

HP Operations Smart Plug-in for IBM WebSphere Application Server

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

Software Version: 7.04

Installation and Configuration Guide



Legal Notices

Warranty

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

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

Copyright Notice

© Copyright 2002-2006, 2008-2010 Hewlett-Packard Development Company, L.P.

Trademark Notices

UNIX® is a registered trademark of The Open Group.

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

Oracle and Java are registered trademarks of Oracle and/or its affiliates.

Documentation Updates

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

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

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

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

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

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

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

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

Support

Visit the HP Software Support Online web site at:

www.hp.com/go/hpsoftwaresupport

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

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

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

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

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

To find more information about access levels, go to:

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

Contents

1	Introduction to HP Operations Smart Plug-in for WebSphere Application Server	13
	About the WebSphere SPI	13
	Smart Plug-in Data	13
	Smart Plug-in Uses and Customizations	13
	Components of the WebSphere SPI	14
	Policies	15
	Tools	15
	Reports	15
	Graphs	15
	Functions of the WebSphere SPI	16
	Collecting and Interpreting Server Performance and Availability Information	16
	Displaying Information	16
	Generating Reports Using HP Reporter	19
	Graphing Data with HP Performance Manager	19
	Customizing Policies and Metrics	20
2	Installing and Upgrading the WebSphere SPI	21
	Installation Packages	24
	Linux	24
	HP-UX	25
	Solaris	26
	Installation Environments	26
	Standard Installation of SPI Components on the HPOM Server	26
	Standalone HP Performance Manager	26
	Standard Installation in an HPOM Cluster Environment for HP-UX	27
	Prerequisites	27
	Hardware Requirements	27
	Software Requirements	27
	Installing the WebSphere SPI	28
	Installing the SPI on HP-UX	28
	Mounting the DVD on HP-UX	28
	Install the WebSphere SPI	29
	Installing the SPI on the HPOM for Linux or Solaris management server	29
	In an HPOM Cluster Environment for HP-UX	31
	Installing the SPI on the Cluster-Aware Management Server for HP-UX	32
	Verifying Installation	32
	Upgrading the WebSphere SPI	32
	Limitations	32
	Upgrade the Management Server from HPOM 8.xx to HPOM 9.0x or 9.10	33

Migrate the WebSphere SPI 6.00 from HPOM 8.xx to HPOM 9.0x or 9.10	33
Migrate the HPOM from one system to another	33
Upgrade the WebSphere SPI 6.00 to WebSphere SPI 7.04 on HPOM 9.0x or 9.10.	34
Upgrading the WebSphere SPI using the HP Operations Smart Plug-in Upgrade Toolkit	34
Upgrading the WebSphere SPI on a Standalone HPOM 9.0x or 9.10 Server through HPOM Console	34
3 Configuring the WebSphere SPI	37
Prerequisites	37
Assign Operator Responsibilities for opc_admin	37
Assign Tools to the Operator	37
Verify the Application Server Status	38
Collect WebSphere Login Information.	38
Connect using JSR 160.	39
Update WebSphere's SDK	39
Configuring the WebSphere SPI	39
Add Nodes to a WebSphere SPI Node Group	40
Assign Categories to the Managed Node.	41
Deploy Instrumentation on the Managed Node	42
Run Discovery	43
Verify the Discovery Process	44
Assign Policies to the Managed Node	45
Deploy the WebSphere SPI Policies	45
Run Configuration	46
Additional Configuration.	47
Conditional Properties	47
Setting Conditional Properties.	47
Configuring a Non-Root HTTPS Agent on a UNIX Managed Node.	47
Configuration in High Availability Environments.	49
Configuration Prerequisites.	49
Configuring the SPI for High Availability Environments	49
Create the WebSphere SPI Monitoring Configuration File	49
Create the Clustered Application Configuration File	50
Configure the WebSphere SPI	51
Discovery in Cluster Environment	52
Deployment Manager	52
Discovery in the Network Deployer Scenario	53
Use Cases	53
Limitations in a Network Deployer Scenario	54
Discovery on Hypervisor Edition.	55
Discovery of WebSphere Portal Servers	55
Integrating with CODA.	56
4 Using the WebSphere SPI Tools	59
Overview.	59
SPI Admin Tools Group	60
Discover or Configure WBSSPI.	61
Init Non-Root	61

Self-Healing Info	61
Start Monitoring	62
Stop Monitoring	62
Start Tracing	63
Stop Tracing	63
Verify	63
View Error File	63
View WBSSPI Graphs	64
WebSphere Admin Tools Group	64
Check WebSphere	64
Start WebSphere	65
Stop WebSphere	65
View WebSphere Logs	66
Metric Reports	66
Tool Bank Reports Generated from Alarms	67
JMX Metric Builder Tools	67
Launching Tools	68
Launching Discover or Configure WBSSPI tool	68
Launching All Tools	68
5 Customizing the WebSphere SPI Policies	69
Overview	69
WebSphere Policy Groups and System PMI Levels	72
Basic Policy Customizations	72
Modifying Metrics Policies	72
Modifying Alarm Generation	74
Advanced Policy Customizations	75
Choosing Metrics to Customize	75
Using the WebSphere SPI Collector/Analyzer Command	76
WebSphere SPI Collector/Analyzer Command Parameters	76
Examples	77
Using JMX Actions Command Parameters	78
Examples	79
Changing the Collection Interval for Scheduled Metrics	80
Changing the Collection Interval for Selected Metrics	81
Customize the Threshold for Different Servers	81
Creating Custom, Tagged Policies	82
Create a New Policy Group	82
Policy Variables	83
Monitoring a WebSphere Server on Unsupported Platforms	83
Requirements for Monitoring Remote Nodes	83
Remote Monitoring	84
Configuring Remote System Monitoring	85
Configure the Remote WebSphere Server System	85
Integrate the HP Performance Agent (Optional)	86
Assign Local Node to a WebSphere SPI Node Group	86
Configuring Remote Logfile Monitoring (Optional)	86

Configure the Logfile Policy for Remote Logfiles	86
Limitations of Remote Monitoring	87
Restoring Default WebSphere SPI Policies	87
Using Policies/Tools to View Annotation Reports.	88
Automatic Action Reports	88
Viewing an Automatic Action Report	88
Tool Bank Reports.	89
Checking the WebSphere SPI Nodes for License Count	90
6 Integrating the WebSphere SPI with HP Reporting and Graphing Solutions	91
Integrating with HP Reporter.	92
Integrating with HP Performance Manager.	94
Integration Example.	94
7 Troubleshooting	101
Self-Healing Info Tool	101
Log File Monitoring	101
Logging	102
Management Server	102
Managed Nodes	103
Troubleshooting the Collection	104
Troubleshooting the Discovery Process	105
Troubleshooting Graphs	108
Troubleshooting Tools	108
Troubleshooting Miscellaneous.	111
Overview of Error Messages	112
8 Removing the WebSphere SPI.	113
Removing the SPI components	113
Remove the WebSphere SPI Software from the Management Server	113
Delete the WebSphere SPI Message groups	115
Delete the WebSphere SPI User Profiles.	115
Remove the Report Package (Optional).	115
Remove the Graph Package (Optional)	115
Removing the WebSphere SPI in a Cluster Environment.	116
A File Locations	117
HPOM Management Server File Locations	117
Managed Node File Locations.	117
Non-Root HTTPS Agent Environment	118
B Configuration	119
Structure.	119
Global Properties	119
GROUP Block	119
NODE Block	120
Server-Specific Properties	120
Property Precedence	120

Configuration Editor	121
Configuration Editor - Tree	121
Configuration Editor - Buttons	123
Configuration Editor - Actions	123
Add Application Server	124
Add Group	126
Add Node	126
Remove Application Server/Remove ALL App Servers	126
Remove Group/Remove ALL Groups	127
Remove Node/Remove ALL Nodes	127
Set Configuration Settings Tab	128
View Current Configuration Tab	129
Configuration Properties	130
Property Definitions	132
Sample Configurations	136
Example 1: Single Node/Two Servers	136
Example 2: Multiple Nodes/Repeated Properties	136
Example 3: WebSphere Servers with Virtual IP Addresses	137
Example 4: Administrative Privileges Using Same Login Information	138
Example 5: Administrative Privileges Using Different Login Information	138
C Error Messages	141
WASSPI-1	142
WASSPI-2	142
WASSPI-3	143
WASSPI-5	144
WASSPI-6	144
WASSPI-7	144
WASSPI-8	145
WASSPI-9	146
WASSPI-10	147
WASSPI-11	147
WASSPI-12	148
WASSPI-13	148
WASSPI-14	149
WASSPI-15	149
WASSPI-16	150
WASSPI-18	150
WASSPI-19	150
WASSPI-20	151
WASSPI-21	151
WASSPI-22	151
WASSPI-23	152
WASSPI-24	152
WASSPI-25	152
WASSPI-26	153

WASSPI-27	153
WASSPI-28	153
WASSPI-29	154
WASSPI-30	154
WASSPI-31	154
WASSPI-32	154
WASSPI-33	154
WASSPI-34	155
WASSPI-35	155
WASSPI-36	155
WASSPI-37	156
WASSPI-38	156
WASSPI-39	156
WASSPI-40	157
WASSPI-41	157
WASSPI-42	157
WASSPI-43	158
WASSPI-201	158
WASSPI-202	158
WASSPI-203	159
WASSPI-204	159
WASSPI-205	159
WASSPI-206	160
WASSPI-207	160
WASSPI-208	160
WASSPI-209	161
WASSPI-210	161
WASSPI-211	161
WASSPI-213	162
WASSPI-214	162
WASSPI-216	162
WASSPI-218	163
WASSPI-219	163
WASSPI-221	163
WASSPI-222	164
WASSPI-223	164
WASSPI-224	164
WASSPI-225	165
WASSPI-226	165
WASSPI-227	165
WASSPI-228	166
WASSPI-229	166
WASSPI-230	166
WASSPI-231	167

WASSPI-232	167
WASSPI-234	167
WASSPI-235	168
WASSPI-236	168
WASSPI-237	168
WASSPI-238	169
WASSPI-241	169
Others	169
Glossary	171
Index	177

1 Introduction to HP Operations Smart Plug-in for WebSphere Application Server

The Smart Plug-in for WebSphere Application Server (WebSphere SPI) enables you to manage WebSphere Application Servers from an HP Operations Manager (HPOM) console. The WebSphere SPI adds monitoring capabilities to HPOM. For more information on HPOM, see *HP Operations Manager for UNIX Concepts Guide*.

About the WebSphere SPI

In conjunction with HPOM, the WebSphere SPI offers centralized tools that help you monitor and manage systems using WebSphere Application Server. From the HPOM console, you can apply performance and problem managing processes to monitor systems using the WebSphere Application Server. The WebSphere SPI metrics are automatically sent to the HP Operations agent. These metrics can generate alarms or be consolidated into reports and graphs to help you analyze trends in server usage, availability, and performance. You can also integrate the WebSphere SPI with HP Reporter and HP Performance Manager (both products must be purchased separately) to obtain additional reporting and graphing flexibility, and capabilities. For details on integrating the WebSphere SPI with other HP products, see [Chapter 6, Integrating the WebSphere SPI with HP Reporting and Graphing Solutions](#).

Smart Plug-in Data

The WebSphere SPI has several server-related metrics that gather data and thus monitor the following:

- Server availability
- Server performance
- Memory usage
- Transaction rates
- Servlet executing times, time-outs, request rates
- JDBC connection status
- Web application processing

Smart Plug-in Uses and Customizations

As a WebSphere Application Server administrator, you can choose the metrics crucial to the operation of WebSphere Application Server by modifying the WebSphere SPI policies. The policies contain settings that allow incoming data to be measured against predefined rules. These rules generate useful information in the form of messages. The messages have color-coding to indicate the severity level. You can review these messages for problem analysis

and resolution. There are several pre-defined corrective actions for specific events or threshold violations. These corrective actions can be triggered automatically or operator-initiated.

Components of the WebSphere SPI

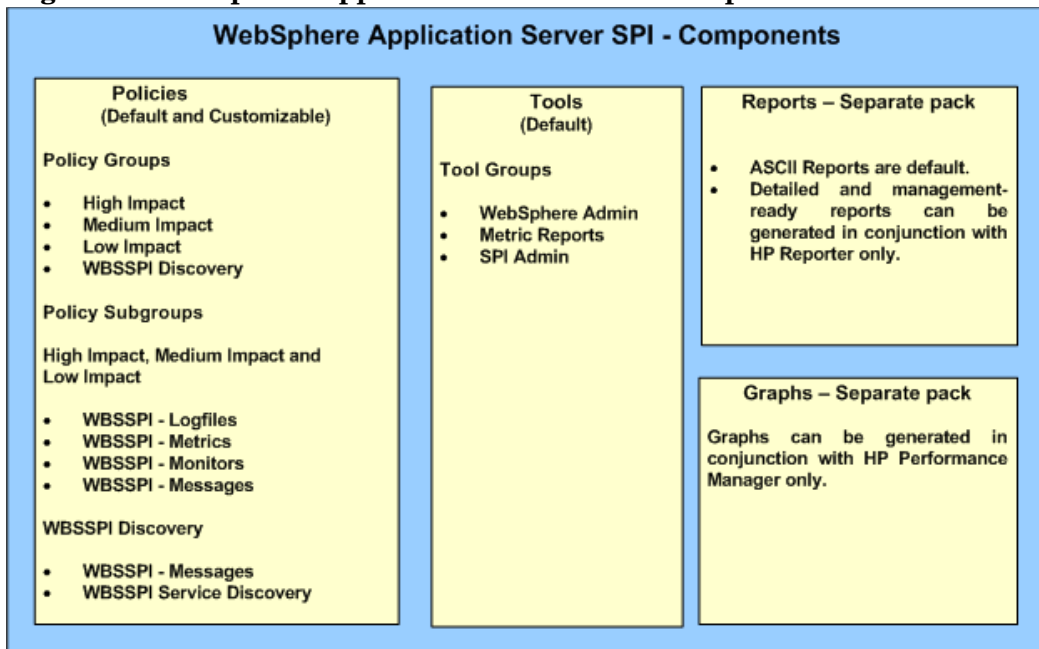
The WebSphere SPI has four main components:

- Policies
- Tools
- Reports
- Graphs

You can use the tools and policies to configure and receive data in the form of messages, annotations, and metric reports. These messages (available in the message browser), annotations (available through message properties), and metric reports (available through tools) provide information about the conditions present in the servers running on specific managed nodes.

The WebSphere SPI configuration tools allow you to configure the management server's connection to selected server instances on specific managed nodes. After you configure the connection, you can assign policies to the nodes. With HP Operations agent software running on the managed nodes, you can use the WebSphere SPI reporting tools to generate metric reports. In addition, you can generate graphs that show the WebSphere SPI data (available through message properties).

Figure 1 WebSphere Application Server SPI - Components



Policies

The WebSphere SPI consists of policies that monitor the WebSphere Application Server. The policies contain settings which allow incoming data to be measured against predefined rules. These rules generate useful information in the form of messages. The messages are coded with different colors to indicate the severity level. You can review these messages for problem analysis and resolution. There are several pre-defined corrective actions for specific events or threshold violations. These corrective actions can be triggered automatically or operator-initiated. When you double-click a message text, corrective actions appear within the **Instructions** tab and automatically generated metric reports appear within the **Annotations** tab in the Message Properties window. Monitoring consists of alarms related to critical events of the tool, and logging important performance metrics of the application server. The metrics that are logged can be used to create graphs. For more information on policies, see [Overview](#) on page 69.

Tools

In conjunction with HPOM, the WebSphere SPI offers centralized tools which help you monitor and manage systems using WebSphere Application Server (WBS AS). The WebSphere SPI tools allow you to configure the management server's connection to selected server instances on specific managed nodes. The WebSphere SPI tools include configuration, troubleshooting, and report-generating utilities. In the Tool Bank window, the SPI for WebSphere tools (WBSSPI:TOOLS) consist of the following tool groups:

- WebSphere Admin (WBSSPI:ADMIN)
- Metric Reports (WBSSPI:REPORTS)
- SPI Admin (WBSSPI:SPI_ADMIN)
- JMX Metric Builder: This tool group is available *only if* you install the SPIJMB software bundle.

For more information on tools, see [Chapter 4, Using the WebSphere SPI Tools](#).

Reports

The SPI package contains the default reporting policies provided by the SPI. Reports are generated by the HP Reporter using the WebSphere SPI data. The reports show consolidated, historical data generated as web pages in management-ready presentation format which helps you analyze the performance of the WebSphere Application Server over a period of time. For details on integrating the WebSphere SPI with HP Reporter to get consolidated reports, see [Chapter 6, Integrating the WebSphere SPI with HP Reporting and Graphing Solutions](#).

Graphs

The SPI package contains the default graphing policies provided by the SPI. Graphs are drawn from metrics that are collected in the datasources created by the SPI. The graphs help you analyze trends in server usage, availability, and performance. For details on integrating the WebSphere SPI with HP Performance Manager to get consolidated graphs, see [Chapter 6, Integrating the WebSphere SPI with HP Reporting and Graphing Solutions](#).

Functions of the WebSphere SPI

The WebSphere SPI messaging, reporting, and action-executing capabilities are based on the HPOM concept of policies. The settings within these policies define various conditions that might occur within the WebSphere Application Server, and allow information to be sent back to the HPOM management server. This helps you to proactively address potential or existing problems and avoid serious disruptions to web transaction processing. The WebSphere SPI performs the functions described in the following sections:

Collecting and Interpreting Server Performance and Availability Information

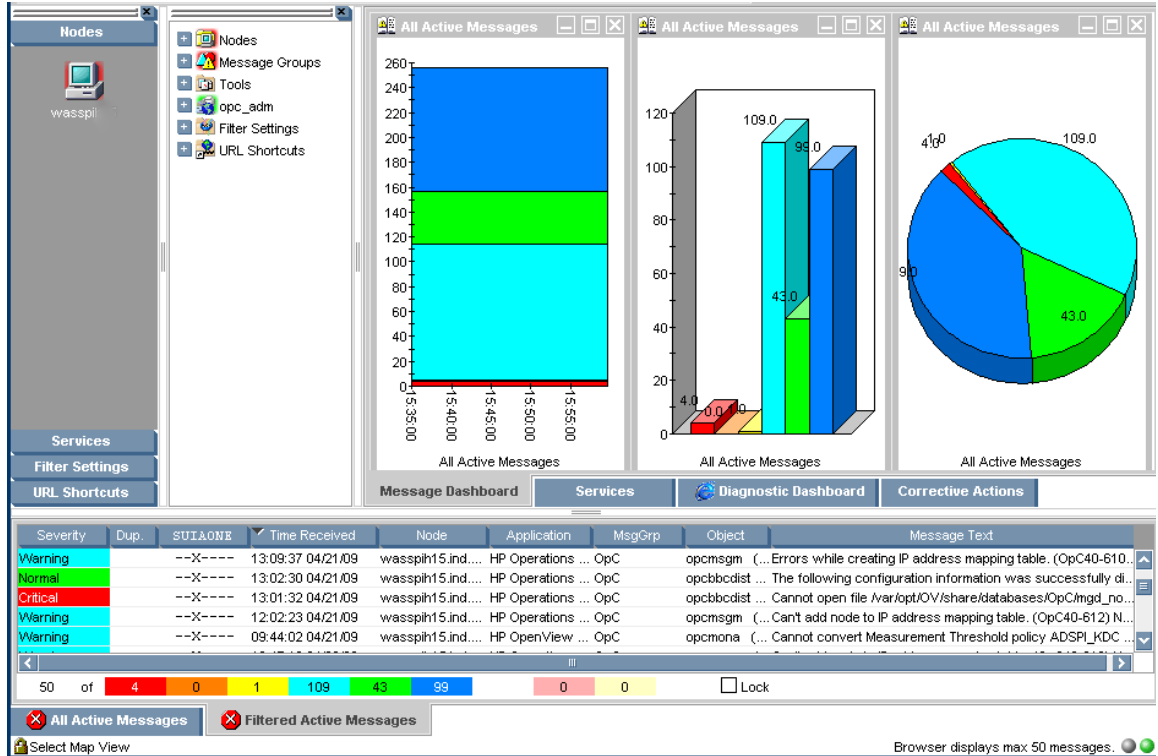
After you configure the WebSphere SPI, and deploy policies on the managed nodes, the SPI starts gathering server performance and availability data. This data is compared with the settings within the deployed policies. The policies define conditions that can occur within the WebSphere Server, such as queue throughput rates, cache use percentages, timeout rates, and average transaction times. The policies monitor these conditions against default thresholds (set within the policies) and trigger messages when a threshold has been exceeded.

Displaying Information

The WebSphere SPI policies generate messages when a threshold is exceeded. These messages can appear as:

Messages in the Message Browser – HP Operations agent software compares the values gathered for the performance and availability of WebSphere Application Server against the monitor policy settings related to those specific areas. The agent software then forwards appropriate messages to the HPOM console. These messages appear with color-coded severity levels in the HPOM message browser. To view the Message Browser, select **Integrations** → **HPOM for Unix Operational UI**.

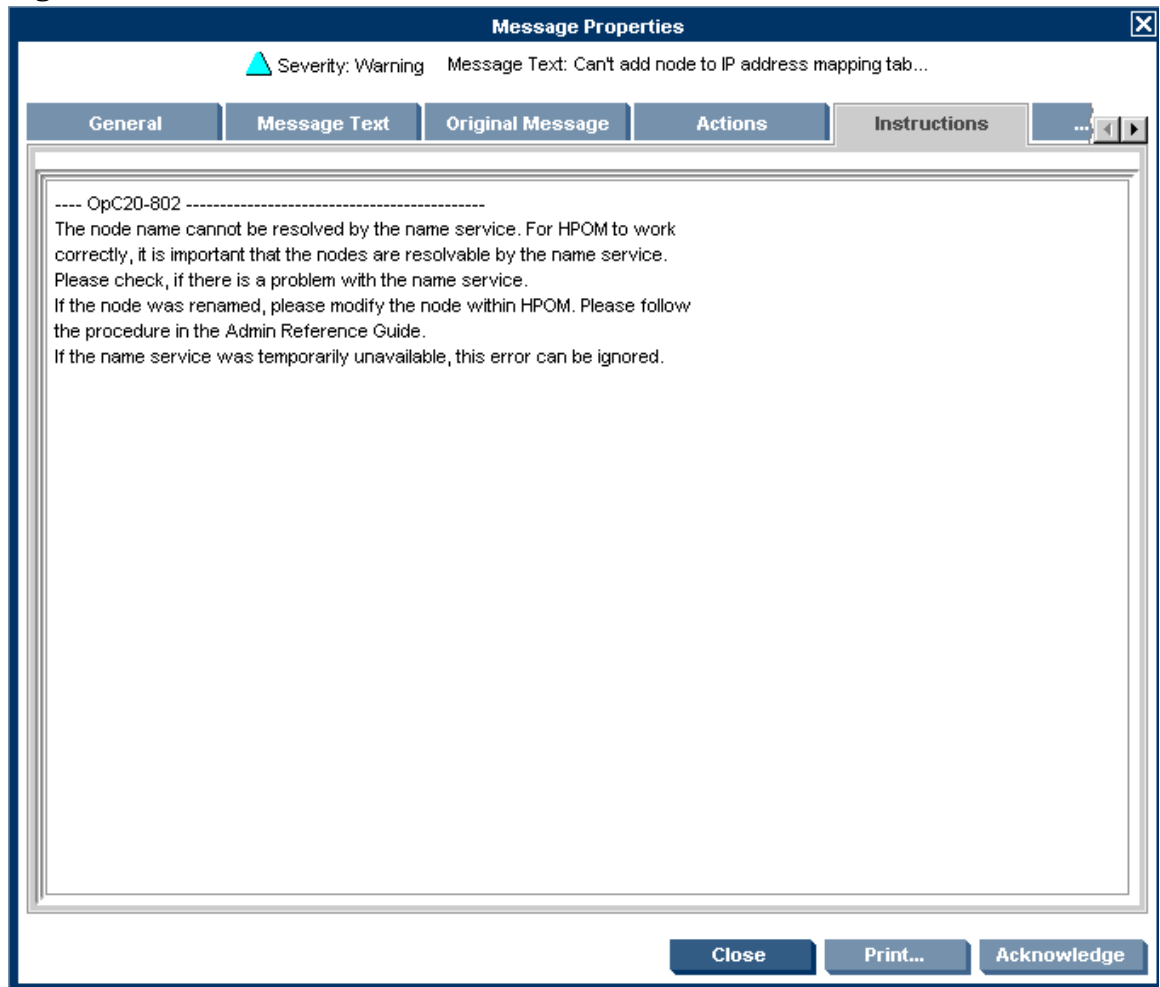
Figure 2 Message Browser



Instruction Text— Messages generated by the WebSphere SPI programs contain instruction text to help analyze and solve problems. You can manually perform corrective actions preassigned to events or they can be triggered automatically.

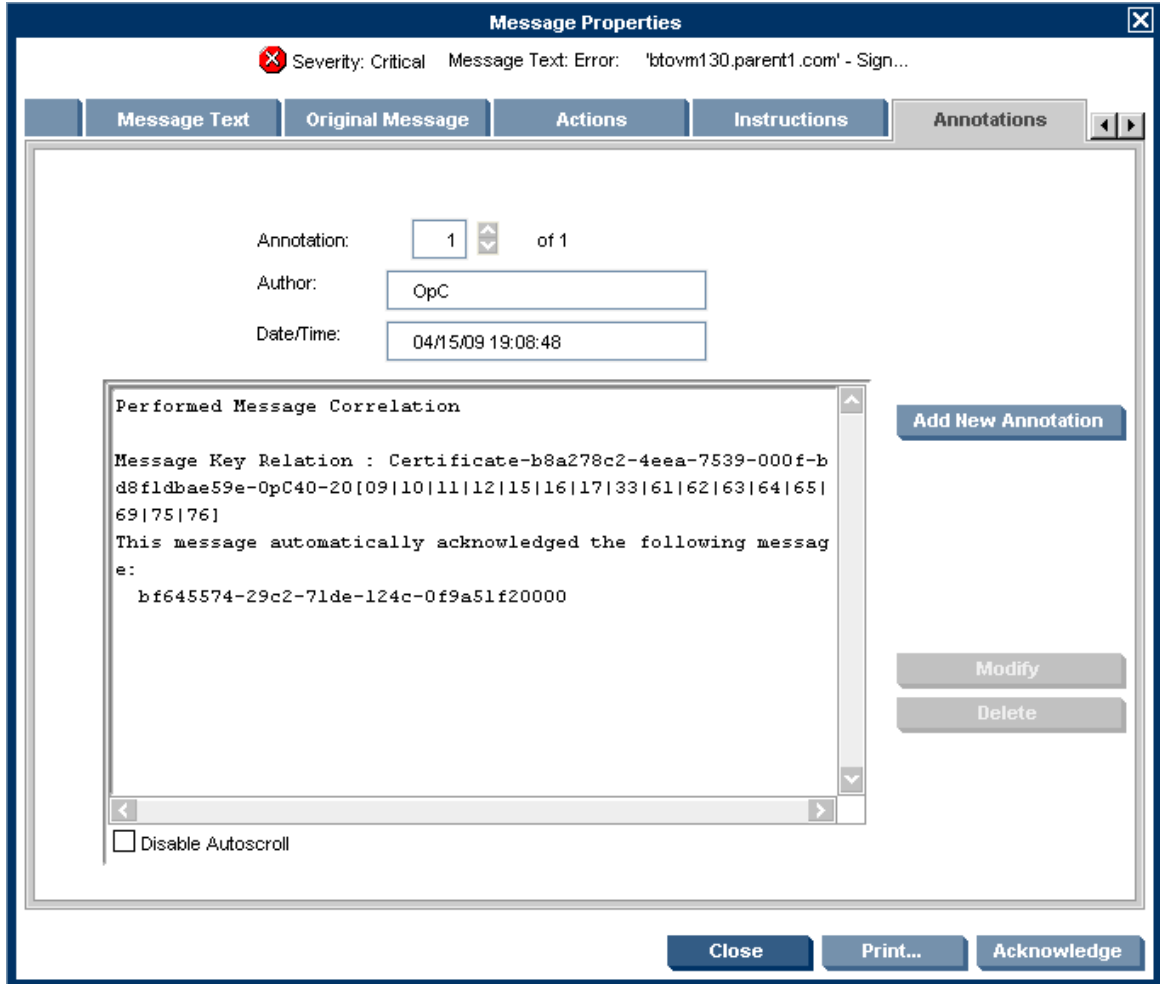
Instruction text is present in the Message Properties window. Double click the Message Text. The Message Properties window appears. To view the instruction text, click the **Instruction** tab. Instruction text is also available in the *HP Operations Smart Plug-in for IBM WebSphere Application Server Reference Guide*.

Figure 3 Instruction Text



ASCII-Text Reports– In addition to the instruction text, some messages cause automatic action reports to be generated. These reports show conditions of a specific WebSphere Application Server instance. If a report is available, you can view it by clicking the **Annotations** tab in the Message Properties window.

Figure 4 ASCII-Text Reports



Generating Reports Using HP Reporter

You can integrate the WebSphere SPI with HP Reporter to provide you with management-ready, web-based reports. The WebSphere SPI Reporter package includes the policies for generating these reports. You can install the Report package on the Reporter Windows system.

After you install the product and complete basic configuration, Reporter generates reports of summarized, consolidated data every night. With the help of these reports you can assess the performance of the WebSphere Application Server over a period of time.

Reporter uses the WebSphere SPI data to generate reports that illustrate for example, servlet request rates, transaction throughput rates, and average transaction execution time.

Graphing Data with HP Performance Manager

Metrics collected by the WebSphere SPI can be graphed. The values can then be viewed for analyzing the trend.

You can integrate the WebSphere SPI with HP Performance Manager to generate and view graphs. (use the **View WBSSPI Graphs** tool from the SPI Admin tools group to view graphs). These graphs show the values of the metrics collected by the WebSphere SPI. You can click

Perform Action to view graphed data from almost all the WebSphere SPI alarm messages. **Perform Action** is present within the **Actions** tab in the Message Properties window. The action launches your Web browser, where you can choose a graph that shows values for the metric that generated the message as well as other related metrics.

Customizing Policies and Metrics

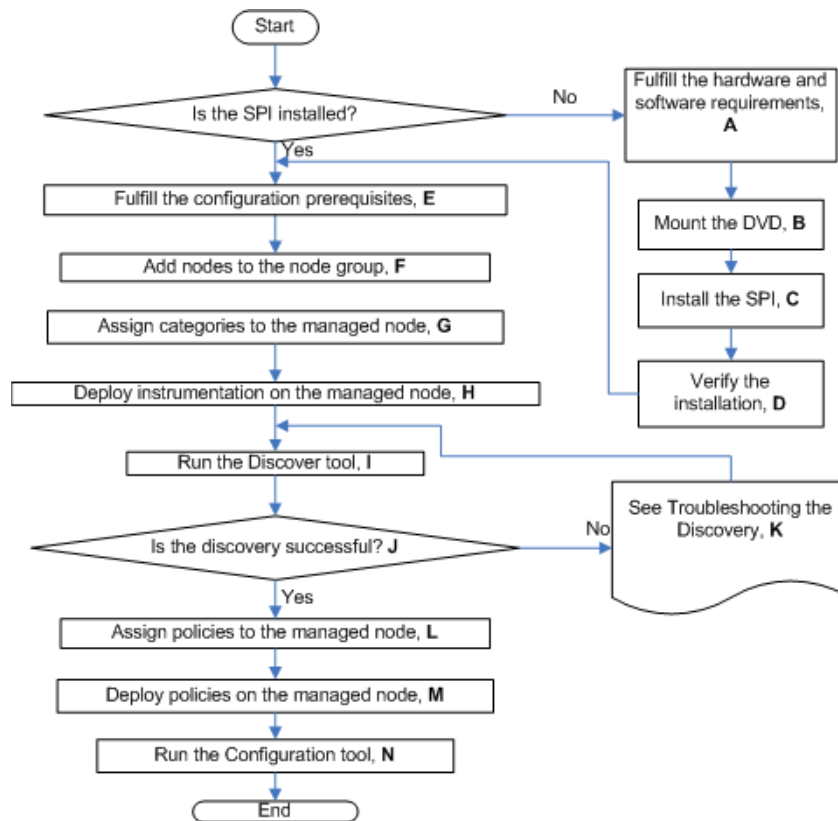
You can use the WebSphere SPI policies without customization, or modify them to suit the needs of your environment. Some modifications and customizations that you can do are:

- Modify the default policies - Within a policy, you can change the default settings for:
 - Collection interval
 - Threshold
 - Message text
 - Duration
 - Severity level of the condition
 - Actions assigned to the condition (operator-initiated or automatic)
- Create custom policy groups - You can create custom policy groups using default policies as a base. For more information, see [Chapter 5, Customizing the WebSphere SPI Policies](#).
- Create custom metrics - You can define your own metrics referred to as User Defined Metrics (UDMs), to expand the monitoring capabilities of the WebSphere SPI. For more information on UDMs, see the *HP Operations Smart Plug-in for User Defined Metrics User Guide*.

2 Installing and Upgrading the WebSphere SPI

This chapter provides information on installation of the WebSphere SPI on different environments. It discusses all the required prerequisites, instructions, and steps for installing the WebSphere SPI. The following flowchart summarizes the steps for installing and configuring the WebSphere SPI.

Figure 5 Flowchart on steps for installing and configuring the SPI for HP-UX



Click a hyperlink below to find detailed information.

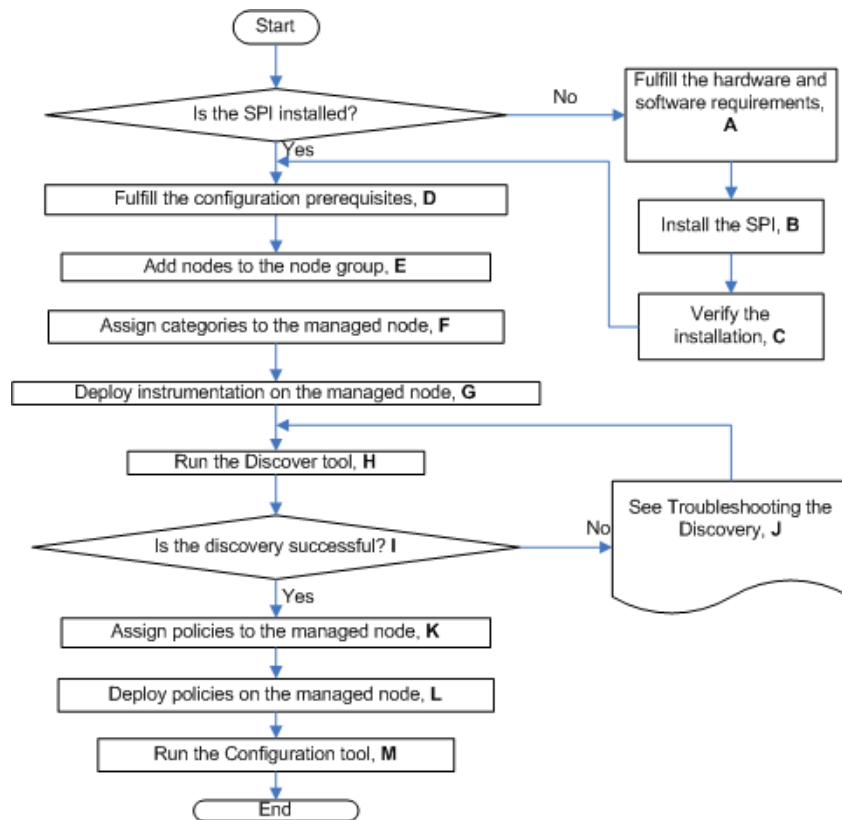
Table 1 References of the legends in the flowcharts

A	Prerequisites on page 27
B	Mounting the DVD on HP-UX on page 28
C	Install the WebSphere SPI on page 29
D	Verifying Installation on page 32
E	Prerequisites on page 37
F	Add Nodes to a WebSphere SPI Node Group on page 40

Table 1 References of the legends in the flowcharts

G	Assign Categories to the Managed Node on page 41
H	Deploy Instrumentation on the Managed Node on page 42
I	Run Discovery on page 43
J	Verify the Discovery Process on page 44
K	Troubleshooting the Discovery Process on page 105
L	Assign Policies to the Managed Node on page 45
M	Deploy the WebSphere SPI Policies on page 45
N	Run Configuration on page 46

Figure 6 Flowchart for installing and configuring the SPI for Linux and Solaris



Click a hyperlink below to find detailed information.

Table 2 References of the legends in the flowcharts

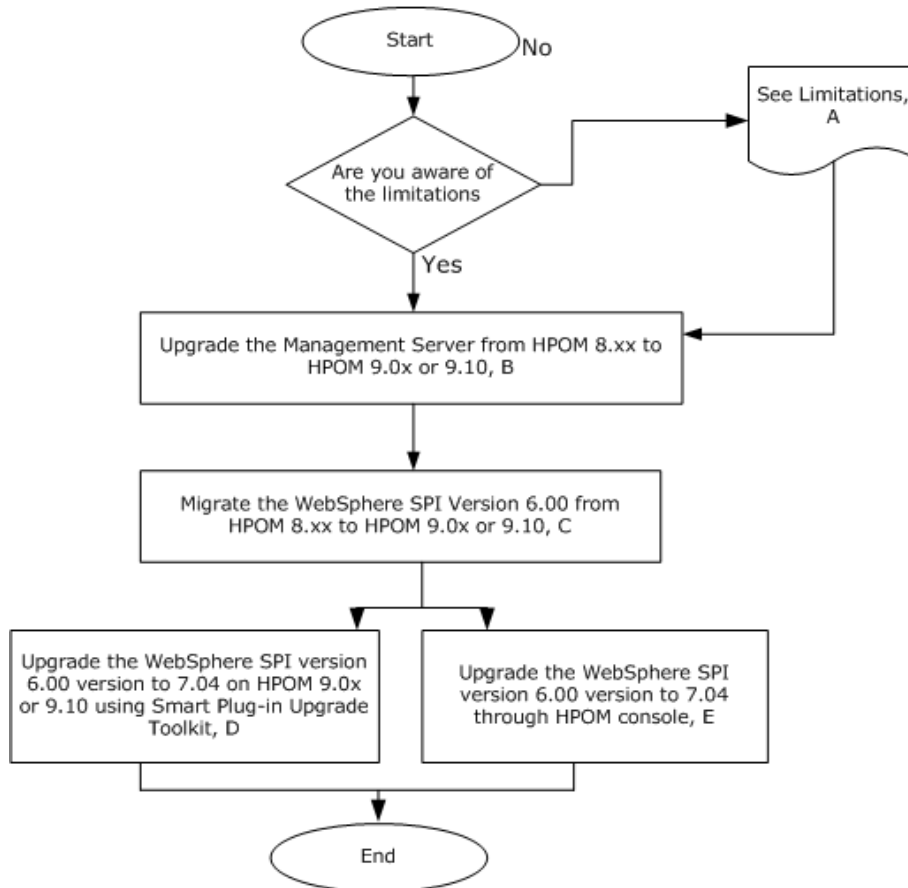
A	Prerequisites on page 27
B	Installing the SPI on the HPOM for Linux or Solaris management server on page 29
C	Verifying Installation on page 32
D	Prerequisites on page 37
E	Add Nodes to a WebSphere SPI Node Group on page 40

Table 2 References of the legends in the flowcharts

F	Assign Categories to the Managed Node on page 41
G	Deploy Instrumentation on the Managed Node on page 42
H	Run Discovery on page 43
I	Verify the Discovery Process on page 44
J	Troubleshooting the Discovery Process on page 105
K	Assign Policies to the Managed Node on page 45
L	Deploy the WebSphere SPI Policies on page 45
M	Run Configuration on page 46

The following flowchart summarizes the steps for upgrading the WebSphere SPI:

Figure 7 Flowchart to upgrade the WebSphere SPI for HP-UX, Linux, and Solaris



Click a hyperlink below to find the detailed information.

Table 3 References of the legends in the flowchart

A	Limitations on page 32
B	Upgrade the Management Server from HPOM 8.xx to HPOM 9.0x or 9.10 on page 33
C	Migrate the WebSphere SPI 6.00 from HPOM 8.xx to HPOM 9.0x or 9.10 on page 33
D	Upgrading the WebSphere SPI using the HP Operations Smart Plug-in Upgrade Toolkit on page 34
E	Upgrading the WebSphere SPI on a Standalone HPOM 9.0x or 9.10 Server through HPOM Console on page 34

Installation Packages

The WebSphere SPI version 7.04 is a patch release. You can download the patches from the following location: <http://support.openview.hp.com/selfsolve/patches>. Instructions to install a patch are available in the patch text.

The WebSphere SPI installation package includes the following:

- SPI Package
- Graph Package
- Reporter Package

These packages are available only when you install the WebSphere SPI from any one of the following:

- SPI DVD for UNIX (SPI DVD 2009)
- SPI DVD for Linux
- SPI DVD for Solaris

The following section lists the installation packages for the WebSphere SPI for HPOM:

- [Linux](#)
- [HP-UX](#)
- [Solaris](#)

Linux

SPI Package

The core package is the `HP_Operations_Smart_Plug-ins_Linux_setup.bin`, which contains all the SPI functionality. The package must be installed on a server managed by HPOM. The SPIs consists of policies and instrumentation (binaries or scripts) that monitor the application server.

Location of the main package:

```
<SPI DVD>\HP_Operations_Smart_Plug-ins_Linux_setup.bin
```


Reporting Package

The package contains the default reporter policies provided by the SPI. These policies are static and cannot be modified unless Crystal Reports 10.0 or later is installed. The Reporter gathers the data from the nodes managed by the SPI through the HPOM server, stores it in its local database, and then creates .html reports based on the default SPI report policies. The name and location of the reporting package is:

```
\WINDOWS\HP_REPORTER\WEBSPI\WBSSPI-Reporter.msi
```

Graphing Package

The package contains the default graphing policies provided by the SPI. Graphs are drawn from metrics that are collected in the datasources created by the SPI. The name and location of the graphing package are:

- For HP-UX: /HPUX/HP_PM/WEBSPI/HPOvSpiWbsG.depot
- For Windows: \WINDOWS\HP_PM\WEBSPI\HPOvSpiWbsG.msi
- For Solaris: /SOLARIS/HP_PM/WEBSPI/HPOvSpiWbsG.sparc
- For Linux: The graph templates packages for WBS SPI are contained in the main packages for Linux mentioned earlier.

HP-UX

SPI Package

The core package is the HP_Operations_Smart_Plug-ins_HPUX.depot, which contains all the SPI functionality. The package must be installed on a server managed by HPOM. The SPIs consists of policies and instrumentation (binaries or scripts) that monitor the application server.

Location: <SPI DVD>\HP_Operations_Smart_Plug-ins_HPUX.depot

Reporting Package

The package contains the default reporter policies provided by the SPI. These policies are static and cannot be modified unless Crystal Reports 10.0 or later is installed. The Reporter gathers the data from the nodes managed by the SPI through the HPOM server, stores it in its local database, and then creates .html reports based on the default SPI report policies. The name and location of the reporting package is:

```
\WINDOWS\OV_REPORTER\WEBSPI\WBSSPI-Reporter.msi
```

Graphing Package

The package contains the default graphing policies provided by the SPI. Graphs are drawn from metrics that are collected in the datasources created by the SPI. The name and location of the graphing package are:

- For Windows: \WINDOWS\OV_PM\WEBSPI\WBSSPI-OVPM.msi
- For HP-UX: The graph templates packages for WBS SPI are contained in the main packages for HP-UX mentioned earlier.

Solaris

SPI Package

The core package is the `HP_Operations_Smart_Plug-ins_Solaris_setup.bin`, which contains all the SPI functionality. The package must be installed on a server managed by HPOM. The SPI consists of policies and instrumentation (binaries or scripts) that monitor the application server.

Location: `<SPI DVD>\HP_Operations_Smart_Plug-ins_Solaris_setup.bin`

Reporting Package

This package contains the default reporter policies provided by the SPI. These policies are static and cannot be modified unless Crystal Reports 10.0 or later is installed. The Reporter gathers the data from the nodes managed by the SPI through the HPOM server, stores it in its local database, and then creates .html reports based on the default SPI report policies. The name and location of the reporting package is:

`\WINDOWS\HP_REPORTER\WEBSPI\WBSSPI-Reporter.msi`

Graphing Package

This package contains the default graphing policies provided by the SPI. Graphs are drawn from metrics that are collected in the datasources created by the SPI. The name and location of the graphing package are:

- For Windows: `\WINDOWS\HP_PM\WEBSPI\HPOvSpiWbsG.msi`
- For Linux: `/LINUX/HP_PM/WEBSPI/HPOvSpiWbsG.rpm`
- For HP-UX: `/HPUX/HP_PM/WEBSPI/HPOvSpiWbsG.depot`
- For Solaris: The graph templates packages for WBS SPI are contained in the main package for Solaris mentioned earlier.

Installation Environments

Standard Installation of SPI Components on the HPOM Server

You can install the full version of HP Performance Manager on the HPOM server. You can select to install only the SPI packages and not the graphing packages through the HP Operations Smart Plug-Ins DVD. However, if the full version of Performance Manager is installed on the same machine, the corresponding packages can be installed or uninstalled on the HPOM server.

Standalone HP Performance Manager

For such a system only the corresponding package of any SPI is enabled and available for selection from the HP Operations Smart Plug-Ins DVD. For example, if a system has only HP Performance Manager installed, the graph package of the WebSphere SPI could be installed on it.

Standard Installation in an HPOM Cluster Environment for HP-UX

In an HPOM cluster environment, you must have installed HPOM 9.0x server on each of the nodes in the cluster. You can install the SPI on each of the nodes in the cluster environment.

Prerequisites

Fulfill the hardware and software requirements before installing the SPI. Install the HPOM server and discovery package before installing the WebSphere SPI. It is not necessary to stop HPOM sessions before beginning the WebSphere SPI installation.

Hardware Requirements

See the *HP Operations Manager for Unix* documents for information on hardware requirements for the management server. See the following Support Matrix (SUMA) link, for information on hardware requirements for the managed nodes:

<http://support.openview.hp.com/selfsolve/document/KM323488>

Software Requirements

Ensure that the following software requirements are met prior to the installation of the WebSphere SPI:

On the Management Server:

HP-UX

- HP Operations Manager for UNIX: 9.0x or 9.10
- HP Performance Manager: 8.20 (required if you want to generate graphs)
- HP Reporter: 3.80 (required if you want to generate web-based reports)
- HP Operations SPI Data Collector (DSI2DDF): 2.40 (for HP-UX, automatically installed while installing the SPI on the management server)
- HP SPI Self-Healing Services (SPI-SHS-OVO): 3.00
- JMX Component (JMXSPI): 7.00
- HP Operations SPI Upgrade Toolkit 2.00

DSI2DDF, SPI-SHS-OVO, and JMXSPI are automatically installed while installing the SPI on the HP-UX management server for the first time.

Linux

- HP Operations Manager for Linux: 9.0x or 9.10
- HP Performance Manager (Linux): 8.21 (required if you want to generate graphs)
- HP Reporter: 3.80 (required if you want to generate web-based reports)
- HP Operations SPI Data Collector (DSI2DDF): 2.41
- HP SPI Self-Healing Services (SPI-SHS-OVO): 3.01
- JMX Component (JMXSPI): 7.01

- HP Operations SPI Upgrade Toolkit: 2.01

Solaris

- HP Operations Manager for Solaris: 9.0x or 9.10
- HP Performance Manager: 8.21 (required if you want to generate graphs)
- HP Reporter: 3.80 (required if you want to generate web-based reports)
- HP Operations SPI Data Collector (DSI2DDF): 2.41
- HP SPI Self-Healing Services (SPI-SHS-OVO): 3.02
- JMX Component (JMXSPI): 7.02
- HP Operations SPI Upgrade Toolkit: 2.02

You have to select the DSI2DDF, SPI-SHS-OVO, and JMXSPI components while installing the SPI on the Solaris management server for the first time.

On the Managed Nodes (for HP-UX, Solaris and Linux):

- HP Performance Agent: 5.00 (required if you want to use HP Performance Agent for data logging)
- HP Operations agent (version 8.60) must be installed and configured

See the following Support Matrix (SUMA) link, for more information on supported versions of HP Operations Manager, Application Servers, HP Performance Agent, HP Operations agent, HP Performance Manager, and HP Reporter:

<http://support.openview.hp.com/selfsolve/document/KM323488>

Installing the WebSphere SPI

Complete the tasks in this section to install the WebSphere SPI.

Installing the SPI on HP-UX

You must install the HP Operations Manager (HPOM) management server and discovery package before installing the WebSphere SPI. It is not necessary to stop HPOM sessions before beginning the WebSphere SPI installation. The discovery package and WebSphere SPI are available on the HP Operations Smart Plug-ins DVD.

Mounting the DVD on HP-UX

To mount the DVD on HP-UX:

- 1 Log on as root user.
- 2 Set the user root's umask by entering:
`umask 027`
- 3 Create a directory to mount the DVD:
`mkdir /<mount_point>`

For example: `mkdir /dvdrom`

- 4 Insert the DVD into the disk drive and mount it as user root by entering:
mount /dev/<dvdrom_drive_name> /<mount_point>

For example, for a local DVD, you can enter:

```
mount /dev/dsk/c0t2d0 /dvdrom
```

You can also run SAM and mount the DVD to a specific path in the Disks and File *Systems* window.

Install the WebSphere SPI

You can install the WebSphere SPI on the HP-UX management server.



The instructions that follow cover a command line swinstall installation. You can also use the graphical user interface. If you are want to create UDMs, you must also install the SPIJMB software bundle. For more information about this software bundle, see the *HP Operations Smart Plug-in for User Defined Metrics User Guide*.

For an HP-UX 11.31 IA management server, type:

```
swinstall -s /dvdrom/HPUX/HP_Operations_Smart_Plug-ins_HPUX.depot  
WBSSPI
```

Installing the SPI on the HPOM for Linux or Solaris management server

To install the SPI on the Linux or Solaris management server, perform any one of the following procedures:

- Installing the SPI through Graphical User Interface
- Installing the SPI through Command Line Interface

Installing the SPI through Graphical User Interface

To install the WebSphere SPI using X-Windows client software:

- 1 Log on as a **root** user.
- 2 Insert the HP Operations Smart Plug-ins DVD into the DVD drive of the Linux or Solaris management server. Mount the DVD if necessary.
- 3 Start the X-windows client software and export the DISPLAY variable by typing the following command:

```
export DISPLAY=<ip address>:0.0
```

- 4 To start the installation, type one of the following commands, according to your management server:

```
./HP_Operations_Smart_Plug-ins_Linux_setup.bin
```

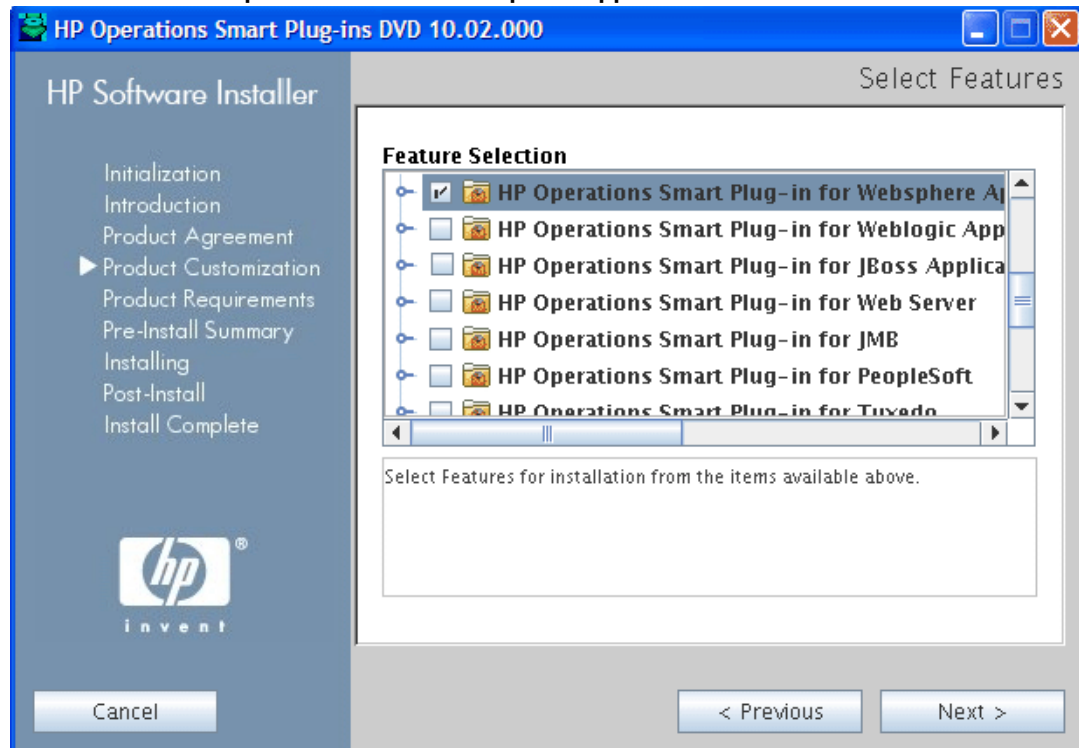
or

```
./HP_Operations_Smart_Plug-ins_Solaris_setup.bin
```

The introductory window appears.

- 5 Select the language from the drop-down list and click **OK**. The Introduction (Install) window appears.
- 6 Click **Next**. The License Agreement window appears.

- 7 Select **I accept the terms of the License Agreement** button and click **Next**. The Select Features window appears.
- 8 Select the **HP Operations SPI for WebSphere Application Server** check box and click **Next**.



➤ By default, the HP Operations Smart Plug-in Common Components are selected.

The Install Check window opens.

- 9 Click **Next**. The Pre-Install Summary window opens.
- 10 Click **Install**.

While installing, you can see the Force reinstallation of already installed component packages check box. You can use either of the following options:

- Select the Force reinstallation of already installed component packages check box to reinstall the selected components, as applicable.
- Clear the Force reinstallation of already installed component packages check box to prevent reinstallation of the selected HP Software components, as applicable. Clearing the check box does not change the currently installed software components.

If the installation fails, you can quit installation. Click **Quit** to stop the installation. This does not uninstall the components installed till then.

The Installing window appears. The Install Complete window appears once the SPI is uninstalled.

- 11 Click **Done** to complete the installation.

Installing the SPI through Command Line Interface

To install the WebSphere SPI through command line interface:

- 1 Log on as a **root** user.

- 2 Insert the HP Operations Smart Plug-ins DVD into the DVD drive of the Linux or Solaris management server. Mount the DVD if necessary.
- 3 To start the installation, type one of the following commands, according to your management server:

```
./HP_Operations_Smart_Plug-ins_Linux_setup.bin -i console
```

or

```
./HP_Operations_Smart_Plug-ins_Solaris_setup.bin -i console
```

- 4 When the prompt, 'Choose Locale...' appears, press the number corresponding to the language you want to choose.
- 5 Press **Enter** to continue. The Introduction screen appears.
- 6 Press **Enter** to continue.
- 7 When the prompt, 'I accept the terms of the License Agreement' for the License information appears, press **Y** to accept the terms and continue installation.
- 8 When the prompt, 'Please select Features' for the selection of the feature appears, press the number corresponding to the feature you want to install.
 - ▶ When you have installed one SPI on the Linux or Solaris management server and want to install another SPI on the server, you have to reselect the previously installed SPI and select the required SPI from the Modify option. If you do not reselect the previously installed SPI, it removes the previously installed SPI and installs the selected SPI on the Linux or Solaris management server.
- 9 Press **Enter**. A series of message appears. Follow the instructions as displayed in the message.

When the installation is complete, you will receive a message which states that the installation is completed successfully.

In an HPOM Cluster Environment for HP-UX

You must first install the HPOM management server on each node in the cluster. When the management server cluster installations are complete, the setup for the installation of the WebSphere SPI is ready.



Before installing, ensure that sufficient disk space (500 MB) is available on each management server for the WebSphere SPI you plan to install. Cancelling the installation process before completion could result in partial installations and require manual removal of the partially installed components.

After installing the HPOM management server:

For the first installation (Node A) and all remaining installations in the cluster — Follow the standard installation procedure by either making the product choices or typing the name of the SPI component you want to install. Once you complete the installation on Node A, proceed to the next node. Repeat the same procedure proceeding from one node to another until you have completed installing the SPI on each of the nodes in the cluster.

Installing the SPI on the Cluster-Aware Management Server for HP-UX

Complete all the tasks in the section [Installing the SPI on HP-UX](#) on page 28 and then proceed to the next management server until the installation on every management server in the cluster is complete.



The HPOM console will not function properly until installations are completed on all nodes in the cluster.

Verifying Installation

HP-UX - Type the command `swlist` to verify the installation of the WebSphere SPI on the management server.

Linux - Type the command `rpm -qa` to verify the installation of the WebSphere SPI on the management server.

Solaris - Type the command `pkginfo -l HPOvSpiWbs` to verify the installation of the WebSphere SPI on the management server.

Linux, HP-UX and Solaris - Verify the `WBSSPI_Install.log` file to check if the installation is successful. The path of this file is `/var/opt/OV/log/SPIInstallLogs`.

Upgrading the WebSphere SPI

You can upgrade the WebSphere SPI from HPOM for UNIX version 8.xx to HPOM for UNIX, Linux, or Solaris version 9.0x or 9.10.

Limitations

Note the following when you plan to install the WebSphere SPI 7.04 on HPOM 9.0x or 9.10:

- You must complete the migration process from HPOM 8.xx to HPOM 9.0x or 9.10 before upgrading the WebSphere SPI.
- After upgrading to the HPOM 9.0x or 9.10, you must move all the managed nodes to the WebSphere SPI 7.04.
- Monitoring a node by combination of SPIs from SPI DVD 2008 and SPI DVD 2009 or SPI DVD 2010 is not supported.
- If you have multiple WebSphere SPI versions deployed on HPOM, you must configure newly added managed nodes using the WebSphere SPI 7.04. In addition, no configuration is possible on the existing or old managed nodes monitored by the WebSphere SPI 6.00.
- Before you start the migration process of HPOM, install all the available patches for the WebSphere SPI 6.00. After you install the WebSphere SPI 7.04, no patches or hotfixes available for WebSphere SPI 6.00 can be installed on the HPOM server.
- To run the user interface related to WebSphere SPI 7.04, you must install X-windows client software on the system from which you will start the HPOM for UNIX 9.0x or 9.10 server operator user interface.
- Before you upgrade the WebSphere SPI 7.04, you must take a backup of the content available in the `/opt/OV/wasspi/wbs` directory.

To upgrade the earlier versions of the WebSphere SPI to WebSphere SPI 7.04, perform the following tasks:

- Upgrade the Management Server from HPOM 8.xx to HPOM 9.0x or 9.10
- Migrate the WebSphere SPI 6.00 from HPOM 8.xx to HPOM 9.0x or 9.10
- Upgrade the WebSphere SPI 6.00 to WebSphere SPI 7.04 on HPOM 9.0x or 9.10



You must take the backup of the content in the `/opt/OV/wasspi/wbs` directory before upgrading the SPI to the version 7.04, in case you want to reuse the old content. When you upgrade the SPI to the new version, the old content in the `/opt/OV/wasspi/wbs` directory will be lost permanently.

Upgrade the Management Server from HPOM 8.xx to HPOM 9.0x or 9.10

Follow the steps documented in the following guides:

- *HP Operations Manager for UNIX 9.00 Installation Guide* for upgrading or migrating HPOM 8.xx to 9.0x.
- *HP Operations Manager for UNIX 9.10 Installation Guide* for upgrading or migrating HPOM 9.0x to 9.10.

Migrate the WebSphere SPI 6.00 from HPOM 8.xx to HPOM 9.0x or 9.10

The instrumentation files and other SPI specific data are migrated while migrating or upgrading HPOM for UNIX 8.xx server (where the WebSphere SPI 6.00 is installed) to HPOM for UNIX 9.0x or 9.10. Some SPI specific data, however, must be migrated manually.

Migrate the HPOM from one system to another

Install HPOM for UNIX version 9.0x or 9.10 on a new system. To perform the migration from one system to another:

- 1 After you complete migrating HPOM for UNIX 8.xx to HPOM for UNIX 9.0x or 9.10, create the following directories on the target HPOM for UNIX 9.0x or 9.10 server:

```
/var/opt/OV/wasspi/wbs/
```

```
/opt/OV/SPISvcDisc/conf/WBSSPI/
```

```
/opt/OV/wasspi/wbs/
```

```
/var/opt/OV/share/conf/SPISvcDisc/WBSSPI/
```

- 2 Copy the files present in the directories created in step 1 from HPOM for UNIX 8.xx to HPOM for UNIX 9.0x or 9.10 server at their respective folders.
- 3 Copy the following files from HPOM for UNIX 8.xx to HPOM for UNIX 9.0x or 9.10 server at their respective directories:

```
/opt/OV/SPISvcDisc/conf/wasspi_wbs_DiscConfig.sh
```

```
/opt/OV/newconfig/inventory/HPOvSpiWbs.xml
```

Upgrade the WebSphere SPI 6.00 to WebSphere SPI 7.04 on HPOM 9.0x or 9.10

You can upgrade the WebSphere SPI either using the HP Operations Smart Plug-in Upgrade Toolkit (SPI Upgrade Toolkit) or through the HPOM for UNIX console.

Upgrading the WebSphere SPI using the HP Operations Smart Plug-in Upgrade Toolkit

The HP Operations Smart Plug-in Upgrade Toolkit (SPI Upgrade Toolkit) version 2.0x helps you upgrade the WebSphere SPI to a higher version while retaining the customizations done on policies. During the WebSphere SPI upgrade process, the SPI Upgrade Toolkit enables you to store the modifications done on the customer version of policies. For a specific policy, the SPI Upgrade Toolkit analyzes and compares three versions—base, customer, and factory—and helps you select the settings of the base, customer, or factory version of the policy, depending on your requirement. To upgrade the WebSphere SPI using the SPI Upgrade Toolkit, follow the instructions defined in *HP Operations Smart Plug-in Upgrade Toolkit UNIX User Guide*.

Upgrading the WebSphere SPI on a Standalone HPOM 9.0x or 9.10 Server through HPOM Console

To upgrade the WebSphere SPI on a standalone HPOM 9.0x or 9.10 server:

- 1 Rename the policy and tool group for WebSphere SPI from *SPI for WebSphere* to *SPI for WebSphere_OLD*. Rename both the Name and the Label (for example, *WBSSPI:TOOLS* to *WBSSPI:TOOLS_OLD*).
- 2 Un-assign the policies or policy groups assigned to the node.
- 3 Kill the rmid and all Java processes started by the SPI on the node.
- 4 Delete the old policies, instrumentation, and datasources on the node manually. The existing data is deleted. Hence, take a backup of your existing data.



Manually delete the existing WebSphere SPI datasource when you upgrade the SPI. For example, `ddfutil /var/opt/OV/wasspi/wbs/datalog/graph.log -rm a11`. A new datasource is created and the existing data is lost. The datasource is deleted irrespective of whether you are using CODA or HP Performance Agent. When you upgrade from a previous installation, all your configuration entries are preserved.

- 5 Install the WebSphere SPI by performing the steps in [Installing the WebSphere SPI](#) on page 28.
- 6 Configure the SPI by performing the steps in [Chapter 3, Configuring the WebSphere SPI](#).

Install the New Report Package (Optional)

If you installed an older version of the WebSphere SPI report package (on your Windows system running Reporter), you must uninstall it, and install the new WebSphere SPI report package.

- 1 On the Windows system running Reporter, from the Control Panel, double-click the **Add/Remove Programs** icon.
- 2 Select the WebSphere SPI report package and click **Remove**.
- 3 Follow the steps to install the WebSphere SPI report package in [Integrating with HP Reporter](#) on page 92.

Install the New Graph Package (Optional)

If you installed an older version of the WebSphere SPI graph package (on your system running HP Performance Manager), you must uninstall it and install the new WebSphere SPI graph package.

On a Windows system running HP Performance Manager:

- 1 From the Control Panel, double-click the **Add/Remove Programs** icon.
- 2 Select the WebSphere SPI graph package (HP Operations SPI for WebSphere Application Server - Graphing Component Integration) and click **Remove**.
- 3 Follow the steps to install the WebSphere SPI report package in [Integrating with HP Performance Manager](#) on page 94.

On an HP-UX system running HP Performance Manager that is not the HPOM management server, follow these steps (if HP Performance Manager is installed on the HPOM management server, the files are automatically updated when you install the SPI software):

- 1 Verify that the graph package is installed by typing `swlist | grep WBSSPI-GRAPHS`.
- 2 Type `swremove WBSSPI-GRAPHS`.
- 3 Follow the steps to install the WebSphere SPI graph package in [Integrating with HP Performance Manager](#) on page 94.

On a Solaris system running HP Performance Manager that is not the HPOM management server, follow these steps (if HP Performance Manager is installed on the HPOM management server, the files are automatically updated when you install the SPI software):

- 1 Verify that the graph package is installed by typing `/usr/bin/pkginfo HPOvSpiWbsG`.
- 2 Type `/usr/sbin/pkgrm HPOvSpiWbsG`.
- 3 Follow the steps to install the WebSphere SPI graph package in [Integrating with HP Performance Manager](#) on page 94.

3 Configuring the WebSphere SPI

To successfully configure the WebSphere SPI, you must complete all configuration prerequisites, WebSphere SPI configuration for managed nodes and the management server, and additional configuration based on your environment.

Prerequisites

Log on to HPOM as an administrator. The Administration user interface window appears. Complete the following tasks before configuring the WebSphere SPI:

- [Assign Operator Responsibilities for opc_adm](#)
- [Assign Tools to the Operator](#)
- [Verify the Application Server Status](#)
- [Collect WebSphere Login Information](#)
- [Connect using JSR 160](#)
- [Update WebSphere's SDK](#)

Assign Operator Responsibilities for opc_adm

To assign operator responsibilities for opc_adm:

- 1 Select **All Users** → **<Operator Name>**. For example, opc_adm.
The User “opc_adm” window appears.
- 2 To change a User’s responsibility, select **Edit Responsibilities....** from the drop-down list as shown in the following figure.
- 3 Select all check boxes for WBSSPI and WebSphere Message Groups.
- 4 Assign the WBSSPI Node or Message Groups to any other appropriate operators.
- 5 Click **Close**.

Assign Tools to the Operator

To assign tools to the operator:

- 1 Click **Browse** and then click **Tool Bank**. In the tool Bank window select the SPI for WebSphere Application Server tool group.
- 2 Select **Assign to User/Profile...** from the **Choose an Action** drop-down list and click **>>** to submit.

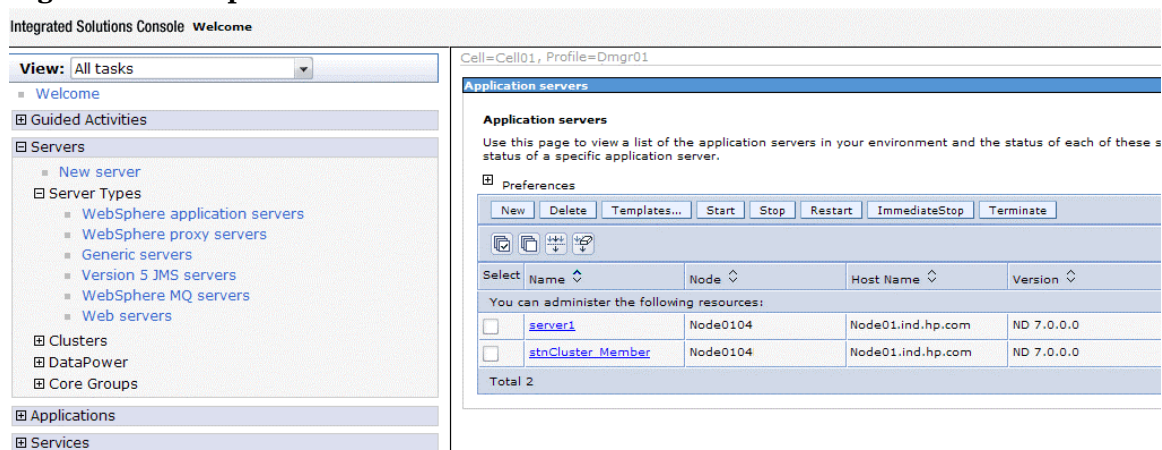
The Selector window appears.

- 3 Under the Selector window, click **All Users**.
- 4 Select the operator to which you want to assign the tools.
- 5 Click **OK**. The WebSphere SPI tools are assigned to the operator.

Verify the Application Server Status

Verify that your application servers are running. For WebSphere Application Server version 6.0 and above, check the status of the server from the WebSphere administrative console.

Figure 8 WebSphere Administrative Console.



If you cannot verify the status of the server using the administrative console, run the following commands on the managed node:

- UNIX and Linux: `<WebSphere_Install_Dir>/bin/serverStatus.sh -all`
For example: `/opt/WebSphere/AppServer/bin/serverStatus.sh -all`
- Windows: `<WebSphere_Install_Dir>\bin\serverStatus.bat -all`
For example: `C:\Program Files\WebSphere\AppServer\bin\serverStatus.bat -all`

Collect WebSphere Login Information

If security is enabled on the WebSphere Server, collect the username and password for each WebSphere Admin Server. The user must have the local WebSphere administrator privileges assigned for the WebSphere Admin Server.

The username and password are required for the WebSphere SPI discovery process to gather basic configuration information and by the WebSphere SPI data collector to collect metrics.

Configuration of WebSphere SPI is simplified if the same username and password are used by each WebSphere Admin Server.

If you are using WebSphere version 6.0 or later, you should be able to use the username and password for users/groups assigned to the administrator or operator role.

If you are using LDAP directory to access the WebSphere Console from LDAP, you must create a user account similar to the user account of LDAP in the local WebSphere instance. You must grant Administrator privileges to this user.

Connect using JSR 160

You can configure the WebSphere Application Server 6.1 or later to use JSR 160 connection to connect to the WebSphere Application Server. JSR160 is a standard way to connect to remote JMX enabled applications using RMI. By default, the JSR 160 connection is disabled.

To enable JSR 160 connection set the **JSR160** flag in the SPI Config file to **true** (By default, this flag is set to **false**). The SPIConfig file is present in the `<AgentDir>/conf/wbsspi` directory.

If you use JSR 160, the application server can run in “security enabled” or “security disabled” mode. In the “security disabled” mode the collector can run in both TRANSIENT mode (started and stopped at regular intervals by `wasspi_ca`) and PERSISTENT mode (once started, it remains until the Application server monitoring is stopped), but in the “security enabled” mode the collector can only run in the Transient mode. To set the collector in Transient mode, add **COLLECTOR_MODE=TRANSIENT** at the end of the SPIConfig file. By default, it will be set to PERSISTENT.

If you are using WebSphere Application Server 6.1 or later, before starting the collector you must set the following values for the attributes in the `<WebSphere_HOME>/profiles/<profile_name>/properties/sas.client.props` file. Set these values for all the profiles that you want to monitor.

- Set the value of `loginSource` attribute to **properties** (the default value is **prompt**).
com.ibm.CORBA.loginSource=properties
- Set the value of `loginUserId` attribute to the WebSphere admin user id and `loginPassword` attribute to the WebSphere admin password:
com.ibm.CORBA.loginUserId=<admin_user>
com.ibm.CORBA.loginPassword=<admin_password>

If you do not update the `sas.client.props` file, the collector will fail.



After updating the `sas.client.props` file, you *must* restart the WebSphere Application Server, if it is running.

Update WebSphere’s SDK

For WebSphere Application Server 6.1 running on Windows nodes, you must update IBM Java SDK 1.5 to level SR4 or later (Java SDK 1.5 SR4 or later) or the collector may fail.

You can download Java SDK 1.5 SR4 or later from <http://www-1.ibm.com>.

Configuring the WebSphere SPI

To configure WebSphere SPI, from the management server, complete the following tasks:

- 1 Add Nodes to a WebSphere SPI Node Group
- 2 Assign Categories to the Managed Node
- 3 Deploy Instrumentation on the Managed Node

- 4 Run Discovery
- 5 Verify the Discovery Process
- 6 Assign Policies to the Managed Node
- 7 Deploy the WebSphere SPI Policies
- 8 Run Configuration

Add Nodes to a WebSphere SPI Node Group

The WebSphere SPI automatically creates the following three node groups that are assigned to the corresponding WebSphere High, Medium, or Low policy group:

- WebSphere-High
- WebSphere-Medium
- WebSphere-Low


When you assign a managed node to a WebSphere SPI node group, you are also assigning the WebSphere SPI Discovery policies you want to deploy on the node.



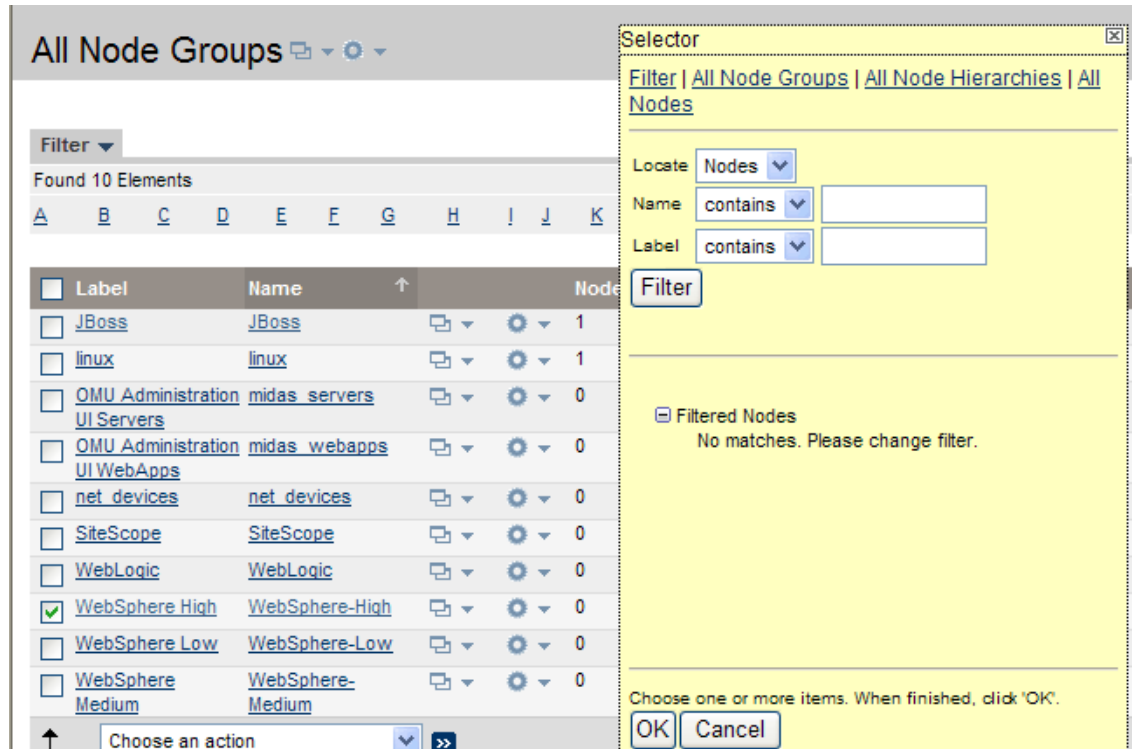
When data collection for the policy group begins, the PMI (Performance Monitoring Infrastructure) level of the node is adjusted as necessary to comply with the policy group's impact level. For example, data collection for a WebSphere High Impact group results in a PMI level adjustment to High for the node if the WebSphere PMI level is currently not at high. For more information, see [WebSphere Policy Groups and System PMI Levels](#) on page 72.

The High policy group contains all the WebSphere SPI metrics, while the Medium group contains Medium and Low metrics, and the Low group contains only Low metrics.

To add nodes to a WebSphere SPI node group:

- 1 Open the Node Bank window and select a WebSphere SPI Node Group (WebSphere-High or WebSphere-Low or WebSphere-Medium).
- 2 Select **Assign Nodes...** from the **Choose an Action** drop-down list and click  to submit.


The Selector window appears.



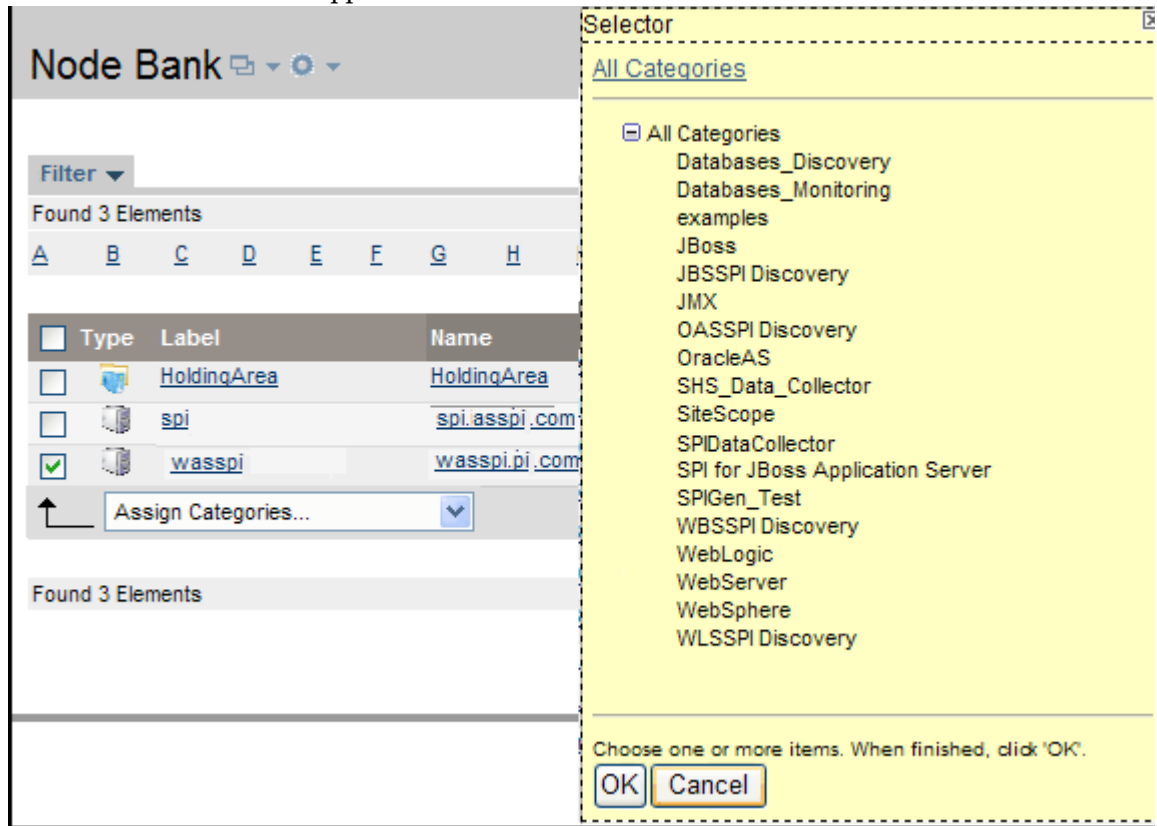
- 3 Click **All Nodes**.
- 4 Select the nodes running WebSphere Application Server.
- 5 Click **OK**.

Assign Categories to the Managed Node

To assign categories to the managed node:

- 1 Open the Node Bank window and select the managed nodes.
- 2 Select **Assign Categories...** from the **Choose an Action** drop-down list and click  to submit.


The Selector window appears.

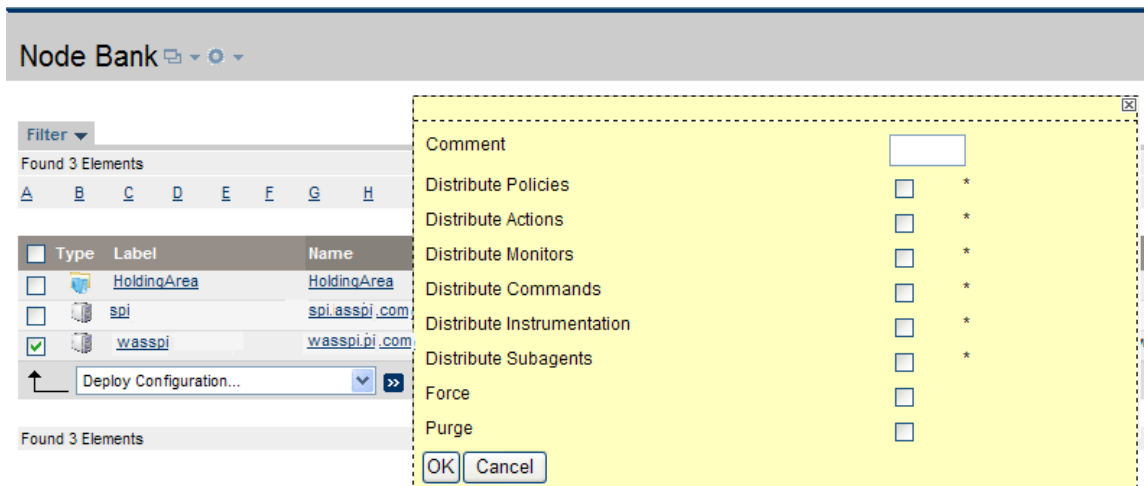


- 3 Select the **WebSphere**, **WBSSPI Discovery** (optional), **JMX**, **SHS_Data_Collector**, and **SPIDataCollector** categories.
- 4 Click **OK**.

Deploy Instrumentation on the Managed Node

To deploy instrumentation on the managed node:

- 1 Open the Node Bank window and select the management server.
- 2 Select **Deploy Configuration...** from the **Choose an Action** drop-down list and click  to submit.



- 3 Select **Distribute Instrumentation** by selecting the corresponding check box.
- 4 Click **OK**. The instrumentations are deployed.

Run Discovery

To run discovery:

- 1 From the HPOM console, select **Integrations** → **HPOM for Unix Operational UI**.
- 2 Select one or more nodes on which you want to launch Discover or Configure WBSSPI tool. To invoke WebSphere interfaces, see [Launching GUIs](#) on page 68.
- 3 Right-click a node and select **Start** → **SPI for WebSphere** → **SPI Admin** → **Discover or Configure WBSSPI**.

The Tool Selector window appears.

- 4 Select the Launch Discover Tool radio button and click **OK**. By default, the Launch Configure Tool radio button is selected. The Introduction window appears.
- 5 Click **Next**. The Configuration Editor appears.
- 6 Set the LOGIN, PASSWORD, HOME, and JAVA_HOME properties in the Configuration editor.

It is mandatory to set the PROFILE_HOME property along with the HOME property to discover WebSphere on Hypervisor Edition or profiles created outside the HOME directory. For more information on discovery of WebSphere on Hypervisor Edition, see [Discovery on Hypervisor Edition](#) on page 56.

► Make sure that the LOGIN, PASSWORD, JAVA_HOME, and HOME properties are set because these are mandatory properties. In earlier versions of the SPI, only LOGIN and PASSWORD were required properties.

- α Select LOGIN/PASSWORD from the **Select a Property to Set...** drop-down list.

The Set Access Info for Default Properties window appears.



The screenshot shows a dialog box titled "WBSSPI Discover Tool: Set Access Info for Default Prop...". The dialog has a blue title bar with standard window controls. The main content area is light gray and contains the following text: "Please enter the Login and Password information. This information is required by the SPI to access a secured application server's environment." Below this text are three input fields: "Login", "Password", and "Verify Password". The "Login" field is currently empty and has a red border. At the bottom of the dialog are two buttons: "OK" and "Cancel".

Enter the username and password collected in [Collect WebSphere Login Information](#) on page 38. The LOGIN and PASSWORD properties are set to this information.

The LOGIN and PASSWORD properties set in this window are used as the default WebSphere Admin Server login and password (they are set at the global properties level). This implies that if no NODE level or server-specific LOGIN and PASSWORD properties are set, this WebSphere login and password are used by the WebSphere SPI to log on to all WebSphere Admin Servers. For more information about the configuration structure, see [Structure](#) on page 119.

If the WebSphere Admin Server login and password are the same for all WebSphere application servers on all HPOM managed nodes, set the LOGIN and PASSWORD properties in the Set Access Info for Default Properties window and click **OK**.

If the WebSphere Admin Server login and password are different for different instances of WebSphere, you must customize the WebSphere SPI configuration by setting the LOGIN and PASSWORD properties at the NODE or server-specific level (for more information about the configuration structure, see [Structure](#) on page 119) and click **OK**:

- b Select HOME from the **Select a Property to Set...** drop-down list and click **Set Property**. Set the value for HOME.
 - c Select JAVA_HOME from the **Select a Property to Set...** drop-down list and click **Set Property**. Set the value for JAVA_HOME.
- 7 Click **Next** to save any changes and exit the editor. The Confirm Operation window appears.
- 8 Verify the nodes on which the operation is to be performed. Click **OK**.
 -  If you click **Cancel** and made changes to the configuration, those changes remain in the configuration on the management server. To make the changes to the selected managed nodes' configuration, you must select those nodes, start the Discover or Configure WBSSPI tool, launch the Discover tool, click **Next** from the configuration editor, and then click **OK**.
 -  Wait for the discovery process to complete before going to the next task. The discovery process might take several minutes to complete.

Verify the Discovery Process

To verify the discovery process:

- 1 Verify that the following message appears in the message browser for each managed node:

```
WASSPI-502: INFO - WBSSPI Discovery is Successful.
```

Depending on the number of managed nodes in your environment, it might take several minutes for these messages to appear for all managed nodes.

- 2 Select **File** → **Reload Configurations**. In the Services tree, open the Application node and look for the WebSphere service.



If the service map is not displayed in the Operational interface, type the following command to assign the services to the operator:

```
opcservice -assign <operator> <service>
```


For example: `opcservice -assign opc_adm <service>`

- 3 Run the **Discover or Configure WBSSPI** tool to verify the properties set by the discovery process. See [Discover or Configure WBSSPI](#) on page 61.

If you are having problems with the discovery process, see [Troubleshooting the Discovery Process](#) on page 105.

Assign Policies to the Managed Node

To assign policies to the managed node:

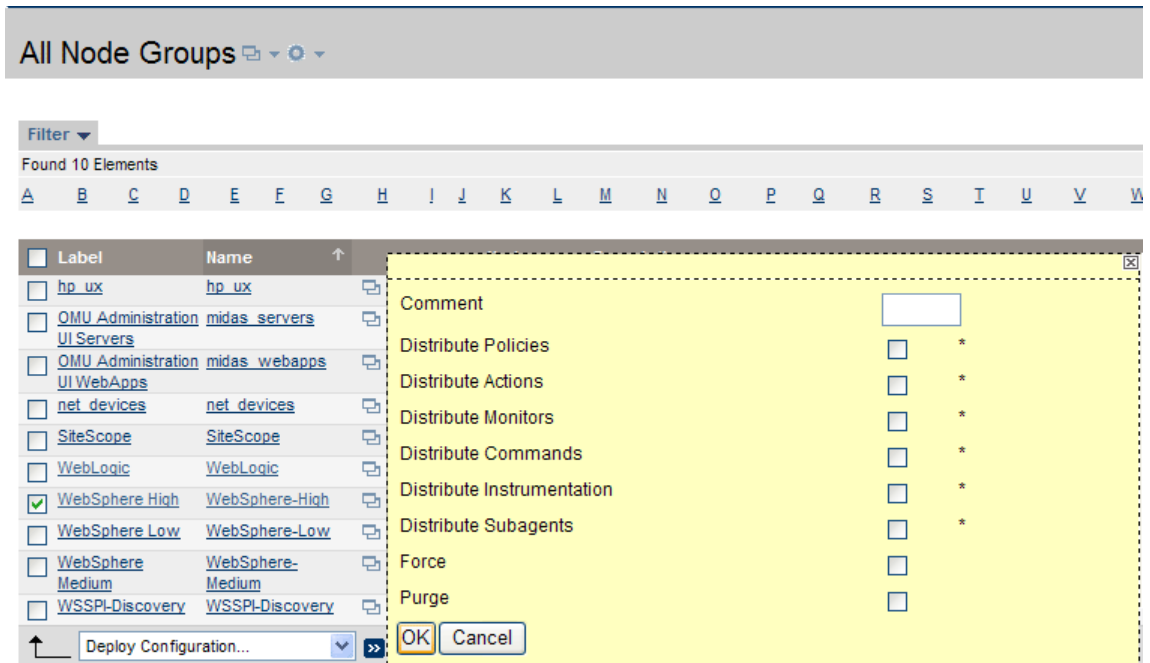
- 1 Open the Node Bank window and select the managed nodes.
- 2 Select **Assign Policies / Policy Groups...** from the **Choose an Action** drop-down list and click  to submit.
The Selector window appears.
- 3 Click **Policy Bank**.
- 4 Select the policies you want to assign to the managed node from the **SPI for WebSphere** policy group.
- 5 Click **OK**.

Deploy the WebSphere SPI Policies

To deploy the WebSphere SPI policies:

- 1 Open the All Node Groups window and select a WebSphere SPI node group.

- 2 Select **Deploy Configuration...** from the **Choose an Action** drop-down list and click  to submit.



- 3 Select **Distribute Policies** by selecting the corresponding check box.
- 4 Click **OK**. The WebSphere SPI policies are now distributed to the selected node group. The WebSphere SPI monitors will run according to their specific collection interval.

➤ If you use HP Reporter, see [Chapter 6, Integrating the WebSphere SPI with HP Reporting and Graphing Solutions](#).

Run Configuration

To run configuration:

- 1 From the HPOM console, select **Integrations** → **HPOM for Unix Operational UI**.
- 2 Select one or more nodes on which you want to launch Discover or Configure WBSSPI tool. To invoke the WebSphere interfaces, see [Launching GUIs](#) on page 68.
- 3 Right-click a node and select **Start** → **SPI for WebSphere** → **SPI Admin** → **Discover or Configure WBSSPI**. The Tool Selector window appears.
- 4 Click **OK**. By default, the Launch Configure Tool radio button is selected. The Introduction window appears.
- 5 Click **Next**. The Configuration Editor appears.
 - Make sure that the LOGIN, PASSWORD, JAVA_HOME, and HOME properties are set. You cannot proceed to the next window if the required properties are not set. See [step 6](#) on page 43 for information on how to set the properties.
- 6 Set the configuration properties at the global or server specific level by selecting the property from the **Select a Property to Set...** drop-down list, click **Set Property**, and set the value for the property. For more information on how to use the configuration editor, see [Appendix B, Configuration](#).

- 7 Click **Save** to save any changes made to the configuration. After you save the changes, you cannot undo the changes automatically.
- 8 Click **Finish** to exit the editor and start configuring the WebSphere SPI on the managed node.



If you click **Cancel**, the changes made by you are not saved to the selected managed nodes' configuration and remain in the configuration on the management server.

For more information about the configuration structure, see [Structure](#) on page 119.

Additional Configuration

Based on your WebSphere Server configuration and application needs, you must complete the WebSphere SPI configuration by setting additional configuration properties or installing and configuring additional components. Setting additional properties and configuring additional components depends on your environment.

Conditional Properties

Based on your WebSphere configuration and application needs, you can set one or more conditional properties. For information about the properties, see [Configuration Properties](#) on page 130.

Setting Conditional Properties

To set the conditional properties, perform the steps in [Run Configuration](#) on page 46.

If you added an application server or added/edited the HOME or PORT properties, run the Discover or Configure WBSSPI tool ([Run Discovery](#) on page 43) on the managed nodes on which the application server/properties were added or edited. Running Discovery updates the service map.

Configuring a Non-Root HTTPS Agent on a UNIX Managed Node

If you are running or planning to run a non-root HTTPS agent on a UNIX managed node:



You must install the OS-dependent Sudo software package on the UNIX managed node. Sudo is free software available from <http://www.sudo.ws>. The OS-dependent software packages are located at the bottom of the download page (<http://www.sudo.ws/sudo/download.html>). For more installation information, see the *HP Operations Smart Plug-in for IBM WebSphere Application Server Release Notes*.

- 1 Switch the HTTPS agent to a non-root user. For more information, see the *HTTPS Agent Concepts and Configuration Guide*.
- 2 On the managed node, set the OV_SUDO variable. As with root or with HP Operations agent user privileges:
 - a Stop all HP Operations agents by running the following command:

```
opcagt -kill
```

- b Set the OV_SUDO variable. Run the following command:


```
ovconfchg -ns ctrl.sudo -set OV_SUDO <sudo_program>
```

In this instance, <sudo_program> is the location (including the absolute pathname) where sudo is installed (for example, /usr/local/bin/sudo).
 - c Start the HP Operations agents by running the following command:


```
opcagt -start
```
 - d Verify OV_SUDO is set by running the following command:


```
ovdeploy -cmd set | grep SUDO
```

The following message appears:

```
OV_SUDO=<sudo_program>
```
- 3 Configure the managed node. These steps *must* be completed to successfully run the SPI in a non-root HTTPS agent environment.
- a From the HPOM management server, deploy actions, commands, and monitors to the managed node.
 - b From the HPOM console, select **Integrations** → **HPOM for Unix Operational UI**.
 - c Select the node on which you want to launch the Init Non-Root tool.
 - d Right-click a node and select **Start** → **SPI for WebSphere** → **SPI Admin** → **Init Non-Root**.
The Init Non-Root Output window appears.
- 4 Edit the /etc/sudoers file using the visudo editor (installed with sudo):
- a On the managed node, log in as root.
 - b Open the /<SPI_Config_DIR>/wasspi_wbs_sudoers file.
In this instance, <SPI_Config_DIR> is the location of the SPI's configuration files on a managed node. See [Managed Node File Locations](#) on page 117.
 - c In a separate window, run the visudo command (for example, type: **/usr/local/sbin/visudo**).
 - d From the wasspi_wbs_sudoers file, copy, and append the following lines to the sudoers file:


```
Cmd_Alias WBSSPI_ADMN = /opt/OV/nonOV/perl/a/bin/perl -S wasspi_admin
*
Cmd_Alias WBSSPI_COLL = /opt/OV/nonOV/perl/a/bin/perl -S wasspi_ca *
Cmd_Alias WBSSPI_DISC = /opt/OV/nonOV/perl/a/bin/perl
wasspi_wbs_discovery.pl
Cmd_Alias WBSSPI_LFEN = /opt/OV/nonOV/perl/a/bin/perl -S wasspi_wbs_le
*
Cmd_Alias WBSSPI_SHSC = /opt/OV/nonOV/perl/a/bin/perl -S
shs_collector.pl *
```

```
Cmd_Alias WBSSPI_ADMNP = /opt/OV/nonOV/perl/a/bin/perl -S \
/var/opt/OV/bin/instrumentation/wasspi_admin *
Cmd_Alias WBSSPI_COLLP = /opt/OV/nonOV/perl/a/bin/perl -S \
/var/opt/OV/bin/instrumentation/wasspi_ca *
Cmd_Alias WBSSPI_DISCP = /opt/OV/nonOV/perl/a/bin/perl \
/var/opt/OV/bin/instrumentation/wasspi_wbs_discovery.pl
Cmd_Alias WBSSPI_LFENP = /opt/OV/nonOV/perl/a/bin/perl -S \
```



```
/var/opt/OV/bin/instrumentation/wasspi_wbs_le *
Cmdnd_Alias WBSSPI_SHSCP = /opt/OV/nonOV/perl/a/bin/perl -S \
/var/opt/OV/bin/instrumentation/shs_collector.pl *
<OV_Agent_username> <nodename> = NOPASSWD: WBSSPI_ADMN, WBSSPI_COLL, \
WBSSPI_DISC, WBSSPI_LFEN, WBSSPI_SHSC, WBSSPI_ADMNP, WBSSPI_COLLP, \
WBSSPI_DISCP, WBSSPI_LFENP, WBSSPI_SHSCP
```

In this instance, *<OV_Agent_username>* is the HP Operations agent user account and *<nodename>* is the name of the managed node.

- e Save the file and exit the visudo editor. Type: **wq**



Steps 3 and 4 must be performed whenever you switch the agent user.

Configuration in High Availability Environments

High availability is a general term used to characterize environments that are business critical and therefore are protected against downtime through redundant resources. Very often, cluster systems are used to reach high availability.

You can configure the WebSphere SPI to accommodate cluster environments where failovers allow uninterrupted availability of WebSphere Application Servers. The WebSphere SPI monitoring, when synchronized with the cluster environment, can switch off from the failed node to the active node.

Configuration Prerequisites

The prerequisites for using the WebSphere SPI in high availability environments are:

- Management Server: HP-UX/Linux/Solaris
- Node: HP-UX MCSG cluster
- HPOM for UNIX 8.xx HTTPS Agent version (for details, see the Agent cluster support matrix.)

Configuring the SPI for High Availability Environments

To configure the WebSphere SPI for use in high availability environments complete the following tasks:

- [Create the WebSphere SPI Monitoring Configuration File](#)
- [Create the Clustered Application Configuration File](#)
- [Configure the WebSphere SPI](#)

Create the WebSphere SPI Monitoring Configuration File

The WebSphere SPI uses a monitoring configuration file *<appl_name>.apm.xml* that works in conjunction with the clustered application configuration file.



<appl_name> is the namespace_name. For more information, see the *HP Operations for UNIX HTTPS Agent Concepts and Configuration Guide*.

The `<appl_name>.apm.xml` file lists all the WebSphere SPI policies on the managed nodes so that you can disable/enable these policies as appropriate, for inactive/active managed nodes.

To create this clustered application configuration file for your WBS environment:

- 1 Use the following syntax to create the `<appl_name>.apm.xml` file:

```
<?xml version="1.0"?>
<APMAApplicationConfiguration>
  <Application>
    <Name> ... </Name>
    <Template> ... </Template>
    <StartCommand>wasspi_perl -S wasspi_clusterSvrApp -opt startMonitor
    $instance</StartCommand>
    <StopCommand>wasspi_perl -S wasspi_clusterSvrApp -opt stopMonitor
    $instance</StopCommand>
  </Application>
</APMAApplicationConfiguration>
```

- 2 Enter application namespace under the `<Name></Name>` tag.
- 3 After the file is created save it in the `$OvDataDir/bin/instrumentation/conf` directory.



If there is only one WBS server running on the node, you must mention *All* under the `<template>` tag.

Sample `<appl_name>.apm.xml` file

```
<?xml version="1.0"?>
<APMAApplicationConfiguration>
  <Application>
    <Name>namespace_name</Name>
    <Template>All</Template>
    <StartCommand>wasspi_perl -S wasspi_clusterSvrApp -opt startMonitor
    $instance</StartCommand>
    <StopCommand>wasspi_perl -S wasspi_clusterSvrApp -opt stopMonitor
    $instance</StopCommand>
  </Application>
</APMAApplicationConfiguration>
```



`<appl_name>.apm.xml` is dependent on the application namespace. It is not dependent on the instance level. Therefore, the start and stop actions are provided with the associated instance name as their first parameter when they are executed at package switch time. The environment variable `$instanceName` is set by CLAW when start or stop tasks are performed.

Create the Clustered Application Configuration File

The clustered application configuration file `apminfo.xml`, working in conjunction with the `<appl_name>.apm.xml` file of the WebSphere SPI, enables you to associate the WebSphere SPI monitored instances with cluster resource groups. As a result, when you move a resource group from one node to another, in the same cluster, monitoring stops on the failed node and starts on the new node.

To create the clustered application configuration file `apminfo.xml`:

- 1 Use a text editor to create the file. The syntax is:

```
<?xml version="1.0" ?>
<APMClusterConfiguration>
  <Application>
    <Name>namespace_name</Name>
    <Instance>
      <Name><Instance Name></Name>
      <Package><Package Name></Package>
    </Instance>
  </Application>
</APMClusterConfiguration>
```

- 2 Enter `namespace_name` under the `<Name></Name>` tag.
- 3 Save the `apminfo.xml` file to the `$OvDataDir/conf/conf` directory.

Sample `apminfo.xml` file

```
<?xml version="1.0" ?>
<APMClusterConfiguration>
  <Application>
    <Name>namespace_name</Name>
    <Instance>
      <Name>instance_name</Name>
      <Package>test</Package>
    </Instance>
  </Application>
</APMClusterConfiguration>
```

Configure the WebSphere SPI

To configure the WebSphere SPI:

- 1 Launch the Discover or Configure WBSSPI tool with virtual node as the target. For details about launching the discovery tool, see [Run Discovery](#) on page 43.
- 2 Launch the Discover or Configure WBSSPI tool with the virtual node as the target. For details about launching the configure tool, see [Run Configuration](#) on page 46. The Configuration Editor appears.
- 3 Use the configuration editor to set the following properties (these properties are in addition to the ones discovered by the Discover tool):

- CLUSTERNAMESPACE
- CLUSTERINSTANCE

These properties should have the same value as defined in `apminfo.xml` file. For example, `CLUSTERNAMESPACE` property must be set to `namespace_name` and `CLUSTERINSTANCE` must be set to `instance_name`.

- 4 Copy the `SiteConfig` file from active node to passive node. The file is available in the `$OvDataDir/conf/wasspi` directory.
- 5 Set the value of `ADMIN_HOST` property to the name of the managed node that was activated because of failover.

Discovery in Cluster Environment

The WebSphere SPI can now monitor the WebSphere Application Servers through the Deployment Manager in a Network Deployer scenario. This monitoring is applicable for WebSphere Application Server version 6.1 and later.

Deployment Manager

The Deployment Manager acts as an intermediate manager for the WebSphere Application Servers running on various nodes.

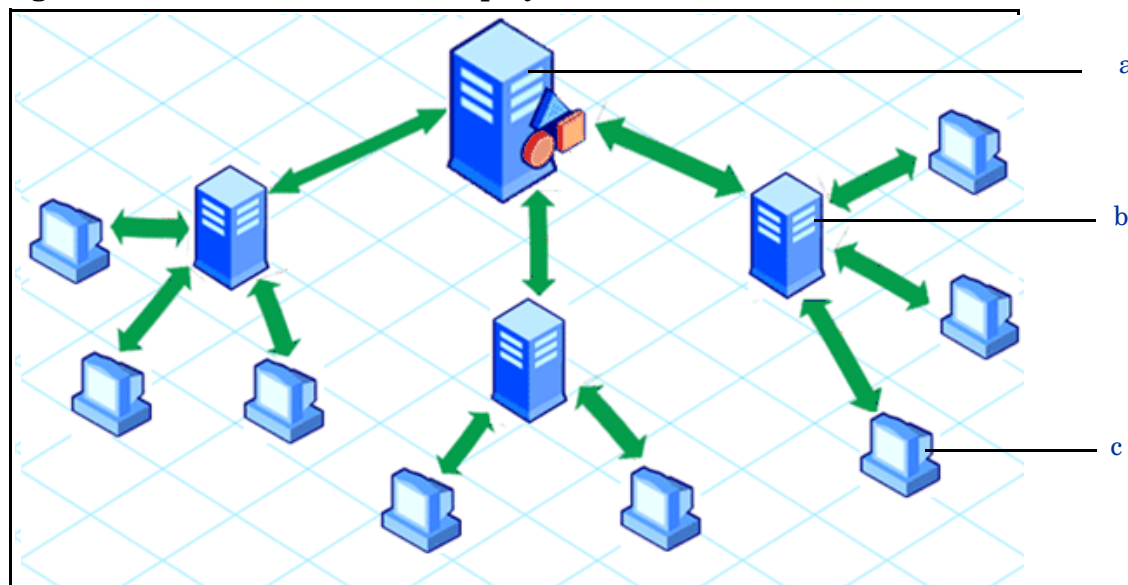
The Deployment Manager manages and collects information about WebSphere Application Servers through node agents. Node Agents are servers that gather information from the WebSphere Application Servers and pass it to the Deployment Managers.

The Deployment Manager also provides basic clustering and caching support, including failover support and workload balancing.

The logical unit comprising one Deployment Manager monitoring several application servers through a set of node agents is called a Cell.

A typical distributed network deployer scenario appears as following:

Figure 9 Distributed Network Deployer



Legend

- a Deployment Manager
- b Node Agent
- c Systems on which WebSphere Application Servers are running

Discovery in the Network Deployer Scenario

In the classic scenario, the discovery process discovers all systems running WebSphere Application Server and populates the `SiteConfig` file with information about all discovered nodes.

However, in a distributed Network Deployer scenario, the WebSphere SPI discovery process performs the following functions:

- Discovers only the Deployment Managers and populates the `SiteConfig` file on the HPOM management server with information about the Deployment Managers. The WebSphere SPI instrumentation files and policies are deployed only on the Deployment Managers.
- The WebSphere SPI creates a `DistributedServerConfig` file on the Deployment Manager node and stores the information regarding the application servers managed by that Deployment Manager. The `DistributedServerConfig` file has information about every discovered application server along with the information about its deployment manager. This is useful if there is more than one Deployment Manager installed on the same node.

Use Cases

The following are a few upgrade scenarios you may face when installing the WebSphere SPI 7.04 in a distributed network deployer environment. If you have a classic set-up in your environment, you can continue using the WebSphere SPI as usual.

Use Case 1: You are a new customer of the WebSphere SPI and want to monitor the distributed WebSphere Network Deployer scenario

- 1 Install the WebSphere SPI on the HPOM management server.
- 2 Deploy the WebSphere SPI policies and instrumentation to all the nodes on which the Deployment Manager is running.
- 3 Run the Discover or Configure WBSSPI tool.

The master `SiteConfig` contains only the details of the Deployment Managers. The details of the application servers on individual nodes are available on the Deployment Manager's Distributed `SiteConfig`. The Distributed `SiteConfig` is available in the `<OvDataDir>/conf/wbsspi` directory.

Use Case 2: You are an existing customer of the WebSphere SPI and want to monitor the distributed network deployer scenario in your environment

- 1 Install the WebSphere SPI on the HPOM management server.
- 2 Deploy the instrumentation to all the nodes where the Deployment Manager is running.
- 3 Manually remove all previous versions of the WebSphere SPI policies from all the individual nodes (where the WebSphere Application Server is running). You can perform this task through the HPOM console.
- 4 (Optional) Manually remove all instrumentation of previous version and the `<OvDataDir>/wasspi/wbs/` directory from all the individual nodes (where the WebSphere Application Server is running). You must perform this task from the managed node, as it cannot be done through the HPOM console.

Use Case 3: If you are an existing customer of the WebSphere SPI and have implemented the network deployer scenario but still want to use the SPI, ignoring the network deployer scenario

- 1 Install the WebSphere SPI on the HPOM management server.
- 2 Run the Discover or Configure WBSSPI tool in discovery mode.
- 3 On the node, go to `<OvDataDir>/conf/wbsspi` directory.
- 4 Open the `SPIConfig` file.
- 5 Set `OVERRIDE_DISTRIBUTED_MODE=true` and `DISTRIBUTED_MODE=false` properties in the `SPIConfig` file. This action ignores the network deployer scenario.
- 6 Save the `SPIConfig` file.
- 7 Run the Discover or Configure WBSSPI tool in discovery mode.
 - ▶ Wait for the discovery process to complete before going to the next task. The discovery process might take several minutes to complete.
- 8 Run the Discover or Configure WBSSPI tool in configure mode.
- 9 Check the list of Application Servers in the config interface. Remove the `Dmgr` instance.
- 10 Click **Save** and **Finish**.

Limitations in a Network Deployer Scenario

The limitations in a network deployer scenario are as follows:

- Log file monitoring is not supported on federated servers.
- The two status related metrics — `WBSSPI_0001 Server Status` and `WBSSPI_0002 Server Status Report` are not collected in the network deployer scenario. However, if the WebSphere SPI is unable to connect to the deployment manager, an alert message indicating that the deployment manager is down appears in the message browser.
- When you launch the View Server Status tool, it displays the status of deployment manager as “unknown”.

Discovery on Hypervisor Edition

The WebSphere SPI discovers and monitors WebSphere Application Server from version 7.0x on Hypervisor Edition.

To discover WebSphere on Hypervisor, set the mandatory property, `PROFILE_HOME` along with `HOME` in the Configuration Editor, while running discovery. See [Run Discovery](#) on page 43.

To set the `PROFILE_HOME` property in the Configuration Editor:

- 1 Select **PROFILE_HOME** from the **Select a Property to Set...** list.
- 2 Click **Set Property**.
- 3 Set the value for **PROFILE_HOME**.

Discovery of WebSphere Portal Servers

The WebSphere SPI discovers and monitors WebSphere Portal Servers.

The WebSphere SPI directly discovers WebSphere Portal Servers along with the Application server, if the login credentials are same for Application server and Portal server instances.

The following sections describe the different cases involved in the discovery of WebSphere Portal Servers:

Case 1: If the Portal Server is federated with the Distribution Manager

Set the credentials for Distributed Managers during discovery and the WebSphere SPI will discover all the servers.

Case 2: If the Portal Server instances are not federated with the Distributed Manager and the Application Server is installed in the Network Deployment mode

Follow the steps in [Use Case 3: If you are an existing customer of the WebSphere SPI and have implemented the network deployer scenario but still want to use the SPI, ignoring the network deployer scenario](#) on page 54.

Case 3: If the Application Server is installed in a standalone mode (Non Distributed Mode) and the Portal Server is also installed on the same node.

The WebSphere SPI discovers all the servers in this case.

If the login credentials for Application server and Portal Server instances are different, follow these steps to run discovery:

- 1 Set the credentials for Application server instance, and run discovery.
- 2 Take a backup of the resulting SiteConfig. The SiteConfig file is located in `</var/opt/OV/wasspi/wbs/conf/SiteConfig>` directory on the node.
- 3 Set the credentials for Portal Server instance, and run discovery.
- 4 Merge the contents of the backed up SiteConfig with the newly generated SiteConfig.

Integrating with CODA

The WebSphere SPI can detect if you are using the HP Performance Agent. If you are using the HP Performance Agent, the WebSphere SPI installation automatically uses it.

If you want to use the HP Operations subagent (CODA), you must configure the managed nodes to do so. This configuration does not support HP Performance Agent.

To use CODA, set up an empty file named `nocoda.opt` and store it on the managed node:

- 1 On the managed node, create a `nocoda.opt` file in the following directory:

Operating System	File Location
HP-UX, Linux and Solaris	<code>/var/opt/OV/conf/dsi2ddf/</code>
AIX	<code>/usr/lpp/OV/conf/dsi2ddf/</code>
Windows	<code>\usr\ov\conf\dsi2ddf\</code>

If the directory `dsi2ddf` does not exist, create it.

- 2 Save the empty file.



Use the latest CODA to avoid the problem of datalogging on 64 bits platforms.

4 Using the WebSphere SPI Tools

This chapter describes the tools offered by the WebSphere SPI, which help you to monitor and manage systems using the WebSphere Application Server. This chapter also details the procedure to launch all the tools, towards the end of this chapter.

These tools enable you to configure the management server's connection to selected server instances on specific managed nodes. The WebSphere SPI tools include configuration, troubleshooting, and report-generating utilities.

Overview

In the Tool Bank window, the WBSSPI:TOOLS group contains the following WebSphere SPI tool groups:

- WebSphere Admin (WBSSPI:ADMIN)
- Metric Reports (WBSSPI:REPORTS)
- SPI Admin (WBSSPI:SPI_ADMIN)
- JMX Metric Builder: This tool group is available *only if* you install the SPIJMB software bundle.

Figure 10 Elements in Tool Group “SPI for WebSphere”

The screenshot shows the 'Elements in Tool Group "SPI for WebSphere"' window. The breadcrumb path is '/Tool Bank / WBSSPI:TOOLS'. The title is 'Administrative and Operator Tools for the SPI for WebSphere Server'. A filter dropdown is set to 'Details SPI for WebSphere Filter'. Below the filter, it says 'Found 3 Elements'. A table lists the elements:

<input type="checkbox"/>	Type	Label	Name	↑	Contents	Target
<input type="checkbox"/>		WebSphere Admin	WBSSPI:ADMIN		0 / 5	WebSphere Admin r
<input type="checkbox"/>		Metric Reports	WBSSPI:REPORTS		0 / 20	Ascii metric reports
<input type="checkbox"/>		SPIAdmin	WBSSPI:SPI_ADMIN		0 / 10	WebSphere SPI Adr

At the bottom, there is an action bar with a dropdown menu labeled 'Choose an action' and a right-pointing arrow button.

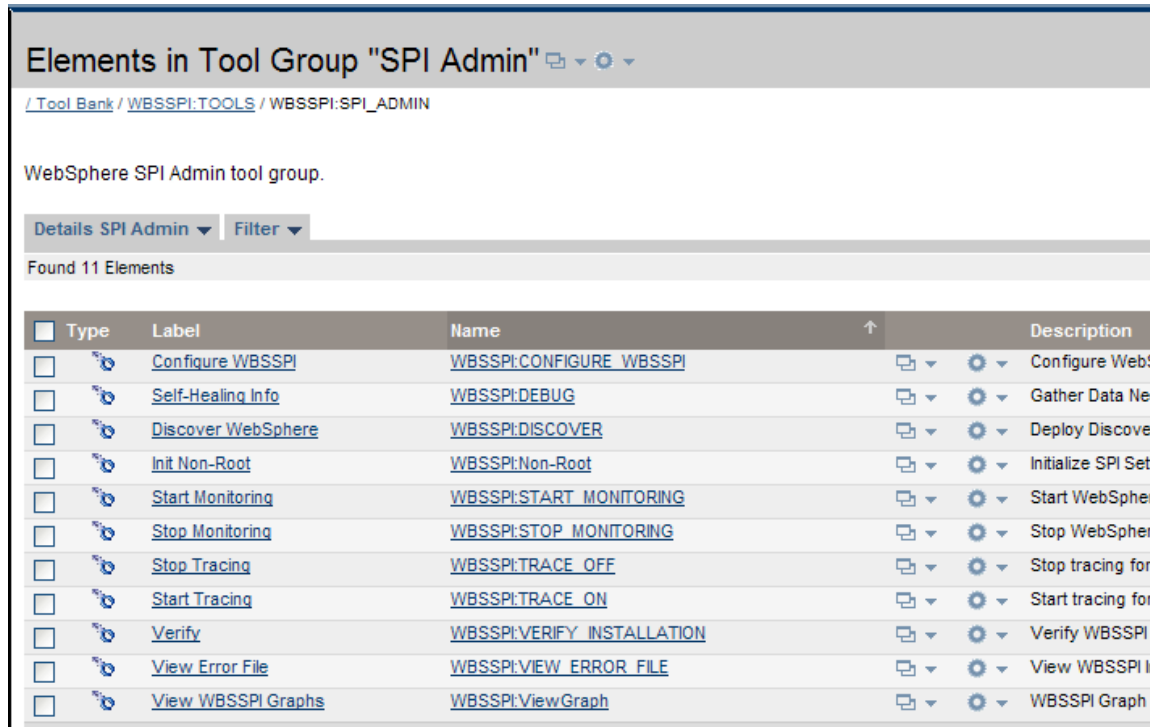
SPI Admin Tools Group

The SPI Admin tools group contains tools that enable you to configure, control, and troubleshoot the WebSphere SPI. These tools require the `root` user permission, therefore it is recommended that this group is assigned to the HPOM administrator.

Additional SPI Admin tools for User Defined Metrics (UDMs) are available with the SPIJMB software bundle. For more information about how to install the software bundle and the additional tools, see the *HP Operations Smart Plug-in for User Defined Metrics User Guide*.

To access the SPI Admin tools, in the Tool Bank window, click **WBSSPI:TOOLS** → **WBSSPI:SPI_ADMIN**.

Figure 11 WebSphere SPI Admin Tool Group



The screenshot shows the 'Elements in Tool Group "SPI Admin"' interface. It includes a breadcrumb trail: / Tool Bank / WBSSPI:TOOLS / WBSSPI:SPI_ADMIN. Below the breadcrumb, there is a description: 'WebSphere SPI Admin tool group.' and a 'Details SPI Admin' dropdown menu. A 'Filter' dropdown is also present. The main content area displays 'Found 11 Elements' and a table with the following columns: Type, Label, Name, and Description. Each row in the table has a checkbox in the 'Type' column and a gear icon in the 'Name' column. The table lists 11 tools with their respective labels and names.

<input type="checkbox"/>	Type	Label	Name	Description
<input type="checkbox"/>		Configure WBSSPI	WBSSPI:CONFIGURE_WBSSPI	Configure WebS
<input type="checkbox"/>		Self-Healing Info	WBSSPI:DEBUG	Gather Data Ne
<input type="checkbox"/>		Discover WebSphere	WBSSPI:DISCOVER	Deploy Discove
<input type="checkbox"/>		Init Non-Root	WBSSPI:Non-Root	Initialize SPI Set
<input type="checkbox"/>		Start Monitoring	WBSSPI:START_MONITORING	Start WebSpher
<input type="checkbox"/>		Stop Monitoring	WBSSPI:STOP_MONITORING	Stop WebSpher
<input type="checkbox"/>		Stop Tracing	WBSSPI:TRACE_OFF	Stop tracing for
<input type="checkbox"/>		Start Tracing	WBSSPI:TRACE_ON	Start tracing for
<input type="checkbox"/>		Verify	WBSSPI:VERIFY_INSTALLATION	Verify WBSSPI
<input type="checkbox"/>		View Error File	WBSSPI:VIEW_ERROR_FILE	View WBSSPI I
<input type="checkbox"/>		View WBSSPI Graphs	WBSSPI:ViewGraph	WBSSPI Graph

The WebSphere SPI Admin tool group contains the following tools:

- Discover or Configure WBSSPI
- Self-Healing Info
- Init Non-Root
- Start Monitoring
- Stop Monitoring
- Start Tracing
- Stop Tracing
- Verify
- View Error File
- View WBSSPI Graphs

Discover or Configure WBSSPI

You can run the discovery or configuration process using the Discover or Configure WBSSPI tool.

The tool Discover or Configure WBSSPI launches the configuration editor. The tool Discover or Configure WBSSPI allows you to either identify instances of a WebSphere Application Server on a managed node from the HPOM console (on selecting Launch Discover Tool option) or maintain the WebSphere SPI configuration by viewing, editing, or setting configuration properties in the configuration editor (on selecting Launch Configure Tool option).

Function

The following functions are performed by the Configure Tool:

- Updates the configuration on the HPOM management server and selected managed nodes.
- Creates the directories and files required by the WebSphere SPI on the selected managed nodes.
- Sets up data sources for reporting and graphing.
- Sets up the WebSphere Server log files and the WebSphere SPI error log file for monitoring.

The Discover Tool updates the configuration on the HPOM management server and selected managed nodes.

Configuration information for all WebSphere instances on all HPOM managed nodes is maintained on the HPOM management server. In addition, every managed node maintains information about WebSphere Application Servers running on that node.

When you make changes using the configuration editor, the changes are saved on the HPOM management server. However, when launching the Discover or Configure WBSSPI tool if you select a node, the changes affecting the selected node are saved on that node itself.

To save any changes on a managed node, you must select that node before launching the Discover or Configure WBSSPI tool otherwise the changes are saved on the management server by default.

Init Non-Root

The Init Non-Root tool simplifies the configuration of a non-root HTTPS agent on a UNIX managed node. For steps to configure a non-root HTTPS agent on a UNIX managed node see [Configuring a Non-Root HTTPS Agent on a UNIX Managed Node](#) on page 47.

Function

The Init Non-Root tool performs the following actions on the selected managed nodes:

- 1 Runs the `wasspi_perl -S wasspi_initnonroot.pl -prod wbs force` command to set the proper SPI path.
- 2 Generates the `wasspi_perl_su` file on the selected managed nodes.

Self-Healing Info

The Self-Healing Info tool collects data that you can send to your HP support representative.

Setup

If you are collecting data for a reproducible problem, follow these steps before running the Self-Healing Info tool:

- 1 Run the Start Tracing tool. For more information, see [Start Tracing](#) on page 63.
- 2 Reproduce the problem.

Function

Self-Healing Info tool performs the following functions:

- Saves data in the following file:
 - on a UNIX or Linux managed node: `/tmp/wasspi_wbs_support.tar`
 - on a Windows managed node: `wasspi_wbs_support.zip` in `%TEMP%` directory.
- ▶ This file might be hidden on some Windows managed nodes. If you do not see the file, open Windows Explorer and, from the **Tools** menu, select **Folder Options**. Click the **View** tab. Under Hidden files and folders, select **Show hidden files and folders**.
- Launches and saves data using the Verify tool (for more information, see [Verify](#) on page 63).

Start Monitoring

The Start Monitoring tool enables you to start the WebSphere SPI from collecting metrics for one application server or all application servers on a managed node.

In the Network Deployer scenario, the Start Monitoring tool, will start monitoring all WebSphere application servers which report to that Deployment Manager. This is applicable when you select either of the following options:

- Dmgr
- All

Function

The Start Monitoring tool starts the collection of metrics for one or all application servers on a managed node.

Stop Monitoring

The Stop Monitoring tool enables you to stop the WebSphere SPI from collecting metrics for one application server or all application servers on a managed node.

Typically, you might stop monitoring on a managed node if the node is not running for a known reason (for example, the node is down for maintenance). Stopping the monitoring prevents unnecessary alarms from being generated.

In the Network Deployer scenario, the Stop Monitoring tool, will stop monitoring all WebSphere application servers which report to that Deployment Manager. This is applicable when you select either of the following options:

- Dmgr
- All

Function

The Stop Monitoring tool stops the collection of metrics for one or all application servers on a managed node.

Start Tracing

The Start Tracing tool enables you to start gathering information about the functioning of the SPI. Run this tool only when instructed by your HP support representative.

The Self-Healing Info tool collects the files created by this tool as a part of the data that the HP support representative can use.

Function

The Start Tracing tool saves information about the functioning of the SPI in a file.

Stop Tracing

The Stop Tracing tool enables you to stop gathering information about the functioning of the SPI. Run this tool only when instructed by your HP support representative.

The Self-Healing Info tool collects the files created by this tool as a part of the data that the HP support representative can use.

Function

The Stop Tracing tool stops saving information about the functioning of the SPI in a file.

Verify

The Verify tool enables you to verify if the files required for the functioning of the SPI (such as instrumentation, library and configuration) are deployed on the managed nodes.



Before you launch the Verify tool, make sure that you have installed the latest version of Self-Healing Service (SHS) component from the SPI DVD.

Function

The Verify tool checks if the files (such as instrumentation, configuration and library) required for the functioning of the SPI are deployed on the managed nodes.

View Error File

The View Error File tool enables you to view the contents of the WebSphere SPI error log file.

Function

The View Error File tool enables you to view the contents of the WebSphere SPI error log file `<Agent_Dir>/wasspi/wbs/log/wasspi_perl.log` where `<Agent_Dir>` typically is:

- `/var/opt/OV` on UNIX and Linux managed nodes
- `\Documents and Settings\All Users\Application Data\HP\HP BTO Software\` on Windows managed nodes

View WBSSPI Graphs

The View Graphs tool launches the WebSphere SPI graphs, generated through HP Performance Manager, in a web browser.

Setup

To run this tool successfully:

- Install the HP Performance Manager.
- Configure Mozilla or Netscape browser on the HP Operations Manager for UNIX. If your browser is Netscape Navigator, use version 6.0 or later.

WebSphere Admin Tools Group

To access the WebSphere Admin tools, in the Tool Bank window click **WBSSPI:TOOLS** → **WBSSPI:ADMIN**.

Figure 12 WebSphere Admin Tool Group

<input type="checkbox"/>	Type	Label	Name	↑	Target
<input type="checkbox"/>		Check WebSphere	WBSSPI:CHECK_WEBSHERE		Selected Nodes
<input type="checkbox"/>		Start WebSphere	WBSSPI:START_WEBSHERE		SMGMTSV
<input type="checkbox"/>		Stop WebSphere	WBSSPI:STOP_WEBSHERE		SMGMTSV
<input type="checkbox"/>		View WebSphere Logs	WBSSPI:VIEW_WEBSHERE_LOG_FILES		SMGMTSV

The WebSphere Admin tool group contains the following tools:

- [Check WebSphere](#)
- [Start WebSphere](#)
- [Stop WebSphere](#)
- [View WebSphere Logs](#)

Check WebSphere

The Check WebSphere tool displays a status report of the WebSphere instances on the selected managed nodes. It enables you to check the status of each application server running on a managed node.

Function

The Check WebSphere tool displays the following information for each application server on the selected nodes:

Information	Description
Server Name	The server name as defined in WebSphere.
Server State	The status of the WebSphere Server.
Start Date	The date when the WebSphere Server was started.
Port	The port on which the WebSphere Server listens.
Admin Server Host	The location of the WebSphere administration server for this WebSphere instance.
Admin Server Port	The port of the WebSphere administration server for a WebSphere instance.
Current Open Socket Count	The number of open sockets for the WebSphere Server.
WebSphere Version	The version number of the WebSphere Server.

If the WebSphere SPI has been configured to not collect metrics for a WebSphere Server, the message `Collection is temporarily OFF for <server_name>` appears.

Start WebSphere

The Start WebSphere tool starts a WebSphere application server from the HPOM console. You can start one or more WebSphere application servers on the selected managed nodes without logging on to each WebSphere administration server.

Setup

The `START_CMD`, `STOP_CMD`, and `USER` configuration properties *must* be set before launching this tool. To set this property, run the Configure tool and select WBS application servers displayed in the left pane. Set the preceding configuration properties for each WBS application server.

Function

The Start WebSphere tool starts one or all application servers on the selected managed nodes.

Stop WebSphere

The Stop WebSphere tool stops a WebSphere application server from the HPOM console. You can stop one or more WebSphere application servers on the selected managed nodes without logging in to each WebSphere administration server.

Setup

The `START_CMD`, `STOP_CMD`, and `USER` configuration properties *must* be set before launching this tool. To set this property, run the Configure tool and select WBS application servers displayed in the left pane. Set the preceding configuration properties for each WBS application server.

Function

The Stop WebSphere tool stops one or all application servers on the selected managed nodes.

View WebSphere Logs

The View WebSphere Logs tool enables you to select and view a WebSphere Server log file without logging in to the system on which a WebSphere Server is running.

Function

The View WebSphere Logs tool performs the following functions:

- When you launch the View WebSphere Logs tool without a parameter, the tool displays a numbered list of available log files for the selected managed node.
- When you launch the View WebSphere Logs tool with an invalid parameter (for example, a non-numeric value or a number that does not correspond to the list of available log files), the tool returns a numbered list of available log files for the selected managed node.
- When you launch the View WebSphere Logs with a valid parameter, the tool returns the contents of the corresponding log file for the managed node.

You can enter only one numeric value in the parameter field. The log file designated to this number (for all managed nodes) will appear. Select one log file for one managed node to view each time you launch the tool.

If you keep the Tool Status window open and re-launch the tool, the output in the Tool Status window accumulates.

Metric Reports

The Metric Reports (WBSSPI:REPORTS) tool group contains reports that show information about WebSphere conditions in the server.

You can generate a report about all WebSphere servers configured on a managed node. To generate a report, select **Integrations** → **HPOM for Unix Operational UI**. Right-click the managed node and select **Start** → **SPI for WebSphere** → **Metric Reports** → **<Name of the Metric Report>**. Each report shows the status of all the configured WebSphere Server instances on the managed node in relation to the metric for which the report is generated. To access the Metric Reports, in the Tool Bank window click **WBSSPI:TOOLS** → **WBSSPI:REPORTS**.

Figure 13 Metric Reports Tool Group

Elements in Tool Group "Metric Reports"

[/ Tool Bank](#) / [WBSSPI:TOOLS](#) / [WBSSPI:REPORTS](#)

Ascii metric reports for Websphere

Details Metric Reports Filter

Found 17 Elements

<input type="checkbox"/>	Type	Label	Name				Description
<input type="checkbox"/>		I005_JVMMemUtilPct	WBSSPI:WBSSPI_0005				Percentage of heap space used in the JVM
<input type="checkbox"/>		I040_ServSessAveLife	WBSSPI:WBSSPI_0040				Average lifetime of a servlet session in minutes
<input type="checkbox"/>		I041_ServSessActSess	WBSSPI:WBSSPI_0041				Number of sessions currently being accessed
<input type="checkbox"/>		I042_ServInvSessRt	WBSSPI:WBSSPI_0042				Number of sessions being invalidated per second
<input type="checkbox"/>		I212_ThreadPoolUtilPct	WBSSPI:WBSSPI_0212				Percentage of threads used in a pool during the last minute
<input type="checkbox"/>		I213_ThreadPoolPctMax	WBSSPI:WBSSPI_0213				Percentage of time number of threads in pool is at or near maximum
<input type="checkbox"/>		I220_EJBPoolUtil	WBSSPI:WBSSPI_0220				Percentage of active beans in the pool (excluding beans in process)
<input type="checkbox"/>		I221_EJBMethRespTime	WBSSPI:WBSSPI_0221				Average EJB response time in milliseconds
<input type="checkbox"/>		I222_EJBMethodCallsRt	WBSSPI:WBSSPI_0222				Number of EJB method calls per minute
<input type="checkbox"/>		I224_EJBEntDatLdStRt	WBSSPI:WBSSPI_0224				Number of times an EJB was written to cache
<input type="checkbox"/>		I246_WebAppServletRespTime	WBSSPI:WBSSPI_0246				Average response time in milliseconds for servlets
<input type="checkbox"/>		I247_WebAppServletErrorRt	WBSSPI:WBSSPI_0247				Number of errors in a servlet per second
<input type="checkbox"/>		I261_JDBCConnPoolWaiters	WBSSPI:WBSSPI_0261				Average Number of threads waiting for a connection
<input type="checkbox"/>		I262_JDBCConnPoolWaitTime	WBSSPI:WBSSPI_0262				Average time that a client waited for a connection
<input type="checkbox"/>		I263_JDBCConnPoolUtil	WBSSPI:WBSSPI_0263				Percentage of connection pool in use
<input type="checkbox"/>		I264_JDBCConnPoolMaxPct	WBSSPI:WBSSPI_0264				Percentage of time that all connections in pool are at or near maximum
<input type="checkbox"/>		I265_JDBCConnPoolTimeoutRt	WBSSPI:WBSSPI_0265				Number of times a client timed out waiting for a connection

Tool Bank Reports Generated from Alarms

An alarm condition can generate a report. These reports are generated automatically and are context sensitive, relating only to a single server on the managed node. These reports appear within the Annotations tab in Message Properties window.

If you configure the message browser to display the **SUIAONE** columns, a flag appears under the **S** column (adjacent to the message) when a report is generated.

JMX Metric Builder Tools

The JMX Metric Builder tools group contains the following tools:

- **Deploy UDM**– Deploys the UDM file.
- **Gather MBean Data**– Collects MBean information to be used with the JMX Metric Builder.
- **JMX Metric Builder**– Launches the JMX Metric Builder tool that is used to create UDMs and browse MBeans.
- **UDM Graph Enable/Disable**– Starts/Stops data collection for UDM graphs. Also starts/stops the HPOM subagent.

For more information about the JMX Metric Builder tools group and steps to install the SPIJMB software bundle, see the *HP Operations Smart Plug-in for User Defined Metrics User Guide*.

Launching Tools

This section describes how you can launch the tools for the WebSphere SPI. The steps in [Launching Discover or Configure WBSSPI tool](#) describe how you can launch the Discover or Configure WBSSPI tool. The steps in [Launching All Tools](#) describe how you can launch all the tools (excluding the Discover or Configure WBSSPI) tool.

Launching GUIs

To launch the GUIs related to the WebSphere SPI:

- 1 Install X-windows client software on the system from which you will launch the HPOM for UNIX 9.0x server Operator GUI.
- 2 Start the X-windows client software.

Launching Discover or Configure WBSSPI tool

See [Run Discovery](#) on page 43 and [Run Configuration](#) on page 46 to know how to launch Discover or Configure WBSSPI tool.

Launching All Tools

To launch all tools:

- 1 From the Administration UI, select **Integrations** → **HPOM for Unix Operational UI**.
- 2 Select the nodes on which you want to launch the tool.
- 3 Right-click a node and select **Start** → **SPI for WebSphere** → **<Tool Group>** → **<Name of the Tool>**. The **<Name of the Tool>** Output window appears.

5 Customizing the WebSphere SPI Policies

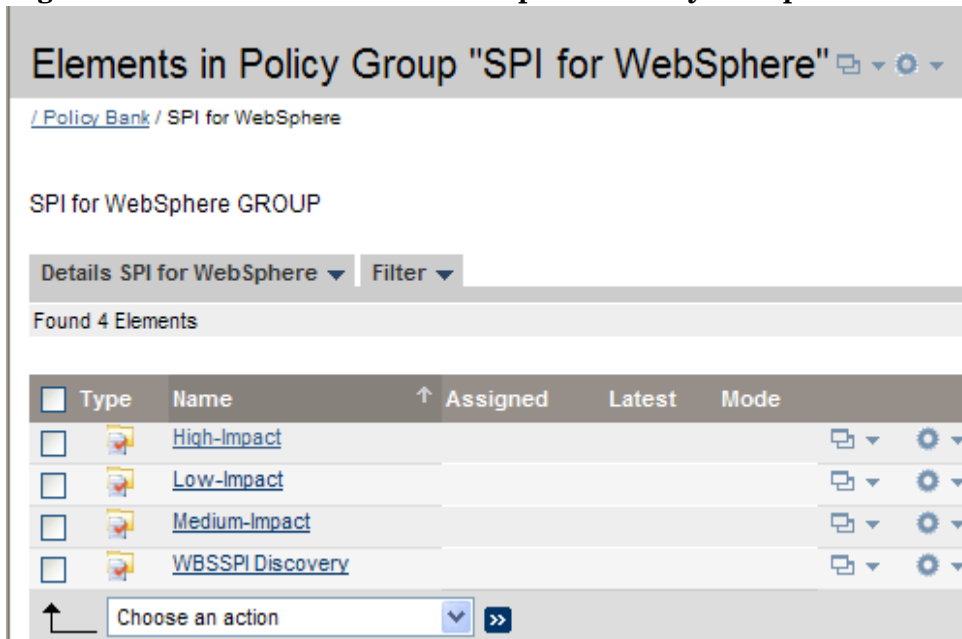
The WebSphere SPI consists of policies which monitor the WebSphere Application Server. This chapter describes policy types and how to modify policies.

Overview

The SPI for WebSphere policy group contains policies grouped into four categories:

- High-Impact
- Low-Impact
- Medium-Impact
- WBSSPI Discovery

Figure 14 Elements in “SPI for WebSphere” Policy Group



High-Impact, Low-Impact, and Medium-Impact groups are based on the impact that their data collection has on system performance. The Low Impact group has only low impact metrics. The Medium Impact group has both medium and low impact metrics. The High Impact group has all metrics: high, medium, and low impact metrics. For complete listings of the specific metrics included in each group, see the *HP Operations Smart Plug-in for WebSphere Application Server Reference Guide*.

All data collection affects performance in some way, with impact varying according to metrics (counter). The overhead cost associated with each WebSphere SPI metric is represented with a rating of high, medium, or low. Metrics with medium or high ratings have higher

performance impacts. The calculation required for the collected data generally requires multiplication, division, or both. A metric with a low rating involves only a minor performance cost since its calculation requires just a single addition or subtraction.

Under these broad categories (High-Impact, Low-Impact, and Medium-Impact), SPI for WebSphere policy group contains the following policy sub-groups and individual policies:

- WBSSPI-Logfiles
- WBSSPI-Metrics
- WBSSPI-Monitors
- WBSSPI-Messages

Figure 15 High-Impact, Low-Impact, and Medium-Impact Policy Groups

Elements in Policy Group "SPI for WebSphere/High-Impact"

/ Policy Bank / SPI for WebSphere / High-Impact

High-Impact GROUP

Details High-Impact Filter

Found 4 Elements

Type	Name	Assigned	Latest	Mode	Smart Plug-in	Categories	Contents
	WBSSPI-Logfiles						0 / 5
	WBSSPI-Metrics						0 / 34
	WBSSPI-Monitors						0 / 5
	WBSSPI-Messages	7.0	7.0	Fixed		WebSphere	

Choose an action

- **WBSSPI-Logfiles** – Contains policies that generate messages based on log file and error text detected in the log files for both the WebSphere Application Server (WAS) and the WebSphere SPI. The information captured from these log files include errors that occur in the operation of WAS or the WebSphere SPI and changes to WebSphere Server configuration.

Figure 16 WBSSPI-Logfiles Policy Sub-Group

Elements in Policy Group "SPI for WebSphere/High-Impact/WBSSPI-Logfiles"

/ Policy Bank / SPI for WebSphere / High-Impact / WBSSPI-Logfiles

WBSSPI-Logfiles GROUP

Details WBSSPI-Logfiles Filter

Found 5 Elements

Type	Name	Assigned	Latest	Mode	Smart Plug-in	Categories	Description
	WBSSPI Error Log	7.0	7.0	Fixed		WebSphere	Monitors the WBSSPI error log
	WBSSPI Java Collector Error Log	7.0	7.0	Fixed		WebSphere	Monitors the WBSSPI Java Collector error log
	WBSSPI Java Discovery Error Log	7.0	7.0	Fixed		WebSphere	Monitors the WBSSPI Java Discovery error log
	WebSphere Activity Log via JMX Notification	7.0	7.0	Fixed		WebSphere	Monitors the WebSphere Application server's messages via JMX notifications
	WebSphere Text Logs	7.0	7.0	Fixed		WebSphere	Monitors the WebSphere Application server's SystemOut, SystemErr, and messages via JMX notifications

Choose an action

- **WBSSPI-Metrics** – Contains metric policies that monitor the performance levels and availability of a WebSphere Application Server.

Each metric policy determines the threshold conditions for the monitored metric, the message text that is sent to the HPOM message browser when the threshold is exceeded, the actions to execute, and the instructions that appear.

- **WBSSPI-Monitor** – Contains collector policies that specify the collection interval of the metric policies. Within the name of each collector policy is its collection interval. For example, the collection interval of policy WBSSPI-High-1h is one hour (where 1h represents one hour). Each collector policy is assigned a collection interval of 5 minutes, 15 minutes, or one hour.

When you open any collector policy, you see the metrics collected within the interval (listed by number, following the `-m` option of the collector/analyzer command `wasspi_ca`).

Each collector policy controls when and what metrics are collected. Specifically, the collector policy does the following:

- Runs the collector/analyzer at each collection interval
- Specifies which metrics are collected

Figure 17 WBSSPI-Monitors Policy Sub-Group

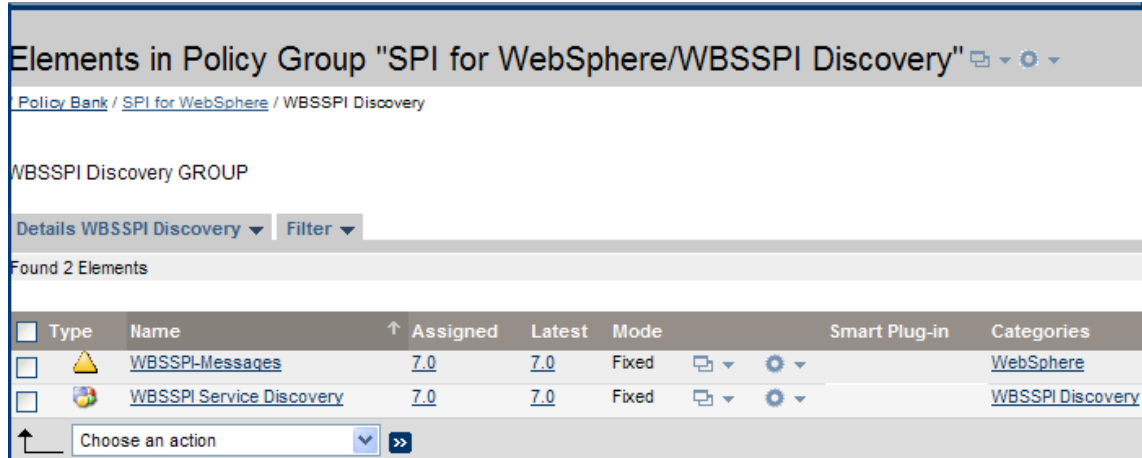
Type	Name	Assigned	Latest	Mode	Smart Plug-in	Categories	Description
	WBSSPI-ConfigCheck	7.0	7.0	Fixed		WebSphere	Check that the managed node is configured
	WBSSPI-High-05min	7.0	7.0	Fixed		WebSphere	Runs the WebSphere Server SPI collector/analyzer every 5 minutes
	WBSSPI-High-15min	7.0	7.0	Fixed		WebSphere	Runs the WebSphere Server SPI collector/analyzer every 15 minutes
	WBSSPI-High-1h	7.0	7.0	Fixed		WebSphere	Runs the WebSphere Server SPI collector/analyzer every 1 hour
	WBSSPI-Performance	7.0	7.0	Fixed		WebSphere	WBSSPI Performance Data Feed (every 5 minutes)

- **WBSSPI-Messages**– It intercepts the WebSphere SPI messages for the HPOM message browser.

The WBSSPI Discovery group is further divided into two policies:

- WBSSPI-Messages
- WBSSPI Service Discovery

Figure 18 WBSSPI Discovery Policy Group



- **WBSSPI Service Discovery** – It updates the configuration on the HPOM management server and managed nodes.
- **WBSSPI-Messages** – It intercepts the WebSphere SPI messages for the HPOM message browser.

WebSphere Policy Groups and System PMI Levels

When you deploy a policy group on a managed node, the PMI level of the node is automatically adjusted to that of the policy group.



PMI levels, once set, do not automatically revert to lower impact levels, even after removing policies from a node or deploying a lower impact level policy group. To lower a PMI level for a node, you must manually reset the PMI level within WebSphere Application Server.

Basic Policy Customizations

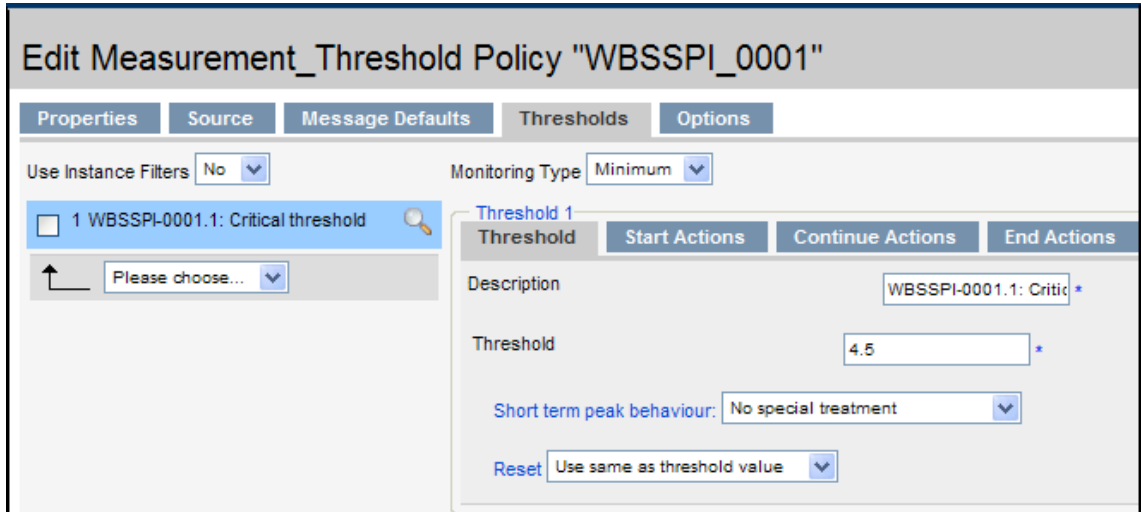
Make copies of the original policies so that the default policies remain intact. Otherwise, your customizations will be overwritten when you upgrade to the next version.

Modifying Metrics Policies

Many metric attributes can be easily modified for all monitored instances of a WebSphere Server by following these steps:

- 1 Open the Policy Bank window.
- 2 Click **SPI for WebSphere** → **High-Impact** or **Low-Impact** or **Medium-Impact** → **WBSSPI-Metrics** policy group.
- 3 Select a metric and click **Edit...** from the drop-down list. The drop-down list appears when you click . The Edit Measurement_Threshold Policy “WBSSPI_00xx” window appears.

- Click the **Thresholds** tab and then, click the condition you want to modify.



- Click the different tabs (**Threshold**, **Start Actions**, **Continue Actions**, and **End Actions**) and modify the attributes. See [Table 4](#) for a list of attributes that you can modify.
- Click **Save**.
- Deploy the modified policy as described in [Deploy the WebSphere SPI Policies](#) on page 45.

Table 4 Metric Attributes

Attributes	Description
Threshold	Enter a value for the metric data, which when exceeded, would signify a problem either about to occur or already occurring.
Duration	Enter a value for the length of time that the incoming data values for a metric can exceed the established threshold before an alarm is generated.
Severity	Click the Start Actions tab and then the Message tab. Select the desired severity setting from the Severity drop-down list.
Message Text	Be careful not to modify any of the parameters—surrounded by <> brackets, beginning with \$—in a message.
Actions	Generate metric reports or add custom programs. In the WebSphere SPI, automatic actions are configured to generate metric reports showing data values, when the threshold was exceeded. You can view the report under the Annotations tab in the Message Properties window.

The following figure shows that a threshold setting of 95 is set for WBSSPI-0005.2. This metric monitors, the total number of times a minute the clients must wait for an available Enterprise JavaBeans (EJB). A value of more than 95 will impact the server response time the client experiences, generating an alarm (a warning message).

Figure 19 Condition No.2 for WBSSPI-0005 (WBSSPI-0005.2)

Data source	
Name	WBSSPI_0005
Type	external
Description	JVM Memory Utilization
Conditions (2) Show all	
Condition	A O N T C
Overview	Condition No.2 - WBSSPI-0005.2: Major threshold (match)
1 match WBSSPI-0005.1: Critical threshold	Match
	Threshold 95 (for 0 hours 20 minutes 0 seconds)
	Set (start)
2 match WBSSPI-0005.2: Major threshold	Severity major
	Application websphere Application Server
	Content WBSSPI-
	0005.2: % of heap space used (<\$VALUE>%) too high (>=<\$THRESHOLD>%) [Policy: <\$NAME>] [Policy: <\$NAME>]
	Message Key <\$NAME>:<\$MSG_NODE_NAME>:<\$MSG_OBJECT>
	Message key relation ^<\$NAME>:<\$MSG_NODE_NAME>:<\$MSG_OBJECT>\$(ignore case)
	Service name WBS_<\$OPTION(map_servername)>_<\$OPTION(map_port)>_<\$OPTION(node)>
	Actions
	Automatic Action wasspi_perl_su -S wasspi_ca -r -m 5 -i "<\$OPTION(servername)>" (execute on node <\$MSG_NODE_NAME>)(creates annotation)
	(Send message after automatic action finished)
	Set (end)
	Severity normal
	Application websphere Application Server
	Content WBSSPI-
	0005.2: % of heap space used (<\$VALUE>%) too high (>=<\$THRESHOLD>%) [Policy: <\$NAME>] [Policy: <\$NAME>]
	Message Key <\$NAME>:<\$MSG_NODE_NAME>:<\$MSG_OBJECT>
	Message key relation ^<\$NAME>:<\$MSG_NODE_NAME>:<\$MSG_OBJECT>\$(ignore case)
	Service name WBS_<\$OPTION(map_servername)>_<\$OPTION(map_port)>_<\$OPTION(node)>
	Server log only on

Modifying Alarm Generation

An alarm can be generated once or multiple times, depending on its Message Generation setting in the Modify Threshold Monitor window.

To modify Message Generation:

- 1 Open the Policy Bank window and click **SPI for WebSphere** → **High-Impact** or **Low-Impact** or **Medium-Impact** → **WBSSPI-Metrics** policy group.
- 2 Select a metric and click **Edit...** from the drop-down list. The drop-down list appears when you click . The Edit Measurement_Threshold Policy “WBSSPI_00xx” window appears.

- 3 Click the **Thresholds** tab and modify the settings for message generation under it.

The screenshot shows the 'Edit Measurement_Threshold Policy' window for 'WBSSPI_0001'. The 'Thresholds' tab is selected. The 'Monitoring Type' is set to 'Minimum'. The 'Threshold 1' configuration is visible, showing a description of 'WBSSPI-0001.1: Critic', a threshold value of '4.5', and a 'Reset' option set to 'Use same as threshold value'.


- 4 Modify the Message Generation settings by selecting the required option from the **Reset** drop-down list:
 - **Use Same as threshold value:** Alarms are generated once when the monitoring threshold value is exceeded. Alarms are reset automatically when metric values are no longer in violation of the thresholds, and are generated again when the threshold is exceeded.
 - **Specify a special reset value...:** Alarms are generated once when the threshold value is exceeded. At the same time, a reset threshold value is activated. Whenever the reset threshold value exceeds the limit, the original threshold value becomes active again. Then, when the threshold value is again exceeded, another alarm is generated and the process starts all over again.
- 5 Click **Save**.
- 6 Redistribute the modified policy (described in [Deploy the WebSphere SPI Policies](#) on page 45).


Advanced Policy Customizations

The policy changes described in this section range from making copies of default policy groups to customize settings, to deleting whole groups of metrics within a policy's command line. This section requires advanced knowledge of the WebSphere SPI metrics.

Choosing Metrics to Customize

Determine which metrics you want to customize, and the policies (within the group) you want to use, and then follow these steps:

- 1 Open the **Policy Bank** window and click **SPI for WebSphere**.
- 2 Select the policy group you want to use, click  and then click **Copy...** from the drop-down list. The Copy Policy Group window appears.
- 3 Rename the group, select the parent group and click **Save**.

- 4 Within the renamed policy group, copy each original policy and rename it (follow the steps 2 and 3).
- 5 Delete the original policies within the renamed policy group by selecting **Delete...** from the **Choose an Action** drop-down list and click  to submit.
- 6 Customize the renamed policies within the group as required.

Creating a new policy group enables you to keep custom policies separate from the original default policies, which you copy and place within the new group.

Using the WebSphere SPI Collector/Analyzer Command

The `wasspi_perl_su -S wasspi_ca -prod wbs` command is used in every collector policy, and named according to its collection interval. You can view the default command line parameters within each collector policy in the Command text box in the Edit Scheduled_Task Policy "*Policy Name*" window.

WebSphere SPI Collector/Analyzer Command Parameters

The WebSphere SPI data collections are started with the `wasspi_ca` command, to which you can add other parameters, as identified in the following table:

Parameter	Description	Syntax
-m (metric)	Specifies the metric numbers or number ranges on which to collect data.	-m <metric_number> Example: -m 1,3-5,9-11,15
-matchver (match version)	Specifies the specific WebSphere application server version to monitor. This option must not be used with the -minver or -maxver options. If no matching versions are found, the command does not run.	-matchver <version_number> Example: -matchver 6
-maxver (maximum version)	Specifies the highest WebSphere application server version to monitor. Use with -minver to specify a range of versions. If no versions are found, the command does not run.	-maxver <version_number> Example: -maxver 7
-minver (minimum version)	Specifies the lowest WebSphere application server version to monitor. Use with -maxver to specify a range of versions. If no versions are found, the command does not run.	-minver <version_number> Example: -minver 6
-r (report)	Generates an ASCII report for the specified metrics	-r
-t (tag)	Creates a new policy group by adding a prefix to an existing collector policy along with the metric numbers.	-m <metric_number> -t <prefix>- Example: -m 220-223 -t DEV-
-i (include)	Lists specific servers to monitor. Must not be used with the -e option.	-i <server_name> Example: -i server1,server3

Parameter	Description	Syntax
-e (exclude)	Excludes specific servers from being monitored. Must not be used with the -i option.	-e <server_name> Example: -e server2,server4
-prod	(production) Identifies the SPIs on which the command is run on the node.	Syntax: -prod <Name of the SPI>- Example: wasspi_perl -S wasspi_ca -prod wbs -m 220-223 -t DEV-
-x	Specifies a property/value as follows:	-x <property>=<property_value>
	alarm: When off, overrides any default alarming defined for the metric.	-x alarm=off
	prefix: Default: JMXUDM_. Specifies the prefix of the metric ID.	-x prefix=SALES_
	print: When on, prints the metric name, instance name, and metric value to STDOUT in addition to any configured alarming or logging.	-x print=on
	log: When off, prevents graphing or reporting functions.	-x log=off

Examples

- To specify metrics to collect:
 - specific data on all configured servers:
`wasspi_ca -prod wbs -m 10-14,25,26`
 - data from specific servers only:
`wasspi_ca -prod wbs -m 245,246,260 -i server1,server2`
- To not collect data from specific servers:
`wasspi_ca -prod wbs -m 220-225 -e server1,server2`

Using JMX Actions Command Parameters

The command parameters described in this section are used to run JMX actions. JMX actions are one or more JMX calls (invoke, get, set) performed on an MBean instance or type. A single JMX call can be performed from the command line. Multiple JMX calls can be specified in an XML file or as a Metric sub-element in a User Defined Metric (UDM) file.

Parameter	Description
-a Required	(action) Indicates a JMX action is performed. Syntax: -a
-i	(include) Enables you to list specific servers on which to perform the JMX actions. If this parameter is not specified, the JMX actions are performed on all configured servers. Syntax: -i <server_name> Example: -i server1,server3
-m	(metric) Specifies the metric ID containing the action to perform. This metric ID must be defined in a UDM file. This option must not be used with the -mbean or -xml options. Syntax: -m <metric_id> Example: -m TestUDM_1000

Parameter	Description
-mbean	<p>Performs a JMX call on the specified MBeans. This option must not be used with the -m or -xml options.</p> <p>Syntax: -mbean <objectname> <action></p> <p>Example: -mbean WebSphere:type=ThreadPool,* -get maximumSize where <action> (a JMX call) is one of the following:</p>
-get	<p>Returns the value of the specified attribute.</p> <p>Syntax: -mbean <objectname> -get <attribute></p> <p>Example: -get maximumSize</p>
-invoke [-type]	<p>Runs an MBean operation with the specified parameters. A type parameter must be specified for operations which accept parameters. -type supports operation overloading. If an operation does not require parameters, -type is not specified.</p> <p>Syntax: -mbean <objectname> -invoke <operation> [-type <parameter_type> <parameter_value>]...</p> <p>In this instance, <parameter_type> is one of the following: short, int, long, double, float, boolean, java.lang.Short, java.lang.Integer, java.lang.Long, java.lang.Double, java.lang.Float, java.lang.Boolean, and java.lang.String.</p> <p>Example: -invoke setInstrumentationLevel -type java.lang.String pmi=L -type boolean true</p>
-set	<p>Assigns the specified value to the specified attribute.</p> <p>Syntax: -mbean <objectname> -set <attribute> <value></p> <p>Example: -set growable true</p>
-o	<p>(object) Specifies an MBean instance.</p> <p>Syntax: -o <mbean_instance></p> <p>Example: -o exampleJMSServer</p>
-xml	<p>Specifies the XML file that contains the JMX actions to perform. This option must not be used with the -m or -mbean options.</p> <p>Syntax: -xml <filename></p> <p>Example: -xml myJMXActions.xml</p>

Examples

- Set the maximum size for an alarming thread pool to 500 (where <\$OPTION(instancename)> specifies an alarming instance):

```
wasspi_perl -S wasspi_ca -prod wbs -a
-mbean WebSphere:type=ThreadPool,* -set maximumSize 500 -o
<$OPTION(instancename)>
```
- Set the instrumentation levels to low on all PMI modules:

```
wasspi_perl -S wasspi_ca -prod wbs -a
-mbean WebSphere:type=Perf,* -invoke setInstrumentationLevel -type
java.lang.String pmi=L
```
- Use the sample UDM TestUDM_1000 in the wasspi_wbs_UDMMetrics-sample.xml file:

```
wasspi_perl -S wasspi_ca -prod wbs -a -m TestUDM_1000
-i examplesServer
```

- Use the sample actions xml file:

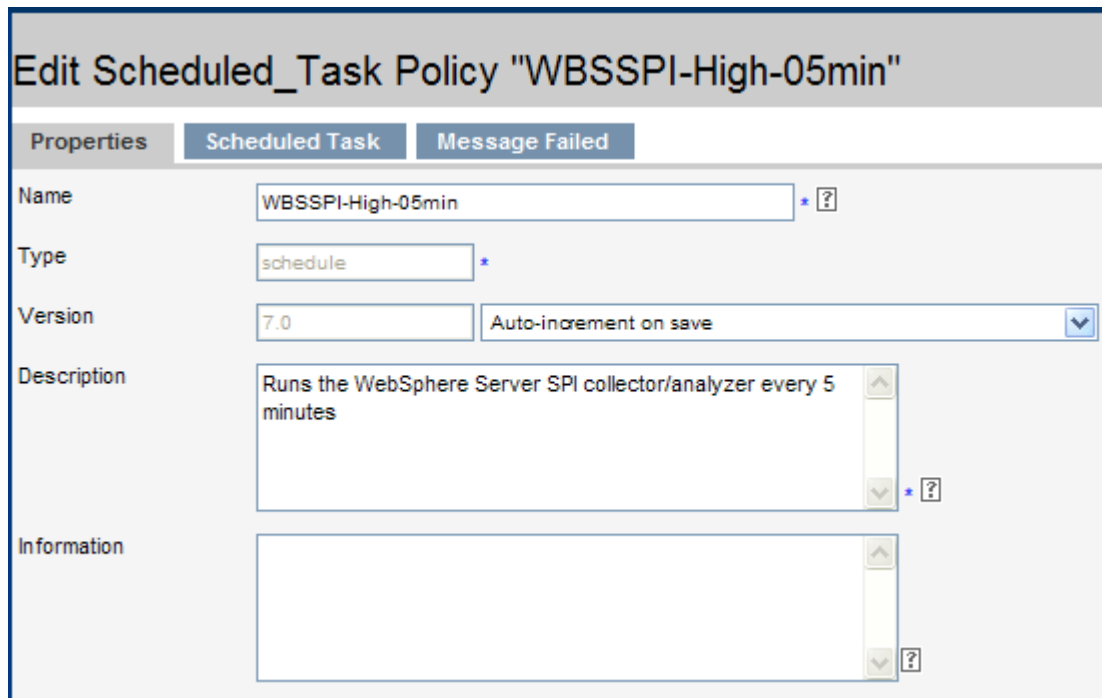
```
wasspi_perl -S wasspi_ca -prod wbs -a
-xml /var/opt/OV/wasspi/wbs/conf/JMXActions-sample.xml
-i examplesServer
```

Changing the Collection Interval for Scheduled Metrics

To change the metric collection interval, simply change the Polling Interval in the appropriate collector policy. For example, to change the collection of default metrics from 5 minutes to 10 minutes for the WebSphere High Impact policy group:

- 1 Open the Policy Bank window and click **SPI for WebSphere** policy group.
- 2 Click **High-Impact** → **WBSSPI-Monitors**.
- 3 Select the collector policy **WBSSPI-High-05min** and click **Edit...** from the drop-down list.

The drop-down list appears when you click . The Edit Scheduled_Task Policy “WBSSPI-High-05min” window appears.



Edit Scheduled_Task Policy "WBSSPI-High-05min"

Properties | Scheduled Task | Message Failed

Name: WBSSPI-High-05min * ?

Type: schedule *

Version: 7.0 Auto-increment on save

Description: Runs the WebSphere Server SPI collector/analyzer every 5 minutes * ?

Information: * ?


Message Failed: * ?

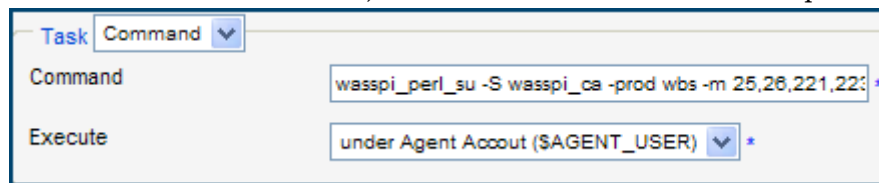
- 4 Change the Name to **WBSSPI-High-10min** and the description accordingly.
- 5 Click the **Scheduled Task** tab and in the Minute box, change the polling interval from 5 minute to 10 minutes. For example, 0, 10, 20....
- 6 Click the **Message Failed** tab and change the message text.
- 7 Distribute the new policies (described in [Deploy the WebSphere SPI Policies](#) on page 45).


Changing the Collection Interval for Selected Metrics

To change the collection interval for selected metrics, copy the appropriate collector policy and rename with a name reflecting the new interval, deleting all but the metrics you are changing. Set the new interval. Edit the original policy to remove the changing metrics.

For example, to change the collection interval to 10 minutes for metrics 221-225:

- 1 Open the Policy Bank window and click **SPI for WebSphere** policy group.
- 2 Click **High-Impact** → **WBSSPI-Monitors**.
- 3 Select the policy **WBSSPI-High-05min** and click **Copy...** from the drop-down list which appears when you click . The Copy Policy WBSSPI-High-05min window appears.
- 4 Change the Name to **WBSSPI-High-10min** and the description accordingly.
- 5 Click the **Scheduled Task** tab.
- 6 In the Command text box, delete all metrics after the -m except 221-225.



- 7 In the Minute box, change the polling interval from 5 minute to 10 minutes. For example, 0, 10, 20....
- 8 Click **Save**.
- 9 In the High-Impact policy group, select the WBSSPI-High-05min policy.
- 10 Click **Edit...** from the drop-down list which appears when you click . The Edit Scheduled_Task Policy “WBSSPI-High-05min” window appears.
- 11 Click the **Scheduled** Task tab.
- 12 Delete 221-225 from the Command text box.
- 13 Click **Save**.
- 14 Redistribute the modified policies as described in [Deploy the WebSphere SPI Policies](#) on page 45.

Customize the Threshold for Different Servers

You can customize the threshold for different servers. For example, you might want to set the threshold to 20 for SERVER_1 for metric 0212 and leave the threshold at 10 for all other servers. To do so, copy the existing condition and modify it to serve as an exception. Follow these steps:

- 1 Double-click the metric to open the metric for customization (for example, double-click **WBSSPI-0212**). The Message and Suppress Conditions window appears.
- 2 Select the desired condition and click **Copy...** to make a copy of the condition.
- 3 Name the condition **WBSSPI-0212 . 2**.
- 4 In the Object Pattern field, enter the following details:
`<ServerName>:<ServerPort>:<NodeName>:<*>:<*>:<*>`

Example: To set threshold for the application server SERVER1, enter the following:

```
SERVER1 :<*>:<*>:<*>:<*>:<*>
```

- 5 Click **Test Pattern Matching...** to test the pattern and verify pattern matching (you must set up a match file first).
- 6 Change the value in the Threshold field from 10 to 20.
- 7 Click **Save**.

Creating Custom, Tagged Policies


Another advanced customization option is to use the tag option (`-t` on the command line), which enables the collector/analyzer to recognize customized policies that have a tag attached to the name. This option provides you with the flexibility of using more than a single set of policies to define conditions pertaining to specific installations of a WebSphere Server. It also preserves policies from being overwritten when you upgrade the WebSphere SPI.

When multiple nodes are managed by a number of groups, this option enables you to create specially tagged policies that are obviously separate from your original setup. In such a case, you would make copies of the policies, rename them with the tag, re-work the collector policy to pick up the tagged names, and assign them to the various groups.

For example, you can create a group of policies and change each policy name to include CLIENT01 in it. You can name a metric monitor policy as CLIENT01-WBSSPI_0212 (retaining the metric number, which must be used) and name the collector policy as FIRST_CLIENT-40-05min. You can then set up another group for SECOND_CLIENT and change all those policies to include the CLIENT02 in the name.

Create a New Policy Group

To create a new policy group:

- 1 Copy the original policy group. In the Policy bank window, select the group, and click **Copy...** from the drop-down list which appears when you click . The Copy Policy Group window appears.
- 2 Name the new group according to your plan to identify the new monitor and collector policies. For example, if you are including CLIENT01 in the policy names, include that within the new policy group name.
- 3 In the Policy bank window, click the policy groups to show all policies and select each policy you plan to use, click **Copy...** from the drop-down list (as given in step 1 and 2), and rename it according to your naming scheme.
 - The names you give the new metric monitor policies in the group should contain the new name followed by the original metric number. For example, a copy of WBSSPI-0001 could be called CLIENT01-WBSSPI_0001.
 - The name you give the new collector monitor policy should also contain the identifying name. You would also modify the scheduled collection for the new group by inserting the `-t` property on the command line. For example:

```
wasspi_ca -m 16 -t CLIENT01-
```
- 4 Delete all original policies from the new group.

Policy Variables

The following variables are used by the WebSphere SPI policies. If you are creating your own policies, you can use these variables.

Name	Description
instancename	The instance for which the metric is being reported for multi-instance metrics.
map_port	See port . This variable could be deprecated in future releases.
map_servername	The application server name with spaces replaced with underscores (“_”). Used for service map keys where spaces are prohibited. Example: my_server
node	The node on which the application server is running. Example: moo1.hp.com
port	The port on which the application server is listening. Corresponds to the PORT configuration property. Example: 9001
servername	The application server name. Corresponds to the NAME configuration property. Example: my server

Monitoring a WebSphere Server on Unsupported Platforms

The WebSphere SPI supports monitoring WebSphere Server systems running on HP-UX, Solaris, Linux (Red Hat), AIX, and Windows 2000. However, it is possible to configure the WebSphere SPI to monitor WebSphere Server systems running on unsupported platforms, in other words, “remote systems.”

This section explains how to determine if your environment is conducive to setting up remote monitoring.

Requirements for Monitoring Remote Nodes

For a WebSphere Server system running on an unsupported platform, you can use the WebSphere SPI to monitor that remote system if the following conditions apply:

- The remote system is covered by a purchased license (using Tier 1 pricing).
- The WebSphere SPI runs on at least one managed node on a supported platform: HP-UX, Solaris, Linux (Red Hat), AIX, or Windows 2000.
- The local/proxy system and remote system must be running the same version of WebSphere Server. For example if the proxy system is running WebSphere Server version 6, the remote system must also be running WebSphere Server version 6.
- (Optional, for logfile monitoring) The remote system runs on a platform supported by the HP Operations agent software.

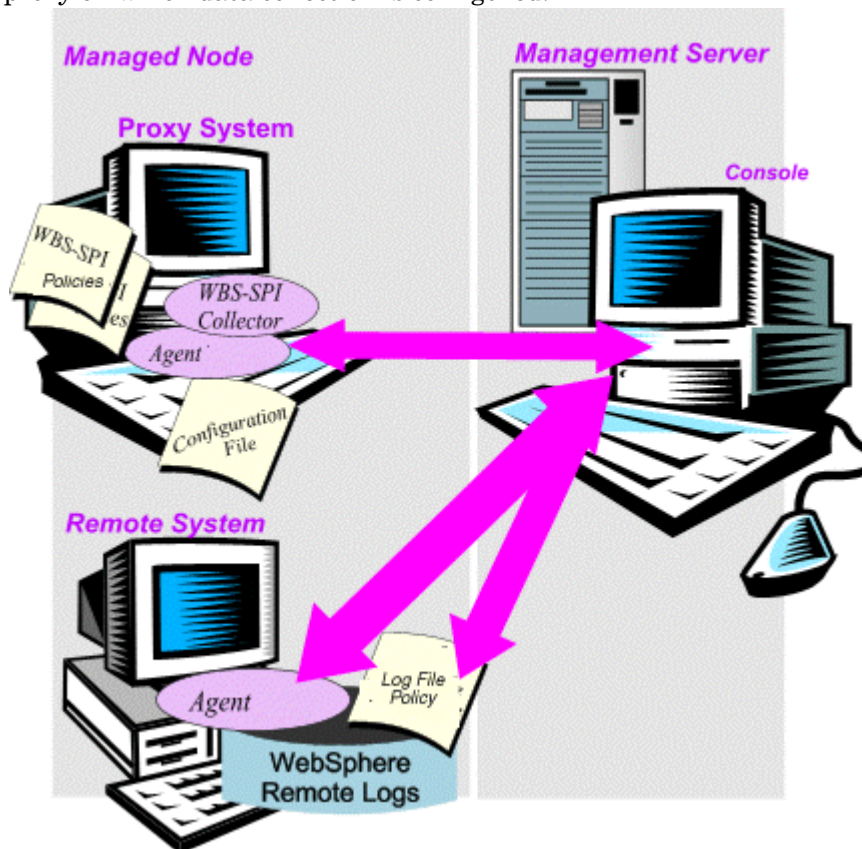
- The proxy node and the remote node should have the same configuration, that means, if the proxy node is a Network Deployer, the remote node should be also be a Network Deployer. Also, if the proxy node is a Non-Network Deployer, the remote node should also be a Non-Network Deployer.

Remote Monitoring

The following section provides an overview of remote monitoring and how to implement it. It also includes details on how to set up the WebSphere SPI to access WebSphere Server metrics and logfiles on unsupported platforms by using both, the WebSphere SPI and HP Operations agent software.

In a standard configuration, the WebSphere SPI programs/policies are deployed on the local, managed node. In a non-standard configuration, the local system is used as a proxy through which remote metric information becomes accessible.

Remote system data collection/interpretation relies on the local managed node to act as the proxy on which data collection is configured.



Configuration entries requirement: Within the configuration, entries for both local and remote systems are included. You can include multiple remote system entries in a local system's section. See example on [Configure the Remote WebSphere Server System](#) on page 85, to know how the remote entry appears (with system IP address).

Policy deployment requirement: Policies for the correct WebSphere PMI level should be deployed on the local node. If you need a separate policy group (for example High Impact or Medium Impact) to cover a different level, you can copy and rename the existing policies and specify the WebSphere Server name on the command line using the `-i` or `-e` options. For information about using these command line parameters, see [Using the WebSphere SPI Collector/Analyzer Command](#) on page 76.

HP Operations agent deployment requirement (optional logfile monitoring): To access remote WebSphere Server logfiles, the HP Operations agent software must be installed on the remote system. Using standard HPOM processes, you can modify the standard logfile policies included with the WebSphere SPI to specify the correct logfile names, and then deploy them to the remote system.

▶ You cannot monitor remote systems using logfile versioning.

Configuring Remote System Monitoring

You can monitor a WebSphere Server on remote systems (running on platforms other than HP-UX, Solaris, Linux, AIX, or Windows 2000) by completing the following tasks:

▶ You *must* not enable administrative security on the remote systems. If you have enabled the administrative security on the remote systems, add the remote node signer to the local node's trust store to configure remote system monitoring.

Configure the Remote WebSphere Server System

Using the Discover or Configure WBSSPI tool in the SPI Admin tools group, configure each local managed node that communicates with a remote WebSphere Server. In the configuration, include additional entries for remote WebSphere Servers.

- 1 From the HPOM console, select **Integrations** → **HPOM for Unix Operational UI**.
- 2 Choose a WebSphere Application Server managed node from which you need to monitor the remote WebSphere Server.
- 3 Right-click on the node and select **Start** → **SPI for WebSphere** → **SPI Admin** → **Discover or Configure WBSSPI**. The Tool Selector window appears.
- 4 Select **Launch Configure Tool** button and click **OK**. The Configuration Editor appears.
- 5 Right-click on the node and select **Add Application Server**. The Configure WBSSPI tool: Add App Server window appears.
- 6 Enter the Application Server Name. This is the name of the remote WebSphere Server.
- 7 Enter the Server Port.
- 8 Set the configuration properties by selecting the property from the **Select a Property to Set...** drop-down list, click **Set Property**, and set the value for the property.

In the configuration that appears, include an entry for each remote WebSphere Server system: LOGIN, PASSWORD, ADDRESS, VERSION, HOME, JAVA_HOME, PROFILE_HOME. The values for LOGIN, PASSWORD, ADDRESS, and VERSION must be of the remote system and the values for HOME, JAVA_HOME, PROFILE_HOME must be of the local system. Enter a user defined value to ALIAS.

For example:

```
SERVER1_ADDRESS=15.155.81.123
SERVER1_ALIAS=dmgr on server1 port 8809
SERVER1_HOME=C:/Program Files/IBM/WebSphere/AppServer
SERVER1_JAVA_HOME=C:/Program Files/IBM/WebSphere/AppServer/java
SERVER1_LOGIN=admin
SERVER1_NAME=dmgr
```

```
SERVER1_PASSWORD=admin
SERVER1_PORT=8809
SERVER1_PROFILE_HOME=C:/Program Files/IBM/WebSphere/AppServer/profiles/
Dmgr01
SERVER1_VERSION=7.0.0
```

- 9 Click **Save** to save any changes made to the configuration. After you save the changes, you cannot undo the changes automatically.
- 10 Click **Next**, select the local server and click **OK**.
- 11 Click **Finish** to exit the editor and start configuring the WebSphere SPI on the local server.



If you click **Cancel**, the changes made by you are not saved to the selected managed nodes' configuration and remain in the configuration on the management server.

After the configuration is successful, run discovery on the local node (see [Run Discovery](#) on page 43) and verify the discovery process (see [Verify the Discovery Process](#) on page 44).

Integrate the HP Performance Agent (Optional)

Since the HP Performance Agent collection occurs on the managed node (not the remote system), if you use PerfView and want to graph the remote system data, make sure that integration is enabled on the (local) managed node.

Assign Local Node to a WebSphere SPI Node Group

Assign the local managed node to the appropriate node group. For example, you can assign the local node to the WebSphere High node group, if the local and remote managed nodes collect metrics that require the system to be set at a high WebSphere PMI level.

Configuring Remote Logfile Monitoring (Optional)


Monitoring remote system logfiles is supported if both the following are true:

- The remote system has an HP Operations agent running on it.
- The system does not re-version logfiles when they roll.

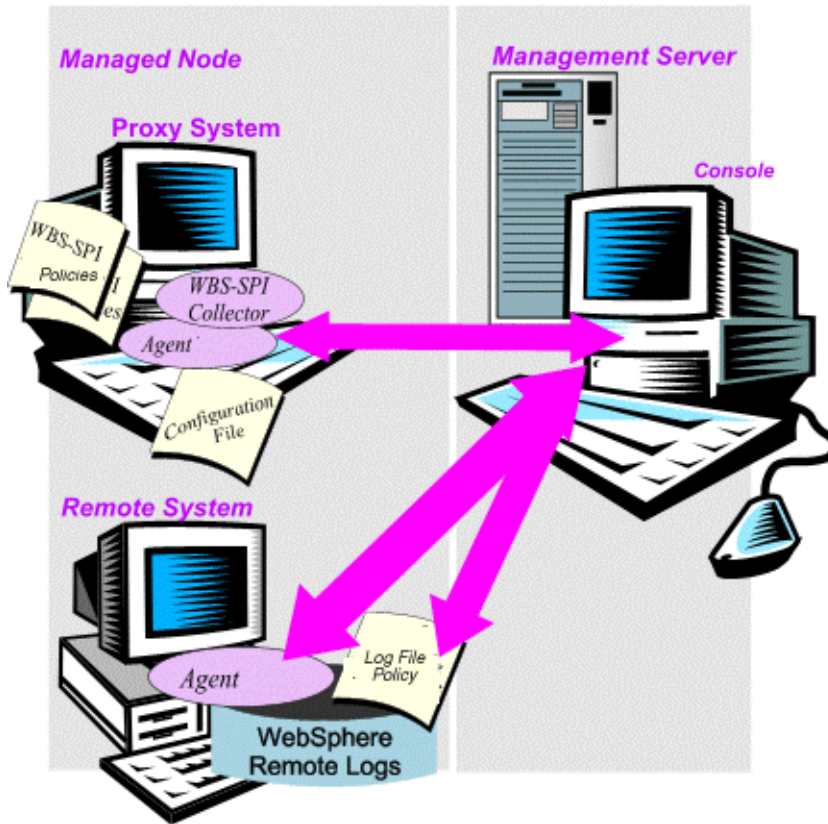
To set up logfile monitoring at the HPOM console, copy the WebSphere SPI logfile policy and then configure, assign, and deploy the copied logfile policy to the remote system.

Configure the Logfile Policy for Remote Logfiles

To configure the logfile policy for remote logfiles:

- 1 Select a copy of the WebSphere Log Policy located under WBSSPI-Logfiles in the SPI for WebSphere group. For example, **SPI for WebSphere** → **High-Impact** → **WBSSPI-Logfiles** → **WBSSPI Error Log**.
- 2 Click **Edit...** from the drop-down list which appears when you click . The Edit LogFile_EntryPolicy “WBSSPI Error Log” window appears.
- 3 Click the **Source** tab and in the **Logfile** text box, enter the location of the logfile on the remote system: `/<path>/<file_name>`.
- 4 Assign and deploy the logfile policy to the remote HPOM managed node.

It is possible to monitor WebSphere Server logfile only if the log file policy and the HP Operations agent are present on the remote system.



Limitations of Remote Monitoring

The limitations of remote monitoring are as follows:

- The WebSphere SPI and the HP Operations agent do not support access to logfiles that are re-versioned each time the logs are rolled.
- You cannot monitor the WebSphere Server logfiles on the remote system if HP Operations agent is not present on the remote system.
- In the HPOM Tool Bank, you cannot run the WebSphere SPI tools on the remote systems.
- The proxy system and remote system must be running the same version of the WebSphere Server.
- The `SERVER<n>_NAME` and `SERVER<n>_PORT` property cannot be the same for the proxy system and the remote system.

Restoring Default WebSphere SPI Policies

When the WebSphere SPI policies are installed in HPOM, the following commands automatically upload them when `swinstall` is run. Any customized policy settings you have done for the previous installation are overwritten.

To restore the default SPI for WebSphere policy groups you have originally installed:

- 1 Delete all current policies.
- 2 Run the command:

```
/opt/OV/bin/OpC/opccfgupld -silent -replace \  
-subentity var/opt/OV/share/tmp/OpC_appl/wasspi/wbs/wbs_set
```

Alternatively, you can use the `-verbose` option instead of the `-silent` option.

Using Policies/Tools to View Annotation Reports

Some policies have actions defined with threshold violations or error conditions that automatically cause reports to appear under the Annotations tab in the Message Properties window. These reports are snapshots of data values collected from the server around the time when the alarm occurred.



The reports discussed in this section are different from those generated by HP Reporter. The HP Reporter shows a more consolidated, historical data generated as web pages in the management-ready presentation format.

You can access the data as follows:

- To view the Message Properties, double-click a message in the HPOM message browser. Click the **Annotations** tab. Reports are available here, showing data values for a single server.
- To view reports:
 - a From the HPOM console, select **Integrations** → **HPOM for Unix Operational UI**.
 - b Select a node for which you want to generate a metric report.
 - c Right-click on the node and select **Start** → **SPI for WebSphere** → **Metric Reports** → **<Name of the Metric Report>**. The reports will show all server data on a node.

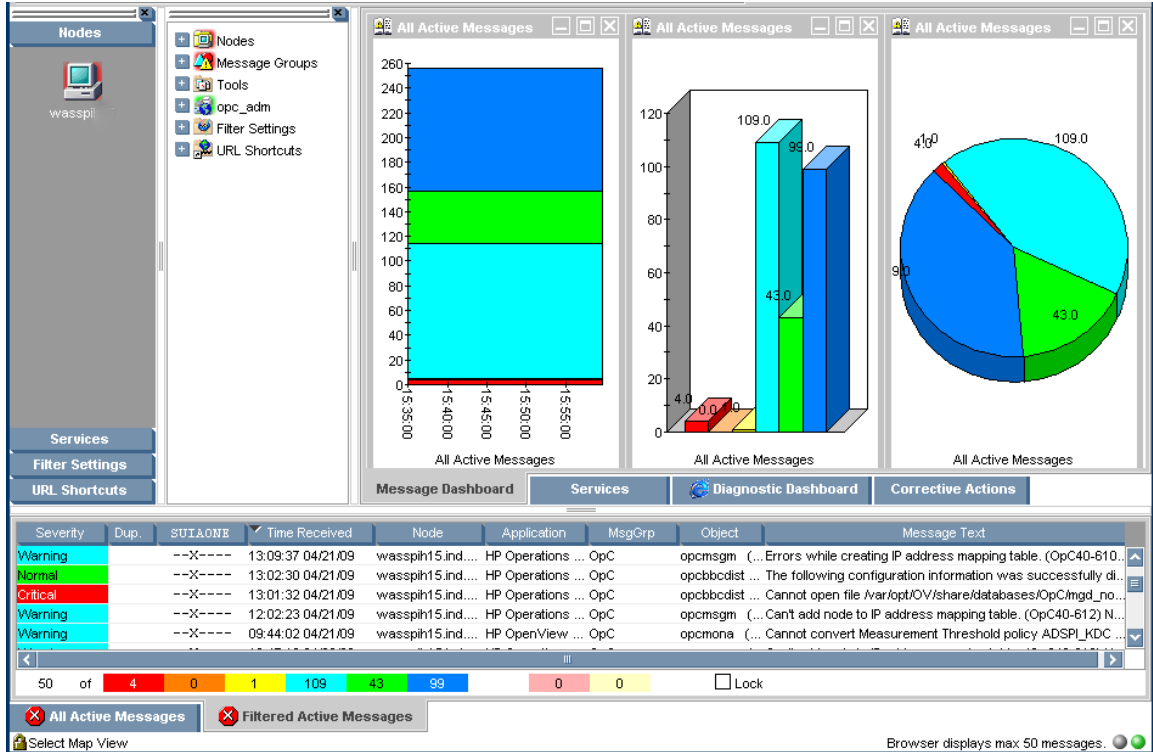
Automatic Action Reports

Many metrics generate Automatic Action Reports. These reports show data on a single WebSphere Application Server instance with an exceeded threshold. They are generated as soon as the alarm is triggered in the HPOM.

Viewing an Automatic Action Report

When an Automatic Action Report is run from HPOM, the server is queried for additional data. If your message browser is set to display the SUIAONE column, you can see an “S” under the “A” column (see the following illustration), which indicates that a successfully generated report is available under the Annotations tab in the Message Properties window.

Figure 20 Message Browser



To view an automatically generated metric report relating to an alarm condition, double-click the Message Text. Click the **Annotations** tab in the Message Properties window.

Tool Bank Reports

Tool Bank reports run for all WebSphere Application Server instances configured on the managed node. The reports generated from the Tool Bank reflect the current state of a WebSphere Application Server on the managed node. To manually generate these reports:

- 1 From the HPOM console, select **Integrations** → **HPOM for Unix Operational UI**.
- 2 Select a node for which you want to generate a metric report.
- 3 Right-click on the node and select **Start** → **SPI for WebSphere** → **Metric Reports** → **<Name of the Metric Report>**.

The WebSphere SPI reports require that the targeted managed node should have a PMI level setting at or above the rating (as shown in the following table) for the metric you are selecting.

Table 5 Performance Impact Ratings (PMI Levels) of Reporting Metrics

Low	5, 42, 222, 224, 247, 265
Medium	40, 221, 246, 262
High	41, 212, 213, 220, 261, 263, 264

Checking the WebSphere SPI Nodes for License Count

You can use the HPOM reporting utility to check the number of policies installed on the managed nodes. In reviewing the number of policies per managed node, you can see if you have consistently installed policies across your managed systems. In addition, you can also make sure that the number of licenses you purchased, is compliant with the report results.

To run the report:

- 1 At the HPOM console select the node or node group that you want to check.
- 2 From the Actions menu, select **Utilities** → **Reports...**
- 3 Select **WBSSPI License Check** from the Reports window.
- 4 Select an output destination and click **OK**.

6 Integrating the WebSphere SPI with HP Reporting and Graphing Solutions

This chapter explains how to integrate the WebSphere Application Server SPI with different HP reporting and graphing products (these products must be purchased separately) which help to view performance and availability and analyze trend.

The WebSphere SPI can be integrated with the following HP reporting and graphing products:

- **HP Reporter-** HP Reporter produces management-ready, web page reports, showing historical and trending information. Working in conjunction with HP Reporter, the WebSphere SPI produces a variety of reports showing consolidated information on the WebSphere Application Server.

After integrating the WebSphere SPI with HP Reporter, HP Reporter generates reports every night, that show the performance and availability of the WebSphere Application Server on configured managed nodes. For information on how to integrate HP Reporter with the WebSphere SPI, see [Integrating with HP Reporter](#) on page 92.

- **HP Performance Agent-** HP Performance Agent collects, summarizes, time stamps, and detects alarm conditions on current and historical data across your system. It provides performance, resource, and end-to-end transaction response time measurements, and supports network and database measurement information. For information about HP Performance Agent, see *HP Performance Agent for UNIX User's Manual*.

The WebSphere SPI automatically uses HP Performance Agent, if you have integrated the HP Performance Agent with the WebSphere SPI. If you want to use the HP Operations subagent (CODA) that is included with HP Operations Manager (does not support HP Performance Agent), you must configure your managed nodes to do so. For more information, see [Integrating with CODA](#) on page 56.

- **HP Performance Insight-** HP Performance Insight is a network management system that collects, processes, and reports data. This data is used to generate reports. For more information on HP Performance Insight, see the *HP Performance Insight Administration Guide*.

For information on how to integrate the WebSphere SPI with HP Performance Insight and generate reports, see the *Application Server Report Pack User Guide*.

- **HP Performance Manager-** HP Performance Manager provides graphing capability. It generates graphs of the WebSphere SPI metrics data.

For information on how to integrate the WebSphere SPI with HP Performance Manager, see [Integrating with HP Performance Manager](#) on page 94. After integrating the WebSphere SPI with HP Performance Manager, graphs are available the following day.


Integrating with HP Reporter

The WebSphere SPI must be installed and configured before it can be integrated with HP Reporter.

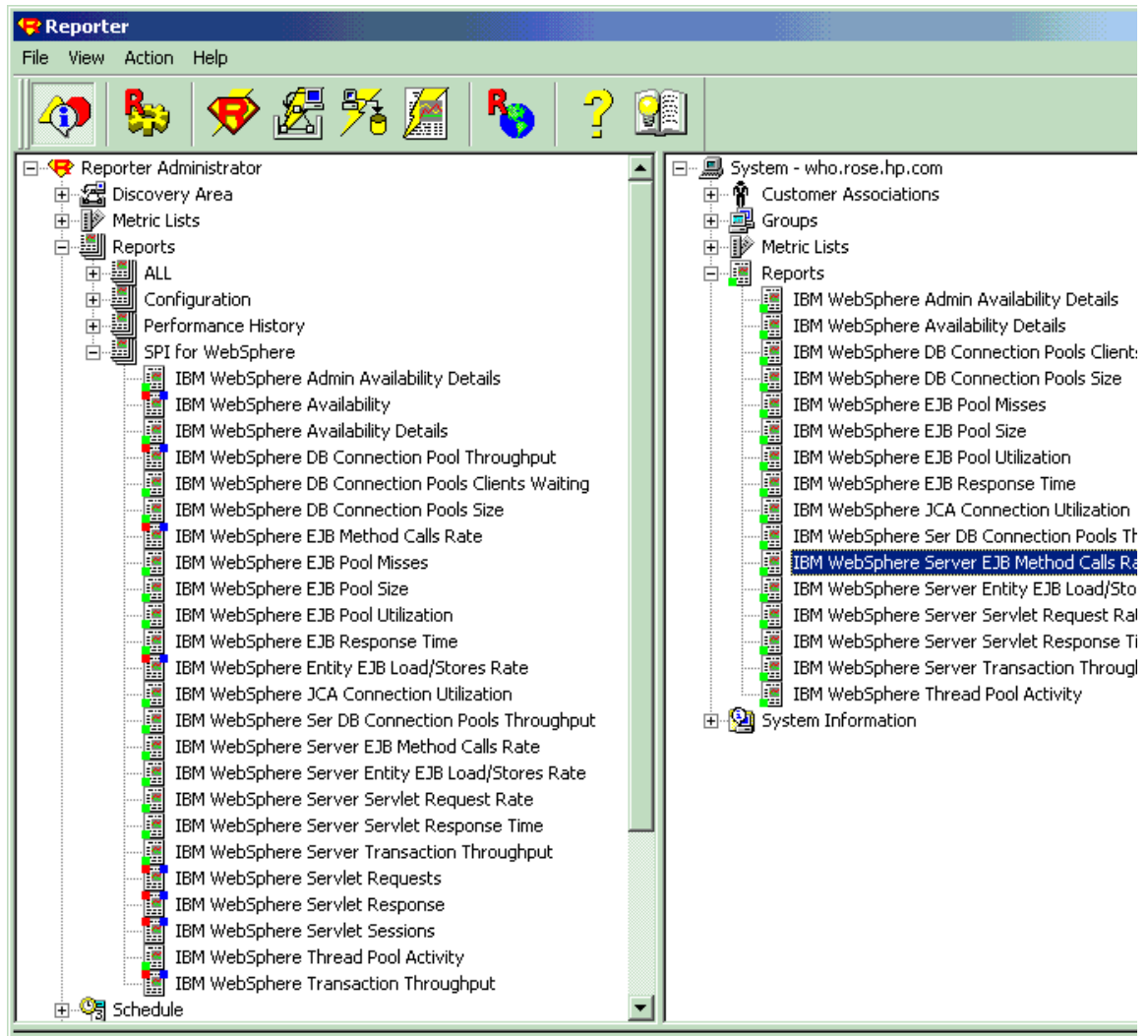
If you are upgrading the WebSphere SPI report package, you must remove the old version before installing the new version. See [Install the New Report Package \(Optional\)](#) on page 34.

The WebSphere SPI report package must be installed on the Windows system running HP Reporter. To install:

- 1 On the Windows client system, insert the Smart Plug-ins DVD-ROM (that contains the reporting packages) into the DVD-ROM drive, and in Windows Explorer, double-click:
`\WINDOWS\HP_REPORTER\WEBSPI\WBSSPI-Reporter.msi`
- 2 Follow the instructions as they appear.
- 3 Check the HP Reporter status pane to note changes to the HP Reporter configuration.

 For Windows 2000 managed nodes, during the installation, an error message might appear that indicates the installer has detected an older version of the installer on your system. You can safely ignore the message and continue.

The HP Reporter main window displays IBM WebSphere Availability and Performance reports.



You can find instructions in the Reporter Help menu for assigning the WebSphere SPI reports to the targeted nodes. To access help, select Reports or Discovered Systems in the left panel of the Reporter main window and right-click it. Select Report Help or Discovered Systems Help from the submenu that appears and see the topic “To assign a report definition to a Discovered Systems Group.”

- 4 Add group and single system reports by assigning reports as desired. See the Reporter help and the *HP Reporter Concepts Guide*.

▶ Group and single system WebSphere SPI reports require that you identify systems by their full name. For example, `abc.xyz.com` is acceptable while `abc` is not.

For information on the reports generated on integrating the WebSphere SPI with HP Reporter and HP Performance Insight, see *HP Operations Smart Plug-in for IBM WebSphere Application Server Reference Guide*.



The browser crashes when the report is huge thus you will not be able to view the report (in HTML). The workaround is to view the reports as a pdf.

Integrating with HP Performance Manager

To integrate the WebSphere SPI with HP Performance Manager:

- 1 Install and configure the WebSphere SPI. Verify that you set the GRAPH_URL property. For more information, see [Property Definitions](#) on page 132.
- 2 If you are upgrading the WebSphere SPI graph package, remove the old version before installing the new version. For more information, see [Install the New Report Package \(Optional\)](#) on page 34.
- 3 Install the graph package.

On a Windows system running HP Performance Manager:

- a Insert the Smart Plug-ins DVD-ROM (that contains the packages) into the DVD-ROM drive, and in Windows Explorer, double-click
`\WINDOWS\HP_PM\WEBSPI\HPOvSpiWbsG.msi`.
- b Follow the instructions as they appear.

On an HP-UX system running HP Performance Manager, which is not the HPOM management server, follow these steps (if HP Performance Manager is installed on the HPOM management server, then the files are already installed when you install the SPI software):

- a Mount the Smart Plug-ins DVD-ROM (that contains the reporting packages) and type:

```
swinstall -s <mount_point>/HPUX/  
HP_Operations_Smart_Plug-ins_HPUX.depot WBSSPI-GRAPHS
```

On a Solaris system running HP Performance Manager, which is not the HPOM management server, follow these steps (if HP Performance Manager is installed on the HPOM management server, then the files are already installed when you install the SPI software):

- a Mount the Smart Plug-ins DVD-ROM (that contains the reporting packages) and type:

```
/usr/sbin/pkgadd -d <mount_point>/SOLARIS/  
HP_Operations_Smart_Plug-ins_Solaris_setup.bin HPOvSpiWbsG
```

- 4 To graph any WebSphere Server metric, use the data source name `WBSSPI_METRICS`.

For information on how to view the graphs, see the HP Performance Manager documentation.



Graphs are available the following day.

Integration Example

The following example describes how to graph multi-instance data stored in a data source by reporting each OBJECTNAME for the METRICID for each SERVERNAME. The result is all data for all instances are reported in one graph. The data for each SERVERNAME can also be displayed in a separate graph.

This example uses the Java interface option of the HP Performance Manager.

- 1 Start the Java Interface option of HP Performance Manager. The Performance Manager Java Interface window appears.

- 2 From the Performance Manager Java Interface window:
 - a Click the **Display** tab at the top of the window, and then the **Sources** tab at the right of the window.
 - b Click next to the Datasource text box and select a data source (WBSSPI_RPT_METRICS).
 - c Click next to the Default Selection text box and select the node on which the data source resides.
- 3 Click the **General** tab at the right of the window.
- 4 From this window,
 - a Select **line** from the **Type** drop-down list. This generates a line graph.
 - b Enter a Date Range.
 - c Enter an interval using the **Points Every** drop-down list.
 - d Click **Label (alphabetical)** if you want the graph key sorted alphabetically.
- 5 Click the **Metrics** tab at the right of the window and click **Add**. The Metric Selection window appears.
- 6 From the Metric Selection window,
 - a Next to the WBSSPI_RPT_METRICS data source, click **+** to expand it in the tree.
 - b Select the **VALUE** check box.
 - c Click **OK**.
- 7 In the window with the Metrics tab selected, VALUE is displayed. Select the line on which VALUE is displayed and click **Properties**. The Metric Properties window appears.
- 8 From the Metric Properties window,
 - a In the Label text box, enter:
 - **@@SERVERNAME : @@OBJECTNAME** if you are creating one graph with all SERVERNAMES
 - **@@OBJECTNAME** if you are creating one graph with one SERVERNAME
 - b In the Marker drop-down list, select any marker other than none.
 - c In the Missing Data drop-down list, select:
 - **previous** to use the previous value if data is missing from the data source
 - **zero** to use the value zero if data is missing from the data source
 - d Click next to the Filter text box. The Metric Filter window appears.
- 9 From the Metric Filter window,
 - a Select **METRICID** from the first drop-down list.
 - b Select **=** from the second drop-down list (if it is not already selected).
 - c Enter a metric number (for example, 11) in the text box.
 - d Click **OK**.
- 10 From the Metric Properties window,
 - a In the Filter text box, append the following:

- `&&SERVERNAME=@&&OBJECTNAME=@@` if you want one graph to display all SERVERNAME/OBJECTNAME combinations.
- `&&SERVERNAME="<server_name>"&&OBJECTNAME=@` if you want one graph to display one SERVERNAME and all OBJECTNAMEs associated with the multi-instance metric.

If you cannot edit the Filter text box, you can edit this item in the graph template file. See [step 13](#).

- b Click **OK**.
- 11 Click **Save As** at the top of the window. The Save As window appears.
- 12 From the Save As window:
 - a Enter a family (for example, **WBSSPI_Graphs**) in the Family text box. The family name serves as a group to organize the graphs.
 - b Enter a name (for example, **metric_11**) in the Name text box to uniquely identify the graph.
 - c It is optional to enter text into the Category text box.
 - d Click **OK**. The information is saved in a graph template file named `VPI_GraphsUser<family>.txt` (for example, `VPI_GraphsUserWBSSPI_Graphs.txt`).

For more information on this window, see the Help menu at the right of the Java Interface window.

- 13 Edit the graph template file. The file is located in the HPOM data directory on the system of the HP Performance Manager instance on which you are working. The graph file might look similar to the graph in following example.


```

#*****
#* OpenView Performance Manager
#* user Defined Graph Templates
#* Last Updated: 07/25/04 04:31_30 AM by [1.2.3.4] moo1
#*****
FAMILY: WBSSPI_Graphs
GRAPH: Metric11
GRAPHBACKGROUND: None
DATERANGE: 1 day
GRAPHMULTIPLEGRAPHS: Yes
POINTSEVERY: raw
DATASOURCE: mwa
SYSTEMNAME: moo1

CLASS: WBSSPI_RPT_METRICS:WBSSPI_RPT_METRICS
METRIC: VALUE
FILTER: METRICID=11&&SERVERNAME=@&&OBJECTNAME=@
LABEL: @@SERVERNAME: @@OBJECTNAME
COLOR: Auto
MARKER: rectangle
MISSINGDATA: previous
END_GRAPH:

#*-----
GRAPH: Metric11_2
GRAPHBACKGROUND: None
DATERANGE: 1 day
GRAPHMULTIPLEGRAPHS: Yes
POINTSERY: raw
DATASOURCE: mwa
SYSTEMNAME: moo1

CLASS: WBSSPI_RPT_METRICS:WBSSPI_RPT_METRICS
METRIC: VALUE
FILTER: METRICID=11
LABEL: @@SERVERNAME: @@OBJECTNAME
COLOR:Auto
MARKER: rectangle
MISSINGDATA: previous
END_GRAPH:

```

There can be more than one set of data for a graph in the graph template file.

- a Add **SUMFROMRAW**: to the end of the first section of each graph (in the preceding example, add **SUMFROMRAW**: after `SYSTEMNAME: moo1`). This enables HP Performance Manager to summarize data from the data source and cannot be added using the interface.
- b If you were unable to edit the Filter text box in the Metrics Properties window in step 10 mentioned earlier, edit the `FILTER` field.
- c Save the file. The graph file now contains the following:

```

*****
#* OpenView Performance Manager
#* user Defined Graph Templates
#* Last Updated: 07/25/04 04:31_30 AM by [1.2.3.4] mool
*****
FAMILY: WBSSPI_Graphs
GRAPH: Metric11
GRAPHBACKGROUND: None
DATERANGE: 1 day
GRAPHMULTIPLEGRAPHS: Yes
POINTSEVERY: raw
DATASOURCE: mwa
SYSTEMNAME: mool
SUMFROMRAW:

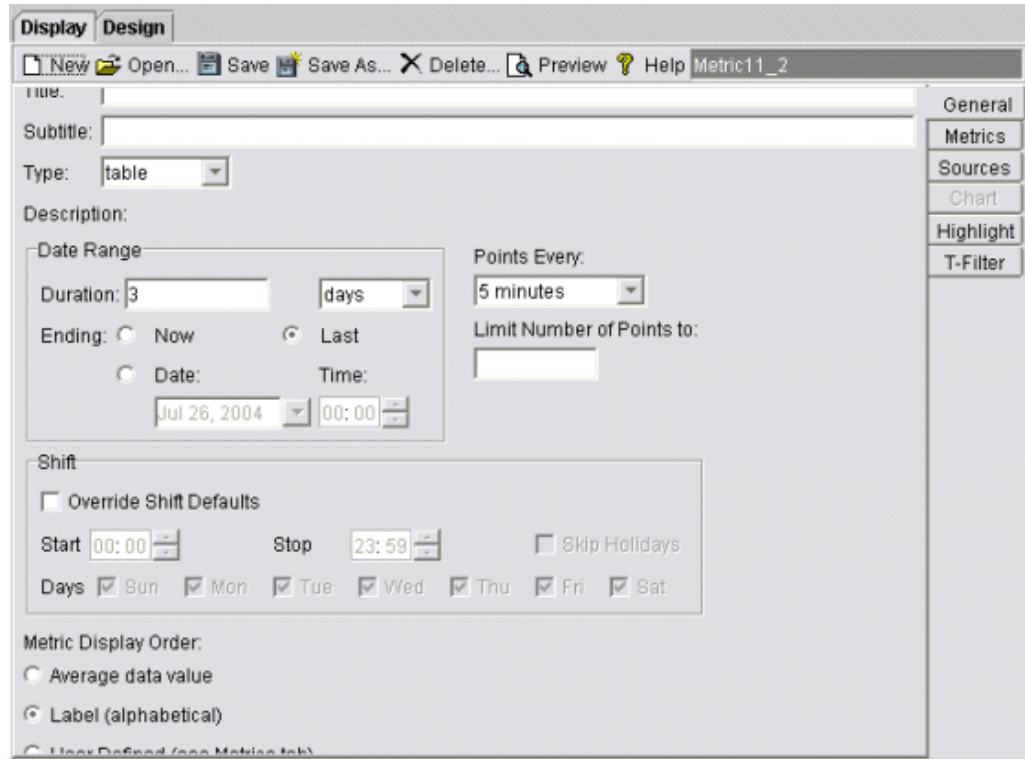
CLASS: WBSSPI_RPT_METRICS:WBSSPI_RPT_METRICS
METRIC: VALUE
FILTER: METRICID=11&&SERVERNAME=@&&OBJECTNAME=@
LABEL: @@SERVERNAME:@@OBJECTNAME
COLOR: Auto
MARKER: rectangle
MISSINGDATA: previous
END_GRAPH:

#*-----
GRAPH: Metric11_2
GRAPHBACKGROUND: None
DATERANGE: 1 day
GRAPHMULTIPLEGRAPHS: Yes
POINTSEVERY: raw
DATASOURCE: mwa
SYSTEMNAME: mool
SUMFROMRAW:

CLASS: WBSSPI_RPT_METRICS:WBSSPI_RPT_METRICS
METRIC: VALUE
FILTER: METRICID=11&&SERVERNAME=@&&OBJECTNAME=@
LABEL: @@SERVERNAME:@@OBJECTNAME
COLOR:Auto
MARKER: rectangle
MISSINGDATA: previous
END_GRAPH:

```

- 14 From the Performance Manager Java Interface window, click the **Display** tab.



- 15 In this window,
 - a In the window below the Sources text box, navigate to the server on which the data source resides.
 - b In the Graphs window, navigate to the family of graphs and select the graph you created.
 - c Enter information into the Date Range dialog box and Points Every text box.
 - d Click **Draw**. The graph appears.

➤ If you edit the graph from the Design tab, the `SUMFROMRAW:` entry is deleted from the graph template file. You must edit the graph template file and re-enter this entry.
- 16 From the SPI, to enable graphing:
 - a From the HPOM console, select **Integrations** → **HPOM for Unix Operational UI**.
 - b Select the nodes which you want to enable for graphing.
 - c Right-click on the nodes and select **Start** → **JMX Metric Builder** → **WBSSPI** → **UDM Graph Enable**. Graphing will be enabled from the SPI.

7 Troubleshooting

This chapter provides information on basic troubleshooting and an overview of the error messages for the WebSphere AS SPI.

Self-Healing Info Tool

The Self-Healing Info tool gathers the WebSphere SPI troubleshooting data and stores this data in a file that you can submit to HP Support for assistance. For information on how to use this tool, see [Self-Healing Info](#) on page 61.

- ▶ The file created by the Self-Healing Info tool might be hidden on some Windows managed nodes. If you do not see the file, open Windows Explorer and, from the Tools menu, select **Folder Options**. Click the **View** tab. Under Hidden files and folders, select **Show hidden files and folders**.

Log File Monitoring

Log file monitoring for WebSphere Application Server is now done through JMX event notification. Log file monitoring is supported on both federated servers as well as standalone installations.

- ▶ Log files are monitored when the collector is running in PERSISTENT mode. By default, the collector runs in PERSISTENT mode.

When the collector runs for the first time, the WebSphere SPI is registered to receive the notifications directly from the WebSphere Application Server. The notification messages are written into log files which are monitored by the WBSSPI LogFile Policies, depending on the configuration of the WebSphere SPI. The following use cases explain the different scenarios:

Use Case 1: You have implemented the network deployer scenario (`DISTRIBUTED_MODE=TRUE` in SPIConfig file).

All notification messages received from all the servers (including deployment manager, node agents, and federated servers) configured to the Distributed Managers are written in the `wbs.log` file. The file is located at `<Agent_Dir>/wasspi/wbs/log/`. By default, `<Agent_Dir>` is `/var/opt/OV/` for UNIX and Linux. For Windows it is `\Documents and Settings\All Users\Application Data\HP\HP BTO Software\`. WebSphere SPI maintains one archived file (`wbs.log.1`) of size 10 MB.

Use Case 2: You have not implemented the network deployer scenario (DISTRIBUTED_MODE=FALSE in SPICongig file).

All notification messages received from the servers, discovered and listed in the SiteConfig file, are written in the `wbs_<servername>.log` file. `<servername>` is the name of the server corresponding to the entry in the SiteConfig file. One log file is maintained for one server.

For example: If there are three discovered servers (S1, S2, S3) in your environment, the notification messages will be written in `wbs_S1.log`, `wbs_S2.log`, and `wbs_S3.log`.

The file is located at `<Agent_Dir>/wasspi/wbs/log/wbs_<servername>.log`. By default, `<Agent_Dir>` is `/var/opt/OV/` for UNIX and Linux. For windows it is `\Documents and Settings\All Users\Application Data\HP\HP BTO Software\`. WebSphere SPI maintains an archived file (`wbs_<servername>.log.1`) of 10 MB for each discovered server.

Use Case 3: You have implemented the network deployer scenario, but want to use the WebSphere SPI discarding the network deployer scenario (OVERRIDE_DISTRIBUTED_MODE=TRUE in SPICongig file).

All notification messages from all servers (which are discovered and listed in the SiteConfig or SPICongig file) are written in the `wbs_<servername>.log` file. `<servername>` is the name of the server corresponding to the entry in SiteConfig. WebSphere SPI maintains one log file for each of the servers.

For example: If there are four discovered servers (S1, S2, S3, and S4) in your environment, the notification messages are written into `wbs_S1.log`, `wbs_S2.log`, `wbs_S3.log`, and `wbs_S4.log`.

The file is located at `<Agent_Dir>/wasspi/wbs/log/`. By default `<Agent_Dir>` is `/var/opt/opt/OV/` for UNIX and Linux. For Windows it is `\Documents and Settings\All Users\Application Data\HP\HP BTO Software\`. WebSphere SPI maintains an archived file (`wbs_<servername>.log.1`) of 10 MB for each discovered server.



JMX Notification does not monitor `SystemOut.log` and `SystemErr.log` files. These files are still monitored through the WebSphere Text Logs policy. Therefore, the WebSphere SPI monitors `SystemOut.log` and `SystemErr.log` files for deployment managers and the configured servers (excluding node agents) only if the files reside on the same node (physical machine) where the SPI is deployed.

Logging

Management Server

The following log file is found on the management server (typically, `/<%OvInstallDir%>/opt/OV`):

File Type	Log
Filename	<code>/<%OvInstallDir%>/wasspi/wbs/log/ <managed_node>_disc_server.log</code>
Description	Records the updates done by the WBSSPI Discovery policy to the management server's configuration for each managed node. Log files are overwritten each time the discovery policy is run on the managed node. Logging to this file is always enabled.

Managed Nodes

The following files for logging are found on the managed nodes running on UNIX or Windows (typically, `<Agent_Dir>/` is `/var/opt/OV/` for UNIX and Linux, and `\Documents and Settings\All Users\Application Data\HP\HP BTO Software\` for Windows):

Directory	<code><Agent_Dir>/wasspi/wbs/log/wasspi_perl.log</code> (archived files have a one digit number appended to the filename)
Description	File used by your HP support representative for debugging. This file gives you information on Perl logging (configuration, discovery, and collection). By default, you can only view the error messages. To view all types of messages (info, warn, and error), run the Start Tracing tool. To stop tracing, run the Stop Tracing tool. For more information on how to run these tools, see Start Tracing on page 63. Three files of different versions are archived.
Directory	<code><Agent_Dir>/wasspi/wbs/log/Discovery.log</code> (archived files have a one-digit number appended to the filename)
Description	File used by your HP support representative for debugging. This file gives you information about the Java discovery logging. By default, you can only view the error messages. To view all types of messages (info, warn, and error), run the Start Tracing tool. To stop tracing, run the Stop Tracing tool. For more information on how to run these tools, see Start Tracing on page 63. Three files of different versions are archived.
Directory	<code><Agent_Dir>/wasspi/wbs/log/Collector.log</code> (archived files have a one-digit number appended to the filename)
Description	File used by your HP support representative for debugging. This file gives you information about the Java Collector logging for the CollectorServer. By default, you can only view the error messages. To view all types of messages (info, warn, and error), run the Start Tracing tool. To stop tracing, run the Stop Tracing tool. For more information on how to run these tools, see Start Tracing on page 63. Three files of different versions are archived.
Directory	<code><Agent_Dir>/wasspi/wbs/log/CollectorClient.log</code> (archived files have a one-digit number appended to the filename)
Description	File used by your HP support representative for debugging. This file gives you information about the Java Collector logging for the CollectorClient. By default, you can only view the error messages. To view all types of messages (info, warn, and error), run the Start Tracing tool. To stop tracing, run the Stop Tracing tool. For more information on how to run these tools, see Start Tracing on page 63. Three files of different versions are archived.

Troubleshooting the Collection

Problem	In a Network Deployer configuration, the collector fails if all the node agents or all the application servers connected to the corresponding node agent stop running. The following error message appears when the collection fails: Unable to collect from server "dmgr" : Empty objectname set returned from queryNames call for objectname 'WebSphere:processType=ManagedProcess,type=Server,*'
Solution	To ensure that the SPI collector works, at least one node agent and one of the corresponding application servers connected to the node agent needs to be running.

Problem	No alarms are received for a metric
Solution	<ul style="list-style-type: none">• Verify that the monitor policy corresponding to the metric is deployed on the node.• Verify that alarm=yes is specified in the <code><Agent_Dir>/wasspi/wbs/conf/MetricDefinitions.xml</code> file for the metric.

Problem	On manually running the collector command on the managed node, the value of the metric is printed as No instance, No data on STDOUT
Solution	Check the Admin Console for the presence of the corresponding MBeans.

Problem	Data is not getting logged
Solution	<ul style="list-style-type: none">• Verify that the SPIDataCollector instrumentation category is deployed on the managed node. This is required to create the datasource WBSSPI_METRICS.• Verify that the WBSSPI-Performance policy is deployed on the node.• Check if the <code><servername>.dat</code> file is created in <code><Agent_Dir>/wasspi/wbs/datalog</code>.• Check if the datasource WBSSPI_METRICS is created.• Verify that graph=yes is specified in the <code><Agent_Dir>/wasspi/wbs/conf/MetricDefinitions.xml</code> for the metrics which are being monitored. Only the metrics which are specified as graph=yes in the <code>MetricDefinitions.xml</code> get logged. The default value is no.

Troubleshooting the Discovery Process

If the discovery process does not automatically discover multiple installations on a Windows managed node, set the HOME property and run the Discover or Configure WBSSPI tool.

If the discovery process does not automatically discover and update the WebSphere SPI configuration:

- 1 Check for errors in the message browser of the managed nodes not being discovered. Follow the instruction text of any error messages displayed.
- 2 Verify that a WebSphere application server is installed on the managed node. If an application server is not installed, install an application server, and complete the configuration tasks listed in [Chapter 3, Configuring the WebSphere SPI](#).
- 3 Verify if the WebSphere application server is running. For information on how to verify the status, see [Verify the Application Server Status](#) on page 38.
- 4 On a UNIX managed node, if the WebSphere application server processes are not running (use `ps -ef` to check for these processes), verify the installation directory of the server.
- 5 Verify that the Discover or Configure WBSSPI tool is not running. Only one process can access the configuration at a time. If Discover or Configure WBSSPI is running, other processes that must access the configuration (like the discovery process) hang until the configuration becomes available.
- 6 Check if the HPOM management server is suppressing duplicate messages:
 - a From the HPOM console, select **Actions** → **Server** → **Configure**. The Configure Management Server window appears.
 - b Look for the **Suppress and count duplicate messages** check box. If this box is checked, uncheck it.
- 7 Check the `<Agent_Dir>/wasspi/wbs/log/discovery.log` file for additional information.
- 8 Restart the HPOM management server:
 - a Stop all HPOM GUIs that are running by selecting **File** → **Exit**.
 - b Stop the HPOM management server processes. Type the following command:
`/opt/OV/bin/ovstop opc ovoacomm`
 - c Delete all HPOM temporary files. All pending messages (messages not saved in the database) and all pending actions (automatic actions, operator-initiated actions, scheduled actions, and command broadcast) are lost. Enter:
`rm -f /var/opt/OV/share/tmp/OpC/mgmt_sv/*`
 - d Restart the HPOM management server process. Type the following command:
`/opt/OV/bin/OpC/opcsv -start`
`/opt/OV/bin/OpC/opcsv -status`
 - e Restart the HPOM GUI. Type: `opc`

Problem	<p>In the SiteConfig file for Windows managed nodes, the value for HOME and JAVA_HOME appears as:</p> <pre>HOME=CProgram FilesIBMWebSphereAppServer JAVA_HOME=CProgram FilesIBMWebSphereAppServerjava</pre> <p>The "\" character is removed from the path.</p>
Solution	<p>Replace the character "\" with "/" or "\\\" in the path for HOME and JAVA_HOME.</p> <p>For example:</p> <pre>HOME=C:/Program Files/IBM/WebSphere/AppServer</pre> <p>Or</p> <pre>HOME=C:\\Program Files\\IBM\\WebSphere\\AppServer</pre>
Problem	<p>Two or more versions of the WebSphere application server are running on a managed node and discovery does not correctly set the properties for the application servers.</p>
Solution	<p>Workaround 1</p> <ol style="list-style-type: none"> 1 Verify the application servers are using non-conflicting ports. If you install an application server in a different home directory, the installer may choose a port used by an existing application server (even if you set the installer to auto-configure non-conflicting ports). 2 If application servers are using the same bootstrap port, modify the port numbers so that each application server uses a unique bootstrap port. 3 Run the Discover tool. <p>Workaround 2</p> <p>If you want to use the same bootstrap port, run the Discover or Configure WBSSPI tool and do the following:</p> <ol style="list-style-type: none"> 1 Set the HOME, JAVA_HOME, VERSION, and other properties that are incorrectly set. 2 Set a unique ALIAS for each application server using the same port. 3 Select Finish.
Problem	<p>The Discovery times out on the node in a network deployer scenario.</p>
Solution	<p>Change the value for timeout for agtrep on the node.</p> <ol style="list-style-type: none"> 1 Run the following command: <code>ovconfchg -edit</code>. 2 Change the value of ACTION_TIMEOUT to a higher value so that Discovery does not timeout. <p>For example: Change ACTION_TIMEOUT=3 to ACTION_TIMEOUT=20 (or more minutes).</p>

Problem	Nightly discovery is not occurring according to the schedule.
Solution	Run the Discover or Configure WBSSPI tool whenever you want to see the new servers or components.

Troubleshooting Graphs

Problem	<p>Netscape fails to refresh graphing data. Specifically, when you use Netscape as the browser to graph your data (graphing capability included with Reporter 3.0 or higher), the browser fails to refresh when new selections are made.</p> <p>For example, in the HPOM console after you drag and drop a managed node onto the WBSSPI Admin tool - View Graphs, Netscape appears and displays a blank WBS SPI graphing page where you can accept or change the following default selections:</p> <p>Server: MyServer_1 Graph Name: Serverstat Data Range: 7 Days (ending now)</p> <p>By clicking Draw, you successfully generate the graph.</p> <p>However, when you select a different server, let's say MyServer_2, you see that the graph that appears after you click the Draw button is the same graph/data as the one you just viewed (for MyServer_1).</p>
Solution	<p>Perform the following steps:</p> <ol style="list-style-type: none">1 In Netscape from the Edit menu select Preferences • Advanced • Cache2 In the segment labeled Document in cache is compared to document on network, select radio button Never.3 After successfully generating the first WBSSPI graph, for any subsequent graphs, always change a minimum of two selections to refresh the data; for example select a different server and a different graph; or select a different graph and a different date range. Any two differing selections work to clear the current graph data from the browser cache. <p>Note: The underlined text <u>Refresh Graph Now</u> at the bottom of the Web page does not work; when clicked, it may return the error: the parameter is incorrect.</p>

Troubleshooting Tools

Problem	Configuration variable SERVER<n>_STOP_CMD missing for server Default Server
Solution	Before you can successfully run the Stop WebSphere tool, you must set the STOP_CMD and USER properties. Set these properties using the Discover or Configure WBSSPI tool. For more information on this tool, see Discover or Configure WBSSPI on page 61.

Problem	Configuration variable <code>SERVER<n>_START_CMD</code> missing for server, Default Server.
Solution	Before you can successfully run the Start WebSphere tool, you must set the <code>START_CMD</code> and <code>USER</code> properties. Set these properties using the Discover or Configure WBSPI tool. For more information on this tool, see Discover or Configure WBSPI on page 61.

Problem	For WebSphere 6.1, Stop WebSphere tool does not stop WebSphere Application Servers.
Cause	Stop WebSphere tool does not work well if security is enabled in WBS and the username or password options are not specified while setting the <code>STOP_CMD</code> property.
Workaround	Edit the <code><connection type>.client.props</code> file on the managed node.

Problem	When launched, the Verify tool gives improper output.
Solution	Before you launch the Verify tool, make sure that you installed the latest version of Self-Healing Service (SHS) component from the SPI DVD. If you upgrade the WebSphere SPI without the SPI DVD, you must upgrade the SHS component also. You can download the SHS component from http://support.openview.hp.com/self_healing_downloads.jsp .

Problem	When launched, the Self-Healing Info tool gives improper output.
Solution	Make sure that you have installed the latest version of Self-Healing Service (SHS) component (version 3.01) from the SPI DVD. If you upgraded the WebSphere SPI without the SPI DVD, you must upgrade the SHS component also. You can download the SHS component from http://support.openview.hp.com/self_healing_downloads.jsp .

Problem	When launching the tools, the applications hang or there is no output.
Solution	The applications will not work if the memory is low. Check the performance of the node and the management server. The physical memory available must be more than 500 MB.

Problem	Check WebSphere tool shows a wrong status for a server instance or does not give any output.
Solution	If a server is up and running but Check WebSphere tool returns the server status as <code>NOT_RUNNING</code> (or does not give any output), turn ON the monitoring for that particular server by using the Start Monitoring tool.

Problem	Datasource not getting created on RHEL 4.0 platform.
Solution	Make sure that you installed the latest version of DSI2DDF component from the SPI DVD. If you upgraded the WebSphere SPI without the SPI DVD, you must upgrade the DSI2DDF component also.
Problem	When the Self-Healing Info tool is run on a Windows managed node, the output file may be hidden.
Solution	If you do not see the file, do the following on the managed node: <ol style="list-style-type: none"> 1 Open Windows Explorer. 2 From the Tools menu, select Folder Options. 3 Click on the View tab. 4 Under Hidden files and folders, select Show hidden files and folders.
Problem	On Linux nodes, the Discover or Configure WBSPI tool can fail without configuring the SPI on the managed Linux node. This happens because some of the configuration processes require uudecode to be present on the local node.
Solution	Ensure that uudecode is installed on the target managed node. It is available in the SHARUTILS package.
Problem	The "Start WebSphere" and "Stop WebSphere" tools fail on Windows nodes if the USER or SERVER<n>_USER configuration property is set. The tool is trying to run the "su" command, which is only available on UNIX.
Solution	Do not set the USER or SERVER<n>_USER property when configuring the SERVER<n>_START_CMD or SERVER<n>_STOP_CMD properties for Windows nodes.
Problem	The "Start WebSphere" and "Stop WebSphere" tools do not work.
Solution	If you have space in the folder name then you should give the entire path of Start/Stop WebSphere command within " ". For example if the path of stopServer is SERVER1_STOP_CMD=C:\ProgramFiles\IBM\WebSphere\AppServer\profiles\Dmgr01\bin\stopServer.bat then stop command in SiteConfig should be SERVER1_STOP_CMD="C:\ProgramFiles\IBM\WebSphere\AppServer\profiles\Dmgr01\bin\stopServer.bat"

Troubleshooting Miscellaneous

Problem	The perl installed with the HPOM agent fails to find the HPOM perl modules if another application (such as Oracle Application Server) sets the PERL5LIB environment variable to point at locations that do not include the HPOM perl lib location.
Solution	<p>Workaround 1</p> <p>Set the PERL5LIB system environment variable:</p> <ol style="list-style-type: none">1 Prepend C:\Program Files\HP OpenView\nonOV\perl\a\lib (the HPOM perl lib path) to the PERL5LIB system environment variable.2 Kill the HPOM agent: <code>opcagt -kill</code>3 Restart the HPOM agent: <code>opcagt -start</code>4 Check the HPOM environment: <code>ovdeploy -cmd set</code>5 If the PERL5LIB variable is not set correctly in the HPOM environment but the system variable is set correctly, reboot the system. <p>Workaround 2</p> <ol style="list-style-type: none">1 Delete the PERL5LIB system environment variable.2 Reboot the system.3 Run the Discover tool. <p>Workaround 3</p> <p>Run discovery on the target node. Enter the following:</p> <pre>1 cd /var/opt/OV/bin/instrumentation 2 wasspi_perl -S wasspi_wbs_discovery.pl</pre> <p>Note : The service map is not generated when the discover script is run locally (is not run from the HPOM management server).</p>
Problem	The <code>wbs.log</code> file grows very large.
Solution	<p>Limit the size of the data saved to the log file each time the logfile encapsulator is run. In the SPIConfig file (located in <code>/var/opt/OV/wasspi/wbs/conf/</code> or <code>/var/opt/OV/conf/wbs/</code> on UNIX platforms and <code>/usr/OV/wasspi/wbs/conf/</code> on Windows platforms), add the following:</p> <pre># maximum number of lines to save to the log file / run LOG_LINE_LIMIT=16667 # maximum number of characters to save from each log file / run LOG_SIZE_PER_FILE_LIMIT=600000</pre>

Problem	For a managed node running Red Hat Linux 4, discovery and/or metric threshold monitor alarming is not functioning AND the following error message is found in the SPI error log: *** glibc detected *** double free or corruption: 0x0937d008 ***
Solution	On the HPOM agent, set the MALLOC_CHECK_ environment variable to 0 (zero) and restart the agent.
Problem	The Web browser cannot be launched from an operator action after you have correctly configured the WBSSPI as instructed in the “ <i>Configure the Management Server to Launch your Web Browser</i> ” task in Chapter 2 of the <i>HP Operations Smart Plug-in for WebSphere Application Server Installation and Configuration Guide</i> .
Solution	Perform these steps: <ol style="list-style-type: none"> 1 Stop and restart the agent from a user other than root by entering the following commands on the managed node: <pre>opcagt -kill</pre> <pre>opcagt -start</pre> 2 Run the operator action.
Problem	In a non-English environment, the message browser does not display error messages correctly.
Solution	Change the character set of the WBSSPI Error Log template and redeploy the template. For example, change the character set from “Shift-JIS” to “Japanese EUC.”

Overview of Error Messages

The WebSphere SPI error messages contain the following information:

- Error Message Number
- Description
- Severity
- Help Text (Probable Cause and Suggested Action)

Error messages can be viewed from the HPOM Message Browser. Double-click the error message to open the message. The Message Properties window appears. Click the **Message Text** tab to view the error message.

For more information on error messages, see [Appendix C, Error Messages](#).

8 Removing the WebSphere SPI

This chapter provides details on how to remove the WebSphere SPI components from different environments.

Removing the SPI components

To completely remove the SPI, remove the SPI components by following the tasks:

- 1 Remove the WebSphere SPI Software from the Management Server
- 2 Delete the WebSphere SPI Message groups
- 3 Delete the WebSphere SPI User Profiles
- 4 Remove the Report Package (Optional)
- 5 Remove the Graph Package (Optional)

Remove the WebSphere SPI Software from the Management Server

You can remove the WebSphere SPI Software from the HP UX , Solaris and Linux management server as follows:

To remove the WebSphere SPI Software from the HP-UX Management server:

- 1 Open a terminal window and log on as root.
- 2 In the terminal window, enter the following:

```
/usr/sbin/swremove WBSPI
```

The **swremove** command removes the files from the software list, directories in `/var/opt/OV/share/databases/OpC/mgd_node/instrumentation/`, directories in `/opt/OV/wasspi/wbs`, node groups, categories, tools, and policies.

To remove the WebSphere SPI through the Graphical User Interface from the Linux or Solaris Management Server, using X-Windows client software:

- 1 Log on as a **root** user.
- 2 Insert the HP Operations Smart Plug-ins DVD into the DVD drive of the Linux or Solaris management server. Mount the DVD if necessary.
- 3 Start the X-windows client software and export the `DISPLAY` variable by typing the following command:

```
export DISPLAY=<ip address>:0.0
```

- 4 To start the removal of the SPI, type one of the following commands, according to your management server:

```
./HP_Operations_Smart_Plug-ins_Linux_setup.bin
```

or

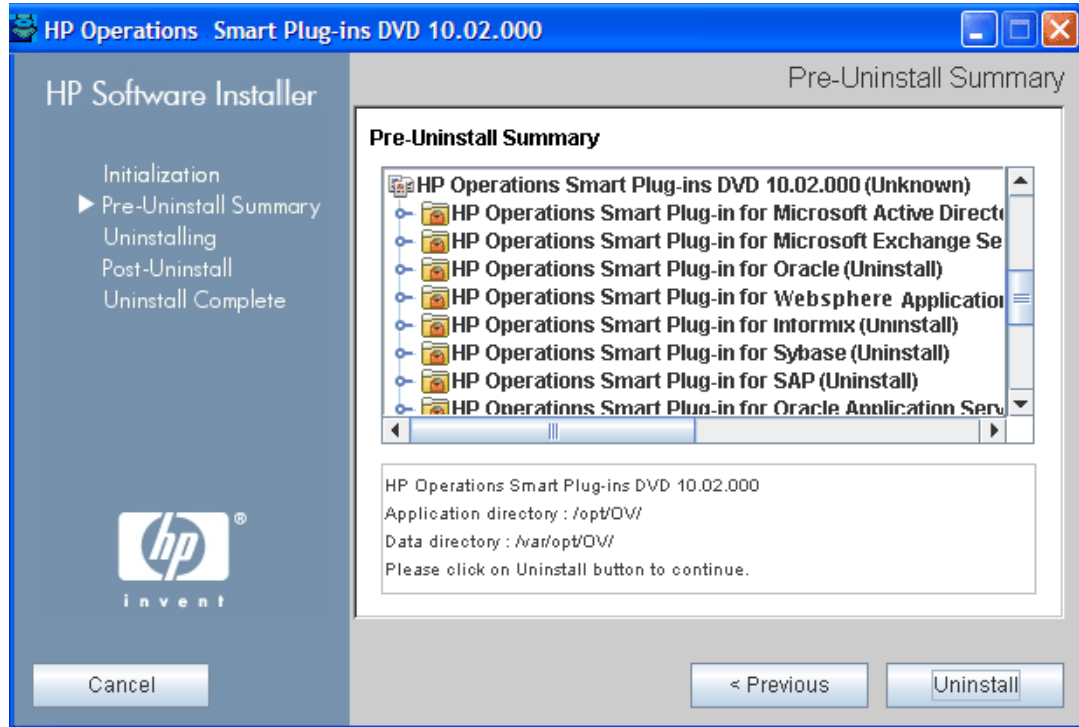
```
./HP_Operations_Smart_Plug-ins_Solaris_setup.bin
```

The introductory window appears.

- 5 Select the language from the drop-down list and click **OK**.

The Application Maintenance window appears.

- 6 Select **Uninstall** button and click **Next**. The Pre-Uninstall Summary window appears.



- ▶ When you have two SPIs installed on the Linux or Solaris management server and you want to remove one SPI out of the two installed SPIs, select **Modify** option and then the SPI you want to retain. Do not select the SPI which you want to remove.

- 7 Click **Uninstall**. The Uninstalling window appears. The Uninstall Complete window appears once the SPI is uninstalled.

- 8 Click **Done** to complete the removal of the SPI.

To remove the WebSphere SPI through the Command Line Interface:

- 1 Login as a **root** user.
- 2 Insert the HP Operations Smart Plug-ins DVD into the DVD drive of the Linux or Solaris management server. Mount the DVD if necessary.
- 3 To start the removal of the SPI, type one of the following commands, according to your management server:

```
./HP_Operations_Smart_Plug-ins_Linux_setup.bin -i console
```


or

```
./HP_Operations_Smart_Plug-ins_Solaris_setup.bin -i console
```


- 4 When the prompt, 'Choose Locale...' appears, press the number corresponding to the language you want to choose.

- 5 Press **Enter** to continue. The Maintenance Selection screen appears.
- 6 Press the appropriate option (number) to start the removal of the SPI.
 - ▶ When you have two SPIs installed on the Linux or Solaris management server and you want to remove one SPI out of the two installed SPIs, select Modify (1) option and then the SPI you want to retain. Do not select the SPI which you want to remove.
- 7 Press **Enter** to continue. When the removal is complete, you will receive a message which states that the removal is completed successfully.

Delete the WebSphere SPI Message groups

- 1 From the Admin interface, open the All Message Groups window.
- 2 Select the check boxes next to the WebSphere and WBSSPI message groups.
- 3 Select **Delete...** from the **Choose an Action** drop-down list and click  to submit.
The WebSphere SPI message groups are deleted.

Delete the WebSphere SPI User Profiles

- 1 From the Admin interface, open the All User Profiles window.
- 2 Select the User Profiles for WebSphere SPI check box.
- 3 Select **Delete...** from the **Choose an Action** drop-down list and click  to submit.
The WebSphere SPI user profiles are deleted.

Remove the Report Package (Optional)

If you installed the WebSphere SPI report package on your Windows system running HP Reporter, remove it. Follow these steps:

- 1 On the Windows system running HP Reporter, from the Control Panel, double-click the **Add/Remove Programs** icon.
- 2 Select the WebSphere SPI report package and click **Remove**.

Remove the Graph Package (Optional)

If you installed the WebSphere SPI graph packages on the HPOM management server and on your system running HP Performance Manager, remove them.

- On the HPOM management server, run the following command:
`/usr/sbin/swremove WBSSPI-GRAPHS`
- On a Windows system running HP Performance Manager:
 - a From the Control Panel, double-click the **Add/Remove Programs** icon.
 - b Select the WebSphere SPI graph package (HP Operations SPI for WebSphere Application Server - Graphing Component Integration) and click **Remove**.

- On an HP-UX system running HP Performance Manager that is not the HPOM management server, follow these steps (if HP Performance Manager is installed on the HPOM management server, the files are removed in [Remove the WebSphere SPI Software from the Management Server](#) on page 113):
 - a Verify that the graph package is installed. Type `swlist | grep WBSSPI-GRAPHS`
 - b Type `swremove WBSSPI-GRAPHS`
- On a Solaris system running HP Performance Manager that is not the HPOM management server, follow these steps (if HP Performance Manager is installed on the HPOM management server, the files are removed in [Remove the WebSphere SPI Software from the Management Server](#) on page 113):
 - a Verify that the graph package is installed. Type `/usr/bin/pkginfo HPOvSpiWbsG`
 - b Type `/usr/sbin/pkgrm HPOvSpiWbsG`

Removing the WebSphere SPI in a Cluster Environment

To remove the WebSphere SPI from each system in the cluster, follow the steps in [Removing the SPI components](#) on page 113.

A File Locations

This appendix contains information on the location of the WebSphere SPI configuration files and error logs in specific directories.

HPOM Management Server File Locations

Operating System	File	File Location
HP-UX	Configuration	/opt/OV/wasspi/wbs/conf
Solaris	Configuration	/opt/OV/wasspi/wbs/conf
Linux	Configuration	/opt/OV/wasspi/wbs/conf

Managed Node File Locations

These file locations are valid if you are migrating the UNIX or Windows node, on which WebSphere SPI is running, to a non-root HTTPS agent environment (UNIX only; if these directories do not exist, see the table under [Non-Root HTTPS Agent Environment](#) on page 118 for UNIX-related file locations):

Operating System	File	File Location
HP-UX, Solaris	Configuration	/var/opt/OV/wasspi/wbs/conf
HP-UX, Solaris	Error Logs	/var/opt/OV/wasspi/wbs/log
Linux	Configuration	/var/opt/OV/wasspi/wbs/conf
Linux	Error Logs	/var/opt/OV/wasspi/wbs/log
AIX	Configuration	/var/opt/OV/wasspi/wbs/conf
AIX	Error Logs	/var/opt/OV/wasspi/wbs/log
Windows (HTTPS)	Configuration	\Documents and Settings\All Users\Application Data\HP\HP BTO Software\wasspi\wbs\conf
Windows (HTTPS)	Error Logs	\Documents and Settings\All Users\Application Data\HP\HP BTO Software\wasspi\wbs\log

Non-Root HTTPS Agent Environment

On newly configured WebSphere SPI managed nodes in the non-root HTTPS agent environment (UNIX only):

Operating System	File	File Location
HP-UX, Solaris	Configuration	/var/opt/OV/conf/wbsspi
HP-UX, Solaris	Error Logs	/var/opt/OV/log/wbsspi
AIX	Configuration	/var/opt/OV/conf/wbsspi
AIX	Error Logs	/var/opt/OV/log/wbsspi

B Configuration

This appendix contains information on the configuration structure, usage of the configuration editor, description of the configuration properties, and sample configurations.

Structure

For examples of the configuration, see [Sample Configurations](#) on page 136. The basic structure of the configuration is (lines preceded by # are treated as comments and so are ignored):

```
# Global Properties
<property>=<value> ...

# GROUP Block
GROUP <group_name>
{
  <node_name> ...
}

# NODE Block
NODE <node_name | group_name>
{
  <property>=<value> ...
}
```

Global Properties

```
# Global Properties
<property>=<value> ...
```

Properties defined at the global level apply to all nodes. However, these global properties can be overridden by properties set within a GROUP or NODE block or by server-specific properties.

GROUP Block

```
# GROUP Block
GROUP <group_name>
{
  <node_name> ...
}
```

GROUP blocks are used to group nodes together that have common properties.

<group_name> identifies the group of nodes with common properties. If a GROUP block <group_name> is repeated within the configuration, the last definition takes precedence.

<node_name> lists the nodes in the group and is the primary node name configured in HPOM.



The node name specified in a GROUP block matches the value returned by the HPOM variable \$OPC_NODES, which is the primary node name configured in HPOM.

Set the common properties of the group using the NODE block.

Using the configuration editor, view, set, or edit GROUP block properties by selecting the Default Properties item in the <Group_Name> folder.

NODE Block

```
# NODE Block
NODE <node_name | group_name>
{
  <property>=<value> ...
}
```

Properties set in a NODE block apply to nodes belonging to the group defined by <group_name> (to set common properties for a group) or to the specified <node_name> (to set properties for a single node).

For a group, type the <group_name> defined by the GROUP block and define the group's common properties.

For a single node, type the <node_name> and define the properties.

If a property definition is repeated within the NODE block, the last definition takes precedence.

Using the configuration editor, view, set, or edit NODE block properties by selecting the Default Properties item in the <Node_Name> folder.

Server-Specific Properties

Each property specified as *SERVER<n>_property* refers to a specific WebSphere Application Server instance. When more than one WebSphere Application Server instance is running on a given managed node, the number <n> differentiates the servers. Numbering begins at “1” and each WebSphere Application Server instance is assigned a unique number.

Property Precedence

The order of precedence (highest to lowest) of properties defined in the configuration are:

- 1 SERVER<n>_property (server-specific)
- 2 NODE <node_name> {<property>} (property defined for a node)
- 3 GROUP<group_name> {<property>} (property defined for a group)
- 4 <property> (global property)

Configuration Editor

Use the configuration editor to view and edit the configuration. You must update the configuration using this editor only. The main components of the configuration editor are:

- Tree
- Buttons
- Actions

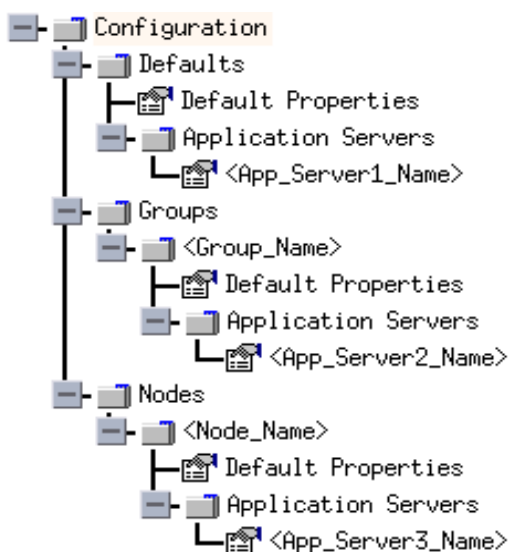
Configuration Editor - Tree

The Configuration Editor tree that appears in the left pane of the Configuration Editor's main window shows the WebSphere SPI configuration in a tree structure.

The following is an example of the tree.



If no application servers or groups are configured, the “Application Servers” and “Groups” folders are not displayed. If you are running the Discover or Configure WBSSPI tool for the first time and you did not select any nodes before you launched the tool, the “Nodes” folder is listed.



The icons are defined as follows:



The configuration properties can be viewed.



The configuration properties can be viewed and set.

The following table lists each item in the tree:

Item Name	Description
Application Servers	A folder that contains a list of all the application servers. This folder can appear under Defaults (global properties), Group_Names (GROUP block), or Node_Names (NODE block).
<Application_Server_Name>	The server name as defined in WebSphere.
Configuration	A folder that contains all the WebSphere SPI configuration information for the WebSphere environment.
Default Properties	Lists the configuration properties that were set. This item appears under Defaults (global properties), Group_Names (GROUP block), or Node_Names (NODE block).
Defaults	A folder that represents the global properties. Default properties set at this level apply to all nodes. However, these properties can be overridden by properties set under the GroupName and Node_Name folders (see Property Precedence on page 120).
Groups	A folder that represents the GROUP block.
<Group_Name>	A folder that identifies the name of a group of nodes with common properties. Default properties set at this level apply to all nodes that belong to the specified group. These properties can be overridden by properties set under the Node_Name folders (see Property Precedence on page 120).
Nodes	A folder that represents the NODE block.
<Node_Name>	A folder that represents a single node whose name matches the value returned by the HPOM variable <\$OPC_NODES>, which is the primary node name configured in HPOM. Default properties set at this level apply to the specified node only (see Property Precedence on page 120).









Configuration Editor - Buttons

The following buttons are available in Discover or Configure WBSSPI-Configuration Editor window:

Button	Description
Cancel	Exit Discover or Configure WBSSPI. If you set configuration properties without saving them, the changes are not saved. If you add or remove an application server, node, or group without saving the change or if you modify a configuration property, a Confirm Cancel window appears. Click Save and Exit to save the changes before exiting, Exit without Save to exit without saving the changes, or Return to Editing to continue editing the configuration (changes are not saved).
Finish	Exit Discover or Configure WBSSPI. Appears instead of the Next button if you launched Discover or Configure WBSSPI without selecting any nodes.
Next	Exit Discover or Configure WBSSPI. Takes you to the “Confirm Operation” window that lists the selected nodes before you started Discover or Configure WBSSPI. The selected managed nodes’ configuration is updated with changes. If you make changes to nodes that were not selected (are not displayed in the “Confirm Operation” window), the changes are saved to the HPOM management server’s configuration, but to make the changes to those managed node’s configuration, you must select those managed nodes from the node bank, restart Discover or Configure WBSSPI, and then exit.
Save	Save changes to the HPOM management server’s configuration and continue editing the configuration. You can also select File → Save to save your changes.

Configuration Editor - Actions

Actions that you can perform depend upon the item that is selected in the tree and from where you access the action. The following actions can be accessed from the Actions menu, File menu, or by right-clicking on an item in the tree.

Action	Description	Selected Tree Item
Add Application Server	Add an application server. See Add Application Server on page 124.	<ul style="list-style-type: none">  Application Servers  Defaults  <Group_Name>  <Node_Name>
Add Group	Create a group to assign nodes that have common properties. See Add Group on page 126.	<ul style="list-style-type: none">  Any item in the tree  Any item in the tree
Add Node	Add a managed node to the Nodes folder. See Add Node on page 126.	<ul style="list-style-type: none">  Any item in the tree  Any item in the tree

Action	Description	Selected Tree Item
Exit	Exit the Discover or Configure WBSPI tool. This action is available from the File menu. If any changes were made that were not saved, the Confirm Cancel window appears.	<ul style="list-style-type: none"> Any item in the tree Any item in the tree
Remove Application Server/Remove ALL App Servers	Remove an application server or all listed application servers. See Remove Application Server/Remove ALL App Servers on page 126.	<ul style="list-style-type: none"> Application Servers <Application_Server_Name>
Remove Group/Remove ALL Groups	Remove a WebSphere SPI group or all listed WebSphere SPI groups. See Remove Group/Remove ALL Groups on page 127.	<ul style="list-style-type: none"> Groups <Group_Name>
Remove Node/Remove ALL Nodes	Remove a managed node or remove all managed nodes. See Remove Node/Remove ALL Nodes on page 127.	<ul style="list-style-type: none"> Nodes <Node_Name>
Save	Save changes to the configuration. This action is available from the File menu only if changes were made to the configuration.	<ul style="list-style-type: none"> Any item in the tree Any item in the tree
Set Configuration Properties tab	Set the WebSphere SPI configuration properties. See Set Configuration Settings Tab on page 128.	<ul style="list-style-type: none"> <Application_Server_Name> Default Properties
View Configuration Settings tab	View the WebSphere SPI configuration properties. See View Current Configuration Tab on page 129.	<ul style="list-style-type: none"> Any item in the tree Any item in the tree

Add Application Server

Add an application server at the global properties, GROUP, or NODE level in the WebSphere SPI configuration.

If a node contains duplicate server names (the NAME property is set to the same value), you are prompted to set the ALIAS property (to uniquely identify each server). For more information about the ALIAS property, see [Property Definitions](#) on page 132.

Before adding an application server,

For WebSphere Server version 6 and above	Set the PORT property to the application server's port number at the application server level of configuration. For more information about setting the PORT property, see Set Configuration Settings Tab on page 128 and Configuration Properties on page 130.
--	--

To add an application server:

- 1 Right-click one of the following items in the tree: Defaults (global properties level), Application Servers (global properties level), *<Group_Name>* (GROUP level), or *<Node_Name>* (NODE level) and select **Add Application Server**. The Configure WBSSPI tool: Add App Server window appears.

- 2 Type the Application Server Name. This is the name of the application server as defined in WebSphere and is case-sensitive.

- 3 Type the Server Port.

If the Use Inherited Server Port check box is selected, you must not enter a port number in the Server Port field.

- 4 If available, select the Use Inherited Server Port: *xxx* check box if you want to use the specified port number ("*xxx*").

If the PORT property is not set, the check box is not available.

If you do *not* want to use the specified port number, clear the check box and enter a port number in the Server Port field.

If you select the check box, you must not enter a port number in the Server Port field.

The specified port number is determined by the value set for the PORT property at the global properties, GROUP, or NODE level:

- If the PORT property is set at the global properties level, the WebSphere SPI is configured to use this same port number on all nodes and groups for all WebSphere application servers. If there is more than one application server per node, only one server can use the inherited server port. Edit the PORT property for the other application servers.
- If the PORT property is set at the GROUP level, the WebSphere SPI is configured to use this same port number for the group for all WebSphere application servers. If there is more than one application server per node in the group, only one server can use the inherited server port. Edit the PORT property for the other application servers.

The port number set at the GROUP level takes precedence over the port number set at the global properties level.

- If the PORT property is set at the NODE level, the WebSphere SPI is configured to use this same port number for that node for all WebSphere application servers. If there is more than one application server per node, only one server can use the inherited server port. Edit the PORT property for the other application servers.

The port number set at the NODE level takes precedence over the port number set at the global properties level.

- 5 Click **OK**.

The NAME and PORT properties are set.

The application server is added and its properties are displayed. You can also set additional configuration properties for this server. For more information, see [Set Configuration Settings Tab](#) on page 128.

- 6 Click **Save** to save your changes.

If you do not want to add this application server, right-click the application server name, select **Remove Application Server**, and click **Save**.

Add Group

Assign nodes to a group that have common properties in the WebSphere SPI configuration.

To add a group:

- 1 Right-click any item in the tree and select **Add Group**. The Configure WBSSPI tool: Add Group window appears.
- 2 Type the Group Name. The group name identifies the group of nodes with common properties and is *not* case-sensitive.
- 3 Click **OK**. The group is added and the Set Configuration Properties tab for the group appears.
- 4 Select **Add Node to Group**, select one node from the list to add to the group, and click **OK**. Repeat this step until all nodes are added to the group.
- 5 Set the configuration properties for this group using the **Select a Property to Set** drop-down list. For more information, see [Set Configuration Settings Tab](#) on page 128.
- 6 Click **Save** to save your changes.

If you do not want to add the group, right-click the group name, select **Remove Group**, and click **Save**.

Add Node

Add a managed node to the WebSphere SPI configuration.

To add a node:

- 1 Right-click any item in the tree and select **Add Node**.
If no additional managed nodes are available to add to the configuration, the following message appears:
All available managed nodes have been added to the configuration.
Click **OK** to exit this action.
- 2 From the drop-down list, select a node to add.
- 3 Click **OK**. The node is added and the Set Configuration Properties tab for the node appears.
- 4 Set the configuration properties for this node using the **Select a Property to Set** pull-down list. For more information, see [Set Configuration Settings Tab](#) on page 128.
- 5 Click **Save** to save your changes.

If you do not want to add the node, right-click the node name, select **Remove Node**, and click **Save**.

Remove Application Server/Remove ALL App Servers

Remove a WebSphere Server or all listed WebSphere Servers from the WebSphere SPI configuration.

To remove an application server:

- 1 Right-click the application server name and select **Remove Application Server**.
The selected application server name is removed from the list and its configuration properties are removed from the configuration.

- 2 Click **Save** to permanently remove the application server.

Click **Cancel** to cancel the removal of the application server (the application server name appears the next time you run Discover or Configure WBSSPI). On the “Confirm Cancel” window, click **Exit without Save**.

To remove ALL application servers:

- 1 Right-click the Application Servers folder and select **Remove ALL App Servers**.

The selected Application Servers folder and all application servers listed in the selected folder are removed (all configuration properties for the listed application servers are removed from the configuration).

- 2 Click **Save** to permanently remove the application servers.

Click **Cancel** to cancel the removal of all application servers (the Application Servers folder and all application server names listed in the folder appear the next time you run Discover or Configure WBSSPI). On the “Confirm Cancel” window, click **Exit without Save**.

Remove Group/Remove ALL Groups

Remove a WebSphere SPI group or all listed WebSphere SPI groups from the WebSphere SPI configuration.

To remove a group:

- 1 Right-click the group server name and select **Remove Group**.

The selected group is removed from the list and its configuration properties are removed from the configuration.

- 2 Click **Save** to permanently remove the group.

Click **Cancel** to cancel the removal of the group (the group name appears the next time you run Discover or Configure WBSSPI). On the “Confirm Cancel” window, click **Exit without Save**.

Remove Node/Remove ALL Nodes

Remove a managed node or all listed managed nodes from the WebSphere SPI configuration.

To remove a node:

- 1 Right-click the node name and select **Remove Node**.

The selected node is removed from the list and its configuration properties are removed from the configuration.

- 2 Click **Save** to permanently remove the node.

Click **Cancel** to cancel the removal of the node (the node name appears the next time you run Discover or Configure WBSSPI). On the “Confirm Cancel” window, click **Exit without Save**.

To remove ALL nodes:

- 1 Right-click the Nodes folder and select **Remove ALL Nodes**.


The selected Nodes folder and all nodes listed in the selected folder are removed (all configuration properties for the listed nodes are removed from the configuration).

- 2 Click **Save** to permanently remove the nodes.

Click **Cancel** to cancel the removal of all nodes (the Nodes folder and all node names listed in the folder appear the next time you run Discover or Configure WBSSPI). On the “Confirm Cancel” window, click **Exit without Save**.

Set Configuration Settings Tab

Set the WebSphere SPI configuration properties at the global properties level or for the selected application servers, groups (GROUP level), or nodes (NODE level).

Items with the  icon are the only items for which you can set configuration properties (Default Properties and `<Application_Server_Name>`).

To set the configuration properties of an item, select the item and click the **Set Configuration Properties** tab in the right pane.

Setting a Property

To set a property in the configuration:

- 1 Select a property from the **Select a Property to Set** drop-down list.
- 2 Select **Set Property**. The property and an empty value field appear in the table.
- 3 Click the empty value field and type a value.
- 4 Repeat steps 1 through 3 for each property to set.
- 5 Click **Save**.



For the LOGIN and PASSWORD properties, when you select **Set Property**, a separate window appears. Type the login and password values in this window.

For more information about individual properties, see [Configuration Properties](#) on page 130.

Modifying a Property

To modify a property (except LOGIN) in the configuration:

- 1 Select the property from the table.
- 2 Double-click the value field.
- 3 Edit the value.

If a node contains duplicate server names (the NAME property is set to the same value), you are prompted to set the ALIAS property (to uniquely identify each server). For more information, see [Property Definitions](#) on page 132.

- 4 Repeat steps 1 through 3 for each property to modify.
- 5 Click **Save**.

To modify the LOGIN property in the configuration:

- 1 Select **LOGIN/PASSWORD** from the **Select a Property to add** drop-down list.
- 2 Select **Set Property**. The Set Access Info for Default Properties window appears.
- 3 Type the new password and verify it.
- 4 Click **OK**.
- 5 Click **Save**.

Removing a Property

To remove a property from the configuration:

- 1 Select the property from the table.
- 2 Click **Remove Property**.
- 3 Repeat steps 1 and 2 for each property to remove.
- 4 Click **Save**.

View Current Configuration Tab

The options under this tab enable you to view all WebSphere SPI configuration properties set in the configuration on the HPOM management server or the WebSphere SPI configuration properties for the selected application servers, groups, or nodes.

To view the configuration properties of an item, select the item and click the **View Current Configuration** tab in the right pane.

The following table describes the view when the specified item is selected.

Item Name	Description of View
Application Servers	View all configuration properties set for all the listed application servers.
<Application_Server_Name>	View all configuration properties set for the application server (these properties can be modified by selecting the Set Configuration Properties tab).
Configurations	View all configuration properties saved in the configuration on the HPOM management server.
Default Properties	View all configuration properties that are set (these properties can be modified by selecting the Set Configuration Properties tab).
Defaults	View all configuration properties set at the global properties level.
Groups	View all configuration properties set for all the listed groups.
<Group_Name>	View all configuration properties set for the specific group.
Nodes	View all configuration properties set for the listed nodes.
<Node_Name>	View all configuration properties set for the specific node.

View Inherited Properties

A **View Inherited Properties** check box appears near the bottom of the window. By selecting this check box, the view of the configuration properties changes to show all inherited properties (those properties defined at a global properties level or GROUP level) that affect the selected item. Inherited properties are denoted by “<*>” appearing after the property.

By clearing this check box, the view shows only the configuration properties set at that level for the selected item.

You can modify the inherited properties at the level they are set. If “<*>” appears after the property, the property cannot be modified at that level. For example, if the property HOME is set at the global properties level (under the Defaults folder), it can only be modified in the Default Properties listed under the Defaults folder. Although HOME appears (with “<*>” after it) in a <Group_Name>’s Default Properties view, you cannot modify it at this level.

Properties set lower in the tree take precedence over those properties set higher in the tree. For example, if the property HOME is set at the global properties level (under the Defaults folder) and the property HOME is set at the GROUP level, the GROUP level property value takes precedence.

Configuration property precedence is as follows (listed from highest to lowest):

- 1 Server-specific
- 2 NODE level
- 3 GROUP level
- 4 Global properties level

Configuration Properties

Table 6 on page 131 lists all properties by WebSphere SPI requirements, where:

Property	Name of the property.
Requirements	Lists the property requirements for specific components where: <ul style="list-style-type: none"> R - Required: the property must be set. C - Conditional: the property might need to be set if certain conditions are met. O - Optional: the property is not required for the component to work. blank - Not Applicable: the property does not affect this component.
WebSphere SPI	Configuration requirements for the WebSphere SPI to work.
Discovery Process	Requirements for the discovery process to work.
Auto-Discovered	The property is automatically set by the discovery process.
Level of Configuration	The level at which this property can be set within the configuration structure.
Default Properties	The global, group, or node level within the configuration structure.
Application Server	The server-specific level within the configuration structure.

Table 6 Properties Listed by the WebSphere SPI Requirements

Property	Requirements		Auto-Discovered	Level of Configuration	
	WebSphere SPI	Discovery Process		Default Properties	Application Server
HOME	R	R	✓	✓	✓
JAVA_HOME	R	R	✓	✓	✓
NAME	R		✓		✓
PORT	R	C	✓	✓	✓
ADDRESS	C	O			✓
ALIAS	C				✓
COLLECT_METADATA	C	O		✓	✓
GRAPH_URL	C			✓	
JMB_JAVA_HOME	C			✓	✓
JMX_CLASSPATH	C			✓	✓
LOGFILE	C				✓
LOGIN	R	R		✓	✓
PASSWORD	R	R		✓	✓
PROFILE_HOME	C		✓	✓	✓
RMID_PORT	C			✓	
RMID_START_TIME	C			✓	
START_CMD	C				✓
STOP_CMD	C				✓
TYPE	C			✓	✓
USER	C			✓	✓
VERSION	C				✓
TIMEOUT	O			✓	✓
UDM_DEFINITIONS_SOURCE	O			✓	✓

Property Definitions

Property	WebSphere SPI Requirements	Description
ADDRESS	Conditional Required if the server is running on a virtual IP address or on a remote node	The domain name or IP address where the server is listening. If not specified, the server is listening on the primary IP of the node on which the server is running. Example: SERVER1_ADDRESS = product.hp.com
ALIAS	Conditional Required if more than one application server on a system share the same server name	Unique name on a managed node assigned to an application server if more than one application server on a system share the same server name. The alias, if set, is the name used in messages, reports, and graphs (otherwise, SERVER<n>_NAME is used). If SERVER<n>_ALIAS is modified, the data for the old alias is saved but is not mapped to the new alias. Example: <pre> NODE petstore.hp.com { SERVER1_NAME=dog SERVER1_ALIAS=beagle SERVER2_NAME=dog SERVER2_ALIAS=dachshund } NODE flying_ace.hp.com { SERVER1_NAME=snoopy SERVER1_ALIAS=beagle SERVER2_NAME=snoopy SERVER2_ALIAS=red_baron } </pre>
COLLECT_METADATA	Conditional Required if you want to use the MBean Explorer in the JMX Metric Builder tool.	Default: OFF. Enter "ON" to collect metadata (MBean information) displayed by the JMX Metric Builder tool. The metadata is used to create UDMs (user defined metrics). Metadata for each MBean server is temporarily saved to the following file: /var/opt/OV/wasspi/wbs/metadata/<managed_node>/<NAME ALIAS>.xml or /var/opt/OV/metadata/wbs/<managed_node>/<NAME ALIAS>.xml (UNIX) or <Agent_Dir>\wasspi\wbs\metadata\<managed_node>\<NAME ALIAS>.xml (Windows) where NAME and ALIAS are the properties set for the managed node and ALIAS is always used if it is set.
GRAPH_URL	Conditional Required if you want to view graphs with HP Performance Manager	The fully-qualified URL used to launch HP Performance Manager. Set at the global level only. Example: GRAPH_URL=http://<server_name>:<port_no>/OVPM default port number is 8081(HP Performance Manager 8.10 on UNIX and Windows)

Property	WebSphere SPI Requirements	Description
HOME	Required	The directory where the WebSphere Server is installed. Example: HOME = /usr/IBM/WebSphere/AppServer or HOME = C:/Program Files/IBM/WebSphere/AppServer
JAVA_HOME	Required	The directory where Java is installed. The java engine is expected to be \$JAVA_HOME/bin/java. Example: \$JAVA_HOME = /opt/WebSphere/AppServer/java/
JMB_JAVA_HOME	Conditional Required if you are using the JMX Metric Builder	The directory where Java (JDK 1.5 or higher) is installed that is used by the JMX Metric Builder on the HPOM management server. The JDK must be version 1.5 or higher.
LOGFILE	Conditional Required only if there are WebSphere logfiles to be monitored that are not the default ones	A comma-separated list of fully qualified filenames of WebSphere Server logfiles. Example: SERVER1_LOGFILE = /opt/WebSphere/myserver/websphere.log SERVER2_LOGFILE = C:\WebSphere\myserver\websphere.log
LOGIN	Required	A WebSphere-defined user (not a system user) that is used to monitor a WebSphere Server. Example: SERVER1_LOGIN = janedoe
NAME ^a	Required	The server name as defined in WebSphere. Use the WebSphere administrative console to obtain this information. Example: SERVER1_NAME = exampleServer
NUM_SERVERS	Optional	The number of WebSphere Servers on the managed node. Example: NUM_SERVERS = 3
PASSWORD	Required	The password for the WebSphere-defined user (USER or SERVER<n>_USER). Example: SERVER1_PASSWORD = janedoe123
PORT ^b	Required	Default: The port number of the application server. The bootstrap port number for the WebSphere application server. Verify that this is the same as the port number listed in the administrative console. Example: SERVER1_PORT = 2809
PROFILE_HOME	Conditional Required for WebSphere Server version 6.0 and later when WebSphere Profiles are created outside the HOME directory	Examples: PROFILE_HOME = /opt/IBM/WebSphere/Profiles PROFILE_HOME = C:\IBM\WebSphere\Profiles

Property	WebSphere SPI Requirements	Description
RMID_START_TIME	<p>Conditional</p> <p>Required if rmid takes longer than 30 seconds to start</p>	<p>Default: 30 (seconds)</p> <p>The amount of time, in seconds, to wait for rmid to start before timing out.</p> <p>Example: RMID_START_TIME=60</p>
START_CMD	<p>Conditional</p> <p>Required if you want to start the WebSphere application server from the HPOM console</p>	<p>A system command that is run when the HPOM Tool Bank Start WebSphere tool is used. This command is run by SERVER<n>_USER which must be configured in order for the Start WebSphere tool to work.</p> <p>NOTE: This command must exit; that is, the WebSphere process must run in the background or as a service, and it must be protected from its parent process dying.</p> <p>Example: SERVER1_START_CMD = /sbin/init.d/WebSphere start</p>
STOP_CMD	<p>Conditional</p> <p>Required if you want to stop the WebSphere application server from the HPOM console</p>	<p>A system command that is run when the HPOM Tool Bank Stop WebSphere tool is used. This command is run by SERVER<n>_USER which must be configured in order for the Stop WebSphere tool to work.</p> <p>Example: SERVER1_STOP_CMD = /sbin/init.d/WebSphere stop</p>
TIMEOUT	<p>Optional</p>	<p>Default: 120 (seconds). The maximum amount of time, in seconds, the WebSphere SPI tries to connect to WebSphere. When the specified time is exceeded, the WebSphere SPI sends an alarm to the message browser indicating that WebSphere is unavailable. If metric I002_ServerStatusRep is being collected, the unavailability of the server is logged.</p> <p>If no time limit is desired, set this property to -1.</p> <p>Example: SERVER1_TIMEOUT=30</p>

Property	WebSphere SPI Requirements	Description
UDM_DEFINITIONS_SOURCE	Optional	Default: nopt/OV/wasspi/wbs/conf/wasspi_wbs_udmDefinitions.xml. The fully qualified path name to or file name of the metric definitions XML file on the HPOM management server. If a path name is set, the wasspi_wbs_udmDefinitions.xml file is the assumed file name of the UDM file. Example: SERVER1_UDM_DEFINITIONS_SOURCE = /opt/OV/wasspi/wbs/conf/udm.xml
USER	Conditional Required if you want to start and/or stop the WebSphere tool server from the HPOM console	The system username for starting and stopping the WebSphere Server from the HPOM Application Bank. The default is the username under which the HP Operations agent runs. Example: SERVER1_USER = websphere
VERSION	Conditional Required if you are configuring remote monitoring	Default: 6.0 0. The version number of the WebSphere Server in the format Major# <space> [Minor#] where: <ul style="list-style-type: none"> Major# - The primary version number (for example, if the version is 6.0.1 the Major# is 6.0) Minor# - The secondary version number (for example, if the version is 6.0.1 the Minor# is 1). If Minor# is not specified, the default value is 0. Example: SERVER1_VERSION = 6.0 1

- For WebSphere Server version 6 and later, the WebSphere administrative console displays the server names of all configured applications servers. Use these names when defining NAME.
- For WebSphere Server version 6 and later, the default value configured for PORT is the port number for the application server. According to the WebSphere documentation, the port number can be found using the administrative console: Servers → Application Servers → server_name → End Points.

The screenshot shows the 'Application servers' page in the WebSphere Integrated Solutions Console. The page title is 'Application servers' and it includes a description: 'Use this page to view a list of the application servers in your environment and the status of each of these servers. You can also use this page status of a specific application server.' Below the description are buttons for 'New', 'Delete', 'Templates...', 'Start', 'Stop', 'Restart', 'ImmediateStop', and 'Terminate'. A table lists the servers:

Select	Name	Node	Host Name	Version	Cluster Name	Status
<input type="checkbox"/>	sarvz1	Node0104	Node01.ind.hp.com	ND 7.0.0.0		→
<input type="checkbox"/>	stoCluster_Member	Node0104	Node01.ind.hp.com	ND 7.0.0.0	stnCluster_on_btovm504	→

Total 2

Sample Configurations

The sample WebSphere SPI configurations with entries in this section illustrate various features and utilization methods.

Example 1: Single Node/Two Servers

The following example is for a single node running two servers: the administration server and one managed server. The properties HOME and JAVA_HOME are global defaults that apply to all servers and nodes. When the file is saved, passwords are encrypted.

```
HOME = /opt/WebSphere/AppServer
JAVA_HOME=/opt/WebSphere/AppServer/java


NODE main.hp.com
{
  SERVER1_NAME= adminserver
  SERVER1_PORT= 900
  SERVER1_LOGIN= system
  SERVER1_PASSWORD = password

  SERVER2_NAME= managedserver
  SERVER2_PORT= 905
  SERVER2_LOGIN= system
  SERVER2_PASSWORD= password
}
```

Example 2: Multiple Nodes/Repeated Properties

The following example shows how you can configure a group of related systems that have numerous properties in common. Some nodes, however, might have one or two properties that you need to specify differently. You can address these kinds of situations in two steps:

- 1 Use the Add Group action in the configuration editor to name the group, specify the nodes in it, and set the configuration properties. See [Add Group](#) on page 126.
- 2 Use the Add Node action in the configuration editor to define individual node properties (either for nodes not in the group or for nodes in the group that have some unique/separate properties). See [Add Node](#) on page 126.

 Properties set for a node take precedence over the same properties set for a group. For the complete order of property precedence, see [Property Precedence](#) on page 120.

In the example, the global default properties HOME and JAVA_HOME are overridden for the node europa.hp.com. Since the start commands are set to use the system init command /sbin/init.d/WebSphere start which runs at system boot and starts all of the WebSphere Servers, we have configured USER to be root.

```
HOME = /opt/WebSphere/AppServer
JAVA_HOME = /opt/WebSphere/AppServer/java
USER = root

GROUP production
```



```

{
  mercury.hp.com
  venus.hp.com
  mars.hp.com
  jupiter.hp.com
}

NODE production
{
  SERVER1_NAME= partsserver
  SERVER1_PORT= 900
  SERVER1_LOGIN= system
  SERVER1_PASSWORD= password
  SERVER1_ADMIN_HOST= earth.hp.com
  SERVER1_ADMIN_PORT= 900
  SERVER1_START_CMD= /sbin/init.d/WebSphere start

  SERVER2_NAME= orderserver
  SERVER2_PORT= 910
  SERVER2_LOGIN= system
  SERVER2_PASSWORD= moresecret
  SERVER2_START_CMD= /sbin/init.d/WebSphere start
}

NODE jupiter.hp.com
{
  SERVER1_PASSWORD= different1password
  SERVER2_PASSWORD= different2password
}

NODE europa.hp.com
{
  SERVER1_HOME = /opt/websphere
  SERVER1_JAVA_HOME = /opt/websphere/java
  SERVER1_NAME= testserver
  SERVER1_PORT= 920
  SERVER1_LOGIN= system
  SERVER1_PASSWORD= mypassword
}

```

Example 3: WebSphere Servers with Virtual IP Addresses

The following example shows how to configure WebSphere Servers that use virtual IP addresses. The property `SERVER<n>_ADDRESS` is set to the name or IP address where the server is listening.

```

NODE saturn.hp.com
{
  SERVER1_HOME = /opt/WebSphere/AppServer
  SERVER1_JAVA_HOME = /opt/WebSphere/AppServer/java
  SERVER1_NAME= partsserver
  SERVER1_PORT= 900
  SERVER1_ADDRESS= juno.hp.com
  SERVER1_LOGIN= system
  SERVER1_PASSWORD= mypassword
}

```

```

SERVER2_HOME = /opt/WebSphere/AppServer
SERVER2_JAVA_HOME = /opt/WebSphere/AppServer/java
SERVER2_NAME= orderserver
SERVER2_PORT= 901
SERVER2_ADDRESS= 15.15.1.1
SERVER2_LOGIN= system
SERVER2_PASSWORD= mypassword
}

```

Example 4: Administrative Privileges Using Same Login Information

The following example shows the location of the LOGIN and PASSWORD properties if this information is used for all WebSphere administrative privileges. When the file is saved, the password is encrypted.

```

HOME = /opt/WebSphere/AppServer
JAVA_HOME = /opt/WebSphere/AppServer/java
LOGIN = admin
PASSWORD = password

NODE main.hp.com
{
  SERVER1_NAME = server1
  SERVER1_PORT = 900

  SERVER2_NAME = server2
  SERVER2_PORT = 905
}

NODE europa.hp.com
{
  SERVER1_HOME = /opt/wbs/appserver
  SERVER1_JAVA_HOME = /opt/wbs/appserver/java
  SERVER1_NAME= testserver
  SERVER1_PORT= 915
}

```

Example 5: Administrative Privileges Using Different Login Information

The following example shows the location of the LOGIN and PASSWORD properties if this information is different for administrative privileges. On the main.hp.com node, SERVER1 and SERVER2 have separate administrative privileges. When the file is saved, the passwords are encrypted.

```

HOME = /opt/WebSphere/AppServer
JAVA_HOME = /opt/WebSphere/AppServer/java

NODE main.hp.com
{
  SERVER1_NAME = server1
  SERVER1_PORT = 900
  SERVER1_LOGIN = server1_admin
  SERVER1_PASSWORD = server1_password
}

```

```
SERVER2_NAME = server2
SERVER2_PORT = 905
SERVER2_LOGIN = server2_admin
SERVER2_PASSWORD = server2_password
}

NODE europa.hp.com
{
  LOGIN = europa_admin
  PASSWORD = europa_password

  SERVER1_NAME= testserver
  SERVER1_PORT= 915

  SERVER2_NAME= anotherserver
  SERVER2_PORT= 920
}
```

C Error Messages

The WebSphere SPI error messages contain the following information:

- Error Message Number
- Description
- Severity
- Help Text (Probable Cause and Suggested Action)

Error messages can be viewed from the HPOM Message Browser. Double-click the error message to open the message. The Message Properties Window appears. Click the **Message Text** tab to view the error message.

WASSPI-1

Description	Unable to create the lock file <filename>. File already exists.
Severity	Critical
Help Text	<p>Probable Cause: Temporary lock files are used to avoid collisions when multiple WebSphere SPI data collector processes attempt to access the same data file. This error occurs when the lock file cannot be created after several attempts because it already exists.</p> <p>Suggested Action: If a file by the same name already exists, it might not have been deleted by a previous run of the WebSphere SPI data collector. You must delete this file manually.</p>

WASSPI-2

Description	Cannot access the SPI configuration.
Severity	Critical
Help Text	<p>Probable Cause: A WebSphere SPI configuration file cannot be located or accessed. Either the file does not exist or there was a problem reading the file.</p> <p>Suggested Action:</p> <ol style="list-style-type: none">1 Verify that the WebSphere SPI has been configured correctly by running the SPI Admin → Verify tool. If the configuration is not correct, run the SPI Admin → Discover or Configure WBSSPI tool.2 See the text following the error message in the WebSphere SPI error log to help identify the underlying cause of the problem, for example, an I/O exception. You can view the SPI error log for a managed node by using the SPI Admin → View Error File tool. The error message can be identified by the date/time stamp.

WASSPI-3

Description	Error parsing command line.
Severity	Critical
Help Text	<p>Probable Cause: The WebSphere SPI data collector command line is incorrectly specified in a schedule policy.</p> <p>Suggested Action:</p> <ol style="list-style-type: none">1 See the text following the error message in the WebSphere SPI error log to help identify the underlying cause of the problem, for example, an I/O exception. You can view the SPI error log for a managed node by using the SPI Admin → View Error File tool. The error message can be identified by the date/time stamp.2 Correct the policy that contains the incorrect command line and redeploy. For more information on the WebSphere SPI data collector command line, see the <i>HP Operations Smart Plug-in for IBM WebSphere Application Server Installation and Configuration Guide</i>.

WASSPI-5

Description	Error processing metric <i><metric_number></i> .
Severity	Major
Help Text	<p>Probable Cause: An error occurred while trying to collect data or perform calculations for the specified metric.</p> <p>Suggested Action: See the text following the error message in the WebSphere SPI error log to help identify the underlying cause of the problem. The error messages previous to this one may also provide more information about the problem. You can view the WebSphere SPI error log for a managed node by using the SPI Admin → View Error File tool. The error message can be identified by the date/time stamp.</p>

WASSPI-6

Description	Required property <i><property_name></i> is missing from the WebSphere configuration.
Severity	Major
Help Text	<p>Probable Cause: The specified required property is missing from the WebSphere SPI configuration file.</p> <p>Suggested Action:</p> <ol style="list-style-type: none">1 Run the SPI Admin → Discover or Configure WBSSPI tool. Verify that you have specified the correct server information for the WebSphere servers on this managed node.2 Verify the property is specified correctly in the WebSphere SPI configuration file (/var/opt/OV/wasspi/wbs/conf/SiteConfig on UNIX platforms or Agent_Dir\wasspi\wbs\conf\SiteConfig on Windows platforms) on the managed node in question.

WASSPI-7

Description	Unable to contact server <i><server_name></i> at url= <i><URL></i> , port= <i><port></i> .
Severity	Critical

Help Text	<p>Probable Cause: The specified server is not running at the specified port.</p> <p>Suggested Action:</p> <ol style="list-style-type: none"> 1 Run the SPI Admin → Discover or Configure WBSSPI tool. Verify that you have specified the correct server information for the WebSphere servers on this managed node. 2 Verify that the properties, <code>SERVERx_NAME</code> and <code>SERVERx_PORT</code> are specified correctly in the WebSphere SPI configuration file (<code>/var/opt/OV/wasspi/wbs/conf/SiteConfig</code> on UNIX platforms or <code>Agent_Dir\wasspi\wbs\conf\SiteConfig</code> on Windows platforms) on the managed node in question. 3 Verify that the WebSphere Application Server is running on the managed node.
------------------	---

WASSPI-8

Description	Error saving graphing or reporting data to file <code><file_name></code> .
Severity	Critical
Help Text	<p>Probable Cause: The specified graphing or reporting data file could not be found or an I/O error occurred when trying to access the file.</p> <p>Suggested Action:</p> <ol style="list-style-type: none"> 1 See the text following the error message in the WebSphere SPI error log to help identify the underlying cause of the problem. You can view the WebSphere SPI error log for a managed node by using the SPI Admin → View Error File tool. The error message can be identified by the date/time stamp. 2 Identify the steps to reproduce the problem. 3 Run the SPI Admin → Start Tracing tool to turn on tracing. Try to reproduce the problem. 4 Run the SPI Admin → Self-Healing Info tool. Contact HP support with the information gathered by this tool.

WASSPI-9

Description	Unable to retrieve property <property_name>.
Severity	Critical
Help Text	<p>Probable Cause: A required property is missing from one of the WebSphere SPI configuration files.</p> <p>Suggested Action:</p> <ol style="list-style-type: none">1 See the text following the error message in the WebSphere SPI error log to help identify the underlying cause of the problem. You can view the WebSphere SPI error log for a managed node by using the SPI Admin → View Error File tool. The error message can be identified by the date/time stamp.2 Run the SPI Admin → Discover or Configure WBSSPI tool. Verify that you have specified the correct information for the WebSphere servers on the managed node in question.3 Verify that the missing property is now specified in the WebSphere SPI configuration file (/var/opt/OV/wasspi/wbs/conf/SiteConfig on UNIX platforms or Agent_Dir\wasspi\wbs\conf\SiteConfig on Windows platforms) on the managed node in question.

WASSPI-10

Description	Encountered problem accessing file <i><filename></i> .
Severity	Critical
Help Text	<p>Probable Cause:</p> <p>The specified file could not be found, created, or accessed. This file could be a temporary file.</p> <p>Suggested Action:</p> <ol style="list-style-type: none">1 See the text following the error message in the WebSphere SPI error log to help identify the underlying cause of the problem. You can view the WebSphere SPI error log for a managed node by using the SPI Admin → View Error File tool. The error message can be identified by the date/time stamp.2 Verify that you have enough disk space to create temporary files.

WASSPI-11

Description	No servers were specified in the WebSphere SPI configuration file.
Severity	Major
Help Text	<p>Probable Cause:</p> <p>The number of WebSphere instances specified in the WebSphere SPI configuration file for the managed node in question is 0.</p> <p>Suggested Action:</p> <ol style="list-style-type: none">1 Run the SPI Admin → Discover or Configure WBSSPI tool. Verify that you have specified the correct server name and port information for the WebSphere servers on this managed node.2 Verify that the property, <code>NUM_SERVERS</code>, in the WebSphere SPI configuration file (<code>/var/opt/OV/wasspi/wbs/conf/SiteConfig</code> on UNIX platforms or <code>Agent_Dir\wasspi\wbs\conf\SiteConfig</code> on Windows platforms) is set to the number of WebSphere Application Servers on this managed node.

WASSPI-12

Description	Command <i><command></i> returned error exit code <i><exit code></i> .
Severity	Critical
Help Text	<p>Probable Cause: A command started by the WebSphere SPI collector has returned an error (non-zero) exit code.</p> <p>Suggested Action:</p> <ol style="list-style-type: none">1 Identify the steps to reproduce the problem.2 Run the SPI Admin → Start Tracing tool to turn on tracing.3 Reproduce the problem.4 Run the SPI Admin → Stop Tracing tool to turn off tracing.5 Run the SPI Admin → Self-Healing Info tool. Contact HP support with the information gathered by this tool.

WASSPI-13

Description	Exception occurred while running an <code>opcmon</code> process.
Severity	Critical
Help Text	<p>Probable Cause: The WebSphere SPI data collector attempted to run a process to execute an <code>opcmon</code> call. Either the process could not be created or was interrupted.</p> <p>Suggested Action: For UNIX systems, make sure the kernel configurable parameters <code>NPROC</code> and <code>MAXUPRC</code> are set high enough to allow process creation.</p>

WASSPI-14

Description	Unable to find file <file_name>.
Severity	Critical
Help Text	<p>Probable Cause: A file required by the WebSphere data collector could not be found.</p> <p>Suggested Action:</p> <ol style="list-style-type: none">1 See the text following the error message in the WebSphere SPI error log to help identify the underlying cause of the problem. The error messages previous to this one may also provide more information about the problem. You can view the WebSphere SPI error log for a managed node by using the SPI Admin → View Error File tool. The error message can be identified by the date/time stamp.2 Run the SPI Admin → Discover or Configure WBSSPI tool on this managed node.

WASSPI-15

Description	Error parsing XML document <file_name>.
Severity	Critical
Help Text	<p>Probable Cause: An error occurred while parsing the specified XML document.</p> <p>Suggested Action:</p> <ol style="list-style-type: none">1 See the text following the error message in the WebSphere SPI error log to help identify the underlying cause of the problem. The error messages previous to this one may also provide more information about the problem. You can view the WebSphere SPI error log for a managed node by using the SPI Admin → View Error File tool. The error message can be identified by the date/time stamp.2 If the XML document was provided by the user, correct the document. For more information on the correct format for a user-defined metric definition document, see the <i>HP Operations Manager Smart Plug-in for IBM WebSphere Application Server Configuration Guide</i>.3 If the XML document is a document that is shipped with the WebSphere SPI, run the SPI Admin → Discover or Configure WBSSPI tool to reinstall the WebSphere SPI configuration files.

WASSPI-16

Description	A bad filter (<i><filter_value></i>) was specified for metric <i><metric_number></i> .
Severity	Major
Help Text	<p>Probable Cause: A metric filter is incorrectly specified in the metric definitions XML document.</p> <p>Suggested Action:</p> <ol style="list-style-type: none">4 If the metric is specified in an XML document that was provided by the user, correct the document. For more information on the correct format for a user-defined metric definition document, see the <i>HP Operations Manager Smart Plug-in for IBM WebSphere Application Server Configuration Guide</i>.1 If the metric is a pre-defined metric that is shipped with the WebSphere SPI, run the SPI Admin → Discover or Configure WBSSPI tool to reinstall the WebSphere SPI configuration files.

WASSPI-18

Description	Error logging to datasource <i><datasource_class_name></i> . Logging process returned exit code <i><exit_code></i> .
Severity	Warning
Help Text	<p>Probable Cause: The <code>ddflog</code> process started by the WebSphere SPI data collector returned a non-zero error code.</p> <p>Suggested Action:</p> <ol style="list-style-type: none">1 Identify the steps to reproduce the problem.2 Run the SPI Admin → Start Tracing tool to turn on tracing. Try to reproduce the problem.3 Run the SPI Admin → Self-Healing Info tool. Contact HP support with the information gathered by this tool.

WASSPI-19

Description	Encountered problem instantiating XSLT transformer with <i><file_name></i> .
Severity	Major
Help Text	<p>Probable Cause: The XSL document that specifies the auto-action report output contains errors.</p> <p>Suggested Action: Run the SPI Admin → Discover or Configure WBSSPI tool on the selected managed node.</p>

WASSPI-20

Description	Encountered problem creating report for metric <i><metric_number></i> .
Severity	Major
Help Text	Probable Cause: An error occurred while producing a text report for the specified metric. Suggested Action: Run the SPI Admin → Discover or Configure WBSSPI tool on the selected managed node.

WASSPI-21

Description	Encountered problem instantiating factory implementation <i><class name></i> .
Severity	Critical
Help Text	Probable Cause: The java property specifying the class name is incorrect or the class does not implement the AppServerFactory interface. Suggested Action: Verify that the java property <code>appserver.implementation</code> is set to the fully qualified name of the class which implements the AppServerFactory interface. For example, if set on the java command-line: <code>-Dappserver.implementation=com.hp.openview.wasspi.WBSAppServerFactory</code>

WASSPI-22

Description	The PMI instrumentation level was changed from <i><old_level></i> to <i><new_level></i> for module <i><module_name></i> in server <i><server_name></i> .
Severity	Warning
Help Text	Probable Cause: A requested metric's impact rating exceeded the instrumentation level settings of the application server. The instrumentation level of the appropriate PMI module was raised to enable collection of the requested metric.

WASSPI-23

Description	Error initializing collector analyzer for server <server_name>.
Severity	Critical
Help Text	<p>Probable Cause An exception was encountered while preparing to monitor server <server_name>.</p> <p>Suggested Action</p> <ol style="list-style-type: none">1 See the text following the error message in the WebSphere SPI error log to help identify the underlying cause of the problem. You can view the WebSphere SPI error log for a managed node by using the SPI Admin → View Error File tool. The error message can be identified by the date/time stamp.2 Identify the steps to reproduce the problem.3 Run the SPI Admin → Start Tracing tool to turn on tracing. Try to reproduce the problem.4 Run the SPI Admin → Self-Healing Info tool. Contact HP support with the information gathered by this tool.

WASSPI-24

Description	Error logging in to server <server_name> with login <login>.
Severity	Critical
Help Text	<p>Probable Cause: A security exception occurred while logging in to server <server_name>.</p> <p>Suggested Action:</p> <ol style="list-style-type: none">1 Run the SPI Admin → Discover or Configure WBSSPI tool on the managed node on which the error occurred and verify that you have specified the correct login and password properties.2 Verify that the login has appropriate permissions.

WASSPI-25

Description	Performance monitoring service is not enabled on server <server_name>.
Severity	Warning
Help Text	<p>Probable Cause: PMI service is not enabled on server <server_name>.</p> <p>Suggested Action:</p> <ol style="list-style-type: none">1 Use the WebSphere Administrative Console to enable PMI on server <server_name>.2 Restart server <server_name>.

WASSPI-26

Description	The data logging process for server <i><server_name></i> timed-out.
Severity	Major
Help Text	<p>Probable Cause</p> <p>Depending on your configuration, either HP Performance Agent or CODA failed to exit before the time-out.</p> <p>Suggested Action</p> <ol style="list-style-type: none">1 Restart CODA using command opcagt -start.2 Restart HP Performance Agent using command mwa restart.

WASSPI-27

Description	RMI collector unable to process <i><command></i> .
Severity	Warning
Help Text	<p>Probable Cause</p> <p>An exception was encountered while performing an rmid-related operation.</p> <p>Suggested Action</p> <ol style="list-style-type: none">1 See the text following the error message in the WebSphere SPI error log to help identify the underlying cause of the problem. The error messages previous to this one may also provide more information about the problem. You can view the WebSphere SPI error log for a managed node by using the SPI Admin → View Error File tool. The error message can be identified by the date/time stamp.2 Identify the steps to reproduce the problem.3 Run the SPI Admin → Start Tracing tool to turn on tracing. Try to reproduce the problem.4 Run the SPI Admin → Self-Healing Info tool. Contact HP support with the information gathered by this tool.

WASSPI-28

Description	RMID on port <i><port></i> has been <i><status></i> .
Severity	Normal

WASSPI-29

Description	Collector server <i><server id></i> for Java home <i><path></i> has been started.
Severity	Normal

WASSPI-30

Description	Failed to start <i><rmid_path></i> on port <i><port></i> .
Severity	Critical
Help Text	Probable Cause: The specified path is already in use. Suggested Action: Run the SPI Admin → Discover or Configure WBSSPI tool. Set the RMID_PORT property to a port number, which is not currently in use.

WASSPI-31

Description	Lost connection to RMI collector while processing <i><command></i> .
Severity	Warning

WASSPI-32

Description	Unable to retrieve metadata for mbean <i><JMX-ObjectName></i> .
Severity	Warning

WASSPI-33

Description	No actions matched server <i><server name></i> , version <i><version></i> .
Severity	Warning
Help Text	Probable Cause: JMXAction elements define FromVersion and ToVersion tags, which do not match the server version. Suggested Action: If the action is valid on the server, adjust either the JMXAction definition's FromVersion/ToVersion elements or the server's VERSION property.

WASSPI-34

Description	Metric <i><metric id></i> does not define any actions.
Severity	Warning
Help Text	Probable Cause: The metric ID specified with the action <code>-m</code> option does not define a JMXActions element. Suggested Action: Correct the action <code>-m</code> option if an incorrect metric ID was specified. Otherwise, add a JMXActions definition to the metric definition.

WASSPI-35

Description	Error executing action <i><action command-line></i> .
Severity	Major
Help Text	Probable Cause: An unexpected error occurred while executing the action. Suggested Action: View the managed node's errorlog to determine the root cause, which is logged following the error message.

WASSPI-36

Description	MBean <i><JMX objectname></i> on server <i><server name></i> , does not expose operation <i><operation name></i> .
Severity	Warning
Help Text	Probable Cause: An action's JMXCalls element defines an operation not exposed by the specified MBean. Suggested Action: Correct the JMXCalls element or remove the operation from the element.

WASSPI-37

Description	MBean <i><JMX objectname></i> on server <i><server name></i> , does not expose attribute <i><attribute name></i> for write.
Severity	Warning
Help Text	<p>Probable Cause: An action's JMXCalls element defines a write attribute exposed by the specified MBean as read-only.</p> <p>Suggested Action: If it is a custom MBean, update the MBean's management interface so the attribute is writable. Otherwise, remove the attribute definition from the JMXCalls element.</p>

WASSPI-38

Description	MBean <i><JMX objectname></i> on server <i><server name></i> , does not expose attribute <i><attribute name></i> .
Severity	Warning
Help Text	<p>Probable Cause: An action's JMXCalls element defines an attribute not exposed by the specified MBean ObjectName.</p> <p>Suggested Action: Correct the JMXCalls element or remove the attribute from the element.</p>

WASSPI-39

Description	Error invoking operation <i><operation name></i> on MBean <i><JMX objectname></i> .
Severity	Major
Help Text	<p>Probable Cause: An unexpected error occurred while invoking an operation on the specified MBean. The managed resource might have thrown an exception.</p> <p>Suggested Action: View the managed node's errorlog to determine the root cause, which is logged following the error message.</p>

WASSPI-40

Description	Error setting attribute <i><attribute name></i> on MBean <i><JMX objectname></i> .
Severity	Major
Help Text	<p>Probable Cause: An unexpected error occurred while setting an attribute on the specified MBean. The managed resource might have thrown an exception.</p> <p>Suggested Action: View the managed node's errorlog to determine the root cause, which is logged following the error message.</p>

WASSPI-41

Description	Error getting attribute <i><attribute name></i> from MBean <i><JMX objectname></i> .
Severity	Major
Help Text	<p>Probable Cause: An unexpected error occurred while getting an attribute from the specified MBean. The managed resource might have thrown an exception.</p> <p>Suggested Action: View the managed node's errorlog to determine the root cause, which is logged following the error message.</p>

WASSPI-42

Description	Error running command <i><command></i> .
Severity	Critical
Help Text	<p>Probable Cause A command started by the WebSphere SPI collector reported an error.</p> <p>Suggested Action</p> <ol style="list-style-type: none">1 Identify the steps to reproduce the problem.2 Run the SPI Admin → Start Tracing tool to turn on tracing.3 Reproduce the problem.4 Run the SPI Admin → Stop Tracing tool to turn off tracing.5 Run the SPI Admin → Self-Healing Info tool. Contact HP support with the information gathered by this tool.

WASSPI-43

Description	Error publishing event <i><event-type></i> .
Severity	Major
Help Text	Probable Cause An unexpected error occurred while a publisher was handling a metric or collecting event. Suggested Action View the managed node's error log to determine the cause, which is logged following the error message.

WASSPI-201

Description	File <i><filename></i> not found.
Severity	Critical
Help Text	Probable Cause: A configuration file could not be found. Suggested Action: Run the SPI Admin → Discover or Configure WBSSPI tool. Verify that correct information has been specified for the WebSphere servers on the managed node on which the error occurred.

WASSPI-202

Description	Cannot read file <i><filename></i> .
Severity	Critical
Help Text	Probable Cause: <ul style="list-style-type: none">• A file could not be opened or it could not be found.• Permissions might be incorrect or a directory might be corrupt. Suggested Action: <ol style="list-style-type: none">1 Run the SPI Admin → Discover or Configure WBSSPI tool. Verify that correct information has been specified for the WebSphere servers on the managed node on which the error occurred.2 Verify that the permissions are correct for the HP Operations agent user to read this file.

WASSPI-203

Description	Cannot write file <i><filename></i> .
Severity	Critical
Help Text	<p>Probable Cause: Permissions might be incorrect, or a file or directory might be corrupt.</p> <p>Suggested Action:</p> <ol style="list-style-type: none">1 Run the SPI Admin → Discover or Configure WBSSPI tool. Verify that correct information has been specified for the WebSphere servers on the managed node on which the error occurred.2 Verify that the permissions are correct for the HP Operations agent user to read this file.

WASSPI-204

Description	Error sending <code>opcmsg</code> <i><message></i> .
Severity	Critical
Help Text	<p>Probable Cause: There was a problem running <code>opcmsg</code>. <code>opcmsg</code> might be missing or not have permissions to execute (HPOM installation errors) or the system process table might be full.</p> <p>Suggested Action: Confirm that the WebSphere SPI-Messages policy has been deployed on the managed node.</p>

WASSPI-205

Description	Error sending <code>opcmon</code> <i><command></i> .
Severity	Critical
Help Text	<p>Probable Cause: There was a problem running <code>opcmon</code>. <code>opcmon</code> might be missing or not have permissions to execute (HPOM installation errors) or the system process table might be full.</p> <p>Suggested Action: Confirm that HPOM is properly installed and deployed on the managed node. Make sure that the process table is not full. If it is, consider having the system administrator increase it.</p>

WASSPI-206

Description	Cannot read directory <i><directory></i> .
Severity	Critical
Help Text	Probable Cause: The permissions on the directory prevent the HP Operations agent user from reading it or the directory is corrupt. Suggested Action: Verify that the permissions are correct for an HP Operations agent user for this directory.

WASSPI-207

Description	Cannot move <i><filename></i> to <i><filename></i> .
Severity	Critical
Help Text	Probable Cause: <ol style="list-style-type: none">1 Insufficient permissions.2 Insufficient disk space.3 File table problems. Suggested Action: <ol style="list-style-type: none">1 Verify that the permissions are correct for the HP Operations agent user.2 Verify that there is enough disk space to create files.3 Run the SPI Admin → Discover or Configure WBSSPI tool.

WASSPI-208

Description	WebSphere SPI must be configured before it can be used.
Severity	Critical
Help Text	Probable Cause: The WebSphere SPI was not configured on this node. Suggested Action: <ol style="list-style-type: none">1 Run the SPI Admin → Discover or Configure WBSSPI tool. Verify that the correct information has been specified for the WebSphere servers on the managed node on which the error occurred.2 Run the SPI Admin → Verify tool on the managed node to confirm that the SPI has been successfully configured.

WASSPI-209

Description	Cannot contact WebSphere Server.
Severity	Critical
Help Text	<p>Probable Cause:</p> <ul style="list-style-type: none">• The server could be down or not responding.• The SPI might be configured incorrectly. <p>Suggested Action:</p> <ol style="list-style-type: none">1 Verify that WebSphere is up and running properly.2 Run the SPI Admin → Discover or Configure WBSSPI tool.3 Run the SPI Admin → Verify tool on the managed node to confirm that the SPI has been successfully configured.

WASSPI-210

Description	Cannot configure SPI.
Severity	Critical
Help Text	<p>Probable Cause:</p> <p>The SPI configuration process failed.</p> <p>Suggested Action:</p> <ol style="list-style-type: none">1 See the text following the error message in the WebSphere SPI error log to help identify the underlying cause of the problem. The error messages previous to this one may also provide more information on the problem. You can view the WebSphere SPI error log for a managed node by using the SPI Admin → View Error File tool. The error message can be identified by the date/time stamp.2 Run the SPI Admin → Discover or Configure WBSSPI tool.

WASSPI-211

Description	Cannot create directory <directory>.
Severity	Critical
Help Text	<p>Probable Cause: There are insufficient permissions for the HP Operations agent user to create the directory or there is insufficient disk space.</p> <p>Suggested Action:</p> <ol style="list-style-type: none">1 Verify that the permissions are correct for the HPOM user for this directory.2 Verify that there is enough disk space.

WASSPI-213

Description	Improper parameters to program <i><name></i> . Usage: <i><usage></i> .
Severity	Critical
Help Text	Probable Cause: The parameters set to the program are incorrect. Suggested Action: Correct the parameters.

WASSPI-214

Description	Cannot run program <i><program name></i> .
Severity	Critical
Help Text	Probable Cause: The program failed to run. The program might be missing, permissions might be incorrect or the process table might be full. Suggested Action: <ol style="list-style-type: none">1 Verify that the file exists. If it is a SPI program and the file is missing, run the SPI Admin → Discover or Configure WBSSPI tool with the managed node selected.2 Verify that the permissions are correct for the HP Operations agent user.

WASSPI-216

Description	Configuration variable <i><name></i> missing for server <i><server_name></i> .
Severity	Critical
Help Text	Probable Cause: A required SPI configuration variable was not found. Suggested Action: <ol style="list-style-type: none">1 Run the SPI Admin → Discover or Configure WBSSPI tool.2 Verify that correct information was specified in the configuration for the managed node on which the error occurred.

WASSPI-218

Description	WebSphere monitoring has been turned OFF for <server_name>.
Severity	Warning
Help Text	Probable Cause: Collection has been turned off for the specified server. Suggested Action: If desired, collection can be turned on by running the SPI Admin → Start Monitoring tool.

WASSPI-219

Description	WebSphere monitoring has been turned ON for <server_name>.
Severity	Critical
Help Text	Probable Cause: Collection has been turned on for the specified server. Suggested Action: If desired, collection can be turned off by running the SPI Admin → Stop Monitoring tool.

WASSPI-221

Description	<file_name> does not exist.
Severity	Critical
Help Text	Probable Cause: The specified file does not exist. If it is a log file, no entries were logged to it. If it is a property file, it has not been configured. Suggested Action: <ul style="list-style-type: none">• Log files: If there have never been any entries written to the file, no action is necessary. Otherwise, run the SPI Admin → Discover or Configure WBSSPI tool.• Property files: Run the SPI Admin → Discover or Configure WBSSPI tool.

WASSPI-222

Description	<file_name> is empty.
Severity	Critical
Help Text	<p>Probable Cause: The specified file is empty. If it is a log file, no entries were logged to it, or the entries were cleaned out. If it is a property file, it is not properly configured.</p> <p>Suggested Action: If the file is a configuration file, run the SPI Admin → Discover or Configure WBSSPI tool.</p>

WASSPI-223

Description	Cannot read <file_name>.
Severity	Critical
Help Text	<p>Probable Cause:</p> <ol style="list-style-type: none">1 A file could not be opened or it could not be found.2 Permissions might be incorrect or a directory might be corrupt. <p>Suggested Action:</p> <ol style="list-style-type: none">1 Run the SPI Admin → Discover or Configure WBSSPI tool. Verify that correct information has been specified for the WebSphere servers on the managed node on which the error occurred.2 Verify that the permissions are correct for the HP Operations agent user to read this file.

WASSPI-224

Description	ddfcamp returned an error configuring <name>.
Severity	Critical
Help Text	<p>Probable Cause: ddfcamp returned an error. This might be because neither HP Performance Agent nor CODA is installed on the system or because an error occurred while configuring the performance agent.</p> <p>Suggested Action:</p> <ol style="list-style-type: none">1 If the performance agent is not installed, this error can be ignored.2 Otherwise, identify the steps to reproduce the problem.3 Run the SPI Admin → Start Tracing tool to turn on tracing. Try to reproduce the problem.4 Run the SPI Admin → Self-Healing Info tool. Contact HP support with the information gathered by this tool.

WASSPI-225

Description	No logfiles were found. Did you run Config WebSphere SPI?
Severity	Critical
Help Text	Probable Cause: The logfile list is empty. Suggested Action: Run the SPI Admin → Discover or Configure WBSSPI tool.

WASSPI-226

Description	Cannot read file <file_name>.
Severity	Critical
Help Text	Probable Cause: <ul style="list-style-type: none">• A file could not be opened or it could not be found.• Permissions might be incorrect or a directory might be corrupt. Suggested Action: <ol style="list-style-type: none">1 Run the SPI Admin → Discover or Configure WBSSPI tool.2 Verify that you specified the correct information for the WebSphere Servers on the managed node on which the error occurred.3 Verify that the permissions are correct for the HP Operations agent user to read this file.

WASSPI-227

Description	No HP Performance Agent is installed. Data source will not be configured.
Severity	Warning
Help Text	Probable Cause: If an Operations performance tool is available, the SPI integrates with it. This warning indicates that none is available. Suggested Action: If you have a HP Performance Agent installed, verify that it is installed correctly and is running; reinstall it if necessary. Otherwise, this message can be ignored.

WASSPI-228

Description	ddflog returned an error logging <logfile-name>: <system-error-msg>.
Severity	Critical
Help Text	<p>Probable Cause: ddflog returned an error. This could be because the SPI was not properly configured to log performance data.</p> <p>Suggested Action:</p> <ol style="list-style-type: none">1 Redeploy SPI for WebSphere and SPIDataCollector instrumentation on the node having the problem.2 Otherwise, examine the system error message, if any, for clues to the problem.3 Run the SPI Admin → Start Tracing tool to turn on tracing. Try to reproduce the problem.4 Run the SPI Admin → Self-Healing Info tool. Contact HP support with the information gathered by this tool.

WASSPI-229

Description	Cannot connect to directory <directory-name>.
Severity	Critical
Help Text	<p>Probable Cause: The directory does not exist, or the agent which runs under the user, does not have appropriate permissions to the directory.</p> <p>Suggested Action: Run the SPI Admin → Discover or Configure WBSSPI tool.</p>

WASSPI-230

Description	Cannot get lock <file> after <time>.
Severity	Critical
Help Text	<p>Probable Cause: The lock file <file> was not cleared in the <time> indicated. This could be due to a very slow running or hung SPI process. Possibly a SPI process that had a lock was killed before the lock was open and cleared.</p> <p>Suggested Action: Make sure no SPI processes are running. Manually remove the lock file.</p>

WASSPI-231

Description	Error starting JRE <JVM_file>: <message>.
Severity	Critical
Help Text	<p>Probable Cause: Some error occurred starting Java. This could be that the specified JVM does not exist, has bad permissions, or that there are system resource limitations such as process table entries or memory, or that the JAVA_HOME variable in the SPI SiteConfig file is not set correctly.</p> <p>Suggested Action:</p> <p>Check for other errors generated at the same time, they might indicate the real cause. If the specified file does not exist, check your JAVA_HOME or HOME variables in the SPI configuration.</p>

WASSPI-232

Description	Server <name> specified on command line, but not in configuration.
Severity	Critical
Help Text	<p>Probable Cause: There was a -i or -e specified on the collector command line which specified a server name that was not listed in the SPI configuration. The collector only knows about servers listed in the configuration.</p> <p>Suggested Action:</p> <ol style="list-style-type: none">1 Specify a correct server name on the command line.2 Run the SPI Admin → Discover or Configure WBSSPI tool.3 Verify the WebSphere server names are correctly listed and spelled in the SPI configuration. Note that the server name is case-sensitive.

WASSPI-234

Description	Error running program <file>, return value: <n>.
Severity	Critical
Help Text	<p>Probable Cause:</p> <p>The SPI attempted to run some tool or auxiliary program and encountered an error doing so. The tool or program is shown in the message as <file> and the return code attempting to run it, is shown as <n>.</p> <p>Suggested Action:</p> <p>If the tool is a SPI tool, make sure the SPI has been installed and configured correctly. If not, reinstall or reconfigure. If it is a system tool, make sure there are no system problems that is preventing the tool from running.</p>

WASSPI-235

Description	Restart of HP Performance Agent failed.
Severity	Warning
Help Text	<p>Probable Cause: The SPI attempted to automatically restart the HP Performance Agent and the automatic attempt failed.</p> <p>Suggested Action: Restart the HP Performance Agent manually using the <code>mwa restart server</code> command.</p>

WASSPI-236

Description	Failure when running XSLT on <code><xml></code> with stylesheet <code><xsl></code> : <code><message></code> .
Severity	Critical
Help Text	<p>Probable Cause: As part of setting up graphing for user defined metrics, a translation of the UDM XML is done. This message indicated that the translation failed for some reason.</p> <p>Suggested Action: Review the message shown. It is most likely that there is an error in the XML.</p>

WASSPI-237

Description	Setting up Data Source <code><datasource></code> .
Severity	Normal
Help Text	This is an informational message that a HP Performance Manager or HP Performance Agent datasource was setup.

WASSPI-238

Description	No User Defined Metrics found.
Severity	Warning
Help Text	<p>Probable Cause: The JMX Metric Builder → WBSSPI → UDM Graph Enable tool was run, but no UDM metrics had been defined.</p> <p>Suggested Action: Run the SPI Admin → Discover or Configure WBSSPI tool and check that the UDM XML file (UDM_DEFINITIONS_FILE property) has been named correctly.</p>

WASSPI-241

Description	Cannot delete file <file>.
Severity	Critical
Help Text	<p>Probable Cause: The SPI attempted to delete a file, but was unable to do so. The protection of the file might be set to prevent an HP Operations agent from deleting it, or that there is some system problem preventing the file from being deleted.</p> <p>Suggested Action: Make sure the protection of the file is correct.</p>

Others

Description	An unknown error appears in the WebSphere SPI error log.
Severity	Warning
Help Text	<p>Suggested Action:</p> <ol style="list-style-type: none">1 See the text following the error message in the WebSphere SPI error log to help identify the underlying cause of the problem. The error messages previous to this one may also provide more information on the problem. You can view the WebSphere SPI error log for a managed node by using the SPI Admin → View Error File tool. The error message can be identified by the date/time stamp.2 Identify the steps to reproduce the problem.3 Run the SPI Admin → Start Tracing tool to turn on tracing. Try to reproduce the problem.4 Run the SPI Admin → Self-Healing Info tool. Contact HP support with the information gathered by this tool.

Glossary

agent

A program or process running on a remote device or computer system that responds to management requests, performs management operations, or sends performance and event notification. An agent can provide access to managed objects and MIB variables, interpret policy for resources and do configuration of resources.

application

Packaged software that provides functionality that is designed to accomplish a set of related tasks. An application is generally more complex than a tool.

ASCII

American Standard Code for Information Interchange.

assigned policy

A policy that has been assigned to one or more resources in the computing environment but which has not yet been deployed or installed on those resources.

automatic action

A pre-configured program or script that is executed in response to an event, message, or a change in information in the management database. without operator intervention.

client

When the context is network systems, a computer system on a network that accesses a service from another computer (server). When the context is software, a program or executable process that requests a service from a server.

client console

An instance of the user interface that appears on the client system while the application runs on a server.

command

An instruction to a computer program that causes a specified operation to be carried out. Commands are typically typed by users on a command line.

configuration

In a network context, the complete set of inter-related systems, devices and programs that make up the network. For example the components of a network may include computer systems, routers, switches, hubs, operating systems and network software. The configuration of the network determines the way that it works and the way that it is used. In a software context, the combination of settings of software parameters and attributes that determine the way the software works, the way it is used, and how it appears.

configuration file

A file that contains specifications or information that can be used for determining how a software program should look and operate.

configure

To define and modify specified software settings to fulfill the requirements of a specified environment, application or usage.

connection

A representation of a logical or physical relationship between objects.

console

An instance of the user interface from which the user can control an application or set of applications.

customization

The process of designing, constructing or modifying software to meet the needs and preferences of a particular customer or user.

customize

To design, construct or modify software to meet the needs and preferences of a particular customer or user.

data type

A particular kind of data; for example database A repository of data that is electronically stored. Typically databases are organized so that data can be retrieved and updated.

deploy

To install and start software, hardware, capabilities, or services so that they work in the business environment.

Deployed application

An application and its components that have been installed and started to work in the business environment.

deployed policy

A policy that is deployed on one or more resources in the computing environment.

deployment

The process of installing and activating software, hardware, capabilities or services so that they work in the business environment.

Deployment package

A software package that can be deployed automatically and installed on a managed node.

error log

An output file containing error messages.

event

An event is an unsolicited notification such as an SNMP trap or WMI notification generated by an agent or process in a managed object or by a user action. Events usually indicate a change in the state of a managed object or cause an action to occur.

HP Operations Manager

A family of network and system management products, and an architecture for those products. HPOM includes development environments and a wide variety of management applications.

Hypertext Transfer Protocol (HTTP).

The protocol that World Wide Web clients and servers use to communicate.

HTTPS

Hypertext Transfer Protocol Secure.

icon

An on-screen image that represents objects that can be monitored or manipulated by the user or actions that can be executed by the user.

managed object

A network, system, software or service object that is both monitored for performance, status and messages and is manipulated by means of actions in the management software.

management console

An instance of the user interface from which the user can control the management application or set of management applications. The console may be on the system that contains the management software or it may be on another system in the management domain.

management server

A server that provides management services, processes, or a management user interface to clients. A management server is a type of management station.

message

A structured, readable notification that is generated as a result of an event, the evaluation of one or more events relative to specified conditions, or a change in application, system, network, or service status.

message browser

A graphical user interface that presents notifications that are generated as a result of an event, the evaluation of one or more events relative to specified conditions or a change in application, system, network, or service status.

message description

Detailed information about an event or message.

message key

A message attribute that is a string used to identify messages that were triggered from particular events. The string summarizes the important characteristics of the event. Message keys can be used to allow messages to acknowledge other messages, and enables for the identification of duplicate messages.

message severity level

A property of a message indicating the level of impact of the event or notification that initiated the message. See also severity level.

metadata

Data that defines data.

metric

A measurement that defines a specific operational or performance characteristic.

Microsoft Management Console (MMC)

A Microsoft product that provides a software framework for the management of IT environments. Management products are added or "snapped into" the management console and thus extend the management capability of the Microsoft Management Console.

module

A self-contained software component that performs a specific type of task or provides for the presentation of a specific type of data. Modules can interact with one another and with other software.

node

When the context is network, a computer system or device (for example, printer, router, bridge) in a network. When the context is a graphical point to point layout, a graphical element in a drawing that acts as a junction or connection point for other graphical elements.

parameter

A variable or attribute that may be given an arbitrary value for use during an execution of either a computer program or a procedure within a program.

parameter type

An abstraction or categorization of a parameter that determines the particular kind of data that is valid for the parameter. For example a parameter type could be IP Address which indicates that parameter values must have 4 numbers separated by decimals with the value for each number being in the range of 0 to 255.

parameter value

A value that is given to a variable.

policy

A set of one or more specifications rules and other information that help automate network, system, service, and process management. Policies can be deployed to various targets (for

example, managed systems, devices, network interfaces) providing consistent, automated administration across the network.

Policy management

The process of controlling policies (for example, creating, editing, tracking, deploying, deleting) for the purposes of network, system or service management.

policy type

An abstraction or categorization of policies based on the function of the policy or the services that the policy supports.

port

If the context is hardware, a location for passing information into and out of a network device. If the context is ECS, a location for passing information into and out of a correlation node.

server

If the context is hardware plus software, a computer system that provides a service (for example, management capabilities, file storage capabilities) to other computer systems (clients) on the network. If the context is a software component, a program or executable process that responds to and services requests issued by clients.

severity level

A property of an object indicating the status of the object. Severity level is based on the impact of events or messages associated with the object.

SMART Plug-In (SPI)

Prepackaged software that installs into a management console and provides management capabilities specific to a given type of business application, database, operating system, or service.

trace log

An output file containing records of the execution of application software

Index

A

- actions, 123
 - customizing, 73
- Add Group action, 126
- adding
 - nodes to WebSphere SPI node group, 40
- Add Node action, 126
- ADDRESS property, 132
- ALIAS property, 132
- annotation reports, 88
- application server
 - verifying status, 38
- Application Servers tree item, 122
- Application Servers view, 129
- assigning operator responsibilities, 37
- automatic action reports, 88

C

- Cancel button, 123
- cell, 52
- Check WebSphere tool, 64
 - what it does, 65
- CODA
 - using, 56
- collecting
 - WebSphere login information, 38
- collection intervals
 - changing, 80
- collector policies, 71
- conditional properties
 - configuring, 47
 - requirements, 47
 - setting, 47
- configuration
 - properties, 130
 - structure, 119
 - syntax, 119

- Configuration Editor, 123
 - buttons, 123
 - tree, 121
- configuration editor, *see Discover or Configure WBSSPI tool*
- configuration example
 - different login information, 138
 - global defaults, 136
 - global login information, 138
 - group and node properties, 136
 - single node/two servers, 136
 - virtual IP addresses, 137
- configuration files
 - location, 117
- Configurations view, 129
- Configuration tree item, 122
- configuring, 37
 - conditional properties, 47
 - management server, 39
 - prerequisites, 37
 - remote systems, 85

- Config WBSSPI tool
 - Add Application Server action
 - Add Application Server action, 124
 - Add Group action, 126
 - Add Node action, 126
 - Application Servers tree item, 122
 - Application Servers view, 129
 - Cancel button, 123
 - Configurations view, 129
 - Configuration tree item, 122
 - Default Properties tree item, 122
 - Default Properties view, 129
 - Defaults tree item, 122
 - Defaults view, 129
 - Finish button, 123
 - Groups tree item, 122
 - Groups view, 129
 - modifying a property, 128
 - Next button, 123
 - Nodes tree item, 122
 - Nodes view, 129
 - Remove ALL App Servers action, 126
 - Remove ALL Groups action, 127
 - Remove ALL Nodes action, 127
 - Remove Application Server action, 126
 - Remove Group action, 127
 - Remove Node action, 127
 - removing a property, 129
 - Save button, 123
 - Set Configuration Properties tab, 128
 - setting a property, 128
 - View Current Configuration tab, 129
 - View Inherited Properties, 129
- creating
 - policy groups, 82
- customizing
 - Basic Policy Customizations, 72
 - creating new policies, 82
 - metrics, 20
 - policies, 75
 - thresholds for different servers, 81

D

- data collection, 13
- data interpretation, 16
- Default Properties tree item, 122
- Default Properties view, 129
- Defaults tree item, 122
- Defaults view, 129
- Deployment Manager, 52
- Deploy UDM tool, 67

- Discover or Configure WBSSPI tool, 61
 - using
 - what it does, 61
- discovery policy, 72
- discovery process
 - verifying, 44
- distributed network deployer scenario, 52
- distributing
 - policies, 45
- duration
 - customizing, 73

E

- error logs
 - location, 117
- error messages, 142 to 169

F

- files, locations on management server/managed
 - nodes, 102, 103
- Finish button, 123

G

- Gather MBean Data tool, 67
- global properties, 119
- GRAPH_URL property, 132
- graphs
 - HP Performance Manager, 91
- GROUP block, 119
- Groups tree item, 122
- Groups view, 129

H

- HOME property, 133
- HP Performance Agent, 91
 - using, 56
- HP Performance Manager
 - integrating with WebSphere SPI, 94

I

- Init Non-Root tool, 61
 - what it does, 61
- installing, 28
 - report package, 92
 - swinstall, 29

J

- JAVA_HOME property, 133
- JMB_JAVA_HOME property, 133
- JMX Metric Builder tool, 67

L

- license count, 90
- limitations
 - remote systems, 87
- logfile monitoring
 - remote systems, 86
- LOGFILE property, 133
- logfiles policies, 70
- LOGIN property, 133

M

- management server
 - configuring, 39
- MeasureWare
 - using, 56
- message policy, 72
- messages
 - message browser, 16
- message text
 - customizing, 73
- metrics
 - customizing, 20
 - data collected, 13
 - modifying collections in the collector policy, 76
- metrics policies, 71
- Metrics Reports tool group, 66
- modifying
 - collection intervals, 80
- modifying a property, 128
- monitoring log files, 101
- Monitor policies, 71

N

- NAME property, 133
- Next button, 123
- Node Agent, 52
- NODE block, 120
- Nodes tree item, 122
- Nodes view, 129
- NUM_SERVERS property, 133

P

- PASSWORD property, 133
- PMI
 - metrics generating WebSphere SPI Reports, 89
 - policy groups level, 72
- policies
 - collector, 71
- policies, 15
 - customizing, 72, 75
 - customizing actions, 73
 - customizing duration, 73
 - customizing message text, 73
 - customizing severity, 73
 - customizing thresholds, 73
 - discovery, 72
 - distributing, 45
 - logfiles, 70
 - message, 72
 - metrics, 71
 - monitor, 71
 - reinstalling, 87
 - WBSSPI-Messages, 72
- policy groups
 - creating, 82
 - creating with tag parameter, 82
 - PMI level, 72
 - WBSSPI Discovery, 72
 - WBSSPI-Logfiles, 70
 - WBSSPI-Metrics, 71
 - WBSSPI-Monitor, 71
- PORT property, 133
- prerequisites
 - configuring, 37
- properties, 130
 - global, 119
 - listed by WebSphere SPI requirements, 131
 - precedence, 120
 - server-specific, 120

R

- reinstalling
 - policies, 87
- remote systems, 83
 - configuring, 85
 - limitations, 87
 - logfile monitoring, 86
 - overview, 84
 - requirements, 83
- Remove ALL App Servers action, 126
- Remove ALL Groups action, 127

- Remove ALL Nodes action, 127
- Remove Application Server action, 126
- Remove Group action, 127
- Remove Node action, 127
- removing a property, 129
- Reporter
 - using, 92
- Reporter reports, 19
- Report package, 19
- report package
 - installing, 92, 115
- reports
 - annotation, 88
 - automatic action, 88
 - generated from alarms, 67
 - HP Performance Insight, 91
 - HP Reporter, 19
 - included, 19
 - Reporter, 91
 - tool bank, 89
 - Tool Bank generated, 66
- reports (automatic action)
 - how they are generated, 88
- requirements
 - remote systems, 83
- RMID_PORT property, 133
- RMID_START_TIME property, 134

S

- Save button, 123
- Self-Healing Info tool, 61
 - required setup, 62
 - what it does, 62
- server-specific properties, 120
- Set Access Info for Default Properties window, 43
- Set Configuration Properties tab, 128
- Set Configuration Settings tab
 - modifying a property, 128
 - removing a property, 129
 - setting a property, 128
- setting a property, 128
- severity
 - customizing, 73
- SPI Admin tool group, 60
- START_CMD property, 134
- Start Monitoring tool, 62
 - what it does, 63

- Start Tracing tool, 63
 - what it does, 63
- Start WebSphere tool, 65
 - what it does, 65
- STOP_CMD property, 134
- Stop Monitoring tool, 62
 - what it does, 63
- Stop Tracing tool, 63
 - what it does, 63
- Stop WebSphere tool
 - what it does, 65
- structure
 - configuration, 119
- swinstall, 29
- syntax
 - configuration, 119

T

- tag option
 - creating custom policy groups, 82
- thresholds
 - customizing, 73
 - settings for different servers, 81
- TIMEOUT property, 134
- Tool Bank
 - reports, 66
- tool bank
 - reports generated, 89
- tools, 15
 - Check WebSphere, 64
 - Deploy UDM, 67
 - Discover or Configure WBSSPI, 61
 - Gather MBean Data, 67
 - Init Non-Root, 61
 - JMX Metric Builder, 67
 - Self-Healing Info, 61
 - Start Monitoring, 62
 - Start Tracing, 63
 - Start WebSphere, 65
 - Stop Monitoring, 62
 - Stop Tracing, 63
 - UDM Graph Disable, 67
 - UDM Graph Enable tool, 67
 - Verify, 63
 - View Error File, 63
 - View Graphs, 64
 - View WebSphere Logs, 66
 - WBSSPI Reports group, 66

U

UDM_DEFINITIONS_FILE property, 135

UDM Graph Disable, 67

UDM Graph Enable, 67

unsupported platforms, 83

upgrading

 WebSphere SPI report package, 115

Use Case

 1, 53

 2, 53

 4, 54

user defined metrics

 graphing, 99

USER property, 135

using

 Discover or Configure WBSSPI tool

Using JMX Actions Command Parameters, 78

 Examples, 79

V

verifying

 application server status, 38

 discovery process, 44

Verify tool, 63

 what it does, 63

VERSION property, 135

View Configuration Settings tab

 View Inherited Properties, 129

View Current Configuration tab, 129

View Error File tool, 63

 what it does, 63

View Graphs tool, 64

 required setup, 64

View Inherited Properties, 129

View WebSphere Logs tool, 66

 what it does, 66

virtual IP addresses

 example configuration, 137

W

wasspi_ca command, 76

wasspi_wbs_ca command

 parameters, 76

 tag option, 82

WBSSPI Discovery policy group, 72

WBSSPI-Logfiles policy group, 70

WBSSPI-Messages policy, 72

WBSSPI-Metrics policy group, 71

WBSSPI-Monitor policy group, 71

WebSphere Admin tool group, 64

WebSphere login information

 collecting, 38

WebSphere SPI

 capabilities, 13

 components, 14

 overview, 16

WebSphere SPI node group

 adding nodes, 40

We appreciate your feedback!

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

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

Product name:

Document title:

Version number:

Feedback:

