HP Operations Smart Plug-in for IBM WebSphere Application Server

for HP Operations Manager for UNIX®

Software Version: 6.00

Configuration Guide

Document Release Date: February 2009

Software Release Date: October 2008

Legal Notices

Warranty

Restricted Rights Legend

Copyright Notices

Trademark Notices

Documentation Updates

This guide's title page 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

You can visit the HP Software Support Online web site at:

http://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 Support Online 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 HP Software 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 find more information about access levels, go to:

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

To register for an HP Passport ID, go to:

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

Contents

1 WebSphere SPI Concepts

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 otherwise unavailable to HPOM. For more information on HPOM, see *HP Operations for UNIX Concepts Guide*.

Introducing the WebSphere SPI

In conjunction with HPOM, the WebSphere SPI offers centralized tools that help you monitor and manage systems using WebSphere Server. From the HPOM console, you can apply performance and problem managing processes to monitor systems using the WebSphere Server. 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 Integrating HP Reporting and Graphing Products with the WebSphere SPI on page 81.

Smart Plug-in Data

The WebSphere SPI has several server-related metrics that gather data about 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 Server administrator, you can choose the metrics crucial to the operation of WebSphere Server by modifying the WebSphere SPI templates. The templates 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 automatically triggered or operator-initiated.

Functions of the WebSphere SPI

The WebSphere SPI messaging, reporting, and action-executing capabilities are based on the HPOM concept of templates. The settings within these templates define various conditions that may occur within the WebSphere 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 following functions described in the following sections:

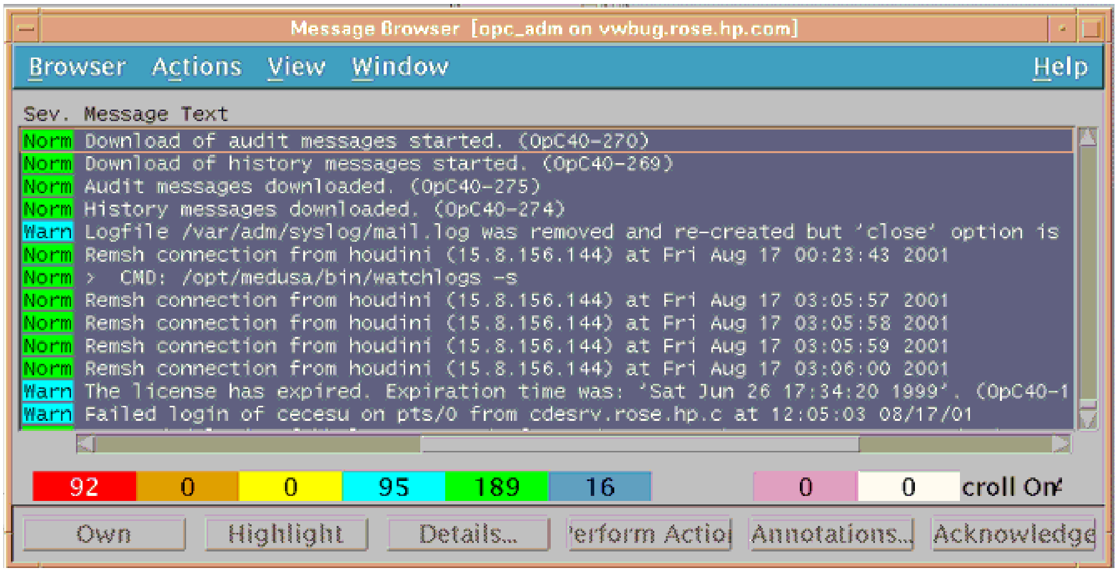
Collecting and Interpreting Server Performance and Availability Information

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

Displaying Information

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

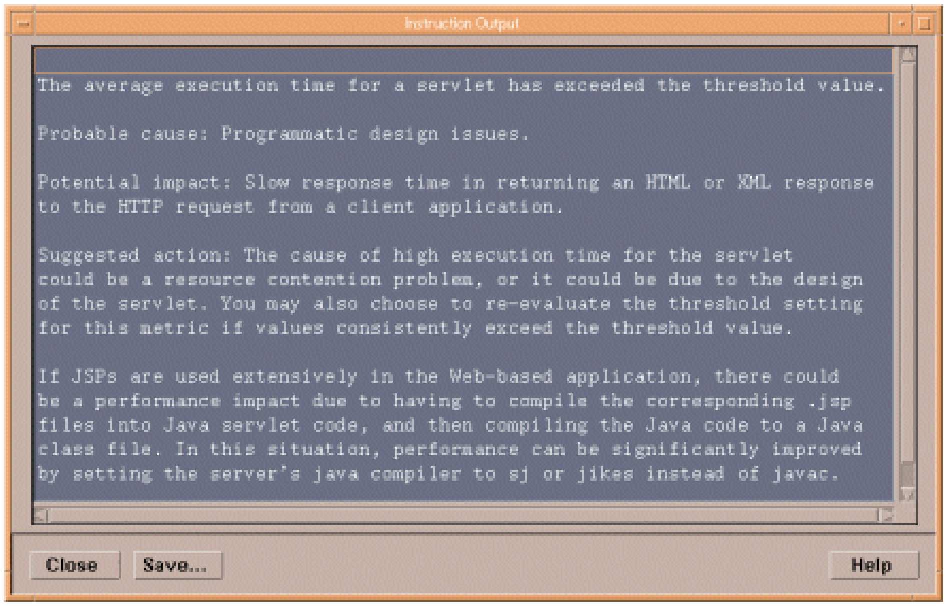
Messages in the Message Browser– HP Operations agent software compares the values gathered for WebSphere Server performance and availability against the monitor template settings related to those specific areas. The agent software then forwards appropriate messages to the HPOM console. These messages appear with color-coded severity levels in the HPOM message browser.



```
Sev. Message Text
Norm Download of audit messages started. (OpC40-270)
Norm Download of history messages started. (OpC40-269)
Norm Audit messages downloaded. (OpC40-275)
Norm History messages downloaded. (OpC40-274)
Warn Logfile /var/adm/syslog/mail.log was removed and re-created but 'close' option is
Norm Remsh connection from houdini (15.8.156.144) at Fri Aug 17 00:23:43 2001
Norm >  CMD: /opt/medusa/bin/watchlogs -s
Norm Remsh connection from houdini (15.8.156.144) at Fri Aug 17 03:05:57 2001
Norm Remsh connection from houdini (15.8.156.144) at Fri Aug 17 03:05:58 2001
Norm Remsh connection from houdini (15.8.156.144) at Fri Aug 17 03:05:59 2001
Norm Remsh connection from houdini (15.8.156.144) at Fri Aug 17 03:06:00 2001
Warn The license has expired. Expiration time was: 'Sat Jun 26 17:34:20 1999'. (OpC40-1
Warn Failed login of cecesu on pts/0 from cdesrv.rose.hp.c at 12:05:03 08/17/01
```

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 usually present in the message details. Instruction text is also available in the *HP Operations Smart Plug-in for BEA WebSphere Server SPI Reference Guide*..



```
The average execution time for a servlet has exceeded the threshold value.

Probable cause: Programmatic design issues.

Potential impact: Slow response time in returning an HTML or XML response
to the HTTP request from a client application.

Suggested action: The cause of high execution time for the servlet
could be a resource contention problem, or it could be due to the design
of the servlet. You may also choose to re-evaluate the threshold setting
for this metric if values consistently exceed the threshold value.

If JSPs are used extensively in the Web-based application, there could
be a performance impact due to having to compile the corresponding .jsp
files into Java servlet code, and then compiling the Java code to a Java
class file. In this situation, performance can be significantly improved
by setting the server's java compiler to sj or jikes instead of javac.
```

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 Server instance. If a report is available, you can find it within the Annotations area of the Message Details.

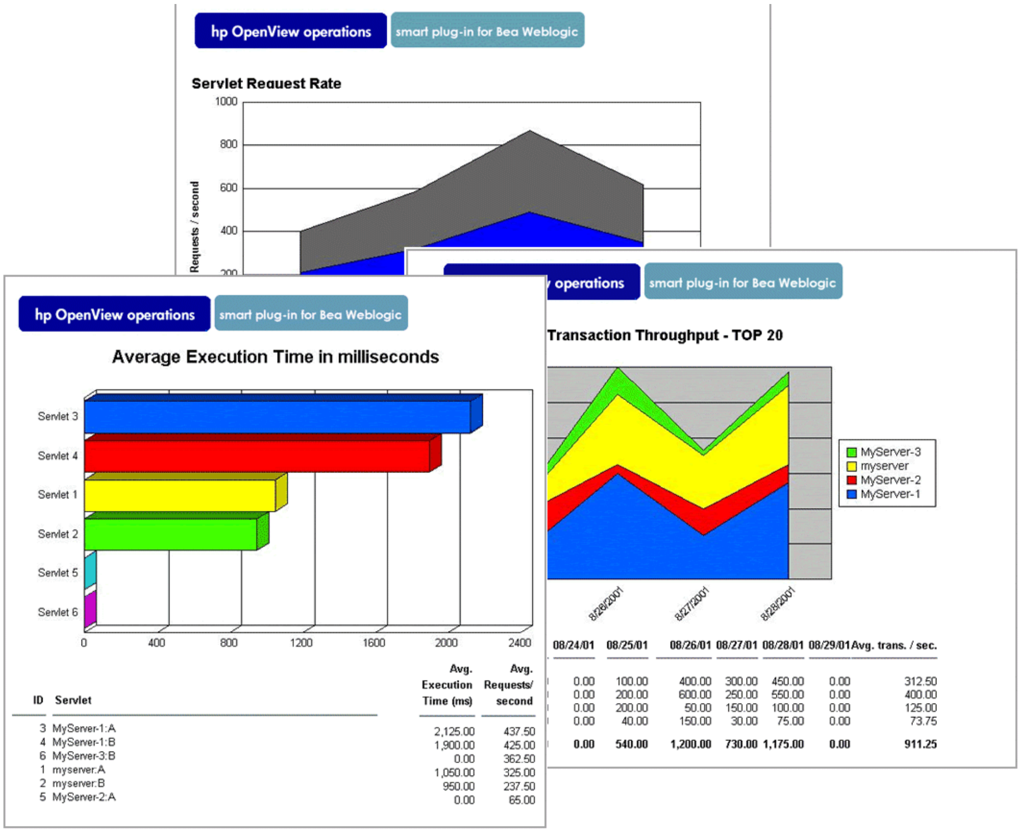
Generating Reports Using HP Reporter

You can integrate the WebSphere SPI with HP Reporter to provide you with management-ready, web-based reports. The WebSphere SPI Report package includes the templates 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 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.

.



ID	Servlet	Avg. Execution Time (ms)	Avg. Requests/ second
3	MyServer-1:A	2,125.00	437.50
4	MyServer-1:B	1,900.00	425.00
6	MyServer-3:B	0.00	362.50
1	myserver:A	1,050.00	325.00
2	myserver:B	950.00	237.50
5	MyServer-2:A	0.00	65.00

08/24/01	08/25/01	08/26/01	08/27/01	08/28/01	08/29/01	Avg. trans. / sec.
0.00	100.00	400.00	300.00	450.00	0.00	312.50
0.00	200.00	600.00	250.00	550.00	0.00	400.00
0.00	200.00	50.00	150.00	100.00	0.00	125.00
0.00	40.00	150.00	30.00	75.00	0.00	73.75
0.00	**540.00**	**1,200.00**	**730.00**	**1,175.00**	**0.00**	**911.25**

Graphing Data with HP Performance Manager

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

You can integrate the WebSphere SPI with HP Performance Manager to generate and view graphs. (use the **View Graphs** application from the WBSSPI Admin applications 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 in the message browser and in the message details (you can access details by either double-clicking the message or clicking **Details...**in the message browser) in the message browser. 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 Templates and Metrics

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

- Modify the default templates - Within a template, 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 template groups– You can create custom template groups using default templates as base. For more information, see Chapter 4, Customizing the WebSphere SPI Templates.
- Create custom metrics– You can define your own metrics or User Defined Metrics (UDMs) to expand the monitoring capabilities of the WebSphere SPI. For more information about UDMs see the *HP Operations Smart Plug-in for User Defined Metrics User Guide*.

WebSphere SPI Components

The WebSphere SPI has two main components:

- Applications (including reports)
- Templates

You can use the applications and templates 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 applications or message details) provide information about the conditions present in the servers running on specific managed nodes.

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

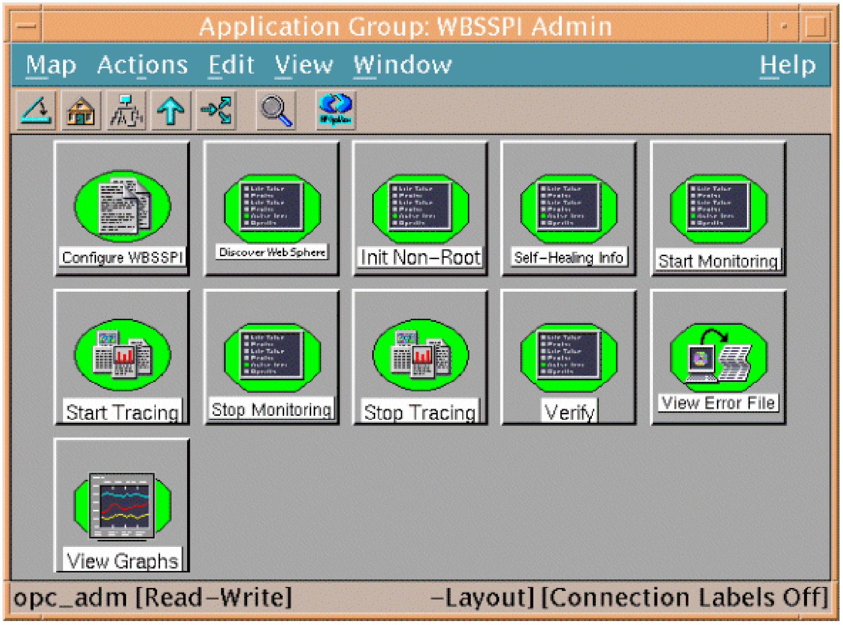
Applications

The WebSphere SPI applications include configuration, troubleshooting, and report-generating utilities. In the Application Bank window, the WebSphere SPI applications are divided into the following groups:

- WBSSPI Admin
- WebSphere
- WBSSPI Reports
- JMX Metric Builder: This application group is available *only if* you install the SPIJMB software bundle.

WBSSPI Admin Applications Group

WBSSPI Admin applications enable you to configure, control, and troubleshoot the WebSphere SPI. You require **`root`** user permission to run WBSSPI Admin applications.



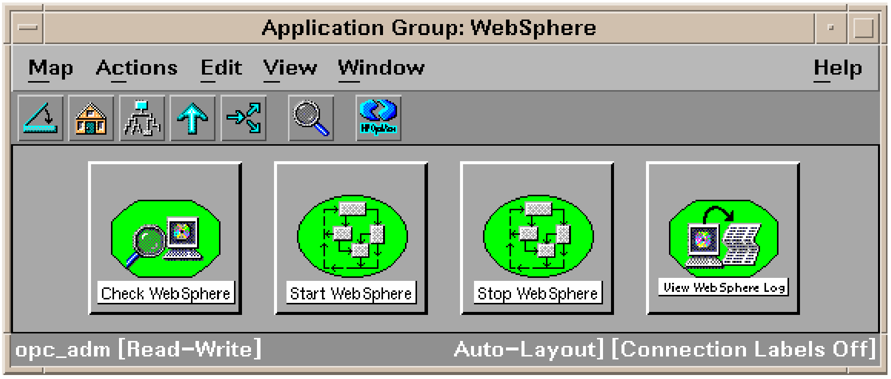
The WBSSPI Admin group contains the following applications (for more information, see Appendix C, Applications):

- **Configure WBSSPI**– Launches the configuration editor and maintains the WebSphere SPI configuration.
- **Discover WebSphere**– Sets basic configuration properties needed for discovery.
- **Init Non-Root**– Simplifies the configuration of a non-root HTTPS agent on a UNIX managed node (OVO for UNIX 8.x only). For all the steps necessary to configure a non-root HTTPS agent on a UNIX managed node, see Configuring a Non-Root HTTPS Agent on a UNIX Managed Node (OVO for UNIX 8.x Only) on page 53.
- **Self-Healing Info**– Collects data that you can send to your HP support representative.
- **Start Monitoring**– Starts the collection of metrics for one application server or all application servers on a managed node. Launch the Verify application to determine if monitoring is started or stopped. By default, monitoring is on.
- **Stop Monitoring**– Stops the collection of metrics for one application server or all application servers on a managed node.
- **Start Tracing**– Starts the collection of tracing information for selected metrics. Launch this application only when instructed by your HP support representative.
- **Stop Tracing**– Stops tracing of the collections of metrics into a file. Run this application only when instructed by your HP support representative.
- **Verify**– Verifies that the WebSphere SPI is properly installed on the server or managed node.
- **View Error File**– Enables you to view the contents of the WebSphere SPI error log file.
- **View Graphs**– Enables you to view the WebSphere SPI graphs, generated by HP Performance Manager, in a web browser (This requires additional setup. For more information see Task 1: Configure the Management Server to Launch Your Web Browser on page 37.

WebSphere Application Group

You can manage WebSphere Server functions by using the applications in the WebSphere Applications group.

To access the WebSphere applications double-click **WBSSPI** → **WebSphere** in the Application Bank window.



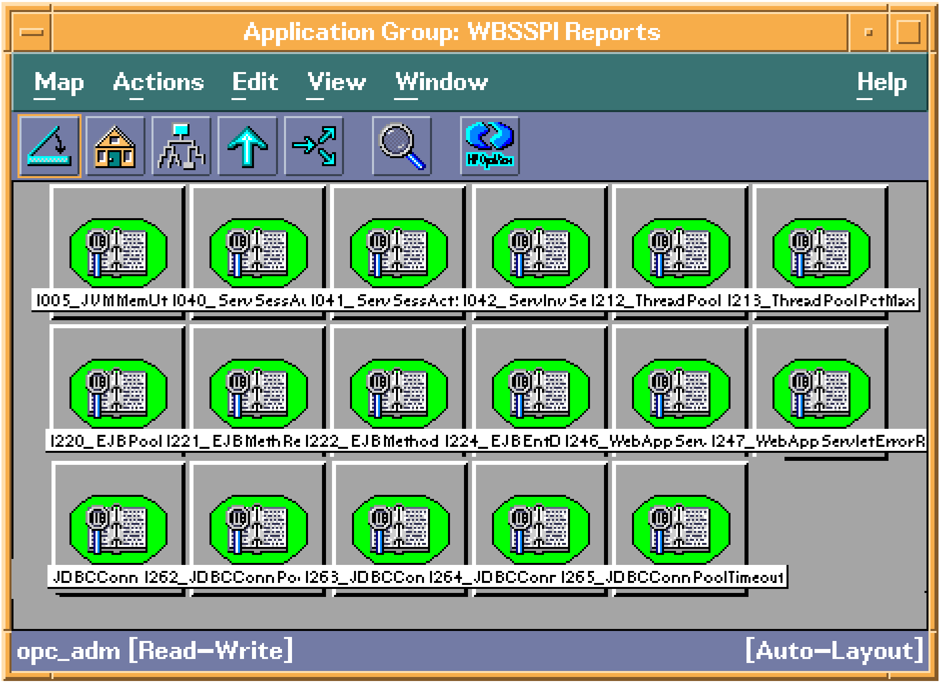
The WebSphere group contains the following applications:

- **Check WebSphere**– Does an interactive status check of selected WebSphere Application Servers.
- **Start WebSphere**– Enables you to start one or all WebSphere Application Servers from the HPOM console (requires setup).
- **Stop WebSphere**– Enables you to stop the WebSphere Application Servers from the HPOM console (requires setup).
- **View WebSphere Logs**– Enables you to view the WebSphereApplication Server log files.

WBSSPI Reports

The WBSSPI Reports 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 by dragging the node to a report in the Application Bank window. 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.



Application 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 section of a message.

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 Applications

The JMX Metric Builder Applications group contains the following applications::

- **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 application 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 Applications group and steps to install the SPIJMB software bundle, see the *HP Operations Smart Plug-in for User Defined Metrics User Guide*.

WebSphere SPI Templates

The SPI for WebSphere template group contains templates grouped into three broad categories:

- WBSSPI-Templates-High Impact
- WBSSPI-Templates-Medium Impact
- WBSSPI-Templates-Low Impact

These are based on the impact that their data collections 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 metric (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 calculations required for the collected data generally require 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, the following template groups are included: SPI for WebSphere template group contains the following template groups and individual templates:

- **WBSSPI-Logfiles** – Contains templates that generate messages based on log file and error text detected in both the WebSphere Server log files and in the WebSphere SPI log files. The information captured from these log files includes errors that occur in the operation of the WebSphere Server or the WebSphere SPI and changes to WebSphere Server configuration.
- **WBSSPI-Metrics** – Contains metric templates that monitor the performance levels and availability of a WebSphere Server.

  Each metric template 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 instructions that appear.

- **WBSSPI-Schedule** – Contains collector templates that specify the collection interval of metric templates. Within the name of each collector template is its collection interval. For example, the collection interval of template WBSSPI-40-High-1h is one hour (where 1h represents one hour). Each collector template is assigned a collection interval of 5 minutes, 15 minutes, or one hour.

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

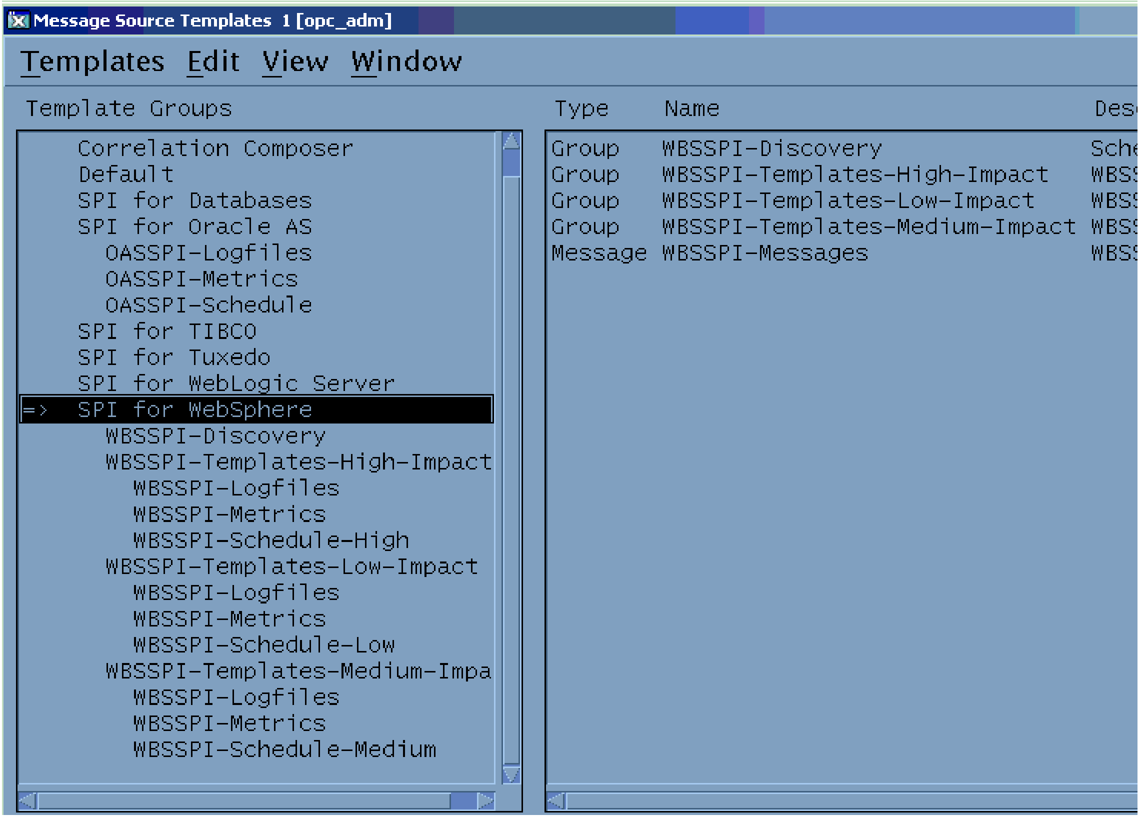
  Each collector template controls when and what metrics are collected. Specifically, the collector template does the following:

  — Runs the collector/analyzer at each collection interval

  — Specifies which metrics are collected

The SPI for WebSphere template group also contains the following individual templates:

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



```
Template Groups
    Correlation Composer
    Default
    SPI for Databases
    SPI for Oracle AS
      OASSPI-Logfiles
      OASSPI-Metrics
      OASSPI-Schedule
    SPI for TIBCO
    SPI for Tuxedo
    SPI for WebLogic Server
=>  SPI for WebSphere
      WBSSPI-Discovery
      WBSSPI-Templates-High-Impact
        WBSSPI-Logfiles
        WBSSPI-Metrics
        WBSSPI-Schedule-High
      WBSSPI-Templates-Low-Impact
        WBSSPI-Logfiles
        WBSSPI-Metrics
        WBSSPI-Schedule-Low
      WBSSPI-Templates-Medium-Impa
        WBSSPI-Logfiles
        WBSSPI-Metrics
        WBSSPI-Schedule-Medium
```

Type	Name	Des
Group	WBSSPI-Discovery	Sche
Group	WBSSPI-Templates-High-Impact	WBSS
Group	WBSSPI-Templates-Low-Impact	WBSS
Group	WBSSPI-Templates-Medium-Impact	WBSS
Message	WBSSPI-Messages	WBSS

WebSphere Template Groups and System PMI Levels

When you deploy a template group on a managed node, the PMI level of the node is automatically adjusted to that of the template group. For example, deploying the WebSphere High Impact template group on a node would result in a PMI setting of “high” for the node.

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

2 Installing, Upgrading, and Removing the WebSphere SPI

Installing the WebSphere SPI

The HPOM management server and discovery package must be installed before you can install 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.

For a complete list of software requirements, see the *HP Smart Plug-in for WebSphere Application Server Release Notes*.

➤ The instructions that follow cover a command line swinstall installation. For HP-UX systems, you can also use the graphical user interface (GUI).

➤ If you are going 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 User Defined Metrics User Guide*.

For an HP-UX 11.23 and 11.31 (PA and IA) management server, type:

```
swinstall -s /cdrom/OV_DEPOT/11.0HPUX.depot WBSSPI
```

On a Solaris management server the packages are supported in both depot and solaris native format.

For a Solaris management server in depot format, type:

```
swinstall -s /cdrom/OV_DEPOT/SOLARIS.depot WBSSPI
```

For a Solaris management server in native format, perform the folowing steps:

1. Before installing the SPI software on the Solaris management server, set **PKG_NONABI_SYMLINKS** to **true** to avoid breakage of existing links during the installation. Type:

   ```
   PKG_NONABI_SYMLINKS=TRUE
   export PKG_NONABI_SYMLINKS
   ```

2. The SPIs have dependencies on “DSI2DDF” and “SPI-SVCDISC-OVO”. These two packages are not available in the native format of solaris. Hence, install “DSI2DDF” and “SPI-SVCDISC-OVO” from SOLARIS.depot before installing from the HPOMSpiDVD-8.1.sparc package.

3. To install from the HPOMSpiDVD-8.1.sparc, type:

   ```
   pkgadd -d /cdrom/OV_DEPOT/HPOMSpiDVD-8.1.sparc
   ```

4. Select the following SPIs for installation:

   - HPOvSpiWbs

- HPOvSpiJmx
- HPOvSpiShs

Removing the WebSphere SPI

Completely removing the WebSphere SPI installation deletes all WebSphere SPI components.

To remove the WebSphere SPI, complete the tasks in the following order:

- Task 1: Remove the WebSphere SPI Software from the Management Server
- Task 2: Remove WebSphere SPI Software from the Node Group and Managed Nodes
- Task 3: Delete WebSphere SPI Templates and Template Groups
- Task 4: Delete WebSphere SPI Applications
- Task 5: Delete the WebSphere SPI Message and Node Groups
- Task 6: Remove the WebSphere SPI Directory
- Task 7: Remove the Report Package (Optional)
- Task 8: Remove the Graph Package (Optional)

Task 1: Remove the WebSphere SPI Software from the Management Server

1. Open a terminal window and log on as root.
2. In the terminal window:
   - For an HP-UX 11.23 and 11.31 (PA and IA) management server, type:

     ```
     /usr/sbin/swremove WBSSPIor
     /usr/sbin/swremove SPIWebSphereAll
     ```

   - For a Solaris management server, type:

     ```
     /usr/sbin/pkgrm HPOvSpiWbs
     /usr/sbin/swremove DSI2DDF
     /usr/sbin/swremove SPI-SVCDISC-OVO
     ```

The **swremove** or **pkgrm** command removes the files from the file system only. The WebSphere SPI templates are still in the HPOM data repository and must be deleted manually. Before the templates can be deleted, they (and the WebSphere SPI software) must be de-assigned from the managed nodes.

Task 2: Remove WebSphere SPI Software from the Node Group and Managed Nodes

1. Open the Node Bank and, from the Actions menu, select **Agents → Assign Templates**.
2. Select the WebSphere node group and all managed nodes to which WebSphere templates were assigned.
3. Press the **Remove nodes/groups** button.
4. Open the Node Group Bank and select the WebSphere node groups.
5. From the Action menu click **Install/Update SW & Config** and select the following check boxes:
   - Templates
   - Actions
   - Monitors
   - Commands
6. Select the **Nodes in List** option button.
7. Select the **Force Update** option button.
8. Click **OK** to remove the Templates, Actions, Commands, and Monitors from the managed nodes. The following message is displayed in the message browser:

   ```
   The following configuration information was successfully distributed:
   Templates Actions Commands Monitors
   ```

Task 3: Delete WebSphere SPI Templates and Template Groups

Starting from the SPI for WebSphere template group, delete all templates and template groups. Once these templates and template groups are deleted, delete the SPI for WebSphere template group.

1 Open the Message Source Templates window and double-click the **SPI for WebSphere** template group.

2 Press **SHIFT+Click** to select all templates and template groups in the SPI for WebSphere template group.

3 Click **Delete from All...**.

4 Click **Yes** in response to the message:

```
Do you really want to delete the template(s)?
```

5 If additional WebSphere SPI templates or template groups are in the SPI for WebSphere template group, repeat steps 2 through 4 until you have deleted all WebSphere SPI templates and template groups from the SPI for WebSphere template group.

6 Go up one level and delete the SPI for WebSphere template group.

If you customized templates (copies of WebSphere SPI default templates) residing in other HPOM template groups, remove them.

Task 4: Delete WebSphere SPI Applications

Unlike templates, applications can all be removed in a single step.

1 Open the Application Bank.

2 Right-click the WBSSPI application group and click **Delete**.

3 Click **Yes** in response to the following message:

```
Do you really want to delete the application group?
```

Task 5: Delete the WebSphere SPI Message and Node Groups

1 From the Window menu select **Message Group Bank**.

2 In the Message Group Bank window right-click the **WBSSPI** group and click **Delete**.

3 Repeat for the **WebSphere** group.

4 From the Window menu select **Node Group Bank**.

5 In the Node Group Bank window right-click the WebSphere (High, Low, and Medium) node group and click **Delete**.

Task 6: Remove the WebSphere SPI Directory

1 From a command line, remove the WebSphere SPI directory by entering:

```
rm -rf /var/opt/OV/wasspi/wbs
```

Task 7: Remove the Report Package (Optional)

If you installed the WebSphere SPI report package (on your Windows system running HP Reporter), remove it:

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

Task 8: 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, follow these steps:

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**.

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 Task 1: Remove the WebSphere SPI Software from the Management Server on page 27):

1. Verify that the graph package is installed. Type **`swlist | grep WBSSPI-GRAPHS`**
2. 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 Task 1: Remove the WebSphere SPI Software from the Management Server on page 27):

1. Verify that the graph package is installed. Type **`/usr/bin/pkginfo HPOvSpiWbsGc`**
2. Type **`/usr/sbin/pkgrm HPOvSpiWbsGc`**

Upgrading the WebSphere SPI

When you upgrade from a previous installation, all your configuration entries are preserved.

To upgrade the WebSphere SPI, follow these steps:

- Task 1: Remove WebSphere SPI Software from the Management Server
- Task 2: Delete WebSphere SPI Templates
- Task 3: Delete WebSphere SPI Applications
- Task 4: Upgrade the Management Server
- Task 5: Assign Operator Responsibilities
- Task 6: Assign Templates
- Task 7: Distribute Templates

- Task 8: Customize Templates
- Task 9: Update WebSphere Log Template
- Task 10: Move Nodes to New Node Group
- Task 11: Delete Node Groups
- Task 12: Distribute Actions, Monitors, Commands, and Templates on page 34
- Task 13: Run the Discover WebSphere Application
- Task 14: Install the New Report Package (Optional)
- Task 15: Install the New Graph Package (Optional)
- Task 16: Configure a Non-Root Agent on a UNIX Managed Node (Optional)

Task 1: Remove WebSphere SPI Software from the Management Server

1. Open a terminal window and log on as root.
2. In the terminal window:
   - For an HP-UX 11.23 and 11.31 (PA and IA) management server, type:

     ```
     /usr/sbin/swremove WBSSPI
     /usr/sbin/swremove WBSSPI-GRAPHS
     ```

   - For a Solaris management server in depot format, type:

     ```
     /usr/sbin/swremove WBSSPI
     /usr/sbin/swremove WBSSPI-GRAPHS
     ```

   - For a Solaris management server in native format, type:

     ```
     /usr/sbin/pkgrm HPOvSpiWbs
     ```

Task 2: Delete WebSphere SPI Templates

Delete all WebSphere SPI templates and template groups that appear under the SPI for WebSphere template group and the SPI for WebSphere template group itself. If you customized any of the default templates, note these changes (these customizations are not saved).

1. Open the Message Source Templates window and double-click the **SPI for WebSphere** template group
2. Press **SHIFT+Click** to select all templates and template groups in the SPI for WebSphere template group.
3. Click the **Delete from All...** button.
4. Click **YES** in response to the message:

   ```
   Do you really want to delete the template(s)?
   ```

5. Repeat steps 2 through 4 until you have deleted all WebSphere SPI templates and template groups from the SPI for WebSphere template group.
6. Go up one level and delete the SPI for WebSphere template group.

If you customized templates (copies of WebSphere SPI default templates) residing in other HPOM template groups, remove them.

Task 3: Delete WebSphere SPI Applications

Unlike templates, all WebSphere SPI applications can be removed in a single step.

1 Open the Application Bank.

2 Right-click the WBSSPI application group and click **Delete**.

3 Click **Yes** in response to the following message:

```
Do you really want to delete the application group?
```

Task 4: Upgrade the Management Server

The WebSphere SPI software is available on the HP Operations Smart Plug-ins DVD.

The following instructions that follow show the command line usage of swinstall. For HP-UX systems, you can also use the graphical user interface (GUI).

For an HP-UX 11.23 and 11.31 (PA and IA) management server, type:

```
swinstall -s /cdrom/OV_DEPOT/11.0HPUX.depot WBSSPI
```

On a Solaris management server the packages are supported in both depot and solaris native format.

For a Solaris management server in depot format, type:

```
swinstall -s /cdrom/OV_DEPOT/SOLARIS.depot WBSSPI
```

For a Solaris management server in native format, perform the folowing steps:

1 Before upgrading the SPI software on the Solaris management server, set **PKG_NONABI_SYMLINKS** to **true** to avoid breakage of existing links during the installation. Type:

```
PKG_NONABI_SYMLINKS=TRUE
export PKG_NONABI_SYMLINKS
```

2 The SPIs have dependencies on “DSI2DDF” and “SPI-SVCDISC-OVO”. These two packages are not available in the native format of solaris. Hence, install “DSI2DDF” and “SPI-SVCDISC-OVO” from SOLARIS.depot before installing from the HPOMSpiDVD-8.1.sparc package.

3 To install from the HPOMSpiDVD-8.1.sparc, type:

```
pkgadd -d /cdrom/OV_DEPOT/HPOMSpiDVD-8.1.sparc
```

4 Select the following SPIs for upgrading:

- HPOvSpiWbs
- HPOvSpiJmx
- HPOvSpiShs

Task 5: Assign Operator Responsibilities

1 Log on to HPOM as administrator (**opc_adm**).

2 Open the User Bank window, right-click the opc_adm user, and click **Modify**.

3 Click **Responsibilities** in the Modify User:opc_adm user window.

4 For WBSSPI and WebSphere Message Groups, ensure all check boxes are selected.

5 Assign the WBSSPI Node or Message Groups to any other appropriate operators.

6 Click **Close**.

Task 6: Assign Templates

Assign the WBSSPI-Discovery and WBSSPI-Messages templates to the management server:

1 Open the Node Bank window and highlight the management server.

2 From the Actions menu, select **Agents** → **Assign Templates**. The Define Configuration window opens.

3 Click **Add**. The Add Configuration window opens.

4 Click **Open Template Window**. The Message Source Templates window opens.

5 From the Message Source Templates window, in the Template Groups pane, select the **SPI for WebSphere** template group.

6 From the Message Source Templates window, in the right pane, select the **WBSSPI-Discovery** and **WBSSPI-Messages** templates.

7 From the Add Configuration window, click **Get Template Selections**. The WBSSPI-Messages and WBSSPI-Discovery templates appear in the right pane.

8 From the Add Configuration window, click **OK**.

Task 7: Distribute Templates

Distribute the WBSSPI-Discovery and WBSSPI-Messages templates to the management server:

1 Open the Node Bank window and highlight the management server.

2 From the Actions menu, select **Agents** → **Install/Update SW & Config**.

3 In the Target Nodes section, select **Nodes in List Requiring Update**.

4 In the Install/Update Software and Configuration window check the **Templates** check box.

5 Select **Force Update**.

6 Click **OK**.

The following message is displayed in the message browser:

```
The following configuration information was successfully distributed:
Templates
```

The WBSSPI-Discovery and WBSSPI-Messages templates are distributed to the management server.

Task 8: Customize Templates

If you noted any customizations in Task 2: Delete WebSphere SPI Templates on page 30, make a copy of the default templates, and then make these same customizations to the copies. In this version of the WebSphere SPI, the templates are no longer grouped by WebSphere version numbers.

Task 9: Update WebSphere Log Template

Update the audit, deprecated, and informational suppress conditions for the WebSphere Log Template:

1 From the Message Source Templates window, open the SPI for WebSphere template group.

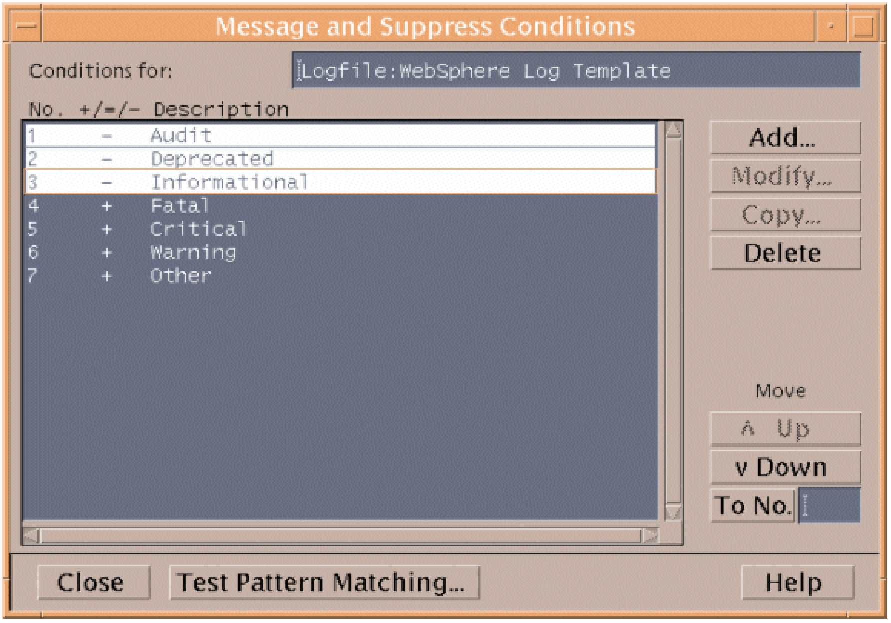
2 Select a WBSSPI-Templates impact group (High, Low, and Medium) and follow these steps:

  a Open the impact group.

  b Open the WBSSPI-Logfiles group.

  c Select the WebSphere Log Template and click **Conditions**.

  d Move the Audit, Deprecated, and Informational conditions to the top of the list.



Conditions for: Logfile:WebSphere Log Template

No.	+/=/-	Description
1	-	Audit
2	-	Deprecated
3	-	Informational
4	+	Fatal
5	+	Critical
6	+	Warning
7	+	Other

  e Click **Close**.

Task 10: Move Nodes to New Node Group

Move all managed nodes that are in the SPI for WebSphere node groups to the new WebSphere node group.

1 Open the Node Bank and select the **SPI for WebSphere** node group.

2 Double-click each subgroup in the **WebSphere 4.0** node group and note the managed nodes in it.

3 Go back to the top level of the node bank (where the WebSphere node group is displayed).

4 Drag and drop, or copy and paste, the nodes (noted in step 2) from the IP submap to the appropriate **WebSphere** node group.

Task 11: Delete Node Groups

Delete all versioned node groups that are in the SPI for WebSphere node group (WebSphere 4.0).

1 Open the Node Bank and select the **SPI for WebSphere** node group.

2 Select the **WebSphere 4.0** and, from the Edit menu, click **Delete**.

3 Click **Yes** in response to the following message:

```
Do you really want to delete the node group?
```

Task 12: Distribute Actions, Monitors, Commands, and Templates

1 At the HPOM console, in the Node Bank window, select the nodes or node group on which to install the WebSphere SPI.

2 From the Node Bank's Actions menu select **Agents** → **Install/Update SW & Config**.

3 In the Install/Update HPOM Software and Configuration window select the following component check boxes:

- Templates
- Actions
- Monitors
- Commands

Using this dialog, deploy updated components to the managed nodes.

4 Check the Force Update check box.

5 Select the Nodes in list button. Upon completion, the following message and appears in the message browser for each managed node:

```
The following configuration information was successfully distributed:
Actions Commands Monitors Templates.
```

➤ You might see some WebSphere SPI errors in the message browser which you can ignore (these errors are the result of the transition to the updated programs). WebSphere SPI templates/programs are updated on the Management Server and selected managed nodes. These errors are resolved when the upgrade is complete.

Task 13: Run the Discover WebSphere Application

You must run the Discover WebSphere application but there is no need to re-enter any of the WebSphere SPI configuration data (all configuration data is preserved). To re-deploy the file, you can drag and drop multiple nodes, node groups, or single nodes. When you re-deploy the file, relevant information is updated, transmitted, and stored on the node.

1 At the HPOM console, select the nodes in the Node Bank window.

2 From the Window menu, select **Application Bank**.

3 In the Application Bank window select **WBSSPI** → **WBSSPI Admin** → **Discover WebSphere**. (If the items do not appear, select **Map** → **Reload**.). The Introduction window opens.

4 Click **Next**. A second Introduction window opens. This window displays information about which properties might be required in order for the discovery process to work.

5 Read this information and click **Next**.

6 Modify the configuration using configuration editor.

➤ If you set the GRAPH_SERVER property, note that this property is no longer supported in the WebSphere SPI. Instead, set the GRAPH_URL property.

➤ If you set the UDM_DEFINITIONS_FILE property, note that this property is not to be supported in future versions of the WebSphere SPI. Note the locations of the UDM files on your managed nodes and delete any occurrence of the UDM_DEFINITIONS_FILE property from your configuration.

If you individually configured UDMs on your managed nodes, you must configure these UDMs on the management server in the `/opt/OV/wasspi/wbs/conf/wasspi_wbs_udmDefnintions.xml` file (or, set the UDM_DEFINITIONS_SOURCE property to use another file).

Once you have consolidated your UDMs on the management server, delete your old UDM files from the managed nodes and distribute the new UDM file to the managed nodes using the Deploy UDM application.

7 Click **Next** to save any changes and exit the editor.

8 The Confirm Operation window opens. 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 in the Node Bank window, start the Discover WebSphere application, click **Next** from the configuration editor, and then click **OK**.

➤ Do not close the Discover WebSphere application window until the discovery process completes. The discovery process might take several minutes to complete.

Task 14: 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 Highlight 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 83.

Your upgrade is now complete.

Task 15: 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, follow these steps:

1. From the Control Panel, double-click the **Add/Remove Programs** icon.
2. Highlight 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 87.

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. Type **`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 87.

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. Type **`/usr/bin/pkginfo HPOvSpiWbsGc`**
2. Type **`/usr/sbin/pkgrm HPOvSpiWbsGc`**
3. Follow the steps to install the WebSphere SPI graph package in Integrating with HP Performance Manager on page 87.

Your upgrade is now complete.

Task 16: Configure a Non-Root Agent on a UNIX Managed Node (Optional)

If you are running or planning to run a non-root HTTPS agent on a UNIX managed node, see Configuring a Non-Root HTTPS Agent on a UNIX Managed Node (OVO for UNIX 8.x Only) on page 53.

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.

Configuration Prerequisites

On the HPOM management server, complete the following tasks before configuring WebSphere SPI:

- Task 1: Configure the Management Server to Launch Your Web Browser
- Task 2: Assign Operator Responsibilities for opc_adm
- Task 3: Assign Templates
- Task 4: Distribute Templates

Task 1: Configure the Management Server to Launch Your Web Browser

The WebSphere SPI uses the ovweb utility to start your web browser for displaying graphed metrics (which requires HP Performance Manager). If you do not use HP Performance Manager, skip this task.

1 Enter the browser invocation command in the `ovweb.conf` file. If no browser invocation command is included in the `ovweb.conf` file, ovweb tries to start the default browser.

➤ `ovweb.conf` file must be located in the directory specified by the environment variable `$OV_CONF` (used by HPOM). To find the HPOM directory structure on your management server, open the `/opt/OV/bin/ov.envvars.sh` file and look for the `$OV_CONF` definition.

The browser invocation command must contain a `%s` to allow WebSphere SPI to pass a URL to the browser. Open the file and insert the command according to the entry syntax and example as follows:

Syntax: `Browser:` *<browser command>* `%s`
Check the web browser setting. To display the WebSphere SPI graphs, ensure that your browser is JavaScript enabled. Check the setting within the browser's Preferences.

2 In Task 3: Launch Discover WebSphere on page 47, if you are using HP Performance Manager, set the GRAPH_URL property.

For more information about launching a browser in HPOM, consult the man pages for `ovweb`, `ovweb.conf`, and `ov.envvars`. To access instructions for enabling graph displays, at a command prompt enter: **`man ovweb`**

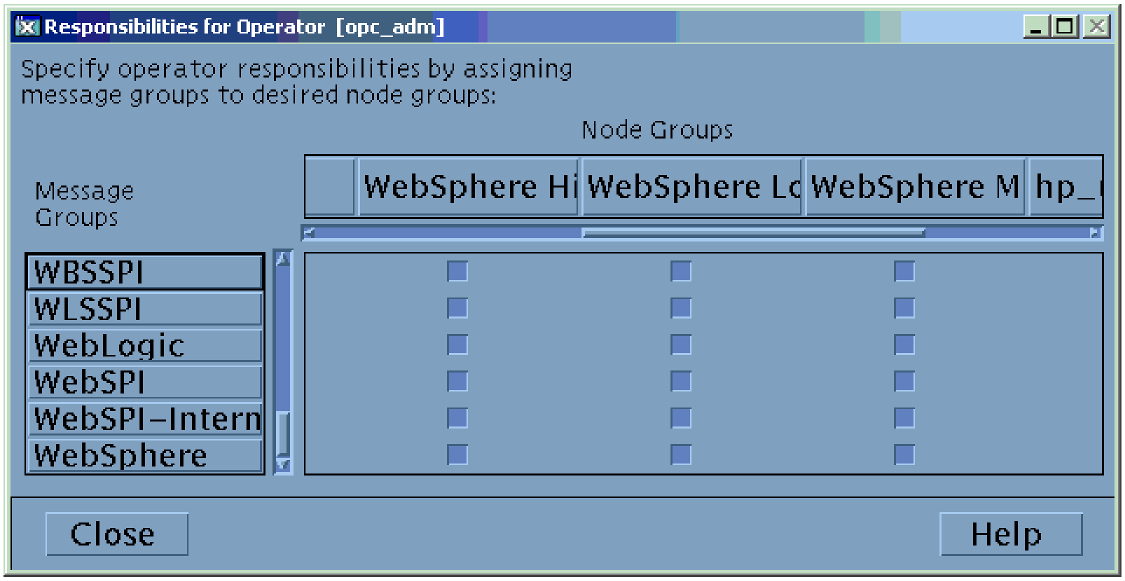
Task 2: Assign Operator Responsibilities for opc_adm

1 Log on to HPOM as administrator (**`opc_adm`**).

2 Open the User Bank window, right-click the opc_adm user, and select **Modify**.

3 Click **Responsibilities** in the Modify User:opc_adm user window.

4 For WBSSPI and WebSphere Message Groups, ensure all boxes are checked.



Specify operator responsibilities by assigning message groups to desired node groups:

Message Groups \ Node Groups	WebSphere Hi	WebSphere Lc	WebSphere M	hp_
WBSSPI	□	□	□	
WLSSPI	□	□	□	
WebLogic	□	□	□	
WebSPI	□	□	□	
WebSPI–Intern	□	□	□	
WebSphere	□	□	□	

5 Assign the WBSSPI Node or Message Groups to any other appropriate operators.

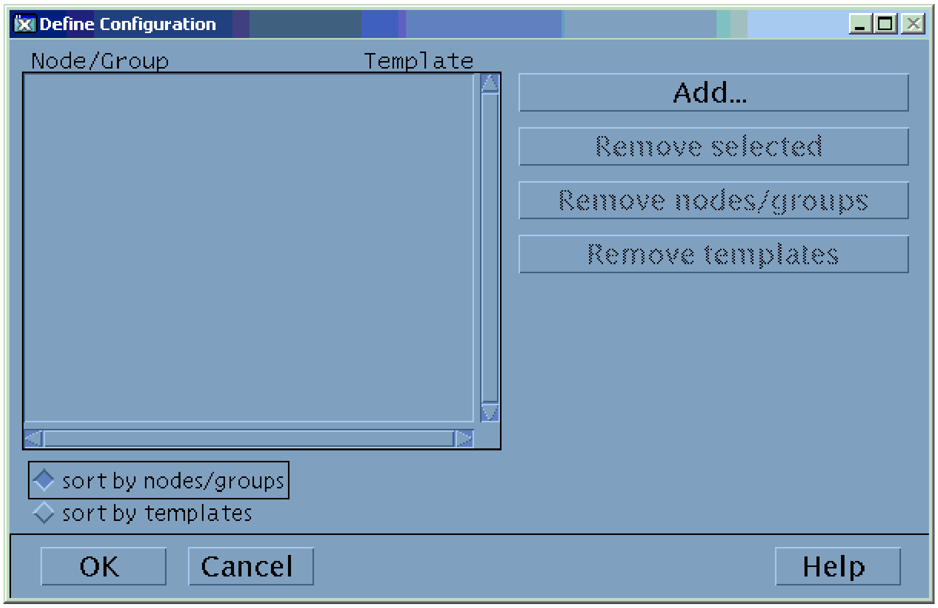
6 Click **Close**.

Task 3: Assign Templates

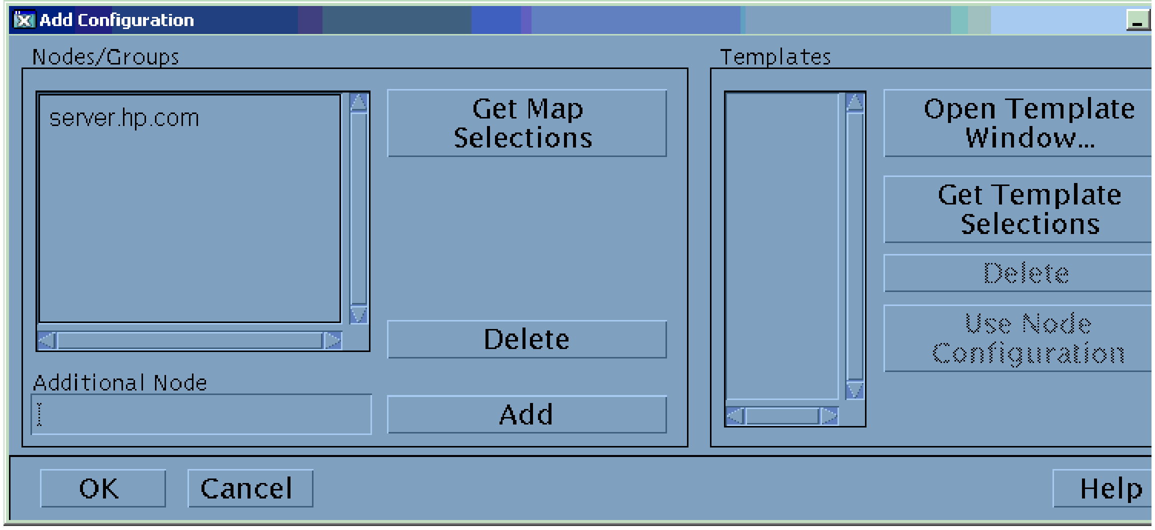
Assign the WBSSPI-Discovery and WBSSPI-Messages templates to the management server:

1 Open the Node Bank window and highlight the management server.

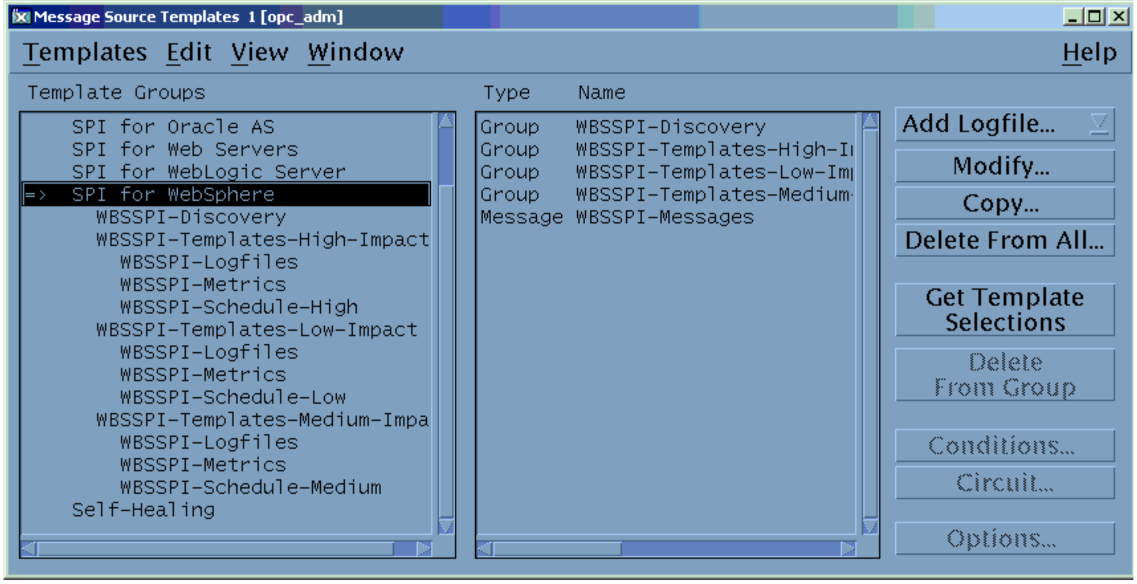
2 From the Actions menu, select **Agents** → **Assign Templates**. The Define Configuration window opens.



3 Click **Add**. The Add Configuration window opens.



4 Click **Open Template Window**. The Message Source Templates window opens.

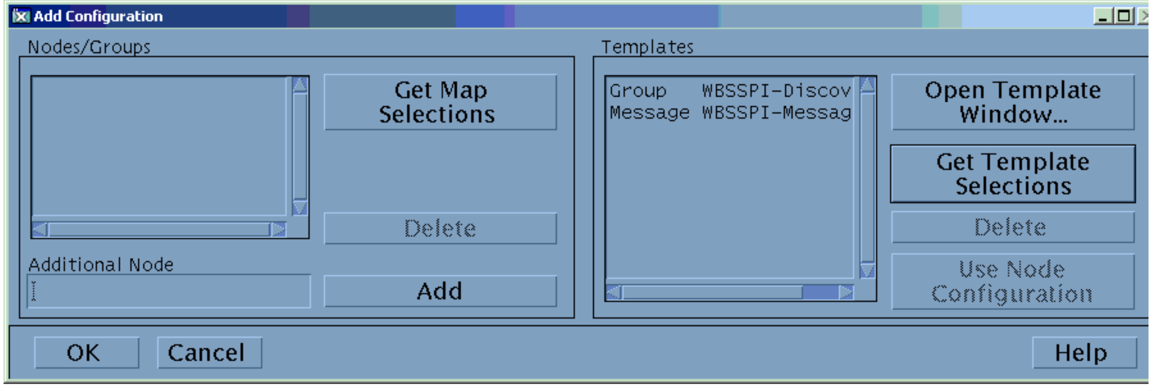


Type	Name
Group	WBSSPI-Discovery
Group	WBSSPI-Templates-High-Ii
Group	WBSSPI-Templates-Low-Im
Group	WBSSPI-Templates-Medium-
Message	WBSSPI-Messages

5 From the Message Source Templates window, in the Template Groups pane, select the **SPI for WebSphere** template group.

6 From the Message Source Templates window, in the right pane, select the **WBSSPI-Discovery** and **WBSSPI-Messages** templates.

7 From the Add Configuration window, click **Get Template Selections**. The WBSSPI-Discovery and WBSSPI-Messages templates appear in the right pane.



Group	WBSSPI-Discov
Message	WBSSPI-Messag

8 In the Add Configuration window, click **OK**.

Task 4: Distribute Templates

Distribute the WBSSPI-Discovery and WBSSPI-Messages templates to the management server:

1 Open the Node Bank window and highlight the management server.

2 From the Actions menu, select **Agents** → **Install/Update SW & Config**.

3 In the Target Nodes section, select **Nodes in List Requiring Update**.

4 In the Install/Update Software and Configuration window check the **Templates** check box.

5 Select **Force Update**.

6 Click **OK**.

The following message is displayed in the message browser:

```
The following configuration information was successfully distributed:
Templates
```

The WBSSPI-Discovery and WBSSPI-Messages templates are distributed to the management server.

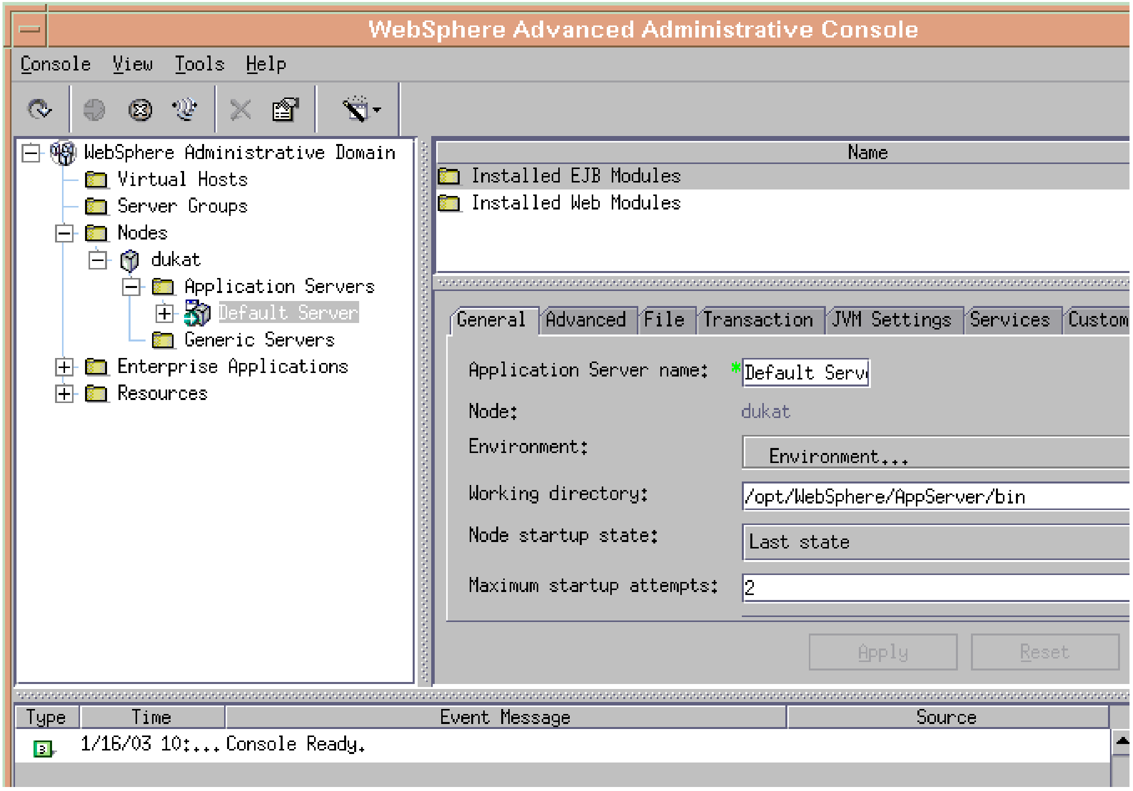
WebSphere SPI Configuration for Managed Nodes

To configure WebSphere SPI, complete the following tasks for each managed node:

- Task 1: Verify the Application Server Status
- Task 2: Collect WebSphere Login Information
- Task 3: Enable PMI
- Task 4: Connect using JSR 160
- Task 5: Update WebSphere's SDK

Task 1: Verify the Application Server Status

Verify that your application servers are running. For WebSphere Server version 4, check the server's status from the WebSphere administrative console. Under the General tab, a colored marker appears next to the Application Server name. A green marker means the server is running. A red marker means the server is not running.



Application Server name: *Default Serv

Node: dukat

Environment: Environment...

Working directory: /opt/WebSphere/AppServer/bin

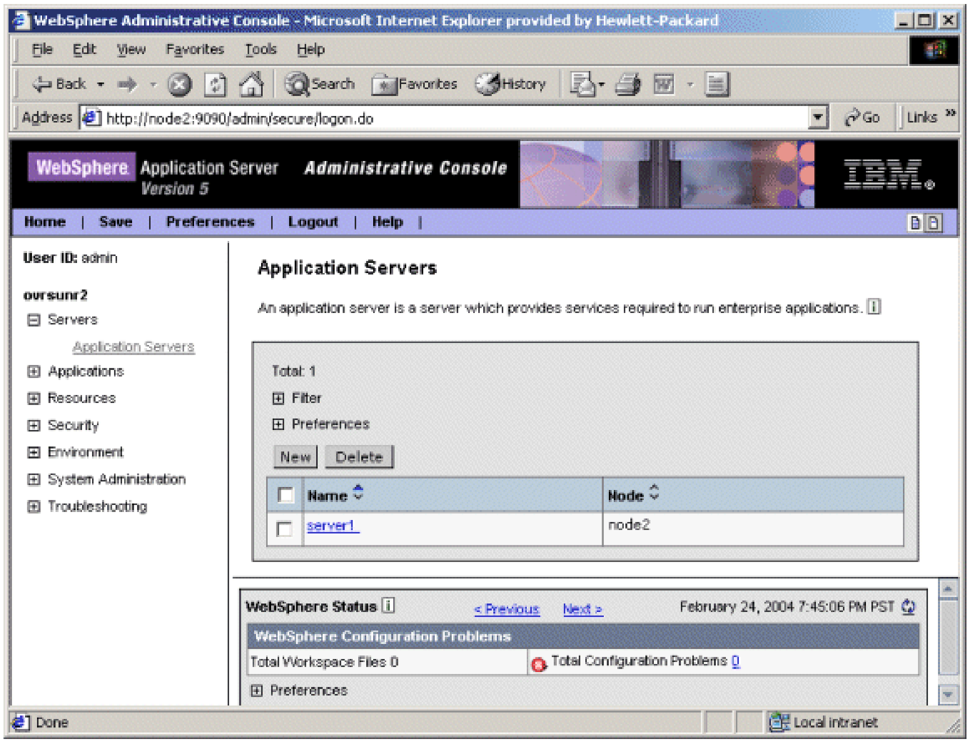
Node startup state: Last state

Maximum startup attempts: 2

Type	Time	Event Message	Source
B	1/16/03 10:...	Console Ready.	

For WebSphere Server version 5 and above, check the server's status from the WebSphere administrative console.

.


WebSphere Administrative Console - Microsoft Internet Explorer provided by Hewlett-Packard
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://node2:9090/admin/secure/logon.do
Go Links
WebSphere Application Server Version 5 Administrative Console
IBM
Home | Save | Preferences | Logout | Help |
User ID: admin
oursunr2
Servers
Application Servers
Applications
Resources
Security
Environment
System Administration
Troubleshooting
Total: 1
Filter
Preferences
New Delete
WebSphere Status
< Previous Next >
February 24, 2004 7:45:06 PM PST
WebSphere Configuration Problems
Total Workspace Files 0
Total Configuration Problems 0
Preferences
Done
Local intranet

Application Servers

An application server is a server which provides services required to run enterprise applications.

	Name	Node
□	server1	node2

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

- UNIX: <*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**

Task 2: 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 needed by 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 5.1.0 or earlier, you must use the default WebSphere Admin Server username and password (the username and password configured when the WebSphere application server was installed/configured).

If you are using WebSphere version 5.1.1 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.

Task 3: Enable PMI

If you are running WebSphere Server version 5, enable PMI using the WebSphere administrative console and restart the server. For more information, see **http://publib.boulder.ibm.com/infocenter/ws51help/index.jsp?topic=/com.ibm.websphere.base.doc/info/aes/ae/tprf_prfstartadmin.html**.

PMI is necessary for collecting metrics.

Task 4: 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. 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 to connect to WebSphere Application Server 6.1 or later, the application server can run in "security enabled" or "security disabled" mode. In the "security disabled" mode the collector can run in both Transient and Persistent mode, but in the "security enabled" mode the collector can only run in the Transient mode. To set the collector in Transient mode, add a line– **COLLECTOR_MODE=TRANSIENT** at the end of the `SPIConfig` file.

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.

Task 5: 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**.

WebSphere SPI Configuration from the Management Server

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

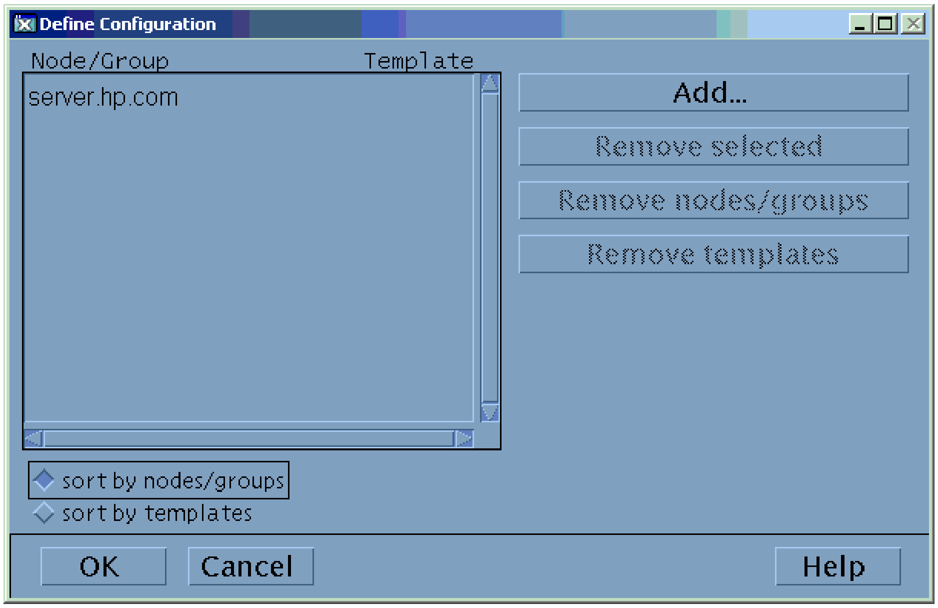
- Task 1: Assign the WBSSPI-Messages Template
- Task 2: Distribute Templates, Actions, Monitors, and Commands
- Task 3: Launch Discover WebSphere
- Task 4: Verify the Discovery Process
- Task 5: Add Nodes to a WebSphere SPI Node Group
- Task 6: Distribute WebSphere SPI Templates
- Task 7: Complete Configuration
- Task 8: Run the Verify Application

Task 1: Assign the WBSSPI-Messages Template

Assign the WBSSPI-Messages template to the managed nodes:

1 Open the Node Bank window and highlight the managed nodes.

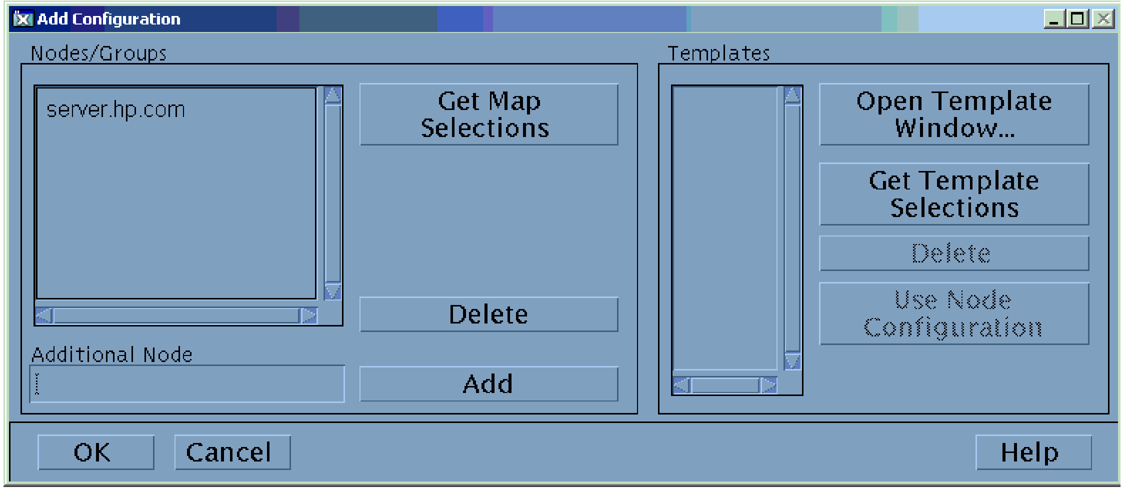
2 From the Actions menu, select **Agents** → **Assign Templates**. The Define Configuration window opens.



Define Configuration

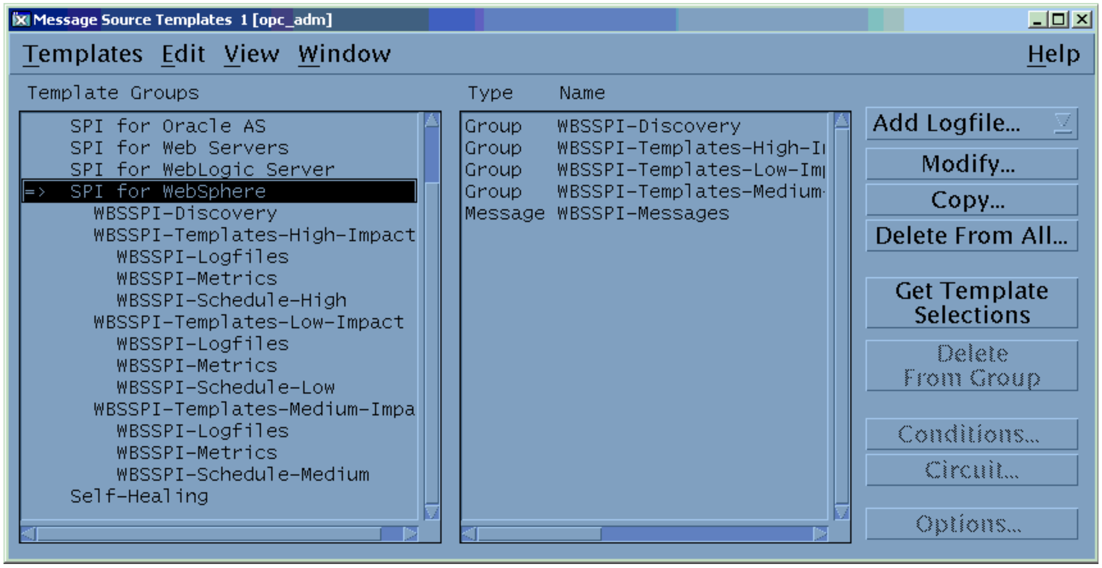
Node/Group	Template
server.hp.com	

3 Click **Add**. The Add Configuration window opens.



server.hp.com

4 Click **Open Template Window**. The Message Source Templates window opens.



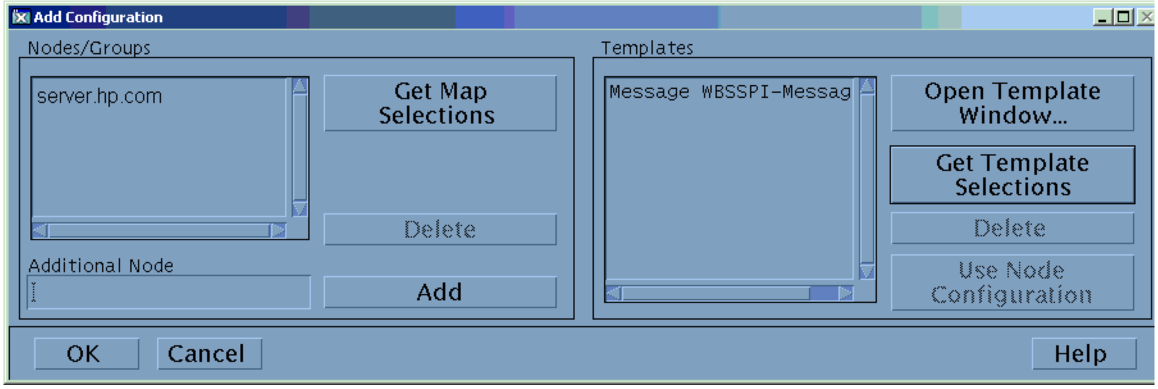
```
    SPI for Oracle AS
    SPI for Web Servers
    SPI for WebLogic Server
=>  SPI for WebSphere
      WBSSPI-Discovery
      WBSSPI-Templates-High-Impact
        WBSSPI-Logfiles
        WBSSPI-Metrics
        WBSSPI-Schedule-High
      WBSSPI-Templates-Low-Impact
        WBSSPI-Logfiles
        WBSSPI-Metrics
        WBSSPI-Schedule-Low
      WBSSPI-Templates-Medium-Impa
        WBSSPI-Logfiles
        WBSSPI-Metrics
        WBSSPI-Schedule-Medium
    Self-Healing
```

```
Group    WBSSPI-Discovery
Group    WBSSPI-Templates-High-Im
Group    WBSSPI-Templates-Low-Im
Group    WBSSPI-Templates-Medium-
Message  WBSSPI-Messages
```

5 In the Template Groups pane, select the **SPI for WebSphere** template group.

6 In the Type and Name pane, select the **WBSSPI-Messages** template.

7 From the Add Configuration window, click **Get Template Selections**. The WBSSPI-Messages template appears in the right pane.



server.hp.com

Message WBSSPI-Messag

8 Click **OK**.

Task 2: Distribute Templates, Actions, Monitors, and Commands

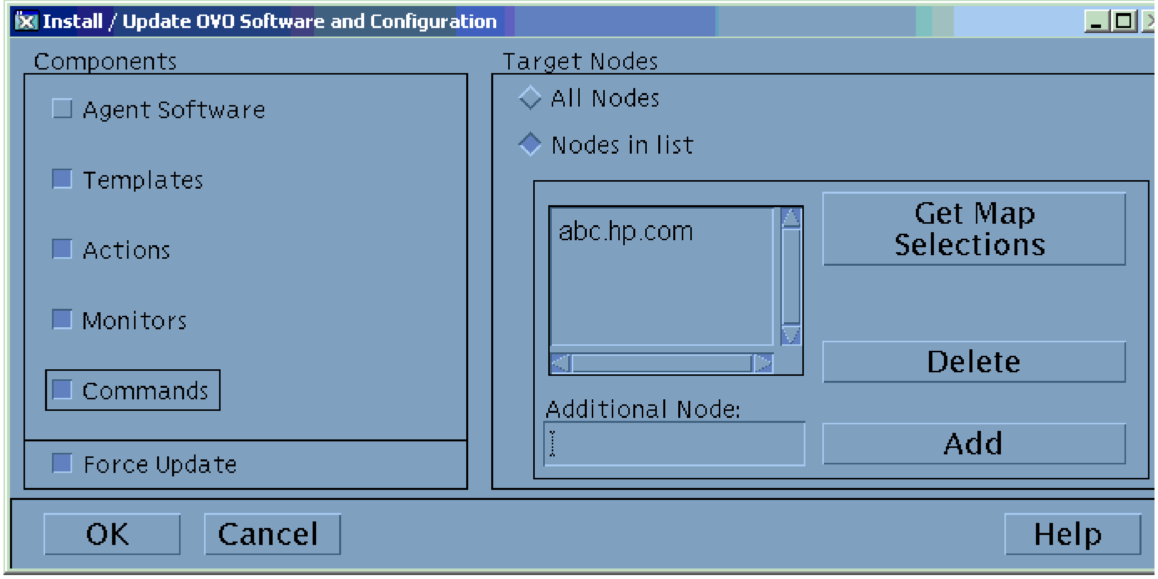
1 Highlight the managed nodes on which to install the SPI components.

2 From the Node Bank window's Actions menu select **Agents** → **Install/Update SW & Config**.

3 In the Install/Update OVO Software and Configuration window select the following component check boxes:

- Templates
- Actions
- Monitors
- Commands

Using this dialog, you deploy program components to the managed nodes.



4 Select the **Force Update** check box.

5 Select the **Nodes in list** option button.

6 Click **OK**.

Upon completion, the following message appears in the message browser for each managed node:

```
The following configuration information was successfully distributed:
Templates Actions Commands Monitors
```

The WebSphere SPI is now installed on the management server and selected managed nodes. If you want to install the WebSphere SPI on other managed nodes, repeat these steps.

Task 3: Launch Discover WebSphere

1 At the HPOM console, highlight the nodes in the Node Bank window.

2 From the Window menu, select **Application Bank**.

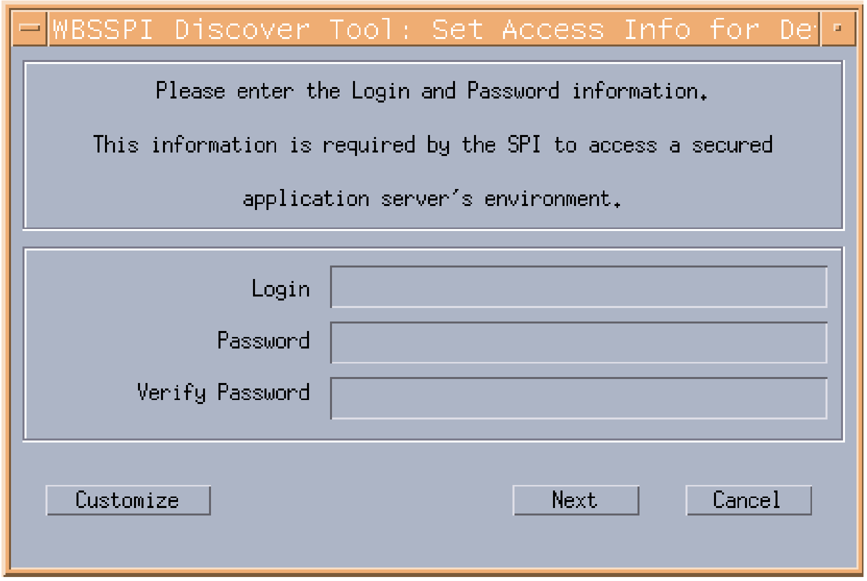
3. From the Application Bank window select **WBSSPI** → **WBSSPI Admin** and double-click **Discover WebSphere**. (If the above does not appear as described, select **Map** → **Reload**.) The Introduction window opens. This window contains brief information about the Discovery application.

4. Click **Next**. A second Introduction window opens. This window displays information about which properties might be required in order for the discovery process to work.

5. Read this information and click **Next**.

6. If you already set the LOGIN and PASSWORD properties, the configuration editor opens. Go to the next step.

   If you have not set the LOGIN and PASSWORD properties, the Set Access Info for Default Properties window opens.



WBSSPI Discover Tool: Set Access Info for De

Please enter the Login and Password information.

This information is required by the SPI to access a secured

application server's environment.

   If security is *not* enabled on the application server, leave these fields blank, click **Next**, and go to step 9.

   If security *is* enabled on the application server, the WebSphere Admin Server login information is required. Enter the username and password collected in Task 2: Collect WebSphere Login Information on page 43. 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). That is, 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 147.

   If the WebSphere Admin Server login and password are the same for all WebSphere application servers on all HPOM managed nodes, follow these steps:

   a. Set the LOGIN and PASSWORD properties in the Set Access Info for Default Properties window.

   b. Click **Next**.

   c. Go to step 9.

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 147):

a. Set the LOGIN and PASSWORD properties to the most commonly used WebSphere login and password in the Set Access Info for Default Properties window.

b. Click **Customize** to open the configuration editor.

7. From the configuration editor, set the configuration properties. For more information about using the configuration editor, see Appendix B, The Configuration.

8. Click **Next** to save any changes and exit the editor.

9. The Confirm Operation window opens. 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 in the Node Bank window, start the Discover WebSphere application, 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.

Task 4: Verify the Discovery Process

1. Verify that the following messages appear in the Discover WebSphere application window (the Discover WebSphere application has completed successfully):

```
Discovery started on node: <node>
Finished running the Discovery application
```

   If the Discover WebSphere application does not complete successfully, the following message appears in the application window:

```
Failed to run discovery on node <node>
```

   For information on troubleshooting the discovery process, see Troubleshooting the Discovery Process on page 103.

2. Verify that the following message appears in the message browser for each managed node:

```
WASSPI-602- Updating the WBSSPI configuration data with discovered
information
```

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

3. If Service Navigator is already running, select **File** → **Reload Configurations**. In the Services tree, open the Application node and look for the WebSphere service.

4. Run the **Configure WBSSPI** application to verify the properties set by the discovery process. See Configure WBSSPI on page 172.

If you are having problems with the discovery process, see Troubleshooting the Discovery Process on page 103.

Task 5: Add Nodes to a WebSphere SPI Node Group

The WebSphere SPI automatically creates three node groups that are assigned the matching WebSphere High, Medium, or Low template group:

- WebSphere High
- WebSphere Medium
- WebSphere Low

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

When data collection for the template group begins, the PMI level of the node is adjusted as necessary to comply with the template 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 Template Groups and System PMI Levels on page 23.

The High template group contains all 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, follow these steps:

1. From the Window menu, open both the Node Group Bank and the Node Bank to display (side-by-side) the WebSphere SPI node group and the managed nodes.
2. Drag and drop managed nodes running a WebSphere Server into the appropriate WebSphere SPI node group, according to the PMI level desired for the node.

Task 6: Distribute WebSphere SPI Templates

1. Open the Node Group Bank window and highlight a WebSphere SPI node group.
2. From the Actions menu, select **Agents** → **Install/Update SW & Config**.
3. In the Target Nodes section, select the **Nodes in List Requiring Update** radio button.
4. In the Install/Update Software and Configuration window check the **Templates** check box.
5. Select **Force Update**.
6. Click **OK**.

   The following message is displayed in the message browser:

   ```
   The following configuration information was successfully distributed:
   Templates
   ```

The WebSphere SPI templates are now distributed to the selected node group. WebSphere SPI monitors now begin running according to their specific collection interval.

If you use HP Reporter, see Integrating HP Reporting and Graphing Products with the WebSphere SPI.

Task 7: Complete Configuration

The configuration information on the management server and managed nodes must be updated. You can do either of the following:

- Wait 10 minutes for the automatic configuration template to run.

  or

- Run the Configure WBSSPI application (which updates the configuration information on the management server and managed nodes). See Configure WBSSPI on page 172.

Task 8: Run the Verify Application

Run the Verify application to verify that WebSphere SPI is properly installed and configured See Verify on page 178.

1 At the HPOM console, select a WebSphere node group in the Node Group Bank window.

2 From the Window menu, select **Application Bank**.

3 In the Application Bank window select **WBSSPI** → **WBSSPI Admin** and double-click **Verify**.

Additional WebSphere SPI Configuration

Based on your WebSphere Server configuration and application needs, you must finish 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 might need to set one or more conditional properties. If you meet a condition, set the properties listed to the left of the condition (these properties are not automatically discovered by the discovery process). For more information about the properties, see Configuration Properties on page 159.

Table 1 Conditional Properties

Conditional Property	When Required
ALIAS	Required if more than one application server on a system shares the same server name. The discovery process automatically sets the `ALIAS` property, but you might want to edit this value because this is the name used in messages, reports, and graphs.
COLLECT_METADATA	Required if you want to use MBean information in the JMX Metric Builder application to create UDMs.
JAVA_HOME	The value of JAVA_HOME must include the path to `JAVA.EXE` (path to the bin directory of Java) and not the path to the actual JAVA_HOME directory. Required if: • You are using a Java version not supplied with the WebSphere Server. • There are multiple Java installation directories.

Table 1 Conditional Properties

Conditional Property	When Required
ADDRESS	Required if a WebSphere Server is configured to a virtual IP address or is on a remote node.
START_CMD, STOP_CMD, and USER	Required if you want to start and stop a WebSphere application server from the HPOM console.
LOGIN and PASSWORD	Required if security is enabled on a WebSphere Server.
MAX_ERROR_LOG_SIZE	Required if you want an error logfile larger than 2 MB.

Setting Conditional Properties

1 At the HPOM console, select the nodes in the Node Bank window.

2 From the Window menu, select **Application Bank**.

3 In the Application Bank window select **WBSSPI** → **WBSSPI Admin** → **Configure WBSSPI**. (If the items do not appear, select **Map** → **Reload**.)

The Introduction window opens.

4 Click **Next**.

5 From the configuration editor, set the properties. For information on using the configuration editor, see The Configuration Editor on page 149.

6 Optionally, click **Save** to save any changes made to the configuration. Once you save your changes, you cannot automatically undo them.

7 Click **Finish** or **Next** to save any changes and exit the editor.

If you click **Next**, the Confirm Operation window opens. Click **OK**.

➤ If you click **Cancel** and make 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 in the Node Bank window, start the Configure WBSSPI application, click **Next** from the configuration editor, and then click **OK**.

8 If you added an application server or added/edited the HOME or PORT properties, run the Discover WebSphere application on the managed nodes on which the application server/properties were added or edited. Running the Discover WebSphere application updates the Service Navigator map.

Configuring a Non-Root HTTPS Agent on a UNIX Managed Node (OVO for UNIX 8.x Only)

If you are running or planning to run a non-root HTTPS agent on a UNIX managed node (OVO for UNIX 8.x only), follow these steps:

➤ 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 root or with HP Operations agent user privileges, follow these steps:

   a Stop all HP Operations agents. Run 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. Run the following command:

   opcagt -start

   d Verify OV_SUDO is set. Run the following command:

   ovdeploy -cmd set | grep SUDO

   The following displayed:

   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 Select the node in the Node Bank window.

   c From the Application Bank window, select **WBSSPI** → **WBSSPI Admin** → **Init Non-Root**.

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 145.

   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:

```
Cmnd_Alias WBSSPI_ADMN = /opt/OV/nonOV/perl/a/bin/perl -S
wasspi_wbs_admin *
Cmnd_Alias WBSSPI_COLL = /opt/OV/nonOV/perl/a/bin/perl -S wasspi_wbs_ca
*
Cmnd_Alias WBSSPI_DISC = /opt/OV/nonOV/perl/a/bin/perl
wasspi_wbs_discovery.pl
Cmnd_Alias WBSSPI_LFEN = /opt/OV/nonOV/perl/a/bin/perl -S wasspi_wbs_le
*
Cmnd_Alias WBSSPI_SHSC = /opt/OV/nonOV/perl/a/bin/perl -S
shs_collector.pl *

Cmnd_Alias WBSSPI_ADMNP = /opt/OV/nonOV/perl/a/bin/perl -S \
/var/opt/OV/bin/instrumentation/wasspi_wbs_admin *
Cmnd_Alias WBSSPI_COLLP = /opt/OV/nonOV/perl/a/bin/perl -S \
/var/opt/OV/bin/instrumentation/wasspi_wbs_ca *
Cmnd_Alias WBSSPI_DISCP = /opt/OV/nonOV/perl/a/bin/perl \
/var/opt/OV/bin/instrumentation/wasspi_wbs_discovery.pl
Cmnd_Alias WBSSPI_LFENP = /opt/OV/nonOV/perl/a/bin/perl -S \
/var/opt/OV/bin/instrumentation/wasspi_wbs_le *
Cmnd_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 every time the agent user is switched.

The WebSphere SPI 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. 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
- Node: HP-UX MCSG cluster
- OVO for UNIX 8.x HTTPS Agent version (for details, see the Agent cluster support matrix.)

Configuring the WebSphere SPI for High Availability Environments

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

- Task 1: Create the WebSphere SPI Monitoring Configuration File
- Task 2: Create the Clustered Application Configuration File
- Task 3: Configure the WebSphere SPI

Task 1: Create the WebSphere SPI Monitoring Configuration File

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 templates on the managed node so that you can disable/enable these templates as appropriate, for inactive/active managed nodes.

To create this clustered application configuration file for your WBS environment, follow these steps:

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

```
<?xml version="1.0"?>
<APMApplicationConfiguration>
   <Application>
      <Name> ... </Name>
      <Template> ... </Template>
      <StartCommand>wasspi_wbs_perl -S wasspi_wbs_clusterSvrApp -opt
      startMonitor $instance</StartCommand>
      <StopCommand>wasspi_wbs_perl -S wasspi_wbs_clusterSvrApp -opt
      stopMonitor $instance</StopCommand>
   </Application>
</APMApplicationConfiguration>
```

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"?>

<APMApplicationConfiguration>

   <Application>
      <Name>namespace_name</Name>
      <Template>All</Template>
      <StartCommand>wasspi_wbs_perl -S wasspi_wbs_clusterSvrApp -opt
      startMonitor $instance</StartCommand>
      <StopCommand>wasspi_wbs_perl -S wasspi_wbs_clusterSvrApp -opt
      stopMonitor $instance</StopCommand>
   </Application>

</APMApplicationConfiguration>
```

➤ `<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.

Task 2: Create the Clustered Application Configuration File

The clustered application configuration file `apminfo.xml`, working in conjunction with the *`<appl_name>`*`.apm.xml` file of WebSphere SPI, enables you to associate 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`, follow these steps:

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>
```

Task 3: Configure the WebSphere SPI

To configure the WebSphere SPI, follow these steps:

1 Launch the Discover WebSphere application with virtual node as the target. For details about launching the discovery application, see Task 3: Launch Discover WebSphere on page 47.

2 Launch the Configure WBSSPI application with the virtual node as the target. The configuration editor opens.

3 Use the configuration editor to set the following properties (these properties are in addition to the ones discovered by the Discover WebSphere application) :

- 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 located 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.

WebSphere SPI Discovery in Cluster Environment

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

Deployment Manager

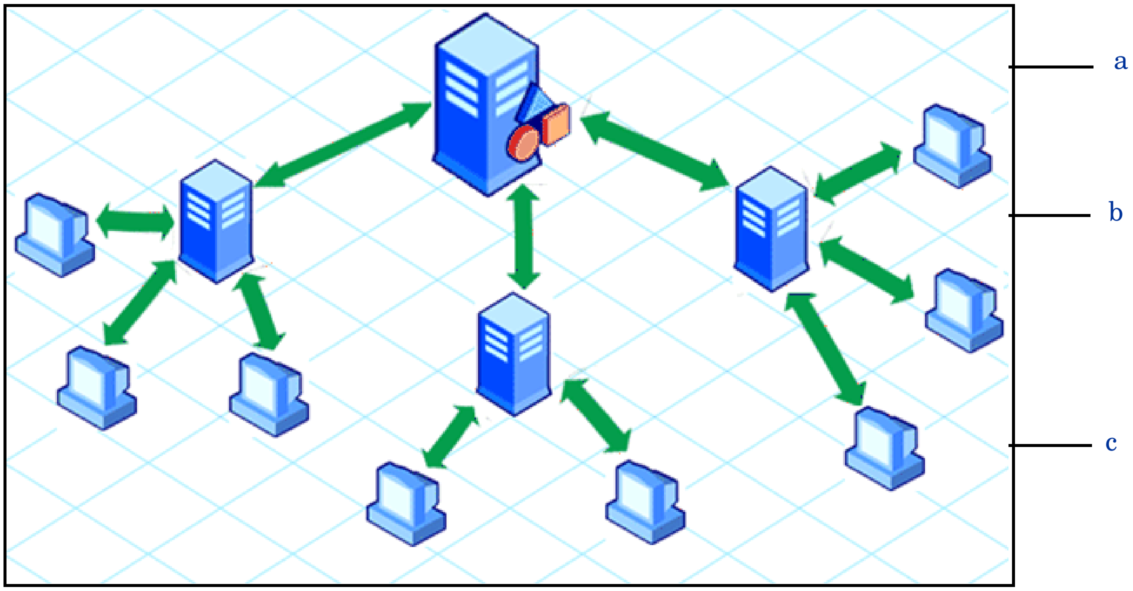
The Deployment Manager acts as an intermediate manager for the WebSphere Application Servers running on various nodes.

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 of 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:



Legend

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

WebSphere SPI 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 secenario, 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 templates are deployed only on the Deployment Managers.
- The WebSphere SPI creates a `DistributedServerConfig` file on the Deployment Manager node and stores in it 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 helpful 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 WebSphere SPI 6.00 in a distributed network deployer environment. If you have a classic set-up in your environment, you can continue using WebSphere SPI as usual.

Use Case 1: You are a new customer of 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 templates and instrumentation to all the nodes on which the Deployment Manager is running.
3. Run the Discover WebSphere Application.

   The master SiteConfig contains only the details of the Deployment Managers. The details of the application servers on individual nodes is 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 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 Deployment Manager is running.
3. Manually remove all previous versions of WebSphere SPI policies from all the individual nodes (where the WebSphere Application Server is running) . You can do this 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, it cannot be done through the HPOM console.

Use Case 3: If you are an existing customer of WebSphere SPI and are planning to implement the network deployer scenario.

⚠ If you follow these steps, you might lose your data. Backup your data before you follow these steps.

Follow steps as in Use Case 1.

Use Case 4: If you are an existing customer of 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 WebSphere Application.
3. Go to <*OvDataDir*>`/conf/wbsspi` directory.
4. Open `SPIConfig` file.
5. Set **`OVERRIDE_DISTRIBUTED_MODE=TRUE`**

   This action ignores the network deployer scenario.
6. Save the `SPIConfig` file.
7. Clean master `SiteConfig` to remove the servers listed in the `SiteConfig` for the corresponding node.
8. Rerun the Discover WebSphere Application.

Limitations in a Network Deployer scenario

- Log file monitoring is not supported on federated servers.
- The four status related metrics — WBSSPI_0001 Server Status, WBSSPI_0002 Server Status Report, WBSSPI_0003 Admin Server Status, and WBSSPI_0004 Admin 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 application, it returns the status of deployment manager as “unknown”.

4 Customizing the WebSphere SPI Templates

As you become familiar with the Smart Plug-in for WebSphere Application Server (WebSphere SPI), you can determine which templates are most useful to you and which you might want to change. This chapter assists you by providing more detail on the templates and how to make those changes.

Basic Template Customizations

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

Modifying Metrics Templates

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

1 Open the Message Source Templates window.

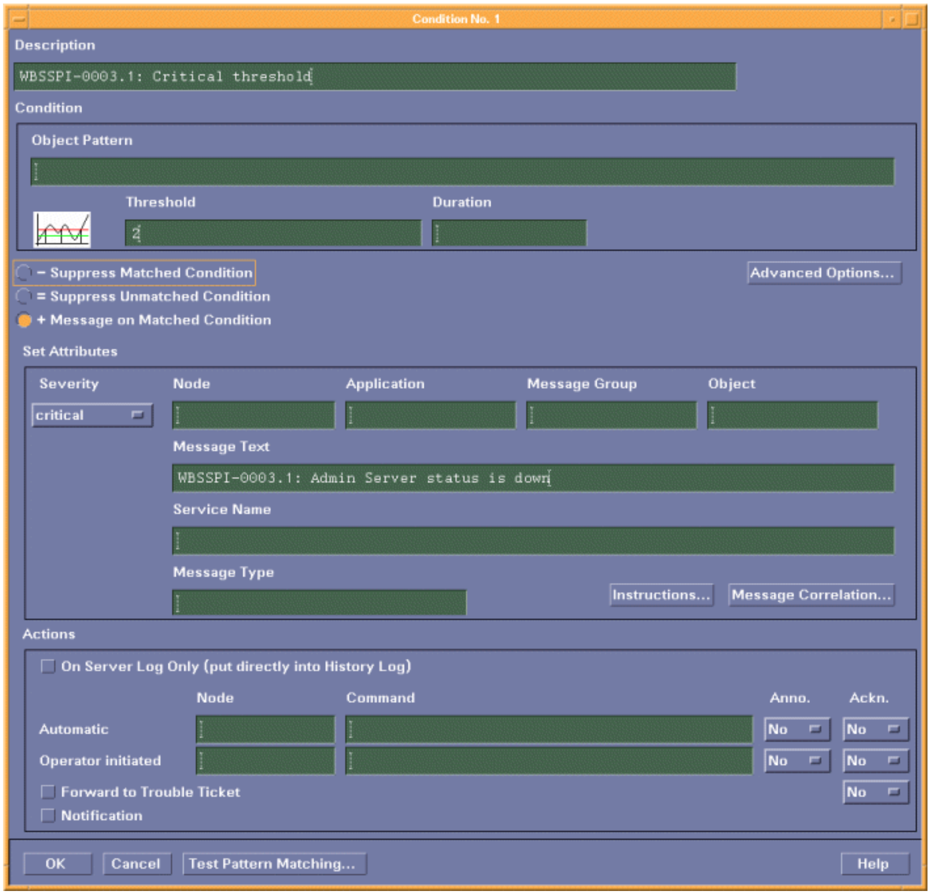
2 Open the SPI for WebSphere template group.

3 Open the desired impact template group and then the WBSSPI-Metrics template group.

4 Double-click the desired metric to open the Message and Suppress Conditions window.

5 Double-click the desired condition to modify (there is usually only one).

The Condition window opens.



Description: WBSSPI-0003.1: Critical threshold

Threshold: 2

● + Message on Matched Condition

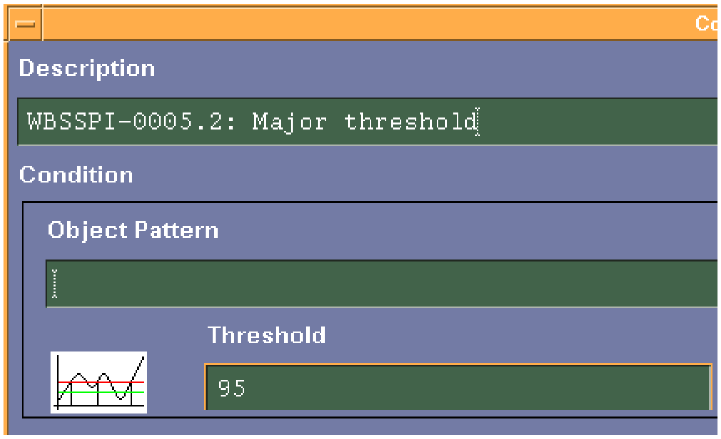
Severity: critical

Message Text: WBSSPI-0003.1: Admin Server status is down

The following attributes can be modified:

- **Threshold**: Enter a value for the metric data that, 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 Severity button and select the desired severity setting.
- **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 at the time an exceeded threshold occurred. You can view a generated WBSSPI report by opening the message's Annotations.

The following illustration of the Condition window shows a threshold setting of 95 for WBSSPI-0005.2. This metric monitors the total number of times per minute clients must wait for an available EJB (enterprise java bean). A value of more than 95 would start to impact the server response time the client experiences, generating an alarm (a warning message).



Description

WBSSPI-0005.2: Major threshold

Condition

Object Pattern

Threshold

95

6 Click **OK**.

7 Re-distribute the modified template (described in Task 6: Distribute WebSphere SPI Templates on page 50).

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 change the change the Message Generation, follow these steps:

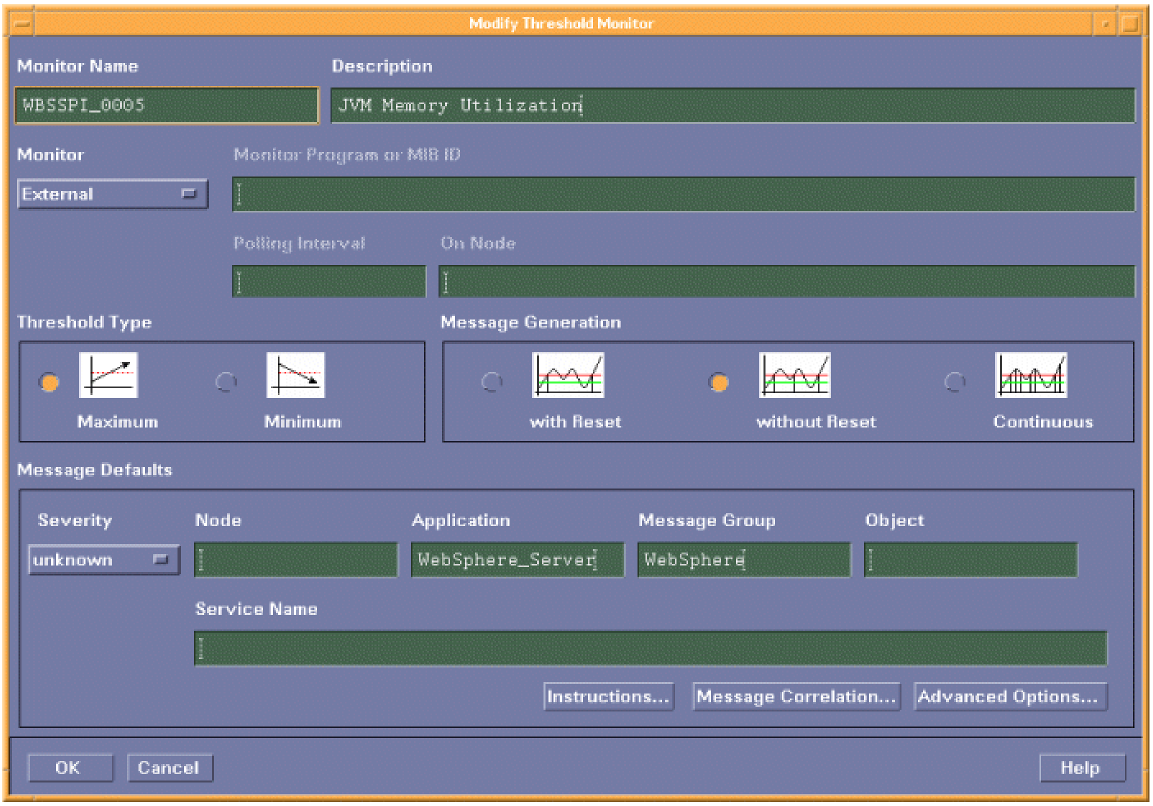
1 Open the Message Source Templates window.

2 Open the SPI for WebSphere template group.

3 Open the desired impact template group and then the WBSSPI-Metrics Template group.

4 Select the template to modify.

5 Click **Modify**. The Modify Threshold Monitor window opens.



Modify Threshold Monitor

Monitor Name: WBSSPI_0005

Description: JVM Memory Utilization

Monitor: External

Monitor Program or MIB ID:

Polling Interval:

On Node:

Threshold Type: ● Maximum ○ Minimum

Message Generation: ○ with Reset ● without Reset ○ Continuous

Message Defaults

Severity	Node	Application	Message Group	Object
unknown		WebSphere_Server	WebSphere	

Service Name:

6 Modify the Message Generation settings:

- **With Reset**: Alarms are generated once when the threshold value is exceeded. At the same time, a reset threshold value is activated. Only when the reset threshold value is exceeded does the original threshold value become active again. Then, when the threshold value is again exceeded, another alarm is generated and the process starts all over again.

- **Without Reset**: Alarms are generated once when the monitoring threshold value is exceeded. Alarms reset automatically when metric values are no longer in violation of the thresholds and are generated again when the threshold is exceeded.

- **Continuously**: Messages are sent/alerts generated each time the metric values are collected and the threshold is exceeded.

7 Click **OK**.

8 Re-distribute the modified template (described in Task 6: Distribute WebSphere SPI Templates on page 50).

Advanced Template Customizations

The template changes described in this section range from making copies of default template groups in order to customize a few settings, to deleting whole groups of metrics within a template's command line. This section is considered advanced because all changes described require some advanced knowledge of the WebSphere SPI metrics.

Choosing Metrics to Customize

Determine which metrics you want to customize and what templates within the group you want to use and then follow these steps:

1. Open the Message Source Templates window.
2. Highlight the group you want to use and click the **Copy...** button.
3. Rename and save the group.
4. Within the renamed template group, copy each original template and rename it.
5. Delete the originals from the new group.
6. Customize the renamed templates within the group, as necessary.

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

Using the WebSphere SPI Collector/Analyzer Command

The `wasspi_wbs_ca` command is used in every collector template, named according to its collection interval. You can view the default command line parameters within each collector template in the Command text box in the Modify Scheduled Action window.

WebSphere SPI Collector/Analyzer Command Parameters

WebSphere SPI data collections are started with the wasspi_wbs_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 4`
`-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 6.1`

Parameter	Description	Syntax
-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 4
-r (report)	Generates an ASCII report for the specified metrics	-r
-t (tag)	Creates a new template group by adding a prefix to an existing collector template 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
-e (exclude)	Excludes specific servers from being monitored. Must not be used with the -i option.	-e *<server_name>* Example: -e server2,server4
-x	Specifies a property/value:	-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_wbs_ca -m 10-14,25,26
    ```

  - data from specific servers only:

    ```
    wasspi_wbs_ca -m 245,246,260 -i server1,server2
    ```

- To not collect data from specific servers:

  ```
  wasspi_wbs_ca -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 subelement in a 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` nor `-xml` options. **Syntax**: `-m` *<metric_id>* **Example**: `-m TestUDM_1000`

Parameter	Description	
-mbean	Performs a JMX call on the specified MBeans. This option must not be used with the -m nor -xml options. **Syntax**: -mbean *<objectname>* *<action>* **Example**: -mbean WebSphere:type=ThreadPool,* -get maximumSize where *<action>* (a JMX call) is one of the following:	
	-get	Returns the value of the apecified attribute. **Syntax:** -mbean *<objectname>* -get *<attribute>* **Example:** -get maximumSize
	-invoke [-type]	Executes 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. **Syntax:** -mbean *<objectname>* -invoke *<operation>* [-type *<parameter_type>* *<parameter_value>*]. . . 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. **Example:** -invoke setInstrumentationLevel -type java.lang.String pmi=L -type boolean true
	-set	Assigns the specified value to the specified attribute. **Syntax:** -mbean *<objectname>* -set *<attribute>* *<value>* **Example**: -set growable true
-o	(object) Specifies an MBean instance. **Syntax**: -o *<mbean_instance>* **Example**: -o exampleJMSServer	
-xml	Specifies the XML file that contains the JMX actions to perform. This option must not be used with the -m nor -mbean options. **Syntax**: -xml *<filename>* **Example**: -xml myJMXActions.xml	

Examples

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

```
wasspi_wbs_perl -S wasspi_wbs_ca -a
-mbean WebSphere:type=ThreadPool,* -set maximumSize 500 -o
<$OPTION(instancename)>
```

- Set the instrumentation levels to low on all PMI modules:

```
wasspi_wbs_perl -S wasspi_wbs_ca -a
-mbean WebSphere:type=Perf,* -invoke setInstrumentationLevel -type
java.lang.String pmi=L
```

- Use the sample UDM TestUDM_1000 in the wbs_UDMMetrics-sample.xml file:

```
wasspi_wbs_perl -S wasspi_wbs-ca -a -m TestUDM_1000
-i examplesServer
```

- Use the sample actions xml file:

```
wasspi_wbs_perl -S wasspi_wbs-ca -a
-xml /var/opt/OV/wasspi/wbs/conf/wbs_JMXActions-sample.xml
-i examplesServer
```

Changing the Collection Interval for Scheduled Metrics

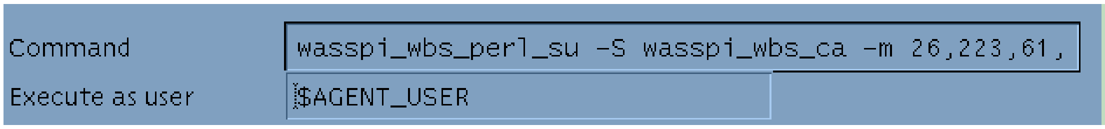
To change the metric collection interval, simply change the Polling Interval in the appropriate collector template. For example, to change the collection of default metrics from 5 minutes to 10 minutes for the WebSphere High Impact template group, follow these steps:

1. Open the Message Source Templates window.
2. Select the template group **SPI for WebSphere** and click **WebSphere-Templates-High-Impact** → **WBSSPI-Schedule-High**.
3. Select the collector template **WBSSPI-40-High-05min**.
4. Click **Modify...** The Modify Scheduled Action window opens.
5. Change the Scheduled Action Name to **`WBSSPI-40-High-10min`**.
6. Change the Schedule interval in the Minute box from 5m to 10m. For example, 0, 10, 20...
7. Distribute the new templates (described in Task 6: Distribute WebSphere SPI Templates on page 50).

Changing the Collection Interval for Selected Metrics

To change the collection interval for selected metrics, copy the appropriate collector template and rename with a name reflecting the new interval, deleting all but the metrics you are changing. Set the new interval. Edit the original template to remove the changing metrics. For example, to change the collection interval to 10 minutes for metrics 221-225, you would follow these steps:

1. Open the Message Source Templates window.
2. Select the template group **SPI for WebSphere** and click **WebSphere-Templates-High-Impact** → **WBSSPI-Schedule-High**.
3. Select the template **WBSSPI-40-High-05min**.
4. Click **Copy...**. The Copy Scheduled Action window opens. In the Schedule Action Name box, change the Scheduled Action Name name to **`WBSSPI-40-High-10min`**.
5. In the command box delete all metrics after `-m` except 221-225.



Command wasspi_wbs_perl_su -S wasspi_wbs_ca -m 26,223,61,

Execute as user $AGENT_USER

6. Change the polling interval to 10m.
7. Click **OK**.
8. In the template group **WBSSPI-Schedule-High**, select the **WBSSPI-40-High-05min** template.

9 Click **Modify**. The Modify Scheduled Action window opens. Delete 221-225 after `-m` from the Command Box.

10 Re-distribute the modified templates as described in Task 6: Distribute WebSphere SPI Templates on page 50.

Customize the Threshold for Different Servers

Customize the threshold as needed. 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 the 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 is displayed.

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>:<>:<*>:<*>*

For 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.

Creating Custom, Tagged Templates

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

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

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

To Create the New Template Group

1 Copy the original template group. In the Message Source Templates window select the group and click **Copy...**.

2 Name the new group according to how you plan to identify the new schedule and collector templates. For example, if you are including CLIENT01 in the template names, include that within the new template group name.

3 In the Message Source Template window, expand the new template group to show all templates and select each template you plan to use, click **Copy...**, and rename it according to your naming scheme.

- The names you give the new metric monitor templates in the group would 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 schedule template would 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_wbs_ca -m 16 -t CLIENT01-
```

4 Delete all original templates from the new group.

Template Variables

The following variables are used by the WebSphere SPI templates. If you are creating your own templates, 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. If you determine that your environment meets the criteria, and you have some expertise using the WebSphere SPI and the WebSphere Server, you can use the information in this section to get started.

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:

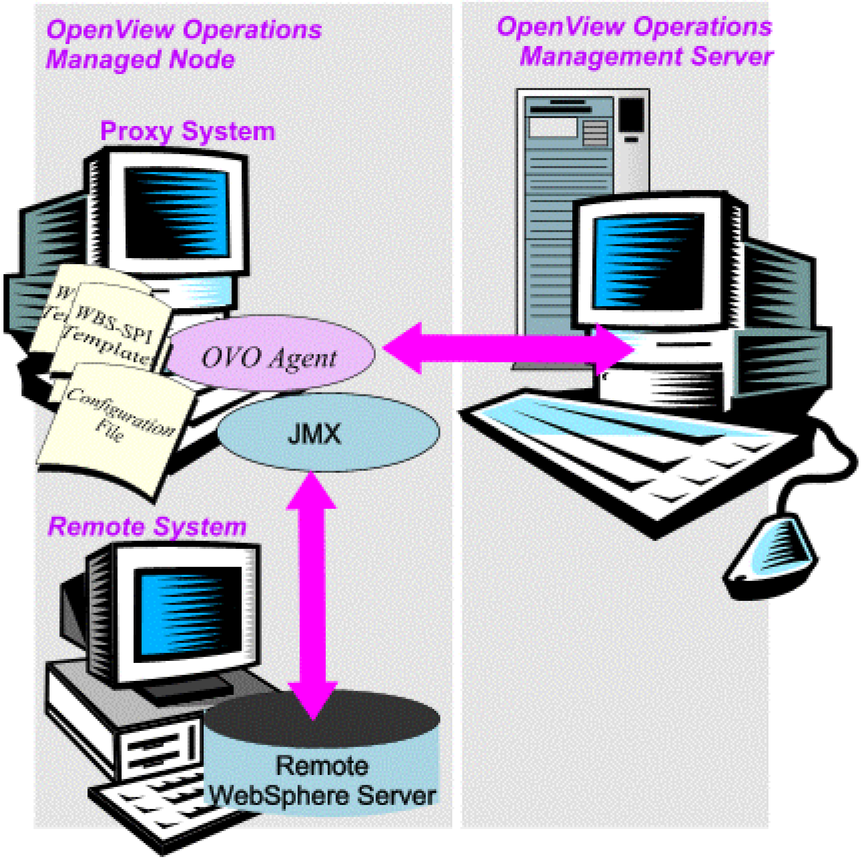
- The remote system is covered by a purchased license (using Tier 1 pricing).
- The WebSphere SPI runs on at least one managed node on a supported platform: HP-UX, Solaris, Linux (Red Hat), AIX, or Windows 2000.
- The local/proxy system and remote system must be running the same version of WebSphere Server. For example if the proxy system is running WebSphere Server version 5, the remote system must also be running WebSphere Server version 5.
- (Optional, for logfile monitoring) The remote system runs on a platform supported by the HP Operations agent software .

Remote Monitoring

The following section provides an overview of remote monitoring and shows how it is implemented. Also included are 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, WebSphere SPI programs/templates 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 Task 1: Configure the Remote WebSphere Server System on page 74, showing how the remote entry appears (with system IP address).

Template deployment requirement: Templates for the correct WebSphere PMI level should be deployed on the local node. If you need a separate template group (for example High Impact or Medium Impact) to cover a different level, you can copy and rename the existing templates 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 65 .

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 templates included with the WebSphere SPI to specify the correct logfile names, and then deploy them to the remote system.

➤ Monitoring remote systems using logfile versioning is not supported.

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.

Task 1: Configure the Remote WebSphere Server System

Using the Configure WBSSPI application in the HPOM WBSSPI Application Bank, configure each local managed node that communicates with a remote WebSphere Server. In the configuration, include additional entries for remote WebSphere Servers.

1 Choose a WebSphere Server managed node from which to monitor the remote WebSphere Server.

2 At the HPOM console, launch the **Configure WBSSPI** application. In the Application Bank window select **WBSSPI** → **WBSSPI Admin** → **Configure WBSSPI**.

3 In the configuration that appears, include an entry for each remote WebSphere Server system: `SERVER`<*n*>`_ADDRESS=`<*DNS server name or IP address*>

Make sure that NUM_SERVERS is set to the correct number of servers (<*n*>) and that HOME and JAVA_HOME are set at the global level.

The following example shows how local and remote WebSphere Servers are configured in the same file. For the remote servers, the `SERVER`<*n*>`_ADDRESS=`<*IP_address*> `(SERVER2_ADDRESS=15.75.27.109 or SERVER2_ADDRESS=hardey.hp.com)` line is added:

```
HOME=/opt/WebServer/AppServer
JAVA_HOME=/opt/WebServer/AppServer/java
NODE local_node {
NUM_SERVERS=2
SERVER1_NAME=lara
SERVER1_PORT=900
SERVER2_NAME=harley
SERVER2_PORT=905
SERVER2_ADDRESS=hardey.hp.com
}
```

There are two WebSphere Servers configured in the preceding configuration. SERVER1 is the local server, running on an HP-UX managed node. SERVER2 is running on an HPOM managed node, that is a non-Red Hat Linux system (a platform unsupported by WebSphere SPI). The remote system is configured similar to that of the local system but contains the new line `SERVER2_ADDRESS=harley.rose.hp.com`.

4 To verify that the SPI is monitoring the remote node, run the following command:

`wasspi_wbs_perl -S wasspi_wbs_ca -m 5 -i` <*remote_server_NAME|ALIAS*> **`-x print=on`**

You must use ALIAS if it is set for the remote server.

Task 2: Integrate the HP Performance Agent (Optional)

Since the HP Performance Agent (also known as the MeasureWare Agent) collection occurs on the managed node (not the remote system), if you use PerfView and would like to graph the remote system data, you must ensure that MeasureWare integration is enabled on the (local) managed node.

Task 3: Assign Local Node to a WebSphere SPI Node Group

Assign the local managed node to the appropriate node group. For example, you would assign the local node to the WBS High node group if the local and remote managed nodes are to collect metrics that require the system 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:

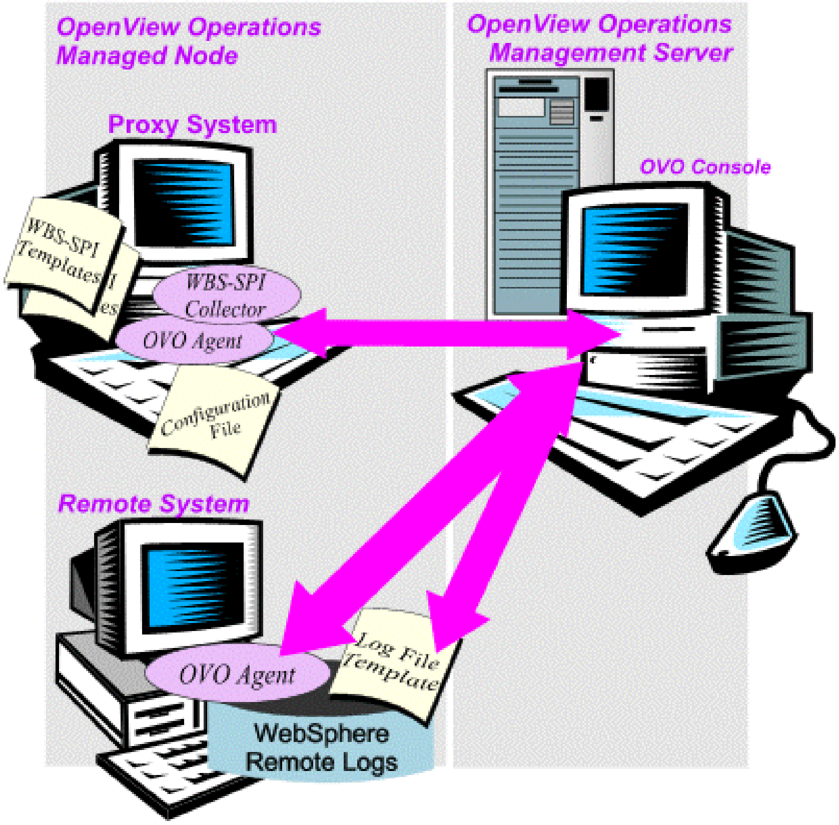
- The remote system that has an HP Operations agent running on it .
- The system does not re-version logfiles when they roll.

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

Configure the Logfile Template for Remote Logfiles

1. Open a copy of the WebSphere Log Template located under WBSSPI-Logfiles in the SPI for WebSphere group. For example, **SPI for WebSphere → WBSSPI-Logfiles**.
2. In the Logfile text box, enter the location of the logfile on the remote system: /<*path*>/<*file_name*>.
3. Assign and deploy the logfile template to the remote HPOM managed node.

The log file template and the HP Operations agent, both present on the remote system, make WebSphere Server logfile monitoring possible.



Limitations of Remote Monitoring

- The WebSphere SPI and the HP Operations agent do not support access to logfiles that are re-versioned each time the logs are rolled.
- When no HP Operations agent is present on the remote system, monitoring of WebSphere Server logfiles on the remote system cannot occur.

- In the HPOM Application Bank, WebSphere SPI applications cannot be executed on remote systems.
- The proxy system and remote system must be running the same version of the WebSphere Server.

Restoring Default WebSphere SPI Templates

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

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

1 Delete all current templates.

   Run the command:

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

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

Using Templates/Applications to View Annotation Reports

Some templates have actions defined with threshold violations or error conditions that automatically cause reports to appear in the message Annotations. These reports are snapshots of data values collected from the server around the time that the alarm occurred.

The reports discussed in this section should not be confused with those generated by HP Reporter, which show more consolidated, historical data generated as web pages in management-ready presentation format.

You can access the data as follows:

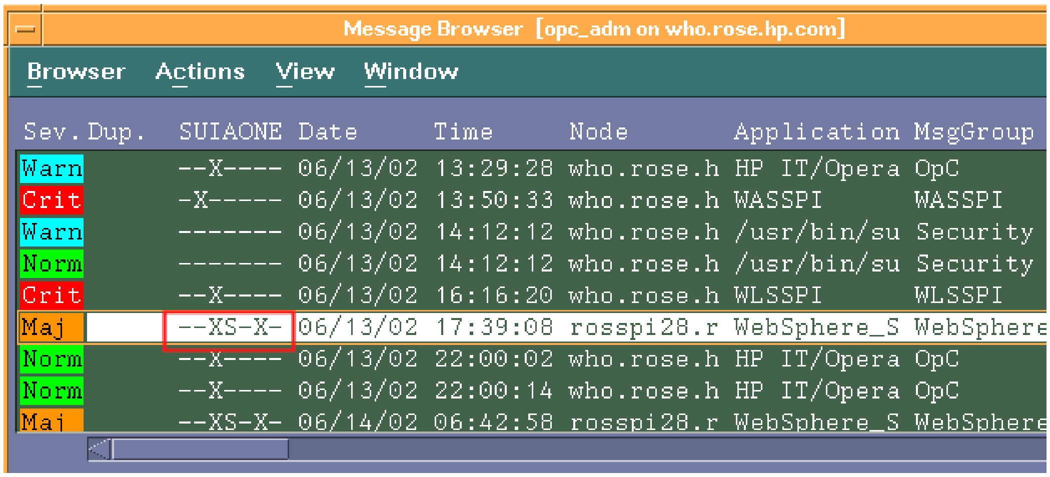
- To view the Message Details. Double-click a message in the HPOM message browser, or just select the message and click Annotations. Reports are available there, showing data values on a single server.
- To view reports. Open both the Node Bank and Application Bank windows. Continue to open application windows **WBSSPI** → **WBSSPI Admin** → **Reports**. Select a node and drag it onto the WebSphere SPI metric report you need. These reports show all server data on a node.

Automatic Action Reports

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

Viewing an Automatic Action Report

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



```
Sev. Dup.  SUIAONE Date     Time     Node       Application MsgGroup
Warn       --X---- 06/13/02 13:29:28 who.rose.h HP IT/Opera OpC
Crit       -X----- 06/13/02 13:50:33 who.rose.h WASSPI      WASSPI
Warn       ------- 06/13/02 14:12:12 who.rose.h /usr/bin/su Security
Norm       ------- 06/13/02 14:12:12 who.rose.h /usr/bin/su Security
Crit       --X---- 06/13/02 16:16:20 who.rose.h WLSSPI      WLSSPI
Maj        --XS-X- 06/13/02 17:39:08 rosspi28.r WebSphere_S WebSphere
Norm       --X---- 06/13/02 22:00:02 who.rose.h HP IT/Opera OpC
Norm       --X---- 06/13/02 22:00:14 who.rose.h HP IT/Opera OpC
Maj        --XS-X- 06/14/02 06:42:58 rosspi28.r WebSphere_S WebSphere
```

To view an automatically generated metric report relating to an alarm condition, click **Annotations...** in the message browser. Column descriptions provide further clarification.

Application Bank Reports

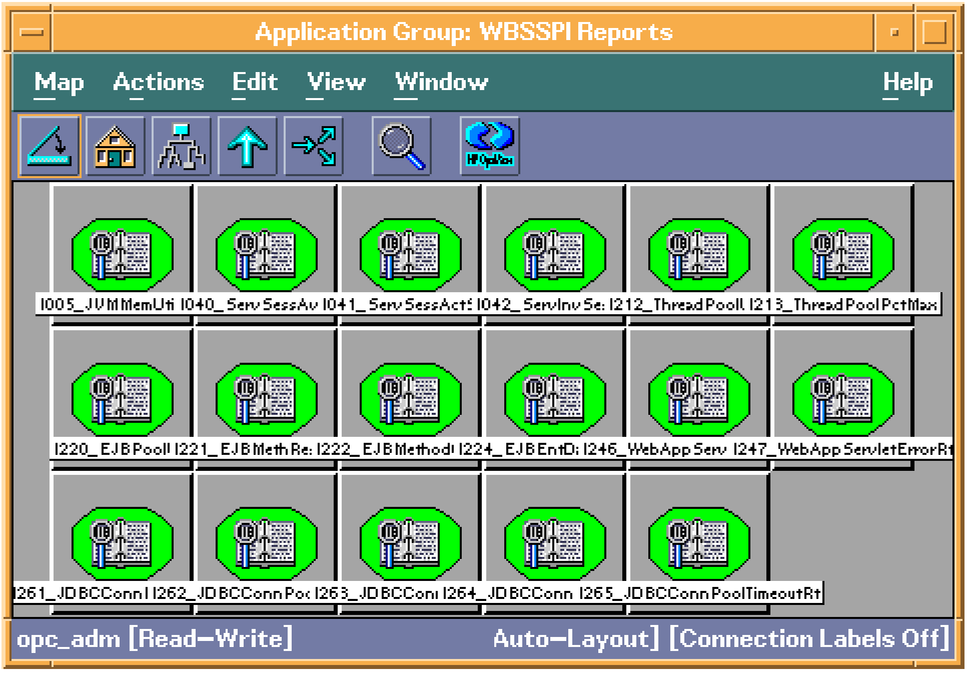
Application Bank reports run for all WebSphere Server instances configured on the managed node. The reports generated from the Application Bank reflect the current state of a WebSphere Server on the managed node. You manually generate these reports in HPOM by dragging the managed node from the Node Bank window to a specific metric report among those shown in the Application Bank window.

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

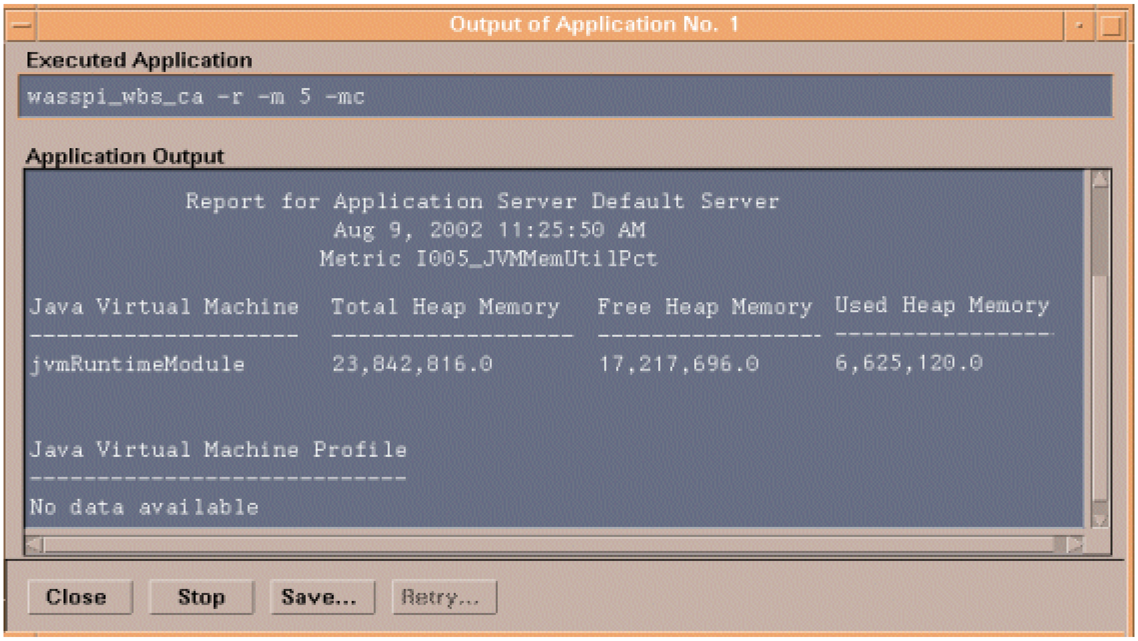
Table 2 Performance Impact Ratings (PMI Levels) of Reporting Metrics

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

When manually generated, a report from the **Application Bank** → **WBSSPI** Reports window shows that metric data for ALL WebSphere Server instances on the managed node.



The following Application Bank report was generated for Metric #5 (I005).



```
wasspi_wbs_ca -r -m 5 -mc
```

```
                  Report for Application Server Default Server
                                 Aug 9, 2002 11:25:50 AM
                                Metric I005_JVMMemUtilPct

Java Virtual Machine    Total Heap Memory    Free Heap Memory    Used Heap Memory
--------------------    -----------------    ----------------    ----------------
jvmRuntimeModule        23,842,816.0         17,217,696.0        6,625,120.0


Java Virtual Machine Profile
----------------------------
No data available
```

Checking WebSphere SPI Nodes for License Count

You can use an HPOM reporting utility to check the number of templates you installed on your managed nodes. In reviewing the number of templates per managed node, you can see if you consistently installed templates across your managed systems. In addition, you can also ensure that the number of licenses you purchased is in compliance 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. In the Reports window among the reports listed select **WBSSPI License Check**.
4. Select an output destination and click **OK**.

5 Integrating HP Reporting and Graphing Products with the WebSphere SPI

The WebSphere SPI can be integrated with the following HP reporting and graphing products (these products must be purchased separately):

- **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 WebSphere SPI with HP Reporter, every night, HP Reporter generates reports that show the performance and availability of a WebSphere Application Server on configured managed nodes. For information on how to integrate HP Reporter with WebSphere SPI, see Integrating with HP Reporter on page 83.

- **HP Performance Agent**: HP Performance Agent collects, summarizes, time stamps, and detects alarm conditions on current and historical resource 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*.

  If you integrated HP Performance Agent with the WebSphere SPI, the WebSphere SPI automatically uses it. 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 82.

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

  For information about how to how to integrate 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 WebSphere SPI metrics data.

  For information on how to integrate WebSphere SPI with HP Performance Manager, see Integrating with HP Performance Manager on page 87. After integrating WebSphere SPI with HP Performance Manager, graphs are available the following day.

Integrating with CODA

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

If you want to use the HP Operations subagent (CODA) included with OVO for UNIX 7.x, 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, Solaris	`/var/opt/OV/conf/dsi2ddf/`
AIX	`/usr/lpp/OV/conf/dsi2ddf/`
Windows	`\usr\ov\conf\dsi2ddf\`

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

2 Save the empty file.

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 Task 14: Install the New Report Package (Optional) on page 35.

The WebSphere SPI report package must be installed on the Windows system running HP Reporter. Follow these steps:

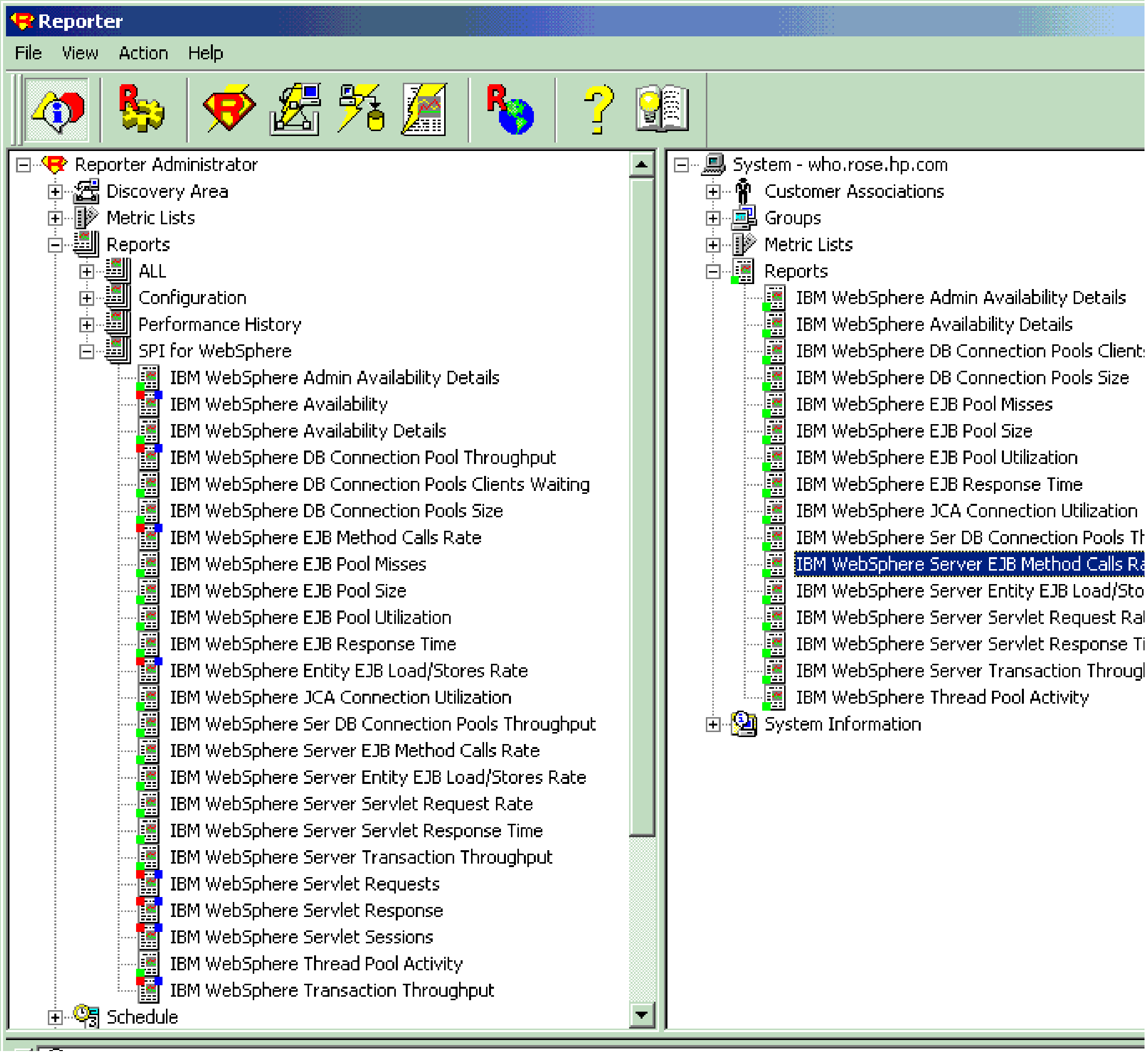
1 On the Windows client system, insert the Smart Plug-ins DVD-ROM (that contains the reporting packages) into the DVD-ROM drive, and in Windows Explorer, double-click: **\OV_REPORTER\WEBSPHERE_SPI_06.00.000\WBSSPI-Reporter.msi**

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.



- Reporter Administrator
  - Discovery Area
  - Metric Lists
  - Reports
    - ALL
    - Configuration
    - Performance History
    - SPI for WebSphere
      - IBM WebSphere Admin Availability Details
      - IBM WebSphere Availability
      - IBM WebSphere Availability Details
      - IBM WebSphere DB Connection Pool Throughput
      - IBM WebSphere DB Connection Pools Clients Waiting
      - IBM WebSphere DB Connection Pools Size
      - IBM WebSphere EJB Method Calls Rate
      - IBM WebSphere EJB Pool Misses
      - IBM WebSphere EJB Pool Size
      - IBM WebSphere EJB Pool Utilization
      - IBM WebSphere EJB Response Time
      - IBM WebSphere Entity EJB Load/Stores Rate
      - IBM WebSphere JCA Connection Utilization
      - IBM WebSphere Ser DB Connection Pools Throughput
      - IBM WebSphere Server EJB Method Calls Rate
      - IBM WebSphere Server Entity EJB Load/Stores Rate
      - IBM WebSphere Server Servlet Request Rate
      - IBM WebSphere Server Servlet Response Time
      - IBM WebSphere Server Transaction Throughput
      - IBM WebSphere Servlet Requests
      - IBM WebSphere Servlet Response
      - IBM WebSphere Servlet Sessions
      - IBM WebSphere Thread Pool Activity
      - IBM WebSphere Transaction Throughput
  - Schedule

- System - who.rose.hp.com
  - Customer Associations
  - Groups
  - Metric Lists
  - Reports
    - IBM WebSphere Admin Availability Details
    - IBM WebSphere Availability Details
    - IBM WebSphere DB Connection Pools Client:
    - IBM WebSphere DB Connection Pools Size
    - IBM WebSphere EJB Pool Misses
    - IBM WebSphere EJB Pool Size
    - IBM WebSphere EJB Pool Utilization
    - IBM WebSphere EJB Response Time
    - IBM WebSphere JCA Connection Utilization
    - IBM WebSphere Ser DB Connection Pools Th
    - IBM WebSphere Server EJB Method Calls Ra
    - IBM WebSphere Server Entity EJB Load/Sto
    - IBM WebSphere Server Servlet Request Ra
    - IBM WebSphere Server Servlet Response Ti
    - IBM WebSphere Server Transaction Throug
    - IBM WebSphere Thread Pool Activity
  - System Information

You can find instructions in the Reporter help for assigning 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. 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 online 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.

WebSphere SPI Reporter Reports

The reports available through the integration of HP Reporter and the WebSphere SPI show consolidated data on server performance and availability on all WebSphere Server systems. In addition, other reports show data for single systems. These reports are available the day following your installation of the WebSphere SPI report package on the HP Reporter Windows system. If you have not yet completed the report package installation, see Integrating with HP Reporter on page 83.

The following tables show all pre-defined reports.

Table 3 All/Group Reports

Report Title	Description	Metric
Availability	Shows the percent uptime for all WebSphere Servers by day.	2
Top 20 Servers— Transaction Throughput	Shows the average throughput for the top 20 execute queues of all servers.	77
Top 20 Servers—JDBC Connection Pool Throughput	Shows the average throughput for all connections pools on the server for the top 20 servers.	66
Top 20 Servers—Servlet Request Rate	Shows the total servlet request rate for the top 20 servers.	45
Top 20 Servers— Servlet Sessions	Shows the total servlet sessions being handled by the top 20 servers.	41
Top 20 Servers— Servlet Average Response Time	Shows the average response time for the top 20 requested servlets for all servers for the reporting period.	245
Top 20 Servers— EJB Method Calls Rate	Shows the number of all EJB method calls per minute for the top 20 servers.	22
Top 20 Servers— Entity EJB Load/Stores Rate	Shows the number of all Entity EJB loads and stores to/from the database per minute for the top 20 servers.	24

Table 4 Single System Reports

Report Title	Description	Metric
Server Availability Details	Contains spectrum graphs showing minutes of uptime by day and hour for each WebSphere Server.	2
Admin Server Availability Details	Shows the uptime percent for each WebSphere Admin server by day.	4
EJB Average Response Time	Shows the average response time for the top 20 EJBs for a server for the reporting period.	221
EJB Method Calls Rate	Shows the number of all EJB method calls per minute for the top 20 EJBs for a server.	22
Entity EJB Load/ Stores Rate	Shows the number of all EJB loads and stores to/from the database per minute for the top 20 EJBs on a server.	224
EJB Pool Utilization	Shows the EJB pool utilization as a percent for the top 20 EJBs on a server.	220

Table 4 Single System Reports

Report Title	Description	Metric
EJB Pool Misses Percent	Shows the percent of time that a call to retrieve an EJB from the pool was not successful during the collection interval for the top 20 EJBs.	225
EJB Pool Size	Shows average pool size for the top 20 EJBs for one server for each day.	223
JDBC Connection Pools Throughput vs. Utilization	Charts throughput against utilization for the JDBC connection pools on the selected server, one chart for each connection pool.	263
JDBC Connection Pools - Size vs. Wait Time	Charts connection pool size against the average wait time for a connection for the JDBC connection pools on the selected server, one chart for each connection pool.	260
JDBC Connection Pools - Clients Waiting vs. TimeoutRate	Charts the number of clients waiting for a database connection from the pool against the timeout rate for waiting clients for the DB connection pools on the selected server, one chart for each connection pool.	265
JCA Connections Utilization - Top 20 Resources	Shows the JCA resource connection pool utilization as a percent.	250
Transaction Throughput	Shows the average transaction throughput for the selected server by day.	77
Thread Pool Activity	Charts the average size of the thread pool against the average number of active threads for all thread pools on the selected server, one chart for each thread pool.	211
Servlet Request Rate	Shows the request rate (per second) for the top 20 servlets for one server for each day.	245
Servlet Average Response Time - Top 20 Servlets	Show the average response time for the top 20 requested servlets for one server for the reporting period.	246

HP Performance Insight Reports for the WebSphere SPI

The reports available through the integration of HP Performance Insight and the WebSphere SPI show consolidated data on server performance and availability on WebSphere application server systems.

The following table shows all pre-defined reports.

Report Title	Description	Metric
Server Availability—Throughput	The server availability chart plots the availability status of the application server on an hourly, daily, and monthly basis. The transaction throughput chart displays the number of transactions processed by the application server per second.	2, 77
EJB Pool Utilization	The percentage of EJB pool utilization.	20
JDBC Throughput—Utilization	The percentage of available JDBC connection in the connection pool and the number of clients serviced by the connection pool per second.	66, 263
Near Real Time Server Availability	The server status for the last six hours.	2, 77
Servlet Request Rate—Response Time	The servlet request rate measures the number of requests for a servlet per second. The servlet response time chart shows the average execution time for an individual servlet.	45, 246
EJB Load-Stores Rate	The number of all entity EJB loads and stores to and from the database per minute for the top 20 servers. For the selected server, lists the top 20 EJBs.	24
EJB Method Calls Rate	The number of all EJB method calls per minute for the top 20 servers.	22
EJB Top 20	The percentage of EJB retrievals that were not successful during the collection interval, average pool size, and average response time in milliseconds for the top 20 EJBs.	25, 221, 223
JDBC Connection Pool Details	The average number of connections allocated per day for the top 20 servers. The DB pool is shown along with clients waiting, client timeout rate, average pool size, and average wait time.	61, 65, 260, 266
Servlet Sessions	The total number of servlet sessions being handled by the top 20 servers.	41
Thread Pool Activity	Comparison of the average size of thread pools with the average number of active threads on the selected server.	210, 211
Transaction Throughput	The average number of transactions processed per second by the top 20 servers for the previous day.	77

Integrating with HP Performance Manager

To integrate the WebSphere SPI with HP Performance Manager, follow these steps:

1 Install and configure the WebSphere SPI. Verify that you completed Task 1: Configure the Management Server to Launch Your Web Browser on page 37. Also, verify that you set the GRAPH_URL property. See Property Definitions on page 161.

2 If you are upgrading the WebSphere SPI graph package, remove the old version before installing the new version. See Task 15: Install the New Graph Package (Optional) on page 36.

3 Install the graph package.

On a Windows system running HP Performance Manager, follow these steps:

a Insert the Smart Plug-ins DVD-ROM (that contains the reporting packages) into the DVD-ROM drive, and in Windows Explorer, double-click **\OV_PM\WEBSPHERE_SPI_06.00.000\WINDOWS\HPOvSpiWbsGc-06.00.000.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, the files are already swinstalled 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>/OV_PM/WEBSPHERE_SPI_06.00.000/HPUX/
HPOvSpiWbsGc-06.00.000.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, 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>/OV_PM/WEBSPHERE_SPI_06.00.000/
SOLARIS/HPOvSpiWbsGc-06.00.000.sparc all
```

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 day following integration.

WebSphere SPI Metrics Available for Graphs

The following tables show the graphs available for mapping collected metric values. Use HP Performance Manager to view any one of the metrics included in any of these tables.

Table 5 JVM

Metric Number/Name	Metric Description
I005_JVMMemUtilPct	Percentage of heap space used in the JVM.

Table 6 Server Performance

Metric Number/Name	Metric Description
I013_ ThrdPoolPctMax	Percentage of time Number of threads in pool reached configured maximum size.
I014_ThrdPoolCrtRt	Number of threads created per minute.

Table 7 Enterprise Java Beans (EJB)

Metric Number/Name	Metric Description
I020_EJBPoolUtil	Percentage of active beans in the pool.
I022_EJBMethCallsRt	Number of EJB method calls per minute.
I024_EJBEntDatLdStRt	Number of times an EJB was written to or loaded from the database per minute.
I025_EJBPoolMissPct	Average Percentage of time a call to retrieve an EJB from the pool failed.
I026_EJBConcLives	Average Number of bean objects in the pool.

Table 8 Servlets

Metric Number/Name	Metric Description
I040_ServSessAveLife	Average lifetime of a servlet session in milliseconds.
I041_ServSessActSess	Number of sessions currently being accessed.
I042_ServInvSessRt	Number of sessions being invalidated per second.

Table 9 Web Applications

Metric Number/Name	Metric Description
I045_WebAppServReqRt	Number of requests for a servlet per second.
I047_WebAppServErrRt	Number of errors in a servlet per second.
I048_WebAppServLoad	Number of servlets currently loaded for a web application.
I049_WebAppServRelRt	Number of servlets reloaded for a web application per minute.

Table 10 JDBC

Metric Number/Name	Metric Description
I061_JDBCConPoolWait	Average number of threads waiting for a connection from connection pools
I062_JDBConPoolWtTim	Average time that a client waited for a connection in milliseconds.
I065_JDBConPoolTimRt	Number of times a client timed out waiting for a connection from the pool per minute.
I066_JDBCConPoolThru	Number of connections allocated and returned by applications per second.

Table 11 Transactions

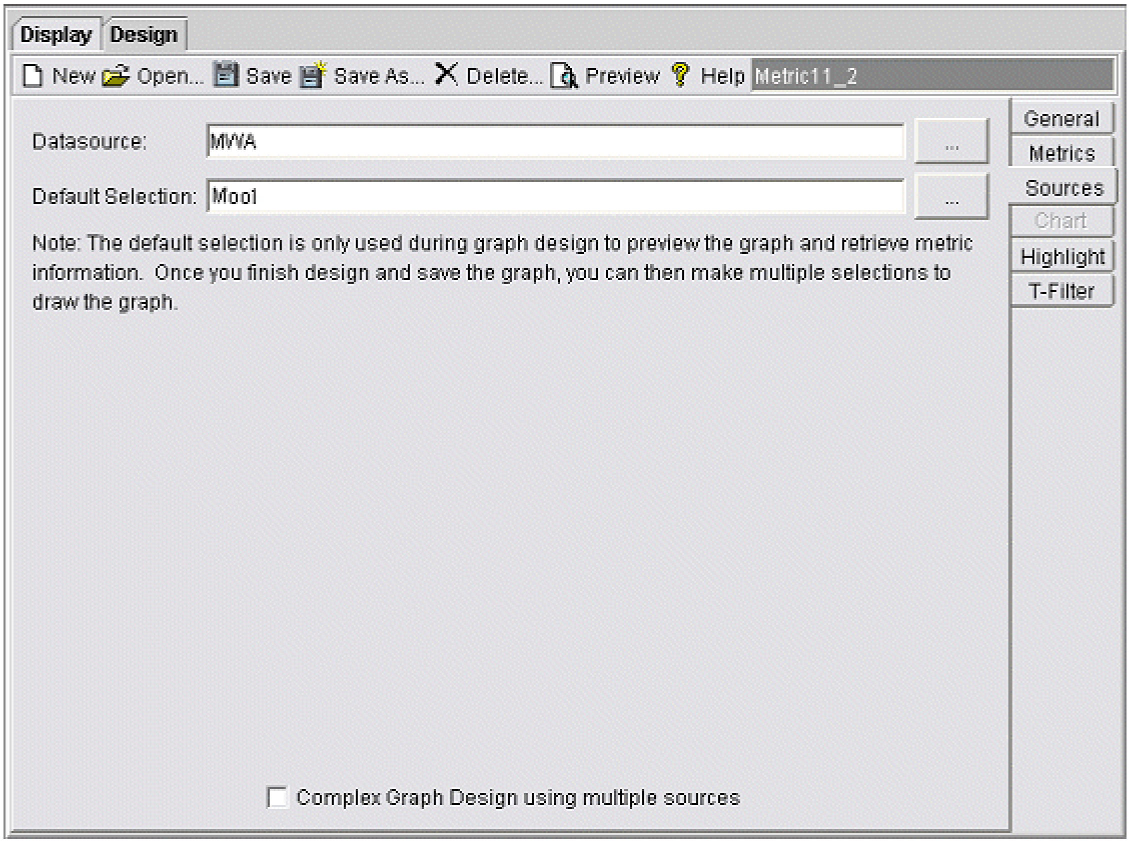
Metric Number/Name	Metric Description
I070_TranGlobDur	Average duration of global transactions.
I071_TranLocDur	Average duration of local transactions.
I072_TranGlobCommDur	Average duration of commits for global transactions.
I073_TranLocCommDur	Average duration of commits for local transactions.
I074_TranRollbackRt	Number per second of global and local transactions rolled back.
I075_TranTimeoutRt	Number per second of timed out global and local transactions.
I076_TranCommitRt	Number per second of global and local transactions that were committed.
I078_TranStartRtt	Number per second of global and local transactions that were begun.

Example Integration

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 HP Performance Manager.

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



Datasource: MWA

Default Selection: Moo1

Note: The default selection is only used during graph design to preview the graph and retrieve metric information. Once you finish design and save the graph, you can then make multiple selections to draw the graph.

☐ Complex Graph Design using multiple sources

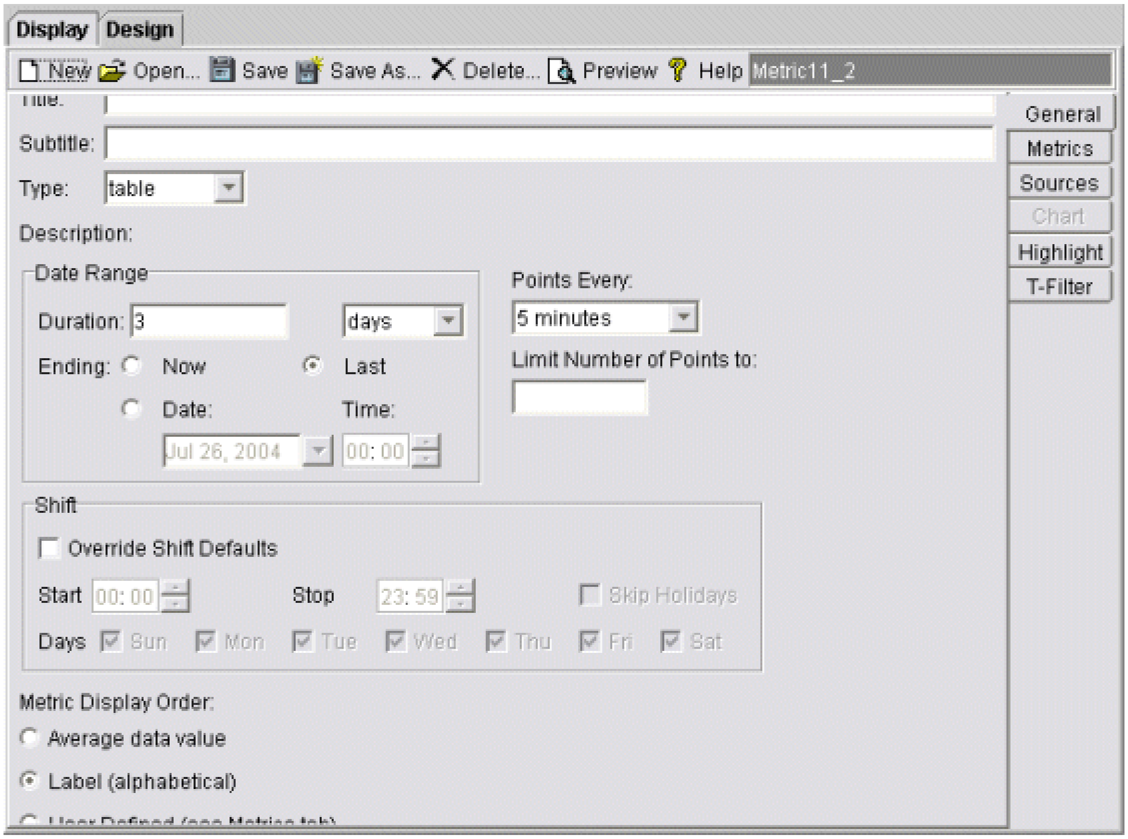
2 From the Performance Manager Java Interface window,

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.



Title:

Subtitle:

Type: table

Description:

Date Range

Duration: 3 days

Ending: ○ Now ● Last

○ Date: Jul 26, 2004 Time: 00: 00

Points Every: 5 minutes

Limit Number of Points to:

Shift

□ Override Shift Defaults

Start 00: 00 Stop 23: 59 □ Skip Holidays

Days ☑ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat

Metric Display Order:

○ Average data value

● Label (alphabetical)

○ User Defined (see Metrics tab)

4 From this window,

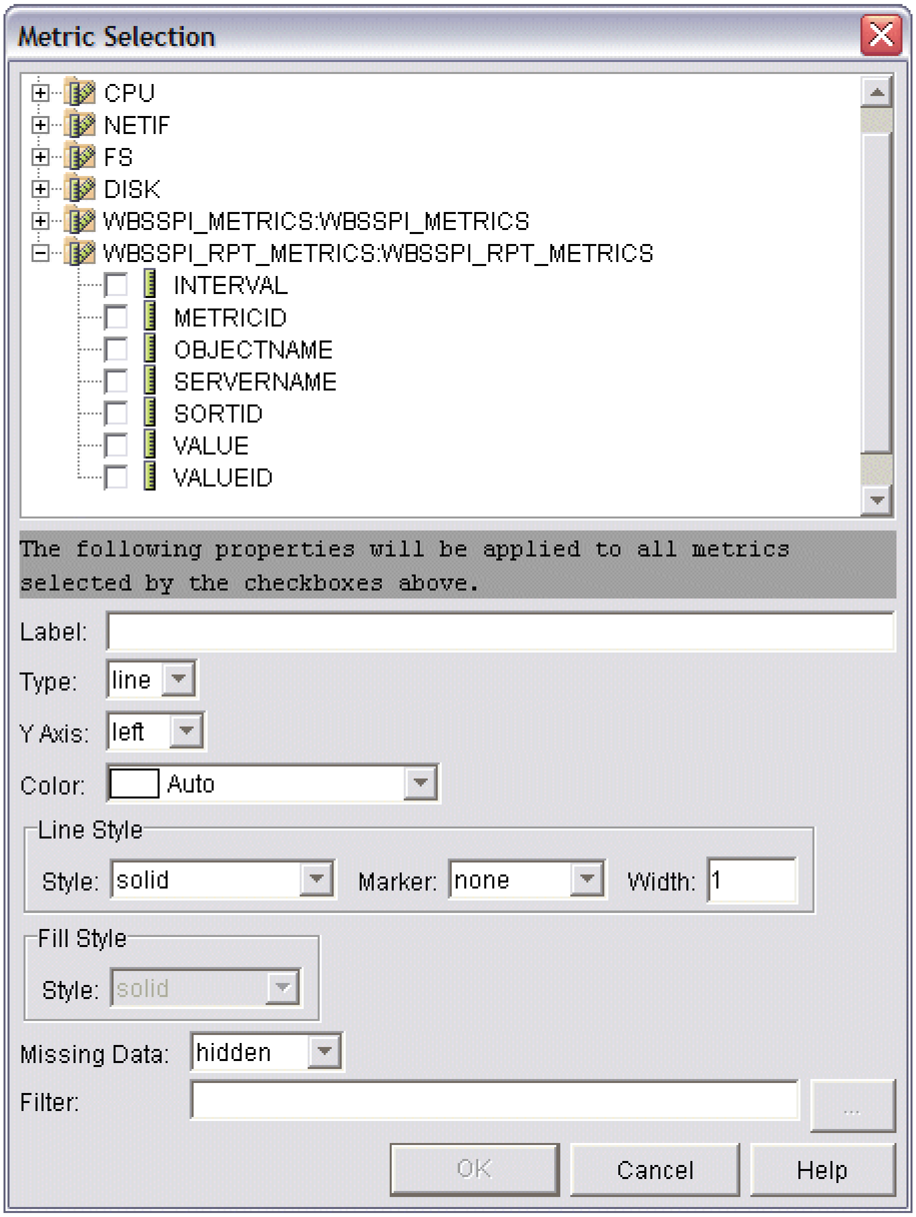
a Select **line** from the Type drop-down list. This generates a line graph.

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 opens.



The following properties will be applied to all metrics selected by the checkboxes above.

Label:

Type: line

Y Axis: left

Color: Auto

Style: solid Marker: none Width: 1

Style: solid

Missing Data: hidden

Filter:

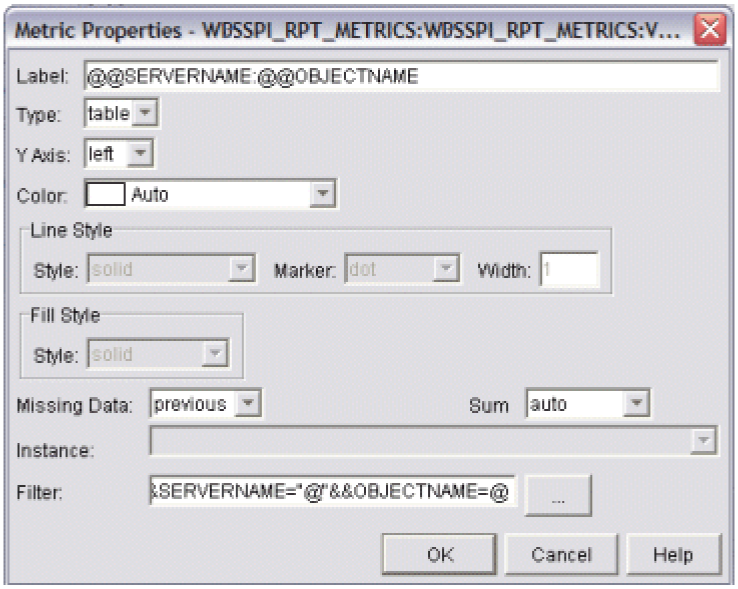
6 From the Metric Selection window,

a Next to the `WBSSPI_RPT_METRICS` data source, click **+** to expand it in the tree.

b Select the check box next to VALUE.

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 opens.



Metric Properties - WBSSPI_RPT_METRICS:WBSSPI_RPT_METRICS:V...

Label: @@SERVERNAME:@@OBJECTNAME

Type: table

Y Axis: left

Color: Auto

Line Style

Style: solid Marker: dot Width: 1

Fill Style

Style: solid

Missing Data: previous Sum auto

Instance:

Filter: &SERVERNAME="@"&&OBJECTNAME=@ ...

OK Cancel Help

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

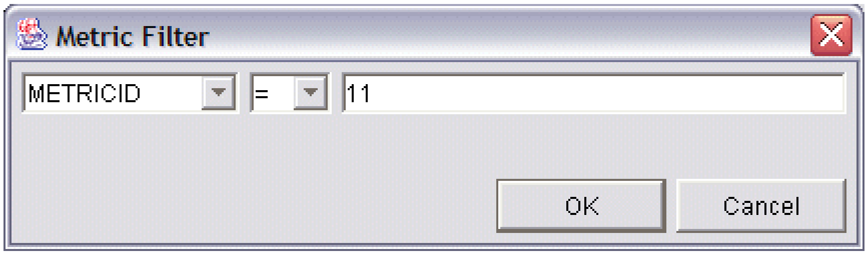
b In the Marker drop-down list, select any marker other than none.

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 opens.



Metric Filter

METRICID = 11

OK Cancel

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:

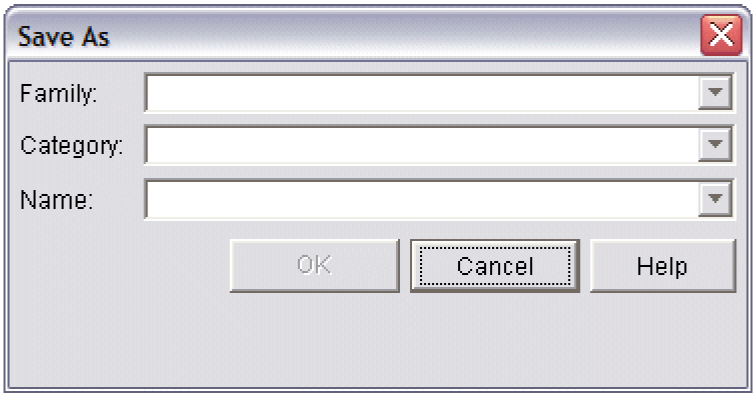
— **&&SERVERNAME=@&&OBJECTNAME=@@** if you want one graph to display all SERVERNAME/OBJECTNAME combinations.

— **&&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 opens.



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 Entering text into the Category text box is optional.

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 about this window, see the online help.

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
POINTSERVERY: 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 example above, add **`SUMFROMRAW:`** after `SYSTEMNAME: moo1`). This enables HP Performance Manager to summarized data from the data source and cannot be added using the GUI.

b If you were unable to edit the Filter text box in the Metrics Properties window in step 10, edit the FILTER field.

c Save the file. The graph file now contains the following:

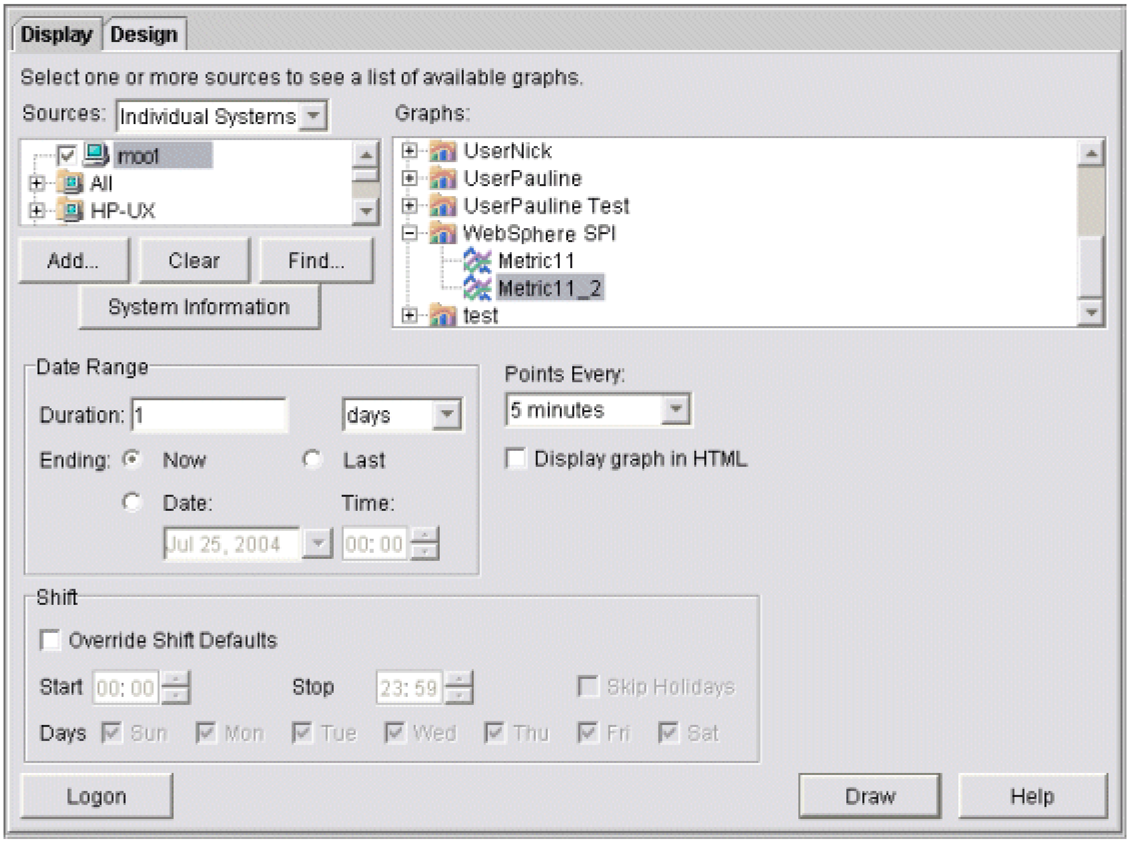
```
#*********************************************
#* OpenView Performance Manager
#* user Defined Graph Templates
#* Last Updated: 07/25/04 04:31_30 AM by [1.2.3.4] moo1
#**********************************************
FAMILY: WBSSPI_Graphs
GRAPH: Metric11
GRAPHBACKGROUND: None
DATERANGE: 1 day
GRAPHMULTIPLEGRAPHS: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



Select one or more sources to see a list of available graphs.

Sources: Individual Systems

Graphs:

Date Range

Duration: 1 days

Ending: ● Now ○ Last

○ Date: Jul 25, 2004 Time: 00:00

Points Every: 5 minutes

□ Display graph in HTML

Shift

□ Override Shift Defaults

Start 00:00 Stop 23:59 □ Skip Holidays

Days ☑ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat

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, enable graphing:

a From the HPOM console, open the Node Bank window and select a node or groups of nodes on which you want to enable graphing.

b Open the Application Bank window.

c In the Application Bank window select **WBSSPI** → **WBSSPI Admin**.

d Double-click **UDM Graph Enable**.

6 Basic Troubleshooting and Error Messages

Using the Self-Healing Info Application

The Self-Healing Info application gathers 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 application, see Self-Healing Info on page 176.

➤ The file created by the Self-Healing Info application 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 and Trace Files

Management Server

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

File Type	Log

Filename	`/`*<%OvInstallDir%>*`/wasspi/wbs/log/`
	`<managed_node>_disc_server.log`

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.

UNIX Managed Nodes

The following log and trace files are found on the managed nodes running on UNIX (typically, `/`*<OvAgentDir>*`/` is `/var/opt/OV/` or `/var/lpp/OV/`):

File Type Log

Filename /<*OvAgentDir*>`/log/javaagent.log`

Description HPOM discovery agent log file containing the status of the HPOM discovery agent. By default, logging to this file is enabled at `LOG_LEVEL` 3. Set the LOG_LEVEL variable in <*OvAgentDir*>`/conf/svcDisc/OvJavaAgent.cfg` to 6 or higher (up to 9) to capture troubleshooting information (the higher the number, the more information is collected). To disable this log, set the LOG_LEVEL to 0. Additional information can be configured in this file to define log file size and the number of archived files kept. By default, the log file size is 1MB and five archived versions are kept.

File Type Log

Directory /<*OvAgentDir*>`/log/wbsspi/config.log`

Description Records output from the WebSphere SPI configuration scripts.

File Type Log

Directory /<*OvAgentDir*>`/log/wbsspi/errorlog`

Description Records WebSphere SPI error messages. This log file is monitored by WebSphere SPI policies.

File Type Log

Directory /<*OvAgentDir*>`/log/wbsspi/discovery.log`

Description Records output from the WebSphere SPI discovery process.

File Type Trace

Filename /<*OvAgentDir*>`/log/wbsspi/discovery.trace` (archived files have a three digit number appended to the filename)

Description Discovery binary trace file used by your HP support representative. By default, tracing to this file is enabled. To disable tracing, in <*OvAgentDir*>`/bin/instrumentation/wasspi_wbs_discovery.pl`, set the $trace_on variable to 0. To enable this trace, set the $trace_on to 1. When instrumentation is deployed, the `wasspi_wbs_discovery.pl` file is overwritten (therefore, if you disable tracing, it becomes enabled when instrumentation is deployed). Five archived versions are kept. A new trace file is created when the discovery policy is run.

File Type Trace

Directory /<*OvAgentDir*>/log/wbsspi/trace.log (archived files have a three digit number appended to the filename)

Description Trace file used by your HP support representative. This file gives information about the CollectorServer, regardless of whether the Collector is set to PERSISTANT or TRANSIENT mode in the SPIConfig file. The default value of the Collector Mode is 'PERSISTENT'.

By default, tracing to this file is disabled. To enable this tracing, use the Start Tracing application.

File Type Trace

Directory /<*OvAgentDir*>/log/wbsspi/traceCollectorClient.log (archived files have a three digit number appended to the filename)

Description Trace file used by your HP support representative. This file gives information about the CollectorClient when the Collector is set to 'PERSISTENT' mode in the SPIConfig file. The default value of the Collector Mode is 'PERSISTENT'.

By default, tracing to this file is disabled. To enable this tracing, use the Start Tracing application.

Windows Managed Nodes

The following log and trace files are found on the managed nodes running on Windows (typically, <*OvDataDir*> is \Program Files\HP OpenView\Installed Packages\{790 ...}\):

File Type Log

Directory \<*OvDataDir*> \wasspi\wbs\log\config.log

Description Records output from configuration scripts.

File Type Log

Directory \<*OvDataDir*> \wasspi\wbs\log\errorlog

Description Records WebSphere SPI error messages. This log file is monitored by WebSphere SPI policies.

File Type Log

Directory \<*OvDataDir*> \wasspi\wbs\log\discovery.log

Description Records output from the WebSphere SPI discovery process.

File Type Trace

Filename `\`<*OvDataDir*>`\wasspi\wbs\log\discovery.trace` (archived files have a three digit number appended to the filename)

Description Discovery binary trace file used by your HP support representative. By default, tracing to this file is enabled. To disable tracing, in <*OvDatatDir*>`\bin\instrumentation\wasspi_wbs_discovery.pl`, set the $trace_on variable to 0. To enable this trace, set the $trace_on to 1. When instrumentation is deployed, the `wasspi_wbs_discovery.pl` file is overwritten (therefore, if you disable tracing, it becomes enabled when instrumentation is deployed). Five archived versions are kept. A new trace file is created when the discovery policy is run.

File Type Trace

Directory `\`<*OvDataDir*> `\wasspi\wbs\log\trace.log` (archived files have a three digit number appended to the filename)

Description Trace file used by your HP support representative. This file gives information about the CollectorServer, regardless of whether the Collector is set to PERSISTANT or TRANSIENT mode in the SPIConfig file. The default value of the Collector Mode is 'PERSISTENT'.

By default, tracing to this file is disabled. To enable this tracing, use the Start Tracing application.

File Type Trace

Directory `\`<*OvDataDir*>`\wasspi\wbs\log\traceCollectorClient.log` (archived files have a three digit number appended to the filename)

Description Trace file used by your HP support representative. This file gives information about the CollectorClient when the Collector is set to 'PERSISTENT' mode in the SPIConfig file. The default value of the Collector Mode is 'PERSISTENT'.

By default, tracing to this file is disabled. To enable this tracing, use the Start Tracing application.

Troubleshooting the Discovery Process

If the discovery process does not automatically discover multiple installations on a Windows managed node, set the HOME_LIST property and run the Discover WebSphere application.

If the discovery process does not automatically discover and update the WebSphere SPI configuration, follow these steps:

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 the WebSphere application server status. The application server must be running. See Task 1: Verify the Application Server Status on page 42.

4 On a Windows managed node, verify the installation directory of the server (`\Program Files\WebSphere\AppServer or \WebSphere\AppServer`). If the WebSphere application server is not installed in the default path, configure the HOME property using the non-default installation path.

5 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. If the WebSphere application server is not installed in the default path, configure the HOME property using the non-default installation path.

Operating System	Default Installation Path (UNIX)
AIX	`/usr/WebSphere/AppServer`
HP-UX, Linux, Solaris	`/opt/WebSphere/AppServer`

6 Verify that the Configure WBSSPI application is not running. Only one process can access the configuration at a time. If Configure WBSSPI is running, other processes that must access the configuration (like the discovery process) hang until the configuration becomes available.

7 Check if the HPOM management server is suppressing duplicate messages:

a From the HPOM console, select **Actions** → **Server** → **Configure**. The Configure Management Server window opens.

b Look for the “Suppress and count duplicate messages” check box. If this box is checked, uncheck it.

8 Check the `/<%OVAgentDir>/log/wbsspi/discovery.log` file for additional information.

9 Restart the HPOM management server:

a Stop all HPOM GUIs that are running by selecting **File** → **Exit**.

b Stop the HPOM management server processes. Enter:
```
/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. Enter:

```
/opt/OV/bin/OpC/opcsv -start
/opt/OV/bin/OpC/opcsv -status
```

e Restart the HPOM GUI. Enter: **opc**

Troubleshooting Applications

Problem	Configuration variable SERVER<*n*>_STOP_CMD missing for server Default Server
Solution	Before you can successfully run the Stop WebSphere application, you must set the STOP_CMD and USER properties. Set these properties using the Configure WBSSPI application. See Configure WBSSPI on page 172 for more information about this application.

Problem	Configuration variable SERVER<*n*>_START_CMD missing for server, Default Server
Solution	Before you can successfully run the Start WebSphere application, you must set the START_CMD and USER properties. Set these properties using the Configure WBSSPI application. See Configure WBSSPI on page 172 for more information about this application.

Problem	For WebSphere 6.1, Stop WebSphere application does not stop WebSphere Application Servers.
Cause	Stop WebSphere application does not work well if security is enabled in WBS and the username/password options are specified while setting the STOP_CMD property.
Workaround	Edit the <*connection type*>.client.props file on the managed node. For details see **http://www-1.ibm.com/support/docview.wss?uid=swg21142299**

Problem	When launched, the Verify application gives improper output.
Solution	Before you launch the Verify application, ensure that you installed the latest version of Self-Healing Service (SHS) component (version 2.20) from the SPI DVD. If you upgrade 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 application gives improper output.
Solution	Ensure that you installed the latest version of Self-Healing Service (SHS) component (version 2.20) from the SPI DVD. If you upgraded 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 applications, 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 application 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 application returns the server status as NOT_RUNNING (or does not give any output), turn ON the monitoring for that particular server by using the Start Monitoring application.

Problem	Datasource not getting created on RHEL 4.0 platform.
Solution	Ensure that you installed the latest version of DSI2DDF component (02.22.000) from the SPI DVD. If you upgraded WebSphere SPI without the SPI DVD, you must upgrade the DSI2DDF component also. You can download the latest DSI2DDF component from: **ftp://ovrntfs.rose.hp.com/prelim/dsi2ddf/02.22/HPUX11.00/ DSI2DDF_A.02.22.00.depot**

Error Messages

This section provides information on error messages resulting from conditions detected in the operation of the WebSphere SPI, not the WebSphere Server. The following error messages are all within the WBSSPI Message Group.

For any given problem, only the most recent error message is displayed (the older error message is automatically acknowledged). This reduces the number of error messages displayed in the message browser.

WASSPI-1

Description	Unable to create the lock file <*filename*>. File already exists.
Severity	Critical
Help Text	**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. **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 should delete this file manually.

WASSPI-2

Description	Cannot access the SPI configuration.
Severity	Critical
Help Text	**Probable Cause**: A WebSphere SPI configuration file could not be located or accessed. Either the file does not exist or there was a problem reading the file. **Suggested Action**: 1 Verify that the collector template that runs the WebSphere SPI data collector specifies the correct directory on the command line. The option `-Dwasspi.config.dir=`*`<configDirectory>`* must be specified on command line invocation of the data collector. <configDirectory> must be /var/opt/OV/conf/wbsspi on Unix platforms or \usr\OV\wasspi\wbs\conf' on Windows platforms. 2 Verify that the WebSphere SPI has been configured correctly by running the Verify utility from the Application Bank. If the configuration is not correct, run the WebSphere SPI configuration utility from the Application Bank to reinstall the files. 3 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 'View Error File' application in the Application Bank window. You can view the SPI error log for a managed node by using the 'View Error File' application in the Application Bank window. The error message can be identified by the date/time stamp.

WASSPI-3

Description	Error parsing command line.
Severity	Critical
Help Text	**Probable Cause**: The WebSphere SPI data collector command line is incorrectly specified in a schedule template. **Suggested Action**: 1 See the text following the error message in the WebSphere SPI error log to help identify the data collector command line syntax error. You can view the SPI error log for a managed node by using the View Error File application in the Application Bank window. The error message can be identified by the date/time stamp. 2 If the error occurred in a schedule template that shipped with the WebSphere SPI, reinstall the SPI and run the WebSphere SPI configuration utility from the Application Bank. 3 If the error occurred in a schedule template not shipped with the WebSphere SPI, correct the schedule template that contains the incorrect command line. See the WebSphere SPI User's Guide for more information on the WebSphere SPI data collector command line.

WASSPI-4

Description	Error getting the metric definitions.
Severity	Critical
Help Text	**Probable Cause**: The WebSphere SPI data collector could not read the metric definitions XML document. This error can be caused by a missing configuration property, an I/O error, an XML parsing error, a missing file, or a corrupted serialized data file. **Suggested Action**: 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 SPI error log for a managed node by using the 'View Error File' application in the Application Bank window. The error message can be identified by the date/time stamp. 2 If the METRIC_DEFINITIONS_FILE property is missing from the WebSphere SPI configuration file, reinstall the SPI and run the SPI configuration utility from the Application Bank. 3 If the problem is with the metric definitions file (MetricDefinitions.xml) that is shipped with the WebSphere SPI, reinstall the WebSphere SPI. Run the SPI configuration utility from the Application Bank. 4 If the problem is with a user-defined metric definitions file that is not shipped with the WebSphere SPI, verify that this XML file adheres to the MetricDefinitions.dtd specification. See the *HP Operations Manager Smart Plug-in for IBM WebSphere Application Server SPI Configuration* Guide for more information on writing user-defined metrics. Reinstall your user-defined metric definition file. Run the SPI configuration utility and verify that the UDM_DEFINITIONS_FILE property in the SPI configuration file, is specified correctly. 5 If the underlying error is `ClassNotFound`, this is an internal error. Report this to HP Support.

WASSPI-5

Description	Error processing metric <*metric_number*>.
Severity	Major
Help Text	**Probable Cause**: An error occurred while trying to collect data or perform calculations for the specified metric. **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 might also provide more information about the problem. You can view the SPI error log for a managed node by using the View Error File application in the Application Bank window. The error message can be identified by the date/time stamp.

WASSPI-6

Description	Required property *<property_name>* is missing from the WebSphere configuration.
Severity	Major
Help Text	**Probable Cause**: The specified required property is missing from the WebSphere SPI configuration file. **Suggested Action**: 1 Run the WebSphere SPI configuration utility from the Application Bank. Verify that you 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/conf/wbsspi/SiteConfig` on Unix platforms or `\usr\OV\wasspi\wbs\conf\SiteConfig` on Windows platforms) on the managed node in question.

WASSPI-7

Description	Unable to contact server <*server_name*> at url=<*URL*>, port=<*port*>.
Severity	Critical
Help Text	**Probable Cause**: The specified server is not running at the specified port. **Suggested Action**: 1 Run the WebSphere SPI configuration utility from the Application Bank. Verify that you specified the correct server name and port information for the WebSphere Servers on this managed node. 2 Verify that the properties, SERVERx_NAME and SERVERx_PORT are specified correctly in the WebSphere SPI configuration file (`/var/opt/OV/conf/wbsspi/SiteConfig` on Unix platforms or `\usr\OV\wasspi\wbs\conf\SiteConfig` on Windows platforms) on the managed node in question. 3 Verify that the WebSphere Server is running on the managed node.

WASSPI-8

Description	Error saving graphing or reporting data to file *`<file_name>`*.
Severity	Critical
Help Text	**Probable Cause**: If the error message specifies the reporting data file, the agent on the managed node might be in an inconsistent state. **Suggested Action**: Restart the agent on the managed node. **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. **Suggested Action**: 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 View Error File application in the Application Bank window. The error message can be identified by the date/time stamp. 2 Identify the steps to reproduce the problem. 3 Turn on tracing and reproduce the problem. See the *HP Operations Manager Smart Plug-in for IBM WebSphere Application Server SPI Configuration Guide* for instructions on how to turn on tracing. 4 Run the Self-Healing Info application. 5 Contact HP support with the information gathered in the previous steps.

WASSPI-9

Description	Unable to retrieve property *`<property_name>`*.
Severity	Critical
Help Text	**Probable Cause**: A required property is missing from one of the WebSphere SPI configuration files. **Suggested Action**: 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 View Error File application in the Application Bank window. The error message can be identified by the date/time stamp. 2 Run the WebSphere SPI configuration utility from the Application Bank. Verify that you 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/conf/wbsspi/SiteConfig` on Unix platforms or `\usr\OV\wasspi\wbs\conf\SiteConfig` on Windows platforms) on the managed node in question.

WASSPI-10

Description	Encountered problem accessing file *<filename>*.
Severity	Critical
Help Text	**Probable Cause**: The specified file could not be found, created, or accessed. This file could be a temporary file. **Suggested Action**: 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 SPI error log for a managed node by using the View Error File application in the Application Bank window. 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	**Probable Cause**: The number of WebSphere instances specified in the WebSphere SPI configuration file for the managed node in question is 0. **Suggested Action**: 1 Run the WebSphere SPI configuration utility from the Application Bank. Verify that you specified the correct server name and port information for the WebSphere Servers on this managed node. 2 Verify that the property, NUM_SERVERS, in the WebSphere SPI configuration file (`/var/opt/OV/conf/wbsspi/SiteConfig` on Unix platforms or `\usr\OV\wasspi\wbs\conf\SiteConfig` on Windows platforms) is set to the number of WebSphere Servers on this managed node.

WASSPI-12

Description	Command <*command*> returned error exit code <*exit code*>.
Severity	Critical
Help Text	**Probable Cause**: A command started by the WebSphere SPI collector has returned an error (non-zero) exit code. **Suggested Action**: 1 Identify the steps to reproduce the problem. 2 Turn on tracing and reproduce the problem. See the WebSphere SPI User's Guide for instructions on how to turn on tracing. 3 Run the Self-Healing Info application. 4 Contact HP support with the information gathered in the previous steps.

WASSPI-13

Description	Exception occurred while running an `opcmon` process.
Severity	Critical
Help Text	**Probable Cause**: The WebSphere SPI data collector attempted to run a process to execute an opcmon call. Either the process could not be created or was interrupted. **Suggested Action**: For UNIX systems, make sure the kernel configurable parameters `NPROC` and `MAXUPRC` are set high enough to allow process creation.

WASSPI-14

Description	Unable to find file <*file_name*>.
Severity	Critical
Help Text	**Probable Cause**: A file required by the WebSphere data collector could not be found. **Suggested Action**: 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 SPI error log for a managed node by using the View Error File application in the Application Bank window. The error message can be identified by the date/time stamp. 2 Reinstall the WebSphere SPI on the managed node. 3 Run the WebSphere SPI configuration utility from the Application Bank.

WASSPI-15

Description	Error parsing XML document <*file_name*>.
Severity	Critical
Help Text	**Probable Cause**: An error occurred while parsing the specified XML document. **Suggested Action**: 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 SPI error log for a managed node by using the View Error File application in the Application Bank window. The error message can be identified by the date/time stamp. 2 If the XML document was provided by the user, correct the document. See the *HP Operations Manager Smart Plug-in for IBM WebSphere Application Server SPI Configuration Guide* for more information about the correct format for a user-defined metric definition document. 3 If the XML document is a document that is shipped with the WebSphere SPI, run the SPI configuration utility from the Application Bank to reinstall the WebSphere SPI configuration files.

WASSPI-16

Description	A bad filter (<*filter_value*>) was specified for metric <*metric_number*>.
Severity	Major
Help Text	**Probable Cause**: A metric filter is incorrectly specified in the metric definitions XML document. **Suggested Action**: 1 If the metric is specified in an XML document that was provided by the user, correct the document. See the *HP Operations Manager Smart Plug-in for IBM WebSphere Application Server SPI Configuration Guide* for more information about the correct format for a user-defined metric definition document. 2 If the metric is a pre-defined metric that is shipped with the WebSphere SPI, run the SPI configuration utility from the Application Bank to reinstall the WebSphere SPI configuration files.

WASSPI-18

Description	Error logging to datasource <*datasource_class_name*>. Logging process returned exit code <*exit_code*>.
Severity	Warning
Help Text	**Probable Cause**: The agent on the managed node might be in an inconsistent state. **Suggested Action**: Restart the agent on the managed node. **Probable Cause**: The ddflog process started by the WebSphere SPI data collector returned a non-zero error code. **Suggested Action**: 1 Identify the steps to reproduce the problem. 2 Turn on tracing and reproduce the problem. See the *HP Operations Manager Smart Plug-in for IBM WebSphere Application Server SPI Configuration Guide* for instructions on how to turn on tracing 3 Run the Self-healing Info application. 4 Contact HP support with the information gathered in the previous steps.

WASSPI-19

Description	Encountered problem instantiating XSLT transformer with <*file_name*>.
Severity	Major
Help Text	**Probable Cause**: The XSL document that specifies the auto action report output contains errors. **Suggested Action**: 1 Reinstall the WebSphere SPI. 2 Run the WebSphere SPI configuration utility from the Application Bank.

WASSPI-20

Description	Encountered problem creating report for metric <*metric_number*>.
Severity	Major
Help Text	**Probable Cause**: An error occurred while producing a text report for the specified metric. **Suggested Action**: 1 Reinstall the WebSphere SPI. 2 Run the WebSphere SPI configuration utility from the Application Bank.

WASSPI-21

Description	Encountered problem instantiating factory implementation <*class name*>.
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 `appserver.implementation` is set to the fully qualified name of the class which implements the AppServerFactory interface. For example, if set on the java command-line: `-Dappserver.implementation=com.hp.openview.wasspi.WBSAppServerFactory`

WASSPI-22

Description	The PMI instrumentation level was changed from <*old_level*> to <*new_level*> for module <*module_name*> in server <*server_name*>.
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	**Probable Cause** An exception was encountered while preparing to monitor server <*server_name*>. **Suggested Action** 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 View Error File application in the Application Bank window. The error message can be identified by the date/time stamp. 2 Identify the steps to reproduce the problem. 3 Turn on tracing and reproduce the problem. See the *HP Operations Manager Smart Plug-in for IBM WebSphere Application Server SPI Configuration Guide* for instructions on how to turn on tracing. 4 Run the Self-healing Info application. 5 Contact HP support with the information gathered in the previous steps.

WASSPI-24

Description	Error logging in to server <*server_name*> with login <*login*>.
Severity	Critical
Help Text	**Probable Cause**: A security exception occurred while logging in to server <*server_name*>. **Suggested Action**: 1 Run the WebSphere SPI configuration utility from the Application Bank. 2 Verify that you specified the correct login and password on the managed node on which the error occurred. 3 Verify that the login has appropriate permissions.

WASSPI-25

Description	Performance monitoring service is not enabled on server <*server_name*>.
Severity	Warning
Help Text	**Probable Cause**: PMI service is not enabled on server <*server_name*>. **Suggested Action**: 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 <*server_name*> timed-out.
Severity	Major
Help Text	**Probable Cause** Depending on your configuration, either HP Performance Agent or CODA failed to exit before the time-out. **Suggested Action** 1 Restart CODA using command **`opcagt -start`**. 2 Restart HP Performance Agent using command **`mwa restart`**.

WASSPI-27

Description	RMI collector unable to process <*command*>.
Severity	Warning
Help Text	**Probable Cause** An exception was encountered while performing an rmid related operation. **Suggested Action** 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 SPI error log for a managed node by using the View Error File application in the Application Bank window. The error message can be identified by the date/time stamp. 2 Identify the steps to reproduce the problem. 3 Turn on tracing and reproduce the problem. See the *HP Operations Manager Smart Plug-in for IBM WebSphere Application Server SPI Configuration Guide* for instructions on how to turn on tracing. 4 Run the Self-healing Info application. 5 Contact HP support with the information gathered in the previous steps.

WASSPI-30

Description	Failed to start <*rmid_path*> on port <*port*>.
Severity	Critical
Help Text	**Probable Cause**: The specified path is already in use. **Suggested Action**: Run the WebSphere SPI configuration utility from the Application Bank. 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 <*command*>.
Severity	Warning

WASSPI-32

Description	Unable to retrieve metadata for mbean <*JMX-ObjectName*>.
Severity	Warning

WASSPI-33

Description	No actions matched server <*server name*>, version <*version*>.
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 <*metric id*> does not define any actions.
Severity	Warning
Help Text	**Probable Cause**: The metric ID specified with the action `-m` option does not define a JMXActions element. **Suggested Action**: Correct the action `-m` option if an incorrect metric ID was specified. Otherwise, add a JMXActions definition to the metric definition.

WASSPI-35

Description	Error executing action <*action command-line*>.
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 <*JMX objectname*> on server <*server name*>, does not expose operation <*operation name*>.
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 <*JMX objectname*> on server <*server name*>, does not expose attribute <*attribute name*> for write.
Severity	Warning
Help Text	**Probable Cause**: An action's JMXCalls element defines a write attribute exposed by the specified MBean as read-only. **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.

WASSPI-38

Description	MBean <*JMX objectname*> on server <*server name*>, does not expose attribute <*attribute name*>.
Severity	Warning
Help Text	**Probable Cause**: An action's JMXCalls element defines an attribute not exposed by the specified MBean ObjectName. **Suggested Action**: Correct the JMXCalls element or remove the attribute from the element.

WASSPI-39

Description	Error invoking operation <*operation name*> on MBean <*JMX objectname*>.
Severity	Major
Help Text	**Probable Cause**: An unexpected error occurred while invoking an operation on the specified MBean. The managed resource might have thrown an exception. **Suggested Action**: View the managed node's errorlog to determine the root cause which is logged following the error message.

WASSPI-40

Description	Error setting attribute <*attribute name*> on MBean <*JMX objectname*>.
Severity	Major
Help Text	**Probable Cause**: An unexpected error occurred while setting an attribute on the specified MBean. The managed resource might have thrown an exception. **Suggested Action**: View the managed node's errorlog to determine the root cause which is logged following the error message.

WASSPI-41

Description	Error getting attribute <*attribute name*> from MBean <*JMX objectname*>.
Severity	Major
Help Text	**Probable Cause**: An unexpected error occurred while getting an attribute from the specified MBean. The managed resource might have thrown an exception. **Suggested Action**: View the managed node's errorlog to determine the root cause which is logged following the error message.

WASSPI-42

Description	Error running command <*command*>.
Severity	Critical
Help Text	**Probable Cause** A command started by the WebSphere SPI collector reported an error. **Suggested Action** 1 Identify the steps to reproduce the problem. 2 Turn on tracing and reproduce the problem. See the WebSphere SPI User's Guide for instructions on how to turn on tracing. 3 Run the Self-healing Info application. 4 Contact HP support with the information gathered in the previous steps.

WASSPI-43

Description	Error publishing event <*event-type*>.
Severity	Major
Help Text	**Probable Cause** An unexpected error occurred while a publisher was handling a metric or collect 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 <*filename*> not found.
Severity	Critical
Help Text	**Probable Cause**: A configuration file could not be found. **Suggested Action**: Run the WebSphere SPI configuration utility from the Application Bank. Verify that the correct information was specified for the WebSphere Servers on the managed node on which the error occurred.

WASSPI-202

Description	Cannot read file <*filename*>.
Severity	Critical
Help Text	**Probable Cause**: • A file could not be opened or it could not be found. • Permissions might be incorrect or a directory might be corrupt. **Suggested Action**: 1 Run the WebSphere SPI configuration utility from the Application Bank. Verify that the correct information was specified for the WebSphere Servers on the managed node on which the error occurred. 2 Verify that the permissions are correct for the ITO user to read this file.

WASSPI-203

Description	Cannot write file <*filename*>.
Severity	Critical
Help Text	**Probable Cause**: Permissions might be incorrect, or a file or directory might be corrupt. **Suggested Action**: 1 Run the WebSphere SPI configuration utility from the Application Bank. Verify that the correct information was specified for the WebSphere Servers on the managed node on which the error occurred. 2 Verify that the permissions are correct for the ITO user to write this file.

WASSPI-204

Description	Error sending `opcmsg` <*message*>.
Severity	Critical
Help Text	**Probable Cause**: There was a problem running `opcmsg`. `opcmsg` might be missing or not have permissions to execute (ITO installation errors) or the system process table might be full. **Suggested Action**: Confirm that ITO is properly installed and deployed to the managed node. Ensure that the process table is not full. If it is, consider having the system administrator increase it.

WASSPI-205

Description	Error sending opcmon <*command*>.
Severity	Critical
Help Text	**Probable Cause**: There was a problem running `opcmon`. `opcmon` might be missing or not have permissions to execute (ITO installation errors) or the system process table might be full. **Suggested Action**: Confirm that ITO is properly installed and deployed to the managed node. Ensure that the process table is not full. If it is, consider having the system administrator increase it.

WASSPI-206

Description	Cannot read directory <*directory*>.
Severity	Critical
Help Text	**Probable Cause**: The permissions on the directory prevent the ITO user from reading it or the directory is corrupt. **Suggested Action**: Verify that the permissions are correct for the ITO user for this directory.

WASSPI-207

Description	Cannot move <*filename*> to <*filename*>.
Severity	Critical
Help Text	**Probable Cause**: 1 Insufficient permissions. 2 Insufficient disk space. 3 File table problems. **Suggested Action**: 1 Verify that the permissions are correct for the ITO user. 2 Verify that there is enough disk space to create files. 3 Run the WebSphere SPI configuration utility from the Application Bank.

WASSPI-208

Description	WBSSPI 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**: 1 Run the WebSphere SPI configuration utility from the Application Bank. Verify that you specified the correct information for the WebSphere Servers on the managed node on which the error occurred. 2 Run the Verify utility from the application band to confirm that the SPI was successfully configured.

WASSPI-209

Description	Cannot contact WebSphere Server.
Severity	Critical
Help Text	**Probable Cause**: • The server could be down or not responding. • The SPI might be configured incorrectly. **Suggested Action**: 1 Verify that WebSphere is up and running properly. 2 Run the WebSphere SPI configuration utility from the Application Bank. Verify that the correct information was specified for the WebSphere Servers on the managed node on which the error occurred.

WASSPI-210

Description	Cannot configure SPI.
Severity	Critical
Help Text	**Probable Cause**: The SPI configuration process failed. **Suggested Action**: 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 provides more information about the problem. You can view the SPI error log for a managed node by using the View Error File application in the Application Bank window. The error message can be identified by the date/time stamp. 2 Reinstall the SPI and run the WebSphere SPI configuration utility from the Application Bank.

WASSPI-211

Description	Cannot create directory <*directory*>.
Severity	Critical
Help Text	**Probable Cause**: There are insufficient permissions for the ITO user to create the directory or there is insufficient disk space. **Suggested Action**: Verify that the permissions are correct for the HPOM user for this directory. Verify that there is enough disk space.

WASSPI-213

Description	Improper parameters to program <*name*>. Usage: <*usage*>.
Severity	Critical
Help Text	**Probable Cause**: The parameters to the program are incorrect. **Suggested Action**: Correct the parameters.

WASSPI-214

Description	Cannot run program <*program name*>.
Severity	Critical
Help Text	**Probable Cause**: The program failed to run. It might be missing, permissions might be incorrect, the process table might be full. **Suggested Action**: 1 Verify that the file exists. If it is a SPI program and the file is missing, reinstall the SPI and run the WebSphere SPI configuration utility from the Application Bank. 2 Verify that the permissions are correct for the ITO user.

WASSPI-216

Description	Configuration variable <*name*> missing for server <*server_name*>.
Severity	Critical
Help Text	**Probable Cause**: A required SPI configuration variable was not found. **Suggested Action**: 1 Run the WebSphere SPI configuration utility from the Application Bank. 2 Verify that the 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 was turned off for the specified server. **Suggested Action**: Collection can be turned on by setting COLLECT = ON in the SiteConfig file in the SPI configuration directory on the managed node. The configuration directory is `/var/opt/OV/conf/wbsspi` on Unix platforms or `\usr\OV\wasspi\wbs\conf` on Windows platforms.

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**: Collection can be turned on by setting COLLECT = OFF in the SiteConfig file in the SPI configuration directory on the managed node. The configuration directory is `/var/opt/OV/conf/wbsspi` on Unix platforms or `\usr\OV\wasspi\wbs\conf` on Windows platforms.

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 ever logged to it. If it is a property file, it has not been configured. **Suggested Action**: Log files: If there have never been any entries written to the file, no action is necessary. Otherwise, run the WebSphere SPI configuration utility from the Application Bank. Property files: Run the WebSphere SPI configuration utility from the application bank.

WASSPI-222

Description	<*file_name*> is empty.
Severity	Critical
Help Text	**Probable Cause**: The specified file is empty. If it is a log file, no entries were ever logged to it, or the entries were cleaned out. If it is a property file, it is not properly configured. **Suggested Action**: If the file is a configuration file, run the WebSphere SPI configuration utility from the Application Bank.

WASSPI-223

Description	Cannot read <*file_name*>.
Severity	Critical
Help Text	**Probable Cause**: 1 A file could not be opened or it could not be found. 2 Permissions might be incorrect or a directory might be corrupt. **Suggested Action**: 1 Run the WebSphere SPI configuration utility from the Application Bank. Verify that you specified the correct information for the WebSphere Servers on the managed node on which the error occurred. 2 Verify that the permissions are correct for the ITO user to read this file.

WASSPI-224

Description	ddfcomp returned an error configuring <*name*>.
Severity	Critical
Help Text	**Probable Cause**: `ddfcomp` returned an error. This could be because neither MeasureWare nor CODA is installed on the system or because of an error configuring MeasureWare or CODA. **Suggested Action**: 1 If the performance agent is not installed, this error can be ignored. 2 Identify the steps to reproduce the problem. 3 Turn on tracing and reproduce the problem. See the *HP Operations Manager Smart Plug-in for IBM WebSphere Application Server SPI Configuration Guide* for instructions on how to turn on tracing. 4 Run the Self-healing Info application. 5 Contact HP Support with the information gathered in the previous steps.

WASSPI-225

Description	No logfiles were found. Did you run Configure WBSSPI?
Severity	Critical
Help Text	**Probable Cause**: The logfile list is empty. **Suggested Action**: Reinstall the SPI and run the WebSphere SPI configuration utility from the Application Bank.

WASSPI-226

Description	Cannot read file <*file_name*>.
Severity	Critical
Help Text	**Probable Cause**: • A file could not be opened or it could not be found. • Permissions might be incorrect or a directory might be corrupt. **Suggested Action**: 1 Run the WebSphere SPI configuration utility from the Application Bank. 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 ITO 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 a performance application is available, the SPI integrates with it. This warning indicates that none is available. **Suggested Action**: If you must have a 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	**Probable Cause**: The agent on the managed node might be in an inconsistent state. **Suggested Action**: Restart the agent on the managed node. **Probable Cause**: `ddflog` returned an error. This could be because the SPI was not properly configured to support logging performance data. **Suggested Action**: 1 Try reconfiguring the WASSPI on the node having the problem. 2 Otherwise, examine the system error message, if any, for clues to the problem. 3 Turn on tracing and reproduce the problem. See the *HP Operations Manager Smart Plug-in for IBM WebSphere Application Server SPI Configuration Guide* for instructions on how to turn on tracing. 4 Run the Self-healing Info application. 5 Contact HP Support with the information gathered in the previous steps.

WASSPI-229

Description	Cannot connect to directory <*directory-name*>
Severity	Critical
Help Text	**Probable Cause**: The directory does not exist, or the user the agent is running under does not have appropriate permissions to the directory. **Suggested Action**: 1 Run the WebSphere SPI configuration utility from the Application Bank 2 Reinstall the SPI and run the WebSphere SPI configuration.

WASSPI-230

Description	Cannot get lock <*file*> after <*time*>
Severity	Critical
Help Text	**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 it had open had been cleared. **Suggested Action**: Make sure no SPI processes are running. Manually remove the lock file.

WASSPI-231

Description	Error starting JRE <*JVM_file*>: <*message*>
Severity	Critical
Help Text	**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. **Suggested Action**: Check your JAVA_HOME or HOME variables in the SPI configuration file. Check for other errors generated at the same time. They might indicate the real cause.

WASSPI-232

Description	Server <*name*> specified on command line, but not in configuration
Severity	Critical
Help Text	**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. **Suggested Action**: 1 Specify a correct server name on the command line. 2 Run the WebSphere SPI configuration utility from the Application Bank. Verify the WebSphere Server names are correctly listed and spelled in the SPI configuration file.

WASSPI-234

Description	Error running program <*file*>, return value: <*n*>
Severity	Critical
Help Text	**Probable Cause**: The SPI attempted to run some application or auxiliary program and encountered an error doing so. The application or program is shown in the message as <*file*> and the return code from attempting to run it is shown as <*n*>. **Suggested Action**: If the application is a SPI application, make sure the SPI has been installed and configured correctly. If not, reinstall or reconfigure. If it is a system application, make sure there are no system problems that prevent the application from running.

WASSPI-235

Description	Restart of MeasureWare agents failed
Severity	Warning
Help Text	**Probable Cause**: The SPI attempted to automatically restart the MeasureWare agents and the automatic attempt failed. **Suggested Action**: Restart the MeasureWare agents manually using the **`mwa restart server`** command.

WASSPI-236

Description	Failure when running XSLT on <*xml*> with stylesheet <*xsl*>: <*message*>
Severity	Critical
Help Text	**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. **Suggested Action**: Review the message shown. It is most likely that there is an error in the XML.

WASSPI-237

Description	Setting up Data Source <*datasource*>
Severity	Normal
Help Text	This is an informational message that a HP Performance Manager or MeasureWare datasource was setup.

WASSPI-238

Description	No User Defined Metrics found
Severity	Warning
Help Text	**Probable Cause**: The UDM Graph Enable application was run, but no UDM metrics had been defined. **Suggested Action**: Check that the UDM XML file has been named correctly.

WASSPI-240

Description	UDM Data Logging integration Complete
Severity	Information
Help Text	The UDM Graph Enable application successfully executed and UDM graph metrics will be available for graphing.

WASSPI-241

Description	Cannot delete file <*file*>
Severity	Critical
Help Text	**Probable Cause**: The SPI attempted to delete a file, but was unable to do so. It might be that the protection of the file is set so that the ITO user cannot delete it, or that there is some system problem preventing the file from being deleted. **Suggested Action**: Make sure the protection of the file is correct.

WASSPI-242

Description	UDM graphing successfully disabled.
Severity	Information
Help Text	The UDM Graph Disable application successfully executed.

WASSPI-254

Description	Java exited with an error
Severity	Critical
Help Text	**Probable Cause**: While running the collector or other java application, either Java encountered an error of some kind, or the Java application exited with an error exit. **Suggested Action**: Check for other errors generated at the same time, they might indicate the real cause. Review the SPI's error log. It might give some other clues.

WASSPI-303

Description	The SPI configuration for <*node_name*> was updated by discovery in the HPOM server.
Help Text	This is a normal operation performed by the Discovery application or the WBSSPI-Discovery scheduled template action. This message is sent to inform an operator that the WBSSPI Discovery has: • Found WebSphere application servers on a managed node that were not been configured, • Found new WebSphere application servers on a configured node • Detected changes in the application servers configuration. The WBSSPI-Discovery components automatically update these changes in the SPI configuration. Review the new configuration details that are included as part of the message text and verify the information for correctness.

WASSPI-501

Description	Retrieving configuration data from the HPOM server
Help Text	This is a normal operation performed by the Discovery application or the WBSSPI-Discovery scheduled template action. Upon successful operation, the entry in the 'A' (Action) column for this message should change from R (running) to S (success). If the entry in this column changes to F (fail), the operation was not completed successfully. Select this node and run the Discovery application again. If the problem persists, see Chapter 3, Configuring the WebSphere SPI for instructions on how to manually configure the WebSphere SPI.

WASSPI-502

Description	Updating the WBSSPI configuration data with discovered information
Help Text	This is a normal operation performed by the Discovery application or the WBSSPI-Discovery scheduled template action. Upon successful operation, the entry in the 'A' (Action) column for this message should change from R (running) to S (success). If the entry in this column changes to F (fail), the operation was not completed successfully. Select this node and run the Discovery application again. If the problem persists, see Chapter 3, Configuring the WebSphere SPI for instructions on how to manually configure the WebSphere SPI.

WASSPI-503

Description	The configuration for <*node_name*> node was automatically updated by the WBSSPI Discovery ...
Help Text	This is a normal operation performed by the WBSSPI Discovery policy action. It sends this message to inform an operator that the WBSSPI Discovery either discovered WebSphere application servers on a managed node that was not configured or detected changes in the application servers configuration. The Discovery components automatically update these changes in the SPI configuration. Review the new configuration details that are included as part of the message text and verify the information for correctness. The new configuration can also be viewed by launching the WBSSPI Configure application.

WASSPI-541

Description	No running WebSphere application servers found

Help Text	**Probable Cause**: A WebSphere application server is not present (or not running) on the node. **Verification**: Verify the presence of an application server on the node, and check that the application server is running. **Suggested Action**: Create or start one or more application servers on the node. Select the node and run the Discovery application again. Make sure that all of the application servers you want to monitor are running, before the WBSSPI-Discovery template is deployed or the Discovery application is launched. Only the servers that are running will be automatically configured. NOTE: If it is confirmed that WebSphere application servers exist on the system and are in the running state, this message indicates that the WBSSPI Discovery is unable to discover the application servers. Try the followings: 1 Launch the Discovery application. 2 Select the Default Properties item corresponding to this managed node. Select the HOME_LIST property from the Select a Property to Set... menu and click **Set Property**. 3 Enter the HOME directory where WebSphere application server programs are installed on this node. If there are more than one installation instance of WebSphere, enter the `HOME` directories, separated by a semicolon. (For example, /opt/WebSphere/AppServer;/ opt/ibm/ WebSphere5/AppServer). 4 Click **Next** and complete the operation. 5 Allow the WBSSPI Discovery application to complete. (A message starting with WASSPI-303 appears in the message browser with the node name embedded in the message text). If the WBSSPI configurations are not properly updated and the application servers are not displayed on the Service Navigator's Services tree, check the WBSSPI Discovery log file called `<OvAgentDir>/log/wbsspi/discovery.log` on the managed node for any ERROR log entries.
	Probable Cause: Unsuccessful login to the secured WebSphere application server environment. **Verification**: Launch the WebSphere administrative console on the node and check if security is enabled. Also make sure that the LOGIN and PASSWORD properties for this node are present and valid in the WBSSPI configuration. Launch the Configure WBSSPI application and verify the accuracy of the information. The PASSWORD information is encrypted for security purposes. **Suggested Action**: Select the node and run the Discovery application. Set the correct LOGIN/PASSWORD properties for the node (overwrite the existing encrypted data). Allow the WBSSPI-Discovery process to run again on the selected node.

Help Text Contd.	**WebSphere Application Server Version 4** **Probable Cause**: WebSphere 4.0 AdminServer is not running on the node. **Verification**: Verify that the WebSphere 4.0 AdminServer is running by launching the administrative console on the node. **Suggested Action**: If the administrative console fails to launch on the node, start the WebSphere 4.0 AdminServer. Select the node and run the Discovery application again. Note: If problem persists, see Chapter 3, Configuring the WebSphere SPI for instructions on how to manually configure the WebSphere SPI. Note: A WebSphere 4.0 AdminServer is identified by the port number it uses. Therefore, precautions should be taken when adding or modifying configuration information. If the port number is not the default value (port 900) or if multiple instances of the AdminServer are present, make sure that correct information is entered for the specific instance of the AdminServer.

WASSPI-561

Description	Failed to communicate with the WebSphere 4 AdminServer on port: *<port_number>*
Help Text	**Probable Cause**: WebSphere 4.0 AdminServer is not running on the node. **Verification**: Verify that the WebSphere 4.0 AdminServer is running by launching the administrative console on the node. **Suggested Action**: If the administrative console fails to launch on the node, please start the WebSphere 4.0 AdminServer. Select the node and run the Discovery application again.
	Probable Cause: Unsuccessful login to the secured WebSphere application server environment. **Verification**: Launch the WebSphere administrative console on the node and check if security is enabled. Also make sure that the LOGIN and PASSWORD properties for this node are present and valid in the WBSSPI configurations. Launch the Configure WBSSPI application and verify the accuracy of the information. The PASSWORD information is encrypted for security purposes. **Suggested Action**: Select the node and run the Discovery application. Set the correct LOGIN/PASSWORD properties for the node (overwrite the existing encrypted data). Allow the WBSSPI-Discovery process to run again on the selected node. Note: If problem persists, see Chapter 3, Configuring the WebSphere SPI for instructions on how to manually configure the WebSphere SPI. Note: A WebSphere 4.0 AdminServer is identified by the port number it uses. Therefore, precautions should be taken when adding or modifying configuration information. If the port number is not the default value (port 900) or if multiple instances of the AdminServer are present, make sure that correct information is entered for the specific instance of the AdminServer.

WASSPI-562

Description	Security access failure. Missing or invalid LOGIN/PASSWORD parameter for WebSphere 4 AdminServer on port: *<port_number>*
Help Text	**Probable Cause**: The values for the LOGIN and PASSWORD properties for this node are missing from the WBSSPI configuration or incorrect information was entered. **Verification**: Launch the WebSphere administrative console on the node and check if security is enabled. Also make sure that the LOGIN and PASSWORD properties for this node are present and valid in the WBSSPI configurations. Launch the Configure WBSSPI application and verify the accuracy of the information. The PASSWORD information is encrypted for security purposes. **Suggested Action**: Select the node and run the Discovery application. Set the correct LOGIN/PASSWORD properties for the node (overwrite the existing encrypted data). Allow the WBSSPI-Discovery process to run again on the selected node. Note: If problem persists, see Chapter 3, Configuring the WebSphere SPI for instructions on how to manually configure the WebSphere SPI. Note: A WebSphere 4.0 AdminServer is identified by the port number it uses. Therefore, precautions should be taken when adding or modifying configuration information. If the port number is not the default value (port 900) or if multiple instances of the AdminServer are present, make sure that correct information is entered for the specific instance of the AdminServer.

WASSPI-563

Description	Security access failure. Invalid LOGIN/PASSWORD parameter for WebSphere 4 AdminServer on port: *<port_number>*
Help Text	**Probable Cause**: The values for the LOGIN and PASSWORD properties for this node are missing from the WBSSPI configurations, or incorrect information was entered. **Verification**: Launch the WebSphere administrative console on the node and check if security is enabled. Also make sure that the LOGIN and PASSWORD properties) for this node are present and valid in the WBSSPI configurations. Launch the Configure WBSSPI application and verify the accuracy of the information. The PASSWORD information is encrypted for security purposes. **Suggested Action**: Select the node and run the Discovery application. Set the correct LOGIN/PASSWORD properties for the node (overwrite the existing encrypted data). Allow the WBSSPI-Discovery process to run again on the selected node. Note: If problem persists, see Chapter 3, Configuring the WebSphere SPI for instructions on how to manually configure the WebSphere SPI. Note: A WebSphere 4.0 AdminServer is identified by the port number it uses. Therefore, precautions should be taken when adding or modifying configuration information. If the port number is not the default value (port 900) or if multiple instances of the AdminServer are present, make sure that correct information is entered for the specific instance of the AdminServer.

WASSPI-564

Description	Security access failure. Unable to communicate with the WebSphere 4 AdminServer on port: *<port_number>*
Help Text	**Probable Cause**: WebSphere 4.0 AdminServer is not running on the node. **Verification**: Verify that the WebSphere 4.0 AdminServer is running by launching the administrative console on the node. **Suggested Action**: If the administrative console fails to launch on the node, please start the WebSphere 4.0 AdminServer. Select the node and run the Discovery application again.
	Probable Cause: The values for the LOGIN and PASSWORD properties for this node are missing from the WBSSPI configurations, or incorrect information was entered. **Verification**: Launch the WebSphere administrative console on the node and check if security is enabled. Also make sure that the LOGIN and PASSWORD properties for this node are present and valid in the WBSSPI configurations. Launch the Configure WBSSPI application and verify the accuracy of the information. The PASSWORD information is encrypted for security purposes. **Suggested Action**: Select the node and run the Discovery application. Set the correct LOGIN/PASSWORD properties for the node (overwrite the existing encrypted data). Allow the WBSSPI-Discovery process to run again on the selected node. Note: If problem persists, see Chapter 3, Configuring the WebSphere SPI for instructions on how to manually configure the WebSphere SPI. Note: A WebSphere 4.0 AdminServer is identified by the port number it uses. Therefore, precautions should be taken when adding or modifying configuration information. If the port number is not the default value (port 900) or if multiple instances of the AdminServer are present, make sure that correct information is entered for the specific instance of the AdminServer.

WASSPI-565

Description	Security access failure. Unable to log in to the WebSphere 4 AdminServer on port: *<port_number>*
Help Text	**Probable Cause**: The values for the LOGIN and PASSWORD properties for this node are missing from the WBSSPI configurations, or incorrect information was entered. **Verification**: Launch the WebSphere administrative console on the node and check if security is enabled. Also make sure that the LOGIN and PASSWORD properties for this node are present and valid in the WBSSPI configurations. Launch the Configure WBSSPI application and verify the accuracy of the information. The PASSWORD information is encrypted for security purposes. **Suggested Action**: Select the node and run the Discovery application. Set the correct LOGIN/PASSWORD properties for the node (overwrite the existing encrypted data). Allow the WBSSPI-Discovery process to run again on the selected node. Note: If problem persists, see Chapter 3, Configuring the WebSphere SPI for instructions on how to manually configure the WebSphere SPI. Note: A WebSphere 4.0 AdminServer is identified by the port number it uses. Therefore, precautions should be taken when adding or modifying configuration information. If the port number is not the default value (port 900) or if multiple instances of the AdminServer are present, make sure that correct information is entered for the specific instance of the AdminServer.

WASSPI-571

Description	Failed to communicate with WebSphere Application Server
Help Text	**WebSphere Application Server versions 5** **Probable Cause**: A WebSphere application server is not present (or not running) on the node. **Verification**: Verify the presence of an application server on the node, and check that the application server is running. **Suggested Action**: Create or start one or more application servers on the node. Select the node and run the Discovery application again. Make sure that all of the application servers you wish to monitor are running, before the WBSSPI-Discovery template is deployed or the Discovery application is launched. Only the servers that are running will be automatically configured.
	WebSphere Application Server versions 5 **Probable Cause**: Unsuccessful login to the secured WebSphere application server environment. **Verification**: Launch the WebSphere administrative console on the node and check if security is enabled. Please also make sure that the LOGIN and PASSWORD properties for this node are present and valid in the WBSSPI configurations. Launch the Configure WBSSPI application and verify the accuracy of the information. The PASSWORD information is encrypted for security purposes. **Suggested Action**: Select the node and run the Discovery application. Set the correct LOGIN/PASSWORD properties for the node (overwrite the existing encrypted data). Allow the WBSSPI-Discovery process to run again on the selected node. Note: If problem persists, see Chapter 3, Configuring the WebSphere SPI for instructions on how to manually configure the WebSphere SPI.

WASSPI-572

Description	WebSphere Login Error - Missing Login Data
Help Text	**WebSphere Application Server versions 5** **Probable Cause**: The values for the LOGIN and PASSWORD properties for this node are missing from the WBSSPI configurations. **Verification**: Launch the WebSphere administrative console on the node and check if security is enabled. Make sure that the LOGIN and PASSWORD properties for this node are present and valid in the WBSSPI configurations. Launch the Configure WBSSPI application and verify the accuracy of the information. The PASSWORD information is encrypted for security purposes. **Suggested Action**: Select the node and run the Discovery application. Set the correct LOGIN/PASSWORD properties for the node (overwrite the existing encrypted data). Allow the WBSSPI-Discovery process to run again on the selected node. Note: If problem persists, see Chapter 3, Configuring the WebSphere SPI for instructions on how to manually configure the WebSphere SPI.

WASSPI-573

Description	WebSphere Login Error - Invalid Login Data
Help Text	**WebSphere Application Server versions 5** **Probable Cause**: The discovery application was unable to authenticate itself in a secured WebSphere Server environment. This is likely due to incorrect values for the LOGIN and PASSWORD properties being provided in the WBSSPI configurations for this node. **Verification**: Launch the WebSphere administrative console on the node and check if security is enabled. Make sure that the LOGIN and PASSWORD properties for this node are present and valid in the WBSSPI configurations. Launch the Configure WBSSPI application and verify the accuracy of the information. The PASSWORD information is encrypted for security purposes. **Suggested Action**: Select the node and run the Discovery application. Set the correct LOGIN/PASSWORD properties for the node (overwrite the existing encrypted data). Allow the WBSSPI-Discovery process to run again on the selected node. Note: If problem persists, see Chapter 3, Configuring the WebSphere SPI for instructions on how to manually configure the WebSphere SPI.

WASSPI-581

Description	INTERNAL ERROR - `<error_message>`
Help Text	**Probable Cause**: Read the error message that accompanies the message text to determine the cause of the problem. The WBSSPI Discovery application might not function properly due to one (or more) of the following conditions on the managed node: • A WBSSPI Discovery application, script, or data file is missing, has been removed, or is placed in non-standard directory paths. • There were problems with the HP agent installation. • The HP agents installation directory cannot be determined. • HPOM operator account that runs the WBSSPI Discovery does not have the permission to open/read the specified file or execute the required script/command. • General network errors. **Suggested Action:** Check with the HPOM or the IT specialist in the organization on matters related to these issues. Once the problems are resolved, select the node and run the Discovery application again. Note: If problem persists, see Chapter 3, Configuring the WebSphere SPI for instructions on how to manually configure the WebSphere SPI. Contact your HP Support representative if the problem cannot be resolved or if further assistance is needed.

WASSPI-585

Description	SYSTEM ERROR - *<error_message>*
Help Text	**Probable Cause**: Read the error message that accompanies the message text to determine the cause of the problem. The WBSSPI Discovery application might not function properly due to one (or more) of the following conditions on the managed node: • Operating system commands used by WBSSPI Discovery are missing, are removed, or placed in non-standard directory paths. • The system's PATH variable has not been set for certain system commands. • Required operating system files or software installation registry cannot be found or is in a non-standard directory path. • HPOM operator account that runs the WBSSPI Discovery does not have the permission to open/read system files or execute the necessary system commands. • General network errors. **Suggested Action**: Check with the HPOM or the IT specialist in the organization on matters related to these issues. Once the problems are resolved, select the node and run the Discovery application again. Note: If problem persists, see Chapter 3, Configuring the WebSphere SPI for instructions on how to manually configure the WebSphere SPI.

WASSPI-591

Description	WEBSPHERE ERROR - *<error_message>*
Help Text	**Probable Cause**: Read the error message that accompanies the message text to determine the cause of the problem. The WBSSPI Discovery application might not function properly due to one (or more) of the following conditions on the managed node: • WebSphere commands used by WBSSPI Discovery are missing, are removed, or placed in non-standard directory paths. • HPOM operator account that runs the WBSSPI Discovery does not have the permission to open/read files or execute commands in the WebSphere installation directories. Suggested Action: Check with the HPOM or the WebSphere application server specialist in the organization on matters related to these issues. Once the problems are resolved, select the node and run the Discovery application again. Note: If problem persists, see Chapter 3, Configuring the WebSphere SPI for instructions on how to manually configure the WebSphere SPI.

Others

Description	An unknown error appears in the WebSphere SPI error log.
Severity	Warning
Help Text	**Suggested Action**: 1 See the text following the error message in the WebSphere SPI error log to help identify the problem. You can view the SPI error log for a managed node by using the View Error File application in the Application Bank window. The error message can be identified by the date/time stamp. 2 Identify the steps to reproduce the problem. 3 Turn on tracing and reproduce the problem. See the *HP Operations Manager Smart Plug-in for IBM WebSphere Application Server SPI Configuration Guide* for instructions on how to turn on tracing. 4 Run the Self-healing Info application. 5 Contact HP Support with the information gathered in the previous steps.

A File Locations

You can find 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`

Managed Node File Locations

On Windows or UNIX managed nodes that were already running the WebSphere SPI and are being switched to a non-root HTTPS agent environment (UNIX only: if these directories do not exist, see the next table for file locations):

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

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

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

B The Configuration

This appendix contains information about the configuration structure, how to use the configuration editor, descriptions of the configuration properties, and samples of the configuration.

Structure

For examples of the configuration, see Sample Configurations on page 167. The basic structure of the configuration is (lines preceded by # are treated as comments and 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, enter the <group_name> defined by the GROUP block and define the group's common properties.

For a single node, enter 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 Server instance. When more than one WebSphere Server instance is running on a given managed node, the number <*n*> differentiates the servers. Numbering begins at "1" and each WebSphere 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 NODE <*group_name*> {<*property*>} (property defined for a group)

4 <*property*> (global property)

The Configuration Editor

Use the configuration editor to view and edit the configuration. You must update the configuration using this editor only.

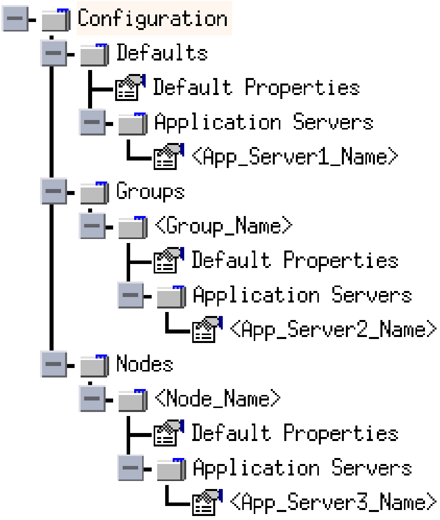
The main features of the configuration editor are the following:

Configure WBSSPI - Tree

The Configure WBSSPI tree that appears in the left pane of the Configure WBSSPI application'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 Configure WBSSPI for the first time and you did not select any nodes before you launched the application, the “Nodes” folder is not displayed.



```
Configuration
    Defaults
        Default Properties
        Application Servers
            <App_Server1_Name>
    Groups
        <Group_Name>
            Default Properties
            Application Servers
                <App_Server2_Name>
    Nodes
        <Node_Name>
            Default Properties
            Application Servers
                <App_Server3_Name>
```

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 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 148).
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 148).
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 148).

Configure WBSSPI - Buttons

The following buttons are available in Configure WBSSPI:

Button	Description
Cancel	Exit Configure WBSSPI. If you set configuration properties without saving them, these changes are not saved. If you added or removed an application server, node, or group without saving the change or if you modified 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 Configure WBSSPI. Appears instead of the **Next** button if you launched Configure WBSSPI without selecting any nodes.
Next	Exit Configure WBSSPI. Takes you to the "Confirm Operation" window that lists the nodes you selected before you started Configure WBSSPI. The selected managed nodes' configurations are updated with your changes. If you made 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 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.

Configure WBSSPI - 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 152.	Application Servers Defaults *<Group_Name>* *<Node_Name>*
Add Group	Create a group to which you can assign nodes that have common properties. See Add Group on page 154.	Any item in the tree Any item in the tree
Add Node	Add a managed node to the Nodes folder. Add Node on page 155.	Any item in the tree Any item in the tree

Action	Description	Selected Tree Item
Exit	Exit the Configure WBSSPI application. This action is available from the File menu. If any changes were made that were not saved, the Confirm Cancel window appears.	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 155.	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 155.	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 156.	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.	Any item in the tree Any item in the tree
Set Configuration Properties tab	Set WebSphere SPI configuration properties. See Set Configuration Settings Tab on page 156.	*<Application_Server_Name>* Default Properties
View Configuration Settings tab	View WebSphere SPI configuration properties. See View Configuration Settings Tab on page 157 .	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 161.

Before adding an application server,

for WebSphere Server version 4:	If the WebSphere administrative server port number is the same for all managed nodes, set the PORT property at the global properties level. If the WebSphere administrative server port number is the same for a group, set the PORT property at the GROUP level. If the WebSphere administrative server port number is the same for a node, set the PORT property at the NODE level Setting the PORT property at those levels enables you to use the "Use inherited Server Port" check box. For more information about this checkbox, see step 4. For more information about setting the PORT property, see Set Configuration Settings Tab on page 156 and Configuration Properties on page 159.
for WebSphere Server version 5, 6.0, and 6.1:	Set the PORT property to the application server's BOOTSTRAP_ADDRESS port number at the application server level of configuration (the BOOTSTRAP_ADDRESS is unique for each server on a managed node). For more information about setting the PORT property, see Set Configuration Settings Tab on page 156 and Configuration Properties on page 159.

To add an application server, follow these steps:

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 Application: Add App Server window appears.

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

3 Enter the Server Port.

For WebSphere Server version 4, this is the bootstrap port number for the WebSphere administrative server.

For WebSphere Server version 5 and above, this is the BOOTSTRAP_ADDRESS port number for the application server.

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, unselect 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, WebSphere SPI is configured to use this same port number on all nodes and groups for all WebSphere version 4 administrative servers or for all WebSphere version 5 and above application servers. For WebSphere version 5 and above, if there is more than one application server per node, only one server can use the inherited server port. The PORT property must be edited for the other application servers.

- If the PORT property is set at the GROUP level, WebSphere SPI is configured to use this same port number for the group for all WebSphere version 4 administrative servers or for all WebSphere version 5 application servers. For WebSphere version 5, if there is more than one application server per node in the group, only one server can use the inherited server port. The PORT property must be edited 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, WebSphere SPI is configured to use this same port number for that node for all WebSphere version 4 administrative servers or for all WebSphere version 5, 6.0, and 6.1 application servers. For WebSphere version 5, 6.0, and 6.1 if there is more than one application server per node, only one server can use the inherited server port. The PORT property must be edited 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. Set Configuration Settings Tab on page 156 for more information.

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, follow these steps:

1 Right-click any item in the tree and select **Add Group**.

The Configure WBSSPI Application: Add Group window opens.

2 Enter 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 is 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** pulldown list. See Set Configuration Settings Tab on page 156.

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, follow these steps:

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 pulldown menu, 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** pulldown list. See Set Configuration Settings Tab.

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, follow these steps:

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 Configure WBSSPI). In the “Confirm Cancel” window, click **Exit without Save**.

To remove ALL application servers, follow these steps:

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 Configure WBSSPI). In 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, follow these steps:

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 Configure WBSSPI). In 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, follow these steps:

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 Configure WBSSPI). In the “Confirm Cancel” window, click **Exit without Save**.

To remove ALL nodes, follow these steps:

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 Configure WBSSPI). In the “Confirm Cancel” window, click **Exit without Save**.

Set Configuration Settings Tab

Set 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, follow these steps:

1. Select a property from the “Select a Property to Set” pulldown menu.
2. Select **Set Property**. The property and an empty value filed appear in the table.
3. Click the empty value field and enter 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 opens. Enter the login and password values in this window.

For more information about individual properties, see Configuration Properties on page 159.

Modifying a Property

To modify a property (except LOGIN) in the configuration, follow these steps:

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). See Property Definitions on page 161.
4. Repeat steps 1 through 3 for each property to modify.
5. Click **Save**.

To modify the LOGIN property in the configuration, follow these steps:

1. Select LOGIN/PASSWORD from the Select a Property to add pulldown menu.
2. Select Set Property. The Set Access Info for Default Properties window opens.
3. Enter the new password and verify password.
4. Click **OK**.
5. Click **Save**.

Removing a Property

To remove a property from the configuration, follow these steps:

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**.

AUTO_DISCOVER

The AUTO_DISCOVER check box that appears near the bottom of the window sets the `AUTO_DISCOVER` property. You can only set this property by selecting or unselecting the check box.

Selecting the check box (default) causes the discovery templates (if distributed) to automatically update the WebSphere SPI configuration information in the service map and configuration. If the discovery templates are not distributed, the service map is created but not updated.

View Configuration Settings Tab

View all WebSphere SPI configuration properties set in the configuration on the HPOMHPOM 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 Configuration Settings** 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 unselecting this check box, the view shows only the configuration properties set at that level for the selected item.

Inherited properties can only be modified 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, `HOME` cannot be modified 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 12 on page 160 lists all properties by WebSphere SPI requirements, where:

Property — Name of the property.

Requirements — Lists the property requirements for specific components where:

- **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.

For a description of the property, see Configuration Properties on page 159.

Table 12 Properties Listed by WebSphere SPI Requirements

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

AUTO_DISCOVER	**Conditional** Required if you do not want the discovery templates to automatically overwrite the configuration information	**Default**: AUTO_DISCOVER check box is selected. Select the AUTO_DISCOVER check box to automatically update the WebSphere configuration information in the service map and configuration. Unselect the AUTO_DISCOVER check box if you do not want the discovery templates to automatically overwrite the configuration information.
COLLECT_ METADATA	**Conditional** Required if you want to use the MBean Explorer in the JMX Metric Builder application.	**Default**: OFF. Enter "ON" to collect metadata (MBean information) displayed by the JMX Metric Builder application. 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 `<%OvAgentDir%>\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.

Property	WebSphere SPI Requirements	Description
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` , the default port number is 8081(PM 8.10 on Unix and Windows)
HOME	**Required**	The directory where the WebSphere Server is installed. **Example**: `HOME = /opt/WebSphere/AppServer` or `HOME = C:\WebSphere\AppServer`
HOME_LIST	**Conditional** Required if the discovery process does not find multiple server installations on the same node	For Windows managed nodes only. A list of WebSphere Server installation directories, each directory separated by a semicolon. Set this property only if there are multiple installations of the WebSphere Server on a Windows managed node that the discovery process does not find. After setting this property, run the Discover WebSphere application.
JAVA_HOME	**Required** Required if using a Java version not supplied with WebSphere	The directory where Java is installed that is used by the collector. The value of JAVA_HOME must include the path to `JAVA.EXE` (path to the Bin directory of Java) and not the path to the actual JAVA_HOME directory. The java engine is expected to be $JAVA_HOME/bin/java. **Example**: `$JAVA_HOME = /opt/WebSphere/AppServer/java/bin`
JMB_JAVA_HOME	**Conditional** Required if you are using the JMX Metric Builder	The directory where Java (JDK 1.4.1 or higher) is installed that is used by the JMX Metric Builder on the HPOM management server. The JDK must be version 1.41 or higher.
JMX_CLASSPATH	**Conditional** Required if you are configuring a JMX collector	The location of the jar files implementing JMX. **Example**: `SERVER1_JMX_CLASSPATH = /JMX/Sun/lib/jmxri.jar`
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	**Conditional** Required if security is enabled on WebSphere	A WebSphere-defined user (not a system user) that is used to monitor a WebSphere Server. **Example**: `SERVER1_LOGIN = janedoe`

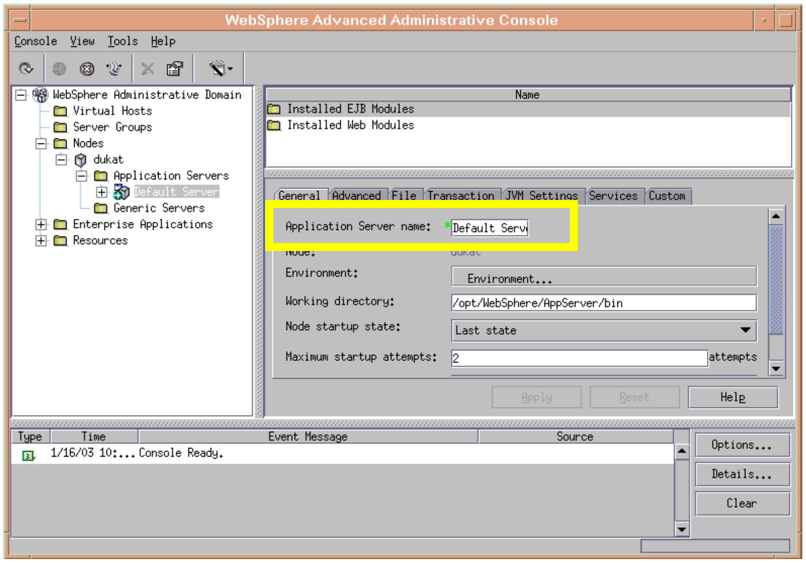
Property	WebSphere SPI Requirements	Description
MAX_ERROR_LOG_ SIZE	**Optional** Required if you want an error logfile larger than 2MB	**Default**: 2MB. The maximum number of MB allowed for the error logfile. When the error logfile reaches the maximum limit, it is renamed as a backup file and logging resumes. When a new backup file replaces an old backup file, the old backup is deleted. **Example**: MAX_ERROR_LOG_SIZE = 20
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	**Conditional** Required if security is enabled on WebSphere	The password for the WebSphere-defined user (`USER` or `SERVER<n>_USER`). **Example**: `SERVER1_PASSWORD = janedoe123`
PORT[b]	**Required**	For WebSphere Server version 4 **Default**: 900. The bootstrap port number for the WebSphere administrative server. Verify that this is the same as the port number configured in admin.config. **Example**: `SERVER1_PORT = 900`
		For WebSphere Server version 5 and above **Default**: The bootstrap 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 6.1
		For WebSphere Server version 6.0
		The directory for the application server profile: `<WebSphere_Home>/profiles/default`.
		For WebSphere Server version 6.1
		The directory for the application server profile: `<WebSphere_Home>/profiles/AppSrv01`.
		Examples:
		`PROFILE_HOME = /opt/WebSphere/AppServer/profiles/default`
		`PROFILE_HOME = C:\WebSphere\AppServer\profiles\AppSrv01`

Property	WebSphere SPI Requirements	Description
RMID_PORT	**Conditional** Required if the default port on which rmid listens is already in use	**Default**: WebSphere Application Server 4: 9243; WebSphere Application Server 5: 9242;JMX connector: 9241 The port on which rmid listens. By default, if an HPOM managed node is monitoring application servers and MBean servers using the JMX connector, the SPI uses two ports (one for the application servers and one for the MBean servers). For example, if you are monitoring a WebSphere Application Server version 5 and an MBean server, the SPI uses port 9242 and 9241. If RMID_PORT is set, the SPI uses this one port for all servers (this property cannot be set at the application server level). For example, if you are monitoring a WebSphere Application Server and an MBean server and set RMID_PORT to 9250, the SPI uses port 9250 only. **Example**: `RMID_PORT=9250`
RMID_START_ TIME	**Conditional** Required if rmid takes longer than 30 seconds to start	**Default**: 30 (seconds) The amount of time, in seconds, to wait for rmid to start before timing out. **Example**: `RMID_START_TIME=60`
START_CMD	**Conditional** Required if you want to start the WebSphere application server from the HPOM console	A system command that is run when the HPOM Application Bank Start WebSphere application is used. This command is run by `SERVER<n>_USER` which must be configured in order for the Start WebSphere application to work. 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. **Example**: `SERVER1_START_CMD = /sbin/init.d/ WebSphere start`
STOP_CMD	**Conditional** Required if you want to stop the WebSphere application server from the HPOM console	A system command that is run when the HPOM Application Bank Stop WebSphere application is used. This command is run by `SERVER<n>_USER` which must be configured in order for the Stop WebSphere application to work. **Example**: `SERVER1_STOP_CMD = /sbin/init.d/ WebSphere stop`
TIMEOUT	**Optional**	Default: 120 (seconds). The maximum amount of time, in seconds, WebSphere SPI tries to connect to WebSphere. When the specified time is exceeded, WebSphere SPI sends an alarm to the message browser indicating hat WebSphere is unavailable. If metric I002_ServerStatusRep is being collected, the unavailability of the server is logged. If no time limit is desired, set this property to -1. **Example**: `SERVER1_TIMEOUT=30`

Property	**WebSphere SPI Requirements**	**Description**
TYPE	**Conditional** Required if you are configuring a JMX collector	**Default**: websphere. The type of JMX connector server. Set to *websphere* for WebSphere Server version 5 and *ovrmi* for other JMX connector servers. **Example**: `SERVER1_TYPE=ovrmi`
UDM_DEFINITIONS_SOURCE	**Optional**	Default: `/opt/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/conf/wbsspi/udm.xml`
USER	**Conditional** Required if you want to start and/or stop the WebSphere application 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**: 4.0 0. The version number of the WebSphere Server in the format `Major#` <space> `[Minor#]` where: • `Major#` - The primary version number (for example, for example, if the version is 4.0.1 the Major# is 4.0) • `Minor#` - The secondary version number (for example, if the version is 4.0.1 the Minor# is 1). If Minor# is not specified, the default value is 0. **Example**: `SERVER1_VERSION = 4.0 1`

a. For WebSphere Server version 4, the WebSphere administrative server displays the server names of all configured application servers in a domain. Use these names when defining NAME.



Name
Installed EJB Modules
Installed Web Modules

Application Server name: Default Serv

Node: dukat

Environment: Environment...

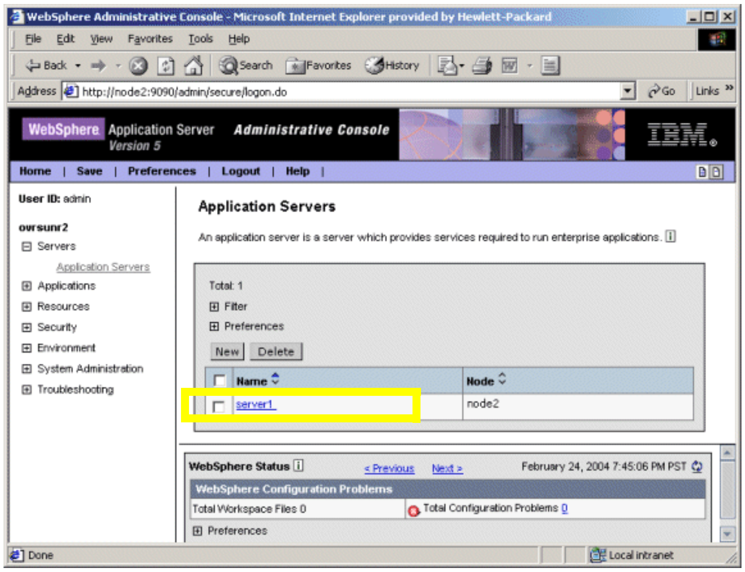
Working directory: /opt/WebSphere/AppServer/bin

Node startup state: Last state

Maximum startup attempts: 2 attempts

Type	Time	Event Message	Source
	1/16/03 10:...	Console Ready.	

For WebSphere Server version 5 and above, the WebSphere administrative console displays the server names of all configured applications servers. Use these names when defining NAME.


WebSphere Administrative Console - Microsoft Internet Explorer provided by Hewlett-Packard
File Edit View Favorites Tools Help
Back Search Favorites History
Go Links
WebSphere Application Server Version 5 Administrative Console
IBM
Home | Save | Preferences | Logout | Help |
oursunr2
Servers
Application Servers
Applications
Resources
Security
Environment
System Administration
Troubleshooting
Filter
Preferences
New
Delete
< Previous
Next >
Preferences
Done
Local intranet

Address http://node2:9090/admin/secure/logon.do

User ID: admin

Application Servers

An application server is a server which provides services required to run enterprise applications.

Total: 1

Name	Node
server1	node2

WebSphere Status February 24, 2004 7:45:06 PM PST

WebSphere Configuration Problems

Total Workspace Files 0 Total Configuration Problems 0

b. For WebSphere Server version 4, the default value configured for PORT is 900. However, if the bootstrap port number is configured in the HOME/bin/admin.config file, use the port number configured in this file. In admin.config, search for com.ibm.ejs.sm.adminServer.bootstrapPort=<nnnnn>

For WebSphere Server version 5 and above, the default value configured for PORT is the bootstrap 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

Sample Configurations

The sample WebSphere SPI configurations with entries contained 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 154.

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 155.

> 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 148.

In the example, the global default properties HOME and JAVA_HOME are overridden for 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= mypssword
}
```

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= mypssword
  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= mypssword
}
```

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 Applications

The WebSphere SPI applications include configuration and troubleshooting utilities.

WBSSPI Admin applications include:

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

WebSphere applications include:

- Check WebSphere
- Start/Stop WebSphere
- View WebSphere Logs

WBSSPI Admin Applications Group

The WBSSPI Admin applications group contains the following applications. These applications require the “root” user permission, therefore it is recommended that this group is assigned to the HPOM administrator.

Additional WBSSPI Admin applications 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 applications, see the *HP Operations Smart Plug-in for User Defined Metrics User Guide.*

Configure WBSSPI

The Configure WBSSPI application launches the configuration editor. You can use the configuration editor to maintain the WebSphere SPI configuration by viewing, editing, or setting configuration properties.

If you are configuring WebSphere SPI for the first time, use the Discover WebSphere application to automatically set basic configuration properties. For more information, see Chapter 3, Configuring the WebSphere SPI.

Function

The Configure WBSSPI application performs the following functions:

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

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 Configure WBSSPI application 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 Configure WBSSPI application otherwise the changes are saved on the management server by default.

To Launch the Configure WBSSPI Application

1. From the HPOM console, select the nodes in the Node Bank window.
2. Select **Application Bank**.
3. In the Application Bank window select **WBSSPI** → **WBSSPI Admin** → **Configure WBSSPI**. (If the items do not appear, select **Map** → **Reload**.)

   The Introduction window opens.
4. Select **Next**.

5 The configuration editor opens. For more information about using the configuration editor, see The Configuration Editor on page 149.

6 Optionally, select **Save** to save any changes made to the configuration. Once you save your changes, you cannot automatically undo them.

7 Select **Finish** or **Next** to save any changes and exit the editor.

If you selected **Next**, the Confirm Operation window opens. Select **OK**.

If you click **Cancel** in the Confirm Operation window, the changes made by you are not saved to the selected managed nodes' configuration and remain in the configuration on the management server. To make the changes to the selected managed nodes' configuration, you must select those nodes in the Node Bank window, launch the Discovery application, click **Next** in the configuration editor, and then click **OK** in the Confirm Operation window.

8 During configuration, if you added an application server or added/edited the HOME and/or PORT properties, run the Discover WebSphere application on the managed nodes on which the application server/properties were added or edited. Running the Discover WebSphere application updates the service map.

Discover WebSphere

The Discover WebSphere application sets basic configuration properties needed for discovery. It also launches the configuration editor through which you can configure the WebSphere SPI by setting initial configuration properties.

Function

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

Configuration information about the all the WebSphere Application Servers running on all managed nodes is maintained on the 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 Configure WBSSPI application 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 Configure WBSSPI application otherwise the changes are saved on the management server by default.

To Launch the Discover WebSphere Application

1 From the HPOM console, double-click **OVO Node Bank**. The OVO Node Bank window opens.

2 From the Window menu, select **Application Bank**. The OVO Application Bank window opens.

3 Select **WBSSPI** → **WBSSPI Admin** and double-click **Discovery**.
(If the above does not appear as described, select **Map** → **Reload**.)

The Introduction window opens. This window contains brief information about the Discovery application.

Select **Next**.

4 A second Introduction window opens. This window displays information about which properties might be required in order for the discovery process to work.

Read this information and select **Next**.

5 If you did not set the WebSphere SPI LOGIN and PASSWORD properties, the Configure Access Info for Default Properties window opens.

If you set the LOGIN and PASSWORD properties, the configuration editor opens. Go to the next step.

Set the LOGIN and PASSWORD properties to the WebSphere login and password configured in Task 2: Collect WebSphere Login Information on page 43. The WebSphere administrative login information is required when security is enabled. If security is not enabled, leave these fields blank, select **Next**, and go to step 9.

The LOGIN and PASSWORD properties set in this window are used as the default WebSphere administrative login and password (they are set at the global properties level). That is, if no NODE level or server-specific LOGIN and PASSWORD properties are set, this WebSphere login and password are used by WebSphere SPI for all administrative privileges. For more information about the configuration structure, see Structure on page 147.

If the WebSphere administrative login and password are the same for all WebSphere application servers on all HPOM managed nodes, follow these steps:

a Set the LOGIN and PASSWORD properties in the Set Access Info for Default Properties window.

b Select **Next**.

c Go to step 9.

If the WebSphere administrative 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 147):

a Set the LOGIN and PASSWORD properties to the most commonly used WebSphere login and password in the Set Access Info for Default Properties window.

b Select **Customize** to open the configuration editor.

6 From the configuration editor, set the configuration properties. For more information about using the configuration editor, see The Configuration Editor on page 149.

7 Select **Next** to save any changes and exit the editor.

8 The Confirm Operation window opens. Select **OK**.

➤ If you select **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 in the Node Bank window, start the Discovery application, select **Next** from the configuration editor, and then select **OK**.

Init Non-Root

The Init Non-Root application simplifies the configuration of a non-root HTTPS agent on a UNIX managed node (OVO for UNIX 8.x only). For all the steps necessary to configure a non-root HTTPS agent on a UNIX managed node see Configuring a Non-Root HTTPS Agent on a UNIX Managed Node (OVO for UNIX 8.x Only) on page 53.

Function

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

1. Runs the `wasspi_wbs_perl -S wasspi_wbs_makePlatdef -force` command to set the proper SPI path configuration and updates the `/var/opt/OV/bin/instrumentation/wasspi_wbs_platdef.pm` and `wasspi_wbs_platdef.prop` files.
2. Generates the `wasspi_wbs_sudoers` configuration file on the selected managed nodes.

To Launch the Init Non-Root Application

1. From the HPOM console, select a node in the Node Bank window.
2. From the Window menu, select **Application Bank**.
3. In the Application Bank window select **WBSSPI** → **WBSSPI Admin** → **Init Non-Root**.

Self-Healing Info

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

Required Setup

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

1. Run the Start Tracing application. For more information, see Start/Stop Tracing on page 177.
2. Reproduce the problem.

Function

Self-Healing Info application performs the following functions:

- Saves data in in the following file:
  - on a UNIX 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 application (for more information, see Verify on page 178).

To Launch the Self-Healing Info Application

1. From the HPOM console, select a node in the Node Bank window.
2. From the Window menu, select **Application Bank**.
3. In the Application Bank window select **WBSSPI** → **WBSSPI Admin** → **Self-Healing Info**.

   You can launch this application to collect data that you can send to the HP support representative.

Required Setup

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

1. Launch the Start Tracing application. For more information see Start/Stop Tracing on page 177.
2. Reproduce the problem.

Start/Stop Monitoring

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

Metrics generate alarms (when thresholds are exceeded) and you can use them to create reports (automatically or manually generated) and graphs. The reports and graphs help in analyzing trends in server usage, availability, and performance.

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.

Run the Verify application to determine if monitoring is started or stopped. By default, monitoring is on.

Function

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

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

To Launch the Start or Stop Monitoring Application

1. From the HPOM console, select a node in the Node Bank window.
2. From the Window menu, select **Application Bank**.
3. In the Application Bank window select **WBSSPI** → **WBSSPI Admin** and double-click **Start Monitoring** or **Stop Monitoring**.

Start/Stop Tracing

The Start or Stop Tracing applications allow you to start or stop gathering tracing information for the collection of metrics. Run this tool only when instructed by your HP support representative.

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

Function

The Start Tracing application saves information about the collection of metrics in a file.

The Stop Tracing application stops saving information about the collection of metrics.

To Launch the Start or Stop Tracing tools

1. From the HPOM console, select a node in the Node Bank window.
2. From the Window menu, select **Application Bank**.
3. In the Application Bank window select **WBSSPI** → **WBSSPI Admin** and double-click **Start Tracing** or **Stop Tracing**.

Verify

The Verify application enables you to verify if WebSphere SPI is installed and configured correctly on the server or managed node.

➤ Before you launch the Verify application, ensure that you installed the latest version of Self-Healing Service (SHS) component from the SPI DVD.

Function

The Verify application performs the following functions:

- On all managed nodes:
  - Checks that the following directories exist:
    - *<OV_AGT_DIR>*`/wasspi/wbs/conf/`
    - *<OV_AGT_DIR>*`/wasspi/wbs/datalog/`
    - *<OV_AGT_DIR>*`/wasspi/wbs/history/`
    - *<OV_AGT_DIR>*`/wasspi/wbs/lib/`
    - *<OV_AGT_DIR>*`/wasspi/wbs/log/`
    - *<OV_AGT_DIR>*`/wasspi/wbs/tmp/`
  - Checks that the following files exist:
    - *<OV_AGT_DIR>*`/wasspi/wbs/conf/MBeanReports.dtd`
    - *<OV_AGT_DIR>*`/wasspi/wbs/conf/MBeanReports.xsl`
    - *<OV_AGT_DIR>*`/wasspi/wbs/conf/MetricDefinitions.dtd`
    - *<OV_AGT_DIR>*`/wasspi/wbs/conf/MetricDefinitions.ser`
    - *<OV_AGT_DIR>*`/wasspi/wbs/conf/MetricMap`
    - *<OV_AGT_DIR>*`/wasspi/wbs/conf/OVTrace.sample`
    - *<OV_AGT_DIR>*`/wasspi/wbs/conf/ReportsHeader.xsl`
    - *<OV_AGT_DIR>*`/wasspi/wbs/conf/ReportsUtil.xsl`
    - *<OV_AGT_DIR>*`/wasspi/wbs/conf/SiteConfig`
    - *<OV_AGT_DIR>*`/wasspi/wbs/conf/SPIConfig`
    - *<OV_AGT_DIR>*`/wasspi/wbs/conf/SPIConfigCfgFiles`
    - *<OV_AGT_DIR>*`/wasspi/wbs/conf/SPIConfigLogFiles`
    - *<OV_AGT_DIR>*`/wasspi/wbs/conf/trigger`
    - *<OV_AGT_DIR>*`/wasspi/wbs/lib/GraphSP.xsl`
    - *<OV_AGT_DIR>*`/wasspi/wbs/lib/JspiCola.jar`
    - *<OV_AGT_DIR>*`/wasspi/wbs/lib/MetricMap.xsl`
    - *<OV_AGT_DIR>*`/wasspi/wbs/lib/xalan.jar`
    - *<OV_AGT_DIR>*`/wasspi/wbs/lib/xerces.jar`

- On Windows managed nodes:
  - Checks that the following files exist:
    - *<OV_AGT_DIR>*`\bin\OpC\cmds\wasspi_wbs_admin.exe`
    - *<OV_AGT_DIR>*`\bin\OpC\cmds\wasspi_wbs_debug.exe`
    - *<OV_AGT_DIR>*`\bin\OpC\cmds\wasspi_wbs_spiapps.exe`
    - *<OV_AGT_DIR>*`\bin\OpC\cmds\wasspi_wbs_udmgraphs.exe`
    - *<OV_AGT_DIR>*`\bin\OpC\cmds\wasspi_wbs_verify.exe`
    - *<OV_AGT_DIR>*`\bin\OpC\monitor\wasspi_wbs_ca.exe`
    - *<OV_AGT_DIR>*`\bin\OpC\monitor\wasspi_wbs_config.exe`
    - *<OV_AGT_DIR>*`\bin\OpC\monitor\wasspi_wbs_files.exe`
    - *<OV_AGT_DIR>*`\bin\OpC\monitor\wasspi_wbs_le.exe`
    - *<OV_AGT_DIR>*`\bin\OpC\monitor\wasspi_wbs_logdata.exe`
    - *<OV_AGT_DIR>*`\bin\OpC\monitor\wasspi_wbs_setpath.exe`
  - Checks that the following files exist and the version is higher than A.01:
    - *<OV_AGT_DIR>*`\bin\OpC\monitor\ddfcomp.exe`
    - *<OV_AGT_DIR>*`\bin\OpC\monitor\ddfcomp_coda.exe`
    - *<OV_AGT_DIR>*`\bin\OpC\monitor\ddflog.exe`
    - *<OV_AGT_DIR>*`\bin\OpC\monitor\ddflog_coda.exe`
    - *<OV_AGT_DIR>*`\bin\OpC\monitor\ddfutil.exe`
    - *<OV_AGT_DIR>*`\bin\OpC\monitor\ddfutil_coda.exe`
- On UNIX managed nodes:
  - Checks that the following files exist:
    - *<OV_AGT_DIR>*`/bin/OpC/cmds/wasspi_wbs_admin`
    - *<OV_AGT_DIR>*`/bin/OpC/cmds/wasspi_wbs_debug`
    - *<OV_AGT_DIR>*`/bin/OpC/cmds/wasspi_wbs_spiapps`
    - *<OV_AGT_DIR>*`/bin/OpC/cmds/wasspi_wbs_udmgraphs`
    - *<OV_AGT_DIR>*`/bin/OpC/cmds/wasspi_wbs_verify`
    - *<OV_AGT_DIR>*`/bin/OpC/monitor/wasspi_setpath`
    - *<OV_AGT_DIR>*`/bin/OpC/monitor/wasspi_wbs_ca`
    - *<OV_AGT_DIR>*`/bin/OpC/monitor/wasspi_wbs_config`
    - *<OV_AGT_DIR>*`/bin/OpC/monitor/wasspi_wbs_config.pl`
    - *<OV_AGT_DIR>*`/bin/OpC/monitor/wasspi_wbs_files`
    - *<OV_AGT_DIR>*`/bin/OpC/monitor/wasspi_wbs_le`
    - *<OV_AGT_DIR>*`/bin/OpC/monitor/wasspi_wbs_lib.pl`
    - *<OV_AGT_DIR>*`/bin/OpC/monitor/wasspi_wbs_logdata`
    - *<OV_AGT_DIR>*`/bin/OpC/monitor/wasspi_xterm`

- Checks that the following files exist and the version is higher than A.01:
  - *<OV_AGT_DIR>*`/bin/OpC/monitor/ddfcomp`
  - *<OV_AGT_DIR>*`/bin/OpC/monitor/ddfcomp_coda`
  - *<OV_AGT_DIR>*`/bin/OpC/monitor/ddflog`
  - *<OV_AGT_DIR>*`/bin/OpC/monitor/ddflog_coda`
  - *<OV_AGT_DIR>*`/bin/OpC/monitor/ddfutil`
  - *<OV_AGT_DIR>*`/bin/OpC/monitor/ddfutil_coda`

In this instance, *`<OV_AGT_DIR>`* is `/var/opt/OV` on a UNIX managed node and on a Windows managed node it depends on the installation of the product.

To Launch the Verify Application

1. From the HPOM console, select a node in the Node Bank window.
2. From the Window menu, select **Application Bank**.
3. In the Application Bank window select **WBSSPI** → **WBSSPI Admin** and double-click **Verify**.

   If the Verify application is successful, the following message appears:

   ```
   Installation is clean
   ```

View Error File

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

Function

The View Error File application enables you to view the contents of the WebSphere SPI error log file `<OV_AGT_DIR>/wasspi/wbs/log/`errorlog where `<OV_AGT_DIR>` typically is:

- `/var/opt/OV` on UNIX managed nodes
- `/Program Files/HP OpenView/Installed Packages/`
  `{790 ...}` on Windows managed nodes

To Launch the View Error File Application

1. From the HPOM console, select a node in the Node Bank window.
2. From the Window menu, select **Application Bank**.
3. In the Application Bank window select **WBSSPI** → **WBSSPI Admin** and double-click **View Error File**.

View Graphs

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

Required Setup

To run this application successfully, install the HP Performance Manager and edit the `ovweb.conf` file. For more information, see Task 1: Configure the Management Server to Launch Your Web Browser on page 37.

If your browser is Netscape Navigator, use version 6.0 or higher. Do not use Netscape Navigator 4.79 with this application.

Function

The View Graphs application launches a web browser to display WebSphere SPI metric data graphed using HP Performance Manager.

To Launch the View Graphs Application

1. From the HPOM console, select a node in the Node Bank window.
2. From the Window menu, select **Application Bank**.
3. In the Application Bank window select **WBSSPI** → **WBSSPI Admin** → **View Graphs**.

WebSphere Applications Group

The WebSphere Applications Group includes the following applications.

Check WebSphere

The Check WebSphere application 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 application 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 this 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.

To Launch the Check WebSphere Application

1 From the HPOM console, select a node in the Node Bank window.

2 From the Window menu, select **Application Bank**.

3 In the Application Bank window select **WBSSPI** → **WebSphere** and double-click **Check WebSphere**.

Start/Stop WebSphere

The Start and Stop WebSphere applications starts or stop a WebSphere application server from the HPOM console. You can start or stop one or more WebSphere Application servers on the selected managed nodes without logging in to each WebSphere Administration Server.

Required Setup

The START_CMD, STOP_CMD, and USER configuration properties *must* be set before launching these applications.

Function

The Start and Stop WebSphere applications start or stop one or all application servers on the selected managed nodes.

To Launch Start/Stop WebSphere

1. From the HPOM console, select a node in the Node Bank window.
2. From the Window menu, select **Application Bank**.
3. In the Application Bank window select **WBSSPI** → **WebSphere** and double-click **Start WebSphere** or **Stop WebSphere**. The START WBS or STOP WBS window opens.
4. Select the server you want to start/stop from the options given.

View WebSphere Logs

The View WebSphere Logs application enables you 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 application performs the following functions:

- When you launch the View WebSphere Logs application without a parameter, the applications returns a numbered list of available log files for the selected managed node.
- When you launch the View WebSphere Logs application 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 application 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 application returns the contents of the corresponding log file for the managed node.

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

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

To Launch the View WebSphere Logs Application

1. From the HPOM console, select a node in the Node Bank window.
2. From the Window menu, select **Application Bank**.
3. In the Application Bank window select **WBSSPI** → **WebSphere** and double-click **View WebSphere Logs**.
4. Select the managed nodes on which you want to view the WebSphere Server log file.
5. Select **Launch**. The Edit Parameters window appears. If you know the number of the log file you want to view, enter it into the Parameters field. Otherwise, leave this field blank to list available log files to view.
6. Select **Launch**. The Application Status window opens.
7. In the Launched Applications field, check the Status of the application for each node:
   - Started/Starting - The application is running.
   - Succeeded - A list of available log files to view appears. Highlight the node in the Launched Applications field and scroll through the Application Output field to view the list of available log files.
   - Failed - The application did not succeed. Highlight the node in the Launched Applications field and scroll through the Application Output field for more information about the problem.
8. Double-click **View WebSphere Logs**.
9. Select the managed nodes on which you want to view the WebSphere Server log file.
10. Select **Launch**. The Edit Parameters window appears.
11. In the Parameters text box, enter the number of the log file you want to view. Only one log file can be selected.

    If you do not remember the number of the log file, go to the Application Status window, highlight the node in the Launched Applications field, scroll through the Application Output filed to view the list of available log files, and enter the number of the log file you want to view in the Edit Parameters window.
12. Select **Launch**.
13. In the Application Status window, highlight the node on which to view the selected log file and scroll through the Application Output filed to view the log file.
14. Repeat steps 8-11 for each log file you want to view.
15. Select **Close** to close the Application Status window.

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

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: