Operations Smart Plug-in for System Infrastructure

Software Version: 12.06
Operations Manager for Windows®, HP-UX, Linux, and Solaris operating systems

User Guide

Document Release Date: May 2018
Software Release Date: May 2018

Legal Notices

Warranty

The only warranties for products and services of Micro Focus and its affiliates and licensors (“Micro Focus”) are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus 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. Except as specifically indicated, valid license from Micro Focus 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

© 2009-2018 Micro Focus or one of its affiliates

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

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

UNIX® is a registered trademark of The Open Group.

Documentation Updates

To check for recent updates or to verify that you are using the most recent edition of a document, go to: https://softwaresupport.softwaregrp.com/.

This site requires that you register for an Passport and to sign in. To register for an Passport ID, click **Register** on the Software Support site or click **Create an Account** on the Passport login page.

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

Support

Visit the Software Support site at: https://softwaresupport.softwaregrp.com/.

Most of the support areas require that you register as an Passport user and to sign in. Many also require a support contract. To register for an Passport ID, click **Register** on the Support site or click **Create an Account** on the Passport login page.

Contents

Chapter 1: Conventions Used in this Document 7
Chapter 2: Introduction 9
Chapter 3: Systems Infrastructure SPI Components 10
Map View on Operations Manager for Windows 10
Map View on Operations Manager for UNIX 12
Tools 13
Policies 14
Graphs 15
Reports 15
Chapter 4: Getting Started 16
On Operations Manager for Windows 16
Starting the SI SPI 17
Deploying Quick Start Policies from Operations Manager for Windows 18
On Operations Manager for UNIX 19
Starting the SI SPI 19
Deploying Quick Start Policies from Operations Manager for UNIX 20
Viewing Reports and Graphs 20
Integrating Performance Manager with Operations Manager for UNIX 21
Updating Reports after Upgrading the SPI 21
Data Collection for Reports 22
Chapter 5: Systems Infrastructure SPI Policies 23
Tracing 23
Discovery Policy 24
Restricting Discovery 24
Policies Monitoring Process and Service 29
Availability Policies 35
SI-ProcessMonitor 35
SI-ZombieProcessCountMonitor 39
Configuration Change Policies 40
SI-ChangeConfigurationMonitor 40

Hardware Monitoring Policies 45
Changing the Port Number 46
Server Health Traps Monitor Policy 47
RAID Controller Traps Monitor Policy 50
NIC Traps Monitor Policy 51
CMC Traps Monitor Policy 52
System Information Traps Monitor Policy 53
Virtual Connect Domain Traps Monitor Policy 54
Cluster Traps Monitor Policy 55
Rack Power Manager Traps Monitor Policy 55
Intelligent Drive Array Traps Monitor Policy 60
Rack Information Traps Monitor Policy 70
UPS Traps Monitor Policy 74
Blade Type 2 Traps Monitor Policy 75
Storage Systems Traps Monitor Policy 77
Virtual Connect Module Traps Monitor Policy 83
SIM Agent Process Monitoring Policy 83
Capacity Policies 84
Disk Capacity Monitor Policy 84
Remote Drive Space Utilization Monitor Policy 91
Remote Drive Space Utilization Monitor Policy for NFS filesystems 92
Remote Drive Space Utilization Monitor Policy for CIFS filesystems 93
Paged and Nonpaged Pool Utilization Policy 94
Log Monitoring Policies 94
Linux System Services Logfile Policies 95
Boot Log Policy 95
Secure Log Policy 95
Kernel Log Policy 96
Windows System Services Logfile Policies 96
NFS Log Policy 96
DNS Log Policy 97
Windows Logon Policy 97
Terminal Service Log Policy 98
Windows Server DHCP 98
Windows Server Disk Error Log Policy 99

AIX System Logfile Monitoring Policies 99
ERRPT Log Monitoring Policy 99
Performance Policies 100
Network Usage and Performance Policy 100
Memory Bottleneck Diagnosis Policy 104
CPU Spike Check Policy 108
CPU Bottleneck Diagnosis Policy 110
Sample Performance Policies 111
Disk Peak Utilization Monitor Policy 112
RealTimeAlerts Policy 113
SI-CPUStealtimeUtilMonitor 117
Adaptive Thresholding Policies 117
Configuring and Deploying SI-ConfigureBaselining Policy 118
Configuring and Deploying SI-AdaptiveThresholdingMonitor Policy 119
Configuring Deviations 120
Configuring Deviations in the SI-ConfigureBaselining Policy 120
Configuring Deviations in the SI-AdaptiveThresholdingMonitor Policy 122
Generating Alert Messages 123
Use Case: Using the Baseline Data for Adaptive Monitoring 124
Monitoring the CPU Utilization 125
Security Policies 126
Failed Login Collector Policy for Windows 127
Last Logon Collector Policy for Windows 127
Failed Login Collector Policy for Linux 128
Last Logon Collector Policy for Linux 129
Bad Login Policy for Linux 129
Bad Login Policy for AIX 130
Logins Policy for AIX 130
Switch User Policy for AIX 131
Sys Log Policy for AIX 132
Bad Logins Policy for HP-UX 132
Logins Policy for HP-UX 132
Switch User Policy for HP-UX 133

Syslog Policy for HP-UX 133
Sun Solaris Bad Logins 134
Sun Solaris Logins 134
Sun Solaris snmp Log Policy 135
Sun Solaris Syslog Policy 136
Deploying SI SPI Policies from Operations Manager for Windows Management Server 136
Deploying SI SPI Policies from Operations Manager for UNIX Management Server 138
Task 1: Assign Policy or Policy group 138
Task 2: Deploy Policies 138
Systems Infrastructure SPI Tool 139
Users Last Login Tool 139
Energy Data Collector 140
Chapter 6: Systems Infrastructure SPI Reports and Graphs 144
Systems Infrastructure SPI Reports 144
Systems Infrastructure SPI Graphs 146
Chapter 7: Troubleshooting 149
Send documentation feedback 153

Chapter 1: Conventions Used in this Document

The following conventions are used in this document.

Convention	Description
Operations Manager for UNIX	Operations Manager for UNIX is used in the document to imply OM on HP-UX, Linux, and Solaris. Wherever required, distinction is made for a specific operating system as: • OM on HP-UX • OM on Linux • OM on Solaris
Infrastructure SPIs	Operations Smart Plug-ins for Infrastructure. The software suite includes three Smart Plug-ins: • Operations Smart Plug-in for Systems Infrastructure • Operations Smart Plug-in for Virtualization Infrastructure • Operations Smart Plug-in for Cluster Infrastructure
SI SPI	Operations Smart Plug-in for Systems Infrastructure
VI SPI	Operations Smart Plug-in for Virtualization Infrastructure
CI SPI	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`.
`$OvDataDir`	The data directory variable on OM for UNIX management server and UNIX managed nodes. 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

Convention	Description
	based on your requirements. The default value is `C:\Program Files\HP\HP BTO Software`.
`$OvInstallDir`	The install directory variable on OM for UNIX management server and UNIX managed nodes. 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.

Chapter 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 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.

> **Note:** Reporter 4.0 is supported on 64-bit Windows operating system.

The SI SPI integrates with other software products such as the Operations Manager (OM), Performance Manager, Performance Agent, and Embedded Performance Component (EPC) of 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 *Operations Smart Plug-in for Systems Infrastructure Release Notes.*

Chapter 3: Systems Infrastructure SPI Components

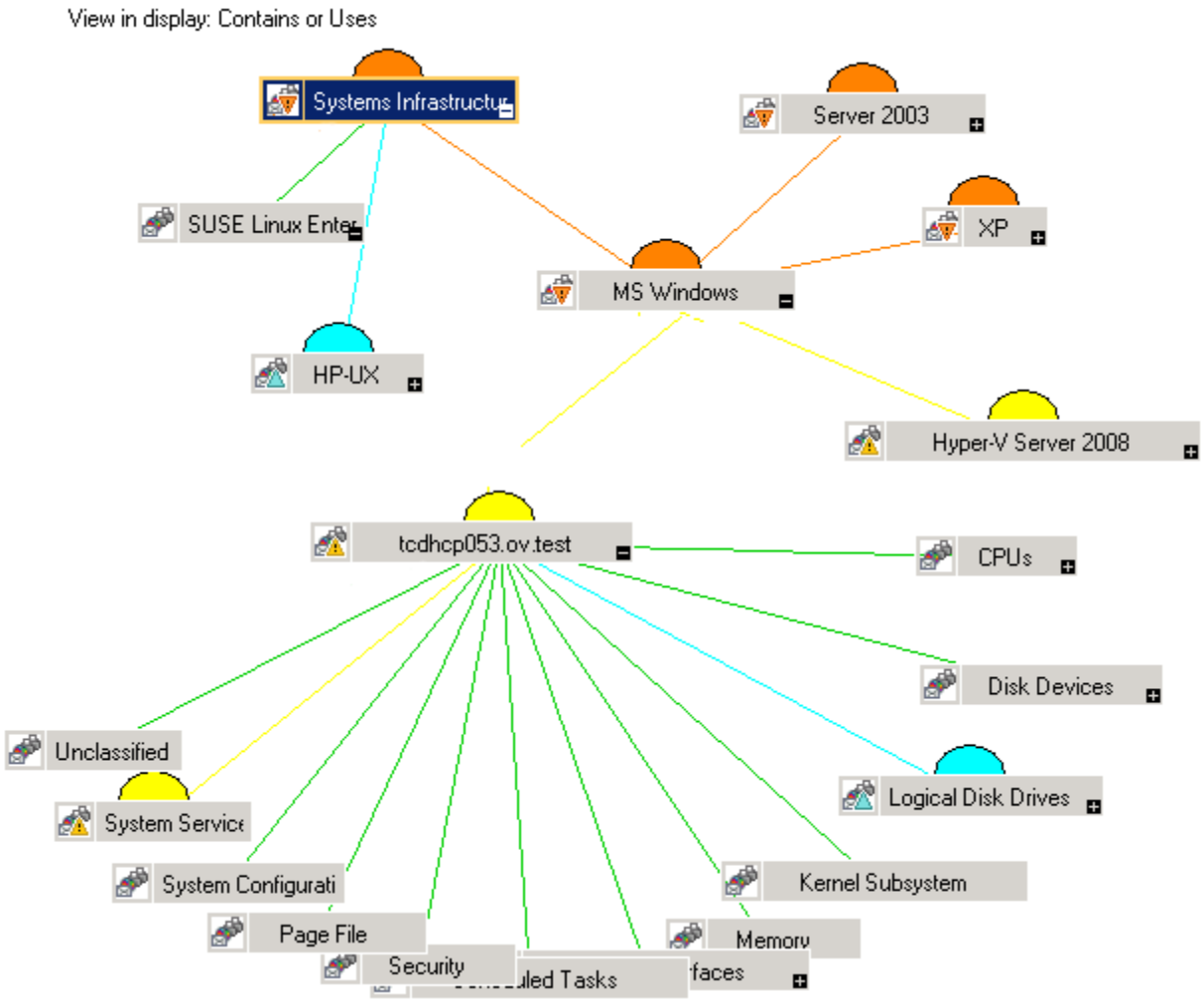
The SI SPI provides preconfigured policies and tools for monitoring the operations, availability, and performance of the managed nodes. These policies and tools, along with discovery, enable you to quickly gain control of the essential elements of your IT infrastructure.

Map View on Operations Manager for Windows

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

After you add a node to the OM console, the SI SPI service discovery policy is automatically deployed to the nodes and adds discovered information to the OM 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 OM 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. The following figure shows the Map view on OM 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 Operations Manager for UNIX

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

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

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

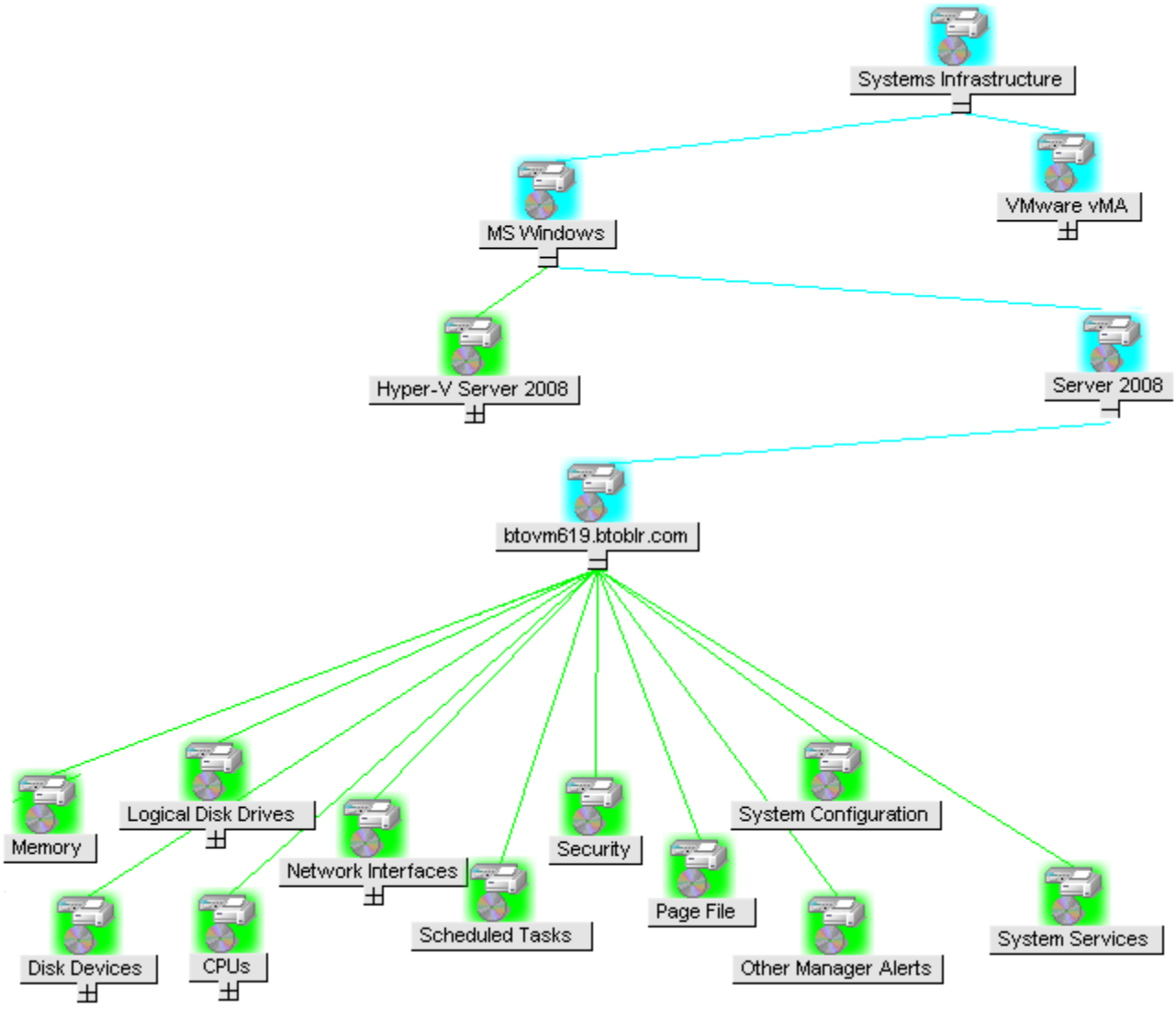
In this instance, *<operator name>* is the operator (for example, opc_adm or opc_op) to which you want to assign the service.

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 OM 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 OM 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" on page 139.

Policies

On Operations Manager for Windows, several default policies are automatically deployed on the supported managed nodes during installation. These policies 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 Operations Manager for Windows Management Server" on page 136.

For OM 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 Operations Manager for UNIX Management Server" on page 138.

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 policies' **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" on page 23.

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. OM is integrated with Performance Manager, a web-based analysis tool that helps you evaluate system performance, look at usage trends, and compare performance between systems. Using 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" on page 146.

Reports

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

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

For information about the reports provided by SI SPI, see "Systems Infrastructure SPI Reports" on page 144.

Chapter 4: Getting Started

After you install the infrastructure SPIs on the Operations Manager for Windows management server or Operations Manager for UNIX management server, you must complete the tasks required to manage your infrastructure.

The deployment checklist summarizes the tasks that you must complete before you start deploying the policies.

Deployment Checklist

Complete (Y/N)	Tasks
	Verify that you have installed OM 9.10 on the management server. On Windows: In addition, verify that Operations Agent version 11.00 or above is installed. On UNIX: In addition, verify that Operations Agent version 12.01 or above is installed. Make sure that you have installed all the available patches and hotfixes for OM and Operations Agent.
	Verify that you have Performance Manager and Reporter installed to generate the graphs and reports.
	Make sure that you give sufficient time to Operations Agent to collect the metrics before you start deploying the monitoring policies.

On Operations Manager for Windows

Follow the steps to getting started on Operations Manager for Windows.

Starting the SI SPI

After you install the SI SPI on the Operations Manager for Windows management server, follow the steps:

1. Add the nodes that you want to monitor. When adding the nodes, the option of **automatic deployment of policies and packages** is selected by default.

   This option enables autodeployment of the following policies on the managed node:

   - SI-SystemDiscovery
   - InfraSPI-Messages
   - OPC_OPCMON_OVERRIDE_THRESHOLD
   - OPC_PERL_INCLUDE_INSTR_DIR
   - AUTO_ADDITION_SETTINGS

   In case of existing nodes (that were added before the installation of Infrastructure SPIs), or where the **automatic deployment of policies and packages** check box was cleared while adding the managed node, manually deploy these policies.

2. To access and deploy the policies (in any order) on the managed nodes, follow these options in any order:

- Select **Policy management** → **Policy groups** → **Infrastructure Management** → **v12.0**→***<language>*** → **Messages**, and deploy InfraSPI-Messages policy.
- Select **Policy management** → **Policy groups** → **Infrastructure Management** → **v12.0**→ ***<language>*** → **Systems Infrastructure** → **AutoDiscovery,** and deploy SI-SystemDiscovery policy.
- Select **Policy management** → **Policy groups** → **Infrastructure Management** → **v12.0**→**Settings and Thresholds** → **Agent Settings**, and deploy the following policies:
  - AUTO_ADDITION_SETTINGS
  - OPC_OPCMON_OVERRIDE_THRESHOLD
  - OPC_PERL_INCLUDE_INSTR_DIR

> **Note:**
>
> - To automatically add guest virtual machines, set the AutoAdd_Guests parameter in the AUTO_ADDITION_SETTINGS policy to True. It is set as False by default.

- If a node is moved from one Windows management server to the other, make sure that you clean up the variables in `infraspi.nodegrp` namespace. If these variables are not cleaned, Auto Addition messages will not be triggered on the new Windows management server.

Deploying Quick Start Policies from Operations Manager for Windows

After the SI SPI discovery runs successfully, the discovered nodes are automatically added to the relevant Infrastructure SPI node groups.

By default, QuickStart policies are assigned to these node groups. When a node is added to the node group, these QuickStart policies are automatically deployed to the managed nodes (if policy autodeployment is enabled).

After the infrastructure is discovered and the service map is populated on the Operations Manager for Windows management server, the QuickStart policies are automatically deployed to the managed nodes (if policy autodeployment is enabled). Available for all three Infrastructure SPIs, QuickStart policies get you started immediately without having to spend much time customizing settings. Autodeployment of policies is enabled by default. 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.

The advanced policies are used in specific scenarios. You can manually deploy these policies as required.

If you turned off autodeployment of policies, you can manually deploy the QuickStart policies by accessing either of the two policies grouping provided by the Infrastructure SPIs. The groupings are based on monitored aspects and vendor and operating system. The monitored aspects based grouping helps you to access and deploy policies to monitor performance, availability, capacity, logs, and security aspects across multiple operating systems. For example, to monitor availability of scheduled job service on your infrastructure, expand:

Infrastructure Management → v12.0 →<language> → Systems Infrastructure → Availability → Scheduled Job Service

The **Policies grouped by Vendor** help you to quickly access the policies relevant to your operating system at one place. For example, to access SI-RHELCronProcessMonitor policy for deploying it on a managed node, expand:

Infrastructure Management → v12.0 →<language> → Systems Infrastructure → Policies grouped by Vendor → RHEL - Advanced Policies → SI-RHELCronProcessMonitor

On Operations Manager for UNIX

Follow the steps for getting started with the Infrastructure SPIs on Operations Manager for UNIX (HP-UX, Linux, and Solaris).

Before you start, make sure that you have installed the latest patches and hotfixes.

List of Patches

OM for HP-UX	OM for Linux	OM for Solaris
PHSS_43465	OML_000057	ITOSOL_00789

Starting the SI SPI

To add managed nodes and to deploy the SI SPI discovery policy, follow these steps:

1. Add the nodes that you want to monitor on the management server. These nodes appear in the Node Bank.

   SI SPI creates the SI-Deployment node group and auto-assigns the following policies to the node group:
   - SI-SystemDiscovery
   - SI-ConfigureDiscovery
   - InfraSPI-Messages
   - OPC_OPCMON_OVERRIDE_THRESHOLD
   - OPC_PERL_INCLUDE_INSTR_DIR
   - AUTO_ADDITION_SETTINGS
2. Add the managed nodes to the SI-Deployment node group.
3. Deploy (distribute) the assigned policies and Infrastructure SPI instrumentation on the managed nodes.

> **Note:** To automatically add guest virtual machines, set the AutoAdd_Guests parameter in the AUTO_ADDITION_SETTINGS policy to True. It is set as False by default.

Deploying Quick Start Policies from Operations Manager for UNIX

After the SI SPI discovery runs successfully, the discovered nodes are automatically added to the relevant Infrastructure SPI node groups.

By default, QuickStart policies are assigned to these node groups. When a node is added to the node group, these QuickStart policies get assigned to the node automatically. You must then deploy these policies manually on the node by selecting **Deploy Configuration** from the **Actions** menu in the Admin GUI.

Available for all three Infrastructure SPIs, QuickStart policies get you started immediately without having to spend much time customizing settings. Automatic assignment of policies is enabled by default.

The groupings are based on *monitored aspects* and *operating systems/vendor*. The monitored aspects based grouping helps you to access and deploy policies to monitor performance, availability, capacity, logs, and security aspects across multiple operating systems. For example, to monitor the availability of a scheduled job service on your infrastructure, select:

/ Policy Bank / Infrastructure Management / v12.0/en / Systems Infrastructure / Availability / Scheduled Job Service

The policies grouped by operating system and vendor help you to quickly access the policies relevant to your operating system at one place. For example, to access SI-CPUSpikeCheck policy for deploying it on a managed node, select:

/ Policy Bank / Infrastructure Management /v12.0 /en / Systems Infrastructure / Policies grouped by Vendor / RHEL - QuickStart Policies

Policies grouped by operating system include two sub groups: QuickStart and Advanced. The QuickStart group includes the policies that are used most often. The advanced policies like the disk utilization policy and the disk capacity monitor policy are used in specific scenarios.

Viewing Reports and Graphs

To generate and view reports and graphs from data collected by the Infrastructure SPIs, you must use Reporter and Performance Manager, respectively, in conjunction with OM. The Infrastructure SPIs

collect and store reporting and graphing data in a data store. The data store can be CODA (Operations Agent data store—also known as embedded performance component) or Performance Agent.

To view graphs on OM for HP-UX, Linux, or Solaris you need to first integrate Performance Manager with the OM management server.

Integrating Performance Manager with Operations Manager for UNIX

To integrate Operations Manager for UNIX (HP-UX, Linux, or Solaris) server with Performance Manager, follow these steps:

- If Performance Manager is installed on the OM server, run the following command:

  # /opt/OV/contrib/OpC/OVPM/install_OVPM.sh

  install_OVPM.sh <nodename>:<port>

  Example: install_OVPM.sh test.ovtest.com:8081

- If Performance Manager is installed on a remote system connected to the OM server, follow these steps:

1. Copy the graph templates from the remote system where Performance Manager is installed to the OM server. To learn about the graph types and their location on the system, see *Performance Manager Administrator Guide*.
2. Run the following command on the OM server:

   # /opt/OV/contrib/OpC/OVPM/install_OVPM.sh

   install_OVPM.sh <nodename>:<port>

   Example: install_OVPM.sh test.ovtest.com:8081

These steps set the host system configuration for Performance Manager, that is used when launching graphs from events in the OM operator GUI.

Updating Reports after Upgrading the SPI

After the upgrade, the existing report files are replaced with the new report files. Run the following command to update the reports.

1. Go to the **Start** menu.
2. Select **Run**.
3. At the prompt, type the command **repcrys** and click **Ok**.

Confirm that all the reports on the management server are in sync with the reports on the Reporter GUI. Click the **Reporter Status** tab in the Reporter GUI to check for the number reports sent to the console and also for any error message.

Data Collection for Reports

The reports provided for the SI SPI depend on policies. The following table lists the reports and policies that are required to be deployed on the managed node to collect data for corresponding reports.

Reports	Policies	Managed Node Platform	SPI
Last Logins/ Unused Logins	SI-MSWindowsLastLogonsCollector	Windows	Systems Infrastructure
Last Logins/ Unused Logins	SI-LinuxLastLogonsCollector	Linux	Systems Infrastructure
Failed Login	SI-MSWindowsFailedLoginsCollector	Windows	Systems Infrastructure
Failed Login	SI-UNIXFailedLoginsCollector	Linux, HP-UX, AIX, Solaris	Systems Infrastructure

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

Chapter 5: 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 addition to these policy subgroups, on the Operations Manager for UNIX Management Server two more policy subgroups for Korean (**ko**) and Spanish (**es**) have been added.

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

Policy Bank → Infrastructure Management → v12.0 →<*language*> → Systems Infrastructure

For information on deploying policies from the management server, see "Deploying SI SPI Policies from Operations Manager for UNIX Management Server" on page 138.

To access the policies on OM for Windows, select the following:

Policy management → Policy groups → Infrastructure Management → v12.0 →<*language*> → Systems Infrastructure.

For information on deploying policies from the management server, see "Deploying SI SPI Policies from Operations Manager for Windows Management Server" on page 136.

> **Note:** The **SI-LinuxSecureLog**, **SI-LinuxBootLog**, **SI-LinuxKernelLog**, **SI-ProcessMonitor** and **SI-LinuxLastLogonsCollector** policies do not work with Operations Agent running in non-root user mode.

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 *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 OM 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 OM 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 Operations Manager management server, which updates the service view with the changes. The default policy group for this policy is:

Infrastructure Management → v12.0 →<*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 `SI-Discovery.cfg` in the following folder:

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

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

> **Note:** 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: vdc0 Or

# DSK_EXCLUDE: vdc1

#

#NET include or exclude parameters should contain Network Interface name(In general
BYNETIF_NAME value)

# Example:

# NET_INCLUDE: lo0 Or

# NET_EXCLUDE: vnet0

#

#CPU include or exclude parameters should contain ID number of the CPU (In general
BYCPU_ID value)

# Example:

# CPU_INCLUDE: 0,1 Or

# 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.

> **Note:** 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 OM 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 OM 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`

Policies Monitoring Process and Service

The default policy groups for these policies are:

- **Infrastructure Management → v12.0 → <language> → Systems Infrastructure → Availability → *<process/service>* → *<os>***
- **Infrastructure Management → v12.0 → <language> → Systems Infrastructure → Policies grouped by vendor → *<os>*-Advanced**

In this instance, **<os>** is the operating system of the managed node. The supported operating systems are AIX, Debian, HP-UX, RHEL, SLES, Solaris, Ubuntu, and Windows. 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 OM 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
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]

Process/ Service Name	Monitoring Policy
SNMP Service	SI-UnixSnmpdProcessMonitor
System Logger	SI-AIXSyslogProcessMonitor
Terminal Services	-
Web Server	SI-AIXWebserverProcessMonitor

Table 2: Monitoring Policies for Debian

Process/ Service Name	Monitoring Policy
Apache	SI-DebianApacheProcessMonitor
Cron	SI-DebianCronProcessMonitor
Exim (Mail Transfer Agent)	SI-DebianEximProcessMonitor
Inetd	SI-DebianInetdProcessMonitor
Named	SI-DebianNamedProcessMonitor
Nfs Server	SI-DebianNfsServerProcessMonitor
Nmbd	SI-DebianNmbdProcessMonitor
Samba	SI-DebianSambaProcessMonitor
Sshd	SI-DebianSshdProcessMonitor

Table 3: 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

Process/ Service Name	Monitoring Policy
RPC Service	-
Scheduled Job Service	SI-HPUXCronProcessMonitor
Secure Login Service	• SI-HPUXSshdProcessMonitor • SI-OpenSshdProcessMonitor[1]
SNMP Service	SI-UnixSnmpdProcessMonitor
System Logger	SI-HPUXSyslogProcessMonitor
Terminal Services	-
Web Server	SI-HPUXWebserverProcessMonitor

Table 4: 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 5: Monitoring Policies for SLES

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-SLESCronProcessMonitor
Secure Login Service	• SI-LinuxSshdProcessMonitor • SI-OpenSshdProcessMonitor[1]
SNMP Service	SI-UnixSnmpdProcessMonitor
System Logger	SI-SLESSyslogProcessMonitor
Terminal Services	-
Web Server	SI-LinuxWebserverProcessMonitor

Table 6: 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	-

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

Table 7: Monitoring Policies for Ubuntu

Process/ Service Name	Monitoring Policy
Atd	SI-UbuntuAtdProcessMonitor
Cron	SI-UbuntuCronProcessMonitor
Inetd	SI-UbuntuInetdProcessMonitor
Nmb Server	SI-UbuntuNmbServerProcessMonitor
Smb Server	SI-UbuntuSmbServerProcessMonitor
Sshd	SI-UbuntuSshdProcessMonitor
Udev	SI-UbuntuUdevProcessMonitor

Table 8: 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

Process/ Service Name	Monitoring Policy
	• 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.

> **Note:** 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

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 default policy group for these policies is:

Infrastructure Management → v12.0 → <*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 OM 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.

SI-ProcessMonitor

SI-ProcessMonitor policy monitors a set of processes in a process group. All processes and process groups that you want to monitor with the SI-SPI must be defined in the configuration file, `procmon.cfg`. Alerts are generated whenever the processes defined in the configuration file either stop running or do not run as expected.

> **Note:** The configuration file can either be overwritten or modified using the `procmon_local.cfg` file. Use TAB as the delimiter in `procmon_local.cfg` files.

> Process groups associated with resource groups are monitored only if the corresponding resource group is online.
>
> SI-ProcessMonitor policy can monitor only 100 processes in 30 seconds.
>
> Ignore the (><) angle brackets that appear in the policy alerts.

SI-ProcessMonitorConfig File Policy:

SI-ProcessMonitorConfig file policy is a configuration file policy created for SI-ProcessMonitor. You must specify the following in the configuration file policy:

- Process groups that you want to monitor
- Location of the `procmon.cfg` file. Ensure you specify the location of the `procmon.cfg` file in the ConfigFileLocation parameter.

After the SI-ProcessMonitorConfig policy is deployed;

- If `procmon.cfg` file is not present, it is created at the location specified in the SI-ProcessMonitorConfig file policy.
- If `procmon.cfg` file is present, it is overwritten by the SI-ProcessMonitorConfig file policy.

The SI-ProcessMonitor policy monitors and displays:

- Processes that exceeds set limits.
- Processes that stop functioning.
- Processes that are out of limits during specified time of the day and day of the week.

Supported Platforms	Red Hat Enterprise Linux Suse Linux Enterprise Server HP-UX IBM-AIX Oracle Solaris Debian Ubuntu
Script parameters	**Description**
ProcMonGroupName	To monitor a process group in the configuration file, use the *ProcMonGroupName* parameter.
ConfigFilePath	Set the path of `procmon.cfg` file

LocalConfigFilePath	Set the path of `procmon_local.cfg` file
UseRepeatAlerts	Set this parameter to 1 to receive repeat alerts during every polling interval or set it to 0 to disable repeat alerts.
Debug	Set the value as: • 0 to disable trace messages. • 1 to receive trace messages on OM console. • 2 to log the messages in the trace file on the managed node. For more details, see "Tracing" on page 23.

Configuration File Syntax

Processes are grouped into process groups, as shown in the figure:

```
[OM_MGMT]
/opt/OV/bin/ovbbccb     -nodaemon        5-23    0,1,2,3,4,5,6    1-
/opt/OV/bin/ovcd        *        5-23    0,1,2,3,4,5,6    1-
/opt/OV/lbin/conf/ovconfd       *        5-23    0,1,2,3,4,5,6    1-
/opt/OV/lbin/sec/ovcs   *        5-23    0,1,2,3,4,5,6    1-
/opt/OV/bin/OpC/ovoareqsdr      -start   5-23    0,1,2,3,4,5,6    1-
/opt/OV/nonOV/jre/b/bin/java    -Dctlname=ovtomcatB -Dsun.lang.ClassLoader.allowAr
@severity=minor
```

In the instance marked in the screenshot:

Process Group name	OM_MGMT
Process name	/opt/OV/bin/ovbbccb
Argument	-nodaemon
Time of the day	5-23
Days of Week	0,1,2,3,4,5,6
Bounds	1-

Note: Name of a process group must be enclosed in square brackets.

Note: A process is identified even if you specify a part of the argument.

Syntax used to define processes and process groups in a configuration file is illustrated in the following table:

Column 1	Column 2	Column 3	Column 4	Column 5
Name	arguments	bounds		

Name @start=<cmd> @severity=<severity>	arguments	bounds		
Name	arguments	time of the day	day of week	bounds
Name @start=<cmd> @severity=<severity>	arguments	time of the day	days of week	bounds

In this instance:

Name: Specifies the name of the process to be monitored.

Arguments: Specifies the arguments that are used to distinguish between multiple processes running simultaneously. If no arguments are present, an asterisk (*) must be specified.

Time of the day: Specifies the time duration (in the 24-hour format) during which a process failure must be reported.

Day of Week: Specifies the day or days to report process failure. Each day of week is identified with a number as listed in the table.

Number	Day
0	Sunday
1	Monday
2	Tuesday
3	Wednesday
4	Thursday
5	Friday
6	Saturday

> **Note:** Numbers should be separated by commas.

Bounds: Specifies the number of instances of named processes. You can specify the number of instance as follows:

n	An exact number
n-	A minimum of n

-n	A maximum of n
m-n	A range of m to n

@Severity: Specifies the severity of alert messages such as Minor, Major or Critical. Default severity is Warning.

@Start: Specifies the command (<cmd>) that must be run during a process failure.

SI-ZombieProcessCountMonitor

SI-ZombieProcessCountMonitor policy (Measurement Threshold) monitors the number of zombie processes and sends alert messages to the OM console whenever there is a threshold violation.

Metrics Used	GBL_ZOMBIE_PROC
Supported Platforms	Red Hat Enterprise Linux Suse Linux Enterprise Server HP-UX IBM AIX Oracle Solaris Debian Ubuntu
Script-Parameter	**Description**
ZombieProcessCountCriticalThreshold	Set the threshold value with the minimum number of zombie processes at which you want to receive a Critical alert.
ZombieProcessCountMajorThreshold	Set the threshold value with the minimum number of zombie processes at which you want to receive a Major alert.
ZombieProcessCountMinorThreshold	Set the threshold value with the minimum number of zombie processes at which you want to receive a Minor alert.
ZombieProcessCountWarningThreshold	Set the threshold value with the minimum number of zombie processes at which you want to receive a Warning alert.
ShowDefunctProcessList	• By default, the value is set to **False**. • Set the value to **True** to display a list of 10

	zombie processes along with their process ID (PID).
Debug	Set the value as: • 0 to disable trace messages. • 1 to receive trace messages on OM console. • 2 to log the messages in the trace file on the managed node. For more details, see "Tracing" on page 23.

Configuration Change Policies

Configuration Change policies monitor files, Windows registry settings, and command outputs for changes.

SI-ChangeConfigurationMonitor

CCI Monitor (Change CI Monitoring or CCIMon) policy monitors files, Windows registry settings, and command outputs for changes listed in the configuration file `ccilist.cfg`. It reads the `ccilist.cfg` file at every run and alerts when there is a change in files, Windows registry settings, and command outputs.

To start monitoring changes, follow the steps:

1. Deploy the following:

   SI-ChangeConfigurationMonitor - Measurement threshold policy for Windows as well as Linux

On Windows	SI-MSWindowsCCIConfig - Configuration File policy for Windows
On LINUX	SI-LinuxCCIConfig – Configuration File policy for Linux and UNIX.
On AIX	SI-AIXCCIConfig - Configuration File policy for AIX.
On Solaris	SI-SunSolarisCCIConfig - Configuration File policy for Solaris
On HP-UX	SI-HPUXCCIConfig - Configuration File policy for HP-UX

2. A `ccilist.cfg` file is created in the `<OvDataDir>/ccimon/configuration` folder.

> **Note:** The `ccilist.cfg` file is the configuration file for monitoring changes on a system. You can modify this file with any editor. For more information see, "Using the ccilist.cfg file for Monitoring" below.
>
> To modify the changes that you want to monitor; add the changes in the `ccilist.cfg` file or in the Configuration File policy and redeploy the policy.

3. The CCI Monitor policy reads the `ccilist.cfg` file at every run and sends alerts when there is a change in files, Windows registry settings, and command outputs listed in the configuration file `ccilist.cfg`.

> **Note:** Ignore the duplicate messages for unknown alerts that appear in the **Application** box, on the **General** tab, in the **Message Properties** window.

Using the ccilist.cfg file for Monitoring

`ccilist.cfg` file located in the `<OvDataDir>/ccimon/configuration` folder, is the configuration file for monitoring changes on system. The CCI Monitor policy reads this file at every run. The policy monitors the following changes on a system:

- Software installed, removed or modified
- Patches/service packs/updates installed
- Changes to Kernel parameters
- Boot configuration
- Registry key
- Kernel image file
- All user accounts
- System service configuration,
- Shared directories, NFS or CIFS (samba) mounts added, modified or removed
- System environment variables

Syntax

Use the following syntax to add all the changes that you want to monitor:

```
<change ci key,cci type,msg group,backup filename,alert severity[,unicode]>
```

In this instance:

- `<change ci key>` - Specifies a registry key, a command or a file name with complete path.
- `<cci type>` - Set this to the following values - cmd, regkey, or file based on the change ci key.

  > **Note:** Registry key (regkey) type is available only for Windows managed nodes.

- `<msg group>` - Specifies the OM message group setting for the change alert.

  > **Note:** The default message group is Misc.

- `<backup filename>` - This is the name with which a backup file is created in the backup folder. The backup file created is used for comparisons with the parent file (provide empty value for monitoring CCI type 'file').

  > **Note:** Backup folder is located in the`<OvDataDir>/tmp` file.

- `<alert severity>` - Specifies the OM alert severity setting.

  > **Note:** The default alert severity is Warning.

- `<[unicode]>` - This is an optional setting. Set this for monitoring command output where the command output is in Unicode format (needed only for Windows).

Examples of using CCI Monitor policy:

1. To monitor the hosts file on Windows and send warning alerts with misc message group, run the command:

   ```
   c:\Windows\System32\drivers\etc\hosts,file,misc,,warning
   ```

   > **Note:** It is not essential to specify the backup file name for file monitoring and hence the field is left blank.

2. To monitor the `sys-temp` folder on Windows for any changes, use command type *change tracking*. Run the following command:

   ```
   dir "%temp%"| findstr /V bytes,cmd,OS,dirtmpbin,warning
   ```

   > **Note:**
   >
   > When the command is executed, `sys-temp` folder is searched for changes. The `findstr` command is used to remove the last few lines of the `dir` command output. The `dir` command output changes often and therefore generates too many false alerts.

> You can use Windows environment variables like %TEMP%. The values of the variable are computed by the Operations Agent user which may not be the Administrator or Domain user. For instance, %TEMP% is most likely evaluated as C:\Windows\Temp if the Operations Agent is running with user credentials of local system admin.

3. To monitor a registry key and its values on Windows, run the command:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\CCIMon,regkey,misc,temp,warning
   ```

4. On Windows, to monitor if opcmona.exe process is running on a node and if it is different from the last run, run the command:

   ```
   wmic process where name='opcmona.exe' get processid,cmd,OS,notepad-
   proc,major,unicode
   ```

   > **Note:** You can also use the command to check for unauthorized software running on a system.
   >
   > The wmic command output is in Unicode format, so the unicode specification is provided in last column.

5. To monitor if there are any new files or other changes in /tmp folder on Linux, run the command:

   ```
   ls -1 /tmp | sort -u,cmd,Misc,ls1tmp.txt,warning
   ```

6. To monitor if there are any user changes on UNIX / Linux, run the command:

   ```
   /etc/passwd,file,Security,,warning
   ```

7. To check for new filesystems mounted on UNIX / Linux, run the command:

   ```
   /etc/mtab,file,OS,,minor
   ```

Removing CCI Monitor Policy

Follow the steps:

1. Undeploy the policies from all nodes.
2. Clean up all files from the folder <OvDataDir>/tmp/ with the following names: *.backup and *.current.

Warnings and Limitations

- The CCI Monitor Policy writes log entries to help understand failures in processing runs. These logs are created with the name CCI Monitor-mm-dd-logfile.log in the <OvLogDir> folder. These files may occupy around 2 MB of space with default logging and a new file is created every day. You

can remove these files using rollover scripts.

- Ensure you deploy only one copy of the CCI Monitor policy on a node. For production uses, it is sufficient to use only the original policy along with the CCI config files. The backup routines are not thread-safe and can cause the monitoring to hang indefinitely due to file concurrency issues.
- The default frequency of monitoring is 1 minute. Monitoring more than twenty changed CIs might slow down the performance of the solution. Hence it is recommended to set up an interval of at least 5 minutes when the number of elements exceeds twenty changed CIs.

Desired State Monitoring

Desired State Monitoring monitors files, windows registry settings, and command outputs.

After deployment, the Desired State Monitoring checks for == in the configuration file **`ccilist.cfg`**. It compares the files, windows registry settings, and command outputs added in the configuration file with the corresponding gold file.

> **Note:** A gold file is a backup or reference file that remains unchanged.

Alerts are generated whenever there is a change in the monitored files, windows registry settings, and command outputs mentioned in the configuration file **`ccilist.cfg`**.

The functionality of Desired State Monitoring is same as that of SI-ChangeConfigurationMonitor (CCIMon) policy. The only difference is that with CCIMon policy, the backup file is overwritten by the current file (**`ccilist.cfg`**) after very run, but with Desired State Monitoring, the gold file (backup or reference file) remains unchanged.

> **Note:** Make sure that you enable Desired State Monitoring only after creating the gold file.

For example:

Let us assume that you want to monitor the file **mtab** located in the **/etc** directory. Backup this file and save it as **mtab.gold** in the **/etc** directory. This is your reference file or gold file which does not change. To monitor the **mtab** file add the following to the configuration file:

`/etc/mtab==/etc/mtab.gold,file,Os,,major`.

The Desired State Monitoring, reads the configuration file **`ccilist.cfg`** and compares the **mtab** file with the **mtab.gold** file. An alert is generated whenever there is a change in the **mtab** file as compared to the **mtab.gold** file.

Syntax used in the following examples for Desired State Monitoring :

1. To monitor the hosts file on Windows and send warning alerts to a miscellaneous message group, run the command:

   Syntax:`filename==reference file name,ccitype,msg group,[backup filename],alert severity,charset`

   Example: `/etc/mtab==/etc/mtab.gold,file,misc,,warning`

2. To monitor a folder on Windows for any changes, use the command type cmd for *change tracking*. Run the following command:

   Syntax:`command==Path of the file containing command output,ccitype,msg group, [backup filename],severity`

   Example: `ls /==/root/list.txt,cmd,Misc,,major`

   > **Note:**
   >
   > When you run the command `ls /`, the resulting output is compared with the content in the file `list.txt`. If any changes are found, alerts are sent to the users.

3. To monitor a registry key and its values on Windows, run the command:

   Syntax:`Registry key=='value of registry key',ccitype,msg group,[backup filename],severity`

   Example: `HKEY_LOCAL_MACHINE\SOFTWARE\config==config,regkey,misc,,warning`

Hardware Monitoring Policies

System Infrastructure SPI 12.06 provides policies that enable you to monitor the health and status of your ProLiant servers. These policies monitor SNMP traps generated by the SIM Agent and send alert messages to the OM console. All these policies are of the type SNMP Interceptor.

The default policy group for these policies is:

Infrastructure Management → v12.0 →*<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 Operations Agent 8.60, add:
  `[eaagt]`

  `SNMP_SESSION_MODE=NO_TRAPD`
- If you are using Operations Agent 12.06, 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 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 OM 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.
MIB ID	SNMP Trap Description
1.3.6.1.4.1.232.0.6003	System will be shut down due to this thermal condition.
1.3.6.1.4.1.232.0.6017	System will be shut down 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 shut down.
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 shut down.
1.3.6.1.4.1.232.0.6024	CPU fan is now OK.
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.
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 OM 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 RAID set 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.
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 OM 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 OM 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.
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 OM 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.
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 OM 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 OM 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 OM 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
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
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
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
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 OM 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.
1.3.6.1.4.1.232.0.3001	Intelligent DriveArray Logical Drive status is FAILED, contained in SNMP Varbind 1.
1.3.6.1.4.1.232.0.3001	Intelligent Drive Array Logical Drive status is RECOVERING, contained in SNMP Varbind 1.
1.3.6.1.4.1.232.0.3001	Intelligent Drive Array Logical Drive status is READY for REBUILD, contained in SNMP Varbind 1.
1.3.6.1.4.1.232.0.3001	Intelligent Drive Array Logical Drive status is REBUILDING, contained in SNMP Varbind 1.
1.3.6.1.4.1.232.0.3001	Intelligent Drive Array Logical Drive status is WRONG DRIVE, contained in SNMP Varbind 1.
1.3.6.1.4.1.232.0.3001	Intelligent Drive Array Logical Drive status is BAD

MIB ID	SNMP Trap Description
	CONNECTION, contained in SNMP Varbind 1.
1.3.6.1.4.1.232.0.3001	Intelligent Drive Array Logical Drive status is OVERHEATING, contained in SNMP Varbind 1.
1.3.6.1.4.1.232.0.3001	Intelligent Drive Array Logical Drive status is SHUTDOWN, contained in SNMP Varbind 1.
1.3.6.1.4.1.232.0.3001	Intelligent Drive Array Logical Drive status is NOT AVAILABLE, status is contained in SNMP Varbind 1.
1.3.6.1.4.1.232.0.3001	Intelligent Drive Array Logical Drive status is UNCONFIGURED, status is contained in SNMP Varbind 1.
1.3.6.1.4.1.232.0.3001	Intelligent Drive Array Logical Drive status is EXPANDING, status is contained in SNMP Varbind 1.
1.3.6.1.4.1.232.0.3001	Intelligent Drive Array Logical Drive status is QUEUED FOR EXPANSION, status is contained in SNMP Varbind 1.
1.3.6.1.4.1.232.0.3002	Intelligent Drive Array Spare Drive status is ACTIVE, status is contained in SNMP Varbind 1.
1.3.6.1.4.1.232.0.3002	Intelligent Drive Array Spare Drive status is INVALID, status is contained in SNMP Varbind 1.
1.3.6.1.4.1.232.0.3002	Intelligent Drive Array Spare Drive status is INACTIVE, status is contained in SNMP Varbind 1.
1.3.6.1.4.1.232.0.3002	Intelligent Drive Array Spare Drive status is FAILED, status is contained in SNMP Varbind 1.
1.3.6.1.4.1.232.0.3002	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.
1.3.6.1.4.1.232.0.3003	Intelligent Drive Array Physical Drive status is FAILED, contained in SNMP Varbind 1.
1.3.6.1.4.1.232.0.3003	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.

MIB ID	SNMP Trap Description
1.3.6.1.4.1.232.0.3005	Intelligent Drive Array Accelerator Board status is ENABLED, status is contained in SNMP Varbind 1.
1.3.6.1.4.1.232.0.3005	Intelligent Drive Array Accelerator Board status is TEMPORARILY DISABLED, status is contained in SNMP Varbind 1.
1.3.6.1.4.1.232.0.3005	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.
1.3.6.1.4.1.232.0.3007	Intelligent Drive Array Accelerator Board Battery status is NOT PRESENT. Status is contained in SNMP Varbind 1.
1.3.6.1.4.1.232.0.3007	Intelligent Drive Array Accelerator Board Battery status is OK. Status is contained in SNMP Varbind 1.
1.3.6.1.4.1.232.0.3007	Intelligent Drive Array Accelerator Board Battery status is failed. Status is contained in SNMP Varbind 1.
1.3.6.1.4.1.232.0.3007	Intelligent Drive Array Accelerator Board Battery status is degraded. Status is contained in SNMP Varbind 1.
1.3.6.1.4.1.232.0.3008	Intelligent DriveArray Logical Drive status is UNCONFIGURED, contained in SNMP Varbind 3.
1.3.6.1.4.1.232.0.3008	Intelligent DriveArray Logical Drive status is EXPANDING, contained in SNMP Varbind 3.
1.3.6.1.4.1.232.0.3008	Intelligent DriveArray Logical Drive status is QUEUED FOR EXPANSION, contained in SNMP Varbind 3.
1.3.6.1.4.1.232.0.3008	Intelligent DriveArray Logical Drive status is NORMAL, contained in SNMP Varbind 3.
1.3.6.1.4.1.232.0.3008	Intelligent DriveArray Logical Drive status is FAILED, contained in SNMP Varbind 3.
1.3.6.1.4.1.232.0.3008	Intelligent Drive Array Logical Drive status is RECOVERING, contained in SNMP Varbind 3.
1.3.6.1.4.1.232.0.3008	Intelligent Drive Array Logical Drive status is READY for REBUILD, contained in SNMP Varbind 3.
1.3.6.1.4.1.232.0.3008	Intelligent Drive Array Logical Drive status is REBUILDING, contained in SNMP Varbind 3

MIB ID	SNMP Trap Description
1.3.6.1.4.1.232.0.3008	Intelligent Drive Array Logical Drive status is WRONG DRIVE, contained in SNMP Varbind 3.
1.3.6.1.4.1.232.0.3008	Intelligent Drive Array Logical Drive status is BAD CONNECTION, contained in SNMP Varbind 3.
1.3.6.1.4.1.232.0.3008	Intelligent Drive Array Logical Drive status is OVERHEATING, contained in SNMP Varbind 3.
1.3.6.1.4.1.232.0.3008	Intelligent Drive Array Logical Drive status is SHUTDOWN, contained in SNMP Varbind 3.
1.3.6.1.4.1.232.0.3008	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.
1.3.6.1.4.1.232.0.3009	Intelligent Drive Array Spare Drive status is INACTIVE, status is contained in SNMP Varbind 3.
1.3.6.1.4.1.232.0.3009	Intelligent Drive Array Spare Drive status is ACTIVE, status is contained in SNMP Varbind 3.
1.3.6.1.4.1.232.0.3009	Intelligent Drive Array Spare Drive status is FAILED, status is contained in SNMP Varbind 3.
1.3.6.1.4.1.232.0.3009	Intelligent Drive Array Spare Drive status is BUILDING, status is contained in SNMP Varbind 3.
1.3.6.1.4.1.232.0.3010	Intelligent Drive Array Physical Drive status is OK, contained in SNMP Varbind 3.
1.3.6.1.4.1.232.0.3010	Intelligent Drive Array Physical Drive status is FAILED, contained in SNMP Varbind 3 on SCSI Bus contained in Varbind 4.
1.3.6.1.4.1.232.0.3010	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.
1.3.6.1.4.1.232.0.3012	Intelligent Drive Array Accelerator Board status is ENABLED, status is contained in SNMP Varbind 3.
1.3.6.1.4.1.232.0.3012	Intelligent Drive Array Accelerator Board status is

MIB ID	SNMP Trap Description
	TEMPORARILY DISABLED, status is contained in SNMP Varbind 3.
1.3.6.1.4.1.232.0.3012	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.
1.3.6.1.4.1.232.0.3014	Intelligent Drive Array Accelerator Board Battery status is NOT PRESENT. Status is contained in SNMP Varbind 3.
1.3.6.1.4.1.232.0.3014	Intelligent Drive Array Accelerator Board Battery status is OK. Status is contained in SNMP Varbind 3.
1.3.6.1.4.1.232.0.3014	Intelligent Drive Array Accelerator Board Battery status is failed. Status is contained in SNMP Varbind 3.
1.3.6.1.4.1.232.0.3014	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.
1.3.6.1.4.1.232.0.3015	Intelligent Drive Array Controller status is FAILED, status is contained in SNMP Varbind 4.
1.3.6.1.4.1.232.0.3015	Intelligent Drive Array Controller has cable problem, status is contained in SNMP Varbind 4.
1.3.6.1.4.1.232.0.3015	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.
1.3.6.1.4.1.232.0.3017	Intelligent Drive Array Spare Drive status is INVALID, status is contained in SNMP Varbind 3.
1.3.6.1.4.1.232.0.3017	Intelligent Drive Array Spare Drive status is INACTIVE, status is contained in SNMP Varbind 3.
1.3.6.1.4.1.232.0.3017	Intelligent Drive Array Spare Drive status is ACTIVE, status is contained in SNMP Varbind 3.
1.3.6.1.4.1.232.0.3017	Intelligent Drive Array Spare Drive status is FAILED, status is contained in SNMP Varbind 3.
1.3.6.1.4.1.232.0.3017	Intelligent Drive Array Spare Drive status is BUILDING, status is

MIB ID	SNMP Trap Description
	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.
1.3.6.1.4.1.232.0.3018	Intelligent Drive Array Physical Drive status is FAILED, contained in SNMP Varbind 3.
1.3.6.1.4.1.232.0.3018	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.
1.3.6.1.4.1.232.0.3020	Intelligent Drive Array Tape Library status is FAILED, status is contained in SNMP Varbind 7 for the tape library.
1.3.6.1.4.1.232.0.3020	Intelligent Drive Array Tape Library status is DEGRADED, status is contained in SNMP Varbind 7 for the tape library.
1.3.6.1.4.1.232.0.3020	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.
1.3.6.1.4.1.232.0.3021	Intelligent Drive Array Tape Library Door Status is CLOSED, status is contained in SNMP Varbind 7.
1.3.6.1.4.1.232.0.3021	Intelligent Drive Array Tape Library Door Status is NOT SUPPORTED, status is contained in SNMP Varbind 7.
1.3.6.1.4.1.232.0.3022	Intelligent Drive Array Tape Drive Status is OK, status is contained in SNMP Varbind 7.
1.3.6.1.4.1.232.0.3022	Intelligent Drive Array Tape Drive Status is DEGRADED, status is contained in SNMP Varbind 7.
1.3.6.1.4.1.232.0.3022	Intelligent Drive Array Tape Drive Status is FAILED, status is contained in SNMP Varbind 7.
1.3.6.1.4.1.232.0.3022	Intelligent Drive Array Tape Drive Status is OFFLINE, status is contained in SNMP Varbind 7.
1.3.6.1.4.1.232.0.3022	Intelligent Drive Array Tape Drive Status is MISSING WAS OK, status is contained in SNMP Varbind 7.
1.3.6.1.4.1.232.0.3022	Intelligent Drive Array Tape Drive Status is MISSING WAS

MIB ID	SNMP Trap Description
	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.
1.3.6.1.4.1.232.0.3025	Intelligent Drive Array Accelerator Board status is ENABLED, status is contained in SNMP Varbind 7.
1.3.6.1.4.1.232.0.3025	Intelligent Drive Array Accelerator Board status is TEMPORARILY DISABLED, status is contained in SNMP Varbind 7.
1.3.6.1.4.1.232.0.3025	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.
1.3.6.1.4.1.232.0.3028	Intelligent Drive Array Controller Board has failed, status is contained in SNMP Varbind 4.
1.3.6.1.4.1.232.0.3028	Intelligent Drive Array Controller Board has cable problem, status is contained in SNMP Varbind 4.
1.3.6.1.4.1.232.0.3028	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.
1.3.6.1.4.1.232.0.3029	Intelligent Drive Array Physical Drive status is FAILED, contained in SNMP Varbind 3.
1.3.6.1.4.1.232.0.3029	Intelligent Drive Array Physical Drive status is PREDICTIVEFAILURE, status is contained in SNMP Varbind 3.
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.

MIB ID	SNMP Trap Description
1.3.6.1.4.1.232.0.3031	Intelligent Drive Array Tape Library status is OK, status is contained in SNMP Varbind 10 for the tape library.
1.3.6.1.4.1.232.0.3031	Intelligent Drive Array Tape Library status is DEGRADED, status is contained in SNMP Varbind 10 for the tape library.
1.3.6.1.4.1.232.0.3031	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.
1.3.6.1.4.1.232.0.3032	Intelligent Drive Array Tape Drive status is OFFLINE, status is contained in SNMP Varbind 7.
1.3.6.1.4.1.232.0.3032	Intelligent Drive Array Tape Drive status is DEGRADED, status is contained in SNMP Varbind 7.
1.3.6.1.4.1.232.0.3032	Intelligent Drive Array Tape Drive status is FAILED, status is contained in SNMP Varbind 10.
1.3.6.1.4.1.232.0.3032	Intelligent Drive Array Tape Drive status is MISSING WAS OK, status is contained in SNMP Varbind 10.
1.3.6.1.4.1.232.0.3032	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.
1.3.6.1.4.1.232.0.3033	Intelligent Drive Array Controller has a CABLE PROBLEM, status is contained in SNMP Varbind 5.
1.3.6.1.4.1.232.0.3033	Intelligent Drive Array Controller is POWERED OFF, status is contained in SNMP Varbind 5.
1.3.6.1.4.1.232.0.3033	Intelligent Drive Array Controller is OK, status is contained in SNMP Varbind 5.
1.3.6.1.4.1.232.0.3034	Intelligent Drive Array Logical Drive status is UNCONFIGURED, contained in SNMP Varbind 6.
1.3.6.1.4.1.232.0.3034	Intelligent Drive Array Logical Drive status is QUEUED FOR EXPANSION, status is contained in SNMP Varbind 6.
1.3.6.1.4.1.232.0.3034	Intelligent DriveArray Logical Drive status is NORMAL, contained in SNMP Varbind 6.
1.3.6.1.4.1.232.0.3034	Intelligent DriveArray Logical Drive status is FAILED, contained in SNMP Varbind 6.

MIB ID	SNMP Trap Description
1.3.6.1.4.1.232.0.3034	Intelligent Drive Array Logical Drive status is RECOVERING, contained in SNMP Varbind 6.
1.3.6.1.4.1.232.0.3034	Intelligent Drive Array Logical Drive status is READY for REBUILD, contained in SNMP Varbind 6.
1.3.6.1.4.1.232.0.3034	Intelligent Drive Array Logical Drive status is REBUILDING, contained in SNMP Varbind 6.
1.3.6.1.4.1.232.0.3034	Intelligent Drive Array Logical Drive status is WRONG DRIVE, contained in SNMP Varbind 6.
1.3.6.1.4.1.232.0.3034	Intelligent Drive Array Logical Drive status is BAD CONNECTION, contained in SNMP Varbind 6.
1.3.6.1.4.1.232.0.3034	Intelligent Drive Array Logical Drive status is OVERHEATING, contained in SNMP Varbind 6.
1.3.6.1.4.1.232.0.3034	Intelligent Drive Array Logical Drive status is SHUTDOWN, contained in SNMP Varbind 6.
1.3.6.1.4.1.232.0.3034	Intelligent Drive Array Logical Drive status is EXPANDING, status is contained in SNMP Varbind 6.
1.3.6.1.4.1.232.0.3034	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.
1.3.6.1.4.1.232.0.3035	Intelligent Drive Array Spare Drive status is INACTIVE, status is contained in SNMP Varbind 6.
1.3.6.1.4.1.232.0.3035	Intelligent Drive Array Spare Drive status is ACTIVE, status is contained in SNMP Varbind 6.
1.3.6.1.4.1.232.0.3035	Intelligent Drive Array Spare Drive status is FAILED, status is contained in SNMP Varbind 6.
1.3.6.1.4.1.232.0.3035	Intelligent Drive Array Spare Drive status is BUILDING, status is contained in SNMP Varbind 6.
1.3.6.1.4.1.232.0.3036	Intelligent Drive Array Physical Drive status is OK, contained in SNMP Varbind 12.
1.3.6.1.4.1.232.0.3036	Intelligent Drive Array Physical Drive status is FAILED, contained in SNMP Varbind 12.
1.3.6.1.4.1.232.0.3036	Intelligent Drive Array Physical Drive status is PREDICTIVEFAILURE, status is contained in SNMP Varbind 12.

MIB ID	SNMP Trap Description
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.
1.3.6.1.4.1.232.0.3038	Intelligent Drive Array Accelerator Board status is ENABLED, status is contained in SNMP Varbind 8.
1.3.6.1.4.1.232.0.3038	Intelligent Drive Array Accelerator Board status is TEMPORARILY DISABLED, status is contained in SNMP Varbind 8.
1.3.6.1.4.1.232.0.3038	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.
1.3.6.1.4.1.232.0.3041	Intelligent Drive Array Tape Library status is DEGRADED, status is contained in SNMP Varbind 11 for the tape library.
1.3.6.1.4.1.232.0.3041	Intelligent Drive Array Tape Library status is FAILED, status is contained in SNMP Varbind 11 for the tape library.
1.3.6.1.4.1.232.0.3041	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.
1.3.6.1.4.1.232.0.3042	Intelligent Drive Array Tape Library Door Status is CLOSED, status is contained in SNMP Varbind 11.
1.3.6.1.4.1.232.0.3042	Intelligent Drive Array Tape Library Door Status is NOT SUPPORTED, status is contained in SNMP Varbind 11.
1.3.6.1.4.1.232.0.3043	Intelligent Drive Array Tape Drive status is DEGRADED, status is contained in SNMP Varbind 11.
1.3.6.1.4.1.232.0.3043	Intelligent Drive Array Tape Drive Status is OK, status is contained in SNMP Varbind 11.
1.3.6.1.4.1.232.0.3043	Intelligent Drive Array Tape Drive Status is FAILED, 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 OFFLINE, status is contained in SNMP Varbind 11.
1.3.6.1.4.1.232.0.3043	Intelligent Drive Array Tape Drive Status is MISSING WAS OK, status is contained in SNMP Varbind 11.
1.3.6.1.4.1.232.0.3043	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.
1.3.6.1.4.1.232.0.3046	Physical Drive Status is FAILED, status is contained in SNMP Varbind 12.
1.3.6.1.4.1.232.0.3046	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 OM 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

MIB ID	SNMP Trap Description
	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.
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.

MIB ID	SNMP Trap Description
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.
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.

MIB ID	SNMP Trap Description
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.
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

MIB ID	SNMP Trap Description
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
1.3.6.1.4.1.232.0.22064	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 OM 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 OM 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
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 OM 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.
1.3.6.1.4.1.232.0.8001	Storage System fan status changed to FAILED, status contained in SNMP Varbind 1.
1.3.6.1.4.1.232.0.8001	Storage System fan status changed to DEGRADED, status contained in SNMP Varbind 1.
1.3.6.1.4.1.232.0.8001	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 shut down 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.

MIB ID	SNMP Trap Description
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.
1.3.6.1.4.1.232.0.8008	Storage System fan status changed to FAILED, status is contained in SNMP Varbind 3.
1.3.6.1.4.1.232.0.8008	Storage System fan status changed to DEGRADED, status is contained in SNMP Varbind 3.
1.3.6.1.4.1.232.0.8008	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.
1.3.6.1.4.1.232.0.8016	Storage System fan status changed to NOT INSTALLED, status is contained in SNMP Varbind 6.
1.3.6.1.4.1.232.0.8016	Storage System fan status changed to OK, status is contained in SNMP Varbind 6.
1.3.6.1.4.1.232.0.8016	Storage System fan status changed to DEGRADED, status is contained in SNMP Varbind 6.
1.3.6.1.4.1.232.0.8016	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.
1.3.6.1.4.1.232.0.8017	Storage System power supply status changed to OK, status is contained in SNMP Varbind 6.
1.3.6.1.4.1.232.0.8017	Storage System power supply 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 DEGRADED, status

MIB ID	SNMP Trap Description
	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.
1.3.6.1.4.1.232.0.8018	Storage System power supply UPS status changed to NO UPS, status is contained in SNMP Varbind 6.
1.3.6.1.4.1.232.0.8018	Storage System power supply UPS status changed to Power FAILED, status is contained in SNMP Varbind 6.
1.3.6.1.4.1.232.0.8018	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.
1.3.6.1.4.1.232.0.8019	Storage System temperature sensor status has changed to DEGRADED, status is contained in SNMP Varbind 6.
1.3.6.1.4.1.232.0.8019	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.
1.3.6.1.4.1.232.0.8020	Storage System fan status changed to NOT INSTALLED, status is contained in SNMP Varbind 6.
1.3.6.1.4.1.232.0.8020	Storage System fan status changed to DEGRADED, status is contained in SNMP Varbind 6.
1.3.6.1.4.1.232.0.8020	Storage System fan status changed to FAILED, status is contained in SNMP Varbind 6.
1.3.6.1.4.1.232.0.8021	Storage System power supply status changed to OK, status is contained in SNMP Varbind 6.
1.3.6.1.4.1.232.0.8021	Storage System power supply status changed to FAILED, status is contained in SNMP Varbind 6.
1.3.6.1.4.1.232.0.8021	Storage System power supply status changed to NOT INSTALLED, status is contained in SNMP Varbind 6.
1.3.6.1.4.1.232.0.8021	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.
1.3.6.1.4.1.232.0.8022	Storage System fan status changed to DEGRADED, status is

MIB ID	SNMP Trap Description
	contained in SNMP Varbind 9.
1.3.6.1.4.1.232.0.8022	Storage System fan status changed to FAILED, status is contained in SNMP Varbind 9.
1.3.6.1.4.1.232.0.8022	Storage System fan status changed to Not Supported, status is contained in SNMP Varbind 9.
1.3.6.1.4.1.232.0.8022	Storage System fan status changed to degraded-Fan1FAILED, status is contained in SNMP Varbind 9.
1.3.6.1.4.1.232.0.8022	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.
1.3.6.1.4.1.232.0.8023	Storage System temperature status changed to DEGRADED, status is contained in SNMP Varbind 9.
1.3.6.1.4.1.232.0.8023	Storage System temperature status changed to FAILED, status is contained in SNMP Varbind 9.
1.3.6.1.4.1.232.0.8023	Storage System temperature status changed to NO TEMP, status is contained in SNMP Varbind 9.
1.3.6.1.4.1.232.0.8023	Storage System temperature status changed to not supported, status is contained in SNMP Varbind 9.
1.3.6.1.4.1.232.0.8024	Storage System power supply status changed to OK, status is contained in SNMP Varbind 9.
1.3.6.1.4.1.232.0.8024	Storage System power supply status changed to DEGRADED, status is contained in SNMP Varbind 9.
1.3.6.1.4.1.232.0.8024	Storage System power supply status changed to FAILED, status is contained in SNMP Varbind 9.
1.3.6.1.4.1.232.0.8024	Storage System power supply status changed to noFltTolPower, status is contained in SNMP Varbind 9.
1.3.6.1.4.1.232.0.8024	Storage System power supply status changed to not supported, status is contained in SNMP Varbind 9.
1.3.6.1.4.1.232.0.8024	Storage System power supply status changed to noFltTolPower-Bay1Missing, status is contained in SNMP Varbind 9.
1.3.6.1.4.1.232.0.8024	Storage System power supply status changed to noFltTolPower-Bay2Missing, status is contained in SNMP Varbind 9.
1.3.6.1.4.1.232.0.8024	Storage System power supply status changed to OK, status is

MIB ID	SNMP Trap Description
	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.
1.3.6.1.4.1.232.8.0.1	Storage System fan status changed to FAILED, status is contained in SNMP Varbind 1.
1.3.6.1.4.1.232.8.0.1	Storage System fan status changed to DEGRADED, status is contained in SNMP Varbind 1.
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.
1.3.6.1.4.1.232.0.8025	Storage system recovery server option status changed to OK, status is contained in SNMP Varbind 5.
1.3.6.1.4.1.232.0.8025	Storage system recovery server option status changed to DEAMON DOWN ACTIVE, status is contained in SNMP Varbind 5.
1.3.6.1.4.1.232.0.8025	Storage system recovery server option status changed to NOSECONDARY, status is contained in SNMP Varbind 5.
1.3.6.1.4.1.232.0.8025	Storage system recovery server option status changed to DEAMON DOWN NOSECONDARY, status is contained in SNMP Varbind 5.
1.3.6.1.4.1.232.0.8025	Storage system recovery server option status changed to LINKDOWN, status is contained in SNMP Varbind 5.
1.3.6.1.4.1.232.0.8025	Storage system recovery server option status changed to DEAMON DOWN LINKDOWN, status is contained in SNMP Varbind 5.
1.3.6.1.4.1.232.0.8025	Storage system recovery server option status changed to SECONDARY RUNNING AUTO, status is contained in SNMP Varbind 5.
1.3.6.1.4.1.232.0.8025	Storage system recovery server option status changed to SECONDARY RUNNING USER, status is contained in SNMP Varbind 5.
1.3.6.1.4.1.232.0.8025	Storage system recovery server option status changed to NOT CONFIGURED, status is contained in SNMP Varbind 5.
1.3.6.1.4.1.232.0.8025	Storage system recovery server option status changed to NOT SUPPORTED, status is contained in SNMP Varbind 5.
1.3.6.1.4.1.232.0.8025	Storage system recovery server option status changed to DISABLED, status is contained in SNMP Varbind 5.
1.3.6.1.4.1.232.0.8025	Storage system recovery server option status changed to evTimeOutError, status is contained in SNMP Varbind 5.

MIB ID	SNMP Trap Description
1.3.6.1.4.1.232.0.8026	Storage System fan status changed to OK, status is contained in SNMP Varbind 9.
1.3.6.1.4.1.232.0.8026	Storage System fan status changed to FAILED, status is contained in SNMP Varbind 9.
1.3.6.1.4.1.232.0.8026	Storage System fan status changed to DEGRADED, status is contained in SNMP Varbind 9.
1.3.6.1.4.1.232.0.8026	Storage System fan status changed to NO FAN, status is contained in SNMP Varbind 9.
1.3.6.1.4.1.232.0.8027	Storage System temperature status is DEGRADED, status is contained in SNMP Varbind 9.
1.3.6.1.4.1.232.0.8027	Storage System temperature status is FAILED, status is contained in SNMP Varbind 9.
1.3.6.1.4.1.232.0.8027	Storage System temperature status is OK, status is contained in SNMP Varbind 9.
1.3.6.1.4.1.232.0.8027	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
1.3.6.1.4.1.232.0.8028	Storage System power supply unit status is FAILED, status is contained in SNMP Varbind 9.
1.3.6.1.4.1.232.0.8028	Storage System power supply unit status is OK, status is contained in SNMP Varbind 9.
1.3.6.1.4.1.232.0.8028	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.
1.3.6.1.4.1.232.0.8029	Storage System fan status changed to FAILED, status is contained in SNMP Varbind 9.
1.3.6.1.4.1.232.0.8029	Storage System fan status changed to DEGRADED, status is contained in SNMP Varbind 9.
1.3.6.1.4.1.232.0.8029	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.

MIB ID	SNMP Trap Description
1.3.6.1.4.1.232.0.8030	Storage System temperature status changed to DEGRADED, status is contained in SNMP Varbind 9.
1.3.6.1.4.1.232.0.8030	Storage System temperature status changed to FAILED, status is contained in SNMP Varbind 9.
1.3.6.1.4.1.232.0.8030	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.
1.3.6.1.4.1.232.0.8031	Storage System power supply status changed to FAILED, status is contained in SNMP Varbind 9.
1.3.6.1.4.1.232.0.8031	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 OM 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 OM 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 → v12.0 → <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, free space available and inode utilization. The policy sends out an alert to the OM console, if the space utilization exceeds or falls below the specified threshold values.

SI-DiskCapacityMonitorConfig File Policy:

SI-DiskCapacityMonitorConfig file policy is a configuration file policy created for SI-DiskCapacityMonitor. In the configuration file policy specify the following:

- All the filesystems that you want to monitor along with the necessary thresholds
- Location of `osspi_global_fsmon.cfg` file. Make sure you enter the same location in Config FilePath script parameter present in SI-DiskCapacityMonitor.

After the SI-DiskCapacityMonitorConfig file policy is deployed, `osspi_global_fsmon.cfg` file is created (if it is not present) along with the filesystems and specified thresholds, at the location specified in the SI-DiskCapacityMonitorConfig file policy. If `osspi_global_fsmon.cfg` file is present, it is overwritten with the filesystems and thresholds mentioned in the SI-DiskCapacityMonitorConfig file policy that is deployed.

You can use the **Fsmon** feature to monitor filesystems and send alert messages based on the thresholds defined. The policy reads the filesystems listed in the following configuration files:

- osspi_fsmon.cfg
- osspi_global_fsmon.cfg
- osspi_local_fsmon.cfg

> **Note:**
>
> The osspi_fsmon.cfg is located at /var/opt/OV/conf/osspi/osspi_fsmon.cfg.
>
> You can create the osspi_global_fsmon.cfg file at a preferred location and then specify the path in the GlobalConfigFilePath script parameter.
>
> You can create the osspi_local_fsmon.cfg file at a preferred location and then specify the path in the LocalConfigFilePath script parameter.

> **Note:** osspi_fsmon.cfg is available only if you have installed OSSPI.
>
> Do not edit the default configuration file, osspi_fsmon.cfg.
>
> Use the osspi_global_fsmon.cfg file to modify or overwrite the osspi_fsmon.cfg file.
>
> Use the osspi_local_fsmon.cfg file to modify or overwrite the osspi_global_fsmon.cfg file.

If you have OSSPI installed, the order of precedence of the configuration files is as follows:

Local file (osspi_local_fsmon.cfg), global file (osspi_global_fsmon.cfg) and then the default file (osspi_fsmon.cfg).

If you do not have OSSPI installed, the order of precedence of the configuration files is as follows:

Local file (osspi_local_fsmon.cfg) and the global file (osspi_global_fsmon.cfg).

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

Metrics Used	FS_MAX_SIZE FS_SPACE_USED FS_SPACE_UTIL FS_TYPE FS_DIRNAME FS_SPACE_RESERVED FS_INODE_UTIL

Supported Platforms	Microsoft Windows Red Hat Enterprise Linux Suse Linux Enterprise Server HP-UX IBM AIX Oracle Solaris Debian Ubuntu
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.
InodeUtilCriticalThreshold	The threshold is expressed as the filesystem Index node (inode) utilization and is available for UNIX only. Set the threshold value at which you want to receive a critical message.
InodeUtilMajorThreshold	Set the threshold value at which you want to receive a major message.
InodeUtilMinorThreshold	Set the threshold value at which you want to receive a minor message.
InodeUtilWarningThreshold	Set the threshold value at which you want to receive a warning

	message.
MessageGroup	Message group for outgoing messages. **OS** is the default message group for all alerts from this policy. You can specify different message groups for different file systems. For example, see Message Group Example.
ExcludeFilesystems	Specify the filesystems or the file system types that you want to exclude from monitoring. If both filesystem and filesystem type are specified, then the filesystem type takes precedence over filesystem.
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" on page 23.
UseFsmonConfigSettings	Set to True, to enable **Fsmon** configuration based thresholds. **Note:** Ensure that you enable continuous action for each of the thresholds defined. Set to False, to enable the default behavior of SI-DiskCapacitiyMonitor policy.
GlobalConfigFilePath	Set the path of `fsmon global` configuration file.
LocalConfigFilePath	Set the path of `fsmon local` configuration file.

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=80,/=65,c:=65**

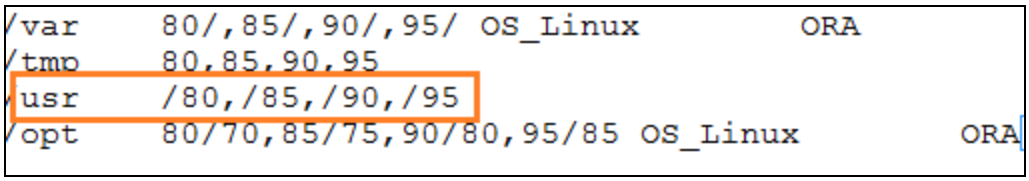
  In this example, the threshold values are set at 65% for the '*/*' and '*C:*' drives, and 80% for all other drives/filesystems on the managed node. If the system utilization for these drives/filesystems exceeds the threshold values, the policy sends out a critical alert.

- **FreeSpaceMajorThreshold=256,E:=200,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.

Configuration File Syntax

File systems are entered in the configuration file as shown in the figure:



In the instance marked in the screenshot:

/usr	File system
80	Warning threshold
85	Minor threshold
90	Major threshold
95	Critical threshold
,	Used to separate Thresholds

Syntax used to define file systems and their threshold values:

Column 1	Column 2	Column 3	Column 4	Column 5
File systems	Warning	Minor	Major	Critical

Note: In the SI-DiskCapacityMonitorConfig File policy, the filesystem and the threshold values must be separated by a single *tab* space and the threshold values must be separated by commas.

Threshold Table	
n/m	Separate limits for space (n) and for inodes (m)
n/	Limit for space and no limit for inodes
/m	No limit for space but limit for inodes
n	Limit is for both space and inodes

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/l, /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**

  The parameters specified in this example are not correct. You should always specify a default value.

- **MessageGroup=OS,/tmp=unix_admin,/ora/*=dba,/var/log?=unix_admin**

  In this example:

  unix_admin is the message group assigned for alerts generated for **/tmp** filesystem.

  dba is the message group assigned for alerts generated for filesystems beginning with **/ora/** followed by 1 or more characters.

  unix_admin is the message group assigned for alerts generated for filesystems beginning with **/var/log** followed by exactly 1 character.

  OS is the message group assigned for alerts generated for the rest of the filesystems.

> **Note:** The threshold values for this policy must be set as an integer or decimal number with a maximum of two digits to the right of the decimal point.

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" on page 23.

Remote Drive Space Utilization Monitor Policy

SI-MSWindowsRemoteDrivesSpaceUtilization

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

Infrastructure Management → v12.0 → <language> → Systems Infrastructure → Capacity → Windows

> **Note:** The SI-MSWindowsRemoteDrivesSpaceUtilization policy generates alert only when the non-agent user runs the policy with admin privileges.

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" on page 23.
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 → v12.0 → <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" on page 23.

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 → v12.0 → <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" on page 23.

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 → v12.0 → <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 OM 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 OM 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 OM 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 → v12.0 → <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 → v12.0 → <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 OM 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 OM 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	Checks for error conditions that match the `<*> sshd\[<#>\]: Failed`

failure	`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 OM 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 OM 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:

Infrastructure Management → v12.0 → <language> → Systems Infrastructure → Logs → MS Windows Server

NFS Log Policy

SI-MSWindowsServer_NFSWarnError

This policy monitors the NFS log file for the NFS server processes and forwards the errors to the OM 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 OM 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 OM 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 OM 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

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 OM 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

Windows Server Disk Error Log Policy

SI-MSWindowsServer_DiskErrors

This policy monitors the System event log file for events with Disk source errors. If the policy detects a disk error like unable to read or write to a block on the disk, it forwards the error log entries to the OM console with a severity level of warning or error. The policy looks for the following errors recorded in the System event log file:

- The device has a bad block of memory
- The device did not respond with in the timeout period
- The driver detected a controller error on device
- The device is not ready for access
- Windows was unable to save all the data for the file
- Detected error on device during a paging operation
- I/O request to the device did not complete or cancel with in the specific timeout
- The file system structure on the disk is corrupt and unusable
- The system failed to flush data to the transaction log
- Reset to device was issued

AIX System Logfile Monitoring Policies

The AIX system logfile monitoring policies monitors the crucial system faults.

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 OM console as messages with severity

Warning. The alerts contain error codes, classes, and outages. The default policy group for this policy is:

Infrastructure Management → v12.0 → <*language*> → Systems Infrastructure → Logs → AIX

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 to prevent or identify the root cause of a developing performance issue.

The default policy group for these policies is:

Infrastructure Management → v12.0 → <language> → Systems Infrastructure → Performance

Network Usage and Performance Policy

SI-NetworkUsageAndPerformance

This policy monitors the system's network usage and shows error rate, collision rate, byte rate and outbound queue length 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

Note: The following metrics used in this policy require 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 BYNETIF_NET_TYPE
Supported Platforms	Microsoft Windows Red Hat Enterprise Linux Suse Linux Enterprise Server HP-UX IBM AIX Oracle Solaris Debian Ubuntu *The script parameters are applicable for 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 rate at which you want to receive a critical severity message. *This parameter is not applicable for Windows.*
NICCollisionRatePctMajorThreshold	You can set a threshold value for collision rate at which you want to receive a critical major message. *This parameter is not applicable for Windows.*
NICCollisionRatePctMinorThreshold	You can set a threshold value for collision rate at which you want to receive a minor severity message. *This parameter is not applicable for Windows.*
NICCollisionRatePctWarningThreshold	You can set a threshold value for collision rate at which you want to receive a warning severity message. *This parameter is not applicable for 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 for 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 for 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 for 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 for 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 for 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 for 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 for 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 for HP-UX, AIX, and Windows.*
NICThresholdMultiplier	Use the parameter to increase the thresholds by a factor X, for handling high bandwidth network cards. If the parameter is not specified explicitly, multiplier value is calculated automatically.
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" on page 23.

Note: The threshold values for this policy can be specified as a default value, and also as individual network interface names, network interface types, or both. If network interface name and network interface type are both specified for a parameter, then the network interface type takes precedence over network interface name.

Using wildcard characters '*' for script parameters

For indicating multiple NIC names, you can use '*' to match one or more characters.

For example: **NICBandwidthUtilWarningThreshold= 4500, eth*=0**.

In this instance, the threshold value 0 will apply to all NIC names whose first three characters match `eth`.

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 OM 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_FREE GBL_MEM_PAGE_REQUEST_RATE GBL_MEM_CACHE_FLUSH_RATE GBL_MEM_SWAPOUT_BYTE_RATE GBL_MEM_PG_SCAN_RATE * These metrics are used only if you install 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 for 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 for 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 for 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 for 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" on page 23.

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 BYCPU_INTERRUPT_RATE
Supported Platforms	Microsoft Windows Red Hat Enterprise Linux Suse Linux Enterprise Server HP-UX IBM AIX Oracle Solaris Debian Ubuntu
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" on page 23.

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 OM 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 for 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" on page 23.

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" on page 23.

The sample policies provided are:

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

Infrastructure Management → v12.0 → <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 → v12.0 → <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 → v12.0 → <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 → v12.0 → <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 OM 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" on page 23.

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

Infrastructure Management → v12.0 → <language> → System Infrastructure → Policies Grouped by Vendor → *<all platforms>* - QuickStart.

Infrastructure Management → v12.0 → <language> → System Infrastructure → Performance.

RealTimeAlerts Policy

RealtimeAlerts policy detects the bottlenecks in CPU, disk, memory, and networking. The Realtime Configuration policy defines the threshold for these parameters. During a threshold breach, alert messages notify the system administrator with no time delay and reduce the downtime in production environment.

> **Note:** You must enable RTMA license on the Operations Agent node for RealTimeAlerts policy to fetch real time data.

To receive alert messages you must deploy the RealTime Configuration policy on the node and also ensure that the **perfd** daemon process and the `cpsh` program are running on the node.

> **Note:** You can run the following command start the **perfd** process:
>
> **On Windows:**
>
> ```
> %ovinstalldir%bin\ovpacmd stop RTMA
> ```
>
> ```
> %ovinstalldir%bin\ovpacmd start RTMA
> ```
>
> **On HP-UX/Linux/Solaris:**
>
> ```
> /opt/perf/bin/pctl restart
> ```

> **On AIX:**
>
> `/usr/lpp/perf/bin/pctl restart`

As a post-deploy action, this policy runs a Perl script (`advisor.pl`) and then sends the advisor output to the `adv.out` file. The following log file monitoring policies are run on a node to read data from the `adv.out` file and send alerts to the OM console:

- Windows - SI-MSWindowsRealtimeAlerts
- Linux or UNIX - SI-LinuxRealtimeAlerts

For more information see " Adviser for the RTMA component" in *Operations Agent User Guide*.

Supported platforms	HPUX RHEL MS Windows Sun Solaris IBM AIX

SI-AIXRealTimeConfig Policy

SI-AIXRealTimeConfig Policy defines thresholds for CPU, disk, memory, and networking.

Supported platforms	IBM AIX
Metrics used	GBL_SWAP_SPACE_UTIL
Metrics used for CPU	GBL_LOADAVG GBL_ACTIVE_CPU GBL_CPU_TOTAL_UTIL
Metrics used for Disk	GBL_DISK_UTIL_PEAK GBL_BLOCKED_IO_QUEUE
Metrics used for Memory	GBL_MEM_UTIL GBL_MEM_PG_SCAN_RATE GBL_MEM_PAGEOUT_BYTE_RATE
Metrics used for Network	GBL_NET_UTIL_PEAK GBL_NET_COLLISON_PCT GBL_NET_PACKET_RATE

SI-HPUXRealTimeConfig Policy

SI-HPUXRealTimeConfig Policy defines thresholds for CPU, disk, memory, and networking.

Supported platforms	HP-UX
Metrics used	GBL_SWAP_SPACE_UTIL
Metrics used for CPU	GBL_ACTIVE_CPU GBL_CPU_TOTAL_UTIL GBL_CPU_QUEUE
Metrics used for Disk	GBL_DISK_UTIL_PEAK GBL_DISK_SUBSYSTEM_QUEUE
Metrics used for Memory	GBL_MEM_UTIL GBL_MEM_PG_SCAN_RATE GBL_MEM_PAGEOUT_BYTE_RATE GBL_MEM_SWAPOUT_BYTE_RATE
Metrics used for Network	GBL_NET_UTIL_PEAK GBL_NET_COLLISION_PCT GBL_NET_PACKET_RATE GBL_NET_OUTQUEUE

SI-LinuxRealTimeConfig Policy

SI-LinuxRealtime Configuration policy defines thresholds for CPU, disk, memory, and networking.

Supported platforms	Linux
Metrics used	GBL_SWAP_SPACE_UTIL
Metrics used for CPU	GBL_LOADAVG GBL_ACTIVE_CPU GBL_CPU_TOTAL_UTIL
Metrics used for Disk	GBL_DISK_UTIL_PEAK GBL_DISK_REQUEST_QUEUE
Metrics used for Memory	GBL_MEM_UTIL GBL_MEM_PAGEOUT_BYTE_RATE
Metrics used for Network	GBL_NET_PACKET_RATE GBL_NET_COLLISION_PCT

	GBL_NFS_CALL_RATE

SI-MSWindowsRealTimeConfig policy

SI-MSWindowsRealtime Configuration Policy defines thresholds for CPU, disk, memory, and networking.

Supported platforms	MS Windows
Metrics used	GBL_SWAP_SPACE_UTIL
Metrics used for CPU	GBL_CPU_TOTAL_UTIL GBL_LOADAVG
Metrics used for Disk	GBL_DISK_UTIL_PEAK GBL_DISK_REQUEST_QUEUE
Metrics used for Memory	GBL_MEM_UTIL GBL_MEM_PAGE_REQUEST_RATE GBL_MEM_CACHE_FLUSH_RATE GBL_MEM_PAGEOUT_RATE
Metrics used for Network	GBL_NET_UTIL_PEAK GBL_NET_PACKET_RATE GBL_NET_OUTQUEUE

SI-SunSolarisRealTimeConfig Policy

SI-SunSolarisRealtime Configuration Policy defines thresholds for CPU, disk, memory, and networking.

Supported platforms	Sun Solaris
Metrics used	GBL_SWAP_SPACE_UTIL
Metrics used for CPU	GBL_LOADAVG GBL_ACTIVE_CPU GBL_CPU_TOTAL_UTIL
Metrics used for Disk	GBL_DISK_UTIL_PEAK GBL_BLOCKED_IO_QUEUE
Metrics used for Memory	GBL_MEM_UTIL GBL_MEM_PG_SCAN_RATE

	GBL_MEM_PAGEOUT_BYTE_RATE
Metrics used for Network	GBL_NET_PACKET_RATE GBL_NET_COLLISION_PCT GBL_NFS_CALL_RATE

SI-CPUStealtimeUtilMonitor

The policy monitors the time that a virtual CPU waits for the physical CPU. This time duration is called "Steal time". The Steal time occurs when the physical CPU is busy processing requests for another virtual CPU.

Metrics used	GBL_CPU_STOLEN_UTIL
Supported Platforms	Linux RHEL Ubuntu Debian
Rules	**Description**
CpuUtilMajorThreshold	Set the threshold value for minimum total CPU utilization time at which you want to receive a Major severity message.
CpuUtilWarningThreshold	Set the threshold value for minimum total CPU utilization time at which you want to receive a Warning severity message.

Adaptive Thresholding Policies

> **Note:**
>
> Infrastructure SPI 12.01 (AdaptiveThresholding) policies will not function with Operations Agent version 11.xx.

Baseline data computed by Operations Agent is used by the SI-AdaptiveThresholdingMonitor policy to monitor performance and resource utilization.

> **Note:** Use the command line options to enable baseline on a Operations Agent node. For more information, see the topic *Configuring Baseline on the Operations Agent Node* in the *Operations*

Agent User Guide.

You can also use the XPL configurations to enable baseline. Follow the steps:

1. On the OM console select **Policy management → Policy groups → Infrastructure Management → v12.0 → Settings and Thresholds → Agent Settings → OPC_PERL_INCLUDE_INSTR_DIR**
2. Set ENABLE_BASELINE to TRUE and then deploy the policy on all desired nodes.

Baseline data is computed only at the end of every hour. If you want the baseline data to be computed immediately after you enable baseline, you must restart the **oacore** process. Run the following command to restart **oacore**:

```
ovc -restart oacore
```

The baseline data is used along with the deviations (N) set in the SI-ConfigureBaselining policy or SI-AdaptiveThresholdingMonitor policy to enable adaptive monitoring or adaptive thresholding. Adaptive thresholding helps to dynamically calculate the optimal threshold values.

To enable Adaptive Thresholding on a Operations Agent node, follow the steps:

1. Configuring and Deploying SI-ConfigureBaselining policy on the node where baselining is configured.
2. Configuring and Deploying SI-AdaptivethresholdingMonitor policy on the Operations Agent node.

Configuring and Deploying SI-ConfigureBaselining Policy

Note: Ensure that baselining is enabled on the Operations Agent node. For more information about enabling baselining, see the topic *Configuring Baseline on the* Operations Agent *Node* in the Operations Agent *User Guide*.

Follow the steps to configure and deploy SI-ConfigureBaselining policy on a node:

1. On the OM console, select **Policy management → Policy groups → Infrastructure Management →v12.0 → <language> → Systems Infrastructure → Performance → Adaptive Thresholding → SI-ConfigureBaselining policy**
2. Open the **SI-ConfigureBaselining** policy → **Data** tab and define the metrics that you want to monitor in *one* of the following formats:
   - To define only the metrics:

     ```
     [Baseline]
     ```

```
<Class>:<Metrics>
```

- To define the metrics and deviations:

  ```
  [Baseline]
  <Class>:<Metrics>,<Warning Deviation>,<Minor Deviation>,<Major Deviation>
  ```

  For more information on configuring deviations, see Configuring Deviations.

3. Deploy SI-ConfigureBaselining policy on the node.

After SI-ConfigureBaselining is deployed, `baseline.cfg` file is created in the following directory:

On Windows

`%ovdatadir%`

On UNIX (and Linux)

`/var/opt/perf/`

> **Note:** This `baseline.cfg` file overwrites the `baseline.cfg` file created while configuring baselining on the node. For more information about configuring baseline, see the topic *Configuring Baseline on the* Operations Agent *Node* in the Operations Agent *User Guide*.

After deploying the SI-ConfigureBaselining policy, check if the baseline data is logged in the database for the metrics defined in the policy.

Configuring and Deploying SI-AdaptiveThresholdingMonitor Policy

Follow the steps to configure and deploy SI-AdaptiveThresholdingMonitor policy on a node:

1. On the OM console, select **Policy management** → **Policy groups** → **Infrastructure Management** →**v12.0** → **<language>** → **Systems Infrastructure** → **Performance** → **Adaptive Thresholding** → **SI-AdaptiveThresholdingMonitor policy**
2. Open the **SI-AdaptivethresholdingMonitor** policy → **Script-Parameters** tab. Default deviations for all monitored metrics are listed in the **Script-Parameters** tab.
3. Set the new deviations and deploy the SI-AdaptiveThresholdingMonitor policy.

> **Note:** To set adaptive threshold values using the SI-AdaptiveThresholdingMonitor policy, baseline data at least for a week must be available.

For more information on configuring deviations, see Configuring Deviations.

The baseline data computed by Operations Agent is used along with the deviations (N) set in the SI-ConfigureBaselining Policy and SI-AdaptiveThresholdingMonitor Policy to set adaptive threshold values for monitoring resource utilization.

Configuring Deviations

You can configure deviations (N) either in the SI-ConfigureBaselining policy or in the SI-AdaptivethresholdingMonitor policy.

> **Note:**
>
> To configure deviations for specific metrics, set the deviations in the SI-ConfigureBaselining policy.
>
> To configure deviations for all metrics, set the deviations in the **Script-Parameters** tab in the SI-AdaptivethresholdingMonitor policy.
>
> If no deviations are set for a metrics in the SI-ConfigureBaselining policy, then the deviations set in the SI-AdaptiveThresholdingMonitor policy are used to calculate adaptive threshold values.

Configuring Deviations in the SI-ConfigureBaselining Policy

1. On the OM console, select **Policy management** → **Policy groups** → **Infrastructure Management** →**v12.0** → **<language>** → **Systems Infrastructure** → **Performance** → **Adaptive Thresholding**→ **SI-ConfigureBaselining policy**.
2. Open the **SI-ConfigureBaselining** policy → **Data** tab, define the metrics and deviations in the following format:

   ```
   [Baseline]

   <Class>:<Metrics>,<Warning Deviation>,<Minor Deviation>,<Major
   Deviation>,<Minimum Value>,<Maximum Value>,<CutOff>
   ```

   For example:

   ```
   [Baseline]

   Global:GBL_MEM_UTIL,-1,0,1,0,100,15
   ```

Instance Based Monitoring

You can also set deviations for specific instances to enable instance based monitoring.

> **Note:** Instance based monitoring is supported only for the following metric classes; filesystem, netif and disk.

Follow the steps to set deviations for specific instances:

1. On the OM console, select **Policy management → Policy groups → Infrastructure Management →v12.0 → <language> → Systems Infrastructure → Performance→ Adaptive Thresholding→ SI-ConfigureBaselining policy.**
2. Open the SI-ConfigureBaselining policy → **Data** tab and define the metrics in the following format:

   ```
   [Baseline]
   <Class>:<Metric>
   ```

3. Set the deviations for specific instances in the following format:

   ```
   [<Class>:<Metric>]
   <Instance>,<Warning Deviation>,<Minor Deviation>,<Major Deviation>,<Minimum Value>,<Maximum Value>,<CutOff>
   ```

   For example:

   Let us assume that you are monitoring 3 disks – dsk0, dsk1 and dsk2. You can set specific deviations for each disk as follows:

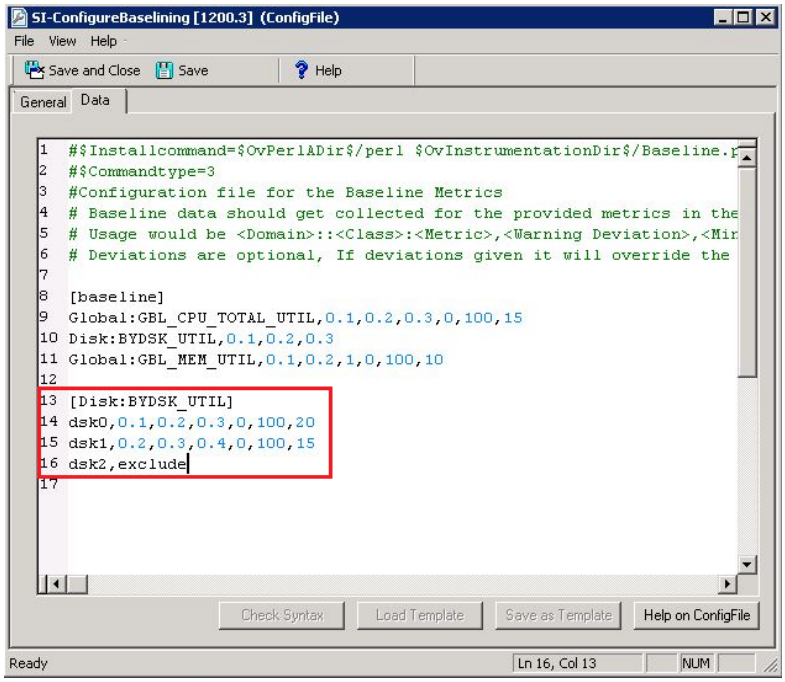
   ```
   [Baseline]
   Disk:BYDSK_UTIL


   [Disk:BYDSK_UTIL]
    dsk0,0.1,0.2,0.3,0,100,20
    dsk1,0.2,0.3,0.4,0,100,15
    dsk2:exclude
   ```

   In this instance:

Disk Monitored	Warning Deviation	Minor Deviation	Major Deviation	Minimum Value	Maximum Value	CutOff
dsk0	0.1	0.2	0.3	0	100	20
dsk1	0.2	0.3	0.4	0	100	15
dsk2	Is excluded from monitoring					

Example of Modifying Threshold in the SI-ConfigureBaselining Policy

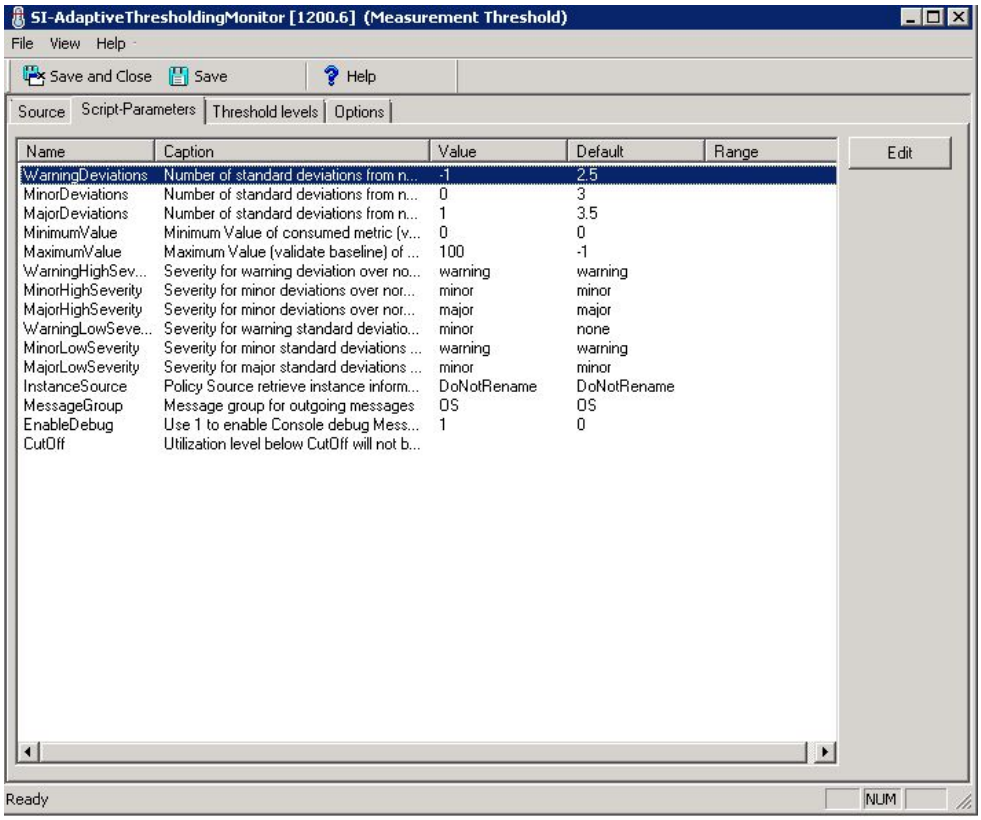


Note: If instance based monitoring defined in the policy, corresponding `.cfg` files are created. If you remove instance level metrics from the policy, corresponding `.cfg` files are also removed.

Configuring Deviations in the SI-AdaptiveThresholdingMonitor Policy

1. On the OM console, select **Policy management → Policy groups → Infrastructure Management →v12.0 → <language> → Systems Infrastructure → Performance → Adaptive Thresholding→ SI-AdaptivethresholdingMonitor policy**.
2. Open the SI-AdaptivethresholdingMonitor policy → **Script-Parameters** tab. The Warning, Minor and Major deviations for all monitored metrics are listed.
3. Set the new threshold values.

Example of Modifying Threshold in the SI-AdaptiveThresholdingMonitor Policy



Generating Alert Messages

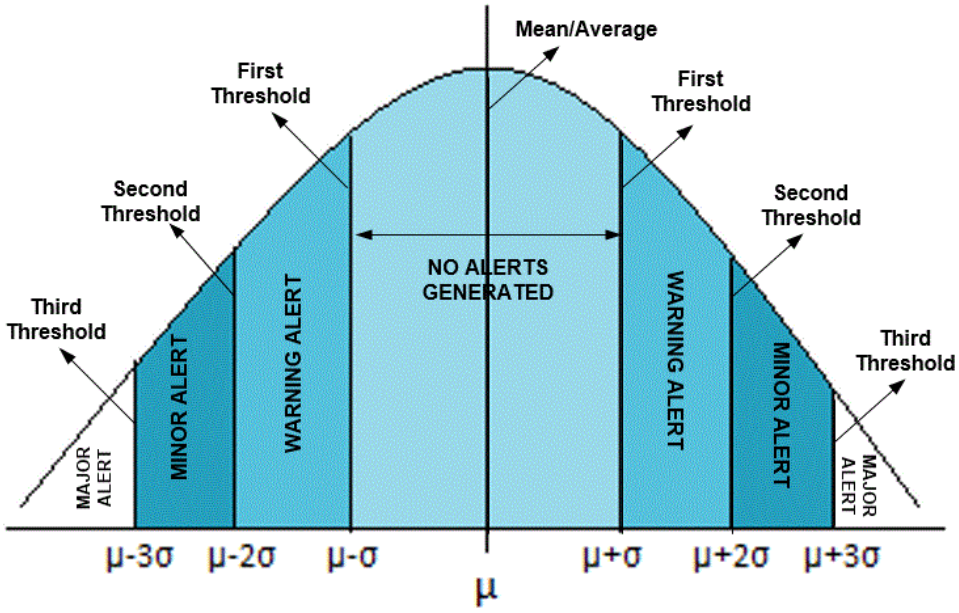
The baseline data (Average and Standard Deviation values) computed by Operations Agent along with the deviations (N) set in the SI-ConfigureBaselining Policy and SI-AdaptiveThresholdingMonitor Policy are used in the following formula to set threshold values:

Range for normal behavior = Historic Average ± N * Historic Standard Deviation

In this instance:

- Historic Average is the average of the historic data computed using the baselining process.
- N is the value of the Warning, Minor or Major deviation.
- Historic Standard Deviation is the Standard Deviation computed using the baselining process.

Alerts are generated whenever the computed threshold values are violated, as shown in the graph:



Alert Type	Explanation
Warning	An alert message with Warning severity is generated when the first threshold, that is, μ±σ is violated. In this instance Warning deviation is 1.
Minor	An alert message with Minor severity is generated when the second threshold, that is, μ±2σ is violated. In this instance Minor deviation is 2.
Major	An alert message with Major severity is generated when the third threshold, that is, μ±3σ is violated. In this instance Major deviation is 3.

Use Case: Using the Baseline Data for Adaptive Monitoring

John is a system administrator who is using the Operations Agent to gather baseline data. To enable adaptive monitoring, he deploys the Infrastructure policies - SI-ConfigureBaselining policy and SI-AdaptivethresholdingMonitor policy on the node.

The baseline data computed by Operations Agent is used along with the deviations (N) set in the SI-ConfigureBaselining Policy (or SI-AdaptiveThresholdingMonitor Policy) to compute adaptive threshold values for monitoring resource utilization.

John decides to monitor the CPU utilization on a Monday morning between 10:00 and 11:00 A.M.

Monitoring the CPU Utilization

Let us assume that the following baseline data is computed using the historical data logged in the datastore on every Monday between 10:00 and 11:00 A.M:

Minimum	Maximum	Historic Average (μ)	Standard Deviation (σ)
5	75	39.03	17.02

Let us assume that John uses the following deviations set in the **Script-Parameters** tab in the SI-AdaptivethresholdingMonitor policy:

Deviations (N)	Value
Warning	1
Minor	2
Major	3

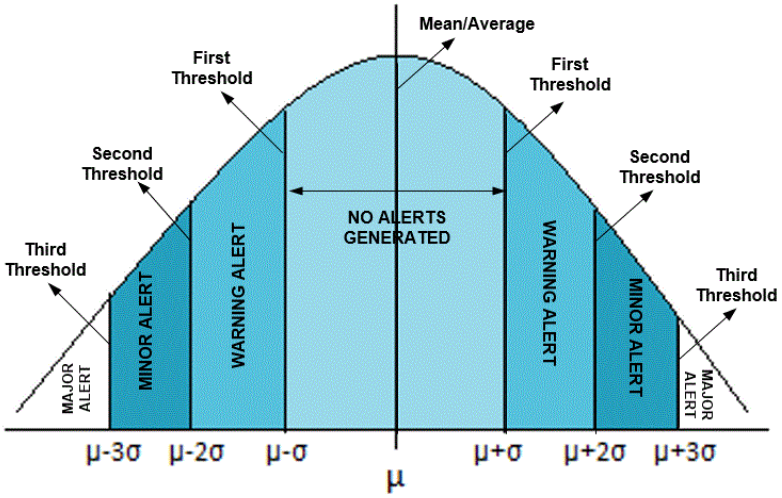
Historic average (39.03), Standard Deviation (17.02) and Deviation (N) values are used in the following formula to set the threshold values:

Range for normal behavior = Historic Average ± N * Historic Standard Deviation

In this instance;

- Historic Average is the average of the Historic Data computed using the baselining process.
- N is the value of the Warning, Minor, or Major deviation.
- Historic Standard Deviation is the Standard Deviation computed using the baselining process.

Alerts are generated whenever the computed thresholds are violated, as shown in the graph:



Alert Type	Explanation
Warning	An alert message with Warning severity is generated when the first threshold, that is, μ±σ is violated. In the example, whenever CPU utilization increases above 56.05% or decreases below 22.01%, a warning alert is generated.
Minor	An alert message with Minor severity is generated when the second threshold, that is, μ±2σ is violated. In the example, whenever CPU utilization increases above 73.07% or decreases below 4.99%, a minor alert is generated.
Major	An alert message with Major severity is generated when the third threshold, that is, μ±3σ is violated. In the example, whenever CPU utilization increases above 90.09% or reaches 0%, a major alert is generated.

Security Policies

Use case: An unauthorized user has tried to gain access to your system using an automated script to enter different combinations of username and password. This leads to several failed login attempts. 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. These policies collect data about the failed login attempts and send alert after a maximum number of attempts is exceeded.

> **Note:** After deploying the security collector policies, ensure to run the policies for at least 5

minutes to collect 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 checks for invalid logins that occur 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 → v12.0 → <*language*> → Systems Infrastructure → Security → Windows

Or

Infrastructure Management → v12.0 → <*language*> → Systems Infrastructure → Policies grouped by Vendor → MS Windows -QuickStart

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 → v12.0 → <*language*> → Systems Infrastructure → Security → Windows

Or

Infrastructure Management → v12.0 → <*language*> → Systems Infrastructure → Policies grouped by Vendor → MS Windows - QuickStart

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 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 → v12.0 → <*language*> → Systems Infrastructure → Security → Linux

Or

Infrastructure Management → v12.0 → <*language*> → Systems Infrastructure → Policies grouped by Vendor → <*os*>-QuickStart

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

> **Note:** The pre-requisites for the SI-UNIXFailedLoginsCollector policy to function correctly when deployed on a Solaris node are:
>
> - The file `/etc/default/login` on the Solaris node must have the following settings:
>
>  ```
>  SYSLOG=YES
>
>  SYSLOG_FAILED_LOGINS=1
>  ```
>
> - Remove the comment from the following line in the `/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
>  ```

Following are the nodes on which the **SI-UNIXFailedLoginsCollector** policy deployed on other nodes:

Nodes	Commands / logfiles to view the failed logins
Solaris	Use the `/var/log/authlog` file to view the failed logins
Linux and	At the command prompt, run the `lastb` command to view failed logins

HP-UX	
AIX	Use the `/etc/security/failedlogin` file to view failed logins

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 the RHEL, Debian, Ubuntu and SLES Linux systems. The policy logs individual instances of login attempts into the SECONDS_SINCE_LASTLOGIN metric in the Embedded Performance Component (EPC) at definite time intervals. By default, the time interval is 1 hour. The information logged in EPC is used to send an alert to the console or generate reports over a period of time. The default policy group for the policy is:

Infrastructure Management → v12.0 → <*language*> → Systems Infrastructure → Security → Linux

Or

Infrastructure Management → v12.0 → <*language*> → Systems Infrastructure → Policies grouped by Vendor → <os> - QuickStart

Bad Login Policy for Linux

SI-LinuxBadLogins

This is a log file monitoring policy that monitors the bad logins `/var/log/btmp` file and alerts users when an incorrect login occurs. By default, the polling interval is 10 seconds. The policy matches the bad login condition with `<*name> <*.tty> <@.datetime> - <@>\(<*>\)<*.machine>` pattern in the `/var/log/btmp` file. If the condition is met, an alert message is sent to the OM console with warning severity.

The default policy group for the policy is:

Infrastructure Management → v12.0 → <*language*> → Systems Infrastructure → Security → Linux

Or

Infrastructure Management → v12.0 → <*language*> → Systems Infrastructure → Policies grouped by Vendor → <os> - QuickStart

Bad Login Policy for AIX

SI-AIXBadLogs

This is a log file monitoring policy that monitors the bad logins `/etc/security/failedlogin` file and alerts users when an incorrect login occurs. By default, the polling interval is 10 seconds. This policy is applicable for local and remote users.

Failed Local Login: The policy checks for the bad login condition with `LOGIN <@.user> <@.tty>` pattern in the `badlogs.log` file. An alert message with a warning severity is sent to the OM console if the condition is met.

Failed Remote Login: The policy checks for the bad login condition with `LOGIN <@.user> <@.tty> <@.host>` pattern in the `badlogs.log` file. An alert message with a warning severity is sent to the OM console if the condition is met.

The default policy group for the policy is:

Infrastructure Management → v12.0 → <*language*> → Systems Infrastructure → Security → AIX

Or

Infrastructure Management → v12.0 → <*language*> → Systems Infrastructure → Policies grouped by Vendor → AIX - QuickStart

Logins Policy for AIX

SI-AIXLogins

This is a log file monitoring policy that monitors the login history `/var/adm/wtmp` file and alerts users when a successful remote login, successful local login, system boot, system shutdown for a user, or system shutdown occurs. By default, polling interval is 10 seconds.

Successful remote login: The policy checks for the successful remote login condition with `LOGIN<@.user> <@.tty> <@.host>` pattern in the `wtmp` file. An alert message is sent to the OM console if the condition is met.

Successful local login: The policy checks for the successful local login condition with `LOGIN<@.user> <@.tty>` pattern in the `wtmp` file. An alert message with warning severity is sent to the OM console if the condition is met.

System Boot: The policy checks for the system boot condition with `BOOT` pattern in the `wtmp` file. An alert message with warning severity is sent to the OM console if the condition is met.

System Shutdown for a User: The policy checks for the system shutdown user condition with `SHUTDOWN<@.user><@.tty>` pattern in the `wtmp` file. An alert message with warning severity is sent to the OM console if the condition is met.

System Shutdown: The policy checks for the system shutdown condition with the `SHUTDOWN` pattern in the `wtmp` file. An alert message with warning severity is sent to the OM console if the condition is met.

The default policy group for the policy is:

Infrastructure Management → v12.0 → <*language*> → Systems Infrastructure → Security → AIX

Or

Infrastructure Management → v12.0 → <*language*> → Systems Infrastructure → Policies grouped by Vendor → AIX - QuickStart

Switch User Policy for AIX

SI-AIXSU

This is a log file monitoring policy that monitors the switch user history `/var/adm/sulog` file. By default, the polling interval is 20 seconds. Alerts are sent to users when the SU command (either successful or failure) is run.

Bad SU: The policy checks for the condition of unsuccessful SU commands execution with `SU<*> - <@.tty> <*.from> - <*.to>` pattern in the `SU` file. An alert message with warning severity is sent to the OM console if the condition is met.

Succeeded SU: The policy checks for the condition of successful SU commands execution with `SU<*> + <@.tty> <*.from> - <*.to>` pattern in the `SU` file. An alert message with warning severity is sent to the OM console if the condition is met.

The default policy group for the policy is:

Infrastructure Management → v12.0 → <*language*> → Systems Infrastructure → Security → AIX

Or

Infrastructure Management → v12.0 → <*language*> → Systems Infrastructure → Policies grouped by Vendor → AIX - QuickStart

Sys Log Policy for AIX

SI-AIXSysLog

This is a log file monitoring policy that monitors messages sent to `/tmp/syslog` file. By default, the polling interval is 1 min.

Printer Paper Out: After you enable logging in the `/etc/syslog.conf` file, the policy checks the messages sent with <*> pattern in the `syslog` file. An alert message is sent to the OM console if the condition is met. Ensure that the exact name of the file that you want to monitor is mentioned in the configuration file and the policy.

The default policy group for the policy is:

Infrastructure Management → v12.0 → <*language*> → Systems Infrastructure → Security → AIX

Bad Logins Policy for HP-UX

SI-HPUXBadLogs

This is a log file monitoring policy that monitors bad logins `/var/adm/btmps` file and alerts users when an incorrect login occurs. By default, the polling interval is 10 seconds.

Failed local login: The policy checks for the bad login condition with `FAILED<@.user> <@.tty> <*.date> <*.time>` pattern in the `btmps` file. An alert message with warning severity is sent to the OM console if the condition is met.

Failed remote login: The policy checks for the bad login condition with `FAILED<@.user> <@.tty><@.host> <*.date> <*.time>` pattern in the `btmps` file. An alert message with warning severity is sent to the OM console if the condition is met.

The default policy group for the policy is:

Infrastructure Management → v12.0 → <*language*> → Systems Infrastructure → Security → HP-UX

Logins Policy for HP-UX

SI-HPUXLogins

This is a log file monitoring policy that monitors the logins in the `/var/adm/wtmps` file and alerts users when an incorrect login occurs. By default, the polling interval is 10 seconds.

Successful local login: The policy checks for the successful login condition with `LOGIN<@.user> <@.tty> <*.date> <*.time>` pattern in the `wtmps` file. An alert message with warning severity is sent to the OM console if the condition is met.

Successful remote login: The policy checks for the successful login condition with `LOGIN<@.user> <@.tty> <@.host> <*.date> <*.time>` pattern in the `wtmps` file. An alert message with warning severity is sent to the OM console if the condition is met.

System Boot: The policy checks for the system boot condition with `BOOT` pattern in the `wtmps` file. An alert message with warning severity is sent to the OM console if the condition is met.

System Shutdown: The policy matches the system shutdown with `SHUTDOWN<@.user> <@.tty>` pattern in the `wtmps` file. An alert message with warning severity is sent to the OM console if the condition is met.

The default policy group for the policy is:

Infrastructure Management → v12.0 → <*language*> → Systems Infrastructure → Security → HP-UX

Switch User Policy for HP-UX

SI-HPUXSu

This is a log file monitoring policy that monitors the switch user events `/var/adm/sulog` file and alerts users in case of any switch user event occurs. By default, the polling interval is 10 seconds.

Suppress messages caused by mondbfile monitor: The policy matches the switch user event condition with `SU<*> + <@.tty> root - oracle` pattern in the `SU` file. An alert message is sent to the OM console if the condition is met.

Syslog Policy for HP-UX

SI-HPUXSyslog

This is a log file monitoring file policy that monitors the messages going into the `var/adm/syslog/syslog.log`. By default, the polling interval is 20 seconds.

The default policy group for the policy is:

Infrastructure Management → v12.0 → <language> → Systems Infrastructure → Security → HP-UX

Sun Solaris Bad Logins

SI-SunSolarisBadLogs

This is log file monitoring policy that monitors failed logins in the `/var/adm/loginlog` file and alerts users when an incorrect login occurs. By default, the polling interval is 10 seconds.

Follow the steps to enable logging of failed logins on Solaris 10 platforms:

1. Run the following command to create the `loginlog` file in the `/var/adm` directory:

   ```
   touch /var/adm/loginlog
   ```

2. Run the following command to set the read and write permissions for root on the `loginlog` file:

   ```
   chmod 600 /var/adm/loginlog
   ```

3. Change group membership to `sys` on the `loginlog` file:

   ```
   chgrp sys /var/adm/loginlog
   ```

4. Set the auth debug in `/etc/syslog.conf` configuration file:

   ```
   auth.debug                      ifdef(`LOGHOST', /var/adm/loginlog, @loghost)
   ```

5. Run the following command to start the logging:

   ```
   svcadm restart svc:/system/system-log:default
   ```

6. Check `/var/adm/loginlog` for failed login logs and deploy the policy.

Failed local/remote login: The policy checks for the failed logins condition with <*.date> Failed keyboard-interactive for <*.user> from <*.ip> port <*.port>. An alert message is sent to the OM console if the conditions are met.

The default policy group for the policy is:

Infrastructure Management → v12.0 → <language> → Systems Infrastructure → Security → Solaris

Sun Solaris Logins

> **Note:** In the **SI-SunSolarisLogins [1200.0] (Logfile Entry)** Window, on the **Source** tab, the pre-

> processing script is specified in the **File to be executed*** box. To generate alerts, ensure you rename the pre-processing script to `/usr/bin/sh/var/opt/OV/bin/instrumentation/osspisecurity.sh w`

SI-SunSolarisLogins

This is a log file monitoring policy that monitors the login details in `/var/adm/wmptx` file and alerts users when a successful remote login or local login or system login or system boot or system shutdown occurs. By default, the polling interval is 10 seconds.

Successful local login: The policy checks for the successful local login condition with `LOGIN<@.user> <@.tty> <@.host>` pattern in `wtmpx` file. An alert message with warning severity is sent to the OM console if the condition is met.

Successful remote login: The policy checks for the successful remote login condition with `LOGIN<@.user> <@.tty> <@.host>` pattern in `wtmpx` file. An alert message with warning severity is sent to the OM console if the condition is met.

System Boot: The policy checks for the system boot condition with `BOOT` pattern in the `wtmpx` file. An alert message with warning severity is sent to the OM console if the condition is met.

System Shutdown for Remote Users: The policy checks for the system shutdown condition with the `SHUTDOWN <@.user> <@,tty>` pattern in the `wtmpx` file. An alert message with warning severity is sent to the OM console if the condition is met.

System Shutdown for Local Users: The policy checks for the system shutdown condition with `SHUTDOWN` pattern in the `wtmpx` file. An alert message with warning severity is sent to the OM console if the condition is met.

The default policy group for the policy is:

Infrastructure Management → v12.0 → <language> → Systems Infrastructure → Security → Solaris

Sun Solaris snmp Log Policy

SI-SunSolarissnmplog

This is a log file monitoring policy that monitors the snmp log file entries in `var/adm/messages` file. By default, the polling interval is 10 minutes. The policy alerts users when the required condition matches successfully.

Snmpd log file entries: The SI-SunSolarissnmplog matches the snmp log file entries with SNMP message failed authentication `<*> IP address :<@.ipaddy>, <*>name used: <@. comname>,` pattern in the `snmplog` file. An alert message is sent to the OM console if the condition is met.

The default policy group for the policy is:

Infrastructure Management → v12.0 → <language> → Systems Infrastructure → Security → Solaris

Sun Solaris Syslog Policy

SI-SunSolarisSyslog

This is a log file monitoring policy that monitors system messages going into system log file `var/adm/messages` and alerts users when a required condition matches successfully. By default, the polling interval is 1 minute.

The default policy group for the policy is:

Infrastructure Management → v12.0 → <language> → Systems Infrastructure → Security → Solaris

Deploying SI SPI Policies from Operations Manager for Windows Management Server

You can manually deploy the policies to the nodes or enable auto deployment of policies.

To enable auto deployment of policies, follow these steps:

1. To enable auto deployment on the server, run the following command:

   /opt/OV/contrib/OpC/autogranting/enableAutoGranting.sh

2. To enable auto deployment for Infra SPI using XPL config change, run the following command:

   ovconfchg -ns infraspi -set AUTODEPLOYMENT true

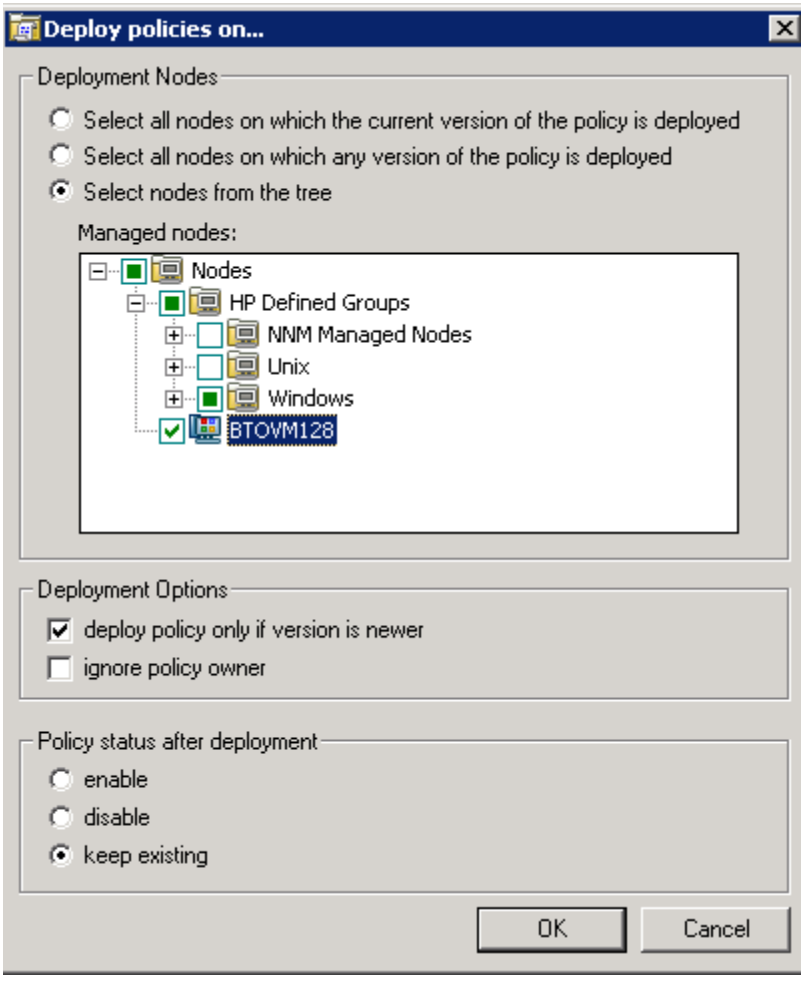
3. To activate the node, run the following command on the management server:

   opcactivate -srv <HPOM Server> -cert_srv <HPOM Server> -f

4. Grant the certificates.
5. Check whether the node is added to the appropriate node group.
6. Verify auto deployment of policies to the node.

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 Operations Manager for UNIX Management Server

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

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

Task 1: Assign Policy or Policy group

1. Log on to OM as the administrator. The OM 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 OM 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 the list of data collected for a particular managed node.

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

Tools → Systems Infrastructure

To access the tool on console or Administration interface for OM 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" on page 127 and "Last Logon Collector Policy for Linux" on page 129.

To launch the tool from the Operations Manager 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 nodes 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 launch 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 Operations Manager 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.

Energy Data Collector

On system where Operations Agent 12.01 is installed, Energy Data Collector along with the Intelligent Platform Management Interface (IPMI) tool collects metrics data and stores it in the datasource named SENSOR.

> **Note:** The IPMI tool functions only if visual C++ 2008 is installed.

Energy Data Collector measures the energy utilization of a physical machine where multiple virtual machines are installed. This tool functions only when Integrated Lights-Out (iLO) is installed on the physical machine.

> **Note:** Integrated Lights-Out (iLO) is a remote server management processor that controls and monitors Servers from a remote location.

The SENSOR datasource is created only after the Energy Data Collector tool is deployed. The SENSOR datasource consists the following metric classes:

- OEM_RESERVED
- POWER_SUPPLY
- FAN
- TEMPERATURE
- MEMORY
- CURRENT

Supported platform	**Linux**
Metrics used for OEM_RESERVED	SNSR_OEM_RESERVED_ID SNSR_OEM_RESERVED_NAME SNSR_OEM_RESERVED_TYPE

	SNSR_OEM_RESERVED_READING SNSR_OEM_RESERVED_UNITS SNSR_OEM_RESERVED_EVENTS
Metrics used for POWER_SUPPLY	SNSR_POWER_SUPPLY_ID SNSR_POWER_SUPPLY_NAME SNSR_POWER_SUPPLY_TYPE SNSR_POWER_SUPPLY_READING SNSR_POWER_SUPPLY_UNITS SNSR_POWER_SUPPLY_EVENTS
Metrics used for FAN	SNSR_FAN_ID SNSR_FAN_NAME SNSR_FAN_TYPE SNSR_FAN_READING SNSR_FAN_UNITS SNSR_FAN_EVENTS
Metrics used for TEMPERATURE	SNSR_TEMPERATURE_ID SNSR_TEMPERATURE_NAME SNSR_TEMPERATURE_TYPE SNSR_TEMPERATURE_READING SNSR_TEMPERATURE_UNITS SNSR_TEMPERATURE_EVENTS
Metrics used for MEMORY	SNSR_MEMORY_ID SNSR_MEMORY_NAME SNSR_MEMORY_TYPE SNSR_MEMORY_READING SNSR_MEMORY_UNITS SNSR_MEMORY_EVENTS
Metrics used for CURRENT	SNSR_CURRENT_ID SNSR_CURRENT_NAME SNSR_CURRENT_TYPE

	SNSR_CURRENT_READING SNSR_CURRENT_UNITS SNSR_CURRENT_EVENTS

Supported platform	**Windows**
Metrics used for OEM_RESERVED	SNSR_OEM_RESERVED_ID SNSR_OEM_RESERVED_NAME SNSR_OEM_RESERVED_TYPE SNSR_OEM_RESERVED_READING SNSR_OEM_RESERVED_UNITS SNSR_OEM_RESERVED_EVENTS
Metrics used for POWER_SUPPLY	SNSR_POWER_SUPPLY_ID SNSR_POWER_SUPPLY_NAME SNSR_POWER_SUPPLY_TYPE SNSR_POWER_SUPPLY_READING SNSR_POWER_SUPPLY_UNITS SNSR_POWER_SUPPLY_EVENTS
Metrics used for POWER_UNIT	SNSR_POWER_UNIT_ID SNSR_POWER_UNIT_NAME SNSR_POWER_UNIT_TYPE SNSR_POWER_UNIT_READING SNSR_POWER_UNIT_UNITS SNSR_POWER_UNIT_EVENTS
Metrics used for FAN	SNSR_FAN_ID SNSR_FAN_NAME SNSR_FAN_TYPE SNSR_FAN_READING SNSR_FAN_UNITS SNSR_FAN_EVENTS
Metrics used for TEMPERATURE	SNSR_TEMPERATURE_ID SNSR_TEMPERATURE_NAME

	SNSR_TEMPERATURE_TYPE SNSR_TEMPERATURE_READING SNSR_TEMPERATURE_UNITS SNSR_TEMPERATURE_EVENTS
Metrics used for MEMORY	SNSR_MEMORY_ID SNSR_MEMORY_NAME SNSR_MEMORY_TYPE SNSR_MEMORY_READING SNSR_MEMORY_UNITS SNSR_MEMORY_EVENTS
Metrics used for CURRENT	SNSR_CURRENT_ID SNSR_CURRENT_NAME SNSR_CURRENT_TYPE SNSR_CURRENT_READING SNSR_CURRENT_UNITS SNSR_CURRENT_EVENTS

Launching the Energy Data Collector on a Windows or Linux Node

Follow the steps:

1. From the console tree select the **Tools** -> **Systems Infrastructure** folder
2. Select the tool group:

   On Windows:

   Energy Data Collectors -> **Windows**

   On Linux:

   Energy Data Collectors -> **Linux**
3. Double click **Start/Stop Collection**. **Select where to launch this tool** window appears.
4. Select a node to launch the tool and then click **Launch**. Edit Parameters window appears.
5. In the Parameters field, type **Start** to start the data collection and then click **Launch**.

> **Note:** To stop the data collection, type **Stop** in the **Parameters** field and then click **Launch**.

Chapter 6: Systems Infrastructure SPI Reports and Graphs

You can integrate the SI SPI with 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 Reporter and Performance Manager with OM.

Systems Infrastructure SPI Reports

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

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

To view reports for SI SPI from OM 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 Reporter is installed on the Operations Manager Management Server, you can view the reports on the management server directly.

If Reporter is installed on a separate system connected to the Operations Manager Management Server, you can view the reports on Reporter system. For more information on integration of Reporter with OM, see *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

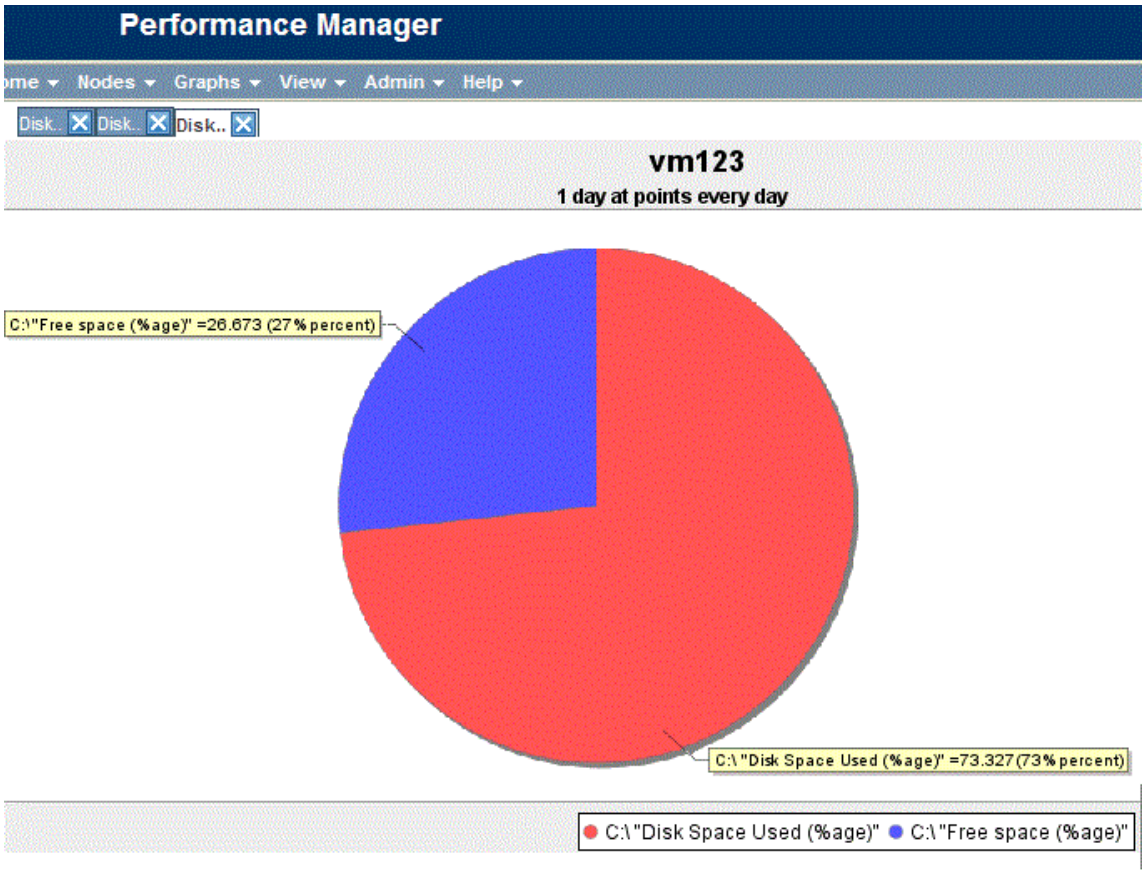
You can generate graphs using Performance Manager for near real-time data gathered from the managed nodes. You can access these graphs from the OM console if you install Performance Manager on an OM management server.

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

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

To access the graphs on OM 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
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

Chapter 7: 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.
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 OM console:
	`An error occurred in the processing of the policy 'SI-DiskCapacityMonitor'. Please check the following errors and take corrective actions. (OpC30-797)`
	`Initialization of collection source "DoNotRename" failed. (OpC30-724)`
	`Cannot find object 'FILESYSTEM' in Coda object list. (OpC30-761)`
	`Searching for 'data source: SCOPE' in the DataSourceList failed. (OpC30-766))`

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

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

Cause	When advanced monitoring policies are edited in user interface mode in OM 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 OM for UNIX.
Solution	To edit the settings in the Measurement Threshold policy, use 'Edit in Raw mode' feature of the OM 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 OM for UNIX (version 9.00) operator console
Solution	Run the following command on the OM 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 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 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 OM 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`

Problem	On a Windows node, even after a new version of the config file policy SI-RealTImeAlerts policy is deployed, alerts are sent to the previous version of policy.
Cause	If the SI-RealTImeAlerts policy is not deployed properly, padv process from the previous version is not killed and it continues to run. Hence alerts are sent to the previous version of the policy.

Solution	Run the following command to get the process ID:
	`ps-ef|grep padv`
	Run the following command to kill the padv process from the previous version:
	`kill <process ID>`

Send documentation feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

Feedback on User Guide (Operations Smart Plug-in for System Infrastructure 12.06)

Just add your feedback to the email and click send.

We appreciate your feedback!