HP OpenView Smart Plug-in for UNIX® Operating Systems

Administrator's Reference

Version: A.03.00

For HP-UX and Solaris OpenView Operations Management Servers

Legal Notices

Warranty.

Hewlett-Packard makes no warranty of any kind with regard to this manual, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

A copy of the specific warranty terms applicable to your Hewlett-Packard product can be obtained from your local Sales and Service Office.

Restricted Rights Legend.

Use, duplication or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause in DFARS 252.227-7013.

Hewlett-Packard Company
United States of America

Rights for non-DOD U.S. Government Departments and Agencies are as set forth in FAR 52.227-19(c)(1,2).

Copyright Notices.

Trademark Notices.

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

Microsoft® is a U.S. registered trademark of Microsoft Corporation.

UNIX® ia a registered trademark of The Open Group.

All other product names are the property of their respective trademark or service mark holders and are hereby acknowledged.

Contents

Contents

Contents

6. Troubleshooting the OSSPI

A. General OSSPI Tips

B. OSSPI Components Without Alternative User Support

Contents

Support

Please visit the HP OpenView web site at:

```
http://openview.hp.com/
```

There you will find contact information and details about the products, services, and support that HP OpenView offers.

The support area of the HP OpenView web site includes:

- Downloadable documentation
- Troubleshooting information
- Patches and updates
- Problem reporting
- Training information
- Support program information

1 Introduction

This chapter provides an overview of the main features and functionality that are provided with the Smart Plug-in for UNIX Operating Systems.

Introducing the OSSPI

The HP OpenView Smart Plug-in for UNIX Operating Systems (OSSPI) is a software product that integrates fully with HP OpenView Operations (OVO) and extends OVO's management scope to include distributed environments of UNIX systems. OVO, formerly VPO/OpC, is a market-leading management solution for networks, systems, databases, and applications in heterogeneous IT environments.

In a setup comprising one or more OVO servers and one or more OVO managed nodes, you can use the OSSPI to monitor the availability and manage the functionality of UNIX operating systems and associated software and hardware. For more information on which operating-system versions are supported by the OSSPI, see the *HP OpenView SMART Plug-in for UNIX Operating Systems Release Notes*.

The OSSPI is also integrated with other HP OpenView products, such as OV Service Navigator, OV Performance, and Coda (**OVO Embedded Performance Component**). This integration allows the users of OSSPI the additional perspective of Service Views. Service Views help users to identify the root-cause of alarms reported on operating systems, associated software services, and, in addition, essential hardware elements such as CPU, memory, swap space and so on. Note that Service Views and performance measurement are only possible if the required *additional* software is already installed and running.

In addition, the functionality of the OSSPI is configured in such a way that it can be used by other HP OpenView SMART Plug-Ins.

Features and Functionality

The Smart Plug-in for UNIX Operating Systems comes with the following features:

- automatic self configuration

- fully customizable

- CIM-based operating-system (OS) service model for the OpenView Service Navigator

- capability to use the OVO Embedded Performance Component and configuration of OVPA and GlancePlus by means of OVO policies

- OS-level system monitoring

- monitoring of computer hardware including; CPU, memory, disks, adapters

- monitoring crucial, kernel-related, table(s) sizes such as file handles and shared memory

- file-system monitoring related to space, errors, availability

- process monitor for OS services, such as; NFS, mail, print, DNS, NTP

- monitoring changes to important configuration files such as `inittab` and `nsswitch.conf`

- a wide range of applications for the quick and easy execution of common OS-related operational tasks

- discovery and monitoring of Sun clusters and associated objects on Solaris managed nodes

- discovery and monitoring of Solstice DiskSuite 4.2.1 objects on Solaris managed nodes

- discovery and monitoring of Veritas Volume Manager 3.x objects on HP-UX and Solaris managed nodes

- message correlation of OVPA/GlancePlus alarms showing the current state of objects

- support for running policies and applications under alternative, non-root user on HTTPS agents with OVO 8.0

2 OSSPI Components

This section describes the components that are added to OVO during the installation of the OSSPI software and how to use them.

In this Section

The information in this section shows the OSSPI components added to OVO during the installation of OSSPI and describes how to use the components to best effect. This section provides detailed information about the following:

- "Application Groups"
- "Message Groups"
- "Node Groups"
- "Policy Groups"
- "Policies"
- "Users and User Profiles"
- "OS Service Views"

Application Groups

The installation of the OSSPI adds a new application group to the OVO
`Application Bank` window. The new application group is called Unix OS
SPI and contains the OSSPI specific application groups as shown in
Figure 2-1.

Figure 2-1   **Unix OS SPI Application Groups**
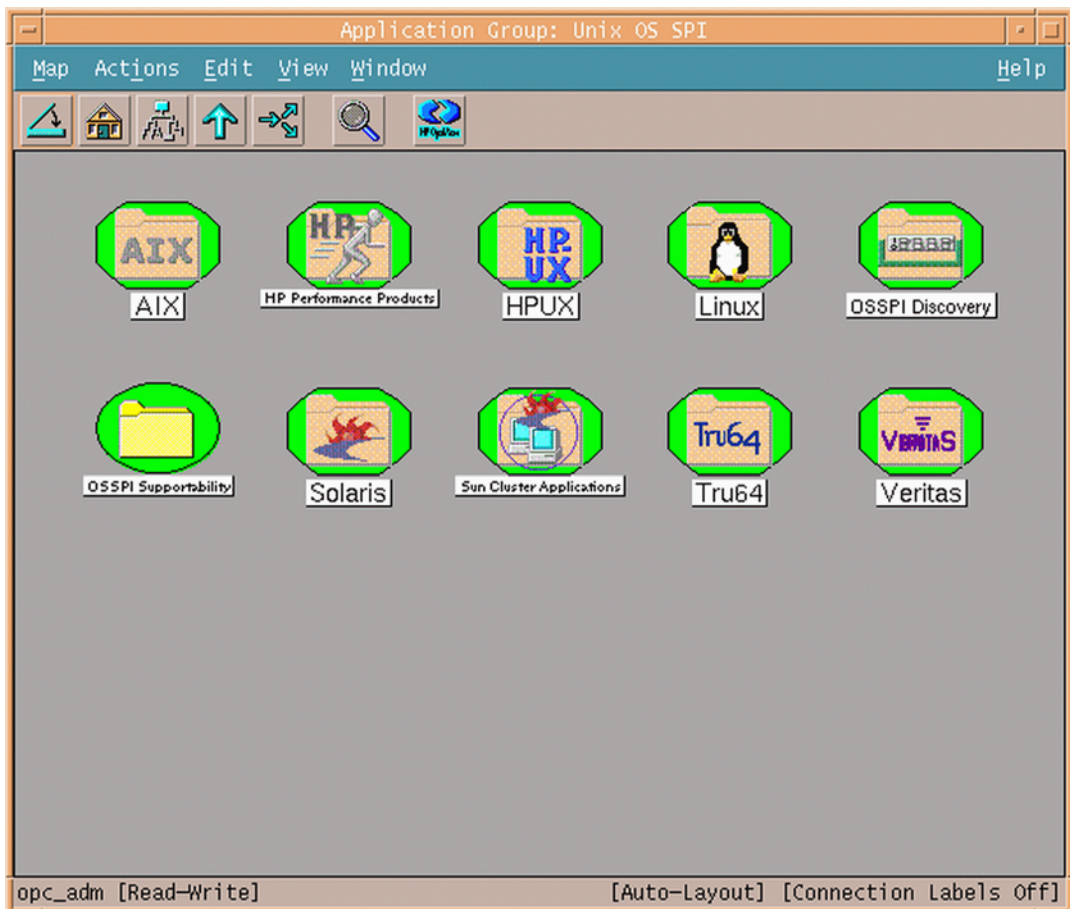
The OSSPI applications are grouped based on platform, product and responsibility. The application groups, explained in detail in the sections that follow, are listed in Table 2-1.

Table 2-1   **Unix OS SPI Application Groups**

Application Group	Description
OSSPI Discovery	This group contains the Discovery application intended to be used by the OVO administrator for discovering services on the OVO managed nodes.
OSSPI Supportability	This group contains applications which are intended to be used by the OVO administrator who is responsible for the administration of the OSSPI, namely; installation, de-installation and troubleshooting.
Platform Specific Groups[a]	**Are the application groups that contain applications specific to the respective platform, as well as generic applications for all the platforms.**
AIX	This group contains applications which are intended to be used by the OVO administrator who is responsible for the administration of AIX nodes.
Linux	This group contains applications which are intended to be used by the OVO administrator who is responsible for the administration of Linux nodes.
Solaris	This group contains applications which are intended to be used by the OVO administrator who is responsible for the administration of Solaris nodes.
HP-UX	This group contains applications which are intended to be used by the OVO administrator who is responsible for the administration of HP-UX nodes.

Table 2-1   **Unix OS SPI Application Groups (Continued)**

Application Group	Description
Tru64	This group contains applications which are intended to be used by the OVO administrator who is responsible for the administration of Tru64 nodes.
Product Specific Groups[a]	**Are the application groups that contain applications specific to the products that integrate with OSSPI.**
HP Performance Products	This group contains applications which are intended to be used by the OVO administrator who is responsible for the administration of managed nodes using HP performance products.
Sun Cluster Applications	This group contains applications which are intended to be used by the OVO administrator who is responsible for the administration of Sun clusters.
Veritas	This group contains applications which are intended to be used by the OVO administrator who is responsible for the administration of VERITAS Volume Manager and VERITAS clusters.

a. This categorization is only to help you in logically grouping the application groups. The platform specific and product specific groups, as they exist in OSSPI, are listed in the rows below each respective entry.

The platform specific and product specific groups are further sub-divided into the Admin and Operator groups. For example, the HP-UX application group is divided into the HP-UX Admin and HP-UX Operator group. The Sun Cluster Applications group is divided into the Sun Cluster Admin and Sun Cluster Operator groups.

The Admin groups contain applications intended to be used by administrators of the platform or product. The administrator is responsible for tasks such as modifying the system, starting or stopping processes, configuring the OSSPI, or running Discovery.

The `Operator` groups contain applications intended to be used by operators. The operator is responsible for tasks such as viewing the status of processes, viewing statistics, or viewing version info.

The Admin and Operator responsibilities are defined in the OSSPI user profiles. Assigning an OSSPI user profile to an OVO user automatically assigns any application groups (along with the applications) contained in the user profile. For more information on user profiles, see "Users and User Profiles" on page 52.

To run any one of the applications in the OSSPI application groups, drag a managed node from the `Node Bank` window (or the `Node Group Bank` window in which the managed node resides) and drop it onto the application you want to run.

OSSPI Discovery

The OSSPI application group `OSSPI Discovery` contains the application which is intended to be used by the OVO administrator for discovering components (also referred to as services) that can be monitored on OVO managed nodes.

Table 2-2   **Application in the OSSPI Discovery Application Group**

Application	Functionality
OSSPI Discovery	Discover services, which runs on the managed node, does the following actions:
	Creates configuration data for the OV Service Navigator
	Uploads the configuration data to the OVO database by means of an operator-initiated action
	Assign nodes to appropriate node groups

OSSPI Supportability

The OSSPI application group OSSPI Supportability contains applications which are intended to be used by the OVO administrator who is responsible for the administration of the OSSPI, namely; installation and de-installation.

Table 2-3 lists the applications present in the OSSPI Supportability application group and provides a brief description of each application's functionality.

Table 2-3   **Applications in the OSSPI Supportability Application Group**

Application	Functionality
OSSPI Clean Node	removes the configuration data generated and used by the OSSPI on the OVO managed node
OSSPI Clean Server	removes the configuration data generated and used by the OSSPI and the OSSPI scripts uploaded on the OVO management server
OSSPI Version	uses the what [a] command to determine the version of *all* the OSSPI executables installed on the OVO managed node by the OSSPI
OSSPI Tracing on/off	enables/disables tracing and sets the trace level, where trace level ranges from 0 to 9; 1=enable, 0=disable

a. Uses osspi_what script for Linux platform.

Platform Specific Application Groups

The platform specific application groups in OSSPI are listed below:

- AIX

- HP-UX

- Linux

- Solaris

- Tru64

Each of these groups contain applications that can be used by the OVO administrator as well as the OVO operator to monitor the respective operating system managed nodes. These application groups are again grouped into the Admin and Operator groups. They contain applications and application groups specific to the platform as well as those applicable to all platforms.The Admin group contains all the applications that you can use to monitor the node. The Operator group contains a subset of these applications, that are relevant to the operators assigned responsibilities.

The Admin and Operator groups contain the following groups:

- OSSPI FS Monitoring: Tools to configure and customize the OSSPI file system utilization monitor

- OSSPI Process Monitoring: Tools to configure and customize the OSSPI process monitor

- OS Tools: Tools to perform system administration on managed nodes in an interactive manner using the OVO GUI.

Figure 2-2 **OSSPI Application Group: HP-UX Admin**

Table 2-4 lists the applications present in the OSSPI FS Monitoring application group and provides a brief description.

Table 2-4 **Applications in the OSSPI FS Monitoring Application Group**

Application	Functionality
OSSPI Edit FS table	open the fstab file in a text editor, for editing
OSSPI FS add global*	add thresholds for *a local* [a] File System to a disk-space configuration file

Table 2-4   **Applications in the OSSPI FS Monitoring Application Group**

Application	Functionality
OSSPI FS add local*	add thresholds for a *local* File System to a disk-space configuration file
OSSPI FS delete global*	delete thresholds for a *global* [b]File System from a disk-space configuration file
OSSPI FS delete local*	delete thresholds for a *local* File System from a disk-space configuration file
OSSPI FS edit local	open the fsmon_local.cfg file in a text editor, for editing
OSSPI FS reactivate global*	reactivate conditions for a *global* File System from a disk-space configuration file
OSSPI FS reactivate local*	reactivate conditions for a *local* File System from a disk-space configuration file
OSSPI FS show global[c]	show conditions for a *global* File System as configured in a disk-space configuration file
OSSPI FS show local[c]	show conditions for a *local* File System as configured in a disk-space configuration file

a. After Discovery the *Local* File System monitor configuration file is generated. You can edit the file.
b. By default the *Global* File System monitor configuration file is present on the management server. You can use the Proc reactivate global tool to modify the configuration file.
c. This is included in the Operator application group.
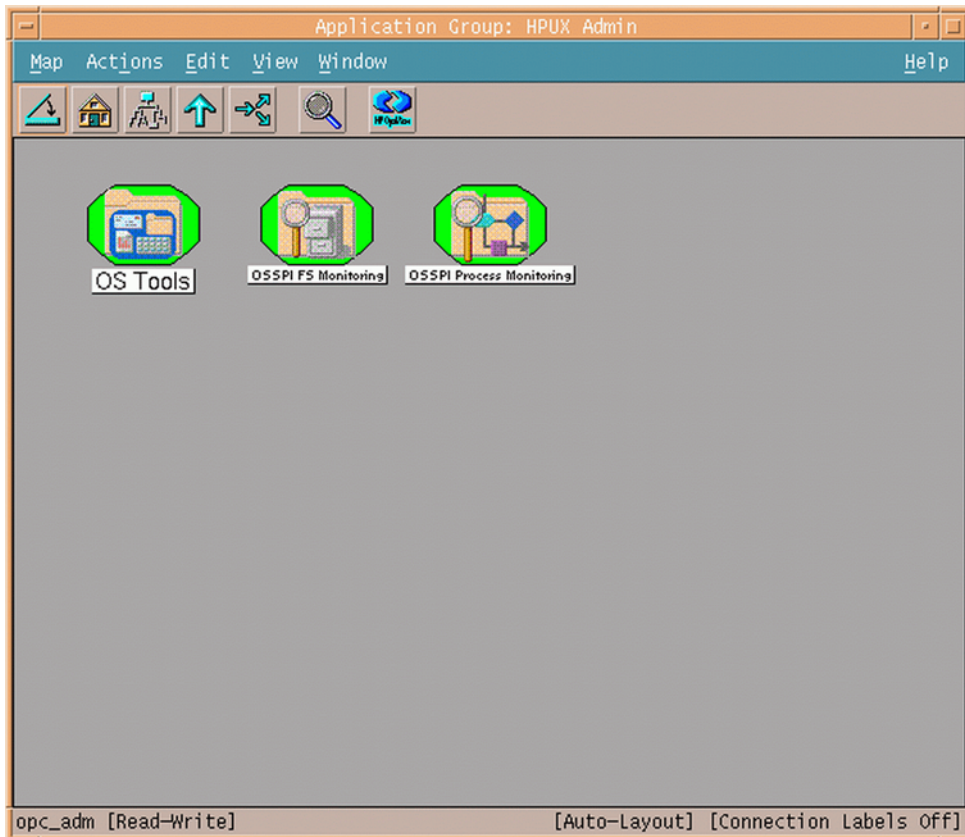
Table 2-5 lists the applications present in the OSSPI Process Monitoring application group and provides a brief description.

Table 2-5   **Applications in the OSSPI Process Monitoring Application Group**

Application	Functionality
OSSPI Proc add*	add a process to a process configuration file
OSSPI Proc add group*	add a process group to a process-group configuration file
OSSPI Proc delete*	delete a process from a process configuration file
OSSPI Proc delete group*	delete a process group from a process configuration file
OSSPI Proc edit global	open the procmon.cfg file in a text editor
OSSPI Proc edit local	open the procmon_local.cfg file in a text editor
OSSPI Proc show local[a]	display a list of local OS processes
OSSPI Proc show global[a]	display a list of normal OS processes

a. This is included in the Operator application group.

Table 2-6 lists the applications present in the OS Tools application group and provides a brief description.

Table 2-6   **Applications in the OS Tools Application Group**

Application	Functionality
Reboot	restart the operating system (reboot) after prompting for confirmation
Shutdown	shut down the OS (halt) after prompting for confirmation

Table 2-6　　　　**Applications in the OS Tools Application Group (Continued)**

Application	Functionality
ifconfig	configure a network interface on the managed node
route	add or delete routes on the managed node
FS mount	mount a local or a remote FS (File System). If no file-system value is given, it displays the contents of the mtab file.
FS umount	*un*-mount local or remote FS (File System). If no file-system value is given, it displays the contents of the mtab file.
NFS stat[a]	display statistical information about Network File Systems for the selected managed node, for example; reads, writes, and lookups for both nfs server and client as an absolute number *and* as a percentage of the total calls. nfsstart (1M) displays statistical information.
ntpstat[a]	display status information about NTP (Network Time Protocol) including error margins for server and peer.
Net stat[a]	display network status information for the selected managed node, for example; routing-table information, configured network interfaces, and active sockets. netstat (1) displays newtork status information.
Disk Space[a]	run the disk free utility, df(1M) (or bdf(1M) on HP-UX systems), which displays the space utilization levels of active file systems on the managed node.
Print Status[a]	run the lpstat (1) command, which displays the status of line printer queues on the managed node.

**Table 2-6**   **Applications in the OS Tools Application Group (Continued)**

Application	Functionality
Processes[a]	run the ps(1) command, which displays the list of processes running on the managed node.
Telnet	connect to managed node, using the telnet network service.
ASCII_SAM[b]	run SAM in character mode (no motif)
Motif_SAM[b]	run SAM motif version
SMIT (AIX)[c]	run the System Management Interface Tool.

a. This is included in the Operator application group.
b. This is an HP-UX specific application
c. This is an AIX specific application

The applications indicated in Table 2-4 and Table 2-5 with an asterisk (*) are configured to run with default parameters that may or may not meet the requirements of your particular environment. OVO allows you to modify these parameters in the application-specific Customized Startup window.

For example, the OSSPI Discovery application writes the information found concerning the OS services running on a managed node to a configuration file located at /var/opt/OV/osspi/conf. Other OSSPI monitor policies use this information to decide which processes to monitor. If you are not interested in monitoring *all* of the OS services discovered by the OSSPI, you need to customize the Delete Process Group application as follows:

Figure 2-3   **Customizing OSSPI Application Startup**
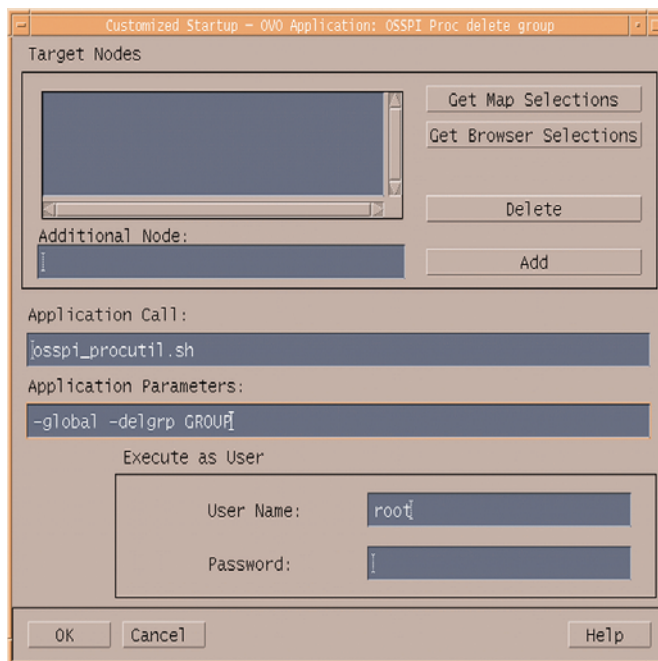
1. Select and right-click the application you want to customize and select the `Customize Startup...` option. The `Customized Startup` window, illustrated in Figure 2-3, opens.

2. Modify the contents of the `Application Parameters` field to suit your requirements. In this example, you can change the parameter *GROUP* with `sendmail`. This *removes* the `sendmail` process group from the list of services to be monitored by the OSSPI.

Product Specific Application Groups

Product-specific application groups contain applications or application groups specific to products that integrate with OSSPI. The application groups for products that currently integrate with OSSPI are:

- HP Performance Products

- Veritas Volume Manager

- Sun Cluster Applications

HP Performance Products

The OSSPI application group HP-UX Performance Products contains applications to be used by the OVO operators working on problems related to system performance (as indicated by messages in OVO). To run any one of the applications in the HP-UX Performance Products application group, drag a managed node from the Node Bank window (or the Node Group Bank window in which the managed node resides) and drop it onto the application you want to run.

The OSSPI application group HP-UX Performance Products contains applications that the OVO administrator can use to:

- view status of HP performance applications running on the managed node

- manage HP GlancePlus

- manage HP OVPA

- manage HP OVPM

Table 2-7 lists the applications present in the HP Performance Products application group and provides a brief description of each application's scope.

Table 2-7　　　　**Applications in the HP Performance Products Group**

Application	Functionality
Configure ttd.conf	edit OV Performance Agent's Transaction Tracker daemon config file
List Processes	show current status of Performance agent and other performance software processes on the node
List Versions	display version details of Performance tools installed
Tail Status Files	display last few lines of performance tool status files
GPM (Motif)	run the HP GlancePlus (Motif) GUI
Glance (Ascii)	run the HP GlancePlus (Ascii) GUI

Table 2-7   **Applications in the HP Performance Products Group**

Application	Functionality
Start OSSPI Glance Processes	starts the OSSPI Glance processes
Status OSSPI Glance Processes	displays the status of OSSPI Glance processes
Stop OSSPI Glance Processes	stops the OSSPI Glance processes
View GP Adviser Syntax	display the OSSPI adviser syntax file for GlancePlus
OVPA showconf	display OSSPI alarmdef definition file for the OVPA agent
Start OVPA	starts OV Performance Agent
Status OVPA	displays status of OV Performance Agent
Stop OVPA	stops OV Performance Agent
Reactivate alarmdef	reinitialize OVPA's Alarm Generator process
Restart PA Servers	restart OVPA server daemon processes
Restart Perf Agt	restart OV Performance Agent processes
Check alarmdef	check the syntax of OV Performance Agent's alarm definitions
Check parm	check the syntax of the OV Performance Agent parm file
Configure perflbd.rc	edit the OVPA perflbd.rc file
Configure parm	edit OVPA's parm (configuration) file
Start utility	start the OVPA utility program
Start Extract	start the OVPA extract program

Table 2-7   **Applications in the HP Performance Products Group**

Application	Functionality
Configure alarmdef	edit default OVPA alarm definitions file
OVPM Console	run the OVPM Console
Start pvalarmd	start OV Performance Manager pvalarm daemons
Stop pvalarmd	stop OVPM alarm daemons

Veritas

The OSSPI application group Veritas contains applications to be used by the OVO operators working on problems connected to VERITAS products (as indicated by messages in OVO). To run any one of the applications in the Veritas application group, drag a managed node from the Node Bank window (or the Node Group Bank window in which the managed node resides) and drop it onto the application you want to run.

The Veritas applications are grouped into the Veritas Admin and Veritas Operator groups.

Table 2-8 lists the applications present in the Veritas Admin and Veritas Operator application groups and provides a brief description of each application's scope.

Table 2-8   **Applications in the Veritas Application Group**

Application	Functionality
Veritas CSCM	display the VERITAS Cluster Server Cluster Manager console
Veritas VMSA	display the VERITAS Volume Manager Storage Administrator console
VxVM Statistics[a]	print statistics information on volumes created using VERITAS Volume Manager.

a. This is included in the Operator application group.

Sun Cluster Applications

The OSSPI application group `Sun Cluster Applications` contains applications to be used by the OVO operators working on problems with Sun Clusters (as indicated by messages in OVO). To run any one of the applications in the `Sun Cluster Applications` application group, drag a managed node from the `Node Bank` window (or the `Node Group Bank` window in which the managed node resides) and drop it onto the application you want to run.

The `Sun Cluster Applications` are grouped into the `Sun Cluster Admin` and `Sun Cluster Operator` groups. For more information on Sun Cluster Applications, see Chapter 5, "Monitoring Sun Clusters."

Message Groups

The OSSPI installs four message groups that are specifically designed to handle messages generated by the policies and monitors started by the OSSPI. Figure 2-4 shows the OSSPI message groups.

Figure 2-4   **OSSPI Message Groups**
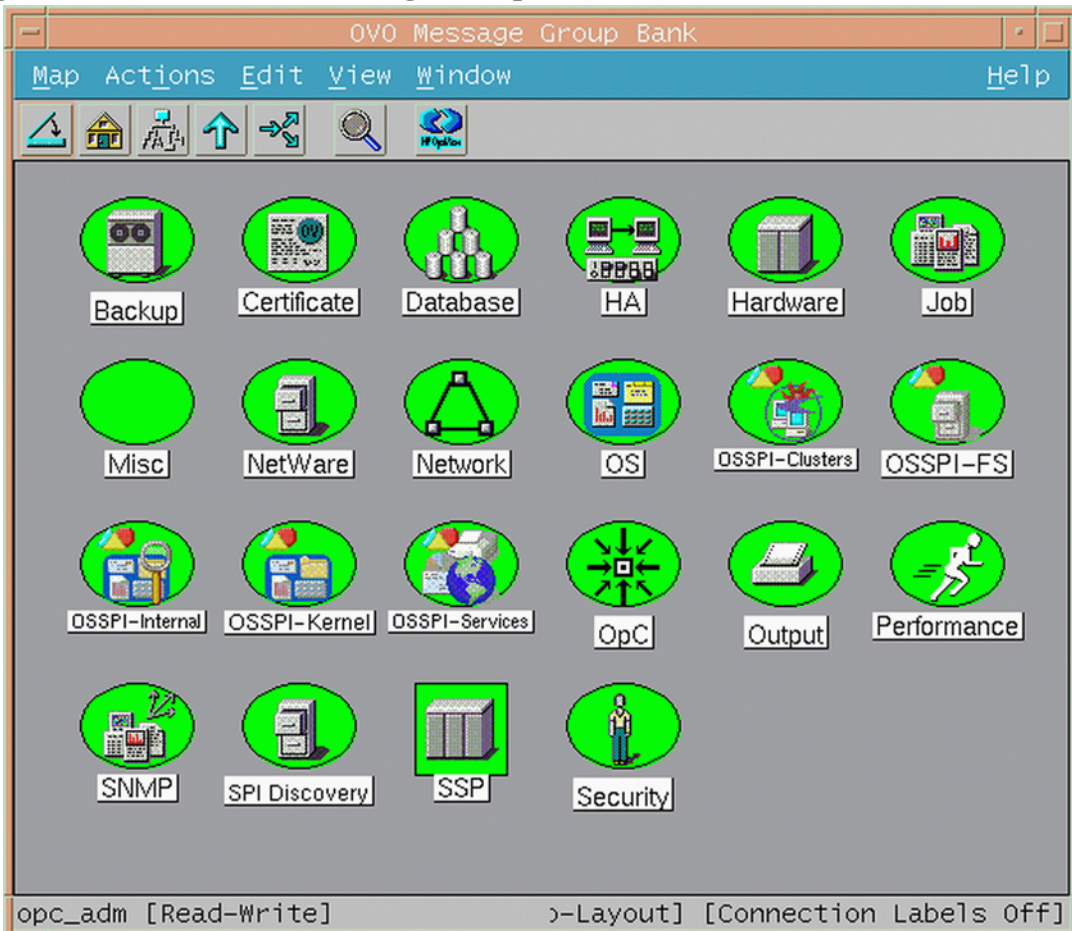
OSSPI generates a variety of messages on Hardware, Network, Output, OS, Performance, and SNMP - areas that may already be covered by pre-defined OVO message groups.

OSSPI assigns relevant messages to existing OVO message groups. Messages that do not belong to the OVO message groups are assigned to one of the following OSSPI-specific message groups:

OSSPI-FS
: Messages relating to the local and network file systems as well as logical volumes

OSSPI-Internal
: Internal messages concerning the operation of the OSSPI itself

OSSPI-Kernel
: Messages relating to the kernel and kernel resources

OSSPI-Services
: Messages relating to the services discovered and monitored by the OSSPI

Note that all OSSPI message groups are assigned by default to *all* the OSSPI user profiles, which are uploaded to OVO during the installation of the OSSPI. This means that assigning any of the OSSPI user profiles to a OVO user ensures that this OVO user receives OSSPI messages automatically assuming the appropriate node groups assigned, too. For more information about OSSPI user profiles, see "Users and User Profiles" on page 52.
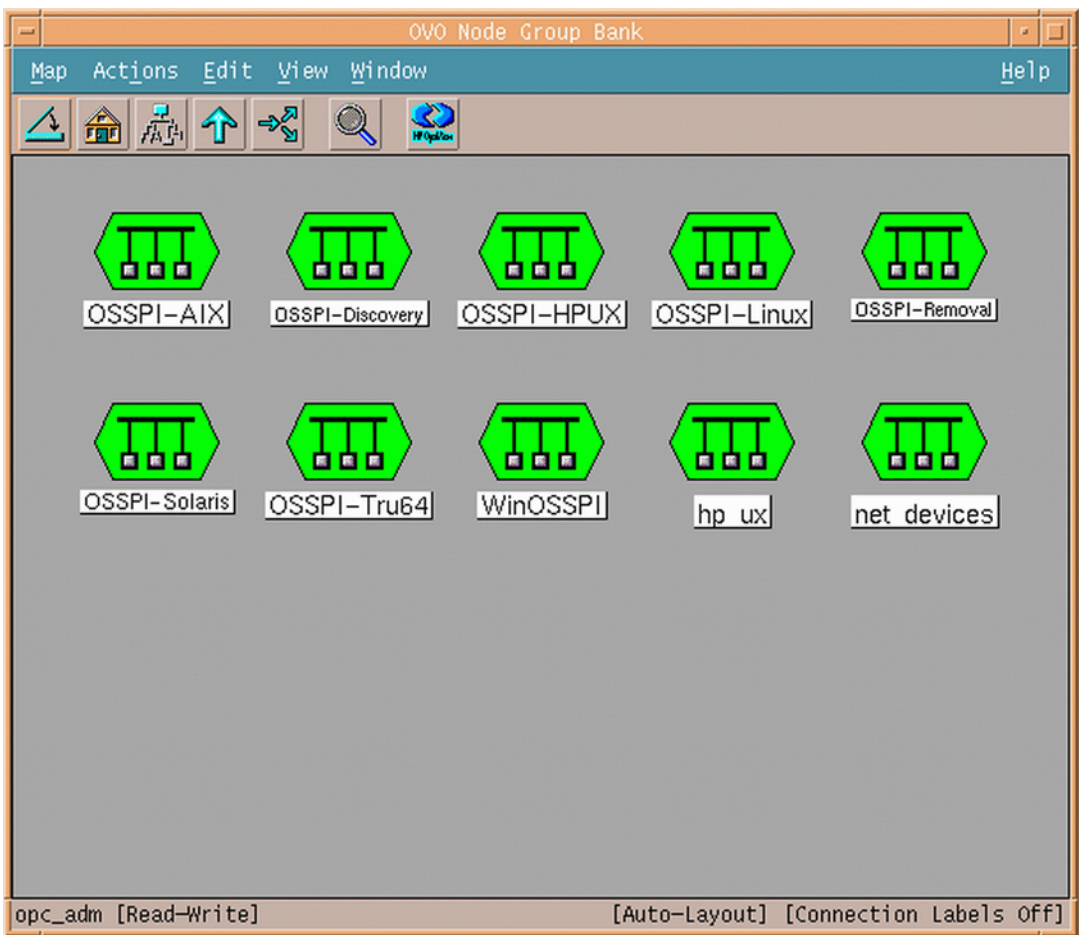
Node Groups

During the installation of the OSSPI software, a number of new, OSSPI-specific node groups are added to the OVO Node Bank window, as illustrated in Figure 2-5 on page 34. The OSSPI-specific node groups installed by the OSSPI are intended to be used in the following way:

OSSPI-AIX   Contains the nodes running AIX that you want to monitor with the OSSPI.

OSSPI-HPUX   Contains the nodes running HP -UX that you want to monitor with the OSSPI.

OSSPI-Linux   Contains the nodes running Linux that you want to monitor with the OSSPI.

OSSPI-Solaris   Contains nodes running Solaris that you want to monitor with the OSSPI.

OSSPI-Tru64   Contains nodes running Tru64 that you want to monitor with the OSSPI.

OSSPI-Discovery   Before running Discovery, all nodes must be placed in this Node group.

OSSPI-Removal   Prepares a node for removing OSSPI configuration data, reset OVPA and Glance Plus alarms to their original settings.

The node groups themselves are empty on installation. Following Discovery the node is assigned to the node group based on the OS running on the node. Example: A node running Linux OS will be assigned to the Linux node group.

Note that the OSSPI node groups are assigned to the OSSPI user profiles, which are described in more detail in "Users and User Profiles" on page 52. This means that OVO users to whom you assign the OSSPI user profiles will automatically receive messages from all those nodes included in the OSSPI node groups.

Figure 2-5   OSSPI Node Groups

Policy Groups

The installation of the OSSPI uploads a number of policy groups to the OVO database. The high-level OSSPI policy groups are assigned automatically to the corresponding high-level OSSPI node groups.

NOTE   Do not distribute the policies before running Discovery. Policies are dependant on the configuration file that is created only after discovery.

For more information about assigning and distributing policies in OVO, see "Getting Started" on page 63.
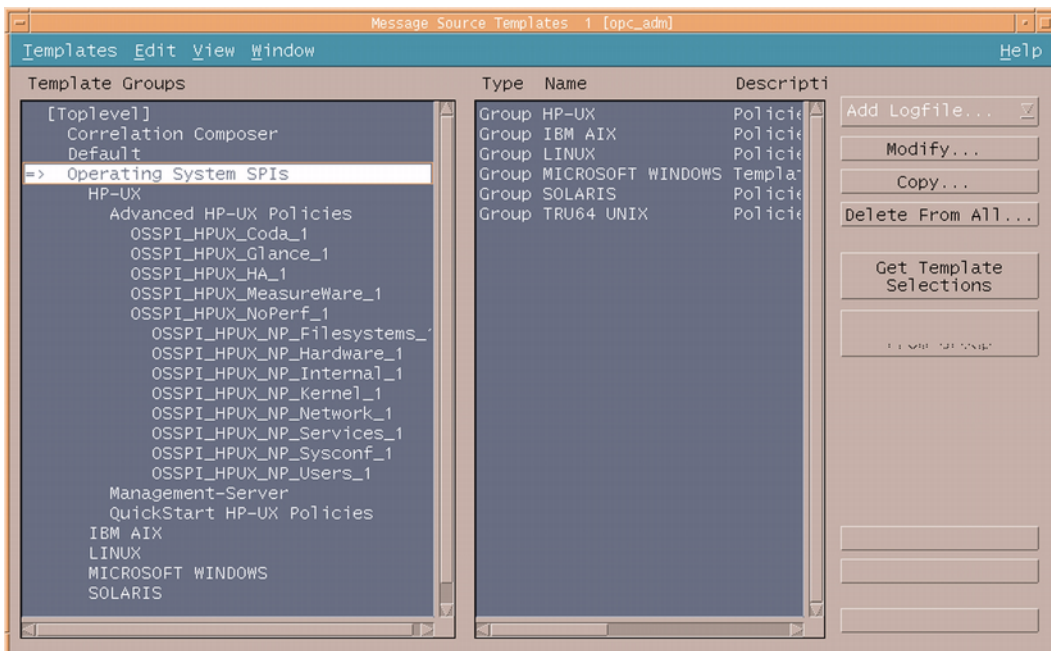
Figure 2-6   OSSPI Policy Groups

Figure 2-6 shows the high-level policy groups that are installed by default with the OSSPI software. The following groups appear under the top-level group, namely `Operating System SPIs`.

- `HP UX`

- `IBM AIX`

- `Linux`

- `Solaris`
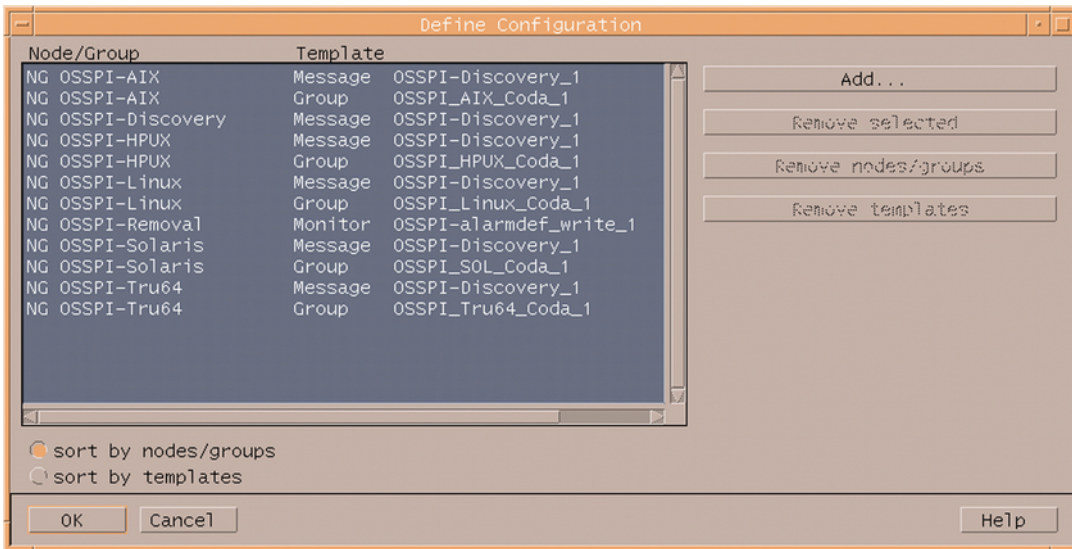
- `Tru64 UNIX`

NOTE   The terms template and policy are used interchangeably in OSSPI, and both terms refer to the same OSSPI component.

Check that the correct default policies and policy groups have been automatically assigned by selecting any one of the newly added nodes and using the following menu option:

`Actions: Agents > Assign Templates...`

The `Define Configuration` window shown in Figure 2-7 on page 37 opens. Check that the correct policy and policy-group assignments have been made.

Figure 2-7   **OSSPI Default Policy Group Assignments**

Note that identical policy groups are installed for HP-UX, AIX, Linux,
Solaris, and Tru64 UNIX and contain similar policies. Table 2-9 on
page 37 lists the high-level groups and provides a short description of
what they do.

Table 2-9   **HP UX Policies and Policy Groups**

Policy Group	Functionality
Quick Start	Policy group containing the basic policies to monitor managed nodes.
Advanced	Policy group containing advanced policies to monitor specific applications on managed nodes.
Management Server	Policy group containing policies to monitor the management server. This group will appear only on HP UX and Solaris management servers.

Table 2-9   **HP UX Policies and Policy Groups (Continued)**

Policy Group	Functionality
OSSPI-Discovery	Policy to be used for discovery-related messages.

The policies in the Quick Start and Management Server groups are described in the section "Policies" on page 41. Table 2-10 on page 38 lists the policy groups in the Advanced group and provides a short description of what they do.

Table 2-10   **Advanced Policies and Policy Groups**

Policy Group [a]	Functionality
OSSPI_*HPUX*_CODA	Policy group to be used to monitor the managed node using the OV embedded performance components.
OSSPI_*HPUX*_Glance	Policy group to be used if GlancePlus performance tools are installed on the managed node you want to monitor with the OSSPI
OSSPI_*HPUX*_MeasureWare	Policy group to be used if OV Performance (formerly MeasureWare) tools are installed on the managed node you want to monitor with the OSSPI.
OSSPI_*HPUX*_NoPerf	Policy group to be used if there are no performance tools installed and running on the managed node.
OSSPI_*HPUX*_HA[b]	Policy group to be used if there are high-availability clusters to be monitored.
OSSPI-alarmdef_write_1	Policy that automatically configures and writes the alarm definition file for OV Performance and GlancePlus.

a. Replace *HPUX* with *AIX*, *Linux*, *Sol*, or *Tru64* for high-level, operating-system-specific policy groups.HP GlancePlus is not supported on Tru64 UNIX operating systems.

b. The HA policy group is available only on *HPUX* and *Solaris* managed nodes.

Table 2-11 lists the policy groups in the OSSPI_HP-UX_Glance policy group. The contents of the OSSPI_HP-UX_Glance policy group are similar to the OSSPI_HP-UX_CODA, OSSPI_HP-UX_MeasureWare and OSSPI_HP-UX_NoPerf policy groups—the names of the policies in the group have been changed to reflect the chosen performance tool.

Table 2-11   **OSSPI_HP-UX_Glance_1 Policy Group**

Policy Group[a]	Functionality
OSSPI_*HPUX_GP_*Filesystems	monitors local and network file-systems utilization and volume group space
OSSPI_*HPUX_GP_*Hardware	monitors the hardware related metrics for the hardware including; CPU, network interfaces, swaps and disk utilization
OSSPI_*HPUX_GP_*Internal	monitors the OSSPI internal processing messages related to OSSPI error, trace logfiles and alarmdef events
OSSPI_*HPUX_GP_*Kernel	monitors the status of the kernel and kernel resources including modifications to the kernel image, file-lock, file-open, process, semaphore, and shared-memory tables
OSSPI_*HPUX_GP_*Network	monitors the network interfaces on the node
OSSPI_*HPUX_GP_*Services	monitors the OS services such as cron and crontab, dns, nfs, print, sendmail, and so on.

Table 2-11   **OSSPI_HP-UX_Glance_1 Policy Group (Continued)**

Policy Group[a]	Functionality
OSSPI_*HPUX_GP*_Sysconf	monitors the modifications made to the system configuration such as `/etc/inetd.conf`
OSSPI_*HPUX_GP*_Users	monitors user activities such as bad logins, login and logout histories, and switch-user events

a. In all references above, replace *HPUX* with *AIX*, *Linux*, *Sol*, or *Tru64* as appropriate for the operating system running on the node, and replace *GP* with *CD*, *MW*, or *NP* for the appropriate performance tools (GP for Glance Plus, CD for Coda, MW for OVPA and NP, if no performance tools are present on the node). HP GlancePlus is not supported on Tru64 UNIX operating systems.

Policies

The policies provided with the OSSPI may be split into the following generic areas:

- Table 2-12, "OSSPI Logfile Policies," on page 41
- Table 2-13, "OSSPI Monitor Policies," on page 43
- Table 2-14, "OSSPI Performance Policies," on page 46
- Table 2-15, "OSSPI Message Interceptor Policies," on page 47

The names of the policies listed in the following tables are abbreviated versions of the actual policy names that appear in the OVO GUI. The full OSSPI policy names have the prefix OSSPI and, where appropriate, an identifier for the operating system, for example; AIX, HPUX, Linux, SOL (for Sun Solaris), or Tru64. In addition, the extension (_#) identifies the policy version.

For example: OSSPI-HPUX-<*Template_Name*>_1 refers to version 1 of the same policy. The platform name is specified within the policy name such as in OSSPI_AIX_cfgmon_1. The policy is specific to the platform. If the policy name does not contain any platform names as in OSSPI-MailQueue, the policy is common to all platforms and changes made in these policies will be reflected for all platforms.

Table 2-12 on page 41 lists the logfile policies installed with the OSSPI, gives a brief description of their scope, and indicates how often the policy polls the logfile for information and updates.

Table 2-12   OSSPI Logfile Policies

Policy Name	Description	Polling Interval
BadLogs	*Un*successful user logins	10s
Boot	Monitors system boot messages, for example; /sbin/rc and /etc/rc.log	1m
Dmesg	Kernel message log	10s
DNSstat	Monitor DNS statistics	30m

Table 2-12   OSSPI Logfile Policies (Continued)

Policy Name	Description	Polling Interval
Logins	Successful user logins	10s
MailAliases	Monitors changes to mail aliases file	10m
MailLog	Monitors the sendmail application logfile	10m
PrintLog	Monitors the print logfile	10m
SNMPConf	Monitors SNMP configuration file entries	10m
SNMPLog	Monitors SNMP logfile entries	10m
Su	Monitors the switch user activities and reports	20s
Syslog	Monitors system log file, for example; /var/adm/syslog/syslog.log on HP-UX	1m
Veritas_log	Monitors the Veritas Volume Manager log file	1m
Cron	Monitors the cron(1M) clock daemon logfile	30s
Syslog (Service-Guard)	Fetches messages from MC/ServiceGuard and forwards to APM	10s
Engine Log (SC)	Fetches messages from SC and forwards to APM	10s
Engine Log (VCS)	Fetches messages from VCS and forwards to APM	10s
Engine Notify Log (VCS)	Fetches messages from VCS and forwards to APM	10s
HACMP logfile	Monitors HACMP cluster logs	1m
Lplog	Monitors line printer daemon logfile	1m

Table 2-12   OSSPI Logfile Policies (Continued)

Policy Name	Description	Polling Interval
OS Msgs	Monitors operating system messages	30s
SIA Log	Monitors SIA logfile	20s

Table 2-13 on page 43 lists the *monitor* policies installed with the OSSPI, gives a brief description of their scope, and indicates how often the monitor policy polls for information and updates.

NOTE   The System Configuration Monitor policy (OSSPI-cfgmon) monitors a generic list of system configuration monitor files. These configuration files such as /etc/inetd.conf, /etc/fstab, /etc/passwd usually exist on the nodes based on the operating system. The policy monitors the timestamp of the files and sends notifications to the message browser when these files undergo any changes. If the policy detects any missing configuration files, it sends a message with a minor severity to the message browser. The Operator may choose to ignore or suppress these messages if the files are not critical for the operating system run on the node.

Table 2-13   OSSPI Monitor Policies

Policy Name	Description	Polling Interval
alarmdef_write	Monitors changes to the alarmdef file	1m
cfgmon[a]	Tracks changes to the system configuration files, for example; the entries in the crontab file, the inetd process, the fstab file and so on.	30m
ChkGlancePid	Monitors the Glance processes run by OSSPI when Glance Plus policies are deployed on the node.	1m
CronProc	Monitors the cron process	15m

Table 2-13   OSSPI Monitor Policies (Continued)

Policy Name	Description	Polling Interval
defect_long[b]	Long-term monitor of bad disk blocks	28d
defect_short [b]	Short-term monitor of bad disk blocks	6h
DNSLookup	Monitors the DNS availability	10m
DNSProc	Monitors the DNS server process	1m
Filesystem	Monitors the file system as well as inode utilization.	5m
InetdProc	Monitors the inetd process	1m
InternalLog	Monitors the size of the OSSPI internal log and trace files	10m
kmon [b]	Monitors the state of the kernel image including: creation date of actual kernel, compiled kernel, and kernel parameter file	1h
MailPerm	Monitors the permissions of the mail files and directories	1h
MailProc	Monitors the sendmail process	10m
MailQueue	Monitors the length of the mail queue	10m
Mount	Monitors the mounted file systems and access	20m
NetInterfaces	Monitors the network interfaces	5m
NFSClientProc	Monitors NFS client processes	5m
NFSServerProc	Monitors NFS server processes	5m
NTPProc	Monitors the ntpd process	10m
QuotaUsage	Monitors the quota usage	30m

Table 2-13   **OSSPI Monitor Policies (Continued)**

Policy Name	Description	Polling Interval
Printenable	Monitors and checks if the printers are enabled	10m
PrintProc	Monitors the print cap process	10m
PrintQueue	Monitors the length of the print queue	10m
PrintPerm	Monitors the print file permissions	1h
Pty_Avail	Monitors the availability	365d
sdsmon	Monitors the Solstice DiskSuite objects. Reports if a new object has been added after discovery or if a discovered object has been deleted	1h
SNMPProc	Monitors the SNMP processes	10m
swapmon	Monitors swap usage	5m
SyslogProc	Monitors the syslog process	1m
Veritas	Monitors the status of Veritas Volume Manager	2m
VeritasProc	Monitors the critical Veritas Volume Manager vxiod and vxconfigd processes	1m
VG	Monitors all logical volume groups, created by Logical Volume Manager Group	1h
cpu_util	Monitors CPU utilization. Requires the sar program	2m
disk_util	Monitors disk space utilization on the root disk	10m
pcntmon	Monitors process table utilization	5m
Swap_util	Monitors SWAP utilization	5m

a. Due to differences between linux (Debian/SuSE linux) distributions, you may encounter warning messages stating that xinetd.conf is not present on the node. These may be safely ignored, if the distribution uses inetd.conf, and not xinetd.conf

b. Not available for AIX.

NOTE　　　　　　The OSSPI-NP_Filesystem_1 policy is a generic policy that is linked to the platform-specific OSSPI file-system policies for AIX, HP-UX, etc. Changes to this file-system-monitor policy will appear in all the other file-system-monitor policies, too.

Table 2-14 lists the Coda and OV Performance policies installed with the OSSPI, gives a brief description of their scope, and indicates how often the policy polls the Coda/OV Performance (or MeasureWare) agent for information and updates. Note that not all the policies listed in Table 2-14 are available for Coda.

Table 2-14　　　　**OSSPI Performance Policies**

Policy Name	Description	Polling Interval
CPU_load	CPU load factors	1m
Disk	Disk I/O on local disks	1m
Flock_Tbl	Monitors file locks in use	5m
Fopen_Tbl	Monitors open files	5m
Filesystem	Monitors disk space	5m
IPC [a]	Monitors the IPC, for example; message, semaphore, and shared-memory tables	5m
Kresources [a]	Monitors the Kernel table space; file locks, open files, and processes.	5m
Lan_Coll	Monitors network I/O rate	
Mem_Load	Monitors the load on memory	1m
Msg_Tbl	Monitors the message table	5m

Table 2-14   **OSSPI Performance Policies (Continued)**

Policy Name	Description	Polling Interval
Proc_Tbl	Monitors process table usage	5m
NetworkAdapter	Monitors network packet collisions and error rates	
Sema_Tbl	Monitors semaphore usage	5m
Shmem_Tbl	Monitors shared memory usage	5m
Swap_Res	Monitors the global swap rate and usage	1m

a. *NOT* present in the Coda policy group

Table 2-15 lists the *OpC* policies installed with the OSSPI, gives a brief description of their scope, and indicates how often the monitor policy polls for information and updates.

Table 2-15   **OSSPI Message Interceptor Policies**

Policy Name	Description	Polling Interval
alarmwriteMsg	Intercepts messages generated during the creation of alarm definition files for OV Performance or Glance Plus.	n/a
Discovery	Intercepts messages from the OSSPI Discovery application	n/a
FilesystemMsg	Intercepts messages related to file system from OSSPI (s) file system monitor	n/a
opcmsg [a]	Intercepts OSSPI internal processing messages as well as alarm messages from OV Performance or Glance Plus.	n/a
procmonmsg	Intercepts messages relating to process status from OSSPI (s) process monitor.	n/a

Table 2-15   **OSSPI Message Interceptor Policies (Continued)**

Policy Name	Description	Polling Interval
xterm	Intercepts messages concerning applications started by OVO on the managed node as well as xterm processes, which failed to start.	n/a

a. This policy duplicates and should replace the original OVO
   opcmsg policy.

NOTE   The OSSPI installs a new and improved version of the opcmsg policy
          alongside the original OVO opcmsg policy. If you assign both opcmsg
          policies to the same managed node, you will receive duplicate messages.
          We recommend you replace the original OVO opcmsg policy with the new
          OSSPI opcmsg policy. If you have made any changes to the original OVO
          opcmsg policy, you will have to migrate these changes to the OSSPI
          version of the opcmsg policy before re-assigning and re-distributing the
          policies to the managed nodes.

          Table 2-16 lists the trap policies installed with the OSSPI, gives a brief
          description of their scope, and indicates how often the policy polls for
          information and updates

Table 2-16   **OSSPI Trap Policies**

Policy Name	Description	Polling Interval
NNM 6.2 Traps	Monitors SNMP traps generated from NNM 6.2	n/a
NNM 6.41 Traps	Monitors SNMP traps generated from NNM 6.41	n/a
NNM 7.0 Traps	Monitors SNMP traps generated from NNM 7.0	n/a
SNMP ECS Traps	Monitors correlated events generated from NNM	n/a

Using the Correlation Composer

The OVO-ECS integration package installs the Correlation Composer policy group that contains the policy to correlate messages from various sources, and the OV Composer application group that provides tools for using and customizing the correlators. The Correlation Composer policy is visible in the Message Source Template window, along with the template group, Operating System SPIs. The OV Composer application group is visible in the application bank along with the Unix OS SPI application group.

Correlation Composer Policy

The Correlation Composer policy uses the OSSPI correlators described in the following table for correlation.

Table 2-17   **OSSPI Correlators**

Correlator	Functionality
osspi_good_ftp_bad_ftp	When an FTP successful message is received within 3 minutes of FTP unsuccessful messages, the FTP unsuccessful messages are discarded.
osspi_good_log_bad_log	When a login successful message is received within 3 minutes of login unsuccessful messages, all the login unsuccessful messages are discarded.
osspi_good_su_bad_su	When a switch user successful message is received within 3 minutes of switch user unsuccessful messages, all the switch user unsuccessful messages are discarded.

Table 2-17   **OSSPI Correlators (Continued)**

Correlator	Functionality
osspi_high_cpu_swap_ut il	Correlates messages from the OSSPI CPU monitor template and the SWAP monitor template, to indicate the probability of thrashing. If messages sent for both are critical, it indicates the probability of thrashing.
osspi_if_down	Correlates the 'Interface down' SNMP trap message generated by NNM, with the message generated by OSSPI instrumentation
osspi_if_down_nfs_prob lems	Correlates messages when 'Interface down' messages are received for an interface from SNMP trap and OSSPI instrumentation, along with NFS problems. The interfaces are checked for the cause of the problem and one common message is sent.
osspi_node_down	Correlates messages from the SNMP trap template and the OSSPI logfile encapsulators, when a node goes down.
osspi_node_up	Correlates messages from the SNMP trap template and the OSSPI logfile encapsulators, when a node comes up.

The correlators listed in Table 2-17 are the pre-defined correlators available with OVO. To add, delete, modify or view the correlators, you can use the Composer UI (Dev) application.

OV Composer Application Group

The OV Composer application group contains applications to be used by OVO administrators working with OSSPI correlators. To run any one of the applications in the OV Composer application group, drag a managed

node from the `Node Bank` window (or the `Node Group Bank` window in which the managed node resides) and drop it onto the application you want to run.

Table 2-18 lists the applications in `OV Composer` application group.

Table 2-18   **Applications in the OV Composer Application Group**

Application	Functionality
`Composer UI (Dev)`	launch the Composer UI to add, delete, modify or view the correlators
`Install Correlators on Agent`	install the correlator fact store on the agent
`Install Correlators on Server`	install the correlator fact store on the server

You can run the `Composer UI (Dev)` application to make changes to the pre-defined correlators. To view the list of correlators in the Composer GUI, you must open the OSSPI correlator fact store. The OSSPI fact store, `osspi_comp.fs`, is available at the location, `/etc/opt/OV/share/conf/OpC/mgmt_sv/CO`.

Users and User Profiles

The OVO administrator uses user profiles to simplify the process of assigning responsibilities to new OVO users. The installation of the OSSPI software adds a number of new user profiles to the OVO `User Profile Bank` window. These user profiles are defined based on platform, product and responsibility areas of the user.

An Administrator and an Operator profile is added for each operating system and product that is monitored by the OSSPI, as illustrated in Figure 2-8. The Janitor, Supportability and Performance profile are sub-profiles that assign to other profiles the responsibility of cleaning up the system, troubleshooting, and monitoring Performance products, respectively.

Figure 2-8   **OSSPI User Profiles**
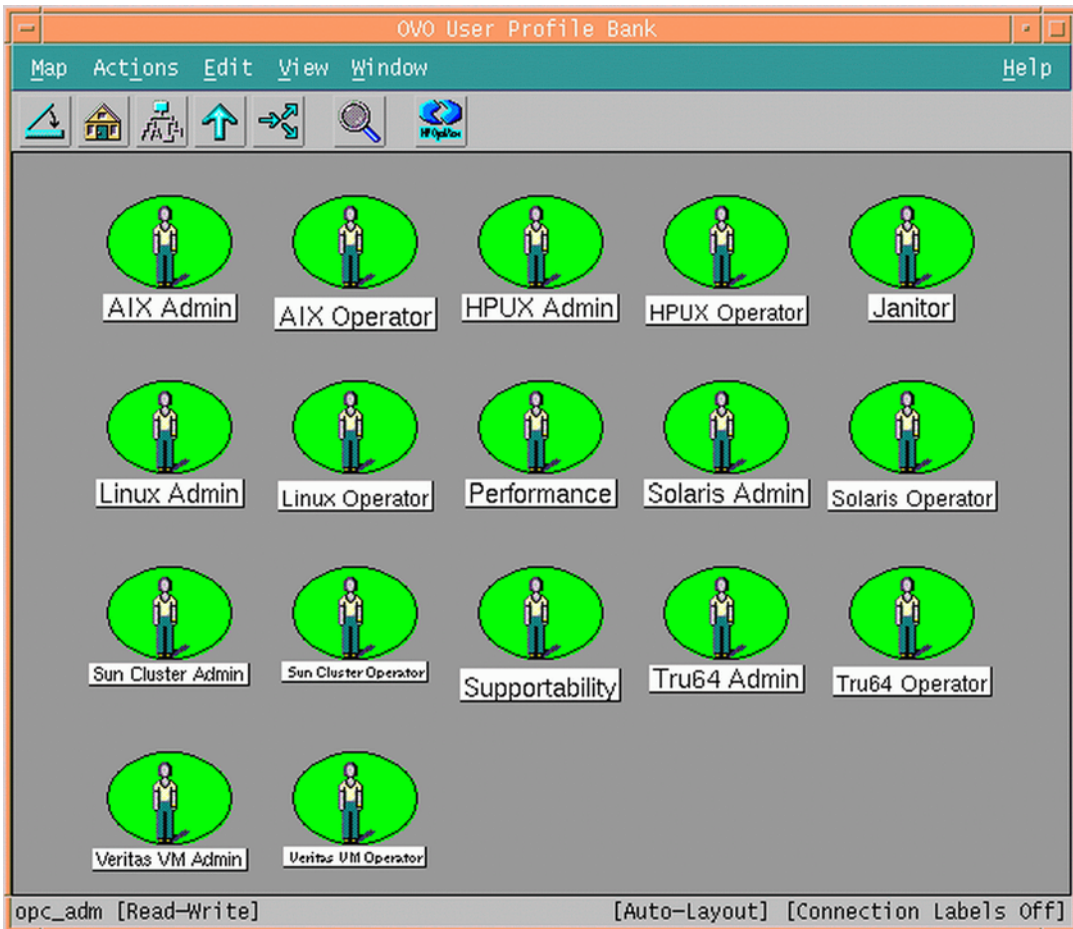
To get a complete list of an OVO user's responsibilities, you can generate a report using the following menu option:

`Actions:Utilities > Reports... > Operator Report`

The OSSPI user profiles define the following areas of responsibility:

The OSSPI User Profile...	is for Users Responsible for...
AIX Admin	the administration of the OSSPI itself as well as the AIX managed nodes, which the OSSPI is monitoring

AIX Operator	the AIX managed nodes, which the OSSPI is monitoring
HPUX Admin	the administration of the OSSPI itself as well as the HP-UX managed nodes, which the OSSPI is monitoring
HPUX Operator	the HP-UX managed nodes, which the OSSPI is monitoring
Linux Admin	the administration of the OSSPI itself as well as the Linux managed nodes, which the OSSPI is monitoring
Linux Operator	the Linux managed nodes, which the OSSPI is monitoring
Solaris Admin	the administration of the OSSPI itself as well as the Solaris managed nodes, which the OSSPI is monitoring
Solaris Operator	the Solaris managed nodes, which the OSSPI is monitoring
Tru64 Admin	the administration of the OSSPI itself as well as the Tru64 UNIX managed nodes, which the OSSPI is monitoring
Tru64 Operator	the Tru64 UNIX managed nodes, which the OSSPI is monitoring
Veritas Admin	the administration of the OSSPI itself as well as VERITAS products, which the OSSPI is monitoring
Veritas Operator	the VERITAS products, which the OSSPI is monitoring
Sun Cluster Admin	the administration of the OSSPI itself as well as Sun clusters, which the OSSPI is monitoring
Sun Cluster Operator	Sun clusters, which the OSSPI is monitoring
Supportability	troubleshooting on the managed nodes, which the OSSPI is monitoring

Performance	the performance of systems, which the OSSPI is monitoring
Janitor	the clean-up of systems, which the OSSPI is monitoring

Table 2-19 shows at a glance how the OSSPI user profiles assign responsibilities to a user's role.

Table 2-19   OSSPI User Profiles: Roles and Responsibilities

Role	OSSPI Responsibilities							
	Platform Specific		Product Specific		Support-ability	Perfor-mance	Clean-Up	Disco-very
	adm	op	adm	op				
Admin	✓		✓			✓	✓	✓
Operator		✓		✓	✓			

Table 2-20 shows at a glance which OSSPI *message* groups are assigned by default to which OSSPI user profiles.

Table 2-20   OSSPI User Profiles: Message Groups

Message Group	OSSPI User Profile									
	AIX		HP-UX		Linux		Solaris		Tru64	
	adm	op	adm	op	adm	op	adm	op	adm	op
OSSPI-FS	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
OSSPI-Internal	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
OSSPI-Kernel	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
OSSPI-Services	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Table 2-21 shows at a glance which OSSPI *node* groups are assigned by default to which OSSPI user profiles.

Table 2-21   **OSSPI User Profiles: Node Groups**

Node Group	OSSPI User Profile									
	AIX		HP-UX		Linux		Solaris		Tru64	
	adm	op	adm	op	adm	op	adm	op	adm	op
OSSPI-Discovery	✓		✓		✓		✓		✓	
OSSPI-AIX	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
OSSPI-HPUX	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
OSSPI-Linux	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
OSSPI-Sol	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
OSSPI-Tru64	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

OS Service Views

The OSSPI integration with the OpenView Service Navigator provides
the user of the OSSPI with the additional perspective of *Service* views.
This feature is available only if the OpenView Service Navigator
software is installed and running. Service views allows individual
systems to be seen in terms of the configured hardware, the installed
software, and the OS *services* that are running. The OSSPI discovers the
services automatically and uses the discovered data to generate the
service OSSPI tree for the OV Service Navigator as illustrated in
Figure 2-9.

Figure 2-9   The OSSPI Services
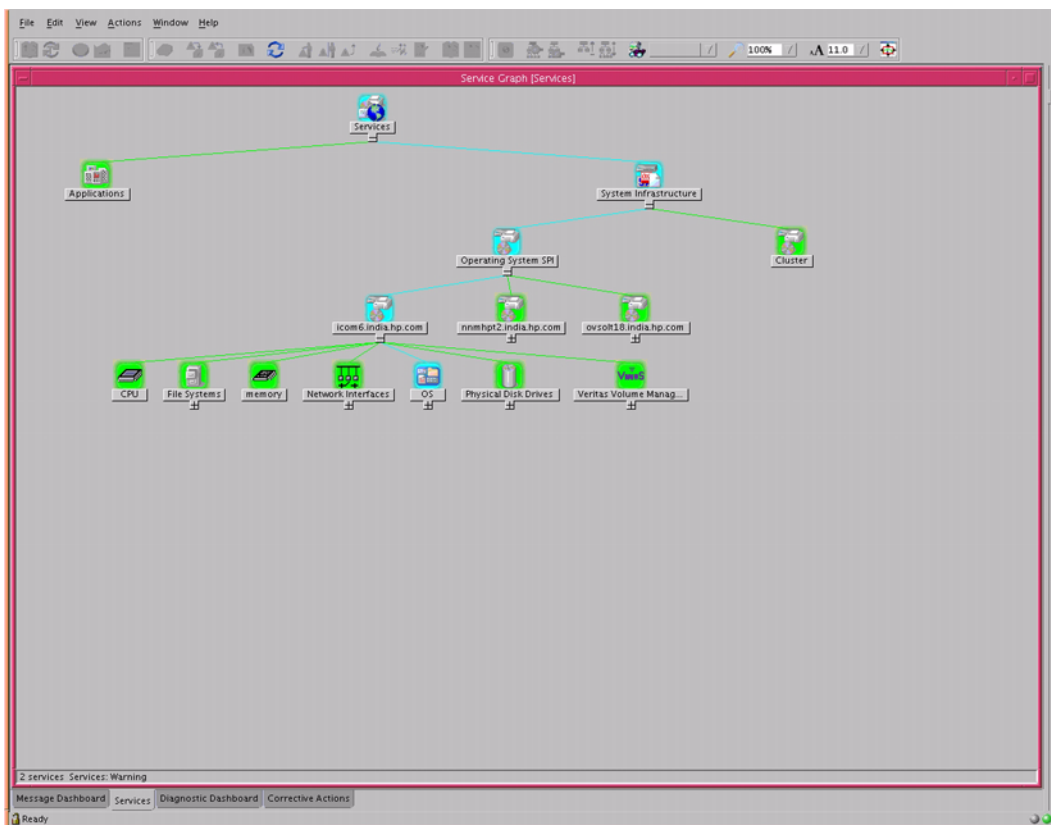
The service graph generated by the OSSPI is a snap shot of the services on the managed nodes at the time at which the OSSPI `Discovery` application was run. If the service configuration on a managed node subsequently changes, you will have to run the discovery process again to have the changes reflected in the OSSPI service tree.

The combination of the two products allows root-cause analysis of any problems in the most crucial elements of the operating system such as CPU, memory, swap space and so on.

Propagation rules for the objects in the OSSPI service tree are defined by default as *unchanged*. This means that a parent service does not change the status of a child object by, for example; attaching a priority to it. Such a scenario would be feasible if a parent service considered the status of one child service to be more important than the status of another child service.

Calculation rules for the OSSPI service tree are set by default to *Most Critical*. This means that if a parent service has more than one child service, it assumes the status equal to the highest severity of its child services. For more information about calculation and propagation rules, as well as how to go about modifying them, see the *HP OpenView ServiceNavigator Concepts and Configuration Guide*.

Service View for Veritas Volume Manager

The service view for Veritas Volume Manager displays volumes containing sub volumes. Grouping is done under the highest level volume. The current version of the OSSPI does not discover RVG and RLINKS. All the unassociated objects are not discovered.

Figure 2-10   Service View for Veritas Volume Manager
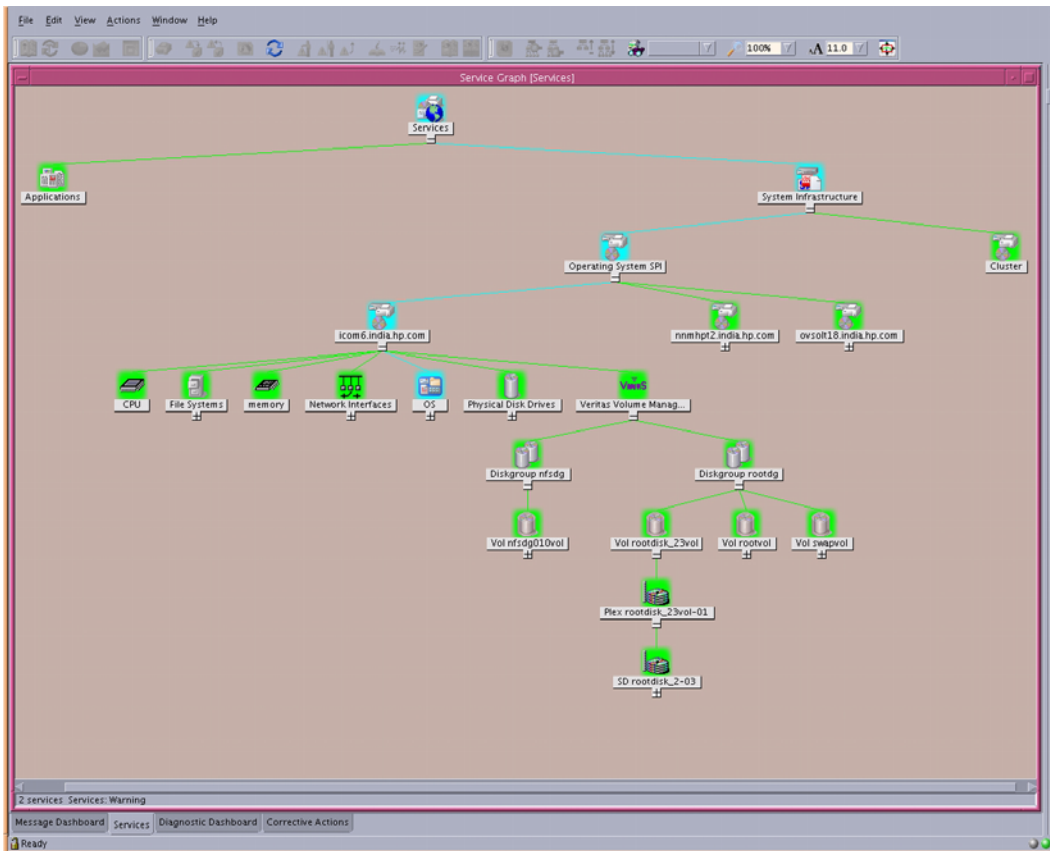
Service View for Logical Volume Manager

Inactive Logical Volumes and Logical Volume Groups created by LVM
are not displayed in the service view which the OSSPI generates.
However, Inactive Volumes created by Veritas Volume Manager are
discovered and displayed in the service view.

Figure 2-11 **Service View for Logical Volume Manager**
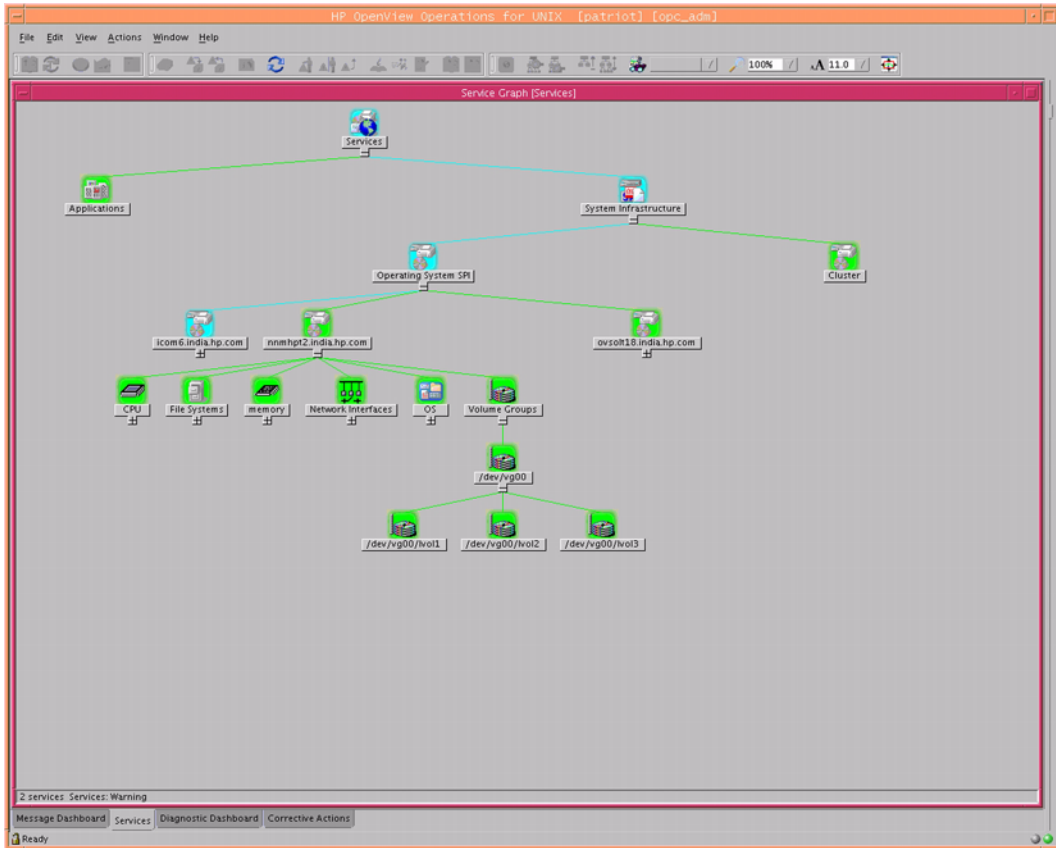
NOTE Inactive Logical Volumes and Logical Volume Groups are not integrated in the service view which the OSSPI generates.

Service View for Solstice DiskSuite

The service graph of Solstice DiskSuite shows a hierarchical representation of its objects. However, unlike the Windows service graph, if, for example, a meta device (d30) is made up of meta device d20 and d10, you must open d30 before d20 and d10 appear in the service graph.

Currently, only State Database Replicas, Hot Spare Pools, Soft
Partitions, Layers and Metadevices in the local disk set are discovered
and monitored.

Figure 2-12   Service View for Solstice DiskSuite
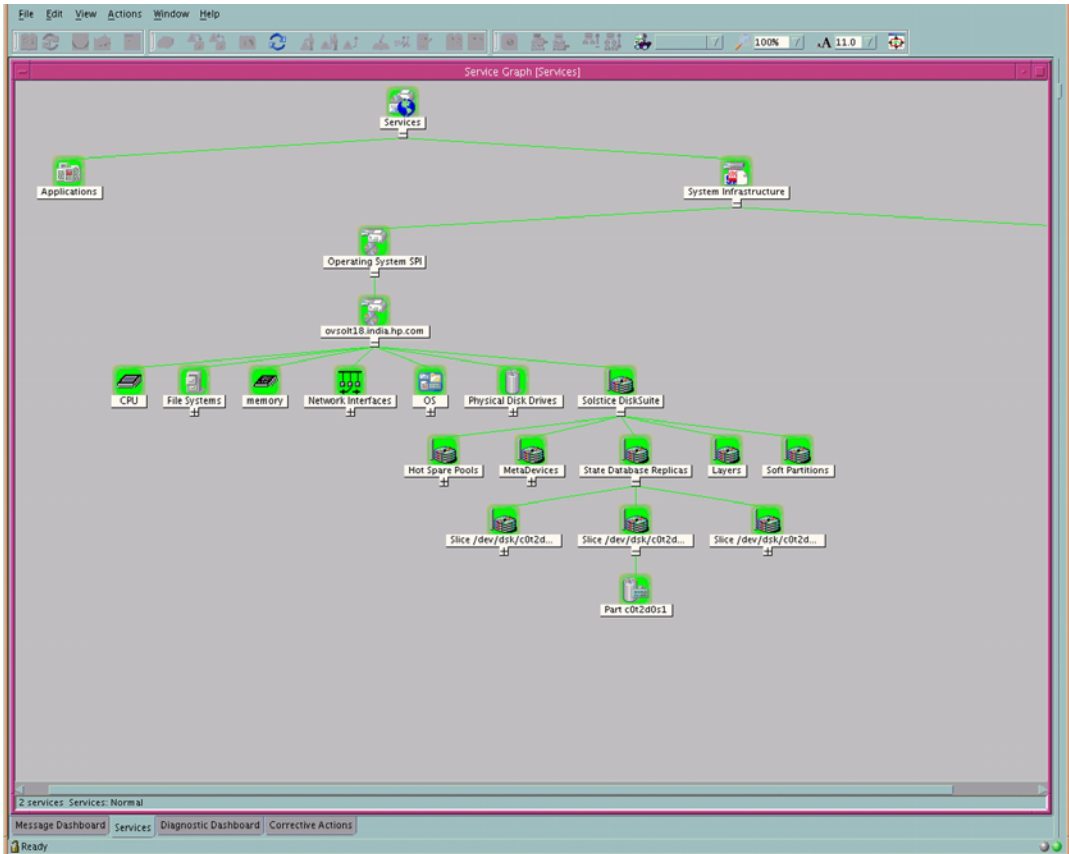
3   Getting Started

This section describes how to perform the initial configuration of the Smart Plug-in for UNIX Operating Systems. Once you have completed the tasks in this section, you will be able to use the features and functionality of the OSSPI.

In this Section

The tasks described in this chapter take you through the initial configuration of the OSSPI software and must be performed as OVO user `opc_adm`. This chapter includes the following topics:

- "Assigning Nodes to the Discovery Group"

- "Assigning User Profiles"

- "Distributing the OSSPI Policies and Instrumentation"

- "Choosing the Performance Tool"

- "Discovering OS Services on Managed Nodes"

- "Distributing the Modified OSSPI Policies"

Assigning Nodes to the Discovery Group

In order to discover the services you want to monitor with OSSPI policies on various OVO managed nodes in your environment, you must add the nodes to the `OSSPI-Discovery` node group. This default node group is added to the OVO `Node Group Bank` window during the installation of OSSPI.

NOTE   We recommend that you do not assign any managed nodes to the other OSSPI node groups at this point in time as this could lead to a large number of meaningless messages appearing in the `Message Browser` window.

1. Open the `Node Group Bank` window and expand (by double-clicking) the `OSSPI-Discovery` node group

2. Drag the managed nodes you want to monitor with the OSSPI from the `Node Bank` window and drop them into the `OSSPI-Discovery` node-group window.

NOTE   If the nodes you want to monitor with the OSSPI are part of an MC/ServiceGuard cluster, place a copy of all *physical* nodes in the MC/SG cluster in the `OSSPI-Discovery` node group. The MC/SG cluster's virtual node has to be added to the `OSSPI-HPUX` node-group as an External (Message allowed) node.

3. Check that the correct, default policies and policy groups have been automatically assigned by selecting any one of the newly added nodes and using the following menu option:

   `Actions: Agents > Assign Templates...`

4. If you want to verify policy assignments for an individual node (or group of nodes), you can use the OVO report feature to generate a list of the policies assigned to a given node, as follows:

   a. In the `Node Bank` (or `Node Group Bank`) window, select the node (or node group) for which you want to generate a report.

b. Click the following menu option:

   `Actions > Utilities > Reports`

c. Select `Node Report` as illustrated in Figure 3-1.

d. Make sure that the OSSPI-specific policies listed in "Verifying Installation of the OSSPI Software" in the *HP OpenView Smart Plug-in for UNIX Operating Systems Installation Guide* are present in the list of policy assignments generated by the report.

Figure 3-1 Generating an OVO Node Report
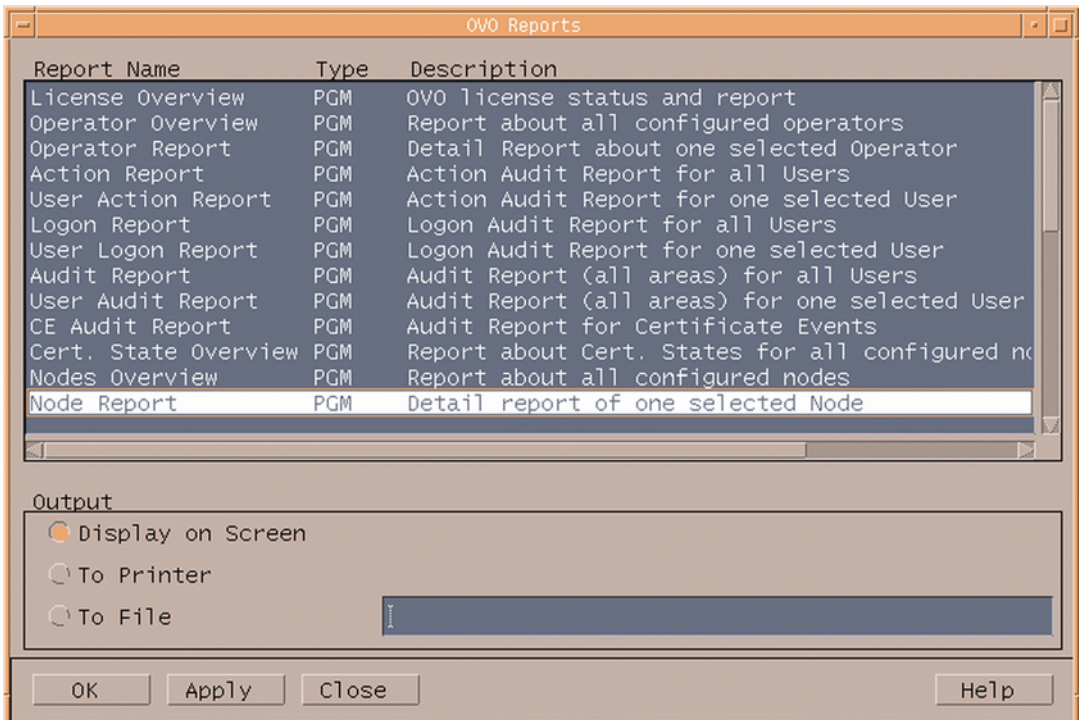
Assigning User Profiles

This section describes how to assign the OSSPI user profiles to the OVO users whom you intend to make responsible for the administration of the OSSPI and the managed nodes on which the OSSPI runs. For more information about user profiles in OVO, see "Users and User Profiles" on page 52.

To assign user profiles to OVO users:

1. Open the User Bank window.

2. Select and right-click the user to whom you want to assign responsibility for the OSSPI (e.g. opc_adm) and choose the following option from the menu that pops up:

   Modify...

   The Modify User: <user> window displays. In this example, *<user>* would be; opc_adm

3. Click the [Profiles...] button. The Profiles of User: *<user>* window appears.

4. Next, open the User Profile Bank window

5. Drag the AIX-admin, the HPUX-admin, the Linux-admin, the Solaris-admin, and the Tru64-admin user profiles from the User Profile Bank window and drop them into the Profiles of User: *<user>* window.

NOTE   The responsibilities in a user profile are *global* and, as a result, not immediately visible in the Responsibility Matrix window of the individual user to whom the user profile is assigned. Similarly, the responsibilities of the user are *local* and only visible in the user's own responsibility matrix. For example, if you assign the HPUX-admin user profile to the OVO user opc_adm, *all* the message groups and node groups assigned in the HPUX-admin user profile are indeed assigned to the OVO user opc_adm even if it does not, at first, appear so in opc_adm's responsibility matrix.

6. In the Modify User: *<user>* window, click [OK].

Distributing the OSSPI Policies and Instrumentation

This section describes how to distribute the OSSPI policies, actions, commands, and monitors to the OVO managed nodes you want to monitor with the OSSPI. To assign and distribute the OSSPI policies, carry out the following steps:

1. In the `Node Group Bank` Window, click the `OSSPI-Discovery` node group, and select the following menu option:

   `Actions:Agents > Install/Update S/W & Config...`

   The `Install/Update S/W & Config...` window opens.

2. Verify that the correct nodes and node groups appear and that the policy assignments you made in the previous step are correctly displayed in the `Assigned Templates` list.

3. Next, check (✓) the items you want to distribute and click `[OK]`.

   ✓ `Templates`

   ✓ `Actions`

   ✓ `Commands`

   ✓ `Monitors`

4. Click `[OK]`

   OVO opens a shell to indicate the progress of the distribution. When the distribution process has completed, a message appears in the `Message Browser` window indicating that the policy distribution completed successfully. You can refresh the browser window using the following menu option in the `Message Browser` window:

   `Browser: Reload`

Choosing the Performance Tool

In this section, you identify which performance tool is running on the OVO managed node so that the correct OSSPI policies can be distributed and the appropriate monitors started. The OSSPI allows you to choose between the following performance-related data sources and uses the following pre/postfixes to distinguish between them in the OVO GUI:

CODA/CD   Coda (OVO Embedded Performance Component)

GP   GlancePlus

MW   OV Performance (formerly MeasureWare)

NP   *No* performance tools are running on the node

To distribute only those policy groups required by the nodes, do as follows:

1. Remove policy groups for performance tools not present on the managed node from the policy-assignment list

2. Distribute policies to the nodes.

To use the OVO GUI to install the OpenView Performance agent:

1. In the `Node Bank` window, select the following menu option:

   `Actions: Subagent > Install/ Update...`

   The `Install / Update Subagents` window opens as shown in Figure 3-2.

Figure 3-2   Installing the OV Performance Agent Package
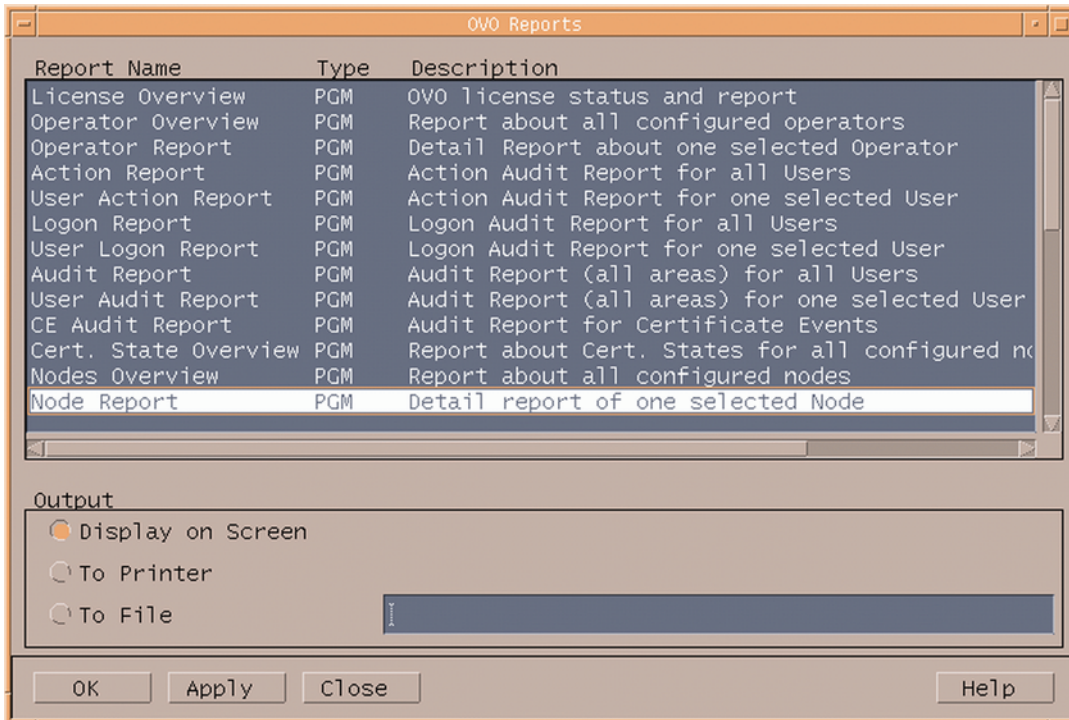
2. Check [✓] the OV Performance Agent button and click [OK]

NOTE   Wait for sometime after the installation of the OV Performance agent is
               completed in order to be sure that the OV Performance agent processes
               have indeed started successfully and are running. Run the Status OVPA
               application in the HP Performance Products group to see if all the OVPA
               processes (alarm gen) are running. All these processes are required to be
               running before any of the OSSPI policies are deployed on the node.

Discovering OS Services on Managed Nodes

In this section, you use the `Discovery` application installed by the OSSPI to find out what services are running on the nodes you want to manage with the OSSPI. The OSSPI uses this information to generate a service-configuration file for the OpenView Service Navigator. To discover which service are running on the nodes you want to monitor with the OSSPI:

1. Start the OVO GUI and open the `Node Bank` window.

2. Open the `Application Bank` window and expand the `OSSPI` application group.

3. Expand the `OSSPI Discovery` group window, drag the node you want to monitor and drop it onto the `Discovery` application in this window.

   This starts the discovery application on the management server. The `Discovery` application runs as root on the management server and initiates a client side discovery on the managed node.

4. The OSSPI displays the progress of the `Discovery` application in a shell. Note that error messages are written to the following file on the OVO management server:

   `/var/opt/OV/log/SPISvcDisc/discovery_error.log`

5. `Discovery` notifies when it fails. You can view the messages in the active message browser to see the current status of `Discovery`.

   Once the discovery application is run, you need to add the node to the appropriate OSSPI node group. Example: `Linux` nodes should be assigned to `OSSPI_Linux` node group.

Discovery Rerun Scenarios

The discovery process takes a snap shot of the state of the services on the managed node at a given point in time. If the service configuration on a managed node subsequently changes, you will have to run the discovery process again to have the changes reflected in the OSSPI service tree. The OSSPI configuration files are also updated with the current set of monitor able files.

Typical Scenarios when OSSPI discovery should be (re) run on the node.

- When the Logical Volume Manager, Veritas Volume Manager, Solstice DiskSuite setup is modified.

- When new hard disks are configured or added.

- When new network adapters are configured or added.

- When services are configured or new services are installed on the nodes. (`named daemon`, `cron daemon`)

- When node is made part of a MC/SG cluster.

Assigning Nodes to Node Groups

If the nodes you want to monitor with the OSSPI are part of an
MC/ServiceGuard cluster, each MC/SG package (or *virtual* node) must be
represented in the OSSPI-HPUX node-group as an *External*
(message-allowed) Node, as illustrated in Figure 3-3 by orapkg1. Note
that this is a *requirement* for shared file system monitoring.

If the nodes you want to monitor with the OSSPI are part of a Sun
cluster, each node of the cluster must be added to the OSSPI-Solaris
node group.

orapkg1 shown in the figure is the package name and must be a *valid*
DNS name resolving to orapkg1.domain.com

Figure 3-3   **Adding External Nodes**
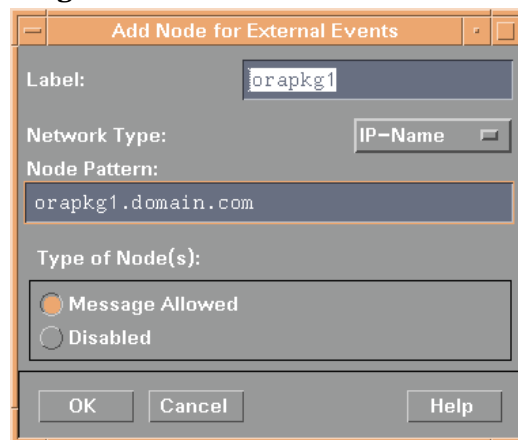
Distributing the Modified OSSPI Policies

To complete the distribution of the OSSPI policies to the OVO managed nodes you want to monitor with the OSSPI, you have to distribute the OSSPI policies a second time, as follows:

1. In the Node Group Bank Window, hold down the **Ctrl** key, click the OSSPI-AIX, OSSPI-HPUX, OSSPI-Linux, OSSPI-Solaris, and OSSPI-Tru64 node groups, and select the following menu option:

   Actions:Agents > Install / Update SW & Config...

   The Install / Update VPO Software and Configuration... window opens.

2. Verify that the correct nodes and node groups appear and that the policy assignments you made in the previous step are correctly displayed in the Assigned Templates list.

3. Next, check [✓] the items you want to distribute. In this case, it is only the new policies assigned in the previous step:

   ✓ Templates

      Actions

      Commands

      Monitors

4. Finally, check [✓] the Force Update option to ensure that modifications are distributed:

   ✓ Force Update

5. Click [OK].

4 Customizing the OSSPI

This chapter describes how to fine-tune the wide variety of functions and features in the OSSPI software to suit the demands of your environment.

In this Section

This section provides reference information which is designed to help you understand how the OSSPI works and, in addition, how to go about adapting it to suit the specific requirements of your particular environment. The section includes:

- "Configuring Performance Tools Centrally with OVO Policies"

- "Configuring OV Performance and GlancePlus"

- "Using Threshold-Monitor Conditions to Set up OV Performance and GlancePlus"

- "Configuring the OVO Embedded Performance Component"

- "Using Threshold-Monitor Conditions to Set up the OVO Embedded Performance Component"

- "Monitoring File Systems with the OSSPI"

- "Monitoring Processes with the OSSPI"

- "Service Discovery"

- "Monitoring OS-Service Configuration Files"

- "Configuring Standard Policies"

- "Modifying Polling Intervals for Monitoring File System Utilization (GlancePlus and OVPA)"

- "Configuring OSSPI to Run as Alternative User"

Configuring Performance Tools Centrally with OVO Policies

If performance tools such as Coda, OV Performance, or GlancePlus are running on the managed nodes which you want to monitor with the OSSPI, you can use OVO message-source policies to configure the performance thresholds *centrally* on the OVO management server. This section and the sections that follow describe how to instruct the OSSPI to read values (default or modified by you) in message-source policy conditions, use the information to define the alarm thresholds required by Coda, OV Performance, or GlancePlus and, where appropriate, tell the respective performance tool to read the updated definitions.

To set up performance thresholds centrally you need to carry out the following high-level tasks:

1. Set up the policies to configure your performance tool.

2. In the policies, define conditions so that alarms of varying severity are dispatched to the performance tool.

For OV Performance, the OSSPI monitors the downloaded policies and automatically scans for changes. If changes are discovered, the OSSPI creates alarm definitions based on the new thresholds and writes the definitions into `/var/opt/OV/osspi/conf/osspi_alarmdef` (`/var/lpp/OV/osspi/conf/osspi_alarmdef` on AIX systems). If the file already exists, a backup is taken (`osspi_alarmdef.old`) and the new values are written into `osspi_alarmdef`. The file `osspi_alarmdef` is included in the central `alarmdef` file as illustrated below. The OSSPI then instructs OV Performance to reread the alarm definitions in the `alarmdef` file:

```
# edited by OSSPI --- BEGIN
include /var/opt/OV/osspi/conf/osspi_alarmdef
# edited by OSSPI --- END
```

The OSSPI writes the definitions for GlancePlus to a *separate* alarm syntax file, `/var/opt/OV/osspi/conf/syntax_gp` (`/var/lpp/OV/osspi/conf/syntax_gp` on AIX systems), then restarts GlancePlus to use these new definitions.

Only file system monitors permit you to set node-specific thresholds.

NOTE	After modifying a policy or any of its conditions, make sure that you re-distribute the policies to the nodes that require it.

## Configuring OV Performance and GlancePlus

The OSSPI allows you to use the OVO GUI to set up new (or modify existing) threshold monitors for OV Performance or GlancePlus. You will need to use the Add Threshold Monitor window or the Modify Threshold Monitor window illustrated in Figure 4-1. When adding or modifying monitor policies, the OSSPI expects you to follow the rules and naming conventions described in this section.

Figure 4-1   The Modify Threshold Monitor Window

The information that follows helps you through the configuration process by describing what information needs to be entered and, where appropriate, in what format for each of the required fields in the Add Threshold Monitor or the Modify Threshold Monitor window.

Monitor Name   A string that *must* begin with one of the following prefixes:

OSSPI-MWA_   for OV Performance monitors

OSSPI-GP_   for GlancePlus monitors

Description   The name of the object to be monitored by OV Performance or GlancePlus, for example: CPU_Bottleneck

Monitor Program or MIB ID   A string composed of the monitor program osspi_null.sh followed by a space and the arguments indicated using the order and syntax specified. Note that the monitor program osspi_null.sh is *required* by OVO:

osspi_null.sh <monitor_name> '<Rule_1>, <Rule_2>, <Rule_n>'

monitor_name   the *name* of the monitor as specified in the Monitor Name field followed by a space

Rule n   threshold rules separated by a comma and a space *and* enclosed in single quotes, for example;

'<rule_1>, <rule_2>, …'

where *rule_n* takes the following form:

<METRIC> <CONDITION>

For example:

GBL_CPU_TOTAL_UTIL > 95 prob 90

The rules compute a value which represents the *STATUS* of the monitored object. *STATUS* can then be compared with the thresholds defined in the monitor conditions.

Polling Interval   Enter a large number, for example; 365 (days). The monitor is not required to run at any time: it is simply used to define conditions.

Threshold Type   Monitor *maximum* thresholds. The thresholds themselves are defined in the monitor conditions as described in "Using Threshold-Monitor Conditions to Set up OV Performance and GlancePlus" on page 80.

Message Generation   Set to: With Reset

Service Name   *Optional* field: enter the name of the service (and sub-service) to which the message is to be assigned—in the following format:

OSSPI:*<service_name>*@@<$MSG_NODE_NAME>

where:

service_name	is the OSSPI *sub-service* name, for example; **cpu**
MSG_NODE_NAME	a variable resolved by OVO to the name of the managed node that generated the message

Object   *Optional* field: if a component such as a file system, disk, or network adapter is present more than once on the managed node you want to monitor, use the Object field to specify a tag which indicates the component *type*. The OSSPI inserts the rules and conditions defined in the policy into the alarmdef or syntax_gp file for *each* instance of the component detected during the discovery process and attaches the tag as a prefix to each rule. The following tags are currently supported:

Disk	system disk
FS	file system
NetworkAdapter	network adapter

Using Threshold-Monitor Conditions to Set up OV Performance and GlancePlus

If you are using the OVO Condition No. # window illustrated in Figure 4-2 on page 82 to set up new (or modify existing) conditions for OSSPI threshold monitors, remember to set the Message on Matched Condition option. Note also that OVO expects you to follow the rules and naming conventions described in this section when adding entries to the following fields:

Description   The name of the policy or monitor whose conditions you want to set up or modify, for example; **OSSPI-MWA_Cpu_load_1.1**

Threshold   Enter the value used to compare with *STATUS* in order to determine
                     whether or not to generate an alarm for the monitored object specified in
                     the Description field of the Threshold Monitor window, as described
                     in "Configuring OV Performance and GlancePlus" on page 78. Note that
                     the thresholds defined in the conditions must appear in the list from first
                     to last in *decreasing* order, with the last condition set to 0 (zero).

Reset   The value zero (**0**)

Duration   Enter the polling interval to be used by OV Performance or GlancePlus to
                     check the *STATUS* of the monitored object. This value must be the same
                     for *all* conditions associated with a single threshold monitor.

Message Text   Use this field to specify the text of the alarm message that is generated
                     and sent to the OVO Message Browser if a threshold is crossed. No OVO
                     variables may be used. Note also that the string "$$" in the Message
                     Text field will be replaced by the value of *STATUS*, which is computed by
                     the threshold-monitor rules you define, as described in "Monitor
                     Program or MIB ID" on page 79.

Severity   For all conditions except the *last* condition, you can select any severity
                     value from the drop-down menu *except* Normal or Unchanged. However,
                     the *last* condition you define for a performance-related threshold monitor
                     is used to determine the message OV Performance or GlancePlus sends
                     as an end-of-alarm message and *must* have the severity Normal.

Figure 4-2   The Condition Number Window
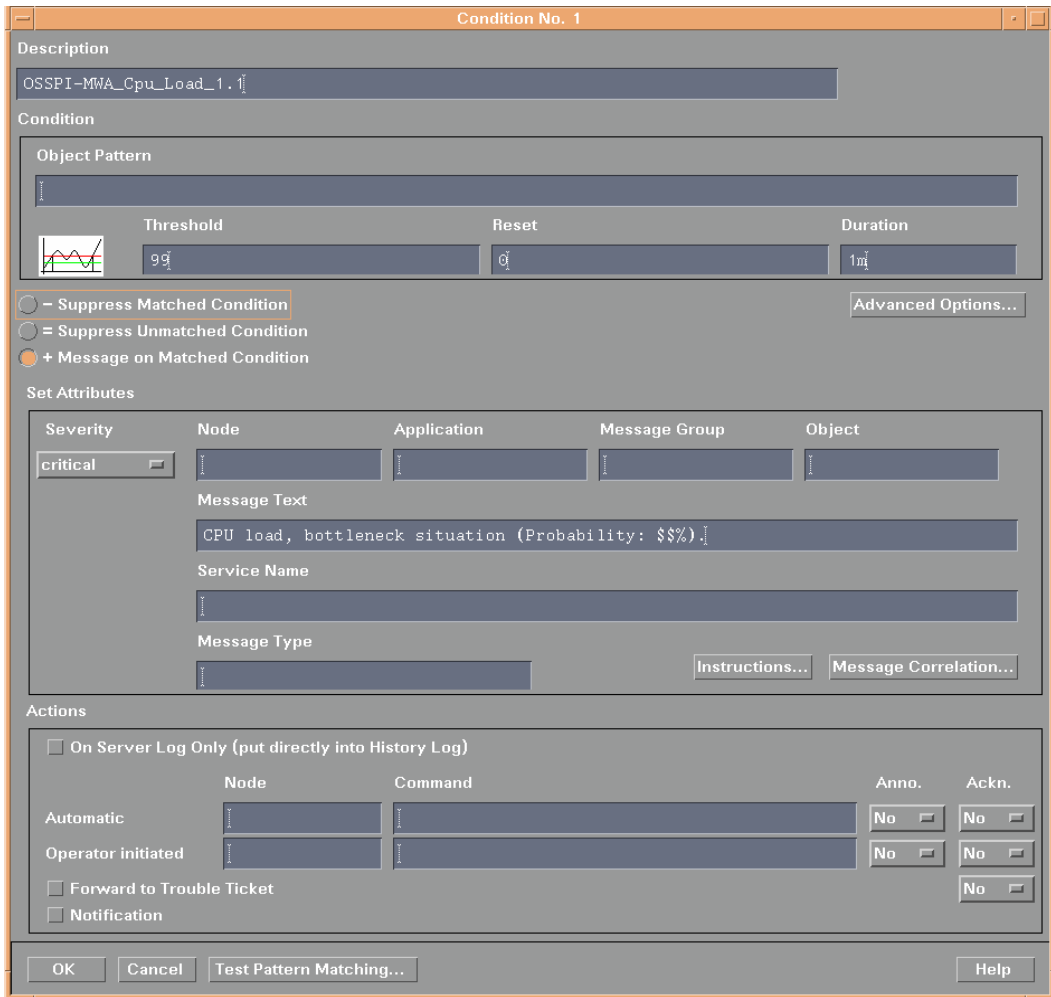
Configuring the OVO Embedded Performance Component

The OSSPI allows you to use the OVO GUI to set up new (or modify existing) threshold monitors for the OVO Embedded Performance Component (Coda). You will need to use the Add Threshold Monitor window or the Modify Threshold Monitor window illustrated in

Figure 4-3. When adding or modifying monitor policies to configure OVO Embedded Performance Component, the OSSPI expects you to follow the rules and naming conventions described in this section.

Figure 4-3   The Modify Threshold Monitor Window
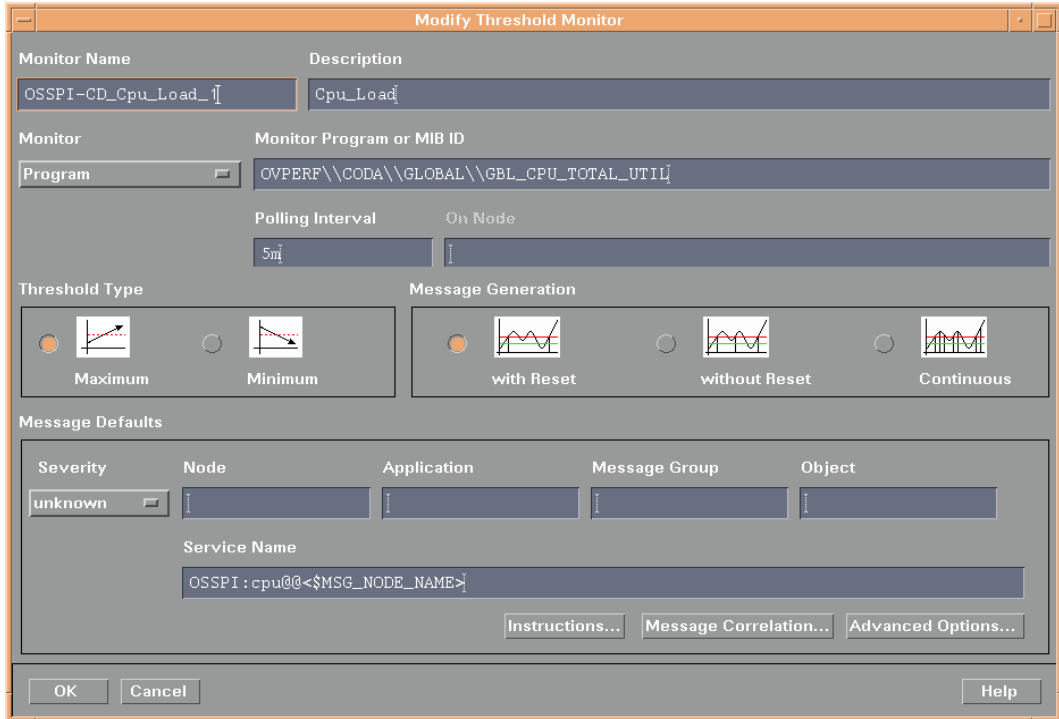
The information that follows helps you through the configuration process by describing what information needs to be entered and, where appropriate, in what format for each of the required fields in the Add Threshold Monitor or the Modify Threshold Monitor window.

Monitor Name   A string that must *begin* with one of the following prefixes:

OSSPI-CODA_   for all Coda monitors

Description   The name of the object to be monitored by Coda, for example: CPU_Load

Monitor Program or MIB ID   Select Program from the pull-down menu and, in the Monitor Program or MIB ID field, enter a string (without spaces) using the order and syntax specified in the following example, including the back-slashes (\):

\\OVPERF\\CODA\\<*OBJECT_TYPE*>\\<*METRIC*>

OVPERF	this is the key for the OV performance component
CODA	this is the datasource for the OVPERF key
OBJECT_TYPE	replace with the type of object you want the OSSPI to use, for example: GLOBAL[1]
METRIC	replace with the short form of the metric source for <*OBJECT_TYPE*>, for example: GBL_CPU_TOTAL_UTIL.

Polling Interval The polling interval for the OVO Embedded Performance Component cannot be configured from the OVO management server. Enter: **5m**

Threshold Type Monitor *maximum* thresholds. The thresholds are defined in the monitor conditions as described in "Using Threshold-Monitor Conditions to Set up the OVO Embedded Performance Component" on page 84.

Message Generation Set to: With Reset

Service Name Optional field: enter the name of the service (and sub-service) to which the message is to be assigned—in the following format:

OSSPI:**<*service_name*>@@<$MSG_NODE_NAME>**

service_name	is the name of the OSSPI *sub-service*, for example: **cpu**
MSG_NODE_NAME	is a variable resolved by OVO to the name of the managed node that generated the message

Using Threshold-Monitor Conditions to Set up the OVO Embedded Performance Component

If you are using the OVO Condition No. # window illustrated in Figure 4-2 on page 82 to set up new (or modify existing) conditions for OSSPI threshold monitors, remember to set the Message on Matched Condition option. Note also that OVO expects you to follow the rules

---

1. See the OVO documentation for information about OVO Embedded Performance Component metrics.

and naming conventions described in this section when adding entries to the fields described in this section and illustrated in Figure 4-4 on page 86.

Description   Enter the name of the OSSPI monitor for the OVO Embedded Performance Component that you want to set up or modify, for example:

`OSSPI-CODA_Cpu_Load_1`

Threshold   Enter the value used to compare with *STATUS* in order to determine whether or not to generate an alarm for the monitored object (e.g. `Cpu_Load`) specified in the Description field of the Threshold Monitor window, as described in "Configuring the OVO Embedded Performance Component" on page 82. Note that the thresholds defined in the conditions must appear in the condition list from first to last in *decreasing* order, with the last condition set to 0 (zero).

Reset   The value zero (**0**)

Duration   Enter the polling interval to be used by the OVO Embedded Performance Component to check the *STATUS* of the monitored object. This value must be the same for *all* conditions associated with a single threshold monitor.

Message Text   Use this field to specify the text of the alarm message that is generated and sent to the OVO Message Browser if a threshold is crossed. Note that you *cannot* use OVO variables in this field.

Severity   For all conditions except the *last* condition, you can select any severity value from the drop-down menu *except* Normal or Unchanged. However, the *last* condition you define for a performance-related threshold monitor is used to determine the message which is sent as an end-of-alarm message and *must* have the severity Normal.

Figure 4-4 **The Condition Number Window**
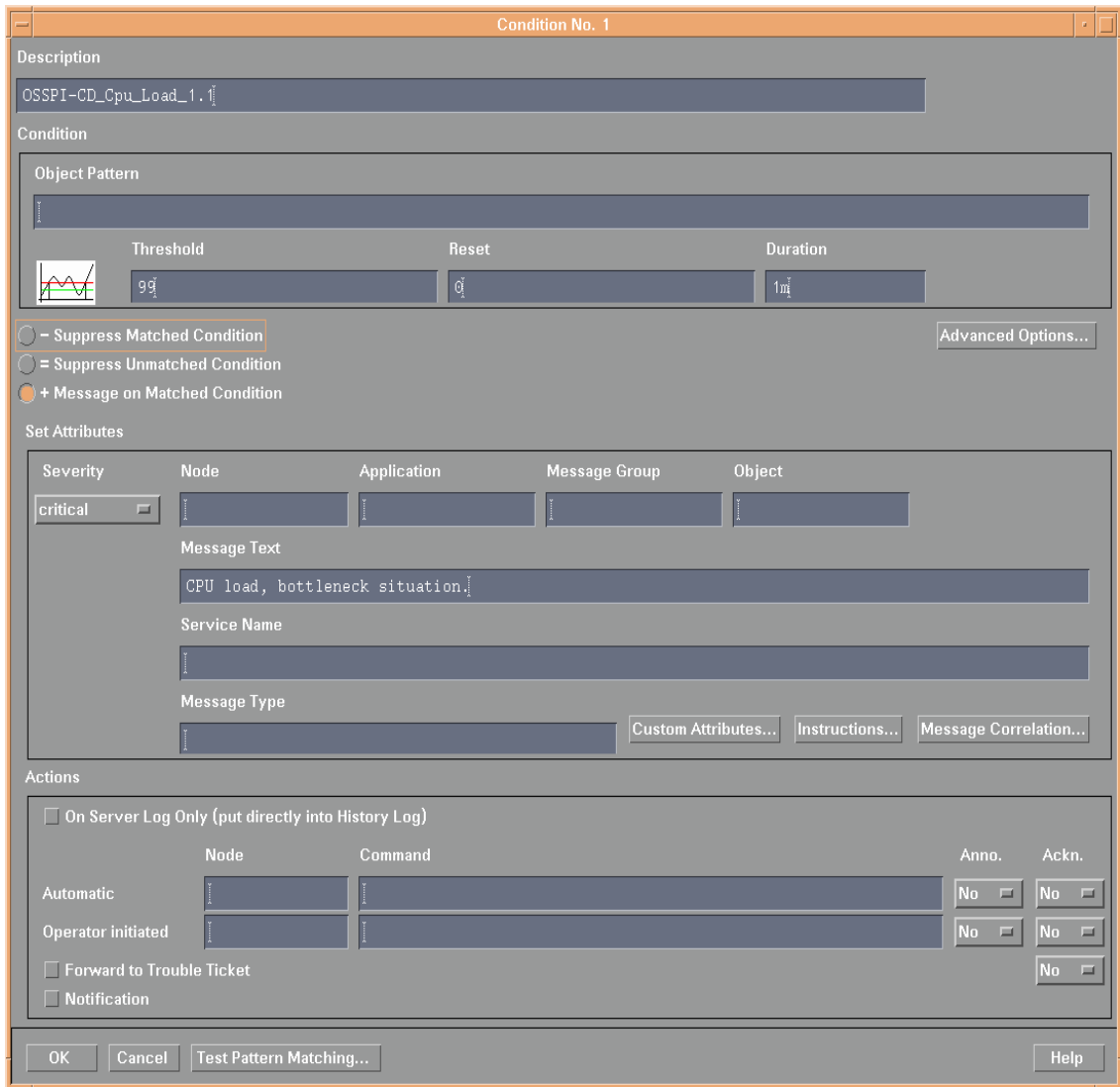
Auto-Acknowledging OV Performance Messages and OV EPC Messages

By default, OV Performance and OV EPC messages are auto-acknowledged in the following manner:

New Message	Acknowledges				
	Critical	Major	Minor	Warning	Normal
Critical	X	X	X	X	X
Major	X	X	X	X	X
Warning	X	X	X	X	X
Normal	X	X	X	X	X

The pattern of acknowledgement follows the state-based browser concept where in only current state or severity of the monitored objects are visible in the browser message. For more information about the state-based browser concept, see the *HP OpenView ServiceNavigator Concepts and Configuration Guide*.

For example, a critical message is sent from node 1 to the OpenView management server about CPU utilization. When file system utilization reaches 89% on CPU on node 1, a warning message is sent. This warning message auto-acknowledges the previously sent critical message and all other (major, minor, warning or normal) messages that node 1 sent about CPU utilization.

Monitoring File Systems with the OSSPI

The generic file-system monitor provided with the Smart Plug-in for UNIX Operating Systems tracks the use of all mounted and supported file systems on any specified host. The file-system monitor is extremely flexible in order to be able to take into account the wide range of possible circumstances under which it can be used. The OSSPI file-system monitor can:

- obtain mount information from system files for all normally mounted disks (local disks as well as remotely mounted filesystems)

- restrict information to listed filesystems (command line) and/or file-system types

- report if file system(s) are overused both in terms of space and/or inodes. Any limits must be specified in a configuration file or in the policy itself (in the case of opcmon(1) calls)

NOTE   The Filesystem policy in each OS-specific policy group references the same *base* policy, namely; OSSPI-NP_Filesystem_1. Thus, if you make any changes in a file-system policy, the changes will appear in all the other file-system policies as well. If you have any requirements that are specific to a particular operating system's file-system monitor, create a monitor policy using OSSPI-NP_Filesystem_1 as a model.

In the Monitor Program or MIB ID field of the Add/Modify Threshold Monitor window, the file-system monitor accepts any one of the following parameters:

-t=<fs_type>   the *type* of filesystem to be monitored, for example: **-t = nfs**

<fs_name>   the *name* of the filesystem to be monitored, for example: **/var**

If no file-system parameters are specified explicitly, the file-system monitor uses the contents of the configuration file generated by the OSSPI and located in the following directory on the managed node, /var/opt/OV/bin/OpC/monitor/osspi_fsmon.cfg (/var/lpp/OV/osspi/conf/osspi_fsmon.cfg on AIX).

After discovery is run, the file system entries are listed in osspi_fsmon.cfg. All the file systems listed in this file are monitored for the specified default thresholds of space and inode utilization.

If you want to selectively monitor file systems, you can create the configurations files, /var/opt/OV/osspi/conf/osspi_global_fs.cfg, and /var/opt/OV/osspi/conf/osspi_local_fs.cfg, in the format similar to osspi_fsmon.cfg. Entries for global file systems are listed in the osspi_global_fs.cfg file. You can set thresholds in this file to globally monitor any file system. To set monitoring thresholds for file systems on specific nodes, edit the osspi_local_fs.cfg file.

NOTE   Do not edit the file osspi_fsmon.cfg, which lists the discovered file systems. Manually editing this file might cause file system monitoring to fail.

While monitoring file systems, precedence is given to the thresholds set in the configuration file, osspi_local_fs.cfg. These thresholds override the values set in osspi_global_fs.cfg, which in turn take precedence over the default thresholds in osspi_fsmon.cfg.

The contents of the file-system monitor's configuration file must match the syntax rules listed below and illustrated in Example 4-1 on page 90:

- the file-system's mount point, for example; /var

- thresholds for disk/inode usage that reflect the following OVO severity levels (warning, minor, major, critical, etc.). The threshold values for disk and inode are separated by a forward slash, for example; 85/90

- the time at which the file-system monitor should run using the 24-hour clock, for example; 18-23 (for eight to eleven o'clock in the evening)

- the day (or days) of the week on which the monitor runs

- optionally, a value (yes/no) to indicate whether or not auto-*extend* is true

The OSSPI discovery process writes the set of mounted file systems to a default configuration file. These file systems are given pre-defined thresholds for disk space and inode usage (separated by a forward slash) for the severity statuses warning, minor, major, and critical in increasing order of severity as illustrated in Example 4-1.

Example 4-1   **Sample Configuration File for the OSSPI File System Monitor**

```
* The lines that start with an astrisk '*' are comments describing the format of this file.

*Each entry in the file represents a file system to be monitored. By default, all mounted file systems are listed

*Each line contains at least five columns; the first identifying the file system,
*the second to fifth specifying the thresholds for monitoring. The first column is
*separated from the second column by a TAB character. The rest of the columns are
*separated by the Comma character. After these five mandatory columns, there can
*be two optional columns. The first to specify the time period of the day to report
*exceptions, and the second to list the days of the week to report exceptions on.
*The optional column 1 is of the format a-b, where a and b can be any values from 0 to 24.
*The second optional column takes the format 0:1:2:3:4:5:6, where 0 represents Sunday and
*so on through to 6 which represents Saturday.

*The permitted formats of each column, and the meaning of each representation is given below:

*Column 1      mount point of filesystem (or "!default")

*Column 2-5    percentage limits for severity levels "warning", "minor", "major",
*              and "critical" (in that order).
*
*              Possible values:
*
*              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

*Opt Col 1     time of day to report exceptions, a-b
*              If a<b, it represents a day time interval, while a>b represents a
*              night time interval

*Opt Col 2     colon separated list of days in the week on which to report exceptions
*              Where 0 is Sunday, and 6 is the Saturday following that
*
*Sample entry:
*              /var    80,85,90,95,0-24,0:1:2:3:4:5:6
*
*              /usr    80/30,85/40,90,95,0-24,0:1:2:3:4:5:6
*
*TO CUSTOMIZE THRESHOLDS:

*Create a file osspi_local_fsmon.cfg in the osspi/conf directory
*using OSSPI's FILESYSTEM APPLICATIONS
*------------------------------------------------------------------------------
*
/      80/30,85/40,90/50,95/55
/usr   80/20,85/30,90/40,95/50,1-15,0:3:4
/opt   80,85,90,95
/var   80,85,90,95
/tmp   70/60,80/75,85,90
```

OSSPI also integrates with performance tools such as Coda, HP OVPA, and HP GlancePlus, for monitoring file systems. OSSPI has four types of file system monitoring template groups, Coda, MeasureWare, Glance, and NoPerf.

The Coda group of templates do not need the configuration files for monitoring file systems, they can be used without running Discovery on the nodes. Also, the threshold levels are the same for all the file systems being monitored. The Coda group of templates do not monitor the inode utilization, and cannot set the date and time for monitoring.

The other template groups monitor file systems based on thresholds set in the configuration file generated by OSSPI after Discovery has run.

Service IDs

The OSSPI file-system monitor automatically attaches service IDs to the `opcmon` and `opcmsg` calls it sends. The service ID sent by the OSSPI takes the following form:

`OSSPI:fs:<fsname>@@<hostname>`

where:

fsname	is the name of the file system you want the OSSPI file-system monitor to check
hostname	is the fully qualified *domain* name or, for an MC/SG package, the fully qualified *package* name of the host on which the file-system is mounted.

Monitoring Processes with the OSSPI

The processes and process groups which you want to monitor with the OSSPI have to be defined in a specific configuration file, the format and contents of which are described in detail in this section. The process monitor can be executed either by means of this configuration file or on the command line with specific parameters.

Using Procmon.cfg

A default configuration file located on the managed node, `/var/opt/OV/osspi/conf/procmon.cfg`, is generated when `Discovery` application is run on the node. However, individual entries in the configuration file (including even single processes in a process group) can be overwritten at any time or extended by means of an additional, local configuration file, `procmon_local.cfg`.

NOTE   Use the `Proc edit global` and `Proc edit local` applications in the `OSSPI Process Monitoring` application group to edit the process monitor configuration file.

Figure 4-5   **Default Policy created by OSSPI to monitor ntp Processes**
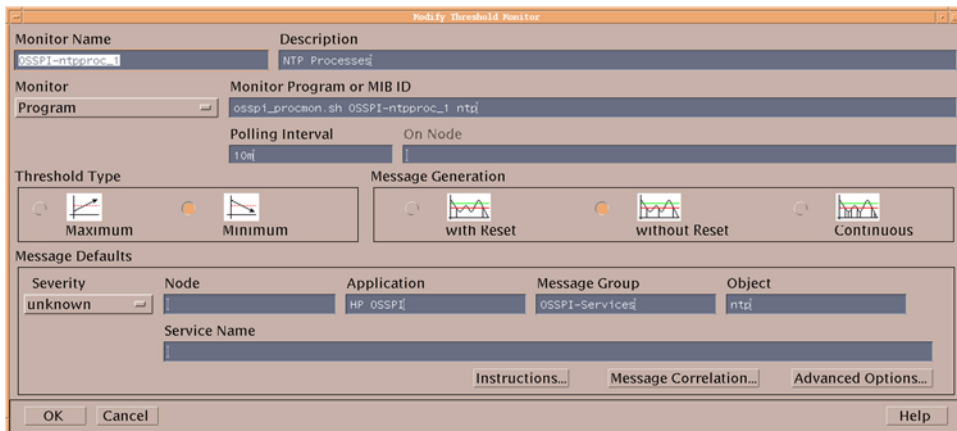
Example 4-2   **Example of the OSSPI Process-Monitor Configuration File**

```
#Process-Monitor Configuration file

#Col1                    Col2    Col3    Col4    Col5
[ntp]
ntpd                      *        1
@start=/etc/init.d/ntpd stop;/etc/init.d/ntpd start

[cron]
cron                      *        1
@start=/etc/init.d/crond stop; /etc/init.d/crond start

[syslog]
syslogd                          -m 0    1
klogd                    -2       1
@start=/etc/init.d/syslog stop; /etc/init.d/syslog start

[snmp]
snmpd                     *       6-20    1,2,3,4,5
@start=/etc/init.d/snmpd stop; /etc/init.d/snmpd start

[portmap]
portmap                   *       6-20    0,1,2,3,4,5,6    1-
@start=/etc/init.d/portmap stop; /etc/init.d/portmap start

[mail]
sendmail                  *       1-
@start=/etc/init.d/sendmail stop; /etc/init.d/sendmail start

[print]
lpd                       *        1
@start=/etc/init.d/lpd stop; /etc/init.d/lpd start

[SAPprocs-1]
proc1                     *        3
proc2                     *        3
@user=user1,user2,user3

[SAPprocs-2]
proc1                     *        1
@user=scott,tiger
```

Figure 4-6   **Example to Monitor SAP Process Groups using Regex Specification for the Section Names**
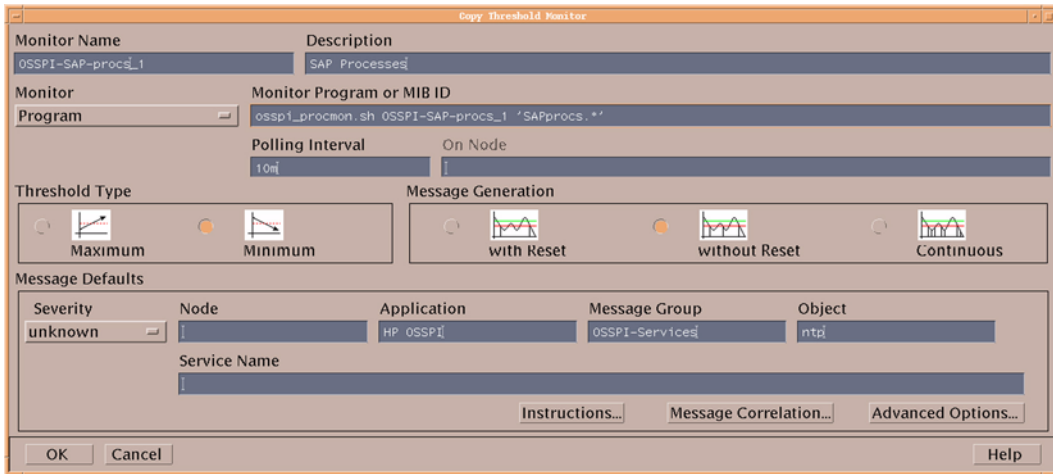
NOTE   In `procmon.cfg`, `procmon_local.cfg`, blank lines are used as separators between process group sections. Therefore, do not add blank lines within a process group section.

Use `OSSPI's Proc*` applications to edit `procmon.cfg` and `procmon_local.cfg.` Avoid editing the files manually.

Example 4-2 on page 93 shows how the contents of the process configuration file generated by the OSSPI `Discovery` application are divided into blocks representing process groups or MC/ServiceGuard packages. The name of the process group or MC/ServiceGuard package must be enclosed in square brackets, for example; [nfssvr] or [*Package_Name*]. This name is used in the OSSPI service tree. Note that the *actual* name of the MC/SG package [orapkg1] must *also* be present—in square brackets and separated from [*Package_Name*] by spaces or **TAB** characters.

The individual processes and MC/SG packages which you want the OSSPI to monitor must be included in the configuration file on a single line (and in columns separated by at least one **TAB** character) according to the syntax rules illustrated in Example 4-2 and Table 4-1 and described in detail in the sections that follow.

Table 4-1   **The Contents and Format of the procmon File**

Column 1	Column 2	Column 3	Column 4	Column 5	Report Type
Name					opcmon
Name	*arguments*				opcmon
Name	*arguments*	*bounds*			opcmsg
Name	*arguments*	*time*	*day of week*		opcmon
Name	*arguments*	*time*	*day of week*	*bounds*	opcmsg
Special					opcmsg
Special	*arguments*	*time*			opcmsg
Special	*arguments*	*time*	*day of week*		opcmsg
Special (@start=<cmd>)	*[<username >[,....]]*				

The OSSPI process monitor parses its configuration file every time it starts in order to detect any changes and, if present, put them into effect immediately. The monitor reports:

- any syntax errors in the configuration file

- which program(s) of a group and which group(s) are affected

- if instance limits are out of bounds

- if instance limits are out of bounds for particular users and if @ user specification is present for the process group in procmon.cfg

If *bounds* are specified, missing processes are reported via opcmsg calls. If *bounds* are *not* present, an opcmon call is executed with an object name constructed according to the following format:

<process_group_name>~<process_name> (user name not specified)

<process_group_name>~<process_name>~<user_name> (user name specified)

where *process_name* can also be the process pid or the file name (containing process names or pids) from column one of the procmon file.

Name/Special   Contains the name of the process to be monitored or a special command. The process name can be entered explicitly or derived in any one of the following ways:

<process_name>

the name of the process as it appears in the process table

@pid=*<pid_number>*

where *pid_number* is the process id number

@file=/etc/*<pidfile>*

where *pidfile* is the name of a file containing the pid(s) line by line

@exec=/opt/SW/*<getpid>*

where *getpid* is the name of a file which, when executed, writes the process id(s) to STDOUT

@start=/opt/*<exec>*

where *<exec>* is the name of a file to be executed (using any arguments in column two of Table 4-1) if a defined condition is not met. One @start token per [block] per user

@user=*[<name>,...]*   where *<name>* is the name of a user to be executed (using any arguments in column one of Table 4-1)

Arguments   You can use arguments to distinguish between multiple processes running in parallel. If no arguments are present, an asterisk (*) is required.

Time   The time period (using the 24-hour clock) in which a failure must be reported if it occurs, for example;

6-22   6 AM to 10 PM

22-6   10 PM to 6 AM the following morning

Day of Week   A list of numbers representing the days of the week (separated by commas) on which failures should be reported, where:

0,1,2,3,4,5,6   Sunday, Mon., Tues., Wed., Thurs., Fri., Saturday

Bounds   The number of instances of *named* processes in any one of the following formats:

n   an *exact* number, n

-n   a *maximum* of n

n-   a *minimum* of n

m-n   a *range*: m to n process instances

Using Command Line

The process *name* or any *special* terms permitted in column 1 (one) of procmon configuration file are also permitted in the Monitor Program or MIB ID field of the Add/Modify Threshold window, but must take the following formats:

program=<*program_name*> [arg=<*arg*>] [*user=<name>[,...]*]

pid=<*pid*>

file=<*pidfile*>

exec=<*exec_file*>

Figure 4-7   Example for Monitoring init Process
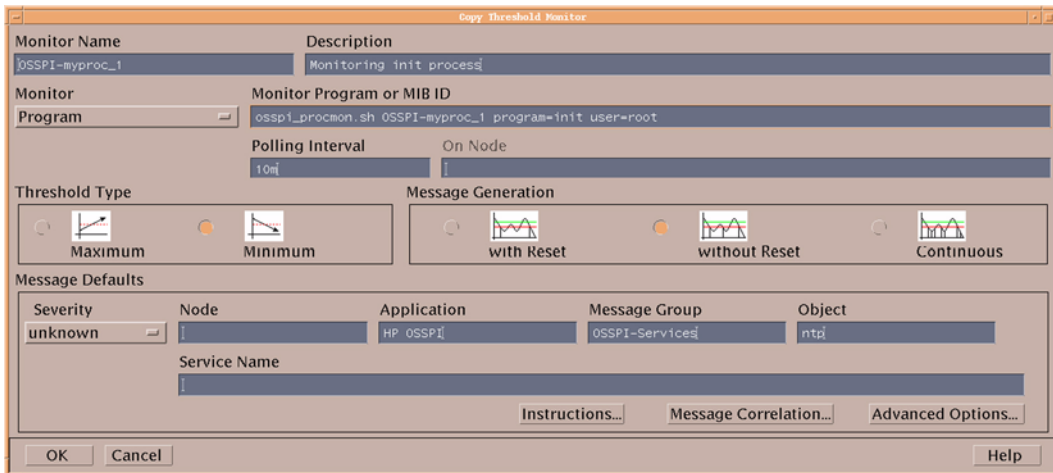
Service IDs

The OSSPI process monitor automatically attaches service IDs to the
opcmon and opcmsg calls it sends. The service ID sent by the OSSPI
takes the following form:

OSSPI:os:svc:<*sectionname*>@@<*hostname*>

where:

sectionname	is the name of the section to be processed, that is; the name in the procmon file enclosed in square brackets, for example; [dns] or [*Package_Name*], as illustrated in Example 4-2 on page 93.
hostname	is the fully qualified *domain* name or, the fully qualified DNS resolvable hostname for the MC/SG package, where the processes are running.
	Note that if the MC/SG package is *not* in a DNS domain, the package information defined in /etc/resolv.conf is appended to the package name.
	If /etc/resolv.conf is not available, the fully qualified domain for the MC/SG package name takes the following form:
	<*Name_of_Package*>.hp-osspi

Service Discovery

The OSSPI discovery process is an OVO application which is installed by the OSSPI and runs on the OVO management server. The service graph generated by the OSSPI is a snap shot of the services on the managed nodes at the time at which the OSSPI Discovery application is run. Changes to the service configuration of a managed node do not appear automatically in the OSSPI service tree, the Discovery application has to be run again in order to update the contents of the Operating System SPI service tree in the OV Service Navigator. However, you can use OVO to configure an operator-initiated action which uses the opcservice(1) command to inform you as soon as the OSSPI's service configuration file has been modified.

The mechanism the OSSPI uses to gather the service information displayed in Figure 2-9 on page 57 is a simple one: a discovery *server* on the OVO management server uses the list of managed nodes as parameters to trigger a discovery *client* on each of the OVO managed nodes listed. The discovery clients on the various OVO managed nodes use **discovery modules** that are installed during the installation of the OSSPI agent software (or indeed by any other OVO SPI) to gather information about the services present on the managed nodes. The discovery server writes error messages to the following file: /var/opt/OV/log/SPISvcDisc/discovery_error.log. For more information about error logs, see ""Error Logging"" on page 134.

The service configuration files compiled by the discovery process are written to the directory $OSSPI_SVR_VAR_CFG_DIR on the management server using the following file-naming conventions:

/var/opt/OV/SPISvcDisc/conf/UNIXOSSPI/UNIXOSSPISvcDisc_${*NODENAME*}.xml

where *NODENAME* is the name of the node on which the discovery application has been run. For more information about how the format of the discovery file changes according to the version of OVO that is installed, see "The Discovery Modules" on page 100.

The Discovery Modules

The discovery modules used by the OSSPI reside together with the other SPI components on the OVO managed node. Once started by the discovery server, the discovery client locates and reads the **Module Registry** (`osspi_discreg.cfg`) on the managed node in order to find out which OS services have to be discovered and which modules are responsible for each service. On OVO 8.0 systems, the file `osspi_discreg.cfg` can be found in the directory, `/var/opt/OV/bin/Instrumentation`, and on OVO 7.x systems, it can be found at `/var/opt/OV/bin/OpC/cmd`.

The information that is discovered by the discovery modules is written to service-configuration files in a format that can be used by the OV Service Navigator to display the services as a tree in the OV Service Navigator GUI. The default format required for is XML.

Each discovery module is responsible for retrieving information from *one* service component. The module stores its findings in a dedicated configuration file. These files are detailed in the following lists:

HP-UX, Linux, Solaris, and Tru64

Hard Disk:	`/var/opt/OV/osspi/conf/harddisk.cfg`
Network IF:	`/var/opt/OV/osspi/conf/netif.cfg`
File System:	`/var/opt/OV/osspi/conf/osspi_fsmon.cfg`
Processes:	`/var/opt/OV/osspi/conf/procmon.cfg`
Disk Defects:[1]	`/var/opt/OV/osspi/conf/osspi_defect.cfg.long`
	`/var/opt/OV/osspi/conf/osspi_defect.cfg.short`

Solstice DiskSuite: `/var/opt/OV/osspi/conf/sds.cfg`

Veritas Volume Manager:[2]

`/var/opt/OV/osspi/conf/osspi_veritas.cfg`

AIX

Hard Disk:	`/var/lpp/OV/osspi/conf/harddisk.cfg`
Network IF:	`/var/lpp/OV/osspi/conf/netif.cfg`
File System:	`/var/lpp/OV/osspi/conf/osspi_fsmon.cfg`

---

1. Disk defects are not supported on Linux, Tru64 UNIX, or AIX operating systems.
2. The Veritas Volume Manager does not discover unassociated objects and rvg volumes.

Processes: `/var/lpp/OV/osspi/conf/procmon.cfg`

The discovery modules are started successively by the discovery client, which logs error messages in the file, `/var/opt/OV/SPISvcDisc/log/discerr.log`. For more information about problems and errors, see Chapter 6, "Troubleshooting the OSSPI," on page 133.

Monitoring OS-Service Configuration Files

The OSSPI_<*Operating System*>_cfgmon policies provide a simple and convenient way to modify the operating-system configuration files which you want to monitor with the OSSPI.

There is a policy for each of the following operating systems:

- OSSPI_AIX_cfgmon for AIX

- OSSPI_HP-UX_cfgmon for HP-UX

- OSSPI_Linux_cfgmon for Linux

- OSSPI_SOL_cfgmon for Solaris

- OSSPI_Tru64_cfgmon for Tru64

The OSSPI monitors the following HP-UX files for changes:

- /etc/inetd.conf

- /etc/inittab

- /etc/fstab

- /etc/profile

- /etc/passwd

- /var/spool

- /var/adm/inetd.sec

NOTE   The list of files monitored by default on IBM AIX, Linux, and Sun Solaris is similar to the HP-UX list above but adjusted to reflect the platform-specific paths and configuration files.

If you feel that the demands and requirements of your particular environment are not adequately covered by the configuration files specified in the default list, you can expand or reduce the list by simply adding to (or deleting from) it, as necessary. To modify the contents of the default list in the OSSPI_HPUX_cfgmon policy, make a copy of the original policy and modify the list of OS configuration files in the *new* file as follows:

1. Start the OVO GUI and open the Message Source Template window

2. Locate and select the OSSPI_HPUX_cfgmon policy

3. Click the [Modify...] button to display the Modify Threshold Monitor window illustrated in Figure 4-1 on page 78

4. Save the changes you have made and redistribute the policies to the appropriate managed nodes

Figure 4-8   Modifying OS Configuration Files
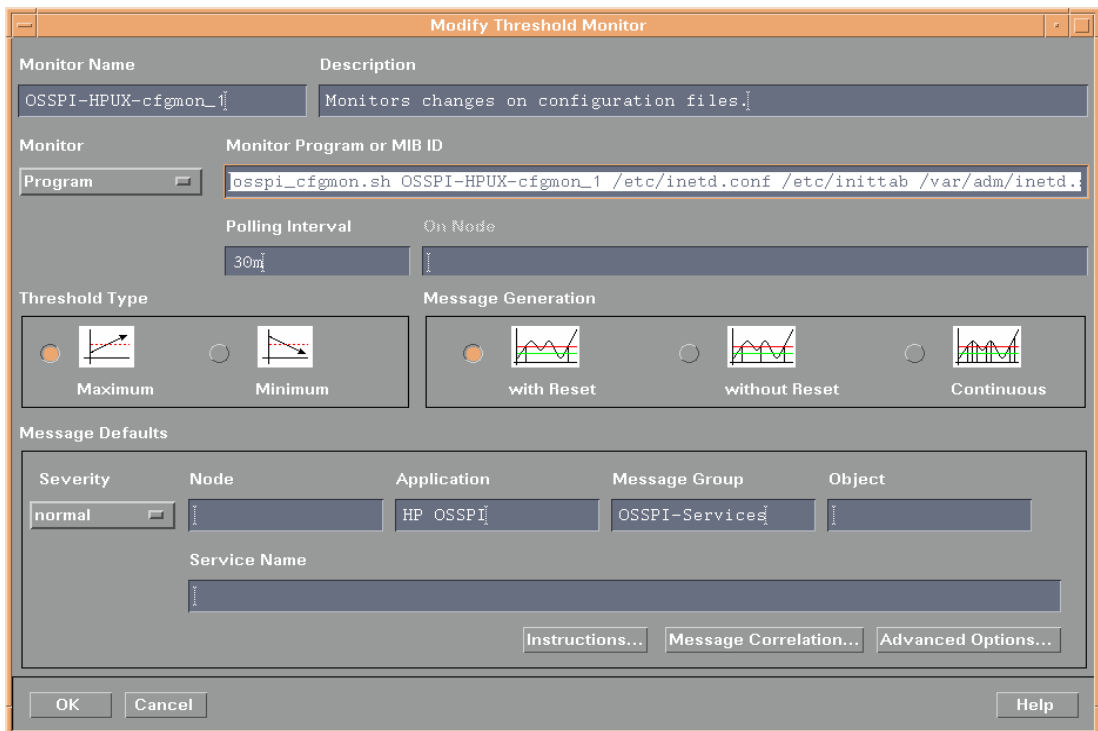
Configuring Standard Policies

OSSPI sets default threshold values and polling intervals for all the monitor policies it provides. This section describes how to use the OVO GUI to modify these default values in the existing OSSPI policies or set up thresholds and polling intervals in new policies to suit the particular requirements of your environment. Note that if you modify existing or create new policies, you have to re-distribute the policies to the managed nodes in order to apply the modifications. The two areas of a standard OSSPI policy which you are most likely to want to modify or define from new are:

- Thresholds
- Polling Intervals

Modifying Thresholds

The default thresholds defined in the OSSPI monitor policies strike a sensible balance between the need to know about critical problems in your environment and network overheads. If the default values do not suit the specific requirements of your particular environment, you can change the type of threshold as well as the defined threshold values quickly and easily by using the `Modify Threshold Monitor` window illustrated in Figure 4-1 on page 78. To open the `Modify Threshold Monitor` window:

1. Open the `Message Source Templates` window

2. Locate the policy you want to modify by expanding the appropriate policy groups

3. If you want to modify the *type* of threshold (maximum or minimum), select the policy you want to modify and click the `[Modify...]` button. Change the threshold type in the `Modify Threshold Monitor` window which appears.

4. If you want to change the threshold *value*, select the policy you want to modify and click the `[Conditions...]` button. The `Message and Suppress Conditions` window appears displaying a list of conditions associated with the policy.

Select a condition and click the [Modify...] button. Change the
threshold value defined in the Threshold field.

5. Click [OK] to save the changes.

6. Redistribute the policies to the managed nodes.

Modifying Threshold Polling Intervals

The default polling intervals defined in the OSSPI's monitor policies are
designed to keep you informed about critical problems in your
environment, in a timely fashion. You can change the polling intervals
easily by modifying the value in the Polling Interval field of the
Modify Threshold Monitor window. To open the Modify Threshold
Monitor window:

1. Open the Message Source Templates window

2. Locate the policy you want to modify by expanding the appropriate
   policy groups

3. Select the policy you want to modify and click the [Modify...]
   button. The Modify Threshold Monitor window appears.

4. Enter a new value in the Polling Interval field.

5. Click [OK] to save the changes.

6. Redistribute the policies to the managed nodes.

Modifying Polling Intervals for Monitoring File System Utilization (GlancePlus and OVPA)

The OSSPI allows you to modify the default polling intervals for a number of GlancePlus and OV Performance policies by including in the file `/var/opt/OV/osspi/conf/osspi.cfg` one of the variables listed in Table 4-2 and specifying a new value for the variable which is different to the default values indicated.

Note that polling intervals for the file-system policies need to be defined in `osspi.cfg` if they are different from the *default* settings. You cannot set conditions in the file-system policies themselves.

Table 4-2   **Keywords in the osspi.conf File**

Keyword	Description	Default Polling Interval
GP_RUN_INTERVAL	interval (in seconds) for GlancePlus to check for and, if necessary, update metrics	30s
GP_FS_CHECK_INTERVAL	string containing an interval specification for sampling of the data gathered by GlancePlus concerning the utilization of filesystem space	1m [a]
MW_FS_CHECK_INTERVAL	string containing an interval specification for sampling of the data gathered by OV Performance concerning the utilization of filesystem space	5m [a]

a. Note that the scope for defining this interval could be limited by the tool itself. Please check the product-specific documentation for details.

Configuring OSSPI to Run as Alternative User

OVO processes normally run under user root on UNIX systems. The root/administrative privileges enable the processes to:

- access files that are normally restricted to privileged access only

- allow a switch user for application specific access rights

- directly access operating system resources such as log files and configuration files

- start application or operating system specific commands

OSSPI processes function in a similar way. But there may be systems within IT environments where it is necessary to limit the number of processes that have full root permissions to a small, well defined and tested group. In addition, you may want to identify the precise processes that manipulate critical system resources. This is not possible if many applications are running under the privileged user.

Configuring OSSPI to run under a user other than root is supported on HTTPS agents with OVO 8.0. You can do this using the ovswitchuser tool. For information on supported agent platforms, refer to the *HP OpenView Smart Plug-ins for OVO/UNIX Release Notes*.

Prior to executing the ovswitchuser.sh script, you must create two directories /var/opt/OV/osspi and /var/opt/OV/SPISvcDisc. Execute the script ovcreatedirs.sh to create the two directories with appropriate permissions. Refer to the *HP OpenView Smart Plug-ins for OVO/UNIX Release Notes* for more information on the script, ovcreatedirs.sh. If the directories already exist, make sure the directory permissions are set to 775, after doing a switchuser.

Refer to the manual, *HP OpenView Operations HTTPS Agent Concepts and Configuration Guide*, for details of running the ovswitchuser tool.

See Appendix B, "OSSPI Components Without Alternative User Support," for the list of OSSPI components that are not supported to run with non-root user privileges.

5 Monitoring Sun Clusters

The SPI for UNIX operating systems can be used to discover and monitor the Sun cluster setups that are a part of your system.

The SPI for UNIX operating systems discovers and monitors the cluster nodes, the shared devices, resource groups, quorum devices, NAFO groups, and interconnects, that make up the cluster.

The discovery module first discovers these components and then the OSSPI monitors the changes to these components.

The following sections explain how the discovery process works and how these components are monitored by OSSPI.

Discovering Sun Cluster Components

The Sun cluster components are also discovered when OSSPI discovery is run to discover all managed nodes. The discovery process creates a configuration file containing a snapshot of the cluster configuration at that instant. All the discovered Sun cluster components are listed in the configuration file, osspi_sc.cfg. The configuration file is updated periodically.

NOTE   Do not edit the configuration file, osspi_sc.cfg. Manually editing this file might cause the cluster monitoring component to fail.

Before you run discovery on the Sun cluster nodes, you must perform some tasks on the management server.

Management Server Settings

For the discovery process to run and effectively discover the cluster components, you must complete the following tasks on the management server.

• Add a message only node with the same name as the cluster name.

  This is used to identify the cluster. Create a message only node for each cluster you want to monitor. All monitor messages from the Sun cluster will send messages to the respective message only node. For more information on creating message only nodes, refer to the section on adding virtual nodes in the manual *HP OpenView Operations HTTPS Agent Concepts and Configuration Guide*.

• The name of the message only node must be changed if the cluster name is changed.

  All future messages about the cluster will be lost if the name of the message only node is not changed when the cluster name changes.

• All cluster nodes must be added to the OSSPI-Solaris node group.

• OSSPI-Solaris node group must be added to the OSSPI administrator's responsibility matrix.

Cluster Service Elements and View

After the discovery process is completed successfully, the service navigator is updated with the Cluster element, which along with the OSSPI element appears directly below System Infrastructure. Each Sun Cluster element appears below the top-level Cluster element. The icon label also identifies the cluster by the cluster name. Each cluster is represented by one such icon. The service elements for each cluster component are represented as child elements below this. The cluster service elements appear in the service view as follows.

Figure 5-1   Service View for Sun Cluster
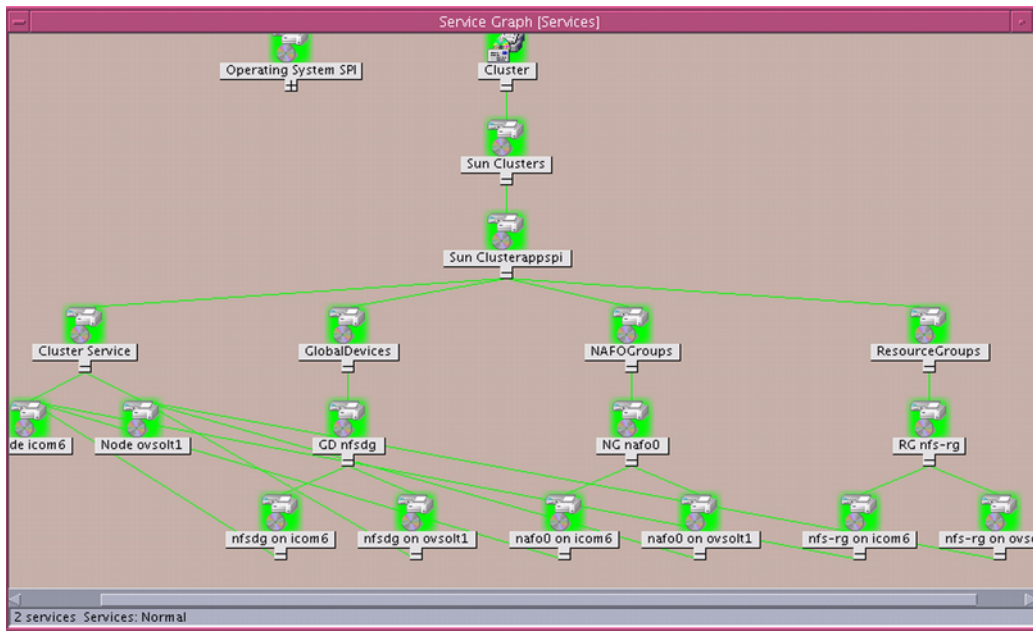
NOTE   Cluster discovery and monitoring has to be done from all the nodes in the cluster. Sun cluster discovery does not occur when the Cluster install or maintenance mode is enabled.

You can see the `Cluster Services`, `Global Devices`, `Resource Groups`, and `NAFO Group` elements in the service view. The cluster nodes appear under `Cluster Services`. The applications to be monitored by OSSPI on the cluster, are grouped under `Resource Groups`.

Monitoring Sun Cluster Components

OSSPI monitors the following components of Sun cluster:

- General Cluster information

- NAFO groups

- Cluster interconnect

- Quorum

- Global devices

- Resource groups, Resources

Monitoring General Cluster Information

Table 5-1 lists the general cluster information monitored by UNIX OS SPI.

Table 5-1   **General Cluster Information**

Cluster Component Monitored	Scenario	Action Taken
Cluster Name	Cluster Name Changes	Sends a Critical message and updates the configurations file. Name of the message only node on the management server must be changed. This text is a part of the message instruction.
Cluster Node list	Cluster Node added or removed	Sends a Normal message and updates the configurations file.
Cluster Node[a]	Cluster Node is down	Sends a Critical message and updates the configurations file

Table 5-1   **General Cluster Information**

Cluster Component Monitored	Scenario	Action Taken
Cluster Node ID	Cluster Node ID changes	Sends a Normal message and updates the configurations file. This message is automatically moved to the history browser.
Cluster Node Private Hostname	Cluster Node Private Hostname Changes	Sends a Normal message and updates the configurations file. This message is automatically moved to the history browser.

a. When a cluster node that was non-functional becomes functional again, a normal message is sent. This normal message acknowledges the previous critical message about the node being non-functional.

Monitoring NAFO Group

Table 5-2 details information regarding monitoring NAFO groups

Table 5-2   **Monitoring NAFO Group**

Cluster Component Monitored	Scenario	Action Taken
NAFO group	NAFO group added or removed	Sends a Normal message and updates the configurations file.
Adapter list in NAFO group	Adapter added to or removed from the list	Sends a Normal message and updates the configurations file.
NAFO group status[a]	Status moves to DOUBT	Sends a Warning message and updates the configurations file.

Table 5-2   **Monitoring NAFO Group**

Cluster Component Monitored	Scenario	Action Taken
NAFO group status[a]	Status moves to DOWN	Sends a Critical message and updates the configurations file.
Active Adapter in the NAFO group[b]	Active Adapter change	Sends a Minor message and updates the configurations file.

a. If a NAFO group that was previously in the DOUBT or DOWN state returns to OK state, a normal message will be sent. This normal message will acknowledge the previous message about the DOUBT or DOWN state.

b. The Sun cluster monitor script updates the OSSPI network interface configuration script (netif.cfg) with the new active adapter. This action will also require osspi_alarm_gp.sh and osspi_alarm_mw.sh to regenerate their respective alarmdef files, if the timestamp of netif.cfg has changed.

Monitoring Cluster Interconnect

Table 5-3 details information on monitoring cluster interconnects.

Table 5-3   **Monitoring Cluster Interconnect**

Cluster Component Monitored	Scenario	Action	Root Cause Analysis (If Applicable)
Cluster Interconnects	Cluster Interconnect Added/Removed	Sends a Normal message and updates the configurations file.	Not Applicable

Table 5-3   **Monitoring Cluster Interconnect**

Cluster Component Monitored	Scenario	Action	Root Cause Analysis (If Applicable)
Cluster Interconnects	Cluster Interconnect Removed	Sends a Warning message and updates the configurations file.	If this removal leaves only one cluster-interconnect originating from this node, warn the administrator about the SPOF scenario.
Cluster Interconnect Status	Only one cluster-interconnect is online and the rest have faulted	Sends a Warning message and updates the configurations file.	This is a potential SPOF scenario
Cluster Interconnect status	Only one cluster-interconnect in waiting state and the rest have faulted.	Sends a Warning message and updates the configurations file.	This is also a potential SPOF scenario when the waiting interconnect comes online
Cluster Interconnect status	Cluster interconnect in Waiting state	Sends a Minor message and updates the configurations file.	Not Applicable

Table 5-3   **Monitoring Cluster Interconnect**

Cluster Component Monitored	Scenario	Action	Root Cause Analysis (If Applicable)
Cluster Interconnect status	Cluster interconnect in Faulted state	Sends a Major message and updates the configurations file.	Message will not be sent if one of the endpoints is a cluster node that is DOWN.
Cluster Interconnect status	All cluster interconnects in Faulted state	No action, this will reported as cluster node DOWN as mentioned above.	Not Applicable

During discovery, if it is found that the Sun cluster setup is a SPOF setup (For example, only one cluster interconnect configured per cluster node), none of the SPOF messages will be sent.

When a cluster interconnect that was in the Faulted state returns back to Path Online state, a Normal message is sent. This message will acknowledge the previous Faulted message.

Monitoring Quorum

Table 5-4 details information on monitoring quorums.

Table 5-4   **Monitoring Quorum**

Cluster component monitored	Scenario	Action
Quorum Devices	Quorum Device Added/Removed	Sends a Normal message and updates the configurations file.

Table 5-4   **Monitoring Quorum**

Cluster component monitored	Scenario	Action
Quorum Device Status	Quorum Device goes offline	Sends a Minor message and updates the configurations file.
Quorum Device Status[a]	Quorum Device goes offline	Sends a Critical message and updates the configurations file.

a. This message also contains an instruction text explaining the possibility of quorum being compromised during cluster formation.

When a Quorum Device that was offline comes back online, a Normal message is sent. This message acknowledges the previous Offline message.

NOTE   Nodes with quorum votes are monitored as cluster nodes and not quorum devices.

Table 5-5 describes changes related to nodes that affect a quorum and the behavior of OSSPI under those conditions.

Table 5-5   **Scenario and Action**

Scenario	Action
When a node is added (it also get a quorum vote)	This will be reported as Node Added as specified earlier.
When a node is moved into maintenance state	This will be reported as Node Status Down as specified earlier.

Monitoring Global Devices

Table 5-6 details information regarding monitoring global devices.

Table 5-6   **Monitoring Global Devices**

Cluster component monitored	Scenario	Action	RootCause Analysis(If Applicable)
Global Devices	Global device Added/Removed	Sends a Normal message and updates the configurations file	Not Applicable
Global Device Status	Status moves to Degraded	Sends a Major message and updates the configurations file	If only one of the cluster nodes in the global devices node list is in UP state.
Global Device Status	Status moves to Degraded	Sends a Minor message and updates the configurations file	If more than one node in the node list is UP.
Global Device Status	Status moves to Offline	Sends a Major message and updates the configurations file.	Not Applicable
Global Device primary	Primary node changes	Sends a Normal message and updates the configurations file.	Not Applicable

When a global device that was in the Degraded or Offline state returns Online, a Normal message is sent. This message acknowledges the previous Degraded or Offline message.

Monitoring Resource Groups, Resources

Table 5-7 details information on monitoring resource groups and resources.

Table 5-7   **Monitoring Resource Groups, Resources**

Cluster Component Monitored	Scenario	Action
Resource Groups	Resource Group Added/Removed	Sends a Normal Message and updates the configurations file.
Resource Group State	State moves to Error_Stop_Failed	Sends a Critical message and updates the configurations file. Message identifies the resource in the resource group that is in Stop Failed state.
Resource Group state	State moves to Online/Offline	Sends a Normal message and updates the configurations file.
Resource Group state (scalable)	Resource Group Online on less than <desired primaries> cluster nodes	Sends a Warning message about possible degradation in performance and updates the configurations file.
Resource Group node list[a]	Only one node in the node list is up	Sends a Warning message, resource group is running in a SPOF mode.

Table 5-7   **Monitoring Resource Groups, Resources**

Cluster Component Monitored	Scenario	Action
Resource State	State moves to Start Failed	Sends a Critical message and updates the configurations file.
Resource State	State moves to Monitor Failed	Sends a Critical message and updates the configurations file.

a. If the resource group when configured, has only one node in its node list, this message will not be sent.

If a resource group that was in the Error_Stop_Failed state returns Online, a Normal message is sent. This message acknowledges the previous Error_Stop_Failed message.

If a resource that was in start failed or monitor failed state returns back online, a normal message is sent. This message acknowledges the previous start failed or monitor failed message.

Application Group: Sun Cluster Applications

The OSSPI application group Sun Cluster Applications contains applications that can be used by OVO users to manage the Sun cluster. Table 5-8 lists the applications present in the Sun Cluster Applications group and provides a brief description.

Table 5-8   **Applications in the Sun Cluster Applications Group**

Application Name	Description
Administer Cluster	Administer the cluster (All functionalities, such as setup, shutdown)
Cluster Config	Configure the cluster
Put Node To Maintenance	Puts the cluster node into maintenance state
Cluster Release Info	Displays the release information of the cluster software and packages of the Sun Cluster
Show Resources Info	Displays the configured Resource Types, Resource Groups and Resources
Cluster Status	Checks the status of all the components of the cluster
Verify Cluster Config	Verifies the cluster configuration
Node Info	Shows node information (Name of the Node, Votes Configured, Private Net Hostname, Transport Adaptors, Quorum Devices, Device Groups, Resource Groups)
Show DID Info	Shows the Disk IDs of the cluster

Table 5-8   **Applications in the Sun Cluster Applications Group (Continued)**

Application Name	Description
Show Device Group Info	Shows Device group information (Name of the Device Group, Type of the Disk Group, Failback Enabled/Disabled, the Nodes the Disk Group can be attached to, Node Order, Meta Devices which are components of the Disk Group, List of nodes where the device is primarily attached) and status
Add Quorum Device	Adds the quorum device
Remove Quorum Device	Removes the quorum device
Put Quorum to Maintenance	Puts Quorum device into maintenance state
Reset Quorum	Reset the Quorum device
Quorum Info	Shows the Quorum device information
Add Resource	Adds a resource to a resource group
Enable Resource	Enables resources of selected resource groups
Disable Resource	Disables resources of selected resource groups
Remove Resource	Removes a resource from resource group
Resource Info	Shows resource information (Resource Group Name, Resource Name, Resource Type, report strong dependencies of other resource groups, report weak dependencies of the other resource groups)
Change Primary	Switch the primary
Create Resource Group	Creates the resource group
Delete Resource Group	Deletes the resource group

Table 5-8   **Applications in the Sun Cluster Applications Group (Continued)**

Application Name	Description
Evacuate Resource Group	Evacuates the resource groups from node
Make Resource Group Managed	Set the selected resource group as managed
Make Resource Group Unmanaged	Set the selected resource group as unmanaged
Put Resource Group Offline	Set the selected resource group offline
Put Resource Group Online	Set the selected resource group online
Resource Group Info	Shows the resource group information (Name of the resource group, Primary nodes to which resource is allocated, Resource group description, List of resources, Maximum number of primary nodes the resource group may be connected, Desired primaries, Value of failback flag, Dependencies on network resources, Dependencies on the other resource groups, Global resources used, Directory path for the resource group administration files and status
Restart Resource Group	Restart the resource group
Shutdown Resource Group	Shutdown the resource group/ Turn on the resource group
Switch Failover Resource Group	Does the switch-over of the failover resource group
Register Resource Type	Register the given resource type

Table 5-8　　　**Applications in the Sun Cluster Applications Group (Continued)**

Application Name	Description
Resource Type Info	Shows the resource type information (Name of the resource type, Installed nodes, Description from the configuration file, Path to the directory where scripts and binaries of the resource types are held, Single instance Yes/No, Failover allowed or not, Dependencies within resource type, Definition Methods, Properties, Resource List)
Add Adapter	Add adapter to NAFO group
Create NAFO Group	Creates NAFO group
Delete NAFO Group	Deletes NAFO group
Find NAFO Group	Show the NAFO group of the active adaptor
Remove Adapter	Remove adapter from NAFO group
Switch Active Adapter	Switch NAFO group's active adapter
Transport Info	Shows information about the transport adapter
Transport Status	Shows the status of the transport adapter

Sun Cluster Policy Group

All the policies for Sun cluster are grouped under the policy group, SC_Monitors.

The Sun cluster policies can be split into the following generic areas:

Monitor Policies, Table 5-9 on page 127

Message Interceptor Policies, Table 5-10 on page 127

Table 5-9 lists the monitor policies installed for Sun cluster. It gives a brief description of the scope, and indicates how often the policy polls for information and updates.

Table 5-9   OSSPI Monitor Policy for Sun Cluster

Policy Name	Description	Polling Interval
scmon	Monitors the Sun cluster components	10m

Table 5-10 lists the message interceptor policies installed for monitoring the Sun cluster messages. It gives a brief description of the scope and indicates how often the policy polls for information and updates.

Table 5-10   OSSPI Message Interceptor Policies for Sun Cluster

Policy Name	Description	Polling Interval
scmsg	Intercepts general Sun cluster messages	n/a
sc-nafomsg	Intercepts messages from the NAFO groups in the cluster	n/a
sc-transportmsg	Intercepts messages from the cluster interconnect	n/a
sc-quorummsg	Intercepts messages from the quorum devices	n/a

Table 5-10   **OSSPI Message Interceptor Policies for Sun Cluster (Continued)**

Policy Name	Description	Polling Interval
sc-gdmsg	Intercepts messages from the global devices in the cluster	n/a
sc-rgmsg	Intercepts messages from the resource groups in the cluster	n/a

Monitoring Cluster File Systems

If no file-system parameters are specified explicitly, the file-system monitor uses the contents of a configuration file generated by the OSSPI and located in the following directories on the managed node, /var/opt/OV/osspi/conf/osspi_fsmon.cfg, /var/opt/OV/osspi/conf/osspi_global_fs.cfg, or /var/opt/OV/osspi/conf/osspi_local_fs.cfg. These files contain a list of all the file systems that you intend to monitor with the OSSPI's generic file-system monitor. For details on file system monitoring, see "Monitoring File Systems with the OSSPI" on page 88

The osspi_fsmon.cfg file may or may not contain entries for the dynamic file systems in the cluster setup. These file systems will be listed only if they are mounted on any of the nodes when discovery is run. The OSSPI file system monitor generates the file osspi_fsmon-hash.cfg, containing the internal data structures of the monitored file systems, every time it is run. The information in this file is used to periodically update osspi_fsmon.cfg.

NOTE   Do not edit the files osspi_fsmon.cfg and osspi_fsmon-hash.cfg, which detail the discovered and monitored file systems respectively. Manually editing these files might cause file system monitoring to fail.

Monitor Cluster Processes

The monitoring of the cluster processes depends on the Process Monitoring infrastructure. These processes run on all cluster nodes and therefore send alarms or messages about their status to the node (On the Management Server) they are executing on. These alarms or messages are not directed to the Message Only Node (cluster name).

Collating Sun Cluster Messages In One Location

All the messages for Sun cluster monitoring can be viewed from one location, though messages are generated from all nodes of the cluster. Implementation of message key correlation ensures that messages are not repeated on the message browser.

The following OSSPI objects ensure that the cluster is monitored effectively and the messages appear at only one location.

- Message Only Node: This node name identifies the Sun cluster being monitored. For the Sun cluster to be monitored, this node must be added to the OSSPI-Solaris node group. All monitor messages from the Sun cluster monitor scripts are sent to the message only node.

- OSSPI-Clusters Message Group: All messages sent about the cluster and it's components are directed to this message group.

- Policy Group: The policy group SC_Monitors contains all the monitor and message policies for Sun cluster.

NOTE   The name of the message only node must be changed if the cluster name is changed.

This design ensures that you can view all Sun cluster messages within the Message Only Node.

6 Troubleshooting the OSSPI

This section describes how to go about troubleshooting the OSSPI and provides tips and tricks that are designed to help you complete the problem-solving process.

In this Section

This chapter contains information designed to help you carry out both every-day, search-and-find operations as well as more detailed troubleshooting of the OSSPI. The chapter is divided into the following sections:

"File Locations"	where the OSSPI stores information, for example; configuration, run time, logs, and so on
"Error Logging"	messages to OSSPI log files concerning configuration errors
"Debugging Scripts"	procedure to debug and view the output of OSSPI scripts
"Tracing"	information generated by the OSSPI scripts and executables when they startup and stop and when they are running
"Message Conditions"	links between message conditions and the messages the conditions generate.

File Locations

During the initial installation of the Smart Plug-in for UNIX Operating Systems software, a number of important files are copied to the OVO management server. Similarly, when you install the OSSPI on the OVO managed node, the agent software (including the policies, actions, commands, and monitors) is copied to defined directory locations on the managed node.

The following lists shows how the installation process creates a number of different directories on the OVO management server and the managed node according to the type of file that is installed—binary, run-time, executable, and so on.

The OVO Management Server

If you need to locate a particular type of file on the OVO management server, use the following list:

File Type...	OSSPI File Location...
Binaries	/opt/OV/osspi/bin/
Documentation	/opt/OV/osspi/doc/
Logs/Discovery	/var/opt/OV/share/osspi/log/
OV Service Navigator/Discovery Output	
	/var/opt/OV/share/osspi/conf/
Temp/Runtime	/var/opt/OV/share/osspi/tmp/
OVO integration	/var/opt/OV/share/tmp/OpC_appl/

The OV Service Navigator/Discovery Output files also contain information about errors that occur during the service-discovery process, for example, if a node is down or not responding.

The OVO Managed Nodes

The following list shows the directory locations for the files the OSSPI installs on a OVO managed node. These are the standard locations for OVO commands, actions, and monitors.

AIX

File Type...	OSSPI File Location...
Binaries	/var/lpp/OV/OpC/
Configuration	/var/lpp/OV/osspi/conf/
Trace/Config	/var/lpp/OV/osspi/conf/
Logs	/var/lpp/OV/osspi/log/
Temp/Runtime	/var/lpp/OV/osspi/tmp/

HP-UX, Linux, Solaris, and Tru64

File Type...	OSSPI File Location...
Binaries	/var/opt/OV/bin/OpC/
Configuration	/var/opt/OV/osspi/conf/
Trace/Config	/var/opt/OV/osspi/conf/
Logs	/var/opt/OV/osspi/log/
Temp/Runtime	/var/opt/OV/osspi/tmp/

Error Logging

The OSSPI scripts and executables write messages to a log file which resides in:

AIX: /var/lpp/OV/osspi/log/osspi.log

HP-UX: /var/opt/OV/osspi/log/osspi.log

Linux: /var/opt/OV/osspi/log/osspi.log

Solaris: /var/opt/OV/osspi/log/osspi.log

Tru64:   /var/opt/OV/osspi/log/osspi.log

For the most part, these messages concern configuration errors. However, the messages can also contain information about abnormal conditions which have occurred during program execution.

NOTE   The OSSPI also monitors the size of the osspi.log log file and, if necessary, cleans it up at regular intervals in order to save disk space.

The entries generated in the osspi.log log file take the (ASCII) format illustrated in the following example and in Example 6-1 and described in detail in Table 6-1:

<mm/dd/yyyy> <hh:mm:ss> [*<severity>*]\ OSSPI(*<program_name>-<pid>*): *<error_text>*

Table 6-1 lists the possible entries in the osspi.log file and describes what the entries mean.

Table 6-1   **Fields in the osspi.log File**

Field Name	Description
<mm/dd/yyyy>	Creation date of logfile entry
<hh:mm:ss>	Creation time of logfile entry
<severity>	Severity level: ERROR, WARNING, INFO
<program_name>	Name of the executable or script
<pid>	Process ID of the executable or script

Table 6-1   **Fields in the osspi.log File (Continued)**

Field Name	Description
<error_text>	Detailed information regarding the logfile entry

Example 6-1 uses a small part of the osspi.log file to illustrate what kind of information the OSSPI writes to the osspi.log file.

Example 6-1   **Excerpt from the osspi.log file**

```
09/29/2000 13:59:09 [INFO] OSSPI(osspi_discclient.sh-14071): Discovery was
started on this node.
09/29/2000 13:59:43 [INFO] OSSPI(osspi_discclient.sh-14071): Discovery ended on
this node.
10/05/2000 10:24:02 [ERROR] OSSPI(osspi_fsutil.sh-7459): addfs: replace tags FS
and Limits with filesystem name and limits and start again
10/05/2000 10:24:14 [ERROR] OSSPI(osspi_fsutil.sh-7469): addfs: replace tag FS
with filesystem name and start again
10/05/2000 10:31:52 [ERROR] OSSPI(osspi_procutil.sh-7986): unknown option -show
10/05/2000 10:32:04 [ERROR] OSSPI(osspi_procutil.sh-7994): unknown option -show
10/10/2000 13:52:41 [INFO] OSSPI(osspi_discclient.sh-29592): Discovery was
started on this node.
10/10/2000 13:53:14 [INFO] OSSPI(osspi_discclient.sh-29592): Discovery ended on
this node.
10/25/2000 14:37:50 [INFO] OSSPI(osspi_discclient.sh-1956): Discovery was
started on this node.
10/25/2000 14:38:24 [INFO] OSSPI(osspi_discclient.sh-1956): Discovery ended on
this node.
10/25/2000 14:45:31 [INFO] OSSPI(osspi_discclient.sh-4897): Discovery was
started on this node.
10/25/2000 14:46:07 [INFO] OSSPI(osspi_discclient.sh-4897): Discovery ended on
this node.
```

Debugging Scripts

If you want to run OSSPI scripts from the command line, you must ensure the variable paths are set correctly, and then run the script.

To run the scripts from the command line, type the commands:

1. `PATH=$PATH:/var/opt/OV/bin/OpC/monitor` (on HP OpenView Operations 7.x)

   or

   `PATH=$PATH:/var/opt/OV/bin/instrumentation` (on HP OpenView Operations 8.0)

2. `export PATH`

3. `<ScriptName>`

To run the script in Debug mode, use the following commands:

1. `ksh -x ./<ScriptName>`

   or

   `sh -x ./<ScriptName>` (on Linux)

If you want to store the output in a file, type the command:

1. `ksh -x ./<ScriptName> > <FileName> 2>&1`

   or

   `sh -x ./<ScriptName> > <FileName> 2>&1` (on Linux)

Tracing

If tracing is enabled, all tracing information generated by the OSSPI scripts and executables is written to the following file:

AIX:	`/var/lpp/OV/osspi/log/osspi.trc`
HP-UX	`/var/opt/OV/osspi/log/osspi.trc`
Linux	`/var/opt/OV/osspi/log/osspi.trc`
Solaris	`/var/opt/OV/osspi/log/osspi.trc`
Tru64	`/var/opt/OV/osspi/log/osspi.trc`

You can enable tracing by setting a flag in the configuration file:

AIX	`/var/lpp/OV/osspi/conf/osspi.cfg`
HP-UX	`/var/opt/OV/osspi/conf/osspi.cfg`
Linux	`/var/opt/OV/osspi/conf/osspi.cfg`
Solaris	`/var/opt/OV/osspi/conf/osspi.cfg`
Tru64	`/var/opt/OV/osspi/conf/osspi.cfg`

To save disk space and simplify searching, the OSSPI limits the size of the `osspi.trc` trace file to 0.5MB. Once the 0.5MB file-size limit is reached, the OSSPI backs up and compresses the file to `osspi_#.trc.gz`, where # is a number from 0-3. This means that there is only ever a maximum of 5 (five) trace files in existence—the current trace file with no number (since it is neither compressed not tarred) and then four compressed and tarred trace files numbered from 0-3. The number 0 (zero) indicates the most recently saved trace file and 3 (three) the oldest. If even more space is required to store trace information, OSSPI deletes the file `osspi_3.trc.gz`, moves 0->1, 1->2, and 2->3, and writes `osspi_0.trc.gz` again. Note that trace level 9 (nine) generates a great deal of information.

NOTE   The OSSPI only allows tracing to be set on OVO managed nodes. If you want to trace the OSSPI on the OVO management server, the OVO management server must also be a managed node.

Table 6-2 illustrates which flags you can set in the osspi.trc and what the flags do.

Table 6-2   **Trace Levels and Objects**

Variable	Range of values	Description
TRACE_LEVEL	0-9	Trace information level. The higher the value the more information is generated and written. Default = 0 (off)
TRACE_OBJ	OSSPI scripts and executables	Definition of objects for which trace information should be written to the trace file.

The entries written to the trace file osspi.trc take a similar form to the entries in the log files, namely;

<mm/dd/yyyy> *<hh:mm:ss>* OSSPI(*<program_name>*-*<pid>*): *<text>*

Table 6-1 on page 137 lists the possible entries in the osspi.trc file and describes what they mean.

Table 6-3   **Fields in the osspi.trc File**

Field Name	Description
<mm/dd/yyyy>	Creation date of logfile entry
<hh:mm:ss>	Creation time of logfile entry
<program_name>	Name of the executable or script
<pid>	Process ID of the executable or script
<text>	Detailed information regarding the trace-file entry

Example 6-2 shows the last twenty lines or so of the osspi.trc file and uses a real-life environment to illustrates what kind of information can be collected when tracing is switched on.

Example 6-2   Excerpt from the osspi.trc file

```
10/25/2000 14:46:18 OSSPI(osspi_cfgmon.sh-5891): /etc/fstab is unchanged.
10/25/2000 14:46:18 OSSPI(osspi_cfgmon.sh-5891): /etc/profile is unchanged.
10/25/2000 14:46:18 OSSPI(osspi_printmon.sh-5702): - checking object
'/var/spool/lp/qstatus:lp:lp:-rw-r--r--' ...
10/25/2000 14:46:18 OSSPI(osspi_cfgmon.sh-5891): /etc/passwd is unchanged.
10/25/2000 14:46:18 OSSPI(osspi_cfgmon.sh-5891): /var/spool/cron/crontab.root is
unchanged.
10/25/2000 14:46:19 OSSPI(osspi_printmon.sh-5702): - checking object
'/var/spool/lp/pstatus:lp:lp:-rw-r--r--' ...
10/25/2000 14:46:19 OSSPI(osspi_cfgmon.sh-5891): /etc/syslog.conf is unchanged.
10/25/2000 14:46:19 OSSPI(osspi_printmon.sh-5702): - checking object
'/var/spool/lp/seqfile:lp:lp:-rw-r--r--' ...
10/25/2000 14:46:23 OSSPI(osspi_mountmon.sh-6091): / is Ok
10/25/2000 14:46:23 OSSPI(osspi_mountmon.sh-6091): /stand is Ok
10/25/2000 14:46:24 OSSPI(osspi_mountmon.sh-6091): /opt is Ok
10/25/2000 14:46:26 OSSPI(osspi_mountmon.sh-6091): /tmp is Ok
10/25/2000 14:46:26 OSSPI(osspi_mountmon.sh-6091): /u01 is Ok
10/25/2000 14:46:27 OSSPI(osspi_mountmon.sh-6091): /home is Ok
10/25/2000 14:46:28 OSSPI(osspi_mountmon.sh-6091): /usr is Ok
10/25/2000 14:46:29 OSSPI(osspi_mountmon.sh-6091): /var is Ok
10/25/2000 14:46:29 OSSPI(osspi_mountmon.sh-6091): reports notmounted: /opt/gnu
10/25/2000 14:46:29 OSSPI(osspi_mountmon.sh-6091): reports notmounted: /opt/xgnu
10/25/2000 14:46:40 OSSPI(osspi_procmon.sh-6310): processing config files
10/25/2000 14:46:40 OSSPI(osspi_printmon.sh-6303): Start queue check on HP-UX...
10/25/2000 14:46:40 OSSPI(osspi_printmon.sh-6307): Starting enable check on
HP-UX...[n.i.]
10/25/2000 14:46:40 OSSPI(osspi_printmon.sh-6303): - found 0 request(s) for
printer PDRequest
10/25/2000 14:46:40 OSSPI(osspi_procmon.sh-6310): processing section snmp
10/25/2000 14:46:40 OSSPI(osspi_procmon.sh-6309): processing config files
10/25/2000 14:46:40 OSSPI(osspi_procmon.sh-6310): looking for process snmpdm
10/25/2000 14:46:41 OSSPI(osspi_procmon.sh-6309): No such process group (mail)
found
```

Message Conditions

Each message generated by an OSSPI policy includes information which indicates exactly which policy and which policy condition was responsible for generating the message.

Select the required message and click the [Instructions...] button in the Message Details window to display the Instruction Output window illustrated in Figure 6-1. The instruction output displays the name of the policy enclosed in square brackets; [OSSPI-Discovery_1.4]. The number before the dot (.) is the policy version number: the number after the dot is the policy condition which was responsible for generating the message. In this example, the message which appeared in the Message Browser was generated by condition number *four* of (version *one*) of the OSSPI-Discovery policy.

Figure 6-1   **The Instruction Output Window**
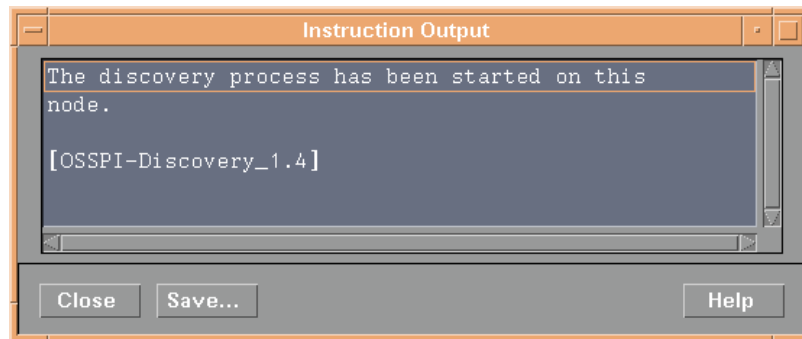
In the Message Source Template window, find and select the policy indicated in the instruction output (OSSPI_Discovery_1.4 in this example) click the [Conditions...] button and scroll down the list of conditions displayed and locate the condition indicated—four (.4) in this example—as shown in Figure 6-2 on page 144.

Figure 6-2   **The Message and Suppress Conditions Window**
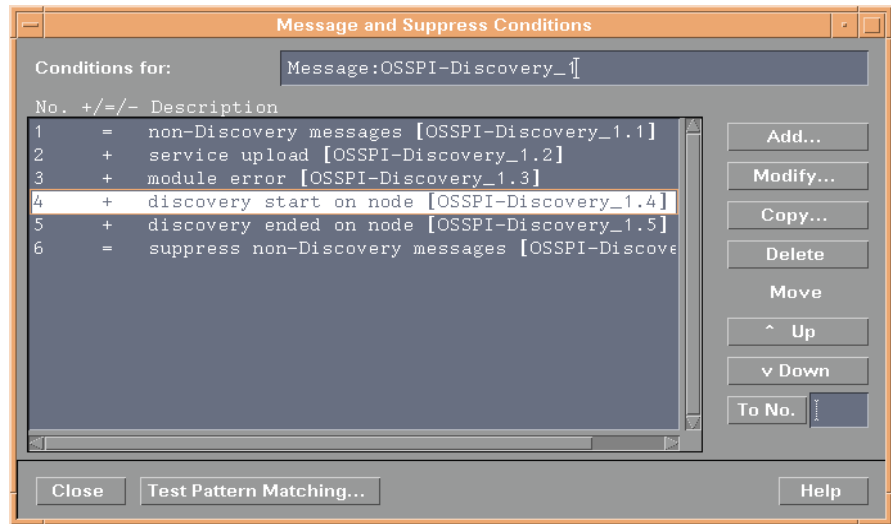
A   General OSSPI Tips

OSSPI Coda Filesystem Monitoring

Nodes running OVPA/Glance 4.0 experience a problem with the default OSSPI coda file system monitor policies (`OSSPI-CD_Filesystem_X`), which use the name *FS* instead of *FILESYSTEM* to monitor file system utilization.

Symptom: When this problem occurs, you might see any of the following messages:

- `Initialization of policy OSSPI-CD_Filesystem_X failed. (OpC30-727)`

- `Cannot find object 'FS' in coda object list.(OpC30-761)`

- `Evaluation of policy OSSPI-CD_Filesystem_X stopped. (OpC30-715)`

Solution: The OSSPI policy calls Coda from the monitor policy as follows:

OVPERF\\CODA**FS**\\FS_SPACE_UTIL

To resolve this problem, make the above change in the monitor program box of the particular policy and force-deploy the modified policy to the specified node.

OVPA 4 installed on a Linux box works only if the above call is made in the monitor program box of the policy as follows:

OVPERF\\CODA**FILESYSTEM**\\FS_SPACE_UTIL

NOTE   The above changes have not been incorporated into OSSPI A.02.52. Customers running OVPA 4.0 on their managed nodes will experience problems due to Coda 8 shipping with OVPA 4.0. In such a scenario, the OV agent does not overwrite the existing coda package, but uses the coda 8 sub-agent itself.

Editing the Global Filesystem Monitor Configuration File

The OSSPI global file system monitor configuration file, **osspi_fsmon.cfg**, is present on the management server at the location `/var/opt/OV/share/databases/OpC/mgd_node/customer/<vendor>/<platform>/<OS>/monitor/osspi_fsmon.cfg.Z` files (for example, `.../sun/sparc/solaris/osspi_fsmon.cfg.Z`)

The file has to be edited on the management server for the particular changes to be global and also be persistent across deployments and redeployments, to all OSSPI-monitored nodes in the network the `osspi_fsmon.cfg` files for the respective platforms.

You may modify the `osspi_fsmon.cfg` files before deploying or distributing them to all managed nodes in the network, including the management server node as explained in the steps below:

1. Uncompress the file `osspi_fsmon.cfg.Z` file. Open the uncompressed file in vi or any other UNIX-based editor to ensure that CRLF characters do not get added to the file.

2. Add new `fs` monitor entries in the following format:

```
<mount_point><TAB><Warning_Threshold><TAB><Minor_threshold><TAB><Major_Threshold><TAB><Critical_Threshold>
```

   Do not enter spaces to delimit the columns. Instead, use tabs.

3. Save and close the file. Compress the file again, and force-deploy monitors to all the nodes.

IMPORTANT   When the `osspi_cleanup_srv.sh` script is run during the OSSPI product upgrade, all the `osspi_fsmon.cfg.Z` files will be deleted. Ensure that backups of all these files, where modifications have been made, are taken before running `osspi_cleanup_srv.sh`. These files are not overwritten during the post-installation configuration phase of the OSSPI package. Upon OSSPI upgrade, these files may be restored back to their original locations.

fsmon_local.cfg not Supported with OVEPC Policy

The OSSPI-CD file system policy does not use values specified in the fsmon_local.cfg file on the node. Thresholds for file systems may be modified by altering the conditions. However, all file systems will have the same thresholds.

All the other file system monitor policies (GP, MW, and NP) use the fsmon_local.cfg file for thresholds.

Supported Versions of OVPA

The following versions of OVPA are supported due to change in behavior of the FS_SPACE_UTIL metric:

- AIX – C.03.80.00

- DEC – C.03.60 & C.03.61

- HPUX – C.03.70.00

- Solaris – C.03.75.00

- Linux – C.04.00.00

To support these versions of OVPA, `osspi_alarm_mw.sh` creates alarmdefs for FS_SPACE_UTIL alarm rules in the following format:

```
Example:alias FS0="/usr(FILESYSTEM)"
```

In the previous versions, alarmdefs, created by `osspi_alarm_mw.sh`, was in the following format:

```
Example: alias FS0="/dev/dsk/c0t0d0s0(FILESYSTEM)"
```

The A.02.52 version of UNIX OS SPI now supports only the mentioned versions of OVPA. HP recommends that customers move to above versions of OVPA for utilizing and alarming on the above metric.

Discovery Time-out due to Blaster Worm

If discovery displays error messages, such as the following, ensure that the DCE patches for Blaster worm are applied on the nodes:

```
######################################

2003/08/15 16:45:35

Discovery started.

Nodes:hpjsdbp.hp.com

waiting...

ERROR: Timeout: There was a problem with at least one of the nodes.

hpjsdtsh.hp.com waiting...

ERROR: Timeout: There was a problem with at least one of the nodes.

power.hp.com waiting...

ERROR: Timeout: There was a problem with at least one of the nodes.

ultra1.hp.com waiting...

ERROR: Timeout: There was a problem with at least one of the nodes.

hpjsdb80.hp.com waiting...

ERROR: Timeout: There was a problem with at least one of the nodes.

hpjsdb77.hp.com waiting...

ERROR: Timeout: There was a problem with at least one of the nodes.

....

######################################
```

View the technical notes at the following locations and install the relevant DCE patches:

- Patches from Entegrity for DCE for Tru64
  <http://support.entegrity.com/private/patches/dce/rpcattacks.shtml>

- Patches from HP for DCE for HP-UX/Linux/Solaris
  <http://support.openview.hp.com/blaster.jsp>

Using the Add Process Group Application

You can add process groups to the Osspi process monitor config file
(`procmon.cfg`) in two ways:

NOTE   The above application will always be run with customized settings set by
the user.

- Right-click the application icon and open the `Customized Startup`
  window. For more information on Customizing OSSPI Application,
  see Figure 2-3 on page 26. Then, add a process directly in the
  yet-to-be-created process group by specifying the following (remove
  existing text):

  ```
  osspi_procmon.sh [-global|-local] -addprc <section>
  <process> ["<args>"] [<time>] [<wkdays>] [<bounds>]
  ```

  Repeat the above step for each process that needs to be added. If the
  section is already present, no new section will be created.

- Create a file with the entire section specification on the particular
  managed node. Ensure that the columns in the file are delimited by
  tabs. Right-click the `Add Process Group` application icon and open
  the `Customized Startup` window. In the subsequent screen, specify
  the complete path of the file instead of the default `FILE` argument.

About Unix OS SPI OVPA/GP Policies

All OSSPI-OVPA/OSSPI-GP policies can be modified as explained:

- Values specified as arguments to the osspi_null.sh script.

  Example:

  osspi_null.sh OSSPI-MWA_Cpu_Load_1 *'GBL_CPU_TOTAL_UTIL >
  95 prob 90, GBL_PRI_QUEUE > 3 prob 5, GBL_PRI_QUEUE > 4
  prob 5'*

  may be modified as

  osspi_null.sh OSSPI-MWA_Cpu_Load_1 *'GBL_CPU_TOTAL_UTIL >
  70 prob 98, GBL_PRI_QUEUE > 4 prob 1, GBL_PRI_QUEUE > 6
  prob 1'*

- Thresholds specified in the conditions to the OSSPI-MWA_* and
  OSSPI-GP_* policies.

  Thresholds specified in the conditions may be modified except for the
  Filesystem utilization monitor policies OSSPI-GP_Filesystem,
  OSSPI-MWA_Filesystem, to suit site needs. For filesystem utilization
  monitoring, thresholds need to be set or modified in the
  fsmon_local.cfg file present on the node.

- Reset duration specified in the conditions to the OSSPI-MWA_* and
  OSSPI-GP_* templates.

  Reset duration may be modified and these will reflect in the
  osspi_alarmdef/syntax_gp files as *wait period*, before when
  GP/OVPA will not alarm even though a certain threshold may be
  reached.

  The above changes will be reflected in the osspi_alarmdef or
  syntax_gp file that is created once the modified policy is deployed to
  the node.

You will not need to modify the following fields due to the reasons listed:

- Setting message keys for message correlation

Message key correlation is achieved through message interceptor policy `OSSPI-opcmsg_X`. The conditions for intercepting OVPA or OVPM alarms, may contain the message key as well as acknowledge message key pattern, for the message key correlation in the following manner

- Message Key = `<$MSG_NODE_NAME>:<$MSG_GRP>:<$MSG_OBJECT>:<$MSG_SEV>`

- Pattern to match = `<$MSG_NODE_NAME>:<$MSG_GRP>:<$MSG_OBJECT>:[Critical:Major:Minor:Warning:Normal]`

The following are the conditions for the `OSSPI-opcmsg` interface policy that may be modified as specified above -

- `MC/SG OV Performance Manager alarms ( REPEAT/END conditions ) [OSSPI-opcmsg...]`

- `MC/SG OV Performance Manager alarms ( START conditions ) [OSSPI-opcmsg...]`

- `OV Performance Manager alarms ( REPEAT/END conditions ) [OSSPI-opcmsg...]`

- `OV Performance Manager alarms ( START conditions ) [OSSPI-opcmsg...]`

- Setting messages to log to history browser, will not work, since the alarms are dispatched from Glance/OVPA - and not from the monitor policy. Use `OSSPI-opcmsg` policy to suppress alarms.

- There is no concept of a polling interval where the OVPA/GP policies run. This is the reason the polling interval is set to 365d. For example, even if the polling interval is changed to K seconds, the `osspi_null.sh` script will be run every K seconds or so, wherein an `opcmon` call is made setting policy name to zero and no changes will get effected in the `osspi_alarmdef.` The only scenario where changes are effected to a new `osspi_alarmdef` file, is when policies are deployed to the node. So, retain the polling interval as 365d, the default setting.

B OSSPI Components Without Alternative User Support

OSSPI processes normally run under user root on UNIX systems. But most OSSPI components can also be run under alternative users. The

alternative user should be the same user that the agent is configured to run under. This section details the OSSPI components that are not supported under non-root user.

NOTE   Sun cluster discovery and monitoring is not supported under non-root user.

For information on configuring OSSPI components to run under non-root user, see "Configuring OSSPI to Run as Alternative User" on page 107.

Discovery under Alternative User

Some Discovery processes do not run under alternative user. This causes related objects to be *not* discovered when discovery is run. Consequently, OSSPI cannot monitor these objects for which service elements are not created. Also, these objects do not appear on the service views.

NOTE   When Discovery is run as alternative user, dependencies between objects are not discovered. This can prevent the propagation of errors or faults.

The following table lists the system objects and process that are not discovered when Discovery runs as non-root user.

Table B-1   **Objects not discovered under non-root user**

Object/Process	HP-UX 11.00	HP-UX 11.11	HP-UX 11.23	Solaris	Linux
Physical Disk	✘	✘	✘	✘	
Swap	✘				✘
Cron			✘		
DNS			✘		✘
Mail			✘		✘
NTP			✘		✘
Print			✘		✘
SNMP			✘		✘
MC/SG			✘	n/a	n/a
IPC			✘		

Policies under Alternative User

The policies and the operating systems on which they do not run under non-root user are detailed in the following table.

Table B-2   **Policies that do not work under non-root user**

Policy Name[a]	HP-UX 11.00	HP-UX 11.11	HP-UX 11.23	Solaris 5.9	Linux Red Hat AS 2.1
Logfile Policies					
BadLogs	✗		✗	✗	
Boot					✗
MailAliases			✗		
MailLog					✗
SNMPConf		✗	✗		
Su	✗	✗	✗	✗	✗
Syslog					✗
Cron			✗		
Monitor Policies					
CronProc	✗	✗	✗	✗	✗
defect_long	✗	✗	✗	✗	✗
defect_short b	✗	✗	✗	✗	✗
DnsProc	✗	✗	✗	✗	✗
InetdProc	✗	✗	✗	✗	✗
MailProc	✗	✗	✗	✗	✗
Mount	✗	✗	✗	✗	✗

Table B-2   **Policies that do not work under non-root user (Continued)**

Policy Name[a]	HP-UX 11.00	HP-UX 11.11	HP-UX 11.23	Solaris 5.9	Linux Red Hat AS 2.1
NFSClientProc	✗	✗	✗	✗	✗
NFSServerProc	✗	✗	✗	✗	✗
NTPProc	✗	✗	✗	✗	✗
SNMPProc	✗	✗	✗	✗	✗
SyslogProc	✗	✗	✗	✗	✗
VeritasProc	✗	✗	✗	✗	✗

a. HP OVPA policies do not run under non-root user.

Applications under Alternative User

The applications and the operating systems on which they do not run under non-root user are detailed in the following table.

Table B-3   **Applications that do not work under non-root user**

Application Name[a]	HP-UX 11.00	HP-UX 11.11	HP-UX 11.23	Solaris	Linux
OSSPI Clean Node	✗	✗	✗	✗	✗
OSSPI Edit FS Table	✗	✗	✗	✗	✗
FS Mount	✗	✗	✗	✗	✗
FS Unmount	✗	✗	✗	✗	✗
Reboot	✗	✗	✗	✗	✗
Shutdown	✗	✗	✗	✗	✗
ifconfig	✗	✗	✗	✗	✗
ASCII_SAM	✗	✗	✗	n/a	n/a
Motif_SAM	✗	✗	✗	n/a	n/a
Veritas Statistics	✗	✗	✗	✗	✗
Start pvalarmd	✗	✗	✗	✗	✗
Stop pvalarmd	✗	✗	✗	✗	✗
Configure ttd.conf	✗	✗	✗	✗	✗

a. HP OVPA applications do not run under non-root user.

NOTE   The OVO agent running under non-root will try to launch any application under non-root user, irrespective of what is specified in the application launch window.

Index

Index

Index

Index

Index