

HP Insight Management Agents User Guide



July 2004 (Third Edition)
Part Number 308447-003
Product Version 7.10

© Copyright 2003, 2004 Hewlett-Packard Development Company, L.P.

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Acrobat and Adobe are trademarks of Adobe Systems Incorporated. Java is a U.S. trademark of Sun Microsystems, Inc. Microsoft, Windows, and Windows NT are U.S. registered trademarks of Microsoft Corporation. UNIX is a registered trademark of The Open Group. Linux is a U.S. registered trademark of Linus Torvalds.

HP Insight Management Agents User Guide

July 2004 (Third Edition)
Part Number 308447-003
Product Version 7.10

Contents

About This Guide

Audience Assumptions	xi
Where to Go for Additional Help	xii
Telephone Numbers	xii

Chapter 1

HP Insight Management Agents for Servers

Accessing HP Insight Management Agents from a Browser for Microsoft Operating Systems	1-1
Accessing HP Insight Management Agents from a Browser for Other Operating Systems	1-1
Browser Requirements	1-2
Updating Netscape Communicator for Tru64 UNIX Workstations	1-4
Security	1-4
Management HTTP Server First-Time Initialization	1-7
Introduction	1-7
What is Management HTTP Server?	1-8
Overview	1-8
Logging In	1-9
System Management Homepage	1-11
Header Frame	1-11
Data Frame	1-12
How to Replicate Passwords and Configuration Data Across Multiple Devices	1-13
Navigating In Management HTTP Server	1-13
Tabs	1-13
Home	1-14
Settings	1-17
Settings Section	1-17
Management HTTP Server Section	1-17
Change Password	1-18
Credits	1-19
Options	1-20
Tasks	1-26
Tools	1-27
Logs	1-27
Subsystem Status Information	1-29
Title Frame	1-29
Summary Page	1-30
Send Test Trap to Trap Destination	1-30
Device Status	1-30
Navigation Frame	1-31
Data Frame	1-31

Group Configuration	1-32
SNMP Configuration	1-35
Options	1-38
Display Inline Help Icons	1-38

Chapter 2

Foundation Agent Information

Management Host Agent	2-1
Running the Host Agent	2-1
Threshold Agent	2-3
Running the Threshold Agent on a SCO UnixWare 7 System	2-3
System	2-4
Software Version Information	2-4
Cluster Information	2-4
Cluster Nodes	2-4
Cluster Resources Groups	2-5
Cluster Networks	2-5
Cluster Interconnect	2-6
Cluster Software	2-6
Storage	2-7
File System Space Used	2-7
Disk Space Usage Bar Graph	2-7
Disk Space Usage Thresholds	2-7
Resetting and Saving Thresholds	2-7
Creating Thresholds	2-8
Modifying Thresholds	2-8
NIC Subsystem	2-9
ServerNet PCI Adapter	2-9
Operating System Information	2-9
Disk Monitoring	2-10
Threshold Alarms	2-11
Performance Status Icons	2-11
Supported OS Performance Properties	2-11
Logical Disks	2-11
Memory	2-12
Network	2-14
Physical Disks	2-15
Processes	2-15
Processors	2-16
Server	2-17
Information Availability to a WMI Consumer	2-21

Chapter 3

Server Agent Information

System	3-1
System Board	3-1
CPUs	3-2
Memory	3-2
Memory Subsystem	3-3
Advanced Memory Protection	3-3
Memory Board Details	3-5
ROM Microcode Patches	3-6
General I/O Devices	3-7
Diskette Drives	3-7
Serial and Parallel Ports	3-8
Universal Serial Bus Port	3-8
Expansion Boards	3-8
Security	3-9
Enclosure Information	3-9
Software Version Information	3-10
System Information	3-10
Asset Control Information	3-11
System Resources	3-12
Storage	3-12
Mass Storage Subsystem	3-12
Processor Utilization	3-12
Auto Recovery	3-13
Environment	3-15
Power Supply	3-16
Power Converter	3-17
Remote Communications	3-18
Tasks	3-20
Logs	3-20
Critical Error Log	3-20
Correctable Errors	3-23
Power On Messages	3-23
Integrated Management Log	3-23
Management Processor	3-25

Chapter 4

Storage Agent Information

Mass Storage Subsystem.....	4-1
IDE Controllers	4-1
IDE Controller Information	4-1
IDE ATAPI Devices.....	4-2
IDE ATA Disk Drives	4-3
IDE ATA Logical Drives	4-5
SCSI Controllers.....	4-6
Drive Array Controllers.....	4-26
Identify Drives.....	4-35
External Array Storage Systems.....	4-56
Identify Drives.....	4-69
Identify Drive	4-82
Associated Source Logical Drive	4-83
Associated Snapshot Resource Volume	4-83
Snapshot Resource Volumes	4-83
Fibre Channel Switch Information.....	4-85
RAID Array Storage Systems	4-86
External Storage Connections.....	4-87
Fiber Channel Connections	4-87
Array Controller Connections	4-88
Fibre Channel Tape Controllers	4-89
Tape Controller Information.....	4-89
Tape Storage System Information	4-90
Tape Drive Information.....	4-92
Tape Drive Error Counts	4-94
Tape Drive Maintenance	4-95

Chapter 5

NIC Agent Information

NIC Subsystem	5-1
Virtual NIC.....	5-1
Single NIC.....	5-1
Teams of NICs.....	5-2
Logical Adapter Information	5-2
NIC Controller Information	5-3
NIC Interface Information	5-5
Receive Statistics.....	5-6
Transmit Statistics	5-6
Ethernet Statistics.....	5-6
Receive Errors	5-7
Transmit Errors.....	5-8
Token Ring Statistics	5-10

Chapter 6**Subsystem Specific to a NetWare Operating System**

Operating System Overview.....	6-1
Summary Page.....	6-1
File System Page.....	6-3
File System.....	6-3
File Volumes.....	6-3
Open Files.....	6-4
User Information Page.....	6-4
Connection Page.....	6-5
Loaded NLMs Page.....	6-6
Server Parameter Page.....	6-6
SET Exceptions.....	6-7
Physical Partition Page.....	6-8
Adapter Information Page.....	6-8

Chapter 7**CR3500 RAID Array SCSI Controller**

Mass Storage RAID Array.....	7-1
RAID Array Status.....	7-1
Drive Information.....	7-2
Physical Drives.....	7-2
Logical Drives.....	7-2
Spare Drives.....	7-2
Mass Storage Physical.....	7-3
Physical Drive Status.....	7-3
Drive Information.....	7-3
RAID Arrays.....	7-3
Mass Storage Controller.....	7-4
Clustered RAID Controller.....	7-4
Mass Storage Summary.....	7-5
CR3500 Shared Storage System.....	7-5
Environment Monitoring Unit.....	7-5
External Expansion Cabinet.....	7-6

Chapter 8**Agent Information Specific to SCO UnixWare 7**

Foundation Agents.....	8-1
SCO UnixWare 7 SNMP Daemon.....	8-1
HP Foundation SMUX Manager.....	8-1
Foundation Agents SMUX Manager Configuration File.....	8-3
Foundation Agents SMUX Manager Configuration File Syntax.....	8-3
Foundation SMUX Manager Configuration File Parameters.....	8-4
Trap Alarm E-mail Configuration File.....	8-5
Foundation Data Collection Agents.....	8-5
HP Foundation Data Registry.....	8-5
Web Agent.....	8-6

Server Agents.....	8-7
HP Server SMUX Manager.....	8-7
Server Agents SMUX Manager Configuration File.....	8-8
Server Agents SMUX Manager Configuration File Syntax.....	8-9
Server SMUX Manager Configuration File Parameters.....	8-10
Storage Agents.....	8-15
Storage SMUX Manager.....	8-16
Trap Alarm E-mail Configuration File.....	8-17
Storage Data Collection Agents.....	8-17
HP Storage Data Registry.....	8-17
Configuring Data Collection Agents.....	8-18
NIC Agents.....	8-22
HP NIC SMUX Manager.....	8-22
Trap Alarm E-mail Configuration File.....	8-23
NIC Data Collection Agent.....	8-24

Appendix A
Troubleshooting

Insight Management Agents for Servers Issues.....	A-1
Inability to Perform Remote Reboot on a Server from the Management Console.....	A-1
Global Unique Identifiers are the Same for All Devices When Using Disk Imaging Software on Servers.....	A-1
When Changing the Access Level, a Valid Account and Password for the System Management Homepage are Accepted, but the Web Page Indicates that a Different Account Is Logged In.....	A-2
When Attempting to Browse to Web-Enabled System Management Software On Port 2381, the Following Message Appears.....	A-3
Known Browser Issues.....	A-4
SNMP Community String Issues.....	A-5
Management Agents for Servers for Windows Issues.....	A-6
Installation Issues.....	A-6
Insight Manager Issues.....	A-7
Other Problems.....	A-11
Management Agents for Servers for NetWare Issues.....	A-12
Inability to Change any Values on the Managed System or to Mark Errors as Corrected.....	A-12
No SNMP Traps or Alarms Received for NetWare.....	A-12
System Restart to Disk-Based Utilities Fails for NetWare.....	A-12
Inability to View Web Pages on the NetWare Server.....	A-12
Management Agents for Servers for SCO UnixWare 7 Issues.....	A-13
HP Systems Insight Manager Issues.....	A-13
SNMP-Based Management Program Issues.....	A-17
Values Cannot Be Changed on the Managed Server.....	A-17
Thresholds Cannot Be Set on HP MIB Items.....	A-17
No SNMP Traps/Alarms are Received.....	A-18
No User-Defined SNMP Traps are Received.....	A-18
Management Agent Issues.....	A-19
Web-Enabled Management Agents for Servers.....	A-20
Error Messages.....	A-20
Problem Using Disk Imaging Software.....	A-27
Global Unique Identifiers Are the Same for All Devices When Using Disk Imaging Software on Servers.....	A-27

Glossary

Index

About This Guide

This user guide contains information about using HP Insight Management Agents for servers, and provides detailed information about accessing and understanding the information provided by the Management Agents and each of the integrated components.

Audience Assumptions

This guide is for the person who installs, administers, and maintains servers. HP assumes you are qualified in installing, using, and administering server software and are familiar with basic administration tasks.

Where to Go for Additional Help

In addition to this guide, the following information sources are available:

- *HP Insight Management Agents Installation Guide*
- HP Insight Manager software

Telephone Numbers

For the name of the nearest HP authorized reseller:

- In the United States, call 1-800-345-1518.
- In Canada, call 1-800-263-5868.

For HP technical support:

- In the United States and Canada, call 1-800-652-6672.
- Outside the United States and Canada, refer to <http://www.hp.com>.

HP Insight Management Agents for Servers

Accessing HP Insight Management Agents from a Browser for Microsoft Operating Systems

The HP Insight Management Agents for Servers enable you to view subsystem and status information from a Web browser, either locally or remotely.

To view data locally on Microsoft® operating systems, access <https://127.0.0.1:2381> or <https://localhost:2381>.

The Management Agents can also be browsed locally by selecting **Start>Programs>HP Management Agents>HP System Management Home Page**.

To view data remotely on Microsoft operating systems, access <https://machine:2381>, where *machine* is the IP address or the computer name under DNS.

NOTE: Notice that the URL is followed by 2381. This is the port or socket number that the HP Insight Management Agents for Servers use to communicate with the browser. If this number is not specified, the browser might attempt to connect to another Web page if the managed server is running a Web server.

After you enter the URL, there is a certificate challenge (refer to the section, “Management HTTP Server First-Time Initialization” in this chapter) followed by a login screen (refer to the section “Logging In” in this chapter).

Accessing HP Insight Management Agents from a Browser for Other Operating Systems

To view data locally on operating systems, other than those from Microsoft, access <http://127.0.0.1:2301> or <http://localhost:2301>.

To view data remotely on operating systems, other than those from Microsoft, access <http://machine:2301>, where *machine* is the IP address or the computer name under DNS.

NOTE: Notice that the URL is followed by 2301. This is the port or socket number that the HP Insight Management Agents for Servers use to communicate with the browser. If this number is not specified, your browser might attempt to connect to another Web page if the managed server is running a Web Server.

After you enter the URL, the System Management Homepage is displayed for servers running operating systems other than those from Microsoft.

Browser Requirements

The minimum browser requirements include support for tables, frames, Java™, JavaScript, and Java Development Kit (JDK) 1.1. Additional browsers, or the browsers mentioned, used with different operating systems, might or might not work correctly, depending on their specific implementations of the required browser technologies.

The requirements are TCP/IP and one of the following browsers:

Table 1-1: Browser Requirements

To View Systems Running	Browser Requirements
Novell NetWare 4.x, 5.x, 6.x	Microsoft Internet Explorer 5.5 and Microsoft Internet Explorer 6.0 Netscape Navigator 4.73 and 6
<ul style="list-style-type: none"> Microsoft Windows® Server 2003 Microsoft Windows 2000 with Service Pack 2 	Microsoft Internet Explorer 5.5 and Microsoft Internet Explorer 6.0 Netscape Navigator 4.73 and 6 NOTE: Navigator requires the JDK 1.1 patch. NOTE: To view the SNMP configuration Web pages, you must use Microsoft Internet Explorer 5.0 or later. Netscape Navigator is not supported. NOTE: HP recommends that you install SNMP services to take full advantage of the management capabilities provided with your ProLiant server. Failing to install SNMP prevents the HP Systems Insight Manager and other enterprise management applications from receiving hardware pre-failure alerts and disables Insight Manager functions, such as advanced ProLiant status polling, inventory reporting, and version control.
Tru64 UNIX® v3.2C and later	Netscape Communicator 4.06 or later

continued

Table 1-1: Browser Requirements *continued*

To View Systems Running	Browser Requirements
Tru64 UNIX v4.0F and later	Netscape Communicator 4.5 or later
SCO UnixWare 7 v7.1.1 SCO UnixWare 7 v7.1.3	<ul style="list-style-type: none"> • Netscape Communicator 4.61 or later • Microsoft Internet Explorer 5.5 • Microsoft Internet Explorer 6.0 • Netscape Communicator v4.61 is present in SCO UnixWare 7.1.1 and 7.1.3 CD
Red Hat Linux Advanced Server 2.1	<ul style="list-style-type: none"> • Windows: Netscape Communicator 4.51 or later • Microsoft Internet Explorer 5.01 with Service Pack 2, IE 5.5, and IE 6.0 • Netscape Communicator v4.78
Red Hat Linux 7.3 Professional	<ul style="list-style-type: none"> • Windows: Netscape Communicator 4.51 or later • Microsoft Internet Explorer 5.01 with Service Pack 2, IE 5.5, and IE 6.0 • Netscape Communicator v4.78
Red Hat Linux 8.0 Professional	<ul style="list-style-type: none"> • Windows: Netscape Communicator 4.51 or later • Microsoft Internet Explorer 5.5 • Microsoft Internet Explorer 6.0 • Netscape Communicator v4.78
SuSE Linux Enterprise Server 7	<ul style="list-style-type: none"> • Windows: Netscape Communicator v4.77 on SuSE Linux Enterprise Server 7

IMPORTANT: You must turn on the following options for the HP Insight Management Agents to work properly:

- Enable Java
- Enable JavaScript
- Accept all cookies

HP Web-Enabled System Management software requires Java for full functionality. At a minimum, the help system relies on a Java applet to provide table of contents, index, and search capability. Depending on what Web-Enabled System Management software is installed, there might be other features that are either partially or fully dependant on the presence of Java support in the browser.

The Sun JVM can be obtained directly from the Management CD produced by HP. The Management CD is shipped with all ProLiant servers and many different server options. In addition, you can obtain a subscription to the Management CD to have the latest available software delivered directly to you. For subscription information, refer to <http://www.hp.com/servers/manage>. The JVM is located in the directory <cd>\INSIGHT7\JVM and is a single, installable package. This version of the JVM is qualified for HP Systems Insight Manager and the Web-Enabled System Management software installed on HP devices.

Java support for Microsoft Internet Explorer can be downloaded from Microsoft. One location to try is <http://www.microsoft.com/java/sdk> where the JVM is contained in the Microsoft SDK for Java. Microsoft Windows Update, <http://windowsupdate.microsoft.com>, can also provide a Microsoft VM (or updated version of the VM if available).

Java support can be downloaded from Sun for both Microsoft Internet Explorer and Netscape Navigator. A good starting location for finding the appropriate download from Sun is <http://java.sun.com>.

For the Tru64 UNIX Server agents, the Netscape option, “Accept cookies originating from the same server as the page being viewed” can be used instead of “Accept all cookies.”

Updating Netscape Communicator for Tru64 UNIX Workstations

Update your version of Netscape Communicator by downloading the software from <http://home.netscape.com/download>.

Security

The HP Insight Management Agents allow SNMP sets for some system parameters. This capability requires security that includes the three predefined users. For agents running on Microsoft and Linux operating systems, there are no default passwords. On a fresh install the administrator password, operator password, and user passwords are configured during installation. For agents running on other operating systems, the default passwords are defined in Table 1-2.

Table 1-2: Password

Account	User Name	Password
anonymous	anonymous	
user	user	public
operator	operator	operator
administrator	administrator	administrator

NOTE: These are the only user accounts available in this release, and they cannot be changed except for the password. Under Tru64 UNIX, the account names, user names, and passwords are lowercase characters.

The Web-Enabled HP Management Agents for Servers for NetWare is located in the WEBAGENT.INI file in the SYS:\SYSTEM\CPQMGMT\WEBAGENT directory. It specifies the level of user who has access to data. The “read=” and “write=” entries in the file set the user accounts required for access, where:

- 0 = no access
- 1 = anonymous
- 2 = user
- 3 = operator
- 4 = administrator

Changing these entries changes the security level.

Anonymous access to information is available without logging in when the System Management Homepage is launched for the first time on operating systems other than those from Microsoft and Linux.

Deploying the Configurations to Servers Running Microsoft Windows

On Microsoft operating systems, anonymous access is disabled by default but can be turned back on by the user through the **Options** link on the System Management Homepage.

There are three types of data:

- Default (read only)
- Sets (read/write)
- Reboot (read/write)

The WEBAGENT.INI file is located in the system_root/cpqmgmt/webagent directory. Do not modify anything except the read/write levels to change the security.

Deploying the Configurations to Servers Running Tru64 UNIX

Under Tru64 UNIX, the location of the WEBAGENT.INI file depends on whether the Management Agents for Tru64 UNIX were installed as part of the base operating system or as an upgrade. You can determine the location of the WEBAGENT.INI file by issuing the following command:

```
# ps -ef | grep -i cpqthresh_mib | grep -v grep
```

The command output resembles one of the following lines:

```
root 12278 1 0.0 ... /usr/sbin/cpqthresh_mib
root 12278 1 0.0 ... /var/opt/CPQIM100/bin/cpqthresh_mib
```

Use the path name displayed in the output of the ps command to locate the WEBAGENT.INI file on your system as follows:

- The WEBAGENT.INI file is located in the directory `/var/im/webagent` if the pathname is `/usr/sbin/cpqthresh_mib`.
- The WEBAGENT.INI file is located in the directory `/var/opt/CPQIMddd/web/im/webagent` if the pathname is `/var/opt/CPQIMddd/bin/cpqthresh_mib`, where the value `ddd` indicates the version of the Management Agents installed on the system.

The Web Agent service must be stopped and restarted for any changes to take effect for Tru64 UNIX operating systems.

Deploying the Configurations to Servers Running Linux

The configuration settings for the Management HTTP Server are stored in three files. The passwords for the Management HTTP Server are stored in `/var/spool/compaq/wbem/CPQHMMMD.ACL`.

The configuration settings for the Management HTTP Server that existed through version 3.x is stored in `/var/spool/compaq/wbem/homepage/cpqhmmmd.ini`.

The configuration settings for the Management HTTP Server that were introduced in version 4.x and later are stored in `/var/spool/compaq/wbem/homepage/cpqhmmdx.ini`.

To deploy the Management HTTP Server configuration to other servers, copy the corresponding ACL file and INI files previously listed.

There are three types of data: Default (read only), Sets (read/write), and Reboot (read/write). The `.ini` files located in `/opt/compaq/webagent` are the configuration files used by the Web-Enabled HP Insight Management Agents.

Deploying the Configurations to Servers Running NetWare

In NetWare, the WEBAGENT.INI file is located in the `sys:\system\cpqmgmt\webagent` directory and specifies the level of user that has access to data. The “read=” and “write=” entries in the file set the user accounts required for access, where: 0 = No access, 1 = anonymous, 2 = user, 3 = operator, and 4 = administrator. Changing these entries changes the security.

The Web Agent service must be stopped and restarted for any changes to take effect. Do not modify anything except the read/write levels to change the security.

Deploying the Configurations to Servers Running SCO UnixWare 7

There are three types of data:

- Default (read only)
- Sets (read/write)
- Reboot (read/write)

The SCO UnixWare 7 WEBAGENT.INI is located in the `/opt/compaq/webagent` directory.

The Web Agent service must be stopped and restarted for any changes to take effect. Do not modify anything except the read/write levels to change the security.

Management HTTP Server First-Time Initialization

Introduction

The System Management Homepage is the one-stop-centralized simple view for all the management information and configuration data generated by Web-Enabled System Management software and utilities. The status of the Management software and utilities installed on the system is aggregated on the System Management Homepage. Integrated Help on the Homepage provides all the pertinent help information for the Management software and utilities on the system.

What is Management HTTP Server?

The Management HTTP Server is a Web server embedded in much of the HP Web-Enabled System Management software.

Overview

After a product that uses the Management HTTP Server has been installed and configured, there are a few things that occur the first time the Management HTTP Server is initiated. Upon initialization, the Management HTTP Server creates a private key and a corresponding self-signed, base64-encoded certificate. This process only occurs the first time that the Management HTTP Server is started, not every time it is started. This certificate is a base64-encoded PEM file. The certificate is stored on the file system as `\compaq\wbem\cert.pem`. The `\compaq\wbem` subdirectory also contains the private key. To protect the key, this subdirectory is only accessible to administrators if the file system allows it. For private key security reasons, it is highly recommended that the Management HTTP Server be installed on Windows NT® file systems (NTFS).

NOTE: For Microsoft Windows operating systems, the `\compaq\wbem` subdirectory must exist on an NTFS file system for the private key to have administrator-only access through the file.

If you feel that the private key has been compromised, the administrator can delete the `\compaq\wbem\cert.pem` file and restart the server. This action prompts the Management HTTP Server to generate a new certificate and private key.

Logging In

The Login dialog box enables you to access any of the available Web agents. To access an agent:

1. Navigate to <https://devicename:2381>. The first time you browse to this link, the Security Alert dialog box appears prompting you to indicate whether or not to trust the server.

NOTE: The Security Alert dialog box shown is specific to Internet Explorer, however Netscape 4.0 and later is supported as well.

NOTE: If you want to implement your own PKI or install your own generated certificates into each managed device, you can install a Certificate Authority Root Certificate onto each browser to be used for management. If this is implemented, the Security Alert dialog box, shown in the following illustration, should not be displayed. If the alert displays when you do not expect it, you might have browsed to the wrong device. You can refer to the online help in your browser for more information about installing the Certificate Authority Root Certificate.



2. Click **Yes**. The Login page appears.

The screenshot shows the 'System Management Homepage for RUMBLEFISH' with the following elements:

- HP logo and title: **System Management Homepage for RUMBLEFISH**
- Login Account: **anonymous** (with a [Refresh Page](#) link)
- IP Address: **16.101.169.204**
- Date/Time: **Friday, September 27, 2002 8:32:53 PM**
- Section Header: **Account Login**
- Warning: **This is a private system. Do not attempt to login unless you are an authorized user. Any authorized or unauthorized access and use may be monitored and can result in criminal or civil prosecution under applicable law.**
- Text: **You are being prompted to provide login account information for RUMBLEFISH.**
- Text: **Please provide the information requested and press the OK button to complete the login process.**
- Text: **A successful login will bring up the original system management information requested, or the Device Home Page if this login was manually initiated. The Password for a login account may be changed at any time by an Account Administrator.**
- Form fields: **User:** dropdown menu (selected: administrator), **Password:** text input field.
- Button: **OK**

NOTE: If you have enabled anonymous access, then the System Management Homepage displays.

3. Select the appropriate account from the User: dropdown list. The options include administrator, operator, or user.
4. Enter the correct password in the Password: field.
5. Click **OK**. The System Management Homepage is displayed.

NOTE: In reference to the Version Control Repository Manager, the anonymous login (if enabled) and the user login, enable you to access all pages. However you cannot configure a repository; delete, copy, or create ProLiant Support Packs; install components; or clear the log. The anonymous login is disabled by default.

System Management Homepage

The System Management Homepage displays all HP Web-Enabled System Management software that provides information. In addition, the System Management Homepage displays various boxes that have borders defining the status of the items contained in that box. Refer to Status Box Indicators for more information. The System Management Homepage is separated into two frames:

- Header frame
- Data frame

The screenshot displays the HP System Management Homepage for RUMBLEFISH. The header includes the HP logo, system model (ProLiant 3000), system status (OK), and current user (administrator). Navigation tabs for Home, Settings, Tasks, and Logs are visible. The main content area shows a 'Failed & Degraded Items' section with 'none' listed. Below this are three status boxes: Performance (OK), Storage (File System Space Used), and System (Operating System Software Version Info). A key at the bottom left explains the status indicators: OK (green check), Degraded (yellow check), Failed (orange X), and Unknown (blue circle).

Header Frame

The header frame is constantly visible regardless of which tab you are viewing. A link, located in the top section, displays the path you are currently viewing.

The System Management Homepage displays:





- System Status
- System Model
- Current User
- Agent Help link

System Status

The System Status icon indicates the overall health of the HP Web-Enabled System Management software. Refer to the following table for a description of the icons.

System Status Icons Legend

Table 1-3: System Status Icons

Icon	Key Word
	Unknown
	OK
	Degraded
	Failed

System Model

The System Model displays the model of the device. In some cases, the System Model might display Unknown if the HP Insight Management Agents are not installed on the device.

Current User

The Current User displays the identity of the user that is currently logged in. If the current user is administrator, operator, or user, then a Logout link is displayed. If anonymous access is enabled, and you are accessing the page anonymously, the Current User displays Anonymous, and the Login link is displayed. If Local Access is enabled, and you are accessing the HP Web-Enabled System Management software from a local machine, the Current User displays Administrator or Anonymous (depending on what level of access has been enabled) and Local Access.

Agent Help Link

The Agent Help link launches the help files in a separate browser window. The help files contain a combination of the help files related to the HP management software and utilities.

Data Frame

The Data Frame displays the status for all HP management software and utilities on the system.

How to Replicate Passwords and Configuration Data Across Multiple Devices

If your enterprise has numerous devices and you wish to share common passwords, configuration information, and certificates of trusted HP Systems Insight Manager servers, this can be accomplished by copying certain files from the desired device to the other devices.

To replicate the user passwords, replicate:

```
\compaq\wbem\cpqhmmmd.ac1
```

To replicate the Management HTTP Server configuration information, replicate:

```
\compaq\wbem\homepage\cpqhmmmd.ini
```

```
\compaq\wbem\homepage\cpqhmmmdx.ini
```

To replicate the certificates of the trusted HP Systems Insight Manager servers, replicate all files that exist in:

```
\compaq\wbem\certs
```

After the desired files have been replicated to a given device, the Management HTTP Server must be restarted for the changes to take affect.

Navigating In Management HTTP Server

Tabs

The System Management Homepage displays up to five tabbed pages that enable you to access and/or configure settings related to participating HP Web-Enabled System Management software. The Tools tab and the Tasks tab are only visible if HP Web-Enabled System Management software provides information for them.

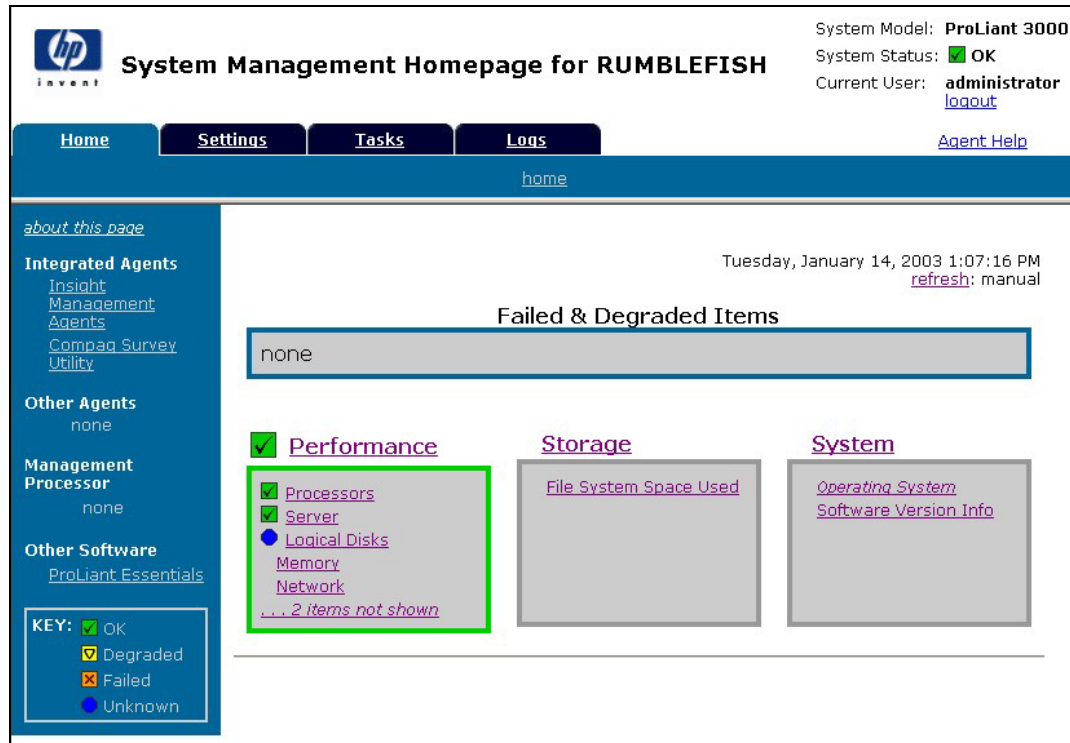
The System Management Homepage tabs that can be displayed are:

- Home
- Settings
- Tasks
- Tools
- Logs

Home

The Home tab is displayed on the System Management Homepage. The following information is displayed on the Home tab:

- Failed & Degraded Items field
- Status boxes
- Left organizational menu



The screenshot shows the HP System Management Homepage for RUMBLEFISH. The top right corner displays system information: System Model: ProLiant 3000, System Status: OK, and Current User: administrator. The main navigation bar includes Home, Settings, Tasks, and Logs. The Home tab is active, showing a 'home' link. The left sidebar contains links for Integrated Agents (Insight Management Agents, Compaq Survey Utility), Other Agents (none), Management Processor (none), and Other Software (ProLiant Essentials). A key at the bottom left defines status icons: OK (green check), Degraded (yellow check), Failed (red X), and Unknown (blue circle). The main content area displays 'Failed & Degraded Items' as 'none'. Below this are three status boxes: Performance (OK), Storage (File System Space Used), and System (Operating System, Software Version Info).

Failed & Degraded Items Box

The Failed & Degraded Items field displays all devices, which have a failed or degraded status, provided by the HP Web-Enabled System Management software. If there are no agents installed or no failed or degraded items, none appear in the Failed & Degraded Items field.

Status Boxes

The HP Web-Enabled System Management software provides the information configured to display in the Management HTTP Server. The information provided by the HP Web-Enabled System Management software is displayed in a box. Each box contains links that enable you to drill down into the HP Web-Enabled System Management software that is providing the data. In addition, each box has a border that indicates the status of the HP Web-Enabled System Management software information contained in the box. Refer to Table 1-4 for a description of the Status Box indicators.

Status Box Indicators

Table 1-4: Status Box Indicators

Indicator	Description
Blue	Unknown
Green	OK
Yellow	Degraded
Orange	Failed
Gray	No Status

Left Organizational Menu

The left organizational menu appears on the Home tab. The left organizational menu contains links to the HP Web-Enabled System Management software to include:

- About this page
- Integrated agents
- Other agents
- Management processor
- Other software
- Key legend

About This Page

The About this page link launches an introduction help file that provides an overview of System Management Homepage.

Integrated Agents

The Integrated Agents section contains participants and links to their entry points if applicable. You can click an agent link to access that particular agent.

NOTE: Participants are agents that are contributing information contained in the System Management Homepage.

Other Agents

The Other Agents section lists the visible HP Web-Enabled System Management software that does not participate in the System Management Homepage. The name of the HP Web-Enabled System Management software provides a link to access the agents if they provide a user interface.

Management Processor

The Management Processor section displays a link to either the Remote Insight Lights-Out Edition Board Web pages or the Integrated Lights-Out hardware Web pages. This information is provided by Insight Management Agents. If no HP Web-Enabled System Management software is installed that provides this information, then None is displayed.

Other Software

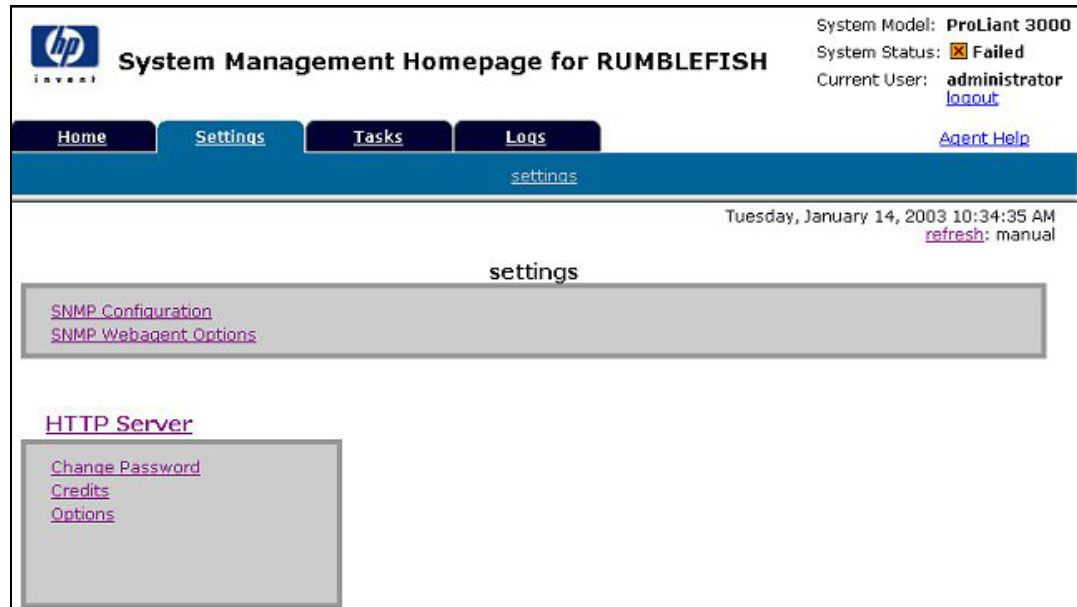
The Other Software section provides information regarding value-added software, as well as links to pages that contain software information, including ProLiant Essentials value-added software on <http://www.hp.com>. For detailed information regarding ProLiant Essentials value-added software, refer to <http://www.hp.com/servers/proliantessentials>.

Key Legend

The Key legend displays a listing of status icons and a brief description of each. For more information regarding the status icons, refer to Table 1-4.

Settings

The Settings tab provides you with the ability to access the agent options and define the Management HTTP Server security settings.



Settings Section

The Settings section provides a listing of participating agents. Each of the participating agents has options already defined.

Management HTTP Server Section

The Management HTTP Server section provides links allowing you to configure your Management HTTP Server settings. The Management HTTP Server section provides links to:

- Change Password
- Credits
- Options

Change Password

The Change Password option enables you to change the Management HTTP Server password.

The screenshot shows the HP System Management Homepage for RUMBLEFISH. The page title is "System Management Homepage for RUMBLEFISH". The current user is "administrator" and the system status is "OK". The page is titled "Change HTTP Server Password". The form includes a "User" dropdown menu set to "administrator", "New Password" and "Confirm Password" text input fields, and a "Change Password" button. A note states: "Only the administrator may change passwords. The New Password and Confirm Password must be identical for the change to be successful. Note: The old password for the User is not needed, since the Account Administrator has the necessary privilege to overwrite an existing password." The breadcrumb trail is "settings -> http_server -> change_password". The date and time are "Thursday, January 16, 2003 2:08:55 PM" and there is a "refresh: manual" link.

Changing the Management HTTP Server Password:

1. Click **Change Password** to change the password for the Management HTTP Server.
2. In the User field, select the user level from the dropdown list.
3. In the New Password field, enter the new password for the user level you selected.
4. In the Confirm Password field, enter the same password you entered in the Password field.
5. Click **Change Password**. A dialog box is displayed indicating whether or not the password was successfully changed.

Credits

The Credits link displays information regarding licensing and credits.

Credits

Use of the OpenSSL Toolkit

This software uses the OpenSSL toolkit. The OpenSSL toolkit is used under a dual license. The conditions of both the OpenSSL License and the original SSLeay license apply to its use

- **This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>).**

```

/* =====
 * Copyright (c) 1998-2000 The OpenSSL Project. All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 *
 * 1. Redistributions of source code must retain the above copyright
 * notice, this list of conditions and the following disclaimer.
 *
 * 2. Redistributions in binary form must reproduce the above copyright
 * notice, this list of conditions and the following disclaimer in
 * the documentation and/or other materials provided with the
 * distribution.
 *
 * 3. All advertising materials mentioning features or use of this
 * software must display the following acknowledgment:
 * "This product includes software developed by the OpenSSL Project
 * for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
 *
 * 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
 * endorse or promote products derived from this software without
 * prior written permission. For written permission, please contact
 * openssl-core@openssl.org.
 *
 * 5. Products derived from this software may not be called "OpenSSL"
 * nor may "OpenSSL" appear in their names without prior written
 * permission of the OpenSSL Project.
 *
 * 6. Redistributions of any form whatsoever must retain the following
 * acknowledgment:
 * "This product includes software developed by the OpenSSL Project
 * for use in the OpenSSL Toolkit (http://www.openssl.org/)"
 *
 * THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
 * EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
 * PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR
 * ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
 * SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
 * NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
 * LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
 * STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
 * ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
 * OF THE POSSIBILITY OF SUCH DAMAGE.
 * =====

```


Options

The Options link accesses the Options page. The Options page enables you to change various Web-based System Management settings. The System Management Setup Wizard initially enables you to set many of the options from this page, however you can access the Options page in order to edit any of the initial settings. The Page Sections divide the available options into three groups:

- Configuration Options
- Trusted Certificates
- Customer Generated Certificates

Page Sections:	
Configuration Options	The list of general options such as anonymous access, local access type, and more
Trusted Certificates	A way to specify the certificates for management applications on trusted servers.
Customer Generated Certificates	A way to extract a PKCS #10 certificate request and import a PKCS #7 generated certificate.

Configuration Options

The Configuration Options section enables you to select the appropriate settings to include:

- **Anonymous access**—Anonymous access is disabled by default. Enabling anonymous access enables a user to access Web Agents without logging in.

Enabling Anonymous Access

- a. Select **Anonymous Access** from the Configuration Options page.
 - b. Click **Save Configuration** in the Configuration Options section to save your settings. The Configuration Options page refreshes.
- **Local Access**—Local Access enables you to set up the Management HTTP Server to automatically configure local IP addresses as part of the selected group. This means that any user with access to the local console is granted full access if administrator is selected. If anonymous is selected, any user has access, limited to unsecured pages, without being challenged for a username and password.

NOTE: If this Management HTTP Server is running on the same machine as HP Systems Insight Manager, Local Access (anonymous) must be enabled for certain features of HP Systems Insight Manager to work. If Local Access (administrator) or Anonymous Access is enabled, that also works, but is not necessary.

- **Logging**—Logging enables you to specify the types of log entries you want to record, and whether or not you want to write to the log at all.

Setting the Logging Options

- a. Select **Logging** to record information in the log file.
 - b. Select **Security Error** or **Security Information** as the type of log to be recorded.
 - c. Click **Save Configuration** in the Configuration Options section to save your settings.
- **IP Restricted Logins**—The Management HTTP Server can restrict login access based on the IP address of the machine from which the login is attempted. These restrictions apply only to direct login attempts and not to logins attempted as part of a trusted HP Systems Insight Manager server's Single Login or Secure Task Execution features.

IP addresses can be explicitly excluded or explicitly included for each type of user. If an IP address is explicitly excluded, it is excluded regardless if it is also explicitly included. If there are any IP addresses in the inclusion list, then only those IP addresses are allowed login access. If there are no IP addresses in the inclusion list, then login access is allowed to any IP addresses not in the exclusion list.

IP address ranges should be listed with the lower end of the range followed by a hyphen followed by the upper end of the range. All ranges are inclusive in that the upper and lower bounds are considered part of the range. IP address ranges and single addresses are separated by semicolons.

IP address ranges should be entered in the following format:

122.23.44.1-122.23.44.255;172.84.100.35;127.0.0.0-127.0.0.255

- Trust Mode—The Trust Mode options enable you to select the security required by your system. There are some situations that require a higher level of security than others, so you are given the options as shown.

Trust Mode

Secure Trust Modes:

Trust By Certificate:
 Setup the HTTP Server to only accept Secure Task Execution requests and Single Login requests that have been signed by an Insight Manager 7 server with a [Trusted Certificate](#).

Other Trust Modes:
Note: These trust modes are considered less secure than certificate based trust modes. HP strongly recommends using Trust by Certificate.

Trust All:
 Setup the HTTP Server to accept Secure Task Execution requests and Single Login requests from any server.

Trust By Name:
 Setup the HTTP Server to only accept Secure Task Execution requests and Single Login requests from servers with the following Insight Manager 7 server names (separate server names with commas or semi-colons).

NOTE: Click **Default Configuration**, located in the Configuration Options section, to return all options back to their original settings.

- Trust By Certificate—The Trust by Certificate mode sets the Management HTTP Server to only accept certain requests from HP Systems Insight Manager servers with Trusted Certificate as shown. This mode requires the submitted server to provide authentication by means of certificates. This mode is the strongest method of security, since it requires certificate data and verifies the digital signature before allowing access.
- Trust All—The Trust All mode sets the Management HTTP Server to accept certain requests from any server. For example, you could use the Trust All option if you have a secure network and everyone in the network is trusted.

NOTE: The Trust All option leaves your system vulnerable to security attacks.

- Trust By Name—The Trust By Name mode sets the Management HTTP Server to only accept certain requests from servers with the HP Systems Insight Manager names designated in the Trust By Name field. The Trust By Name option is easy to configure, and prevents non-malicious access. For example, you could use the Trust By Name option if you have a secure network with two separate groups of administrators in two separate divisions. It would prevent one group from installing software to the wrong system. This option does not verify anything other than the HP Systems Insight Manager server name submitted.

Using the Trust By Name Option

1. Select **Trust By Name**.
2. Enter the name of the server you want to allow access. If you want to trust more than one HP Systems Insight Manager server, separate the server names with a semicolon.

NOTE: Although Trust By Name mode is a slightly stronger method of security than the Trust All mode, it still leaves your system vulnerable to security attacks.

Trusted Certificates

The Trusted Certificates section enables you to manage your certificates in the Trusted Certificates list.

Trusted Certificates

Certificates are used to establish the trust relationship between Insight Manager 7 and the HTTP Server. To add a certificate to the Trusted Certificates List, cut and paste the base64 encoded certificate into the text box and press the 'Submit Cert' button.

Insight Manager 7 Certificate Data:

Insight Manager 7 certificates can also be retrieved through HTTP requests. To retrieve the public certificate, enter the server name in the text box below and press the 'Get Cert' button.

Insight Manager 7 Server Name:

Using the Trusted Certificates Option:

1. In the HP Systems Insight Manager Server Name field, enter the name of the server from which you wish to receive a certificate.
2. Click **Get Cert**. The certificate data is displayed.
3. Click **Add Cert** to add the displayed certificate to the Trusted Certificates list.

NOTE: If you have the base64-encoded certificate file for HP Systems Insight Manager, cut and past this certificate information into the HP Systems Insight Manager Certificate Data box, and click **Submit Cert**.

NOTE: If HP Systems Insight Manager is reinstalled or a new certificate is regenerated, you must remove the trusted servers and start again with step a. Even though the HP Systems Insight Manager server name is the same in the list, the underlying certificate has changed.

Customer Generated Certificates

The Customer Generated Certificates option enables you to use certificates that are not generated by HP. If this option is selected, the self-signed certificate that was originally generated by the Management HTTP Server is replaced with one that was issued by a Certificate Authority.

The first step of the process causes the Management HTTP Server to create a Certificate Request (PKCS #10). This request utilizes the original private key that was associated with the self-signed certificate and generates the appropriate data for certificate request (the private key never leaves the server).

The next step is sending the request to a Certificate Authority. After the Certificate Authority has returned PKCS #7 data, the final step is importing the data into the Management HTTP Server.

After the PKCS #7 data has been successfully imported, the original `\compaq\wbem\cert.pem` certificate file is overwritten with the device certificate from that PKCS #7 envelope. The same private key is used for the new imported certificate as was used with the previous self-signed certificate.

Customer Generated Certificates

The HTTP Server can create Certificate Request (PKCS #10) data which can be sent to a Certificate Authority (CA) at a later time. This data is base64 encoded. The CA will process this request and return a response file (PKCS #7) which can be imported into the HTTP Server. Use the button below to create the PKCS #10 Certificate Request data.

The HTTP Server imports base64 encoded PKCS #7 data which a Certificate Authority returned based upon an earlier Certificate Request (PKCS #10). Cut and paste the PKCS #7 information into the text box below and press the button below to import it into the HTTP Server.

PKCS #7 Data:

Using the Customer Generated Certificate Option

1. Click **Create PKCS #10 Data**. A screen is displayed indicating that the PKCS #10 Certificate Request data has been successfully generated.
2. Copy the certificate data.

3. Send PKCS #10 certificate request data to a Certificate Authority and ask them to send you the certificate request reply data in the form of PKCS #7 format. Request that the reply data be in base64-encoded format. If your organization has its own PKI/Certificate Server implemented, send the PKCS#10 data to the Certificate Authority manager and request the PKCS#7 reply data.

NOTE: The selected certificate signer generally charges a fee.

4. When the certificate signer sends the PKCS#7 certificate request reply data to you, copy the data from the PKCS#7 certificate request reply and paste the copied data in the PKCS #7 Data field.
5. Click **Import PKCS #7 Data**. A message displays indicating whether or not the Customer Generated certificate was successfully imported.
6. Stop the services.
7. Restart the services.
8. Browse to the managed device that contains the imported certificate.
9. Select **view the certificate** when prompted by the browser. Be sure the signer is listed as the signer you used, and **not** listed as HP, before importing the certificate into your browser. Alternatively, you can import root CA cert into all the browsers on your network to avoid being prompted.

NOTE: If the certificate issuer's organizational unit (OU) is still listed as the Management HTTP Server, start over with step 1.

NOTE: If the certificate signer of your choice sends you the certificate data in base64-encoded form instead of PKCS #7 data, you must copy the base64-encoded file to the filename `/compaq/WBEM/Cert.pem` and reboot the machine.

NOTE: Click **Default Configuration** to revert to default settings. This does not remove imported Trusted HP Systems Insight Manager certificates or imported Customer Generated certificates.

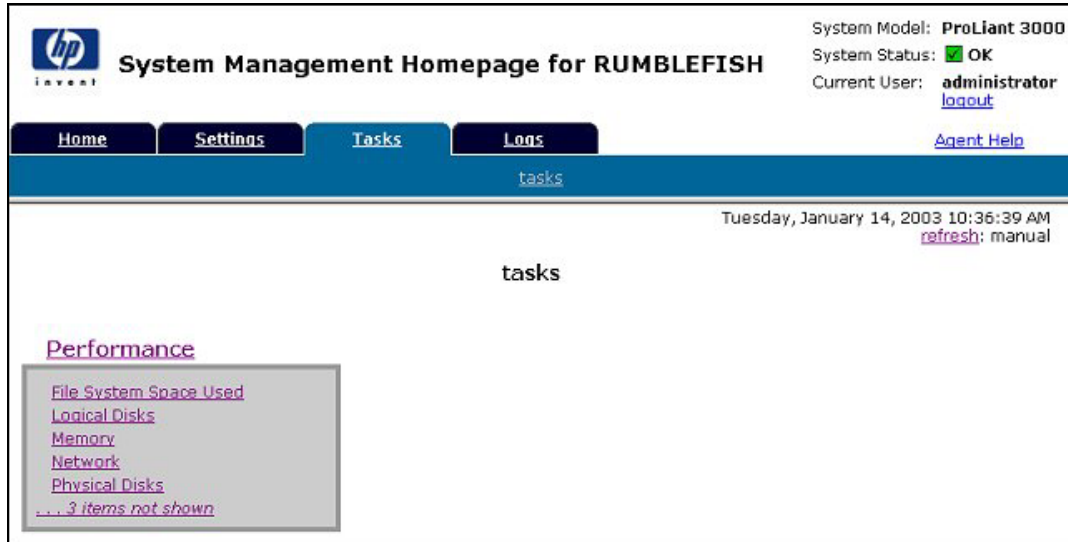
NOTE: After you have successfully imported the PKCS#7 certificate, you might see a dialog box. To eliminate this box, import the certificate.

NOTE: Import the authority certificate into your browser as a Trusted Root Certification Authority. Your Certificate Authority can provide you with their certificate and you can import it into your browser using the normal process. For details on how to import a certificate, refer to the help files that came with your browser.

Tasks

The Tasks tab displays links to task-oriented pages provided by participating HP Web-Enabled System Management software.

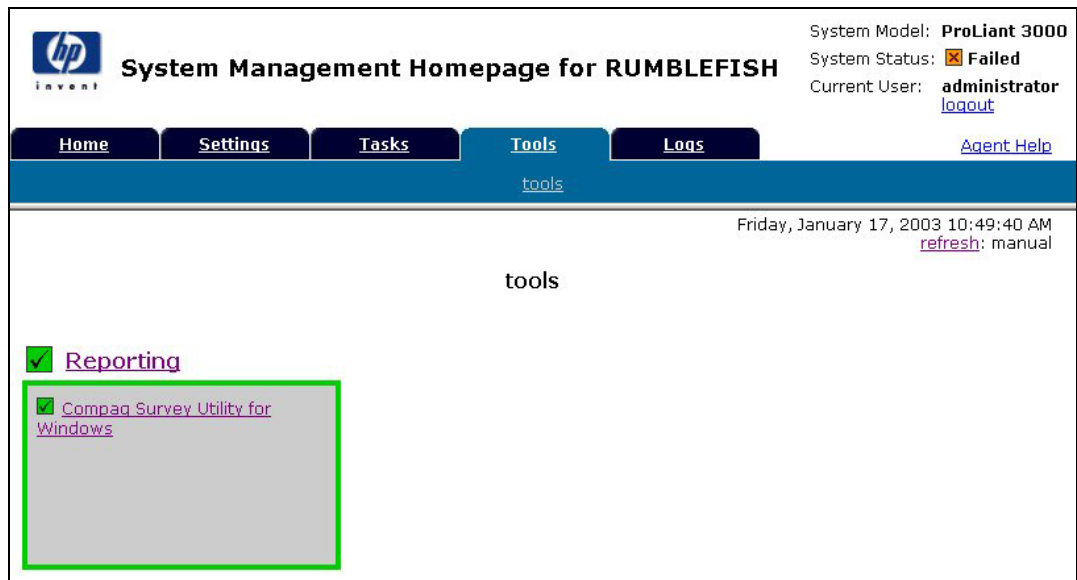
NOTE: If the HP Web-Enabled System Management software provides no tasks, the Tasks tab is not visible.



Tools

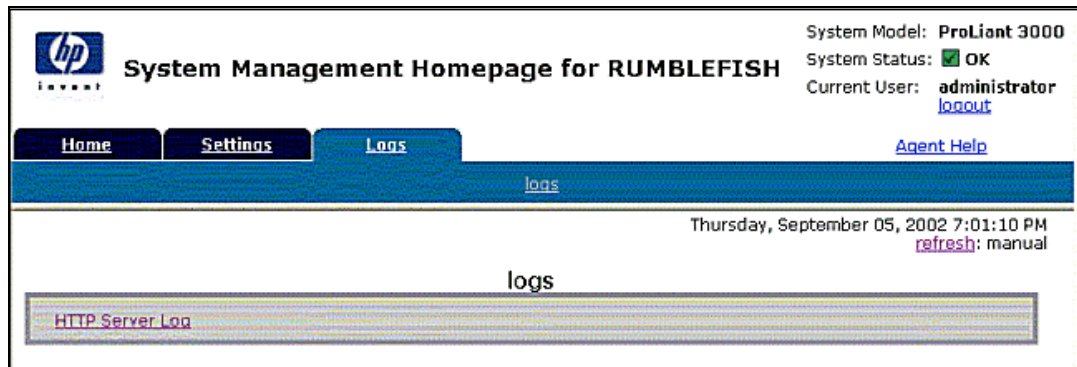
The HP Web-Enabled System Management software provides information that is displayed on the Tools tab. For example, if the Survey Utility is installed on the device, then a link to the Survey Utility is displayed on this tab.

NOTE: If the HP Web-Enabled System Management software provides no information, the Tools tab is not visible.



Logs

The Logs tab includes various log information. Any logs contained in the installed HP Web-Enabled System Management software can be displayed on this tab. For example, if the Version Control Agent is installed, a link to the Version Control Agent log is displayed on the Logs page. You can access the entry point to the log shown by clicking the link.



Management HTTP Server Log

The Management HTTP Server Log contains primarily security-related events. This log is helpful when troubleshooting security problems in participating HP Web-Enabled System Management software.

hp **System Management Homepage for RUMBLEFISH**

System Model: **ProLiant 3000**
 System Status: **Failed**
 Current User: **administrator**
[logout](#)

[Home](#) [Settings](#) [Tasks](#) [Tools](#) [Logs](#) [Agent Help](#)

logs -> http_server_log

HTTP Server Log File

```

SECURITY ERROR   Severity=1   Mon Feb 25 11:20:05 2002
Unable to load certificate file during SSL Server Initialization

SECURITY INFORMATION   Severity=0   Mon Feb 25 11:20:08 2002
A new private key and self signed certificate were generated.

SECURITY ERROR   Severity=1   Mon Feb 25 11:20:08 2002
Private key could not be successfully secured via the file system protection.

SECURITY INFORMATION   Severity=0   Mon Feb 25 11:21:13 2002
Login Succeeded: as user 'administrator' from 16.101.169.204

SECURITY ERROR   Severity=1   Mon Feb 25 11:25:23 2002
Unable to acquire the SSL port needed for SSL Server capabilities.

HELPPFILE INFORMATION   Severity=0   Mon Feb 25 11:25:24 2002
Help File Aggregation started.

HELPPFILE INFORMATION   Severity=0   Mon Feb 25 11:25:24 2002
Help File Aggregation completed.

HELPPFILE INFORMATION   Severity=0   Mon Feb 25 11:25:26 2002
Help File Aggregation started.

HELPPFILE INFORMATION   Severity=0   Mon Feb 25 11:25:26 2002
Help File Aggregation completed.
    
```


Subsystem Status Information

Select **Insight Management Agents** from the System Management Homepage tab to view subsystem and status information for the device. This section describes how to navigate through the management information.

The date and time displayed at the bottom of the Summary page shows the local time the page was last received by your Web browser. To refresh this frame, select the **Manually Refreshed** link at the bottom of the page.

Title Frame

The Title Frame, located in the upper-left corner of the browser window, displays the following links:

- Agent Help—Use this link to navigate to this help page.
- Summary—Use this link to quickly navigate back to the list of degraded or failed components on the Summary Page.
- Device Home—Use this link to return to the System Management Homepage.
- Options—Use this link to go to the Options Page and set options for Display Mode (frames or no frames), Help icons, and Auto Refresh intervals.

Management Agents
Version 6.20.0.0
[Agent Help](#) [Summary](#) [Device Home](#) [Options](#)

Condition Legend
 Unknown OK
 Degraded Failed

CONFIGURATION
[System Info](#)
 [System Board](#)
 [Exp. Boards](#)
[System Resources](#)

Summary ?

RUMBLEFISH: ProLiant 3000

Contact Information: N/A
 Location: N/A
 IP Address: 16.101.169.204
 Current Webagent User: administrator [login](#) [logout](#)

Failed or Degraded Items

Item Name:	Category:
<input checked="" type="checkbox"/> Integrated Log	Recovery

[Manually Refreshed](#) @ Monday, February 10, 2003 2:29:02 PM

Summary Page

The Summary page displays the device name, type, contact information and location, IP addresses, current webagent user and if the system supports it, Unit Identifier LED Status is displayed, as well as a list of failed or degraded items. To view detailed information about a failed or degraded item, click the link provided.

Unit Identifier LED Status—enables users to flag a particular server in a rack containing many units. The Summary screen indicates if the Unit Identification LED is off. If the system does not support Unit Identifier LED, the Summary screen shows that the Unit Identifier LED is not available. Only “operator” and “administrator” webagent users are authorized to change the Unit Identifier LED on or off with a button that is present.





Send Test Trap to Trap Destination

The **Send Test Trap** button allows users to send test traps to the trap destination. For NetWare, the trap destination needs to be set in SYS:\ETC\TRAPTARG.CFG first. Refer to the documentation supplied by the OS provider to set the trap destination using the INETCFG utility.

Device Status

The colored icons next to the individual items in the following list indicate the status of each item.

Table 1-5: Device Status Icons

	Device status is unknown.
	Device status is OK.
	Device status is degraded.
	Device status is failed.

NOTE: In the no-frames version of this software, the Summary page fills the entire browser window. Each subsequent page has the equivalent of the contents of the Title Frame at the top with links to Help, Summary, Device, Home, and Options pages. The Summary page in the no-frames version displays all device categories and items within each category sorted by status. To view detailed information about an item, click the item.

Navigation Frame

The Navigation Frame, located below the Title Frame on the left side of the browser window, lists all of the subsystems with components that are available for the devices.

The icons next to the various items in the list indicate the status of those items. A legend for the icons is displayed in the Title Frame. Select a component in the left frame to display detailed information about it in the right frame.

Information about the following subsystems is available in other chapters found in this reference guide:

- Configuration Subsystem
- Mass Storage Subsystem
- NIC Subsystem
- Utilization Subsystem
- Recovery Subsystem
- Windows NT Operating System
- Novell NetWare Operating System

The SNMP Configuration under the Configuration Subsystem can be used to configure Server SNMP Service and HP Insight Management Agents for servers that are running Microsoft operating systems.

NOTE: Only blade server-based systems display the Enclosure Information link. Clicking the Enclosure Information link takes you to the Enclosure Information page.

Data Frame

The Data Frame comprises the remainder of the browser window and displays detailed information about the selected items. This window also displays the Summary Page when the Summary option is selected from the Title Frame.

NOTE: Some items might split the Data Frame into sub-frames that follow the same organizational structure as the main frame with navigation data in a sub-frame on the left and detailed information in a sub-frame on the right.

Group Configuration

Group Configuration of the Web Agent is one of the tasks in HP Systems Insight Manager that operates using Secure Task Execution (STE). During task setup you can view and edit the source device's configuration. This configuration can then be copied to a target set or a group of devices. This can be useful for copying existing configurations from a source device to multiple destinations. The destinations are determined by the selected query. The *HP Systems Insight Manager Technical Reference Guide* is located on the Management CD and on the web at <http://www.hp.com/servers/proliant/manage>.

NOTE: HP Insight Management Agents must have at least one community string predefined with READ-CREATE rights. Additionally, the HP Insight Management Agents must have sets enabled. To enable sets go to **Control Panel>Management Agents**.

The group configuration support-based thresholds have three items that can be set using the HP Systems Insight Manager group configuration screen.

- CPU Thresholds
- Page File Thresholds
- Cache Hits Thresholds

Select a source device and click **Next** from the HP Systems Insight Manager screen. Select the **Edit** link from the group configuration tree display for the HP Subsystem Status information. Select **Threshold Settings>Threshold Properties**. If the cursor is placed over any of the threshold settings, a tool tip states, "Threshold warning and critical value settings, a value of 0 means it is not set." You can select one or more of the settings before saving the configuration information. You do not need to select all settings. The warning and critical levels are grouped together for each setting.

Warning and critical threshold limits can be set for the properties where indicated in the following list. Alarms are sent when the performance property value meets the threshold conditions and stays for 15 data-collection intervals. The data-collection interval is set in the Management Agents Control Panel applet under Windows Control Panel Settings. Alarms are sent to the configured destinations through SNMP and e-mail.

NOTE: To set thresholds the user must have administrator access on the managed device.

CPU Threshold

% CPU Time—The percentage of time that all processors are executing a non-idle thread. Designed as a primary indicator of processor activity, this counter is calculated by measuring the time that each processor spends executing the thread of the idle process in each sample interval, and subtracting that value from 100%. (Each processor has an idle thread that consumes cycles when no other threads are ready to run.) It can be viewed as the percentage of the sample interval spent doing useful work. This counter displays the average percentage of busy time observed during the sample interval. This percentage is calculated by monitoring the time the service was inactive, and then subtracting that value from 100%.

Total CPU Threshold Configuration

Total Server CPU Thresholds

% Total CPU Utilization: 2%

Manually Refreshed @ Tuesday, September 03, 2002 5:09:42 PM

Setting Thresholds: Click on threshold indicator with mouse and drag to the desired threshold value and save to set it.

Warning Critical Disabled (below 5%)

Save Thresholds

Manually Refreshed @ Tuesday, September 03, 2002 5:09:40 PM

Page File Thresholds

Paging File Usage Percent (Thresholds Supported)—The percentage of the Page File instance in use. A lower percentage is better.

The screenshot displays the 'Page File Threshold Configuration' window. On the left is a navigation pane with links for 'SNMP Configuration', 'Snm Agent', 'Security', 'Trap', 'Management Agents', 'CPU Thresholds', 'Pagefile Thresholds', and 'Cache Thresholds'. The 'Pagefile Thresholds' link is selected. The main content area is titled 'Page File Threshold Configuration' and features a blue header bar with a green checkmark and the text 'Server Page File Thresholds'. Below this, a progress bar shows '% Total PageFile Usage: 3%' with a yellow warning icon at 31 and a red critical icon at 76. A timestamp reads 'Manually Refreshed @ Tuesday, September 03, 2002 5:10:06 PM'. A 'Setting Thresholds' section explains that users can click and drag threshold indicators. Three indicators are shown: 'Warning' (yellow triangle), 'Critical' (red inverted triangle), and 'Disabled(below 5%)' (grey inverted triangle). A 'Save Thresholds' button is located at the bottom. A second timestamp at the bottom left reads 'Manually Refreshed @ Tuesday, September 03, 2002 5:09:40 PM'.

Cache Hits Thresholds

Copy Read Hits Percent (Thresholds Supported)—The percentage of cache copy read requests that hit the cache, that is, they did not require a disk read to provide access to the page in the cache. A copy read is a file-read operation that is satisfied by a memory copy from a page in the cache to the buffer of the application.

NOTE: The higher the value, the better the performance. Threshold limits must be set accordingly.

SNMP Configuration

With the use of group configuration, administrators are now able to quickly change the SNMP configuration settings on multiple devices with a single operation, utilizing HP Systems Insight Manager. To learn more about creating an SNMP Group Configuration Control Task, refer to the *HP Systems Insight Manager Technical Reference Guide*. The following example details how to set the service on a single device.

SNMP Agent Configuration

The SNMP Agent Configuration screen is used to view and set the SNMP (Win32 Service) Agent configuration.

The SNMP Agent screen enables setting the contact, location and service type for the SNMP service.

If you change the SNMP Agent configuration, you must click **Apply** to send the configuration request to the server. If the server is running Windows NT 4.0, the SNMP service settings do not take effect until you click **Restart Agents**.

- Contact—displays the contact person responsible for the SNMP management of the server
- Location—displays the location of the server
- Service—displays the service type for the server

Wait until you have completed changing all of the settings before clicking **Restart Agents**. You cannot refresh the page or make other changes while the restart is occurring. After you click **Restart Agents**, refresh the page to view the updated information.

SNMP Security Configuration

The SNMP Security Configuration screen is used to view and set the SNMP (Win32 Service) Security configuration.

The SNMP Agent screen allows setting the SNMP Community String, Accepted Host List, and Send Authentication Trap settings for the SNMP service.

The security rights for an accepted community name are NONE, NOTIFY, READ_ONLY, READ_WRITE, and READ_CREATE.

The accepted host list is the host names or IP addresses of the machines from which the server is allowed to accept SNMP requests.

NOTE: The accepted host list always has “127.0.0.1” listed by default so that SNMP and the Web Agent service function correctly.

You can disable or enable the Send Authentication Trap flag.

You can add, edit, or remove security configurations. After the changes have been made on the browser, you must click **Apply**.

If the server is running Windows NT 4.0, the SNMP security settings do not take effect until you click **Restart Agents**. Wait until you have completed changing all of the settings (Agent, Security, Traps) before clicking **Restart Agents**. You cannot refresh the page or make other changes while the restart is occurring. After you click **Restart Agents**, refresh the page to view the updated information.

SNMP Trap Configuration

The SNMP Trap Configuration screen is used to set the SNMP (Win32 Service) Trap community names and destinations.

The trap destination hosts are a semicolon-delimited list of servers where the traps for a specific community name are sent. To enable your ProLiant server to send alerts to HP Systems Insight Manager and other management applications, you must configure the appropriate trap destinations. Trap destinations can be input as an IP address, and IPX address, or a host name.

You can add, edit, or remove trap destinations. After the changes have been made on the browser, you must click **Apply**.

If the server is running Windows NT 4.0, the SNMP trap settings do not take effect until you click **Restart Agents**. Wait until you have completed changing all of the settings (Agent, Security, Traps) before clicking **Restart Agents**. You cannot refresh the page or make other changes while the restart is occurring. After you click **Restart Agents**, refresh the page to view the updated information.

HP Insight Management Agents Configuration

The HP Insight Management Agents Configuration screen is used to view and set the HP Insight Management Agents configuration.

It allows settings for Server Role, Data Collection Interval, SNMP Sets, and Remote Reboot settings.

If you make Management Agents Configuration changes, you must click **Restart Agents** for changes to the HP Insight Management Agents (Server Agents, Foundation Agents, Storage Agents, and NIC Agents) settings to take effect on the server.

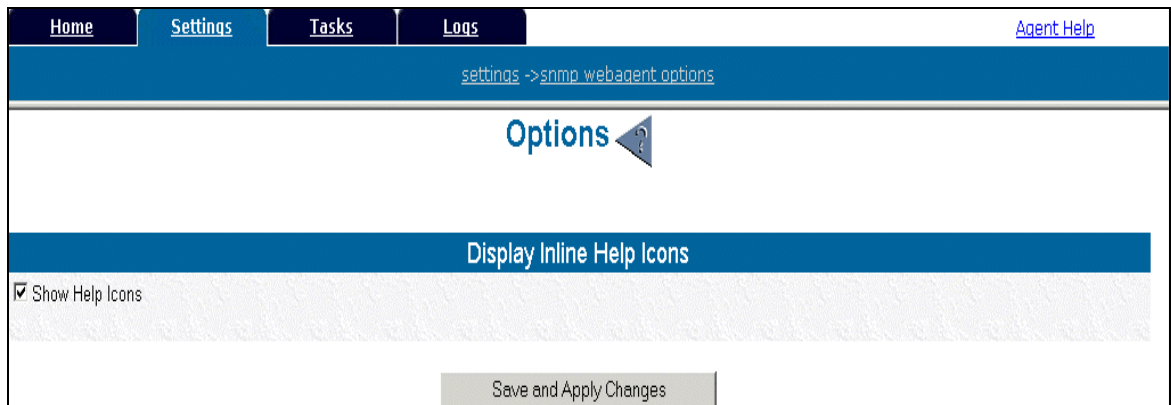
- **Server Role**—Displays the description of the system's role or function. You can also set the Server Role text on multiple devices by creating a Group Configuration Task in HP Systems Insight Manager. To learn more about how to set the server role refer to the *HP Systems Insight Manager Technical Reference Guide*.
- **Data Collection Interval**—Displays the time interval that the HP Insight Management Agents collect the data from the server.
- **SNMP Sets**—Displays whether or not the SNMP Sets are enabled. When it is disabled, sets are not allowed by anyone.
- **Remote Reboots**—Displays whether or not remote reboot of the server is allowed.

Wait until you have completed changing all of the settings before clicking **Restart Agents**. You cannot refresh the page or make other changes while the restart is occurring. After you click **Restart Agents**, refresh the page to view the updated information.

Options

Display Inline Help Icons

The Display Inline Help icons allow you the option of choosing to display the help icon or not. If you choose to make a change to the default of displaying the help icon, clear **Show Help Icons**, and then click **Save and Apply Changes**.



Foundation Agent Information

Management Host Agent

The Management Host agent gathers data for the HP Host OS MIB. This data includes:

- Server/host name and OS version number
- CPU utilization information (for each CPU) over 1-minute, 5-minute, 30-minute, and 60-minute intervals
- File system information (for each mounted file system)
- Software version information

Running the Host Agent

SCO UnixWare 7 Systems

To run the host agent, add the following line to the Foundation SNMP Multiplexing (SMUX) Manager configuration file `/opt/compaq/foundation/etc/config`:

```
agent = "cmahostd" -p 15 -s OK -t OK;
```

The following command line arguments can be used:

- `-p poll_time`—specifies the number of seconds to wait between data collection intervals (15 seconds in this example). The minimum value allowed is one second. The maximum value allowed is 60 seconds.
- `-s set_state`—specifies whether SNMP set commands are allowed for this agent. A `set_state` of OK (default) means that SNMP set commands are allowed. A `set_state` of NOT_OK means that SNMP set commands are not allowed.
- `-t trap_state`—specifies whether SNMP trap commands are allowed for this agent. A `trap_state` of OK (default) means that SNMP trap commands are allowed. A `trap_state` of NOT_OK means that SNMP trap commands are not allowed.

The host agent is automatically started at Foundation SMUX Manager startup and automatically stopped at Foundation SMUX Manager shutdown. Refer to `/opt/compaq/foundation/etc/registry.mib` for a complete list of supported MIB items.

NetWare Systems

Support for Desktop Intelligent Manageability is designed to provide a list of desktop PCs that have logged onto the server running CPQHOST. CPQAGIN should be used to set up the server to run CPQHOST and support Desktop Management. CPQAGIN will edit the system login script to include the execution of a discovery program (CPQCLNT.EXE). If the desktop logging into the server supports Desktop Management, the discovery program will write the desktop's system name, IP and/or IPX address, as well as other information to SYS:CPQDATA. CPQHOST then polls SYS:CPQDATA, reads any information from logged-in desktops, and adds that information to the list of logged-in desktops. Only desktops that support HP Desktop Management will appear in the list supported by CPQHOST and Insight Manager.

Configuring Client Data Collection

To set up the system to collect client data:

1. Load the Desktop Management Support files.
 - If you have selected Desktop Management during SmartStart setup or you have installed Management Agents for Servers version 2.60 or higher, the Desktop Management Support files have already been copied to your system. At the system console prompt, enter:

```
LOAD CPQAGIN
```

- If you have not installed Management Agents for Servers version 2.60 or greater, insert the Management CD into your CD-ROM drive. At the system console prompt, enter:

```
LOAD [CD DRIVE] : \AGENTS\NETWARE\ENG\COMPAQ\ CPQAGIN
```

At the opening menu, select **Copy New NetWare Agents to System** and follow the on-screen instructions. Do not exit the installation program.

2. Select **Client Management** from the opening menu and follow the on-screen instructions.
3. To manage a workstation (client) that is logged into a NetWare 4.x/IntranetWare 4.11 environment using a NetWare Directory Services (NDS) connection, add the following three lines to the container login script where the user ID resides:

```
map ins s2:=sys:\public
#cpqclnt.exe \\servername\SYS\PUBLIC
map del s2:
```

After completing these instructions, Client Management will be installed and configured on your system.

Threshold Agent

The Threshold agent is designed to provide support for HP Insight Manager user-defined thresholds. It also provides a generic way to set thresholds on objects in any HP SNMP MIB.

Users can set thresholds on counter or gauge MIB variables. Each selected MIB variable is periodically sampled by the threshold agent at a rate defined by the user.

MIB data values are compared to user-configured thresholds. If a configured threshold is exceeded, an alarm trap is sent to the configured SNMP trap destination and (optionally) to e-mail. User-configured alarm thresholds are permanently saved in the data registry until the user deletes them.

For further information about setting thresholds, refer to the *HP Systems Insight Manager User Guide* help file.

Running the Threshold Agent on a SCO UnixWare 7 System

To run the Threshold Agent, add the following line to the Foundation SMUX Manager configuration file `/opt/compaq/foundation/etc/config`:

```
agent = "cmathreshd" -p 1 -s OK -t OK;
```

The following command line arguments can be used:

- `-p poll_time`—specifies the rate at which the threshold agent checks to see if any MIB items need to be sampled. The suggested value (and the minimum allowed) is 1 second.
- `-s set_state`—specifies whether SNMP set commands are allowed for this agent. A `set_state` of `OK` (default) means that SNMP set commands are allowed. A `set_state` of `NOT_OK` means that SNMP set commands are not allowed.
- `-t trap_state`—specifies whether SNMP trap commands are allowed for this agent. A `trap_state` of `OK` (default) means that SNMP trap commands are allowed. A `trap_state` of `NOT_OK` means that SNMP trap commands are not allowed.

This agent is automatically started at Foundation SMUX Manager startup and automatically stopped at Foundation SMUX Manager shutdown. Refer to `/opt/compaq/foundation/etc/registry.mib` for a complete list of supported MIB items.

The Threshold entries can be removed using the following procedure:

1. Run the Foundation SMUX Manager stop script to stop the Threshold agent by entering:


```
sh /etc/init.d/cmafdtnsmux stop
```
2. Delete the threshold entries from the Threshold data registry file by entering:


```
rm /var/spool/compaq/foundation/registry/threshold/entry.*
```
3. Run the Foundation SMUX Manager start script file to restart the Threshold Agent by entering:


```
sh /etc/init.d/cmafdtnsmux start
```

System

Software Version Information

The Software Version section displays the versions of the system software installed on this machine: BIOS, Drivers, and agents.

This section also displays a string that specifies the version of HP Insight Management Agents running on the system.

Cluster Information

The Cluster Information section displays the overall status of a cluster. It also displays the state of the cluster service running on each node, as well as the worst-case status of the shared resources of each node.

Information about cluster nodes, resource groups, networks, interconnects, and software might appear.

Cluster Nodes

The Cluster Node section contains information about the systems that are members (nodes) of the cluster. This section displays the names of the nodes, status of the cluster service running on the nodes, and the status of the shared resources. Values for cluster service status can be:

- **Up**—The node is operating as an active member of a cluster. A node that is up can respond to updates to the cluster database, can host and manage groups, and can maintain communication with other nodes in the cluster.
- **Paused**—The node is operating as an active member of a cluster but cannot host any resources or resource groups. The node is up but cluster activity is paused. Nodes that are undergoing maintenance are typically placed in this state.
- **Joining**—The node is in the process of joining a cluster. This is a temporary state.
- **Down**—The node is trying to form or rejoin a cluster or is down. A node that is down is not an active cluster member and it might or might not be running. The Cluster Service might have started and then failed or might have failed to start.
- **Unknown**—An error has occurred and the exact state of the node could not be determined, or that the node status is unavailable.

Cluster Resources Groups

The Cluster Resources Groups display the cluster resources by resource group. The following information might appear.

- **Name**—Displays the name of the resource and the color status associated with the resource state.
- **State**—Displays the current state of the resource, which can be one of the following:
 - **Online**—The resource is online and functioning normally.
 - **Offline**—The resource is offline.
 - **Online pending**—The resource is in the process of coming online.
 - **Offline pending**—The resource is in the process of going offline.
 - **Failed**—The resource has failed.
 - **Unknown**—The resource has not responded and the exact state is undetermined.
- **Type**—Displays the resource type, which is acquired from the cluster service.
- **Owner**—Displays the name of the node in the cluster that currently owns this resource.
- **Identification**—Displays information based on the resource type. If the type is Physical Disk, identification displays the drive letter, the physical identification, and the logical drive number. For disks, this is the physical ID entered at the server for this disk or the serial number if nothing was entered. If the type is IP Address, then the IP address appears. Any other resource type displays N/A.

Cluster Networks

The Cluster Network section displays the following information about the networks connected to the cluster nodes:

- **Name**—Displays the name of the network.
- **Role**—Displays how the network is used for communication by the cluster, which can be one of the following:
 - **Internal**—The network is used for internal cluster communication.
 - **Client**—The network is used to connect client systems to the cluster.
 - **Client/Internal**—The network is used to connect client systems and for internal cluster communication.
 - **None**—The network is not used by the cluster for communication.

- State—displays the current state of the network, which can be one of the following:
 - Online—The network is online and functioning normally.
 - Offline—The network is offline.
 - Partitioned—The network is operational, but two or more nodes on the network cannot communicate. Typically, a path-specific problem has occurred.
 - Unavailable—The network is unavailable to the cluster because the role of the network is None.
 - Unknown—The network has not yet responded and the exact state is undetermined.
- Address Mask—Displays the address mask used by the network in the format specified by the transport type.
- Description—Displays the text network description if one was entered.

Cluster Interconnect

The Cluster Interconnect section displays the following information about the adapters used for cluster interconnections:

- Network—Displays the name of the network.
- Address—Displays the address used by the interconnect in the format specified by the transport type.
- Transport—Displays the network transport protocol used by the interconnect.
- Node—Displays the name of the system in which the adapter is installed.
- Physical ID—Displays the physical identification of the interface card including the name, the slot number, and base I/O address, if available.

Cluster Software

The Cluster Software section displays the file name, version number, and description of the HP Insight Management Agents cluster software.

Storage

File System Space Used

Select the **File System Space Used** item from the Mass Storage list to display the name of each volume, the number of megabytes used by that volume out of the total available, the number of megabytes unused by that volume, and the percentage of total space used. If disk space usage thresholds are set for any of the volumes, they are represented by arrows at the top of the disk space usage bar graph.

Disk Space Usage Bar Graph

The bar graph uses a color code to indicate disk space status. The bar is blue if the disk space usage is at or below the warning and critical thresholds, or if no thresholds have been set for the volume. The bar is yellow if the disk space usage is above the warning threshold and below the critical threshold. The bar is red if the disk space usage is above the critical threshold. The unused space on the volume appears in gray.

Disk Space Usage Thresholds

The disk space usage threshold values are displayed inside triangular-shaped indicators above the disk space usage bar graph. A yellow indicator is used for the warning threshold and a red indicator is used for the critical threshold. If the indicator is gray, then a threshold has not been created for this volume, or the threshold has been disabled.

Resetting and Saving Thresholds

If you have security access to create, modify, or delete thresholds, two buttons appear at the end of the page:

- Reset to Original Values
- Save Thresholds

If there is more than one volume, a Synchronize thresholds for all volumes checkbox appears. Select the **Synchronize thresholds for all volumes** checkbox to set all critical thresholds to the highest critical threshold value, and to set all warning thresholds to the highest warning threshold value. If you change one threshold, the same threshold on all of the other volumes automatically changes to the same value.

Select **Reset to Original Values** to return to the original threshold, or the values from the last time the thresholds were saved. This option also clears the Synchronize thresholds for all volumes checkbox so that thresholds can be set individually. Select **Save Thresholds** to save any thresholds that have been modified and delete any disabled thresholds.

Creating Thresholds

1. To create a threshold, select the gray threshold indicator with the left mouse button, holding the button down and dragging the indicator to the right until you reach the appropriate value. The threshold value displayed in the indicator changes as you are dragging.
2. Release the mouse button.
3. Select **Save Threshold** to create the threshold with the displayed value.

Modifying Thresholds

To modify a threshold, select the threshold indicator with the left mouse button, holding the button down and dragging the indicator to the right until you reach the appropriate value. The threshold value displayed in the indicator changes as you drag. Release the mouse button.

NOTE: If the indicator moves below six percent, it changes to gray to indicate that it is disabled. When you save the thresholds, disabled thresholds are deleted. A critical threshold can never go above 99 percent, or lower than a warning threshold plus three percent. Therefore, if the warning threshold is 85 percent, the valid range for the critical threshold is 88 percent to 99 percent. If a warning threshold is 95 percent, the valid range for the warning threshold is six percent to 92 percent.

Deleting Thresholds

- To delete a threshold, select the threshold indicator with the left mouse button, holding the button down and dragging the threshold indicator to the left until the indicator turns gray.
- When you save the thresholds, disabled thresholds are deleted.

NIC Subsystem

ServerNet PCI Adapter

The ServerNet PCI Adapter (SPA) provides a dedicated, redundant, high-performance communication link between clustered Windows NT servers. The following information about the SPA is available in this section.

- Vendor—Displays the vendor.
- Model—Displays the product model.
- Version—Displays the hardware version.
- Status—Displays the overall status. The color of the arrows on the ServerNet icon also indicates the overall status. The following conditions are valid:
 - OK (green)
 - Degraded (yellow)
 - Failed (red)
 - Unknown (blue)
- Time-Out Errors—Displays the number of requests to the SPA that were not acknowledged and cannot be completed.
- X-Port—Displays the status of the X-port of the SPA. The following conditions are valid:
 - OK (green)—Indicates both the X and Y ports are operating normally
 - Degraded (yellow)—Indicates either the X or Y port has degraded or failed
 - Failed (red)—Indicates both the X and Y ports have failed
 - Unknown (blue)—Indicates and unknown condition
- Y-Port—Displays the status of the Y-port of the ServerNet PCI Adapter. The following conditions are valid:
 - OK (green)—Indicates both the X and Y ports are operating normally
 - Degraded (yellow)—Indicates either the X or Y port has degraded or failed
 - Failed (red)—Indicates both the X and Y ports have failed
 - Unknown (blue)—Indicates and unknown condition

Operating System Information

The Performance Monitor Agent provides statistics and enables thresholds to be set for various system performance parameters. Information is available for the following subsystems: System, Server, Processor, Memory, Paging File, Cache, Physical Disk, Logical Disk, Network, TCP, and Processes.

The Performance Monitor Agent is a sub-agent of the Foundation Agent. This agent replaces the previous OS Management Agent (Patrol for Compaq) and the previous threshold settings are not maintained. The agent obtains performance data from the Microsoft OS-supported Windows Management Information (WMI). WMI is installed as part of the OS on Microsoft Windows Server 2003 and Windows 2000. For Microsoft Windows NT 4, WMI must be installed by the user.

NOTE: If the system does not have WMI installed, download and install it from the Microsoft website at <http://www.microsoft.com/downloads/release.asp?ReleaseID=18491>.

The install status of the Performance Monitor Agent is verified from **Start>Settings>Control Panel** under the services section of the HP Insight Management Agents Control Panel applet. If needed, to activate the Performance Monitor Information feature, select **Performance Monitor** from the Inactive Agents section and click **Add**. The Performance Monitor information appears under the Active Agents section.

Disk Monitoring

To enable physical and logical disk monitoring on Windows NT and Windows 2000 systems, run:

```
DISKPERF [-Y[D|V] | -N[D|V]] [\\computername]
```

- -Y sets the system to start all disk performance counters when the system is restarted.
- -YD enables disk performance counters for physical drives, when the system is restarted.
- -YV enables disk performance counters for logical drives or storage volumes when the system is restarted.
- -N sets the system to disable all disk performance counters when the system is restarted.
- -ND disables the disk performance counters for physical drives
- -NV disables the disk performance counters for logical drives.
- \\computername is the name of the computer you want to see or set disk performance counter use.

For Windows 2000, this command turns Disk Performance Monitoring on and off as needed.

For Windows NT 4, Disk Performance Monitoring cannot be turned off after it is turned on.

For Windows Server 2003, Disk Performance Monitoring is on by default and cannot be turned off.

Threshold Alarms

Warning and critical threshold limits can be set for the properties where indicated. Alarms are sent when the performance property value meets the threshold conditions and stays for 15 data collection intervals. The data collection interval is set in the Management Agents Control Panel applet under Windows Control Panel Settings. Alarms are sent to the configured destinations through SNMP and e-mail.

In order to set thresholds, the user must have administrator rights and have read-write or read-create access in the SNMP security settings.

The Alarm Monitoring Time Interval is 15 data collection intervals.

Performance Status Icons

Performance status icons appear next to those performance items with adjustable thresholds (indicated by the UNKNOWN, OK, DEGRADED, or FAILED status icons).

Supported OS Performance Properties

Logical Disks

- Volume—Name of the logical drive for which statistical information is gathered.
- Free Space (MB)—Unallocated space on the disk drive in megabytes. One megabyte equals 1,048,576 bytes.
- Free Space %—Ratio of the free space available on the logical disk unit to the total usable space provided by the selected logical disk drive.
- Queue Length—Average number of both read and write requests that were queued for the selected disk during the sample interval.
- Disk Busy Time % (Thresholds Supported)—Percentage of elapsed time that the selected disk drive is servicing read or write requests.

Memory

- **Available KBytes**—Amount of physical memory available to processes running on the computer. It is calculated by summing space on the Zeroed, Free, and Stand-by memory lists. Free memory is ready for use. Zeroed memory is memory filled with zeros to prevent later processes from seeing data used by a previous process. Standby memory is memory removed from a working set (its physical memory) of a process enroute to disk, but is still available to be recalled. This counter displays the last observed value only; it is not an average.
- **Pages/sec**—Number of pages read from or written to disk to resolve hard page faults. (Hard page faults occur when a process requires code or data that is not in its working set or elsewhere in physical memory, and must be retrieved from disk). This counter was designed as a primary indicator of the faults that cause system-wide delays. It is the sum of Memory: Pages Input/sec and Memory: Pages Output/sec. It is counted in numbers of pages, so it can be compared to other counts of pages, such as Memory: Page Faults/sec, without conversion. It includes pages retrieved to satisfy faults in the file system cache (usually requested by applications) and in non-cached mapped memory files. This counter displays the difference between the values observed in the last two samples, divided by the duration of the sample interval.
- **Pages Input/sec**—Number of pages read from disk to resolve hard page faults. (Hard page faults occur when a process requires code or data that is not in its working set or elsewhere in physical memory, and must be retrieved from disk). This counter was designed as a primary indicator of the faults that cause system-wide delays. It includes pages retrieved to satisfy faults in the file system cache (usually requested by applications) and in non-cached mapped memory files. This counter counts numbers of pages, and can be compared to other counts of pages, such as Memory: Page Faults/sec, without conversion. This counter displays the difference between the values observed in the last two samples, divided by the duration of the sample interval.
- **Pages Output/sec**—Number of pages written to disk to free up space in physical memory. Pages are written back to disk only if they are changed in physical memory, so they are likely to hold data, not code. A high rate of pages output might indicate a memory shortage. Windows NT writes more pages back to disk to free up space when physical memory is in short supply. This counter counts numbers of pages, and can be compared to other counts of pages, without conversion. This counter displays the difference between the values observed in the last two samples, divided by the duration of the sample interval.
- **Page Reads/sec**—Number of times the disk was read to resolve hard page faults. (Hard page faults occur when a process requires code or data that is not in its working set or elsewhere in physical memory, and must be retrieved from disk). This counter was designed as a primary indicator of the kinds of faults that cause system-wide delays. It includes reads to satisfy faults in the file system cache (usually requested by applications) and in non-cached mapped memory files. This counter counts numbers of read operations, without regard to the numbers of pages retrieved by each operation. This counter displays the difference between the values observed in the last two samples, divided by the duration of the sample interval.

- **Page Writes/sec**—Number of times pages were written to disk to free up space in physical memory. Pages are written to disk only if they are changed while in physical memory, so they are likely to hold data, not code. This counter counts write operations, without regard to the number of pages written in each operation. This counter displays the difference between the values observed in the last two samples, divided by the duration of the sample interval.
- **Page Faults/sec**—Overall rate at which the faulted pages are handled by the processor. It is measured in numbers of pages faulted per second. A page fault occurs when a process requires code or data that is not in its working set (its space in physical memory). This counter includes both hard faults (those that require disk access) and soft faults (where the faulted page is found elsewhere in physical memory). Most processors can handle large numbers of soft faults without consequence. However, hard faults can cause significant delays. This counter displays the difference between the values observed in the last two samples, divided by the duration of the sample interval.
- **Cache Bytes**—Sum of the System Cache Resident Bytes, System Driver Resident Bytes, System Code Resident Bytes, and Pool Paged Resident Bytes counters. This counter displays the last observed value only. It is not an average.
- **Cache Faults/sec**—Number of faults that occur when a page sought in the file system cache is not found and must be retrieved from elsewhere in memory (a soft fault) or from disk (a hard fault). The file system cache is an area of physical memory that stores recently used pages of data for applications. Cache activity is a reliable indicator of most application I/O operations. This counter counts the number of faults, without regard for the number of pages faulted in each operation.
- **Pool Nonpaged Bytes**—Number of bytes in the nonpaged pool, an area of system memory (physical memory used by the operating system) for objects that cannot be written to disk, but must remain in physical memory as long as they are allocated. Memory: Pool Nonpaged Bytes is calculated differently than Process: Pool Nonpaged Bytes, so it might not equal Process: Pool Nonpaged Bytes: _Total. This counter displays the last observed value only. It is not an average.
- **Cache Copy Reads/sec**—Frequency of reads from pages of the file system cache that involve a memory copy of the data from the cache to the buffer of the application.
- **Cache Copy Read Hits %**—Percentage of cache copy read requests that hit the cache, that is, they did not require a disk read to provide access to the page in the cache. A copy read is a file read operation that is satisfied by a memory copy from a page in the cache to the buffer of the application.

Network

TCP

- Active Connections—Number of times TCP connections have made a direct transition to the SYN-SENT state from the CLOSED state.
- Established Connections—Number of times TCP connections, which the current state is either ESTABLISHED or CLOSE-WAIT.
- Established Connections—Number of TCP connections for which the current state is either ESTABLISHED or CLOSE-WAIT.
- Segments/sec—Rate at which TCP segments are sent or received using the TCP protocol.
- Segments Retransmitted/sec—Rate at which segments are retransmitted, that is, segments transmitted containing one or more previously transmitted bytes.
- Connection Failures—Number of times TCP connections have made a direct transition to the CLOSED state from the SYN-SENT state or the SYN-RCVD state, and the number of times TCP connections have made a direct transition to the LISTEN state from the SYN-RCVD state.

Controller

- Total Bytes/sec—Rate at which bytes are sent and received on the interface, including framing characters.
- Packets/sec—Rate at which packets are sent and received on the network interface.
- Output Queue Length—Length of the output packet queue (in packets). If this length is longer than 2, delays are being experienced and the bottleneck should be found and eliminated if possible. Since the requests are queued by the Network Driver Interface Specification or NDIS in this implementation, this length is always 0.
- Packet Outbound Errors—Number of outbound packets that could not be transmitted because of errors.
- Packet Receive Errors—Number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
- Current Bandwidth (Mbits/sec)—Estimate of the current bandwidth of the interface in megabits per second. For interfaces that do not vary in bandwidth or for those where no accurate estimation can be made, this value is the nominal bandwidth.
- Bytes Sent/sec—Rate at which bytes are sent on the interface, including framing characters.
- Bytes Received/sec—Rate at which bytes are received on the interface, including framing characters.
- Packets Sent/sec—Rate at which packets are sent on the network interface.
- Packets Received/sec—Rate at which packets are received on the network interface.

Physical Disks

- Volume—Name of the physical drive for which statistical information is gathered.
- Queue Length—Average number of both read and write requests that were queued for the selected disk during the sample interval.
- Disk Busy Time %—Percentage of elapsed time that the selected disk drive is servicing read or writes requests.

Processes

- Process—Name of the task for which statistical information is gathered.
- Threads—Number of threads currently active in this process. An instruction is the basic unit of execution in a processor, and a thread is the object that executes instructions. Every running process has at least one thread.
- Private Bytes—Current number of bytes this process has allocated that cannot be shared with other processes.
- PageFile Bytes—Current number of bytes this process has used in the paging files. Paging files are used to store pages of memory used by the process that are not contained in other files. All processes share paging files and a lack of space in paging files can prevent other processes from allocating memory.
- Working Set—Current number of bytes in the working set of this process. The working set is the set of memory pages touched recently by the threads in the process. If free memory in the computer is above a threshold, pages are left in the working set of a process even if they are not in use. When free memory falls below a threshold, pages are trimmed from working sets. If they are needed they are soft-faulted back into the working set before they leave main memory.
- Page Faults/sec—Rate at which the page faults occur in the executing threads within this process. A page fault occurs when a thread refers to a virtual memory page that is not in its working set in main memory. This does not cause the page to be fetched from disk if it is on the standby list and already in main memory, or if it is in use by another process with whom the page is shared.
- % CPU Time—Percentage of elapsed time that all the threads of this process used the processor to execute instructions. An instruction is the basic unit of execution in a computer, a thread is the object that executes instructions, and a process is the object created when a program is run. Code executed to handle some hardware interrupts and trap conditions are included in this count. On multi-processor machines, the maximum value of the counter is 100% times the number of processors.

- **% Privileged CPU Time**—Percentage of elapsed time that the threads of the process have spent executing code in privileged mode. When a Windows NT system service is called, the service often runs in privileged mode to gain access to system-private data. Such data is protected from access by threads executing in user mode. Calls to the system can be explicit or implicit, such as page faults or interrupts. Unlike some early operating systems, Windows NT uses process boundaries for subsystem protection in addition to the traditional protection of user and privileged modes. These subsystem processes provide additional protection. Therefore, some work done by Windows NT on behalf of your application might appear in other subsystem processes in addition to the privileged time in your process.

Processors

- **CPU**—Name of the processor for which statistical information is gathered.
- **Interrupts/sec**—Average number of hardware interrupts the processor is receiving and servicing in each second, it does not include Deferred Procedure Calls or DPCs, which are counted separately. This value is an indirect indicator of the activity of devices that generate interrupts, such as the system clock, the mouse, disk drivers, data communication lines, network interface cards, and other peripheral devices. These devices normally interrupt the processor when they have completed a task or require attention. Normal thread execution is suspended during interrupts. Most system clocks interrupt the processor every 10 ms, creating a background of interrupt activity. This counter displays the difference between the values observed in the last two samples, divided by the duration of the sample interval.
- **% User CPU Time**—Percentage of non-idle processor time spent in user mode. (User mode is a restricted processing mode designed for applications, environment subsystems, and integral subsystems. The alternative, privileged mode, is designed for OS components and enables direct access to hardware and all memory. The OS switches application threads to privileged mode to access operating system services.) This counter displays the average busy time as a percentage of the sample time.
- **% Privileged CPU Time**—Percentage of non-idle processor time spent in privileged mode. (Privileged mode is a processing mode designed for operating system components and hardware-manipulating drivers. It enables direct access to hardware and all memory. The alternative, user mode, is a restricted processing mode designed for applications, environment subsystems, and integral subsystems. The operating system switches application threads to privileged mode to access operating system services.) **% Privileged CPU Time** includes time servicing interrupts and DPCs. A high rate of privileged time might be attributable to many interrupts generated by a failing device. This counter displays the average busy time as a percentage of the sample time.
- **% DPC Time**—Percentage of time that the processor spent receiving and servicing deferred procedure calls (DPCs) during the sample interval. (DPCs are interrupts that run at a lower priority than standard interrupts). **% DPC Time** is a component of **% Privileged Time** because DPCs are executed in privileged mode. They are counted separately and are not a component of the interrupt counters. This counter displays the average busy time as a percentage of the sample time.

- **% Interrupt Time**—Percentage of time the processor spent receiving and servicing hardware interrupts during the sample interval. This value is an indirect indicator of the activity of devices that generate interrupts, such as the system clock, the mouse, disk drivers, data communication lines, network interface cards, and other peripheral devices. These devices normally interrupt the processor when they have completed a task or require attention. Normal thread execution is suspended during interrupts. Most system clocks interrupt the processor every 10 ms, creating a background of interrupt activity. This counter displays the average busy time as a percentage of the sample time.
- **% CPU Time (Thresholds Supported)**—Percentage of time that the processor is executing a non-idle thread. Designed as a primary indicator of processor activity, this counter is calculated by measuring the time that the processor spends executing the thread of the idle process in each sample interval, and subtracting that value from 100%. (Each processor has an idle thread, that consumes cycles when no other threads are ready to run.) It can be viewed as the percentage of the sample interval spent doing useful work. This counter displays the average percentage of busy time observed during the sample interval. It is calculated by monitoring the time, the service was inactive, and then subtracting that value from 100%.

Server

Server Agents

Installation and Configuration Utility

The Management Agents for Servers Installation is used to install and configure Management Agents for Servers.

Web-Enabled Server Agent

The Web-Enabled Server Management provides Web pages containing management information about servers.

Insight Base System Agent

The Insight Base System Agent is designed to operate on any Industry Standard Architecture (ISA), Extended Industry Standard Architecture (EISA), or Peripheral Component Interface (PCI) server. The agent provides system configuration information to management applications, such as Insight Manager.

The agent uses industry-standard data to build configuration information. If the system hardware does not conform to ISA, EISA, or PCI standard interfaces, information about that system might be incomplete or unobtainable.

The agent uses a text file to convert encoded information about products and adapters installed in a system into a more descriptive format.

Server Health Agent

The Server Health Agent is designed to provide information about the current configuration and status of the health features of HP systems to Insight Manager or other SNMP requesters. The agent notifies users and the management console of any CPU/system fan failures, memory module failures, DC-DC converter failures, or processor cache failures. The Health Agent can perform a graceful shutdown of the operating system under conditions in which any of these critical errors have occurred. The Health Agent monitors the utilization of processors and PCI/EISA system buses.

The supported health features include Automatic Server Recovery (ASR) configuration and status, the critical error log, and the corrected memory log.

You can use sets to update health configuration information. The following list is an example of some of the information that might be updated if the SET capability is enabled:

- ASR Reboot to OS or to Utilities
- Paging enabled and Pager Number
- Action when a degraded thermal condition is detected

Remote Insight Agent

The Remote Insight Agent provides support for the HP Remote Insight board. This agent collects management data, such as configuration and fault information from the Remote Insight board, and sends it at a configurable interval to Insight Manager. This agent provides forwarding of traps using the Remote Insight board. Additionally, this agent supports Insight Manager, which enables the remaining agent data to be retrieved through a Point-to-Point Protocol (PPP) connection with the Remote Insight board.

Novell Console Commands for the Remote Insight Agent

The Remote Insight Agent (CPQRISA.NLM) has several commands that are activated from the NetWare system console. These commands can be used to modify characteristics of the Remote Insight Board without requiring a network or asynchronous connection with Insight Manager.

To display the commands, at the NetWare system prompt, enter:

```
RIB help
```

The following commands are displayed:

- `RIB Battery On`—Turns on the Remote Insight board battery (the default is On), and enables you to access the board while the system is powered off.

NOTE: This command is only applicable to Remote Insight boards that contain batteries.

- `RIB Battery Off`—Turns off the Remote Insight Board battery. This function is particularly useful when the system is powered off for an extended period of time.
NOTE: This command is only applicable to Remote Insight Boards that contain batteries.
- `RIB Alerts On`—Enables the report of alerts to you through the dial-out function. (The default is On.)
- `RIB Alerts Off`—Disables the report of alerts (for example, power off or reboot alert) to you through the dial-out function. This function is particularly useful for preventing dial out during a reboot.
- `RIB Pending Shutdown`—System reset alerts are not sent for the next reboot if scheduled system maintenance is expected and no alerts are desired. After the system reboots, this option is automatically disabled. When disabled, the board will process alerts as configured.
- `RIB Reset`—Forces a reset of the board's processor and firmware.

For more information on the Remote Insight Board, refer to the *HP Remote Insight Lights-Out Edition User Guide* located on the Management CD.

System Health

- `System Up Time`—Elapsed time (in seconds) that the computer has been running since it was last started. This counter displays the difference between the start time and the current time.
- `Total Threads`—Number of threads in the computer at the time of data collection. This count is an instantaneous count, not an average over the time interval. A thread is the basic executable entity that can execute instructions in a processor.
- `Context Switches/sec`—Combined rate at which all processors on the computer are switched from one thread to another. Context switches occur when a running thread voluntarily relinquishes the processor, is pre-empted by a higher priority ready thread, or switches between user mode and privileged (kernel) mode to use an executive or subsystem service. The context switches/sec rate for all threads running on all processors in the computer is measured in numbers of switches. Context switch counters on the system and thread objects display the difference between the values observed in the last two samples, divided by the duration of the sample interval.
- `Processor Queue Length`—Number of threads in the processor queue. There is a single queue for processor time even on computers with multiple processors. Unlike the disk counters, this counter counts ready threads only, not threads that are running. A sustained processor queue of greater than two threads generally indicates processor congestion. This counter displays the last observed value only. It is not an average.
- `Total Processes`—Number of processes in the computer at the time of data collection. This count is an instantaneous count, not an average over the time interval. Each process represents the running of a program.
- `% Registry Usage`—Percentage of the Total Registry Quota Allowed that is currently being used by the system. This counter displays the current percentage value only. It is not an average.

Security

- Access Permission Errors—Number of times opens on behalf of clients has failed with `STATUS_ACCESS_DENIED`. This object can indicate random attempts to access files that are not properly protected.
- Access Granted Errors—Number of times access to files opened successfully were denied. This object can indicate attempts to access files without proper access authorization.
- Server Logon Errors—Number of failed logon attempts to the server. This object can indicate whether the password guessing programs are being used to violate the security on the server.
- Server Sessions Errored-Out—Number of sessions that have been closed because unexpected error conditions or sessions have reached the auto-disconnect timeout and have been disconnected normally.

Server Utilization

- (Network Utilization) Total Bytes/sec—Total bytes per second that a server has sent to and received from the network. This value provides an overall indication of how busy the server is.
- Server Sessions—Number of sessions currently active in the server. This object indicates current server activity.
- Context Block Queue/sec—Rate per second at which the work context blocks must be placed on the FSP queue of the server to await server action.
- % Total PageFile Usage (Thresholds Supported) —Amount in percent of the Page File instance in use. Refer to Process Object: Page File Bytes.

Information Availability to a WMI Consumer

For Windows 2000, the formatted OS performance data is available by registering a Windows WMI provider that supplies the formatted final OS performance data. The data is populated in WMI under the specific classes as follows:

Namespace: root\default

Object Class: CPQ_System_Performance

Sub-classes:

- CPQ_System
 - ContextSwitchRate
 - CpqQueueLength
 - Processes
 - RegistryUsage
 - SystemUpTime
 - TotalThreads
- CPQ_Server
 - AccessPermissionErrors
 - ContextBlockQueueRate
 - GrantedAccessErrors
 - LogonErrors
 - ServerSessions
 - SessionsErroredOut
 - TotalByteRate
- CPQ_Processor
 - CpuTimePercent
 - CpuUserTimePercent
 - InterruptRate
 - PercentDPCTime
 - PercentInterruptTime
 - PrivelegedCpuTimePercent
 - Processor

- CPQ_Memory
 - AvailableKBytes
 - CacheBytes
 - CacheFaultRate
 - PageFaultRate
 - PageInputRate
 - PageOutputRate
 - PageRate
 - PageReadsPersec
 - PageWritesPersec
 - PoolNonpagedBytes
- CPQ_PagingFile
 - PageFileUsagePercent
 - PagingFile
- CPQ_Cache
 - CopyReadHitsPercent
 - CopyReadRate
- CPQ_PhysicalDisk
 - CurrentDiskQueueLength
 - DiskBytesPersec
 - DiskQueueLength
 - DiskReadBytesPersec
 - DiskReadsPersec
 - DiskTimePercent
 - DiskTransfersPersec
 - DiskWriteBytesPersec
 - DiskWritesPersec
 - PhysicalDisk
- CPQ_LogicalDisk
 - DiskQueueLength
 - DiskTimePercent
 - FreeMegabytes
 - FreeSpacePercent

- LogicalDisk
- CPQ_NetworkInterface
 - BytesReceivedPersec
 - BytesSentPersec
 - CurrentBandwidth
 - NetworkInterface
 - OutputQueueLength
 - PacketOutboundErrs
 - PacketRate
 - PacketReceiveErrs
 - PacketsReceivedPersec
 - PacketsSentPersec
 - TotalByteRate
- CPQ_Tcp (CPQ_Tcpv4 for Windows Server 2003)
 - ConnectionFailures
 - ConnectionsActive
 - ConnectionsEstablished
 - SegmentsRate
 - SegmentsRetransmitRate
- CPQ_Process
 - CpuTimePercent
 - PageFaultRate
 - PageFileBytes
 - PrivateBytes
 - PrivelegedTimePercent
 - Process
 - ThreadCount
 - WorkingSet

Under Windows Server 2003, the formatted data is also available under the WMI CIMV2 namespace as:

- Namespace: root\CIMv2
- Sub-classes of CIM_StatisticalInformation\Win32_Perf\Win32_PerfFormattedData

Server Agent Information

System

System Board

The following information about the system board displayed might vary depending on the device type.

- **Product Name**—Displays the type of device or client PC.
- **System ROM Version**—Identifies the current system ROM version by date. This information can help you track the configuration of the device or client and can be useful for diagnosing service problems. If your system is an HP computer, other information, such as the Family Code and Type Code is given.
- **Redundant ROM Version**—Identifies the backup system ROM version by date. This field will not show if a Redundant ROM is not available.
- **Remote ROM-based Diagnostics**—Displays the date of the current Remote ROM-based Diagnostics for this device. This field shows N/A if Remote ROM-based Diagnostics are not present.
- **Hours in Service**—Displays the number of hours the operating system has been running on this device since the operating system software was installed.
- **Serial Number**—Displays the serial number of the device or client system board. Use this number for identification and registration purposes. N/A displays if you do not have a device or client that supports the asset management feature. Use the System Configuration Utility (or the appropriate utility for your device or client) to enter a system serial number if one does not display and you have a device that supports the asset management feature.
- **Bus Type**—Identifies the device or client bus type as EISA, EISA/PCI, PCI or PCI-X.
- **Board Rev**—Displays the system board revision number.

CPUs

The following information about each processor in the system is available. This information might vary depending on device type.

- **Processor**—Lists the type of processor and its speed. For devices, the colored ball indicates the status of each processor.
- **Coprocessor**—Displays the type and speed of the coprocessor on the device or client PC, such as 80387 at 33 MHz, or W 3167 at 33 MHz.
- **Slot**—Lists the number of the slot where the processor is installed. Use this information for identification purposes.
- **Slot 0**—Indicates that a CPU or a memory module is connected directly to the system board and not in an expansion board.
- **Socket**—Displays the currently selected processor's socket. Use this information for identification purposes.
- **Cache**—Displays the amount of device or client hardware cache available. For example, Cache L2: 64KB indicates 64 KB of secondary level cache between the processor and system memory.
- **Action**—Indicates what action, if any, should be taken for the currently selected processor. Possible values include No Action Needed and Replace processor.
- **Step**—Displays the revision level of the processor.

NOTE: Contact your HP authorized reseller or Hewlett-Packard Company regarding your ProLiant Servers Pre-Failure Warranty to see if the processor module is under warranty.

Memory

Device memory information is indicated in the following list:

- **Total Memory [KB]**—is the total amount of memory available on the device or client PC, such as 8192 KB.
- **Correctable Memory**—Memory errors are corrected by the Error Correcting Code (ECC) memory subsystem when they occur. The correctable memory field displays the status of the Correctable Memory as one of the following:
 - **Logging**—ECC memory correction is supported and error logging is enabled.
 - **Disabled**—ECC memory correction is supported, but errors are not logged for this device.

When a certain rate of errors is exceeded, the health driver automatically disables logging of these errors and sends an alarm. The errors are corrected, but are no longer logged. Logging is re-enabled when the driver is reloaded or the operating system restarts.

- Not Supported—Logging of correctable memory errors is not available for this device. Either the device does not support ECC memory or the driver is not loaded.
- Unknown—You might need to upgrade the driver software and Server Agents. The Server Agent cannot determine the status of the device.

Memory Subsystem

Memory subsystem information is displayed when you click this hyperlink. If Advanced Memory Protection is configured, the following details are displayed.

Advanced Memory Protection

- AMP Mode Status—Displays status of the Advanced Memory Protection sub-system. The following states are supported:
 - Unknown—The system does not support Advanced Memory Protection or the Management Agent cannot determine the status.
 - Not Protected—The system supports Advanced Memory Protection, but the system is not protected because the user has removed a component or the system is in a degraded state. This is generally used on first generation AMP servers.
 - Protected—The system supports Advanced Memory Protection and is in a protected state. This state is generally used on first generation AMP servers.
 - Degraded—The system supports Advanced Memory Protection but an error has occurred and the system is no longer protected.
 - DIMM ECC—The system is protected by DIMM ECC only.
 - Mirroring—The system supports Advanced Memory Protection and is configured in mirrored mode. The system is currently mirrored and no faults have been detected.
 - Degraded Mirroring—The system supports Advanced Memory Protection and is configured in mirrored mode. However, one or more faults have been detected and the system is no longer mirrored.
 - Online Spare—The system supports Advanced Memory Protection and is configured in online spare mode. The system is currently in online spare mode and no faults have been detected. Online spare uses a DIMM or bank of DIMMs as a redundant memory that can be switched to real-time when DIMM failure occurs.
 - Degraded Online Spare—The system supports Advanced Memory Protection and is configured in online spare mode. However, one or more faults have been detected and the system is using the spare.
 - RAID-XOR—The system supports Advanced Memory Protection and is configured in RAID-XOR mode. The system is currently in RAID-XOR mode and no faults have been detected. RAID-XOR is a memory RAID technique that uses the XOR-ing of bits to create the redundant memory segment.
 - Degraded RAID-XOR—The system supports Advanced Memory Protection and is configured in RAID-XOR mode. However, one or more faults have been detected and the system is using the redundant memory.

- Advanced ECC—The system supports Advanced Memory Protection and is configured in Advanced ECC mode. The system is currently in Advanced ECC mode and no faults have been detected.
- Degrade ECC—The system supports Advanced Memory Protection and is configured in Advanced ECC mode. However, the number of DIMM errors has exceeded the threshold.
- AMP Available Types—displays the options available.
 - RAID-XOR—The system is configured for Advanced Memory Protection using the RAID-XOR engine.
 - Dual Board Mirroring—The system is configured for Mirrored Advanced Memory Protection within a dual memory board configuration. The mirrored memory can be swapped with memory on the same memory board or with memory on the second memory board.
 - Single Board Mirroring—The system is configured for Mirrored Advanced Memory Protection within a single memory board.
 - Advanced ECC—The system is configured for the Advanced ECC type of Advanced Memory Protection.
 - Mirroring—The system is configured for Mirrored Advanced Memory Protection. Newer systems provide mirroring down to the cache line level but mirrored board pairs will still exist so that degraded boards can be hot-plugged while the system is running.
 - Online Spare—The system is configured for Online Spare Advanced Memory Protection.
- AMP Configured Types—displays the currently active type of Advanced Memory Protection based on the types available. The following are supported:
 - Unknown—The Management Agent cannot determine the Advanced Memory Protection fault tolerance. You might need to upgrade your software.
 - None—The system is not configured for Advanced Memory fault tolerance.Additional AMP Configured Types can be found in the AMP Available Types section.
- Board—The slot in which the memory board or cartridge is installed.
- Board Status—This provides the current status of the Advanced Memory Protection memory board or cartridge. The following status values are supported:
 - Unknown—The condition of this memory board or cartridge could not be determined.
 - OK—The memory board or cartridge is operating normally.
 - Advanced EEC—The memory board or cartridge is operating normally and additional Advanced Memory Protection (AMP) information is available. The memory board is operating in Advanced EEC mode.
 - Online Spare—The memory board or cartridge is operating normally and additional Advanced Memory Protection (AMP) information is available. The memory board is operating in Online Spare mode.

- Mirrored—The memory board or cartridge is operating normally and additional Advanced Memory Protection (AMP) is available. The memory board is operating in Mirrored mode.
- Mirrored, Single Bit Error—The AMP has detected a single bit error but is still in Mirrored mode. Select the board number to browse to the Memory Board Details page to determine which module produced the error.
- Memory RAID—The memory board or cartridge is operating normally and additional AMP information is available. The memory board is operating in Memory RAID-XOR mode.
- Memory RAID, Single Bit Error—The AMP has detected a single bit error but is still in Memory RAID mode. Select the board number to browse to the Memory Board Details page to determine which module produced the error.
- DIMM ECC—A memory module has failed on the given memory board. Check the Memory Module page to determine which module has failed.
- Unlock Error—The memory board locking mechanism has failed. Try replacing the board.
- Configuration Error—The memory modules have been populated incorrectly or the member board has been installed in the wrong slot. Refer to the server manual for proper memory configurations.
- Bus Error—The memory bus has a failure.
- Power Error—The memory board failed to power up properly. Try reseating the board.
- Present—This indicates if the memory board is present and seated properly.
- Locked—This indicates if the memory board lock is closed.
- Hot Plug—This indicates if a hot plug operating is valid for the memory board slot. If “YES” is displayed, it indicates that the user can remove a board from a populated slot or insert a board into an empty slot. “NO” indicates that a hot-plug operation is not valid on this slot.

Memory Board Details

This section describes Advanced Memory Protection (AMP) details about the memory modules of a given memory board installed in the system. The following items may be displayed:

- Socket Number—Displays the socket number for the memory module.
- Status—Displays the status of the memory module.

NOTE: It might not always be possible to determine exactly which memory modules or how much of each module is being used by the operating system or for redundancy.

- Unknown—The status cannot be determined or AMP is not available.
- Not Present—The socket is empty.

- Good—The memory module is working properly. It might be in use by the operating system or being used as redundant memory.
- Good, In Use—The memory module is working properly. Some or all of the memory on the module is being used by the operating system.
- Configuration Error—The memory modules have been populated incorrectly. Refer to the server manual for proper memory configurations.
- DIMM ECC Error or Degrade—An error has occurred on the given memory module. It should be replaced as soon as possible.
- Type—Displays the following value depending on the type of memory module selected.
 - Board—The memory module is permanently mounted (not modular) on a system board or memory expansion board.
 - Single width module
 - Double width module
 - SIMM (Single Inline Memory Module)
 - PCMCIA (Personal Computer Memory Card International Association technology memory module)
 - DIMM (Dual Inline Memory Module)
- Size—Displays the size of the memory module.
- Speed—Displays the speed of the memory module.
- Technology—Displays the possible values for the memory module technology field, including:
 - FMP—Fast-Page Mode
 - EDO—Extended Data Out
 - BEDO—Burst Extended Data Out
 - Synchronous—Synchronous DRAM
 - Unknown—The technology cannot be determined or the system does not support AMP.

ROM Microcode Patches

This section on ROM-Microcode Patches displays the following information:

- Patch ID—Displays the number of a particular microcode patch.
- Date—Displays a patch's date of manufacture.
- Family specifies the valid family, model, and step that apply to a patch.
- Model—Displays the model number of a patch.
- Step—Displays the revision level of a patch.

This section displays information about the following I/O devices.

- **Keyboard Type**—Describes the keyboard attached to your monitored system. For example, 101-key Enhanced Keyboard.
- **Video Type**—Describes the type of video in use with the monitored system. For example, EGA or VGA might display here.
- **Auxiliary Input**—Indicates whether the auxiliary input (pointing device or mouse port) is enabled or disabled. If you have an EISA-based machine, use the System Configuration Utility to change this value. If you have an ISA-based machine, use SETUP to change this value.

General I/O Devices

This section displays information about the following I/O devices.

- **Keyboard Type**—Describes the keyboard attached to your monitored system. For example, 101-key Enhanced Keyboard.
- **Video Type**—Describes the type of video in use with the monitored system. For example, EGA or VGA might display here.
- **Auxiliary Input**—Indicates whether the auxiliary input (pointing device or mouse port) is enabled or disabled. If you have an EISA-based machine, use the System Configuration Utility to change this value. If you have an ISA-based machine, use SETUP to change this value.

Diskette Drives

This section lists and describes the device diskette drives.

Serial and Parallel Ports

This section displays the serial ports and the parallel ports that have been enabled for this unit, along with their corresponding I/O addresses.

The industry-standard addresses for parallel ports are as follows:

- Primary Port set to 378h
- Secondary Port set to 3BCh

The industry-standard addresses for serial ports are as follows:

- COM1 set to 3F8h
- COM2 set to 2F8h

These addresses are sometimes changed because of conflicts with another device. Communication ports that have been disabled do not show up in this window.

Universal Serial Bus Port

This section displays the Universal Serial Bus (USB) ports that have been enabled for this unit.

Expansion Boards

This section on expansion boards displays a list of their associated slot numbers. You can also view System Resources that are used by each board. Use the Expansion Boards feature to keep track of boards on the device and which resources are being used.

The Expansion Boards section provides additional information about PCI slots in the system, such as the width and speed of the PCI slot.

Security

The Security section displays each of the following security parameters as either `Enabled` or `Disabled` for the selected device.

- **Power On Password**—Prevents use of the computer until the password is entered.
- **Network Server Mode**—Displays the status of the network server (enabled or disabled).
- **Quick Lock Password**—Disables the keyboard without exiting the application. The keyboard is enabled with a power-on password.
- **Quick Blank**—Blanks the screen without exiting the application. The screen is enabled with a power-on password.
- **Diskette Boot Control**—Prevents startup of the computer from the diskette drives. Some computers use diskette boot control to prevent startup of the computer from all removable media, such as CD-ROMs and LS-120 diskette drives.
- **Serial Port Control**—Prevents the transfer of data through the integrated serial interface (COM ports).
- **Parallel Port Control**—Prevents the transfer of data through the integrated parallel port.
- **USB Port Control**—Prevents the transfer of data through the integrated universal serial bus (USB) port.
- **Floppy Disk Control**—Prevents writing to the diskette drives and allows read-only access.
- **Fixed Disk Control**—The state of the access control for the fixed disk interface embedded on the system board.

Enclosure Information

If your system is a blade server-based system, the navigation frame displays the Enclosure Information link under the Configuration section. The middle Navigation frame is the Enclosure Information window and it displays the detailed information about the enclosure. By clicking each of the links, the user will be able to display the enclosure's detailed information in the data frame.

- **Rack Asset**—Contains information about the rack.
- **Server Enclosure/Server Modulebe27**—Contains information about the server blade.
- **Power Enclosure**—Indicates the condition of the power sub-system for the power chassis, along with the redundancy state and load balance state.

If the enclosure is a Power enclosure then the following items will also be listed at the bottom of the General Information Screen:

- Condition
- Redundant
- Load State
- Input Power Type
- Maximum Power

NOTE: The iLO driver and the Rack Management Dispatch Service must be installed for the Rack Information sub-agent to communicate with the rack infrastructure.

Software Version Information

This section displays the versions of the system software installed on this machine.

System Information

HP Systems Insight Manager automatically collects configuration information for all devices in the Responsible Device List. Filtering subsystems, which enable you to filter your devices on such things as processor type or network operating system, uses this information. The type of information collected during Configuration Data Collection is useful for asset management.

The following system information is displayed in the Responsible Device List. Information varies depending on the device type.

General Information

- Product name—Displays the type of device or client PC.
- Operating system—Displays the type of operating system installed on the device.
- SMBIOS Version—Displays the version of SMBIOS on the device if applicable and available.
- Machine ID (System Board)—Displays the identification number of the machine.
- Type of expansion bus—Identifies the device or client bus type as EISA, EISA/PCI, PCI or PCI-X.

Description Information

- System Name—Displays the name of the device.
- Description—Displays a description of the device, including hardware and software.
- Network Management Up Time—Displays the amount of time since the network management portion of the system was last reinitialized.
- Contact Information—Displays the name of the person to contact about this device.
- Location—Displays the physical location of the device.
- IP Address—Displays the network location of the device.

Asset Control Information

- Serial Number—Displays the serial number of the device or client system board. Use this for identification and registration purposes. N/A displays if you do not have an HP device or client that supports the asset management feature. Use the System Configuration Utility (or the appropriate HP utility for your device or client) to enter a system serial number if one does not display and you have an HP device or client that supports the asset management feature.
- Product ID—Displays the Product ID of the server and is used to uniquely identify a server. Provide the Serial Number and the Product ID when communicating with HP Service for warranty service.
- Asset Tag—Displays a changeable asset control number and is used for identification purposes.
- Board Rev—Displays the system board revision number.
- Monitor Model—Displays the monitor model. Use this item for identification purposes.
- Monitor Serial Number—Displays the serial number for the monitor. Use this number for identification purposes.
- Monitor Manufacture Date—Displays the monitor's date of manufacture.

System Resources

This section on system resources lists the resources in use by the device or client workstation in the following order:

1. **IRQ Numbers**—The Interrupt Request number displays, followed by the slot number of the board that is using this interrupt.
2. **Port Address**—The port address range displays, followed by the slot number of the board that is using this I/O port range.
3. **DMA Channels**—The DMA channel displays, followed by the slot number of the board that is using this channel.
4. **Memory**—The memory range displays, followed by the slot number of the board that is using this memory.

NOTE: A slot number of “system” in the device, or “embedded” in the client workstation, refers to slot zero.

Storage

Mass Storage Subsystem

The Mass Storage Subsystem section displays a list of floppy drives, including drive letter and type.

Processor Utilization

This window displays information about the device’s EISA bus, PCI bus, and system processor utilization. The EISA bus bar graph displays the percentage of total possible utilization for the EISA bus over the specified period of time. Use this graph to determine if the EISA bus is a performance bottleneck.

The PCI bus bar graph displays the percentage of total possible utilization for the PCI bus over a specified period of time. Use this graph to determine if the PCI bus is a performance bottleneck.

The system processor bar graphs display the percentage of total possible system processor utilization over the specified period of time. A bar graph is displayed for every processor installed in the device. Use this graph to determine if the system processor is a performance bottleneck.

NOTE: If the device has not passed the selected interval, or if the feature is not supported, a message displays indicating the feature is not available.

Auto Recovery

This section on Auto Recovery provides Automatic Server Recovery (ASR) configuration information, tells you when the server was last reset, and enables you to modify pager settings. You can modify the Status, ASR Reset Boot Option, Pager Status, Pager Dial String, and Pager Message settings.

The following items display on this window.

General Information

- Status—Displays the status of ASR. The possible values are:
 - Enabled—ASR is enabled for this server.
 - Disabled—ASR is disabled for this server. To change this status, run the System Configuration Utility or perform a Set on this item.
 - Not Available—ASR is not available for this server or your driver is not loaded. ASR is available only on operating systems using the ASR software support provided by HP.
 - Unknown—You might need to upgrade your support software or Server Agents. The Server Agent cannot determine the status.
- Last Reset—Displays how the last server reset was performed. The following values are possible:
 - ASR—The last reset was performed by ASR. Check the Critical Error Log to determine what might have caused ASR.
 - ASR-Cleared—The last reset was performed by ASR. The degraded condition caused by the ASR reset has been cleared. Degraded ASR conditions can be cleared by selecting the Clear ASR button on the Auto Server Recovery window.
 - Manual—The last reset was performed manually.
 - Unknown—You might need to upgrade your driver software or Server Agents. The Server Agent cannot determine the status of the device.

If the last reset was an ASR reset, the ASR condition will be degraded.

- **Timeout**—Displays how many minutes ASR will wait before initiating the recovery process.

ASR depends on the software support to routinely notify the ASR hardware that the server is operating properly.

To change the Timeout setting, use the System Configuration Utility. Specify a prudent period of time for this field before resetting the system and activating the recovery process after a fault occurs. If the timeout period is set too low on a heavily used server, the timeout could occur before the software support has time to service the timer.

- **ASR Hardware Version**—Displays the version of the hardware supporting ASR. Use this information for identification purposes.

Reboot

- **Reset Boot Option**—Displays what the server will boot after an ASR reset occurs. When the recovery process is initiated, ASR will reset the server, test all memory, de-allocate any bad memory blocks, and page you (if modem is present in the server and paging is enabled).
- **ASR Reset Limit**—Displays the number of consecutive times that ASR will attempt recovery.

The ASR feature can restart a server after a critical hardware or software error occurs. ASR will attempt the recovery process a limited number of consecutive times. You cannot change this number. If the server continues to experience hardware or software errors and the number of recovery cycles exceeds this limit, the server will log an error to the Critical Error Log and continue to boot the System Configuration Utilities from the hard drive.

Use the ASR Reset Limit feature in conjunction with the ASR Reset Count feature in the same window. The ASR Reset Count feature displays the number of times that ASR has rebooted the server. If the ASR Reset Count is approaching the reset limit, immediately investigate the server for problems by checking the Critical Error Log and running System Diagnostics.

ASR Reset Count—Displays how many times the ASR feature has rebooted the server. ASR will reboot (or reset) the server a limited number of times. If the ASR Reset Count is incremented:

1. Check the Critical Error Log to determine if a serious problem exists.
2. If you suspect a software problem, consult your operating system documentation.
3. If you suspect a hardware problem, run Diagnostics to determine if a problem exists.

The ASR Reset count is reset to 0 when the system is reset manually.

Pager

- **Pager Status**—Displays the status of the pager.
If a modem is installed in the server and paging is enabled, ASR can send an alarm to a pager when a critical error occurs. The status can be:
 - **Enabled**—Paging will occur.
 - **Disabled**—Paging will not occur.
 - **Unknown**—You might need to upgrade your support software or Server Agents for the Server Agent to be able to determine the status of this pager.
- **Pager Dial String**—Displays the pager dial string that the server will dial when an alarm occurs. If a modem is installed in the server and paging is enabled, ASR will send an alarm to a pager and deliver a pager message.
- **Pager Message**—Displays the pager message sent when an ASR occurs. The pager message is a numeric value of up to seven digits (characters must be 0 through 9) that identifies the server experiencing the hardware or software failure. There is an additional space for a pound sign (#), which many pagers require for ending a sequence. The numbers are chosen to uniquely identify the server so you know which server experienced a problem.
- **Serial Port**—Displays the communication port that is enabled for use with the ASR feature. For example, this port might be Serial Port 1. ASR will use this port to page the system administrator, and the administrator will use this port when dialing into the device. You can set the Serial Port value.

Environment

This section on Environment displays details on the device environment. The following information is available.

System Information

- **Degraded Action**—Enables you to designate what action will be taken when the device environment becomes degraded. The options are:
 - **Continue**—The health or wellness driver will signal the operating system to continue functioning in situations where the temperature is too high or too low. In more serious temperature situations, the device shuts down automatically.
 - **Shut Down**—The health or wellness driver will signal the operating system to shut down in situations where the temperature is too high or too low. In more serious temperature situations, the device shuts down automatically.
 - **Unknown**—You might need to upgrade your driver software or Server Agents if the Server Agents cannot determine the status of the device.

- Temperature—displays the current temperature condition of the system or client PC. This value can be:
 - OK—The temperature is within normal operating range.
 - Degraded—The temperature is above normal for airflow obstructions. Be sure that the cover is on.
 - CAUTION—Do not operate the system with the cover removed. Proper airflow is possible only when the cover is in place and properly secured.
 - Failed—The temperature is outside the normal operating range and could permanently damage the system. The system will automatically shut down to prevent damage to hardware or data loss.
- NOTE:** A Failed condition will not occur in a client PC since the power supply for the client will be cut off in the event the thermal condition reaches a permanently damaging level.
- Unknown—You might need to upgrade your driver software or Server Agents if the Server Agents cannot determine the status of the device. If you are managing a client with an Unknown temperature status, the client might not support thermal detection.
- Fans display an entry for each of the device or system processor fans. The status of each fan can be:
 - OK—The fan is operational.
 - Failed—The fan has failed. The device will shut down automatically to prevent damage to hardware or data loss. Replace the fan.
 - Unknown—You might need to upgrade your driver software or Server Agents if the Server Agents cannot determine the status of this setting.

Power Supply

This section displays information about the power supplies.

The following entries might be displayed:

- Location—Displays the bay where the power supply is located.
- Status—Displays the status of the power supply. The following values are possible:
 - OK—A power supply is installed and operating normally.
 - Failed—A power supply is installed and is no longer operating. Replace the power supply.
 - Not Installed—Nothing is installed in this power supply bay.
 - Unknown—The Server Agent is unable to determine if this storage system power supply bay is occupied.
- Serial Number—Displays the serial number of the power supply. This information can be used for identification purposes.
- Firmware Revision—Displays the firmware revision of the power supply.

- Present—Represents whether the power supply is present in the chassis.
- Used Capacity (%)—Represents the current power supply capacity which is a percentage of its maximum capacity.
- Used Capacity (W)—Represents the power supply capacity in watts.
- Max Capacity—Represents the maximum capacity of the power supply in watts.
- Model—Represents the power supply model name.
- Voltage—Represents the input main voltage of the power supply in volts.
- Redundant—Represents the redundancy state of the power supply. The following values are possible:
 - Redundant
 - Not Redundant
 - Unknown
- Hot Pluggable—Represents if the power supply is capable of being removed and/or inserted while the system is in an operational state. The following values are possible:
 - Hot Plug
 - Not Hot Plug
 - Unknown

Power Converter

The Power Converter section displays information about the power converters. The following entries might be displayed:

- Slot and Socket—Displays the location of the power converter.
- Status—Displays the status of the power converter. The following values are possible:
 - OK—A power converter is installed and operating normally.
 - Degraded—A power converter is installed and is operating in a degraded state. Replace the power converter.
 - Failed—A power converter is installed and is no longer operating. Replace the power converter.
 - Unknown—The Server Agent is unable to determine the status of this power converter.

Remote Communications

This section of Remote communications displays details about the status of the Integrated Remote Console (IRC) and the Rapid Recovery communications configuration.

The following fields display:

- Integrated Remote Console Status—indicates whether the IRC is supported and enabled. Possible values include Not Supported, Unknown, Enabled, and Disabled.
 - If IRC is not present on this device, the field displays “Not Supported.”
 - If IRC cannot determine the status of this setting, the field displays “Unknown.”
 - If IRC is present and enabled, the field displays “Enabled.”
 - If IRC is present but disabled, the field displays “Disabled.”

Three things can cause IRC to be disabled even though you enabled it:

1. The COM port for which IRC is configured does not exist.
2. The COM port for which IRC is configured is a PCI device.
3. The IRQ for which IRC is configured does not match the COM port for which IRC is configured.

Remote PC Communications to System Configuration Utilities

- Network Access—Displays the status of the ASR Network Remote Console feature. The following values might display in this field:
 - Enabled—Remote Console network access is enabled. If the server ASR reboots to System Configuration Utilities (see Reset Boot Option in Automatic Server Recovery Window) or if you reboot to System Configuration Utilities from Insight Manager by pressing the Reboot Button in the Device View Window, then network remote access is enabled. You might access System Configuration Utilities through Remote Console.
 - Disabled—Remote Console network access is not enabled.
 - Unknown—You might need to upgrade your driver software or Server Agents if the Server Agents cannot determine the status of this setting.

- **Dial-In Status**—Displays whether the ASR feature will put the modem into auto-answer mode after an ASR reboot. The following values might display in this field:
 - **Enabled**—Remote Console dial-in access is enabled by putting the modem into auto-answer mode. If the server ASR reboots to System Configuration Utilities (see Reset Boot Option in Automatic Server Recovery Window) or if you reboot to System Configuration Utilities from Insight Manager by pressing the Reboot button in the Device View Window, then modem remote access is enabled. You might access System Configuration Utilities through Remote Console using a modem connection.
 - If you have enabled Dial-Out Status, a dial-out connection will be attempted first. If that connection fails, then dial-in access is enabled. If the dial-out connection is successful, then dial-in is enabled after that connection is terminated.
 - **Disabled**—This feature is not enabled. ASR will not put the modem in auto-answer mode.
 - **Unknown**—You might need to upgrade your driver software or Server Agents if the Server Agents cannot determine the status of this setting.
- **Dial-Out Status**—After the ASR feature has attempted to deliver an alarm by means of the pager, if the Dial Out Status is enabled and a proper Dial-Out String has been provided, ASR will dial a remote PC. When a session is established, the server administrator can use a third-party terminal emulation program to run the System Configuration Utilities to diagnose the problem.

Possible values are:

- **Enabled**—ASR will dial the Dial-Out String and attempt to set up a connection to a remote PC. ASR will attempt the connection five times. If a connection is not established and the Dial-In Status is enabled, ASR will put the modem into auto-answer mode so that the server administrator can dial in.
 - **Disabled**—This feature is not enabled. ASR will not attempt a remote connection. However, if the Dial-In Status is enabled, ASR will put the modem into auto-answer mode so that the server administrators can dial-in.
 - **Unknown**—You might need to upgrade your driver software or Server Agents if the Server Agents cannot determine the status of this setting.
- **Dial-Out String**—After the ASR feature has attempted to deliver an alarm by means of the pager, if the Dial-Out Status is enabled and a proper Dial-Out String is provided in this field, ASR will attempt to dial a remote PC. When a session is established, the system administrator can use a third-party terminal emulation program to run the System Configuration Utilities to diagnose the problem.
 - **Serial Port**— displays the communication port that is enabled for use with the ASR feature. For example, this port might be Serial Port 1. ASR will use this port to page the system administrator, and the administrator will use this port when dialing in to the device.

Tasks

Reboot Server

The Recovery Subsystem option enables you to initiate a reboot from the browser. You will be warned before the system allows you to continue the rebooting process. The following reboot options are available:

- Warm Reboot—Initiates the device's normal boot sequence.
- Reboot to Utilities—Loads System Configuration Utilities.
- Reboot to ROM-Based-Setup—Loads ROM-Based-Setup when rebooting.
- Cold Reboot—Shuts down the system without shutting down the operating system. This option is only available if Insight Manager is communicating directly with a Remote Insight board. This option should only be used if you are unable to gracefully shut down the operating system.

To reboot the device, select a reboot option and click Reboot. A text page displays notifying you that the reboot was successfully requested.

NOTE: The reboot option is not available for all devices.

Logs

Critical Error Log

The Critical Error Log records non-correctable memory errors, as well as catastrophic hardware and software errors that cause a system to fail. This information helps you to identify quickly and correct the problem, minimizing downtime.

This section displays a description of critical errors. The date and time of each error is followed by a brief description of the error. The time shown is rounded to the nearest hour.

If critical errors are marked with an exclamation point (!), indicating corrective action is required, the log condition is degraded. To eliminate the exclamation mark and indicate that an entry has been corrected, select the entries you wish to clear and click the **Correct Marked Entries** button or run System Diagnostics on the device. An asterisk (*) indicates the log entry to which the Last Failure Message applies.

IMPORTANT: Agents must have sets enabled and you must have the correct SNMP Community string to be able to mark entries as corrected.

The following list describes errors that might be logged. If you receive any of these errors, run System Diagnostics on your system or consult your software documentation.

- **Abnormal Program Termination**—A device has detected a fatal software error resulting in a device failure.
- **ASR Base Memory Parity Error**—The system detected a data error in base memory following a reset due to an ASR timeout.
- **ASR Extended Memory Parity Error**—The system detected a data error in extended memory following a reset due to an ASR timeout.
- **ASR Memory Parity Error**—The system ROM was unable to allocate enough memory to create a stack. It was unable to put a message on the screen or continue booting the server.
- **ASR Reset Limit Reached**—The maximum number of system resets has been reached. The System Configuration Utilities will be loaded.
- **ASR Reset Occurred**—No error data is logged.
- **ASR Test Event**—An ASR Test Event was generated by the user through the system utilities. No action is required since the event was user-generated to test the ASR configuration.
- **ASR Timeout NMI**—The server has generated an ASR NMI because the ASR timer has not been refreshed. This generally indicates a driver has not relinquished control of the processor causing a server failure. The resulting ASR NMI was generated to log this event.
- **CPU Internal Corrected Error Threshold Exceeded**—The system has detected that a processor has exceeded the threshold for the number of internal ECC cache errors.
- **CPU Processor Power Module Failed**—The system has detected that a processor's power module has failed.
- **Critical Temperature**—The system's critical temperature has been exceeded and auto shutdown has been initiated.
- **Error Detected On Bootup**—The system detected an error during the Power-On Self-Test.
- **Exception**—The processor has detected a critical exception resulting in a device failure.
- **Fan Failure**—The system or processor fan failed.
- **NMI-Processor Local Error**—The processor experienced a fatal error resulting in a device failure.
- **NMI-Expansion Board Error**—A board on the expansion bus indicated an error condition causing a device failure.
- **NMI-Expansion Bus Arbitration Error**—Memory refresh cycles were delayed, potentially leading to data loss. The error results in a system failure.
- **NMI-Expansion Bus Master Time-out**—A bus master expansion board in the indicated slot did not release the bus after its maximum time resulting in a device failure.

- NMI-Expansion Bus Slave Time-out—A board on the expansion bus delayed a bus cycle beyond the maximum time resulting in a device failure.
- NMI-Failsafe Timer Expiration—The software was unable to reset the system failsafe timer, resulting in a system failure.
- NMI-Processor Address Error 1—A processor internal address parity checking error occurred, resulting in a device failure.
- NMI-Processor Address Error 2—The processor detected an address parity error during an inquire cycle.
- NMI-Processor Cache Parity Error—A data error occurred within the processor cache, resulting in a system failure.
- NMI-Processor Internal Error 1—A processor internal parity error occurred, resulting in a device failure.
- NMI-Processor Internal Error 2—The processor detected an internal parity error or a functional redundancy error.
- NMI-Processor Parity Error—The processor detected a data error resulting in a device failure.
- NMI-Software Generated Interrupt—Software indicated a system error resulting in a system failure.
- NMI-System Concurrency Error—A potential error condition was detected within the Data Flow Manager, resulting in a system failure.
- NMI-Uncorrectable Memory Error—The device experienced an uncorrectable memory parity error resulting in a device failure.
- NMI-Unknown Error Type—The device driver does not recognize this NMI. You might need to upgrade your health driver.
- Processor Failure—The processor failed during the Power-On Self-Test.
- Server Manager Failure—An error occurred in the server interface with the Server Manager.
- UPS A/C Line Failure/Shutdown or Battery Low—The device has initiated a UPS or operating system shutdown, or the battery is almost depleted after an AC line failure.

The Last Failure Message on this window displays the last failure message associated with a critical error.

Correctable Errors

This alarm indicates that a block of memory has failed or is failing and might need to be replaced. This condition is generally non-critical since the memory controller can correct the problem. However, this type of error indicates that a memory component is failing or has failed in the system issuing the alarm. The system continues to correct any errors it can.

Memory errors are corrected by the ECC memory subsystem when they occur. If you notice an increase in these errors, correct the problems as soon as possible. Further degradation of the memory components might occur, and then errors can no longer be correctable.

Power On Messages

The Power On Messages section displays the Power-On messages logged when the device was turned on. Refer to your device documentation for a listing of possible Power-On error messages and their meanings. Click the **Clear Power-On Message** button to clear the Power-On message log. This button is only available if there are messages to clear.

Integrated Management Log

The Integrated Management Log records system events, critical errors, Power-On message errors, and memory errors. The log also records catastrophic hardware and software errors that typically cause a system to fail. This information helps to quickly identify and correct the problem and minimize downtime.

Each event log entry has a status to identify the severity of the event:

- Informational—General information about a system event.
- Repaired—An entry has been repaired. Users must mark entries as repaired.
- Caution—A non-fatal error condition has occurred.
- Critical—A component of the system has failed.

If any events in the log have a condition of Caution, the overall log condition will be marked as degraded. If Critical events exist in the log, the overall log condition will be marked as failed.

To clear a degraded or failed event log, mark the log entry as repaired after you have repaired the condition that caused a log entry to be generated. Perform the following steps:

1. Highlight the log entries in the Integrated Management Log.
2. Click the **Mark Repaired** button. This button is located at the bottom of the Integrated Management Log Section of the Web Browser.

IMPORTANT: Agents must have sets enabled and you must have the correct SNMP Community string to be able to mark log entries as corrected.

IMPORTANT: You must enter the Monitor and Control community strings for this device. The HP Insight Management Agents and HP Systems Insight Manager will use these community strings to communicate with the OS SNMP service. If you elect not to create a Control community string, it will not be possible to perform certain operations, such as clearing the integrated management log or changing agent configuration settings.

The Description column gives a brief description of the error or event. The Update Time column contains the last time this log was updated. The Status column contains the status of the log entry.

Refer to the *Integrated Management Log User Guide* for more information.

Remote Insight Board Event Log

The Event Log section displays the list of events stored in the Remote Insight Board event log. A user with the appropriate authority can clear these events. Each event includes the following information:

- Index—Displays a numeric index for each event.
- Time of Event—Displays the time the event occurred.
- Description—Displays a text description of the event.

Management Processor

Remote Insight

The Remote Insight displays the following information:

General Information

- **Model**—Displays the edition of the Remote Insight in the server.
- **Hardware Version**—Displays the Hardware revision of Remote Insight model on the server.
- **Serial Number**—Displays the Remote Insight serial number.
- **ROM Version**—Displays the Remote Insight firmware version and date.
- **iLO Security Override Switch**—Displays the Integrated Lights-Out security state. The iLO Security Override Switch field is supported only in case of Integrated Lights-Out models.
- **Mouse**—Displays whether the mouse is connected to the Remote Insight Board. The mouse is not supported for Remote Insight Lights-Out models.
- **Keyboard**—Displays whether the keyboard is connected to Remote Insight Board. The Keyboard will not be displayed for Remote Insight Lights-Out models.
- **Interface Status**—Displays the Remote Insight interface status.

Alarm

If your system supports Remote Insight Lights-Out Edition, the following alerts are available:

- **Status**—Indicates if alerts are enabled at the Remote Insight Board. This is a global flag and governs all users. If alerts are disabled, alarms will not be sent.
- **Pending Alarm**—Displays if the alert is unable to determine the state of the Remote Insight Board, or if all alerts have been delivered or if there are alerts pending that still must be sent.

If your system supports the Integrated Lights-Out Management Processor, the following alerts are available:

- **Remote Insight Alerts**—Allow users to enable or disable the alerts by clicking the button provided.
- **Host Alerts**—Allow users to enable or disable the alerts by clicking on the button provided.
- **Pending Alarm**—Displays if the alert is unable to determine the state of the Remote Insight Board, or if all alerts have been delivered or if there are alerts pending that still must be sent

Battery

Battery Status indicates the status of the Remote Insight board battery. When the Remote Insight board battery is enabled and there is a host power failure, the Remote Insight board battery provides a minimum of 30 minutes of operation. This enables the Remote Insight board to send alerts to the users that were specified during configuration.

Battery Condition—Displays the condition of the battery. The following values are possible.

- OK—The battery is charged and functional.
- Failed—The battery must be replaced.
- Disconnected—The battery has been disconnected.

Battery Charge—Displays the percentage of the charge in the Remote Insight board battery.

Power

- Auxiliary Power—Displays whether or not the auxiliary power (External Power Cable and/or Internal Power Cable, which is a 30-pin cable or a 16-pin cable) is connected to the Remote Insight Board.
- Virtual Power Button—Displays whether or not the virtual power button cable is connected to the Remote Insight Board.

NOTE: The Power section is not supported for Integrated Lights-Out management processor.

Modem/COM Port Settings

A series of tables is displayed providing information about any Remote Insight Board modems or communication ports. The first table title will indicate the type of device described like “Internal Modem,” “External Port,” “External Modem,” “External Direct Connect,” or “External Xon Xoff.” The tables might contain the following:

- Model—Displays the model of the communication device.
- Data Settings—Contains the data settings for the communication device including:
 - Alarms—Displays if the Remote Insight firmware will use this communication device to deliver traps.
 - Non-PPP—Displays if non-PPP connections are allowed on this port.
 - Baud Rate—Displays the baud rate to be used on this port.
 - Data Bits—Displays the number of data bits to be used on this port.
 - Stop Bits—Displays the number of stop bits to be used on this port.
 - Parity—Displays the type of parity to be used on this port.

- Pager Settings—Displays pager settings for the communication device.
 - Alarms—Displays if the Remote Insight Board firmware will use this port to deliver pages.
 - Message—Displays the message that will be in the body of the page.
 - Baud Rate—Displays the baud rate to use for pager messages.
 - Data Bits—Displays the number of data bits to use for pager messages.
 - Stop Bits—Displays the number of stop bits to use for pager messages.
 - Parity—Displays the type of parity to use for pager messages.
- Modem Control Strings—Contains the modem control strings for the communication device including:
 - Reset—Displays the string used to reset the modem.
 - Initialize—Displays the string used to initialize the modem.
 - Dial Prefix—Displays the string pre-pended to phone numbers before dialing.

Self Test Results

The Self Test Results section indicates various error-status depending on the Remote Insight model. The following is the list of error-status fields:

- Busmaster I/O Reads
- Memory
- Internal Modem Firmware
- Internal Modem
- External Port
- Keyboard Interface
- Battery Interface
- NVRAM Interface
- NVRAM Write/Read/Verify
- Video SideCard
- PCMCIA
- NIC
- Mouse
- CPLD
- SRAM
- EEPROM
- I2C

Reset Remote Insight

The Reset Remote Insight button is used to reset the Remote Insight Board. After the Remote Insight Board is reset, HP Insight Management Agents will take a minimum of two minutes to reconnect with the Remote Insight depending upon the poll interval.

NOTE: If the Reset button is displayed then this feature is supported by the HP Insight Management Agents for this particular Remote Insight model.

Remote Insight NIC

The NIC section displays the following information about the NIC in the Remote Insight Board. Not all fields are supported by all models of Remote Insight Board and/or NIC.

- Model—Displays the NIC model.
- DNS Name—Displays the fully qualified DNS name assigned to this Remote Insight Board.
- Type—Displays if the NIC is embedded or pcmcia and whether it is Ethernet or token ring.
- IP Address—Displays the IP address for this NIC.
- Subnet Mask—Displays the subnet mask for this NIC.
- Gateway—Displays the default gateway configured for this NIC.
- Status—Displays if this NIC is enabled or disabled.
- Physical Address—Displays the MAC address for this NIC.
- Duplex—Displays if the controller is in half duplex, full duplex or does not support a duplex state.
- Speed—Displays the speed of the NIC.
- Max Packet Size—Displays the maximum packet size of the NIC.
- Transmit/Receive Statistics—Displays the following set of statistics for the NIC:
 - Bytes—Displays the number of bytes transmitted/received.
 - Total Packets—Displays the number of packets transmitted/received.
 - Unicast Packets—Displays the number of unicast packets transmitted/received.
 - Non-Unicast Packets—Displays the number of non-unicast packets transmitted/received.
 - Discarded Packets—Displays the number of packets discarded during transmit/receive.
 - Error Packets—Displays the number of error packets found during transmit/receive.
 - Unknown Protocols—Displays the number of unknown protocol packets received.
 - Queue Length—Displays the number of outstanding packets in the transmit queue.

Storage Agent Information

Mass Storage Subsystem

IDE Controllers

Select an IDE controller entry from the Mass Storage list to display a submenu containing separate entries for IDE Controller Information, IDE ATA disk drives connected to the controller, and IDE ATAPI devices connected to the controller. Device types include disks, DVD/CD-ROM drives, tape drives, processors, scanners, optical drives, WORM drives, and so on. The following items might appear depending on the type of controller:

- IDE Controller Information
- IDE ATAPI Devices
- IDE ATA Disk Drives
- IDE ATA Logical Drives

IDE Controller Information

Select a controller entry from the Mass Storage list to display the following information:

Model—Displays the controller's model string, used for identification purposes.

Slot—Displays the physical slot number where the controller is installed in the system or N/A if slot number is not available.

Firmware Version—Displays the firmware version of the controller.

IDE ATAPI Devices

The information displayed for each IDE ATAPI device entry in the submenu includes condition graphic and device location: Primary or Secondary channel, Master device 0 or Slave device 1. If the Storage Agents cannot determine the channel then Channel unknown will be displayed. If the device position cannot be determined then Device unknown will be displayed. You might need to upgrade your driver software or the Storage Agents. Select any of the devices from the submenu to display more information about the devices. The following information is displayed for all devices:

Device Type—Identifies the type of ATAPI device. The following values are valid:

- Disk—A direct-access device, such as a disk drive.
- Removable Media Disk—A removable media device, such as a floppy disk drive.
- Tape—A sequential-access device, such as a tape drive.
- Printer—A printer device.
- Processor—An operating device, such as a central processing unit or ProLiant Storage System.
- WORM drive—A write-once, read-many times device.
- DVD/CD-ROM—A DVD-ROM or CD-ROM device. It can be a read-only device or a read-write device.
- PD-CD Drive—A combination CD-ROM drive and removable media read-write drive.
- Scanner—A scanning device.
- Optical—An optical memory or storage device.
- Jukebox—A media-changer device, such as a tape or CD library.
- Communications Device—A communications device, such as a LAN bridge.
- Unknown—The Storage Agents could not determine the device type. You might need to upgrade your support software or Storage Agents.

Model—Displays the model of the device.

Firmware Revision—Displays the firmware version of the device.

IDE ATA Disk Drives

The information displayed for each IDE ATA disk drive entry in the submenu includes condition graphic and disk drive location: Primary or Secondary channel, Master device 0 or Slave device 1. If the Storage Agents cannot determine the channel then Channel unknown will be displayed. If the device position cannot be determined then Device unknown will be displayed. You might need to upgrade your driver software or the Storage Agents. Select any of the disk drives from the submenu to display more information about the disk drives. The following information is displayed for all disk drives:

Model—Displays the model of the disk drive.

Status—displays the current status of the disk drive. The following values are valid:

- **OK**—The disk drive is operating normally.
- **S.M.A.R.T. Error**—The S.M.A.R.T. predictive failure monitoring predicts imminent failure of this disk drive. Schedule replacement before actual failure occurs.
- **Failed**—The disk drive has failed and must be replaced.
- **Unknown**—The Storage Agents cannot determine the status of the disk drive. You might need to upgrade your driver software or Storage Agents.

S.M.A.R.T. Support—Indicates whether S.M.A.R.T. support is available for this disk drive. The following values are valid:

- **Available**—This drive supports predictive failure monitoring.
- **Not Available**—This drive does not support predictive failure monitoring.
- **Unknown**—The Storage Agents cannot determine if the drive supports predictive failure monitoring. You might need to upgrade your driver or Storage Agents.

Serial Number—Displays the serial number of the disk drive.

Firmware Revision—Displays the firmware version of the disk drive.

Capacity (MB)—Displays the capacity of the drive in megabytes. For example, 210 identifies a 210-megabyte drive. A megabyte is defined as 1,048,576 bytes. The capacity value shown might differ from the stated size of the drive due to different definitions of a megabyte. Many hardware manufacturers use the value of 1,000,000 for megabyte instead of 1,048,576.

Transfer Mode—Displays the data transfer mode of the disk drive. The following values are valid:

- PIO Mode 0—The data transfer mode is programmed input/output mode 0.
- PIO Mode 1—The data transfer mode is programmed input/output mode 1.
- PIO Mode 2—The data transfer mode is programmed input/output mode 2.
- PIO Mode 3—The data transfer mode is programmed input/output mode 3.
- PIO Mode 4—The data transfer mode is programmed input/output mode 4.
- DMA Mode 0—The data transfer mode is direct memory access mode 0.
- DMA Mode 1—The data transfer mode is direct memory access mode 1.
- DMA Mode 2—The data transfer mode is direct memory access mode 2.
- Ultra DMA Mode 0—The data transfer mode is ultra direct memory access mode 0.
- Ultra DMA Mode 1—The data transfer mode is ultra direct memory access mode 1.
- Ultra DMA Mode 2—The data transfer mode is ultra direct memory access mode 2.
- Ultra DMA Mode 3—The data transfer mode is ultra direct memory access mode 3.
- Ultra DMA Mode 4—The data transfer mode is ultra direct memory access mode 4.
- Ultra DMA Mode 5—The data transfer mode is ultra direct memory access mode 5.
- Unknown—The Storage Agents cannot determine the disk drive data transfer mode.

Logical Drives

This is a list of logical drives that includes this physical drive as a member. Select one of the listed logical drives to see more information about the drive.

IDE ATA Logical Drives

A list of logical drives associated with the controller displays in the Mass Storage submenu. Each logical drive in the list displays the condition, logical drive number and the fault tolerance of that logical drive. Select one of the logical drive entries to display the following information.

Status—Displays the status of the logical drive. The logical drive can be in one of the following states:

- **OK**—Indicates that the logical drive is in normal operation mode.
- **Degraded**—Indicates that at least one physical drive has failed, but the logical drive's RAID level lets the drive continue to operate with no data loss.
- **Rebuilding**—Indicates that the logical drive is rebuilding a physical drive. When complete, the logical drive will return to normal operation.
- **Failed**—Indicates that more physical drives have failed than the RAID level of the logical drive can handle without data loss.
- **Unknown**—The agent cannot determine the logical drive status. You might need to upgrade your software.

Fault Tolerance—Displays the fault tolerance mode of the logical drive. The following values are valid:

- **RAID 0**—Fault tolerance is not enabled. You will experience data loss for that logical drive if one physical drive fails.
- **RAID 1**—Drive mirroring is the highest level of fault tolerance. It is the only method offering fault tolerance protection if no more than two physical drives are selected. Drive mirroring creates fault tolerance by storing duplicate data on two drives. This is the most costly fault tolerance method because it requires 50 percent of the drive capacity to store the redundant data. If a physical drive fails, the mirror drive provides a backup copy of the files and normal system operations are not interrupted.
- **RAID 0+1**—Drive mirroring is the highest level of fault tolerance. There must be four drives for RAID 0+1. This is the most costly fault tolerance method because it requires 50 percent of the drive capacity to store the redundant data. If a physical drive fails, the mirror drive provides a backup copy of the files and normal system operations are not interrupted. This mirroring feature can withstand multiple simultaneous drive failures as long as the failed drives are not mirrored to each other.
- **Unknown**—The agent cannot determine the RAID level of this logical drive. You might need to upgrade your software.

Capacity—Displays the size of the logical drive in megabytes. For example, 120 indicates that the logical drive is 120 megabytes. Use this data to determine whether the drive will be large enough to accommodate your needs.

The capacity utility defines a megabyte as 1,048,576 bytes. The capacity value shown might differ from the stated size of the drive due to different definitions of a megabyte. Many hardware manufacturers use the value of 1,000,000 for megabyte instead of 1,048,576.

Stripe Size—Displays the size of a logical drive stripe in kilobytes.

Disk Rebuilding—Identifies the physical drive that is being rebuilt. The identity of the physical drive will only be displayed when the status of the logical drive is Rebuilding, otherwise, N/A will be displayed.

Physical Drives

This is a list of physical drives that make up the logical drive. Select one of the listed physical drives to see more information about the drive.

Spare Drives

This is a list of physical drives that can be used to replace a failed physical drive if the fault tolerance mode is RAID 1 or RAID 0+1. Select one of the listed spare drives to see more information about the drive.

SCSI Controllers

Select a SCSI controller entry from the Mass Storage list to display a submenu containing separate entries for Controller Information, SCSI devices connected to the controller, and Storage System information. Device types include disks, DVD/CD-ROM drives, tape drives, processors, tape libraries, CD libraries, scanners, optical drives, WORM drives, and so on. The following items might be displayed depending on the type of controller:

- Controller Information
- SCSI Device Information
- SCSI Bus Information
- SCSI Physical Drives
- Tape Library
- Tape Devices
- CD Storage System
- Storage Systems

Controller Information

Select a controller entry from the Mass Storage list to display the following information:

Model—Displays the controller's model ID, used for identification purposes. The following values are valid:

- Compaq 32-Bit Fast-SCSI-2 Controller
- Compaq Systempro/XL Integrated SCSI-2 Port
- Compaq Integrated Fast SCSI-2/P Controller
- Compaq 32-Bit Fast-Wide SCSI-2/E Controller
- Compaq 32-Bit Fast-Wide SCSI-2/P Controller
- Compaq Wide-Ultra SCSI Controller
- Compaq Wide-Ultra2 SCSI Controller
- Compaq 64-Bit Dual Channel Wide-Ultra2 SCSI Controller
- Compaq Wide Ultra3 SCSI Adapter
- HP 64-Bit/133MHz PCI-X 2CH Ultra320 HBA
- The StorageWorks Library Adapter
- Third-party SCSI Controller Model
- Unknown—The driver software or storage agents might need to be upgraded, or you have a SCSI controller in the system that the Storage Agents do not recognize.

Status—Displays the current status of the controller. The following values are valid:

- OK—The controller is operating normally.
- Failed—The controller has failed and is no longer operating.
- Unknown—You might need to upgrade your driver software or Storage Agents or the Storage Agents cannot determine the status of the controller.

Serial Number—Displays the serial number of the SCSI controller. This number can be used for identification purposes.

Firmware Version—Displays the SCSI controller's BIOS firmware version number. This information is not available for all SCSI controllers.

Bus Width—Displays the physical width of the data transfer bus of the SCSI controller. The following values are valid:

- Narrow (8 bits)—The controller supports a narrow 8-bit data transfer bus.
- Wide (16 bits)—The controller supports a wide 16-bit data transfer bus.
- Unknown—The agent is unable to determine the physical width of the data transfer bus. You might need to upgrade your software.

Hard Resets—Displays the number of times the SCSI Hardware Interface Driver detected that the SCSI bus has been reset since the driver was loaded.

Hard resets occasionally occur due to device errors. If this value rises dramatically, there might be a problem. Check the SCSI Bus Information for unusually high error counts. A device with a large number of bus errors might be failing and require replacement.

Soft Resets—Displays the number of times the SCSI Hardware Interface Driver has issued a reset command to all devices on a SCSI bus since the driver was loaded. Soft resets occur when the device driver is initializing the SCSI bus for operation or when device errors have left the bus in an ambiguous, non-operational state.

If this value rises dramatically, there might be a problem. Check the SCSI Bus Information for unusually high error counts. If there is a device with a large number of bus errors, it might be failing and require replacement.

Timeouts—Displays the number of times the SCSI Hardware Interface Driver issued a SCSI command but did not receive a reply within a specific amount of time. This count is kept from the time the driver was loaded.

Timeouts might occur when a device fails to process a request because the SCSI bus was busy. However, if this value rises dramatically, there might be a problem. Check to see if non-disk SCSI devices (such as tape drives) reside on the SCSI bus with the drives. Non-disk devices can require the SCSI bus for long periods of time, resulting in timeouts.

SCSI Device Information

The information displayed for each SCSI device entry in the submenu includes condition graphic, location (SCSI ID), and device type. Select any of the physical devices from the submenu to display more information about the device. The following information is a list of device types and the information displayed for all SCSI devices:

Device Type—Identifies the type of SCSI device. The following values are valid:

- **Disk**—A direct-access device, such as a disk drive.
- **Removable Disk**—A removable media device, such as a floppy disk drive.
- **Tape**—A sequential-access device, such as a tape drive.
- **Printer**—A printer device.
- **Processor**—An operating device, such as a central processing unit or ProLiant Storage System.
- **WORM drive**—A write-once, read-many times device.
- **DVD/CD-ROM**—A DVD-ROM or CD-ROM device. It can be a read-only device or read-write device.
- **Power Drive CD-ROM**—A storage device that can read from a CD and write to or read from an optical disk.
- **CR3500 RAID Controller**—A three-channel SCSI RAID controller.

- Scanner—A scanning device.
- Optical—An optical memory or storage device.
- Jukebox—A media-changer device, such as a jukebox.
- Tape Library—A tape library or autoloader device.
- Communications Device—A communications device, such as a LAN bridge.
- Unknown—You might need to upgrade your support software or Storage Agents.

The following items returned by the SCSI inquiry command can be used for identification purposes:

Vendor—Displays the vendor's name for the SCSI device.

Model—Displays a description of the SCSI device model.

Firmware Version—Displays the firmware revision level of the SCSI device.

Tape Library

Select a tape library entry in the SCSI controller submenu to display a list of information and status associated with the selected tape library. The following information is displayed.

Status—Displays the current status of the tape library. The following values are valid:

- OK—Indicates that the library is in normal operation mode. No user action is necessary.
- Degraded—Indicates that the library has degraded in some manner.
- Failed—Indicates that the library has failed and can no longer return data. The library might need to be replaced.
- Offline—Indicates that the Storage Agents can no longer communicate with the library. This could be caused by a cabling problem or the library might be powered off.
- Unknown—The status of the tape library cannot be determined. Ensure the latest drivers and Storage Agents are installed.

Model—Displays the tape library model.

Serial Number—Displays the unit serial number for the library. It can be used for identification purposes.

Firmware Version—Displays the firmware revision level of the tape library as returned by the SCSI inquiry command.

Service Hours—Displays the number of hours in service.

Total Moves—Displays the total number of moves.

Door Status—Displays the tape library door status. The following values are valid:

- Open—Indicates that the tape library door is open.
- Closed—Indicates that the tape library is closed.
- Not supported—Indicates that the tape library does not detect or report door status.
- Unknown—The door status of the tape library cannot be determined. Ensure the latest drivers and Storage Agents are installed.

Temperature—Displays the tape library temperature status. The following values are valid:

- OK—Indicates that the temperature of the library is within normal operating limits.
- Safe Temperature Exceeded—Indicates that the temperature of the library has exceeded the safe operational temperature. The library will continue to operate under this warning.
- Maximum Temperature Exceeded—Indicates that the temperature of the library has exceeded the normal operating limits to the extent that the library might no longer function.
- Not supported—Indicates that the library cannot detect or report the temperature status.
- Unknown—The temperature status of the tape library cannot be determined. Ensure the latest drivers and Storage Agents are installed.

Redundancy—Displays the tape library redundancy status, which denotes the presence of internal redundant components, such as fans, power supplies, etc. The following values are valid:

- Active—Indicates that the library is capable of detecting and reporting redundant components, there are enough redundant units installed, and redundancy is active.
- Capable—Indicates that the library is capable of detecting and reporting redundant components but there are not enough redundant units installed to make redundancy active.
- Not capable—Indicates that the library is capable of detecting and reporting redundant components but there are no components that support redundancy.
- Not supported—Indicates that the library cannot detect or report redundancy status.
- Unknown—The redundancy status of the tape library cannot be determined. Ensure the latest drivers and Storage Agents are installed.

Hot Swap—Displays the tape library hot swap status which denotes the presence of hot swappable internal components, such as drives, fans, power supplies, etc. The following values are valid:

- **Capable**—Indicates that the library is capable of detecting and reporting hot-swappable internal components and has at least one hot-swappable component.
- **Not capable**—Indicates that the library is capable of detecting and reporting hot swappable internal components but there are no hot-swappable components installed.
- **Not supported**—Indicates that the library cannot detect or report hot-swap status.
- **Unknown**—The hot-swap status of the tape library cannot be determined. Ensure the latest drivers and Storage Agents are installed.

Last Known Error—Displays the hexadecimal error status code including text information, if available. Refer to your hardware documentation for more information.

Associated Tape Drives—Displays a list of tape drives associated with the tape storage system.

Tape Devices

Select a tape device entry in the SCSI controller submenu to display a list of information and status associated with the selected tape device. The following information is displayed.

Status—Displays the status of the SCSI Tape drive that you selected. The following values are valid:

- **OK**—Indicates the tape drive is operating normally.
- **Failed**—Indicates the tape drive has failed and might need to be replaced.
- **Offline**—Indicates the tape drive is offline and can no longer return data. No further status is available.
- **Missing—Was OK**—Indicates a tape drive that was located in the system and had a status of OK, which has been removed.
- **Missing—Was Failed**—Indicates a tape drive that was located in the system and had a status of failed has been removed.
- **Missing—Was Offline**—Indicates a tape drive that was located in the system and had a status of offline has been removed.
- **Unknown**—The Storage Agents cannot determine the status of this tape drive. You might need to upgrade your driver software or Storage Agents.

Model—Displays a description of the SCSI tape device model as returned by the SCSI inquiry command. Use this item for identification purposes.


Firmware Version—Displays the firmware revision level of the tape device as returned by the SCSI inquiry command.

Serial Number—Displays the serial number assigned to the tape device. This value is based on the serial number as returned by the SCSI inquiry command, but might have been shortened due to space limitations. Use this item for identification purposes.

NOTE: Not all tape devices support serial numbers.

Placement—Indicates whether the physical drive is in an internal or external storage system. The following values are valid:

- **Internal**—The physical drive is in an internal storage system.
- **External**—The physical drive is in an external storage system.
- **Unknown**—The physical drive is not in a storage system or the Storage Agents cannot determine the drive placement.

—This symbol indicates that the drive is a hot-plug drive.

Library Drive—Indicates whether the tape drive is included in a tape library. The following values are valid:

- **Yes**—The tape drive is included in a tape library.
- **No**—The tape drive is not included in a tape library.
- **Unknown**—The Storage Agents are unable to determine if the tape drive is included in a tape library.

Media Changer Information—Displays the autoloader media changer information. This only displays when the tape device is an autoloader.

- **Model**—Displays a description of the SCSI tape autoloader media changer model as returned by the SCSI inquiry command.
- **Firmware Version**—Displays the firmware revision level of the tape autoloader media changer as returned by the SCSI inquiry command.
- **Serial Number**—Displays the serial number assigned to the tape autoloader media changer. This value is based on the serial number as returned by the SCSI inquiry command.
- **Magazine Size**—Displays the magazine size of the SCSI tape autoloader media changer.

Tape Errors—Displays the number of read and write errors that have been encountered with the currently loaded tape. Over time, a tape device might produce these errors. These errors are usually caused by bad media sections on the drive. If this value rises dramatically, you might need to clean the device.

NOTE: The number of tape errors will be equal to or greater than the combined total for re-reads, re-writes and uncorrectable errors.

Re-reads—Displays the number of read errors corrected through tape drive retries. Over time, all drives produce these errors. If you notice a rapid increase in the value for Recovered Read Errors or Hard Read Errors, a problem might exist with the drive. The value increases every time the physical drive detects and corrects another error. If this value rises dramatically, you might need to clean the device.

Re-writes—Displays the number of write errors corrected through tape drive retries or other drive recovery mechanisms. Over time, all drives produce these errors.

Having a large number of retry corrected errors does not necessarily indicate that the drive is failing. However, as a precaution, replace a drive that has an abnormally high amount of errors when compared to similar drives. If this count increases rapidly, you might need to clean or replace the drive.

Uncorrectable—Displays the number of read errors that could not be recovered by a tape drive's ECC algorithm, retries, or any other recovery mechanism. Over time, a drive might produce these errors. These errors are usually caused by bad media sections on the tape.

Tape Drive Heads Need Cleaning—Indicates the tape heads on the drive must be cleaned. If they must be cleaned, a cleaning tape must be placed in the drive or the autoloader.

NOTE: A value of Not Supported indicates that the tape drive does not support this feature. You might need to upgrade your firmware to the latest revision.

As routine maintenance, the drive heads should be cleaned according to the recommended schedule for your specific drive.

Cleaning Tape Needs Replacement—Indicates the cleaning tape associated with the autoloader is at the end of the tape. If the cleaning tape is at the end of the tape, a new cleaning tape must be placed in the autoloader.

NOTE: A value of "Not Supported" indicates that the tape drive does not support this feature. You might need to upgrade your firmware to the latest revision.

Number of Cleanings Performed—Indicates the number of times that the tape drive has been cleaned. If a tape drive is cleaned too much it can damage the tape heads.

NOTE: A value of Not Supported indicates that the tape drive does not support this feature.

CD Storage System

Select the CD Storage System entry in the SCSI controller submenu to display Library Information and information for CD-ROM drives associated with the storage system.

CD Library Information

Select the Library Information entry from the CD Storage System list to display the following information.

Status—Displays the current fault light status of the CD Library. The following values are valid:

- OK—The library is operating normally.
- Failed—Indicates that the CD library fault light is in a failed state. The fault light is activated for hardware errors (Sense Code 04h) with additional Sense codes—40h-4fh except the parity error. The LED will remain on until it is power cycled.
- Unknown—The state of the library cannot be determined.

Vendor—Displays the vendor name for the CD Library. This item can be used for identification purposes.

Model—Displays the model name of the CD Library. This value can be used for identification purposes.

Serial Number—Displays the serial number of the CD Library. This value can be used for identification purposes.

Firmware Version—Displays the firmware revision of the CD Library.

CD-ROM Drive Information

Select a CD-ROM drive from the CD Storage System list to display the following information:

- Vendor—Displays the vendor name for the CD-ROM drive.
- Model—Displays the model name of the CD-ROM drive.
- Firmware Rev—Displays the firmware revision of the CD-ROM drive.
- LUN—Displays the logical unit number of the CD-ROM drive.

Storage Systems

Select a storage system item from the SCSI controller submenu to display the following information about ProLiant Storage Systems.

Box Type—Displays the type of drive enclosure, or box. The following types of enclosures are possible:

- **External Storage System**—Outside the machine.
- **Internal Storage System**—Inside the machine.
- **Unknown**—The Storage Agents do not recognize the drive enclosure. You might need to upgrade your software.

Vendor—Displays the name of the vendor that produces this drive enclosure or box type. Use this information for identification purposes.

Model—Displays the model of the storage system. Use this information for identification purposes.

Firmware Revision—Displays the firmware revision of the drive enclosure or box. Use this information for identification purposes.

Board Revision—Displays the board revision level of this storage system backplane.

Serial Number—Displays the serial number of the drive enclosure or box. Use this information for identification purposes.

Thermal Status—Displays the temperature status of the drive system. The following values are possible:

- **OK**—The temperature is within normal operating range.
- **Degraded**—The temperature is outside of normal operating range. Be sure the cover is on the ProLiant Storage System.
- **Failed**—The temperature is outside of normal operating range, and could permanently damage the system. Ensure that the fans are spinning and check the room temperature.
- **Unknown**—The Storage Agents do not recognize the thermal status. You might need to upgrade your software.
- **No Temperature**—This server does not support temperature monitoring.

Fan Status—Displays the status of the fan subsystem in the drive enclosure, or box. The following values are possible:

- OK—The fan subsystem is working properly.
- Failed—A fan has failed and there are not enough fans in the fan subsystem to keep the enclosure cool. Check your fan subsystem as soon as possible. Continued operation might cause failure of the drives.
- Degraded—A fan has failed but there are still enough fans in the fan subsystem to keep the enclosure cool.
- Unknown—The Storage Agents do not recognize the status of the fan subsystem. You might need to upgrade your software.
- No Fan—This server does not have a fan.

Backplane Speed—Displays the speed of the storage system backplane. The following values are possible:

- Ultra3—The storage system is capable of Ultra3 speeds.
- Ultra320—The storage system is capable of Ultra320 speeds.
- Unknown—The Storage Agents are unable to determine the storage system backplane speed. You might need to upgrade your software.

Drive Bays—Displays the number of drive bays provided by this storage system. If duplexing hardware is used with the storage system, the drive bay number is less than the number of physical drive bays in the enclosure.

Duplex Option—Displays the duplex option installed in this storage system. The following values are possible:

- Duplex Top—This storage system is the top part of a duplexed unit.
- Duplex Bottom—This storage system is the bottom part of a duplexed unit.
- None—A duplex option is not installed.

Power Supply Status—Displays the status of the Redundant Power supply.

- OK—All component power supplies that make up the redundant power supply are in normal working order.
- Degraded—One of the component power supplies that make up the redundant power supply has failed. The drive system (either a drive subsystem or a power supply for the main unit) continues to operate. However, if the remaining power supply should fail, the drive system will lose all power and data loss could occur. To correct this situation, schedule a time to bring the device down and replace the failed power supply.
- Unknown—The Storage Agents do not recognize the redundant power supply. You might need to upgrade your software.
- No Redundant Power Supply—This ProLiant server does not support a redundant power supply.

SCSI Physical Drives

Select a SCSI physical drive from the SCSI controller submenu to display the following information:

Status—Displays the status of the physical drive selected.

- OK—The physical drive is operating normally.
- Failed—The physical drive has failed and can no longer return data. The drive might need to be replaced.
- Not Configured—The physical drive is not configured. Ensure that all of the drive switches are properly set.
- Bad Cable—A physical drive is not responding. Check the cables connected to the drive.
- Predictive Failure—One of the physical drive thresholds has been exceeded.
- Offline—The physical drive is offline and can no longer return data. No further status is available.
- Missing was OK—A physical drive that was located in the system and had a status of OK has been removed.
- Missing was Failed—A physical drive that was located in the system and had a status of failed has been removed.
- Missing was Predictive Failure—A physical drive that was located in the system and had a status of Predictive Failure has been removed.
- Missing was Offline—A physical drive that was located in the system and had a status of offline has been removed.
- Unknown—The Storage Agents cannot determine the status of this drive. You might need to upgrade your driver software or Storage Agents.

NOTE: OK, Predictive Failure, and Unknown are the only values associated with clients.

Action—Displays the action that is required for this device. The possible values are:

- Replace Drive—Replace this drive.
- Replace S.M.A.R.T. Drive—A S.M.A.R.T. hard drive predicts imminent failure. Schedule replacement before actual failure.
- No Action Required—The drive is operating normally and no action is required.

Capacity—Displays the size of the physical drive in megabytes. A megabyte is 1,048,576 bytes.

Many hardware manufacturers use a megabyte value of 1,000,000 instead of 1,048,576. This might result in discrepancies between the manufacturer's stated size and the size reported by this application.

Model—Displays the model of the SCSI physical drive.

Firmware Version—Displays the firmware revision level of the SCSI physical drive.

Serial Number—Displays the serial number assigned to the physical drive. This value is based on the serial number as returned by the SCSI inquiry command, but might have been shortened due to space limitations. Use this item for identification purposes.

Service Hours—Displays the total number of hours that a physical drive has been operating. If physical drive statistics are being saved across power cycles (check the SCSI Drive Statistics Preserved), then this value has been kept since the physical drive was installed. Otherwise, this value has been kept since the driver was loaded.

S.M.A.R.T. Support—Indicates if S.M.A.R.T. support is available for this SCSI drive. The following values are valid:

- Not Available—Predictive failure monitoring is not available for this drive.
- Available—This drive supports predictive failure monitoring.
- Unknown—The Storage Agents cannot determine if the drive supports predictive failure monitoring. You might need to upgrade your driver or Storage Agents.

Placement—Indicates if the physical drive is in an internal or external storage system. The following values are valid:

- Internal—The physical drive is in an internal storage system.
- External—The physical drive is in an external storage system.
- Unknown—The physical drive is not in a storage system or the Storage Agents cannot determine the drive placement.

↕—This symbol indicates that the drive is a hot-plug drive.

Rotational Speed—Indicates the rotational speed of the drive in revolutions per minute.

Drive Indicators

Select a SCSI physical drive from the SCSI controller submenu to display information on actions to take when a SCSI physical drive is not operating properly.

Use the Predictive Indicators to predict that a drive, which is now operating normally, might need to be replaced. The numerical data associated with these items displays after the item name. For example, “Used Realloc: 122” indicates that there are 122 used reallocation sectors for this drive. The Predictive Indicators are:

- **Used Reallocs**—Displays the number of sectors of the reallocation area that have been used by the physical drive.

Because of the nature of magnetic disks, certain sectors on a drive might have media defects. The reallocation area is part of the drive that the drive manufacturer sets aside to compensate for these defects. The controller writes information addressed from these unusable sectors to available sectors in the reallocation area. If too many sectors have been reallocated, there might be a problem with the drive. The number of reallocation sectors reserved for this purpose is drive-specific, and you must contact the drive vendor for these values.

- **Spinup Time**—Monitors the time it takes for a physical drive to spin up to full speed.

Drives require time to gain momentum and reach operating speed. As cars are tested to go from 0 mph to 60 mph in X number of seconds, drive manufacturers have preset expectations for the time it takes the drive to spin to full speed. Drives that do not meet these expectations might have problems. If this value increases over time, the drive might be having problems spinning up. Replace the drive as a precaution.

The spinup value is shown in tenths of a second. If the drive takes 12 seconds to spin up, the value would be 120. The value might be 0 if you are monitoring a physical drive and you use a warm boot to reset the system. During a warm boot, the drives continue to spin.

- **Timeouts**—Displays the number of times that the SCSI Hardware Interface Driver issued a SCSI command but did not receive a reply within a specific amount of time. The count is kept from the time the driver was loaded. Timeouts might occur when a device fails to process a request because the SCSI bus was busy.

If the count is greater than zero and the drive has failed, complete the following steps to attempt to correct the problem without replacing the drive:

- a. Ensure that all system and storage system cables are intact and seated properly. You might need to replace the cables.
- b. Be sure that the ProLiant Storage System is plugged in and powered on. Be sure the power supply is functioning.
- c. Check the physical proximity of the system to other electrical devices. Since electrical noise might cause a timeout error, check the AC circuit for other electrical devices.
- d. Timeouts can be caused when two or more drives are set to the same SCSI ID. Be sure that the ProLiant and system SCSI IDs do not conflict.

- e. On a ProLiant Storage System, check the SCSI ID cable on the drive tray. If the cable is damaged or incorrectly installed, SCSI Timeouts can occur. Refer to the documentation accompanying the Hot-Plug Drive Tray Service Spare Kit.
- f. Be sure that the system temperature is within specified limits. Be sure that fans are operating and are not blocked.

In some instances, drive failure can cause timeouts. If you continue to receive many of these errors, replace the drive.

Problem Indicator—Use this utility to determine when a drive failure has occurred that might be correctable without replacing the drive. If the drive has failed and the problem indicator is non-zero, place your cursor over the field and press the **F1** key. The context-sensitive Help for the item includes information on correcting the problem.

Failure Indicator—Use this utility to determine the cause of failure for a failed drive. If the drive has failed and this counter is non-zero, replace the drive. If the drive condition is OK and the failure indicator is not zero, the drive might have an intermittent problem and you might have to replace it. There is no other corrective action for this error.

Self-Test Errors—Displays the number of times that a physical drive failed its self-test. The physical drive does a self-test each time the system is turned on. The number of self-test errors is counted from the time shown in the Service Hours item on the SCSI Physical Drive window.

If the self-test error count is not zero and the drive has failed, replace the drive. If this count is non-zero, but the drive has not failed, it could signal an intermittent problem with the drive. If the number of errors increases over time, replace the drive.

Drive Statistics

Select a SCSI physical drive from the SCSI controller submenu to display statistics about a specific SCSI physical drive. You can use the run-time statistics to monitor the health of a specific drive. The following information displays:

Sectors Read—Displays the total number of sectors read from the physical disk drive since the time listed in the Service Hours item in the SCSI Physical Drive section.

Sectors Written—Displays the total number of sectors written to the physical disk drive since the time listed in the Service Hours item in the SCSI Physical Drive section.

NOTE: If sectors read and written are always zero or N/A on Microsoft Windows 2000 you must install Service Pack 2 or higher. You also must enable the logical and physical disk performance counters. Run `DiskPerf.exe -Y` in a command window and then reboot the system.

Hard Read Errors—Displays the number of read errors that could not be recovered by a physical drive's ECC algorithm, retries, or any other recovery mechanism. These errors are counted over the time listed in the Service Hours item in the SCSI Physical Drive section.

Over time, a drive might produce hard read errors. These errors are usually caused by bad media sections on the drive.

Hard Write Errors—Displays the number of write errors that could not be recovered by physical drive retries. These errors are counted over the time listed in the Service Hours item in the SCSI Physical Drive section. Over time, a drive might produce these errors. These errors are usually caused by bad media sections on the drive.

When a hard write error occurs, the physical drive will remap the bad sector. If the physical drive attempt to remap the sector is unsuccessful, NetWare Hot Fix Redirection logic will attempt to remap the sector. Windows NT will hot fix bad sectors on HPFS and NTFS file systems.

Recovered Read Errors—Displays the number of read errors corrected through physical drive retries or other drive recovery mechanisms. Over time, all drives produce these errors. The number of errors is counted over the time shown in the Service Hours item in the SCSI Physical Drive section.

Having a large number of retry corrected errors does not necessarily indicate that the drive is failing. However, as a precaution, you can replace a drive that has an abnormally high amount of errors when compared to similar drives. If the number of errors increases rapidly, you might need to replace the drive.

Recovered Write Errors—Displays the number of write errors corrected through physical drive retries or other drive recovery mechanisms. Over time, all drives produce these errors. The number of errors is counted from the time shown in the Service Hours item in the SCSI Physical Drive section.

Having a large number of retry corrected errors does not necessarily indicate that the drive is failing. However, as a precaution, you might wish to replace a drive that has an abnormally high amount of errors when compared to similar drives. If this count increases rapidly, you might need to replace the drive.

Seek Errors—Displays the number of seek errors that a physical drive detects. A seek error is a seek that failed. The number of errors is counted over the time shown in the Service Hours item in the SCSI Physical Drive section.

Seek errors will occasionally occur over time. Having a large number of seek errors does not necessarily indicate that the drive is failing. However, as a precaution, you might wish to replace a drive that has an abnormally high amount of errors when compared to similar drives. If this count increases rapidly, you might need to replace the drive.

ECC Corr Reads—Displays the number of times the drive used the ECC algorithm to recover data for read requests. The number of errors is counted over the time listed in the Service Hours item in the SCSI Physical Drive section.

ECC-corrected reads occasionally occur over time. Having a large number of ECC-corrected errors does not necessarily indicate that the drive is failing. However, if a particular drive has an abnormally high amount of ECC-corrected reads compared to similar drives, you might replace the drive as a precaution. If this count increases rapidly, you might replace the drive.

SCSI Logical Drives

Select a SCSI logical drive from the SCSI controller submenu to display the following information:

Status shows the status of the physical drive selected.

- **OK**—The logical drive is in normal operation mode. No user action is required.
- **Failed**—There are more failed physical drives than the fault tolerance mode of the logical drive can handle without data loss.
- **Unconfigured**—The logical drive is not configured. Run the logical drive configuration utility to configure the logical drive.
- **Recovering**—The logical drive is using Interim Recovery Mode. In Interim Recovery Mode, at least one physical drive has failed, but the logical drive's fault tolerance mode lets the logical drive continue to operate with no data loss. You should replace the failed drive as soon as possible.
- **Ready for Rebuild**—The logical drive is ready for Automatic Data Recovery. The physical drive that failed has been replaced, but the logical drive is still operating in Interim Recovery Mode.
- **Rebuilding**—The logical drive is currently re-synchronizing the data across the physical drives in the logical drive.
- **Wrong Drive**—The wrong physical drive was replaced after a physical drive failure. You must return the drive incorrectly replaced and replace the failed drive.
- **Bad Connection**—A physical drive is not responding. Check the cables connecting the physical drive.
- **Degraded**—The logical drive is in a degraded state.
- **Disabled**—The logical drive is disabled. The logical drive configuration utility can enable or disable the logical drive.
- **Unknown**—The Storage Agents cannot determine the status of this drive. You might need to upgrade your driver software or Storage Agents.
- **Capacity** displays the size of the logical drive in megabytes. A megabyte is 1,048,576 bytes. Drive manufacturers sometimes use the number 1,000,000 as a megabyte when giving drive capacities so this value might differ from the advertised size of a drive.
- **Fault Tolerance** displays the fault tolerance mode of the logical drive. The possible values are:
 - **None**—(RAID 0) fault tolerance is not enabled. If a physical drive reports an error, the data cannot be recovered.
 - **Mirroring**—(RAID 1/RAID 0+1) is the highest level of fault tolerance. It is the only method offering fault tolerance protection if no more than two physical drives are selected. Drive mirroring creates fault tolerance by storing duplicate data on two drives. There must be an even number of drives. This is the most costly fault tolerance method because it requires 50 percent of the drive capacity to store the redundant data.

- **Data Guarding**—(RAID 4) assures data reliability while using only a small percent of the logical drive storage capacity. A designated, single physical drive contains parity data. If a drive fails, the controller uses the data on the parity drive and the data on the remaining drives to reconstruct data from the failed drive. This allows the system to continue operating with slightly reduced performance until you replace the drive.
- **Distributed Data Guarding**—(RAID 5) stores parity data across all the physical drives in the array and allows more simultaneous read operations and higher performance than data guarding (RAID 4). If a drive fails, the controller uses the parity data and the data on the remaining drives to reconstruct data from the failed drive. The system then continues operating with a slightly reduced performance until you replace the failed drive.
- **Enhanced Mirroring**—(RAID 1E) is used when there are more than two physical disks. Each mirrored stripe is written to a disk and is mirrored to an adjacent disk. If a failure is detected, the data is rebuilt using the data from the mirrored stripes on the other drives.
- **Unknown**—The Storage Agents cannot determine the fault tolerance of this logical drive. You might need to upgrade your driver software or Storage Agents.

Stripe Size—The size of a logical drive stripe or group of data written to a physical drive in kilobytes. It might be zero in some fault-tolerance modes like *None* and *Mirroring*.

Percent Rebuild Complete displays the percent complete of the resynchronization of the data. When the value reaches 100, the rebuilding process is complete. The logical drive continues to operate with slightly reduced performance during the rebuild. This value is only active when the logical drive has a status of *Rebuilding*.

Physical Drives

A list of physical drives that are members of this logical drive. Select one of the listed physical drives to see more information about the drive.

Spare Drives

A list of spare drives that can be used by this logical drive to replace a failed drive. Select one of the listed spare drives to see more information about the drive.

SCSI Bus Information

Select a SCSI device from the SCSI controller submenu to display more information about the device. The following information might appear depending on the type of device:

Parity Errors—Displays the number of parity errors that occurred on the SCSI bus while the bus was processing commands. The error count is kept from the time the SCSI Hardware Interface Driver was loaded.

Parity errors might occasionally occur over time. If this number rises dramatically, and you suspect a problem, complete the following:

1. Check the cabling to ensure that the cables are not damaged and that they are intact and properly shielded from possible RFI.

2. Check to ensure that all required terminating resistors on all devices on the SCSI bus are present.
3. Check to ensure that each device on the SCSI bus has a unique SCSI ID.

Phase Errors—Displays the number of times the SCSI bus entered an invalid operating state while processing commands. The number of errors is counted from the time the SCSI Hardware Interface Driver was loaded.

If you see any phase errors, the device might have a problem. Phase errors can be caused by a device that is not operating correctly. If the phase errors continue to increase, replace the device.

Select Timeouts—Displays the number of times the controller attempted to start communications with a device and received no response from the device. The number of errors is counted from the time the SCSI Hardware Interface Driver was loaded.

The number of select timeouts should always be 0. Any other number of timeouts might indicate a problem with the device. The SCSI controller will attempt to reset the device, but if the value continues to increase, power cycle the device.

A large number for this item does not indicate a problem. It shows that the device does not support certain advanced SCSI commands that the device driver issued.

Message Rejects—Displays the number of times the device rejected a command because the device does not support the specific operation. The number of errors is counted since the SCSI Hardware Interface Driver was loaded.

Physical Width—Displays the actual width of the data transfer bus for this device. The following values are valid:

- **Narrow (8 bits)**—The device supports a narrow 8-bit data transfer bus.
- **Wide (16 bits)**—The device supports a wide 16-bit data transfer bus.
- **Unknown**—The Storage Agents are unable to determine the physical data transfer width for this device.

Current Width—Displays the width of the data transfer bus that was negotiated between the controller and the device. If this value is less than the device physical data bus width, the device will not provide maximum performance. Maximum throughput is achieved when both the SCSI controller and device support a wide 16-bit data bus. The following values are valid:

- **Narrow (8 bits)**—The negotiated data bus transfer width is narrow (8 data bits).
- **Wide (16 bits)**—The negotiated data bus transfer width is wide (16 data bits).
- **Unknown**—The Storage Agents are unable to determine the current data transfer width negotiated for this device.

Current Speed—Displays the current negotiated data transfer speed for this device. The possible values are:

- **Asynchronous**—The negotiated data transfer speed for this device is asynchronous.

- SCSI-1—The negotiated data transfer speed for this device is 5 million transfers per second.
- Fast—The negotiated data transfer speed for this device is 10 million transfers per second.
- Ultra—The negotiated data transfer speed for this device is 20 million transfers per second.
- Ultra2—The negotiated data transfer speed for this device is 40 million transfers per second.
- Ultra3—The negotiated data transfer speed for this device is 80 million transfers per second.
- Ultra320—The negotiated data transfer speed for this device is 160 million transfers per second.
- Unknown—The agent is unable to determine the current negotiated data transfer speed for this device.

NOTE: If the current data transfer width is Narrow (8 bits) then the speed in megabytes per second is equal to the million transfers per second speed. If the current width is Wide (16 bits) then the speed in megabytes per second is twice the million transfers per second speed. For example, if the current speed is Ultra and the width is Wide then the speed would be 40 megabytes per second.

Drive Array Controllers

This section displays general and status information about drive arrays. Select a drive array controller entry from the Mass Storage list to display a submenu containing separate entries for Array Controller Information, Physical Drives, Logical Drives, and Storage System information. The following items display:

- Array controller information
- Array accelerator information
- Physical drive information
- Logical drive information
- Tape storage system information
- Tape drive information
- Storage system information

Array Controller Information

Select an array controller from the Mass Storage list to display information for SMART and SMART-2 Array Controllers.

The SMART Controller is an intelligent 32-bit EISA-based array controller containing up to two Fast SCSI-2 ports, which allow support of up to 14 drives when combined with the ProLiant Storage System. The SMART Controller provides several modes of fault tolerance, including RAID 1, RAID 4, and RAID 5. On-line spares can be used across both SCSI ports.

The SMART-2 Array Controller is the next generation SMART drive array controller. It can be EISA- or PCI-based. Its features include a modular architecture, faster processor, support for fast and wide SCSI drives, and a removable cache daughter card. The SMART-2 Array Controller supports multiple logical volumes on a single set of physical drives (array). Additionally, the SMART-2 Array Controller supports online volume expansion, which allows an existing logical volume to be reconfigured without data loss while the system is online.

The following information displays for each controller:

Model—Displays the type of controller card. The valid types are:

- IDA—Compaq 32-Bit Intelligent Drive Array Controller—The physical drives are located inside the system.
- IDA Expansion—Compaq 32-Bit Intelligent Drive Array Expansion Controller—The physical drives are located in the Array Expansion System that is connected to the system by a cable.
- IDA-2—Compaq Intelligent Drive Array-2 Controller (IDA-2)—The physical drives are located inside the system.
- SMART—The physical drives can be located inside the system or externally using the ProLiant Storage System.
- SMART-2/E—The physical drives can be located inside the system or externally using the ProLiant Storage System.
- SMART-2/P—The physical drives can be located inside the system or externally using the ProLiant Storage System.
- SMART-2SL—The physical drives can be located inside the system or externally using the ProLiant Storage System.
- SMART-2DH—The physical drives can be located inside the system or externally using the ProLiant Storage System.
- SMART-221—The physical drives can be located inside the system or externally using the ProLiant Storage System.
- SMART-3100ES—This controller provides support for three internal Wide-Ultra SCSI-3 storage bays with up to 15 physical drives per bay.
- SMART-3200—The physical drives can be located inside the system or externally using the ProLiant Storage System.
- Smart Array-4200—The physical drives can be located inside the system or externally in a ProLiant Storage System that is connected to the system by a cable.
- Smart Array-4250ES—The physical drives are located inside the system.
- Smart Array 431—The physical drives can be located inside the system or externally in a ProLiant Storage System that is connected to the system by a cable.
- Integrated Smart Array—The physical drives can be located inside the system or externally in a ProLiant Storage System that is connected to the system by a cable.
- Smart Array 5300—The physical drives can be located inside the system or externally in a ProLiant Storage System that is connected to the system by a cable.
- Smart Array 5312—The physical drives can be located inside the system or externally in a ProLiant Storage System that is connected to the system by a cable.
- Smart Array 5i—The physical drives can be located inside the system or externally in a ProLiant Storage System that is connected to the system by a cable.

- Smart Array 532—The physical drives can be located inside the system or externally in a ProLiant Storage System that is connected to the system by a cable.
- Smart Array 6i—The physical drives can be located inside the system or externally in a ProLiant Storage System that is connected to the system by a cable.
- Smart Array 641—The physical drives can be located inside the system or externally in a ProLiant Storage System that is connected to the system by a cable.
- Smart Array 642—The physical drives can be located inside the system or externally in a ProLiant Storage System that is connected to the system by a cable.
- Smart Array 6400—The physical drives can be located inside the system or externally in a ProLiant Storage System that is connected to the system by a cable.
- Smart Array 6400 EM—The physical drives can be located inside the system or externally in a ProLiant Storage System that is connected to the system by a cable.
- RAID LC2—The physical drives are located inside the system.
- Unknown—You might need to upgrade your driver software or Storage Agents. You have a drive array controller in the system that the Storage Agents do not recognize.

Controller Status—Displays the array controller board status. The following values are valid:

- OK—The array controller is operating properly.
- General Failure—The array controller has failed.
- Cable Problem—The array controller has a cable problem. Check all cables to the controller.
- Powered Off—The array controller does not have power. Replace the controller and restore power to the controller's slot.
- Unknown—Indicates that the Storage Agents are unable to determine the status of the controller. You might need to upgrade the Storage Agents.

Current Role—Displays the current role of the array controller for duplexed array controllers. The following values are valid:

- Not Duplexed—This array controller is not duplexed.
- Active—This duplexed array controller is the active controller.
- Backup—This duplexed array controller is the backup controller.
- Unknown—Indicates that the Storage Agents are unable to determine the role of the controller. You might need to upgrade the Storage Agents.

Redundancy Mode—Displays the redundancy type for the controller. The following values are valid:

- **Not Redundant**—This array controller is not in a redundant configuration.
- **Driver Duplexing**—The array controller is using a controller duplexing algorithm implemented exclusively in the operating system driver.
- **Firmware Active/Standby**—The array controller is using an active/standby algorithm implemented in the controller firmware and the operating system driver.
- **Firmware Primary/Secondary**—The array controller is using a primary/secondary algorithm implemented in the controller firmware and the operating system driver.
- **Unknown**—Indicates that the Storage Agents cannot determine the redundancy type for the controller. You might need to upgrade the Storage Agents.

Redundancy Error—Displays the redundancy error for the controller. The following values are valid:

- **No Failure**—No failures have been detected.
- **No Redundant Controller**—No redundant controller is installed.
- **Different Hardware**—The other controller indicates a different hardware model.
- **No Link**—A link to the other controller could not be established.
- **Different Firmware**—The other controller indicates a different firmware version.
- **Different Cache**—The other controller indicates a different cache size.
- **Other Cache Failure**—The other controller indicates a cache failure.
- **No Drives**—This controller cannot see any attached drives, but the other controller can.
- **Other No Drives**—This controller can Refer to the attached drives, but the other controller cannot.
- **Unsupported Drives**—One or more attached drives has been determined to be incapable of properly supporting redundant controller operation.
- **Expand in Progress**—An expand operation is in progress. Redundant operation not supported until the expand operation is complete.
- **Unknown**—Indicates that the Storage Agents are unable to determine the redundancy error for the controller. You might need to upgrade the Storage Agents.

Firmware Version—Lists the firmware version of the array controller. This value can be used to help identify a particular revision of the controller.

Product Revision—Displays the revision of the array controller board. This value can be used to help identify a particular revision of the controller.

Serial Number—Displays the serial number for the array controller. Use this number for identification purposes.

Processor Usage—Displays the total percentage of the processor usage, expressed as a number from 0 to 100 inclusive.

Command Count—Displays the total number of read and write commands processed in this sample. This value is expressed as read and write commands per second.

Command Latency—Displays the average command latency for this sample in units of 1/10,000 of a second.

ADG Enabler Status—Displays the array controller RAID ADG Enabler Module status. The module enables advanced controller features such as Advanced Data Guarding. The following values are valid:

- **Not Supported**—Indicates that the RAID ADG Enabler Module is not supported by this type of controller.
- **Not Present**—Indicates that the RAID ADG Enabler Module is not present or is not accessible.
- **Fully Functional**—Indicates that the RAID ADG Enabler Module is functional and accessible.
- **Bad Signature**—Indicates that the RAID ADG Enabler Module has an incorrect signature.
- **Bad Checksum**—Indicates that the RAID ADG Enabler Module checksum failed.
- **Present—Upgrade Firmware**—Indicates that the RAID ADG Enabler Module is installed, but a firmware upgrade is required to make it fully functional.
- **Unknown**—Indicates that the Storage Agents do not recognize the RAID ADG Enabler Module. You might need to upgrade the Storage Agents.

Daughter Board Type—Displays the type of daughter board installed on the array controller. The following values are valid:

- **Not Supported**—Indicates that the array controller does not support daughter boards or it does not support daughter board identification.
- **Not Present**—Indicates that a daughter board is not installed on the array controller.
- **SCSI**—Indicates that a SCSI daughter board is installed on the array controller.
- **Fibre**—Indicates that a Fibre daughter board is installed on the array controller.
- **Unknown**—Indicates that the daughter board type is not recognized. You might need to upgrade the Storage Agents.

Rebuild Priority—Displays the logical drive rebuild priority of the controller. The following values are valid:

- Low—Indicates the rebuild priority is low.
- Medium—Indicates the rebuild priority is medium.
- High—Indicates the rebuild priority is high.
- Unknown—Indicates that the rebuild priority is not recognized. You might need to upgrade the Storage Agents.

Expand Priority—Displays the logical drive expand priority of the controller. The following values are valid:

- Low—Indicates the expand priority is low.
- Medium—Indicates the expand priority is medium.
- High—Indicates the expand priority is high.
- Unknown—Indicates that the expand priority is not recognized. You might need to upgrade the Storage Agents.

Number of Ports—Displays the number of SCSI ports on the controller. Sometimes port is also referred to as bus or channel. The number of ports does not indicate the number of connectors.

Array Accelerator Information

Select the accelerator item from the Mass Storage submenu to display the following information:

Status—Displays the status of the array accelerator. The following values are valid:

- Enabled—Cache operations are currently configured and enabled for at least one logical drive.
- Temporarily Disabled—Cache operations have been temporarily disabled. Check the Array Accelerator Error Code for the monitored item to determine why the cache operations have been temporarily disabled.
- Permanently Disabled—Cache operations have been permanently disabled. Check the Array Accelerator Error Code for the monitored item to determine why the cache operations have been disabled.
- Unavailable—An Array Accelerator has not been configured.
- Unknown—The Storage Agents cannot determine the status of the Array Accelerator. You might need to upgrade the Storage Agents.

Bad Data—Indicates the possibility of data loss due to a battery problem when the system was powered on. The following values are valid:

- Possible —At power-on, the battery pack was not sufficiently charged. Because the battery pack did not retain sufficient charge when the system resumed power, the Array Accelerator has not retained any data that might have been stored in the cache. If no data was in the cache, no data was lost. Several situations might have caused this condition:
 - If the system was without power for eight days, and the battery pack was on (the battery pack activates only if the system loses power unexpectedly), any data that might have been stored was lost.
 - There might be a problem with the battery pack. Refer to the Battery Status monitored item for more information.
 - The Array Accelerator board has been replaced with a new board that has a discharged battery pack. No data has been lost in this case, and posted reads or writes will automatically be enabled when the battery pack reaches full charge.
- None—No data loss occurred. At power up, the battery pack was properly charged.
- Unknown—The Storage Agents do not recognize the status. You might need to update your software.

Battery Status—Displays the status of the battery pack on the Array Accelerator. The battery pack can recharge only when the system is powered on.

- OK—The battery pack is fully charged.
- Failed—The battery pack is below a sufficient voltage level and has not fully recharged within the maximum 36 hours. Your board should be serviced as soon as possible.
- Recharging—The battery power is less than 75 percent. The array controller is attempting to recharge the battery pack. A battery pack can take 36 hours to fully recharge. After 36 hours, if the battery pack has not recharged, it is considered failed.
- Degraded—The battery pack is still operating, but one of the batteries in the pack has failed to recharge properly. Your board should be serviced as soon as possible.
- Not Present—The battery pack is not present. (Some controllers do not have a battery-backed cache.)
- Unknown—The Storage Agents do not recognize the battery status. You might need to update your software.

Error Code—Displays the status of the cache operations. The following values are valid:

- None—Cache operations are currently configured and enabled for at least one logical drive. No cache errors have occurred.
- Bad Configuration—Cache operations are temporarily disabled. This error could be caused if the Array Accelerator was switched from one controller to another. Schedule maintenance time to ensure that the board has been properly configured for this system.

NOTE: If data from another system was stored on the board, you must reconfigure it. Reconfiguring the board will destroy any stored data.

- Low Battery—Cache operations are temporarily disabled due to insufficient battery power. Check the Battery Status monitored item for more information.

- **Disable Command Issued**—Cache operations are temporarily disabled. This condition should not exist when the system regains power.
- **No Resources**—Cache operations are temporarily disabled. The controller does not have sufficient resources to perform cache operations. For example, when a replaced drive is being rebuilt, there will not be sufficient resources. After the operation requiring the resources has completed, this condition will clear and cache operations will resume.
- **Not Connected**—Cache operations are temporarily disabled. The Array Accelerator has been configured but is not currently attached to the controller. Check the alignment of the board and connections.
- **Bad Mirror Data**—Cache operations have been permanently disabled. The Array Accelerator stores mirrored copies of all data. If data exists in the cache when the system is first powered up, the Array Accelerator performs a data compare test between the mirrored copies. If the data does not match, an error has occurred. Data might have been lost and the board might need servicing.
- **Read Failure**—Cache operations have been permanently disabled. The Array Accelerator stores mirrored copies of all data. While reading the data, memory parity errors occurred so both copies were corrupted and cannot be retrieved. Data has been lost. Have the board serviced.
- **Write Failure**—Cache operations have been permanently disabled. This error occurs when an unsuccessful attempt was made to write data to the Array Accelerator. Data could not be written to write cache memory in duplicate due to the detection of parity errors. This error does not indicate data loss. Have the board serviced.
- **Configuration Changed**—Cache operations have been permanently disabled. The configuration of the logical drives has changed. Reconfigure the Array Accelerator.
- **Expand in Progress**—Cache operations are temporarily disabled due to an expand of a logical drive. When the expand operation completes, the accelerator will be enabled.
- **Snapshot in Progress**—Cache operations are temporarily disabled due to a snapshot operation that is queued up or in progress. When the snapshot operation completes, the accelerator will be enabled.
- **Redundant Low Battery**—Cache operations are temporarily disabled. The redundant controller has insufficient cache battery power.
- **Redundant Size Mismatch**—Cache operations are temporarily disabled. The cache sizes on the redundant controllers do not match.
- **Redundant Cache Failure**—Cache operations are temporarily disabled. The cache on the redundant controller has failed.
- **Excessive ECC Errors**—Cache operations have been permanently disabled. The number of cache lines experiencing excessive ECC errors has reached a preset limit.
- **ADG Enabler Missing**—Indicates that write cache operations have been temporarily disabled. An advanced data guarding logical drive is configured but the RAID ADG Enabler Module is broken or missing.

- **POST ECC Errors**—Indicates that write cache operations have been permanently disabled. The cache has been disabled due to a large number of ECC errors detected while testing the cache during the Power-On Self-Test (POST).
- **Unknown**—The Storage Agents do not recognize the error code. You might need to update your software.

Serial Number—Displays the serial number for the Array Accelerator. Use this number for identification purposes.

Total Memory—Displays the total amount of accelerator memory in megabytes, including both battery-backed and non-battery-backed memory.

Write Cache—Displays the percentage of cache memory allocated for posted write caching or the amount of memory allocated for the write cache in Kbytes. If Kbytes are displayed then the actual amount of usable memory is half the amount shown because the data is kept in duplicate (mirrored).

Read Cache—Displays the percentage of cache memory allocated for read ahead caching or the amount of memory allocated for the read cache in Kbytes. If Kbytes are displayed then the actual amount of usable memory is half the amount shown because the data is kept in duplicate (mirrored).

NOTE: Read cache is not available on IDA-2 or SCSI Managed Array Technology (SMART) controllers. Values for these controllers will be 0.

Write Errors—Displays the total number of write memory parity errors that were detected while writing to the Array Accelerator.

Write parity errors occur when the system detects that information has not been transferred to the Array Accelerator correctly. A parity bit is included for each byte of information stored in memory. When the microprocessor reads or writes data, the system counts the value of the bits in each byte. If the total does not match the system's expectations, a parity error has occurred.

Read Errors—Displays the total number of read memory parity errors that were detected while reading from the Array Accelerator. The mirrored copy of data in the write cache can be accessed to obtain correct data if a memory parity error occurs.

Memory parity errors occur when the system detects that information has not been transferred correctly. A parity bit is included for each byte of information stored in memory. When the microprocessor reads or writes data, the system counts the value of the bits in each byte. If the total does not match the system's expectations, a parity error has occurred. A bad memory chip, memory corruption, or lack of memory refresh might cause memory parity errors.

Identify Drives

Select the length of time to blink the LEDs of a physical drive that are connected to this controller from the dropdown list box, and then click the **Start** button. The page will automatically refresh and display an image of a blinking drive and a Stop button. Click the **Stop** button to end blinking before the time expires.

After the drive lights stop blinking the page will have to be manually refreshed to display the Start button. There might be a delay, depending on the length of the Insight Management Agents data collection interval, after the drive lights stop blinking and before the Start button appears.

Only drives in hot-plug trays are supported since the LEDs are part of the tray. If an individual logical drive or physical drive on this controller is selected to blink while the drives connected to this controller are currently blinking then the other drives will stop blinking and only the selected drive will blink.

When there are redundant controllers, only the active controller can be used to blink the drives connected to the controller.

IMPORTANT: The Start or Stop button only appears if you are logged on as an administrator or an operator, SNMP sets are enabled, and a SNMP Community string has been defined with “write” access. Go back to the Summary page, and select **login** to login as an administrator or operator. SNMP sets can be enabled in the Insight Management Agents for Servers control panel applet on the SNMP Settings page. A SNMP Community string with “write” access can be defined in the SNMP Service Properties Security page located in Computer Management under Services. The drive icon lights will not blink in Microsoft Internet Explorer unless **Play animations in web pages** is enabled in the Tools menu Internet Options under the Advanced tab in the Multimedia section.

Physical Drive Information

This section provides an overview of all disk drives attached to the controller. Each physical drive is listed as a separate entry in the Mass Storage submenu. The information displayed next to the physical drive includes the condition of the drive, the location of the drive (port and drive number) and drive size. Select any of the physical drives from the Mass Storage submenu to display more information about the drive. The following information displays:

Status—Indicates the status of the SCSI physical drive. The possible values are:

- OK—The drive is functioning properly.
- Failed—The drive is no longer operating and should be replaced.
- Predictive Failure—The physical drive has a predictive failure error and should be replaced.
- Unknown—The physical drive cannot be monitored at this time. This might be because:
 - The device driver for this drive might have been unloaded.
 - The logical drive might have failed and been deactivated by the operating system. In this case, the last known status was OK.
 - The Storage Agents do not recognize the drive. You might need to upgrade your software.

Action—Displays the action that is required for this device. The following values are valid:

- Replace Drive—Replace this drive. If the drive condition is Failed, check the Predictive Indicators, Problem Indicators, and Failure Indicators for a possible cause of the failure.
- Replace S.M.A.R.T. Drive—The S.M.A.R.T. hard drive predicts imminent failure. Schedule replacement of the drive before an actual failure occurs.
- No Action Required—The drive is operating normally and no action is required.

Capacity—Displays the size of the physical drive in megabytes. For example, 120 indicates that the physical drive is 120 megabytes.

Model—Displays a description of the physical drive. The text depends on the manufacturer of the drive and the drive type.

NOTE: If a drive fails, note the model to identify the type of drive necessary for replacement.

Firmware Version—Displays the physical drive firmware version number. Be sure you have the most recent version of the firmware because older versions might not support all of the newest features.

Serial Number—Displays the serial number assigned to the physical drive. This value is based on the serial number as returned by the SCSI inquiry command but might be modified due to space limitations. This item can be used for identification purposes.

Service Hours—Displays the current number of hours of service (the number of hours that a physical drive has been spinning) since the drive was stamped. The drive was stamped when it left the factory.

For example, if the Current Service Hours value is 604, the drive has been operating for 604 hours. If an error occurred at 499 Service Hours, it occurred after 499 hours of service.

S.M.A.R.T. Support—Indicates whether or not the SCSI physical drive supports S.M.A.R.T. The possible values are:

- Available—This drive supports predictive failure monitoring.
- Not available—Predictive failure monitoring is not available for this drive.
- Unknown—The Storage Agents cannot determine if the drive supports predictive failure monitoring. You might need to upgrade your driver or Storage Agents.

NOTE: A value of Unknown indicates that the agents cannot determine this information from the physical drive.

Current Width—Displays the current negotiated data transfer width for the physical drive. The possible values are:

- Narrow (8 bits)—The negotiated data transfer width for this drive is narrow (8 data bits).
- Wide (16 bits)—The negotiated data transfer width for this drive is wide (16 data bits).
- Unknown—The Storage Agents are unable to determine the current negotiated data transfer width for this drive.


Current Speed—Displays the current negotiated data transfer speed for the physical drive. The possible values are:

- **Asynchronous**—The current data transfer speed for this drive is asynchronous.
- **Fast**—The current data transfer speed for this drive is 10 million transfers per second.
- **Ultra**—The current data transfer speed for this drive is 20 million transfers per second.
- **Ultra2**—The current data transfer speed for this drive is 40 million transfers per second.
- **Ultra3**—The current data transfer speed for this drive is 80 million transfers per second.
- **Ultra320**—The negotiated data transfer speed for this device is 160 million transfers per second.
- **Unknown**—The agent is unable to determine the current negotiated data transfer speed for this drive.

NOTE: If the current data transfer width is Narrow (8 bits) then the speed in megabytes per second is equal to the million transfers per second speed. If the current width is Wide (16 bits) then the speed in megabytes per second is twice the million transfers per second speed. For example, if the current speed is Ultra and the width is Wide then the speed would be 40 megabytes per second.

Placement—Indicates whether the physical drive is in an internal or external storage system. The following values are valid:

- **Internal**—The physical drive is in an internal storage system.
- **External**—The physical drive is in an external storage system.
- **Unknown**—The physical drive is not in a storage system or the Storage Agents cannot determine the drive placement.

—This symbol indicates that the drive is a hot-plug drive.

Rotational Speed—Indicates the rotational speed of the drive in revolutions per minute.

Identify Drive

Select the length of time to blink the LEDs of a physical drive from the dropdown list box and then select the **Start** button. The page will automatically refresh and display an image of a blinking drive and a **Stop** button. Select the **Stop** button to end blinking before the time expires.

After the drive lights stop blinking the page will have to be manually refreshed to display the **Start** button. There might be a delay, depending on the length of the Insight Management Agents data collection interval, after the drive lights stop blinking and before the **Start** button can be displayed.

Only drives in hot-plug trays are supported since the LEDs are part of the tray. Only one drive on a selected controller might be identified at a time. If a different drive is selected while another drive is currently blinking then the other drive will stop blinking and the selected drive will blink.

IMPORTANT: The **Start** or **Stop** button will only be displayed if you are logged on as an administrator or an operator, SNMP sets are enabled, and a SNMP Community string has been defined with “write” access. Go back to the Summary page and select **login** to log in as an administrator or operator. SNMP sets can be enabled in the Management Agents for Servers control panel applet on the SNMP Settings page. A SNMP Community string with “write” access can be defined in the SNMP Service Properties Security page located in Computer Management under Services. The drive icon lights will not blink in Microsoft Internet Explorer unless **Play animations in web pages** is enabled in the Tools menu Internet Options under the Advanced tab in the Multimedia section.

Logical Drive Information

Select one of the listed logical drives to see more information about the drive.

Spare Information

This section provides additional information about the spare drive, including status and the number of physical drives it will replace, if any. This section is available only if this physical drive is configured as a spare drive. The following information is available:

Status—Displays the status of the on-line spare drive. The following values are possible:

- **Building**—A physical drive has failed. Automatic Data Recovery is in progress to recover data to the on-line spare.
- **Active**—A physical drive has failed. Automatic Data Recovery is complete. The system is using the on-line spare as a replacement for the failed drive.
- **Failed**—The on-line spare has failed and is no longer available for use.
- **Inactive**—The monitored system has an on-line spare configured, but is not currently in use.
- **Unknown**—You might need to upgrade your software.

When the status is Building, one of the following will be displayed to indicate the progress of the Automatic Data Recovery.

- **Percent Rebuild Complete**—Displays the percent complete of the rebuild. When the value reaches 100, the rebuilding process is complete. The drive array continues to operate in interim recovery mode during the rebuild.
- **Rebuild Blocks Left**—Displays the number of blocks of data that still must be redistributed. When the value reaches 0, the rebuilding process is complete. The array continues to operate interim recovery mode during the rebuild.

Replaced Drives—Identifies the failed physical drives in the logical drive that the spare drive has replaced. Use this monitored item to identify the failed drives and replace those drives as soon as possible.

If N/A appears, the spare has not begun operating in place of the failed drive.

Predictive Indicators

Use the Predictive Indicators to predict when a drive, which is now operating normally, might need to be replaced.

S.M.A.R.T. Status—Displays the S.M.A.R.T. status as reported by the physical drive. This is only displayed if the drive supports S.M.A.R.T. predictive failure. The possible values are:

- **Other**—The Storage Agent is unable to determine the status of S.M.A.R.T. predictive failure monitoring for this drive.
- **OK**—Indicates the drive is functioning properly.
- **Replace Drive**—Indicates that the drive has a S.M.A.R.T. predictive failure error and should be replaced.

The following predictive indicators will not be displayed if the physical drive does not support any of the indicators and S.M.A.R.T. status is available.

The numerical data associated with these items displays after the item name. For example, Used Realloc: 122 means that there are 122 used reallocation sectors for this drive. The status of these items can be OK or Replace Drive. If the status is Replace Drive, replace the drive, or an actual drive failure might occur in the future. The Predictive Indicators are:

Functional Test 1, 2, and 3—Provides information about a series of tests that indicates how well a physical drive works. The Status of these items can be OK or Replace Drive. If the status is Replace Drive, replace the drive, or an actual drive failure might occur in the future.

These tests compare the way the physical drive currently operates when performing various tasks with the way it worked when it was new.

Used Realloc—Displays the number of sectors of the reallocation area that have been used by the physical drive. The status of this item can be OK or Replace Drive. If the status is Replace Drive, replace the drive, or an actual drive failure might occur in the future.

Because of the nature of magnetic disks, certain sectors on a drive might have media defects. The reallocation area is part of the drive that the drive manufacturer sets aside to compensate for these defects. The array controller writes information addressed from the unusable sectors to available sectors in the reallocation area. If too many sectors have been reallocated, there might be a problem with the drive.

Spinup Time—Displays the time it takes for a physical drive to spin up to full speed. The Status of this item can be OK or Replace Drive. If the status is Replace Drive, replace the drive, or an actual drive failure might occur in the future.

Drives require time to gain momentum and reach operating speed. As cars are tested to go from 0 mph to 60 mph in X number of seconds, drive manufacturers have preset expectations for the time it takes the drive to spin to full speed. Drives that do not meet these expectations might have problems.

The spinup time value is shown in tenths of a second. Thus, if the drive takes 12 seconds to spin up, the value would be 120. The value might be 0 for this monitored item under one of the following conditions:

- You are monitoring a physical drive that is part of the managed system's internal drive array storage, and you use a warm boot to reset the monitored system. During a warm boot, the drives continue to spin.
- You are monitoring a physical drive in a ProLiant Storage System or an Intelligent Array Expansion System and you reset the managed system but not the ProLiant or Intelligent Array Expansion System.
- The physical drive might be configured to start up immediately when the system is powered on, instead of waiting for the controller to start it.

Problem Indicators

Use the Problem Indicators to determine when a drive failure has occurred that might be correctable without replacing the drive. The Problem Indicators are:

Fail Recov Reads—Displays the number of read errors that occurred while Automatic Data Recovery was being performed from this physical drive to another drive. If a read error occurs, Automatic Data Recovery stops.

Other Timeouts—Displays the number of times the drive did not respond with an interrupt within a controller-defined period of time after a command had been issued. This monitored item does not include Data Request (DRQ) timeouts.

If the other timeouts count is not zero and the drive has failed, you might be able to correct the problem without replacing the drive. Follow the steps below:

1. Be sure that all system and storage system cables are intact and seated properly. You might need to replace the cables.
2. Be sure that a ProLiant Storage System is plugged in and powered on. Be sure the power supply is functioning.

IMPORTANT: Never turn off a ProLiant Storage System when the attached system is still turned on.

3. Check the physical proximity of the system to other electrical devices. Since electrical noise might cause this error, check the AC circuit for other electrical devices.
4. Timeouts can be caused when two or more drives are set to the same SCSI ID. Ensure that the ProLiant and system SCSI IDs do not conflict.
5. On a ProLiant Storage System, check the SCSI ID cable on the drive tray. If the cable is damaged or incorrectly installed, SCSI Timeouts can occur. Refer to the documentation accompanying the Hot-Plug Drive Tray Service Spare Kit.
6. Be sure that the system temperature is within specified limits. Ensure that the fans are operating and are not blocked.
7. In some instances, drive failure can cause timeouts. If you continue to receive many of these errors, replace the drive.

SCSI Bus Faults—Displays the number of times that SCSI bus parity, overrun, or underrun errors have been detected on the SCSI bus. Since the controller will retry the operation, SCSI bus faults can cause a drop in performance, or, in some cases, data corruption.

If the count is not zero and the drive has failed, complete the following steps to attempt to correct the problem without replacing the drive:

1. Be sure that all system and storage system cables are intact and seated properly. You might need to replace the cables.
2. Check the physical proximity of the system to other electrical devices. Since electrical noise might cause a Bus Fault error, check the AC circuit for other electrical devices.
3. Be sure that the system temperature is within specified limits. Ensure that fans are operating and are not blocked.
4. SCSI Bus Faults can be caused when two or more drives are set to the same SCSI ID. Ensure that ProLiant and system SCSI IDs do not conflict.
5. In some instances, drive failure can cause SCSI Bus Faults. If you continue to receive many of these errors, replace the drive.

IRQ Deglitch—Displays the number of times that a glitch has been detected on the drive interface cable. Since the controller will retry the operation, glitches can cause a drop in performance or, in some cases, data corruption. Glitches indicate electrical noise on the drive cable or an intermittent failure of the drive electronics.

This item is considered a Problem Indicator that might be correctable without replacing the drive. If this counter is not zero and the drive has failed:

1. Be sure that all system and storage system cables are intact and seated properly. You might need to replace cables.
2. Check the physical proximity of the system to other electrical devices. Since electrical noise might cause a glitch error, check the AC circuit for other electrical devices.
3. If you continue to receive many of these errors, replace the drive.

NOTE: If the drive has not failed, the above counts simply provide a cumulative record of past errors that have been corrected.

Failure Indicators

Use the Failure Indicators to determine the cause of a drive failure. Typically, the number of failures is zero when the drive is operating normally. If a counter is not zero and the drive has not failed, there could be an intermittent problem that might require the drive to be replaced. The Failure Indicators are:

- **Spinup Errors**—When the physical drive fails due to the failure of a spin-up command, a Spinup Error occurs. If the failure count is not zero and the drive has failed, replace the drive.

If the counter is not zero and the drive is OK (has not failed), there might be an intermittent problem that requires drive replacement. If you observe that the count is increasing over time, replace the drive.

- **Aborted Commands**—The Aborted Commands counter records the number of times that a physical SCSI drive returned an Aborted Command status when a SCSI command was attempted. This error count indicates unsuccessful termination of the SCSI command. When the physical drive is failed due to aborted commands that could not be retried successfully, Aborted Commands errors occur. If the number of errors is not zero and the drive has failed, replace the drive.

If the counter is not zero and the drive is OK (has not failed), there might be an intermittent problem that requires drive replacement. If you observe that the count is increasing over time, replace the drive.

- **Reallocation Aborts**—When the physical drive is failed due to an error that occurred when the controller was trying to reallocate a bad sector, a Reallocation Abort error occurs.

Because of the nature of magnetic disks, certain sectors on a drive might have media defects. The reallocation area part of the drive is set aside to compensate for these defects. The array controller writes information addressed from unusable sectors to available sectors in the reallocation area.

If the number of reallocation abort errors is not zero and the drive has failed, replace the drive. If the counter is not zero and the drive is OK (has not failed), there might be an intermittent problem that requires drive replacement. If you observe that the count is increasing over time, replace the drive.

- **Media Failures**—When this physical drive fails due to unrecoverable media errors, a Media Failure occurs.

If the number of media failure errors is not zero and the drive has failed, replace the drive. If the counter is not zero and the drive is OK (has not failed), there might be an intermittent problem that requires drive replacement. If you observe that the count is increasing over time, replace the drive.

- **Format Errors**—When a format operation fails because the controller was unable to remap a bad sector, a Format Error occurs.

If the number of format errors is not zero and the drive has failed, replace the drive. If the counter is not zero and the drive is OK (has not failed), there might be an intermittent problem that requires drive replacement. If you observe that the count is increasing over time, replace the drive.

- **Hardware Errors**—The Hardware Errors counter records the number of times that a physical SCSI drive returned a Hardware Error status when a SCSI command was attempted. This error status indicates unsuccessful termination of the SCSI command. The controller typically retries this command several times before failing the drive.

If the number of hardware errors is not zero and the drive has failed, replace the drive. If the counter is not zero and the drive is OK (has not failed), there might be an intermittent problem that requires drive replacement. If you observe that the count is increasing over time, replace the drive.

- **Not Ready Errors**—When a physical drive returns a not ready status when it should be ready, a Drive Not Ready Error occurs. This error could occur if a drive spins down unexpectedly or if the drive never becomes ready after the spin up command is issued.

If the number of not ready errors is not zero and the drive has failed, replace the drive. If the counter is not zero and the drive is OK (has not failed), there might be an intermittent problem that requires drive replacement. If you observe that the count is increasing over time, replace the drive.

- **Bad Target Errors**—When a physical drive performs an action that does not conform to the SCSI-2 port protocol, the SCSI port is reset.

If the number of bad target errors is not zero and the drive has failed, replace the drive. If the counter is not zero and the drive is OK (has not failed), there might be an intermittent problem that requires drive replacement. If you observe that the count is increasing over time, replace the drive.

- **Fail Recov Writes**—Indicates whether write errors occurred while Automatic Data Recovery was being performed to this physical drive. If a write error occurs, Automatic Data Recovery stops. These errors indicate that the physical drive has failed.

If the number of fail recov writes is not zero and the drive has failed, replace the drive. If the counter is not zero and the drive is OK (has not failed), there might be an intermittent problem that requires drive replacement. If you observe that the count is increasing over time, replace the drive.

- **Self-Test Errors**—Indicates if a physical drive failed its self-test. The physical drive does a self-test each time the system is turned on.

If the number of self-test errors is not zero and the drive has failed, replace the drive. If the counter is not zero and the drive is OK (has not failed), there might be an intermittent problem that requires drive replacement. If you observe that the count is increasing over time, replace the drive.

The previous information is available for those drives that have been stamped with monitoring and performance data enabled. The drive was stamped when it left the factory.

Statistics

This section displays statistics about a specific drive array controller physical drive. You can use the run-time statistics to monitor the health of a specific drive. The following information displays:

- **Sectors Read**—Displays the total number of sectors read from the physical drive since the drive was stamped. The drive was stamped when it left the factory.
- **Hard Read Errors**—Displays the number of read errors that could not be recovered by a physical drive's ECC algorithm or through retries. Over time, a drive might produce these errors. If you receive these errors, a problem might exist with your drive.

The severity of these errors depends on whether the managed system is running in a fault tolerant mode. With fault tolerance, the controller can remap data to eliminate the problems caused by these errors.

- **Recovered Read Errors**—Displays the number of read errors corrected through physical drive retries. Over time, all drives produce these errors. If you notice a rapid increase in the value for Recovered Read Errors or Hard Read Errors, a problem might exist with the drive. Expect more errors for this monitored item than for Hard Read Errors.
- **Total Seeks**—Displays the total number of seek operations during seek tests performed by the physical drive since the drive was stamped. The drive was stamped when it left the factory.

During normal reads and writes to the drive, the drive does implied seeks to the location where data resides. These are not included in this count.

- **Seek Errors**—Displays the number of seek errors that a physical drive detects. A seek error is a seek that failed. Over time, a drive usually produces these errors. If you notice a rapid increase in the value shown for Seek Errors, this physical drive might be failing. Only an unusually rapid increase in these errors indicates a problem.

- **Sectors Written**—Displays the total number of sectors written to the physical drive since the drive was stamped. The drive was stamped when it left the factory.
- **Hard Write Errors**—Displays the number of write errors that could not be recovered by a physical drive. Over time, a drive might produce these errors. If you notice an increase in the value shown for Hard Write Errors or Recovered Write Errors, a problem might exist with the drive. The counter value increases every time the physical drive detects another error. On average, these errors should occur less frequently than read errors.
- **Recovered Write Errors**—Displays the number of write errors corrected through physical drive retries or recovered by a physical drive on a monitored system. Over time, a drive might produce these errors. If you notice an increase in the value shown for Recovered Write Errors or Hard Write Errors, a problem might exist with the drive.

The Recovered Write Errors value increases every time the physical drive detects and corrects an error. Only an unusually rapid increase in these errors indicates a problem. On average, these errors should occur less frequently than read errors.

- **Hot-Plug Count**—Indicates the number of times this physical drive was removed by a hot-plug event from a ProLiant Storage System since the drive was stamped. The drive was stamped when it left the factory.
- **DRQ Timeouts**—Displays the number of times that a physical drive continued to request data but did not get a command completion. This value increases every time a DRQ timeout occurs for the physical drive.

A defective drive or cable might cause DRQ timeouts to occur. If you see an increase in these errors, ensure that the cables connecting the drive are intact.

Logical Drive Information

A list of logical drives associated with the controller displays in the Mass Storage submenu. Each logical drive in the list displays the condition, logical drive number and the fault tolerance of that logical drive. Select one of the logical drive entries to display the following information.

Status—Displays the status of the logical drive. The logical drive can be in one of the following states:

- **OK**—Indicates that the logical drive is in normal operation mode.
- **Failed**—Indicates that more physical drives have failed than the fault tolerance mode of the logical drive can handle without data loss.
- **Unconfigured**—Indicates that the logical drive is not configured.
- **Interim recovery**—Indicates that the logical drive is using Interim Recovery Mode. In Interim Recovery Mode, at least one physical drive has failed, but the logical drive's fault tolerance mode lets the drive continue to operate with no data loss.
- **Ready rebuild**—Indicates that the logical drive is ready for Automatic Data Recovery. The physical drive that failed has been replaced, but the logical drive is still operating in Interim Recovery Mode.

- **Rebuilding**—Indicates that the logical drive is currently doing Automatic Data Recovery. During Automatic Data Recovery, fault tolerance algorithms restore data to the replacement drive.
- **Wrong drive**—Indicates that the wrong physical drive was replaced after a physical drive failure.
- **Bad connect**—Indicates that a physical drive is not responding.
- **Overheating**—Indicates that the drive array enclosure that contains the logical drive is overheating. The drive array is still functioning, but should be shut down.
- **Shutdown**—Indicates that the drive array enclosure that contains the logical drive has overheated. The logical drive is no longer functioning.
- **Expanding**—Indicates that the logical drive is currently doing Automatic Data Expansion. During Automatic Data Expansion, fault tolerance algorithms redistribute logical drive data to the newly added physical drive.
- **Not available**—Indicates that the logical drive is currently unavailable. If a logical drive is expanding and the new configuration frees additional disk space, this free space can be configured into another logical volume. If this is done, the new volume will be set to not available.
- **Queued for expansion**—Indicates that the logical drive is ready for Automatic Data Expansion. The logical drive is in the queue for expansion.
- **Unknown**—You might need to upgrade your software.

When the status is Rebuilding one of the following will be displayed to indicate the progress of the rebuild.

- **Percent Rebuild Complete**—Displays the percent complete of the rebuild. When the value reaches 100, the rebuilding process is complete. The drive array continues to operate in interim recovery mode while the drive is rebuilding.
- **Rebuild Blocks Left**—Displays the number of blocks of data that still must be redistributed. When the value reaches 0, the rebuilding process is complete. The array continues to operate in interim recovery mode while the drive is rebuilding.

Rebuilding Drive—Identifies the physical drive that failed. The logical drive is rebuilding using a spare drive in place of this failed drive.

When the status is Expanding one of the following will be displayed to indicate the progress of the expansion.

- **Percent Expand Complete**—Displays the percent complete of the expansion. When a logical volume is expanding, the drive must redistribute the logical volume data across the physical drives. When the value reaches 100, the expansion process is complete.
- **Expand Blocks Left**—Displays the number of blocks of data that still must be redistributed. When the value reaches 0, the expansion process is complete. The array continues to operate normally while the drive is expanding.

Fault Tolerance—Displays the fault tolerance mode of the logical drive. To change the fault tolerance mode, run the Array Configuration Utility.

The following values are valid for the Logical Drive Fault Tolerance:

- **None**—(RAID 0) Fault tolerance is not enabled. If a physical drive reports an error, the data cannot be recovered by the Drive Array.
- **Mirroring**—(RAID 1/RAID 0+1) The highest level of fault tolerance. It is the only method offering fault tolerance protection if no more than two physical drives are selected. Drive mirroring creates fault tolerance by storing duplicate data on two drives. There must be an even number of drives. This is the most costly fault tolerance method because it requires 50 percent of the drive capacity to store the redundant data.
- **Data Guarding**—(RAID 4) Assures data reliability while using only a small percent of the logical drive storage capacity. A designated, single physical drive contains parity data. If a drive fails, the controller uses the data on the parity drive and the data on the remaining drives to reconstruct data from the failed drive. This allows the system to continue operating with slightly reduced performance until you replace the drive.
- **Distributed Data Guarding**—(RAID 5) Stores parity data across all the physical drives in the array and allows more simultaneous read operations and higher performance than data guarding (RAID 4). If a drive fails, the controller uses the parity data and the data on the remaining drives to reconstruct data from the failed drive. The system then continues operating with a slightly reduced performance until you replace the failed drive.
- **Advanced Data Guarding**—(RAID ADG) The fault tolerance method that provides the highest level of data protection. It stripes data and parity across all the physical drives in the configuration to ensure the uninterrupted availability of uncorrupted data. This fault-tolerance method is similar to RAID 5 in that parity data is distributed across all drives in the array, except in RAID ADG the capacity of multiple drives is used to store parity data. Assuming the capacity of two drives is used for parity data, this allows continued operation despite simultaneous failure of any two drives in the array, whereas RAID 4 and RAID 5 can only sustain failure of a single drive.
- **Unknown**—You might need to upgrade your software.

Capacity—Displays the size of the logical drive in megabytes. For example, 120 indicates that the logical drive is 120 megabytes. Use this data to determine whether the drive will be large enough to accommodate your needs.

The capacity utility defines a megabyte as 1,048,576 bytes. The capacity value shown might differ from the stated size of the drive due to different definitions of a megabyte. Many hardware manufacturers use the value of 1,000,000 for megabyte instead of 1,048,576.

Accelerator—Indicates whether the logical drive has an Array Accelerator board configured and enabled. The following values are valid:

- Enabled—The Array Accelerator board is configured and enabled for this logical drive.
- Disabled—The Array Accelerator board is configured but not enabled for this logical drive.
- Unavailable—There is no Array Accelerator board configured for this logical drive.
- Unknown—The Storage Agents do not recognize the Array Accelerator board. You might need to upgrade your software.

Stripe Size—Displays the size of a logical drive stripe in kilobytes.

Total Read and Write Requests—Displays the total number of read and write requests for the logical volume, expressed in reads and writes per second.

Reads—Displays the number of read requests for the logical volume, expressed in reads per second.

Writes—Displays the number of write requests for the logical volume, expressed in writes per second.

Sectors Read—Displays the number of sectors read for the logical volume for this interval. This value is expressed in sectors per second.

Sectors Written—Displays the number of sectors written for the logical volume for this interval. This value is expressed in sectors per second.

Identify Drive

Select the length of time to blink the LEDs of the physical drive that make up the logical drive from the dropdown list box, and then click the **Start** button. The page will automatically refresh and display an image of a blinking drive and a Stop button. Click the **Stop** button to end blinking before the time expires.

After the drive lights stop blinking the page will have to be manually refreshed to display the **Start** button. There might be a delay, depending on the length of the Insight Management Agents data collection interval, after the drive lights stop blinking and before the Start button appears.

Only drives in hot-plug trays are supported since the LEDs are part of the tray. Spare drives that are included in the logical drive will also blink. Only one logical drive on a selected controller might be identified at a time. If a different drive is selected while another drive is currently blinking then the other drive will stop blinking and the selected drive will blink.

IMPORTANT: The Start or Stop button only appears if you are logged on as an administrator or an operator, SNMP sets are enabled, and a SNMP Community string has been defined with “write” access. Go back to the Summary page and select **login** to login as an administrator or operator. SNMP sets can be enabled in the Insight Management Agents for Servers control panel applet on the SNMP Settings page. A SNMP Community string with “write” access can be defined in the SNMP Service Properties Security page located in Computer Management under Services. The drive icon lights will not blink in Microsoft Internet Explorer unless **Play animations in web pages** is enabled in the Tools menu Internet Options under the Advanced tab in the Multimedia section.

Physical Drives

Select one of the listed physical drives to see more information about the drive.

Spare Drives

Select one of the listed spare drives to see more information about the drive.

Tape Storage System Information

Select the Tape Storage System Information entry from the Mass Storage submenu to display the following information.

Status—Displays the status of the tape storage system. The following values are valid:

- OK—Indicates that the library is operating normally.
- Degraded—Indicates the library has degraded in some manner.
- Failed—Indicates the library has failed and can no longer return data. The library might need to be replaced.
- Offline—Indicates the Storage Agents can no longer communicate with the library. This could be caused by a cabling problem or the library might be powered off.
- Unknown—The state of the tape library cannot be determined. You might need to upgrade the Storage Agents.

Model—Displays the model name of the tape library. Use this value for identification purposes.

Firmware Revision—Displays the firmware revision level of the tape library. The level can be used for identification purposes.

Serial Number—Displays the unit serial number for the tape library. Use this value for identification purposes.

Current Width—Displays the current negotiated data transfer width for the tape library. The possible values are:

- **Narrow (8 bits)**—The negotiated data transfer width for this tape library is narrow (8 data bits).
- **Wide (16 bits)**—The negotiated data transfer width for this tape library is wide (16 data bits).
- **Unknown**—The Storage Agents are unable to determine the current negotiated data transfer width for this tape library.

Current Speed—Displays the current negotiated data transfer speed for the tape library. The possible values are:

- **Asynchronous**—The current data transfer speed for this tape library is asynchronous.
- **Fast**—The current data transfer speed for this tape library is 10 million transfers per second.
- **Ultra**—The current data transfer speed for this tape library is 20 million transfers per second.
- **Ultra2**—The current data transfer speed for this tape library is 40 million transfers per second.
- **Ultra3**—The current data transfer speed for this tape library is 80 million transfers per second.
- **Unknown**—The agent is unable to determine the current negotiated data transfer speed for this tape library.

NOTE: If the current data transfer width is Narrow (8 bits) then the speed in megabytes per second is equal to the million transfers per second speed. If the current width is Wide (16 bits) then the speed in megabytes per second is twice the million transfers per second speed. For example, if the current speed is Ultra and the width is Wide then the speed would be 40 megabytes per second.

Door Status—Displays the status of the door. The following values are valid:

- **Not Supported**—The device does not support the door status.
- **Closed**—The door is closed.
- **Open**—The door is open.
- **Unknown**—The state of the tape library door cannot be determined. You might need to upgrade the Storage Agents.

Total Moves—Displays the number of tape moves for the library loader arm.

Service Hours—Displays the number of hours of operation for the library.

Last Known Error—Displays the last error returned by the tape library.

Associated Tape Drives

Select one of the listed associated tape drives to see more information about the drive.

Tape Drive Information

Select one of the tape drive entries from the Mass Storage submenu to display the following information about that drive.

Status—Displays the status of the tape drive. The following values are valid:

- OK—Indicates the tape drive is operating normally.
- Degraded—Indicates the tape drive has degraded in some manner.
- Failed—Indicates the tape drive has failed and can no longer return data. The tape drive might need to be replaced.
- Offline—Indicates the Storage Agents can no longer communicate with the tape drive. This could be caused by a cabling problem or the tape drive might be powered off.
- Missing—Was OK—Indicates that a tape drive that was located in a system and had a status of OK has been removed.
- Missing—Was Offline—Indicates that a tape drive that was located in a system and had a status of offline has been removed.
- Unknown—Indicates that the state of the tape drive cannot be determined. You might need to upgrade the Storage Agents.

Model—Displays the model name of the tape drive. Use this value for identification purposes.

Firmware Revision—Displays the firmware revision level of the tape drive. Use this value for identification purposes.

Serial Number—Displays the unit serial number for the tape drive. Use this value for identification purposes.

NOTE: Not all tape devices support serial numbers.

Current Width—Displays the current negotiated data transfer width for the tape drive. The possible values are:

- Narrow (8 bits)—The negotiated data transfer width for this drive is narrow (8 data bits).
- Wide (16 bits)—The negotiated data transfer width for this drive is wide (16 data bits).
- Unknown—The Storage Agents are unable to determine the current negotiated data transfer width for this drive.

Current Speed—Displays the current negotiated data transfer speed for the tape drive. The possible values are:


- Asynchronous—The current data transfer speed for this drive is asynchronous.
- Fast—The current data transfer speed for this drive is 10 million transfers per second.
- Ultra—The current data transfer speed for this drive is 20 million transfers per second.
- Ultra2—The current data transfer speed for this drive is 40 million transfers per second.
- Ultra3—The current data transfer speed for this drive is 80 million transfers per second.
- Unknown—The agent is unable to determine the current negotiated data transfer speed for this drive.

NOTE: If the current data transfer width is Narrow (8 bits) then the speed in megabytes per second is equal to the million transfers per second speed. If the current width is Wide (16 bits) then the speed in megabytes per second is twice the million transfers per second speed. For example, if the current speed is Ultra and the width is Wide then the speed would be 40 megabytes per second.

Magazine Size—Displays the magazine size of the autoloader tape drives. For single tape devices, the magazine size will be N/A.

Placement—Indicates whether the physical drive is in an internal or external storage system. The following values are valid:

- Internal—The physical drive is in an internal storage system.
- External—The physical drive is in an external storage system.
- Unknown—The physical drive is not in a storage system or the Storage Agents cannot determine the drive placement

—This symbol indicates that the drive is a hot-plug drive.

Library Drive—Indicates whether the tape drive is included in a tape library. The following values are valid:

- Yes—The tape drive is included in a tape library.
- No—The tape drive is not included in a tape library.
- Unknown—The Storage Agents are unable to determine if the tape drive is included in a tape library.

Tape Errors—Displays the total number of read and write errors encountered. This value is maintained from the moment the Tape Hardware Interface driver was loaded.

Tape errors might occasionally occur. If this value rises dramatically, clean the device. If you continue to have errors, you might have a problem. Some common causes of these errors include RFI on the bus cables, bad or missing terminating resistors on the drives, or having more than one device with the same SCSI ID. Ensure the bus cable is free of obstructions and that the devices on the bus are properly configured.

Uncorrectable—Displays the total number of read and write errors, which could not be corrected. This value is maintained from the moment the Tape Hardware Interface driver was loaded.

Uncorrectable errors might occasionally occur. If this value rises dramatically, clean the device. If you continue to have errors, you might have a problem. Some common causes include RFI on the bus cables, bad or missing terminating resistors on the drives, or having more than one device with the same SCSI ID. Ensure the bus cable is free of obstructions and that the devices on the bus are properly configured.

Rereads—Displays the number of times blocks that had to be reread from the device. This value is maintained from the moment the Tape Hardware Interface driver was loaded.

Reread errors might occasionally occur. If this value rises dramatically, clean the device. If you continue to have rereads, you might have a problem. Some common causes include RFI on the bus cables, bad or missing terminating resistors on the drives or having more than one device with the same SCSI ID. Ensure the bus cable is free of obstructions and that the devices on the bus are properly configured.

Rewrites—Displays the number of times blocks that had to be rewritten to the device. This value is maintained since the Tape Hardware Interface driver was loaded.

Rewrite errors might occasionally occur. If this value should rise dramatically, you might need to clean the device. If you continue to have rewrites, you might have a problem. Some common causes include RFI on the bus cables, bad or missing terminating resistors on the drives, or having more than one device with the same SCSI ID. Ensure the bus cable is free of obstructions and that the devices on the bus are properly configured.

Tape Drive Heads Need Cleaning—Indicates whether the tape drive must be cleaned. To clean the tape heads, insert a cleaning tape into the drive and run through a cleaning cycle. The following values are valid:

- **Yes**—The tape drive requires a cleaning tape session in order to clean the heads.
- **No**—The tape drive does not require any cleaning tape session.
- **Not Supported**—The tape drive does not support monitoring of the cleaning required status.

Cleaning Tape Needs Replacement—Indicates whether the cleaning tape that is inserted in an autoloader must be replaced because its cleaning capability is exhausted (it is at the end of the tape). This variable can be in one of the following states:

- **Yes**—The autoloader tape drive requires a new cleaning tape to be inserted.
- **No**—The tape drive does not require a new cleaning tape.
- **Not Supported**—The tape drive does not support monitoring of the cleaning tape replacement status.

NOTE: This variable is only applicable to autoloader tape drives.

Storage Systems

Select a storage system item from the Mass Storage list to display the storage system information. There are two types of storage systems: External Array Storage Systems and ProLiant Storage Systems. The ProLiant Storage System information is listed below:

Box Type—Displays the type of drive enclosure, or box. The following types are possible:

- External Storage System—Outside the machine
- Internal Storage System—Inside the machine
- Unknown—The Storage Agents do not recognize the drive enclosure. You might need to upgrade your software.

Vendor—Displays the name of the vendor that produces this drive enclosure, or box type. Use this information for identification purposes.

Firmware Revision—Displays the firmware revision of the drive enclosure or box. Use this information for identification purposes.

Serial Number—Displays the serial number of the drive enclosure or box. Use this information for identification purposes.

Fan Status—Displays the status of the fan subsystem in the drive enclosure, or box. The following values are possible:

- OK—The fan subsystem is working properly.
- Failed—A fan has failed and there are not enough fans in the fan subsystem to keep the enclosure cool. Check your fan subsystem as soon as possible. Continued operation might cause failure of the drives.
- Degraded—A fan has failed but there are still enough fans in the fan subsystem to keep the enclosure cool.
- Unknown—The Storage Agents do not recognize the status of the fan subsystem. You might need to upgrade your software.
- No Fan—This ProLiant device does not have a fan.

Backplane Speed—Displays the speed of the storage system backplane. The following values are possible:

- Ultra3—The storage system is capable of Ultra3 speeds.
- Ultra320—The storage system is capable of Ultra320 speeds.
- Unknown—The Storage Agents are unable to determine the storage system backplane speed. You might need to upgrade your software.

Drive Bays—Displays the number of drive bays provided by this storage system. If duplexing hardware is used with the storage system, the drive bay number is less than the number of physical drive bays in the enclosure.

Model—Displays the model of the storage system. Use this information for identification purposes.

Board Revision—Displays the board revision level of this storage system backplane.

Thermal Status—Displays the temperature status of the drive system. The following values are possible:

- **OK**—The temperature is within normal operating range.
- **Degraded**—The temperature is outside of normal operating range. Check to be sure the cover is on the ProLiant Storage System.
- **Failed**—The temperature is outside of normal operating range, and could permanently damage the system. Ensure that the fans are spinning, and check the room temperature.
- **Unknown**—The Storage Agents do not recognize the thermal status. You might need to upgrade your software.
- **No Temperature**—This ProLiant system does not support temperature monitoring.

Duplex Option—Displays the duplex option installed in this storage system. The following values are possible:

- **Duplex Top**—This storage system is the top part of a duplexed unit.
- **Duplex Bottom**—This storage system is the bottom part of a duplexed unit.
- **None**—A duplex option is not installed.

Power Supply Status—Displays the status of the Redundant Power supply. The following values are possible:

- OK—All component power supplies that make up the redundant power supply are in normal working order.
- Degraded—One of the component power supplies that make up the redundant power supply has failed. The drive system (either a drive subsystem or a power supply for the main unit) continues to operate; however, if the remaining power supply should fail, the drive system will lose all power and data loss could occur. To correct this situation, schedule a time to bring the device down and replace the failed power supply.
- Unknown—The Storage Agents do not recognize the redundant power supply. You might need to upgrade your software.
- No Redundant Power Supply—This ProLiant server does not support a redundant power supply.

External Array Storage Systems

This section displays general and status information about external array storage systems. Select an external array storage system entry from the Mass Storage list to display a submenu containing separate entries for storage systems, array controllers, physical drives, and logical drives. The following items display:

- Storage System Information
- Array Controller Information
- Accelerator Information
- Physical Drive Information
- Logical Drive Information
- Snapshot Resource Volumes
- Fibre Channel Switch Information
- RAID Array Storage Systems
- External Storage Connections

Storage System Information

Select the Storage System Information entry from the Mass Storage submenu to display the following information about an external array storage system:

Storage System Chassis Information

Model—Displays the model name of the storage system chassis. The valid model names are:

- StorageWorks RAID Array 4000/4100
- StorageWorks Modular SAN Array 1000
- StorageWorks Modular Smart Array 500 formerly known as Smart Array Cluster Storage
- StorageWorks Enterprise/Modular RAID Array
- StorageWorks Enterprise Virtual Array
- StorageWorks Modular Smart Array 500 G2
- StorageWorks Modular Smart Array 20
- StorageWorks Modular Smart Array 1500 CS
- Unknown—The Storage Agents do not recognize the storage system chassis. You might need to upgrade your driver or Storage Agents software.

Name—Displays the user-defined name (or serial number, if preferred) of this storage system chassis.

Connection—Displays the type of connection between the server and the box. The following values are possible:

- Fibre Attached—This chassis is attached to the server through Fibre Channel.
- SCSI Attached—This chassis is attached to the server with a SCSI cable.
- Unknown—The Storage Agents are unable to determine the type of connection.

Serial Number—Displays the storage system chassis serial number, which is normally displayed on the front panel. Use this information for identification purposes.

IO Slots—Displays whether an array controller is installed. If an array controller is installed then the type of array controller is displayed. The following values are possible:

- Not Installed—An array controller is not installed in the I/O slot.
- Fibre Array—A Fibre Channel array controller is installed in the I/O slot.
- SCSI Array—A SCSI array controller is installed in the I/O slot.
- Unknown Array—The Storage Agents cannot identify the type of array controller installed in the I/O slot. The Storage Agents might need to be upgraded to a later version.
- Unknown—The Storage Agents are unable to determine what is installed in the I/O slot.

IO Module Type—Displays the storage system chassis SCSI I/O module type that is installed. The following values are possible:

- 2 Port Ultra3 SCSI Module—A 2 Port Ultra3 SCSI I/O Module is installed.
- 4 Port Shared Storage Module—A 4 Port Shared Storage Module for the Smart Array Cluster Storage is installed.
- 4 Port - Upgrade Firmware—A 4-Port Shared Storage Module for the Smart Array Cluster Storage is installed, but the current controller firmware does not support it. The controller firmware must be upgraded.
- 2 Port Ultra320 SCSI Module—A 2 Port Ultra320 SCSI I/O Module is installed.
- 4 Port Ultra320 SCSI Module—A 4 Port Ultra320 SCSI I/O Module is installed.
- 1 Port Ultra320 SCSI Module—A 1 Port Ultra320 SCSI I/O Module is installed.
- Unknown—The Storage Agents cannot determine the I/O module type for this storage system.

RSO Status—Displays the status of the Recovery Server Option. Two servers are connected to the storage system so that when one fails the other server takes control of the storage system. The following values are possible:

- OK—The recovery server option is installed and the other server is working correctly.
- Secondary Running—Auto—The recovery server option is installed, but the secondary (standby) server is running in place of the primary server. The secondary server assumed control automatically.
- Secondary Running—User—The recovery server option is installed, but the secondary (standby) server is running in place of the primary server. The secondary server assumed control by manual intervention.
- Link Down—The recovery server option is installed, but the communications link to the secondary (standby) server is down.
- No Secondary—The recovery server option is installed, but the communications link to the secondary (standby) server has never been established.
- Disabled—The recovery server option is installed, but it has been disabled by software. This is done to temporarily prevent the secondary server from taking over when the primary server is brought down. This is used to perform maintenance and other tasks on the primary server.
- Not Configured—The recovery server option is supported, but is not configured on this storage system.
- Not Supported—The recovery server option is not supported for this storage system.
- Daemon Down – OK—The recovery server option is installed, but the RSO operating system daemon is not running. The last RSO status was OK.
- Daemon Down—Link Down—The recovery server option is installed, but the RSO operating system daemon is not running. The last RSO status was Link Down.

- **Daemon Down—No Secondary**—The recovery server option is installed, but the RSO operating system daemon is not running. The last RSO status was No Secondary.
- **Daemon Down—Disabled**—The recovery server option is installed, but the RSO operating system daemon is not running. The last RSO status was Disabled.
- **EV Timeout Error**—The recovery server option environment variable, that contains the status, cannot be accessed. The attempted access timed out.
- **Unknown**—The Storage Agents cannot determine the recovery server option status for this storage system.

Internal or External Storage System Information

This information is not available for all types of storage systems. Internal storage system information will be displayed with the External Array Storage System Information. External storage systems will be listed in the Mass Storage submenu under Storage Boxes. Select the storage system in the submenu to display the external storage system information. The following information will be displayed for the storage system backplane:

Vendor—Displays the name of the vendor of storage system backplane. It can be used for identification purposes.

Model—Displays the model name of the storage system backplane. It can be used for identification purposes.

Firmware Revision—Displays the firmware revision level of storage system backplane.

Board Revision—Displays the board revision level of storage system backplane.

Serial Number—Displays the serial number of the storage system backplane. All backplanes do not have a serial number. In this case N/A will be displayed.

Version—Displays the version of storage system backplane.

Fan Status—Displays the current status of the fans in the storage system backplane. The following values are possible:

- **OK**—The fans are installed and operating normally.
- **Degraded**—At least one fan has failed, but there is still sufficient cooling capacity to allow the storage system to continue. The failed fan should be replaced.
- **Failed**—One or more fans have failed and there is insufficient cooling capacity to protect the storage system from damage. The failed fans should be replaced.
- **Not Installed**—This storage system backplane does not have a fan installed.
- **Not Supported**—This storage system does not support reporting fan status through this storage system backplane. The fan status is reported through the first backplane on this storage system.
- **Unknown**—The Storage Agent is unable to determine the fan status.

Speed—Displays the speed of the storage system backplane. The following values are possible:

- Ultra3—The storage system is capable of Ultra3 speeds.
- Ultra320—The storage system is capable of Ultra320 speeds.
- SATA—The storage system is capable of SATA speeds.
- Unknown—The Storage Agents are unable to determine the storage system backplane speed. You might need to upgrade your software.

Drive Bays—Displays the number of bays on this storage system backplane.

Temperature Status—Displays the current temperature status of the storage system backplane. The following values are possible:

- OK—The temperature is within the normal operating range.
- Degraded—The temperature is outside of the normal operating range.
- Failed—The temperature has exceeded the safe operating temperature and could permanently damage the storage system.
- Not Monitored—This storage system does not support temperature monitoring.
- Not Supported—This storage system does not support reporting the temperature status through this storage system backplane. The temperature status is reported through the first backplane on this storage system.
- Unknown—The Storage Agent is unable to determine the temperature status.

Placement—Indicates the location of the storage system backplane. The following values are valid:

- Internal—The storage system backplane is located inside the external array storage system chassis.
- External—The storage system backplane is located outside the external array storage system chassis in an external storage system.
- Unknown—The Storage Agent could not determine the location of the storage system backplane.

Power Supply Status—Displays the current status of the storage system backplane fault tolerant power supply. The following values are possible:

- **OK**—The fault tolerant power supply is operating normally.
- **Degraded**—One of the redundant power supplies has failed. Replace the failed power supply.
- **Failed**—All of the power supplies have failed. Replace the failed power supplies.
- **Not Redundant**—This storage system does not have a redundant power supply.
- **Not Supported**—This storage system does not support reporting fault tolerant power supply status through this backplane. The fault tolerant power supply status is reported through the first backplane on this storage system.
- **Unknown**—The Storage Agent is unable to determine the fault tolerant power supply status.

Duplex Option—Displays the storage system backplane duplex option. The following values are possible:

- **Not Duplexed**—This storage system is not duplexed.
- **Duplex Top**—This is the top portion of a duplexed storage system.
- **Duplex Bottom**—This is the bottom portion of a duplexed storage system.
- **Unknown**—The Storage Agents are unable to determine if this storage system is duplexed.

Backplane Information

This information is not available for all types of storage systems.

Firmware Revision—Displays the revision level of storage system backplane.

Drive Bays—Displays the number of drive bays on this storage system backplane.

Duplex—Displays the storage system backplane duplex option. The following values are possible:

- **Not Duplexed**—This storage system is not duplexed.
- **Duplex Top**—This is the top portion of a duplexed storage system.
- **Duplex Bottom**—This is the bottom portion of a duplexed storage system.
- **Unknown**—The Storage Agents are unable to determine if this storage system is duplexed.

Asset Information

This information is not available for all types of storage systems.

Board—Displays the type of board (system, power, or SCSI).

Serial Number—Displays the serial number of the board.

Board Revision—Displays the revision number of the board.

Power Supply Information

This information is not available for all types of storage systems.

Description—Displays the description of the power supply. The following values are possible:

- Power Bay 1—The power supply is installed in the first power supply bay.
- Power Bay 2—The power supply is installed in the second power supply bay.
- Power Supplies—This is a composite of all the installed power supplies.
- Unknown—The Storage Agents do not recognize the bay. You might need to upgrade your software.

Status—Displays the status of the power supply. The following values are possible:

- OK—A power supply is installed and operating normally.
- Degraded—At least one of multiple power supplies has failed or lost power.
- Failed—A power supply is installed and is no longer operating. Replace the power supply.
- Not Installed—Nothing is installed in this power supply bay.
- Unknown—The Storage Agents are unable to determine if this storage system power supply bay is occupied.

Serial Number—Displays the serial number of the power supply. Use this information for identification purposes.

Board Revision—Displays the board revision of the power supply.

Firmware Revision—Displays the firmware revision of the power supply.

Temperature Information

This information is not available for all types of storage systems.

Description—Displays the description of the temperature sensor. The following values are possible:

- Fan Bay—This temperature sensor is located on the fan module in the fan bay.

- Backplane—This temperature sensor is located on the SCSI drive backplane.
- Unknown—The Management Agent is unable to determine the location of this storage system temperature sensor.

Status—Displays the status of the temperature sensor. The following values are possible:

- OK—The temperature is OK.
- Degraded—The temperature is degraded.
- Failed—The temperature is failed.
- Unknown—The Storage Agents are unable to determine the storage system temperature sensor status.

Current Value—Displays the current temperature value.

Limit Value—Displays the threshold value of the temperature sensor.

Fan Information

This information is not available for all types of storage systems.

Description—Displays the description of the fan module. The following values are possible:

- Fan Bay—This fan module is installed in the fan bay.
- Fans—This is a composite of all the installed fan modules.
- Unknown—The Storage Agents are unable to determine the location of this storage system fan module.

Status—Displays the status of the fan module. The following values are possible:

- OK—The fan module is installed and operating normally.
- Degraded—The fan module degraded.
- Failed—The fan module is failed. Replace the fan module.
- Not Installed—The fan module is not installed.
- Unknown—The Storage Agent is unable to determine if this storage system fan module is installed.

Serial Number—Displays the serial number for the fan module. Use this information for identification purposes.

Board Revision—Displays the board revision of the fan module.

Array Controller Information

This section displays the following information about array controllers that are installed in a storage system.

Model—Displays the model name of the controller card. The valid model names are:

- StorageWorks RAID Array 4000/4100 Controller
- StorageWorks Modular SAN Array 1000 Controller
- StorageWorks Modular Smart Array 500 Controller formerly known as Smart Array Cluster Storage Controller
- StorageWorks HSG80 RAID Array Controller
- StorageWorks HSV110 Virtual Array Controller
- StorageWorks Modular Smart Array 500 G2 Controller
- StorageWorks Modular Smart Array 20 Controller
- Unknown—The Storage Agents do not recognize the array controller in the storage system. You might need to upgrade your driver or Storage Agents software.

Firmware Version—Displays the version of the controller's firmware.

Serial Number—Displays the serial number of the controller. Use this information for identification purposes.

Product Revision—Displays the product revision of the controller. Use this value to further identify a particular revision of the controller model.

World Wide Port Name—Displays the unique Fibre Channel port name for the controller. Use this value to further identify a particular controller.

World Wide Node Name—Displays the unique Fibre Channel node name for the controller. Use this value to further identify a particular controller.

Rebuild Priority—Displays the logical drive rebuild priority of the controller. The following values are valid:

- Low—Indicates the rebuild priority is low.
- Medium—Indicates the rebuild priority is medium.
- High—Indicates the rebuild priority is high.
- Unknown—Indicates that the rebuild priority is not recognized. You might need to upgrade the Storage Agents.

Expand Priority—Displays the logical drive expand priority of the controller. The following values are valid:

- Low—Indicates the expand priority is low.
- Medium—Indicates the expand priority is medium.
- High—Indicates the expand priority is high.
- Unknown—Indicates that the expand priority is not recognized. You might need to upgrade the Storage Agents.

Controller Status—Displays the status of the controller hardware. The following values are valid:

- OK—The controller is operating normally.
- Failed—The controller has failed and is no longer operating.
- Offline—The controller is offline.
- Redundant Path Offline—There are multiple connection paths to this controller. At least one connection path is available and at least one connection path is not available.
- Unknown—Indicates that the Storage Agents are unable to determine the status of the controller. You might need to upgrade the Storage Agents.

Current Role—Displays the array controller's current role for duplexed array controllers. The following values are valid:

- Not Duplexed—This array controller is not duplexed.
- Active—This duplexed array controller is the active controller.
- Backup—This duplexed array controller is the backup controller.
- Unknown—Indicates that the Storage Agents are unable to determine the role of the controller. You might need to upgrade the Storage Agents.

Redundancy Type—Displays the type of redundant configuration. The following values are valid:

- Not Redundant—This array controller is not in a redundant configuration.
- Firmware Active/Standby—The array controller is using an active/standby algorithm implemented in the controller firmware and the operating system driver.
- Firmware Primary/Secondary—The array controller is using a primary/secondary algorithm implemented in the controller firmware and the operating system driver.
- Unknown—Indicates that the Storage Agents are unable to determine the type of redundancy for the controller. You might need to upgrade the Storage Agents.

Redundancy Error—Displays the redundancy error for the controller. The following values are valid:

- No Failure—No failures have been detected.
- No Redundant Controller—No redundant controller is installed.
- Different Hardware—The other controller indicates a different hardware model.
- No Link—A link to the other controller could not be established.
- Different Firmware—The other controller indicates a different firmware version.
- Different Cache—The other controller indicates a different cache size.
- Other Cache Failure—The other controller indicates a cache failure.
- No Drives—This controller cannot see any attached drives, but the other controller can.

- Other No Drives—This controller can Refer to the attached drives, but the other controller cannot.
- Unsupported Drives—One or more attached drives has been determined to be incapable of properly supporting redundant controller operation.
- Expand in Progress—An expand operation is in progress. Redundant operation not supported until the expand operation is complete.
- Unknown—Indicates that the Storage Agents are unable to determine the redundancy error for the controller. You might need to upgrade the Storage Agents.

Accelerator Information

This section displays the following information about Fibre array controllers that are installed in a storage system.

Status—Displays the status of the Fibre Channel Array Accelerator (FCAA). The status can be one of the following:

- Enabled—Cache operations are currently configured and enabled for at least one logical drive.
- Temporarily Disabled—Cache operations have been temporarily disabled. Check the Array Accelerator Error Code for the monitored item to determine why the cache operations have been temporarily disabled.
- Permanently Disabled—Operations have been permanently disabled. Check the Array Accelerator Error Code for the monitored item to determine why the cache operations have been permanently disabled.
- Unavailable—An Array Accelerator has not been configured.

Battery Status—Displays the status of the battery pack on the Array Accelerator. The battery pack can recharge only when the system is powered on. The status can be one of the following:

- OK—The battery pack is fully charged.
- Failed—The battery pack is below a sufficient voltage level and has not fully recharged within the maximum 36 hours. Your board should be serviced as soon as possible.
- Charging—The battery power is less than 75%. The array controller is attempting to recharge the battery pack. A battery pack can take as long as 36 hours to fully recharge. If the battery pack has not recharged after 36 hours, it is considered failed.
- Degraded—The battery pack is still operating but one of the batteries in the pack has failed to recharge properly. Your board should be serviced as soon as possible.
- Not Present—The battery pack is not present. (Some controllers do not have a battery-backed cache.)

Bad Data—Indicates possible data loss due to a battery problem when the system was powered on. The following values are valid:

- **Possible**—At power on, the battery pack was not sufficiently charged. The Array Accelerator has not retained any data that might have been stored in the cache because the battery pack did not retain sufficient charge when the system resumed power. If no data was in the cache, no data was lost. Several situations might have caused this condition, including:
 - If the system was without power for eight days and the battery pack was on (the battery pack activates only if the system loses power unexpectedly), any data that might have been stored was lost.
 - There might be a problem with the battery pack. Refer to the Battery Status monitored item for more information.
 - The Array Accelerator board has been replaced with a new board that has a discharged battery pack. No data has been lost in this case and posted reads and writes will automatically be enabled when the battery pack reaches full charge.
- **None**—No data loss occurred. At power on, the battery pack was properly charged.

Read Errors—Displays the total number of read memory parity errors that were detected while reading from the Array Accelerator. If a memory parity error occurs, the mirrored copy of data in the write cache can be accessed to obtain correct data.

Memory parity errors occur when the system detects that information has not been transferred correctly. A parity bit is included for each byte of information stored in memory. When the microprocessor reads or writes data, the system counts the value of the bits in each byte. If the total does not match the system's expectations, a parity error occurs. A bad memory chip, memory corruption, or lack of memory refresh might cause memory parity errors.

Write Errors—Displays the total number of write memory parity errors that were detected while writing to the Array Accelerator.

Write parity errors occur when the system detects that information has not been transferred to the Array Accelerator correctly. A parity bit is included for each byte of information stored in memory. When the microprocessor reads or writes data, the system counts the value of the bits in each byte. If the total does not match the system's expectations, a parity error occurs.

Total Memory—Displays the total amount of accelerator memory in megabytes, including both battery-backed and non battery-backed memory.

Write Cache—Displays the amount of memory allocated for the write cache in megabytes. The actual amount of usable memory is half the amount shown because data is kept in duplicate (mirrored).

Read Cache—Displays the memory allocated for the read cache in megabytes.

Serial Number—Displays the serial number of the accelerator board. Use this value to further identify the cache controller.

Error Code—Displays the status of the cache operations. The status can be one of the following:

- None—Write cache operations are currently configured and enabled for at least one logical drive. No write cache errors have occurred.
- Bad Configuration—Write cache operations are temporarily disabled. The Array Accelerator board was configured for a different controller. This error could be caused if boards were switched from one system to another. Rerun the EISA Configuration Utility and ensure that the board has been properly configured for this system.

NOTE: If data from another system was stored on the board, rerunning EISA Configuration will cause the data to be lost.
- Low Battery Power—Write cache operations are temporarily disabled due to insufficient battery power. View the Battery Status object instance for more information.
- Disable Command Issued—Write cache operations are temporarily disabled. The device driver issues this command when the server is taken down. This condition should not exist when the system regains power.
- No Resources Available—Write cache operations are temporarily disabled. The controller does not have sufficient resources to perform write cache operations. For example, when a replaced drive is being rebuilt, there will not be sufficient resources. After the operation that requires the resources has completed, this condition will clear and write cache operations will resume.
- Board Not Connected—Write cache operations are temporarily disabled. The Array Accelerator board has been configured but is not currently attached to the controller. Check the alignment of the board and connections.
- Bad Mirror Data—Write cache operations have been permanently disabled. The Array Accelerator board stores mirrored copies of all data. If data exists on the board when the system is first powered up, the board performs a data compare test between the mirrored copies. If the data does not match, an error has occurred. Data might have been lost. Your board might need servicing.
- Read Failure—Write cache operations have been permanently disabled. The Array Accelerator board stores duplicate copies of all data. While reading the data from the board, memory parity errors have occurred so both copies were corrupted and cannot be retrieved. Data has been lost. Have the board serviced.
- Write Failure—Write cache operations have been permanently disabled. This error occurs when an unsuccessful attempt was made to write data to the Array Accelerator board. Data could not be written to write cache memory in duplicate due to the detection of parity errors. This error does not indicate data loss. Have the Array Accelerator board serviced.
- Config Command—Write cache operations have been permanently disabled. The configuration of the logical drives has changed. Reconfigure the Array Accelerator board.
- Expand in Progress—Cache operations are temporarily disabled due to an expand of a logical drive. When the expand operation completes, the accelerator will be enabled.

- Snapshot in Progress—Cache operations are temporarily disabled due to a snapshot operation that is queued up or in progress. When the snapshot operation completes, the accelerator will be enabled.
- Redundant Low Battery—Cache operations are temporarily disabled. The redundant controller has insufficient cache battery power.
- Redundant Size Mismatch—Cache operations are temporarily disabled. The cache sizes on the redundant controllers do not match.
- Redundant Cache Failure—Cache operations are temporarily disabled. The cache on the redundant controller has failed.
- Excessive ECC Errors—Cache operations have been permanently disabled. The number of cache lines experiencing excessive ECC errors has reached a preset limit.
- POST ECC Errors—Indicates that write cache operations have been permanently disabled. The cache has been disabled due to a large number of ECC errors detected while testing the cache during the POST.
- Unknown—The Storage Agents do not recognize the error code. You might need to update your software.

Identify Drives

Select the length of time to blink the LEDs of a physical drive that are connected to this controller from the dropdown list box and then click the **Start** button. The page will automatically refresh and display an image of a blinking drive and a Stop button. Click the **Stop** button to end blinking before the time expires.

After the drive lights stop blinking the page will have to be manually refreshed to display the Start button. There might be a delay, depending on the length of the Insight Management Agents data collection interval, after the drive lights stop blinking and before the Start button appears.

Only drives in hot-plug trays are supported since the LEDs are part of the tray. If an individual logical drive or physical drive on this controller is selected to blink while the drives connected to this controller are currently blinking then the other drives will stop blinking and only the selected drive will blink.

When there are redundant controllers only the active controller can be used to blink the drives connected to the controller.

IMPORTANT: The Start or Stop button only appears if you are logged on as an administrator or an operator, SNMP sets are enabled, and a SNMP Community string has been defined with “write” access. Go back to the Summary page and select **login** to login as an administrator or operator. SNMP sets can be enabled in the Insight Management Agents for Servers control panel applet on the SNMP Settings page. A SNMP Community string with “write” access can be defined in the SNMP Service Properties Security page located in Computer Management under Services. The drive icon lights will not blink in Microsoft Internet Explorer unless **Play animations in web pages** is enabled in the Tools menu Internet Options under the Advanced tab in the Multimedia section.

Physical Drive Information

This section provides an overview of all disk drives attached to the controller. Each physical drive is listed as a separate entry in the Mass Storage submenu. The information displayed next to the physical drive includes the condition, location of the drive (port and drive number) and drive size. Select any of the physical drives from the Mass Storage submenu to display more information about the drive. The following information can be displayed:

Status—Displays the status of the physical drive. The following values are possible:

- **OK**—The drive is functioning properly.
- **Unconfigured**—Indicates the drive is present, but is not part of any logical drive configuration.
- **Threshold Exceeded**—Indicates that the drive has a threshold-exceeded error and should be replaced.
- **Predictive Failure**—Indicates that the drive has a predictive failure error and should be replaced.
- **Failed**—The drive is no longer operating and should be replaced.
- **Unknown**—The physical drive cannot be monitored at this time. This might be because:
 - The device driver for this drive might have been unloaded.
 - The logical drive might have failed and been deactivated by the operating system. In this case, the last known status was OK.
 - The Storage Agent does not recognize the drive. You might need to upgrade your software.

Action—Displays the action that is required for this drive. The following values are valid:

- **Replace Drive**—Replace this drive. If the drive condition is Failed, check the Predictive Indicators, Problem Indicators, and Failure Indicators for a possible cause of the failure.
- **No Action Required**—The drive is operating normally and no action is required.

Capacity—Displays the size of the physical drive in megabytes. For example, 120 indicates that the physical drive is 120 megabytes.

Model—Displays a description of the physical drive. The text depends on the manufacturer of the drive and the drive type.

If a drive fails, note the model to identify the type of drive necessary for replacement.

Firmware Version—Displays the physical drive firmware version number. Be sure that you have the most recent version of the firmware because older versions might not support all of the newest features.

Serial Number—Displays the serial number assigned to the physical drive. This value is based upon the serial number as returned by the SCSI inquiry command but might be modified due to space limitations. This item can be used for identification purposes.

Service Hours—Displays the current number of hours of service (the number of hours that a physical drive has been spinning) since the drive was stamped. The drive was stamped when it left the factory or when you ran System Diagnostics on your new drive.

For example, if the Current Service Hours value is 604, the drive has been operating for 604 hours. If an error occurred at 499 Service Hours, it occurred after 499 hours of service.

S.M.A.R.T. Support—Indicates whether or not the SCSI physical drive supports S.M.A.R.T. The possible values are:

- Available—This drive supports predictive failure monitoring.
- Not available—Predictive failure monitoring is not available for this drive.
- Unknown—The Storage Agents cannot determine if the drive supports predictive failure monitoring. You might need to upgrade your driver or Storage Agents.

NOTE: A value of Unknown indicates that the agents are unable to determine this information from the physical drive.

Current Width—Displays the current negotiated data transfer width for the physical drive. The possible values are:

- Narrow (8 bits)—The negotiated data transfer width for this drive is narrow (8 data bits).
- Wide (16 bits)—The negotiated data transfer width for this drive is wide (16 data bits).
- Unknown—The Storage Agents are unable to determine the current negotiated data transfer width for this drive.


Current Speed—Displays the current negotiated data transfer speed for the physical drive. The possible values are:

- Asynchronous—The current data transfer speed for this drive is asynchronous.
- Fast—The current data transfer speed for this drive is 10 million transfers per second.
- Ultra—The current data transfer speed for this drive is 20 million transfers per second.
- Ultra2—The current data transfer speed for this drive is 40 million transfers per second.
- Ultra3—The current data transfer speed for this drive is 80 million transfers per second.
- Ultra320—The current data transfer speed for this drive is 160 million transfers per second.
- Unknown—The agent is unable to determine the current negotiated data transfer speed for this drive.

NOTE: If the current data transfer width is Narrow (8 bits) then the speed in megabytes per second is equal to the million transfers per second speed. If the current width is Wide (16 bits) then the speed in megabytes per second is twice the million transfers per second speed. For example, if the current speed is Ultra and the width is Wide then the speed would be 40 megabytes per second.

Placement—Indicates whether the physical drive is in an internal or external storage system. The following values are valid:

- Internal—The physical drive is in an internal storage system.
- External—The physical drive is in an external storage system.
- Unknown—The physical drive is not in a storage system or the Storage Agents cannot determine the drive placement.

—This symbol indicates that the drive is a hot-plug drive.

Rotational Speed—Indicates the rotational speed of the drive in revolutions per minute.

Drive Type—Indicates the type of physical drive. The following values are valid:

- Parallel SCSI—The physical drive is a parallel SCSI drive.
- SATA—The physical drive is a Serial ATA drive.
- SAS—The physical drive is a Serial Attached SCSI drive.
- Unknown—The Storage Agents cannot determine the drive type.

SATA Version—Indicates the version of Serial ATA. The following values are valid:

- One—The Serial ATA version is one.
- Two—The Serial ATA version is two.

Unknown—The Storage Agents cannot determine the Serial ATA version or the drive is not a SATA drive.

Identify Drive

Select the length of time to blink the LEDs of a physical drive from the dropdown list box and then click the **Start** button. The page will automatically refresh and display an image of a blinking drive and a Stop button. Click the **Stop** button to end blinking before the time expires.

After the drive lights stop blinking the page will have to be manually refreshed to display the Start button. There might be a delay, depending on the length of the Insight Management Agents data collection interval, after the drive lights stop blinking and before the Start button appears.

Only drives in hot-plug trays are supported since the LEDs are part of the tray. Only one drive on a selected controller might be identified at a time. If a different drive is selected while another drive is currently blinking then the other drive will stop blinking and the selected drive will blink.

IMPORTANT: The Start or Stop button only appears if you are logged on as an administrator or an operator, SNMP sets are enabled, and a SNMP Community string has been defined with “write” access. Go back to the Summary page and select **login** to login as an administrator or operator. SNMP sets can be enabled in the Insight Management Agents for Servers control panel applet on the SNMP Settings page. A SNMP Community string with “write” access can be defined in the SNMP Service Properties Security page located in Computer Management under Services. The drive icon lights will not blink in Microsoft Internet Explorer unless **Play animations in web pages** is enabled in the Tools menu Internet Options under the Advanced tab in the Multimedia section.

Logical Drive Information

Select one of the listed logical drives to see more information about the drive.

Spare Information

This section provides additional information about the spare drive, including status and the number of physical drives it will replace, if any. This section is available only if this physical drive is configured as a spare drive. The following information is available:

Status—Displays the status of the on-line spare drive. The following values are possible:

- **Building**—A physical drive has failed. Automatic Data Recovery is in progress to recover data to the on-line spare.
- **Active**—A physical drive has failed. Automatic Data Recovery is complete. The system is using the on-line spare as a replacement for the failed drive.
- **Failed**—The on-line spare has failed and is no longer available for use.
- **Inactive**—The monitored system has an online spare configured, but is not currently in use.
- **Unknown**—You might need to upgrade your software.

When the status is **Building** the following will be displayed to indicate the progress of the Automatic Data Recovery.

- **Percent Rebuild Complete**—Displays the percent complete of the rebuild. When the value reaches 100, the rebuilding process is complete. The drive array continues to operate in interim recovery mode during the rebuild.

Replaced Drives—Identifies the failed physical drives in the logical drive that the spare drive has replaced. Use this monitored item to identify the failed drives and replace those drives as soon as possible.

If N/A displays, the spare has not begun operating in place of the failed drive.

Predictive Indicators

Use the Predictive Indicators to predict when a drive, which is now operating normally, might need to be replaced.

S.M.A.R.T. Status—Displays the S.M.A.R.T. status as reported by the physical drive. This is only displayed if the drive supports S.M.A.R.T. predictive failure. The possible values are:

- **Other**—The Storage Agent is unable to determine the status of S.M.A.R.T. predictive failure monitoring for this drive.
- **OK**—Indicates the drive is functioning properly.
- **Replace Drive**—Indicates that the drive has a S.M.A.R.T. predictive failure error and should be replaced.

The following predictive indicators will not be displayed if the physical drive does not support any of the indicators and S.M.A.R.T. status is available.

The numerical data associated with these items displays after the item name. For example, **Used Realloc: 122** means that there are 122 used reallocation sectors for this drive. The status of these items can be **OK** or **Replace Drive**. If the status is **Replace Drive**, replace the drive, or an actual drive failure might occur in the future. The Predictive Indicators are:

Functional Test 1, 2, and 3 provides information about a series of tests that indicates how well a physical drive works. The Status of these items can be **OK** or **Replace Drive**. If the status is **Replace Drive**, replace the drive, or an actual drive failure might occur in the future.

These tests compare the way the physical drive currently operates when performing various tasks with the way it worked when it was new.

Used Realloc—Displays the number of sectors of the reallocation area that have been used by the physical drive. The Status of this item can be **OK** or **Replace Drive**. If the status is **Replace Drive**, replace the drive, or an actual drive failure might occur in the future.

Because of the nature of magnetic disks, certain sectors on a drive might have media defects. The reallocation area is part of the drive that the drive manufacturer sets aside to compensate for these defects. The array controller writes information addressed from the unusable sectors to available sectors in the reallocation area. If too many sectors have been reallocated, there might be a problem with the drive.

Spinup Time—Displays the time it takes for a physical drive to spin up to full speed. The status of this item can be **OK** or **Replace Drive**. If the status is **Replace Drive**, replace the drive, or an actual drive failure might occur in the future.

Drives require time to gain momentum and reach operating speed. As cars are tested to go from 0 mph to 60 mph in x number of seconds, drive manufacturers have preset expectations for the time it takes the drive to spin to full speed. Drives that do not meet these expectations might have problems.

The value is shown in tenths of a second. Thus, if the drive took 12 seconds to spin up, the value would be 120.

Problem Indicators

Use the Problem Indicators to determine when a drive failure has occurred that might be correctable without replacing the drive. The Problem Indicators are:

Fail Recov Reads—Displays the number of read errors that occurred while Automatic Data Recovery was being performed from this physical drive to another drive. If a read error occurs, Automatic Data Recovery stops.

Other Timeouts—Displays the number of times the drive did not respond with an interrupt within a controller-defined period of time after a command had been issued. This monitored item does not include DRQ timeouts.

If the count is not zero and the drive has failed, you might be able to correct the problem without replacing the drive.

1. Ensure that all system and storage system cables are intact and seated properly. You might need to replace the cables.
2. Ensure that a supported storage system is plugged in and powered on. Be sure the power supply is functioning.

IMPORTANT: Never turn off a storage system when the attached system is still turned on.

3. Check the physical proximity of the system to other electrical devices. Since electrical noise might cause this error, check the AC circuit for other electrical devices.
4. Timeouts can be caused when two or more drives are set to the same SCSI ID. Ensure that the ProLiant and system SCSI IDs do not conflict.
5. On a ProLiant Storage System, check the SCSI ID cable on the drive tray. If the cable is damaged or incorrectly installed, SCSI Timeouts can occur. Refer to the documentation accompanying the Hot-Plug Drive Tray Service Spare Kit.
6. Be sure that the system temperature is within specified limits. Ensure that the fans are operating and are not blocked.
7. In some instances, drive failure can cause Timeouts. If you continue to receive many of these errors, replace the drive.

You can reset Other Timeouts using System Diagnostics. Follow these steps for System Diagnostics 8.19 or later:

1. Reboot the system with the System Diagnostics diskette in drive A.
2. Press **Enter** at the Welcome screen.
3. At the Main menu, select **(Computer Checkup) Test**.
4. Select **Continue** at the Note: screen.
5. Select **Prompted Diagnostics** at the next screen. Select **Continue** at any Warning panels that might display.
6. At the Test Options screen, select **Interactive Testing (single device)**.
7. At the Device Selection menu, select the type of drive that indicated Other Timeouts.
8. At the Test Selection menu, select **Drive Monitoring Diagnostics Test**.
9. If the next screen offers you a choice of logical drives, select the logical drive associated with the physical drive indicating Other Timeouts or select **Test All Drives**.
10. Diagnostics will display the 1736-22 error if Other Timeouts are discovered. Press **Enter**.
11. Select **Yes** at the next screen to reset Other Timeouts.

SCSI Bus Faults—Displays the number of times that SCSI bus parity, overrun, or underrun errors have been detected on the SCSI bus. Since the controller will retry the operation, SCSI bus faults can cause a drop in performance, or, in some cases, data corruption.

If the count is not zero and the drive has failed, you might be able to correct the problem without replacing the drive. Follow the steps below:

1. Be sure that all system and storage system cables are intact and seated properly. You might need to replace the cables.
2. Check the physical proximity of the system to other electrical devices. Since electrical noise might cause a Bus Fault error, check the AC circuit for other electrical devices.
3. Be sure that the system temperature is within specified limits. Ensure that fans are operating and are not blocked.
4. SCSI Bus Faults can be caused when two or more drives are set to the same SCSI ID. Be sure that ProLiant and system SCSI IDs do not conflict.
5. In some instances, drive failure can cause SCSI Bus Faults. If you continue to receive many of these errors, replace the drive.

NOTE: If the drive has not failed, the above counts simply provide a cumulative record of past errors that have been corrected.

Failure Indicators

Use the Failure Indicators to determine the cause of a drive failure. Typically, the number of failures is zero when the drive is operating normally. If a counter is not zero and the drive has not failed, there could be an intermittent problem that might require the drive to be replaced. The Failure Indicators are:

- **Spinup Errors**—When the physical drive fails because a spin-up command has failed, a Spinup Error occurs. If the count is not zero and the drive has failed, replace the drive.

If the failure count is not zero and the drive is OK (has not failed), there might be an intermittent problem that requires drive replacement. If you observe that the count is increasing over time, replace the drive.
- **Aborted Commands**—The Aborted Commands counter records the number of times that a physical SCSI drive returned an Aborted Command status when a SCSI command was attempted. This error count indicates unsuccessful termination of the SCSI command. When the physical drive is failed because of aborted commands that could not be retried successfully, Aborted Commands errors occur. If the count is not zero and the drive has failed, replace the drive.

If the number of aborted commands is not zero and the drive is OK (has not failed), there might be an intermittent problem that requires drive replacement. If you observe that the count is increasing over time, replace the drive.
- **Format Errors**—When a format operation fails because the controller was unable to remap a bad sector, a Format Error occurs.

If the number of format errors is not zero and the drive has failed, replace the drive. If the counter is not zero and the drive is OK (has not failed), there might be an intermittent problem that requires drive replacement. If you observe that the count is increasing over time, replace the drive.
- **Hardware Errors**—The Hardware Errors counter records the number of times that a physical SCSI drive returned a Hardware Error status when a SCSI command was attempted. This error status indicates unsuccessful termination of the SCSI command. The controller typically retries this command several times before failing the drive. If the count is not zero and the drive has failed, replace the drive.

If the number of hardware errors is not zero and the drive is OK (has not failed), there might be an intermittent problem that requires drive replacement. If you observe that the count is increasing over time, replace the drive.
- **Not Ready Errors**—When a physical drive returns a “not ready” status when it should be ready, a Drive Not Ready Error occurs. This error could occur if a drive spins down unexpectedly, or if the drive never becomes ready after the spin up command is issued.

If the number of not ready errors is not zero and the drive has failed, replace the drive. If the counter is not zero and the drive is OK (has not failed), there might be an intermittent problem that requires drive replacement. If you observe that the count is increasing over time, replace the drive.

- **Bad Target Errors**—When a physical drive performs an action that does not conform to the SCSI-2 port protocol, the SCSI port is reset. If the count is not zero and the drive has failed, replace the drive.

If the number of bad target errors is not zero and the drive is OK (has not failed), there might be an intermittent problem that requires drive replacement. If you observe that the count is increasing over time, replace the drive.

- **Fail Recov Writes**—Indicates whether write errors occurred while Automatic Data Recovery was being performed to this physical drive. If a write error occurs, Automatic Data Recovery stops. These errors indicate that the physical drive has failed.

If the number of fail recov writes is not zero and the drive has failed, replace the drive. If the counter is not zero and the drive is OK (has not failed), there might be an intermittent problem that requires drive replacement. If you observe that the count is increasing over time, replace the drive.

- **Media Failures**—When this physical drive is failed due to unrecoverable media errors, a Media Failure occurs.

If the number of media failure errors is not zero and the drive has failed, replace the drive. If the counter is not zero and the drive is OK (has not failed), there might be an intermittent problem that requires drive replacement. If you observe that the count is increasing over time, replace the drive.

Statistics

This section displays statistics about a specific drive array controller physical drive. You can use the run-time statistics to monitor the health of a specific drive. The following information displays.

Sectors Read—Displays the total number of sectors read from the physical drive since the drive was stamped. The drive was stamped when it left the factory or when you ran System Diagnostics on your new drive.

Hard Read Errors—Displays the number of read errors that could not be recovered by a physical drive's ECC algorithm or through retries. Over time, a drive might produce these errors. If you receive these errors, a problem might exist with your drive.

The severity of these errors depends on whether the managed system is running in a fault tolerant mode. With fault tolerance, the controller can remap data to eliminate the problems caused by these errors.

Recovered Read Errors—Displays the number of read errors corrected through physical drive retries. Over time, all drives produce these errors. If you notice a rapid increase in the value for Recovered Read Errors or Hard Read Errors, a problem might exist with the drive. Expect more errors for this monitored item than for Hard Read Errors.

Total Seeks—Displays the total number of seek operations during seek tests performed by the physical drive since the drive was stamped. The drive was stamped when it left the factory or when you ran System Diagnostics on your new drive.

During normal reads and writes to the drive, the drive does implied seeks to the location where data resides. These are not included in this count.

Seek Errors—Displays the number of seek errors that a physical drive detects. A seek error is a seek that failed. Over time, a drive usually produces these errors. If you notice a rapid increase in the value shown for Seek Errors, this physical drive might be failing. Only an unusually rapid increase in these errors indicates a problem.

Sectors Written—Displays the total number of sectors written to the physical drive since the drive was stamped. The drive was stamped when it left the factory or when you ran System Diagnostics on your new drive.

Hard Write Errors—Displays the number of write errors that could not be recovered by a physical drive. Over time, a drive might produce these errors. If you notice an increase in the value shown for Hard Write Errors or Recovered Write Errors, a problem might exist with the drive. On average, these errors should occur less frequently than read errors.

Recovered Write Errors—Displays the number of write errors corrected through physical drive retries or recovered by a physical drive on a monitored system. Over time, a drive might produce these errors. If you notice an increase in the value shown for Recovered Write Errors or Hard Write Errors, a problem might exist with the drive.

The value increases every time the physical drive detects and corrects an error. Only an unusually rapid increase in these errors indicates a problem. On average, these errors should occur less frequently than read errors.

Hot-Plug Count—Indicates the number of times this physical drive was removed by a hot-plug event from a ProLiant Storage System since the drive was stamped. The drive was stamped when it left the factory or when you ran System Diagnostics on your new drive.

Logical Drive Information

A list of logical drives associated with the controller displays in the Mass Storage submenu. Each logical drive in the list displays the condition, the logical drive number and the fault tolerance of that logical drive. Select one of the logical drive entries to display the following information.

Status—Displays the status of the logical drive. The logical drive can be in one of the following states:

- OK—The logical drive is in normal operation mode.
- Failed—More physical drives have failed than the fault tolerance mode of the logical drive can handle without data loss.
- Unconfigured—The logical drive is not configured.
- Interim Recovery—The logical drive is using Interim Recovery Mode. In Interim Recovery Mode, at least one physical drive has failed, but the logical drive's fault tolerance mode lets the drive continue to operate with no data loss.
- Ready for Rebuild—The logical drive is ready for Automatic Data Recovery. The physical drive that failed has been replaced, but the logical drive is still operating in Interim Recovery Mode.
- Rebuilding—The logical drive is currently doing Automatic Data Recovery. During Automatic Data Recovery, fault tolerance algorithms restore data to the replacement drive.
- Wrong Drive—The wrong physical drive was replaced after a physical drive failure.
- Bad connect—A physical drive is not responding.
- Overheating—The drive array enclosure that contains the logical drive is overheating. The array is still functioning, but should be shut down.
- Shutdown—The drive array enclosure that contains the logical drive has overheated. The logical drive is no longer functioning.
- Expanding—The logical drive is currently doing Automatic Data Expansion. During Automatic Data Expansion, fault tolerance algorithms redistribute logical drive data to the newly added physical drive.
- Not available—The logical drive is currently unavailable. If a logical drive is expanding and the new configuration frees additional disk space, this free space can be configured into another logical volume. If this is done, the new volume will be set to Not Available.
- Queued for Expansion—The logical drive is ready for Automatic Data Expansion. The logical drive is in the queue for expansion.

When the status is Rebuilding the following will be displayed to indicate the progress of the operation.

- **Percent Rebuild Complete**—Displays the percent complete of the rebuild. When the value reaches 100, the rebuilding process is complete. The drive array continues to operate in interim recovery mode while the drive is rebuilding.
- **Rebuilding Drive**—Identifies the physical drive that failed. The logical drive is rebuilding using a spare drive in place of this failed drive.

When the status is Expanding the following will be displayed to indicate the progress of the operation.

- **Percent Expand Complete**—Displays the percent complete of the expansion. When a logical volume is expanding, the drive must redistribute the logical volume data across the physical drives. When the value reaches 100, the expansion process is complete.

Fault Tolerance—Displays the fault tolerance mode of the logical drive. To change the fault tolerance mode, run the System Configuration Utility.

The following values are valid for the Logical Drive Fault Tolerance:

- **None**—Fault tolerance is not enabled (referred to as RAID 0). If a physical drive reports an error, the data cannot be recovered by the drive array controller.
- **Mirroring**—For each physical drive, there is a second physical drive containing identical data (also known as RAID 1). If a drive fails, the data can be retrieved from the mirrored drive.
- **Data Guarding**—One of the physical drives is used as a data guard drive and contains the exclusive OR of the data on the remaining drives (also known as RAID 4). If a failure is detected, the drive array controller rebuilds the data using the data guard information plus information from the other drives.
- **Distributed Data Guarding**—Distributed data guarding (sometimes referred to as RAID 5) is similar to data guarding, but instead of storing the parity information on one drive, the information is distributed across all of the drives. If a failure is detected, the Drive Array Controller rebuilds the data using the data guard information from all the drives.
- **Advanced Data Guarding**—(RAID ADG) is the fault tolerance method that provides the highest level of data protection. It stripes data and parity across all the physical drives in the configuration to ensure the uninterrupted availability of uncorrupted data. This fault-tolerance method is similar to RAID 5 in that parity data is distributed across all drives in the array, except in RAID ADG the capacity of multiple drives is used to store parity data. Assuming the capacity of two drives is used for parity data, this allows continued operation despite simultaneous failure of any two drives in the array, whereas RAID 4 and RAID 5 can only sustain failure of a single drive.
- **Unknown**—You might need to upgrade your software.

Capacity—Displays the size of the logical drive in megabytes. For example, 120 indicates that the logical drive is 120 megabytes. Use this data to determine whether the drive will be large enough to accommodate your needs.

The capacity utility defines a megabyte as 1,048,576 bytes. The capacity value shown might differ from the stated size of the drive due to different definitions of a megabyte. Many hardware manufacturers use the value of 1,000,000 for megabyte instead of 1,048,576.

Accelerator—Indicates whether the logical drive has an Array Accelerator board configured and enabled. The following values are valid:

- Enabled—The Array Accelerator board is configured and enabled for this logical drive. Run the System Configuration Utility to change this value.
- Disabled—The Array Accelerator board is configured but not enabled for this logical drive. Run the System Configuration Utility to change this value.
- Unavailable—There is no Array Accelerator board configured for this logical drive.
- Unknown—The Storage Agents do not recognize the Array Accelerator board. You might need to upgrade your software.

Stripe Size—Displays the size of a logical drive stripe in kilobytes.

Identify Drive

Select the length of time to blink the LEDs of a physical drive that make up the logical drive from the dropdown list box and then click the **Start** button. The page will automatically refresh and display an image of a blinking drive and a Stop button. Click the **Stop** button to end blinking before the time expires.

After the drive lights stop blinking the page will have to be manually refreshed to display the Start button. There might be a delay, depending on the length of the Insight Management Agents data collection interval, after the drive lights stop blinking and before the Start button appears.

Only drives in hot-plug trays are supported since the LEDs are part of the tray. Spare drives that are included in the logical drive will also blink. Only one logical drive on a selected controller might be identified at a time. If a different drive is selected while another drive is currently blinking then the other drive will stop blinking and the selected drive will blink.

IMPORTANT: The Start or Stop button only appears if you are logged on as an administrator or an operator, SNMP sets are enabled, and a SNMP Community string has been defined with “write” access. Go back to the Summary page and select **login** to login as an administrator or operator. SNMP sets can be enabled in the Insight Management Agents for Servers control panel applet on the SNMP Settings page. A SNMP Community string with “write” access can be defined in the SNMP Service Properties Security page located in Computer Management under Services. The drive icon lights will not blink in Microsoft Internet Explorer unless **Play animations in web pages** is enabled in the Tools menu Internet Options under the Advanced tab in the Multimedia section.

Physical Drives

Select one of the listed physical drives to see more information about the drive.

Spare Drives

Select one of the listed spare drives to see more information about the drive.

Associated Source Logical Drive

Select the listed source logical drive to Refer to the logical drive information for the source logical drive.

Associated Snapshot Resource Volume

Select the listed snapshot resource volume to Refer to the logical drive information for the snapshot resource volume.

Snapshot Resource Volumes

A list of snapshot resource volumes associated with the controller displays in the Mass Storage submenu if there are any snapshot resource volumes configured. Each snapshot resource volume in the list displays the condition, the logical drive number and the fault tolerance of that snapshot resource volume. Select one of the snapshot resource volume entries to display logical drive information, the Snapshot Resource Volume Information and the Snapshot Information.

Snapshot Resource Volume Information

The Snapshot Resource Volume Information includes the status, if creation is allowed, number of disabled instances, and total space, growth space and creation space available.

Status—Displays the status of the snapshot resource volume. The following values are valid:

- OK—The snapshot resource volume is in normal operation mode.
- Unknown Failure—Indicates an unknown failure has occurred.
- Resource Volume Disconnected—The snapshot resource volume has been disconnected from the source volume.
- Source Volume Not Located—The source volume could not be located.
- Resource Volume Not Located—The snapshot resource volume could not be located.
- Source Volume Failed—The source volume has failed.
- Resource Volume Failed—The snapshot resource volume has failed.
- Source Volume Not Available—The snapshot source volume is not available.
- Resource Volume Not Available—The snapshot resource volume is not available.
- Resource Volume Obsolete—The snapshot resource volume is obsolete.
- Resource Volume Obsolete and Failed—The snapshot resource volume is obsolete and failed.

- Unknown—The Storage Agents were unable to determine the status of the snapshot resource volume.

Disabled Instances—Displays the number of disabled snapshot instances on this snapshot resource volume.

Snapshot Creation—Indicates if snapshot creation is allowed on this resource volume. The following values are valid:

- Allowed—Snapshot creation is allowed.
- Not Allowed—Snapshot creation is not allowed.
- Unknown—The Storage Agents were unable to determine if snapshot creation is allowed on this snapshot resource volume.

Total Space—Displays the total amount of space available in the snapshot resource pool.

Growth Space—Displays the amount of space available for the current active snapshot.

Creation Space—Displays the amount of space available for new snapshot creation.

Snapshot Information

The Snapshot Information includes the instance number, space used, creation date and time, if it is mounted, and type of access allowed.

Instance—Displays the snapshot instance number.

Space Used—Displays the amount of space used by the snapshot.

Date Time—Displays the date and time the snapshot was created.

Mounted—Indicates if the snapshot is currently mounted. The following values are valid:

- Mounted—The snapshot is currently mounted.
- Not Mounted—The snapshot is not currently mounted.
- Unknown—The Storage Agents were unable to determine if the snapshot is mounted or not mounted.

Access—Indicates the current access for the snapshot. The following values are valid:

- Read/Write—The current snapshot access is read/write.
- Read Only—The current snapshot access is read only.
- Unknown—The Storage Agents were unable to determine the current access of the snapshot.

Fibre Channel Switch Information

The Fibre channel switch information includes the name, location, storage system slot, worldwide node name, worldwide port name, IP address, subnet mask, and gateway address. If the IP address is configured, a Configure Switch button appears.

Firmware Revision—Displays the firmware revision of the switch.

Location—Indicates the switch location if it resides within an external array storage system. The following values are valid:

- **Internal**—The switch is located inside the external array storage system chassis.
- **External**—The switch is located outside the external array storage system chassis.
- **Unknown**—The switch does not reside within an external array storage system chassis or the Storage Agents were unable to determine the location of the switch.

Network Link Status—Displays the network connection link status of the switch. The following values are valid:

- **Active**—The network connection link status is active.
- **Inactive**—The network connection link status is inactive.
- **Unknown**—The Storage Agents were unable to determine the network connection link status of the switch.

Connection Status—Displays the Fibre channel connection status of the switch. The following values are valid:

- **OK**—The Fibre channel connection status is ok.
- **Offline**—The Fibre channel connection status is offline.
- **Unknown**—The Storage Agents were unable to determine the Fibre channel connection status of the switch.

Storage System Slot—Displays the physical slot number of the storage system in which this switch resides. If the switch does not reside inside a storage system chassis then N/A will be displayed.

World Wide Node Name—Displays the worldwide node name of the switch.

World Wide Port Name—Displays the worldwide port name of the switch.

IP Address—Displays the IP address of the switch.

Subnet Mask—Displays the IP subnet mask of the switch.

Gateway Address—Displays the gateway IP address of the switch.

Manage Switch—A link to the management application for the switch. Clicking on the button will launch a separate browser window and load the management application for the switch.

If the IP address, subnet mask, and gateway address have not been configured or the Network Link Status is inactive you will not be able to launch the management application. The switch must be connected to a network and the switch must be configured by the Array Configuration Utility XE 1.30 or later before the management application can be launched from the browser.

RAID Array Storage Systems

Select the RAID Array Storage Systems item from the Mass Storage submenu to display the following information for each storage system:

Name—Identifies the type of storage system for identification purposes.

Status—Displays the current status of the storage system. The following values are valid:

- Good—Indicates that the system is working properly.
- Warning—indicates that at least one component of the system failed.
- Agent Not Running—Indicates that the StorageWorks Agent is not running. You must restart the StorageWorks Agent.
- Communication Loss—Indicates that the storage system has a communication or cable problem. Check all cable connections to the host server.
- Unknown—Indicates that the Storage Agent does not recognize the state of the storage system. You might need to upgrade the Storage Agents.

Controller 1 Serial #—The storage system's first controller serial number which can be used for identification purposes.

Controller 2 Serial #—The storage system's second controller serial number which can be used for identification purposes.

External Storage Connections

Select the External Storage Connections item from the Mass Storage menu to display the host controllers installed in the system and the host controller's current condition and model name.

Fiber Channel Connections

The following information is displayed for the external storage connections to the fiber channel host controller.

Status—Displays the status for this controller. The following values are valid:

- OK—Indicates the host controller is operating normally.
- Failed—Indicates the host controller has failed and should be replaced.
- Shutdown—Indicates the host controller has been shut down.
- Loop Degraded—Indicates the Fibre channel connection is degraded.
- Loop Failed—Indicates the Fibre channel connection is failed.
- Unknown—Indicates the Storage Agents cannot determine the status of the host controller.

Serial Number—Displays the serial number of the host controller. The serial number is not available for all host controllers. In this case N/A will be displayed.

Location—Displays the physical slot where the host controller resides in the system. For example, if this value is three, the controller is located in slot three of your computer.

World Wide Port Name—Displays the unique Fibre Channel port name for this controller.

World Wide Node Name—Displays the unique Fibre Channel node name for this controller.

Storage Systems—Displays all of the attached storage systems. Select a storage system entry to display the related Storage System Information.

IO Slot—Displays the storage system I/O slot number that is connected to the host controller.

Tape Controllers—Displays all of the Fibre Channel tape controllers attached to the host controller. Select a tape controller entry to display the related Tape Controller Information.

Switches—Displays all of the supported Fibre channel switches attached to the host controller. Select a switch to display the related Fibre Channel Switch Information.

Array Controller Connections

The following information is displayed for the external storage connections to the host array controller.

Status—Displays the status for this controller. The following values are valid:

- OK—The array controller is operating properly.
- General Failure—The array controller has failed.
- Cable Problem—The array controller has a cable problem. Check all cables to the controller.
- Powered Off—The array controller does not have power. Replace the controller and restore power to the controller's slot.
- Unknown—Indicates that the Storage Agents are unable to determine the status of the controller. You might need to upgrade the Storage Agents.

Firmware Version—Lists the firmware version of the array controller. This value can be used to help identify a particular revision of the controller.

Location—Displays the physical slot where the array controller resides in the system. For example, if this value is three, the controller is located in slot three of your computer.

Serial Number—Displays the serial number of the array controller. The serial number is not available for all host controllers. In this case N/A will be displayed.

Storage System—Displays the attached storage system. Select the storage system entry to display the related Storage System Information.

Controller Bus—Displays the array controller's bus number for the connection to this storage system.

The condition of the connection path, the storage system I/O slot number and the status of each connection path to the storage system is displayed. The following values are valid for the connection path status:

- OK—The connection path is operating properly.
- Offline—The connection path is offline.
- Unknown—Indicates that the Storage Agents are unable to determine the status of the connection path. You might need to upgrade the Storage Agents.

Fibre Channel Tape Controllers

This section displays general and status information about Fibre Channel tape controllers. Select a Fibre Channel tape controller entry from the Mass Storage list to display a submenu containing separate entries for tape controllers, tape storage systems, and tape drives. The following items display:

- Tape Controller Information
- Tape Storage System Information
- Tape Drive information

Tape Controller Information

Select the tape controller item from the Mass Storage submenu to display the following information:

Controller Status—Displays the status of the tape controller. The following values are valid:

- OK—The tape controller is operational.
- Offline—The tape controller is offline. The tape controller might be powered off or there might be a cabling problem.
- Unknown—The agent cannot determine the status of the tape controller.

Firmware Version—Displays the tape controller firmware revision number. If the worldwide name is not supported, this field displays N/A.

World Wide Name—Displays the worldwide name of the controller. This value can be used to further identify a particular tape controller. If the worldwide name is not supported, this field displays N/A.

Serial Number—Displays the serial number for the tape controller. Use this value for identification purposes.

Tape Storage System Information

Select the Tape Storage System Information entry from the Mass Storage submenu to display the following information.

Status—Displays the status of the tape storage system. The following values are valid:

- OK—Indicates that the library is operating normally.
- Degraded—Indicates the library has degraded in some manner.
- Failed—Indicates the library has failed and can no longer return data. The library might need to be replaced.
- Offline—Indicates the Storage Agents can no longer communicate with the library. This could be caused by a cabling problem or the library might be powered off.
- Unknown—The state of the tape library cannot be determined. You might need to upgrade the Storage Agents.

Model—Displays the model name of the tape library. Use this value for identification purposes.

Firmware Revision—Displays the firmware revision level of the tape library. The level can be used for identification purposes.

Serial Number—Displays the unit serial number for the tape library. Use this value for identification purposes.

Service Hours—Displays the number of hours of operation for the library.

Total Moves—Displays the number of tape moves for the library loader arm.

Door Status—Displays the status of the door. The following values are valid:

- Not Supported—The device does not support the door status.
- Closed—The door is closed.
- Open—The door is open.
- Unknown—The state of the tape library door cannot be determined. You might need to upgrade the Storage Agents.

Temperature—Displays the tape library temperature status. The following values are valid:

- OK—Indicates that the temperature of the library is within normal operating limits.
- Safe Temperature Exceeded—Indicates that the temperature of the library has exceeded the safe operational temperature. The library will continue to operate under this warning.
- Maximum Temperature Exceeded—Indicates that the temperature of the library has exceeded the normal operating limits to the extent that the library might no longer function.
- Not supported—Indicates that the library cannot detect or report the temperature status.
- Unknown—The temperature status of the tape library cannot be determined. Ensure the latest drivers and Storage Agents are installed.

Redundancy—Displays the tape library redundancy status, which denotes the presence of internal redundant components such as fans, power supplies, etc. The following values are valid:

- Active—Indicates that the library is capable of detecting and reporting redundant components, there are enough redundant units installed, and redundancy is active.
- Capable—Indicates that the library is capable of detecting and reporting redundant components but there are not enough redundant units installed to make redundancy active.
- Not capable—Indicates that the library is capable of detecting and reporting redundant components but there are no components that support redundancy.
- Not supported—Indicates that the library cannot detect or report redundancy status.
- Unknown—The redundancy status of the tape library cannot be determined. Be sure the latest drivers and Storage Agents are installed.

Hot Swap—Displays the tape library hot swap status which denotes the presence of hot swappable internal components, such as drives, fans, power supplies, etc. The following values are valid:

- Capable—Indicates that the library is capable of detecting and reporting hot swappable internal components and has at least one hot swappable component.
- Not capable—Indicates that the library is capable of detecting and reporting hot swappable internal components but there are no hot swappable components installed.
- Not supported—Indicates that the library cannot detect or report hot swap status.
- Unknown—The hot swap status of the tape library cannot be determined. Ensure the latest drivers and Storage Agents are installed.

Last Known Error—Displays the last error returned by the tape library.

Associated Tape Drives—Displays a list of tape drives associated with the tape storage system.

Tape Drive Information

Select one of the tape drive entries from the Mass Storage submenu to display the following information about that drive.

Status—displays the status of the tape drive. The following values are valid:

- OK—Indicates the tape drive is operating normally.
- Degraded—Indicates the tape drive has degraded in some manner.
- Failed —Indicates the tape drive has failed and can no longer return data. The tape drive might need to be replaced.
- Offline—Indicates the Storage Agents can no longer communicate with the tape drive. This could be caused by a cabling problem or the tape drive might be powered off.
- Missing—Was OK—Indicates that a tape drive that was located in a system and had a status of OK has been removed.
- Missing—Was Offline—Indicates that a tape drive that was located in a system and had a status of offline has been removed.
- Unknown—The state of the tape drive cannot be determined. You might need to upgrade the Storage Agents.

Model—Displays the model name of the tape drive. Use this value for identification purposes.

Firmware Revision—Displays the firmware revision level of the tape drive. Use this value for identification purposes.

Serial Number—Displays the unit serial number for the tape drive. Use this value for identification purposes.

Current Width—Displays the current negotiated data transfer width for the tape drive. The possible values are:

- Narrow (8 bits)—The negotiated data transfer width for this drive is narrow (8 data bits).
- Wide (16 bits)—The negotiated data transfer width for this drive is wide (16 data bits).
- Unknown—The Storage Agents are unable to determine the current negotiated data transfer width for this drive.

Current Speed—Displays the current negotiated data transfer speed for the tape drive. The possible values are:

- Asynchronous—The current data transfer speed for this drive is asynchronous.
- Fast—The current data transfer speed for this drive is 10 million transfers per second.
- Ultra—The current data transfer speed for this drive is 20 million transfers per second.
- Ultra2—The current data transfer speed for this drive is 40 million transfers per second.
- Ultra3—The current data transfer speed for this drive is 80 million transfers per second.
- Unknown—The agent is unable to determine the current negotiated data transfer speed for this drive.

NOTE: If the current data transfer width is Narrow (8 bits) then the speed in megabytes per second is equal to the million transfers per second speed. If the current width is Wide (16 bits) then the speed in megabytes per second is twice the million transfers per second speed. For example, if the current speed is Ultra and the width is Wide then the speed would be 40 megabytes per second.

Library Drive—Indicates whether the tape drive is included in a tape library. The following values are valid:

- Yes—The tape drive is included in a tape library.
- No—The tape drive is not included in a tape library.
- Unknown—The Storage Agents are unable to determine if the tape drive is included in a tape library.

Hot Plug—Indicates whether the tape drive supports hot-plug replacement. The following values are valid:

- Yes —The tape drive supports hot-plug replacement.
- No—The tape drive does not support hot-plug replacement.
- Unknown—The Storage Agents are unable to determine if this drive supports hot-plug replacement.

Drive Bay—Displays the bay number where the tape drive is located for drives in a hot-plug storage system.

Tape Drive Error Counts

Tape Errors—Displays the total number of read and write errors encountered. This value is maintained from the moment the Tape Hardware Interface driver was loaded.

Tape errors might occasionally occur. If this value rises dramatically, clean the device. If you continue to have errors, you might have a problem. Some common causes of tape errors include RFI on the bus cables, bad or missing terminating resistors on the drives, or having more than one device with the same SCSI ID. Ensure the bus cable is free of obstructions and that the devices on the bus are properly configured.

Uncorrectable—Displays the total number of read and write errors that could not be corrected. This value is maintained from the moment the Tape Hardware Interface driver was loaded.

Uncorrectable errors might occasionally occur. If this value rises dramatically, clean the device. If you continue to have errors, you might have a problem. Some common causes of uncorrectable errors include RFI on the bus cables, bad or missing terminating resistors on the drives, or having more than one device with the same SCSI ID. Ensure the bus cable is free of obstructions and that the devices on the bus are properly configured.

Rereads—Displays the number of times blocks that had to be reread from the device. This value is maintained from the moment the Tape Hardware Interface driver was loaded.

Reread errors might occasionally occur. If this value rises dramatically, clean the device. If you continue to have rereads, you might have a problem. Some common causes include RFI on the bus cables, bad or missing terminating resistors on the drives, or having more than one device with the same SCSI ID. Ensure the bus cable is free of obstructions and that the devices on the bus are properly configured.

Rewrites—Displays the number of times blocks that had to be rewritten to the device. This value is maintained since the Tape Hardware Interface driver was loaded.

Re-write errors might occasionally occur. If this value rises dramatically, clean the device. If you continue to have rewrites, you might have a problem. Some common causes include RFI on the bus cables, bad or missing terminating resistors on the drives, or having more than one device with the same SCSI ID. Ensure the bus cable is free of obstructions and that the devices on the bus are properly configured.

Tape Drive Maintenance

Tape Drive Heads Need Cleaning—Indicates whether the tape drive heads must be cleaned. To clean the tape heads, insert a cleaning tape into the device and run through a cleaning cycle.

The following values are valid:

- **Yes**—The tape drive requires a cleaning tape session to clean the heads.
- **No**—The tape drive does not require any cleaning tape session.
- **Not Supported**—The tape drive does not support monitoring of the cleaning required status.

Cleaning Tape Needs Replacement—Indicates whether the cleaning tape that is inserted in an autoloader must be replaced because its cleaning capability is exhausted (it is at the end of the tape).

This variable can be in one of the following states:

- **Yes**—The autoloader tape drive requires a new cleaning tape to be inserted.
- **No**—The tape drive does not require a new cleaning tape.
- **Not Supported**—The tape drive does not support monitoring of the cleaning tape replacement status.

NOTE: This variable is only applicable to autoloader tape drives.

NIC Agent Information

NIC Subsystem

The Insight NIC Management Agents display all logical NICS that are configured on the system you are viewing. The following items appear in the NIC section of the navigation frame:

- Virtual NIC
- Single NIC
- Teams of NICs

Virtual NIC

The Virtual NIC is the TCP/IP Loopback interface. It is provided by operating systems to enable a computer to send packets to itself. A packet is the fundamental unit of transmission on the physical network.

Select the Virtual NIC to view detailed Interface Information.

Single NIC

A single NIC is composed of one physical adapter. Select a single NIC from the list to view more information about that NIC.

NOTE: The information displayed might vary depending on the type of NIC. For example, Ethernet Statistics appear for Ethernet adapters.

The following types of information are available depending on the type of NIC:

- NIC Controller Information
- NIC Interface Information
- Ethernet Statistics
- Token Ring Statistics

Teams of NICs

A team of NICs is composed of two or more physical adapters that present a single, logical interface on the network. Select a NIC team from the navigation frame to view detailed information about that team. The Logical Adapter Information appears by default. You can also select one of the physical adapters in the team to display additional information about that adapter.

There are three kinds of NIC teams:

- **Network Fault Tolerant Team**—The logical adapter has two or more physical adapters associated with it. One physical adapter is active on the network, and the other physical adapters are hot standbys.
- **Transmit Load Balancing Team**—The logical adapter has more than one physical adapter associated with it. One physical adapter transmits and receives data, while the others only transmit. If the receiving adapter fails, one of the other adapters assumes this role.
- **Switch-Assisted Load Balancing**—The logical adapter has more than one physical adapter associated with it. All physical adapters can receive and transmit data. This requires a switch that cooperates with the adapters. If any adapter fails, the load is spread among the remaining adapters.

The following types of information are available for a selected NIC team:

- Logical Adapter Information
- NIC Controller Information
- Ethernet Statistics

Logical Adapter Information

The following Logical Adapter Information is available for all NIC teams:

- **Description**—Displays a description of the NIC Team (Network Fault Tolerant Team, Transmit Load Balancing team, or Switch-Assisted Load Balancing Team).
- **Status**—Displays the overall status of the NIC team.
 - OK (green)
 - Degraded (yellow)
 - Failed (red)
 - Unknown (blue)
- **Group Type**—Displays the group type of the NIC team (Network Fault Tolerant, Transmit Load Balancing, or Switch-Assisted Load Balancing).

- **Switchover Mode**—Displays the method used to determine when traffic switches from one adapter to another. There are three types of Switchover Modes:
 - **Manual**—Indicates the logical adapter has more than one physical adapter associated with it. Network traffic only switches from the active adapter to the standby adapter under user control. This Switchover Mode is only available for Network Fault Tolerant Teams.
 - **Fail on Fault**—Indicates the logical adapter has more than one physical adapter associated with it. If the active adapter fails, network traffic automatically switches to a standby adapter. The standby adapter remains active until some action (such as manual switch or system restart) restores the primary adapter to active. This is the default Switchover Mode for all team types and is the only available Switchover Mode for Transmit Load Balancing Teams and Switch-Assisted Load Balancing Teams.
 - **Preferred Primary**—Indicates the logical adapter has more than one physical adapter associated with it. If the active adapter fails, network traffic automatically switches to a standby adapter. If the original primary adapter recovers from the failure, it automatically becomes active again. This Switchover Mode is only available for Network Fault Tolerant Teams.
- **Physical (MAC) Address**—Displays the physical address presented on the network by the logical team.

NIC Controller Information

The following information displays about NIC controllers.

- **Model**—Displays the NIC controller model, such as the Compaq NetFlex-2 Controller. Use this information for identification purposes.
- **Status**—Displays one of four valid states:
 - **OK**—The controller is operating normally.
 - **Failed**—The controller has failed and is no longer operating.
 - **Unknown**—You might need to upgrade your driver software or Insight NIC Agent. The Insight NIC Agent cannot determine the status of the controller.
 - **Link Failure**—Adapter does not have link.
- **Slot**—Displays the physical location of the NIC. For example, if this value is three, then the NIC is located in slot three of your computer. Use this information for identification purposes.

The NIC interface slot value is embedded if the NIC is integrated onto the system board. If the slot is unknown or the NIC is an ISA card, the slot value is N/A.
- **Port**—Displays the value one for a single-headed NIC, or the port number for a multiple-headed NIC.

- Duplex—Displays the current state of the Full Duplex Ethernet Support. NICs support the Full Duplex Ethernet if they are attached to a device that also supports Full Duplex.
The following duplex values are possible:
 - N/A—The Insight NIC Agent cannot determine the current state of the Full Duplex Ethernet Support. You might need to upgrade your software.
 - Not Supported—Either the hardware does not support duplex, or the Insight NIC Agent cannot determine the current state of the Full Duplex Ethernet Support for this NIC.
 - Half—The NIC is currently running in half duplex mode.
 - Full—The NIC is currently running in full duplex mode.
- Base I/O Address—Specifies the starting address of the I/O port used to communicate with this device. Use this information for identification purposes. No other device can use this I/O port address.
- IRQ—Displays the hardware interrupt that this NIC uses to communicate with the device driver. Use this information for reference purposes.
- Base Memory Address—Displays the base memory address used by this NIC. If this device does not use system memory or this information is unavailable, this value is N/A. Use this information for identification purposes.
- DMA Channel—Displays the number of the DMA channel used for this NIC. If this device does not use a DMA channel, or if this information is unavailable, this value is N/A. Use this information for identification purposes.
- Physical (MAC) Address—Displays the physical address presented on the network by the physical adapter.
- Role—Displays the following states:
 - Team Member—Any adapter in a Switch-Assisted Load Balancing Team.
 - Primary—The primary adapter in the group, or the only adapter in a group consisting of a single adapter. The primary adapter in a Fail-On-Fault group handles all the network traffic unless it fails. The primary adapter in a Transmit Load Balancing group receives all traffic. The physical address of this adapter is the default address of the group.
 - Secondary—In a Fail-On-Fault group, this is the standby adapter. This adapter does not handle network traffic, other than periodic test packets. In a Transmit-Load-Balancing group, this adapter is in a secondary role and transmits packets to increase bandwidth.

NIC Interface Information

This section of NIC Interface Information displays the following information:

- **Interface Status**—Displays one of the following states:
 - **Unknown**—Indicates that the interface status cannot be determined.
 - **OK**—Indicates that the interface is up.
 - **Degraded**—Indicates that the interface is up and functional, but performance and redundancy are degraded. This occurs when some physical interface team fails to operate.
 - **Failed**—Indicates that the interface is down and no network traffic is occurring. Error counts might help you determine if a problem has occurred. The software might not be configured properly.
- **Max Packet Size**—Displays the maximum-allowable packet size in bytes. Use this information to compare with other stations. In general, if you are using a high data-transfer application, a higher Max Packet Size provides better performance. If this item is 0, it cannot be obtained from the hardware or support software.
- **Last Status Change**—Displays the time at which the interface entered its current operational state. Use this item to determine the length of time the interface has remained in its current state. If the time when the interface entered its current operational state is unknown, N/A appears in this field.
- **Physical (MAC) Address**—Displays the physical address presented on the network by the physical adapter. Other devices cannot use this physical address resource. The address is usually burned onto the board, and can be used to map into network analyzer tools.
- **Speed**—Displays the nominal rate of speed of the NIC in megabits per second. For example, Token Ring speeds are typically 4 or 16 megabytes. Ethernet speed is typically 10 or 100 megabytes. If the value is 0, either the speed is 0 or the value is unobtainable from the hardware or support software.

Use this information to help you determine the configuration of the NIC. If an error appears under Ring Open Status in the Token Ring Status window, check the configured speed. The NIC might be set to the wrong speed if *Beaconing* or *Ring Failed* appears under Ring Open Status. For example, a conflict exists if the NIC is configured at 4 megabits per second and the Token Ring is set at 16 megabits per second.

Receive Statistics

- Bytes—Displays the number of bytes received.
- Total packets—Displays the total number of received packets.
- Unicast packets—Displays the number of received packets that have a single destination.
- Non-unicast packets—Displays the number of received packets that have multiple destinations.
- Discarded packets—Displays the number of received packets that are discarded.
- Error packets—Displays the number of received packets that have errors.
- Unknown protocols—Displays the number of received packets that have unknown protocols.

Transmit Statistics

- Bytes—Displays the number of bytes transmitted.
- Total packets—Displays the total number of transmitted packets.
- Unicast packets—Displays the number of transmitted packets that have a single destination.
- Non-unicast packets—Displays the number of transmitted packets that have multiple destinations.
- Discarded packets—Displays the number of transmitted packets that are discarded.
- Error packets—Displays the number of transmitted packets that have errors.
- Queue length—Displays the number of packets in the transmit queue.

Ethernet Statistics

Information about Receive Errors and Transmit Errors appears in the Ethernet Statistics window. Information indicated as N/A is unobtainable from the hardware or support software.

Receive Errors

- **Total Errors**—Displays the number of Ethernet errors received on this interface. The count includes alignment errors, FCS errors, frames that were too long, and MAC receive errors. This value is for total errors received on the interface. Since you might have multiple interfaces on one NIC, this value might not represent the total number of errors received by the NIC.

If the Total Errors value is 0, either no errors have been received or the information is unobtainable from the hardware or support software.

- **Alignment Errors**—Displays the number of alignment errors that have occurred for this interface since the network interface supporting software was loaded. The receiver checks the frame alignment after the packet has failed the Cyclical Redundancy Check (CRC). Misaligned packets do not end on an 8-bit boundary. All packets contain a set number of bytes and must end after a defined number of bytes. Packets that do not end on a byte boundary fail the alignment check.
- **FCS Errors**—Displays the number of FCS errors that have occurred for this interface since the network interface supporting software was loaded. The FCS field contains a 4-byte CRC value. The transmitting station calculates the CRC while sending the packet. The CRC value is placed in the FCS field. The receiving station calculates the CRC while receiving the packet and matches the resulting value against the contents of the FCS field. If the numbers do not match, a FCS error has occurred.

Track and resolve these errors. The two primary causes of FCS errors are cabling and component problems.

If you receive FCS errors, determine if Alignment errors or Late Collision errors have occurred. Cabling problems, such as shorts or noise caused by electromagnetic interference, are most likely to blame for CRC/Alignment errors. Improper cabling (not following cable specifications) is the most likely cause for late collisions.

- **Frame Too Long**—Displays the number of times a receiving station found an oversized frame for this interface since the network interface supporting software was loaded. To avoid processing corrupt packets, the receiving station checks several packet characteristics, including the frame size. If a frame is larger than 1518 bytes (including the FCS field), it is considered oversized. If the network is experiencing oversized frames:
 - a. Be sure you have the latest version of the LAN driver. A faulty LAN driver might cause oversized frames.
 - b. Check the routers. If a router connects two dissimilar network types and does not enforce the proper frame size restrictions on either side, it might transmit illegal-length frames. Check with the router manufacturer.
 - c. Use a network analyzer to find the NIC responsible for sending illegal-length frames. Examine the 48-bit source address in the frame header. This pinpoints the responsible NIC.

- **MAC Received Errors**—Increments each time an error occurs for this interface that does not fall into any of the other error categories shown on the screen. For example, this value increases if a frame that is too short is detected. If you see an excessive number of MAC Received errors, use a network analyzer to check for short frame errors. The NIC might need to be replaced.

Transmit Errors

- **Total Errors**—Displays the total number of Ethernet errors generated from this interface. This count includes carrier sense errors, late collisions, excessive collisions, MAC transmit errors, multiple collision frames, single collision frames, and deferred transmits. This value is for total errors transmitted on the interface. Since you might have multiple interfaces on one NIC, this value might not represent the total number of errors transmitted by the NIC.

If the Total Errors value is 0, either no errors have been received or the information is unobtainable from the hardware or support software.

- **Carrier Sense Errors**—Displays the number of frames transmitted with carrier sense errors for this interface since the network interface supporting software was loaded. The carrier sense signal is an ongoing activity of a data station that detects whether another station is transmitting. Carrier sense errors are detected when a station transmits a frame and does not detect its own signal on the wire.
- **Late Collisions**—Displays the number of late collisions that have occurred for this interface since the network interface supporting software was loaded. Late collisions might be a symptom of cabling problems. A late collision is one that occurred 64 bytes or more into the packet.

Late collisions might indicate that a segment is longer than allowed by the wiring specifications. For example, if you are using 10Base-2 wiring, also known as Thinnet, the maximum segment length is 185 meters.

A station assumes control of the cable segment if it has already transmitted 64 bytes. If another node at the far end of the segment has not yet seen the packet and transmits, this packet collides with the first transmission after the first 64 bytes are sent.

Be sure that your segment length does not exceed the maximum length allowed.

Because the location of cabling problems can be very difficult to detect on an Ethernet network, shorten an Ethernet segment (remove portions of the network to isolate problems) until the problems are no longer seen, and then expand the network until the problem recurs.

- **Excessive Collisions**—Displays the number of Excessive Collisions that have occurred for this interface since the network interface supporting software was loaded. A station might attempt to transmit up to 16 times before it must abort the attempt. After the abort occurs, the Excessive Collision counter increases.

If you see an increase in deferred transmissions as well as excessive collisions, your network is extremely busy and this segment of the LAN is overcrowded. Reduce the traffic by reorganizing your LAN or adding a NIC to the device. For example, if you have 100 stations on one Ethernet bus, break the bus into two Ethernet buses by adding a NIC to your device. This balances the load by putting 50 stations on one bus and 50 on the other. If there are a few isolated stations creating the traffic, put those stations on a separate bus.

Faulty components might be the cause of excessive collisions.

- **MAC Transmit Errors**—Increments each time an error occurs for this interface that does not fall into any of the other error categories shown on the screen. An excessive number of MAC Transmit errors might indicate a problem with the NIC. Check the cabling. You might need to replace the NIC.
- **Multiple Collision Frames**—Displays the number of multiple collisions that have occurred for this interface since the network interface supporting software was loaded. Multiple collisions are frames involved in more than one collision before being successfully transmitted. These errors mean that the network is experiencing moderate to heavy traffic. If multiple collisions become more frequent, the count for excessive collisions escalates.
- **Single Collision Frames**—Displays the number of single collisions that have occurred for this interface since the network interface supporting software was loaded. Single collisions are frames that are involved in a single collision and then are transmitted successfully. These errors show that the network has light to moderate traffic. If single collisions become more frequent, the count for multiple collisions escalates.
- **Deferred Transmits**—Displays the number of frames that were deferred before transmission because the medium was busy. These are deferred transmissions for this interface since the network interface supporting software was loaded, but frames involved in collisions are not counted. Frames that wait before transmission are counted.

Deferred transmissions occur when the network is extremely busy. High counts of multiple collisions and excessive collisions also occur.

Deferred transmissions indicate that this segment of the LAN is overcrowded. Reduce the traffic by reorganizing the LAN. For example, if you have 100 stations on one Ethernet bus break the bus into two Ethernet buses by adding a NIC to your device. This configuration balances the load by putting 50 stations on one bus and 50 on the other. If a few isolated stations create the traffic, put them on a separate bus.

Token Ring Statistics

The following Token Ring Statistics are displayed in this window. Information indicated as N/A is unobtainable from the hardware or support software.

- **Lost Frame Errors**—Indicates that a sending station was unable to complete the transmission because the frame that was sent never returned to the originator. When a station sends a frame, that frame normally returns after completing the circuit. If the frame does not return intact, this error increments.

These errors might occur if another station inserts itself into a ring or removes itself from the ring, interrupting the clock cycle. Large noise spikes, such as lightning, could also cause these errors.

If you see excessive Lost Frame errors, there might be a problem with the Multi-Access Unit (MAU) or hub. Use a network analyzer to isolate the problem area.

- **Internal Errors**—Indicate that the NIC has detected a problem with itself. Run the diagnostics from the NIC manufacturer to verify that a problem exists. You might need to replace the NIC.
- **Receive Congestion**—Increments when a station receives a frame, but cannot copy the data for some reason. The station might not have enough buffer space to copy the data.

Excessive traffic to a specific station might cause Receive Congestion Errors. If certain stations continue to experience Receive Congestion Errors, check the network design. It is also possible that the software on the PC is not running efficiently enough to handle interrupts from the network.

- **Token Errors**—Reported by the active monitor for one of the following reasons:
 - The active monitor detects that a frame has gone around the ring more than once, either because the sender removed itself from the ring before stripping the frame, or because there are two active monitors present on the network. The active monitor purges the network and clears the condition in either case.
 - A station reserved a token at a high priority and then removed itself from the network. The active monitor detects the token traversing the ring more than once as it searches for the station that requested the high priority. The active monitor purges the ring.
 - The active monitor detects that no token or frame is received for 10 milliseconds. This usually occurs when a station inserts or removes itself from the ring. When several stations insert or remove themselves from the ring at the same time, the counter escalates rapidly. This condition could occur when the power is off temporarily and then returned. In this example, several stations would try to insert themselves onto the ring at the same time, disrupting the signal. If this condition occurs check your MAU. Use a network analyzer to isolate the problem area.

The active monitor detected a token that was returned to it containing a token violation. In this case, you also see line errors along the ring. The active monitor purges the ring, but also check for the following:

- Failing cable—Packet data traveling through shorted or damaged cabling might become corrupt before reaching the destination station and cause line errors and token errors.
- Segment not grounded properly—Improper grounding of a segment might enable ground-induced noise to corrupt data flow and cause line errors and token errors.
- Noisy cable—Interference or noise produced by motors or other devices can distort the signals and cause CRC/Alignment errors, which increments the line error count and might cause token errors.

If you cannot find the problem after checking the previous conditions, use a network analyzer to isolate the station corrupting the frame. The analyzer should indicate which station is causing the problem and let you know if the NIC should be replaced.

- Frame Copy Errors—Occurs when a NIC receives a frame that is destined exclusively for itself, but the NIC detects that a station upstream has set the address recognize bit and copied the frame. This means that you have two NICs with the same network physical address, and you must change one of the addresses. Each NIC must have a unique network physical address.
- Transmit Beacons—Increments when there is a break on the Token Ring or you have a defective NIC on the ring. If you see even one transmit beacon, investigate the problem immediately.

The break is detected by the station immediately downstream of the break when that station stops receiving tokens or frames. This station then sends a series of beacon frames around the ring to notify the ring that a break has occurred immediately upstream.

A network analyzer helps to pinpoint the station that is sending the beacon frames and identify which station is directly upstream of the station sending the beacon.

- Abort Transmit Errors—Increments when a station transmits an abort delimiter while transmitting.

An aborted transmit occurs if the NIC is unable to complete the transmission of a frame that it has already started onto the network. For example, if the NIC was unable to access its packet buffer memory fast enough to keep pace with sending the data stream onto the wire, the NIC aborts the transmit. When the NIC aborts the transmit, it places a special bits sequence on the wire known as an abort delimiter, which signals to other stations on the Token Ring that the packet data is invalid.

Many NICs do not support aborting transmits, preferring instead to shut down with a fatal error and remove the NIC from the ring. Those NICs that support aborting transmits report this error.

If an about transmit error is reported, run the diagnostics from the NIC manufacturer to determine if there is a problem.

- Removes—Increments when the manager station issues a “Remove station from the ring” command. See your network administrator to determine why the station was removed from the ring.

- **Soft Errors**—Increments when the NIC detects recoverable errors. These errors are typically reported when nodes enter and exit the Token Ring. These are considered normal, nonfatal errors. The NIC corrects the error, but the error is reported to the LAN management station and counted. Check other error counts to determine if a serious error has occurred.
- **Recoveries**—Increments any time the active monitor changes from one station to another. The active monitor changes when the current active monitor removes itself from the network or has detected a problem with itself. If this item increments excessively, check the other error counts to determine if a problem exists.
- **Hard Errors**—Usually happen in conjunction with transmitted beacons. This value increases each time a station receives or sends a beacon, which occurs numerous times when a beacon is being transmitted.

If the Transmit Beacons count is incrementing as well, then this interface is sending beacons on the network. If Transmit Beacons is not incrementing, then this interface is not transmitting beacons, but detecting beacons being sent.

A network analyzer helps to pinpoint the station that is sending the beacon frames and identify which station is directly upstream of the station sending the beacon.

Perform the following steps:

- a. Check the station immediately upstream from the station that is sending the beacon. Swap out the transceiver, transceiver cable, and transceiver attachment point, one at a time. If you find a faulty component, replace it.
 - b. Check the receiver on the station that sent out the beacon frames to ensure that it is capable of receiving frames. If the receiver is not working properly, the NIC might have erroneously assumed that there were no frames or tokens. Run diagnostics from the NIC manufacturer to pinpoint the problem.
 - c. Check the cabling for breaks or disruptions.
 - d. Your MAU or hub might be at fault. Use the diagnostics from the MAU manufacturer to determine if a problem exists.
- **Lobe Faults**—Caused when the network is in test mode and finds a problem with one of the lobe wires running from the MAU to each station. The network enters test mode under two conditions:
 - a. When a station powers on and attempts to insert itself onto the network, the test on the lobe wire begins. If the test fails, a lobe wire fault occurs.
 - b. If hard errors occur, the NIC enters test mode. If the self-test fails, a lobe wire fault occurs.

If a Lobe Wire Fault occurs, check for the following:

- Failing cable—Be sure that your lobe wire is working and intact.
- Failing repeater, transceiver, or controller card—Repeaters, transceivers, and controller cards can disrupt the network signal, transmit erroneous signals on the wire, or ignore incoming packets. Perform the following steps:
 - a. If your NIC is continuously transmitting, it causes erroneous signals or “jabber.” Replace a jabbering receiver to ensure proper network performance.
 - b. Swap out the transceiver, transceiver cable, and transceiver attachment point, one at a time. If you find a faulty component, replace it.
 - c. Your MAU or hub might be at fault. Use the diagnostics from the MAU manufacturer to help you determine if a problem exists.
- Line Errors—Increments each time a station detects a line error. Each station either repeats or copies a frame and checks the frame for validation. If the data in the frame is corrupted, each station that detects the corrupted frame increments its own line-error count.
- Signal Loss—Usually happens in conjunction with other errors, such as burst errors, token errors, line errors, and transmitted beacons. This error indicates that the station temporarily or permanently lost the clock signal on the Token Ring. Check other error conditions to determine if a serious error has occurred.
- Burst Errors—Increments every time the adapter detects the absence of clock transitions. Burst errors occur in Token Ring networks when the signal is momentarily disrupted. Each time a station inserts itself into the ring or removes itself from the ring, a burst error might occur.

If you detect that one station has an abnormally high burst error count compared to other stations, you might need to replace the NIC. For example, if most stations average two burst errors per day, and one station shows 27, that station might have a faulty NIC. The station that is directly downstream of the device causing the problem usually detects the burst error. Use the Upstream Address of the station detecting burst errors to determine NIC faulty.

If excessive burst errors continue to occur on the ring, you might need to replace the MAU or hub. Use a network analyzer to isolate the problem area.

- **Frequency Errors**—Occur when a station detects that the active monitor is not working in the proper frequency. Ring Recovery occurs and another active monitor is chosen.

The active monitor generates a clock signal, which it passes to each standby monitor. The standby monitor compares this signal to its own reference clock. If the signal is not within the proper frequency boundaries, a frequency error occurs.

NOTE: Not all stations report this error, because not all NIC manufacturers support this feature. This error is not common. If there is a problem with the active monitor, other errors usually occur that help you determine the station that is at fault.

If you see frequency errors, use a network analyzer to determine which station was the active monitor causing the problem. Remember that the station with the problem is not the current active monitor. The active monitor experiencing the problem was replaced when the problem was detected.

- **AC Errors**—Also referred to as Address Recognized Indication/Frame Copied Indicator (ARI/FCI) errors. These errors occur when a station detects that an upstream station did not correctly set the bits on a frame.

If an AC error occurs, during your next planned maintenance:

- a. Ensure that the NIC is compliant with the protocol in use. The NIC that did not set the bit (the station directly upstream of the station that reported the problem) is not participating in the low-level protocol and might not be completely compliant with the 802.5 protocol.
 - b. Replace the NIC to see if the problem still occurs.
- **Single Station**—Increments when the interface senses that it is the only station on the ring. This happens if the interface is the first one up on a ring, or if there is a hardware problem. Check for the following:
 - a. Your MAU or hub might be at fault. Use the diagnostics from the MAU manufacturer to determine if a problem exists.
 - b. Check the cable between the NIC and the MAU. Replace the cable if necessary.
 - c. Run the diagnostics from the NIC manufacturer to determine if there is a problem with the NIC. Replace the NIC if necessary.

Subsystem Specific to a NetWare Operating System

Operating System Overview

HP now provides operating system management for NetWare environments. If you are running NetWare 4.x with NetWare Management Agent from Novell installed or NetWare 5.0, you can see the NetWare operating system information on the server being monitored. The information you can view includes file system information, user information, connection information, NetWare Loaded Modules (NLM) information, server parameters, partition information, and adapter information. By displaying the information as a subsystem in the Insight Management Agents by means of a browser, you can monitor both your hardware and operating system from one application.

NOTE: To ensure security, some NetWare Operating System information is accessible only when the user is logged in as an administrator or an operator. If you do not have administrator or operator access, `Information Unavailable` appears on certain pages and tables.

Summary Page

The Summary page describes basic information about the selected NetWare server. The following information is listed:

- NetWare Server Name—The physical name of this NetWare server.
- Internal Net Number—The internal IPX network number of this server.
- Serial Number—The serial number of the NetWare Operating System instance running on this server.
- Operating System—The version number of the NetWare Operating System running on this server.
- Release Date—The release date of the NetWare Operating System running on this server.
- Time Zone—The time zone in which this server resides. The string is in the same format as in the NetWare `SET TIMEZONE` command.
- Login State—The current login state of this server.

NOTE: The login state of a server can be not applicable, enabled, or disabled.

- Language—The national language in use on this server. The language can be one of the following:

Table 6-1: Available languages

Canadian French	Finnish	Portuguese
Chinese	French	Russian
Danish	German	Spanish
Dutch	Italian	Swedish
English	Japanese	Other

- Directory Services Name—The Directory Services full-distinguished name of this NetWare server. Only the operator and administrator have the right to retrieve this information.
- Bindery Context—The container objects where the bindery services contexts is set. Only the operator and administrator have the right to retrieve this information.
- Directory Tree—The name of the NetWare directory services tree containing this server. Only the operator and administrator have the right to retrieve this information.
- System Time—The date and time kept by this server.
- Up Time—The time (in hundredths of a second) since this server was last restarted.
- User Count—The number of entries in the User Account Table. Only the operator and administrator have the right to retrieve this information.
- Logged-In Users—The number of licensed connections (logins) in this file server. Only the operator and administrator have the right to retrieve this information.

File System Page

The File System page provides the file system information for the server. The page is divided into three sections: File System, File Volumes, and Open Files.

File System

The File System section displays the following information:

- Reads (Kbytes)—The total number of KBytes read by the file system. This value provides a measure of server activity.
- Writes (Kbytes)—The total number of KBytes written by the file system. This value provides a measure of server activity.
- Maximum Open Files—The maximum number of open files allowed in the file system.
- Open Files—The current number of open files in the file system.
- Maximum Record Locks—The maximum number of record locks allowed in the file system.
- Record Locks—The current number of record locks in the file system.
- Maximum Directory Tree Depth—The number of levels of subdirectories NetWare supports.

File Volumes

The File Volumes table lists all of the NetWare volumes, both mounted and not mounted.

- ID—A unique value that identifies each NetWare volume on the server. The value for each volume must remain constant from one re-initialization of the agent to the next re-initialization.
- Volume Name—The name of the physical volume, which might differ from the Directory Services (DS) name.
- Volume Size (Kbytes)—The size of the physical volume in KBytes.
- Free Space (Kbytes)—The free space on the physical volume in KBytes. As this number approaches zero, the volume is running out of space for new or expanding files.
- Block Size (bytes)—The block size on the volume in bytes.
- Segment Count—The number of segments making up this volume.
- Mount Status—The mount state of the volume, which can be 1 mounted or 2 dismounted.

NOTE: If the volume is not mounted, all the other values in the File Volumes table, except Volume Name, are valid.

- DS Name—The full Directory Services distinguished name for the volume, or the zero-length string if the distinguished name is not applicable.

Open Files

The Open Files table lists all of the open files on the server. If a file is opened by more than one connection, multiple entries for the same file appear in the table. Only the operator and administrator have the right to retrieve this information. The information in this table is sorted by File Name value by default. The Open Files table lists the following values:

- Connection—The number of the connection that opened the file.
- File Name (sortable)—The name of the open file including the directory path.
- Login Name (sortable)—The name of the user (if any) who opened the file. If the file was opened by the system or by an NLM, the Login Name is a zero-length string.
- Volume Name (sortable)—The name of the NetWare physical volume containing the open file.

User Information Page

The User Information page lists all user accounts in this file server. Users in the table might or might not be logged in at the time the page is viewed. The page is divided into two sections: General Information and User Information.

General Information

The General Information section displays the following information:

- User Count—The number of entries in the User Account Table.
- Logged-In Users—The number of licensed connections (logins) in this file server.
- Maximum Logins—The maximum number of licensed connections (logins) supported by this file server. The value is zero if the maximum number is unlimited.
- Connection Count—The current number of entries in the Connection Table. The current number of connections to this file server includes connection 0 (zero), which is the system connection.
- Maximum Connections—The maximum number of connections supported by this file server. The value is zero if the maximum number is unlimited.

User Information

NOTE: Only the operator and administrator have the right to retrieve user information.

The User Information table is sorted by the Name value by default. The table displays the following information for each user.

- Name (sortable)—The user login name (the Directory Services full distinguished name where appropriate).
- Disk Usage (Kbytes) (sortable)—The amount of disk space, in KBytes, the user is occupying across all volumes on this server.
- Account (sortable)—The status of the user account, which can be either valid or expired.
- Password (sortable)—The status of the user password, which can be either valid or expired.
- Full Name (sortable)—The user full name.
- Last Login Name (sortable)—The last user to log in to this server.

Connection Page

NOTE: Only the operator and administrator have the right to retrieve this connection information.

The Connection page displays NetWare connection information and lists all connections used, including those used by Workstations, NLMs, and Attachments. The information on this page is sorted by the Name value by default. The Connection page displays the following information for each connection:

- Number—The connection number. Connection 0 (zero) is used by the system.
- Name (sortable)—The login name (the Directory Services full distinguished name where appropriate).
- Status (sortable)—A value that represents the login status of the user. A user can have multiple statuses at the same time. A status can be one of the following:

Table 6-2: Available status conditions

Not logged in	Audited
Logged in	Authenticated temporary
Need security change	Audit connection recorded
MacStation	DS audit connection recorded
Connection abort	Logout in progress

- Address (sortable)—The transport address and domain of the connection.
- Connection Time (sortable)—The date and time the connection was established.

Loaded NLMs Page

The Loaded NLMs page is sorted by loaded order by default. The page displays the following information for each module:

- Name (sortable)—The name of the NLM that is currently loaded on the server.
- Memory (bytes) (sortable)—The total memory, in bytes, used by the NLM. This value is a composite of Short Term Memory, Semi-Permanent Memory, and Non-movable Cache Memory allocated by the NLM, plus the sizes of the code and data sections of this instance of an NLM.
- Description (sortable)—A brief description of the NLM.
- Version (sortable)—The major and minor version numbers of the NLM.

Server Parameter Page

The Server Parameter page includes a table of the NetWare set parameters. This table emulates the NetWare SET command.

NOTE: Only the operator and administrator have the right to retrieve this server parameter information.

In the middle frame, server parameters are categorized by their features. When a category link is clicked from the middle frame, only the server parameters that fit into this category show up in the frame on the right. The server parameter table in the frame on the right is sorted by the Name value by default and the table displays the following information:

- Name—The name of the settable parameter.
- Value—The current value of the parameter.
- Range—The range of value can be set on the parameter. An Out of Range warning is given if the administrator or operator tries to do an invalid set.
- Description—A brief description of the NetWare set parameter.

The Set Parameter table enables the administrator and operator to remotely change the server operating system configuration and parameter settings through the Web browser. The modifiable variable can be categorized as follows:

- **String**—The maximum length for the string field is the upper-limit settable length of the string. If the length of the set string exceeds the defined maximum length, an Out of Range warning appears and the set is aborted.
- **Boolean**—The OFF and ON radio buttons are used to set the Boolean type parameter. Click the radio button to select either OFF or ON, and then click **SET**. The set is done.
- **Ticks**—For the convenience of the administrator or operator, the Ticks-type parameter is calculated and displayed as seconds. So when do a set, modify the amount of the seconds in the text field, and click **SET**. If the seconds set is not in the range of the predefined seconds, and an Out of Range warning appears and the set is aborted.
- **TimeOffset**—In the format of +/- XX:XX:XX (hour:minute:second). To do a set, modify the value in the predefined format in the text field, and click **SET**.
- **BlockShift**—An integer typeset. Modify the value in the text field, and click **SET**.
- **Trigger**—An integer typeset. Modify the value in the text field, and click **SET**.

In NetWare 4.x, all the sets done through command line or Monitor utility take effect immediately, but the sets are lost when the server is rebooted. The Web Agent overcomes this drawback by writing the SET command in Autoexec.ncf when a set is committed through the Web Agent browser so it is a permanent set. In NetWare 5.x, the SET command is not added in the Autoexec.ncf, because the operating system can remember the set even after the reboot.

SET Exceptions

In both NetWare 4.x and NetWare 5.x, when the administrator or operator tries to do a set on a variable that is only settable through the Startup.ncf file, a SET XXXXX=XXXX line is added in the Startup.ncf file. Although, the set does not take effect until the remote server is restarted, when set is clicked, a warning message appears.

In NetWare 5.x, when trying to do a lower-than-current-value set on alert message nodes, an HTTP post error warning appears. Be alert, because the operating system is denying this set. If this set is done through the command line or Monitor utility, the same denial occurs.

Physical Partition Page

The Physical Partition page displays a table of physical partitions for long-term storage devices contained by the host. The table on this page is sorted by the Type value by default.

- Type (sortable)—The type of this physical partition. The types listed can be:
 - NetWare
 - DOS
 - InwDos
 - Other
- Description (sortable)—A brief description of this partition.
- Size (sortable)—The size (in Kilobytes) of this physical partition.

Adapter Information Page

The Adapter Information page displays general information for each adapter board in the host. The Adapter table is sorted by the Description value by default.

Description—A description of the hardware information for the adapter. The description usually includes manufacturer, model, and version information. For LAN adapters, the short board name and the burnt-in MAC address of the boards are listed.

CR3500 RAID Array SCSI Controller

Mass Storage RAID Array

This section displays RAID array information. Five banners appear in this section.

RAID Array Status

Status—Displays the status of the RAID array. The following conditions are valid:

- Good—The RAID array is fully operational.
- Reduced—The RAID array is operating in a degraded or reduced state. One or more of the physical drives that make up the RAID array are either missing or failed. However, the RAID array can continue to operate without data loss.
- Failed—The RAID array is not operational.
- Reconstructing—The RAID array is regenerating the data from a failed physical drive onto a replacement drive that is part of the RAID array. All user data remains available during the reconstruction process, but some performance reduction might occur when a request requires access to the device being reconstructed.
- Initialization—The controller is writing its file structure onto the member devices of a RAID array.

RAID Level—Displays the RAID level and a brief description of the selected RAID array.

Drive Information

Capacity—Displays the total capacity of the RAID array in megabytes.

Physical Drives

Physical Drive Channel—Displays the channel number, also referred to as the “port.”

Physical Drive SCSI ID—Displays the SCSI ID number.

Logical Drives

Logical Drives—Lists the logical drives.

Spare Drives

Controller—Displays the controller name.

Spare Status—Displays the status of the online spare drive. The following conditions are valid:

- Hot Spare—The drive attached to this channel is kept spinning whenever the controller is powered up. It is to be automatically brought online to replace a failed drive.
- Warm Spare—The drive attached to this channel is not spun up until a disk in the array fails. It is to be automatically brought online to replace a failed drive.
- Adding Spare—The drive is in the process of becoming a spare drive.

Mass Storage Physical

This section displays physical drives attached to the CR3500 RAID Controller. Three banners appear in this section.

Physical Drive Status

The following conditions are valid:

- On Line—The drive attached to this channel is a fully-functional member of this RAID set.
- Off Line—The drive attached to this channel is not a member of the RAID set.
- Hot Spare—The drive attached to this channel is kept spinning whenever the controller is powered up. It is to be automatically brought online to replace a failed drive.
- Warm Spare—The drive attached to this channel is not spun up until a disk in the array fails. It is to be automatically brought online to replace a failed drive.
- Creating—The drive is currently being created as part of a RAID set.
- Rebuilding—The drive is currently being rebuilt.
- Formatting—The drive is currently being formatted.

Action—Provides a brief description of an action you can take depending on the physical drive condition

Drive Information

- Capacity—Displays the total capacity of the selected drive in megabytes
- Firmware Version—Displays the firmware revision of the selected drive
- Drive Owner—Lists a descriptive name for the drive owner
- Model—Displays the model number of the selected drive
- Vendor—Displays the vendor of the selected drive

RAID Arrays

RAID Arrays—Lists the RAID arrays by channel number and SCSI ID

Mass Storage Controller

This section displays Array Controller information.

Clustered RAID Controller

Controller Status—Displays the current controller status. The following conditions are valid:

- OK—All controller functions are operating normally.
- Degraded—The controller is operating in a degraded or reduced state.
- Failed—The controller is inoperable.

Current Role—Displays if the controller is in simplex or duplex role.

Firmware Version—Displays the current software revision.

Serial Number—Displays the controller serial number.

Drive Ownership—Lists a descriptive name for the drive owner.

Rebuild Rate—Displays the rebuild rate. The rebuild rate ranges from 1 to 100. The controller rebuilds while at the same time it handles I/O activity. A rate below 50 emphasizes I/O response over the RAID rebuild. A rate above 50 puts a higher priority on the RAID rebuild at the expense of I/O activity.

Create Rate—Displays the create rate. The create rate ranges from 1 to 100. The controller creates RAID sets while, at the same time, handles I/O activity. A rate below 50 emphasizes I/O response over the RAID set creation. A rate above 50 puts a higher priority on the RAID set creation at the expense of I/O activity.

Cache Size—Displays the cache size in megabytes.

DIMM A Size—Displays the Dual Inline Memory Module A size in megabytes.

DIMM B Size—Displays the Dual Inline Memory Module B size in megabytes .

Mass Storage Summary

CR3500 Shared Storage System

This section displays degraded or failed devices in the CR3500 Shared Storage System.

The following is a list of devices in CR3500 Shared Storage System:

- Clustered RAID Controller
- RAID Array
- Physical Drive
- Spare Drive
- Environment Monitoring Unit

Environment Monitoring Unit

This section displays the Environment Monitoring Unit information.

Primary enclosure temperature status—Displays the current primary enclosure temperature status. The following conditions are valid:

- OK—The primary enclosure temperature is within normal parameters.
- Critical—The controller temperature sensor has detected a critical temperature condition in the primary enclosure.
- Non-critical—The controller temperature sensor has detected an abnormal temperature condition in the primary enclosure.
- Unknown—The enclosure temperature information is unavailable.

Primary enclosure temperature—Displays the current primary enclosure temperature in degrees Celsius.

Primary enclosure fan status—Displays the current primary enclosure fan status. The following conditions are valid:

- OK—The fan status is normal.
- Critical—The fan has failed.
- Unknown—The enclosure fan status information is unavailable.

Primary power supply status—Displays the current primary power supply status. The following conditions are valid:

- OK—The power supply status is normal.
- Critical—The power supply is installed and marked as failed.
- Not Installed—One of the redundant power supplies has been removed.
- Unknown—The power supply status information is unavailable.

External Expansion Cabinet

This section displays the External Expansion Cabinet information.

Power Supply Status—Displays the current status. The following conditions are valid:

- OK—All power supply parameters are normal.
- Non-Critical—The redundant power supply is reporting a fault that is not critical to operation.
- Not Installed—One of the redundant power supplies has been removed.
- Unknown—The power supply information is unavailable.

Fan Status displays the current fan status. The following conditions are valid:

- OK—All fans are operating normally.
- Critical—A fan has failed.
- Non-Critical—A fan is in a degraded condition.
- Not Installed—The fan has been removed.
- Unknown—The fan status information unavailable.

Temperature Status—Displays the current temperature status. The following conditions are valid:

- OK—All temperature sensors are reporting normal.
- Critical—Temperatures have reached the critical level, and failure might be imminent.
- Non-Critical—The temperature is outside of the normal range, but has not reached the critical level.
- Not Installed—The temperature sensors cannot be read.
- Unknown—The temperature status information is unavailable.

Agent Information Specific to SCO UnixWare 7

Foundation Agents

SCO UnixWare 7 SNMP Daemon

An SNMP daemon is provided with SCO UnixWare 7 and is located in `/usr/sbin/in.snmpd`. The SNMP daemon provides SNMP service over UDP/IP-based networks.

The SNMP daemon communicates with multiple vendor-supplied SMUX peer agents, running on the local SCO UnixWare 7 system, through TCP client connections. Remote management consoles issue SNMP get and set packets over a UDP/IP network to the local SNMP daemon.

The SNMP daemon is started and stopped from a shell script. It is started automatically at system startup and stopped automatically at system shutdown.

You can manually start and stop the SNMP daemon by entering the following commands:

```
sh /etc/init.d/snmp start
sh /etc/init.d/snmp stop
```

NOTE: Stopping the SNMP daemon causes the HP SMUX Managers to terminate.

HP Foundation SMUX Manager

The HP Foundation SMUX Manager extends the SNMP “enterprise” MIB to include HP MIB data. The HP Foundation SMUX Manager supports get, set, and trap operations on data items defined in the HP host and threshold MIBs.

HP Foundation MIB data is gathered by data collection agent processes (Host OS and Threshold Agents). Each agent collects and saves MIB data in files that are read by the cSMUX Manager during SNMP get commands. SNMP set commands are routed by the Foundation SMUX Manager to the agent responsible for managing the selected MIB data item. SNMP trap commands are generated by data collection agents and routed by the Foundation SMUX Manager to the SNMP daemon.

At Foundation SMUX Manager startup time, HP host and threshold MIB items in the file `/opt/compaq/foundation/etc/cmafdtntsmuxd.defs` are registered with the SNMP daemon. Not all HP MIB items listed in the file `cmafdtntsmuxd.defs` might be supported by SCO UnixWare 7 Management data collection agents. Only HP MIB items listed in the Foundation Data Registry MIB file `/opt/compaq/foundation/etc/registry.mib` are supported by SCO UnixWare 7 Foundation data collection agents.

During the installation, the Foundation SMUX Manager Agent is configured to start up automatically when the SCO UnixWare 7 system enters multiuser mode and to shut down automatically when the SCO UnixWare 7 system exits the multiuser mode.

Issue the following command to enable automatic startup of the SMUX Manager:

```
ln -s /opt/compaq/foundation/etc/cmafdtntsmux
/etc/rc2.d/S98cmafdtntsmux
```

Issue the following command to disable automatic startup of the SMUX Manager:

```
rm /etc/rc2.d/S98cmafdtntsmux
```

Issue the following command to manually start the SMUX Manager:

```
sh /etc/init.d/cmafdtntsmux start
```

If automatic startup of the Foundation SMUX Manager is enabled, automatic shutdown should also be enabled.

Issue the following commands to enable automatic shutdown of the Foundation SMUX Manager:

```
ln -s /opt/compaq/foundation/etc/cmafdtntsmux
/etc/rc0.d/K01cmafdtntsmux
ln -s /opt/compaq/foundation/etc/cmafdtntsmux
/etc/rc1.d/K01cmafdtntsmux
```

Issue the following commands to disable automatic shutdown of the SMUX Manager:

```
rm /etc/rc0.d/K01cmafdtntsmux
rm /etc/rc1.d/K01cmafdtntsmux
```

Issue the following command to manually stop the SMUX Manager:

```
sh /etc/init.d/cmafdtntsmux stop
```

Foundation Agents SMUX Manager Configuration File

The configuration file `/opt/compaq/foundation/etc/config` configures runtime variables during initialization of the HP Foundation SMUX Manager software. The default Foundation SMUX Manager configuration file can be used without any modification. It can also be edited to meet the particular needs of your system.

NOTE: If the configuration file is edited, the Foundation SMUX Manager software must be restarted before the configuration modification is effective. You can do this by entering the following commands:

```
sh /etc/init.d/cmafdtasmux stop
sh /etc/init.d/cmafdtasmux start
```

Foundation Agents SMUX Manager Configuration File Syntax

The Foundation Agents SMUX Manager Configuration file syntax requires that:

- All configuration file commands be terminated by a semicolon
- All string parameters be delimited by double quotes, for example:
`"cmahostd"`
- Commands be commented out by adding "C"-style comment delimiters around the desired line, for example:

```
/* agent = "cmahostd" -p 60 -s OK -t OK; */
```

Syntax errors detected while parsing the configuration file are written to the file `/var/spool/compaq/agenterrs.log`. The presence of any syntax errors terminates the Foundation SMUX Manager initialization procedure.

The following is an example of the Foundation SMUX Manager configuration:

```

/*****
#ident "© 2003 Hewlett-Packard Development Company L.P."
#ident "@(#)config 1.10 99/06/03"
*****
*
* Module: HP Foundation SMUX Manager Configuration File.
*
*****
*****/

/*****

```

The following are data collection agents that are not started automatically at system boot time.

Table 8-1: Data Collection Agents

* Agent Name	Poll	Set	Trap
*	Time	State	State
*	(seconds)	(OK = Enabled)	
*		(NOT_OK = Disabled)	
*/			
agent = "cmahostd"	-p 15	-s OK	-t OK
agent = "cmathreshd"	-p 1	-s OK	-t OK

Foundation SMUX Manager Configuration File Parameters

This topic defines the syntax of the parameters contained in the configuration file `/opt/compaq/foundation/etc/config`.

The `agent` command starts an agent process to collect status data from the specified device. Monitoring for this agent can be disabled by deleting the line or adding comment delimiters around the desired line as shown:

```
/* agent = ; */
```

Multiple `agent` command lines can be specified. However, each must have a unique `agent_path` name.

Syntax:

```
agent = "agent_path" -p poll_time -s set_state -t trap_state;
```

The pathname to the HP supplied agent binary file is `agent_path`. The `poll_time` parameter (required) defines the frequency (in seconds) of status data updates from the agent. The `set_state` parameter is used to enable or disable SNMP sets for items this agent supports. The `trap_state` parameter is used to enable or disable trap messages from this agent.

For example:

```
agent = "cmahostd" -p 15 -s OK -t OK;
```

NOTE: Increasing the `agent poll_time` setting improves system performance but decreases the data collection rate. Conversely, decreasing the `agent poll_time` setting increases the data collection rate but can decrease system performance.

Trap Alarm E-mail Configuration File

HP Management Agents for Servers are capable of sending e-mail notifications in addition to the SNMP traps. The configuration file `/opt/compaq/mailcfg` configures the e-mail command which is read by the Foundation SMUX Manager during its initialization. This file is shared by SMUX Managers from all HP Management Agents for Servers packages.

NOTE: If this configuration file is edited, the Foundation SMUX Manager software must be restarted before the configuration modification is effective. You can do this by entering the following commands:

```
sh /etc/init.d/cmafdtnsmux stop
sh /etc/init.d/cmafdtnsmux start
```

Syntax of the e-mail command:

```
mail = "mail_path -s 'subject_line' destination(s)";
```

The name of the installed SCO UnixWare 7 system mail program is `mail_path`. The `subject_line` parameter defines how a subject line is entered for the mailer used in the system. Note that the subject line must be enclosed in single quotes. The `destination(s)` parameter defines where to send trap alert messages. Multiple mail destinations might be defined in the mail line, separated by spaces.

For example:

```
mail = "/bin/mailx -s 'HP Management Agents Trap Alert' root
admin1";
```

Foundation Data Collection Agents

Each HP Foundation data collection agent gathers and saves MIB data to files in the HP Foundation Data Registry. The data collection agents periodically update MIB data at configurable poll intervals.

The agent responsible for managing the selected MIB data item performs SNMP set commands. Data collection agents generate SNMP trap commands.

The Foundation SMUX Manager agent starts all the Foundation data collection agents. Refer to the Foundation Agents SMUX Manager Configuration File topic.

HP Foundation Data Registry

The HP Foundation data registry (`/var/spool/compaq/foundation/registry`) is composed of standard SCO UnixWare 7 directories and associated files. Each file in the data registry is a logical object containing "n" related data items.

NOTE: Only HP MIB items listed in the Foundation Data Registry MIB file `/opt/compaq/foundation/etc/registry.mib` are supported by SCO UnixWare 7 Foundation data collection agents.

Web Agent

The Web Agent runs as a daemon and converts SNMP information into HTML so that it can be viewed from a Web browser. The Web Agent provides Web pages containing management information about HP ProLiant servers.

The Web Agent enables users to view subsystem and status information of HP ProLiant Servers from a Web browser, either locally or remotely. The Web Agent also provides extensive SET capabilities. Refer to the *Web-Enabled HP Management Agents User Guide* for more information about the Web Agent. This guide can be found on the Management CD at `/docs/eng/imaug.pdf`.

- To view data locally, use the following URLs:

```
http://127.0.0.1:2301/
```

or

```
http://localhost:2301/
```

- To view data remotely, use the following URL:

```
http://machine:2301/
```

where *machine* is the IP address or the computer name under DNS.

NOTE: Notice that the URL is followed by `:2301`. This is the port number that the Web Agent uses to communicate with the browser. If this number is not specified, the browser might connect to another Web page if the managed server is running a Web server.

After entering the URL, the Device Home Page appears. Click the **Management Agents** icon to start viewing the Web pages provided by the Web Agent.

During the Foundation Agents package installation, the Web Agent is configured to start up automatically when the SCO UnixWare 7 system enters multiuser mode and to shut down automatically when the SCO UnixWare 7 system leaves the multiuser mode.

Enter the following command to enable automatic startup of the Web Agent:

```
In -s /opt/compaq/foundation/etc/cmaweb /etc/rc2.d/S98cmaweb
```

Enter the following command to disable automatic startup of the Web Agent:

```
rm /etc/rc2.d/S98cmaweb
```

If automatic startup of the Web Agent is enabled, automatic shutdown should also be enabled. Enter the following commands to enable automatic shutdown:

```
In -s /opt/compaq/foundation/etc/cmaweb /etc/rc0.d/K01cmaweb
In -s /opt/compaq/foundation/etc/cmaweb /etc/rc1.d/K01cmaweb
```

Issue the following commands to disable automatic shutdown of the agent:

```
rm /etc/rc0.d/K01cmaweb
rm /etc/rc1.d/K01cmaweb
```

All four packages carry the data component consisting of template files, gif files, and html files in the form of a compressed tar file that is extracted during installation of the package under the Web Agent root directory `/opt/compaq/webagent`. During removal of the package, the same files are removed from `/opt/compaq/webagent`.

Server Agents

HP Server SMUX Manager

The HP Server SMUX Manager extends the SNMP “enterprise” MIB to include Compaq MIB data. The HP Server SMUX Manager supports get, set, and trap operations on data items defined in the following HP MIBs:

- System Information MIB
- Standard Equipment Information MIB
- Server Health MIB
- Remote Insight Board Related Information MIB

HP Server MIB data is gathered by data collection agent processes (System Health, Standard Equipment, and Remote Insight Agents). Each agent collects and saves MIB data in files that are read by the Server SMUX Manager during SNMP get commands. The Server SMUX Manager routes the agent responsible for managing the selected MIB data item to the agent responsible for managing the selected MIB data item routes SNMP set commands. SNMP trap commands are generated by data collection agents and routed by the Server SMUX Manager to the SNMP daemon.

At Server SMUX Manager startup time, ProLiant Server MIB items in the file `/opt/compaq/server/etc/cmasvrsmuxd.defs` are registered with the SNMP daemon. Not all HP MIB items listed in the file `cmasvrsmuxd.defs` can be supported by SCO UnixWare 7 Server data collection agents. Only HP MIB items listed in the Server Data Registry MIB file `/opt/compaq/server/etc/registry.mib` are supported by SCO UnixWare 7 Server data collection agents.

During the installation, the Server SMUX Manager Agent is configured to start up automatically when the SCO UnixWare 7 system enters multiuser mode and to shut down automatically when the SCO UnixWare 7 system exits the multiuser mode.

Issue the following command to enable automatic startup:

```
ln -s /opt/compaq/server/etc/cmasvrsmux /etc/rc2.d/S98cmasvrsmux
```

Issue the following command to disable automatic startup of the Server SMUX Manager:

```
rm /etc/rc2.d/S98cmasvrsmux
```

Issue the following command to manually start the Server SMUX Manager:

```
sh /etc/init.d/cmasvrsmux start
```

If automatic startup of the Server SMUX Manager is enabled, automatic shutdown should also be enabled.

Issue the following commands to enable automatic shutdown of the Server SMUX Manager:

```
ln -s /opt/compaq/server/etc/cmasvrsmux /etc/rc0.d/K01cmasvrsmux
```

```
ln -s /opt/compaq/server/etc/cmasvrsmux /etc/rc1.d/K01cmasvrsmux
```

Issue the following commands to disable automatic shutdown of the Server SMUX Manager:

```
rm /etc/rc0.d/K01cmasvrsmux
```

```
rm /etc/rc1.d/K01cmasvrsmux
```

Issue the following command to manually stop the Server SMUX Manager:

```
sh /etc/init.d/cmasvrsmux stop
```

Server Agents SMUX Manager Configuration File

The configuration file `/opt/compaq/server/etc/config` configures runtime variables during initialization of the HP Server SMUX Manager software. The default Server SMUX Manager configuration file can be used without any modification. It can also be edited to meet the particular needs of your system.

NOTE: If the configuration file is edited, the Server SMUX Manager software must be restarted before the configuration modification is effective. Restart the software by entering the following commands:

```
sh /etc/init.d/cmasvrsmux stop  
sh /etc/init.d/cmasvrsmux start
```


Server Agents SMUX Manager Configuration File Syntax

The Server Agents SMUX Manager Configuration file syntax requires that:

- All configuration file commands be terminated by a semicolon.
- All string parameters be delimited by double quotes, for example:
"cmastdeqd"
- Commands be commented out by adding "C"-style comment delimiters around the desired line, for example:

```
/* agent = "cmastdeqd" -p 60 -s OK -t OK; */
```

Syntax errors detected while parsing the configuration file are written to the file `/var/spool/compaq/agenterrs.log`. The presence of any syntax errors terminates the Server SMUX Manager initialization procedure.

The following is an example of the Server SMUX Manager configuration:

```

/*****
#ident "© 2003 Hewlett-Packard Development Company L.P."
#ident "@(#) config 1.10 99/06/03"
*****
* Module:hp Server SMUX Manager Configuration File.
*
*****
*****/
/*****/

```

The following are data collection agents that are not started automatically at system boot time.

Table 8-2: Data collection agents

* Agent Name	Poll	Set	Trap	Reboot
*	Time	State	State	State
*	(seconds)	(OK = Enabled)		
*		(NOT_OK = Disabled)		
*/				
agent = "cmastdeqd"	-p 60	-s OK	-t OK	-r OK

Server SMUX Manager Configuration File Parameters

This topic defines the syntax of the parameters contained in the configuration file `/opt/compaq/server/etc/config`.

The agent command starts an agent process. Monitoring for this agent can be disabled by deleting the line or adding comment delimiters around the desired line as shown:

```
/* agent = ; */
```

Multiple agent command lines can be specified. However, each must have a unique `agent_path` name.

```
Syntax: agent = "agent_path" -p poll_time -s set_state -t  
trap_state -r reboot_state;
```

The pathname to the HP supplied agent binary file is `agent_path`. The `poll_time` parameter (required) defines the frequency (in seconds) of status data updates from the agent. The `set_state` parameter is used to enable or disable SNMP sets for items this agent supports. The `trap_state` parameter is used to enable or disable trap messages from this agent. The `reboot_state` parameter is used only by the Standard Equipment Agent to enable and disable remote reboot from the management console.

For example:

```
agent = "cmastdeqd" -p 60 -s NOT_OK -t NOT_OK -r OK;
```

NOTE: Increasing the agent `poll_time` setting improves system performance but decreases the data collection rate. Conversely, decreasing the agent `poll_time` setting increases the data collection rate but can decrease system performance.

Trap Alarm E-mail Configuration File

HP Management Agents for Servers are capable of sending e-mail notifications in addition to the SNMP traps. The configuration file `/opt/compaq/mailcfg` configures the e-mail command that is read by the Server SMUX Manager during its initialization. This file is shared by SMUX Managers from all HP Management Agents for Servers packages.

NOTE: If this configuration file is edited, the Server SMUX Manager software must be restarted before the configuration modification is effective. You can do this by entering the following commands:

```
sh /etc/init.d/emasvrsmux stop
sh /etc/init.d/emasvrsmux start
```

Syntax of the e-mail command:

```
mail = "mail_path -s 'subject_line' destination(s)";
```

The name of the installed SCO UnixWare 7 system mail program is `mail_path`. The `subject_line` parameter defines how a subject line is entered for the mailer used in the system. The subject line must be enclosed in single quotes. The `destination(s)` parameter defines where to send trap alert messages. Multiple mail destinations can be defined in the mail line, separated by spaces.

For example:

```
mail = "/bin/mailx -s 'HP Management Agents Trap Alert' root
admin1";
```

Server Data Collection Agents

Each HP Server data collection agent gathers and saves MIB data to files in the HP Data Registry. The data collection agents periodically update MIB data at configurable poll intervals.

The agent responsible for managing the selected MIB data item performs SNMP set commands. Data collection agents generate SNMP trap commands.

Only the Standard Equipment Agent is started by the Server SMUX Manager. System Health and Remote Insight Agents are started by their own startup script.

HP Server Data Registry

The HP Server data registry (`/var/spool/compaq/server/registry`) is comprised of standard SCO UnixWare 7 directories and associated files. Each file in the data registry is a logical object containing "n" related data items.

NOTE: Only HP MIB items listed in the Server Data Registry MIB file `/opt/compaq/server/etc/registry.mib` are supported by SCO UnixWare 7 Server data collection agents.

Configuring Server Data Collection Agents

For more information on configuring Server Data Collection Agents, choose from the following:

- Standard Equipment Agent
- System Health Agent
- Remote Insight Agent

Standard Equipment Agent

The Standard Equipment Agent gathers data for the HP Standard Equipment MIB. The data includes:

- EISA/PCI slot information
- Processor and coprocessor information
- Standard peripheral information (serial ports, diskette drives, and so on)

To run the Standard Equipment Agent, add the following line to the Server SMUX Manager configuration file `/opt/compaq/server/etc/config`:

```
agent = "cmastdeqd" -p 60 -s OK -t OK -r OK;
```

The following command line arguments can be used:

- `-p poll_time`—Specifies the number of seconds to wait between data collection intervals. The minimum allowed value is 1 second, and the default value is 60 seconds.
- `-s set_state`—Specifies whether SNMP set commands are allowed for this agent. A `set_state` of `OK` (default) means that SNMP set commands are allowed. A `set_state` of `NOT_OK` means that SNMP set commands are not allowed.
- `-t trap_state`—Specifies whether SNMP trap commands are allowed for this agent. A `trap_state` of `OK` (default) means that SNMP trap commands are allowed. A `trap_state` of `NOT_OK` means that SNMP trap commands are not allowed.
- `-r reboot_state`—Specifies whether a remote management station can reboot this device. A `reboot_state` of `OK` (default) means that remote reboots are allowed. A `reboot_state` of `NOT_OK` means that remote reboots are not allowed.

This agent is automatically started at Server SMUX Manager startup and automatically stopped at Server SMUX Manager shutdown. Refer to `/opt/compaq/server/etc/registry.mib` for a complete list of supported MIB items.

System Health Agent

The System Health Agent gathers data for the HP Health MIB. The data collected include critical (NMI) errors, correctable memory (ECC) errors, system hang/panic detection, temperature conditions, and fan failures.

Critical errors are monitored by the System Health driver. A critical error, such as an uncorrectable memory error, is logged in the Integrated Management Log or the Critical Error Log. The System Health Agent then retrieves the error.

Correctable memory errors (ECC) are monitored by the System Health driver. If a correctable memory error occurs, the error is corrected and logged in the Integrated Management Log or the Correctable Error Log. The System Health Agent then retrieves the error.

The System Health driver monitors the operating temperature of the system. If the normal operating temperature is exceeded or a cooling fan fails, System Health driver sends a notice of the problem, makes an entry in the Integrated Management Log or the System Health Log, and then (optionally) shuts the system down to avoid hardware damage. Automatic shutdown is configured through the HP System Configuration Utility. Health log information can be displayed using the Inspect Utility.

The System Health driver detects fan failure. If a required fan or a processor fan fails, the system can be gracefully shut down.

During the installation, the System Health Agent is configured to start up automatically when the SCO UnixWare 7 system enters multiuser mode and shut down automatically when the SCO UnixWare 7 system leaves multiuser mode.

Issue the following command to enable automatic startup:

```
ln -s /opt/compaq/server/etc/cmahealth /etc/rc2.d/S99cmahealth
```

Issue the following command to disable automatic startup of the System Health Agent:

```
rm /etc/rc2.d/S99cmahealth
```

If automatic startup of the System Health Agent is enabled, automatic shutdown should also be enabled.

Issue the following commands to enable automatic shutdown of the agent:

```
ln -s /opt/compaq/server/etc/cmahealth /etc/rc0.d/K02cmahealth
```

```
ln -s /opt/compaq/server/etc/cmahealth /etc/rc1.d/K02cmahealth
```

Issue the following commands to disable automatic shutdown of the System Health Agent:

```
rm /etc/rc0.d/K02cmahealth
```

```
rm /etc/rc1.d/K02cmahealth
```

Issue the following command to manually start the System Health Agent:

```
sh /etc/init.d/cmahealth start
```

Issue the following command to manually stop the System Health Agent:

```
sh /etc/init.d/cmahealth stop
```

Refer to `/opt/compaq/server/etc/registry.mib` for a complete list of supported MIB items.

Remote Insight Agent

The Remote Insight agent gathers data for the HP Remote Insight MIB. The data includes:

- Configuration and statistical information of the Remote Insight Board (RIB)
- Events logged onto the RIB
- Configuration and status of the Remote Insight asynchronous communication ports
- Configuration and statistical information of the Remote Insight NIC (for HP Remote Insight/PCI Board only)

The Remote Insight Agent allows remote dial back accesses to the server SNMP data through the Remote Insight board PPP connection.

During installation, the Remote Insight Agent is configured to start up automatically when the SCO UnixWare 7 system enters multiuser mode and to shut down automatically when the SCO UnixWare 7 system leaves the multiuser mode.

Issue the following command to enable automatic startup of Remote Insight Agent:

```
ln -s /opt/compaq/server/etc/cmasm2 /etc/rc2.d/S99cmasm2
```

Issue the following command to disable automatic startup of the Remote Insight Agent:

```
rm /etc/rc2.d/S99cmasm2
```

Issue the following command to manually start the Remote Insight agent:

```
sh /etc/init.d/cmasm2 start [poll_time]
```

where `poll_time` is the number of seconds to wait between data collection intervals. The suggested `poll_time` is 60 seconds (default). The minimum `poll_time` is 5 seconds.

If automatic startup of the Remote Insight Agent is enabled, automatic shutdown should also be enabled.

Issue the following commands to enable automatic shutdown:

```
ln -s /opt/compaq/server/etc/cmasm2 /etc/rc0.d/K01cmasm2
```

```
ln -s /opt/compaq/server/etc/cmasm2 /etc/rc1.d/K02cmasm2
```

Issue the following commands to disable automatic shutdown of the agent:

```
rm /etc/rc0.d/K01cmasm2
rm /etc/rc1.d/K02cmasm2
```

Issue the following command to manually stop the agent:

```
sh /etc/init.d/cmasm2 stop
```

Refer to `/opt/compaq/server/etc/registry.mib` for a complete list of supported MIB items.

- To enable PPP access to the server, provide read and write permission for the local loopback IP address (or 0.0.0.0) in the files `/etc/netmgt/snmpd.trap` and `/etc/netmgt/snmpd.comm`.

Storage Agents

HP Storage SMUX Manager Agent

The HP Storage SMUX Manager extends the SNMP “enterprise” MIB to include HP Storage MIB data. The HP Storage SMUX Manager supports get, set, and trap operations on data items defined in the HP Storage MIB.

Data collection agent processes gather HP Storage MIB data. Each agent collects and saves MIB data in files that are read by the HP Storage SMUX Manager during SNMP get commands. SNMP set commands are routed by the HP Storage SMUX Manager to the agent responsible for managing the selected Storage MIB data item. SNMP trap commands are generated by data collection agents and routed by the HP Storage SMUX Manager to the SNMP daemon.

At HP Storage SMUX Manager startup time, all HP MIB items in the file `/opt/compaq/storage/etc/cmastorsmuxd.defs` are registered with the SNMP daemon. Not all HP Storage MIB items listed in the file `cmastorsmuxd.defs` are supported by SCO UnixWare 7 Management data collection agents.

During installation, the HP Storage SMUX Manager Agent is configured to start up automatically when the SCO UnixWare 7 system enters multiuser mode and shut down automatically when the SCO UnixWare 7 system exits the multiuser mode.

Issue the following command to enable automatic startup:

```
ln -s /opt/compaq/storage/etc/cmastorsmux
/etc/rc2.d/S98cmastorsmux
```

Issue the following command to disable automatic startup of the HP Storage SMUX Manager:

```
rm /etc/rc2.d/S98cmastorsmux
```

Issue the following command to manually start the HP Storage SMUX Manager:

```
sh /etc/init.d/cmastorsmux start
```

If automatic startup of the HP Storage SMUX Manager is enabled, automatic shutdown should also be enabled.

Issue the following commands to enable automatic shutdown of the HP Storage SMUX Manager:

```
ln -s /opt/compaq/storage/etc/cmastorsmux
/etc/rc0.d/K01cmastorsmux
ln -s /opt/compaq/storage/etc/cmastorsmux
/etc/rc1.d/K01cmastorsmux
```

Issue the following commands to disable automatic shutdown of the HP Storage SMUX Manager:

```
rm /etc/rc0.d/K01cmastorsmux
rm /etc/rc1.d/K01cmastorsmux
```

Issue the following command to manually stop the HP Storage SMUX Manager:

```
sh /etc/init.d/cmastorsmux stop
```

Storage SMUX Manager

Issue the following command to stop or start the Storage SMUX Manager:

```
sh /etc/init.d/cmastorsmux stop
sh /etc/init.d/cmastorsmux start
```


Trap Alarm E-mail Configuration File

HP Management Agents for Servers are capable of sending e-mail notifications in addition to SNMP traps. The configuration file `/opt/compaq/mailcfg` configures the e-mail command that is read by SMUX Manager during its initialization. This file is shared by SMUX Managers from all Management Agents for Servers packages.

NOTE: If this configuration file is edited, the SMUX Manager software must be restarted before the configuration modification is effective. You can do this by entering the following commands:

```
sh /etc/init.d/cmastorsmux stop
sh /etc/init.d/cmastorsmux start
```

Syntax of the e-mail command:

```
mail = "mail_path -s 'subject_line' destination(s)";
```

The name of the installed SCO UnixWare 7 system mail program is `mail_path`. The `subject_line` parameter defines how a subject line is entered for the mailer used in the system. The subject line must be enclosed in single quotes. The `destination(s)` parameter defines where to send trap alert messages. Multiple mail destinations might be defined in the mail line, separated by spaces.

For example:

```
mail = "/bin/mailx -s 'HP Management Agents Trap Alert' root
admin1";
```

Storage Data Collection Agents

Each HP data collection agent gathers and saves Storage MIB data to files in the HP Storage Data Registry. The data collection agents periodically update MIB data at configurable poll intervals.

The agent responsible for managing the selected MIB data item performs SNMP set commands. Data collection agents generate SNMP trap commands.

Some hardware-dependent data collection agents start automatically at boot time (this feature can be disabled). Other agents run only when started by the HP Storage SMUX Manager agent.

HP Storage Data Registry

The HP Storage data registry (`/var/spool/compaq/storage/registry`) is composed of standard SCO UnixWare 7 directories and associated files. Each file in the data registry is a logical object containing “n” related data items. For instance, IDA Physical Drive #1 contains only those MIB items related to that drive.

NOTE: Only HP Storage MIB items listed in the Data Registry MIB file `/opt/compaq/storage/etc/registry.mib` are supported by SCO UnixWare 7 data collection agents.

Configuring Data Collection Agents

For more information on configuring Data Collection Agents, select from the following:

- SCSI Agent
- IDA Monitoring Agent
- FCA Monitoring Agent

SCSI Agent

The SCSI agent gathers data for the HP SCSI MIB and the HP Storage System MIB. This data includes:

- Physical mapping and configuration data for each HP SCSI Controller.
- SCSI device inventory and error statistics for SCSI bus errors. Information is provided for SCSI attached devices including disk, tape, and CD-ROM drives.
- Usage, error statistics, and status for SCSI hard drives. Additional status information is provided for the HP ProLiant Storage System and HP hot-pluggable drives.

If there is a SCSI controller in the system, the SCSI agent should be automatically started when the SCO UnixWare 7 system enters multiuser mode.

Issue the following command to manually start the agent:

```
sh /etc/init.d/cmascsi start [poll_time]
```

where `poll_time` is the number of seconds to wait between data collection intervals. The suggested `poll_time` is 30 seconds (default). The minimum `poll_time` is 5 seconds.

NOTE: Increasing the agent `poll_time` setting improves system performance but decreases the data collection rate. Conversely, decreasing the agent `poll_time` setting increases the data collection rate but can decrease system performance.

Issue the following command to manually stop the SCSI agent:

```
sh /etc/init.d/cmascsi stop
```

Issue the following command to enable automatic startup:

```
ln -s /opt/compaq/storage/etc/cmascsi /etc/rc2.d/S99cmascsi
```

Issue the following command to disable automatic startup of the SCSI agent:

```
rm /etc/rc2.d/S99cmascsi
```

Issue the following commands to enable automatic shutdown of the agent:

```
ln -s /opt/compaq/storage/etc/cmascsi /etc/rc0.d/K01cmascsi
ln -s /opt/compaq/storage/etc/cmascsi /etc/rc1.d/K02cmascsi
```

Issue the following commands to disable automatic shutdown of the agent:

```
rm /etc/rc0.d/K01cmascsi
rm /etc/rc1.d/K01cmascsi
```

Refer to `/opt/compaq/storage/etc/registry.mib` for a complete list of supported Storage MIB items.

IDA Monitoring Agent

The IDA Monitoring agent gathers data for the HP Intelligent Drive Array (IDA) MIB. The data includes:

- IDA controller information
- IDA accelerator information
- IDA logical drive information
- IDA physical drive information

During installation, the IDA Monitoring agent is configured to start up automatically when the SCO UnixWare 7 system enters multiuser mode and shut down automatically when the SCO UnixWare 7 system exits multiuser mode.

Issue the following command to enable automatic startup:

```
ln -s /opt/compaq/storage/etc/cmaida /etc/rc2.d/S99cmaida
```

Issue the following command to disable automatic startup of the IDA Monitoring agent:

```
rm /etc/rc2.d/S99cmaida
```

Issue the following command to manually start the IDA Monitoring agent:

```
sh /etc/init.d/cmaida start [poll_time]
```

where `poll_time` is the number of seconds between data collection intervals. The suggested `poll_time` is 60 seconds (default). The minimum `poll_time` is 5 seconds.

NOTE: Increasing the agent `poll_time` setting improves system performance but decreases the data collection rate. Conversely, decreasing the agent `poll_time` setting increases the data collection rate but can decrease system performance.

If automatic startup of the IDA Monitoring agent is enabled, automatic shutdown should also be enabled.

Issue the following commands to enable automatic shutdown of the agent:

```
ln -s /opt/compaq/storage/etc/cmaida /etc/rc0.d/K01cmaida
ln -s /opt/compaq/storage/etc/cmaida /etc/rc1.d/K02cmaida
```

Issue the following commands to disable automatic shutdown of the agent:

```
rm /etc/rc0.d/K01cmaida
rm /etc/rc1.d/K02cmaida
```

Issue the following command to manually stop the agent:

```
sh /etc/init.d/cmaida stop
```

Refer to `/opt/compaq/storage/etc/registry.mib` for a complete list of supported Storage MIB items.

NOTE: You must install the “mpio” package if your system has IDA controllers running in redundant mode. Use the following command to install the “mpio” package from the SCO UnixWare 7 installation CD disk 1:

```
pkgadd -d cdrom1 mpio
```

FCA Monitoring Agent

The FCA Monitoring agent gathers data for the HP Fibre Channel Array (FCA) MIB. The data includes:

- FCA host controller information
- FCA array controller information
- FCA array accelerator information
- FCA logical drive information
- FCA physical drive information
- FCA storage system chassis information
- FCA storage system power supply information
- FCA storage system fan information
- FCA storage system temperature information
- FCA storage system backplane information

During installation, the FCA Monitoring agent is configured to start up automatically when the SCO UnixWare 7 system enters multiuser mode and shut down automatically when the SCO UnixWare 7 system exits the multiuser mode.

Issue the following command to enable automatic startup:

```
ln -s /opt/compaq/storage/etc/cmafca /etc/rc2.d/S99cmafca
```

Issue the following command to disable automatic startup of the FCA Monitoring agent:

```
rm /etc/rc2.d/S99cmafca
```

Issue the following command to manually start the agent:

```
sh /etc/init.d/cmafca start [poll_time]
```

where `poll_time` is the number of seconds between data collection intervals. The suggested `poll_time` is 60 seconds (default). The minimum `poll_time` is 5 seconds.

NOTE: Increasing the agent `poll_time` setting improves system performance but decreases the data collection rate. Conversely, decreasing the agent `poll_time` setting increases the data collection rate but can decrease system performance.

If automatic startup of the FCA Monitoring agent is enabled, automatic shutdown should also be enabled.

Issue the following commands to enable automatic shutdown of the agent:

```
ln -s /opt/compaq/storage/etc/cmafca /etc/rc1.d/K02cmafca
ln -s /opt/compaq/storage/etc/cmafca /etc/rc0.d/K01cmafca
```

Issue the following commands to disable automatic shutdown of the agent:

```
rm /etc/rc1.d/K02cmafca
rm /etc/rc0.d/K01cmafca
```

Issue the following command to manually stop the agent:

```
sh /etc/init.d/cmafca stop
```

Refer to `/opt/compaq/storage/etc/registry.mib` for a complete list of supported Storage MIB items.

NOTE: Before each hard drive in the FCA storage can be used, a stamping procedure must be performed. To perform this stamping procedure, run the utility program located in the directory file `/usr/bin/compaq/diags/casa/casacfg`.

NIC Agents

HP NIC SMUX Manager

The NIC SMUX Manager extends the SNMP “enterprise” MIB to include MIB data. The NIC SMUX Manager supports get, set, and trap operations on data items defined in the NIC MIB and the MIB-2 Transmission dot3 (Ethernet) and dot5 (token ring) MIBs defined in RFC1398 and RFC1231, respectively.

HP NIC MIB data is gathered by the data collection agent process (NIC agent). The NIC agent collects and saves MIB data in files that are read by the NIC SMUX Manager during SNMP get commands. The NIC SMUX Manager routes SNMP set commands to the NIC agent. SNMP trap commands are generated by NIC agent and routed by the NIC SMUX Manager to the SNMP daemon.

At NIC SMUX Manager startup time, NIC MIB items in the file `/opt/compaq/nic/etc/cmanicsmuxd.defs` are registered with the SNMP daemon. Not all MIB items listed in the file `cmanicsmuxd.defs` can be supported by SCO UnixWare 7 NIC data collection agent. Only MIB items listed in the NIC Data Registry MIB file `/opt/compaq/nic/etc/registry.mib` are supported by SCO UnixWare 7 NIC data collection agent.

During the installation, the NIC SMUX Manager Agent is configured to start up automatically when the SCO UnixWare 7 system enters multiuser mode and shut down automatically when the SCO UnixWare 7 system exits the multiuser mode.

Issue the following command to enable automatic startup:

```
ln -s /opt/compaq/nic/etc/cmanicsmux /etc/rc2.d/S98cmanicsmux
```

Issue the following command to disable automatic startup of the NIC SMUX Manager:

```
rm /etc/rc2.d/S98cmanicsmux
```

Issue the following command to manually start the NIC SMUX Manager:

```
sh /etc/init.d/cmanicsmux start
```

If automatic startup of the NIC SMUX Manager is enabled, automatic shutdown should also be enabled.

Issue the following commands to enable automatic shutdown of the NIC SMUX Manager:

```
ln -s /opt/compaq/nic/etc/cmanicsmux /etc/rc0.d/K01cmanicsmux
```

```
ln -s /opt/compaq/nic/etc/cmanicsmux /etc/rc1.d/K01cmanicsmux
```

Issue the following commands to disable automatic shutdown of the NIC SMUX Manager:

```
rm /etc/rc0.d/K01cmanicsmux
rm /etc/rc1.d/K01cmanicsmux
```

Issue the following command to manually stop the NIC SMUX Manager:

```
sh /etc/init.d/cmanicsmux stop
```

Trap Alarm E-mail Configuration File

Management Agents for Servers are capable of sending e-mail notifications in addition to the SNMP traps. The configuration file `/opt/compaq/mailcfg` configures the e-mail command read by the NIC SMUX Manager during its initialization. This file is shared by SMUX Managers from all Management Agents for Servers packages.

NOTE: If this configuration file is edited, the NIC SMUX Manager software must be restarted before the configuration modification is effective. Restart the software by entering the following commands:

```
sh /etc/init.d/cmanicsmux stop
sh /etc/init.d/cmanicsmux start
```

Syntax of the e-mail command:

```
mail = "mail_path -s 'subject_line' destination(s)";
```

The name of the installed SCO UnixWare 7 system mail program is `mail_path`. The `subject_line` parameter defines how a subject line is entered for the mailer used in the system. The subject line must be enclosed in single quotes. The `destination(s)` parameter defines where to send trap alert messages. Multiple mail destinations can be defined in the mail line, separated by spaces.

For example:

```
mail = "/bin/mailx -s 'HP Management Agents Trap Alert' root
admin1";
```

NIC Data Collection Agent

The NIC agent gathers data for the NIC MIB and the MIB-2 Transmission dot3 (Ethernet) and dot5 (token ring) MIBs defined in RFC1398 and RFC1231, respectively. The data includes:

- Physical mapping and configuration data for each network interface. Information is provided for HP controllers, most EISA NICs, ISA NICs with EISA configuration files, and AMD PCI NIC.
- Network error statistics for Ethernet interfaces. Information is provided for HP controllers. Limited information is provided for other NICs.
- Network status and error statistics for token ring interfaces. Information is provided for HP controllers. Limited information is provided for other NICs.

During installation, the NIC agent is configured to start up automatically when the SCO UnixWare 7 system enters multiuser mode and shut down automatically when the SCO UnixWare 7 system leaves the multiuser mode.

Issue the following command to enable automatic startup:

```
ln -s /opt/compaq/nic/etc/cmanic /etc/rc2.d/S99cmanic
```

Issue the following command to disable automatic startup of the NIC agent:

```
rm /etc/rc2.d/S99cmanic
```

Issue the following command to manually start the agent:

```
sh /etc/init.d/cmanic start
```

If automatic startup of the NIC agent is enabled, automatic shutdown should also be enabled.

Issue the following commands to enable automatic shutdown:

```
ln -s /opt/compaq/nic/etc/cmanic /etc/rc0.d/K02cmanic  
ln -s /opt/compaq/nic/etc/cmanic /etc/rc1.d/K02 cmanic
```

Issue the following commands to disable automatic shutdown of the NIC agent:

```
rm /etc/rc0.d/K02cmanic  
rm /etc/rc1.d/K02cmanic
```

Issue the following command to manually stop the agent:

```
sh /etc/init.d/cmanic stop
```

Refer to `/opt/compaq/nic/etc/registry.mib` for a complete list of supported MIB items.

Insight Management Agents for Servers Issues

Inability to Perform Remote Reboot on a Server from the Management Console

1. Load CPQAGIN.
2. Verify that Remote Reboot is enabled.
3. Verify that Sets are enabled.

Global Unique Identifiers are the Same for All Devices When Using Disk Imaging Software on Servers

Solution 1: If the disk image has not been taken, perform the following after installing the Insight Management Agents on the source machine and capture the image before restarting the Insight Management Agents.

1. Uninstall all Insight Management Agents from one of the devices.
2. Use the Disk Imaging software to copy the configuration from the device without the Insight Management Agents installed.
3. Use the disk image to copy to the target devices.
4. Reinstall the Insight Management Agents on all the devices.

Solution 2: If the disk image has already been deployed, perform the following to remove the image from each target device. The following information is divided by network Operating Systems.

- NetWare—The Globally Unique Identifier information is stored in a 16-byte file on the SYS:\SYSTEM subdirectory of the NetWare server. This file is created and populated with the Globally Unique Identifier when HP Systems Insight Manager performs an SNMP SET command to the NetWare server. To remove the permanence of the Globally Unique Identifier:
 - a. Delete the file \SYSTEM\CPQBSSA.CFG in the NetWare SYS volume.
 - b. After the file is deleted, restart the Management Agents and HP Systems Insight Manager assigns a new Globally Unique Identifier when the system is discovered.

- Microsoft Windows NT—Insight Management Agents create the Globally Unique Identifier information in an entry in the Microsoft Windows NT registry. To remove permanence of the Globally Unique Identifier:
 - a. Remove the entry:
`HKEY_LOCAL_MACHINE\SOFTWARE\Compaq Insight Agent\hostGUID`
 - b. After the entry is removed, restart the Insight Management Agents services. A new Globally Unique Identifier is automatically generated.
- SCO UnixWare 7—The Globally Unique Identifier information is stored in a file that is created and populated with the Globally Unique Identifier when HP Systems Insight Manager performs an SNMP SET command to the SCO UnixWare 7 server. To remove the permanence of the Globally Unique Identifier:
 - a. Delete the following file from the SCO UnixWare 7 system:
`/var/spool/Compaq/foundation/registry/cpqhoguid.dat`
 - b. After this file has been deleted, restart the Management Agents. HP Systems Insight Manager assigns a new Globally Unique Identifier when the system is discovered.

When Changing the Access Level, a Valid Account and Password for the System Management Homepage are Accepted, but the Web Page Indicates that a Different Account Is Logged In

For some browsers, this occurs when pages previously accessed are stored in the cache of the browser (Internet caching). When accessing these pages again, the browser displays them from the cache, instead of regenerating the pages. Management HTTP Server does not support Internet caching. To disable Internet caching:

1. From Microsoft Internet Explorer:
 - a. Select **Tools>Internet Options**.
 - b. Select **Settings** under the **General** tab.
 - c. Be sure that you have the **Every Visit to the page** radio button selected in the Check for newer versions of the stored pages section.
2. For Netscape:
 - a. Select **Edit Preferences>Advanced** (expand)>**Cache**.
 - b. Under the Compare the page in the cache to the page on the network heading, select the **every time I view the page** radio button.

NOTE: Be sure you have enabled cookies in the browser. They are required for security.

When Attempting to Browse to Web-Enabled System Management Software On Port 2381, the Following Message Appears

This system is not fully configured and is not accessible because there is not a valid administrator password. An administrator password must be configured by either reinstalling the Web-enabled System Management software or following the instructions in the Security white paper located at <http://www.hp.com/manage>.

The system was installed without configuring the passwords for the administrator, operator, or user accounts. Setting an administrator password is required for Web-Enabled System Management software to function correctly.

To resolve, perform one of the following actions:

- Consult the installation instructions for your Web-Enabled System Management software for information about how to use the system software configuration tool to preconfigure components before silent updates.
- Reinstall the software after configuring the component package to contain an account password.
- Install the software using a manual procedure to be prompted for the password on the managed device.
- Use the HP Systems Insight Manager application launch feature to update the CPQHMMMD.ACL on servers already installed.

NOTE: The HP Systems Insight Manager application launch feature should only be administered as a last resort.

NOTE: For more information on overall security features, refer to the *Understanding HP Systems Insight Manager Security* white paper (15PJ-1001A-WWEN) on the Management CD.

The Windows NT Software has been tested with the following browsers:

- Microsoft Internet Explorer 4.01, 5.0, or later and Netscape Communicator 4.51, 4.7, or later on Windows 95, Windows 98, Windows Millennium Edition, Windows NT 4.0, and Windows 2000
- SNMP configuration pages have been tested under Microsoft Internet Explorer 5.0 or later. Netscape Communicator is not supported.

The Novell NetWare software has been tested with the following browsers:

- Microsoft Internet Explorer 4.01, 5.0, or later and Netscape Communicator 4.51, 4.7, or later on Windows 95, Windows 98, Windows Millennium Edition, Windows NT 4.0, and Windows 2000

The SCO UnixWare 7 software has been tested with the following browsers:

- Microsoft Internet Explorer 5.0 and Netscape Communicator 4.70 on Windows NT 4.0 and Windows 2000
- Netscape Communicator 4.61 on SCO UnixWare 7.1.1 and SCO UnixWare 7.1.3

The minimum browser requirements must be met for the Insight Management Agents for Servers to work correctly.

Depending on how they were implemented, some browsers might or might not work correctly when used with different operating systems.

Known Browser Issues

- Internet Explorer does not print background colors and images by default.
- When switching from the Insight Management Agents browser window to another application, colors in the browser window change or flash. This is not specific to the window, but might happen when looking at other pages with a browser under the same conditions.
- When the browser window is resized with Netscape Navigator 4.x, the window or frames within the window might go blank. This is because JavaScript in the page is not being evaluated. To view the screen, right-click in the frame and select **Reload Frame**.
- Frame sizes are optimized for medium-sized fonts. If you switch your browser to use larger or smaller fonts, then you must manually adjust the frame layout.
- A JavaScript error might occur when displaying an IML page containing a very large IML in Netscape Navigator.

NOTE: A large IML does not cause an error in Internet Explorer, but it does take a long time to load (more than four minutes).

- When a set operation is executed in Internet Explorer, the browser opens a new window to display the updated template page if the security settings are configured to medium or high. To resolve this problem, set the security level to low.

To set the security level to low:

- a. Select **Internet Options** from the **View** menu in the browser.
 - b. Select the **Security** tab, and then click **Custom Level**.
 - c. Select **Low**.
 - d. Click **Reset>OK**.
- There are known browser issues in the Management Agents for Tru64 UNIX. However, many have been corrected in later releases. Refer to the *Management Agents for AlphaServers for Tru64 UNIX Reference Guide*.

SNMP Community String Issues

- In NetWare, the community string can be changed through the INETCFG utility. After the community string has been changed, the administrator must restart the server at a convenient time to have the change take effect. This restarts the Novell SNMP with the new community string and enables the Web Agent to utilize it.
- In Windows NT, if the SNMP community string is changed, the SNMP service does not recognize the change until the SNMP service is stopped and restarted from the Services Control Panel applet. If the SNMP service is not stopped and restarted, then the Web Agent is unable to get any SNMP data and the HTML pages do not contain any data.
Service Pack 4 for Microsoft Windows NT 4.0 enables SNMP community strings with read-only access or no access to be added to a system. If a read-only or read/write community string has not been defined, then the Web Agent is unable to get any SNMP data and the HTML pages do not contain any data. Unless a read/write community string is defined, you do not have write access, even if you log on to the Web Agent as administrator or operator.
- In Windows Server 2003, manually configure the community string:
 - a. From the Start menu, select **Programs>Administrative Tools>Services**.
 - b. Double-click **SNMP Service**, and then select the **Traps** tab.
 - c. In the Community Names field, enter a community name string. If a community name already exists, select it. If one does not exist, enter `public` in the Community Names field, and select Add. The default community string for Insight Manager is `public`. If a different community string is entered here, it must also be entered on the management console that is responsible for the system. To change the community string (community strings are case-sensitive) in HP Systems Insight Manager, refer to the *HP Systems Insight Manager User Guide* section, “Setting Up SNMP Community Strings.”
 - d. Under the Trap Destinations list, click **Add**.
 - e. In the IP Host/Address or IPX Address field, enter the IP address of the management console. This address identifies the management console to receive the alert when the Server Agents detect a significant event.
 - f. Click **Add>OK**.

IMPORTANT: For Windows Server 2003, Windows 2000, Windows NT, NetWare 5.1, and NetWare 6.0 (SNMP Only), you must enter the Monitor and Control community strings for this device. The Insight Management Agents and HP Systems Insight Manager use these community strings to communicate with the OS SNMP service. If you elect not to create a Control community string, certain operations cannot be performed, such as clearing the IML or changing agent configuration settings.
- In Tru64 UNIX, the SNMP daemon must be stopped and restarted before a change in the SNMP community string is recognized. To stop and start the SNMP daemon, log in as `root` and use the following commands, respectively.

```
# /usr/sbin/snmpd stop
#/usr/sbin/snmpd start
```

Management Agents for Servers for Windows Issues

As a preliminary troubleshooting step, always examine the Windows Event Log by starting the Event Viewer application. Management Agents for Servers and other installed software log significant events into the Windows Event Log, which might help in diagnosing a problem. Also, always install all HP drivers from the SmartStart CD before installing the Management Agents for Servers.

Installation Issues

Cannot Manage an HP 32-Bit SCSI-2 Controller

If you add an HP 32-bit SCSI-2 controller to an existing managed server, you must activate the SCSI Information agent.

1. From the Control Panel, run the Management Agents.
2. Select the **Service** tab to display the list of active and inactive agents. A SCSI filter monitor is required for SCSI management.
3. Select **SCSI Information** from the list of Inactive Agents, and then click **Add** to move it to the Active Agents list.
4. Click **OK**. When prompted to restart the Management Agents, click **Yes**.

Insight Manager Cannot Manage a System

If you installed the Microsoft SNMP service after installing the Management Agents for Servers, you must run **Install** from the Management CD, and select **Express** to automatically update the Management Agents.

Cannot Delete the CPQMGMT.CPL File When Uninstalling or Upgrading

If you are running Windows 2000, you must close the Control Panel before deleting the CPQMGMT.CPL file.

Insight Manager Issues

Device Not Manageable

A BLACK indicator appears for the device on the device list.

1. Verify that the TCP/IP and SNMP services are installed and running under Windows. Check the Services Control Panel application for status.
2. Verify that Management Agents for Servers are installed and running under Windows. Check the Services Control Panel application for Insight Agents.
3. Verify that the device community string matches the community string specified in Insight Manager. The device community string is located in the Networks Control Panel application under Configure SNMP Service. The Insight Manager community string is set in the Device Setup window from the management console (select **Device Setup** from the Task List window). For more information, refer to “Setting Up SNMP Community Strings” in the *HP Insight Manager User Guide*.

NOTE: Community strings are case-sensitive.

4. Verify that network communications with Insight Manager are operational. Invoke the Windows ping command from an MS-DOS prompt.
5. If the SNMP service was installed after the Management Agents for Servers software, then rerun the Server Agents setup program. Always install the agent software **after** the SNMP service.

A Majority of Buttons for the Device are Disabled

The System Information Agent is not loaded.

Open the Server Agents Control Panel by double-clicking the icon in the Windows Control Panel. Verify that the System Information Agent is located under the active Agents.

Missing Network Interface Controller Information

Management Agents for Servers for Windows provides full information on NICs if three conditions are met.

1. The interface must be bound to the TCP/IP protocol stack. You can verify the NIC bindings by entering the Bindings section of the Network Control Panel application.
2. The interface cannot be bound to an intermediate driver (“virtual NIC”) unless the intermediate driver is specifically supported by the HP NIC Agents. Examples of supported intermediate drivers are HP Network Fault-Tolerant drivers.
3. To include all of the interface statistics, the NIC driver must support the optional NDIS Object IDs (OIDs) for management information. All HP controllers support these OIDs. For other controllers, contact your hardware vendor.

Missing Drive Array Physical Drive Information

The HP Drive Array device driver can provide full information on HP Drive Arrays only when the drives are properly initialized. All drives currently shipped with HP systems were initialized in the factory. However, if you replaced a drive because of a hardware failure, or if you purchased the computer system before this service was provided, these drives might not be initialized.

1. Shut down Windows from the Start menu by selecting **Shutdown>Restart**.
2. Run HP Diagnostics. If you do not have HP Diagnostics on the hard drive, create an HP diagnostics diskette using Diskette Builder. Insert the HP Diagnostics diskette into the diskette drive of the monitored system, or run Diagnostics from the hard drive.
3. Restart the system.
4. At the Main Program menu, select **Test Computer**.
5. At the next display screen, select **View Device List**.

NOTE: The HP Diagnostics utility initializes physical drives attached to HP Drive Arrays.

Disk Subsystem Button Disabled in the Disk Storage Window

This might result because the Drive Array Agent is not loaded.

Open the Management Agents by selecting the icon from the Windows Control Panel. Verify that the Drive Array Information is located in the Active Agents lists.

SCSI Adapter Button is Disabled

This might result because the HP device driver is not loaded.

Load the device driver using one of the following methods:

- If you have an HP SCSI controller in your monitored system, load the correct device driver. Refer to the ProLiant Support Pack for Microsoft Windows 2000 or the ProLiant Support Pack for Microsoft Windows NT 4.0 for details on loading the appropriate driver. If the SCSI device is located on a SCSI controller that is not supported, such as the HP 6260 controller, the button remains disabled.
- If the SCSI device driver was installed after the Management Agents software, run the install program from the distribution media and select **Update Express**. The Management Agents for Servers software does not load SCSI device monitor software unless an instrumented device driver, such as an HP SCSI device driver, is present.
- If the SCSI Adapter button is disabled, open the Management Agents by selecting the icon from the Windows Control Panel. Verify that the SCSI Information agent is located in the Active Agents list.

Disk Subsystem Button is Missing in the Disk Storage Window

A missing Drive Array or SCSI Adapter button indicates that the monitored device is not properly configured.

Run the HP System Configuration Utility to configure your system properly, or run the Setup Utility to configure your ISA system properly.

No SNMP Traps or Alarms Received

SNMP is not configured correctly.

1. Open the **Network Control Panel** by selecting the icon from the Windows Control Panel, select the **SNMP Service**, and click **Configure**.
2. Verify that the SNMP Service is correctly configured with the appropriate destination information. Be sure the community name and host name/IP address is configured correctly.
3. Use the Event Viewer to see if the system event log is full. If the event log is full, SNMP cannot generate traps.
4. Use Test Trap from the Management Agents for Servers Control Panel to verify correct operation.

Problems Using Thresholds and SNMP Address-Specific Security

Management Agents for Servers cannot read thresholds when SNMP address-specific security is enabled. Thresholds can be configured from Insight Manager, but no traps are received. When an agent event with ID 2355, Category 9 occurs, the following text appears in the System Event Log:

```
The Threshold Server Agent SNMP API failed. The data contains the error code.
```

This error occurs because the device cannot issue SNMP requests to itself.

1. From the Control Panel, select the **Network** icon.
2. In the Installed Network Software List, select **SNMP Service**.
3. Select **Configure>Security**.
4. In the SNMP Security Configuration dialog box, enter localhost or the address 127.0.0.1 to the list of host addresses from which the SNMP agent accepts packets.
5. Click **OK** to exit the SNMP Security Configuration dialog box.
6. Click **OK** to exit the Network Settings dialog box.
7. Reboot to make the changes take effect.

Problems if the Address 127.0.0.1 is not Added to SNMP Host List

The following problems occur **only** if the address 127.0.0.1 is not added to the SNMP host list if SNMP host security is used in Windows NT or Windows 2000.

- The following Event Log error messages appear:

```
The HP Foundation Agents service could not terminate agent  
"CPQMHOST". The data contains the error code.  
  
The HP Foundation Agents service could not start agent  
"CPQMHOST". The data contains the error code.
```
- NIC information does not appear.
- Server Status Information appears incorrectly. For example, the Server Status information is highlighted in green. However, when the customer drills down to mass storage, the Server Status information is highlighted in red. Therefore, the upper-level view of the information incorrectly displays the status of the server.

The customer must add the address 127.0.0.1 to the SNMP host list if SNMP host security is used. The Management CD provides a utility that adds the address 127.0.0.1 to the host list if the customer does not want to add it manually. The utility file is named lhost.exe and is located in SP12205.

Missing ProLiant Storage System Information

The ProLiant Storage System driver is not installed.

Verify that the ProLiant Storage System driver appears under the Devices Control Panel icon in Windows NT 4.0. In Windows 2000 select the **Administrative Tools Control Panel** icon and then the **Computer Management** icon. The driver is shown under the System Devices in Device Manager. If it is not listed, install it from the ProLiant Support Pack for Microsoft Windows NT 4.0 or the ProLiant Support Pack for Microsoft Windows 2000.

ASR POST Failure Reported

This is caused by an older version of the Systems Management driver.

Upgrade the Systems Management driver from the latest version of the SmartStart CD.

Management Agents for Servers

The Windows NT software has been tested with Microsoft Internet Explorer 4.0 on Microsoft Windows NT 4.0, and with Netscape Navigator 4.04 on Microsoft Windows NT 4.0.

The minimum browser requirements must be met for the Web-Enabled Management Agents for Servers to work correctly.

Depending on how they were implemented, some browsers might not work correctly when used with different operating systems.

Other Problems

Tape Device Error Detected by Windows Backup

At startup, the Windows backup application returns the following error message:

```
Tape Drive Error Detected
```

A tape drive has been detected and the tape driver has been started. However, the tape drive is not responding. Be sure the tape device power is on and cables are properly connected.

This message appears if the SCSI Information Agent is collecting data from the tape drive while the backup software is attempting to start (since only exclusive access to the tape drive is allowed). If this message appears:

1. Select **Operation>Hardware Setup**.
2. Reselect the tape drive to use. If these actions do not eliminate the error message, the tape drive might not be functioning properly.

Management Agents for Servers for NetWare Issues

Inability to Change any Values on the Managed System or to Mark Errors as Corrected

1. Verify that the SNMP NLM was loaded with the proper community string settings.
2. Verify that the community string setting on your management application agrees with the one set on your NetWare server when you loaded the SNMP NLM. For Insight Manager, select **Device Setup** from the Task List window. The community string is set in the Device Setup window.
3. Verify that sets are enabled using CPQAGIN.

No SNMP Traps or Alarms Received for NetWare

Verify that the TRAPTARG.CFG file contains appropriate destination information. A sample TRAPTARG.CFG file is located on the Server Management Agents for NetWare diskette in the \NOVELL\ETC directory. It should be stored on your NetWare SYS volume in the \ETC directory. When entering trap target addresses, be sure you enter the address in the appropriate protocol section and indent each address.

System Restart to Disk-Based Utilities Fails for NetWare

If you click **Reboot** on the Insight Manager display, and select the option to boot to the disk-based utilities, the server might fail to start the disk-based utilities. Use the System Configuration Utility to verify that the utilities are actually installed on the system partition.

Inability to View Web Pages on the NetWare Server

1. Verify that the latest Novell operating system patch is installed on the server to provide a recent version of TCPIP.NLM. Download the latest patch from the Novell Website, and install the patch on the server.
2. Verify that a HOSTS file resides on the NetWare server in the SYS:ETC subdirectory. The HP HMMO Utility (CPQHMMO) requires a HOSTS file to support server Web pages from the server. This file contains the IP address and the server name.

NOTE: The Novell NetWare software has been tested with Microsoft Internet Explorer 4.0, 5.0, or higher and Netscape Navigator 4.05, 4.51, and 4.70.

Management Agents for Servers for SCO UnixWare 7 Issues

HP Systems Insight Manager Issues

The Utilization Button is Grayed-Out

Check the Host OS agent status with the SCO UnixWare 7 command `ps -ef | grep cmahostd`. If the agent is not running, verify that the agent startup line in the Foundation SMUX Configuration file, `/opt/compaq/foundation/etc/config`, has not been commented out. If the agent is commented out or missing in the Foundation SMUX Configuration file, uncomment or add the startup line, then stop and restart the Foundation SMUX Manager using following commands:

```
/etc/init.d/cmafdtntsmux stop
/etc/init.d/cmafdtntsmux start
```

If the agent is running and not reporting data, or if it was correctly started but is no longer running, check the file `/var/spool/compaq/agenterrs.log` for error messages. You must be logged in as `root` to access this file.

File System Space Used Information is Missing in the Mass Storage Window

Check the Host OS agent status with the SCO UnixWare 7 command `ps -ef | grep cmahostd`. If the agent is not running, verify that the agent startup line in the Foundation SMUX Configuration file, `/opt/compaq/foundation/etc/config`, has not been commented out. If the agent is commented out or missing in the Foundation SMUX Configuration file, uncomment or add the startup line, then stop and restart the Foundation SMUX Manager using following commands:

```
/etc/init.d/cmafdtntsmux stop
/etc/init.d/cmafdtntsmux start
```

If the agent is running and not reporting data, or if it was correctly started but is no longer running, check the file `/var/spool/compaq/agenterrs.log` for error messages. You must be logged in as `root` to access this file.

System Board, Expansion Boards, or Configuration Buttons are Grayed-Out

Check the Standard Equipment agent status with the SCO UnixWare 7 command `ps -ef | grep cmastdeqd`. If the agent is not running, verify the agent startup line in the Server SMUX configuration file, `/opt/compaq/server/etc/config`, has not been commented out. If the agent is commented out or missing in the Server SMUX Configuration file, uncomment or add the startup line, then stop and restart the Server SMUX Manager using:

```
/etc/init.d/cmasvrsmux stop
/etc/init.d/cmasvrsmux start
```

If the agent is running and not reporting data, or if it was correctly started but is no longer running, check the file `/var/spool/compaq/agenterrs.log` for error messages. You must be logged in as `root` to access this file.

SCSI Drive Information is Missing in the Mass Storage Window

Check the SCSI agent status with the SCO UnixWare 7 command `ps -ef | grep cmascsid`. If the agents are not running, they must be started (refer to the start/stop documentation for the appropriate agent).

If the agent is running and not reporting data or, if it was correctly started but is no longer running, check the file `/var/spool/compaq/agenterrs.log` for error messages. You must be logged in as `root` to access this file.

Added SCSI Devices Do Not Appear

To minimize system overhead, the `cmascsid` process does not search for new hardware every `poll_time`. There will be a delay of up to 32 times the poll interval, which is normally every 30 seconds, up to 16 minutes in the default case, before new SCSI devices are discovered by `cmascsid` and reported to Insight Manager. After the hardware has been discovered, its status is checked each `poll_time` and reported to Insight Manager when it has changed.

SCSI Activity Counters Seem too Low

All SCSI activity counters are restarted each time the operating system is rebooted. When Insight Manager displays the counters as rates, the rate is based on the difference between the last two instances the device was polled by Insight Manager. The numbers obtained by Insight Manager are the values based on the last time the `cmascsid` process checked them before the poll by Insight Manager. The poll time of the `cmascsid` process can be reduced to improve the accuracy of the rates reported by Insight Manager.

SCSI Hard Drive Serial Number or Capacity is Missing or 0-Value

Most SCSI hard drives do not make this information available to the host when the drive media are not spinning. Hot-pluggable drives do not start spinning until the operating system attempts to open them. Obtaining this information requires access to the drive. After the drive is first opened, to minimize system overhead, there can be a delay of up to 32 times the poll time of the `cmaocsid` process before updated information is available to Insight Manager.

A Large Number of SCSI Bus Timeouts Appear for a Drive

A SCSI bus timeout occurs when the SCSI agent attempts to select a device on the SCSI bus and send it a command, but no device answers for that SCSI ID within a specified time. After every 32 times the `cmaocsid` process polls, it checks the SCSI bus for new devices. For each SCSI ID where no device responds, a SCSI bus timeout is recorded. The device might fail to respond because a HP hot-pluggable drive is removed or an external device is not powered. This counter should not increase while a powered drive configured for this ID is properly connected to the SCSI bus and the SCSI bus is properly terminated.

A SCSI Controller Button is Grayed-Out

Information about the configuration of the device indicates that a SCSI controller is installed but no further information is available. Several conditions result in a grayed-out button:

- The SCSI agent process `cmaocsid` might not be running.
- The HP System Configuration Utility might have disabled the SCSI controller.
- This might be an unsupported controller.

Drive Array is Missing in the Mass Storage Window

Check the Mass Storage agent status with the SCO UnixWare 7 command `ps -ef | grep cmaidad`. If the agent is not running, it must be started (refer to the start/stop documentation for the appropriate agent).

If the agent is running and not reporting data, or if it was correctly started but is no longer running, check the file `/var/spool/compaq/agenterrs.log` for error messages. You must be logged in as `root` to access this file.

Indicator and Statistics Buttons are Grayed-Out in the Drive Array Physical Drive Window

You have not stamped the physical drives in this drive array controller. Run the HP Diagnostics utility to stamp the drives.

IDA Controllers Are Grayed-Out In the Mass Storage Window

Check the IDA Monitoring agent status with the SCO UnixWare 7 command `ps -ef | grep cmaidad`. If the agent is not running, it must be started (refer to the start/stop documentation for the appropriate agent).

FCA Controllers are Grayed-Out in the Mass Storage Window

Check the FCA Monitoring agent status with the SCO UnixWare 7 command, `ps -ef | grep cmafca`. If the agent is not running, it must be started (refer to the start/stop documentation for the appropriate agent).

Recovery Button is Grayed-Out in the Device View Window

- Check to be sure your system supports the System Health agent features. These features are supported only on ProLiant servers.
- Check the System Health agent status with the SCO UnixWare 7 command `ps -ef | grep cmahealthd`. If the agent is not running, it must be started (refer to the start/stop documentation for the System Health agent).

Auto Recovery Button is Grayed-Out in the Recovery Window

- Check to be sure your system supports this feature. This feature is supported only on ProLiant servers.
- Check the System Health agent status with the SCO UnixWare 7 command `ps -ef | grep cmahealthd`. If the agent is not running, it must be started (refer to the start/stop documentation for the System Health agent).

Correctable Memory Button is Grayed-Out

Correctable memory errors cannot be obtained from your system.

- Check to be sure your system supports this feature. This feature is supported only on ProLiant servers.
- Check the System Health agent status with the SCO UnixWare 7 command `ps -ef | grep cmahealthd`. If the agent is not running, it must be started (refer to the start/stop documentation for the System Health agent).

Environment Button is Grayed-Out in the Recovery Window

Information about the environmental conditions of the system cannot be obtained.

- Check the System Health agent status with the SCO UnixWare 7 command `ps -ef | grep cmahealthd`. If the agent is not running, it must be started (refer to the start/stop documentation for the System Health agent).
- Check to be sure your system supports this feature. This feature is supported only on ProLiant servers.

Remote Insight Button is Grayed-Out in the Recovery Window

A grayed-out Remote Insight button can be caused by one of the following:

- The Remote Insight Controller might not be configured properly.
- The Remote Insight driver might not be installed.
- The Remote Insight Agent `casm2d` might not be running.

SNMP-Based Management Program Issues

Values Cannot Be Changed on the Managed Server

Be sure that the SNMP daemon, the SMUX Manager and the agent processing the set are all running. Check the agent command line arguments in the `/opt/compaq/foundation/etc/config`, `/opt/compaq/server/etc/config`, or `/etc/init.d/cma` files. Verify that the argument `-s OK` is present for the agent. This enables SNMP sets for this agent only.

Verify that the server SNMP community string name defined in the file `/etc/netmgt/snmpd.comm` matches the community string defined at the management console. If you are using Insight Manager, view the Task List window and select **Server Setup** for your device (for more information, refer to the section covering community strings in the Insight Manager User Guide help file). Also, verify that the server SNMP access permissions in `/etc/netmgt/snmpd.comm` are set to WRITE (to enable read/write access).

Thresholds Cannot Be Set on HP MIB Items

Check the Threshold agent status with the SCO UnixWare 7 command `ps -ef | grep cmathreshd`. If the agent is not running, verify that the agent startup line in the Foundation SMUX Configuration file, `/opt/compaq/foundation/etc/config`, has not been commented out. If the agent is commented out or missing in the Foundation SMUX Configuration file, uncomment or add the startup line, then stop and restart the Foundation SMUX Manager using following command:

```
/etc/init.d/cmafdtmsmux stop
/etc/init.d/cmafdtmsmux start
```

If the agent is running and not reporting data or, if it was correctly started but is no longer running, check the file `/var/spool/compaq/agenterrs.log` for error messages. You must be logged in as `root` to access this file.

Verify that the server SNMP community string name defined in the file `/etc/netmgt/snmpd.comm` matches the community string defined at the management console. If you are using Insight Manager, view the Task List window and select **Server Setup** for your device (for more information, refer to the *HP Insight Manager User Guide*). Also, verify that the server SNMP access permissions in `/etc/netmgt/snmpd.comm` are set to WRITE (this means read/write access).

If sets still do not work, stop the Foundation SMUX Manager software using `sh /etc/init.d/cmafdtnsmux stop`. Delete previous alarm threshold files with the command `rm -f /var/spool/compaq/foundation/registry/threshold/`, then start the Foundation SMUX Manager using `sh /etc/init.d/cmafdtnsmux start`.

No SNMP Traps/Alarms are Received

Be sure that SNMP daemon, the SMUX Manager, and the agent that generates the trap are all running.

Check the `/etc/netmgt/snmpd.trap` file on your SCO UnixWare 7 device. Be sure an IP address is defined that matches the IP address of your management station, followed by the SNMP trap port 162. Test traps by setting a threshold on an item that will cause a trap using the Set Threshold feature of Insight Manager (refer to the section, Set Threshold, in the *HP Insight Manager User Guide* for more information).

If traps still do not function, try having your SCO UnixWare 7 device send traps to itself. Run the SCO UnixWare 7 SNMP trap-receive utility, `trap_rece`. Next, generate a trap using the SCO UnixWare 7 `trap_send` utility. The SCO UnixWare 7 `trap_rece` should display the trap. Be sure there are no blank lines or extra spaces in the `/etc/netmgt/snmpd` files. The `snmpd` daemon is very particular about the contents of the `/etc/netmgt/snmpd` files.

No User-Defined SNMP Traps are Received

Check the Threshold agent status with the SCO UnixWare 7 command `ps -ef | grep cmathreshd`. If the agent is not running, verify the agent startup line in the Foundation SMUX Configuration file, `/opt/compaq/foundation/etc/config`, has not been commented out. If the agent is commented out or missing in the Foundation SMUX Configuration file, uncomment or add the startup line, and then stop and restart the Foundation SMUX Manager using:

```
/etc/init.d/cmafdtnsmux stop
/etc/init.d/cmafdtnsmux start
```

Check the Threshold agent command line arguments. Verify that the argument `-t OK` is present in the `/opt/compaq/foundation/etc/config` file. This enables traps for this agent only.

If the agent is running and not reporting data or, if it was correctly started but is no longer running, check the file `/var/spool/compaq/agenterrs.log` for error messages. You must be logged in as `root` to access this file.

Management Agent Issues

Disabling SNMP Sets for a Specific Agent

Stop the SMUX Manager and the agents associated with the desired MIB. Change the agent command line argument set switch to `-s NOT_OK` in the `/opt/compaq/foundation/etc/config`, `/opt/compaq/server/etc/config`, or `/etc/init.d/cma` file. This disables SNMP sets for this agent only. Restart the stopped SMUX Manager and agent.

Disabling SNMP Traps for a Specific Agent

Stop the SMUX Manager and the agent. Change the agent command line argument trap switch to `-t NOT_OK` in the `/opt/compaq/foundation/etc/config`, `/opt/compaq/server/etc/config`, or `/etc/init.d/cma` file. This disables SNMP traps for this agent only. Restart the stopped SMUX Manager and agent.

Disabling Remote Reboot

Stop the Server SMUX Manager. Edit the file `/opt/compaq/server/etc/config`. Change the `cmastdeqd` agent command line reboot switch to `-r NOT_OK`. This disables SNMP reboots for this device only. Restart Server SMUX Manager.

“cmascsid” Process Does Not Start Automatically as the System Enters Multiuser Mode

Enter the `sh /etc/init.d/cmascsi start` command to start the process. If the process does not start, refer to the message preceding the command, and be sure that the `/etc/init.d/cmascsi` file is linked to the `/opt/compaq/storage/etc/cmascsi` file. The `/var/spool/compaq/agenterrs.log` file might contain additional information. You must be logged in as `root` to access this file.

SMUX Manager Will Not Run

Check the `/var/spool/compaq/agenterrs.log` file. If you find the message `youLoseBig` or `inProgress`, be sure that the SNMP daemon can be restarted.

To restart the SNMP daemon, enter `sh /etc/init.d/snmp stop` and `sh /etc/init.d/snmp start`. You should see the message `SNMP successfully started`. Then enter the following to start the SMUX Manager:

```
sh /etc/init.d/cmafdtnsmux start
sh /etc/init.d/cmasvrsmux start
sh /etc/init.d/cmastorsmux start
sh /etc/init.d/cmanicsmux start
```

Web-Enabled Management Agents for Servers

The SCO UnixWare 7 software has been tested with the following browsers:

- Microsoft Internet Explorer 6.0, Netscape Communicator 6.0 on Windows NT 4.0 and Windows 2000
- Netscape Communicator 4.61 on SCO UnixWare 7.1.1 and SCO UnixWare 7.1.3

The minimum browser requirements must be met for the Web-Enabled Management Agents for Servers to work correctly.

Depending on how they were implemented, some browsers might not work correctly when used with different operating systems.

Error Messages

This topic lists the various error messages the SMUX Manager SCO UnixWare 7 support software can produce and provides information about how each problem can be resolved.

These messages can appear in two places:

- At the Console—Messages from the installation and configuration utilities generally appear at the console or at the terminal from which they are run.
- In the Agent/Standard error log file—Messages from the monitoring agents are written to this log file. Syntax errors found in the SMUX Manager configuration files and trap alarm e-mail configuration file are also reported here. The name of this file is `/var/spool/compaq/agenterrs.log`.

Most error messages have a message code appended at the end. Message codes have the form AAAADDDD, where AAAA represents letters and DDDD represents digits. All the “SMUXDDDD” messages contain the identification, for example, `cmafdtnsmuxd`, `cmasvrsmuxd`, `cmastorsmuxd`, or `cmanicsmuxd`, of the SMUX Manager. The messages are listed in the order of the message code, so you can easily find them in this topic regardless of where the message appears.

SNMP Error Messages

```
snmpd: authentication failure from: ip_address
```

The SNMP daemon has detected an attempt to access data from an IP address that is not listed in its SNMP community names file `/etc/netmgt/snmpd.comm`. Add a community name with the correct IP address to the community names file. Stop and then restart the SNMP daemon. Restart the SMUX Manager.

```
smux: couldn't bind to the requested address. Error starting the  
TCP server: Bad file number
```

The SNMP software encountered an error while initializing. Wait a few minutes and try to restart the SNMP daemon. Restart the SMUX Manager software.

Miscellaneous Error Messages

Table A-1: Miscellaneous Error Messages

Message	Description
SMUX3000 agent: Error on sigaction call, error code (SMUX3000)	The specified agent is not able to set its signal handler using the <code>sigaction</code> system call. Stop and restart the SMUX Manager software. If the problem reoccurs, disable the agent, then stop and restart the SMUX Manager software.
SMUX3001 agent: Insufficient parameters (SMUX3001)	A data collection agent was started with an invalid number of command line arguments. Refer to the command line argument documentation for the appropriate agent. Correct the arguments and then manually restart the agent software.
SMUX3002 agent: Invalid polling rate (SMUX3002)	A data collection agent was started with an invalid data poll time. Refer to the command line argument documentation for the appropriate agent pertaining to poll time. Adjust the poll time and then manually restart the agent software.
SMUX3005 agent: Bad type argument: name (SMUX3005)	The specified agent encountered an error of type name while processing its command line arguments. Supply the correct command line argument. Restart the specified agent.
SMUX3006 agent: Unknown mail command: opcode (SMUX3006)	An internal error condition has been detected. Stop and then restart the SMUX Manager software.
SMUX3008 agent: Status reply failed command, device name (SMUX3008)	The agent software cannot execute the given command on the named device. Verify that the device exists and has correct file permissions. Stop and then restart the SMUX Manager software.
SMUX3009 agent: Can't init signal: reason (SMUX3009)	The agent software cannot initialize a signal. Stop and then restart the SMUX Manager software.
SMUX3020 agent: Can't operation the file: name (SMUX3020)	The specified agent is not able to access the named file. Check that the file exists and has valid permissions. Stop and then restart the SMUX Manager software.
SMUX3021 Can't send SCO UnixWare 7 mail message: message (SMUX3021)	The message cannot be sent to SCO UnixWare 7 mail. Check the syntax of the SCO UnixWare 7 mail message line in the SMUX Configuration file. Verify that SCO UnixWare 7 mail is properly functioning. Stop and then restart the SMUX Manager software.

continued

Table A-1: Miscellaneous Error Messages *continued*

Message	Description
SMUX3022 agent: Unknown command line option: option (SMUX3022)	The specified agent cannot be started because of a bad command line argument. Supply the correct command line argument. Stop and then restart the SMUX Manager software.
SMUX3023 agent: Can't operation object: name (SMUX3023)	The specified agent cannot perform the operation on the named object file. Stop and then restart the SMUX Manager and the specified agent.
SMUX3030 agent: Can't get name list from kernel /unix (SMUX3030)	The specified agent is not able to read the name list from the kernel executable file. Check the permissions on the file /unix. Verify that /unix is the currently executing kernel. Stop and then restart the SMUX Manager software.
SMUX3031 agent: Can't open kernel memory device /dev/kmem (SMUX3031)	The specified agent is not able to open the kernel memory special device file. Check the permissions on the file /dev/kmem. Stop and then restart the SMUX Manager software.
SMUX3032 agent: Can't read kernel variable name, error code (SMUX3032)	The specified agent is not able to read a variable from kernel memory. Verify that /unix is the currently executing kernel. Stop and then restart the SMUX Manager software.
SMUX3033 module: Can't allocate memory for use (SMUX3033)	The software is not able to allocate memory. Try to correct the problem by restarting the SMUX Manager software. If the problem continues, tune the SCO UnixWare 7 kernel to increase the user process memory limit.
SMUX3034 agent: Can't operation the file /etc/mnttab, error code (SMUX3034)	The specified agent is not able to access the mount table file. Check that the file exists and has valid permissions. If the mount table file is missing or invalid, reboot the monitored server. Otherwise, stop and then restart the SMUX Manager software.
SMUX4000 cmaXXXsmuxd: smux_init: error (SMUX4000)	The SMUX Manager software encountered an error while initializing. Verify that the SNMP will run using the /etc/init.d/snmp start command. Stop and then restart the SMUX Manager software.
SMUX4001 cmaXXXsmuxd: smux_wait: error (SMUX4001)	The SMUX Manager software encountered an error while waiting for an SNMP packet. Verify that the SNMP daemon is running. Stop and then restart the SMUX Manager software.

continued

Table A-1: Miscellaneous Error Messages *continued*

Message	Description
SMUX4002 cmaXXXsmuxd: smux_register: error (SMUX4002)	The SMUX Manager software encountered an error while registering the MIB with the SNMP daemon. Stop and then restart the SMUX Manager software.
continuedSMUX4003 cmaXXXsmuxd: smux_trap: error (SMUX4003)	The SMUX Manager software encountered an error while sending a cold start trap to the SNMP daemon. Verify that valid trap destinations exist in the file /etc/netmgt/snmpd.trap. Stop and then restart the SMUX Manager software.
SMUX4004 cmaXXXsmuxd: smux_response: error (SMUX4004)	The SMUX Manager software encountered an error during a response from the SNMP daemon. Stop and then restart the SNMP daemon. Stop and then restart the SMUX Manager software.
SMUX4005 cmaXXXsmuxd: smux_simple_open: error (SMUX4005)	The SMUX Manager software encountered an error while opening the SMUX peer file /etc/netmgt/snmpd.peers. Verify that the peers file exists and has correct file permissions. Stop and then restart the SNMP daemon. Stop and then restart the SMUX Manager software.
SMUX4010 agent: Can't convert text to object: name (SMUX4010)	An internal error condition has been detected. Verify that the name exists in the MIB file /opt/compaq/xxx/etc/cmasmuxd.defs (xxx is one of foundation, server, storage, and NIC). Stop and then restart the SMUX Manager software.
SMUX4011 agent: SMUX registration of name failed (SMUX4011)	An internal error condition has been detected. Stop and then restart the SMUX Manager software.
SMUX4012 agent: unexpected operation: code (SMUX4012)	An internal error condition has been detected. Stop and then restart the SMUX Manager software.
SMUX4013 agent: bad operation: code (SMUX4013)	An internal error condition has been detected. Stop and then restart the SMUX Manager software.
SMUX4014 agent: Unknown command: code (SMUX4014)	An internal error condition has been detected. Stop and then restart the SMUX Manager software.

continued

Table A-1: Miscellaneous Error Messages *continued*

Message	Description
SMUX4015 agent: Syntax undefined for object: name (SMUX4015)	An internal error condition has been detected. Stop and then restart the SMUX Manager software.
SMUX4016 cmaXXXsmuxd: Can't find name in /etc/netmgt/snmpd.peers (SMUX4016)	The SMUX Manager software cannot find the SMUX peer name in the file /etc/netmgt/snmpd.peers. Verify that the peers file exists and has correct file permissions. Stop and then restart the SMUX Manager after verifying that the following lines appears in /etc/netmgt/snmpd.peers: "cmafdtnsmuxd" 1.3.6.1.4.1.232 "compaq_passwd" "cmasvrsmuxd" 1.3.6.1.4.1.232 "compaq_passwd" "cmastorsmuxd" 1.3.6.1.4.1.232 "compaq_passwd" "cmanicsmuxd" 1.3.6.1.4.1.232 "compaq_passwd"
SMUX4017 cmaXXXsmuxd: Can't find or interpret MIB file: filename (SMUX4017)	The SMUX Manager software cannot find the MIB file. Verify that the MIB file exists in /opt/compaq/xxx/etc/cmasmuxd.defs (xxx is one of foundation, server, storage, and NIC) and has correct file permissions. Stop and then restart the SMUX Manager software.
SM4020 parse: Can't interpret file: file (SMUX4020)	The SMUX Manager software is not able to open its configuration file. Verify that the file exists and has valid permissions. It might be necessary to recover the file from a backup copy. Stop and then restart the SMUX Manager software (refer to /opt/compaq/etc/config).
SMUX4022 cmaXXXsmuxd: Can't send snmp trap: error (SMUX4022)	The SMUX Manager software cannot send a trap to the SNMP. Be sure a valid IP address is defined in the file /etc/netmgt/snmpd.trap. Stop and then restart the SMUX Manager software.

continued

Table A-1: Miscellaneous Error Messages *continued*

Message	Description
SMUX4023 cmaXXXsmuxd: Can't find executable to fork: agent (SMUX4023)	The stat system call failed on the specified agent-executable file agent. Verify that the agent-executable file exists and that it has correct file permission settings. If this does not correct the problem, disable the agent by commenting out the agent entry in the SMUX Manager configuration file. Stop and then restart the SMUX Manager software.
SMUX4024 cmaXXXsmuxd: Can't exec agent: agent (SMUX4024)	The exec system call failed on the specified agent-executable file agent. Verify that the agent-executable file exists and that it has correct file permission settings. If this does not correct the problem, disable the agent by commenting out the agent entry in the SMUX Manager configuration file. Stop and then restart the SMUX Manager software.
SMUX4025 cmaXXXsmuxd: Can't fork agent agent (SMUX4025)	The SMUX Manager software cannot create a process to run the agent. Tune the SCO UnixWare 7 kernel to increase the maximum number of processes. If this does not correct the problem, disable the agent by commenting out the agent entry in the SMUX Manager configuration file. Stop and then restart the SMUX Manager software.
SMUX4026 parse: file, line number: description (SMUX4026)	The SMUX Manager software found a syntax error in the configuration file. Correct the error. Stop and then restart the SMUX Manager software.
SMUX4027 cmaXXXhostd: Cannot open SNMP API connection (SMUX4027)	The cmahostd could not open an SNMP connection to localhost. Localhost might not be configured to perform SNMP operations. Check the /etc/netmgt/snmpd.comm file and correct.
CPQ6001 cmanicd: Couldn't get interface list from /etc/strcf. (CPQ6001)	The Network Interface Controller data collection agent failed to access the SCO UnixWare 7 Streams configuration file containing the list of interfaces to monitor. Check that the /etc/strcf file exists and is readable.
CPQ6002 cmanicd: Couldn't get object ifmap.1-n. (CPQ6002)	The Network Interface Controller data collection agent failed to access an instance of the Host OS MIB Interface Physical Map object. Stop and then restart the agent and the SMUX Manager.
CPQ6003 cmanicd: Unknown interface type x. (CPQ6003)	The Network Interface Controller data collection agent received an interface type other than Ethernet or token ring from one of the monitored interfaces.

continued

Table A-1: Miscellaneous Error Messages *continued*

Message	Description
CPQ6005 cmanicd: do_init failure following find_obj failure: object.1-n. (CPQ6005).	The Network Interface Controller data collection agent failed to access a database object. Restart the agent.
CPQ6006 cmanicd: mcat function failed. (CPQ6006)	The Network Interface Controller data collection agent failed to collect multicast address information from one of the monitored interfaces. Replace the device driver for this interface with one that supports all of the required LLI facilities.
CPQ6007 cmanicd: malloc function failed. (CPQ6007)	The NIC data collection agent failed to acquire memory for an interface multicast address information. Since this implies a system-wide memory shortage, correct the memory shortage problem and restart the system.
cmaidad: RET_DRV_THRESHOLD failed, device = name, slot = number	The drives in this controller have not been factory-stamped. You should run the Diagnostics Utility to stamp the drives.

Problem Using Disk Imaging Software

Global Unique Identifiers Are the Same for All Devices When Using Disk Imaging Software on Servers

Solution 1

If the disk image has not been taken, perform the following after installing the Management Agents on the source machine and capture the image before restarting the Management Agents.

1. Uninstall all Management Agents from one of the devices.
2. Use the Disk Imaging software to copy the configuration from the device without the Management Agents installed.
3. Use the disk image to copy to the target devices.
4. Reinstall the Management Agents on all the devices.

Solution 2

If the disk image has already been deployed, perform the following to remove the image from each target device.

1. The Globally Unique Identifier information is stored in a 16-byte file on the SYS:\SYSTEM subdirectory of the NetWare server. This file is created and populated with the Globally Unique Identifier when HP Systems Insight Manager performs an SNMP SET command to the NetWare server.
2. To remove the permanence of the Globally Unique Identifier, delete the file \SYSTEM\CPQBSSA.CFG, in the NetWare SYS volume.
3. After the file is deleted, restart the Management Agents. HP Systems Insight Manager assigns a new Globally Unique Identifier when the system is discovered.

Glossary

Automatic Server Recovery (ASR)

A server feature designed to automatically restart your server after a critical hardware or software error. If a critical error occurs, the server records the error in the Server Health Logs, reboots the system, and pages you (if you have installed a modem at the server).

Client

A computer connected to a server on the network.

Community String

The SNMP Community String is similar to a password, offering a limited amount of protection for the SNMP data.

HP Management Agents for Servers

Software that can query a manageable server and provide information that responds to SNMP requests for data.

HP Utilities

HP Utilities have the capability to set up or modify your system and include various diagnostic programs.

Corrected Memory Log

This log contains a list of corrected memory errors.

Desktop Management

A feature of HP Systems Insight Manager that allows you to monitor HP PCs being used as clients.

In-band

Refers to the capacity to deliver information through existing network hardware. Synonymous with “on the network.”

Logical Drive

Multiple physical drives connected in a HP Drive Array to the same controller and combined to create logical drives. All available physical drive capacity is used by the logical drive as if it were a larger drive subsystem. By combining several physical drives, special fault tolerance and performance features can be used.

Managed Device

A device managed by a management console. Devices include servers, clients, routers, switches, and hubs. Servers and clients cannot be managed devices unless they have HP Management Agents installed.

Management Information Base (MIB)

The document or file that defines all manageable traps known to the management agent and management application.

Management Console

The PC, workstation, or server that is running HP Systems Insight Manager.

Monitored Item

The item that HP Insight Manager manages or monitors, or the information that HP System Insight Manager collects.

NetWare Peripheral Architecture (NWP)

The goal of the NetWare Peripheral Architecture (NWP) is to provide NetWare Version 4.x, and IntranetWare customers with broader and more reliable driver support for host adapters and storage devices.

NetWare Loadable Module (NLM)

Used to refer to executables which run under the Novell NetWare operating system.

Network Interface Controller (NIC)

An adapter card installed in a PC, workstation, or server that allows the PC or workstation to communicate with other devices connected to the same network. This term usually implies a local area network (LAN) adapter card.

Out of Band

Referring to the capacity to deliver information by modem. Synonymous with “off the network.”

Physical Drive

Multiple physical drives connected in a HP Array Controller to the same controller and combined to create logical drives. The logical drives use all of the available physical drive capacity as if it were a larger drive subsystem. By combining several physical drives, you can use special fault tolerance and performance features.

Point-to-Point Protocol (PPP)

A standard defined by the Internet Engineering Task Force. PPP provides a standard method for transporting multiple protocols over a point-to-point link.

ProLiant Extended Feature Supplement (EFS) for UnixWare 7

A collection of device drivers to provide maximum performance with HP ProLiant hardware and SCO/Caldera software. It also includes several utilities to monitor and increase the performance of HP ProLiant servers.

Simple Network Management Protocol (SNMP)

SNMP defines a set of commands that a management application uses to retrieve or change the values of items a management agent makes available.

SNMP Multiplexing (SMUX)

The protocol defining a mechanism for communication between SNMP agent and multiple user daemons (called SMUX peers). The SMUX protocol has the advantage of being vendor-independent. With SMUX, a single SNMP agent can be used to control and monitor devices from different vendors, regardless of how each vendor has implemented SMUX peers in their own products.

Threshold

A preset limit that produces an alarm when reached or exceeded.

Trap

An indicator of a change or an error condition. *Also called* alarm.

Uninterruptible Power Supply (UPS)

A battery that supplies continuous power to a computer system in the event of a power failure.

Windows Management Instrumentation (WMI)

Windows 2000 and Windows 98 extensions to WDM which provide an interface between the operating system and instrumented components, allowing the instrumented components to provide information and notifications.

A

- accounts, user 1-5
- Adapter Information Page 6-8
- array controllers 7-1
- ASR POST failure A-10
- asset information 3-11
- Automatic Server Recovery (ASR) 3-13
- auxiliary input 3-7

B

- batteries 2-18
- boot procedures 3-20
- browser A-3

C

- Client data collection 2-2
- clusters
 - Foundation Agents 2-4
 - RAID Array controller 7-4
- colors in browser A-4
- community strings, SNMP A-5, A-12
- community strings, SNMP A-7
- Compaq CR3500 RAID Array SCSI Controller
 - clustered controller 7-4
 - entire array information 7-1
 - environment monitoring unit 7-5
 - external expansion cabinet 7-6
 - physical drive 7-3
- Compaq Foundation Agents
 - configuration subsystem 2-4
 - mass storage subsystem 2-7
 - NIC subsystem 2-9
- Compaq NIC Agents
 - controller 5-3
 - ethernet statistics 5-6
 - interface 5-5
 - logical adapter 5-2
 - token ring statistics 5-10
 - types of configurations 5-1
- configuration 2-2
- configuration subsystem 3-10

- Connection Page 6-5
- console, Remote Insight Agent commands 2-18
- controllers, RAID Array 7-1, 7-4
- correctable memory, Server Agents 3-23
- CPQAGIN.NLM 2-17
- CPQBSSA.NLM 2-17
- CPQHTHSA.NLM 2-18
- CPQMGMGT.CPL A-6
- CPQRISA.NLM 2-18
- CPQWEBAG.NLM 2-17
- CR3500 RAID Array SCSI Controller
 - controller 7-4
 - entire array information 7-1
 - environment monitoring unit 7-5
 - external expansion cabinet 7-6
 - physical drive 7-3
- critical errors, Server Agents 3-20

D

- Data Frame 1-31
- Device Status 1-30
- devices, not manageable message A-7
- disk space, Foundation Agents 2-7
- disk storage, button problems A-8, A-9
- disk subsystem buttons, missing A-9
- diskette drives, Server Agents 3-7, 3-12
- Drive Array, troubleshooting A-8
- drives
 - diskette 3-7, 3-12
 - RAID Array 7-1
 - spare 7-2

E

- EISA bus 3-12
- environment monitoring unit 7-5
- environment, Server Agents 3-15
- errors, critical, Server Agents 3-20
- ethernet statistics, NIC Agents 5-6
- Event Viewer application A-6
- expansion boards, Server Agents 3-8
- external expansion cabinet 7-6

F

File System Page 6-3
file systems, space used 2-7
floppy drives, Server Agents 3-7, 3-12
Foundation Agents
 configuration subsystem 2-4
 mass storage subsystem 2-7
 NIC subsystem 2-9

H

health, server 2-18
help resources xii
HP 32-Bit SCSI-2 Controller A-6
HP authorized reseller xii
HP Insight Base System Agent 2-17
HP Insight Manager troubleshooting A-6, A-7
HP Management Agents for Servers
 troubleshooting A-6
HP Server Agent Installation and Configuration
 utility 2-17
HP Server Agents 2-17
HP Server Health Agent 2-18

I

I/O devices, Server Agents 3-6
icons, device A-7
icons, device status 1-30
IML page A-4
Insight Base System Agent 2-17
installation
 Server Agent Installation and Configuration
 utility 2-17
 troubleshooting A-6
integrated management log, Server Agents 3-23
Integrated Remote Console (IRC) 3-18
interconnect, cluster 2-6
IRC (Integrated Remote Console) 3-18

K

keyboards 3-6

L

Loaded NLMs Page 6-6
logical adapter, NIC Agents 5-2
logical drives 7-2
login 2-2
logs, integrated management
 critical errors 3-20
 Server Agents 3-23

M

Management Agents for Servers
 troubleshooting A-6
Management HTTP Server 1-8
marking of errors as corrected A-12
memory, Server Agents 3-2, 3-5, 3-23
Microsoft Internet Explorer, issues A-4
Microsoft Windows NT
 browser requirements A-3
 community string settings A-5

N

Navigation Frame 1-31
Netscape Communicator, issues A-4
NetWare
 browser requirements A-3
 community string settings A-5
 Remote Insight Agent commands 2-18
network communications, checking A-7
network information, clustered systems 2-5
network interface controller (NIC),
 troubleshooting A-7
NIC (Network Interface Controller) Agents
 controller 5-3
 ethernet statistics 5-6
 interface 5-5
 logical adapter 5-2
 token ring statistics 5-10
 types of configurations 5-1
NIC subsystem, Foundation Agents 2-9
NLMs (NetWare Loaded Modules) 6-6
no Frames version 1-30
nodes, cluster 2-4
Novell NetWare
 community string settings A-5
 Remote Insight Agent commands 2-18

O

Open Files 6-4
operating systems
 NetWare browser requirements A-3
 NetWare community string settings A-5
 Novell NetWare 2-18
 Windows 2000 A-6
 Windows NT browser requirements A-3
 Windows NT community string settings A-5

P

pager information, ASR 3-15
parallel ports, Server Agents 3-8
parameters, NetWare 6-6
partitions, physical, NetWare 6-8
passwords 1-5

PCI adapter, ServerNet 2-9
 PCI bus 3-12
 physical drives 7-3
 Physical Partition Page 6-8
 port/socket numbers, URL 1-1
 power components
 converter 3-17
 power supply 3-16
 power on messages 3-23
 PPP connection 2-18
 processors
 Server Agents 3-2
 utilization information 3-12
 Proliant storage system, missing information A-10

R

RAID array controllers
 controller 7-4
 entire array information 7-1
 environment monitoring unit 7-5
 external expansion cabinet 7-6
 physical drive 7-3
 Rapid Recovery 3-18
 reboot
 ASR 3-14
 recovery subsystem 3-20
 reboot problems A-1
 recovery subsystem, Server Agents 3-20
 remote communications
 Compaq Utilities 3-18
 Server Agents 3-18
 Remote Insight Agent 2-18
 Remote Insight Lights-Out Edition 3-25
 remote reboot problems A-1
 resetting server 3-14
 resource groups, cluster 2-5
 restart problems A-1
 ROM microcode patches 3-6

S

SCO UnixWare, browser requirements A-4
 SCSI adapter button, disabled A-8
 SCSI controller 7-1
 SCSI Information Agent A-6
 security
 NetWare 6-1
 Server Agents 3-9
 setting browser A-4
 thresholds A-9
 security 1-5
 serial ports, Server Agents 3-8
 Server Agents 2-17
 configuration subsystem 3-10
 mass storage subsystem 3-12

Server Health Agent 2-18
 Server Parameter Page 6-6
 ServerNet PCI adapter 2-9
 servers
 health monitoring 2-18
 Web-enabled monitoring of 2-17
 servers, designated See also HP Management Agents
 for Servers
 SET exceptions 6-7
 shared storage system, RAID Array 7-5
 Simple Network Management Protocol (SNMP),
 community strings A-5
 single NIC 5-1
 SNMP (Simple Network Management Protocol)
 address problems A-9
 community strings A-7
 troubleshooting traps A-12
 SNMP (Simple Network Management Protocol),
 community strings A-5
 software, cluster 2-6
 spare drives
 RAID Array 7-2
 subsystem button, disabled A-8
 Summary Page 6-1
 system board, Server Agents 3-1
 System Management Homepage 1-7
 system resources, Server Agents 3-12
 system restart problems A-12

T

tape device errors A-11
 team of NICs 5-2
 telephone numbers xii
 thresholds
 Foundation Agents 2-7
 SNMP A-9
 timeout, ASR 3-14
 Title Frame 1-29
 token ring statistics 5-10
 trap messages
 troubleshooting A-12
 troubleshooting
 Web-enabled Management Agents A-3
 troubleshooting A-6

U

universal serial bus port 3-8
 user accounts 1-5
 User Information Page 6-4
 utilization subsystem, Server Agents 3-12

V

values, inability to change A-12
version information
 ASR 3-14
virtual NIC 5-1

W

WEBAGENT.INI 1-5
Web-enabled Management Agents
 troubleshooting A-11
Web-enabled Management Agents for Servers

 accessing 1-1
 troubleshooting A-3
Web-enabled Server Agent 2-17
websites
 accessing Server Agent 1-1
Windows 2000
 troubleshooting issues A-6
Windows NT
 browser requirements A-3
 community string settings A-5