. Enter the Bash shell.
5. Run the command ./install.sh present in the disk directory.
6. When prompted by the installation scripts, select Y to complete the installation.

Uninstalling MegaRAID Storage Manager Software for Solaris 10 x86

Follow these steps to uninstall the MegaRAID Storage Manager software on a system running Solaris 10 x86:

1. Execute the Uninstaller.sh file located in /opt/MegaRaidStorageManager directory.
2. When prompted by the uninstallation scripts, select Y to complete the installation.

   **Note:** To shut down the MegaRAID Storage Manager Framework service, run the `svcadm disable -t MSMFramework` command.
   It is advisable to stop the Monitor service before stopping the MegaRAID Storage Manager Framework service.
   To stop the Monitor service, run `svcadm disable -t MSMMonitor`.

   To start the Framework service, run `svcadm enable MSMFramework`.

   When the service is in maintenance state, run the `svcadm clear MSMFramework` command and `svcadm clear MSMMonitor` command.

   To start the monitor service, run `svcadm enable MSMMonitor` command.

   To check the status of the MegaRAID Storage Manager services, run the command `svcs -a | grep -i msm`.

Installing MegaRAID Storage Manager Software for Solaris 10 SPARC

Follow these steps to install the MegaRAID Storage Manager software on a system running Solaris 10 SPARC:

1. Copy the `MegaRaidStorageManager-SOLSPARC-8.10-...tar.gz` file to a temporary folder.
2. Untar the `MegaRaidStorageManager-SOLSPARC-8.10-...tar.gz` file using the following command:
   ```
   tar -zxvf MegaRaidStorageManager-SOLSPARC-8.10-...tar.gz
   ```
   This step creates a new disk directory.
3. Go to the new disk directory and read the `readme.txt` file.
4. Enter the Bash shell.
5. Run the command `./install.sh` present in the disk directory.
6. When prompted by the installation scripts, select Y to complete the installation.

Uninstalling MegaRAID Storage Manager Software for Solaris 10 SPARC

Follow these steps to uninstall the MegaRAID Storage Manager software on a system running Solaris 10 SPARC:

1. Execute the Uninstaller.sh file located in /opt/MegaRaidStorageManager directory.
2. When prompted by the uninstallation scripts, select Y to complete the installation.

   **Note:** To shut down the MegaRAID Storage Manager Framework service, run the `svcadm disable -t MSMFramework` command.
   It is advisable to stop the Monitor service before stopping the MegaRAID Storage
Manager Framework service.
To stop the Monitor service, run `svcadm disable -t MSMMonitor`.

To start the Framework service, run `svcadm enable MSMFramework`.

When the service is in maintenance state, run the `svcadm clear MSMFramework` command and `svcadm clear MSMMonitor` command.

To start the monitor service, run `svcadm enable MSMMonitor` command.

To check the status of the MegaRAID Storage Manager services, run the command `svcs -a | grep -i msm`.

---

**MegaRAID Storage Manager Software Customization**

You can customize your logo and the splash screen by editing the `msm.properties` file present in the `<installation-directory/MegaRAID Storage Manager>` folder.

The `msm.properties` file has no values for the following keys:

- `CHANNELLOGO=
- `CHANNELSPLASHSCREEN=

No default values are assigned for these keys, therefore the MegaRAID Storage Manager software uses the default LSI logo and the splash screen.

To customize the logo and the splash screen, enter the logo and the splash screen file name against these entries.

To enter the file names, follow these steps:

1. Open the file `msm.properties` in the `<installation-directory/MegaRAID Storage Manager>` folder.
2. Enter the value for the logo file against the key `CHANNELLOGO`.
3. Enter the value for the splash screen file against the key `CHANNELSPLASHSCREEN`.
4. Save the file.
5. Place these two images in the `<installation-directory/MegaRAID Storage Manager>` folder.
6. Start the application.

Following are some important points that you need to keep in mind:

- File names for both entries should not have any spaces. For example, the valid file name would be: `logo_test_1.png` or `LogoTest1.png` or `TEST_SPLASH_FILE.jpg`.
- The logo image dimensions should not exceed 160 * 85 (width * height).
- The splash screen image dimensions should not exceed 390 * 260 (width * height).

After making these changes, you can view the changes with the new splash screen and the logo in the MegaRAID Storage Manager software when you log in to the MegaRAID Storage Manager software.
Installing and Supporting MegaRAID Storage Manager Software on VMware

This section documents the installation of the MegaRAID Storage Manager software on VMware ESX (also known as Classic) and VMware ESXi operating systems.

Installing MegaRAID Storage Manager Software on VMware ESX (VMware Classic)

VMware does not support any graphic components and hence you can install only the server component of the MegaRAID Storage Manager software. To install, run the script .%/vmware_install.sh from the installation disk.

The installer prompts you for the following information:

- End user license agreement
- Operating system (VMware 3.5 or VMware 4.x)
- Select the Storelib (Inbox Storelib or Storelib from MSM package)

Uninstalling MegaRAID Storage Manager Software for VMware

To uninstall the server component of the MegaRAID Storage Manager software on VMware, use the Uninstall command in the Program menu or run the script /usr/local/MegaRAID Storage Manager/uninstaller.sh.

You need to keep in mind the following points:

1. A MegaRAID Storage Manager software upgrade is supported in this release. This release can be upgraded by future releases.
2. To shut down the MegaRAID Storage Manager Framework service, run the following command:

   /etc/init.d/vivaldiframeworkd stop

   It is recommended that you stop the Monitor service before you stop the MegaRAID Storage Manager Framework service. To stop the Monitor service, run the following command:

   /etc/init.d/mrmonitor stop

   The Linux RPM of the MegaRAID Storage Manager software works under the console with minimal changes. Hardware RAID is currently supported in ESX 4.x.

Important: There is a known limitation that virtual drives that are created or deleted will not be reflected to the kernel. The workaround is to reboot the server or to run esxcfg-rescan <vmhba#> from COS shell.

Supporting MegaRAID Storage Manager Software on the VMware ESXi Operating System

This section describes the product requirements needed to support the VMware ESXi operating system. Classic VMware includes a Service Console that is derived from the Linux 2.4 kernel but with reduced functionality.

The MegaRAID Storage Manager server part cannot be installed directly in VMware ESXi. Management is possible only through Common Information Model (CIM) providers. These CIM providers integrated into the ESXi system build an interface between the hardware driver of the LSI MegaRAID controller and remote applications, such as the MegaRAID Storage Manager.
software. Management is performed through the MegaRAID Storage Manager software installed on a remote machine (Linux/Windows).

VMware ESX 4.0 comes with the Small Footprint CIM Broker (CFCB) CIM Object Manager (or CIMOM). A CIMOM manages the communication between providers, which interact with the hardware, and a CIM client, where the administrator manages the system.

SFCB supports Common Manageability Programming Interface (CMPI)-style providers. CMPI defines a common standard used to interface Manageability Instrumentation (providers, instrumentation) to Management Brokers (CIM Object Manager). CMPI standardizes Manageability Instrumentation, which lets you write and build instrumentation once and run it in different CIM environments (on one platform).

Network communication is a key element for a proper communication between the ESXi CIM provider and the LSI management software. Please make sure that the network settings are correct by making the following changes:

- For networks that do not have DNS configured, the “hosts” file in the machine on which the MegaRAID Storage Manager software is installed must be edited as follows:
  1. Add an entry to map the VMware host’s IP address with the host name. This is for the discovery process to happen correctly. In the absence of this entry, the VMware host would be discovered as 0.0.0.0.
  2. Add an entry to map its own IP address (not the loop back address) with the Hostname. This is to ensure that the Asynchronous Event Notifications (AENs) are delivered correctly.
- For networks that have DNS configured, perform the following:
  1. Provide the correct DNS server IP address when you do the initial configurations for the VMware host.
  2. In the hosts file of the machine on which the MegaRAID Storage Manager software is installed, add an entry to map its own IP address (not the loop back address) with the host name, to ensure that the Asynchronous Event Notifications are delivered correctly.

**Discovery and login**

You can start the MegaRAID Storage Manager software from a remote Windows/Linux machine that has the MegaRAID Storage Manager software installed in complete mode.

1. On the Host View window that appears, click Configure Hosts. The Configure Host window appears as shown below.
2. Select **Display all the systems in the network of local server.**

3. Click **Save Settings.** A confirmation dialog appears asking you to confirm your settings. Click **OK** in the confirmation dialog to start the discovery process.

   The ESXi server appears in the list of found hosts as shown in the following figure.
4. Double click your ESXi host. The following figure appears.

**Figure 3  Login on the Host Server**

5. Enter the root account name and password of the ESXi Host in the **User Name** and **Password** fields respectively.

6. Click Login.

After you log in, the dashboard view provides an overview of the system and covers the properties of the virtual drives and the physical drives, the total capacity, configured capacity, unconfigured capacity, background operations in progress, the MegaRAID Storage Manager software features and their status (enabled or disabled), and the actions you can perform, such as creating a virtual drive and updating the firmware.

**Limitations of Installation and Configuration**

For more information about these limitations, see Differences in the MegaRAID Storage Manager Software for VMware ESXi.
• No active event notification is available, for example, by pop-up or email.
• No status information is available for the controller.
• Events are collected as long as the MegaRAID Storage Manager software runs on the Client.
• The MegaRAID Storage Manager software responds more slowly.

Differences in the MegaRAID Storage Manager Software for VMware ESXi

The following are some of the differences in the MegaRAID Storage Manager software utility when you manage a VMware ESXi server:

• The following limitations apply to the system information exposed through the application:
  – Only the IP address and the host name is displayed.
  – The operating system type and the operating system architecture is not displayed.
  – No support is available for the controller health information.
• Authentication support.
  – The MegaRAID Storage Manager software allows the CIMOM server authentication with the user ID and the password for VMware.
  – Access to VMware ESXi hosts is controlled based on the user privileges. Only root users can have ‘Full Access’ while the non-root users can have only ‘View Only’ access.
  – Multiple root users can simultaneously login using ‘Full Access’ mode to access the VMware ESXi server.
• Event logging.
  Event logging support is available for the VMware ESXi operating system, but it works differently than the normal MegaRAID Storage Manager framework mode. The event logging feature for the MegaRAID Storage Manager Client connected to a VMware ESXi system behaves as follows:
  – There is no support for retrieving initial logs (the events that occurred before a client logs in). Only those events that occur after a client logs appear in the event logger dialog.
  – System logs are not displayed.
  – The “Save log” feature is not supported; however, the “Save Log as Text” is supported.
  – The “View Log” option allows you to view the logs saved in a text file on the event logger dialog.
  – The event descriptions might not be identical to a normal MegaRAID Storage Manager Client because the descriptions come from the firmware through the provider.
  – There is no filtering of events, unlike other operating systems because of the lack of Monitor Service support.
  – Refreshing of the MegaRAID Storage Manager GUI after any updates on the firmware is slower for a client connected to VMware ESXi hosts, compared to one connected to a Windows/Linux/Solaris hosts.
• It takes a while to discover the CIMOM servers. If you start the MegaRAID Storage Manager client immediately after you install the MegaRAID Storage Manager software (or restart Framework service), you will not be able to discover any hosts in the network.
• VMware ESXi is supported only in a complete installation of the MegaRAID Storage Manager software; stand-alone, client-only, and server-only modes do not support VMware ESXi management.
VMware ESXi is supported on following operating systems:
- Microsoft Windows Server
- Linux RHEL
- SuSE Linux

Uninstalling MegaRAID Storage Manager Software

You can uninstall the MegaRAID Storage Manager software by using the Uninstall command in the Program menu. See the section for your operating system for the MegaRAID Storage Manager software uninstall procedures for your specific operating system.

Installing and Configuring an SNMP Agent

A Simple Network Management Protocol (SNMP)-based management application can monitor and manage devices through SNMP extension agents. The MegaRAID SNMP sub agent reports the information about the RAID controller, virtual drives, physical devices, enclosures, and other items as per the SNMP request. The SNMP application monitors these devices for issues that might require administrative attention.

This section describes the installation and configuration of the LSI MegaRAID SNMP agent on Linux, Solaris, and Windows operating systems.

**Note:** The complete installation of the MegaRAID Storage Manager software installs the SNMP agent. However, you can install the SNMP agent (installer) on a system separately, without the MegaRAID Storage Manager software being installed.

Prerequisite for LSI SNMP Agent RPM Installation

The LSI SNMP agent application depends on the standard SNMP Utils package. Make sure that the SNMP-Util package is present in the system before you install the LSI SNMP agent RPM.

The SNMP-Util package includes the RPM's net-snmp-libs, net-snmp-utils, and additional dependent RPMs.

Make sure that these RPM are installed from the operating system media before you install the LSI SNMP agent RPM.

Installing and Configuring an SNMP Agent on Linux

This section explains how to install and configure the SAS SNMP Agent for the SuSE Linux and Red Hat Linux operating systems. To do this, perform the following steps:

**Note:** This procedure requires that you have Net-SNMP agent installed on the Linux machine.

The RPM has not been created to support -U version.
The RPM -U will probably fail with this RPM.

1. Install the LSI SAS SNMP Agent using `rpm -ivh <sas rpm>`. 
Note: After installation, find the SAS MIB file LSI-AdapterSAS.mib under the /etc/lsi_mrdsnmp/sas directory.

RPM makes the necessary modification needed in the snmpd.conf file to run the agent.

Note: Before installation, check whether there is any pass command that starts with 1.3.6.1.4.1.3582 OID in snmpd.conf. If so, delete all of the old pass commands that start with 1.3.6.1.4.1.3582 OID. (This situation could occur if an earlier version of LSI SNMP Agent was installed in the system.)

The snmpd.conf file structure should be the same as lsi_mrdsnmpd.conf. For reference, a sample conf file (lsi_mrdsnmpd.conf) is in the /etc/lsi_mrdsnmp directory.

2. To run an SNMP query from a remote machine, add the IP address of that machine in the snmpd.conf file, as in the following example:

   com2sec snmpclient 172.28.136.112 public

   In this example, the IP address of the remote machine is 172.28.136.112.

3. To receive an SNMP trap to a particular machine, add the IP address of that machine in the com2sec section of the snmpd.conf file.

   For example, to get a trap in 10.0.0.144, add the following to snmpd.conf.

   # sec.name source community
   com2sec snmpclient 10.0.0.144 public

4. To run/stop the snmpd daemon, enter the following command:

   /etc/init.d/snmpd start/stop

5. To start/stop the SAS SNMP Agent daemon before issuing a SNMP query, enter the following command:

   /etc/init.d/lsi_mrdsnmpd start/stop

   You can check the status of the SAS SNMP Agent daemon by issuing the following command:

   /etc/init.d/lsi_mrdsnmpd status

6. Issue an SNMP query in this format:

   snmpwalk -v1 -c public localhost .1.3.6.1.4.1.3582

7. You can get the SNMP trap from a local machine by issuing the following command:

   snmptrapd -P -F "%02.h:%02.j TRAP%w.%q from %A %v\n"

   Note: To receive a trap in a local machine with Net-SNMP version 5.3, you must modify the snmptrapd.conf file (generally located at /var/net-snmp/snmptrapd.conf). Add "disableAuthorization yes" in snmptrapd.conf and then execute "sudo snmptrapd -P -F "%02.h:%02.j TRAP%w.%q from %A %v\n".

   It is assumed that snmpd.conf is located at /etc/snmp for Red Hat and /etc for SLES. You can change the file location from /etc/init.d/lsi_mrdsnmpd file.

You can install SNMP without the trap functionality. To do so, set the "TRAPIND" environment variable to "N" before running RPM.

Before you install a new version, you must uninstall all previous versions.

For SLES 10, perform the following steps to run SNMP:
1. Copy /etc/snmp/snmpd.conf to /etc/snmpd.conf.
2. Modify the /etc/init.d/snmpd file and change SNMPDCONF=/etc/snmp/snmpd.conf entry to SNMPDCONF=/etc/snmpd.conf.
3. Run LSI SNMP rpm.

Installing and Configuring an SNMP Agent on Solaris

This section explains how to install and configure the SAS SNMP Agent for the Solaris operating system. To install and configure SNMP for Solaris, perform the procedures described in the following sections:

- Prerequisites
- Installing SNMP on Solaris
- LSI SAS SNMP MIB Location
- Starting, Stopping, and Checking the Status of the LSI SAS SNMP Agent
- Configuring snmpd.conf
- Configuring SNMP Traps
- Uninstalling the SNMP Package

Prerequisites

This package requires that you have the Solaris System Management Agent installed on the Solaris machine.

Installing SNMP on Solaris

To install SNMP for Solaris, perform the following procedure:

1. Unzip the LSI SAS SNMP Agent package.
2. Run the install script by executing the following command:
   
   # ./install.sh

   **Note:** The installation will exit if there are any existing versions of storelib and sassnmp installed on the Solaris machine. Uninstall the existing version by using the following commands:
   
   # pkgrm storelib (to uninstall storelib library)
   # pkgrm sassnmp (to uninstall LSI SAS SNMP Agent)

LSI SAS SNMP MIB Location

After you install the LSI SAS SNMP Agent package, the MIB file LSI-AdapterSAS.mib is installed under /etc/lsi_mrdsnmp/sas directory.

Starting, Stopping, and Checking the Status of the LSI SAS SNMP Agent

The following commands are used to start, stop, restart, and check the status of the Solaris System Management Agent (net snmpd) daemon:

- Start: # svcadm enable svc:/application/management/sma:default
- Stop: # svcadm disable svc:/application/management/sma:default
The following commands are used to start, stop, restart, and check the status of the SAS SNMP Agent daemon:

- **Start:** 
  
  ```bash
  #/etc/init.d/lsi_mrdsnmpd start
  ```

- **Stop:** 
  
  ```bash
  #/etc/init.d/lsi_mrdsnmpd stop
  ```

- **Restart:** 
  
  ```bash
  #/etc/init.d/lsi_mrdsnmpd restart
  ```

- **Status:** 
  
  ```bash
  #/etc/init.d/lsi_mrdsnmpd status
  ```

### Configuring snmpd.conf

By default, the SNMP queries (walk, get) can be executed from any remote machine without any changes to the `snmpd.conf` file. To quickly add a new community and client access, perform the following steps:

1. **Stop the SMA service by executing the following command:**
   
   ```bash
   # svcadm disable svc:/application/management/sma:default
   ```

2. **Add read-only and read-write community names.**

   a. Add a read-only community name and client/hostname/ipaddress under "SECTION: Access Control Setup" in the `/etc/sma/snmp/snmpd.conf` file, as shown in the following excerpt:

   ```plaintext
   # SECTION: Access Control Setup
   # This section defines who is allowed to talk to your running SNMP Agent.
   # rocommunity: a SNMPv1/SNMPv2c read-only access
   # community name
   # arguments: community
   # [default|hostname|network/bits] [oid]
   # rocommunity snmpclient 172.28.157.149
   ```

   b. Add a read-write community name and client/hostname/ipaddress under "SECTION: Access Control Setup" in the `/etc/sma/snmp/snmpd.conf` file, as shown in the following excerpt:

   ```plaintext
   # SECTION: Access Control Setup
   # This section defines who is allowed to talk to your running snmp agent.
   # rocommunity: a SNMPv1/SNMPv2c read-only access
   # community name
   # arguments: community
   # [default|hostname|network/bits] [oid]
   # rwcommunity snmpclient 172.28.157.149
   ```

3. **Start the SMA service by using the following command:**

   ```bash
   # svcadm restart svc:/application/management/sma:default
   ```

   **Note:** Online indicates that the SMA is started. Disabled indicates that the SMA is stopped.
# svcadm enable svc:/application/management/sma:default

Note: Refer to the command `man snmpd.conf` for more information about configuring the `snmpd.conf` file.

Configuring SNMP Traps

To receive SNMP traps, perform the following steps:

1. Stop the LSI SAS SNMP Agent by using the following command:
   
   `#/etc/init.d/lsi_mrdsnmpd stop`

2. Edit the `/etc/lsi_mrdsnmp/sas/sas_TrapDestination.conf` file and add the IP address as shown in the following excerpt:

   ```
   #################################################
   # Agent Service needs the IP addresses to sent trap
   # The trap destination may be specified in this file # or using snmpd.conf
   # file. Following indicators can # be set on "TrapDestInd" to instruct the
   # agent to
   # pick the IPs as the destination.
   # 1 - IPs only from snmpd.conf
   # 2 - IPs from this file only
   # 3 - IPs from both the files
   #################################################
   TrapDestInd 2
   ####################################################
   # Trap Destination IP##################################
   127.0.0.1   public
   172.28.157.149 public
   ####################################################
   ```

3. Start the LSI SAS SNMP Agent by entering the following command:

   `#/etc/init.d/lsi_mrdsnmpd start`

Uninstalling the SNMP Package

The `uninstall.sh` script is located under the `/etc/lsi_mrdsnmp/sas` directory. Use the following command to uninstall the package:

```
# cd /etc/lsi_mrdsnmp/sas
# ./uninstall.sh
```

Installing a SNMP Agent on Windows

This section explains how to install and configure the SAS SNMP Agent for the Windows operating system.

Installing SNMP Agent

Perform the following steps to install the SNMP Agent:

1. Run `setup.exe` from DISK1.
2. Use the SNMP Manager to retrieve the SAS data (it is assumed that you have compiled `LSI-AdapterSAS.mib` file already).
The LSI-AdapterSAS.mib file is available under %ProgramFiles%\LSI Corporation\SNMPAgent\SAS directory.

3. Use a trap utility to get the traps.

Note: Before you install the Agent, make sure that the SNMP Service is already installed in the system.

Installing SNMP Service for Windows

If you do not have the SNMP Service installed on your system, perform the following steps to install the SNMP Service for a Windows system:

1. Select Add/Remove Programs from Control Panel.
2. Select Add/Remove Windows Components in the left side of the Add/Remove Programs window.
4. Click Next and follow any prompts to complete the installation procedure.

Configuring SNMP Service on the Server Side

Perform the following steps to configure the SNMP Service on the server side.

1. Select Administrative Tools from the Control Panel.
2. Select Services from the Administrative Tools window.
3. Select SNMP Service in the Services window.
4. Open SNMP Service.
5. Click the Security tab and make sure that Accept SNMP Packets from any host is selected.
6. Click the Traps tab, and select the list of host IPs to which you want the traps to be sent with the community name.

Prerequisites to Running MegaRAID Storage Manager Remote Administration

The MegaRAID Storage Manager software requires port 3071 and port 5571 to be open to function. Follow these steps to prepare to run the MegaRAID Storage Manager Remote Administration.

1. Configure the system with a valid IP address.
   Make sure that there is no IP address conflict in the sub network.
   Ports such as 3071 and 5571 are open and available for the MegaRAID Storage Manager framework communication.
2. Disable the security manager and the firewall.
   Configure the multicasting.
   Make sure that the Class D multicast IP addresses are registered (at least 229.111.112.12 should be registered for the MegaRAID Storage Manager software to work); if not, create a static route using the following command:
   ```bash
   Route add 229.111.112.12 dev eth1
   ```
3. Install the MegaRAID Storage Manager software. If the MegaRAID Storage Manager software is already installed, restart the MegaRAID Storage Manager framework.
Startup and Main Windows

This section has the following topics:

- Starting MegaRAID Storage Manager Software
- Logging in to a Server
- MegaRAID Storage Manager Main Menu Window
- Menu Options

Starting MegaRAID Storage Manager Software

You must have administrative privileges to use the MegaRAID® Storage Manager software in either full-access or in view-only mode. Follow these steps to start the MegaRAID Storage Manager software on various platforms.

- To start MegaRAID Storage Manager software on a Microsoft® Windows® system, either select Start-> Programs->MegaRAID Storage Manager->StartupUI or double-click the MegaRAID Storage Manager software shortcut on the desktop.
- To start MegaRAID Storage Manager software on a Red Hat® Linux™ system, select Applications-> System Tools->MegaRAID Storage Manager->StartupUI.
- To start MegaRAID Storage Manager software on a system running SuSE™ Linux/SLES 9 SP1 or SuSE 10, select Start->System->More Programs->MegaRAID Storage Manager.
- To start MegaRAID Storage Manager software on a system running Solaris™ 10, select Launch-> Applications->Utilities->MegaRAID Storage Manager StartupUI.

If the MegaRAID Storage Manager software is installed in a stand-alone Workstation configuration, enter your user name and password when the login prompt appears.

Logging in to a Server

When you start a client or server installation of the MegaRAID Storage Manager software, the Select Server window appears, as shown in Figure 4. The remote servers appear, along with their IP address, operating system, and health status.

**Note:** If you have performed a local mode installation, the Server Login window will directly appear for you to login.
The Select Server window shows an icon for each server on which the MegaRAID Storage Manager software is installed. The servers are color-coded with the following definitions:

- **Green**: The server is operating properly.
- **Yellow**: The server is running in a partially degraded state (possibly because a drive in a virtual drive has failed).
- **Orange**: The server is running in a degraded state.
- **Red**: The server storage configuration has failed.

To log in to a server, follow these steps:

1. Double-click the icon of the server that you want to access.
   The Server Login window appears.
2. Select an access mode from the drop-down menu.
   - Select **Full Access** if you need to both view the current server configuration and change the configuration.
   - Select **View Only** if you only need to view the server configuration.
3. Enter your user name and password, and click **Login**.
   If the computer is networked, this is the login to the computer itself, not the network login.
If your user name and password are correct for the login mode you have chosen, the MegaRAID Storage Manager main menu screen appears.

**Note:** To access servers on a different subnet, type the IP address of a server in the desired subnet, where the MegaRAID Storage Manager is running, in the box at the bottom of the Server Select screen and click **Discover Host**.

For the VMware CIMOM, the server button does not denote the health of the server. The button is always green regardless of the health of the system.

The VMware server does not show the system health and the operating system labels. It shows only the host name and the IP address of the server. When connecting to a VMware server on a different subnet, one or more Frameworks have to be running in the subnet to connect to the CIMOM.

4. Double-click the icon of the server that you want to access.

   The Server Login window appears.

5. Select an access mode from the drop-down menu.

   – Select **Full Access** if you need to both view the current configuration and change the configuration.

   – Select **View Only** if you need to only view and monitor the configuration.

   **Note:** When connected to VMware system, the Server Login screen shows only one label for access, “Full Access”. Multiple users can have full access to the VMware server.

6. Enter your user name and password, and click **Login**.

   **Note:** If the computer is networked, this is the login to the computer itself, not the network login.

7. Enter the root/administrator user name and the password to use Full Access mode.

   **Note:** In the Linux operating system, if you belong to the root user group, you can log in; you do not have to be a user with the user name “root.”

If your user name and password are correct for the Login mode you have chosen, the MegaRAID Storage Manager main menu screen appears.

---

**MegaRAID Storage Manager Main Menu Window**

These topics describe the panels in the main MegaRAID Storage Manager main menu:

- Dashboard/Physical View/Logical View
- Properties/Graphical View Tabs
- Event Log Panel

---

**Dashboard/Physical View/Logical View**

The left panel of the MegaRAID Storage Manager window displays the Dashboard view, the Physical view, or the Logical view of the system and the attached devices, depending on which tab is selected.
The **Dashboard** view displays an overview of the system and covers the following features, as shown in the following figure:

- Properties of the virtual drives and the physical drives
- Total capacity, configured capacity, and unconfigured capacity
- Background operations in progress
- MegaRAID Storage Manager software features and their status (enabled or disabled)
- Actions you can perform, such as creating a virtual drive and updating the firmware
- Links to Online Help

**Figure 5  Dashboard View**

The **Physical** view displays the hierarchy of physical devices in the system, as shown in Figure 6. At the top of the hierarchy is the system itself, followed by the controller and the backplane. One or more controllers are installed in the system. The controller label identifies the MegaRAID controller, such as the MegaRAID SAS 9260-8i controller, so that you can easily differentiate between multiple controllers. Each controller has one or more ports. Drives and other devices are attached to the ports. The properties for each item appear in the right panel of the screen.
The *Logical* view shows the hierarchy of controllers, virtual drives, the drives, and the drive groups that make up the virtual drives, as shown in the following figure. The properties for these components appear in the right panel.
Chip Temperature and Controller Temperature

In the physical view and the logical view, you can view the chip temperature and the controller temperature under controller properties for the controller, as shown in the following figure.

You can see the temperature values only for PERC controllers from PERC 7.5 onwards.
Physical Drive Temperatures

The temperature for the physical drive appears in the following figure.

Figure 8  Chip and Controller Temperature

Figure 9  Physical Drive Temperature
Shield State

This section describes the Shield state in the MegaRAID Storage Manager software.

Physical devices in the MegaRAID firmware transit between different states. If the firmware detects a problem or a communication loss for a physical drive, it transitions the physical drive to a bad (FAILED/UNCONF BAD) state. To avoid transient failures, an interim state called the Shield state appears before marking the physical drive as a bad state.

The Shield state is an interim state of a physical drive for diagnostic operations. The results of the diagnostic tests determine if the physical drive is good or bad. If any of the diagnostics tests fail, the physical drive will transition to a BAD state (FAILED or UNCONF BAD).

The three possible Shield states are Unconfigured - Shielded, Configured - Shielded, and Hotspare - Shielded.

Shield State Physical View

Follow these steps to view the Shield state under the physical view tab.

1. Click the Physical tab in the device tree.

   The icon indicates a Shield State.

   The Physical View Shield state is shown in the following figure.

   ![Physical View Shield State](image)

Logical View Shield State

Follow these steps to view the Shield state under the Logical tab.

1. Click the Logical tab in the device tree.

   The icon indicates a Shield state.

   The Logical View Shield state is shown in the following figure.

   ![Logical View Shield State](image)
**Figure 11** Logical View Shield State

![Logical View Shield State](image)

**Viewing the Physical Drive Properties**

Follow these steps to view the Physical properties of the drive in the Shield state.

1. Click the **Physical** or **Logical** tab in the device tree.
2. The 🟢 icon indicates a Shield state.
3. Click the physical drive to view the properties.

   The device properties are displayed, as shown in the following figure.

**Figure 12** Physical Drive Properties of a Drive in Shield State

![Physical Drive Properties](image)

The status of the drive must be the Shield type.

**Viewing Server Profile of a Drive in Shield State**

Follow these steps to view the server properties of the drive in a shield state.

1. Click the **Dashboard** tab in the device tree.
2. Click the **View Server Profile** link in the dashboard view.
The server profile information is displayed, as shown in the following figure.

**Figure 13 Server Profile View of a Drive in Shield State**

![Server Profile View](image)

### Parity Size

Parity size is used for storing parity information on RAID 5, RAID 6, RAID 50, and RAID 60 virtual drives.

Follow these steps to view the Parity Size.

1. In the Logical view, click the **Virtual Drive** node.
2. For RAID 5, RAID 6, RAID 50, and RAID 60, the **parity size** is displayed as shown in the following figure.

**Figure 14 Parity Size**

![Parity Size](image)
Mirror Data Size

Mirror data size determines the size used for storing redundant information on RAID 1 and RAID 10 virtual drives.

Follow these steps to view the mirror data size.

1. In the Logical view, click the Virtual Drive node.

Mirror data size is displayed for RAID 1 and RAID 10 Volumes, as shown in the following figure.

![Figure 15 Mirror Data Size](image)

The Parity size and the Mirror data size will not be displayed for RAID 0 and RAID 00 volumes.

Metadata Size

The metadata size field displays the total space used for metadata.

Follow these steps to view the metadata size.

1. In the Logical view or the Physical view, click the controller node.

The total space used for metadata is displayed in this field, as shown in the following figure.
The size units displayed are as follows:

If the size is less than 1 MB (1024 KB), the size is displayed in KB.
If the size is greater than or equal to 1 MB but less than 1 GB (1024 MB), the size is displayed in MB.
If the size is greater than or equal to 1 GB, but less than 1 TB (1024 GB), the size is displayed in GB.

Emergency Hotspare

When a drive within a redundant virtual drive fails or is removed, the MegaRAID firmware automatically rebuilds the redundancy of the virtual drive by providing an emergency hotspare (EHSP) drive; even if no commissionable dedicated or global hotspare drive is present.

Emergency Hotspare for Physical Drives

The Emergency Hotspare property determines whether a particular drive is capable of becoming an emergency hotspare. This property is displayed under the controller properties, only if the Global Hotspare for Emergency and the Unconfigured Good for Emergency controller properties are enabled.

Follow these steps to view the Emergency Hotspare property:

1. In the Logical view or Physical view, click the drive for which you want to view hotspare properties.

The emergency hotspare property is displayed under general properties, as shown in the following figure. This property denotes whether a particular drive is capable of becoming a Hotspare.
Emergency Hotspare Property for Controllers

The Emergency Hotspare properties under the controller properties are configured based on enabling or disabling the following properties:

- Global Hotspare for Emergency
- Unconfigured Good for Emergency
- Emergency for SMARTer

Follow these steps to view the emergency hotspare property for controllers:

1. Click the controller node in the device tree.

The emergency hotspare properties are displayed, as shown in the following figure.

Commissioned Hotspare

The commissioned hotspare is used to determine if the online drive has a commissioned hotspare.
Follow these steps to check if the drive has commissioned hotspare.

1. Click the online physical drive node in the device tree.

The commissioned hotspare property is displayed, as shown in the following figure.

![Commissioned Hotspare](image)

This property is displayed only for online physical drives.

**Device Icons**

Small icons represent the servers, controllers, and other devices. Here are the icons for the most often represented devices:

- **Status**
- **Server**
- **Controller**
- **Backplane**
- **Enclosure**
- **Port**
- **Drive group**
- **Virtual drive**
- **Online drive**
- **Unconfigured good drive**
- **Foreign unconfigured good drive**
- **Power save mode**
- **Dedicated hot spare**
- **Global hot spare**
- **Battery backup unit**
- **Tape drive**
- **CD-ROM**
- **Locked SED**
• Unlocked SED

**Note:** The MegaRAID Storage Manager software shows the icons for tape drive devices; however, no tape-related operations are supported by the utility. If these operations are required, use a separate backup application.

A red circle to the right of an icon indicates that the device has failed. For example, the red circle indicates that a drive has failed: 🟧 lodging •. A yellow circle to the right of an icon indicates that a device is running in a partially degraded state; the data is still safe, but data could be lost if another drive fails. An orange circle to the right of an icon indicates that a device is running in a degraded state.

**Properties/Graphical View Tabs**

The right panel contains either one tab or two tabs, depending on the kind of device you select in the left panel and depending on your login mode (full-access or view-only).

- The *Properties* tab displays information about the selected device. For example, if a controller icon is selected in the left panel, the Properties tab lists the controller name, NVRAM size, device port count, and flash size.

- The *Graphical View* tab displays information about the temperature, fans, power supplies, and voltage sensors. To display a graphical view of a drive, click an enclosure icon in the left panel of the MegaRAID Storage Manager main menu screen, and click the Graphical View tab.

**Event Log Panel**

The lower part of the screen displays the event log entries for the selected server or for the stand-alone workstation. New event log entries appear during the session. Each entry has an ID, an error level indicating the severity of the event, the timestamp and date, and a brief description of the event.

For more information about the Event Log, see *Alert Delivery Methods*. For more information about the event log entries, see *Events and Messages*.

**Menu Options**

The following are brief descriptions of the main selections on the MegaRAID Storage Manager menu bar. *Figure 20* shows the menu bar.

**Manage Menu** – The Manage menu has a Refresh option for updating the display in the MegaRAID Storage Manager window (refresh is seldom required; the display normally updates automatically) and an Exit option to end your session on the MegaRAID Storage Manager software. The Server menu item shows all the servers that were discovered by a scan. In addition, you can perform a check consistency, initialize multiple virtual groups, and show the progress of group operations on virtual drives.

**Go To Menu** – The Go To menu is available when you select a controller, drive group, physical drive, virtual drive, or battery backup unit in the main menu screen. The menu options vary depending on the type of device selected in the left panel of the MegaRAID Storage Manager main menu. The options also vary depending on the current state of the selected device. For example, if you select an offline drive, the Make Drive Online option appears in the Physical Drive menu.
Configuration options are also available for you to access the Configuration wizard that you use to perform configuration drive groups and virtual drives. To access the Wizard, select the controller in the left panel, and select **Go To->Controller->Create Virtual Drive**, as shown in the following figure.

**Figure 20  Create Virtual Drive Menu Options**

![Create Virtual Drive Menu Options](image)

**Log Menu** – The Log menu includes options for saving and clearing the message log. For more information, see [Alert Delivery Methods](#) and [Events and Messages](#).

**Tools Menu** – On the Tools menu you can select **Tools->Configure Alerts** to access the Configure Alerts screen, which you can use to set the alert delivery rules, event severity levels, exceptions, and email settings. For more information, see [Configuring Alert Notifications](#).

**Help Menu** – On the Help menu you can select **Help->Contents** to view the MegaRAID Storage Manager online help file. You can select **Help->About MegaRAID Storage Manager** to view the version information for the MegaRAID Storage Manager software.

**Note:** When you use the MegaRAID Storage Manager software online help, you might see a warning message that Internet Explorer has restricted the file from showing active content. If this warning appears, click on the active content warning bar, and enable the active content.

If you are using a Linux operating system, you must install Firefox® or Mozilla® for the MegaRAID Storage Manager software online help to display.

When connected to the VMWare server, only the IP address and the host name information appear. Additional information, such as the operating system name, version, and architecture do not appear.
Configuration

You can use the MegaRAID Storage Manager software to perform the following configuration tasks:

- Creating a New Configuration
- Creating Hot Spares
- Changing Adjustable Task Rates
- Changing Power Settings
- Changing Virtual Drive Properties
- Changing a Virtual Drive Configuration
- Deleting a Virtual Drive

The MegaRAID Storage Manager software enables you to easily configure the controllers, drives, and other storage-related devices installed on a server or on a workstation. The configuration utility simplifies the process of creating drive groups and virtual drives. You can use the Simple Configuration mode to have the MegaRAID Storage Manager software automatically create the best possible configuration using the available drives. You can use the Advanced Configuration mode to have greater flexibility than simple configuration because you can select the drives and the virtual drive settings when you create a virtual drive. In addition, you can use the advanced configuration procedure to create spanned drive groups.

**Note:** When you access the MegaRAID Storage Manager software, select Full Access if you need to view the current configuration and to change the configuration. Select View Only if you need to only view and monitor the configuration.

### Creating a New Configuration

You can use the MegaRAID Storage Manager software to create new storage configurations on systems with LSISAS controllers. You can create configurations using the following modes:

- **Simple configuration** specifies a limited number of settings and has the system select drives for you. This option is the easiest way to create a virtual drive.

- **Advanced configuration** lets you choose additional settings and customize virtual drive creation. This option provides greater flexibility when creating virtual drives for your specific requirements.

The following subsections define RAID levels and explain how to create simple and advanced storage configurations:

- Understanding RAID Levels
- Creating a Virtual Drive Using Simple Configuration
- Creating a Virtual Drive Using Advanced Configuration

### Understanding RAID Levels

RAID means **Redundant Array of Independent Disks**. When you create storage configurations, you can use several different types of RAID technology, called **RAID levels**, to create multiple-
drive arrays, or drive groups, on which data will be stored. The computer operating system sees each drive group as a single virtual drive, not as a collection of individual drives.

- **A RAID 0** drive group has two or more drives. Data is divided into small blocks (stripes) that is written successively to all the drives in the drive group. Thus, at the same time the data block #1 is written to drive 1, data block #2 is being written to drive 2, and so on. Using RAID 0 is obviously faster than writing an entire file to one drive, and reading files is faster as well. RAID 0 is a good choice if fast read/write capability is the most important objective. However, RAID 0 drive groups are not fault tolerant and cannot be protected with hot spare drives.

- **A RAID 00** drive group is a spanned drive group that creates a striped set from a series of RAID 0 drive groups.

- **A RAID 1** drive group has exactly two drives. Data is written simultaneously to both drives, so that one drive is a mirror of the other. If one of the drives fails, the data is still protected. A hot spare drive can be used to automatically replace a failed mirrored drive. RAID 1 provides a high level of data protection. However, data writes are slower than with a RAID 0 drive group because all data must always be written to two drives. Also, the two-drive RAID 0 drive group has only one drive of actual capacity.

- **A RAID 10** drive group is a spanned drive group that creates a striped set from a series of mirrored drives. The drive group can sustain multiple drive losses as long as no two drives lost comprise a single pair of one mirror.

- **A RAID 5** drive group requires a minimum of three drives. Blocks of data and parity information are written across all drives. The parity information is used to recover the data if one drive fails in the drive group. A hot spare drive can be used to automatically replace a failed drive. The disadvantage of RAID 5 is a relatively slow write cycle (two reads and two writes are required for each block written). RAID 5 is best suited for networks that perform many small I/O transactions simultaneously. Because each drive contains both data and parity, many writes can take place concurrently.

- **A RAID 50** is a spanned drive group in which data is striped across multiple RAID 5 drive groups. Thus, RAID 50 provides the features of both RAID 0 and RAID 5. RAID 50 breaks up data into smaller blocks, and then stripes the blocks of data to each RAID 5 drive group. A minimum of six drives is required. RAID 50 can sustain one to four drive failures without losing data, if each failed drive is in a different RAID 5 drive group.

  **Note:** Having virtual drives of different RAID levels, such as RAID 0 and RAID 5, in the same drive group is not allowed. For example, if an existing RAID 5 virtual drive is created out of partial space in an array, the next virtual drive in the array has to be RAID 5 only.

- **A RAID 6** drive group, which requires a minimum of three drives, is similar to a RAID 5 drive group. Blocks of data and parity information are written across all drives. The parity information is used to recover the data if one or two drives fail in the drive group. A hot spare drive can be used to automatically replace a failed drive. RAID 6 provides more data protection than RAID 5; the data is still safe if a second drive fails while the first failed drive is being rebuilt.

- **A RAID 60** drive group provides the features of both RAID 0 and RAID 6, and includes both parity and disk striping across multiple drive groups. RAID 60 provides a high level of data protection through the use of a second parity block in each stripe. A RAID 60 virtual drive can survive the loss of two drives in each of the RAID 6 sets without losing data. RAID 60 is best implemented on two RAID 6 drive groups with data striped across both drive groups. Use RAID 60 for data that requires a very high level of protection from loss.
Optimum Controller Settings for CacheCade - SSD Caching

- Write Policy: Write Back
- IO Policy: Cached IO
- Read Policy: No Read Ahead
- Stripe Size: 64 KB

Optimum Controller Settings for FastPath

- Write Policy: Write Through
- IO Policy: Direct IO
- Read Policy: No Read Ahead
- Stripe Size: 64 KB

Creating a Virtual Drive Using Simple Configuration

Simple configuration mode is the quickest and easiest way to create a new storage configuration. When you select simple configuration mode, the system creates the best configuration possible using the available drives.

**Note:** You cannot create spanned drives using the simple configuration procedure. To create spanned drives, use the advanced configuration procedure described in Creating a Virtual Drive Using Advanced Configuration.

Follow these steps to create a new storage configuration in a simple configuration mode.

1. Access the Create Virtual Drive dialog by performing either of the following steps:
   - Right-click the controller node in the device tree in the left frame of the MegaRAID Storage Manager main menu screen, and select Create Virtual Drive.
   - Select the controller node, and select Operations->Create Virtual Drive in the menu bar, as shown in the following figure.
The dialog for choosing the configuration mode (simple or advanced) appears, as shown in the following figure.

**Figure 22 Virtual Drive Creation Mode**

2. Select the Simple radio button and click Next.

   The Create Virtual Drive - Allocate capacity dialog appears, as shown in the following figure. If unconfigured drives are available, you have the option to use those unconfigured drives. If unconfigured drives are available, the Create Drive Group Settings window appears and you can go to step 4.

**Figure 23 Create Virtual Drive**

3. Perform either of the two options:
   - If a drive group exists, select the radio button to use the free capacity of the existing drive group and click Next. Continue with step 4.
The Create Virtual Drive - Drive Group and Virtual Drive Settings window appears, as shown in the following figure. If different types of drives are attached to the controller, such as HDD, SSD, SAS, and SATA, an option is available to allow drive type mixing.

- If unconfigured drives are available, select the radio button to use the unconfigured drives, and click **Next**. Continue with step 10.

The Summary window (Figure 25) appears.

**Figure 24  Create Drive Group Settings**

4. If you want to allow different types of drives in a configuration, select the **Use the drive type mixing** check box.

   **Note:** For best results, do not use drive type mixing.

5. Select a RAID level for the virtual drive.

   When you use simple configuration, the RAID controller supports RAID levels 1, 5, and 6. In addition, it supports independent drives (configured as RAID 0). The screen text gives a brief description of the RAID level that you select. The RAID levels that you can choose depends on the number of drives available.

6. Select the **Assign a hot spare** check box if you want to assign a dedicated hot spare to the new virtual drive.

   If an unconfigured good drive is available, that drive is assigned as a hot spare. Hot spares are drives that are available to replace failed drives automatically in a redundant virtual drive.

7. Select the **Use drive security** check box if you want to set a drive security method.

   The LSI SafeStore™ Data Security Service encrypts data and provides disk-based key management for your data security solution. This solution protects the data in the event of the theft or loss of drives.

8. Use the drop-down menu in the **Virtual drives** field to select the number of virtual drives you want to create.

9. Select the capacity for the virtual drives. Each virtual drive has the same capacity.
10. Click **Next**.

The **Create Virtual Drive - Summary** window appears, as shown in the following figure. This window shows the selections you made for a simple configuration.

**Figure 25  Create Virtual Drive - Summary Window**

![Create Virtual Drive - Summary Window](image)

11. Click **Back** to return to the previous window to change any selections or click **Finish** to accept and complete the configuration.

The new virtual drive is created after you click **Finish**. After the configuration is completed, a dialog box notifies you that the virtual drives were created successfully.

**Note:** If you create a large configuration using drives that are in a powersave mode, it could take several minutes to spin up the drives. A progress bar appears as the drives spin up. If any of the selected unconfigured drives fail to spin up, a box appears that identifies the drive or drives.

**Creating a Virtual Drive Using Advanced Configuration**

The advanced configuration procedure provides an easy way to create a new storage configuration. Advanced configuration gives you greater flexibility than simple configuration because you can select the drives and the virtual drive parameters when you create a virtual drive. In addition, you can use the advanced configuration procedure to create spanned drive groups.

Follow these steps to create a new storage configuration in the advanced configuration mode. This example shows the configuration of a spanned drive group.

1. Access the Create Virtual Drive dialog by performing either of the following steps:
   - Right-click on the controller node in the device tree in the left frame of the MegaRAID Storage Manager main menu screen, and select **Create Virtual Drive**.
   - Select the controller node, and select **Go To->Controller->Create Virtual Drive** in the menu bar, as shown in the following figure.
The dialog for the choosing the configuration mode (simple or advanced) appears, as shown in the following figure.

2. Click **Advanced** and press **Next**.
3. The Create Drive Group Settings window appears, as shown in the following figure.
4. Select the following items on the Create Drive Group Settings window:

   a. Select the RAID level desired for the drive group from the drop-down menu. To make a spanned drive, select **RAID 10**, **RAID 50**, or **RAID 60** in the **RAID level** field.

      Drive Group 0 and Span 0 appear in the **Drive groups** field when you select **RAID 10**, **RAID 50**, or **RAID 60**.

      The RAID controller supports RAID levels 1, 5, 6, 10, 50, and 60. In addition, it supports independent drives (configured as RAID 0 and RAID 00). The screen text gives a brief description of the RAID level you select. The RAID levels you can choose depends on the number of drives available.

   b. Scroll down the menu for the **Drive security method** field if you want to set a drive security method.

      The drive security feature provides the ability to encrypt data and use disk-based key management for your data security solution. This solution provides protection to the data in the event of the theft or loss of drives.

   c. Select *unconfigured* drives from the list of drives, and click **Add >** to add them to the drive group.

      The selected drives appear under **Span 0** below **Drive Group 0**, as shown in the following figure.
d. Click **Create Span** to create a second span in the drive group.

e. Select *unconfigured* drives from the list of drives, and click **Add >** to add them to the second drive group.

f. The selected drives appear under **Span 1** below **Drive Group 0**, as shown in the following figure.
g. Click **Create Drive Group** to make a drive group with the spans.

h. Click **Next** to complete this step.

The Virtual Drive Settings window appears, as shown in the following figure. The drive group and the default virtual drive settings appear. The options to update the virtual drive or remove the virtual drive are grayed out until you create the virtual drive.
5. Change any virtual drive settings, if desired.

   See Creating a Virtual Drive Using Simple Configuration for more information about the virtual drive settings.

6. Click **Create Virtual Drive**.

   The new virtual drive appears under the drive group, as shown in the following figure. The options **Update Virtual Drive** and **Remove Virtual Drive** are available. **Update Virtual Drive** allows you to change the virtual drive settings and **Remove Virtual Drive** allows you to delete the virtual drive.
7. Click **Next**.

The Create Virtual Drive - Summary window appears, as shown in the following figure. This window shows the selections you made for advanced configuration.

**Figure 33  Create Virtual Drive Summary Window**

8. Click **Back** to return to the previous screen to change any selections or click **Finish** to accept and complete the configuration.

The new storage configuration will be created and initialized.
Note: If you create a large configuration using drives that are in powersave mode, it could take several minutes to spin up the drives. A progress bar appears as the drives spin up. If any of the selected unconfigured drives fail to spin up, a box appears that identifies the drive or drives.

After the configuration is completed, a dialog box notifies you that the virtual drives were created successfully. If more drive capacity exists, the dialog box asks whether you want to create more virtual drives. If no more drive capacity exists, you are prompted to close the configuration session.

9. Select Yes or No to indicate whether you want to create additional virtual drives.

   If you select Yes, the system takes you to the Create Virtual Drive screen. If you select No, the utility asks whether you want to close the wizard.

10. If you selected No in the previous step, select Yes or No to indicate whether you want to close the wizard.

    If you select Yes, the configuration procedure closes. If you select No, the dialog box closes, and you remain on the same page.

---

Converting JBOD Drives to Unconfigured Good

You can convert JBOD drives to Unconfigured Good using the Create Virtual Drive or the Make Unconfigured Good drive options with a single configuration.

Perform the following steps to configure JBOD to Unconfigured Good drives by using any one of the following options.

1. Perform one of the following steps:
   - Right-click the controller node in the device tree in the left frame of the MegaRAID Storage Manager window and select Create Virtual Drive.
   - Select the controller node and select Go To->Controller->Create Virtual Drive.

The Create Virtual Drive - JBOD to Unconfigured Good Conversion wizard appears as shown in the following figure.
The **JBOD Drives** box displays the available JBOD drives available in the system.

2. Select the drives which you want configured as Unconfigured Good and then click **Convert**. Clicking on **Convert** configures the selected JBODs to Unconfigured Good Drives.

   **Note:** If you do not want to make any JBOD as Unconfigured good drive(s), select the checkbox **Do not convert JBOD drives to unconfigured good drives**. The MegaRAID Storage Manager application does not change any selected JBODs to unconfigured good drives.

3. Click **Next**.
   
The Create Virtual Drive screen appears as shown in Figure 24.

### Converting JBOD to Unconfigured Good from the MegaRAID Storage Manager Main Menu

You also can convert JBOD to Unconfigured Good by clicking the **Controller->Make Configured Good** option from the MegaRAID Storage Manager main menu window.

The **Make Configured Good** dialog appears as shown in the following figure.
1. Select the JBOD drives to be configured as Unconfigured Good.
2. Click OK.
   The selected JBOD drives are configured as Unconfigured Good.

Creating Hot Spares

Hot spares are drives that are available to automatically replace failed drives in a redundant virtual drive (RAID 1, 5, 6, 10, 50, 60). There are two kinds of hot spares:

- **Dedicated** hot spares, which are available for a specified drive group
- **Global** hot spares, which are available to any drive group defined on the controller

**Note:** The capacity of the drives you assign as dedicated hot spares should be equal to or greater than the capacity of the other drives in the drive group.

To create a global hot spare, follow these steps:

1. Select the Physical tab in the left panel of the MegaRAID Storage Manager main menu screen and click the icon of an unused drive.
   For each drive, the screen displays the port number, enclosure number, slot number, drive state, drive capacity, and drive manufacturer.
2. Select either Go To->Physical Drive->Assign Global Hot Spare or Go To->Physical Drive->Assign Dedicated Hot Spare.
3. If you selected Assign Dedicated Hot Spare, select a drive group from the list that appears. The hot spare is dedicated to the drive group that you selected.
   If you selected Assign Global Hot Spare, skip this step, and go to the step 4. The hot spare is available to any virtual drive on a specific controller.
4. Click Go to create the global hot spare.
   The drive state for the drive changes to dedicated hot spare or global hot spare, depending on your selection.
Changing Adjustable Task Rates

If you want to change the Rebuild rate and other task rates for a controller, you must first log onto the server in Full Access mode. (LSI recommends not changing the adjustable task rates from their defaults.) Follow these steps to set the adjustable task rates:

1. Select a controller icon in the Physical tab or the Logical tab in the left panel of the MegaRAID Storage Manager main menu window.

2. Select Go To->Controller->Set Adjustable Task Rates from the menu bar, as shown in the following figure.

Figure 36 Set Adjustable Task Rates Menu

![Set Adjustable Task Rates Menu](image)

The Set Adjustable Task Rates dialog appears, as shown in the following figure.

Figure 37 Set Adjustable Task Rates Dialog Box

![Set Adjustable Task Rates Dialog Box](image)
3. Enter changes, as needed, to any of the task rates:
   - **Rebuild Rate.** Enter a number from 0 to 100 to control the rate at which a rebuild will be performed on a drive when one is necessary. The higher the number, the faster the rebuild will occur (and the system I/O rate may be slower as a result).
   - **Patrol Rate.** Enter a number from 0 to 100 to control the rate at which patrol reads will be performed. Patrol read monitors drives to find and resolve potential problems that might cause drive failure. The higher the number, the faster the patrol read will occur (and the system I/O rate may be slower as a result).
   - **Background Initialization (BGI) Rate.** Enter a number from 0 to 100 to control the rate at which virtual drives are initialized “in the background.” Background initialization establishes mirroring or parity for a RAID virtual drive while allowing full host access to the virtual drive. The higher the number, the faster the initialization will occur (and the system I/O rate may be slower as a result).
   - **Check Consistency Rate.** Enter a number from 0 to 100 to control the rate at which a consistency check is done. A consistency check scans the consistency data on a fault tolerant virtual drive to determine if the data has become corrupted. The higher the number, the faster the consistency check is performed (and the system I/O rate may be slower as a result).
   - **Reconstruction Rate.** Enter a number from 0 to 100 to control the rate at which reconstruction of a virtual drive occurs. The higher the number, the faster the reconstruction occurs (and the system I/O rate may be slower as a result).

4. Click **Go** to accept the new task rates.

5. When the warning message appears, click **OK** to confirm that you want to change the task rates.

   **Note:** The Controller Operations tab also has options for disabling or silencing the alarm on the controller. Ordinarily you should leave the alarm enabled so it can warn you of abnormal conditions on the controller. You might need to silence the alarm if, for example, the alarm is malfunctioning and is sounding continuously.

---

### Changing Power Settings

The RAID controller includes Dimmer Switch™ technology that conserves energy by placing certain available online drives into a powersave mode. In a powersave mode, the drives use less energy, and the fan and the enclosure requires less energy to cool and house the drives. Also, this technology helps avoid application time-outs caused by spin-up delays and drive wear caused by excessive spin-up/down cycles.

You can use the **Power Settings** field in MegaRAID Storage Manager software to choose whether to allow unconfigured drives or hot spares to enter a powersave mode.

   **Note:** The Dimmer Switch technology is enabled by default.

When they are in the powersave mode, unconfigured drives and drives configured as hot spares (dedicated or global) can be spun down. When spun down, the drives stay in powersave mode except for periodic maintenance, including:

- Periodic background media scans (Patrol Read) to find and correct media defects to avoid losing data redundancy (hot spare drives only)
- Use of a hot spare to rebuild a degraded drive group (hot spare drives only)
• Update of Disk Data Format (DDF) and other metadata when you make changes to RAID configurations (hot spare drives and unconfigured drives)

  **Note:** If your controller does not support this option, the **Power Settings** field does not appear.

Follow these steps to change the powersave setting.

1. Select a controller icon in the **Physical** tab or the **Logical** tab in the left panel of the MegaRAID Storage Manager main menu window.

2. Select **Go To->Controller->Power Settings** from the menu bar.

   The Power Settings dialog appears, as shown in the following figure.

**Figure 38  Powersave Mode Checkbox**

![Powersave Mode Checkbox](image)

3. Click the **Allow unconfigured drives to enter powersave mode** check box and then click **OK**.

   The second Power Settings dialog appears, as shown in the following figure.

**Figure 39  Spin Down Time Delay Setting**

![Spin Down Time Delay Setting](image)

4. Enter the time delay, in minutes, before the unconfigured drives spin down automatically.

   After the specified time, the drives spin down automatically.

5. Click **OK**.
Your power settings are saved. In the Physical tab of the MegaRAID Storage Manager main menu window, the nodes for the unconfigured good drives that are spun down appear with -Powersave after their status.

**Changing Power Settings Using the Dimmer Switch Enhancement**

Follow these steps to change the power settings using the Dimmer Switch™ enhancement.

1. Select a controller icon in the **Physical** tab or in the **Logical** tab in the left panel of the MegaRAID Storage Manager window.
2. Select **Go To>Controller->Manage Power Settings** from the menu bar.
   
   The Manage Power Settings dialog appears as displayed in the following figure.

   ![Manage Power Save Settings](image)

3. Select the **Unconfigured Drives** check box; the Unconfigured drives will enter the powersave mode.
4. Select the **Hot spare Drives** check box; the Hot spare drives will enter the powersave mode.
5. Select the **Configured Drives** check box; the Configured drives will enter the power save mode.
6. Select the Drive standby time (alt+d) using the drop-down selector from the **Drive standby time** field.

   **Note:** The Drive Standby time drop-down selector is enabled only if any of the above mentioned check boxes are selected. The drive standby time can be 30 minutes, 1 hour, 1.30 hours, 2 hours through 24 hours.

7. Select the mode from the **Select power save mode** field.
   
   The mode can be **Auto**, **Max**, or **Max without cache**.
8. Click **OK**.
   
   The Power-Save settings are saved and the confirmation dialog appears.
9. Click Yes to confirm the changes to the power-save settings.

**Power Save Settings - Advanced**

You can schedule the drive active time by selecting the *Start time* and *End time* in the **Power Save Settings - Advanced** window.

Perform the following steps to schedule the drive active time.

1. Select the **Advanced** button.

   The **Power Save Settings - Advanced** dialog appears as shown in the following figure.

   **Figure 41  Power Save Settings - Advanced**

   ![Power Save Settings - Advanced](image)

2. Select the **Start time** and the **End time** from the **Schedule drive active time** field.

3. Click **OK**.

   The schedule drive active time is done.

   **Note:** Select the **Do not schedule drive active time** check box, if you do not want to schedule the drive active time.

**Automatically Spin up Drives**

The Dimmer Switch technology also allows the controller to automatically spin up the drives that are in Power-Save mode.

Perform the following steps to arrive at the **Manage Power Save Settings** screen.

1. Right click on Drive group and select **Power Settings**.

   The Manage Power Save Settings dialog appears, as shown in the following figure.
2. Select the power save mode from the drop-down selector.
   
   The values are Max, Max without cache, Auto, None, and controller defined.
   
   **Note:** The Controller Defined option enables the system to inherit the controller Power-Save mode for online drives.

3. Click OK.

**Power-Save Mode**

You can set the Power-Save mode when you create a virtual drive by using the **Select power save mode** field in the **Create Drive Group - Drive Group Settings** dialog, as shown in the following figure.

**Figure 43 Create Drive Group - Drive Group Settings (Automatic Spin Up)**
Power Save Mode - SSD Drives

If you select the Max mode or the Max without cache mode in the Select power save mode field in the above displayed figure, select one or more SSD drives, and then click Create Drive Group, a confirmation dialog appears. The dialog states that the Max mode and the Max without cache mode cannot be used for SSD drives and that Controller Defined will be selected as the power save mode.

Changing Virtual Drive Properties

Warning: Do not enable drive caching on a mirrored drive group (RAID 1 or RAID 1E). If you do, data can be corrupted or lost in the event of a sudden power loss. A warning appears if you try to enable drive caching for a mirrored drive group.

Note: For virtual drives with SAS drives only, set the drive write cache policy set to Disabled, by default. For virtual drives with SATA drives only, set the drive write cache policy to Enabled, by default.

You can change a virtual drive’s Read Policy, Write Policy, and other properties at any time after the drive is created. To do this change, follow these steps:

1. Select a virtual drive icon in the Physical tab or the Logical tab in the left panel of the MegaRAID Storage Manager main menu screen.
2. Select Go To->Virtual Drive->Set Virtual Drive Properties from the menu bar.
3. Change the Disk Cache Policy in the drop-down menu.
   The options are Unchanged (unchanged from whatever the current cache policy is), Enabled, and Disabled.
4. Click OK to accept the changes.

Changing a Virtual Drive Configuration

You can use the Modify Drive Group Wizard in the MegaRAID Storage Manager software to change the configuration of a virtual drive by adding drives to the virtual drive, removing drives from it, or changing its RAID level.

Caution: Be sure to back up the data on the virtual drive before you change its configuration.

Note: You cannot change the configuration of a RAID 10, or RAID 50, or RAID 60 virtual drive. You cannot change a RAID 0, RAID 1, RAID 5, or RAID 6 configuration if two or more virtual drives are defined on a single drive group. (The Logical tab shows which drive groups and drives are used by each virtual drive.)

Accessing the Modify Drive Group Wizard

Note: The Modify Drive Group Wizard was previously known as the Reconstruction Wizard.

Perform the following steps to access the Modify Drive Group Wizard options:

1. Click the Logical tab in the left panel of the MegaRAID Storage Manager main menu screen.
2. Select a drive group in the left panel of the window.

3. Either select Go To->Drive Group->Modify Drive Group on the menu bar, or right-click the virtual drive icon to access the Modify Drive Group Wizard.

   The following warning appears about rebooting virtual drives containing boot partitions that are undergoing RAID-level migration or capacity expansion operations. Back up your data before you proceed.

   **Figure 44  Reboot Warning Message**

![Reboot Warning Message](image)

4. Select the Confirm check box, and click Yes.

   A warning to back up your data appears, as shown in the following figure.

   **Figure 45  Warning to Back up Data**

![Warning to Back up Data](image)

5. Select the Confirm check box, and click Yes.

   The Modify Drive Group Wizard screen appears, as shown in the following figure.
The following sections explain the Modify Drive Group Wizard options.

### Adding a Drive or Drives to a Configuration

**Caution:** Be sure to back up the data on the virtual drive before you add a drive to it.

Follow these steps to add a drive or drives to a configuration with the Modify Drive Group Wizard.

1. Click the **Logical** tab in the left panel of the MegaRAID Storage Manager main menu.
2. Select a drive group in the left panel of the window.
3. Either select **Go To->Drive Group->Modify Drive Group** on the menu bar, or right-click the virtual drive icon to access the Modify Drive Group Wizard.

   The Modify Drive Group Wizard appears.

4. Select the RAID level that you want to change (migrate) the drive group to and click **Next**.

   The following dialog appears. It lists the drives you can add and it states whether you have to add a minimum number of drives to change the RAID level from the current level to the new RAID level.
5. Select the check box next to any unconfigured drives that you want to add and click **Next**.

   **Note:** The drive or drives you add must have the same capacity as or greater capacity than the drives already in the drive group, or you cannot change the RAID level.

   The Summary screen appears. This screen shows the current settings and what the settings will be after the drives are added.

6. Review the configuration information.

   Click **Back** if you need to change any selections.

7. Click **Finish** to accept the changes.

   A confirmation message appears. The message states that this operation cannot be aborted and asks whether you want to continue.

8. Click **Yes** to accept and complete the addition of the drives to the drive group.

### Removing a Drive from a Configuration

**Caution:** Be sure to back up the data on the virtual drive before you remove a drive from it.

Follow these steps to remove a drive from a RAID 1 configuration or a RAID 1E configuration.

   **Note:** This option is not available for RAID 0 configurations.

1. Click the **Logical** tab in the left panel of the MegaRAID Storage Manager main menu screen.
2. Click a drive icon in the left panel of the screen.
3. Either select **Go To->Physical Drive->Make Drive Offline** on the menu bar, or right-click the drive and select **Make Drive Offline** from the menu.

   A confirmation message appears. The message states that this operation cannot be aborted and asks whether you want to continue.

4. Click **Yes** to accept and complete the removal of the drive from the drive group.
Replacing a Drive

**Caution:** Make sure to back up the data on the virtual drive before you replace a drive.

Follow these steps to add a replacement drive and to copy the data from the drive that was removed to the replacement drive.

1. Click the **Logical** tab in the left panel of the MegaRAID Storage Manager main menu.
2. Select a drive in the left panel of the window.
3. Either select **Go To->Physical Drive->Replace Physical Drive** on the menu bar, or right-click the virtual drive icon to access the Modify Drive Group Wizard.

   The screen with the replacement drive appears, as shown in the following figure.

   ![Drive Replacement Window](image)

4. Select a replacement drive.

   A confirmation message appears.

5. Click **Yes**.

   This replaces a drive and copies the data to the selected component.

Migrating the RAID Level of a Virtual Drive

As the amount of data and the number of drives in your system increase, you can use RAID-level migration to change a virtual drive from one RAID level to another. You do not have to power down or reboot the system when you make this change.

When you migrate a virtual drive to another RAID level, you can keep the same number of drives, or you can add drives. In some cases, you have to add a certain number of drives to migrate the virtual drive from one RAID level to another. The screen indicates the minimum number of drives you are required to add.

**Caution:** Be sure to back up the data on the virtual drive before you change the RAID level.

Follow these steps to change the RAID level of the virtual drive with the Modify Drive Group Wizard:

1. Click the **Logical** tab in the left panel of the MegaRAID Storage Manager main menu screen.
2. Select a drive group in the left panel of the window.
3. Either select Go To->Drive Group->Modify Drive Group on the menu bar, or right-click the virtual drive icon to access the Modify Drive Group Wizard.

The Modify Drive Group Wizard appears, as shown in the following figure.

**Figure 49  Modify Drive Group Wizard**

4. On the Modify Drive Group Wizard screen, select the RAID level that you want to change (migrate) the drive group to, and click Next.

The following screen appears. The screen states the number of drives that you have to add to change the RAID level from the current level to a new RAID level that requires more drives.

**Figure 50  Add Drive(s) to the Current Configuration Screen**

5. Select the check box next to the unconfigured drive or drives to add, and click Next.

**Note:** The drive or drives you add must have the same capacity as or greater capacity than the drives already in the drive group, or you cannot change the RAID level.
The Summary screen appears. This screen shows the current settings and what the settings will be after the drives are added.

6. Review the configuration information.
   You can click Back if you need to change any selections.

7. Click Finish to accept the changes.
   A confirmation message appears. The message states that this operation cannot be aborted and asks whether you want to continue.

8. Click Yes to accept and complete the migration to the new RAID level.
   The operation begins on the virtual disk. To monitor the progress of the RAID level change, select Manage->Show Progress in the menu bar.

New Drives Attached to a MegaRAID Controller

When you insert a new drive on a MegaRAID system, if the inserted drive does not contain valid DDF metadata, the drive appears as JBOD for MegaRAID entry-level controllers, such as the SAS 9240-4i/8i. If the drive does contain valid DDF metadata, its drive state is Unconfigured Good.

A new drive in JBOD drive state is exposed to the host operating system as a stand-alone drive. Drives in a JBOD drive state are not part of the RAID configuration because they do not have valid DDF records. The operating system can install and run anything on JBOD drives.

Automatic rebuilds always occur when the drive slot status changes, for example, when you insert a drive or remove a drive, so that a hot spare can be used. However, a new drive in JBOD drive state (without a valid DDF record), does not perform an automatic rebuild.

To start an automatic rebuild on the new JBOD drive, you have to change the drive state from JBOD to Unconfigured Good. (Rebuilds start only on Unconfigured Good drives.) After you set the drive state to Unconfigured Good, the drive state information always remains on the drive, and you can use the drive for configuration.

See Marking a Drive Offline or Missing for the procedure to change a drive to the Unconfigured Good drive state. See Rebuilding a Drive for the procedure to rebuild a drive.

Deleting a Virtual Drive

Warning: Make sure to back up the data on the virtual drive before you delete it, and make sure that the operating system is not installed on this virtual drive.

You can delete virtual drives to rearrange the storage space. Before you can do this, you must be logged on to the server in Full Access mode. To delete a virtual drive, follow these steps:

1. Back up all of the user data on the virtual drive you intend to delete.
2. On the MegaRAID Storage Manager main menu window, select the Logical tab, and click the icon of the virtual drive you want to delete.
3. Select Go To->Virtual Drive->Delete Virtual Drive.
4. When the warning messages appear, click Yes to confirm that you want to delete the virtual drive.
   You are asked twice whether you want to delete the virtual disk to avoid deleting the virtual disk by mistake.
5. When the first warning message appears, click the Confirm check box, and click **Yes**.

6. When the second warning message appears, click the Confirm check box, and click **Yes**.

   The virtual drive is deleted, and the screen is refreshed.
Monitoring Controllers and Its Attached Devices

The MegaRAID Storage Manager software enables you to monitor the activity of all the controllers present in the system and the devices attached to them.

When you perform an operation on devices (such as the creation of a new virtual drive) or when devices automatically go from an optimal state to a different state (such as a created virtual drive goes to a degraded state or a Battery Backup Unit goes bad), the MegaRAID Storage Manager software gets those events from the controller and gives a notification to you, using different alert delivery methods.

This section contains the following topics:

- Alert Delivery Methods
- Configuring Alert Notifications
- Monitoring Server Events
- Monitoring Controllers
- Monitoring Drives
- Monitoring Virtual Drives
- Monitoring Enclosures
- Monitoring Rebuilds and Other Processes

Alert Delivery Methods

Based on the severity level (Information, Warning, Critical and Fatal), the default alert delivery methods change. By default, each severity level has one or more alert delivery methods configured for it, as shown in Table 1. To modify these alert delivery methods, see Configuring Alert Notifications. The different alert delivery methods are as follows:

- Vivaldi Log/MegaRAID Storage Manager Log
- System Log
- Pop-up Notification
- E-mail Notification
Table 1  Severity Level and Default Alert Delivery Methods

<table>
<thead>
<tr>
<th>Severity Level</th>
<th>Default Alert Delivery Method</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information</td>
<td>Vivaldi log/MegaRAID Storage Manager log and System log</td>
<td>Informational message. No user action is necessary.</td>
</tr>
<tr>
<td>Warning</td>
<td>Vivaldi log/MegaRAID Storage Manager log and System log</td>
<td>Some component might be close to a failure point.</td>
</tr>
<tr>
<td>Critical</td>
<td>Vivaldi log/MegaRAID Storage Manager log, System log, and Popup Notification</td>
<td>A component has failed, but the system has not lost data.</td>
</tr>
<tr>
<td>Fatal</td>
<td>Vivaldi log/MegaRAID Storage Manager log, System log, Popup Notification, and E-mail Notification</td>
<td>A component has failed, and data loss has occurred or will occur.</td>
</tr>
</tbody>
</table>

**Vivaldi Log / MegaRAID Storage Manager Log**

By default, all the severity events appear in the Vivaldi log/MegaRAID Storage Manager log and are displayed at the bottom of the MegaRAID Storage Manager main menu window. Each message that appears in this log has a severity level that indicates the importance of the event (severity), a date and timestamp (when it occurred), and a brief description, as show in the following figure.
You can double-click on an event to display the same information in a separate window. For a list of all events, see Events and Messages. The status bar at the bottom of the screen indicates whether the log is a MegaRAID Storage Manager server log or a locally stored log file.

When a Vivaldi log/MegaRAID Storage Manager log appears, the Log menu has the following options:

- **Save Log**: Saves the current log to a .log file.
- **Save Log Text**: Saves the current log in .txt format.
- **Load**: Enables you to load a local .log file in the bottom of the MegaRAID Storage Manager main menu window. If you select the Load menu, you will not be able to view the current log.
- **Rollback to Current Log**: This menu appears if we have loaded the logs from a local .log file. Once you select this menu, you can view the current log.
- **Clear Log**: Clears the current log information, if you have full access (versus view-only access). You have the option to save the log first.

**System Log**

By default, all the severity events are logged in the local syslog. Based on the operating system you are using, the system log is logged in the following syslog locations:

- In Windows, the system log is logged in Event Viewer -> Application.
- In Linux, the system log is logged in /var/log/messages.
- In Solaris, the system log is logged in /var/adm/messages.
Pop-up Notification

By default, fatal and critical events are displaying in a pop-up notification. Pop-up notification is started automatically when you are login in to the operating system. Through this feature, you can view multiple events in a single pop-up window as shown in following figure.

Figure 52 Pop-up Notification

E-mail Notification

By default, fatal events are displayed as e-mail notifications. Based on your configuration, the e-mail notifications are delivered to you as shown in the following figure.

In the e-mail notification, besides the event's description, the email also contains system information and the controller’s image details. Using this additional information, you can find out the system and the controller on which the fatal error occurred.
Configuring Alert Notifications

The Alert Notification Configuration feature allows you to control and configure the alerts that the MegaRAID Storage Manager software sends when various system events occur.

Select **Tools->Configure Alerts** on the main menu screen, as shown in the following figure.

Figure 54  Alert Notification Configuration Menu

The Configure Alerts window appears, as shown in the following figure. The window contains three tabs: **Alert Settings**, **Mail Server**, and **Email**. You can use each tab to perform tasks for that particular topic.
Figure 55  Configure Alerts

You can select the **Alert Settings** tab to perform the following actions:

- Edit the alert delivery method for different severity levels.
- Change the method of delivery for each individual event.
- Change the severity level of each individual event.
- Save an .xml backup file of the entire alert configuration.
- Load all the values from a previously saved backup into the dialog to edit or save these values as the current alert notification configuration.

**Note:** When you load a saved backup file, all unsaved changes made in the current session will be lost.

You can select the **Mail Server** tab to perform the following actions:

- Enter or edit the sender email address.
- Enter the SMTP server name or the IP address.
- Enter the SMTP server authentication related information (user name and password).

  **Note:** These fields are optional and are filled only when the SMTP server requires authentication.

- Save an .xml backup file of the entire alert configuration.
- Load all of the values from a previously saved backup into the dialog to edit or save these values as the current alert notification configuration.

  **Note:** When you load a saved backup file, all unsaved changes made in the current session will be lost.

You can select the **Email** tab to perform the following actions:

- Add new email addresses for recipients of alert notifications.
• Send test messages to the recipient email addresses.
• Remove email addresses of recipients of alert notifications.
• Save an .xml backup file of the entire alert configuration.
• Load all of the values from a previously saved backup into the dialog to edit or save these values as the current alert notification configuration.

  **Note:** When you load a saved backup file, all unsaved changes made in the current session will be lost.

This section also includes the following topics:

• **Editing Alert Delivery Methods**
• **Changing Alert Delivery Methods for Individual Events**
• **Changing the Severity Level for Individual Events**
• **Rollback to Default Individual Event Configuration**
• **Entering or Editing the Sender Email Address and SMTP Server**
• **Authenticating the SMTP Server**
• **Adding Email Addresses of Recipients of Alert Notifications**
• **Testing Email Addresses of Recipients of Alert Notifications**
• **Removing Email Addresses of Recipients of Alert Notifications**
• **Saving Backup Configurations**
• **Loading Backup Configurations**

### Editing Alert Delivery Methods

You can edit the default alert delivery methods, such as pop-up, email, system log, or the Vivaldi Log / MegaRAID Storage Manager log to different severity level (Information, Warning, Critical and Fatal).

Perform the following steps to edit the alert delivery methods:

1. On the Configure Alerts window, click the **Alerts Setting** tab.
2. Under the **Alerts Delivery Methods** heading, select one of the severity levels.
3. Click **Edit**. The Edit dialog appears, as shown in the following figure.

#### Figure 56 Edit Dialog

![Edit Dialog](image)

4. Select the desired alert delivery methods for alert notifications at the event severity level.
5. Click **OK** to set the delivery methods used for the severity level that you selected.
Changing Alert Delivery Methods for Individual Events

You can change the alert delivery options for an event without changing the severity level.

1. On the Configure Alerts window, click the **Alerts Setting** tab.
   
   The **Alerts Setting** portion of the window appears.

2. Click **Change Individual Events**.
   
   The **Change Individual Events** dialog appears, as shown in the following figure. The dialog shows the events by their ID number, description, and the severity level.

   ![Change Individual Events](image)

   **Figure 57** Change Individual Events

3. Click an event in the list to select it.
   
   The current alert delivery methods appear for the selected event under the **Alert Delivery Methods** heading.

4. Select the desired alert delivery methods for the event.

5. Click **OK** to return to the **Configure Alerts** window.
   
   You may click Cancel to discard your current changes and to go back to the **Configure Alerts** window.

6. In the **Configure Alerts** window, click **OK**. This saves all the changes made to the event.

   **Note:** You can click **Restore Defaults** to revert back to the default alert delivery method and the default severity level of an individual event. For more information, see Rollback to Default Individual Event Configuration.
Changing the Severity Level for Individual Events

To change the event severity level for a specific event, perform the following steps:

Note: See Table 1 for details about the severity levels.

1. On the Configure Alerts window, click the Alerts Setting tab.
   The Alerts Setting portion of the window appears.
2. Click Change Individual Events. The Change Individual Events dialog appears. The dialog shows the events by their ID number, description, and severity level.
3. Click an event in the list to select it. The current severity appears in the Severity cell for the selected event.
4. Click the Severity cell for the event. The Event Severity drop-down menu appears for that event, as shown in the following figure.

Figure 58 Change Individual Events Severity Level Menu

5. Select a different severity level for the event from the menu.
6. Click OK to return to the Configure Alerts window.
   You may click Cancel to discard your current changes and to go back to the Configure Alerts window.
7. In the Configure Alerts window, click OK to save all the changes made to the events.

Rollback to Default Individual Event Configuration

To revert back to the default alert delivery method and the default severity level of an individual event, perform the following steps:

1. On the Configure Alerts window, click the Alerts Setting tab.
   The Alerts Setting portion of the window appears.
2. Click Change Individual Events.
   The Change Individual Events dialog appears, as shown in Figure 57. The dialog shows the events by their ID number, description, and the severity level.
3. Click Restore Defaults.
   The Change Individual Events dialog appears with the default alert delivery method and the default severity level of all individual events.
4. Click OK to return to the **Configure Alerts** window.

5. In the **Configure Alerts** window, click OK to save all the changes made to the events.

**Entering or Editing the Sender Email Address and SMTP Server**

You can use the **Configure Alerts** window to enter or edit the sender e-mail address and the SMTP server.

1. On the **Configure Alerts** window, click the **Mail Server** tab.
   
   The **Mail Server** options appear, as shown in the following figure.

   **Figure 59  Mail Server Options**

   ![Mail Server Options](image)

2. Enter a sender’s email address in the **Sender email address** field or edit the existing sender email address.

3. Enter your SMTP server name/IP Address in the **SMTP Server** field or edit the existing details.

4. If your SMTP server requires authentication for sending an email, then select the **This Server requires authentication** check box.

5. Click **OK**.

**Authenticating the SMTP Server**

You can use the **Configure Alerts** window to authenticate the SMTP server, providing an extra level of security while sending an e-mail from the MegaRAID Storage Manager server.

To enter or modify the SMTP server authentication information, perform the following steps

1. On the **Configure Alerts** window, click the **Mail Server** tab.
   
   The **Mail Server** options appear, as shown in **Figure 59**.
2. If your SMTP server requires authentication for sending an email, select the **This Server requires authentication** check box. If your SMTP server does not require authentication, you may go directly to step 5.

   **Note:** The **This Server requires authentication** check box is selected by default.

3. Enter a user name in the **User name** field. (Optional - if **This Server requires authentication** check box is selected).

4. Enter the password in the **Password** field. (Optional - if **This Server requires authentication** check box is selected).

5. Click **OK**.

### Adding Email Addresses of Recipients of Alert Notifications

The **Email** tab in the Configure Alerts window shows the email addresses of the recipients of the alert notifications. The MegaRAID Storage Manager software sends alert notifications to those email addresses. Use the Configure Alerts window to add or remove email addresses of recipients and to send test messages to recipients that you add.

To add email addresses of recipients of the alert notifications, perform the following steps:

1. Click the **E-mail** tab in the Configure Alerts window.

   **Figure 60  Adding Email Settings**

   ![Adding Email Settings](image)

   2. Enter the email address you want to add in the **New recipient email address** field.

   3. Click **Add**. The new email address appears in the **Recipient email addresses** field.

### Testing Email Addresses of Recipients of Alert Notifications

Use the **Email** tab in the Configure Alerts window to send test messages to the email addresses that you added for the recipients of alert notifications.

1. Click the **Email** tab on the Configure Alerts window.

   The **Email** section of the window appears, as shown in the above figure.
2. Click an email address in the **Recipient email addresses** field.
3. Click **Test**.
4. Confirm whether the test message was sent to the email address.
   A pop-up message indicates if the test message sent to the email address was successful. If the MegaRAID Storage Manager software cannot send an email message to the email address, an error message appears.

**Removing Email Addresses of Recipients of Alert Notifications**

Use the **Email** tab in the Configure Alerts window to remove email addresses of the recipients of alert notifications.

1. Click the **Email** tab on the Configure Alerts window.
   The **Email** section of the window appears, as shown in the previous figure.
2. Click an email address in the **Recipient email addresses** field.
   The **Remove** button, which was grayed out, is now active.
3. Click **Remove**. The email address is deleted from the list.

**Saving Backup Configurations**

You can save an **.xml** backup file of the entire alert configuration. This includes all the settings on the three tabs (Alert Settings, Mail Server, and Email).

1. On the **Configure Alerts** window, click the **Alert Setting** tab, **Mail Server** tab, or the **Email** tab.
2. Click **Save Backup**. The drive directory appears.
3. Enter a filename with an **.xml** extension for the backup configuration (in the format `filename.xml`).
4. Click **Save**. The drive directory disappears.
5. Click **OK**. The backup configuration is saved and the **Configure Alerts** window closes.

**Loading Backup Configurations**

You can load all of the values from a previously saved backup into the **Configure Alert** window (all tabs) to edit or save these values as the current alert notification configuration.

**Note:** If you choose to load a backup configuration and the Configure Alerts window currently contains changes that have not yet been saved as the current alert notification configuration, the changes will be lost. You are prompted to confirm your choice.

1. On the **Configure Alerts** window, click the **Alert Setting** tab, **Mail Server** tab, or **Email** tab.
2. Click **Load Backup**.
   You are prompted to confirm your choice. The drive directory appears from which you can select a backup configuration to load.
3. Select the backup configuration file (it should be in **.xml** format).
4. Click **Open**. The drive directory disappears.
5. Click **OK**. The backup configuration is saved and the **Configure Alerts** window closes.
Monitoring Server Events

The MegaRAID Storage Manager software enables you to monitor the activity of MegaRAID Storage Manager users in the network.

When a user logs on/logs off from the application, the event message appears in the log displayed at the bottom of the MegaRAID Storage Manager screen (the Vivaldi log/MegaRAID Storage Manager Log). These event messages have a severity level, a date and timestamp (User log on/log off time), and a brief description that contains a user name, client IP address, an access mode (full/view only) and a client system time.

Monitoring Controllers

When the MegaRAID Storage Manager software is running, you can see the status of all the controllers in the left panel. If a controller is operating normally, the controller icon looks like this: 🔴. If a controller has failed, a small red circle appears next to the icon.

To display the complete controller information, click on a controller icon in the left panel of the MegaRAID Storage Manager main menu. The controller properties appear in the right panel as shown in the following figure. Most of the information on this tab is self-explanatory.

Figure 61 Controller Properties

- The Rebuild rate, Patrol read rate, Reconstruction rate, Consistency check rate, and BGI rate (background initialization) are all user selectable. For more information, see Changing Adjustable Task Rates.
Monitoring Controllers and Its Attached Devices

- The **BBU Present** field indicates whether a battery backup unit is installed or not.
- The **Alarm Enabled** field indicates whether the controller has an alarm to alert the user with an audible tone when there is an error or a problem on the controller. Options are available for disabling or silencing the alarm by right clicking on a controller icon or by selecting Go To ->Controller menu.

The controller properties are defined in the Glossary.

### Monitoring Drives

When the MegaRAID Storage Manager software is running, you can see the status of all the drives in the left panel. If a drive is operating normally, the icon looks like this: . If a drive has failed, a small red circle appears to the right of the icon.

To display the complete drive Information, click on a drive icon in the left panel of the MegaRAID Storage Manager main menu. The drive properties appear in the right panel as shown in the following figure. The information on this tab is self-explanatory. There are no user-selectable properties for physical devices. Icons for other storage devices, such as CD-ROM drives and DAT drives, can also appear in the left panel.

**Figure 62 Drive Properties**

The **Power Status** property displays the status **On** when a drive is spun up and displays the status **Powersave** when a drive is spun down. Note that SSD drives and other drives that never spin down still show **On**.
If the drives are in a disk enclosure, you can identify which drive is represented by a disk icon on the left. To do this, follow these steps:

1. Click the drive icon in the left panel.
2. Select **Go To->Physical Drive->Start Locating Drive** tab in the right panel.
   
   The LED on the drive in the enclosure starts blinking to show its location.

   **Note:** LEDs on drives that are global hot spares do not blink.

3. To stop the drive light on the enclosure from blinking, select **Go To->Physical Drive->Stop Locating Drive**.

**Running a Patrol Read**

A patrol read periodically verifies all sectors of the drives connected to a controller, including the system reserved area in the RAID configured drives. You can run a patrol read for all RAID levels and for all hot spare drives. A patrol read is initiated only when the controller is idle for a defined period and has no other background activities.

You can set the patrol read properties and start the patrol read operation, or you can start the patrol read without changing the properties.

1. Click a controller icon in the left panel.
2. Select **Go To->Controller->Set Patrol Read Properties** or right-click on a controller and select **Set Patrol Read Properties** from the menu.

   The Patrol Read - Set properties window appears, as shown in the following figure.

   **Figure 63  Patrol Read - Set Properties**

3. Select an operation mode for patrol read from the following options:
   
   – **Automatic**: Patrol read runs automatically at the time interval you specify on this window.

   – **Manual**: Patrol read runs only when you manually start it, by selecting **Start Patrol Read** from the controller options window.
– **Disabled**: Patrol read does not run.

4. (Optional) Specify a maximum count of drives to include in the patrol read. The count must be a number from 1 to 255.

5. (Optional) Click virtual drives in the list under the heading **Virtual Drives** to include in the patrol read and click **Add >** or click **Add All >>** to include all of the virtual drives.

6. (Optional) Change the frequency at which the patrol read runs.
   The default frequency is weekly (168 hours), which is suitable for most configurations. The other options are hourly, daily, and monthly.

   **Note:** LSI recommends that you leave the patrol read frequency and other patrol read settings at the default values to achieve the best system performance. If you decide to change the values, record the original default values here so you can restore them later, if necessary:
   - **Patrol Read Frequency:** ____________
   - **Continuous Patrolling:** Enabled/Disabled
   - **Patrol Read Task Rate:** ____________

7. (Optional) Set Patrol Read to run at a specific time.
   The default setting for the patrol read is to start when you click **OK** on this window. To change the default setting so that the patrol read starts at a specific time, follow these steps (otherwise, skip this step and proceed to step 8):
   a. Deselect the **Perform Patrol Read when I click OK** check box.
   b. Select the month, year, day, and time to start the patrol read.

8. Click **OK** to enable your patrol read selections.

   **Note:** Patrol read does not report on its progress while it is running. The patrol read status is reported only in the event log.

9. Click **Go** to enable these Patrol Read options.

   To start a patrol read without changing the patrol read properties, follow these steps:
   1. Click a controller icon in the left panel of the MegaRAID Storage Manager main menu screen.
   2. Select **Go To->Controller->Start Patrol Read** in the menu bar or right-click a controller and select **Start Patrol Read** from the menu.
   3. When prompted, click **Yes** to confirm that you want to start a patrol read.

**Patrol Read Task Rates**

You have the option to change the patrol read **task rate**. The task rate determines the amount of system resources that are dedicated to a patrol read when it is running. LSI recommends, however, that you leave the patrol read task rate at its default setting.

If you raise the task rate above the default, the foreground tasks will run more slowly and it may seem that the system is not responding. If you lower the task rate below the default, rebuilds and other background tasks might run very slowly and might not complete within a reasonable time. For more information, about the patrol read task rate, see **Changing Adjustable Task Rates**.
Monitoring Virtual Drives

When the MegaRAID Storage Manager software is running, you can see the status of all virtual drives. If a virtual drive is operating normally, the icon looks like this: ⚫. Color-coded circles appear next to the icon to indicate the following:

- **Green**: The server is operating properly.
- **Yellow**: The server is running in a partially degraded state (for example, if a drive has failed); the data is still safe, but data could be lost if another drive fails.
- **Orange**: The server is running in a degraded state.
- **Red**: The server storage configuration has failed.

When the Logical tab is selected, the panel on the left shows which drives are used by each virtual drive. The same drive can be used by multiple virtual drives.

To display complete virtual drive information, click the Logical tab in the left panel, and click on a virtual drive icon in the left panel. The properties appear in the right panel as shown in the following figure. The RAID level, strip size, and access policy of the virtual drive are set when the virtual drive is configured.

**Figure 64 Virtual Drive Properties**

You can change the read policy, write policy, and other virtual drive properties. To change these properties, see Changing Virtual Drive Properties.
Note: You can change the Read Policy, Write Policy, and other virtual drive properties by selecting the virtual drive icon and then selecting Go To->Virtual Drive ->Set Virtual Drive Properties in the menu bar.

If the drives in the virtual drive are in a disk enclosure, you can identify them by making their LEDs blink. To identify the drives, follow these steps:

1. Click the virtual drive icon in the left panel.
2. Either select Go To->Virtual Drive->Start Locating Virtual Drive, or right-click a virtual drive and select Start Locating Virtual Drive from the menu.
   The LEDs on the drives in the virtual drive start blinking (except for the hot spare drives).
3. To stop the LEDs from blinking, select Go To->Virtual Drive->Stop Locating Virtual Drive or right-click a virtual drive and select Stop Locating Virtual Drive from the menu.

Monitoring Enclosures

When the MegaRAID Storage Manager software is running, you can see the status of all enclosures connected to the server by selecting the Physical tab in the left panel. If an enclosure is operating normally, the icon looks like this: 
If an enclosure is not functioning normally—for example, if a fan has failed—an orange, yellow, or red circle appears to the right of the icon.

Information about the enclosure appears in the right panel when you select the Properties tab on the main menu screen. A graphical display of enclosure information appears when you select the Graphical View tab.

The display in the center of the screen shows how many slots of the enclosure are actually populated by the drives and the lights on the drives show the drive status. The information on the right shows you the status of the temperature sensors, fans, and power supplies in the enclosure.

To view the enclosure properties, in the physical view click on the Enclosure node. The Enclosure Properties are displayed, as shown in the following figure.

Figure 65 Enclosure Properties

<table>
<thead>
<tr>
<th>Vendor ID</th>
<th>Dell</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enclosure ID</td>
<td>5</td>
</tr>
<tr>
<td>Enclosure Type</td>
<td>SIE</td>
</tr>
<tr>
<td>Enclosure Model</td>
<td>MD2000z</td>
</tr>
<tr>
<td>Enclosure Location</td>
<td>123456</td>
</tr>
<tr>
<td>Firmware Version</td>
<td>A.04</td>
</tr>
<tr>
<td>Serial Number</td>
<td>D02345676</td>
</tr>
<tr>
<td>Connector</td>
<td>Port A</td>
</tr>
<tr>
<td>Number of Slots</td>
<td>15</td>
</tr>
</tbody>
</table>

Monitoring Battery Backup Units

When the MegaRAID Storage Manager software is running, you can monitor the status of all of the BBUs connected to controllers in the server. If a BBU is operating normally, the icon looks like this: 
If a BBU fails, a red dot appears next to the icon.
To show the properties for a BBU, perform the following steps:

1. On the main menu screen, click the **Physical** tab to open the physical view.
2. Select the BBU icon in the left panel.

The BBU properties appear in the right panel. The BBU properties include the following:

- The number of times the BBU has been recharged (cycle count).
- The full capacity of the BBU, plus the percentage of its current state of charge, and the estimated time until it will be depleted.
- The current BBU temperature, voltage, current, and remaining capacity.
- If the battery is charging, the estimated time until it is fully charged.
- The battery state, which says if it is in operational state.
- If battery replacement is required.
- The BBU retention time, which gives the total number of hours the battery can support the current capacity reserve.

The BBU Properties are displayed, as shown in the following two figures.

**Figure 66** Battery Backup Unit Properties for iBBU Battery

**Figure 67** Battery Backup Unit Properties for TMM-C Battery

**Battery Learn Cycle**

Learn cycle is a battery calibration operation that is performed by the controller periodically to determine the condition of the battery. You can start battery learn cycles manually or automatically.
To choose automatic battery learn cycles, enable automatic learn cycles. To choose manual battery learn cycles, disable automatic learn cycles.

If you enable automatic learn cycles, you can delay the start of the learn cycles for up to 168 hours (7 days). If you disable automatic learn cycles, you can start the learn cycles manually, and you can choose to receive a reminder to start a manual learn cycle.

### Setting Learn Cycle Properties

To set the learn cycle properties, perform the following steps:

1. Click the **Physical** tab to open the Physical view.
2. Select the **BBU** icon in the left panel.
3. Select **Go To->BBU->Set Learn Cycle Properties**. The Set Learn Cycle Properties window appears, as shown in the following figure.

![Set Learn Cycle Properties](image)

4. Select one of the two automatic learn cycles:
   - Select the **Enable** radio button to enable an automatic learn cycle.
   - Select the **Disable** radio button to disable an automatic learn cycle.

5. You can delay the start of the next learn cycle up to 7 days (168 hours) by specifying the hours in the **Delay scheduled learn cycle by** field.

6. Select the **Remind me when to start a learn cycle** check box to receive a reminder to start a manual learn cycle.

**Note:** After selecting **Disable**, if you select **Enable**, the controller firmware resets the battery module properties to initiate an immediate battery learn cycle. The **Next Learn cycle** field (in Figure 66 or Figure 67) will not be updated until the battery relearn is completed. Once the relearning cycle is completed, the value in the **Next Learn cycle** field will display the new date and the time of the next battery learning cycle.
Starting a Learn Cycle Manually

To start the learn cycle properties manually, perform the following steps:

1. Click the **Physical** tab to open the Physical view.
2. Select the **BBU** icon in the left panel.
3. Select **Go To->BBU->Start Learn Cycle**.

Another way to start the learn cycle is to right-click the **BBU** icon and select **Start Learn Cycle** from the pop-up menu.

Monitoring Rebuilds and Other Processes

The MegaRAID Storage Manager software allows you to monitor the progress of rebuilds and other lengthy processes in the Group Show Progress window. To open this window, follow these steps:

Follow these steps to monitor the progress of these operations.

1. Open the show progress window, by selecting **Manage->Show Progress** on the menu bar.

**Figure 69** Group Show Progress Menu

The Group Show Progress window appears, as shown in the following figure.
The Group Show Progress window displays a percent-complete indicator for drive rebuilds. Rebuilds may take a long time to complete and cannot be aborted. An up-arrow appears above the drive icon while it is being rebuilt.

Operations on virtual drives appear in the left panel of the window, and operations on drives appear in the right panel. The type of operations that appear in this window are as follows:

- Initialization of a virtual drive (see Initializing a Virtual Drive)
- Rebuild (see Rebuilding a Drive)
- Consistency check (see Running a Consistency Check)

A Modify Drive Group process cannot be aborted. To abort any other ongoing process, click the **Abort** button next to the status indicator. Click **Abort All** to abort all ongoing processes. Click **Close** to close the window.
Maintaining and Managing Storage Configurations

This section explains how to use the MegaRAID Storage Manager software to maintain and manage storage configurations. You must log on to the server in Full Access mode in order to perform these maintenance and management tasks. This section has the following topics:

- Initializing a Virtual Drive
- Running a Group Initialization
- Running a Consistency Check
- Rebuilding a Drive
- Marking a Drive Offline or Missing
- Removing a Drive
- Upgrading the Firmware

Initializing a Virtual Drive

When you create a new virtual drive with the Configuration Wizard, you can select the Quick Init or Full Init option to initialize the disk immediately. However, you can select No Init if you want to initialize the virtual drive later.

To initialize a virtual drive after the configuration process, follow these steps:

1. Click the Logical tab in the left panel of the MegaRAID Storage Manager main menu screen, and click the icon of the virtual drive that you want to initialize.
2. Select Go To->Virtual Drive->Start Initialization. The Initialize dialog appears.
3. Select the virtual drive or drives to initialize.

   Caution: Initialization erases all data on the virtual drive. Make sure to back up any data you want to keep before you initialize. Make sure the operating system is not installed on the virtual drive you are initializing.
4. Select the Fast Initialization check box if you want to use this option.
   Fast Initialization quickly formats the virtual drive by writing zeros to the first few sectors of the drives in the virtual drive. Regular initialization takes longer, depending on the number and the size of the drives in the virtual drive.
   If you leave the box unchecked, the MegaRAID Storage Manager software will run a Full Initialization on the virtual drive. For more information, see Changing Virtual Drive Properties.
5. Click Start to start the initialization. You can monitor the progress of the initialization. For more information, see Changing Virtual Drive Properties.

Running a Group Initialization

Initialization prepares the storage medium for use. You can run an initialization on multiple drives at one time. Follow these steps to run a group consistency check.
1. Select **Manage->Initialize**. The Group Initialization dialog appears, as shown in the following figure.

**Figure 71  Group Initialization**

![Group Initialization](image)

2. Either check the virtual drives on which to run the initialization on or click **Select All** to select all the virtual drives.

3. Click **Start**.

You can monitor the progress of the group initialization. For more information, see Monitoring Rebuilds and Other Processes.

---

**Running a Consistency Check**

You should periodically run a consistency check on fault-tolerant virtual drives (RAID 1, 5, 6, 10, 50, or 60 configurations; RAID 0 does not provide data redundancy). A consistency check scans the virtual drive to determine whether the data has become corrupted and needs to be restored.

For example, in a system with parity, checking consistency means computing the data on one drive and comparing the results to the contents of the parity drive. You must run a consistency check if you suspect that the data on the virtual drive might be corrupted.

**Note:** Make sure to back up your data before running a consistency check if you think the data might be corrupted.

To run a consistency check, first set the consistency check properties and then schedule the consistency check. The following sections explains how to:
• Set the properties – Setting the Consistency Check Settings
• Schedule the check – Scheduling a Consistency Check
• Run the consistency check – Running a Group Consistency Check

**Setting the Consistency Check Settings**

Follow these steps to set the properties for a consistency check:

1. Click the Physical tab or Logical tab in the main menu window and select a controller.
2. Select Go To->Controller->Set Consistency Check Properties, as shown in the following figure.

**Figure 72  Set Consistency Check Properties Option**

The Set Consistency Check Properties dialog appears, as shown in the following figure.
3. Choose one of the two options:
   - **Stop Consistency Check on Error**: The RAID controller stops the consistency check operation if the utility finds an error.
   - **Continue Consistency Check and Fix Errors**: The RAID controller continues the consistency check if the utility finds an error, and then fixes the error.

4. Click **Ok**.

### Scheduling a Consistency Check

Follow these steps to set the properties for a consistency check:

1. Click the **Physical** tab or **Logical** tab in the main menu screen, and select the controller.
2. Select **Go To->Controller->Schedule Consistency Check**. The Schedule Consistency dialog appears, as shown in the following figure.
3. Perform the following steps to schedule the consistency check:
   a. Select how often to run the consistency check from the drop-down menu. You can click Advanced for more detailed date options.
   b. (Optional) Select the Run consistency check continuously check box.
   c. Select the month, day, and year on which to start the consistency check.
   d. Select the time of day to start the consistency check.

4. Click Ok.

   You can monitor the progress of the consistency check. For more information, see Monitoring Rebuilds and Other Processes.

Running a Group Consistency Check

You can run a consistency check on multiple drives at one time. Follow these steps to run a group consistency check:

1. Select Manage->Check Consistency. The Group Consistency Check dialog appears, as shown in the following figure.
2. Either select the virtual drives on which to run the consistency check on, or click **Select All** to select all of the virtual drives.

3. Click **Start**.

You can monitor the progress of the group consistency check. For more information, see [Monitoring Rebuilds and Other Processes](#).

## Scanning for New Drives

You can use the Scan for Foreign Configuration option to find drives with foreign configurations. A foreign configuration is a RAID configuration that already exists on a replacement set of physical disks that you install in a computer system. In addition, if one or more drives are removed from a configuration, by a cable pull or drive removal, for example, the configuration on those drives is considered a foreign configuration by the RAID controller. Drives that are foreign are listed on the physical drives list with a special symbol in the MegaRAID Storage Manager software.

The utility allows you to import the existing configuration to the RAID controller or clear the configuration so you can create a new configuration using these drives. You can preview the foreign configuration before you decide whether to import it.

The MegaRAID Storage Manager software normally detects newly installed drives and displays icons for them in the MegaRAID Storage Manager main menu window. If for some reason the MegaRAID Storage Manager software does not detect a new drive (or drives), you can use the Scan for Foreign Configuration command to find it.
Follow these steps to scan for a foreign configuration:

1. Select a controller icon in the left panel of the MegaRAID Storage Manager window.
2. Select Go To->Controller->Scan for Foreign Configuration.

   If the MegaRAID Storage Manager software detects any new drives, it displays a list of them on the screen. If not, it notifies you that no foreign configuration is found.
3. Follow the instructions on the screen to complete the drive detection.

---

Rebuilding a Drive

If a drive in a redundant virtual drive (RAID 1, 5, 6, 10, 50, or 60) fails, the MegaRAID Storage Manager software automatically rebuilds the data on a hot spare drive to prevent data loss. The rebuild is a fully automatic process, so it is not necessary to issue a Rebuild command. You can monitor the progress of drive rebuilds in the Group Show Progress window. To open this window, select Group Operations->Show Progress.

If a single drive in a RAID 1, RAID 5, RAID 10, or RAID 50 virtual drive fails, the system is protected from data loss. A RAID 6 virtual drive can survive two failed drives. A RAID 60 virtual drive can survive two failed drives in each span in the drive group. Data loss is prevented by using parity data in RAID 5, RAID 6, RAID 50, and RAID 60, and data redundancy in RAID 1 and RAID 10.

The failed drive must be replaced, and the data on the drive must be rebuilt on a new drive to restore the system to fault tolerance. (Or the data can be rebuilt on the failed drive, if the drive is still operational.) If dedicated hot spares or global hot spare disks are available, the failed drive is rebuilt automatically without any user intervention.

A red circle to the right of the drive icon indicates that a drive has failed. A yellow circle appears to the right of the icon of the virtual drive that uses this drive which indicates that the virtual drive is in a degraded state; the data is still safe, but data could be lost if another drive fails.

Follow these steps to rebuild a drive:

1. Right-click the icon of the failed drive and select Rebuild.
2. Click Yes when the warning message appears. If the drive is still good, a rebuild will start.

   You can monitor the progress of the rebuild in the Group Show Progress window by selecting Manage->Show Progress. If the drive cannot be rebuilt, an error message appears. Continue with step 3.
3. Shut down the system, disconnect the power cord, and open the computer case.
4. Replace the failed drive with a new drive of equal capacity.
5. Close the computer case, reconnect the power cord, and restart the computer.
6. Restart the MegaRAID Storage Manager software.

   When the new drive spins up, the drive icon changes back to normal status, and the rebuild process begins automatically. You can monitor the progress of the rebuild in the Group Show Progress window by selecting Manage->Show Progress.

If you want to force a drive into Fail status to trigger a rebuild, right-click the drive icon, and select Make Drive Offline. A red circle appears next to the drive icon. Right-click the icon, and select Rebuild from the pop-up menu. A drive rebuild cannot be aborted.
A drive rebuild is also started if you select **Make Drive Online** from the pop-up menu.

**New Drives Attached to a MegaRAID Controller**

When you insert a new drive on a MegaRAID system and if the inserted drive does not contain valid DDF metadata, the drive displays as JBOD for MegaRAID entry-level controllers, such as the SAS 9240-4i/8i. If the drive does contain valid DDF metadata, its drive state is Unconfigured Good.

A new drive in JBOD drive state is exposed to the host operating system as a stand-alone drive. Drives in JBOD drive state are not part of the RAID configuration because they do not have valid DDF records. The operating system can install and run anything on JBOD drives.

Automatic rebuilds always occur when the drive slot status changes, for example, when you insert a drive or remove a drive, so that a hot spare can be used. However, a new drive in JBOD drive state (without a valid DDF record), does not perform an automatic rebuild.

To start an automatic rebuild on the new JBOD drive, you have to change the drive state from JBOD to Unconfigured Good. (Rebuilds start on Unconfigured Good drives only.) After you set the drive state to Unconfigured Good, the drive state information always remains on the drive, and you can use the drive for configuration.

**Marking a Drive Offline or Missing**

If a drive is currently part of a redundant configuration and you want to use it in another configuration, you can use the MegaRAID Storage Manager commands to remove the drive from the first configuration and change the drive state to Unconfigured Good.

**Caution:** After you perform this procedure, *all data on that drive is lost.*

To remove the drive from the configuration without harming the data on the virtual drive, follow these steps:

1. In the MegaRAID Storage Manager main menu, select **Go To->Physical Drive->Make Drive Offline**.
   
   The drive status changes to Offline.

2. Select **Go To->Physical Drive->Mark Drive as Missing**.
   
   The drive status changes to Unconfigured Good.

   **Caution:** After you perform this step, the data on this drive is no longer valid.

3. If necessary, create a hot spare drive for the virtual drive from which you have removed the drive. For information on creating a hot spare drive, see **Creating Hot Spares**.

   When a hot spare is available, the controller rebuilds the data on the virtual drive. You can now use the removed drive for another configuration. If the MegaRAID Storage Manager software detects that a drive in a virtual drive has failed, it makes the drive offline. If this happens, you must remove the drive and replace it. You cannot make the drive usable for another configuration by using the **Mark physical disk as missing** and **Rescan** commands.
Removing a Drive

You may sometimes need to remove a non-failed drive that is connected to the controller. For example, you may need to replace the drive with a larger drive. Follow these steps to remove a drive safely:

1. Click the icon of the drive in the left panel, and click the Operations tab in the right panel.
2. Select Prepare for Removal, and click Go.
3. Wait until the drive spins down and remove it.
   If you change your mind, select Undo Prepare for Removal and click Go.

Upgrading the Firmware

The MegaRAID Storage Manager software enables you to easily upgrade the controller firmware. To avoid data loss because of dirty cache on the controller, the utility forces the virtual disks into Write through mode after a firmware upgrade. It is in this mode until the server reboots. In the Write through mode, the controller sends a data transfer completion signal to the host when the disk subsystem has received all the data in a transaction. This way, in case of a power outage, the controller does not discard the dirty cache.

Follow these steps to upgrade the controller firmware:

1. In the left panel of the MegaRAID Storage Manager main menu window, click on the icon of the controller you need to upgrade.
2. On the main menu screen, select Go To->Controller->Update Controller Firmware.
3. Click Browse for the .rom flash update file, as shown in the following figure.

Figure 76 Locate the Controller Firmware File

![Figure 76 Locate the Controller Firmware File](image)

4. After you locate the file, click Open.
   The MegaRAID Storage Manager software displays the version of the existing firmware and the version of the new firmware file. The MegaRAID Storage Manager software does not allow you to overwrite a newer version of the firmware with an older version.
5. When you are prompted to indicate whether you want to upgrade the firmware, click Yes.
   The controller is updated with the new firmware code contained in the .rom file.
6. Reboot the system after the new firmware is flashed.

   The new firmware does not take effect until reboot.
Using the MegaRAID Advanced Software

The MegaRAID Storage Manager software supports advanced software features that offer improved performance, data protection, and availability.

Note: Only certain RAID controllers support advanced software features. Make sure that your RAID controllers support the advanced software features before you use the procedures in this section.

The MegaRAID advanced software includes the following features:

- MegaRAID Recovery
- MegaRAID CacheCade™
- MegaRAID FastPath™
- MegaRAID RAID 6
- MegaRAID RAID 5

This section contains the following topics:

- MegaRAID Software Licensing
- MegaRAID Recovery
- CacheCade - SSD Caching Advanced Software Option
- FastPath Advanced Software
- LSI SafeStore Encryption Services

MegaRAID Software Licensing

The MegaRAID software licensing authorizes you to enable the MegaRAID advanced software features present in the MegaRAID Storage Manager application. You need to obtain the activation key to enable and use the advanced software features present in the controller. You can also implement the rehosting process by configuring the key vault, if you want to transfer the advanced features from one controller to another.

Managing MegaRAID Advanced Software

The MegaRAID Advanced Software wizard allows you to use the advanced software features. Perform the following steps to enable the activation key to use the advanced features:

1. Select the Physical view or the Logical view tab in the left panel of the MegaRAID Storage Manager window, and click a controller icon.
2. Choose either one of the following options:
   a. Select Go To -> Controller -> Manage MegaRAID Advanced Software Options.
   b. Click Manage MegaRAID Advanced Software Options from the dashboard under the feature portlet.

The Manage MegaRAID Advanced Software Options wizard appears.
• If none of the advanced software options present in the controller are in a boot mode, Figure 77 appears.

• If even one of the advanced software options present in the controller is in a boot mode, Figure 78 appears. You cannot activate any advanced software option from this window as this is a view-only window.

Figure 77  Manage MegaRAID Advanced Software Options
The **Activated MegaRAID Advanced Software** Options table consists of **Advanced Software Option**, **License**, and **Mode** columns.

- The **Advanced Software** Option column displays the list of advanced softwares present in the controller.
- The **License** column displays the license details for the list of advanced softwares present in the **Advanced Software** column. The license details validate if the software is under trial period, or if it can be used without any trial period (Unlimited).
- The **Mode** column displays the current status of the advanced software. The current status can be Secured, Not secured, or Factory installed.

**Note:** The **Mode** column appears only if the key vault is present.

3. Click the link [LSI Advanced Software License Management Portal](http://www.lsi.com/channel/products/advanced_software) to obtain the license authorization code and activation key.


Both the **Safe ID** field and the **Serial Number** field consists of a pre-defined value generated by the controller. Alternatively, you can copy the value and paste it in text box for the applicable field.

4. Click **Activate**.
The **Activate MegaRAID Advanced Software – Choose Method** wizard appears as shown in the following figure.

**Activation Key**

**Figure 79  Activate MegaRAID Advanced Software – Choose Method**

Perform the following steps to enter the Activation key:

1. Click the **LSI Advanced Software License Management Portal** link to obtain a License Authorization Code (LAC) and an Activation Key.
2. Use any one of the following options to enter the activation key:
   a. Select the **Enter an Activation Key** option, and enter the *activation key* in the **Activation Key** field.
   b. Select **Select an Activation Key file** and click **Browse** to get the path of the *activation Key* file.
3. Click **Next**.

After you click **Next**, the **Activate MegaRAID Advanced Software – Summary** wizard appears, as shown in the following figure.

**ELSE**

Based on some scenarios, the application responds by displaying corresponding messages as shown in **Application Scenarios and Messages**.

**Advanced MegaRAID Software Status Summary**

After you enter the *activation key* and click **Next**, the **Activate MegaRAID Advanced Software – Summary** wizard (as shown in the following figure) displays the list of the advanced software options along with the *former status* and the *new status* in the controller.

- The **Advanced Software** column displays the currently available software in the controller.
• The **Former Status** column displays the status of the available advanced software prior to entering the activation key.

• The **New Status** column displays the status of the available advanced software, after entering the activation key.

**Figure 80  Activate MegaRAID Advanced Software – Summary**

4. Click **Finish**.

   The status of the advanced software is enabled, and the advanced features will be secured in the Key Vault.

**Application Scenarios and Messages**

   – **Scenario # 1**
     
     If you enter an *invalid* activation key, the following message appears.

   **Figure 81  Invalid Activation Key**

      – **Scenario # 2**

      If you enter an *incorrect* activation key file, the following message appears.

   **Figure 82  Incorrect Activation Key**

      – **Scenario # 3**

      If you enter an *incorrect* activation key, and if there is a mismatch between the activation key and the controller, the following message appears.
Figure 83  Activation Key Mismatch

Note: Entering a space in the Activation Key field disables the Next button in Figure 79.

If you click Cancel in the Activate MegaRAID Advanced Software – Choose Method, as shown in Figure 79, the following confirmation dialog appears.

Figure 84  Confirmation Dialog Box

Activating an Unlimited Key Over a Trial Key

When you activate an unlimited key over a trial key, the message, "The existing trial key will be deactivated and all the advanced software associated with it will be disabled", appears (indicated in pink text in the following figure).

Figure 85  Activating an Unlimited Key over a Trial Key

Activating a Trial Software

When you activate a trial software, a message “This trial software expires in 30 days” is displayed (indicated in yellow text in the following figure).
Activating an Unlimited Key

When you activate an unlimited key or a trial key, a message “Review the summary and go back if you need to make corrections” is displayed as shown in the following figure.

Reusing the Activation Key

If you are using an existing activated key, the features have been transferred to the Key Vault, and a message appears, as shown in the following figure.
Securing Advanced MegaRAID Software

When you want to transfer the advanced software from the controller to the Key Vault, use the Securing Advanced MegaRAID Software - Confirmation wizard. This wizard is conditional and will appear only when a Key Vault and unsecured keys exist.

Use any one of the following options to view the Securing Advanced MegaRAID Software - Confirmation wizard.

- Select the Physical View tab in the left panel of the MegaRAID Storage Manager main menu, and click a controller icon.
- Select Go To -> Controller -> Manage MegaRAID Advanced Software Options wizard.

After you select the check box, the Yes button is enabled. This situation implies that the advanced software is secured in the Key Vault.

If the advanced software is not secured, the Secure MegaRAID Advanced Software - Confirmation dialog box appears as shown in Figure 84.

Configuring Key Vault (Re-hosting Process)

Re-hosting is a process of transferring the advanced software features from one controller to another. To implement the re-hosting process, you need to configure the Configure Key Vault button in the Manage MegaRAID Software Options wizard, as shown in Figure 77.

1. Choose any one of the following options to configure the Key Vault.
• Click **Configure Key Vault** in the **Manage MegaRAID Advanced Software** options wizard from **Figure 77**.
• Select **Go To -> Controller -> Manage Premium Feature**.

The **Configure Key Vault-Confirm Re-Hosting Process** wizard appears, as shown in the following figure.

**Figure 90 Configure Key Vault**

2. Select the **I acknowledge that I have completed the re-hosting process in the LSI Advanced Software License Management Portal** check box.

3. Click **Next**.

   The **Configure Key Vault- Secure Advanced Software Options** wizard appears as shown in the following figure.

**Figure 91 Configure Key Vault - Secure Advanced Software Options**
4. Click Finish and the advanced software options are secured in the key vault.

**Note:** The Next button in the Configure Key Vault wizard is enabled only when you select the check box.

This wizard is conditional and will pop-up only if the rehosting process is necessary when the key vault is present and unsecured keys are also present, both at the same time.

**Re-hosting Complete**

If you want to transfer the advanced software options from one controller to another, use the rehosting process. The re-hosting process ensures that these options are secured in the Key Vault. You have to configure the Key Vault in order to complete the re-hosting process.

1. Use any one of the following options to complete the re-hosting process.
   - Click the Configure Key Vault button from the Manage MegaRAID Advanced Software Options wizard.
   - Select Go To -> Controller -> Manage MegaRAID Advanced Software Options wizard.
     The Re-hosting Process - Complete wizard appears as shown in the following figure.

**Figure 92 Confirm Re-hosting**

2. Select the I acknowledge that I have completed the re-hosting process in the LSI Advanced Software License Management Portal check box if you want to complete the re-hosting process.
   This setting ensures that the advanced software features are transferred to the controller.

3. Click Cancel if you do not want to complete the re-hosting process.

**Deactivate Trial Software**

When you want to deactivate the trial software, use the Deactivate All Trial Software wizard.
Perform the following steps to enable the deactivate trial software button.

1. Click **Deactivate All Trial Software** in the **Manage MegaRAID Advanced Software Options** wizard as shown in **Figure 77**.

   **The Deactivate All Trial Software - Confirmation** dialog appears as shown in the following figure.

   ![Deactivate All Trial Software - Confirmation](image)

2. Select the **Confirm** check box, if you want to deactivate the software applications that are being used with a trial key.

3. Click **Yes** button.

   The trial software is deactivated.

---

**MegaRAID Recovery**

MegaRAID Recovery, also known as Snapshot, offers a simplified way to recover data and provides automatic protection for the boot volume. You can use the Recovery feature to take a snapshot of a volume and to restore a volume or a file. The Snapshot functionality allows you to capture data changes to the volume and if the data is deleted accidentally or maliciously, you can restore the data from the view or roll back to a snapshot at a previous point-in-time (PiT). MegaRAID Recovery supports up to eight snapshots of PiTs for each volume.

Each Recovery PiT volume snapshot is typically a fraction of the original volume size, because it tracks only the changes that are made to a volume after the PiT is created. Disk space for PiTs is reserved in the Snapshot Repository virtual drive, and the PiT is expanded in small increments as new data is written to the volume. Multiple PiTs of each volume can be retained online, enabling frequent snapshots to be stored in a space-efficient manner.

This section contains the following topics:

- Enabling the Recovery Advanced Software
- Snapshot Repository
- Selecting the Virtual Drive
- Scheduling Snapshots
- Editing Snapshots
- Snapshot Base Details
Enabling the Recovery Advanced Software

You can enable the Recovery advanced software in the MegaRAID Storage Manager software. When you enable Recovery, you create two virtual drives, one as a Snapshot Base or a source and the other as a Snapshot Repository. The base virtual drive contains the data that is stored in the repository virtual drive.

Follow these steps to enable MegaRAID Recovery.

1. Click the **Logical** tab on the main menu window for the Logical view.
2. Select and highlight a virtual drive from the list of virtual drives.
   
   This virtual drive is the Snapshot Base virtual drive.

   **Note:** A base virtual drive and a repository virtual drive can be associated with the same drives or a common set of drives, or the two virtual drives can be located on two completely separate set of drives. Using a separate set of drives for the base virtual drive and the repository virtual drives provides a performance advantage over using a common set of drives.

3. Select **Go To -> Virtual Drive -> Enable MegaRAID Recovery** on the menu bar, as shown in the following figure.
The Enable MegaRAID Recovery Wizard appears, as shown in the following figure. This wizard allows you to select the virtual drive to use as the snapshot repository.

**Snapshot Repository**

You can select an existing virtual drive, or create a new virtual drive to use as the snapshot repository.

1. Use any one of the options to select or create a new virtual drive.
   - Select the virtual drive to use as the Snapshot Repository in the **Snapshot Repository** field from the Enable MegaRAID Recovery Wizard wizard as shown in the following figure.
   - Click **Create New** to create a new virtual drive to use as the Snapshot Repository.

When you create a new virtual drive, the newly created virtual drive gets appended to the existing rows in the **Snapshot Repository** field.
The **Snapshot Repository** field displays the details of the default virtual drives existing in the system, if there are any.

- The **Name** column displays the name of the virtual drive.
- The **Status** column displays the status of the virtual drive.
- The **Available Capacity** column displays the available capacity on the virtual drive.
- The **Total Capacity** displays the total capacity of the virtual drive.

If the default virtual drives do not exist in the system, the **Snapshot Repository** field columns are blank.

The status of the virtual drive can be optimal, degraded, or partially degraded.

2. In the **Select Capacity** field, use the drop-down selector to select the appropriate capacity to use for changes to the base virtual drive.

The capacity is dependent on how write-intensive the application is that you are taking snapshots of. The available capacity is the largest free block of capacity on the snapshot repository virtual drive.

**Note:** Please refer to the tips provided for allocating capacity in the following figure.

If you designate all of the capacity for the virtual drive repository, you cannot use the same virtual drive as a repository for other volumes.
Selecting the Virtual Drive

You can select the virtual drive to use as the snapshot repository and also allocate the capacity for the virtual drive from the snapshot repository.

Follow these steps to select the virtual drive in the **Snapshot Repository** field.

1. Select the virtual drive to be used as the snapshot repository to hold the snapshot information. The selected virtual drive is highlighted as shown in the following figure.

![Enable MegaRAID Recovery Wizard - Displaying the Selected Virtual Drive](image)

**Figure 96** Enable MegaRAID Recovery Wizard - Displaying the Selected Virtual Drive

2. In the **Select Capacity** field, use the drop-down selector to select the appropriate capacity to use for changes to the base virtual drive.

3. Click **Next**. The **Enable MegaRAID Recovery wizard - Create Snapshot Schedule** wizard appears. This wizard allows you to schedule snapshots.

Scheduling Snapshots

You can select an existing snapshot schedule or create a new snapshot schedule for the virtual drives.

Follow these steps to schedule snapshots.

1. Select any one of the options shown in the **Enable MegaRAID Recovery - Create Snapshot Schedule** wizard, as shown in the following figure, to schedule snapshots.
Figure 97  Enable MegaRAID Recovery - Create Snapshot Schedule

- Add virtual drive to existing schedule - This option allows you to add a virtual drive to a pre-existing schedule already defined in the system.
  
  The **Schedule** field displays the schedule details of the virtual drive.
  
  - The **Frequency** column displays the frequency of the snapshot schedule. The frequency of the snapshot can be daily or weekly.
  
  - The **Next Snapshot** column displays the date and time of the next scheduled snapshot.
  
  - The **Scheduled Virtual Drives** column represents the details of the default virtual drives present in the system.

- Create new schedule - This option allows you to create a new schedule to the virtual drive.
  
  - In the **Frequency** field, use the drop-down selector to select the frequency of the snapshot (daily or weekly).
  
  - In the **Time** field, use the drop-down selector to select the time of the scheduled snapshot.

- **Do not schedule any automatic snapshots** - This option prevents you from capturing automatic snapshots from the system.

2. Click **Next**. The **Enable MegaRAID Recovery - Editing Snapshot Properties** wizard appears, as shown in the following figure. You can edit the settings for automatic snapshots.

**Editing Snapshots**

You can edit the property settings that are already defined for the automatic snapshots using the options, as shown in the following figure.
1. Select any one of the options to edit snapshots.
   a. Automatically delete the oldest snapshot
      If you choose this option, the oldest snapshot present in the system automatically gets deleted.
   b. Stop taking snapshots
      If you choose this option, the application stops taking snapshots.
   c. Take a snapshot on every reboot (recommended for boot virtual drives)
      To use this option, select the Take a snapshot on every reboot (recommended for boot virtual drives) check box.
      This option provides you a snapshot taken on boot after each successful shutdown. You can use this snapshot of the boot virtual drive to restore the operating system on the virtual drive in case the virtual drive becomes corrupted.

2. Click Finish.
   A Confirm Enable Snapshots dialog appears. This dialog prompts you to make sure whether you want to enable snapshots on a virtual drive or not.

Figure 99   Confirm Enable Snapshots
3. If the answer is Yes, select the Confirm check box.

When you select the check box, the Yes button gets enabled. The snapshots get enabled on the virtual drive.

This virtual drive becomes a snapshot repository. Use it only for storing snapshot-related data.

If you click No, the snapshots will not be enabled on the selected virtual drive.

Note: After you enable snapshots on this virtual drive, you cannot change the allocated percentage of capacity or the snapshot repository without first disabling snapshots and losing any snapshot data.

**Snapshot Base Details**

You can view the snapshot base details of the virtual base drive.

Follow these steps to view the details of the snapshot of the virtual base drive.

1. Select the Logical tab on the main menu window from the MegaRAID Storage Manager software.

2. Click a base virtual drive in the left frame.

   After you click the base virtual drive, in the right frame you can view the base virtual drive information in the Properties tab under Snapshot Base Details (highlighted in pink).

**Figure 100  Snapshot Base Details**

![](image)

**Manage Snapshots**

You can create snapshots, delete snapshots, create views, and also edit, pause or delete schedules using the Manage Snapshots wizard.

1. Select Go To -> Virtual Drive -> Manage Snapshot wizard on the menu bar, as shown in the following figure.
2. You can edit the snapshot schedule by clicking **Edit Schedule**, pause the snapshot schedule by clicking **Pause**, and delete the snapshot schedule by clicking **Delete**.

The **Snapshot** field displays the snapshot details.
- The **Name** column displays the name of the snapshot.
- The **Status** column displays the status of the snapshot.
- The **Capacity Used** column displays the capacity consumed by the snapshot.

You can create the snapshot button by clicking **Create Snapshot**, and delete the snapshot by clicking **Delete Snapshot**.

In the **View Details** field, you can create a view by clicking **Create View** and edit the settings for automatic snapshots by clicking **Advanced**.

**Editing Schedule**

You can edit the schedule using the **Edit Schedule** screen. You can change the frequency of the snapshot, the day in which the snapshot needs to be taken, and the time during which the snapshot needs to be taken.

1. Click **Edit Schedule** in the Manage Snapshots wizard in **Figure 101**, if you want to edit the snapshot schedule.

   The **Edit Schedule** screen appears, as shown in the following figure.
Figure 102  Edit Schedule

In the **Frequency** field, use the drop-down selector to edit the frequency of the snapshot already taken. The frequency can be daily or weekly.

In the **Day** field, use the drop-down selector to edit the day of the snapshot already taken. The days can be from Monday through Sunday.

In the **Time** field, use the drop-down selector to edit the time of the snapshot already taken.

After you select all of the above fields, the virtual drives matching these fields will appear in the **Virtual drives on this schedule** check box.

2. Select the **Virtual drives on this schedule** check box and click **OK**.

The virtual drive details are edited.

**Advanced Settings**

You can edit the settings for the automatic snapshots. You can automatically delete the oldest snapshot, or stop taking snapshots, or take a snapshot on every reboot.

1. Click **Advanced** in the **Manage Snapshots wizard**, as shown in **Figure 101**.

   The Advanced screen appears as shown in the following figure.

![Advanced Settings](image)

You can edit the settings by selecting one of the following options.
– **Automatically delete the oldest snapshot** option, if you want to delete the oldest snapshot
– **Stop taking snapshots** option, if you want to stop taking snapshots
– **Take a snapshot on every reboot (recommended for boot virtual drive)** option, if you want a snapshot on every reboot.

2. Click **OK**.
   The settings are edited.

**Create View Using Manage Snapshots Wizard**

You can create views using the **Create View** button present in the **Manage Snapshots** area under the **View Details** field. The view provides the snapshot details of the virtual drive available at that particular time.

Follow these steps to create views of the snapshots.

1. Click **Create View** button in the **Manage Snapshots** wizard.
   The **Create View** dialog appears as shown in the following figure.

![Create View](image)

2. In the **View name** field, enter the name of the view.
3. In the **Write capacity** field, use the drop-down selector to allocate capacity for writes to the view.
4. Click **OK**.
   The capacity is allocated for writes to the view.

**Viewing Snapshot Details**

If the view details of the snapshot are available at that particular time for the virtual drive, the view details appear under the view details in the **Manage snapshots** wizard as shown in the following figure.
No View Details for Snapshot

When there is no view for the snapshot, the following message appears in the View details area as shown in the following figure.

Figure 106 No View Present for the Snapshot
No Snapshot Schedule

When there are virtual drives with no snapshot schedule, the following message appears as shown in the following figure.

**Figure 107  Virtual Drives with No Snapshot Schedule**

![Graphical Representation of Repository Virtual Drive](image)

Click **Add to Schedule** to add to a snapshot schedule or click **New Schedule** to add a new snapshot schedule.

**Graphical Representation of Repository Virtual Drive**

To view the graphical representation of the repository virtual drive, do the following:

1. Click the Logical view on the main menu window.
2. Click the Snapshot Repository virtual drive in the left frame.
3. Click the Snapshots tab in the right frame. The following figure appears, which shows the graphical representation of the virtual drive details.
Deleting a Snapshot

You can delete only the oldest snapshot.

Follow these steps to delete a snapshot.

1. Click the Logical tab on the main menu window in the Logical view.
2. Select a Required Base virtual drive from the list of virtual drives in the left frame.
3. Select Go To -> Virtual Drive -> Manage Snapshots on the menu bar. The window that appears shows the Snapshot Base details and any existing snapshots.
4. Click the oldest snapshot in the timeline.
5. Click the Delete Snapshot button.

This action deletes the oldest snapshot.

Disabling MegaRAID Recovery

Follow these steps to disable MegaRAID recovery.

1. Click the Logical tab on the main menu window in the Logical view.
2. Select and highlight a required base virtual drive from the list of virtual drives.
3. Select Go To -> Virtual Drive -> Disable MegaRAID Recovery on the menu bar. The following confirmation dialog appears.
4. Select the Confirm check box if you want to disable snapshots. When you select this check box, the Yes button gets enabled. The snapshots get disabled on the virtual drive. If you click No, the snapshots will not be disabled on the selected virtual drive.

CacheCade - SSD Caching Advanced Software Option

The MegaRAID CacheCade™ feature improves application performance by expanding the MegaRAID read-caching capacity. The CacheCade™ feature uses high-performing CacheCade - SSD Caching software as a secondary tier of cache to provide faster reads and to maximize transactional I/O performance.

The following settings are the optimal controller settings for CacheCade - SSD Caching:

- Write Policy: Write Back
- IO Policy: Cached IO
- Read Policy: No Read Ahead
- Stripe Size: 64 KB

Using the CacheCade - SSD Caching Advanced Software Option

Perform the following steps to use the CacheCade™ advanced software feature.

1. Click a RAID controller icon in the left frame.
2. Select Controller -> Create CacheCade on the menu bar, as shown in the following figure.
The Wizard screen appears.

3. Click on unconfigured CacheCade - SSD Caching drives in the left frame to select the drives for the CacheCade drive group, as shown in the following figure.

After you select the unconfigured drives, the **Add ->** button is available.

4. Click **Add ->** to move the selected drives to the drive group in the right frame, as shown in the following figure.
After you move the selected drives, the Create CacheCade Drive Group button is available.

5. Click Create CacheCade Drive Group.

6. Click Next.

Use the next screen that appears to select parameters for the cache disk.

7. Enter a name for the CacheCade - SSD Caching virtual drive in the CacheCade VD name text box, and click Create.

Depending on the number of drives, you might have the option to set the capacity of the CacheCade - SSD Caching drive.

The CacheCade drive group icon appears in the menu screen, as shown in the following figure.

Figure 113 CacheCade Drive Group Icon
8. Click **Next**.

The summary window appears, as shown in the following figure. This window displays the drive group name, the number of drives, the total capacity, the free capacity, the CacheCade virtual drive name, and the capacity being used.

**Figure 114 CacheCade Virtual Drive Summary Screen**

9. Click **Finish**.

A confirmation message displays after the CacheCade - SSD Caching virtual drive is successfully created. The CacheCade - SSD Caching drive icon appears next to the RAID controller in the left frame, as shown in the following figure.

**Figure 115 CacheCade - SSD Caching Drive Icon in MegaRAID Storage Manager Software**
SSD Disk Cache Policy

The MegaRAID firmware provides support to change the write-cache policy for SSD media of individual physical drives.

The MegaRAID firmware does not allow any user application to modify the write-cache policies of any SSD media. The host applications can modify this property through the new logical device (LD) addition or LD property change. When SSDs are configured in a mixed disk group with HDDs, the Physical Device Write-Cache Policy setting of all the participating drives changes to match the SSD cache policy setting.

Follow these steps to view the SSD cache property.

1. Click the controller node in the device tree.
   
   The Controller Properties screen appears, as shown in the following figure.

   **Figure 116  Controller Properties – SSD Disk Cache Policy**

   ![Controller Properties – SSD Disk Cache Policy](image)

   - Virtual Drive Settings

   If the SSD cache property is enabled in the controller properties screen as shown, in the above figure, then you cannot select the disk cache policy for the virtual drives having only SSD drives or a mix of SSD drives and HDD drives during virtual drive creation. The value of the disk cache policy is unchanged and the drop-down menu is disabled.

   Follow these steps to view the virtual drive settings.

   1. Right-click the controller node in the device tree.

   2. Select the **Create Virtual Drive** menu option.
3. Select **Advanced Configuration**, and click **Next**.
4. Create **Drive Group**, and click **Next**.

**Figure 117  Virtual Drive Settings**

The value of the Disk Cache Policy will be unchanged, and the drop-down combo box will be disabled.

**Set Virtual Drive Properties**

Follow these steps to set virtual drive properties.

1. Right click on virtual drive node in the logical view of the device tree.
2. Select **Set Virtual Drive** Properties.
   The Set Virtual Drive Properties dialog appears, as shown in the following figure.
You cannot select the Disk cache policy for the virtual drives having only SSD drives or a mix of SSD and HDD during VD creation. The value of the Disk Cache Policy will be “Unchanged” and can be set for only HDD drives.

Non-SED Secure Erase Support

This section describes the firmware changes required to securely erase data on non-SEDs (normal HDDs).

SEDs securely erase their internal encryption keys, effectively destroying all of the data present on the drive. For Non–SED drives, the erase operation consists of a series of write operations to a drive that overwrites every user-accessible sector of the drive with specified patterns. It can be repeated in multiple passes using different data patterns for enhanced security. The sanitization technique is more secure than a simple format operation and is commonly called a “clearing” operation, similar to the existing physical drive clear command.

Follow these steps to set physical drive properties.

1. In the Physical view, right click the **Physical Drive** node.
2. Select the **Drive Erase** option.

   The **Mode Selection - Drive Erase** dialog appears, as shown in the following figure.
3. You can select the various modes available under the **Select the mode for Drive Erase operation.**
   - **Simple** – (Alt + S)
     
     When you select this option and click **OK**, the Drive Erase message box appears, as shown in the following figure.
   - **Normal** – (Alt + N)
     
     Select this option and click of **OK**. The the following figure is displayed.
   - **Thorough** – (Alt + T)
     
     Select this option and click of **OK**. The the following figure is displayed.

**Figure 120  Drive Erase Message**

**Group Show Progress for Drive Erase**

The physical drive erase operation is a time-consuming operation and is performed as a background task. It posts events to notify users of the progress.

Follow these steps to check the progress of physical drive erase operation.

1. Click the **Show Progress** toolbar icon in the MegaRAID Storage Manager software. You can also select **Show Progress** from the dashboard or select **Show Progress** from the Manage menu.
2. Click the **More info** link under the Background Operations portlet.
   The progress bar appears, as shown in the following figure.

**Figure 121  Group Show Progress**

3. On clicking the Abort All button, the Drive Erase operation stops and the progress bar is not displayed.

**Virtual Drive Erase**

The virtual drive erase operates on a specified virtual drive and overwrites all user-accessible locations. It supports non-zero patterns and multiple passes. Virtual drive erase optionally deletes the virtual drive and erases the data within the virtual drive’s LBA range. Virtual drive erase is a background operation, and it posts events to notify users of their progress.

Follow these steps to open the Virtual Drive Erase menu.

1. In the Logical view, right-click the Virtual Drive node.
2. Click on the Virtual Drive node, select top level navigation and click **Go to**.
3. Select **Virtual Drive** and select **Events & Response**.
   The Virtual Drive Erase Menu opens, as shown in the following figure.
The menu has the following options.

- **Simple** – (Alt + S) – After you select this option and click OK and if Delete Virtual Drive after Erase is selected, the following figure is displayed; otherwise, Figure 124 is displayed.
- **Normal** – (Alt + N) – After you select this option and click OK, and if Delete Virtual Drive after Erase is selected, the following figure is displayed; otherwise, Figure 124 is displayed.
- **Thorough** – (Alt + T) – After you select this option and click OK and if Delete Virtual Drive after Erase is selected, the following figure is displayed; otherwise, Figure 124 is displayed.
- **Delete Virtual Drive after Erase** – (Alt + D) – When you select this option, the virtual drive is erased and the following figure is displayed; otherwise, Figure 124 is displayed.
- **OK** – (Alt + O) – Click OK and if Delete Virtual Drive after Erase is checked, the following figure is displayed; otherwise, Figure 124 is displayed.
- **Cancel** – (Alt + C) – When you select this option, the dialog closes, and the MegaRAID Storage Manager navigates back to Physical view.

**Figure 123 Warning Message for Virtual Drive Erase**

- Click Yes to erase the virtual drive.
- Click No to cancel the erase and close the dialog.
• Click **Yes** to erase the virtual drive.
• Click **No** to cancel the erase and close the dialog.

**Group Show Progress for Virtual Drive Erase**

The virtual drive erase operation is a time-consuming operation and is performed as a background task. It posts events to notify users of the progress.

Follow these steps to view the progress of virtual drive erase operation in the Group Show Progress-Virtual Drive window.

1. Click the **Show Progress** toolbar icon. You can either select **Show Progress** from the Manage menu or select the **More info** Link under Background Operations portlet on the dashboard.

   The Virtual Drive Erase progress bar appears, as shown in the following figure.
Background Suspend/Resume Support

MegaRAID provides a background suspend or resume support feature that enhances the functionality where in the background operations running on a physical drive or on a virtual drive can be suspended for some time, and resumed later using the Resume option.

The background operations, including consistency-check, rebuild, background initialization, and patrol read, are supported by an abort operation. If any operation is stopped before completion, it is considered to be aborted. An aborted operation cannot be resumed from the place where it was stopped.

A suspended operation can be resumed later by using the Resume option, and the suspended operation resumes from the point where the operation was suspended last.

Follow these steps to perform a suspend and resume operation.

1. Go to the Group Show Progress dialog, and perform the following tasks. You also can select Show Progress from the Manage menu, or select the More info link under the Background Operations portlet on the dashboard.

   The Group Show Progress dialog appears, as shown in the following figure.
**FastPath Advanced Software**

MegaRAID FastPath is a high-performance IO accelerator for CacheCade software drive groups connected to a MegaRAID controller card. SSDs have a read performance advantage over HDDs and use less power. This feature dramatically boosts storage subsystem bandwidth and overall transactional application performance when used with a 6Gb/s MegaRAID SATA+SAS controller. For more information on how to use FastPath advanced software, see the Setting FastPath Options section.

The FastPath feature supports full optimization of CacheCade - SSD Caching and hard disk drive (HDD) virtual disk groups to deliver an improvement in read and write IOPS that is three times...
greater than MegaRAID controllers not utilizing FastPath technology. Also, the FastPath advanced software is faster and more cost-effective than current flash-based adapter card solutions.

**Setting FastPath Options**

Perform the following steps to use the FastPath advanced software.

1. Click the **Logical** tab on the main menu window in the Logical view.
2. Click a virtual drive icon in the left frame.
3. Select **Virtual Drive -> Set Virtual Drive Properties** on the menu bar, as shown in the following figure.

![Set Virtual Drive Properties Menu](image)

The **Set Virtual Drive Properties** window appears. It shows the default settings for the FastPath advanced software:

- Write Policy: Write Thru
- IO Policy: Direct IO
- Read Policy: No Read Ahead
- Dish Cache Policy: Enabled
- Stripe Size: 64KB
4. Click **OK**.
   A confirmation dialog appears.
5. Select the **Confirm** check box and click **Yes** to confirm that you want to set the virtual drive properties.

**LSI SafeStore Encryption Services**

LSI SafeStore Encryption Services offer the ability to encrypt data on drives and use drive-based key management to provide data security. This solution provides data protection in the event of theft or loss of physical drives. If you remove a self-encrypting drive from its storage system or the server it is housed in, the data on that drive is encrypted and useless to anyone who attempts to access without the appropriate security authorization.
This section describes how to enable, change, and disable drive security, and how to import a foreign configuration using the SafeStore Encryption Services advanced software.

The SafeStore Encryption Services advanced software provides drive security to create secure virtual drives by using the External Key Management (EKM) and the Local Key Management (LKM).

- **Enabling Drive Security Using EKM**
- **Enabling Drive Security Using LKM**

### Enabling Drive Security Using EKM

EKM is used for key management when a large number of systems are deployed. You can automate and manage the life cycle of keys and unlock configurations using EKM.

Another important feature of EKM is that you can use EKM without human intervention to perform operations like drive migration and controller replacement.

MegaRAID accomplishes the task of obtaining keys by interacting with the EKM agent. The EKM agent talks to the EKM server (EKMS) through a network and gets the security key for the controller.

Keys are retrieved or created to perform the following tasks.

- Create secure virtual drives.
- Insert drives to replace failed drives in a secure configuration.
- Re-key the system based on EKMS policies or user request.
- Gain access to a secured configuration during boot.
- Unlock and import secured drives during migration.

You can perform the following configurations to enable the drive security to create secure virtual drives using the EKM mode with the support of EKM servers.

- EKM mode is supported by the MegaRAID Storage Manager software and EKMS is present.
- EKM mode is supported by the MegaRAID Storage Manager software and EKMS is not present.
- Change current security settings or switch between modes.
- Change security settings when the user is in EKM and wants to switch to LKM.
- Import Foreign Drives.

### Supporting EKM Mode

When you choose EKM for drive security, and decide to configure when **EKM mode is supported, and EKMS is present**, the application responds to different behaviors based on the scenarios that take place at that particular time.

The first scenario occurs when EKM is enabled, and the second scenario occurs when EKM is enabled and EKMS is present. The details of these scenarios are described further in this section.

Perform the following steps to configure, EKM mode is supported, and EKMS is present.

1. Select the **Physical** tab in the left panel of the MegaRAID Storage Manager window, and select a controller icon.
2. Choose any one of the following options to arrive at the Drive Security Choose Mode wizard.
   - Select Go To> Controller> Enable Drive Security in the main navigation bar in the top portion of the MegaRAID Storage Manager window.
   - Right-click the controller icon, and click Enable Drive Security menu.

The Drive Security Choose Mode wizard appears, as shown in the following figure.

**Figure 128 Drive Security Choose Mode**

3. Select External Key management (EKM).

4. Click OK.

   After you click OK, two scenarios occur based on the availability of EKMS.

**Scenario # 1 - EKM is enabled**

When EKM is enabled, you can see the confirmation message as shown in the following figure. The message displayed ensures that security is enabled on the controller using EKMS.

**Figure 129 Confirm External Key Management Mode Enabled**

Note: On the right hand side frame of the controller properties, in Drive Security Properties, you can see the key management mode is EKM.

**Scenario # 2 - EKM is selected, and EKMS is not present**
When EKM is selected and EKMS is not present, you have to restart the system. When you restart the system, the system restart message appears as shown in the following figure.

**Figure 130  System Restart**

![System Restart](image)

When the system restarts the boot agent generates the security keys for the controller.

*Note:* If the MegaRAID Storage Manager application does not support EKM, the EKM option is greyed out.

**Change Security Settings - LKM**

When you select the Change Security Settings in the Change Security wizard, as shown in the following figure, two options are provided for you. If you select the first option, Change current security settings, you can change the drive security settings on the controller. If you select the second option, Switch to External Key Management (EKM) mode, you can switch from LKM mode to EKM mode.

Use any of the following options to enable the Change Security Settings wizard.

1. Select the Physical View tab in the left panel of the MegaRAID Storage Manager window, and click a controller icon.
2. Select **Go To -> Controller -> Change Security Settings** in the menu bar or right-click on the controller icon, and click **Change Security Settings** from the menu.

   The Drive Security Choose Mode wizard appears, as shown in the following figure.

**Figure 131  Change Security Settings**

![Change Security Settings](image)

3. Select the Change current security settings option, if you want to change the drive security settings on the controller using the LKM mode.
4. Select **Switch to External key management (EKM) mode**, if you want to switch over from LKM mode to EKM mode.

5. Click **OK**.

After you click OK and have switched to the EKM mode, the **Authentication Drive Security Key** dialog appears.

### Authentication Drive Security Key

After the **Authentication Drive Security Key** dialog appears, you have to enter the authentication drive security key (currently the LKM key) in the **Authentication Drive Security Key** dialog as shown in the following figure.

**Figure 132  Authentication Drive Security Key**

If you enter a valid authentication key, you will see a confirmation message indicating that EKM is enabled as shown in the following figure.

**Figure 133  Confirmation Message When EKM is Enabled**

Based on the application’s response at that particular point of time, you come across two scenarios. The first scenario is, if **EKMS is selected and EKMS is not present**, and the second scenario is, if you enter a wrong security key in the **Authentication Drive Security Key** dialog.

### Scenario # 1 - EKM is selected and EKMS is not present

When **EKMS is selected and EKMS is not present**, you have to restart the system, and during re-boot the boot agent generates the security keys.

When you restart the system, the system restart message appears as shown in the following figure.
Figure 134  System Restart

[Image]

Scenario #2 - Entering a wrong security key

If you enter a wrong security key in the Authentication Drive Security Key dialog box, an error message appears as shown in the following figure.

Figure 135  Error Message When User Enters the Wrong Security Key

[Image]

Change Security Settings - EKM

When you select the Change Security Settings in the Change Security wizard as shown in the following figure, two options are provided for you. If you select the first option, that is, Change current security settings, you can traverse to the EKM mode. If you select the second option, Switch to Local Key Management (LKM) mode you can switch over to LKM mode.

Perform the following steps to configure the Change Security Settings wizard.

1. Select the Physical View tab in the left panel of the MegaRAID Storage Manager main menu screen, and click a controller icon.
2. Select Go To -> Controller -> Change Security Settings in the main navigation bar which is present in the top portion of the MegaRAID Storage Manager screen.
3. Right click on the controller icon, and click Change Security Settings.
   
   The Change Security Settings wizard appears, as shown in the following figure.
Figure 136  Change Security Settings

When you select the **Change current security settings** option, you get a different EKM key for the controller.

Based on the application's response two scenarios occur - the first scenario is, when **EKM server is present**, and the second scenario is, when **EKM server is not present**.

**Scenario # 1- EKM server is present**

If EKM server is present, you will get a confirmation message indicating that the drive security is enabled on the controller as shown in the following figure.

**Figure 137  EKMS server is present**

**Scenario # 2 - EKM server is not present**

When EKM server is not present, you have to restart the system, and during re-boot the boot agent generates the security keys.

When you restart the system, the system restart message appears, as shown in the following figure.

**Figure 138  System Restart**
Importing Foreign Drives

You can import foreign drives in the LKM or EKM mode. Based on the mode selected and the secured drives, the following scenarios occur.

- Import Foreign Drives – LKM mode, EKM Secured Locked Drives are present.
- Import Foreign Drives – EKM mode, LKM secured locked drives are present.
- Import Foreign Drives – EKM mode, EKM secured locked drives are present.

Perform the following steps to configure the Scan Foreign Configuration wizard.

1. Select the Physical View tab in the left panel of the MegaRAID Storage Manager main menu window, and click a controller icon.
2. Choose any one of the following options to enable the Scan Foreign Configuration wizard.
   - Right-click the controller node in the device tree in the left frame of the MegaRAID Storage Manager main menu screen, and select Scan Foreign Configuration.
   - Select Go To -> Controller -> Scan Foreign Configuration in the menu bar.

If a foreign configuration is detected, the Foreign Configuration Detected screen appears. If you choose Import and click OK, the Unlock Foreign drives wizard appears.

Importing Foreign Drives to LKM

When a virtual drive is secured with EKM mode, and if you change the security settings from EKM mode to LKM mode, and want to import those foreign configured virtual drives, the following dialog appears.

Figure 139 Importing Foreign Drives- EKM to LKM

Importing Foreign Drives to EKM

When a virtual drive is secured with the LKM mode and is in Foreign state, if you want to switch from LKM to EKM and then import the foreign configuration, you need to provide the LKM key for each virtual drive.
The locked drives field display the drives that are locked with LKM mode.

The Security Key displays the LKM security key for the VD.

After you enter the security key in the Security key field, the system tries to unlock each of the locked foreign drives using the security key. If at least one drive is unlocked, then the Import preview screen is displayed. If no drives are unlocked, the Incorrect security Key dialog is displayed.

Importing Foreign Drives to EKM

When a virtual drive is secured with EKM mode, and that virtual drive is in foreign state, and if you switch to EKM mode, and if you want to import to foreign configuration, then the dialog appears as shown in the following figure.
Enabling Drive Security Using LKM

This section describes how to enable, change, and disable drive security, and how to import a foreign configuration using the SafeStore Encryption Services advanced software.

To enable security on the drives, you need to perform the following actions to set drive security:

- Enter a security key identifier.
  
  A security key identifier appears whenever you have to enter a security key. If you have more than one security key, the identifier helps you determine which security key to enter.

- Enter a security key.
  
  After you create a security key, you have the option to create secure virtual drives using the key. You have to use the security key to perform certain operations.

You can improve security by entering a password. To provide additional security, you can require the password whenever anyone boots the server.

Perform the following steps to enable drive security.

1. Select the Physical View tab in the left panel of the MegaRAID Storage Manager main menu screen, and click a controller icon.
2. Select **Go To -> Controller -> Change Drive Security -> Enable**.

   The Enable Drive Security window appears, as shown in the following figure.

   **Figure 142 Enable Drive Security - Security Key Identifier**

3. Use the default security key identifier or enter a new security key identifier.
Note: If you create more than one security key, make sure that you change the security key identifier. Otherwise, you cannot differentiate between the security keys.

4. Click **Suggest Security Key** to have the system create a security key or you can enter a new security key.

5. Enter the new security key again to confirm, as shown in the following figure.

   **Note:** If you forget the security key, you will lose access to your data. Be sure to record your security key information. You might need to enter the security key to perform certain operations.

   The security key is case-sensitive. It must be between 8 and 32 characters and contain at least one number, one lowercase letter, one uppercase letter, and one non-alphanumeric character (e.g. `< > @ +`). The space character is not permitted.

   **Note:** Non-US keyboard users must be careful not to enter DBCS characters in the security key field. Firmware works with the ASCII character set only.

   The following figure shows the security key entered and confirmed on this window.

**Figure 143 Enable Drive Security - Security Key**

6. (Optional) Select the **Pause for password at boot time** check box.

   If you choose this option, you have to enter the password whenever you boot the server.

7. (Optional) Select the **Enforce strong password security** check box.

   If you choose this option, make sure the password is between eight and thirty-two characters and contain at least one number, one lowercase letter, one uppercase letter, and one non-alphanumeric character.
alphanumeric character (e.g. < > @ +). The space character is not permitted. The password is case-sensitive.

8. (Optional) Enter a password in the **Password** field and then enter the same password in the **Confirm** field, as shown in the following figure.

Warning messages appear if there is a mismatch between the characters entered in the **Password** field and the **Confirm** field, or if there is an invalid character entered.

**Important:** Be sure to record the password. If you lose the password, you could lose access to your data.

The following figure shows the password entered and confirmed on this window.

**Figure 144 Enable Drive Security - Password**

![Enable Drive Security - Password](image)

9. Click **Next**.

The Confirm Enable Drive Security screen appears, as shown in the following figure, to show the changes requested to the drive security settings.

**Important:** If you forget the security key, you will lose access to your data. Be sure to record your security key. You might need to enter the security key to perform certain operations.
10. Select the **I recorded the security settings for future reference** check box and then click **Yes** to confirm that you want to enable drive security on this controller and have recorded the security settings for future reference.

The MegaRAID Storage Manager software enables drive security and returns you to the main menu window.

**Change Security Settings - LKM**

Perform the following steps to change the encryption settings for the security key identifier, security key, and password.

1. Select the **Physical View** tab in the left panel of the MegaRAID Storage Manager main menu screen, and click a controller icon.

2. Select **Go To -> Controller -> Change Drive Security.**

   The Change Security Settings – Introduction screen appears. This screen lists the actions you can perform, which include editing the security key identifier, security key, and the password.

3. Click **Next.**

   The Change Security Settings - Security Key ID screen appears.

4. Keep the existing security key identifier or enter a new security key identifier.

   **Important:** If you change the security key, LSI highly recommends that you change the security key identifier. Otherwise, you cannot differentiate between the security keys.

5. Click **Next.**
The Change Security Settings - Security Key screen appears.

6. Click **Use the existing drive security key** to use the existing drive security key or enter a new security key and then enter the new security key again to confirm.

**Important:** If you forget the security key, you will lose access to your data. Be sure to record your security key information. You might need to enter the security key to perform certain operations.

The security key is case-sensitive. It must be between 8 and 32 characters and contain at least one number, one lowercase letter, one uppercase letter, and one non-alphanumeric character (e.g. `< > @ +). The space character is not permitted.

**Note:** Non-US keyboard users must be careful not to enter DBCS characters in the security key field. Firmware works with the ASCII character set only.

7. Click **Next**.

The Authenticate Drive Security Settings Screen appears. Authentication is required for the changes that you requested to the drive security settings.

8. Enter the current security key to authenticate the changes.

The Change Security Settings - Password screen appears.

9. If you choose to, click the option to use a password in addition to the security key.

10. If you chose to use a password, either enter the existing password or enter a new password, and enter the password again to confirm.

The text box for the passphrase can hold up to 32 characters. The key must be at least eight characters.

The next screen that appears describes the changes you made and asks you whether you want to confirm these changes.

11. Click the checkbox to confirm that you have recorded the security settings for future reference and then click **Yes** to confirm that you want to change the drive security settings.

The MegaRAID Storage Manager software updates the existing configuration on the controller to use the new security settings and returns you to the main menu.

### Disabling Drive Security

**Important:** If you disable drive security, your existing data is not secure and you cannot create any new secure virtual drives. Disabling drive security does not affect the security of data on foreign drives. If you removed any drives that were previously secured, you still need to enter the password when you import them. Otherwise, you cannot access the data on those drives.

**Note:** If there are any secure drive groups on the controller, you cannot disable drive security. A warning screen appears if you attempt to do so. To disable drive security, you must first delete the virtual drives on all of the secure drive groups.

Perform the following steps to disable drive security.

1. Select the **Physical View** tab in the left panel of the MegaRAID Storage Manager main menu, and click a controller icon.

2. Select **Go To -> Controller -> Disable Drive Security**.
The Confirm Disable Drive Security screen appears.

3. To disable drive security, click **Yes**.

   The MegaRAID Storage Manager software disables drive security and returns you to the main menu.

   **Note:** If you disable drive security, you cannot create any new encrypted virtual drives and the data on all encrypted unconfigured drives will be erased. Disabling drive security will not affect the security or data of foreign drives.

**Importing or Clearing a Foreign Configuration**

A foreign configuration is a RAID configuration that already exists on a replacement set of drives that you install in a computer system. You can use the MegaRAID Storage Manager software to import the foreign configuration to the RAID controller or to clear the foreign configuration so you can create a new configuration using these drives.

To import a foreign configuration, you must do the following:

- Enable security to allow importation of locked foreign configurations. (You can import unsecured or unlocked configurations when security is disabled.)
- Run a scan for foreign configurations.
- If a locked foreign configuration is present and security is enabled, enter the security key and unlock the configuration.
- Import the foreign configuration.
In addition, if one or more drives are removed from a configuration, by a cable pull or drive removal for example, the configuration on those drives is considered a foreign configuration by the RAID controller.

Verify whether any drives are left to import as the locked drives can use different security keys. If there are any drives left, repeat the import process for the remaining drives. After all the drives are imported, there is no configuration to import.

**Note:** When you create a new configuration, the MegaRAID Storage Manager software shows only the unconfigured drives. Drives that have existing configurations, including foreign configurations, will not appear. To use drives with existing configurations, you must first clear the configuration on those drives.

Perform the following steps to import or clear a configuration.

1. Enable drive security to allow importation of locked foreign drives.
   See [Enabling Drive Security Using LKM](#) for the procedure used to enable drive security.

2. After you create a security key, right-click the controller icon and click **Scan for Foreign Configuration**.
   If there are locked drives (security is enabled), the Unlock foreign drives dialog appears.

3. Enter the security key to unlock the configuration.
   The Foreign Configuration Detected dialog appears, as shown in the following figure.

4. Click **Import** to import the foreign configuration from all of the foreign drives, **Clear** to remove the configuration from all foreign drives, or **Advanced** to preview and import specific foreign configurations.

5. Click **OK**.
   **Note:** The operation cannot be reversed after it is started. Imported drives display as **Online** in the MegaRAID Storage Manager menu.

6. Repeat the import process for any remaining drives.
   Because locked drive can use different security key, you must verify whether there are any remaining drives to imported.

   **Note:** When you create a new configuration, the MegaRAID Storage Manager software shows only the unconfigured drives. Drives that have existing configurations, including foreign configurations, will not appear. To use drives with existing configurations, you must first clear the configuration on those drives.
Foreign Configurations in Cable Pull and Drive Removal Scenarios

If one or more drives are removed from a configuration, by a cable pull or drive removal, for example, the configuration on those drives is considered a foreign configuration by the RAID controller.

The following scenarios can occur with cable pulls or drive removals. Use the Foreign Configuration Preview screen to import or clear the foreign configuration in each case.

Note: If you want to import the foreign configuration in any of the following scenarios, you should have all of the drives in the enclosure before you perform the import operation.

Scenario #1: If all of the drives in a configuration are removed and re-inserted, the controller considers the drives to have foreign configurations. –

Import or clear the foreign configuration. If you select Import, automatic rebuilds will occur in redundant virtual drives.

Note: Start a consistency check immediately after the rebuild is complete to ensure data integrity for the virtual drives.

Scenario #2: If some of the drives in a configuration are removed and re-inserted, the controller considers the drives to have foreign configurations. –

Import or clear the foreign configuration. If you select Import, automatic rebuilds will occur in redundant virtual drives.

Note: Start a consistency check immediately after the rebuild is complete to ensure data integrity for the virtual drives.

Scenario #3: If all of the drives in a virtual drive are removed, but at different times, and re-inserted, the controller considers the drives to have foreign configurations. –

Import or clear the foreign configuration. If you select Import, all drives that were pulled before the virtual drive became offline will be imported and then automatically rebuilt. Automatic rebuilds will occur in redundant virtual drives.

Scenario #4: If the drives in a non-redundant virtual drive are removed, the controller considers the drives to have foreign configurations. –

Import or clear the foreign configuration. No rebuilds will occur after the import operation because there is no redundant data to rebuild the drives.

Managing Link Speed

The Managing Link Speed feature allows you to change the link speed between the controller and an expander or between the controller and a drive that is directly connected to the controller.

All phys in a SAS port must have the same maximum link speed setting. If the phys in a SAS port have different link speeds, the firmware uses the lowest link speed for that SAS port.

Follow these steps to change the link speed.

1. Right-click a controller in the left frame of the MegaRAID Storage Manager main menu and select Manage Link Speed.
Select a controller in the left frame of the MegaRAID Storage Manager main menu, and then select **Go To>Controller>Manage Link Speed** in the menu bar.

The **Manage Link Speed** dialog appears, as shown below. The **Manage Link Speed** dialog also lets you view the link speed between the controller and an expander or between the controller and a drive that is directly connected to the controller.

**Figure 148 Manage Link Speed**

The SAS Address column displays the SAS address that uniquely identifies a device in the SAS domain.

The Phy column displays the system-supported phy link values. The phy link values are from 0 through 7.

The Select Link Speed column displays the phy link speeds.

2. Select the desired link speed from the Select Link Speed field using the drop-down selector.

The link speed values are Auto, 1.5, 3.0 or 6.0 Gbps. By default, the link speed in the controller is *Auto* or the value last saved by the user.

3. Click **OK**.

The link speed value is now reset. The change takes place after you restart the system.

The message box appears, as shown below.
Figure 149  System Restart

Please restart the system for the changes to take effect. Make sure to stop all the I/Os and other operations before you restart your system.
Events and Messages

This topic lists the MegaRAID Storage Manager events that can appear in the event log.

MegaRAID Storage Manager software monitors the activity and performance of all controllers in the server and the devices attached to them. When an event occurs, such as the removal of a drive or the creation of a new drive group, an event message appears in the log displayed at the bottom of the MegaRAID Storage Manager screen. The messages are also logged in the Windows Application log (Event Viewer).

Each message that appears in the event log has a Severity Level that indicates the category of the event, as shown in the following table.

### Table 2  Event Error Levels

<table>
<thead>
<tr>
<th>Severity Level</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information</td>
<td>Informational message. No user action is necessary.</td>
</tr>
<tr>
<td>Warning</td>
<td>Some component may be close to a failure point.</td>
</tr>
<tr>
<td>Critical</td>
<td>A component has failed, but the system has not lost data.</td>
</tr>
<tr>
<td>Fatal</td>
<td>A component has failed, and data loss has occurred or will occur.</td>
</tr>
</tbody>
</table>

The following table lists all of the MegaRAID Storage Manager event messages. The event message descriptions include placeholders for specific values that are determined when the event is generated. For example, in message No. 1 in the Event Messages table, “%s” is replaced by the firmware version, which is read from the firmware when the event is generated.

### Table 3  Event Messages

<table>
<thead>
<tr>
<th>Number</th>
<th>Severity Level</th>
<th>Event Text</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x0000</td>
<td>Information</td>
<td>MegaRAID firmware initialization started (PCI ID %04x/%04x/%04x/%04x)</td>
</tr>
<tr>
<td>0x0001</td>
<td>Information</td>
<td>MegaRAID firmware version %s</td>
</tr>
<tr>
<td>0x0002</td>
<td>Fatal</td>
<td>Unable to recover cache data from TBBU</td>
</tr>
<tr>
<td>0x0003</td>
<td>Information</td>
<td>Cache data recovered from TBBU successfully</td>
</tr>
<tr>
<td>0x0004</td>
<td>Information</td>
<td>Configuration cleared</td>
</tr>
<tr>
<td>0x0005</td>
<td>Warning</td>
<td>Cluster down; communication with peer lost</td>
</tr>
<tr>
<td>0x0006</td>
<td>Information</td>
<td>Virtual drive %s ownership changed from %02x to %02x</td>
</tr>
<tr>
<td>0x0007</td>
<td>Information</td>
<td>Alarm disabled by user</td>
</tr>
<tr>
<td>0x0008</td>
<td>Information</td>
<td>Alarm enabled by user</td>
</tr>
<tr>
<td>0x0009</td>
<td>Information</td>
<td>Background initialization rate changed to %d%%</td>
</tr>
<tr>
<td>0x000a</td>
<td>Fatal</td>
<td>Controller cache discarded due to memory/battery problems</td>
</tr>
<tr>
<td>0x000b</td>
<td>Fatal</td>
<td>Unable to recover cache data due to configuration mismatch</td>
</tr>
<tr>
<td>0x000c</td>
<td>Information</td>
<td>Cache data recovered successfully</td>
</tr>
<tr>
<td>Number</td>
<td>Severity Level</td>
<td>Event Text</td>
</tr>
<tr>
<td>--------</td>
<td>----------------</td>
<td>------------</td>
</tr>
<tr>
<td>0x000d</td>
<td>Fatal</td>
<td>Controller cache discarded due to firmware version incompatibility</td>
</tr>
<tr>
<td>0x000e</td>
<td>Information</td>
<td>Consistency Check rate changed to %d%%</td>
</tr>
<tr>
<td>0x000f</td>
<td>Fatal</td>
<td>Fatal firmware error: %s</td>
</tr>
<tr>
<td>0x0010</td>
<td>Information</td>
<td>Factory defaults restored</td>
</tr>
<tr>
<td>0x0011</td>
<td>Information</td>
<td>Flash downloaded image corrupt</td>
</tr>
<tr>
<td>0x0012</td>
<td>Critical</td>
<td>Flash erase error</td>
</tr>
<tr>
<td>0x0013</td>
<td>Critical</td>
<td>Flash timeout during erase</td>
</tr>
<tr>
<td>0x0014</td>
<td>Critical</td>
<td>Flash error</td>
</tr>
<tr>
<td>0x0015</td>
<td>Information</td>
<td>Flashing image: %s</td>
</tr>
<tr>
<td>0x0016</td>
<td>Information</td>
<td>Flash of new firmware image(s) complete</td>
</tr>
<tr>
<td>0x0017</td>
<td>Critical</td>
<td>Flash programming error</td>
</tr>
<tr>
<td>0x0018</td>
<td>Critical</td>
<td>Flash timeout during programming</td>
</tr>
<tr>
<td>0x0019</td>
<td>Critical</td>
<td>Flash chip type unknown</td>
</tr>
<tr>
<td>0x001a</td>
<td>Critical</td>
<td>Flash command set unknown</td>
</tr>
<tr>
<td>0x001b</td>
<td>Critical</td>
<td>Flash verify failure</td>
</tr>
<tr>
<td>0x001c</td>
<td>Information</td>
<td>Flush rate changed to %d seconds</td>
</tr>
<tr>
<td>0x001d</td>
<td>Information</td>
<td>Hibernate command received from host</td>
</tr>
<tr>
<td>0x001e</td>
<td>Information</td>
<td>Event log cleared</td>
</tr>
<tr>
<td>0x001f</td>
<td>Information</td>
<td>Event log wrapped</td>
</tr>
<tr>
<td>0x0020</td>
<td>Fatal</td>
<td>Multi-bit ECC error: ECAR=%x, ELOG=%x, (%s)</td>
</tr>
<tr>
<td>0x0021</td>
<td>Warning</td>
<td>Single-bit ECC error: ECAR=%x, ELOG=%x, (%s)</td>
</tr>
<tr>
<td>0x0022</td>
<td>Fatal</td>
<td>Not enough controller memory</td>
</tr>
<tr>
<td>0x0023</td>
<td>Information</td>
<td>Patrol Read complete</td>
</tr>
<tr>
<td>0x0024</td>
<td>Information</td>
<td>Patrol Read paused</td>
</tr>
<tr>
<td>0x0025</td>
<td>Information</td>
<td>Patrol Read Rate changed to %d%%</td>
</tr>
<tr>
<td>0x0026</td>
<td>Information</td>
<td>Patrol Read resumed</td>
</tr>
<tr>
<td>0x0027</td>
<td>Information</td>
<td>Patrol Read started</td>
</tr>
<tr>
<td>0x0028</td>
<td>Information</td>
<td>Reconstruction rate changed to %d%%</td>
</tr>
<tr>
<td>0x0029</td>
<td>Information</td>
<td>Reconstruction rate changed to %d%%</td>
</tr>
<tr>
<td>0x002a</td>
<td>Information</td>
<td>Shutdown command received from host</td>
</tr>
</tbody>
</table>
### Table 3  
Event Messages (Cont.)

<table>
<thead>
<tr>
<th>Number</th>
<th>Severity Level</th>
<th>Event Text</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x002b</td>
<td>Information</td>
<td>Test event: %s</td>
</tr>
<tr>
<td>0x002c</td>
<td>Information</td>
<td>Time established as %s; (%d seconds since power on)</td>
</tr>
<tr>
<td>0x002d</td>
<td>Information</td>
<td>User entered firmware debugger</td>
</tr>
<tr>
<td>0x002e</td>
<td>Warning</td>
<td>Background Initialization aborted on %s</td>
</tr>
<tr>
<td>0x002f</td>
<td>Warning</td>
<td>Background Initialization corrected medium error (%s at %lx)</td>
</tr>
<tr>
<td>0x0030</td>
<td>Information</td>
<td>Background Initialization completed on %s</td>
</tr>
<tr>
<td>0x0031</td>
<td>Fatal</td>
<td>Background Initialization completed with uncorrectable errors on %s</td>
</tr>
<tr>
<td>0x0032</td>
<td>Fatal</td>
<td>Background Initialization detected uncorrectable double medium errors (%s at %lx on %s)</td>
</tr>
<tr>
<td>0x0033</td>
<td>Critical</td>
<td>Background Initialization failed on %s</td>
</tr>
<tr>
<td>0x0034</td>
<td>Progress</td>
<td>Background Initialization progress on %s is %s</td>
</tr>
<tr>
<td>0x0035</td>
<td>Information</td>
<td>Background Initialization started on %s</td>
</tr>
<tr>
<td>0x0036</td>
<td>Information</td>
<td>Policy change on %s from %s to %s</td>
</tr>
<tr>
<td>0x0038</td>
<td>Warning</td>
<td>Consistency Check aborted on %s</td>
</tr>
<tr>
<td>0x0039</td>
<td>Warning</td>
<td>Consistency Check corrected medium error (%s at %lx)</td>
</tr>
<tr>
<td>0x003a</td>
<td>Information</td>
<td>Consistency Check done on %s</td>
</tr>
<tr>
<td>0x003b</td>
<td>Information</td>
<td>Consistency Check done with corrections on %s</td>
</tr>
<tr>
<td>0x003c</td>
<td>Fatal</td>
<td>Consistency Check detected uncorrectable double medium errors (%s at %lx on %s)</td>
</tr>
<tr>
<td>0x003d</td>
<td>Critical</td>
<td>Consistency Check failed on %s</td>
</tr>
<tr>
<td>0x003e</td>
<td>Fatal</td>
<td>Consistency Check completed with uncorrectable data on %s</td>
</tr>
<tr>
<td>0x003f</td>
<td>Warning</td>
<td>Consistency Check found inconsistent parity on %s at strip %lx</td>
</tr>
<tr>
<td>0x0040</td>
<td>Warning</td>
<td>Consistency Check inconsistency logging disabled on %s (too many inconsistencies)</td>
</tr>
<tr>
<td>0x0041</td>
<td>Progress</td>
<td>Consistency Check progress on %s is %s</td>
</tr>
<tr>
<td>0x0042</td>
<td>Information</td>
<td>Consistency Check started on %s</td>
</tr>
<tr>
<td>0x0043</td>
<td>Warning</td>
<td>Initialization aborted on %s</td>
</tr>
<tr>
<td>0x0044</td>
<td>Critical</td>
<td>Initialization failed on %s</td>
</tr>
<tr>
<td>0x0045</td>
<td>Progress</td>
<td>Initialization progress on %s is %s</td>
</tr>
<tr>
<td>0x0046</td>
<td>Information</td>
<td>Fast initialization started on %s</td>
</tr>
<tr>
<td>0x0047</td>
<td>Information</td>
<td>Full initialization started on %s</td>
</tr>
<tr>
<td>Number</td>
<td>Severity Level</td>
<td>Event Text</td>
</tr>
<tr>
<td>--------</td>
<td>----------------</td>
<td>------------</td>
</tr>
<tr>
<td>0x0048</td>
<td>Information</td>
<td>Initialization complete on %s</td>
</tr>
<tr>
<td>0x0049</td>
<td>Information</td>
<td>LD Properties updated to %s (from %s)</td>
</tr>
<tr>
<td>0x004a</td>
<td>Information</td>
<td>Reconstruction complete on %s</td>
</tr>
<tr>
<td>0x004b</td>
<td>Fatal</td>
<td>Reconstruction stopped due to unrecoverable errors</td>
</tr>
<tr>
<td>0x004c</td>
<td>Fatal</td>
<td>Reconstruct detected uncorrectable double medium errors (%s at %lx on %s at %lx)</td>
</tr>
<tr>
<td>0x004d</td>
<td>Progress</td>
<td>Reconstruction progress on %s is %s</td>
</tr>
<tr>
<td>0x004e</td>
<td>Information</td>
<td>Reconstruction resumed on %s</td>
</tr>
<tr>
<td>0x004f</td>
<td>Fatal</td>
<td>Reconstruction resume failed due to configuration mismatch</td>
</tr>
<tr>
<td>0x0050</td>
<td>Information</td>
<td>Reconstruction started on %s</td>
</tr>
<tr>
<td>0x0051</td>
<td>Information</td>
<td>State change on %s from %s to %s</td>
</tr>
<tr>
<td>0x0052</td>
<td>Information</td>
<td>Drive Clear aborted on %s</td>
</tr>
<tr>
<td>0x0053</td>
<td>Critical</td>
<td>Drive Clear failed on %s (Error %02x)</td>
</tr>
<tr>
<td>0x0054</td>
<td>Progress</td>
<td>Drive Clear progress on %s is %s</td>
</tr>
<tr>
<td>0x0055</td>
<td>Information</td>
<td>Drive Clear started on %s</td>
</tr>
<tr>
<td>0x0056</td>
<td>Information</td>
<td>Drive Clear completed on %s</td>
</tr>
<tr>
<td>0x0057</td>
<td>Warning</td>
<td>Error on %s (Error %02x)</td>
</tr>
<tr>
<td>0x0058</td>
<td>Information</td>
<td>Format complete on %s</td>
</tr>
<tr>
<td>0x0059</td>
<td>Information</td>
<td>Format started on %s</td>
</tr>
<tr>
<td>0x005a</td>
<td>Critical</td>
<td>Hot Spare SMART polling failed on %s (Error %02x)</td>
</tr>
<tr>
<td>0x005b</td>
<td>Information</td>
<td>Drive inserted: %s</td>
</tr>
<tr>
<td>0x005c</td>
<td>Warning</td>
<td>Drive %s is not supported</td>
</tr>
<tr>
<td>0x005d</td>
<td>Warning</td>
<td>Patrol Read corrected medium error on %s at %lx</td>
</tr>
<tr>
<td>0x005e</td>
<td>Progress</td>
<td>Patrol Read progress on %s is %s</td>
</tr>
<tr>
<td>0x005f</td>
<td>Fatal</td>
<td>Patrol Read found an uncorrectable medium error on %s at %lx</td>
</tr>
<tr>
<td>0x0060</td>
<td>Critical</td>
<td>Predictive failure: CDB: %s</td>
</tr>
<tr>
<td>0x0061</td>
<td>Fatal</td>
<td>Patrol Read puncturing bad block on %s at %lx</td>
</tr>
<tr>
<td>0x0062</td>
<td>Information</td>
<td>Rebuild aborted by user on %s</td>
</tr>
<tr>
<td>0x0063</td>
<td>Information</td>
<td>Rebuild complete on %s</td>
</tr>
<tr>
<td>0x0064</td>
<td>Information</td>
<td>Rebuild complete on %s</td>
</tr>
</tbody>
</table>
### Table 3  Event Messages (Cont.)

<table>
<thead>
<tr>
<th>Number</th>
<th>Severity</th>
<th>Event Text</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x0065</td>
<td>Critical</td>
<td>Rebuild failed on %s due to source drive error</td>
</tr>
<tr>
<td>0x0066</td>
<td>Critical</td>
<td>Rebuild failed on %s due to target drive error</td>
</tr>
<tr>
<td>0x0067</td>
<td>Progress</td>
<td>Rebuild progress on %s is %s</td>
</tr>
<tr>
<td>0x0068</td>
<td>Information</td>
<td>Rebuild resumed on %s</td>
</tr>
<tr>
<td>0x0069</td>
<td>Information</td>
<td>Rebuild started on %s</td>
</tr>
<tr>
<td>0x006a</td>
<td>Information</td>
<td>Rebuild automatically started on %s</td>
</tr>
<tr>
<td>0x006b</td>
<td>Critical</td>
<td>Rebuild stopped on %s due to loss of cluster ownership</td>
</tr>
<tr>
<td>0x006c</td>
<td>Fatal</td>
<td>Reassign write operation failed on %s at %lx</td>
</tr>
<tr>
<td>0x006d</td>
<td>Fatal</td>
<td>Unrecoverable medium error during rebuild on %s at %lx</td>
</tr>
<tr>
<td>0x006e</td>
<td>Information</td>
<td>Corrected medium error during recovery on %s at %lx</td>
</tr>
<tr>
<td>0x006f</td>
<td>Fatal</td>
<td>Unrecoverable medium error during recovery on %s at %lx</td>
</tr>
<tr>
<td>0x0070</td>
<td>Information</td>
<td>Drive removed: %s</td>
</tr>
<tr>
<td>0x0071</td>
<td>Warning</td>
<td>Unexpected sense: %s, CDB%ss, Sense: %s</td>
</tr>
<tr>
<td>0x0072</td>
<td>Information</td>
<td>State change on %s from %s to %s</td>
</tr>
<tr>
<td>0x0073</td>
<td>Information</td>
<td>State change by user on %s from %s to %s</td>
</tr>
<tr>
<td>0x0074</td>
<td>Warning</td>
<td>Redundant path to %s broken</td>
</tr>
<tr>
<td>0x0075</td>
<td>Information</td>
<td>Redundant path to %s restored</td>
</tr>
<tr>
<td>0x0076</td>
<td>Information</td>
<td>Dedicated Hot Spare Drive %s no longer useful due to deleted drive group</td>
</tr>
<tr>
<td>0x0077</td>
<td>Critical</td>
<td>SAS topology error: Loop detected</td>
</tr>
<tr>
<td>0x0078</td>
<td>Critical</td>
<td>SAS topology error: Unaddressable device</td>
</tr>
<tr>
<td>0x0079</td>
<td>Critical</td>
<td>SAS topology error: Multiple ports to the same SAS address</td>
</tr>
<tr>
<td>0x007a</td>
<td>Critical</td>
<td>SAS topology error: Expander error</td>
</tr>
<tr>
<td>0x007b</td>
<td>Critical</td>
<td>SAS topology error: SMP timeout</td>
</tr>
<tr>
<td>0x007c</td>
<td>Critical</td>
<td>SAS topology error: Out of route entries</td>
</tr>
<tr>
<td>0x007d</td>
<td>Critical</td>
<td>SAS topology error: Index not found</td>
</tr>
<tr>
<td>0x007e</td>
<td>Critical</td>
<td>SAS topology error: SMP function failed</td>
</tr>
<tr>
<td>0x007f</td>
<td>Critical</td>
<td>SAS topology error: SMP CRC error</td>
</tr>
<tr>
<td>0x0080</td>
<td>Critical</td>
<td>SAS topology error: Multiple subtractive</td>
</tr>
<tr>
<td>0x0081</td>
<td>Critical</td>
<td>SAS topology error: Table to table</td>
</tr>
<tr>
<td>0x0082</td>
<td>Critical</td>
<td>SAS topology error: Multiple paths</td>
</tr>
<tr>
<td>Number</td>
<td>Severity</td>
<td>Event Text</td>
</tr>
<tr>
<td>--------</td>
<td>----------</td>
<td>---------------------------------------------------------------------------</td>
</tr>
<tr>
<td>0x0083</td>
<td>Fatal</td>
<td>Unable to access device %s</td>
</tr>
<tr>
<td>0x0084</td>
<td>Information</td>
<td>Dedicated Hot Spare created on %s (%s)</td>
</tr>
<tr>
<td>0x0085</td>
<td>Information</td>
<td>Dedicated Hot Spare %s disabled</td>
</tr>
<tr>
<td>0x0086</td>
<td>Critical</td>
<td>Dedicated Hot Spare %s no longer useful for all drive groups</td>
</tr>
<tr>
<td>0x0087</td>
<td>Information</td>
<td>Global Hot Spare created on %s (%s)</td>
</tr>
<tr>
<td>0x0088</td>
<td>Information</td>
<td>Global Hot Spare %s disabled</td>
</tr>
<tr>
<td>0x0089</td>
<td>Critical</td>
<td>Global Hot Spare does not cover all drive groups</td>
</tr>
<tr>
<td>0x008a</td>
<td>Information</td>
<td>Created %s</td>
</tr>
<tr>
<td>0x008b</td>
<td>Information</td>
<td>Deleted %s</td>
</tr>
<tr>
<td>0x008c</td>
<td>Information</td>
<td>Marking LD %s inconsistent due to active writes at shutdown</td>
</tr>
<tr>
<td>0x008d</td>
<td>Information</td>
<td>Battery Present</td>
</tr>
<tr>
<td>0x008e</td>
<td>Warning</td>
<td>Battery Not Present</td>
</tr>
<tr>
<td>0x008f</td>
<td>Information</td>
<td>New Battery Detected</td>
</tr>
<tr>
<td>0x0090</td>
<td>Information</td>
<td>Battery has been replaced</td>
</tr>
<tr>
<td>0x0091</td>
<td>Critical</td>
<td>Battery temperature is high</td>
</tr>
<tr>
<td>0x0092</td>
<td>Warning</td>
<td>Battery voltage low</td>
</tr>
<tr>
<td>0x0093</td>
<td>Information</td>
<td>Battery started charging</td>
</tr>
<tr>
<td>0x0094</td>
<td>Information</td>
<td>Battery is discharging</td>
</tr>
<tr>
<td>0x0095</td>
<td>Information</td>
<td>Battery temperature is normal</td>
</tr>
<tr>
<td>0x0096</td>
<td>Fatal</td>
<td>Battery has failed and cannot support data retention. Please replace the battery.</td>
</tr>
<tr>
<td>0x0097</td>
<td>Information</td>
<td>Battery relearn started</td>
</tr>
<tr>
<td>0x0098</td>
<td>Information</td>
<td>Battery relearn in progress</td>
</tr>
<tr>
<td>0x0099</td>
<td>Information</td>
<td>Battery relearn completed</td>
</tr>
<tr>
<td>0x009a</td>
<td>Critical</td>
<td>Battery relearn timed out</td>
</tr>
<tr>
<td>0x009b</td>
<td>Information</td>
<td>Battery relearn pending: Battery is under charge</td>
</tr>
<tr>
<td>0x009c</td>
<td>Information</td>
<td>Battery relearn postponed</td>
</tr>
<tr>
<td>0x009d</td>
<td>Information</td>
<td>Battery relearn will start in 4 days</td>
</tr>
<tr>
<td>0x009e</td>
<td>Information</td>
<td>Battery relearn will start in 2 day</td>
</tr>
<tr>
<td>0x009f</td>
<td>Information</td>
<td>Battery relearn will start in 1 day</td>
</tr>
<tr>
<td>0x00a0</td>
<td>Information</td>
<td>Battery relearn will start in 5 hours</td>
</tr>
</tbody>
</table>
## Table 3  Event Messages (Cont.)

<table>
<thead>
<tr>
<th>Number</th>
<th>Severity Level</th>
<th>Event Text</th>
</tr>
</thead>
<tbody>
<tr>
<td>0xA1</td>
<td>Information</td>
<td>Battery removed</td>
</tr>
<tr>
<td>0xA2</td>
<td>Information</td>
<td>Current capacity of the battery is below threshold</td>
</tr>
<tr>
<td>0xA3</td>
<td>Information</td>
<td>Current capacity of the battery is above threshold</td>
</tr>
<tr>
<td>0xA4</td>
<td>Information</td>
<td>Enclosure (SES) discovered on %s</td>
</tr>
<tr>
<td>0xA5</td>
<td>Information</td>
<td>Enclosure (SAFTE) discovered on %s</td>
</tr>
<tr>
<td>0xA6</td>
<td>Critical</td>
<td>Enclosure %s communication lost</td>
</tr>
<tr>
<td>0xA7</td>
<td>Information</td>
<td>Enclosure %s communication restored</td>
</tr>
<tr>
<td>0xA8</td>
<td>Critical</td>
<td>Enclosure %s fan %d failed</td>
</tr>
<tr>
<td>0xA9</td>
<td>Information</td>
<td>Enclosure %s fan %d inserted</td>
</tr>
<tr>
<td>0xAA</td>
<td>Critical</td>
<td>Enclosure %s fan %d removed</td>
</tr>
<tr>
<td>0xAB</td>
<td>Critical</td>
<td>Enclosure %s power supply %d failed</td>
</tr>
<tr>
<td>0xAC</td>
<td>Information</td>
<td>Enclosure %s power supply %d inserted</td>
</tr>
<tr>
<td>0xAD</td>
<td>Critical</td>
<td>Enclosure %s power supply %d removed</td>
</tr>
<tr>
<td>0xAE</td>
<td>Critical</td>
<td>Enclosure %s SIM %d failed</td>
</tr>
<tr>
<td>0xAF</td>
<td>Information</td>
<td>Enclosure %s SIM %d inserted</td>
</tr>
<tr>
<td>0xB0</td>
<td>Critical</td>
<td>Enclosure %s SIM %d removed</td>
</tr>
<tr>
<td>0xB1</td>
<td>Warning</td>
<td>Enclosure %s temperature sensor %d below warning threshold</td>
</tr>
<tr>
<td>0xB2</td>
<td>Critical</td>
<td>Enclosure %s temperature sensor %d below error threshold</td>
</tr>
<tr>
<td>0xB3</td>
<td>Warning</td>
<td>Enclosure %s temperature sensor %d above warning threshold</td>
</tr>
<tr>
<td>0xB4</td>
<td>Critical</td>
<td>Enclosure %s temperature sensor %d above error threshold</td>
</tr>
<tr>
<td>0xB5</td>
<td>Critical</td>
<td>Enclosure %s shutdown</td>
</tr>
<tr>
<td>0xB6</td>
<td>Warning</td>
<td>Enclosure %s not supported; too many enclosures connected to port</td>
</tr>
<tr>
<td>0xB7</td>
<td>Critical</td>
<td>Enclosure %s firmware mismatch</td>
</tr>
<tr>
<td>0xB8</td>
<td>Warning</td>
<td>Enclosure %s sensor %d bad</td>
</tr>
<tr>
<td>0xB9</td>
<td>Critical</td>
<td>Enclosure %s phy %d bad</td>
</tr>
<tr>
<td>0xBA</td>
<td>Critical</td>
<td>Enclosure %s is unstable</td>
</tr>
<tr>
<td>0xBB</td>
<td>Critical</td>
<td>Enclosure %s hardware error</td>
</tr>
<tr>
<td>0xBC</td>
<td>Critical</td>
<td>Enclosure %s not responding</td>
</tr>
<tr>
<td>0xBD</td>
<td>Information</td>
<td>SAS/SATA mixing not supported in enclosure; Drive %s disabled</td>
</tr>
<tr>
<td>0xBE</td>
<td>Information</td>
<td>Enclosure (SES) hotplug on %s was detected, but is not supported</td>
</tr>
<tr>
<td>Number</td>
<td>Severity Level</td>
<td>Event Text</td>
</tr>
<tr>
<td>--------</td>
<td>----------------</td>
<td>------------</td>
</tr>
<tr>
<td>0x00bf</td>
<td>Information</td>
<td>Clustering enabled</td>
</tr>
<tr>
<td>0x00c0</td>
<td>Information</td>
<td>Clustering disabled</td>
</tr>
<tr>
<td>0x00c1</td>
<td>Information</td>
<td>Drive too small to be used for auto-rebuild on %s</td>
</tr>
<tr>
<td>0x00c2</td>
<td>Information</td>
<td>BBU enabled; changing WT virtual drives to WB</td>
</tr>
<tr>
<td>0x00c3</td>
<td>Warning</td>
<td>BBU disabled; changing WB virtual drives to WT</td>
</tr>
<tr>
<td>0x00c4</td>
<td>Warning</td>
<td>Bad block table on drive %s is 80% full</td>
</tr>
<tr>
<td>0x00c5</td>
<td>Fatal</td>
<td>Bad block table on drive %s is full; unable to log block %lx</td>
</tr>
<tr>
<td>0x00c6</td>
<td>Information</td>
<td>Consistency Check Aborted due to ownership loss on %s</td>
</tr>
<tr>
<td>0x00c7</td>
<td>Information</td>
<td>Background Initialization (BGI) Aborted Due to Ownership Loss on %s</td>
</tr>
<tr>
<td>0x00c8</td>
<td>Critical</td>
<td>Battery/charger problems detected; SOH Bad</td>
</tr>
<tr>
<td>0x00c9</td>
<td>Warning</td>
<td>Single-bit ECC error: ECAR=%x, ELOG=%x, (%s); warning threshold exceeded</td>
</tr>
<tr>
<td>0x00ca</td>
<td>Critical</td>
<td>Single-bit ECC error: ECAR=%x, ELOG=%x, (%s); critical threshold exceeded</td>
</tr>
<tr>
<td>0x00cb</td>
<td>Critical</td>
<td>Single-bit ECC error: ECAR=%x, ELOG=%x, (%s); further reporting disabled</td>
</tr>
<tr>
<td>0x00cc</td>
<td>Critical</td>
<td>Enclosure %s Power supply %d switched off</td>
</tr>
<tr>
<td>0x00cd</td>
<td>Information</td>
<td>Enclosure %s Power supply %d switched on</td>
</tr>
<tr>
<td>0x00ce</td>
<td>Critical</td>
<td>Enclosure %s Power supply %d cable removed</td>
</tr>
<tr>
<td>0x00cf</td>
<td>Information</td>
<td>Enclosure %s Power supply %d cable inserted</td>
</tr>
<tr>
<td>0x00d0</td>
<td>Information</td>
<td>Enclosure %s Fan %d returned to normal</td>
</tr>
<tr>
<td>0x00d1</td>
<td>Information</td>
<td>BBU Retention test was initiated on previous boot</td>
</tr>
<tr>
<td>0x00d2</td>
<td>Information</td>
<td>BBU Retention test passed</td>
</tr>
<tr>
<td>0x00d3</td>
<td>Critical</td>
<td>BBU Retention test failed!</td>
</tr>
<tr>
<td>0x00d4</td>
<td>Information</td>
<td>NVRAM Retention test was initiated on previous boot</td>
</tr>
<tr>
<td>0x00d5</td>
<td>Information</td>
<td>NVRAM Retention test passed</td>
</tr>
<tr>
<td>0x00d6</td>
<td>Critical</td>
<td>NVRAM Retention test failed!</td>
</tr>
<tr>
<td>0x00d7</td>
<td>Information</td>
<td>%s test completed %d passes successfully</td>
</tr>
<tr>
<td>0x00d8</td>
<td>Critical</td>
<td>%s test FAILED on %d pass. Fail data: errorOffset=%x goodData=%x badData=%x</td>
</tr>
<tr>
<td>0x00d9</td>
<td>Information</td>
<td>Self check diagnostics completed</td>
</tr>
<tr>
<td>0x00da</td>
<td>Information</td>
<td>Foreign Configuration detected</td>
</tr>
<tr>
<td>0x00db</td>
<td>Information</td>
<td>Foreign Configuration imported</td>
</tr>
<tr>
<td>0x00dc</td>
<td>Information</td>
<td>Foreign Configuration cleared</td>
</tr>
</tbody>
</table>
### Table 3  Event Messages (Cont.)

<table>
<thead>
<tr>
<th>Number</th>
<th>Severity</th>
<th>Event Text</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x00dd</td>
<td>Warning</td>
<td>NVRAM is corrupt; reinitializing</td>
</tr>
<tr>
<td>0x00de</td>
<td>Warning</td>
<td>NVRAM mismatch occurred</td>
</tr>
<tr>
<td>0x00df</td>
<td>Warning</td>
<td>SAS wide port %d lost link on PHY %d</td>
</tr>
<tr>
<td>0x00e0</td>
<td>Information</td>
<td>SAS wide port %d restored link on PHY %d</td>
</tr>
<tr>
<td>0x00e1</td>
<td>Warning</td>
<td>SAS port %d, PHY %d has exceeded the allowed error rate</td>
</tr>
<tr>
<td>0x00e2</td>
<td>Warning</td>
<td>Bad block reassigned on %s at %lx to %lx</td>
</tr>
<tr>
<td>0x00e3</td>
<td>Information</td>
<td>Controller Hot Plug detected</td>
</tr>
<tr>
<td>0x00e4</td>
<td>Warning</td>
<td>Enclosure %s temperature sensor %d differential detected</td>
</tr>
<tr>
<td>0x00e5</td>
<td>Information</td>
<td>Drive test cannot start. No qualifying drives found</td>
</tr>
<tr>
<td>0x00e6</td>
<td>Information</td>
<td>Time duration provided by host is not sufficient for self check</td>
</tr>
<tr>
<td>0x00e7</td>
<td>Information</td>
<td>Marked Missing for %s on drive group %d row %d</td>
</tr>
<tr>
<td>0x00e8</td>
<td>Information</td>
<td>Replaced Missing as %s on drive group %d row %d</td>
</tr>
<tr>
<td>0x00e9</td>
<td>Information</td>
<td>Enclosure %s Temperature %d returned to normal</td>
</tr>
<tr>
<td>0x00ea</td>
<td>Information</td>
<td>Enclosure %s Firmware download in progress</td>
</tr>
<tr>
<td>0x00eb</td>
<td>Warning</td>
<td>Enclosure %s Firmware download failed</td>
</tr>
<tr>
<td>0x00ec</td>
<td>Warning</td>
<td>%s is not a certified drive</td>
</tr>
<tr>
<td>0x00ed</td>
<td>Information</td>
<td>Dirty cache data discarded by user</td>
</tr>
<tr>
<td>0x00ee</td>
<td>Information</td>
<td>Drives missing from configuration at boot</td>
</tr>
<tr>
<td>0x00ef</td>
<td>Information</td>
<td>Virtual drives (VDs) missing drives and will go offline at boot: %s</td>
</tr>
<tr>
<td>0x00f0</td>
<td>Information</td>
<td>VDs missing at boot: %s</td>
</tr>
<tr>
<td>0x00f1</td>
<td>Information</td>
<td>Previous configuration completely missing at boot</td>
</tr>
<tr>
<td>0x00f2</td>
<td>Information</td>
<td>Battery charge complete</td>
</tr>
<tr>
<td>0x00f3</td>
<td>Information</td>
<td>Enclosure %s fan %d speed changed</td>
</tr>
<tr>
<td>0x00f4</td>
<td>Information</td>
<td>Dedicated spare %s imported as global due to missing arrays</td>
</tr>
<tr>
<td>0x00f5</td>
<td>Information</td>
<td>%s rebuild not possible as SAS/SATA is not supported in an array</td>
</tr>
<tr>
<td>0x00f6</td>
<td>Information</td>
<td>SEP %s has been rebooted as a part of enclosure firmware download. SEP will be unavailable until this process completes.</td>
</tr>
<tr>
<td>0x00f7</td>
<td>Information</td>
<td>Inserted PD: %s Info: %s</td>
</tr>
<tr>
<td>0x00f8</td>
<td>Information</td>
<td>Removed PD: %s Info: %s</td>
</tr>
<tr>
<td>0x00f9</td>
<td>Information</td>
<td>VD %s is now OPTIMAL</td>
</tr>
</tbody>
</table>
## Table 3  Event Messages (Cont.)

<table>
<thead>
<tr>
<th>Number</th>
<th>Severity</th>
<th>Event Text</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x00fa</td>
<td>Warning</td>
<td>VD %s is now PARTIALLY DEGRADED</td>
</tr>
<tr>
<td>0x00fb</td>
<td>Critical</td>
<td>VD %s is now DEGRADED</td>
</tr>
<tr>
<td>0x00fc</td>
<td>Fatal</td>
<td>VD %s is now OFFLINE</td>
</tr>
<tr>
<td>0x00fd</td>
<td>Warning</td>
<td>Battery requires reconditioning; please initiate a LEARN cycle</td>
</tr>
<tr>
<td>0x00fe</td>
<td>Warning</td>
<td>VD %s disabled because RAID-5 is not supported by this RAID key</td>
</tr>
<tr>
<td>0x00ff</td>
<td>Warning</td>
<td>VD %s disabled because RAID-6 is not supported by this controller</td>
</tr>
<tr>
<td>0x0100</td>
<td>Warning</td>
<td>VD %s disabled because SAS drives are not supported by this RAID key</td>
</tr>
<tr>
<td>0x0101</td>
<td>Warning</td>
<td>PD missing: %s</td>
</tr>
<tr>
<td>0x0102</td>
<td>Warning</td>
<td>Puncturing of LBAs enabled</td>
</tr>
<tr>
<td>0x0103</td>
<td>Warning</td>
<td>Puncturing of LBAs disabled</td>
</tr>
<tr>
<td>0x0104</td>
<td>Critical</td>
<td>Enclosure %s EMM %d not installed</td>
</tr>
<tr>
<td>0x0105</td>
<td>Information</td>
<td>Package version %s</td>
</tr>
<tr>
<td>0x0106</td>
<td>Warning</td>
<td>Global affinity Hot Spare %s commissioned in a different enclosure</td>
</tr>
<tr>
<td>0x0107</td>
<td>Warning</td>
<td>Foreign configuration table overflow</td>
</tr>
<tr>
<td>0x0108</td>
<td>Warning</td>
<td>Partial foreign configuration imported, PDs not imported:%s</td>
</tr>
<tr>
<td>0x0109</td>
<td>Information</td>
<td>Connector %s is active</td>
</tr>
<tr>
<td>0x010a</td>
<td>Information</td>
<td>Board Revision %s</td>
</tr>
<tr>
<td>0x010b</td>
<td>Warning</td>
<td>Command timeout on PD %s, CDB:%s</td>
</tr>
<tr>
<td>0x010c</td>
<td>Warning</td>
<td>PD %s reset (Type %02x)</td>
</tr>
<tr>
<td>0x010d</td>
<td>Warning</td>
<td>VD bad block table on %s is 80% full</td>
</tr>
<tr>
<td>0x010e</td>
<td>Fatal</td>
<td>VD bad block table on %s is full; unable to log block %lx (on %s at %lx)</td>
</tr>
<tr>
<td>0x010f</td>
<td>Fatal</td>
<td>Uncorrectable medium error logged for %s at %lx (on %s at %lx)</td>
</tr>
<tr>
<td>0x0110</td>
<td>Information</td>
<td>VD medium error corrected on %s at %lx</td>
</tr>
<tr>
<td>0x0111</td>
<td>Warning</td>
<td>Bad block table on PD %s is 100% full</td>
</tr>
<tr>
<td>0x0112</td>
<td>Warning</td>
<td>VD bad block table on PD %s is 100% full</td>
</tr>
<tr>
<td>0x0113</td>
<td>Fatal</td>
<td>Controller needs replacement, IOP is faulty</td>
</tr>
<tr>
<td>0x0114</td>
<td>Information</td>
<td>CopyBack started on PD %s from PD %s</td>
</tr>
<tr>
<td>0x0115</td>
<td>Information</td>
<td>CopyBack aborted on PD %s and src is PD %s</td>
</tr>
<tr>
<td>0x0116</td>
<td>Information</td>
<td>CopyBack complete on PD %s from PD %s</td>
</tr>
<tr>
<td>0x0117</td>
<td>Progress</td>
<td>CopyBack progress on PD %s is %s</td>
</tr>
<tr>
<td>Number</td>
<td>Severity Level</td>
<td>Event Text</td>
</tr>
<tr>
<td>---------</td>
<td>----------------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>0x0 118</td>
<td>Information</td>
<td>CopyBack resumed on PD %s from %s</td>
</tr>
<tr>
<td>0x0119</td>
<td>Information</td>
<td>CopyBack automatically started on PD %s from %s</td>
</tr>
<tr>
<td>0x011a</td>
<td>Critical</td>
<td>CopyBack failed on PD %s due to source %s error</td>
</tr>
<tr>
<td>0x011b</td>
<td>Warning</td>
<td>Early Power off warning was unsuccessful</td>
</tr>
<tr>
<td>0x011c</td>
<td>Information</td>
<td>BBU FRU is %s</td>
</tr>
<tr>
<td>0x011d</td>
<td>Information</td>
<td>%s FRU is %s</td>
</tr>
<tr>
<td>0x011e</td>
<td>Information</td>
<td>Controller hardware revision ID %s</td>
</tr>
<tr>
<td>0x011f</td>
<td>Warning</td>
<td>Foreign import shall result in a backward incompatible upgrade of configuration metadata</td>
</tr>
<tr>
<td>0x0120</td>
<td>Information</td>
<td>Redundant path restored for PD %s</td>
</tr>
<tr>
<td>0x0121</td>
<td>Warning</td>
<td>Redundant path broken for PD %s</td>
</tr>
<tr>
<td>0x0122</td>
<td>Information</td>
<td>Redundant enclosure EMM %s inserted for EMM %s</td>
</tr>
<tr>
<td>0x0123</td>
<td>Information</td>
<td>Redundant enclosure EMM %s removed for EMM %s</td>
</tr>
<tr>
<td>0x0124</td>
<td>Warning</td>
<td>Patrol Read can't be started, as PDs are either not ONLINE, or are in a VD with an active process, or are in an excluded VD</td>
</tr>
<tr>
<td>0x0125</td>
<td>Information</td>
<td>Copyback aborted by user on PD %s and src is PD %s</td>
</tr>
<tr>
<td>0x0126</td>
<td>Critical</td>
<td>Copyback aborted on hot spare %s from %s, as hot spare needed for rebuild</td>
</tr>
<tr>
<td>0x0127</td>
<td>Warning</td>
<td>Copyback aborted on PD %s from PD %s, as rebuild required in the array</td>
</tr>
<tr>
<td>0x0128</td>
<td>Fatal</td>
<td>Controller cache discarded for missing or offline VD %s</td>
</tr>
<tr>
<td></td>
<td></td>
<td>When a VD with cached data goes offline or missing during runtime, the cache for the VD is discarded. Because the VD is offline, the cache cannot be saved.</td>
</tr>
<tr>
<td>0x0129</td>
<td>Information</td>
<td>Copyback cannot be started as PD %s is too small for src PD %s</td>
</tr>
<tr>
<td>0x012a</td>
<td>Information</td>
<td>Copyback cannot be started on PD %s from PD %s, as SAS/SATA is not supported in an array</td>
</tr>
<tr>
<td>0x012b</td>
<td>Information</td>
<td>Microcode update started on PD %s</td>
</tr>
<tr>
<td>0x012c</td>
<td>Information</td>
<td>Microcode update completed on PD %s</td>
</tr>
<tr>
<td>0x012d</td>
<td>Warning</td>
<td>Microcode update timeout on PD %s</td>
</tr>
<tr>
<td>0x012e</td>
<td>Warning</td>
<td>Microcode update failed on PD %s</td>
</tr>
<tr>
<td>0x012f</td>
<td>Information</td>
<td>Controller properties changed</td>
</tr>
<tr>
<td>0x0130</td>
<td>Information</td>
<td>Patrol Read properties changed</td>
</tr>
<tr>
<td>0x0131</td>
<td>Information</td>
<td>CC Schedule properties changed</td>
</tr>
<tr>
<td>0x0132</td>
<td>Information</td>
<td>Battery properties changed</td>
</tr>
<tr>
<td>Number</td>
<td>Severity</td>
<td>Event Text</td>
</tr>
<tr>
<td>---------</td>
<td>----------</td>
<td>---------------------------------------------------------------------------</td>
</tr>
<tr>
<td>0x0133</td>
<td>Warning</td>
<td>Periodic Battery Relearn is pending. Please initiate manual learn cycle as Automatic learn is not enabled</td>
</tr>
<tr>
<td>0x0134</td>
<td>Information</td>
<td>Drive security key created</td>
</tr>
<tr>
<td>0x0135</td>
<td>Information</td>
<td>Drive security key backed up</td>
</tr>
<tr>
<td>0x0136</td>
<td>Information</td>
<td>Drive security key from escrow, verified</td>
</tr>
<tr>
<td>0x0137</td>
<td>Information</td>
<td>Drive security key changed</td>
</tr>
<tr>
<td>0x0138</td>
<td>Warning</td>
<td>Drive security key, re-key operation failed</td>
</tr>
<tr>
<td>0x0139</td>
<td>Warning</td>
<td>Drive security key is invalid</td>
</tr>
<tr>
<td>0x013a</td>
<td>Information</td>
<td>Drive security key destroyed</td>
</tr>
<tr>
<td>0x013b</td>
<td>Warning</td>
<td>Drive security key from escrow is invalid</td>
</tr>
<tr>
<td>0x013c</td>
<td>Information</td>
<td>VD %s is now secured</td>
</tr>
<tr>
<td>0x013d</td>
<td>Warning</td>
<td>VD %s is partially secured</td>
</tr>
<tr>
<td>0x013e</td>
<td>Information</td>
<td>PD %s security activated</td>
</tr>
<tr>
<td>0x013f</td>
<td>Information</td>
<td>PD %s security disabled</td>
</tr>
<tr>
<td>0x0140</td>
<td>Information</td>
<td>PD %s is reprovisioned</td>
</tr>
<tr>
<td>0x0141</td>
<td>Information</td>
<td>PD %s security key changed</td>
</tr>
<tr>
<td>0x0142</td>
<td>Fatal</td>
<td>Security subsystem problems detected for PD %s</td>
</tr>
<tr>
<td>0x0143</td>
<td>Fatal</td>
<td>Controller cache pinned for missing or offline VD %s</td>
</tr>
<tr>
<td>0x0144</td>
<td>Fatal</td>
<td>Controller cache pinned for missing or offline VDs: %s</td>
</tr>
<tr>
<td>0x0145</td>
<td>Information</td>
<td>Controller cache discarded by user for VDs: %s</td>
</tr>
<tr>
<td>0x0146</td>
<td>Information</td>
<td>Controller cache destaged for VD %s</td>
</tr>
<tr>
<td>0x0147</td>
<td>Warning</td>
<td>Consistency Check started on an inconsistent VD %s</td>
</tr>
<tr>
<td>0x0148</td>
<td>Warning</td>
<td>Drive security key failure, cannot access secured configuration</td>
</tr>
<tr>
<td>0x0149</td>
<td>Warning</td>
<td>Drive security pass phrase from user is invalid</td>
</tr>
<tr>
<td>0x014a</td>
<td>Warning</td>
<td>Detected error with the remote battery connector cable</td>
</tr>
<tr>
<td>0x014b</td>
<td>Information</td>
<td>Power state change on PD %s from %s to %s</td>
</tr>
<tr>
<td>0x014c</td>
<td>Information</td>
<td>Enclosure %s element (SES code 0x%x) status changed</td>
</tr>
<tr>
<td>0x014d</td>
<td>Information</td>
<td>PD %s rebuild not possible as HDD/CacheCade - SSD Caching mix is not supported in a drive group</td>
</tr>
<tr>
<td>0x014e</td>
<td>Information</td>
<td>Copyback cannot be started on PD %s from %s, as HDD/CacheCade - SSD Caching mix is not supported in a drive group</td>
</tr>
<tr>
<td>Number</td>
<td>Severity Level</td>
<td>Event Text</td>
</tr>
<tr>
<td>---------</td>
<td>----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>0x014f</td>
<td>Information</td>
<td>VD bad block table on %s is cleared</td>
</tr>
<tr>
<td>0x0150</td>
<td>Information</td>
<td>SAS topology error: 0x%lx</td>
</tr>
<tr>
<td>0x0151</td>
<td>Information</td>
<td>VD cluster of medium errors corrected for %s at %lx (on %s at %lx)</td>
</tr>
<tr>
<td>0x0152</td>
<td>Information</td>
<td>Controller requests a host bus rescan</td>
</tr>
<tr>
<td>0x0153</td>
<td>Information</td>
<td>Controller repurposed and factory defaults restored</td>
</tr>
<tr>
<td>0x0154</td>
<td>Information</td>
<td>Drive security key binding updated</td>
</tr>
<tr>
<td>0x0155</td>
<td>Information</td>
<td>Drive security is in EKM mode</td>
</tr>
<tr>
<td>0x0156</td>
<td>Warning</td>
<td>Drive security failed to communicate with EKMS</td>
</tr>
<tr>
<td>0x0157</td>
<td>Information</td>
<td>%s needs key to be %s %s</td>
</tr>
<tr>
<td>0x0158</td>
<td>Warning</td>
<td>%s secure failed</td>
</tr>
<tr>
<td>0x0159</td>
<td>Critical</td>
<td>Controller encountered a fatal error and was reset</td>
</tr>
<tr>
<td>0x015a</td>
<td>Information</td>
<td>Snapshots enabled on %s (Repository %s)</td>
</tr>
<tr>
<td>0x015b</td>
<td>Information</td>
<td>Snapshots disabled on %s (Repository %s) by the user</td>
</tr>
<tr>
<td>0x015c</td>
<td>Critical</td>
<td>Snapshots disabled on %s (Repository %s), due to a fatal error</td>
</tr>
<tr>
<td>0x015d</td>
<td>Information</td>
<td>Snapshot created on %s at %s</td>
</tr>
<tr>
<td>0x015e</td>
<td>Information</td>
<td>Snapshot deleted on %s at %s</td>
</tr>
<tr>
<td>0x015f</td>
<td>Information</td>
<td>View created at %s to a snapshot at %s for %s</td>
</tr>
<tr>
<td>0x0160</td>
<td>Information</td>
<td>View at %s is deleted, to snapshot at %s for %s</td>
</tr>
<tr>
<td>0x0161</td>
<td>Information</td>
<td>Snapshot rollback started on %s from snapshot at %s</td>
</tr>
<tr>
<td>0x0162</td>
<td>Fatal</td>
<td>Snapshot rollback on %s internally aborted for snapshot at %s</td>
</tr>
<tr>
<td>0x0163</td>
<td>Information</td>
<td>Snapshot rollback on %s completed for snapshot at %s</td>
</tr>
<tr>
<td>0x0164</td>
<td>Progress</td>
<td>Snapshot rollback progress for snapshot at %s, on %s is %s</td>
</tr>
<tr>
<td>0x0165</td>
<td>Warning</td>
<td>Snapshot space for %s in snapshot repository %s, is 80%% full</td>
</tr>
<tr>
<td>0x0166</td>
<td>Critical</td>
<td>Snapshot space for %s in snapshot repository %s, is full</td>
</tr>
<tr>
<td>0x0167</td>
<td>Warning</td>
<td>View at %s to snapshot at %s, is 80%% full on snapshot repository %s</td>
</tr>
<tr>
<td>0x0168</td>
<td>Critical</td>
<td>View at %s to snapshot at %s, is full on snapshot repository %s</td>
</tr>
<tr>
<td>0x0169</td>
<td>Critical</td>
<td>Snapshot repository lost for %s</td>
</tr>
<tr>
<td>0x016a</td>
<td>Warning</td>
<td>Snapshot repository restored for %s</td>
</tr>
<tr>
<td>0x016b</td>
<td>Critical</td>
<td>Snapshot encountered an unexpected internal error: 0x%lx</td>
</tr>
<tr>
<td>0x016c</td>
<td>Information</td>
<td>Auto Snapshot enabled on %s (snapshot repository %s)</td>
</tr>
<tr>
<td>Number</td>
<td>Severity Level</td>
<td>Event Text</td>
</tr>
<tr>
<td>---------</td>
<td>----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>0x016d</td>
<td>Information</td>
<td>Auto Snapshot disabled on %s (snapshot repository %s)</td>
</tr>
<tr>
<td>0x016e</td>
<td>Critical</td>
<td>Configuration command could not be committed to disk, please retry</td>
</tr>
<tr>
<td>0x016f</td>
<td>Information</td>
<td>COD on %s updated as it was stale</td>
</tr>
<tr>
<td>0x0170</td>
<td>Warning</td>
<td>Power state change failed on %s (from %s to %s)</td>
</tr>
<tr>
<td>0x0171</td>
<td>Warning</td>
<td>%s is not available</td>
</tr>
<tr>
<td>0x0172</td>
<td>Information</td>
<td>%s is available</td>
</tr>
<tr>
<td>0x0173</td>
<td>Information</td>
<td>%s is used for CacheCade - SSD Caching with capacity 0x%lx logical blocks</td>
</tr>
<tr>
<td>0x0174</td>
<td>Information</td>
<td>%s is using CacheCade - SSD Caching %s</td>
</tr>
<tr>
<td>0x0175</td>
<td>Information</td>
<td>%s is no longer using CacheCade - SSD Caching %s</td>
</tr>
<tr>
<td>0x0176</td>
<td>Critical</td>
<td>Snapshot deleted due to resource constraints for %s in snapshot repository %s</td>
</tr>
<tr>
<td>0x0177</td>
<td>Warning</td>
<td>Auto Snapshot failed for %s in snapshot repository %s</td>
</tr>
<tr>
<td>0x0178</td>
<td>Warning</td>
<td>Controller reset on-board expander</td>
</tr>
<tr>
<td>0x0179</td>
<td>Warning</td>
<td>CacheCade - SSD Caching (%s) capacity changed and is now 0x%lx logical blocks</td>
</tr>
<tr>
<td>0x017a</td>
<td>Warning</td>
<td>Battery cannot initiate transparent learn cycles</td>
</tr>
<tr>
<td>0x017b</td>
<td>Information</td>
<td>Premium feature %s key was applied for - %s</td>
</tr>
<tr>
<td>0x017c</td>
<td>Information</td>
<td>Snapshot schedule properties changed on %s</td>
</tr>
<tr>
<td>0x017d</td>
<td>Information</td>
<td>Snapshot scheduled action is due on %s</td>
</tr>
<tr>
<td>0x017e</td>
<td>Information</td>
<td>Performance Metrics: collection command 0x%lx</td>
</tr>
<tr>
<td>0x017f</td>
<td>Information</td>
<td>Premium feature %s key was transferred - %s</td>
</tr>
<tr>
<td>0x0180</td>
<td>Information</td>
<td>Premium feature serial number %s</td>
</tr>
<tr>
<td>0x0181</td>
<td>Warning</td>
<td>Premium feature serial number mismatched. Key-vault serial num - %s</td>
</tr>
<tr>
<td>0x0182</td>
<td>Warning</td>
<td>Battery cannot support data retention for more than %d hours. Please replace the battery</td>
</tr>
<tr>
<td>0x0183</td>
<td>Information</td>
<td>%s power policy changed to %s (from %s)</td>
</tr>
<tr>
<td>0x0184</td>
<td>Warning</td>
<td>%s cannot transition to max power savings</td>
</tr>
<tr>
<td>0x0185</td>
<td>Information</td>
<td>Host driver is loaded and operational</td>
</tr>
<tr>
<td>0x0186</td>
<td>Information</td>
<td>%s mirror broken</td>
</tr>
<tr>
<td>0x0187</td>
<td>Information</td>
<td>%s mirror joined</td>
</tr>
<tr>
<td>0x0188</td>
<td>Warning</td>
<td>%s link %d failure in wide port</td>
</tr>
<tr>
<td>0x0189</td>
<td>Information</td>
<td>%s link %d restored in wide port</td>
</tr>
</tbody>
</table>
### Table 3  Event Messages (Cont.)

<table>
<thead>
<tr>
<th>Number</th>
<th>Severity Level</th>
<th>Event Text</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x018a</td>
<td>Information</td>
<td>Memory module FRU is %s</td>
</tr>
<tr>
<td>0x018b</td>
<td>Warning</td>
<td>Cache-vault power pack is sub-optimal. Please replace the pack</td>
</tr>
<tr>
<td>0x018c</td>
<td>Warning</td>
<td>Foreign configuration auto-import did not import any drives</td>
</tr>
<tr>
<td>0x018d</td>
<td>Warning</td>
<td>Cache-vault microcode update required</td>
</tr>
<tr>
<td>0x018e</td>
<td>Warning</td>
<td>CacheCade(TM) (%s) capacity exceeds maximum allowed size, extra capacity is not used</td>
</tr>
<tr>
<td>0x018f</td>
<td>Warning</td>
<td>LD (%s) protection information lost</td>
</tr>
<tr>
<td>0x0190</td>
<td>Information</td>
<td>Diagnostics passed for %s</td>
</tr>
<tr>
<td>0x0191</td>
<td>Critical</td>
<td>Diagnostics failed for %s</td>
</tr>
<tr>
<td>0x0192</td>
<td>Information</td>
<td>Server Power capability Diagnostic Test Started</td>
</tr>
<tr>
<td>0x0193</td>
<td>Information</td>
<td>Drive Cache settings enabled during rebuild for %s</td>
</tr>
<tr>
<td>0x0194</td>
<td>Information</td>
<td>Drive Cache settings restored after rebuild for %s</td>
</tr>
<tr>
<td>0x0195</td>
<td>Information</td>
<td>Drive %s commissioned as Emergency spare</td>
</tr>
<tr>
<td>0x0196</td>
<td>Warning</td>
<td>Reminder: Potential non-optimal configuration due to drive %s commissioned as emergency spare</td>
</tr>
<tr>
<td>0x0197</td>
<td>Information</td>
<td>Consistency Check suspended on %s</td>
</tr>
<tr>
<td>0x0198</td>
<td>Information</td>
<td>Consistency Check resumed on %s</td>
</tr>
<tr>
<td>0x0199</td>
<td>Information</td>
<td>Background Initialization suspended on %s</td>
</tr>
<tr>
<td>0x019a</td>
<td>Information</td>
<td>Background Initialization resumed on %</td>
</tr>
<tr>
<td>0x019b</td>
<td>Information</td>
<td>Reconstruction suspended on %s</td>
</tr>
<tr>
<td>0x019c</td>
<td>Information</td>
<td>Rebuild suspended on %</td>
</tr>
<tr>
<td>0x019d</td>
<td>Information</td>
<td>Copyback suspended on %</td>
</tr>
<tr>
<td>0x019e</td>
<td>Information</td>
<td>Reminder: Consistency Check suspended on %</td>
</tr>
<tr>
<td>0x019f</td>
<td>Information</td>
<td>Reminder: Background Initialization suspended on %</td>
</tr>
<tr>
<td>0x01a0</td>
<td>Information</td>
<td>Reminder: Reconstruction suspended on %</td>
</tr>
<tr>
<td>0x01a1</td>
<td>Information</td>
<td>Reminder: Rebuild suspended on %</td>
</tr>
<tr>
<td>0x01a2</td>
<td>Information</td>
<td>Reminder: Copyback suspended on %</td>
</tr>
<tr>
<td>0x01a3</td>
<td>Information</td>
<td>Reminder: Patrol Read suspended</td>
</tr>
<tr>
<td>0x01a4</td>
<td>Information</td>
<td>Erase aborted on %</td>
</tr>
<tr>
<td>0x01a5</td>
<td>Critical</td>
<td>Erase failed on %s (Error %02x)</td>
</tr>
<tr>
<td>0x01a6</td>
<td>Progress</td>
<td>Erase progress on %s is %s</td>
</tr>
</tbody>
</table>
### Table 3  
**Event Messages (Cont.)**

<table>
<thead>
<tr>
<th>Number</th>
<th>Severity Level</th>
<th>Event Text</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x01a7</td>
<td>Information</td>
<td>Erase started on %s</td>
</tr>
<tr>
<td>0x01a8</td>
<td>Information</td>
<td>Erase completed on %s</td>
</tr>
<tr>
<td>0x01a9</td>
<td>Information</td>
<td>Erase aborted on %s</td>
</tr>
<tr>
<td>0x01aa</td>
<td>Critical</td>
<td>Erase failed on %s</td>
</tr>
<tr>
<td>0x01ab</td>
<td>Progress</td>
<td>Erase progress on %s is %s</td>
</tr>
<tr>
<td>0x01ac</td>
<td>Information</td>
<td>Erase started on %s</td>
</tr>
<tr>
<td>0x01ad</td>
<td>Information</td>
<td>Erase complete on %s</td>
</tr>
<tr>
<td>0x01ae</td>
<td>Warning</td>
<td>Potential leakage during erase on %s</td>
</tr>
<tr>
<td>0x01af</td>
<td>Warning</td>
<td>Battery charging was suspended due to high battery temperature</td>
</tr>
<tr>
<td>0x01b0</td>
<td>Information</td>
<td>NVCache firmware update was successful</td>
</tr>
<tr>
<td>0x01b1</td>
<td>Warning</td>
<td>NVCache firmware update failed</td>
</tr>
<tr>
<td>0x01b2</td>
<td>Fatal</td>
<td>%s access blocked as cached data in CacheCade(TM) is unavailable</td>
</tr>
<tr>
<td>0x01b3</td>
<td>Information</td>
<td>CacheCade(TM) disassociate started on %s</td>
</tr>
<tr>
<td>0x01b4</td>
<td>Information</td>
<td>CacheCade(TM) disassociate completed on %s</td>
</tr>
<tr>
<td>0x01b5</td>
<td>Critical</td>
<td>CacheCade(TM) disassociate failed on %s</td>
</tr>
<tr>
<td>0x01b6</td>
<td>Progress</td>
<td>CacheCade(TM) disassociate progress on %s is %s</td>
</tr>
<tr>
<td>0x01b7</td>
<td>Information</td>
<td>CacheCade(TM) disassociate aborted by user on %s</td>
</tr>
<tr>
<td>0x01b8</td>
<td>Information</td>
<td>Link speed changed on SAS port %d and PHY %d</td>
</tr>
<tr>
<td>0x01b9</td>
<td>Warning</td>
<td>Advanced Software Options was deactivated for - %s</td>
</tr>
<tr>
<td>0x01ba</td>
<td>Information</td>
<td>%s is now accessible</td>
</tr>
<tr>
<td>0x01bb</td>
<td>Information</td>
<td>%s is using CacheCade(TM)</td>
</tr>
<tr>
<td>0x01bc</td>
<td>Information</td>
<td>%s is no longer using CacheCade(TM)</td>
</tr>
<tr>
<td>0x01bd</td>
<td>Warning</td>
<td>Patrol Read aborted on %s</td>
</tr>
</tbody>
</table>
access policy – A virtual drive property indicating what kind of access is allowed for a particular virtual drive. The possible values are Read/Write, Read Only, or Blocked.

alarm enabled – A controller property that indicates whether the controller’s onboard alarm is enabled.

alarm present – A controller property that indicates whether the controller has an onboard alarm. If present and enabled, the alarm is sounded for certain error conditions.

array – See drive group.

BBU present – A controller property that indicates whether the controller has an onboard battery backup unit to provide power in case of a power failure.

BGI rate – A controller property indicating the rate at which the background initialization of virtual drives will be carried out.

BIOS – Basic Input/Output System. The computer BIOS is stored on a flash memory chip. The BIOS controls communications between the microprocessor and peripheral devices, such as the keyboard and the video controller, and miscellaneous functions, such as system messages.

cache – Fast memory that holds recently accessed data. Use of cache memory speeds subsequent access to the same data. When data is read from or written to main memory, a copy is also saved in cache memory with the associated main memory address. The cache memory software monitors the addresses of subsequent reads to see if the required data is already stored in cache memory. If it is already in cache memory (a cache hit), it is read from cache memory immediately and the main memory read is aborted (or not started). If the data is not cached (a cache miss), it is fetched from main memory and saved in cache memory.

cache flush interval – A controller property that indicates how often the data cache is flushed.

caching – The process of using a high speed memory buffer to speed up a computer system’s overall read/write performance. The cache can be accessed at a higher speed than a drive subsystem. To improve read performance, the cache usually contains the most recently accessed data, as well as data from adjacent drive sectors. To improve write performance, the cache may temporarily store data in accordance with its write back policies.

capacity – A property that indicates the amount of storage space on a drive or virtual drive.

coerced capacity – A drive property indicating the capacity to which a drive has been coerced (forced) to make it compatible with other drives that are nominally the same capacity. For example, a 4 Gbyte drive from one manufacturer may be 4,196 Mbytes, and a 4 Gbyte from another manufacturer may be 4,128 Mbytes. These drives could be coerced to a usable capacity of 4,088 Mbytes each for use in a drive group in a storage configuration.

coercion mode – A controller property indicating the capacity to which drives of nominally identical capacity are coerced (forced) to make them usable in a storage configuration.

consistency check – An operation that verifies that all stripes in a virtual drive with a redundant RAID level are consistent and that automatically fixes any errors. For RAID 1 drive groups, this operation verifies correct mirrored data for each stripe.
**consistency check rate** – The rate at which consistency check operations are run on a computer system.

**controller** – A chip that controls the transfer of data between the microprocessor and memory or between the microprocessor and a peripheral device such as a drive. RAID controllers perform RAID functions such as striping and mirroring to provide data protection. MegaRAID Storage Manager software runs on LSI SAS controllers.

**copyback** – The procedure used to copy data from a source drive of a virtual drive to a destination drive that is not a part of the virtual drive. The copyback operation is often used to create or restore a specific physical configuration for a drive group (for example, a specific arrangement of drive group members on the device I/O buses). The copyback operation can be run automatically or manually.

Typically, a drive fails or is expected to fail, and the data is rebuilt on a hot spare. The failed drive is replaced with a new drive. Then the data is copied from the hot spare to the new drive, and the hot spare reverts from a rebuild drive to its original hot spare status. The copyback operation runs as a background activity, and the virtual drive is still available online to the host.

**current write policy** – A virtual drive property that indicates whether the virtual drive currently supports Write Back mode or Write Through mode.

- In Write Back mode the controller sends a data transfer completion signal to the host when the controller cache has received all of the data in a transaction.
- In Write Through mode the controller sends a data transfer completion signal to the host when the drive subsystem has received all of the data in a transaction.

**default write policy** – A virtual drive property indicating whether the default write policy is Write Through or Write Back. In Write Back mode the controller sends a data transfer completion signal to the host when the controller cache has received all of the data in a transaction. In Write Through mode the controller sends a data transfer completion signal to the host when the drive subsystem has received all of the data in a transaction.

**device ID** – A controller or drive property indicating the manufacturer-assigned device ID.

**device port count** – A controller property indicating the number of ports on the controller.

**drive cache policy** – A virtual drive property indicating whether the virtual drive cache is enabled, disabled, or unchanged from its previous setting.

**drive group** – A group of drives attached to a RAID controller on which one or more virtual drives can be created. All virtual drives in the drive group use all of the drives in the drive group.

**drive state** – A drive property indicating the status of the drive. A drive can be in one of the following states:

- Unconfigured Good: A drive accessible to the RAID controller but not configured as a part of a virtual drive or as a hot spare.
- Hot Spare: A drive that is configured as a hot spare.
- Online: A drive that can be accessed by the RAID controller and will be part of the virtual drive.
- Rebuild: A drive to which data is being written to restore full redundancy for a virtual drive.
- Failed: A drive that was originally configured as Online or Hot Spare, but on which the firmware detects an unrecoverable error.
• Unconfigured Bad: A drive on which the firmware detects an unrecoverable error; the drive was Unconfigured Good or the drive could not be initialized.

• Missing: A drive that was Online, but which has been removed from its location.

• Offline: A drive that is part of a virtual drive but which has invalid data as far as the RAID configuration is concerned.

• None: A drive with an unsupported flag set. An Unconfigured Good or Offline drive that has completed the prepare for removal operation.

drive subsystem – A collection of drives and the hardware that controls them and connects them to one or more controllers. The hardware can include an intelligent controller, or the drives can attach directly to a system I/O bus controller.

drive type – A drive property indicating the characteristics of the drive.

fast initialization – A mode of initialization that quickly writes zeroes to the first and last sectors of the virtual drive. This allows you to immediately start writing data to the virtual drive while the initialization is running in the background.

fault tolerance – The capability of the drive subsystem to undergo a single drive failure per drive group without compromising data integrity and processing capability. LSI SAS RAID controllers provides fault tolerance through redundant drive groups in RAID levels 1, 5, 6, 10, 50, and 60. They also support hot spare drives and the auto-rebuild feature.

firmware – Software stored in read-only memory (ROM) or programmable ROM (PROM). Firmware is often responsible for the behavior of a system when it is first turned on. A typical example would be a monitor program in a system that loads the full operating system from drive or from a network and then passes control to the operating system.

foreign configuration – A RAID configuration that already exists on a replacement set of drives that you install in a computer system. MegaRAID Storage Manager software allows you to import the existing configuration to the RAID controller, or you can clear the configuration so you can create a new one.

formatting – The process of writing a specific value to all data fields on a drive, to map out unreadable or bad sectors. Because most drives are formatted when manufactured, formatting is usually done only if a drive generates many media errors.

hole – In MegaRAID Storage Manager, a hole is a block of empty space in a drive group that can be used to define a virtual drive.

host interface – A controller property indicating the type of interface used by the computer host system: for example, PCIX.

host port count – A controller property indicating the number of host data ports currently in use.

host system – Any computer system on which the controller is installed. Mainframes, workstations, and stand-alone desktop systems can all be considered host systems.

hot spare – A standby drive that can automatically replace a failed drive in a virtual drive and prevent data from being lost. A hot spare can be dedicated to a single redundant drive group or it can be part of the global hot spare pool for all drive groups controlled by the controller.
When a drive fails, MegaRAID Storage Manager software automatically uses a hot spare to replace it and then rebuilds the data from the failed drive to the hot spare. Hot spares can be used in RAID 1, 5, 6, 10, 50, and 60 storage configurations.

initialization – The process of writing zeros to the data fields of a virtual drive and, in fault-tolerant RAID levels, generating the corresponding parity to put the virtual drive in a Ready state. Initialization erases all previous data on the drives. Drive groups will work without initializing, but they can fail a consistency check because the parity fields have not been generated.

IO policy – A virtual drive property indicating whether Cached I/O or Direct I/O is being used. In Cached I/O mode, all reads are buffered in cache memory. In Direct I/O mode, reads are not buffered in cache memory. Data is transferred to cache and the host concurrently. If the same data block is read again, it comes from cache memory. (The IO Policy applies to reads on a specific virtual drive. It does not affect the read ahead cache.)

LKM – Local Key Management

load-balancing – A method of spreading work between two or more computers, network links, CPUs, drives, or other resources. Load balancing is used to maximize resource use, throughput, or response time.

media error count – A drive property indicating the number of errors that have been detected on the drive media.

migration – The process of moving virtual drives and hot spare drives from one controller to another by disconnecting the drives from one controller and attaching them to another one. The firmware on the new controller will detect and retain the virtual drive information on the drives.

mirroring – The process of providing complete data redundancy with two drives by maintaining an exact copy of one drive’s data on the second drive. If one drive fails, the contents of the other drive can be used to maintain the integrity of the system and to rebuild the failed drive.

multipathing – The firmware provides support for detecting and using multiple paths from the RAID controllers to the SAS devices that are in enclosures. Devices connected to enclosures have multiple paths to them. With redundant paths to the same port of a device, if one path fails, another path can be used to communicate between the controller and the device. Using multiple paths with load balancing, instead of a single path, can increase reliability through redundancy.

name – A virtual drive property indicating the user-assigned name of the virtual drive.

non-redundant configuration – A RAID 0 virtual drive with data striped across two or more drives but without drive mirroring or parity. This provides for high data throughput but offers no protection in case of a drive failure.

NVRAM – Acronym for non-volatile random access memory. A storage system that does not lose the data stored on it when power is removed. NVRAM is used to store firmware and configuration data on the RAID controller.

NVRAM present – A controller property indicating whether an NVRAM is present on the controller.

NVRAM size – A controller property indicating the capacity of the controller’s NVRAM.
offline – A drive is offline when it is part of a virtual drive but its data is not accessible to the virtual drive.

patrol read – A process that checks the drives in a storage configuration for drive errors that could lead to drive failure and lost data. The patrol read operation can find and sometimes fix any potential problem with drives prior to host access. This enhances overall system performance because error recovery during a normal I/O operation may not be necessary.

patrol read rate – The user-defined rate at which patrol read operations are run on a computer system.

product info – A drive property indicating the vendor-assigned model number of the drive.

product name – A controller property indicating the manufacturing name of the controller.

RAID – A group of multiple, independent drives that provide high performance by increasing the number of drives used for saving and accessing data. A RAID drive group improves input/output (I/O) performance and data availability. The group of drives appears to the host system as a single storage unit or as multiple virtual drives. Data throughput improves because several drives can be accessed simultaneously. RAID configurations also improve data storage availability and fault tolerance. Redundant RAID levels (RAID levels 1, 5, 6, 10, 50, and 60) provide data protection.

RAID 0 – Uses data striping on one or more drives to provide high data throughput, especially for large files in an environment that requires no data redundancy.

RAID 00 – Uses data striping on two or more drives in a spanned drive group to provide high data throughput, especially for large files in an environment that requires no data redundancy.

RAID 1 – Uses data mirroring on pairs of drives so that data written to one drive is simultaneously written to the other drive. RAID 1 works well for small databases or other small applications that require complete data redundancy.

RAID 5 – Uses data striping and parity data across three or more drives (distributed parity) to provide high data throughput and data redundancy, especially for applications that require random access.

RAID 6 – Uses data striping and parity data across three or more drives (distributed parity) to provide high data throughput and data redundancy, especially for applications that require random access. RAID 6 can survive the failure of two drives.

RAID 10 – A combination of RAID 0 and RAID 1 that uses data striping across two mirrored drive groups. It provides high data throughput and complete data redundancy.

RAID 50 – A combination of RAID 0 and RAID 5 that uses data striping across two drive groups with parity data. It provides high data throughput and complete data redundancy.

RAID 60 – A combination of RAID 0 and RAID 6 that uses data striping across two drive groups with parity data. It provides high data throughput and complete data redundancy. RAID 60 can survive the failure of two drives in each RAID set in the spanned drive group.

RAID level – A virtual drive property indicating the RAID level of the virtual drive. MegaRAID SAS RAID controllers support RAID levels 0, 1, 5, 6, 00, 10, 50, and 60.
**raw capacity** – A drive property indicating the actual full capacity of the drive before any coercion mode is applied to reduce the capacity.

**read policy** – A controller attribute indicating the current Read Policy mode. In Always Read Ahead mode, the controller reads sequentially ahead of requested data and stores the additional data in cache memory, anticipating that the data will be needed soon. This speeds up reads for sequential data, but there is little improvement when accessing random data. In No Read Ahead mode, read ahead capability is disabled. In Adaptive Read Ahead mode, the controller begins using read ahead if the two most recent drive accesses occurred in sequential sectors. If the read requests are random, the controller reverts to No Read Ahead mode.

**rebuild** – The regeneration of all data to a replacement drive in a redundant virtual drive after a drive failure. A drive rebuild normally occurs without interrupting normal operations on the affected virtual drive, though some degradation of performance of the drive subsystem can occur.

**rebuild rate** – The percentage of central processing unit (CPU) resources devoted to rebuilding data onto a new drive after a drive in a storage configuration has failed.

**reclaim virtual drive** – A method of undoing the configuration of a new virtual drive. If you highlight the virtual drive in the Configuration Wizard and click the Reclaim button, the individual drives are removed from the virtual drive configuration.

**reconstruction rate** – The user-defined rate at which a reconstruction operation is carried out.

**redundancy** – A property of a storage configuration that prevents data from being lost when one drive fails in the configuration.

**redundant configuration** – A virtual drive that has redundant data on drives in the drive group that can be used to rebuild a failed drive. The redundant data can be parity data striped across multiple drives in a drive group, or it can be a complete mirrored copy of the data stored on a second drive. A redundant configuration protects the data in case a drive fails in the configuration.

**revertible hot spare** – When you use the Replace Member procedure, after data is copied from a hot spare to a new drive, the hot spare reverts from a rebuild drive to its original hot spare status.

**revision level** – A drive property that indicates the revision level of the drive’s firmware.

**SAS** – Acronym for Serial Attached SCSI. SAS is a serial, point-to-point, enterprise-level device interface that leverages the Small Computer System Interface (SCSI) protocol set. The SAS interface provides improved performance, simplified cabling, smaller connectors, lower pin count, and lower power requirements when compared to parallel SCSI.

**SATA** – Acronym for Serial Advanced Technology Attachment. A physical storage interface standard. SATA is a serial link that provides point-to-point connections between devices. The thinner serial cables allow for better airflow within the system and permit smaller chassis designs.

**SCSI device type** – A drive property indicating the type of the device, such as drive.

**serial no.** – A controller property indicating the manufacturer-assigned serial number.

**strip size** – The portion of a stripe that resides on a single drive in the drive group.

**stripe size** – A virtual drive property indicating the length of the interleaved data segments that the RAID controller writes across multiple drives, not including parity drives. For example, consider
a stripe that contains 64 KB of drive space and has 16 KB of data residing on each drive in the stripe. In this case, the stripe size is 64 KB and the strip size is 16 KB. The user can select the stripe size.

**striping** – A technique used to write data across all drives in a virtual drive. Each stripe consists of consecutive virtual drive data addresses that are mapped in fixed-size units to each drive in the virtual drive using a sequential pattern. For example, if the virtual drive includes five drives, the stripe writes data to drives one through five without repeating any of the drives. The amount of space consumed by a stripe is the same on each drive. Striping by itself does not provide data redundancy. Striping in combination with parity does provide data redundancy.

**subvendor ID** – A controller property that lists additional vendor ID information about the controller.

**uncorrectable error count** – A controller property that lists the number of uncorrectable errors detected on drives connected to the controller. If the error count reaches a certain level, a drive will be marked as failed.

**vendor ID** – A controller property indicating the vendor-assigned ID number of the controller.

**vendor info** – A drive property listing the name of the vendor of the drive.

**virtual drive** – A storage unit created by a RAID controller from one or more drives. Although a virtual drive may be created from several drives, it is seen by the operating system as a single drive. Depending on the RAID level used, the virtual drive may retain redundant data in case of a drive failure.

**virtual drive state** – A virtual drive property indicating the condition of the virtual drive. Examples include Optimal and Degraded.

**write-back** – In Write-Back Caching mode, the controller sends a data transfer completion signal to the host when the controller cache has received all of the data in a drive write transaction. Data is written to the drive subsystem in accordance with policies set up by the controller. These policies include the amount of dirty/clean cache lines, the number of cache lines available, and elapsed time from the last cache flush.

**write policy** – See *Default Write Policy*.

**write-through** – In Write-Through Caching mode, the controller sends a data transfer completion signal to the host when the drive subsystem has received all of the data and has completed the write transaction to the drive.