Managing ProLiant servers with Linux

HOWTO

Abstract

This HOWTO provides instructions to help system administrators install, upgrade, and remove Version 7.5.0 (or later) of the following HP Linux management software:

- HP System Health Application and Insight Management Agents (hpasm)
- HP OpenIPMI Device Driver (hp-OpenIPMI)
- HP Lights-Out Drivers and Agents (hprsm)
- HP NIC Agents (cmanic)
- The HP System Management Homepage (hpsmh)

This HOWTO also includes prerequisites for using this software with and without errata kernels, contains usage information for the above-mentioned products, and provides reference links to installation instructions for HP Systems Insight Manager and HP ProLiant Essentials Rapid Deployment Pack.

The HP ProLiant Support Pack (PSP) is a set of bundled software components for maintaining and deploying software on HP ProLiant servers and is available for download from www.hp.com/servers/swdrivers. For installing the complete set of Linux software drivers and management agents, refer to the appropriate PSP for Linux.

1 Software architecture

This section describes the features and architecture of the following systems:

- HP System Health Application and HP ProLiant Insight Management Agents (hpasm)
- HP Lights-Out Drivers and Agents (hprsm)
- HP NIC Agents (cmanic)
- HP System Management Homepage (hpsmh)

Descriptions for HP management consoles for Linux are also described.

1-1 System Health Application and Insight Management Agents (hpasm)

The System Health Application and Insight Management Agents (hpasm) package collects and monitors important operational data on ProLiant servers. Contained within the hpasm package are the following components:

- Health Monitor
- Integrated Management Log (IML) Viewer Application (cpqimlview)
- HP Integrated Management Logging (IML) utility (hplog)
- HP Unique Identifier utility (hpuid)
- Insight Management Agents

ProLiant servers are equipped with hardware sensors and firmware to monitor certain abnormal conditions, such as abnormal temperature readings, fan failures, error correction coding (ECC) memory errors, etc. The Health Monitor monitors these conditions and reports them to the administrator by printing messages on the console (preserved in /var/log/messages). Health Monitor also logs the condition to the ProLiant Integrated Management Log (IML). The IML is dedicated, Non-Volatile RAM (NVRAM) that can be viewed and maintained by the cpqimlview or hplog application.

The ProLiant Insight Management Agents are included to provide proactive notification of server events through the HP Systems Insight Manager console. Alternatively, the ProLiant Insight Management Agents allow the status of the server to be monitored or checked using a standard Web browser. Insight Management Agents include the following:

- Foundation agent (consists of Server Peer Agent, Host OS Agent, and Threshold Agent)
- Server agent (consists of Standard Equipment Agent, System Health Agent, and Performance Agent)
- Storage agent (consists of IDA, IDE, SCSI, and FCA Agents, and Event Agent)

ProLiant servers contain an Integrated Lights-Out (iLO) controller that, with optional software, allows secure remote management of the server including IML management and graphical remote console.

Servers without the embedded iLO controller can be configured with an optional Remote Insight Lights-Out Edition II (RILOE II) adapter. The System Health Application and Insight Management Agents (hpasm) package works with the Lights-Out Drivers and Agents (hprsm) package to provide secure remote management of the server including IML management and graphical remote console.

Hpasm Version 7.5.1 includes three binary modules (listed in Table 1). These modules are automatically selected depending on the HP ProLiant Advanced System Management hardware available.

Note:
To determine the type of HP ProLiant Advanced System Management hardware installed, check the ProLiant server specifications located on www.hp.com.

Table 1. hpasm Version 7.5.1 binary modules

Binary module		Details
hpasmd		
	Location	/opt/compaq/hpasmd/bin/hpasmd
	Description	The hpasmd application will automatically load on ProLiant servers that have either the ASM or the legacy iLO hardware.
hpasmxld*		
	Location	/opt/compaq/hpasmd/bin/hpasmxld
	Description	The "hpasmxld" application will automatically load on ProLiant servers that have the HP Integrated Lights-Out 2 (iLO 2) management controller and the "hp-OpenIPMI" package is installed. The iLO 2 management controller contains an Intelligent Platform Interface (IPMI) Version 2.0 Base Management Controller (BMC) that replaces the operating system-based software management functionality provided by the legacy "hpasmd" application. The "hpasmxld" application is also dependent on the "hp-OpenIPMI" package. The "hp-OpenIPMI" package is a "GNU GENERAL PUBLIC LICENSE" (GPL) high performance enhancement of the IPMI device drivers that ship with standard Linux distributions. The hpasmxld package will be automatically selected by the hpasm initialization scripts (/etc/init.d/hpasm, /opt/compaq/hpasmd/etc/hpasmd) if the hp-OpenIPMI package is installed and the iLO 2 management controller is present.
		The corresponding hp-OpenIPMI package for ProLiant servers is available for download at http://h20000.www2.hp.com/bizsupport/TechSupport/Product.jsp?lang=en&cc=us&taskId=135&prodTypeId=15351&prodCatId=241435.

Binary module	Details
hpasmlited*	
Location	/opt/compaq/hpasmd/bin/hpasmlited
Description	The "hpasmlited" application will automatically load on HP ProLiant servers with the iLO 2 management controller and and the "hp-OpenIPMI" package NOT installed. The hpasmlited application is designed to work with the standard IPMI device drivers that ship with the Linux distributions. The IPMI device drivers that ship with the Linux distributions are not as efficient as the "hp-OpenIPMI" drivers due to the constant polling method used for detecting system management events. The "hpasmlited" application has the ability to log raw IPMI messages (as does the hp-OpenIPMI package) to the /var/log/messages file to assist with debugging IPMI BMC integration issues.

* The "hpasmxld" application is more efficient than the "hpasmlited" application as a result of leveraging the high performance hp-OpenIPMI package, which includes support for IPMI 2.0 OEM message channels and messages.

Another source of information includes the following man pages provided with the hpasm package:

- hpasm
- cpqimlview
- hpuid
- hplog

These man pages include detailed information on error messages and possible action that the administrator may take.

Additional information about Insight Management Agents is available at the following locations:

- www.hp.com/servers/manage
- http://h18000.www1.hp.com/products/servers/management/agents.html

1-1-1 Health Monitor

The Health Monitor augments the hardware features built into ProLiant servers. Basic features, such as temperature, fan, power supply, and memory monitoring are standard on almost all ProLiant servers. On some ProLiant servers, the Health Monitor supports features such as variable speed fans, server lights that give a visual indication of a possible error condition, and Advanced Memory Protection (AMP). The AMP feature allows the capability of reserving memory for fail over if a Single Bit Correctable Error (SBCE) threshold is exceeded.

Note:
On some ProLiant servers, the entire memory subsystem can be mirrored to survive an uncorrectable memory error. Without AMP, uncorrectable memory errors are always fatal and cause a kernel panic. AMP allows a server to continue execution until the faulty memory can be replaced. Mirrored AMP solutions usually allow removing the memory board with the faulty memory dual in-line memory module (DIMM) and replacing the faulty DIMM while the server continues execution. When the repaired AMP memory board is inserted back into the server, the AMP mirror will automatically be restored. This allows mission critical 7 X 24 applications to continue execution without interruption or downtime.

The following sections explain the features provided by the Health Monitor for the overall health of the ProLiant server.

1-1-1-1 System temperature monitoring

A ProLiant server may contain several temperature sensors. On ProLiant servers with intelligent temperature sensors, check the current and threshold temperatures by running hplog -t.

If the normal operating range is exceeded for any of these sensors, the Health Monitor does the following:

- Displays a message to the console stating the problem.
- Makes an entry in the system health log and the operating system log.

Additionally, on some servers, the fans will gradually increase to full speed in an attempt to cool the server as the external environment temperature increases. If the server exceeds the normal operating range and does not cool down within 60 seconds, the operating system will, in most cases, be shutdown to close the file systems.

Tip:
On servers that do not have variable speed fans, the server will be shutdown unless the ROM-Based Setup Utility (RBSU) Thermal Shutdown feature is disabled (this feature is enabled by default). Use RBSU to control the shutdown option.

1-1-1-2 System fan monitoring

A ProLiant server may contain fan sensors. On ProLiant servers with intelligent fan sensors, check the status of the fans by running hplog -f.

If a cooling fan fails and there is no secondary redundant fan, the Health Monitor does the following:

- Displays a message to the console stating the problem.
- Makes an entry in the system health log and the operating system log.
- Shuts the system down (optionally) to avoid hardware damage.

Use RBSU to control the shutdown option.

If a secondary or redundant fan is present when a fan fails, the Health Monitor does the following:

- Activates the redundant fan if not already running.
- Displays a message on the console.
- Makes an entry in the system health log and the operating system log.

1-1-1-3 Monitoring the system fault tolerant power supply

If the server contains a redundant power supply, the power load is shared equally between the power supplies. Check the status of the power supplies by running hplog -p. If a primary power supply fails, the server automatically switches over to a backup power supply. The Health Monitor does the following:

- Monitors the system for power failure and for physical presence of power supplies.
- Reports when the power supplies experience a change in shared power load.
- Displays a message to the console stating the problem.
- Makes an entry in the system health log and the operating system log.

1-1-1-4 ECC memory monitoring and advanced memory protection

If a correctable ECC memory error occurs, the Health Monitor logs the error in the health log, including the memory address causing the error. If too many errors occur at the same memory location, the driver disables the ECC error interrupts to prevent flooding the console with warnings (the hardware automatically corrects the ECC error).

On servers with AMP, the driver will attempt to log an error if a memory board has been inserted, removed, or incorrectly configured, and optionally if an Online Spare Switchover or Mirrored Memory engaged event occurs.

The Health Monitor does the following:

- Displays a message on the console stating the problem
- Makes an entry in the system health log

This server feature is configured using RBSU. On ProLiant servers that do not support AMP mirroring, an uncorrectable (double bit) memory error will cause the operating system to halt abruptly. Logging of the error may not be possible if the error occurs in memory used by the Health Monitor.

1-1-1-5 Automatic server recovery

Automatic Server Recovery (ASR) is configured using RBSU available during the initial boot of the server by pressing the F9 key when prompted. This feature is implemented using a "heartbeat" timer that continually counts down. The Health Monitor frequently reloads the counter to prevent it from counting down to zero. If the ASR counts down to zero, it is assumed that the operating system has locked up and the system will automatically attempt to reboot. Events that may contribute to the operating system locking up include:

- A peripheral device, such as a Peripheral Component Interconnect Specification (PCI) adapter, that generates numerous spurious interrupts when it fails.
- A high priority software application consumes all the available central processing unit (CPU) cycles and does not allow the operating system scheduler to run the ASR timer reset process.
- A software or kernel application consumes all available memory, including the virtual memory space (for example, swap). This may cause the operating system scheduler to cease functioning.
- A critical operating system component, such as a file system, fails and causes the operating system scheduler to cease functioning.
- Any other event besides an ASR timeout that causes a Non-Maskable Interrupt (NMI) to be generated.

The ASR feature is a hardware-based timer. If a true hardware failure occurs, the Health Monitor might not be called, but the server will be reset as if the power switch were pressed. The ProLiant ROM code may log an event to the IML when the server reboots.

The Health Monitor is notified of ASR timeout through a NMI. If possible, the driver will attempt to perform the following actions:

- Displays a message on the console stating the problem
- Makes an entry in the IML
- Attempts to gracefully shut down the operating system to close the file systems

There is no guarantee that the operating system will gracefully shutdown. This shutdown depends on the type of error condition (software or hardware) and its severity. The Health Monitor logs a series of messages when an ASR event occurs. The presence or absence of these messages can provide some insight into the reason for the ASR event. The order of the messages is important, since the ASR event is always a symptom of another error condition.

1-1-2 Console messages

When events occur outside of normal operations, the Health Monitor may display a console message or log a message to the IML. Operational messages, such as fan failures or temperature violations, are logged to the standard /var/log/messages file. Messages specific to device drivers (such as NMI type messages) can be viewed using dmesg, if the system is not completely locked up.

The hpasm man page documents how to interpret the messages produced by the Health Monitor.

1-1-3 HP Integrated Management Log Viewers (cpqimlview)

The information in the IML may be viewed through the IML Viewer application, which resides in the RPM file. The IML records system events, critical errors, power-on messages, memory errors, and any catastrophic hardware or software errors that typically cause a system to fail. The IML Viewer allows the manipulation of this data.

The IML Viewer is an application that runs in both an X Windows and text (terminal) environment. Type the following to run the IML Viewer:

```
cpqimlview
```

The IML Viewer automatically displays the current entries in the IML. The graphical X Windows version is shown in Figure 1.

Figure 1. IML Viewer entries
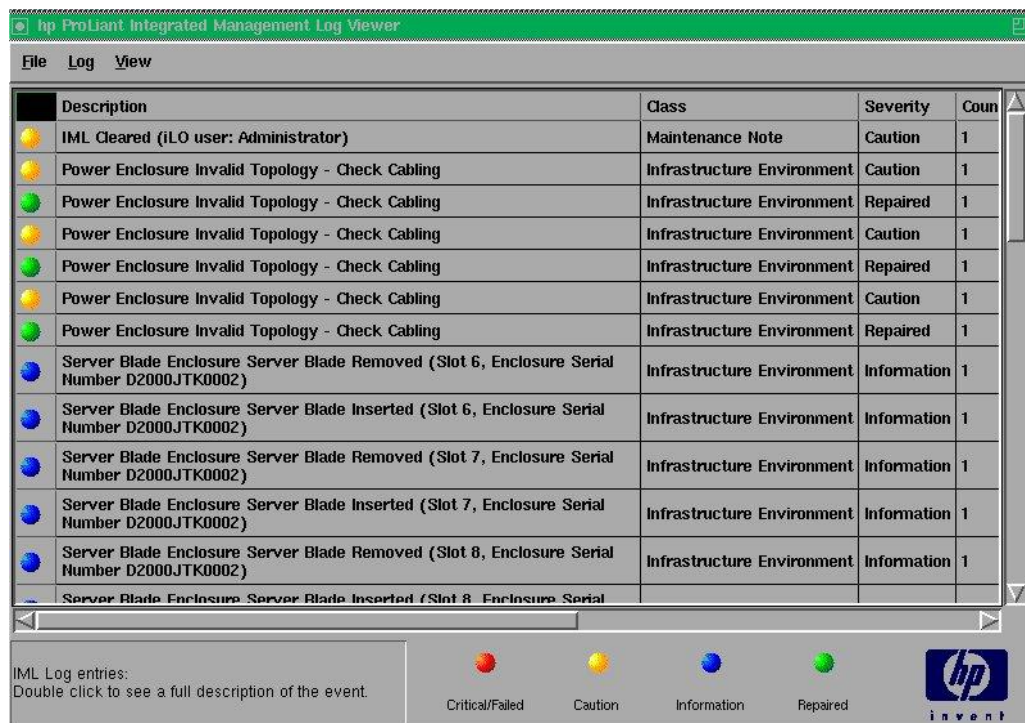
Each event in the IML Viewer has one of the following statuses to identify the severity of the event:

- Information—presents general information about a system event.
- Repaired—indicates that this entry has been repaired.
- Caution—indicates that a non-fatal error condition has occurred.
- Critical/Failed—indicates that a component of the system has failed.

The severity of the event and other information in the IML Viewer helps to quickly identify and correct problems, thus minimizing downtime. The IML Viewer allows several capabilities to enhance the ability to identify, correct, and document server health.

Table 2 describes the menu options available.

Table 2. IML Viewer menu options

Menu	Menu Option	Description
File menu	Option	Open a previously saved file and display the contents in the IML Viewer.
	Save As	Save the current entries of the IML to a file. This operation does not affect the current contents of the IML. It allows archival of IML data for input into a text editor, spreadsheet application, or IML Viewer for use when working with HP to diagnose issues. The File Name entry should specify the full path for the desired file name. If no path is specified, the file will be saved in the current directory.
	Exit	Close the IML Viewer window and exit the application.
Log menu	Clear All Entries	Clear the IML. HP recommends saving the current contents into a file before emptying the log.
	Mark As Repaired	Mark a specific entry as repaired.
	Add Maintenance Note	Mark a specific entry with maintenance information.
View menu	Filter	Filter IML events to display only desired event types. Event types such as Class, Status, Update Time, and Initial Time can be used to filter IML events.
	Refresh Now	Re-read and re-display entire current IML.
	Sort Events	Sort IML events by event types; for example, sort by Description, Class, Status, Count Initial Time, Update Time, or ID.

1-1-4 HP Integrated Management Logging Utility (hplog)

The hp ProLiant Integrated Management Logging utility (hplog) allows system administrators to view IML pages. Commands are listed in Table 3.

Table 3. /proc descriptions

Command	Description
hplog –t	Shows the current temperature and the threshold levels of all temperature sensors.
hplog –f	Shows the status of all fans.
hplog –p	Shows the status of all power supplies.
hplog –t	Shows the current temperature and the threshold levels of all temperature sensors.

1-1-5 HP Unique Identifier Utility (hpuid)

The hp Unique Identifier utility (hpuid) allows local manipulation of the ProLiant Unique IDentifier (UID) blue light on selected ProLiant servers. The hpuid utility allows the light to be turned on and off and will display the current status of the light (Table 4).

Table 4. /proc descriptions

Command	Description
hpuid –d	Disable the UID (Blue) Light
hpuid –e	Enable the UID (Blue) Light
hpuid –s	Status of the UID (Blue) Light

1-1-6 Insight Management Agents

The hpasm package contains the following Insight Management Agents: Foundation agent, Server agent, Storage agent, and Data Collection Agents.

<u>1-1-6-1 Foundation Agent</u>

A Foundation agent consists of the sub-agent components listed in Table 5.

Table 5. Sub-agents of the Foundation Agent

Sub-agent	Description
Server Peer Agent	The Peer Agent extends the SNMP "enterprise" Management Information Base (MIB) to include HP specific data, specifically enterprise ID 232. The Peer Agent supports SNMP get, set, and trap operations on MIB branches under "enterprises.232." At SNMP agent startup, cmaX reads MIB information files referenced in the master file opt/compaq/cmaobjects.conf. These referenced MIB information files are either /opt/compaq/server/etc/cmasvrobjects.conf and /opt/compaq/foundation/etc/cmafdtnobjects.conf (on older versions of hpasm) -Or- /opt/compaq/foundation/etc/cmaobjects.mibver (on newer versions of hpasm). During installation, the Peer Agents are configured to start automatically when the SNMP agent is running and should be started after the SNMP agent snmpd is started and should be killed after snmpd is killed.
Host OS Agent	The Host OS Agent gathers data for the Host OS MIB, including: - Server/host name and operating system version numberProcessor utilization information (for each processor) over 1-minute, 5-minute, 30-minute, and 60-minute intervals - Linux file system information (for each mounted file system) - Software version information The Host OS Agent executable is /opt/compaq/foundation/bin/cmahostd.

Sub-agent	Description
Threshold Agent	The Threshold Agent implements the Threshold MIB. Users can set thresholds on counter- or gauge-type MIB variables. The Threshold Agent periodically samples each selected MIB variable 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 to Linux email (configurable through trapemail entries in /opt/compaq/cma.conf file). User-configured alarm thresholds are permanently saved in the data registry until deleted by the user.
	The Threshold Agent executable is /opt/compaq/foundation/bin/cmathreshd.

For more information on threshold configurations, refer to the HP Systems Insight Manager Help file. This guide can be found on the Management CD or on the HP website at www.hp.com/go/hpsim.

1-1-6-2 Server Agent

A Server Agent consists of the sub-agent components listed in Table 6.

Table 6. Sub-agents of the Server Agent

Sub-agent	Description
Standard Equipment Agent (cmastdeqd)	The Standard Equipment Agent gathers data for the Standard Equipment MIB. The data includes:
	• PCI slot information
	• Processor and coprocessor information
	• Standard peripheral information (serial ports, diskette drives, and so on)
	The Standard Equipment Agent executable is /opt/compaq/server/etc/cmastdeqd.
System Health Agent (cmahealthd)	The System Health Agent gathers data for the Health MIB. The data collected include critical (NMI) errors, correctable memory (ECC) errors, system hang/panic detection, temperature conditions, and fan failures. The System Health Agent then retrieves these errors from the Health Monitor. The System Helath Agent executable is /opt/compaq/server/bin/cmahealthd.
Performance Agent (cmaperfd)	The Performance Monitor Agent provides statistics and allows 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.

1-1-6-3 Storage Agent

The Storage agent consists of IDA, IDE, SCSI, and FCA Sub-agents, and Event Agent components. The Storage agent collects information from the Fibre Channel, drive array, SCSI, and IDE subsystems at periodic intervals, makes the collected data available to the SNMP agent, and provides SNMP alerts.

Each Storage Data Collection Agent gathers and saves Storage MIB data to files in the 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.

The Storage data registry (/var/spool/compaq/hpasm/registry) is composed of standard Linux directories and associated files. Each file in the data registry is a logical object containing "n" related data items.

The -p poll_time command line argument, which can be used with the Storage Agents, specifies the number of seconds to wait between data collection intervals. The minimum allowed value is 1 second and the default value is 15 seconds.

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 may decrease system performance.

A Storage Agent consists of the sub-agent components listed in Table 7.

Table 7. Sub-agents of the Storage Agent

Sub-agent	Description
IDA Agent (cmaidad)	The IDA Agent gathers data for the IDA MIB. The data includes: • IDA controller information • IDA accelerator information • IDA logical drive information • IDA physical drive information The IDA Agent is located in /opt/compaq/storage/bin/cmaidad. The suggested poll_time is 15 seconds (default). The minimum poll_time is 5 seconds.
IDE Agent (cmaided)	The IDE Agent gathers data for the IDE MIB. The data includes: • IDE host controller information • ATA disk information • ATAPI device information The IDE Agent is located in /opt/compaq/storage/bin/cmaided. The suggested poll_time is 15 seconds. The minimum poll_time is 5 seconds.
FCA Agent (cmafcad)	The FCA agent gathers data for the 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 The FCA Agent is located in /opt/compaq/storage/bin/cmafcad. The suggested poll_time is 15 seconds (default). The minimum poll_time is 5 seconds.

Sub-agent	Description
SCSI Agent (cmascsid)	The SCSI Agent gathers data for the SCSI MIB. The data includes: • SCSI host controller information • SCSI disk drive information • SCSI tape drive information The SCSI Agent is located in /opt/compaq/storage/bin/cmascsid. The suggested poll time is 15 seconds. The minimum poll time is 5 seconds.
Event Deamon (cmaeventd)	The Event Daemon gathers storage hardware events from firmware and passes them on to other agents upon request. The Event Daemon is located in /opt/compaq/storage/bin/cmaeventd.

1-1-7 Data Collection Agents

Data Registries are composed of standard Linux directories and associated files. Each file in the data registry is a logical object containing "n" related data items.

The MIB items supported by the Data Collection Agents are listed in the /opt/compaq/foundation/etc/cmafdtnobjects.conf file. The MIB items supported by the Server Data Collection Agents are listed in the /opt/compaq/server/etc/cmasvrobjects.conf file.

During installation, each agent is configured to start automatically after SNMP Agent (snmpd) is started and to stop after snmpd is stopped.

1-2 HP Open-IPMI Driver (hp-OpenIPMI)

The hp-OpenIPMI device driver is a derivative work of the IPMI device driver that ships with the standard Linux kernel. This driver has been enhanced to include bug fixes in addition to supporting a PCI Base Management Controller (BMC) such as provided by the HP Integrated Lights-Out 2 (iLO 2) management controller. The file, /opt/hp/hp-OpenIPMI/IPMI.txt, is also a derivative of the Documentation/IPMI.txt file included with the standard Linux kernel. This file has been enhanced to document the additional parameters that may be passed to the ipmi_si.ko driver. The hp-OpenIPMI device driver enhancements are expected to be incorporated into the OpenIPMI device driver (www.openipmi.org) and subsequently, the standard Linux kernel. This driver may be used with other applications in addition to the HP Advanced System Management XL (hpasmxl) application.

1-3 HP Lights-Out Drivers and Agents (hprsm)

The HP Lights-Out Drivers and Agents package contains the following drivers and agents:

- Remote Insight Driver (cpqrid)
- iLO Management Interface Driver (cpqci)
- Remote Insight/Integrated Lights-Out Agent (cmasm2d)
- Rack Agent (cmarackd)
- Rack Infrastructure Interface Service (cpqriisd)
- Compaq BL Rack Upgrade utility (cpqblru)

1-3-1 Remote Insight Driver (cpqrid)

The Remote Insight Driver (cpqrid) enables the routing of SNMP traffic out of the Remote Insight Lights-Out Edition and Remote Insight Lights-Out Edition II adapters. These adapters are equipped with an integrated network interface card (NIC) that is used to manage the card through its Web interface or through Systems Insight Manager. A further task of the driver is to expose the IML of the system through the management adapters.

The adapter itself operates without any additional driver (for example, the Remote Log In and Virtual Floppy features are available). The driver only enhances the capabilities of the adapter.

Integrated Lights-Out allows browser access to ProLiant servers through a seamless, hardware-based graphical Remote Console, Virtual Power Button, and Virtual Floppy. This functionality does not require an OS driver.

1-3-2 iLO Management Interface Driver (cpqci)

The iLO Management Interface Driver (cpqci) enables iLO data collection and integration with the ProLiant Management Agents and the rack infrastructure interface service. The driver enables communication routing of SNMP traffic from the ProLiant Management Agents through the dedicated iLO management NIC.

1-3-3 Remote Insight/Integrated Lights-Out Agent (cmasm2d)

The Remote Insight/Integrated Lights-Out Agent (cmasm2d) gathers data for the Remote Insight/Integrated Lights-Out MIB. The data includes:

- Configuration and statistical information for the Remote Insight Board or Integrated Lights-Out (RIB/RILOE/iLO)
- Events logged on to the RIB or iLO
- Configuration and statistical information for the Remote Insight/Integrated Lights-Out NIC

1-3-4 Rack Agent (hprackd)

The Rack Agent (hprackd) monitors the rack health through the systems management microprocessor on the server, the microprocessor on the server enclosure, and the microprocessor on the power enclosure.

1-3-5 ProLiant Rack Infrastructure Interface Service (cpqriis)

The ProLiant Rack Infrastructure Interface Service (cpqriis) enables communication through the Integrated Lights-Out Management Component to the rack infrastructure. The HP ProLiant Rack Infrastructure Interface Service (cpqriis) opens and sustains communication with the Integrated Lights-Out management controller.

This communication link is vital to obtain a connection to the ProLiant BL p-Class enclosure management controllers in the back of the rack. Without this connection other applications like the Rack Upgrade Utility and Rack Agent will not work.

The service also receives any type of alerts from the Rack Infrastructure and logs those into the OS logging facility.

1-3-6 Compaq BL Rack Upgrade Utility (cpqblru)

Compaq BL Rack Upgrade utility (cpqblru) sends ROM RUNTIME images to the various BL-p enclosure management controllers in the rack.

1-3-6-1 cpqblru for Linux operating systems

To flash all Management Modules, execute the following command:

```
cpqblru -a cpqrmm###.bin
```

For more options, refer to the manpage by executing the command:

```
man cpqblru
```

To flash all Management Modules, complete the following steps:

1. Click on Start -> Programs -> Compaq system tools -> Compaq BL rack upgrade utility
2. Click on Browse to select the firmware image
3. Select the enclosures you wish to upgrade.
4. Click Start to begin the flash process.

1-3-7 Management hardware supported

The Remote Insight Driver is supported on the Remote Insight Lights-Out Edition and Remote Insight Board Lights-Out Edition II adapters. Documentation on these adapters can be found at www.hp.com/servers/manage.

For documentation on Integrated Lights-Out, which is supported by the iLO Management Interface Driver, visit http://h18013.www1.hp.com/manage/ilo-description.html.

Refer to the QuickSpecs for each product to determine the servers and operating systems supported.

1-4 NIC Agent (cmanic)

The NIC Agent collects information from network interface controllers at periodic intervals, make the collected data available to the SNMP agent, and provide SNMP alerts. The NIC Agent gathers data for the NIC MIB from NIC device drivers supporting the /proc file system reporting format. The data includes:

- Physical mapping and configuration data for each network interface.
- Network statistics for Ethernet interfaces. Information is provided for HP controllers. Limited information may be provided for third-party NICs.

A NIC Agent README file is placed in the /opt/compaq/nic/etc directory after installation. The README file contains the most current information about the NIC Agent.

1-5 HP System Management Homepage (hpsmh)

The HP System Management Homepage is a web-based interface that consolidates and simplifies single system management for HP servers running Linux operating systems. The System Management Homepage aggregates and displays data from Web Agents and other HP Web-enabled System Management Software that includes HP Insight Diagnostics, the Array Configuration Utility and the HP Software Version Control Agents. The System Management Homepage enables IT administrators to view in-depth hardware configuration and status data, performance metrics, system thresholds, diagnostics and software version control information using a single intuitive interface.

Additional information about Insight Management Agents is available at the following location: http://h18013.www1.hp.com/products/servers/management/agents/index.html.

Customers without automatic monitoring tools can view status on servers that have the HP System Management Homepage, previously called ProLiant Management Agents, installed using a standard Web browser. The HP System Management Homepage responds to port 2381 (if the installed browser supports SSL encryption). For example, point the browser to https://192.1.1.20:2381or https://localhost:2381 (the "https://" portion of the address is required).

The HP System Management Homepage allows you to view subsystem and status information from a Web browser, either locally or remotely.

Tip:

To install System Management Homepage (hpsmh), you must be logged in as root user and refer to "hpsmh Installation Guide" for instructions on how to install hpsmh http://h20000.www2.hp.com/bc/docs/support/SupportManual/c00293371/c00293371.pdf.

1-6 Systems Insight Manager

HP System Insight Manager (HP SIM) combines the strengths of Insight Manager 7, HP Toptools, and HP Servicecontrol Manager to deliver a single tool for managing HP ProLiant, Integrity, and HP 9000 systems running Linux and other OS. The core HP SIM software uses WBEM to deliver the essential capabilities required to manage all HP server platforms.

HP SIM can be extended to provide system management with plug-ins for HP clients, storage, power, and printer products. Plug-in applications for workload management, capacity management, virtual machine management, and partition management through the Integrity Essentials enable you to pick the value-added software required to deliver complete lifecycle management for your hardware assets.

For installation information, refer to the "Installing on Linux" section of the HP Systems Insight Manager Installation and User Guide, which is available for download at http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html.

2 Manual Installation

This section covers prerequisites for installation and explains how to install, upgrade, and remove the packages for HP System Health Application and Insight Management Agents (hpasm), HP Lights-Out Drivers and Agents for Linux (hprsm), and NIC Agents (cmanic).

2-1 Prerequisite: Linux library and package dependency files

For the hpasm and hprsm to install and work properly, you must install the required library or package for the Linux distribution (see Table 9).

Table 9. Web Agent requirements

Linux distribution	Hpasm required library or package	Hprsm required library or package
Red Hat Enterprise Linux 4	bash	glibc-kernheaders
	coreutils	glibc-headers
	gawk	glibc-devel
	*glibc(>=2.3.4-2) [i386]	gcc
	gpm(>=1.20.1-66)	rpm-build
	grep	kernel-devel OR kernel-smp-devel OR kernel-hugemem-devel (depends on which kernel is running).
	*libgcc(>=3.4.3-9.EL4)[i386]	
	*libstdc++(>=3.4.3-9.EL4)[i386]	The files listed in the section above need to be explicitly selected and installed during or after OS installation.
	ncurses(>=5.4-13)	
	sed	
	All files above are installed automated if you choose the OS default installation.	
	*compat-libstdc++(>=296-2.96-132.7.2)[i386]	
	lm_sensor	
	net-snmp	
	net-snmp-libs	
	sysVinit	
	tcl	
	tclx	
	tixwish	
	tk	
	The files listed in the section above need to be explicitly selected and installed during or after OS installation	
	*Must install this file for x86_64 platform.	

17

Linux distribution	Hpasm required library or package	Hprsm required library or package
SUSE LINUX Enterprise Server 9	bash coreutils gawk glibc(>=2.3.3-98.38) grep libgcc-3.3.3-43.28 libstdc++-3.3.3-43.28 ncurses(>=5.4-61.4) net-snmp sed sysvinit All files above are installed automated if you choose the OS default installation.	gcc glibc-devel kernel-source (depends on which kernel is running). The files listed in the section above need to be explicitly selected and installed during or after OS installation

For full functionality, the hpsmh requires the following components:

- SNMP stack of the Linux distribution
- Java Virtual Machine Version 1.4.1 (or greater)

2-1-1 Installing the HP System Health Application and Insight Management Agents (hpasm)

If you have a previous version of the HP System Health Application and Insight Management Agent (hpasm), the HP OpenIPMI Device Driver (hp-OpenIPMI), the HP Lights-Out Drivers and Agents (hprsm), or the NIC Agents (cmanic) installed, you must uninstall these components before installing the new RPM files.

To determine if these components are loaded, type the commands listed in the "To verify installation" column in Table 10; to remove the component, type the command shown in the "To remove" column.

Table 10. Loaded components

Component	To verify installation	To remove
HP System Health Application and Insight Management Agents	%rpm –q hpasm	%rpm -e cmanic
HP Light-Out Drivers and Agents	%rpm –q hprsm	%rpm -e hprsm
HP OpenIPMI Device Driver	%rpm –q hp-OpenIPMI	%rpm –e hp-OpenIPMI
NIC Agents	%rpm –q cmanic	%rpm -e hpasm

Note:
Remove cmanic or hprsm before removing hpasm because of driver dependencies.

If concurrent access on the RPM database is attempted, the following messages may result:

- rpmQuery: rpmdbOpen() failed
- cannot get shared lock on database
- rpmQuery: rpmdbOpen() failed

To install hpasm, you must login as the "root" user; and then type:

```
rpm –ivh hpasm-<version>.<distribution>.<platform>.rpm
```

Note:
The version number for the RPM file depends on the supported systems and functionality. The distribution refers to the Linux distribution supported by the RPM. The platform refers to the processor architecture the RPM was built to support. The RPM file has a binary compiled for the supported distribution with the default kernel.

After the installation process, complete the following steps:

1. To configure and activate agents, type the following:
   ```
   %hpasm activate
   ```

2. Provide basic Simple Network Protocol (SNMP) information, when prompted. The drivers and agents are inserted immediately. However, the Health Monitor may take more than two minutes to load, which is expected behavior. On systems with variable speed fans, the fans may start spinning more slowly if the temperature is reasonably low.

3. To check if the Health Monitor is loaded properly, type the following command prompt (which is only available when logged in as "system administrator", "super user", or "root"):
   ```
   ps –efm | grep hpasmd
   ```

   You should see a listing of the processes named hpasmd. There will be 12+ of these entries.
4. To check if the agents are loaded properly, type the following command:
   ```
   ps –ef | grep cma
   ```

   The following information displays, indicating that the agents are running:
   ```
       cmafdtn: cmathreshd cmahostd cmapeerd
       cmasvr: cmastdeqd cmahealthd cmaperfd
       cmastor: cmaeventd cmaidad cmafcad cmaided cmascsid
   ```
   For more information about these components, refer to the online documentation by typing:
   ```
   %man hpasm
   ```

2-1-2 Installing the HP OpenIPMI Driver (hp-OpenIPMI)

The Linux kernel ".config" file must have IPMI support enabled for rebuilds. This is not the default on some older Linux distributions. If a different Linux kernel (e.g. an errata kernel) is used in place of the supported version of Linux, the standard Linux Kernel build environment will need to be installed. Error messages will be displayed during the rebuild process indicating which Linux packages are missing.

If a previous version of the hp-OpenIPMI package has been installed, it must be removed before this package can be installed. To remove the previous version and any packages dependent on it, type the following:

```
%/etc/init.d/hpasm stop
%rpm –e hp-OpenIPMI
```

To install hp-OpenIPMI RPM, type the following at the command prompt:

```
%rpm –ivh hp-OpenIPMI-<version>.rpm
%/etc/init.d/hpasm start
```

To verify that the HP OpenIPMI Driver is loaded, type the following command prompt:

```
%lsmod | grep ipmi
```

Entries for the following modules display:

- ipmi_si
- ipmi_devintf
- ipmi_msghandler

For more information about these components, refer to the online documentation by typing:

```
%man hp-OpenIPMI
```

2-1-3 Installing the HP Lights-Out Drivers and Agents (hprsm)

The hprsm package requires the hpasm package to be installed first.

You can check for the presence of the hpasm package by typing:

```
% rpm -q hpasm
```

To install the hprsm RPM, type the following at the command prompt:

```
%rpm –ivh hprsm-<version>.<distribution>.<platform>.rpm
```

The RPM file has a binary that is compiled for the default kernel of the supported distribution. To install the RPM on a non-default kernel, you must also install the kernel sources for the compiled kernel.

Note:
The hprsm RPM will attempt to detect if a RILOE adapter is present before inserting the cpqrid driver. If a RILOE adapter is not present, the RSM RPM will default to the cpqci driver.

For more information about these components, refer to the online documentation by typing:

```
%man hprsm
%man cpqrid
%man cpqci
%man cpqriisd
%man cpqblru
```

2-2 NIC Agents (cmanic)

The cmanic package requires the hpasm package to be installed first.

To install the NIC Agents, type the following at the command prompt:

```
%rpm –ivh cmanic-<version>.<platform>.rpm
```

2-3 Uninstalling drivers and agents

There are two options for preventing the drivers and agents from running, uninstalling, and starting or stopping drivers. For information on uninstalling or unloading drivers or agents, refer to the "Starting and stopping agents and services" section.

Table 11 lists the commands for uninstalling the entire contents of the hpasm, hprsm, and cmanic packages.

Table 11. Uninstall drivers and agents commands

Uninstall Command	Description
`%rpm –e hpasm`	Removes the hpasm package from your system.
`%rpm –e hp-OpenIPMI`	Removes the hp-OpenIPMI package from your system.
`%rpm –e hprsm`	Removes the hprsm package from your system.
`%rpm –e cmanic`	Removes the cmanic package from your system.

Caution:
If the hpasm package was running, it will be shut down first. If you reboot the system, the hpasm package will not be inserted at bootup time.

2-4 Updating drivers and agents

The following sections provide information on updating specific drivers and agents.

2-4-1 hpasm package contents

RPM provides the option to upgrade a package.

Before upgrading, uninstall any RPM packages that are dependent upon the hpasm package, such as the Lights-Out Drivers and Agents, the Storage Agents, and the NIC Agents. These packages are dependent upon a specific hpasm package version.

Caution:
Attempting to install these packages on an unsupported hpasm package version might result in an unstable system.

To uninstall any packages present on the server, type the following, in exact order:

```
rpm -e cmanic
rpm -e hprsm
rpm -e hpasm
```

To upgrade the hpasm package, install the latest hpasm package, type the following command:

```
rpm -ivh hpasm-<version>.<distribution>.<platform>.rpm
```

The cpqhealth package cannot upgraded. Remove the previous version by typing the following command before installing the newer version of hpasm:

```
rpm -e cpqhealth
```

After installing a package, the agents do not start immediately. To start or activate the agents, type the following command:

```
%hpasm activate
```

The software guides you through various questions which relate to the way SNMP should be configured with the ProLiant Management Agents. The last question pertains to which agents, if any, should be started during the standard boot process. The Health Monitor will always be loaded; however, you may control the agents' behavior.

To start the hpasm package manually, type the following command:

```
/etc/init.d/hpasm start
```

2-4-2 hprsm package contents

If you are upgrading from a previous version of the hprsm package, type:

```
%rpm -Uvh hprsm-<version>.<distribution>.<platform>.rpm
```

2-4-3 NIC Agent contents

If you are upgrading from a previous version of the NIC Agent, type:

```
%rpm -Uvh cmanic-<version>.<platform>.rpm
```

3 Customization

This section includes advanced topics on data center customization.

3-1 Configuration files

The ProLiant Management Agents Configuration file, /opt/compaq/cma.conf, is shared by all HP ProLiant Management Agents packages. Currently, exclude directives, taint directives, trap email notification configuration and base socket number (used by cmaX) are supported. The agents are capable of sending email notifications in addition to SNMP traps. The trapemail entries in /opt/compaq/cma.conf configure the email commands, which are then read by the Peers software during their initialization.

The exclude directives allow customization of which agents to start automatically. Any drivers and agents included on this line will not be started by the run level scripts.

In addition, this file allows a "notaint" line which restricts the loading of HP proprietary management drivers (such as cpqrid or cpqci).

The exclude and notaint entries can be modified using the hpasm activate or hpasm reconfigure commands.

If trapemail entries are edited, the Peers software must be restarted before the configuration modification is effective. The command to restart the agent is:

```
#/etc/init.d/hpasm restart agent
```

The syntax of the trapemail lines is as follows:

```
trapemail mail_command
```

The keyword "trapemail" indicates that the rest of the line is the command for sending trap email. In mail_command, you must provide the full path of your email command, the subject, and the recipients.

Multiple trapemail lines may be defined in /opt/compaq/cma.conf. A default line will be added during installation if none exists:

```
trapemail /bin/mail -s 'HP Insight Management Agents Trap Alarm'
root
```

The mail_command can be any Linux command that reads standard input. For example, using trapemail /usr/bin/logger will log trap messages to system log file (/var/log/messages).

The cmaXSocketBase entry in configuration file /opt/compaq/cma.conf configures the starting socket port used for communications between cmaX and Peers. The entry is not needed unless the "bind() failed!" message displayed in the Agents log file /var/spool/compaq/cma.log.

This entry should be listed in the configuration file as follows:

```
cmaXSocketBase 12345
```

If cmaXSocket Base entry is edited, the snmpd and Peers software must be restarted before the configuration modification is effective. You can do this by entering the following commands:

```
#/etc/init.d/snmpd restart
#/etc/init.d/hpasm restart agent
```

You may also manipulate the /opt/compaq/cma.conf file which contains one or more exclude directives. Any string after the exclude keyword is interpreted as an agent name that should not be started. Examples include:

```
exclude cmahealthd

exclude cmastdeqd
```

These two lines exclude two agents from the startup: the Health Agent (cmahealthd) and the Standard Equipment Agent (cmastdeqd).

3-2 Configuring the hprsm package

The Remote Insight/integrated Lights-Out Agent executable is /opt/compaq/server/bin/cmasm2d.

For Remote Insight/integrated Lights-Out Agents to work properly, the localhost (127.0.0.1) requires SNMP READ (get) privileges at a minimum. The localhost SNMP WRITE (set) privileges are required for enabling SNMP WRITE (set) capability in the Remote Insight/integrated Lights-Out Agent.

The Rack Agent executable is /opt/compaq/server/bin/cmarackd.

Command line arguments can be used with these agents.

To create a custom hprsm package, type the following command:

```
/opt/compaq/hprsm/etc/rebuild
```

The completed packages will be copied to the /usr/src/redhat/RPMS/i386 or /usr/src/packages/RPMS/i386 directory. The RPMs are versioned as "CUSTOM" to distinguish these RPMs from the standard drivers.

3-3 Starting and stopping agents and services

After the initial install, both the ProLiant Management Agents and the Health Monitor are loaded. Upon a reboot, a run-level script in /etc/init.d/hpasm reloads the driver and agents, even if a different kernel was used for the new run.

To modify which hpasm components are run, see Table 12 for a list of available options. Other agents and services may also be started, stopped, and restarted and are also listed in the table. The hpasm and hprsm commands may be proceeded with the following: "/etc/init.d/hpasm" (for a generic Linux installation), "service hpasm" (for a Red Hat Linux installation), or "rc hpasm" (for a SUSE LINUX installation). (For hprsm commands, replace the "hpasm" portion of the previous examples.)

Table 12. Available commands for modifying components

Command	Description
hpasm activate	This command should be issued only once after the initial install.
	Exception: When the hpasm package is installed through the ProLiant Support Pack or another unattended install mechanism, it is unnecessary to execute this command.
	A series of questions prompts the user to configure SNMP and the Web Agent (similar to the hpasm configure command).
	This command ensures start up of the contained agents and drivers during boot.
hpasm start	Starts every software component in hpasm (Health Monitor and Agents).
hpasm stop	Stops all software components in hpasm in reverse order from how they were started.
hpasm start hpasmd	Starts the Health Monitor (hpasm) only.
hpasm stop hpasmd	Stops the Health Monitor (hpasm) and every agent dependent upon it.
hpasm start agent	Starts every ProLiant Management Agent.
hpasm restart [args]	This command is shorthand for the following:
	hpasm stop [args]
	hpasm start [args]
hpasm reconfigure	Stops the Health Monitor and Agents.
	Reconfigures snmpd configuration and uses existing state as a basis.
	Stops and starts SNMP.
	Starts the Health Monitor and Agents.
hpasm configure	Stops the Health Monitor and Agents.
	Resets snmpd configuration and configures snmpd.
	Stops and starts SNMP.
	Starts the Health Monitor and Agents.
hpasm unconfigure	Stops the Health Monitor and Agents.
	Unconfigures snmpd configuration back to its initial state.
	Stops and starts SNMP.
%/etc/init.d/hprsm start <agent> %/etc/init.d/hprsm stop <agent>	Starts the hprsm package contents. Stops the hprsm package contents.
/etc/init.d/hprsm start cpqriisd or service hprsm start cpqriisd (for Red Hat Linux distributions)	Invokes the Rack Infrastructure Service manually. Note: If the server is a ProLiant BL p-Class server, The Rack Infrastructure Service should start immediately after the hprsm package is installed.

3-4 Parameters

This section lists parameters for various agents and services.

Table 13 includes the command line arguments that can be passed to the NIC agents (cmanicd) from the /opt/compaq/nic/bin/cmanicd script.

Table 13. Parameters for NIC agents

Parameter	Description
-p poll_time	Specifies the number of seconds between data caching and poll intervals. NIC drivers are only queried when a request comes in and the cached information is older than the specified poll interval. The default value is 20 seconds. The minimum poll time is 10 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 the NIC Agent is allowed to send traps or not. A trap_state of OK (default) indicates the NIC Agent may send SNMP traps. A trap_state of NOT_OK means that NIC Agent is not allowed to send traps.

For example, to set the poll interval to 30 seconds and prevent traps, change PFLAGS= to PFLAGS="-p30 -t NOT_OK" in the /opt/compaq/nic/etc/cmanicd script.

Traps are configured using the standard SNMP configuration file (snmpd.conf). Refer to the snmpd.conf manual page for the most current configuration information. When snmpd.conf or snmpd.local.conf configuration files are changed or when the SNMPCONFPATH environment variable is changed, the cmanic daemon must be restarted.

If default High or Medium firewall configuration is selected during the installation of Red Hat Linux 7.2, external SNMP requests will be rejected by the system and the server will become unmanageable. There are significant security implications to configuring firewall. Consider the ipfw, ipchains, ipchains-save, and ipchains-restore man pages as mandatory reading before making any change to firewall configuration.

The system should start accepting SNMP requests from Systems Insight Manager or other management consoles with the following command:

```
#ipchains -I input -s 16.101.168.68/255.255.255.255 \d
16.101.169.69/255.255.255.255 161:161 \

I eth0 -p udp -j ACCEPT
```

In the example above, 16.101.168.68 is the IP address of a remote system running management console (or issuing SNMP requests) and 16.101.169.69 is the IP address of the interface "eth0" of the server running Red Hat Linux 7.2.

The Rack Infrastructure Interface Service is contained in an executable called cpqriisd which resides in the /sbin directory. It can be invoked by using the commands in Table 14.

Table 14. Command options for the Rack Infrastructure Service

Option	Description
-F	This option will "daemonize" the process and will start the daemon up in a production level environment. Usage is recommended. An easier way to accomplish this task is to execute the hprsm run-level script.
-D	This option starts the service in a debug environment. stdin and stdout will go to the console; typing "e" will quit the daemon. Alerts are logged onto the same text console.
-V	This option enables the verbosity of the output. The default behavior is to output to both /var/log/messages and tty1 – tty10.
-?	This option reports the version of the service and informs the user of the other options described above.

3-5 Custom builds and packaging

The hprsm package can be installed on "custom" or patched Linux kernels. There is a source wrapper file that abstracts the Linux functionality from the remainder of the driver code. If there is a Linux kernel symbol mismatch, the driver script (/opt/compaq/cpqci/cpcpqci or /opt/compaq/cpqrid/cpcpqrid) will check to see if the Linux kernel source files are present. If so, the script will automatically rebuild and load the driver. If the Linux kernel source files are not present, a warning message will be displayed.

To successfully install the hprsm RPM package, the following criteria must be met:

- All kernel sources for the currently running kernel must be installed on the server.
- The link /lib/modules/`uname –r`/build must exist and be linked to the directory containing the (possibly patched) kernel sources.
- The standard build tools, such as gcc, ld, make, and touch must be loaded on the server.
- The file /lib/modules/`uname –r`/build/include/linux/version.h must exist and match the version of the booting kernel on the development server and the version of the booting kernel on any other server where this custom RPM will be deployed.

Many servers do not have all of this software available. Therefore, HP provides a self replication mechanism that creates a custom RPM that can be deployed without these dependencies. This custom RPM is automatically created with rebuilt cpqci and cpqrid drivers when the hprsm package is installed, but a manual process is also available if more customization is desired.

The hprsm RPM places deliverables in the /opt/compaq directory. Those deliverables are subdivided into several directories. The rebuild script is provided in the /opt/compaq/hprsm/etc location.

To create a custom hprsm package (after the requirements have been met), execute the following:

```
/opt/compaq/hprsm/etc/rebuild
```

The completed packages will be copied to the /usr/src/redhat/RPMS/i386 or /usr/src/packages/RPMS/i386 directory. The RPMs are versioned as "custom" to distinguish these RPMs from the standard drivers.

3-5-1 Rebuilding the hprsm package

To recreate hprsm package version 6.40.0 or later for fast redeployment, type:

```
% /opt/compaq/hprsm/etc/rebuild
```

This command creates a custom RPM which does not need to rebuild the drivers. Instead, this package lands only on servers containing a kernel version identical to the one used to build the custom RPM.

To customize the rebuild step even further, you can perform a minimal rebuild. Since hprsm contains many software components, there are cases where you may need a minimal RPM, containing only a choice few deliverables. For example, consider a situation where you do not desire agents. In this case, use Red Hat Linux 8.0 as our base OS distribution. We assume that we want to deploy hprsm on a Linux errata kernel (2.4.18-27.8.0.smp) and not the stock kernel that came with the distribution (2.4.18-14smp).

We have a rebuild script which resides in /opt/compaq/hprsm/etc. The rebuild script uses two files, hprsm.txt and hprsm-manifest.txt, in the same directory. The hprsm-manifest.txt file contains a list of files and directories used during the rebuild. Since we do not want the agents running, we can safely omit the agent executables. To avoid startup errors, you should also edit /etc/init.d/hprsm and remove the agent names from the PNAMES and AGENTS variables at the beginning of the file.

Furthermore, that package contains the cpqrid and cpqci drivers for a multitude of stock kernel versions. Since we are building on an errata kernel, these precompiled versions become an unnecessary burden. Therefore, we can delete the precompiled versions from our custom build as well.

Even though it would be permissible to simply comment out the files in question from hprsm-manifest.txt, we will be a little more conservative by omitting files within directories, while preserving the directories themselves. Then, before issuing the rebuild command, we will delete the files in question from our file system so they will not be picked up. This strategy is also valid for the case where the manifest describes a whole directory structure, but certain files in it have become undesirable.

First, start to delete the following directory content:

```
# Delete all the hprsm agents
rm -f /opt/compaq/server/bin/cmasm2d

rm -f /opt/compaq/server/bin/cmarackd

rm -rf /sbin/cpqriisd

# Delete cpqrid and cpqci drivers for other, unused kernels
find /opt/compaq/ -name 'cpqrid.o' | grep -v 2.4.18-27.8.0 | xargs
rm -f

find /opt/compaq/ -name 'cpqci.o' | grep -v 2.4.18-27.8.0 | xargs
rm -f
```

Next, clean up hprsm-manifest.txt file to remove the occurrence of the deleted files. As discussed above, preserve the directories in which these files reside.

```
files
%defattr (755,root,root)
/etc/init.d/hprsm
/opt/compaq/hprsm/hprsm
/opt/compaq/cpqrid/cpcpqrid
/opt/compaq/cpqci/cpcpqci
/opt/compaq/server/cpserver
/opt/compaq/server/setuphelper
%defattr(755,root,root)
/sbin/cpqblru
%defattr(644,root,root)
```

```
/opt/compaq/cpqrid/drivers/cpqrid.o
/opt/compaq/cpqrid/drivers/kernel.txt
/opt/compaq/cpqci/driver/cpqci.o
/opt/compaq/cpqci/driver/kernel.txt
%defattr(755,root,root)
/usr/lib/libcpqipmb.so
/usr/lib/libcpqipmb.so.1
/usr/lib/libcpqipmb.so.1.0
%defattr(755,root,root)
/opt/compaq/server
%defattr(644,root,root)
/usr/share/man/man4/cpqrid.4.gz
/usr/share/man/man4/cpqci.4.gz
/usr/share/man/man4/cpqriisd.4.gz
/usr/share/man/man4/cpqblru.4.gz
/usr/share/man/man4/hprsm.4.gz
```

Now it is time to rebuild:

```
% /opt/compaq/hprsm/etc/rebuild

Custom RPM(s) available: /usr/src/redhat/RPMS/i386/hprsm-7.1.1-
custom.i386.rpm
```

The custom RPM is much smaller in size. Deploying is now automatic and will start only the cpqrid or cpqci driver.

3-5-2 Using the HP ProLiant BL Rack Upgrade Utility

The HP ProLiant BL Rack Upgrade Utility upgrades the firmware on the server blade and power management modules in the rack.

For iLO reflash and firmware upgrade information, refer to the Integrated Lights-Out User Guide located at http://h18013.www1.hp.com/manage/ilo-description.html.

```
cpqblru [-eql?]  [-a address1,address2,...]  [-c
chassis1,chassis2,...]
```

Table 15. ProLiant BL Rack Upgrade Utility parameters

Parameter	Description
-a address1,address2,...	This optional parameter considers only enclosures with address1, address2, etc. The list of addresses must be composed of 16-bit quantities separated by commas. The addresses can be obtained by running –q (see below). No white spaces are allowed in between. If no comma-separated list is given, all possible addresses in the rack are considered.
-c chassis1, chassis2,...	This optional parameter considers only enclosures with positions chassis1, chassis2, etc. that are counted from the bottom. The list must be composed of small numbers that are legal positions in the rack. No white spaces are allowed in between the commas and the numbers. A list such as 1,2,5, for instance, would signify the bottom, second-to-bottom, and fifth-to-bottom enclosures.
-e	Disregard the local enclosure (for example, the enclosure containing the server from which we flash) in the flashing. This parameter is given in conjunction with –a or –c.
-l	Disregard anything but the local enclosure (for example, the enclosure containing the server from which we flash). This parameter should not be given with –a or –c.
-q	This parameter queries the chassis positions, their serial numbers, and their firmware status and returns their addresses.

The man page for this utility may be viewed by typing man cpqblru at the command prompt.

Please note the following while upgrading ProLiant BL p-Class enclosure management controllers:

- During a flash upgrade, only the primary firmware image is reflashed. All controllers have a backup image. The backup image is used for recovery purposes when a flash upgrade is interrupted or otherwise fails. Restoring the backup firmware image is rarely needed and is covered in the Integrated Lights-Out User Guide located at: http://h18013.www1.hp.com/manage/ilo-description.html.

- When updating enclosure management controllers in more than one enclosure, the new image must be transmitted twice (first to the local enclosure and second to the remote enclosure(s) using broadcast mode). The update process can take up to 10 minutes or more. The upgrade process notifies the user if the upgrade succeeded or failed.

- The reflash operation consumes all bandwidth of the bus connecting the management controllers. Consequently, other software components, such as the ProLiant Rack Agent might not report up-to-date information during the flash upgrade.

3-5-3 Installing System Management Homepage on Linux IA_32 systems

To install System Management Homepage on IA_32 systems, your system must meet the minimum requirements. For more information regarding minimum requirements, refer to Chapter 2. Installation Overview and Requirements in the System Management Homepage Installation Guide: http://h20000.www2.hp.com/bc/docs/support/SupportManual/c00293371/c00293371.pdf.

In addition, you must have the hpsmh-2.0.0.linux.i386.rpm rpm.

Note:
The general 32-bit RPM List is not installed by default.

To install System Management Homepage, enter the following command line:

```
rpm –ivh hpsmh-2.0.0-linux.i386.rpm
```

A message appears indicating the System Management Homepage installed successfully with default configuration values.

3-5-4 Mass deployment with hpasm

HP provides a self replication mechanism that creates a custom RPM that can be deployed without kernel dependencies.

The hpasm RPM places deliverables in the /opt/compaq directory. Those deliverables are subdivided into several directories. The rebuild script is provided in the /opt/compaq/hpasm/etc location. This script is also soft linked under the /sbin directory under the name hpasm_rebuild.

To create a custom hpasm package, execute the following:

```
hpasm_rebuild
or
/opt/compaq/hpasm/etc/rebuild
```

The completed packages will be copied to the /usr/src/redhat/RPMS/i386 or /usr/src/packages/RPMS/i386 directory. The RPMs are versioned as "CUSTOM" to distinguish these RPMs from the standard drivers.

To insert the monitor at bootup time, a link to /etc/init.d/hpasm is created in Run Levels 2 through 5. If there is a problem with the Health monitor, you can bring the system up in maintenance mode (init 1, also known as single user mode) or use interactive boot to correct the issue.

This command creates a custom RPM which does not rebuild all drivers. Instead, these packages land only on servers containing a kernel version identical to the one used to give the hpasm_rebuild command.

To specify configuration settings before issuing the rebuild command, perform either of these actions:

- Type the following after RPM installation:

```
% hpasm activate
```

- Type the following after the activation step:

```
% service hpasm configure
```

The script logic creates a file called hpasmrc that stores the latest configuration settings. Here is an example of such a file:

```
# install mode
export CMASILENT="YES"
# kernel version
export CMAKERNELVERSION="2.4.18-27.8.0smp"
#local rw community string
export CMALOCALHOSTRWCOMMSTR=""
#local ro community string
export CMALOCALHOSTROCOMMSTR=""
#rw authorized management stations (multiples allowed)
export CMAMGMTSTATIONRWIPORDNS=""
#rw authorized mangamane station community string (multiplies
allowed)
export CMAMGMTSTATIONRWCOMMSTR=""
#ro authorized management stations (multiples allowed)
export CMAMGMTSTATIONROIPORDNS=""
#ro authorized mangamane station community string (multiplies
allowed)
export CMAMGMTSTATIONROCOMMSTR=""
#default trap community string
export CMADEFTRAPCOMMSTR=""
#trap recipients (multiples allowed)
export CMATRAPDESTINATIONIPORDNS=""
#trap recipient community strings (multiples allowed)
export CMATRAPDESTINATIONCOMMSTR=""
#system contact
export CMASYSCONTACT=""
#system location
export CMASYSLOCATION=""
#agent exclusion on startup
export CMAAGENTEXCLUDESTR="cmawebd cmafdtnpeerd cmahostd
cmathreshd cmasvrpeerd cmahealthd cmastdeqd cpqriisd cmasm2d
cmarackd"
#HTTP server passwords
export HPHTTPSERVERADMINPASSWD=""
export HPHTTPSERVEROPERATORPASSWD=""
export HPHTTPSERVERUSERPASSWD=""
```

When a rebuild command is issued, this file will be picked up and used on the deployment of the custom RPM.

The CMAKERNELVERSION parameter provides additional protection. If a custom RPM package is deployed with a CMAKERNELVERSION that does not match the current kernel, the package would refuse a silent install and instead revert back to the usual interactive mode (creating the need to type hpasm activate).

The first step is to manipulate /etc/hpasmrc to look like the sample file mentioned previously. In this file, we do not use any settings except CMASILENT=YES (to make the configuration automatic); CMAKERNELVERSION is set to the kernel we want to support, and CMAAGENTEXCLUDESTR has a list containing all the agents. This will cause the agent exclusion later.

Next, we will have to manipulate the rebuild process.

The rebuild script resides in /opt/compaq/hpasm/etc. This script uses two files, hpasm.txt and hpasm-manifest.txt, in the same directory. The hpasm-manifest.txt file contains a list of files and directories used during the rebuild. Since we do not want the agents running, we can safely omit the agent executables. Keep in mind that this is only safe because we excluded all agents from running, which makes the run-level scripts ignore the file locations we are about to delete.

Now, we need to clean up hpasm-manifest.txt file in order to remove the occurrence of the deleted files. As discussed above, we will preserve the directories in which these files reside.

```
%files
%defattr (755,root,root)
/opt/Compaq/hpasm/et/hpasm
/opt/compaq/hpasm/etc/common.functions
/opt/compaq/hpasm/etc/cpqasm.functions
/opt/compaq/hpasm/etc/foundation.functions
/opt/compaq/hpasm/etc/server.functions
/opt/compaq/hpasm/etc/rebuild
/opt/compaq/hpasm/addon/cmad
/opt/compaq/hpasm/addon/condcopy
/opt/compaq/hpasm/addon/condrem
/opt/compaq/hpasm/addon/sancheck
/opt/compaq/hpasm/addon/libcpqci.so
/opt/compaq/hpasm/addon/libcpqci.so.1
/opt/compaq/hpasm/addon/libcpqci.so.1.0
/opt/compaq/hpasm/addon/libcmaX.so
/etc/init.d/hpasm
/etc/casmd.conf
/etc/cevtdl.conf
/etc/cevtdm.conf
%defattr(644,root,root)
/opt/compaq/hpasm/distro.txt
/opt/compaq/hpasm/hpasm.license
/opt/compaq/hpasm/etc/hpasm.txt
/opt/compaq/hpasm/etc/hpasm-manifest.txt
/opt/compaq/hpasm/addon/condcopy.txt
/opt/compaq/hpasm/addon/sancheck.txt
/opt/compaq/hpasm/addon/cpqbssa.txt
/opt/compaq/hpasm/addon/cmasvrobjects.conf
%defattr(755,root,root)
/usr/share/man/man4/hpasm.4.gz
/usr/share/man/man8/cpqimlview.8.gz
/usr/share/man/man8/hpuid.8.gz
/usr/share/man/man8/hplog.8.gz
/sbin/bootcfg
/sbin/cpqimlview
/sbin/cpqimlview.tcl
/sbin/imlbe
/sbin/hpimlview
/sbin/hpuid
/sbin/hplog
/usr/share/pixmaps/hplogo.xbm
/usr/share/pixmaps/m_blue.gif
/usr/share/pixmaps/m_fail.gif
/usr/share/pixmaps/m_green.gif
/usr/share/pixmaps/m_red.gif
/usr/share/pixmaps/m_yellow.gif
%defattr(-,root,root)
/opt/compaq/foundation/bin
/opt/compaq/foundation/etc/cmafdtn
/opt/compaq/foundation/etc/cmafdtnpeerd
/opt/compaq/foundation/etc/cmahostd
/opt/compaq/foundation/etc/cmathreshd
/opt/compaq/foundation/etc/cmawebd
#/opt/compaq/foundation/etc/hpwebsetup
/opt/compaq/foundation/etc/cmafdtnobjects.conf
/opt/compaq/foundation/etc/snmpd.conf.cma
/opt/compaq/webagent
```

```
%defattr(-,root,root)
/opt/compaq/server/bin
/opt/compaq/server/etc/cmasvr
/opt/compaq/server/etc/cmasvrpeerd
/opt/compaq/server/etc/cmahealthd
/opt/compaq/server/etc/cmastdeqd
```

Notice that some of the deleted files reside in subdirectories that were specified in the original manifest file (highlighted in green above). Other files were listed and are now omitted, but we ensured that their directories still exist (highlighted in yellow above).

Now, it is time to rebuild.

```
% hpasm_rebuild
....
Custom RPM(s) available: /usr/src/redhat/RPMS/i386/hpasm-6.40.0-
custom.i386.rpm
```

The custom RPM is much smaller in size.

```
[root@ilo8j22jqx1700r root]# ls -la
/usr/src/redhat/RPMS/i386/hpasm-6.40.0-custom.i386.rpm
-rw-r--r--    1 root      root       622457 Jul 22 14:16
/usr/src/redhat/RPMS/i386/hpasm-6.40.0-custom.i386.rpm
```

Deploying is now automatic and will start only the Health Monitor.

```
[root@ilo8j22jqx1700r i386]# rpm -e hpasm
[root@ilo8j22jqx1700r i386]# rpm -ivh hpasm-6.40.0-custom.i386.rpm
Preparing...
########################################### [100%]
   1:hpasm
########################################### [100%]
Please read the Licence Agreement for this software at


         /opt/compaq/hpasm/hpasm.license

By Not removing this package, you are accepting the terms
of the "License for HP Value Added Software".


====================================================================
NOTE: New snmpd.conf entries were added to the top of
/etc/snmp/snmpd.conf
====================================================================
====================================================================
NOTE: New cma.conf entries were added to the top of
/opt/compaq/cma.conf
====================================================================
HP HTTP server's passwords were all preserved to their previous
setting.

Following environment variables were used to configure
snmpd/agents:
    CMAAGENTEXCLUDESTR
    HPHTTPSERVEROVERWRITE

Starting HP Server Management Drivers and Agents, please wait ...
casmd: hp ProLiant Advanced Server Management Monitoring . . .
cevtd: hp ProLiant Event Logging daemon started . . .
The hpasm RPM has installed successfully.
[root@ilo8j22jqx1700r i386]# lsmod
Module                    Size  Used by    Tainted: P
cpqasm                   335904   2
cpqevt                     9376   2  [cpqasm]
```

4 Conclusion

This HOWTO provides instructions for installing, upgrading, and removing Linux management software, including the prerequisites for using this software with and without errata kernels, and contains usage information for HP System Health Application and Insight Agents(hpasm), HP Lights-Out Drivers and Agents (hprsm), and HP NIC Agents (cmanic).

Appendix A – Error messages

Messages logged if an ASR event occurs are listed in Table 16.

Table 16. Error messages

Message number	Details	
Message 1	"NMI - Automatic Server Recovery timer expiration - Hour %d - %d/%d/%d"	
	Description	This message indicates that the Health Monitor detected an ASR timeout and is attempting to gracefully shut down the operating system. Absence of this message may indicate a critical hardware failure (such as a non-correctable ECC error on a memory DIMM) or some other severe event. This is the first of a series of messages displayed to the console. This message will not be logged to the IML and most likely will not be listed in any system logs.
	Recommended action	Review all the messages logged to the IML to see if any previous errors have been logged (for example, a corrected single-bit memory error might have been logged).
Message 2	"ASR Lockup Detected: %s"	
	Description	This message indicates that the Health Monitor detected an ASR timeout and is attempting to gracefully shutdown the operating system. Absence of this ASR message may indicate a critical hardware failure (such as a non-correctable ECC error on a memory DIMM) or some other severe event. This will be the first ASR message logged to the IML (if logging is possible).
	Recommended action	Review all the messages logged to the IML to see if any previous errors have been logged.
Message 3	"casm: ASR performed a successful OS shutdown"	
	Description	This ASR message indicates that the Health Monitor detected an ASR timeout and has gracefully shut down the operating system. Absence of this message may indicate a hardware failure (such as a non-correctable ECC error on a memory DIMM), a high priority process consuming all the available CPU cycles (software failure) or possibly that a device, such as a storage or network controller is flooding the system with interrupts. This will be the second ASR message logged to the IML if logging is possible.
	Recommended action	If this ASR message is present, this usually indicates a software type error such as a high priority process consuming all the available CPU cycles. Linux tools, such as SAR (system activity report) can be used in conjunction with the ASR facility to locate the process causing the problem.
Message 4	"ASR Detected by System ROM"	
	Description	This message indicates that the ProLiant Server ROM detected an ASR timeout. This message is almost always present in the IML when an ASR timeout occurs. If this is the only ASR message logged to the IML, this may indicate a hardware failure (such as a non-correctable ECC error on a memory DIMM). The ASR feature on a ProLiant server will hard reset the server when the timeout expires, with no software intervention required.

Message number	Details	
	Recommended action	If this is the only ASR message present, this usually indicates a hardware type error (such as an unrecoverable memory error). Try moving the server memory DIMMs to different slots to see if more information can be logged. Review all IML messages that previously occurred to see if any other component has given an indication of failure or temperature limits that might have exceeded normal operating thresholds.

During operation, the service logs events from the infrastructures on tty1 through tty10 (if available), as well as /var/log/messages. If this produces too much text on the screen, adding the option"V0x0" to the hprsm startup script will silence the text.

The service acts as an enabler for other ProLiant value-add software, such as the Rack Agent and the Rack Upgrade Utility.

If the service goes away after a few seconds, there is a failure to initiate communication with the iLO management controller. The failure reason will be logged into the message log. If the service is stopped, dependent applications like the Rack Firmware Upgrade Utility will terminate as well.

Table 17 lists possible issues.

Table 17. cpqriisd messages

Message number	Details	
Message 1	Could not setup server semaphores	
	Could not destroy server semaphores	
	Up sem: Ioctl Failure !	
	Down sem: Ioctl Failure !	
	Down sem	
	Down sem: Ioctl Failure !	
	Down sem	
	get sem: Ioctl Failure !	
	set sem: Ioctl Failure !	
	Description	These messages indicate that synchronization objects called "semaphores" cannot be set up correctly. This issue is most likely occurred because the iLO driver is absent.
	Recommended action	Install the iLO driver.
Message 2	Warning: Shared Memory Segment exists	
	Killing process %s pid %d pgid %d	
	Description	These messages indicate that the daemon encountered a shared memory segment that was not cleaned up properly.
	Recommended action	No action required, since this message is informational. This warning will be removed in a later version of the Rack Infrastructure Interface Service.

Message number	Details	
Message 3	Multiple copies of this daemon may be running - exiting...	
	Description	This message is an issue with Version 1.0.0 of the Rack Infrastructure Interface Service, which disallows the starting of two copies of the service.
	Recommended action	Only one copy of the daemon should be running at any time.
Message 4	Setup Shared Memory failed!	
	Description	This message indicates that a common OS resource, "shared memory," is not available. This issue could be due to high utilization, but most likely a memory segment from Version 1.0.0 of this service was left behind erroneously.
	Recommended action	Install Version 1.1.0-2 of the service.
Issue 5	Semaphore %s interrupted in %s Local Semaphore %s interrupted in %s	
	Description	This type of message will be logged if the service is terminated abruptly (for example, through the "kill" command).
	Recommended action	No action required since this message is informational.
Issue 6	Alert only seems to reach %d out of %d client applications	
	Description	The alerts coming from the infrastructure seem to be dispatched to a subset of registered clients only. Most likely, a client terminated suddenly without properly deregistering itself.
	Recommended action	This message does not indicate a problem with the Rack Infrastructure Interface Service; however, there might be a problem with the HP ProLiant Rack Daemon (cmarackd). Restart cmarackd to verify that the problem persists. If so, contact your HP field service engineer.
Issue 7	ILO exceeded the number of allotted back offs, is it stuck?	
	Description	iLO responds with a "backoff" command indicating a busy state, which is a temporary condition. If this condition lasts too long (5000 tries), the message will appear. Recommended Action : Verify that iLO is not under extreme network load, such as a ping flood.
	Recommended action	Verify that iLO is not under extreme network load, such as a ping flood. Otherwise, contact your HP field service engineer.
Issue 8	Data returned is too short for any transaction	
	Description	Data corruption from iLO has occurred. The data received will be ignored.

Message number	Details	
	Recommended action	Reboot iLO by navigating to the Network Settings tab in the iLO Web interface and clicking Apply. If you continue to see this message, contact your HP field service engineer.
Issue 9	watchdog sees no dispatch threads	
	cpqci watchdog: close channel!	
	cpqci watchdog: reopen channel!	
	Description	These messages indicate that iLO was reset and that the service is trying to reopen communication.
	Recommended action	No action required, since this message is informational.
Issue 10	Problems setting up shared memory	
	Problems setting up semaphores	
	Problems setting up local semaphore	
	Problems setting up watchdog thread	
	Problems setting up IPMI channel	
	Problems setting up dispatch thread	
	Problems setting up secondary dispatch thread	
	Problems setting up dispatch threads	
	Did not receive initial handshake	
	Problems pushing IPMI traffic over channel!	
	Problems setting up dispatch data	
	Problems setting up stats data	
	Problems setting up dynamic mem allocator!	
	Problems setting up hash table!	
	Problems setting up communication with channel!	
	Problems setting up watchdog thread!	
	Description	These messages indicate a problem that occurred during initialization of the service. The main reasons for failure include:
		• Absence of the iLO Driver
		• iLO encountered problems and is in an undefined state
		• OS is running out of resources (for example, memory, threads, semaphores, etc.)
	Recommended action	Verify that the iLO Driver is installed and reboot the server.
Issue 11	start failed. started and stopped. -- failed.	
	Description	This message indicates that the service terminated itself because of problems.
	Recommended action	Install Version 1.1.0-2 of the service. Verify that the iLO Driver is installed and reboot the server. If problems persist, contact your HP field service engineer.

Message number	Details	
Issue 12	Dispatcher still sees %d clients…	
	Description	A client does not respond properly to impending shutdown. Consequently, the service waits for approximately 5 seconds, outputs this message, and exits.
	Recommended action	No action required since this message is informational. However, this message could also indicate that the HP ProLiant Rack Daemon (cmarackd) has died.
Issue 13	Checksum on SEEPROM %2.2x do not match for header (%2.2x)	
	Description	This message indicates that the EEPROMs in the infrastructure are corrupt.
	Recommended action	Contact your HP field service engineer for resolution.
Issue 14	Error: copy ipmb response with negative length %d Error: copy ipmb response with excessive length %d	
	Description	These messages indicate that a corrupt response from the infrastructure was received.
	Recommended action	Reboot the HP ProLiant Power Module.

Appendix B – Troubleshooting

This section describes common problems that might occur during installation and operation of the hpasm, hprsm, and cmanic packages.

Table 18 describes issues and workarounds for the hpasm package. Any problems reported to HP should include the following files:

- /var/log/messages
- /var/log/boot (for Red Hat Linux distributions)
- /var/log/warn (for SUSE LINUX distributions)
- /var/log/dmesg (for Red Hat Linux distributions)
- /opt/compaq/cpqhealth/cpqhealth_boot.log
- /opt/compaq/cpqhealth/cpqhealth_boot.log.old (if it exists)

Table 18. Known issues for hpasm

Issue number	Details	
Issue 1	Non-certified machines	
	Symptom	When the hpasm RPM file is installed, the following message displays: `hpasm:  This driver is not supported on this system` The driver is not inserted into the list of modules.
	Cause	The Health Monitor cannot be initialized at this time due to a conflict in ROM internal tables or the server is not supported. This driver is only supported on servers that have the ProLiant Advanced Server Management (ASM) ASIC (PCI identifier 0x0e11a0f0 or the Integrated Lights-Out Management ASIC (PCI identifier 0x0e11b203)). No other ProLiant servers are supported. Verify that the appropriate ASM ASIC is present. Use the following commands to perform the check: `cat /proc/bus/pci/devices	grep –I 0e11a0f0` `cat /proc/bus/pci/devices	grep –I 0e11b203` One of these commands should succeed and return information. Also, check to see if a later ROM version is available for this server.
	Workaround	There is no workaround, since this driver functions as designed.
Issue 2	The hpasm package custom build does not work	
	Symptom	The hpasm_rebuild script logs messages to the console and exits.
	Cause	You must execute the custom build script as user name "root." The RPM must be available to you and you should start the script with the version of the package that you installed (for example 6.30.0).
	Workaround	Install RPM and make sure it is available from your PATH variable.

Issue number	Details	
Issue 3	No console messages	
	Symptom	No console messages appear on the text screens (for instance, Ctrl+Alt+F1), but the error messages get logged properly in `/var/log/messages`. If you run KDE or Gnome, xterms will not show the console messages originating from the Health Monitor.
	Cause	The syslogd daemon is configured somewhat differently than other distributions; the system messages will not appear on the lower digit terminals (tty1-9).

	Workaround	If you do not want the message to be logged on the system, configure it differently by modifying `/etc/syslog.conf` in the following way:
		
		``
		# Log all kernel messages to the console.
		# Logging much else clutters up the screen.
		kern.* /dev/console
		# Log anything (except mail) of level info or higher.
		# Don't log private authentication messages!
		*.info;mail.none;news.none;authpriv.none
		/var/log/messages
		``
		
		After sending a HUP signal to syslogd process ID, you should see your kernel messages appearing on all consoles.
		
		`"kill -1 <pid of syslogd>"`

Issue 4	Failure in cpqimlview	
Option A	Symptom	When starting cpqimlview, the IML Viewer, you may see the following message: "ERROR: tclX not installed. tclX must be installed to use the IML viewer."
	Cause	The IML Viewer is a tcl-based application, so it will not compile or run if this package is not present.
	Workaround	Install the tclx RPM package (for example, tclx-8.2.0-32).
Option B	Symptom	When starting cpqimlview, the IML Viewer, you may see the following message: "Cannot open/dev/cdt. Wellness driver may not be installed." Once this error message appears, the IML is not functioning.
	Cause	The problem lies in the fact that the Health Monitor is not inserted on your system. A reason could be that your system is not certified for the current version of the hpasm package.
	Workaround	Try removing the hpasm package and reinstalling it. ``` rpm -e hpasm rpm -ivh hpasm-<version>.<distribution>.i386.rpm ``` This workaround will insert the Health Monitor (verify by typing lsmod). If the driver is not working, the system is not certified for the hpasm package.

Issue number	Details	
Issue 5	Superuser only	41

	Symptom	You will experience the following problems:
		
		 • Commands like insmod, modprobe, rmmod, or rpm are not available.
		 • The RPM install will fail because file permissions are being denied (see below).
		
		    "Failed to open //var/lib/rpm/packages.rpm
		    error: cannot open //var/lib/rpm/packages.rpm"
		
		 • The command cpqimlview is not known or fails because of file permissions.

	Cause	Preparing a driver install necessitates access to system administrator rights.
	Workaround	Be sure to log in as "root" before you attempt the driver install.
Issue 6	The agents do not seem to expose their data through SNMP; my management console does not see any status.	
	Symptom	Through SNMP browsers or other management software, the servers appear dead. No SNMP traffic is available through them.

	Cause	This can be caused by many things. Here is a checklist of the most common problems:
		
		 • SNMP is not running.
		 • The agents and/or drivers have not started properly (see Issue 7).
		 • The snmpd.conf file is misconfigured.
		   – rwcommunity is undefined for either localhost or the management console
		   – -community string mismatches the one from the management console
		   – trapsink or trapcommunity is undefined. Trapcommunity may be undefined for localhost.
		 • Firewalling software is enabled on the system and set up to block SNMP traffic.
		 • The cmaX extension is absent from the snmp stack.

	Workaround	Complete any of the following procedures to work around this issue: • Install and start snmp. • Install and start the ProLiant Management Agents. • A sample configuration file could look like the following: ``` rwcommunity public localhost rwcommunity public your.management.console trapcommunity public trapsink your.management.console public trapsink localhost public ``` The example above would assume that your community string is "public" and "your.management.console" is the domain name of your management console. • Disable the firewall (iptables/ipchains need to be turned off). • Install the SNMP stack from the Linux distribution CD.

Table 19 describes common problems that might occur during installation and operation of the Host OS Agent, the Standard Equipment Agent, the SCSI Agent, the System Health Agent, the Threshold Agent, and the Peer Agents. In most cases, a workaround is available.

Table 19. Known issues for agents

Issue	Details
Issue 1	Cannot manage server from Systems Insight Manager, grayed-out utilization button, or missing file system space used information in the mass storage window.
Workaround	To work around this issue, complete the following steps: 1. Check if the network is working by pinging the server from the system running Systems Insight Manager. 2. Make sure that Systems Insight Manager is using the correct community string, which is defined in the server's snmpd.conf files (refer to #man 5 snmp_config for default snmp.conf files). 3. Make sure that post-installation configurations have been performed properly, if needed. 4. Check the Host OS Agent status with the Linux command ps –ef | grep cmahostd. If the agent is not running, make sure that the Server Management Drivers and Agents script is installed properly under /etc/init.d (for Red Hat Linux, use `#/sbin/chkconfig –list cmafdtn` command). Start the Host OS Agent manually using the following command: `#/opt/ ompaq/foundation/etc/cmafdtn start cmahostd` If the Host OS Agent is running and not reporting data, or if it was correctly started but is no longer running, check the file /var/spool/ ompaq/cma.log for error messages. You must be logged in as "root" to access this file.
Issue 2	Grayed-out system board, expansion boards, or configuration buttons.
Workaround	Check the Standard Equipment Agent status with the Linux command ps –ef | grep cmastdeqd. If the agent is not running, make sure that Server Agents Start script is installed properly under /etc/init.d/ (for Red Hat Linux, use the #/sbin/chkconfig –list cmasvr command). Start the Standard Equipment Agent manually using the following command: `#/opt/compaq/server/etc/cmasvr start cmastdeqd` If the agent is running and not reporting data, or if the agent was correctly started but is no longer running, check the file /var/spool/compaq/cma.log for error messages. You must be logged in as "root" to access this file.
Issue 3	Missing SCSI drive information in the mass storage window.
Workaround	Check the SCSI Agent status with the 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/cma.log for error messages. You must be logged in as "root" to access this file.

Issue	Details	
Issue 4	Added SCSI devices do not appear.	
	Workaround	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 ProLiant Management Console. Once the hardware has been discovered, its status is checked each poll_time and reported to ProLiant Management Console when it has changed.
Issue 5	Missing or 0-value SCSI hard drive serial number or capacity.	
	Workaround	Most SCSI hard drives do not make this information available to the host when the drive media is 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 may be a delay of up to 32 times the poll_time of the cmascsid process before updated information is available to ProLiant Management Console.
Issue 6	Grayed-out button for a SCSI controller	
	Workaround	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 "cmascsid" may not be running. • The SCSI controller may have been disabled by the System Configuration Utility. • This may be an unsupported controller.
Issue 7	Missing or grayed-out storage controllers in the mass storage window.	
	Workaround	Check the Mass Storage Agent status with the Linux command ps -ef | grep cma. You should see entries for cmaidad, cmafca, cmascsid, cmaided. • 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.
Issue 8	Grayed-out recovery button in the device view window, grayed-out auto recovery button in the recovery window, or grayed-out environment button in the recovery window.	
	Workaround	To work around this issue, complete the following steps: 1. Check to make sure your system supports the System Health Agent features. These features are supported only on HP ProLiant servers. 2. Check the System Health Agent status with the Linux 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).

Issue	Details
Issue 9	Grayed-out Remote Insight button in the recovery window

Workaround	A grayed-out Remote Insight button can be caused by one of the following: • The Remote Insight Controller may not be configured properly. • The Remote Insight Driver may not be installed. • The Remote Insight Agent cmasm2d may not be running.

Issue	Details
Issue 10	Unable to change any values on the managed server or no SNMP traps/alarms are received

Workaround	To work around this issue, complete the following steps:

1. Make sure that the SNMP Agent, the Peer agent, and the agent processing the set are all running.
2. Check the agent command line arguments in the agent's start script files.
3. Verify that either the argument -s OK is present or that default set_state is OK for the agent. This process enables SNMP sets for this agent only.
4. Verify that the server SNMP community string defined in your snmpd.conf (using rwcommunity keyword) matches the community string defined at the management console.

   If you are using Systems Insight Manager, the community string can be set in Device Setup window. For more information, refer to the section on community strings in the Systems Insight Manager User Guide Help file.

   If you changed the snmpd.conf files, you need to refresh snmpd and agents with the following commands:

   ```
   #killall - HUP snmpd
   #/etc/init.d/hpasm restart agents
   ```
5. Test the traps by setting a threshold on an item that will cause a trap using the Set Threshold feature of Systems Insight Manager. Refer to the section "Set Threshold" in the Systems Insight Manager user guide for more information.

   If traps still do not function, have your Linux device send traps to itself. Run the Linux SNMP trap receiving utility snmptrapd –P.

   Next, generate a trap to localhost using the Linux snmptrap utility. The Linux command snmptrapd –P should display the trap. (See man snmptrapd and man snmptrap for more information).

Issue	Details
Issue 11	Unable to set thresholds on MIB items or no user-defined SNMP traps are received
Workaround	Check the Threshold Agent status with the Linux command: `ps -ef	grep cmathreshd`. If the agent is not running, make sure that the Server Management Drivers and Agents script is installed properly under /etc/init.d/ (for Red Hat Linux, use `#/sbin/chkconfig -list cmafdtn` command). Start the Threshold Agent using following command:  `#/opt/compaq/foundation/etc/cmafdtn start cmathreshd`  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/cma.log` for error messages. You must be logged in as root to access this file. Verify that the server SNMP community string defined in your `snmpd.conf` (using rwcommunity keyword) matches the community string defined at the management console. If you are using Systems Insight Manager, the community string can be set in the Device Setup Window. For more information, refer to the section on community strings in the Systems Insight Manager User Guide Help file. If sets still do not work, perform the following procedure: 1. Stop the Threshold Agent using the following command: `#/opt/compaq/foundation/etc/cmafdtn stop cmathreshd` 2. Delete previous alarm threshold files with the following command: `#/opt/compaq/foundation/etc/cmafdtn stop cmathreshd` 3. Start the Threshold Agent using the following command: `#/opt/compaq/foundation/etc/cmafdtn start cmathreshd`
Issue 12	Disabling SNMP sets for a specific agent
Workaround	Stop the agent associated with the desired MIB. Change the agent command line argument set switch to -s NOT_OK in the /etc/init.d/cma* file. This disables SNMP sets for this agent only. Restart the agent.
Issue 13	Disabling SNMP traps for a specific agent
Workaround	Stop the agent. Change the agent command line argument trap switch to -t NOT_OK in the /etc/init.d/cma* file. This disables SNMP traps for this agent only. Restart the stopped agent.
Issue 14	Disabling remote reboot
Workaround	Stop the Server Standard Equipment Agent using following command: `#/opt/compaq/server/etc/cmasvr stop cmastdeqd` Edit `/opt/compaq/server/etc/cmastdeqd` and change the cmastdeqd agent command line reboot switch to -r NOT_OK. This disables SNMP reboots for this device only. Restart Standard Equipment agent.
Issue 15	Peer Agents will not run

Workaround	Check the `/var/spool/compaq/cma.log` file for messages. If it is caused by no running snmpd, then configure snmpd to start automatically during boot. If you changed the `snmpd.conf` files, you must refresh snmpd and agents with following commands:
	
	`#killall -HUP snmpd`
	`#/etc/init.d/hpasm restart agents`

Appendix C – hpasm and hprsm command lines and arguments

Table 20 lists the command lines and Table 21 lists the command arguments for hpasm and hprsm.

Table 20. Command lines for hpasm and hprsm

Component	Description	Command
hpasm Foundation package, collectively started by /opt/compaq/foundation/etc/cmafdtn {start | stop | restart}		
Cmahostd	Host daemon to collect data about installed software, firmware, and agent conditions.	/opt/compaq/foundation/etc/cmahostd
Cmapeerd	Host daemon collected data make available to SNMP requesters	/opt/compaq/foundation/etc/cmapeerd
Cmathreshd	Daemon to monitor MIB items to exceed a certain threshold.	/opt/compaq/foundation/etc/cmathreshd
hpasm Server package, collectively started by /opt/compaq/server/etc/cmaserv {start | stop}		
Cmahealthd	Host daemon to collect temperature	/opt/compaq/server/etc/cmahealthd
Cmastdeqd	Host daemon to collect PCI/EISA slot information	/opt/compaq/server/etc/cmastdeqd
Cmaperfd	Daemon to collect performance data for CPU	/opt/compaq/server/etc/cmaperfd
hpasm Storage package, collectively started by /opt/compaq/storage/etc/cmastor		
Cmaidad	Agent to collect data from cciss/cpqarray drivers.	/opt/compaq/storage/etc/cmaidad
Cmaided	Agent to collect data from IDE devices.	/opt/compaq/storage/etc/cmaided
Cmafcad	Agent to collect data from the cpqfc driver.	/opt/compaq/storage/etc/cmafcad
Cmascsid	Agent to collect data from SCSI storage devices.	/opt/compaq/storage/etc/cmascsid
hprsm package		
cmasm2d	Agent to collect data from iLO/RILOE.	/opt/compaq/server/etc/cmasm2d
Cmarackd	Agent to collect data from the ICE infrastructure.	/opt/compaq/server/etc/cmarackd

Note: All agents support -p, -s, -t as startup parameters.

Note: Each agent has an associated run level script which is located in /opt/compaq/<agent group>/etc/<agent name>. All important settings such as poll time arguments are contained in these individual scripts.

Table 21. Command arguments for hpasm and hprsm

Command line argument	Description
-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.

Call to action

Send comments about this paper to TechCom@HP.com.