Dell OpenManage™ Server Administrator

Messages Reference Guide

Notes and Notices

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

NOTICE: A NOTICE indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

Trademarks used in this text: The *DELL* logo and *Dell OpenManage* are trademarks of Dell Inc.; *Microsoft* and *Windows* are registered trademarks of Microsoft Corporation; *Novell* and *NetWare* are registered trademarks of Novell, Inc.; *Red Hat* is a registered trademark of Red Hat, Inc.

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

July 2004

Contents

1 Introduction

Messages Not Described in This Guide **7**

Understanding Event Messages **8**

Sample Event Message Text 9

Viewing Event Messages **9**

Viewing Events in Windows 2000 and Windows Server 2003 10

Viewing Events in NetWare 10

Viewing Events in Red Hat Linux 10

Viewing the Event Information 11

Understanding the Event Description 11

2 Event Message Reference

Miscellaneous Messages **15**

Temperature Sensor Messages **17**

Cooling Device Messages **19**

Voltage Sensor Messages **21**

Current Sensor Messages **23**

Chassis Intrusion Messages **26**

Redundancy Unit Messages **28**

Power Supply Messages **30**

Memory Device Messages **33**

Fan Enclosure Messages **34**

AC Power Cord Messages **36**

Hardware Log Sensor Messages **37**

Processor Sensor Messages **38**

3 Storage Management Message Reference

Alert Monitoring and Logging **41**

Viewing Alerts **41**

Alert Severity Levels **42**

SNMP Support for Storage Management Alerts **42**

SNMP Trap Forwarding 42

SNMP Trap Definitions 43

SNMP Trap Variables 43

Viewing SNMP Traps **43**

Viewing Traps with HP OpenView Network Node Manager 43

Alert Descriptions and Corrective Actions **44**

Index 73

Tables

Table 1-1.	Event Description Reference	11
Table 2-1.	Miscellaneous Messages	15
Table 2-2.	Temperature Sensor Messages	17
Table 2-3.	Cooling Device Messages	20
Table 2-4.	Voltage Sensor Messages	21
Table 2-5.	Current Sensor Messages	24
Table 2-6.	Chassis Intrusion Messages	27
Table 2-7.	Redundancy Unit Messages	29
Table 2-8.	Power Supply Messages	31
Table 2-9.	Memory Device Messages	34
Table 2-10.	Fan Enclosure Messages	35
Table 2-11.	AC Power Cord Messages	36
Table 2-12.	Hardware Log Sensor Messages	37

Table 2-13. Processor Sensor Messages 39
Table 3-1. Storage Management Alert Severity 42
Table 3-2. Storage Management Messages 44

1

Introduction

Dell OpenManage Server Administrator produces event messages stored primarily in the operating system or Server Administrator event logs and sometimes in SNMP traps. This document describes the event messages created by Server Administrator version 1.8.1 or later and displayed in the Server Administrator Alert log.

Server Administrator creates events in response to sensor status changes and other monitored parameters. The Server Administrator event monitor uses these status change events to add descriptive messages to the operating system event log or the Server Administrator Alert log.

Each event message that Server Administrator adds to the Alert log consists of a unique identifier called the event ID for a specific event source category and a descriptive message. The event message includes the severity, cause of the event, and other relevant information, such as the event location and the monitored item's previous state.

Tables provided in this guide list all Server Administrator event IDs in numeric order. Each entry includes the event ID's corresponding description, severity level, and cause. Message text in angle brackets (for example, *<State>*) describes the event-specific information provided by the Server Administrator.

Messages Not Described in This Guide

This guide describes only event messages created by Server Administrator and displayed in the Server Administrator Alert log. For information on other messages produced by your system, consult one of the following sources:

- Your system's *Installation and Troubleshooting Guide*
- Other system documentation
- Operating system documentation
- Application program documentation

For RAID messages, see the *Dell OpenManage Array Manager* User's Guide.

Understanding Event Messages

This section describes the various types of event messages generated by the Server Administrator. When an event occurs on your system, the Server Administrator sends information about one of the following event types to the systems management console:

- **Information** — An event that describes the successful operation of a unit, such as a power supply turning on or a sensor reading returning to normal.
- **Warning** — An event that is not necessarily significant, but may indicate a possible future problem, such as crossing a warning threshold.
- **Error** — A significant event that indicates actual or imminent loss of data or loss of function, such as crossing a failure threshold or a hardware failure.

The Server Administrator generates events based on status changes in the following sensors:

- **Temperature Sensor** — Helps protect critical components by alerting the systems management console when temperatures become too high inside a chassis; also monitors a variety of locations in the chassis and in any attached systems.
- **Fan Sensor** — Monitors fans in various locations in the chassis and in any attached systems.
- **Voltage Sensor** — Monitors voltages across critical components in various chassis locations and in any attached systems.
- **Current Sensor** — Monitors the current (or amperage) output from the power supply (or supplies) in the chassis and in any attached systems.
- **Chassis Intrusion Sensor** — Monitors intrusion into the chassis and any attached systems.
- **Redundancy Unit Sensor** — Monitors redundant units (critical units such as fans, AC power cords, or power supplies) within the chassis; also monitors the chassis and any attached systems. For example, redundancy allows a second or *n*th fan to keep the chassis components at a safe temperature when another fan has failed. Redundancy is normal when the intended number of critical components are operating. Redundancy is degraded when a component fails but others are still operating. Redundancy is lost when there is one less critical redundancy device than required.
- **Power Supply Sensor** — Monitors power supplies in the chassis and in any attached systems.
- **Memory Prefailure Sensor** — Monitors memory modules by counting the number of ECC memory corrections.
- **Fan Enclosure Sensor** — Monitors protective fan enclosures by detecting their removal from and insertion into the system, and by measuring how long a fan enclosure is absent from the chassis. This sensor monitors the chassis and any attached systems.
- **AC Power Cord Sensor** — Monitors the presence of AC power for an AC power cord.
- **Hardware Log Sensor** — Monitors the size of a hardware log.
- **Processor Sensor** — Monitors the processor status in the system.

Sample Event Message Text

The following example shows the format of the event messages logged by Server Administrator.

```
EventID: 1000

Source: Server Administrator

Category: Instrumentation Service

Type: Information

Date and Time: Mon Oct 21 10:38:00 2002

Computer: <computer name>

Description:

Server Administrator starting

Data: Bytes in Hex
```

Viewing Event Messages

In Server Administrator, an event log is used to record information about important events. You can view the event log using an event viewer. Each operating system's event viewer accesses the applicable operating system event log.

The location of the event log file depends on the operating system you are using.

- In the Microsoft® Windows® 2000 Advanced Server and Windows Server 2003 operating systems, messages are logged to the system event log and optionally to a unicode text file, **dcsys32.log** (viewable using Notepad), that is located in the *install_path***omsa\log** directory. The default *install_path* is **C:\Program Files\Dell\OpenManage**.
- In the Novell® NetWare® versions 5.*x* and 6.*x* operating systems, messages are logged to a text file, **DCSYS32.LOG**, (viewable using a unicode text editor from a client attached to the system), that is located in the **\system\dell\omanage\omsa\log** directory.
- In the Red Hat® Linux operating system, messages are logged to the system log file. The default name of the system log file is **/var/log/messages**. You can view the messages file using a text editor such as vi or emacs.

NOTE: Logging messages to a unicode text file is optional. By default, the feature is disabled. To enable this feature, modify the **Event Manager** section of the **dcemdy32.ini** file as follows:

- In Windows, locate the file at *install_path***dataeng\ini** and set `UnitextLog.enabled=True`. The default *install_path* is **C:\Program Files\Dell\OpenManage**. Restart the **Systems Management Event Manager** service.
- In Red Hat Linux, locate the file at **/usr/lib/dell/openmanage/dataeng/ini** and set `UnitextLog.enabled=True`. Issue the **service dataeng restart** command to restart the systems management event manager service. This will also restart the systems management data manager and SNMP services.

- In Novell NetWare, locate the file at **\system\dell\omanage\dataeng\ini** and set `UnitextLog.enabled=True`. Issue the **omstop** command and then issue the **omstart** command to restart the systems management event manager service. This will also restart the systems management data manager and SNMP services.

The following subsections explain how to open the Windows 2000, Windows Server 2003, NetWare, and Red Hat Linux event viewers.

Viewing Events in Windows 2000 and Windows Server 2003

1. Click the **Start** button, point to **Settings**, and click **Control Panel**.
2. Double-click **Administrative Tools**, and then double-click **Event Viewer**.
3. In the **Event Viewer** window, click the **Tree** tab and then click **System Log**.

   The **System Log** window displays a list of recently logged events.
4. To view the details of an event, double-click one of the event items.

NOTE: You can also view the separate event log file by editing the **dcsys32.log** file in the *install_path***omsa\log** directory. The default *install_path* is **C:\Program Files\Dell\OpenManage**.

Viewing Events in NetWare

1. Using a Windows system, map a drive to the *nwserver***sys** directory, where *nwserver* is the name of your NetWare system.
2. From the mapped drive, locate the **DCSYS32.LOG** file in the **\system\dell\omanage\omsa\log** directory.
3. View the **DCSYS32.LOG** file with Notepad or any other unicode-capable text editor.

Viewing Events in Red Hat Linux

1. Log in as **root**.
2. Use a text editor such as vi or emacs to view the file named **/var/log/messages**.

The following example shows the Linux message log, **/var/log/messages**. The text in boldface type indicates the message text.

NOTE: These messages are typically displayed as one long line. In the following example, the message is displayed using line breaks to help you see the message text more clearly.

```
...
Feb 6 14:20:51 server01 Server Administrator: Instrumentation
Service EventID: 1000
Server Administrator starting
```

Feb 6 14:20:51 server01 Server Administrator: Instrumentation Service EventID: 1001
Server Administrator startup complete

Feb 6 14:21:21 server01 Server Administrator: Instrumentation Service EventID: 1254 **Chassis intrusion detected Sensor location: Main chassis intrusion Chassis location: Main System Chassis Previous state was: OK (Normal) Chassis intrusion state: Open**

Feb 6 14:21:51 server01 Server Administrator: Instrumentation Service EventID: 1252 **Chassis intrusion returned to normal Sensor location: Main chassis intrusion Chassis location: Main System Chassis Previous state was: Critical (Failed) Chassis intrusion state: Closed**

Viewing the Event Information

The event log for each operating system contains some or all of the following information:

- **Date** — The date the event occurred.
- **Time** — The local time the event occurred.
- **Type** — A classification of the event severity: Information, Warning, or Error.
- **User** — The name of the user on whose behalf the event occurred.
- **Computer** — The name of the system where the event occurred.
- **Source** — The software that logged the event.
- **Category** — The classification of the event by the event source.
- **Event ID** — The number identifying the particular event type.
- **Description** — A description of the event. The format and contents of the event description vary, depending on the event type.

Understanding the Event Description

Table 1-1 lists in alphabetical order each line item that may appear in the event description.

Table 1-1. Event Description Reference

Description Line Item	Explanation
`Action performed was: <Action>`	Specifies the action that was performed, for example: `Action performed was: Power cycle`
`Action requested was: <Action>`	Specifies the action that was requested, for example: `Action requested was: Reboot, shutdown OS first`

Table 1-1. Event Description Reference *(continued)*

Description Line Item	Explanation
<Additional power supply status information>	Specifies information pertaining to the event, for example: `Power supply input AC is off, Power supply POK (power OK) signal is not normal, Power supply is turned off`
`Chassis intrusion state: <Intrusion state>`	Specifies the chassis intrusion state (open or closed), for example: `Chassis intrusion state: Open`
`Chassis location: <Name of chassis>`	Specifies name of the chassis that generated the message, for example: `Chassis location: Main System Chassis`
`Configuration error type: <type of configuration error>`	Specifies the type of configuration error that occurred, for example: `Configuration error type: Revision mismatch`
`Current sensor value (in Amps): <Reading>`	Specifies the current sensor value in amps, for example: `Current sensor value (in Amps): 7.853`
`Date and time of action: <Date and time>`	Specifies the date and time the action was performed, for example: `Date and time of action: Sat Jun 12 16:20:33 2004`
`Discrete current state: <State>`	Specifies the state of the current sensor, for example: `Discrete current state: Good`
`Discrete temperature state: <State>`	Specifies the state of the temperature sensor, for example: `Discrete temperature state: Good`
`Discrete voltage state: <State>`	Specifies the state of the voltage sensor, for example: `Discrete voltage state: Good`

`Fan sensor value: <Reading>`	Specifies the fan speed in revolutions per minute (RPM) or On/Off, for example:
	`Fan sensor value (in RPM): 2600`
	`Fan sensor value: Off`

`Log type: <Log type>`	Specifies the type of hardware log, for example: `Log type: ESM`

Table 1-1. Event Description Reference *(continued)*

Description Line Item	Explanation
`Memory device bank location: <Bank name in chassis>`	Specifies the name of the memory bank in the system that generated the message, for example: `Memory device bank location: Bank_1`
`Memory device location: <Device name in chassis>`	Specifies the location of the memory module in the chassis, for example: `Memory device location: DIMM_A`
`Number of devices required for full redundancy: <Number>`	Specifies the number of power supply or cooling devices required to achieve full redundancy, for example: `Number of devices required for full redundancy: 4`

`Possible memory module event cause: <list of causes>`	Specifies a list of possible causes for the memory module event, for example:
	`Possible memory module event cause: Single bit warning error rate exceeded`
	`Single bit error logging disabled`

`Power Supply type: <type of power supply>`	Specifies the type of power supply, for example: `Power Supply type: VRM`
`Previous redundancy state was: <State>`	Specifies the status of the previous redundancy message, for example: `Previous redundancy state was: Lost`
`Previous state was: <State>`	Specifies the previous state of the sensor, for example: `Previous state was: OK (Normal)`
`Processor sensor status: <status>`	Specifies the status of the processor sensor, for example: `Processor sensor status: Configuration error`
`Redundancy unit: <Redundancy location in chassis>`	Specifies the location of the redundant power supply or cooling unit in the chassis, for example: `Redundancy unit: Fan Enclosure`
`Sensor location: <Location in chassis>`	Specifies the location of the sensor in the specified chassis, for example: `Sensor location: CPU1`

Table 1-1. Event Description Reference *(continued)*

Description Line Item	Explanation
`Temperature sensor value: <Reading>`	Specifies the temperature in degrees Celsius, for example: `Temperature sensor value (in degrees Celsius): 30`
`Voltage sensor value (in Volts): <Reading>`	Specifies the voltage sensor value in volts, for example: `Voltage sensor value (in Volts): 1.693`

2

Event Message Reference

The following tables lists in numerical order each event ID and its corresponding description, along with its severity and cause.

NOTE: For corrective actions, see the appropriate documentation.

Miscellaneous Messages

Miscellaneous messages in Table 2-1 indicate that certain alert systems are up and working.

Table 2-1. Miscellaneous Messages

Event ID	Description	Severity	Cause
0000	`Log was cleared`	Information	User cleared the log from Server Administrator.
0001	`Log backup created`	Information	The log was full, copied to backup, and cleared.
1000	`Server Administrator starting`	Information	Server Administrator is beginning to initialize.
1001	`Server Administrator startup complete`	Information	Server Administrator completed its initialization.
1002	`A system BIOS update has been scheduled for the next reboot`	Information	The user has chosen to update the flash basic input/output system (BIOS).
1003	`A previously scheduled system BIOS update has been canceled`	Information	The user decides to cancel the flash BIOS update, or an error occurs during the flash.

Table 2-1. Miscellaneous Messages *(continued)*

Event ID	Description	Severity	Cause
1004	Thermal shutdown protection has been initiated	Error	This message is generated when a system is configured for thermal shutdown due to an error event. If a temperature sensor reading exceeds the error threshold for which the system is configured, the operating system shuts down and the system powers off. This event may also be initiated on certain systems when a fan enclosure is removed from the system for an extended period of time.
1005	SMBIOS data is absent	Warning	The system management BIOS does not contain a valid system management BIOS version 2.2 or higher, or the BIOS is corrupted.
1006	Automatic System Recovery (ASR) action was performed Action performed was: <*Action*> Date and time of action: <*Date and time*>	Error	This message is generated when an automatic system recovery action is performed due to a hung operating system. The action performed and the time of action are provided.
1007	User initiated host system control action Action requested was: <*Action*>	Information	User requested a host system control action to reboot, power off, or power cycle the system. Alternatively the user had indicated protective measures to be initiated in the event of a thermal shutdown.
1008	Systems Management Data Manager Started	Information	Systems Management Data Manager services were started.
1009	Systems Management Data Manager Stopped	Information	Systems Management Data Manager services were stopped.

Temperature Sensor Messages

Temperature sensors listed in Table 2-2 help protect critical components by alerting the systems management console when temperatures become too high inside a chassis. The temperature sensor messages use additional variables: sensor location, chassis location, previous state, and temperature sensor value or state.

Table 2-2. Temperature Sensor Messages

Event ID	Description	Severity	Cause
1050	Temperature sensor has failed Sensor location: *<Location in chassis>* Chassis location: *<Name of chassis>* Previous state was: *<State>* **If sensor type is not discrete:** Temperature sensor value (in degrees Celsius): *<Reading>* **If sensor type is discrete:** Discrete temperature state: *<State>*	Information	A temperature sensor on the backplane board, system board, or the carrier in the specified system failed. The sensor location, chassis location, previous state, and temperature sensor value are provided.
1051	Temperature sensor value unknown Sensor location: *<Location in chassis>* Chassis location: *<Name of chassis>* **If sensor type is not discrete:** Temperature sensor value (in degrees Celsius): *<Reading>* **If sensor type is discrete:** Discrete temperature state: *<State>*	Information	A temperature sensor on the backplane board, system board, or drive carrier in the specified system could not obtain a reading. The sensor location, chassis location, previous state, and a nominal temperature sensor value are provided.

Table 2-2. Temperature Sensor Messages *(continued)*

Event ID	Description	Severity	Cause
1052	Temperature sensor returned to a normal value Sensor location: *<Location in chassis>* Chassis location: *<Name of chassis>* Previous state was: *<State>* **If sensor type is not discrete:** Temperature sensor value (in degrees Celsius): *<Reading>* **If sensor type is discrete:** Discrete temperature state: *<State>*	Information	A temperature sensor on the backplane board, system board, or drive carrier in the specified system returned to a valid range after crossing a failure threshold. The sensor location, chassis location, previous state, and temperature sensor value are provided.
1053	Temperature sensor detected a warning value Sensor location: *<Location in chassis>* Chassis location: *<Name of chassis>* Previous state was: *<State>* **If sensor type is not discrete:** Temperature sensor value (in degrees Celsius): *<Reading>* **If sensor type is discrete:** Discrete temperature state: *<State>*	Warning	A temperature sensor on the backplane board, system board, or drive carrier in the specified system exceeded its warning threshold. The sensor location, chassis location, previous state, and temperature sensor value are provided.

Table 2-2. Temperature Sensor Messages *(continued)*

Event ID	Description	Severity	Cause
1054	Temperature sensor detected a failure value Sensor location: *<Location in chassis>* Chassis location: *<Name of chassis>* Previous state was: *<State>* **If sensor type is not discrete:** Temperature sensor value (in degrees Celsius): *<Reading>* **If sensor type is discrete:** Discrete temperature state: *<State>*	Error	A temperature sensor on the backplane board, system board, or drive carrier in the specified system exceeded its failure threshold. The sensor location, chassis location, previous state, and temperature sensor value are provided.
1055	Temperature sensor detected a non-recoverable value Sensor location: *<Location in chassis>* Chassis location: *<Name of chassis>* Previous state was: *<State>* **If sensor type is not discrete:** Temperature sensor value (in degrees Celsius): *<Reading>* **If sensor type is discrete:** Discrete temperature state: *<State>*	Error	A temperature sensor on the backplane board, system board, or drive carrier in the specified system detected an error from which it cannot recover. The sensor location, chassis location, previous state, and temperature sensor value are provided.

Cooling Device Messages

Cooling device sensors listed in Table 2-3 monitor how well a fan is functioning. Cooling device messages provide status and warning information for fans in a particular chassis.

Table 2-3. Cooling Device Messages

Event ID	Description	Severity	Cause
1100	Fan sensor has failed Sensor location: <*Location in chassis*> Chassis location: <*Name of chassis*> Previous state was: <*State*> Fan sensor value: <*Reading*>	Information	A fan sensor in the specified system is not functioning. The sensor location, chassis location, previous state, and fan sensor value are provided.
1101	Fan sensor value unknown Sensor location: <*Location in chassis*> Chassis location: <*Name of chassis*> Previous state was: <*State*> Fan sensor value: <*Reading*>	Information	A fan sensor in the specified system could not obtain a reading. The sensor location, chassis location, previous state, and a nominal fan sensor value are provided.
1102	Fan sensor returned to a normal value Sensor location: <*Location in chassis*> Chassis location: <*Name of chassis*> Previous state was: <*State*> Fan sensor value: <*Reading*>	Information	A fan sensor reading on the specified system returned to a valid range after crossing a warning threshold. The sensor location, chassis location, previous state, and fan sensor value are provided.
1103	Fan sensor detected a warning value Sensor location: <*Location in chassis*> Chassis location: <*Name of chassis*> Previous state was: <*State*> Fan sensor value: <*Reading*>	Warning	A fan sensor reading in the specified system exceeded a warning threshold. The sensor location, chassis location, previous state, and fan sensor value are provided.

Table 2-3. Cooling Device Messages *(continued)*

Event ID	Description	Severity	Cause
1104	Fan sensor detected a failure value Sensor location: *<Location in chassis>* Chassis location: *<Name of chassis>* Previous state was: *<State>* Fan sensor value: *<Reading>*	Error	A fan sensor in the specified system detected the failure of one or more fans. The sensor location, chassis location, previous state, and fan sensor value are provided.
1105	Fan sensor detected a non-recoverable value Sensor location: *<Location in chassis>* Chassis location: *<Name of chassis>* Previous state was: *<State>* Fan sensor value: *<Reading>*	Error	A fan sensor detected an error from which it cannot recover. The sensor location, chassis location, previous state, and fan sensor value are provided.

Voltage Sensor Messages

Voltage sensors listed in Table 2-4 monitor the number of volts across critical components. Voltage sensor messages provide status and warning information for voltage sensors in a particular chassis.

Table 2-4. Voltage Sensor Messages

Event ID	Description	Severity	Cause
1150	Voltage sensor has failed Sensor location: *<Location in chassis>* Chassis location: *<Name of chassis>* Previous state was: *<State>* **If sensor type is not discrete:** Voltage sensor value (in Volts): *<Reading>* **If sensor type is discrete:** Discrete voltage state: *<State>*	Information	A voltage sensor in the specified system failed. The sensor location, chassis location, previous state, and voltage sensor value are provided.

Table 2-4. Voltage Sensor Messages *(continued)*

Event ID	Description	Severity	Cause
1151	Voltage sensor value unknown Sensor location: *<Location in chassis>* Chassis location: *<Name of chassis>* Previous state was: *<State>* **If sensor type is not discrete:** Voltage sensor value (in Volts): *<Reading>* **If sensor type is discrete:** Discrete voltage state: *<State>*	Information	A voltage sensor in the specified system could not obtain a reading. The sensor location, chassis location, previous state, and a nominal voltage sensor value are provided.
1152	Voltage sensor returned to a normal value Sensor location: *<Location in chassis>* Chassis location: *<Name of chassis>* Previous state was: *<State>* **If sensor type is not discrete:** Voltage sensor value (in Volts): *<Reading>* **If sensor type is discrete:** Discrete voltage state: *<State>*	Information	A voltage sensor in the specified system returned to a valid range after crossing a failure threshold. The sensor location, chassis location, previous state, and voltage sensor value are provided.
1153	Voltage sensor detected a warning value Sensor location: *<Location in chassis>* Chassis location: *<Name of chassis>* Previous state was: *<State>* **If sensor type is not discrete:** Voltage sensor value (in Volts): *<Reading>* **If sensor type is discrete:** Discrete voltage state: *<State>*	Warning	A voltage sensor in the specified system exceeded its warning threshold. The sensor location, chassis location, previous state, and voltage sensor value are provided.

Table 2-4. Voltage Sensor Messages *(continued)*

Event ID	Description	Severity	Cause
1154	Voltage sensor detected a failure value Sensor location: *<Location in chassis>* Chassis location: *<Name of chassis>* Previous state was: *<State>* **If sensor type is not discrete:** Voltage sensor value (in Volts): *<Reading>* **If sensor type is discrete:** Discrete voltage state: *<State>*	Error	A voltage sensor in the specified system exceeded its failure threshold. The sensor location, chassis location, previous state, and voltage sensor value are provided.
1155	Voltage sensor detected a non-recoverable value Sensor location: *<Location in chassis>* Chassis location: *<Name of chassis>* Previous state was: *<State>* **If sensor type is not discrete:** Voltage sensor value (in Volts): *<Reading>* **If sensor type is discrete:** Discrete voltage state: *<State>*	Error	A voltage sensor in the specified system detected an error from which it cannot recover. The sensor location, chassis location, previous state, and voltage sensor value are provided.

Current Sensor Messages

Current sensors listed in Table 2-5 measure the amount of current (in amperes) that is traversing critical components. Current sensor messages provide status and warning information for current sensors in a particular chassis.

Table 2-5. Current Sensor Messages

Event ID	Description	Severity	Cause
1200	Current sensor has failed Sensor location: *<Location in chassis>* Chassis location: *<Name of chassis>* Previous state was: *<State>* **If sensor type is not discrete:** Current sensor value (in Amps): *<Reading>* **If sensor type is discrete:** Discrete current state: *<State>*	Information	A current sensor on the power supply for the specified system failed. The sensor location, chassis location, previous state, and current sensor value are provided.
1201	Current sensor value unknown Sensor location: *<Location in chassis>* Chassis location: *<Name of chassis>* Previous state was: *<State>* **If sensor type is not discrete:** Current sensor value (in Amps): *<Reading>* **If sensor type is discrete:** Discrete current state: *<State>*	Information	A current sensor on the power supply for the specified system could not obtain a reading. The sensor location, chassis location, previous state, and a nominal current sensor value are provided.

Table 2-5. Current Sensor Messages *(continued)*

Event ID	Description	Severity	Cause
1202	Current sensor returned to a normal value Sensor location: *<Location in chassis>* Chassis location: *<Name of chassis>* Previous state was: *<State>* **If sensor type is not discrete:** Current sensor value (in Amps): *<Reading>* **If sensor type is discrete:** Discrete current state: *<State>*	Information	A current sensor on the power supply for the specified system returned to a valid range after crossing a failure threshold. The sensor location, chassis location, previous state, and current sensor value are provided.
1203	Current sensor detected a warning value Sensor location: *<Location in chassis>* Chassis location: *<Name of chassis>* Previous state was: *<State>* **If sensor type is not discrete:** Current sensor value (in Amps): *<Reading>* **If sensor type is discrete:** Discrete current state: *<State>*	Warning	A current sensor on the power supply for the specified system exceeded its warning threshold. The sensor location, chassis location, previous state, and current sensor value are provided.

Table 2-5. Current Sensor Messages *(continued)*

Event ID	Description	Severity	Cause
1204	Current sensor detected a failure value Sensor location: *<Location in chassis>* Chassis location: *<Name of chassis>* Previous state was: *<State>* **If sensor type is not discrete:** Current sensor value (in Amps): *<Reading>* **If sensor type is discrete:** Discrete current state: *<State>*	Error	A current sensor on the power supply for the specified system exceeded its failure threshold. The sensor location, chassis location, previous state, and current sensor value are provided.
1205	Current sensor detected a non-recoverable value Sensor location: *<Location in chassis>* Chassis location: *<Name of chassis>* Previous state was: *<State>* **If sensor type is not discrete:** Current sensor value (in Amps): *<Reading>* **If sensor type is discrete:** Discrete current state: *<State>*	Error	A current sensor in the specified system detected an error from which it cannot recover. The sensor location, chassis location, previous state, and current sensor value are provided.

Chassis Intrusion Messages

Chassis intrusion messages listed in Table 2-6 are a security measure. Chassis intrusion means that someone is opening the cover to a system's chassis. Alerts are sent to prevent unauthorized removal of parts from a chassis.

Table 2-6. Chassis Intrusion Messages

Event ID	Description	Severity	Cause
1250	Chassis intrusion sensor has failed Sensor location: *<Location in chassis>* Chassis location: *<Name of chassis>* Previous state was: *<State>* Chassis intrusion state: *<Intrusion state>*	Information	A chassis intrusion sensor in the specified system failed. The sensor location, chassis location, previous state, and chassis intrusion state are provided.
1251	Chassis intrusion sensor value unknown Sensor location: *<Location in chassis>* Chassis location: *<Name of chassis>* Previous state was: *<State>* Chassis intrusion state: *<Intrusion state>*	Information	A chassis intrusion sensor in the specified system could not obtain a reading. The sensor location, chassis location, previous state, and chassis intrusion state are provided.
1252	Chassis intrusion returned to normal Sensor location: *<Location in chassis>* Chassis location: *<Name of chassis>* Previous state was: *<State>* Chassis intrusion state: *<Intrusion state>*	Information	A chassis intrusion sensor in the specified system detected that a cover was opened while the system was operating but has since been replaced. The sensor location, chassis location, previous state, and chassis intrusion state are provided.
1253	Chassis intrusion in progress Sensor location: *<Location in chassis>* Chassis location: *<Name of chassis>* Previous state was: *<State>* Chassis intrusion state: *<Intrusion state>*	Warning	A chassis intrusion sensor in the specified system detected that a system cover is currently being opened and the system is operating. The sensor location, chassis location, previous state, and chassis intrusion state are provided.

Table 2-6. Chassis Intrusion Messages *(continued)*

Event ID	Description	Severity	Cause
1254	Chassis intrusion detected Sensor location: *<Location in chassis>* Chassis location: *<Name of chassis>* Previous state was: *<State>* Chassis intrusion state: *<Intrusion state>*	Error	A chassis intrusion sensor in the specified system detected that the system cover was opened while the system was operating. The sensor location, chassis location, previous state, and chassis intrusion state are provided.
1255	Chassis intrusion sensor detected a non-recoverable value Sensor location: *<Location in chassis>* Chassis location: *<Name of chassis>* Previous state was: *<State>* Chassis intrusion state: *<Intrusion state>*	Error	A chassis intrusion sensor in the specified system detected an error from which it cannot recover. The sensor location, chassis location, previous state, and chassis intrusion state are provided.

Redundancy Unit Messages

Redundancy means that a system chassis has more than one of certain critical components. Fans and power supplies, for example, are so important for preventing damage or disruption of a computer system that a chassis may have "extra" fans or power supplies installed. Redundancy allows a second or *n*th fan to keep the chassis components at a safe temperature when the primary fan has failed. Redundancy is normal when the intended number of critical components are operating. Redundancy is degraded when a component fails but others are still operating. Redundancy is lost when the number of components functioning falls below the redundancy threshold. Table 2-7 lists the redundancy unit messages.

The number of devices required for full redundancy is provided as part of the message when applicable for the redundancy unit and the platform. For details on redundancy computation, see the respective platform documentation.

Table 2-7. Redundancy Unit Messages

Event ID	Description	Severity	Cause
1300	Redundancy sensor has failed Redundancy unit: *<Redundancy location in chassis>* Chassis location: *<Name of chassis>* Previous redundancy state was: *<State>*	Information	A redundancy sensor in the specified system failed. The redundancy unit location, chassis location, previous redundancy state, and the number of devices required for full redundancy are provided.
1301	Redundancy sensor value unknown Redundancy unit: *<Redundancy location in chassis>* Chassis location: *<Name of chassis>* Previous redundancy state was: *<State>*	Information	A redundancy sensor in the specified system could not obtain a reading. The redundancy unit location, chassis location, previous redundancy state, and the number of devices required for full redundancy are provided.
1302	Redundancy not applicable Redundancy unit: *<Redundancy location in chassis>* Chassis location: *<Name of chassis>* Previous redundancy state was: *<State>*	Information	A redundancy sensor in the specified system detected that a unit was not redundant. The redundancy location, chassis location, previous redundancy state, and the number of devices required for full redundancy are provided.
1303	Redundancy is offline Redundancy unit: *<Redundancy location in chassis>* Chassis location: *<Name of chassis>* Previous redundancy state was: *<State>*	Information	A redundancy sensor in the specified system detected that a redundant unit is offline. The redundancy unit location, chassis location, previous redundancy state, and the number of devices required for full redundancy are provided.

Table 2-7. Redundancy Unit Messages *(continued)*

Event ID	Description	Severity	Cause
1304	Redundancy regained Redundancy unit: *<Redundancy location in chassis>* Chassis location: *<Name of chassis>* Previous redundancy state was: *<State>*	Information	A redundancy sensor in the specified system detected that a "lost" redundancy device has been reconnected or replaced; full redundancy is in effect. The redundancy unit location, chassis location, previous redundancy state, and the number of devices required for full redundancy are provided.
1305	Redundancy degraded Redundancy unit: *<Redundancy location in chassis>* Chassis location: *<Name of chassis>* Previous redundancy state was: *<State>*	Warning	A redundancy sensor in the specified system detected that one of the components of the redundancy unit has failed but the unit is still redundant. The redundancy unit location, chassis location, previous redundancy state, and the number of devices required for full redundancy are provided.
1306	Redundancy lost Redundancy unit: *<Redundancy location in chassis>* Chassis location: *<Name of chassis>* Previous redundancy state was: *<State>*	Warning or Error (depending on the number of units that are functional)	A redundancy sensor in the specified system detected that one of the components in the redundant unit has been disconnected, has failed, or is not present. The redundancy unit location, chassis location, previous redundancy state, and the number of devices required for full redundancy are provided.

Power Supply Messages

Power supply sensors monitor how well a power supply is functioning. Power supply messages listed in Table 2-8 provide status and warning information for power supplies present in a particular chassis.

Table 2-8. Power Supply Messages

Event ID	Description	Severity	Cause
1350	Power supply sensor has failed Sensor location: *<Location in chassis>* Chassis location: *<Name of chassis>* Previous state was: *<State>* Power Supply type: *<type of power supply>* *<Additional power supply status information>* **If in configuration error state:** Configuration error type: *<type of configuration error>*	Information	A power supply sensor in the specified system failed. The sensor location, chassis location, previous state, and additional power supply status information are provided.
1351	Power supply sensor value unknown Sensor location: *<Location in chassis>* Chassis location: *<Name of chassis>* Previous state was: *<State>* Power Supply type: *<type of power supply>* *<Additional power supply status information>* **If in configuration error state:** Configuration error type: *<type of configuration error>*	Information	A power supply sensor in the specified system could not obtain a reading. The sensor location, chassis location, previous state, and additional power supply status information are provided.

Table 2-8. Power Supply Messages *(continued)*

Event ID	Description	Severity	Cause
1352	Power supply returned to normal Sensor location: *<Location in chassis>* Chassis location: *<Name of chassis>* Previous state was: *<State>* Power Supply type: *<type of power supply>* *<Additional power supply status information>* **If in configuration error state:** Configuration error type: *<type of configuration error>*	Information	A power supply has been reconnected or replaced. The sensor location, chassis location, previous state, and additional power supply status information are provided.
1353	Power supply detected a warning Sensor location: *<Location in chassis>* Chassis location: *<Name of chassis>* Previous state was: *<State>* Power Supply type: *<type of power supply>* *<Additional power supply status information>* **If in configuration error state:** Configuration error type: *<type of configuration error>*	Warning	A power supply sensor reading in the specified system exceeded a user-definable warning threshold. The sensor location, chassis location, previous state, and additional power supply status information are provided.

Table 2-8. Power Supply Messages *(continued)*

Event ID	Description	Severity	Cause
1354	Power supply detected a failure Sensor location: *<Location in chassis>* Chassis location: *<Name of chassis>* Previous state was: *<State>* Power Supply type: *<type of power supply>* *<Additional power supply status information>* **If in configuration error state:** Configuration error type: *<type of configuration error>*	Error	A power supply has been disconnected or has failed. The sensor location, chassis location, previous state, and additional power supply status information are provided.
1355	Power supply sensor detected a non-recoverable value Sensor location: *<Location in chassis>* Chassis location: *<Name of chassis>* Previous state was: *<State>* Power Supply type: *<type of power supply>* *<Additional power supply status information>* **If in configuration error state:** Configuration error type: *<type of configuration error>*	Error	A power supply sensor in the specified system detected an error from which it cannot recover. The sensor location, chassis location, previous state, and additional power supply status information are provided.

Memory Device Messages

Memory device messages listed in Table 2-9 provide status and warning information for memory modules present in a particular system. Memory devices determine health status by monitoring the ECC memory correction rate and the type of memory events that have occurred.

NOTE: A critical status does not always indicate a system failure or loss of data. In some instances, the system has exceeded the ECC correction rate. Although the system continues to function, you should perform system maintenance as described in Table 2-9.

NOTE: In Table 2-9, *<status>* can be either `critical` or `non-critical`.

Table 2-9. Memory Device Messages

Event ID	Description	Severity	Cause

1403	`Memory device status is <status>`
	`Memory device location: <location in chassis>`
	`Possible memory module event cause: <list of causes>`
		Warning	A memory device correction rate exceeded an acceptable value. The memory device status and location are provided.

1404	`Memory device status is <status>`
	`Memory device location: <location in chassis>`
	`Possible memory module event cause: <list of causes>`
		Error	A memory device correction rate exceeded an acceptable value, a memory spare bank was activated, or a multibit ECC error occurred. The system continues to function normally (except for a multibit error). Replace the memory module identified in the message during the system's next scheduled maintenance. Clear the memory error on multibit ECC error. The memory device status and location are provided.

Fan Enclosure Messages

Some systems are equipped with a protective enclosure for fans. Fan enclosure messages listed in Table 2-10 monitor whether foreign objects are present in an enclosure and how long a fan enclosure is missing from a chassis.

Table 2-10. Fan Enclosure Messages

Event ID	Description	Severity	Cause
1450	Fan enclosure sensor has failed Sensor location: <*Location in chassis*> Chassis location: <*Name of chassis*>	Information	The fan enclosure sensor in the specified system failed. The sensor location and chassis location are provided.
1451	Fan enclosure sensor value unknown Sensor location: <*Location in chassis*> Chassis location: <*Name of chassis*>	Information	The fan enclosure sensor in the specified system could not obtain a reading. The sensor location and chassis location are provided.
1452	Fan enclosure inserted into system Sensor location: <*Location in chassis*> Chassis location: <*Name of chassis*>	Information	A fan enclosure has been inserted into the specified system. The sensor location and chassis location are provided.
1453	Fan enclosure removed from system Sensor location: <*Location in chassis*> Chassis location: <*Name of chassis*>	Warning	A fan enclosure has been removed from the specified system. The sensor location and chassis location are provided.
1454	Fan enclosure removed from system for an extended amount of time Sensor location: <*Location in chassis*> Chassis location: <*Name of chassis*>	Error	A fan enclosure has been removed from the specified system for a user-definable length of time. The sensor location and chassis location are provided.

Table 2-10. Fan Enclosure Messages *(continued)*

Event ID	Description	Severity	Cause
1455	Fan enclosure sensor detected a non-recoverable value Sensor location: *<Location in chassis>* Chassis location: *<Name of chassis>*	Error	A fan enclosure sensor in the specified system detected an error from which it cannot recover. The sensor location and chassis location are provided.

AC Power Cord Messages

AC power cord messages listed in Table 2-11 provide status and warning information for power cords that are part of an AC power switch, if your system supports AC switching.

Table 2-11. AC Power Cord Messages

Event ID	Description	Severity	Cause
1500	AC power cord sensor has failed Sensor location: *<Location in chassis>* Chassis location: *<Name of chassis>*	Information	An AC power cord sensor in the specified system failed. The AC power cord status cannot be monitored. The sensor location and chassis location information are provided.
1501	AC power cord is not being monitored Sensor location: *<Location in chassis>* Chassis location: *<Name of chassis>*	Information	The AC power cord status is not being monitored. This occurs when a system's expected AC power configuration is set to **nonredundant**. The sensor location and chassis location information are provided.
1502	AC power has been restored Sensor location: *<Location in chassis>* Chassis location: *<Name of chassis>*	Information	An AC power cord that did not have AC power has had the power restored. The sensor location and chassis location information are provided.

Table 2-11. AC Power Cord Messages *(continued)*

Event ID	Description	Severity	Cause
1503	AC power has been lost Sensor location: *<Location in chassis>* Chassis location: *<Name of chassis>*	Warning	An AC power cord has lost its power, but there is sufficient redundancy to classify this as a warning. The sensor location and chassis location information are provided.
1504	AC power has been lost Sensor location: *<Location in chassis>* Chassis location: *<Name of chassis>*	Error	An AC power cord has lost its power, and lack of redundancy requires this to be classified as an error. The sensor location and chassis location information are provided.
1505	AC power has been lost Sensor location: *<Location in chassis>* Chassis location: *<Name of chassis>*	Error	An AC power cord sensor in the specified system failed. The AC power cord status cannot be monitored. The sensor location and chassis location information are provided.

Hardware Log Sensor Messages

Hardware logs provide hardware status messages to systems management software. On certain systems, the hardware log is implemented as a circular queue. When the log becomes full, the oldest status messages are overwritten when new status messages are logged. On some systems, the log is not circular. On these systems, when the log becomes full, subsequent hardware status messages are lost. Hardware log sensor messages listed in Table 2-12 provide status and warning information about the noncircular logs that may fill up, resulting in lost status messages.

Table 2-12. Hardware Log Sensor Messages

Event ID	Description	Severity	Cause
1550	Log monitoring has been disabled Log type: *<Log type>*	Information	A hardware log sensor in the specified system is disabled. The log type information is provided.

Table 2-12. Hardware Log Sensor Messages *(continued)*

Event ID	Description	Severity	Cause
1551	`Log status is unknown` `Log type: <Log type>`	Information	A hardware log sensor in the specified system could not obtain a reading. The log type information is provided.
1552	`Log size is no longer near or at capacity` `Log type: <Log type>`	Information	The hardware log on the specified system is no longer near or at its capacity, usually as the result of clearing the log. The log type information is provided.
1553	`Log size is near or at capacity` `Log type: <Log type>`	Warning	The size of a hardware log on the specified system is near or at the capacity of the hardware log. The log type information is provided.
1554	`Log size is full` `Log type: <Log type>`	Error	The size of a hardware log on the specified system is full. The log type information is provided.
1555	`Log sensor has failed` `Log type: <Log type>`	Error	A hardware log sensor in the specified system failed. The hardware log status cannot be monitored. The log type information is provided.

Processor Sensor Messages

Processor sensors monitor how well a processor is functioning. Processor messages listed in Table 2-13 provide status and warning information for processors in a particular chassis.

Table 2-13. Processor Sensor Messages

Event ID	Description	Severity	Cause
1600	Processor sensor has failed Sensor Location: *<Location in chassis>* Chassis Location: *<Name of chassis>* Previous state was: *<State>* Processor sensor status: *<status>*	Information	A processor sensor in the specified system is not functioning. The sensor location, chassis location, previous state and processor sensor status are provided.
1601	Processor sensor value unknown Sensor Location: *<Location in chassis>* Chassis Location: *<Name of chassis>* Previous state was: *<State>* Processor sensor status: *<status>*	Information	A processor sensor in the specified system could not obtain a reading. The sensor location, chassis location, previous state and processor sensor status are provided.
1602	Processor sensor returned to a normal value Sensor Location: *<Location in chassis>* Chassis Location: *<Name of chassis>* Previous state was: *<State>* Processor sensor status: *<status>*	Information	A processor sensor in the specified system transitioned back to a normal state. The sensor location, chassis location, previous state and processor sensor status are provided.
1603	Processor sensor detected a warning value Sensor Location: *<Location in chassis>* Chassis Location: *<Name of chassis>* Previous state was: *<State>* Processor sensor status: *<status>*	Warning	A processor sensor in the specified system is in a throttled state. The sensor location, chassis location, previous state and processor sensor status are provided.

Table 2-13. Processor Sensor Messages *(continued)*

Event ID	Description	Severity	Cause
1604	Processor sensor detected a failure value Sensor Location: *<Location in chassis>* Chassis Location: *<Name of chassis>* Previous state was: *<State>* Processor sensor status: *<status>*	Error	A processor sensor in the specified system is disabled, has a configuration error, or experienced a thermal trip. The sensor location, chassis location, previous state and processor sensor status are provided.
1605	Processor sensor detected a non-recoverable value Sensor Location: *<Location in chassis>* Chassis Location: *<Name of chassis>* Previous state was: *<State>* Processor sensor status: *<status>*	Error	A processor sensor in the specified system has failed. The sensor location, chassis location, previous state and processor sensor status are provided.

3

Storage Management Message Reference

Storage Management's alert or event management features let you monitor the health of storage resources such as controllers, channels, array disks, and virtual disks.

Alert Monitoring and Logging

The Disk Management Service performs alert monitoring and logging. By default, the Disk Management Service starts when the managed system starts up. If you stop the Disk Management Service, then alert monitoring and logging stops. Alert monitoring does the following:

- Updates the status of the storage object that generated the alert.
- Propagates the storage object's status to all the related higher objects in the storage hierarchy. For example, the status of a lower-level object will be propagated up to the status displayed on the Health tab for the top-level storage object.
- Logs an alert into the Alert log and Windows application log.
- Sends an SNMP trap if the operating system's SNMP service is installed and enabled.

NOTE: Storage Management does not log alerts regarding the data I/O path. These alerts are logged by the respective RAID drivers in the system alert log.

Viewing Alerts

Storage Management generates alerts that are added to the Windows application alert log and to the Server Administrator Alert log. To view these alerts in Server Administrator:

1. Select the **System** object in the tree view.
2. Select the **Logs** tab.
3. Select the **Alert** subtab.

NOTE: You can also view these alerts in the Microsoft Windows Event Viewer. Every alert consists of the following:

- **Severity** — Shows the severity of alert.
- **Date and Time** — Date and time when Storage Management logged the alert.
- **Description** — A brief description of the alert. To expand or collapse the alert description, click the **Description** column heading.

Alert Severity Levels

Each alert message in the Storage Management alert log has a severity level. The severity level is displayed in the **Severity** field of the alert message. The severity level indicates the nature of the alert.

The alert severity levels are as follows:

Table 3-1. Storage Management Alert Severity

Alert Severity	Component Status
OK/Normal	No action is required. The alert is provided for informational purposes and does not indicate an error condition. For example, the alert may indicate the normal start or stop of an operation.
Warning/Non-critical	A component requires attention. This alert indicates a potential problem, but does not necessarily mean that the system has currently lost data or is nonfunctional. For example, a Warning/Non-critical alert may indicate that a component (such as a temperature probe in an enclosure) has crossed a warning threshold.
Critical/Failure/Error	A component has either failed or failure is imminent. This alert indicates a serious problem such as data loss or a loss of function. For example, a Critical/Failure/Error alert may indicate that an array disk has failed.

SNMP Support for Storage Management Alerts

By default, Storage Management installs SNMP trap forwarding support. For this support to function, you should have SNMP installed on the managed system prior to installing Storage Management.

NOTE: For more information on installation requirements and SNMP, see the Server Administrator documentation.

SNMP Trap Forwarding

The alerts displayed in the Storage Management alert log are forwarded to the Windows application alert log. If you have SNMP installed on the managed system (and the SNMP service is running), the Storage Management alerts in the Windows application alert log will be forwarded as SNMP traps. In order for these traps to be viewable, however, a target system or application must be configured to receive these traps. SNMP traps that are generated by Storage Management can be viewed in any standard SNMP-compatible enterprise management console.

The Windows SNMP service must be configured to forward the SNMP traps to the target system or application. When forwarding to an application, the application should also be configured to receive the SNMP traps. The IT Assistant application is already configured to receive the SNMP traps generated by Storage Management.

See your Windows operating system documentation for information on configuring the operating system to forward SNMP traps. This information may be located under such topics as “setting up SNMP” or “SNMP traps.” When configuring SNMP for Windows, be sure that the SNMP traps are forwarded to the correct server. For information on configuring an application to receive SNMP traps, see the documentation for that application.

SNMP Trap Definitions

The Storage Management management information base (MIB) defines the SNMP traps that Storage Management generates. These traps correspond to the alerts documented in the “Alert Descriptions and Corrective Actions" section. The MIB is located in a subdirectory of the Storage Management installation directory. The subdirectory location for the MIB is ..\sm\mibs\dcstorag.mib.

NOTE: Storage Management supports trap forwarding on both 32-bit and 64-bit operating systems.

SNMP Trap Variables

The Storage Management SNMP traps use a set of variables that are included with every trap. These variables are the following:

- messageIDEvent
- descriptionEvent
- locationEvent
- objectNameEvent
- objectOIDEvent
- objectNexusEvent
- currentStatusEvent
- previousStatusEvent

Viewing SNMP Traps

SNMP traps that are generated by Storage Management can be viewed in any standard SNMP-compatible enterprise management console. These traps are defined in the Storage Management management information base (MIB). These traps correspond to the alerts documented in the “Alert Descriptions and Corrective Actions” section. For more information on the MIB and its structure, as well as a change history of the SNMP traps, see the *Dell OpenManage Server Administrator SNMP Reference Guide*. For more information on configuring SNMP, see "SNMP Support for Storage Management Alerts."

Viewing Traps with HP OpenView Network Node Manager

To view trap alerts with strings inserted with HP OpenView Network Node Manager (NNM), perform the following steps:

1. Load the Storage Management MIB (arymgr.mib) into the HP OpenView NNM. The arymgr.mib file is located in the Management Information Base (MIB) directory of your Storage Management installation directory.
2. Select **OK** when prompted to load a **TRAP-TYPE/NOTIFICATION-TYPE** macro. The system loads all of the trap definitions into HP OpenView.

For more information on loading MIBs into HP OpenView, see the HP OpenView documentation.

Alert Descriptions and Corrective Actions

The following sections describe alerts generated by the RAID or SCSI controllers supported by Storage Management. The alerts are displayed in the Server Administrator Alert subtab or through Windows Event Viewer. These alerts can also be forwarded as SNMP traps to other applications.

SNMP traps are generated for the alerts listed in the following sections. These traps are included in the Storage Management management information base (MIB). The SNMP traps for these alerts use all of the SNMP trap variables. For more information on SNMP support and the MIB, see "SNMP Support for Storage Management Alerts."

To locate an alert, scroll through the following table to find the alert number displayed on the Server Administrator Alert tab or search this HTML file for the alert message text or number. See "Alert Severity Levels" for more information on severity levels.

For more information regarding alert descriptions and the appropriate corrective actions, see the online help.

Table 3-2. Storage Management Messages

Event ID	Description	Severity	Cause and Action	SNMP Trap Numbers	Array Manager Event Number
2048	Device failed	Critical / Failure / Error	Cause: A physical disk in the array failed. The failed disk may have been identified by the controller or channel. Performing a consistency check can also identify a failed disk. Action: Replace the failed array disk. You can identify which disk has failed by locating the disk that has a red "X" for its status. Perform a rescan after replacing the disk.	754, 804, 854, 904, 954, 1004, 1054, 1104, 1154, 1204	500

Table 3-2. Storage Management Messages

Event ID	Description	Severity	Cause and Action	SNMP Trap Numbers	Array Manager Event Number
2049	Array disk removed	Warning / Non-critical	Cause: A physical disk has been removed from the array. A user may have also executed the "Prepare to Remove" task. This alert can also be caused by loose or defective cables or by problems with the enclosure. Action: If a physical disk was removed from the array, either replace the disk or restore the original disk. You can identify which disk has been removed by locating the disk that has a red "X" for its status. Perform a rescan after replacing or restoring the disk. If a disk has not been removed from the array, then check for problems with the cables. See the online help for more information on checking the cables. Make sure that the enclosure is powered on. If the problem persists, check the enclosure documentation for further diagnostic information.	903	501
2050	Array disk offline	Warning / Non-critical	Cause: A physical disk in the array is offline. A disk can be made offline during a Prepare to Remove operation or because a user manually put the disk offline. Action: Perform a rescan. You can also select the offline disk and perform a Make Online operation.	903	502
2052	Array disk inserted	Ok / Normal	Cause: This alert is provided for informational purposes. Action: None.	901	504
2053	Virtual disk created	Ok / Normal	Cause: This alert is provided for informational purposes. Action: None.	1201	505

Table 3-2. Storage Management Messages

Event ID	Description	Severity	Cause and Action	SNMP Trap Numbers	Array Manager Event Number
2054	Virtual disk deleted	Warning / Non-critical	Cause: A virtual disk has been deleted. "Performing a Reset Configuration" may detect that a virtual disk has been deleted and generate this alert. Action: None.	1203	506
2055	Virtual disk configuration changed	Ok / Normal	Cause: This alert is provided for informational purposes. Action: None.	1201	507
2056	Virtual disk failed	Critical / Failure / Error	Cause: One or more physical disks included in the virtual disk have failed. If the virtual disk is non-redundant (does not use mirrored or parity data), then the failure of a single physical disk can cause the virtual disk to fail. If the virtual disk is redundant, then more physical disks have failed than can be rebuilt using mirrored or parity information. Action: Create a new virtual disk and restore from a backup.	1204	508

Table 3-2. Storage Management Messages

Event ID	Description	Severity	Cause and Action	SNMP Trap Numbers	Array Manager Event Number
2057	Virtual disk degraded	Warning / Non-critical	Cause 1: This alert message occurs when a physical disk included in a redundant virtual disk fails. Because the virtual disk is redundant (uses mirrored or parity information) and only one physical disk has failed, the virtual disk can be rebuilt. Action 1: Configure a hot spare for the virtual disk if one is not already configured. Rebuild the virtual disk. When using an SS 2/SC, 3/SC, 2/DC, 3/DCL, 3/DC, 3/QC, 4/SC, 4/DC, 4e/DC, 4/Di, or CERC ATA100/4ch controller, rebuild the virtual disk by first configuring a hot spare for the disk, and then initiating a write operation to the disk. The write operation will initiate a rebuild of the disk. Cause 2: A physical disk in the array has been removed. Action 2: If a physical disk was removed from the array, either replace the disk or restore the original disk. You can identify which disk has been removed by locating the disk that has a red "X" for its status. Perform a rescan after replacing the disk.	1203	509
2058	Virtual disk check consistency started	Ok / Normal	Cause: This alert is provided for informational purposes. Action: None.	1201	520
2059	Virtual disk format started	Ok / Normal	Cause: This alert is provided for informational purposes. Action: None.	1201	521

Table 3-2. Storage Management Messages

Event ID	Description	Severity	Cause and Action	SNMP Trap Numbers	Array Manager Event Number
2061	Virtual disk initialization started	Ok / Normal	Cause: This alert is provided for informational purposes. Action: None.	1201	523
2063	Virtual disk reconfiguration started	Ok / Normal	Cause: This alert is provided for informational purposes. Action: None.	1201	525
2064	Virtual disk rebuild started	Ok / Normal	Cause: This alert is provided for informational purposes. Action: None.	1201	526
2065	Array disk rebuild started	Ok / Normal	Cause: This alert is provided for informational purposes. Action: None.	901	527
2067	Virtual disk check consistency cancelled	Ok / Normal	Cause: The check consistency operation cancelled because a physical disk in the array has failed or because a user cancelled the check consistency operation. Action: If the physical disk failed, then replace the physical disk. You can identify which disk failed by locating the disk that has a red "X" for its status. Perform a rescan after replacing the disk. When performing a consistency check, be aware that the consistency check can take a long time. The time it takes depends on the size of the physical disk or the virtual disk.	1201	529

Table 3-2. Storage Management Messages

Event ID	Description	Severity	Cause and Action	SNMP Trap Numbers	Array Manager Event Number
2070	Virtual disk initialization cancelled	Ok / Normal	Cause: The virtual disk initialization cancelled because a physical disk included in the virtual disk has failed or because a user cancelled the virtual disk initialization. Action: If a physical disk failed, then replace the physical disk. You can identify which disk has failed by locating the disk that has a red "X" for its status. Perform a rescan after replacing the disk. Restart the format array disk operation. Restart the virtual disk initialization.	1201	532
2076	Virtual disk check consistency failed	Critical / Failure / Error	Cause: An array disk included in the virtual disk failed or there is an error in the parity information. A failed array disk can cause errors in parity information. Action: Replace the failed array disk. You can identify which disk has failed by locating the disk that has a red "X" for its status. Rebuild the array disk. When finished, restart the check consistency operation.	1204	538
2079	Virtual disk initialization failed	Critical / Failure / Error	Cause: An array disk included in the virtual disk has failed or a user has cancelled the initialization. Action: If an array disk has failed, then replace the array disk.	1204	541
2080	Array disk initialize failed	Critical / Failure / Error	Cause: The array disk has failed or is corrupt. Action: Replace the failed or corrupt disk. You can identify a disk that has failed by locating the disk that has a red "X" for its status. Restart the initialization.	904	542

Table 3-2. Storage Management Messages

Event ID	Description	Severity	Cause and Action	SNMP Trap Numbers	Array Manager Event Number
2081	Virtual disk reconfiguration failed	Critical / Failure / Error	Cause: An array disk included in the virtual disk has failed or is corrupt. A user may also have cancelled the reconfiguration. Action: Replace the failed or corrupt disk. You can identify a disk that has failed by locating the disk that has a red "X" for its status. If the array disk is part of a redundant array, then rebuild the array disk. When finished, restart the reconfiguration.	1204	543
2082	Virtual disk rebuild failed	Critical / Failure / Error	Cause: An array disk included in the virtual disk has failed or is corrupt. A user may also have cancelled the rebuild. Action: Replace the failed or corrupt disk. You can identify a disk that has failed by locating the disk that has a red "X" for its status. Restart the virtual disk rebuild.	1204	544
2083	Array disk rebuild failed	Critical / Failure / Error	Cause: An array disk included in the virtual disk has failed or is corrupt. A user may also have cancelled the rebuild. Action: Replace the failed or corrupt disk. You can identify a disk that has failed by locating the disk that has a red "X" for its status. Rebuild the virtual disk rebuild.	904	545
2085	Virtual disk check consistency completed	Ok / Normal	Cause: This alert is provided for informational purposes. Action: None.	1201	547
2086	Virtual disk format completed	Ok / Normal	Cause: This alert is provided for informational purposes. Action: None.	1201	548

Table 3-2. Storage Management Messages

Event ID	Description	Severity	Cause and Action	SNMP Trap Numbers	Array Manager Event Number
2088	Virtual disk initialization completed	Ok / Normal	Cause: This alert is provided for informational purposes. Action: None.	1201	550
2089	Array disk initialize completed	Ok / Normal	Cause: This alert is provided for informational purposes. Action: None.	901	551
2090	Virtual disk reconfiguration completed	Ok / Normal	Cause: This alert is provided for informational purposes. Action: None.	1201	552
2091	Virtual disk rebuild completed	Ok / Normal	Cause: This alert is provided for informational purposes. Action: None.	1201	553
2092	Array disk rebuild completed	Ok / Normal	Cause: This alert is provided for informational purposes. Action: None.	901	554
2094	Predictive Failure reported. If this disk is part of a redundant virtual disk, select the 'Offline' option and then replace the disk. Then configure a hot spare and it will start the rebuild automatically. If this disk is a hot spare, select the 'Prepare to Remove' option and then replace the disk. If this disk is part of a non-redundant disk, you should back up your data immediately. If the disk fails, you will not be able to recover the data.	Warning / Non-critical	Cause: The array disk is predicted to fail. Many array disks contain Self Monitoring Analysis and Reporting Technology (S.M.A.R.T.). When enabled, SMART monitors the health of the disk based on indications such as the number of write operations that have been performed on the disk. Action: Replace the array disk. Even though the disk may not have failed yet, it is strongly recommended that you replace the disk. Review the message text for additional information.	903	570

Table 3-2. Storage Management Messages

Event ID	Description	Severity	Cause and Action	SNMP Trap Numbers	Array Manager Event Number
2095	SCSI sense data. If this disk is part of a redundant virtual disk, select the 'Offline' option and then replace the disk. Then configure a hot spare and it will start the rebuild automatically. If this disk is a hot spare, select the 'Prepare to Remove' option and then replace the disk. If this disk is part of a non-redundant disk, you should back up your data immediately. If the disk fails, you will not be able to recover the data.	Warning / Non-critical	Cause: An array disk has failed, is corrupt, or is otherwise experiencing a problem. Action: Replace the array disk. Even though the disk may not have failed yet, it is strongly recommended that you replace the disk. Review the message text for additional information.	903	571
2098	Global hot spare assigned	Ok / Normal	Cause: A user has assigned an array disk as a global hot spare. This alert is provided for informational purposes. Action: None.	901	574
2099	Global hot spare unassigned	Ok / Normal	Cause: A user has unassigned an array disk as a global hot spare. This alert is provided for informational purposes. Action: None.	901	575

Table 3-2. Storage Management Messages

Event ID	Description	Severity	Cause and Action	SNMP Trap Numbers	Array Manager Event Number
2100	Temperature exceeded the maximum warning threshold	Warning / Non-critical	Cause: The array disk enclosure is too hot. A variety of factors can cause the excessive temperature. For example, a fan may have failed, the thermostat may be set too high, or the room temperature may be too hot. Action: Check for factors that may cause overheating. For example, verify that the enclosure fan is working. You should also check the thermostat settings and examine whether the enclosure is located near a heat source. Make sure the enclosure has enough ventilation and that the room temperature is not too hot. See the enclosure documentation for more diagnostic information.	1053	591
2101	Temperature dropped below the minimum warning threshold	Warning / Non-critical	Cause: The array disk enclosure is too cool. Action: Check whether the thermostat setting is too low and whether the room temperature is too cool.	1053	592

Table 3-2. Storage Management Messages

Event ID	Description	Severity	Cause and Action	SNMP Trap Numbers	Array Manager Event Number
2102	Temperature exceeded the maximum failure threshold	Critical / Failure / Error	Cause: The array disk enclosure is too hot. A variety of factors can cause the excessive temperature. For example, a fan may have failed, the thermostat may be set too high, or the room temperature may be too hot. Action: Check for factors that may cause overheating. For example, verify that the enclosure fan is working. You should also check the thermostat settings and examine whether the enclosure is located near a heat source. Make sure the enclosure has enough ventilation and that the room temperature is not too hot. See the enclosure documentation for more diagnostic information.	1054	593
2103	Temperature dropped below the minimum failure threshold	Critical / Failure / Error	Cause: The array disk enclosure is too cool. Action: Check whether the thermostat setting is too low and whether the room temperature is too cool.	1054	594
2104	Controller battery is reconditioning	Ok / Normal	Cause: This alert is provided for informational purposes. Action: None.	1151	581
2105	Controller battery recondition is completed	Ok / Normal	Cause: This alert is provided for informational purposes. Action: None.	1151	582

Table 3-2. Storage Management Messages

Event ID	Description	Severity	Cause and Action	SNMP Trap Numbers	Array Manager Event Number
2106	Smart FPT exceeded	Warning / Non-critical	Cause: A disk on the specified controller has received a SMART alert (predictive failure) indicating that the disk is likely to fail in the near future. Action: Replace the disk that has received the SMART alert. If the array disk is a member of a non-redundant virtual disk, then back up the data before replacing the disk. Removing an array disk that is included in a non-redundant virtual disk will cause the virtual disk to fail and may cause data loss.	903	585
2107	Smart configuration change	Critical / Failure / Error	Cause: A disk has received a SMART alert (predictive failure) after a configuration change. The disk is likely to fail in the near future. Action: Replace the disk that has received the SMART alert. If the array disk is a member of a non-redundant virtual disk, then back up the data before replacing the disk. Removing an array disk that is included in a non-redundant virtual disk will cause the virtual disk to fail and may cause data loss	904	586

Table 3-2. Storage Management Messages

Event ID	Description	Severity	Cause and Action	SNMP Trap Numbers	Array Manager Event Number
2108	Smart warning	Warning / Non-critical	Cause: A disk has received a SMART alert (predictive failure). The disk is likely to fail in the near future. Action: Replace the disk that has received the SMART alert. If the array disk is a member of a non-redundant virtual disk, then back up the data before replacing the disk. Removing an array disk that is included in a non-redundant virtual disk will cause the virtual disk to fail and may cause data loss.	903	587

Table 3-2. Storage Management Messages

Event ID	Description	Severity	Cause and Action	SNMP Trap Numbers	Array Manager Event Number
2109	Smart warning temperature	Warning / Non-critical	Cause: A disk has reached an unacceptable temperature and received a SMART alert (predictive failure). The disk is likely to fail in the near future. First Action: Determine why the array disk has reached an unacceptable temperature. A variety of factors can cause the excessive temperature. For example, a fan may have failed, the thermostat may be set too high, or the room temperature may be too hot or cold. Verify that the fans in the server or enclosure are working. If the array disk is in an enclosure, you should check the thermostat settings and examine whether the enclosure is located near a heat source. Make sure the enclosure has enough ventilation and that the room temperature is not too hot. See the enclosure documentation for more diagnostic information. Second Action: If you cannot identify why the disk has reached an unacceptable temperature, then replace the disk. If the array disk is a member of a non-redundant virtual disk, then back up the data before replacing the disk. Removing an array disk that is included in a non-redundant virtual disk will cause the virtual disk to fail and may cause data loss.	903	588

Table 3-2. Storage Management Messages

Event ID	Description	Severity	Cause and Action	SNMP Trap Numbers	Array Manager Event Number
2110	Smart warning degraded	Warning / Non-critical	Cause: A disk is degraded and has received a SMART alert (predictive failure). The disk is likely to fail in the near future. Action: Replace the disk that has received the SMART alert. If the array disk is a member of a non-redundant virtual disk, then back up the data before replacing the disk. Removing an array disk that is included in a non-redundant virtual disk will cause the virtual disk to fail and may cause data loss.	903	589
2111	Failure prediction threshold exceeded due to test - No action needed	Warning / Non-critical	Cause: A disk has received a SMART alert (predictive failure) due to test conditions. Action: None.	903	590
2112	Enclosure was shut down	Critical / Failure / Error	Cause: The array disk enclosure is either hotter or cooler than the maximum or minimum allowable temperature range. Action: Check for factors that may cause overheating or excessive cooling. For example, verify that the enclosure fan is working. You should also check the thermostat settings and examine whether the enclosure is located near a heat source. Make sure the enclosure has enough ventilation and that the room temperature is not too hot or too cold. See the enclosure documentation for more diagnostic information.	854	602

Table 3-2. Storage Management Messages

Event ID	Description	Severity	Cause and Action	SNMP Trap Numbers	Array Manager Event Number
2113	Server was shut down	Critical / Failure / Error	Cause: The array disk enclosure is either hotter or cooler than the maximum or minimum allowable temperature range. Action: Check for factors that may cause overheating or excessive cooling. For example, verify that the enclosure fan is working. You should also check the thermostat settings and examine whether the enclosure is located near a heat source. Make sure the enclosure has enough ventilation and that the room temperature is not too hot or too cold. See the enclosure documentation for more diagnostic information.	854	603
2114	A consistency check on a virtual disk has been paused (suspended)	Ok / Normal	Cause: The check consistency operation on a virtual disk was paused by a user. Action: To resume the check consistency operation, right-click the virtual disk in the Storage Management tree view and select Resume Check Consistency.	1201	604
2115	A consistency check on a virtual disk has been resumed	Ok / Normal	Cause: The check consistency operation on a virtual disk has resumed processing after being paused by a user. Action: This alert is provided for informational purposes.	1201	605

Table 3-2. Storage Management Messages

Event ID	Description	Severity	Cause and Action	SNMP Trap Numbers	Array Manager Event Number
2116	A virtual disk and its mirror have been split	Ok / Normal	Cause: A user has caused a mirrored virtual disk to be split. When a virtual disk is mirrored, its data is copied to another virtual disk in order to maintain redundancy. After being split, both virtual disks retain a copy of the data, although because the mirror is no longer intact, updates to the data are no longer copied to the mirror. Action: This alert is provided for informational purposes.	1201	606
2117	A mirrored virtual disk has been unmirrored	Ok / Normal	Cause: A user has caused a mirrored virtual disk to be unmirrored. When a virtual disk is mirrored, its data is copied to another virtual disk in order to maintain redundancy. After being unmirrored, the disk formerly used as the mirror returns to being an array disk and becomes available for inclusion in another virtual disk. Action: This alert is provided for informational purposes.	1201	607
2118	Change write policy	Ok / Normal	Cause: A user has changed the write policy for a virtual disk. Action: This alert is provided for informational purposes.	1201	601

Table 3-2. Storage Management Messages

Event ID	Description	Severity	Cause and Action	SNMP Trap Numbers	Array Manager Event Number
2120	Enclosure firmware mismatch	Warning / Non-critical	Cause: The firmware on the EMM modules is not the same version. It is required that both modules have the same version of the firmware. This alert may be caused when a user attempts to insert an EMM module that has a different firmware version than an existing module. Action: Download the same version of the firmware to both EMM modules.	853	672
2121	Device returned to normal	Ok / Normal	Cause: A device that was previously in an error state has returned to a normal state. For example, if an enclosure became too hot and subsequently cooled down, then you may receive this alert. Action: This alert is provided for informational purposes.	752, 802, 852, 902, 952, 1002, 1052, 1102, 1152, 1202	None

Table 3-2. Storage Management Messages

Event ID	Description	Severity	Cause and Action	SNMP Trap Numbers	Array Manager Event Number
2122	Redundancy degraded	Warning / Non-critical	Cause: One or more of the enclosure components has failed. For example, a fan or power supply may have failed. Although the enclosure is currently operational, the failure of additional components could cause the enclosure to fail. Action: Identify and replace the failed component. To identify the failed component, select the enclosure in the tree view and click the Health subtab. Any failed component will be identified with a red X on the enclosure's Health subtab. Alternatively, you can select the Storage object and click the Health subtab. The controller status displayed on the Health subtab indicates whether a controller has a failed or degraded component. See the enclosure documentation for information on replacing enclosure components and for other diagnostic information.	1305	None

Table 3-2. Storage Management Messages

Event ID	Description	Severity	Cause and Action	SNMP Trap Numbers	Array Manager Event Number
2123	Redundancy lost	Warning / Non-critical	Action: Identify and replace the failed components. To identify the failed component, select the Storage object and click the Health subtab. The controller status displayed on the Health subtab indicates whether a controller has a failed or degraded component. Click the controller that displays a Warning or Failed status. This action displays the controller Health subtab which displays the status of the individual controller components. Continue clicking the components with a Warning or Health status until you identify the failed component. See the online help for more information. See the enclosure documentation for information on replacing enclosure components and for other diagnostic information.	1306	None
2124	Redundancy normal	Ok / Normal	Cause: Data redundancy has been restored to a virtual disk or an enclosure that previously suffered a loss of redundancy. Action: This alert is provided for informational purposes.	1304	None

Table 3-2. Storage Management Messages

Event ID	Description	Severity	Cause and Action	SNMP Trap Numbers	Array Manager Event Number
2126	SCSI sense sector reassign	Warning / Non-critical	Cause: A sector of the disk is corrupted and data cannot be maintained on this portion of the disk. Action: If the disk is part of a non-redundant virtual disk, then replace the disk. Any data residing on the corrupt portion of the disk may be lost and you may need to restore from backup. If the disk is part of a redundant virtual disk, then any data residing on the corrupt portion of the disk will be reallocated elsewhere in the virtual disk.	903	None
2127	Background initialization started	Ok / Normal	Cause: Background initialization of a virtual disk has started. This alert is provided for informational purposes. Action: None.	1201	683
2128	Background initialization cancelled	Ok / Normal	Cause: Background initialization of a virtual disk has been cancelled. A user or the firmware may have stopped background initialization. Action: None.	1201	684
2129	Background initialization failed	Critical / Failure / Error	Cause: Background initialization of a virtual disk has failed. Action: None.	1204	685
2130	Background initialization completed	Ok / Normal	Cause: Background initialization of a virtual disk has completed. This alert is provided for informational purposes. Action: None.	1201	686

Table 3-2. Storage Management Messages

Event ID	Description	Severity	Cause and Action	SNMP Trap Numbers	Array Manager Event Number
2131	Firmware version mismatch	Warning / Non-critical	Cause: The firmware on the controller is not a supported version. Action: Install a supported version of the firmware. If you do not have a supported version of the firmware available, it can be downloaded from the Dell support site at **support.dell.com**. If you do not have a supported version of the firmware available, check with your support provider for information on how to obtain the most current firmware.	753	None
2132	Driver version mismatch	Warning / Non-critical	Cause: The controller driver is not a supported version. Action: Install a supported version of the driver. If you do not have a supported driver version available, it can be downloaded from the Dell support site at **support.dell.com**. If you do not have a supported version of the driver available, check with your support provider for information on how to obtain the most current driver.	753	None
2135	Array Manager is installed on the system	Warning / Non-critical	Cause: Storage Management has been installed on a system that has an Array Manager installation. Action: Installing Storage Management and Array Manager on the same system is not a supported configuration. Uninstall either Storage Management or Array Manager.	103	None

Table 3-2. Storage Management Messages

Event ID	Description	Severity	Cause and Action	SNMP Trap Numbers	Array Manager Event Number
2137	Communication timeout	Warning / Non-critical	Cause: The controller is unable to communicate with an enclosure. There are several reasons why communcation may be lost. For example, there may be a bad or loose cable. An unusual amount of I/O may also interrupt communication with the enclosure. In addition, communication loss may be caused by software, hardware, or firmware problems, bad or failed power supplies, and enclosure shutdown. Action: Check for problems with the cables. See the online help for more information on checking the cables. You should also check to see if the enclosure has degraded or failed components. To do so, select the enclosure object in the tree view and click the Health subtab. The Health subtab displays the status of the enclosure components. Verify that the controller has supported driver and firmware versions installed and that the enclosure management modules (EMMs) are each running the same version of supported firmware.	853	688, 610, 611
2138	Enclosure alarm enabled	Ok / Normal	Cause: A user had enabled the enclosure alarm. This alert is provided for informational purposes. Action: None.	851	676
2139	Enclosure alarm disabled	Ok / Normal	Cause: A user has disabled the enclosure alarm. Action: None.	851	677

Table 3-2. Storage Management Messages

Event ID	Description	Severity	Cause and Action	SNMP Trap Numbers	Array Manager Event Number
2140	Dead disk segments restored	Ok / Normal	Cause: Disk space that was formerly "dead" or inaccessible to a redundant virtual disk has been restored. This alert is provided for informational purposes. Action: None.	1201	None
2141	Array disk dead segments recovered	Ok / Normal	Cause: Portions of the array disk that were formerly inaccessible have been recovered. This alert is provided for informational purposes. Action: None.	901	None
2142	Controller rebuild rate has changed	Ok / Normal	Cause: A user has changed the controller rebuild rate. This alert is provided for informational purposes. Action: None.	751	680
2143	Controller alarm enabled	Ok / Normal	Cause: A user has enabled the controller alarm. This alert is provided for informational purposes. Action: None.	751	678
2144	Controller alarm disabled	Ok / Normal	Cause: A user has disabled the controller alarm. This alert is provided for informational purposes. Action: None.	751	679
2145	Controller battery low	Warning / Non-critical	Cause: The controller battery charge is low. Action: Recondition the battery. See the online help for more information	1153	580

Table 3-2. Storage Management Messages

Event ID	Description	Severity	Cause and Action	SNMP Trap Numbers	Array Manager Event Number
2146	Bad block replacement error	Warning / Non-critical	Cause: A portion of an array disk is damaged. **See the** *Dell OpenManage Storage Management User's Guide* **for more information.** Action: See the online help for more information.	753	691
2147	Bad block sense error	Warning / Non-critical	Cause: A portion of an array disk is damaged. See the online help for more information. Action: See the online help for more information.	753	691
2148	Bad block medium error	Warning / Non-critical	Cause: A portion of an array disk is damaged. See the online help for more information. Action: See the online help for more information.	753	691
2149	Bad block extended sense error	Warning / Non-critical	Cause: A portion of an array disk is damaged. See the online help for more information. Action: See the online help for more information.	753	691
2150	Bad block extended medium error	Warning / Non-critical	Cause: A portion of an array disk is damaged. See the online help for more information. Action: See the online help for more information.	753	691
2151	Asset tag changed	Ok / Normal	Cause: A user has changed the enclosure asset tag. This alert is provided for informational purposes. Action: None.	851	None

Table 3-2. Storage Management Messages

Event ID	Description	Severity	Cause and Action	SNMP Trap Numbers	Array Manager Event Number
2152	Asset name changed	Ok / Normal	Cause: A user has changed the enclosure asset name. This alert is provided for informational purposes. Action: None.	851	None
2153	Service tag changed	Warning / Non-critical	Cause: An enclosure service tag was changed. In most circumstances, this service tag should only be changed by Dell support or your service provider. Action: Ensure that the tag was changed under authorized circumstances.	851	None
2154	Maximum temperature probe warning threshold value changed	Ok / Normal	Cause: A user has changed the value for the maximum temperature probe warning threshold. This alert is provided for informational purposes. Action: None	1051	None
2155	Minimum temperature probe warning threshold value changed	Ok / Normal	Cause: A user has changed the value for the minimum temperature probe warning threshold. This alert is provided for informational purposes. Action: None.	1051	None
2156	Controller alarm has been tested	Ok / Normal	Cause: The controller alarm test has run successfully. This alert is provided for informational purposes. Action: None.	751	None
2157	Controller configuration has been reset	Ok / Normal	Cause: A user has reset the controller configuration. See the online help for more information. This alert is provided for informational purposes. Action: None.	751	None

Table 3-2. Storage Management Messages

Event ID	Description	Severity	Cause and Action	SNMP Trap Numbers	Array Manager Event Number
2158	Array disk online	Ok / Normal	Cause: An offline array disk has been made online. This alert is provided for informational purposes. Action: None.	901	None
2159	Virtual disk renamed	Ok / Normal	Cause: A user has renamed a virtual disk. This alert is provided for informational purposes. Action: None.	1201	608
2160	Dedicated hotspare assigned	Ok / Normal	Cause: A user has assigned an array disk as a dedicated hot spare to a virtual disk. See the online help for more information. This alert is provided for informational purposes. Action: None.	901	574
2161	Dedicated hotspare unassigned	Ok / Normal	Cause: A user has unassigned an array disk as a dedicated hot spare to a virtual disk. See the online help for more information. This alert is provided for informational purposes. Action: None	901	575
2162	Communication regained	Ok / Normal	Cause: Communication with an enclosure has been restored. This alert is provided for informational purposes. Action: None.	851	None
2163	Rebuild completed with errors	Ok / Normal	Cause: See the online help for more information. Action: See the online help for more information.	904	690

Table 3-2. Storage Management Messages

Event ID	Description	Severity	Cause and Action	SNMP Trap Numbers	Array Manager Event Number
2164	See readme.txt for a list of validated controller driver versions	Ok / Normal	Cause: Storage Management is unable to determine whether the system has the minimum required versions of the RAID controller drivers. Action: This alert is generated for informational purposes. See the Readme file for driver and firmware requirements. In particular, if Storage Management experiences performance problems, you should verify that you have the minimum supported versions of the drivers and firmware installed.	751	None
2165	The RAID controller firmware and driver validation was not performed. The configuration file cannot be opened.	Warning / Non-critical	Cause: Storage Management is unable to determine whether the system has the minimum required versions of the RAID controller firmware and drivers. This situation may occur for a variety of reasons. For example, the installation directory path to the configuration file may not be correct. The configuration file may also have been removed or renamed. Action: Reinstall Storage Management	753	None
2166	The RAID controller firmware and driver validation was not performed. The configuration file is out of date or corrupted.	Warning / Non-critical	Cause: Storage Management is unable to determine whether the system has the minimum required versions of the RAID controller firmware and drivers. This situation has occurred because a configuration file is unreadable or missing data. The configuration file may be corrupted. Action: Reinstall Storage Management	753	None

Index

Numerics

0000, 15
0001, 15
1000, 15
1001, 15
1002, 15
1003, 15
1004, 16
1005, 16
1006, 16
1007, 16
1008, 16
1009, 16
1050, 17
1051, 17
1052, 18
1053, 18
1054, 19
1055, 19
1100, 20
1101, 20
1102, 20
1103, 20
1104, 21
1105, 21
1150, 21
1151, 22
1152, 22
1153, 22
1154, 23
1155, 23
1200, 24
1201, 24
1202, 25
1203, 25
1204, 26
1205, 26
1250, 27
1251, 27
1252, 27
1253, 27
1254, 28
1255, 28
1300, 29
1301, 29
1302, 29
1303, 29
1304, 30
1305, 30
1306, 30
1350, 31
1351, 31
1352, 32
1353, 32
1354, 33
1355, 33
1403, 34
1404, 34
1450, 35
1451, 35
1452, 35
1453, 35
1454, 35
1455, 36
1500, 36
1501, 36
1502, 36
1503, 37
1504, 37
1505, 37
1550, 37
1551, 38
1552, 38
1553, 38
1554, 38
1555, 38
1600, 39
1601, 39

1602, 39
1603, 39
1604, 40
1605, 40
2048, 44
2049, 45
2050, 45
2052, 45
2053, 45
2054, 46
2055, 46
2056, 46
2057, 47
2058, 47
2059, 47
2061, 48
2063, 48
2064, 48
2065, 48
2067, 48
2070, 49
2076, 49
2079, 49
2080, 49
2081, 50
2082, 50
2083, 50
2085, 50
2086, 50
2088, 51
2089, 51
2090, 51
2091, 51
2092, 51
2094, 51
2095, 52
2098, 52
2099, 52
2100, 53
2101, 53
2102, 54
2103, 54
2104, 54
2105, 54
2106, 55
2107, 55
2108, 56
2109, 57
2110, 58
2111, 58
2112, 58
2113, 59
2114, 59
2115, 59
2116, 60
2117, 60
2118, 60
2120, 61
2121, 61
2122, 62
2123, 63
2124, 63
2126, 64
2127, 64
2128, 64
2129, 64
2130, 64
2131, 65
2132, 65
2135, 65
2137, 66
2138, 66
2139, 66
2140, 67
2141, 67
2142, 67
2143, 67
2144, 67
2145, 67
2146, 68
2147, 68
2148, 68
2149, 68
2150, 68
2151, 68
2152, 69
2153, 69
2154, 69
2155, 69
2156, 69

2157, 69
2158, 70
2159, 70
2160, 70
2161, 70
2162, 70
2163, 70
2164, 71
2165, 71
2166, 71

A

A consistency check on a virtual disk has been paused (suspended), 59
A consistency check on a virtual disk has been resumed, 59
A mirrored virtual disk has been unmirrored, 60
A previously scheduled system BIOS update has been canceled, 15
A system BIOS update has been scheduled for the next reboot, 15
A virtual disk and its mirror have been split, 60
AC power cord is not being monitored, 36
AC power cord messages, 36
AC power cord sensor, 8
AC power cord sensor has failed, 36
AC power has been lost, 37
AC power has been restored, 36
Array disk dead segments recovered, 67
Array disk initialize completed, 51
Array disk initialize failed, 49
Array disk inserted, 45
Array disk offline, 45
Array disk online, 70
Array disk rebuild completed, 51
Array disk rebuild failed, 50
Array disk rebuild started, 48
Array disk removed, 45
Array Manager is installed on the system, 65
Asset name changed, 69
Asset tag changed, 68
Automatic System Recovery (ASR) action was performed, 16

B

Background initialization cancelled, 64
Background initialization completed, 64
Background initialization failed, 64
Background initialization started, 64
Bad block extended medium error, 68
Bad block extended sense error, 68
Bad block medium error, 68
Bad block replacement error, 68
Bad block sense error, 68

C

Change write policy, 60
Chassis intrusion detected, 28
Chassis intrusion in progress, 27
chassis intrusion messages, 26
Chassis intrusion returned to normal, 27
chassis intrusion sensor, 8
Chassis intrusion sensor detected a non-recoverable value, 28
Chassis intrusion sensor has failed, 27
Chassis intrusion sensor value unknown, 27
Communication regained, 70
Communication timeout, 66
Controller alarm disabled, 67

Controller alarm enabled, 67
Controller alarm has been tested, 69
Controller battery is reconditioning, 54
Controller battery low, 67
Controller battery recondition is completed, 54
Controller configuartion has been reset, 69
Controller rebuild rate has changed, 67
cooling device messages, 19
current sensor, 8
Current sensor detected a failure value, 26
Current sensor detected a non-recoverable value, 26
Current sensor detected a warning value, 25
Current sensor has failed, 24
current sensor messages, 23
Current sensor returned to a normal value, 25
Current sensor value unknown, 24

D

Dead disk segments restored, 67
Dedicated hotspare assigned, 70
Dedicated hotspare unassigned, 70
Device failed, 44
Device returned to normal, 61
Driver version mismatch, 65

E

Enclosure alarm disabled, 66
Enclosure alarm enabled, 66
Enclosure firmware mismatch, 61
Enclosure was shut down, 58
event description reference, 11
Event Log
viewing entries, 41

F

Failure prediction threshold exceeded due to test, 58
Fan enclosure inserted into system, 35
fan enclosure messages, 34
Fan enclosure removed from system, 35
Fan enclosure removed from system for an extended amount of time, 35
fan enclosure sensor, 8
Fan enclosure sensor detected a non-recoverable value, 36
Fan enclosure sensor has failed, 35
Fan enclosure sensor value unknown, 35
fan sensor, 8
Fan sensor detected a failure value, 21
Fan sensor detected a non-recoverable value, 21
Fan sensor detected a warning value, 20
Fan sensor has failed, 20
Fan sensor returned to a normal value, 20
Fan sensor value unknown, 20
Firmware version mismatch, 65

G

Global hot spare assigned, 52
Global hot spare unassigned, 52

H

hardware log sensor, 8

L

Log backup created, 15
Log monitoring has been disabled, 37

Log size is near or at capacity, 38
Log size returned to a normal level, 38
Log status is unknown, 38
Log was cleared, 15

M

Maximum temperature probe warning threshold value changed, 69
Memory device ECC Correctable error count crossed a warning threshold, 34
Memory device ECC Correctable error count sensor crossed a failure threshold, 34
memory device messages, 33
Memory device monitoring has been disabled, 34
memory prefailure sensor, 8
messages
AC power cord, 36
chassis intrusion, 26
cooling device, 19
current sensor, 23
fan enclosure, 34
memory device, 33
miscellaneous, 15
power supply, 30
processor sensor, 38
redundancy unit, 28
storage management, 44
temperature sensor, 17
voltage sensor, 21
Minimum temperature probe warning threshold value changed, 69

P

Power supply detected a failure, 33
Power supply detected a warning, 32
power supply messages, 30
Power supply returned to normal, 32
power supply sensor, 8
Power supply sensor detected a non-recoverable value, 33
Power supply sensor has failed, 31
Power supply sensor value unknown, 31
Predictive Failure reported, 51
processor sensor, 8
Processor sensor detected a failure value, 40
Processor sensor detected a non-recoverable value, 40
Processor sensor detected a warning value, 39
Processor sensor has failed, 39
Processor sensor returned to a normal state, 39
Processor sensor value unknown, 39

R

Rebuild completed with errors, 70
Redundancy degraded, 30, 62
Redundancy is offline, 29
Redundancy lost, 30, 63
Redundancy normal, 63
Redundancy not applicable, 29
Redundancy regained, 30
Redundancy sensor has failed, 29
Redundancy sensor value unknown, 29
redundancy unit messages, 28
redundancy unit sensor, 8

S

SCSI sense data, 52
SCSI sense sector reassign, 64
See readme.txt for a list of validated controller driver versions, 71
sensor
AC power cord, 8
chassis intrusion, 8
current, 8

fan, 8
fan enclosure, 8
hardware log, 8
memory prefailure, 8
power supply, 8
processor, 8, 38
redundancy unit, 8
temperature, 8
voltage, 8

Server Administrator starting, 15

Server Administrator startup complete, 15

Server was shut down, 59

Service tag changed, 69

Smart configuration change, 55

Smart FPT exceeded, 55

Smart warning, 56

Smart warning degraded, 58

Smart warning temperature, 57

SMBIOS data is absent, 16

SNMP support, configuring, 42

SNMP traps, 43

system management data manager started, 16

system management data manager stopped, 16

T

Temperature dropped below the minimum failure threshold, 54

Temperature dropped below the minimum warning threshold, 53

Temperature exceeded the maximum failure threshold, 54

Temperature exceeded the maximum warning threshold, 53

temperature sensor, 8

Temperature sensor detected a failure value, 19

Temperature sensor detected a non-recoverable value, 19

Temperature sensor detected a warning value, 18

Temperature sensor has failed, 17

temperature sensor messages, 17

Temperature sensor returned to a normal value, 18

Temperature sensor value unknown, 17

The RAID controller firmware and driver validation was not performed., 71

Thermal shutdown protection has been initiated, 16

U

understanding
event description, 11

User initiated host system reset, 16

V

Viewing
SNMP traps, 43

viewing
event information, 11
event messages, 9
events in NetWare, 10
events in Red Hat Linux, 10
events in Windows 2000, 10

Virtual disk check consistency cancelled, 48

Virtual disk check consistency completed, 50

Virtual disk check consistency failed, 49

Virtual disk check consistency started, 47

Virtual disk configuration changed, 46

Virtual disk created, 45

Virtual disk degraded, 47

Virtual disk deleted, 46

Virtual disk failed, 46

Virtual disk format completed, 50

Virtual disk format started, 47

Virtual disk initialization cancelled, 49

Virtual disk initialization completed, 51

Virtual disk initialization failed, 49

Virtual disk initialization started, 48

Virtual disk rebuild completed, 51

Virtual disk rebuild failed, 50

Virtual disk rebuild started, 48

Virtual disk reconfiguration completed, 51

Virtual disk reconfiguration failed, 50

Virtual disk reconfiguration started, 48

Virtual disk renamed, 70

voltage sensor, 8

Voltage sensor detected a failure value, 23

Voltage sensor detected a non-recoverable value, 23

Voltage sensor detected a warning value, 22

Voltage sensor has failed, 21

voltage sensor messages, 21

Voltage sensor returned to a normal value, 22

Voltage sensor value unknown, 22