HP Operations Smart Plug-in for Systems Infrastructure

for HP Operations Manager for Windows®, HP-UX, Linux, and Solaris

Software Version: 2.01

User Guide

Document Release Date: February 2012
Software Release Date: February 2012

Legal Notices

Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

Copyright Notice

Trademark Notices

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

Adobe® and Acrobat® are trademarks of Adobe Systems Incorporated.

Java is a registered trademark of Oracle and/or its affiliates.

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

http://h20230.www2.hp.com/selfsolve/manuals

This site requires that you register for an HP Passport and sign in. To register for an HP Passport ID, go to:

http://h20229.www2.hp.com/passport-registration.html

Or click the **New users - please register** link on the HP Passport login page.

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HP sales representative for details.

Support

Visit the HP Software Support Online web site at:

www.hp.com/go/hpsoftwaresupport

This web site provides contact information and details about the products, services, and support that HP Software offers.

HP Software online support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the support web site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract. To register for an HP Passport user ID, go to:

http://h20229.www2.hp.com/passport-registration.html

To find more information about access levels, go to:

http://h20230.www2.hp.com/new_access_levels.jsp

Contents

1 Conventions Used in this Document 7

2 Introduction 9

3 Systems Infrastructure SPI Components 11

Map View on HPOM for Windows 11

Map View on HPOM for UNIX 12

Tools 14

Policies 14

Graphs 15

Reports 15

4 Systems Infrastructure SPI Policies and Tools 17

Systems Infrastructure SPI Policies 17

Tracing 17

Discovery Policy 18

Restricting Discovery 18

Availability Policies 21

Policies Monitoring Process and Service 21

Hardware Monitoring Policies 26

Capacity Policies 61

Log Monitoring Policies 74

Linux System Services Logfile Policies 74

Windows System Services Logfile Policies 75

AIX System Logfile Monitoring Policies 77

Performance Policies 78

Security Policies 102

Deploying SI SPI Policies from HPOM for Windows Management Server 103

Deploying SI SPI Policies from HPOM for UNIX Management Server 104

Systems Infrastructure SPI Tool 105

Users Last Login Tool 105

5 Systems Infrastructure SPI Reports and Graphs 107

Systems Infrastructure SPI Reports 107

Systems Infrastructure SPI Graphs 109

6 Troubleshooting 113

1 Conventions Used in this Document

The following conventions are used in this document.

Convention	Description
HPOM for UNIX	HPOM for UNIX is used in the document to imply HPOM on HP-UX, Linux, and Solaris. Wherever required, distinction is made for a specific operating system as: • HPOM on HP-UX • HPOM on Linux • HPOM on Solaris
Infrastructure SPIs	HP Operations Smart Plug-ins for Infrastructure. The software suite includes three Smart Plug-ins: • HP Operations Smart Plug-in for Systems Infrastructure • HP Operations Smart Plug-in for Virtualization Infrastructure • HP Operations Smart Plug-in for Cluster Infrastructure
SI SPI	HP Operations Smart Plug-in for Systems Infrastructure
VI SPI	HP Operations Smart Plug-in for Virtualization Infrastructure
CI SPI	HP Operations Smart Plug-in for Cluster Infrastructure
`%OvDataDir%`	The data directory variable on Windows management server and managed nodes. This variable is set by the installer. You can reset the path based on your requirements. The default value is `C:\Documents and Settings\All Users\Application Data\HP\HP BTO Software`.

Convention	Description
`$OvDataDir`	The data directory variable on HPOM for UNIX management server and UNIX managed nodes. You must manually create this variable. The data directory on all UNIX nodes and servers is as follows: • HP-UX (nodes and server): `/var/opt/OV` • Linux (nodes and server): `/var/opt/OV` • Solaris (nodes and server): `/var/opt/OV` • AIX (nodes): `/var/opt/OV` You cannot modify these values.
`%OvInstallDir%`	The installation directory variable on Windows management server and managed nodes. This variable is set by the installer. You can reset the path based on your requirements. The default value is `C:\Program Files\HP\HP BTO Software`.
`$OvInstalDir`	The install directory variable on HPOM for UNIX management server and UNIX managed nodes. You must manually create this variable. The install directory on all UNIX nodes and servers is as follows: • HP-UX (nodes and server): `/opt/OV` • Linux (nodes and server): `/opt/OV` • Solaris (nodes and server): `/opt/OV` • AIX (nodes): `/usr/lpp/OV` You cannot modify these values.

2 Introduction

Systems infrastructure is the foundation or base infrastructure that is integral to an enterprise. It includes CPU, operating system, disk, memory, and network resource that need to be continuously monitored to ensure availability, performance, security, and smooth functioning of underlying physical systems. Monitoring systems infrastructure enables you to achieve greater efficiency and productivity. It also helps to correlate, identify, and correct root cause of infrastructure faults and performance degradations.

The Systems Infrastructure Smart Plug-ins (SI SPI) monitors the system infrastructure for the Microsoft Windows, Linux, Oracle Solaris, IBM AIX, and HP-UX systems. The SI SPI helps to analyze the system performance based on monitoring aspects such as capacity, availability, and utilization.

The SI SPI is a part of the HP Operations Smart Plug-ins for Infrastructure suite (Infrastructure SPIs). The other components in the suite include the Virtualization Infrastructure Smart Plug-ins (VI SPI), the Cluster Infrastructure Smart Plug-ins (CI SPI), the Report pack, and the Graph pack. Installation of SI SPI is mandatory while installing other components from the Infrastructure SPIs media.

The Report Pack is not available on HPOM for Windows 9.00 because HP Reporter does not support 64-bit installation.

The SI SPI integrates with other HP software products such as the HP Operations Manager (HPOM), HP Performance Manager, HP Performance Agent, and Embedded Performance Component (EPC) of HP Operations agent. The integration provides policies, tools, and the additional perspective of Service Views.

For information about the operating system versions supported by the SI SPI, see the *HP Operations Smart Plug-in for Systems Infrastructure Release Notes*.

3 Systems Infrastructure SPI Components

The SI SPI provides preconfigured policies and tools for monitoring the operations, availability, and performance of the managed nodes. These policies and tools, along with discovery, enable you to quickly gain control of the essential elements of your IT infrastructure.

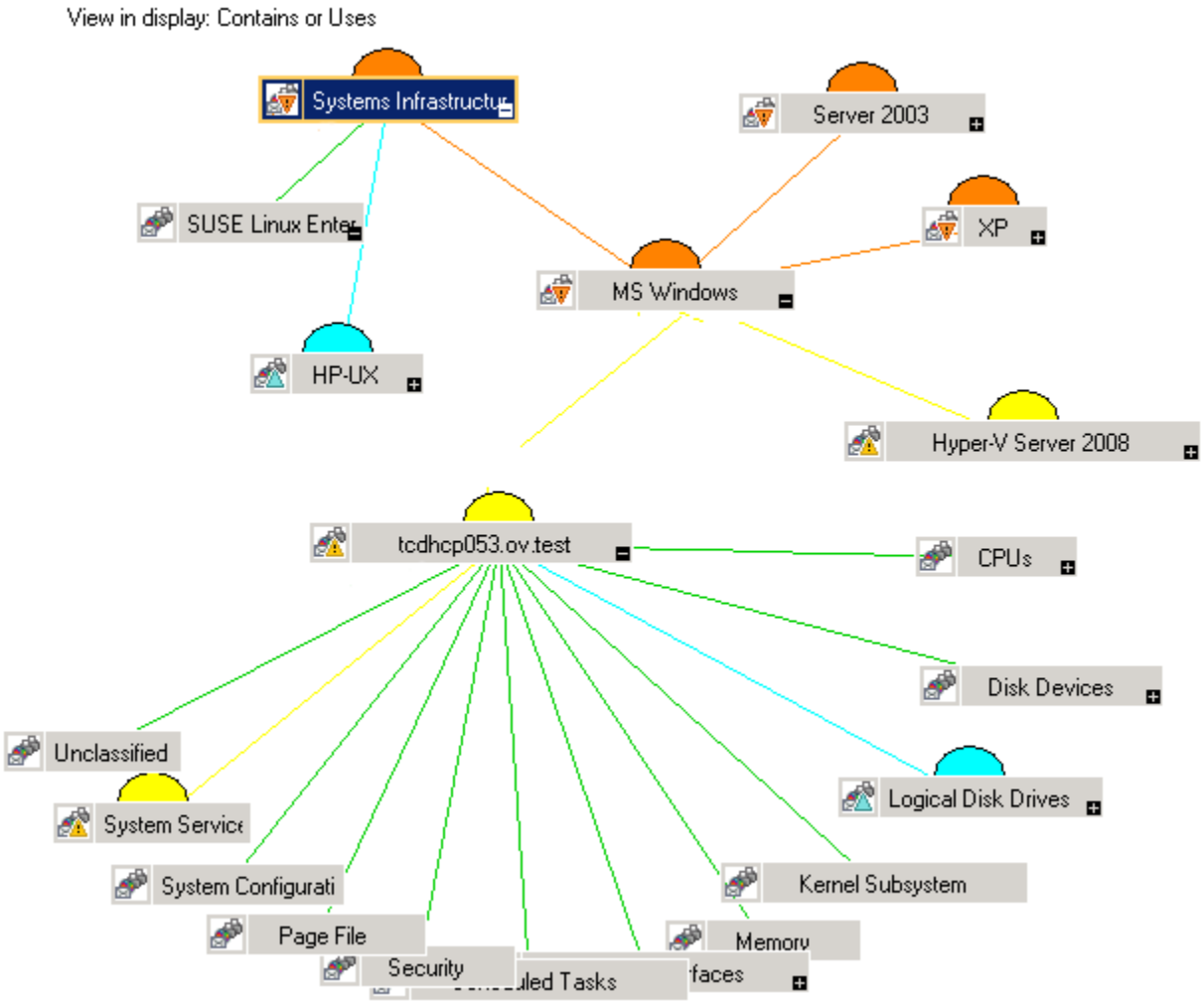
Map View on HPOM for Windows

Before the discovery policy identifies the node, read the *Starting the SI SPI* section of the *HP Operations Infrastructure Smart Plug-ins Installation Guide*. This section describes about the prerequisites for deploying the SI SPI policies.

After you add a node to the HPOM console, the SI SPI service discovery policy is automatically deployed to the nodes and adds discovered information to the HPOM Services area. This information is used to populate the SI SPI map view for nodes and services.

The map view displays the real-time status of your infrastructure environment. To view, select **Services** from the HPOM console, and click **Systems Infrastructure**. Map view graphically represents the structural view of your entire service or node hierarchy in the infrastructure environment including any subsystems or subservices.

Figure 1 Map view on HPOM for Windows



The icons and lines in your map are color-coded to indicate the severity levels of items in the map and to show status propagation. Use the map view to drill down to the level in your node or service hierarchy where a problem is occurring.

The graphical representation of discovered elements in the service views enables speedy diagnosis of problems.

- To view the root cause of any problem indicated in your message browser, click **View** → **Root Cause**.
- To display the services and system components affected by a problem, click **View** → **Impacted**.

Map View on HPOM for UNIX

Before the discovery policy identifies the node, read the *Starting the SI SPI* section of the *HP Operations Infrastructure Smart Plug-ins Installation Guide*. This section describes about the prerequisites for deploying the SI SPI policies.

The map view displays the real-time status of your infrastructure environment. To ensure that the operator can view the service map in the HPOM for HP-UX, Solaris, and Linux Operational interface, run the following commands on the management server:

```
opcservice -assign <operator name> SystemServices
```

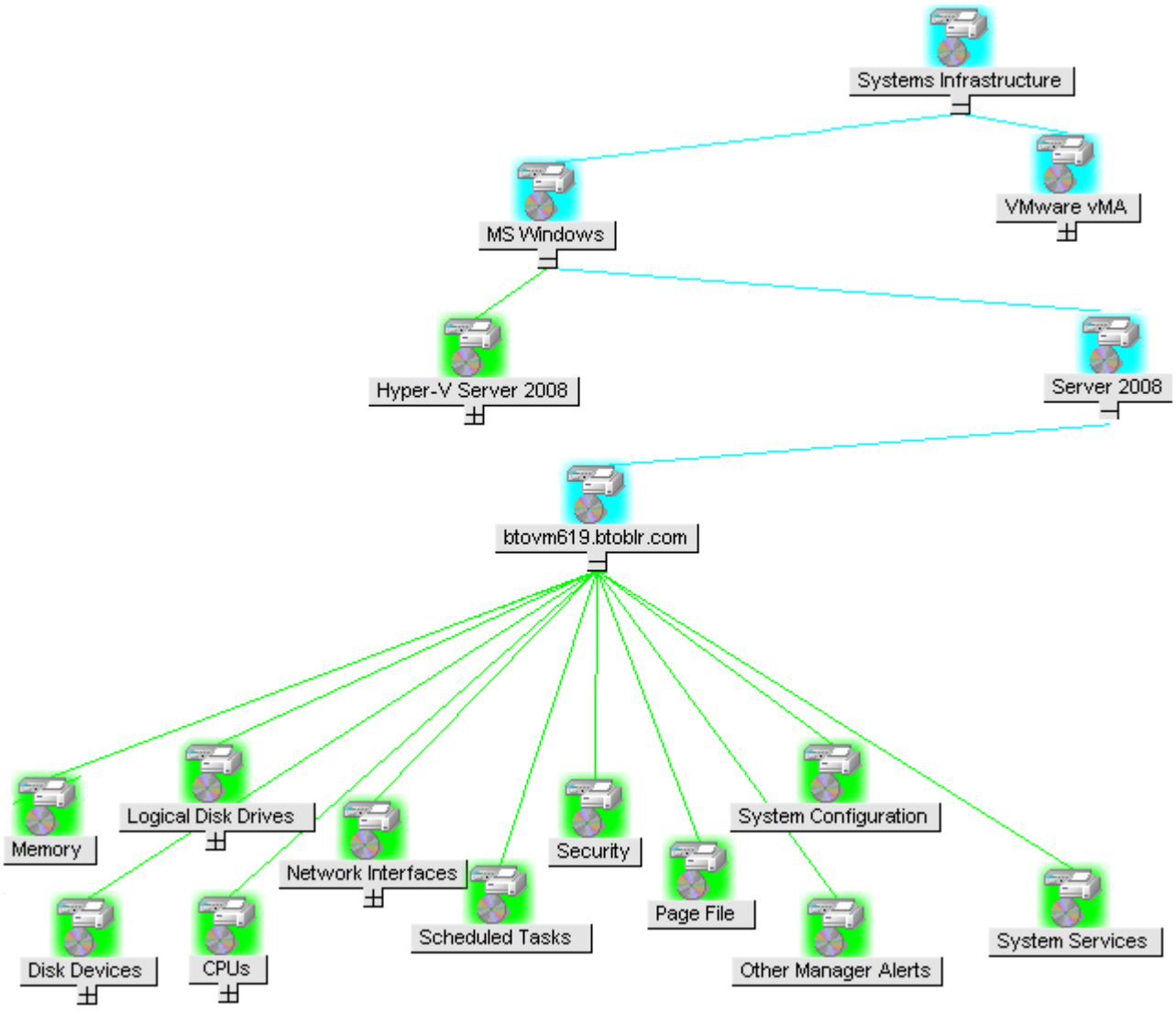
In this instance, *<operator name>* is the operator (for example, opc_adm or opc_op) to which you want to assign the service.

The SI SPI service discovery policy does not automatically deploy policies to the nodes. You can manually deploy these.

To see the map view, follow these steps:

1. Launch the HPOM Operational interface.
2. Log on using your user name and password.
3. Select **Services** → **Systems Infrastructure** → **Show Graph**, to view the map view.

Figure 2 Map view on HPOM for UNIX/ Linux/ Solaris



The map view graphically represents the structural view of your entire service or node hierarchy in the infrastructure environment including any subsystems or subservices.

Tools

The SI SPI tools display data collected for a particular managed node. For information about the tools provided by SI SPI, see Systems Infrastructure SPI Tool.

Policies

On HPOM for Windows, several default policies are automatically deployed on the supported managed nodes during installation. These can be used as-is to begin receiving system infrastructure related data and messages from the environment. You can choose to turn off automatic deployment of policies when services are discovered. In addition, you can modify and save preconfigured policies with new names to create custom policies for your own specialized purposes.

For information on deploying policies from the management server, see Deploying SI SPI Policies from HPOM for Windows Management Server.

For HPOM for HP-UX, Linux, or Solaris, the SI SPI service discovery policy does not automatically deploy policies to the nodes. You can manually deploy them.

For information on deploying policies from the management server, see Deploying SI SPI Policies from HPOM for UNIX Management Server on page 104.

The SI SPI policies begin with SI for easy identification and modification. The policy types are as follows:

- **Service/Process Monitoring policies** provide a means for monitoring system services and processes.
- **Logfile Entry policies** capture status or error messages generated by the system nodes.
- **Measurement Threshold policies** define conditions for each metric so that the collected metric values can be interpreted and alerts or messages can be displayed in the message browser. Each measurement threshold policy compares the actual metric value against the specified or auto threshold. A mismatch between the threshold and the actual metric value generates a message and instruction text that helps you resolve a situation.
- **Scheduled Task policies** determine what metric values to collect and when to start collecting metric. The policies define the collection interval. The collection interval indicates how often data is collected for a specific group. The scheduled task policy has two functions: to run the collector or analyzer at each collection interval on a node and to collect data for all metrics listed within the polices' **Command** text box.
- **Service Discovery policy** discovers individual system nodes instances and builds a map view for all SI SPI discovered instances.

For more information about the policies provided by SI SPI, see Systems Infrastructure SPI Policies.

Graphs

The SI SPI enables you to view and trace out the root cause of any discrepancy in the normal behavior of an element being monitored. HPOM is integrated with HP Performance Manager, a web-based analysis tool that helps you evaluate system performance, look at usage trends, and compare performance between systems. Using HP Performance Manager you can see any of the following:

- Graphs such as line, bar, or area
- Tables for data such as process details
- Baseline graphs
- Dynamic graphs in Java format that allow you to turn off display of individual metrics or hover over a point on a graph and see the values displayed

You can view the data represented graphically for quick and easy analysis of a serious or critical error message reported. For more information about the graphs provided by SI SPI, see Systems Infrastructure SPI Graphs.

Reports

You can integrate the SI SPI by installing the HP Reporter to generate web-based reports on metric data.

If HP Reporter is installed on the HPOM management server for Windows, you can view reports from the console. To view a report, expand **Reports** in the console tree, and then double-click individual reports.

If HP Reporter is installed on a separate system connected to the HPOM management server (for Windows, UNIX, Linux, or Solaris operating system), you can view the reports on HP Reporter system. For more information on integration of HP Reporter with HPOM, see *HP Reporter Installation and Special Configuration Guide*.

For information about the reports provided by SI SPI, see Systems Infrastructure SPI Reports.

4 Systems Infrastructure SPI Policies and Tools

The SI SPI provides a wide range of policies and tools to help manage your infrastructure. The policies help you monitor systems and the tools display data collected for these systems.

Systems Infrastructure SPI Policies

A policy is a rule or set of rules that help you automate monitoring. The SI SPI policies help you monitor systems in Windows, Linux, Solaris, AIX, and HP-UX environments. Most policies are common to all environments, but there are some policies that are relevant only to a particular environment and must be deployed only on the relevant platform. Deployment of policy to an unsupported platform may lead to unexpected behavior or cause the policy to fail.

The folder Infrastructure Management group contains a subgroup arranged according to language. For example, the subgroup for English policies is **en**, for Japanese language is **ja**, and for Simplified Chinese language is **zh**.

In the console tree, the SI SPI policies are listed at the following location:

Policy management → **Policy groups** → **Infrastructure Management** → ***<language>*** → **Systems Infrastructure**.

For information on deploying policies from the management server, see Deploying SI SPI Policies from HPOM for Windows Management Server.

For HPOM for UNIX (HP-UX, Linux, or Solaris), the policy group on the console or Administration interface is:

Policy Bank → **Infrastructure Management** → ***<language>*** → **Systems Infrastructure**

For information on deploying policies from the management server, see Deploying SI SPI Policies from HPOM for UNIX Management Server.

Tracing

The policies for monitoring capacity and performance contain a script parameter for tracing: *Debug* or *DebugLevel*. Using this parameter you can enable tracing. You can assign any of the following values:

- Debug=0, no trace messages will be sent.
- Debug=1, trace messages will be sent to the console.
- Debug=2, trace messages will be logged in a trace file on the managed node. The trace file location on managed node is `$OvDataDir/Log`.

To view the script parameters:

1. Log on as Root user.
2. Double-click the desired policy. The policy window opens.

3 Select the Script-Parameters tab. The script parameters for that policy are listed.

You can also modify the parameter value based on your requirements. For information on how to edit script parameter values, see *HP Operations Smart Plug-in for Infrastructure Concepts Guide*.

Discovery Policy

The **SI-SystemDiscovery** policy gathers service information from the managed nodes such as hardware resources, operating system attributes, and applications.

Whenever you add a node to the appropriate node group in the HPOM console, the discovery modules deployed along with the SI-SystemDiscovery policy run service discovery on the node. These service discovery modules gather and send back the information to HPOM in the form of XML snippets. These snippets generate a service tree that provides a snapshot of services deployed on managed nodes at the time the SI SPI discovery process runs. After the first deployment, the autodiscovery policy is set to run periodically. Each time the discovery agent runs, it compares the service information retrieved with the results of the previous run. If the discovery agent finds any changes or additions to the services running on the managed node since the previous run, it sends a message to the HPOM management server, which updates the service view with the changes. The default policy group for this policy is:

Infrastructure Management → *<language>* → Systems Infrastructure → AutoDiscovery

Restricting Discovery

The **SI-ConfigureDiscovery** policy is a ConfigFile policy that enables you to include or exclude the discovery of specified resources on a virtual machine.

The SI-SystemDiscovery policy by default discovers all the services and resources running on a node. You may however, not want to see all the resources in the service map.

To restrict discovery, you must deploy the SI-ConfigureDiscovery policy before running the discovery policy.

The SI-ConfigureDiscovery policy has the configuration switch to include or exclude resources on all for virtual machines across all the virtualization technologies that Infrastructure SPI supports.

After you deploy this policy to a node, it saves a configuration file `SIDiscovery.cfg` in the following folder:

UNIX: `/var/opt/OV/conf/sispi/configuration`

Windows:`%Ovdatadir%\Data\conf\sispi\configuration`

If the `SIDiscovery.cfg` file is not present in the `/var/opt/OV/conf/sispi/configuration/` folder, SI discovery will by default discover all the resources.

The `SIDiscovery.cfg` file contains the following information:

```
#To include or exclude a particular resource in SI discovery, add the
particular value under the respective Resource.
#The resources which can be restricted or expanded for being discovered are
mentioned below:
#
#File System
#Disk
#Network
```

```
#CPU
#
#The values which can be part of the INCLUDE and EXCLUDE parameters with
respect to each of the resources can be as follows:
#
#FS include or exclude parameters should contain File system path(In
general FS_DIRNAME value)
#Example:
#FS_INCLUDE:     /etc*Or
#FS_EXCLUDE:     /zones*
#
#DSK include or exclude parameters should contain name of the Disk
device(In general BYDSK_DEVNAME value)
#Example:
#DSK_INCLUDE:vdc0Or
#DSK_EXCLUDE:vdc1
#
#NET include or exclude parameters should contain Network Interface
name(In general BYNETIF_NAME value)
#Example:
#NET_INCLUDE:lo0Or
#NET_EXCLUDE:vnet0
#
#CPU include or exclude parameters should contain ID number of the CPU (In
general BYCPU_ID value)
#Example:
#CPU_INCLUDE:0,1Or
#CPU_EXCLUDE:2,3
#
#Multiple entries should be separate with comma -
#For example if one wants to exclude 2 of the File Systems, then the
following entry should configured:
#FS_INCLUDE:/zones*,/etc*
#
#Resource Name and value should be separated with ":" -
#For example if one wants to add FS_EXCLUDE, then the following entry
should be configured separated with ":"
#FS_EXCLUDE:     /zones*
#
#Different resources(_INCLUDE and _EXCLUDE) should be separated with
"===". As in the below case, FS, DSK, NET and CPU are
#separated with "==="
##########################################################################
#########################################################
===
FS_INCLUDE:
FS_EXCLUDE:     /zones*
===
DSK_INCLUDE:
DSK_EXCLUDE:
===
NET_INCLUDE:
NET_EXCLUDE:
===
CPU_INCLUDE:
```

CPU_EXCLUDE:

To include or exclude resources from being discovered, edit the `SIDiscovery.cfg` file as per the instructions provided in the file.

If you provide specific resource names under the INCLUDE parameter, SI discovery will discover only those resources and show them in the service map. If you provide specific resource names under the EXCLUDE parameter, SI discovery *will not* discover those resources and will not show them in the service map.

You can either specify the entire resource name or use the wild card (*****).

You can set only one parameter. It can be either EXCLUDE or INCLUDE. If you set values for both the parameters or do not set values for either of the parameters, the SI discovery policy discovers all the resources by default.

If you set wrong instance values for the INCLUDE parameter, SI discovery will not discover that specific resource instance and send the following alert message with severity Warning to the HPOM console:

Improper usage as _INLUCDE parameter is not having the correct value.

However, if you set wrong instance values for the EXCLUDE parameter, SI discovery will discover that resource instance.

The **SI-SystemDiscovery** policy sends the following alert message with severity Warning to the HPOM console if it fails to open or read the `SIDiscovery.cfg` file:

Improper usage as both _INCLUDE and _EXCLUDE are configured.

Example

On an Oracle Solaris container with three non-global zones named email server, webserver1 and webserver2, there may be several file systems like:

```
/etc/svc/volatile
/tmp
/var/run
/zones/emailserver/root/etc/svc/volatile
/zones/emailserver/root/tmp
/zones/emailserver/root/var/run
/zones/webserver1/root/etc/svc/volatile
/zones/webserver1/root/tmp
/zones/webserver1/root/var/run
/zones/webserver2/root/etc/svc/volatile
/zones/webserver2/root/tmp
/zones/webserver2/root/var/run
```

- If you want to discover only specific file systems, modify the `SIDiscovery.cfg` file by entering *one* of the following values for the INCLUDE parameter:
  - FS_INCLUDE: **/zones/webserver2***
  - FS_INCLUDE: **/zones/webserver2/root/etc/svc/volatile**
- If you do not want to discover specific file systems, modify the `SIDiscovery.cfg` file by entering *one* of the following values for the EXCLUDE parameter:
  - FS_EXCLUDE: **/zones/emailserver***
  - FS_EXCLUDE: **/zones/emailserverroot/tmp**

Availability Policies

Availability monitoring helps to ensure adequate availability of resources. It is important to identify unacceptable resource availability levels. The current load on IT infrastructure is computed and compared with threshold levels to see if there is any shortfall in resource availability.

As the usage of IT resources changes, and functionality evolves, the amount of disk space, processing power, memory, and other parameters also change. It is essential to understand the current demands, and how they change over time. Monitoring these aspects over a period of time is beneficial in understanding the impact on IT resource utilization.

A server role describes the primary function of the server such as fax server, email server, and so on. A system can have one single server role or multiple server roles installed. Each server role can include one or more role services described as sub-elements of a role. The availability policies monitor the availability of role services on the managed nodes.

The preconfigured availability policies are automatically installed if the role services managed by these policies are discovered on the selected node by the SI SPI. The default policy group for these policies is:

Infrastructure Management → *<language>* → Systems Infrastructure → Availability

The availability policies monitor the availability of the processes and services on the Linux, Windows, Solaris, AIX, and HP-UX managed nodes. The policies send a message to HPOM when the process is unavailable or when the status of the service changes (for example, from running to stopped or disabled). You can define the status to monitor and the action to take if the status changes.

The availability policies are grouped based on the server roles and sub grouped based on the operating system. You can select the required policy according to the operating system on the managed node.

Policies Monitoring Process and Service

The default policy groups for these policies are:

- **Infrastructure Management → *<language>* → Systems Infrastructure → Availability → *<process/ service>* → *<os>***
- **Infrastructure Management → *<language>* → Systems Infrastructure → Policies grouped by vendor → *<os>* - Advanced**

Here **<os>** denotes the operating system AIX, HP-UX, RHEL, SLES, Windows, or Solaris. The following tables list the processes and services along with the corresponding monitor policies that are provided on the supported platforms.

Infrastructure SPIs provide availability policies for process monitoring on the Solaris zones. Solaris machines have global and local zones (or containers). The policies monitor availability of Solaris processes and send out an alert message to HPOM when not available.

Table 1 Monitoring Policies for AIX

Process/ Service Name	Monitoring Policy
DHCP Server	SI-AIXDHCPProcessMonitor
DNS Server	SI-AIXNamedProcessMonitor
Email Service	SI-AIXSendmailProcessMonitor

Table 1 Monitoring Policies for AIX

Process/ Service Name	Monitoring Policy
Fax Service	-
File Services	SI-AIXNfsServerProcessMonitor
Firewall Service	-
Internet Service	SI-AIXInetdProcessMonitor
Network Services	-
Print Service	• SI-AIXQdaemonProcessMonitor • SI-AIXLpdProcessMonitor
RPC Service	SI-AIXPortmapProcessMonitor
Scheduled Job Service	SI-AIXCronProcessMonitor
Secure Login Service	SI-OpenSshdProcessMonitor[1]
SNMP Service	SI-UnixSnmpdProcessMonitor
System Logger	SI-AIXSyslogProcessMonitor
Terminal Services	-
Web Server	SI-AIXWebserverProcessMonitor

Table 2 Monitoring Policies for HP-UX

Process/ Service Name	Monitoring Policy
DHCP Server	SI-HPUXBootpdProcessMonitor
DNS Server	SI-HPUXNamedProcessMonitor
Email Service	SI-HPUXSendmailProcessMonitor
Fax Service	-
File Services	SI-HPUXNfsServerProcessMonitor
Firewall Service	-
Internet Service	SI-HPUXInetdProcessMonitor
Network Services	-
Print Service	SI-HPUXLpschedProcessMonitor
RPC Service	-
Scheduled Job Service	SI-HPUXCronProcessMonitor
Secure Login Service	• SI-HPUXSshdProcessMonitor • SI-OpenSshdProcessMonitor[1]
SNMP Service	SI-UnixSnmpdProcessMonitor

Table 2 Monitoring Policies for HP-UX

Process/ Service Name	Monitoring Policy
System Logger	SI-HPUXSyslogProcessMonitor
Terminal Services	-
Web Server	SI-HPUXWebserverProcessMonitor

Table 3 Monitoring Policies for RHEL

Process/ Service Name	Monitoring Policy
DHCP Server	SI-LinuxDHCPProcessMonitor
DNS Server	SI-LinuxNamedProcessMonitor
Email Service	SI-LinuxSendmailProcessMonitor
Fax Service	-
File Services	• SI-LinuxNfsServerProcessMonitor • SI-LinuxSmbServerProcessMonitor
Firewall Service	-
Internet Service	SI-LinuxXinetdProcessMonitor
Network Services	-
Print Service	SI-LinuxCupsProcessMonitor
RPC Service	-
Scheduled Job Service	SI-RHELCronProcessMonitor
Secure Login Service	• SI-LinuxSshdProcessMonitor • SI-OpenSshdProcessMonitor[1]
SNMP Service	SI-UnixSnmpdProcessMonitor
System Logger	SI-RHELSyslogProcessMonitor
Terminal Services	-
Web Server	SI-LinuxWebserverProcessMonitor

Table 4 Monitoring Policies for SLES

Process/ Service Name	SLES
DHCP Server	SI-LinuxDHCPProcessMonitor
DNS Server	SI-LinuxNamedProcessMonitor
Email Service	SI-LinuxSendmailProcessMonitor
Fax Service	-

Table 4 Monitoring Policies for SLES

Process/ Service Name	SLES
File Services	• SI-LinuxNfsServerProcessMonitor • SI-LinuxSmbServerProcessMonitor
Firewall Service	-
Internet Service	SI-LinuxXinetdProcessMonitor
Network Services	-
Print Service	SI-LinuxCupsProcessMonitor
RPC Service	-
Scheduled Job Service	SI-SLESCronProcessMonitor
Secure Login Service	• SI-LinuxSshdProcessMonitor • SI-OpenSshdProcessMonitor[1]
SNMP Service	SI-UnixSnmpdProcessMonitor
System Logger	SI-SLESSyslogProcessMonitor
Terminal Services	-
Web Server	SI-LinuxWebserverProcessMonitor

Table 5 Monitoring Policies for Solaris

Process/ Service Name	Monitoring Policy
DHCP Server	SI-SunSolarisDHCPProcessMonitor
DNS Server	SI-SunSolarisNamedProcessMonitor
Email Service	SI-SunSolarisSendmailProcessMonitor
Fax Service	-
File Services	SI-SunSolarisNfsServerProcessMonitor
Firewall Service	-
Internet Service	SI-SunSolarisInetdProcessMonitor
Network Services	-
Print Service	SI-SunSolarisLpdProcessMonitor
RPC Service	-
Scheduled Job Service	SI-SunSolarisCronProcessMonitor
Secure Login Service	• SI-SunSolarisSshdProcessMonitor • SI-OpenSshdProcessMonitor[1]
SNMP Service	SI-UnixSnmpdProcessMonitor

Table 5 Monitoring Policies for Solaris

Process/ Service Name	Monitoring Policy
System Logger	SI-SunSolarisSyslogProcessMonitor
Terminal Services	-
Web Server	SI-SunSolarisWebserverProcessMonitor

Table 6 Monitoring Policies for Windows

Process/ Service Name	Monitoring Policy
DHCP Server	SI-MSWindowsDHCPServerRoleMonitor
DNS Server	SI-MSWindowsDNSServerRoleMonitor
Email Service	-
Fax Service	SI-MSWindowsFaxServerRoleMonitor
File Services	• SI-MSWindowsWin2k3FileServicesRoleMonitor • SI-MSWindowsDFSRoleMonitor • SI-MSWindowsFileServerRoleMonitor • SI-MSWindowsNFSRoleMonitor
Firewall Service	SI-MSWindowsFirewallRoleMonitor
Internet Service	-
Network Services	• SI-MSWindowsRRAServicesRoleMonitor • SI-MSWindowsNetworkPolicyServerRoleMonitor
Print Service	SI-MSWindowsPrintServiceRoleMonitor
RPC Service	SI-MSWindowsRpcRoleMonitor
Scheduled Job Service	SI-MSWindowsTaskSchedulerRoleMonitor
Secure Login Service	SI-OpenSshdProcessMonitor[1]
SNMP Service	SI-MSWindowsSnmpProcessMonitor
System Logger	SI-MSWindowsEventLogRoleMonitor
Terminal Services	• SI-MSWindowsTSWebAccessRoleMonitor • SI-MSWindowsTSGatewayRoleMonitor • SI-MSWindowsTerminalServerRoleMonitor • SI-MSWindowsTSLicensingRoleMonitor
Web Server	SI-MSWindowsWebServerRoleMonitor

[1]The policy is supported on AIX, HP-UX, Linux, MS windows, and Solaris operating systems. Make sure you install *openssh* packages before deploying this policy on any of the supported platforms.

When the current process monitoring policy for Solaris is deployed on a global zone, the SI SPI will monitor all processes running on global zone and non-global zone without differentiating the zone that the process belongs to. Hence, to monitor processes running on global zone, the threshold level must be set to include the non-global processes.

For example: If there are 'x' non-global zone processes, that are part of a global zone, then the threshold level must be set to include all the processes of global and non-global zones; x+1

You will get duplicate alerts, if you deploy the same policy on a global and non-global zone, where the non-global zone is part of the global zone.

Policies not supported on non-global zones

- SI-CPUSpikeCheck
- SI-PerNetifInbyteBaseline-AT
- SI-PerNetifOutbyteBaseline-AT
- SI-PerDiskAvgServiceTime-AT
- SI-PerDiskUtilization-AT

Hardware Monitoring Policies

System Infrastructure SPI 2.00 provides policies that enable you to monitor the health and status of your HP ProLiant servers. These policies monitor SNMP traps generated by the SIM Agent and send alert messages to the HPOM console. All these policies are of the type SNMP Interceptor.

The default policy group for these policies is:

Infrastructure Management → <*language*> → **Systems Infrastructure** → **Hardware** → **HP ProLiant**.

Required Configuration:

- Ensure that the SNMP service is up and running.
- To enable hardware monitoring, open the `xpl config` file on the node and add the following line under the `eaagt` namespace:
  - If you are using HP Operations agent 8.60, add:

    ```
    [eaagt]
    SNMP_SESSION_MODE=NO_TRAPD
    ```

  - If you are using HP Operations agent 11.00, add:

    ```
    [eaagt]
    SNMP_SESSION_MODE=NETSNMP
    ```

- On Linux nodes where SIM Agent is installed, open the SNMP configuration file located at `/etc/snmp/snmpd.conf` and append the following line at the end:

  `trapsink` <*hostname of the node*>
- On Windows nodes, check if the following SIM Agents are installed:
  - Foundation Agent
  - NIC Agent
  - Server Agent

- Storage Agent

If these are not installed, install HP Insight Management for the Windows Servers 2003/ 2008 x64 Editions.

Changing the Port Number

By default, the `opctrapi` is configured on port number 162 to receive SNMP traps and CMIP event. To change the port number, follow these steps:

1. Check SNMP service is running.

   For Windows, do the following:

   a. Click **Start** → **Run** → type `services.msc`. The **Services** dialog box opens.

   b. Select **SNMP Service**.

   c. Check if the SNMP service `Status=Started`.

   For UNIX, type the command:

   ```
   # service snmp status
   ```

2. Check if `opctrapi` is configured on the default port number 162.

   For Windows, type the command:

   ```
   netstat -anb | findstr opctrapi
   ```

   For UNIX, type the command:

   ```
   # netstat -anp | grep 162
   ```

3. To change the XPL configuration settings on the managed node, type the command:

   ```
   # ovconfchg -ns eaagt -set SNMP_TRAP_PORT <any allowed port>
   ```

4. Add `SNMP_TRAP_PORT= <any allowed port>` under the namespace `eaagt`.

5. To return all the attributes in the `eaagt` namespace, type the command:

   ```
   # ovconfget eaagt
   ```

6. To restart the `opctrapi`, type the command:

   ```
   # ovc -restart opctrapi
   ```

7. Confirm if the port number has changed.

   For Windows, type the command:

   ```
   netstat -anb | findstr opctrapi
   ```

   For UNIX, type the command:

   ```
   # netstat -anp | grep <changed port>
   ```

Server Health Traps Monitor Policy

SI-HPProLiant_CPQHLTHTraps

The SI-HPProLiant_CPQHLTHTraps policy intercepts SNMP traps related to the health of the server and sends an alert to the HPOM console every time a trap is generated. The policy monitors the following SNMP traps:

MIB ID	SNMP Trap Description
1.3.6.1.2.1.11.6.0	coldStart.
1.3.6.1.2.1.11.6.1	warmStart.
1.3.6.1.2.1.11.6.2	linkDown.
1.3.6.1.2.1.11.6.3	linkUp.
1.3.6.1.4.1.232.0.6003	System will be shutdown due to this thermal condition.
1.3.6.1.4.1.232.0.6017	System will be shutdown due to this thermal condition.
1.3.6.1.4.1.232.0.6004	Temperature out of range. Shutdown may occur.
1.3.6.1.4.1.232.0.6018	Temperature out of range. Shutdown may occur.
1.3.6.1.4.1.232.0.6019	Temperature has returned to normal range.
1.3.6.1.4.1.232.0.6005	Temperature has returned to normal range.
1.3.6.1.4.1.232.0.6040	Temperature status failed on Chassis contained in SNMP Varbind 3, Location contained in SNMP Varbind 4.
1.3.6.1.4.1.232.0.6041	Temperature status has degraded on Chassis contained in SNMP Varbind 4, Location contained in SNMP Varbind 5.
1.3.6.1.4.1.232.0.6041	Temperature out of range on Chassis contained in SNMP Varbind 4, Location contained in SNMP Varbind 5.Shutdown may occur soon.
1.3.6.1.4.1.232.0.6042	Temperature Normal on Chassis contained in SNMP Varbind 3, location contained in SNMP Varbind 4.
1.3.6.1.4.1.232.0.6007	An optional fan is not operating normally.
1.3.6.1.4.1.232.0.6021	An optional fan is not operating normally.
1.3.6.1.4.1.232.0.6006	Required fan not operating normally. Shutdown may occur.
1.3.6.1.4.1.232.0.6020	Required fan not operating normally.
1.3.6.1.4.1.232.0.6020	System fan has failed.
1.3.6.1.4.1.232.0.6022	System fan has returned to normal operation.
1.3.6.1.4.1.232.0.6008	System fan has returned to normal operation.
1.3.6.1.4.1.232.0.6009	CPU fan has failed. Server will be shutdown.
1.3.6.1.4.1.232.0.6010	CPU fan is now OK.
1.3.6.1.4.1.232.0.6023	CPU fan has failed. Server will be shutdown.
1.3.6.1.4.1.232.0.6024	CPU fan is now OK.

MIB ID	SNMP Trap Description
1.3.6.1.4.1.232.0.6035	The Fan Degraded on Chassis contained in SNMP Varbind 3, Fan contained in SNMP Varbind 4.
1.3.6.1.4.1.232.0.6036	The Fan Failed on Chassis contained in SNMP Varbind 3, Fan contained in SNMP Varbind 4.
1.3.6.1.4.1.232.0.6037	The Fans are no longer redundant on Chassis contained in SNMP Varbind 3.
1.3.6.1.4.1.232.0.6055	The Fault Tolerant Fans have returned to a redundant state for the specified chassis.
1.3.6.1.4.1.232.0.6048	The Power Supply is OK on Chassis in SNMP Varbind 3.
1.3.6.1.4.1.232.0.6049	The Power Supply is degraded on Chassis in SNMP Varbind 3.
1.3.6.1.4.1.232.0.6050	The Power Supply is failed on Chassis in SNMP Varbind 3.
1.3.6.1.4.1.232.0.6014	The server power supply status has become degraded.
1.3.6.1.4.1.232.0.6028	The server power supply status has become degraded.
1.3.6.1.4.1.232.0.6030	The Power Supply Degraded on Chassis contained in SNMP Varbind 3, Bay contained in SNMP Varbind 4.
1.3.6.1.4.1.232.0.6054	Fault Tolerant Power Supplies Power Redundancy Restored.
1.3.6.1.4.1.232.0.6031	The Power Supply Failed on Chassis contained in SNMP Varbind 3, Bay contained in SNMP Varbind 4.
1.3.6.1.4.1.232.0.6032	The Power Supplies are no longer redundant on Chassis contained in SNMP Varbind 3.
1.3.6.1.4.1.232.0.6043	Power Converter Degraded on Chassis in SNMP Varbind 3, Slot in SNMP Varbind 4, Socket in SNMP Varbind 5.
1.3.6.1.4.1.232.0.6044	Power Converter Failed on Chassis in SNMP Varbind 3, Slot in SNMP Varbind 4, Socket in SNMP Varbind 5.
1.3.6.1.4.1.232.0.6045	Power Converters are no longer redundant on Chassis contained in SNMP Varbind 3.
1.3.6.1.4.1.232.0.6012	Server is operational again after thermal shutdown.
1.3.6.1.4.1.232.0.6027	Errors occurred during server restart.
1.3.6.1.4.1.232.0.6059	Memory board or cartridge bus error detected.
1.3.6.1.4.1.232.0.6063	The Management processor failed to reset.
1.3.6.1.4.1.232.0.6025	Server is operational again after ASR shutdown.
1.3.6.1.4.1.232.0.6016	Too many memory errors tracking now disabled.
1.3.6.1.4.1.232.0.6016	Error tracking is now enabled.
1.3.6.1.4.1.232.0.6002	Too many memory errors tracking now disabled.
1.3.6.1.4.1.232.0.6026	Server is operational again after thermal shutdown.

MIB ID	SNMP Trap Description
1.3.6.1.4.1.232.0.6061	The Management processor is currently in reset.
1.3.6.1.4.1.232.0.6062	The Management processor is ready.
1.3.6.1.4.1.232.0.6013	Errors occurred during server restart.

The policy contains a rule for each of these SNMP traps. After the problem is resolved the previous alert message is automatically acknowledged.

RAID Controller Traps Monitor Policy

SI-HPProLiant_CPQRCTraps

The SI-HPProLiant_CPQRCTraps policy intercepts SNMP traps related to the performance and availability of the RAID Controller and sends an alert to the HPOM console every time a trap is generated. The policy monitors the following traps:

MIB ID	SNMP Trap Description
1.3.6.1.4.1.232.141.3.8.0.27	The temperature in the expansion cabinet has triggered a critical condition detected by the controller.
1.3.6.1.4.1.232.141.3.8.6.26	cpqCrExpCabTemperatureWarningTrap.
1.3.6.1.4.1.232.141.3.8.0.22	One of the power supplies in the expansion cabinet has failed.
1.3.6.1.4.1.232.141.3.8.0.20	Fan has failed in expansion cabinet.
1.3.6.1.4.1.232.141.3.7.0.25	The temperature in the primary enclosure has returned to normal.
1.3.6.1.4.1.232.141.3.2.0.2	The primary controller in the subsystem has recovered.
1.3.6.1.4.1.232.141.3.8.0.29	One of the power supplies in the expansion cabinet has recovered.
1.3.6.1.4.1.232.141.3.3.0.6	The RAIDset has failed and is off-line.
1.3.6.1.4.1.232.141.3.8.0.28	The temperature in the expansion cabinet has returned to normal.
1.3.6.1.4.1.232.141.3.2.0.1	The primary controller in the subsystem has failed.
1.3.6.1.4.1.232.141.3.7.0.16	One of the cooling fans in the primary enclosure has failed.
1.3.6.1.4.1.232.141.3.2.0.4	The secondary controller in the subsystem has recovered.
1.3.6.1.4.1.232.141.3.7.0.19	One of the power supplies in the primary enclosure has recovered.
.1.3.6.1.4.1.232.141.3.5.6.31	cpqCrPhyDiskFailureTrap.
1.3.6.1.4.1.232.141.3.7.0.24	The temperature in the primary enclosure has triggered a critical condition detected by the controller.
1.3.6.1.4.1.232.141.3.5.0.10	A disk device has recovered.
1.3.6.1.4.1.232.141.3.7.0.17	One of the cooling fans in the primary enclosure has recovered.

MIB ID	SNMP Trap Description
1.3.6.1.4.1.232.141.3.5.6.30	cpqCrPhyDiskInformationTrap.
1.3.6.1.4.1.232.141.3.2.0.3	The secondary controller in the subsystem has failed.
1.3.6.1.4.1.232.141.3.8.0.21	One of the cooling fans in the expansion cabinet has recovered.
1.3.6.1.4.1.232.141.3.5.0.11	A disk device has failed.
1.3.6.1.4.1.232.141.3.7.0.23	Primary enclosure temperature warning.
1.3.6.1.4.1.232.141.3.7.0.18	One of the power supplies in the primary enclosure has failed.

The policy contains a rule for each of these SNMP traps. After the problem is resolved the previous alert message is automatically acknowledged.

NIC Traps Monitor Policy

SI-HPProLiant_CPQNICTraps

The SI-HPProLiant_CPQNICTraps policy intercepts SNMP traps related to the performance and availability of the Network Interface Card (NIC) and sends an alert to the HPOM console every time a trap is generated. The policy monitors the following traps:

MIB ID	SNMP Trap Description
1.3.6.1.4.1.232.0.11005	NIC Status is OK.
1.3.6.1.4.1.232.0.11006	NIC Status is Failed.
1.3.6.1.4.1.232.0.11007	NIC switchover occurred.
1.3.6.1.4.1.232.0.11008	NIC Status is OK.
1.3.6.1.4.1.232.0.11009	NIC Status is Failed.
1.3.6.1.4.1.232.0.11010	NIC switchover.
1.3.6.1.2.1.11.6.2	linkDown.
1.3.6.1.2.1.11.6.3	linkUp.
1.3.6.1.4.1.232.0.18006	Connectivity lost for logical adapter in slot contained in SNMP Varbind 3, port contained in SNMP Varbind 4.
1.3.6.1.4.1.232.6.18012	cpqNic3ConnectivityLost.
1.3.6.1.4.1.232.6.18011	cpqNic3ConnectivityRestored.
1.3.6.1.4.1.232.0.18009	NIC Virus-like Activity Detected Trap.
1.3.6.1.4.1.232.0.18010	NIC Virus-like Activity No Longer Detected Trap.

The policy contains a rule for each of these SNMP traps. After the problem is resolved the previous alert message is automatically acknowledged.

CMC Traps Monitor Policy

SI-HPProLiant_CPQCMCTraps

The SI-HPProLiant_CPQCMCTraps policy intercepts SNMP traps related to the health of the Console Management Controller (CMC) in terms of power consumption, smoke, humidity, temperature, and fan. The policy sends an alert to the HPOM console every time a trap is generated.

It monitors the following traps:

MIB ID	SNMP Trap Description
1.3.6.1.4.1.232.153.0.153013	Status of smoke presence in rack as detected by CMC is Present, the status is contained in SNMP Varbind 5.
1.3.6.1.4.1.232.153.0.153013	Status of smoke presence in rack as detected by CMC is Normal, the status is contained in SNMP Varbind 5.
1.3.6.1.4.1.232.153.0.153005	Status of voltage-supply to CMC is OverMax, status is contained in SNMP Varbind 5.
1.3.6.1.4.1.232.153.0.153005	Status of voltage-supply to CMC is UnderMin, status is contained in SNMP Varbind 5.
1.3.6.1.4.1.232.153.0.153005	Status of voltage-supply to CMC is Normal, status is contained in SNMP Varbind 5.
1.3.6.1.4.1.232.153.0.153001	Temperature in rack sensed by CMC temperature sensor 1 has exceeded High threshold, status is contained in SNMP Varbind 5.
1.3.6.1.4.1.232.153.0.153001	Temperature in rack as sensed by CMC temperature sensor 1 has gone below Minimum threshold, status is contained in SNMP Varbind 5.
1.3.6.1.4.1.232.153.0.153002	Temperature in rack as sensed by CMC temperature sensor 1 is NORMAL, status is contained in SNMP Varbind 5.
1.3.6.1.4.1.232.153.0.153002)	Temperature in rack as sensed by CMC temperature sensor 2 has exceeded High threshold, status is contained in SNMP Varbind 5. (
1.3.6.1.4.1.232.153.0.153002	Temperature in rack as sensed CMC temperature sensor 2 has gone below Minimum Threshold, status is contained in SNMP Varbind 5.
1.3.6.1.4.1.232.153.0.153002	Temperature in rack as sensed by CMC temperature sensor 2 is NORMAL, status is contained in SNMP Varbind 5.
1.3.6.1.4.1.232.153.0.153006	Status of humidity is OverMax, status is contained in SNMP Varbind 5.
1.3.6.1.4.1.232.153.0.153006	Status of humidity is UnderMin, status is contained in SNMP Varbind 5.
1.3.6.1.4.1.232.153.0.153006	Status of humidity is normal, status is contained in SNMP Varbind 5.
1.3.6.1.4.1.232.153.0.153003	Status of Fan 1 in rack is Normal, status is contained in SNMP Varbind 5.

MIB ID	SNMP Trap Description
1.3.6.1.4.1.232.153.0.153003	Status of Fan 1 in rack is AutoOff, status is contained in SNMP Varbind 5.
1.3.6.1.4.1.232.153.0.153003	Status of Fan 1 in rack is SmokeOff, status is contained in SNMP Varbind 5.
1.3.6.1.4.1.232.153.0.153003	Status of Fan 1 in rack is DoorOff, status is contained in SNMP Varbind 5.
1.3.6.1.4.1.232.153.0.153004	Status of Fan 2 in rack is AutoOn, status is contained in SNMP Varbind 5.
1.3.6.1.4.1.232.153.0.153004	Status of Fan 2 in rack is AutoOff, status is contained in SNMP Varbind 5.
1.3.6.1.4.1.232.153.0.153004	Status of Fan 2 in rack is SmokeOff, status is contained in SNMP Varbind 5.
1.3.6.1.4.1.232.153.0.153004	Status of Fan 2 in rack is DoorOff, status is contained in SNMP Varbind 5.

The policy contains a rule for each of these SNMP traps. After the problem is resolved the previous alert message is automatically acknowledged.

System Information Traps Monitor Policy

SI-HPProLiant_CPQSysInfoTraps

The SI-HPProLiant_CPQSysInfoTraps policy intercepts SNMP traps related to system information in terms of the state of the battery, monitor, Hot Plug Slot Board, memory, and hood. The policy sends an alert to the HPOM console every time a trap is generated.

It monitors the following traps:

MIB ID	SNMP Trap Description
1.3.6.1.4.1.232.0.2012	Battery contained in SNMP Varbind 3 has degraded charging capacity.
1.3.6.1.4.1.232.0.2011	Battery contained in SNMP Varbind 3 has failed.
1.3.6.1.4.1.232.0.2013	Battery contained in SNMP Varbind 3 has calibration error.
1.3.6.1.4.1.232.0.2003	The monitor condition has been set to degraded.
1.3.6.1.4.1.232.0.2004	The monitor condition has been set to failed.
1.3.6.1.4.1.232.0.2002	The monitor condition has been set to OK.
1.3.6.1.4.1.232.0.2006	The Memory Module ECC status has been set to OK.
1.3.6.1.4.1.232.0.2005	The Memory Module ECC status has been set to degraded.
1.3.6.1.4.1.232.0.2009	Hot Plug Slot Board Inserted into Chassis contained in SNMP Varbind 3, Slot contained in SNMP Varbind 4.

MIB ID	SNMP Trap Description
1.3.6.1.4.1.232.0.2010	Hot Plug Slot Board Failed in Chassis contained in SNMP Varbind 3, Slot contained in SNMP Varbind 4, Error contained in SNMP ind 5.
1.3.6.1.4.1.232.0.2008)	Hot Plug Slot Board Removed from Chassis.
1.3.6.1.4.1.232.0.2007	The system's memory configuration has changed.
1.3.6.1.4.1.232.0.2001	Hood is removed from unit.

The policy contains a rule for each of these SNMP traps. After the problem is resolved the previous alert message is automatically acknowledged.

Virtual Connect Domain Traps Monitor Policy

SI-HPProLiant_VCDomainTraps

The SI-HPProLiant_VCDomainTraps policy intercepts SNMP traps related to virtual connect domain. The policy sends an alert to the HPOM console every time a trap is generated.

It monitors the following traps:

MIB ID	SNMP Trap Description
1.3.6.1.4.1.11.5.7.5.2.1.2.0.5	vcFcFabricManagedStatusChange
1.3.6.1.4.1.11.5.7.5.2.1.2.0.3	vcCheckpointCompleted
1.3.6.1.4.1.11.5.7.5.2.1.2.0.9	vcProfileManagedStatusChange
1.3.6.1.4.1.11.5.7.5.2.1.2.0.6	vcModuleManagedStatusChange
1.3.6.1.4.1.11.5.7.5.2.1.2.0.8	vcPhysicalServerManagedStatusChange
1.3.6.1.4.1.11.5.7.5.2.1.2.0.1	vcDomainManagedStatusChange
1.3.6.1.4.1.11.5.7.5.2.1.2.0.2	vcCheckpointTimeout

The policy contains a rule for each of these SNMP traps. After the problem is resolved the previous alert message is automatically acknowledged.

Cluster Traps Monitor Policy

SI-HPProLiant_CPQCLUSTraps

The SI-HPProLiant_CPQCLUSTraps policy intercepts SNMP traps related to clusters in terms of the state of the battery, monitor, Hot Plug Slot Board, memory, and hood. The policy sends an alert to the HPOM console every time a trap is generated.

It monitors the following traps:

MIB ID	SNMP Trap Description
1.3.6.1.4.1.232.0.15001	Cluster contained in SNMP Varbind 3 has become degraded.
1.3.6.1.4.1.232.0.15002	Cluster contained in SNMP Varbind 3 has failed.
1.3.6.1.4.1.232.0.15003	Cluster service on contained in SNMP Varbind 3 has become degraded.
1.3.6.1.4.1.232.0.15004	Cluster service on node contained in SNMP Varbind 3 has failed.
1.3.6.1.4.1.232.0.15007	Cluster resource contained in SNMP Varbind 3 has become degraded.
1.3.6.1.4.1.232.0.15005	Cluster resource contained in SNMP Varbind 3 has failed.
1.3.6.1.4.1.232.0.15008	Cluster network contained in SNMP Varbind 3 has become degraded.
1.3.6.1.4.1.232.0.15006	Cluster network contained in SNMP Varbind 3 has failed.

The policy contains a rule for each of these SNMP traps. After the problem is resolved the previous alert message is automatically acknowledged.

Rack Power Manager Traps Monitor Policy

SI-HPProLiant_CPQRPMTraps

The SI-HPProLiant_CPQRPMTraps policy intercepts SNMP traps related to Rack Power Manager. The policy sends an alert to the HPOM console every time a trap is generated.

It monitors the following traps:

MIB ID	SNMP Trap Description
1.3.6.1.4.1.232.154.2.1	A UPS device is reporting a Connection Lost
1.3.6.1.4.1.232.154.2.2	A UPS device is reporting a Connection Lost
1.3.6.1.4.1.232.154.2.3	CRPM failed to find an IP address for the device hostname
1.3.6.1.4.1.232.154.2.4	CRPM failed to connect to a device
1.3.6.1.4.1.232.154.2.5	cpqRPMTrapDeviceSettingsChanged
1.3.6.1.4.1.232.154.2.10001	A CMC device is reporting temperature 1 below minimum threshold
1.3.6.1.4.1.232.154.2.10002	A CMC device is reporting temperature 1 above warning threshold
1.3.6.1.4.1.232.154.2.10003	A CMC device is reporting temperature 1 above maximum threshold
1.3.6.1.4.1.232.154.2.10004	A CMC device is reporting temperature 1 has returned to a normal

MIB ID	SNMP Trap Description
1.3.6.1.4.1.232.154.2.10005	A CMC device is reporting temperature 2 below minimum threshold
1.3.6.1.4.1.232.154.2.10006	A CMC device is reporting temperature 2 above warning threshold
1.3.6.1.4.1.232.154.2.10007	A CMC device is reporting temperature 2 above maximum threshold
1.3.6.1.4.1.232.154.2.10008	A CMC device is reporting temperature 2 has returned to a normal temperature
1.3.6.1.4.1.232.154.2.10011	A CMC device is reporting voltage below minimum threshold
1.3.6.1.4.1.232.154.2.10012	A CMC device is reporting voltage above maximum threshold
1.3.6.1.4.1.232.154.2.10013	A CMC device is reporting voltage has returned to normal
1.3.6.1.4.1.232.154.2.10021	A CMC device is reporting humidity below minimum threshold
1.3.6.1.4.1.232.154.2.10022	A CMC device is reporting humidity above maximum threshold
1.3.6.1.4.1.232.154.2.10023	A CMC device is reporting humidity has returned to normal
1.3.6.1.4.1.232.154.2.10031	A CMC device is reporting smoke detected
1.3.6.1.4.1.232.154.2.10032	A CMC device is reporting smoke cleared
1.3.6.1.4.1.232.154.2.10041	A CMC device is reporting shock detected
1.3.6.1.4.1.232.154.2.10042	A CMC device is reporting shock cleared
1.3.6.1.4.1.232.154.2.10051	A CMC device has entered an alarm condition for auxiliary input 1
1.3.6.1.4.1.232.154.2.10052	A CMC device is reporting auxiliary input 1 alarm cleared
1.3.6.1.4.1.232.154.2.10053	A CMC device has entered an alarm condition for auxiliary input 2
1.3.6.1.4.1.232.154.2.10054	A CMC device is reporting auxiliary input 2 alarm cleared
1.3.6.1.4.1.232.154.2.10101	A CMC device is reporting input 1 has been opened
1.3.6.1.4.1.232.154.2.10102	A CMC device is reporting input 1 has been closed
1.3.6.1.4.1.232.154.2.10103	A CMC device is reporting input 2 has been opened
1.3.6.1.4.1.232.154.2.10104	A CMC device is reporting input 2 has been closed
1.3.6.1.4.1.232.154.2.10105	A CMC device is reporting input 3 has been opened
1.3.6.1.4.1.232.154.2.10106	A CMC device is reporting input 3 has been closed
1.3.6.1.4.1.232.154.2.10107	A CMC device is reporting input 4 has been opened
1.3.6.1.4.1.232.154.2.10108	A CMC device is reporting input 4 has been closed

MIB ID	SNMP Trap Description
1.3.6.1.4.1.232.154.2.10111	A CMC device is reporting lockset 1 has been unlocked
1.3.6.1.4.1.232.154.2.10112	A CMC device is reporting lockset 1 has failed to lock
1.3.6.1.4.1.232.154.2.10113	A CMC device is reporting an error with lockset 1
1.3.6.1.4.1.232.154.2.10114	A CMC device is reporting lockset 1 has been locked
1.3.6.1.4.1.232.154.2.10116	A CMC device is reporting lockset 2 has been unlocked
1.3.6.1.4.1.232.154.2.10117	A CMC device is reporting lockset 2 has failed to lock
1.3.6.1.4.1.232.154.2.10118	A CMC device is reporting an error with lockset 2
1.3.6.1.4.1.232.154.2.10119	A CMC device is reporting lockset 2 has been locked
1.3.6.1.4.1.232.154.2.10134	A CMC device is reporting lockset 1 is normal
1.3.6.1.4.1.232.154.2.10135	A CMC device is reporting lockset 2 is normal
1.3.6.1.4.1.232.154.2.20001	cpqRPMTrapUPSInputVoltageBelowMin
1.3.6.1.4.1.232.154.2.20002	cpqRPMTrapUPSInputVoltageAboveMax
1.3.6.1.4.1.232.154.2.20003	cpqRPMTrapUPSInputVoltageNormal
1.3.6.1.4.1.232.154.2.20011	cpqRPMTrapUPSOutputVoltageBelowMin
1.3.6.1.4.1.232.154.2.20012	cpqRPMTrapUPSOutputVoltageAboveMax
1.3.6.1.4.1.232.154.2.20014	A UPS device is reporting an overload condition
1.3.6.1.4.1.232.154.2.20015	A UPS device is reporting an overload condition has cleared
1.3.6.1.4.1.232.154.2.20022	cpqRPMTrapUPSBatteryDepleted
1.3.6.1.4.1.232.154.2.20023	cpqRPMTrapUPSBatteryLevelNormal
1.3.6.1.4.1.232.154.2.20032	cpqRPMTrapUPSOnBypass
1.3.6.1.4.1.232.154.2.20101	cpqRPMTrapUPSTemperatureLow
1.3.6.1.4.1.232.154.2.20102	cpqRPMTrapUPSTemperatureHigh
1.3.6.1.4.1.232.154.2.20103	A UPS device is reporting temperature is Normal
1.3.6.1.4.1.232.154.2.20111	A UPS device is reporting a general UPS failure
1.3.6.1.4.1.232.154.2.20112	A UPS device is reporting a general UPS failure Cleared
1.3.6.1.4.1.232.154.2.20121	A UPS device is reporting a battery failure
1.3.6.1.4.1.232.154.2.20122	A UPS device is reporting a battery failure cleared
1.3.6.1.4.1.232.154.2.20131	A UPS device is reporting a diagnostic test failed
1.3.6.1.4.1.232.154.2.20132	A UPS device is reporting a diagnostic test succeeded
1.3.6.1.4.1.232.154.2.20141	Input (Utility) for UPS: measured input frequency is outside of either the upper or lower frequency limit specification for normal operation

MIB ID	SNMP Trap Description
1.3.6.1.4.1.232.154.2.20142	UPS Measured input frequency is normal
1.3.6.1.4.1.232.154.2.20151	A UPS device has been started while on battery power
1.3.6.1.4.1.232.154.2.20152	A UPS device has been started while on utility power
1.3.6.1.4.1.232.154.2.20161	A UPS device is reporting bypass not available
1.3.6.1.4.1.232.154.2.20162	A UPS device is reporting bypass not available error has been cleared
1.3.6.1.4.1.232.154.2.20171	cpqRPMTrapUPSUtilityFail
1.3.6.1.4.1.232.154.2.20172	cpqRPMTrapUPSUtilityFailCleared
1.3.6.1.4.1.232.154.2.20181	cpqRPMTrapUPSUtilityNotPresent
1.3.6.1.4.1.232.154.2.20182	cpqRPMTrapUPSUtilityNotPresentCleared
1.3.6.1.4.1.232.154.2.20191	cpqRPMTrapUPSBypassManualTurnedOn
1.3.6.1.4.1.232.154.2.20192	cpqRPMTrapUPSBypassManualTurnedOff
1.3.6.1.4.1.232.154.2.20201	A UPS device is reporting a fault in the input wiring
1.3.6.1.4.1.232.154.2.20202	A UPS device is reporting the input wiring is NORMAL
1.3.6.1.4.1.232.154.2.21007	A UPS device is reporting temperature is out of range
1.3.6.1.4.1.232.154.2.21008	A UPS device is reporting temperature is NORMAL
1.3.6.1.4.1.232.154.2.21011	A UPS device is reporting shutdown pending condition
1.3.6.1.4.1.232.154.2.21012	The UPS is no longer pending shutdown
1.3.6.1.4.1.232.154.2.21013	A UPS device is reporting a shutdown imminent condition
1.3.6.1.4.1.232.154.2.21014	A UPS device is reporting a shutdown imminent condition cleared
1.3.6.1.4.1.232.154.2.21019	A UPS device is reporting output voltage is out of Range
1.3.6.1.4.1.232.154.2.21020	A UPS device is reporting output voltage is Normal
1.3.6.1.4.1.232.154.2.21021	A UPS device is reporting input voltage is out of range
1.3.6.1.4.1.232.154.2.21021	A UPS device is reporting input voltage is out of range
1.3.6.1.4.1.232.154.2.21023	A UPS device is reporting a loss of redundancy
1.3.6.1.4.1.232.154.2.21024	A UPS device is reporting a loss of redundancy cleared
1.3.6.1.4.232.154.2.21029	A UPS device is reporting an On Buck condition
1.3.6.1.4.232.154.2.21031	A UPS device is reporting an On Boost condition
1.3.6.1.4.1.232.154.2.21033	The UPS has been powered off with user interaction
1.3.6.1.4.1.232.154.2.21034	The UPS output has been restored
1.3.6.1.4.1.232.154.2.21035	A UPS device is reporting a fan failure has occurred

MIB ID	SNMP Trap Description
1.3.6.1.4.1.232.154.2.21036	A UPS device is reporting a fan failure has cleared
1.3.6.1.4.1.232.154.2.21037	A UPS device is reporting an Emergency Power Off (EPO) command
1.3.6.1.4.1.232.154.2.21041	A UPS device is reporting an output Breaker or Relay has failed
1.3.6.1.4.1.232.154.2.21042	A UPS device is reporting an output Breaker is functioning normally
1.3.6.1.4.1.232.154.2.21045	A UPS device is reporting a cover panel has been removed
1.3.6.1.4.1.232.154.2.21046	A UPS device is reporting a cover panel has been replaced
1.3.6.1.4.1.232.154.2.21047	A UPS device is operating in auto bypass mode
1.3.6.1.4.1.232.154.2.21048	A UPS device is not operating in auto bypass mode
1.3.6.1.4.1.232.154.2.21053	A UPS device is reporting batteries are not connected to the UPS
1.3.6.1.4.1.232.154.2.21054	A UPS device is reporting batteries are reconnected to the UPS
1.3.6.1.4.1.232.154.2.21055	A UPS device is reporting low battery
1.3.6.1.4.1.232.154.2.21056	A UPS device is reporting low battery cleared
1.3.6.1.4.1.232.154.2.21057	A UPS device is reporting batteries are completely discharged
1.3.6.1.4.1.232.154.2.21058	A UPS device is reporting batteries are completely discharged
1.3.6.1.4.1.232.154.2.21059	A UPS device is operating in manual bypass mode
1.3.6.1.4.1.232.154.2.21060	A UPS device is operating in NORMAL mode
1.3.6.1.4.1.232.154.2.21063	A UPS device is reporting on battery condition
1.3.6.1.4.1.232.154.2.21064	A UPS device is reporting on Power Utility condition
1.3.6.1.4.1.232.154.3.1	A critical alarm has occurred
1.3.6.1.4.1.232.154.3.2	A warning alarm has occurred for UPS
1.3.6.1.4.1.232.154.2.3	CRPM failed to find an IP address for the device hostname
1.3.6.1.4.1.232.154.3.4	An alarm has cleared for UPS
1.3.6.1.4.1.232.154.2.50001	cpqRPMTestTrap
1.3.6.1.4.1.232.154.2.29999	cpqRPMTrapUPSDCStartOccurredCleared
1.3.6.1.4.1.232.154.2.29998	cpqRPMTrapUPSDCStartOccurred

The policy contains a rule for each of these SNMP traps. After the problem is resolved the previous alert message is automatically acknowledged.

Intelligent Drive Array Traps Monitor Policy

SI-HPProLiant_FwdDriveArrayTraps

The SI-HPProLiant_FwdDriveArrayTraps policy intercepts SNMP traps related to Compaq's Intelligent Drive Array. The policy sends an alert to the HPOM console every time a trap is generated.

The policy monitors the following traps:

MIB ID	SNMP Trap Description
1.3.6.1.4.1.232.0.3001	Intelligent DriveArray Logical Drive status is NORMAL, contained in SNMP Varbind 1.
	Intelligent DriveArray Logical Drive status is FAILED, contained in SNMP Varbind 1.
	Intelligent Drive Array Logical Drive status is RECOVERING, contained in SNMP Varbind 1.
	Intelligent Drive Array Logical Drive status is READY for REBUILD, contained in SNMP Varbind 1.
	Intelligent Drive Array Logical Drive status is REBUILDING, contained in SNMP Varbind 1.
	Intelligent Drive Array Logical Drive status is WRONG DRIVE, contained in SNMP Varbind 1.
	Intelligent Drive Array Logical Drive status is BAD CONNECTION, contained in SNMP Varbind 1.
	Intelligent Drive Array Logical Drive status is OVERHEATING, contained in SNMP Varbind 1.
	Intelligent Drive Array Logical Drive status is SHUTDOWN, contained in SNMP Varbind 1.
	Intelligent Drive Array Logical Drive status is NOT AVAILABLE, status is contained in SNMP Varbind 1.
	Intelligent Drive Array Logical Drive status is UNCONFIGURED, status is contained in SNMP Varbind 1.
	Intelligent Drive Array Logical Drive status is EXPANDING, status is contained in SNMP Varbind 1.
	Intelligent Drive Array Logical Drive status is QUEUED FOR EXPANSION, status is contained in SNMP Varbind 1.

MIB ID	SNMP Trap Description
1.3.6.1.4.1.232.0.3002	Intelligent Drive Array Spare Drive status is ACTIVE, status is contained in SNMP Varbind 1.
	Intelligent Drive Array Spare Drive status is INVALID, status is contained in SNMP Varbind 1.
	Intelligent Drive Array Spare Drive status is INACTIVE, status is contained in SNMP Varbind 1.
	Intelligent Drive Array Spare Drive status is FAILED, status is contained in SNMP Varbind 1.
	Intelligent Drive Array Spare Drive status is BUILDING, status is contained in SNMP Varbind 1.
1.3.6.1.4.1.232.0.3003	Intelligent Drive Array Physical Drive status is OK, contained in SNMP Varbind 1.
	Intelligent Drive Array Physical Drive status is FAILED, contained in SNMP Varbind 1.
	Intelligent Drive Array Physical Drive status is PREDICTIVEFAILURE, status is contained in SNMP Varbind 1.
1.3.6.1.4.1.232.0.3004	Intelligent Drive Array Physical Drive threshold passed, status is contained in SNMP Varbind 1.
1.3.6.1.4.1.232.0.3005	Intelligent Drive Array Accelerator Board status is INVALID, status is contained in SNMP Varbind 1.
	Intelligent Drive Array Accelerator Board status is ENABLED, status is contained in SNMP Varbind 1.
	Intelligent Drive Array Accelerator Board status is TEMPORARILY DISABLED, status is contained in SNMP Varbind 1.
	Intelligent Drive Array Accelerator Board status is PERMANENTLY DISABLED, contained in SNMP Varbind 1.
	Intelligent Drive Array Accelerator Board status is PERMANENTLY DISABLED, contained in SNMP Varbind 1.
1.3.6.1.4.1.232.0.3006	Intelligent Drive Array Accelerator lost battery power. Data Loss possible.
1.3.6.1.4.1.232.0.3007	Intelligent Drive Array Accelerator Board Battery status is RECHARGING. Status is contained in SNMP Varbind 1.
	Intelligent Drive Array Accelerator Board Battery status is NOT PRESENT. Status is contained in SNMP Varbind 1.
	Intelligent Drive Array Accelerator Board Battery status is OK. Status is contained in SNMP Varbind 1.
	Intelligent Drive Array Accelerator Board Battery status is failed. Status is contained in SNMP Varbind 1.
	Intelligent Drive Array Accelerator Board Battery status is degraded. Status is contained in SNMP Varbind 1.

MIB ID	SNMP Trap Description
1.3.6.1.4.1.232.0.3008	Intelligent DriveArray Logical Drive status is UNCONFIGURED, contained in SNMP Varbind 3.
	Intelligent DriveArray Logical Drive status is EXPANDING, contained in SNMP Varbind 3.
	Intelligent DriveArray Logical Drive status is QUEUED FOR EXPANSION, contained in SNMP Varbind 3.
	Intelligent DriveArray Logical Drive status is NORMAL, contained in SNMP Varbind 3.
	Intelligent DriveArray Logical Drive status is FAILED, contained in SNMP Varbind 3.
	Intelligent Drive Array Logical Drive status is RECOVERING, contained in SNMP Varbind 3.
	Intelligent Drive Array Logical Drive status is READY for REBUILD, contained in SNMP Varbind 3.
	Intelligent Drive Array Logical Drive status is REBUILDING, contained in SNMP Varbind 3
	Intelligent Drive Array Logical Drive status is WRONG DRIVE, contained in SNMP Varbind 3.
	Intelligent Drive Array Logical Drive status is BAD CONNECTION, contained in SNMP Varbind 3.
	Intelligent Drive Array Logical Drive status is OVERHEATING, contained in SNMP Varbind 3.
	Intelligent Drive Array Logical Drive status is SHUTDOWN, contained in SNMP Varbind 3.
	Intelligent Drive Array Logical Drive status is NOT AVAILABLE, status is contained in SNMP Varbind 3.
1.3.6.1.4.1.232.0.3009	Intelligent Drive Array Spare Drive status is INVALID, status is contained in SNMP Varbind 3.
	Intelligent Drive Array Spare Drive status is INACTIVE, status is contained in SNMP Varbind 3.
	Intelligent Drive Array Spare Drive status is ACTIVE, status is contained in SNMP Varbind 3.
	Intelligent Drive Array Spare Drive status is FAILED, status is contained in SNMP Varbind 3.
	Intelligent Drive Array Spare Drive status is BUILDING, status is contained in SNMP Varbind 3.

MIB ID	SNMP Trap Description
1.3.6.1.4.1.232.0.3010	Intelligent Drive Array Physical Drive status is OK, contained in SNMP Varbind 3.
	Intelligent Drive Array Physical Drive status is FAILED, contained in SNMP Varbind 3 on SCSI Bus contained in Varbind 4.
	Intelligent Drive Array Physical Drive status on SCSI Bus is PREDICTIVEFAILURE, status is contained in SNMP Varbind 3 on SCSI Bus Number contained in Varbind 4.
1.3.6.1.4.1.232.0.3011	Intelligent Drive Array Physical Drive threshold passed, status is contained in SNMP Varbind 3.
1.3.6.1.4.1.232.0.3012	Intelligent Drive Array Accelerator Board status is INVALID, status is contained in SNMP Varbind 3.
	Intelligent Drive Array Accelerator Board status is ENABLED, status is contained in SNMP Varbind 3.
	Intelligent Drive Array Accelerator Board status is TEMPORARILY DISABLED, status is contained in SNMP Varbind 3.
	Intelligent Drive Array Accelerator Board status is PERMANENTLY DISABLED, contained in SNMP Varbind 3.
1.3.6.1.4.1.232.0.3013	Intelligent Drive Array Accelerator lost battery power. Data loss possible.
1.3.6.1.4.1.232.0.3014	Intelligent Drive Array Accelerator Board Battery status is RECHARGING. Status is contained in SNMP Varbind 3.
	Intelligent Drive Array Accelerator Board Battery status is NOT PRESENT. Status is contained in SNMP Varbind 3.
	Intelligent Drive Array Accelerator Board Battery status is OK. Status is contained in SNMP Varbind 3.
	Intelligent Drive Array Accelerator Board Battery status is failed. Status is contained in SNMP Varbind 3.
	Intelligent Drive Array Accelerator Board Battery status is degraded. Status is contained in SNMP Varbind 3.
1.3.6.1.4.1.232.0.3015	Intelligent Drive Array Controller status is OK, status is contained in SNMP Varbind 4.
	Intelligent Drive Array Controller status is FAILED, status is contained in SNMP Varbind 4.
	Intelligent Drive Array Controller has cable problem, status is contained in SNMP Varbind 4.
	Intelligent Drive Array Controller is powered off, status is contained in SNMP Varbind 4.
1.3.6.1.4.1.232.0.3016	Controller in slot is now active.

MIB ID	SNMP Trap Description
1.3.6.1.4.1.232.0.3017	Intelligent Drive Array Spare Drive status is INVALID, status is contained in SNMP Varbind 3.
	Intelligent Drive Array Spare Drive status is INACTIVE, status is contained in SNMP Varbind 3.
	Intelligent Drive Array Spare Drive status is ACTIVE, status is contained in SNMP Varbind 3.
	Intelligent Drive Array Spare Drive status is FAILED, status is contained in SNMP Varbind 3.
	Intelligent Drive Array Spare Drive status is BUILDING, status is contained in SNMP Varbind 1.
1.3.6.1.4.1.232.0.3018	Intelligent Drive Array Physical Drive status is OK, contained in SNMP Varbind 3.
	Intelligent Drive Array Physical Drive status is FAILED, contained in SNMP Varbind 3.
	Intelligent Drive Array Physical Drive status is PREDICTIVEFAILURE, status is contained in SNMP Varbind 3.
1.3.6.1.4.1.232.0.3019	Intelligent Drive Array Physical Drive threshold passed.
1.3.6.1.4.1.232.0.3020	Intelligent Drive Array Tape Library status is OK, status is contained in SNMP Varbind 7 for the tape library.
	Intelligent Drive Array Tape Library status is FAILED, status is contained in SNMP Varbind 7 for the tape library.
	Intelligent Drive Array Tape Library status is DEGRADED, status is contained in SNMP Varbind 7 for the tape library.
	Intelligent Drive Array Tape Library status is OFFLINE, status is contained in SNMP Varbind 7 for the tape library.
1.3.6.1.4.1.232.0.3021	Intelligent Drive Array Tape Library Door Status is OPEN, status is contained in SNMP Varbind 7.
	Intelligent Drive Array Tape Library Door Status is CLOSED, status is contained in SNMP Varbind 7.
	Intelligent Drive Array Tape Library Door Status is NOT SUPPORTED, status is contained in SNMP Varbind 7.

MIB ID	SNMP Trap Description
1.3.6.1.4.1.232.0.3022	Intelligent Drive Array Tape Drive Status is OK, status is contained in SNMP Varbind 7.
	Intelligent Drive Array Tape Drive Status is DEGRADED, status is contained in SNMP Varbind 7.
	Intelligent Drive Array Tape Drive Status is FAILED, status is contained in SNMP Varbind 7.
	Intelligent Drive Array Tape Drive Status is OFFLINE, status is contained in SNMP Varbind 7.
	Intelligent Drive Array Tape Drive Status is MISSING WAS OK, status is contained in SNMP Varbind 7.
	Intelligent Drive Array Tape Drive Status is MISSING WAS OFFLINE, status is contained in SNMP Varbind 7.
1.3.6.1.4.1.232.0.3023	Intelligent Drive Array Tape Drive cleaning is required.
1.3.6.1.4.1.232.0.3024	Cleaning tape needs replacing.
1.3.6.1.4.1.232.0.3025	Intelligent Drive Array Accelerator Board status is INVALID, status is contained in SNMP Varbind 7.
	Intelligent Drive Array Accelerator Board status is ENABLED, status is contained in SNMP Varbind 7.
	Intelligent Drive Array Accelerator Board status is TEMPORARILY DISABLED, status is contained in SNMP Varbind 7.
	Intelligent Drive Array Accelerator Board status is PERMANENTLY DISABLED, status is contained in SNMP Varbind 7.
1.3.6.1.4.1.232.0.3026	Intelligent Drive Array Accelerator lost battery power.Data Loss possible.
1.3.6.1.4.1.232.0.3027	Intelligent Drive Array Accelerator battery failed.
1.3.6.1.4.1.232.0.3028	Intelligent Drive Array Controller Board Status is OK, status is contained in SNMP Varbind 4.
	Intelligent Drive Array Controller Board has failed, status is contained in SNMP Varbind 4.
	Intelligent Drive Array Controller Board has cable problem, status is contained in SNMP Varbind 4.
	Intelligent Drive Array Controller Board is POWEREDOFF, status is contained in SNMP Varbind 4.
1.3.6.1.4.1.232.0.3029	Intelligent Drive Array Physical Drive status is OK, contained in SNMP Varbind 3.
	Intelligent Drive Array Physical Drive status is FAILED, contained in SNMP Varbind 3.
	Intelligent Drive Array Physical Drive status is PREDICTIVEFAILURE, status is contained in SNMP Varbind 3.

MIB ID	SNMP Trap Description
1.3.6.1.4.1.232.0.3030	Intelligent Drive Array Physical Drive threshold passed.
1.3.6.1.4.1.232.0.3031	Intelligent Drive Array Tape Library status is FAILED, status is contained in SNMP Varbind 10 for the tape library.
	Intelligent Drive Array Tape Library status is OK, status is contained in SNMP Varbind 10 for the tape library.
	Intelligent Drive Array Tape Library status is DEGRADED, status is contained in SNMP Varbind 10 for the tape library.
	Intelligent Drive Array Tape Library status is OFFLINE, status is contained in SNMP Varbind 10 for the tape library.
1.3.6.1.4.1.232.0.3032	Intelligent Drive Array Tape Drive Status is OK, status is contained in SNMP Varbind 7.
	Intelligent Drive Array Tape Drive status is OFFLINE, status is contained in SNMP Varbind 7.
	Intelligent Drive Array Tape Drive status is DEGRADED, status is contained in SNMP Varbind 7.
	Intelligent Drive Array Tape Drive status is FAILED, status is contained in SNMP Varbind 10.
	Intelligent Drive Array Tape Drive status is MISSING WAS OK, status is contained in SNMP Varbind 10.
	Intelligent Drive Array Tape Drive status is MISSING WAS OFFLINE, status is contained in SNMP Varbind 10.
1.3.6.1.4.1.232.0.3033	Intelligent Drive Array Controller status is GENERAL FAILURE, status is contained in SNMP Varbind 5.
	Intelligent Drive Array Controller has a CABLE PROBLEM, status is contained in SNMP Varbind 5.
	Intelligent Drive Array Controller is POWERED OFF, status is contained in SNMP Varbind 5.
	Intelligent Drive Array Controller is OK, status is contained in SNMP Varbind 5.

MIB ID	SNMP Trap Description
1.3.6.1.4.1.232.0.3034	Intelligent Drive Array Logical Drive status is UNCONFIGURED, contained in SNMP Varbind 6.
	Intelligent Drive Array Logical Drive status is QUEUED FOR EXPANSION, status is contained in SNMP Varbind 6.
	Intelligent DriveArray Logical Drive status is NORMAL, contained in SNMP Varbind 6.
	Intelligent DriveArray Logical Drive status is FAILED, contained in SNMP Varbind 6.
	Intelligent Drive Array Logical Drive status is RECOVERING, contained in SNMP Varbind 6.
	Intelligent Drive Array Logical Drive status is READY for REBUILD, contained in SNMP Varbind 6.
	Intelligent Drive Array Logical Drive status is REBUILDING, contained in SNMP Varbind 6.
	Intelligent Drive Array Logical Drive status is WRONG DRIVE, contained in SNMP Varbind 6.
	Intelligent Drive Array Logical Drive status is BAD CONNECTION, contained in SNMP Varbind 6.
	Intelligent Drive Array Logical Drive status is OVERHEATING, contained in SNMP Varbind 6.
	Intelligent Drive Array Logical Drive status is SHUTDOWN, contained in SNMP Varbind 6.
	Intelligent Drive Array Logical Drive status is EXPANDING, status is contained in SNMP Varbind 6.
	Intelligent Drive Array Logical Drive status is NOT AVAILABLE, status is contained in SNMP Varbind 6.
1.3.6.1.4.1.232.0.3035	Intelligent Drive Array Spare Drive status is INVALID, status is contained in SNMP Varbind 6.
	Intelligent Drive Array Spare Drive status is INACTIVE, status is contained in SNMP Varbind 6.
	Intelligent Drive Array Spare Drive status is ACTIVE, status is contained in SNMP Varbind 6.
	Intelligent Drive Array Spare Drive status is FAILED, status is contained in SNMP Varbind 6.
	Intelligent Drive Array Spare Drive status is BUILDING, status is contained in SNMP Varbind 6.

MIB ID	SNMP Trap Description
1.3.6.1.4.1.232.0.3036	Intelligent Drive Array Physical Drive status is OK, contained in SNMP Varbind 12.
	Intelligent Drive Array Physical Drive status is FAILED, contained in SNMP Varbind 12.
	Intelligent Drive Array Physical Drive status is PREDICTIVEFAILURE, status is contained in SNMP Varbind 12.
1.3.6.1.4.1.232.0.3037	Intelligent Drive Array Physical Drive threshold passed, the physical drive index is contained in SNMP Varbind 5.
1.3.6.1.4.1.232.0.3038	Intelligent Drive Array Accelerator Board status is INVALID, status is contained in SNMP Varbind 8.
	Intelligent Drive Array Accelerator Board status is ENABLED, status is contained in SNMP Varbind 8.
	Intelligent Drive Array Accelerator Board status is TEMPORARILY DISABLED, status is contained in SNMP Varbind 8.
	Intelligent Drive Array Accelerator Board status is PERMANENTLY DISABLED, contained in SNMP Varbind 8.
1.3.6.1.4.1.232.0.3039	Intelligent Drive Array Accelerator lost battery power. Data Loss possible.
1.3.6.1.4.1.232.0.3040	Intelligent Drive Array Accelerator battery failed.
1.3.6.1.4.1.232.0.3041	Intelligent Drive Array Tape Library status is OK, status is contained in SNMP Varbind 11 for the tape library.
	Intelligent Drive Array Tape Library status is DEGRADED, status is contained in SNMP Varbind 11 for the tape library.
	Intelligent Drive Array Tape Library status is FAILED, status is contained in SNMP Varbind 11 for the tape library.
	Intelligent Drive Array Tape Library status is OFFLINE, status is contained in SNMP Varbind 11 for the tape library.
1.3.6.1.4.1.232.0.3042	Intelligent Drive Array Tape Library Door Status is OPEN, status is contained in SNMP Varbind 11.
	Intelligent Drive Array Tape Library Door Status is CLOSED, status is contained in SNMP Varbind 11.
	Intelligent Drive Array Tape Library Door Status is NOT SUPPORTED, status is contained in SNMP Varbind 11.

MIB ID	SNMP Trap Description
1.3.6.1.4.1.232.0.3043	Intelligent Drive Array Tape Drive status is DEGRADED, status is contained in SNMP Varbind 11.
	Intelligent Drive Array Tape Drive Status is OK, status is contained in SNMP Varbind 11.
	Intelligent Drive Array Tape Drive Status is FAILED, status is contained in SNMP Varbind 11.
	Intelligent Drive Array Tape Drive Status is OFFLINE, status is contained in SNMP Varbind 11.
	Intelligent Drive Array Tape Drive Status is MISSING WAS OK, status is contained in SNMP Varbind 11.
	Intelligent Drive Array Tape Drive Status is MISSING WAS OFFLINE, status is contained in SNMP Varbind 11.
1.3.6.1.4.1.232.0.3044	Intelligent Drive Array Tape Drive cleaning is required.
1.3.6.1.4.1.232.0.3045	Cleaning tape needs replacing.
1.3.6.1.4.1.232.0.3046	Physical Drive Status is OK, status is contained in SNMP Varbind 12.
	Physical Drive Status is FAILED, status is contained in SNMP Varbind 12.
	Physical Drive Status is PREDICTIVEFAILURE, status is contained in SNMP Varbind 12.
1.3.6.1.4.1.232.0.3047	Spare Status has changed.

The policy contains a rule for each of these SNMP traps. After the problem is resolved the previous alert message is automatically acknowledged.

Rack Information Traps Monitor Policy

SI-HPProLiant_CPQRackTraps

The SI-HPProLiant_CPQRackTraps policy intercepts SNMP traps related to rack information in terms of temperature, power, and status. The policy sends an alert to the HPOM console every time a trap is generated.

It monitors the following traps:

MIB ID	SNMP Trap Description
1.3.6.1.4.1.232.0.22002	The enclosure name has changed to SNMP Varbind 5 in rack SNMP Varbind 3.
1.3.6.1.4.1.232.0.22003	The enclosure in SNMP Varbind 5 has been removed from rack SNMP Varbind 3.
1.3.6.1.4.1.232.0.22004	The enclosure in SNMP Varbind 5 has been inserted into rack SNMP Varbind 3.
1.3.6.1.4.1.232.0.22005	The enclosure in SNMP Varbind 5 temperature sensor in rack SNMP Varbind 3 has been set to failed.
1.3.6.1.4.1.232.0.22006	The enclosure in SNMP Varbind 5 temperature sensor in rack SNMP Varbind 3 has been set to degraded.

MIB ID	SNMP Trap Description
1.3.6.1.4.1.232.0.22007	The enclosure in SNMP Varbind 5 temperature sensor in rack SNMP Varbind 3 has been set to ok.
1.3.6.1.4.1.232.0.22008	The enclosure in SNMP Varbind 5 fan in rack SNMP Varbind 3 has been set to failed.
1.3.6.1.4.1.232.0.22009	The enclosure in SNMP Varbind 5 fan in rack SNMP Varbind 3 has been set to degraded.
1.3.6.1.4.1.232.0.22010	The enclosure in SNMP Varbind 5 fan in rack SNMP Varbind 3 has been set to ok.
1.3.6.1.4.1.232.0.22011	The enclosure in SNMP Varbind 5 fan in rack SNMP Varbind 3 has been removed.
1.3.6.1.4.1.232.0.22012	The enclosure in SNMP Varbind 5 fan in rack SNMP Varbind 3 has been inserted.
1.3.6.1.4.1.232.0.22013	The power supply in SNMP Varbind 7 in enclosure SNMP Varbind 5 in rack SNMP Varbind 3 has been set to failed.
1.3.6.1.4.1.232.0.22014	The power supply in SNMP Varbind 7 in enclosure SNMP Varbind 5 in rack SNMP Varbind 3 has been set to degraded.
1.3.6.1.4.1.232.0.22015	The power supply in SNMP Varbind 7 in enclosure SNMP Varbind 5 in rack SNMP Varbind 3 has been set to ok.
1.3.6.1.4.1.232.0.22016	The power supply in SNMP Varbind 7 in enclosure SNMP Varbind 5 in rack SNMP Varbind 3 has been removed.
1.3.6.1.4.1.232.0.22017	The power supply in SNMP Varbind 7 in enclosure SNMP Varbind 5 in rack SNMP Varbind 3 has been inserted.
1.3.6.1.4.1.232.0.22018	The power subsystem in enclosure SNMP Varbind 5 in rack SNMP Varbind 3 is no longer redundant.
1.3.6.1.4.1.232.0.22019	The rack power supply detected an input line voltage problem in power supply SNMP Varbind 6, enclosure in SNMP Varbind 5, rack in SNMP Varbind 3.
1.3.6.1.4.1.232.0.22020	The power subsystem in enclosure SNMP Varbind 5 in rack SNMP Varbind 3 is in an overload condition.
1.3.6.1.4.1.232.0.22021	The server shutdown due to lack of power blade SNMP Varbind 6, in enclosure SNMP Varbind 5, in rack SNMP Varbind 3.
1.3.6.1.4.1.232.0.22022	Server power on prevented to preserve redundancy in blade SNMP Varbind 6, in enclosure SNMP Varbind 5, in rack SNMP Varbind 3.
1.3.6.1.4.1.232.0.22023	Inadequate power to power on blade SNMP Varbind 6, in enclosure SNMP Varbind 5, in rack SNMP Varbind 3.
1.3.6.1.4.1.232.0.22024	Inadequate power to power on blade SNMP Varbind 6, in enclosure SNMP Varbind 5, in rack SNMP Varbind 3.
1.3.6.1.4.1.232.0.22025	Inadequate power to power on blade SNMP Varbind 6, in enclosure SNMP Varbind 5, in rack SNMP Varbind 3.
1.3.6.1.4.1.232.0.22026	Server power on via manual override on blade SNMP Varbind 6,in enclosure SNMP Varbind 5, in rack SNMP Varbind 3.
1.3.6.1.4.1.232.0.22027	Fuse open fuse SNMP Varbind 6, in enclosure SNMP Varbind 5,in rack SNMP Varbind 3.

MIB ID	SNMP Trap Description
1.3.6.1.4.1.232.0.22028	Server blade in SNMP Varbind 6 removed from position SNMP Varbind 7, in enclosure SNMP Varbind 5, in rack SNMP Varbind 3.
1.3.6.1.4.1.232.0.22029	Server blade in SNMP Varbind 6 inserted from position SNMP Varbind 7,in enclosure SNMP Varbind 5,in rack SNMP Varbind 3.
1.3.6.1.4.1.232.0.22030	Power subsystem not load balanced in enclosure SNMP Varbind 5, in rack SNMP Varbind 3.
1.3.6.1.4.1.232.0.22031	Power subsystem DC power problem in enclosure SNMP Varbind 5, in rack SNMP Varbind 3.
1.3.6.1.4.1.232.0.22033	Unknown power consumption in rack SNMP Varbind 3.
1.3.6.1.4.1.232.0.22032	Power subsystem AC facility input power exceeded in enclosure SNMP Varbind 5, in rack SNMP Varbind 3.
1.3.6.1.4.1.232.0.22034	Power subsystem load balancing wire missing for enclosure SNMP Varbind 5, in rack SNMP Varbind 3.
1.3.6.1.4.1.232.0.22035	Power subsystem has too many power enclosures SNMP Varbind 5, in rack SNMP Varbind 3.
1.3.6.1.4.1.232.0.22036	Power subsystem has been improperly configured in enclosure SNMP Varbind 5, in rack SNMP Varbind 3.
1.3.6.1.4.1.232.0.22037	The Onboard Administrator status has been set to degraded.
1.3.6.1.4.1.232.0.22038	The Onboard Administrator status has been set to ok.
1.3.6.1.4.1.232.0.22039	The Onboard Administrator has been removed.
1.3.6.1.4.1.232.0.22042	A server blade e-keying has failed and there is a port mapping problem between a server mezz card and the interconnect, in Blade SNMP Varbind 6, in position SNMP Varbind 7,in enclosure SNMP Varbind 5,in rack SNMP Varbind 3.
1.3.6.1.4.1.232.0.22040	The Onboard Administrator has been inserted.
1.3.6.1.4.1.232.0.22041	The Onboard Administrator has taken the role of primary in enclosure SNMP Varbind 5, in rack SNMP Varbind 3.
1.3.6.1.4.1.232.0.22043	Server blade e-keying has returned to normal operation, in Blade SNMP Varbind 6, in position SNMP Varbind 7, in enclosure SNMP Varbind 5, in rack SNMP Varbind 3.
1.3.6.1.4.1.232.0.22044	The interconnect has been removed from the enclosure, in interconnect SNMP Varbind 6, in position SNMP Varbind 7, in enclosure SNMP Varbind 5, in rack SNMP Varbind 3.
1.3.6.1.4.1.232.0.22045	Interconnect has been inserted into the enclosure, in interconnect SNMP Varbind 6, in position SNMP Varbind 7, in enclosure SNMP Varbind 5, in rack SNMP Varbind 3.
1.3.6.1.4.1.232.0.22046	The interconnect status has been set to failed, in interconnect SNMP Varbind 6, in position SNMP Varbind 7, in enclosure SNMP Varbind 5, in rack SNMP Varbind 3.
1.3.6.1.4.1.232.0.22047	The interconnect status has degraded, in interconnect SNMP Varbind 6, in position SNMP Varbind 7, in enclosure SNMP Varbind 5, in rack SNMP Varbind 3.

MIB ID	SNMP Trap Description
1.3.6.1.4.1.232.0.22048	The interconnect status has been set to ok, in interconnect SNMP Varbind 6, in position SNMP Varbind 7, in enclosure SNMP Varbind 5, in rack SNMP Varbind 3.
1.3.6.1.4.1.232.0.22049	Server Blade requested to low power
1.3.6.1.4.1.232.0.22050	Server Blade has been removed from the enclosure
1.3.6.1.4.1.232.0.22051	Server Blade has been inserted into the enclosure
1.3.6.1.4.1.232.0.22052	cpqRackServerBladeStatusRepaired
1.3.6.1.4.1.232.0.22053	cpqRackServerBladeStatusDegraded
1.3.6.1.4.1.232.0.22054	cpqRackServerBladeStatusCritical
1.3.6.1.4.1.232.0.22055	cpqRackServerBladeGrpCapTimeout
1.3.6.1.4.1.232.0.22056	cpqRackServerBladeUnexpectedShutdown
1.3.6.1.4.1.232.0.22057	cpqRackServerBladeMangementControllerFirmwareUpdating
1.3.6.1.4.1.232.0.22058	cpqRackServerBladeMangementControllerFirmwareUpdateComplete
1.3.6.1.4.1.232.0.22059	cpqRackServerBladeSystemBIOSFirmwareUpdating
1.3.6.1.4.1.232.0.22060	cpqRackServerBladeSystemBIOSFirmwareUpdateCompleted
1.3.6.1.4.1.232.0.22061	cpqRackServerBladeFrontIOBlankingActive
1.3.6.1.4.1.232.0.22062	cpqRackServerBladeRemoteFrontIOBlankingInactive
1.3.6.1.4.1.232.0.22063	cpqRackServerBladeDiagnosticAdaptorInserted
1.3.6.1.4.1.232.0.22064	cpqRackServerBladeDiagnosticAdaptorRemoved
	cpqRackServerBladeDiagnosticAdaptorRemoved
1.3.6.1.4.1.232.0.22065	cpqRackServerBladeEnteredPXEBootMode
1.3.6.1.4.1.232.0.22066	cpqRackServerBladeExitedPXEBootMode
1.3.6.1.4.1.232.0.22067	cpqRackServerBladeWarmReset
1.3.6.1.4.1.232.0.22068	cpqRackServerBladePOSTCompleted
1.3.6.1.4.1.232.0.22069	cpqRackServerBladePoweredOn
1.3.6.1.4.1.232.0.22070	cpqRackServerBladePoweredOff
1.3.6.1.4.1.232.0.22071	cpqRackInformationalEAETrap
1.3.6.1.4.1.232.0.22072	cpqRackMinorEAETrap
1.3.6.1.4.1.232.0.22073	cpqRackMajorEAETrap
1.3.6.1.4.1.232.0.22074	cpqRackCriticalEAETrap
1.3.6.1.4.1.232.0.22075	cpqRackPowerMinorEAETrap
1.3.6.1.4.1.232.0.22076	cpqRackPowerMajorEAETrap
1.3.6.1.4.1.232.0.22077	cpqRackPowerCriticalEAETrap

The policy contains a rule for each of these SNMP traps. After the problem is resolved the previous alert message is automatically acknowledged.

UPS Traps Monitor Policy

SI-HPProLiant_CPQUPSTraps

The SI-HPProLiant_CPQUPSTraps policy intercepts SNMP traps related to Uninterrupted Power Supply (UPS) in terms of status, battery, and actions initiated by UPS. The policy sends an alert to the HPOM console every time a trap is generated.

It monitors the following traps:

MIB ID	SNMP Trap Description
1.3.6.1.4.1.232.0.12001	UPS reports AC line power failure.
1.3.6.1.4.1.232.0.12002	UPS reports AC line power has returned.
1.3.6.1.4.1.232.0.12003	UPS has initiated server shutdown.
1.3.6.1.4.1.232.0.12004	Server now operational after UPS shutdown.
1.3.6.1.4.1.232.0.12005	UPS battery low server will soon lose power.
1.3.6.1.4.1.232.0.12006	UPS reports AC line power failure.
1.3.6.1.4.1.232.0.12007	UPS reports AC line power has returned.
1.3.6.1.4.1.232.0.12008	UPS has initiated server shutdown.
1.3.6.1.4.1.232.0.12009	Server now operational after UPS shutdown.
1.3.6.1.4.1.232.0.12010	UPS battery is low server will soon lose power.
1.3.6.1.4.1.232.0.12011	UPS has been overloaded.
1.3.6.1.4.1.232.0.12012	UPS battery is about to fail.
1.3.6.1.4.1.232.0.12013	cpqUpsGenericCritical
1.3.6.1.4.1.232.0.12014	cpqUpsGenericInfo

The policy contains a rule for each of these SNMP traps. After the problem is resolved the previous alert message is automatically acknowledged.

Blade Type 2 Traps Monitor Policy

SI-HPProLiant_BladeType2Traps

The SI-HPProLiant_BladeType2Traps policy intercepts SNMP traps related to Blade Type 2. The policy sends an alert to the HPOM console every time a trap is generated.

It monitors the following traps:

MIB ID	SNMP Trap Description
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.1	bt2SwPrimaryPowerSupplyFailure
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.35	bt2SwUfdfoLtMUP
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.32	bt2SwFanFailure

MIB ID	SNMP Trap Description
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.48	bt2SwHotlinksBackupUp
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.46	bt2SwHotlinksMasterUp
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.17	bt2SwVrrpNewBackup
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.36	bt2SwUfdfoGlobalEna
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.28	bt2SwSaveComplete
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.37	bt2SwUfdfoGlobalDis
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.2	bt2SwDefGwUp
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.47	bt2SwHotlinksMasterDn
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.38	bt2SwUfdfoLtDAutoEna
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.5	bt2SwDefGwNotInService
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.41	bt2SwCubeRemoved
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.49	bt2SwHotlinksBackupDn
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.27	bt2SwApplyComplete
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.45	bt2SwCistTopologyChanged
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.16	bt2SwVrrpNewMaster
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.40	bt2SwCubeInserted
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.29	bt2SwFwDownloadSucess
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.18	bt2SwVrrpAuthFailure
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.34	bt2SwUfdfoLtMFailure
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.44	bt2SwStgTopologyChanged
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.3	bt2SwDefGwDown
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.4	bt2SwDefGwInService
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.42	bt2SwStgNewRoot
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.50	bt2SwHotlinksNone
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.22	bt2SwTempExceedThreshold
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.31	bt2SwTempReturnThreshold
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.39	bt2SwUfdfoLtDAutoDis
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.30	bt2SwFwDownloadFailure
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.33	bt2SwFanFailureFixed
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.43	bt2SwCistNewRoot
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.26	bt2SwRackLocationChange
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.19	bt2SwLoginFailure

The policy contains a rule for each of these SNMP traps. After the problem is resolved the previous alert message is automatically acknowledged.

Storage Systems Traps Monitor Policy

SI-HPProLiant_CPQSSTraps

The SI-HPProLiant_CPQSSTraps policy intercepts SNMP traps related to storage systems in terms of fan status, temperature, and power supply. The policy sends an alert to the HPOM console every time a trap is generated.

It monitors the following traps:

MIB ID	SNMP Trap Description
1.3.6.1.4.1.232.0.8001	Storage System fan status changed to OK, status contained in SNMP Varbind 1.
	Storage System fan status changed to FAILED, status contained in SNMP Varbind 1.
	Storage System fan status changed to DEGRADED, status contained in SNMP Varbind 1.
	This unit does not support fan monitoring, status contained in SNMP Varbind 1.
1.3.6.1.4.1.232.0.8002	Storage System will be shutdown because of temperature failure.
1.3.6.1.4.1.232.0.8003	Storage System temperature DEGRADED.
1.3.6.1.4.1.232.0.8004	Storage System temperature OK.
1.3.6.1.4.1.232.0.8005	Storage System side panel is reinstalled on unit.
1.3.6.1.4.1.232.0.8006	Storage System side panel is removed from unit.
1.3.6.1.4.1.232.0.8007	Storage System power supply unit has become degraded.
1.3.6.1.4.1.232.0.8008	Storage System fan status changed to OK, status is contained in SNMP Varbind 3.
	Storage System fan status changed to FAILED, status is contained in SNMP Varbind 3.
	Storage System fan status changed to DEGRADED, status is contained in SNMP Varbind 3.
	Storage System fan status changed to NO FAN, status is contained in SNMP Varbind 3.
1.3.6.1.4.1.232.0.8009	Storage System Temperature Failure.
1.3.6.1.4.1.232.0.8010	Storage System temperature DEGRADED.
1.3.6.1.4.1.232.0.8011	Storage System temperature OK.
1.3.6.1.4.1.232.0.8012	Storage System side panel is reinstalled on unit.
1.3.6.1.4.1.232.0.8013	Storage System side panel is removed from unit.
1.3.6.1.4.1.232.0.8014	Storage System power supply unit has become DEGRADED.
1.3.6.1.4.1.232.0.8015	Storage System power supply unit has become DEGRADED.

MIB ID	SNMP Trap Description
1.3.6.1.4.1.232.0.8016	Storage System fan status changed to NOT INSTALLED, status is contained in SNMP Varbind 6.
	Storage System fan status changed to OK, status is contained in SNMP Varbind 6.
	Storage System fan status changed to DEGRADED, status is contained in SNMP Varbind 6.
	Storage System fan status changed to FAILED, status is contained in SNMP Varbind 6.
1.3.6.1.4.1.232.0.8017	Storage System power supply status changed to NOT INSTALLED, status is contained in SNMP Varbind 6.
	Storage System power supply status changed to OK, status is contained in SNMP Varbind 6.
	Storage System power supply status changed to FAILED, status is contained in SNMP Varbind 6.
	Storage System power supply status changed to DEGRADED, status is contained in SNMP Varbind 6.
1.3.6.1.4.1.232.0.8018	Storage System power supply UPS status changed to OK, status is contained in SNMP Varbind 6.
	Storage System power supply UPS status changed to NO UPS, status is contained in SNMP Varbind 6.
	Storage System power supply UPS status changed to Power FAILED, status is contained in SNMP Varbind 6.
	Storage System power supply UPS status changed to Battery low, status is contained in SNMP Varbind 6.
1.3.6.1.4.1.232.0.8019	Storage System temperature sensor status has changed to OK, status is contained in SNMP Varbind 6.
	Storage System temperature sensor status has changed to DEGRADED, status is contained in SNMP Varbind 6.
	Storage System temperature sensor status has changed to FAILED, status is contained in SNMP Varbind 6.
1.3.6.1.4.1.232.0.8020	Storage System fan status changed to OK, status is contained in SNMP Varbind 6.
	Storage System fan status changed to NOT INSTALLED, status is contained in SNMP Varbind 6.
	Storage System fan status changed to DEGRADED, status is contained in SNMP Varbind 6.
	Storage System fan status changed to FAILED, status is contained in SNMP Varbind 6.

MIB ID	SNMP Trap Description
1.3.6.1.4.1.232.0.8021	Storage System power supply status changed to OK, status is contained in SNMP Varbind 6.
	Storage System power supply status changed to FAILED, status is contained in SNMP Varbind 6.
	Storage System power supply status changed to NOT INSTALLED, status is contained in SNMP Varbind 6.
	Storage System power supply status changed to DEGRADED, status is contained in SNMP Varbind 6.
1.3.6.1.4.1.232.0.8022	Storage System fan status changed to OK, status is contained in SNMP Varbind 9.
	Storage System fan status changed to DEGRADED, status is contained in SNMP Varbind 9.
	Storage System fan status changed to FAILED, status is contained in SNMP Varbind 9.
	Storage System fan status changed to Not Supported, status is contained in SNMP Varbind 9.
	Storage System fan status changed to degraded-Fan1FAILED, status is contained in SNMP Varbind 9.
	Storage System fan status changed to degraded-Fan2FAILED, status is contained in SNMP Varbind 9.
1.3.6.1.4.1.232.0.8023	Storage System temperature status changed to OK, status is contained in SNMP Varbind 9.
	Storage System temperature status changed to DEGRADED, status is contained in SNMP Varbind 9.
	Storage System temperature status changed to FAILED, status is contained in SNMP Varbind 9.
	Storage System temperature status changed to NO TEMP, status is contained in SNMP Varbind 9.
	Storage System temperature status changed to not supported, status is contained in SNMP Varbind 9.

MIB ID	SNMP Trap Description
1.3.6.1.4.1.232.0.8024	Storage System power supply status changed to OK, status is contained in SNMP Varbind 9.
	Storage System power supply status changed to DEGRADED, status is contained in SNMP Varbind 9.
	Storage System power supply status changed to FAILED, status is contained in SNMP Varbind 9.
	Storage System power supply status changed to noFltTolPower, status is contained in SNMP Varbind 9.
	Storage System power supply status changed to not supported, status is contained in SNMP Varbind 9.
	Storage System power supply status changed to noFltTolPower-Bay1Missing, status is contained in SNMP Varbind 9.
	Storage System power supply status changed to noFltTolPower-Bay2Missing, status is contained in SNMP Varbind 9.
	Storage System power supply status changed to OK, status is contained in SNMP Varbind 9.
1.3.6.1.4.1.232.8.0.1	Storage System fan status changed to OK, status is contained in SNMP Varbind 1.
	Storage System fan status changed to FAILED, status is contained in SNMP Varbind 1.
	Storage System fan status changed to DEGRADED, status is contained in SNMP Varbind 1.

MIB ID	SNMP Trap Description
1.3.6.1.4.1.232.0.8025	Storage system recovery server option status changed to DEAMON DOWN DISABLED, status is contained in SNMP Varbind 5.
	Storage system recovery server option status changed to OK, status is contained in SNMP Varbind 5.
	Storage system recovery server option status changed to DEAMON DOWN ACTIVE, status is contained in SNMP Varbind 5.
	Storage system recovery server option status changed to NOSECONDARY, status is contained in SNMP Varbind 5.
	Storage system recovery server option status changed to DEAMON DOWN NOSECONDARY, status is contained in SNMP Varbind 5.
	Storage system recovery server option status changed to LINKDOWN, status is contained in SNMP Varbind 5.
	Storage system recovery server option status changed to DEAMON DOWN LINKDOWN, status is contained in SNMP Varbind 5.
	Storage system recovery server option status changed to SECONDARY RUNNING AUTO, status is contained in SNMP Varbind 5.
	Storage system recovery server option status changed to SECONDARY RUNNING USER, status is contained in SNMP Varbind 5.
	Storage system recovery server option status changed to NOT CONFIGURED, status is contained in SNMP Varbind 5.
	Storage system recovery server option status changed to NOT SUPPORTED, status is contained in SNMP Varbind 5.
	Storage system recovery server option status changed to DISABLED, status is contained in SNMP Varbind 5.
	Storage system recovery server option status changed to evTimeOutError, status is contained in SNMP Varbind 5.
1.3.6.1.4.1.232.0.8026	Storage System fan status changed to OK, status is contained in SNMP Varbind 9.
	Storage System fan status changed to FAILED, status is contained in SNMP Varbind 9.
	Storage System fan status changed to DEGRADED, status is contained in SNMP Varbind 9.
	Storage System fan status changed to NO FAN, status is contained in SNMP Varbind 9.

MIB ID	SNMP Trap Description
1.3.6.1.4.1.232.0.8027	Storage System temperature status is DEGRADED, status is contained in SNMP Varbind 9.
	Storage System temperature status is FAILED, status is contained in SNMP Varbind 9.
	Storage System temperature status is OK, status is contained in SNMP Varbind 9.
	Storage System temperature status changed to NO TEMP, status is contained in SNMP Varbind 9.
1.3.6.1.4.1.232.0.8028	Storage System power supply unit status is DEGRADED, status is contained in SNMP Varbind 9
	Storage System power supply unit status is FAILED, status is contained in SNMP Varbind 9.
	Storage System power supply unit status is OK, status is contained in SNMP Varbind 9.
	Storage System power supply unit status is noFltTolPower, status is contained in SNMP Varbind 9.
1.3.6.1.4.1.232.0.8029	Storage System fan status changed to OK, status is contained in SNMP Varbind 9.
	Storage System fan status changed to FAILED, status is contained in SNMP Varbind 9.
	Storage System fan status changed to DEGRADED, status is contained in SNMP Varbind 9.
	Storage System fan status changed to NO FAN, status is contained in SNMP Varbind 9.
1.3.6.1.4.1.232.0.8030	Storage System temperature status changed to OK, status is contained in SNMP Varbind 9.
	Storage System temperature status changed to DEGRADED, status is contained in SNMP Varbind 9.
	Storage System temperature status changed to FAILED, status is contained in SNMP Varbind 9.
	Storage System temperature status changed to NO TEMP, status is contained in SNMP Varbind 9.
1.3.6.1.4.1.232.0.8031	Storage System power supply status changed to DEGRADED, status is contained in SNMP Varbind 9.
	Storage System power supply status changed to FAILED, status is contained in SNMP Varbind 9.
	Storage System power supply status changed to noFltTolPower, status is contained in SNMP Varbind 9.

The policy contains a rule for each of these SNMP traps. After the problem is resolved the previous alert message is automatically acknowledged.

Virtual Connect Module Traps Monitor Policy

SI-HPProLiant_VCModuleTraps

The SI-HPProLiant_VCModuleTraps policy intercepts the SNMP trap related to virtual connect module. The policy sends an alert to the HPOM console every time the trap is generated.

It monitors the following trap:

MIB ID	SNMP Trap Description
1.3.6.1.4.1.11.5.7.5.2.3.2.11	vcModPortInputUtilizationUp

The policy contains a rule for this SNMP trap. After the problem is resolved the previous alert message is automatically acknowledged.

SIM Agent Process Monitoring Policy

SI-SIMAgentProcessMonitor

The SI-SIMAgentProcessMonitor policy is a measurement threshold policy that checks if the IM agent is installed. The policy runs every five minutes and sends a message to the HPOM console if the IM agent is uninstalled or down.

Capacity Policies

Capacity monitoring helps to deliver performance at the required service level and cost. It ensures that the capacity of the IT infrastructure corresponds to the evolving demands of the business. It helps identify the under utilized and over utilized resources. Monitoring these aspects over a period of time is beneficial in understanding the impact on IT resource utilization. You can analyze current and historical performance of systems resources to accurately predict future capacity needs. The default policy group for these policies is:

Infrastructure Management → <*language*> → **Systems Infrastructure** → **Capacity**

Disk Capacity Monitor Policy

SI-DiskCapacityMonitor

This policy monitors capacity parameters of the disks on the managed node. For each disk, the policy checks for space utilization and free space available. In case the free space availability or space utilization exceeds the threshold values specified, the policy sends out an alert to the HPOM console.

This policy supports the use of wildcard characters '*' and '?' and using default values for all the script parameters. For more information, see Using wildcard characters '*' and '?' for all script parameters and Using default values for all script parameters.

Metrics Used	• FS_MAX_SIZE • FS_SPACE_USED • FS_SPACE_UTIL
Supported Platforms	• Microsoft Windows • Red Hat Enterprise Linux • Suse Linux Enterprise Server • HP-UX • IBM AIX • Oracle Solaris

Script-Parameter	**Description**
SpaceUtilCriticalThreshold	The threshold is expressed as the space utilized on the disk. Set the threshold value at which you want to receive a critical message.
SpaceUtilMajorThreshold	Set the threshold value at which you want to receive a major message.
SpaceUtilMinorThreshold	Set the threshold value at which you want to receive a minor message.
SpaceUtilWarningThreshold	Set the threshold value at which you want to receive a warning message.
FreeSpaceCriticalThreshold	The threshold is expressed as the free space (in MBs) available on the disk or filesystem. Set the threshold value for minimum free space on the disk, below which you want to receive a critical message.
FreeSpaceMajorThreshold	Set the threshold value for minimum free space on the disk, below which you want to receive a major message.
FreeSpaceMinorThreshold	Set the threshold value for minimum free space on the disk, below which you want to receive a minor message.
FreeSpaceWarningThreshold	Set the threshold value for minimum free space on the disk, below which you want to receive a warning message.
MessageGroup	Message group for outgoing messages.
ExcludeFilesystems	Specify the filesystems that need to be excluded from monitoring.
Debug	Set the value as **`0`** to disable trace messages, as **`1`** to receive trace messages on the console, and as **`2`** to log the messages in the trace file on the managed node. For details, see Tracing.

You can set different thresholds for the drives or filesystems on the managed node. The policy parameters can take multiple comma separated values for setting these thresholds. These are described in the following examples:

- **`FreeSpaceMinorThreshold 45`**

In this example, the threshold value is set at 45 MB for all disks or filesystems on the managed node. If the free space available on disks or filesystems falls below the threshold value, the policy sends a minor severity alert.

- **`SpaceUtilCriticalThreshold /=65,95,c:=65`**

In this example, the threshold values are set at 65% for the '/' and '*C:*' drives, and 95% for all other drives/filesystems on the managed node. If the system utilization for these drives/filesystems exceeds the threshold values, the policy sends out a critical alert.

- **`FreeSpaceMajorThreshold E:=200,256,F:=512,c:=1024,/=1024`**

In this example, the threshold values are set at 200 for '*E:*' drive, 512 for '*F:*' drive, 1024 for '*C:*' drive, 1024 for '/' drive, and 256 for the remaining drives on the managed node. If the free space available falls below the threshold values, the policy sends a major alert.

Using wildcard characters '*' and '?' for all script parameters

Use '*' to match one or more characters and '?' to match exactly one character. These are described in the following examples:

- **`ExcludeFilesystems=/,/boot,/v*/?log`**

In this example, filesystems '/', '/boot' and filesystem such as '/var/vlog' that match the pattern '/v*/?log', are excluded from monitoring.

The following examples show the use of wildcard characters for filesystems:

- **`/var/*`** match filesystems with names **`/var/1, /var/log, /var/log/tmp`**.
- **`/var/?`** match filesystems with names **`/var/a, /var/b`** but does not match filesystems with names **`/var/abc, /var/xyzh`**.
- **`/var/??log`** match filesystems with names **`/var/ablog, /var/fslog`** but does not match filesystems with names **`/var/alog, /var/log`**.
- **`/var*/?log`** match filesystems with names **`/var1/alog, /var123/blog`** but does not match filesystems with names **`/var/log, /var123/log, /var/1log.`**

Using default values for all script parameters

Specify default values for the script parameters. The policies only work if there are default values without overriding the filesystem names. These are described in the following examples:

- **`SpaceUtilMinorThreshold=80,/=30,/boot=40`**

In this example, 30 is the threshold for '/', 40 is the threshold for '/boot' and 80 is the default threshold for the rest of the filesystems.

- **`SpaceUtilMinorThreshold=/=30`**

In this example, such parameters are not allowed; you should always specify a default value.

Swap Capacity Monitor Policy

SI-SwapCapacityMonitor

This policy monitors the swap space utilization of the system.

Metrics Used	• GBL_SWAP_SPACE_AVAIL • GBL_SWAP_SPACE_UTIL
Supported Platforms	• Microsoft Windows • Red Hat Enterprise Linux • Suse Linux Enterprise Server • HP-UX • IBM AIX • Oracle Solaris
Script-Parameter	**Description**
SwapSpaceUtilCriticalThreshold	The threshold is expressed as the percentage (0 to 100%) of swap space utilization on the node. Set the threshold value for minimum free swap space on the disk at which you want to receive a critical severity message.
SwapSpaceUtilMajorThreshold	Set the threshold value for minimum swap space utilized on the node at which you want to receive a major severity message.
SwapSpaceUtilMinorThreshold	Set the threshold value for minimum space utilized on the node at which you want to receive a minor severity message.
SwapSpaceUtilWarningThreshold	Set the threshold value for minimum space utilized on the node at which you want to receive a warning severity message.
FreeSwapSpaceAvailCriticalThreshold	The threshold is expressed as the free swap space (in MBs) available on the disk/filesystem. Set the threshold value for minimum free space on the disk at which you want to receive a critical severity message.
FreeSwapSpaceAvailMajorThreshold	Set the threshold value for minimum free swap space on the disk at which you want to receive a major severity message.
FreeSwapSpaceAvailMinorThreshold	Set the threshold value for minimum free swap space on the disk at which you want to receive a minor severity message.
FreeSwapSpaceAvailWarningThreshold	Set the threshold value for minimum free swap space on the disk at which you want to receive a warning severity message.
MessageGroup	Message group for outgoing messages.
Debug	Set the value as **0** to disable trace messages, as **1** to receive trace messages on the console, and as **2** to log the messages in the trace file on the managed node. For details, see Tracing.

Memory Utilization Monitor Policy

SI-MemoryUtilization-AT

This policy monitors the overall memory usage by operating systems. The policy uses the automatic threshold determination to automatically calculate the threshold values according to the memory usage on previous days.

This policy relies on historical data. For accurate results, deploy the policy only after a week of data collection by the performance agent.

Metrics Used	GBL_MEM_UTIL
Supported Platforms	• Microsoft Windows • Red Hat Enterprise Linux • Suse Linux Enterprise Server • HP-UX • IBM AIX • Oracle Solaris
Script-Parameter	**Description**
MessageApplication	Type an appropriate value that helps you identify the messages sent by the policy to the management console.
DataSource	Displays the HP Embedded Performance Component (EPC) data source name as CODA.
DataObject	Displays the HP Embedded Performance Component (EPC) data object name as Global.
DataMetric	Displays the HP Embedded Performance Component (EPC) metric name as GBL_MEM_UTIL.
BaselinePeriod	Type the time period you want to define as a baseline period, such as '3600 seconds'. This period moves with the current time. The most recent 3600-second (1-hour) period becomes the current baseline period.
MinimumValue	Displays the minimum value of memory consumption as indicated by the metric.
MaximumValue	Displays the maximum value of memory consumption as indicated by the metric.
WarningDeviations	Displays the number of standard deviation away from normal at which the policy will send a warning message to HPOM console. Set an appropriate value for the parameter. To disable the parameter, set value as *5*.
MinorDeviations	Displays the number of standard deviation away from normal at which the policy will send a minor message to HPOM console. Set an appropriate value for the parameter greater than the specified value for WarningDeviations. To disable the parameter, set value as *5*.

MajorDeviations	Displays the number of standard deviation away from normal at which the policy will send a major message to HPOM console. Set an appropriate value for the parameter greater than the specified value for MinorDeviations. To disable the parameter, set value as *5*.
WarningHighSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or exceeds the sample data average by the value specified in *WarningDeviations*. To disable the parameter, set value as *none*.
MinorHighSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or exceeds the sample data average by the value specified in *MinorDeviations*. To disable the parameter, set value as *none*.
MajorHighSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or exceeds the sample data average by the value specified in *MajorDeviations*. To disable the parameter, set value as *none*.
WarningLowSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or falls below the sample data average by the value specified in *WarningDeviations*. To disable the parameter, set value as *none*.
MinorLowSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or falls below the sample data average by the value specified in *MinorDeviations*. To disable the parameter, set value as *none*.
MajorLowSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or falls below the sample data average by the value specified in *MajorDeviations*. To disable the parameter, set value as *none*.
InstanceSource	Do not edit the parameter value.
MemUtilCutOff	Set a value below which you do not want to monitor memory utilization.
DebugLevel	Set the value as **0** to disable trace messages, as **1** to receive trace messages on the console, and as **2** to log the messages in the trace file on the managed node. For details, see Tracing.
MessageGroup	Message group for outgoing messages.

Swap Utilization Monitor Policy

SI-SwapUtilization-AT

This policy monitors the overall swap space used by the systems on the managed node. The policy uses the automatic threshold determination to automatically calculate the threshold values according to the swap space usage on previous days.

This policy relies on historical data. For accurate results, deploy the policy only after a week of data collection by the performance agent.

Metrics Used	GBL_SWAP_SPACE_USED
Supported Platforms	• Microsoft Windows • Red Hat Enterprise Linux • Suse Linux Enterprise Server • HP-UX • IBM AIX • Oracle Solaris
Script-Parameter	**Description**
MessageApplication	Type an appropriate value that helps you identify the messages sent by the policy to the management console.
DataSource	Displays the HP Embedded Performance Component (EPC) data source name as CODA.
DataObject	Displays the HP Embedded Performance Component (EPC) data object name as Global.
DataMetric	Displays the HP Embedded Performance Component (EPC) metric name as GBL_SWAP_SPACE_USED.
BaselinePeriod	Type the time period you want to define as a baseline period, such as '3600 seconds'. This period moves with the current time. The most recent 3600-second (1-hour) period becomes the current baseline period.
MinimumValue	Displays the minimum swap space usage as indicated by the metric.
MaximumValue	Displays the maximum swap space usage as indicated by the metric.
WarningDeviations	Displays the number of standard deviation away from normal at which the policy will send a warning message to HPOM console. Set an appropriate value for the parameter. To disable the parameter, set value as *5*.
MinorDeviations	Displays the number of standard deviation away from normal at which the policy will send a minor message to HPOM console. Set an appropriate value for the parameter greater than the specified value for WarningDeviations. To disable the parameter, set value as *5*.

MajorDeviations	Displays the number of standard deviation away from normal at which the policy will send a major message to HPOM console. Set an appropriate value for the parameter greater than the specified value for MinorDeviations. To disable the parameter, set value as *5*.
WarningHighSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or exceeds the sample data average by the value specified in *WarningDeviations*. To disable the parameter, set value as *none*.
MinorHighSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or exceeds the sample data average by the value specified in *MinorDeviations*. To disable the parameter, set value as *none*.
MajorHighSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or exceeds the sample data average by the value specified in *MajorDeviations*. To disable the parameter, set value as *none*.
WarningLowSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or falls below the sample data average by the value specified in *WarningDeviations*. To disable the parameter, set value as *none*.
MinorLowSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or falls below the sample data average by the value specified in *MinorDeviations*. To disable the parameter, set value as *none*.
MajorLowSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or falls below the sample data average by the value specified in *MajorDeviations*. To disable the parameter, set value as *none*.
InstanceSource	Do not edit the parameter value.
DebugLevel	Set the value as **0** to disable trace messages, as **1** to receive trace messages on the console, and as **2** to log the messages in the trace file on the managed node. For details, see Tracing.
MessageGroup	Message group for outgoing messages.
SwapUtilCutOff	Set a value below which you do not want to monitor swap utilization.

Per CPU Utilization Monitor Policy

SI-PerCPUUtilization-AT

This policy monitors the utilization for each CPU on the managed node. This policy processes each CPU instance separately for every interval. The policy uses automatic threshold determination to automatically calculate the threshold values according to the CPU utilization on previous days.

This policy relies on historical data. For accurate results, deploy the policy only after a week of data collection by the performance agent.

Metrics Used	BYCPU_CPU_TOTAL_UTIL
Supported Platforms	• Microsoft Windows • Red Hat Enterprise Linux • Suse Linux Enterprise Server • HP-UX • IBM AIX • Oracle Solaris
Script-Parameter	**Description**
MessageApplication	Type an appropriate value that helps you identify the messages sent by the policy to the management console.
DataSource	Displays the HP Embedded Performance Component (EPC) data source name as CODA.
DataObject	Displays the HP Embedded Performance Component (EPC) data object name as Global.
DataMetric	Displays the HP Embedded Performance Component (EPC) metric name as BYCPU_CPU_TOTAL_UTIL.
BaselinePeriod	Type the time period you want to define as a baseline period, such as '3600 seconds'. This period moves with the current time. The most recent 3600-second (1-hour) period becomes the current baseline period.
MinimumValue	Displays the minimum value of CPU consumption as indicated by the metric.
MaximumValue	Displays the maximum value of CPU consumption as indicated by the metric.
WarningDeviations	Displays the number of standard deviation away from normal at which the policy will send a warning message to HPOM console. Set an appropriate value for the parameter. To disable the parameter, set value as *5*.
MinorDeviations	Displays the number of standard deviation away from normal at which the policy will send a minor message to HPOM console. Set an appropriate value for the parameter greater than the specified value for WarningDeviations. To disable the parameter, set value as *5*.

MajorDeviations	Displays the number of standard deviation away from normal at which the policy will send a major message to HPOM console. Set an appropriate value for the parameter greater than the specified value for MinorDeviations. To disable the parameter, set value as *5*.
WarningHighSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or exceeds the sample data average by the value specified in *WarningDeviations*. To disable the parameter, set value as *none*.
MinorHighSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or exceeds the sample data average by the value specified in *MinorDeviations*. To disable the parameter, set value as *none*.
MajorHighSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or exceeds the sample data average by the value specified in *MajorDeviations*. To disable the parameter, set value as *none*.
WarningLowSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or falls below the sample data average by the value specified in *WarningDeviations*. To disable the parameter, set value as *none*.
MinorLowSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or falls below the sample data average by the value specified in *MinorDeviations*. To disable the parameter, set value as *none*.
MajorLowSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or falls below the sample data average by the value specified in *MajorDeviations*. To disable the parameter, set value as *none*.
InstanceSource	Do not edit the parameter value.
DebugLevel	Set the value as **0** to disable trace messages, as **1** to receive trace messages on the console, and as **2** to log the messages in the trace file on the managed node. For details, see Tracing.
MessageGroup	Message group for outgoing messages.
CPUUtilCutOff	Set a value below which you do not want to monitor CPU utilization.

Remote Drive Space Utilization Monitor Policy

SI-MSWindowsRemoteDriveSpaceUtilization

The SI-MSWindowsRemoteDriveSpaceUtilization policy monitors space utilization level for remote drives on Microsoft Windows platform. The default policy group for the policy is:

Infrastructure Management → *<language>* → Systems Infrastructure → Capacity → Windows

Source Type	WMI
Supported Platforms	Microsoft Windows
Script-Parameter	**Description**
SpaceUtilCriticalThreshold	The threshold is expressed as the percentage (0 to 100%) of space utilization on the monitored remote drive. Set the threshold value for minimum free space on the drive at which you want to receive a critical severity message.
SpaceUtilMajorThreshold	Set the threshold value for minimum free space on the drive at which you want to receive a major severity message.
SpaceUtilMinorThreshold	Set the threshold value for minimum free space on the drive at which you want to receive a minor severity message.
SpaceUtilWarningThreshold	Set the threshold value for minimum free space on the drive at which you want to receive a warning severity message.
MessageGroup	Message group for outgoing messages.
Debug	Set the value as `0` to disable trace messages, as `1` to receive trace messages on the console, and as `2` to log the messages in the trace file on the managed node. For details, see Tracing.
AssignMessageToRemoteHost	Set the value to 1 to display the source of the alert message as the remote host. By default, the messages are assigned to the managed node from which the message is sent out.

Remote Drive Space Utilization Monitor Policy for NFS filesystems

SI-LinuxNfsUtilizationMonitor

The SI-LinuxNfsUtilizationMonitor policy monitors space utilization level for NFS remote filesystems on Linux platforms. The default policy group for the policy is:

Infrastructure Management → *<language>* → Systems Infrastructure → Capacity → Linux

Supported Platforms	• Red Hat Enterprise Linux • Suse Linux Enterprise Server
Script-Parameter	**Description**
SpaceUtilCriticalThreshold	The threshold is expressed as the percentage (0 to 100%) of space utilization on the monitored remote filesystem. Set the threshold value for minimum free space on the filesystem at which you want to receive a critical severity message.

SpaceUtilMajorThreshold	Set the threshold value for minimum free space on the filesystem at which you want to receive a major severity message.
SpaceUtilMinorThreshold	Set the threshold value for minimum free space on the filesystem at which you want to receive a minor severity message.
SpaceUtilWarningThreshold	Set the threshold value for minimum free space on the filesystem at which you want to receive a warning severity message.
NfsFileSystemType	Specify the filesystem type that you would like to monitor for space utilization level. For example, if you specify NFS, the policy will monitor all NFS remote filesystems for space utilization level.
AssignMessageToRemoteHost	Set the value to 1 to display the source of the alert message as the remote host. By default, the messages are assigned to the managed node from which the message is sent out.
MessageGroup	Message group for outgoing messages.
Debug	Set the value as **0** to disable trace messages, as **1** to receive trace messages on the console, and as **2** to log the messages in the trace file on the managed node. For details, see Tracing.

Remote Drive Space Utilization Monitor Policy for CIFS filesystems

SI-LinuxCifsUtilizationMonitor

The SI-LinuxCifsUtilizationMonitor policy monitors space utilization level for CIFS remote filesystems on Linux platforms. The default policy group for the policy is:

Infrastructure Management → *<language>* → Systems Infrastructure → Capacity → Linux

Supported Platforms	• Red Hat Enterprise Linux • Suse Linux Enterprise Server
Script-Parameter	**Description**
SpaceUtilCriticalThreshold	The threshold is expressed as the percentage (0 to 100%) of space utilization on the monitored remote filesystem. Set the threshold value for minimum free space on the filesystem at which you want to receive a critical severity message.
SpaceUtilMajorThreshold	Set the threshold value for minimum free space on the filesystem at which you want to receive a major severity message.
SpaceUtilMinorThreshold	Set the threshold value for minimum free space on the filesystem at which you want to receive a minor severity message.

SpaceUtilWarningThreshold	Set the threshold value for minimum free space on the filesystem at which you want to receive a warning severity message.
CifsFileSystemType	Specify the filesystem type that you would like to monitor for space utilization level. For example, if you specify CIFS, the policy will monitor all CIFS remote filesystems for space utilization level. The policy can be used to monitor *cifs* and *smb* file system types.
AssignMessageToRemoteHost	Set the value to 1 to display the source of the alert message as the remote host. By default, the messages are assigned to the managed node from which the message is sent out.
MessageGroup	Message group for outgoing messages.
Debug	Set the value as **0** to disable trace messages, as **1** to receive trace messages on the console, and as **2** to log the messages in the trace file on the managed node. For details, see Tracing.

Paged and Nonpaged Pool Utilization Policy

SI-MSWindowsPagedPoolUtilization and **SI-MSWindowsNonPagedPoolUtilization**

The SI-MSWindowsPagedPoolUtilization policy monitors the memory when the registry data is written to the paging file. The SI-MSWindowsNonPagedPoolUtilization policy monitors the memory that stores the data when the system is unable to handle page faults. The default policy group for the policy is:

Infrastructure Management → *<language>* → Systems Infrastructure → Capacity → Windows

Metrics Used	• GBL_MEM_PAGED_POOL_BYTES • GBL_MEM_NONPAGED_POOL_BYTES
Supported Platforms	Microsoft Windows
Script-Parameter	**Description**
BaselinePeriod	Type the time period you want to define as a baseline period, such as '900 seconds'. This period moves with the current time. The most recent 900-second period becomes the current baseline period.

WarningDeviations	Displays the number of standard deviation away from normal at which the policy will send a warning message to HPOM console. Set an appropriate value for the parameter. To disable the parameter, set value as *4.5*.
MinorDeviations	Displays the number of standard deviation away from normal at which the policy will send a minor message to HPOM console. Set an appropriate value for the parameter greater than the specified value for WarningDeviations. To disable the parameter, set value as *5.5*
MajorDeviations	Displays the number of standard deviation away from normal at which the policy will send a major message to HPOM console. Set an appropriate value for the parameter greater than the specified value for MinorDeviations. To disable the parameter, set value as *7.5*.

Log Monitoring Policies

SI SPI provides logfile policies to monitor crucial logs for the managed nodes. The default policy group for these policies is:

Infrastructure Management → *<language>* → Systems Infrastructure → Logs

Linux System Services Logfile Policies

The Linux system services logfile policies monitor the crucial system service logs for Red Hat and Suse enterprise Linux editions. The default policy group for these policies is:

Infrastructure Management → *<language>* → Systems Infrastructure → Logs → Linux

Boot Log Policy

SI-LinuxBootLog

This policy monitors the boot log file `/var/log/boot.log` and alerts in case of any system boot errors. The default polling interval is 5 minutes.

This policy checks for the following conditions:

Condition	Description
Service startup failed	Checks for error conditions that match the `<*> <@.service>: <@.daemon> startup failed` pattern in the boot log file. If any matches are found, this condition sends a message with minor severity to the HPOM console with the appropriate message attributes.
Service failed	Checks for error conditions that match the `<*> <@.service>: <*.msg> failed` pattern in the log file. If any matches are found, this condition sends a message with critical severity to the HPOM console with the appropriate message attributes.

Secure Log Policy

SI-LinuxSecureLog

This policy monitors the log file in `/var/log/secure and /var/log/messages,` and alerts in case of any secure login failure. The default polling interval is 5 minutes.

This policy checks for the following condition:

Condition	Description
Authentication failure	Checks for error conditions that match the `<*> sshd\[<#>\]: Failed password for <@.user> from <*.host> port <#> ssh2` pattern in the secure log file. If any matches are found, this condition sends a message with minor severity to the HPOM console with the appropriate message attributes.

Kernel Log Policy

SI-LinuxKernelLog

This policy monitors the kernel log file `/var/log/messages` and alerts in case of any kernel service failure. The default polling interval is 5 minutes.

This policy checks for the following condition:

Condition	Description
Kernel service failure	Checks for error conditions that match the `<*> kernel: <@.service>: <*.msg> failed` pattern in the kernel log file. If any matches are found, this condition sends a message with minor severity to the HPOM console with the appropriate message attributes.

Windows System Services Logfile Policies

The Windows Server logfile policies monitor the crucial system service logs for Microsoft Windows 2008 or later versions. The default policy group for these policies is:

NFS Log Policy

SI-MSWindowsServer_NFSWarnError

This policy monitors the NFS log file for the NFS server processes and forwards the errors to the HPOM console with a severity level of warning or error. The default polling interval is 1 minute. The policy looks for the following errors recorded in the NFS log file:

- The NFS server detected a low disk space condition and has stopped recording audits.
- The audit log has reached its maximum file size.
- The NFS server could not register with RPC Port Mapper.
- The NFS driver failed during phase 2 initialization.

DNS Log Policy

SI-MSWindowsServer_DNSWarnError

This policy monitors the log file for the Microsoft DNS server service and its corresponding process and forwards the error log entries to the HPOM console with a severity level of warning or error. The default polling interval is 1 minute. The policy looks for the following errors recorded in the DNS log file:

- The DNS server could not allocate memory for the resource record.
- The DNS server was unable to service a client request due a shortage of available memory.
- The DNS server could not create a zone transfer thread.
- The DNS server encountered an error while writing to a file.
- The DNS server could not initialize the remote procedure call (RPC) service.

Windows Logon Policy

SI-MSWindowsServer_WindowsLogonWarnError

This policy monitors the Windows logon and initialization event logs and forwards the error log entries to the HPOM console with a severity level of warning or error. The default polling interval is 1 minute. The policy looks for the following errors recorded in the Windows log file:

- Windows license is invalid
- Windows license activation failed
- The Windows logon process has failed to switch the desktop
- The Windows logon process has unexpectedly terminated
- The Windows logon process has failed to spawn a user application
- The Windows logon process has failed to terminate currently logged on user's processes
- The Windows logon process has failed to disconnect the user session

Terminal Service Log Policy

SI-MSWindowsServer_TerminalServiceWarnError

This policy monitors the log file for Windows Terminal service and its corresponding process and forwards the error log entries to the HPOM console with a severity level of warning or error. The default polling interval is 1 minute. The policy looks for the following errors recorded in the Windows Terminal service log file:

- A connection request was denied because the terminal server is currently configured to not accept connections
- Auto-reconnect failed to reconnect the user to the session because authentication failed
- Terminal service failed to start
- The terminal server received large number of incomplete connections

Windows Server DHCP Error

SI-MSWindowsServer_DHCPWarnError

This policy monitors the log file for DHCP server and client services and their corresponding processes, and forwards the error log entries to the HPOM console with a severity level of warning or error. The default polling interval is 1 minute. The policy looks for the following errors recorded in the Windows Terminal service log file:

- Iashlpr cannot contact the NPS service
- There are no IP addresses available for BOOTP clients in the scope or superscope
- The DHCP server is unable to reach the NPS server for determining the client's NAP access state
- There are no IP addresses available for lease in the scope or superscope
- The DHCP/BINL service on the local computer has determined that it is not authorized to start
- The DHCP service failed to initialize the audit log
- The DHCP/BINL service on this workgroup server has encountered another server with IP Address
- The DHCP service failed to restore the DHCP registry configuration
- The DHCP service was unable to read the global BOOTP file name from the registry
- The DHCP service is not servicing any clients because there are no active interfaces.
- There is no static IP address bound to the DHCP server
- The DHCP server service failed to register with Service Controller
- The DHCP server service failed to initialize its registry parameters

AIX System Logfile Monitoring Policies

The AIX system logfile monitoring policies monitors the crucial system faults. The default policy group for these policies is:

Infrastructure Management → *<language>* → Systems Infrastructure → Logs → AIX

ERRPT Log Monitoring Policy

SI-AIXErrptLog

The output of 'errpt' command is stored as system errors in the `errpt.log` file. The SI-AIXErrptLog policy monitors the log file and sends the log entries to the HPOM console as messages with severity Warning. The alerts contain error codes, classes, and outages.

Performance Policies

Performance monitoring helps to preempt performance disruption and identify when the infrastructure issues can threaten service quality. You can use the collected performance data to correlate events across the entire infrastructure of servers, operating systems, network devices, and applications in order to prevent or identify the root cause of a developing performance issue.

The default policy group for these policies is:

Infrastructure Management → *<language>* → Systems Infrastructure → Performance

Disk Performance Policy

SI-PerDiskAvgServiceTime-AT

This policy monitors the disk performance on the managed node and sends out an alert when the disk write and read service time violates the threshold levels. It is mandatory that this policy needs Performance Agent to be running on the managed node.

This policy relies on historical data. For accurate results, deploy the policy only after a week of data collection by the performance agent

Metrics Used	BYDSK_AVG_SERVICE_TIME
Supported Platforms	• Microsoft Windows • Red Hat Enterprise Linux • Suse Linux Enterprise Server • HP-UX • IBM AIX • Oracle Solaris
Script-Parameter	**Description**
MessageApplication	Type an appropriate value that helps you identify the messages sent by the SI-PerDiskAvgServiceTime-AT policy to the management console.
DataSource	Displays the HP Embedded Performance Component (EPC) data source name as SCOPE.
DataObject	Displays the HP Embedded Performance Component (EPC) data object name as DISK.
DataMetric	Displays the HP Embedded Performance Component (EPC) metric name as BYDSK_AVG_SERVICE_TIME.
BaselinePeriod	Type the time period you want to define as a baseline period, such as '3600 seconds'. This period moves with the current time. The most recent 3600-second (1-hour) period becomes the current baseline period.
MinimumValue	Displays the minimum average time spent in processing each read or write disk request as indicated by the metric.

MaximumValue	Displays the maximum average time spent in processing each read or write disk request as indicated by the metric.
WarningDeviations	Displays the number of standard deviation away from normal at which the policy will send a warning message to HPOM console. Set an appropriate value for the parameter. To disable the parameter, set value as *5*.
MinorDeviations	Displays the number of standard deviation away from normal at which the policy will send a minor message to HPOM console. Set an appropriate value for the parameter greater than the specified value for WarningDeviations. To disable the parameter, set value as *5*.
MajorDeviations	Displays the number of standard deviation away from normal at which the policy will send a major message to HPOM console. Set an appropriate value for the parameter greater than the specified value for MinorDeviations. To disable the parameter, set value as *5*.
WarningHighSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or exceeds the sample data average by the value specified in *WarningDeviations*. To disable the parameter, set value as *none*.
MinorHighSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or exceeds the sample data average by the value specified in *MinorDeviations*. To disable the parameter, set value as *none*.
MajorHighSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or exceeds the sample data average by the value specified in *MajorDeviations*. To disable the parameter, set value as *none*.
WarningLowSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or falls below the sample data average by the value specified in *WarningDeviations*. To disable the parameter, set value as *none*.
MinorLowSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or falls below the sample data average by the value specified in *MinorDeviations*. To disable the parameter, set value as *none*.

MajorLowSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or falls below the sample data average by the value specified in *MajorDeviations*. To disable the parameter, set value as *none*.
InstanceSource	Do not edit the parameter value.
DebugLevel	Set the value as **0** to disable trace messages, as **1** to receive trace messages on the console, and as **2** to log the messages in the trace file on the managed node. For details, see Tracing.
MessageGroup	Message group for outgoing messages.
DiskIOCutOff	Set a value below which you do not want to monitor the disk write and reads service time.

Global CPU Utilization Monitor Policy

SI-GlobalCPUUtilization-AT

This policy monitors the performance of the CPUs on the managed node and sends out an alert when the utilization across all CPUs violates the threshold levels.

This policy relies on historical data. For accurate results, deploy the policy only after a week of data collection by the performance agent

Metrics Used	GBL_CPU_TOTAL_UTIL
Supported Platforms	• Microsoft Windows • Red Hat Enterprise Linux • Suse Linux Enterprise Server • HP-UX • IBM AIX • Oracle Solaris
Script-Parameter	**Description**
MessageApplication	Type an appropriate value that helps you identify the messages sent by the SI-GlobalCPUUtilization-AT policy to the management console.
DataSource	Displays the HP Embedded Performance Component (EPC) data source name as CODA.
DataObject	Displays the HP Embedded Performance Component (EPC) data object name as GLOBAL.
DataMetric	Displays the HP Embedded Performance Component (EPC) metric name as GBL_CPU_TOTAL_UTIL.

BaselinePeriod	Type the time period you want to define as a baseline period, such as '3600 seconds'. This period moves with the current time. The most recent 3600-second (1-hour) period becomes the current baseline period.
MinimumValue	Displays the minimum percentage of time the CPUs were not idle, as indicated by the metric.
MaximumValue	Displays the maximum percentage of time the CPUs were not idle, as indicated by the metric.
WarningDeviations	Displays the number of standard deviation away from normal at which the policy will send a warning message to HPOM console. Set an appropriate value for the parameter. To disable the parameter, set value as *5*.
MinorDeviations	Displays the number of standard deviation away from normal at which the policy will send a minor message to HPOM console. Set an appropriate value for the parameter greater than the specified value for WarningDeviations. To disable the parameter, set value as *5*.
MajorDeviations	Displays the number of standard deviation away from normal at which the policy will send a major message to HPOM console. Set an appropriate value for the parameter greater than the specified value for MinorDeviations. To disable the parameter, set value as *5*.
WarningHighSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or exceeds the sample data average by the value specified in *WarningDeviations*. To disable the parameter, set value as *none*.
MinorHighSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or exceeds the sample data average by the value specified in *MinorDeviations*. To disable the parameter, set value as *none*.
MajorHighSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or exceeds the sample data average by the value specified in *MajorDeviations*. To disable the parameter, set value as *none*.
WarningLowSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or falls below the sample data average by the value specified in *WarningDeviations*. To disable the parameter, set value as *none*.

MinorLowSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or falls below the sample data average by the value specified in *MinorDeviations*. To disable the parameter, set value as *none*.
MajorLowSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or falls below the sample data average by the value specified in *MajorDeviations*. To disable the parameter, set value as *none*.
InstanceSource	Do not edit the parameter value.
DebugLevel	Set the value as `0` to disable trace messages, as `1` to receive trace messages on the console, and as `2` to log the messages in the trace file on the managed node. For details, see Tracing.
MessageGroup	Message group for outgoing messages.

Run Queue Length Monitor Policy

SI-RunQueueLengthMonitor-AT

This policy monitors the number of processes waiting in the run queue of the CPU and sends out an alert when the number of processes in run queue violates the threshold levels

This policy relies on historical data. For accurate results, deploy the policy only after a week of data collection by the performance agent.

Metrics Used	GBL_RUN_QUEUE
Supported Platforms	• Microsoft Windows • Red Hat Enterprise Linux • Suse Linux Enterprise Server • HP-UX • IBM AIX • Oracle Solaris
Script-Parameter	**Description**
MessageApplication	Type an appropriate value that helps you identify the messages sent by this policy to the management console.
DataSource	Displays the HP Embedded Performance Component (EPC) data source name as CODA.
DataObject	Displays the HP Embedded Performance Component (EPC) data object name as GLOBAL.
DataMetric	Displays the HP Embedded Performance Component (EPC) metric name as GBL_RUN_QUEUE.

BaselinePeriod	Type the time period you want to define as a baseline period, such as '3600 seconds'. This period moves with the current time. The most recent 3600-second (1-hour) period becomes the current baseline period.
MinimumValue	Displays the minimum average number of threads/ processes waiting in the run queue over the interval, as indicated by the metric.
MaximumValue	Displays the maximum average number of threads/ processes waiting in the run queue over the interval, as indicated by the metric.
WarningDeviations	Displays the number of standard deviation away from normal at which the policy will send a warning message to HPOM console. Set an appropriate value for the parameter. To disable the parameter, set value as *5*.
MinorDeviations	Displays the number of standard deviation away from normal at which the policy will send a minor message to HPOM console. Set an appropriate value for the parameter greater than the specified value for WarningDeviations. To disable the parameter, set value as *5*.
MajorDeviations	Displays the number of standard deviation away from normal at which the policy will send a major message to HPOM console. Set an appropriate value for the parameter greater than the specified value for MinorDeviations. To disable the parameter, set value as *5*.
WarningHighSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or exceeds the sample data average by the value specified in *WarningDeviations*. To disable the parameter, set value as *none*.
MinorHighSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or exceeds the sample data average by the value specified in *MinorDeviations*. To disable the parameter, set value as *none*.
MajorHighSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or exceeds the sample data average by the value specified in *MajorDeviations*. To disable the parameter, set value as *none*.
WarningLowSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or falls below the sample data average by the value specified in *WarningDeviations*. To disable the parameter, set value as *none*.

MinorLowSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or falls below the sample data average by the value specified in *MinorDeviations*. To disable the parameter, set value as *none*.
MajorLowSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or falls below the sample data average by the value specified in *MajorDeviations*. To disable the parameter, set value as *none*.
InstanceSource	Do not edit the parameter value.
DebugLevel	Set the value as `0` to disable trace messages, as `1` to receive trace messages on the console, and as `2` to log the messages in the trace file on the managed node. For details, see Tracing.
MessageGroup	Message group for outgoing messages.

Network Usage and Performance Policy

SI-NetworkUsageAndPerformance

This policy monitors the system's network usage and shows error rates and collisions to identify potential network bottlenecks. The SI-NetworkUsageAndPerformance policy monitors the physical NICs of only the vMA machines.

The policy does not monitor performance data for package collision on the Windows operating system, as the BYNETIF_COLLISION metric is not available on it

The following metrics used in this policy require HP Performance Agent to be running on the managed node: BYNETIF_UTIL and BYNETIF_QUEUE.

Metrics Used	• BYNETIF_IN_PACKET • BYNETIF_ID • BYNETIF_OUT_PACKET • BYNETIF_ERROR • BYNETIF_COLLISION • BYNETIF_OUT_BYTE_RATE • BYNETIF_IN_BYTE_RATE • BYNETIF_UTIL • BYNETIF_QUEUE • BYNETIF_NAME
Supported Platforms	• Microsoft Windows • Red Hat Enterprise Linux • Suse Linux Enterprise Server • HP-UX • IBM AIX • Oracle Solaris *The script parameters are applicable on all the above mentioned platforms, unless specified otherwise in the parameter description.*

Script-Parameter	**Description**
NICByteRateCriticalThreshold	This parameter monitors the average number of bytes transferred every second and sends a critical severity message if the value exceeds the threshold. You can set a threshold value at which you want to receive the message.
NICByteRateMajorThreshold	You can set a threshold value for average number of bytes transferred every second at which you want to receive a major severity message.
NICByteRateMinorThreshold	You can set a threshold value for average number of bytes transferred every second at which you want to receive a minor severity message.
NICByteRateWarningThreshold	You can set a threshold value for average number of bytes transferred every second at which you want to receive a warning severity message.
NICErrPktRatePctCriticalThreshold	Packet error rate is the ratio, in percentage, of the number of packets not successfully transmitted, to the total number of packets sent. This parameter monitors the packet error rate and sends a critical severity message if the value exceeds the threshold.
NICErrPktRatePctMajorThreshold	You can set a threshold value for packet error rate at which you want to receive a major severity message.

NICErrPktRatePctMinorThreshold	You can set a threshold value for packet error rate at which you want to receive a minor severity message.
NICErrPktRatePctWarningThreshold	You can set a threshold value for packet error rate at which you want to receive a warning severity message.
NICCollisionRatePctCriticalThreshold	This parameter monitors the ratio, in percentage, of collision packets to the total number of packets transmitted. You can set a threshold value for collision error rate at which you want to receive a critical severity message. *This parameter is not applicable on Windows.*
NICCollisionRatePctMajorThreshold	You can set a threshold value for collision error rate at which you want to receive a critical major message. *This parameter is not applicable on Windows.*
NICCollisionRatePctMinorThreshold	You can set a threshold value for collision error rate at which you want to receive a minor severity message. *This parameter is not applicable on Windows.*
NICCollisionRatePctWarningThreshold	You can set a threshold value for collision error rate at which you want to receive a warning severity message. *This parameter is not applicable on Windows.*
NICOutBoundQueueLengthCriticalThreshold	This parameter denotes the number of packets waiting in the outbound queue length for all network interfaces. Set a threshold value for outbound queue length at which you want to receive a critical severity message. *This parameter is applicable only on HP-UX and Windows.*
NICOutBoundQueueLengthMajorThreshold	Set a threshold value for outbound queue length at which you want to receive a major severity message. *This parameter is applicable only on HP-UX and Windows.*
NICOutBoundQueueLengthMinorThreshold	Set a threshold value for outbound queue length at which you want to receive a minor severity message. *This parameter is applicable only on HP-UX and Windows.*
NICOutBoundQueueLengthWarningThreshold	Set a threshold value for outbound queue length at which you want to receive a warning severity message. *This parameter is applicable only on HP-UX and Windows.*

NICBandwidthUtilCriticalThreshold	This parameter denotes the percentage of bandwidth used with respect to the total available bandwidth. Set a threshold value for bandwidth utilization at which you want to receive a critical severity message. *This parameter is applicable only on HP-UX, AIX, and Windows.*
NICBandwidthUtilMajorThreshold	Set a threshold value for bandwidth utilization at which you want to receive a major severity message. *This parameter is applicable only on HP-UX, AIX, and Windows.*
NICBandwidthUtilMinorThreshold	Set a threshold value for bandwidth utilization at which you want to receive a minor severity message. *This parameter is applicable only on HP-UX, AIX, and Windows.*
NICBandwidthUtilWarningThreshold	Set a threshold value for bandwidth utilization at which you want to receive a warning severity message. *This parameter is applicable only on HP-UX, AIX, and Windows.*
MessageGroup	You can type an appropriate value that helps you to identify the messages sent by this policy. Whenever a threshold is violated, the policy appends the value from this parameter in the message before sending it to the management console.
Debug	Set the value as **0** to disable trace messages, as **1** to receive trace messages on the console, and as **2** to log the messages in the trace file on the managed node. For details, see Tracing.

Memory Bottleneck Diagnosis Policy

SI-MemoryBottleneckDiagnosis

This policy monitors the physical memory utilization and the bottlenecks. Memory bottleneck condition occurs when the memory utilization is high and the available memory is very low. It causes the system to slow down affecting overall performance. High memory consumption results in excessive page outs, high page scan rate, swap-out byte rate, and page request rate eventually slowing down the system.

The policy first checks for memory bottleneck threshold violations, if the condition is not met it checks for memory usage threshold violations. If both conditions for memory bottleneck and memory usage, are not met, the policy checks for free page table condition. By default the free page table thresholds contain Microsoft recommended values on the Windows systems. In case of violation of multiple threshold values indicating a high utilization, the policy sends a message to the HPOM console with appropriate message attributes. The message also displays a list of top 10 memory hogging processes.

The multiple metrics used to evaluate a memory bottleneck condition use different threshold values on various platforms. To enable the right threshold values for a specific platform, deploy the threshold overrides policies onto the managed node.

ThresholdOverrides_Linux defines appropriate threshold values for the memory metrics on a Linux platform.

ThresholdOverrides_Windows defines appropriate threshold values for the memory metrics on a Windows platform.

Metrics Used	• GBL_MEM_UTIL • GBL_MEM_PAGEOUT_RATE • GBL_MEM_PAGEOUT_BYTE_RATE • GBL_MEM_PAGE_REQUEST_RATE* • GBL_MEM_CACHE_FLUSH_RATE * • GBL_MEM_PG_SCAN_RATE • GBL_MEM_PHYS * These metrics are used only if you install HP performance Agent on the managed node.
Supported Platforms	• Microsoft Windows • Red Hat Enterprise Linux • Suse Linux Enterprise Server • HP-UX • IBM AIX • Oracle Solaris
Script-Parameter	**Description**
MemPageOutRateCriticalThreshold	The threshold is expressed as the total number of pages swapped out from the physical memory to the disk per second. Set the threshold value for pages swapped out at which you want to receive a critical message.
MemPageOutRateMajorThreshold	Set the threshold value for pages swapped out at which you want to receive a major message.
MemPageOutRateMinorThreshold	Set the threshold value for pages swapped out at which you want to receive a minor message.
MemPageOutRateWarningThreshold	Set the threshold value for pages swapped out at which you want to receive a warning message.
MemUtilCriticalThreshold	The threshold is expressed as the percentage (0 to 100%) of physical memory utilization on the node. Set the threshold value for minimum memory utilized on the disk at which you want to receive a critical severity message.
MemUtilMajorThreshold	Set the threshold value for minimum memory utilized on the node at which you want to receive a major severity message.

MemUtilMinorThreshold	Set the threshold value for minimum memory utilized on the node at which you want to receive a minor severity message.
MemUtilWarningThreshold	Set the threshold value for minimum memory utilized on the node at which you want to receive a warning severity message.
MemPageScanRateCriticalThreshold	The threshold is expressed as the total number of pages swapped in from the physical memory to the disk per second. Set the threshold value for pages swapped in at which you want to receive a critical message.
MemPageScanRateMajorThreshold	Set the threshold value for pages swapped in at which you want to receive a major message.
MemPageScanRateMinorThreshold	Set the threshold value for pages swapped in at which you want to receive a minor message.
MemPageScanRateWarningThreshold	Set the threshold value for pages swapped in at which you want to receive a warning message.
MemPageReqRateHighThreshold	Set the threshold value for the number of page requests from disk per second.
MemCacheFlushRateHighThreshold	Set the threshold value for the rate at which the file system cache flushes its contents to disk.
FreeMemAvailCriticalThreshold	The threshold is expressed as the free physical memory (in MBs) available on the disk or filesystem. Set the threshold value for minimum free memory on the disk at which you want to receive a critical severity message.
FreeMemAvailMajorThreshold	Set the threshold value for minimum free memory on the disk at which you want to receive a major severity message.
FreeMemAvailMinorThreshold	Set the threshold value for minimum free memory on the disk at which you want to receive a minor severity.
FreeMemAvailWarningThreshold	Set the threshold value for minimum free memory on the disk at which you want to receive a warning severity.
MemSwapoutByteRateCriticalThreshold	The threshold is expressed as the number of pages scanned per second by the pageout daemon (in MBs). Set the threshold value for minimum free memory on the disk at which you want to receive a critical severity message.
MemSwapoutByteRateMajorThreshold	Set the threshold value for minimum free memory on the disk at which you want to receive a major severity message.

MemSwapoutByteRateMinorThreshold	Set the threshold value for minimum free memory on the disk at which you want to receive a minor severity.
MemSwapoutByteRateWarningThreshold	Set the threshold value for minimum free memory on the disk at which you want to receive a warning severity.
FreePageTableCriticalThreshold	The threshold is expressed as the number of free page tables available on the system. Set the threshold value for minimum free page table entry on the disk at which you want to receive a critical severity message. *This parameter is applicable only on Windows.*
FreePageTableMajorThreshold	Set the threshold value for minimum free page table entry on the disk at which you want to receive a major severity message. *This parameter is applicable only on Windows.*
FreePageTableMinorThreshold	Set the threshold value for minimum free page table entry on the disk at which you want to receive a minor severity message. *This parameter is applicable only on Windows.*
FreePageTableWarningThreshold	Set the threshold value for minimum free page table entry on the disk at which you want to receive a warning severity message. *This parameter is applicable only on Windows.*
MessageGroup	You can type an appropriate value that helps you to identify the messages sent by this policy. Whenever a threshold is violated, the policy appends the value from this parameter in the message before sending it to the management console.
Debug	Set the value as **0** to disable trace messages, as **1** to receive trace messages on the console, and as **2** to log the messages in the trace file on the managed node. For details, see Tracing.

CPU Spike Check Policy

SI-CPUSpikeCheck

This is a processor performance monitoring policy. A system experiences CPU spike when there is a sharp rise in the CPU usage immediately followed by a decrease in usage. SI-CPUSpikeCheck policy monitors CPU spikes per CPU busy time in system mode, per CPU busy time in user mode, and total busy time per CPU.

Metrics Used	• BYCPU_CPU_USER_MODE_UTIL • BYCPU_CPU_SYS_MODE_UTIL • BYCPU_ID • BYCPU_CPU_TOTAL_UTIL
Supported Platforms	• Microsoft Windows • Red Hat Enterprise Linux • Suse Linux Enterprise Server • HP-UX • IBM AIX • Oracle Solaris

Script-Parameter	**Description**
CpuUtilCriticalThreshold	The threshold is expressed as the total CPU time when the CPU is busy. In other words, the total CPU utilization time. It consists of total CPU time spent in user mode and system mode. Set the threshold value for minimum total CPU utilization time at which you want to receive a critical severity message.
CpuUtilMajorThreshold	Set the threshold value for minimum total CPU utilization time at which you want to receive a major severity message.
CpuUtilMinorThreshold	Set the threshold value for minimum total CPU utilization time at which you want to receive a minor severity message.
CpuUtilWarningThreshold	Set the threshold value for minimum total CPU utilization time at which you want to receive a warning severity message.
CpuUtilUsermodeCriticalThreshold	The threshold is expressed as the percentage (0 to 100%) of CPU time when CPU is busy in user mode. Set the threshold value for minimum CPU busy time at which you want to receive a critical severity message.
CpuUtilUsermodeMajorThreshold	Set the threshold value for minimum CPU busy time in user mode at which you want to receive a major severity message.
CpuUtilUsermodeMinorThreshold	Set the threshold value for minimum CPU busy time in user mode at which you want to receive a minor message.
CpuUtilUsermodeWarningThreshold	Set the threshold value for minimum CPU busy time in user mode at which you want to receive a warning message.

CpuUtilSysmodeCriticalThreshold	The threshold is expressed as the percentage (0 to 100%) of CPU time when CPU is busy in system mode. Set the threshold value for minimum CPU busy time at which you want to receive a critical severity message.
CpuUtilSysmodeMajorThreshold	Set the threshold value for minimum CPU busy time in system mode at which you want to receive a major severity message.
CpuUtilSysmodeMinorThreshold	Set the threshold value for minimum CPU busy time in system mode at which you want to receive a minor message.
CpuUtilSysmodeWarningThreshold	Set the threshold value for minimum CPU busy time in system mode at which you want to receive a warning message.
InterruptRateCriticalThreshold	The threshold is expressed as the average number of device interrupts per second for the CPU during the sampling interval. Set the threshold value for minimum CPU interrupt rate at which you want to receive a critical severity message.
InterruptRateMajorThreshold	Set the threshold value for minimum CPU interrupt rate at which you want to receive a major severity message.
InterruptRateMinorThreshold	Set the threshold value for minimum CPU interrupt rate at which you want to receive a minor severity message.
InterruptRateWarningThreshold	Set the threshold value for minimum CPU interrupt rate at which you want to receive a warning severity message.
MessageGroup	Message group for outgoing messages.
Debug	Set the value as **0** to disable trace messages, as **1** to receive trace messages on the console, and as **2** to log the messages in the trace file on the managed node. For details, see Tracing.

CPU Bottleneck Diagnosis Policy

SI-CPUBottleneckDiagnosis

This policy detects CPU bottlenecks like exceeding the thresholds for CPU utilization percentage, processor queue length, total number of CPU on the system, and operating systems.

If the threshold for CPU utilization is violated along with threshold for number of processes in the queue waiting for CPU time, the policy sends a message to the HPOM console with the appropriate message attributes. The message displays a list of the top 10 CPU hogging processes.

Metrics used for machines which have the DataSource SCOPE enabled.	• GBL_CPU_TOTAL_UTIL • GBL_ACTIVE_CPU • GBL_CPU_QUEUE* • GBL_LOADAVG • GBL_INTERRUPT_RATE • GBL_CSWITCH_RATE * This metrics is applicable only on HP-UX platform.
Metrics used for machines which do not have the DataSource SCOPE enabled.	• GBL_CPU_TOTAL_UTIL • GBL_ACTIVE_CPU • GBL_RUN_QUEUE • GBL_INTERRUPT_RATE
Supported Platforms	• Microsoft Windows • Red Hat Enterprise Linux • Suse Linux Enterprise Server • HP-UX • IBM AIX • Oracle Solaris

Script-Parameter	**Description**
GlobalCpuUtilCriticalThreshold	The threshold is expressed as the summarized CPU utilization. Set the threshold value for minimum summarized CPU utilization at which you want to receive a critical message.
GlobalCpuUtilMajorThreshold	Set the threshold value for minimum summarized CPU utilization at which you want to receive a major message.
GlobalCpuUtilMinorThreshold	Set the threshold value for minimum summarized CPU utilization at which you want to receive a minor message.

GlobalCpuUtilWarningThreshold	Set the threshold value for minimum summarized CPU utilization at which you want to receive a warning message.
MessageGroup	You can type an appropriate value that helps you to identify the messages sent by this policy. Whenever a threshold is violated, the policy appends the value from this parameter in the message before sending it to the management console.
Debug	Set the value as `0` to disable trace messages, as `1` to receive trace messages on the console, and as `2` to log the messages in the trace file on the managed node. For details, see Tracing.

Per Disk Utilization-AT policy

SI-PerDiskUtilization-AT

This policy monitors utilization for each disk on the managed node. This policy processes each disk instance separately for every interval. The policy uses the automatic threshold determination to automatically calculate the threshold values according to the disk utilization on previous days. It is mandatory that this policy needs Performance Agent to be running on the managed node.

This policy relies on historical data. For accurate results, deploy the policy only after a week of data collection by the performance agent.

Metrics Used	BYDSK_UTIL
Supported Platforms	• Microsoft Windows • Red Hat Enterprise Linux • Suse Linux Enterprise Server • HP-UX • IBM AIX • Oracle Solaris
Script-Parameter	**Description**
MessageApplication	Type an appropriate value that helps you identify the messages sent by the SI-PerDiskUtilization-AT policy to the management console.
DataSource	Displays the HP Embedded Performance Component (EPC) data source name as SCOPE.
DataObject	Displays the HP Embedded Performance Component (EPC) data object name as DISK.
DataMetric	Displays the HP Embedded Performance Component (EPC) metric name as BYDSK_UTIL.
BaselinePeriod	Type the time period you want to define as a baseline period, such as ‘3600 seconds’. This period moves with the current time. The most recent 3600-second (1-hour) period becomes the current baseline period.

MinimumValue	Displays the minimum value of disk utilization as indicated by the metric.
MaximumValue	Displays the maximum value of disk utilization as indicated by the metric.
WarningDeviations	Displays the number of standard deviation away from normal at which the policy will send a warning message to HPOM console. Set an appropriate value for the parameter. To disable the parameter, set value as *5*.
MinorDeviations	Displays the number of standard deviation away from normal at which the policy will send a minor message to HPOM console. Set an appropriate value for the parameter greater than the specified value for WarningDeviations. To disable the parameter, set value as *5*.
MajorDeviations	Displays the number of standard deviation away from normal at which the policy will send a major message to HPOM console. Set an appropriate value for the parameter greater than the specified value for MinorDeviations. To disable the parameter, set value as *5*.
WarningHighSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or exceeds the sample data average by the value specified in *WarningDeviations*. To disable the parameter, set value as *none*.
MinorHighSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or exceeds the sample data average by the value specified in *MinorDeviations*. To disable the parameter, set value as *none*.
MajorHighSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or exceeds the sample data average by the value specified in *MajorDeviations*. To disable the parameter, set value as *none*.
WarningLowSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or falls below the sample data average by the value specified in *WarningDeviations*. To disable the parameter, set value as *none*.
MinorLowSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or falls below the sample data average by the value specified in *MinorDeviations*. To disable the parameter, set value as *none*.

MajorLowSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or falls below the sample data average by the value specified in *MajorDeviations*. To disable the parameter, set value as *none*.
InstanceSource	Do not edit the parameter value.
Debug	Set the value as **0** to disable trace messages, as **1** to receive trace messages on the console, and as **2** to log the messages in the trace file on the managed node. For details, see Tracing.
MessageGroup	Message group for outgoing messages.
DiskUtilCutOff	Set a value below which you do not want to monitor disk utilization.

Network Interface Outbyte Rate Policy

SI-PerNetifOutbyteBaseline-AT

This policy monitors the network interface outbyte rate for a network interface in a given interval. It monitors the outgoing bytes on each network interface on the managed node individually. This policy processes each instance of network interface separately for every interval. The policy uses automatic threshold determination to automatically calculate the threshold values according to the network interface outbyte rate on previous days.

This policy relies on historical data. For accurate results, deploy the policy only after a week of data collection by the performance agent. The policy does not monitor the physical NIC of vMA machines.

Metrics Used	BYNETIF_OUT_BYTE_RATE
Supported Platforms	• Microsoft Windows • Red Hat Enterprise Linux • Suse Linux Enterprise Server • HP-UX • IBM AIX • Oracle Solaris
Script-Parameter	**Description**
MessageApplication	Type an appropriate value that helps you identify the messages sent by the SI-PerNetifOutbyteBaseline-AT policy to the management console.
DataSource	Displays the HP Embedded Performance Component (EPC) data source name as CODA.
DataObject	Displays the HP Embedded Performance Component (EPC) data object name as NETIF.
DataMetric	Displays the HP Embedded Performance Component (EPC) metric name as BYNETIF_OUT_BYTE_RATE.

BaselinePeriod	Type the time period you want to define as a baseline period, such as '3600 seconds'. This period moves with the current time. The most recent 3600-second (1-hour) period becomes the current baseline period.
MinimumValue	Displays the minimum value of network interface outbyte rate as indicated by the metric.
MaximumValue	Displays the maximum value of network interface outbyte rate as indicated by the metric.
WarningDeviations	Displays the number of standard deviation away from normal at which the policy will send a warning message to HPOM console. Set an appropriate value for the parameter. To disable the parameter, set value as *5*.
MinorDeviations	Displays the number of standard deviation away from normal at which the policy will send a minor message to HPOM console. Set an appropriate value for the parameter greater than the specified value for WarningDeviations. To disable the parameter, set value as *5*.
MajorDeviations	Displays the number of standard deviation away from normal at which the policy will send a major message to HPOM console. Set an appropriate value for the parameter greater than the specified value for MinorDeviations. To disable the parameter, set value as *5*.
WarningHighSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or exceeds the sample data average by the value specified in *WarningDeviations*. To disable the parameter, set value as *none*.
MinorHighSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or exceeds the sample data average by the value specified in *MinorDeviations*. To disable the parameter, set value as *none*.
MajorHighSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or exceeds the sample data average by the value specified in *MajorDeviations*. To disable the parameter, set value as *none*.
WarningLowSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or falls below the sample data average by the value specified in *WarningDeviations*. To disable the parameter, set value as *none*.

MinorLowSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or falls below the sample data average by the value specified in *MinorDeviations*. To disable the parameter, set value as *none*.
MajorLowSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or falls below the sample data average by the value specified in *MajorDeviations*. To disable the parameter, set value as *none*.
Debug	Set the value as **0** to disable trace messages, as **1** to receive trace messages on the console, and as **2** to log the messages in the trace file on the managed node. For details, see Tracing.
MessageGroup	Message group for outgoing messages.
ByNetifOutByteCutOff	Set a value below which you do not want to monitor the outbyte rate.

Network Interface Inbyte Rate Policy

SI-PerNetifInbyteBaseline-AT

This policy monitors the inbyte rate for a network interface in a given interval. It monitors the incoming bytes on each network interface on the managed node individually. This policy processes each instance of network interface separately for every interval. The policy uses the automatic threshold determination to automatically calculate the threshold values according to the network interface inbyte rate on previous days.

This policy relies on historical data. For accurate results, deploy the policy only after a week of data collection by the performance agent. The policy does not monitor the physical NIC of vMA machines.

Metrics Used	BYNETIF_IN_BYTE_RATE
Supported Platforms	• Microsoft Windows • Red Hat Enterprise Linux • Suse Linux Enterprise Server • HP-UX • IBM AIX • Oracle Solaris
Script-Parameter	**Description**
MessageApplication	Type an appropriate value that helps you identify the messages sent by the policy to the management console.
DataSource	Displays the HP Embedded Performance Component (EPC) data source name as CODA.
DataObject	Displays the HP Embedded Performance Component (EPC) data object name as NETIF.

DataMetric	Displays the HP Embedded Performance Component (EPC) metric name as BYNETIF_IN_BYTE_RATE.
BaselinePeriod	Type the time period you want to define as a baseline period, such as '3600 seconds'. This period moves with the current time. The most recent 3600-second (1-hour) period becomes the current baseline period.
MinimumValue	Displays the minimum value of network interface inbyte rate as indicated by the metric.
MaximumValue	Displays the maximum value of network interface inbyte rate as indicated by the metric.
WarningDeviations	Displays the number of standard deviation away from normal at which the policy will send a warning message to HPOM console. Set an appropriate value for the parameter. To disable the parameter, set value as *5*.
MinorDeviations	Displays the number of standard deviation away from normal at which the policy will send a minor message to HPOM console. Set an appropriate value for the parameter greater than the specified value for WarningDeviations. To disable the parameter, set value as *5*.
MajorDeviations	Displays the number of standard deviation away from normal at which the policy will send a major message to HPOM console. Set an appropriate value for the parameter greater than the specified value for MinorDeviations. To disable the parameter, set value as *5*.
WarningHighSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or exceeds the sample data average by the value specified in *WarningDeviations*. To disable the parameter, set value as *none*.
MinorHighSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or exceeds the sample data average by the value specified in *MinorDeviations*. To disable the parameter, set value as *none*.
MajorHighSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or exceeds the sample data average by the value specified in *MajorDeviations*. To disable the parameter, set value as *none*.
WarningLowSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or falls below the sample data average by the value specified in *WarningDeviations*. To disable the parameter, set value as *none*.

MinorLowSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or falls below the sample data average by the value specified in *MinorDeviations*. To disable the parameter, set value as *none*.
MajorLowSeverity	Displays the severity of the alert messages to be sent to HPOM console in case the current data meets or falls below the sample data average by the value specified in *MajorDeviations*. To disable the parameter, set value as *none*.
Debug	Set the value as **0** to disable trace messages, as **1** to receive trace messages on the console, and as **2** to log the messages in the trace file on the managed node. For details, see Tracing.
MessageGroup	Message group for outgoing messages.
ByNetifInByteCutOff	Set a value below which you do not want to monitor the inbyte rate.

Sample Performance Policies

SI SPI provides sample performance policies that can be used to monitor the performance of processes running on a system. You can use these policies as template to create copies and modify them as per your requirements.

Script-Parameter	Description
ProcessName	Type the name of the process that you want to monitor.
ProcessArguments	Type the process arguments, if any.
MessageGroup	Message group for outgoing messages.
CPUUsageHighWaterMark or MemoryUsageHighWaterMark	Type a threshold value for process CPU or memory usage above which you want to receive an alert.
Debug	Set the value as **0** to disable trace messages, as **1** to receive trace messages on the console, and as **2** to log the messages in the trace file on the managed node. For details, see Tracing.

The sample policies provided are:

- **SI-JavaProcessMemoryUsageTracker** policy monitors memory usage for Java process running on your system. The default policy group for the policy is:

  Infrastructure Management → *<language>* → Systems Infrastructure → Performance → Process Resource Usage Monitor Samples

- **SI-JavaProcessCPUUsageTracker** policy monitors the CPU usage for the Java process running on your system. The default policy group for the policy is:

  Infrastructure Management → *<language>* → Systems Infrastructure → Performance → Process Resource Usage Monitor Samples

- **SI-MSWindowsSvchostCPUUsageTracker** policy monitors the CPU usage for the svchost processes running on your system. The default policy group for the policy is:

  Infrastructure Management → *<language>* → Systems Infrastructure → Performance → Process Resource Usage Monitor Samples → Windows

- **SI-MSWindowsSvchostMemoryUsageTracker** policy monitors the memory usage for the svchost processes running on your system. The default policy group for the policy is:

  Infrastructure Management → *<language>* → Systems Infrastructure → Performance → Process Resource Usage Monitor Samples → Windows

Disk Peak Utilization Monitor Policy

SI-DiskPeakUtilMonitor

This policy monitors the utilization level of the disk on the system. It checks whether the utilization level is full. In case the disk utilization level exceeds the threshold values specified, the policy sends out an alert message to the HPOM console.

Metrics Used	• GBL_FS_SPACE_UTIL_PEAK
Supported Platforms	• Microsoft Windows • Red Hat Enterprise Linux • Suse Linux Enterprise Server • HP-UX • IBM AIX • Oracle Solaris
Script-Parameter	**Description**
DiskPeakUtilCriticalThreshold	The threshold is expressed as the utilization level of fullest disk in percentage. Set the threshold value at which you want to receive a critical message.
DiskPeakUtilMajorThreshold	Set the threshold value at which you want to receive a major message.
DiskPeakUtilMinorThreshold	Set the threshold value at which you want to receive a minor message.
DiskPeakUtilWarningThreshold	Set the threshold value at which you want to receive a warning message.
MessageGroup	Message group for outgoing messages.
Debug	Set the value as `0` to disable trace messages, as `1` to receive trace messages on the console, and as `2` to log the messages in the trace file on the managed node. For details, see Tracing.

In the console tree, the SI-DiskPeakUtilMonitor policy is listed at the following locations:

- **Infrastructure Management → <*language*> → System Infrastructure → Policies Grouped by Vendor → <*all platforms*> - QuickStart.**
- **Infrastructure Management → <*language*> → System Infrastructure → Performance.**

Security Policies

Suppose an unauthorized user tried to break into your system by entering different combinations of username and password, or by deploying an automated script to do this. Such attempts may result in too many login failures. To identify and preempt such a risk, you can deploy the System Infrastructure security policies to periodically check the number of failed logins on your system. For instance, these policies collect failed login data and send alerts in case of too many attempts.

After deploying the security collector policies, make sure that you let the policies run for at least 5 minutes to collect the required data.

Failed Login Collector Policy for Windows

SI-MSWindowsFailedLoginsCollector

This is a scheduled task policy that checks for the number of failed login attempts on Microsoft Windows. It check for invalid logins, either due to unknown username or incorrect password on the managed node. The policy logs individual instances of failed login into the GBL_NUM_FAILED_LOGINS metric in Embedded Performance Component (EPC) at definite time intervals. By default, the time interval is 1 hour. The recorded information stored in EPC can be used to send an alert to the console or generate reports for the number of invalid logins over a period of time. The default policy group for the policy is:

Infrastructure Management → *<language>* → Systems Infrastructure → Security → Windows

Last Logon Collector Policy for Windows

SI-MSWindowsLastLogonsCollector

This is a scheduled task policy that checks for the logon details of all the active local user accounts on Microsoft Windows. The policy logs individual instances of user logon into the SECONDS_SINCE_LASTLOGIN metric in Embedded Performance Component (EPC) at definite time intervals. By default, the time interval is 1 hour. The recorded information stored in EPC can be used to send an alert to the console or generate reports for the number of user logons over a period of time. The default policy group for the policy is:

Infrastructure Management → *<language>* → Systems Infrastructure → Security → Windows

Failed Login Collector Policy for Linux

SI-UNIXFailedLoginsCollector

This is a scheduled task policy that checks for the number of failed login attempts on RHEL and SLES Linux systems, HP-UX, AIX and Solaris. The policy checks for invalid logins, either due to unknown username or incorrect password on the managed node. The policies log individual instances of failed login into the GBL_NUM_FAILED_LOGINS metric in Embedded Performance Component (EPC) at definite time intervals. By default, the time interval is 1 hour. The recorded information stored in EPC can be used to send an alert to the console or generate reports for the number of invalid logins over a period of time. The default policy group for the policy is:

- **Infrastructure Management → *<language>* → Systems Infrastructure → Security → Linux**
- **Infrastructure Management → *<language>* → Systems Infrastructure → Policies grouped by Vendor → *<os>* - QuickStart**

  In this instance, the ***<os>*** can be AIX, HP-UX, SLES, RHEL, or Solaris

The pre-requisites for SI-UNIXFailedLoginsCollector policy to function correctly when deployed on a solaris node are:

- The file `/etc/default/login` on solaris node must have the following settings:

  SYSLOG=YES

  SYSLOG_FAILED_LOGINS=1

- Remove the comment from the following line in `/etc/syslog.conf` file or add the line if it is not present.

  auth.notice ifdef(`LOGHOST', /var/log/authlog, @loghost)

- Refresh `syslogd` using the following command:

  svcadm refresh system/system-log

SI-UNIXFailedLoginsCollector policy deployed on other nodes

Nodes	Commands / logfiles used to display the failed logins
Solaris	`/var/log/authlog`
Linux	`lastb` command
HP-UX	`lastb` command
AIX	`/etc/security/failedlogin` log

Last Logon Collector Policy for Linux

SI-LinuxLastLogonsCollector

This is a scheduled task policy that checks for the logon details of all the active local user accounts on RHEL and SLES Linux systems. The policy logs individual instances of user logon into the SECONDS_SINCE_LASTLOGIN metric in Embedded Performance Component (EPC) at definite time intervals. By default, the time interval is 1 hour. The recorded information stored in EPC can be used to send an alert to the console or generate reports for the number of user logons over a period of time. The default policy group for the policy is:

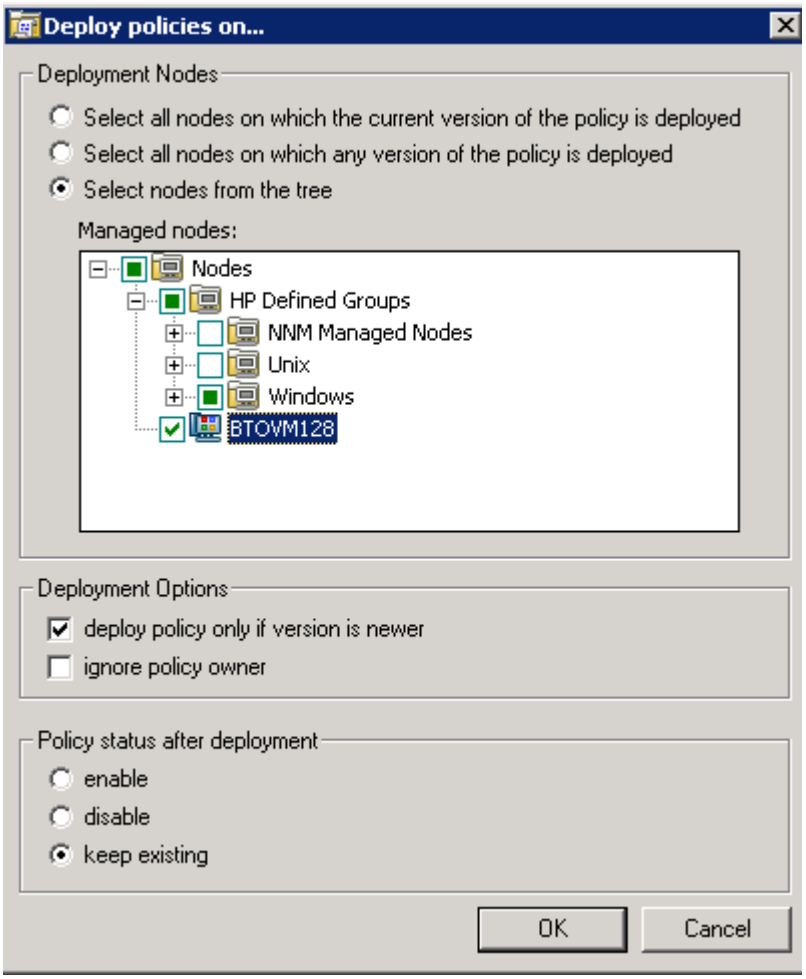
Infrastructure Management → ***<language>*** → **Systems Infrastructure** → **Security** → **Linux**

Deploying SI SPI Policies from HPOM for Windows Management Server

To manually deploy policies from the management server, follow these steps:

1. Right-click the policy you want to deploy.
2. From the menu, select **All Tasks**.

3 Select **Deploy on**. The Deploy policies on dialog box opens.



4 Select the option **Select nodes from the tree**. From the list of managed nodes, select the nodes where you want to deploy the policy.

5 Click **OK**.

Deploying SI SPI Policies from HPOM for UNIX Management Server

Before you deploy policies, make sure that the nodes have been added to the management server and have HP Operations Agent software installed. For more information on how to add nodes to the management server, refer to the *HP Operations Manager for Unix Online Help*.

To deploy policies from the management server for HPOM for UNIX (HP-UX, Linux, or Solaris) follow these steps:

Task 1: Assign Policy or Policy group

1 Log on to HPOM as the administrator. The HPOM Administration interface appears.

2 Click **Policy Bank** under the Objects Bank category. The Policy Bank window opens.

3 In the Policy Bank window, select the policy or policy groups you want to assign to a node or a node group.

4 Select **Assign to Node/Node group...** from the **Choose an Action** drop-down box and click submit.

The select window opens.

5 Select the node or the node groups and click **OK**.

The selected policies are assigned to the nodes.

Task 2: Deploy Policies

1 From the HPOM Administration interface, click **Node Bank** under the Objects Bank category. The Node Bank window opens.

2 In the Node Bank window, select the nodes or node groups on which you want to deploy policies.

3 Select **Deploy Configuration...** from the **Choose an Action** drop-down box and click submit.

The selector window opens.

4 Select the **Distribute Policies** check box and click **OK**.

The policies are deployed on the selected nodes.

Systems Infrastructure SPI Tool

Tools enable you to manage services on managed nodes and view a list of data collected for a particular managed node.

To access the SI SPI tool on HPOM for Windows, select the following:

Tools → Systems Infrastructure

To access the tool on console or Administration interface for HPOM for UNIX/ Linux, select the following:

Tool Bank → Systems Infrastructure

Users Last Login Tool

When launched on a managed node, the Users Last Login tool displays a list of all active users along with their last login details. Before launching the tool, make sure you have deployed the corresponding last logon collector policy. To know more about the last logon collector policies, see Last Logon Collector Policy for Windows and Last Logon Collector Policy for Linux.

To launch the tool from the HPOM for Windows management server, follow these steps:

1 From the console tree **Tools** folder, select the **Systems Infrastructure** folder.

2 Select the **Users Last Login** tool from the details pane and right-click to open the shortcut menu.

3 Select **All Tasks→Launch Tool...** to open the **Select where to launch this tool** dialog box.

The dialog box displays a list of the managed nodes on which the selected tool can be launched.

4 Select the check box for each node to which you want to apply the tool. Selecting the **Nodes** folder selects the entire group of tools the folder contains.

5 Click **Launch.**

The **Tool Status** dialog box opens to display the results of the launch operation.

You can save the results of the apply tool operations. Select one or more lines in the **Launched Tools** box and click **Save**. The output is saved in text format.

To launch the tool from HPOM for UNIX management server, follow these steps:

1. Select **Tools** → **Systems Infrastructure** in the Java interface.
2. Right-click the <*tool name*> tool, select **Start Customized**.

   Start Tool - Customized Wizard window opens.
3. Under the nodes list, select the node to launch the tool.
4. On the wizard, click **Get Selections**.

   The node is added to the Selected Nodes list.
5. Click **Next**.

   On the page specify additional information needed to run the tool, you can specify the additional information or leave the fields blank.
6. Click **Finish**.

   The tool output appears.

5 Systems Infrastructure SPI Reports and Graphs

You can integrate the SI SPI with HP Reporter to generate reports based on collected metric data from the managed nodes. The reports provide a picture of system resources. You can also generate graphs to analyze the metric data collected. To generate and view reports and graphs from data collected by the SI SPI, use HP Reporter and HP Performance Manager with HPOM.

Systems Infrastructure SPI Reports

The reports provide an overall picture of system resources. You can integrate the SI SPI with HP Reporter to generate reports based on collected metric data from the managed nodes.

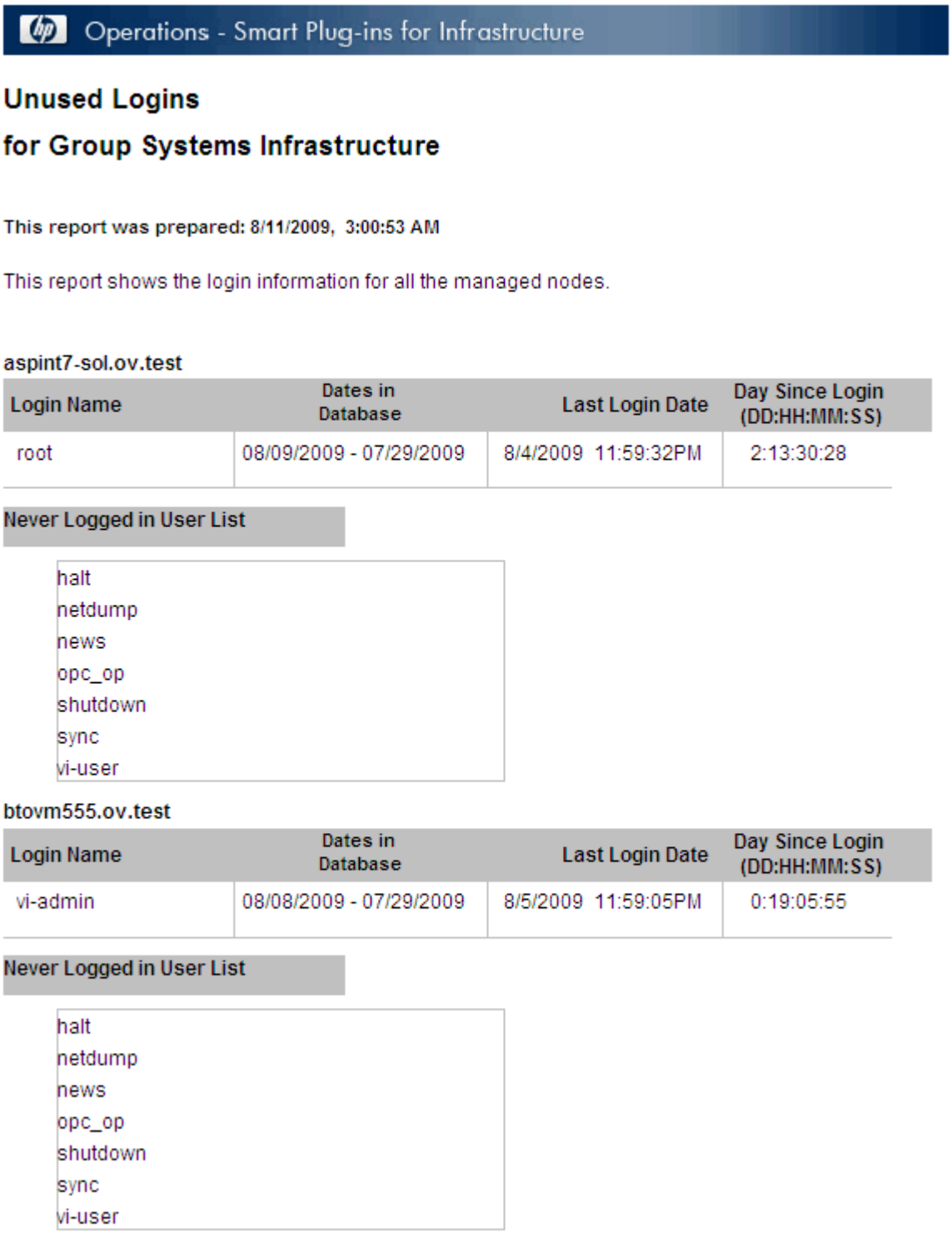
You can access SI SPI reports from the HPOM for Windows console. To install HP Reporter package for SI SPI, see *HP Operations Smart Plug-in for Infrastructure Installation Guide.*

To view reports for SI SPI from HPOM for Windows, expand **Reports** → **Systems Infrastructure** in the console tree. To display a report, select the desired report, right-click, and then select **Show report**.

If HP Reporter is installed on the HPOM management server, you can view the reports on the management server directly.

If HP Reporter is installed on a separate system connected to the HPOM management server, you can view the reports on HP Reporter system. For more information on integration of HP Reporter with HPOM, see *HP Reporter Installation and Special Configuration Guide*. The following is an example report.

Figure 3 Sample report for Systems Infrastructure SPI



Operations - Smart Plug-ins for Infrastructure

Unused Logins

for Group Systems Infrastructure

This report was prepared: 8/11/2009, 3:00:53 AM

This report shows the login information for all the managed nodes.

aspint7-sol.ov.test

Login Name	Dates in Database	Last Login Date	Day Since Login (DD:HH:MM:SS)
root	08/09/2009 - 07/29/2009	8/4/2009 11:59:32PM	2:13:30:28

Never Logged in User List

halt
netdump
news
opc_op
shutdown
sync
vi-user

btovm555.ov.test

Login Name	Dates in Database	Last Login Date	Day Since Login (DD:HH:MM:SS)
vi-admin	08/08/2009 - 07/29/2009	8/5/2009 11:59:05PM	0:19:05:55

Never Logged in User List

halt
netdump
news
opc_op
shutdown
sync
vi-user

The SI SPI provides the following reports:

Report/ Report Title	Purpose
System Last Login	This report displays the date when a particular login was last used on the managed node. It also displays a list of users who have never logged in. The information is sorted by day and time. You can use this information to identify the unused or obsolete user accounts.
System Failed Login	This report displays a list of all failed login attempts on the managed node. You can use this information to identify unauthorized users repeatedly trying to login the managed node.
System Availability	This report displays the availability information for the systems. You can use this information to know the system uptime percentage and system downtime time for the range of dates in the database excluding outside of shifts, weekends, or holidays.
Top CPU Process	This report displays the top systems with high CPU consumption. You can use this information to analyze the systems with high CPU cycles consumed during the reporting interval.
Top Memory Process	This report displays the top systems with high memory consumption. You can use this information to analyze the systems with high memory consumed during the reporting interval.

Systems Infrastructure SPI Graphs

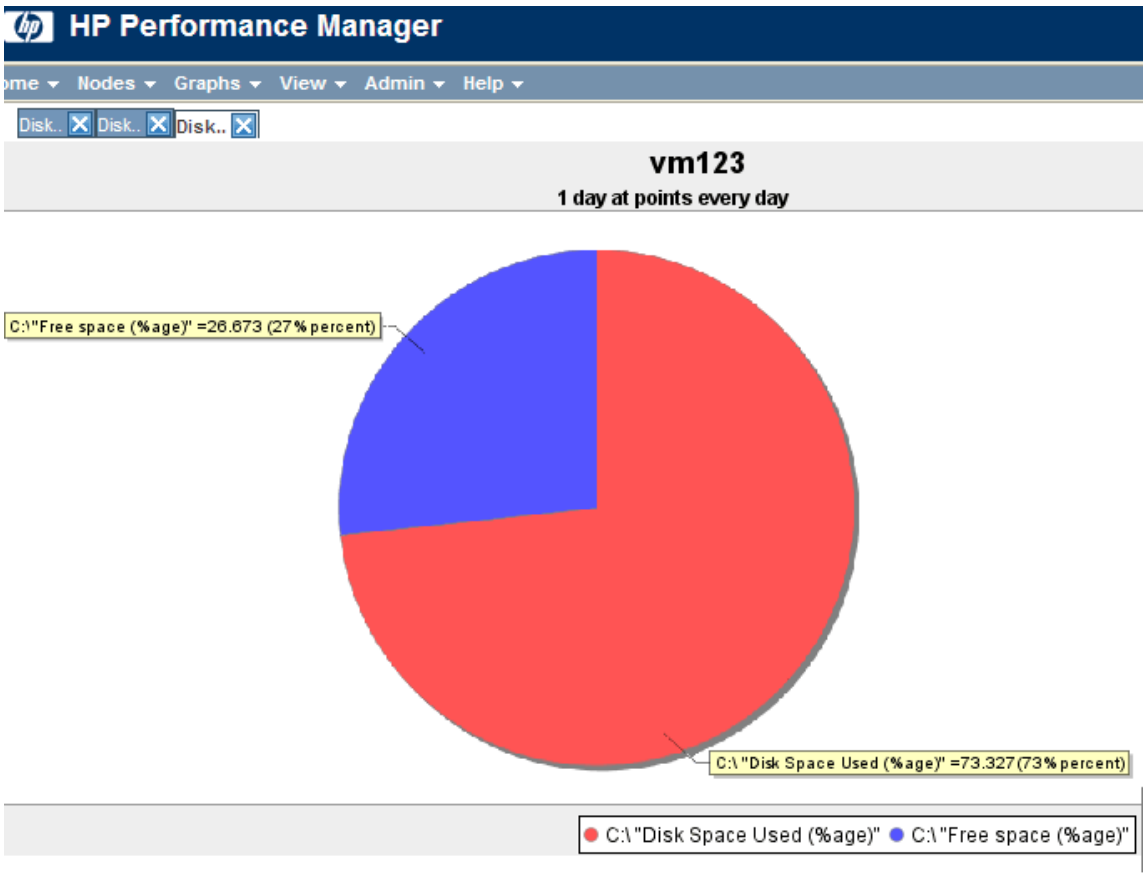
You can generate graphs using HP Performance Manager for near real-time data gathered from the managed nodes. You can access these graphs from the HPOM console if you install HP Performance Manager on an HPOM management server.

The SI SPI provides a set of pre-configured graphs. They are located on the HPOM console tree in the Graphs folders. You can access this Graphs folder only if you install HP Performance Manager on the HPOM management server. The following is an example graph.

To access the graphs on HPOM for Windows, select **Graphs→ Infrastructure Performance**

To access the graphs on HPOM for UNIX/ Linux/Solaris, select the active message, open the Message Properties window, and click **Actions.** Under the Operator initiated action section, click **Perform**. Alternatively you can, right-click active message, select **Perform/Stop Action** and click **Perform Operator-Initiated Action**.

Figure 4 Sample graph for Systems Infrastructure SPI



The SPI for Systems Infrastructure provides the following graphs:

Graph	Graph Configurations
Disk	• Disk Utilization • Disk Summary • Disk Throughput • Disk Space • Disk Space (Pie Chart) • Disk Details
Global Performance	• Global History • Global Run Queue Baseline • Global Details • Multiple Global Forecasts

Graph	Graph Configurations
CPU	• CPU Summary • CPU Utilization Summary • Individual CPUs • CPU Comparison • CPU Gauges • CPU Details • Global CPU Forecasts • Seasonal CPU Forecasts
Network	• Network Summary • Individual Networks • Network Interface Details
Memory	• Memory Summary • Physical Memory Utilization
Configuration	• Configuration Details • System Configuration
Transactions	• Transaction Health • Transaction History • Transaction Details • Transaction Response Forecasts
File System	• File System Details
Application	• Application CPU Gauges • Application CPU Forecast • Application History • Application Details
Process	• Process Details

6 Troubleshooting

This chapter helps you troubleshoot SI SPI problems and provides you with information to help you avoid problems from occurring.

Problem	The Hardware Monitoring policies do not send any alerts.
Cause	-
Solution	Follow these steps: • Start the `snmpd` services if they have stopped. **`# /etc/init.d/snmpd start`** • Ensure that `opctrapi` is configured on port number 162.

Problem	Warning/error messages on the HPOM console:
	`An error occurred in the processing of the policy 'SI-PerDiskUtilization-AT'. Please check the following errors and take corrective actions. (OpC30-797)`
	`Initialization of collection source "DoNotRename" failed. (OpC30-724)`
	`Cannot find object 'DISK' in Coda object list. (OpC30-761)`
	`Searching for 'data source: SCOPE' in the DataSourceList failed. (OpC30-766))`

Cause	This error occurs when the SI-PerDiskUtilization-AT policy is deployed to a node that does not have the HP Performance Agent installed on the node. The SI-PerDiskUtilization-AT policy uses metrics provided by SCOPE for the calculations, and requires HP Performance Agent for proper functioning.
Solution	Install the HP Performance Agent on the managed node for the policy to function properly.

Problem	Advanced Monitoring policies modified in HPOM for UNIX Administrator GUI fail to run after deployment to managed nodes.

Cause	When advanced monitoring policies are edited in user interface mode in HPOM for UNIX policy editor, syntax errors are induced into the Perl code module. This causes the policy to fail to execute. Errors such as the following appear:
	`An error occurred in the processing of the policy 'SI-LinuxSshdProcessMonitor'. Please check the following errors and take corrective actions. (OpC30-797)`
	`Error during evaluation of threshold level "Processes - Fill Instance list" (OpC30-728)`
	`Execution of instance filter script failed. (OpC30-714)`
	`Perl Script execution failed: syntax error at PerlScript line 11, near "1`
	
	`#BEGIN_PROCESSES_LIST`
	`#ProcName=/usr/sbin/sshd`
	`#Params=`
	`#Params=`
	`#MonMode=>=`
	`#ProcNum=1`
	`#END_PROCESSES_LIST`
	`@ProcNames"`
	`Missing right curly or square bracket at PerlScript line 17, within string`
	`syntax error at PerlScript line 17, at EOF`
	`. (OpC30-750)`
	The un-edited advanced monitoring policies (Measurement Threshold type) work fine when deployed from HPOM for UNIX.

Solution	To edit the settings in the Measurement Threshold policy, use 'Edit in Raw mode' feature of the HPOM for UNIX Administrator GUI to change the policy contents. This requires you to know the syntax of the policy data file.

Problem	Operator initiated commands fail to launch the SI SPI graphs from HPOM for UNIX (version 9.00) operator console
Cause	-
Solution	Run the following command on the HPOM server: **`/opt/OV/contrib/OpC/OVPM/install_OVPM.sh <OMUServerName>:8081`**

Problem	Discovery procedures and data collection gives error with non-English names.
Cause	Although the SI SPI can be deployed successfully on a non-English HP Operations Manager, using non-English names for a system results in error. This happens because non-English names are not recognized by the store collection PERL APIs in the HP Operations Agent.
Solution	Make sure that the names for clusters and resource groups are in English.

Problem	Alert Messages while System Discovery automatically adds nodes.
Cause	While automatically adding nodes for cluster and virtualized environments, the system discovery policy generates alert messages with normal severity. These messages take a while to get acknowledged as the auto-addition feature of the policy takes time to populate the node bank.
Solution	Disable the Auto-addition feature by changing the following default values in the XPL configuration parameters: • *AutoAdd_ClusterNode*: Default value is “True”. Change it to “False”. • *AutoAdd_Cluster_RG_IP*: Default value is “True”. Change it to “False”. • *AutoAdd_HypervisorNode*: Default value is “True”. Change it to “False”. • *AutoAdd_Guests*: Default value is “False”. Change it to “True”.

Problem	Warning/error messages on the HPOM console: `Check the following errors and take corrective actions. (OpC30-797) Error during evaluation of threshold level "CPU Spikes level Critical" (OpC30-728) Execution of threshold script failed. (OpC30-712) Perl Script execution failed: Can't locate OvTrace.pm in @INC (@INC contains: /usr/lpp/OV\lbin\eaagt\perl /usr/lpp/OV/lbin/eaagt/perl /var/opt/OV/bin/instrumentation /usr/lpp/OV/nonOV/perl/a/lib/5.8.8/aix-thread-multi /usr/lpp/OV/nonOV/perl/a/lib/5.8.8 /usr/lpp/OV/nonOV/perl/a/lib/site_perl/5.8.8/aix-thread-multi /usr/lpp/OV/nonOV/perl/a/lib/site_perl/5.8.8 /usr/lpp/OV/nonOV/perl/a/lib/site_perl .) at PerlScript line 136.` `BEGIN failed--compilation aborted (in cleanup) Can't locate OvTrace.pm in @INC (@INC contains: /usr/lpp/OV\lbin\eaagt\perl /usr/lpp/OV/lbin/eaagt/perl /var/opt/OV/bin/instrumentation /usr/lpp/OV/nonOV/perl/a/lib/5.8.8/aix-thread-multi /usr/lpp/OV/nonOV/perl/a/lib/5.8.8 /usr/lpp/OV/nonOV/perl/a/lib/site_perl/5.8.8/aix-thread-multi /usr/lpp/OV/nonOV/perl/a/lib/site_perl/5.8.8 /usr/lpp/OV/nonOV/perl/a/lib/site_perl .) at PerlScript line 136.` `BEGIN failed--compilation aborted at PerlScript line 136.` `. (OpC30-750)`
Cause	This error occurs on any policy and any *.pm file when the instrumentation is not deployed on the node correctly.
Solution	Forcefully deploy the instrumentation on the node.

Problem	StoreCollection throws coda_SetUTF8: coda_set_fcn_mismatch_data_type (80004005) error for SI-MSWindowsFailedLoginsCollector policy.
Solution	Run the following commands on the Windows node to recycle the CODA files: 1 `ovc -stop coda` 2 `rm -rf /var/opt/OV/datafiles/coda*` 3 `ovc -start coda`

We appreciate your feedback!

If an email client is configured on this system, by default an email window opens when you click on the bookmark “Comments”.

In case you do not have the email client configured, copy the information below to a web mail client, and send this email to **docfeedback@hp.com**

Product name:

Document title:

Version number:

Feedback: